UNIVERSITÄT AUGSBURG
Mathematisch-Naturwissenschaftlich-Technische Fakultät
Institut für Mathematik

Galoisgruppe - alt und neu

BACHELORARBEIT

Dilan Baçaru

02. April 2015

Name: Dilan Baçaru
Martikelnummer: 1187496
Betreuer: Prof. Dr. Jost-Hinrich Eschenburg

Erklärung zur Bachelorarbeit

Hiermit erkläre ich, Dilan Baçaru, dass die vorliegende Bachelorarbeit eigenständig und nur unter Verwendung der angegebenen Hilfsmittel und Quellen angefertigt wurde.

Ort, Datum	Unterschrift

Inhaltsverzeichnis

Évariste Galois

1 Einleitung

In der Algebra beschäftigt man sich größtenteils mit der Auflösung von Gleichungssystemen. Während anfangs für die Gleichungen von Grad 2,3 und 4 Formeln für die Lösungen gefunden wurden, scheiterte man lange an dem Versuch die allgemeine Gleichung höheren Grades zu lösen.

Évariste Galois (geb. 25. Oktober 1811, †30. Mai 1832) ist eine der bedeutendsten Persönlichkeiten, die uns bezüglich dieses Problems eine bis heute sehr wichtige und zu seiner Zeit bahnbrechende Forschung hinterließen. Galois' Geschichte ist traurig, unter anderem, weil seine Arbeiten zu seiner Zeit keine Anerkennung erhielten und größtenteils abgelehnt wurden. Seine Arbeiten befassten sich mit der Existenz von Lösungesformeln für Gleichungen höheren Grades.
Galois kam bei einem Pistolenduell ums Leben und schrieb eine Nacht vor seinem Tod an seinen Freund Chevalier einen Brief, in dem er ihn bat, seine Arbeiten an Gauß und Jacobi weiterzuleiten. Obwohl Gauß und Jacobi die Arbeiten von Galois erhielten, hörte man von Galois' Forschungen vorerst nichts. Schließlich erkannte Joseph Liouville die Bedeutung von Galois' Arbeiten und veröffentlichte sie im Jahr 1843 in seinem Journal.

In seiner Forschung ordnete Galois jeder Polynomgleichung eine Gruppe von Permutationen zu, die heute unter dem Namen Galoisgruppe bekannt ist. Allgemein dient die Galoisgruppe als Maß für den Unterschied zwischen Grundkörper und Lösungskörper der Gleichung.
Mit ihr entwickelte Galois eine Methode, genannt Galois-Theorie, die die Frage der Lösbarkeit einer Gleichung beantwortet.

Diese Arbeit beschäftigt sich mit der Bestimmung der Galoisgruppe eines Polynoms. Ursprünglich wurden die Elemente der Galoisgruppe als Symmetrien der Nullstellen beschrieben, also diejenigen Permutationen, die alle Relationen zwischen den Nullstellen erhalten:

$$G^{alt} := \{\sigma \in S_n : \quad \sigma H \in R \quad \forall H \in R\}$$

R ist die Menge der Relationen zwischen den Nullstellen von f. Und schon steht man einem Problem gegenüber:

Wie bestimmen wir alle Relationen zwischen den Nullstellen?

Vergisst man eine Relation, so kann dies bereits zur falschen Galoisgruppe führen. Doch auch Galois war sich dieses Problems bewusst und fand einen Ausweg:
Die Bestimmung der Symmetrien mit Hilfe eines sogenannten primitiven Elements. Zu den unterschiedlichen Nullstellen $\alpha_1, ..., \alpha_n$ eines Polynoms f von Grad n gibt es ein Element t, genannt primitives Element, mit dem die Nullstellen darstellbar sind: $\alpha_1, ..., \alpha_n$ sind Polynome in t, also wenn t in h_i eingesetzt wird, ist das die Nullstelle α_i. Werden die Wurzeln des Minimalpolynoms von t in diese Polynome h_i eingesetzt, so erhält man wiederum Nullstellen von f, jedoch nicht unbedingt jeweils die i-ten. Die Nullstellen treten in einer anderen Reihenfolge auf und diese Umordnung ist eine Symmetrie der Nullstellen, also ein Element von G^{alt}.
Es geht sogar weiter: Die Bestimmung der Elemente der Galoisgruppe mit Hilfe einer einzigen Relation.
Dafür benutzt man in dem oben beschriebenen Ausweg ein ganz besonderes primi-

tives Element, welches durch $\alpha_1, ..., \alpha_n$ eingesetzt in einer Galois-Resolvente entsteht. Die Galois-Resolvente ist ein Polynom V in n Variablen, sodass $V(x_{\sigma 1}, ..., x_{\sigma n})$ für jedes $\sigma \in S_n$ einen anderen Wert annimmt: $|\{V(x_{\sigma 1}, ..., x_{\sigma n}); \sigma \in S_n\}| = n!$

Die Elemente der Galoisgruppe wird auch auf eine "moderne" Weise beschrieben: Dedekind definierte die Elemente durch Autotmorphismen, die auf den Grundkörper eingeschränkt die Identitätsabbildung sind.

$$G^{neu} := \{\sigma \in \mathrm{Aut}(L) : \quad \sigma|_K = id_K\}$$

2 Galoisgruppe - alt

In den folgenden Unterkapiteln werden nun Bedingungen und Begriffe, die in der Definition der Galoisgruppe eines Polynoms vorkommen, näher analysiert, um dann die ursprüngliche Beschreibung der Galoisgruppe in seiner Gesamtheit zu betrachten. Zuerst stellen wir eine Methode vor, die die Berechnung der Koeffizienten eines Polynoms mit seinen Nullstellen ermöglicht:

2.1 Elementarsymmetrische Polynome - Satz von Viète

Die meisten Mathematiker versuchten das Nullstellenproblem von Polynomen ($P(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 \stackrel{!}{=} 0$) zu lösen, indem sie aus den Koeffizienten Formeln bildeten, die (möglicherweise) zur Berechnung der Nullstellen dienen. Der bedeutende Mathematiker François Viète[1] begab sich auf einen neuen Weg und betrachtete das Nullstellenproblem aus einer eher ungewöhnlicheren Perspektive:
Er bestimmte aus den gegebenen Lösungen die Koeffizienten des Polynoms.

Beispiel: $n = 2: \quad P(x) = x^2 + a_1 x^1 + a_0$
P habe zwei Nullstellen bei α_1 und α_2, also $P(x) = (x-\alpha_1)(x-\alpha_2)$.

$$\begin{aligned} \Rightarrow \quad x^2 + a_1 x^1 + a_0 &= (x-\alpha_1)(x-\alpha_2) \\ &= x^2 - (\alpha_1+\alpha_2)x + \alpha_1\alpha_2 \\ \Rightarrow \quad a_1 = -(\alpha_1+\alpha_2) \quad &\text{und} \quad a_0 = \alpha_1\alpha_2 \end{aligned}$$

Die Koeffizienten a_1 und a_0 stehen in einer Beziehung zu den Nullstellen α_1 und α_2.

Sei nun $P(x) = x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0 \in K[x]$ mit $a_{n-1}, ..., a_0 \in K$ und $P(x) = 0$ für $x = \alpha_1, ..., \alpha_n \in L$.[2] Wir zerlegen P in Linearfaktoren:

$$\begin{aligned} P(x) &= (x-\alpha_1)\cdot(x-\alpha_2)\cdot ... \cdot (x-\alpha_n) \\ \Rightarrow \quad x^n + a_{n-1}x^{n-1} + ... + a_0 &= (x-\alpha_1)\cdot(x-\alpha_2)\cdot ... \cdot (x-\alpha_n) \end{aligned}$$

Die rechte Seite der Gleichung wird ausmultipliziert. Wie beim obigen Beispiel finden sich vor den Potenzen nun Ausdrücke, die sich aus den n verschiedenen Wurzeln des Polynoms zusammensetzen. Die Gleichheiten dieser Ausdrücke zu den Koeffizienten $a_1, ..., a_{n-1}$ von P ist gegeben, da die Koeffizienten eines Polynoms eindeutig bestimmt sind[[A]S.293]. Deshalb können wir folgende Gleichungen aufschreiben:

$$\begin{aligned} a_{n-1} &= (-1)^1(\alpha_1 + ... + \alpha_n) &&= (-1)^1 \sum_j \alpha_j \\ a_{n-2} &= (-1)^2(\alpha_1\alpha_2 + ... + \alpha_{n-1}\alpha_n) &&= (-1)^2 \sum_{i<j} \alpha_i\alpha_j \\ &\vdots \\ a_{n-k} &= (-1)^k \sum_{j_1<...<j_k} \alpha_{j_1}\cdot\alpha_{j_2}\cdot ... \cdot \alpha_{j_k} \\ &\vdots \\ a_0 &= (-1)^n \alpha_1 \cdot ... \cdot \alpha_n \end{aligned}$$

[1] Französischer Mathematiker, 1540 - 1603
[2] L ist hierbei der Lösungskörper des Polynoms

Die blau hervorgehobenen Terme werden als Polynome bzw. Funktionen in den Variablen $\alpha_1, ..., \alpha_n$ aufgefasst und heißen **elementar-symmetrische Polynome** in $\alpha_1, \ldots, \alpha_n$. Allgemein schreibt man für die k-te elementar-symmetrische Funktion :

$$e_k(x_1, \ldots, x_n) \quad = \quad \sum_{j_1 < \ldots < j_k} x_{j_1} \cdot x_{j_2} \cdot \ldots \cdot x_{j_k}$$

Bemerkung 2.1. Die Polynome e_k sind symmetrisch. Die neu gewonnenen Ausdrücke für die Koeffizienten sind also unabhängig von der Anordnung der Nullstellen. Jedes symmetrische Polynom entsteht durch ein Polynom in $e_1, ..., e_n$ [$[B]S.30 - 12.1$].

Bemerkung 2.2. Um die Koeffizienten eines normierten Polynomes von Grad n wie beschrieben darzustellen, ist die Existenz von genau n verschiedenen Nullstellen notwendig.

Der hier erklärte Prozess ist in der Mathematik als **Wurzelsatz von Viète** bekannt, der kurzgefasst besagt, dass man die Koeffizienten eines normierten Polynoms durch seine Wurzeln bestimmen kann: $a_{n-i} = (-1)^i e_i(\vec{\alpha})$.

In der Defintion der Galoisgruppe wird eine der Bedingungen an das Polynom sein, dass seine Diskriminante ungleich Null ist. Die Bedeutung und Wichtigkeit dieser Bedingung wird nun im nächsten Unterkapitel dargelegt.

2.2 Diskriminante eines Polynoms

Die Diskriminante[3] eines Polynoms wird zur Untersuchung der Mehrfachheit von Nullstellen herangezogen. Sie ist das Produkt der Differenzen der Nullstellen.

Zur Erinnerung: Sei f ein Polynom mit Nullstellen in $\alpha_1, ..., \alpha_n$.
Dann kann man f als Produkt von Linearfaktoren[4] schreiben:

$$f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 = (x - \alpha_1)(x - \alpha_2) \cdot \ldots \cdot (x - \alpha_n)$$

Sei $k \in \{1, \ldots, n\}$: α_k ist eine einfache Nullstelle, falls $(x - \alpha_k)$ in der Linearfaktorzelegnung von f nur einmal auftritt. α_k ist eine mehrfache Nullstelle, falls $(x - \alpha_k)$ in der Linearfaktorzelegnung von f mindestens zweimal auftritt.

Beispiel: Diskriminante eines Polynoms von Grad 2:
Die Nullstellen des Polynoms $f(x) = ax^2 + bx + c \in \mathbb{R}[x]$ liefert uns die Mitternachtsformel

$$x_{1/2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

und die Diskriminante ist $D_f := \sqrt{b^2 - 4ac}$. Mit D können wir genauere Aussagen über die Nullstellen treffen:

[3] Der Begriff stammt aus dem lateinischen Wort dicriminare(= unterscheiden).

[4] Linearfaktoren sind Polynome mit Grad 1. Kann man ein Polynom als Produkt von Linearfaktoren schreiben, so sagt man auch: Das Polynom zerfällt in Linearfaktoren.

$$D_f^2 \quad = \quad \begin{cases} < 0 & \textit{es gibt keine Lösung} \\ = 0 & \textit{es gibt eine doppelte Nullstelle} \\ > 0 & \textit{es gibt zwei unterschiedliche Lösungen} \end{cases}$$

Die allgemeine Formel der Diskriminante eines Polynoms von Grad n wird folgendermaßen definiert [[D]$S.302-303$]:

$$\boxed{D_f := (-1)^{\frac{n(n-1)}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)}$$

Man kann also sagen: Besitzt f mindestens eine mehrfache Nullstelle, dann ist mindestens eines der Produkte der Diskriminante D_f gleich Null, d.h. $\alpha_i - \alpha_j = 0$ mit $i \neq j$. Die Diskriminante ist nicht Null, falls das Polynom keine mehrfache Nullstelle besitzt.
D_f ist ohne die Kenntnis der Nullstellen aus den Koeffizienten bestimmbar: Da D_f ein symmetrisches Polynom ist, ist es laut Bemerkung 2.1 als Polynom in $e_1, ..., e_n$ darstellbar.

In der Definition der Galoisgruppe wird gefordert, dass $D_f \neq 0$. Wir stellen uns nun die Frage, was passiert, falls die Diskriminante des Polynoms gleich Null ist. Diesen Fall betrachten wir nun genauer:

Annahme: Sei $f \in K[x]$, $deg(f) = n$, ein Polynom mit $D_f = 0$.
f hat mindestens eine mehrfache Nullstelle. Sei α_k für ein festes, aber beliebiges k eine doppelte Nullstelle: $\alpha_k = \alpha_{k+1}$ und $f(\alpha_k) = f(\alpha_{k+1}) = 0$
Dann ist auch $f'(\alpha_k) = f'(\alpha_{k+1}) = 0$ [[E]$S.53$]. $(x - \alpha_k) \in L[x]$ teilt die Polynome f und f', wobei f' die Ableitung von f bezeichnet. Über dem Lösungskörper L haben also f und f' einen gemeinsamen Teiler: $ggT(f, f') \neq 1$

Behauptung:
f und f' haben auch einen gemeinsamen Teiler über dem Grundkörper K.

