Die Unlösbarkeit der Gleichung fünften Grades durch Radikale

Teilnehmer:

Max Bender	Andreas-Oberschule
Marcus Gawlik	Georg-Forster-Oberschule
Anton Milge	Georg-Forster-Oberschule
Leonard Poetzsch	Georg-Forster-Oberschule
Gabor Radtke	Georg-Forster-Oberschule
Miao Zhang	Andreas-Oberschule

Gruppenleiter:

Jürg Kramer	Humboldt-Universität zu Berlin, Mitglied im DFG-Forschungszentrum MATHEON „Mathematik für Schlüsseltechnologien“

Die Gruppe beschäftigte sich mit der Frage nach der Lösbarkeit der allgemeinen Gleichung fünften Grades durch Radikale. Zunächst wurde dazu festgestellt, dass lineare, quadratische, kubische und quartische Gleichungen durch Radikale lösbar sind.
Mit Hilfe von N.-H. Abels Originalarbeit aus dem 19. Jh. erarbeitete sich die Gruppe dann das Ergebnis, dass die allgemeine Gleichung fünften Grades nicht durch Radikale lösbar ist.
Dazu musste sich die Gruppe einige Grundlagen der Gruppen- sowie der Körpertheorie erarbeiten. Speziell spielte das Verständnis der symmetrischen Gruppe S_5 von fünf Elementen eine wichtige Rolle.

Die Unlösbarkeit der allgemeinen Gleichung fünften Grades durch Radikale

1 Einleitung

Die allgemeine Gleichung eines Polynoms n-ten Grades mit den Koeffizienten $\sigma_1, \ldots, \sigma_n$ lautet

$$f(X) = X^n - \sigma_1 X^{n-1} \pm \ldots + (-1)^{n-1}\sigma_{n-1}X + (-1)^n\sigma_n.$$

Nach dem Fundamentalsatz der Algebra besitzt ein solches Polynom genau n Nullstellen $x_1, \ldots, x_n \in \mathbb{C}$. Somit lässt sich die Funktion eindeutig als Produkt ihrer Linearfaktoren darstellen

$$f(X) = (X - x_1) \cdot (X - x_2) \cdot \ldots \cdot (X - x_n).$$

Nach dem Vietaschen Wurzelsatz ergeben sich folgende Zusammenhänge zwischen den Nullstellen $x_1, \ldots, x_n$ und den Koeffizienten $\sigma_1, \ldots, \sigma_n$

$$\begin{array}{rcccc} \sigma_1 & = & \sigma(x_1, \ldots, x_n) & = & x_1 + \ldots + x_n, \\ \sigma_2 & = & \sigma(x_1, \ldots, x_n) & = & x_1 \cdot x_2 + x_1 \cdot x_3 + \ldots + x_{n-1} \cdot x_n, \\ \vdots & & & & \\ \sigma_n & = & \sigma(x_1, \ldots, x_n) & = & x_1 \cdot x_2 \cdot \ldots \cdot x_n. \end{array}$$

Aufgrund ihrer Symmetrie verändern sich die Werte dieser Funktionen beim Vertauschen (Permutieren) der Variablen nicht. Sie werden deshalb die *elementarsymmetrischen Polynome* in den Variablen $x_1, \ldots, x_n$ genannt. Von großer Bedeutung für den sich später ergebenden Widerspruch ist, dass die $x_1, \ldots, x_n$ als variabel vorausgesetzt werden. Das bedeutet, dass keine algebraischen Zusammenhänge zwischen den Variablen $x_1, \ldots, x_n$ bestehen dürfen. Als Vorbereitung auf die nachfolgende, grundlegende Definition betrachten wir das Beispiel einer quadratischen Gleichung, d.h.

$$X^2 - \sigma_1 X + \sigma_2 = 0. \tag{1}$$

Die beiden Lösungen dieser Gleichung lassen sich mithilfe der p, q-Formel berechnen zu

$$x_{1,2} = \frac{\sigma_1}{2} \pm \sqrt{\frac{\sigma_1^2}{4} - \sigma_2}.$$

Dabei sieht man, dass die auftretenden Funktionen $p = \sigma_1/2$ und $R = \sigma_1^2/4 - \sigma_2$ rationale Funktionen (in diesem Fall sogar Polynome) in den elementarsymmetrischen Polynomen σ_1, σ_2 sind.

