Die Ideen der Galois-Theorie

Wohl selten war eine wissenschaftliche Entdeckung von so dramatischen Umständen begleitet wie die des erst zwanzigjährigen Mathematikers Evariste Galois. Mit einem in der Nacht zum 30. März 1832 verfaßten Brief übersendet Galois einem Freund Manuskripte, die seine Forschungsergebnisse der vorangegangenen Monate beinhalten. Am nächsten Morgen stellt sich Galois einem vereinbarten Duell, wird dabei schwer verwundet und stirbt am Tag darauf.

Galois Entdeckungen, ihm zum Ehren später Galois-Theorie genannt, lösen eine Fragestellung der Algebra: Unter welchen Bedingungen ist eine Gleichung in einer Unbekannten auflösbar? Noch wichtiger als das gelöste Problem ist allerdings die von Galois dazu verwendete Methode. Ihre Inhalte, namentlich der Begriff der Gruppe, aber auch die Vorgehensweise, unterschiedliche Typen von mathematischen Objekten geschickt miteinander zu verknüpfen, sind heute zum unverzichtbaren Bestandteil der Mathematik geworden.

Die Darstellung der Galois-Theorie erfolgt in modernen Lehrbüchern meist sehr abstrakt. Im Sinne der universellen Bedeutung ist dies zweifellos unabdingbar. Leider wird aber dem mathematischen Laien dadurch der Blick auf die wesentlichen Ideen Galois versperrt. Dem soll hier, wenn auch im bescheidenen Rahmen, abgeholfen werden.

Das Problem

Ausgangspunkt für Galois war das damals ungelöste Problem, das die Lösung von Gleichungen in einer Unbekannten wie etwa

$$x^2 - 2x - 4 = 0$$

oder

$$x^3 - 3x^2 - 3x - 1 = 0$$

betrifft.

Seit dem 16. Jahrhundert sind für solche Gleichungen allgemeine (Auf-)Lösungsformeln bekannt, solange der Grad, also die höchste Potenz der Unbekannten x, nicht größer als 4 ist. Mit den Lösungsformeln können die Lösungen ausgehend von den Koeffizienten, also den Konstanten der Gleichung, durch endlich viele Rechenschritte bestimmt werden. Dabei werden – und das ist die wesentliche Eigenschaft – neben den vier Grundrechenarten nur Wurzeloperationen benötigt. Verwendet man die Lösungsformeln bei den beiden oben angeführten Gleichungen, erhält man

$$x_1 = 1 + \sqrt{5}$$

als eine Lösung der ersten Gleichung sowie

$$x_1 = 1 + \sqrt[3]{2} + \sqrt[3]{4}$$

für die zweite Gleichung.

Beide Gleichungen besitzen noch weitere Lösungen. 1799 bewies der damals 22-jährige Carl Friedrich Gauß, daß eine Gleichung n-ten Grades n Lösungen besitzt. Allerdings bedarf diese Aussage einer Kommentierung: Kann beispielsweise eine Gleichung dritten Grades in eine Form der Gestalt

$$(x - x_1)(x - x_2)(x - x_3) = 0$$

umgewandelt werden, dann sind offensichtlich die Zahlen x_1, x_2 und x_3 die Lösungen der Gleichung - und keine anderen Zahlen sonst. Zu einer Gleichung n-ten Grades kann man immer, so der von Gauß bewiesene Satz, n Zahlen x_1, x_2, ..., x_n finden, so daß die Gleichung entsprechend zerlegt werden kann. Damit besitzt eine Gleichung n-ten Grades stets n Lösungen.

Allerdings müssen die Lösungen nicht unbedingt reell sein, also einer auf dem Zahlenstrahl lokalisierbaren und damit real vorstellbaren Größe entsprechen. Möglich sind vielmehr auch Lösungen im Bereich der komplexen Zahlen, das sind Zahlen der Form a + bi, wobei die Zahl i die Eigenschaft einer Quadratwurzel von -1 besitzt: $i \cdot i = -1$. Außerdem kann es durchaus vorkommen, daß einige der Lösungen x_1, x_2, ... übereinstimmen; auf solche Gleichungen wollen wir hier nicht eingehen – es wird lediglich angemerkt, daß ihre Auflösung auf den Fall mit lauter verschiedenen Lösungen zurückgeführt werden kann.

