

**EINFÜHRUNG IN DIE ALGEBRA
UNIVERSITÄT AUGSBURG
SOMMERSEMESTER 2014**

J.-H. ESCHENBURG

I. Gleichungen

1. “ALGEBRA”

Das Wort “Geometrie” ist griechischen Ursprungs (Geo-metrie = Erd-Messung), das Wort “Algebra” dagegen kommt aus dem Arabischen. Es stammt von dem arabischen Verb “dschabr” = “vervollständigen”. In mathematischer Bedeutung tritt es zum ersten Mal um 825 n.Chr. in dem Buchtitel “Hisab al-dschabr wa-l-muqabala” (Rechenverfahren durch Vervollständigen und Ausgleichen) des persisch-arabischen Mathematikers Al-Chwarizmi¹ auf, von dessen Namen übrigens auch das Wort “Algorithmus” (Rechenverfahren) abgeleitet wurde.² Die beiden Worte “al-dschabr” (das Vervollständigen) und “al-muqabala” (das Ausgleichen) bezeichnen zwei Sorten von Umformungen von Gleichungen zum Zwecke der leichteren Lösung: Beseitigung negativer Terme durch Vervollständigung (al-dschabr) sowie Verkleinerung positiver Terme auf beiden Seiten durch Ausgleich (al-muqabala). Als Beispiele nennt Al-Chwarizmi:³

$$\begin{aligned}x^2 &= 40x - 4x^2 \\5x^2 &= 40x,\end{aligned}$$

sowie

$$\begin{aligned}50 + 3x + x^2 &= 29 + 10x \\21 + x^2 &= 7x.\end{aligned}$$

Von Anfang an also war die Algebra verbunden mit dem Lösen von Gleichungen der Form

$$f(x) = 0$$

Date: 27. Juli 2014.

¹Abu Dscha’far Muhammad ibn Musa al-Chwarizmi, ca. 780 - 850 n.Chr., vermutlich persischer Herkunft, hat vorwiegend in Bagdad gelebt und am dortigen “Haus der Weisheit” gelehrt und gearbeitet.

²<http://de.wikipedia.org/wiki/Algorithmus>

³<http://www-history.mcs.st-and.ac.uk/Biographies/Al-Khwarizmi.html>

mit

$$f(x) = a_0x^n + a_1x^{n-1} + \dots + a_n, \quad (1)$$

wobei n eine beliebige natürliche Zahl⁴ ist, der *Grad* der Gleichung, und a_0, a_1, \dots, a_n gegebene Zahlen sind, die *Koeffizienten* der Gleichung. Dagegen ist x eine Zahl, die wir noch nicht kennen, die wir erst suchen, eine “Unbekannte”. Die Aufgabe ist eben gerade, diese Zahl oder diese Zahlen x (wenn es mehrere davon gibt) zu finden; die so gefundenen Werte x sind die *Lösungen* der Gleichung $f(x) = 0$, manchmal auch *Wurzeln* genannt.

Den Ausdruck (1) kann man allerdings nicht nur für die gesuchten Zahlen x auswerten, sondern ebenso für jede andere Zahl; er beschreibt eine *Funktion*, eine Rechenoperation, die *jeder beliebigen* Zahl x eine andere Zahl $f(x)$ zuordnet. In dieser Formulierung hat der Buchstabe x eine neue Bedeutung bekommen: Aus einer “Unbekannten” wurde eine “Unbestimmte”: eine variable Zahl, eine Art Joker, für die wir jede echte Zahl einsetzen dürfen. Die Funktion $f(x)$ in (1) ist allerdings von einer besonderen Art, die für die Algebra typisch ist: Die rechte Seite von (1) ist eine Summe von Vielfachen (“Linearkombination”) von Potenzen der Variablen x . Einen solchen Ausdruck nennt man ein *Polynom*,⁵ und die höchste vorkommende Potenz heißt der *Grad* des Polynoms. Für den Grad eines Polynoms f schreiben wir ∂f . In dieser neuen Sprache kann man die Aufgabe des Gleichungslösens so formulieren: Gesucht sind die *Nullstellen* des Polynoms f , also diejenigen Zahlen x , die in $f(x)$ eingesetzt den Wert Null ergeben. Die Untersuchung der Nullstellen von Polynomen in einer Variablen x oder auch in mehreren Variablen⁶ x, y, z oder x_1, \dots, x_k , $k \in \mathbb{N}$, ist bis heute eine wichtige Aufgabe der Algebra.

Es ist einfach, für eine gegebene Zahl x den Wert $f(x)$ zu berechnen, aber das Gleichungslösen ist die Umkehraufgabe: Der Wert $f(x)$ ist gegeben, nämlich 0, gesucht ist das x , das diesen Wert ergibt. Diese Aufgabe ist nicht so einfach. Für die Grade 1 bis 4 gibt es Formeln, die die Unbekannte aus den Koeffizienten mit Hilfe der vier Grundrechenarten und dem Wurzelziehen berechnen; für die quadratische Gleichung $x^2 - ax = b$ ist das die berühmte “Mitternachtsformel”

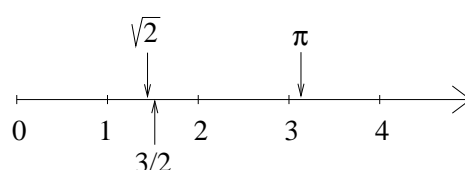
⁴Die *natürlichen Zahlen* sind die positiven ganzen Zahlen. Die Menge der natürlichen Zahlen wird mit \mathbb{N} bezeichnet, $\mathbb{N} = \{1, 2, 3, \dots\}$.

⁵Griechisch Poly-nom = vielfacher Ausdruck, eben eine Summe mit vielen Summanden. Jeder einzelne Summand ist ein “Monom” = einzelner Ausdruck.

⁶Bei einem Polynom in mehreren Variablen x_1, \dots, x_k , sind die einzelnen Summanden (Monome) nicht nur Vielfache von Potenzen x_1, x_1^2, x_2^3 usw., sondern auch von Produkten verschiedener Variablen, z.B. $x_1 \cdot x_2$ oder $x_1^2 \cdot x_2^3 \cdot x_3$.

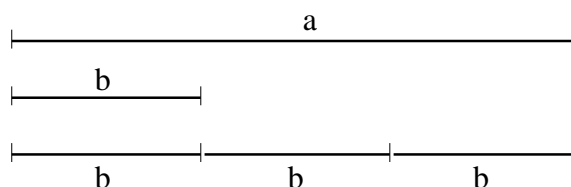
$x = \frac{1}{2}(a \pm \sqrt{a^2 + 4b})$. Wir werden alle diese Formeln verstehen lernen. Für den Grad 5 gibt es immer noch eine Art Lösungsformel, aber man benötigt neben den Grundrechenarten und dem Wurzelziehen noch eine neue Rechenart. Ab Grad 6 kennt man Lösungsformeln nur noch in Spezialfällen. Warum das so ist, warum manche Gleichungen leicht und andere schwer oder mit beschränkten Mitteln gar nicht lösbar sind, darüber gibt die *Galois-Theorie*⁷ Auskunft, die wir in den Grundzügen erklären wollen.

2. DAS GEMEINSAME MASS



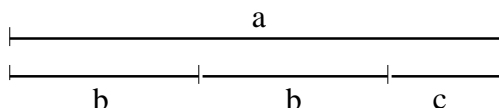
Wir Heutigen sind gewohnt, uns ein geometrisches Bild von den (positiven) Zahlen zu machen: Sie liegen auf dem Zahlenstrahl, der bei Null anfängt und durch die natürlichen Zahlen $1, 2, 3, \dots$ gleichmäßig unterteilt ist wie unser Zentimetermaß. Dazwischen haben die Brüche ihre genaue Position, zum Beispiel liegt $\frac{3}{2}$ genau auf der Mitte zwischen 1 und 2. Vielleicht wissen wir noch, dass wir mit den Brüchen nicht auskommen, dass es noch weitere Zahlen dazwischen gibt, sogenannte Irrationalzahlen wie $\sqrt{2}$ oder π , aber auch deren Position auf dem Zahlenstrahl ist genau fixierbar.

Dieses Bild ist neuzeitlich. In der Antike kannte man zunächst nur die natürlichen Zahlen. Sie dienten zum Zählen von endlichen Mengen, irgendwelchen Zusammenfassungen von Individuen. Doch schon früh wusste man auch, dass die Zahlen noch zu etwas anderem dienen konnten: zum Vergleichen von *Größen*. Das waren zum Beispiel Längen, Flächen- und Rauminhalte, Massen, Zeitspannen. Da es keine allgemein anerkannten Maßeinheiten gab, konnte man solche Größen nicht einfach durch Zahlen ausdrücken. Aber man konnte zwei von ihnen miteinander vergleichen, zum Beispiel eine größere Strecke a mit einer kleineren b .

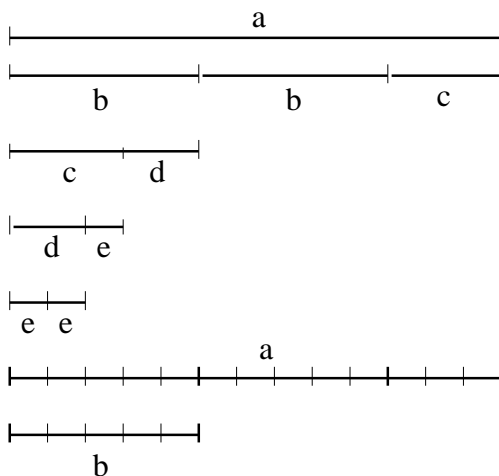


⁷Évariste Galois, 1811 (Bourg-la-Reine) - 1832 (Paris)

Im besten Fall konnte man a genau durch mehrfaches Aneinanderlegen von b gewinnen, wie in unserer Figur, in der wir $a = 3b$ erhalten. Weder a noch b sind Zahlen, aber gemeinsam definieren sie eine Zahl, nämlich ihr *Verhältnis* $a/b = 3$. Aber was machen wir, wenn es nicht auskommt? In unserer zweiten Figur passt b zweimal in a hinein, und es bleibt noch ein Rest c . Dieser ist kleiner als b , sonst würde ja noch ein drittes Exemplar von b in a hineinpassen.



Zunächst können wir nur sagen, dass das Verhältnis a/b zwischen 2 und 3 liegen muss. Um es genauer zu bestimmen, müssen wir c mit b vergleichen. Das geht auf gleiche Weise wie vorher: Wir haben eine große und eine kleine Strecke, statt a und b diesmal b und c , und wieder prüfen wir, wie oft c in b hineinpasst: in unserer Figur einmal, und es bleibt ein Rest d , der kleiner als c ist. Nun vergleichen wir d mit c ; wieder geht d einmal in c hinein mit einem Rest e , der in unserem Beispiel schließlich genau zweimal in d aufgeht.



Rechnen wir zurück, so ist

$$\begin{aligned} d &= 2e \\ c &= d + e = 2e + e = 3e \\ b &= c + d = 3e + 2e = \underline{5e} \\ a &= 2b + c = 2 \cdot 5e + 3e = \underline{13e}. \end{aligned}$$

Wir stellen also fest, dass zwar b in a nicht ganzzahlig aufgeht, dass es aber eine kleinere Strecke e gibt, die sowohl in a als auch in b ganzzahlig aufgeht, 13-mal in a und 5-mal in b . Wir haben keine Maßeinheit gebraucht, um dies festzustellen; die beiden Strecken haben sich nämlich

die für den Vergleich am besten geeignete Maßeinheit, ihr “gemeinsames Maß” e , selbst gesucht. Damit können wir wieder das genaue Verhältnis a/b feststellen, nämlich $13/5$. Wenn a und b bereits selbst natürliche Zahlen sind (ganze Vielfache einer irgendwie gewählten Maßeinheit), dann ist das gemeinsame Maß der größte gemeinsame Teiler (ggT) von a und b , der also auf diese Weise ermittelt werden kann.⁸

Das Verfahren heißt *Wechselwegnahme* oder *euklidischer Algorithmus*, weil es von *Euklid*⁹ beschrieben worden ist. Es ist aber sehr viel älter und war zum Beispiel Pythagoras¹⁰ vor 500 v.Chr. bestens bekannt. Dieser hatte die Bedeutung des Verfahrens voll erkannt und soll in den Jubelruf “Alles ist Zahl” ausgebrochen sein, weil sich auf diese Weise die Verhältnisse beliebiger Größen, aus welchem Bereich auch immer sie stammen mochten, durch ein Verhältnis von Zahlen ausdrücken ließen. Es war die Geburtsstunde der angewandten Mathematik.

Doch nur wenige Jahre später schüttete ein Schüler des Pythagoras, vermutlich Hippasos,¹¹ reichlich Wasser in diesen schönen Wein, und zwar durch eine der folgenreichsten mathematischen Erkenntnisse der Antike: Es gibt Strecken a und b , deren Verhältnis mit der Wechselwegnahme niemals genau ermittelt werden kann; immer bleibt noch ein Rest und das Verfahren endet nie. Vermutlich geschah diese Entdeckung am *Goldenen Schnitt*. Dabei wird eine Strecke a so in zwei

⁸ Wenn wir die aus der Figur zu entnehmenden Gleichungen

$$(1) a = 2b + c, \quad (2) b = c + d, \quad (3) c = d + e$$

anders herum auflösen, können wir umgekehrt das gemeinsame Maß e durch die gegebenen Größen a und b ausdrücken; diese Beobachtung wird auch für Polynome wichtig werden, die bekanntlich eine ganz ähnliche Division mit Rest zulassen.

$$(3) e = c - d, \quad (2) d = b - c, \quad (1) c = a - 2b$$

und daraus

$$e \stackrel{1}{=} c - d \stackrel{2}{=} c - (b - c) = 2c - b \stackrel{3}{=} 2(a - 2b) - b = 2a - 5b.$$

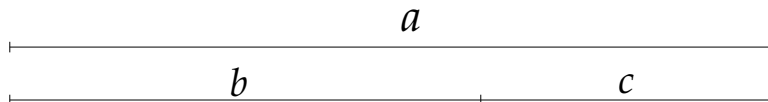
Probe: $a = 13, b = 5 \Rightarrow 2a - 5b = 26 - 25 = 1$. Übrigens gibt es noch andere Darstellungen des gemeinsamen Maßes durch a und b , zum Beispiel $e = 8b - 3a$ (Probe: $8 \cdot 5 - 3 \cdot 13 = 40 - 39 = 1$). Auf diese letztere Darstellung stößt man, wenn man zu den obigen Gleichungen noch die Gleichung (4) $d = e + e$ hinzunimmt: $e \stackrel{4}{=} d - e \stackrel{3}{=} d - (c - d) = 2d - c \stackrel{2}{=} 2(b - c) - c = 2b - 3c \stackrel{1}{=} 2b - 3(a - 2b) = 8b - 3a$.

⁹Euklid von Alexandria, ca. 325 - 265 v.Chr. (Alexandria, Ägypten), fasste um 300 v.Chr. das gesamte mathematische Wissen seiner Zeit in seinem Lehrbuch “Elemente” zusammen. Die Proportionenlehre findet sich im 5. Buch der “Elemente”.

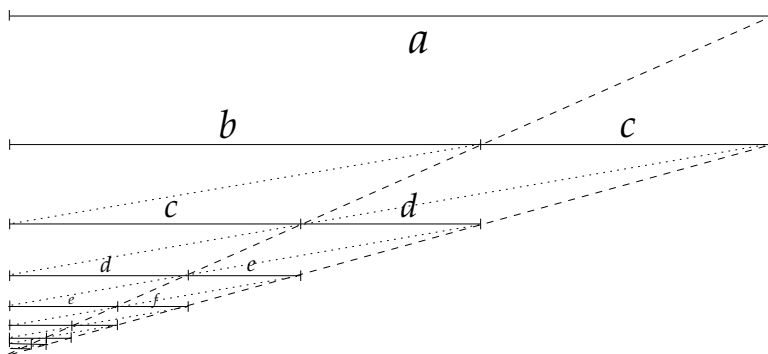
¹⁰Pythagoras von Samos, ca. 570 - 510 v.Chr.

¹¹Hippasos von Metapont, ca. 550 - 470 v.Chr., Metapont (Süditalien)

ungleiche Teile b und c unterteilt, dass sie sich zum größeren Teil b so verhält wie b zum Rest c , also $a/b = b/c$ oder $\frac{b+c}{b} = \frac{b}{c}$.¹²



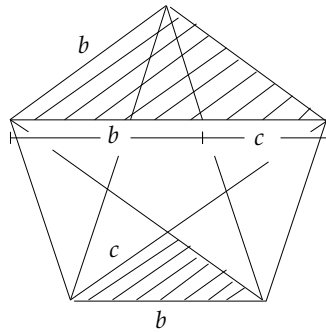
Die Teilstrecke b passt also einmal in a hinein, und der Rest c steht zu b wieder im gleichen Verhältnis wie vorher b zu a , also $b/c = a/b$. Beim Vergleich von c mit b stehen wir daher wieder vor der gleichen Situation; b und c bilden ein verkleinertes Abbild von a und b , weil ja die Verhältnisse (Proportionen) gleich sind. Wieder passt c einmal in b hinein, und für den Rest d gilt wiederum $b/c = c/d$.



Diese Situation wiederholt sich auf jeder Stufe; das Verfahren bricht niemals ab und wir finden deshalb kein gemeinsames Maß.

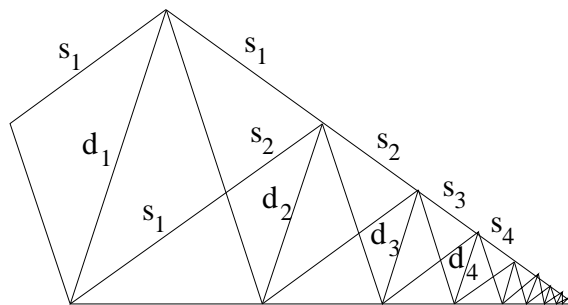
Der Goldene Schnitt war in der Zeit um 500 v.Chr. nicht nur den Mathematikern, sondern auch den Künstlern bestens bekannt und fand vielfache Verwendung. Die Schule des Pythagoras hatte sogar ein besonders enges Verhältnis dazu, denn ihr Symbol war das Pentagramm, der Diagonalenstern des regelmäßigen Fünfecks, und je zwei Diagonalen unterteilen sich gegenseitig im Verhältnis des goldenen Schnittes. Dies folgt aus der *Ähnlichkeit* (gleiche Form bei unterschiedlicher Größe) der beiden in der nachfolgenden Figur schraffierten gleichschenkligen Dreiecke:

¹²Aus der Gleichung $\frac{b+c}{b} = \frac{b}{c}$ lässt sich der Wert dieses Verhältnisses $x = a/b = b/c$ ermitteln: $x = \frac{b}{c} = \frac{b+c}{b} = 1 + \frac{c}{b} = 1 + \frac{1}{x}$. Multiplikation mit x auf beiden Seiten ergibt die quadratische Gleichung $x^2 = x + 1$ mit der positiven Lösung $x = \frac{1}{2}(1 + \sqrt{5}) \approx 1,618$ (die zweite Lösung $\frac{1}{2}(1 - \sqrt{5})$ ist negativ). Diese Zahl x und ihr Kehrwert $\frac{1}{x} = x - 1 = \frac{1}{2}(\sqrt{5} - 1) \approx 0,618$ werden *Goldener Schnitt* genannt.



Das Verhältnis von großer und kleiner Seite ist in den beiden ähnlichen Dreiecken dasselbe, also folgt das goldene Schnittverhältnis $\frac{b+c}{b} = \frac{b}{c}$.

Mit dieser Konstruktion können wir sehr anschaulich erkennen, dass es wirklich kein gemeinsames Maß zwischen a und b oder zwischen b und c gibt (nicht nur, dass wir keins finden konnten). Möglicherweise ist auch Hippasos so zu seiner Erkenntnis gelangt. Dazu betrachten wir eine Kette von immer kleineren Fünfecken, wobei die Seite s_k des k -ten Fünfecks die Diagonale d_{k+1} des $(k+1)$ -ten Fünfecks ist:



Aus der Figur sehen wir $d_2 = s_1$ und $s_2 = d_1 - s_1$, allgemein

$$(*) \quad d_{k+1} = s_k, \quad s_{k+1} = d_k - s_k.$$

Wenn d_1 und s_1 ein gemeinsames Maß hätten, also ganze Vielfache einer Strecke e wären (wie klein diese auch immer sein mag), dann wären auch $d_2 = s_1$ und $s_2 = d_1 - s_1$ ganze Vielfache von e , und durch Wiederholung des Schlusses würde dasselbe für alle d_k und s_k gelten: Alle sind ganzzahlige Vielfache von e , und doch werden sie beliebig klein und schließlich kleiner als e , ein Widerspruch!¹³

Diagonale und Seitenlänge des regelmäßigen Fünfecks besitzen somit kein gemeinsames Maß, sie sind *inkommensurabel*. Ihr Verhältnis (das

¹³Es ist sehr bemerkenswert, dass gerade das ganzzahlige Gleichungssystem (*) zu einer Nicht-Ganzzahligkeits-Aussage führt: Diagonale und Seitenlänge sind nicht ganzzahlige Vielfache eines gemeinsamen Maßes.

goldene Schnittverhältnis) lässt sich nicht mehr als Verhältnis ganzer Zahlen schreiben; es ist *irrational*.^{14 15}

Pythagoras' Erkenntnis "Alles ist Zahl" war daher falsch, solange man unter "Zahl" nur die natürlichen Zahlen und ihre Verhältnisse verstand. Das Zahlverständnis änderte sich aber im Verlauf der folgenden zwei Jahrhunderte; man fing an, auch irrationale Verhältnisse zwischen Größen als Zahlen anzuerkennen. Der Ersatz für die Darstellung von Größenverhältnissen $\frac{a}{b}$ als Verhältnis natürlicher Zahlen $\frac{k}{n}$ war das *Archimedische Axiom*,¹⁶ das Archimedes selbst aber dem Eudoxos¹⁷ zuschreibt:

Zu je zwei Größen a, b mit $a > b$ gibt es eine natürliche Zahl k mit $kb \leq a < (k + 1)b$.

Wenn wir diesen Grundsatz statt auf a und b auf na und b für eine beliebig große Zahl $n \in \mathbb{N}$ anwenden, finden wir ein $k \in \mathbb{N}$ mit

$$kb \leq na < (k + 1)b$$

und damit $\frac{k}{n} \leq \frac{a}{b} < \frac{k+1}{n} = \frac{k}{n} + \frac{1}{n}$. Das Verhältnis $\frac{a}{b}$ ist also fast gleich dem ganzzahligen Verhältnis $\frac{k}{n}$; es weicht davon um höchstens $\frac{1}{n}$ ab.

Dies war die erste bewusst durchgeführte *Zahlbereichserweiterung* der Mathematikgeschichte. Die *reellen Zahlen* \mathbb{R} waren geboren als Größenverhältnisse, die durch Verhältnisse ganzer Zahlen zwar nicht immer ausgedrückt, aber doch angenähert werden konnten.

3. DIE BINOMISCHE FORMEL

Ein *Binom* ist ein Ausdruck der Form $(a + b)^n$ mit $n \in \mathbb{N}$. Für kleine n wissen wir, wie wir eine solche Potenz *ausmultiplizieren*, d.h. mit Hilfe des *Distributivgesetzes*¹⁸ als Summe schreiben:

$$(a + b)^2 = (a + b)(a + b)$$

¹⁴Die *rationalen Zahlen* \mathbb{Q} (von lat./engl. "ratio" = Verhältnis) sind die Quotienten ganzer Zahlen k/n (Brüche). "Irrational" bedeutet: Kein Verhältnis ganzer Zahlen.

¹⁵Der Goldene Schnitt ist nicht nur irgend eine irrationale Zahl, sondern die "irrationalste" Zahl überhaupt: In jedem Schritt passt der Rest nur einmal in die Teilstrecke hinein, er ist also fast so groß wie diese, und deshalb sind wir maximal weit von einem rationalen Verhältnis entfernt.

¹⁶Archimedes von Syrakus, ca. 287 - 212 v.Chr.

¹⁷Eudoxos von Knidos, ca. 408 - 355 v.Chr.

¹⁸Das *Distributivgesetz* lautet $(u_1 + u_2)v = u_1v + u_2v$ für beliebige Zahlen u_1, u_2, v . Wir brauchen auch die Version mit mehr als zwei Summanden: $(u_1 + u_2 + u_3)v = (u_1 + u_2)v + u_3v = u_1v + u_2v + u_3v$ und allgemeiner $(u_1 + \dots + u_n)v = u_1v + \dots + u_nv$ für beliebige Anzahlen n von Zahlen u_1, \dots, u_n . Formal beweist man dies durch vollständige Induktion, siehe die folgende Fußnote 19.

$$\begin{aligned}
&= a(a+b) + b(a+b) \\
&= aa + ab + ba + bb \\
&= a^2 + 2ab + b^2, \\
(a+b)^3 &= (a+b)^2(a+b) \\
&= (aa + ab + ba + bb)(a+b) \\
&= aaa + \underline{aba} + \underline{baa} + \underline{bba} + \underline{aab} + \underline{abb} + \underline{bab} + bbb \\
&= a^3 + \underline{3a^2b} + \underline{3ab^2} + b^3.
\end{aligned}$$

Die Summanden von $(a+b)^3$ in der vorletzten Zeile sind sämtliche ab -Sequenzen der Länge 3, d.h. Produkte aus je drei Faktoren vom Typ a oder b , wobei wir zunächst die Reihenfolge der Faktoren beachten. Auf diese kommt es aber beim Produkt nicht an, deshalb können wir im letzten Schritt alle Produkte mit gleicher Anzahl von a - und b -Faktoren zusammenfassen. Ebenso ist es mit $(a+b)^n$ für beliebiges n . Ausmultiplizieren ergibt die Summe aus allen ab -Sequenzen der Länge n .¹⁹

Jede solche Sequenz ist ein Produkt der Form $a^{n-k}b^k$. Wieviele gibt es davon für festes k ? Die k Plätze in einer solchen Sequenz, an denen ein b steht, bilden eine k -elementige Teilmenge der Menge $\{1, \dots, n\}$, und es gibt ebenso viele Sequenzen vom Typ $a^{n-k}b^k$ wie k -elementige Teilmengen von $\{1, \dots, n\}$. Die Anzahl der k -elementigen Teilmengen von $\{1, \dots, n\}$ wird mit $\binom{n}{k}$ (“ n über k ” oder “ k aus n ”) bezeichnet. Wie können wir diese Anzahl berechnen? Das ist wie beim Lottospielen. Bei jeder Lottoziehung wird eine 6-elementige Teilmenge von $\{1, \dots, 49\}$ gezogen. Für die erste gezogene Kugel gibt es 49 Möglichkeiten, für die zweite noch 48, weil eine Kugel bereits entfernt wurde, und so fort bis zur sechsten Kugel, für deren Ziehung noch 44 Möglichkeiten bestehen. Insgesamt gibt es also $49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44$ mögliche Ziehungen. Aber es kommt nicht auf die Reihenfolge an, in der die Kugeln gezogen wurden.

¹⁹ Dies beweist man formal durch den Schritt von n auf $n+1$, auch *vollständige Induktion* genannt: Für $n=1$ steht links $a+b$; das ist offensichtlich die Summe aller ab -Sequenzen der Länge 1 (diese sind a und b). Wenn wir diese Aussage für ein beliebiges, aber festes n schon bewiesen haben (IV = “Induktionsvoraussetzung”; zum Beispiel für $n=1$ ist diese bereits erfüllt), dann können wir sie auch für die nächste Zahl $n+1$ (zum Beispiel für 2) folgern, denn

$$\begin{aligned}
(a+b)^{n+1} &= (a+b)^n(a+b) \\
&\stackrel{IV}{=} (\text{Summe aller } ab\text{-Sequenzen der Länge } n) \cdot (a+b) \\
&= (\text{Summe aller } ab\text{-Sequenzen der Länge } n) \cdot a \\
&\quad + (\text{Summe aller } ab\text{-Sequenzen der Länge } n) \cdot b \\
&= \text{Summe aller } ab\text{-Sequenzen der Länge } n+1,
\end{aligned}$$

denn jede ab -Sequenz der Länge $n+1$ endet mit a oder b und davor steht eine beliebige ab -Sequenz der Länge n .

Es gibt $6! = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$ mögliche Reihenfolgen für 6 Kugeln.²⁰ Die Anzahl der 6-elementigen Teilmengen von $\{1, \dots, 49\}$ ist daher

$$\binom{49}{6} = \frac{49 \cdot 48 \cdot 47 \cdot 46 \cdot 45 \cdot 44}{6!} = 49 \cdot 47 \cdot 46 \cdot 3 \cdot 44 \approx 14 \text{ Millionen.}$$

(Eine davon wird gezogen; die Wahrscheinlichkeit für einen Sechser im Lotto ist also ungefähr Eins zu 14 Millionen.) Die gleiche Überlegung gilt für die Anzahl der k -elementigen Teilmengen von $\{1, \dots, n\}$:

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot \dots \cdot (n-k+1)}{k!} = \frac{n!}{k!(n-k)!} \quad (2)$$

(der letzte Ausdruck ist die Erweiterung des Bruchs in der Mitte mit $(n-k)!$). Wir erhalten nunmehr die allgemeine binomische Formel

$$(a+b)^n = a^n + na^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \binom{n}{3}a^{n-3}b^3 + \dots + b^n.$$

Solche großen Summen schreibt man übersichtlicher mit dem *Summen-symbol*:

$$(a+b)^n = \sum_{k=0}^n \binom{n}{k} a^{n-k} b^k. \quad (3)$$

Diese Schreibweise bedeutet, dass man im Ausdruck $\binom{n}{k} a^{n-k} b^k$ für k nacheinander die Zahlen $0, 1, 2, \dots, n$ einsetzt, damit die Ausdrücke $\binom{n}{0} a^n b^0 = a^n$, $\binom{n}{1} a^{n-1} b^1 = na^{n-1}b$, $\binom{n}{2} a^{n-2} b^2 = \frac{n(n-1)}{2} a^{n-2} b^2$, \dots , $\binom{n}{n} a^0 b^n = b^n$ erhält und diese aufsummiert.

4. DIE TSCHIRNHAUS-TRANSFORMATION

Das Ziel der traditionellen Algebra war, eine Gleichung der Form

$$x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n = 0$$

zu lösen, mit anderen Worten, die Nullstellen des Polynoms

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n \quad (4)$$

zu finden. Eine Lösungsidee besteht darin, die Gleichung $f(x) = 0$ durch eine Variablentransformation $\tilde{x} = g(x)$ zu vereinfachen. Im einfachsten Fall ist $g(x) = x - a$ für eine Konstante a . Nach der binomischen Formel ist dann

$$\begin{aligned} x^n &= (\tilde{x} + a)^n \\ &= \tilde{x}^n + na\tilde{x}^{n-1} + \binom{n}{2}a^2\tilde{x}^{n-2} + \dots + a^n, \\ a_1 x^{n-1} &= a_1 (\tilde{x} + a)^{n-1} \end{aligned}$$

²⁰ $6!$ spricht man "6-Fakultät". Allgemein ist $k! = k \cdot (k-1) \cdot \dots \cdot 2 \cdot 1$ die Zahl der *Möglichkeiten* (lat. facultas), k Gegenstände anzuordnen, in eine Reihenfolge zu bringen: Für den ersten Gegenstand gibt es k mögliche Plätze, für den zweiten noch $k-1$ usw. Außerdem setzt man $0! = 1$ (leeres Produkt).

$$= \underline{a_1 \tilde{x}^{n-1}} + a_1(n-1)a\tilde{x}^{n-2} + a_1\binom{n-1}{2}a^2\tilde{x}^{n-3} + \dots$$

Wenn wir nun a so wählen, dass $na = -a_1$ gilt (also $a = -a_1/n$ setzen), heben sich die unterstrichenen Terme mit \tilde{x}^{n-1} gegenseitig weg und die verschobene Variable $\tilde{x} = x + \frac{a_1}{n}$ erfüllt eine Gleichung ohne \tilde{x}^{n-1} -Term,

$$\tilde{x}^n + \tilde{a}_2\tilde{x}^{n-2} + \dots + \tilde{a}_n = 0$$

für neue Konstanten $\tilde{a}_2, \dots, \tilde{a}_n$, z.B. $\tilde{a}_2 = a_2 - \frac{n-1}{2n} a_1^2$.

Wenn man dies auf eine quadratische Gleichung

$$x^2 + ax + b = 0$$

anwendet, also die Substitution²¹ $x = \tilde{x} - \frac{a}{2}$ vornimmt, dann lautet die transformierte Gleichung

$$0 = \left(\tilde{x} - \frac{a}{2}\right)^2 + a\left(\tilde{x} - \frac{a}{2}\right) + b = \tilde{x}^2 + \frac{a^2}{4} - \frac{a^2}{2} + b = \tilde{x}^2 - \frac{a^2}{4} + b$$

und wir gelangen zur "Mitternachtsformel" $x + \frac{a}{2} = \tilde{x} = \frac{1}{2}\sqrt{a^2 - 4b}$.

Mit komplizierteren Transformationen $\tilde{x} = g(x)$ lassen sich weitere Terme in der Gleichung $f(x) = 0$ beseitigen; für den \tilde{x}^{n-2} -Term braucht man z.B. eine quadratische Transformation $\tilde{x} = x^2 + ux + v$, siehe Seite 32, Beispiel 2. Dies wurde von *Tschirnhaus*²² beobachtet. Er glaubte, mit dieser Methode alle Polynomgleichungen lösen zu können, indem er sukzessive alle Terme beseitigte und mit einer reinen Wurzelgleichung $\tilde{x}^n + \tilde{a}_n = 0$ endete, wie im Fall der quadratischen Gleichung. Aber um die Koeffizienten des Polynoms g zu bestimmen, muss man bei den weiteren Termen bald Gleichungen lösen, die komplizierter sind als die Ausgangsgleichung!

5. DIE KUBISCHE GLEICHUNG

Das europäische Mittelalter war in mathematischer Hinsicht eine Zeit des Stillstandes. Mathematik fand anderswo statt, vor allem in der islamischen Welt, die das antike Erbe übernahm und fortführte und mit der indischen Mathematik verband. Die Algebra wuchs neben der Geometrie zu einem eigenständigen Zweig der Mathematik heran. Europa nahm diese Entwicklung erst im ausgehenden Mittelalter zur Kenntnis. Dann begann eine rege Übersetzungstätigkeit, besonders in Spanien und Süditalien, wo die beiden Kulturen in Kontakt standen. Auch viele der antiken Schriften wurden erst durch Rückübersetzung aus dem

²¹Wenn man es mit Gleichungen zu tun hat und die Variablen transformieren will, kann man dies in Form einer *Substitution* machen, bei der die alten Variablen x durch die neuen \tilde{x} ausgedrückt werden; dann kann man den entsprechenden Ausdruck von \tilde{x} direkt anstelle von x in die Gleichung einsetzen.

²²Ehrenfried Walther von Tschirnhaus, 1651 (bei Görlitz) - 1708 (Dresden)

Arabischen in Europa wieder zugänglich, was schließlich zur “Wiedergeburt” (*Renaissance*) der antiken Wissenschaft in Europa führte.

Der erste substantielle Beitrag der europäischen Mathematik zur Algebra war um 1520 die Lösung der *kubischen Gleichung*²³

$$x^3 + ax = b. \quad (5)$$

Man sieht zunächst nicht, wie diese Gleichung gelöst werden kann. Aber es gibt andere kubische Gleichungen, deren Lösung auf der Hand liegt: Die Gleichung

$$(x + u)^3 = v^3 \quad (6)$$

hat offensichtlich die Lösung

$$x = v - u. \quad (7)$$

Die Idee ist nun, die einfache Gleichung (6) auf die Form der schwierigen (5) zu bringen: Es gilt

$$(x + u)^3 = x^3 + 3x^2u + 3xu^2 + u^3 = x^3 + 3xu(x + u) + u^3,$$

und weil wir $x + u$ gemäß (7) durch v ersetzen können (das ist der Trick), verwandelt sich (6) in die Gleichung

$$x^3 + 3uvx = v^3 - u^3. \quad (8)$$

Diese Gleichung ist tatsächlich von der Form (5) mit

$$a = 3uv, \quad b = v^3 - u^3. \quad (9)$$

Wenn also die Koeffizienten a, b der “schwierigen” Gleichung (5) die Form (9) haben, dann ist $x = v - u$ eine Lösung. Um solche u und v zu finden, müssen wir die Gleichungen (9) nach u und v auflösen:

$$u = a/(3v), \quad v^3 = b + u^3 = b + a^3/(3v)^3.$$

Multiplizieren wir die letzte Gleichung noch einmal mit v^3 , so erhalten wir eine quadratische Gleichung für v^3 , nämlich $v^6 = bv^3 + (\frac{a}{3})^3$. Quadratische Gleichungen können wir lösen: $v^3 = \frac{b}{2} \pm \sqrt{D}$ mit $D := (\frac{a}{3})^3 + (\frac{b}{2})^2$, und folglich $-u^3 = b - v^3 = \frac{b}{2} \mp \sqrt{D}$. Als Lösung $x = v - u$ erhalten wir daher

$$x = \sqrt[3]{b/2 + \sqrt{D}} + \sqrt[3]{b/2 - \sqrt{D}}, \quad D = (a/3)^3 + (b/2)^2. \quad (10)$$

Diese Formel wurde um 1520 von del Ferro²⁴ entdeckt, der sie aber nur an einen seiner Schüler weitergab. Davon erfuhr Tartaglia²⁵ und

²³Die allgemeinste kubische Gleichung ist $x^3 + ax^2 + bx = c$. Sie lässt sich aber durch die einfachste Tschirnhaus-Transformation auf die Form (5) bringen, wie im vorigen Abschnitt 4 gezeigt.

²⁴Scipione del Ferro, 1465 - 1526, Bologna

²⁵Nicolo Tartaglia, 1499 - 1557, Brescia, Venedig

fand die Formel 1535 selbst. Er gab sie 1539 an seinen Freund Cardano²⁶ weiter, der sie 1545 in seinem Buch “Ars Magna” veröffentlichte;²⁷ seither heißt sie *Cardanosche Formel*. Danach waren Cardano und Tartaglia nicht mehr so gut befreundet.

Beispiel 1: $x^3 - 6x = 9$. Dann ist

$$\frac{a}{3} = -2, \quad \frac{b}{2} = \frac{9}{2}, \quad D = -8 + \frac{81}{4} = \frac{81 - 32}{4} = \frac{49}{4}.$$

Damit ist $\sqrt{D} = \frac{7}{2}$ und $\frac{b}{2} + \sqrt{D} = \frac{9+7}{2} = 8$ und $\frac{b}{2} - \sqrt{D} = \frac{9-7}{2} = 1$, also $x = \sqrt[3]{8} + \sqrt[3]{1} = 2 + 1 = 3$. Probe: $3^3 - 6 \cdot 3 = 27 - 18 = 9$.

Beispiel 2: $x^3 - 6x = 4$. Dann ist

$$\frac{a}{3} = -2, \quad \frac{b}{2} = 2, \quad D = -8 + 4 = -4.$$

Jetzt haben wir ein Problem: Weil D negativ ist, können wir die Quadratwurzel \sqrt{D} nicht ziehen! Die Lösungsmethode scheint zu versagen. Cardano wusste keinen Rat und gab diesem Fall den Namen *Casus irreducibilis* (unlösbarer Fall). Das war eigentlich ein Skandal, denn das Polynom $f(x) = x^3 - 6x - 4$ hat mit Sicherheit Nullstellen, weil $f(0) = -4$ und $f(3) = 27 - 18 - 4 = 5$; die Werte von f steigen also zwischen $x_0 = 0$ und $x_1 = 3$ von $f(x_0) = -4$ auf $f(x_1) = 5$ und müssen irgendwo dazwischen die Null treffen.²⁸ Man muss im vorliegenden Fall auch nicht lange danach suchen: $x = -2$ ist eine Nullstelle, denn $f(-2) = -8 + 12 - 4 = 0$. Aber Cardano wusste nicht, wie man diese Lösung mit seiner Formel finden sollte.

6. DIE IMAGINÄREN ZAHLEN

Gut 20 Jahre nach Cardanos “Ars Magna” unternahm ein Ingenieur namens Bombelli²⁹ einen neuen Anlauf und war erfolgreich. Wir erklären seine Methode am Beispiel 2 des vorigen Abschnittes. Bombelli wusste, dass negative Zahlen wie -4 keine Quadratwurzel haben, denn das Quadrat negativer wie positiver Zahlen ist positiv, Minus mal Minus ergibt Plus.³⁰ Aber wir können einmal so tun, als gäbe es solche

²⁶Girolamo Cardano, 1501 - 1576, Mailand, Pavia

²⁷Anlass war die Lösung der *quartischen Gleichung* durch Cardanos Schüler Lodovico Ferrari (Bologna 1522 - 1565), wobei die Lösung der kubischen Gleichung verwendet wurde.

²⁸Der *Zwischenwertsatz* der Analysis berechnet diese Nullstelle sogar.

²⁹Rafaele Bombelli, 1526 - 1572, Bologna

³⁰Auch diese Erkenntnisse waren noch nicht so alt. Erst seit Kurzem hatte man gelernt, mit negativen Zahlen zu rechnen. Ursache hierfür war das besonders in Oberitalien aufkommende Banken- und Kreditwesen. Damit erst hatte man

Zahlen doch (sie wurden später “*imaginäre*” Zahlen genannt, Zahlen, die nur in der Vorstellung existieren) und damit wie gewohnt rechnen. Eigentlich genügt sogar eine einzige “*imaginäre*” Zahl, nämlich $i := \sqrt{-1}$; denn dann wäre $i^2 = -1$ und damit $(2i)^2 = 4i^2 = -4$, also $\sqrt{-4} = 2i$. Die Lösung gemäß Cardanos Formel (10) ist demnach

$$x = \sqrt[3]{2+2i} + \sqrt[3]{2-2i}. \quad (11)$$

Doch was sollen wir mit einem solchen Ergebnis anfangen? Wie sollen wir die 3. Wurzel aus $2+2i$ ziehen? Das wusste auch Bombelli nicht.³¹ Aber die Umkehrung, die 3. Potenz solcher Zahlen konnte er immerhin berechnen, zum Beispiel:

$$\begin{aligned} (-1+i)^3 &= -1 + 3i - 3i^2 + i^3 \\ &= -1 + 3i + 3 - i \\ &= -1 + 3 + (3-1)i \\ &= 2 + 2i \end{aligned}$$

und ebenso $(-1-i)^3 = 2-2i$. Das ist ein Glücksfall für unser Beispiel: Die dritte Potenz ergibt genau die Zahlen, deren dritte Wurzel wir suchen; diese sind also *Kubikzahlen*, dritte Potenzen bekannter Zahlen, wie auch 1 und 8 in Beispiel 1. Also ist $\sqrt[3]{2 \pm 2i} = -1 \pm i$ und aus (11) erhalten wir

$$x = (-1+i) + (-1-i) = -2.$$

Wie durch Zauberei sind die “*imaginären*” Wurzeln negativer Zahlen verschwunden und wir erhalten die uns schon bekannte Lösung $x = -2$.

Bombelli veröffentlichte seine Ergebnisse 1572 in seinem Algebra-Lehrbuch. Eine Sternstunde der Mathematik: Er hatte es gewagt, die Grenzen der bisherigen Vorstellung (“*Quadratwurzeln negativer Zahlen gibt es nicht*”) zu verlassen, und gelangte damit zu richtigen Ergebnissen! Er hatte eine weitere Zahlbereichserweiterung gewagt. Es dauerte mehr als zwei Jahrhunderte, bis die “*imaginären Zahlen*” ihrer Mystik ganz entkleidet und voll akzeptiert waren. Summen von reellen und imaginären Zahlen, wie sie bei den Rechnungen aufgetreten sind, nennt man *komplexe* (= “*zusammengesetzte*”) Zahlen.

Man muss sich bei den komplexen Zahlen allerdings von einigen gewohnten Vorstellungen trennen. Zum Beispiel stimmt es nicht mehr, dass eine Größe sich durch Hinzufügen (Addition) einer anderen vermehrt, aber das war ja schon bei den negativen Zahlen nicht mehr wahr. Dieses Phänomen wurde unter dem Namen *Interferenz* zu einer

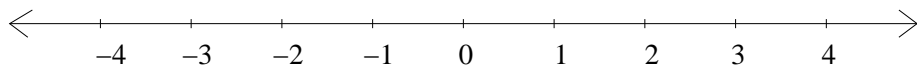
die reellen Zahlen vervollständigt und war vom Zahlenstrahl zur Zahlengeraden übergegangen.

³¹Man vergleiche aber S. 23.

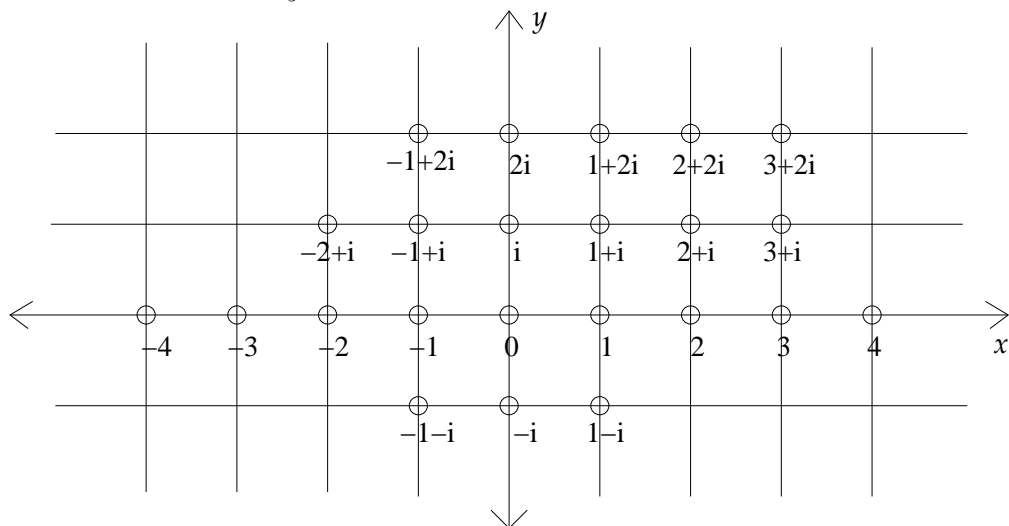
Grundtatsache der Physik des 20. Jahrhunderts, aus der die komplexen Zahlen deshalb nicht mehr wegzudenken sind.³²

Außerdem muss man sich eine neue geometrische Vorstellung von den Zahlen machen: Zahlenstrahl und Zahlengerade werden durch die *Zahlenebene* abgelöst. Diesen Schritt hat erst *C.F. Gauß* um 1800 vollzogen.

