6. Der Hauptsatz der Galoistheorie

Im letzten Kapitel haben wir jeder Körpererweiterung L/K eine Gruppe zugeordnet, nämlich die Galoisgruppe $\mathrm{Gal}(L/K)$ aller K-Automorphismen von L. Wir wollen nun das eigentliche Hauptresultat der Galoistheorie beweisen, das wir bereits am Anfang von Kapitel 5 angekündigt hatten: dass im Fall einer galoisschen Körpererweiterung die Zwischenkörper von L/K bijektiv den Untergruppen von $\mathrm{Gal}(L/K)$ entsprechen. Auch in diesem Kapitel seien dazu noch alle Körpererweiterungen endlich und von Charakteristik 0.

Eine Richtung dieser Bijektion können wir mit unseren bisherigen Methoden schon konstruieren, nämlich die Zuordnung einer Untergruppe von $\mathrm{Gal}(L/K)$ zu einem Zwischenkörper von L/K.

Notation 6.1 (Zwischenkörper $\mapsto$ Untergruppe)**.** Es sei L/K eine Körpererweiterung. Wir bezeichnen mit $\mathscr{Z}$ die Menge der Zwischenkörper von L/K und mit $\mathscr{U}$ die Menge der Untergruppen von $\mathrm{Gal}(L/K)$. Ist $Z \in \mathscr{Z}$ ein Zwischenkörper und $\sigma \in \mathrm{Gal}(L/Z)$ ein Automorphismus von L, der Z fest lässt, so lässt σ natürlich auch den kleineren Körper K fest und liegt damit auch in $\mathrm{Gal}(L/K)$. Also ist $\mathrm{Gal}(L/Z)$ eine Untergruppe von $\mathrm{Gal}(L/K)$, und wir erhalten so eine Abbildung

$$\begin{array}{rccc} \Psi\colon & \mathscr{Z} & \longrightarrow & \mathscr{U} \\ & Z & \longmapsto & \mathrm{Gal}(L/Z). \end{array}$$

Für die umgekehrte Richtung, also um einer Untergruppe einen Zwischenkörper zuzuordnen, benötigen wir die folgende Konstruktion.

Definition 6.2 (Fixkörper)**.** Es seien L ein Körper und $G \leq \mathrm{Aut}(L)$ eine Untergruppe der Automorphismengruppe von L. Dann heißt

$$L^G := \{a \in L\colon\ \sigma(a) = a \text{ für alle } \sigma \in G\}$$

der **Fixkörper** von G in L (man prüft sofort nach, dass dies in der Tat ein Unterkörper von L ist).

Beispiel 6.3. Es seien $L = \mathbb{C}$ und $G = \{\mathrm{id}_\mathbb{C}, \sigma\}$, wobei $\sigma : \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ die komplexe Konjugation ist. Dann ist G offensichtlich eine Gruppe von Automorphismen von $\mathbb{C}$. Der zugehörige Fixkörper besteht aus den Elementen von $\mathbb{C}$, die von allen Automorphismen in G festgehalten werden, also

$$\begin{aligned} L^G &= \{z \in \mathbb{C}\colon\ \mathrm{id}(z) = z \text{ und } \sigma(z) = z\} \\ &= \{z \in \mathbb{C}\colon\ \overline{z} = z\} \\ &= \mathbb{R}. \end{aligned}$$

Notation 6.4 (Untergruppe $\mapsto$ Zwischenkörper)**.** Mit den Bezeichnungen aus Notation 6.1 sei nun $G \in \mathscr{U}$ eine Untergruppe von $\mathrm{Gal}(L/K)$. Da dann alle Elemente von G Automorphismen von L sind, die K fest lassen, enthält der Fixkörper L^G natürlich K und ist damit ein Zwischenkörper von L/K. Wir haben also eine Abbildung

$$\begin{array}{rccc} \Phi\colon & \mathscr{U} & \longrightarrow & \mathscr{Z} \\ & G & \longmapsto & L^G. \end{array}$$

Beispiel 6.5. Für die Körpererweiterung $L/K = \mathbb{C}/\mathbb{R}$ ist $G := \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \sigma\}$ nach Beispiel 5.3 (a), wobei $\sigma : \mathbb{C} \to \mathbb{C}$, $z \mapsto \overline{z}$ wie in Beispiel 6.3 die komplexe Konjugationsabbildung ist. Da $\mathbb{C}/\mathbb{R}$ als Körpererweiterung vom Grad 2 nach der Gradformel aus Satz 2.17 keine echten Zwischenkörper haben kann, ist die Menge der Zwischenkörper dieser Körpererweiterung gleich $\mathscr{Z} = \{\mathbb{R}, \mathbb{C}\}$. Andererseits ist die Galoisgruppe $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ isomorph zu $\mathbb{Z}_2$ und hat damit nur die trivialen Untergruppen, d. h. die Menge der Untergruppen von $\mathrm{Gal}(\mathbb{C}/\mathbb{R})$ ist $\mathscr{U} = \{G, \{\mathrm{id}\}\}$. Die Abbildungen Ψ

