Drei Beispiele zum Hauptsatz der GALOIS–Theorie

(12.8) BEISPIEL: Seien $\alpha := e^{\frac{2\pi i}{5}} \in \mathbb{C}$ und $L := \mathbb{Q}(\alpha)$. Die Galois–Gruppe $G := \mathrm{Gal}(L:\mathbb{Q})$ wird in Aufgabe 38a berechnet. $f := T^4 + T^3 + T^2 + T + 1 \in \mathbb{Q}[T]$ ist das Minimalpolynom von α über $\mathbb{Q}$ mit $\mathrm{Null}_L(f) = \{\alpha, \alpha^2, \alpha^3, \alpha^4\}$. Daher besteht G nach (10.6) aus den 4 $\mathbb{Q}$–Automorphismen $\sigma_1, \sigma_2, \sigma_3, \sigma_4$, die durch ihre Werte für α eindeutig festgelegt sind:

σ	$\sigma(\alpha)$	$\mathrm{ord}(\sigma)$
σ_1	α	1
σ_2	α^2	4
σ_3	α^3	4
σ_4	α^4	2

Wegen $[L:\mathbb{Q}] = [\mathbb{Q}(\alpha):\mathbb{Q}] = \mathrm{grad}(f) = 4 = |G|$ ist $L:\mathbb{Q}$ eine Galois–Erweiterung. Da G ein Element der Ordnung 4 enthält, ist G zyklisch und daher isomorph zu $\mathbb{Z}_4$. Nach dem Satz von Lagrange kann eine Untergruppe $U \leq (G, \circ)$ nur die Ordnung 1,2 oder 4 haben (dies sind die positiven Teiler von 4).

$|U| = 1 \implies U = \{\sigma_1\}$ ($\sigma_1 = \mathrm{id}_L$ ist das neutrale Element in G).

$|U| = 4 \implies U = G$.

$|U| = 2 \in \mathbb{P} \implies U$ ist zyklisch und wird von einem Element der Ordnung 2 erzeugt. Da σ_4 das einzige Element der Ordnung 2 ist, gibt es auch genau eine Untergruppe der Ordnung 2, nämlich $U = <\sigma_4> = \{\sigma_1, \sigma_4\}$.

Die Galois–Gruppe G besitzt also nur eine echte Untergruppe. Da $L:\mathbb{Q}$ eine Galois–Erweiterung ist, gibt es nach dem Hauptsatz der Galois–Theorie auch nur einen echten Zwischenkörper.

Untergruppenverband von G	Zwischenkörperverband von $L:\mathbb{Q}$
G	$L^G = \mathbb{Q}$
$\vert$	$\vert$
$<\sigma_4>$	$L^{<\sigma_4>} = \mathbb{Q}(\sqrt{5})$ $*)$
$\vert$	$\vert$
$<\sigma_1>$	$L^{<\sigma_1>} = L$

Nachweis von *): Sei $U := <\sigma_4>$. Aus (11.6a) folgt $[L^U:\mathbb{Q}] = \dfrac{[L:\mathbb{Q}]}{|U|} = \dfrac{4}{2} = 2$. Nun ist $\beta := \alpha + \alpha^4 \overset{**)}{=} \dfrac{1}{2}(\sqrt{5} - 1) \notin \mathbb{Q}$ ein Fixelement von σ_4; denn

$$\sigma_4(\beta) = \sigma_4(\alpha + \alpha^4) = \sigma_4(\alpha) + \sigma_4(\alpha^4) = \alpha^4 + \alpha = \beta\,.$$

Damit gilt $\beta \in L^U$ und $\mathbb{Q} \subset \mathbb{Q}(\beta) \subseteq L^U$. Aus Gradgründen folgt $L^U = \mathbb{Q}(\beta)$. Außerdem gilt wegen **) $\mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{5})$. Folglich $L^U = \mathbb{Q}(\sqrt{5})$.

