Fachbereich Mathematik
Prof. Dr. Nils Scheithauer
Walter Reußwig

TECHNISCHE UNIVERSITÄT DARMSTADT

WS 08/09 3. Februar 2009

Algebra

14. Übung mit Lösungshinweisen

Aufgabe 63 Sei $\mathbb{L}/\mathbb{K}$ galoissch mit Galoisgruppe $G = \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ und $|G| = p$ für p prim. Zeige, daß für ein Element $\alpha \in \mathbb{L}$ folgende Aussagen äquivalent sind:

(1) Es ist $\alpha \in \mathbb{K}$.

(2) Es ist $\alpha \in \mathbb{L}^G$.

(3) Es gibt ein $\mathrm{id} \neq \sigma \in G$ mit $\sigma(\alpha) = \alpha$.

Lösung: (1) $\Leftrightarrow$ (2) Da $\mathbb{L}/\mathbb{K}$ galoissch ist, ist $\mathbb{L}^G = \mathbb{K}$.
(2) $\Rightarrow$ (3) Hier ist nichts zu zeigen.
(3) $\Rightarrow$ (2) Da die Galoisgruppe G auf den Körper $\mathbb{L}$ wirkt, erhalten wir aus der Bahnformel

$$p = |G| = |\{\sigma(\alpha) : \sigma \in G\}| \cdot |\{\sigma \in G : \sigma(\alpha) = \alpha\}|.$$

Da p nur zwei Teiler hat und die zweite Menge mindestens zwei Elemente besitzt, folgt

$$|\{\sigma \in G : \sigma(\alpha) = \alpha\}| = p,$$

also ist α unter allen Elementen aus G fix.
Alternativ: Es gibt nur eine Gruppe mit Ordnung p, die zyklische Gruppe mit p Elementen. Da nun jedes nicht triviale Element die Gruppe erzeugt, ist α genau dann fix unter einem nicht trivialen Automorphismus, wenn es fix unter allen Automorphismen ist.

Aufgabe 64 (Zyklische Galoiserweiterungen) Sei $\mathbb{K}$ ein Körper der Charakteristik 0, ξ eine n-te primitive Einheitswurzel und $\xi \in \mathbb{K}$. Sei weiter $a \in \mathbb{K}$, α eine Wurzel des Polynoms $f := X^n - a$ und $\mathbb{L} = \mathbb{K}(\alpha)$.

(a) Zeige, daß $\mathbb{L}/\mathbb{K}$ galoissch ist.

(b) Zeige, daß für jedes $\sigma \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$ auch $\sigma(\alpha)$ eine Wurzel von f ist.

(c) Zeige, daß $\frac{\sigma(\alpha)}{\alpha}$ eine n-te Einheitswurzel ist.

Wir setzen $\xi_\sigma := \frac{\sigma(\alpha)}{\alpha}$ für $\sigma \in \mathrm{Gal}(\mathbb{L}, \mathbb{K})$.

(d) Zeige, daß die Abbildung $\varphi : \mathrm{Gal}(\mathbb{L}, \mathbb{K}) \to U_n$, $\varphi(\sigma) := \xi_\sigma$ ein injektiver Gruppenhomomorphismus ist.

(e) Folgere, daß $\mathrm{Gal}(\mathbb{L}, \mathbb{K})$ zyklisch ist.

Lösung: (a) Die Nullstellen von f sind genau die Elemente $\{\alpha, \xi \cdot \alpha, ..., \xi^{n-1} \cdot \alpha\} \subseteq \mathbb{K}(\alpha)$. Somit ist $\mathbb{K}(\alpha)$ der Zerfällungskörper von f und die Erweiterung ist normal und separabel, also galoissch.