2 Die Problemstellung

Für die Fortführung ist es zunächst wichtig, einige Bezeichnungen einzuführen. Dazu sei $\mathbb{C}[x_1, \ldots, x_n]$ die Menge der Polynome in $x_1, \ldots, x_n$ mit komplexen Koeffizienten. Ein Quotient zweier Polynome $P, Q \in \mathbb{C}[x_1, \ldots, x_n]$ heißt rationale Funktion. Entsprechend bezeichnen wir mit

$$\mathbb{C}(x_1, \ldots, x_n) := \left\{ \frac{P}{Q} \;\middle|\; P, Q \in \mathbb{C}[x_1, \ldots, x_n] \right\}$$

den Körper aller rationalen Funktionen in den n Variablen $x_1, \ldots, x_n$. Analog sei $\mathbb{C}[\sigma_1, \ldots, \sigma_n]$ die Menge der Polynome in $\sigma_1, \ldots, \sigma_n$ bzw. $\mathbb{C}(\sigma_1, \ldots, \sigma_n)$ der Körper der rationalen Funktionen in $\sigma_1, \ldots, \sigma_n$. Wir haben

$$\mathbb{C}[\sigma_1, \ldots, \sigma_n] \subseteq \mathbb{C}[x_1, \ldots, x_n]$$

und

$$\mathbb{C}(\sigma_1, \ldots, \sigma_n) \subseteq \mathbb{C}(x_1, \ldots, x_n).$$

Im Beispiel (1) wurde ein Polynom zweiten Grades mit der p, q-Formel gelöst. Dabei ergab sich die Form

$$x_1 = p + \sqrt{R} \tag{2}$$

mit $p, R \in \mathbb{C}(\sigma_1, \sigma_2)$. Wir stellen uns nun die Frage, ob i.A. die Nullstellen von f durch solche Radikale darstellbar sind. Die Form der Gleichung (2) und die Cardano-Formeln für Polynome dritten und vierten Grades motivieren dabei die folgende Definition.

Definition. Eine Nullstelle $x = x_j$ heißt durch Radikale darstellbar, falls es ein $m \in \mathbb{N}$ und rationale Funktionen $R, p, p_1, \ldots, p_{m-1} \in \mathbb{C}(\sigma_1, \ldots, \sigma_n)$ gibt, so dass

$$x = p + p_1 \sqrt[m]{R} + \ldots + p_{m-1} \left(\sqrt[m]{R} \right)^{m-1}$$

gilt; dabei gilt $\sqrt[m]{R} \notin \mathbb{C}(\sigma_1, \ldots, \sigma_n)$.

Wir können folgende Vereinfachungen erreichen:

- $p_1 = 1$.
- m eine Primzahl.

Ersetzt man nämlich R durch R/p_1^m, so erhält man $p_1 = 1$ und verändert die Voraussetzungen nicht. Auf den Fall $m =$ Primzahl sind wir geführt, indem wir eine Iteration der obigen Darstellung vornehmen.

Annahme. Um herauszufinden, ob die Nullstellen von f als Radikale darstellbar sind, treffen wir die Annahme, dass die Gleichung $f(X) = 0$ eine solche Lösung besitzt. Nach der ersten Vereinfachung ist die angenommene Lösung also von der Form

$$x_1 = p + \sqrt[m]{R} + \ldots + p_{m-1} \left(\sqrt[m]{R} \right)^{m-1}.$$

Im Weiteren wird es unser Ziel sein, einen **Widerspruch** zu dieser Annahme herzuleiten.

3 Der erste Beweisschritt

Wir schränken nun auf den Fall $n = 5$ ein; außerdem erinnern wir uns daran, dass m eine Primzahl ist. Wir nehmen also an, dass unsere Ausgangsgleichung $f(X) = 0$ eine Lösung der Form

$$x_1 = p + \sqrt[m]{R} + \ldots + p_{m-1} \left(\sqrt[m]{R} \right)^{m-1} \tag{3}$$

besitzt.
Bevor wir im ersten Beweisschritt fortfahren, haben wir noch die m-ten Einheitswurzeln ζ^j einzuführen; dabei ist

$$\zeta = e^{2\pi i/m} = \cos\left(\frac{2\pi}{m}\right) + i \cdot \sin\left(\frac{2\pi}{m}\right)$$

und $j = 0, \ldots, m-1$ ist. Wir erinnern daran, dass die m Einheitswurzeln $1, \zeta, \zeta^2, \ldots, \zeta^{m-1}$ im Einheitskreis der komplexen Ebene (mit dem Ursprung als Zentrum) ein regelmäßiges m-Gon einbeschreiben.

