Satz. *Sei $n \in \mathbb{N}$ und $g_n \in \mathbb{Z}[x]$ das n-te Kreisteilungspolynom über $\mathbb{Q}$. Dann ist g_n irreduzibel über $\mathbb{Q}[X]$.*

Beweis. Es genügt zu zeigen, dass das normierte Polynom g_n in $\mathbb{Z}[x]$ irreduzibel ist. Sei $h(x) \in \mathbb{Z}[x]$ ein irreduzibler Faktor von $g_n(x)$. Dann gibt es ein $f(x) \in \mathbb{Z}[x]$ mit $g_n = h \cdot f$, und die Polynome f und h sind beide normiert. Weiters sei $\zeta \in F$ eine Wurzel von h und p eine Primzahl mit $\mathrm{ggT}(p, n) = 1$. Zunächst wird gezeigt, dass auch ζ^p eine Wurzel von h ist: Wegen $\mathrm{ggT}(p, n) = 1$ ist ζ^p eine primitive n-te Einheitswurzel, also eine Wurzel von g_n. Damit ist ζ^p entweder Wurzel von h oder f.

Angenommen, ζ^p ist eine Wurzel von $f(x) = \sum_{i=0}^{t} a_i x^i$, dann ist ζ eine Wurzel von $f(x^p)$, und somit muss $h(x)$ ein Teiler von $f(x^p)$ in $\mathbb{Q}[x]$ sein. Also gibt es ein $k(x) \in \mathbb{Q}[x]$ mit $f(x^p) = h(x)k(x)$. Aus der Eindeutigkeit bei der Division mit Rest in $\mathbb{Q}[x]$ und $\mathbb{Z}[x]$ folgt $k(x) \in \mathbb{Z}[x]$.

Die kanonische Projektion $\mathbb{Z} \to \mathbb{Z}_p$ mit $b \mapsto \bar{b}$ induziert einen Ringepimorphismus $\mathbb{Z}[x] \to \mathbb{Z}_p[x]$ mit

$$g = \sum_{i=0}^{s} b_i x^i \mapsto \bar{g} = \sum_{i=0}^{s} \bar{b}_i x^i.$$

Daher gilt $\bar{f}(x^p) = \bar{h}(x)\bar{k}(x)$ in $\mathbb{Z}_p[x]$. Wegen $\chi(\mathbb{Z}_p) = p$ folgt $\bar{f}(x)^p = \bar{f}(x^p) = \bar{h}(x)\bar{k}(x)$, und ein irreduzibler Faktor von $\bar{h}(x)$ mit Grad größer gleich 1 muss $\bar{f}(x)^p$ und damit auch $\bar{f}(x)$ teilen.

Andererseits ist $g_n(x)$ ein Faktor von $x^n - 1$, d. h. es gilt $x^n - 1 = g_n(x)r(x) = f(x)h(x)r(x)$ für ein $r(x) \in \mathbb{Z}[x]$. Daraus folgt $x^n - \bar{1} = \overline{x^n - 1} = \bar{f}(x)\bar{h}(x)\bar{r}(x)$. Da $\bar{f}$ und $\bar{h}$ einen gemeinsamen Faktor haben, muss $x^n - \bar{1} \in \mathbb{Z}_p[x]$ eine mehrfache Nullstellen im Zerfällungskörper haben. Das ist aber ein Widerspruch, da wegen $\mathrm{ggT}(p, n) = 1$ alle n-ten Einheitswurzeln verschieden sind.

Somit ist für jede Primzahl p mit $p \nmid n$ auch ζ^p eine Nullstelle von h. Da jede primitive Einheitswurzel ξ als $\xi = \zeta^{p_1 \cdots p_s}$ für (nicht notwendigerweise verschiedene) Primzahlen p_i mit $p_i \nmid n$ dargestellt werden kann, folgt induktiv, dass auch ξ eine Nullstelle von h ist. □