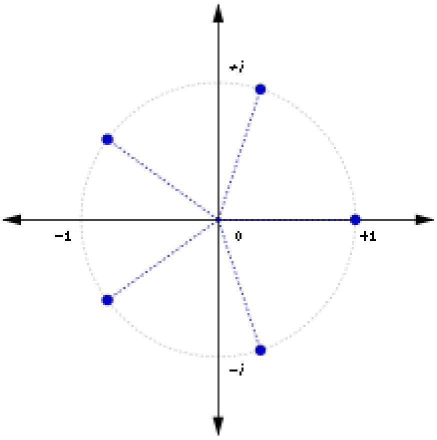
WIKIPEDIA

Root of unity

In mathematics, a **root of unity**, occasionally called a de Moivre number, is any complex number that gives 1 when raised to some positive integer power n. Roots of unity are used in many branches of mathematics, and are especially important in number theory, the theory of group characters, and the discrete Fourier transform



The 5th roots of unity in thecomplex plane

In field theory and ring theory the notion of root of unity also applies to any ring with a multiplicative identity element. Any algebraically closed field has exactly n nth roots of unity if n is not divisible by the characteristic of the field.

Contents

General definition

An ***n*th root of unity**, where n is a positive integer (i.e. $n = 1, 2, 3, \ldots$), is a number z satisfying the equation[1][2]

$$z^n = 1.$$

Unless otherwise specified, the roots of unity may be taken to be complex numbers (including the number 1, and the number –1 if n is even, which are complex with a 0 coefficient in the imaginary part), and in this case, the nth roots of unity are

$$\exp\left(\frac{2k\pi i}{n}\right) = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}, \qquad k = 0, 1, \ldots, n-1.$$

Subsequent sections of this article will comply with this. However the defining equation of roots of unity is meaningful over any field (and even over any unital ring) F, and this allows considering roots of unity in F. Whichever is the field F, the roots of unity in F are either complex numbers, if the characteristic of F is 0, or, otherwise, belong to a finite field. Conversely, every nonzero element in a finite field is a root of unity in that field. See Root of unity modulo n and Finite field for further details.

An nth root of unity is **primitive** if it is not a kth root of unity for some smaller k:

$$z^k \neq 1 \qquad (k = 1, 2, 3, \ldots, n-1).$$

If n is a prime number, all nth roots of unity, except 1, are primitive.

Elementary properties

Every nth root of unity z is a primitive ath root of unity for some a where $1 \le a \le n$. In fact, if $z^1 = 1$ then z is a primitive first root of unity, otherwise if $z^2 = 1$ then z is a primitive second (square) root of unity, otherwise, ..., and, as z is a root of unity, one eventually finds a first a such that $z^a = 1$.

If z is an nth root of unity and $a \equiv b \pmod{n}$ then $z^a = z^b$. In fact, by the definition of congruence, $a = b + kn$ for some integer k, and

$$z^a = z^{b+kn} = z^b z^{kn} = z^b (z^n)^k = z^b 1^k = z^b.$$

Therefore, given a power z^a of z, it can be assumed that $1 \le a \le n$. This is often convenient.

Any integer power of an nth root of unity is also an nth root of unity:

$$(z^k)^n = z^{kn} = (z^n)^k = 1^k = 1.$$

Here k may be negative. In particular, the reciprocal of an nth root of unity is its complex conjugate, and is also an nth root of unity:

$$\frac{1}{z} = z^{-1} = z^{n-1} = \bar{z}.$$

Let z be a primitive nth root of unity. Then the powers $z, z^2, \ldots, z^{n-1}, z^n = z^0 = 1$ are all distinct. Assume the contrary that $z^a = z^b$ where $1 \le a < b \le n$. Then $z^{b-a} = 1$. But $0 < b - a < n$, which contradicts z being primitive.

Since an nth-degree polynomial equation can only have n distinct roots, this implies that the powers of a primitive root z, $z^2, \ldots, z^{n-1}, z^n = z^0 = 1$ are all of the nth roots of unity.

