Galois-Theorie Anfänge

Evariste Galois (1811-1832) entdeckte als 20-Jähriger, dass mit dem Gleichungsauflösen durch Wurzelterme eine wiederholte Untergruppenbildung einer speziellen Permutationsgruppe der Lösungen (Galois-Gruppe) einhergeht. Emil Artin (1898-1962) bewies um 1930 auf völlig neuartige Weise diesen Zusammenhang. Er erwies sich von grundlegender Bedeutung für die Untersuchung algebraischer Strukturen.

Wir gehen von der biquadratischen Gleichung

$x^4 - 5x^2 + 3 = 0$ aus und deren (mit $u = x^2$ einfach zu ermittelnden) Lösungen:

$$x_{1/2} = \pm\sqrt{10 + 2\sqrt{13}}$$
$$x_{3/4} = \pm\sqrt{10 - 2\sqrt{13}}$$

Daher gilt (Satz von Viëta):

$$\begin{aligned} x^4 - 5x^2 + 3 &= (x - x_1)(x - x_2)(x - x_3)(x - x_4) \\ &= x^4 - (x_1 + x_2 + x_3 + x_4)x^3 \\ &\quad + (x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4)x^2 \\ &\quad - (x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4)x + x_1x_2x_3x_4 \end{aligned}$$

und insbesondere für die Gleichung:

$$\begin{aligned} x_1 + x_2 + x_3 + x_4 &= 0 \\ x_1x_2 + x_1x_3 + x_2x_3 + x_1x_4 + x_2x_4 + x_3x_4 &= -5 \\ x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 &= 0 \\ x_1x_2x_3x_4 &= 3 \end{aligned}$$

An der Zerlegung der Gleichung in Linearfaktoren ist zu erkennen, dass diese Identitäten auch bei einer Vertauschung (Permutierung) der Lösungen bestehen bleiben. Entsprechende Überlegungen können für jede Gleichung mit verschiedenen Lösungen angestellt werden. Die 4! Permutationen bilden eine Gruppe.

Beziehungen, die charakteristischer für die Lösungen sind, lauten:

$$\begin{aligned} x_1 + x_2 &= 0 & x_2^2 \cdot x_3^2 &= 3 \\ x_3 + x_4 &= 0 & x_2^2 \cdot x_4^2 &= 3 \\ x_1^2 \cdot x_3^2 &= 3 & (2x_1x_2 + 5)^2 &= 13 \\ x_1^2 \cdot x_4^2 &= 3 & (2x_3x_4 + 5)^2 &= 13 \end{aligned}$$

Galois-Gruppe

Wenn wir jetzt nur an denjenigen Permutationen interessiert sind, die diese Identitäten berücksichtigen, d. h. die Identitäten in sich oder auf andere überführen, so fallen von den 4! die meisten heraus und es verbleibt die 8-elementige Gruppe, die von $\sigma_1 = (12)$ und $\sigma_2 = (1324)$ erzeugt wird und zusätzlich die Permutationen $\sigma_1^2,\ \sigma_2^2,\ \sigma_2^3,\ \sigma_2 \circ \sigma_1$ (zuerst σ_1), $\sigma_2^2 \circ \sigma_1,\ \sigma_2^3 \circ \sigma_1$ enthält:

$$\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \qquad \sigma_2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix} \qquad \sigma_1^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} = \mathrm{id}$$

$$\sigma_2^2 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\sigma_2^3 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix}$$

$$\sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

$$\sigma_2^2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$\sigma_2^3 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Diese Permutationen berücksichtigen alle polynomialen Lösungs-Beziehungen mit Koeffizienten in $\mathbb{Q}$. Sie bilden daher die Galois-Gruppe G der Gleichung

