Aufgabe F13T1A2 (5+5+5 Punkte)

Sei $f = x^2 - 2 \in \mathbb{Q}[x]$. Sei weiter $f_0 = x$ und für $n \geq 1$ sei $f_n = f_{n-1}(f) = f(f_{n-1})$ das n-fach iterierte Polynom, also

$$f_1 = x^2 - 2, \quad f_2 = (x^2-2)^2 - 2, \quad f_3 = ((x^2-2)^2-2)^2 - 2 \quad \text{usw.}$$

Zeigen Sie:

(a) Alle Polynome f_n sind irreduzibel.

(b) Sei $z_n = e^{\pi i/2^{n+1}}$ eine primitive 2^{n+2}-te Einheitswurzel. Für k ungerade ist $2\cos\frac{k\pi}{2^{n+1}} = z_n^k + z_n^{-k}$ eine Nullstelle von f_n.

(c) Die Galoisgruppe von f_2 über $\mathbb{Q}$ ist abelsch.

Lösung:

zu (a) Wir beweisen durch vollständige Induktion, dass das Bild $\bar{f}_n$ von f_n in $\mathbb{Z}/4\mathbb{Z}[x]$ durch $\bar{f}_n = x^{2^n} + \bar{2}$ gegeben ist. Für $n = 1$ ist dies offenbar der Fall. Setzen wir die Aussage nun für n voraus. Dann gilt $\bar{f}_{n+1} = \bar{f}(\bar{f}_n) = \bar{f}(x^{2^n} + \bar{2}) = (x^{2^n} + \bar{2})^2 - \bar{2} = x^{2^{n+1}} + \bar{4}x^{2^n} + \bar{4} - \bar{2} = x^{2^{n+1}} + \bar{2}$. Damit ist die Gleichung für alle $n \in \mathbb{N}$ bewiesen. Außerdem ist das Polynom f_1 normiert, und auf Grund der Gleichung $f_{n+1} = f_n^2 - 2$ ist mit f_n auch f_{n+1} normiert, für alle $n \in \mathbb{N}$.

Sei nun $n \in \mathbb{N}$, und seien $a_0, ..., a_{2^n} \in \mathbb{Z}$ die Koeffizienten mit $f_n = \sum_{r=0}^{2^n} a_r x^r$. Weil jedes f_n normiert ist, gilt jeweils $a_{2^n} = 1$, insbesondere $2 \nmid a_{2^n}$. Wegen $\bar{f}_n = x^{2^n} + \bar{2}$ gilt darüber hinaus $2 \mid a_r$ für $0 \leq r < 2^n$ und $a_0 \equiv 2 \bmod 4$, also $4 \nmid a_0$. Weil f_n normiert ist, ist f_n auch primitiv. Somit sind alle Voraussetzungen des Eisenstein-Kriteriums sind erfüllt. Folglich ist f_n in $\mathbb{Z}[x]$ und nach dem Gaußschen Lemma auch in $\mathbb{Q}[x]$ irreduzibel.

zu (b) Wiederum beweisen wir die Aussage durch vollständige Induktion über n. Für $n = 1$ ist z_1 nach Definition eine primitive achte Einheitswurzel. Für jedes ungerade $k \in \mathbb{Z}$ ist z_1^{2k} somit eine primitive vierte Einheitswurzel, also $z_1^{2k} \in \{\pm i\}$. Im Fall $z_1^{2k} = i$ gilt $z_1^{-2k} = -i$, und wir erhalten

$$f_1(z_1 + z_1^{-1}) \quad = \quad (z_1^k + z_1^{-k})^2 - 2 \quad = \quad z_1^{2k} + 2 + z_1^{-2k} - 2 \quad = \quad z_1^{2k} + z_1^{-2k} \quad = \quad i + (-i) \quad = \quad 0.$$