From the preceding, it follows that if z is a primitive nth root of unity:

$$z^a = z^b \iff a \equiv b \pmod{n}.$$

If z is not primitive there is only one implication:

$$a \equiv b \pmod{n} \implies z^a = z^b.$$

An example showing that the converse implication is false is given by:

$$n = 4, \quad z = -1, \quad z^2 = z^4 = 1, \quad 2 \not\equiv 4 \pmod{4}.$$

Let z be a primitive nth root of unity and let k be a positive integer. From the above discussion, z^k is a primitive ath root of unity for some a. Now if $z^{ka} = 1$, ka must be a multiple of n. The smallest number that is divisible by both n and k is their least common multiple, denoted by $\operatorname{lcm}(n, k)$. It is related to their greatest common divisor, $\gcd(n, k)$, by the formula:

$$kn = \gcd(k,n)\ \operatorname{lcm}(k,n),$$

i.e.

$$\operatorname{lcm}(k,n) = k\frac{n}{\gcd(k,n)}.$$

Therefore, z^k is a primitive ath root of unity where

$$a = \frac{n}{\gcd(k,n)}.$$

Thus, if k and n are coprime, z^k is also a primitive nth root of unity, and therefore there are $\varphi(n)$ (where φ is Euler's totient function) distinct primitive nth roots of unity. (This implies that if n is a prime number, all the roots except $+1$ are primitive.)

In other words, if $\mathrm{R}(n)$ is the set of all nth roots of unity and $\mathrm{P}(n)$ is the set of primitive ones, $\mathrm{R}(n)$ is a disjoint union of the $\mathrm{P}(n)$:

$$\mathrm{R}(n) = \bigcup_{d\,|\,n} \mathrm{P}(d),$$

where the notation means that d goes through all the divisors of n, including 1 and n.

Since the cardinality of $\mathrm{R}(n)$ is n, and that of $\mathrm{P}(n)$ is $\varphi(n)$, this demonstrates the classical formula

$$\sum_{d\,|\,n} \varphi(d) = n.$$

Group properties

Group of all roots of unity

The product and the multiplicative inverse of two roots of unity are also roots of unity. In fact, if $x^m = 1$ and $y^n = 1$, then $(x^{-1})^m = 1$, and $(xy)^k = 1$, where k is the least common multiple of m and n.

Therefore, the roots of unity form an abelian group under multiplication. This group is the torsion subgroup of the circle group

Group of nth roots of unity

The product and the multiplicative inverse of two nth roots of unity are also nth roots of unity. Therefore, the nth roots of unity form a group under multiplication.

Given a primitive nth root of unity ω, the other nth roots are powers of ω. This means that the group of the nth roots of unity is a cyclic group. It is worth remarking that the term of *cyclic group* originated from the fact that this group is a subgroup of the circle group.

Galois group of the primitive nth roots of unity

Let $\mathbb{Q}(\omega)$ be the field extension of the rational numbers generated over $\mathbb{Q}$ by a primitive nth root of unity. As every nth root of unity is a power of ω, the field $\mathbb{Q}(\omega)$ contains all nth roots of unity.

If k is an integer, ω^k is a primitive nth root of unity if and only if k and n are coprime. In this case, the map

$$\omega \mapsto \omega^k$$

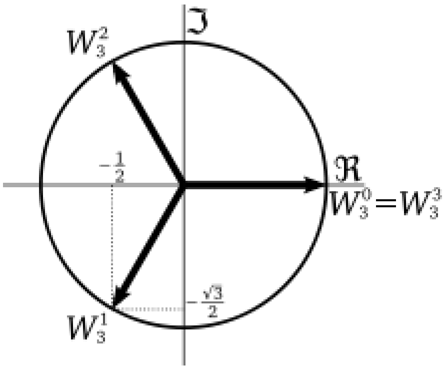
induces an automorphism of $\mathbb{Q}(\omega)$, which maps every nth root of unity to its kth power. Every automorphism of $\mathbb{Q}(\omega)$ is obtained in this way, and these automorphisms form the Galois group of $\mathbb{Q}(\omega)$ over the field of the rationals.

