Aufgabe F15T2A3 (12 Punkte)

Sei p eine Primzahl und $a \in \mathbb{Z}$ keine p-te Potenz in $\mathbb{Z}$. Man zeige, dass das Polynom $x^p - a$ über $\mathbb{Q}$ irreduzibel ist.

Hinweis: Betrachte die Nullstellen von $x^p - a$ in $\mathbb{C}$ und untersuche den konstanten Term eines echten Teilers von $x^p - a$ auf Ganzzahligkeit.

Lösung:

Zunächst gilt $a \neq 0$, da $0^p = 0$ gilt und a in $\mathbb{Z}$ keine p-te Potenz ist. Sei nun $\zeta \in \mathbb{C}^\times$ eine primitive p-te Einheitswurzel. Dann sind die Nullstellen des Polynoms $f = x^p - a$ gegeben durch $\alpha_k = \zeta^k \sqrt[p]{a}$, für $0 \leq k < p$. Insbesondere gilt $|\alpha_k| = \sqrt[p]{|a|}$ für den komplexen Absolutbetrag sämtlicher Nullstellen. Nehmen wir nun an, dass f über $\mathbb{Q}[x]$ reduzibel ist. Dann ist f nach dem Gaußschen Lemma sogar in $\mathbb{Z}[x]$ reduzibel. Es gibt also Polynome $g, h \in \mathbb{Z}[x]$, beides keine Einheiten in $\mathbb{Z}[x]$, mit $f = gh$. Weil f normiert ist, müssen die Leitkoeffizienten von g und h beide gleich 1 oder -1 sein. Nach eventueller Ersetzung von g, h durch $-g, -h$ können wir davon ausgehen, dass g und h beide normiert sind. Weil g und h keine Einheiten sind, sind die Polynomgrade $m = \mathrm{grad}(g)$ und $n = \mathrm{grad}(h)$ beide größer als Null, also $0 < m, n < p$.

Der konstante Term $a_0 \in \mathbb{Z}$ von g ist das Produkt von insgesamt m Nullstellen des Polynoms f. Weil jede dieser Nullstellen vom Betrag $\sqrt[p]{|a|}$ ist, gilt $|a_0| = |a|^{m/p}$ und somit $|a_0|^p = |a|^m$. Dies ist nur möglich, wenn alle Primfaktoren in $|a| \in \mathbb{N}$ mit Vielfachheiten vorkommen, die von p geteilt werden. Sind nämlich $|a_0| = \prod_{i=1}^r p_i^{e_i}$ und $|a| = \prod_{i=1}^r p_i^{f_i}$ die Primfaktorzerlegungen von $|a_0|$ und $|a|$, mit $r \in \mathbb{N}_0$, verschiedenen Primzahlen $p_1, ..., p_r$ und $e_1, f_1, ..., e_r, f_r \in \mathbb{N}_0$, dann folgt aus $|a_0|^p = |a|^m$ die Gleichung

$$\prod_{i=1}^{r} p_i^{pe_i} \quad = \quad \prod_{i=1}^{r} p_i^{mf_i}$$

und somit $pe_i = mf_i$ für $1 \leq i \leq r$. Wegen $\mathrm{ggT}(m, p) = 1$ folgt daraus $p | f_i$ für $1 \leq i \leq r$. Dies zeigt, dass $|a|$ eine p-te Potenz ist; es gibt also ein $b \in \mathbb{N}$ mit $|a| = b^p$, was zu $a \in \{\pm b^p\}$ äquivalent ist. Der Fall $a = b^p$ ist nach Voraussetzung ausgeschlossen. Ist p ungerade, dann ist auch $a = -b^p = (-b)^p$ laut Vorausetzung nicht möglich. Also muss $p = 2$ sein. Dann wiederum ist a nach Voraussetzung kein Quadrat in $\mathbb{Z}$. Also ist $x^p - a = x^2 - a$ irreduzibel in $\mathbb{Z}[x]$ und nach dem Gaußschen Lemma auch im Polynomring $\mathbb{Q}[x]$.