Prof. Dr. H. Brenner **Osnabrück SS 2009**

Einführung in die Algebra

Vorlesung 26

Einheitswurzeln

DEFINITION 26.1. 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 Satz 19.7 ist diese Gruppe zyklisch mit einer Ordnung, die n teilt.

DEFINITION 26.2. 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 26.3. *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

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

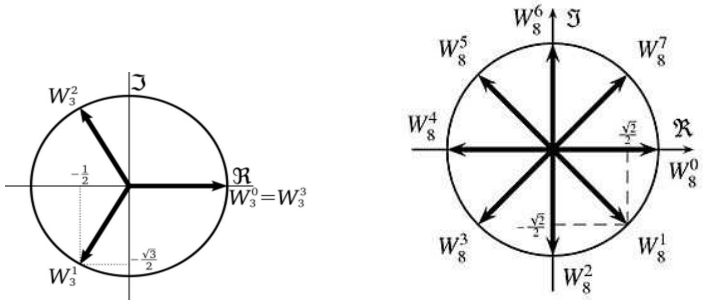
Beweis. Der Beweis verwendet einige Grundtatsachen über die *komplexe Exponentialfunktion*. Es ist

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

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 26.4. 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,

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

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

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

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

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

Lemma 26.6. *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*

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

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

Beweis. Es sei K_n der n-te Kreisteilungskörper über $\mathbb{Q}$. Wegen $(e^{2\pi i/n})^n = 1$ ist $\mathbb{Q}[e^{2\pi i/n}] \subseteq K_n$. Wegen $(e^{2\pi i/n})^k = e^{2\pi ik/n}$ 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.

Beispiel 26.7. 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

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

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 $\mathbb{Q}$.

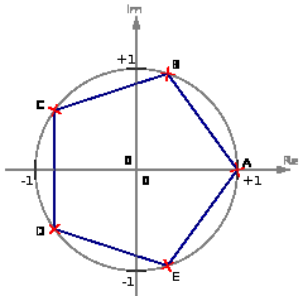
Lemma 26.8. *Sei p eine Primzahl. Dann ist der p-te Kreisteilungskörper gleich*

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

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

Beweis. Der p-te Kreisteilungskörper wird nach Lemma 26.6 von $e^{2\pi i/p}$ erzeugt, er ist also isomorph zu $\mathbb{Q}[X]/(P)$, wobei P das Minimalpolynom von $e^{2\pi i/p}$ bezeichnet. Als Einheitswurzel ist $e^{2\pi i/p}$ eine Nullstelle von $X^p - 1$ und wegen $e^{2\pi i/p} \neq 1$ ist $e^{2\pi i/p}$ eine Nullstelle von $X^{p-1} + X^{p-2} + \ldots + X^1 + 1$. Das Polynom $X^{p-1} + X^{p-2} + \ldots + X^1 + 1$ ist irreduzibel nach Aufgabe 22.12 und daher handelt es sich nach Lemma 21.13 um das Minimalpolynom von $e^{2\pi i/p}$. □

Weiter unten werden wir für jedes n die Minimalpolynome der primitiven n-ten Einheitswurzeln bestimmen.



BEISPIEL 26.9. Der fünfte Kreisteilungskörper wird von der komplexen Zahl $e^{2\pi i/5}$ erzeugt. Er hat aufgrund von Lemma 26.8 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 25.3, dass die fünften Einheitswurzeln konstruierbare Zahlen sind.

Kreisteilungspolynome

DEFINITION 26.10. Sei $n \in \mathbb{N}_+$ und seien $z_1, \ldots, z_{\varphi(n)}$ die primitiven komplexen Einheitswurzeln. Dann heißt das Polynom

$$\Phi_n = \prod_{i=1}^{\varphi(n)} (X - z_i) \in \mathbb{C}[X]$$

das n-te *Kreisteilungspolynom*.

Nach Konstruktion hat das n-te Kreisteilungspolynom den Grad $\varphi(n)$.

LEMMA 26.11. *Sei $n \in \mathbb{N}_+$. Dann gilt in $\mathbb{C}[X]$ die Gleichung*

$$X^n - 1 = \prod_{d|n} \Phi_d\,.$$

Beweis. Jede der n verschiedenen n-ten Einheitswurzeln besitzt eine Ordnung d, die ein Teiler von n ist. Eine n-te Einheitswurzel der Ordnung d ist eine primitive d-te Einheitswurzel. Die Aussage folgt daher aus

$$\begin{aligned} X^n-1 &= \prod_{z \text{ ist } n\text{-te Einheitswurzel}} (X-z) \\ &= \prod_{d|n} \Big(\prod_{z \text{ ist primitive } d\text{-te Einheitswurzel}} (X-z) \Big) \\ &= \prod_{d|n} \Phi_d. \end{aligned}$$

□

Lemma 26.12. *Die Koeffizienten der Kreisteilungspolynome liegen in $\mathbb{Z}$.*

Beweis. Induktion über n. Für $n=1$ ist $\Phi_1 = X-1 \in \mathbb{Z}[X]$. Für beliebiges n betrachten wir die in Lemma 26.11 bewiesene Darstellung

$$X^n-1 = \prod_{d|n} \Phi_d = \Big(\prod_{d|n,\, d \neq n} \Phi_d \Big) \cdot \Phi_n \, .$$

Der linke Faktor ist ein normiertes Polynom und er besitzt nach der Induktionsvoraussetzung Koeffizienten in $\mathbb{Z}$. Daraus folgt mit Aufgabe 26.5, dass auch Φ_n Koeffizienten in $\mathbb{Z}$ besitzt. □

Grundlegend ist die folgende Aussage.

