
Übungen zur Vorlesung *Algebra I*
Blatt 13 – Musterlösung

Hinweis: Dies ist ein freiwilliges Zusatzblatt, welches weder korrigiert noch besprochen wird, für die Vorbereitung auf die Klausur jedoch hilfreich ist.

Aufgabe 13.1. (Multiplikativität des Gruppenindex)

Seien G, H, K Gruppen, für die $K \leq H \leq G$ gilt und für welche die Gruppenindizes $[G : H]$ und $[H : K]$ endlich sind.

Behauptung: $[G : K]$ ist endlich ist und es gilt

$$[G : K] = [G : H][H : K].$$

Beweis: Wir haben:

- $[G : K] = |\{gK \mid g \in G\}|$,
- $[G : H] = |\{gH \mid g \in G\}|$,
- $[H : K] = |\{hK \mid h \in H\}|$.

Betrachte die Abbildung

$$\varphi: \{gK \mid g \in G\} \rightarrow \{gH \mid g \in G\},$$

mit der Abbildungsvorschrift $\varphi(gK) = gH$ für $g \in G$. Wir zeigen, dass φ eine wohldefinierte surjektive Abbildung ist:

- Wohldefiniiertheit:

– $\text{Im}(\varphi) \subseteq \{gH \mid g \in G\}$: Klar.

- Vertreterunabhängigkeit:

Seien $g_1, g_2 \in G$ mit $g_1K = g_2K$. Zu zeigen: $\varphi(g_1K) = \varphi(g_2K)$.

Wegen Proposition 15.7(2) gilt $g_1^{-1}g_2 \in K$. Da $K \leq H$, gilt also insbesondere $g_1^{-1}g_2 \in H$. Erneutes Anwenden von Proposition 15.7(2) ergibt damit $\varphi(g_1K) = g_1H = g_2H = \varphi(g_2K)$.

- Surjektivität: Für $g \in G$ gilt $\varphi(gK) = gH$.

Wir zeigen nun, dass für jedes $g \in G$ das Urbild $\varphi^{-1}(gH)$ die Kardinalität $[H : K]$ hat. Daraus folgt letztlich die Behauptung. Sei also $g \in G$. Wir bemerken zunächst, dass

$$\varphi^{-1}(gH) = \{g'K \mid g' \in G, g'H = gH\},$$

und wir erinnern uns, dass die Bedingung $gH = g'H$ nach Proposition 15.7(2) äquivalent ist zu $g^{-1}g' \in H$. Nun betrachten wir die Abbildung

$$\psi: \varphi^{-1}(gH) \rightarrow \{hK \mid h \in H\}$$

mit der Abbildungsvorschrift $\psi(g'K) = g^{-1}g'K$ für $g' \in G$ mit $g'K \in \varphi^{-1}(gH)$ bzw. mit $g'H = gH$. Wir zeigen, dass ψ eine wohldefinierte Bijektion ist:

- Wohldefiniertheit:

$$- \text{Im}(\psi) \subseteq \{hK \mid h \in H\}:$$

Sei $g' \in G$ mit $g'K \in \varphi^{-1}(gH)$ bzw. mit $g'H = gH$. Nach Proposition 15.7(2) gilt $g^{-1}g' \in H$ und folglich

$$\psi(g'K) = g^{-1}g'K = \underbrace{(g^{-1}g')}_{\in H}K \in \{hK \mid h \in H\}.$$

- Vertreterunabhängigkeit:

Seien $g', g'' \in G$ mit $g'K, g''K \in \varphi^{-1}(gH)$ bzw. mit $g'H = g''H = gH$. Gilt $g'K = g''K$, so ergibt die Multiplikation von links mit g^{-1} , dass auch $\psi(g'K) = g^{-1}g'K = g^{-1}g''K = \psi(g''K)$ gilt.

- Injektivität:

Seien $g', g'' \in G$ mit $g'K, g''K \in \varphi^{-1}(gH)$ bzw. mit $g'H = g''H = gH$, und gelte $\psi(g'K) = \psi(g''K)$. Wegen $g^{-1}g'K = g^{-1}g''K$ ergibt die Multiplikation von links mit g , dass auch $g'K = gg^{-1}g'K = gg^{-1}g''K = g''K$ gilt.

