Prof. Dr. H. Brenner **Osnabrück SS 2015**

Elemente der Algebra

Vorlesung 27

Das Delische Problem

Die Bewohner der Insel Delos befragten während einer Pestepidemie 430 v. Chr. das Orakel von Delphi. Sie wurden aufgefordert, den würfelförmigen Altar des Apollon zu verdoppeln.

Wir kommen zur ersten Konsequenz von unserer systematischen Untersuchung der konstruierbaren Zahlen auf die klassischen Konstruktionsprobleme.

KOROLLAR 27.1. *Die Würfelverdopplung mit Zirkel und Lineal ist nicht möglich.*

Beweis. Wir betrachten einen Würfel mit der Kantenlänge 1 und dem Volumen 1. Die Konstruktion eines Würfels mit dem doppelten Volumen würde bedeuten, dass man die neue Kantenlänge, also $2^{1/3}$ mit Zirkel und Lineal konstruieren könnte. Das Minimalpolynom von $2^{1/3}$ ist $X^3 - 2$, da dieses offenbar $2^{1/3}$ annulliert und nach Lemma 6.9 irreduzibel ist, da in $\mathbb{Q}$ keine dritte Wurzel aus 2 existiert. Nach Korollar 26.7 ist $2^{1/3}$ nicht konstruierbar, da 3 keine Zweierpotenz ist. □

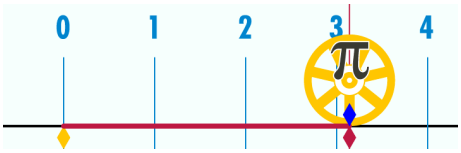
Die Quadratur des Kreises

Satz 27.2. *Es ist nicht möglich, zu einem vorgegebenen Kreis ein flächengleiches Quadrat mit Zirkel und Lineal zu konstruieren.*

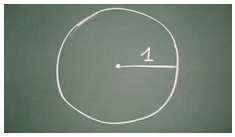
Beweis. Wenn es ein Konstruktionsverfahren gäbe, so könnte man insbesondere den Einheitskreis mit dem Radius 1 quadrieren, d.h. man könnte ein Quadrat mit der Seitenlänge $\sqrt{\pi}$ mit Zirkel und Lineal konstruieren. Nach Korollar 26.6 muss aber eine konstruierbare Zahl algebraisch sein. Nach dem Satz von Lindemann ist aber π und damit auch $\sqrt{\pi}$ transzendent. □

Es gibt natürlich einige geometrische Methoden die Zahl π zu erhalten, z.B. die Abrollmethode und die Schwimmbadmethode.

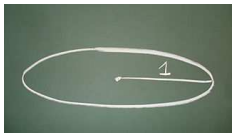
Beispiel 27.3. Die einfachste Art, die Zahl π geometrisch zu konstruieren, ist die *Abrollmethode*, bei der man einen Kreis mit Durchmesser 1 einmal exakt abrollt. Die zurückgeführte Entfernung ist genau der Kreisumfang, also π.



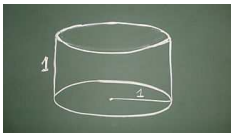
Beispiel 27.4.



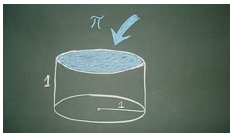
Wir starten mit einem Einheitskreis,



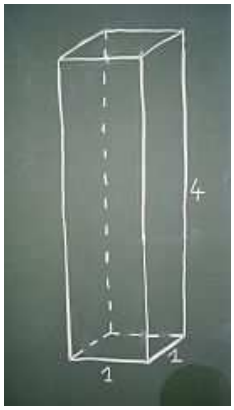
den wir als Grundfläche



eines Schwimmbeckens der Höhe 1 nehmen.

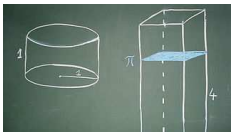


Das füllen wir randvoll mit Wasser auf.