Der von Gauß bewiesene Satz ist eine reine Existenzaussage – über konkrete Werte der Lösungen oder Verfahren, wie sie berechnet werden, sagt er nichts aus.

Nachdem hunderte von Jahren alle Versuche, eine allgemeine Lösungsformel für die Gleichung fünften Grades zu finden, gescheitert waren, begannen sich zum Ende des 18. Jahrhunderts Zweifel auszubreiten, ob eine solche Formel auf der Basis von Wurzelausdrücken überhaupt existiert. Ein insgesamt schlüssiger Beweis dieser Vermutung gelang aber erst 1824 dem norwegischen Mathematiker Niels Henrik Abel.

Damit war klar, daß es keine Formel gibt, die zu jeder Gleichung die Lösungen in Form von Wurzelausdrücken angibt. Wie sieht es aber für spezielle Gleichungen aus, wie zum Beispiel

$$x^5 + 15x - 44 = 0$$

oder

$$x^5 - x - 1 = 0.$$

Sind diese beiden Gleichungen fünften Grades auflösbar, das heißt, gibt es Wurzelausdrücke für sämtliche Lösungen oder nicht? Galois Ergebnisse ermöglichen eine Antwort: Nur die erste Gleichung ist auflösbar, beispielsweise ist

$$x_1 = \sqrt[5]{-1+\sqrt{2}} + \sqrt[5]{3+2\sqrt{2}} + \sqrt[5]{3-2\sqrt{2}} + \sqrt[5]{-1-\sqrt{2}},$$

eine Lösung, wohingegen die Lösungen der zweiten Gleichung nicht derart durch Wurzeln darstellbar sind!

Zu betonen ist, daß Wurzelausdrücke für die Lösungen nicht deshalb gesucht werden, um numerische Werte zu berechnen. Das Interesse an ihnen resultiert ausschließlich aus grundsätzlichen Erwägungen heraus – vergleichbar etwa mit Dreieckskonstruktionen in der Geometrie, wo auch dem „ob“ und „wie“ mehr Gewicht als dem konkreten Resultat zugemessen wird.

Dagegen reicht es bei praktischen Anwendungen, wenn die numerischen Werte der Lösungen berechnet werden, etwa (in willkürlich gewählter Reihenfolge)

$x_1 = 4{,}51521655...$, $x_2 = 0{,}84506656...$, $x_3 = 0{,}31321057...$, $x_4 = -1{,}67349369...$,

wenn die Gleichung

$$x^4 - 4x^3 - 4x^2 + 8x - 2 = 0$$

zu lösen ist.

Numerische Resultate können mit einer Vielzahl von effektiven Näherungsverfahren bestimmt werden. Die meisten von ihnen arbeiten iterativ, das heißt, sie liefern schrittweise immer genauere Werte. Ist die gewünschte Genauigkeit erreicht, wird das Verfahren abgebrochen. Wurzelausdrücke für die Lösungen lassen sich aus rein numerischen Ergebnissen allerdings kaum ableiten.

Die Galois-Gruppe einer Gleichung

Die Vorgehensweise von Galois ist für die heutige Mathematik sehr typisch, zu seiner Zeit war sie gewiß revolutionär: Jeder Gleichung wird ein Objekt zugeordnet, heute Galois-Gruppe genannt, dessen Eigenschaften Aufschluß darüber geben, ob die Gleichung auflösbar ist oder nicht.

Konstruiert wird die Galois-Gruppe mit Hilfe von (Rechen-)Ausdrücken wie

$$x_1 + x_2 x_2 - x_2 x_3,$$

die sich aus den Lösungen x_1, x_2, ... mittels der Grundrechenarten bilden lassen. Auch ohne Kenntnis der Lösungen ist es häufig möglich, die Werte solcher Ausdrücke zu bestimmen. So ist die Summe aller Lösungen immer gleich dem mit -1 multiplizierten Koeffizienten der zweithöchsten x-Potenz. Beispielsweise für die genannte Gleichung vierten Grades gilt

