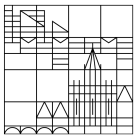
Fachbereich Mathematik und Statistik
Prof. Dr. Salma Kuhlmann
Gabriel Lehéricy
Simon Müller
WS 2016-2017

Universität Konstanz



Übungen zur Vorlesung Algebra B3

Blatt 13-Lösung

Ich erinnere die folgenden Tatsachen, die für die Berechnung von Galoisgruppen besonders nützlich sind:

Tatsache 1: Sei L/K eine Erweiterung und $\alpha_1, \dots, \alpha_n \in K$ mit $L = K(\alpha_1, \dots, \alpha_n)$. Dann ist jeder K-Automorphismus σ von L durch $\sigma(\alpha_1), \dots, \sigma(\alpha_n)$ vollständig bestimmt.

Beweis: Jedes $x \in L$ lässt sich als $f(\alpha_1, \dots, \alpha_n)$ schreiben, wobei $f \in K(X_1, \dots, X_n)$. Weil die Koeffizienten von f in K liegen, gilt dann $\sigma(f(\alpha_1, \dots, \alpha_n)) = f(\sigma(\alpha_1), \dots, \sigma(\alpha_n))$.

Tatsache 2: Sei L/K eine galoissche Erweiterung, $\alpha \in K$ mit $L = K(\alpha)$ und $g = m_{\alpha,K}$. Dann existiert für jede Nullstelle β von g ein eindeutiger K-Automorphismus σ_β von L mit $\sigma_\beta(\alpha) = \beta$. Außerdem ist die Abbildung:

$$\begin{aligned} \{\text{Nullstellen von } g\} &\to Gal(L/K) \\ \beta &\mapsto \sigma_\beta \end{aligned}$$

eine Bijektion.

Beweis: Die existenz von σ_β folgt aus dem Satz 3 der 9-ten Vorlesung (mit $F = F' = K$ und $\phi = id$), die Eindeutigkeit ist durch Tatsache 1 gegeben. Die oben angegebene Abbildung ist offensichtlich injektiv. Zur surjektivität: Sei $\sigma \in Gal(L/K)$; weil die Koeffizienten von g in K liegen, gilt $g(\alpha) = 0 \Rightarrow g(\sigma(\alpha)) = 0$, also ist $\sigma(\alpha)$ eine Nullstelle von g.

Diese zwei Tatsachen dürfen Sie immer ohne Beweis anwenden.

Aufgabe 1

a) Sei L/K eine endliche Erweiterung und $S \subseteq L$ eine Teilmenge, so dass $L = K(S)$. Zeigen Sie, dass es eine endliche Teilmenge R von S gibt, so dass $L = K(R)$

Induktion auf $n := [L : K]$. Fall $n = 1$: Es gilt $L = K(x)$ für jedes $x \in S$. Induktionsschritt: für $n > 1$ gilt $L \neq K$ also gibt es $x \in S \backslash K$. Nach dem Gradsatz gilt $[L : K] = [L : K(x)][K(x) : K]$, und wegen $x \notin K$ gilt $[K(x) : K] > 1$, also ist $[L : K(x)] < n$. Weil $L = K(x)(S)$ können wir dann die Induktionsvoraussetzung anwenden: es existiert eine endliche Teilmenge R von S mit $L = K(x)(R)$. Dann gilt $L = K(\{x\} \cup R)$, wobei $\{x\} \cup R$ eine endliche Teilmenge von S ist.

b) Sei L/K eine endliche normale Erweiterung. Zeigen Sie, dass L der Zerfällungskörper einer endlichen Familie von Polynomen in $K[X]$ ist.

Nach Definition von normaler Erweiterung ist L der Zerfällungskörper einer (möglicherweise unendlichen) Familie $\mathcal{F}$ von Polynomen von $K[X]$. Nach Definition von Zerfällungskörper wird L von der Menge S aller Nullstellen aller Polynome in $\mathcal{F}$ erzeugt. Nach a) gibt es eine endliche Teilmenge R von S mit $L = K(R)$. Zu jedem $r \in R$ gibt es ein f_r in $\mathcal{F}$ mit $f_r(r) = 0$. Dann ist L der Zerfällungskörper der endlichen Familie $\{f_r \mid r \in R\}$.

