Grundideen der Galoistheorie

Eine Kurzeinführung für Interessierte (fast) ohne Vorkenntnisse[1]

von

Daniel Grieser (Oldenburg)

Mai 2007

Zusammenfassung: Die Fragen, die die Galoistheorie beantwortet, sind faszinierend und mit Schulwissen zu verstehen. Die Methoden zu ihrer Beantwortung gelten jedoch als für Schüler praktisch gar nicht und für Lehrer nur sehr schwer zugänglich, da zunächst ein großer Berg an Algebra bewältigt werden muss. In diesem Artikel wird die zentrale Idee der Galoistheorie erklärt und dabei nicht mehr als Oberstufenwissen vorausgesetzt.

Einleitung

Galoistheorie – der heilige Gral der Mathematik für viele, schillernder Gipfel der Algebra, nur erreichbar durch zähes Studium von mindestens drei Semestern höherer Algebra und auch dann oft nur halb verstanden. Für andere die Ausgeburt an Abstraktion, Paradigma der Realitätsferne, der Nicht-Anwendbarkeit von Mathematik.

Holen wir die Galoistheorie von ihrem Gipfel herunter, machen wir sie zur mathematischen Allgemeinbildung!

Die Fragen faszinieren: Lässt sich jeder Winkel mit Zirkel und Lineal dritteln? Gibt es eine Lösungsformel für beliebige polynomiale Gleichungen? Diese Fragen lassen sich mit ein wenig Schulwissen verstehen. Wer die üblichen Konstruktionen mit Zirkel und Lineal und die Lösungsformel für quadratische Gleichungen kennt, hat ein Gefühl dafür, was gesucht ist. Doch die Art der Fragestellung überrascht, eröffnet neue Horizonte des Denkens: Wie kann man grundsätzlich die Möglichkeit solcher Konstruktionen oder Lösungsformeln in Frage stellen? Ist das noch Mathematik, ist es nicht Philosophie? Und doch lassen sich diese Fragen mathematisch, mit aller Strenge und logischer Gewissheit mit NEIN beantworten. Dies ist Galois' Theorie.[2]

[1] Erschienen in: Mathematische Bildung – Mathematische Leistung. Festschrift für Michael Neubrand zum 60. Geburtstag. A. Peter-Koop, A. Bikner-Ahsbahs (Hrsg.). Verlag Franzbecker, 2007.

[2] Ein paar historische Anmerkungen: Genau genommen stammen viele der Ideen, die im Folgenden erklärt werden, nicht von Galois selbst. Dass Permutationen bei algebraischen Gleichungen eine Rolle spielen, war schon Lagrange 1770 bewusst. Die Unlösbarkeit der allgemeinen Gleichung 5. Grades durch Radikale wurde schon vor Galois von P. Raffine 1799 (mit einem kleinen Fehler) und N. Abel 1824 gezeigt. Doch erst Galois bemerkte um 1830 die zentrale Verbindung polynomialer Gleichungen zu Gruppen von Permutationen. Daher trägt diese Theorie heute seinen Namen.

So einfach die Fragen, so unzugänglich bleiben für viele die Antworten. In den modernen Darstellungen muss man sich erst durch eine gehörige Portion Gruppen- und Körpertheorie schlagen. Die wenigsten Lehramtsstudenten kommen im Fachstudium so weit, daher bleibt dieser Schatz den meisten Lehrern und Schülern verborgen. Und selbst wenn man die Mühen auf sich genommen hat und alles brav nachvollziehen konnte, bleibt ein Unwohlsein: Die Antworten auf die Eingangsfragen ergeben sich scheinbar als zufällige Nebenprodukte, und man fragt sich: Wo ist ‚es' eigentlich passiert? Was bringt das Ding zum Laufen? Wie kann sich jemand so etwas ausgedacht haben?

Zu Galois' Zeiten gab es keine Gruppentheorie; Galois hat den Gruppenbegriff erst erfunden, für den Zweck seiner Theorie! Dass ein genetisches Verständnis bei der modernen Darstellung kaum möglich ist, verwundert daher kaum.

In diesem Artikel werden zentrale Grundideen der Galoistheorie entwickelt, ohne den Gruppen- oder Körperbegriff vorauszusetzen, anhand des Problems, Lösungsformeln für polynomiale Gleichungen zu finden. Die Darstellung sollte für jeden verständlich sein, der ein paar Grundlagen über Polynome, etwa die Lösungsformel für die quadratische Gleichung und die Formeln von Vieta kennt – beides wird aber auch hergeleitet, die quadratische Formel unter ungewohntem Blickwinkel. Natürlich wird auch der Wille vorausgesetzt, sich auf eine neue Idee einzulassen, mit ihr zu spielen, sie konsequent zu verfolgen. Komplexe Zahlen brauchen wir auch – das ist nur natürlich, da polynomiale Gleichungen nicht immer reelle Lösungen besitzen[3]. Trotzdem: Alles Schulmathematik.

Ich hoffe, diese spannende Theorie zumindest in Ansätzen interessierten Schülern und Lehrern zugänglich zu machen, und auch denjenigen, die sie als Nebenprodukt der Körpertheorie kennengelernt haben und damit nicht zufrieden waren, eine mögliche Antwort auf die Frage ‚Wie kann man auf so etwas bloß kommen?' anzubieten.