$$x_1 + x_2 + x_3 + x_4 = 4.$$

Bei derselben Gleichung ebenfalls leicht bestimmbar sind

$$x_1 x_3 + x_2 x_4 = 0$$

und

$$(x_2 + x_4 + x_1 x_2 x_3 x_4)^2 = 8.$$

Etwas aufwendiger darzustellen sind die Werte der folgenden Ausdrücke:

$$\begin{aligned} x_1 - x_2 + x_3 - x_4 &= 4\sqrt{2} \\ x_1x_2 + x_3x_4 &= -2 + 2\sqrt{7} \\ x_1x_4 + x_3x_2 &= -2 - 2\sqrt{7} \\ x_1 - x_3 &= 2(3 + 2\sqrt{2}) \end{aligned}$$

Genau zu beschreiben, wie man solche Identitäten findet, würde hier zu weit führen. Nur soviel: Man ist keineswegs darauf angewiesen, die Gleichungen mit Hilfe der numerischen Werte nachzuprüfen, soweit dies aufgrund der nie ganz vermeidbaren Rundungsfehler überhaupt möglich ist. Vielmehr ist jeder dieser Ausdrücke Lösung einer Gleichung, die aus der Ausgangsgleichung bestimmt werden kann und zwar mit allgemeinen Formeln, die nur Grundoperationen enthalten. So ist etwa der Ausdruck $x_1x_3 + x_2x_4$ für alle Gleichungen vierten Grades Lösung einer Gleichung dritten Grades, die eine Berechnung des Wertes ermöglicht. Im hier gewählten Beispiel geht dies bemerkenswert einfach, man erhält den Wert 0.

Hingegen sind für andere Gleichungen vierten Grades meist umfangreiche Wurzeloperationen notwendig, um die Werte der genannten Ausdrücke darzustellen. So gesehen, spielgeln diese Identitäten Beziehungen zwischen den Lösungen wider, die auf eine gegenüber dem allgemeinen Fall verminderte Komplexität schließen lassen. Galois Verdienst ist es nun, solche Sachverhalte meßbar und klassifizierbar gemacht zu haben. Dazu verwendet man all jene Ausdrücke mit den Lösungen x_1, x_2, ..., deren Wert gleich 0 ist. Bei der vorliegenden Gleichung gehören dazu Ausrücke wie $x_1x_3 + x_2x_4$ oder auch

$$(x_2 + x_4 + x_1 x_2 x_3 x_4)^2 + 4\, x_1 x_2 x_3 x_4.$$

Die Gesamtheit der Ausdrücke mit Wert 0 ist als ganzes nur schwer überschaubar. Galois entwickelte aber eine elegante Methode, die für die Gleichungsauflösung wesentlichen Daten zu charakterisieren. Dies geschieht konkret dadurch, daß man alle möglichen Wege sucht, die Lösungen x_1, x_2, ... so miteinander zu vertauschen, daß jeder Ausdruck mit Wert 0 diesen nicht verändert.

Werden beispielsweise die Lösungen x_1 und x_2 einerseits und x_3 und x_4 andererseits miteinander vertauscht, dann wandelt sich der erste Ausdruck $x_1x_3 + x_2x_4$ zu $x_2x_4 + x_1x_3$, bleibt also unverändert. Der zweite Ausdruck

$$(x_2 + x_4 + x_1 x_2 x_3 x_4)^2 + 4 x_1 x_2 x_3 x_4$$

verwandelt sich zu

$$(x_1 + x_3 + x_2 x_1 x_4 x_3)^2 + 4 x_1 x_2 x_3 x_4,$$

allerdings bleibt der Wert 0 erhalten!

Unter den 4! („4 Fakultät“) = 4·3·2·1 = 24 möglichen Vertauschungen der vier Lösungen gibt es insgesamt acht Vertauschungen, die alle Ausdrücke mit Wert 0 wertmäßig unverändert lassen. Sie zusammen bilden die Galois-Gruppe. Dazu zählt natürlich auch jene „Vertauschung“ p_0, die alles auf seinem Platz beläßt. Die mit p_4 bezeichnete Vertauschung ist die schon beschriebene:

	x_1	x_2	x_3	x_4
p_0	x_1	x_2	x_3	x_4
p_1	x_3	x_2	x_1	x_4
p_2	x_1	x_4	x_3	x_2
p_3	x_3	x_4	x_1	x_2
p_4	x_2	x_1	x_4	x_3
p_5	x_4	x_1	x_2	x_3
p_6	x_2	x_3	x_4	x_1
p_7	x_4	x_3	x_2	x_1