Beweis. Dazu nehme man an, dass über K $ggT(f, f') = 1$ gilt. Mit dem Euklidschen Algorithmus kann man 1 schreiben als: $1 = kf + lf'$ für $k, l \in K[x]$. Diese Gleichung müsste auch über L erfüllt sein($K \subset L$). Dies führt zum Widerspruch, denn laut Voraussetzung sind f und f' über L nicht teilerfremd.
Also haben f und f' in K einen gemeinsamen Teiler, d.h. $ggT(f, f') \neq 1$ über K. □

Fazit: Gilt $D_f = 0$ für ein Polynom f, dann hat es einen Teiler und ist also nicht irreduzibel[5] über K. Dann ergibt es mehr Sinn die Galoisgruppe des Teilers von f, der die Nullstellen von f mit Vielfachheit Eins hat, zu betrachten.

Ein Polynom $f \in K[x]$, dessen irreduzible Faktoren über K nur einfache Nullstellen

[5] Ein Polynom ($\in K[x]$) heißt irreduzibel, falls man es durch kein anderes Polynom ($\in K[x]$) teilen kann.

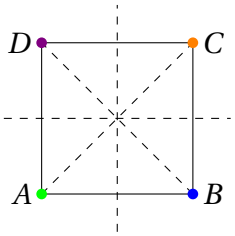
haben, heißt **separabel**. Unser Polynom erfüllt die Bedingung $D_f \neq 0$, ist also insbesondere ein separables Polynom, dessen irreduzible Faktoren nicht gleiche Nullstellen haben.

2.3 Symmetriegruppe der Wurzeln

Die Galoisgruppe wird als die Symmetriegruppe der Wurzeln eines Polynoms definiert. Dazu gehen wir nun kurz darauf ein, was überhaupt die Symmetrien der Nullstellen sind.
Sei X eine beliebige Menge und $S(X) := \{f : X \to X : \quad \text{f ist bijektiv }\}$. ($S(X)$, $\circ$) ist die **symmetrische Gruppe** mit der Verknüpfung $\circ$ von Abbildungen als Gruppenoperation. Falls $X = \{1,...,n\}$ dann bezeichnen wir $S(X) =: S_n$ als **Permutationsgruppe**. Allgemein ist die **Symmetriegruppe** eine Untergruppe der symmetrischen Gruppe und sie enthält nur die Permutationen, die die Relationen, welche zwischen den Elementen von X bestehen, erhalten.

Zur Veranschaulichung betrachten wir zuerst ein einfaches geometrisches Beispiel. Die Symmetriegruppe einer geometrischen Figur enthält diejenigen Abbildungen unter denen die Figur invariant bleibt. Drehungen bzw. Spiegelungen ordnen Ecken, Seiten und Flächen um, aber die Figur selbst bleibt unverändert.

Beispiel: *Quadrat* $Q_2 := [-1,1] \times [-1,1]$



Wir stellen uns die Frage, aus welchen Permutationen von $S(Q_2)$ sich die Symmetriegruppe der Ecken A, B, C und D des Quadrates zusammensetzt. Dabei identifizieren wir Q_2 mit der Menge $\{A, B, C, D\}$: $\quad S(Q_2) \cong S(A, B, C, D)$
Unter den Symmetrien müssen die Verbindungen zwischen den Ecken erhalten bleiben: Beispielsweise ist A mit D und B über jeweils eine Kante verbunden, aber nicht mit C. Die Symmetrien müssen diese Kanten erhalten, damit die Geometrie der Figur unverändert bleibt.

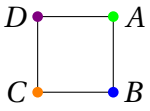
Sei s eine Symmetrie mit $sA = B$. Wir stellen uns die Frage wie die anderen Ecken umgeordnet werden, sodass die Kanten zwischen den Ecken erhalten bleiben. Damit die Kanten unter s erhalten bleiben, muss AB auf BA oder BC abgebildet werden:
Wird die Kante AB mit BA vertauscht, so ist $sD = C$ und $sC = D$. Wird die Kante AB jedoch mit BC vertauscht, so ist $sD = A$ und $sC = D$. Wenn $s(AB) = AB$ ist $s = id$.

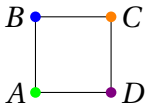
Die möglichen Umordnungen der Symmetrien schreiben wir nun in eine Tabelle nieder:

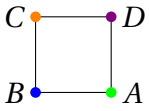
A	$\mapsto$	A	B	C	D
AB	$\mapsto$	AB oder AD	BA oder BC	CB oder CD	DA oder DC
C	$\mapsto$	C	D	A	B
D	$\mapsto$	D oder B	C oder A	D oder B	C oder A

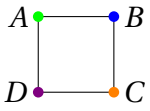
Acht aus 24 Permutationen des $S(A,B,C,D)$ sind Symmetrien. Darunter sind vier Drehungen und vier Spiegelungen.

1. Die Symmetrien $\sigma_1 = \binom{ABCD}{CBAD}$, $\sigma_2 = \binom{ABCD}{ADCB}$, $\sigma_3 = \binom{ABCD}{BADC}$ und $\sigma_4 = \binom{ABCD}{DCAB}$ sind die Spiegelungen an den Diagonalen bzw. an den Mittellinien:

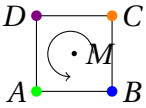


und


bzw.


und


2. Die Symmetrien $\sigma_5 = \binom{ABCD}{BCDA}$, $\sigma_6 = \binom{ABCD}{CDAB}$, $\sigma_7 = \binom{ABCD}{DABC}$ und $\sigma_8 = \binom{ABCD}{ABCD} = id_{Q_2}$ drehen Q_2 um den Mittelpunkt M.



Die Symmetriegruppe der Ecken des Quadrates Q_2 enthält also acht Elemente:

$$\{\sigma_1,\sigma_2,\sigma_3,\sigma_4,\sigma_5,\sigma_6,\sigma_7,id_{Q_2}\}$$

Anhand dieses Beispieles wird folgendes klar: Die Ecken der Figur werden untereinander umgeordnet, doch die Verbindungen zwischen den Ecken bleiben erhalten. Nun liegt die Kunst darin, diese geometrische Erklärung auf die Symmetriegruppe der Nullstellen zu übertragen.
Die Elemente der Symmetriegruppe der Wurzeln eines Polynoms sind ebenfalls Permutationen. Diese Permutationen ordnen die Wurzeln unter der Bedingung, dass bestimmte Beziehungen zwischen ihnen erhalten bleiben, um.
Diese "Beziehungen" sind die algebraischen Relationen zwischen den Wurzeln. Genauer: Relationen sind Polynome in n-Variablen und

$$R := \{H \in K[x_1,...,x_n] : \quad H(\vec{\alpha}) = H(\alpha_1,...,\alpha_n) = 0\} \quad \subset K[x_1,...,x_n]$$

beschreibt die Menge aller Relationen zwischen den Nullstellen $\alpha_1,...,\alpha_n$ des Polynoms.

Behauptung 2.1. R ist ein Ideal[6] des Rings $K[x_1,...,x_n]$.

Beweis. R ist Untergruppe der additiven Gruppe des Rings $K[x_1,...,x_n]$, da:
1. $0 \in R$: $H(\vec{0}) = 0$ für alle $H \in R$
2. Seien $H, \tilde{H} \in R$: $\quad (H+\tilde{H})(\vec{\alpha}) = H(\vec{\alpha}) + \tilde{H}(\vec{\alpha}) = 0 \qquad \Rightarrow H+\tilde{H} \in R$

Und R ist dann ein Ideal, da:
3. Seien $H \in R$ und $J \in K[x_1,...,x_n]$: $\quad (H \cdot J)(\vec{\alpha}) = H(\vec{\alpha}) \cdot J(\vec{\alpha}) = 0 \cdot J(\vec{\alpha}) = 0$
$\Rightarrow H \cdot J \in R$ □

[6]Definition - Ideal: Die Untergruppe eines Rings heißt **Ideal**, falls sie abgeschlossen unter der Multiplikation mit Elementen aus dem Ring ist.

Die Relationen in R sollen unter den Elementen der Symmetriegruppe der Wurzeln erhalten bleiben: R bleibt unter der Wirkung der Symmetriegruppe invariant. Was man sich unter dieser Wirkung vorstellt, wird im folgenden Kapitel erklärt.

2.4 Wirkung von Permutationen auf ein Polynom

Sei $\sigma \in S_n$ eine n- stellige Permutation und $f \in K[x_1,...,x_n]$ ein Polynom über K in n Variablen. Wendet man σ auf f an, so werden die Variablen untereinander vertauscht:

$$\sigma f(x_1,...,x_n) = f(x_{\sigma(1)},...,x_{\sigma(n)})$$

Behauptung 2.2. Die Permutationsgruppe S_n wirkt auf die Menge $K[x_1,...,x_n]$.

Beweis. Um zu zeigen, dass es sich bei der Abbildung $\tau : S_n \times K[x_1,...,x_n] \to K[x_1,...,x_n]$ mit $(\sigma, f) \mapsto \sigma f$ tatsächlich um eine Wirkung handelt, werden die beiden Axiome der Gruppenwirkung[7] nachgewiesen:

1. Das neutrale Element der Gruppe S_n ist die Identitätsabbildung $e_{S_n} = id$. Also: $e_{S_n} f = id\ f = f$ für alle $f \in K[\vec{x}]$.
2. Für alle $\sigma, \eta \in S_n$ und $f \in K[x_1,...,x_n]$ gilt $(\sigma\eta)f = \sigma(\eta f)$, da:
   Für $\sigma(\eta f)(x_1,...,x_n) = \eta f(x_{\sigma 1},...,x_{\sigma n})$ substituieren wir mit $\tilde{x}_i := x_{\sigma i}$,$i \in \{1,...,n\}$.
   $\Rightarrow$ $\eta f(\tilde{x}_1,...,\tilde{x}_n) = f(\tilde{x}_{\eta 1},...,\tilde{x}_{\eta n})$
   Mit der Rücksubstitution $\tilde{x}_{\eta i} = x_{\sigma\eta i}$ erhalten wir also:
   $$f(\tilde{x}_{\eta 1},...,\tilde{x}_{\eta n}) = f(x_{\sigma\eta 1},...,x_{\sigma\eta n}) = (\sigma\eta)f(x_1,...,x_n)$$

□

Erinnerung: Ein Polynom f in mehreren Variablen heißt symmetrisch, falls f bei jeder Umordnung der Variablen unverändert bleibt. Im Bezug auf die Wirkung von S_n auf $K[x_1,...,x_n]$ ist f symmetrisch, wenn es unter allen Permutationen von S_n erhalten bleibt: $\sigma f = f \quad \forall \sigma \in S_n$

Von den Elementen der Symmetriegruppe der Wurzeln wird erwartet, dass jedes Polynom H aus R, also jede Relation zwischen den Wurzeln, erhalten bleibt:

$$\sigma H(\vec{\alpha}) = 0 \quad \text{mit } \sigma \in S(\alpha_1,...,\alpha_n)$$

Die Umordnung der Nullstellen können wir auch mit der Permutation ihrer Indizes beschreiben. Die symmetrische Gruppe der Wurzeln $\alpha_1,...,\alpha_n$ identifizieren wir so mit der symmetrischen Gruppe der Menge $\{1,...,n\}$:

$$S(\{\alpha_1,...,\alpha_n\}) \quad \cong \quad S(\{1,...,n\})$$

Bemerkung 2.3. Da die Relationen im Allgemeinen nicht notwendig symmetrisch sind, kann man nicht davon ausgehen, dass sie unter allen Permutationen aus S_n erhalten bleiben.

[7] Definition der Wirkung: Sei G eine Gruppe und X eine Menge. Die Abbildung $\tau : G \times X \to X$, $(g,x) \mapsto gx$, die die Eigenschaften $ex = x$ (e ist das neutrale Element von G) und $(gh)x = g(hx)$ für alle $x \in X$ und $g,h \in G$ erfüllt, nennt man Wirkung von G auf X

2.5 Definition

Nachdem nun die notwendigen Begriffe erarbeitet wurden, können wir die Galoisgruppe betrachten.

Definition 2.1. Galoisgruppe
Das Polynom $f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 \in K[x]$ habe die Nullstellen $\alpha_1, \ldots, \alpha_n$. Die Diskriminante von f sei nicht Null. Und $R \subset K[x_1, \ldots, x_n]$ sei die Menge der Relationen der Nullstellen, $\quad R := \{H \in K[x_1, ..., x_n] : \quad H(\alpha_1, \ldots, \alpha_n) = 0\}$.
$(S_n \cong)\ S(\{\alpha_1, ..., \alpha_n\})$ ist die Permutationsgruppe der Wurzeln von f. Dann nennt man die Symmetriegruppe der Wurzeln die **Galoisgruppe des Polynoms** f:

$$\boxed{G_f := \{\sigma \in S_n : \quad \sigma H \in R \quad \forall H \in R\}}$$

Satz 2.1. *Die Galoisgruppe G_f ist eine Untergruppe von S_n.*

Beweis. G_f ist eine Teilmenge von S_n, da für alle $\sigma \in G_f$: $\quad \sigma \in S_n$.

1. $id \in G_f$:
   $id \cdot H(\vec{\alpha}) = H(\vec{\alpha}) = 0 \quad \Rightarrow id \cdot H \in R$ für alle $H \in R$
2. Für $\sigma, \tau \in G_f$ ist auch $\sigma \circ \tau \in G_f$:
   Da $\tau \in G_f$, ist τH eine Relation in R und da $\sigma \in G_f$ ist $\sigma(\tau H)$ auch eine Relation in R.
   Mit $(\sigma \circ \tau)H = \sigma(\tau H) \in R$ folgt die Behauptung.
3. Für $\sigma \in G_f$ ist auch $\sigma^{-1} \in G_f$:
   σ hat eine endliche Ordnung, $\sigma^k = id$ für ein $k \in \mathbb{N}$. Laut U2 ist $\underbrace{\sigma \circ \sigma \circ \ldots \circ \sigma}_{\text{k-1 mal}} \in G_f$.
   Mit $\sigma^{-1} = \sigma^{k-1}$ folgt die Behauptung. □

Die Galoisgruppe G_f ist eine Gruppe, da: $G_f \subset S_n$ und die Elemente der Permutationsgruppe S_n erfüllen die Eigenschaften: Assoziativgesetz, $id \circ \sigma = \sigma = \sigma \circ id$ und $\sigma \circ \sigma^{-1} = \sigma^{-1} \circ \sigma = id$.[8]

Bemerkung 2.4.
1. Mit der Definition der Galoisgruppe wird die Notwendigkeit der Bedingung $D_f \neq 0$ deutlicher.
2. Je größer die Menge der Relationen ist, desto kleiner ist die Galoisgruppe, da die Anzahl der Permutationen, die alle Relationen zwischen den Wurzeln erhalten, kleiner wird.
3. Zwei unterschiedliche Polynome, deren Nullstellenmengen verschieden sind, können die gleiche Galoisgruppe haben. Denn damit die Galoisgruppen gleich sind, müssen die Relationen der Nullstellenmengen nicht gleich sein, sondern nur die Permutationen, die diese Relationen erhalten.