- Surjektivität:

Sei $h \in H$. Setze $g' = gh \in G$. Es gilt $g'H = ghH = gH$, also $g'K \in \varphi^{-1}(gH)$. Wir erhalten außerdem $\psi(g'K) = g^{-1}g'K = g^{-1}ghK = hK$.

Wir haben also eine surjektive Abbildung φ von $\{gK \mid g \in G\}$ in die nach Voraussetzung endliche Menge $\{gH \mid g \in G\}$ und für jedes Urbild eines Elements unter dieser Abbildung eine Bijektion ψ zu der nach Voraussetzung endlichen Menge $\{hK \mid h \in H\}$. Ersteres ergibt den Faktor $[G : H]$ und letzteres den Faktor $[H : K]$. Insgesamt erhalten wir

$$[G : K] = [G : H][H : K].$$

Insbesondere ist auch der Gruppenindex $[G : K]$ endlich. □

Bemerkung: Noch formaler könnte eine Bijektion

$$\sigma: \{gK \mid g \in G\} \rightarrow \{gH \mid g \in G\} \times \{hK \mid h \in H\}$$

konstruiert werden. Damit erhält man ebenfalls

$$\begin{aligned} [G : K] &= |\{gK \mid g \in G\}| \\ &= |\{gH \mid g \in G\} \times \{hK \mid h \in H\}| \\ &= |\{gH \mid g \in G\}| \cdot |\{hK \mid h \in H\}| \\ &= [G : H][H : K]. \end{aligned}$$

Aufgabe 13.2. (Galoiserweiterungen)

Seien F , K und E Körper mit $F \subseteq K \subseteq E$.

Behauptung:

- (i) Falls E/F eine normale Erweiterung ist, dann ist auch E/K eine normale Erweiterung.
- (ii) Falls E/F eine separable Erweiterung ist, dann ist auch E/K eine separable Erweiterung.
- (iii) Falls E/F eine Galoiserweiterung ist, dann ist auch E/K eine Galoiserweiterung.
- (iv) Falls E/F eine Galoiserweiterung ist und $\text{Gal}(E/K) \trianglelefteq \text{Gal}(E/F)$ gilt, dann ist K/F eine Galoiserweiterung.

Beweis:

- (i) Bemerke zunächst, dass jede normale Körpererweiterung algebraisch ist. Sei nun E/F normal. Dann ist E der Zerfällungskörper einer Menge $\mathcal{E} \subseteq F[x]$. Wegen $F[x] \subseteq K[x]$, ist E insbesondere der Zerfällungskörper einer Menge $\mathcal{E} \subseteq K[x]$. Also ist auch E/K normal.
- (ii) Bemerke zunächst, dass jede separable Körpererweiterung algebraisch ist. Sei nun E/F separabel und sei $\alpha \in E$. Dann ist das Minimalpolynom $m_{\alpha,F}(x)$ separabel. Wegen $m_{\alpha,F}(\alpha) = 0$ wissen wir nach Proposition 10.3, dass das Minimalpolynom $m_{\alpha,K}(x)$ das Polynom $m_{\alpha,F}(x)$ in $K[x]$ teilt. Folglich muss auch das Minimalpolynom $m_{\alpha,K}(x)$ separabel sein, denn jede mehrfache Nullstelle von $m_{\alpha,K}(x)$ wäre auch eine mehrfache Nullstelle von $m_{\alpha,F}(x)$.
- (iii) Sei E/F eine Galoiserweiterung. Dann ist E/F endlich, normal und separabel. Nach (i) und (ii) ist E/K ebenfalls normal und separabel. Nach Satz 10.11 gilt $\infty > [E : F] = [E : K][K : F]$. Also muss auch E/K endlich sein. Dies zeigt, dass E/K eine Galoiserweiterung ist.
- (iv) Sei E/F eine Galoiserweiterung und gelte $\text{Gal}(E/K) \trianglelefteq \text{Gal}(E/F)$. Zu zeigen: K/F ist eine Galoiserweiterung.

- K/F ist endlich:
Nach Satz 10.11 gilt $[E : F] = [E : K][K : F]$. Als Galoisweiterung ist E/F endlich, es gilt also $[E : F] < \infty$. Insbesondere muss auch $[K : F] < \infty$ gelten.
- K/F ist separabel:
Sei $\alpha \in K \subseteq E$. Nach (ii) ist E/K eine Galoisweiterung, also insbesondere separabel. Daher ist auch das Minimalpolynom $m_{\alpha,F}(x)$ separabel.
- K/F ist normal:
Setze $H := \text{Gal}(E/K)$ und $G := \text{Gal}(E/F)$. Da E/K nach (ii) eine Galoisweiterung ist, gilt $\text{Inv}(H) = \text{Inv}(\text{Gal}(E/K)) = K$ nach Satz 24.3(a). Aus $H \trianglelefteq G$ folgt außerdem mit Satz 24.5(iii), dass $\text{Inv}(H)/F$ normal ist. Somit ist K/F normal.