Wir nehmen ein zweites Schwimmbecken mit quadratischer Grundfläche 1×1 und Höhe 4.

Der Inhalt des ersten Schwimmbeckens wird



in das zweite Schwimmbecken gegossen.

Der Wasserstand im zweiten Schwimmbecken ist exakt π.

Einheitswurzeln

DEFINITION 27.5. Es sei K ein Körper und $n \in \mathbb{N}_+$. Dann heißen die Nullstellen des Polynoms

$$X^n - 1$$

in K die n-ten *Einheitswurzeln* in K.

Die 1 ist für jedes n eine n-te Einheitswurzel, und die -1 ist für jedes gerade n eine n-te Einheitswurzel. Es gibt maximal n n-te Einheitswurzel, da das Polynom $X^n - 1$ maximal n Nullstellen besitzt. Die Einheitswurzeln bilden also insbesondere eine endliche Untergruppe (mit $x^n = 1$ und $y^n = 1$ ist auch $(xy)^n = 1$, usw.) der Einheitengruppe des Körpers. Nach einem Satz, den wir nicht bewiesen haben, ist diese Gruppe zyklisch mit einer Ordnung, die n teilt.

DEFINITION 27.6. Eine n-te Einheitswurzel heißt *primitiv*, wenn sie die Ordnung n besitzt.

Man beachte, dass ein Erzeuger der Gruppe der Einheitswurzeln nur dann primitiv heißt, wenn es n verschiedene Einheitswurzeln gibt. Wenn ζ eine primitive n-te Einheitswurzel ist, so sind genau die ζ^i mit $i < n$ und i teilerfremd zu n die primitiven Einheitswurzeln. Insbesondere gibt es, wenn es überhaupt primitive Einheitswurzeln gibt, genau $\varphi(n)$ primitive Einheitswurzeln, wobei $\varphi(n)$ die eulersche φ-Funktion bezeichnet. Die komplexen Einheitswurzeln lassen sich einfach beschreiben.

LEMMA 27.7. *Sei $n \in \mathbb{N}_+$. Die Nullstellen des Polynoms $X^n - 1$ über $\mathbb{C}$ sind*

$$e^{2\pi ik/n} = \cos\frac{2\pi k}{n} + i\sin\frac{2\pi k}{n}, k = 0, 1, \ldots, n-1.$$

In $\mathbb{C}[X]$ gilt die Faktorisierung

$$X^n - 1 = (X-1)(X - e^{2\pi i/n})\cdots(X - e^{2\pi i(n-1)/n})$$

Beweis. Der Beweis verwendet einige Grundtatsachen über die komplexe Exponentialfunktion. Es ist

$$\left(e^{2\pi ik/n}\right)^n = e^{2\pi ik} = \left(e^{2\pi i}\right)^k = 1^k = 1.$$

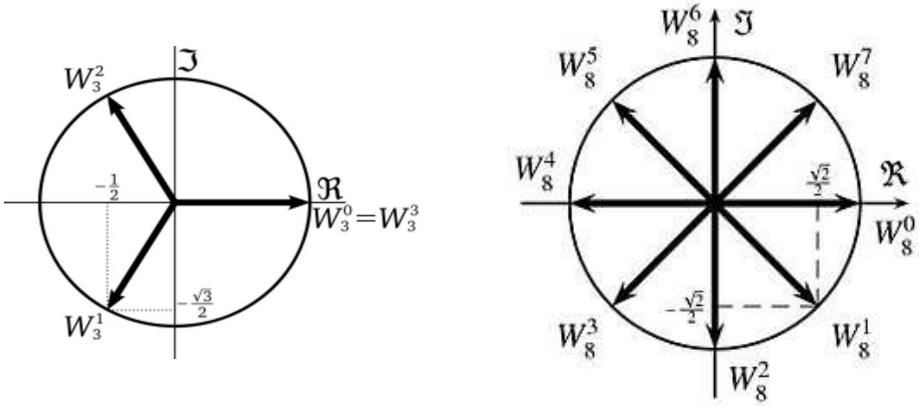
Die angegebenen komplexen Zahlen sind also wirklich Nullstellen des Polynoms $X^n - 1$. Diese Nullstellen sind alle untereinander verschieden, da aus