7. DIE KOMPLEXE ZAHLENEBENE



Wo könnten wir die neue Zahl $i = \sqrt{-1}$ auf unserer Zahlengeraden unterbringen? Nicht rechts von der Null, denn dort sind die positiven Zahlen, deren Quadrat ja wieder positiv ist, also nicht -1 . Auch nicht links davon, denn das Quadrat negativer Zahlen ist ebenfalls positiv (Minus mal Minus = Plus). Die Null selbst ist es auch nicht, denn ihr Quadrat ist Null, nicht -1 . Auf der Zahlengeraden ist einfach kein Platz für diese Zahl; sie wird also *daneben* untergebracht werden müssen, und damit kommen wir in die zweite Dimension, in die *Ebene*. Mit der Zahl i haben wir uns allerdings noch viele weitere Zahlen "eingehandelt": die Vielfachen von i und deren Summen mit den gewöhnlichen reellen Zahlen. In der Ebene finden sie alle ihren Platz: Der Zahl $x + yi$ (für reelle Zahlen x, y) werden wir den Punkt (x, y) mit den kartesischen Koordinaten x und y zuweisen.



³²www.quantenphysik-schule.de, www.didaktik.physik.uni-erlangen.de

Alle diese Zahlen zusammen bilden die Menge der *komplexen Zahlen*, die mit dem Symbol \mathbb{C} bezeichnet wird:

$$\mathbb{C} = \{x + yi : x, y \in \mathbb{R}\}$$

Die Rechenoperationen haben wir schon gesehen; sie ergeben sich aus den (weiterhin gültigen) Rechenregeln zusammen mit der Gleichung, die i definiert, $i \cdot i = -1$:

$$(x + yi) \pm (u + vi) = (x \pm u) + (y \pm v)i, \quad (12)$$

$$(x + yi)(u + vi) = (xu - yv) + (xv + yu)i, \quad (13)$$

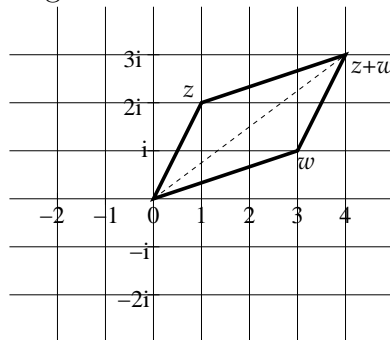
$$\frac{1}{x + yi} = \frac{x - yi}{x^2 + y^2} = \frac{x}{x^2 + y^2} + \frac{-y}{x^2 + y^2}i \quad (14)$$

durch Erweitern mit $x - iy$, denn $(x + yi)(x - yi) = x^2 + y^2$. Diese Gleichungen zeigen, dass auch für die *komplexen Zahlen* die vier Grundrechenarten erklärt und die üblichen Rechenregeln erfüllt sind. Einen solchen Zahlbereich nennen wir einen *Körper*. Wir haben damit bereits drei verschiedene Körper kennengelernt: die rationalen Zahlen \mathbb{Q} , die reellen Zahlen \mathbb{R} und die komplexen Zahlen \mathbb{C} . Auch die “rationalen komplexen Zahlen” $\mathbb{Q} + \mathbb{Q}i$ bilden einen Körper. Wir werden noch viele weitere kennenlernen.

Wir wollen für komplexe Zahlen eigene Namen einführen, z.B. z und w (später werden x auch für komplexe Variable verwenden). Für $z = x + yi$ nennen wir x den *Realteil* und y den *Imaginärteil* und schreiben

$$x = \operatorname{Re} z, \quad y = \operatorname{Im} z.$$

Wir können nun die *Addition* bei komplexen Zahlen geometrisch ebenso wie bei reellen Zahlen deuten, nämlich als Aneinanderlegen von zwei Stäben, die jetzt allerdings unterschiedliche Richtungen haben können.



Die Operation $x + yi \mapsto x - yi$ (Spiegelung an der x -Achse) nennen wir *komplexe Konjugation* und bezeichnen sie mit einem Querstrich:

$$z = x + yi \mapsto \bar{z} = x - yi.$$

Sie wurde eingeführt wegen ihrer guten Recheneigenschaften:³³

$$\overline{z \pm w} = \bar{z} \pm \bar{w}, \quad \overline{z \cdot w} = \bar{z} \cdot \bar{w}, \quad \overline{z/w} = \bar{z}/\bar{w}. \quad (15)$$

Auch bei komplexen Zahlen $z = x + yi$ gibt es einen *Absolutbetrag*

$$|z| = \sqrt{x^2 + y^2} = \sqrt{z\bar{z}}. \quad (16)$$

Nach Pythagoras³⁴ ist $|z|$ die Länge der Strecke von 0 nach z in der xy -Ebene. Der Betrag einer komplexen Zahl ist eine positive reelle Zahl (nur für $z = 0$ ist $|z| = 0$) und erfüllt dieselben Rechenregeln wie der Betrag einer reellen Zahl:

Satz 7.1.

$$|z + w| \leq |z| + |w| \quad (17)$$

$$|z| \cdot |w| = |zw|. \quad (18)$$

Beweis. Die zweite Gleichung (18) ist die einfachere: $|z|^2|w|^2 = z\bar{z}w\bar{w} = zw\bar{z}\bar{w} = zw\overline{z\bar{w}} = |zw|^2$ mit (15). Die erste Gleichung (17) folgt, weil $\operatorname{Re} z \leq |z|$ für jede komplexe Zahl z , da

$$|z| = \sqrt{x^2 + y^2} \geq \sqrt{x^2} = |x| \geq x = \operatorname{Re} z,$$

und insbesondere

$$(*) \quad \operatorname{Re}(z\bar{w}) \leq |z\bar{w}| = |z||\bar{w}| = |z||w|.$$

Andererseits ist³⁵

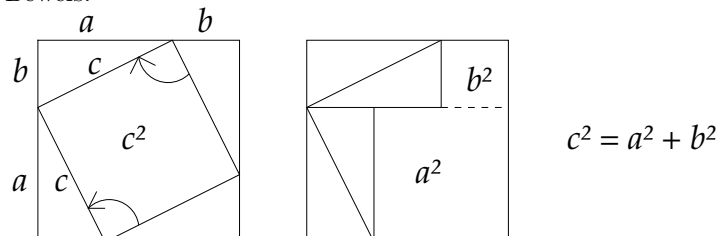
$$(**) \quad 2 \operatorname{Re}(z\bar{w}) = z\bar{w} + \overline{z\bar{w}} = z\bar{w} + \bar{z}w,$$

denn für $w = u + vi$ ist $\bar{w} = \overline{u - vi} = u + vi = w$. Daher gilt:

$$\begin{aligned} |z + w|^2 &= (z + w)(\bar{z} + \bar{w}) \\ &= z\bar{z} + z\bar{w} + w\bar{z} + w\bar{w} \\ &\stackrel{(**)}{=} |z|^2 + 2 \operatorname{Re}(z\bar{w}) + |w|^2 \end{aligned}$$

³³Eine solche Selbstabbildung des Körpers, die mit allen vier Grundrechenarten vertauscht, nennen wir einen *Körperautomorphismus*, ein wichtiger Begriff der Algebra, der mit Körpererweiterungen verbunden ist, in diesem Fall mit der Erweiterung von \mathbb{R} zu \mathbb{C} .

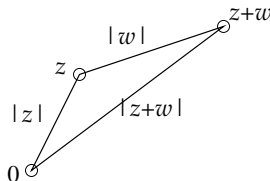
³⁴Indischer Beweis:



³⁵Für jedes $z \in \mathbb{C}$ gilt $\operatorname{Re} z = \frac{1}{2}(z + \bar{z})$ und $\operatorname{Im} z = \frac{1}{2i}(z - \bar{z})$

$$\begin{aligned}
& \stackrel{(*)}{\leq} |z|^2 + 2|z||w| + |w|^2 \\
& = (|z| + |w|)^2. \quad \square
\end{aligned}$$

Gleichung (17) heißt *Dreiecksungleichung*, denn sie sagt, dass im Dreieck $\Delta(0, z, z + w)$ eine Seite kürzer ist als die beiden anderen zusammen; der direkte Weg von 0 nach $z + w$ ist kürzer als der Umweg über z .



8. DIE EXPONENTIALFUNKTION

Die *Exponentialfunktion* ist die wohl wichtigste Funktion der Mathematik, denn sie verbindet die zwei Grundrechenarten Addition und Multiplikation miteinander. Sie ist folgendermaßen definiert:

$$\exp(x) = 1 + x + \frac{x^2}{2} + \cdots + \frac{x^k}{k!} + \cdots = \sum_{k=0}^{\infty} \frac{x^k}{k!} \quad (19)$$

Dass hier “unendlich viele” Terme summiert werden, soll uns nicht stören; für große Zahlen k ist der Summand $\frac{x^k}{k!}$ betragsmäßig winzig klein³⁶ und spielt für die Summation keine wesentliche Rolle mehr; dies wird in der Analysis genau untersucht.³⁷

Satz 8.1. Für alle $x, y \in \mathbb{C}$ gilt

$$\exp(x) \exp(y) = \exp(x + y). \quad (20)$$

³⁶ $\left| \frac{x^k}{k!} \right| = \left| \frac{x}{1} \cdot \frac{x}{2} \cdot \cdots \cdot \frac{x}{k} \right| = \frac{|x|}{1} \cdot \frac{|x|}{2} \cdot \cdots \cdot \frac{|x|}{k}$, wobei $\frac{|x|}{j} < \frac{1}{2}$ für große j , sobald nämlich $j > 2|x|$. Bis auf einen konstanten Faktor ist $\left| \frac{x^k}{k!} \right|$ also kleiner als eine Potenz von $\frac{1}{2}$, und deren Summen werden niemals größer als Eins: $\frac{1}{2} + \frac{1}{4} = \frac{3}{4}$, $\frac{1}{2} + \frac{1}{4} + \frac{1}{8} = \frac{7}{8}$ usw.

³⁷Wer eine schnelle Erklärung sucht, warum die Exponentialfunktion gerade so definiert ist, der leite sie einmal ab. Die Ableitung von $\frac{x^k}{k!}$ ist $\frac{kx^{k-1}}{k!} = \frac{x^{k-1}}{(k-1)!}$. In der Ableitung $\exp'(x)$ treten daher exakt dieselben Terme auf wie in $\exp(x)$, es gilt also $\exp' = \exp$. Die Exponentialfunktion ist gleich ihrer Ableitung und beschreibt daher Prozesse, bei denen der jeweilige Zuwachs (die Ableitung) gleich (oder proportional) zum jeweiligen Bestand ist. Das sind natürliche Wachstums- und Zerfallsprozesse: Was neu hinzukommt, trägt sofort zur weiteren Vermehrung bei.

Beweis. Nach der Binomischen Formel (3) und (2) ist

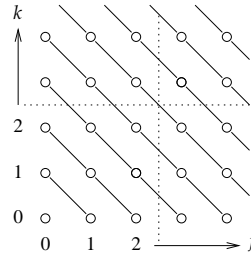
$$\frac{1}{m!}(x+y)^m \stackrel{(2)}{=} \sum_{j=0}^m \frac{1}{m!} \binom{m}{j} x^j y^{m-j} = \sum_{j=0}^m \frac{1}{j!(m-j)!} x^j y^{m-j}$$

und damit

$$\exp(x+y) = \sum_{m=0}^{\infty} \sum_{j=0}^m \frac{x^j y^{m-j}}{j!(m-j)!}. \quad (21)$$

Andererseits gilt aber auch

$$\exp(x)\exp(y) = \sum_{j=0}^{\infty} \sum_{k=0}^{\infty} \frac{x^j y^k}{j! k!} \stackrel{(*)}{=} \sum_{m=0}^{\infty} \sum_{j=0}^m \frac{x^j y^{m-j}}{j!(m-j)!}.$$



Bei (*) wurden die Summanden der Doppelsumme umgeordnet: Statt über j und k wurde über j und $m := j + k$ summiert und k durch $m - j$ ersetzt.³⁸ \square

Die Zahl $\exp(1) = \sum_{k=0}^{\infty} \frac{1}{k!} \approx 2,718$ wird zu Ehren von Euler³⁹ mit dem Buchstaben e bezeichnet. Nach (20) folgt dann

$$\exp(2) = \exp(1+1) = \exp(1)\exp(1) = e^2$$

und $\exp(n) = e^n$ für alle $n \in \mathbb{N}$ (vollständige Induktion), außerdem

$$\exp(-1) \cdot e = \exp(-1)\exp(1) = \exp(0) = 1$$

und damit $\exp(-1) = 1/e = e^{-1}$, und schließlich

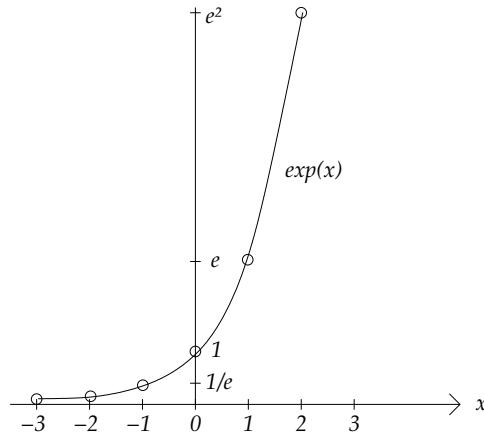
$$\exp(1/2) = \sqrt{e} = e^{1/2},$$

denn $\exp(\frac{1}{2})^2 = \exp(\frac{1}{2})\exp(\frac{1}{2}) = \exp(\frac{1}{2} + \frac{1}{2}) = \exp(1) = e$. So sehen wir $\exp(x) = e^x$ für alle rationalen Zahlen x . Deshalb schreiben wir für beliebige (reelle und sogar komplexe) Zahlen x nun auch $\exp(x) = e^x$, obwohl z.B. $e^{\sqrt{2}}$ oder gar e^i als Potenzen gar keinen Sinn machen (man kann e nicht i -mal mit sich selbst multiplizieren!); erst mit der Exponentialfunktion haben wir diesem Ausdruck einen Sinn gegeben und damit den Begriff der *Potenz* erweitert. Hier ist der bekannte nach

³⁸Die unendlichen Summen werfen Fragen der Konvergenz auf, die in diesem Fall harmlos sind und die wir der Analysis überlassen ("Cauchy-Produkt-Formel").

³⁹Leonhard Euler, 1707 (Basel) - 1783 (St. Petersburg)

rechts sehr steil ansteigende und nach links sich sehr schnell der x -Achse annähernde Graph der reellen e -Funktion: Alle Summanden $\frac{x^k}{k!}$ mit $x > 0$ sind positiv und streben für $x \rightarrow \infty$ monoton gegen ∞ , was den rechten Teil des Graphen erklärt, und weil e^{-x} der Kehrwert von e^x ist ($e^{-x}e^x = e^{x-x} = e^0 = 1$), ist der linke Teil des Graphen ebenfalls positiv und schmiegt sich an die x -Achse an.



Was aber passiert, wenn wir für x *imaginäre* Werte $x = it$, $t \in \mathbb{R}$ einsetzen? Das Ergebnis ist überraschend: Die Werte der Funktion $t \mapsto e^{it}$ wachsen in keiner Richtung, sondern behalten für alle t den Betrag Eins. Dazu müssen wir $|e^{it}|^2 = e^{it} \cdot \overline{e^{it}}$ berechnen. Für die *komplexe Konjugation* gilt⁴⁰

$$\overline{e^z} = \overline{\sum_k z^k/k!} = \sum_k \overline{z^k}/k! = e^{\overline{z}}$$

für alle $z \in \mathbb{C}$. Speziell für $z = it$ mit $t \in \mathbb{R}$ ist $\overline{z} = -it$, also $\overline{e^{it}} = e^{-it} = e^{-it}$ und damit

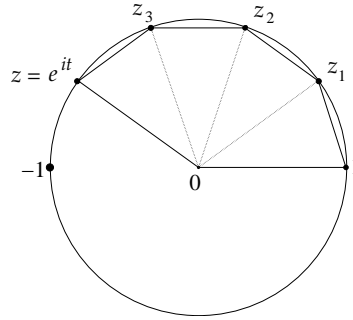
$$|e^{it}|^2 = e^{it} \cdot \overline{e^{it}} = e^{it} e^{-it} = e^{it-it} = e^0 = 1. \quad (22)$$

Die komplexe Zahl e^{it} liegt also für alle $t \in \mathbb{R}$ auf der Einheitskreislinie!

Welche geometrische Bedeutung hat dabei die Zahl t ? Sie ist der Winkel zwischen 1 und e^{it} , im Bogenmaß gemessen, d.h. $|t|$ ist die Länge des Kreisbogens zwischen den beiden Punkten 1 und e^{it} , und das Vorzeichen von t ist positiv, wenn der Kreis nach links, d.h. gegen den Uhrzeigersinn durchlaufen wird, und in der anderen Richtung ist t negativ.

⁴⁰Dabei benötigen wir neben den algebraischen Eigenschaften $\overline{z+w} = \overline{z} + \overline{w}$ und $\overline{z \cdot w} = \overline{z} \cdot \overline{w}$ beim Grenzübergang von der endlichen zur unendlichen Summe auch die Stetigkeit der komplexen Konjugation: Wenn $|z_n - z| \rightarrow 0$, dann $|\overline{z_n} - \overline{z}| = |\overline{z_n - z}| = |z_n - z| \rightarrow 0$.

Wie können wir uns davon überzeugen? Wir müssen zunächst die Länge des Kreisbogens zwischen $z_0 = 1$ und $z = e^{it}$ definieren. Dazu unterteilen wir den Bogen durch eine große Anzahl n von Zwischenpunkten $z_k = e^{ikt/n}$ mit $k = 0, \dots, n$.



Die Länge s dieses Kreisbogens wird von unten angenähert durch die Summe der Abstände zwischen benachbarten Unterteilungspunkten, nämlich

$$s_n = |z_0 - z_1| + |z_1 - z_2| + \dots + |z_{n-1} - z_n| = \sum_{k=1}^n |z_{k-1} - z_k|. \quad (23)$$

Wenn wir die Unterteilungspunkte immer dichter wählen, also $n \rightarrow \infty$ streben lassen, dann konvergiert s_n gegen die Länge s des Kreisbogens.

Den Ausdruck s_n können wir explizit berechnen:⁴¹ Da $z_k = e^{k \cdot it/n} = (e^{it/n})^k$ für alle k , folgt

$$\begin{aligned} z_{k-1} - z_k &= e^{i(k-1)t/n} - e^{ikt/n} \\ &= e^{i(k-1)t/n} (1 - e^{it/n}), \\ |z_{k-1} - z_k| &= \underbrace{|e^{i(k-1)t/n}|}_{=1} \cdot |1 - e^{it/n}| = |1 - e^{it/n}|. \end{aligned}$$

Damit sind alle Summanden auf der rechten Seite von (23) gleich und

$$s_n = n \cdot |1 - e^{it/n}| = |it| \cdot \left| \frac{1 - e^{it/n}}{it/n} \right| = |t| \cdot |f(it/n)|$$

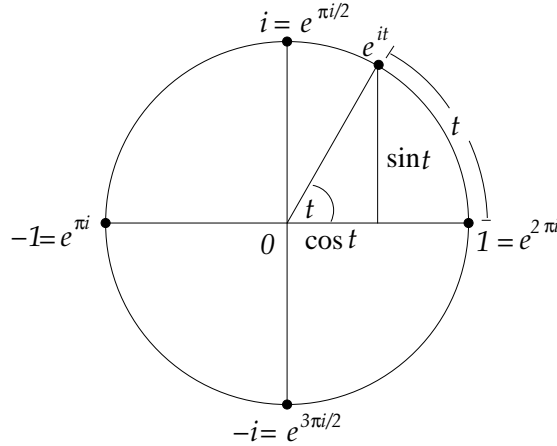
mit

$$f(z) := \frac{e^z - 1}{z} = \frac{1}{z} \left(z + \frac{1}{2!} z^2 + \frac{1}{3!} z^3 + \dots \right) = 1 + \frac{1}{2!} z + \frac{1}{3!} z^2 + \dots$$

Dies ist eine (stetige) Funktion, die bei $z = 0$ den Wert $f(0) = 1$ hat. Da it/n für $n \rightarrow \infty$ gegen 0 strebt (da $1/n \rightarrow 0$), folgt $f(it/n) \rightarrow f(0) = 1$

⁴¹Man beachte $e^{kz} = e^{z+\dots+z} = e^z \cdot \dots \cdot e^z = (e^z)^k$ für alle $z \in \mathbb{C}$ (genaueres Argument mit Induktion über k).

und wir erhalten $s_n \rightarrow |t|$. Somit ist $|t|$ die Länge des Bogens und damit gleich dem Winkel, in Bogenmaß gemessen: $t = \angle(1, 0, e^{it})$.



An dieser Stelle kommt die Kreiszahl π ins Spiel; 2π ist nach Definition die Gesamtlänge der Einheitskreislinie, die Länge des Halbkreisbogens zwischen 1 und -1 ist π . Daraus ergeben sich die bemerkenswerten Beziehungen

$$e^{2\pi i} = 1, \quad e^{\pi i} = -1, \quad e^{i(t+2\pi)} = e^{it} e^{2\pi i} = e^{it}, \quad e^{it} = \cos t + i \sin t$$

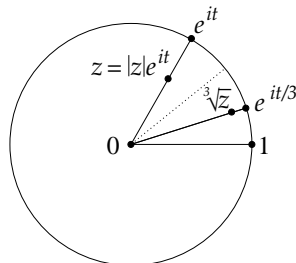
Nun können wir auch die komplexe *Multiplikation* geometrisch interpretieren: Wenn wir zwei komplexe Zahlen $z = e^{it}$ und $w = e^{is}$ auf der Einheitskreislinie miteinander multiplizieren, so addieren sich die beiden Winkel t und s :

$$z \cdot w = e^{it} \cdot e^{is} = e^{i(s+t)}.$$

Wenn die Zahlen z und w dagegen beliebigen positiven Abstand $|z|$ und $|w|$ vom Nullpunkt haben, so liegen jedenfalls $z/|z|$ und $w/|w|$ auf der Einheitskreislinie und lassen sich demnach in der Form e^{it} und e^{is} darstellen, also gilt

$$z \cdot w = |z|e^{it} \cdot |w|e^{is} = |z||w|e^{i(s+t)}.$$

Die Beträge werden multipliziert, die Winkel addiert.



Eine Folgerung ist, dass wir jetzt aus einer beliebigen komplexen Zahl z die n -te Wurzel ziehen können, für jedes n : Für $z = |z|e^{it}$ ist $w := \sqrt[n]{|z|} \cdot e^{it/n}$ eine n -te Wurzel von z , denn $w^n = |z| \cdot e^{it} = z$. Es gibt aber noch weitere n -te Wurzeln, insgesamt n , nämlich $w_k = \sqrt[n]{|z|} \cdot e^{i(t+2\pi k)/n}$ für $k = 0, \dots, n-1$, denn $w_k = w\zeta$ mit $\zeta = e^{2\pi ik/n}$; diese Zahlen erfüllen $\zeta^n = 1$; sie heißen deshalb n -te *Einheitswurzeln*, und es gilt $w_k^n = w^n \zeta^n = w^n$.

9. DER "FUNDAMENTALSATZ DER ALGEBRA"

Die komplexen Zahlen wurden eingeführt, um Quadratwurzeln aus negativen Zahlen ziehen zu können, die bei der Lösungsformel kubischer Gleichungen als Hilfsgrößen auftraten; damit konnte man gewöhnliche (reelle) Lösungen kubischer Gleichungen berechnen. Jetzt haben wir gesehen, dass man in \mathbb{C} nicht nur Quadratwurzeln, sondern überhaupt alle Wurzeln beliebigen Grades ziehen kann. Gauß ging noch einen Schritt weiter und zeigte, dass in \mathbb{C} überhaupt jede Polynomgleichung $f(x) = 0$ eine Lösung hat. Das ist der sogenannte *Fundamentalsatz der Algebra*.

Satz 9.1. *Für jedes (normierte)⁴² Polynom*

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n = x^n \left(1 + \frac{a_1}{x} + \dots + \frac{a_n}{x^n} \right) \quad (24)$$

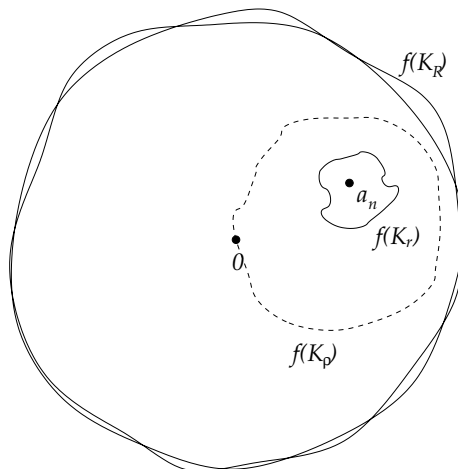
mit $n \in \mathbb{N} = \{1, 2, 3, \dots\}$ und $a_1, \dots, a_n \in \mathbb{C}$ gibt es ein $x \in \mathbb{C}$ mit $f(x) = 0$.

Gauß selbst hat u.a. folgendes einfache Argument gegeben. Für jedes $\rho > 0$ betrachten wir die Kreislinie

$$K_\rho = \{x \in \mathbb{C} : |x| = \rho\} = \{\rho e^{it} : t \in [0, 2\pi]\}$$

und deren Bild $f(K_\rho)$. Ist $\rho = r$ sehr klein, dann liegt $f(K_\rho)$ ganz nahe bei $f(0) = a_n$. Wenn $a_n \neq 0$ (andernfalls ist $f(0) = 0$ und wir haben eine Nullstelle), wird die Null von $f(K_\rho)$ nicht umlaufen. Ist dagegen $\rho = R$ sehr groß, so ist $f(Re^{it}) = R^n \left(e^{int} + \frac{a_1}{R} e^{i(n-1)t} + \dots + \frac{a_n}{R^n} \right) \approx R^n e^{int}$, und das Bild der Kreislinie $f(K_\rho)$ umläuft die Null n -mal. Zwischen $\rho = r$ und $\rho = R$ muss sich die Null-Umlaufszahl von $f(K_\rho)$ also ändern. Das kann nur geschehen, wenn die Null überstrichen wird, wenn also ein $f(K_\rho)$ die Null enthält. Auf der Kreislinie K_ρ muss demnach eine Nullstelle von f liegen.

⁴²Ein Polynom heißt *normiert*, wenn der höchste Koeffizient Eins ist.



Das Argument von Gauß in der hier gegebenen Form benutzt das Konzept der *Umlaufszahl* der geschlossenen Linie (“Kurve”) $f(K_\rho)$: Man ermittelt den zurückgelegten Gesamtwinkel bei einem vollständigen Durchlauf der Kurve. Weil Anfangs- und Endposition die gleichen sind, muss der Gesamtwinkel ein ganzes Vielfaches von $2\pi = 360^\circ$ sein; dieses Vielfache nennt man die Umlaufszahl. Bei stetiger Deformation der Kurve kann sich diese Zahl nicht ändern, es sei denn, dass die Kurvenschar die Null überquert.

Ein anderes Argument, das dieses Konzept nicht benötigt, stammt von Argand,⁴³ einem Zeitgenossen von Gauß. Zu dem durch (24) gegebenen Polynom f betrachten wir die Funktion $|f| : \mathbb{C} \rightarrow \mathbb{R}_+$. Mit (24) sehen wir, dass $|f(x)|$ groß wird, sobald $|x|$ genügend groß ist, sagen wir $|x| > R$. Damit muss $|f|$ irgendwo an einem Punkt x_1 (mit $|x_1| \leq R$) ein Minimum annehmen.⁴⁴ Wenn $|f(x_1)| = 0$, ist x_1 eine Nullstelle. Den Gegenfall $|f(x_1)| > 0$ werden wir zum Widerspruch führen. Durch Verschieben des Arguments (Substitution $x = \tilde{x} + x_1$) dürfen wir $x_1 = 0$ annehmen; dann ist $f(0) = a_n$ und nach unserer Annahme ist $a_n \neq 0$.

Wir schreiben f in der Form $f(x) = x^n + \dots + a_{n-k}x^k + a_n$ für ein $k \in \{1, \dots, n\}$, wobei die letzten beiden nicht-verschwindenden Terme explizit aufgeführt sind. Wir approximieren nun f durch diese letzten beiden Terme, also durch $g(x) = a_{n-k}x^k + a_n$. Der Fehler ist

$$|f(x) - g(x)| \leq |x|^n + |a_1||x|^{n-1} + \dots + |a_{n-k-1}||x|^{k+1}.$$

⁴³Jean Robert Argand, 1768 (Genf) - 1822 (Paris)

⁴⁴In der Analysis lernen wir, dass die stetige Funktion $|f|$ auf dem Kreis $D_R = \{x \in \mathbb{C} : |x| \leq R\}$ ein Minimum annimmt; außerhalb von D_R dagegen ist $|f|$ groß.

Statt einer Nullstelle von f suchen wir nun eine Nullstelle x_o von g , was einfach ist: x_o ist eine k -te Wurzel von $-a_n/a_{n-k}$,

$$x_o^k = -a_n/a_{n-k}.$$

Für $0 < t < 1$ ist $|g(tx_o)| < |a_n|$, genauer

$$g(tx_o) = a_{n-k}t^k x_o^k + a_n = a_n(1 - t^k).$$

Andererseits ist $|f(tx_o) - g(tx_o)|$ klein von Ordnung $k + 1$:

$$\begin{aligned} |f(tx_o) - g(tx_o)| &\leq t^n |x_o^n| + \dots + t^{k+1} |a_{n-k-1} x_o^{k+1}| \\ &\leq C t^{k+1} \end{aligned}$$

mit $C := |x_o^n| + \dots + |a_{n-k-1} x_o^{k+1}|$. Damit ist auch $|f(tx_o)| < |a_n|$ für kleine positive t :

$$\begin{aligned} |f(tx_o)| &\leq |g(tx_o)| + |f(tx_o) - g(tx_o)| \\ &\leq |a_n|(1 - t^k) + C t^{k+1} \\ &= |a_n|(1 - t^k(1 - (C/|a_n|)t)) \\ &< |a_n| \end{aligned}$$

falls $(C/|a_n|)t < 1$, also $t < |a_n|/C$. Der Minimalwert von $|f|$ war $|a_n|$, aber jetzt haben wir einen Wert von $|f|$ gefunden, der noch kleiner ist: ein Widerspruch!

10. ALLE NULLSTELLEN

Die Menge $\mathbb{K}[x]$ aller Polynome über einem Körper \mathbb{K} (d.h. die Koeffizienten a_0, \dots, a_n liegen in \mathbb{K}) haben einiges gemeinsam mit der Menge der ganzen Zahlen $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$: Wie ganze Zahlen kann man auch Polynome addieren, subtrahieren und multiplizieren, nur die Division macht Probleme, denn der Quotient von Polynomen ist meistens kein Polynom mehr, ebenso wie der Quotient ganzer Zahlen meistens keine ganze Zahl ist. Wenn doch, wenn k/n wieder eine ganze Zahl oder f/g wieder ein Polynom ist, nennen wir k *teilbar* durch n und f *teilbar* durch g , symbolisch $n|k$ und $g|f$ (sprich: n teilt k und g teilt f). Ein solcher Bereich, in dem die drei Grundrechenarten Addition, Subtraktion und Multiplikation erklärt sind, nennt man einen *Ring*.

Die Ringe $\mathbb{K}[x]$ und \mathbb{Z} haben aber noch mehr gemeinsam: In beiden Bereichen kann man den *euklidischen Algorithmus* anwenden: Sind k und n ganze Zahlen mit $|k| \geq |n| > 0$, dann kann man k durch n mit Rest teilen: $k : n = p$ Rest r , d.h. es gibt ganze Zahlen r und p mit $|r| < |n|$ und $k = pn + r$. Ebenso bei Polynomen: Sind f und g Polynome mit $\partial f \geq \partial g > 0$ (Grad von $f \geq$ Grad von g), dann finden wir Polynome r und p mit $\partial r < \partial g$ und $f : g = p$ Rest r , d.h. $f = pg + r$. Ringe mit euklidischem Algorithmus heißen *euklidische*

*Ringe.*⁴⁵ Mit dem euklidischen Algorithmus kann man eine Division mit Rest durchführen oder auch den größten gemeinsamen Teiler (ggT) bestimmen, vgl. Seite 4. Eine Konsequenz davon ist der folgende Satz:

Satz 10.1. *Ist $x_o \in \mathbb{K}$ eine Nullstelle des Polynom $f \in \mathbb{K}[x]$, dann wird f von dem linearen Polynom $g = x - x_o$ geteilt, $(x - x_o) \mid f$, genauer $f = pg$ mit $\partial p = \partial f - 1$.*

Beweis. Gemäß dem euklidischen Algorithmus (Division mit Rest) gilt $f : g = p$ Rest r oder $f = pg + r$, wobei $\partial r < \partial g = 1$. Damit ist $\partial r = 0$, also ist r eine Konstante. Bei x_o ausgewertet ergibt sich $r = f(x_o) - p(x_o)g(x_o) = 0$, also ist $f = pg$, d.h. $g \mid f$. Weil $\partial f = \partial p + \partial g = \partial p + 1$, folgt $\partial p = \partial f - 1$. \square

Korollar 10.1. *Ein Polynom $f \in \mathbb{K}[x]$ vom Grad $n \geq 1$ hat höchstens n Nullstellen.*

Beweis. Ist x_1 die erste Nullstelle, so ist $f(x) = (x - x_1)f_1(x)$ mit $\partial f_1 = n - 1$. Ist $x_2 \neq x_1$ eine zweite Nullstelle, so ist $0 = f(x_2) = (x_2 - x_1)f_1(x_2)$, also ist $f_1(x_2) = 0$. Damit ist $x - x_2$ ein Teiler von f_1 , also $f_1 = (x - x_2)f_2$ mit $\partial f_2 = n - 2$, usw. Wenn es k Nullstellen für f gibt, erhalten wir (durch vollständige Induktion) ein Polynom f_k vom Grad $n - k$, und wenn dann noch eine weitere Nullstelle x_{k+1} hinzukommt, folgt wieder $(x - x_{k+1}) \mid f_k$. Bei n Nullstellen ist f_n vom Grad Null, also eine Konstante $f_n = a \in \mathbb{K}$, und $a \neq 0$, sonst wäre auch $f_{n-1} = 0$, aber $\partial f_{n-1} = 1$. Eine weitere Nullstelle x_{n+1} wäre auch Nullstelle von $f_n = a$, aber die Konstante $a \neq 0$ hat keine Nullstellen. Deshalb kann es höchstens n Nullstellen geben. \square

Korollar 10.2. *Wenn \mathbb{K} unendlich viele Elemente hat, sind die Koeffizienten von jedem $f \in \mathbb{K}[x]$ durch die Funktion f eindeutig bestimmt.*

Beweis. Wenn einerseits⁴⁶ $f(x) = a_0x^n + \dots + a_n = \sum_{k=0}^n a_kx^{n-k}$ und andererseits $f(x) = b_0x^n + \dots + b_n = \sum_{k=0}^n b_kx^{n-k}$ für alle $x \in \mathbb{K}$, so ist die Differenz dieser beiden Ausdrücke gleich Null, d.h. das Polynom $g(x) := \sum_{k=0}^n c_kx^{n-k}$ mit $c_k = a_k - b_k$ hat unendlich viele Nullstellen,

⁴⁵Dazu muss auch eine *Gradfunktion* auf dem Ring R gegeben sein, eine Funktion $\partial : R \rightarrow \mathbb{N}_o = \{0, 1, 2, \dots\}$ mit der Eigenschaft $\partial(ab) = \partial a + \partial b$ für alle $a, b \in R$. Für $R = \mathbb{Z}$ ist ∂ der Betrag: $\partial n = |n|$.

⁴⁶Wir verwenden hier das *Summensymbol*: $\sum_{k=0}^n a_kx^{n-k}$ bedeutet, dass für die Variable k in a_kx^{n-k} nacheinander die Werte $0, 1, 2, \dots, n$ eingesetzt und alle diese Ausdrücke addiert werden.

nämlich alle $x \in \mathbb{K}$. Nach Korollar 10.1 muss $\partial g = 0$ gelten, also sind alle Koeffizienten c_k gleich Null außer vielleicht c_n , aber auch dieser muss Null sein, weil dann $g(x) = c_n$ und $g(x) = 0$. Somit ist $a_k = b_k$ für alle k . \square

Mit dem Fundamentalsatz 9.1, Seite 23, erhalten wir für $\mathbb{K} = \mathbb{C}$:

Satz 10.2. *Jedes Polynom $f \in \mathbb{C}[x]$ über den komplexen Zahlen ist ein Produkt von Polynomen vom Grad 1 (“Linearfaktoren”),*

$$f(x) = a(x - x_1) \cdot \dots \cdot (x - x_n) \quad (25)$$

mit $a, x_1, \dots, x_n \in \mathbb{C}$.

Beweis. Induktion über $n = \partial f$: Für $n = 0$ ist nichts zu zeigen; wir haben dann bereits $f = a$. Induktionsschritt $n - 1 \rightarrow n$: Ist f ein Polynom vom Grad $\partial f = n \geq 1$, dann hat f nach Satz 9.1 in \mathbb{C} eine Nullstelle, die wir x_n (statt x_o) nennen wollen, und nach Satz 10.1 wird f von $g = x - x_n$ geteilt, $f = pg$ für ein $p \in \mathbb{C}[x]$. Da $n = \partial f = \partial p + \partial g = \partial p + 1$, ist $\partial p = n - 1$. Für p ist deshalb die Behauptung nach Induktionsannahme bereits wahr,

$$p = a(x - x_1) \cdot \dots \cdot (x - x_{n-1})$$

und damit $f = pg = a(x - x_1) \dots (x - x_{n-1})(x - x_n)$. \square

Bemerkung 1: Die Zahlen x_1, \dots, x_n brauchen nicht alle verschieden zu sein. Wenn eine von ihnen k -mal vorkommt, z.B. $x_1 = x_2 = \dots = x_k$, dann nennt man sie eine *Nullstelle der Ordnung k* . In diesem Fall verschwindet bei $x = x_1$ nicht nur $f(x) = (x - x_1)^k g(x)$, sondern auch seine Ableitung $f'(x) = k(x - x_1)^{k-1} g(x) + (x - x_1)^k g'(x) = (x - x_1)^{k-1} \tilde{g}(x)$, und das gleiche gilt für die höheren Ableitungen $f'', f''', \dots, f^{(k-1)}$.

Bemerkung 2: Ein Körper \mathbb{K} mit der Eigenschaft, dass jedes Polynom $f \in \mathbb{K}[x]$ in Linearfaktoren zerfällt, heißt *algebraisch abgeschlossen*. Der Körper \mathbb{C} hat also diese Eigenschaft, \mathbb{R} und \mathbb{Q} nicht: Über \mathbb{R} zerfällt das Polynom $x^2 + 1$ nicht in Linearfaktoren (sonst läge die Wurzel aus -1 in \mathbb{R}), in \mathbb{Q} auch nicht das Polynom $x^2 - 2$, da $\sqrt{2} \notin \mathbb{Q}$. Es gibt aber einen viel kleineren Teilkörper⁴⁷ von \mathbb{C} mit dieser Eigenschaft: den Körper der *algebraischen Zahlen*. Eine Zahl $x_o \in \mathbb{C}$ heißt *algebraisch*, wenn es ein Polynom mit rationalen Koeffizienten $0 \neq f \in \mathbb{Q}[x]$ gibt mit $f(x_o) = 0$. Erstaunlicherweise bilden die algebraischen Zahlen einen Teilkörper (schon das ist gar nicht selbstverständlich), der algebraisch abgeschlossen ist [5, 1.3, 1.6].

⁴⁷Ein *Teilkörper* von \mathbb{C} ist eine Teilmenge $\mathbb{K} \subset \mathbb{C}$, die unter den vier Grundrechenarten abgeschlossen ist: Für alle $a, b \in \mathbb{K}$ sind auch $a \pm b$, $a \cdot b$ und a/b (sofern $b \neq 0$) wieder Elemente von \mathbb{K} .

11. DER WURZELSATZ VON VIETA

Wenn ein Polynom $f \in \mathbb{K}[x]$ in Linearfaktoren zerfällt, hat es zwei Darstellungen, (1) und (25),

$$\begin{aligned} f(x) &= a_0x^n + a_1x^{n-1} + \cdots + a_n \\ &= a(x - x_1) \cdots (x - x_n). \end{aligned}$$

Wenn wir das Produkt in der zweiten Formelzeile ausmultiplizieren, können wir die beiden Darstellungen miteinander vergleichen. Zum Beispiel für $n = 2$:

$$f(x) = a(x - x_1)(x - x_2) = ax^2 - a(x_1 + x_2)x + ax_1x_2.$$

Die Koeffizienten des Polynoms f sind aber eindeutig bestimmt nach Korollar 10.2; Vergleich mit $f(x) = a_0x^2 + a_1x + a_2$ ergibt also

$$a_0 = a, \quad a_1 = -a(x_1 + x_2), \quad a_2 = ax_1x_2.$$

Insbesondere im Fall $a_0 = a = 1$ bestehen die folgenden Relationen zwischen Koeffizienten und Lösungen: $a_1 = -(x_1 + x_2)$, $a_2 = x_1x_2$. Dies war die Beobachtung von Vieta,⁴⁸ nicht nur für quadratische Polynome, sondern im Prinzip für jedes Polynom mit $a_0 = 1$ (*normierte Polynome*). Wir müssen nur das Produkt⁴⁹

$$f(x) = (x - x_1) \cdots (x - x_n) = \prod_{j=1}^n (x - x_j)$$

ausmultiplizieren. Wie das geht, haben wir schon im Abschnitt 3 über die Binomische Formel gesehen: Aus jedem Faktor wird einer der beiden Summanden ausgewählt, davon das Produkt gebildet und dann alle möglichen Ausdrücke dieser Art summiert. Einen Term mit der x -Potenz x^{n-k} erhalten wir also, wenn wir $(n-k)$ -mal den Summanden x auswählen und k -mal den anderen Summanden $-x_j$. Der Koeffizient a_k von x^{n-k} wird somit bis auf das Vorzeichen $(-1)^k$ die Summe über alle Produkte von je k (verschiedenen) Nullstellen x_j sein. Beispiel $n = 3$: Es ist $f(x) = x^3 + a_1x^2 + a_2x + a_3$ mit

$$a_1 = -(x_1 + x_2 + x_3), \quad a_2 = x_1x_2 + x_1x_3 + x_2x_3, \quad a_3 = -x_1x_2x_3.$$

Allgemein gilt

$$a_j = (-1)^j e_j(x_1, \dots, x_n) \tag{26}$$

⁴⁸François Viète, lat. Vieta, 1540 - 1603 (Paris)

⁴⁹Das *Produktsymbol* ist analog zum *Summensymbol* definiert: $\prod_{j=1}^n (x - x_j)$ bedeutet, in dem Ausdruck $(x - x_j)$ für den variablen Index j nacheinander die Werte $1, 2, \dots, n$ einzusetzen und alle diese Ausdrücke zu multiplizieren.

mit

$$\begin{aligned} e_1(x_1, \dots, x_n) &= x_1 + \dots + x_n = \sum_j x_j, \\ e_2(x_1, \dots, x_n) &= x_1x_2 + \dots + x_{n-1}x_n = \sum_{i<j} x_ix_j, \\ e_k(x_1, \dots, x_n) &= \sum_{j_1<\dots<j_k} x_{j_1} \cdot \dots \cdot x_{j_k}, \\ e_n(x_1, \dots, x_n) &= x_1 \cdot \dots \cdot x_n. \end{aligned}$$

Die so erhaltenen Ausdrücke in x_1, \dots, x_n sind *symmetrisch*:⁵⁰ Sie ändern ihren Wert nicht, wenn wir die x_1, \dots, x_n in einer beliebigen anderen Reihenfolge einsetzen, sie sind *invariant unter Permutationen*.⁵¹ Diese Ausdrücke haben noch eine Besonderheit: Es kommen keine Potenzen vor, sondern nur Produkte unterschiedlicher x_j . Man nennt sie die *elementar-symmetrischen Polynome* in den Variablen x_1, \dots, x_n , “elementar” deshalb, weil sich alle anderen symmetrischen Polynome aus ihnen zusammensetzen lassen, wie wir sehen werden, so wie sich in der Chemie die Stoffe aus den Elementen zusammensetzen lassen.

Was haben wir damit erreicht? Wir haben eigentlich das falsche Problem gelöst: Statt aus den Koeffizienten a_1, \dots, a_n die Lösungen (Wurzeln) x_1, \dots, x_n zu berechnen, haben wir das Umgekehrte erreicht, nämlich aus den Wurzeln x_1, \dots, x_n mit Hilfe von (26) die Koeffizienten a_1, \dots, a_n bestimmt. Wir haben also die *Koeffizienten* a_j als Funktionen der Wurzeln x_i geschrieben: Ist ein beliebiger Satz von n Zahlen x_1, \dots, x_n gegeben,⁵² so finden wir mit (26) sofort die Koeffizienten a_1, \dots, a_n eines normierten Polynoms, dessen Lösungen genau x_1, \dots, x_n sind.

⁵⁰Eine Funktion von zwei Variablen $f(x_1, x_2)$ heißt *symmetrisch*, wenn $f(x_2, x_1) = f(x_1, x_2)$, also z.B. $f(2, 3) = f(3, 2)$. Wenn es mehr als zwei Variable gibt, bedeutet Symmetrie, dass man zwei beliebige Variable vertauschen kann, ohne den Wert zu ändern. Durch mehrfaches Vertauschen von zwei Variablen kann man jede beliebige Reihenfolge erreichen.

⁵¹Eine *Permutation* einer endlichen Menge M , zum Beispiel $M = \{1, \dots, n\}$ oder $M = \{x_1, \dots, x_n\}$, ist eine umkehrbare (bijektive) Abbildung $\pi : M \rightarrow M$, eine “Umordnung” von M .