und Φ aus den Notationen 6.1 und 6.4 sind nun

$$\begin{aligned} \Psi: \quad \mathscr{Z} &\longrightarrow \mathscr{U} \\ \mathbb{R} &\longmapsto \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = G \\ \mathbb{C} &\longmapsto \mathrm{Gal}(\mathbb{C}/\mathbb{C}) = \{\mathrm{id}\} \end{aligned}$$

und nach Beispiel 6.3

$$\begin{aligned} \Phi: \quad \mathscr{U} &\longrightarrow \mathscr{Z} \\ G &\longmapsto \mathbb{C}^G = \mathbb{R} \\ \{\mathrm{id}\} &\longmapsto \mathbb{C}^{\{\mathrm{id}\}} = \mathbb{C}. \end{aligned}$$

Die Abbildungen Ψ und Φ sind hier also invers zueinander. Unser Ziel ist es zu zeigen, dass dies für jede galoissche Körpererweiterung der Fall ist. Die Hauptarbeit hierfür steckt in dem folgenden vorbereitenden Lemma.

Lemma 6.6 (Lemma von Artin). *Es seien L ein Körper und $G \leq \mathrm{Aut}(L)$ eine endliche Gruppe von Automorphismen von L. Ist dann $K = L^G$ der Fixkörper von G, so gilt*

$$[L:K] \leq |G|.$$

(In der Tat werden wir in Bemerkung 6.8 noch sehen, dass sogar immer die Gleichheit gilt.)

Beweis. Es sei $G = \{\sigma_1, \ldots, \sigma_n\}$ mit $n = |G|$. Nach Definition des Grades einer Körpererweiterung müssen wir zeigen, dass die Dimension von L als K-Vektorraum höchstens gleich n ist, d. h. dass je $n+1$ Elemente $a_1, \ldots, a_{n+1} \in L$ linear abhängig über K sind.

Dazu betrachten wir für solche $a_1, \ldots, a_{n+1}$ das lineare Gleichungssystem

$$\sum_{i=1}^{n+1} \sigma_j(a_i) \cdot x_i = 0 \qquad \text{für alle } j = 1, \ldots, n \tag{1}$$

in den Variablen $x_1, \ldots, x_{n+1} \in L$. Da dies ein System mit n Gleichungen in $n+1$ Variablen ist, besitzt es eine nicht-triviale Lösung. Wir wählen nun eine solche nicht-triviale Lösung, die mit maximal vielen Nullen beginnt und so normiert ist, dass der nächste Eintrag gleich 1 ist, d. h. so dass

$$x_1 = \cdots = x_s = 0 \quad \text{und} \quad x_{s+1} = 1 \tag{2}$$

für ein $s \geq 0$ gilt und keine nicht-triviale Lösung mit $x_1 = \cdots = x_{s+1} = 0$ existiert.

Wir behaupten zunächst, dass für jedes $\sigma \in G$ dann auch $(\sigma(x_1), \ldots, \sigma(x_{n+1}))$ eine Lösung des Gleichungssystems (1) ist. In der Tat rechnet man dies leicht nach: für alle $j = 1, \ldots, n$ ist

$$\sum_{i=1}^{n+1} \sigma_j(a_i) \cdot \sigma(x_i) = \sigma\left(\sum_{i=1}^{n+1} (\sigma^{-1} \circ \sigma_j)(a_i) \cdot x_i \right) = \sigma(0) = 0,$$

da ja $\sigma^{-1} \circ \sigma_j \in G$ gilt und der Ausdruck in der großen Klammer damit genau eine der linken Seiten des Gleichungssystems (1) ist. Weil σ als Körperhomomorphismus die Elemente 0 und 1 festhält, gilt nach (2) auch für diese Lösung

$$\sigma(x_1) = \cdots = \sigma(x_s) = 0 \quad \text{und} \quad \sigma(x_{s+1}) = 1. \tag{3}$$

Nun bilden die Lösungen des Gleichungssystems (1) aber natürlich einen Vektorraum. Damit ist auch die Differenz $(y_1, \ldots, y_{n+1}) := (x_1 - \sigma(x_1), \ldots, x_{n+1} - \sigma(x_{n+1}))$ unserer beiden gefundenen Lösungen eine Lösung von (1) – und für diese gilt nach (2) und (3) offensichtlich

$$y_1 = \cdots = y_{s+1} = 0.$$

Wegen der Maximalität von s unter den nicht-trivialen Lösungen von (1) bedeutet dies, dass $(y_1, \ldots, y_{n+1}) = (0, \ldots, 0)$ die triviale Lösung sein muss. Also gilt $y_i = 0$, d. h. $\sigma(x_i) = x_i$ für alle $i = 1, \ldots, n+1$.

