F15-T2-A3

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.)

Lösungsvorschlag. Die Nullstellen von $X^p - a \in \mathbb{Q}[X]$ in $\mathbb{C}$ sind bekannt und von der Form $\zeta_p^i \sqrt[p]{a}$ für ζ_p eine p-te Einheitswurzel. Nenne von nun an $\alpha_i := \zeta_p^i \sqrt[p]{a}$. Angenommen, $X^p - a$ wäre reduzibel, besäße also einen Faktor $g(X) \in \mathbb{Q}[X]$ mit $\deg(g) = r < p$. Seien $\{\alpha_i \ : \ i \in I \subsetneq \{0, \dots, p-1\}, \ |I| = r\}$ die Nullstellen von g, also

$$g(X) = \prod_{i \in I} (X - \alpha_i).$$

Wie im Hinweis empfohlen betrachten wir den konstanten Faktor von g, der sich zu

$$g_0 := (-1)^r \prod_{i \in I} \alpha_i = \zeta_p^{\sum_{i \in I} i} \sqrt[p]{a^r}$$

berechnet. Nun soll also $g_0 \in \mathbb{Z}$ gelten. Wegen $\sqrt[p]{a^r} \in \mathbb{R}$ muss jedenfalls $\zeta_p^{\sum_{i \in I} i} \in \mathbb{R}$ gelten, also $g_0 = \pm \sqrt[p]{a^r} \in \mathbb{Z}$. Damit muss also a^r eine p-te Wurzel in $\mathbb{Z}$ sein. Da p prim ist, also $\mathrm{ggT}(r, p) = 1$. muss damit schon a eine p-te Wurzel in $\mathbb{Z}$ sein.
Eine etwas elegantere Umformulierung: Wir nehmen wieder an, dass $X^p - a$ einen echten Faktor $g(X)$ mit $\deg(g) = r < p$ besitzt – hier nehmen wir zudem ohne Einschränkung an, dass g irreduzibel ist. Seien nun β_i, $i = 1, \dots, r$ die Nullstellen von g, β eine beliebige davon. Setze $L := \mathbb{Q}(\beta)$. Dann ist die Norm $N_{L/\mathbb{Q}}(\beta)$ ja gerade definiert durch

$$N_{L/\mathbb{Q}}(\beta) = (-1)^r \prod_{i=1}^{r} \beta_i \in \mathbb{Q},$$

mit anderen Worten ist $N_{L/\mathbb{Q}}(\beta)$ gerade der konstante Koeffizient von g und somit insbesondere schon ein Element in $\mathbb{Z}$. Wir wissen, dass die Norm multiplikativ ist, also

$$N_{L/\mathbb{Q}}(\beta)^p = N_{L/\mathbb{Q}}(\beta^p) = N_{L/\mathbb{Q}}(a) = a^r,$$

was bedeutet $a^r = N_{L/\mathbb{Q}}(\beta)^p$ ist eine p-te Potenz in $\mathbb{Z}$. Wie in der ursprünglichen Version folgern wir wegen $\mathrm{ggT}(r, p) = 1$, dass bereits a eine p-te Potenz in $\mathbb{Z}$ gewesen sein muss.