(b) Es gilt

$$\sigma(\alpha)^n = \sigma(\alpha^n) = \sigma(a) = a.$$

(c) Es gilt

$$\left(\frac{\alpha}{\sigma(\alpha)}\right)^n = \frac{\alpha^n}{\sigma(\alpha^n)} = \frac{a}{a} = 1.$$

(d) Es gilt

$$\sigma(\alpha) = \xi_\sigma \cdot \alpha.$$

Wir erhalten

$$\begin{aligned}
\xi_{\sigma\circ\tau} &= \frac{\sigma \circ \tau(\alpha)}{\alpha} \\
&= \frac{\sigma(\tau(\alpha))}{\alpha} \\
&= \frac{\sigma(\xi_\tau \alpha)}{\alpha} \\
&= \xi_\tau \cdot \frac{\sigma(\alpha)}{\alpha} \\
&= \xi_\tau \cdot \xi_\sigma \\
&= \xi_\sigma \cdot \xi_\tau.
\end{aligned}$$

Somit ist die Abbildung wie behauptet ein Gruppenhomomorphismus, wobei verwendet wurde, daß jede n-te Einheitswurzel bereits in $\mathbb{K}$, also im Fixkörper aller Automorphismen, liegt. Die Abbildung φ ist injektiv: Wäre $\varphi(\sigma) = 1$, so wäre α fix unter σ. Da es aber eine Basis von $\mathbb{L}$ aus Potenzen von α gibt, ist solch ein Automorphismus bereits die Identität auf $\mathbb{L}$. Also gilt $\ker(\varphi) = \{\mathrm{id}\}$.

(e) Aus dem Homomorphiesatz wissen wir

$$\mathrm{im}(\varphi) \cong \mathrm{Gal}(\mathbb{L}, \mathbb{K})/\ker(\varphi) \cong \mathrm{Gal}(\mathbb{L}, \mathbb{K}).$$

Damit ist die Galoisgruppe der Erweiterung isomorph zu einer Untergruppe einer zyklischen Gruppe, also somit ebenfalls zyklisch und insbesondere abelsch.

Aufgabe 65 (Auflösbare Gruppen) Eine *Normalreihe* einer Gruppe G ist eine Kette von Untergruppen

$$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_n = \{\mathbb{1}\}.$$

Die Quotientengruppen G_i/G_{i+1} heißen die *Faktoren* der Normalreihe. Eine Gruppe G heißt *auflösbar*, wenn es eine Normalreihe von G mit abelschen Faktoren gibt.

(a) Zeige, daß jede abelsche Gruppe G auflösbar ist.

(b) Zeige, daß jede Untergruppe H einer auflösbaren Gruppe G ebenfalls auflösbar ist.

(c) Zeige, daß die Gruppe S_n für $n > 4$ nicht auflösbar ist.

Hinweis: *Du kannst als bekannt vorraussetzen, daß die alternierende Gruppe A_n für $n \neq 4$ eine einfache Gruppe ist.*

Lösung: (a) In diesem Fall ist bereits $G \trianglerighteq \{\mathbb{1}\}$ eine Normalreihe mit abelschen Faktoren.

(b) Es sei $H \subseteq G$ eine Untergruppe. Setze $H_0 := H$ und $H_{i+1} := G_{i+1} \cap H_i$. Dann ist H_{i+1} ein Normalteiler in H_i: Sei $\varphi_i : G_i \to I$ ein Gruppenhomomorphismus mit Kern G_{i+1}. Dann ist $\psi_i := (\varphi_i)_{|H_i}$ ebenfalls ein Gruppenhomomorphismus mit Kern

$$\{g \in H_i : \varphi_i(g) = \mathbb{1}\} = \ker(\varphi_i) \cap H_i = G_{i+1} \cap H_i = H_{i+1}.$$

Somit ist H_{i+1} ebenfalls ein Normalteiler in H_i.
Weiter ist der Quotient H_i/H_{i+1} abelsch. Dies folgt aus

$$H_i/H_{i+1} \cong \mathrm{im}(\psi_i) \subseteq \mathrm{im}(\varphi_i).$$

Da das Bild von φ_i abelsch ist, da G auflösbar war, ist auch das Bild von ψ_i als Untergruppe einer abelschen Gruppe abelsch. Somit ist

$$H = H_0 \trianglerighteq H_1 \trianglerighteq ... \trianglerighteq H_n = \{\mathbb{1}\}$$

eine Normalreihe von H mit abelschen Faktoren und H ist auflösbar.