Nach langwierigen Überlegungen, welche aber im wesentlichen nur Methoden der Linearen Algebra und die Berechnung des größten gemeinsamen Teilers von Polynomen benötigen, stellen wir fest, dass mit der Lösung (3) gleichzeitig auch

$$\begin{aligned} x_2 &= p + \zeta \sqrt[m]{R} + \ldots + p_{m-1} \left(\zeta \sqrt[m]{R}\right)^{m-1} \\ &\vdots \\ x_m &= p + \zeta^{m-1} \sqrt[m]{R} + \ldots + p_{m-1} \left(\zeta^{m-1} \sqrt[m]{R}\right)^{m-1} \end{aligned}$$

Lösungen der Ausgangsgleichung $f(X) = 0$ sind. Diese stellen sich als paarweise verschieden heraus, d.h. wir haben somit m verschiedene Lösungen der Ausgangsgleichung. Da nun aber $f(X)$ ein Polynom vom Grad $n = 5$ ist, kann es höchstens 5 verschiedene Nullstellen haben, d.h. wir haben $m \leq 5$. Da m aber eine Primzahl ist, haben wir den Beweis auf die Fälle

$$m = 2, m = 3, m = 5$$

reduziert. Diese gilt es im Folgenden zu untersuchen. Dabei beschränken wir uns hier auf die Betrachtung des Falls $m = 5$; der Fall $m = 2$ lässt sich analog behandeln. Schließlich lässt sich zeigen, dass der Fall $m = 3$ gar nicht auftreten kann.

4 Der zweite Beweisschritt

Wir gehen aus von den m Gleichungen

$$\begin{aligned} x_1 &= p + \sqrt[m]{R} + \ldots + p_{m-1} \left(\sqrt[m]{R}\right)^{m-1}, \\ x_2 &= p + \zeta \sqrt[m]{R} + \ldots + p_{m-1} \left(\zeta \sqrt[m]{R}\right)^{m-1}, \\ &\vdots \\ x_m &= p + \zeta^{m-1} \sqrt[m]{R} + \ldots + p_{m-1} \left(\zeta^{m-1} \sqrt[m]{R}\right)^{m-1}. \end{aligned}$$

Indem wir

$$y_1 = p,\ y_2 = \sqrt[m]{R},\ y_3 = p_2 \left(\sqrt[m]{R}\right)^2, \ldots,\ y_m = p_{m-1} \left(\sqrt[m]{R}\right)^{m-1}$$

setzen, erhalten wir das lineare Gleichungssystem

$$\begin{array}{ccccccccccc}
y_1 & + & y_2 & + & y_3 & + & \dots & + & y_m & = & x_1 \\
y_1 & + & \zeta y_2 & + & \zeta^2 y_3 & + & \dots & + & \zeta^{m-1} y_m & = & x_2 \\
\vdots & & & & & & & & & & \\
y_1 & + & \zeta^{m-1} y_2 & + & \zeta^{2(m-1)} y_3 & + & \dots & + & \zeta^{(m-1)^2} y_m & = & x_m.
\end{array}$$