1 Überblick

Wir betrachten eine polynomiale Gleichung

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 \tag{1}$$

und wollen eine Lösungsformel finden, also eine Formel, die die Lösungen x mittels der gegebenen Koeffizienten $a_0, \ldots, a_{n-1}$ ausdrückt.

Die wunderbare Grundidee der Galoistheorie ist, dass man dieses Problem als ‚Reduktion von Symmetrie' formulieren kann. Dies wird gleich erklärt werden. Indem wir diese Idee konsequent verfolgen, erhalten wir zunächst ein neues Verständnis der ‚quadratischen Formel' (d.h. des Falls $n = 2$), dann eine Lösungsformel im Fall $n = 3$, eine Strategie für alle n, und schließlich sogar eine Idee, wie man die Nicht-Existenz einer allgemeinen Lösungsformel für $n \geq 5$ zeigen könnte. Nebenbei taucht ganz natürlich das Konzept der Gruppe auf.

2 Einstieg

Für $n = 1$ ist die Gleichung einfach $x + a_0 = 0$, also ist

$$x = -a_0$$

[3]Siehe dazu Fußnote 4.

die einzige Lösung. Eine Lösungsformel!

Für $n = 2$ lautet die Gleichung $x^2 + a_1 x + a_0 = 0$, und aus der Schule ist die Lösungsformel

$$\begin{aligned} x_1 = &\quad -\tfrac{a_1}{2} \quad + \quad \sqrt{\left(\tfrac{a_1}{2}\right)^2 - a_0} \\ x_2 = &\quad -\tfrac{a_1}{2} \quad - \quad \sqrt{\left(\tfrac{a_1}{2}\right)^2 - a_0}. \end{aligned}$$

bekannt (zumindest im Fall $\left(\frac{a_1}{2}\right)^2 - a_0 \geq 0$; im Folgenden lassen wir auch komplexe Zahlen als Lösungen zu, brauchen uns also um diese Einschränkung nicht zu kümmern[4]).

3 Die Formeln von Vieta

Für die folgenden Überlegungen ist es wesentlich, den Unterschied zwischen *Existenz von Lösungen* und *Formeln für Lösungen* zu verstehen: Der Fundamentalsatz der Algebra garantiert, dass (1) stets Lösungen besitzt, aber er gibt keine Formel an. Etwa im Fall $n = 3$, für reelle Koeffizienten a_0, a_1, a_2, ist es aus anschaulichen Überlegungen klar, dass es eine Lösung gibt: Für sehr große x dominiert der x^3 Term, also ist die linke Seite von (1) positiv und analog für sehr negative x negativ, also muss sie zwischendurch irgendwo gleich Null sein. Wo, weiß man damit aber nicht.

Wir setzen hier den Fundamentalsatz der Algebra voraus[5]. Genauer setzen wir voraus, dass sich das Polynom in (1) als Produkt von Linearfaktoren

$$x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = (x - x_1) \cdot (x - x_2) \cdot \ldots \cdot (x - x_n) \qquad (2)$$

schreiben lässt, für gewisse (komplexe) Zahlen $x_1, \ldots, x_n$. Offenbar sind dann $x_1, \ldots, x_n$ genau die Lösungen von (1) [6].

Durch Ausmultiplizieren der rechten Seite von (2) und Vergleichen entsprechender Potenzen von x folgt:

$$\begin{aligned} a_{n-1} &= -(x_1 + x_2 + \cdots + x_n) = -\sum_{i=1}^{n} x_i \\ a_{n-2} &= x_1x_2 + x_1x_3 + \ldots + x_{n-1}x_n = \sum_{\substack{i,j=1 \\ 1<j}}^{n} x_i x_j \\ &\vdots \\ a_0 &= (-1)^n x_1 \cdot \ldots \cdot x_n. \end{aligned} \qquad (3)$$

[4] Wer komplexe Zahlen vermeiden will, kann von vorneherein annehmen, dass alle Lösungen von (1) reell sind. Die Symmetrieidee lässt sich auch dann nachvollziehen. Spätestens bei der Behandlung der kubischen Gleichung werden sie aber selbst unter dieser Annahme gebraucht; das war schon Cardano 1545 bekannt (als ‚Casus Irreducibilis') und führte damals zu einer größeren Akzeptanz der komplexen Zahlen.

[5] Bemerkenswert ist, dass wir den Fundamentalsatz zwar zunächst annehmen, dass aber die Korrektheit der damit hergeleiteten Lösungsformeln (für $n = 3$) direkt, ohne den Fundamentalsatz, nachgeprüft werden kann: Einfach in die Gleichung (1) einsetzen.

[6] (2) folgt durch wiederholtes Herausteilen von Linearfaktoren aus dem Fundamentalsatz. Die Zahlen $x_1, \ldots, x_n$ müssen nicht alle verschieden sein. Kommt dieselbe Zahl mehrmals vor, spricht man von einer mehrfachen (doppelten, dreifachen, ...) Nullstelle.

