Die Suche nach einer Lösungsformel, die nie existierte: Galoistheorie

Vortrag beim 25. Berliner Tag der Mathematik — ab 9. Klasse

Dirk Kussin

TU Berlin

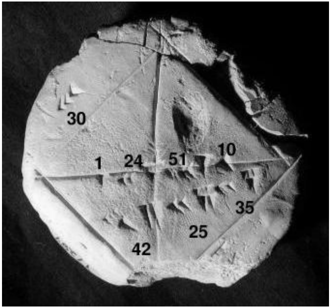
Berlin, 30. April 2022

Grundlegende Problemstellung in der Algebra: Lösung von Gleichungen.

(Quadratische Gleichungen)

$$x^2 + px + q = 0$$

Dies konnten schon die alten Babylonier vor fast 4000 Jahren! (Vgl. quadratische Ergänzung.)



Keilschrift-Tafel zur Darstellung von $\sqrt{2}$

Heute ist jeder Schülerin und jedem Schüler bekannt:

(p-q-Formel)

$$x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}$$

Beobachtung

Die Formel berechnet die Lösung aus dem Bereich der Koeffizienten (p und q) nur mit Hilfe der Operationen $+$, $-$, $\cdot$, $/$ und (Quadrat-) Wurzelziehen $\sqrt{}$.

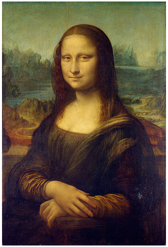
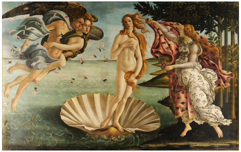
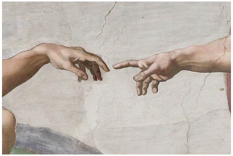
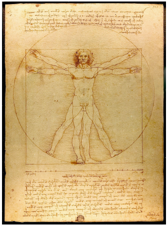
Die Formel ist für alle Koeffizienten p und q gleich.

Möchte ähnliche Lösungsformel auch für höhere Grade haben.

(Kubische Gleichungen)

$$x^3 + px + q = 0$$

Zwischen der Lösung der quadratischen Gleichung und der der kubischen lagen gut 3000 Jahre!

Italienische Renaissance

$$x^3 + px + q = 0$$

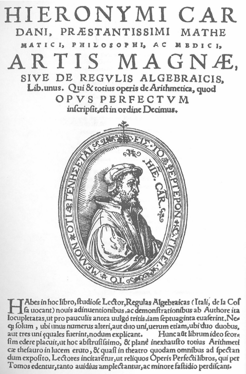
Eine Lösung ist gegeben durch:

(Cardanische Formel: G. Cardano 1545)

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$$

Weitere Lösungen ergeben sich durch Modifikation davon.

Große Kunst



HIERONYMI CAR
DANI, PRÆSTANTISSIMI MATHE
MATICI, PHILOSOPHI, AC MEDICI,
ARTIS MAGNÆ,
SIVE DE REGVLIS ALGEBRAICIS,
Lib. unus. Qui & totius operis de Arithmetica, quod
OPVS PERFECTVM
inscripsit, est in ordine Decimus.

HAbes in hoc libro, studiose Lector, Regulas Algebraicas (Itali, de la Cossa uocant) nouis adinuentionibus, ac demonstrationibus ab Authore ita locupletatas, ut pro pauculis antea uulgò tritis, iam septuaginta euaserint. Neque solum, ubi unus numerus alteri, aut duo uni, uerum etiam, ubi duo duobus, aut tres uni æquales fuerint, nodum explicant. Hunc aũt librum ideo seorsim edere placuit, ut hoc abstrusissimo, & planè inexhausto totius Arithmeticæ thesauro in lucem eruto, & quasi in theatro quodam omnibus ad spectandum exposito, Lectores incitarẽtur, ut reliquos Operis Perfecti libros, qui per Tomos edentur, tanto auidius amplectantur, ac minore fastidio perdiscant.

Ars Magna von Gerolamo Cardano, erschienen 1545

Vorher schon: del Ferro (1515), Tartaglia (1535), und auch für Grad 4: Ferrari (1540). Cardano veröffentlichte diese Ergebnisse erstmals in seinem Buch.