Nach der bekannten Theorie der linearen Gleichungssysteme sind die Lösungen $y_1, y_2, \dots, y_m$ gegeben als Quotienten von Polynomen in den Koeffizienten des Gleichungssystems, d.h. $y_1, y_2, \dots, y_m$ sind rationale Funktionen in $x_1, x_2, \dots, x_n$. Insbesondere stellen wir fest

$$\sqrt[m]{R} \in \mathbb{C}(x_1, \dots, x_n).$$

Zum Beispiel berechnet man im Fall $m = 3$ leicht

$$\sqrt[3]{R} = \frac{x_1 + \zeta^2 \cdot x_2 + \zeta \cdot x_3}{3}.$$

5 Der dritte Beweisschritt

Die symmetrische Gruppe S_n vom Index n ist definiert als die Menge aller Permutationen von n Elementen. Eine Permutation π ist dabei einfach eine Anordnung der n Elemente, wobei jedes Element in der neuen Anordnung genau einmal vorkommen soll und je zwei verschiedenen Elementen auch zwei verschiedene Bildelemente zugeordnet werden. Wir können sie also auch als injektive Abbildung der Menge der n Elemente auf sich selbst auffassen. Eine Permutation ist also insbesondere bijektiv. Wir arbeiten im Folgenden mit den natürlichen Zahlen von 1 bis n als Elementen. Diese Permutationen finden ihre Anwendung nun bei Polynomen und rationalen Funktionen in den n Variablen $x_1, \dots, x_n$. Wir lassen dabei eine Permutation auf die Indizes wirken. Sei also $\pi \in S_n$ eine Permutation. Dann definieren wir

$$g^\pi(x_1, \dots, x_n) := g(x_{\pi(1)}, \dots, x_{\pi(n)}),$$

wobei $g \in \mathbb{C}(x_1, \dots, x_n)$ ist. Nun definieren wir weiter die "Wertemenge" von g durch

$$W(g) := \{g^\pi \mid \pi \in S_n\}.$$

Eine rationale Funktion g mit $W(g) = \{g\}$, also $|W(g)| = 1$, nennen wir eine symmetrische rationale Funktion. Man überzeugt sich leicht davon, dass man Permutieren und Addieren bzw. Multiplizieren vertauschen kann, da diese beiden Prozesse völlig unabhängig voneinander sind. Induktiv erhält man dann, dass dies sogar für mehrere Summanden und Faktoren einer Summe bzw. eines Produkts gilt. Als Spezialfall, bei dem die Faktoren alle gleich sind, erhalten wir somit folgendes Vertauschungsgesetz für Potenzen:

$$(g^\pi)^r = (g^r)^\pi \quad (r \in \mathbb{N}).$$

Daraus folgt insbesondere für $r = m = 5$

$$(g^\pi)^5 = \left(g^5\right)^\pi = \left(\left(\sqrt[5]{R}\right)^5\right)^\pi = R^\pi = R.$$

Letzteres Gleichheitszeichen gilt wegen der Voraussetzung $R \in \mathbb{C}(\sigma_1, \ldots, \sigma_n)$. Somit ist wie $\sqrt[5]{R}$ auch $\left(\sqrt[5]{R}\right)^\pi$ eine Lösung der Gleichung

$$z^5 - R = 0.$$

Diese Lösungen sind aber als fünfte Wurzeln alle von der Form

$$z_j = \zeta^j \cdot \sqrt[5]{R} \quad (j \in \{0, \ldots, 4\}).$$

Daraus folgt also

$$\left(\sqrt[5]{R}\right)^\pi = \zeta^j \cdot \sqrt[5]{R}$$

mit einem $j \in \{0, \ldots, 4\}$. Mithilfe von etwas Gruppentheorie (Operationen, Bahnen und Stabilisatoren) kann man zeigen, dass auch wirklich jedes der z_j $(j = 0, \ldots, 4)$ als Bild angenommen wird, d.h. dass es zu jedem dieser z_j auch wirklich eine Permutation $\pi \in S_n$ gibt mit

$$\left(\sqrt[5]{R}\right)^\pi = \zeta^j \cdot \sqrt[5]{R}.$$

Somit folgern wir aus den obigen Überlegungen und dem letzten Argument, dass

$$W\left(\sqrt[5]{R}\right) = \left\{\sqrt[5]{R}, \zeta \cdot \sqrt[5]{R}, \ldots, \zeta^4 \cdot \sqrt[5]{R}\right\}$$

gilt und erhalten dann $\left|W\left(\sqrt[5]{R}\right)\right| = 5$.

6 Der Widerspruch

Wir erinnern zunächst nochmals daran, dass wir mit der allgemeinen Gleichung fünften Grades arbeiten, d.h. wir nehmen an, dass die Nullstellen $x_1, \ldots, x_5$ unabhängige Variablen sind, also keiner algebraischen Gleichung (mit komplexen Koeffizienten) genügen.

