Bemerkungen zur Auflösung von Polynomgleichungen durch Radikale

Klaus Pommerening

Oktober 1979 – Überarbeitung April 2020

1 Fragestellung – motivierendes Vorspiel zur Galois-Theorie

1.1 Einleitung

Historisch gesehen – von etwa 1500 bis 1900 – ist das Wort „Algebra“ ein Synonym für „Auflösung von Gleichungen höheren Grades“.

Die „Gleichung“

$$f(x) = 0$$

bedeutet:

Gegeben ist ein Polynom $f \in K[X]$, also mit Koeffizienten in einem Körper K (oder einem Ring) in einer „Unbestimmten“ X:

$$f = a_n X^n + \cdots + a_0 \quad \text{mit } a_n, \ldots, a_0 \in K.$$

Der Körper K darf ein abstrakter Körper sein, wir können uns aber auch gerne einen der Körper $K = \mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ der rationalen, reellen oder komplexen Zahlen vorstellen und X einfach als „Platzhalter“.

Gesucht sind eine oder alle „Nullstellen“ oder „Wurzeln“ x von f, also Elemente $x \in K$ (zunächst) mit $f(x) = 0$, d. h.

$$a_n x^n + \cdots + a_0 = 0.$$

Beispiele

1. Gleichung ersten Grades (oder „lineare Gleichung“), hier ist $f = aX + b$ mit a, $b \in K$, $a \neq 0$. Klar ist:

   $$f(x) = 0 \Longleftrightarrow x = -\frac{b}{a}\,.$$

   Unser Polynom f hat also in K genau eine Nullstelle x, nämlich $x = -b/a$, und diese lässt sich „rational“ durch die Koeffizienten ausdrücken, d. h. mit Hilfe der rationalen Operationen $+$, $-$, $\times$ und $/$.

2. Gleichung zweiten Grades (oder „quadratische Gleichung“), hier ist

$$f = aX^2 + bX + c \quad \text{mit } a,\, b,\, c \in K,\, a \neq 0.$$

Die einfache Beobachtung, dass x genau dann Nullstelle von f ist, wenn es Nullstelle des Polynoms

$$\frac{f}{a} = X^2 + \frac{b}{a}\,X + \frac{c}{a}$$

ist, erlaubt uns, das Problem der Auflösung von Gleichungen zweiten Grades auf die etwas einfacher gebauten Polynome der Form $f = X^2 + pX + q$ zu reduzieren, uns also auf normierte Polynome zu beschränken. Dann gilt:

$$\begin{aligned}
f(x) = 0 &\iff x^2 + px + q = 0 \\
&\iff \left(x + \frac{p}{2}\right)^2 = \frac{p^2}{4} - q \quad (\text{„quadratische Ergänzung“}) \\
&\iff x + \frac{p}{2} = \pm\sqrt{\frac{p^2}{4} - q} \\
&\iff x = -\frac{p}{2} \pm \sqrt{\frac{p^2}{4} - q}
\end{aligned}$$

Also lässt sich jede Lösung x rational durch die Koeffizienten ausdrücken **mit Hilfe einer Quadratwurzel**

$$\sqrt{\Delta} \quad \text{mit } \Delta = p^2 - 4q.$$

(D. h., der Radikand wurde von seinem Nenner 4 befreit.) Wir haben gezeigt, dass jede Nullstelle x von f die Form

$$x = \frac{-p \pm \sqrt{\Delta}}{2}$$

hat[1]. Das können null, eine oder zwei Lösungen sein, je nachdem ob Δ in K gar keine, eine oder zwei verschiedene Quadratwurzeln hat. Wenn wir uns hier vorstellen, dass $K \subseteq \mathbb{C}$ aus komplexen Zahlen besteht, so gibt es genau eine Lösung, wenn $\Delta = 0$, und genau zwei Lösungen in $\mathbb{C}$, wenn $\Delta \neq 0$ – diese beiden müssen aber nicht im Körper K liegen, z. B. wenn $K = \mathbb{Q}$ und $\Delta = 2$. (Außerdem gilt die Lösungsformel nur, wenn $2 \neq 0$ in K, d. h., wenn K nicht die Charakteristik 2 hat.)

Die Größe $\Delta = p^2 - 4q \in K$ heißt übrigens **Diskriminante** des quadratischen Polynoms $f = X^2 + pX + q \in K[X]$. Wenn wir die beiden verschiedenen Nullstellen von f mit x_1 und x_2 bzeichnen, gilt

$$\begin{aligned}
x_1 - x_2 &= \frac{-p + \sqrt{\Delta}}{2} - \frac{-p - \sqrt{\Delta}}{2} = \sqrt{\Delta}, \\
\Delta &= (x_1 - x_2)^2.
\end{aligned}$$

[1] Eine dieser Lösungsformel vergleichbare Methode zur Auflösung quadratischer Gleichungen war schon im alten Babylon bekannt.

An dieser Formel sieht man sogar direkt, dass die Diskriminante gebau dann Null ist, wenn die beiden Nullstellen zu einer zweifachen Nullstelle zusammenfallen. Im reellen Fall, also $K \subseteq \mathbb{R}$, kann man an der Diskriminante sogar ablesen, ob es keine, genau eine oder zwei verschiedene *reelle* Nullstellen gibt:

$$\begin{array}{ll} \Delta < 0: & \text{keine reelle Nullstelle} \\ \Delta = 0: & \text{genau eine reelle Nullstelle} \\ \Delta > 0: & \text{zwei reelle Nullstellen} \end{array}$$

1.2 Rationale Ausdrücke

Die allgemeine Definition, was ein „rationaler Ausdruck“ ist, wird durch den Körperbegriff abstrakt gefasst.

Stellen wir uns zunächst eine Menge $S \subseteq \mathbb{C}$ von komplexen Zahlen vor. Die Menge aller „rationalen Ausdrücke in S“ baut man dann sukzessive so auf:

- „Monome“ in S als endliche Produkte:

$$M = \prod_{j=1}^{m} s_j^{\nu_j} \quad \text{mit } m \in \mathbb{N},\ s_j \in S,\ \nu_j \in \mathbb{N} = \{0, 1, 2, \ldots\}$$

  (einschließlich der 1 als leeres Produkt)

- „Polynome“ in S als endliche Linearkombinationen von Monomen:

$$f = \sum_{i=1}^{n} a_i M_i \quad \text{mit } n \in \mathbb{N},\ a_i \in \mathbb{Q},\ M_i \text{ Monome}$$

  (einschließlich der 0 als leere Summe und der ganzen Zahlen als Summen von Einsen)

- Quotienten f/g von „Polynomen“ mit $g \neq 0$ (einschließlich der rationalen Zahlen)

Die Menge $\mathbb{Q}(S)$ der rationalen Ausdrücke (sprich: „$\mathbb{Q}$ adjungiert S“) besteht aus allen solchen Quotienten, also aus allem, was sich in endlich vielen Schritten mithilfe der „Grundrechenarten“ $+$, $-$, $\times$ und $/$ aus den Elementen von S herstellen lässt.

Behauptung: Die Teilmenge $\mathbb{Q}(S) \subseteq \mathbb{C}$ ist ein Körper.

Zum Beweis schauen wir auf die Ausdrücke der Gestalten

$$\frac{f_1}{g_1} \pm \frac{f_2}{g_2} = \frac{g_2 f_1 \pm g_1 f_2}{g_1 g_2}, \quad \frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}, \quad \frac{1}{f/g} = \frac{g}{f} \quad (\text{falls } f \neq 0)$$

und sehen, dass dies wieder rationale Ausdrücke in S sind; der einzig nötige Zwischenschritt ist: Das Produkt zweier Monome ist wieder ein Monom.

Verallgemeinerung: Sind $K \subseteq L$ zwei beliebige Körper und $S \subseteq L$ eine Teilmenge, so bildet man genauso $K(S)$.

Bemerkung: Wir verlangen von einem Körper stets $1 \neq 0$. Ein Teilkörper soll immer 0 und 1 enthalten. D. h., die einelementige Menge $\{0\}$ wird nicht als Körper zugelassen.

Damit kommen wir zu unserer ersten abstrakten Ausschweifung:

Hilfssatz 1 *Sei L ein Körper.*

(i) *Sei $\mathfrak{M}$ eine Menge von Teilkörpern $M \subseteq L$. Dann ist auch*

$$K = \bigcap_{M \in \mathfrak{M}} M$$

ein Teilkörper von L.