$x^4 - 5x^2 + 3 = 0.$

Nach Galois kann der Nachweis mit einem Polynom erfolgen (Algebraische Körpererweiterung),

$$\prod_{\tau \in G} \left(t - (m_1 x_{\tau(1)} + m_2 x_{\tau(2)} + m_3 x_{\tau(3)} + m_4 x_{\tau(4)}) \right) = t^8 - 100t^6 + 3118t^4 - 30900t^2 + 5625$$

wobei die m_i so gewählt werden, dass die Terme $m_1 x_{\tau(1)} + m_2 x_{\tau(2)} + m_3 x_{\tau(3)} + m_4 x_{\tau(4)}$ für alle 4! Permutationen paarweise verschieden sind, hier z. B. $m_1 = 1$, $m_2 = -2$, $m_3 = 3$, $m_4 = 4$.
Man beachte, dass das Polynom dann stets ganzzahlig ist.

Wir nähern uns schrittweise den Lösungen und fügen $\mathbb{Q}$ die Wurzel $\sqrt{13}$ hinzu. Nun sind zusätzlich aussagekräftigere Beziehungen wie

$2x_1x_2 + 5 = \sqrt{13}$

$2x_3x_4 + 5 = \sqrt{13}$

möglich. Sie werden nur noch von der Hälfte der Permutationen berücksichtigt, und zwar von der Galois-Untergruppe: $\sigma_1^2 = \mathrm{id},\ \sigma_2^2,\ \sigma_2 \circ \sigma_1,\ \sigma_2^3 \circ \sigma_1$. Es kann bewiesen werden, dass das Adjungieren einer m-ten Wurzel die Galoisgruppe auf den m-ten Teil verkleinert. Das sukzessive Hinzufügen der Wurzeln $\sqrt{10 + 2\sqrt{13}}$ und $\sqrt{10 - 2\sqrt{13}}$ führt wegen der weiteren zwei Halbierungen zur Identität.

Galois-Gruppe

Wie sehr die Galois-Gruppe die Eigenschaften der Lösungen erfasst,
zeigt die biquadratische Gleichung

$x^4 - 5x^2 + 5 = 0$ mit den Lösungen:

$$x_{1/2} = \pm\frac{1}{2}\sqrt{10 + 2\sqrt{5}}$$
$$x_{3/4} = \pm\frac{1}{2}\sqrt{10 - 2\sqrt{5}}$$

Die Galois-Gruppe besteht aus lediglich 4 Elementen: $\sigma = (1324)$, σ^2, σ^3, $\sigma^4 = \mathrm{id}$
Maple verfügt über die Anweisung galois$(x^4 - 5x^2 + 5)$.
Es muss zwei polynomiale Lösungs-Terme geben, die mit der Permutation (12) nicht verträglich sind. Wir finden:

$$x_1x_3(x_1^2 - x_3^2) = 5$$
$$x_2x_3(x_2^2 - x_3^2) = -5$$

Im Unterschied zur vorigen Gleichung $x^4 - 5x^2 + 3 = 0$ kann z.B. x_3 durch x_1 ausgedrückt werden:

$$\sqrt{10 - 2\sqrt{5}} = \frac{4\sqrt{5}}{\sqrt{10 + 2\sqrt{5}}}$$

Im Körper $\mathbb{Q}(\sqrt{5}, \sqrt{10 + 2\sqrt{5}})$ sind daher schon alle Lösungen enthalten.

Die Adjunktion von $\sqrt{5}$ zu $\mathbb{Q}$ führt zur zweielementigen Galois-Untergruppe $\{\mathrm{id}, \sigma^2\}$.
σ^3 fällt heraus, beachte hierzu:

$$x_1x_3 = \sqrt{5}$$
$$x_2x_4 = \sqrt{5}$$
$$x_1x_4 = -\sqrt{5}$$
$$x_2x_3 = -\sqrt{5}$$

Jede Permutation der Galois-Gruppe kann auf genau eine Weise zu einem Automorphismus von $\mathbb{Q}(x_{1/2}, x_{3/4})$ (Zerfällungskörper), der die Elemente von $\mathbb{Q}$ festlässt und die x_i vertauscht, fortgesetzt werden. Die Bezeichnung wird beibehalten.