Aufgabe 2
Für diese Aufgabe dürfen Sie ohne Beweis die folgende Behauptung benutzen:
Sei $n \in \mathbb{N}$, $\zeta_n := e^{\frac{2i\pi}{n}}$ und $k \in \mathbb{N}$. Dann haben ζ_n und ζ_n^k genau dann das gleiche Minimalpolynom über $\mathbb{Q}$, wenn $ggT(n,k) = 1$.

Sei $n \in \mathbb{N}$ und $f := X^n - 1 \in \mathbb{Q}[X]$ und sei K der Zerfällungskörper von f. Zeigen Sie, dass $\mathrm{Gal}(K/\mathbb{Q})$ eine abelsche Gruppe der Ordnung $\phi(n)$ ist, wobei ϕ die eulersche phi-Funktion bezeichnet. Bestimmen Sie dann den Grad der Erweiterung $K/\mathbb{Q}$.

K wird von den Nullstellen von f erzeugt. Sei $\zeta_n := e^{\frac{2i\pi}{n}}$. Die Nullstellen von f sind die ζ^k für $k \in \{0 \ldots, n-1\}$, also gilt $K = \mathbb{Q}(\zeta)$. Sei $g := m_{\zeta,\mathbb{Q}}$. Um die Galoisgruppe zu berechnen, müßen wir zunächst die Nullstellen von g bestimmen (siehe Tatsache 2 oben).
Wegen $f(\zeta) = 0$ gilt $g \mid f$. Die Nullstellen von g sind also in der Menge $\{1, \zeta, \ldots, \zeta^{n-1}\}$ enthalten. Nach dem Hinweis ist also die Menge der Nullstellen von g genau $\{\zeta^k \mid ggT(n,k) = 1\}$.
Nach Tatsache 2 gilt also $Gal(K/\mathbb{Q}) = \{\sigma_k \mid 0 \leq k \leq n-1 \wedge ggT(k,n) = 1\}$, wobei σ_k durch $\sigma_k(\zeta) = \zeta^k$ definiert ist. Man betrachte jetzt die Abbildung:

$$(\mathbb{Z}/n\mathbb{Z})^* \to Gal(K/\mathbb{Q})$$
$$k \mapsto \sigma_k$$

Man kann leicht zeigen, dass dies ein Gruppenisomorphismus von $((\mathbb{Z}/n\mathbb{Z})^*, .)$ nach $Gal(K/\mathbb{Q})$ ist, also gilt $|Gal(K/\mathbb{Q})| = \phi(n)$. Weil die Erweiterung $K/\mathbb{Q}$ galoissch ist, gilt $[K : \mathbb{Q}] = |Gal(K/\mathbb{Q})| = \phi(n)$.

Aufgabe 3
Sei $K := \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Zeigen Sie, dass die Erweiterung $K/\mathbb{Q}$ galoissch ist. Bestimmen Sie dann $\mathrm{Gal}(K/\mathbb{Q})$ und geben Sie alle Zwischenkörper der Erweiterung $K/\mathbb{Q}$ an.

Wir wissen schon aus Blatt 6, dass $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Das ist der Zerfällungskörper des separablen Polynoms $(X^2 - 2)(X^2 - 3)$, also ist $\mathbb{Q}(\sqrt{2} + \sqrt{3})/\mathbb{Q}$ galoissch. Nach dem Gradsatz gilt $[K : \mathbb{Q}] = [K : \mathbb{Q}(\sqrt{3})][\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$. $X^2 - 3$ ist das Minimalpolynom von $\sqrt{3}$ über $\mathbb{Q}$ und $X^2 - 2$ das Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}(\sqrt{3})$ (weil $\sqrt{2} \notin \mathbb{Q}(\sqrt{3})$), also gilt $[K : \mathbb{Q}] = 4$.