Ohne Beweis zitieren wir den folgenden Satz.

Satz. Ist $g \in \mathbb{C}(x_1, \ldots, x_5)$ eine rationale Funktion mit der Eigenschaft $|W(g)| = 5$, so ist g (ohne Beschränkung der Allgemeinheit) von der Form

$$g = g(x_1, \ldots, x_5) = q_0 + q_1 \cdot x_1 + q_2 \cdot x_1^2 + q_3 \cdot x_1^3 + q_4 \cdot x_1^4$$

mit symmetrischen Funktionen $q_0, q_1, \ldots, q_4 \in \mathbb{C}(\sigma_1, \ldots, \sigma_5)$.

Nach dem zweiten Beweisschritt ist $\sqrt[5]{R} \in \mathbb{C}(x_1, \ldots, x_5)$. Da nach dem dritten Beweisschritt weiter $|W(\sqrt[5]{R})| = 5$ gilt, können wir den vorhergehenden Satz anwenden. Wir finden, dass $\sqrt[5]{R}$ die Gestalt

$$\sqrt[5]{R} = q_0 + q_1 \cdot x_1 + q_2 \cdot x_1^2 + q_3 \cdot x_1^3 + q_4 \cdot x_1^4$$

hat, wobei $q_0, q_1, \ldots, q_4 \in \mathbb{C}(\sigma_1, \ldots, \sigma_5)$ sind.
Wir wenden nun die Permutation

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 5 & 1 \end{pmatrix}$$

auf die rationale Funktion $\sqrt[5]{R}$ an und erhalten

$$\begin{aligned} \left(\sqrt[5]{R}\right)^\pi &= \left(q_0 + q_1 \cdot x_1 + q_2 \cdot x_1^2 + q_3 \cdot x_1^3 + q_4 \cdot x_1^4\right)^\pi \\ &= q_0^\pi + q_1^\pi \cdot x_2 + q_2^\pi \cdot x_2^2 + q_3^\pi \cdot x_2^3 + q_4^\pi \cdot x_2^4 \\ &= q_0 + q_1 \cdot x_2 + q_2 \cdot x_2^2 + q_3 \cdot x_2^3 + q_4 \cdot x_2^4 ; \end{aligned}$$

dabei haben wir insbesondere beachtet, dass $x_1^\pi = x_2$ ist und dass die Funktionen $q_0, q_1, \ldots, q_4$ symmetrisch sind.

Nach dem dritten Beweisschritt wissen wir andererseits, dass ein $j \in \{0, \ldots, 4\}$ existiert, so dass

$$\left(\sqrt[5]{R}\right)^{\pi} = \zeta^j \cdot \sqrt[5]{R}$$

gilt. Zusammen mit der vorhergehenden Rechnung erhalten wir somit die Relation

$$\begin{aligned} &q_0 + q_1 \cdot x_2 + q_2 \cdot x_2^2 + q_3 \cdot x_2^3 + q_4 \cdot x_2^4 = \\ &\zeta^j \cdot q_0 + \zeta^j \cdot q_1 \cdot x_1 + \zeta^j \cdot q_2 \cdot x_1^2 + \zeta^j \cdot q_3 \cdot x_1^3 + \zeta^j \cdot q_4 \cdot x_1^4 \,. \end{aligned}$$

Zusammengenommen genügen $x_1, \ldots, x_5$ somit der polynomialen Gleichung

$$\begin{aligned} &q_0 \,(1 - \zeta^j) + q_1 \,(x_2 - \zeta^j \cdot x_1) + q_2 \,(x_2^2 - \zeta^j \cdot x_1^2) + \\ &q_3 \,(x_2^3 - \zeta^j \cdot x_1^3) + q_4 \,(x_2^4 - \zeta^j \cdot x_1^4) = 0 \,. \end{aligned}$$

Dies stellt aber einen **Widerspruch** zur angenommenen algebraischen Unabhängigkeit der Variablen $x_1, \ldots, x_5$ dar.

Damit ist – zumindest im Fall $m = 5$ – gezeigt, dass die allgemeine Gleichung fünften Grades sich nicht mithilfe von Radikalen lösen lässt.