Zum Beispiel für $n = 2$:

$$x^2+a_1x+a_0 = (x-x_1)(x-x_2) = x^2-x_1x-xx_2+x_1x_2 = x^2-(x_1+x_2)x+x_1x_2,$$

und da dies für alle x gilt, folgt aus dem Identitätssatz für Polynome

$$\begin{aligned} a_1 &= -(x_1 + x_2) \\ a_0 &= x_1x_2 \end{aligned} \tag{4}$$

Analog für $n = 3$:

$$\begin{aligned} a_2 &= -(x_1 + x_2 + x_3) \\ a_1 &= x_1x_2 + x_1x_3 + x_2x_3 \\ a_0 &= -x_1x_2x_3 \end{aligned} \tag{5}$$

4 Symmetrie

Die große Idee der Galoistheorie ist, dass Symmetrieüberlegungen ein Schlüssel zur Lösung unseres Problems (1) sein können.
Was bedeutet Symmetrie? Betrachten wir die Ausdrücke auf der rechten Seite von (3). Sie sind vollständig symmetrisch in dem Sinn, dass sie sich bei beliebiger Permutation (d.h. Änderung der Reihenfolge) der $x_1, \ldots, x_n$ nicht ändern. Für $n = 2$ ist z. B. $x_2 + x_1 = x_1 + x_2$ und $x_2x_1 = x_1x_2$.

Es gibt noch weitere vollständig symmetrische Ausdrücke in $x_1, \ldots, x_n$, zum Beispiel (für $n = 2$) $x_1^2 + x_2^2$, $x_1^3 + x_2^3$ und $(x_1 - x_2)^2$. Kann man diese durch $x_1 + x_2$ und x_1x_2 ausdrücken? Ein wenig Herumspielen mit der binomischen Formel

$$(x_1 + x_2)^2 = x_1^2 + 2x_1x_2 + x_2^2,$$

ergibt

$$x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = a_1^2 - 2a_0,$$

und aus

$$(x_1 + x_2)^3 = x_1^3 + 3x_1^2x_2 + 3x_1x_2^2 + x_2^3 = x_1^3 + 3x_1x_2(x_1 + x_2) + x_2^3,$$

erhält man

$$x_1^3 + x_2^3 = (x_1 + x_2)^3 - 3x_1x_2(x_1 + x_2) = -a_1^3 + 3a_0a_1.$$

Ähnlich geht

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = a_1^2 - 4a_0.$$

Nach dieser Vorübung überrascht vielleicht nicht der folgende Satz.

Satz (Hauptsatz über symmetrische Funktionen[7])**:** Ist f eine vollständig symmetrische Funktion von $x_1, \ldots, x_n$, so lässt sich f als Funktion von $a_0, \ldots, a_{n-1}$

[7]Der Begriff ‚Funktion' ist hier absichtlich etwas vage gelassen. Für unseren Kontext wesentlich sind Polynome in $x_1, \ldots, x_n$ (d. h. Ausdrücke, die man aus $x_1, \ldots, x_n$ und beliebigen komplexen Zahlen durch Addition, Subtraktion, Multiplikation erhält). Dann gilt: Ist f Polynom, so auch g. Der Satz gilt aber auch, wenn man beliebige Funktionen $f, g : \mathbb{C}^n \to \mathbb{C}$ (oder $\mathbb{R}^n \to \mathbb{C}$) betrachtet oder an jeder Stelle ‚Funktion' durch ‚stetige Funktion', ‚differenzierbare Funktion ', ‚analytische Funktion ', ... ersetzt.

(gegeben wie in (3)) schreiben, d. h. es existiert eine Funktion g derart, dass

$$f(x_1, \ldots, x_n) = g(a_0, \ldots, a_{n-1}).$$

Der Begriff ‚vollständig symmetrisch' wird unten in (8) genauer erklärt.

Ein Beweis mittels Induktion (für Polynome) ist nicht allzu schwierig. Hier ist es sinnvoller, ein paar weitere Beispiele (etwa für $n = 3$) zu rechnen:

Übung:

$$\begin{aligned} x_1^2 + x_2^2 + x_3^2 &= a_2^2 - 2a_1 \\ x_1^3 + x_2^3 + x_3^3 &= -a_2^3 + 3a_2a_1 - 3a_0. \end{aligned} \tag{5a}$$

Ein vollständig symmetrischer Ausdruck, der weiter unten wichtig sein wird, ist

$$D_n := \prod_{\substack{i,j=1 \\ i<j}}^{n} (x_i - x_j)^2,$$

die sogenannte **Diskriminante**.
Z. B. ist

$$D_2 = (x_1 - x_2)^2 = a_1^2 - 4a_0 \tag{6}$$

$$D_3 = (x_1-x_2)^2(x_2-x_3)^2(x_1-x_3)^2 = a_2^2a_1^2+18a_2a_1a_0-4a_2^3a_0-4a_1^3-27a_0^2 \tag{7}$$

Das ist schon ziemlich kompliziert.

5 Ein neuer Blick auf das Problem

Gegeben sind $a_0, \ldots, a_{n-1}$, gesucht sind $x_1, \ldots, x_n$. Sie stehen mittels (3) in Beziehung zueinander. Mittels des Hauptsatzes können wir das Problem umformulieren:

> **Zu unbekannten Zahlen $x_1, \ldots, x_n$ kennen wir die Werte sämtlicher vollständig symmetrischer Ausdrücke in $x_1, \ldots, x_n$. Bestimme $x_1, \ldots, x_n$ selbst!**

Da jeder der Ausdrücke $x_1, x_2, \ldots, x_n$ für sich nicht symmetrisch ist, könnten wir dies als ein Problem der *Symmetriereduzierung* bezeichnen.