Da dies für alle $\sigma \in G$ gilt, liegen alle x_i im Fixkörper $K = L^G$ von G. Die Gleichung

$$\sum_{i=1}^{n+1} a_i \cdot x_i = 0,$$

die (für $\sigma_j = \mathrm{id}$) ja im Gleichungssystem (1) enthalten ist, besagt damit gerade, dass die $a_1, \dots, a_{n+1}$ linear abhängig über K sind. Damit ist die Dimension von L als K-Vektorraum höchstens gleich n. □

Mit dem Lemma von Artin können wir neben den Bedingungen aus Satz 5.8 nun noch eine weitere angeben, die äquivalent dazu ist, dass eine Körpererweiterung L/K galoissch ist – nämlich dass K ein Fixkörper (von irgendeiner Gruppe) in L ist.

Folgerung 6.7 („galoissch = Fixkörper“)**.** *Für eine Körpererweiterung L/K gilt*

$$L/K \text{ galoissch} \quad \Longleftrightarrow \quad K = L^G \text{ für ein } G \leq \mathrm{Aut}(L).$$

In diesem Fall ist dann $\mathrm{Gal}(L/K) = G$.

Beweis.

„⇐“ Es sei $K = L^G$ für ein $G \leq \mathrm{Aut}(L)$. Beachte, dass dann $G \leq \mathrm{Gal}(L/K)$ gelten muss, da nach der Definition des Fixkörpers jedes Element von G den Körper K fest lässt. Andererseits gilt für die Ordnungen der Gruppen G und $\mathrm{Gal}(L/K)$ aber auch

$$\begin{aligned} |\mathrm{Gal}(L/K)| &\leq [L:K] && \text{(Lemma 5.2 (c))} \\ &\leq |G| && \text{(Lemma 6.6 von Artin)} \end{aligned}$$

(beachte, dass G als Untergruppe von $\mathrm{Gal}(L/K)$ endlich und das Lemma von Artin daher anwendbar ist). Zusammen ist dies natürlich nur möglich, wenn $G = \mathrm{Gal}(L/K)$ und $|\mathrm{Gal}(L/K)| = [L:K]$ (und auch $[L:K] = |G|$) gilt. Also ist L/K galoissch, und wir haben auch bereits die Zusatzbehauptung in der Folgerung gezeigt.

„⇒“ Wir betrachten den Fixkörper $L^{\mathrm{Gal}(L/K)}$, der wie in Notation 6.4 erläutert ein Zwischenkörper von L/K ist. Nach dem bereits bewiesenen Teil „⇐“ ist die Körpererweiterung $L/L^{\mathrm{Gal}(L/K)}$ galoissch mit Galoisgruppe $\mathrm{Gal}(L/K)$. Damit folgt

$$\begin{aligned} [L:L^{\mathrm{Gal}(L/K)}] &= |\mathrm{Gal}(L/K)| && (L/L^{\mathrm{Gal}(L/K)} \text{ galoissch} \\ & && \text{mit Galoisgruppe } \mathrm{Gal}(L/K)) \\ &= [L:K] && (L/K \text{ galoissch nach Voraussetzung}) \\ &= [L:L^{\mathrm{Gal}(L/K)}] \cdot [L^{\mathrm{Gal}(L/K)}:K] && \text{(Gradformel aus Satz 2.17).} \end{aligned}$$

Also ist $[L^{\mathrm{Gal}(L/K)}:K] = 1$ und damit $K = L^{\mathrm{Gal}(L/K)}$ wie behauptet ein Fixkörper. □

Bemerkung 6.8 (Gleichheit im Lemma von Artin)**.** Ist L ein Körper und $K = L^G$ der Fixkörper einer endlichen Gruppe $G \leq \mathrm{Aut}(L)$, so haben wir im Beweis des Teils „⇐“ von Folgerung 6.7 gesehen, dass dann $[L:K] = |G|$ gilt. Im Lemma 6.6 von Artin gilt also sogar immer die Gleichheit. Wir haben dort nur deswegen nur die schwächere Aussage $[L:K] \leq |G|$ gezeigt, um den Beweis kürzer und übersichtlicher zu halten.

Wir haben nun alle Vorbereitungen getroffen, um die bereits angekündigte Korrespondenz zwischen Zwischenkörpern einer galoisschen Körpererweiterung L/K und Untergruppen ihrer Galoisgruppe $\mathrm{Gal}(L/K)$ zu beweisen.

Folgerung 6.9 (**Hauptsatz der Galoistheorie**)**.** *Es sei L/K eine galoissche Körpererweiterung. Wie in den Notationen 6.1 und 6.4 bezeichne $\mathscr{Z}$ die Menge der Zwischenkörper von L/K und $\mathscr{U}$ die Menge der Untergruppen von* $\mathrm{Gal}(L/K)$.