⁵²Einen solchen Satz von Zahlen in einem Körper \mathbb{K} nennen wir ein *n-Tupel*, analog zu Tripel ($n = 3$), Quadrupel ($n = 4$) usw. oder auch eine *Vektor*, wenn die Zahl n fest steht. Ein Vektor ist also einfach ein Satz von n Zahlen. Wir führen dafür ein eigenes Symbol ein: $\vec{x} := (x_1, \dots, x_n)$, und die Menge aller dieser n -Tupel nennen wir \mathbb{K}^n . Für $\mathbb{K} = \mathbb{R}$ können wir uns unter \mathbb{K}^2 und \mathbb{K}^3 die (koordinatisierte) Ebene oder den Raum vorstellen.

Beispiel: Wie lauten die Koeffizienten des normierten quartischen Polynoms $f(x) = x^4 - ax^3 + bx^2 - cx + d$ mit den Nullstellen $x_1 = -1$, $x_2 = 2$, $x_3 = -3$, $x_4 = 4$?

$$\begin{aligned} a &= x_1 + x_2 + x_3 + x_4 = -1 + 2 - 3 + 4 = 2 \\ b &= x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 \\ &= -2 + 3 - 4 - 6 + 8 - 12 = -13 \\ c &= x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 \\ &= 6 - 8 + 12 - 24 = -14 \\ d &= x_1x_2x_3x_4 = 24 \end{aligned}$$

Das Polynom lautet also $f(x) = x^4 - 2x^3 - 13x^2 + 14x + 24$.

Aber wir haben viel mehr erreicht: Wir betrachten die Koeffizienten nun nicht länger einfach als gegebene Zahlen, sondern als Funktionen der n Wurzeln,⁵³ und zwar als sehr spezielle Funktionen, eben die elementarsymmetrischen. Im nächsten Abschnitt werden wir die Bedeutung dieser Funktionen kennen lernen.

12. SYMMETRISCHE POLYNOME

Satz 12.1. Hauptsatz über symmetrische Polynome:⁵⁴ *Jedes symmetrische Polynom $f(\vec{x})$ mit $\vec{x} := (x_1, \dots, x_n)$ lässt sich als Polynom in den elementarsymmetrischen Polynomen $e_1(\vec{x}), \dots, e_n(\vec{x})$ darstellen.*

Beweis. Jedes Polynom f von n Veränderlichen x_1, \dots, x_n ist eine Linearkombination (Summe von Vielfachen) von *Monomen*, Ausdrücke der Gestalt

$$m(\vec{x}) = x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}$$

mit $k_1, \dots, k_n \in \mathbb{N}_0 = \{0, 1, 2, 3, \dots\}$. Wenn σ eine Permutation ist, d.h. eine umkehrbare Abbildung $\sigma : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$, dann macht σ aus dem Vektor \vec{x} den neuen Vektor

$$\sigma\vec{x} = (x_{\sigma(1)}, \dots, x_{\sigma(n)}). \quad (27)$$

Ist zum Beispiel $\vec{x} = (3, -4, 1)$ und σ die Permutation, die die Zahlenreihe 1, 2, 3 auf 2, 3, 1 abbildet (also $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 1$; Kurzschreibweise: $\sigma = 231$), dann ist $\sigma\vec{x} = (x_2, x_3, x_1) = (-4, 1, 3)$. Wenn nun f unter σ *invariant* ist, $f(\sigma\vec{x}) = f(\vec{x})$ für alle $\vec{x} \in \mathbb{K}^n$, dann muss mit jedem

⁵³Wir betrachten die Wurzeln x_1, \dots, x_n damit als *Variable*; wir haben es also nicht mehr mit einer einzelnen Gleichung $f(x) = 0$ zu tun, deren Lösungen x_1, \dots, x_n spezielle Zahlen sind (Unbekannte), sondern mit *allen* Gleichungen n -ter Ordnung, wobei x_1, \dots, x_n beliebige komplexe Zahlen sind (Unbestimmte); jeder Satz von n Zahlen x_1, \dots, x_n bestimmt eine andere Gleichung.

⁵⁴Albert Girard, 1595 (St. Mihiel, Lothringen) - 1632 (Leiden, Niederlande). Andere Autoren sagen, dass der beschriebene Algorithmus auf Newton (Sir Isaac Newton, 1642 - 1727) zurückgeht. Ich habe ihn aus [7] gelernt.

Monom $m(\vec{x}) = x_1^{k_1} \dots x_n^{k_n}$ auch das Monom $m(\sigma\vec{x}) = x_{\sigma(1)}^{k_1} \dots x_{\sigma(n)}^{k_n}$ in f (mit gleichem Koeffizienten) auftreten.⁵⁵ Wenn f unter *allen* Permutationen invariant ist, kommen alle diese Ausdrücke für beliebige σ vor, stets mit dem gleichen Koeffizienten. Es treten also alle Reihenfolgen der Variablen x_1, \dots, x_n auf. Weil wir das Produkt beliebig umordnen dürfen, können wir stattdessen auch sagen, dass jede Reihenfolge der Exponenten k_1, \dots, k_n auftritt. In einer dieser Reihenfolgen treten die Zahlen k_1, \dots, k_n in absteigender Ordnung (monoton fallend) auf. Wir können deshalb sagen: Wenn f invariant unter Permutationen ist, dann besteht f aus Linearkombinationen von Ausdrücken $x_1^{k_1} \dots x_n^{k_n} + \text{Permutationen}$, wobei $k_1 \geq \dots \geq k_n$. Den Term " $x_1^{k_1} \dots x_n^{k_n} + \text{Permutationen}$ " werden wir mit $[x_1^{k_1} \dots x_n^{k_n}]$ oder noch kürzer mit $[k_1, \dots, k_n]$ abkürzen. Die elementarsymmetrischen Polynome werden in dieser Schreibweise zu $e_j = [x_1 \dots x_j] = [1, \dots, 1, 0, \dots, 0]$ (genau j Einsen) für $j = 1, \dots, n$.

Diese Ausdrücke ordnen wir nun "lexikographisch".⁵⁶ Wir sagen

$$[k_1, \dots, k_n] > [l_1, \dots, l_m],$$

wenn $k_j > l_j$ an der ersten Stelle j , wo $k_j \neq l_j$ (also wenn $k_i = l_i$ für $i < j$ und $k_j > l_j$).

Wenn wir nun ein beliebiges symmetrisches Polynom f gegeben haben, suchen wir darin den höchsten Term (bezüglich dieser Ordnung) $a[k_1, \dots, k_n]$ mit $a \in \mathbb{K}$ und gehen über zu $f_1 = f - \tilde{f}$ mit

$$\tilde{f} = a e_1^{k_1 - k_2} e_2^{k_2 - k_3} \dots e_n^{k_n}. \quad (28)$$

Der höchste Term von \tilde{f} ist⁵⁷

$$[(x_1)^{k_1 - k_2} (x_1 x_2)^{k_2 - k_3} \dots (x_1 \dots x_n)^{k_n}] = [x_1^{k_1} x_2^{k_2} \dots x_n^{k_n}]$$

ebenso wie der höchste Term von f , deshalb verschwindet dieser Term in f_1 , und der höchste Term von f_1 ist niedriger als der von f . Jetzt wiederholen wir das Verfahren mit f_1 anstelle von f und erhalten ein noch niedrigeres Polynom f_2 . Da unter jedem Term nur endlich viele andere liegen, erreichen wir nach endlich vielen Stellen ein konstantes Polynom. Fügen wir alles zusammen, so haben wir f als Polynom (Summe von Vielfachen von Produkten der Variablen) in den Variablen e_1, \dots, e_n geschrieben. \square

⁵⁵Z.B. für $\sigma = 231$ und $(k_1, k_2, k_3) = (5, 3, 7)$ ist $\sigma(x_1^5 x_2^3 x_3^7) = x_2^5 x_3^3 x_1^7 = x_1^7 x_2^5 x_3^3$.

⁵⁶In einem Lexikon sind die Wörter ebenso geordnet: "Akte" steht vor "Aktie", denn die ersten drei Buchstaben stimmen überein und der vierte entscheidet die Reihenfolge, da "e" im Alphabet vor "i" kommt.

⁵⁷Die Potenz von x_1 zum Beispiel ist $k_1 - k_2 + k_2 - k_3 + \dots + k_{n-1} - k_n + k_n = k_1$.

Da die Koeffizienten a_1, \dots, a_n nach (26) bis auf Vorzeichen die elementarsymmetrischen Polynome in den Wurzeln x_1, \dots, x_n sind, erhalten wir:

Korollar 12.1. *Sind x_1, \dots, x_n die Wurzeln eines normierten Polynoms $f(x) = x^n + a_1x^{n-1} + \dots + a_n$, dann gilt für jedes symmetrische Polynom s in n Variablen: $s(x_1, \dots, x_n)$ ist ein Polynomausdruck in den Koeffizienten a_1, \dots, a_n und damit aus den Koeffizienten berechenbar.*

Beispiel 1. Bei einer quadratischen Gleichung $x^2 + ax + b = 0$ ist $x_1 + x_2 = -a$ und $x_1x_2 = b$. Wir können x_1, x_2 berechnen, wenn wir auch noch $x_1 - x_2$ kennen. Dieser Ausdruck ist nicht symmetrisch, aber sein Quadrat: $(x_1 - x_2)^2 = x_1^2 + x_2^2 - 2x_1x_2$. Der letzte Term $-2x_1x_2$ ist bereits gleich $2b$. Die ersten beiden Summanden $x_1^2 + x_2^2$ bilden ein anderes symmetrisches Polynom, das wir sofort in elementarsymmetrische zerlegen können:⁵⁸ $x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1x_2 = a^2 - 2b$ und damit $(x_1 - x_2)^2 = a^2 - 4b$. Daraus ergibt sich die "Mitternachtsformel" $x_{1,2} = \frac{1}{2}(x_1 + x_2 \pm (x_1 - x_2)) = \frac{1}{2}(-a \pm \sqrt{a^2 - 4b})$.

Beispiel 2. Im Abschnitt 4 wurde die quadratische *Tschirnhaus-Transformation* erwähnt: Gegeben sei eine Gleichung

$$(1) \quad f(x) = x^n + a_2x^{n-2} + \dots + a_n = 0,$$

mit (unbekannten) Lösungen x_1, \dots, x_n , für die bereits $a_1 = 0$, also $e_1 = 0$ gilt. Da $(e_1)^2 = p_2 + 2e_2$, wobei wir $p_k = \sum_i x_i^k$ setzen, folgt $p_2 = -2e_2 = -2a_2$. Die Gleichung (1) kann durch eine quadratische Transformation $\tilde{x}_i = g(x_i)$ verwandelt werden in eine Gleichung für \tilde{x} ,

$$(2) \quad (\tilde{x} - \tilde{x}_1) \dots (\tilde{x} - \tilde{x}_n) = \tilde{x}^n + \tilde{a}_1\tilde{x}^{n-1} + \tilde{a}_2\tilde{x}^{n-2} + \dots + \tilde{a}_n = 0,$$

für die $\tilde{a}_1 = 0$ und $\tilde{a}_2 = 0$ gilt. Wenn wir (2) lösen können, dann gewinnen wir die Lösungen x_i von (1) durch Auflösen der quadratischen Gleichung $g(x_i) = \tilde{x}_i$. Dazu setzen wir

$$(3) \quad \tilde{x}_i = g(x_i) = tx_i + x_i^2 - q_2$$

mit $q_2 := p_2/n = -2a_2/n$ und einem noch freien Parameter t . Die Koeffizienten von (2) sind $\tilde{a}_j = (-1)^j e_j(\vec{\tilde{x}})$. Insbesondere ist

$$-\tilde{a}_1 = \sum \tilde{x}_i \stackrel{(3)}{=} tp_1 + p_2 - p_2 = 0,$$

⁵⁸Wir können auch den im Beweis des vorstehenden Satz 12.1 gegebenen Algorithmus anwenden: Von $x_1^2 + x_2^2 = [2, 0]$ ist $(e_1)^{2-0}(e_2)^0 = (e_1)^2 = (x_1 + x_2)^2$ abzuziehen; die Differenz ist $-2x_1x_2 = -2e_2$, also $x_1^2 + x_2^2 = (e_1)^2 - 2e_2$.

denn $p_1 = e_1 = 0$. Weiterhin

$$\begin{aligned} -2\tilde{a}_2 = \tilde{p}_2 &= \sum \tilde{x}_i^2 \\ &\stackrel{(3)}{=} t^2 p_2 + p_4 + nq_2^2 + 2(tp_3 - q_2 p_2 - tp_1 q_2) \\ &= p_2 t^2 + 2p_3 t + p_4 + nq_2^2 - 2p_2 q_2. \end{aligned}$$

Die Forderung $\tilde{a}_2 = 0$ führt also auf eine quadratische Gleichung für t :

$$p_2 t^2 + 2p_3 t + p_4 + nq_2^2 - 2p_2 q_2 = 0,$$

wobei $p_3(\vec{x})$ und $p_4(\vec{x})$ als symmetrische Polynome in \vec{x} wieder durch die Koeffizienten a_2, a_3, a_4 ausgedrückt werden können. Auch die übrigen Koeffizienten \tilde{a}_i lassen sich als symmetrische Polynome in \vec{x} und damit durch a_2, \dots, a_n ausdrücken. Die Gleichung (2) hat also die Form

$$(2) \quad \tilde{x}^n + \tilde{a}_3 \tilde{x}^{n-3} + \dots + \tilde{a}_n = 0$$

mit bekannten Koeffizienten $\tilde{a}_3, \dots, \tilde{a}_n$. Hat man eine Lösung $\tilde{x} = \tilde{x}_j$ von (2) gefunden, so errechnet man die entsprechende Lösung x_j von (1) aus der quadratischen Gleichung (3).

Beispiel 3. Die *Diskriminante* eines Polynoms f entscheidet, ob f mehrfache Nullstellen besitzt; bis auf das Vorzeichen $\pm = (-1)^{n(n-1)/2}$ ist das der Ausdruck

$$\Delta(\vec{x}) = \pm \prod_{i \neq j} (x_i - x_j). \quad (29)$$

Dieses Polynom ist offensichtlich symmetrisch, daher lässt sich die Diskriminante ohne Kenntnis der Nullstellen aus den Koeffizienten berechnen. Für $n = 2$ zum Beispiel, d.h. für die quadratische Gleichung $x^2 - ax + b = 0$ ist

$$-\Delta = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2 = (e_1)^2 - 4e_2 = a^2 - 4b.$$

Wir wollen diese Rechnung auch noch für die kubische Gleichung $x^3 - ax^2 + bx - c = 0$,⁵⁹ für $n = 3$ durchführen. Dann ist

$$\Delta = (x_1 - x_2)^2 (x_1 - x_3)^2 (x_2 - x_3)^2. \quad (30)$$

Als erstes müssen wir dieses Polynom in die Ausdrücke $[k_1, k_2, k_3]$ zerlegen. Die möglichen Terme entsprechen den Zerlegungen der Zahl 6, wobei der größte Anteil höchstens 4 sein darf, das sind 420, 411, 330, 321, 222. Wir müssen nur die Kombinationen zählen, mit

⁵⁹Die Vorzeichen sind so gewählt, dass a, b, c gleich den elementarsymmetrischen Polynomen $e_1(\vec{x}), e_2(\vec{x}), e_3(\vec{x})$ sind.

denen wir jeden dieser 5 Terme erreichen können. Statt $(x_1 - x_2)$ schreiben wir $(1 - 2)$ usw.

(1 - 2)	(1 - 2)	(1 - 3)	(1 - 3)	(2 - 3)	(2 - 3)	$\pm \vec{k}$	
1	1	1	1	2	2	420	
1	1	1	1	2	-3	-411	·2
1	1	1	-3	2	2	-321	·2
1	1	-3	-3	2	2	222	
1	-2	1	1	2	2	-330	·2
1	-2	1	1	2	-3	321	·4
1	-2	1	-3	2	-3	-222	·8
-2	-2	1	1	-3	-3	222	

Somit ist $\Delta = [420] - 2[411] - 2[330] + 2[321] - 6[222]$. Der höchste Term ist $[420]$. Nach dem Algorithmus, Gleichung (28), müssen wir also $(e_1)^2(e_2)^2$ davon abziehen. Auch dieses Polynom zerlegen wir in seine Bestandteile:

(1 + 2 + 3)	(1 + 2 + 3)	(12 + 13 + 23)	(12 + 13 + 23)	\vec{k}	
1	1	12	12	420	
1	1	12	13	411	·2
1	1	12	23	321	·2
1	1	23	23	222	
1	2	12	12	330	·2
1	2	12	13	321	·4
1	2	13	23	222	·4
1	3	12	12	321	·2
1	3	12	23	222	·4
2	2	13	13	222	
2	3	12	13	222	·4
3	3	12	12	222	

Somit ist $(e_1)^2(e_2)^2 = [420] + 2[411] + 2[330] + 8[321] + 15[222]$.

Der zweithöchste Term ist $[411]$. Dieser wird mit Hilfe von $(e_1)^{4-1}(e_2)^{1-1}(e_3)^1 = (e_1)^3 e_3$ beseitigt, vgl. (28):

(1 + 2 + 3)	(1 + 2 + 3)	(1 + 2 + 3)	123	\vec{k}	
1	1	1	123	411	
1	1	2	123	321	·3
1	2	3	123	222	·6

Also ist $(e_1)^3 e_3 = [411] + 3[321] + 6[222]$.

Der nächstniedrige Term ist $[330]$, den wir mit $(e_1)^{3-3}(e_2)^{3-0}(e_3)^0 = (e_2)^3$ beseitigen.

(12 + 13 + 23)	(12 + 13 + 23)	(12 + 13 + 23)	\vec{k}	
12	12	12	330	
12	12	13	321	·3
12	13	23	222	·6

Der nächste Term ist $[321]$, der mit $(e_1)^{3-2}(e_2)^{2-1}(e_3)^1 = e_1 e_2 e_3$ weggehoben wird:

(1 + 2 + 3)	(12 + 13 + 23)	123	\vec{k}	
1	12	123	321	
1	23	123	222	
2	13	123	222	
3	12	123	222	

Also ist $e_1 e_2 e_3 = [321] + 3[222]$.

Der letzte Term ist [222]. Dieser wird durch $(e_1)^{2-2}(e_2)^{2-2}(e_3)^2 = (e_3)^2$ weggehoben, wobei genau $(e_3)^2 = (x_1x_2x_3)^2 = [222]$.

Nun können wir Δ berechnen:

	420	411	330	321	222	
Δ	1	-2	-2	2	-6	
$(e_1)^2(e_2)^2$	1	2	2	8	15	·(-1)
$(e_1)^3e_3$		-4	-4	-6	-21	
$(e_2)^3$		1		3	6	·4
$e_1e_2e_3$			-4	6	3	
$(e_3)^2$			1	3	6	·4
				18	27	
				1	3	·(-18)
					-27	
					1	·27
					0	

Somit ist $\Delta - (e_1)^2(e_2)^2 + 4(e_1)^3e_3 + 4(e_2)^3 - 18e_1e_2e_3 + 27(e_3)^2 = 0$, also

$$\Delta = a^2b^2 - 4a^3c - 4b^3 + 18abc - 27c^2. \quad (31)$$

Die Rechnung vereinfacht sich wesentlich, wenn wir gleich $a = 0$ voraussetzen.

Bemerkung: Rekursionsformeln. Wie hängen die elementarsymmetrischen Polynome e_i für die Dimensionen n und $n - 1$ miteinander zusammen? Wir bezeichnen sie mit e_i und \tilde{e}_i . Alle e_i bestehen aus Summanden, in denen x_n höchstens einmal vorkommt. Wenn wir die Terme mit Faktor x_n von denen ohne Faktor x_n trennen, sehen wir

$$\begin{aligned} e_1 &= \tilde{e}_1 + x_n \\ e_i &= \tilde{e}_i + \tilde{e}_{i-1}x_n \quad \text{für } i = 2, \dots, n \\ e_{n+1} &= \tilde{e}_n x_n \end{aligned}$$

oder zusammengefasst

$$e_j = \tilde{e}_j + \tilde{e}_{j-1}x_n \quad (32)$$

für $j = 1, \dots, n + 1$ mit $\tilde{e}_0 = 1$ und $\tilde{e}_{n+1} = 0$.

13. LAGRANGESCHE RESOLVENTEN

Der Hauptsatz über symmetrische Funktionen führt in einfachen Fällen zu Lösungsverfahren für Polynomgleichungen $f(x) = 0$, nämlich mit folgender Überlegung. Bekannt sind uns alle symmetrischen Polynome in den Wurzeln $\vec{x} = (x_1, \dots, x_n)$. Das sind die polynomialen Ausdrücke $s(\vec{x})$, deren Wert ungeändert bleibt, wenn wir die Variablen x_1, \dots, x_n in einer anderen Reihenfolge einsetzen, die also invariant unter allen Permutationen der Variablen sind. Gesucht sind die Wurzeln

x_j . Diese sind selbst Polynome in (x_1, \dots, x_n) , nämlich die Projektionen $x_j : \vec{x} \mapsto x_j$;⁶⁰ sie sind natürlich unter keiner Permutation (außer der trivialen, die gar nichts verändert) gemeinsam invariant. Die Überlegung ist nun, den Übergang $a_i \rightsquigarrow x_j$ nicht in einem Schritt zu bewältigen, sondern “halbvariante” Ausdrücke $y_1(\vec{x}), \dots, y_r(\vec{x})$ dazwischen zu schieben, sogenannte *Resolventen*, wobei die Polynome $y_k(\vec{x})$ diesmal nicht unter allen, sondern nur unter manchen Permutationen gemeinsam invariant sind, und alle y_k sollen aus y_1 durch Anwenden aller übrigen Permutationen entstehen (sie bilden zusammen eine *Bahn* unter allen Permutationen). Die y_k sind dann Lösungen von Gleichungen, deren Koeffizienten die elementarsymmetrischen Polynome in den $y_k(\vec{x})$ sind; weil die Permutationen der x_1, \dots, x_k auch die $y_k(\vec{x})$ permutieren, sind die Koeffizienten symmetrische Polynome in \vec{x} und daher durch die Koeffizienten a_i ausdrückbar. Wenn die y -Gleichung einfacher ist als die x -Gleichung, haben wir das Problem $a_i(\vec{x}) \rightsquigarrow \vec{x}$ in zwei einfachere Teilprobleme zerlegt: $a_i(\vec{x}) \rightsquigarrow y_k(\vec{x}) \rightsquigarrow \vec{x}$.

Ein sehr simples Beispiel hatten wir schon bei $n = 2$, bei der quadratischen Gleichung $x^2 - ax + b = 0$ gesehen, Beispiel 1 auf Seite 32: Der Ausdruck $u = x_2 - x_1$ ist nicht invariant unter der Vertauschung, der einzigen nicht-identischen Permutation, aber sein Quadrat ist es. Dieses lässt sich also durch die Koeffizienten darstellen, $(x_2 - x_1)^2 = a^2 - 4b$, und damit ist $x_2 + x_1 = a$ und $x_2 - x_1 = \pm\sqrt{a^2 - 4b}$.

Für kubische Gleichungen $x^3 - ax^2 + bx - c = 0$ können wir ähnliche Ausdrücke u betrachten, allerdings gibt es jetzt drei Lösungen x_1, x_2, x_3 . An die Stelle von $x_2 + x_1$ und $x_2 - x_1$ treten die drei Ausdrücke

$$u = x_3 + \omega x_2 + \omega^2 x_1 \quad (33)$$

für jede “dritte Einheitswurzel”⁶¹ $\omega \in \mathbb{C}$ mit $\omega^3 = 1$, also

$$\omega \in \{1, e^{2\pi i/3}, e^{-2\pi i/3}\}.$$

Für die Permutation $\sigma = (123)$ (Ringtausch $1 \mapsto 2 \mapsto 3 \mapsto 1$)⁶² ist

$$\sigma u(\vec{x}) = x_1 + \omega x_3 + \omega^2 x_2 = \omega u(\vec{x}).$$

Für $\omega = 1$ ist $u = x_3 + x_2 + x_1$ bereits symmetrisch, nämlich gleich a , und für $\omega = \omega_{\pm} = e^{\pm 2\pi i/3}$ ist jedenfalls $\omega^3 = 1$, also ist die dritte

⁶⁰Man nennt die Abbildung $(x_1, \dots, x_n) \mapsto x_j$ die j -te *Projektion*; der Vektor $\vec{x} = (x_1, \dots, x_n)$ wird auf seine Komponente mit der Nummer j abgebildet. Das sind die einfachsten Abbildungen von mehreren Variablen: Weglassen von Variablen!

⁶¹Diese sind analog zu den Faktoren ± 1 (“zweite Einheitswurzeln”) in $x_2 \pm x_1$

⁶²Mit $(k_1 k_2 \dots k_r)$ bezeichnen wir allgemein den Ringtausch (Zyklus) $k_1 \mapsto k_2 \mapsto \dots \mapsto k_r \mapsto k_1$; alle übrigen Elemente der Menge $\{1, \dots, n\}$ bleiben fest. Einfachstes Beispiel ist (12), die Vertauschung von 1 und 2.

Potenz $y(\vec{x}) := u(\vec{x})^3$ invariant unter σ . Wir erhalten damit zwei “halb-invariante” Ausdrücke, die unter (123) und (132) invariant sind und von (12), (13), (23) vertauscht werden;⁶³ deshalb bilden sie eine Bahn unter allen Permutationen: $y_{\pm} = (u_{\pm})^3$ mit $u_{\pm} = x_3 + \omega_{\pm}x_2 + \omega_{\mp}x_1$. Diese sind die Lösungen der quadratischen Gleichung

$$y^2 - py + q = 0 \quad (34)$$

mit $p = y_+ + y_- = u_+^3 + u_-^3$ und $q = y_+y_- = (u_+u_-)^3$. Die Koeffizienten p, q sind invariant unter allen Permutationen und können deshalb durch a, b, c ausgedrückt werden; das Ergebnis ist

$$\begin{aligned} p &= 2a^3 - 9ab + 27c \\ q &= (a^2 - 3b)^3 \end{aligned} \quad (35)$$

Die Lösung von (34) ist

$$2y_{\pm} = p \pm \sqrt{p^2 - 4q}. \quad (36)$$

Im Fall $a = 0$ ist $p = 27c$ und $q = -27b^3$, also mit $\tilde{c} = \frac{c}{2}$ und $\tilde{b} = \frac{b}{3}$

$$y_{\pm} = 27 \left(\tilde{c} \pm \sqrt{\tilde{c}^2 + \tilde{b}^3} \right). \quad (37)$$

Aus den $u_{\pm} = \sqrt[3]{y_{\pm}}$ und a können wir wirklich die Lösungen x_1, x_2, x_3 gewinnen:

$$\begin{aligned} x_3 + x_2 + x_1 &= a & (a) \\ x_3 + \omega_+x_2 + \omega_-x_1 &= u_+ & (b) \\ x_3 + \omega_-x_2 + \omega_+x_1 &= u_- & (c) \end{aligned}$$

Die Gleichungen (a) + (b) + (c), (a) + $\omega_-(b) + \omega_+(c)$, (a) + $\omega_+(b) + \omega_-(c)$ bestimmen x_3, x_2, x_1 :

$$\begin{aligned} 3x_3 &= a + u_+ + u_- \\ 3x_2 &= a + \omega_-u_+ + \omega_+u_- \\ 3x_1 &= a + \omega_+u_+ + \omega_-u_- \end{aligned} \quad (38)$$

Im Fall $a = 0$ ist mit (37)

$$x_3 = \sqrt[3]{\tilde{c} + \sqrt{\tilde{c}^2 + \tilde{b}^3}} + \sqrt[3]{\tilde{c} - \sqrt{\tilde{c}^2 + \tilde{b}^3}}, \quad (39)$$

wie schon in (10) gesehen. Aber jetzt haben wir auch die beiden anderen Wurzeln bestimmt:

$$x_{1,2} = \omega_{\pm} \sqrt[3]{\tilde{c} + \sqrt{\tilde{c}^2 + \tilde{b}^3}} + \omega_{\mp} \sqrt[3]{\tilde{c} - \sqrt{\tilde{c}^2 + \tilde{b}^3}}. \quad (40)$$

⁶³Die Polynome τu für die sechs Permutationen τ sind $u_+, \omega u_+, \omega^2 u_+$ und $u_-, \omega u_-, \omega^2 u_-$ mit $u_{\pm} = x_3 + \omega_{\pm}x_2 + \omega_{\mp}^2 x_1$. Da $\omega^3 = 1$, gibt es bei den dritten Potenzen $y = u^3$ nur zwei solche Ausdrücke y_{\pm} .

Berechnung von $q = (u_+u_-)^3$: Mit $\omega_+\omega_- = 1$ und $\omega_{\pm}^2 = \omega_{\mp}$ und $\omega_+ + \omega_- = -1$ ist

$$\begin{aligned} u_+u_- &= (x_3 + \omega_+x_2 + \omega_-x_1)(x_3 + \omega_-x_2 + \omega_+x_1) \\ &= [(x_1)^2] - e_2 \\ &= (e_1)^2 - 3e_2 \\ &= a^2 - 3b, \end{aligned}$$

weil $(x_1)^2 + (x_2)^2 + (x_3)^2 = (x_1 + x_2 + x_3)^2 - 2(x_1x_2 + x_1x_3 + x_2x_3)$.

Berechnung von p, q : Nach (33) ist

$$u^3 = [(x_1)^3] + 3r + 6e_3$$

mit $[(x_1)^3] = (x_1)^3 + (x_2)^3 + (x_3)^3$ und

$$r = (\omega x_3 + \omega^2 x_2)x_3x_2 + (\omega^2 x_3 + \omega x_1)x_3x_1 + (\omega x_2 + \omega^2 x_1)x_2x_1.$$

Da $(\omega_{\pm})^2 = \omega_{\mp}$ und $\omega_+ + \omega_- = 2 \cos \frac{2\pi}{3} = -1$, folgt

$$p = u_+^3 + u_-^3 = 2[(x_1)^3] - 3s + 12e_3$$

mit

$$s = (x_3 + x_2)x_3x_2 + (x_3 + x_1)x_3x_1 + (x_2 + x_1)x_2x_1 = [(x_1)^2x_2],$$

wobei die eckigen Klammern wieder bedeuten, dass alle Permutationen hinzuaddiert werden sollen. Gemäß dem Algorithmus im Abschnitt 11 müssen wir das symmetrische Polynom $s = [(x_1)^2x_2] = [210]$ mit dem Ausdruck $(e_1)^{2-1}e_2^{1-0} = e_1e_2$ vergleichen:

$$\begin{aligned} e_1e_2 &= (x_1 + x_2 + x_3)(x_1x_2 + x_1x_3 + x_2x_3) \\ &= [(x_1)^2x_2] + 3x_1x_2x_3. \end{aligned} \quad (41)$$

Also ist $s = e_1e_2 - 3e_3$ und damit

$$p = 2[(x_1)^3] - 3e_1e_2 + 21e_3.$$

Es bleibt die Potenzsumme $[(x_1)^3] = [100]$ zu bestimmen durch Vergleich mit $(e_1)^3$:

$$\begin{aligned} (e_1)^3 &= (x_1 + x_2 + x_3)^3 = [(x_1)^3] + 3[(x_1)^2x_2] + 6x_1x_2x_3 \\ &\stackrel{(41)}{=} [(x_1)^3] + 3e_1e_2 - 3e_3. \end{aligned}$$

Somit

$$p = 2(e_1)^3 - 9e_1e_2 + 27e_3 = 2a^3 - 9ab + 27c. \quad (42)$$

Also sind y_{\pm} Lösungen der quadratischen Gleichung $y^2 - py + q = 0$ mit

$$\begin{aligned} p &= 2a^3 - 9ab + 27c \\ q &= (a^2 - 3b)^3 \end{aligned} \quad (43)$$

Die "Mitternachtsformel" liefert $2y_{\pm} = p \pm \sqrt{p^2 - 4q}$.

Die Ausdrücke u wie in (33) machen nicht nur für $n = 3$, sondern für jedes n Sinn: Wenn ω eine n -te Einheitswurzel ist, $\omega^n = 1$, und x_1, \dots, x_n die Lösungen einer Gleichung $x^n + a_1x^{n-1} + \dots + a_n = 0$, dann ist

$$u_{\omega} = x_n + \omega x_{n-1} + \dots + \omega^{n-1}x_1 \quad (44)$$

ein solcher Ausdruck, genannt *Lagrangesche Resolvente*.⁶⁴ Unter der Permutation $\sigma = (12 \dots n)$, die den Ringtausch $1 \mapsto 2 \mapsto \dots \mapsto n \mapsto 1$ bezeichnet, verhält er sich wie folgt:

$$\sigma u_\omega = \omega u_\omega,$$

und $y_\omega := (u_\omega)^n$ ist daher "halbvariant", nämlich invariant unter σ . Aber leider gibt es viele ähnliche Ausdrücke, die aus y_ω durch Permutation von x_1, \dots, x_n entstehen, und erst alle zusammen sind sie die Lösungen einer Gleichung, deren Koeffizienten wir aus a_1, \dots, a_n berechnen können. Bereits bei $n = 4$ gibt es 6 solche Ausdrücke; um sie zu finden, müssten wir also eine Gleichung 6. Grades (statt 4. Grades) lösen!⁶⁵

14. DIE LÖSUNG DER QUARTISCHEN GLEICHUNG

Die allgemeine quartische Gleichung

$$f(x) = x^4 - ax^3 + bx^2 - cx + d = 0 \quad (45)$$

kann aber mit einer verwandten Methode gelöst werden. Wir haben die Vorzeichen so gewählt, dass a, b, c, d genau die elementarsymmetrischen Funktionen in $\vec{x} = (x_1, x_2, x_3, x_4)$ sind. Diese sind invariant unter allen Permutationen. Die Resolventen sind Polynome $y_k(\vec{x})$, die nur unter den Permutationen $\rho = (12)(34)$, $\sigma = (13)(24)$, $\tau = (14)(23)$ invariant sind, wobei (ij) die einfache Vertauschung von i und j bezeichnet; $(12)(34)$ ist also die Permutation, die 1234 in die Reihenfolge 2143 umordnet. Ein solcher Ausdruck ist

$$y_1 = (x_1 + x_2)(x_3 + x_4) :$$

Natürlich ist $\rho y_1 = (x_2 + x_1)(x_4 + x_3) = y_1$, aber erstaunlicherweise gilt auch $\sigma y_1 = (x_3 + x_4)(x_1 + x_2) = y_1$ und $\tau y_1 = (x_4 + x_3)(x_2 + x_1) = y_1$. Wendet man aber beliebige Permutationen auf y_1 an, so ist y_1 nicht mehr invariant, sondern es entstehen noch zwei weitere Polynome, in denen die Variablen permutiert sind:

$$y_2 = (x_1 + x_3)(x_2 + x_4), \quad y_3 = (x_1 + x_4)(x_2 + x_3).$$

Auch sie sind invariant unter ρ, σ, τ . Die drei Zahlen $y_k = y_k(\vec{x})$, $k = 1, 2, 3$, sind die Lösungen der kubischen Gleichung

$$y^3 - uy^2 + vy - w = 0 \quad (46)$$

⁶⁴Joseph-Louis de Lagrange, 1736 (Turin) - 1813 (Paris)

⁶⁵Allerdings lässt sich diese Gleichung 6. Grades in y auf eine quadratische Gleichung in y^3 reduzieren [3, p. 19] und damit lösen. Aber ab Grad 5 scheitert die Methode endgültig.

mit $u = e_1(\vec{y})$, $v = e_2(\vec{y})$, $w = e_3(\vec{y})$, wobei $\vec{y} = (y_1, y_2, y_3)$. Als Funktionen von \vec{x} betrachtet (\vec{y} ist ja selbst eine Funktion von \vec{x}) sind u, v, w symmetrische Polynome: Jede Permutation π von (x_1, \dots, x_4) definiert eine Permutation von (y_1, y_2, y_3) , und diese ändert nicht den Wert der elementarsymmetrischen Polynome $e_i(\vec{y})$. Deshalb können die Koeffizienten u, v, w von (46) als Polynomausdrücke in den Koeffizienten a, b, c, d von (45) angegeben werden; sie sind also bekannt. Genauer erhalten wir durch wiederholte Anwendung unseres Algorithmus:

$$\left. \begin{aligned} u &= 2b \\ v &= b^2 + ac - 4d \\ w &= abc - a^2d - c^2 \end{aligned} \right\} \quad (47)$$

Die kubische Gleichung (46) können wir lösen (vgl. Abschnitt 5) und ermitteln damit die Zahlen y_1, y_2, y_3 . Daraus sind die x_1, x_2, x_3, x_4 leicht zu berechnen: Setzen wir $z_i = x_1 + x_i$ mit $i = 2, 3, 4$, so gilt wegen $a = x_1 + x_2 + x_3 + x_4$

$$z_i^2 - az_i = -y_{i-1}, \quad (48)$$

und z_i ist eine Lösung dieser quadratischen Gleichung. Da $z_2 + z_3 + z_4 = 2x_1 + a$, haben wir x_1 ermittelt und damit auch $x_i = z_i - x_1$ für $i = 2, 3, 4$.

Berechnung der Koeffizienten u, v, w : Wenn wir x_i einfach mit i abkürzen ($i = 1, 2, 3, 4$), so ist

$$\begin{aligned} y_1 &= (1+2)(3+4) = 13 + 14 + 23 + 24, \\ y_2 &= (1+3)(2+4) = 12 + 14 + 23 + 34, \\ y_3 &= (1+4)(2+3) = 12 + 13 + 24 + 34. \end{aligned}$$

Damit ist

$$\begin{aligned} u &= y_1 + y_2 + y_3 \\ &= 13+14+23+24 + 12+14+23+34 + 12+13+24+34. \end{aligned}$$

Wir brauchen wieder nur diejenigen Summanden hinzuschreiben, bei denen die Potenzen von 1,2,3,4 in absteigender Reihenfolge auftreten ("absteigende Terme"); die anderen gewinnen wir durch Permutation. Die Teilsummen, deren Summanden durch Permutation eines Summanden entstehen, bezeichnen wir wieder mit eckigen Klammern; zum Beispiel $[12] = 12 + 13 + 14 + 23 + 24 + 34$. Damit ist $u = 2[12]$, und da $[12] = e_2 = b$, folgt sofort

$$u = 2b. \quad (49)$$

Weiterhin gilt

$$\begin{aligned} v &= y_1y_2 + y_1y_3 + y_2y_3 \\ &= (13 + 14 + 23 + 24)(12 + 14 + 23 + 34) \\ &\quad + (13 + 14 + 23 + 24)(12 + 13 + 24 + 34) \\ &\quad + (12 + 14 + 23 + 34)(12 + 13 + 24 + 34). \end{aligned}$$

Beim Ausmultiplizieren werden Terme leicht übersehen; wir wollen uns daher zunächst überlegen, welche Terme überhaupt vorkommen können. Das Polynom v hat Grad 4, und $1 = x_1$ kommt höchstens mit Potenz 2 vor; die möglichen Terme sind also die Zerlegungen von $4 = k_1 + k_2 + k_3 + k_4$ mit $2 \geq k_1 \geq k_2 \geq k_3 \geq k_4 \geq 0$. Diese sind 2200, 2110,

1111. Nun gehen wir alle Kombinationen mit absteigenden Potenzen durch und schreiben (zeilenweise) diejenigen auf, die zum entsprechenden Term gehören.

2200	2110	1111
	13 · 12	14 · 23 + 23 · 14
	13 · 12	13 · 24 + 24 · 13
12 · 12	12 · 13	12 · 34 + 34 · 12

Also gilt

$$v = [2200] + 3[2110] + 6[1111].$$

Um v mit a, b, c, d auszudrücken, müssen wir die entsprechenden Produkte der elementarsymmetrischen Polynome abziehen. Für 2200 ist das

$$(e_1)^{2-2}(e_2)^2 = (e_2)^2 = (12 + 13 + 14 + 23 + 24 + 34)^2,$$

und wir erhalten für $(e_2)^2$ die folgenden Koeffizienten:

2200	2110	1111
$(12)^2$	$2 \cdot 12 \cdot 13$	$2 \cdot (12 \cdot 34 + 13 \cdot 24 + 14 \cdot 23)$

Zu 2110 gehört $(e_1)^{2-1}(e_2)^{1-1}e_3 = e_1e_3$, wobei

$$\begin{aligned} e_1e_3 &= (1 + 2 + 3 + 4)(123 + 124 + 134 + 234) \\ &= [1 \cdot 123] + [1 \cdot 234] + [2 \cdot 134] + [3 \cdot 124] + [4 \cdot 123] \\ &= [2110] + 4 \cdot [1111]. \end{aligned}$$

Der letzte Term [1111] ist bereits elementarsymmetrisch, nämlich e_4 . Wir erhalten:

	2200	2110	1111 = e_4	
v	1	3	6	
$(e_2)^2$	1	2	6	· (-1)
		1		
e_1e_3		1	4	· (-1)
			-4	

Somit $v - (e_2)^2 - e_1e_3 = -4e_4$ und damit

$$v = b^2 + ac - 4d. \tag{50}$$

Der letzte Koeffizient w ist ein Polynom vom Grad 6 mit höchster Potenz 3:

$$\begin{aligned} w &= y_1y_2y_3 \\ &= (13 + 14 + 23 + 24)(12 + 14 + 23 + 34)(12 + 13 + 24 + 34). \end{aligned}$$

Die möglichen Zerlegungen sind also 3300, 3210, 3111, 2220, 2211, aber die erste, 3300, tritt nicht auf, weil 12 nur in zwei Faktoren vorkommt.

3210	3111	2220	2211
13 · 12 · 24	13 · 12 · 14	13 · 23 · 12	13 · 12 · 24
	13 · 14 · 12	23 · 12 · 13	14 · 23 · 12
			23 · 14 · 12
			24 · 12 · 13

Das zu 3210 gehörige Produkt elementarsymmetrischer Polynome ist

$$e_1e_2e_3 = (1 + 2 + 3 + 4)(12 + 13 + 14 + 23 + 24 + 34)(123 + 124 + 134 + 234)$$

mit den folgenden Komponenten:

3210	3111	2220	2211
1 · 12 · 123	1 · 12 · 134	1 · 23 · 123	1 · 12 · 234
	1 · 13 · 124	2 · 13 · 123	1 · 23 · 124
	1 · 14 · 134	3 · 12 · 123	1 · 24 · 123
			2 · 12 · 134
			2 · 13 · 124
			2 · 14 · 123
			3 · 12 · 124
			4 · 12 · 123

Das zu 3111 gehörige Produkt ist

$$\begin{aligned}
 (e_1)^2 e_4 &= (1 + 2 + 3 + 4)^2 1234 \\
 &= [1 \cdot 1 \cdot 1234] + 2[1 \cdot 2 \cdot 1234] \\
 &= [3111] + 2 \cdot [2211].
 \end{aligned}$$

Zu 2220 gehört

$$\begin{aligned}
 (e_3)^2 &= (123 + 124 + 134 + 234)^2 \\
 &= [123 \cdot 123] + 2 \cdot [123 \cdot 124] \\
 &= [2220] + 2 \cdot [2211]
 \end{aligned}$$

und zu 2211 schließlich (aber das wird gar nicht mehr gebraucht)

$$\begin{aligned}
 e_2 e_4 &= (12 + 13 + 14 + 23 + 24 + 34) 1234 \\
 &= [12 \cdot 1234] = [2211].
 \end{aligned}$$

Jetzt können wir w berechnen:

	3210	3111	2220	2211	
w	1	2	2	4	
$e_1 e_2 e_3$	1	3	3	8	· (-1)
		-1	-1	-4	
$(e_1)^2 e_4$		1		2	
			-1	-2	
$(e_3)^2$			1	2	
				0	

Somit $w - e_1 e_2 e_3 + (e_1)^2 e_4 + (e_3)^2 = 0$, also

$$w = abc - a^2 d - c^2. \tag{51}$$

Beispiel:

$$(*) \quad x^4 - 2x^3 - 13x^2 + 14x + 24 = 0$$

mit $a = 2$, $b = -13$, $c = -14$, $d = 24$. Nach (49,50,51) ist

$$\begin{aligned}
 u &= 2b = -26 \\
 v &= b^2 + ac - 4d \\
 &= 169 - 28 - 96 = 45 \\
 w &= abc - a^2 d - c^2 \\
 &= 28 \cdot 13 - 96 - 14 \cdot 14 \\
 &= 14 \cdot (26 - 14) - 96 = (14 - 8) \cdot 12 = 72.
 \end{aligned}$$

Die zugehörige kubische Gleichung lautet also

$$(**) \quad y^3 + 26y^2 + 45y - 72 = 0.$$

Eine Lösung von $(**)$ ist $y_1 = 1$, denn $1 + 26 + 45 - 72 = 0$. Wir können die linke Seite von $(**)$ also durch $y - 1$ teilen und erhalten $(y^3 + 26y^2 + 45y - 72) : (y - 1) = y^2 + 27y + 72$. Die Lösungen der quadratischen Gleichung $y^2 + 27y + 72 = 0$ sind⁶⁶ $y_2 = -24$ und $y_3 = -3$. Für $z = x_1 + x_i$ ($i = 2, 3, 4$) finden wir mit (48) die Gleichung $z^2 - 2z = -y$ mit $y \in \{1, -24, -3\}$, also $(z - 1)^2 = -y + 1 \in \{0, 25, 4\}$ und $z \in \{1, 1 \pm 5, 1 \pm 2\}$. Welche Lösung der quadratischen Gleichung jeweils die richtige ist, muss ausprobiert werden; hier sind die richtigen Lösungen $1, 1 - 5, 1 + 2$, also: $x_1 + x_2 = 1$, $x_1 + x_3 = -4$, $x_1 + x_4 = 3$. Die Summe dieser drei Terme ist einerseits $2x_1 + 2$, weil $x_1 + x_2 + x_3 + x_4 = a = 2$, andererseits ist sie gleich $1 - 4 + 3 = 0$, also ist $2x_1 + 2 = 0$ und damit $x_1 = -1$ sowie $x_2 = 1 + 1 = 2$, $x_3 = 1 - 4 = -3$, $x_4 = 1 + 3 = 4$. Dies sind in der Tat die Lösungen von $(*)$, vgl. das Beispiel Seite 30.

