Der Geometrische Quotient im mathematischen Netzwerk

Helmut Konz

2. Januar 2018

Inhaltsverzeichnis

1 Vorwort **5**

2 Das Polynom $a^n - b^n$ **6**

3 $G(n, a, 1)$, der Spezialfall $b = 1$ **8**
3.1 $G(n, 10, 1)$, Quersummenregel für die Basis 10 8
3.2 Quersummenregel für andere Stellenwertsysteme 9
3.3 Das Dualsystem 9

4 Die Koeffizienten eines Polynoms **11**
4.1 Die Koeffizientensumme 11
4.2 Die alternierende Koeffizientensumme 12
4.3 Ganzzahlige Lösungen algebraischer Gleichungen 13
4.4 Ein Ideal in $\mathbb{R}[x]$ 14

5 Der Linearfaktor **16**
5.1 Linearfaktor und Nullstelle 16
5.2 Die quadratische Gleichung in der Normalform 17
5.3 Die quadratische Gleichung und der Satz von Viëta 18
5.4 Paarweise komplexe Nullstellen 18

6 Probleme aus Wettbewerben **20**
6.1 Ein Problem aus dem Wettbewerb mathématiques sans frontières 2015 . 20
6.1.1 Komplexe Einheitswurzeln 20

6.1.2 Die Ecke $z_0 = 1$ . . . 21
6.1.3 Beispiele . . . 22
6.1.4 Hexagon . . . 22
6.1.5 Reguläres Neuneck . . . 23
6.2 Bundeswettbewerb Mathematik 2016 zweite Runde . . . 23
6.2.1 Dreieckszahlen . . . 23
6.2.2 Lösung . . . 24

7 Der Geometrische Quotient **26**
7.1 Darstellung des Geometrischen Quotienten als Polynom . . . 26
7.2 Der Grenzwert $lim_{b\to a}G(n,a,b)$ . . . 27
7.3 Die Verallgemeinerung des Exponenten . . . 27
7.3.1 $G(-n,a,b)$, negativer Exponent . . . 27
7.3.2 $G(\frac{1}{2},a,b)$, Exponent $\frac{1}{2}$ . . . 27
7.3.3 $G(\frac{1}{n},a,b)$, Exponent $\frac{1}{n}$ . . . 28
7.3.4 $G(\frac{n}{m},a,b)$, Exponent $\frac{n}{m}$ . . . 28
7.3.5 reeller Exponent . . . 29

8 Die Ableitung einer Funktion **30**
8.1 Ableitung von Polynomen . . . 30
8.2 Ableitung von Wurzelfunktionen . . . 31
8.3 Die Ableitung von e^x . . . 31
8.4 Die Ableitung von Sinus und Cosinus . . . 32
8.5 Die Produktregel . . . 33
8.6 Die Quotientenregel . . . 34
8.7 Die Kettenregel . . . 34
8.8 Ableitung bei Parameterdarstellung . . . 35
8.9 Punkte maximaler Krümmung . . . 36
8.9.1 Exponentialfunktion . . . 37
8.9.2 Kubische Funktion . . . 37

9 Das bestimmte Integral **39**

10 Symmetrische Polynome **40**
10.1 Der Quotient als symmetrisches Polynom . . . 40
10.2 Darstellung des Quotienten in elementarsymmetrischen Polynomen . . . 42
10.3 Quadratische Gleichung und symmetrische Polynome . . . 43
10.4 Nichtlineare Gleichungssysteme . . . 44
10.5 Ein Problem aus dem Bundeswettbewerb Mathematik 2006 . . . 46

11 Die kubische Gleichung **48**
11.1 Die Lösung der kubischen Gleichung 48
11.2 Der direkte Weg zur Lösung 48
11.3 Systematischer Weg nach Galois 49
11.3.1 Die dritten Einheitswurzeln 49
11.3.2 Die Verringerung der Symmetrie 50
11.3.3 Die kubische Diskriminante 51
11.4 Praktische Anwendung der Cardano'schen Formel 52

12 Die geometrische Reihe **54**
12.1 Das St. Ives Problem 54
12.2 Besonderheiten der geometrischen Reihe 55
12.2.1 Das Geometrische an der Geometrischen Reihe 55
12.2.2 Konvergenz der Geometrischen Folge 55
12.2.3 Konvergenz der Geometrischen Reihe 57
12.3 Finanzmathematik 57
12.3.1 Die Geldschöpfung 57
12.3.2 Bewertung vermietbarer Immobilien 59

13 Wurzeln im Nenner **61**
13.1 Algebraischer Hintergrund 61
13.1.1 Irrationalität von $\sqrt{2}$ 61
13.1.2 Erweiterungskörper 62
13.2 Umformung mit der geometrischen Reihe 62
13.3 Die beiden Strukturen des Erzeugnisses 63
13.4 Einfaches Beispiel 63
13.4.1 Beispiel aus dem Schulbuch 66
13.5 Kehrwert einer komplexen Zahl 67
13.6 Der Körper der komplexen Zahlen 68
13.7 Die Gauß'sche Zahlenebene 70
13.8 Endliche Körper 70
13.8.1 Restklassenkörper 70
13.8.2 Die Potenzmenge 72
13.8.3 Die symmetrische Gruppe S_3 74
13.8.4 Die Symmetriegruppe des gleichseitigen Dreiecks 74
13.8.5 Gebrochen lineare Funktionen als Gruppe 75
13.8.6 Die Verknüpfungstabelle von S_3 76
13.8.7 Die Tafel der Symmetriegruppe 76
13.8.8 Permutationsmatrizen 77
13.8.9 Die symmetrische Gruppe $\mathbf{S_3}$ als Faktorgruppe 80

14 Die Mittelwertsätze der Analysis **83**
14.1 Steigung und Stetigkeit 83
14.2 Der Mittelwertsatz der Differentialrechnung 84
14.2.1 Einige spezielle Potenzen 84
14.2.2 Eine Besonderheit des arithmetischen Mittelwertes 85
14.3 Der Mittelwertsatz der Integralrechnung 86

15 Primzahlen **89**
15.1 Nur primes n kann primes m erzeugen 89
15.2 Mersenne-Zahlen und vollkommene Zahlen 89
15.3 Test auf Primalität 90
15.4 Es gibt keine größte Primzahl 91
15.5 Der Beweis von Kummer 91

16 Der Goldene Schnitt **92**
16.1 Goldene Fraktale 92
16.2 Goldenes Glücksrad 96
16.3 Goldener Schnitt versus $1:1$ 96
16.3.1 Ein Spiel für zwei Spieler und ein Glücksrad 96
16.3.2 Wer anfängt, ist im Vorteil 96
16.3.3 Berechnung des Vorteils 97
16.3.4 Der Andere darf zweimal drehen 97
16.3.5 Was hat sich geändert? 98
16.3.6 B darf noch öfter hintereinander drehen 99
16.3.7 Der Sektor von A wird verkleinert 99
16.3.8 Die ideale Aufteilung 100
16.3.9 Kombination der beiden Möglichkeiten 101
16.3.10 Der allgemeine Fall 101
16.3.11 Goldener Schnitt die bessere Teilung? 102

17 Taylor **103**

1 Vorwort

Kaum ein Gegenstand aus dem Mathematikunterricht ist bekannter als die Quersummenregel zur Überprüfung der Teilbarkeit durch die Zahl drei. Manche erinnern sich auch daran, dass die Quersummenregel auch für die Teilbarkeit durch neun gilt.
Irgendwie ahnt man, dass das mit dem Dezimalsystem zusammenhängt. Wir werden jedoch gleich sehen, dass die Quersummenregel für die Zahl drei auch im Hexadezimalsystem gültig ist, nicht jedoch die für die Zahl neun.
Es soll der Versuch gemacht werden, zu zeigen, die Mathematik kein Gebäude ist, welches immer mehr in die Höhe wächst, woraus sich ergeben würde, dass jedes Stockwerk in diesem Gebäude die darunterliegenden voraussetzt. Vielmehr ist die Mathematik ein Netzwerk mit Knoten und Maschen. Mathematik treiben - man beachte die Dynamik in dieser Redeweise - ist etwas Vorwärtsdrängendes. Man braucht also gewissermaßen Fahrzeuge , mit denen man in diesem Netz herumfahren kann. Der Vergleich mit dem Internet drängt sich geradezu auf. Dort spricht man von einem Surfbrett. Mit diesem gleitet man durch das Netz. Diese Arbeit soll exemplarisch ein solches Gefährt für die Mathematik darstellen und zeigen, wie man sich mit ihm fortbewegen kann.
Das Beispiel ist der Quotient $\frac{a^n-b^n}{a-b}$. Dieser dient als Augangspunkt für diverse Exkursionen in Teilgebiete der Mathematik. Wegen der Häufigkeit seines Vorkommens hat er einen Namen verdient. Er soll im Folgenden Geometrischer Quotient genannt werden. Als Notation wird entsprechend gewählt

$$G(n, a, b)$$

wobei noch anzugeben ist, aus welchen Mengen die Elemente n, a, b zu nehmen sind.

2 Das Polynom $a^n - b^n$

Dieses Polynom ist eines der interessantesten in der Mathematik, da es unglaublich viele Eigenschaften hat, die in die verschiedensten Gebiete der Mathematik hineinreichen. Es stellt den Zähler des Geometrischen Quotienten dar.

$$a^n - b^n = (a - b)G(n, a, b)$$

Zunächst einmal überzeugen wir uns von einer Teilbarkeitseigenschaft. Wenn $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$ liegen, dann ist dieses Polynom für jedes n durch $a - b$ teilbar, wobei natürlich $a \neq b$ sein muss.
Für $n = 2$ ist diese Aussage identisch mit einer binomischen Formel:

$$a^2 - b^2 = (a - b)G(2, a, b) = (a - b)(a + b) \iff \frac{a^2 - b^2}{a - b} = a + b$$

Diese Äquivalenz besteht bei genauem Hinsehen nur für $a \neq b$. Der Fall $a = b$ erfordert eine gesonderte Betrachtung, die später noch folgen wird.
Diese Aussage lässt sich auch in der „modulo“-Schreibweise darstellen.

$$a^2 - b^2 \equiv 0 \; mod(a - b)$$

Wir überzeugen uns durch vollständige Induktion, dass der Exponent 2 durch jede andere natürliche Zahl ersetzt werden kann.

$$a^n - b^n \equiv 0 \; mod(a - b)$$

Für $n = 1$ ist nichts zu zeigen.
Sei die Aussage für $n = k$ erfüllt, so gilt für $n = k + 1$ durch additives Einfügen einer Null in der Form

$$0 = -a^k b + a^k b$$

$$a^{k+1} - b^{k+1} = a^{k+1} - a^k b + a^k b - b^{k+1}$$

Daraus ergibt sich

$$a^{k+1} - b^{k+1} = a^k(a - b) + b(a^k - b^k)$$

Damit ist offenbar auch

$$a^{k+1} - b^{k+1} \equiv 0 \; mod(a - b)$$

womit alles gezeigt ist.
Das additive Einfügen einer Null ist eine recht anspruchsvolle Methode zur Termumformung. Sie wird oft in der Formulierung: „Wir addieren ... und ziehen es gleich wieder

ab.“Da stellt sich fast jeder intuitiv die Frage, warum er es denn erst addiert, wenn er es gleich wider abzieht. Dann hätte er es doch gleich lassen können. Die Folge ist Unverständnis. Der Hauptgedanke dieser Methode wird dadurch verschüttet. Die Null wird eingefügt als Summe von Zahl und Gegenzahl. Anschließend werden Zahl und Gegenzahl nach dem Assoziativgesetz unterschiedlichen Teilsummen zugeordnet. Diese Teilsummen lassen dann Umformungen zu, die vorher nicht möglich waren. Das macht die Methode erfolgreich.

Wir betrachten hierzu noch ein Beispiel aus dem Oxford Zugangstest von 2015.

Prüfe, ob die Zahl

$$3^{2015} - 2^{2015}$$

eine Primzahl ist!

Die Antwort ist nein, denn

$$3^{2015} - 2^{2015} = \frac{3^{5\cdot 403} - 2^{5\cdot 403}}{3^5 - 2^5}(3^5 - 2^5) = \frac{a^{403} - b^{403}}{a - b}(3^5 - 2^5)$$

mit $a = 3^5$ und $b = 2^5$.

Damit haben wir eine Zerlegung in zwei Faktoren, die beide ganzzahlig und von 1 verschieden sind.