Nachweis von **): $\beta = \alpha + \alpha^4 = \alpha + \overline{\alpha} = 2 \cdot \mathrm{Re}(\alpha) = 2 \cdot \cos\left(\frac{2\pi}{5}\right) = 2 \cdot \frac{1}{4}(\sqrt{5}-1)$ (s.Aufg. 4) .

Da die Galois–Gruppe abelsch ist, ist nach (12.7) $\mathbb{Q}(\sqrt{5}) : \mathbb{Q}$ eine Galois–Erweiterung , was natürlich hier einfacher aus Aufgabe 46 folgt.

(12.9) BEISPIEL: Sei $L := \mathbb{Q}(\sqrt{3}, \sqrt{5})$. Nach Aufgabe 38b) gilt $L = \mathbb{Q}(\alpha)$ mit $\alpha := \sqrt{3} + \sqrt{5}$, und $f := T^4 - 16T^2 + 4 \in \mathbb{Q}[T]$ ist das Minimalpolynom von $\alpha/\mathbb{Q}$. Sei $\beta := -\sqrt{3} + \sqrt{5}$. Dann ist $N = \{\alpha, -\alpha, \beta, -\beta\}$ die Nullstellenmenge von f in L, so daß nach (10.6) gilt $|\mathrm{Gal}(L : \mathbb{Q})| = 4 = [L : \mathbb{Q}]$. Folglich ist $L : \mathbb{Q}$ eine Galois–Erweiterung . Die 4 $\mathbb{Q}$–Automorphismen $\sigma_1, \sigma_2, \sigma_3, \sigma_4$ von L sind durch ihre Werte für α eindeutig festgelegt:

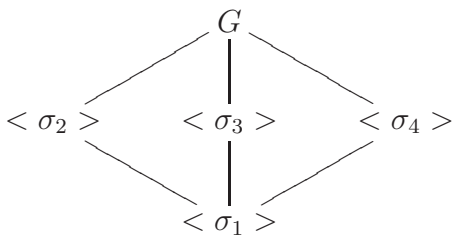
σ	$\sigma(\alpha)$	$\sigma(\sqrt{3})$	$\sigma(\sqrt{5})$	$\mathrm{ord}(\sigma)$
σ_1	α	$\sqrt{3}$	$\sqrt{5}$	1
σ_2	$-\alpha$	$-\sqrt{3}$	$-\sqrt{5}$	2
σ_3	β	$-\sqrt{3}$	$\sqrt{5}$	2
σ_4	$-\beta$	$\sqrt{3}$	$-\sqrt{5}$	2

Damit ist die Galois–Gruppe$G$ von $L : \mathbb{Q}$ bekannt. Außer den Untergruppen $< \sigma_1 >$ und G kann es nur noch Untergruppen der Ordnung 2 geben. Eine solche Untergruppe $U \leq G$ wird von einem Element der Ordnung 2 erzeugt (davon gibt es genau 3 Stück), und für sie gilt wieder nach (11.6a) $[L^U : \mathbb{Q}] = \frac{[L : \mathbb{Q}]}{|U|} = \frac{4}{2} = 2$.

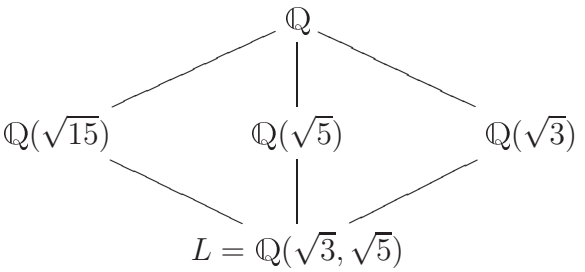
Sei $U =< \sigma_2 >$. Aus der Tabelle folgt: $\sigma_2(\sqrt{15}) = \sigma_2(\sqrt{3} \cdot \sqrt{5}) = (-\sqrt{3}) \cdot (-\sqrt{5}) = \sqrt{15}$, d.h. $\sqrt{15} \in L^U$. Aus $\mathbb{Q} \subset \mathbb{Q}(\sqrt{15}) \subseteq L^U$ folgt dann $L^U = \mathbb{Q}(\sqrt{15})$. Entsprechend erhält man

$$L^V = \mathbb{Q}(\sqrt{5}) \text{ für } V :=< \sigma_3 > \text{ und } L^W = \mathbb{Q}(\sqrt{3}) \text{ für } W :=< \sigma_4 >.$$