(ii) *Sei $K \subseteq L$ ein Teilkörper und $S \subseteq L$. Sei*

$$\mathfrak{M} = \{M \mid K \subseteq M \subseteq L \text{ Zwischenkörper mit } S \subseteq M\}.$$

Dann ist

$$K(S) = \bigcap_{M \in \mathfrak{M}} M.$$

Insbesondere ist $K(S)$ der kleinste Teilkörper von L, der K und S enthält.

(iii) *Es gibt einen kleinsten Teilkörper von L.*

Beweis. (i) Klar ist $0, 1 \in K$. Ebenso, dass für $a, b \in K = \bigcap M$ mit $b \neq 0$ auch $a + b$, $a - b$, $a \cdot b$, $1/b \in K$.

(ii) Da $K(S)$ ein Körper ist, ist $K(S) \in \mathfrak{M}$, also $K(S) \supseteq \bigcap M$. Da umgekehrt für jeden Teilkörper $M \in \mathfrak{M}$ sowohl $K \subseteq M$ als auch $S \subseteq M$, folgt $K(S) \subseteq M$, also $K(S) \subseteq \bigcap M$.

(iii) Zwar kann man (i) nicht direkt anwenden, aber ähnlich schließen: Setzt man $\mathfrak{M}$ gleich der Menge aller Teilkörper von L, insbesondere $L \in \mathfrak{M}$, so ist der Durchschnitt $\bigcap M$ über die nichtleere Menge der $M \in \mathfrak{M}$ in jedem Teilkörper enthalten, also der kleinste unter ihnen. $\diamond$

Bemerkungen

1. Der kleinste Teilkörper heißt **Primkörper**. Der Primkörper von $\mathbb{R}$ und $\mathbb{C}$ ist $\mathbb{Q}$. Allgemeiner ist der Primkörper eines jeden Körpers der Charakteristik 0 (isomorph zu) $\mathbb{Q}$, der eines Körpers der Primzahlcharakteristik p (isomorph zu) $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

2. Für einen Körper K bezeichnen wir (wie schon in der Einleitung, Abschnitt 1.1) mit $K[X]$ die Menge aller Polynome in der Größe X. Sei $f \in K[X]$,

$$f = a_n X^n + \cdots + a_0.$$

Sei $\mathbb{F}$ der Primkörper von K. Dann ist[2] $K_0 = \mathbb{F}(a_0, \ldots, a_n)$ der kleinste Körper, der alle Koeffizienten von f enthält, sozusagen der „natürliche Definitionsbereich“ des Polynoms f. Er besteht genau aus den rationalen Ausdrücken in den Koeffizienten von f.

1.3 Gleichungen ersten und zweiten Grades

Die Überlegungen aus Abschnitt 1.1 lassen sich jetzt in die folgende Form bringen:

Satz 1 *Sei K ein Körper und $L \supseteq K$ ein Erweiterungskörper[3].*

(i) *Sei $f = aX + b \in K[X]$, $a \neq 0$, ein Polynom vom Grad 1. Dann hat f in L genau die eine Nullstelle $x = -b/a$. Diese liegt in K.*

(ii) *Sei $f = X^2 + pX + q \in K[X]$ ein normiertes Polynom vom Grad 2, und es sei $\operatorname{char} K \neq 2$ (d. h. $2 := 1 + 1 \neq 0$ in K). Dann sind folgende Aussagen äquivalent:*

1. *f hat eine Nullstelle in L.*
2. *Es gibt ein $\delta \in L$ mit $\delta^2 = p^2 - 4q$.*

Ist das erfüllt, so gibt es höchstens zwei Nullstellen; diese haben die Form $x_{1,2} = (-p \pm \delta)/2$ und liegen im Körper $K(\delta) \subseteq L$.

Aufgaben

1. Seien $L \supseteq K$, $\delta \in L - K$ mit $\delta^2 = d \in K$.
   (a) Dann hat jedes Element von $K(\delta)$ die Form $a + b\delta$ mit $a, b \in K$; insbesondere ist $K(\delta)$ ein zweidimensionaler K-Vektorraum.
   (b) Die Abbildung $\sigma : a + b\delta \mapsto a - b\delta$ ist ein K-Automorphismus von $K(\delta)$ (d. h. ein Vektorraum- und Körperautomorphismus); und jeder K-Automorphismus ist entweder die identische Abbildung $\mathbf{1}$ oder σ.
   (c) Ist $f \in K[X]$ und $x \in K(\delta)$ eine Nullstelle von f, so auch σx. Was bedeutet das im Spezialfall $K = \mathbb{R}$, $L = \mathbb{C}$, $d = -1$?
   (d) Ist $K \subseteq \mathbb{R}$ und $d > 0$, so ist σ nicht stetig. Anleitung: Ein stetiger Automorphismus eines Teilkörpers $L \subseteq \mathbb{R}$ ist notwendig die identische Abbildung.
2. Warum ist $\mathbb{Q}(\sqrt{2}) \neq \mathbb{Q}(\sqrt{3})$?

[2] Bei expliziter Aufzählung der Elemente von S wird üblicherweise die Mengenklammer weggelassen.
[3] Wir vermeiden die Begriffe „Oberkörper“ und „Unterkörper“.

1.4 Gleichungen dritten Grades

Wie beim Grad 2 können wir uns bei Gleichungen vom Grad 3 („kubischen Gleichungen“) auf normierte Polynome beschränken, also auf Polynome der Gestalt

$$f = X^3 + aX^2 + bX + c \in K[X].$$

Das Analogon zur quadratischen Ergänzung führt zwar nicht zur Lösung, aber immerhin zu einer weiteren Vereinfachung:

$$\begin{aligned} f &= \left(X + \frac{a}{3}\right)^3 - \frac{1}{3}\,a^2 X - \frac{a^3}{27} + bX + c \\ &= \left(X + \frac{a}{3}\right)^3 + \underbrace{\left(b - \frac{a^2}{3}\right)}_{p} \cdot \left(X + \frac{a}{3}\right) + \underbrace{\left(c + \frac{2a^3}{27} - \frac{ab}{3}\right)}_{q}. \end{aligned}$$

Für $y = x + a/3$ gilt[4]

$$f(x) = 0 \Longleftrightarrow y^3 + py + q = 0.$$

Wir brauchen also „nur“ die Nullstellen des Polynoms $X^3 + pX + q$ zu bestimmen, d. h., wir nehmen o. B. d. A. an, dass $f = X^3 + pX + q$.

Eine weitere Transformation („italienischer Trick“) wird zu einer expliziten Lösungsformel führen, erfunden von DEL FERRO[5] 1515 und unabhängig von TARTAGLIA[6] 1534, zuerst publiziert von CARDANO[7] 1545.

Wir setzen voraus, dass $p \neq 0$ – ansonsten müssen wir für die Lösung ja nur eine dritte Wurzel ziehen und haben somit eine explizite Lösungsformel. Mit dem Ansatz $x = u + v$ gewinnen wir einen Freiheitsgrad, über den wir später verfügen können. Damit gilt:

$$\begin{aligned} f(x) = 0 &\iff u^3 + 3u^2 v + 3uv^2 + v^3 + p\,(u + v) + q = 0 \\ &\iff u^3 + v^3 + q + (3uv + p)(u + v) = 0 \\ &\Longleftarrow uv = -\frac{p}{3} \quad \text{(insbesondere } u \neq 0), \quad u^3 + v^3 + q = 0 \\ &\iff uv = -\frac{p}{3}\,, \quad u^3 - \frac{p^3}{27u^3} + q = 0 \\ &\iff uv = -\frac{p}{3}\,, \quad (u^3)^2 + q\,u^3 - \frac{p^3}{27} = 0 \end{aligned}$$

(Bei dem Schritt, der nur eine Implikation, aber keine Äquivalenz ist, haben wir den zusätzlichen Freiheitsgrad geopfert.) Damit haben wir das Problem auf eine quadratische Gleichung für u^3 reduziert. Sie wird gelöst von

$$u^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\,.$$

[4] Das ist der lineare Spezialfall der Tschirnhaus-Transformation, benannt nach Ehrenfried Walther von Tschirnhaus, 1651–1708, der glaubte, eine allgemeine Methode zur Lösung von Gleichungen höheren Grades gefunden zu haben.

