Die Irreduzibilität der Kreisteilungspolynome

Lukas-Fabian Moser, SS 2013

Eine n-*te Einheitswurzel* ist eine komplexe Zahl $\zeta \in \mathbb{C}$ mit $\zeta^n = 1$; es gibt n Stück von ihnen, nämlich genau die Ecken des regelmäßigen n-Ecks in der Gaußschen Zahlenebene um den Ursprung, das 1 als Ecke hat.

Ist ζ eine Einheitswurzel, so nennt man das kleinste $n \geqslant 1$ mit $\zeta^n = 1$ die *Ordnung* von ζ, notiert als $\operatorname{ord}\zeta = n$. (Dies ist genau die Ordnung von ζ in der multiplikativen Gruppe $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$). Ist ζ eine n-te Einheitswurzel, so gilt stets $\operatorname{ord}\zeta \mid n$; gilt $\operatorname{ord}\zeta = n$, so sagt man, ζ sei eine *primitive* n-te Einheitswurzel.

Ist ζ eine primitive n-te Einheitswurzel, so sind die Potenzen $1, \zeta, \ldots, \zeta^{n-1}$ lauter verschiedene n-te Einheitswurzeln, und da es nur n Stück von ihnen gibt, ist somit jede n-te Einheitswurzel eine Potenz von ζ. Genau dann ist eine Potenz ζ^d wieder primitiv, wenn $\operatorname{ggT}(n, d) = 1$ ist. (Dies sind alles wohlbekannte Überlegungen, wenn man sie als Aussagen über Erzeuger der zyklischen Gruppe $\langle\zeta\rangle \subset \mathbb{C}^*$ auffaßt.)

Für jedes $d \geqslant 1$ nennt man das Polynom

$$\Phi_n := \prod_{\zeta \text{ primitive } n\text{-Einheitswurzel}} (X - \zeta) \in \mathbb{C}[X]$$

das n-*te Kreisteilungspolynom*. Da die n-ten Einheitswurzeln genau die Nullstellen des Polynoms $X^n - 1$ sind, und da jede n-te Einheitswurzel eine primitive d-te Einheitswurzel ist für genau einen Teiler d von n, gilt

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

Aus dieser Gleichung kann man induktiv folgern, daß sogar $\Phi_n \in \mathbb{Z}[X]$ gilt für alle n.

Dazu benötigt man das folgende

Lemma. *Sind $F, G \in \mathbb{C}[X]$ normierte Polynome, und sind G und FG ganzzahlig, so ist auch F ganzzahlig.*

Beweis. Da G normiert ist, führt der Algorithmus zur Polynomdivision von FG durch G in keinem Schritt aus $\mathbb{Z}[X]$ heraus; aber sein Resultat ist F. □

Nun kann man durch Induktion die Ganzzahligkeit der Φ_n zeigen: Für $n = 1$ ist $\Phi_1 = X - 1 \in \mathbb{Z}[X]$, und in der Gleichung $X^n - 1 = \Phi_n \cdot \prod_{d|n, d\neq n} \Phi_d$ ist der zweite Faktor nach Induktionsvoraussetzung schon ganzzahlig, woraus nach dem Lemma $\Phi_n \in \mathbb{Z}[X]$ folgt.

Für *rationale* Polynome kann man im Lemma sogar auf die Voraussetzung der Ganzzahligkeit von G verzichten, was später von Bedeutung sein wird:
Lemma. *Sind $F, G \in \mathbb{Q}[X]$ normierte Polynome, und ist FG ganzzahlig, so sind ist auch F und G ganzzahlig.*

Beweis. Es sei $F = \frac{1}{a}F_0$ und $G = \frac{1}{b}G_0$ mit $a, b \in \mathbb{Z}$ und $F_0, G_0 \in \mathbb{Z}[X]$, wobei wir annehmen können, daß die Koeffizienten von F_0 und G_0 jeweils keinen gemeinsamen Teiler haben. Dann folgt $abFG = F_0G_0$. Da FG ganzzahlig ist, sind also die Koeffizienten beider Seiten durch ab teilbar. Sei nun p ein Primfaktor von ab. Dann sind die Bilder $\overline{F_0}$ und $\overline{G_0}$ in $\mathbb{Z}/p\mathbb{Z}[X]$ beide nicht das Nullpolynom, also auch ihr Produkt nicht (!), und das bedeutet, daß die Koeffizienten von F_0G_0 nicht alle durch p teilbar sind, Widerspruch. Also besitzt ab keine Primfaktoren, und das bedeutet $a, b \in \{\pm 1\}$, also $F, G \in \mathbb{Z}[X]$. □

