WIKIPEDIA

Einheitswurzel

In der Algebra werden Zahlen, deren n-te Potenz die Zahl 1 ergibt, n-te **Einheitswurzeln** genannt.

Inhaltsverzeichnis

Definition

Es sei R ein kommutativer Ring mit Einselement und $n \geq 1$ eine natürliche Zahl. Ein Element $\zeta \in R$ heißt eine n-te Einheitswurzel, wenn es eine der beiden gleichwertigen Bedingungen erfüllt:

- $\zeta^n = 1$
- ζ ist Nullstelle des Polynoms $X^n - 1$

Die n-ten Einheitswurzeln in R bilden eine Untergruppe der multiplikativen Gruppe $R^\times$, die oft mit $\mu_n(R)$ bezeichnet wird.

Eine n-te Einheitswurzel ζ heißt *primitiv,* falls $\zeta^m \neq 1$ für $m = 1, \ldots, n-1$ gilt.

Einheitswurzeln in den komplexen Zahlen

Im Körper $\mathbb{C}$ der komplexen Zahlen sind

$$\exp\left(\frac{2\pi \mathrm{i}\, k}{n}\right), \quad k = 0, 1, \ldots, n-1$$

die n-ten Einheitswurzeln, wobei i die imaginäre Einheit ist. Setzt man

$$\zeta_n = \exp\left(\frac{2\pi \mathrm{i}}{n}\right),$$

so ist ζ_n primitiv, und diese Zahlen bekommen (in der gleichen Reihenfolge) die einfache Gestalt

$$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}.$$

Ist klar, um welches n es sich handelt, lässt man den unteren Index häufig fallen.

Gruppe der Einheitswurzeln

Da 1 und mit ζ_n^i und ζ_m^j auch $\zeta_n^i \zeta_m^j = \zeta_{nm}^{im+jn}$ Einheitswurzeln sind, ist die Menge $\mu(\mathbb{C})$ aller Einheitswurzeln eine Gruppe. Die Abbildung

$$f\colon \mathbb{Q} \to \mu(\mathbb{C}), \quad \frac{k}{n} \mapsto \exp\left(\frac{2\pi \mathrm{i}\, k}{n}\right)$$

ist surjektiv. Der Kern dieser Abbildung ist $\mathbb{Z}$. Die Gruppe der komplexen Einheitswurzeln ist daher isomorph zu der Faktorgruppe $\mathbb{Q}/\mathbb{Z}$.

Geometrischer Bezug

Die n-ten Einheitswurzeln lassen sich in der komplexen Zahlenebene geometrisch anschaulich interpretieren: Sie sind die auf dem Einheitskreis (mit Mittelpunkt 0 und Radius 1) liegenden Ecken eines regelmäßigen n-Ecks, wobei eine der Ecken die Zahl 1 ist, denn diese ist für jedes $n \geq 1$ eine n-te Einheitswurzel.

Realteil und Imaginärteil der Einheitswurzeln $\zeta_n^k = x_k + \mathrm{i}\, y_k$ sind damit die Koordinaten der Ecken des n-Ecks auf dem Kreis, d. h. für $k = 0, 1, \ldots, n-1$ ist

$$x_k = \cos(2\pi k/n) = \cos(360^\circ \cdot k/n) \quad \text{und} \quad y_k = \sin(2\pi k/n) = \sin(360^\circ \cdot k/n).$$

Mehr siehe unter Radizieren komplexer Zahlen.

Summe der Einheitswurzeln

Ist ζ eine n-te Einheitswurzel, so gilt

$$1 + \zeta + \zeta^2 + \cdots + \zeta^{n-1} = \begin{cases} n & \text{falls } \zeta = 1 \\ 0 & \text{sonst.} \end{cases}$$

Diese Aussage folgt unmittelbar aus der geometrischen Summenformel und ist ein Spezialfall der analogen Aussage für Charaktere von Gruppen.

Beispiele

Die zweiten, dritten und vierten Einheitswurzeln

Die zweiten Einheitswurzeln sind

$$\zeta_1 = -1, \quad \zeta_2 = 1;$$

die dritten Einheitswurzeln sind

$$\zeta_1 = -\frac{1}{2} + \frac{\mathrm{i}}{2}\sqrt{3}, \quad \zeta_2 = -\frac{1}{2} - \frac{\mathrm{i}}{2}\sqrt{3}, \quad \zeta_3 = 1;$$

die vierten Einheitswurzeln sind wieder von einfacherer Form:

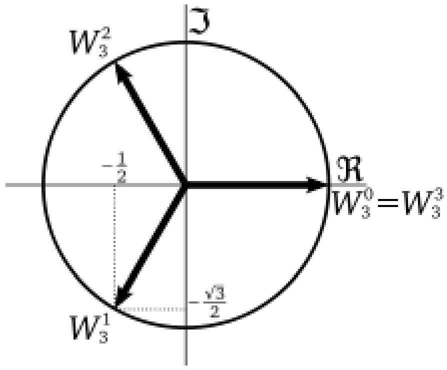
$$\zeta_1 = \mathrm{i}, \quad \zeta_2 = -1, \quad \zeta_3 = -\mathrm{i}, \quad \zeta_4 = 1.$$

Die fünften Einheitswurzeln

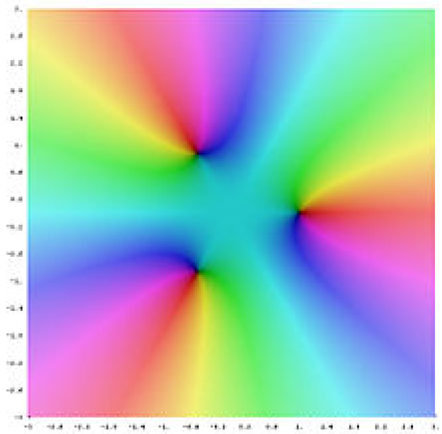
Aus

$0 = 1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$

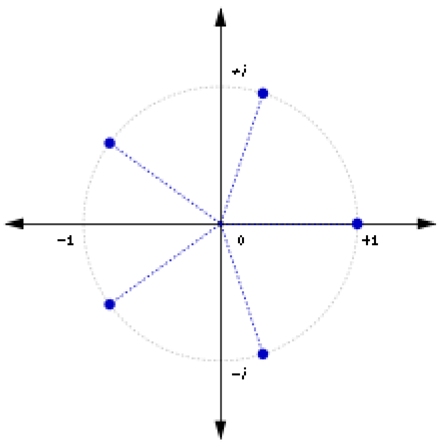
folgt



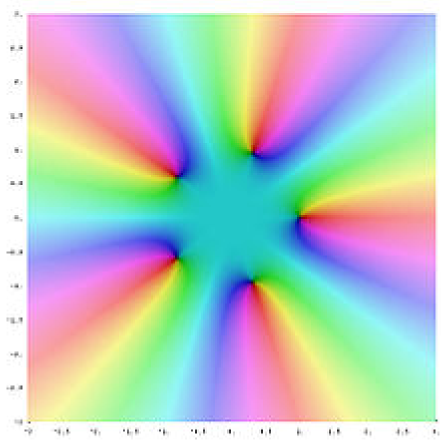
Die dritten Einheitswurzeln



Die Funktion $z \mapsto z^3 - 1$



Die fünften Einheitswurzeln



Die Funktion $z \mapsto z^5 - 1$

$$0 = \frac{1}{\zeta^2} + \frac{1}{\zeta} + 1 + \zeta + \zeta^2 = \left(\zeta + \frac{1}{\zeta}\right)^2 + \left(\zeta + \frac{1}{\zeta}\right) - 1 = w^2 + w - 1$$

für $w = \zeta + \frac{1}{\zeta} = \zeta + \zeta^4 = 2\cos(72^\circ)$. Lösen dieser quadratischen Gleichung liefert $w = -\frac{1}{2} \pm \sqrt{\frac{5}{4}}$. Da der Winkel 72° im 1. Quadranten liegt, ist w positiv, und damit ist $\cos(72^\circ) = \frac{\sqrt{5}-1}{4}$ der Realteil von ζ. Der Imaginärteil ist nach dem Satz des Pythagoras $\sin(72^\circ) = \sqrt{\frac{\sqrt{5}+5}{8}}$.

Eigenschaften der Einheitswurzeln

Einheitswurzeln in (kommutativen) Körpern

Ist $p := \operatorname{char}(K) \neq 0$ die Charakteristik des Körpers K, dann ist $\zeta = 1$ eine p-fache Nullstelle des Polynoms $X^p - 1$. Ist p nicht Teiler der Ordnung n, dann gelten die folgenden Aussagen auch für Körper mit Primzahlcharakteristik p. Für zusätzliche Eigenschaften der Einheitswurzeln in solchen Körpern siehe Endlicher Körper#Multiplikative Gruppe und diskreter Logarithmus

- Ist K ein (kommutativer) Körper und $n \in \mathbb{N}$, dann bilden die Elemente $\zeta \in K$ mit $\zeta^n = 1$ eine zyklische Untergruppe U der multiplikativen Gruppe $K^\times$.
- Die Gruppenordnung von U ist stets ein Teiler von n.