Dieser Gedanke lässt sich verallgemeinern.
Wenn der Exponent n keine Primzahl ist, dann ist auch $a^n - b^n$ keine.
Denn wenn $n = rs$ eine Produktdarstellung von n ist,bei der weder r noch s gleich 1 ist, dann gilt

$$a^n - b^n = \frac{a^{rs} - b^{rs}}{a^r - b^r} \cdot \frac{a^r - b^r}{a - b}$$

Substituieren wir noch $c = a^r$ und $d = b^r$, dann haben wir

$$a^n - b^n = \frac{c^s - d^s}{c - d} \cdot \frac{a^r - b^r}{a - b}$$

und damit eine Produktdarstellung von $a^n - b^n$.

3 $G(n, a, 1)$, der Spezialfall $b = 1$

In diesem Fall lautet die Aussage

$$a^n - 1 \equiv 0 \; mod \; (a - 1)$$

Daraus folgt sofort

$$a^n \equiv 1 \; mod \; (a - 1)$$

Diese Tatsache hat weitreichende Folgen.

3.1 $G(n, 10, 1)$, Quersummenregel für die Basis 10

Setzen wir $a = 10$, so folgt

$$10^n \equiv 1 \; mod \; 9$$

Eine dezimal dargestellte Zahl hat die Form

$$\sum_{i=0}^{i=n} c_i 10^i$$

Betrachten wir nur den Neunerrest, so erhalten wir

$$\sum_{i=0}^{i=n} c_i 10^i \equiv \sum_{i=0}^{i=n} c_i \; mod \; 9$$

da ja jede Zehnerpotenz wie gesehen den Neunerrest 1 hat. Die Summe auf der rechten Seite heißt Quersumme. Damit haben wir bereits die Quersummenregel für die Zahl 9. Die Regel für die Zahl 3 folgt daraus, dass 3 ein Teiler von 9 ist. Das sieht man so:

$$10^n \equiv 1 \; mod \; 9$$

bedeutet

$$10^n = q \cdot 9 + 1$$

Daraus folgt

$$10^n = (q \cdot 3) \cdot 3 + 1$$

Das bedeutet, dass alle Zehnerpotenzen auch beim Teilen durch drei den Rest eins haben.

3.2 Quersummenregel für andere Stellenwertsysteme

Wenn wir das Dezimalsystem verlassen und eine andere Basis unseres Stellenwertsystems einführen, so bringen wir die Quersummenregel offenbar mit in das neue System. Wenn die Basis b ist, gilt die Regel für $b-1$ und alle Teiler von $b-1$.
Das heißt z.B. für das in der Informatik viel verwendete Hexadezimalsystem, dass die Quersummenregel für den Teiler 15 funktioniert und auch für die 3, weil diese ein Teiler von 15 ist.

3.3 Das Dualsystem

Im Dualsystem gilt $b = 2$. Damit hätten wir die Quersummenregel für den Modul 1, der trivialerweise jede Zahl teilt. Trotzdem hat die Quersumme auch hier eine Bedeutung. Sie gibt nämlich die Anzahl der Einsen an, die in der Codierungstheorie bei der Fehlererkennung eine große Rolle spielt. Man nennt diese Anzahl das Gewicht. Das Gewicht von 10011 ist demnach 3.
Hamming hat als erster erkannt, dass man damit die Voraussetzungen für automatische Fehlerkorrrektur schaffen kann. Er hat vorgeschlagen, als Nachrichten, die digital übermittelt werden, Bitfolgen fester Länge n zu nehmen. Längere Nachrichten werden dann in sogenannte Pakete der Länge n zerlegt. So wird es heute im Internet auch gemacht.

Die Bitfolge kann als Vektor aufgefasst werden, der nur 0 und 1 als Komponenten haben kann, also ein Binärvektor. Dann bilden alle diese Binärvektoren einen Vektorraum der Dimension n über dem Körper $\mathbb{F}_2$

$$\mathbb{F}_2^n$$

Dieser Vektorraum kann mit dem Konzept des Gewichts (Hamming weight) metrisiert werden. Dazu definiert man als Abstand $d(b_1, b_2)$ zweier Vektoren b_1 und b_2 das Gewicht g der Summe.

$$d(b_1, b_2) = g(b_1 + b_2)$$

Das Interessante an dieser Definition ist, dass bei der Addition entsprechender Komponenten bei der Summe die Komponente den Wert 0 hat, wenn sie gleich sind, und den Wert 1, wenn sie verschieden sind. Dann gibt das Gewicht der Summe die Anzahl der Komponenten an, die verschieden sind.
Diese Definition erfüllt alle drei Bedingungen, die wir an eine Metrik stellen.
Der Abstand eines Vektors von sich selbst ist 0.
Diese Bedingung ergibt sich daraus, dass bei Gleichheit aller Komponenten eines Binärvektors die Summe mit sich selbst der Nullvektor ist. Dessen Gewicht ist 0. Die zweite Bedingung ist, dass der Vektor b_1 von b_2 denselben Abstand hat wie b_2 von b_1.

$$d(b_1, b_2) = d(b_2, b_1)$$

Diese Bedingung ist erfüllt, da der Grundkörper kommutativ ist.
Die dritte Bedingung ist die sogenannte Dreiecksungleichung. Diese besagt, dass der direkte Abstand zwischen zwei Vektoren stets kleiner und höchstens gleich der Summe der Abstände zu einem dritten Vektor ist. (Der direkte Weg muss kürzer als jeder Umweg sein.)

$$d(b_1, b_2) \leq d(b_1, b_3) + d(b_3, b_2)$$

Dass diese Bedingung ebenfalls erfüllt ist, sieht man so:
Wenn sich die beiden entsprechenden Komponenten von b_1 und b_2 unterscheiden, dann ist eine 0 und die andere 1. Die Summe wäre also 1 und damit wäre sie im Gewicht enthalten. Werden die Summen über einen dritten Vektor ermittelt, so hat dieser an der entsprechenden Stelle (Komponente) einen der Werte 0 oder 1. Daher ist eine dieser zwei Teilsummen 0 und die andere 1, und damit ist die Summe 1. Damit verbleibt diese Stelle im Gewicht.

Stimmen die beiden Komponenten jedoch überein, so sind sie nicht im Gewicht vorhanden. Hat der dritte Vektor dieselbe Komponente, so bleibt alles beim Alten und die Stelle ist weiterhin nicht im Gewicht vorhanden. Hat er eine andere, dann unterscheidet er sich von beiden und jedes Teilgewicht erhöht sich um 1 und damit das Gesamtgewicht um 2.

Mit dieser Metrik schafft man jetzt Umgebungen einzelner Bitfolgen, das heißt, es wird nicht mehr jede Bitfolge als gültige Nachricht zugelassen, sondern nur noch eine Teilmenge.

Diese Teilmenge wird so konstruiert, dass jede zulässige Nachricht eine Umgebung hat und alle Umgebungen disjunkt sind. Dann genügt es, dass die empfangene und möglicherweise beschädigte Nachricht in einer der Umgebungen liegt, um sicher dekodiert zu werden.
Auf diese Weise stecken zum Beispiel CD-Player Kratzer weg.

4 Die Koeffizienten eines Polynoms

Es folgen hier einige Eigenschaften von Polynomen. Diese bilden einen Ring, weil bekanntlich nicht jede Polynomdivision aufgeht. Je nach Anzahl der Variablen und der Menge, aus der die Koeffizienten stammen, erhalten wir unterschiedliche Polynomringe.

Die Menge der Koeffizienten muss mindestens selbst ein Ring sein. So bilden die Polynome über den ganzen Zahlen einen Ring, aber nicht über den natürlichen.

Ein wenig von den sehr interessanten Erscheinungen im Bereich etwa der Polynomringe über endlichen Ringen und Körpern haben wir schon bei der Quersummenregel in Stellenwertsystemen kennen gelernt. Im Folgenden beschränken wir uns aber auf den Ring der Polynome über dem Körper der reellen Zahlen.

Zur Bezeichnung dieser Ringe ist es international üblich, den Grundring(Körper) anzugeben gefolgt von den Variablen in eckigen Klammern. So gehört das Polynom $a^n - b^n$ mit reellen Koeffizienten zu

$$\mathbb{R}[a, b]$$

Beschränken wir uns auf ganze Zahlen, so schreiben wir

$$\mathbb{Z}[a, b]$$

und schließlich für die Polynome in einer Veränderlichen x und mit Koeffizienten aus $\mathbb{R}$

$$\mathbb{R}[x]$$

4.1 Die Koeffizientensumme

Setzen wir in dem Polynom $a^n - b^n$ wie eben $b = 1$ und außerdem $a = x$, so erhalten wir ein Polynom aus $\mathbb{R}[x]$, womit sich die Beziehung

$$x^n \equiv 1 \bmod (x - 1)$$

ergibt.
Ein Polynom aus $\mathbb{R}[x]$ kann dargestellt werden in der Form

$$\sum_{i=0}^{i=n} c_i x^i$$

Das bedeutet für die Division durch $x-1$

$$\sum_{i=0}^{i=n} c_i x^i \equiv \sum_{i=0}^{i=n} c_i \mod (x-1)$$

Hier heißt die Summe auf der rechten Seite die Koeffizientensumme. Die Analogie zur Quersumme ist offensichtlich.

Aus dieser Überlegung können wir folgern, dass bei verschwindender Koeffizientensumme Teilbarkeit durch $x-1$ vorliegt. Demnach enthält das Polynom in der Produktform den Faktor $x-1$. Das wiederum bedeutet, dass die zugehörige algebraische Gleichung

$$\sum_{i=0}^{i=n} c_i x^i = 0$$

die 1 als Lösung hat.

Nach dem Fundamentalsatz der Algebra können dann natürlich noch bis zu $n-1$ weitere Lösungen hinzukommen.

Ganz besonders einfach liegt der Fall bei den quadratischen Gleichungen in der Normalform. Falls die Koeffizientensumme verschwindet, ist eine Lösung wie gesehen die 1.

Da nach dem Wurzelsatz von Viëta das Produkt der Lösungen gleich dem absoluten Glied ist, stellt dieses selbst die zweite Lösung dar.

Beispiel: die Gleichung

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

hat die Lösungen 1 und -3.

4.2 Die alternierende Koeffizientensumme

Mit geringem Mehraufwand kann die -1 als Lösung einer algebraischen Gleichung gefunden werden. Dazu berechnet man die alternierende Koeffizientensumme, d.h. die Koeffizienten werden abwechselnd addiert und subtrahiert. Verschwindet diese Summe, so ist -1 eine Lösung.

In der Praxis ist das Verfahren jedoch etwas unpraktisch, da fehlende Koeffizienten nicht einfach ignoriert werden können, da bei jedem Summanden ein Vorzeichenwechsel eintritt. Das Polynom

$$x^3 + 2x + 3$$

liefert als altenierende Koeffizientensumme nicht 2, was man beim unaufmerksamen Drauflosrechnen erhält, sondern 0 wegen

$$1 - 0 + 2 - 3 = 0$$

Sicherer ist das Auffinden der Lösung -1 mit dem Horner-Schema.

4.3 Ganzzahlige Lösungen algebraischer Gleichungen

Der Wurzelsatz von Viëta besagt, dass jede Lösung ξ das absolute Glied teilt. Somit liegen alle ganzzahligen Lösungen in der Teilermenge des absoluten Gliedes.

Nach unseren bisherigen Überlegungen können wir aber noch mehr sagen.

Gegeben sei eine algebraische Gleichung

$$c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n = 0$$

Falls ξ eine Lösung ist, gilt

$$c_0 + c_1 \xi + c_2 \xi^2 + \cdots + c_n \xi^n = 0$$

Bezeichnen wir mit C die Koeffizientensumme, so gilt

$$c_0 + c_1 + c_2 + \cdots + c_n = C$$

Nun bilden wir die Differenz aus den beiden letzten Gleichungen und erhalten

$$c_1(\xi - 1) + c_2(\xi^2 - 1) + \cdots + c_n(\xi^n - 1) = -C$$

Jeder Summand auf der linken Seite enthält den Faktor $\xi - 1$ und damit gilt

$$C \equiv 0 \bmod (\xi - 1)$$

Somit hilft die Teilermenge der Koeffizientensumme bei der Suche weiter.