[5] Scipione del Ferro, 1465–1526

[6] Nicolo Tartaglia, 1499–1557

[7] Gerolamo Cardano, 1501–1576, *Ars magna sive de Regulis Algebraicis*

Aus der Bedingung $u^3 + v^3 + q = 0$ leiten wir her

$$v^3 = -q - u^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}\,.$$

(Hätten wir bei der Formel für u^3 die negative Quadratwurzel gewählt, würde das also auf eine Vertauschung von u und v hinauslaufen.) Damit erhalten wir eine Formel (genannt CARDANO-Formel), die garantiert Lösungen liefert:

$$u = \sqrt[3]{-\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad v = \sqrt[3]{-\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}, \quad x = u + v \tag{1}$$

mit der Nebenbedingung $uv = -p/3$. Für die dritten Wurzeln haben wir jeweils drei Möglichkeiten, die Nebenbedingung reduziert die möglichen neun Kombinationen aber auf drei. Das ist allerdings unerheblich, es reicht überhaupt ein Lösungspaar (u, v) gefunden zu haben – ist nämlich $\rho \in K$ eine dritte Einheitswurzel $\neq 1$, so sind $(\rho u, \rho^2 v)$ und $(\rho^2 u, \rho v)$ zwei weitere Lösungspaare.

Bemerkungen

1. Man kann den Summanden v in der Herleitung auch unterdrücken, indem man gleich $x = u - p/3u$ substituiert. Das macht die Herleitung allerdings weder einfacher noch verständlicher.

2. Die Formel (1) liefert auch Lösungen, wenn $p = 0$ oder $q = 0$.

   (a) $p = 0$ führt auf $u = 0$, $v = x$, $v^3 = -q$, also auf die offensichtliche Lösung $x = \sqrt[3]{-q}$.

   (b) $q = 0$ führt auf $v^3 = -u^3$, also z. B. $v = -u$, $x = 0$. Da $u^3 = \sqrt{-p^3/27}$, können wir $u = \sqrt{-p/9}$ und $v = -\sqrt{-p/9}$ nehmen und die beiden anderen Lösungen für x aus dieser Quadratwurzel mithilfe der Einheitswurzel ρ kombinieren.

3. Wenn $p \neq 0$ ist auch $u \neq 0$, und wir können den zweiten Teil der Lösungsformel (1) durch

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

   ersetzen. Das sieht zwar nicht gut aus, erspart aber das Ziehen einer weiteren dritten Wurzel.

4. Die Herleitung war dank unserem souveränen Umgang mit Quadratwurzeln aus negativen Zahlen nicht sonderlich kompliziert. Die Mathematiker taten sich allerdings noch bis ins 19. Jahrhundert damit schwer und mussten als Folge davon eine unerfreuliche Menge von Fallunterscheidungen treffen, um negative Radikanden zu vermeiden. Das gelang nicht vollständig. Mehr dazu später.

5. Für das kubische Polynom $f = X^3 + pX + q \in K[X]$ nennen wir den Ausdruck unter der Quadratwurzel, mit dem Faktor $27 \cdot 4$ von den Nennern befreit,

$$\Delta = 4p^3 + 27q^2 \in K,$$

die **Diskriminante**. Mit ihr kann man die Lösungsformel so ausdrücken:

$$x = \underbrace{\sqrt[3]{-\frac{q}{2} + \frac{\sqrt{\Delta}}{6\sqrt{3}}}}_{u} \underbrace{-\sqrt[3]{-\frac{q}{2} - \frac{\sqrt{\Delta}}{6\sqrt{3}}}}_{v}$$

Aus den drei Nullstellen

$$x_1 = u + v, \quad x_2 = \rho u + \rho^2 v, \quad x_3 = \rho^2 u + \rho v$$

erhalten wir

$$\begin{aligned} x_1 - x_2 &= (1-\rho)\, u + (1-\rho^2)\, v = (1-\rho)[u + (1+\rho)\, v] \\ x_1 - x_3 &= (1-\rho^2)\, u + (1-\rho)\, v = (1-\rho)[(1+\rho)\, u + v] \\ x_2 - x_3 &= (\rho-\rho^2)\, u + (\rho^2-\rho)\, v = \rho\,(1-\rho)[u - v] \end{aligned}$$

Wir bilden das Produkt und nützen aus, dass $1 + \rho + \rho^2 = 0$, also $(1+\rho)^2 = \rho$:

$$\begin{aligned} (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) &= \rho\,(1-\rho)^3 \cdot [(1+\rho)u^2 + uv + (1+\rho)^2 uv + (1+\rho)v^2][u - v] \\ &= \rho\,(1-\rho)^3 \cdot [(1+\rho)u^2 + (1+\rho)uv + (1+\rho)v^2][u - v] \\ &= -\rho^3\,(1-\rho)^3 \cdot [u^2 + uv + v^2][u - v] \\ &= (\rho-1)^3 \cdot (u^3 - v^3) \\ &= (\rho-1)^3 \cdot 2 \cdot \frac{\sqrt{\Delta}}{6\sqrt{3}} = 3\rho(1-\rho) \cdot \frac{\sqrt{\Delta}}{\sqrt{27}} \end{aligned}$$

da $(\rho-1)^3 = \rho^3 - 3\rho^2 + 3\rho - 1 = 3\rho(1-\rho)$. Wenn wir diesen Ausdruck quadrieren, beachten wir $(1-\rho)^2 = 1 - 2\rho + \rho^2 = -3\rho$ und erhalten

$$[(x_1 - x_2)(x_1 - x_3)(x_2 - x_3)]^2 = -27\rho^3 \cdot \frac{\Delta}{27} = -\Delta,$$

also wieder eine Formel, die die Diskriminante[8] durch die Nullstellen ausdrückt.

1.5 Mathematische Formulierung

Die Herleitung im vorigen Abschnitt wirkte nicht an allen Stellen zwingend. Es kam aber nur darauf an, überhaupt eine Lösung zu finden. Der Gedankengang aus Abschnitt 1.4 lässt sich mathematisch präzise so zusammenfassen:

[8] *Achtung*: Die allgemeingültige Definition der Diskriminante entspricht eigentlich unserem $-\Delta$.

Satz 2 *Sei K ein Körper der Charakteristik $\neq 2, 3$. Sei $f = X^3 + pX + q \in K[X]$ ein Polynom vom Grad 3 mit $p \neq 0$ und $L \supseteq K$ ein Erweiterungskörper.*

(i) *Es gebe ein $\delta \in L$ mit $\delta^2 = \frac{q^2}{4} + \frac{p^3}{27}$ und ein $u \in L$ mit $u^3 = -\frac{q}{2} + \delta$. Dann ist $u \neq 0$, und $x_1 = u + v$ mit $v = -\frac{p}{3u}$ eine Nullstelle von f.*

(ii) *Außerdem gebe es ein $\rho \in L$, $\rho \neq 1$, mit $\rho^3 = 1$. Dann sind auch $x_2 = \rho u + \rho^2 v$ und $x_3 = \rho^2 u + \rho v$ Nullstellen von f*

Insbesondere ist $x_1 \in K(\delta, u)$ und $x_2, x_3 \in K(\delta, u, \rho)$.

Wenn wir das bekannte Ergebnis akzeptieren, dass ein Polynom dritten Grades genau drei Nullstellen bei korrekter Zählung von Vielfachheiten hat, erkennen wir auch, dass wir damit sämtliche Lösungen der Gleichung dritten Grades gefunden haben. Um sie auszudrücken, müssen wir eventuell eine Quadratwurzel und eine Kubikwurzel sowie eine nichttriviale dritte Einheitswurzel an den ursprünglichen Körper K adjungieren.

Beispiel

Sei $K = \mathbb{Q}$, $L = \mathbb{C}$, $f = X^3 - 15X - 4 \in \mathbb{Q}[X]$, also $p = -15$, $q = -4$. Dann ist $\delta^2 = 4 - 125 = -121$, also können wir mit $\delta = 11i \in \mathbb{C}$ weiterarbeiten. Daraus erhalten wir:

$$u^3 = 2 + 11i, \quad v^3 = -q - u^3 = 2 - 11i,$$

und somit die verblüffende Formel

$$x_1 = u + v = \sqrt[3]{2 + 11i} + \sqrt[3]{2 - 11i}\,,$$

verblüffend, weil die Nullstelle $x = 4$ direkt ins Auge springt! Aber schon Bombelli[9] hat gemerkt, dass $u = 2 + i$, $v = 2 - i$. Denn

$$(2 \pm i)^3 = 8 \pm 12i - 6 \mp i = 2 \pm 11i.$$

Also $x_1 = 4$.