Daß diese Vertauschungen den Wert 0 eines Ausdrucks unverändert lassen, kann mit einem allgemeinen Verfahren von Galois bestätigt werden (siehe Kasten). Umgekehrt verliert durch jede andere Vertauschung mindestens ein Ausdruck seinen Wert 0. Werden zum Beispiel nur die Lösungen x_1 und x_2 miteinander vertauscht, dann ändert sich der Wert von $x_1x_3 + x_2x_4 = 0$ in $x_2x_3 + x_1x_4 = -1 - 2\sqrt{7}$.

Die Bestimmung der Galois-Gruppe

Die Suche nach allen aus den Lösungen x_1, x_2, ... gebildeten Ausdrücken mit Wert 0 ist in der Praxis kaum realisierbar (was die theoretische Bedeutung allerdings nicht schmälert). Zwar können immer endliche viele „Basis"-Ausdrücke gefunden werden, aus denen die (unendliche) Gesamtheit durch einfache Formeln abgeleitet werden kann. Wären solche Basis-Ausdrücke bekannt, müßten die Vertauschungen der Lösungen nur an ihnen getestet werden. Noch einfacher geht es aber mit einem Verfahren von Galois, bei dem sogar nur ein einziger Ausdruck getestet werden braucht.

Man beginnt damit, einen Ausdruck zu suchen, der bei allen möglichen Vertauschungen lauter verschiedene Werte annimmt. Meist erfüllt bereits eine „Zufalls"-Wahl die gewünschte Eigenschaft, bei der Gleichung vierten Grades beispielsweise $t = -x_2 + x_3 - 2x_4$. Galois bewies, daß es immer einen solchen, heute Galois-Resolvente genannten Ausdruck t gibt und daß er dann stets die folgende, wichtige Eigenschaft erfüllt: Alle Lösungen x_1, x_2, ... können allein mit Hilfe von Grundoperationen aus t und den Koeffizienten der Gleichung berechnet werden. Jedem Ausdruck der Lösungen x_1, x_2, ... entspricht daher ein Ausdruck in t, so daß alle Aussagen über Ausdrücke der Lösungen x_1, x_2, ... in Aussagen über Ausdücke mit dem einzigen Wert t übersetzt werden können. Damit wird es möglich, die Wirkung der Vertauschungen ausschließlich anhand der Wirkung auf den Wert von t zu untersuchen. Und das geht am besten, wenn man eine möglichst einfache Gleichung konstruiert, die t als Lösung hat und deren Koeffizienten durch Grundoperationen aus denen der Ausgangsgleichung berechnet werden können. Beispielsweise erfüllt die oben angeführte Galois-Resolvente für die untersuchte Gleichung vierten Grades die Gleichung

$$t^8 + 16t^7 - 40t^6 - 1376t^5 - 928t^4 + 34048t^3 + 22208t^2 - 253184t + 72256 = 0.$$

Interpretiert man diese, nicht mehr zu vereinfachende Gleichung in der Form

$$(-x_2 + x_3 - 2x_4)^8 + 16(-x_2 + x_3 - 2x_4)^7 + ... = 0,$$

so kann die Galois-Gruppe allein anhand daran gefunden werden: Für eine Vertauschung der zur ursprünglichen Gleichung gehörenden Lösungen x_1, x_2, ... muß nämlich geprüft werden, ob bei ihr die Gültigkeit der Gleichung bestehen bleibt oder nicht. Offensichtlich geht das nur, wenn mit der Vertauschung der Wert von t in eine andere Lösung der Gleichung achten Grades überführt wird. Diese acht Lösungen entsprechen damit genau den Vertauschungen der Galois-Gruppe:

$$-x_2 + x_3 - 2x_4,\ -x_2 + x_1 - 2x_4,\ ...,\ -x_3 + x_2 - 2x_1.$$

Mit der Galois-Gruppe ist ein vorläufiger Endpunkt bei der Analyse einer Gleichung erreicht: Ohne Rückgriff auf die ursprüngliche Gleichung kann nämlich allein anhand der Galois-Gruppe entschieden werden, ob die Gleichung auflösbar ist oder nicht. Mehr noch: Bei auflösbaren Gleichungen gehen sogar die zur Auflösung notwendigen Wurzelgrade aus der Galois-Gruppe hervor.