Beispiel:

$$x^3 - 10x^2 + 31x - 30 = 0$$

Die Koeffizientensumme C ist -8. Die Teilermenge ist

$$\{\pm 1; \pm 2; \pm 4; \pm 8\}$$

Wenn wir zu allen Teilern 1 addieren, erhalten wir als mögliche Lösungen

$$\{0; 2; -1; 3; -3; 5; -7; 9\}$$

Die Teilermenge von -30 ist

$$\{\pm 1; \pm 2; \pm 3; \pm 5; \pm 10; \pm 15; \pm 30\}$$

Im Durchschnitt finden sich

$$\{-1; 2; -3; 3; 5\}$$

Damit ist die Suche merklich eingegrenzt. Nun rechnet man nach, z.B. mit dem Horner-Schema, ob die Gleichung erfüllt ist, und findet als Lösungsmenge

$$\{2; 3; 5\}$$

4.4 Ein Ideal in $\mathbb{R}[x]$

Betrachtet man die Menge aller Polynome mit verschwindender Koeffizientensumme in $\mathbb{R}[x]$, so bilden diese offenbar einen Unterring. Es liegt aber nicht nur Abgeschlossenheit bei der Multiplikation vor.

Das Produkt zweier Polynome mit verschwindender Koeffizientensumme ist auch ein Polynom dieses Typs, jedoch genügt es, wenn ein Faktor im Produkt die verschwindende Koeffizientensumme hat.

Diese Zusatzeigenschaft, die manchmal magnetische Eigenschaft genannt wird, macht den Unterring zum sogenannten Ideal. Die bekanntesten Beispiele für Ideale sind die „Reihen“ bei den ganzen Zahlen.

$$\cdots -9, -6, -3, 0, 3, 6, 9, \cdots$$

Dieses Ideal prägt der Menge $\mathbb{R}[x]$ eine Struktur auf. Betrachtet man zwei Polynome als äquivalent, wenn sie in der Koeffizientensumme übereinstimmen, so sind alle Merkmale einer Äquivalenzrelation erfüllt und damit eine disjunkte Klasseneinteilung erzeugt.

Die Differenz zweier äquivalenter Polynome liegt im Ideal. Die so erzeugte Klasseneinteilung ist selbst wieder eine Ringstruktur, man nennt sie den Faktorring.

Da alle Eigenschaften von $\mathbb{Z}$ vorhanden sind ist die Abbildung, die jedem Polynom seine Koeffizientensumme zuweist, ein Isomorphismus.

Dass das alles nicht selbstverständlich ist, erkennt man daran, dass es mit der alternierenden Koeffizientensumme schon nicht mehr geht.

Betrachtet man zwei Polynome als äquivalent, wenn sie dieselbe alternierende Koeffizientensumme haben, so liefert das zwar eine Klasseneinteilung, aber die Menge dieser so entstehenden Klassen selbst hat noch nicht einmal eine Gruppenstruktur.

5 Der Linearfaktor

5.1 Linearfaktor und Nullstelle

Betrachten wir ein Polynom $f(x)$ aus $\mathbb{R}[x]$ und zusätzlich den Funktionswert von f an einer beliebigen Stelle ξ. Es sei dargestellt in der Form

$$f(x) = a_0 + a_1x + a_2x^2 + a_3x^3 \cdots a_nx^n = \sum_{i=0}^{n} a_ix^i$$

Dann gilt für die Stelle ξ

$$f(\xi) = a_0 + a_1\xi + a_2\xi^2 + a_3\xi^3 \cdots a_n\xi^n = \sum_{i=0}^{n} a_i\xi^i$$

Bilden wir die Differenz, so fällt a_0 weg und wir erhalten

$$f(x) - f(\xi) = a_1(x-\xi) + a_2(x^2-\xi^2) + a_3(x^3-\xi^3) \cdots a_n(x^n-\xi^n) = \sum_{i=1}^{n} a_i(x^i-\xi^i)$$

Jeder Summand enthält offenbar den Faktor $(x-\xi)$. Dieser lässt sich nach dem Distributivgesetz abspalten und es ergibt sich

$$f(x) - f(\xi) = (x-\xi)g(x)$$

wobei $g(x)$ ein Polynom ist. Dieses Polynom ist sogar eindeutig, denn gäbe es etwa ein Polynom $h(x)$, welches ebenfalls diese Bedingung erfüllt, so kommen wir durch Bildung der Differenz auf

$$0 = (x-\xi)(g(x) - h(x))$$

Das könnte nur erfüllt werden, wenn einer der Faktoren auf der rechten Seite identisch verschwinden würde, was offensichtlich nicht der Fall ist.

Falls ξ eine Nullstelle ist, gilt $f(\xi) = 0$ und damit

$$f(x) = (x-\xi)g(x)$$

Die Stelle ξ ist also genau dann Nullstelle, wenn $f(x)$ den Linearfaktor $(x-\xi)$ hat.

5.2 Die quadratische Gleichung in der Normalform

Das Auffinden der Lösung einer quadratischen Gleichung, die in der Normalform

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

vorliegt, ist offenbar dasselbe Problem wie das Auffinden der Nullstellen von

$$f(x) = x^2 + px + q$$

Nach den Ergebnissen des vorigen Abschnitts liegt hier ein Spezialfall vor, nämlich für $n = 2$. Daher gilt

$$f(x) - f(\xi) = x^2 - \xi^2 + p(x - \xi)$$

Durch Abspalten des Linearfaktors erhalten wir daraus

$$f(x) - f(\xi) = (x - \xi)(x + \xi + p)$$

Da ξ beliebig gewählt werden kann, nehmen wir einen Wert, der zur Übereinstimmung der beiden Faktoren auf der rechten Seite führt.

$$x - \xi = x + \xi + p \implies \xi = -\frac{p}{2}$$

Diesen Wert erhalten wir für $-f(\xi)$

$$-f(-\frac{p}{2}) = \frac{p^2}{4} - q$$

Die rechte Seite nennt man bekanntlich Diskriminante.

Addition von $-f(-\frac{p}{2})$ auf beiden Seiten liefert:

$$f(x) = \left(x + \frac{p}{2}\right)^2 - \left(\frac{p^2}{4} - q\right)$$

Falls die Diskriminante nichtnegativ ist, existiert die Wurzel und wir erhalten

$$f(x) = \left(x + \frac{p}{2} + \sqrt{\frac{p^2}{4} - q}\right)\left(x + \frac{p}{2} - \sqrt{\frac{p^2}{4} - q}\right)$$

Da jeder Linearfaktor eine Nullstelle und damit eine Lösung der Gleichung liefert, lässt sich die Lösungsmenge der Gleichung so darstellen:

$$\mathbb{L} = \left\{-\frac{p}{2} + \sqrt{\frac{p^2}{4} - q} \quad ; \quad -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q}\right\}$$

5.3 Die quadratische Gleichung und der Satz von Viëta

Einen alternativen Zugang zur Lösungsformel für quadratische Gleichungen liefert der Satz von Viëta und die damit zusammenhängenden symmetrischen Polynome.

Für die quadratische Gleichung

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

gilt:

$$\begin{aligned} -p &= x_1 + x_2 \\ q &= x_1 x_2 \end{aligned}$$

Auf der rechten Seite stehen jeweils Polynome in x_1 und x_2, die wegen der Kommutativgesetze der Addition bzw der Multiplikation bei Vertauschung der Variablen ihren Wert beibehalte. Sie heißen symmetrische Polynome, die beiden hier speziell elementarsymmetrische Polynome. Es gilt der Hauptsatz für symmetrische Polynome. Dieser besagt, dass jedes symmetrische Polynom durch die elementarsymmetrischen ausgedrückt werden kann.

Das gilt dann auch für

$$D = (x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = p^2 - 4q$$

D heißt Diskriminante der quadratischen Gleichung. Wenn wir die Wurzel aus der Diskriminante ziehen können, folgt aus den Identitäten

$$\begin{aligned} x_1 &= \tfrac{1}{2}((x_1 + x_2) + (x_1 - x_2)) &= \tfrac{1}{2}(-p + \sqrt{p^2 - 4q}) \\ x_2 &= \tfrac{1}{2}((x_1 + x_2) - (x_1 - x_2)) &= \tfrac{1}{2}(-p - \sqrt{p^2 - 4q}) \end{aligned}$$

die bekannte Lösungsformel. Der Vorteil dieser Methode, die schon die Grundgedanken zur Galoistheorie enthält, besteht in der Möglichkeit zur Verallgemeinerung auf höhere Grade.

5.4 Paarweise komplexe Nullstellen

Der Fundamentalsatz der Algebra garantiert uns, dass jedes Polynom in $\mathbb{R}$ eine Produktdarstellung hat. Die Zerlegung ist möglich bis auf Faktoren vom Grade höchstens

2. Kann ein Faktor vom Grade 2 nicht in Linearfaktoren zerlegt werden, dann nennt man ihn irreduzibel. Betrachtet man das Polynom dagegen in $\mathbb{C}$, dann lassen sich auch die irreduziblen Faktoren in Linearfaktoren zerlegen. Da jedem Linearfaktor eine Nullstelle (nicht notwendig verschieden) entspricht, liefern die irreduziblen Faktoren zwei zusätzliche Nullstellen. Aus den Überlegungen dieses Abschnittes ergibt sich, dass diese beiden zusätzlichen Nullstellen zueinander konjugiert komplex sind.

Dazu betrachten wir wieder die quadratische Funktion

$$f(x) = x^2 + px + q$$

Für eine komplexe Nullstelle gilt

$$z = a + bi \quad \text{mit} \quad a, b \in \mathbb{R}$$

Dann ist die konjugiert komplexe Zahl dazu

$$\overline{z} = a - bi$$

Die zweite zusätzliche Nullstelle bezeichnen wir mit

$$w = c + di$$

Dann gilt nach dem Satz von Viëta

$$z + w = a + bi + c + di = -p$$

Durch Koeffizientenvergleich ergibt sich

$$d = -b$$

Für das Produkt gilt

$$zw = ac - bd + (ad + bc)i = q \quad \Rightarrow \quad ad + bc = 0 \quad \Rightarrow \quad a = c$$

.

Somit ist

$$w = \overline{z}$$

6 Probleme aus Wettbewerben

6.1 Ein Problem aus dem Wettbewerb mathématiques sans frontières 2015

Der Satz

Sei ein reguläres n-Eck im Einheitskreis gegeben. Dann hat das Produkt der Abstände einer Ecke von allen anderen Ecken den Wert n.

6.1.1 Komplexe Einheitswurzeln

In der Gauß'schen Zahlenebene stellen die Wurzeln des Polynoms

$$p_n(z) = z^n - 1$$

die Ecken eines regulären n-Ecks im Einheitskreis dar.

Eine der Wurzeln ist stets

$$z_n = 1$$

Die reelle Achse ist Symmetrieachse, so dass es zu jeder Ecke z_i auch die konjugiert komplexe $\overline{z}_i = z_{n-i}$ gibt.

Der Abstand einer der anderen Wurzeln von $z_n = 1$ aus beträgt $|1 - z_i|$.

Dieser Betrag hat die Darstellung

$$|1 - z_i|^2 = (1 - z_i)(1 - \overline{z}_i)$$

Spalten wir den zu der Lösung $z_n = 1$ gehörenden Linearfaktor durch Polynomdivision ab, so erhalten wir

$$p_{n-1}(z) = (z^n - 1) : (z - 1) = \sum_{0}^{n-1} z^i$$

Den restlichen $n-1$ Wurzeln $\{z_i \quad i = 1 \ldots n-1\}$ entsprechen Linearfaktoren, die die Produktdarstellung von p_{n-1} ermöglichen (Fundamentalsatz der Algebra).

$$p_{n-1}(z) = \prod_{1}^{n-1}(z - z_i)$$

Damit gilt die Gleichung

$$\sum_{0}^{n-1} z^i = \prod_{1}^{n-1} (z - z_i)$$

6.1.2 Die Ecke $z_0 = 1$

Setzen wir nun $z = 1$.

Dann erhalten wir auf der linken Seite die Koeffizientensumme n.

Die rechte Seite ist das Produkt der Abstände von $z_0 = 1$.