The rules of exponentiation imply that the composition of two such automorphisms is obtained by multiplying the exponents. It follows that the map

$$k \mapsto \left(\omega \mapsto \omega^k\right)$$

defines a group isomorphism of the units in the ring of integers modulo n onto the group of automorphisms of $\mathbb{Q}(\omega)$.

Trigonometric expression



The 3rd roots of unity

De Moivre's formula, which is valid for all real x and integers n, is

$$(\cos x + i \sin x)^n = \cos nx + i \sin nx.$$

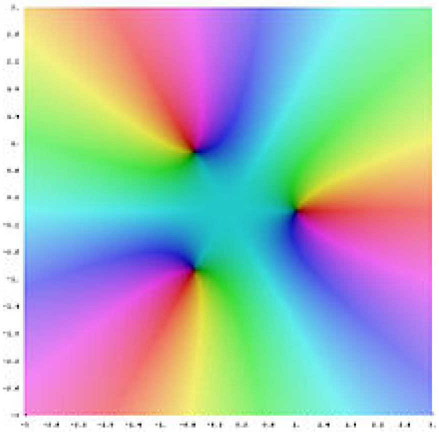
Setting $x = \frac{2\pi}{n}$ gives a primitive nth root of unity:

$$\left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}\right)^n = \cos 2\pi + i \sin 2\pi = 1,$$

but for $k = 1, 2, \ldots, n - 1$,

$$\left(\cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}\right)^k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \neq 1,$$

satisfying the criterion for primitivity. Here the real term and the coefficient in the imaginary term are trigonometric numbers



Plot of $z^3 - 1$, in which a zero is represented by the color black. See Domain coloring for interpretation.

This formula shows that on the complex plane the nth roots of unity are at the vertices of a regular n-sided polygon inscribed in the unit circle, with one vertex at 1. (See the plots for $n = 3$ and $n = 5$ on the right.) This geometric fact accounts for the term "cyclotomic" in such phrases as cyclotomic field and cyclotomic polynomial; it is from the Greek roots "cyclo" (circle) plus "tomos" (cut, divide).

Euler's formula

$$e^{ix} = \cos x + i \sin x,$$

which is valid for all real x, can be used to put the formula for the nth roots of unity into the form

$$e^{2\pi i \frac{k}{n}} \qquad 0 \leq k < n.$$

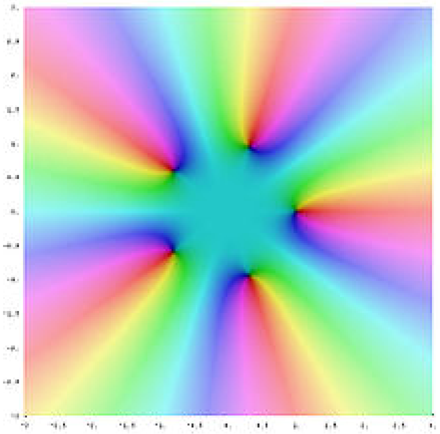
It follows from the discussion in the previous section that this is a primitive nth-root if and only if the fraction $\frac{k}{n}$ is in lowest terms, i.e. that k and n are coprime.

Algebraic expression

The nth roots of unity are, by definition, the roots of the polynomial $x^n - 1$, and are thus algebraic numbers. As this polynomial is not irreducible (except for $n = 1$), the primitive nth roots of unity are roots of an irreducible polynomial of lower degree, called the cyclotomic polynomial, and often denoted Φ_n. The degree of Φ_n is given by Euler's totient function, which counts (among other things) the number of primitive nth roots of unity. The roots of Φ_n are exactly the primitive nth roots of unity.

Galois theory can be used to show that cyclotomic polynomials may be conveniently solved in terms of radicals. (The trivial form $\sqrt[n]{1}$ is not convenient, because it contains non-primitive roots, such as 1, which are not roots of the cyclotomic polynomial, and because it does not give the real and imaginary parts separately.) This means that, for each positive integer n, there exists an expression built from integers by root extractions, additions, subtractions, multiplications, and divisions (nothing else), such that the primitive nth roots of unity are exactly the set of values that can be obtained by choosing values for the root extractions (k possible values for a kth root). (For more details see § Cyclotomic fields, below.)