Dieselbe Rechung liefert $f_1(z_1 + z_1^{-1}) = 0$ auch im Fall $z_1^{2k} = -i$. Sei nun $n \in \mathbb{N}$, und setzen wir die Aussage für n voraus. Nach Induktionsvoraussetzung ist $z_n^k + z_n^{-k}$ für jedes ungerade $k \in \mathbb{Z}$ eine Nullstelle von f_n. Wegen $f_{n+1} = f_n(f)$ und $z_{n+1}^2 = z_n$ gilt nun für jedes ungerade $k \in \mathbb{Z}$ jeweils

$$f_{n+1}(z_{n+1}^k + z_{n+1}^{-k}) \quad = \quad f_n(f(z_{n+1}^k + z_{n+1}^{-k})) \quad = \quad f_n((z_{n+1}^k + z_{n+1}^{-k})^2 - 2) \quad =$$

$$f_n(z_{n+1}^{2k} + 2 + z_{n+1}^{-2k} - 2) \quad = \quad f_n(z_n^k + z_n^{-k}) \quad = \quad 0$$

wobei im letzten Schritt die Induktionsvoraussetzung angewendet wurde.

zu (c) Nach Teil (b) sind die Elemente $z_2^k + z_2^{-k}$ für jedes ungerade $k \in \mathbb{Z}$ Nullstellen von f_2. Wegen $|z_2| = 1$ ist z_2^{-k} jeweils das zu z_2^k konjugiert-komplexe Element. Daraus folgt $z_2^k + z_2^{-k} = 2\mathrm{Re}(z_2^k) = 2\mathrm{Re}(e^{k\pi i/8}) = 2\cos(\frac{k\pi}{8})$. Weil die Kosinusfunktion auf dem Intervall $[0,\pi]$ streng monoton fallend ist, sind durch $2\cos(\frac{k\pi}{8})$ mit $k \in \{1,3,5,7\}$ vier verschiedene Nullstellen von f_2 gegeben. Wegen $\mathrm{grad}(f_2)$ ist dies die genaue Menge der Nullstellen von f_2 in $\mathbb{C}$. Somit ist

$$L \quad = \quad \mathbb{Q}(2\cos(\tfrac{\pi}{8}), 2\cos(\tfrac{3\pi}{8}), 2\cos(\tfrac{5\pi}{8}), 2\cos(\tfrac{7\pi}{8}))$$

der Zerfällungskörper von f_2 in $\mathbb{C}$. Als Zerfällungskörper eines Polynoms über $\mathbb{Q}$ ist L normal über $\mathbb{Q}$, insbesondere algebraisch. Wegen $\mathrm{char}(\mathbb{Q}) = 0$ ist L damit auch separabel über $\mathbb{Q}$. Insgesamt ist $L|\mathbb{Q}$ eine Galois-Erweiterung.

Weil z_2 eine primitive 16-te Einheitswurzel ist, handelt es sich bei $\mathbb{Q}(z_2)$ um den 16-ten Kreisteilungskörper. Laut Vorlesung ist $\mathbb{Q}(z_2)|\mathbb{Q}$ galoissch, mit Galoisgruppe $G = \mathrm{Gal}(\mathbb{Q}(z_2)|\mathbb{Q})$ isomorph zu $(\mathbb{Z}/16\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Insbesondere ist G abelsch. Wegen $\cos(\frac{k\pi}{8}) = z_2^k + z_2^{-k} \in \mathbb{Q}(z_2)$ für $k = 1,3,5,7$ ist L ein Teilkörper von $\mathbb{Q}(z_2)$. Weil es sich bei $L|\mathbb{Q}$ um eine normale Teilerweiterung von $\mathbb{Q}(z_2)|\mathbb{Q}$ handelt, ist $\mathrm{Gal}(f_2|\mathbb{Q}) = \mathrm{Gal}(L|\mathbb{Q})$ laut Vorlesung isomorph zu einer Faktorgruppe von G. Als Faktorgruppe einer abelschen Gruppe ist auch $\mathrm{Gal}(f_2|\mathbb{Q})$ abelsch.