3 (p-ter Kreisteilungskörper). Es sei $p \in \mathbb{P}$ und

$$\Phi_p = \frac{X^p - 1}{X - 1} = \sum_{i=0}^{p-1} X^i \in \mathbb{Q}[X].$$

(i) Zeigen Sie, dass Φ_p irreduzibel ist. (*Hinweis*: Man betrachte $\Phi_p(X+1)$.)

(ii) Es sei K eine Körpererweiterung von $\mathbb{Q}$ mit $K = \mathbb{Q}(\zeta)$ für ein $\zeta \in K$ und $\Phi_p(\zeta) = 0$. Zeigen Sie, dass K bereits Zerfällungskörper von Φ_p über $\mathbb{Q}$ ist.

(iii) Bestimmen Sie $\mathrm{Gal}_{\mathbb{Q}} K$ und zeigen Sie $\mathrm{Gal}_{\mathbb{Q}} K \cong \mathbb{Z}_p^\times$.

(iv) Im Fall $p = 7$, bestimmen Sie alle Zwischenkörper von $K \supset \mathbb{Q}$. Stellen Sie die Zwischenkörper, sowie die Untergruppen von $\mathrm{Gal}_{\mathbb{Q}} K$, jeweils in einem Diagramm dar.

Beweis: (i) Es ist

$$\Phi_p(X+1) = \frac{(X+1)^p - 1}{X} = \sum_{j=1}^{p} \binom{p}{j} X^{j-1} \in \mathbb{Z}[X] \subset \mathbb{Q}[X].$$

Es gilt $p \mid \binom{p}{j}$ für $j \in [1, p-1]$. (Das haben wir bereits in Blatt 10, Übung 1 gesehen.) Weiters ist $\binom{p}{1} = p$ und $\binom{p}{p} = 1$. Damit ist das Eisenstein'sche Irreduzibilitätskriterium anwendbar, also ist $\Phi_p(X+1)$ irreduzibel in $\mathbb{Z}[X]$. Das Lemma von Gauss impliziert, dass $\Phi_p(X+1)$ auch irreduzibel in $\mathbb{Q}[X]$ ist. Weil $\mathbb{Q}[X] \to \mathbb{Q}[X], f \mapsto f(X+1)$ ein Ringautomorphismus ist, ist auch Φ_p irreduzibel in $\mathbb{Q}[X]$.

(ii) Es ist $\zeta^p = 1$ aber $\zeta \neq 1$, wegen $\Phi_p(1) = p-1 \neq 0$. Somit muss $\mathrm{ord}_{K^\times}(\zeta) = p$ gelten. Für $i, j \in \mathbb{Z}$ ist deshalb genau dann $\zeta^i = \zeta^j$, wenn gilt $i \equiv j \mod p$. Damit sind ζ, ζ^2, ..., ζ^{p-1} paarweise verschieden. Für alle $i \in [1, p-1]$ ist $i + p\mathbb{Z} \in \mathbb{Z}_p^\times$, und deshalb $\mathbb{Z}_p = \{ij \mid j \in \mathbb{Z}_p\}$. Deshalb gilt

$$\Phi_p(\zeta^i) = \sum_{j=0}^{p-1} \zeta^{ij} = \sum_{j=0}^{p-1} \zeta^j = \Phi_p(\zeta) = 0.$$

Damit besitzt Φ_p in K bereits $p-1$ verschieden Nullstellen, zerfällt also in Linearfaktoren. Nach Definition entsteht K aus $\mathbb{Q}$ durch Adjunktion von Nullstellen von Φ_p. Also ist K ein Zerfällungskörper von Φ_p über $\mathbb{Q}$.