Was haben wir damit gewonnen?

> **Wir können Zwischenziele formulieren und zu lösen versuchen, nämlich statt der vollständig symmetrischen $(a_1, \ldots, a_n)$ oder vollständig unsymmetrischen $(x_1, \ldots, x_n)$ Ausdrücke auch ‚teilweise symmetrische' betrachten.**

Das Wunder:

Dies führt zur Lösung!

Was soll ‚teilweise symmetrisch' heißen? Ein Ausdruck $f(x_1, \ldots, x_n)$ ist vollständig symmetrisch, falls

$$f(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)}) \tag{8}$$

für alle Permutationen π gilt.

‚Teilweise symmetrisch' heißt, dass (8) nur für einige Permutationen gilt.
Beispiel: Der Ausdruck

$$W(x_1, x_2, x_3) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$$

erfüllt (8) für die Permutationen

$$\pi = \mathrm{id},\ \pi : 1 \to 2 \to 3 \to 1,\ \pi : 1 \to 3 \to 2 \to 1, \tag{9}$$

(id = Identität, d.h. $\mathrm{id}(i) = i\,\forall i$, also keine Umordnung) wechselt aber unter den drei anderen Permutationen von $\{1, 2, 3\}$ das Vorzeichen, z. B.

$$W(x_2, x_1, x_3) = (x_2 - x_1)(x_1 - x_3)(x_3 - x_2) = -W(x_1, x_2, x_3).$$

Die Permutationen (9) heißen **gerade**, die anderen **ungerade**.

6 Lösung der Gleichung dritten Grades, Vorspiel

Durch konsequentes Verfolgen der Idee der Symmetriereduktion können wir die kubische Gleichung lösen.

1. Schritt:
Gegeben sind die vollständig symmetrischen Ausdrücke a_0, a_1, a_2 und damit auch D_3 (siehe (7)).

2. Schritt:
Eine der beiden Quadratwurzeln von $D_3 = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$ ist $W(x_1, x_2, x_3) = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$ (die andere Quadratwurzel ist das negative davon). Also:

> **Durch Ziehen einer Quadratwurzel haben wir aus einem vollständig symmetrischen Ausdruck einen Ausdruck erhalten, der nur noch unter geraden Permutationen symmetrisch ist.**

Die halbe Strecke von vollständig symmetrisch zu vollständig unsymmetrisch ist also geschafft!

3. Schritt:
Die große Frage ist nun: Wie gelange ich von einem Ausdruck, der nur unter geraden Permutationen symmetrisch ist, zu einem gänzlich unsymmetrischen? Wir versuchen, das Vorgehen von Schritt 1 und Schritt 2 zu imitieren:

1. Hoffnung: Aus a_2, a_1, a_0 und $W(x_1, x_2, x_3)$ lässt sich **jeder** Ausdruck in x_1, x_2, x_3, der unter geraden Permutationen symmetrisch ist, berechnen.
(Dies wäre eine Verallgemeinerung des Hauptsatzes über symmetrische Funktionen.)

2. Hoffnung: Wir können einen oder mehrere gänzlich unsymmetrische Ausdrücke angeben (diese würden dem W im 2. Schritt entsprechen), so dass gilt:

- eine Potenz dieser Ausdrücke ist symmetrisch unter geraden Permutationen

- x_1, x_2, x_3 lassen sich mittels dieser Ausdrücke berechnen.

In Abschnitt 8 gehen die beiden Hoffnungen in Erfüllung, in Abschnitt 9 fassen wir die so erhaltene Lösungsmethode zusammen. Die Formeln werden dabei kompliziert. Behält man aber das Ziel im Auge, ist es nicht schwierig.

7 Quadratische Gleichung: Ein neuer Blickwinkel

Zunächst sehen wir uns die quadratische Gleichung unter dem neuen Blickwinkel an:

1. Schritt:
Gegeben sind $a_1 = -(x_1+x_2)$, $a_0 = x_1x_2$ und damit $D_2 = (x_1-x_2)^2 = a_1^2-4a_0$.

2. Schritt:
Ist $\sqrt{D_2}$ eine der Quadratwurzeln von D_2, so folgt

$$\sqrt{D_2} = x_1 - x_2 \quad \text{oder} \quad \sqrt{D_2} = x_2 - x_1. \tag{10}$$

Diese sind nicht mehr symmetrisch.

Schluss:
Wegen

$$\begin{array}{rcl} x_1 & = & \frac{1}{2}\left[(x_1 + x_2) + (x_1 - x_2)\right] \\ x_2 & = & \frac{1}{2}\left[(x_1 + x_2) - (x_1 - x_2)\right] \end{array} \tag{11}$$

lassen sich nun x_1, x_2 berechnen:

$$x_1 = -\frac{a_1}{2} + \frac{1}{2}\sqrt{D_2},\ x_2 = -\frac{a_1}{2} - \frac{1}{2}\sqrt{D_2}$$

(im ersten Fall von (10); im anderen Fall sind x_1, x_2 einfach vertauscht.)
Das ist die bekannte Formel!