For $n = 1$, the cyclotomic polynomial is $\Phi_1(x) = x - 1$ Therefore, the only primitive first root of unity is 1, which is a non-primitive nth root of unity for every n greater than 1.


Plot of $z^5 - 1$, in which a zero is represented by the color black.

We have $\Phi_2(x) = x + 1$. Thus −1 is the only primitive second (square) root of unity, which is also a non-primitive nth root of unity for every even $n > 2$.

The only real roots of unity are 1 and −1; all the others are non-real complex numbers.

We have $\Phi_3(x) = x^2 + x + 1$. Thus the primitive third (cube) roots of unity are the roots of this quadratic polynomial and are

$$\frac{-1 + i\sqrt{3}}{2}, \frac{-1 - i\sqrt{3}}{2}.$$

As $\Phi_4(x) = x^2 + 1$, the two primitive fourth roots of unity are i and $-i$.

As $\Phi_5(x) = x^4 + x^3 + x^2 + x + 1$, the four primitive fifth roots of unity are the roots of this quartic polynomial, which may be explicitly solved in terms of radicals, giving the roots

$$\left\{ \frac{u\sqrt{5} - 1}{4} + v\,i\,\frac{\sqrt{10 + 2u\sqrt{5}}}{4} \;\middle|\; u, v \in \{-1, 1\} \right\}.$$

As $\Phi_6(x) = x^2 - x + 1$, there are two primitive sixth roots of unity, which are the negatives (and also the square roots) of the two primitive cube roots:

$$\left\{ \frac{1 + i\sqrt{3}}{2}, \frac{1 - i\sqrt{3}}{2} \right\}.$$

Gauss proved that a primitive nth root of unity can be expressed using only square roots, addition, subtraction, multiplication and division if and only if it is possible to construct with compass and straightedge the regular n-gon. This is the case if and only if n is either a power of two or the product of a power of two and Fermat primes that are all different.

As 7 is not a Fermat prime, the seventh roots of unity are the first that require cube roots. There are 6 primitive seventh roots of unity; thus their computation involves solving a cubic polynomial, and therefore computing a cube root. The three real parts of these primitive roots are the roots of a cubic polynomial; thus they may be expressed in terms of square and cube roots. However, as these three roots are real, we are in the case of casus irreducibilis, and any expression of these real parts in terms of radicals necessarily involves a nonreal complex number

As $\Phi_8(x) = x^4 + 1$, the four primitive eighth roots of unity are the square roots of the primitive fourth roots $\pm i$. They are thus

$$\pm\frac{\sqrt{2}}{2} \pm i\frac{\sqrt{2}}{2}.$$

See heptadecagon for the real part of a 17th root of unity

Periodicity

If z is a primitive nth root of unity, then the sequence of powers

$$\dots, z^{-1}, z^0, z^1, \dots$$

is n-periodic (because $z^{j+n} = z^j \cdot z^n = z^j \cdot 1 = z^j$ for all values of j), and the n sequences of powers

$$s_k\colon \dots, z^{k\cdot(-1)}, z^{k\cdot 0}, z^{k\cdot 1}, \dots$$

for $k = 1, \dots, n$ are all n-periodic (because $z^{k\cdot(j+n)} = z^{k\cdot j}$). Furthermore, the set $\{s_1, \dots, s_n\}$ of these sequences is a basis of the linear space of all n-periodic sequences. This means that *any* n-periodic sequence of complex numbers

$$\dots, x_{-1}, x_0, x_1, \dots$$

can be expressed as a linear combination of powers of a primitive nth root of unity:

$$x_j = \sum_k X_k \cdot z^{k\cdot j} = X_1 z^{1\cdot j} + \cdots + X_n \cdot z^{n\cdot j}$$

for some complex numbers $X_1, \dots, X_n$ and every integer j.

This is a form of Fourier analysis. If j is a (discrete) time variable, then k is a frequency and X_k is a complex amplitude.