(a) *Die Abbildungen* Ψ *und* Φ *aus den Notationen 6.1 und 6.4 liefern eine Bijektion*

$$\begin{array}{rccl} & \mathscr{Z} & \overset{1:1}{\longleftrightarrow} & \mathscr{U} \\ & Z & \longmapsto & \mathrm{Gal}(L/Z) \quad = \Psi(Z) \\ \Phi(G) = & L^G & \longmapsto & G. \end{array}$$

(b) *Die Korrespondenz aus (a) dreht Inklusionen um:*

$$\begin{aligned} &\textit{für } Z_1, Z_2 \in \mathscr{Z} \textit{ mit } Z_1 \leq Z_2 \textit{ gilt } \Psi(Z_2) \leq \Psi(Z_1); \\ &\textit{für } G_1, G_2 \in \mathscr{U} \textit{ mit } G_1 \leq G_2 \textit{ gilt } \Phi(G_2) \leq \Phi(G_1). \end{aligned}$$

(c) *In der Korrespondenz aus (a) entsprechen die Grade der Zwischenkörper den Ordnungen der Untergruppen: sind* $Z \in \mathscr{Z}$ *und* $G \in \mathscr{U}$ *mit* $G = \Psi(Z)$ *(also* $Z = \Phi(G)$*), so gilt*

$$[L : Z] = |G|.$$

Beweis.

(a) Wir müssen zeigen, dass $\Psi \circ \Phi = \mathrm{id}$ und $\Phi \circ \Psi = \mathrm{id}$.

Für $\Psi \circ \Phi = \mathrm{id}$ sei $G \in \mathscr{U}$, also $G \leq \mathrm{Gal}(L/K)$. Nach dem Zusatz in Folgerung 6.7 ist dann $\mathrm{Gal}(L/Z) = G$ für den Fixkörper $Z = L^G$. Damit gilt

$$G \overset{\Phi}{\longmapsto} L^G = Z \overset{\Psi}{\longmapsto} \mathrm{Gal}(L/Z) = G.$$

Also ist $\Psi \circ \Phi = \mathrm{id}$. Beachte, dass wir für diesen Teil *nicht* benötigt haben, dass die Körpererweiterung L/K galoissch ist!

Für $\Phi \circ \Psi = \mathrm{id}$ sei $Z \in \mathscr{Z}$, also $K \leq Z \leq L$. Nach Lemma 5.17 (b) ist mit L/K auch L/Z galoissch. Folgerung 6.7 angewendet auf L/Z ergibt also $Z = L^G$ mit $G = \mathrm{Gal}(L/Z)$. Damit haben wir

$$Z \overset{\Psi}{\longmapsto} \mathrm{Gal}(L/Z) = G \overset{\Phi}{\longmapsto} L^G = Z,$$

und somit auch $\Phi \circ \Psi = \mathrm{id}$.

(b) Beide Aussagen sind unmittelbar aus den Definitionen klar:

- Ist $Z_1 \leq Z_2$, so erfüllt jeder Isomorphismus $\sigma : L \to L$ mit $\sigma|_{Z_2} = \mathrm{id}$ natürlich auch $\sigma|_{Z_1} = \mathrm{id}$. Damit gilt dann $\mathrm{Gal}(L/Z_2) \leq \mathrm{Gal}(L/Z_1)$.
- Ist $G_1 \leq G_2$, so wird jedes Element von L, das von den Automorphismen in G_2 fest gelassen wird, natürlich insbesondere auch von denen in G_1 fest gelassen. Also gilt dann $L^{G_2} \leq L^{G_1}$.

(c) Wegen $Z = L^G$ ist dies exakt die Aussage aus Bemerkung 6.8. □

10

Beispiel 6.10. Es sei L/K die Körpererweiterung des Zerfällungskörpers von $f = t^3 - 2$ über $\mathbb{Q}$ aus Beispiel 5.12, also $K = \mathbb{Q}$ und

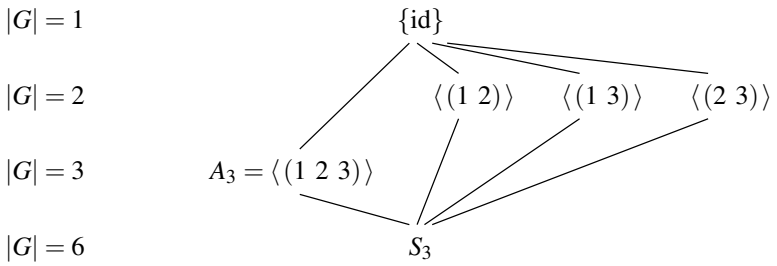
$$L = \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}\big(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\big),$$

wobei

$$a_1 = \sqrt[3]{2}, \quad a_2 = \sqrt[3]{2}\, e^{\frac{2\pi i}{3}}, \quad a_3 = \sqrt[3]{2}\, e^{\frac{4\pi i}{3}}$$

die Nullstellen von f in $\mathbb{C}$ sind. Wir hatten in Beispiel 5.12 bereits gesehen, dass L/K galoissch mit Galoisgruppe $\mathrm{Gal}(L/K) = S_3$ ist, wobei die Elemente von S_3 genau den möglichen Permutationen der drei Nullstellen a_1, a_2, a_3 entsprechen. Auf diese Körpererweiterung wollen wir nun den Hauptsatz der Galoistheorie aus Folgerung 6.9 anwenden.