Weil die Erweiterung $K/\mathbb{Q}$ galoissch ist, gilt dann $|Gal(K/\mathbb{Q})| = 4$. Wir suchen jetzt die Elemente von $Gal(K/\mathbb{Q})$. Wir bemerken zunächst, dass $Gal(K/\mathbb{Q}(\sqrt{3}))$ und $Gal(K/\mathbb{Q}(\sqrt{2}))$ in $Gal(K/\mathbb{Q})$ enthalten sind und suchen Elemente in $Gal(K/\mathbb{Q}(\sqrt{3}))$ und $Gal(K/\mathbb{Q}(\sqrt{2}))$. Nach Tatsache 2 gibt es $\sigma \in Gal(K/\mathbb{Q}(\sqrt{3}))$ mit $\sigma(\sqrt{2}) = -\sqrt{2}$. Ähnlich gibt es $\tau \in Gal(K/\mathbb{Q}(\sqrt{2}))$ mit $\tau(\sqrt{3}) = -\sqrt{3}$. Wir haben also zwei Elemente σ, τ von $Gal(K/\mathbb{Q})$ gefunden. Sie erzeugen eine Guppe der Ordnung 4, deren Wirkung auf K durch die folgende Tabelle gegeben ist:

	id	σ	τ	$\sigma\tau$
$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$
$\sqrt{3}$	$\sqrt{3}$	$\sqrt{3}$	$-\sqrt{3}$	$-\sqrt{3}$

Weil $|Gal(K/\mathbb{Q})| = 4$, gibt es keine weitere $\mathbb{Q}$-Automorphismen von K, also gilt $Gal(K/\mathbb{Q}) = \{id, \sigma, \tau, \sigma\tau\}$. Man erkennt dann, dass $Gal(K/\mathbb{Q})$ die kleinsche Vierergruppe ist (die kleinsche Vierergruppe ist die einzige Gruppe der Ordnung 4, die kein Element der Ordnung 4 hat).
Um die Zwischenkörper der Erweiterung zu finden, wenden wir den Hauptsatz der Galoistheorie an. Wir suchen zunächst die Untergruppen von $Gal(K/\mathbb{Q})$, und berechnen dann die entsprechenden Fixkörper. Die Untergruppen von $Gal(K/\mathbb{Q})$ sind $H_1 = \{id\}$, $H_2 = \{id, \sigma\}$, $H_3 = \{id, \tau\}$, $H_4 = \{id, \sigma\tau\}$ und $H_5 = G$. Wir suchen jetzt $Inv(H_2)$. σ fixiert $\sqrt{3}$, also ist $\mathbb{Q}(\sqrt{3}) \subseteq Inv(H_2)$. Außerdem gilt nach dem Hauptsatz $[Inv(H_2) : \mathbb{Q}] = [G : H_2] = 2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ und daraus folgt $Inv(H_2) = \mathbb{Q}(\sqrt{3})$. Ähnlich zeigt man $Inv(H_3) = \mathbb{Q}(\sqrt{2})$ und $Inv(H_4) = \mathbb{Q}(\sqrt{6})$.
Die Zwischenkörper sind also $K_1 = Inv(H_1) = K$, $K_2 = Inv(H_2) = \mathbb{Q}(\sqrt{3})$, $K_3 = Inv(H_3) = \mathbb{Q}(\sqrt{2})$, $K_4 = Inv(H_4) = \mathbb{Q}(\sqrt{6})$ und $K_5 = Inv(G) = \mathbb{Q}$.

Aufgabe 4
Sei $f = X^4 - 3 \in \mathbb{Q}[X]$ und K der Zerfällungskörper von f. Bestimmen Sie Gal$(K/\mathbb{Q})$ und finden Sie alle Zwischenkörper der Erweiterung $K/\mathbb{Q}$.

