Aufgabe F13T3A5

Für $n \in \mathbb{N}$ sei $\zeta_n := e^{2\pi i/n}$ und $k_n = \mathrm{kgV}\{1, ..., n\}$ das kleinste gemeinsame Vielfache der Zahlen $1, ..., n$. Zeigen Sie, für alle $n \in \mathbb{N}$, die folgenden Formeln über die Grade von Körpererweiterungen:

(a) $[\mathbb{Q}(\zeta_1, ..., \zeta_n) : \mathbb{Q}] = \Phi(k_n)$, wobei Φ die Eulersche Φ-Funktion bezeichnet.

(b) $[\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2}) : \mathbb{Q}] = k_n$.

Lösung:

zu (a) Zunächst beweisen wir die Gleichung

$$\mathbb{Q}(\zeta_1, ..., \zeta_n) \quad = \quad \mathbb{Q}(\zeta_{k_n}).$$

„$\subseteq$" Nach Voraussetzung ist k_n ein Vielfaches von d für $1 \le d \le n$. Es gibt also jeweils ein ℓ_d mit $k_n = d\ell_d$. Wegen $(\zeta_{k_n})^{\ell_d} = (e^{2\pi i/k_n})^{\ell_d} = e^{2\pi i \ell_d/k_n} = e^{2\pi i/d} = \zeta_d$ für $1 \le d \le n$ sind die Zahlen $\zeta_1, ..., \zeta_n$ in $\mathbb{Q}(\zeta_{k_n})$ enthalten. Weil $\mathbb{Q}(\zeta_1, ..., \zeta_n)$ nach Definition der kleinste Zwischenkörper von $\mathbb{C}|\mathbb{Q}$ ist, der diese Elemente enthält, folgt daraus die behauptete Inklusion.

„$\supseteq$" Weil $\mathbb{Z}$ ein Hauptidealring ist, gibt es ein $m \in \mathbb{N}$ mit

$$\left(\frac{k_n}{1}, \frac{k_n}{2}, ..., \frac{k_n}{n}\right) \quad = \quad (m).$$

Wegen $\frac{k_n}{d} \in (m)$ gibt es jeweils ein $a_d \in \mathbb{Z}$ mit $\frac{k_n}{d} = a_d m$ für $1 \le d \le n$, was zu $a_d dm = k_n$ umgeformt werden kann. Es gilt also $\frac{k_n}{m} = da_d$ und somit $d \mid \frac{k_n}{m}$ für $1 \le d \le n$. Es folgt $k_n \mid \frac{k_n}{m}$ wegen $k_n = \mathrm{kgV}(1, 2, ..., n)$. Daraus wiederum folgt, dass ein $b \in \mathbb{Z}$ mit $\frac{k_n}{m} = bk_n \Leftrightarrow k_n = bmk_n$ existiert. Es muss also $bm = 1$ und damit $m = 1$ gelten. Insgesamt haben wir also

$$\left(\frac{k_n}{1}, \frac{k_n}{2}, ..., \frac{k_n}{n}\right) \quad = \quad (1)$$

nachgewiesen. Insbesondere ist 1 in diesem Ideal enthalten, es gibt also $a_1, ..., a_n \in \mathbb{Z}$ mit $\sum_{d=1}^{n} a_d \frac{k_n}{d} = 1$. Es folgt

$$\frac{1}{k_n} = \sum_{d=1}^{n} \frac{a_d}{d} \quad \Rightarrow \quad \frac{2\pi i}{k_n} = \sum_{d=1}^{n} a_d \frac{2\pi i}{d} \quad \Rightarrow \quad e^{2\pi i/k_n} = \prod_{d=1}^{n} (e^{2\pi i/d})^{a_d} \quad \Rightarrow \quad \zeta_{k_n} = \prod_{d=1}^{n} \zeta_d^{a_d}.$$

Die letzte Gleichung zeigt, dass ζ_{k_n} im Körper $\mathbb{Q}(\zeta_1, ..., \zeta_n)$ enthalten ist. Weil es sich bei $\mathbb{Q}(\zeta_{k_n})$ um den kleinsten Zwischenkörper von $\mathbb{C}|\mathbb{Q}$ handelt, der ζ_{k_n} enthält, folgt $\mathbb{Q}(\zeta_{k_n}) \subseteq \mathbb{Q}(\zeta_1, ..., \zeta_n)$.