$$\sigma^2(\sqrt{5}) = \sigma^2(x_1)\sigma^2(x_3) = x_2x_4 = \sqrt{5}$$

legt die Vermutung nahe, dass der Fixpunktkörper der Automorphismen-Untergruppe $\{\mathrm{id}, \sigma^2\}$ der Körper $\mathbb{Q}(\sqrt{5})$ ist. Er besteht aus allen Elementen $a + b\sqrt{5}$ mit $a, b \in \mathbb{Q}$.
Quotienten können diese Form auch annehmen (erweitern und 3. binomische Formel beachten).

Dass $\mathbb{Q}(\sqrt{5})$ der Fixpunktkörper von $\{\mathrm{id}, \sigma^2\}$ ist, kann mit der Galois-Theorie nach Artin mit

$[\mathbb{Q}(x_{1/2}, x_{3/4}) : \mathbb{Q}(\sqrt{5})] = |\{\mathrm{id}, \sigma^2\}| = 2$ bestätigt werden.

Allgemein gehört zu jeder Untergruppe der Galois-Gruppe ein Zwischenkörper (Fixpunktkörper). Die Umkehrung gilt auch. Sie ist eindeutig.

Galois-Theorie Anfänge

Die Automorphismen der Galois-Gruppe bilden $\mathbb{Q}(\sqrt{5})$ auf sich ab, da mit
$\sqrt{5} \cdot \sqrt{5} = 5$ und somit $\sigma(\sqrt{5}) \cdot \sigma\sqrt{5}) = 5$ für $\sigma(\sqrt{5})$ nur $+\sqrt{5}$ oder $-\sqrt{5}$ infrage kommen.
Die von der Identität verschiedene Abbildung lautet daher: $\sigma(a + b\sqrt{5}) = a - b\sqrt{5}$

Der Fixpunktkörper $L \subset E$ zu einer Galois-Untergruppe U kann (meistens) auf einfache Weise ermittelt werden. Sei z. B. $U = \{\tau_1, \tau_2, \tau_3, \tau_4\}$.
Für jedes Element e aus E bleibt die sogenannte Spur $S(e) = \tau_1(e) + \tau_2(e) + \tau_3(e) + \tau_4(e)$ durch alle Abbildungen aus U fix ($\tau_n \circ U = U$).
Zu jedem Element l aus L kann ein passendes e_l aus E gefunden werden mit $S(e_l) = l$ (beachte: S ist linear).
Mit einer Basis $\{e_1, e_2, \dots e_m\}$ für E wird L daher von $\{S(e_1), S(e_2), \dots, S(e_m)\}$ erzeugt. Diese Elemente müssen nicht alle verschieden sein.

Betrachten wir noch einmal die Galois-Gruppe der Gleichung

$$x^4 - 5x^2 + 3 = 0$$

$G = \{\ \sigma_1 = (12),\ \sigma_2 = (1324),\ \sigma_1^2 = \mathrm{id},\ \sigma_2^2,\ \sigma_2^3,\ \sigma_2 \circ \sigma_1,\ \sigma_2^2 \circ \sigma_1,\ \sigma_2^3 \circ \sigma_1\ \}$

und ihre Galois-Untergruppe: $U = \{\ \sigma_1^2,\ \sigma_2^2,\ \sigma_2 \circ \sigma_1,\ \sigma_2^3 \circ \sigma_1\ \}$

nach der Adjunktion von $\sqrt{13}$.