Wir suchen zuerst die Nullstellen von f, weil K von ihnen erzeugt ist. Es gilt für alle $x \in \mathbb{C}$: $x^4 = 3 \Leftrightarrow (\frac{x}{\sqrt[4]{3}})^4 = 1 \Leftrightarrow \frac{x}{\sqrt[4]{3}} \in \{1, i, -1, -i\}$. Die Nullstellen von f sind also $\alpha, i\alpha, -\alpha, -i\alpha$, wobei $\alpha = \sqrt[4]{3}$. Es folgt, dass $K = \mathbb{Q}(\alpha, i\alpha, -\alpha, -i\alpha) = \mathbb{Q}(\alpha, i)$.
Wir suchen zunächst den Grad der Erweiterung $K/\mathbb{Q}$. $X^4 - 3$ ist irreduzibel über $\mathbb{Q}$ nach Eisenstein mit $p = 3$ und Lemma von Gauss, also ist es das Minimalpolynom von α über $\mathbb{Q}$, also gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$. Ausserdem ist i eine Nullstelle von $X^2 + 1 \in \mathbb{Q}(\alpha)[X]$, und es gilt $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$, also $i \notin \mathbb{Q}(\alpha)$, also ist $X^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}(\alpha)$, also ist $[K : \mathbb{Q}(\alpha)] = 2$. Nach dem Gradsatz gilt $[K : \mathbb{Q}] = \underbrace{[K : \mathbb{Q}(\alpha)]}_{=2}\underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}]}_{=4} = [K : \mathbb{Q}(i)]\underbrace{[\mathbb{Q}(i) : \mathbb{Q}]}_{=2}$. Aus dieser Gleichung folgt, dass $[K : \mathbb{Q}(i)] = 4$, also ist $X^4 - 3$ das Minimalpolynom von α über $\mathbb{Q}(i)$. Es folgt auch $[K : \mathbb{Q}] = 8$, und weil die Erweiterung $K/\mathbb{Q}$ galoissch ist, gilt dann $|Gal(K/\mathbb{Q})| = 8$.
Wir suchen jetzt die Elemente von $Gal(K/\mathbb{Q})$. Es ist zunächst einfacher, Elemente von $Gal(K/\mathbb{Q}(i))$ und $Gal(K/\mathbb{Q}(\alpha))$ zu finden; dafür wenden wir Tatsache 2 an. Weil $X^4 - 3$ das Minimalpolynom von α über $\mathbb{Q}(i)$ ist, gibt es Nach Tatsache 2 ein $\sigma \in Gal(K/\mathbb{Q}(i))$ mit $\sigma(\alpha) = i\alpha$. Ähnlich gibt es $\tau \in Gal(K/\mathbb{Q}(\alpha))$ mit $\tau(i) = -i$.
Mit τ und σ werden schon 8 paarweise verschiedene Automorphismen erzeugt, deren Wirkung auf K durch die folgende Tabelle gegeben ist:

	id	τ	σ	σ^2	σ^3	$\tau\sigma$	$\tau\sigma^2$	$\tau\sigma^3$
i	i	$-i$	i	i	i	$-i$	$-i$	$-i$
α	α	α	$i\alpha$	$-\alpha$	$-i\alpha$	$-i\alpha$	$-\alpha$	$i\alpha$

