

Einführung in die Algebra

Vorlesung 27

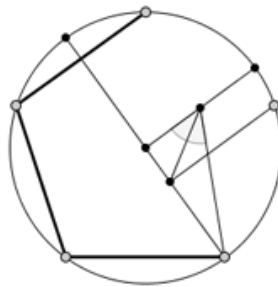
Konstruierbare Einheitswurzeln

DEFINITION 1. Sei $n \in \mathbb{N}_+$. Man sagt, dass *das regelmäßige n -Eck mit Zirkel und Lineal konstruierbar* ist, wenn die komplexe Zahl

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

eine konstruierbare Zahl ist.

Die Menge der komplexen Einheitswurzeln $e^{\frac{2\pi i k}{n}}$, $k = 0, \dots, n-1$, bilden die Eckpunkte eines regelmäßigen n -Ecks, wobei 1 eine Ecke bildet. Alle Eckpunkte liegen auf dem Einheitskreis. Die Ecke $e^{\frac{2\pi i}{n}}$ ist eine primitive Einheitswurzel; wenn diese mit Zirkel und Lineal konstruierbar ist, so sind auch alle weiteren Eckpunkte konstruierbar. Bei $n = 1, 2$ kann man sich darüber streiten, ob man von einem regelmäßigen n -Eck sprechen soll, jedenfalls gibt es die zugehörigen Einheitswurzeln und diese sind aus \mathbb{Q} , also erst recht konstruierbar. Das regelmäßige Dreieck ist ein gleichseitiges Dreieck und dieses ist konstruierbar nach Beispiel 26.7, da der dritte Kreisteilungskörper eine quadratische Körpererweiterung von \mathbb{Q} ist (man kann einfacher auch direkt zeigen, dass ein gleichseitiges Dreieck aus seiner Grundseite heraus konstruierbar ist). Das regelmäßige Viereck ist ein Quadrat mit den Eckpunkten $1, i, -1, -i$, und dieses ist ebenfalls konstruierbar. Das regelmäßige Fünfeck ist ebenfalls konstruierbar, wie in Beispiel 26.9 bzw. Aufgabe 26.9 gezeigt wurde. Wir werden im Folgenden sowohl positive als auch negative Resultate zur Konstruierbarkeit von regelmäßigen n -Ecken vorstellen.



LEMMA 2. Sei $m = kn$, $m, k, n \in \mathbb{N}_+$. Dann gelten folgende Aussagen.

- (1) Das regelmäßige 2^r -Eck, $r \in \mathbb{N}$, ist konstruierbar.
- (2) Wenn das regelmäßige m -Eck konstruierbar ist, so ist auch das regelmäßige n -Eck und das regelmäßige k -Eck konstruierbar.

- (3) Wenn n und k teilerfremd sind und wenn das regelmäßige n -Eck und das regelmäßige k -Eck konstruierbar sind, so ist auch das regelmäßige m -Eck konstruierbar.

Beweis. (1) folgt daraus, dass eine Winkelhalbierung stets mit Zirkel und Lineal durchführbar ist. (2) Nach Voraussetzung ist $e^{\frac{2\pi i}{nk}}$ konstruierbar. Dann ist auch nach Lemma 24.8 die Potenz

$$\left(e^{\frac{2\pi i}{nk}}\right)^n = e^{\frac{2\pi i}{k}}$$

konstruierbar. (3) Seien nun $e^{\frac{2\pi i}{n}}$ und $e^{\frac{2\pi i}{k}}$ konstruierbar und n und k teilerfremd. Nach Satz 4.1 gibt es dann ganze Zahlen r, s mit $rn + sk = 1$. Daher ist auch

$$\left(e^{\frac{2\pi i}{n}}\right)^s \left(e^{\frac{2\pi i}{k}}\right)^r = \left(e^{\frac{2\pi i k}{nk}}\right)^s \left(e^{\frac{2\pi i n}{nk}}\right)^r = e^{\frac{2\pi i s k}{nk}} e^{\frac{2\pi i r n}{nk}} = e^{\frac{2\pi i (sk + rn)}{nk}} = e^{\frac{2\pi i}{nk}}$$

konstruierbar. □

Aus diesem Lemma kann man in Zusammenhang mit den oben erwähnten Konstruktionsmöglichkeiten folgern, dass die regelmäßigen $3 \cdot 2^r$ -Ecke, die regelmäßigen $5 \cdot 2^r$ -Ecke und die regelmäßigen $15 \cdot 2^r$ -Ecke für jedes r konstruierbar sind.

SATZ 3. Sei n eine natürliche Zahl derart, dass das regelmäßige n -Eck konstruierbar ist. Dann ist $\varphi(n)$ eine Zweierpotenz.

