

Musterlösung Serie 27

KREISTEILUNGSKÖRPER, ABELSCHER KÖRPERERWEITERUNGEN

1. Sei $\underline{X} := (X_1, X_2, X_3, X_4)$ ein Satz unabhängiger Variablen über einem Körper K , und sei $\underline{S} := (S_1, S_2, S_3, S_4)$ das Tupel der zugehörigen elementarsymmetrischen Polynome.

- (a) Bestimme ein primitives Element der Erweiterung $K(\underline{X})/K(\underline{S})$.
 (b) Sei $\Delta := \langle (1\ 2)(3\ 4), (1\ 3)(2\ 4) \rangle \triangleleft S_4$ die Kleinsche Vierergruppe. Bestimme $K(\underline{X})^\Delta$ durch explizite Erzeugende über $K(\underline{S})$.

Lösung: (a) Das Element $X_1^3 X_2^2 X_3$ hat trivialen Stabilisator in S_4 , ist also für kein $1 \subsetneq \Gamma \leq S_4$ in $K(\underline{X})^\Gamma$ enthalten. Das bedeutet, dass $\text{Gal}(K(\underline{X})/K(\underline{S}))(X_1^3 X_2^2 X_3)$ trivial ist, und mit dem Hauptsatz der Galoistheorie folgt $K(\underline{S})(X_1^3 X_2^2 X_3) = K(\underline{X})$.

(b) Sei T eine weitere unabhängige Variable. Nach Satz 7.5.3 der Vorlesung wird $K(\underline{X})^\Delta$ über $K(\underline{S})$ dann durch die Koeffizienten des Polynoms

$$\begin{aligned} \prod_{\delta \in \Delta} (T - \delta(X_1^3 X_2^2 X_3)) &= (T - X_1^3 X_2^2 X_3)(T - X_2^3 X_1^2 X_4)(T - X_3^3 X_4^2 X_1)(T - X_4^3 X_3^2 X_2) \\ &= T^4 - (X_1^3 X_2^2 X_3 + X_2^3 X_1^2 X_4 + X_3^3 X_4^2 X_1 + X_4^3 X_3^2 X_2)T^3 \\ &\quad + (X_1^3 X_2^2 X_3 X_2^3 X_1^2 X_4 + X_1^3 X_2^2 X_3 X_3^3 X_4^2 X_1 + X_1^3 X_2^2 X_3 X_4^3 X_3^2 X_2 \\ &\quad + X_2^3 X_1^2 X_4 X_3^3 X_4^2 X_1 + X_2^3 X_1^2 X_4 X_4^3 X_3^2 X_2 + X_3^3 X_4^2 X_1 X_4^3 X_3^2 X_2)T^2 \\ &\quad - (X_2^3 X_1^2 X_4 X_3^3 X_4^2 X_1 X_4^3 X_3^2 X_2 + X_1^3 X_2^2 X_3 X_3^3 X_4^2 X_1 X_4^3 X_3^2 X_2 \\ &\quad + X_1^3 X_2^2 X_3 X_2^3 X_1^2 X_4 X_4^3 X_3^2 X_2 + X_1^3 X_2^2 X_3 X_2^3 X_1^2 X_4 X_3^3 X_4^2 X_1)T \\ &\quad + X_1^3 X_2^2 X_3 X_2^3 X_1^2 X_4 X_3^3 X_4^2 X_1 X_4^3 X_3^2 X_2 \\ &= T^4 - (X_1^3 X_2^2 X_3 + X_1^2 X_2^3 X_4 + X_1 X_3^3 X_4^2 + X_2 X_3^2 X_4^3)T^3 \\ &\quad + X_1 X_2 X_3 X_4 (X_1^4 X_2^4 + X_1^3 X_2 X_3^3 X_4 + 2X_1^2 X_2^2 X_3^2 X_4^2 + X_1 X_2^3 X_3 X_4^3 + X_3^4 X_4^4)T^2 \\ &\quad - (X_1 X_2 X_3 X_4)^3 (X_2 X_3^2 X_4^3 + X_1 X_3^3 X_4^2 + X_1^2 X_2^3 X_4 + X_1^3 X_2^2 X_3)T \\ &\quad + X_1^6 X_2^6 X_3^6 X_4^6 \end{aligned}$$

erzeugt. Durch Ignorieren von Termen in $K(\underline{S})$ erhalten wir die beiden Erzeuger

$$\begin{aligned} X_1^3 X_2^2 X_3 + X_1^2 X_2^3 X_4 + X_1 X_3^3 X_4^2 + X_2 X_3^2 X_4^3, \\ X_1^4 X_2^4 + X_1^3 X_2 X_3^3 X_4 + X_1 X_2^3 X_3 X_4^3 + X_3^4 X_4^4. \end{aligned}$$