Das sieht man so:

Da $\mathbb{C}$ ein Körper ist, gilt das Kommutativgesetz der Multiplikation. Wir können also die Faktoren beliebig vertauschen, ohne das Produkt zu verändern. Insbesondere gilt dann für die umgekehrte Reihenfolge

$$\prod_{1}^{n-1} (1 - z_{n-i}) = \prod_{1}^{n-1} (z - z_i)$$

und daher

$$\left(\prod_{1}^{n-1} (1 - z_i) \right)^2 = \prod_{1}^{n-1} (1 - z_i) \cdot \prod_{1}^{n-1} (1 - z_{n-i})$$

Die reelle Achse ist Symmetrieachse des $n-$Ecks. Daher entsprechen gegenüberliegenden Ecken konjugiert komplexe Zahlenwerte.

$$z_{n-i} = \overline{z}_i$$

Dann haben wir

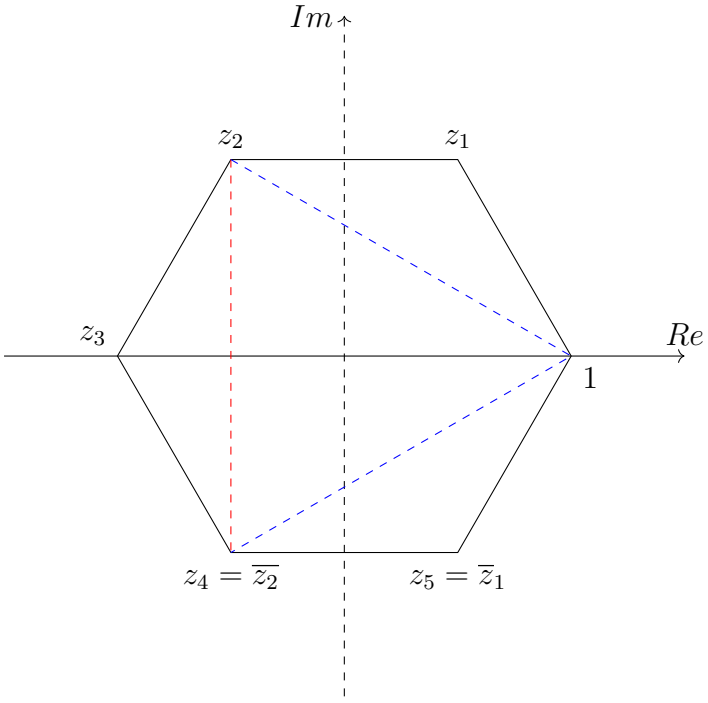
$$\left(\prod_{1}^{n-1} (1 - z_i) \right)^2 = \prod_{1}^{n-1} (1 - z_i) \cdot \prod_{1}^{n-1} (1 - \overline{z_i}) = \prod_{1}^{n-1} (1 - z_i)(\overline{1 - z_i}) = \prod_{1}^{n-1} |1 - z_i|^2$$

Das bedeutet

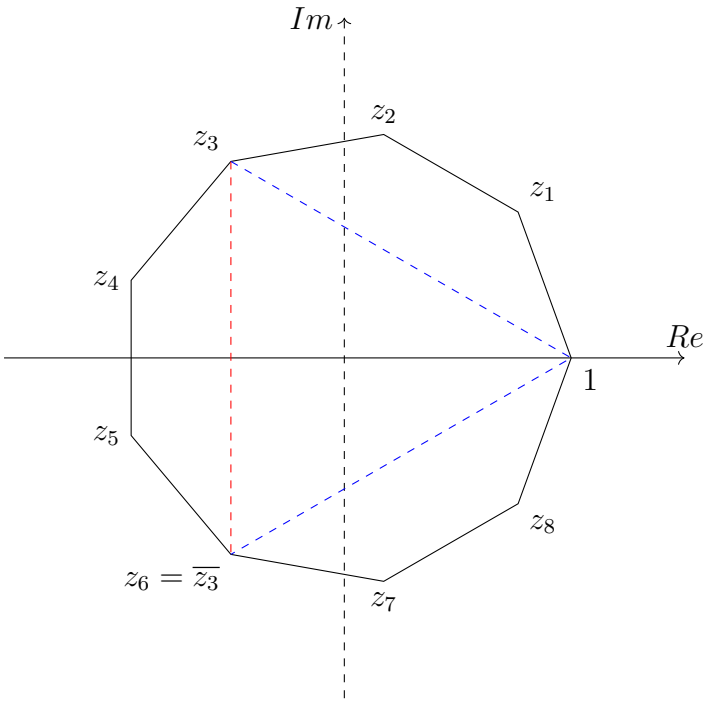
$$\sum_{0}^{n-1} 1 = n = \prod_{1}^{n-1} |1 - z_i|$$

6.1.3 Beispiele

6.1.4 Hexagon



6.1.5 Reguläres Neuneck



6.2 Bundeswettbewerb Mathematik 2016 zweite Runde

6.2.1 Dreieckszahlen

Beweise, dass es unendlich viele positive ganze Zahlen gibt, die sich nicht als Summe aus einer Dreieckszahl und einer Primzahl darstellen lassen!
Dreieckszahlen sind Zahlen der Form

$$\frac{n}{2}(n+1)$$

6.2.2 Lösung

Es wird gezeigt, dass eine Teilmenge der Dreieckszahlen die Kriterien erfüllt.

Eine unendliche Menge solcher Zahlen sind die Dreieckszahlen der Form

$$\{r_\lambda = \frac{k}{2}(k+1) \quad \text{mit} \quad k = 2\lambda^2, \quad \lambda = 2, 3, 4, \ldots\}$$

Zu zeigen ist, dass keine der Differenzen mit kleineren Dreieckszahlen eine Primzahl sein kann. Dazu bezeichnen wir die Differenzen mit

$$_kd_j = \frac{k}{2}(k+1) - \frac{j}{2}(j+1)$$

$$_kd_j = \frac{1}{2}(k^2 - j^2 + k - j) = \frac{1}{2}(k-j)(k+j+1) \quad j = 1, 2, \ldots, k-2, k-1$$

Der letzte Faktor $k + j + 1$ ist offenbar stets ≥ 3.

Wenn der Faktor $k-j$ die Werte 1 oder 2 annimmt, darf der zweite Faktor keine Primzahl sein.

Für $k - j = 1$ gilt

$$j = k - 1 \rightarrow k + k - 1 + 1 = 2k$$

$$_kd_{k-1} = \frac{1}{2}(k-j)(k+j+1) = k$$

Für $k - j = 2$ gilt

$$j = k - 2 \rightarrow k + k - 2 + 1 = 2k - 1$$

$$_kd_{k-2} = \frac{1}{2}(k-j)(k+j+1) = 2k - 1$$

Für $k = 2\lambda^2$ können in beiden Fällen keine Primzahlen auftreten.

$$_kd_{k-1} = 2\lambda^2$$

und

$$_k d_{k-2} = 2 \cdot 2\lambda^2 - 1 = (2\lambda - 1)(2\lambda + 1)$$

Es ergibt sich die unendliche Folge für

$$k = 8, 18, 32, 50, 98, 128, \ldots$$

und damit sind die Zahlen

$$36, 171, 528, 1275, 4851, \ldots, \lambda^2(2\lambda^2 + 1) \quad \text{mit} \quad \lambda = 2, 3, 4, \ldots$$

eine unendliche Folge mit der gewünschten Eigenschaft.

7 Der Geometrische Quotient

Bisher haben wir uns nur mit dem Rest dieser Division beschäftigt. Aber auch der Quotient hat einige bemerkenswerte Eigenschaften.

7.1 Darstellung des Geometrischen Quotienten als Polynom

Wie wir bereits wissen, ist der Geometrische Quotient $G(n,a,b) = \frac{a^n - b^n}{a-b}$ auch wieder ein Polynom. Es hat die Darstellung

$$G(n,a,b) = \sum_{i=0}^{i=n-1} a^{n-1-i}b^i$$

Zum Beweis schreiben wir

$$a^n - b^n = (a-b)\sum_{i=0}^{n-1} a^{n-1-i}b^i$$

und beweisen diese Formel durch vollständige Induktion.
Für $n = 1$ ist nichts zu zeigen. Gilt sie für $n = k$, so ist

$$\begin{aligned}
a^{k+1} - b^{k+1} &= a^{k+1} - ab^k + ab^k - b^{k+1} \\
&= a(a^k - b^k) + (a-b)b^k \\
&= a(a-b)\sum_{i=0}^{k-1} a^{k-1-i}b^i + (a-b)b^k \\
&= (a-b)(a\sum_{i=0}^{k-1} a^{k-1-i}b^i + b^k) \\
&= (a-b)(\sum_{i=0}^{k-1} a^{k-i}b^i + a^0b^k) \\
&= (a-b)(\sum_{i=0}^{k} a^{k-i}b^i)
\end{aligned}$$

Damit ist alles gezeigt.

7.2 Der Grenzwert $lim_{b\to a}G(n,a,b)$

Offenbar liegen keinerlei Singularitäten vor und wir können ohne Weiteres $b = a$ setzen. Dadurch reduziert sich unser Polynom von zwei Variablen auf ein Polynom in einer Variablen.

$$\sum_{i=0}^{i=n-1} a^{n-1} = na^{n-1}$$

Das bedeutet, dass die Singularität des Quotienten $\frac{a^n-b^n}{a-b}$ für $a = b$ hier gar nicht vorkommt. Es gilt also:

$$\lim_{b\to a} \frac{a^n - b^n}{a-b} = na^{n-1}$$

7.3 Die Verallgemeinerung des Exponenten

Dieser Grenzwert kann so verallgemeinert werden, dass statt n jede beliebige, von null verschiedene, Zahl auftreten kann.

Alle folgenden Überlegungen gehen davon aus, dass der Exponent nicht verschwindet.

7.3.1 $G(-n,a,b)$, negativer Exponent

Zunächst ergibt sich durch Termumformung

$$\frac{a^{-n} - b^{-n}}{a-b} = \frac{\frac{1}{a^n} - \frac{1}{b^n}}{a-b} = -\frac{a^n - b^n}{a^n b^n (a-b)}$$

Demnach ist

$$\lim_{b\to a} \frac{a^{-n} - b^{-n}}{a-b} = -\lim_{b\to a} \frac{\sum_{i=0}^{n-1} a^{n-1-i}b^i}{a^n b^n} = -\frac{na^{n-1}}{a^{2n}} = -na^{-n-1}$$

7.3.2 $G(\frac{1}{2},a,b)$, Exponent $\frac{1}{2}$

Wir beginnen wieder mit der Termumformung

$$\frac{\sqrt{a} - \sqrt{b}}{a-b} = \frac{\sqrt{a} - \sqrt{b}}{(\sqrt{a})^2 - (\sqrt{b})^2}$$

Für $a \neq b$ erhalten wir hieraus

$$\frac{\sqrt{a}-\sqrt{b}}{a-b}=\frac{1}{\sqrt{a}+\sqrt{b}}$$

und damit für den Grenzwert $b \to a$

$$\lim_{b\to a}\frac{1}{\sqrt{a}+\sqrt{b}}=\frac{1}{2\sqrt{a}}=\frac{1}{2}a^{-\frac{1}{2}}$$

7.3.3 $G(\frac{1}{n},a,b)$, Exponent $\frac{1}{n}$

Analog zum vorigen Abschnitt formen wir um.

$$\frac{a^{\frac{1}{n}}-b^{\frac{1}{n}}}{a-b}=\frac{a^{\frac{1}{n}}-b^{\frac{1}{n}}}{(a^{\frac{1}{n}})^n-(b^{\frac{1}{n}})^n}=\frac{1}{\sum_{i=0}^{n-1}(a^{\frac{1}{n}})^{n-1-i}(b^{\frac{1}{n}})^i}$$

Daraus ergibt sich

$$\lim_{b\to a}\frac{a^{\frac{1}{n}}-b^{\frac{1}{n}}}{a-b}=\frac{1}{n}(a^{-\frac{1}{n}})^{n-1}=\frac{1}{n}a^{\frac{1}{n}-1}$$

7.3.4 $G(\frac{n}{m},a,b)$, Exponent $\frac{n}{m}$

Wir substituieren in

$$\frac{a^{\frac{n}{m}}-b^{\frac{n}{m}}}{a-b}$$

$$a^{\frac{1}{m}}=c \qquad b^{\frac{1}{m}}=d$$

und erhalten

$$\frac{c^n-d^n}{c^m-d^m}=\frac{\frac{c^n-d^n}{c-d}}{\frac{c^m-d^m}{c-d}}$$

durch Grenzübergang folgt daraus

$$\lim_{d\to c}\frac{\frac{c^n-d^n}{c-d}}{\frac{c^m-d^m}{c-d}}=\frac{nc^{n-1}}{mc^{m-1}}=\frac{n}{m}c^{n-m}$$

Durch Resubstitution wird daraus

$$\frac{n}{m}c^{n-m}=\frac{n}{m}(a^{\frac{1}{m}})^{n-m}=\frac{n}{m}a^{\frac{n-m}{m}}=\frac{n}{m}a^{\frac{n}{m}-1}$$

womit wieder die schon bekannte Regel erfüllt wird.