- Ist sie gleich n, so sagt man, K „enthält die n-ten Einheitswurzeln“ und nennt U „die Gruppe der n-ten Einheitswurzeln“.
- Eine n-te Einheitswurzel ist genau dann primitiv, wenn sie die Gruppe der n-ten Einheitswurzeln erzeugt. Die Ordnung einer primitiven n-ten Einheitswurzel ζ_n ist n. Die primitiven n-ten Einheitswurzeln sind genau die Nullstellen des n-ten Kreisteilungspolynoms.
- Ist ζ_n eine primitive n-te Einheitswurzel, dann ist ζ_n^k eine primitive $\frac{n}{\mathrm{ggT}(k,n)}$-te Einheitswurzel (größter gemeinsamer Teiler).
- Die Anzahl der primitiven n-ten Einheitswurzeln ist $\varphi(n)$ (Eulersche Phi-Funktion).
- Erweiterungen von $\mathbb{Q}$, die durch Adjunktion von Einheitswurzeln entstehen, heißen Kreisteilungskörper.
- Eine endliche multiplikative Untergruppe U eines (kommutativen) Körpers K ist zyklisch.

Beweis der letzten Aussage: U ist eine abelsche Torsionsgruppe. Sie ist also zu einem direkten Produkt

$$U = \prod_{p\in\mathbb{P}} U_{(p)} \quad \text{mit} \quad U_{(p)} := \left\{ u \in U \,\middle|\, \bigvee_{i\in\mathbb{N}} (u^{p^i} = 1) \right\}$$

isomorph ($\mathbb{P}$:= Menge der positiven Primzahlen). Und die $U_{(p)}$ sind zyklisch, weil die Gruppenelemente der Ordnung p^i allesamt Nullstellen von $X^{p^i} - 1$ sind und damit Potenzen voneinander. Schließlich ist wegen der Teilerfremdheit von Potenzen verschiedener Primzahlen das direkte Produkt zyklisch.

Beispiel für Einheitswurzeln in nicht-kommutativen (Schief)körpern

Im nicht-kommutativen Schiefkörper der Quaternionen $\mathbb{H}$ hat das Polynom $X^2 - 1$ die unendlich vielen Nullstellen

$$\epsilon = \epsilon_0 + \epsilon_1 \mathbf{i} + \epsilon_2 \mathbf{j} + \epsilon_3 \mathbf{k}$$

mit

$$\epsilon_0 = 0 \ \wedge \ \epsilon_1^2 + \epsilon_2^2 + \epsilon_3^2 = 1.$$

Die Quaternionengruppe ist eine endliche nicht-kommutative Untergruppe der multiplikativen Gruppe $\mathbb{H}^\times$. Sie hat die Ordnung 8 und den Exponenten 4. Für weitere endliche Untergruppen von $\mathbb{H}^\times$ siehe Quaternion#Die endlichen Untergruppen.

Einheitswurzeln in Restklassenringen

- Im Ring $\mathbb{Z}_{2^n+1} = \mathbb{Z}/(2^n+1)\mathbb{Z}$ der ganzen Zahlen modulo (2^n+1) ist die Zahl 2 eine primitive $2n$-te Einheitswurzel, denn in diesem Ring gilt $2^n = -1$.
- Im Ring $\mathbb{Z}_{2^n-1} = \mathbb{Z}/(2^n-1)\mathbb{Z}$ der ganzen Zahlen modulo (2^n-1) ist die Zahl 2 eine primitive n-te Einheitswurzel.

Diese beiden speziellen Restklassenringe sind für die Computeralgebra höchst bedeutsam, denn sie ermöglichen eine nochmals drastisch beschleunigte Variante der schnellen diskreten Fouriertransformation. Dies liegt darin begründet, dass Addition und Multiplikation dieser Restklassenringe durch entsprechende zyklische Addition und Multiplikation in einem unwesentlich größeren Restklassenring ersetzt werden können, und damit in binärer Zahlendarstellung die Multiplikation mit Potenzen der Zahl 2 eine zyklische binäre Shift-Operation bedeutet, was wesentlich schneller durchführbar ist als eine allgemeine Multiplikation zweier Zahlen. Die erhebliche Zeitersparnis für die diskrete Fourier-Transformation ergibt sich aus der Tatsache, dass während der schnellen Fouriertransformation viele Multiplikationen mit der gewählten Einheitswurzel durchzuführen sind.

Literatur

- Siegfried Bosch: *Algebra.* 7. Auflage. Springer-Verlag, Berlin 2009, ISBN 978-3-540-92811-9, Abschnitt 4.5 (eingeschränkte Vorschau in der Google-Buchsuche).