Beispiel

$$x^3 + 3x - 36 = 0$$

$$x = \sqrt[3]{18 + \sqrt{325}} + \sqrt[3]{18 - \sqrt{325}}$$

Andererseits ist offenbar $x = 3$ eine Lösung!

Beispiel

$$x^3 - 7x + 6 = 0$$

$$x = \sqrt[3]{-3 + \sqrt{-\frac{100}{27}}} + \sqrt[3]{-3 - \sqrt{-\frac{100}{27}}}$$

Beachte: Quadratwurzel aus negativer Zahl!
Andererseits sind offenbar $x = 1$, 2 und -3 alle Lösungen!

Fazit

Formel nicht immer praktisch. Sog. komplexe Zahlen unerlässlich.

$$x^5 + ax^4 + bx^3 + cx^2 + dx + e = 0$$

oder spezieller

$$x^5 + px + q = 0$$

Frage

Gibt es auch für Gleichungen vom Grad 5 (oder höher) ähnliche Formeln, die die Lösungen nur mit $+$, $-$, $\cdot$, $/$ und (höheres) Wurzelziehen $\sqrt[n]{}$ aus den Koeffizienten der Gleichung berechnen?

Für die Lösung dieser Frage wurden weitere 250 Jahre benötigt!

Wichtige (Vor-) Arbeiten dazu wurden von Girard, Newton, Gauß und anderen geleistet, und besonders auch von Lagrange (in einer 1770 in Berlin verfassten Arbeit).

Die Antwort wurde erst von Ruffini (-1813, noch lückenhaft) und Abel (um 1824; 1826 verbessert in Berlin) gefunden. Die Antwort ist negativ:

Satz (von Ruffini-Abel)

Für Grad 5 *(und höher) gibt es keine allgemeine Lösungsformel (im obigen Sinne) mehr.*

Um es klar zu sagen: Ruffini und Abel haben bewiesen, dass es allgemein keine solche Formel geben kann.

Niels Henrik Abel (1802–1829)

Was der Satz von Ruffini-Abel aber nicht thematisiert, ist die (offensichtliche) Feststellung, dass $\overline{\text{gewisse}}$ Gleichungen fünften Grades mittels $+$, $-$, $\cdot$, $/$ und Wurzelziehen $\sqrt[n]{}$ lösbar sind.
Z. B. ist dies offensichtlich für eine Gleichung wie

$$x^5 - 2 = 0$$

Hier ist eine Lösung gegeben durch

$$x = \sqrt[5]{2}$$

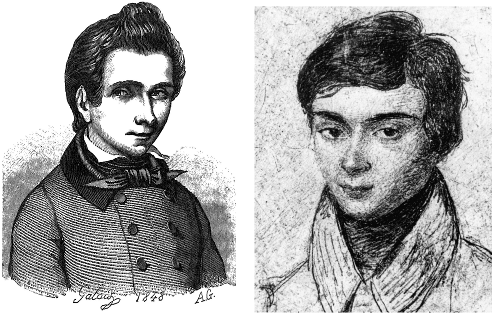
Die weiteren (vier) Lösungen bekommt man durch einen einfachen Mechanismus (innerhalb der komplexen Zahlen).

Es gibt noch viele weitere "auflösbare" Gleichungen.

Frage

Wie entscheidet man, welche Gleichungen "auflösbar" (im obigen Sinne) sind und welche nicht?

Die genialen Ideen zur (vollständigen) Beantwortung dieser Frage stammen von



Évariste Galois (1811–1832)

Durch seine revolutionären, mathematischen Denkweisen, gilt er als der Begründer der modernen Algebra. Auch politisch war er in den Wirren der Revolution aktiv, kam dafür ins Gefängnis, wurde der Hochschule verwiesen und starb im Alter von 20 Jahren in einem Duell.

$$f(x) \;=\; x^5 + ax^4 + bx^3 + cx^2 + dx + e \;=\; 0$$

Galois betrachtete "abstrakt" die Gesamtheit aller (fünf) Lösungen, $x = A, B, C, D, E$. (Man kann annehmen, dass man die Gleichung nicht in welche kleineren Grades zerlegen kann, sonst wäre es einfach.)
Es gilt dann ("Abspalten von Nullstellen von $f(x)$ als Linearfaktoren")

$$f(x) \;=\; (x-A)\cdot(x-B)\cdot(x-C)\cdot(x-D)\cdot(x-E)$$

Galois betrachtete nun die "Symmetrien" der Gleichung. Was ist damit gemeint?
Zunächst kann man die 5 Lösungen permutieren:

$$ABCDE,\; BCDEA,\; CDEAB,\; DEABC,\; EABCD,\; BACDE,\; \ldots$$

Insgesamt gibt es hier $1\cdot 2\cdot 3\cdot 4\cdot 5 = 120$ Möglichkeiten.