7.3.5 reeller Exponent

Die reelle Zahl r sei dargestellt als Grenzwert einer Folge rationaler Zahlen.

$$r = \lim_{n \to \infty} r_n$$

Dann gilt:

$$\lim_{n \to \infty} \lim_{b \to a} \frac{a^{r_n} - b^{r_n}}{a - b} = \lim_{n \to \infty} r_n a^{r_n - 1} = r a^{r-1}$$

8 Die Ableitung einer Funktion

Unter der Ableitung einer Funktion einer reellen Veränderlichen an der Stelle x_1 versteht man bekanntlich den Grenzwert des Differenzenquotienten

$$\lim_{x_2 \to x_1} \frac{f(x_2) - f(x_1)}{x_2 - x_1}$$

8.1 Ableitung von Polynomen

Für die Potenzfunktion $f(x) = x^n$ ist das der Grenzwert des geometrischen Quotienten. Diesen Grenzwert kennen wir bereits. Wir lassen dabei, wie üblich, den Index beim Grenzwert weg.

$$\lim_{x_2 \to x_1} \frac{x_2^n - x_1^n}{x_2 - x_1} = nx^{n-1}$$

Mit der für die Ableitung üblichen Schreibweise nach Leibniz haben wir

$$f'(x) = nx^{n-1}$$

Die ebenfalls, besonders in der Physik übliche Schreibweise nach Newton liefert

$$\dot{y}(x) = nx^{n-1}$$

Daneben haben wir noch die Schreibweise als Differentialquotient.

$$\frac{dy}{dx} = nx^{n-1}$$

Für Polynome gilt

$$f(x) = \sum_{i=0}^{n} c_i x^i$$

Daher

$$\lim_{x_2 \to x_1} \frac{\sum_{i=0}^{n} c_i x_2^i - \sum_{i=0}^{n} c_i x_1^i}{x_2 - x_1}$$

Das können wir als Summe von geometrischen Quotienten umformen.

$$\lim_{x_2 \to x_1} \sum_{i=0}^{n} c_i \frac{x_2^i - x_1^i}{x_2 - x_1}$$

und erhalten

$$f'(x) = \sum_{i=0}^{n} c_i i x^{i-1}$$

8.2 Ableitung von Wurzelfunktionen

Aus der Verallgemeinerung des geometrischen Quotienten auf rationale und sogar reelle Exponenten ergeben sich die entsprechenden Ableitungsregeln. Als Beispiel diene

$$f(x) = \sqrt{x} = x^{\frac{1}{2}} \quad \longrightarrow \quad f'(x) = \frac{1}{2} x^{-\frac{1}{2}} = \frac{1}{2\sqrt{x}}$$

8.3 Die Ableitung von e^x

Die Ableitung von e^x ergibt sich aus

$$e^x = \lim_{n \to \infty} (1 + \frac{x}{n})^n$$

Da auch die Ableitung durch einen Grenzprozess definiert ist, liegen zwei Grenzprozesse vor, die vertauschbar sind.

$$
\begin{aligned}
(e^x)' &= \lim_{n\to\infty}((1+\frac{x}{n})^n)' \\
(e^x)' &= \lim_{n\to\infty}(n(1+\frac{x}{n})^{n-1}\cdot\frac{1}{n}) \\
(e^x)' &= \lim_{n\to\infty}(1+\frac{x}{n})^{n-1} \\
(e^x)' &= \lim_{n\to\infty}(1+\frac{x}{n})^{n}(1+\frac{x}{n})^{-1} \\
(e^x)' &= \lim_{n\to\infty}(1+\frac{x}{n})^{n}\cdot\lim_{n\to\infty}(1+\frac{x}{n})^{-1} \\
(e^x)' &= \lim_{n\to\infty}(1+\frac{x}{n})^{n}\cdot\lim_{n\to\infty}\frac{n}{n+x} \\
(e^x)' &= \lim_{n\to\infty}(1+\frac{x}{n})^{n}\cdot 1 \\
(e^x)' &= e^x
\end{aligned}
$$

8.4 Die Ableitung von Sinus und Cosinus

Durch die Darstellung von $\sin x$ und $\cos x$ als Potenzreihen können wir unsere bisherigen Betrachtungen auch hierauf anwenden.

$$f(x) = \sin x = \sum_0^\infty (-1)^n \frac{x^{2n+1}}{(2n+1)!}$$

$$f'(x) = \lim_{x_2\to x_1}\frac{\sin x_2 - \sin x_1}{x_2 - x_1}$$

$$f'(x) = \lim_{x_2\to x_1}\frac{\sum_0^\infty (-1)^n \frac{x_2^{2n+1}}{(2n+1)!} - \sum_0^\infty (-1)^n \frac{x_1^{2n+1}}{(2n+1)!}}{x_2 - x_1}$$

$$f'(x) = \lim_{x_2 \to x_1} \frac{\sum_0^\infty (-1)^n \frac{x_2^{2n+1} - x_1^{2n+1}}{(2n+1)!}}{x_2 - x_1}$$

Durch Vertauschen der beiden Grenzprozesse erhalten wir

$$f'(x) = \sum_0^\infty (-1)^n \frac{\lim_{x_2 \to x_1} \frac{x_2^{2n+1} - x_1^{2n+1}}{x_2 - x_1}}{(2n+1)!}$$

und damit

$$f'(x) = \sum_0^\infty (-1)^n \frac{x^{2n}}{(2n)!}$$

Das ist der Cosinus

$$f'(x) = \cos x$$

8.5 Die Produktregel

Wenn die Funktion $f(x)$ eine Produktdarstellung $f(x) = u(x)v(x)$ hat, dann gilt für die Ableitung

$$f'(x) = \lim_{x_2 \to x_1} \frac{u(x_2)v(x_2) - u(x_1)v(x_1)}{x_2 - x_1}$$

Mit der Methode des Einfügens einer Null ergibt sich

$$f'(x) = \lim_{x_2 \to x_1} \frac{u(x_2)v(x_2) - u(x_1)v(x_2) + u(x_1)v(x_2) - u(x_1)v(x_1)}{x_2 - x_1}$$

und daraus

$$f'(x) = \lim_{x_2 \to x_1} \frac{u(x_2) - u(x_1)}{x_2 - x_1} v(x_2) + \lim_{x_2 \to x_1} u(x_1) \frac{v(x_2) - v(x_1)}{x_2 - x_1}$$

Im Grenzfall gibt es keinen Unterschied mehr zwischen x_1 und x_2. Wir lassen den Index dann weg.

$$f'(x) = u'(x)v(x) + u(x)v'(x)$$

Wenn wir noch die unabhängige Variable x weglasssen, gewinnen wir die übersichtliche Formel

$$(uv)' = u'v + uv'$$

8.6 Die Quotientenregel

Die Quotientenregel ergibt sich aus der Produktregel durch impliziertes Differenzieren.

$$f(x) = \frac{u(x)}{v(x)} \quad \text{abgekürzt} \quad f = \frac{u}{v}$$

Wir multiplizieren beide Seiten mit v und bilden auf beiden Seiten die Ableitung

$$(fv)' = u'$$
$$f'v + fv' = u'$$
$$f'v + \frac{u}{v}v' = u'$$

Auflösen nach f' ergibt

$$f' = \frac{u'v - uv'}{v^2} \quad \text{oder} \quad \left(\frac{u}{v}\right)' = \frac{u'v - uv'}{v^2}$$

8.7 Die Kettenregel

Wenn zwei Funktionen in der Weise verschachtelt sind, dass der Funktionswert der inneren Funktion der Eingabewert der äußeren Funktion ist, dann spricht man von einer Verkettung dieser Funktionen. Wie die einzelnen Ableitungen dieser Funktionen zur Ableitung der Verkettung führen, zeigt die Kettenregel.

Wir bedienen uns dabei der Schreibweise für die Ableitung mit dem Differentialquotienten.

$$f(x) = g(h(x))$$

$$f'(x) = \lim_{x_2 \to x_1} \frac{g(h(x_2)) - g(h(x_1))}{x_2 - x_1}$$

$$f'(x) = \lim_{x_2 \to x_1} \frac{g(h(x_2)) - g(h(x_1))}{h(x_2) - h(x_1)} \cdot \frac{h(x_2 - h(x_1)}{x_2 - x_1}$$

$$f'(x) = \frac{d(g(x))}{d(h(x))} \cdot \frac{d(h(x))}{dx}$$

Zur besseren Übersicht kürzen wir ab.

$$f' = \frac{dg}{dh} \cdot h'$$

Die Ableitung einer Verkettung ist demnach das Produkt aus der äußeren Ableitung und der inneren.

8.8 Ableitung bei Parameterdarstellung

Meistens wird eine Funktion durch einen Term In der Veränderlichen x angegeben. Beispiel

$$y = x^2$$

Dabei bezeichnet man x als unabhängige, y als abhängige Variable. Die Bezeichnung ist asymmetrisch. Vertauscht man die Rollen von x und y, so erhält man die Umkehrfunktion. Sollen x und y jedoch gleichberechtigt sein, muss eine Darstellung herangezogen werden, die die Symmetrie zum Ausdruck bringen kann.

Das Gewünschte leistet die Parameterform. Dabei wird eine neue Variable eingeführt, von der jetzt sowohl x als auch y abhängen.

Als Beispiel betrachten wir die Kreisgleichung

$$y = \sqrt{r^2 - x^2}$$

Ohne allzu viel Phantasie können wir uns vorstellen, dass bei einer physikalischen Betrachtung einer Kreisbewegung keine Richtung bevorzugt wird. Wir bringen also einen Aspekt in ein Problem, der diesem nicht angemessen ist. Stellen wir die Kreisgleichung in der Parameterform dar so wird dieser Fehler vermieden. Die neue Variable hat eine natürliche Interpretation als Zeit.

$$x = \cos(t) \qquad y = \sin(t)$$

Die Ableitung erhalten wir aus der Definition

$$f'(x) = \lim_{x_2 \to x_1} \frac{y_2 - y_1}{x_2 - x_1} = \lim_{x_2 \to x_1} \frac{\frac{y_2 - y_1}{t_2 - t_1}}{\frac{x_2 - x_1}{t_2 - t_1}}$$

Wir haben es jetzt mit zwei Ableitungen zu tun, einmal nach x und einmal nach t. Zur Unterscheidung hat sich eingebürgert, die Ableitung nach t mit einem hochgestellten Punkt zu bezeichnen.

$$f'(x) = \frac{\dot{y}}{\dot{x}}$$

Alternativ dazu haben wir die Möglichkeit, bei der Parameterform zu bleiben und die Ableitung ebenfalls in Parameterform anzugeben.

Bei der Kreisgleichung gilt dann

$$\dot{x} = -\sin(t) \qquad \dot{y} = \cos(t)$$

8.9 Punkte maximaler Krümmung

Dieses Beispiel soll zeigen, dass jede Schreibweise für die Ableitung ihre Vor- und Nachteile hat. Hier soll der Vorteil der Punktschreibweise beim impliziten Ableiten gezeigt werden.