An dieser Stelle fragen wir uns, wie es möglich ist, alle Relationen zwischen den Nullstellen zu finden. Eine Idee wäre, die Erzeugenden des Ideals R zu bestimmen. Da uns

[8] Verknüpfungen von Abbildungen erfüllen die Assoziativität. σ^{-1} ist das inverse Element zu σ, welches eine endliche Ordnung hat: $\sigma^k = id$ für ein $k \in \mathbb{N}$. Dann gilt: $\sigma^{-1} = \sigma^{k-1} \quad \Rightarrow \sigma^{-1} \circ \sigma = \sigma^{k-1} \circ \sigma = \sigma^k = id = \sigma \circ \sigma^{k-1} = \sigma \circ \sigma^{-1}$.

jedoch nicht alle Elemente von R bekannt sind, ist keine Sicherheit darüber gegeben, dass wir alle Erzeugenden erfassen. Falls zur Bestimmung der Galoisgruppe nur die uns bekannten Relationen herangezogen werden, besteht die Gefahr, dass die Galoisgruppe zu klein oder zu groß ist.
Im folgenden wird ein Verfahren vorgestellt, welches dabei hilft, fehlende Relationen zwischen den Nullstellen zu finden.

2.6 Relationenmenge

Sei R_0 die Relationenmenge, die alle "bekannten" Relationen, einschließlich die Viète-Relationen, die wir aus den elementarsymmetrischen Polynomen erhalten (Siehe 2.1), enthält.
Bestimmen wir die Galoisgruppe mit Hilfe von R_0, besteht folgende Gefahr: Sei $H \in R_0$. Falls für ein $\sigma \in S_n$ die Relation σH mit $\sigma H = 0$ nicht ein Element von R_0 ist, könnte die Galoisgruppe, welche nur die Relationen aus R_0 erhält, zu klein sein. Mit folgendem Verfahren werden diese fehlenden Relationen ergänzt.

Verfahren:
Sei $\sigma_1 \in S_n$ eine beliebige Permutation mit $\sigma_1^l = id$, $l \in \mathbb{N}$ und sei $U_1 := <\sigma_1> = \{\sigma_1, \sigma_1^2, ..., \sigma_1^l = id\} \subset S_n$ die davon erzeugte Untergruppe.
Mit dieser Untergruppe erweitern wir R_0:

$$R_1 := \bigcup_{\tau \in U_1} \tau R_0$$

FALLS $(R_1) = (1) = K[\vec{x}]$, "fällt" σ_1 weg und R_0 wird mit Hilfe einer anderen Untergruppe $<\sigma>$, $\sigma \neq \sigma_1$, erweitert.

FALLS $(R_1) \neq (1) = K[\vec{x}]$, dann wählen wir ein weiteres $\sigma_2 \in G\, U_1$ und erweitern R_1 zu einer Menge

$$R_2 := \bigcup_{\tau \in U_2} \tau R_1 = \bigcup_{\tau \in U_2} \tau R_0$$

mit $U_2 := <\sigma_2> \cup U_1$ für ein beliebiges $\sigma_2 \notin U_1$.

Diese beiden Fälle spielen wir dann für die Erweiterung R_2 von R_1 durch.

Nach einer endlichen Anzahl von Schritten endet dieser Vorgang: Sei k, $1 \leq k \leq n!$, die Anzahl der Schritte, dann ist $R_k := \bigcup_{\tau \in U_k} \tau R_{k-1}$ nicht mehr erweiterbar.

U_k erhält alle Relationen in R_k.
Man beachte, dass es weitere, noch nicht erfasste Relationen geben kann, die von U_k nicht erhalten werden. Folglich ist G_f eine echte Untergruppe von U_k.

Beispiel: Für R_0 = (Viète-Relationen) endet das Verfahren sofort und $U_1 = S_n$.

Bemerkung 2.5. Den ersten Fall wiederholen wir solange, bis wir eine Permutation finden, sodass $(R_1) \neq (1)$. Gibt es eine solche Permutation nicht, so lässt sich R_0 nicht erweitern. Ist jede Erweiterung von R_1 bereits der Ring $K[\vec{x}]$, dann ist R_1 die einzige Erweiterung von R_0.

Um dem Problem der Bestimmung von Relationen zu entgehen, betrachten wir nun die Möglichkeit, die Galoisgruppe mit Hilfe eines primitiven Elements zu bestimmen:

2.7 Galois-Resolvente

Der Begriff "Resolvente" stammt von Lagrange und bezeichnet Hilfsgrößen zum Lösen einer Gleichung. Doch die Lagrangen Resolventen waren für Galois' Arbeit nicht geeignet. Er suchte nach einer Resolvente, die ihm half die Lösungen einer Gleichung zu analysieren.

Das Polynom $f \in K[x]$ habe getrennte Nullstellen $\alpha_1, ..., \alpha_n$. Sei $t \in K(\alpha_1, ..., \alpha_n)$ ein **primitives Element** von $K(\alpha_1, ..., \alpha_n)$, d.h. $K(t) = K(\alpha_1, ..., \alpha_n)$. Die Elemente von $K(t)$ werden mit Polynomen in t dargestellt: Insbesondere existiert für $\alpha_i \in K(t)$, $i \in \{1, ..., n\}$, also ein $h_i \in K[x]$, sodass $\alpha_i = h_i(t)$.

Sei $t \notin K$ ein beliebiges Element und m_t sein Minimalpolynom über K mit $deg(m_t) = s \in \mathbb{N}$. Neben t hat m_t genau $s-1$ weitere Nullstellen $t_2, ..., t_s$. Diese Nullstellen $t_2, ..., t_s$ heißen die **Galois-Konjugierten** zu t.

Setzen wir eine Galois-Konjugierte t' zu t in die Polynome h_i ein, erhalten wir die Nullstellen von f, jedoch in einer anderen Reihenfolge:

Satz 2.2. *Seien $\alpha_1, ..., \alpha_n$ die getrennten Nullstellen eines separablen Polynoms $f \in K[x]$. Sei $t := V(\alpha_1, ..., \alpha_n)$ ein primitives Element mit $V \in K[\vec{x}]$. h_i, für $i \in \{1, ..., n\}$, seien Polynome in K mit $\alpha_i = h_i(t)$.*
1) Dann existiert für jedes zu t Galois-Konjugiertes t' genau eine Symmetrie $\sigma \in S_n$ der Nullstellen, sodass:

$$\sigma\alpha_i = h_i(t') \quad \text{für alle } i \in \{1, ..., n\}$$

2) Es gilt auch die Umkehrung: Zu jeder Symmetrie σ der Nullstellen, gibt es genau ein zu t Galois-Konjugiertes t', sodass: $\sigma\alpha_i = h_i(t')$ für alle $i \in \{1, ..., n\}$
3) Mit dieser bijektiven Zuordnung gilt:

$$t' = V(\sigma\alpha_1, ..., \sigma\alpha_n)$$

An dieser Stelle wird nur der Beweis zur ersten Behauptung angeführt. Den Beweis findet man auch in [E] S. 129f.

Beweis. Sei also t' eine galoissche Konjugierte von t. Sei $\phi := f \circ h_i$ für ein beliebiges $i \in \{1, ..., n\}$. t ist eine Nullstelle von ϕ, da $\phi(t) = f(h_i(t)) = f(\alpha_i) = 0$.

Dann ist auch t' eine Nullstelle von ϕ, da:
Sei m_t das Minimalpolynom von t, also das normierte, irreduzible Polynom, welches t als Nullstelle besitzt. Da t eine Nullstelle von ϕ ist, ist m_t ein Teiler von ϕ. Für ein $g \in K[x]$ ist also $\phi = m_t \cdot g$. Die Nullstellen von m_t sind auch Nullstellen von ϕ, insbesondere $\phi(t') = 0$.

Mit $0 = \phi(t') = f(h_i(t'))$ ist $h_i(t')$ eine Nullstelle von f. Die Nullstellen von f sind bereits gegeben und deshalb gilt:

$$h_i(t') \in \{\alpha_1, ..., \alpha_n\}$$

Sei $h_i(t') = h_j(t')$ für $i, j \in \{1, ..., n\}$. Dann ist t' eine Nullstelle von $h_i - h_j \in K[x]$. Wie oben ist m_t ein Teiler von $h_i - h_j$ und damit sind die Nullstellen von m_t auch Nullstellen von $h_i - h_j$

$$\Rightarrow h_i(t) = h_j(t) \qquad \Rightarrow \alpha_i = h_i(t) = h_j(t) = \alpha_j$$

Die Nullstellen von f sind unterschiedlich, also ist $i = j$. Aus $h_i(t') = h_j(t')$ folgt also $i = j$. Da jedem $h_i(t')$ eine Nullstelle von f eindeutig zugeordnet wird, ist $h_1(t'), ..., h_n(t')$ eine Permutation von $\alpha_1, ..., \alpha_n$:
Es existiert also ein $\sigma \in S_n$ mit $\sigma\alpha_i = h_i(t')$ für alle $i \in \{1, ..., n\}$.

Eindeutigkeit von σ:
Sei τ auch eine Permutation mit $\tau\alpha_i = h_i(t')$ für alle $i \in \{1, ..., n\}$. Da $\sigma\alpha_i = h_i(t')$ und wegen der eindeutigen Zuordnung von $h_i(t')$, ist $\tau\alpha_i = h_i(t') = \sigma\alpha_i$. Also folgt $\tau = \sigma$ und damit die Eindeutigkeit der Permutation.

Dieses Permutation σ ist eine Symmetrie der Nullstellen:
Sei $H \in K[\vec{x}]$ eine Relation zwischen den Nullstellen von f, $H(\alpha_1, ..., \alpha_n) = 0$. Mit $\alpha_i = h_i(t)$ ist auch $H(h_1(t), ..., h_n(t)) = 0$. Dann ist t' eine Nullstelle von $H(h_1(x), ..., h_n(x))$

$$\Rightarrow 0 = H(h_1(t'), ..., h_n(t')) = H(\sigma\alpha_1, ..., \sigma\alpha_n)$$

Also erhält σ die Relationen zwischen den Nullstellen von f und ist eine Symmetrie. □

Bemerkung 2.6. Zur Bestimmung der Symmetrien zwischen den Nullstellen ist es nicht ausreichend, nur die Relationen $H_i(\vec{\alpha}) = 0 \ \forall i \in \{1, ..., n\}$, mit $H_i(\vec{x}) := x_i - h_i(V(\vec{x}))$, zu betrachten. Zusätzlich ist die Kenntnis über die Galois-Konjugierten $t', t'', ...$ zu $V(\vec{\alpha})$ notwendig.

In Satz 2.2 ist t ein primitives Element $t := V(\alpha_1, ..., \alpha_n)$ mit $V \in K[\vec{x}]$. Nun werden wir ein primitives Element t betrachten, wobei V ein ganz besonderes Polynom ist:

Eine **Galois-Resolvente** ist ein Polynom $V \in K[x_1, ..., x_n]$ mit folgender Eigenschaft:

$$\sigma V(\alpha_1, ..., \alpha_n) \text{ hat für alle } \sigma \in S_n \text{ unterschiedliche Werte}$$

Jede Permutation der Nullstellen ändert also den Wert von $V(\alpha_1, ..., \alpha_n)$ und $|\{V(x_{\sigma 1}, ..., x_{\sigma n}); \sigma \in S_n\}| = n!$.
Insbesondere ist $V(\alpha_1, ..., \alpha_n)$ ein primitves Element von $K(\alpha_1, ..., \alpha_n)$ [[E]S.135].