(Symmetrien)

Symmetrien der Gleichung $f(x) = 0$ sind nur solche Permutationen, die "algebraische" Beziehungen zwischen den Lösungen bewahren.

Dazu ein Beispiel. Der Einfachheit halber eines vom Grad 4.

$$x^4 - 5x^2 + 6 \;=\; 0$$

Dies ist quadratisch in x^2, und mit der p-q-Formel erhalten wir die Lösungen

$$A = \sqrt{2}\,, \quad B = -\sqrt{2}\,, \quad C = \sqrt{3}\,, \quad D = -\sqrt{3}$$

Insgesamt gibt es $1 \cdot 2 \cdot 3 \cdot 4 = 24$ Permutationen von $ABCD$.

Es gibt aber gewisse “algebraische” Beziehungen zwischen den A, B, C, D. Zum Beispiel:

$$A + B = 0, \quad A^2 = 2 = B^2, \quad C + D = 0, \quad C^2 = 3 = D^2, \quad AC - BD = 0$$

Wenn man nun A und B vertauscht, und/oder C und D, so gelten die gleichen Beziehungen weiterhin.
Aber nicht, wenn man z. B. A und C vertauscht!
Wenn also nur solche Permutationen “erlaubt” sind (und die wir dann “Symmetrien” nennen), die obige Beziehungen bewahren, so bleiben von den 24 nur folgende 4 Permutationen übrig:

$$ABCD, \ BACD, \ ABDC, \ BADC$$

Man kann diese Symmetrien miteinander verknüpfen. Z. B. kann man erst A und B vertauschen (ergibt $BACD$), und dann C und D, so ergibt dies $BADC$. Und jede Symmetrie hat auch eine “umgekehrte” Symmetrie. Die Symmetrien bilden also, was Galois eine Gruppe nannte, und was Mathematiker heute immer noch so nennen. Die Symmetriegruppe der Gleichung. (Heute nennt man sie Galoisgruppe.)

Frage

Wozu das ganze?

Galois erkannte, dass die Gleichung $f(x) = 0$ nur dann auflösbar ist, wenn es "nicht zu viele" Symmetrien gibt, wenn die Symmetriegruppe also nicht zu kompliziert ist. Genauer:

Satz (Galois 1831)

Eine Gleichung $f(x) = 0$ fünften Grades ist immer dann auflösbar, wenn sie nur 5, 10 oder 20 Symmetrien hat. In allen anderen Fällen (dann gibt es 60 oder 120 Symmetrien) ist sie nicht auflösbar.

Beispiel 1

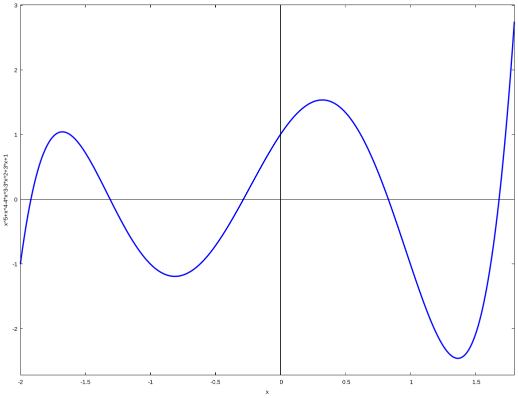
$$x^5 - 2 = 0$$

Hier gibt es genau 20 Symmetrien. Das passt also dazu, dass diese Gleichung durch $x = \sqrt[5]{2}$ auflösbar ist.

Beispiel 2

$$x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1 = 0$$

Man kann leicht zeigen, dass wenn x eine Lösung ist, dann auch $x^2 - 2$. Es gibt 5 reelle Lösungen, siehe Nullstellen im Funktionsgraphen:



Funktionsgraph

Bezeichnen wir sie von links nach rechts mit A, B, C, D, E, so sehen wir, dass $x \mapsto x^2 - 2$ aus $ABCDE$ die Permutation $ECABD$ macht. Wendet man immer wieder diese Transformation an, so erhalten wir $ABCDE \mapsto ECABD \mapsto DAECB \mapsto BEDAC \mapsto CDBEA \mapsto ABCDE$, und dies sind alle 5 Symmetrien. Diese Gleichung ist also auflösbar.