Für solche Aussagen ist nicht nur die Größe der Galois-Gruppe von Bedeutung. Eine Rolle spielen im gewissen Rahmen auch die Vertauschungen selbst, wobei es allerdings einzig auf Beziehungen ankommt, wie sie zwischen den Vertauschungen der Galois-Gruppe bestehen. Eine Möglichkeit, diese vollständig zu tabellieren, ist die sogeanannte Gruppentafel (siehe Kasten). So kann dann allein anhand der Gruppentafel (oder einer äquivalenten Beschreibung der Gruppe) entschieden werden, ob eine Gleichung auflösbar ist oder nicht!

Die Auflösung einer Gleichung

Wie kann eine so enge Beziehung zwischen der Auflösung einer Gleichung und ihrer Galois-Gruppe zustande kommen? Zumindest ansatzweise soll hier angedeutet werden, warum die Galois-Gruppe einer auflösbaren Gleichung ganz bestimmte Eigenschaften haben muß. Dazu ist zunächst der Prozeß einer Gleichungsauflösung detailliert zu charakterisien. Um Komplikationen zu vermeiden, etwa daß einige Lösungen durch Wurzelausdrücke dargestellt werden können und andere nicht, werden nur solche Gleichungen untersucht, die nicht sofort vereinfacht werden können. Das heißt, keine Lösung x_1, ... x_n darf eine Gleichung erfüllen, die einfacher ist als die ursprüngliche – also mit niedrigerem Grad und Koeffizienten, die mittels Grundoperationen aus denen der Ausgangsgleichung hervorgehen können. Ein Resultat der Galois-Theorie besagt, daß dies gleichbedeutend damit ist, daß jede Lösung auf eine beliebige andere Lösung mit zumindest einer Vertauschung aus der Galois-Gruppe geschoben werden kann.

Der Auflösungsprozeß einer Gleichung verläuft, sofern er überhaupt möglich ist, immer schrittweise. Zur Abgrenzung der einzelnen Schritte bieten sich die Wurzeln als herausragende Operationen an. Dabei geht der Radikand jeweils unter ausschließlicher Verwendung der vier Grundoperationen aus Werten vorangegangener Schritte sowie aus Koeffizienten der Gleichung hervor. Es läßt sich zudem immer einrichten, daß alle Wurzelgrade Primzahlen sind.

Die Gruppentafel einer Galois-Gruppe

Führt man zwei Vertauschungen der Galois-Gruppe nacheinander aus, dann entsteht wieder eine Vertauschung. Läßt jede der beiden Vertauschungen bei Ausdrücken den Wert, sofern er gleich 0 ist, unverändert, dann gilt dies auch für die zusammengesetzte Vertauschung. Diese gehört damit ebenfalls zu Galois-Gruppe.

Als Beispiel nehmen wir die Vertauschungen p_1 und p_6 der hier konstruierten Galois-Gruppe. Die Lösung x_1 wird durch die Vertauschung p_1 auf die Stelle von x_3 geschoben. Da x_3 von der zweiten Vertauschung p_6 nach x_4 geschoben wird, ergibt sich für x_1 insgesamt ein Wechsel nach x_4. Für die anderen Lösungen verfährt man entsprechend und erhält:

	x_1	x_2	x_3	x_4
erst p_1 ...	x_3	x_2	x_1	x_4
... und dann p_6	x_4	x_3	x_2	x_1

Ein Blick auf die Tabelle der Vertauschungen zeigt, daß es sich bei der zusammengesetzten Vertauschung um p_7 handelt. Bei der Gruppentafel handelt es sich ähnlich wie bei einer Einmal-Eins-Tafel um eine Tabelle, in der alle Möglichkeiten, zwei Vertauschungen nacheinander auszuführen, zusammengestellt sind. Tabelliert sind also alle Ergebnisse der Form „erst p und dann q“:

q \ p	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7
p_0	p_0	p_1	p_2	p_3	p_4	p_5	p_6	p_7
p_1	p_1	p_0	p_3	p_2	p_6	p_7	p_4	p_5
p_2	p_2	p_3	p_0	p_1	p_5	p_4	p_7	p_6
p_3	p_3	p_2	p_1	p_0	p_7	p_6	p_5	p_4
p_4	p_4	p_5	p_6	p_7	p_0	p_1	p_2	p_3
p_5	p_5	p_4	p_7	p_6	p_2	p_3	p_0	p_1
p_6	p_6	p_7	p_4	p_5	p_1	p_0	p_3	p_2
p_7	p_7	p_6	p_5	p_4	p_3	p_2	p_1	p_0

Alle Beziehungen, wie sie zwischen den Vertauschungen bestehen, können aus der Gruppentafel ersehen werden. Nicht mehr erkennbar ist, wie die Lösungen durch die Vertauschungen bewegt werden.

Beispielsweise kann Gleichung die schon untersuchte Gleichung vierten Grades

$$x^4 - 4x^3 - 4x^2 + 8x - 2 = 0$$

aufgelöst werden:

$$x_{1,3} = 1 + \sqrt{2} \pm \sqrt{3 + \sqrt{2}}$$

$$x_{2,4} = 1 - \sqrt{2} \pm \sqrt{3 - \sqrt{2}}$$

Die drei Auflösungschritte werden durch die Zwischenwerte

$$\sqrt{2},\ \sqrt{3+\sqrt{2}} \text{ und } \sqrt{3-\sqrt{2}}$$

markiert. Aus ihnen und den Koeffizienten ergeben sich schließlich alle vier Lösungen durch Grundoperationen.

Fortgesetzte Auslese von Vertauschungen

Die einzelnen Schritte der Gleichungsauflöung können nun in Beziehung zur Galois-Gruppe gesetzt werden. Dazu wird innerhalb der Galois-Gruppe ein schrittweiser Ausleseprozeß konstruiert, dessen Schritte exakt den Schritten der Auflösung entsprechen. Dies geschieht dadurch, daß die zur Definition der Galois-Gruppe verwendete Gesamtheit von Ausdrücken mit den Lösungen x_1, x_2, ... mit jedem Auflösungschritt erweitetert wird. Konkret wird jeweils jeder Ausdruck zugelassen, dessen Wert aus den Koeffizienten der Gleichung und allen vorangegangenen Zwischenwerten durch Grundoperationen hervorgehen kann. Wie bei der Konstruktion der Galois-Gruppe werden schließlich alle Vertauschungen herausgesucht, die bei der nun vergrößerten Gesamtheit von Ausdrücken die Werte unverändert lassen.

Durch die ansteigenden Anforderungen erhält man in jedem Schritt höchstens die Vertauschungen des vorangegangenen Schrittes, meist jedoch deutlich weniger. Insgesamt ergibt sich daher ein Ausleseprozeß innerhalb der Galois-Gruppe.

Als Beispiel für den beschreibenen Ausleseprozeß bieten sich die Zwischenwerte der für die Gleichung vierten Grades gegebenen Auflösung an:

Aufgrund des ersten Zwischenwertes $\sqrt{2}$ vergrößert sich die in Betracht zu ziehende Gesamtheit von Ausdrücken beispielsweise um $x_1 - x_2 + x_3 - x_4 = 4\sqrt{2}$. Unter den acht Vertauschungen der Galois-Gruppe fallen p_4, p_5, p_6 und p_7 der Auslese zum Opfer, da sie auf der linken Seite der Gleichung das Vorzeichen ändern. Hingegen lassen die Vertauschungen p_0 bis p_3 den fraglichen, aber auch die anderen dazugekommenen Ausdrücke wertmäßig unverändert.

Kommt dann noch der zweite Zwischenwert $\sqrt{3+\sqrt{2}}$ hinzu, sind zusätzlich Ausdrücke wie

$$x_1 - x_3 = 2\sqrt{3+\sqrt{2}}$$

und

$$x_1 = 1+\sqrt{2}+\sqrt{3+\sqrt{2}}$$

bei der Auslese der Vertauschungen zu berücksichtigen.. Von den bislang verbliebenen Vertauschungen p_0 bis p_3 lassen nur p_0 und p_2 den Wert von x_1 - x_3 unverändert, während die beiden anderen ein Vorzeichenwechsel bewirken.