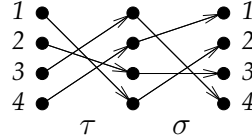
15. GRUPPEN

Zum besseren Verständnis der Rechenverfahren müssen wir erkennen, dass die Permutationen eine eigene kleine "Rechenwelt" bilden, eine *Gruppe*. Was bedeutet eigentlich "rechnen"? In den meisten Fällen nimmt man zwei Elemente einer Menge, zum Beispiel die Zahlen 3 und 4, und macht daraus eine neue Zahl, z.B. $3 + 4 = 7$. Genauso kann man mit Permutationen rechnen. Das sind ja umkehrbare Abbildungen einer endlichen Menge auf sich selbst (stellvertretend für alle Mengen mit n Elementen können wir die Menge $\{1, \dots, n\}$ wählen), und aus zwei Abbildungen können wir eine neue machen durch *Verkettung* (Komposition, Hintereinanderschaltung). Zum Beispiel werden die Zahlen 1, 2, 3, 4 (kurz: 1234) in die Reihenfolge 4132 gebracht mit Hilfe der Abbildung $\left(\sigma = 4132 : \begin{array}{l} 1 \mapsto 4 \\ 2 \mapsto 1 \\ 3 \mapsto 3 \\ 4 \mapsto 2 \end{array}\right)$. Haben wir nun eine zweite Permutation, z.B. $\left(\tau = 4312 : \begin{array}{l} 1 \mapsto 4 \\ 2 \mapsto 3 \\ 3 \mapsto 1 \\ 4 \mapsto 2 \end{array}\right)$, dann können wir die beiden Abbildungen hintereinanderschalten (*verketteten*) und bekommen eine neue Permutation $\sigma \circ \tau$, definiert durch

$$(\sigma \circ \tau)(k) = \sigma(\tau(k))$$

⁶⁶ $(y + \frac{27}{2})^2 = y^2 + 27y + \frac{27^2}{4} = \frac{9^3}{4} - 72 = \frac{9}{4} \cdot (81 - 32) = (\frac{3}{2} \cdot 7)^2 \Rightarrow y = -\frac{27}{2} \pm \frac{21}{2}$.

für alle $k \in \{1, \dots, n\}$. Insgesamt erhalten wir $\left(\sigma \circ \tau : \begin{matrix} 1 \mapsto 2 \\ 2 \mapsto 3 \\ 3 \mapsto 4 \\ 4 \mapsto 1 \end{matrix}\right) = 2341$, denn $(\sigma \circ \tau)(1) = \sigma(\tau(1)) = \sigma(4) = 2$, $\sigma(\tau(2)) = \sigma(3) = 3$, $\sigma(\tau(3)) = \sigma(1) = 4$ und $\sigma(\tau(4)) = \sigma(2) = 1$. Oder im Bild:



Wir haben also $4132 \circ 4312 = 2341$ berechnet.⁶⁷

Wir können auch drei oder mehr Permutationen verketteten, und dabei kommt es nicht auf Klammerungen an,⁶⁸ denn

$$((\rho \circ \tau) \circ \sigma)(k) = (\rho \circ \tau)(\sigma(k)) = \rho(\tau(\sigma(k)))$$

und auch $(\rho \circ (\tau \circ \sigma))(k) = \rho((\tau \circ \sigma)(k)) = \rho(\tau(\sigma(k)))$. Das Gesetz

$$(\rho \circ \tau) \circ \sigma = \rho \circ (\tau \circ \sigma) \quad (52)$$

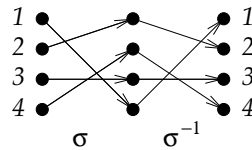
nennt man *Assoziativgesetz*; es gilt allgemein für die Verkettungen beliebiger Abbildungen.

Schließlich gibt es Permutationen mit besonderen Eigenschaften bezüglich der Verkettung: Da ist zunächst die “identische Permutation” $\text{id} = \epsilon = 1234$, die gar nichts umordnet: $\epsilon(k) = k$ für alle k . Für sie gilt

$$\epsilon \circ \sigma = \sigma \circ \epsilon = \sigma. \quad (53)$$

Ferner lässt sich jede Permutation rückgängig machen, indem man einfach die Pfeile umdreht: Die Umkehrung der Permutation $\sigma : 1234 \mapsto 4132$ ist $4132 \mapsto 1234$ oder (richtig geordnet) $1234 \mapsto 2431$; wir nennen diese Permutation σ^{-1} , die *inverse* Permutation zu σ . Die beiden Permutationen σ und σ^{-1} machen sich gegenseitig rückgängig:

$$\sigma^{-1} \circ \sigma = \sigma \circ \sigma^{-1} = \epsilon. \quad (54)$$



Eine solche kleine Rechenwelt nennen wir eine *Gruppe*. Hier ist die offizielle

⁶⁷Ein Gesetz, das wir vom Zahlenrechnen gewohnt sind, gilt hier allerdings nicht, das *Kommutativgesetz*: In den meisten Fällen ist $\sigma \circ \tau \neq \tau \circ \sigma$. In unserem Beispiel etwa ist $4132 \circ 4312 = 2341$, aber $4312 \circ 4132 = 2413$.

⁶⁸Das gleiche Gesetz ist uns auch von der Addition und Multiplikation von Zahlen bekannt: $(a + b) + c = a + (b + c)$ und $(ab)c = a(bc)$.

Definition: Eine (abstrakte) *Gruppe* $(G, e, *, ()^{-1})$, kurz G , ist eine Menge G mit einem ausgezeichneten Element $e \in G$, genannt *Neutralelement*, sowie zwei Abbildungen⁶⁹

$$\begin{aligned} G \times G &\rightarrow G, & (g, h) &\mapsto g * h & \text{("Gruppenoperation")}, \\ G &\rightarrow G, & g &\mapsto g^{-1} & \text{("Inversion")}, \end{aligned}$$

die folgende Gesetze erfüllen: Für alle $g, h, k \in G$ gilt:

G1: Assoziativgesetz: $(g * h) * k = g * (h * k)$,

G2: Neutralelement: $e * g = g * e = g$,

G3: Inverses: $g * g^{-1} = g^{-1} * g = e$.

Eine Gruppe $(G, *)$ heißt *kommutativ* oder *abelsch*,⁷⁰ wenn zusätzlich gilt:

G0: Kommutativgesetz: $g * h = h * g$.

Eine solche Definition ist wie eine Spielregel, zum Beispiel für Schach: In der Schachanleitung steht nicht, wie ein Springer oder ein Läufer aussieht, aus welchem Material die Figuren gefertigt sind usw., sondern nur, wie sie ziehen und schlagen. Ebenso sagen wir bei der Gruppdefinition nicht, wie die Gruppenoperation $*$ definiert wird, sondern nur, welche Eigenschaften sie hat. Wir haben dafür eigens das Symbol $*$ gewählt, das sonst in der Mathematik wenig Verwendung findet. Wenn wir eine konkrete Gruppe vorliegen haben, wird $*$ durch die Gruppenoperation dieser Gruppe ersetzt.

Dieser abstrakten Auffassung entspricht der Begriff des *Isomorphismus*. Ein *Homomorphismus* zwischen zwei Gruppen G und H ist eine Abbildung $\phi : G \rightarrow H$, die die Gruppenoperationen erhält:

$$\phi(g * g') = \phi(g) * \phi(g'), \quad \phi(g^{-1}) = \phi(g)^{-1}$$

für alle $g, g' \in G$. Ein *Isomorphismus* zwischen G und H ist ein umkehrbarer Homomorphismus $\phi : G \rightarrow H$; seine Umkehrabbildung $\psi = \phi^{-1}$ ist dann automatisch auch ein Homomorphismus.⁷¹ Die beiden Gruppen G und H können völlig unterschiedlich definiert sein; wenn sie *isomorph* sind, d.h. wenn es einen Isomorphismus $\phi : G \rightarrow H$ gibt,

⁶⁹Sind A, B Mengen, so bezeichnet $A \times B$ die *Paarmenge* oder das *kartesische Produkt* von A und B , d.h. die Menge der Paare

$$A \times B = \{(a, b) : a \in A, b \in B\}.$$

⁷⁰Niels Henrik Abel, 1802 (Frindoe bei Stavanger) - 1829 (Froland, Norwegen)

⁷¹Für alle $h, h' \in H$ ist $\phi(\psi(h * h')) = h * h'$ und $\phi(\psi(h) * \psi(h')) = \phi(\psi(h)) * \phi(\psi(h')) = h * h'$, also $\phi(\psi(h * h')) = \phi(\psi(h) * \psi(h'))$. Anwenden von ϕ^{-1} auf beiden Seiten ergibt $\psi(h * h') = \psi(h) * \psi(h')$. Ebenso $\phi(\psi(h^{-1})) = \phi(\psi(h))^{-1}$ und daraus $\psi(h^{-1}) = \psi(h)^{-1}$.

betrachten wir sie als gleich. Wir schreiben $G \cong H$, wenn G und H isomorphe Gruppen sind.

Beispiel 1: Die Permutationen der Menge $\{1, \dots, n\}$ bilden eine Gruppe, die wir S_n nennen (“Symmetrische Gruppe”);⁷² bei ihr ist die Gruppenoperation die Verkettung, $* = \circ$, und das Neutralelement ist die identische Abbildung, $e = \text{id}$. Diese Gruppe ist nicht kommutativ für $n \geq 3$.

Beispiel 2: Der ganzen Zahlen \mathbb{Z} mit der Addition bilden eine kommutative Gruppe; dort ist $* = +$ und $e = 0$, und das Inverse von $n \in \mathbb{Z}$ wird mit $-n$ bezeichnet. Das Gesetz (G3) in \mathbb{Z} lautet dann $n + (-n) = (-n) + n = 0$.

Beispiel 3: Die Menge der *Einheitswurzeln*

$$\Omega_n = \{x \in \mathbb{C} : x^n = 1\} = \{e^{2\pi ik/n} : k = 1, \dots, n\}$$

mit der Multiplikation bildet eine kommutative Gruppe;⁷³ hier ist $* = \cdot$ die Multiplikation und das Neutralelement ist $e = 1$.

Definition: Eine *Untergruppe* einer Gruppe $(G, *)$ ist eine Teilmenge $H \subset G$, die selbst eine Gruppe bildet, weil sie unter der Gruppenoperation und der Inversion von G erhalten bleibt: Für alle Elemente $h, h' \in H$ gilt:

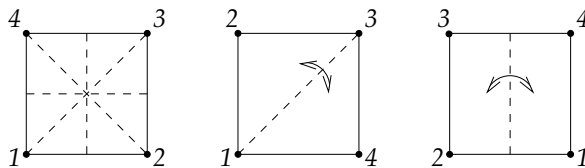
- UG1:** $e \in H$,
- UG2:** $h * h' \in H$,
- UG3:** $h^{-1} \in H$.

Ein Beispiel einer Untergruppe der Symmetrischen Gruppe ist die *Symmetriegruppe* einer Figur, eines Polygons (Vielecks) in der Ebene \mathbb{R}^2 .⁷⁴ Das ist die Menge der Drehungen und Spiegelungen, die die Figur invariant lässt. Schaltet man zwei Symmetrien hintereinander, erhält man wieder eine Symmetrie, und die Identität und die Inverse einer Symmetrie sind wieder Symmetrien, deshalb bilden die Symmetrien eine Gruppe, eine Untergruppe der Permutationen der Eckpunkte.

⁷²Der Name kommt von den *symmetrischen Polynomen* her, Abschnitt 12.1. Dies sind genau diejenigen Polynome in n Variablen x_1, \dots, x_n , die unter allen Permutationen der Variablenmenge $\{x_1, \dots, x_n\}$ unverändert (“invariant”) bleiben.

⁷³In der Tat ist Ω_n eine Untergruppe (s.u.) einer viel größeren Gruppe, der Gruppe $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ aller nichtverschwindenden komplexen Zahlen mit der Multiplikation als Gruppenoperation.

⁷⁴Das Polygon im \mathbb{R}^2 kann auch durch einen Polyeder (Vielflächner) im \mathbb{R}^3 oder sogar im \mathbb{R}^n ersetzt werden.



Bei einem Quadrat zum Beispiel seien die Ecken zyklisch mit den Zahlen 1,2,3,4 bezeichnet. In seiner Symmetriegruppe liegen die Permutationen 1432 (Spiegelung an der Diagonalen von 1 nach 3) und 2143 (Spiegelung an der senkrechten Mittellinie), aber nicht z.B. die Permutation 2134, genauer $1234 \mapsto 2134$, weil 2 und 3 durch eine Kante des Quadrats verbunden sind, ihre Bilder 1 und 3 aber nicht. Die Symmetrien des Vierecks bilden also eine echte Teilmenge der Permutationsgruppe S_4 , und zwar eine Untergruppe, denn die Komposition und die Umkehrung von Symmetrien sind Symmetrien.

16. GRUPPENWIRKUNGEN

Eine *Wirkung* (*Operation*) einer Gruppe G auf einer Menge X ist eine Abbildung $\phi : G \times X \rightarrow X$, Kurzschreibweise $\phi(g, x) = \phi_g(x) = gx$, mit folgenden Eigenschaften:

GW1: $ex = x$,

GW2: $g(hx) = (gh)x$

für alle $g, h \in G$ und $x \in X$, wobei e das Neutralelement von G ist.⁷⁵ Zum Beispiel ist die *Symmetrische Gruppe* (Permutationsgruppe) $G = S_n$ bereits durch ihre Wirkung auf $X = \{1, \dots, n\}$ definiert. Dieselbe Gruppe wirkt aber auch auf anderen Mengen, zum Beispiel auf der Menge $X = \mathbb{K}[x_1, \dots, x_n]$ der Polynome in n Veränderlichen durch Permutation der Variablen.⁷⁶ Ebenso wirkt die Symmetriegruppe einer Figur auf den Punkten dieser Figur, besonders den Eckpunkten. Jede Gruppe G wirkt auf drei verschiedene Weisen auf sich selbst ($X = G$): durch *Linkstranslation* $\phi_g(x) = gx$, durch *Rechtstranslation* $\phi_g(x) = xg^{-1}$ und durch *Konjugation* $\phi_g(x) = gxg^{-1}$.

⁷⁵Man kann auch sagen: Eine Gruppenwirkung ist ein Homomorphismus $\phi : G \rightarrow \text{Bij}(X)$, $g \mapsto \phi_g$ von G in die Gruppe der bijektiven Abbildungen von X auf sich. Die Gesetze GW1 und GW2 sind genau die Gesetze für einen Gruppenhomomorphismus.

⁷⁶Nach Definition ist $\sigma f(x_1, \dots, x_n) = f(x_{\sigma 1}, \dots, x_{\sigma n})$ für alle $\sigma \in S_n$ und alle $f \in \mathbb{K}[x_1, \dots, x_n]$. Wir müssen (GW1) und (GW2) zeigen. Offensichtlich gilt $\sigma f = f$ für $\sigma = \text{id}$. Wenn $\sigma, \tau \in S_n$, dann ist $\tau f(x_1, \dots, x_n) = f(x_{\tau 1}, \dots, x_{\tau n}) =: g(x_1, \dots, x_n)$. Also ist $\sigma(\tau f)(x_1, \dots, x_n) = \sigma g(x_1, \dots, x_n) = g(x_{\sigma 1}, \dots, x_{\sigma n}) \stackrel{\tilde{x}_j := x_{\sigma j}}{=} g(\tilde{x}_1, \dots, \tilde{x}_n) = f(\tilde{x}_{\tau 1}, \dots, \tilde{x}_{\tau n}) \stackrel{\tilde{x}_{\tau k} := x_{\sigma \tau k}}{=} f(x_{\sigma \tau 1}, \dots, x_{\sigma \tau n}) = (\sigma \tau) f(x_1, \dots, x_n)$.

Ist eine Wirkung einer Gruppe G auf einer Menge X gegeben, so ist für jedes $x \in X$ die Menge

$$G_x = \{g \in G : gx = x\} \quad (55)$$

eine Untergruppe von G , denn $ex = x$ und mit $g, h \in G_x$ ist $gh \in G_x$, weil $(gh)x = g(hx) = gx = x$, und falls $g \in G_x$, ist auch $g^{-1} \in G_x$, denn $g^{-1}x = g^{-1}gx = ex = x$. Diese Untergruppe heißt *Standgruppe* oder *Stabilisator* von x unter der Gruppenwirkung ϕ . Jedes $x' = gx \in Gx$ ist gleichberechtigt; es gilt $Gx' = Gx$.

Die Teilmenge von X , die aus einem Element x durch Anwenden aller Elemente von G entsteht, heißt *Bahn* oder *Orbit* von x , geschrieben

$$Gx = \{gx : g \in G\}. \quad (56)$$

Alle Elemente $gx, g \in G$, einer Bahn sind gleichberechtigt, denn wegen (GW2) gilt $Ggx = Gx$. Die Standgruppe für jedes $gx \in Gx$ ist *konjugiert* zu G_x :

$$G_{gx} = gG_xg^{-1}, \quad (57)$$

denn für jedes $h \in G_x$ ist $ghg^{-1}(gx) = ghx = gx$, also ist $gG_xg^{-1} \subset G_{gx}$, aber umgekehrt ist aus demselben Grund $g^{-1}G_{gx}g \subset G_x$, also $G_{gx} \subset gG_xg^{-1}$.

Satz 16.1. *Die Anzahl der Elemente einer Bahn Gx (mit $|G| < \infty$) ist*

$$|Gx| = |G|/|G_x|. \quad (58)$$

Beweis. Das ist Teil einer allgemeineren Aussage: Gegeben endliche Mengen A, B und eine surjektive⁷⁷ Abbildung $f : A \rightarrow B$. Zu jedem $b \in B$ sei $f^{-1}(b) := \{a \in A : f(a) = b\}$ das *volle Urbild* von b . Für $b, \tilde{b} \in B$ mit $b \neq \tilde{b}$ sind $f^{-1}(b)$ und $f^{-1}(\tilde{b})$ *disjunkt*, $f^{-1}(b) \cap f^{-1}(\tilde{b}) = \emptyset$, denn kein a wird gleichzeitig auf b und \tilde{b} abgebildet. Also ist A die disjunkte Vereinigung der $f^{-1}(b)$, $b \in B$ und damit gilt

$$|A| = \sum_{b \in B} |f^{-1}(b)|. \quad (59)$$

Dies wenden wir an auf die surjektive Abbildung $f : G \rightarrow Gx$, $f(g) = gx$. Das Urbild von x ist $f^{-1}(x) = \{g \in G : gx = x\} = G_x$, und das Urbild von $gx \in Gx$ ist $f^{-1}(gx) = \{\tilde{g} \in G : \tilde{g}x = gx\}$, und $\tilde{g}x = gx$

⁷⁷ $f : A \rightarrow B$ ist *surjektiv*, wenn $f(A) = B$, d.h. jedes $b \in B$ ist wirklich von der Form $f(a)$, es gibt $a \in A$ mit $b = f(a)$

$\iff g^{-1}\tilde{g}x = x \iff g^{-1}\tilde{g} \in G_x \iff \tilde{g} \in gG_x := \{gh : h \in G_x\}$.⁷⁸
 Also ist $|f^{-1}(gx)| = |gG_x| = |G_x|$. Alle Urbilder haben also gleich viele Elemente k und (59) spezialisiert sich zu $|A| = |B| \cdot k$. In unserem Fall ist $k = |G_x|$, also $|G| = |Gx| \cdot |G_x|$. \square

Bemerkung: Die Standgruppe G_{gx} ist genau dann gleich für jedes $gx \in Gx$, wenn $gG_xg^{-1} = G_x$ für alle $g \in G$; solche Untergruppen nennt man *normale* Untergruppen oder *Normalteiler*.⁷⁹ Allgemeiner ist der Durchschnitt aller Standgruppen G_{gx} ein Normalteiler. In dem zu Beginn des Abschnitts 13 skizzierten Auflösungsverfahren kam es darauf an, dass die “halbinvarianten” Polynome y eine kurze Bahn bilden. Dann sind die Standgruppen groß und haben deshalb einen gemeinsamen Schnitt. Im Fall $n = 3$ ist dieser Durchschnitt die Gruppe $A_3 = \{e, (123), (132)\}$, im Fall $n = 4$ ist es die *Kleinsche Vierergruppe*

$$V = \{e, (12)(34), (13)(24), (14)(23)\}.$$

Beides sind abelsche Normalteiler. Ab $n = 5$ besitzt die S_n nur noch die alternierende Gruppe A_n (siehe folgenden Abschnitt) als einzigen Normalteiler, und dieser ist nicht-abelsch und enthält selbst keine Normalteiler mehr. Wie wir sehen werden, ist dies der Grund, warum es für die allgemeine Gleichung mit Grad ≥ 5 keine Auflösungsformeln geben kann.

⁷⁸Ist $H \subset G$ eine Untergruppe, so heißt die Teilmenge $gH = \{gh : h \in H\} \subset G$ die *Nebenklasse* von H durch g . Die Menge der Nebenklassen (eine Menge von Teilmengen von G) bezeichnen wir mit $G/H = \{gH : g \in G\}$. Wir zeigen hier, dass die Elementen von G/G_x genau die Urbilder von $f : g \mapsto gx$ sind und dass G/G_x somit bijektiv auf Gx abgebildet wird.

⁷⁹Ist $H \subset G$ eine Untergruppe, so operiert H auf G durch $\phi : (h, g) \mapsto gh^{-1} : H \times G \rightarrow G$. Die Bahnen dieser Wirkung, die Mengen $gH = \{gh^{-1} : h \in H\}$ für jedes $g \in G$ heißen *Nebenklassen*, und die Menge der Bahnen (Nebenklassen) wird mit G/H bezeichnet. Da $|gH| = |H|$ für alle $g \in G$, haben alle Bahnen gleich viele Elemente, und da G die disjunkte Vereinigung aller gH ist, folgt $|G| = \sum_{gH \in G/H} |gH| = |G/H| \cdot |H|$. Insbesondere ist $|H|$ ein Teiler von $|G|$; das ist der *Satz von Lagrange*.

Im Fall, dass $H \subset G$ ein *Normalteiler* ist, wird G/H selbst zu einer Gruppe: Das Neutralelement ist eH , die Gruppenmultiplikation $gH \cdot \tilde{g}H := g\tilde{g}H$ und das Inverse von gH ist $g^{-1}H$. Gruppenmultiplikation und Inverses sind “wohldefiniert”, hängen also nur von gH und $\tilde{g}H$, nicht von g und \tilde{g} ab: Wenn wir $g \in gH$ durch $gh \in gH$ und $\tilde{g} \in \tilde{g}H$ durch $\tilde{g}h' \in \tilde{g}H$ ersetzen, dann ist $gh\tilde{g}h'H = gh\tilde{g}H = g\tilde{g}h^{-1}h\tilde{g}H = g\tilde{g}h'H = g\tilde{g}H$, weil $h' = \tilde{g}^{-1}h\tilde{g} \in H$ (Normalteiler-Eigenschaft). Ebenso gilt $(gh)^{-1}H = h^{-1}g^{-1}H = g^{-1}gh^{-1}g^{-1}H = g^{-1}h''H = g^{-1}H$, weil $h'' = gh^{-1}g^{-1} \in H$.

17. DIE ALTERNIERENDE GRUPPE

Eine interessante Untergruppe von S_n ist die *Alternierende Gruppe* A_n . Um diese zu definieren, bemerken wir zunächst, dass sich jede Permutation als Komposition von *Transpositionen* schreiben lässt. Transpositionen sind Vertauschungen (ij) von nur zwei Zahlen $i, j \in \{1, \dots, n\}$; alle anderen Zahlen behalten ihren Platz bei. Dies folgt aus der fast offensichtlichen Tatsache, dass man jede Anordnung durch eine Folge von Vertauschungen in die natürliche Reihenfolge bringen kann.⁸⁰ Die Alternierende Gruppe⁸¹ A_n besteht aus denjenigen Permutationen, die Komposition einer *geraden* Anzahl von Transpositionen ist; sie werden *gerade Permutationen* genannt. Sie bilden tatsächlich eine Untergruppe: Das Neutralelement kann man durch zwei (oder null) Transpositionen $(12)(12)$ schreiben, die Komposition von zwei Produkten von Transpositionen mit jeweils einer geraden Zahl von Faktoren ist gerade, und das Inverse eines Produktes $\sigma = \tau_1 \circ \dots \circ \tau_{2k}$ von Transpositionen τ_1, \dots, τ_{2k} ist wieder von der gleichen Form, nämlich $\sigma^{-1} = \tau_{2k} \circ \dots \circ \tau_1$.

Dennoch gibt es ein Problem. Die Darstellung einer Permutation als Komposition von Transpositionen ist nämlich keineswegs eindeutig, zum Beispiel gilt $231 = (13) \circ (12)$, aber auch $231 = (12) \circ (23)$. Könnte es da nicht auch eine Permutation σ geben, die sowohl durch eine gerade wie durch eine ungerade Anzahl von Transpositionen dargestellt werden kann? Dann wäre die A_n gar keine echte Untergruppe, denn durch Nachschalten von σ könnte man aus jeder ungeraden eine gerade Permutation machen. Aber dies ist nicht der Fall: Zwar kann die Anzahl der benötigten Transpositionen durchaus bei verschiedenen Darstellungen unterschiedlich sein (zum Beispiel könnte man ja eine Transposition 2-mal hinzufügen), aber ihre *Parität* (gerade - ungerade) bleibt immer die gleiche. Um dies zu sehen, muss man die Parität von Permutationen etwas anders definieren, unabhängig von einer speziellen Darstellung.

Dazu benötigt man den Begriff des *Fehlstandes* einer Permutation σ . Ein *Fehlstand* ist ein Zahlenpaar (i, j) mit $i < j$ und $\sigma(i) > \sigma(j)$.

⁸⁰Induktion über $n \geq 2$: $n = 2$: S_2 besteht nur aus $\text{id} = (12)(12)$ und (12) . $n - 1 \rightarrow n \geq 3$: Ist eine beliebige Permutation $\sigma = k_1 \dots k_n \in S_n$ gegeben, so ist die Zahl n irgend eines der k_j , mit $\sigma(j) = n$. Schalten wir die Transposition $\tau = (jn)$ davor, so ist $\sigma(\tau(n)) = \sigma(j) = n$, also ist $\sigma' = \sigma \circ \tau \in S_{n-1}$, weil $\sigma'(n) = n$. Nach Induktionsvoraussetzung ist σ' Komposition von Transpositionen und damit auch $\sigma = \sigma' \circ \tau$.

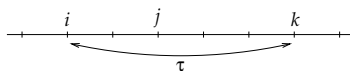
⁸¹ Der Name kommt von den *alternierenden* Polynomen her, Polynome in den Variablen x_1, \dots, x_n , die bei Vertauschung von je zwei Variablen ihr Vorzeichen ändern, wie zum Beispiel $x_1^2 x_2 - x_2^2 x_1$. Solche Polynome sind unter Permutationen in A_n invariant, weil eine gerade Anzahl von Vorzeichenänderungen sich aufhebt.

Zum Beispiel hat $\sigma : 1234 \mapsto 2341$ die Fehlstände 14 (da $2 > 1$), 24 (da $3 > 1$), 34 (da $4 > 1$); die übrigen Zahlenpaare 12, 13, 23 sind keine Fehlstände. Die Anzahl der Fehlstände ist also ungerade (gleich 3).

Lemma 17.1. *Die Anzahl der Fehlstände einer Permutation σ hat die gleiche Parität wie die Anzahl der Transpositionen in jeder beliebigen Darstellung von σ als Komposition von Transpositionen.*

Beweis. Es genügt zu zeigen, dass die Komposition von σ mit einer beliebigen Transposition $\tau = (ik)$ die Parität der Fehlstände-Anzahl ändert. Die Transposition τ hat genau die folgenden Fehlstände:

- (1) (i, k) ,
- (2) (i, j) mit $i < j < k$,
- (3) (j, k) mit $i < j < k$.



Da die Anzahl der Paare unter (2) und (3) gleich ist (nämlich gleich $r =$ Länge des Zwischenraums zwischen k und i , also $r = k - i - 1$), ist die Zahl der Fehlstände von τ ungerade, nämlich $2r + 1$. Also verdreht τ eine ungerade Anzahl von Paaren ij , und die Parität der Fehlstände von σ und $\tau \circ \sigma$ ist unterschiedlich. Das Neutralelement id hat keinen Fehlstand. Ist nun $\sigma = \tau_r \circ \dots \circ \tau_1 \circ \text{id}$, dann wechselt die Anzahl der Fehlstände mit jeder neu hinzukommenden Transposition τ_j die Parität, insgesamt r -mal. Die Fehlständezahl von σ hat demnach die gleiche Parität wie r . \square

18. DIE GALOISGRUPPE

Gegeben sei ein Polynom $f \in \mathbb{K}[x]$,

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_0 \quad (60)$$

mit Koeffizienten in einem Körper \mathbb{K} , dem *Koeffizientenkörper*, zum Beispiel $\mathbb{K} = \mathbb{Q}$. Wir interessieren uns für die Gleichung $f(x) = 0$. Die Lösungen (Wurzeln) seien $\alpha_1, \dots, \alpha_n$. Wir setzen voraus, dass alle α_j voneinander verschieden sind, dass also die Diskriminante ungleich Null ist (was man ja aus den Koeffizienten ablesen kann).⁸² Die *Galoisgruppe* G ist die Symmetriegruppe der Wurzeln: diejenige Untergruppe

⁸²Ein solches Polynom heißt *separabel*. Wenn f nicht *irreduzibel* über \mathbb{K} ist, dann heißt f separabel, wenn alle irreduziblen Faktoren separabel sind. Wir werden aber etwas mehr voraussetzen, nämlich dass alle Nullstellen voneinander verschieden sind.

der Permutationsgruppe S_n der Menge $\{\alpha_1, \dots, \alpha_n\}$, die die bekannten⁸³ algebraischen Relationen zwischen den Wurzeln erhalten. Es sei uns also eine Menge $R \subset \mathbb{K}[x_1, \dots, x_n]$ (“Relationen”) bekannt⁸⁴ mit⁸⁵

$$H(\vec{\alpha}) := H(\alpha_1, \dots, \alpha_n) = 0 \quad (61)$$

für alle $H \in R$. Die *Galoisgruppe* ist dann die folgende Untergruppe G von S_n :

$$G = \{\sigma \in S_n : \sigma H \in R \text{ für alle } H \in R\} \quad (62)$$

Beispiel 1: Bekannt sind uns stets die Relationen $e_j(\vec{\alpha}) = (-1)^j a_j$ des Vietaschen Wurzelsatzes (vgl. Abschnitt 11), weil ja die Koeffizienten a_j gegeben sind. Da die e_j symmetrische Polynome sind, gilt automatisch $e_j(\sigma \vec{x}) = e_j(\vec{x})$.

Beispiel 2: Wenn das Polynom f reduzibel ist, $f = gh$ für zwei Polynome g, h (über unserem Koeffizientenkörper) vom Grad k und $n-k$, so ist jede Wurzel von f eine Wurzel von g oder h , denn $g(x)h(x) = 0 \Rightarrow g(x) = 0$ oder $h(x) = 0$. Wenn g und h keine gemeinsamen Nullstellen haben, können wir annehmen, dass die ersten k Nullstellen $\alpha_1, \dots, \alpha_k$ zu g gehören und $\alpha_{k+1}, \dots, \alpha_n$ die Nullstellen von h sind. Dann haben wir viel mehr Relationen zwischen den Wurzeln: Die elementarsymmetrischen Funktionen in $\alpha_1, \dots, \alpha_k$ sind (bis auf das Vorzeichen) die Koeffizienten von g , die in $\alpha_{k+1}, \dots, \alpha_n$ die Koeffizienten von h . Die beiden Sorten von Nullstellen werden durch die Elemente der Galoisgruppe nicht vermischt. Wenn keine weiteren Relationen vorliegen, ist G das *direkte Produkt* der symmetrischen Gruppen S_k (Permutationen von x_1, \dots, x_k) und S_{n-k} (Permutationen von x_{k+1}, \dots, x_n), d.h. als Menge ist G das kartesische Produkt (Menge der Paare) $S_k \times S_{n-k}$,

⁸³Später werden wir *alle* $h \in \mathbb{K}[x_1, \dots, x_n]$ mit $h(\alpha_1, \dots, \alpha_n) = 0$ als “bekannt” ansehen. Das Problem dabei ist, dass wir vielleicht nicht alle diese Ausdrücke kennen. Unser Vorwissen über die Gleichung geht also in unsere Definition der Galoisgruppe ein. Die Galoisgruppe ist in diesem Sinn nicht einem einzigen Polynom zugeordnet, sondern allen Polynomen, für die diese Relationen gelten. Manchmal können wir aber sehen, dass wirklich alle Relationen berücksichtigt sind, siehe Fußnote 88. In Teil II werden wir diese Frage systematisch lösen.

⁸⁴Sind Relationen $H_1, \dots, H_r \in R$ gegeben, also $H_i(\vec{\alpha}) = 0$ für $i = 1, \dots, r$, so sind auch alle Linearkombinationen H von (nicht-leeren) Produkten der H_1, \dots, H_r “bekannte” Relationen, denn offensichtlich gilt $H(\vec{\alpha}) = 0$. Das gleiche gilt für HJ mit $J \in R$ und beliebiges $J \in \mathbb{K}[\vec{x}]$; alle solche Polynome müssen in R aufgenommen werden. R ist ein *Ideal* im Ring $\mathbb{K}[\vec{x}]$.

⁸⁵Zur Unterscheidung wollen wir die Elemente von $\mathbb{K}[\vec{x}]$ möglichst mit Großbuchstaben bezeichnen.

und die Gruppenoperationen sind komponentenweise definiert.⁸⁶ Das gilt entsprechend für $r \geq 2$ Faktoren, $f = f_1 \dots f_r$. Wenn wir wissen, dass f über unserem Koeffizientenkörper in Linearfaktoren zerfällt, ist die Galoisgruppe also trivial (besteht nur aus dem Neutralelement), weil jeder Linearfaktor $x - \alpha_j$ jeweils nur eine Wurzel besitzt.

Beispiel 3: Die Diskriminante $\Delta(\vec{x}) = \pm \prod_{i \neq j} (x_i - x_j)$ ist eine symmetrische Funktion von \vec{x} und damit durch die Koeffizienten a_j ausdrückbar (vgl. Seite 33). Die Gleichung $\prod_{i \neq j} (\alpha_i - \alpha_j) = \pm \Delta$ ist daher noch keine neue Relation zwischen den Wurzeln. Aber in dem Ausdruck $\prod_{i \neq j} (x_i - x_j)$ kommt ja jeder Faktor doppelt vor mit unterschiedlichem Vorzeichen, $x_i - x_j$ und $x_j - x_i$. Eine Quadratwurzel von $\Delta(\vec{x})$ ist daher der Ausdruck

$$D(\vec{x}) = \prod_{i < j} (x_i - x_j). \quad (63)$$

Wenn uns diese Quadratwurzel $D = \sqrt{\Delta}$ ebenfalls bekannt ist, dann haben wir eine weitere Relation $\prod_{i < j} (\alpha_i - \alpha_j) = D$, die nicht mehr von allen Permutationen invariant gelassen wird, denn jede Transposition dreht in einem Faktor das Vorzeichen um.⁸⁷ Nur die geraden Permutationen lassen diese Relation invariant, da sie bei einer geraden Anzahl von Faktoren in D das Vorzeichen ändern. Die Galoisgruppe wird in diesem Fall also A_n oder (wenn noch weitere Relationen bekannt sind) eine Untergruppe davon sein.

Beispiel 4: Für die Gleichung $x^n = 1$, also $f(x) = x^n - 1$, ist bekannt, dass für jede Wurzel α (*Einheitswurzel*) auch die Potenzen α^k Wurzeln sind, denn $(\alpha^k)^n = (\alpha^n)^k = 1^k = 1$. Wählen wir α_1 als die Wurzel mit dem kleinsten Winkel, $\alpha_1 = \zeta := e^{2\pi i/n}$, dann sind alle anderen Wurzeln Potenzen davon:

$$\alpha_j = (\alpha_1)^j. \quad (64)$$

Dies sind Relationen zwischen den Wurzeln, die von den Elementen der Galoisgruppe G respektiert werden müssen.⁸⁸ Ist $\sigma \in G$ mit $\sigma(\alpha_1) = \alpha_k = (\alpha_1)^k$, so muss deshalb auch $\sigma(\alpha_j) = \sigma(\alpha_1)^j$ gelten, also

$$\sigma(\alpha_1^j) = (\alpha_1^k)^j = (\alpha_1^j)^k.$$

⁸⁶Sind G, H Gruppen, so sind die Gruppenoperationen im direkten Produkt $G \times H$ folgendermaßen definiert: $(g, h) * (g', h') = (g * g', h * h')$ und $(g, h)^{-1} = (g^{-1}, h^{-1})$. Das Neutralelement ist $e = (e_G, e_H)$.

⁸⁷ $D(\vec{x})$ ist ein *alternierendes Polynom*, vgl. Fußnote 81.

⁸⁸Fügt man noch die Gleichung $\alpha_n = 1$ hinzu, dann ist es tatsächlich nur die Gleichung $x^n = 1$, deren Lösungen diese Relationen erfüllen, denn aus (64) folgt $(\alpha_1)^n = 1$ und $(\alpha_j)^n = (\alpha_1)^{nj} = 1$, also sind $\alpha_1, \dots, \alpha_n$ genau die Lösungen der Gleichung $x^n = 1$.

Damit gilt $\sigma(\alpha) = \alpha^k$ für alle Wurzeln α , d.h. σ ordnet jeder Wurzel ihre k -te Potenz zu. Allerdings eignet sich nicht jede Potenz k , zum Beispiel $k = n$ nicht, denn $\alpha^n = 1$ für jede Wurzel α ; die Abbildung $\alpha \mapsto \alpha^n$ ist also nicht umkehrbar auf der Menge der Wurzeln. Allgemein kann $\pi_k : \alpha \mapsto \alpha^k$ keine Permutation der Wurzeln sein, wenn

$$(*) \quad (\alpha_j)^k = 1$$

für irgend ein $j < n$. Aber $\alpha_j = (\alpha_1)^j$, somit ist $(*)$ äquivalent zu $1 = (\alpha_j)^k = (\alpha_1)^{jk}$, was bedeutet, dass jk ein Vielfaches von n sein muss, $jk = rn$ (keine anderen Potenzen von α_1 sind gleich 1). Damit haben k und n einen gemeinsamen Teiler.⁸⁹ Umgekehrt, wenn k und n einen gemeinsamen Teiler t haben, also $k = k't$ und $n = n't$, dann folgt $k'n = k'n't = kn'$. Daraus folgt $(*)$ für $j = n'$, denn $(x_{n'})^k = (x_1^{n'})^k = (x_1^n)^{k'} = 1$. Also ist

$$G = \{\pi_k : \alpha \mapsto \alpha^k : k < n, \text{ggT}(k, n) = 1\}.$$

Die Einheitswurzeln $(\alpha_1)^k$ mit $\text{ggT}(k, n) = 1$ sind also genauso gut wie α_1 selber; ihre Potenzen durchlaufen die ganze Einheitswurzel-Menge $\Omega_n = \{\alpha \in \mathbb{C} : \alpha^n = 1\}$. Sie heißen *primitive Einheitswurzeln*.

Beispiel 5: Die Gleichung $x^n = a$ hat die Lösungen

$$\alpha_j = \zeta^j \sqrt[n]{a} \quad (65)$$

für $j = 1, \dots, n$ mit $\zeta := e^{2\pi i/n}$. Dabei ist a gegeben (“bekannt”), aber $\sqrt[n]{a}$ und ζ kennen wir vielleicht nicht; deshalb können wir (65) nicht als algebraische Relation zwischen den Wurzeln ansehen (wenn doch, ist die Galoisgruppe trivial, d.h. sie besteht nur aus der identischen Permutation). Wir müssen (65) deshalb durch Relationen ersetzen, in denen $\sqrt[n]{a}$ und ζ nicht mehr vorkommen. Der Quotient von zwei Wurzeln ist schon besser, denn er enthält $\sqrt[n]{a}$ nicht mehr:

$$\alpha_j/\alpha_k = \zeta^{j-k}. \quad (66)$$

Vergleich von zwei solchen Ausdrücken ergibt eine Relation⁹⁰ ohne ζ ,

$$\alpha_j/\alpha_k = \alpha_p/\alpha_q \iff j - k =_n p - q. \quad (67)$$

Mit “ $=_n$ ” meinen wir, dass die Gleichung “modulo n ” zu lesen ist,⁹¹ also bis auf Addition von ganzen Vielfachen von n , da ja $x_j = x_{j+n}$

⁸⁹Aus $jk = rn$ folgt, dass $\frac{rn}{k} = j$ ganzzahlig ist. Wenn k und n keinen gemeinsamen Teiler hätten, müsste $\frac{r}{k}$ ganz sein, aber dann wäre $j = \frac{r}{k}n \geq n$, im Widerspruch zu $j < n$.

⁹⁰Hochmultiplizieren der Nenner macht aus (67) eine Polynomgleichung.

⁹¹Andere Schreibweise: $j - k \equiv p - q \pmod{n}$ oder $j - k \equiv p - q(n)$.

nach (65). Die Relation (67) muss unter jeder Permutation σ in der Galoisgruppe G erhalten bleiben, also

$$\sigma j - \sigma k =_n \sigma p - \sigma q \iff j - k =_n p - q. \quad (68)$$

Diese Bedingung wird von den Abbildungen $\tau_p : j \mapsto j + p$ sowie $\mu_m : j \mapsto mj$ (jeweils modulo n) für feste Zahlen p, m erfüllt. Während τ_p , die “Translation mit p modulo n ”, für jedes p eine Permutation von $\{1, \dots, n\}$ ist, gilt dies für μ_m (“Multiplikation mit m modulo n ”) nur für gewisse m . Zum Beispiel für $n = 4$ ist $\mu_2(2) = 4$ und $\mu_2(4) = 8 =_4 4$; also werden 2 und 4 auf den gleichen Wert 4 abgebildet und μ_2 ist daher keine Permutation der Zahlen $\{1, 2, 3, 4\}$. Dieses Unglück passiert immer dann, wenn n und m einen gemeinsamen Teiler p haben: $n = rp$ und $m = sp$. Dann ist nämlich $\mu_m(r) = spr = sn =_n \mu_m(n)$. Wenn dagegen m und n teilerfremd sind und $\mu_m(k) =_n \mu_m(k')$, dann teilt n das Produkt $m(k - k')$ und damit $k - k'$, also ist $k =_n k'$ und μ_m ist injektiv,⁹² also eine Permutation von $\{1, \dots, n\}$, denn für $k, l \in \{1, \dots, n\}$ bedeutet $k =_n l$ schon $k = l$.⁹³ Kombinieren wir die beiden Sorten von Permutationen, so erhalten wir⁹⁴

$$G = \{j \mapsto mj + p \bmod n : m, p \in \{1, \dots, n\}, \text{ggT}(m, n) = 1\}. \quad (69)$$

Wenn dagegen die Einheitswurzeln ζ^j als bekannt gelten, so muss die Galoisgruppe die stärkeren Relationen (66) erhalten: $\alpha_j = \zeta^{j-k} x_k$ oder $\zeta^j x_k = \alpha_{j+k}$. Insbesondere gilt $\alpha_j = \zeta^j \alpha_n$ und $\alpha_{\sigma j} = \zeta^j \alpha_{\sigma n}$ für alle $\sigma \in G$. Setzen wir $\sigma(n) = p$, so folgt

$$\alpha_{\sigma j} = \zeta^j \alpha_p = \alpha_{j+p},$$

also ist $\sigma j =_n j + p$. Es bleiben also nur die “Translationen” $j \mapsto j + p$ in (69).

Wenn dagegen eine n -te Wurzel $b = \sqrt[n]{a}$ bekannt ist (d.h. in unserem Koeffizientenkörper liegt), die Einheitswurzel ζ aber als unbekannt gilt, dann erfüllt $\tilde{x} = x/b$ die Gleichung $\tilde{x}^n = 1$ des vorigen Beispiels 4.

⁹² Eine Abbildung $f : X \rightarrow Y$ für zwei Mengen X, Y heißt *injektiv*, wenn $f(x) \neq f(x')$ für alle $x, x' \in X$ mit $x \neq x'$. Oder im Umkehrschluss: Wenn doch $f(x) = f(x')$ gilt, dann muss auch schon $x = x'$ gelten. In unserem Zusammenhang: “ μ_m injektiv” heißt: $\mu_m(k) =_n \mu_m(k') \Rightarrow k =_n k'$.

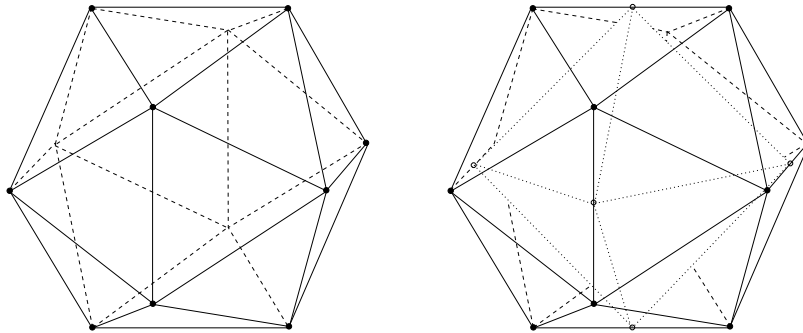
⁹³ Eine Permutation ist *bijektiv*, also gleichzeitig injektiv und *surjektiv*. Eine Abbildung $f : X \rightarrow Y$ heißt *surjektiv*, wenn ihr Bild $\text{Bild}(f) = f(X) = \{f(x) : x \in X\}$ bereits ganz Y ist. Wenn $Y = X$ und X eine endliche Menge mit n Elementen ist, dann folgt aus “injektiv” bereits “surjektiv”: Da f injektiv, hat $f(X)$ ebenso viele Elemente wie X . Andererseits ist $f(X)$ aber eine Teilmenge von X . Also müssen in $f(X)$ schon alle n Elemente von X vorkommen, denn mehr gibt es nicht.

⁹⁴Eine Funktion der Form $j \mapsto mj + p$ nennt man *affin*; die Galoisgruppe G der Gleichung $x^n = a$ besteht also aus den umkehrbaren affinen Funktionen modulo n .