Choosing for the primitive nth root of unity

$$z = e^{\frac{2\pi i}{n}} = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

allows x_j to be expressed as a linear combination of $\cos$ and $\sin$:

$$x_j = \sum_k A_k \cos\frac{2\pi jk}{n} + \sum_k B_k \sin\frac{2\pi jk}{n}.$$

This is a discrete Fourier transform

Summation

Let $\mathrm{SR}(n)$ be the sum of all the nth roots of unity, primitive or not. Then

$$\mathrm{SR}(n) = \begin{cases} 1, & n = 1 \\ 0, & n > 1. \end{cases}$$

For $n = 1$ there is nothing to prove. For $n > 1$, it is "intuitively obvious" from the symmetry of the roots in the complex plane. For a rigorous proof, let z be a primitive nth root of unity. Then the set of all roots is given by z^k, $k = 0, 1, \dots, n-1$, and their sum is given by the formula for a geometric series:

$$\sum_{k=0}^{n-1} z^k = \frac{z^n - 1}{z - 1} = 0.$$

Let $\operatorname{SP}(n)$ be the sum of all the primitive$n$th roots of unity. Then

$$\operatorname{SP}(n) = \mu(n),$$

where $\mu(n)$ is the Möbius function.

In the section Elementary facts, it was shown that if $\operatorname{R}(n)$ is the set of all nth roots of unity and $\operatorname{P}(n)$ is the set of primitive ones, $\operatorname{R}(n)$ is a disjoint union of the$\operatorname{P}(n)$:

$$\operatorname{R}(n) = \bigcup_{d\,|\,n} \operatorname{P}(d),$$

This implies

$$\operatorname{SR}(n) = \sum_{d\,|\,n} \operatorname{SP}(d).$$

Applying the Möbius inversion formulagives

$$\operatorname{SP}(n) = \sum_{d\,|\,n} \mu(d) \operatorname{SR}\left(\frac{n}{d}\right).$$

In this formula, if$d < n$, then $\operatorname{SR}(\tfrac{n}{d}) = 0$, and for $d = n$: $\operatorname{SR}(\tfrac{n}{d}) = 1$. Therefore, $\operatorname{SP}(n) = \mu(n)$.

This is the special case$c_n(1)$ of Ramanujan's sum$c_n(s)$, defined as the sum of the$s$th powers of the primitive$n$th roots of unity:

$$c_n(s) = \sum_{\substack{a=1 \\ \gcd(a,n)=1}}^{n} e^{2\pi i \frac{a}{n} s}.$$

Orthogonality

From the summation formula follows anorthogonality relationship: for$j = 1, \dots, n$ and$j' = 1, \dots, n$

$$\sum_{k=1}^{n} \overline{z^{j\cdot k}} \cdot z^{j'\cdot k} = n \cdot \delta_{j,j'}$$

where δ is the Kronecker delta and z is any primitive$n$th root of unity.

The $n \times n$ matrix U whose (j, k)th entry is

$$U_{j,k} = n^{-\frac{1}{2}} \cdot z^{j\cdot k}$$

defines a discrete Fourier transform. Computing the inverse transformation using gaussian elimination requires $O(n^3)$ operations. However, it follows from the orthogonality that$U$ is unitary. That is,

$$\sum_{k=1}^{n} \overline{U_{j,k}} \cdot U_{k,j'} = \delta_{j,j'},$$

and thus the inverse of U is simply the complex conjugate. (This fact was first noted by Gauss when solving the problem of trigonometric interpolation). The straightforward application of U or its inverse to a given vector requires $O(n^2)$ operations. The fast Fourier transform algorithms reduces the number of operations further to $O(n \log n)$.

Cyclotomic polynomials

The zeroes of the polynomial

$$p(z) = z^n - 1$$

are precisely the nth roots of unity, each with multiplicity 1. The nth **cyclotomic polynomial** is defined by the fact that its zeros are precisely the *primitive* nth roots of unity, each with multiplicity 1.

$$\Phi_n(z) = \prod_{k=1}^{\varphi(n)} (z - z_k)$$

where $z_1, z_2, z_3, \ldots, z_{\varphi(n)}$ are the primitive nth roots of unity, and $\varphi(n)$ is Euler's totient function. The polynomial $\Phi_n(z)$ has integer coefficients and is an irreducible polynomial over the rational numbers (i.e., it cannot be written as the product of two positive-degree polynomials with rational coefficients). The case of prime n, which is easier than the general assertion, follows by applying Eisenstein's criterion to the polynomial

$$\frac{(z+1)^n - 1}{(z+1) - 1},$$

and expanding via the binomial theorem.