(c) Aus der Gruppentheorie ist bekannt, daß S_n nur den Normalteiler A_n besitzt und dieser ist für $n \neq 4$ eine einfache Gruppe. Da für $n > 4$ die Gruppe A_n nicht abelsch ist, gibt es keine Normalreihe von S_n mit abelschen Faktoren. Also ist S_n nicht auflösbar.

Aufgabe 66 (Auflösbare Galoiserweiterungen) Es sei $\mathbb{K}$ ein Körper der Charakteristik 0 und f ein Polynom aus $\mathbb{K}[X]$ vom Grad > 0. Weiter sei der Zerfällungskörper von f durch Radikale auflösbar mit Kette von Zwischenkörpern

$$\mathbb{K} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq ... \subseteq \mathbb{K}_m = \mathbb{L},$$

so daß $\mathbb{L}/\mathbb{K}$ galoissch ist und $\mathbb{L}$ den Zerfällungskörper von f enthalte. Weiter entstehe $\mathbb{K}_1$ durch Adjunktion einer n-ten primitiven Einheitswurzel zu $\mathbb{K}$ und $\mathbb{K}_{i+1}$ durch Adjunktion einer Nullstelle eines geeigneten Polynoms $f_{i+1} = X^{d_i} - a_i$ zu $\mathbb{K}_i$, wobei $a_i \in \mathbb{K}_i$ liege und jedes d_i die Zahl n teile.

(a) Zeige, daß $\xi^{\frac{n}{d_i}}$ für jedes $1 \leq i \leq m$ eine primitive d_i-te Einheitswurzel ist.

(b) Zeige, daß $\mathbb{K}_{i+1}/\mathbb{K}_i$ und $\mathbb{K}_1/\mathbb{K}_0$ abelsche Galoiserweiterungen sind.

Es bezeichne G_i die Galoisgruppe $\mathrm{Gal}(\mathbb{L}, \mathbb{K}_i)$.

(c) Zeige, daß die zum Erweiterungsturm korrespondierende Reihe von Gruppen

$$\mathrm{Gal}(\mathbb{L}, \mathbb{K}) = G_0 \supseteq G_1 \supseteq ... \supseteq G_{m-1} \supseteq G_m = \{\mathbb{1}\}$$

eine Normalreihe von G mit abelschen Faktoren ist. Folgere, daß die Galoisgruppe eines durch Radikale auflösbaren Polynoms eine auflösbare Gruppe ist.

(d) Sei $f \in \mathbb{K}[X]$ ein Polynom und $\mathbb{L}/\mathbb{K}$ eine wie in der Vorlesung definierte Auflösung durch Radikale des Zerfällungskörpers von f. Sei die Erweiterung $\mathbb{L}/\mathbb{K}$ zusätzlich galoissch. Zeige, daß es einen Körperturm

$$\mathbb{K} = \tilde{\mathbb{K}}_0 \subseteq \tilde{\mathbb{K}}_1 \subseteq ... \subseteq \tilde{\mathbb{K}}_m = \mathbb{L}$$

gibt, welche die Eigenschaften der Aufgabenstellung besitzt und den Zerfällungskörper von f durch Radikale auflöst.

Man kann zeigen, daß, wenn der Zerfällungskörper $\mathbb{F}$ von f durch Radikale auflösbar ist als Zwischenkörper von $\mathbb{L}/\mathbb{K}$, daß dann der Zerfällungskörper auch durch Radikale auflösbar ist als Zwischenkörper von $\tilde{\mathbb{L}}/\mathbb{K}$, so daß diese Körpererweiterung zusätzlich galoissch ist.

(e) Die Galoisgruppe des Zerfällungskörpers des Polynoms $X^5 - X - 1 \in \mathbb{Q}[X]$ über $\mathbb{Q}$ ist die S_5. Folgere, daß es keine Lösungsformel für die Nullstellen von f geben kann, welche durch ineinandergeschachtelte Wurzelausdrücke von Koeffizienten von f gegeben ist. Somit kann es kein Pendant zur pq-Formel für Polynome vom Grad 5 geben.