8 Lösung der Gleichung dritten Grades, Abschluss

Wir wenden uns zunächst der 2. Hoffnung in Abschnitt 6 zu. Wir benötigen hierzu ein kleines hübsches Hilfsmittel: Die dritten Einheitswurzeln.

Was ist die dritte Wurzel aus 1? Natürlich 1. Gibt es weitere? Reelle nicht, komplexe aber schon: Man rechnet leicht nach, dass $-\frac{1}{2} \pm i\frac{\sqrt{3}}{2}$ auch die dritte Potenz eins haben. Schreibt man $\omega = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, so ist $\omega^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ und $\omega^3 = 1$, und $1, \omega, \omega^2$ sind alle dritten Wurzeln von 1 (es kann ja nicht mehr als drei Nullstellen der Gleichung $x^3 - 1 = 0$ geben). Es gilt

$$\omega^2 + \omega + 1 = 0. \tag{12}$$

Die dritten Einheitswurzeln kann man trickreich für unsere Zwecke einsetzen: Sei

$$\begin{array}{rcl} b_0 & = & x_1 + x_2 + x_3 \\ b_1 & = & \omega x_1 + \omega^2 x_2 + x_3 \\ b_2 & = & \omega^2 x_1 + \omega x_2 + x_3 \end{array} \tag{13}$$

(also $b_i = \sum_{j=1}^{3} \omega^{ij} x_j$, $i = 0, 1, 2$).
Dann gilt:

- b_0 ist vollständig symmetrisch, $b_0 = -a_2$
- $(b_1)^3$ und $(b_2)^3$ sind symmetrisch unter geraden Permutationen, denn zum Beispiel ist
$$b_1(x_3, x_1, x_2) = \omega \cdot b_1(x_1, x_2, x_3)$$
also folgt aus $\omega^3 = 1$, dass
$$b_1(x_3, x_1, x_2)^3 = b_1(x_1, x_2, x_3)^3$$
- x_1, x_2, x_3 lassen sich aus b_0, b_1, b_2 berechnen:
$$\begin{aligned} x_1 &= \tfrac{1}{3}(b_0 + \omega^2 b_1 + \omega b_2) \\ x_2 &= \tfrac{1}{3}(b_0 + \omega b_1 + \omega^2 b_2) \\ x_3 &= \tfrac{1}{3}(b_0 + b_1 + b_2) \end{aligned} \tag{14}$$
(also: $x_j = \frac{1}{3} \sum_{i=0}^{2} \omega^{-ij} b_i$) wie sofort aus $\omega^2 + \omega + 1 = 0$ folgt.

Damit erfüllen b_0, b_1, b_2 die 2. Hoffnung! Dies ist übrigens völlig analog zum Vorgehen bei der quadratischen Gleichung, denn die zweiten Einheitswurzeln sind ± 1, und daher funktionierte dort der analoge Trick mit $b_0 = x_1 + x_2$, $b_1 = x_1 - x_2$.
Nun zur 1. Hoffnung:
Das stimmt zwar allgemein, es genügt aber, die konkreten Ausdrücke $(b_1)^3$ und $(b_2)^3$ mittels a_2, a_1, a_0 und W auszudrücken. Wegen $b_2(x_1, x_2, x_3) = b_1(x_2, x_1, x_3)$ genügt es, b_1 zu betrachten:
Mühseliges Ausmultiplizieren ergibt

$$b_1^3 = x_1^3 + x_2^3 + x_3^3 + 3\omega A + 3\omega^2 B + 6x_1x_2x_3 \tag{15}$$

mit $A = x_1^2x_2 + x_2^2x_3 + x_3^2x_1$, $B = x_1x_2^2 + x_2x_3^2 + x_3x_1^2$; außerdem

$$W = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) = B - A. \tag{16}$$

Wir brauchen aber A und B einzeln! Beobachtung: $A + B$ ist vollständig symmetrisch. Also lässt es sich mittels a_0, a_1, a_2 ausdrücken (vgl. (5)), und dann erhält man A, B: Für $A + B$ liegt es nahe, a_1a_2 zu betrachten: Man rechnet

$$-a_1a_2 = 3x_1x_2x_3 + A + B = -3a_0 + A + B. \tag{17}$$

Aus (16), (17) folgt

$$A = \frac{1}{2}(3a_0 - a_1a_2 - W),\ B = \frac{1}{2}(3a_0 - a_1a_2 + W).$$

Mit Hilfe von (5a) erhalten wir nun aus (15):

$$b_1^3 = -a_2^3 + 3a_2a_1 - 3a_0 + \frac{3}{2}\omega(3a_0 - a_1a_2 - W) + \frac{3}{2}\omega^2(3a_0 - a_1a_2 + W) - 6a_0.$$

Dies lässt sich mittels $\omega + \omega^2 = -1$, $\omega - \omega^2 = i\sqrt{3}$ vereinfachen zu

$$b_1^3 = -a_2^3 + \frac{9}{2}a_2a_1 - \frac{27}{2}a_0 - \frac{3}{2}i\sqrt{3}W. \tag{18}$$

b_2^3 erhält man hieraus, indem man W durch $-W$ ersetzt. Fertig!