Aliter: Wir probieren es mit der Summe aller Δ -Konjugierten des primitiven Elements aus (a), also mit

$$\sum_{\delta \in \Delta} \delta(X_1^3 X_2^2 X_3) = X_1^3 X_2^2 X_3 + X_1^2 X_2^3 X_4 + X_1 X_3^3 X_4^2 + X_2 X_3^2 X_4^3.$$

Wir rechnen explizit nach, dass sein Stabilisator in S_4 schon gleich Δ ist. Also liegt es in keinem kleineren Zwischenkörper, und es ist schon alleine ein Erzeugendes von $K(\underline{X})^\Delta$ über $K(\underline{S})$.

Aliter: Wir suchen Δ -invariante homogene Polynome von möglichst kleinem Grad. Alle solche vom Grad 0 oder 1 sind schon S_4 -invariant, interessieren uns also nicht. In Grad 2 finden wir aber die Δ -invarianten Polynome $X_1X_2 + X_3X_4$ und $X_1X_3 + X_2X_4$ und $X_1X_4 + X_2X_3$. Der Stabilisator von $X_1X_2 + X_3X_4$ in S_4 ist $\langle \Delta \cup \{(1\ 2), (3\ 4)\} \rangle$ (isomorph zu D_4), der Stabilisator von $X_1X_3 + X_2X_4$ ist $\langle \Delta \cup \{(1\ 3), (2\ 4)\} \rangle$. Der Schnitt dieser beiden Stabilisatoren ist genau Δ , deshalb sind die Polynome $X_1X_2 + X_3X_4$ und $X_1X_3 + X_2X_4$ Erzeuger von $K(\underline{X})^\Delta$ über $K(\underline{S})$ (und $X_1X_4 + X_2X_3$ ist als Bonus mit dabei).

2. Sei $n \geq 3$ und $\zeta \in \mathbb{C}$ eine primitive n -te Einheitswurzel. Zeige:

$$\mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\zeta + \zeta^{-1})$$

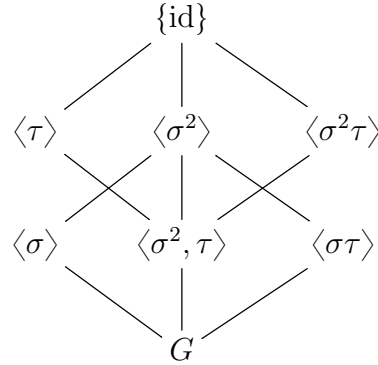
und bestimme den Grad $[\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})]$.

Lösung: Sei $K := \mathbb{Q}(\zeta) \cap \mathbb{R}$. Da ζ^{-1} zu ζ komplex konjugiert ist, gilt $\zeta + \zeta^{-1} \in \mathbb{R}$, also ist $\mathbb{Q}(\zeta + \zeta^{-1}) \subset K$. Wegen $\zeta \notin \mathbb{R}$ ist weiter $K \subsetneq \mathbb{Q}(\zeta)$, also folgt $[\mathbb{Q}(\zeta)/K] \geq 2$. Andererseits ist ζ eine Nullstelle des quadratischen Polynoms $X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X]$, folglich gilt $[\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})] = 2$ und somit ist $\mathbb{Q}(\zeta + \zeta^{-1}) = K$.

3. Sei $\zeta \in \mathbb{C}$ eine primitive 15-te Einheitswurzel. Erstelle eine Liste aller Zwischenkörper der Erweiterung $\mathbb{Q}(\zeta)/\mathbb{Q}$ mitsamt Inklusionen.