Da $L : \mathbb{Q}$ eine Galois–Erweiterung ist, sind dies auch die einzigen echten Zwischenkörper, da G genau 3 echte Untergruppen besitzt.



Untergruppenverband von G



Zwischenkörperverband von $L : \mathbb{Q}$

Da die Galois–Gruppe abelsch ist, ist nach (12.7) $E : \mathbb{Q}$ für jeden Zwischenkörper E von $L : \mathbb{Q}$ eine Galois–Erweiterung , was natürlich hier wieder einfacher aus Aufgabe 46 folgt.

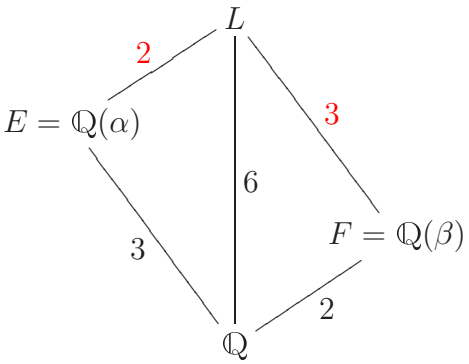
(12.10) BEISPIEL: Sei $L := \mathbb{Q}(\alpha, \beta) \subseteq \mathbb{C}$ mit $\alpha := \sqrt[3]{2}$ und $\beta := i\sqrt{3}$.

Die Galois–Gruppe von $L : \mathbb{Q}$ wurde bereits in den Übungen bestimmt. $f := T^3 - 2$ ist das Minimalpolynom von $\alpha/\mathbb{Q}$ und $g := T^2 + 3$ das Minimalpolynom von $\beta/\mathbb{Q}$. Damit gilt $\text{grad}_Q(\alpha) = 3$ und $\text{grad}_Q(\beta) = 2$. Nach Aufgabe 29 ist dann

$$[L : \mathbb{Q}] \;=\; 2 \cdot 3 \;=\; 6$$

Die Galoisgruppe $G := \text{Gal}(L : \mathbb{Q})$ hat dann höchstens 6 Elemente: $\underline{|G| \leq 6}$. Definiere:

$$E := \mathbb{Q}(\alpha) \quad \text{und} \quad F := \mathbb{Q}(\beta)$$



Aus $[E : \mathbb{Q}] = 3$ und $[F : \mathbb{Q}] = 2$ folgt mit dem Gradsatz $[L : E] = 2$ und $[L : F] = 3$

Es ist $L = E(\beta)$. Das Polynom $g = T^2 + 3 \in E[T]$ hat β als Nullstelle und ist wegen $[L : E] = 2$ das Minimalpolynom von β/E.

Es ist $L = F(\alpha)$. Das Polynom $f = T^3 - 2 \in F[T]$ hat α als Nullstelle und ist wegen $[L : F] = 3$ das Minimalpolynom von α/F.

Sei $V := \text{Gal}(L : E) \leq G$. Da $L = E(\beta)$ eine einfache Körpererweiterung von E ist, wird V durch die Nullstellen von g, die in L liegen, beschrieben. Diese sind β und $-\beta$. Also

$$V = \text{Gal}(L : E) \;=\; \{\text{id}_L, \tau\}$$

Dabei ist $\tau : L \longrightarrow L$ ein E–Automorphismus von L mit $\tau(\beta) = -\beta$. Insbesondere gilt $\tau(\alpha) = \alpha$ (da $\alpha \in E$) , $\tau(a) = a \;\; \forall\, a \in \mathbb{Q}$ und $\text{ord}(\beta) = 2$.