9 Zusammenfassung der Lösung der kubischen Gleichung

I) Berechne D_3 aus a_0, a_1, a_2 mittels (7).

II) Sei W eine der Quadratwurzeln aus D_3.

III) Berechne b_1^3, b_2^3 aus a_0, a_1, a_2, W mittels (18).

IV) Ziehe dritte Wurzeln aus b_1^3, b_2^3, erhalte so b_1, b_2 und damit x_1, x_2, x_3 mittels (14) und $b_0 = -a_2$.

Setzt man alles ineinander ein, erhält man ein Ungetüm an Formel. Aber immerhin eine Lösungsformel.

Doch Vorsicht: Im Schritt IV ist es wichtig, die richtigen dritten Wurzeln zu ziehen: Genau wie die eins hat jede Zahl (außer null) drei dritte Wurzeln. Ist c eine davon, dann sind ωc und $\omega^2 c$ die beiden anderen, denn z.B. $(\omega c)^3 = \omega^3 c^3 = c^3$. Da man vor Schritt IV nur den Wert b_1^3 kennt, kann man nicht sicher sein, ob man als dritte Wurzel nicht ‚aus Versehen' ωb_1 oder $\omega^2 b_1$ statt b_1 erhalten hat (beachte: b_1^3 ist eine komplexe Zahl), und dann stimmen die Formeln (14) nicht mehr, nicht mal nach Vertauschungen! Ersetzt man allerdings gleichzeitig b_1 durch ωb_1 und b_2 durch $\omega^2 b_2$ (oder b_1 durch $\omega^2 b_1$ und b_2 durch ωb_2), bleibt (14) bis auf Vertauschungen korrekt. Diese Kopplung drückt sich dadurch aus, dass (verwende (13)!)

$$b_1 b_2 = x_1^2 + x_2^2 + x_3^2 - x_1 x_2 - x_2 x_3 - x_3 x_1 = a_2^2 - 3a_1 \tag{19}$$

vollständig symmetrisch ist. IV) sollte nun so modifiziert werden:

IV') Bestimme eine dritte Wurzel aus b_1^3, nenne diese b_1 und bestimme dann b_2 aus (19), und dann x_1, x_2, x_3 aus (14).

Die Nichteindeutigkeit der Quadratwurzel in II) macht keine solchen Probleme, da sie in III) nur eine Vertauschung von b_1^3 und b_2^3 bewirkt.

Abschließende Bemerkung: Die komplizierten Formeln für die Gleichung dritten Grades vereinfachen sich erheblich, wenn man $a_2 = 0$ annimmt. Dann bleiben von den fünf Termen in der Diskriminante (7) nur zwei übrig. Dies kann man, ausgehend von einer allgemeinen Gleichung, durch die Substitution $y = x - a_2/3$ immer erreichen. Nach etwas Rechnen erhält man

$$x_3 = \sqrt[3]{-\frac{a_0}{2} - \sqrt{\tilde{D}}} + \sqrt[3]{-\frac{a_0}{2} + \sqrt{\tilde{D}}},$$

wobei $\tilde{D} = -\frac{1}{4\cdot 27} D = \left(\frac{a_0}{2}\right)^2 + \left(\frac{a_1}{3}\right)^3$. Diese Lösungsformel heißt auch *Cardano-Formel*. Dabei muss man, wie oben erklärt, die ‚richtigen' dritten Wurzeln nehmen. x_1 erhält man, indem man die erste Kubikwurzel mit ω und die zweite mit ω^2 multipliziert, und x_2 durch Vertauschen von ω und ω^2.

10 Was genau heißt ‚teilweise symmetrisch'?

Um Gleichungen höheren Grades behandeln zu können, sollten wir uns genauer ansehen, welche Zwischenziele (vgl. Abschnitt 5) eigentlich möglich sind und wie man von einem zum nächsten gelangt.

Ein ‚Zwischenziel' war durch eine ‚teilweise Symmetrie' charakterisiert, also durch eine Menge G von Permutationen π, für die (8) für gewisse Funktionen f gilt. Welche Mengen G können dabei auftreten?
Aus (8) sieht man:

- Ist $\pi \in G$ und $\sigma \in G$, so folgt $\pi \circ \sigma \in G$. $\pi \circ \sigma$ bezeichnet die Hintereinanderausführung (Komposition) von π und σ, d.h. $(\pi \circ \sigma)(i) = \pi(\sigma(i))$. Denn setzt man $y_i = x_{\pi(i)},\ i = 1, \ldots, n$, so folgt aus $\sigma \in G$, dass

  $$f(y_1, \ldots, y_n) = f(y_{\sigma(1)}, \ldots, y_{\sigma(n)}) = f\left(x_{\pi(\sigma(1))}, \ldots, x_{\pi(\sigma(n))}\right)$$

  und mit (8), angewendet mit y statt x, folgt

  $$f(x_1, \ldots, x_n) = f\left(x_{\pi(\sigma(1))}, \ldots, x_{\pi(\sigma(n))}\right),$$

  was gerade $\pi \circ \sigma \in G$ bedeutet.