Lösung: (a) Es ist für $0 < l < d_i$ die Zahl $l \cdot \frac{n}{d_i}$ echt kleiner als n, also ist $\xi^{l \cdot \frac{n}{d_i}} \neq 1$. Das die angegebene Zahl eine d_i-te Einheitswurzel ist, ist offensichtlich, nach unserer einleitenden Bemerkung ist diese primitiv, weil ξ primitiv war.

(b) Alle Vorraussetzungen von Aufgabe 64 sind erfüllt. Somit ist $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_i)$ eine zyklische Galoiserweiterung.

(c) Da $\mathbb{K}_{i+1}/\mathbb{K}_i$ galoissch ist, ist G_{i+1} normal in G_i mit Quotient $G_i/G_{i+1} \cong \mathrm{Gal}(\mathbb{K}_{i+1}, \mathbb{K}_i)$. Dieser Quotient ist zyklisch, also insbesondere abelsch. Somit ist die angegebene Reihe eine Normalreihe von G mit abelschen Faktoren, also ist G auflösbar.
Da die Galoisgruppe des Zerfällungskörpers von f eine Untergruppe von G ist, ist diese ebenfalls auflösbar, da Untergruppen auflösbarer Gruppen wieder auflösbar sind nach Aufgabe 65.

(d) Es ist $\mathbb{L} = \mathbb{K}(A_1, ..., A_m)$, wobei jedes A_i die Nullstellenmenge des Polynoms $f_i := X^{n_i} - a_i \in \mathbb{K}_i[X]$ ist. Jede der Mengen A_i enthält mit einer Nullstelle α_i von f_i auch die Nullstelle $\xi_i\alpha_i$, wobei ξ_i eine n_i-te Einheitswurzel ist. Somit brauchen wir alle n_i-ten Einheitswurzeln in unserer Erweiterung. Wählen wir $N := kgV(n_i)$, und adjungieren im ersten Schritt zu $\mathbb{K}$ die primitve N-te Einheitswurzel dazu, so teilt jedes n_i das N und die erste Erweiterung $\mathbb{K}(\xi_N)/\mathbb{K}$ ist galoissch. Nun adjungieren wir im zweiten Schritt eine Nullstelle von f_1 dazu und erhalten $\tilde{\mathbb{K}}_2$, über welchem f_1 zerfällt. Im nächsten Schritt adjungieren wir eine Nullstelle von f_2 zu $\tilde{\mathbb{K}}_2$ dazu, Dank der Geometrie der Nullstellen und der Existenz der Einheitswurzel zerfällt f_2 ebenfalls, usw...

(e) Nach Aufgabe 65 wissen wir, daß S_5 nicht auflösbar ist. Somit können die Nullstellen von f nicht durch iteriertes Wurzelziehen ausgedrückt werden, da jede Radikalerweiterung des Zerfällungskörpers von f eine nicht auflösbare Gruppe als Untergruppe hätte, also keine Normalreihe mit abelschen Faktoren besitzen dürfte. Damit kann es diese Radikalerweiterung nicht geben.

Aufgabe 67 (Mehr zu auflösbaren Gruppen) Die *Kommutatorgruppe* $[G, G]$ einer Gruppe G ist die kleinste Untergruppe von G, die alle Kommutatoren $[g, h] := ghg^{-1}h^{-1}$ enthält.

(a) Zeige, daß eine Gruppe genau dann abelsch ist, wenn $[G, G] = \{\mathbb{1}\}$ gilt.

(b) Zeige, daß $[G, G]$ die kleinste normale Untergruppe von G mit abelschem Quotienten ist.

Wir setzen $G^0 := G$ und $G^{n+1} := [G^n, G^n]$. Die Gruppe G^{n+1} heißt die $n + 1$-*te iterierte Kommutatorgruppe von* G.

(c) Zeige, daß eine Gruppe G genau dann auflösbar ist, wenn es eine Zahl $n \in \mathbb{N}$ gibt mit $G^n = \{\mathbb{1}\}$.