19. DIE LÖSUNG DER QUINTISCHEN GLEICHUNG

Lösungsformeln für die Gleichungen dritten und vierten Grades wurden schon im 16. Jahrhundert gefunden, aber die Gleichung 5. Grades widerstand allen Versuchen, eine Lösungsformel zu finden. Erst um 1800 gelang es Ruffini⁹⁵ und Abel zu zeigen, dass es keine Lösungsformel geben kann, die außer den vier Grundrechenarten nur Wurzeln (beliebigen Grades) benutzt, wir werden noch sehen, warum. Aber Hermite⁹⁶ und Felix Klein⁹⁷ fanden dennoch einen Lösungsweg, der hier kurz skizziert werden soll.⁹⁸

Wir nehmen an, dass eine Diskriminantenwurzel D bekannt ist (vgl. Beispiel 2 auf Seite 53); die Galoisgruppe der quintischen Gleichung ist daher die Gruppe A_5 , vgl. Seite 50. Diese Gruppe wiederum hat mit einem der platonischen Körper zu tun, dem *Ikosaeder*, der von zwanzig gleichseitigen Dreiecken mit 12 Eckpunkten und 30 Kanten begrenzt wird.



Wir können das Ikosaeder so positionieren, dass 6 der 30 Kanten parallel zu den drei Raumachsen sind; die Mittelpunkte dieser Kanten können wir durch die Kanten eines einbeschriebenen *Oktaeders*⁹⁹ verbinden. Nach einer Drehung des Ikosaders übernehmen 6 andere Kanten diese Rolle. Somit enthält das Ikosaeder $30/6 = 5$ Oktaeder, die durch die Drehungen des Ikosaders permutiert werden. Auf diese Weise definiert jede Ikosaederdrehung eine Permutation der Menge der einbeschriebenen Oktaeder, die wir mit der Zahlenmenge $\{1, \dots, 5\}$ identifizieren können, und verschiedene Drehungen definieren verschiedene

⁹⁵Paolo Ruffini, 1765 (Valentano) - 1822 (Modena)

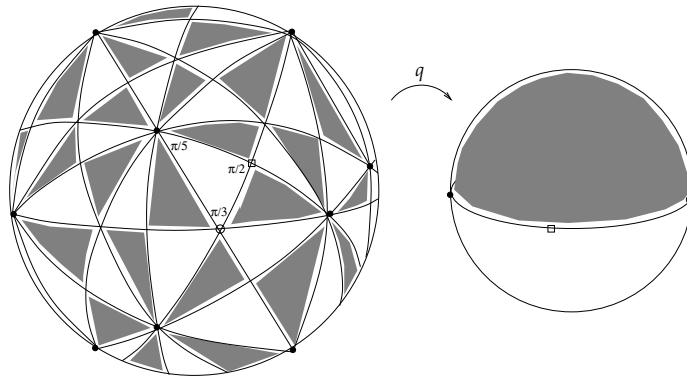
⁹⁶Charles Hermite, 1822 (Dieuze, Lothringen) - 1901 (Paris)

⁹⁷Felix Klein, 1849 (Düsseldorf) - 1925 (Göttingen)

⁹⁸J.-H. Eschenburg, L. Hefendehl-Hebeker: Die Gleichung 5. Grades: Ist Mathematik erzählbar? Math. Semesterberichte 47 (2000), 193 - 220, www.math.uni-augsburg.de/~eschenbu

⁹⁹Das Oktaeder ist die Doppelpyramide über einem Quadrat, begrenzt von 8 gleichseitigen Dreiecken.

Permutationen. Die Ikosaedergruppe wird dadurch zu einer Untergruppe der Gruppe S_5 , die $5! = 120$ Elemente besitzt. Weil der Ikosaeder 20 Flächen hat, deren jede nach oben gedreht werden kann, und jede Fläche von drei Kanten berandet wird, deren jede nach vorne gedreht werden kann, gibt es $20 \cdot 3 = 60$ Positionen des Ikosaeders und ebenso viele Drehungen. Die Ikosaedergruppe wird damit zu einer Untergruppe mit 60 Elementen von S_5 , und die einzige solche Untergruppe ist die A_5 . Die Drehgruppe des Ikosaeders ist also isomorph zur A_5 . Wenn wir jedes der 20 Dreiecke durch die Schwerelinien in 6 Teildreiecke aufteilen und das so entstandene Muster auf die Kugelfläche auftragen, die die Ikosaederecken enthält, dann entstehen auf der Kugelfläche 120 sphärische Dreiecke mit Winkeln $\frac{\pi}{2}$, $\frac{\pi}{3}$ und $\frac{\pi}{5}$. Jedes zweite Dreieck wird gefärbt, und die Drehgruppe des Ikosaeders bildet alle gefärbten Dreiecke ebenso wie alle ungefärbten aufeinander ab.



Wir betrachten nun eine Funktion q von der Kugelfläche auf die Kugelfläche, die die gefärbten Dreiecke auf die obere Halbkugel und die ungefärbten auf die untere Halbkugel abbildet und dabei invariant unter der Ikosaedergruppe ist: $q(gx) = q(x)$ für alle Punkte x der Kugelfläche und jede Ikosaederdrehung g . Wenn wir die Kugelfläche mit $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ identifizieren,¹⁰⁰ wobei eine der Ikosaederecken auf den Punkt ∞ zu liegen kommt, dann kann man q als Quotienten von Polynomen (rationale Funktion) ausdrücken: $q = f^3/h^5$ mit Polynomen f, h , deren Koeffizienten aus den gegebenen Daten berechnet werden können (die genauen Formeln sind für uns aber nicht bedeutsam):

$$\begin{aligned} 12f(x) &= x^{20} - 228x^{15} + 494x^{10} + 228x^5 + 1 \\ h(x) &= x^{11} - 11x^6 - x \end{aligned}$$

¹⁰⁰Das geschieht mit Hilfe der *Stereographischen Projektion*; vgl. z.B. mein Skriptum "Geometrie", Seite 82, auf www.math.uni-augsburg.de/~eschenbu.

Diese rationale Funktion q übernimmt die Rolle der k -ten Potenz, der rationalen Funktion $x \mapsto x^k$; ihre Umkehrfunktion¹⁰¹ wird die neu benötigte Rechenart sein, analog zur k -ten Wurzel, der Umkehrung der k -ten Potenz.

Gegeben sei nun eine allgemeine Gleichung 5. Grades. Durch *Tschirnhaus-Transformationen* kann man die ersten beiden Koeffizienten zum Verschwinden bringen und die Gleichung in der Form

$$x^5 + ax^2 + bx + c = 0 \quad (70)$$

schreiben. Weil der x^4 -Koeffizient verschwindet, gilt die lineare Beziehung

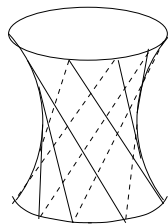
$$e_1(\vec{x}) = x_1 + \cdots + x_5 = 0. \quad (71)$$

Weil auch der x^3 -Koeffizient verschwindet, gilt die quadratische Beziehung $e_2(\vec{x}) = 0$, aber wegen $p_2 = e_1^2 - 2e_2$ (mit $p_2(\vec{x}) = \sum_i x_i^2$) kann diese Beziehung auch in der Form

$$p_2(\vec{x}) = x_1^2 + \cdots + x_5^2 = 0 \quad (72)$$

geschrieben werden. Das ist wegen (71) eigentlich eine Gleichung in vier Variablen, da z.B. $x_5 = -(x_1 + \cdots + x_4)$. Außerdem genügt es, $\vec{x} = (x_1, \dots, x_5)$ nur bis auf ein Vielfaches zu bestimmen, also nur $\vec{x}' = t\vec{x}$ mit unbekanntem $t \in \mathbb{C}$. Denn $e_3(\vec{x}') = t^3 e_3(\vec{x}) = -t^3 a$ und analog $e_4(\vec{x}') = t^4 b$, also ist $t = -\frac{ae_4(\vec{x}')}{be_3(\vec{x}')}$ leicht zu berechnen. Wir können also eine der fünf Koordinaten willkürlich gleich Eins setzen; dann wird (72) zu einer Beziehung zwischen drei Koordinaten. Die Lösungsmenge dieser quadratischen Gleichung ist eine *Fläche* (zwei Koordinaten lassen sich willkürlich vorgeben, dann kann die dritte aus der Gleichung berechnet werden), eine "Quadrik" Q . Wir kennen solche Quadriken aus der reellen Geometrie, zum Beispiel den Hyperboloiden

$$Q_H = \{(x, y, z) : x^2 + y^2 - z^2 = 1\}.$$



¹⁰¹Die Funktion q ist natürlich nicht eindeutig umkehrbar: Ist x ein Punkt im Inneren eines der Dreiecke, sagen wir, eines gefärbten, so hat $q(x)$ in jedem anderen gefärbten Dreieck ebenfalls ein Urbild x' mit $q(x') = q(x)$. Alle diese 60 Urbilder stehen für die Umkehrfunktion zur Auswahl, ähnlich wie ja auch die k -te Wurzel $\sqrt[k]{y}$ k verschiedene Werte annehmen kann.

Das Besondere: Auf dieser krummen Fläche liegen zwei Scharen von Geraden! Diese zweifache Geradenschar sieht man noch einfacher, wenn man (72) (nach Einsetzen von $x_5 = -(x_1 + \dots + x_4)$ und $x_4 = 1$) durch eine lineare Variablensubstitution $\vec{x} = \vec{x}(\lambda, \mu, \nu)$ auf die Form

$$\lambda\mu = \nu \quad (73)$$

gebracht hat, denn für jedes konstante λ oder μ beschreibt diese Gleichung eine Gerade. Über den reellen Zahlen gibt es zwar auch Quadriken ohne Geraden, zum Beispiel die Sphäre, die Lösungsmenge der Gleichung $x^2 + y^2 + z^2 = 1$, aber über den komplexen Zahlen können wir jede (nicht-entartete) Quadrik durch eine lineare Substitution auf die Form (73) bringen.

Jede Permutation $\sigma \in S_5$ erhält die Gleichungen (71), (72) und damit ihre Lösungsmenge, die Quadrik Q . Außerdem bildet σ Geraden auf Geraden ab. Wenn σ gerade ist ($\sigma \in A_5$), so werden die Geraden der beiden Scharen $\lambda = \text{const}$ und $\mu = \text{const}$ auf Geraden der gleichen Schar abgebildet, die ungeraden Permutationen dagegen vertauschen die beiden Scharen. Jedes $\sigma \in A_5$ wirkt also auf den Punkten (λ, μ) in der Form $(\lambda, \mu) \mapsto (\sigma_1(\lambda), \sigma_2(\mu))$, und die Abbildungen $\sigma_j : \hat{\mathbb{C}} \rightarrow \hat{\mathbb{C}}$ ($j = 1, 2$) sind Ikosaederdrehungen, wobei $\hat{\mathbb{C}}$ wieder mit der Kugel­fläche identifiziert wird. Also sind $q(\lambda)$ und $q(\mu)$ invariant unter der A_5 und daher berechenbare Funktionen der Koeffizienten a, b, c .¹⁰² Durch Umkehrung von q gewinnen wir λ aus $q(\lambda)$ und μ aus $q(\mu)$ und aus λ, μ und $\nu = \lambda\mu$ den Vektor \vec{x}' und daraus schließlich \vec{x} .

¹⁰²Wenn ein Polynom $f(\vec{x})$ nur unter A_n statt S_n invariant ist, setzen wir $f^*(\vec{x}) = f(x_2, x_1, x_3, \dots)$. Dann sind $f + f^*$ und $(f - f^*)^2$ invariant unter S_n und daher rationale Funktionen der elementarsymmetrischen Polynome e_i . Damit sind auch f und f^* aus den Koeffizienten berechenbar.

II. Körpererweiterungen

20. KÖRPER

Bisher haben wir einige Methoden kennen gelernt, um Gleichungen zu lösen. Galois und seinen Vorgängern (Ruffini, Gauß, Abel) ging es aber auch darum zu verstehen, warum viele Gleichungen eben *nicht* durch einfache Formeln gelöst werden können. Damit zusammen hängt die Unlösbarkeit einiger geometrischer Konstruktionsprobleme mit Zirkel und Lineal, die schon in der Antike gestellt worden sind, die sog. Delischen Probleme:¹⁰³ Warum kann man jeden Winkel mit Zirkel und Lineal halbieren, aber nicht dritteln? Warum kann man das Quadrat verdoppeln, aber nicht den Würfel? Auch die Quadratur des Kreises gehört in diese Reihe [5].

Dazu müssen wir an den Begriff des *Körpers* erinnern, eines Zahlbereichs, in dem alle vier Grundrechenarten unbeschränkt durchgeführt werden können; nur das Teilen durch die Null ist unmöglich. Um die Frage zu klären, mit welchen Hilfsmitteln (Formeln oder geometrische Mittel) eine Gleichung zu lösen ist, genügt nicht die Feststellung, dass wir alle Lösungen im Körper \mathbb{C} der komplexen Zahlen finden können. Stattdessen müssen wir von einem Körper \mathbb{K} ausgehen, dem *Koeffizientenkörper*, dessen Elemente uns als "bekannt" gelten und der insbesondere die Koeffizienten a_1, \dots, a_n unserer Gleichung

$$f(x) = x^n + a_1x^{n-1} + \dots + a_n = 0 \quad (74)$$

enthält. Wenn diese Koeffizienten zum Beispiel ganze Zahlen sind, können wir $\mathbb{K} = \mathbb{Q}$ wählen, den Körper der *rationalen Zahlen*

$$\mathbb{Q} = \{k/n : k \in \mathbb{Z}, n \in \mathbb{N}\}. \quad (75)$$

Dem gegenüber steht der Körper \mathbb{L} , der *Lösungskörper*, der auch noch alle Lösungen $\alpha_1, \dots, \alpha_n$ von (74) enthält. Natürlich können wir $\mathbb{L} = \mathbb{C}$ wählen, aber wir wollen genauer sein: Wir suchen den *kleinsten* Körper \mathbb{L} , der sowohl \mathbb{K} als auch $\alpha_1, \dots, \alpha_n$ enthält. Wir nennen ihn den *Zerfällungskörper* von f , denn er ist der kleinste Körper, der \mathbb{K} enthält und in dem f in Linearfaktoren zerfällt, $f(x) = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_n)$.

Hier ist die offizielle Definition eines Körpers:

¹⁰³Angeblich befragten die Bewohner der kleinen griechischen Insel Delos, die im Jahre 430 v. Chr. von einer Pestepidemie heimgesucht wurde, das Orakel von Delphi um Rat. Das Orakel empfahl als Mittel zur Erlösung von der Seuche, den würfelförmigen Altar im Tempel des Apollon dem Rauminhalte nach zu verdoppeln, unter Beibehaltung der würfelförmigen Gestalt. <http://www.ebeltberatung.de/ZumDelischenProblem.pdf>

Definition. Ein *Körper* ist eine Menge \mathbb{K} mit zwei verschiedenen ausgezeichneten Elementen, Null 0 und Eins 1 benannt, und vier Abbildungen $+, \cdot : \mathbb{K} \times \mathbb{K} \rightarrow \mathbb{K}$ (Addition und Multiplikation) sowie $- : \mathbb{K} \rightarrow \mathbb{K}$ und $(\)^{-1} : \mathbb{K}^* \rightarrow \mathbb{K}^*$ (additiv und multiplikativ Inverses) mit $\mathbb{K}^* = \mathbb{K} \setminus \{0\}$ mit folgenden Eigenschaften:

K1: $(\mathbb{K}, 0, +, -)$ ist eine abelsche Gruppe,

K2: $(\mathbb{K}^*, 1, \cdot, (\)^{-1})$ ist eine abelsche Gruppe,

K3: $a \cdot (b + c) = a \cdot b + a \cdot c \quad \forall a, b, c \in \mathbb{K}$ (“Distributivgesetz”)¹⁰⁴

Statt $a + (-b)$ schreiben wir $a - b$ (Differenz), für $a \cdot b$ auch ab und für $a(b)^{-1}$ auch ab^{-1} oder a/b (Quotient).

Mit diesen grundlegenden Rechengesetzen (Axiomen) haben wir den Begriff “Körper” definiert. Damit sind keineswegs alle bekannten Rechengesetze aufgelistet, sie folgen aber aus diesen Grundregeln. Zum Beispiel:

1: *Irgendwas mal Null gleich Null:* $a \cdot 0 = 0 = 0 \cdot a \quad \forall a \in \mathbb{K}$,

denn $a \cdot 0 \stackrel{K1}{=} a \cdot (0 + 0) \stackrel{K3}{=} a \cdot 0 + a \cdot 0$, und durch Subtraktion von $a \cdot 0$ (Addition von $-(a \cdot 0)$) auf beiden Seiten folgt $0 = a \cdot 0$.

2: *Minus mal Plus gleich Minus:* $(-a) \cdot b = -(a \cdot b) \quad \forall a, b \in \mathbb{K}$,

denn $(-a) \cdot b + a \cdot b \stackrel{K3}{=} ((-a) + a) \cdot b \stackrel{K1}{=} 0 \cdot b \stackrel{1}{=} 0$, und durch Subtraktion von $a \cdot b$ (Addition von $-(a \cdot b)$) auf beiden Seiten folgt $(-a) \cdot b = -(a \cdot b)$.

3: *Minus mal Minus gleich Plus:* $(-a) \cdot (-b) = a \cdot b \quad \forall a, b \in \mathbb{K}$,

denn $(-a) \cdot (-b) + (-a \cdot b) \stackrel{2}{=} (-a) \cdot (-b) + (-a) \cdot b \stackrel{K3}{=} (-a) \cdot ((-b) + b) \stackrel{K1}{=} (-a) \cdot 0 \stackrel{1}{=} 0$, woraus durch Addition von $a \cdot b$ auf beiden Seiten die Behauptung folgt.

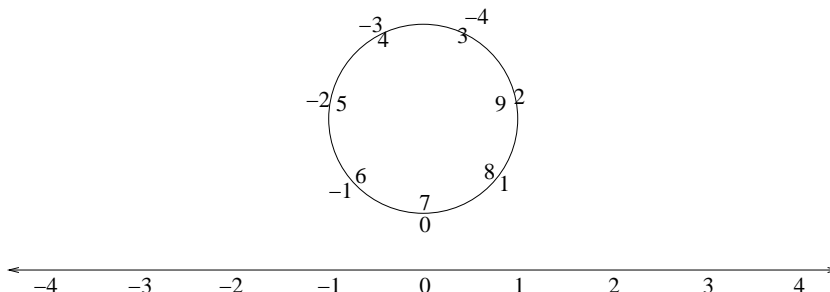
Beispiele von Körpern haben wir schon kennengelernt: \mathbb{Q} , \mathbb{R} und \mathbb{C} . Dagegen bilden die ganzen Zahlen $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ keinen Körper (sondern nur einen *Ring*),¹⁰⁵ denn man kann in \mathbb{Z} nicht unbeschränkt dividieren; $1/4$ oder $3/5$ sind keine ganzen Zahlen mehr.

Erstaunlicherweise kann sich dieser Befund ändern, wenn wir die ganzen Zahlen nicht wie gewöhnlich auf einer Geraden anordnen, sondern im Kreis, so dass nach einer Runde immer zwei Zahlen aufeinanderfallen,

¹⁰⁴Das Symbol \forall ist die Abkürzung für “für alle”.

¹⁰⁵In einem Ring R (mit Eins) wird das Axiom (K2) abgeschwächt: $(R \setminus \{0\}, 1, \cdot)$ ist keine Gruppe, denn das Gruppenaxiom (G3) (Existenz des Inversen, Seite 45) gilt nicht mehr unbeschränkt. Die Menge der invertierbaren Elemente (zu denen 1 gehört) bilden aber immer noch eine Gruppe R^\times mit der Multiplikation als Gruppenoperation. Diese kann aber sehr klein sein, z.B. $\mathbb{Z}^\times = \{1, -1\}$.

wobei wir Zahlen, die auf der Kreislinie an derselben Stelle stehen, als “gleich” ansehen.



Auf dem Kreis in unserer Figur wird jede siebte Zahl als gleich angesehen, also beispielsweise 1 und 8 oder 2 und 9, wie bei den Wochentagen: Jeder siebte Tag hat den gleichen Namen (z.B. Montag). Das ist die Rechnung “modulo 7”, die wir schon benutzt haben (Seite 54). Zwei Zahlen $p, p' \in \mathbb{Z}$ werden modulo 7 genau dann als gleich (“kongruent”) angesehen ($p =_7 p'$ oder $p \equiv p' (7)$), wenn sie auf dem Kreis an derselben Stelle stehen, wenn also $p' - p$ ein ganzes Vielfaches von 7 ist, oder noch anders ausgedrückt, wenn p' und p bei Division durch 7 den gleichen Rest lassen, zum Beispiel $4 : 7 = 0$ Rest 4 und $11 : 7 = 1$ Rest 4, aber auch $-3 : 7 = -1$ Rest 4 (denn $(-1) \cdot 7 = -7$ und $-7 + 4 = -3$). Die Mengen kongruenter Zahlen modulo 7, wie beispielsweise $\{\dots, -10, -3, 4, 11, 18, \dots\}$, werden deshalb auch als *Restklassen modulo 7* bezeichnet.¹⁰⁶ Wir können modulo 7 wie gewohnt rechnen.¹⁰⁷ Damit finden wir dann doch ein multiplikativ Inverses zu 4, eine ganze Zahl x mit $4 \cdot x =_7 1$, nämlich $x = 2$, weil $4 \cdot 2 = 8 =_7 1$. Ebenso sehen wir $3 \cdot 5 =_7 1$ und¹⁰⁸ $6 \cdot 6 =_7 1$, denn $15 = 2 \cdot 7 + 1 =_7 1$ und $36 = 5 \cdot 7 + 1 =_7 1$. Damit hat jede Zahl $n \neq_7 0$ ein multiplikativ Inverses modulo 7, und wir können wieder unbeschränkt dividieren (außer durch Null). Die Restklassen ganzer Zahlen modulo 7 bilden daher einen Körper mit 7

¹⁰⁶Noch eine weitere Interpretation: Die Menge $7\mathbb{Z} = \{7k : k \in \mathbb{Z}\}$ ist eine Untergruppe der Gruppe $(\mathbb{Z}, +)$, die auf \mathbb{Z} durch *Translation* wirkt (vgl. Seite 47: $\phi : 7\mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$, $\phi(7k, n) = n + 7k$). Die Restklassen modulo 7 sind die Bahnen dieser Wirkung. Die Menge der Bahnen einer Gruppe G , die auf einer Menge X wirkt, bezeichnet man mit X/G , hier also mit $\mathbb{Z}/7\mathbb{Z}$.

¹⁰⁷Dazu ist eigentlich etwas zu zeigen, nämlich: Wenn $p' =_7 p$ und $q' =_7 q$, dann gilt auch $p' + q' =_7 p + q$ und $p' - q' =_7 p - q$ und $p' \cdot q' =_7 p \cdot q$. Dies folgt, weil $p' = p + 7j$ und $q' = q + 7k$ für gewisse $j, k \in \mathbb{Z}$. Erst mit dieser Zusatzüberlegung wird klar, dass die Ergebnisse von modulo-Rechnungen nicht davon abhängen, welches Element der Restklasse (z.B. 4 oder -3) ich jeweils für die Rechnung benutzt habe.

¹⁰⁸Besser noch kann man $6 =_7 -1$ benutzen; dann ist $6 \cdot 6 =_7 (-1) \cdot (-1) = 1$.

Elementen, den wir mit¹⁰⁹ \mathbb{F}_7 bezeichnen. Die 7 Elemente können wir mit 1, 2, 3, 4, 5, 6, 7 oder auch mit $-3, -2, -1, 0, 1, 2, 3$ (oder mit noch anderen Elementen von jeder Restklasse) bezeichnen.

Ebenso können wir \mathbb{F}_p für jede Primzahl p definieren als Menge der Restklassen modulo p ; jedes \mathbb{F}_p bildet einen Körper.¹¹⁰ In diesem Sinne gibt jede einzelne Primzahl p Anlass zu einem jeweils unterschiedlichen endlichen Körper \mathbb{F}_p , einer eigenen Rechenwelt. Speziell für $p = 2$ erhalten wir den kleinstmöglichen Körper $\mathbb{F}_2 = \{0, 1\}$. Es gibt genau zwei Restklassen modulo 2, die Menge der geraden Zahlen und die der ungeraden, wobei 0 für die geraden und 1 für die ungeraden steht.

In \mathbb{F}_p gilt offensichtlich die Gleichung

$$p \cdot 1 := \underbrace{1 + \cdots + 1}_{p\text{-mal}} = 0.$$

Einen Körper mit dieser Eigenschaft nennen wir *von Charakteristik p* . Wir werden sehen, dass es außer \mathbb{F}_p noch viele andere endliche Körper der Charakteristik p gibt, nämlich jeweils einen zu jeder Potenz p^k von p . In Körpern wie $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ gilt keine Gleichung $p \cdot 1 = 0$, nur $0 \cdot 1 = 0$; deshalb heißen diese Körper *von Charakteristik Null*.

21. KÖRPERERWEITERUNGEN

Wenn man Lösungen von Gleichungen $f(x) = 0$ finden will, muss man oft den ursprünglichen Körper, in dem die Koeffizienten der Gleichung liegen, zu einem größeren Zahlbereich erweitern: Die Lösungen

¹⁰⁹Die englische Bezeichnung für den mathematischen Begriff "Körper" ist "field", daher der Buchstabe \mathbb{F} .

¹¹⁰Zum Beweis müssen wir zeigen, dass wir unbeschränkt dividieren können: Zu jeder Zahl $m \neq_p 0$ gibt es eine ganze Zahl x mit $m \cdot x =_p 1$. Das folgt weil die Abbildung $\mu_m : x \mapsto m \cdot x : \mathbb{F}_p \rightarrow \mathbb{F}_p$ surjektiv ist, vgl. Seite 55, bes. Fußnote 93. Hier ist eine zweite Beweisversion, die etwas abstraktere Algebra benutzt und sich deshalb auch auf Polynome anstelle ganzer Zahlen übertragen lässt: Die Menge $p\mathbb{Z} = \{pn : n \in \mathbb{Z}\} \subset \mathbb{Z}$ ist nicht nur eine Untergruppe von $(\mathbb{Z}, +)$, sondern ein *Ideal*. Eine Teilmenge T eines Ringes R heißt *Ideal*, wenn $rt \in T$ für alle $r \in R$ und $t \in T$ gilt, kurz, wenn $RT \subset T$. Solch ein Ideal ist $p\mathbb{Z}$, und weil p eine Primzahl ist, ist es *maximal*: Es gibt keine Ideale T zwischen $p\mathbb{Z}$ und \mathbb{Z} , $p\mathbb{Z} \subset T \subset \mathbb{Z}$, außer $p\mathbb{Z}$ und \mathbb{Z} selber. Diese Eigenschaft vererbt sich auf den Ring $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$: Es gibt keine Ideale zwischen $\{0\}$ und \mathbb{F}_p . Deshalb ist \mathbb{F}_p ein Körper: Für jedes $m \in \mathbb{F}_p$ ist $m\mathbb{F}_p$ ein Ideal, muss also gleich \mathbb{F}_p sein, insbesondere gilt $1 \in m\mathbb{F}_p$ und somit gibt es ein $x \in \mathbb{F}_p$ mit $mx = 1$.

Warum ist das Ideal $p\mathbb{Z}$ maximal? Um das zu sehen, betrachten wir ein Ideal T mit $p\mathbb{Z} \subset T \subset \mathbb{Z}$. Wenn T ein Element q enthält, das nicht in $p\mathbb{Z}$ liegt, dann ist nach dem euklidischen Algorithmus $r = \text{ggT}(q, p)$ auch in T , vgl. Fußnote 8. Weil p eine Primzahl und $q \notin p\mathbb{Z}$, folgt $r = 1$, also ist $1 \in T$ und damit $T = \mathbb{Z} \cdot 1 = \mathbb{Z}$.

der Gleichung $x^2 = x + 1$ mit rationalen (sogar ganzzahligen) Koeffizienten sind nicht mehr rational, wie wir im Abschnitt 2 sahen, ebenso wenig wie die der Gleichung $x^2 = p$ für jede Primzahl p . Die Lösungen der Gleichung $x^2 + 1 = 0$ sind nicht einmal mehr reell.

Wir werden es daher gewöhnlich mit zwei Körpern zu tun haben, dem Koeffizientenkörper \mathbb{K} und einem größeren \mathbb{L} mit $\mathbb{K} \subset \mathbb{L}$, in dem eine oder mehrere Lösungen liegen. Die Rechenoperationen in \mathbb{K} sind die von \mathbb{L} , nur eben auf Elemente der Teilmenge $\mathbb{K} \subset \mathbb{L}$ angewandt. Dann heißt \mathbb{K} ein *Teilkörper* von \mathbb{L} und \mathbb{L} ein *Erweiterungskörper* von \mathbb{K} . Genauer gilt:

Definition: Ein *Teilkörper* eines Körpers \mathbb{L} ist eine Teilmenge $\mathbb{K} \subset \mathbb{L}$ mit folgender Eigenschaft: Für alle $x, y \in \mathbb{K}$ sind $x + y$, $x - y$, $x \cdot y$, x/y (falls $y \neq 0$) wieder Elemente von \mathbb{K} .

Wenn man also die Rechenoperationen von \mathbb{L} auf Elemente der Teilmenge \mathbb{K} anwendet, bleibt man in \mathbb{K} , und damit erfüllt \mathbb{K} ebenfalls die Körperaxiome (Seite 61). Schwieriger scheint die Umkehrung: Wie konstruiere ich Erweiterungskörper eines gegebenen Körpers \mathbb{K} mit bestimmten Eigenschaften? Wir können dafür abstrakte Konstruktionen der Algebra verwenden.¹¹¹ Aber wenn unser Ausgangskörper \mathbb{K} ein Teilkörper von \mathbb{C} ist und wir eine Nullstelle eines Polynoms $f \in \mathbb{K}[x]$ suchen, sind wir in einer komfortableren Situation, weil \mathbb{C} ja diese Nullstelle bereits enthält; wir können \mathbb{L} also als Teilkörper von \mathbb{C} konstruieren.¹¹² Wenn $\alpha \in \mathbb{C} \setminus \mathbb{K}$ die gesuchte Nullstelle ist, $f(\alpha) = 0$, dann erweitern wir \mathbb{K} um dieses Element α und nehmen alle Elemente hinzu, die sich aus \mathbb{K} und α durch Anwenden der vier Grundrechenarten ergeben; den so konstruierten Teilkörper von \mathbb{C} (den kleinsten Körper, der \mathbb{K} und α enthält) nennen wir $\mathbb{K}(\alpha)$; wir sagen, dass α zu \mathbb{K} adjungiert ist.

¹¹¹ Zum Beispiel gibt es folgende Konstruktion: Ist $f \in \mathbb{K}[x]$ ein irreduzibles Polynom, also eins, das sich nicht mehr als $f = gh$ zerlegen lässt für nichtkonstante Polynome $g, h \in \mathbb{K}[x]$ (analog zu einer Primzahl im Ring \mathbb{Z}), dann ist $(f) := f\mathbb{K}[x]$ ein maximales Ideal (dank dem euklidischen Algorithmus), und der Ring $\mathbb{L} = \mathbb{K}[x]/(f)$ ist daher ein Körper, entsprechend der zweiten Beweisversion in Fußnote 110. Wir schreiben die Elemente von \mathbb{L} (Restklassen von Polynomen modulo f) als $[g]$ oder $[g(x)]$ für beliebige $g \in \mathbb{K}[x]$. Die Konstanten in \mathbb{K} liegen als Teilkörper in \mathbb{L} , und das Polynom $x \in \mathbb{K}[x]$ wird zu einem Element $[x] \in \mathbb{L}$. Setzen wir dieses in das Polynom $f(x) = x^n + a_1x^{n-1} + \dots + a_n$ ein, so erhalten wir $f([x]) = [f(x)] =$ Restklasse von f , aber diese ist ja gerade Null in $\mathbb{K}[x]/(f)$. Also haben wir abstrakt einen Körper \mathbb{L} konstruiert, in dem f eine Nullstelle besitzt.

¹¹²Das geht allerdings nicht, wenn wir z.B. Erweiterungskörper von \mathbb{F}_p suchen.

Wie groß ist $\mathbb{K}(\alpha)$? Wieviele neue Elemente haben wir uns “eingehandelt”? Ein Maß dafür ist der *Grad der Körpererweiterung*, den wir jetzt definieren wollen. Denken wir noch einmal an die Erweiterung von \mathbb{R} zu \mathbb{C} zurück, Abschnitt 7. Wir haben \mathbb{C} als $\mathbb{R} + i\mathbb{R}$ geschrieben. Entsprechend, wenn $\mathbb{L} \supset \mathbb{K}$ eine Körpererweiterung ist, suchen wir Elemente $\alpha_1, \dots, \alpha_n \in \mathbb{L}$ mit

$$\mathbb{L} = \mathbb{K} + \alpha_1\mathbb{K} + \dots + \alpha_n\mathbb{K}. \quad (76)$$

Wenn dies gelingt,¹¹³ nennen wir die Körpererweiterung *endlich* oder *algebraisch*, und die Menge $\{1, \alpha_1, \dots, \alpha_n\}$ nennen wir ein *Erzeugendensystem* von \mathbb{L} über \mathbb{K} . Der *Grad* der Körpererweiterung $\mathbb{L} \supset \mathbb{K}$, genannt $[\mathbb{L} : \mathbb{K}]$, ist dann die kleinstmögliche Zahl von Summanden in (76), die kleinstmögliche Anzahl der Elemente eines Erzeugendensystems. Um eine solche kleinstmögliche Darstellung zu erhalten, müssen wir ausschließen, dass eine *lineare Relation* zwischen den Elementen $1, \alpha_1, \dots, \alpha_n$ besteht, eine Gleichung der Form

$$c_0 + c_1\alpha_1 + \dots + c_n\alpha_n = 0 \quad (77)$$

mit $c_0, c_1, \dots, c_n \in \mathbb{K}$, die nicht alle gleichzeitig Null sind, denn in diesem Fall können wir mindestens eines der α_j durch die anderen ausdrücken, womit der Summand $\alpha_j\mathbb{K}$ in (76) entbehrlich wird. Man nennt $1, \alpha_1, \dots, \alpha_n$ *linear unabhängig über \mathbb{K}* , wenn diese notwendige Bedingung erfüllt ist und keine Relation der Form (77) besteht, außer der trivialen natürlich, wo alle Koeffizienten c_0, \dots, c_n gleich Null sind. Mit Linearer Algebra folgt, dass diese Bedingung bereits hinreichend ist: Ein linear unabhängiges Erzeugendensystem $\{1, \alpha_1, \dots, \alpha_n\}$, auch *Basis* genannt, hat bereits die minimale Anzahl von Elementen.¹¹⁴

¹¹³Dies muss keineswegs der Fall sein, nicht einmal, wenn wir \mathbb{K} nur durch eine einzige Zahl α erweitern: $\mathbb{L} = \mathbb{K}(\alpha)$ ist der kleinste Körper, der \mathbb{K} und α enthält. Aber es kann sein, dass α nicht *algebraisch* ist, nicht Nullstelle irgend eines Polynoms über \mathbb{K} . Dann ist $\mathbb{K}(\alpha) \supset \mathbb{K} + \alpha\mathbb{K} + \alpha^2\mathbb{K} + \dots$, und wir kommen an kein Ende. Solche Zahlen α und solche Körpererweiterungen heißen *transzendent*. Zum Beispiel ist die Zahl π transzendent, was 1882 von Ferdinand von Lindemann, 1852 (Hannover) - 1939 (München) bewiesen wurde.

¹¹⁴Für Hörerinnen und Hörer mit Vorkenntnissen in Linearer Algebra: Der Erweiterungskörper \mathbb{L} ist ein Vektorraum über \mathbb{K} ; wir können ja Elementen von \mathbb{L} addieren und mit “Skalaren” aus \mathbb{K} multiplizieren. Ein System $\{1, \alpha_1, \dots, \alpha_n\} \subset \mathbb{L}$, das (76) erfüllt, ist ein *Erzeugendensystem* dieses Vektorraums, und wenn es keine Relation der Form (77) gibt, ist es linear unabhängig. Sind beide Bedingungen erfüllt, so ist $\{1, \alpha_1, \dots, \alpha_n\}$ eine *Basis* des \mathbb{K} -Vektorraums \mathbb{L} . Die Anzahl $n + 1$ der Basiselemente ist die *Dimension* $\dim_{\mathbb{K}} \mathbb{L}$, und damit ist der Grad der Körpererweiterung die Dimension von \mathbb{L} über \mathbb{K} , $[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}} \mathbb{L}$.

Wie groß also ist $[\mathbb{K}(\alpha) : \mathbb{K}]$, wenn α Wurzel (Nullstelle) eines normierten Polynoms $f(x) = x^n + a_1x^{n-1} + \dots + a_n$ ist? Es gibt vielleicht verschiedene solche Polynome; wir wollen aber f so wählen, dass der Grad von f kleinstmöglich ist; dann heißt f *Minimalpolynom* für α .¹¹⁵ Eine Basis sollte die Elemente $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ enthalten, denn diese sind linear unabhängig (sonst wäre α Nullstelle eines Polynoms $c_{n-1}x^{n-1} + \dots + c_1x + c_0$ von kleinerem Grad), und sicherlich sind α^n und alle höheren Potenzen nicht in der Basis enthalten, weil

$$\alpha^n = -(a_1\alpha^{n-1} + \dots + a_n). \quad (78)$$

Also ist $\mathbb{K}[\alpha] := \mathbb{K} + \mathbb{K}\alpha + \dots + \mathbb{K}\alpha^{n-1} \subset \mathbb{K}(\alpha)$. Aber kommen wir damit aus? Wo ist zum Beispiel das Inverse α^{-1} ? In der Tat gilt:

Satz 21.1. *Ist α Nullstelle eines Polynoms $f \in \mathbb{K}[x]$ von kleinstmöglichem Grad n , so ist $\{1, \alpha, \dots, \alpha^{n-1}\}$ eine Basis von $\mathbb{K}(\alpha)$ über \mathbb{K} , und folglich ist $\mathbb{K}(\alpha) = \mathbb{K}[\alpha]$ und $[\mathbb{K}(\alpha) : \mathbb{K}] = n$.*

Beweis. Wir müssen nur zeigen, dass das Inverse β^{-1} eines Ausdrucks $0 \neq \beta = \alpha^m + b_1\alpha^{m-1} + \dots + b_m$ mit $b_1, \dots, b_m \in \mathbb{K}$ wieder von der gleichen Form $1/\beta = \alpha^k + c_1\alpha^{k-1} + \dots + c_k$ ist, also in $\mathbb{K}[\alpha]$ liegt. Dies machen wir durch Induktion über m . Für $m = 0$ ist $\beta = b \in \mathbb{K}$ in \mathbb{K} invertierbar. Für $m > 0$ dürfen wir $m < n$ annehmen, weil wir α^n und jede höhere Potenz von α mit (78) durch eine Summe niedrigerer α -Potenzen ersetzen können. Wir setzen $\gamma = \alpha^k + c_1\alpha^{k-1} + \dots + c_k$ mit $k = n - m$, wobei $c_1, \dots, c_k \in \mathbb{K}$ noch zu bestimmen sind, und berechnen $\delta = \beta\gamma$:

$$\begin{aligned} \delta &= (\alpha^m + b_1\alpha^{m-1} + \dots + b_m)(\alpha^k + c_1\alpha^{k-1} + \dots + c_k) \\ &= \alpha^n + (b_1 + c_1)\alpha^{n-1} + (b_2 + b_1c_1 + c_2)\alpha^{n-2} + \dots + b_m c_k \\ &\stackrel{(78)}{=} (b_1 + c_1 - a_1)\alpha^{n-1} + (b_2 + b_1c_1 + c_2 - a_2)\alpha^{n-2} + \dots + b_m c_k - a_n. \end{aligned}$$

Durch Wahl der Koeffizienten c_1, \dots, c_k von γ können wir die Koeffizienten von $\alpha^{n-1}, \dots, \alpha^{n-k}$ in δ zum Verschwinden bringen:

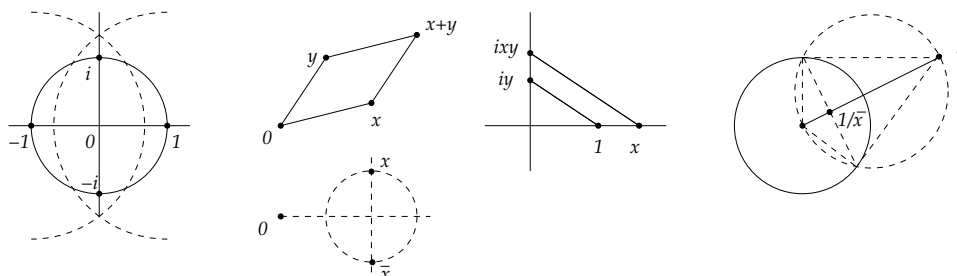
$$c_1 = a_1 - b_1, \quad c_2 = a_2 - b_2 - b_1c_1 = a_2 - b_2 - b_1(a_1 - b_1), \quad \dots$$

¹¹⁵ Das Minimalpolynom von α ist eindeutig: Sind f, g normierte Polynome vom Grad n , beide mit Nullstelle α , so sind f und g über $\mathbb{K}(\alpha)$ nicht teilerfremd. Dann sind sie auch über \mathbb{K} nicht teilerfremd, sonst würden sie $1 = \text{ggT}(f, g)$ darstellen: $1 = af + bg$ mit $a, b \in \mathbb{K}[x]$ (euklidischer Algorithmus). Da diese Gleichung in jedem Erweiterungskörper richtig bleibt, könnten f und g über $\mathbb{K}(\alpha)$ nicht $x - \alpha$ als gemeinsamen Teiler haben. Damit haben f und g einen gemeinsamen Teiler h über \mathbb{K} , und wenn $h \neq f$, gibt es ein Polynom von kleinerem Grad mit Nullstelle α , entweder h oder f/h .

Damit ist δ von kleinerem Grad als m in α und nach Induktionsvoraussetzung in $\mathbb{K}[\alpha]$ invertierbar. Somit ist auch $\beta^{-1} = \gamma\delta^{-1} \in \mathbb{K}[\alpha]$.¹¹⁶ \square

22. KONSTRUKTIONEN MIT ZIRKEL UND LINEAL

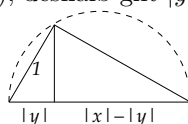
Bereits mit Satz 21.1 können wir zeigen, dass bestimmte in der Antike gestellte Konstruktionsprobleme mit Zirkel und Lineal nicht lösbar sind. Dazu müssen wir verstehen, welche Punkte der Ebene überhaupt mit Zirkel und Lineal konstruierbar sind. Wir geben zwei Punkte vor und betrachten sie als die Zahlen 0 und 1 in der komplexen Ebene \mathbb{C} . Wir wollen die Menge \mathbb{K} der konstruierbaren Zahlen kennen lernen. Mit dem Zirkel ziehen wir den Kreis durch 1 mit Mittelpunkt 0 und bekommen so auch die Zahl -1 als Schnitt dieses Kreises mit der Geraden durch 0 und 1, der reellen Achse. Da wir den 90-Grad-Winkel konstruieren können, erhalten wir auch die imaginäre Achse durch 0 senkrecht zur reellen und damit die Punkte $\pm i$ als Schnitt der imaginären Achse mit dem Kreis. Damit sind $\pm 1, \pm i \in \mathbb{K}$ (ganz links). Die weiteren Figuren zeigen, dass mit $x, y \in \mathbb{K}$ auch $x + y \in \mathbb{K}$ und für $x, y \in \mathbb{K} \cap \mathbb{R}$ auch $ixy \in \mathbb{K}$, also $xy = (-i)ixy \in \mathbb{K}$. Wenn x, y komplex sind, so setzen sich Real- und Imaginärteil des Produkts aus Produkten reeller Zahlen zusammen, siehe (13) auf Seite 16, deshalb gilt $xy \in \mathbb{K}$ für alle $x, y \in \mathbb{K}$. Die Zeichnung ganz rechts zeigt, dass mit $x \in \mathbb{K}$ auch $1/\bar{x} \in \mathbb{K}$,¹¹⁷ und damit auch $1/x \in \mathbb{K}$ (untere Figur). Somit ist \mathbb{K} ein Körper, ein Teilkörper von \mathbb{C} , der jedenfalls die rationalen Zahlen \mathbb{Q} umfasst.

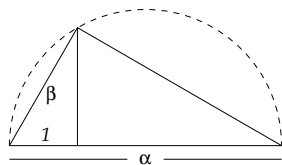


Aber es gilt noch mehr: Mit jedem $\alpha \in \mathbb{K}$ ist auch $\beta := \sqrt{\alpha} \in \mathbb{K}$.

¹¹⁶Ein alternativer Beweis benutzt Fußnote 111: $\mathbb{K}(\alpha)$ ist isomorph zu $\mathbb{K}[x]/(f)$ mit $\alpha \mapsto [f]$.

¹¹⁷Da $y := 1/\bar{x} = x/|x|^2$, liegen x und y auf einem gemeinsamen von 0 ausgehenden Strahl. Alle drei rechtwinkligen Dreiecke (Thales-Kreis!) in der nachfolgenden Figur sind ähnlich (gleiche Winkel), deshalb gilt $|y|/1 = 1/|x|$.





In der Figur ist $\beta = \sqrt{\alpha}$, denn wegen der Ähnlichkeit des linken und des großen rechtwinkligen Dreiecks gilt $\beta/1 = \alpha/\beta$ und damit $\beta = \sqrt{\alpha}$.

Wir halten also fest: Die Menge \mathbb{K} der konstruierbaren Zahlen bildet einen Erweiterungskörper von \mathbb{Q} , der “quadratisch abgeschlossen” ist, d.h. mit jedem $\alpha \in \mathbb{K}$ ist auch $\sqrt{\alpha} \in \mathbb{K}$. Andererseits wollen wir zeigen, dass \mathbb{K} nicht noch größer ist:

Satz 22.1. *Jede Konstruktion mit Zirkel und Lineal ist höchstens eine quadratische Erweiterung des Körpers der bereits konstruierten Zahlen.*

Beweis. Die bereits konstruierten Zahlen seien mit \mathbb{K} bezeichnet; sie bilden einen Körper mit $\mathbb{Q} \subset \mathbb{K} \subset \mathbb{C}$. Es gibt drei mögliche Konstruktionen neuer Punkte:

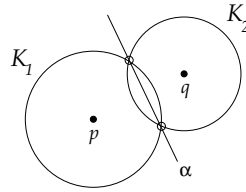
- (1) Schnitt von zwei Geraden,
- (2) Schnitt von Gerade und Kreis,
- (3) Schnitt von zwei Kreisen.