- Ist $\pi \in G$, so ist auch das Inverse $\pi^{-1} \in G$. Dies ist definiert durch: $\pi^{-1}(j) = i$, falls $\pi(i) = j$. Denn mit $y_i = x_{\pi(i)},\ i = 1, \ldots, n$, ist $x_j = y_{\pi^{-1}(j)},\ j = 1, \ldots, n$, also sagt (8)

  $$f\left(y_{\pi^{-1}(1)}, \ldots, y_{\pi^{-1}(n)}\right) = f(y_1, \ldots, y_n),$$

  also $\pi^{-1} \in G$.

Eine Menge von Permutationen mit diesen beiden Eigenschaften nennt man eine **Gruppe** (bzgl. der Operation $\circ$, also Komposition) oder auch **Permutationsgruppe**. Das ist die Geburt des Gruppenbegriffs![8]

Sprechweise: Ist G eine Permutationsgruppe, so nennen wir einen Ausdruck $f(x_1, \ldots, x_n)$ **G-symmetrisch**, falls (8) für alle $\pi \in G$ gilt.

11 Eine allgemeine Methode

Wie erhalten wir eine Lösungsformel für die Nullstellen $x_1, \ldots, x_n$ der Gleichung

$$x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0?$$

[8] Dies ist der alte, von Galois eingeführte und im 19. Jahrhundert meist verwendete Gruppenbegriff. Im heutigen Sprachgebrauch ist eine Gruppe eine Menge mit einer zweistelligen Operation, die assoziativ ist und für die ein neutrales Element und zu jedem Element ein Inverses existieren. Z. B. ist die Menge S_n aller Permutationen von $\{1, \ldots, n\}$, mit Komposition als Operation, eine Gruppe. Unser G nennt man heutzutage eine **Untergruppe** von S_n. Es ist natürlich selbst auch eine Gruppe.
Man kann zeigen, dass jede endliche Gruppe ‚gleich' (genauer: isomorph) ist zu einer Untergruppe von S_n, für ein geeignetes $n \in \mathbb{N}$. Also sind der alte und neue Gruppenbegriff (zumindest für endliche Gruppen) im Wesentlichen gleich.

Die teilweisen Symmetrien, also die Permutationsgruppen, wollten wir als Zwischenschritte bei der Lösung der Gleichung verwenden. Die Koeffizienten $a_0, \ldots, a_{n-1}$ sind vollständig symmetrisch, entsprechen also der Gruppe $G = S_n$ aller Permutationen von $\{1, \ldots, n\}$, die gesuchten Lösungen $x_1, \ldots, x_n$ sind vollkommen unsymmetrisch, entsprechen also der ‚trivialen' Gruppe $G = \{\mathrm{id}\}$ [9].

Also:

I) Finde Permutationsgruppen $G_0, G_1, \ldots, G_k$ mit

$$S_n = G_0 \supset G_1 \supset \ldots \supset G_k = \{\mathrm{id}\}.$$

II) Für $i = 1, \ldots, k$ tu folgendes:
Finde G_i-symmetrische Ausdrücke $W_{i1}, W_{i2}, \ldots$ und eine natürliche Zahl p_i, so dass gilt:

a) die p_i-ten Potenzen dieser Ausdrücke sind sogar G_{i-1}-symmetrisch.

b) Aus diesen Ausdrücken lassen sich mittels algebraischer Operationen sämtliche G_i-symmetrischen Ausdrücke gewinnen.

(‚Algebraische Operationen' sind hier $+, -, \cdot$.) Bei der kubischen Gleichung war $k = 2$ und $G_1 = \{\text{gerade Permutationen}\}$. Falls es gelingt, die Schritte I) und II) durchzuführen, erhalten wir eine Formel für $x_1, \ldots, x_n$, in der nur algebraische Operationen und p_1'te, …, p_k'te Wurzeln vorkommen[10].
Denn: Fangen wir mit $i = k$ an und wenden IIb) auf $x_1, \ldots, x_n$ an. Dies liefert Formeln für $x_1, \ldots, x_n$ in Termen von $W_{k1}, W_{k2}, \ldots$. Da $(W_{kj})^{p_k}$ G_{k-1}-symmetrisch ist (nach IIa)), lässt es sich algebraisch aus $W_{k-1,1}, W_{k-1,2}, \ldots$ berechnen (wegen IIb) für $i = k - 1$). Das heißt gerade, dass

$$W_{k1} = \sqrt[p_k]{\text{algebraischer Ausdruck in } W_{k-1,1}, W_{k-1,2}, \ldots}$$

und ähnlich für $W_{k2}, \ldots$.
Nun verfahren wir analog mit $W_{k-1,1}, \ldots$, reduzieren auf $W_{k-2,1}, \ldots$ etc., bis wir bei $i = 1$ ankommen, wo wir dann $(W_{11})^{p_1}$, $(W_{12})^{p_1}, \ldots$ mittels der Koeffizienten $a_0, \ldots, a_{n-1}$ algebraisch ausdrücken können, also die gesuchte Formel erhalten.