Beispiel 3

$$x^5 - 6x + 3 = 0$$

hat 120 Symmetrien. Also können wir daraus schließen, dass es hierfür keine Lösungsformel gibt.

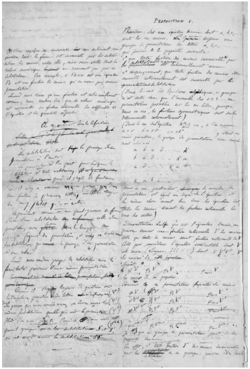
Beispiel 4

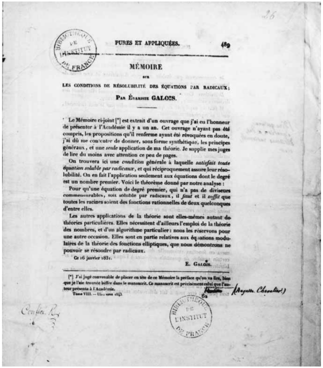
$$x^5 + 15x + 12 = 0$$

hat genau 20 Symmetrien, und man kann zeigen, dass eine Lösung gegeben ist durch

$$x = \sqrt[5]{\frac{-75 - 21\sqrt{10}}{125}} + \sqrt[5]{\frac{-75 + 21\sqrt{10}}{125}} + \sqrt[5]{\frac{225 - 72\sqrt{10}}{125}} + \sqrt[5]{\frac{225 + 72\sqrt{10}}{125}}$$

Galois' Arbeit dazu wurde am 16. Januar 1831 von ihm eingereicht, aber erst 1846 in einer mathematischen Zeitschrift veröffentlicht.





PURES ET APPLIQUÉES. 489

MÉMOIRE

SUR

LES CONDITIONS DE RÉSOLUBILITÉ DES ÉQUATIONS PAR RADICAUX;

PAR ÉVARISTE GALOIS.

Le Mémoire ci-joint [*] est extrait d'un ouvrage que j'ai eu l'honneur de présenter à l'Académie il y a un an. Cet ouvrage n'ayant pas été compris, les propositions qu'il renferme ayant été révoquées en doute, j'ai dû me contenter de donner, sous forme synthétique, les principes généraux, et une *seule* application de ma théorie. Je supplie mes juges de lire du moins avec attention ce peu de pages.

On trouvera ici une *condition* générale à laquelle *satisfait toute équation soluble par radicaux*, et qui réciproquement assure leur résolubilité. On en fait l'application seulement aux équations dont le degré est un nombre premier. Voici le théorème donné par notre analyse :

Pour qu'une équation de degré premier, qui n'a pas de diviseurs commensurables, soit soluble par radicaux, il *faut* et il *suffit* que toutes les racines soient des fonctions rationnelles de deux quelconques d'entre elles.

Les autres applications de la théorie sont elles-mêmes autant de théories particulières. Elles nécessitent d'ailleurs l'emploi de la théorie des nombres, et d'un algorithme particulier : nous les réservons pour une autre occasion. Elles sont en partie relatives aux équations modulaires de la théorie des fonctions elliptiques, que nous démontrons ne pouvoir se résoudre par radicaux.

Ce 16 janvier 1831.

E. GALOIS.

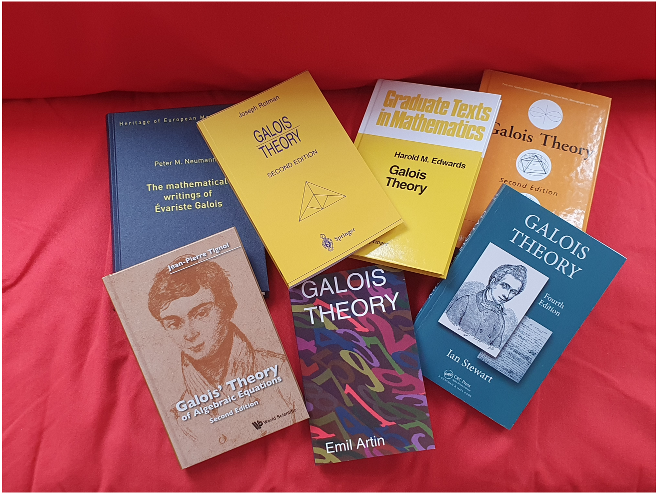
[*] J'ai jugé convenable de placer en tête de ce Mémoire la préface qu'on va lire, bien que je l'aie trouvée biffée dans le manuscrit. Ce manuscrit est précisément celui que l'auteur présenta à l'Académie.