Wir stellen fest, dass *die* Cardano-*Formel schon in einfachen Beispielen die optimale Form der Lösung verschleiert.*

Um auch die beiden anderen Lösungen explizit anzugeben, verwenden wir

$$\rho = \frac{-1 + i\sqrt{3}}{2}, \quad \rho^2 = \frac{1 - 3 - 2i\sqrt{3}}{4} = \frac{-1 - i\sqrt{3}}{2}, \quad \rho^3 = \rho \cdot \rho^2 = \frac{1 + 3}{4} = 1\,,$$

$$\begin{aligned}
\rho u &= \frac{-1 + i\sqrt{3}}{2} \cdot (2 + i) = \frac{-2 - i + 2i\sqrt{3} - \sqrt{3}}{2} \\
\rho^2 v &= \frac{-1 - i\sqrt{3}}{2} \cdot (2 - i) = \frac{-2 + i - 2i\sqrt{3} - \sqrt{3}}{2} \\
\rho^2 u &= \frac{-1 - i\sqrt{3}}{2} \cdot (2 + i) = \frac{-2 - i - 2i\sqrt{3} + \sqrt{3}}{2} \\
\rho v &= \frac{-1 + i\sqrt{3}}{2} \cdot (2 - i) = \frac{-2 + i + 2i\sqrt{3} + \sqrt{3}}{2}
\end{aligned}$$

[9] Rafael Bombelli, 1527–1572, ging recht souverän mit imaginären Zahlen um.

Damit erhalten wir

$$\begin{aligned} x_2 &= \rho u + \rho^2 v = \frac{-4 - 2\sqrt{3}}{2} = -2 - \sqrt{3}, \\ x_3 &= \rho^2 u + \rho v = \frac{-4 + 2\sqrt{3}}{2} = -2 + \sqrt{3}, \end{aligned}$$

und stellen, wiederum verblüfft, fest, dass am Ende *drei reelle Lösungen herauskommen, obwohl wir heftig mit komplexen Zahlen rechnen mussten.*

Aufgaben

1. Bestimme mittels der CARDANO-Formel die einzige reelle Lösung x der Gleichung $x^3 - x^2 + x - 1$. (Sie ist leicht zu erraten, aber hier soll die Formel ausgewertet werden.)

2. Das gleiche für $x^3 + 3x - 4 = 0$.

3. Vereinfache die Ausdrücke

$$\sqrt[3]{2 + \sqrt{5}} + \sqrt[3]{2 - \sqrt{5}} \quad \text{und} \quad \sqrt{2} - \sqrt{3} + \sqrt{5 - \sqrt{24}}.$$

   Zum Vergleich: Was liefert ein Taschenrechner (oder eine Calc-App)?

4. Die Gleichung von DE MOIVRE ist

$$x^5 + p\,x^3 + \frac{1}{5}\,p^2 x + r = 0.$$

   Sie wird (für $\operatorname{char} K \neq 2, 5$) analog zum „italienischen Ansatz“ durch die Substitution $x = y - p/5y$ gelöst. Leite eine Lösungsformel her.

1.6 Historische Anmerkungen

Gleichungslösen in der Renaissance

Bei den Mathematikern der Renaissance, hauptsächlich Italienern, im 16. Jahrhundert waren noch nicht einmal die negativen, geschweige denn die komplexen Zahlen etabliert! Das führte zu exzessiven Fallunterscheidungen in den Lösungsformeln. Außerdem mussten sie alles durch Worte oder Zahlenbeispiele ausdrücken – die heutige „symbolische“ Schreibweise der Gleichungen mit Buchstaben für gegebene und unbekannte Größen und Potenzen geht auf VIETA[10] zurück (1579).

Die Auflösung der Gleichung vierten Grades durch ähnliche (aber natürlich nochmal kompliziertere) Formeln wurde 1545 von FERRARI[11] entdeckt und ebenfalls in der *Ars magna* von CARDANO veröffentlicht.

[10] François Viète (= Vieta), 1540–1603
[11] Lodovico Ferrari, 1522–1565

Werke

- del Ferro und Tartaglia gaben ihre Ergebnisse nur mündlich weiter.
- Cardano: *Ars magna sive de Regulis Algebraicis*, Nürnberg 1545.
- Vieta: *Canon mathematicus seu ad triangula*, 1579.

Warum wurden die komplexen Zahlen erfunden?

Sie wurden *nicht* erfunden, um quadratische Gleichungen zu lösen – obwohl diese irreführende Ansicht weit verbreitet ist. Die Mathematiker hätten gut mit der Regel leben können, dass eine (reelle) quadratische Gleichung keine, eine oder zwei Lösungen hat – das stimmt nämlich perfekt mit der Anschauung überein, siehe Abbildung 1.

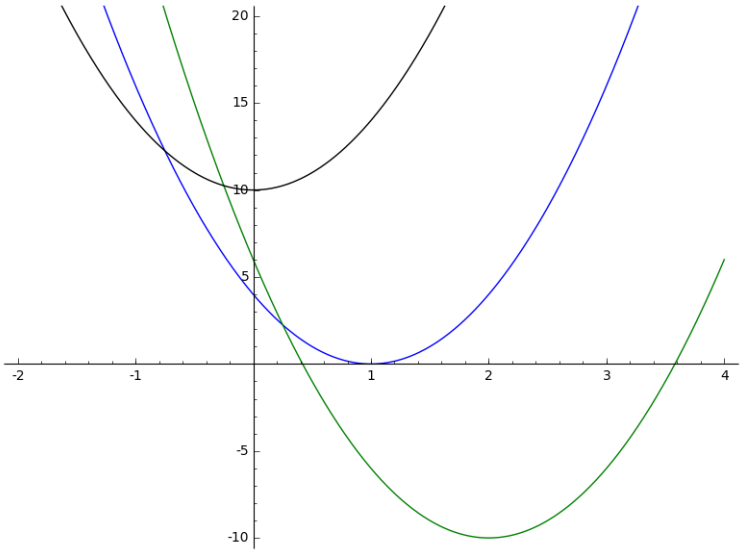

Abbildung 1: Nullstellen verschiedener quadratischer Polynome

Anders ist es bei den Gleichungen dritten Grades: Obwohl unser Beispiel in Abschnitt 1.5 auf *drei reelle Lösungen* führte, siehe Abbildung 2, enthält die Lösungsformel *komplexe, nicht-reelle* Zahlen, und niemand fand einen Weg, diese zu umgehen – wir werden später (Abschnitt 2.4) sehen, warum. Hier saß der Dorn im Fleisch der konservativen Mathematiker und zwang sie schließlich, die komplexen Zahlen zu akzeptieren.

- Ihren ersten Auftritt haben sie bei Bombelli, der auch schon feststellte, dass (bei reellen Gleichungen) eine komplexe Nullstelle immer zusammen mit der konjugiert komplexen auftritt. Er beschrieb komplexe Zahlen (in heutiger Terminologie ausgedrückt) als Linearkombinaionen von ± 1 und $\pm i$ mit positiven Koeffizienten.

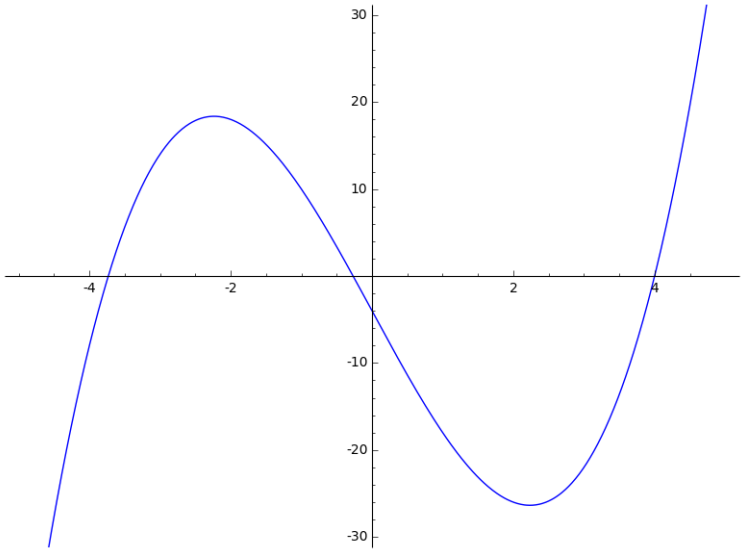

Abbildung 2: Nullstellen eines kubischen Polynoms

- Die geometrische Deutung in der komplexen Zahlenebene wird schon von Euler[12] in seinem Spätwerk um 1780 verwendet, wo er sie sogar in Polarkoordinaten beschreibt.