Wir gehen davon aus, dass $L = Q(\sqrt{13})$ der Fixkörper von U ist
und dass für $\sigma \in G$ gilt: $\sigma(L) = L$

Rechenbeispiele wie

$$(\sigma_2^3)^{-1} \circ \underbrace{(\sigma_2^3 \circ \sigma_1)}_{\in U} \circ \sigma_2^3 = \sigma_2 \circ \sigma_1 \in U$$

$$(\sigma_2^2 \circ \sigma_1)^{-1} \circ \sigma_2^2 \circ\ (\sigma_2^2 \circ \sigma_1) = \sigma_2^2 \in U$$

deuten darauf hin, dass die Untergruppe U in einer besonderen Beziehung zur Galois-Gruppe G steht. Um das aufzudecken, schauen wir uns an, was die Abbildung $\sigma^{-1} \circ \tau \circ \sigma$ ($\sigma \in G$, $\tau \in U$) auf dem Zerfällungskörper speziell auf der Teilmenge L bewirkt.
Die Abbildung muss wieder ein Element von G sein. σ bildet L auf sich ab, τ verändert nichts, σ^{-1} macht die Abbildung wieder rückgängig.
Die Elemente von L bleiben also fest, d. h. $\sigma^{-1} \circ \tau \circ \sigma$ muss mit einem Element aus U übereinstimmen. Wir erhalten $\sigma^{-1} \circ U \circ \sigma = U$ für $\sigma \in G$ (in endlichen Gruppen haben die Nebenklassen U, aU, Ub gleich viele Elemente).

Die Untergruppe U ist also ein Normalteiler von G.
Mit dieser einschränkenden Bedingung kann letztendlich nachgewiesen werden, dass es Gleichungen fünften Grades gibt, die nicht mit Wurzeltermen auflösbar sind, wie z. B. $x^5 - x + 1 = 0$, $x^5 - x + 2 = 0$, deren Galois-Gruppe aus allen 5! Permutationen bestehen.

Algebraische Körpererweiterung

Wir betrachten noch einmal die Gleichung

$x^4 - 5x^2 + 3 = 0$ und deren Lösung

$x_1 = \sqrt{10 + 2\sqrt{13}}$

Die Elemente des Körpers $\mathbb{Q}(x_1)$ besitzen die Darstellung $a + bx_1 + cx_1^2 + dx_1^3$
und bilden einen Vektorraum mit der Basis $\{1, x_1, x_1^2, x_1^3\}$.
Eine durch Multiplikation entstehende Potenz x_1^4 kann durch $5x_1^2 - 3$ ersetzt werden,
x_1^5 durch $5x_1^3 - 3x_1$, usw.

Aus anderer Sicht werden den Elementen des Polynomrings $\mathbb{Q}[x_1]$
Nullelemente $(x_1^4 - 5x_1^2 + 3) \cdot p(x_1)$ mit $p(x_1) \in \mathbb{Q}[x_1]$ hinzugefügt.
Es entsteht der Restklassenring $\mathbb{Q}(x_1) = \mathbb{Q}[x_1]/(f(x_1))$.

Wie erfolgt die Division, z.B. $\dfrac{1}{x_1^3 + x_1}$?

Der Euklidische Algorithmus liefert

$1 = \left(\frac{1}{3} + \frac{2}{9}x^2\right)(x^4 - 5x^2 + 3) + \left(x - \frac{2}{9}x^3\right)(x^3 + x)$ und damit

$$\frac{1}{x_1^3 + x_1} = x_1 - \frac{2}{9}x_1^3$$

Maple
$p := x^3 + x;$
$q := x^4 - 5 \cdot x^2 + 3;$
$gcdex(p, q, x, 'f', 'g');$
$'f' = f;\ 'g' = g;$

$$f = x - \frac{2}{9}x^3$$
$$g = \frac{1}{3} + \frac{2}{9}x^2$$

Offensichtlich führt die Adjunktion einer anderen Lösung zu einer isomorphen Körpererweiterung.