Üblicherweise beginnt man dabei mit der Menge $\mathscr{U}$ der Untergruppen von $\mathrm{Gal}(L/K)$, da man über diese in der Regel zunächst mehr weiß als über die Menge $\mathscr{Z}$ der Zwischenkörper von L/K. In unserem Fall hier sind z. B. alle Untergruppen von $\mathrm{Gal}(L/K) = S_3$ aus den „Algebraischen Strukturen“ bekannt [G, Beispiel 5.13]; sie sind im folgenden Diagramm dargestellt.



Man nennt eine solche Darstellung ein *Untergruppendiagramm* von $\mathrm{Gal}(L/K) = S_3$. Wir haben die Untergruppen dabei von oben nach unten nach aufsteigender Ordnung sortiert; zwei Untergruppen sind dabei durch Linien miteinander verbunden, wenn die oben stehende eine Untergruppe der unten stehenden ist. In unserem einfachen Fall ist dabei keine echte Untergruppe in einer anderen enthalten, so dass alle Linien entweder im obersten Punkt $\{\mathrm{id}\}$ beginnen oder im untersten Punkt S_3 enden – dies kann in einem komplizierteren Beispiel aber natürlich anders sein.

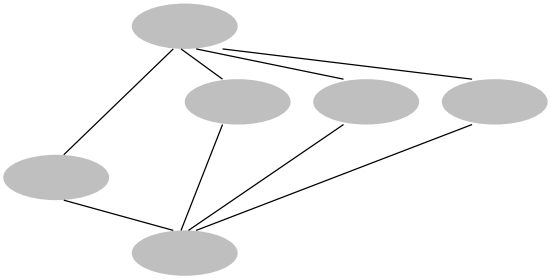
Die Korrespondenz zwischen diesen Untergruppen und den Zwischenkörpern von L/K aus dem Hauptsatz der Galoistheorie in Folgerung 6.9 besagt nun zunächst, dass die Zwischenkörper von L/K in exakt das gleiche Schema passen, dass das *Zwischenkörperdiagramm* also wie im folgenden Bild aussehen muss.

$[L:Z] = 1 \ \Rightarrow \ [Z:K] = 6$

$[L:Z] = 2 \ \Rightarrow \ [Z:K] = 3$

$[L:Z] = 3 \ \Rightarrow \ [Z:K] = 2$

$[L:Z] = 6 \ \Rightarrow \ [Z:K] = 1$



Dabei bedeuten die Linien diesmal, dass der unten stehende Körper ein Teilkörper des oben stehenden ist. Teil (a) des Hauptsatzes besagt dabei zunächst nur, dass diese Zwischenkörper in 1:1-Beziehung zu den Untergruppen aus dem obigen Diagramm stehen. Teil (b) zeigt, dass die Linien zwischen den einzelnen Positionen in beiden Diagrammen gleich sind, und Teil (c) besagt, dass die Zeilenstruktur in beiden Diagrammen übereinstimmt, wobei die Ordnung $|G|$ der Untergruppe nun als Grad $[L:Z]$ von L über dem zugehörigen Zwischenkörper interpretiert werden muss. Die jeweiligen Grade $[Z:K]$ ergeben sich daraus dann natürlich wegen $[L:K] = 6$ mit der Gradformel aus Satz 2.17.

Welche Zwischenkörper stehen nun an den einzelnen Stellen dieses Diagramms? Klar ist natürlich, dass ganz oben der Zwischenkörper mit $[L:Z] = 1$, also $Z = L = \mathbb{Q}\left(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\right)$ steht, und ganz unten der mit $[Z:K] = 1$, also $Z = K = \mathbb{Q}$. Um den ersten Eintrag in der zweiten Zeile zu bestimmen, müssen wir gemäß der Abbildung Φ in Folgerung 6.9 (a) den Fixkörper $L^{\langle(1\ 2)\rangle}$ bestimmen. Nun entspricht das Element $(1\ 2)$ in S_3 aber gerade dem Automorphismus $\sigma : L \to L$ mit $\sigma(a_1) = a_2$, $\sigma(a_2) = a_1$ und $\sigma(a_3) = a_3$. Also ist a_3 und damit auch $\mathbb{Q}(a_3)$ offensichtlich im Fixkörper $L^{\langle(1\ 2)\rangle}$ enthalten. Da dieser gesuchte Fixkörper gemäß unserem Diagramm Grad 3 über $\mathbb{Q}$ hat und der Grad von $\mathbb{Q}(a_3)$ über $\mathbb{Q}$ bereits 3 ist, gilt sogar schon $L^{\langle(1\ 2)\rangle} = \mathbb{Q}(a_3)$: dies ist der gesuchte Eintrag im Zwischenkörperdiagramm. Auf die gleiche Art sieht man, dass die beiden anderen Einträge dieser Zeile $\mathbb{Q}(a_2)$ und $\mathbb{Q}(a_1)$ sind.