12 Funktioniert die Methode?

Die große Frage ist, ob man ein $k \in \mathbb{N}$ und Gruppen $G_1, \ldots, G_k$ derart finden kann, dass Schritt II) wirklich funktioniert. Dies führt automatisch zu einem der Hauptbegriffe der Gruppentheorie. Man kann nämlich zeigen:
Schritt II) für einen Index i ist genau dann durchführbar, wenn gilt:

A) G_i ist ein **Normalteiler** von G_{i-1}, d. h. für alle $\pi \in G_i$ und alle $\sigma \in G_{i-1}$ ist $\sigma \circ \pi \circ \sigma^{-1} \in G_i$.

[9] Genauer: Die einzige Permutation, die **jeden** der Ausdrücke $x_1, \ldots, x_n$ in sich überführt, ist $\pi = \mathrm{id}$. Betrachtet man nur einen Ausdruck, etwa x_1, so wird er auch (etwa für $n = 3$) von der Permutation $1 \mapsto 1, 2 \mapsto 3 \mapsto 2$ in sich überführt.

[10] Auf das Problem der Mehrdeutigkeit von Wurzeln wollen wir hier nicht näher eingehen. Es kann ähnlich wie im Fall $n = 3$ behandelt werden.

B) Die Quotientengruppe G_{i-1}/G_i ist zyklisch, d. h. es existiert ein $g \in \mathbb{N}$ und ein $\tau \in G_{i-1}$, so dass sich jedes $\sigma \in G_{i-1}$, in der Form $\sigma = \tau^j \circ \pi$ für geeignete $j \in \{0, 1, \ldots, g-1\}$ und $\pi \in G_i$ schreiben lässt.

A) ist recht leicht einzusehen, für B) braucht man ein klein wenig Gruppentheorie. Weitaus schwieriger zu zeigen ist der folgende Satz.

Satz: Sei $n \in \mathbb{N}$. Es existieren $k \in \mathbb{N}$ und Gruppen $S_n = G_0 \supset G \supset \ldots \supset G_k = \{\mathrm{id}\}$, für die A) und B) für $i = 1, \ldots, k$ gelten, genau dann, wenn $n \leq 4$.

Man sagt: Die Gruppen S_1, S_2, S_3, S_4 sind **auflösbar**, die Gruppen S_n ($n \geq 5$) nicht.
Daraus erhält man zunächst Lösungsformeln für $n = 4$. Für $n \geq 5$ folgt daraus aber nur, dass unsere Methode nicht funktionieren kann. Vielleicht funktioniert aber eine andere Methode und liefert doch die ersehnte Lösungsformel? Nein!

Satz: Sei $n \geq 5$. Es gibt keine Formel, die die Lösungen $x_1, \ldots, x_n$ der Gleichung $x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0$ durch die Koeffizienten $a_0, \ldots, a_{n-1}$ allein mittels wiederholter algebraischer Operationen und Wurzelziehen berechnet.

Man sagt: Die allgemeine Gleichung fünfter oder höherer Ordnung ist nicht in Radikalen lösbar. Die Beweisidee ist, dass man aus einer solchen Formel sukzessive Gruppen $G_0, G_1, \ldots, G_k$ gewinnen könnte, die A) und B) für jedes $i = 1, \ldots, k$ erfüllen. k ist die Verschachtelungstiefe von Wurzeln. G_1 ist im Wesentlichen die Symmetrie der im Innersten liegenden Wurzelausdrücke etc.
Dies lässt sich wirklich sauber am besten in der Sprache der Körpertheorie ausdrücken, und daher soll die kurze Einführung in die Galoistheorie hier enden.

13 Zusammenfassung

Hier noch einmal die Hauptideen in Telegrammform:

- Auflösen der Polynom-Gleichung n-ter Ordnung entspricht dem Berechnen der unsymmetrischen Ausdrücke $x_1, \ldots, x_n$ aus den symmetrischen Ausdrücken $a_0 = \pm x_1 \cdots x_n, \ldots, a_{n-1} = -(x_1 + \cdots + x_n)$.
- Wurzelziehen kann die Symmetrie reduzieren, aber nur auf Normalteiler mit zyklischer Quotientengruppe.
- Für $n \leq 4$ kann man von der Menge aller Symmetrien, S_n, zur vollständigen Asymmetrie, $\{\mathrm{id}\}$, über sukzessive Normalteiler mit zyklischer Quotientengruppe gelangen. Für $n \geq 5$ nicht.
- Daher gibt es Lösungsformeln für $n \leq 4$, aber nicht für $n \geq 5$.

14 Literatur

Natürlich kann in diesem kurzen Artikel nur ein Einblick gegeben werden. Wer Galois-Theorie vollständig verstehen will, sollte ein paar Grundlagen über Gruppen und Körper lernen, wie sie in Algebra-Büchern stehen. Es gibt auch Bücher ausschließlich zum Thema Galois-Theorie. Besonders gut gefällt mir das Buch von H. Edwards (Galois theory, Springer-Verlag, 1984), da es die ursprüngliche Arbeit von Galois und die Zusammenhänge dieser alten mit der modernen

Sichtweise erklärt und damit meiner Darstellung hier am nächsten kommt. Eine hübsche Darstellung mit viel Geschichte und alternativen Lösungsansätzen stammt von J.-P. Tignol (Galois' theory of algebraic equations, World Scientific, 2001). E. Artins Buch (Galoissche Theorie, Verlag Harri Deutsch, 1988) ist ein Klassiker, in dem es etwas geradliniger zur Sache geht.