(d) Sei G eine Gruppe, N ein Normalteiler in G und $Q := G/N$ die Quotientengruppe. Zeige, daß G genau dann auflösbar ist, wenn N und Q auflösbar sind.

(e) Warum ist ein (semi-)direktes Produkt von auflösbaren Gruppen G und H wieder auflösbar?

Lösung: (a) Ist G abelsch, so gilt $ghg^{-1}h^{-1} = gg^{-1}hh^{-1} = \mathbb{1}$. Umgekehrt, gilt $[g, h] = \mathbb{1}$, so vertauschen g und h. Da alle Kommutatoren verschwinden, vertauschen je zwei beliebige Elemente. Damit ist die Gruppe abelsch.

(b) Betrachte $g[G, G]g^{-1}$ für ein beliebiges $g \in G$. Da $[G, G]$ von Kommutatoren erzeugt wird, wird auch $g[G, G]g^{-1}$ von konjugierten Kommutatoren erzeugt, da die Konjugation mit g ein Gruppenautomorphismus ist. Weiter sehen wir

$$g[h_1, h_2]g^{-1} = gh_1h_2h_1^{-1}h_2^{-1}g^{-1} = gh_1g^{-1}gh_2g^{-1}gh_1^{-1}g^{-1}gh_2^{-1} = [gh_1g^{-1}, gh_2g^{-1}],$$

also ist ein konjugierter Kommutator wieder ein Kommutator und wir erhalten $[G,G] = g[G,G]g^{-1}$. Die Untergruppe $[G,G]$ ist also normal in G.
Es sei G/N abelsch. Sei φ die Quotientenabbildung. Dann sehen wir $\varphi([g,h]) = [\varphi(g),\varphi(h)] = \mathbb{1}$. Somit liegt die von den Kommutatoren erzeugte Untergruppe im Kern von φ, also folgt $[G,G] \subseteq N$. Damit enthält jeder Normalteiler mit abelschem Quotienten automatisch $[G,G]$ und ist somit größer als $[G,G]$.

(c) Angenommen, $G^n = \{\mathbb{1}\}$. Dann ist

$$G = G^0 \trianglerighteq G^1 \trianglerighteq ... \trianglerighteq G^n = \{\mathbb{1}\}$$

eine Normalreihe mit abelschen Quotienten, also ist G auflösbar.
Ist G auflösbar und

$$G = G_0 \trianglerighteq G_1 \trianglerighteq ... \trianglerighteq G_n = \{\mathbb{1}\}$$

eine Normalreihe mit abelschen Quotienten, so gilt $G^m \subseteq G_m$ für alle $0 \leq i \leq n$. Dies zeigen wir via Induktion.
Für $i = 0$ ist die Behauptung trivialerweise wahr, da $G_0 = G^0$ gilt.
Es gelte $G^i \subseteq G_i$ für ein $i \geq 0$. Dann erhalten wir, da G_i/G_{i+1} abelsch ist, $[G_i,G_i] \subseteq G_{i+1}$. Wir sehen also

$$G^{i+1} = [G^i,G^i] \subseteq [G_i,G_i] \subseteq G_{i+1}.$$

(d) Ist G auflösbar, so ist auch N auflösbar. Weiter ist der Quotientenhomomorphismus $\pi : G \to Q$ surjektiv und bildet Kommutatoren in Kommutatoren ab, also $\pi(G^1) \subseteq Q^1$. Da π surjektiv ist, liegt jeder Kommutator aus Q^1 im Bild von π, also gilt sogar

$$\pi([G,G]) = [Q,Q].$$

Analog folgt

$$\pi(G^i) = Q^i,$$

also ist Q auflösbar.
Seien nun Q und N auflösbar und n so gewählt, daß $N^n = Q^n = \{\mathbb{1}\}$ gelte. Dann erhalten wir

$$\pi(G^n) = Q^n = \{\mathbb{1}\},$$

also $G^n \subseteq N$. Daraus folgt aber nun

$$G^{2n} \subseteq N^n = \{\mathbb{1}\}$$

und damit ist G auflösbar.