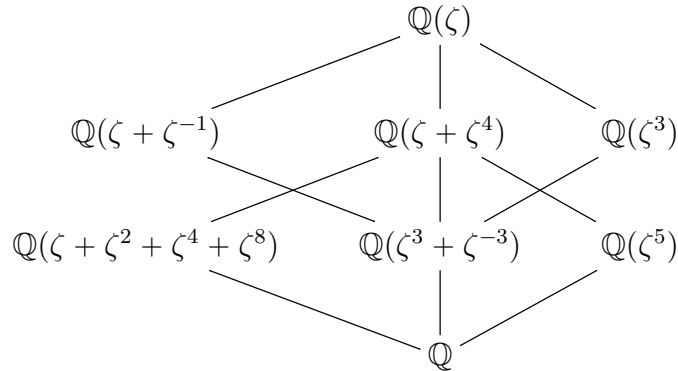
Lösung: Aus der Irreduzibilität des Kreisteilungspolynoms Φ_{15} folgt, dass $G := \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = (\mathbb{Z}/15\mathbb{Z})^\times$ ist. Wegen des chinesischen Restsatzes gilt $\mathbb{Z}/15\mathbb{Z} \cong \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{F}_5^\times \times \mathbb{F}_3^\times$ und somit $(\mathbb{Z}/15\mathbb{Z})^\times \cong \mathbb{F}_5^\times \times \mathbb{F}_3^\times$. Hier ist \mathbb{F}_5^\times zyklisch der Ordnung $5 - 1 = 4$, und \mathbb{F}_3^\times ist zyklisch der Ordnung $3 - 1 = 2$. Konkret hat zum Beispiel die Restklasse von 2 die verschiedenen Potenzen $2, 4, 8, 16 \cong 1 \pmod{15}$, entspricht also einem Element $\sigma \in G$ der Ordnung 4. Die Restklasse von -1 liegt nicht in der von 2 mod 5 erzeugten Untergruppe von $(\mathbb{Z}/15\mathbb{Z})^\times$ und entspricht einem Element $\tau \in G$ der Ordnung 2. Somit ist $G = \langle \sigma \rangle \times \langle \tau \rangle$ und es gilt $\sigma(\zeta) = \zeta^2$ und $\tau(\zeta) = \zeta^{-1}$.

Wir machen nun eine Aufstellung aller Untergruppen von G mit allen Inklusionen (die Vollständigkeitskontrolle überlassen wir dem Leser):



Die entsprechenden Zwischenerweiterungen sind:

- $\mathbb{Q}(\zeta)^{\{\text{id}\}} = \mathbb{Q}(\zeta)$.
- $\mathbb{Q}(\zeta)^G = \mathbb{Q}$.
- Es ist $\tau(\zeta + \zeta^{-1}) = \zeta^{-1} + \zeta$, also $\zeta + \zeta^{-1} \in \mathbb{Q}(\zeta)^{\langle \tau \rangle}$. Zudem ist ζ eine Nullstelle des Polynoms $X^2 - (\zeta + \zeta^{-1})X + 1 \in \mathbb{Q}(\zeta + \zeta^{-1})[X]$, also ist $[\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta + \zeta^{-1})] \leq 2$ und somit $\mathbb{Q}(\zeta)^{\langle \tau \rangle} = \mathbb{Q}(\zeta + \zeta^{-1})$.
- Es ist $\sigma^2(\zeta + \zeta^4) = \zeta^4 + \zeta$, also $\zeta + \zeta^4 \in \mathbb{Q}(\zeta)^{\langle \sigma^2 \rangle}$. Zudem hat $\zeta + \zeta^4$ unter G genau die weiteren Konjugierten $\zeta^2 + \zeta^8$, $\zeta^{-1} + \zeta^{-4}$ und $\zeta^{-2} + \zeta^{-8}$, also ist $|\text{Hom}(\mathbb{Q}(\zeta + \zeta^4), \overline{\mathbb{Q}})| = [\mathbb{Q}(\zeta + \zeta^4)/\mathbb{Q}] = 4$ und somit $\mathbb{Q}(\zeta)^{\langle \sigma^2 \rangle} = \mathbb{Q}(\zeta + \zeta^4)$.
- Es ist $(\sigma^2 \tau)(\zeta^3) = (\zeta^3)^{-4} = \zeta^3$, also $\zeta^3 \in \mathbb{Q}(\zeta)^{\langle \sigma^2 \tau \rangle}$. Zudem ist ζ^3 eine primitive 5-te Einheitswurzel, also ist $[\mathbb{Q}(\zeta^3)/\mathbb{Q}] = 4$ und $\mathbb{Q}(\zeta)^{\langle \sigma^2 \tau \rangle} = \mathbb{Q}(\zeta^3)$.
- Es ist $\sigma(\zeta + \zeta^2 + \zeta^4 + \zeta^8) = \zeta^2 + \zeta^4 + \zeta^8 + \zeta$, also $\zeta + \zeta^2 + \zeta^4 + \zeta^8 \in \mathbb{Q}(\zeta)^{\langle \sigma \rangle}$. Zudem ist $\zeta + \zeta^2 + \zeta^4 + \zeta^8 \notin \mathbb{Q}$, also $[\mathbb{Q}(\zeta + \zeta^2 + \zeta^4 + \zeta^8)/\mathbb{Q}] \geq 2$ und somit $\mathbb{Q}(\zeta)^{\langle \sigma \rangle} = \mathbb{Q}(\zeta + \zeta^2 + \zeta^4 + \zeta^8)$.
- Es ist $\tau(\zeta^3 + \zeta^{-3}) = \zeta^{-3} + \zeta^3$ und $\sigma^2(\zeta^3 + \zeta^{-3}) = (\zeta^3)^4 + (\zeta^{-3})^4 = \zeta^{-3} + \zeta^3$, also $\mathbb{Q}(\zeta^3 + \zeta^{-3}) \subset \mathbb{Q}(\zeta)^{\langle \sigma^2, \tau \rangle}$. Zudem ist $\zeta^3 + \zeta^{-3} \notin \mathbb{Q}$, also $[\mathbb{Q}(\zeta^3 + \zeta^{-3})/\mathbb{Q}] \geq 2$ und somit $\mathbb{Q}(\zeta)^{\langle \sigma^2, \tau \rangle} = \mathbb{Q}(\zeta^3 + \zeta^{-3})$.
- Es ist $(\sigma \tau)(\zeta^5) = (\zeta^5)^{-2} = \zeta^5$, also ist $\zeta^5 \in \mathbb{Q}(\zeta)^{\langle \sigma \tau \rangle}$. Zudem ist ζ^5 eine primitive dritte Einheitswurzel, also ist $[\mathbb{Q}(\zeta^5)/\mathbb{Q}] = 2$ und $\mathbb{Q}(\zeta)^{\langle \sigma \tau \rangle} = \mathbb{Q}(\zeta^5)$.



4. Konstruiere ein irreduzibles Polynom $f \in \mathbb{Q}[X]$ vom Grad 5 mit Galoisgruppe $\cong \mathbb{Z}/5\mathbb{Z}$. Beschreibe die komplexen Nullstellen von f durch Radikale.

Lösung: Nach dem Satz von Kronecker-Weber wird der Zerfällungskörper von f ein Unterkörper eines Kreisteilungskörpers sein. Wir suchen also einen solchen vom Grad 5 über \mathbb{Q} . Die kleinstmögliche Zahl $n \geq 1$, so dass der Grad $[\mathbb{Q}(\mu_n)/\mathbb{Q}] = |(\mathbb{Z}/n\mathbb{Z})^\times|$ ein Vielfaches von 5 ist, ist $n = 11$. Dann ist $\text{Gal}(\mathbb{Q}(\mu_{11})/\mathbb{Q}) \cong (\mathbb{Z}/11\mathbb{Z})^\times$ zyklisch der Ordnung 10. Deren Untergruppe $\{\pm 1\}$ ist normal der Ordnung 2; ihre Faktorgruppe ist also zyklisch der Ordnung 5. Nach dem Hauptsatz der Galois-theorie Teil (e) ist der zugehörige Zwischenkörper folglich zyklisch vom Grad 5 über \mathbb{Q} .