Zu (1): Die Geraden seien parametrisiert durch $\alpha(s) = as + b$ und $\beta(t) = ct + d$ mit $a, b, c, d \in \mathbb{K}$ und $s, t \in \mathbb{R}$. Dabei sind $a, c \neq 0$ und $a \notin \mathbb{R}c$, weil sonst die Geraden parallel oder identisch sind. Im Schnittpunkt gilt Gleichheit der beiden definierenden Ausdrücke: $as + b = ct + d$ oder $as - ct = d - b =: e$. Realteil und Imaginärteil dieser Gleichung sind zwei reelle lineare Gleichungen für die reellen Variablen s, t , und die Lösung ist ein rationaler Ausdruck¹¹⁸ in a, c, e .

Zu (2): Der Kreis mit Mittelpunkt $p \in \mathbb{K}$ und Radius $0 < r \in \mathbb{K}$ ist die Menge $K = \{x \in \mathbb{C} : |x - p|^2 = r^2\}$ mit $p, r \in \mathbb{K}$, $r > 0$, schneidet die Gerade $\alpha(t) = at + b$ (mit $a, b \in \mathbb{K}$) dort, wo $x = \alpha(t)$ die Gleichung $|x - p|^2 = r^2$ erfüllt. Das ist eine quadratische Gleichung für t mit Koeffizienten in \mathbb{K} : Mit $c = b - p \in \mathbb{K}$ ist $|\alpha(t) - p|^2 = |at + b - p|^2 = |at + c|^2 = (at + c)\overline{(at + c)} = t^2|a|^2 + t(a\bar{c} + \bar{a}c) + |c|^2$, also erfüllt $\alpha(t)$ die Gleichung (*) $\iff |a|^2 t^2 + (a\bar{c} - \bar{a}c)t = r^2 - |c|^2$.

Zu (3):

¹¹⁸(1) $a_1 s - c_1 t = e_1$, (2) $a_2 s - c_2 t = e_2 \implies$
 $a_2(1) - a_1(2): (a_1 c_2 - a_2 c_1)t = a_1 e_2 - a_2 e_1,$
 $c_2(1) - c_1(2): (c_2 a_1 - c_1 a_2)t = c_2 e_1 - c_1 e_2.$



Der Schnittpunkt von zwei Kreisen $K_1 = \{x : |x - p|^2 = r^2\}$ und $K_2 = \{x : |x - q|^2 = s^2\}$ mit $p, q, r, s \in \mathbb{K}$ wird auf (2) zurückgeführt. Zur Abkürzung setzen wir¹¹⁹ $\langle x, y \rangle := \operatorname{Re}(x\bar{y})$. Die Schnittpunkte erfüllen gleichzeitig die beiden Gleichungen

$$\begin{aligned} r^2 &= |x - p|^2 = |x|^2 + |p|^2 - 2\langle p, x \rangle, \\ s^2 &= |x - q|^2 = |x|^2 + |q|^2 - 2\langle q, x \rangle. \end{aligned}$$

Bilden wir die Differenz, so wird der quadratische Term $|x|^2$ eliminiert und mit $v = p - q \in \mathbb{K}$ und $u = |p|^2 - |q|^2 - r^2 + s^2 \in \mathbb{K}$ erhalten wir die Gleichung (*) $2\langle v, x \rangle = u$. Eine Lösung ist $x_o = \frac{1}{2}uv/|v|^2 \in \mathbb{K}$, denn $2\langle v, x_o \rangle = u\langle v, v \rangle/|v|^2 = u$. Ist x eine zweite Lösung, so gilt $2\langle v, x - x_o \rangle = 2\langle v, x \rangle - 2\langle v, x_o \rangle = u - u = 0$, also ist $x - x_o \in i\mathbb{R}v$, siehe Fußnote 119. Die Lösungen von (*) bilden also eine Gerade $x = \alpha(t) = x_o + tiv$ mit $t \in \mathbb{R}$ und $x_o, iv \in \mathbb{K}$, und der Schnittpunkt der beiden Kreise ist der Schnittpunkt der Geraden α mit einem der beiden Kreise. Nach (2) ist dazu wieder eine quadratische Gleichung mit Koeffizienten in \mathbb{K} zu lösen. \square

Der Körper der konstruierbaren Zahlen ist also eine iterierte Erweiterung von \mathbb{Q} durch immer neue Quadratwurzeln. Weil das Polynom $x^2 - a$ Grad 2 hat, ist jede solche Erweiterung vom Grad 2 (Satz 21.1). Das folgende Lemma zeigt, dass bei mehrfacher Erweiterung die Körpergrade multipliziert werden:

Lemma 22.1. *Sind $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{K}''$ endliche Körpererweiterungen, so gilt*

$$[\mathbb{K}'' : \mathbb{K}] = [\mathbb{K}'' : \mathbb{K}'] \cdot [\mathbb{K}' : \mathbb{K}]. \quad (79)$$

Beweis. Es seien

$$\{\alpha_i : i = 1, \dots, r\} \text{ und } \{\beta_j : j = 1, \dots, s\}$$

Basen von \mathbb{K}' über \mathbb{K} und von \mathbb{K}'' über \mathbb{K}' . Dann behaupten wir, dass

$$B = \{\alpha_i\beta_j : i = 1, \dots, r, j = 1, \dots, s\}$$

¹¹⁹ Ist $x = x_1 + x_2i$ und $y = y_1 + y_2i$ mit $x_1, y_1, x_2, y_2 \in \mathbb{R}$, dann ist $x\bar{y} + \bar{x}y = x\bar{y} + \overline{x\bar{y}} = 2\operatorname{Re} x\bar{y} = 2(x_1y_1 + x_2y_2)$; dies ist zweimal das Skalarprodukt $\langle x, y \rangle = x_1y_1 + x_2y_2$ der Vektoren $x, y \in \mathbb{R}^2 = \mathbb{C}$. Dieses ist gleich Null, wenn $x\bar{y}$ rein imaginär ist, $x\bar{y} \in i\mathbb{R}$, also $x|y|^2 = x\bar{y}y \in i\mathbb{R}y$ und damit $x \in i\mathbb{R}y$. Da die Multiplikation mit i geometrisch die 90-Grad-Drehung ist, bedeutet $x \in i\mathbb{R}y$, dass x und y senkrecht aufeinander stehen.

eine Basis von \mathbb{K}'' über \mathbb{K} ist. Dazu sind zwei Dinge zu zeigen:

B erzeugt \mathbb{K}'' über \mathbb{K} : Ist $\gamma \in \mathbb{K}''$, so ist $\gamma = \sum_j \lambda_j \beta_j$ mit $\lambda_j \in \mathbb{K}'$ und für jedes λ_j gibt es $\mu_{ij} \in \mathbb{K}$ mit $\lambda_j = \sum_i \mu_{ij} \alpha_i$, somit ist $\gamma = \sum_j \sum_i \mu_{ij} \alpha_i \beta_j$.

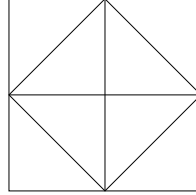
B ist linear unabhängig: Wenn es Zahlen $\nu_{ij} \in \mathbb{K}$ gibt mit $\sum_{i,j} \nu_{ij} \alpha_i \beta_j = 0$, also $\sum_j \mu_j \beta_j = 0$ mit $(*) \mu_j = \sum_i \nu_{ij} \alpha_i \in \mathbb{K}'$, dann sind alle $\mu_j = 0$, weil die $\beta_j \in \mathbb{K}''$ über \mathbb{K}' linear unabhängig sind, aber nach $(*)$ sind dann auch alle $\nu_{ij} = 0$, weil die $\alpha_i \in \mathbb{K}'$ über \mathbb{K} linear unabhängig sind. \square

Satz 22.2. *Wenn $\alpha \in \mathbb{K}$ in n Schritten aus rationalen Zahlen konstruierbar ist, dann liegt α in einer Körpererweiterung $\mathbb{K}' \supset \mathbb{Q}$ mit Grad $[\mathbb{K}' : \mathbb{Q}] = 2^k$ für ein $k \leq n$.*

Beweis. Jeder neue Konstruktionsschritt gibt eine Körpererweiterung vom Grad 1 oder 2, und alle diese Grade werden nach Lemma 22.1 miteinander multipliziert. Deshalb ist der Grad der Körpererweiterung, die α enthält, eine Zweierpotenz 2^k mit $k \leq n$. \square

23. WÜRFELVERDOPPLUNG UND WINKELDREITEILUNG

Während die Konstruktion eines Quadrats mit doppeltem Flächeninhalt sehr einfach ist und schon in der Antike bekannt war,



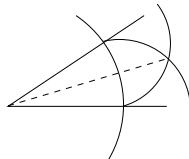
fand man keine Konstruktion mit Zirkel und Lineal für die Seitenlänge eines Würfels mit doppeltem Volumen. Mit anderen Worten, man konnte $\sqrt[3]{2}$ nicht konstruieren. Das wundert uns nun nicht mehr, denn $\alpha = \sqrt[3]{2}$ erfüllt die Gleichung $\alpha^3 = 2$, nach Satz 21.1 gilt also¹²⁰ $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 3$. Wäre α mit Zirkel und Lineal konstruierbar, dann müsste es nach

¹²⁰Wir müssen noch überprüfen, dass es kein rationales Polynom mit Nullstelle $\sqrt[3]{2}$ und kleinerem Grad als $f(x) = x^3 - 2$ gibt. Dazu stellen wir mit Euklids Argument zunächst fest, dass $\sqrt[3]{2}$ irrational ist: Wäre $\sqrt[3]{2} = k/n$ mit $k, n \in \mathbb{N}$ und k, n dann wäre $k^3 = 2n^3$, also wäre k^3 und damit k durch 2 teilbar, $k = 2m$, also $2n^3 = 8m^3$, somit wären n^3 und n ebenfalls durch 2 (sogar durch 4) teilbar, im Widerspruch zur Teilerfremdheit von k und n . Deshalb gibt es kein Polynom vom Grad 1 über \mathbb{Q} mit Nullstelle $\sqrt[3]{2}$. Gäbe es ein solches Polynom g vom Grad 2, dann wären g und f über dem Erweiterungskörper $\mathbb{Q}(\sqrt[3]{2})$ nicht mehr teilerfremd, weil sie den gemeinsamen Teiler $x - \sqrt[3]{2}$ besäßen, also auch nicht über \mathbb{Q} , siehe Fußnote 115. Damit besäßen sie über \mathbb{Q} einen gemeinsamen Teiler vom Grad 1 (was wir

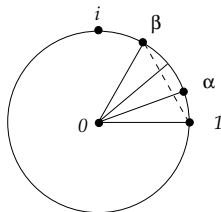
Satz 22.2 in einer Körpererweiterung \mathbb{K}' über \mathbb{Q} vom Grad 2^k liegen. Also wäre $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{K}'$, aber das wäre ein Widerspruch zu 22.1, denn 3 ist kein Teiler von 2^k . Es gilt also:

Satz 23.1. $\sqrt[3]{2}$ ist keine konstruierbare Zahl.

Das nächste Problem aus der Antike ist die Winkel-Dreiteilung mit Zirkel und Lineal. Während die Halbierung eines beliebigen Winkels einfach ist,



fand man keine entsprechende Konstruktion, um einen beliebigen Winkel in drei gleiche Teile zu teilen. Wieder können wir sofort sagen, woran das liegt: Wenn $\beta = e^{i\gamma} \in \mathbb{K}_n$ (wobei \mathbb{K}_n den Körper der in n Konstruktionsschritten aus \mathbb{Q} entstehenden Zahlen bezeichnet) und $\alpha = e^{i\gamma/3} \notin \mathbb{K}_n$, dann löst $x = \alpha$ die Gleichung $x^3 = \beta$, also ist $\mathbb{K}_n(\alpha)$ nach Satz 22.2 eine Erweiterung vom Grad 3 von \mathbb{K}_n und kann deshalb nicht konstruierbar sein. Allerdings müssen wir sicherstellen, dass es kein Polynom von kleinerem Grad über \mathbb{K}_n mit Nullstelle α gibt. Dies ist sicher nicht für jeden Winkel richtig, zum Beispiel nicht für $\alpha = \pi/2 = 90^\circ$, denn der Winkel 30° ist konstruierbar durch Halbieren des gleichseitigen Dreiecks. Aber bereits der Winkel 20° ist nicht konstruierbar:



Satz 23.2. Der (konstruierbare) Winkel $\pi/3 = 60^\circ$ kann mit Zirkel und Lineal nicht gedrittelt werden.

Beweis. Wir suchen eine Lösung $x = \alpha$ der Gleichung $x^3 = \beta$ mit $\beta = e^{i\pi/3} = \frac{1}{2}(1 + i\sqrt{3})$. Mit $x = u + iv$ ist

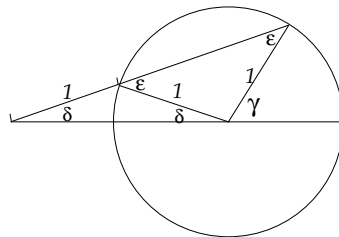
$$x^3 = u^3 - 3uv^2 + i(3u^2v - v^3) \stackrel{!}{=} (1 + i\sqrt{3})/2,$$

also $u^3 - 3u(1 - u^2) = \frac{1}{2}$, da $v^2 = 1 - u^2$ wegen $1 = |x|^2 = u^2 + v^2$. Also erhalten wir $4u^3 - 3u = \frac{1}{2}$, und $w = 2u$ löst die ganzzahlige Gleichung

ausgeschlossen haben) oder 2, aber im letzteren Fall wäre $f = gh$, und h wäre wiederum ein Teiler vom Grad 1, was nicht geht.

$w^3 - 3w = 1$. Analog zu Euklid können wir zeigen, dass diese Gleichung keine rationale Lösung hat: Wenn $w = k/n$ für teilerfremde $k, n \in \mathbb{Z}$, so gilt (*) $k^3 - 3kn^2 = n^3$. Wenn n ungerade ist, dann haben k^3 und $3kn$ die gleiche Parität, also ist die linke Seite gerade, Widerspruch. Wenn n gerade ist, dann muss nach (*) auch k gerade sein, aber k und n sind teilerfremd, Widerspruch.¹²¹ Also besitzt das ganzzahlige Polynom $f(w) = w^3 - 3w - 1$ keine Lösungen in \mathbb{Q} , und damit kann es kein Polynom mit kleinerem Grad mit derselben Nullstelle w geben (vgl. Fußnote 115). Nach Satz 21.1 hat $\mathbb{Q}(w) = \mathbb{Q}(u)$ Grad 3 über \mathbb{Q} , also $\mathbb{Q}(u) \not\subset \mathbb{K}$ nach Satz 22.2, und somit ist u nicht konstruierbar.

Bemerkung: Schon Archimedes¹²² hat aber gezeigt, dass jeder Winkel gedrittelt werden kann, wenn man nur ein bisschen stärkere Hilfsmittel zur Konstruktion verwendet, nämlich ein Lineal, auf dem man Markierungen anbringen kann. Dann bekommt man die Winkeldreiteilung durch folgende Konstruktion:



Denn die Winkelsumme des Dreiecks im Kreis ist $180^\circ = 2\epsilon + 180^\circ - \delta - \gamma$, also (*) $2\epsilon = \gamma + \delta$. Die Winkelsumme des linken gleichschenkligen Dreiecks dagegen ergibt $180^\circ = 2\delta + 180^\circ - \epsilon$, also $\epsilon = 2\delta$, und mit (*) folgt $\gamma = 3\delta$.

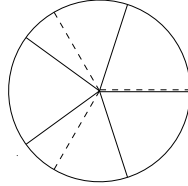
24. KONSTRUKTION REGELMÄSSIGER VIELECKE

Regelmäßige p -Ecke (gleiche Winkel, gleiche Kantenlängen) sind konstruierbar für $p = 3, 4, 5, 6$, aber zum Beispiel nicht für $p = 18$, weil der Winkel $20^\circ = 360^\circ/18$ nicht konstruierbar ist, wie wir gesehen haben (Satz 23.2), doch erstaunlicherweise geht es für $p = 17$, wie Gauß gezeigt hat, was wir gleich verstehen werden. Für welche p genau können wir das regelmäßige p -Eck konstruieren? Wir wollen uns auf den Fall beschränken, dass p eine Primzahl ist; ist $p = qr$ ein Produkt teilerfremder Zahlen, dann ist das p -Eck genau dann konstruierbar, wenn das

¹²¹Etwas übersichtlicher wird dieses Argument, wenn man die Gleichung (*) "modulo 2" reduziert, also die Koeffizienten als Elemente von $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ betrachtet. In \mathbb{F}_2 gilt $x^2 = x$ und $-3 = 1$, also reduziert sich (*) zu $k - kn = n$. Die einzig mögliche Lösung ist $k = n = 0$.

¹²²Archimedes von Syrakus, ca. 287 - 212 v.Chr.

q -Eck und das r -Eck konstruierbar sind, wie in der Figur am Beispiel $q = 5$ und $r = 3$ demonstriert:¹²³



Wir fragen also, ob die Lösungen der Gleichung $x^p = 1$, nämlich $x = \alpha_k = \zeta^k$ mit $\zeta = e^{2\pi i/p}$, in einem der Körper \mathbb{K}_n liegt, dessen Elemente der in n Schritten mit Zirkel und Lineal aus \mathbb{Q} konstruiert werden können. Dazu sehen wir uns noch einmal Beispiel 4 auf Seite 53 an. Die Galoisgruppe G dieser Gleichung besteht aus den Potenzen $\pi_k : \alpha \mapsto \alpha^k$ auf der Menge der Wurzeln, wobei k und p teilerfremd sein müssen. Da p prim ist, ist diese Bedingung für alle $k < p$ erfüllt, die Galoisgruppe hat also $p - 1$ Elemente¹²⁴ und operiert auf den Wurzeln $\alpha_1, \dots, \alpha_{p-1}$ *transitiv*,¹²⁵ und damit ist das *Kreisteilungspolynom*

$$f(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \dots + x + 1 \quad (80)$$

irreduzibel, vgl. Beispiel 2 auf Seite 52. Somit ist $\mathbb{Q}(\zeta)$ eine Erweiterung von \mathbb{Q} vom Grad $p - 1$. Wenn $\zeta \in \mathbb{K}_n$, dann muss $p - 1$ ein Teiler von 2^n sein, also selbst eine Zweierpotenz, $p - 1 = 2^s$. Für welche Zweierpotenz 2^s ist $p = 2^s + 1$ aber eine Primzahl? Für $s = 3$ zum Beispiel nicht, denn $8 + 1 = 9$.

Lemma 24.1. *Wenn $2^s + 1$ eine Primzahl ist, dann ist s selbst eine Zweierpotenz, $s = 2^r$.*

Beweis. Obwohl dies nur eine Aussage über ganze Zahlen ist, benutzt der Beweis Polynome. Er geschieht durch Kontraposition.¹²⁶ Ist s keine Zweierpotenz, dann besitzt s einen ungeraden Faktor: $s = mk$ mit k ungerade. Dann hat das Polynom $x^k + 1$ die Nullstelle $x = -1$ und ist also durch $x + 1$ teilbar, $(x + 1) \mid (x^k + 1)$. Diese Teilbarkeit bleibt bestehen, wenn wir für x einen ganzzahligen Wert einsetzen, zum Beispiel $x = 2^m$:

$$(2^m + 1) \mid (2^{mk} + 1) = 2^s + 1.$$

Somit kann $2^s + 1$ keine Primzahl sein. □

¹²³Das Argument stimmt nicht mehr für Primzahl-Potenzen; zum Beispiel ist das 9-Eck nicht konstruierbar.

¹²⁴Es ist die multiplikative Gruppe \mathbb{F}_p^* des Körpers \mathbb{F}_p .

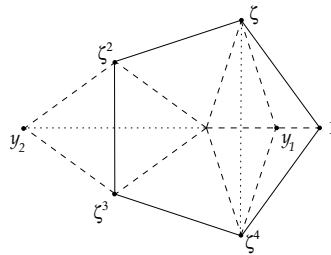
¹²⁵Eine Wirkung $\phi : G \times X \rightarrow X$ heißt *transitiv*, wenn es nur eine einzige Bahn gibt, wenn also zu jedem $x, x' \in X$ ein $g \in G$ existiert mit $gx = x'$.

¹²⁶Statt " $A \Rightarrow B$ " beweist man "nicht $B \Rightarrow$ nicht A ".

Bemerkung: Eine Zahl der Form $F_r = 2^{2^r} + 1$, $r = 0, 1, 2, \dots$, heißt *Fermatzahl*.¹²⁷ Die ersten 5 Fermatzahlen 3, 5, 17, 257, 65537 sind Primzahlen, aber im Jahr 1732 entdeckte Leonhard Euler, dass $F_5 = 4\,294\,967\,297 = 641 \cdot 6700417$ ist. Man vermutet sogar, dass unter den Fermatzahlen keine weitere Primzahl mehr vorkommt; bis F_{32} wurde dies bestätigt.

Gauß hat gezeigt, dass das p -Eck auch wirklich konstruierbar ist, wenn p eine Fermatsche Primzahl ist. Wir wollen das am Beispiel des 5-Ecks und des 17-Ecks demonstrieren und benutzen dazu die Methode der “halbvarianten” Polynome, vgl. Seite 36.

5-Eck:



Die Nullstellen von (80) sind $\zeta, \zeta^2, \zeta^3, \zeta^4$ mit $\zeta = e^{2\pi i/5}$. Die Galoisgruppe G besteht aus den Potenzen $\pi_k(x) = x^k$ mit $k = 1, 2, 3, 4$ und wird zum Beispiel von π_2 erzeugt,¹²⁸ denn $(\pi_2)^2 = \pi_4$, $(\pi_2)^3 = \pi_8 = \pi_3$,¹²⁹ und $(\pi_2)^4 = \pi_{16} = \pi_1 = \text{id}$. Die Potenzen $(\pi_2)^2 = \pi_4$ und $(\pi_2)^4 = \text{id}$ bilden eine Untergruppe $H \subset G$ mit Bahnen $H\zeta = \{\zeta^4, \zeta\}$ und $H\zeta^2 = \{\zeta^3, \zeta^2\}$, und die Summe der Elemente jeder Bahn bildet je ein H -invariantes Polynom $y_1 = \zeta + \zeta^4 = 2 \operatorname{Re} \zeta$ und $y_2 = \zeta^2 + \zeta^3 = 2 \operatorname{Re} \zeta^2$.¹³⁰ Dies sind die Lösungen der quadratischen Gleichung $0 = (y - y_1)(y - y_2) = y^2 - ay + b$ mit

$$a = y_1 + y_2 = \zeta + \zeta^4 + \zeta^2 + \zeta^3 = -1,$$

weil ζ Nullstelle des Kreisteilungspolynoms ist, vgl. (80). Ferner ist

$$b = y_1 y_2 = (\zeta + \zeta^4)(\zeta^2 + \zeta^3) = \zeta^3 + \zeta^4 + \zeta + \zeta^2 = -1,$$

und damit erfüllt y die Gleichung

$$y^2 + y - 1 = 0. \tag{81}$$

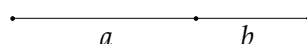
¹²⁷Pierre de Fermat, 1607 - 1665 (Frankreich)

¹²⁸Eine Gruppe G wird von einem Element $g_o \in G$ erzeugt, wenn jedes Element $g \in G$ eine Potenz von g_o ist, $g = g_o^j$ für ein $j \in \mathbb{Z}$, wobei $g^1 = g$, $g^{j+1} = g^j g$, $g^{-j} = (g^{-1})^j$. Eine Gruppe, die von einem Element erzeugt wird, heißt *zyklisch*.

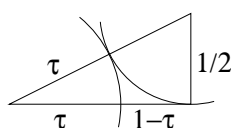
¹²⁹Die Potenzen werden modulo 5 gerechnet, weil $x^5 = 1$, zum Beispiel $x^8 = x^{5+3} = x^5 \cdot x^3 = 1 \cdot x^3 = x^3$.

¹³⁰Man beachte $\zeta^4 = \zeta^{-1} = \bar{\zeta}$ und $\zeta^3 = \zeta^{-2} = \bar{\zeta}^2$.

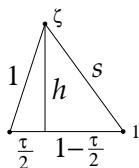
Dies ist die Gleichung des *Goldenen Schnittes* τ : Dabei wird eine Strecke so in zwei ungleiche Teile a und b zerlegt, dass sich die Gesamtstrecke $a + b$ zum größeren Teil a verhält wie der größere zum kleineren,

$$\frac{a}{b} = \frac{a+b}{a} = 1 + \frac{b}{a}.$$


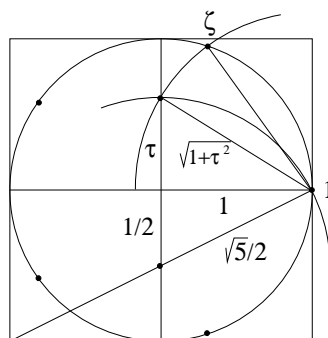
Der goldene Schnitt ist dann das Verhältnis $\tau = \frac{b}{a} = \frac{a}{b} - 1 = \frac{1}{\tau} - 1$, also $\tau^2 = 1 - \tau$, und somit ist $y = \tau$ die positive Lösung von (81). Als Lösung einer quadratischen Gleichung mit ganzzahligen Koeffizienten kann τ mit Zirkel und Lineal konstruiert werden, zum Beispiel so:



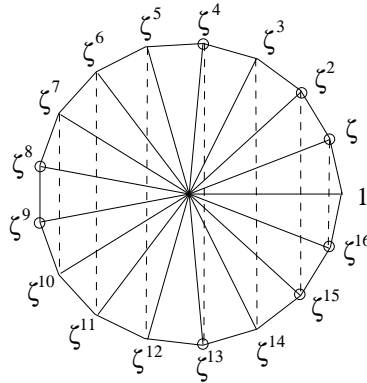
Die Gleichung $\tau = y_1 = \zeta + \zeta^{-1}$ ergibt durch Multiplikation mit ζ eine quadratische Gleichung für ζ , nämlich $\zeta^2 - \tau\zeta + 1 = 0$ mit der Lösung $\zeta = \frac{\tau}{2} \pm i\sqrt{1 - (\frac{\tau}{2})^2}$. Die Quadratwurzel $\sqrt{1 - (\frac{\tau}{2})^2}$ ist die Höhe h in der folgenden Figur:



Aus derselben Figur kann man aber auch sofort die Seitenlänge des 5-Ecks entnehmen: $s^2 = (1 - \frac{\tau^2}{4}) + (1 - \frac{\tau}{2})^2 = 1 - \frac{\tau^2}{4} + 1 + \frac{\tau^2}{4} - \tau = 2 - \tau = 1 + \tau^2$, da $\tau^2 = 1 - \tau$. Die folgende Konstruktion der Seitenlänge $s = \sqrt{1 + \tau^2}$ war bereits Albrecht Dürer bekannt:¹³¹



¹³¹Albrecht Dürer (Nürnberg 1471 - 1528), "Unterweysung der Messung, mit dem Zirkel und Richtscheyt, Nürnberg 1525

17-Eck:

Das 17-Eck (vgl. [7]) besteht aus den Lösungen der Gleichung $x^{17} = 1$, der Menge Ω_0 der Potenzen $\neq 1$ von $\zeta = e^{2\pi i/17}$,

$$\Omega_0 = \{\zeta^k : k = 1, \dots, 16\}.$$

Die Galoisgruppe $G = \{\pi_k : k = 1, \dots, 16\} \cong \mathbb{F}_{17}^*$ wird wieder von einem einzigen Element erzeugt,¹³² zum Beispiel von π_3 , denn $\pi_3^k = \pi_{3^k}$, und die Dreierpotenzen modulo 17 durchwandern alle Zahlen $1, \dots, 16$:

$$\begin{array}{llll} 3^1 \stackrel{17}{\equiv} 3, & 3^2 \stackrel{17}{\equiv} 9, & 3^3 \stackrel{17}{\equiv} 27 \stackrel{17}{\equiv} 10, & 3^4 \stackrel{17}{\equiv} 30 \stackrel{17}{\equiv} -4 \stackrel{17}{\equiv} 13, \\ 3^5 \stackrel{17}{\equiv} -12 \stackrel{17}{\equiv} 5, & 3^6 \stackrel{17}{\equiv} 15 \stackrel{17}{\equiv} -2, & 3^7 \stackrel{17}{\equiv} -6 \stackrel{17}{\equiv} 11, & 3^8 \stackrel{17}{\equiv} 33 \stackrel{17}{\equiv} -1 \stackrel{17}{\equiv} 16, \\ 3^9 \stackrel{17}{\equiv} -3 \stackrel{17}{\equiv} 14, & 3^{10} \stackrel{17}{\equiv} -9 \stackrel{17}{\equiv} 8, & 3^{11} \stackrel{17}{\equiv} -10 \stackrel{17}{\equiv} 7, & 3^{12} \stackrel{17}{\equiv} 4, \\ 3^{13} \stackrel{17}{\equiv} 12, & 3^{14} \stackrel{17}{\equiv} 2, & 3^{15} \stackrel{17}{\equiv} 6, & 3^{16} \stackrel{17}{\equiv} 1, \end{array}$$

oder in Kurzform:

$$\begin{array}{c|cccccccc} k & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3^k & 3 & 9 & 10 & 13 & 5 & 15 & 11 & 16 \\ \hline k & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 \\ 3^k & 14 & 8 & 7 & 4 & 12 & 2 & 6 & 1 \end{array} \quad (82)$$

Die geraden Potenzen $\{\pi_3^{2k} : k = 1, \dots, 8\}$ bilden eine Untergruppe $H_1 \subset G$ mit zwei Bahnen auf Ω_0 , nämlich

$$\Omega_1 = \{\zeta^k : k \in \{9, 13, 15, 16, 8, 4, 2, 1\}\}$$

(in der obigen Figur markiert) sowie

$$\Omega'_1 = \Omega_0 \setminus \Omega_1 = \{\zeta^k : k \in \{3, 10, 5, 11, 14, 7, 12, 6\}\}.$$

Die Summe über die Bahn Ω_1 ergibt das H_1 -invariante Polynom $y_1 = 2 \operatorname{Re}(\zeta + \zeta^2 + \zeta^4 + \zeta^8)$. Jedes $\sigma \in G$ bildet Ω_1 entweder auf sich selbst oder auf die andere Bahn Ω'_1 ab. Deshalb besteht die Bahn von y_1 unter

¹³²Diese Eigenschaft gilt für jede endliche Untergruppe der multiplikativen Gruppe \mathbb{K}^* eines Körpers \mathbb{K} , siehe [6, Theorem 44, Seite 39].

G nur aus zwei Elementen, y_1 und $y'_1 = s - y_1 = 2 \operatorname{Re}(\zeta^3 + \zeta^5 + \zeta^6 + \zeta^7)$ mit $s := \sum_{j=1}^{16} \zeta^j = -1$. Also sind y_1, y'_1 die Lösungen einer quadratischen Gleichung $y^2 - ay + b = 0$ mit Koeffizienten $a = y_1 + y'_1 = s = -1$ und¹³³ $b = y_1 y'_1 = 4 \sum_{j=1}^{16} \zeta^j = -4$. Also löst $y = y_1$ die quadratische Gleichung $y^2 + y = 4$ und ist somit konstruierbar, ebenso wie die zweite Lösung $y'_1 = -(1 + y_1)$.

Die Gruppe H_1 wirkt transitiv auf Ω_1 und Ω'_1 . Sie wird von $\pi_3^2 = \pi_9$ erzeugt (d.h. sie besteht aus Iterierten von π_9) und enthält jedes zweite Element in der Tabelle (82). Jedes vierte Element liegt in der von $\pi_3^4 = \pi_{13}$ erzeugten Untergruppe $H_2 = \{\pi_3^{4k} : k = 1, \dots, 4\} = \{\pi_k : k \in \{13, 16, 4, 1\}\}$. Diese zerlegt Ω_1 wiederum in zwei Bahnen,

$$\Omega_2 = H_2 \zeta = \{\zeta^k : k \in \{13, 16, 4, 1\}\}$$

und $\Omega_1 \setminus \Omega_2$, und ebenso wird Ω'_1 zerlegt in

$$\Omega'_2 = H_2 \zeta^3 = \{\zeta^k : k \in \{3, 5, 14, 12\}\}$$

und $\Omega'_1 \setminus \Omega'_2$. Die Summe über die Elemente der Bahn Ω_2 ist das H_2 -invariante Polynom

$$y_2 = 2 \operatorname{Re}(\zeta + \zeta^4),$$

und wieder besteht die Bahn von y_2 unter H_1 aus zwei Elementen y_2 und $y_1 - y_2 = 2 \operatorname{Re}(\zeta^2 + \zeta^8)$. Diese lösen eine quadratische Gleichung $y^2 - cy + d = 0$ mit Koeffizienten $c = y_2 + (y_1 - y_2) = y_1$ und¹³⁴ $d = y_2(y_1 - y_2) = -1$. Also löst $y = y_2$ die Gleichung $y^2 - y_1 y = 1$ und ist damit konstruierbar.

Ebenso ist die Summe über die Bahn Ω'_2 ein H_2 -invariantes Polynom,

$$y'_2 = 2 \operatorname{Re}(\zeta^3 + \zeta^5),$$

und die Bahn von y'_2 besteht aus y'_2 und $y'_1 - y'_2$, den Lösungen einer quadratischen Gleichung $y^2 - c'y + d' = 0$ mit $c' = y'_2 + y'_1 - y'_2 = y'_1$ und $d' = y'_2(y'_1 - y'_2) = -1$ wie oben. Also löst $y = y'_2$ die quadratische Gleichung $y^2 - y'_1 y = 1$ und ist damit konstruierbar.

Die Gruppe H_2 wirkt transitiv auf Ω_2 und wird erzeugt von π_3^4 . Das Quadrat des Erzeugenden, $\pi_3^8 = \pi_{16}$, bildet zusammen mit $\pi_1 = \operatorname{id}$ eine Untergruppe H_3 (denn $(\pi_3^8)^2 = \pi_1$). Diese zerlegt Ω_2 wiederum in zwei Bahnen, $\Omega_3 = \{\zeta, \bar{\zeta}\}$ und $\Omega_2 \setminus \Omega_3 = \{\zeta^4, \bar{\zeta}^4\}$, und die Bahnsummen

¹³³Die acht ζ^k von y_1 multipliziert mit den acht ζ^l von y'_1 ergeben 64 Summanden der Form ζ^j . Da $\zeta^k \neq \zeta^l$, sind alle j zwischen 1 und 16, und aus Symmetriegründen treten alle gleich oft auf, also jeweils viermal.

¹³⁴Das Produkt hat 16 Terme, und alle Elemente von Ω_0 kommen genau einmal vor.

$y_3 = 2 \operatorname{Re} \zeta$ und $y_2 - y_3 = 2 \operatorname{Re} \zeta^4$ sind die Lösungen einer quadratischen Gleichung $y^2 - ey + f = 0$ mit Koeffizienten $e = y_3 + y_2 - y_3 = y_2$ und

$$f = y_3(y_2 - y_3) = (\zeta + \bar{\zeta})(\zeta^4 + \bar{\zeta}^4) = 2 \operatorname{Re}(\zeta^5 + \zeta^3) = y'_2.$$

Also löst $y = y_3$ die quadratische Gleichung $y^2 - y_2y + y'_2 = 0$, deren Koeffizienten konstruierbar sind, somit ist auch $y_3 = 2 \operatorname{Re} \zeta$ konstruierbar. Um ζ zu konstruieren, kann man noch einen weiteren Schritt anfügen oder gleich $\operatorname{Im} \zeta$ konstruieren aus der Bedingung $|\zeta| = 1$, also $(\operatorname{Re} \zeta)^2 + (\operatorname{Im} \zeta)^2 = 1$.

25. IRREDUZIBILITÄT ÜBER \mathbb{Z}

Wir haben schon gesehen, dass die Irreduzibilität eines Polynoms sehr wichtig ist; zum Beispiel gilt der Satz $[\mathbb{K}(\alpha) : \mathbb{K}] = n$ für eine Nullstelle α eines Polynoms $f \in \mathbb{K}[x]$ vom Grad n nur dann, wenn f irreduzibel ist. Wenn f ein Produkt von anderen Polynomen ist, $f = gh$, können wir besser gleich die Nullstellen von g und h suchen, was einfacher ist, weil g und h kleineren Grad haben. Aber wie erkennen wir, ob ein Polynom f irreduzibel ist oder nicht?

Das ist ganz analog wie bei Primzahlen. Wie erkennen wir, ob 199 eine Primzahl ist? Das geht bekanntlich mit dem *Sieb des Eratosthenes*.¹³⁵ Wenn nicht, gibt es einen Primteiler von 199, der kleiner oder gleich $\sqrt{199}$ ist, also kleiner als $\sqrt{225} = 15$. Wir brauchen also nur Primzahlen < 15 zu testen. Für 2 (ungerade), 3 (Quersumme nicht durch 3 teilbar) und 5 (letzte Dezimale ist nicht 0 oder 5) sehen wir sofort, dass es keine Teiler sind, für 7 und 13 benutzen wir Division mit Rest oder die verbesserte Quersummenregel: Weil $10 =_7 3$ und $100 = 98 + 2 =_7 2$, ist $199 = 1 \cdot 100 + 9 \cdot 10 + 9 =_7 1 \cdot 2 + 9 \cdot 3 + 9 = 38 =_7 3$ nicht durch 7 teilbar, und weil $10 =_{13} -3$ und $100 = 91 + 9 =_{13} 9$, ist $199 =_{13} 1 \cdot 9 - 9 \cdot 3 + 9 = -9 =_{13} 4$ nicht durch 13 teilbar. Bei 11 ist es noch einfacher: Die Differenz der Summen der geraden und der ungeraden Stellen von 199 ist nicht durch 11 teilbar.

Ebenso bei Polynomen: wann ist ein Polynom $f \in \mathbb{K}[x]$ vom Grad n "prim", also unteilbar, *irreduzibel*? Wenn nicht, gibt es ein irreduzibles Polynom mit Grad $\leq n/2$, das f teilt; nur solche irreduziblen Polynome brauchen wir zu testen.

Bei ganzzahligen Polynomen $f \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ lassen sich Teilbarkeit in \mathbb{Z} und $\mathbb{Z}[x]$ auf einfache Weise verbinden; die Methode geht auf Kronecker¹³⁶ zurück. Für $f, g \in \mathbb{Z}[x]$ und jedes $k \in \mathbb{Z}$ gilt:

$$g \mid f \Rightarrow g(k) \mid f(k). \quad (83)$$

¹³⁵Eratosthenes von Kyrene, ca. 275 v.Chr. (Kyrene) - 194 v.Chr. (Alexandria)

¹³⁶Leopold Kronecker, 1823 (Liegnitz) - 1891 (Berlin)

Beispiel 1. Ist $f(x) = x^5 + x^4 + 2x^2 + 2x + 1$ irreduzibel über \mathbb{Z} ? Wir müssen nur Polynome $g(x)$ mit Grad 1 oder 2 testen. Wir haben $f(0) = 1$, $f(1) = 7$, $f(-1) = 1$, $f(-2) = -11$, $f(2) = 61$. Nach (83) gilt $g(0)|1$, also $g(0) = \pm 1$. Wäre g von Ordnung 1, $g(x) = x + b$, dann wäre $-b$ eine Nullstelle von f , aber $g(0) = b = \pm 1$ ist keine Nullstelle. Es bleiben quadratische Polynome $g(x) = x^2 + ax + 1$ oder $g(x) = x^2 + ax - 1$. Nach (83) gilt im ersten Fall $g(1) = 2 + a | f(1) = 7$ und andererseits $g(-1) = 2 - a | f(-1) = 1$, also $2 - a \in \{\pm 1\}$ und damit $a \in \{1, 3\}$ und $2 + a \in \{3, 5\}$, aber diese Zahlen erfüllen die erste Bedingung $2 + a | 7$ nicht. Im zweiten Fall $g = x^2 + ax - 1$ erhalten wir $g(1) = a | f(1) = 7$ und $g(-1) = -a | f(-1) = 1$, also $a = \pm 1$. Für $a = -1$ ist $g(-2) = 4 + 2 - 1 = 5$, dies ist kein Teiler von $f(-2) = -11$. Also bleibt $a = 1$ und $g(x) = x^2 + x - 1$. Aber $g(2) = 5$ ist kein Teiler von $f(2) = 61$. Somit ist f irreduzibel über \mathbb{Z} .

Bei ganzzahligen Polynomen $f \in \mathbb{Z}[x]$ gibt es noch ein anderes starkes Hilfsmittel: Reduktion modulo p für eine Primzahl p . Wir fassen dazu das Polynom f auf als Polynom über $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit den gleichen Koeffizienten, nur "modulo p " gelesen. Wenn das Polynom in $\mathbb{Z}[x]$ zerfällt, $f = gh$ mit $g, h \in \mathbb{Z}[x]$, dann gilt das gleiche für die entsprechenden Polynome in $\mathbb{F}_p[x]$.

Beispiel 2: $f(x) = x^5 + 6x^4 + 3x^3 + 2x^2 + 4x + 3 \in \mathbb{Z}[x]$. Dieses Polynom reduzieren wir modulo 2, fassen es also als Polynom über \mathbb{F}_2 auf. Da kommt es nur auf "gerade" (0) oder "ungerade" (1) an:

$$\tilde{f}(x) = x^5 + x^3 + 1 \in \mathbb{F}_2[x].$$

Offensichtlich ist $\tilde{f}(0) = 1 = \tilde{f}(1)$, es gibt also keine Linearfaktoren. Die quadratischen Polynome sind x^2 , $x^2 + 1$, $x^2 + x$, $x^2 + x + 1$, und nur das letztere ist irreduzibel, da $x^2 + 1 = (x + 1)^2$ über \mathbb{F}_2 . Wir brauchen also nur die Division durch $x^2 + x + 1$ zu testen (Vorzeichen spielen in \mathbb{F}_2 keine Rolle):

$$\begin{array}{r} x^5 + x^3 + 1 \quad : \quad x^2 + x + 1 \quad = \quad x^3 + x^2 + x \quad \text{Rest} \quad x + 1 \\ \hline x^5 \quad \quad \quad + x^3 \quad + 1 \\ x^5 \quad + x^4 \quad + x^3 \\ \hline \quad \quad x^4 \quad \quad \quad + 1 \\ \quad \quad x^4 \quad + x^3 \quad + x^2 \\ \hline \quad \quad \quad x^3 \quad + x^2 \quad + 1 \\ \quad \quad \quad x^3 \quad + x^2 \quad + x \\ \hline \quad \quad \quad \quad \quad \quad x \quad + 1 \end{array}$$

Also ist f über \mathbb{Z} irreduzibel.

Diese Methode lässt sich noch etwas verfeinern zum *Kriterium von Eisenstein*:¹³⁷

Satz 25.1. *Ist $f = a_0x^n + a_1x^{n-1} + \dots + a_n \in \mathbb{Z}[x]$ mit $p \mid a_1, \dots, a_n$ für eine Primzahl p , aber p sei kein Teiler von a_0 (sonst könnte man ja f/p betrachten), und p^2 sei kein Teiler von a_n . Dann ist f irreduzibel in $\mathbb{Z}[x]$.*

Beweis. Wir nehmen an, dass $f = gh$ über \mathbb{Z} mit $g = b_0x^k + \dots + b_k$ und $h = c_0x^l + \dots + c_l$, wobei $k + l = n$. Reduktion modulo p ergibt $\tilde{a}_0x^n = \tilde{f} = \tilde{g}\tilde{h}$. Andererseits ist

$$gh(x) = b_0c_0x^n + (b_0c_1 + c_0b_1)x^{n-1} + (b_0c_2 + b_1c_1 + b_2c_0)x^{n-2} + \dots + b_kc_l.$$

Da $gh(x) = f(x) \equiv_p a_0x^n$, sind alle Koeffizienten rechts außer dem vordersten durch p teilbar, aber b_0 und c_0 sind nicht durch p teilbar. Deshalb sind b_1, \dots, b_k und c_1, \dots, c_l durch p teilbar und $a_n = b_kc_l$ also durch p^2 . Aber das hatten wir ausgeschlossen. \square

Beispiel 3a. $f(x) = x^5 - 4x + 2$ ist irreduzibel nach Eisenstein für $p = 2$, denn die Koeffizienten sind durch 2 teilbar, aber der letzte nicht durch 4.

Beispiel 3b: $f(x) = (x^p - 1)/(x - 1) = x^{p-1} + x^{p-2} + \dots + 1$ (Kreisteilungspolynom), wobei p eine Primzahl ist. Statt $f(x)$ betrachten wir $f(x + 1)$. Nach der binomischen Formel (vgl. Abschnitt 3) ist

$$\begin{aligned} f(x + 1) &= ((x + 1)^p - 1) / x \\ &= (x^p + \binom{p}{1}x^{p-1} + \dots + \binom{p}{p-1}x) / x \\ &= x^{p-1} + \binom{p}{1}x^{p-2} + \dots + \binom{p}{p-1}. \end{aligned}$$

Alle Koeffizienten sind durch p teilbar, aber der letzte $\binom{p}{p-1} = p$ ist nicht durch p^2 teilbar, also ist $f(x + 1)$ irreduzibel nach Eisenstein, somit auch $f(x)$.