Satz 2.3. *Das separable Polynom f habe n verschiedene Nullstellen $\alpha_1, ..., \alpha_n$. $V \in K[\vec{x}]$ sei eine Galois-Resolvente von f. Dann ist $t := V(\alpha_1, ..\alpha_n)$ ein primitives Element. Sei g das Minimalpolynom von t und $\tau \in S_n$. Dann gilt:*

$$\tau \in G_f \qquad \Longleftrightarrow \qquad g(\tau V(\alpha_1, ..., \alpha_n)) = 0$$

Beweis. " $\Leftarrow$ " Sei $g(\tau V(\alpha_1, ..., \alpha_n)) = 0$.
Dann ist $\tau V(\alpha_1, ..., \alpha_n) =: t_\tau$ ein Galois-Konjugiertes zu t. Mit Satz 2.2 gibt es für jedes Galois-Konjugiertes t' zu t genau eine Symmetrie $\sigma \in S_n$ der Nullstellen, sodass $t' = \sigma V(\alpha_1, ..., \alpha_n)$. Es existiert also eine Symmetrie σ mit $t_\tau = \sigma V(\alpha_1, ..., \alpha_n)$.
Da V eine Galois-Resolvente ist, sind die Werte $\sigma V(\alpha_1, ..., \alpha_n)$ für alle $\sigma \in S_n$ unterschiedlich. Deshalb gibt es nur eine Permutation, die $t_\tau = \sigma V(\alpha_1, ..., \alpha_n)$ erfüllt. Also ist $\tau = \sigma$ und τ eine Symmetrie der Nullstellen von f: $\tau \in G_f$
" $\Rightarrow$ " Sei $\tau \in G_f$.
τ ist also eine Symmetrie der Nullstellen $\alpha_1, ..., \alpha_n$. Laut Satz 2.2 gibt es genau ein Galois-Konjugiertes t' von t, sodass $t' = \tau V(\alpha_1, ..., \alpha_n)$.
Also: $0 = g(t') = g(\tau V(\alpha_1, ..., \alpha_n))$. □

Die Fülle der Relationen reduziert sich also auf eine einzige Relation, mit der die Permutationen der Galoisgruppe bestimmt werden:

$$\boxed{H(\alpha_1,...,\alpha_n) := g(V(\alpha_1,...,\alpha_n)) = 0}$$

Das Minimalpolynom eines primitiven Elements $V(\vec{\alpha})$ ist nicht immer leicht bestimmbar. Zur Bestimmung des Minimalpolynoms gehen wir folgendermaßen vor:

Verfahren:
$g(x) := \prod_{\sigma \in S_n} (x - \sigma V(\vec{\alpha}))$ ist ein Polynom mit Nullstelle in $V(\vec{\alpha})$. Wir suchen eine Untergruppe U von S_n, sodass das Polynom $\prod_{\sigma \in U} (x - \sigma V(\vec{\alpha}))$ Koeffizienten aus den ganzen Zahlen und eine Nullstelle in $V(\vec{\alpha})$ hat. Dann suchen wir eine Untergruppe U' von U, sodass $\prod_{\sigma \in U'} (x - \sigma V(\vec{\alpha}))$ ein ganzzahliges Polynom ist und Nullstelle $V(\vec{\alpha})$ hat.
Diesen Prozess wiederholen wir solange, bis wir die kleinste Untergruppe $U^{min} = \bigcap_{g_U \in \mathbb{Z}[x]} U$, $g_U := \prod_{\sigma \in U} (x - \sigma V(\alpha))$, erhalten, sodass $\prod_{\sigma \in U^{min}} (x - \sigma V(\vec{\alpha}))$ ein irreduzibles Polynom mit Nullstelle in $V(\vec{\alpha})$ ist.
Dieses Polynom ist dann das Minimalpolynom von $V(\vec{\alpha})$ und die Permutationen in U^{min} sind die Symmetrien der Nullstellen von f.

2.8 Beispiele

Beispiel 1: $f(x) = x^4 + 1 \quad \in \mathbb{Q}[x]$

In diesem Beispiel können wir die Nullstellen des Polynoms einfach bestimmen. Die Nullstelle $\alpha_1 := \sqrt{i}$ sieht man leicht. Weitere Nullstellen sind:

$$\alpha_2 := \sqrt{i}\zeta_4, \alpha_3 := \sqrt{i}\zeta_4^2 \text{ und } \alpha_4 := \sqrt{i}\zeta_4^3 \quad \text{mit } \zeta_4 := e^{\frac{2\pi i}{4}}$$

Mit $\sqrt{i} = \sqrt{0 + i \cdot 1} = \sqrt{cos(\pi/2) + i \cdot sin(\pi/2)} = \sqrt{e^{\frac{\pi i}{2}}} = e^{\frac{\pi i}{4}}$ gibt es die Möglichkeit die Nullstellen von f mit der e-Funktion darzustellen:

$$\alpha_{k+1} = e^{\frac{\pi i}{4} + \frac{2\pi i}{4} \cdot k} \text{ für } k \in \{0,1,2,3\}$$

Diese Darstellung liefert uns eine Beziehung der Nullstellen von f zu der ersten Nullstelle α_1. α_2, α_3 und α_4 sind ungeraden Potenzen von α_1: $\alpha_2 = \alpha_1^3, \alpha_3 = \alpha_1^5$ und $\alpha_4 = \alpha_1^7$
Diese Beziehungen sollen unter den Permutationen der Galoisgruppe erhalten bleiben.
Wie zuvor geschildert wurde, besteht hier das Problem, dass wir nicht wissen, ob die bekannten Relationen alle Elemente von $R = \{H \in \mathbb{Q}[\vec{x}] : \quad H(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = 0\}$ erzeugen. Dieses Problem umgehen wir, indem wir die Permutationen mit Hilfe des Satzes 2.2, S. 13, bestimmen:

Wir nehmen an, die Nullstellen von f seien uns unbekannt. $\alpha \notin \mathbb{Q}$ sei solch eine Nullstelle von f: $\alpha^4 = -1$.
Dann sind ungerade Potenzen von α wieder Nullstellen: für jede ungerade Zahl $k \in \mathbb{N}$ gilt

$$(\alpha^k)^4 = (\alpha^4)^k = (-1)^k = -1.$$

α erfüllt die Gleichung $\alpha^8 = 1$, insbesondere also $\alpha^9 = \alpha$. Drei weitere Nullstellen von f sind dann α^3, α^5 und α^7. Diese sind verschieden, da:
Sei $k, l \in \{1,3,5,7\}, \quad k < l$:

$$\alpha^l = \alpha^k \quad \Leftrightarrow \quad \alpha^l - \alpha^k = 0 \quad \Leftrightarrow \quad \alpha^k(\alpha^{l-k} - 1) = 0 \quad \Leftrightarrow \quad \alpha^k = 0 \text{ oder } \alpha^{l-k} = 1$$

Dann wäre, aber $\alpha^4 \neq -1$.

Die Nullstellen von f nummerieren wir: $\alpha_1 := \alpha$, $\alpha_2 := \alpha^3$, $\alpha_3 := \alpha^5$ und $\alpha_4 := \alpha^7$

Sei $V \in \mathbb{Q}[\vec{x}]$ mit $V(x_1, ..., x_4) = x_1$. Ein primitives Element von $K(\alpha_1, ..., \alpha_4)$ ist $\alpha = t := V(\alpha_1, ..., \alpha_4)$. Da f über $\mathbb{Q}$ irreduzibel ist und eine Nullstelle in t hat, ist es bereits das Minimalpolynom von t. Dann sind $\alpha_2, \alpha_3, \alpha_4$ die Galois-Konjugierten zu t.
Die Nullstellen von f sind Polynome $h_i \in \mathbb{Q}$ in α_1:

$$\alpha_1 = h_1(\alpha_1), \quad \alpha_2 = h_2(\alpha_1), \quad \alpha_3 = h_3(\alpha_1) \quad \text{und } \alpha_4 = h_4(\alpha_1)$$

mit $h_i(x) = x^{2i-1}, i \in \{1,2,3,4\}$

σ_j sei für alle $j \in \{1,2,3,4\}$ eine Permutation mit $\sigma_j 1 = j$, also $\alpha_j = \sigma_j \alpha_1$. Die Symmetrie zwischen den Nullstellen ist durch folgende Gleichungen bestimmt:

$$\alpha_{\sigma_j i} - h_i(\alpha_j) = 0 \text{ für alle } i \in \{1,2,3,4\}$$

In folgenden Rechnungen beachten wir, dass eine Nullstelle α_j die Gleichung $\alpha_j^4 = -1$, also auch $\alpha_j^8 = 1$ erfüllt:
$\alpha_{\sigma_j i} = h_i(\sigma_j V(\vec{\alpha})) = h_i(\alpha_{\sigma_j 1}) = \alpha_{\sigma_j 1}^{2i-1} = \alpha_j^{2i-1} = (\alpha_1^{2j-1})^{2i-1} = \alpha_1^{(2j-1)(2i-1)}$ und mit $(2j-1)(2i-1) = 2k-1$ für $k := 2ij - i - j + 1$ ist dann $\alpha_{\sigma_j i} = \alpha_1^{2k-1}$. Also gilt

$\sigma_j \alpha_i = \sigma_j(h_i(\alpha_1)) = h_i(\alpha_j) = \alpha_k$ und $\sigma_j i = k \mod 4$.
Bei festem $\sigma_j 1 = j$ berechnen wir $\sigma_j i$ und erhalten folgende Symmetrien der Nullstellen: $\sigma_1 = id$, $\sigma_2 = \binom{1234}{2143}$, $\sigma_3 = \binom{1234}{3412}$, $\sigma_4 = \binom{1234}{4321}$

Also lautet die Galoisgruppe von f: $G_f = \{id, \sigma_2, \sigma_3, \sigma_4\}$

Beispiel 2: $f(x) = x^4 - 10x^2 + 1 \quad \in \mathbb{Q}[x]$ $[[E] S.127 - 128]$

Aus der biquadratischen Gleichung $x^4 - 10x^2 + 1 = 0$ erhalten wir durch die Substitution $u := x^2$ die Gleichung $u^2 - 10u + 1 = 0$. Die Lösungen dieser Gleichung bestimmen wir mit der Mitternachtsformel:
$u_{1/2} = \frac{+10 \pm \sqrt{100-4}}{2} = 5 \pm 2\sqrt{6} \qquad \Rightarrow x^2 = 5 \pm 2\sqrt{6}$ löst die Gleichung $u^2 - 10u + 1 = 0$
Da $5 \pm 2\sqrt{6} = 2 + 3 \pm 2\sqrt{2}\sqrt{3} = (\sqrt{2} \pm \sqrt{3})^2$, sind die Lösungen u_1 und u_2 die Wurzeln von $(\sqrt{2}+\sqrt{3})^2$ und $(\sqrt{2}-\sqrt{3})^2$. Also sind die Nullstellen von f:
$\alpha_1 := \sqrt{u_1} = \sqrt{2}+\sqrt{3}, \quad \alpha_2 := -\sqrt{u_1} = -\sqrt{2}-\sqrt{3}, \quad \alpha_3 := \sqrt{u_2} = \sqrt{2}-\sqrt{3}$ und $\alpha_4 := -\sqrt{u_2} = -\sqrt{2}+\sqrt{3}$

Die Symmetrien der Nullstellen bestimmen wir mit Satz 2.2:

Hier ist $t := \alpha_1 = \sqrt{2}+\sqrt{3}$ mit $V(x_1, ..., x_4) = x_1$ ein primitives Element. Wir können $\sqrt{3}$ und $\sqrt{2}$ mit Polynomen in t darstellen:
$$t^2 = 5 + 2\sqrt{6} \quad \Rightarrow \sqrt{6} = \tfrac{1}{2}(t^2 - 5), \text{ also ist } \sqrt{6} \in \mathbb{Q}(t)$$
Und mit $t^3 = 11\sqrt{2} + 9\sqrt{3}$ ist
$$t^3 - 9t = 2\sqrt{2} - 0\sqrt{3} \quad \text{und} \quad -t^3 + 11t = 0\sqrt{2} + 2\sqrt{3},$$
also folgt
$$\sqrt{2} = \tfrac{1}{2}(t^3 - 9t) \in \mathbb{Q}(t) \quad \text{und} \quad \sqrt{3} = \tfrac{1}{2}(-t^3 + 11t) \in \mathbb{Q}(t)$$
Da f über $\mathbb{Q}$ irreduzibel ist und eine Nullstelle in α_1, ist f das Minimalpolynom zu α_1. Dann sind α_2, α_3 und α_4 die Galois-Konjugierten zu α_1.

Die Nullstellen von f sind Polynome $h_i \in \mathbb{Q}$, $i \in \{1,2,3,4\}$, in α_1:
$$\alpha_1 = h_1(\alpha_1), \quad \alpha_2 = h_2(\alpha_1), \quad \alpha_3 = h_3(\alpha_1) \quad \text{und } \alpha_4 = h_4(\alpha_1)$$
mit $h_1(x) = x$, $h_2(x) = -x$, $h_3(x) = x^3 - 10x$ und $h_4(x) = -x^3 + 10x$

σ_j sei eine Permutation mit $\sigma_j 1 := j$, $j \in \{1,2,3,4\}$, also $\sigma_j \alpha_1 = \alpha_j$. Diese Symmetrie zwischen den Nullstellen ist durch folgende Gleichungen eindeutig festgelegt:
$$\alpha_{\sigma_j i} = h_i(\alpha_j) \quad \forall i \in \{1,2,3,4\}$$

Wir berechnen nun für festes j die Umordnung der Nullstellen unter σ_j genau:
$j = 1$: $h_1(\alpha_1) = \alpha_1$, $h_2(\alpha_1) = \alpha_2$, $h_3(\alpha_1) = \alpha_3$
und $h_4(\alpha_1) = \alpha_4 \qquad \Rightarrow \sigma_1 = id$
$j = 2$: $h_1(\alpha_2) = \alpha_2$, $h_2(\alpha_2) = -\alpha_2 = \alpha_1$, $h_3(\alpha_2) = \alpha_2^3 - 10\alpha_2 = \alpha_4$
und $h_4(\alpha_2) = -\alpha_2^3 + 10\alpha_2 = \alpha_3 \qquad \Rightarrow \sigma_2 = \binom{1234}{2143}$
$j = 3$: $h_1(\alpha_3) = \alpha_3$, $h_2(\alpha_3) = -\alpha_3 = \alpha_4$, $h_3(\alpha_3) = \alpha_3^3 - 10\alpha_3 = \alpha_1$
und $h_4(\alpha_3) = -\alpha_3^3 + 10\alpha_3 = \alpha_2 \qquad \Rightarrow \sigma_3 = \binom{1234}{3412}$
$j = 4$: $h_1(\alpha_4) = \alpha_4$, $h_2(\alpha_4) = -\alpha_4 = \alpha_3$, $h_3(\alpha_4) = \alpha_3^3 - 10\alpha_3 = \alpha_2$
und $h_4(\alpha_4) = -\alpha_4^3 + 10\alpha_4 = \alpha_1 \qquad \Rightarrow \sigma_4 = \binom{1234}{4321}$

Also lautet die Galoisgruppe von f: $G_f = \{id, \sigma_2, \sigma_3, \sigma_4\}$

Beispiel 3: $f(x) = x^n - 1 \quad \in \mathbb{Q}[x]$

Die Potenzen(eins bis n) der n-ten Einheitswurzel $\zeta_n := e^{\frac{2\pi i}{n}}$ sind die verschiedenen Nullstellen von f, die für ein $k \in \{1, ..., n\}$ folgendermaßen definiert werden: $\alpha_k := \zeta_n^k$
Also ist jede Nullstelle eine Potenz von α_1: $\alpha_k = \zeta_n^k = (\zeta_n^1)^k = (\alpha_1)^k$

Mit Satz 2.2 bestimmen wir die Galoisgruppe von f:
Ein primitives Element ist in diesem Fall die Wurzel $t := \alpha_1$ mit $V(\vec{x}) = x_1 \in \mathbb{Q}[x]$. Um die Galois-Konjugierten von α_1 zu bestimmen, müssen wir zuerst das Minimalpolynom finden. Das Minimalpolynom einer n-ten Einheitswurzel ist das n-te Kreisteilungspolynom

$$\phi_n := \prod_{1 \le k < n, \mathrm{ggT}(k,n)=1} (x - \alpha_1^k).$$

ϕ_n ist irreduzibel über $\mathbb{Q}$. [[A]S.452]
Sei $s-1$ die Anzahl der Elemente von $\{k \in \mathbb{N} : 1 \le k < n, \mathrm{ggT}(k,n) = 1\}$. Dann gibt es genau $s-1$ Galois-Konjugierte $t_2, ..., t_s$ zu α_1:

$$t_j := \alpha_{k_j} \quad \text{mit } \mathrm{ggT}(k_j, n) = 1,\ j \in \{2, ..., s\}$$

Die Wurzeln $\alpha_1, ..., \alpha_n$ von f sind die Polynome $h_i \in \mathbb{Q}[x]$, $i \in \{1, ..., n\}$, in α_1,

$$\alpha_1 = h_1(\alpha_1), \quad \alpha_2 = h_2(\alpha_1), \quad \ldots \quad , \alpha_n = h_n(\alpha_1),$$

mit $h_i(x) = x^i$.