Um diesen explizit zu beschreiben, wähle eine primitive elfte Einheitswurzel $\zeta \in \mu_{11}$. Dann ist $\zeta + \zeta^{-1}$ invariant unter $\{\pm 1\}$, liegt also in dem gesuchten Zwischenkörper. Wegen $\zeta^2 - (\zeta + \zeta^{-1})\zeta + 1 = 0$ ist andererseits $[\mathbb{Q}(\mu_{11})/\mathbb{Q}(\zeta + \zeta^{-1})] \leq 2$. Wie in der obigen Aufgabe 2 folgt daraus, dass der gesuchte Zwischenkörper gleich $\mathbb{Q}(\zeta + \zeta^{-1})$ ist.

Um das Minimalpolynom von $\zeta + \zeta^{-1}$ zu bestimmen, potenzieren wir und rechnen:

$$\begin{aligned} (\zeta + \zeta^{-1})^5 &= \zeta^5 + 5\zeta^3 + 10\zeta + 10\zeta^{-1} + 5\zeta^{-3} + \zeta^{-5} \\ (\zeta + \zeta^{-1})^4 &= \zeta^4 + 4\zeta^2 + 6 + 4\zeta^{-2} + \zeta^{-4} \\ (\zeta + \zeta^{-1})^5 + (\zeta + \zeta^{-1})^4 &= 4\zeta^3 + 3\zeta^2 + 9\zeta + 5 + 9\zeta^{-1} + 3\zeta^{-2} + 4\zeta^{-3} \\ (\zeta + \zeta^{-1})^3 &= \zeta^3 + 3\zeta + 3\zeta^{-1} + \zeta^{-3} \\ (\zeta + \zeta^{-1})^2 &= \zeta^2 + 2 + \zeta^{-1} \\ (\zeta + \zeta^{-1})^5 + (\zeta + \zeta^{-1})^4 - 4(\zeta + \zeta^{-1})^3 - 3(\zeta + \zeta^{-1})^2 &= -3\zeta - 1 - 3\zeta^{-1}. \end{aligned}$$

Also ist $\zeta + \zeta^{-1}$ eine Nullstelle des normierten Polynoms

$$f(X) := X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1 \in \mathbb{Z}[X].$$

Wegen $[\mathbb{Q}(\zeta + \zeta^{-1})/\mathbb{Q}] = 5 = \deg(f)$ muss dies schon das Minimalpolynom von $\zeta + \zeta^{-1}$ über \mathbb{Q} sein. Seine Nullstellen sind genau die Galois-konjugierten von $\zeta + \zeta^{-1}$,

also die Zahlen $\zeta^k + \zeta^{-k}$ für $k = 1, \dots, 5$. Da $\zeta^{\pm k}$ bereits eine 11-te Wurzel aus 1 ist, ist dies eine Darstellung durch Radikale, wie gewünscht.

5. (*Artin-Schreier Theorie*) Sei K ein Körper der Charakteristik $p > 0$. Sei L/K galoissch mit $\Gamma := \text{Gal}(L/K) = \langle \gamma \rangle$ zyklisch der Ordnung p .

(a) Bestimme die Jordansche Normalform von γ betrachtet als Endomorphismus des K -Vektorraumes L .

(b) Zeige: Es existiert ein $a \in L$ mit $\gamma(a) = a + 1$.

(c) Zeige: Es existiert ein $a \in L$ mit $L = K(a)$ und $a^p - a \in K$.

Vergleiche Serie 22 Aufgabe 3.

Lösung: (a) Wegen $\gamma^p = \text{id}_L$ ist das Minimalpolynom von γ ein Teiler von $X^p - 1 = (X - 1)^p \in K[X]$. Der einzige Eigenwert von γ ist also 1 und damit ist γ trigonalisierbar über K . Weiter ist die Anzahl Jordan-Blöcke der Matrix gleich der geometrischen Vielfachheit von 1. Wegen

$$\{a \in L \mid \gamma(a) = a\} = L^{\langle \gamma \rangle} = K$$

hat der Eigenraum zum Eigenwert 1 die K -Dimension 1. Also ist die geometrische Vielfachheit gleich 1, und die Jordansche Normalform von γ ist

$$\begin{pmatrix} 1 & 1 & & 0 \\ & \ddots & \ddots & \\ & & 1 & 1 \\ 0 & & & 1 \end{pmatrix}.$$