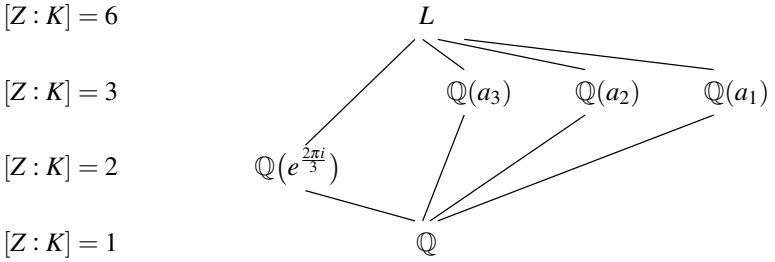
Für den Eintrag in der dritten Zeile müssen wir analog den Fixkörper $L^{\langle(1\ 2\ 3)\rangle}$ berechnen. Hier entspricht das Element $(1\ 2\ 3)$ von S_3 dem Automorphismus $\sigma : L \to L$ mit $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$ und $\sigma(a_3) = a_1$. Keine der drei Nullstellen von f liegt also im gesuchten Fixkörper. Allerdings ist

diesmal

$$\sigma\big(e^{\frac{2\pi i}{3}}\big) = \sigma\Big(\frac{a_2}{a_1}\Big) = \frac{\sigma(a_2)}{\sigma(a_1)} = \frac{a_3}{a_2} = e^{\frac{2\pi i}{3}}$$

und damit $\mathbb{Q}\big(e^{\frac{2\pi i}{3}}\big) \leq L^{\langle (1\ 2\ 3)\rangle}$. Wie oben ist nun aber $[\mathbb{Q}\big(e^{\frac{2\pi i}{3}}\big) : \mathbb{Q}] = 2 = [L^{\langle (1\ 2\ 3)\rangle} : \mathbb{Q}]$ und damit bereits $L^{\langle (1\ 2\ 3)\rangle} = \mathbb{Q}\big(e^{\frac{2\pi i}{3}}\big)$ – dies ist also der noch fehlende Eintrag im Diagramm.

Insgesamt haben wir jetzt also das folgende Zwischenkörperdiagramm erhalten.



Natürlich ist die Existenz aller dieser Zwischenkörper in diesem einfachen Fall schon aus der ursprünglichen Definition

$$L = \mathbb{Q}(a_1, a_2, a_3) = \mathbb{Q}\big(\sqrt[3]{2}, e^{\frac{2\pi i}{3}}\big)$$

offensichtlich gewesen. Der Hauptsatz der Galoistheorie besagt allerdings nun, dass dies auch wirklich die einzigen Zwischenkörper der betrachteten Körpererweiterung sind.

In komplizierteren Fällen sind die Zwischenkörper natürlich meistens nicht so einfach zu sehen wie in dem obigen Beispiel. Wir wollen in der folgenden Aufgabe daher ein Verfahren entwickeln, mit dem man den zu einer Untergruppe gehörenden Fixkörper auf einfache Weise explizit berechnen kann.

Aufgabe 6.11 (Berechnung von Fixkörpern)**.** Es sei L/K eine galoissche Körpererweiterung. Nach dem Satz 4.28 vom primitiven Element können wir sie als einfache Körpererweiterung schreiben, also $L = K(a)$ für ein $a \in L$.

Für eine Untergruppe $G \leq \mathrm{Gal}(L/K)$ setzen wir nun

$$f := \prod_{\sigma \in G} (t - \sigma(a)) \quad \in L[t].$$

Ferner seien $\lambda_0, \ldots, \lambda_n \in L$ die Koeffizienten von f, also $f = \sum_{i=0}^{n} \lambda_i t^i$. Ist dann $Z = L^G$ der zu G gehörige Zwischenkörper von L/K in der Galois-Korrespondenz, so zeige man:

(a) $f \in Z[t]$.

(b) f ist das Minimalpolynom von a über Z und über $K(\lambda_0, \ldots, \lambda_n)$.

(c) $Z = K(\lambda_0, \ldots, \lambda_n)$.

Aufgabe 6.12. Bestimme für die folgenden Körpererweiterungen L/K das Untergruppendiagramm von $\mathrm{Gal}(L/K)$ und das Zwischenkörperdiagramm von L/K:

(a) $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$;

(b) $\mathbb{Q}(e^{\frac{2\pi i}{7}})/\mathbb{Q}$.

Aufgabe 6.13. Zu einem Polynom $f \in K[t]$ über einem Körper K sei $L = K(a_1, \ldots, a_n)$ der Zerfällungskörper, wobei $a_1, \ldots, a_n$ die (verschiedenen) Nullstellen von f in L sind. Bekanntlich ist dann $\mathrm{Gal}(L/K) \leq S_n$. Wir setzen

$$z := \prod_{i<j} (a_i - a_j).$$

Man zeige:

(a) Die sogenannte *Diskriminante* z^2 (siehe auch Bemerkung 5.15) liegt in K.

(b) Ist $\mathrm{Gal}(L/K) \leq A_n$, dann ist sogar $z \in K$.