Satz. *Die Polynome Φ_n sind* irreduzibel *über $\mathbb{Q}$; insbesondere ist also Φ_n das Minimalpolynom jeder primitiven n-ten Einheitswurzel.*

Die Hauptarbeit im Beweis des Satzes leistet das folgende

Lemma. *Ist die primitive n-te Einheitswurzel ζ Nullstelle des irreduziblen Polynoms $F \in \mathbb{Q}[X]$, und ist p eine Primzahl mit $p \nmid n$, so ist auch ζ^p eine Nullstelle von F.*

Beweis des Satzes (mit Hilfe des Lemmas). Es sei ζ eine primitive n-te Einheitswurzel, und es sei $F \in \mathbb{Q}[X]$ ihr Minimalpolynom über $\mathbb{Q}$, d.h. F ist irreduzibel (und normiert) mit $F(\zeta) = 0$. Der Satz ist bewiesen, wenn wir $F = \Phi_n$ zeigen können. Wegen $\Phi_n(\zeta) = 0$ gilt $F \mid \Phi_n$, so daß wir nur $\Phi_n \mid F$ zeigen müssen, und dazu ist zu zeigen, daß jede weitere primitive n-te Einheitswurzel ebenfalls Nullstelle von F ist.

Jede weitere n-te Einheitswurzel hat die Form ζ^d für ein gewisses $d \geqslant 0$, und sie ist genau dann primitiv, wenn $\mathrm{ggT}(n, d) = 1$ ist. Dann gilt aber $d = p_1 \cdot \ldots \cdot p_s$ mit gewissen (nicht notwendig verschiedenen) Primzahlen, die alle kein Teiler von n sind. Wiederholte Anwendung des Lemmas zeigt nun, daß mit ζ auch ζ^{p_1}, $(\zeta^{p_1})^{p_2} = \zeta^{p_1p_2}$, etc. – und schließlich $\zeta^{p_1p_2\cdot\ldots\cdot p_s} = \zeta^d$ Nullstellen von F sind. □

Beweis des Lemmas. Sowohl ζ als auch ζ^p sind n-te Einheitswurzeln, also Nullstellen von $X^n - 1$. Insbesondere ist $X^n - 1 = F \cdot G$ mit einem Polynom $G \in \mathbb{Q}[X]$, und nach dem zweiten Ganzzahligkeitslemma oben gilt $F, G \in \mathbb{Z}[X]$. Nehmen wir an, daß ζ^p keine Nullstelle von F wäre; dann müßte also $G(\zeta^p) = 0$ sein, so daß ζ eine Nullstelle von $G(X^p)$ wäre. Da F das Minimalpolynom von ζ ist, folgt damit $G(X^p) = F \cdot H$ mit $H \in \mathbb{Q}[X]$, und wieder gilt sogar $H \in \mathbb{Z}[X]$.

Der Clou ist nun, überzugehen nach $\mathbb{Z}/p\mathbb{Z}[X]$ (wir schreiben $\overline{F}$, $\overline{G}$, $\overline{H}$ für die dortigen Bilder unserer Polynome). Dort gilt weiterhin $X^n - \overline{1} = \overline{F} \cdot \overline{G}$ und $\overline{G}(X^p) = \overline{F} \cdot \overline{H}$. Der Clou ist aber, daß $\overline{G}(X^p) = \overline{G}(X)^p$ gilt: Denn Potenzieren mit p ist in Charakteristik p additiv, und $\overline{a}^p = \overline{a}$ für alle $\overline{a} \in \mathbb{Z}/p\mathbb{Z}$ nach dem Satz von Euler–Fermat.

Damit haben wir in $\mathbb{Z}/p\mathbb{Z}[X]$ die folgenden Beziehungen: $X^n - \overline{1} = \overline{F} \cdot \overline{G}, \overline{G}^p = \overline{F} \cdot \overline{H}$. Das bedeutet aber, daß $X^n - \overline{1}$ einen mehrfachen Faktor besitzt: Denn jeder irreduzible Faktor von $\overline{F}$ muß wegen $\overline{G}^p = \overline{F} \cdot \overline{H}$ auch in $\overline{G}$ auftreten, und wegen $X^n - \overline{1} = \overline{F} \cdot \overline{G}$ tritt er damit in $X^n - \overline{1}$ doppelt auf. Aber das kann nicht sein: Denn die Existenz doppelter Nullstellen (in irgendwelchen genügend großen Erweiterungskörpern) läßt sich durch Ableiten überprüfen; die Ableitung von $X^n - \overline{1}$ ist $\overline{n} \cdot X^{n-1} \neq 0$ wegen $p \nmid n$, und dieses Polynom hat keine gemeinsamen Nullstellen mit $X^n - \overline{1}$, welches deswegen keine mehrfachen Nullstellen besitzen kann. □