σ_j, $j \in \{2, ..., s\}$, sei eine Permutation zwischen den Nullstellen mit $\sigma_j 1 := j$. Für jede Galois-Konjugierte $\alpha_j = \sigma_j \alpha_1$ bestimmen wir die zugehörige Symmetrie zwischen den Nullstellen aus den Gleichungen

$$\alpha_{\sigma_j i} = h_i(t_j) \quad \text{für alle } i \in \{1, ...n\}$$

Wir können nun $\sigma_j i$ errechnen:

$$\alpha_{\sigma_j i} = h_i(t_j) = (\alpha_{k_j})^i = (\alpha_1^{k_j})^i = \alpha_1^{k_j i} = \alpha_1^{k_j i \bmod n}$$
$$\Rightarrow \quad \sigma_j i = k_j i \mod n$$

Also permutiert σ_j jede Nullstelle auf ihre k_j-te Potenz unter der Bedingung $\mathrm{ggT}(k_j, n) = 1$.

Die Galoisgruppe von f lautet:

$$G_f = \{i \mapsto k_j i \mod n | ggT(k_j, n) = 1, k_j < n\}$$

Beispiel 4: $f(x) = x^n - a \quad \in \mathbb{Q}(\zeta)[x]$ mit $\zeta := e^{\frac{2\pi i}{n}}$

Eine Wurzel von f ist $\sqrt[n]{a}$, also sind die anderen Nullstellen $\zeta^k \sqrt[n]{a}$. Sei $\alpha_k := \zeta^k \sqrt[n]{a}$ und sei $\sqrt[n]{a}^j$ für alle $j \in \{1, ..., n-1\}$ irrational.

Mit Satz 2.2 bestimmen wir die Galoisgruppe von f über $\mathbb{Q}(\zeta)$:
$t := \alpha_n = \sqrt[n]{a}$ ist ein primitives Element mit $V(\vec{x}) = x_n$, $V \in \mathbb{Q}(\zeta)[x]$. Das Minimalpoly-

nom von α_n ist f, da keine kleinere Kombination der Linearfaktoren $(x-\zeta^k\sqrt[n]{a})$ von f ein Polynom in $\mathbb{Q}(\zeta)[x]$ ist (weil die Potenzen $\sqrt[n]{a}^j$ mit $j<n$ in den Koeffizienten auftauchen) und f also irreduzibel ist. Die Galois-Konjugierten von α_n sind die Nullstellen $\alpha_1,...,\alpha_{n-1}$.
Die Wurzeln von f sind Polynom $h_i \in \mathbb{Q}(\zeta)[x]$, $i \in \{1,...,n\}$, in α_n:

$$\alpha_1 = h_1(\alpha_n), \quad \alpha_2 = h_2(\alpha_n), \quad ... \quad , \alpha_n = h_n(\alpha_n)$$

mit $\quad h_i(x) := \zeta^i x$

σ_j sei für alle $j \in \{1,...,n\}$ eine Permutation der Nullstellen mit $\sigma_j n := j$. Für jede Galois-Konjugierte $\alpha_j = \sigma_j \alpha_1$ bestimmen wir die zugehörige Symmetrie aus den Gleichungen

$$\alpha_{\sigma_j i} = h_i(\alpha_j)$$

Unter Beachtung von $\zeta^n = 1$ errechnen wir $\sigma_j i$:

$$\alpha_{\sigma_j i} = h_i(\alpha_j) = \zeta^i \alpha_j = \zeta^i \zeta^j \sqrt[n]{a} = \zeta^{i+j}\sqrt[n]{a} = \zeta^{i+j \bmod n}\sqrt[n]{a}$$
$$\Rightarrow \quad \sigma_j i = i + j \mod n$$

Die Galoisgruppe von f lautet also:

$$G_f = \{i \mapsto i + j \mod n | j \in \{1,...,n\}\}$$

Zuletzt betrachten wir nun die Verallgemeinerung der Beispiele 1 und 2:

Beispiel 5: Biquadratische Gleichung $\quad f(x) = x^4 - 2ax^2 + b$

Sei f ein irreduzibles Polynom. Wir bestimmen die Nullstellen dieser Gleichung mit der Substitution $u := x^2$:

$$u^2 - 2au + b = 0 \quad \text{für } u_{1/2} = \frac{2a \pm \sqrt{4a^2 - 4b}}{2} = a \pm \sqrt{a^2 - b}$$

Mit $u = x^2$ folgt $f(x) = 0$ für $x = \pm\sqrt{a \pm \sqrt{a^2 - b}}$.
Die Nullstellen von f sind also:

$$\alpha_1 = \sqrt{a + \sqrt{a^2 - b}}, \quad \alpha_2 = -\sqrt{a + \sqrt{a^2 - b}}$$
$$\alpha_3 = \sqrt{a - \sqrt{a^2 - b}}, \quad \alpha_4 = -\sqrt{a - \sqrt{a^2 - b}}$$

Beh.: α_1 ist ein primitives Element genau dann, wenn $\sqrt{b} \in \mathbb{Q}$.

Beweis.
$''\Rightarrow''$ Sei α_1 ein primitives Element. Und sei $w := \sqrt{a^2 - b}$.
Dann ist $\alpha_3 \in \mathbb{Q}(\alpha_1)$ und

$$\alpha_1 \alpha_3 = \sqrt{a + w}\sqrt{a - w} = \sqrt{a^2 - w^2} = \sqrt{a^2 - a^2 + b} = \sqrt{b}$$

Also ist $\sqrt{b} \in \mathbb{Q}$.

$''\Leftarrow''$ Sei $\sqrt{b} \in \mathbb{Q}$.
Mit der ersten Nullstelle von f können nun alle anderen Nullstellen erzeugt werden:

$$\alpha_2 = -\alpha_1, \quad \alpha_3 = \frac{\sqrt{b}}{\alpha_1} \quad \text{und} \quad \alpha_4 = -\frac{\sqrt{b}}{\alpha_1}$$

Da also $\alpha_2, \alpha_3, \alpha_4 \in \mathbb{Q}(\alpha_1)$, ist α_1 ein primitives Element. □

Sei $\sqrt{b} \in \mathbb{Q}$. Mit Satz 2.2 bestimmen wir nun die Elemente der Galoisgruppe: $t := \alpha_1$ ist ein primitives Element und $V(\vec{x}) = x_1$. Da f irreduzibel ist, sind α_2, α_3 und α_4 die Galois-Konjugierten zu α_1.
Die Wurzeln $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ sind Funktionen h_i in α_1,

$$\alpha_1 = h_1(\alpha_1), \quad \alpha_2 = h_2(\alpha_1), \quad \alpha_3 = h_3(\alpha_1), \quad \alpha_4 = h_4(\alpha_1)$$

mit $h_1 = id$, $h_2(x) = -x$, $h_3(x) = \sqrt{b}/x$ und $h_4(x) = -\sqrt{b}/x$.

Sei σ_j, $j \in \{1,2,3,4\}$, die Permutation mit $\sigma_j 1 = j$, also $\sigma_j \alpha_1 = \alpha_j$. Die Umordnung der Nullstellen unter σ_j wird durch folgende Gleichungen eindeutig festgelegt:

$$\alpha_{\sigma_j i} = h_i(\alpha_j) \quad \forall i \in \{1,2,3,4\}$$

Für festes $j \in \{1,2,3,4\}$ erhalten wir also folgende Umordnungen:

$j = 1$: $h_1(\alpha_1) = \alpha_1$, $h_2(\alpha_1) = \alpha_2$, $h_3(\alpha_1) = \alpha_3$
und $h_4(\alpha_1) = \alpha_4$ $\Rightarrow \sigma_1 = id$

$j = 2$: $h_1(\alpha_2) = \alpha_2$, $h_2(\alpha_2) = -\alpha_2 = \alpha_1$, $h_3(\alpha_2) = \sqrt{b}/\alpha_2 = \alpha_4$
und $h_4(\alpha_2) = -\sqrt{b}/\alpha_2 = \alpha_3$ $\Rightarrow \sigma_2 = \binom{1234}{2143}$

$j = 3$: $h_1(\alpha_3) = \alpha_3$, $h_2(\alpha_3) = -\alpha_3 = \alpha_4$, $h_3(\alpha_3) = \sqrt{b}/\alpha_3 = \alpha_1$
und $h_4(\alpha_3) = -\sqrt{b}/\alpha_3 = \alpha_2$ $\Rightarrow \sigma_3 = \binom{1234}{3412}$

$j = 4$: $h_1(\alpha_4) = \alpha_4$, $h_2(\alpha_4) = -\alpha_4 = \alpha_3$, $h_3(\alpha_4) = \sqrt{b}/\alpha_4 = \alpha_2$
und $h_4(\alpha_4) = -\sqrt{b}/\alpha_4 = \alpha_1$ $\Rightarrow \sigma_4 = \binom{1234}{4321}$

Also lautet die Galoisgruppe von f:

$$G_f = \{id, \sigma_2, \sigma_3, \sigma_4\}$$

Hierbei ist in den Beispielen 1 und 2 $b = 1$.

3 Galoisgruppe - neu

Die ursprüngliche Beschreibung der Galoisgruppe in Kapilel 2.5 findet man heutzutage in den algebraischen Arbeiten seltener. Diejenige Beschreibung der Galoisgruppe die heute im Gebrauch ist, führte Dedekind in seiner Vorlesung 1855/56 ein. Er beschrieb nicht die Galoisgruppe eines Polynoms, sondern viel allgemeiner die einer Körpererweiterung.

Zum Verständnis ist es nun wieder notwendig sich an einige Begriffe zu erinnern.

3.1 Einige Begriffe

3.1.1 Automorphismus

Der Automorphismus eines Körpers K ist eine Abbildung $\phi : K \to K$ mit folgenden Eigenschaften:

- ϕ ist bijektiv, also umkehrbar
- $\phi(0) = 0$ und $\phi(1) = 1$
- $\forall a, b \in K$ gilt : $\phi(ab) = \phi(a)\phi(b)$ und $\phi(a+b) = \phi(a) + \phi(b)$

Ein Automorphismus ist also ein bijektiver Homomorphismus, dessen Definitions- und Wertebereich derselbe ist.
Die Komposition und die Umkehrung von Automorphismen sind ebenfalls Automorphismen, deshalb ist die Menge aller Automorphismen eines Körpers K eine Gruppe. Dabei ist die Gruppenoperation die Hintereinanderschaltung $\circ$ von Abbildungen.
Die Automorphismengruppe wird mit $Aut(K)$ bezeichnet.

3.1.2 Körpererweiterung

Sei $K \subseteq L$ ein Teilkörper[9] von L. Dann nennt man L **Erweiterungskörper** von K und $L \supset K$ **Körpererweiterung**. Beispielsweise ist $\mathbb{C}$ ein Erweiterungskörper von $\mathbb{R}$ und $\mathbb{R}$ ist Teilkörper von $\mathbb{C}$: Also ist $\mathbb{C} \supset \mathbb{R}$ eine Körpererweiterung.

Der Körper $K(a)$ entsteht durch die **Adjunktion** eines Elements $a \notin K$ an einen Körper K. $K(a)$ ist der kleinste Körper, der K und a enthält. Bei der Adjunktion wird K nicht nur um ein einziges Element erweitert, sondern bereichert sich auch durch die Elemente, die aus Addition, Subtraktion, Multiplikation, Division von a mit allen $k \in K$ entstehen.
Die Elemente von $K(a)$ beschreiben wir durch rationale Funktionen in a:

$$K(a) = \{\tfrac{f(a)}{g(a)} : f, g \in K[x], g(a) \neq 0\}$$

Mit dem Ring $K[a]$ bezeichnt man die Menge aller Polynom von $K[x]$ in a:[10]

$$K[a] = \{g(a) : \quad g \in K[x]\}$$

Sei a ein über K algebraisches Element, d.h. es existiert ein Polynom $(0 \neq) f \in K[x]$ mit

[9] Ein Teilkörper K von L erfüllt die Eigenschaften: für $a, b \in K$ sind auch $a+b, a-b, ab$ und $b^{-1} \in K$

[10] Oft wird es auch als Bild des Einsetzungshomomorphismus beschrieben: $K[a] :=\text{im}(\psi_a)$. Sei $L \supset K$ eine Körpererweiterung und $a \in L$. $\psi_a : K[x] \to L$ mit $g(x) \mapsto g(a)$ heißt Einsetzungshomomorphismus.