Beweis. Die Voraussetzung besagt, dass die primitive Einheitswurzel $\zeta = e^{\frac{2\pi i}{n}}$ konstruierbar ist. Dann muss nach Korollar 25.3 der Grad des Minimalpolynoms von ζ eine Zweierpotenz sein. Nach Korollar 26.14 ist das Minimalpolynom von ζ das n -te Kreisteilungspolynom, und dieses hat den Grad $\varphi(n)$. Also muss $\varphi(n)$ eine Zweierpotenz sein. □

Winkeldreiteilung

Wir sind nun in der Lage, das Problem der Winkeldreiteilung zu beantworten.

KOROLLAR 4. Das regelmäßige 9-Eck ist nicht mit Zirkel und Lineal konstruierbar.

Beweis. Wäre das regelmäßige 9-Eck konstruierbar, so müsste nach Satz 27.3 $\varphi(9)$ eine Zweierpotenz sein. Es ist aber $\varphi(9) = 2 \cdot 3 = 6$. □

SATZ 5. Es ist nicht möglich, einen beliebig vorgegebenen Winkel mittels Zirkel und Lineal in drei gleich große Teile zu unterteilen.

Beweis. Es genügt, einen (konstruierbaren) Winkel α anzugeben derart, dass $\alpha/3$ nicht konstruierbar ist. Wir betrachten $\alpha = 120$ Grad, welcher konstruierbar ist, da die dritten Einheitswurzeln konstruierbar sind, weil sie nämlich

in einer quadratischen Körpererweiterung von \mathbb{Q} liegen. Dagegen ist der Winkel $\alpha/3 = 120/3 = 40$ nicht konstruierbar, da andernfalls das regelmäßige 9-Eck konstruierbar wäre, was nach Korollar 27.4 aber nicht der Fall ist. \square

Wir geben noch einen weiteren Beweis, dass die Winkeldreiteilung mit Zirkel und Lineal nicht möglich ist.

LEMMA 6. *Es sei $F \in \mathbb{Z}[X]$ ein normiertes Polynom vom Grad ≤ 3 ohne Nullstelle in \mathbb{Z} . Dann ist F irreduzibel in $\mathbb{Q}[X]$.*

Beweis. Aufgrund von Lemma 20.13 und der Gradvoraussetzung genügt es zu zeigen, dass es keine Faktorzerlegung $F = GH$ in $\mathbb{Z}[X]$ mit $\text{grad}(G) = 1$ geben kann. Sei also angenommen, dass $G = aX + b \in \mathbb{Z}[X]$ ein Teiler von F ist. Der Leitkoeffizient a teilt den Leitkoeffizienten von F , also 1, daher muss $a \in \mathbb{Z}$ eine Einheit sein. Dann ist $a = \pm 1$ und somit ist $\pm b$ eine Nullstelle im Widerspruch zur Voraussetzung. \square

Einfache Beispiele wie $F = (2X + 1)^2$ zeigen, dass ohne die Voraussetzung normiert die Aussage nicht stimmt. Dass ein ganzzahliges normiertes Polynom keine ganzzahligen Nullstellen besitzt, ist im Allgemeinen einfach zu zeigen. Für n betragsmäßig groß kann man durch eine einfache Abschätzung zeigen, dass es dafür keine Nullstelle geben kann, und für n in einem verbleibenden überschaubaren Bereich kann man durch explizites Ausrechnen feststellen, ob eine Nullstelle vorliegt oder nicht.

BEMERKUNG 7. Wir geben noch einen weiteren Beweis, dass die Winkeldreiteilung nicht möglich ist, der nicht auf der allgemeinen Irreduzibilität der Kreisteilungspolynome beruht. Wir zeigen, dass man den Winkel 20 Grad nicht konstruieren kann (obwohl man 60 Grad konstruieren kann). Aufgrund der *Additionstheoreme für die trigonometrischen Funktionen* gilt

$$\cos 3\alpha = 4 \cos^3 \alpha - 3 \cos \alpha$$

und damit

$$\begin{aligned} (2 \cos 20)^3 - 3(2 \cos 20) - 1 &= 2(4 \cos^3 20 - 3 \cos 20 - \frac{1}{2}) \\ &= 2(\cos 60 - \frac{1}{2}). \\ &= 0 \end{aligned}$$

Also wird $2 \cos 20$ von Polynom $X^3 - 3X - 1$ annulliert. Dieses Polynom hat keine ganzzahlige Nullstelle und ist daher nach Lemma 27.6 irreduzibel. Also muss es das Minimalpolynom von $2 \cos 20$ sein. Daher kann $2 \cos 20$ nach Korollar 25.5 nicht konstruierbar sein und damit ebensowenig $\cos 20$.

Fermatsche Primzahlen

Die Frage der Konstruierbarkeit von regelmäßigen n -Ecken führt uns zu Fermatschen Primzahlen.