Sei $U := \text{Gal}(L : F) \leq G$. Da $L = F(\alpha)$ eine einfache Körpererweiterung von F ist, wird U durch die Nullstellen von f, die in L liegen, beschrieben. Mit $\varepsilon := \frac{1}{2}(\beta - 1) \in L$ sind dies $\alpha, \varepsilon\alpha, \varepsilon^2\alpha$. Es gilt nämlich $\varepsilon \in L$, $\varepsilon^2 = \overline{\varepsilon} \in L$ und $\varepsilon^3 = 1$ (d.h. ε ist eine dritte Einheitswurzel). Man rechnet nach: $f(\varepsilon\alpha) = 0$ und $f(\varepsilon^2\alpha) = 0$. Folglich enthält U genau 3 Elemente:

$$U := \text{Gal}(L : F) \;=\; \{\text{id}_L, \sigma_1, \sigma_2\}$$

Dabei sind $\sigma_j : L \longrightarrow L$ F–Automorphismen von L mit $\sigma_1(\alpha) = \varepsilon\alpha$, $\sigma_2(\alpha) = \varepsilon^2\alpha$. Außerdem gilt $\sigma_j(\beta) = \beta$ (da $\beta \in F$) und $\sigma_j(a) = a \;\; \forall\, a \in \mathbb{Q}$. Wegen $|U| = 3$ ist U zyklisch und jedes Element $\neq \text{id}_L$ hat die Ordnung 3, und es gilt $\sigma_2 = \sigma_1^2$. Setze: $\underline{\sigma := \sigma_1}$.

$$V = \langle\tau\rangle \leq G \;\; (\text{ord}(\tau) = 2) \;\; , \;\; U = \langle\sigma\rangle \leq G \;\; (\text{ord}(\sigma) = 3)$$

Nach dem Satz von Lagrange sind 2 und 3 Teiler von $|G|$. Damit ist aber auch $6 = 2 \cdot 3$ ein Teiler von $|G|$, folglich $\underline{6 \leq |G|}$. Mit der obigen entgegengesetzten Ungleichung ergibt sich

$$|\mathrm{Gal}(L:\mathbb{Q})| \;=\; 6 \;=\; [L:\mathbb{Q}]$$

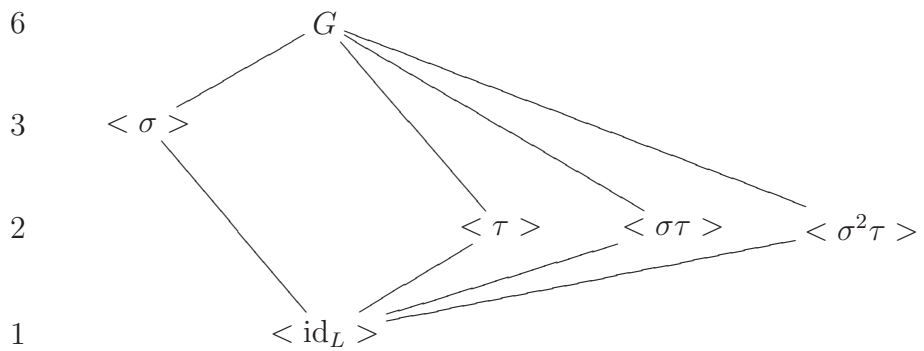
Damit ist $L:\mathbb{Q}$ eine **Galois–Erweiterung**. Eine nichtabelsche Gruppe der Ordnung 6 ist isomorph zur symmetrischen Gruppe S_3, eine abelsche Gruppe der Ordnung 6 ist isomorph zur zyklischen Gruppe $\mathbb{Z}_6$. Wir wollen uns nun überlegen, daß G nicht abelsch ist. Dazu berechnen wir:

$\tau(\varepsilon) = \frac{1}{2}(\tau(\beta) - 1) = \frac{1}{2}(-\beta - 1) = \overline{\varepsilon} = \varepsilon^2$. Es ergibt sich

$(\sigma \circ \tau)(\alpha) = \sigma(\alpha) = \varepsilon\alpha \;\;,\;\; (\tau \circ \sigma)(\alpha) = \tau(\varepsilon\alpha) = \tau(\varepsilon)\tau(\alpha) = \varepsilon^2\alpha$, d.h. $\underline{\sigma \circ \tau \neq \tau \circ \sigma}$. Also:

$$\boxed{G \cong S_3}$$

$G = \{\mathrm{id}_L, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\}$. Die Elemente σ und σ^2 haben die Ordnung 3, $\tau, \sigma\tau, \sigma^2\tau$ die Ordnung 2. Echte Untergruppen von G sind von der Ordnung 2 oder 3 , sind also zyklisch und werden von einem Element der Ordnung 2 bzw. 3 erzeugt. Deshalb gibt es 3 Untergruppen der Ordnung 2 und eine Untergruppe der Ordnung 3, die 2 Elemente der Ordnung 3 enthalten muß . Der **Untergruppenverband** von G sieht damit folgendermaßen aus:



Wir wollen nun alle Zwischenkörper von $L:\mathbb{Q}$ bestimmen. Da dies eine Galois–Erweiterung ist, müssen wir nur die Fixgruppen zu allen Untergruppen von G berechnen.

$\underline{L^G = \mathbb{Q}}$ und $\underline{L^{\langle \mathrm{id}_L \rangle} = L}$ ist klar.

Für eine beliebige Untergruppe $W \leq G$ gilt nach (11.6a)

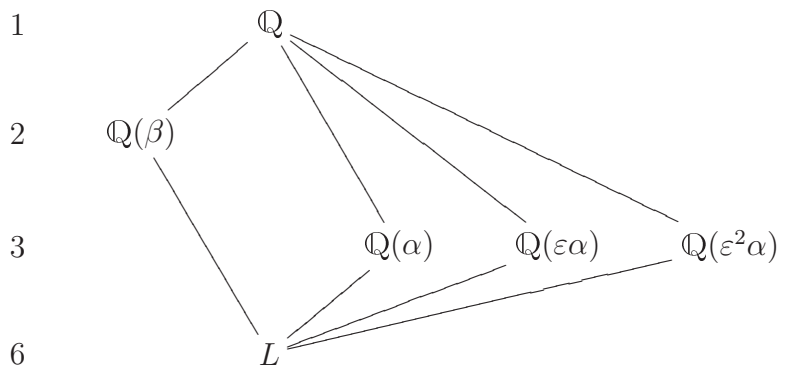
$$(\star) \qquad [L^W:\mathbb{Q}] \;=\; \frac{[L:\mathbb{Q}]}{|W|} \;=\; \frac{6}{|W|}$$

$\underline{U = \langle\sigma\rangle}$ $[L^U:\mathbb{Q}] = \dfrac{6}{3} = 2$, $\sigma(\beta) = \beta \;\Longrightarrow\; \beta \in \mathrm{Fix}(\sigma) = L^U \;\Longrightarrow\; F = \mathbb{Q}(\beta) \subseteq L^U$. Da beide Körper den Grad 2 über $\mathbb{Q}$ haben, folgt $\underline{L^U = \mathbb{Q}(\beta) = F}$.