$f(a) = 0$. Dann ist $K[a]$ ein Körper und $K[a] = K(a)$. [[A]S.376]

Es ist auch die Adjunktion einer Menge $A := \{a_1, ..., a_n\} \not\subset K$ an den Körper K möglich. $K(A) = K(a_1, ..., a_n)$ ist dann der kleinste Körper, der K und $\{a_1, ..., a_n\}$ enthält.
Die Darstellung von $K(a_1, ..., a_n)$ mit Polynomen begründet sich aus der schrittweisen Adjunktion von $a_1, ..., a_n$ an K:
Seien $a_1, ..., a_n$ über K algebraisch. Für ein beliebiges a_l, $l \in \{1, ..., n\}$, ist die Gleichheit

$$K(a_1, ..., a_l) = K(a_1, ..., a_{l-1})(a_l) = K(a_1, ..., a_{l-1})[a_l]$$

erfüllt.[[A]S.374; [B]S.82]
An K adjungieren wir Schritt für Schritt die Elemente a_1 bis a_n und erhalten mit der obigen Gleichheit:

$$K(a_1, ..., a_n) = K[a_1, ..., a_n] = \{g(a_1, ..., a_n) : \quad g \in K[\vec{x}]\}$$

Wir werden die Galoisgruppe einer Körpererweiterung, die speziell der Zerfällungskörper eines Polynoms ist, betrachten:

3.1.3 Zerfällungskörper

Sei $f \in K[x]$ ein normiertes, separables Polynom mit $deg(f) = n$. f habe n unterschiedliche und einfache Nullstellen $\alpha_1, ..., \alpha_n$. Man nennt einen Erweiterungskörper $L \supset K$ **Zerfällungskörper** von f, falls er der kleinste Körper ist, in dem f über L in Linearfaktoren zerfällt. Also:

1. $\alpha_1, ..., \alpha_n \in L$: $\quad f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot ... \cdot (x - \alpha_n)$
2. $\nexists \tilde{L}$ mit $K \subset \tilde{L} \subsetneq L$ in dem f in Linearfaktoren zerfällt.

Fazit: L ist der kleinste Körper, der K und $\{\alpha_1, ..., \alpha_n\}$ enthält.
$L = K(\alpha_1, ..., \alpha_n) = K(\vec{\alpha})$ [[A]S.415]

3.2 Definition

Nachdem wir einige in der Definition gebräuchliche Begriffe eingeführt haben, können wir die Galoisgruppe betrachten.

Definition 3.1. Galoisgruppe
Die **Galoisgruppe einer Körpererweiterung** $L \supset K$ bildet sich aus denjenigen Automorphismen der Körpers L, die die Elemente aus dem Körper K fix lassen. Die Galoisgruppe wird mit $Gal(L, K)$ bezeichnet:

$$\boxed{Gal(L, K) \quad := \quad \{\sigma \in \mathrm{Aut}(L) : \quad \sigma|_K = id_K\}}$$

Beispielsweise bestimmen wir die Galoisgruppe der Körpererweiterung $\mathbb{C} \supset \mathbb{R}$ [[B]S.82]:
Die Automorphismen der Galoisgruppe $Gal(\mathbb{C}, \mathbb{R})$ lassen $\mathbb{R}$ fix.
Sei $\phi \in Gal(\mathbb{C}, \mathbb{R})$, da $\phi(i)^2 = \phi(i^2) = \phi(-1) = -1$ ist

$$\phi(i) = +i \quad \text{oder} \quad \phi(i) = -i.$$

Und mit $\phi(x + iy) = \phi(x) + \phi(i)\phi(y)$, $x, y \in \mathbb{R}$, ist

$$\phi(x + iy) = x + iy \quad \text{oder} \quad \phi(x + iy) = x - iy.$$

Also ist ϕ die Identität oder die komplexe Konjugation:

$$Gal(\mathbb{C},\mathbb{R}) = \{id, \phi_k\} \quad \text{mit } \phi_k(x) = \bar{x}$$

Wir betrachtetn nun die Galoisgruppe von $L \supset K$ für ein Erweiterungskörper L, der Zerfällungskörper eines separablen Polynoms $f \in K[x]$ ist. Es besteht die Möglichkeit, dass zwei oder mehrere irreduzible Faktoren von f die gleiche Nullstelle haben.
Unsere Forderung an f ist mehr: Wie im vorherigen Kapitel betrachten wir Polynome, die nur einfache Nullstellen haben. Seien also $\alpha_1, ..., \alpha_n$ getrennte[11] Nullstellen von f und $L = K(\alpha_1, ..., \alpha_n)$.

Wir stellen uns die Frage: Was genau machen die Elemente von $Gal(K(\vec{\alpha}), K)$?

Da $\sigma \in Gal(L,K)$ ein Automorphismus ist, bildet σ die Nullstellen von f bijektiv aufeinander ab:

Satz 3.1. *Die Menge der Nullstellen bleibt unter der Wirkung der Galoisgruppe invariant. Für $\sigma \in Gal(L,K)$ gilt also:*

$$\sigma(W_f) = W_f \quad \textit{mit } W_f := \{\alpha_1, ..., \alpha_n\}$$

Beweis. Seien $\alpha_1, ..., \alpha_n$ die Nullstellen von f, $\quad f(\alpha_i) = 0$ mit $i \in \{1, ..., n\}$.
Für $f(x) := \sum_{i=0}^{n} a_i x^i$ gilt $(\sigma \circ f)(x) = f(\sigma x) \quad \forall x \in L$:

$$\sigma(f(x)) = \sigma(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \underbrace{\sigma(a_i)}_{=a_i, \text{da } \sigma|_K = id_K} \sigma(x^i) \overset{\sigma(x^i)=\sigma(\overbrace{x\cdot ...\cdot x}^{i-mal})=\sigma(x)\cdot ...\cdot\sigma(x)}{=}$$
$$= \sum_{i=0}^{n} a_i (\sigma(x))^i = f(\sigma(x))$$

Da $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) \overset{\sigma Autom.}{=} 0$ folgt also:

$$\sigma(\{\alpha_1, ..., \alpha_n\}) \subset \{\alpha_1, ..., \alpha_n\} \qquad (**)$$

Ein Automorphismus ist umkehrbar: $\sigma^{-1} := \tau$ ist wieder ein Automorphismus. Dann ist wie in (**) $\quad \tau(\{\alpha_1, ..., \alpha_n\}) \subset \{\alpha_1, ..., \alpha_n\}$

$$\Rightarrow \quad \underbrace{\sigma(\tau(\{\alpha_1, ..., \alpha_n\}))}_{=\{\alpha_1,...,\alpha_n\}} \subset \sigma(\{\alpha_1, ..., \alpha_n\}) \quad \Rightarrow \quad \{\alpha_1, ..., \alpha_n\} \subset \sigma(\{\alpha_1, ..., \alpha_n\})$$

Folglich erhalten wir die Gleichheit: $\quad \sigma(\{\alpha_1, ..., \alpha_n\}) = \{\alpha_1, ..., \alpha_n\}$ □

Damit haben wir gezeigt, dass die Nullstellenmenge eines Polynoms unter den Elementen der Galoisgruppe erhalten bleibt. Also: G wirkt auf die Nullstellenmenge W_f.

Jedes Element der Galoisgruppe $\sigma \in Gal(L,K)$ ist durch seine Wirkung auf die Wurzelmenge eindeutig bestimmt, da $L = K(\alpha_1, ..., \alpha_n)$. Mit der Eindeutigkeit von $\sigma(\alpha_1), ..., \sigma(\alpha_n) \in W_f$ und $\sigma|_K = id_K$ wissen wir, wie $L = K(\alpha_1, ..., \alpha_n)$ unter σ abgebildet wird.

$$\psi \quad : \begin{cases} Gal(L,K) \to S_{W_f} \\ \sigma \mapsto \sigma|_{W_f} \end{cases} \quad \text{ist ein Gruppenhomomorphismus:}$$

[11] Für ein separables Polynom, das nur einfache Nullstellen hat, sprechen wir von getrennten Nullstellen.

Für $\sigma, \tau \in Gal(L,K)$ ist $\psi(\sigma \circ \tau) = \psi(\sigma) \circ \psi(\tau)$:

$$\psi(\sigma \circ \tau) = (\sigma \circ \tau)|_{W_f} = \sigma|_{W_f} \circ \tau|_{W_f} = \psi(\sigma) \circ \psi(\tau)$$

Im folgenden identifizieren wir die Permutation der Nullstellenmenge W_f unter σ mit der Permutation der Menge $\{1,...,n\}$, $S_{W_f} \cong S_n$: Für $\sigma|_{W_f} : W_f \to W_f$ definieren wir $\bar{\sigma} := \psi(\sigma) \in S_n$ mit $\bar{\sigma} : \{1,...,n\} \to \{1,...,n\} \quad \Rightarrow \sigma(\alpha_i) = \alpha_{\bar{\sigma} i}$

Behauptung 3.1. Der Homomorphismus ψ ist injektiv und $Gal(L,K)$ ist isomorph zu einer Untergruppe von S_n.

Beweis. Für $\sigma, \tau \in Gal(L,K)$ und $\psi(\sigma) = \psi(\tau)$ ist $\sigma = \tau$:
$\psi(\sigma) = \psi(\tau) \quad \Rightarrow \bar{\sigma} = \bar{\tau} \quad \Rightarrow \sigma(\alpha_i) = \tau(\alpha_i) \quad \forall i \in \{1,...,n\}$, d.h. σ und τ stimmen auf der Wurzelmenge $\{\alpha_1,...,\alpha_n\}$ überein.
Die Elemente von K werden von den Automorphismen der Galoisgruppe fix gelassen, $\sigma|_K = id_K = \tau|_K$. Also stimmen σ und τ auf K und auf der Nullstellenmenge überein.
Also gilt: $\sigma = \tau$ auf ganz $L = K(\alpha_1,...,\alpha_n)$ und damit folgt die Injektivität von ψ

$\psi : Gal(L,K) \to S_n$ ist ein injektiver Gruppenhomomorphismus und damit eine Einbettung von $Gal(L,K)$ in S_n. Für eine Isomorphie zwischen $Gal(L,K)$ und S_n ist die Surjektivität von ψ nicht gegeben. Jedoch wird ψ surjektiv, wenn wir die Bildmenge von ψ verkleinern, sodass diese nur die Elemente $\psi(Gal(L,K)) \subset S_n$ enthält. Die neue Bildmenge ist eine Untergruppe[12] von S_n und $\psi : Gal(L,K) \to \psi(Gal(L,K))$ ist bijektiv. □

Bemerkung 3.1. Zwei unterschiedliche Polynome in $K[x]$ haben die selbe Galoisgruppe, falls ihr Zerfällungskörper L gleich ist.

Der Lösungsweg, der zur Bestimmung der Galoisgruppe in den Beispielen verwendet wird, setzt eine wichtige Grundkenntnis über die Fortsetzung von Körperhomomorphismen voraus. Wir bestimmen die einzelnen Elemente der Galoisgruppe, indem wir ein Isomorphismus auf den Erweiterungskörper fortsetzen.

3.3 Fortsetzung von Körperhomomorphismen

Einschub: Seien K und K' zwei unterschiedliche Körper und sei f ein Polynom, dessen Koeffizienten in K liegen, $f \in K[x]$. Mit einem Ringhomomorphismus bildet man f auf ein Polynom ab, dessen Koeffizienten in K' liegen, indem man die Koeffizienten von f nach K' abbildet. Für einen Körperhomomorphismus $\mu : K \to K'$ sei dieser Ringhomomorphismus dann folgendermaßen definiert:

$$\begin{array}{rcl} K[x] \to K'[x] \qquad \text{mit} \quad f(x) & \mapsto & f^{\mu}(x) \\ a_n x^n + ... + a_0 & \mapsto & \mu(a_n)x^n + ... + \mu(a_0) \end{array}$$

Zuerst zeigen wir, dass die Fortsetzung eines Körperhomomorphismus Nullstellen auf Nullstellen abbildet:

[12] Allgemein gilt: Sei $\phi : G \to H$ ein Gruppenhomomorphismus, dann ist $im(\phi) = \phi(G) = \{\phi(g) | g \in G\}$ eine Untergruppe von H. [[A]S.141]

Lemma 3.1. *$L \supset K$ und $L' \supset K'$ seien Körpererweiterungen. ϕ sei ein Homomorphismus von L nach L' und die Fortsetzung von $\mu : K \to K'$. Für ein algebraisches Element $\alpha \in L$ sei $m_\alpha \in K[x]$ das zugehörige Minimalpolynom. Dann ist auch $\phi(\alpha) \in L'$ eine Nullstelle von $m_\alpha^\mu(x) \in K'[x]$.*

Beweis. $m_\alpha^\mu(\phi(\alpha)) = \sum_{j=0}^{n} \mu(a_j)\phi(\alpha)^j \overset{\phi|_K=\mu}{=} \sum_{j=0}^{n} \phi(a_j)\phi(\alpha)^j \overset{\phi Hom.}{=} \phi(\sum_{j=0}^{n} a_j\alpha^j) = \phi(0) = 0$

mit $m^\mu(x) = \sum_{j=0}^{n} \mu(a_j)x^j$ □

Im folgenden zeigen wir nun die Existenz eine Fortsetzung ϕ für jede weitere Nullstelle β von m_α mit $\phi(\alpha) = \beta$:

Satz 3.2. *Fortsetzungssatz*
Sei μ ein Körperhomomorphismus von K nach K'. $L \supset K$ und $L' \supset K'$ seien algebraische Körpererweiterungen. Für ein $\alpha \in L$ sei $m_\alpha \in K[x]$ das Minimalpolynom mit $deg(m_\alpha) > 1$. Eine Nullstelle des Minimalpolynoms $m_\alpha^\mu \in K'[x]$ sei $\beta \in L'$.
Dann existiert eine Fortsetzung ϕ von μ:

$$\phi : K(\alpha) \to K'(\beta) \quad \text{mit } \phi|_K = \mu \text{ und } \phi(\alpha) = \beta$$

Beweis. Seien die Voraussetzungen aus dem Satz gegeben. Man definiere eine Abbildung $\phi : K(\alpha) \to K'(\beta)$ mit $\phi(g(\alpha)) := g^\mu(\beta)$.