- Unabhängig davon und voneinander haben auch Wessel[13] 1797 und Argand[14] 1806 die komplexe Zahlenebene „erfunden“. Bei Wessel ist der Bezug zu komplexen Zahlen allerdings nicht explizit erkennbar – er definierte in der Ebene die „Multiplikation von Strecken mit Richtung“ (heute würden wir von ebenen Vektoren sprechen) und gab geometrische Anwendungen davon. Vom Lösen von Gleichungen erwähnte er nichts. Da seine Arbeit in dänisch verfasst (und er ein mathematischer Außenseiter) war, bleib sie über hundert Jahre lang unbeachtet.

- Argand verwendete die geometrische Deutung der komplexen Zahlen für einen (auch heute noch beeindruckend eleganten) Beweis des „Fundamentalsatzes der Algebra“.

- Auch Cauchy[15] hat wie selbstverständlich die komplexen Zahlen samt ihrer geometrischen Beschreibung verwendet. Er gab allerdings noch 1821 eine sehr unklare Definition dieser Zahlen und bezeichnete die Formel

$$\cos(a+b) + \sqrt{-1} \cdot \sin(a+b) = (\cos a + \sqrt{-1} \cdot \sin a) \cdot (\cos b + \sqrt{-1} \cdot \sin b)$$

[12] Leonhard Euler, 1707–1783
[13] Caspar Wessel, 1745–1818
[14] Jean-Robert Argand, 1768–1822
[15] Augustin-Louis Cauchy, 1789–1857

die in der Eulerschen Schreibweise einfacher als

$$e^{i\,(a+b)} = e^{ia} \cdot e^{ib}$$

geschrieben würde, als „sinnlos, aber nützlich“.

- Gauss[16] hat also weder die komplexen Zahlen noch die komplexe Zahlenebene erfunden, obwohl sie nach ihm als „Gaußsche Zahlenebene“ bezeichnet wird. Er hat den komplexen Zahlen allerdings durch eine Publikation 1831 zur allgemeinen Akzeptanz verholfen. Dass sein Name mit dieser Trivialität unlösbar verbunden ist, hat er angesichts seiner gewaltigen mathematischen Leistungen nicht verdient!

Werke

- Bombelli: *L' Algebra*, Bologna 1572.
- Euler: *De formulis differentialibus angularibus maxime irrationalibus, quas tamen per logarithmos et arcus circulares integrale licet.* Vorgetragen an der St. Petersburger Akademie der Wissenschaften 1777, gedruckt 1797.
- Wessel: *Om directionens analytiske betegning*, Kopenhagen 1797.
- Argand: *Essai sur une manière de représenter les quantités imaginaires dans les constructions géométriques*, Paris 1806.
- Cauchy: *Cours d'Analyse de L'École Royale Polytechnique. Analyse Algébrique.* Paris 1821.
- Gauss: *Theoria residuorum biquadraticorum. Commentatio secunda.* Göttingische gelehrte Anzeigen 23.4.1831.

Es fällt auf, dass die früheren Autoren und auch noch Cauchy die *Existenz* der komplexen Zahlen anzweifeln und ihre geometrische Deutung zwar verwenden, aber nicht als Begründung ihrer Existenz ansehen – ein Konflikt, den wir heute kaum noch nachvollziehen können. Die Begründung für die Existenz kann man erst bei Argand feststellen (mit etwas Fantasie auch schon bei Wessel) und dann natürlich auch bei Gauss.

1.7 Auflösung durch Radikale

Wir wollen nun allgemein formalisieren: Was bedeutet es, „eine Gleichung durch Radikale aufzulösen“?

- Für eine quadratische Gleichung über dem Körper K fanden wir die Lösungen in einem Erweiterungskörper $K(\delta) \supseteq K$ mit $\delta^2 \in K$, d. h. unter Hinzuziehung einer Quadratwurzel.

[16] Carl Friedrich Gauß, 1777–1855

- Für eine kubische Gleichung brauchten wir mehrere Wurzeln, quadratische und kubische – wir können uns das als „Turm“ von Erweiterungskörpern vorstellen:

$$K \underbrace{\subseteq}_{\delta^2 \in K} K(\delta) \underbrace{\subseteq}_{u^3 \in K(\delta)} K(\delta, u) \underbrace{\subseteq}_{\rho^3 \in K} K(\delta, u, \rho),$$

  bei dem auf jeder Stufe eine „reine“ Wurzel, also ein „Radikal“, adjungiert wird.

Wir wollen also außer rationalen Ausdrücken in Lösungsformeln (oder -algorithmen) auch reine Wurzeln (Radikale) zulassen. Das wird jetzt in eine allgemeine Definition gefasst:

Definition. Sei K ein Körper.

(i) Sei $L \supseteq K$ ein Erweiterungskörper. Ein Element $\delta \in L$ heißt **Radikal über** K, wenn $\delta^n \in K$ für eine natürliche Zahl $n \geq 1$ ist. (Mit anderen Worten, wenn δ Nullstelle eines „reinen“ Polynoms $X^n - a \in K[X]$ ist.)

(ii) $L \supseteq K$ heißt **einfache Radikalerweiterung**, wenn $L = K(\delta)$ mit einem Radikal δ über K.

(iii) $L \supseteq K$ heißt **Radikalerweiterung**, wenn es eine Kette

$$K = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_m = L$$

von Körpern gibt, so dass K_i jeweils einfache Radikalerweiterung von K_{i-1} ist für $i = 1, \ldots, m$.

(iv) Ein Polynom $f \in K[X]$ heißt **auflösbar durch Radikale über** K, wenn es eine Radikalerweiterung von K gibt, die alle Nullstellen von f enthält.

(v) Sei $f = a_n X^n + \cdots + a_0 \in K[X]$ und $\mathbb{F}$ der Primkörper von K. Dann heißt $\mathbb{F}(a_0, \ldots, a_n)$ der **Koeffizientenkörper** von f; das ist also der kleinste Körper, der alle Koeffizienten von f enthält und somit aus allen Elementen besteht, die sich rational durch die Koeffizienten von f ausdrücken lassen.

(vi) Ein Polynom heißt **auflösbar durch Radikale**, wenn es *über seinem Koeffizientenkörper* auflösbar durch Radikale ist. (Mit anderen Worten, wenn sich alle Nullstellen rational durch die Koeffizienten und (möglicherweise verschachtelte) Radikale ausdrücken lassen.

Bemerkungen

1. Bei (iii) reicht es anzunehmen, dass jeweils $K_i = K_{i-1}(\delta_i)$ mit $\delta_i^{n_i} \in K$, wobei n_i eine *Primzahl* ist, d. h., man braucht nur Radikale von Primzahlgrad zuzulassen. Für einen zusammengesetzten Exponenten führt die Identität $\delta^{mn} = (\delta^m)^n$ nämlich sonst einfach zu einem Zwischenschritt $K \subseteq K(\delta^m) \subseteq K(\delta)$ von einfachen Radikalerweiterungen.

2. **Über** $\mathbb{R}$ ist jedes Polynom durch Radikale auflösbar, weil $\mathbb{C} = \mathbb{R}(i)$ Radikalerweiterung ist. (Das sagt der „Fundamentalsatz der Algebra“.) Das heißt aber *nicht*, dass jedes reelle Polynom durch Radikale auflösbar ist, nämlich *über seinem Koeffizientenkörper*.

3. Nach (i) sind alle Einheitswurzeln Radikale.

Damit stoßen wir auf zwei grundlegende, miteinander verbundene **Probleme**:

1. Welche Polynome sind auflösbar durch Radikale?

2. Wie findet man zu einem Erweiterungskörper $L \supseteq K$ geeignete Zwischenkörper?

Antworten dazu werden durch die Galois-Theorie gegeben.

Aufgaben

1. Sei $K = \mathbb{F}_2$ der Körper mit zwei Elementen. Gibt es eine Erweiterung $L = K(\delta)$ mit $\delta^2 \in K$, in der das Polynom $f = X^2 + X + 1$ eine Nullstelle hat? Ist f durch Radikale auflösbar?

2. Sei K ein Körper und $f = X^4 + aX^2 + bX + c \in K[X|$ ein Polynom vom Grad 4 mit $c \neq 0$.

   (i) Zeige[17]: Es gibt eine Radikalerweiterung $L \supseteq K$, in der f eine Nullstelle hat.