Every nth root of unity is a primitive dth root of unity for exactly one positive divisor d of n. This implies that

$$z^n - 1 = \prod_{d\,|\,n} \Phi_d(z).$$

This formula represents the factorization of the polynomial $z^n - 1$ into irreducible factors.

$$\begin{aligned}
z^1 - 1 &= z - 1\\
z^2 - 1 &= (z - 1)\cdot(z + 1)\\
z^3 - 1 &= (z - 1)\cdot(z^2 + z + 1)\\
z^4 - 1 &= (z - 1)\cdot(z + 1)\cdot(z^2 + 1)\\
z^5 - 1 &= (z - 1)\cdot(z^4 + z^3 + z^2 + z + 1)\\
z^6 - 1 &= (z - 1)\cdot(z + 1)\cdot(z^2 + z + 1)\cdot(z^2 - z + 1)\\
z^7 - 1 &= (z - 1)\cdot(z^6 + z^5 + z^4 + z^3 + z^2 + z + 1)\\
z^8 - 1 &= (z - 1)\cdot(z + 1)\cdot(z^2 + 1)\cdot(z^4 + 1)
\end{aligned}$$

Applying Möbius inversion to the formula gives

$$\Phi_n(z) = \prod_{d\,|n} \left(z^{\frac{n}{d}} - 1\right)^{\mu(d)} = \prod_{d\,|n} \left(z^d - 1\right)^{\mu\left(\frac{n}{d}\right)},$$

where μ is the Möbius function.

So the first few cyclotomic polynomials are

$$\begin{aligned}
\Phi_1(z) &= z - 1\\
\Phi_2(z) &= (z^2 - 1)\cdot(z - 1)^{-1} = z + 1\\
\Phi_3(z) &= (z^3 - 1)\cdot(z - 1)^{-1} = z^2 + z + 1\\
\Phi_4(z) &= (z^4 - 1)\cdot(z^2 - 1)^{-1} = z^2 + 1\\
\Phi_5(z) &= (z^5 - 1)\cdot(z - 1)^{-1} = z^4 + z^3 + z^2 + z + 1\\
\Phi_6(z) &= (z^6 - 1)\cdot(z^3 - 1)^{-1}\cdot(z^2 - 1)^{-1}\cdot(z - 1) = z^2 - z + 1\\
\Phi_7(z) &= (z^7 - 1)\cdot(z - 1)^{-1} = z^6 + z^5 + z^4 + z^3 + z^2 +z + 1\\
\Phi_8(z) &= (z^8 - 1)\cdot(z^4 - 1)^{-1} = z^4 + 1
\end{aligned}$$

If p is a prime number, then all the pth roots of unity except 1 are primitive pth roots, and we have

$$\Phi_p(z) = \frac{z^p - 1}{z - 1} = \sum_{k=0}^{p-1} z^k.$$

Substituting any positive integer ≥ 2 for z, this sum becomes a base z repunit. Thus a necessary (but not sufficient) condition for a repunit to be prime is that its length be prime.

Note that, contrary to first appearances, *not* all coefficients of all cyclotomic polynomials are 0, 1, or −1. The first exception is Φ_{105}. It is not a surprise it takes this long to get an example, because the behavior of the coefficients depends not so much on n as on how many odd prime factors appear in n. More precisely, it can be shown that if n has 1 or 2 odd prime factors (e.g., $n = 150$) then the nth cyclotomic polynomial only has coefficients 0, 1 or −1. Thus the first conceivable n for which there could be a coefficient besides 0, 1, or −1 is a product of the three smallest odd primes, and that is $3\cdot5\cdot7 = 105$. This by itself doesn't prove the 105th polynomial has another coefficient, but does show it is the first one which even has a chance of working (and then a computation of the coefficients shows it does). A theorem of Schur says that there are cyclotomic polynomials with coefficients arbitrarily large in absolute value. In particular, if $n = p_1\cdot p_2\cdot \cdots \cdot p_t$, where $p_1 < p_2 < \cdots < p_t$ are odd primes, $p_1 + p_2 > p_t$, and t is odd, then $1 - t$ occurs as a coefficient in the nth cyclotomic polynomial.[3]

Many restrictions are known about the values that cyclotomic polynomials can assume at integer values. For example, if p is prime, then $d \mid \Phi_p(d)$ if and only $d \equiv 1 \pmod p$.