Satz 26.13. *Die Kreisteilungspolynome Φ_n sind irreduzibel über $\mathbb{Q}$.*

Beweis. Nehmen wir an, dass Φ_n nicht irreduzibel über $\mathbb{Q}$ ist. Dann gibt es nach Lemma 20.13 eine Zerlegung $\Phi_n = FG$ mit normierten Polynomen $F, G \in \mathbb{Z}[X]$ von kleinerem Grad. Wir fixieren eine primitive n-te Einheitswurzel ζ. Dann ist nach Definition der Kreisteilungspolynome $\Phi_n(\zeta) = 0$ und daher ist (ohne Einschränkung) $F(\zeta) = 0$. Wir können annehmen, dass F irreduzibel und normiert ist, also das Minimalpolynom von ζ ist.Wir werden zeigen, dass jede primitive n-te Einheitswurzel ebenfalls eine Nullstelle von F ist. Dann folgt aus Gradgründen $\operatorname{grad}(F) = \varphi(n) = \operatorname{grad}(\Phi_n)$ im Widerspruch zur Reduzibilität. Jede primitive Einheitswurzel kann man schreiben als ζ^k mit einer zu n teilerfremden Zahl k. Es genügt dabei, den Fall ζ^p mit einer zu n teilerfremden Primzahl p zu betrachten, da sich jedes ζ^k sukzessive als p-Potenz erhalten lässt (wobei man ζ sukzessive durch ζ^p ersetzt und $F(\zeta^p) = 0$ verwendet). Nehmen wir also an, dass $F(\zeta^p) \neq 0$ ist. Dann muss $G(\zeta^p) = 0$ sein. Daher ist ζ eine Nullstelle des Polynoms $G(X^p)$ und daher gilt $FH = G(X^p)$ mit $H \in \mathbb{Q}[X]$, da ja F das Minimalpolynom von ζ ist. Wegen Aufgabe 26.5 gehören die Koeffizienten von H zu $\mathbb{Z}$. Wir betrachten nun die Polynome Φ_n, F, G, H modulo p, also als Polynome in $\mathbb{Z}/(p)[X]$, wobei wir dafür $\overline{\Phi_n}, \overline{F}$ usw. schreiben. Aufgrund des Frobenius-Homomorphismus

in Charakteristik p und Satz 14.14 gilt

$$\overline{G}(X^p) = (\overline{G}(X))^p \, .$$

Daher ist

$$\overline{FH} \, = \, \overline{G}(X^p) \, = \, (\overline{G}(X))^p .$$

Sei nun $\mathbb{Z}/(p) \subseteq L$ der Zerfällungskörper von $X^n - 1$ über $\mathbb{Z}/(p)$, so dass über L insbesondere auch $\overline{\Phi_n}$ und damit auch $\overline{F}$ in Linearfaktoren zerfällt. Sei $u \in L$ eine Nullstelle von $\overline{F}$. Dann ist u wegen der obigen Teilbarkeitsbeziehung auch eine Nullstelle von $\overline{G}$. Wegen $\overline{\Phi_n} = \overline{FG}$ ist dann u eine mehrfache Nullstelle von $\overline{\Phi_n}$. Damit besitzt auch $X^n - 1$ eine mehrfache Nullstelle in L. Nach dem formalen Ableitungskriterium ist aber $(X^n - 1)' = (n \bmod p)X^{n-1}$ und dieser Koeffizient ist nicht null. Also erzeugt das Polynom $X^n - 1$ und seine Ableitung das Einheitsideal, so dass es nach Aufgabe 23.14 keine mehrfache Nullstellen geben kann und wir einen Widerspruch erhalten. □

Korollar 26.14. *Der n-te Kreisteilungskörper K_n über $\mathbb{Q}$ hat die Beschreibung*

$$K_n = \mathbb{Q}[X]/(\Phi_n) \, ,$$

wobei Φ_n das n-te Kreisteilungspolynom bezeichnet. Der Grad des n-ten Kreisteilungskörpers ist $\varphi(n)$.

Beweis. Es ist $K_n = \mathbb{Q}[\zeta]$, wobei ζ eine primitive n-te Einheitswurzel ist. Nach Definition des Kreisteilungspolynoms ist $\Phi_n(\zeta) = 0$ und nach Satz 26.13 ist das Kreisteilungspolynom irreduzibel, so dass es sich um das Minimalpolynom von ζ handeln muss. Also ist nach Satz 21.12 $K_n \cong \mathbb{Q}[X]/(\Phi_n)$. □

Abbildungsverzeichnis