Zum Abschluss dieses Kapitels wollen wir noch eine zusätzliche Aussage über die Galois-Korrespondenz beweisen, die in der Literatur häufig noch als Teil des Hauptsatzes angesehen wird. Ist Z ein Zwischenkörper einer galoisschen Körpererweiterung L/K, so haben wir in Lemma 5.17 (b) gesehen, dass dann auch die „obere" Erweiterung L/Z galoissch ist. Man kann sich nun natürlich fragen, unter welchen Bedingungen auch die „untere" Erweiterung Z/K galoissch ist. Auf der anderen Seite kann man für eine Untergruppe $G \leq \mathrm{Gal}(L/K)$ untersuchen, ob G vielleicht sogar ein Normalteiler in $\mathrm{Gal}(L/K)$ ist. Wir wollen nun zeigen, dass sich diese beiden Eigenschaften in der Galois-Korrespondenz genau entsprechen (die Eigenschaft (c) im folgenden Satz, die ebenfalls dazu äquivalent ist, ist eine eher technische Bedingung, die wir hier nur aufführen, da sie im Beweis benötigt wird).

Satz 6.14 (Ergänzung zum Hauptsatz der Galoistheorie)**.** *Es sei L/K eine galoissche Körpererweiterung. Ferner sei Z ein Zwischenkörper von L/K, der in der Galois-Korrespondenz aus Folgerung 6.9 der Untergruppe $G \leq \mathrm{Gal}(L/K)$ entspricht, also $Z = L^G$ und $G = \mathrm{Gal}(L/Z)$. Dann sind äquivalent:*

(a) *Z/K ist galoissch.*

(b) *$G \trianglelefteq \mathrm{Gal}(L/K)$ ist ein Normalteiler.*

(c) *Für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt $\sigma(Z) \subset Z$ (und damit nach Aufgabe 5.5 sogar $\sigma(Z) = Z$).*

In diesem Fall ist dann $\mathrm{Gal}(Z/K) \cong \mathrm{Gal}(L/K)/G$.

Beweis.

(a) $\Rightarrow$ (c): Da Z/K galoissch ist, ist Z nach Satz 5.8 der Zerfällungskörper eines Polynoms $f \in K[t]$, also $Z = K(a_1, \ldots, a_n)$ mit den Nullstellen $a_1, \ldots, a_n$ von f in Z. Ist nun $\sigma \in \mathrm{Gal}(L/K)$, so bildet σ die Menge $\{a_1, \ldots, a_n\}$ dieser Nullstellen nach Lemma 5.2 (a) auf sich ab. Also folgt $\sigma(a_i) \in K(a_1, \ldots, a_n) = Z$ für alle $i = 1, \ldots, n$ und damit auch $\sigma(Z) \subset Z$.

(b) $\Rightarrow$ (c): Es seien $\sigma \in \mathrm{Gal}(L/K)$ und $\tau \in G = \mathrm{Gal}(L/Z)$. Dann gilt für alle $a \in \sigma(Z)$

$$(\sigma \circ \tau \circ \sigma^{-1})(a) = (\sigma \circ \tau)(\underbrace{\sigma^{-1}(a)}_{\in Z}) = \sigma(\sigma^{-1}(a)) = a,$$

da τ das Element $\sigma^{-1}(a) \in Z$ fest lässt. Es ist dann also $\sigma \circ \tau \circ \sigma^{-1} \in \mathrm{Gal}(L/\sigma(Z))$. Weil G nach Voraussetzung ein Normalteiler in $\mathrm{Gal}(L/K)$ ist, folgt also für alle $\sigma \in \mathrm{Gal}(L/K)$

$$\mathrm{Gal}(L/Z) = \sigma \circ G \circ \sigma^{-1} \subset \mathrm{Gal}(L/\sigma(Z)),$$

d. h. die nach der Galois-Korrespondenz zum Zwischenkörper Z gehörige Untergruppe $\mathrm{Gal}(L/Z)$ ist in der zum Zwischenkörper $\sigma(Z)$ gehörigen Untergruppe $\mathrm{Gal}(L/\sigma(Z))$ enthalten. Nach dem Hauptsatz der Galoistheorie aus Folgerung 6.9 gilt für die Zwischenkörper selbst dann die umgekehrte Inklusion $\sigma(Z) \subset Z$.

(c) $\Rightarrow$ (a) und (b): Für alle $\sigma \in \mathrm{Gal}(L/K)$ gilt nach Voraussetzung $\sigma(Z) = Z$, d. h. wir können σ zu einem K-Automorphismus von Z einschränken. Es gibt also einen Gruppenhomomorphismus

$$F : \mathrm{Gal}(L/K) \to \mathrm{Gal}(Z/K), \quad \sigma \mapsto \sigma|_Z$$

mit Kern

$$\mathrm{Ker}\, F = \{\sigma \in \mathrm{Gal}(L/K) : \ \sigma|_Z = \mathrm{id}\} = \mathrm{Gal}(L/Z) = G.$$