   Anleitung: Für Elemente u, v, w eines Erweiterungskörpers von K gilt

   $$f = (X^2 + uX + v)(X^2 - uX + w) \Longleftrightarrow (*),$$

   wobei $(*)$ ein System aus drei (nichtlinearen) Gleichungen für u, v, w ist. Leite daraus eine kubische Gleichung für u über K, eine quadratische Gleichung für v über $K(u)$ und eine lineare Gleichung für w in $K(u, v)$ ab und zeige, dass Lösungen dieser drei Gleichungen die Bedingung $(*)$ erfüllen.

   (ii) Führt die Konstruktion in (i) zu einer expliziten Lösungsformel?

[17] Unter der Annahme, dass es überhaupt eine Körpererweiterung gibt, in der man die benötigten Wurzeln ziehen kann. Also etwa, dass K in einem algebraisch abgeschlossenen Körper enthalten ist. Für den „klassischen“ Fall $K \subseteq \mathbb{C}$ sagt der „Fundamentalsatz der Algebra“, dass man dafür $\mathbb{C}$ nehmen kann. Historisch war es umgekehrt: Der Ansatz $(*)$ diente Euler als Ausgangspunkt für einen (lückenhaften) Beweis des Fundamentalsatzes.

2 Anwendung – Was gibt uns die Galois-Theorie?

2.1 Die Grundidee der Galois-Theorie (ohne Beweise)

LAGRANGE[18] formulierte sinngemäß als erfolgversprechenden Ansatz zur Auflösung von Gleichungen, d. h. zum sukzessiven Finden geeigneter Radikale:

> Permutiere die Nullstellen des Polynoms und finde Ausdrücke, die bei einigen, aber nicht bei allen Permutationen invariant sind.

Im Beispiel der kubischen Gleichung, siehe Abschnitt 1.4, war das das Produkt der Nullstellendifferenzen

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1).$$

Es ist unter der zyklischen Vertauschung (123)[19] invariant, nicht aber unter der Transposition (12). Sein Quadrat ist die Diskriminante, $\delta^2 = -\Delta$, es lässt sich also als Quadratwurzel über dem Koeffizientenkörper erzeugen, und die Lösung ist über $K(\delta)$ durch kubische Wurzeln ausdrückbar, siehe Satz 2. Der von einem „teilweise“ invarianten Ausdruck erzeugte Zwischenkörper ist also entscheidend für den Aufbau einer Radikal-Erweiterung im Sinne von Abschnitt 1.7.

Die gleiche Idee kann man auch bei VANDERMONDE[20] finden, wenn auch nicht so weit vertieft wie bei LAGRANGE. Auch GAUSS hatte zumindest im Spezialfall der Kreisteilung, also der Konstruktionen mit Zirkel und Lineal, ähnliche Ideen, auch wenn er den Begriff der Invarianz nicht explizit machte. Erst GALOIS[21] gelang es, diesen Ansatz systematisch zum Erfolg zu führen.

Die moderne Fassung der Idee wurde erstmals von DEDEKIND[22] ab 1856 in seinen Vorlesungen klar beschrieben:

> Betrachte den „Zerfällungskörper“ L, der über dem Koeffizientenkörper K durch die Nullstellen erzeugt wird und seine Automorphismengruppe G. Dann liefern die für Untergruppen von G invarianten Elemente die gesuchten Zwischenkörper.

Werke

- LAGRANGE: *Réflexions sur la résolution algébrique des équations*, 1770.
- GALOIS: *Mémoire sur les conditions de résolubilité des équations par radicaux.* 1830 eingereicht, nicht veröffentlicht – bis 1832 redaktionelle Überarbeitungen. Publiziert in: J. Math. Pure Appl. 11 (1846) durch LIOUVILLE.
- DEDEKIND: *Vorlesungen über Zahlentheorie*, Göttingen, XI. Supplement in der 4. Auflage 1894.

[18] Joseph-Louis Lagrange, 1736–1813
[19] also der Permutation $x_1 \mapsto x_2$, $x_2 \mapsto x_3$ $x_3 \mapsto x_1$ in Zyklenschreibweise
[20] Alexandre-Théophile Vandermonde, 1735–1796
[21] Évariste Galois, 1811–1832
[22] Richard Dedekind, 1831–1916

2.2 Einige Ergebnisse der Galois-Theorie (ohne Beweise)

Satz 1 *Sei K ein Körper und $f \in K[X]$ ein irreduzibles Polynom vom Grad n. Sei x eine Nullstelle von f in einem Erweiterungskörper L. Dann ist der Körper $K(x)$ als Vektorraum n-dimensional.*

Die Vektorraum-Dimension $\mathrm{Dim}_K L$ eines Erweiterungskörpers $L \supseteq K$ heißt auch der **Grad** von L über K. Es gilt die Körpergradformel:

Satz 2 *Seien $M \supseteq L \supseteq K$ Körper. Dann ist*

$$\mathrm{Dim}_K M = \mathrm{Dim}_L M \times \mathrm{Dim}_K L.$$

Definition. Ein Körpererweiterung $L \supseteq K$ heißt

(i) **endlich**, wenn $\mathrm{Dim}_K L$ endlich ist,

(ii) **algebraisch**, wenn jedes Element $x \in L$ Nullstelle eines Polynoms $f \in K[X]$ ist,

(iii) **separabel**, wenn jedes Element $x \in L$ Nullstelle eines separablen irreduziblen Polynoms $f \in K[X]$ ist,

(iv) **normal**, wenn jedes irreduzible Polynom $f \in K[X]$, das eine Nullstelle in L hat, in L sogar vollständig in Linearfaktoren zerfällt,

(v) **Galois-Erweiterung**, wenn sie normal und separabel ist,

(vi) **Zerfällungskörper** eines Polynoms $f \in K[X]$, wenn f in $L[X]$ in Linearfaktoren zerfällt und L mit dieser Eigenschaft minimal ist.

Dabei heißt ein Polynom separabel, wenn alle Nullstellen in welchem Erweiterungskörper auch immer paarweise verschieden sind. In Charakteristik 0 sind irreduzible Polynome automatisch separabel, weil sie sonst einen gemeinsamen Teiler mit ihrer Ableitung hätten.

Ist $M \supseteq K$ ein Körper, über dem f in Linearfaktoren zerfällt, und sind $(x_1, \ldots, x_n)$ die Nullstellen von f in M, so ist $L = K(x_1, \ldots, x_n)$ Zerfällungskörper von f,

Satz 3 *Sei K ein Körper, $f \in K[X]$ ein irreduzibles Polynom und $L \supseteq K$ ein Zerfällungskörper von f. Dann ist L normale Erweiterung von K. Ist f außerdem separabel, so ist L Galois-Erweiterung.*

Satz 4 *Sei L ein Körper, $G \subseteq \mathrm{Aut}\, L$ eine endliche Gruppe von Automorphismen von L. Sei $K = L^G$ die Fixpunktmenge von G, d. h. die Menge aller Körperelemente, die von allen Automorphismen in G fest gelassen werden. Dann ist $L \supseteq K$ eine Galois-Erweiterung, $G = \mathrm{Aut}_K L$, und $\mathrm{Dim}_K L = \#G$.*

Korollar 1 *Sei $L \supseteq K$ eine endliche Körpererweiterung und $G = Aut_K L$. Dann sind folgende Aussagen äquivalent:*

(i) *$L \supseteq K$ ist Galois-Erweiterung.*

(ii) $\mathrm{Dim}_K L = \#G$.

(iii) $K = L^G$.

Sei weiter $f \in K[X]$ ein irreduzibles Polynom und $L \supseteq K$ ein Zerfällungskörper von f. Dann heißt die Gruppe $\mathrm{Aut}_K L$ der Körperautomorphismen von L, die K elementweise fest lassen, die **Galois-Gruppe** von f (über K)[23].

Korollar 2 *Sei K ein Körper, $f \in K[X]$ ein irreduzibles und separables Polynom und $L \supseteq K$ ein Zerfällungskörper von f. Sei G die Galois-Gruppe von f über K. Dann ist $L^G = K$ und* $\mathrm{Dim}_K L = \#G$.

Darüber hinaus bildet G die Menge der Nullstellen von f in sich ab, d. h., G ist durch diese Operation auf natürliche Weise als Untergruppe der vollen symmetrischen Gruppe $\mathcal{S}_n$ dargestellt, wenn n der Grad von f ist.