□

Hilfsresultat (*).

Sei E/L eine Galoisweiterung und $\alpha \in E$ mit $E = L(\alpha)$ (d.h. α ist primitives Element). Dann existiert zu jeder Nullstelle $\beta \in E$ von $m_{\alpha,L}(x)$ ein *eindeutiger* L -Automorphismus σ_β von E mit $\sigma_\beta(\alpha) = \beta$. Insbesondere ist die Abbildung

$$\psi: \{\beta \in E \mid m_{\alpha,L}(\beta) = 0\} \rightarrow \text{Gal}(E/L), \beta \rightarrow \sigma_\beta$$

bijektiv.

Beweis:

- Existenz von σ_β :
Folgt aus Satz 9.14 mit $F = F' = L$, $K = K' = E$, $\varphi = \text{id}_L$ und $p(x) = m_{\alpha,L}(x)$.
- Eindeutigkeit von σ_β :
Sei σ_β ein L -Automorphismus von E mit $\sigma_\beta(\alpha) = \beta$ und sei $\gamma \in E = L(\alpha)$. Nach Aufgabe 7.1(a) gibt es $p(x) \in F[x]$ mit $\gamma = p(\alpha)$. Nun folgt

$$\sigma_\beta(\gamma) = \sigma_\beta(p(\alpha)) = p(\sigma_\beta(\alpha)) = p(\beta),$$

da $\sigma_\beta|_L = \text{id}_L$ und $\sigma_\beta(\alpha) = \beta$. Dies zeigt, dass σ_β durch die Eigenschaften $\sigma_\beta|_L = \text{id}_L$ und $\sigma_\beta(\alpha) = \beta$ eindeutig bestimmt ist.

- Die Wohldefiniertheit von ψ folgt aus der *eindeutigen* Wahl von σ_β .
- Injektivität von ψ :
Seien $\beta_1, \beta_2 \in E$ Nullstellen von $m_{\alpha,L}(x)$ mit $\sigma_{\beta_1} = \sigma_{\beta_2}$. Dann gilt

$$\beta_1 = \sigma_{\beta_1}(\alpha) = \sigma_{\beta_2}(\alpha) = \beta_2.$$

- Surjektivität von ψ :

Sei $\sigma \in \text{Gal}(E/L)$. Setze $\beta = \sigma(\alpha) \in E$. Dann ist β eine Nullstelle von $m_{\alpha,L}(x)$, denn $\sigma|_L = \text{id}$ impliziert

$$m_{\alpha,L}(\beta) = m_{\alpha,L}(\sigma(\alpha)) = \sigma(m_{\alpha,L}(\alpha)) = \sigma(0) = 0$$

(in der Tat „kommutiert“ σ hier mit $m_{\alpha,L}(x)$, denn σ fixiert L und die Koeffizienten von $m_{\alpha,L}(x)$ liegen in L). Weiter folgt aus der Eindeutigkeit von σ_β , dass $\psi(\beta) = \sigma_\beta = \sigma$.

□

Aufgabe 13.3. (Galois-Korrespondenz I)

Sei $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Zeigen Sie, dass $K/\mathbb{Q}$ eine Galoiserweiterung ist.

Bemerkung: Nach Aufgabe 6.3(b) gilt $K = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

(i) **Behauptung:** $K/\mathbb{Q}$ ist eine Galoiserweiterung.

Beweis:

Nach Satz 24.3 genügt es zu zeigen, dass K der Zerfällungskörper eines separablen Polynoms $p(x) \in \mathbb{Q}[x]$ ist. Wir zeigen, dass K der Zerfällungskörper des separablen Polynoms $p(x) = (x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x]$ ist:

- $p(x)$ ist separabel:
Das Polynom hat die vier verschiedenen einfachen Nullstellen $\pm\sqrt{2}, \pm\sqrt{3}$.
- K ist der Zerfällungskörper von $p(x)$:
Die Nullstellen von $p(x)$ in $\mathbb{C}$ sind $\pm\sqrt{2}$ und $\pm\sqrt{3}$. Diese sind schon alle in K enthalten. Weiterhin gilt $K = \mathbb{Q}(\sqrt{2}, -\sqrt{2}, \sqrt{3}, -\sqrt{3})$, weshalb K schon der Zerfällungskörper von $p(x)$ ist.

