Übungsblatt 12

Aufgabe 1. Seien p eine Primzahl und $n \in \{p, 2p\}$. Zeigen Sie, dass die Galoisgruppe des Polynoms $X^n - 1 \in \mathbb{Q}[X]$ zyklisch ist.

Beweis. Im Beweis zur Aufgabe 2 zeigen wir, dass für alle $n \in \mathbb{N}$ gilt

$$\mathrm{Gal}(X^n - 1) = \mathrm{Gal}(\mathbb{Q}(\zeta)|\,\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^*,$$

wobei ζ eine primitive n–te Einheitswurzel in $\overline{\mathbb{Q}}$ ist. Ist $p = 2$, so gilt für $n = 2 \cdot 2 = 4$

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/4\mathbb{Z})^* = \langle\overline{3}\rangle.$$

Für $n = p = 2$ gilt

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/2\mathbb{Z})^* = \langle\overline{1}\rangle.$$

Sei nun $p > 2$, so erhalten wir für $n = p$, dass $(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z})^*$ eine endliche multiplikative Untergruppe eines Körpers und somit zyklisch ist. Ist $n = 2p$, so gilt nach dem chinesischen Restsatz

$$(\mathbb{Z}/n\mathbb{Z})^* = (\mathbb{Z}/2p\mathbb{Z})^* \cong (\mathbb{Z}/2\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^* \cong (\mathbb{Z}/p\mathbb{Z})^*.$$

Also ist in allen Fällen die Gruppe $(\mathbb{Z}/n\mathbb{Z})^*$ zyklisch. □

Aufgabe 2. Bestimmen Sie die Galoisgruppe des Polynoms $X^{15} - 1 \in \mathbb{Q}[X]$.

Nach Proposition 4.23 ist $X^n - 1 = \prod_{d|n} \Phi_d$, wobei Φ_d das d–te Kreisteilungspolynom ist. Der Zerfällungskörper von $X^n - 1$ ist also $L := \mathbb{Q}(\zeta_{d_1}, \ldots, \zeta_{d_k})$, wobei ζ_{d_i} eine primitive d_i–te Einheitswurzel ist und $1 = d_1 < d_2 < \ldots < d_{k-1} < d_k = n$ die Teiler von n durchläuft. Nun kann man aus ζ_n die anderen vorkommenden primitiven Einheitswurzeln zurückgewinnen. Das Element $\zeta_n^{\frac{n}{d}}$ ist eine d–te Einheitswurzel, denn

$$\left(\zeta_n^{\frac{n}{d}}\right)^d = \zeta_n^n = 1$$

und sie ist primitiv

$$\left|\zeta_n^{\frac{n}{d}}\right| = \frac{|\zeta_n|}{\mathrm{ggT}(\frac{n}{d}, |\zeta_n|)} = \frac{n}{\mathrm{ggT}(n, \frac{n}{d})} = d.$$

Also erhalten wir den Zerfällungskörper $L = \mathbb{Q}(\zeta_{d_1}, \ldots, \zeta_{d_k}) = \mathbb{Q}(\zeta_n)$. Für $n = 15$ liefert das Korollar 4.20 und der chinesische Restsatz

$$\mathrm{Gal}(L|\,\mathbb{Q}) \cong (\mathbb{Z}/15\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/5\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z},$$

wobei $(\mathbb{Z}/5\mathbb{Z})^*$ als endliche multiplikative Untergruppe vom Körper $\mathbb{Z}/5\mathbb{Z}$ zyklisch der Ordnung 4 ist.

Aufgabe 3. Es bezeichne ϕ die Eulersche ϕ–Funktion. Zeigen Sie, dass für $n \in \mathbb{N}$

(1) die Gleichung $\phi(n) = n \prod_{p|n,\, p \text{ prim}} (1 - p^{-1})$ gilt,

(2) die Gleichung $n = \sum_{d \in \mathbb{N},\ d|n} \phi(d)$ gilt,

(3) für $a \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$ die Kongruenz $a^{\phi(n)} \equiv 1 \mod n$ gilt und

(4) es nur endlich viele $m \in \mathbb{N}$ gibt mit $\phi(m) = n$.