Für die Krümmung κ einer Kurve gilt

$$\kappa = \frac{\ddot{y}}{(1+\dot{y}^2)^{\frac{3}{2}}}$$

Das formen wir um zu

$$\kappa \cdot (1+\dot{y}^2)^{\frac{3}{2}} = \ddot{y}$$

und leiten beide Seiten ab.

$$\dot{\kappa}(1+\dot{y}^2)^{\frac{3}{2}} + \kappa \cdot \frac{3}{2}(1+\dot{y}^2)^{\frac{1}{2}} \cdot 2\dot{y}\ddot{y} = \dddot{y}$$

Für das Krümmungsmaximum gilt $\dot{\kappa} = 0$.

$$3\dot{y}\ddot{y}^2 = \dddot{y}(1+\dot{y}^2)$$

8.9.1 Exponentialfunktion

Das bedeutet zum Beispiel für $y = e^x$

$$3e^{3x} = e^x + e^{3x} \longrightarrow 2e^{2x} = 1 \rightarrow x = -\frac{1}{2}\log(2)$$

8.9.2 Kubische Funktion

Wir betrachten zunächst die Funktion $y = x^3$. Die Ableitungen sind

$$\begin{aligned} \dot{y} &= 3x^2 \\ \ddot{y} &= 6x \\ \dddot{y} &= 6 \end{aligned}$$

Dann gilt

$$3(3x^2) \cdot 36x^2 = 6(1 + 9x^4) \rightarrow 324x^4 = 6 + 54x^4 \rightarrow x = \pm\sqrt{\frac{1}{45}}$$

Jetzt nehmen wir eine Variante mit Maximum und Minimum: $y = x^3 - 3x$.

$$\begin{aligned} \dot{y} &= 3x^2 - 3 \\ \ddot{y} &= 6x \\ \dddot{y} &= 6 \end{aligned}$$

Dann gilt

$$3(3x^2 - 3) \cdot 36x^2 = 6(1 + 9x^4 - 18x^2 + 9) \rightarrow 324x^4 - 324x^2 = 6 + 54x^4 - 96x^2 + 54$$

$$x = \pm 1.03$$

Bemerkenswert ist, dass das Krümmungsmaximum nicht mit den Extremwerten der Funktion zusammenfällt.

9 Das bestimmte Integral

Wenn wir eine Zahlenmenge M durch eine einzelne Zahl repräsentieren wollen, dann ist meist der Mittelwert die geeignete Wahl. Dazu werden alle Zahlen aus der Zahlenmenge addiert und das Ergebnis durch die Anzahl geteilt.

Bekanntlich muss der so erhaltene Mittelwert nicht als Element in der Zahlenmenge M vorkommen.
Beispiel

$$M = \{1, 5, 15\} \quad \rightarrow \quad \overline{m} = 7$$

Die Zahlenmenge M kann beliebig groß sein, muss aber endlich sein, da wir anderenfalls keine Anzahl zum Dividieren hätten.

Wenn wir den durchschnittlichen Wert einer Funktion in einem Intervall finden wollen, haben wir es mit einer unendlichen Menge zu tun.

Um das Problem auf den endlichen Fall zurück zu führen, treffen wir eine Auswahl an Funktionswerten. Die kleinste Auswahl besteht in einem einzigen Funktionswert.

So unwahrscheinlich es klingen mag, aber eine sehr große Klasse von Funktionen hat diese Eigenschaft, dass ein Funktionswert genügt. Diesen liefert der Mittelwertsatz der Differentialrechnung.

Dieser macht eine Aussage über ein Paar von Funktionen, nämlich einer Funktion f und ihrer Ableitung f'.

10 Symmetrische Polynome

Der Begriff des symmetrischen Polynoms ist erst sinnvoll ab zwei Variablen und bezeichnet solche Polynome, die bei allen Vertauschungen dieser Variablen denselben Wert liefern.

10.1 Der Quotient als symmetrisches Polynom

Vertauscht man bei unserem Quotienten a und b, so behält er seinen Wert bei. Diese Eigenschaft haben auch die symmetrischen Polynome, die wir hier kurz betrachten werden.
Klar ist, dass Summe und Produkt zweier symmetrischer Polynome wieder symmetrische Polynome sind. Daher stellt sich die Frage, ob es elementar symmetrische Polynome gibt, die alle anderen erzeugen. Diese gibt es und sie sind aus dem Satz von Viëta zu ermitteln.
Dieser besagt, dass Summe und Produkt der Lösungen die Koeffizienten der quadratischen Gleichung bestimmen. Summe und Produkt sind kommutativ, womit wir schon zwei elementar symmetrische Polynome angeben können.

$$\sigma_1 = a + b$$

$$\sigma_2 = a \cdot b$$

Ersetzen wir bei unserem Quotienten die Differenz durch die Summe

$$a^n + b^n$$

so nennt man diesen Term Potenzsumme. Offenbar sind alle Potenzsummen symmetrische Polynome, da sie bei der Vertauschung der Variablen ihren Wert behalten. Hier folgen jetzt einige Potenzsummen mit zwei Variablen. Die Potenzsummen $s_n = a^n + b^n$ in der Darstellung durch elementarsymmetrische Polynome nennt man Newton'sche Identitäten. Sie können durch die Rekursionsformel

$$s_{n+1} = s_n\sigma_1 - s_{n-1}\sigma_2 \quad \text{mit} \quad s_1 = a + b \quad s_0 = 2$$

ermittelt werden.

n	$a^n + b^n$	elementare Darstellung
0	$1 + 1$	2
1	$a + b$	σ_1
2	$a^2 + b^2$	$\sigma_1^2 - 2\sigma_2$
3	$a^3 + b^3$	$\sigma_1^3 - 3\sigma_1\sigma_2$
4	$a^4 + b^4$	$\sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2$
5	$a^5 + b^5$	$\sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1\sigma_2^2$
6	$a^6 + b^6$	$\sigma_1^6 - 6\sigma_1^4\sigma_2 + 9\sigma_1^2\sigma_2^2 - 2\sigma_2^3$
7	$a^7 + b^7$	$\sigma_1^7 - 7\sigma_1^5\sigma_2 + 14\sigma_1^3\sigma_2^2 - 7\sigma_1\sigma_2^3$

Zu erwähnen ist noch, dass für die Potenzsummen modulo einer Primzahl gilt:

$$a^p + b^p \equiv (a + b)^p \mod p$$

Das ist eine Eigenschaft der Binomialkoeffizienten.

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Für den Fall, dass n Primzahl ist, kann es nicht gekürzt werden, da beide Faktoren im Nenner kleiner als n sind und wegen der Primalität von n auch kein Produkt entstehen kann, welches gleich n ist. Daher bleibt der Faktor n erhalten und der Binomialkoeffizient ist ein Vielfaches von n. Ausnahme sind die Fälle $k = 0$ und $k = n$. Hier haben die Binomialkoeffizienten den Wert 1. Daher gilt für primes n

$$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \equiv a^n + b^n \mod n$$

10.2 Darstellung des Quotienten in elementarsymmetrischen Polynomen

Da der Quotient ein symmetrisches Polynom ist, muss es eine solche Darstellung geben.

Die folgende Tabelle gibt die Darstellung für $n \leq 8$ an.

n	elementare Darstellung
0	1
1	σ_1
2	$\sigma_1^2 - \sigma_2$
3	$\sigma_1^3 - 2\sigma_1\sigma_2$
4	$\sigma_1^4 - 3\sigma_1^2\sigma_2 + \sigma_2^2$
5	$\sigma_1^5 - 4\sigma_1^3\sigma_2 + 3\sigma_1\sigma_2^2$
6	$\sigma_1^6 - 5\sigma_1^4\sigma_2 + 6\sigma_1^2\sigma_2^2 - \sigma_2^3$
7	$\sigma_1^7 - 6\sigma_1^5\sigma_2 + 10\sigma_1^3\sigma_2^2 - 4\sigma_1\sigma_2^3$

Die Zeilen dieser Tabelle, also die geometrischen Quotienten für verschiedene n, können mit derselben Rekursionsformel wie bei den Potenzsummen gewonnen werden. Der einzige Unterschied liegt im Wert für $n = 0$. Dieser ist bei den Potenzsummen 2, bei den Quotienten 1.

$$g_{n+1} = g_n\sigma_1 - g_{n-1}\sigma_2 \quad \text{mit} \quad g_1 = a + b \quad g_0 = 1$$

10.3 Quadratische Gleichung und symmetrische Polynome

Kehren wir noch einmal zurück zu der Lösungsvariante mit der Diskriminante. Die elementarsymmetrischen Polynome für zwei Variable sind

$$\begin{aligned} \sigma_1 &= x_1 + x_2 \\ \sigma_2 &= x_1 x_2 \end{aligned}$$

Die Differenz $x_1 - x_2$ ist nicht symmetrisch, wohl aber das Quadrat davon. Demnach muss dieses eine Darstellung in elementarsymmetrischen Polynomen haben. Es gilt

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1 x_2$$

und damit

$$(x_1 - x_2)^2 = \sigma_1^2 - 4\sigma_2$$

Nach Viëta ist das gleich

$$(x_1 - x_2)^2 = p^2 - 4q$$

Damit ist die Diskriminante bei den symmetrischen Funktionen eingeordnet. Zur Lösung der quadratischen Gleichung müssen wir die Wurzel aus dieser Diskriminante ziehen können. Wir haben dann

$$x_1 = \frac{1}{2}((x_1 + x_2) + (x_1 - x_2)) = \frac{1}{2}\left(\sigma_1 + \sqrt{\sigma_1^2 - 4\sigma_2}\right)$$

$$x_2 = \frac{1}{2}((x_1 + x_2) - (x_1 - x_2)) = \frac{1}{2}\left(\sigma_1 - \sqrt{\sigma_1^2 - 4\sigma_2}\right)$$

Setzen wir wieder nach Viëta $\sigma_1 = -p$ und $\sigma_2 = q$, so erhalten wir die bekannte Lösungsformel.

Wir sehen also, wie ausgehend von vollständiger Symmetrie durch Symmetriereduktion die Lösung gewonnen wird. Ist diese Reduktion nicht möglich (negative Diskriminante), dann gibt es auch keine Lösung.

10.4 Nichtlineare Gleichungssysteme

Die symmetrischen Polynome bieten eine sehr effektive Methode zur Auflösung nichtlinearer Gleichungssysteme, wie an dem folgenden, sehr einfachen Beispiel gezeigt werden soll.

$$x^3 + y^3 = 9$$
$$x + y = 3$$

Ersetzt man die Potenzsummen durch die elementarsymmetrischen Polynome, so erhält man

$$\sigma_1^3 - 3\sigma_1\sigma_2$$
$$\sigma_1 = 3$$

Damit ergibt sich für σ_2

$$27 - 9\sigma_2 = 9$$

und daraus

$$\sigma_2 = 2$$

Nach Viëtabilden σ_1 und σ_2 die Koeffizienten einer quadratischen Gleichung in der Normalform

$$x^2 - \sigma_1 x + \sigma_2 = 0$$

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

Wegen der verschwindenden Koeffizientensumme sind die Lösungen 1 und 2.
Ein weniger triviales Beispiel ist

$$x^4 + y^4 = 17$$

$$x^2 + y^2 = 5$$

Durch die Newton'schen Identitäten ergibt sich

$$\begin{aligned} \sigma_1^4 - 4\sigma_1^2\sigma_2 + 2\sigma_2^2 &= 17 \\ \sigma_1^2 - 2\sigma_2 &= 5 \end{aligned}$$

Hieraus kann σ_1 eliminiert werden, und man erhält

$$\sigma_2^2 = 4$$

und damit

$$\sigma_2 = -2 \vee 2$$

Damit ist

$$\sigma_1^2 = 9 \vee 1$$

und

$$\sigma_1 = -3 \vee 3 \vee -1 \vee 1$$

Unter Beachtung der Bedingung $\sigma_1^2 - 2\sigma_2 = 5$ sind diese quadratischen Gleichungen möglich

$$\begin{aligned} x^2 + 3x + 2 &= 0 \\ x^2 - 3x + 2 &= 0 \\ x^2 + x - 2 &= 0 \\ x^2 - x - 2 &= 0 \end{aligned}$$

Daraus ergibt sich die Lösungsmenge

$$\mathbb{L} = \{(1;2), (-1;2), (1;-2), (-1;-2)\}$$

10.5 Ein Problem aus dem Bundeswettbewerb Mathematik 2006

Es ist zu zeigen, dass die Gleichung

$$x^3 + y^3 = 4(x^2y + xy^2 + 1)$$

nicht mit ganzen Zahlen x und y erfüllt werden kann.
Links wie rechts finden sich symmetrische Polynome. Ersetzt man sie durch ihre elementarsymmetrische Darstellung, so ergibt sich

$$\sigma_1^3 - 3\sigma_1\sigma_2 = 4\sigma_1\sigma_2 + 4$$

Das vereinfachen wir zu

$$\sigma_1^3 - 7\sigma_1\sigma_2 = 4$$

Dadurch wird offensichtlich, dass ein Teilbarkeitsproblem durch die Primzahl 7 entsteht. Die linke Seite kann faktorisiert werden.

$$\sigma_1(\sigma_1^2 - 7\sigma_2) = 4$$

Hieraus folgt zunächst, dass σ_1 nicht verschwindet. Seien λ und μ Teiler von 4 mit $\lambda\mu = 4$, so ist $\sigma_1 = \lambda$ und demzufolge

$$\sigma_1^2 - 7\sigma_2 = \mu$$

Das ergibt zusammen

$$\lambda^2 - \mu = 7\sigma_2$$

Somit müsste die linke Seite ebenso wie die rechte durch 7 teilbar sein. Wir müssen also nur noch zeigen, dass das nicht der Fall ist.

$$\begin{aligned} \lambda^2 - \mu &\equiv 0 \quad mod\ 7 \\ \lambda^2 &\equiv \mu \quad mod\ 7 \\ \lambda^3 &\equiv 4 \quad mod\ 7 \end{aligned}$$

Jetzt kommt man auf zwei Wegen zum gewünschten Widerspruch. Entweder zeigt man explizit für alle Siebenerreste, dass keiner die 4 als dritte Potenz hat, oder man quadriert nochmals beide Seiten und erhält:

$$\lambda^6 \quad \equiv \quad 2 \quad mod\, 7$$

Da 7 Primzahl und $\lambda \neq 0$ ist, kann der kleine Satz von Fermat angewendet werden. Dieser besagt:
Für jede ganze Zahl ($a \neq 0$) und jede Primzahl p gilt

$$a^{p-1} \equiv 1\ mod\ p$$

Bei der gestellten Aufgabe liegt aber Kongruenz zu 2 vor, was im Widerspruch zu diesem Satz steht.