$$e^{2\pi ik/n} = e^{2\pi i\ell/n}$$

mit $0 \leq k \leq \ell \leq n-1$ sofort durch betrachten des Quotienten $e^{2\pi i(\ell-k)/n} = 1$ folgt, und daraus

$$\ell - k = 0.$$

Es gibt also n explizit angegebene Nullstellen und daher müssen dies alle Nullstellen des Polynoms sein. Die explizite Beschreibung in Koordinaten folgt aus der eulerschen Formel. □



Kreisteilungskörper

DEFINITION 27.8. Der n-te *Kreisteilungskörper* ist der Zerfällungskörper des Polynoms

$$X^n - 1$$

über $\mathbb{Q}$.

Offenbar ist 1 eine Nullstelle von $X^n - 1$. Daher kann man $X^n - 1$ durch $X - 1$ teilen und erhält, wie man schnell nachrechen kann,

$$X^n - 1 = (X - 1)(X^{n-1} + X^{n-2} + \cdots + X + 1).$$

Wegen $1 \in \mathbb{Q}$ ist daher der n-te Kreisteilungskörper auch der Zerfällungskörper von

$$X^{n-1} + X^{n-2} + \cdots + X + 1\,.$$

Es gibt auch Kreisteilungskörper über anderen Körpern, da es ja stets Zerfällungskörper gibt. Wir beschränken uns aber auf die Kreisteilungskörper über $\mathbb{Q}$, die wir auch mit K_n bezeichnen. Da $X^n - 1$ in der oben explizit beschriebenen Weise über $\mathbb{C}$ in Linearfaktoren zerfällt, kann man K_n als Unterkörper von $\mathbb{C}$ realisieren, und zwar ist K_n der von allen n-ten Einheitswurzeln erzeugte Unterkörper von $\mathbb{C}$. Dieser wird sogar schon von einer einzigen primitiven Einheitswurzel erzeugt, wofür wir den folgenden Begriff einführen.

DEFINITION 27.9. Eine Körpererweiterung $K \subseteq L$ heißt *einfach*, wenn es ein Element $x \in L$ gibt mit

$$L = K(x)\,.$$

LEMMA 27.10. *Sei $n \in \mathbb{N}_+$. Dann wird der n-te Kreisteilungskörper über $\mathbb{Q}$ von $e^{2\pi i/n}$ erzeugt. Der n-te Kreisteilungskörper ist also*

$$K_n = \mathbb{Q}\left(e^{2\pi i/n}\right) = \mathbb{Q}[e^{2\pi i/n}].$$

Insbesondere ist jeder Kreisteilungskörper eine einfache Körpererweiterung von $\mathbb{Q}$

Beweis. Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$. Wegen $\left(e^{2\pi i/n}\right)^n = 1$ ist $\mathbb{Q}[e^{2\pi i/n}] \subseteq K_n$. Wegen $\left(e^{2\pi i/n}\right)^k = e^{2\pi ik/n}$ gehören auch alle anderen Einheitswurzeln zu $\mathbb{Q}[e^{2\pi i/n}]$, also ist $\mathbb{Q}[e^{2\pi i/n}] = K_n$. □

Statt $e^{\frac{2\pi i}{n}}$ kann man auch jede andere n-te primitive Einheitswurzel als Erzeuger nehmen. Das Minimalpolynom zu einem Erzeuger von K_n heißt das n-te *Kreisteilungspolynom*. Der Grad des n-ten Kreisteilungspolynoms ist der Grad des n-ten Kreisteilungskörpers über $\mathbb{Q}$. Dieser Grad ist stets $\varphi(n)$, was wir aber nicht beweisen werden.