□

(ii) Bestimmen Sie $\text{Gal}(K/\mathbb{Q})$.

Lösung: Wir gehen Schritt für Schritt vor.

(1) Zähle die Elemente in $\text{Gal}(K/\mathbb{Q})$:

Wir haben

$$[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{3})]}_{=2} \underbrace{[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]}_{=2} = 2 \cdot 2 = 4.$$

Tatsächlich haben wir $m_{\sqrt{2}, \mathbb{Q}(\sqrt{3})} = x^2 - 2 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\sqrt{3})[x]$ sowie $m_{\sqrt{3}, \mathbb{Q}} = x^2 - 3 \in \mathbb{Q}[x]$, denn beide Polynome sind irreduzibel (wende beispielsweise Eisenstein mit 2 bzw. 3 sowie Lemma von Gauß an). Aus Lemma 23.5 folgt

$$|\text{Gal}(K/\mathbb{Q})| = [K : \mathbb{Q}] = 4.$$

(2) Betrachte geeignete Untergruppen:

(Problem: Es werden zwei Elemente adjungiert, nur eins wäre leichter.)

Betrachte zunächst nur die Teilgruppen $\text{Gal}(K/\mathbb{Q}(\sqrt{2}))$ und $\text{Gal}(K/\mathbb{Q}(\sqrt{3}))$ von $\text{Gal}(K/\mathbb{Q})$ (vgl. Proposition 23.4).

(3) Wende Hilfsresultat (*) an:

- Sei $\tau \in \text{Gal}(K/\mathbb{Q}(\sqrt{2}))$ der eindeutige $\mathbb{Q}(\sqrt{2})$ -Automorphismus von K mit $\tau(\sqrt{3}) = -\sqrt{3}$.
- Sei $\sigma \in \text{Gal}(K/\mathbb{Q}(\sqrt{3}))$ der eindeutige $\mathbb{Q}(\sqrt{3})$ -Automorphismus von K mit $\sigma(\sqrt{2}) = -\sqrt{2}$.

(4) Erstelle Verknüpfungstabelle, um genügend verschiedene Elemente zu finden:

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

Wir haben also 4 verschiedene Elemente $\text{id}, \sigma, \tau, \sigma\tau$ in der 4-elementigen Gruppe $\text{Gal}(K/\mathbb{Q})$ gefunden. Somit erhalten wir

$$\text{Gal}(K/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \sigma\tau\}.$$

(5) Vergleiche ggf. mit bekannten Gruppen:

Aus der obigen Verknüpfungstabelle wird klar, dass

$$\text{Gal}(K/\mathbb{Q}) = \{\text{id}, \sigma, \tau, \sigma\tau\} \simeq C_2 \times C_2 = V_4 \text{ (Kleinsche Vierergruppe).}$$

□

(iii) Geben Sie alle Zwischenkörper der Erweiterung $K/\mathbb{Q}$ an.

Lösung: Ziel ist es, den Hauptsatz der Galois-Theorie (HGT) anzuwenden.

- Bestimme die UG von $\text{Gal}(K/\mathbb{Q})$:
 - $H_1 = \{\text{id}\}$
 - $H_2 = \{\text{id}, \sigma\} = \langle \sigma \rangle$
 - $H_3 = \{\text{id}, \tau\} = \langle \tau \rangle$
 - $H_4 = \{\text{id}, \sigma\tau\} = \langle \sigma\tau \rangle$
 - $H_5 = \{\text{id}, \sigma, \tau, \sigma\tau\} = \text{Gal}(K/\mathbb{Q})$

Prüfe, dass dies in der Tat alle UG sind (Gruppeneigenschaften).

- Bestimme die entsprechenden Fixkörper:
 - Offensichtlich gilt $K_1 := \text{Inv}(H_1) = K$.

– Beh.: $K_2 := \text{Inv}(H_2) = \mathbb{Q}(\sqrt{3})$.