DEFINITION 8. Eine Primzahl der Form $2^s + 1$, wobei s eine positive natürliche Zahl ist, heißt *Fermatsche Primzahl*.

Es ist unbekannt, ob es unendlich viele Fermatsche Primzahlen gibt. Es ist noch nicht mal bekannt, ob es außer den ersten fünf Fermat-Zahlen

$$3, 5, 17, 257, 65537$$

überhaupt weitere Fermat-Zahlen gibt, die prim sind.

LEMMA 9. Bei einer Fermatschen Primzahl $2^s + 1$ hat der Exponent die Form $s = 2^r$ mit einem $r \in \mathbb{N}$.

Beweis. Wir schreiben $s = 2^k u$ mit u ungerade. Damit ist

$$2^{2^k u} + 1 = (2^{2^k})^u + 1.$$

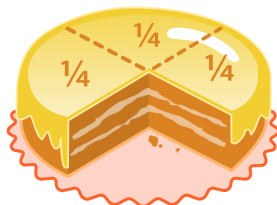
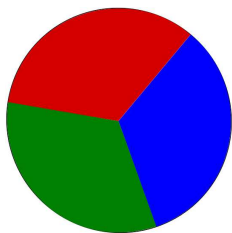
Für ungerades u gilt generell die polynomiale Identität (da -1 eine Nullstelle ist)

$$X^u + 1 = (X + 1)(X^{u-1} - X^{u-2} + X^{u-3} - \dots + X^2 - X + 1).$$

Also ist $2^{2^k} + 1 \geq 3$ ein Teiler von $2^{2^k u} + 1$. Da diese Zahl nach Voraussetzung prim ist, müssen beide Zahlen gleich sein, und dies bedeutet $u = 1$. \square

Eine Fermatsche Primzahl ist nach diesem Lemma also insbesondere eine Fermat-Zahl im Sinne der folgenden Definition.

DEFINITION 10. Eine Zahl der Form $2^{2^r} + 1$, wobei r eine natürliche Zahl ist, heißt *Fermat-Zahl*.



SATZ 11. Ein reguläres n -Eck ist genau dann mit Zirkel und Lineal konstruierbar, wenn die Primfaktorzerlegung von n die Gestalt hat

$$n = 2^\alpha p_1 \cdots p_k,$$

wobei die p_i verschiedene Fermatsche Primzahlen sind.

Beweis. Wir zeigen nur die eine Richtung, dass bei einem konstruierbaren regelmäßigen n -Eck die Zahl n die angegebene numerische Bedingung erfüllen muss. Es sei $n = 2^\alpha p_1^{r_1} \cdots p_k^{r_k}$ die Primfaktorzerlegung von n mit den verschiedenen ungeraden Primzahlen p_i , $i = 1, \dots, k$, und positiven Exponenten $k_i \geq 1$ (und $\alpha \geq 0$). Nach Satz 27.3 muss die eulersche Funktion eine Zweierpotenz sein, also

$$\varphi(n) = 2^t.$$

Andererseits gilt nach Korollar 15.16 die Beziehung

$$\varphi(n) = 2^{\alpha-1}(p_1 - 1)p_1^{r_1-1}(p_k - 1)p_k^{r_k-1}$$

(bei $\alpha = 0$ ist der Ausdruck $2^{\alpha-1}$ zu streichen). Da dies eine Zweierpotenz sein muss, dürfen die ungeraden Primzahlen nur mit einem Exponenten 1 (oder 0) auftreten. Ferner muss jede beteiligte Primzahl p die Gestalt $p = 2^s + 1$ haben, also eine Fermatsche Primzahl sein. Für die andere Richtung muss man aufgrund von Lemma 27.2 lediglich zeigen, dass für eine Fermatsche Primzahl p das regelmäßige p -Eck konstruierbar ist. Dies haben wir für $p = 3, 5$ explizit getan. Gauss selbst hat eine Konstruktion für das reguläre 17-Eck angegeben. Für die anderen Fermatschen Primzahlen (bekannt oder nicht) folgt die Konstruierbarkeit aus der Galoistheorie. \square

Abbildungsverzeichnis

Quelle = Pentagon construct.gif, Autor = TokyoJunkie (= Benutzer Mosmas auf PD), Lizenz = en.wikipedia.org	1
Quelle = Pie 2.svg, Autor = Benutzer Cronholm 144 auf Commons, Lizenz = CC-by-sa 3.0	4
Quelle = Cake quarters.svg, Autor = Benutzer Acdx, R. S. Shaw auf Commons, Lizenz = PD	4
Quelle = Luxembourg Vianden Nut-fair 10.jpg, Autor = Benutzer PlayMistyForMe auf Commons, Lizenz = CC-by-sa 3.0	4