11 Die kubische Gleichung

11.1 Die Lösung der kubischen Gleichung

Substituiert man in der kubischen Gleichung

$$x^3 + ax^2 + bx + c = 0$$

die Unbekannte x durch $x - \frac{a}{3}$, so fällt das quadratische Glied weg und wir erhalten eine reduzierte kubische Gleichung der Form

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

Diese lässt sich mit rein algebraischen Mitteln auflösen, was wir mit Hilfe der symmetrischen Polynome zeigen wollen.

11.2 Der direkte Weg zur Lösung

Dazu betrachten wir zunächst das folgende quadratische Polynom Q:

$$Q(x) = (x - x_1)(x - x_2) = x^2 - (x_1 + x_2)x + x_1x_2$$

und ersetzen x_1 und x_2 durch die dritten Potenzen zweier geeigneter Zahlen $a^3 = x_1$ und $b^3 = x_2$. Damit geht das Polynom über in

$$Q(x) = (x - a^3)(x - b^3) = x^2 - (a^3 + b^3)x - a^3b^3$$

Die Koeffizienten sind offenbar symmetrische Polynome in a und b. Diese ersetzen wir durch die elementarsymmetrischen Polynome und erhalten

$$Q(x) = x^2 - (\sigma_1^3 - 3\sigma_1\sigma_2)x + \sigma_2^3$$

Jetzt substituieren wir in der reduzierten kubischen Gleichung $x = \sigma_1$ und erhalten

$$\sigma_1^3 + p\sigma_1 + q = 0$$

Die Lösung der kubischen Gleichung gelingt durch die keinesfalls naheliegende, aber strategisch erfolgreiche Addition einer Null:

$$\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_1\sigma_2 + p\sigma_1 + q = 0$$

Ebenfalls nicht naheliegend, aber erfolgreich ist das Faktorisieren des dritten und vierten Summanden.

$$\sigma_1^3 - 3\sigma_1\sigma_2 + \sigma_1(3\sigma_2 + p) + q = 0$$

Für

$$\sigma_2 = -\frac{p}{3}$$

ergibt sich

$$\sigma_1^3 - 3\sigma_1\sigma_2 = -q$$

Diese Terme können wir nun in das oben angeführte Polynom Q einsetzen, wobei wir für die bessere Übersicht die Variable x in z umbenennen, und erhalten eine quadratische Gleichung

$$z^2 + qz - \left(\frac{p}{3}\right)^3 = 0$$

Deren Lösungen sind nach den vorigen Betrachtungen a^3 und b^3.

$$a^3 = -\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}$$

Diese Formel ist nach Cardano benannt.
Hat man also a^3 bestimmt, dann kennt man auch a. Wegen $\sigma_2 = ab$ erhält man b aus

$$ab = -\frac{p}{3}$$

und gewinnt wegen $\sigma_1 = a + b$ so eine Lösung für σ_1. Das war aber genau die Substitution für x.

11.3 Systematischer Weg nach Galois

11.3.1 Die dritten Einheitswurzeln

Die kubische Gleichung

$$x^3 - 1 = 0$$

hat nach dem Fundamentalsatz der Algebra drei Lösungen. Eine ist reell, die beiden anderen sind konjugiert komplex.

$$\mathbb{L} = \left\{1, \quad -\tfrac{1}{2} + \tfrac{i}{2}\sqrt{3}, \quad -\tfrac{1}{2} - \tfrac{i}{2}\sqrt{3}\right\}$$

Setzen wir zur Abkürzung

$$\tau = -\frac{1}{2} + \frac{i}{2}\sqrt{3}$$

so erhalten wir

$$\mathbb{L} = \left\{1, \quad \tau, \quad \tau^2\right\}$$

Die Summe der drei Lösungen verschwindet

$$1 + \tau + \tau^2 = 0$$

Daraus ergeben sich für beliebige Werte x_1, x_2 und x_3

$$\begin{aligned} b_0 &= x_1 + x_2 + x_3 \\ b_1 &= \tau x_1 + \tau^2 x_2 + x_3 \\ b_2 &= \tau^2 x_1 + \tau x_2 + x_3 \end{aligned}$$

Das gilt insbesondere auch für die drei Lösungen einer kubischen Gleichung. Umgekehrt lassen sich die drei x-Werte aus den b_i bestimmen.

$$\begin{aligned} x_1 &= \tfrac{1}{3}(b_0 + \tau^2 b_1 + \tau b_2) \\ x_2 &= \tfrac{1}{3}(b_0 + \tau b_1 + \tau^2 b_2) \\ x_3 &= \tfrac{1}{3}(b_0 + b_1 + b_2) \end{aligned}$$

11.3.2 Die Verringerung der Symmetrie

Die Lösungsidee von Galois beruht auf der Verringerung von Symmetrie. Die Koeffizienten der Gleichung sind allesamt symmetrische Funktionen der drei Lösungen, wie im Satz von Viëta angegeben. Die Lösungen selber sind vollständig unsymmetrisch. Diese Idee wird bereits an der Lösungsformel für quadratische Gleeichungen sichtbar. Die Diskriminante ist eine symmetrische Funktion der Lösungen, die Wurzel daraus ist es nicht. Diese ändert bei Vertauschung das Vorzeichen.

Die Diskriminante der kubischen Gleichung ist

$$D = (x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2$$

Sie ist vollständig symmetrisch und kann daher durch die elementarsymmetrischen Polynome und damit auch durch die Koeffizienten dargestellt werden. Zieht man daraus die Quadratwurzel, so ist diese nur noch gegenüber zyklischen Vertauschungen symmetrisch. Damit sollte ein Teilschritt in Richtung Lösung gewonnen sein.

Der letzte Schritt besteht dann darin, einen kubischen Term zu finden, der durch die Koeffizienten und die Quadratwurzel aus der Diskriminante dargestellt werden kann.

Dazu bieten sich b_1 und b_2 aus dem vorherigen Abschnitt an.

11.3.3 Die kubische Diskriminante

Die elementarsymmetrischen kubischen Polynome sind

$$\begin{aligned}\sigma_1 &= x_1 + x_2 + x_3\\ \sigma_2 &= x_1x_2 + x_2x_3 + x_3x_1\\ \sigma_3 &= x_1x_2x_3\end{aligned}$$

$$D = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$$

$$D = ((x_1 + x_2)^2 - 4x_1x_2)((x_2 + x_3)^2 - 4x_2x_3)((x_3 + x_1)^2 - 4x_3x_1)$$

$$\begin{aligned}&(x_1 + x_2)^2(x_2 + x_3)^2(x_3 + x_1)^2\\ &-4x_1x_2(x_2 + x_3)^2(x_3 + x_1)^2\\ &-4x_2x_3(x_1 + x_2)^2(x_3 + x_1)^2\\ &-4x_3x_1(x_1 + x_2)^2(x_2 + x_3)^2\\ &+16x_1x_2^2x_3(x_1 + x_3)^2\\ &+16x_1^2x_2x_3(x_2 + x_3)^2\\ &+16x_1x_2x_3^2(x_1 + x_2)^2\\ &-64x_1^2x_2^2x_3^2\end{aligned}$$

$$(x_1 + x_2)(x_2 + x_3)(x_3 + x_1) = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 + 2x_1x_2x_3$$

$$\sigma_1\sigma_2 = x_1^2x_2 + x_1^2x_3 + x_1x_2^2 + x_1x_3^2 + x_2^2x_3 + x_2x_3^2 + 3x_1x_2x_3$$

$$(x_1 + x_2)(x_2 + x_3)(x_3 + x_1) = \sigma_1\sigma_2 + \sigma_3$$

11.4 Praktische Anwendung der Cardano'schen Formel

Die Cardanoformel ist äußerst sperrig und wird in der Schule, wenn überhaupt, nur ganz selten behandelt. Es gibt bekanntlich sehr gute und schnelle Approximationsverfahren. Ebenso kann man ganzzahlige Lösungen mit der an anderer Stelle beschriebenen Methode über die Koeffizientensumme schnell ermitteln. Bei nicht ganzzahligen Lösungen und wenn man Wert auf Exaktheit legt, ist die Formel unverzichtbar. Ein Beispiel soll das verdeutlichen.
Wir betrachten die Gleichung

$$x^3 + 6x - 20 = 0$$

Nach der Cardano-Formel ist

$$a = \sqrt[3]{10 + \sqrt{108}}$$

Daraus ergibt sich für b:

$$b = -\frac{6}{3\sqrt[3]{10 + \sqrt{108}}}$$

Jetzt muss man erst mal sehen, dass man durch Erweitern mit

$$\sqrt[3]{10 - \sqrt{108}}$$

den Nenner dieses Bruches rational machen kann.

$$b = -\frac{6\sqrt[3]{10 - \sqrt{108}}}{3\sqrt[3]{-8}} = \sqrt[3]{10 - \sqrt{108}}$$

Wir erhalten also als Lösung

$$x = \sqrt[3]{10 + \sqrt{108}} + \sqrt[3]{10 - \sqrt{108}}$$

Das war es aber noch nicht, denn nach binomischer Formel gilt

$$(1+\sqrt{3})^3 = 1^3 + 3 \cdot 1^2\sqrt{3} + 3 \cdot 1 \cdot (\sqrt{3})^2 + (\sqrt{3})^3 = 10 + 6\sqrt{3} = 10 + \sqrt{108}$$

Entsprechend gilt

$$(1-\sqrt{3})^3 = 10 - \sqrt{108}$$

Damit ergibt sich für x

$$x = 1 + \sqrt{3} + 1 - \sqrt{3} = 2$$

Man sieht, wie schwer die Ganzzahligkeit der Lösung zu erkennen ist.
Starten wir stattdessen gleich mit der Suche nach ganzzahligen Lösungen, so erhalten wir als Koeffizientensumme den Wert -13 und finden wir über deren Teilermenge

$$\{\pm 1; \pm 13\}$$

als mögliche Lösungen

$$0; 2; -12; 14$$

Die Null ist es nicht, da das absolute Glied nicht verschwindet. Auch -12 und 14 können es nicht sein, da sie keine Teiler des absoluten Gliedes sind. Es bleibt als einziges 2 übrig und die Probe überzeugt von der Richtigkeit.

12 Die geometrische Reihe

12.1 Das St. Ives Problem

As I was going to St Ives

I met a man with seven wives

And every wife had seven sacks

And every sack had seven cats

And every cat had seven kits

Kits, cats, sacks, wives

How many were going to St Ives?

Dieses Kinderlied, welches um 1750 erstmals erwähnt wird, spricht dafür, dass die geometrische Reihe damals schon bekannt war. Die Summe, die zu finden ist, lautet

$$1 + 7 + 7^2 + 7^3 + 7^4$$

Das ist aber gleichbedeutend mit

$$\frac{7^5 - 1}{7 - 1} = 2801$$

Exakte Logik verlangt als Lösung jedoch 1, da der Erzähler denen begegnet, die von St. Ives weggehen. Gefragt ist jedoch, wieviele hingehen.
Noch exaktere Logik verneint die Lösbarkeit überhaupt, da noch andere, die nicht im Lied vorkommen, mit nach St. Ives gehen könnten.
Ein ähnliches Problem kommt im Papyrus Rhind von 1650 v. Chr. vor.