1. ϕ ist wohldefiniert: Sei $g(\alpha) = \tilde{g}(\alpha)$
$\Rightarrow$ $(g - \tilde{g})(\alpha) = 0$, da aber m_α das kleinste Polynom in $K[x]$ mit α als Nullstelle ist, gilt: m_α teilt $g - \tilde{g}$
Dann existiert ein $t \in K[x]$ mit $m_\alpha \cdot t = g - \tilde{g}$ $\Rightarrow m_\alpha^\mu \cdot t^\mu = (g - \tilde{g})^\mu$.
Mit β als Nullstelle von m_α^μ ist auch $(g-\tilde{g})^\mu(\beta) = m_\alpha^\mu(\beta)\, t^\mu(\beta) = 0$ $\Rightarrow$ $g^\mu(\beta) = \tilde{g}^\mu(\beta)$
Also ist $\phi(g(\alpha)) = \phi(\tilde{g}(\alpha))$

2. ϕ ist ein Homomorphismus: Sei $a, b \in K(\alpha)$, $a = g(\alpha)$ und $b = \tilde{g}(\alpha)$
$\phi(a + b) = \phi(g(\alpha) + \tilde{g}(\alpha)) = \phi((g + \tilde{g})(\alpha)) = (g + \tilde{g})^\mu(\beta) = g^\mu(\beta) + \tilde{g}^\mu(\beta) = \phi(g(\alpha)) + \phi(\tilde{g}(\alpha)) = \phi(a) + \phi(b)$
$\phi(ab) = \phi(g(\alpha)\tilde{g}(\alpha)) = \phi((g\tilde{g})(\alpha)) = (g\tilde{g})^\mu(\beta) = g(\beta)^\mu \tilde{g}^\mu(\beta) = \phi(g(\alpha))\phi(\tilde{g}(\alpha)) = \phi(a)\phi(b)$

Mit $\phi(\alpha) = \beta$ und $\phi(k) = \mu(k)$ für $k \in K$(d.h. $\phi|_K = \mu$) ist ϕ die gewünschte Fortsetzung von μ.
(Siehe auch $[[A]S.426 - 429]$) □

Bemerkung 3.2. Ist der Körperhomomorphismus μ aus dem Satz ein Isomorphismus, so ist die Fortsetzung von μ auch ein Isomorphismus:
$\phi|_K = \mu$ ist bijektiv und mit der Eindeutigkeit von $\phi(\alpha)$ bildet ϕ den Körper $K(\alpha)$ bijektiv auf $K'(\beta)$ ab.

Was hinter diesen Fortsetzungen im Bezug auf die Galoisgruppe steht, wird in den folgenden Beispielen im nächsten Kapitel deutlicher.

3.4 Beispiele

Beispiel 1:[13] $f(x) = x^3 - 2 \quad \in \mathbb{Q}[x]$

Die Linearfaktorzerlegung von f ist $f(x) = (x - \sqrt[3]{2})(x - \sqrt[3]{2}e^{\frac{2\pi i}{3}})(x - \sqrt[3]{2}(e^{\frac{2\pi i}{3}})^2)$ und der Zerfällungskörper von f über $\mathbb{Q}$ lautet:

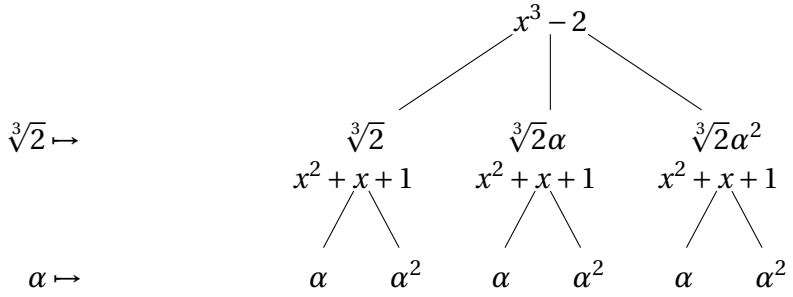
$$L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{\frac{2\pi i}{3}}, \sqrt[3]{2}(e^{\frac{2\pi i}{3}})^2) = \mathbb{Q}(\sqrt[3]{2}, \alpha) \quad \text{mit } \alpha = \zeta_3 = e^{\frac{2\pi i}{3}}$$

Mit Satz 3.2 bestimmen wir die Elemente der Galoisgruppe. Zuerst finden wir nun die Fortsetzungen von $\mu : \mathbb{Q} \to \mathbb{Q}$ mit $\mu = id_{\mathbb{Q}}$:

Minimalpolynom von $\sqrt[3]{2}$ über $\mathbb{Q}$:
$m_{\sqrt[3]{2},\mathbb{Q}}(x) = x^3 - 2$ ist irreduzibel[14] in $\mathbb{Q}[x]$ und ist das Polynom kleinsten Grades mit Nullstelle in $\sqrt[3]{2}$. Wir zerlegen $m_{\sqrt[3]{2},\mathbb{Q}} =: g_1$ in Linearfaktoren:
$g_1(x) = (x - \sqrt[3]{2})(x - \sqrt[3]{2}\alpha)(x - \sqrt[3]{2}\alpha^2)$ und $\sqrt[3]{2}\alpha^2$, $\sqrt[3]{2}\alpha$ und $\sqrt[3]{2}$ sind die Nullstellen des Minimalpolynoms.

Minimalpolynom von α über $\mathbb{Q}(\sqrt[3]{2})$:
Das erste Polynom kleinen Grades mit α als Nullstelle, das uns dabei in den Sinn kommt, ist das Polynom $p(x) = x^3 - 1$. Jedoch ist dieses nicht in $\mathbb{Q}(\sqrt[3]{2})[x]$ irreduzibel, da es $x - 1 \in \mathbb{Q}(\sqrt[3]{2})[x]$ als Teiler hat.
$m_{\alpha,\mathbb{Q}(\sqrt[3]{2})}(x) = x^2 + x + 1$ ist irreduzibel in $\mathbb{Q}(\sqrt[3]{2})[x]$ und das Polynom kleinsten Grades mit $m_{\alpha,\mathbb{Q}(\sqrt[3]{2})}(\alpha) = (e^{\frac{2\pi i}{3}})^2 + e^{\frac{2\pi i}{3}} + 1 = -\frac{1}{2} - \frac{\sqrt{3}}{2}i - \frac{1}{2} + \frac{\sqrt{3}}{2}i + 1 = 0$. Dieses $m_{\alpha,\mathbb{Q}(\sqrt[3]{2})} =: g_2$ zerlegen wir in Linearfaktoren: $g_2(x) = (x - \alpha)(x - \alpha^2)$. α und α^2 sind die Nullstellen von g_2.

Die Fortsetzungen von μ können wir nun an folgendem Baumdiagramm ablesen:



Man beachte, dass $\mu : \mathbb{Q} \to \mathbb{Q}$ mit $\mu = id_{\mathbb{Q}}$ und $g_2^{\mu} = g_2$.

Die Isomorphismen aus dem Baumdiagramm schreiben wir in einer Tabelle nieder:

[13] Die in diesem Beispielen verwendete Methode lehrte Arturo Mancino, ein ehemalige Mitarbeiter der Mathematischen Fakultät der Universität Augsburg.

[14] Diejenigen Polynome, die $m_{\sqrt[3]{2},\mathbb{Q}}$ teilen würden, sind nicht in $\mathbb{Q}[x]$ enthalten, da $\sqrt[3]{2} \notin \mathbb{Q}$.

	ϕ_1	ϕ_2	ϕ_3	ϕ_4	ϕ_5	ϕ_6
$\mathbb{Q}(\sqrt[3]{2},\alpha) \to$	$\mathbb{Q}(\sqrt[3]{2},\alpha)$	$\mathbb{Q}(\sqrt[3]{2},\alpha^2)$	$\mathbb{Q}(\sqrt[3]{2}\alpha,\alpha)$	$\mathbb{Q}(\sqrt[3]{2}\alpha,\alpha^2)$	$\mathbb{Q}(\sqrt[3]{2}\alpha^2,\alpha)$	$\mathbb{Q}(\sqrt[3]{2}\alpha^2,\alpha^2)$
$\sqrt[3]{2} \mapsto$	$\sqrt[3]{2}$	$\sqrt[3]{2}$	$\sqrt[3]{2}\alpha$	$\sqrt[3]{2}\alpha$	$\sqrt[3]{2}\alpha^2$	$\sqrt[3]{2}\alpha^2$
$\alpha \mapsto$	α	α^2	α	α^2	α	α^2

Da $\mathbb{Q}(\sqrt[3]{2},\alpha) = \mathbb{Q}(\sqrt[3]{2},\alpha^2)$, $\mathbb{Q}(\sqrt[3]{2}\alpha,\alpha) = \mathbb{Q}(\sqrt[3]{2},\alpha)$ und $\mathbb{Q}(\sqrt[3]{2}\alpha^2,\alpha) = \mathbb{Q}(\sqrt[3]{2},\alpha)$, sind diese sechs Fortsetzungen von μ auf den Körper L Automorphismen, also die Elemente der Galoisgruppe der Körpererweiterung $L \supset K$.

Also lautet die Galoisgruppe:

$$G(\mathbb{Q}(\sqrt[3]{2},\alpha),\mathbb{Q}) = \{id = \phi_1, \phi_2, \phi_3, \phi_4, \phi_5, \phi_6\}$$

Beispiel 2: $L = \mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$

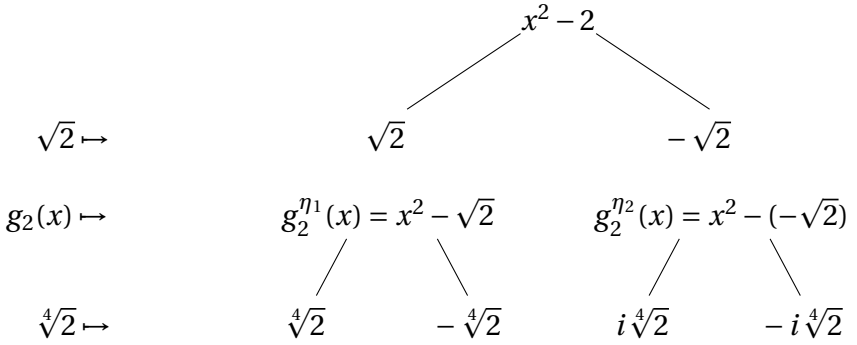
Man beachte, dass L kein Zerfällungskörper eines Polynoms in $\mathbb{Q}[x]$ ist.

Zur Bestimmung der Automorphismen der Galoisgruppe ziehen wir uns wieder Satz 3.2 zur Hilfe und bestimmen zuerst die Fortsetzungen von $\mu : \mathbb{Q} \to \mathbb{Q}$ mit $\mu = id_{\mathbb{Q}}$ auf den Körper $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$:

Minimalpolynom von $\sqrt{2}$ über $\mathbb{Q}$:
$m_{\sqrt{2},\mathbb{Q}}(x) = x^2 - 2$ ist das Polynom kleinsten Grades mit $\sqrt{2}$ als Nullstelle und ist irreduzibel, da es in $\mathbb{Q}$ keine Nullstellen hat. $g_1(x) := m_{\sqrt{2},\mathbb{Q}}(x) = (x+\sqrt{2})(x-\sqrt{2})$ zerfällt über $\mathbb{Q}(\sqrt{2})$ in Linearfaktoren und hat die Nullstellen $\sqrt{2}, -\sqrt{2} \in \mathbb{Q}(\sqrt{2})$.

Minimalpolynom von $\sqrt[4]{2}$ über $\mathbb{Q}(\sqrt{2})$:
$g_2(x) := m_{\sqrt[4]{2},\mathbb{Q}(\sqrt{2})}(x) = x^2 - \sqrt{2}$ ist irreduzibel in $\mathbb{Q}(\sqrt{2})[x]$, da es in $\mathbb{Q}(\sqrt{2})$ keine Nullstellen hat. g_2 zerfällt über $\mathbb{Q}(\sqrt{2}, \sqrt[4]{2})$ in Linearfaktoren.

Wie in dem vorherigen Beispiel lesen wir die Fortsetzungen von μ an unserem Baumdiagramm ab:



Wir erhalten folgende Isomorphismen:

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
$\mathbb{Q}(\sqrt{2},\sqrt[4]{2})\to$	$\mathbb{Q}(\sqrt{2},\sqrt[4]{2})$	$\mathbb{Q}(\sqrt{2},-\sqrt[4]{2})$	$\mathbb{Q}(-\sqrt{2},i\sqrt[4]{2})$	$\mathbb{Q}(-\sqrt{2},-i\sqrt[4]{2})$
$\sqrt{2}\mapsto$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
$\sqrt[4]{2}\mapsto$	$\sqrt[4]{2}$	$-\sqrt[4]{2}$	$i\sqrt[4]{2}$	$-i\sqrt[4]{2}$

Nicht jede dieser vier Isomorphismen ist auch ein Automorphismus von $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})$: Da $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})\neq\mathbb{Q}(\sqrt{2},i\sqrt[4]{2})$ sind ϕ_3 und ϕ_4 keine Automorphismen. Mit $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})=\mathbb{Q}(\sqrt{2},-\sqrt[4]{2})$ sind ϕ_1 und ϕ_2 die einzigen Automorphismen.
Also lautet die Galoisgruppe der Körpererweiterung $\mathbb{Q}(\sqrt{2},\sqrt[4]{2})\supset\mathbb{Q}$:

$$Gal(\mathbb{Q}(\sqrt{2},\sqrt[4]{2}))=\{\phi_1,\phi_2\}$$

Beispiel 3: $f(x)=x^4+1\in\mathbb{Q}[x]$

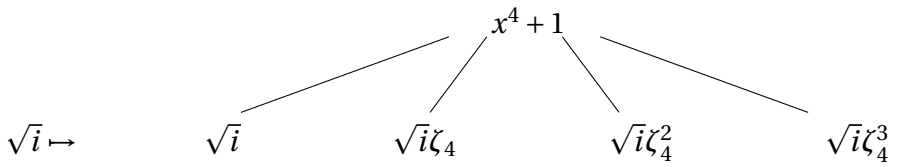
$f(x)=x^4+1=(x-\sqrt{i})(x-\sqrt{i}\zeta_4)(x-\sqrt{i}\zeta_4^2)(x-\sqrt{i}\zeta_4^3)$ mit $\zeta_4:=e^{\frac{2\pi i}{4}}$ ist die Linearfaktorzerlegung und $\mathbb{Q}(\sqrt{i})$ der Zerfällungskörper von f. Man beachte: $\zeta_4\in\mathbb{Q}(\sqrt{i})$, da $\sqrt{i}=e^{\frac{i\pi}{4}}$ und $\zeta_4=\sqrt{i}^2$.