Beispiel 27.11. Wir bestimmen einige Kreisteilungskörper für kleine n. Bei $n = 1$ oder 2 ist der Kreisteilungskörper gleich $\mathbb{Q}$. Bei $n = 3$ ist

$$X^3 - 1 = (X-1)(X^2 + X + 1)$$

und der zweite Faktor zerfällt

$$X^2 + X + 1 = \left(X + \frac{1}{2} - i\frac{\sqrt{3}}{2}\right)\left(X + \frac{1}{2} + i\frac{\sqrt{3}}{2}\right).$$

Daher ist der dritte Kreisteilungskörper der von $\sqrt{-3} = \sqrt{3}i$ erzeugte Körper, es ist also $K_3 = \mathbb{Q}[\sqrt{-3}]$ eine quadratische Körpererweiterung der rationalen Zahlen.

Bei $n = 4$ ist natürlich

$$\begin{aligned} X^4 - 1 &= (X^2-1)(X^2+1) \\ &= (X-1)(X+1)(X^2+1) \\ &= (X-1)(X+1)(X-i)(X+i). \end{aligned}$$

Der vierte Kreisteilungskörper ist somit $\mathbb{Q}[i] \cong \mathbb{Q}[X]/(X^2+1)$, also ebenfalls eine quadratische Körpererweiterung von $\mathbb{Q}$.

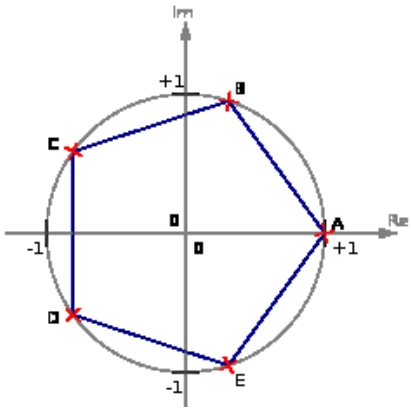
Der Beweis der folgenden wichtigen Aussage beruht auf Überlegungen, die wir nicht entwickelt haben.

Lemma 27.12. *Sei p eine Primzahl. Dann ist der p-te Kreisteilungskörper gleich*

$$\mathbb{Q}[X]/(X^{p-1} + X^{p-2} + \cdots + X^1 + 1)$$

Insbesondere besitzt der p-te Kreisteilungskörper den Grad $p-1$ über $\mathbb{Q}$.

Beweis. Dieser Beweis wurde in der Vorlesung nicht vorgeführt. □



Beispiel 27.13. Der fünfte Kreisteilungskörper wird von der komplexen Zahl $e^{2\pi i/5}$ erzeugt. Er hat aufgrund von Lemma 27.8 die Gestalt

$$K_5 \cong \mathbb{Q}[X]/(X^4+X^3+X^2+X+1)\,,$$

wobei die Variable X als $e^{2\pi i/5}$ (oder eine andere primitive Einheitswurzel) zu interpretieren ist. Sei $x = e^{2\pi i/5}$ und setze $u = 2x^4+2x+1$. Aus Symmetriegründen muss dies eine reelle Zahl sein. Es ist

$$\begin{aligned} u^2 &= 4x^8+4x^2+1+8x^5+4x^4+4x \\ &= 4x^3+4x^2+1+8+4x^4+4x \\ &= 5+4(x^4+x^3+x^2+x+1) \\ &= 5. \end{aligned}$$

Es ist also $u = \sqrt{5}$ (die positive Wurzel) und somit haben wir eine Folge von quadratischen Körpererweiterungen

$$\mathbb{Q} \subset \mathbb{Q}[\sqrt{5}] \subset K_5\,.$$

Dies zeigt aufgrund von Satz 26.5, dass die fünften Einheitswurzeln konstruierbare Zahlen sind.

Abbildungsverzeichnis