F23-T3-A4

Es sei $\zeta \in \mathbb{C}$ eine primitive 7-te Einheitswurzel, und es seien $a := \zeta+\zeta^6$ und $b := \zeta+\zeta^2+\zeta^4$.

a) Geben Sie einen konkreten Isomorphismus zwischen der Einheitengruppe von $\mathbb{Z}/7\mathbb{Z}$ und der Galoisgruppe von $\mathbb{Q}(\zeta)|\mathbb{Q}$ an.

b) Zeigen Sie, dass die Körpererweiterungen $\mathbb{Q}(a)|\mathbb{Q}$ und $\mathbb{Q}(b)|\mathbb{Q}$ galoisch sind, und bestimmen Sie die zugehörigen Galoisgruppen bis auf Isomorphie.

c) Bestimmen Sie die Minimalpolynome von a und b über $\mathbb{Q}$.

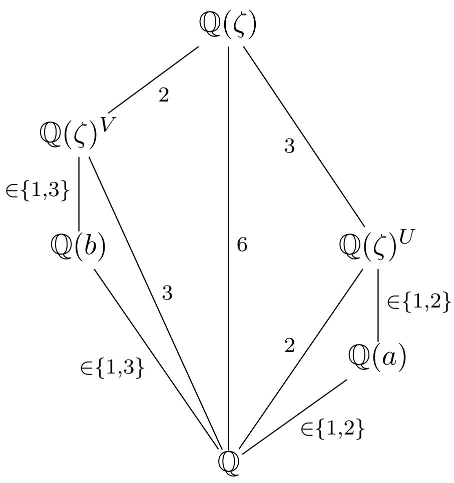
Lösungsvorschlag. Zu a). Für ein $[n] \in (\mathbb{Z}/7\mathbb{Z})^\times$ ist n teilerfremd zu 7, und ζ^n ebenfalls eine primitive 7-te Einheitswurzel und eine Nullstelle des Minimalpolynoms $\Phi_7(X)$ von ζ über $\mathbb{Q}$. Man bemerke, dass ζ^n dabei ein wohldefinierter Ausdruck ist, denn es gilt $\zeta^7 = 1$. Wir können damit den Isomorphismus angeben:

$$\begin{aligned} (\mathbb{Z}/7\mathbb{Z})^\times &\longrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q}) \\ [n] &\longmapsto \sigma_n : \mathbb{Q}(\zeta) \to \mathbb{Q}(\zeta), \zeta \mapsto \zeta^n. \end{aligned}$$

Zu b). Es ist $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ nach Teilaufgabe a) abelsch, sodass jede Untergruppe ein Normalteiler ist und nach dem Hauptsatz der Galoistheorie jede Zwischenerweiterung normal über dem Grundkörper $\mathbb{Q}$. Die Separabilität folgt aus der Separabilität von $\mathbb{Q}(\zeta)|\mathbb{Q}$, sodass $\mathbb{Q}(a)|\mathbb{Q}$ und $\mathbb{Q}(b)|\mathbb{Q}$ galoisch sind.
Um die Gruppen besser zu verstehen, wollen wir die Zwischenkörper $\mathbb{Q}(a)$ und $\mathbb{Q}(b)$ als Fixkörper verstehen. Die Untergruppen von $\mathrm{Gal}(\mathbb{Q}(\zeta)|\mathbb{Q})$ sind unter der Verwendung der Isomorphie aus Teilaufgabe a) leicht zu identifizieren als $U := \{\sigma_1, \sigma_6\}$ und $V := \{\sigma_1, \sigma_2, \sigma_4\}$. Damit gilt für die Körpergrade $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)^U] = |U| = 2$ und $[\mathbb{Q}(\zeta) : \mathbb{Q}(\zeta)^V] = |V| = 3$. Wir wollen $a \in \mathbb{Q}(\zeta)^U$ und $b \in \mathbb{Q}(\zeta)^V$ überprüfen und nach Definition des Fixkörpers genügt es zu berechnen:

- $\sigma_1(a) = a$
- $\sigma_6(a) = \zeta^6 + (\zeta^6)^6 = \zeta^6 + \zeta^{36} = \zeta^6 + \zeta = a$
- $\sigma_1(b) = b$
- $\sigma_2(b) = \zeta^2 + (\zeta^2)^2 + (\zeta^2)^4 = \zeta^2 + \zeta^4 + \zeta^8 = \zeta^2 + \zeta^4 + \zeta = b$
- $\sigma_4(b) = \zeta^4 + (\zeta^4)^2 + (\zeta^4)^4 = \zeta^4 + \zeta^8 + \zeta^{16} = \zeta^4 + \zeta + \zeta^2 = b$

Wir halten die bisherigen Ergebnisse in dem Körperturm fest:



Es gilt außerdem $a, b \notin \mathbb{Q}$, denn angenommen dies wäre der Fall, könnten wir $q, q' \in \mathbb{Q}$ finden mit $\zeta + \zeta^6 = q$ und $\zeta + \zeta^2 + \zeta^4 = q'$ und sehen damit ζ als Nullstelle von $X^6 + X - q$ und $X^4 + X^2 + X - q'$. Das ist ein Widerspruch dazu, dass $\Phi_7(X)$ das Minimalpolynom von ζ über $\mathbb{Q}$ ist.
Daraus ergibt sich $\mathbb{Q}(\zeta)^U = \mathbb{Q}(a)$, bzw. $\mathbb{Q}(\zeta)^V = \mathbb{Q}(b)$ und weiter $[\mathbb{Q}(a) : \mathbb{Q}] = 2$, bzw. $[\mathbb{Q}(b) : \mathbb{Q}] = 3$. Die gesuchten Galoisgruppen sind also zyklisch da von Primzahlordnung und wir bekommen letztendlich $\mathrm{Gal}(\mathbb{Q}(a)|\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z}$, bzw. $\mathrm{Gal}(\mathbb{Q}(b)|\mathbb{Q}) \cong \mathbb{Z}/3\mathbb{Z}$.
Zu c). Nach Teilaufgabe b) genügt es, Polynome mit dem entsprechenden Grad zu finden. Unter Beachtung von

- $a = \zeta^6 + \zeta$
- $a^2 = \zeta^5 + \zeta^2 + 2$
- $a^3 = 3\zeta^6 + \zeta^4 + \zeta^3 + 3\zeta$
- $b = \zeta^4 + \zeta^2 + \zeta$
- $b^2 = 2\zeta^6 + 2\zeta^5 + \zeta^4 + 2\zeta^3 + \zeta^2 + \zeta$

sieht man leicht, dass $f = X^3 + X^2 - 2X - 1$, bzw. $g = X^2 + X + 2$ Polynome sind in $\mathbb{Q}[X]$ mit Nullstelle a, bzw. b und es gilt $[\mathbb{Q}(a) : \mathbb{Q}] = \deg(f)$, bzw. $[\mathbb{Q}(b) : \mathbb{Q}] = \deg(g)$. Damit sind die beiden Minimalpolynome gefunden.