Beweis. (1) Sei $n = \prod_{p \in \mathbb{P}} p^{e_p}$ die Primfaktorzerlegung von n, so gilt nach Lemma 4.15

$$\phi(n) = \prod_{p \in \mathbb{P}} \phi(p^{e_p}) = \prod_{p \in \mathbb{P}} p^{e_p}(1 - p^{-1}) = \left(\prod_{p \in \mathbb{P}} p^{e_p}\right) \cdot \left(\prod_{p \in \mathbb{P}} (1 - p^{-1})\right) = n \prod_{p \in \mathbb{P}} (1 - p^{-1}).$$

(2) Es gilt

$$\{1,\dots,n\} = \bigcup_{d|n}^{\cdot} \{k \mid 1 \le k \le n,\ \mathrm{ggT}(k,n) = d\}$$

und für alle $d|n$

$$\phi\left(\frac{n}{d}\right) = |\{k|1 \le k \le n,\ \mathrm{ggT}(k,n) = d\}|\,.$$

Wir erhalten also

$$\begin{aligned} n &= |\,\{1,\dots,n\}\,| \\ &= \left|\bigcup_{d|n}^{\cdot} \{k \mid 1 \le k \le n,\ \mathrm{ggT}(k,n) = d\}\right| \\ &= \sum_{d|n} |\,\{k \mid 1 \le k \le n,\ \mathrm{ggT}(k,n) = d\}\,| \\ &= \sum_{d|n} \phi\left(\frac{n}{d}\right) \\ &= \sum_{d|n} \phi(n)\,. \end{aligned}$$

Alternativ kann man mittels Vorlesung auch wie folgt argumentieren

$$n = \deg(X^n - 1) = \deg\left(\prod_{d|n} \Phi_d\right) = \sum_{d|n} \deg(\Phi_d) = \sum_{d|n} \phi(d).$$

(3) Sei $a \in \mathbb{N}$ mit $\mathrm{ggT}(a,n) = 1$, so gilt $\overline{a} \in (\mathbb{Z}/n\mathbb{Z})^*$. Das Lemma von Lagrange liefert

$$a^{|(\mathbb{Z}/n\mathbb{Z})^*|} = a^{\phi(n)} \equiv 1 \mod n.$$

(4) Sei $p > n+1$, so gilt $p \nmid m$, denn ansonsten gelte nach dem ersten Teil der Aufgabe $n < p-1 \mid \phi(m) = n$, ein Widerspruch. Aus dem Kleinen Fermat folgt

$$p^n - 1 = p^{\phi(m)} - 1 \equiv 0 \mod m.$$

Also ist m ein Teiler von $p^n - 1$ und da es nur endlich viele Teiler von $p^n - 1$ gibt, ist die Behauptung bewiesen.

□

Aufgabe 4. Es sei ζ eine primitive 12–te Einheitswurzel über $\mathbb{Q}$. Bestimmen Sie alle Zwischenkörper der Erweiterung $\mathbb{Q}(\zeta)|\mathbb{Q}$.

Nach Korollar 4.20 und dem chinesischem Restsatz gilt mit $L := \mathbb{Q}(\zeta)$

$$\mathrm{Gal}(L|\mathbb{Q}) \cong (\mathbb{Z}/12\mathbb{Z})^* \cong (\mathbb{Z}/3\mathbb{Z})^* \times (\mathbb{Z}/4\mathbb{Z})^* \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}\,.$$

Die Gruppe $\mathrm{Gal}(L|\mathbb{Q})$ ist also die Kleinsche Vierergruppe und die Untergruppen wurden in Blatt 11 Aufgabe 2 berechnet. Sie lauten

$$\{\mathrm{id}_L\},\ \{\mathrm{id}_L, \sigma\} \text{ für } \sigma \in \mathrm{Gal}(L|\mathbb{Q}) \text{ und } \mathrm{Gal}(L|\mathbb{Q}).$$