(b) Sei $\{v_1, \dots, v_n\}$ die K -Basis von L , die der Jordanschen Normalform von γ entspricht. Dann gilt $\gamma(v_1) = v_1$ und $\gamma(v_2) = v_1 + v_2$. Für $a := \frac{v_2}{v_1}$ gilt dann

$$\gamma(a) = \frac{\gamma(v_2)}{\gamma(v_1)} = \frac{v_1 + v_2}{v_1} = a + 1.$$

(c) Das Element a aus (b) liegt nicht in K , da $\gamma(a) \neq a$ gilt. Es erzeugt also einen Zwischenkörper $K \subsetneq K(a) \subset L$. Da $[L/K] = p$ prim ist, folgt aus der Multiplikativität des Körpergrades, dass $K(a) = L$ gilt. Weiter ist

$$\gamma(a^p - a) = \gamma(a)^p - \gamma(a) = (a + 1)^p - (a + 1) = a^p - a$$

und somit $a^p - a \in K$.

*6. Sei L/K eine endliche Körpererweiterung vom Grad m . Für jedes $\alpha \in L$ ist die Norm $N_{L/K}(\alpha)$ definiert als Determinante der K -linearen Abbildung $\mu_\alpha: L \rightarrow L$, $x \mapsto \alpha x$. Zeige:

- (a) Ist $X^n + \sum_{k=0}^{n-1} a_k X^k$ das Minimalpolynom von $\alpha \in L$ über K , so gilt $N_{L/K}(\alpha) = (-1)^m a_0^{m/n}$.
- (b) Die Norm induziert einen Homomorphismus $L^\times \rightarrow K^\times$, $\alpha \mapsto N_{L/K}(\alpha)$.
- (c) Ist L/K separabel und $\text{Hom}_K(L, \overline{K}) = \{\sigma_1, \dots, \sigma_m\}$ für einen algebraischen Abschluss \overline{K} von K , so gilt $N_{L/K}(\alpha) = \sigma_1(\alpha) \cdots \sigma_m(\alpha)$.
- (d) (*Hilberts Satz 90*) Ist L/K galoissch und $\text{Gal}(L/K)$ zyklisch mit Erzeugendem σ und ist $\alpha \in L^\times$ mit $N_{L/K}(\alpha) = 1$, so ist $\alpha = \sigma(\beta)/\beta$ für ein $\beta \in L^\times$.

Lösung: (a) Da α den Grad n über K hat, ist $(1, \alpha, \dots, \alpha^{n-1})$ eine Basis von $K(\alpha)$ über K . Sei ausserdem $(\beta_1, \dots, \beta_{m/n})$ eine Basis von L über $K(\alpha)$. Wie im Beweis der Multiplikativität des Körpergrads ist dann

$$(\beta_1, \alpha\beta_1, \dots, \alpha^{n-1}\beta_1, \beta_2, \dots, \alpha^{n-1}\beta_{m/n})$$

eine Basis von L über K . Bezüglich dieser hat die Darstellungsmatrix von μ_α die Blockform

$$\begin{pmatrix} B & 0 & \cdots & 0 \\ 0 & \alpha B & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & B \end{pmatrix} \quad \text{für} \quad B := \begin{pmatrix} 0 & \cdots & 0 & -a_0 \\ 1 & \cdots & 0 & -a_1 \\ 0 & \cdots & 0 & \vdots \\ \vdots & \ddots & 0 & -a_{n-2} \\ 0 & \cdots & 0 & 1 - a_{n-1} \end{pmatrix} \in M_{n \times n}(K).$$

Aus $\det(B) = (-1)^n a_0$ folgt somit $N_{L/K}(\alpha) = \det(B)^{m/n} = (-1)^m a_0^{m/n}$.

(b) Zunächst stellen wir fest, dass für jedes $\alpha \in L^\times$ die lineare Abbildung μ_α bijektiv ist; also ist in der Tat $N_{L/K}(\alpha) \in K^\times$. Für je zwei Elemente $\alpha, \beta \in L^\times$ gilt weiter $\mu_{\alpha\beta} = \mu_\alpha \circ \mu_\beta$. Aus der Multiplikativität der Determinante folgt also $N_{L/K}(\alpha\beta) = N_{L/K}(\alpha) \cdot N_{L/K}(\beta)$.