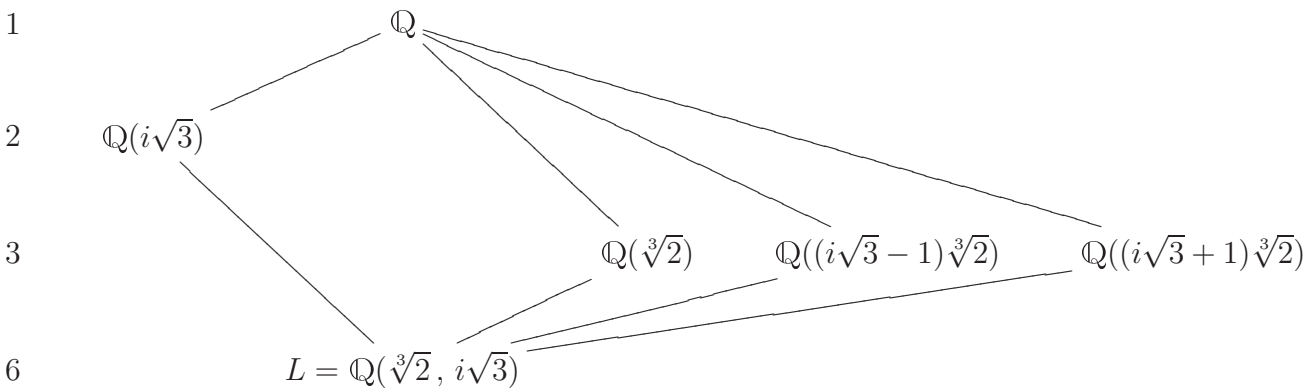
$\underline{V = \langle\tau\rangle}$ Nach $(\star)$ gilt $[L^V:\mathbb{Q}] = 3$. Wegen $\tau(\alpha) = \alpha$ ist $E = \mathbb{Q}(\alpha) \subseteq L^V$, woraus wieder aus Gradgründen die Gleichheit folgt: $\underline{L^V = \mathbb{Q}(\alpha)}$. Entsprechend begründet man:

$\underline{L^{\langle\sigma\tau\rangle} \;=\; \mathbb{Q}(\varepsilon^2\alpha)}$, da $\sigma\tau(\varepsilon^2\alpha) = \sigma(\varepsilon\alpha) = \varepsilon^2\alpha$ $\qquad$ $\underline{L^{\langle\sigma^2\tau\rangle} \;=\; \mathbb{Q}(\varepsilon\alpha)}$, da $\sigma^2\tau(\varepsilon\alpha) = \varepsilon\alpha$

Damit sind alle Zwischenkörper von $L : \mathbb{Q}$ bestimmt, und wir erhalten den folgenden **Zwischenkörperverband** von $L : \mathbb{Q}$:



oder konkreter:



Zum Abschluß wollen wir auch hier wieder die Frage klären, welche Zwischenkörper Galois–Erweiterungen vom Grundkörper $\mathbb{Q}$ sind. Nach Teil II) des Hauptsatzes sind dies genau die Zwischenkörper E von $L : \mathbb{Q}$, für die die Galois–Gruppe $\mathrm{Gal}(L : E)$ Normalteiler in G ist. Bekannt ist, daß $U =< \sigma >$ der einzige nichttriviale Normalteiler von G ist. Da also

$$U \;=\; \mathrm{Gal}(L : L^U) \;=\; \mathrm{Gal}(L : \mathbb{Q}(\beta))$$

Normalteiler in G ist, ist $\underline{\mathbb{Q}(\beta) : \mathbb{Q}}$ eine Galois–Erweiterung . Dagegen sind die Zwischenkörper

$$\mathbb{Q}(\alpha)\ ,\ \mathbb{Q}(\varepsilon\alpha)\ ,\ \mathbb{Q}(\varepsilon^2\alpha)\,,$$

die alle den Grad 3 über $\mathbb{Q}$ haben, **keine** Galois–Erweiterungen von $\mathbb{Q}$, da die zugehörigen Galois–Gruppen $< \tau >, < \sigma\tau >, < \sigma^2\tau >$ alle **keine** Normalteiler in G sind.