Bew.: Da $\sigma \in H_2$ das Element $\sqrt{3}$ fixiert, gilt $\mathbb{Q}(\sqrt{3}) \subseteq \text{Inv}(H_2)$. Ferner gilt

$$[\text{Inv}(H_2) : \mathbb{Q}] \stackrel{\text{HGT}}{=} [\text{Gal}(K/\mathbb{Q}) : H_2] \stackrel{\text{Lagrange}}{=} \frac{4}{2} = 2 = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$$

und somit schließlich $\mathbb{Q}(\sqrt{3}) = \text{Inv}(H_2)$. $\diamond$

– Beh.: $K_3 := \text{Inv}(H_3) = \mathbb{Q}(\sqrt{2})$.

Bew.: Da $\tau \in H_3$ das Element $\sqrt{2}$ fixiert, gilt $\mathbb{Q}(\sqrt{2}) \subseteq \text{Inv}(H_3)$. Ferner gilt

$$[\text{Inv}(H_3) : \mathbb{Q}] \stackrel{\text{HGT}}{=} [\text{Gal}(K/\mathbb{Q}) : H_3] \stackrel{\text{Lagrange}}{=} \frac{4}{2} = 2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$$

und somit schließlich $\mathbb{Q}(\sqrt{2}) = \text{Inv}(H_3)$. $\diamond$

– Beh.: $K_4 := \text{Inv}(H_4) = \mathbb{Q}(\sqrt{2}\sqrt{3})$.

Bew.: Da $\sigma\tau \in H_4$ das Element $\sqrt{2}\sqrt{3}$ fixiert (Zwischenrechnung: $\sigma\tau(\sqrt{2}\sqrt{3}) = \sigma(\sqrt{2}(-\sqrt{3})) = (-\sqrt{2})(-\sqrt{3}) = \sqrt{2}\sqrt{3}$), gilt $\mathbb{Q}(\sqrt{2}\sqrt{3}) \subseteq \text{Inv}(H_4)$. Ferner gilt

$$[\text{Inv}(H_4) : \mathbb{Q}] \stackrel{\text{HGT}}{=} [\text{Gal}(K/\mathbb{Q}) : H_4] \stackrel{\text{Lagrange}}{=} \frac{4}{2} = 2 = [\mathbb{Q}(\sqrt{2}\sqrt{3}) : \mathbb{Q}]$$

und somit schließlich $\mathbb{Q}(\sqrt{2}\sqrt{3}) = \text{Inv}(H_4)$. $\diamond$

– Nach Satz 24.3 gilt $K_5 := \text{Inv}(H_5) = \mathbb{Q}$, da $K/\mathbb{Q}$ nach (i) eine Galoiserweiterung ist.

Zwischenkörper der Erweiterung $K/\mathbb{Q}$:

$$K_1 = K = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}), K_2 = \mathbb{Q}(\sqrt{3}), K_3 = \mathbb{Q}(\sqrt{2}), K_4 = \mathbb{Q}(\sqrt{2}\sqrt{3}) = \mathbb{Q}(\sqrt{2 \cdot 3}) = \mathbb{Q}(\sqrt{6}), K_5 = \mathbb{Q}.$$

□

Aufgabe 13.4. (Galois-Korrespondenz II)

Sei $f(x) = x^4 - 2 \in \mathbb{Q}[x]$ und sei L ein Zerfällungskörper von f .

(i) **Behauptung:** Es gilt $\text{Gal}(L/\mathbb{Q}) \cong D_4$.

Beweis: Was steckt dahinter?

– Bestimmen Sie $\text{Gal}(L/\mathbb{Q})$ (vgl. Aufgabe 13.3(ii)).

(0) Verstehe L :

L wird als Zerfällungskörper von f durch die Nullstellen von f erzeugt. Diese sind $\alpha, -\alpha, i\alpha, -i\alpha$, wobei $\alpha = \sqrt[4]{2}$. Also erhalten wir

$$L = \mathbb{Q}(\pm\alpha, \pm i\alpha) = \mathbb{Q}(\alpha, i\alpha) = \mathbb{Q}(\alpha, i).$$

- (1) Zähle die Elemente in $\text{Gal}(L/\mathbb{Q})$:

Da $f(x)$ irreduzibel ist (wende beispielsweise Eisenstein mit 2 sowie Lemma von Gauß an), ist $f(x) = m_{\alpha, \mathbb{Q}}(x)$ und somit $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg(f) = 4$. Zudem ist $g(x) = x^2 + 1 \in \mathbb{Q}[x] \subseteq \mathbb{Q}(\alpha)[x]$ irreduzibel, da $\deg(g) = 2$, $\mathbb{Q}(\alpha) \subseteq \mathbb{R}$ und $g(x)$ keine Nullstelle in $\mathbb{R}$ hat. Somit ist $g(x) = m_{i, \mathbb{Q}(\alpha)}(x)$ und folglich

$$\underbrace{[\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)]}_{= [\mathbb{Q}(\alpha)(i) : \mathbb{Q}(\alpha)]} = \deg(g) = 2.$$

Insgesamt erhalten wir

$$[L : \mathbb{Q}] = [\mathbb{Q}(\alpha, i) : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 4 \cdot 2 = 8.$$

Aus Lemma 23.5 folgt

$$|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 8.$$

- (2) Betrachte geeignete Untergruppen:

(Problem: Es werden zwei Elemente adjungiert, nur eins wäre leichter.)

Betrachte zunächst nur die Teilgruppen $\text{Gal}(L/\mathbb{Q}(\alpha))$ und $\text{Gal}(L/\mathbb{Q}(i))$ von $\text{Gal}(L/\mathbb{Q})$ (vgl. Proposition 23.4).

- (3) Wende Hilfsresultat (*) an:

- Bemerke zunächst, dass $L = \mathbb{Q}(i)(\alpha)$ und

$$4 = [L : \mathbb{Q}] = [\mathbb{Q}(i)(\alpha) : \mathbb{Q}(i)] \underbrace{[\mathbb{Q}(i) : \mathbb{Q}]}_{=2}.$$

Dies impliziert, dass $[L : \mathbb{Q}(i)] = 4$. Insbesondere ist $m_{\alpha, \mathbb{Q}(i)}(x) = f(x)$. Sei nun $\sigma \in \text{Gal}(L/\mathbb{Q}(i))$ der eindeutige $\mathbb{Q}(i)$ -Automorphismus von L mit $\sigma(\alpha) = i\alpha$.

- Wir wissen bereits, dass $m_{i, \mathbb{Q}(\alpha)}(x) = g(x) = x^2 - 1$. Dieses Polynom hat die Nullstellen i und $-i$. Sei $\tau \in \text{Gal}(L/\mathbb{Q}(\alpha))$ der eindeutige $\mathbb{Q}(\alpha)$ -Automorphismus von L mit $\tau(i) = -i$.

- (4) Erstelle Verknüpfungstabelle, um genügend verschiedene Elemente zu finden:

	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	$i\alpha$	$-\alpha$	$-i\alpha$	$-i\alpha$	$-\alpha$	$i\alpha$

Wir haben also 8 verschiedene Elemente $\text{id}, \tau, \sigma, \sigma^2, \sigma^3, \tau\sigma, \tau\sigma^2, \tau\sigma^3$ in der 8-elementigen Gruppe $\text{Gal}(L/\mathbb{Q})$ gefunden. Somit erhalten wir

$$\text{Gal}(L/\mathbb{Q}) = \{\text{id}, \tau, \sigma, \sigma^2, \sigma^3, \tau\sigma, \tau\sigma^2, \tau\sigma^3\} = \langle \tau, \sigma \rangle.$$

- (5) Vergleiche ggf. mit bekannten Gruppen:

Aus der obigen Verknüpfungstabelle wird klar, dass $\text{Gal}(L/\mathbb{Q}) = \langle \tau, \sigma \rangle \simeq D_4$. □

(ii) Beschreiben Sie die 10 verschiedenen Untergruppen von D_4 .

Lösung: Was steckt dahinter?

– Bestimmen Sie die UG von $\text{Gal}(L/\mathbb{Q})$ (vgl. Aufgabe 13.3(iii)).

Nach Lagrange haben die UG von D_4 wegen $|D_4| = 8$ die Ordnungen 1, 2, 4, 8.

Setze $H_1 := \{\text{id}\}$ und $H_{10} := G := \text{Gal}(L/\mathbb{Q}) = \langle \sigma, \tau \rangle$.

- Welche Elemente in G haben die Ordnung 2?