(c) Die Bilder von α unter den Einbettungen $\sigma_1, \dots, \sigma_m$ sind gerade die verschiedenen Nullstellen $\alpha_1, \dots, \alpha_n$ des Minimalpolynoms von α . Sei $\text{Hom}_K(K(\alpha), \overline{L}) = \{\tau_1, \dots, \tau_n\}$. Jedes τ_i hat genau $[L/K(\alpha)] = m/n$ Fortsetzungen auf L . Das impliziert für jedes $1 \leq j \leq n$, dass $|\{1 \leq i \leq m : \sigma_i(\alpha) = \alpha_j\}| = m/n$ ist. Nach dem Satz von Vieta ist $\alpha_1 \cdots \alpha_n = (-1)^n a_0$, und somit ist $\sigma_1(\alpha) \cdots \sigma_m(\alpha) = (\alpha_1 \cdots \alpha_n)^{m/n} = ((-1)^n a_0)^{m/n} = (-1)^m a_0^{m/n} = N_{L/K}(\alpha)$.

(d) Die gesuchte Bedingung an β ist äquivalent zu $\sigma(\beta) = \alpha\beta$. Wir finden ein solches β durch Ansatz. Nach der Vorlesung sind $\text{id}, \sigma, \dots, \sigma^{m-1}$ als Elemente des L -Vektorraums aller Abbildungen $L \rightarrow L$ linear unabhängig. Folglich ist ihre L -Linearkombination

$$\varphi := \text{id} + \alpha^{-1} \cdot \sigma + \alpha^{-1}\sigma(\alpha^{-1}) \cdot \sigma^2 + \dots + \alpha^{-1}\sigma(\alpha^{-1}) \dots \sigma^{m-2}(\alpha^{-1}) \cdot \sigma^{m-1}$$

ungleich null. Wähle ein beliebiges $\gamma \in L$ mit $\beta := \varphi(\gamma) \neq 0$. Nach Voraussetzung und (c) gilt

$$N_{L/K}(\alpha) = \alpha \cdot \sigma(\alpha) \dots \sigma^{m-1}(\alpha) = 1.$$

Mittels einer direkten Rechnung impliziert dies $\alpha^{-1}\sigma(\beta) = \beta$. Für dieses ist dann $\alpha = \frac{\sigma(\beta)}{\beta}$, wie gewünscht.

*7. (*Irreduzibilität des Kreisteilungspolynoms*) Für jede ganze Zahl $n \geq 1$ ist das n -te Kreisteilungspolynom definiert durch $\Phi_n(X) := \prod (X - \zeta)$, wobei ζ alle Einheitswurzeln in \mathbb{C} der genauen Ordnung n durchläuft. Zeige:

(a) Für jedes $n \geq 1$ gilt

$$X^n - 1 = \prod_{m|n} \Phi_m(X).$$

(b) Jedes Φ_n ist ein normiertes Polynom in $\mathbb{Z}[X]$.

Sei nun $f \in \mathbb{Z}[X]$ ein normierter irreduzibler Faktor von Φ_n mit Nullstelle $\xi \in \mathbb{C}$.

(c) Zeige: Für jede nichtnegative ganze Zahl k existiert ein eindeutiges Polynom $g_k \in \mathbb{Z}[X]$ mit $\deg(g_k) < \deg(f)$ und $f(\xi^k) = g_k(\xi)$. Zeige ausserdem, dass die Menge $\{g_k : k \in \mathbb{Z}_{\geq 0}\}$ endlich ist.

(d) Sei $a := \sup\{|u| : u \text{ ist Koeffizient eines } g_k\}$. Zeige: Ist $k = p$ prim, so teilt p alle Koeffizienten von g_p . Schliesse daraus, dass für alle $p > a$ das Polynom g_p gleich Null ist. [*Hinweis: $f(\xi^p) = f(\xi^p) - f(\xi)^p$*]

(e) Folgere: Wenn alle Primfaktoren einer ganzen Zahl m grösser als a sind, dann gilt $f(\xi^m) = 0$.

(f) Zeige: Für jede zu n teilerfremde ganze Zahl r gilt $f(\xi^r) = 0$. [*Hinweis: Betrachte $m := r + n \prod_{p \leq a, p|r} p$.*]

(g) Zeige, dass das n -te Kreisteilungspolynom Φ_n irreduzibel ist.