Tome VIII. — [illegible] 1843. 62

Teil des Originalmanuskripts, 1. Seite Druckfahnen

Abbildungen aus: Peter M. Neumann, The mathematical writings of Évariste Galois, EMS 2011

Heute ist Galois' großer Einfluss nicht mehr wegzudenken.

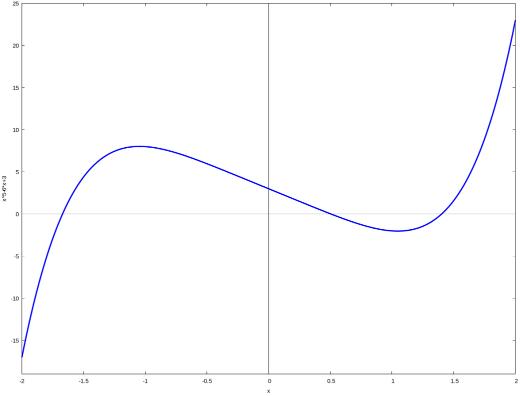


Bücher über Galois' Theorie

Zu Beispiel 3: Skizze für 120 Symmetrien

$$x^5 - 6x + 3 = 0$$

Gibt genau 3 reelle Nullstellen A, B und C:



Funktionsgraph

Zu Beispiel 3 (Fortsetzung)

Gibt also genau zwei nicht-reelle, komplexe Nullstellen D und E.

Diese treten als komplex-konjugiertes Paar auf.

Eine Symmetrie besteht darin, diese beiden zu vertauschen:

$$D \leftrightarrow E \quad \text{also} \quad ABCDE \leftrightarrow ABCED$$

Es gibt auch immer (wie in Beispiel 2) die “zyklischen” Symmetrien[1]

$$ABCDE \mapsto BCDEA \mapsto CDEAB \mapsto DEABC \mapsto EABCD \mapsto ABCDE$$

Dies folgt z. B. aus einem Satz von Cauchy (1845). (Wusste auch Galois.)

Man sieht, dass sich damit alle 120 Permutationen erzeugen lassen, dies also allesamt Symmetrien sind.

[1] Bei geeigneter Reihenfolge der A, B, C, D, E.

Zu Beispiel 1: Skizze für 20 Symmetrien

$$f(x) = x^5 - 2 = 0$$

$A = \sqrt[5]{2}$ ist eine (reelle) Lösung.
Es gibt vier weitere nicht-reelle, komplexe Lösungen B, C, D, E.
Auch hier gibt es wieder die 5 "zyklischen" Permutationen.

Sei ω eine 5. "Einheitswurzel" $\neq 1$: $\omega^5 = 1$.
Gleichung $x^5 - 1 = 0$ hat die 5 Lösungen

$$1, \quad \omega, \quad \omega^2, \quad \omega^3, \quad \omega^4$$

Dann: die 5 komplexen Lösungen von $f(x) = 0$ sind

$$A, \quad B = \omega A, \quad C = \omega^2 A, \quad D = \omega^3 A, \quad E = \omega^4 A$$

4 weitere Symmetrien durch Transformationen des Typs

$$\omega A \mapsto \omega^2 A \mapsto \omega^4 A \mapsto \omega^8 A = \omega^3 A \mapsto \omega^6 A = \omega A$$

Zu Beispiel 1 (Fortsetzung)

Zusammen also: die 5 zyklischen Permutationen von oben

$$ABCDE \mapsto BCDEA \mapsto CDEAB \mapsto DEABC \mapsto EABCD \mapsto ABCDE$$

und die 4 zyklischen Permutationen (A fest)

$$ABCDE \mapsto ACEBD \mapsto AEDCB \mapsto ADBEC \mapsto ABCDE$$

und alle Kombinationen daraus: ergibt $5 \cdot 4 = 20$ Symmetrien.