Transitivität

Sei $p(x)$ ein irreduzibles Polynom mit den verschiedenen Nullstellen x_1, x_2, …, x_n.
Greifen wir 2 Nullstellen x^* und x^{**} heraus, so gibt es aufgrund der Überlegungen zur algebraischen Körpererweiterung einen Isomorphismus

$$K(x^*) \quad \xrightarrow{\sigma} \quad K(x^{**}) \qquad \text{mit} \quad \sigma(x^*) = x^{**}.$$

σ kann (auf verschiedene Weisen) zu einem Isomorphismus auf dem Zerfällungskörper $K(x_1, x_2, \ldots, x_n)$ fortgesetzt werden und gehört somit zur Galoisgruppe G von $p(x)$ (G operiert transitiv auf den Nullstellen). Dieses Wissen ist bei der Bestimmung einer Galoisgruppe hilfreich.

Die Fortsetzung von σ erfolgt durch schrittweise Adjunktion der übrigen Nullstellen.

$$K(x^*, x_k) = K(x^*)(x_k) \quad \xrightarrow{\sigma^*} \quad K(x^{**})(x_l) \qquad \text{mit} \quad \sigma^*(x_k) = x_l.$$
$$\ldots$$

Hierbei ist x_k eine (beliebige) Nullstelle mit $x_k \notin K(x^*)$.
x_l muss dann so gewählt werden, dass eine isomorphe Struktur entsteht.
Bei genauerer Hinsicht wird klar, welche Nullstellen welchen Polynoms hierfür nur infrage kommen.

Die Struktur von $K(x^*)(x_k)$ wird durch das Minimalpolynom von x_k bestimmt (es teilt $p(x)$ in $K(x^*)[x]$). Die Nullstellen des unter σ isomorphen Bildes dieses Polynoms sind für x_l geeignet.

Algebraische Elemente

Sei l ein Element eines Zerfällungskörpers L über K.
Wie sieht das Minimalpolynom $p(x)$ von l aus?

Mit l wäre auch $\sigma(l)$ eine Nullstelle für $\sigma \in G$ (Galoisgruppe).
Nehmen wir an, dass hierdurch k verschiedene Nullstellen vorliegen (Bahn).
Das Minimalpolynom hätte dann in L (auch) die Linearfaktoren $(x - \sigma_i(l))$, $i = 1 \ldots k$.

Deren Produkt ergibt bereits das Minimalpolynom

$$p(x) = \prod_{i=1}^{k} (x - \sigma_i(l)) = x^k + a_{k-1}x^{k-1} + \ldots + a_0.$$

Es ist nachzuweisen, dass die Koeffizienten aus K sind.
Aus der Produktdarstellung ist ersichtlich, dass die Automorphismen von G das Produkt in sich überführen. Für die Koeffizienten von $p(x)$ gilt dann $\sigma(a_i) = a_i$ für $\sigma \in G$,
d. h. dass sie im Fixkörper K liegen.

Im Übrigen wird $|\,G\,|$ von k geteilt.
Hierzu ist die Anzahl der verschiedenen Bilder $\sigma(l)$ mit $\sigma \in G$ zu ermitteln.
Die Elemente einer Nebenklasse der Untergruppe $U = \{\sigma \in G \,|\, \sigma(l) = l\}$, deren Abbildungen l unverändert lassen, führen zum selben Bild.
Die Anzahl der Nebenklassen teilt die Ordnung von G.

Für ein algebraisches Element t, dass den Zerfällungskörper erzeugt (primitives Element), für dass also $L = K(x_1, x_2, \ldots, x_n) = K(t)$ gilt, eignet sich die Darstellung:

$$t = m_1x_1 + m_2x_2 + m_3x_3 + m_4x_4$$

Die $m_i \in K$ sind so zu wählen, dass die Linearfaktoren von

$$p(x) = \prod_{\sigma \in G} (x - \sigma(t)) = \prod_{\sigma \in G} \big(x - (m_1x_{\sigma(1)} + m_2x_{\sigma(2)} + m_3x_{\sigma(3)} + m_4x_{\sigma(4)})\big)$$

verschieden sind, $p(x)$ somit den Grad $|\,G\,| = [L : K]$ hat.