Aus den Fortsetzungen von $\mu:\mathbb{Q}\to\mathbb{Q}$ mit $\mu=id_{\mathbb{Q}}$, die wir mit Satz 3.2 erhalten, bestimmen wir die Elemente der Galoisgruppe der Körpererweiterung $\mathbb{Q}(\sqrt{i})\supset\mathbb{Q}$.

Minimalpolynom von $\sqrt{i}$ über $\mathbb{Q}$:
$m_{\sqrt{i},Q}(x)=x^4+1$ ist das Polynom kleinsten Grades, welches $\sqrt{i}$ als Nullstelle hat und es ist irreduzibel:
Wir betrachte zunächst die Irreduzibilität des Polynoms $f(x+1)=(x+1)^4+1$.

$$f(x+1)=(x^2+2x+1)(x^2+2x+1)+1=x^4+4x^3+6x^2+4x+2$$

Für $p:=2\in\mathbb{Q}$ ist $f(x+1)$ nach dem Eisenstein-Kriterium (Siehe [[A]S.337]) irreduzibel, da p die Koeffizienten $4,6,4,2$ teilt und p^2 den letzten Koeffizienten 2 nicht teilt.
Da $f(x+1)$ irreduzibel ist, ist auch $f(x)$ irreduzibel in $\mathbb{Q}[x]$, [[E]S.90].
Wir können $g_1:=m_{\sqrt{i},Q}$ in Linearfaktoren zerlegen:
$g_1(x)=(x-\sqrt{i})(x-\sqrt{i}\zeta_4)(x-\sqrt{i}\zeta_4^2)(x-\sqrt{i}\zeta_4^3)$ und $\sqrt{i},\sqrt{i}\zeta_4,\sqrt{i}\zeta_4^2$ und $\sqrt{i}\zeta_4^3$ sind die Nullstellen von g_1.



Aus diesem Baumdiagramm lesen wir die Fortsetzungen von μ auf den Körper $\mathbb{Q}(\sqrt{i})$ ab. Diese Isomorphismen schreiben wir nun in eine Tabelle:

	ϕ_1	ϕ_2	ϕ_3	ϕ_4
$\mathbb{Q}(\sqrt{i}) \rightarrow$	$\mathbb{Q}(\sqrt{i})$	$\mathbb{Q}(\sqrt{i\zeta_4})$	$\mathbb{Q}(\sqrt{i\zeta_4^2})$	$\mathbb{Q}(\sqrt{i\zeta_4^3})$
$\sqrt{i} \mapsto$	$\sqrt{i}$	$\sqrt{i\zeta_4}$	$\sqrt{i\zeta_4^2}$	$\sqrt{i\zeta_4^3}$

Da $\mathbb{Q}(\sqrt{i\zeta_4}), \mathbb{Q}(\sqrt{i\zeta_4^2}), \mathbb{Q}(\sqrt{i\zeta_4^3}) = \mathbb{Q}(\sqrt{i})$, sind ϕ_1, ϕ_2, ϕ_3 und ϕ_4 Automorphismen und die Elemente der Galoisgruppe.

Also:

$$Gal(\mathbb{Q}(\sqrt{i}), \mathbb{Q}) = \{\phi_1, \phi_2, \phi_3, \phi_4\}$$

Setzt man die Nullstellen von f in diese Automorphismen ein, so sieht man eingeschränkt auf der Nullstellenmenge die Gleichheit der Automorphismen zu den Permutationen aus dem Beispiel 1 in Kapitel 2.8.

4 Gleichheit der Definitionen

Die Galoisgruppe einer Körpererweiterung stimmt mit der Galoisgruppe eines Polynoms,die in Kapitel 3.2 beziehungsweise 2.5 definiert wurden, überein. Genauer ist $\psi(Gal^{\text{alt}}) = Gal^{\text{neu}}$. Dies wird im folgenden Satz bewiesen [[B] S.84]:

Satz 4.1. *Gleichheit der Definitionen*
Das Polynom $f \in K[x]$ habe getrennte Nullstellen $\alpha_1, ..., \alpha_n$ und $L = K(\vec{\alpha})$ sei der Zerfällungskörper von f. Die Menge der Relationen zwischen den Nullstellen sei $R := \{H \in K[\vec{x}] | H(\vec{\alpha}) = 0\}$ und $G := Gal(L, K)$ sei die Galoisgruppe der Körpererweiterung $L \supset K$. $\psi : G \to S_n$ ist die Abbildung mit $\sigma \mapsto \bar{\sigma}$. Dann gilt:

$$\psi(G) = G_R := \{\bar{\sigma} \in S_n | \quad \bar{\sigma} H \in R \quad \forall H \in R\}$$

Beweis. "$\subset$" Sei $\sigma \in G$ und $\psi(\sigma) = \bar{\sigma} \in S_n$
Dann ist $(\sigma\alpha_1, ..., \sigma\alpha_n) = (\alpha_{\bar{\sigma}1}, ..., \alpha_{\bar{\sigma}n})$
Da die Koeffizienten der Relationen $H \in R$ unter den Automorphismen von G fix gelassen werden, gilt: $\sigma(H(\alpha_1, ..., \alpha_n)) = H(\alpha_{\bar{\sigma}1}, ..., \alpha_{\bar{\sigma}n})$
$\Rightarrow \quad (\bar{\sigma} H)(\vec{\alpha}) = H(\bar{\sigma}\alpha_1, ..., \bar{\sigma}\alpha_n) = H(\alpha_{\bar{\sigma}1}, ..., \alpha_{\bar{\sigma}n}) = \sigma(H(\alpha_1, ..., \alpha_n)) = \sigma(0) = 0$
Also ist: $\bar{\sigma} \in G_R$ und damit $\psi(G) \supset G_R$

"$\supset$" Sei $\bar{\sigma} \in G_R$
Zu zeigen: Es gibt ein $\sigma \in G$, sodass $\sigma(\alpha_i) = \alpha_{\bar{\sigma}i} \quad \forall i \in \{1, ..., n\}$ und $\sigma|_K = id_K$.
Uns ist bekannt, wie die Elemente von $L = K(\vec{\alpha})$ aussehen: Sei $g(\vec{\alpha})$ mit $g \in K[\vec{x}]$ ein solches Element. Dann definieren wir $\sigma(g(\vec{\alpha})) := (\bar{\sigma} g)(\vec{\alpha})$ wobei $(\bar{\sigma} g)(\vec{\alpha}) = g(\bar{\sigma}\vec{\alpha})$ ist. Da unter $\bar{\sigma}$ die Nullstellenmenge $\{\alpha_1, ..., \alpha_n\}$ erhalten bleibt, ist $g(\bar{\sigma}\vec{\alpha}) \in L$ und damit $\sigma : L \to L$. Da $\bar{\sigma}$ nur die Nullstellen permutiert, lässt σ die Elemente des Körpers K fix.

Wir müssen die Wohldefiniertheit von σ zeigen, d.h. verschiedene Beschreibungen eines Elements in L werden mit σ auf den selben Wert zugewiesen: Sei $\tilde{g}(\vec{\alpha}) = g(\vec{\alpha})$ mit $\tilde{g}, g \in K[\vec{x}]$.
Dann definieren wir mit $g(\vec{\alpha}) - \tilde{g}(\vec{\alpha}) = 0$ eine Relation zwischen den Nullstellen $\alpha_1, ..., \alpha_n$: $\quad H := g - \tilde{g} \quad \in R$. Da $\bar{\sigma} \in G_R$ ist auch $\bar{\sigma} H$ eine Relation in R.
$\Rightarrow \quad (\bar{\sigma} H)(\vec{\alpha}) = H(\alpha_{\bar{\sigma}1}, ..., \alpha_{\bar{\sigma}n}) = g(\alpha_{\bar{\sigma}1}, ..., \alpha_{\bar{\sigma}n}) - \tilde{g}(\alpha_{\bar{\sigma}1}, ..., \alpha_{\bar{\sigma}n}) = 0$
$\Rightarrow \quad (\bar{\sigma} g)(\vec{\alpha}) = (\bar{\sigma}\tilde{g})(\vec{\alpha}) \qquad \Rightarrow \quad \sigma(g(\vec{\alpha})) = \sigma(\tilde{g}(\vec{\alpha}))$
Also ist σ ist wohldefiniert.

□

5 Vergleich

Sei $G^{neu} := \{\sigma \in \text{Aut}(L) : \quad \sigma|_K = id_K\}$ und $G^{alt} := \{\sigma \in S_n : \quad \sigma H \in R \quad \forall H \in R\}$. In den vorherigen Kapiteln haben wir die Galoisgruppe betrachtet und die Gleichheit von G^{alt} und G^{neu} gesehen. Nun sollten wir G^{alt} und G^{neu} gegeneinander abwägen.

Ein Unterschied liegt in der Verständlichkeit der beiden Beschreibungen der Galoisgruppe: Die Fülle der Begriffe, die notwendig sind, um G^{alt} zu beschreiben, ist umfangreich. Nachdem wir die elementar-symmetrischen Polynome und den Begriff Diskriminante eingeführt haben, musste für das richtige Verständnis von G^{alt} die Symmetriegruppe und der damit verbundene Relationenbegriff genau betrachtet werden. Zudem war es notwendig die Wirkung der Permutationen auf die Relationen zu analysieren.
Hier ist G^{neu} deutlich im Vorteil, da es für ein richtiges Verständnis ausreichend war die Begriffe Automorphismus, Körpererweiterung und Zerfällungskörper einzuführen.

Die Verfahren zur Bestimmung von G^{alt} und G^{neu} weisen einige Vor- und Nachteile auf:
Bei der Bestimmung mit G^{neu} ist es notwendig, zuerst den Zerfällungskörper des Polynoms zu finden. Die Unkenntnis über die Nullstellen bereitet uns hier gewisse Schwierigkeiten.
Eine weitere Schwierigkeit ist folgende: Die Reihenfolge, in der wir die Elemente adjungieren, muss geschickt gewählt werden, damit die Bestimmung der zugehörigen Minimalpolynome so einfach wie möglich wird. Zudem ist die Irreduzibilität der Minimalpolynome nicht immer einfach zu zeigen.
Vorteilhaft ist jedoch, dass nach einer geschickten Wahl und der Bestimmung der Minimalpolynome der adjungierten Elemente eine sehr schnelle und einfache Bestimmung der Elemente von G^{neu} folgt. Außerdem ist ein weiterer Vorteil, dass alle Polynome, die über dem gleichen Körper zerfallen, die gleiche Galoisgruppe haben.
Mit G^{neu} bestimmen wir nicht nur die Galoisgruppe eines Polynoms, sondern viel allgemeiner die Galoisgruppe einer beliebigen Körpererweiterung, siehe Beispiel 2 in 3.4.

Zur Bestimmung von G^{alt} brauchen wir zuerst die Relationenmenge und hier tauchte die Schwierigkeit auf eine vollständigen Relationenmenge festzulegen.
Die Aussage über die Gleicheit von G^{alt} zweier unterschiedlichen Polynome ist nicht unbedingt trivial: Trotz unterschiedlicher Relationenmengen besteht die Möglichkeit einer Gleichheit, falls die Permutationen, unter denen die Relationen erhalten bleiben, gleich sind.

Die Notwendigkeit der Kenntnis über die Nullstellen liefert uns einen weiteren Unterschied: Die Relationenmenge in G^{alt} ist auch ohne Nullstellen bestimmbar, wohingegen die Bestimmung des Zerfällungskörpers L einer Kenntnis bedarf.

Bei der Bestimmung von G^{alt} mit Hilfe eines primitiven Elements können Schwierigkeiten dabei auftreten, das Minimalpolynom eines primitives Elements und seine Galois-Konjugierten zu finden. Es ist nicht unbedingt einfach ein Polynom über einen

bestimmten Körper zu finden, welches ein primitives Element als Nullstelle hat, und dessen Irreduzibilität nachzuweisen.

Es stellt sich nun folgenden Frage:
Welche Art die Galoisgruppe zu bestimmen ist nun die Bessere?
Nachdem in dieser Arbeit ein Einblick in beide Verfahren gewährt wurde, kann jeder diese Frage individuell beantworten. Die Beschreibung von G^{alt} ist für das Gebiet der Geometrie passend. Vor allem das Beispiel $x^n + 1$ stellt man sich gerne geometrisch vor: Die Nullstellen dieses Polynoms liegen auf dem Einheitskreis. Verbindet man jeweils benachbarte Nullstellen, so erhält man ein n-Eck. Die Permutationen der Galoisgruppe ordnen die Nullstellen, also die Ecken des Vielecks um, ohne die Verbindungen zwischen den Ecken zu verändern.
Die Beschreibeung von G^{neu} hingegen ist eine algebraische: Die Elemente der Galoisgruppe beschrieben als bijektive Automorphismen, die die Nullstellenmenge eines Polynoms in ihrem Bild nicht verändern.

Fazit für mich: Auch wenn die Bestimmung von G^{neu} mir leichter fiel, hatte ich mehr Gefallen an der Bestimmung von G^{alt}. Denn bei dieser tauchten immer wieder Schwierigkeiten auf, doch man hatte einen Weg sie zu beheben. Und es ist beeindruckend, dass Galois sich diesen Schwierigkeiten bereits bewusst war und sie lösen konnte. Zudem ist es fazinierend, dass Galois' Erfindung die heutigen Mathematiker immer noch beschäftigt und bis heute noch ein aktuelles Thema ist.

Literaturverzeichnis

[*A*] Michael Holz, Repetitorium Algebra, 3. Auflage, Binomi Verlag 2010
[*B*] J.-H. Eschenburg, Skriptum: Einführung in die Algebra, Universität Augsburg, So-Se2014
[*C*] Christian Karpfinger, Kurt Meyberg; Algebra Gruppen-Ringe-Körper 3. Auflage, Springer 2013
[*D*] Gerd Fischer; Lehrbuch der Algebra, 2. Auflage, Vieweg+Teubner 2011
[*E*] Marc Nieper-Wißkirchen; Lehrbuch: Galoissche Theorie, Dezember 2013
[*F*] Joseph Rotman; Galois Theory, 2. Auflage, Springer
[*G*] Harold M. Edwards; Galois Theory, Springer
[*H*] http://de.wikipedia.org/wiki/EvaristeGalois