Aufgabe H19T3A5 (12 Punkte)

Es seien $p \geq 3$ eine Primzahl und $\zeta \in \mathbb{C}$ eine primitive p-te Einheitswurzel.

(a) Sei $a \in \mathbb{N}$. Zeigen Sie, dass das Polynom $x^{a+1} - 1$ ein Teiler des Polynoms $x^{2a} - x^{a+1} - x^{a-1} + 1$ in $\mathbb{Q}[x]$ ist und bestimmen Sie den Quotienten.

(b) Zeigen Sie, dass die Körpererweiterung $\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q}$ galoissch ist und dass $\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q})$ zyklisch von Ordnung $\frac{1}{2}(p-1)$ ist.

Lösung:

zu (a) Es gilt $(x^{a+1} - 1)(x^{a-1} - 1) = x^{2a} - x^{a-1} - x^{a+1} + 1$. Also ist $x^{a+1} - 1$ tatsächlich ein Teiler von $x^{2a} - x^{a+1} - x^{a-1} + 1$, und der Quotient ist $x^{a-1} - 1$.

zu (b) Zunächst zeigen wir, dass $\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q}$ eine Galois-Erweiterung ist. Aus der Vorlesung ist bekannt, dass die Erweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$ galoissch ist und $G = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z}$ gilt. Die Galoisgruppe der Erweiterung ist also zyklisch von Ordnung $p-1$. Ebenso ist $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(p) = p-1$ bekannt, wobei φ die Eulersche φ-Funktion bezeichnet. Nun ist $\mathbb{Q}(\zeta + \zeta^{-1})$ wegen $\zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)$ ein Zwischenkörper von $\mathbb{Q}(\zeta)|\mathbb{Q}$. Nach dem Hauptsatz der Galoistheorie entspricht diesem Zwischenkörper die Untergruppe $N = \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}(\zeta + \zeta^{-1}))$ von G. Weil G als zyklische Gruppe insbesondere abelsch ist, sind alle Untergruppen von G Normalteiler. Aus $N \trianglelefteq G$ wiederum folgt, dass auch $\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q}$ eine Galois-Erweiterung ist.

Nun bestimmen wir die Ordnung von $H = \mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q})$. Weil $\mathbb{Q}(\zeta + \zeta^{-1})$ ein Zwischenkörper von $\mathbb{Q}(\zeta)|\mathbb{Q}$ ist, liefert die Gradformel

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1}] \cdot [\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}].$$

Um den Grad $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]$ zu bestimmen, betrachten wir das Polynom $f = x^2 - (\zeta + \zeta^{-1})x + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[x]$. Dieses Polynom ist normiert und hat ζ als Nullstelle. Außerdem ist es irreduzibel. Denn wäre dies nicht der Fall, dann wäre die Nullstelle ζ wegen $\mathrm{grad}(f) = 2$ im Grundkörper $\mathbb{Q}(\zeta + \zeta^{-1})$ enthalten. Weil $\zeta \in \mathbb{C}$ eine Einheitswurzel ist, gilt $\zeta\bar{\zeta} = |\zeta|^2 = 1$ und somit $\bar{\zeta} = \zeta^{-1}$. Für jede komplexe Zahl z ist $z + \bar{z} = 2\mathrm{Re}(z)$ reell. Also gilt dasselbe auch für $\zeta + \zeta^{-1} = \zeta + \bar{\zeta}$, und folglich ist $\mathbb{Q}(\zeta + \zeta^{-1})$ in $\mathbb{R}$ enthalten. Aber andererseits gilt wegen $p \geq 3$ die Ungleichung $\sin(\frac{2\pi}{p}) \neq 0$ und somit $\zeta = \cos(\frac{2\pi}{p}) + i\sin(\frac{2\pi}{p}) \in \mathbb{C} \setminus \mathbb{R}$. Damit ist $\zeta \in \mathbb{Q}(\zeta + \zeta^{-1})$ ausgeschlossen. Insgesamt ist f damit das Minimalpolynom von ζ über $\mathbb{Q}(\zeta + \zeta^{-1})$, und es folgt $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = [\mathbb{Q}(\zeta + \zeta^{-1})(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})] = \mathrm{grad}(f) = 2$. Damit wiederum erhalten wir

$$[\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] \quad = \quad \frac{[\mathbb{Q}(\zeta) : \mathbb{Q}]}{[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta + \zeta^{-1})]} \quad = \quad \frac{p-1}{2}.$$

Weil $\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q}$ eine Galois-Erweiterung ist, folgt $|H| = |\mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1})|\mathbb{Q})| = [\mathbb{Q}(\zeta + \zeta^{-1}) : \mathbb{Q}] = \frac{1}{2}(p-1)$ für die Ordnung der Gruppe H.

Aus der Galoistheorie ist auch bekannt, dass $H = \mathrm{Gal}(\mathbb{Q}(\zeta + \zeta^{-1}|\mathbb{Q}))$ zur Faktorgruppe G/N isomorph ist. Nun ist allgemein jede Faktorgruppe einer zyklischen Gruppe selbst zyklisch; daraus folgt insgesamt, dass H eine zyklische Gruppe der Ordnung $\frac{1}{2}(p-1)$ ist. Ist nämlich G eine beliebige zyklische Gruppe und $g \in G$ mit $G = \langle g \rangle$, und N ein Normalteiler von G, so gilt $G/N = \langle gN \rangle$. Denn ist $g_1 N \in G/N$ ein beliebiges Element, mit $g_1 \in G$, dann existiert wegen $G = \langle g \rangle$ ein $m \in \mathbb{Z}$ mit $g_1 = g^m$. Daraus folgt $g_1 N = g^m N = (gN)^m \in \langle gN \rangle$.