Sei $L = \mathbb{Q}(x_1, x_2, x_3, x_4)$ der Zerfällungskörper des Polynoms $x^4 - 5x^2 + 5$ (siehe Seite 3).
Wir wählen $m_1 = 1$, $m_2 = 0$, $m_3 = 1$, $m_4 = 0$.
Die Elemente aus L können dann polynomial in $t = x_1 + x_3$ dargestellt werden.
t ist Nullstelle von $p(x) = x^4 - 10x^2 + 5$.

Primitives Element

Um für eine Körpererweiterung die Existenz von t mit $K(\alpha_1, \alpha_2, \ldots, \alpha_n) = K(t)$ zu beweisen, reicht der Nachweis für $n = 2$ aus: $K(\alpha, \beta) = K(t)$
$K(\alpha_1, \alpha_2, \alpha_3) = K(\alpha_1, \alpha_2)(\alpha_3) = K(t, \alpha_3)$ zeigt, wie es weiter ginge.

Ein naheliegender Ansatz für t wäre eine Linearkombination von α und β, oder vereinfacht: $t = \alpha + m\beta$
Um $K(\alpha, \beta) = K(\alpha + m\beta)$ zu erhalten, ist das m so zu wählen, dass $\beta \in K(\alpha + m\beta)$ ist.
Dann wäre auch $\alpha \in K(\alpha + m\beta)$ und die Gleichheit ersichtlich.

Statt $\beta \in K(\alpha + m\beta)$ wird $(x - \beta) \in K(t)[x]$ gezeigt.

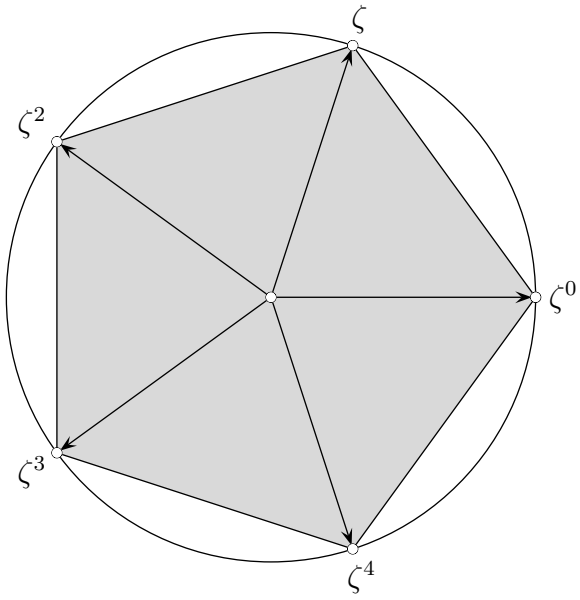
Hierzu werden zwei Polynome mit Koeffizienten in $K(t)$ benötigt, deren einzige gemeinsame Nullstelle β ist. Ihr größter gemeinsamer Teiler $(x-\beta)$ kann mit dem euklidischen Algorithmus in $K(t)$ ermittelt werden.
Sei f das Minimalpolynom von β mit den Nullstellen β, β_2, …, β_l.
Mit dem Minimalpolynom g von α erhalten wir mit $g(\alpha + m\beta - bx)$ ein weiteres Polynom mit der Nullstelle β, beachte $g(\alpha) = 0$. m wird nun so gewählt, dass sich die Nullstellen γ_k dieses Polynoms von den Nullstellen β_2, …, β_l unterscheiden. Dies ist möglich, wenn K als unendlich vorausgesetzt wird (nur für eine endliche Anzahl der $m's$ gibt es eine Übereinstimmung: $\alpha + m\beta - b\gamma_k = \beta_m$).
Damit der größte gemeinsame Teiler $(x-\beta)^k$ die Vielfachheit $k = 1$ hat, muss β noch als separabel (nur einfache Nullstellen) vorausgesetzt werden.
Von den Elementen $\alpha_1, \alpha_2, \ldots, \alpha_n$ muss daher eines (z. B. α_1) algebraisch und die übrigen separabel sein. Ein primitives Element existiert dann in der Form: $t = \alpha_1 + m_2\alpha_2 + \ldots + m_n\alpha_n$