(iii) Ist $\sigma \in \mathrm{Gal}_{\mathbb{Q}} K$, so muss $\sigma(\zeta)$ eine Nullstelle von Φ_p sein (Satz 13.3). Umgekehrt gibt es zu jeder Nullstelle ζ' von Φ_p einen $\mathbb{Q}$-Automorphismus σ mit $\sigma(\zeta) = \zeta'$ (Korollar 9.9). Wir haben aber gerade gesehen, dass $\{\zeta, \zeta^2, \ldots, \zeta^{p-1}\}$

die Menge der Nullstellen von Φ_p ist. Für jedes $j \in [1, p-1]$ gibt es also ein $\sigma_j \in \mathrm{Gal}_{\mathbb{Q}} K$ mit $\sigma_j(\zeta) = \zeta^j$, und es ist $\sigma_i \neq \sigma_j$ für $i \neq j$. Wir erhalten

$$\mathrm{Gal}_{\mathbb{Q}} K = \{\sigma_1, \dots, \sigma_{p-1}\}.$$

Wir behaupten nun, dass

$$\mathrm{Gal}_{\mathbb{Q}} K \to \mathbb{Z}_p^\times,\ \sigma_j \to j + p\mathbb{Z}.$$

ein Isomorphismus ist. Aus dem bereits Gezeigten ist klar, dass die behauptete Abbildung eine Bijektion ist. Sind $i,\ j \in [1, p-1]$ und ist $k \in [1, p-1]$ das eindeutig bestimmte Element mit $k \equiv ij \mod p$, so ist $\sigma_j \circ \sigma_i(\zeta) = \sigma_j(\zeta^i) = \sigma_j(\zeta)^i = (\zeta^j)^i = \zeta^{ij} = \zeta^k$, somit also $\sigma_j \circ \sigma_i = \sigma_k$. Deswegen ist die Abbildung auch ein Homomorphismus.

(iv) Es ist $\mathrm{Gal}_{\mathbb{Q}} K \cong \mathbb{Z}_7^\times \cong \mathbb{Z}_6$. [1] Beispielsweise durch Probieren findet man, dass gilt $\mathbb{Z}_7^\times = \langle 3 + 7\mathbb{Z} \rangle$ (Achtung: Multiplikativ! Es ist z.B. $2 + 7\mathbb{Z}$ kein Erzeuger, weil $2^3 \equiv 8 \equiv 1 \mod 7$ und somit ist $\mathrm{ord}_{\mathbb{Z}_7^\times}(2+7\mathbb{Z}) = 3$). Damit ist $\mathrm{Gal}_{\mathbb{Q}} K = \langle \sigma_3 \rangle$. Die Untergruppen einer zyklischen Gruppe der Ordnung n stehen in Bijektion zu den Teilern von n. Neben $\mathrm{Gal}_{\mathbb{Q}} K$ selbst und der trivialen Gruppe, sind also

$$\begin{aligned} \langle \sigma_3^2 \rangle &= \{\mathrm{id}, \sigma_3^2, \sigma_3^4\} = \{\mathrm{id}, \sigma_2, \sigma_4\}, \text{ und} \\ \langle \sigma_3^3 \rangle &= \{\mathrm{id}, \sigma_3^3\} = \{\mathrm{id}, \sigma_6\} \end{aligned}$$

die einzigen Untergruppen von $\mathrm{Gal}_{\mathbb{Q}} K$. Es ist $\sigma_6(\zeta) = \zeta^6 = \zeta^{-1}$, und somit wird $\zeta + \zeta^{-1}$ von $\langle \sigma_3^3 \rangle$ fixiert. Weil $(1, \zeta, \dots, \zeta^6)$ nach Satz 9.7 eine $\mathbb{Q}$-Basis von K bildet, ist $\zeta + \zeta^{-1} = \zeta + \zeta^6 \notin \mathbb{Q}$. Damit erzeugt $\zeta + \zeta^{-1}$ den Fixkörper von $\langle \sigma_3^3 \rangle$.