(e) Im (semi-)direkten Produkt von G und H ist eine der Faktoren ein Normalteiler und der andere der Quotient des Produktes nach diesem. Somit ist das (semi-)direkte Produkt als eine Erweiterung auflösbarer Gruppen wieder auflösbar.

Hausübungen

Aufgabe H27 (Kreisteilungskörper I) Sei a eine primitive siebte Einheitswurzel, dann ist $\mathbb{Q}(a)/\mathbb{Q}$ galoissch als Zerfällungskörper von $\Phi_7 = X^6 + X^5 + ... + X + 1$. Es bezeichne G die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}(a), \mathbb{Q})$.

(a) Zeige, daß ein $\sigma \in G$ existiert mit $\sigma(a) = a^3$.

(b) Zeige, daß σ die Gruppe G erzeugt.

(c) Zeige, daß für jedes $z \in \mathbb{Q}(a)$ die Gleichung $\sigma^3(z) = \overline{z}$ gilt, sofern wir $\mathbb{Q}(a) \subseteq \mathbb{C}$ verstehen.

(d) Bestimme das Minimalpolynom von $b := a + a^6$ und von $c := a + a^2 + a^4$ in $\mathbb{Q}[X]$.

(e) Zeige, daß die einzigen echten Zwischenkörper der Erweiterung $\mathbb{Q}(a)/\mathbb{Q}$ durch die Erweiterungen $\mathbb{Q}(b)/\mathbb{Q}$ und $\mathbb{Q}(c)/\mathbb{Q}$ gegeben sind.

LÖSUNG: (a) Da Φ_7 in $\mathbb{Q}[X]$ irreduzibel und $\mathbb{Q}(a)/\mathbb{Q}$ galoissch ist, gibt es einen Automorphismus σ mit $\sigma(a) = a^3$.

(b) Da der Erweiterungsgrad $[\mathbb{Q}(a) : \mathbb{Q}] = 6 = |\mathrm{Gal}(\mathbb{Q}(a), \mathbb{Q})|$ gilt, reicht es zu zeigen, daß σ die Ordnung 6 hat. Dies folgt nun leicht aus folgenden Rechnungen

$$\begin{aligned}
\sigma(a) &= a^3 \\
\sigma(a^3) &= \sigma(a)^3 = a^9 = a^2 \\
\sigma(a^2) &= \sigma(a)^2 = a^6 \\
\sigma(a^6) &= \sigma(a)^6 = a^{18} = a^4 \\
\sigma(a^4) &= \sigma(a)^4 = a^{12} = a^5 \\
\sigma(a^5) &= \sigma(a)^5 = a^{15} = a.
\end{aligned}$$

Somit hat σ die Ordnung 6 und erzeugt die Galoisgruppe.

(c) Die komplexe Konjugation ist ebenso ein Automorphismus wie σ, also reicht es, den Wert auf einem algebraischen Erzeuger, hier a, zu kennen. Aus $\sigma^3(a) = a^6 = \overline{a}$ folgt die Behauptung, egal welche primitive 6-te Einheitswurzel wir gewählt haben, siehe in den Rechnungen aus (b).