Lösung: (a) Es ist $X^n - 1 = \prod (X - \zeta)$, wobei ζ alle komplexen Zahlen mit $\zeta^n = 1$ durchläuft. Jede solche ist eine Einheitswurzel der Ordnung m für genau einen Teiler $m|n$. Daraus folgt die gesuchte Gleichung.

(b) Nach Konstruktion ist jedes Φ_n ein normiertes Polynom in $\mathbb{C}[X]$; ausserdem liegt $\Phi_1(X) = X - 1$ in $\mathbb{Z}[X]$. Die allgemeine Aussage folgt aus (a) durch Induktion über n .

(c) Since f is monic and irreducible, it is the minimal polynomial of ξ over \mathbb{Q} . Consequently $\mathbb{Q}(\xi) \cong \mathbb{Q}[X]/(f(X))$ is an algebraic extension of \mathbb{Q} of degree $\deg(f)$ with the basis $1, \xi, \dots, \xi^{\deg(f)-1}$ over \mathbb{Q} . Thus $f(\xi^k) \in \mathbb{Q}(\xi)$ can be expressed in at most one way as $f(\xi^k) = g_k(\xi)$ with $g_k \in \mathbb{Z}[X]$ of degree $< \deg(f)$, and we only have to check existence. Let g_k be the remainder of $f(X^k)$ divided by the monic polynomial f ; then g_k satisfies the desired properties.

Since the set $\{\xi^k : k \in \mathbb{Z}_{\geq 0}\}$ is finite, by uniqueness, so is the set of the g_k 's.

(d) Since exponentiation by p is a ring homomorphism modulo p (the Frobenius of degree p), we have $f(X^p) \equiv f(X)^p$ modulo $p\mathbb{Z}[X]$. In other words there exists a polynomial $h(X) \in \mathbb{Z}[X]$ with $f(X^p) = f(X)^p + ph(X)$. By the same argument as in (a) there exists a unique polynomial $k \in \mathbb{Z}[X]$ of degree less than $\deg(f)$ with $h(\xi) = k(\xi)$. Since $f(\xi) = 0$, it follows that

$$g_k(\xi) = f(\xi^p) = ph(\xi) = pk(\xi).$$

By the uniqueness of g_p we conclude that $g_p = pk \in p\mathbb{Z}[X]$.

If $p > a$, all coefficients of g_p have absolute value less than p and are divisible by p ; hence they are zero; thus $g_p = 0$.

(e) For every prime $p > a$ we have $f(\xi^p) = g_p(\xi) = 0$ by (b). Thus ξ^p is another root of f . As f is irreducible, we therefore have $\xi^p = \gamma(\xi)$ for some $\gamma \in \text{Gal}(\mathbb{Q}(\mu_n)/\mathbb{Q})$. For every k it follows that

$$f(\xi^{pk}) = f(\gamma(\xi)^k) = \gamma(f(\xi^k)) = \gamma(g_k(\xi)) = g_k(\gamma(\xi)) = g_k(\xi^k).$$

Thus the assertions of (a) and (b) are equally true for ξ^p in place of ξ with the same polynomials g_k .

Now we can prove (e) in general by induction on the number of prime factors of m . If this number is ≤ 1 , we are already done. Otherwise write $m = pm'$ with a prime p . Then by the above we have $f(\xi^p) = 0$, and applying the induction hypothesis with (m', ξ^p) in place of (m, ξ) we deduce that $f(\xi^{pm'}) = 0$, as desired.

(f) Set $m := r + n\ell$ with $\ell := \prod_{p \leq a, p \nmid r} p$. Then any prime $p \leq a$ not dividing r divides ℓ ; hence it does not divide m . Any prime $p \leq a$ dividing r does not divide n by assumption; so it also does not divide $n\ell$; hence it does not divide m . Together this shows that all prime divisors of m are greater than a . Since $\xi^n = 1$, from (c) we therefore deduce that $f(\xi^r) = f(\xi^m) = 0$.

(g) By assumption ξ is a root of unity of precise order n . Thus the numbers ξ^r for $r \in (\mathbb{Z}/n\mathbb{Z})^\times$ are the distinct roots of unity of precise order n , that is, exactly all roots of Φ_n . By (f) they are all zeros of f ; hence $f = \Phi_n$. Thus Φ_n is irreducible.