Es ist

$$\begin{aligned} \sigma_2(\zeta + \zeta^2 + \zeta^4) &= \zeta^2 + (\zeta^2)^2 + (\zeta^2)^4 = \zeta^2 + \zeta^4 + \zeta, \text{ und} \\ \sigma_4(\zeta + \zeta^2 + \zeta^4) &= \zeta^4 + (\zeta^4)^2 + (\zeta^4)^4 = \zeta^4 + \zeta + \zeta^2. \end{aligned}$$

Wieder folgt $\zeta + \zeta^2 + \zeta^4 \notin \mathbb{Q}$, und deshalb erzeugt $\zeta + \zeta^2 + \zeta^4$ den Fixkörper von $\langle \sigma_3^2 \rangle$. [2]

Zusatz: Wir setzen $\alpha = \zeta + \zeta^2 + \zeta^4$. Aus Blatt 8, Übung 4, wissen wir, dass es ein $\beta \in \mathbb{Q}(\alpha)$ gibt mit $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ und $\beta^2 \in \mathbb{Q}$. Wir können noch versuchen $\mathbb{Q}(\alpha)$ in dieser Form darzustellen. Dazu bestimmen wir zuerst das Minimalpolynom von α (wegen $\Phi_p(\zeta) = 0$ ist $-1 = \sum_{j=1}^{p-1} \zeta^j$):

$$\alpha^2 = \zeta^2 + \zeta^3 + \zeta^5 + \zeta^3 + \zeta^4 + \zeta^6 + \zeta^5 + \zeta^6 + \zeta = -1 + (\zeta^3 + \zeta^5 + \zeta^6) = -2 - \alpha,$$

also ist $X^2 + X + 2$ das Minimalpolynom von α über $\mathbb{Q}$. Vervollständigen des Quadrates gibt $X^2 + X + 2 = (X + \frac{1}{2})^2 + \frac{7}{4}$. Mit $\beta = 2\alpha + 1$ erhalten wir also $\mathbb{Q}(\alpha) = \mathbb{Q}(\beta)$ mit $\beta^2 = -7$. Man schreibt auch $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{-7})$. □

[1] Weil jede endliche Untergruppe der multiplikativen Gruppe eines Körpers zyklisch ist.

[2] Für eine allgemeine Strategie um einen Erzeuger des Fixkörpers zu finden, siehe Musterlösung zu Blatt 11, Übung 2.

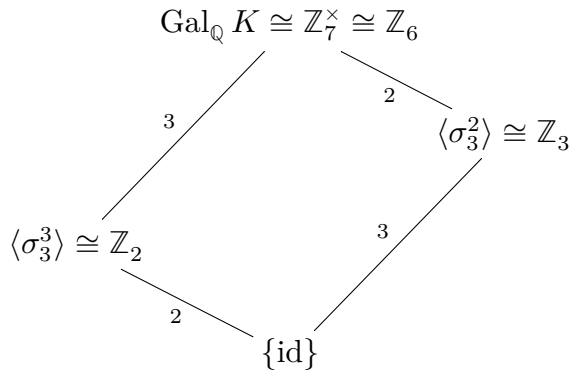

Abbildung 1: Untergruppenverband der zyklischen Gruppe $\mathrm{Gal}_{\mathbb{Q}} \cong \mathbb{Z}_7^\times \cong \mathbb{Z}_6$.

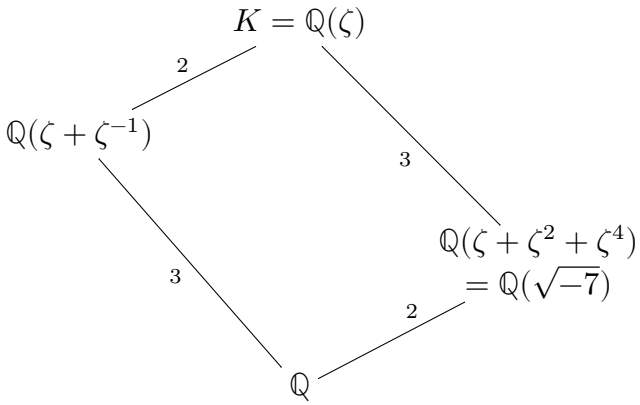

Abbildung 2: Zwischenkörper von $\mathbb{Q} \subset \mathbb{Q}(\zeta)$.