Weil $|Gal(K/\mathbb{Q})| = 8$ gilt, gibt es keine weitere $\mathbb{Q}$-Automorphismen von K. Durch $\sigma^4 = \tau^2 = id$ und $\tau\sigma\tau = \sigma$ erkennt man die Gruppe D_4, also gilt $Gal(K/\mathbb{Q}) \cong D_4$.
Wir suchen jetzt die Zwischenkörper von $K/\mathbb{Q}$. Wir wenden den Hauptsatz der Galoishteorie an, indem wir zunächst die Untergruppen von $Gal(K/\mathbb{Q})$ suchen und dann die entsprechenden Fixkörper berechnen. Nach Lagrange haben alle Untergruppen von $Gal(K/\mathbb{Q})$ die Odnung $1, 2, 4$, oder 8. Es gibt 5 Elemente der Ordnung 2 in $Gal(K/\mathbb{Q})$, jedes von ihnen erzeugt eine Untergruppe der Ordnung 2: $H_1 = \{id, \tau\}$, $H_2 = \{id, \sigma^2\}$ $H_3 = \{id, \tau\sigma\}$ $H_4 = \{id, \tau\sigma^2\}$ $H_5 = \{id, \tau\sigma^3\}$. Wir suchen jetzt die Untergruppen der Ordnung 4. Sie werden entweder von einem Element der Ordnung 4 oder von 2 Elementen der Ordnung 2 erzeugt. Die einzigen Elemente der Ordnung 4 sind σ und σ^3, beide erzeugen die Gruppe $H_6 := \{id, \sigma, \sigma^2, \sigma^3\}$. Um andere Untergruppen der Ordnung 4 zu finden, betrachtet man alle Untergruppen, die von zwei Elementen der Ordung 2 erzeugt sind. Es gibt $H_7 :=< \sigma^2, \tau >= \{id, \sigma^2, \tau, \tau\sigma^2\}$ und $H_8 :=< \sigma^2, \tau\sigma >= \{id, \sigma^2, \tau\sigma, \tau\sigma^3\}$; man sollte hier prüfen, dass diese Mengen unter Multiplikation abgeschlossen sind. Es gibt keine weitere Untergruppen der Ordnung 4, weil $< \tau, \tau\sigma >=< \tau, \tau\sigma^3 >=< \tau\sigma, \tau\sigma^2 >=< \tau\sigma^2, \tau\sigma^3 >= Gal(K/\mathbb{Q})$.
Die Untergruppen von $Gal(K/\mathbb{Q})$ sind also $H_0 := \{id\}, H_1, \ldots, H_8, H_9 := Gal(K/\mathbb{Q})$. Wir müßen jetzt die entsprechenden Fixkörper $K_0, \ldots, K_9$ bestimmen. Es gilt $K_0 = K$ und $K_9 = \mathbb{Q}$. Nach dem Hauptsatz wissen wir, dass $[K_n : \mathbb{Q}] = [G : H_n]$ für alle $n \in \{1, \ldots, 8\}$. τ fixiert α, also $\mathbb{Q}(\alpha) \subseteq K_1$, außerdem gilt $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 = [G : H_1] = [K_1 : \mathbb{Q}]$, also muss $K_1 = \mathbb{Q}(\alpha)$ gelten. Ähnlich zeigt man $K_2 = \mathbb{Q}(i, \alpha^2)$ $K_3 = \mathbb{Q}(\alpha - i\alpha)$, $K_4 = \mathbb{Q}(i\alpha)$ $K_5 = \mathbb{Q}(\alpha + i\alpha)$, $K_6 = \mathbb{Q}(i)$, $K_7 = \mathbb{Q}(\alpha^2)$, $K_8 = \mathbb{Q}(i\alpha^2)$.

Zusatzaufgabe für Interessierte
Sei $K := \mathbb{Q}(\sqrt[8]{2}, i)$. Zeigen Sie:

(a) $Gal(K/\mathbb{Q}(i)) \cong C_8$

Sei $\alpha := \sqrt[8]{2}$. Wir zeigen zunächst, dass $|Gal(K/\mathbb{Q}(i))| = 8$. Weil $i \notin \mathbb{Q}(\sqrt[8]{2})$ gilt, ist $X^2 + 1$ das Minimalpolynom von i über $\mathbb{Q}(\alpha)$, also gilt nach dem Gradsatz:
$[K : \mathbb{Q}] = \underbrace{[K : \mathbb{Q}(\alpha)]}_{=2}\underbrace{[\mathbb{Q}(\alpha) : \mathbb{Q}]}_{=8} = [K : \mathbb{Q}(i)]\underbrace{[\mathbb{Q}(i) : \mathbb{Q}]}_{=2}$, also gilt $[K : \mathbb{Q}(i)] = 8$ und $X^8 - 2$ ist dann das Minimalpolynom von α über $\mathbb{Q}(i)$. Weil die Erweiterung $K/\mathbb{Q}(i)$ galoissch ist (es ist der Zerfällungskörper von $X^8 - 2$) gilt dann $|Gal(K/\mathbb{Q}(i))| = 8$. Die Nullstellen von f sind die $\alpha\zeta_8^k$ für $k \in \{0, \ldots, 7\}$, wobei $\zeta_8 = e^{\frac{i\pi}{4}}$. Nach Tatsache 2 gibt es $\sigma \in Gal(K/\mathbb{Q}(i))$ mit $\sigma(\alpha) = \zeta_8\alpha$. Wir müßen jetzt nur prüfen, dass $|\sigma| = 8$: dann ist $Gal(K/\mathbb{Q}(i)) =< \sigma >$, eine zyklische Gruppe der Ordnung 8. Es gilt $\zeta_8 = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$. Wegen $\sigma(i) = i$ und $\sigma(\sqrt{2}) = \sigma(\alpha)^4$ gilt also $\sigma(\zeta_8) = \zeta_8^5$. Damit kann man $\sigma^2, \ldots, \sigma^7$ bestimmen, indem man $\sigma^k(\alpha)$ berechnet. Man sieht dann, dass $id, \sigma, \sigma^2, \ldots, \sigma^7$ paarweise verschieden sind.