26. IRREDUZIBILITÄT ÜBER \mathbb{Q}

Jede Polynomgleichung $f(x) = 0$ über den rationalen Zahlen \mathbb{Q} lässt sich durch Hochmultiplizieren der Nenner (genauer, des *kgV*, des kleinsten gemeinsamen Vielfachen der Nenner) zu einer ganzzahligen Gleichung umformen. Im letzten Abschnitt haben wir gesehen, wie wir die Irreduzibilität über \mathbb{Z} prüfen können. Folgt daraus auch die Irreduzibilität über \mathbb{Q} ? Auch wenn f keine Zerlegung $f = gh$ in ganzzahlige Polynome zulässt, könnte es nicht eine solche Zerlegung in rationale Polynome geben? Das verneint ein allgemeines Resultat von *Gauß*:

¹³⁷Ferdinand Gotthold Max Eisenstein, 1823 - 1852 (Berlin)

Satz 26.1. *Wenn $f \in \mathbb{Z}[x] \subset \mathbb{Q}[x]$ über \mathbb{Q} reduzibel ist, d.h. $f = gh$ mit $g, h \in \mathbb{Q}[x]$, dann auch über \mathbb{Z} , genauer $f = g_o h_o$ für $g_o, h_o \in \mathbb{Z}[x]$, wobei g, h rationale Vielfache von g_o, h_o sind.*

Beweis. Wir dürfen annehmen, dass f *primitiv* ist, d.h. die Koeffizienten von f haben keinen gemeinsamen Teiler d ; andernfalls würden wir zu $f/d \in \mathbb{Z}[x]$ übergehen. Es gelte $f = gh$ mit $g, h \in \mathbb{Q}[x]$. Durch Hochmultiplizieren des Nenners und danach ggf. Ausdividieren des größten gemeinsamen Teilers der Koeffizienten wird jedes rationale Polynom ein rationales Vielfaches eines primitiven ganzzahligen Polynoms, also $g = ag_o$ und $h = bh_o$ mit $g_o, h_o \in \mathbb{Z}[x]$ primitiv und $a, b \in \mathbb{Q}$. Dann ist auch $f_o := g_o h_o$ primitiv, siehe das nachfolgende Lemma. Für die beiden primitiven ganzzahligen Polynome f und f_o gilt also $f = gh = r f_o$ für die rationale Zahl $r = ab = k/l$, wobei $k \in \mathbb{Z}$, $l \in \mathbb{N}$ teilerfremd sind. Dann folgt

$$lf = kf_o,$$

also sind die Koeffizienten von kf_o alle durch l teilbar. Weil k, l teilerfremd, sind auch die Koeffizienten von f_o durch l teilbar, also ist $l = 1$, denn f_o ist primitiv. Dann ist $f = kf_o$, und somit sind die Koeffizienten von f durch k teilbar; weil f primitiv, ist $k = \pm 1$ und somit haben wir die Zerlegung $f = \pm g_o h_o$ in $\mathbb{Z}[x]$. \square

Lemma 26.1. *Sind $g, h \in \mathbb{Z}[x]$ primitiv, dann ist auch $gh \in \mathbb{Z}[x]$ primitiv.*

Beweis. Andernfalls gibt es eine Primzahl p , die alle Koeffizienten von gh teilt. Dann ist die Reduktion von gh modulo p das Nullpolynom (alle Koeffizienten gleich Null)¹³⁸ über \mathbb{F}_p , also gilt $\tilde{g}\tilde{h} = 0$, wobei \tilde{g} und \tilde{h} die Reduktionen modulo p von g und h bezeichnen. Aber daraus folgt $\tilde{g} = 0$ oder $\tilde{h} = 0$, im Widerspruch zur Primitivität von g und h . \square

Korollar 26.1. *Die Nullstellen von jedem ganzzahligen normierten Polynom f sind entweder ganzzahlig oder irrational.*

Beweis. Wenn $g(x) = x - \frac{k}{l}$ ein Teiler von f in $\mathbb{Q}[x]$ ist ($k, l \in \mathbb{Z}$ teilerfremd), dann ist $g_o(x) = lx - k$ nach Satz 26.1 ein Teiler von f in $\mathbb{Z}[x]$, aber daraus folgt $l = 1$, weil $f(x) = x^n + a_1 x^{n-1} + \dots + a_n$. \square

¹³⁸Ein Polynom $\neq 0$ kann über \mathbb{F}_p überall Null sein, zum Beispiel $f(x) = \prod_{\alpha \in \mathbb{F}_p} (x - \alpha)$. Beispiel: $x^2 + x = x(x + 1)$ über \mathbb{F}_2 . Dies ist dennoch nicht das Nullpolynom.

27. DIE GALOISGRUPPE EINER KÖRPERERWEITERUNG

Ein *Automorphismus* eines Körpers \mathbb{K} ist eine umkehrbare Abbildung $\sigma : \mathbb{K} \rightarrow \mathbb{K}$, die mit den Körper-Operationen (den vier Grundrechenarten) vertauscht: σ bildet 0 und 1 auf sich selbst ab und erfüllt

$$\sigma(a + b) = \sigma(a) + \sigma(b), \quad \sigma(ab) = \sigma(a)\sigma(b) \quad (84)$$

für alle $a, b \in \mathbb{K}$. Die Umkehrabbildung $\tau = \sigma^{-1}$ ist automatisch wieder ein Körperautomorphismus,¹³⁹ ebenso wie die Verkettung zweier Automorphismen. Die Automorphismen von \mathbb{K} bilden daher eine Gruppe $\text{Aut}(G)$ (mit der Verkettung \circ als Gruppenoperation). Bisher haben wir nur einen Körperautomorphismus gesehen: die komplexe Konjugation in \mathbb{C} (Seite 16). Für die Algebra spielen sie eine bedeutende Rolle:

Definition: Für jede Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ definiert man die *Galoisgruppe*

$$G = \text{Gal}(\mathbb{L}, \mathbb{K}) = \{\sigma \in \text{Aut}(\mathbb{L}) : \sigma|_{\mathbb{K}} = \text{id}_{\mathbb{K}}\}. \quad (85)$$

Zum Beispiel ist $\text{Gal}(\mathbb{C}, \mathbb{R}) = \{\text{id}, \kappa\}$ mit $\kappa(x) = \bar{x}$ (komplexe Konjugation).¹⁴⁰

Die Galoisgruppe einer Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ kann sehr klein sein, sogar trivial, zum Beispiel im Fall $\mathbb{K} = \mathbb{Q}$ und $\mathbb{L} = \mathbb{Q}(\alpha)$ mit $\alpha = \sqrt[3]{2}$. Jedes $\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K})$ erhält das ganzzahlige Polynom $f(x) = x^3 - 2$, d.h. $\sigma(f(x)) = f(\sigma x)$. Insbesondere ist mit α auch $\sigma\alpha$ Nullstelle von f , denn $f(\sigma\alpha) = \sigma(f(\alpha)) = \sigma(0) = 0$. Damit folgt aber $\sigma\alpha = \alpha$, denn f hat keine andere Nullstelle in \mathbb{L} , und somit ist $\sigma = \text{id}$ auf ganz \mathbb{L} . Die Galoisgruppe gibt uns in diesem Fall also keine Information über die Körpererweiterung.

Es gibt aber andere Beispiele, sogenannte *normale Körpererweiterungen* oder *Galoiserweiterung* $\mathbb{L} \supset \mathbb{K}$, wobei \mathbb{L} der volle *Zerfällungskörper* eines Polynoms $f \in \mathbb{K}[x]$ mit getrennten Nullstellen $\alpha_1, \dots, \alpha_n$ ist. Das ist der kleinste Erweiterungskörper von \mathbb{K} , der alle Nullstellen $\alpha_1, \dots, \alpha_n$ von f enthält, $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\vec{\alpha})$. Er besteht nach Definition aus allen rationalen Ausdrücken $H(\vec{\alpha})/J(\vec{\alpha})$ für beliebige Polynome $H, J \in \mathbb{K}[\vec{x}]$. Allerdings zeigt Satz 21.1, dass man mit Polynomen auskommt, $\mathbb{L} = \mathbb{K}[\vec{\alpha}]$, wie man durch sukzessive Adjunktion der Wurzeln sieht:

$$\mathbb{K}(\alpha_1, \dots, \alpha_{k+1}) = \mathbb{K}(\alpha_1, \dots, \alpha_k)[\alpha_{k+1}].$$

¹³⁹Für jedes $a, b \in \mathbb{K}$ sei $\tilde{a} = \tau a$ und $\tilde{b} = \tau b$. Für die Rechenoperationen $* = +$ und $* = \cdot$ gilt dann $\tau(a * b) = \tau(\sigma(\tilde{a}) * \sigma(\tilde{b})) = \tau(\sigma(\tilde{a} * \tilde{b})) = \tilde{a} * \tilde{b} = \tau a * \tau b$.

¹⁴⁰Beweis: Ist $\sigma \in \text{Gal}(\mathbb{C}, \mathbb{R})$, so erfüllt $\sigma(i)$ die Gleichung $\sigma(i)^2 = -1$, also ist $\sigma(i) = \pm i$. Damit ist $\sigma(u + iv) = \sigma(u) + \sigma(i)\sigma(v) = u \pm iv$ für alle $u, v \in \mathbb{R}$.

In diesem Fall $\mathbb{L} = \mathbb{K}(\bar{\alpha})$ ist $\text{Gal}(\mathbb{L}, \mathbb{K})$ die früher definierte Galoisgruppe von f (siehe Abschnitt 18 auf Seite 51); das werden wir gleich zeigen (Satz 27.1, Seite 84). Zunächst sei aber $\mathbb{L} \supset \mathbb{K}$ noch eine beliebige Körpererweiterung.

Lemma 27.1. *Es sei $f \in \mathbb{K}[x]$ und $N(f, \mathbb{L}) = \{x \in \mathbb{L} : f(x) = 0\}$ die Nullstellenmenge von f in \mathbb{L} . Dann gilt für jedes $\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K})$:*

- (a) $f(\sigma x) = \sigma f(x)$ für jedes $x \in \mathbb{L}$,
- (b) $\sigma(N(f, \mathbb{L})) = N(f, \mathbb{L})$.

Beweis. Es sei $f(x) = \sum_{j=0}^n a_{n-j}x^j$, dann ist

$$\sigma(f(x)) = \sum_{j=0}^n \sigma(a_{n-j})(\sigma x)^j = \sum_{j=0}^n a_{n-j}(\sigma x)^j = f(\sigma x),$$

da $a_{n-j} \in \mathbb{K}$ und daher $\sigma(a_{n-j}) = a_{n-j}$. Ist $\alpha \in \mathbb{L}$ eine Nullstelle, $f(\alpha) = 0$, so gilt $f(\sigma\alpha) = \sigma f(\alpha) = \sigma(0) = 0$, deshalb ist

$$(1) \quad \sigma(N(f, \mathbb{L})) \subset N(f, \mathbb{L}).$$

Die Gleichheit folgt, weil für $\tau = \sigma^{-1}$ ebenso gilt:

$$(2) \quad \tau(N(f, \mathbb{L})) \subset N(f, \mathbb{L}),$$

also

$$N(f, \mathbb{L}) = \sigma\tau(N(f, \mathbb{L})) \stackrel{(2)}{\subset} \sigma(N(f, \mathbb{L})) \stackrel{(1)}{\subset} N(f, \mathbb{L}). \quad \square$$

Ist nun $f \in \mathbb{K}[x]$ Polynom mit getrennten Nullstellen $\alpha_1, \dots, \alpha_n$ und $\mathbb{L} \supset \mathbb{K}$ eine Körpererweiterung, die alle α_i enthält, dann lässt $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ die Teilmenge $N(f) = \{\alpha_1, \dots, \alpha_n\} \subset \mathbb{L}$ invariant (Teil (b) des vorangehenden Lemmas). Die Einschränkung auf $N(f)$ ist daher eine Wirkung von G auf $N(f)$, und durch die Nummerierung der Nullstellen ist $N(f)$ mit $\{1, \dots, n\}$ identifiziert.

$$\begin{array}{ccc} N(f) & \xrightarrow{\cong} & \{1, \dots, n\} \\ \sigma \downarrow & & \downarrow \bar{\sigma} \\ N(f) & \xrightarrow{\cong} & \{1, \dots, n\} \end{array}$$

jedes $\sigma \in G$ permutiert $N(f) \cong \{1, \dots, n\}$, bildet also α_i ab auf $\alpha_{\bar{\sigma}i}$ für eine Permutation $\bar{\sigma} \in S_n$, und die Abbildung $\phi : \sigma \rightarrow \bar{\sigma} : G \rightarrow S_n$ ist ein Gruppenhomomorphismus.

Lemma 27.2. *Ist $\mathbb{L} = \mathbb{K}(\bar{\alpha})$ Zerfällungskörper eines Polynoms mit getrennten Nullstellen $\alpha_1, \dots, \alpha_n$, dann ist der Homomorphismus $\phi : \sigma \rightarrow \bar{\sigma} : G \rightarrow S_n$ injektiv und macht G zu einer Untergruppe von S_n .*

Beweis. Ist $\bar{\sigma} = \bar{\tau}$, so gilt $\sigma(\alpha_j) = \tau(\alpha_j)$ für alle j . Da \mathbb{L} durch \mathbb{K} (das unter σ, τ fix ist) sowie $\alpha_1, \dots, \alpha_n$ erzeugt wird, gilt $\sigma = \tau$ auf ganz \mathbb{L} . \square

Nun können wir zeigen, dass die frühere Definition der Galoisgruppe mit der jetzt gegebenen übereinstimmt:

Satz 27.1. *Es sei $f \in \mathbb{K}[x]$ ein Polynom mit getrennten Nullstellen $\alpha_1, \dots, \alpha_n$ und $\mathbb{L} = \mathbb{K}(\vec{\alpha})$ der Zerfällungskörper von f . Wir betrachten die Menge R aller Relationen zwischen den Nullstellen,*

$$R = \{H \in \mathbb{K}[\vec{x}] : H(\vec{\alpha}) = 0\}.$$

Es sei $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ und $\phi : G \rightarrow S_n$ wie oben. Dann gilt

$$\phi(G) = G_R := \{\bar{\sigma} \in S_n : \bar{\sigma}H \in R \text{ für alle } H \in R\}. \quad (86)$$

Beweis. “ \subset ”: Es sei $\sigma \in G$ und $\bar{\sigma} = \sigma|_{N(f)} \in S_n$, wobei $N(f) = \{\alpha_1, \dots, \alpha_n\}$ mit $\{1, \dots, n\}$ identifiziert ist. Wir setzen

$$\sigma(\vec{\alpha}) = (\sigma\alpha_1, \dots, \sigma\alpha_n) = (\alpha_{\bar{\sigma}1}, \dots, \alpha_{\bar{\sigma}n}).$$

Für jedes $H \in R$ ist

$$(\bar{\sigma}H)(\vec{\alpha}) = H(\bar{\sigma}\vec{\alpha}) \stackrel{*}{=} \sigma(H(\vec{\alpha})) = 0.$$

(Dabei gilt “ $\stackrel{*}{=}$ ”, weil die Koeffizienten von H in \mathbb{K} liegen und von σ fix gelassen werden; nur die α_i werden permutiert.) Somit ist $\bar{\sigma} \in G_R$.

“ \supset ”: Es sei $\bar{\sigma} \in G_R \subset S_n$. Wir müssen dazu einen Automorphismus σ von \mathbb{L} finden, der \mathbb{K} fix lässt. Jedes Element von $\mathbb{L} = \mathbb{K}(\vec{\alpha})$ ist von der Form $F(\vec{\alpha})$ mit $F \in \mathbb{K}[\vec{x}]$. Wir setzen

$$\sigma(F(\vec{\alpha})) := F(\bar{\sigma}\vec{\alpha}) = (\bar{\sigma}F)(\vec{\alpha}).$$

Wir müssen zeigen, dass dies wohldefiniert ist: Wenn $F(\vec{\alpha}) = \tilde{F}(\vec{\alpha})$, dann soll $(\bar{\sigma}F)(\vec{\alpha}) = (\bar{\sigma}\tilde{F})(\vec{\alpha})$ gelten. Dies ist richtig, weil $H = \tilde{F} - F \in R$, denn $\tilde{F}(\alpha) - F(\alpha) = 0$. Also ist $\bar{\sigma}H \in R$ und damit

$$(\bar{\sigma}F)(\vec{\alpha}) - (\bar{\sigma}\tilde{F})(\vec{\alpha}) = (\bar{\sigma}H)(\vec{\alpha}) = 0. \quad \square$$

28. FORTSETZUNG VON KÖRPER-ISOMORPHISMEN

Wie groß ist die Galoisgruppe $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ einer Körpererweiterung $\mathbb{L} \supset \mathbb{K}$? Jedes Element von G ist eine Fortsetzung der identischen Abbildung $\text{id}_{\mathbb{K}}$ auf \mathbb{K} zu einem Automorphismus von \mathbb{L} . Wir fragen daher etwas allgemeiner: Gegeben seien zwei Körper \mathbb{K} und $\tilde{\mathbb{K}}$, die *isomorph* sind, d.h. es gebe eine bijektive Abbildung $\sigma : \mathbb{K} \rightarrow \tilde{\mathbb{K}}$, die die Rechenoperationen von \mathbb{K} in die von $\tilde{\mathbb{K}}$ überführt, einen *Körper-Isomorphismus*: $\sigma(0) = 0$, $\sigma(1) = 1$ und

$$\sigma(a + b) = \sigma(a) + \sigma(b), \quad \sigma(ab) = \sigma(a)\sigma(b).$$

Wie können wir σ auf den Zerfällungskörper eines Polynoms über \mathbb{K} mit getrennten Nullstellen fortsetzen? Genauer: Für jedes solche Polynom $f(x) = x^n + a_1x^{n-1} + \dots + a_n \in \mathbb{K}[x]$ mit Nullstellen $\alpha_1, \dots, \alpha_n$ haben wir ein entsprechendes Polynom $\tilde{f}(x) = x^n + \sigma(a_1)x^{n-1} + \dots + \sigma(a_n) \in \tilde{\mathbb{K}}[x]$ mit Nullstellen $\tilde{\alpha}_1, \dots, \tilde{\alpha}_n$, das wir auch σf nennen wollen. Die Nullstellenmengen $N(f)$ von f und $N(\tilde{f})$ von \tilde{f} sind aber völlig unabhängig voneinander durchnummeriert; da sie nicht zu \mathbb{K} bzw. $\tilde{\mathbb{K}}$ gehören, schafft σ keine Beziehung zwischen ihnen. Nun seien $\mathbb{L} = \mathbb{K}(\vec{\alpha})$ und $\tilde{\mathbb{L}} = \tilde{\mathbb{K}}(\vec{\tilde{\alpha}})$ die Zerfällungskörper von f und \tilde{f} . Auf wieviele Weisen können wir σ zu einem Körperisomorphismus $\hat{\sigma} : \mathbb{L} \rightarrow \tilde{\mathbb{L}}$ fortsetzen? Die Antwort gibt der folgende Satz, der diese Isomorphismen zählt:

Satz 28.1. *Gegeben sei ein Körperisomorphismus $\sigma : \mathbb{K} \rightarrow \tilde{\mathbb{K}}$ und ein Polynom $f \in \mathbb{K}[x]$ mit getrennten Nullstellen und mit Zerfällungskörper \mathbb{L} sowie $\tilde{f} = \sigma f$ mit Zerfällungskörper $\tilde{\mathbb{L}}$. Dann ist die Anzahl der Fortsetzungen $\hat{\sigma} : \mathbb{L} \rightarrow \tilde{\mathbb{L}}$ gleich dem Grad der Körpererweiterung,*

$$|\{\hat{\sigma} \in \text{Iso}(\mathbb{L}, \tilde{\mathbb{L}}) : \hat{\sigma}|_{\mathbb{K}} = \sigma\}| = [\mathbb{L} : \mathbb{K}]. \quad (87)$$

Beweis. Wir beweisen dies durch Induktion über den Grad der Körpererweiterung $[\mathbb{L} : \mathbb{K}]$. Wenn $[\mathbb{L} : \mathbb{K}] = 1$, ist $\mathbb{L} = \mathbb{K}$ und es gibt genau eine (triviale) Fortsetzung. Nun sei $[\mathbb{L} : \mathbb{K}] > 1$. Dann zerfällt f über \mathbb{K} nicht in Linearfaktoren, sonst wäre wieder $\mathbb{L} = \mathbb{K}$. Es gibt also mindestens einen irreduziblen Faktor f_1 von f mit Grad $d \geq 2$. Wir wählen eine Nullstelle α von f_1 . Jede Fortsetzung $\hat{\sigma}$ bildet α auf eine der d Nullstellen von $\tilde{f}_1 = \sigma f_1$ ab, denn $\tilde{f}_1(\hat{\sigma}\alpha) = \hat{\sigma}(f_1(\alpha)) = \hat{\sigma}(0) = 0$. Damit gibt es auch genau d verschiedene Möglichkeiten, σ auf $\mathbb{K}(\alpha) \subset \mathbb{L}$ fortzusetzen. Wir halten eine dieser Möglichkeiten $\hat{\sigma}(\alpha) = \tilde{\alpha}$ fest und haben damit die Einschränkung σ_1 von $\hat{\sigma}$ auf $\mathbb{K}(\alpha)$ bereits festgelegt: $\hat{\sigma}|_{\mathbb{K}(\alpha)} = \sigma_1 : \mathbb{K}(\alpha) \rightarrow \tilde{\mathbb{K}}(\tilde{\alpha})$. Jetzt müssen wir noch σ_1 von $\mathbb{K}(\alpha)$ auf \mathbb{L} fortsetzen. Hier können wir die Induktionsvoraussetzung anwenden, denn nach Lemma 22.1 und Satz 21.1 ist

$$[\mathbb{L} : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(\alpha)] \cdot [\mathbb{K}(\alpha) : \mathbb{K}] = [\mathbb{L} : \mathbb{K}(\alpha)] \cdot d > [\mathbb{L} : \mathbb{K}(\alpha)].$$

Wir fassen f jetzt als Polynom über $\mathbb{K}(\alpha)$ auf; immer noch ist \mathbb{L} der Zerfällungskörper von f auch über $\mathbb{K}(\alpha)$. Nach Induktionsvoraussetzung ist also die Anzahl der Fortsetzungen $\hat{\sigma} : \mathbb{L} \rightarrow \tilde{\mathbb{L}}$ von $\sigma_1 : \mathbb{K}(\alpha) \rightarrow \tilde{\mathbb{K}}(\tilde{\alpha})$ gleich $[\mathbb{L} : \mathbb{K}(\alpha)] = [\mathbb{L} : \mathbb{K}]/d$. Da die Anzahl der Fortsetzungen σ_1 auf $\mathbb{K}(\alpha)$ gleich d ist, ist die Zahl der Fortsetzungen von σ insgesamt gleich $d \cdot [\mathbb{L} : \mathbb{K}]/d = [\mathbb{L} : \mathbb{K}]$. \square

Korollar 28.1. *Ist $\mathbb{L} \supset \mathbb{K}$ der Zerfällungskörper eines Polynoms $f \in \mathbb{K}[x]$ mit getrennten Nullstellen, so gilt*

$$|\text{Gal}(\mathbb{L}, \mathbb{K})| = [\mathbb{L} : \mathbb{K}]. \quad (88)$$

29. AUFLÖSBARKEIT DURCH RADIKALE

Warum gibt es für die allgemeine Gleichung von fünftem und höherem Grad keine Auflösungsformeln mehr? Das können wir auf ganz ähnliche Weise zeigen wie die Nicht-Konstruierbarkeit mancher Figuren mit Zirkel und Lineal: Diese Hilfsmittel reichen einfach nicht aus. Aber während wir bei den geometrischen Konstruktionsaufgaben nur den Grad der Körpererweiterung zu berücksichtigen brauchten, sind jetzt etwas feinere Hilfsmittel notwendig, eben die Galoisgruppe.

Die mit Zirkel und Lineal konstruierbaren Zahlen liegen in einer Körpererweiterung $\mathbb{K}_r \supset \mathbb{Q}$ durch (iterierte) Quadratwurzeln:

$$\mathbb{K}_0 = \mathbb{Q}, \quad \mathbb{K}_{j+1} = \mathbb{K}_j(\alpha_j) \text{ mit } \alpha_j^2 \in \mathbb{K}_j.$$

Jetzt dagegen geht es um Körpererweiterungen durch (iterierte) Wurzeln von beliebigem Grad, wenn man fordert, dass in einer Auflösungsformel nur die vier Grundrechenarten sowie (iterierte) Wurzeln beliebigen Grades vorkommen dürfen, wie zum Beispiel in der Cardanoschen Formel

$$x = \alpha = \sqrt[3]{b + \sqrt{a^3 + b^2}} + \sqrt[3]{b - \sqrt{a^3 + b^2}}$$

für die Lösung der kubischen Gleichung $x^3 + 3ax = 2b$, siehe (10). Wenn also eine Lösung $x = \alpha$ einer Gleichung $f(x) = 0$ mit $f \in \mathbb{Q}[x]$ durch eine solche Formel dargestellt werden kann, durch "Radikale" (Wurzeln) aufgelöst werden kann, dann muss α in einer Körpererweiterung $\mathbb{K}_r \supset \mathbb{Q}$ liegen, wobei

$$\mathbb{K}_0 = \mathbb{Q}, \quad \mathbb{K}_{j+1} = \mathbb{K}_j(\alpha_j) \text{ mit } \alpha_j^{n_j} \in \mathbb{K}_j.$$

Da auch hier die Konstruktion von \mathbb{K}_r aus vielen Teilschritten besteht, müssen wir analog zu Lemma 22.1 zunächst verstehen, wie sich die Galoisgruppen bei mehrfachen Körpererweiterungen verhalten.

Lemma 29.1. *Sind $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{L}$ endliche Körpererweiterungen, so ist $\text{Gal}(\mathbb{L}, \mathbb{K}')$ eine Untergruppe von $\text{Gal}(\mathbb{L}, \mathbb{K})$. Ist $\mathbb{K}' \supset \mathbb{K}$ eine normale Körpererweiterung, also Zerfällungskörper eines Polynoms $g \in \mathbb{K}[x]$ mit getrennten Nullstellen, dann lassen die Elemente $\text{Gal}(\mathbb{L}, \mathbb{K})$ den Körper \mathbb{K}' invariant,¹⁴¹ und $\text{Gal}(\mathbb{L}, \mathbb{K}')$ ist sogar Normalteiler von $\text{Gal}(\mathbb{L}, \mathbb{K})$.*

¹⁴¹Man beachte den Unterschied zwischen "invariant" und "fest" oder "fix". Jedes $\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K})$ lässt \mathbb{K} fix, d.h. $\sigma(a) = a$ für jedes $a \in \mathbb{K}$, aber \mathbb{K}' nur invariant, d.h. $\sigma(\mathbb{K}') = \mathbb{K}'$ oder $\sigma(\alpha) \in \mathbb{K}'$ für alle $\alpha \in \mathbb{K}'$.

Beweis. Die Gruppe $\text{Gal}(\mathbb{L}, \mathbb{K}')$ besteht aus allen Automorphismen von \mathbb{L} , die \mathbb{K}' fest lassen. Das ist eine stärkere Bedingung als nur den kleineren Körper \mathbb{K} festzulassen, deshalb ist $\text{Gal}(\mathbb{L}, \mathbb{K}')$ eine Teilmenge und damit eine Untergruppe¹⁴² von $\text{Gal}(\mathbb{L}, \mathbb{K})$. Ist \mathbb{K}' der Zerfällungskörper von $f \in \mathbb{K}[x]$, so erhält jedes $\tau \in \text{Gal}(\mathbb{L}, \mathbb{K})$ das Polynom g , also seine Nullstellenmenge und damit seinen Zerfällungskörper \mathbb{K}' . Für alle $\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K}')$ und $\tau \in \text{Gal}(\mathbb{L}, \mathbb{K})$ ist nun $\tau^{-1}\sigma\tau \in \text{Gal}(\mathbb{L}, \mathbb{K}')$, denn für jedes $\alpha \in \mathbb{K}'$ ist $\tau\alpha \in \mathbb{K}'$ und somit $\sigma\tau\alpha = \tau\alpha$, und $\tau^{-1}\sigma\tau\alpha = \alpha$. Deshalb ist $\text{Gal}(\mathbb{L}, \mathbb{K}')$ Normalteiler in $\text{Gal}(\mathbb{L}, \mathbb{K})$. \square

Lemma 29.2. *Es seien $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{L}$ endliche Körpererweiterungen und $\mathbb{K}' \supset \mathbb{K}$ sowie $\mathbb{L} \supset \mathbb{K}$ seien normal, d.h. \mathbb{K}' und \mathbb{L} seien die Zerfällungskörper von Polynomen $g, f \in \mathbb{K}[x]$ mit getrennten Nullstellen. Dann gilt*

$$\text{Gal}(\mathbb{K}', \mathbb{K}) \cong \text{Gal}(\mathbb{L}, \mathbb{K}) / \text{Gal}(\mathbb{L}, \mathbb{K}'). \quad (89)$$

Beweis. Jedes $\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K})$ lässt \mathbb{K}' nach dem vorstehenden Lemma invariant, also definiert die Einschränkung $\bar{\sigma} = \sigma|_{\mathbb{K}'}$ einen Automorphismus von \mathbb{K}' , der \mathbb{K} fest lässt, also ein Element von $\text{Gal}(\mathbb{K}', \mathbb{K})$. Umgekehrt lässt sich jedes $\bar{\sigma} \in \text{Gal}(\mathbb{K}', \mathbb{K})$ auf \mathbb{L} fortsetzen zu einem Element $\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K})$, wie Satz 28.1 gezeigt hat. Die Einschränkungsabbildung $\rho : \text{Gal}(\mathbb{L}, \mathbb{K}) \rightarrow \text{Gal}(\mathbb{K}', \mathbb{K})$, $\sigma \mapsto \bar{\sigma}$, definiert also einen surjektiven Gruppenhomomorphismus. Dabei ist $\bar{\sigma} = \text{id} \iff \sigma \in \text{Gal}(\mathbb{L}, \mathbb{K}')$; der Kern des Homomorphismus ρ , die Menge $\ker \rho = \rho^{-1}(\text{id}) = \{\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K}) : \bar{\sigma} = \text{id}_{\mathbb{K}'}\}$ ist also der Normalteiler $\text{Gal}(\mathbb{L}, \mathbb{K}')$. Damit folgt die Behauptung aus dem *Homomorphiesatz*, siehe folgendes Lemma. \square

Lemma 29.3. *Es seien G, H Gruppen und $\rho : G \rightarrow H$ ein surjektiver Gruppenhomomorphismus. Dann ist $K = \ker \rho = \{g \in G : \rho(g) = e\}$ ein Normalteiler in G , und ρ definiert einen Isomorphismus*

$$\bar{\rho} : G/K \rightarrow H, \quad gK \mapsto \rho(g).$$

Beweis. K ist Untergruppe, denn $e \in K$, weil $\rho(e) = e$, und mit $k, k' \in K$ ist auch $kk' \in K$, weil $\rho(kk') = \rho(k)\rho(k') = e \cdot e = e$, und K ist Normalteiler, weil $\rho(gkg^{-1}) = \rho(g)\rho(k)\rho(g^{-1}) = \rho(g)\rho(k)\rho(g^{-1}) = e$. Die Abbildung $\bar{\rho}$ ist wohldefiniert, d.h. $\bar{\rho}(gK)$ hängt nur von gK ab, nicht von g selbst: Wenn wir g durch gk ersetzen für ein $k \in K$ (also $gK = gkK$), dann ist $\rho(gk) = \rho(g)\rho(k) = \rho(g)e = \rho(g)$. Sie ist injektiv: Wenn $\rho(gK) = \rho(\tilde{g}K)$, dann ist $\rho(g) = \rho(\tilde{g})$ und damit $e = \rho(g)^{-1}\rho(\tilde{g}) = \rho(g^{-1}\tilde{g})$, also ist $g^{-1}\tilde{g} = k \in K$ und somit $\tilde{g} = gk$,

¹⁴²Wenn σ und τ den Körper \mathbb{K}' fest lassen, dann auch $\sigma\tau$, und das Neutralelement id lässt ohnehin alles fest.

also $\tilde{g}K = gK$. Die Abbildung $\bar{\rho}$ ist surjektiv, weil ρ surjektiv ist. Sie ist ein Gruppenhomomorphismus, denn $\bar{\rho}(gK \cdot \tilde{g}K) = \bar{\rho}(g\tilde{g}K) = \rho(g\tilde{g}) = \rho(g)\rho(\tilde{g}) = \bar{\rho}(gK)\bar{\rho}(\tilde{g}K)$. \square

Satz 29.1. *Es sei $f \in \mathbb{K}[x]$ ein Polynom mit getrennten Nullstellen und \mathbb{L} sein Zerfällungskörper. Dieser entstehe aus \mathbb{K} durch sukzessive Adjunktion von r Wurzeln der Grade n_1, \dots, n_r . Der Grundkörper \mathbb{K} möge alle n_j -ten Einheitswurzeln enthalten für $j = 1, \dots, r$. Dann ist die Gruppe $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ auflösbar, d.h. es gibt eine absteigende Reihe von Untergruppen*

$$G = G_0 \supset G_1 \supset G_2 \supset \dots \supset G_r = \{\text{id}\}$$

derart, dass G_j in G_{j-1} ein Normalteiler und G_{j-1}/G_j abelsch ist für $j = 1, \dots, r$.¹⁴³

Beweis. Nach Voraussetzung gibt es zu dem Zerfällungskörper $\mathbb{L} \supset \mathbb{K}$ von f eine Folge von Teilkörpern

$$\mathbb{K} = \mathbb{K}_0 \subset \mathbb{K}_1 \subset \dots \subset \mathbb{K}_r = \mathbb{L}$$

derart, dass $\mathbb{K}_{j+1} = \mathbb{K}_j(\beta_j)$ mit $\beta_j^{n_j} \in \mathbb{K}_j$. Wir setzen $G_j = \text{Gal}(\mathbb{L}, \mathbb{K}_j)$, dann ist

$$G = G_0 \supset G_1 \supset \dots \supset G_r = \{\text{id}\}.$$

Nach Lemma 29.2 ist G_{j+1} ein Normalteiler in G_j , und $G_{j+1}/G_j \cong \text{Gal}(\mathbb{K}_j(\beta_j) : \mathbb{K}_j)$. Da $x = \beta_j$ die Gleichung $x^{n_j} = b_j$ mit $b_j = \beta_j^{n_j} \in \mathbb{K}_j$ löst, ist die Gruppe $\text{Gal}(\mathbb{K}_j(\beta_j) : \mathbb{K}_j)$ abelsch (sogar zyklisch) nach Beispiel 5, Seite 54. Damit ist G auflösbar. \square

Bemerkung 1. Die Voraussetzungen sind eigentlich zu stark. Wir wollen eigentlich nicht voraussetzen, dass $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ genau durch Adjunktion der Wurzeln β_1, \dots, β_r entsteht, sondern nur, dass die α_i mit Hilfe dieser Wurzeln ausgedrückt werden kann. Also sollte nicht $\mathbb{L} = \mathbb{K}_r$, sondern nur $\mathbb{L} \subset \mathbb{K}_r$ gelten. Nach Lemma 29.2 gilt dann aber $\text{Gal}(\mathbb{L}, \mathbb{K}) \cong \text{Gal}(\mathbb{K}_r, \mathbb{K}) / \text{Gal}(\mathbb{K}_r, \mathbb{L})$, und die Eigenschaft von $G = \text{Gal}(\mathbb{K}_r, \mathbb{K})$, auflösbar zu sein, vererbt sich auf die Quotientengruppe $\text{Gal}(\mathbb{K}_r, \mathbb{K}) / \text{Gal}(\mathbb{K}_r, \mathbb{L})$.

Bemerkung 2. Man kann auf die Adjunktion der Einheitswurzeln in der Voraussetzung verzichten. Dann muss man in jedem Schritt die benötigten Einheitswurzeln adjungieren; die zugehörige Galoisgruppe ist ebenfalls abelsch nach Beispiel 4, Seite 53. Statt des Zerfällungskörpers \mathbb{L}_o erhält man einen größeren Körper \mathbb{L} mit $\text{Gal}(\mathbb{L}, \mathbb{Q})$ auflösbar

¹⁴³ Die Eigenschaft, "auflösbar" zu sein, ist ja rein gruppentheoretisch. Die Bezeichnung stammt aber aus dem Zusammenhang mit der Auflösung von Gleichungen.

(siehe Fußnote 143), und $\text{Gal}(\mathbb{L}_o, \mathbb{Q}) = \text{Gal}(\mathbb{L}, \mathbb{Q}) / \text{Gal}(\mathbb{L}, \mathbb{L}_o)$ ist dann ebenfalls auflösbar.

30. NICHT-AUFLÖSBARKEIT BEI GRAD $n \geq 5$

Wir wollen zunächst zeigen, dass die symmetrische Gruppe S_n nicht auflösbar ist und daher ist eine Gleichung n -ten Grades mit Galoisgruppe S_n , $n \geq 5$, nicht durch Radikale gelöst werden kann für alle $n \geq 5$. Wir zeigen sogar mehr, nämlich dass A_n der einzige echte Normalteiler von S_n ist und A_n selbst sogar eine *einfache* Gruppe ist, d.h. überhaupt keinen echten Normalteiler besitzt.

Ein Normalteiler N in einer Gruppe G ist invariant unter Konjugation und daher Vereinigung von *Konjugationsklassen* von G . Die Konjugationsklassen in S_n sind leicht zu bestimmen: Jede Permutation $\sigma \in S_n$ lässt sich in ja disjunkte Zykeln zerlegen¹⁴⁴ und bestimmt damit eine *Partition* (additive Zerlegung) von n , nämlich die Längen der Zykeln in σ . Zum Beispiel zu $\sigma = \begin{bmatrix} 123456789 \\ 384627195 \end{bmatrix} = (13467)(2895)$ gehört die Zerlegung $9 = 5 + 4$. Konjugieren wir ein Produkt von disjunkten Zykeln, so ändern sich nur die Einträge in den Zykeln, aber nicht ihre Längen, und umgekehrt sind zwei Permutationen mit den gleichen Zykellängen konjugiert. Jede Partition von n beschreibt damit eine Konjugationsklasse. Zum Beispiel ist $\tau = (1497)(25386)$ zu σ konjugiert unter der Permutation $\begin{bmatrix} 123456789 \\ 215378649 \end{bmatrix}$, die die Zahlen in entsprechenden Zykeln von σ und τ austauscht. Für $n = 5$ gibt es die Partitionen 5 , $4 + 1$, $3 + 2$, $3 + 2 \cdot 1$, $2 \cdot 2 + 1$, $2 + 3 \cdot 1$, $5 \cdot 1$. Jede Konjugationsklasse von G ist eine Bahn unter der Wirkung von G auf sich selbst ($X = G$) durch $\phi : G \times G \rightarrow G$, $\phi_g(x) = gxg^{-1}$; ihre Länge ergibt sich aus der Formel $|G\sigma| = |G|/|G_\sigma|$ (Satz 16.1, Seite 48). Haben wir eine Permutation σ in disjunkte Zykeln zerlegt, $\sigma = \zeta_1 \dots \zeta_k$, dann ist ihre Standgruppe unter der Wirkung durch Konjugation leicht zu bestimmen: Es ist das direkte Produkt der von den Zykeln ζ_j erzeugten zyklischen Gruppen sowie der Permutationsgruppen der Mengen gleichlanger Zykeln.¹⁴⁵ Für die Konjugationsklassen von $G = S_5$ mit

¹⁴⁴Es sei $\sigma \in S_n$ beliebig. Der erste Zykel ist $\zeta_1 = (1, \sigma 1, \sigma^2 1, \dots, \sigma^{k_1} 1)$, wobei k_1 die kleinste natürliche Zahl mit $\sigma^{k_1+1} 1 = 1$ ist. Wenn ζ_1 noch nicht alle Zahlen $1, \dots, n$ enthält, wählt man eine Zahl $j \in \{1, \dots, n\} \setminus \{1, \sigma 1, \dots, \sigma^{k_1} 1\}$; dazu gibt es eine kleinste Zahl k_2 mit $\sigma^{k_2+1} j = j$; der zweite Zykel in σ ist $\zeta_2 = (j, \sigma j, \dots, \sigma^{k_2} j)$, usw. Beispiel: $\begin{bmatrix} 123456789 \\ 384627195 \end{bmatrix} = (13467)(2895)$.

¹⁴⁵Beweis: Ist $\sigma = \zeta_1 \dots \zeta_k$, so ist $\tau\sigma\tau^{-1} = \tilde{\zeta}_1 \dots \tilde{\zeta}_k$, wobei die Einträge von $\tilde{\zeta}_j$ die τ -Bilder der Einträge von ζ_j sind: Ist $\zeta_j = (i_1, \dots, i_l)$, so ist $\tilde{\zeta}_j = \tau\zeta_j\tau^{-1} = (\tau i_1, \dots, \tau i_l)$. Nun sei $\tau \in G_\sigma$, also $\tau\sigma\tau^{-1} = \sigma$. Wenn ζ_j der einzige Zykel der Länge l ist, dann muss $\tilde{\zeta}_j = \zeta_j$ gelten, d.h. $(\tau i_1, \dots, \tau i_l)$ ist nur eine zyklische Permutation von (i_1, \dots, i_l) , also ist $\tau|_{\{i_1, \dots, i_l\}} \in \langle \zeta_j \rangle$. Wenn verschiedene Zyklen $\zeta_{j_1}, \dots, \zeta_{j_r}$ der

$|G| = 5! = 120$ folgt so für die Größe der Standgruppe und die Längen der Konjugationsklassen:

Partition von σ	5	4 + 1	3 + 2	3 + 2 · 1	2 · 2 + 1	2 + 3 · 1	5 · 1
$ G_\sigma $	5	4	3 · 2	3 · 2	2 · 2 · 2	2 · 6	120
$ G\sigma $	24	30	20	20	15	10	1

In der Tat addieren sich die Zahlen der letzten Zeile zu 120 auf. Die möglichen Normalteiler $N \subset S_5$ müssten sich aus solchen Konjugationsklassen zusammensetzen, wobei die Klasse des Neutralelements id dazu gehört, die nur ein Element hat, und $|N|$ muss ein Teiler der Gruppenordnung $|S_5| = 120$ sein. Die Teiler von 120 sind 60, 40, 30, 24, 20, 15, 12, 10, 8, 5, 4, 3, 2. Die kleinen Zahlen sind nicht möglich, weil die kleinste Konjugationsklasse $\neq \{\text{id}\}$ schon 10 Elemente hat. Da die Zahlen $|G\sigma|$ in der letzten Zeile der obigen Tabelle Teiler von 120 sind, aber die Klasse des Neutralelement immer dazu kommt, brauchen wir außer $\{\text{id}\}$ noch mindestens zwei weitere Konjugationsklassen und haben somit schon mehr als 25 Elemente in N . Die Zahlen 30 und 40 lassen sich aus den Zahlen $|G_\sigma|$ nicht zusammensetzen, erst $60 = 1 + 24 + 15 + 20$ ist möglich. Es gibt zwei Konjugationsklassen mit Länge 20, aber die vom Typ 3+2 ist nicht möglich, denn ein Element dieser Klasse, z.B. (123)(45) ergibt mit gewissen Elementen der Klasse 5 zusammen ein Element der nicht erlaubten Klasse $2 + 3 \cdot 1$, z.B. (15432)(123)(45) = (35). Die einzig möglichen Konjugationsklassen, abgesehen von $\{\text{id}\}$, sind also die vom Typ 5, $2 \cdot 2 + 1$, $3 + 2 \cdot 1$; diese bilden zusammen die Untergruppe A_5 der geraden Permutationen.

In A_5 spaltet sich die S_5 -Konjugationsklasse 5 mit 24 Elementen noch einmal in zwei A_5 -Konjugationsklassen mit je 12 Elementen auf, denn zum Beispiel die Zykeln (12345) und (12354) sind nicht unter geraden Permutationen konjugiert, sondern nur unter ungeraden wie (45). Aus den Zahlen 1, 12, 12, 15, 20 lässt sich aber kein echter Teiler von 60 zusammensetzen (der größte ist 30), wenn 1 dabeisein muss. Deshalb ist A_5 einfach.

Satz 30.1. *Die Gruppe A_n ist einfach für alle $n \geq 5$.*

Beweis. Der Beweis geschieht durch Induktion nach n für $n \geq 5$. Den Induktionsanfang bei $n = 5$ haben wir schon gemacht. Von jetzt an sei $n \geq 6$. Die Gruppe A_{n-1} ist nach Induktionsvoraussetzung einfach, und sie ist in A_n enthalten als die Untergruppe, die die letzte Zahl n der Zahlen $\{1, \dots, n\}$ fest lässt. Wir nehmen an, dass ein Normalteiler

Länge l in der Zerlegung $\sigma = \zeta_1 \dots \zeta_k$ vorkommen, kann $\tau \zeta_{j_s} \tau^{-1}$ ein anderer Zykel derselben Länge sein; es gibt also eine Permutation $\pi \in S_r$ mit $\tau \zeta_{j_s} \tau^{-1} = \zeta_{j_{\pi s}}$. Diese Bedingungen an τ sind auch hinreichend, jedes solche τ liegt in G_σ .

$H \subset A_n$ gegeben ist. Dann ist $H \cap A_{n-1}$ ein Normalteiler in A_{n-1} . Weil A_{n-1} einfach ist, muss $H \cap A_{n-1} = A_{n-1}$ oder $H \cap A_{n-1} = \{\text{id}\}$ gelten.

Fall 1: $H \cap A_{n-1} = A_{n-1}$, also $A_{n-1} \subset H$. Als Untergruppe von A_n wirkt H auf der Menge $X = \{1, \dots, n\}$, und weil $H \neq \{\text{id}\}$ Normalteiler ist, wirkt H transitiv: Wenn $\sigma \in H$ mit $\sigma(1) = j$ für irgend ein $j \in \{2, \dots, n\}$, dann gibt es zu jedem $k \in \{2, \dots, n\}$ eine Permutation $\tau \in A_n$ mit $\tau 1 = 1$ und $\tau j = k$, und $\tau \sigma \tau^{-1} 1 = \tau \sigma 1 = \tau j = k$, und $\tau \sigma \tau^{-1} \in H$. Die Standgruppe von n unter H enthält A_{n-1} , und nach Satz 16.1 ist $n = |Hn| = |H|/|H_n| \leq |H|/|A_{n-1}|$, also $|H| \geq n|A_{n-1}| = |A_n|$, somit $H = A_n$.