Cyclotomic polynomials are solvable in radicals, as roots of unity are themselves radicals. Moreover, there exist more informative radical expressions for nth roots of unity with the additional property[4] that every value of the expression obtained by choosing values of the radicals (for example, signs of square roots) is a primitive nth root of unity. This was already shown by Gauss in 1797.[5] Efficient algorithms exist for calculating such expressions.[6]

Cyclic groups

The nth roots of unity form under multiplication a cyclic group of order n, and in fact these groups comprise all of the finite subgroups of the multiplicative group of the complex number field. A generator for this cyclic group is a primitive nth root of unity.

The nth roots of unity form an irreducible representation of any cyclic group of order n. The orthogonality relationship also follows from group-theoretic principles as described in character group.

The roots of unity appear as entries of the eigenvectors of any circulant matrix, i.e. matrices that are invariant under cyclic shifts, a fact that also follows from group representation theory as a variant of Bloch's theorem.[7] In particular, if a circulant Hermitian matrix is considered (for example, a discretized one-dimensional Laplacian with periodic boundaries[8]), the orthogonality property immediately follows from the usual orthogonality of eigenvectors of Hermitian matrices.

Cyclotomic fields

By adjoining a primitive nth root of unity to $\mathbf{Q}$, one obtains the nth cyclotomic field $\mathbf{Q}(\exp(2\pi i/n))$. This field contains all nth roots of unity and is the splitting field of the nth cyclotomic polynomial over $\mathbf{Q}$. The field extension $\mathbf{Q}(\exp(2\pi i/n))/\mathbf{Q}$ has degree $\varphi(n)$ and its Galois group is naturally isomorphic to the multiplicative group of units of the ring $\mathbf{Z}/n\mathbf{Z}$.

As the Galois group of $\mathbf{Q}(\exp(2\pi i/n))/\mathbf{Q}$ is abelian, this is an abelian extension. Every subfield of a cyclotomic field is an abelian extension of the rationals. It follows that every nth root of unity may be expressed in term of k-roots, with various k not exceeding $\varphi(n)$. In these cases Galois theory can be written out explicitly in terms of Gaussian periods: this theory from the *Disquisitiones Arithmeticae* of Gauss was published many years before Galois.[9]

Conversely, *every* abelian extension of the rationals is such a subfield of a cyclotomic field – this is the content of a theorem of Kronecker, usually called the *Kronecker–Weber theorem* on the grounds that Weber completed the proof.

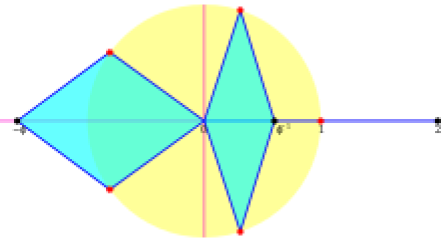
Relation to quadratic integers

For $n = 1, 2$, both roots of unity 1 and −1 belong to $\mathbf{Z}$.

For three values of n, the roots of unity are quadratic integers:

- For $n = 3, 6$ they are Eisenstein integers ($D = -3$).
- For $n = 4$ they are Gaussian integers ($D = -1$): see imaginary unit.

For four other values of n, the primitive roots of unity are not quadratic integers, but the sum of any root of unity with its complex conjugate (also an nth root of unity) is a quadratic integer.

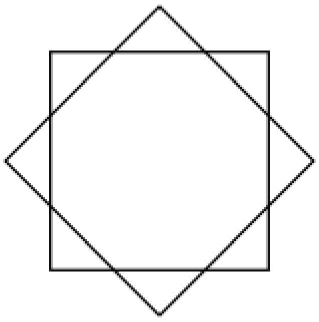


In the complex plane, the red points are the fifth roots of unity and the blue points are the sums of a fifth root of unity and its complex conjugate.