Insbesondere ist $G = \mathrm{Gal}(L/Z)$ damit als Kern eines Morphismus ein Normalteiler in $\mathrm{Gal}(L/K)$ [G, Lemma 6.7], was (b) zeigt. Außerdem folgt

$$\begin{aligned}
[L:K] &= |\mathrm{Gal}(L/K)| && (L/K \text{ galoissch})\\
&= |\mathrm{Gal}(L/K)/\mathrm{Gal}(L/Z)| \cdot |\mathrm{Gal}(L/Z)| && (\text{Satz von Lagrange [G, Satz 5.10]})\\
&= |\mathrm{Im}\, F| \cdot |\mathrm{Gal}(L/Z)| && (\text{Homomorphiesatz [G, Satz 6.17]})\\
&\leq |\mathrm{Gal}(Z/K)| \cdot |\mathrm{Gal}(L/Z)| && (\mathrm{Im}\, F \leq \mathrm{Gal}(Z/K))\\
&\leq [Z:K] \cdot [L:Z] && (\text{Lemma 5.2 (c)})\\
&= [L:K]. && (\text{Gradformel aus Satz 2.17})
\end{aligned}$$

Also muss hier überall die Gleichheit gelten. Insbesondere ist damit $|\mathrm{Gal}(Z/K)| = [Z:K]$ (d. h. Z/K ist galoissch, was (a) zeigt) und $\mathrm{Im}\, F = \mathrm{Gal}(Z/K)$ (was mit dem Homomorphiesatz [G, Satz 6.17] den Isomorphismus $\mathrm{Gal}(Z/K) \cong \mathrm{Gal}(L/K)/G$, also die Zusatzbehauptung zeigt). □

Beispiel 6.15. Wir betrachten noch einmal das Beispiel 6.10 des Zerfällungskörpers von $t^3 - 2$ über $\mathbb{Q}$ und überprüfen dort die Äquivalenz (a) $\Leftrightarrow$ (b) aus Satz 6.14:

(a) Die Untergruppe $A_3 = \langle (1\ 2\ 3) \rangle$ von S_3 ist nach [G, Beispiel 6.8] als Kern der Signumsabbildung ein Normalteiler. Auf der anderen Seite ist der zugehörige Zwischenkörper $\mathbb{Q}\left(e^{\frac{2\pi i}{3}}\right)$ nach Lemma 5.17 (a) galoissch über $\mathbb{Q}$, da diese Körpererweiterung Grad 2 hat.

(b) Die Untergruppe $\langle (1\ 2) \rangle$ von S_3 ist nach [G, Beispiel 6.6 (c)] kein Normalteiler. Dementsprechend ist auch der zugehörige Zwischenkörper $\mathbb{Q}(a_3)$ nicht galoissch über $\mathbb{Q}$: in ihm hat das irreduzible Polynom $t^3 - 2 \in \mathbb{Q}[t]$ nämlich eine Nullstelle a_3, zerfällt aber nicht in Linearfaktoren (siehe Satz 5.8). Dasselbe Argument gilt natürlich auch für die beiden anderen zweielementigen Untergruppen von S_3.

Beispiel 6.16. Es sei Z ein Zwischenkörper einer galoisschen Körpererweiterung L/K mit $[Z:K] = 2$, also $[L:Z] = \frac{1}{2}[L:K] = \frac{1}{2}|\mathrm{Gal}(L/K)|$. Für die zugehörige Untergruppe $G = \mathrm{Gal}(L/Z)$ gilt dann nach Folgerung 6.9 (c) also $|G| = \frac{1}{2}|\mathrm{Gal}(L/K)|$.

Beachte, dass in diesem Fall die Körpererweiterung Z/K nach Lemma 5.17 (a) immer galoissch ist. Auf der anderen Seite ist die Untergruppe $G \leq \mathrm{Gal}(L/K)$ dann nach [G, Aufgabe 6.9 (a)] auch stets ein Normalteiler, da sie genau halb so viele Elemente hat wie $\mathrm{Gal}(L/K)$. In diesem Fall kannten wir die Äquivalenz von (a) und (b) in Satz 6.14 also schon vorher.

Die folgende Aufgabe zeigt, wie man ein ähnliches Normalteilerkriterium mit Hilfe der Galoistheorie in eines für Zwischenkörper umschreiben kann:

Aufgabe 6.17. Es sei L/K eine galoissche Körpererweiterung und $G \leq \mathrm{Gal}(L/K)$ eine Untergruppe. Aus [G, Aufgabe 6.9 (b)] wissen wir, dass G ein Normalteiler von $\mathrm{Gal}(L/K)$ ist, wenn es keine andere Untergruppe von $\mathrm{Gal}(L/K)$ gibt, die genau so viele Elemente wie G hat.

Welche entsprechende Aussage über Zwischenkörper von L/K erhält man hieraus aus der Galois-Korrespondenz mit Hilfe von Satz 6.14? Kannst du diese Aussage auch direkt ohne Verwendung von Satz 6.14 beweisen?

Aufgabe 6.18. Es sei G die Galoisgruppe eines irreduziblen Polynoms vom Grad n über einem Körper K.

Man zeige: Ist G abelsch, so gilt $|G| = n$.

Gilt auch die Umkehrung?