Satz 5 *Sei K ein Körper der Charakteristik* 0[24] *und $f \in K[X]$ ein irreduzibles und separables Polynom mit Galois-Gruppe G. Dann ist f genau dann durch Radikale auflösbar, wenn G eine auflösbare Gruppe ist.*

2.3 Kubische Polynome

Sei weiterhin K ein Körper und $f \in K[X]$ irreduzibel und separabel vom Grad 3. Wegen des Grades 3 bedeutet die Irreduzibilität, dass f in K keine Nullstelle hat, denn bei einer Faktorisierung müsste zwingend ein Faktor vom Grad 1 auftreten. Es sei $L \supseteq K$ ein Zerfällungskörper von f, d. h., f zerfällt in $L[X]$ in Linearfaktoren

$$f = (X - x_1)(X - x_2)(X - x_3)$$

mit den drei verschiedenen Nullstellen $x_1, x_2, x_3 \in L$. Die Galois-Gruppe G von f operiert auf $\{x_1, x_2, x_3\}$ also als Untergruppe von $\mathcal{S}_3$. Diese symmetrische Gruppe wird von den Zykeln

$$\sigma = (123) \quad \text{und} \quad \tau = (23)$$

erzeugt, die auf den Nullstellen so wirken:

$$\begin{aligned} \sigma x_1 = x_2, \quad \sigma x_2 = x_3, \quad \sigma x_3 = x_1, \\ \tau x_1 = x_1, \quad \tau x_2 = x_3, \quad \tau x_3 = x_2. \end{aligned}$$

[23] Damit das wohldefiniert ist, muss man zeigen, dass Zerfällungskörper bis auf Isomorphie eindeutig bestimmt sind.

[24] der Einfachheit halber – sonst wird die Aussage etwas komplizierter

Insbesondere ist der Grad durch die Relation $\mathrm{Dim}_K L|6$ eingeschränkt. Für das Produkt

$$\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1) \in L$$

(wie erinnern uns aus Abschnitt 1.4, dass $\delta^2 = -\Delta \in K$ die Diskriminante ist) gilt

$$\sigma\delta = \delta \quad \text{und} \quad \tau\delta = -\delta.$$

Wir betrachten die Kette

$$K \subseteq K(\delta) \subseteq K(\delta, x_1) \subseteq L.$$

Da $\delta^2 \in K$, ist der Grad $\mathrm{Dim}_K K(\delta) = 1$ oder 2. Insbesondere bleibt f auch über $K(\delta)$ irreduzibel, denn wäre eine Nullstelle von f in $K(\delta)$, müsste der Grad nach Satz 1 genau 3 sein. Es folgt $\mathrm{Dim}_{K(\delta)} K(\delta, x_1) = 3$ und somit $\mathrm{Dim}_K L$ Vielfaches von 3, also $= 3$ oder 6.

Fall 1, $\mathrm{Dim}_K L = 3$: Dann ist $L = K(\delta, x_1)$ (und $\delta \in K$, $\tau \notin G$).

Fall 2, $\mathrm{Dim}_K L = 6$: Dann ist $G = \mathcal{S}_3$, also $\delta \notin K = L^G$ wegen $\tau\delta = -\delta$. Es folgt $\mathrm{Dim}_K K(\delta) = 2$, und nach Satz 2 ist $\mathrm{Dim}_K K(\delta, x_1) = 2 \cdot 3 = 6$. Also auch in diesem Fall $L = K(\delta, x_1)$.

Zusammengefasst:

Hilfssatz 1 *Unter den obigen Voraussetzungen ist $K(\delta, x_1)$ Zerfällungskörper von f, insbesondere normal, und $K(\delta, x_1) = K(\delta, x_2) = K(\delta, x_3)$.*

2.4 Reelle Nullstellen kubischer Polynome

Damit können wir das CARDANO-Formel-Problem aus Abschnitt 1.6 lösen: Sind bei der Lösung einer reellen Gleichung dritten Grades mit drei reellen Lösungen (dem sogenannten *casus irreducibilis*) komplexe Zahlen in der Lösungsformel vermeidbar? Wir werden sehen, dass dies nicht der Fall ist: Es gibt keine Radikal-Erweiterung, die ganz in $\mathbb{R}$ liegt und eine Nullstelle enthält.

Nehmen wir also einen Körper $K \subseteq \mathbb{R}$ und ein Polynom $f \in K[X]$, das in K keine, in $\mathbb{R}$ aber drei verschiedene Nullstellen x_1, x_2, x_3 hat; insbesondere ist f in $K[X]$ irreduzibel. Sei $\delta = (x_1 - x_2)(x_2 - x_3)(x_3 - x_1)$.

Annahme: Es gibt eine Radikal-Erweiterung $K \subseteq L \subseteq \mathbb{R}$, die x_1 enthält.

Unter dieser Annahme gibt es erst recht eine solche Radikal-Erweiterung von $K(\delta)$. (Der Umweg über $K(\delta)$ ist der entscheidende Beweistrick!) Wir finden also eine Kette

$$K \subseteq K_0 = K(\delta) \subseteq \ldots \subseteq K_{n-1} \subseteq K_n \subseteq \mathbb{R},$$

worin alle Schritte $K_{i-1} \subseteq K_i$ einfache Radikal-Erweiterungen sind, o. B. d. A. von Primzahlgrad, mit $x_1 \notin K_{n-1}$, $x_1 \in K_n$. Über K_{n-1} bleibt f irreduzibel, denn sonst läge eine

seiner Nullstellen $x \in K_{n-1}$, aber dann auch ganz $K(\delta, x_1) = K(\delta, x)$ nach Hilfssatz 1. Als einfache Radikal-Erweiterung ist $K_n = K_{n-1}(a)$ mit $a \notin K_{n-1}$, $b = a^p \in K_{n-1}$ für eine Primzahl p. Nach Satz 2 kann es keinen echten Zwischenkörper zwischen K_{n-1} und K_n geben. Also ist $K_n = K_{n-1}(x_1)$, und somit vom Grad 3, und $p = 3$.

Da $x_1 \in K_n$, ist auch $K(\delta, x_1) \subseteq K_n$. Nach Hilfssatz 1 gilt also auch $x_2, x_3 \in K_n$, und daher ist K_n Zerfällungskörper von f über K_{n-1}, insbesondere normal. Also zerfällt auch das irreduzible Polynom $X^3 - b$ über K_n. Dessen Nullstellen sind aber a, ρa, $\rho^2 a$ mit der nichttrivialen Einheitswurzel $\rho = (-1 + \sqrt{-3})/2$, die definitiv nicht reell ist, Widerspruch!

Damit ist (KNESER[25] 1893 zugeschrieben) bewiesen, was LEIBNIZ schon vermutet hatte:

Satz 6 *Sei $f \in \mathbb{R}[X]$ ein Polynom vom Grad 3, irreduzibel über seinem Koeffizientenkörper und mit drei verschiedenen reellen Nullstellen. Dann gibt es für keine der Nullstellen eine Lösungsformel mit nur reellen Radikalen. Insbesondere ist der Zerfällungskörper $\subseteq \mathbb{R}$ selbst keine Radikal-Erweiterung.*

2.5 Symmetrische Polynome

Wir verlassen kurz mal den momentanen Kontext und betrachten den Polynomring $K[t] = K[t_1, \ldots, t_n]$ über einem Körper K in den Unbestimmten $t_1, \ldots, t_n$. Jede Permutation $\sigma \in \mathcal{S}_n$ induziert einen Automorphismus von $K[t]$ durch $\sigma t_i := t_{\sigma i}$, der sich auch auf den Quotientenkörper $K(t)$ fortsetzt. Diese Operation der symmetrischen Gruppe $\mathcal{S}_n$ lässt die **elementarsymmetrischen Polynome**

$$\begin{aligned} s_1 &= t_1 + \cdots + t_n, \\ &\vdots \\ s_i &= \sum_{\substack{I \subseteq \{1,\ldots,n\} \\ \#I = i}} \prod_{i \in I} t_i \\ &\vdots \\ s_n &= t_1 \cdots t_n, \end{aligned}$$

invariant. Diese erzeugen einen Teilkörper $K(s) = K(s_1, \ldots, s_n) \subseteq K(t)$. Der Hauptsatz über symmetrische Polynome in einer schwachen Version lässt sich so formulieren:

Satz 7 *$K(s) = K(t)^{\mathcal{S}_n}$. Insbesondere ist $K(t) \supseteq K(s)$ eine Galois-Erweiterung vom Grad $n!$.*

Beweis. Da $K(s) \subseteq K(t)^{\mathcal{S}_n}$, ist nur noch zu zeigen, dass der Grad $\leq n!$ ist. Das wird durch Induktion über n bewiesen. Der Induktionsanfang $n = 1$ ist trivial: $K(s) = K(t)$ und $\mathcal{S}_1 = \mathbf{1}$.

