Kreisteilungspolynome

Sei $n \geq 1$ und sei $L/\mathbb{Q}$ der Zerfällungskörper des Polynoms $X^n - 1$. Da $G(L/\mathbb{Q})$ die primitiven n-ten Einheitswurzeln permutiert, gilt

$$\Phi_n(X) = \prod_{\substack{\zeta \in \mu_n(L) \\ \zeta \text{primitiv}}} (X - \zeta) \in \mathbb{Q}[X].$$

Das Polynom $\Phi_n(X)$ heisst das *n-te Kreisteilungspolynom.*

Bemerkung 1. Da das Polynom $X^n - 1$ primitiv ist, $\Phi_n(X)|(X^n - 1)$, und $\Phi_n(X)$ Leitkoeffizient 1 hat, folgt mit dem Gauß-Lemma, dass $\Phi_n(X)$ sogar Koeffizienten in $\mathbb{Z}$ hat und primitiv ist.

Für eine Primzahl p gilt ist jede p-te Einheitswurzel $\zeta \neq 1$ primitiv, so dass also gilt

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

Wir haben in den Übungen gesehen, dass dieses Polynom irreduzibel ist (Eisenstein Kriterium). Wir zeigen nun die folgende allgemeinere Aussage:

Satz 1. *Für jedes $n \geq 1$, ist das Kreisteilungspolynom $\Phi_n(X) \in \mathbb{Q}[X]$ irreduzibel.*

Beweis. Nach dem Gauß-Lemma genügt es zu zeigen, dass $\Phi_n(X)$ irreduzibel in $\mathbb{Z}[X]$ ist. Sei also $\Phi_n(X) = f(X)g(X)$ wobei wir ohne Einschränkung annehmen, dass $f(X)$ irreduzibel und primitiv ist, sowie $g(X)$ primitiv (Gauß-Lemma). Wir zeigen nun die folgende Aussage:

(*) Für jede Primzahl p mit $\mathrm{ggT}(p, n) = 1$ und jede primitive n-te Einheitswurzel $\zeta \in L$ gilt die Implikation $f(\zeta) = 0 \Rightarrow f(\zeta^p) = 0$.

Angenommen (*) gilt nicht. Dann gibt es also eine primitive n-te Einheitswurzel ζ, so dass $f(\zeta) = 0$, aber $f(\zeta^p) \neq 0$. Da ζ^p selbst eine primitive Einheitswurzel und damit eine Nullstelle von $\Phi_n(X)$ ist, folgt $g(\zeta^p) = 0$. Demnach ist ζ eine Nullstelle von $g(X^p)$. Da $f(X)$ irreduzibel ist mit $f(\zeta) = 0$ gilt $g(X^p) = f(X)h(X)$. Wir betrachten nun den Restklassenhomomorphismus

$$\mathbb{Z}[X] \longrightarrow \mathbb{F}_p[X], \ r(X) \mapsto \overline{r}(X)$$

und rechnen

$$\overline{g}(X)^p = \overline{g}(X^p) = \overline{f}(X)\overline{h}(X).$$

Damit gilt auch

$$\overline{\Phi_n}(X)^p = \overline{f}(X)^p \overline{g}(X)^p = \overline{f}(X)^{p+1}\overline{h}(X). \tag{1}$$

Sei nun $M/\mathbb{F}_p$ ein Zerfällungskörper des Polynoms $\overline{\Phi_n}(X) \in \mathbb{F}_p[X]$. Wegen der Annahme $\mathrm{ggT}(p, n) = 1$ gilt $\frac{d}{dX}\overline{\Phi_n}(X) \neq 0$, so dass also $\overline{\Phi_n}(X)$ in M nur einfache Nullstellen hat. Da $\overline{f}(X)$ ein Teiler von $\overline{\Phi_n}(X)$ ist, zerfällt auch $\overline{f}(X)$ in $M[X]$ in Linearfaktoren, hat also insbesondere eine Nullstelle. Sei ξ eine solche Nullstelle. Dann impliziert (1) nach dem Schubladenprinzip jedoch, dass ξ eine mehrfache Nullstelle von $\overline{\Phi_n}(X)$ sein muss. Ein Widerspruch, mit dem also (*) gezeigt ist.

Wir schließen nun den Beweis wie folgt: Die primitiven n-ten Einheitswurzeln in L sind genau die Zahlen ζ^m mit $m \in (\mathbb{Z}/n\mathbb{Z})^*$, also $\mathrm{ggT}(m,n) = 1$. In der Primzerlegung eines Vertreters eines solchen m in $\mathbb{N}$ kommen also nur Primzahlen p vor mit $\mathrm{ggT}(p,n) = 1$. Da $f(X)$ irreduzibel ist, besitzt $f(X)$ in L eine Nullstelle ζ. Durch iterative Anwendung von (*) auf alle Primfaktoren $p_1, p_2, \ldots, p_r$ des Vertreters von m schliessen wir nun, dass auch

$$\zeta^{p_1}, (\zeta^{p_1})^{p_2}, \ldots, \zeta^m$$

Nullstellen von f sein müssen. Also sind alle primitiven n-ten Einheitswurzeln in L Nullstellen von f. Dann muss aber $f = \Phi_n(X)$ gelten, so dass $\Phi_n(X)$ insbesondere irreduzibel ist. □

Korollar 1. *Die Primzerlegung von $X^n - 1 \in \mathbb{Q}[X]$ in irreduzible Faktoren ist gegeben durch*

$$X^n - 1 = \prod_{d|n} \Phi_d(X). \tag{2}$$

Beweis. Dies ist nun klar, denn die Nullstellen von $X^n - 1$ in einem Zerfällungskörper sind genau die n-ten Einheitswurzeln. Doch jede n-te Einheitswurzel ξ ist eine primitive d-te Einheitswurzel für $d = \mathrm{ord}(\xi)$ und es gilt $d|n$. □

Beispiel 1. Mit Formel (2) aus Korollar 1 können wir die Kreisteilungspolynome rekursiv durch Polynomdivision berechnen. Die ersten Polynome sind:

$$\begin{aligned}
\Phi_1(X) &= X - 1 \\
\Phi_2(X) &= X + 1 \\
\Phi_3(X) &= X^2 + X + 1 \\
\Phi_4(X) &= X^2 + 1 \\
\Phi_5(X) &= X^4 + X^3 + x^2 + 1 \\
\Phi_6(X) &= X^2 - X + 1 \\
\Phi_7(X) &= X^6 + X^5 + X^4 + X^3 + X^2 + X + 1 \\
\Phi_8(X) &= X^4 + 1 \\
&\vdots
\end{aligned}$$

Wir erhalten also zum Beispiel

$$X^8 - 1 = \Phi_1(X)\Phi_2(X)\Phi_4(X)\Phi_8(X) = (X-1)(X+1)(X^2+1)(X^4+1).$$

Es gibt aber auch effizientere Methoden, die Kreisteilungspolynome zu bestimmen, zum Beispiel durch die sogenannte Möbius-Inversion.