Fall 2: $H \cap A_{n-1} = \{\text{id}\}$: Da $A_{n-1} = \{\sigma \in A_n : \sigma n = n\}$, gibt es kein $\sigma \in H \setminus \{\text{id}\}$ mit $\sigma n = n$. Jedes $\sigma \in H$ ist also bereits durch seinen Wert σn festgelegt; gäbe es ein von σ verschiedenes $\tau \in H$ mit $\tau n = \sigma n$, dann würde $\tau^{-1}\sigma$ die Zahl n festhalten. Und doch können wir ein solches τ konstruieren, wenn $n \geq 6$ und $H \neq \{\text{id}\}$. Weil H als Normalteiler von A_n transitiv auf $\{1, \dots, n\}$ wirkt (siehe Fall 1), finden wir ein $\sigma \in H$ mit $\sigma(n) = 1$ und setzen $\sigma(n-1) = j$. Nun wählen wir $\rho \in A_n$ mit $\rho(n) = n$, $\rho(n-1) = n-1$, $\rho(1) = 1$ und $\rho(j) = k \neq j$, z.B. $\rho = (jkl)$, wobei $j, k, l \in \{2, \dots, n-2\}$ alle verschieden sind. Für $\tau = \rho\sigma\rho^{-1} \in H$ gilt dann $\tau(n) = \rho\sigma(n) = \rho(1) = 1 = \sigma(n)$, aber $\tau(n-1) = \rho\sigma(n-1) = \rho(j) = k \neq \sigma(n-1)$, also $\sigma \neq \tau$, Widerspruch! \square

31. DER HAUPTSATZ DER GALOISTHEORIE

Zu einer Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ haben wir die *Galoisgruppe*

$$G = \text{Gal}(\mathbb{L}, \mathbb{K}) = \{\sigma \in \text{Aut}(\mathbb{L}) : \sigma|_{\mathbb{K}} = \text{id}\}$$

definiert. Speziell wählen wir \mathbb{L} als den *Zerfällungskörper* \mathbb{L}_f eines Polynoms $f \in K[x]$ mit getrennten Nullstellen; dann sagt uns die Galoisgruppe etwas darüber aus, wie schwierig es ist, die Gleichung $f(x) = 0$ zu lösen. Die Nullstellenmenge von f sei $N(f) = \{\alpha_1, \dots, \alpha_n\} \subset \mathbb{L}$. Der *Hauptsatz der Galoistheorie* stellt eine enge Verbindung her zwischen den Untergruppen $G_1 \subset G$ und den Zwischenkörpern \mathbb{K}_1 mit $\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{L}$. Jeder Untergruppe $G_1 \subset G$ kann man ihre Fixpunktmenge

$$\mathbb{L}^{G_1} := \{\alpha \in \mathbb{L} : \sigma\alpha = \alpha \ \forall \sigma \in G_1\} \quad (90)$$

zuordnen, und diese ist ein Teilkörper von \mathbb{L} , denn mit $\alpha, \beta \in \mathbb{L}^{G_1}$ gilt offensichtlich auch $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in \mathbb{L}^{G_1}$. Da $\mathbb{K} \subset \mathbb{L}^{G_1}$ (weil \mathbb{K} ja fix unter ganz G ist), ist \mathbb{L}^{G_1} ein Zwischenkörper, der *Fixkörper* der Untergruppe $G_1 \subset G \subset \text{Aut}(\mathbb{L})$. Umgekehrt können wir einem

Zwischenkörper \mathbb{K}_1 mit $\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{L}$ eine Untergruppe von G zuordnen, die Galoisgruppe von \mathbb{K}_1 :

$$\text{Gal}(\mathbb{L}, \mathbb{K}_1) = \{\sigma \in \text{Aut}(\mathbb{L}) : \sigma|_{\mathbb{K}_1} = \text{id}\}. \quad (91)$$

Der Hauptsatz sagt, dass diese beiden Zuordnungen zueinander invers sind:

Satz 31.1. *Es sei $f \in \mathbb{K}[x]$ ein Polynom mit getrennten Nullstellen, $\mathbb{L} = \mathbb{L}_f \supset \mathbb{K}$ sein Zerfällungskörper (Galoiserweiterung) und $G = \text{Gal}(\mathbb{L}, \mathbb{K})$. Dann gilt: Die Zwischenkörper \mathbb{K}_1 mit $\mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{L} = \mathbb{L}_f$ sind genau die Fixkörper der Untergruppen $G_1 \subset G$. Die beiden Zuordnungen*

$$\begin{aligned} \{\text{Untergruppen}\} &\rightarrow \{\text{Zwischenkörper}\} \\ G \supset G_1 &\mapsto \mathbb{L}^{G_1} \subset \mathbb{L}, \\ \{\text{Zwischenkörper}\} &\rightarrow \{\text{Untergruppen}\} \\ \mathbb{L} \supset \mathbb{K}_1 &\mapsto \text{Gal}(\mathbb{L}, \mathbb{K}_1) \subset G \end{aligned}$$

verkehren die Inklusionen (sie sind “antiton” bezüglich der Inklusion) und sie sind zueinander invers:

$$\text{Gal}(\mathbb{L}, \mathbb{L}^{G_1}) = G_1, \quad \mathbb{L}^{\text{Gal}(\mathbb{L}, \mathbb{K}_1)} = \mathbb{K}_1. \quad (92)$$

Da $\text{Gal}(\mathbb{L}, \mathbb{L}^{G_1})$ aus den Automorphismen von \mathbb{L} besteht, die \mathbb{L}^{G_1} fix lassen, gehört G_1 auch dazu; es könnte aber vielleicht noch weitere solche Automorphismen geben:

$$\text{Gal}(\mathbb{L}, \mathbb{L}^{G_1}) \supset G_1. \quad (93)$$

Weil $\text{Gal}(\mathbb{L}, \mathbb{K}_1)$ den Körper \mathbb{K}_1 fix lässt, liegt \mathbb{K}_1 eben im Fixkörper von $\text{Gal}(\mathbb{L}, \mathbb{K}_1)$, aber diese Gruppe könnte ja vielleicht noch weitere Elemente von \mathbb{L} fix lassen:

$$\mathbb{L}^{\text{Gal}(\mathbb{L}, \mathbb{K}_1)} \supset \mathbb{K}_1. \quad (94)$$

Dass bei beiden Inklusionen in Wahrheit Gleichheit gilt, sehen wir aus dem folgenden Satz von Artin:¹⁴⁶

Satz 31.2. *Es sei $\mathbb{L} \supset \mathbb{K}$ eine Galoiserweiterung, $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ und $G_1 \subset G$ eine Untergruppe. Der Fixkörper von G_1 sei $\mathbb{K}_1 = \mathbb{L}^{G_1} \supset \mathbb{K}$. Dann ist \mathbb{L} der Zerfällungskörper eines irreduziblen Polynoms g über \mathbb{K}_1 , d.h. $g \in \mathbb{K}_1[x]$, und es gilt $G_1 = \text{Gal}(\mathbb{L}, \mathbb{K}_1)$.*

Beweis. Für jedes $\alpha \in \mathbb{L}$ betrachten wir die Bahn $G_1\alpha = \{\alpha_1, \dots, \alpha_m\}$ unter der Wirkung von G_1 auf \mathbb{L} und das Polynom

$$g_\alpha(x) = (x - \alpha_1) \dots (x - \alpha_m)$$

¹⁴⁶Emil Artin, 1898 (Wien) - 1962 (Hamburg)

mit Nullstellen $\alpha_1, \dots, \alpha_m$. Da jedes $\sigma \in G_1$ die Wurzeln permutiert (sie bilden ja eine Bahn von G_1), werden die Koeffizienten von g_α (als symmetrische Polynome in $\vec{\alpha}$) von σ fix gelassen, liegen also in $\mathbb{L}^{G_1} = \mathbb{K}_1$. Somit ist $g_\alpha \in \mathbb{K}_1[x]$.

Wir werden im nächsten Abschnitt sehen, dass der Körper \mathbb{L} über \mathbb{K} von einem einzigen Element $\alpha \in \mathbb{L}$ erzeugt wird, dem *primitiven Element*, also $\mathbb{L} = \mathbb{K}(\alpha)$, und wir wählen $g = g_\alpha$ für dieses Element α . Insbesondere ist $\mathbb{L} = \mathbb{K}(\alpha) = \mathbb{K}_1(\alpha)$ der Zerfällungskörper von g über \mathbb{K}_1 , denn auch die anderen Nullstellen von g (die Elemente von $G_1\alpha$) liegen ja in \mathbb{L} . Somit haben wir

$$\begin{aligned} \text{einerseits: } [\mathbb{L} : \mathbb{K}_1] &= [\mathbb{K}_1(\alpha) : \mathbb{K}_1] \leq \partial g = m \leq |G_1|, \\ \text{andererseits: } [\mathbb{L} : \mathbb{K}_1] &= |\text{Gal}(\mathbb{L}, \mathbb{K}_1)| \geq |G_1|, \end{aligned}$$

da $\text{Gal}(\mathbb{L}, \mathbb{K}_1) \supset G_1$, und somit gilt $\text{Gal}(\mathbb{L}, \mathbb{K}_1) = G_1$. \square

Beweis von Satz 31.1: Wenn die Untergruppe G_1 gegeben ist, so haben wir $G_1 = \text{Gal}(\mathbb{L}, \mathbb{L}^{G_1})$ nach dem gerade bewiesenen Satz 31.2, also gilt Gleichheit in (93). Wenn andererseits der Zwischenkörper \mathbb{K}_1 gegeben ist, dann ist $G_1 := \text{Gal}(\mathbb{L}, \mathbb{K}_1)$ nach Satz 31.2 zugleich die Galoisgruppe der Körpererweiterung $\mathbb{L} \supset \mathbb{L}^{G_1}$ und somit

$$[\mathbb{L} : \mathbb{K}_1] = |G_1| = [\mathbb{L} : \mathbb{L}^{G_1}],$$

also folgt Gleichheit in (94). Die Umkehrung der Inklusionen folgt aus der Definition: Je größer G_1 , desto kleiner der Fixkörper \mathbb{L}^{G_1} , und je größer \mathbb{K}_1 , desto kleiner die Galoisgruppe $\text{Gal}(\mathbb{L}, \mathbb{K}_1)$. \square

32. DER SATZ VOM PRIMITIVEN ELEMENT

Satz 32.1. *Ist $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n) \supset \mathbb{K}$ eine endliche Körpererweiterung, so gibt es ein $\alpha \in \mathbb{L}$ ("primitives Element") mit $\mathbb{L} = \mathbb{K}(\alpha)$.*

Beweis. Wir zeigen die Existenz eines primitiven Elements durch Induktion über die Anzahl n der adjungierten Elemente. Für $n = 1$ ist nichts zu zeigen.

Induktionsschritt $n - 1 \rightarrow n$, $n \geq 2$: Es ist

$$\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n) = \mathbb{K}(\alpha_1)(\alpha_2, \dots, \alpha_n).$$

Nach Induktionsvoraussetzung ist $\mathbb{L} = \mathbb{K}(\alpha_1)(\beta)$ für ein $\beta \in \mathbb{L}$. Wir setzen

$$\alpha = c\alpha_1 + \beta$$

für ein geeignetes (noch zu bestimmendes) $c \in \mathbb{K}$. Wir betrachten die Minimalpolynome f und g für α_1 und β , die normierten Polynome kleinsten Grades über \mathbb{K} mit diesen Nullstellen. Dann ist α_1 eine einfache Nullstelle von f , denn f ist irreduzibel (gäbe es einen Teiler f_1 ,

so wäre f_1 oder f/f_1 ein Polynom von kleinerem Grad mit Nullstelle α_1). Mit einer Verschiebung des Arguments wird α_1 auch Nullstelle von (einer Modifikation von) g , nämlich von

$$g_c(x) := g(-cx + \alpha) \in \mathbb{K}(\alpha)[x].$$

Dann ist $g_c(\alpha_1) = g(-c\alpha_1 + c\alpha_1 + \beta) = g(\beta) = 0$, also ist α_1 gemeinsame Nullstelle von f und g_c . Durch Wahl von c (siehe unten) können wir erreichen, dass α_1 die *einzig*e gemeinsame Nullstelle ist. Somit ist $\text{ggT}(f, g_c) = x - \alpha_1$. Da beide Polynome f, g_c in $\mathbb{K}(\alpha)[x]$ liegen, gilt das gleiche für ihren größten gemeinsamen Teiler, und somit $\alpha_1 \in \mathbb{K}(\alpha)$. Dann ist auch $\beta = \alpha - c\alpha_1 \in \mathbb{K}(\alpha)$ und damit

$$\mathbb{L} = \mathbb{K}(\alpha_1, \beta) \subset \mathbb{K}(\alpha) \subset \mathbb{L},$$

also folgt Gleichheit und insbesondere $\mathbb{L} = \mathbb{K}(\alpha)$.

Wahl von $c \in \mathbb{K}$: Wir wollen c so wählen, dass α_1 die einzige gemeinsame Nullstelle von f und g_c ist, dass also die übrigen Nullstellen $\alpha_2, \dots, \alpha_n$ von f keine Nullstellen von g_c sind. Dabei ist

$$g_c(\alpha_j) = g(-c\alpha_j + \alpha) = g(-c\alpha_j + c\alpha_1 + \beta) = g(c(\alpha_1 - \alpha_j) + \beta),$$

und damit ist $g_c(\alpha_j) \neq 0 \iff c(\alpha_1 - \alpha_j) + \beta \notin N_g = \{\beta_1, \dots, \beta_r\}$, wobei N_g die Nullstellenmenge von g ist (mit $\beta_1 = \beta$). Für $j \in \{2, \dots, n\}$ ist $\alpha_1 - \alpha_j \neq 0$ und damit $g_c(\alpha_j) \neq 0 \iff c(\alpha_1 - \alpha_j) + \beta \neq \beta_k \iff c \neq (\alpha_1 - \alpha_j)^{-1}(\beta_k - \beta)$ für $k = 1, \dots, r$ und $j = 2, \dots, n$. Ein solches c existiert, weil \mathbb{K} unendlich viele Elemente hat. \square

33. NORMALE KÖRPERERWEITERUNGEN

Eine Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ heißt *normal* oder *Galoiserweiterung*, wenn \mathbb{L} der Zerfällungskörper eines Polynoms $f \in \mathbb{K}[x]$ mit getrennten Nullstellen ist, oder äquivalent, wenn $\mathbb{K} = \mathbb{L}^G$ für $G = \text{Gal}(\mathbb{L}, \mathbb{K})$.¹⁴⁷

Satz 33.1. *Gegeben sei eine normale Körpererweiterung $\mathbb{L} \supset \mathbb{K}$ mit Galoisgruppe $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ und ein Zwischenkörper $\mathbb{K}_1, \mathbb{K} \subset \mathbb{K}_1 \subset \mathbb{L}$. Dann sind die folgenden Aussagen äquivalent:*

- (a) $\mathbb{K}_1 \supset \mathbb{K}$ ist normale Körpererweiterung, $\mathbb{K}_1 = \mathbb{L}_g$,
- (b) $G_1 = \text{Gal}(\mathbb{L}, \mathbb{K}_1)$ ist ein Normalteiler von $G = \text{Gal}(\mathbb{L}, \mathbb{K})$.

Beweis. Wir zeigen, dass beide Eigenschaften zu einer dritten äquivalent sind, nämlich

- (c) Jedes $\sigma \in G = \text{Gal}(\mathbb{L}, \mathbb{K})$ lässt \mathbb{K}_1 invariant, $\sigma\mathbb{K}_1 = \mathbb{K}_1$.

¹⁴⁷“ \implies ”: $[\mathbb{L} : \mathbb{K}] = |G|$, aber auch $[\mathbb{L} : \mathbb{L}^G] = |G|$ nach Satz 31.2. Daraus folgt $\mathbb{K} = \mathbb{L}^G$, da ja bereits $\mathbb{K} \subset \mathbb{L}^G$. “ \Leftarrow ”: Direkt aus Satz 31.2: Da $\mathbb{K} = \mathbb{L}^G$, ist \mathbb{L} Zerfällungskörper eines Polynoms mit getrennten Nullstellen über \mathbb{K} .

“(c) \Rightarrow (a)” folgt direkt aus Satz 31.2, Seite 92.

“(a) \Rightarrow (c)”: $\mathbb{K}_1 = \mathbb{L}_g = \mathbb{K}(N_g) \Rightarrow \sigma(N_g) = N_g \Rightarrow \sigma(\mathbb{K}_1) = \mathbb{K}_1 \forall \sigma \in G$.

“(c) \Rightarrow (b)”: $G_1 = \ker \phi$ für $\phi : G \rightarrow \text{Gal}(\mathbb{K}_1, \mathbb{K})$, $\sigma \mapsto \sigma|_{\mathbb{K}_1}$.¹⁴⁸

“(b) \Rightarrow (c)”: $\sigma G_1 \sigma^{-1} = G_1 \Rightarrow \mathbb{K}_1 = \mathbb{L}^{G_1} = \mathbb{L}^{\sigma G_1 \sigma^{-1}} = \sigma \mathbb{L}^{G_1} = \sigma \mathbb{K}_1$.¹⁴⁹

□

34. LÖSUNG BEI AUFLÖSBARER GALOISGRUPPE

Das Ziel dieses Abschnittes ist die Umkehrung von Satz 29.1, nach dem jede durch Radikale auflösbare Gleichung eine auflösbare Galoisgruppe hat. Die von Galois bewiesene Umkehrung ist:

Satz 34.1. *Es sei $\mathbb{L} \supset \mathbb{K}$ eine normale Körpererweiterung, d.h. \mathbb{L} ist der Zerfällungskörper eines Polynoms $f \in \mathbb{K}[x]$ mit getrennten Nullstellen $\alpha_1, \dots, \alpha_n$. Wenn die Galoisgruppe $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ auflösbar ist, dann kann die Gleichung durch Radikale aufgelöst werden, d.h. jedes α_j kann durch eine Formel, in der nur die Grundrechenarten und iterierte Wurzeln vorkommen, aus den Koeffizienten a_1, \dots, a_n von f berechnet werden.*

Die Gruppe G ist bekanntlich genau dann auflösbar, wenn es eine absteigende Kette von Untergruppen gibt,

$$G \supset G_1 \supset \dots \supset G_r = \{e\}, \quad (95)$$

derart, dass G_{j+1} ein Normalteiler in G_j ist und der Quotient G_j/G_{j+1} (vgl. Fußnote 79, Seite 49) abelsch ist. Wir werden den Satz 34.1 durch Induktion nach der Länge r der Kette beweisen. Nach dem “Hauptsatz” Satz 31.1 gibt es zu (95) eine Kette von Körpern

$$\mathbb{K} \subset \mathbb{K}_1 \subset \dots \subset \mathbb{K}_r = \mathbb{L}, \quad (96)$$

und nach Satz 33.1 im vorigen Abschnitt ist $\mathbb{K}_j \subset \mathbb{K}_{j+1}$ eine normale Körpererweiterung mit abelscher Galoisgruppe (Lemma 29.1, Seite 86). Wir werden also zunächst Körpererweiterungen mit abelscher, zunächst sogar zyklischer Galoisgruppe untersuchen:

Lemma 34.1. *Es sei $\mathbb{L} \supset \mathbb{K}$ normale Körpererweiterung, $\mathbb{L} = \mathbb{L}_f = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ Zerfällungskörper eines Polynoms $f(x) = x^n + a_1 x^{n-1} + \dots + a_n \in \mathbb{K}[x]$ mit getrennten Nullstellen $\alpha_1, \dots, \alpha_n$, und \mathbb{K} enthalte die Menge $\Omega = \{\omega \in \mathbb{C} : \omega^n = 1\}$ der n -ten Einheitswurzeln. Die Galoisgruppe $G = \text{Gal}(f) = \text{Gal}(\mathbb{L}, \mathbb{K})$ werde von dem Zyklus $\sigma =$*

¹⁴⁸Der Kern eines Gruppenhomomorphismus ist ja stets ein Normalteiler!

¹⁴⁹ $\alpha \in \mathbb{L}^{\sigma G_1 \sigma^{-1}} \iff \forall \tau \in G_1 \sigma \tau \sigma^{-1} \alpha = \alpha \iff \tau \sigma^{-1} \alpha = \sigma^{-1} \alpha \iff \sigma^{-1} \alpha \in \mathbb{L}^{G_1} \iff \alpha \in \sigma \mathbb{L}^{G_1}$.

(12...n) erzeugt. Dann gibt es $\beta_2, \dots, \beta_n \in \mathbb{L}$ mit $(\beta_j)^n = b_j \in \mathbb{K}$ und $\mathbb{L} = \mathbb{K}(\beta_2, \dots, \beta_n)$, d.h. \mathbb{L} wird von n -ten Wurzeln über \mathbb{K} erzeugt.

Beweis. Wir benutzen die *Lagrangeschen Resolventen* wie schon im Abschnitt 13: Für jedes $\omega \in \Omega$ setzen wir $\beta_\omega = \sum_{j=1}^n \omega^j \alpha_j$. Dann ist $\sigma \beta_\omega = \sum_j \omega^j \alpha_{j+1} \stackrel{k:=j+1}{=} \sum_k \omega^{k-1} \alpha_k = \omega^{-1} \sum_k \omega^k \alpha_k = \omega^{-1} \beta_\omega$ (die Indizes j und k werden modulo n gerechnet) und $\sigma(\beta_\omega)^n = (\sigma \beta_\omega)^n = (\omega^{-1} \beta_\omega)^n = (\beta_\omega)^n$, da $\omega^n = 1$. Weil die Galoisgruppe G von σ erzeugt wird, gilt $b_\omega := (\beta_\omega)^n \in \mathbb{L}^G = \mathbb{K}$. Nur für $\omega = 1$ ist $\beta_\omega = \beta_1 = \sum_j \alpha_j = -a_1 \in \mathbb{K}$. Die übrigen $\omega \in \Omega \setminus \{1\}$ nummerieren wir als $\omega_2, \dots, \omega_n$ und setzen $\beta_j = \beta_{\omega_j}$; das sind die gesuchten n -ten Wurzeln von $b_j = b_{\omega_j} \in \mathbb{K}$. Wir müssen noch zeigen, dass wir umgekehrt die α_j als Linearkombinationen der β_ω darstellen können. Zunächst ist

$$\sum_{\omega} \beta_{\omega} = \sum_{\omega} \sum_j \omega^j \alpha_j = \sum_j \left(\sum_{\omega} \omega^j \right) \alpha_j = n \alpha_n,$$

denn $\sum_{\omega} \omega^j$ ist die Summe über alle Einheitswurzeln, und diese ist Null,¹⁵⁰ außer im Fall $j = n$, denn $\omega^n = 1$. Die übrigen α_j erhalten wir auf ähnliche Weise:

$$\sum_{\omega} \omega^k \beta_{\omega} = \sum_j \sum_{\omega} \omega^k \omega^j \alpha_j = \sum_j \left(\sum_{\omega} \omega^{j+k} \right) \alpha_j = n \alpha_{n-k},$$

denn es gilt auch $\sum_{\omega} \omega^{j+k} = 0$, außer im Fall $j+k = n$, also $j = n-k$, wo n -mal die Eins aufsummiert wird. \square

Lemma 34.2. *Es sei $\mathbb{L} = \mathbb{L}_f \supset \mathbb{K}$ Zerfällungskörper eines irreduziblen Polynoms $f \in \mathbb{K}[x]$ mit Nullstellen $\alpha_1, \dots, \alpha_n$, und $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ habe Primzahlordnung, d.h. $|G| = p$ sei Primzahl, dann gilt $p = n$ und G wird (bei richtiger Nummerierung der Wurzeln) von dem Zyklus $\sigma = (12\dots n)$ erzeugt.*

Beweis. Da f irreduzibel ist, wirkt G transitiv auf der Nullstellenmenge $\{\alpha_1, \dots, \alpha_n\}$. Die Bahn $G\alpha_1$ hat also die Länge n . Andererseits gilt $n = |G\alpha_1| = |G|/|H|$, wobei $H = G_{\alpha_1}$ die Standgruppe von α_1 unter der Wirkung von G ist, siehe Abschnitt 16, Seite 47. Also folgt $p = |G| = |G\alpha_1||H| = n|H|$, und somit ist n ein Teiler der Primzahl p , also $n = p$. Jedes Element $\sigma \in G$ mit $\sigma \neq \text{id}$ hat eine Ordnung¹⁵¹ $k > 1$,

¹⁵⁰Algebraische Begründung: Jedes $\omega \in \Omega \setminus \{1\}$ ist Nullstelle des Polynoms $(x^n - 1)/(x - 1) = x^{n-1} + x^{n-2} + \dots + x + 1$. Geometrische Begründung: Da die $\omega \in \Omega$ gleichmäßig auf dem Rand des Einheitskreises verteilt sind, ist ihr arithmetisches Mittel (ihr Schwerpunkt) $\frac{1}{n} \sum_{\omega \in \Omega} \omega$ gleich dem Kreismittelpunkt Null.

¹⁵¹Die Ordnung eines Gruppenelements $g \in G$ ist die kleinste Zahl $k \in \mathbb{N}$ mit $g^k = e$. Dabei sind $g^0 := e$, $g^1 := g$, $g^{j+1} := gg^j$ die Potenzen von g . Durch

und die von σ erzeugte Untergruppe $\langle \sigma \rangle \subset G$ hat k Elemente. Damit ist k ein Teiler der Gruppenordnung $|G| = p$ (Satz von Lagrange, siehe Fußnote 79, Seite 49), also $k = p = n$ und $\langle \sigma \rangle = G$. Bei entsprechender Nummerierung der Wurzeln folgt $\sigma^j \alpha_1 = \alpha_{j+1}$, also wirkt σ auf $\{\alpha_1, \dots, \alpha_n\} \cong \{1, \dots, n\}$ als Zykel $(12 \dots n)$. \square

Lemma 34.3. *Es sei $\mathbb{L}_f = \mathbb{L} \supset \mathbb{K}$ der Zerfällungskörper eines Polynoms $f \in \mathbb{K}[x]$ mit getrennten Nullstellen und $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ sei abelsch.¹⁵² Dann ist f durch Radikale auflösbar.*

Beweis. Wir benutzen Induktion über die Gruppenordnung $|G|$; Induktionsanfang $|G| = 1$ ist trivial. Wenn G zyklisch von Primzahlordnung ist, folgt die Behauptung aus den beiden voranstehenden Lemmas. Wenn nicht, können wir ein $\sigma \in G$ mit Ordnung p wählen für einen Primteiler p von $|G|$. So ein Element gibt es sicher, denn wenn ein Element $\hat{\sigma} \in G$ eine Ordnung $n = kp$ hat, dann hat $\hat{\sigma}^k$ die Ordnung p . Die Untergruppe $G_1 = \langle \sigma \rangle$ ist Normalteiler, denn jede Untergruppe einer abelschen Gruppe ist Normalteiler (die Konjugation in einer abelschen Gruppe ist trivial). Zu der Gruppenkette $\{\text{id}\} \subset G_1 \subset G$ gehört nach dem Hauptsatz 31.1 eine Körperkette $\mathbb{L} \supset \mathbb{K}_1 \supset \mathbb{K}$, und die Körpererweiterungen $\mathbb{L} \supset \mathbb{K}_1$ sowie $\mathbb{K}_1 \supset \mathbb{K}$ sind normal mit Galoisgruppen G_1 und G/G_1 . Nach Lemma 34.2 und 34.1 wird $\mathbb{L} \supset \mathbb{K}_1$ durch p -te Wurzeln von Elementen von \mathbb{K}_1 erzeugt, und auf $\mathbb{K}_1 \supset \mathbb{K}$ können wir die Induktionsvoraussetzung anwenden, da $|G/G_1| < |G|$, also ist auch $\mathbb{K}_1 \supset \mathbb{K}$ eine Erweiterung durch Radikale. \square

Der Beweis von Satz 34.1 folgt nun durch Induktion über die Länge r der Kette (95) von G in der Voraussetzung “ G auflösbar”. Siehe auch das Ende des folgenden Abschnittes.

35. ZWEI KURZE NACHTRÄGE

Der erste Nachtrag bezieht sich auf Transitivität der Wirkung der Galoisgruppe $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ mit $\mathbb{L} = \mathbb{L}_f = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ auf die Nullstellenmenge $N_f = \{\alpha_1, \dots, \alpha_n\}$, wenn $f \in \mathbb{K}[x]$ eine Polynom mit getrennten Nullstellen ist. In Beispiel 2 auf Seite 52 haben wir gesehen, dass G nicht transitiv wirkt, wenn f reduzibel ist ($f = f_1 f_2$ mit $f_1, f_2 \in$

Induktion über j gilt $g^j g^k = g^{j+k}$ für alle $j, k \in \mathbb{N}$ und auch $g^j (g^{-1})^k = g^{j-k}$ für $k \leq j$. Deshalb setzt man $(g^{-1})^k =: g^{-k}$. Wenn $|G|$ endlich ist, kann es nur endlich viele verschiedene Potenzen g^j geben, somit muss es $j, k \in \mathbb{N}$ geben mit $g^j = g^{j+k}$ und damit $e = g^{-j} g^{j+k} = g^k$. Es gibt also $k \in \mathbb{N}$ mit $g^k = e$; das kleinste solche k ist die Ordnung von g . Die von g erzeugte Untergruppe $\langle g \rangle$ besteht dann genau aus den Elementen $g, g^2, \dots, g^k = e$, hat also k Elemente.

¹⁵²Dieser Satz stammt von N.H. Abel, daher die Bezeichnung “abelsche Gruppe” für kommutative Gruppen.

$\mathbb{K}[x]$, beide vom Grad ≥ 1). Die Umkehrung, dass G transitiv wirkt, wenn f irreduzibel ist, haben wir verschiedentlich behauptet, aber nie bewiesen. Dabei ist es ganz einfach:

Satz 35.1. *Ist $f \in \mathbb{K}[x]$ irreduzibel mit Nullstellen¹⁵³ $\alpha_1, \dots, \alpha_n$ und $\mathbb{L} = \mathbb{L}_f$, dann operiert $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ transitiv auf der Nullstellenmenge $N_f = \{\alpha_1, \dots, \alpha_n\}$.*

Beweis. Andernfalls gibt es eine Bahn $G\alpha_1 = \{\alpha_1, \dots, \alpha_k\}$ (bei geeigneter Nummerierung) mit $k < n$. Die Koeffizienten des Polynoms

$$g(x) = (x - \alpha_1) \cdot \dots \cdot (x - \alpha_k)$$

sind die elementarsymmetrischen Polynome in $\alpha_1, \dots, \alpha_k$. Da jedes Element $\sigma \in G$ diese Nullstellen (die Elemente der Bahn $G\alpha_1$) permutiert, sind die Koeffizienten von g fix unter σ , liegen also in $\mathbb{L}^G = \mathbb{K}$. Damit ist $g \in \mathbb{K}[x]$, und g ist ein echter Teiler von f , vom Grad $k < n$. Also ist f dann nicht irreduzibel. \square

Der zweite Nachtrag bezieht sich darauf, dass man das gleiche Polynom ja über verschiedenen Körpern betrachten kann, zum Beispiel über \mathbb{Q} und über $\mathbb{Q}(\zeta_1, \dots, \zeta_r)$ für gewisse Einheitswurzeln ζ_1, \dots, ζ_r ; mehrfach haben wir ja angenommen, dass der Grundkörper verschiedene Einheitswurzeln enthält, die für die Konstruktionen gebraucht werden. Gegeben sei also ein Polynom $f \in \mathbb{K}[x]$ mit getrennten Nullstellen $\alpha_1, \dots, \alpha_n$ und sein Zerfällungskörper $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$. Außerdem gebe es noch eine weitere (beliebige) Körpererweiterung $\mathbb{K}^* \supset \mathbb{K}$. Dann können wir f auch als Polynom über \mathbb{K}^* auffassen, und der Zerfällungskörper über \mathbb{K}^* ist $\mathbb{L}^* = \mathbb{K}^*(\alpha_1, \dots, \alpha_n)$. In welchem Verhältnis stehen die beiden Galoisgruppen $G = \text{Gal}(\mathbb{L}, \mathbb{K})$ und $G^* = \text{Gal}(\mathbb{L}^*, \mathbb{K}^*)$? Jedes $\sigma \in G^*$ ist ein Automorphismus von \mathbb{L}^* , der \mathbb{K}^* fix lässt, also auch $\mathbb{K} \subset \mathbb{K}^*$, und die Nullstellen $\alpha_1, \dots, \alpha_n$ von f permutiert. Also lässt σ auch $\mathbb{L} = \mathbb{K}(\alpha_1, \dots, \alpha_n)$ invariant, und $\sigma|_{\mathbb{L}} \in \text{Gal}(\mathbb{L}, \mathbb{K})$. Wenn $\sigma|_{\mathbb{L}} = \text{id}$, dann ist $\sigma(\alpha_j) = \alpha_j$ für $j = 1, \dots, n$ und damit $\sigma = \text{id}$, da $\mathbb{L}^* = \mathbb{K}^*(\alpha_1, \dots, \alpha_n)$ und \mathbb{K}^* fix bleibt. Also ist der Einschränkungshomomorphismus

$$\phi : \sigma \mapsto \sigma|_{\mathbb{L}} : \text{Gal}(\mathbb{L}^*, \mathbb{K}^*) \rightarrow \text{Gal}(\mathbb{L}, \mathbb{K}) \quad (97)$$

¹⁵³Die Nullstellen eines irreduziblen Polynoms $f \in \mathbb{K}[x]$ sind getrennt: Gibt es nämlich eine doppelte Nullstelle, so ist dies eine gemeinsame Nullstelle von f und seiner Ableitung f' , womit diese beiden Polynome über \mathbb{K} nicht mehr teilerfremd sind - zunächst über $\mathbb{L} = \mathbb{L}_f$, aber dann auch über \mathbb{K} : Wären sie teilerfremd über \mathbb{K} , könnten wir nach dem euklidischen Algorithmus die Eins darstellen: $1 = af + bf'$ mit $a, b \in \mathbb{K}[x]$, aber diese Relation würde auch in \mathbb{L} gelten, also wären f und f' auch in \mathbb{L} teilerfremd, Widerspruch! Damit ist f nicht irreduzibel, falls es eine mehrfache Nullstelle gibt.

injektiv¹⁵⁴ (weil $\ker \phi = \{\text{id}\}$). Also lässt sich $\text{Gal}(\mathbb{L}^*, \mathbb{K}^*)$ als Untergruppe von $\text{Gal}(\mathbb{L}, \mathbb{K})$ auffassen. Wir haben damit bewiesen:

Satz 35.2. *Ist $\mathbb{K}^* \supset \mathbb{K}$ und sind \mathbb{L} und \mathbb{L}^* die Zerfällungskörper eines Polynoms $f \in \mathbb{K}[x]$ mit getrennten Nullstellen über \mathbb{K} und \mathbb{K}^* , so ist der Einschränkungshomomorphismus (97) injektiv und macht $\text{Gal}(\mathbb{L}^*, \mathbb{K}^*)$ zu einer Untergruppe von $\text{Gal}(\mathbb{L}, \mathbb{K})$.*

Deshalb können wir in Satz 34.1 ohne Einschränkung der Allgemeinheit annehmen, dass \mathbb{K} alle in der Konstruktion benötigten Einheitswurzeln enthält: Wenn nicht, gehen wir zu einem Erweiterungskörper $\mathbb{K}^* \supset \mathbb{K}$ über, der sie enthält; da die Galoisgruppe $\text{Gal}(\mathbb{L}, \mathbb{K})$ nach Voraussetzung auflösbar ist, ist es auch die Untergruppe $\text{Gal}(\mathbb{L}^*, \mathbb{K}^*)$.

36. NACHWORT

Gleichungen zu lösen ist eine traditionelle Aufgabe der Mathematik. In dieser Vorlesung ging es um die Lösung von Polynomgleichungen in einer Variablen, $f(x) = 0$. Im Laufe der Vorlesung wie auch der Geschichte der Mathematik hat sich die Fragestellung verschoben von “Wie finde ich eine Lösung?” zu “Wann kann man die Lösungen mit den gegebenen Hilfsmitteln finden, wann nicht?” Diese Frage wurde beantwortet von Évariste Galois, über den Joseph Rotman [6, Seite 65] schreibt: “Ich bin voll Bewunderung für das Genie von Galois (1811-1832). Er löste ein bedeutendes mathematisches Problem seiner Zeit, und seine Lösung ist wunderschön. Dabei schuf er zwei mächtige Theorien, Gruppentheorie und Galoistheorie, und sein Werk ist noch heute einflussreich. Und all das erreichte er im Alter von 19 Jahren; im Jahr darauf wurde er ums Leben gebracht.”¹⁵⁵

¹⁵⁴Das darf man nicht mit der Situation von Lemma 29.2, Seite 87 verwechseln, wo man gleichfalls einen Einschränkungshomomorphismus betrachtet, der aber keineswegs injektiv ist. Aber dort hat man einen Zwischenkörper \mathbb{K}' mit $\mathbb{K} \subset \mathbb{K}' \subset \mathbb{L}$ vorliegen und schränkt ein $\sigma \in \text{Gal}(\mathbb{L}, \mathbb{K})$ auf diesen Zwischenkörper \mathbb{K}' ein; dann hat der Einschränkungshomomorphismus einen Kern, nämlich $\text{Gal}(\mathbb{L}, \mathbb{K}')$. Jetzt dagegen ist \mathbb{L} kein Zwischenkörper der Körpererweiterung $\mathbb{L}^* \supset \mathbb{K}^*$, denn $\mathbb{K}^* \not\subset \mathbb{L}$, sondern $\mathbb{K} \subset \mathbb{K}^*$ und die Körpererweiterungen $\mathbb{L}^* \supset \mathbb{K}^*$ und $\mathbb{L} \supset \mathbb{K}$ entstehen parallel auf die gleiche Weise durch Adjunktion der Nullstellen von f .

¹⁵⁵Galois starb am 31. Mai 1832 an einer Schussverletzung aus einem Duell, dessen genaue Ursache nie geklärt werden konnte. Am 29. Mai, dem Vorabend des Duells, schrieb er an seinen Freund August Chevallier einen langen Brief, in dem er seine wichtigsten mathematischen Erkenntnisse noch einmal zusammenfasste. Seine wichtigste Arbeit, “Mémoire sur les conditions de résolubilité des équations par radicaux” (Februar 1830) war 1831 abgelehnt worden und wurde erst 1846 durch Joseph Liouville veröffentlicht. Siehe http://fr.wikipedia.org/wiki/Évariste_Galois

Meinen Hörerinnen und Hörern möchte ich für ihre Geduld und Aufmerksamkeit danken. Ein besonderes Bedürfnis ist es mir, Erich Dorner für das beständige Korrekturlesen des Manuskripts zu danken. Für Hinweise auf Ungereimtheiten und Fehler bin ich auch weiterhin dankbar.

LITERATUR

- [1] H.-W. Alten et al.: 4000 Jahre Algebra. Springer 2003
- [2] E. Artin: Galois Theory. Notre Dame 1955
- [3] H.M. Edwards: Galois Theory. Springer 1984
- [4] S. Lang: Algebra, Addison-Wesley 1978
- [5] M. Nieper-Wißkirchen: Galoissche Theorie (Preprint)
- [6] J. Rotman: Galois Theory, Springer 1990
- [7] L. van der Waerden: Algebra, Erster Teil. Springer 1966

INDEX

- Abel, 45, 56, 97
- Addition, 16
- Adjunktion, 64
- affin, 55
- Ähnlichkeit, 6
- Al-Chwarizmi, 1
- Algebra, 1, 2
- algebraisch abgeschlossen, 27
- Algorithmus, 1
- alternierend, 50, 53
- A_n , 50, 53, 89, 90
- antiton, 92
- Archimedes, 8, 72
- Argand, J.R., 24
- Artin, E., 92
- Assoziativgesetz, 44, 45
- auflösbar, 89, 95
- Ausmultiplizieren, 28
- ausmultiplizieren, 8
- Automorphismus, 82
- Axiom, 61

- Bahn, 36, 37, 48, 49, 73
- Basis, 65
- Betrag, 17
- bijektiv, 29, 47, 55
- Binom, 8
- Bombelli, R., 13

- Cardano, G., 13, 14
- Casus Irreducibilis, 13
- Charakteristik, 63

- disjunkt, 48
- Diskriminante, 33
- Distributivgesetz, 8, 61
- Dürer, A., 75

- Ebene, 15
- Einheitswurzel, 53
- Einheitswurzeln, 23
- Einschränkung, 87, 98
- Eisenstein, G., 80
- Eisenstein-Kriterium, 80
- elementar-symmetrisch, 29
- Eratosthenes, 78
- Erweiterungskörper, 64
- erzeugen, 74

- Erzeugendensystem, 65
- Eudoxos, 8
- euklidischer Algorithmus, 5, 25
- euklidischer Ring, 26
- Euler, L., 19, 74
- Exponentialfunktion, 18, 19

- (f) , 64
- Fakultät, 10
- Fehlstand, 50
- Fermat, 74
- Fermatzahl, 74
- Ferrari, L., 13
- fix, 86
- Fixkörper, 91
- Fundamentalsatz, 23
- Fünfeck, 6
- Funktion, 2

- Galois, 95, 99
- Galois, E., 3
- Galoiserweiterung, 82
- Galoisgruppe, 51, 82
- Gauß, C.F., 15, 23, 72, 74, 80
- Gemeinsames Maß, 5
- ggT, 5
- Girard, A., 30
- Gleichung, 1
 - kubische, 12, 36
 - quartische, 13, 39
 - quintische, 56
- Goldener Schnitt, 5, 6, 8, 75
- Grad, 2, 26, 65
- Graph, 20
- Größen, 3
- Gruppe, 44
 - abelsche, 45, 49, 61, 97
 - auflösbare, 88
 - einfach, 90
 - einfache, 89
 - zyklische, 74, 88, 89

- halbinvariant, 36, 37, 39, 49, 74
- Hauptsatz, 91
- Homomorphiesatz, 87
- Homomorphismus, 45

- Ideal, 52, 63, 64

- Ikosaeder, 56
- imaginär, 14, 20
- Imaginärteil, 16
- Induktion, 8, 9, 19
- injektiv, 55
- inkommensurabel, 7
- Interferenz, 14
- invariant, 29, 30, 46, 86
- Inverse, 44
- irrational, 8
- irreduzibel, 78, 98
- isomorph, 45, 84

- $\mathbb{K}(\alpha)$, 64
- Kern, 87
- kgV, 80
- Koeffizienten, 2, 29
- Koeffizientenkörper, 51
- Kommutativgesetz, 44, 45
- Komplexe Konjugation, 16, 82
- komplexe Konjugation, 20
- Komplexe Zahlen, 14–16
- kongruent, 62
- Konjugation, 47
- Konjugationsklasse, 89
- Körper, 16, 60, 61
- Körpererweiterung, 8, 14
 - algebraische, 65
 - endliche, 65
 - normale, 82, 86, 94
- Körperisomorphismus, 84
- Kreis, 20–22
- Kreisteilungspolynom, 73, 80
- Kronecker, L., 78
- Kubikzahl, 14

- Lagrange
 - Satz von, 49
- \mathbb{L}_f , 91
- Lindemann, F.v., 65
- linear unabhängig, 65
- Linearfaktor, 27
- Linearkombination, 2
- Linkstranslation, 47
- Lösung, 2

- Minimalpolynom, 66, 93
- Mitternachtsformel, 2, 11, 32, 36, 37
- modulo, 54

- Möglichkeit, 10
- Monom, 30
- Multiplikation, 22, 55

- n -Tupel, 29
- Natürliche Zahlen \mathbb{N} , 2
- Nebenklasse, 49
- Neutralelement, 45
- Newton, 30
- normal, 49
- Normalteiler, 49, 86
- normiertes Polynom, 28
- Nullstelle, 2

- Oktaeder, 56
- Operation, 47
- Ordnung
 - eines Gruppenelements, 96
- Ordnung von Nullstellen, 27

- Parität, 50
- Partition, 89
- Permutation, 29, 55
 - gerade, 53
- π , 65
- π , 22
- Polyeder, 46
- Polygon, 46
- Polynom, 2
 - irreduzibles, 51, 64, 73, 78, 80
 - primitives, 81
 - separables, 51
- Potenz, 14, 19, 96
- primitive Einheitswurzeln, 54
- Primitives Element, 93
- Produkt
 - direktes, 52
 - kartesisches, 45
- Projektion, 36

- Quadratwurzel, 13
- Quadrik, 58

- Radikal, 86, 89
- Rationale Zahlen, 8, 60
- Realteil, 16
- Rechtstranslation, 47
- reduzibel, 52, 97
- Reelle Zahlen, 8
- Relation

- algebraische, 28, 52
 - lineare, 65
- Renaissance, 12
- Resolvente, 36, 39, 96
- Restklasse, 62
- Ring, 25, 61

- Schach, 45
- Skalarprodukt, 69
- S_n , 46, 89
- Stabilisator, 48
- Standgruppe, 48
- Stetigkeit, 20
- Substitution, 11, 24
- Summensymbol, 10
- surjektiv, 48, 55
- Symmetriegruppe, 46
- Symmetrische Gruppe, 46, 89
- Symmetrische Polynome, 46

- teilbar, 25
- Teilkörper, 27, 64
- transitiv, 73, 91, 98
- Translation, 55, 62
- Transposition, 50
- Tschirnhaus, 11, 32, 58

- Unbekannte, 2
- Unbestimmte, 2
- unendlich, 20
- Untergruppe, 48
- Urbild, 48

- Variable, 2, 30
- Vektor, 29
- Verhältnis, 4
- Verkettung, 43
- Vierergruppe, 49
- Vieta, F., 28

- Winkel, 20
- Winkeldreiteilung, 72
- Wirkung, 47, 62
- Wurzel, 2

- Zahl, 3, 5, 8, 13–15, 20
 - algebraische, 27, 65
 - transzendente, 65
- Zahlenebene, 15
- Zerfällungskörper, 60, 82
- Zerfällungskörper, 91
- Zwischenwertsatz, 13
- Zykel, 89
- Zyklus, 36

INHALTSVERZEICHNIS

1. “Algebra”	1
2. Das gemeinsame Maß	3
3. Die binomische Formel	8
4. Die Tschirnhaus-Transformation	10
5. Die kubische Gleichung	11
6. Die imaginären Zahlen	13
7. Die komplexe Zahlenebene	15
8. Die Exponentialfunktion	18
9. Der “Fundamentalsatz der Algebra”	23
10. Alle Nullstellen	25
11. Der Wurzelsatz von Vieta	28
12. Symmetrische Polynome	30
13. Lagrangesche Resolventen	35
14. Die Lösung der quartischen Gleichung	39
15. Gruppen	43
16. Gruppenwirkungen	47
17. Die Alternierende Gruppe	50
18. Die Galoisgruppe	51
19. Die Lösung der quintischen Gleichung	56
20. Körper	60
21. Körpererweiterungen	63
22. Konstruktionen mit Zirkel und Lineal	67
23. Würfelverdopplung und Winkeldreiteilung	70
24. Konstruktion regelmäßiger Vielecke	72
25. Irreduzibilität über \mathbb{Z}	78
26. Irreduzibilität über \mathbb{Q}	80
27. Die Galoisgruppe einer Körpererweiterung	82
28. Fortsetzung von Körper-Isomorphismen	84
29. Auflösbarkeit durch Radikale	86
30. Nicht-Auflösbarkeit bei Grad $n \geq 5$	89
31. Der Hauptsatz der Galoistheorie	91
32. Der Satz vom primitiven Element	93
33. Normale Körpererweiterungen	94
34. Lösung bei auflösbarer Galoisgruppe	95
35. Zwei kurze Nachträge	97
36. Nachwort	99
Literatur	100
Index	101