[25] Adolf Kneser, 1862–1930

Sei nun $n \geq 2$. Wir betrachten den Zwischenschritt

$$K(t) \overset{b)}{\supseteq} K(s, t_n) \overset{a)}{\supseteq} K(s).$$

Bei der Körpererweiterung a) ist t_n Nullstelle des Polynoms

$$(X - t_1) \cdots (X - t_n) = X^n - s_1 X^{n-1} \pm \ldots \pm s_n \in K(s)[X]$$

vom Grad n. Also $\mathrm{Dim}_{K(s)} K(s, t_n) \leq n$.

Für die Körpererweiterung b) bezeichnen wir die elementarsymmetrischen Polynome in $t_1, \ldots, t_{n-1}$ mit $u_1, \ldots, u_{n-1}$. Setzen wir noch $u_0 = 1$ und $u_n = 0$, so gilt offensichtlich

$$s_j = u_j + t_n u_{j-1} \quad \text{für } j = 1, \ldots, n.$$

Die Erweiterung

$$K(s)(t_n) = K(t_n)(u) \subseteq K(t_n)(t_1, \ldots, t_{n-1}) = K(t)$$

hat nach Induktionsannahme den Grad $\leq (n-1)!$. Die Körpergradformel gibt für die Zusammensetzung den Grad $\leq n!$. $\diamond$

Korollar 3 *Die elementarsymmetrischen Polynome $s_1, \ldots, s_n$ sind über K algebraisch unabhängig.*

Beweis. Der Transzendenzgrad[26] von $K(s)$ ist gleich dem von $K(t)$, also n. $\diamond$

Hilfssatz 2 *Das Polynom $F = (X - t_1) \cdots (X - t_n) \in K(s)[X]$ ist über $K(s)$ irreduzibel.*

Beweis.[27] Ein echter Teiler g müsste (bis auf einen Faktor in $K(s)$) bei geeigneter Numerierung die Gestalt

$$g = (X - t_1) \cdots (X - t_r) \quad \text{mit } 1 \leq r < n$$

haben. Das bedeutet aber, dass $t_1 + \cdots + t_r \in K(s)$ unter der Gruppe $\mathcal{S}_n$ invariant sein müsste. Also z. B., wenn t_r durch t_{r-1} ersetzt wird, Widerspruch. $\diamond$

Korollar 4 *$K(t)$ ist der Zerfällungskörper von F über $K(s)$.*

[26] dessen Kenntnis hier als bekannt angenommen wird

[27] unter Verwendung der Teilbarkeitslehre von Polynomen

2.6 Das allgemeine Polynom vom Grad 5 oder mehr ist nicht durch Radikale auflösbar.

Naiv betrachtet soll **das allgemeine Polynom** vom Grad n der Ausdruck

$$f = X^n + a_1 X^{n-1} + \cdots + a_n$$

sein, bei dem die Koeffizienten einfach Unbestimmte ohne jede weitere Relation sind. Eine Formel für eine Nullstelle dieses Polynoms würde also durch Einsetzen von „konkreten“ Werten für die Koeffizienten auch Nullstellen für jedes gegebene Poynom vom Grad n liefern. D. h., eine Lösungsformel für Nullstellen von f wäre eine Lösungsformel für alle Polynome vom Grad n.

Mathematisch korrekt läßt sich das fassen, indem wir über einem Primkörper $\mathbb{F}$ einen Polynomring $\mathbb{F}[a_1, \ldots, a_n]$ in n Unbestimmten $a_1, \ldots, a_n$ betrachten. Sein Quotientenkörper

$$K = \mathbb{F}(a_1, \ldots, a_n)$$

besteht dann genau aus allem, was sich rational durch $a_1, \ldots, a_n$ ausdrücken lässt, ist also der Koeffizientenkörper von $f = X^n + a_1 X^{n-1} + \cdots + a_n$.

Durch die Zuordnung $a_j \mapsto s_j$ wird der Körper K in den rationalen Funktionenkörper $\mathbb{F}(t)$ eingebettet, und f wird zu dem in Abschnitt 2.5 betrachteten Polynom F. Daher ist f über K irreduzibel und separabel, und die Galois-Gruppe von f ist (isomorph zu) $\mathcal{S}_n$. Aus der Gruppentheorie wissen wir, dass die Gruppe $\mathcal{S}_n$ nur für $n \leq 4$ auflösbar ist. Damit ist, jedenfalls in Charakteristik 0, gezeigt:

Satz 8 *Das allgemeine Polynom vom Grad n ist für $n \geq 5$ nicht durch Radikale auflösbar.*

2.7 Auflösung von Polynomen vom Grad 4

Die Auflösung der Gleichung vierten Grades durch Radikale war ja mit elementaren Methoden recht leicht, siehe die Aufgabe in Abschnitt 1.7 – vorausgesetzt, man findet den passenden Ansatz. Hier wollen wir sehen, wie die Galois-Theorie dabei systematisch helfen kann.

Sei K ein Körper der Charakteristik $\neq 2, 3$ und $f \in K[X]$ ein irreduzibles separables Polynom mit Zerfällungskörper L, Nullstellen $x_1, x_2, x_3, x_4 \in L$ und Galois-Gruppe $G = \mathrm{Aut}_K L \subseteq \mathcal{S}_4$.

Die symmetrische Gruppe $\mathcal{S}_4$ hat die Ordnung 24 und hat eine Kleinsche Vierergruppe als Normalteiler:

$$V = \{\mathbf{1}, (12)(34), (13)(24), (14)(23)\} \trianglelefteq \mathcal{S}_4 \,.$$

Für den Normalteiler $H = V \cap G \trianglelefteq G$ sollte der „Invariantenkörper“ L^H also ein *für die Auflösung geeigneter Zwischenkörper* sein.

Die drei Größen

$$\begin{aligned} y_1 &:= (x_1+x_2)(x_3+x_4) \\ y_2 &:= (x_1+x_3)(x_2+x_4) \\ y_3 &:= (x_1+x_4)(x_2+x_3) \end{aligned}$$

sind unter V (aber nicht unter $\mathcal{S}_4$) invariant, liegen also in L^H, aber mutmaßlich nicht in K. Ihre elementarsymmetrischen Kombinationen

$$\begin{aligned} y_1+y_2+y_3 &= 2\,x_1x_2+2\,x_1x_3+2\,x_1x_4+2\,x_2x_3+2\,x_2x_4+2\,x_3x_4 = 2p\,, \\ y_1y_2+y_2y_3+y_3y_1 &= \ldots = p^2-4r, \\ y_1y_2y_3 &= \ldots = -q^2, \end{aligned}$$

liegen in K, also sind y_1, y_2, y_3 die drei Nullstellen des kubischen Polynoms

$$Y^3-2p\,Y^2+(p-4r)\,Y+q^2 \in K[Y]$$

und sind somit über K durch Radikale darstellbar. Dieses Polynom heißt die **kubische Resolvente** von f. Da $K(y)$ deren Zerfällungskörper ist, ist es eine normale Erweiterung von K.

Um daraus x_1, x_2, x_3 und x_4 zu bestimmen, betrachten wir drei weitere Hilfsgrößen, die Quadratwurzeln über $K(y)$ sind:

$$\begin{aligned} z_1 = x_1+x_2 = -x_3-x_4 &\implies z_1^2 = -y_1, \\ z_2 = x_1+x_3 = -x_2-x_4 &\implies z_2^2 = -y_2, \\ z_3 = x_1+x_4 = -x_2-x_3 &\implies z_3^2 = -y_3. \end{aligned}$$

Es ist $z_1+z_2+z_3 = 3\,x_1+x_2+x_3+x_4 = 2\,x_1$, also

$$x_1 = \frac{1}{2}\,(z_1+z_2+z_3).$$

Ebenso folgt

$$\begin{aligned} x_2 &= \frac{1}{2}\,(z_1-z_2-z_3), \\ x_3 &= \frac{1}{2}\,(-z_1+z_2-z_3), \\ x_3 &= \frac{1}{2}\,(-z_1-z_2+z_3), \end{aligned}$$

und damit sind die Nullstellen von f durch (ziemlich verschachtelte) Radikale ausgedrückt, entsprechend der Kette

$$K \subseteq K(y) \subseteq K(y,z) = L$$

von Erweiterungskörpern.

Aufgaben

1. Bestimme die Nullstellen von $X^4+2\,X^2+2X+5/4$.