$\tau, \sigma^2, \tau\sigma, \tau\sigma^2, \tau\sigma^3$ (vgl. Verknüpfungstabelle)

Diese erzeugen UG der Ordnung 2:

- $H_2 := \{\text{id}, \tau\} = \langle \tau \rangle$
- $H_3 := \{\text{id}, \sigma^2\} = \langle \sigma^2 \rangle$
- $H_4 := \{\text{id}, \tau\sigma\} = \langle \tau\sigma \rangle$
- $H_5 := \{\text{id}, \tau\sigma^2\} = \langle \tau\sigma^2 \rangle$
- $H_6 := \{\text{id}, \tau\sigma^3\} = \langle \tau\sigma^3 \rangle$

- Welche Elemente in G haben die Ordnung 4?

σ, σ^3 (vgl. Verknüpfungstabelle)

Diese erzeugen UG der Ordnung 4:

- $H_7 := \{\text{id}, \sigma, \sigma^2, \sigma^3\} = \langle \sigma \rangle = \langle \sigma^3 \rangle$

- Wie bekomme ich weitere UG der Ordnung $4 = 2 \cdot 2$?

Durch zwei Elemente mit Ordnung jeweils 2:

- $H_8 := \langle \tau, \sigma^2 \rangle = \{\text{id}, \tau, \sigma^2, \tau\sigma^2\}$
- $H_9 := \langle \tau\sigma, \sigma^2 \rangle = \{\text{id}, \tau\sigma, \sigma^2, \tau\sigma^2\}$

Bemerke: $\langle \tau, \tau\sigma \rangle = \langle \tau, \tau\sigma^3 \rangle = \langle \tau\sigma, \tau\sigma^2 \rangle = \langle \tau\sigma^2, \tau\sigma^3 \rangle = G = H_{10}$.

Somit wurden alle 10 UG von $\text{Gal}(L/\mathbb{Q}) \simeq D_4$ gefunden. □

(iii) Bestimmen Sie die Zwischenkörper der Erweiterung $L/\mathbb{Q}$ und geben Sie für jeden Zwischenkörper F ein primitives Element für F über $\mathbb{Q}$ an.

Lösung: Ziel ist es, den HGT anzuwenden (vgl. Aufgabe 13.3(iii)).

Bemerke zunächst, dass $f(x)$ nach Korollar 13.8 separabel ist, da $f(x)$ und $Df(x) = 4x^3$ offensichtlich teilerfremd sind. Somit ist $L/\mathbb{Q}$ nach Satz 24.3 eine Galoiserweiterung, weil L der Zerfällungskörper von f ist.

- Die UG von $\text{Gal}(L/\mathbb{Q})$ haben wir bereits in (ii) bestimmt.
- Bestimme die entsprechenden Fixkörper:
 - Offensichtlich gilt $K_1 := \text{Inv}(H_1) = L$.
 - Nach Satz 24.3 gilt $K_{10} := \text{Inv}(H_{10}) = \mathbb{Q}$, da $L/\mathbb{Q}$ eine Galoiserweiterung ist.

– Beh.: $K_2 := \text{Inv}(H_2) = \mathbb{Q}(\alpha)$.

Bew.: Da $\tau \in H_2$ das Element α fixiert, gilt $\mathbb{Q}(\alpha) \subseteq \text{Inv}(H_2)$. Ferner gilt $|\text{Gal}(L/\mathbb{Q})| = [L : \mathbb{Q}] = 8$ nach Lemma 23.5, was

$$[\text{Inv}(H_2) : \mathbb{Q}] \stackrel{\text{HGT}}{=} [\text{Gal}(L/\mathbb{Q}) : H_2] \stackrel{\text{Lagrange}}{=} \frac{8}{2} = 4 = [\mathbb{Q}(\alpha) : \mathbb{Q}]$$

impliziert, und somit schließlich $\mathbb{Q}(\sqrt{3}) = \text{Inv}(H_2)$. ◇

Analog zeigt man:

- $K_3 := \text{Inv}(H_3) = \mathbb{Q}(i + \alpha^2)$
- $K_4 := \text{Inv}(H_4) = \mathbb{Q}(\alpha - i\alpha)$
- $K_5 := \text{Inv}(H_5) = \mathbb{Q}(i\alpha)$
- $K_6 := \text{Inv}(H_6) = \mathbb{Q}(\alpha + i\alpha)$
- $K_7 := \text{Inv}(H_7) = \mathbb{Q}(i)$
- $K_8 := \text{Inv}(H_8) = \mathbb{Q}(\alpha^2)$
- $K_9 := \text{Inv}(H_9) = \mathbb{Q}(i\alpha^2)$

□

Viel Erfolg bei der Klausurvorbereitung!