For $n = 5, 10$, none of the non-real roots of unity (which satisfy a quartic equation) is a quadratic integer, but the sum $z + \bar{z} = 2\,\mathrm{Re}\,z$ of each root with its complex conjugate (also a 5th root of unity) is an element of the ring $\mathbf{Z}[\frac{1+\sqrt{5}}{2}]$ ($D = 5$). For two pairs of non-real 5th roots of unity these sums are inverse golden ratio and minus golden ratio.

For $n = 8$, for any root of unity $z + \bar{z}$ equals to either 0, ±2, or $\pm\sqrt{2}$ ($D = 2$).

For $n = 12$, for any root of unity, $z + \bar{z}$ equals to either 0, ±1, ±2 or $\pm\sqrt{3}$ ($D = 3$).



In the complex plane, the corners of the two squares are the eighth roots of unity

See also

- Argand system
- Circle group, the unit complex numbers
- Group scheme of roots of unity
- Primitive root modulo *n*
- Dirichlet character
- Ramanujan's sum
- Kummer ring
- Witt vector
- Teichmüller character

Notes

1. Hadlock, Charles R. (2000). *Field Theory and Its Classical Problems, Volume 14* (https://books.google.com/books?id=5s1p0CyafnEC&pg=PA84). Cambridge University Press. pp. 84–86. ISBN 978-0-88385-032-9.
2. Lang, Serge (2002). "Roots of unity". *Algebra* (https://books.google.com/books?id=Fge-BwqhqIYC&pg=PA276). Springer. pp. 276–277. ISBN 978-0-387-95385-4.

3. Emma Lehmer, *On the magnitude of the coefficients of the cyclotomic polynomial*, Bulletin of the American Mathematical Society 42 (1936), no. 6, pp. 389–392.
4. Landau, Susan; Miller, Gary L. (1985). "Solvability by radicals is in polynomial time". *Journal of Computer and System Sciences*. **30** (2): 179–208. doi:10.1016/0022-0000(85)90013-3 (https://doi.org/10.1016/0022-0000%2885%2990013-3).
5. Gauss, Carl F. (1965). *Disquisitiones Arithmeticae*. Yale University Press. pp. §§359–360. ISBN 0-300-09473-6.
6. Weber, Andreas; Keckeisen, Michael. "Solving Cyclotomic Polynomials by Radical Expressions" (http://cg.cs.uni-bonn.de/personal-pages/weber/publications/pdf/WeberA/WeberKeckeisen99a.pdf) (PDF). Retrieved 2007-06-22.
7. T. Inui, Y. Tanabe, and Y. Onodera, *Group Theory and Its Applications in Physics* (Springer, 1996).
8. Gilbert Strang, "The discrete cosine transform (http://epubs.siam.org/sam-bin/dbq/article/33674)," *SIAM Review* **41** (1), 135–147 (1999).
9. The *Disquisitiones* was published in 1801, Galois was born in 1811, died in 1832, but wasn't published until 1846.

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, Zbl 0984.00001
- Milne, James S. (1998). "Algebraic Number Theory". *Course Notes*.
- Milne, James S. (1997). "Class Field Theory". *Course Notes*.
- Neukirch, Jürgen (1999). *Algebraic Number Theory*. *Grundlehren der mathematischen Wissenschaften*. **322**. Berlin: Springer-Verlag. ISBN 978-3-540-65399-8. MR 1697859. Zbl 0956.11021.
- Neukirch, Jürgen (1986). *Class Field Theory*. Berlin: Springer-Verlag. ISBN 3-540-15251-2.
- Washington, Lawrence C. (1997). *Cyclotomic fields* (2nd ed.). New York: Springer-Verlag. ISBN 0-387-94762-0.
- Derbyshire, John (2006). "Roots of Unity". *Unknown Quantity*. Washington, D.C.: Joseph Henry Press. ISBN 0-309-09657-X.

Further reading

- Storer, Thomas (1967). *Cyclotomy and difference sets*. Chicago: Markham Publishing Company. Zbl 0157.03301.