(b) $Gal(K/\mathbb{Q}(\sqrt{2})) \cong D_4$.

Wir wissen schon, dass $[K : \mathbb{Q}] = 16$ und $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, also muss nach dem Gradsatz $[K : \mathbb{Q}(\sqrt{2})] = 8$ gelten. Mit dem Gradsatz zeigt man auch, dass $[\mathbb{Q}(\alpha) : \mathbb{Q}(\sqrt{2}, i)] = 4$, also ist $X^4 - \sqrt{2}$ das Minimalpolynom von α über $\mathbb{Q}(\sqrt{2}, i)$. Die Nullstellen dieses Polynoms sind

$\alpha, i\alpha, -\alpha, -i\alpha$. Nach Tasache 2 gibt es $\sigma \in Gal(K, \mathbb{Q}(i, \sqrt{2}))$ mit $\sigma(\alpha) = i\alpha$. Man zeigt ähnlich, dass es $\tau \in Gal(K/\mathbb{Q}(\sqrt{2}, \alpha))$ mit $\tau(i) = -i$ gibt. Der Beweis läuft dann wie bei Aufgabe 4.

(c) $Gal(K/\mathbb{Q}(i\sqrt{2})) \cong Q_8$, die Quaternionengruppe (siehe Aufgabe 10.4)

Es gilt $[\mathbb{Q}(i\sqrt{2}) : \mathbb{Q}] = 2$ ($X^2 + 2$ ist das Minimalpolynom), also $[K : \mathbb{Q}(i\sqrt{2})] = 8$. $X^8 - 2$ ist also noch das Minimalpolynom von α über $\mathbb{Q}(i\sqrt{2})$. Nach Tatsache 2 gibt es $\sigma_0, \ldots, \sigma_7$ in $Gal(K/\mathbb{Q}(i\sqrt{2}))$ mit $\sigma_k(\alpha) = \alpha\zeta_8^k$. Aus $\sigma_k(i\sqrt{2}) = i\sqrt{2}$ und $\sigma_k(\sqrt{2}) = \sigma(\alpha)^4$ folgt $\sigma_k(\zeta) = \zeta$, falls $2 \mid k$ und $\sigma_k(\zeta) = \zeta^3$, falls $2 \nmid k$. Damit kann man $\sigma_k^2(\alpha)$ und $\sigma_k\sigma_l(\alpha)$ explizit berechnen für alle k, l. Man sieht dann, dass $\sigma_4^2 = id, \sigma_1^2 = \sigma_2^2 = \sigma_3^2 = \sigma_4 = \sigma_1\sigma_2\sigma_3$, $\sigma_1\sigma_4 = \sigma_5, \sigma_2\sigma_4 = \sigma_6, \sigma_3\sigma_4 = \sigma_7$. Das entspricht der Definition von Q_8 in Aufgabe 10.4 (mit $-1 := \sigma_4, i := \sigma_1, j := \sigma_2, k := \sigma_3$).