Anzumerken bleibt noch:
In einer endlichen Körpererweiterung $L : K$ gibt es zu jedem Element $\alpha \in L$ ein $n \in \mathbb{N}$, so dass die Elemente α, α^2, …, α^n linear abhängig sind. Hieraus ergibt sich ein Polynom in $K[x]$ mit α als Nullstelle. α ist somit algebraisch.

Um für algebraische Elemente α und β das Minimalpolynom der Summe zu ermitteln, sind daher Potenzen $(\alpha + \beta)^k$ für $k \leq [L : K]$ auszurechnen und zusammenzufassen, ein lineares Gleichungssystem zu lösen und im sich ergebenden Polynom den irreduziblen Faktor mit der Nullstelle $(\alpha+\beta)$ zu bestimmen.

$x^5 - 2 = 0$

Die fünf Lösungen dieser Gleichung lauten $\sqrt[5]{2}\zeta^i,\ i = 0 \ldots 4$,
wobei die ζ^i die 5-ten Einheitswurzeln sind.



Die Galois-Gruppe $G(\mathbb{Q}(\sqrt[5]{2}, \zeta) : \mathbb{Q})$ besteht aus 20 Automorphismen,
die auf folgende Weise ermittelt werden können.

Die Abbildungen aus $G(\mathbb{Q}(\zeta) : \mathbb{Q})$ sind durch $\zeta \longrightarrow \zeta^i,\ i = 1 \ldots 4$, bestimmt.
$G(\mathbb{Q}((\sqrt[5]{2}, \zeta) : \mathbb{Q}(\zeta))$ besteht mit $\sigma(\sqrt[5]{2}) = \zeta\sqrt[5]{2}$ aus den Abbildungen $\{\mathrm{id}, \sigma, \sigma^2, \sigma^3, \sigma^4\}$.

Die Elemente $\tau \in G(\mathbb{Q}(\zeta) : \mathbb{Q})$ können auf einfache Weise auf $\mathbb{Q}(\sqrt[5]{2}, \zeta)$ mit $\tau^*(a) = a$
für $a \notin \mathbb{Q}(\zeta)$ fortgesetzt werden.

$G(\mathbb{Q}(\sqrt[5]{2}, \zeta) : \mathbb{Q})$ setzt sich somit aus der Verkettung der fortgesetzten Elemente aus $G(\mathbb{Q}(\zeta) : \mathbb{Q})$
mit denen aus $G(\mathbb{Q}(\sqrt[5]{2}, \zeta) : \mathbb{Q}(\zeta))$ zusammen.

Das Vorgehen ist allgemeingültig. Die Galois-Gruppe einer endlichen Galoiserweiterung $K : k$ kann so bestimmt werden, falls für einen Zwischenkörper L die Galois-Gruppen $G(K : L)$ und $G(L : k)$ bekannt sind.

Für $t = \zeta + \sqrt[5]{2}$ erhalten wir das Minimalpolynom

$$p(x) = \prod_{\phi \in G} \big(x - \phi(t)\big) = \prod_{\substack{i=1\ldots4 \\ j=0\ldots4}} \big(x - \zeta^i - \zeta^j \cdot \sqrt[5]{2}\big)$$

$$= t^{20} + 5t^{19} + 15t^{18} + 35t^{17} + 70t^{16} + 113t^{15} + \ldots + 40t^4 - 255t^3 - 45t^2 + 135t + 81$$

Äquivalenzrelation, Restklassen, Kleiner Satz von Fermat, Satz von Euler
Algebraische Körpererweiterung
Startseite