(d) Die Bahn von b unter $< \sigma >$ ist

$$\{a + a^6, a^3 + a^4, a^2 + a^5\},$$

also ist das Minimalpolynom von a gegeben durch

$$m_{b,\mathbb{Q}}(X) = (X - a - a^6)(X - a^2 - a^5)(X - a^3 - a^4).$$

Ausrechnen der Terme liefert mit der Relation $\Phi_7(a) = 0$ die Gestalt

$$m_{b,\mathbb{Q}}(X) = X^3 + X^2 - 2X - 1.$$

Die Bahn von c unter $< \sigma >$ ist

$$\{a + a^2 + a^4, a^3 + a^5 + a^6\},$$

also ist das Minimalpolynom von a gegeben durch

$$m_{c,\mathbb{Q}}(X) = (X - a - a^2 - a^4)(X - a^3 - a^5 - a^6).$$

Ausrechnen der Terme liefert

$$m_{c,\mathbb{Q}}(X) = X^2 + X + 2.$$

(e) Die Galoisgruppe ist als zyklische Gruppe isomorph zu $\mathbb{Z}_6 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3$. Damit gibt es genau eine Untergruppe der Ordnung 2 und der Ordnung 3 und diese sind Normalteiler, da die Gruppe abelsch ist. Also gibt es genau 2 Zwischenkörper der Erweiterung und diese sind ebenfalls galoissch über $\mathbb{Q}$. Andererseits gilt $[\mathbb{Q}(b) : \mathbb{Q}] = 3$ und $[\mathbb{Q}(c) : \mathbb{Q}] = 2$, und diese sind Zwischenkörper. Somit sind beide Erweiterungen galoissch und die einzigen Zwischenkörper von $\mathbb{Q}(a)/\mathbb{Q}$.

Aufgabe H28 (Kreisteilungskörper II) Sei $\mathbb{L} := \mathbb{Q}(\xi_8)$ der achte Kreisteilungskörper über $\mathbb{Q}$, es sei also ξ_8 eine primitive achte Einheitswurzel. Bestimme die Galoisgruppe der Erweiterung, deren Untergruppen und alle Zwischenkörper der Erweiterung. Welche der Zwischenkörper sind ebenfalls galoissch über $\mathbb{Q}$?

LÖSUNG: Die Galoisgruppe von $\mathbb{L}/\mathbb{Q}$ ist isomorph zu $\mathbb{Z}_8^\times \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Dies sehen wir dadurch, daß jede der Zahlen $\{1, 3, 5, 7\}$ in $\mathbb{Z}_8$ invertierbar ist und ihr Quadrat 1 ergibt. Weiter ist $\Phi_8 = X^4 + 1$ das achte Kreisteilungspolynom, also erfüllt die primitive achte Einheitswurzel a in $\mathbb{Q}(a)$ die Gleichung $a^4 = -1$.
Da X^4+1 irreduzibel über $\mathbb{Q}$ ist, ist der Erweiterungsgrad $[\mathbb{Q}(a) : \mathbb{Q}] = 4$ und $\{1, a, a^2, a^3\}$ ist eine $\mathbb{Q}$-Basis von $\mathbb{Q}(a)$. Es gibt nun genau drei nichtriviale Galoisautomorphismen, welche eindeutig durch ihre Wirkung auf a bestimmt sind.

$$\sigma_1(a) := a^3, \quad \sigma_2(a) := -a, \quad \sigma_3(a) := -a^3.$$

Jeder dieser Automorphismen ist selbstinvers und der Fixkörper eines dieser Automorphismen ist ein Zwischenkörper der Erweiterung. Wir sehen leicht ein

$$\begin{aligned} \mathrm{Fix}(\sigma_1) &= \mathbb{Q}(a + a^3), \\ \mathrm{Fix}(\sigma_2) &= \mathbb{Q}(a^2), \\ \mathrm{Fix}(\sigma_3) &= \mathbb{Q}(a - a^3). \end{aligned}$$

Alle diese Zwischenkörper sind galoissch über $\mathbb{Q}$, da die Galoisgruppe abelsch ist.

Aufgabe H29 (Bonusaufgabe: Inverses Galoisproblem) Zeige mit Hilfe der Theorie über Kreisteilungserweiterungen, daß es eine galoissche Körpererweiterung $\mathbb{L}/\mathbb{Q}$ gibt mit $\mathrm{Gal}(\mathbb{L}, \mathbb{Q}) = \mathbb{Z}_7$.

LÖSUNG: Die Zahl 43 ist eine Primzahl, also ist $\mathbb{Z}_{43}^\times$ zur zyklischen Gruppe $\mathbb{Z}_{42}$ isomorph. Diese enthält $\mathbb{Z}_6$ als Normalteiler mit Quotienten $\mathbb{Z}_7$, also gibt es einen Zwischenkörper des 43-ten Kreisteilungskörpers, welcher $\mathbb{Z}_7$ als Galoisgruppe über $\mathbb{Q}$ hat nach dem Hauptsatz der Galoistheorie.