Nach Korollar 4.20 werden die Elemente von $\mathrm{Gal}(L|\mathbb{Q})$ durch folgende Zuordnungen induziert

$$\sigma_k : \zeta \mapsto \zeta^k,$$

wobei $k \in \{l \mid 1 \le l \le 12,\ \mathrm{ggT}(l,12) = 1\} = \{1,5,7,11\}$. Die Galoiskorrespondenz liefert also die folgenden Unterkörper

$$L^{\{\mathrm{id}_L\}} = L,\ L^{\{\mathrm{id}_L, \sigma_5\}} = \mathbb{Q}(\zeta^3),\ L^{\{\mathrm{id}_L, \sigma_7\}} = \mathbb{Q}(\zeta^2),\ L^{\{\mathrm{id}_L, \sigma_{11}\}} = \mathbb{Q}(\zeta^3 - 2\zeta) = \mathbb{Q}(\sqrt{3}),\ L^{\mathrm{Gal}(L|\mathbb{Q})} = \mathbb{Q}\,.$$

Wir berechnen im Folgenden exemplarisch $L^{\{\mathrm{id}_L,\sigma_5\}}$ und $L^{\{\mathrm{id}_L,\sigma_{11}\}}$.
Das 12–te Kreisteilungspolynom ist $X^4 - X^2 + 1$ und daraus folgt

$$L = \mathbb{Q}[\zeta] = \{a + b\zeta + c\zeta^2 + d\zeta^3 \mid a, b, c, d \in \mathbb{Q}\}.$$

Sei $x := a + b\zeta + c\zeta^2 + d\zeta^3 \in L$ mit

$$a+b\zeta+c\zeta^2+d\zeta^3 = x = \sigma_5(x) = a+b\zeta^5+c\zeta^{10}+d\zeta^{15} = a+b\zeta^5+c\zeta^{10}+d\zeta^3 = (a+c)-b\zeta-c\zeta^2+(b+d)\zeta^3,$$

wobei $\zeta^5 = \zeta\zeta^4 = \zeta(\zeta^2-1) = \zeta^3-\zeta$ und $\zeta^{10} = -\zeta^2+1$ benutzt wurde. Ein Koeffizientenvergleich liefert $b = c = 0$, also gilt $x = a + d\zeta^3$ und somit $L^{\{\mathrm{id}_L,\sigma_5\}} = \{a + d\zeta^3 \mid a, d \in \mathbb{Q}\} = \mathbb{Q}(\zeta^3)$.
Dasselbe Vorgehen für $L^{\{\mathrm{id}_L,\sigma_{11}\}}$ liefert

$$a+b\zeta+c\zeta^2+d\zeta^3 = x = \sigma_{11}(x) = a+b\zeta^{11}+c\zeta^{22}+d\zeta^{33} = a+b\zeta^{11}+c\zeta^{10}+d\zeta^9 = (a+c)+b\zeta-c\zeta^2-(b+d)\zeta^3.$$

Ein Koeffizientenvergleich liefert $c = 0$, $-2d = b$ und somit erhalten wir $x = a + -d\zeta + d\zeta^3 = a + d(\zeta^3 - 2\zeta)$. Also gilt $L^{\{\mathrm{id}_L,\sigma_{11}\}} = \{a+d(\zeta^3-2\zeta) \mid a, d \in \mathbb{Q}\} = \mathbb{Q}(\zeta^3-2\zeta)$ und wegen $(\zeta^3-2\zeta)^2 = 3\zeta^2(-\zeta^2+1) = 3$ erhalten wir insgesamt $L^{\{\mathrm{id}_L,\sigma_{11}\}} = \mathbb{Q}(\sqrt{3})$.