Der dritte Zwischenwert ist darstellbar durch

$$x_2 - x_4 = 2\sqrt{3-\sqrt{2}},$$

von den Vertauschungen p_0 und p_2 bleibt nur noch die erste übrig, da p_2 bei x_2 - x_4 das Vorzeichen ändert. Daß – wie nach jeder vollständigen Gleichungsauflösung – keine echte Vertauschung mehr übrig geblieben sein kann, ist auch daran zu erkennen, daß alle Lösungen x_1,..., x_4 mittels Grundoperationen aus den Zwischenwerten bestimmt werden können.

Auflösung der Gleichung	Ausleseprozeß bei den Vertauschungen
$\sqrt{3-\sqrt{2}}$	p_0
↑ Quadratwurzel	
$\sqrt{3+\sqrt{2}}$	$p_0,\ p_2$
↑ Quadratwurzel	
$\sqrt{2}$	$p_0,\ p_2,\ p_2,\ p_3$
↑ Quadratwurzel	
Koeffizienten der Gleichung	$p_0,\ p_2,\ p_2,\ p_3$ $p_4,\ p_5,\ p_6,\ p_7$

Im Auflösungsprozeß notwendige Grundoperationen sind nicht dargestellt.

Wie Wurzeln in der Galois-Gruppe wirken

Wie schon anhand des Beispiels zu vermuten ist, kann ein einzelner Ausleseschritt innerhalb der Galois-Gruppe keineswegs beliebige Formen annehmen, vielmehr gilt folgende Gesetzmäßigkeit: Bewirkt eine Wurzel mit Primzahlgrad p überhaupt eine echte Auslese, dann lassen sich die Vertauschungen vor dem Ausleseprozeß in p gleich große Klassen einteilen, wobei eine Klasse genau die nach der Auslese übrigbleibenden Vertauschungen umfaßt. Sortiert man außerdem die Vertauschungen am linken und oberen Rand der Gruppentafel klassenweise, dann zerfällt das Innere in p^2 gleich große Teilquadrate, von denen jede nur Vertauschungen aus einer einzigen Klasse enthält.

Zur Erläuterung bietet sich wieder das Beispiel an (weitergehende Information grundsätzlicher Art findet man im Kasten): Für den ersten Schritt müssen die Vertauschungen nicht umsortiert werden, da sie bereits oben entsprechend den beiden Klassen, nämlich p_0 bis p_3 einerseits und p_4 bis p_7 andererseits, angelegt ist. Die Zerlegung der Gruppentafel in vier Teilquadrate, die jeweils nur die Vertauschungen einer Klasse enthalten, ist daher offensichtlich.

Das aus ihnen gebildete obere Teilquadrat kann nun so umsortiert werden, daß die Zerlegung zur Auslese nach p_0, p_2 möglich wird:

q \ p	p_0	p_2	p_1	p_3
p_0	p_0	p_2	p_1	p_3
p_2	p_2	p_0	p_3	p_1
p_1	p_1	p_3	p_0	p_2
p_3	p_3	p_1	p_2	p_0

Der noch ausstehende Teil des Auflösungsprozesses wird durch das Teilquadrat oben links charakterisiert. Es kann sofort in vier 1×1-Teilquadrate zerlegt werden, was dem zweiten Auflösungsschritt entspricht.

Nicht alle Gleichungen sind auflösbar!

Wie dargelegt muß es für Galois-Gruppen von auflösbaren Gleichungen immer einen Ausleseprozeß geben, der von der vollen Gruppe bis zur Vertauschung p_0 verläuft und dessen Schritte die beschriebene Klasseneinteilung aufweisen. Daher folgt im Umkehrschluß, daß eine Gleichung, in deren Galois-Gruppe solches unmöglich ist, nicht auflösbar sein kann. Ein Beispiel ist die schon genannte Gleichung $x^5 - x - 1 = 0$, deren Galois-Gruppe 120 Vertauschungen enthält. Möglich zunächst nur eine Zerlegung in vier Teilquadrate, allerdings kann das

dabei entstehende 60×60-Teilquadrat selbst nicht mehr weiter zerlegt werden! Ist man bereit, auf jegliche mathematische Eleganz zu verzichten, kann sogar ein Computer solche Resultate bestätigen.