Weil laut Vorlesung für jedes $m \in \mathbb{N}$ jeweils $[\mathbb{Q}(\zeta_m) : \mathbb{Q}] = \Phi(m)$ gilt, erhalten wir

$$[\mathbb{Q}(\zeta_1, ..., \zeta_n) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\zeta_{k_n}) : \mathbb{Q}] \quad = \quad \Phi(k_n).$$

zu (b) Hier beweisen wir zunächst die Gleichung

$$\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2}) \quad = \quad \mathbb{Q}(\sqrt[k_n]{2}).$$

„$\subseteq$" Wie bereits in Teil (a) festgestellt, gibt es für jedes $d \in \mathbb{N}$ mit $1 \leq d \leq n$ ein $\ell_d \in \mathbb{N}$ mit $k_n = d\ell_d$. Es folgt

$$(\sqrt[k_n]{2})^{\ell_d} \quad = \quad (2^{\frac{1}{k_n}})^{\ell_d} \quad = \quad 2^{\frac{\ell_d}{k_n}} \quad = \quad 2^{\frac{1}{d}} \quad = \quad \sqrt[d]{2}$$

und somit $\sqrt[d]{2} \in \mathbb{Q}(\sqrt[k_n]{2})$ für $1 \leq d \leq n$. Weil $\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2})$ nach Definition der kleinste Zwischenkörper von $\mathbb{C}|\mathbb{Q}$ ist, der diese Elemente enthält, folgt $\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2}) \subseteq \mathbb{Q}[k_n]2$.

„$\supseteq$" In Teil (a) wurde gezeigt, dass $a_1, ..., a_n \in \mathbb{Z}$ existieren, so dass die Gleichung $\frac{1}{k_n} = \sum_{d=1}^{n} \frac{a_d}{d}$ erfüllt ist. Daraus folgt

$$\sqrt[k_n]{2} \quad = \quad 2^{\frac{1}{k_n}} \quad = \quad 2^{\sum_{d=1}^{n} \frac{a_d}{d}} \quad = \quad \prod_{d=1}^{n} 2^{\frac{a_d}{d}} \quad = \quad \prod_{d=1}^{n} (\sqrt[d]{2})^{a_d}.$$

Die Gleichung zeigt, dass $\sqrt[k_n]{2}$ im Körper $\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2})$ enthalten ist. Weil $\mathbb{Q}(\sqrt[k_n]{2})$ nach Definition der kleinste Zwischenkörper von $\mathbb{C}|\mathbb{Q}$ ist, der $\sqrt[k_n]{2}$ enthält, folgt $\mathbb{Q}(\sqrt[k_n]{2}) \subseteq \mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2})$.

Nach dem Eisenstein-Kriterium ist das Polynom $f_n = x^{k_n} - 2$ im Polynomring $\mathbb{Q}[x]$ irreduzibel, außerdem normiert. Wegen $f_n(\sqrt[k_n]{2}) = 0$ ist es also das Minimalpolynom von $\sqrt[k_n]{2}$ über $\mathbb{Q}$. Wir erhalten

$$[\mathbb{Q}(\sqrt[1]{2}, ..., \sqrt[n]{2}) : \mathbb{Q}] \quad = \quad [\mathbb{Q}(\sqrt[k_n]{2} : \mathbb{Q}] \quad = \quad \mathrm{grad}(f_n) \quad = \quad k_n.$$