Wie Vertauschungen bei Wurzelausdrücken wirken

Im untersuchten Beispiel halbiert sich bei jedem Auflösungschritt die Zahl der Vertauschungen. Am besten läßt das erkennen, wenn man die neu hinzugekommenen Zwischenwerte

$$\sqrt{2},\ \sqrt{3+\sqrt{2}} \text{ und } \sqrt{3-\sqrt{2}}$$

jeweils durch einen Ausdruck der Lösungen x_1, x_2, ... darstellt. Dann kann nämlich der Ausleseschritt allein anhand von diesem Ausdruck vorgenommen werden. Eine Hälfte der zu prüfenden Vertauschungen läßt nämlich den Wert des Ausdrucks unverändert, während die andere sein Vorzeichen ändert. Es läßt sich zeigen, daß entsprechendes immer der Fall ist, allerdings müssen bei höheren Wurzelgraden auch nicht-reelle Wurzeln der 1 herangezogen werden. Beispielsweise beginnt die Auflösung der schon angeführten Gleichung $x^3 - 3x^2 - 3x - 1 = 0$, deren Galois-Gruppe drei Vertauschungen umfaßt, mit dem Zwischenwert $\sqrt[3]{2}$. Mit Hilfe des Ausdrucks

$$x_1^3 - 3x_1 - 2 = \sqrt[3]{2}$$

kann nun die Auslese vorgenommen werden. Die dritte Potenz ist gleich einer ganzen Zahl, also bleibt $(x_1^3 - 3\,x_1 - 2)^3$ bei Vertauschungen der Galois-Gruppe wertmäßig unverändert. Für den Ausdruck $x_1^3 - 3\,x_1 - 2$ hat das zur Folge, daß die Vertauschungen der Galois-Gruppe eine Multiplikation mit einer dritten Wurzel von 1 bewirken. Beispielsweise ist

$$x_2^3 - 3x_2 - 2 = (-\tfrac{1}{2} + i\tfrac{\sqrt{3}}{2}) \cdot \sqrt[3]{2}.$$

Nicht auflösbar sind, von seltenen Exoten wie etwa der Gleichung $x^5 + 15x - 44 = 0$ (die Galois-Gruppe enthält 10 Vertauschungen) abgesehen, auch andere Gleichungen fünften Grades. Die Auflösbarkeit von Gleichungen fünften und höheren Grades wird somit zur Ausnahmeerscheinung.

Mit der Galois-Theorie läßt sich aber nicht nur die Nicht-Auflösbarkeit einer Gleichung nachweisen. Umgekehrt können zu jedem Ausleseprozeß, der die beschriebenen Eigenschaften besitzt, Wurzelformeln für sämtliche Lösungen abgeleitet werden. Auflösung einer Gleichung und Ausleseprozeß innerhalb der Galois-Gruppe sind damit vollkommen äquivalent! Diese enge Korrespondez zwischen Gleichung und Auflösungsprozeß einerseits und Galois-Gruppe und

Ausleseprozeß andererseits ist die Essenz von Galois Entdeckung. In der Fachsprache wird dem auch in der Bezeichnung Rechnung getragen: Was hier Ausleseprozeß genannt wird, nennt man schlicht „Auflösung einer Gruppe“.

Literaturhinweise

Galois Theory, Harold M. Edwards. Springer, New York 1984 (enthält u.a. die kommentierte Originalarbeit von Galois).

Galoissche Theorie, E. Artin. Harri Deutsch, Zürich 1973.

Algebra, Band I., B.L.van der Waerden. Springer, Berlin 1971.

Das kurze Leben des Evariste Galois, Tony Rothman, Spektrum der Wissenschaft, Juni 1982.

Tel. ++49/(0)6431-8537;

WWW: http://www.bewersdorff-online.de;

EMail: joerg.bewersdorff@t-online.de