12.2 Besonderheiten der geometrischen Reihe

12.2.1 Das Geometrische an der Geometrischen Reihe

Die geometrische Reihe ergibt sich aus

$$\sum_{i=0}^{n-1} a^{n-1-i}b^i = \frac{a^n - b^n}{a - b}$$

indem man $a = 1$ und $b = q$ setzt.

$$\sum_{i=0}^{n-1} q^i = \frac{1 - q^n}{1 - q}$$

Schon der allgemeine Quotient hat die Eigenschaft, dass seine Summanden jeweils geometrische Mittelwerte ihrer beiden Nachbarn sind. Das hat der geometrischen Reihe ihren Namen gegeben. Für die Geometrische Folge trifft diese Eigenschaft natürlich auch zu.
Betrachten wir das Produkt der beiden Nachbarn eines Summanden $a^{n-1-i}b^i$ aus der obigen Reihe

$$a^{n-1-i-1}b^{i-1} \cdot a^{n-1-i+1}b^{i+1}$$

durch Vereinfachung ergibt sich

$$a^{2n-2i}b^{2i}$$

Daraus erhält man

$$a^{n-1-i}b^i = (a^{2n-2i}b^{2i})^{\frac{1}{2}}$$

womit die angekündigte Mittelwerteigenschaft gezeigt ist.

12.2.2 Konvergenz der Geometrischen Folge

Von der Geometrischen Folge ausgehend ist für $0 < q < 1$

$$\lim_{n\to\infty} q^n = 0$$

Es liegt demnach eine Nullfolge vor.
Wie sieht man das?
Als allgemein anerkannte Definition für eine Nullfolge gilt, dass diese vorliegt, wenn von einer bestimmten Nummer N an alle Folgenglieder kleiner sind als ein vorgeschriebener ebenfalls kleiner Wert. Diese Definition ist gedanklich ziemlich schwierig, weil sie paralleles Vorwärts- und Rückwärtsdenken erfordert. Als Vergleich kann man ein Spiel betrachten. Der eine Spieler gibt eine kleine, positive Zahl vor. Der Begriff der

kleinen, positiven Zahl ist so verbreitet in der Mathematik, dass er einen Namen bekommen hat. Dieser hat, wie üblich, nur einen einzigen Buchstaben und heißt

$$\epsilon$$

Es mag übertrieben erscheinen, einem einzelnen Buchstaben eine ganze, abgesetzte Zeile zu widmen. Die abschreckende Wirkung dieses Buchstabens auf alle, die sich mit der Analysis auseinandersetzen mussten, rechtfertigt es vielleicht.
Wir betrachten ein Spiel. Spieler A gibt das ϵ vor. Spieler B muss nun ein N vorweisen können, von dem er sagen kann, dass Spieler A kein Glied in der Folge finden kann, für welches $n > N$ und zusätzlich $q^n > \epsilon$.
Die folgende Tabelle soll das veranschaulichen, wobei wir $q = \frac{1}{2}$ setzen.

ϵ (Vorgabe A)	N (Antwort B)
0.1	4
0.01	7
0.001	10
10^{-6}	20

Auffällig ist hier, dass sich Spieler A viel mehr anstrengen muaa, als Spieler B. Dieser kann irgendwie leicht kontern. Wir begegnen hier einer Eigenschaft der Logarithmusfunktion. Wenn Spieler A sagt ϵ, dann stellt Spieler B die Ungleichung

$$\left(\frac{1}{2}\right)^N < \epsilon$$

auf und bestimmt N mit

$$N > \frac{\log \epsilon}{\log(\frac{1}{2})}$$

Allgemeiner gilt für eine beliebiges $q < 1$

$$N < \frac{log(\epsilon)}{log(q)}$$

Die Basis der Logarithmen spielt keine Rolle.
Gemeinsames Ergebnis aller Methoden ist, dass die Geometrische Foge eine Nullfolge ist, wenn $q < 1$.

Damit ist die Konvergenzbedingung erfüllt. Zu jedem $\epsilon > 0$ gibt es ein N mit

$$n > N \;\Rightarrow\; q^n < \epsilon$$

12.2.3 Konvergenz der Geometrischen Reihe

Setzt man beim Geometrischen Quotienten $a = 1$ und $b = q$, so erhält man die Geometrische Reihe

$$G(n, 1, q) = 1 + q + q^2 + q^3 + \cdots + q^n = \sum_{i=0}^{n} = \frac{1 - q^n}{1 - q}$$

Falls q zusätzlich die Bedingung $q < 1$ erfüllt, konvergiert die Geometrische Reihe.

$$\lim_{n\to\infty} (1 + q + q^2 + q^3 + \cdots + q^n) = \lim_{n\to\infty} \frac{1 - q^n}{1 - q} = \frac{1}{1 - q}$$

Die Konvergenz folgt aus der Konvergenz der Geometrischen Folge, die im vorigen Abschnitt gezeigt wurde.

$$\lim_{n\to\infty} \frac{1 - q^n}{1 - q} = \lim_{n\to\infty} \frac{1}{1 - q} - \lim_{n\to\infty} \frac{q^n}{1 - q} = \frac{1}{1 - q} - \lim_{n\to\infty} \frac{q^n}{1 - q}$$

Für den Subtrahenden ganz rechts gilt

$$\lim_{n\to\infty} \frac{q^n}{1 - q} = \frac{\lim_{n\to\infty} q^n}{1 - q} = 0$$

12.3 Finanzmathematik

Als Anwendungen sollen zwei Beispiele aus der Finanzmathematik dienen, die Geldschöpfung und die Bewertung eines Hauses durch den Mietwert.

12.3.1 Die Geldschöpfung

Eine Person P_1 hat 1000 € in bar und zahlt diese bei ihrer Bank auf ihr dortiges Konto ein. Statt des Bargelds hat sie nun ein Bankguthaben. Da sich die Vermögensverhältnisse dieser Person nicht geändert haben, betrachtet man die Geldmenge als die Summe aus dem Bargeld und den Bankguthaben.
Die Bank ihrerseits verdient ihr Geld mit Krediten und wird daher einen solchen einer Person P_2 gewähren. Wenn die Person P_2 das geliehene Geld bei einer anderen Bank einzahlt, dann haben P_1 und P_2 zusammen 2000 € Guthaben, über die sie verfügen können, obwohl ursprünglich nur 1000 € da waren. Man kann den Gedanken fortführen, dass auch die Bank von P_2 das Geld nicht behält, sondern an P_3 ausleiht. Diese

Person zahlt das Geld bei ihrer Bank ein und so sind bereits 3000 € verfügbares Geld entstanden.
Auf diese Weise kann eine unbegrenzte Verfügungsmasse entstehen, was einer totalen Inflation gleichkäme. Die Einrichtung einer Zentralbank, bei der alle angeschlossenen Geschäftsbanken ein Guthaben unterhalten müssen, löst das Problem. Die Zentralbank legt einen Satz fest, der von jedem eingezahlten Betrag einbehalten und diesem Guthaben zugeführt werden muss. Dieser Satz heißt Mindestreservesatz.
Nehmen wir an, er betrage 20%. Dann muss die Bank von P_1 200 € einbehalten und darf nur 800 € weiterverleihen. Die nächste Bank muss davon 160 € einbehalten und darf nur noch 560 € weiterverleihen.
Wie groß ist die verfügbare Geldmenge U_n, wenn n Personen in einer solchen Kreditkette stehen?

$$U_n = 1000\,€ \cdot (1 + 0.8 + 0.8^2 + 0.8^3 + \cdots + 0.8^n) = 1000\,€ \cdot G(n, 1, 0.8)$$

Offenbar liegt hier eine geometrische Reihe vor, deren Summe wir leicht angeben können.

$$U_n = 1000\,€ \cdot \frac{1 - 0.8^n}{1 - 0.8}$$

Da der Faktor 0.8 kleiner ist als 1, konvergiert diese Reihe und wir erhalten für eine große Zahl an Marktteilnehmern

$$U = 1000\,€ G(\infty, 1, 0.8) = 1000\,€ \cdot \frac{1}{1 - 0.8} = 1000\,€ \cdot 5 = 5000\,€$$

Das heißt, aus den ursprünglichen 1000 € ist eine größere verfügbare Geldmenge geworden. 5000 € bilden jedoch die obere Grenze, unabhängig davon, wieviele Personen beteiligt sind. Die hinzugekommene Menge von 4000 € nennt man die Geldschöpfung. Die Zentralbank hat daher die zusätzliche Aufgabe, dafür zu sorgen, dass nicht einfach Geld aus dem Hut gezaubert wird, sondern dass an die Kreditvergabe Bedingungen geknüpft werden. Der Geldschöpfung muss nämlich immer eine entsprechende Wertschöpfung gegenüberstehen.
Stellt die Zentralbank fest, dass zuviel Geld da ist und somit Inflation droht, dann kann sie sozusagen im Handstreich die Geldmenge verringern. Sie beschließt auf ihrer nächsten Sitzung, dass der Mindestreservesatz auf 25% angehoben wird. An die Stelle des Faktors 0.8 tritt der Faktor 0.75. Das Bedeutet

$$U = 1000\,€ \cdot \frac{1}{1 - 0.75} = 1000\,€ \cdot 4 = 4000\,€$$

Die Geldmenge ist deutlich geschrumpft.
Mit einer Senkung des Mindestreservesatzes kann die Zentralbank dem Markt mehr Geld zur Verfügung stellen.

12.3.2 Bewertung vermietbarer Immobilien

Nehmen wir an, wir haben einen Zinssatz von 4% pro Jahr. Dann wächst ein Kapital K_0 in einem Jahr auf $K_1 = K_0 \cdot 1.04$. Umgekehrt können wir den Wert von K_1, das erst in einem Jar entsteht, heute mit dem geringen Wert K_0 bewerten. Wir nennen das Diskontieren und den heutigen Wert Barwert. Demnach hat ein Kapital K_{10}, welches erst in zehn Jahren entsteht, den Barwert (heutigen Wert)

$$B_{10} = K_{10} \cdot \left(\frac{1}{1.04}\right)^{10}$$

Die Barwerte der Jahresmieten J der nächsten n Jahre können daher zu einem Gesamtbarwert R_n addiert werden.

$$R_n = B_0 + B_1 + B_2 + \cdots + B_n$$

Daraus ergibt sich für den vorliegenden Fall:

$$R_n = J \cdot \left(1 + \left(\frac{1}{1.04}\right) + \left(\frac{1}{1.04}\right)^2 + \cdots + \left(\frac{1}{1.04}\right)^n\right) = J \cdot G(n, \frac{1}{1.04}, 1)$$

Wieder ist der Faktor (Diskontierungsfaktor) kleiner als eins und es liegt Konvergenz vor.

$$R = J \cdot \frac{1}{1 - \frac{1}{1.04}}$$

Damit ist

$$R = J \cdot G(\infty, \frac{1}{1.04}, 1) = J \cdot \frac{1.04}{0.04} = J \cdot 26$$

Somit hat eine mit 700 € monatlich vermietete Wohnung einen Wert von

$$700\,€ \cdot 12 \cdot 26 = 218400\,€$$

Steigen die Zinsen z.B. auf 5%, so ändert sich die Bewertung auf

$$R = J \cdot G(\infty, \frac{1}{1.05}, 1) = J \cdot \frac{1.05}{0.05} = J \cdot 21$$

Die genannte Wohnung hat dann einen Wert von

$$700\,€ \cdot 12 \cdot 21 = 176400\,€$$

Wie man sieht, bedeuten steigende Zinsen sinkende Immobilienpreise. Daraus folgt, dass es zu Zeiten billigen Baugeldes ziemlich teuer ist, zu bauen. Ist dagegen das Baugeld teuer, braucht man weniger für das Bauen zu zahlen. Die zum Bauen aufzubringende Geldmenge ist anscheinend immer diesselbe. Es variiert lediglich die Verteilung auf Bank und Baugewerbe.
Es lohnt also nicht, beim Bauen auf fallende Zinsen zu hoffen. Ebensowenig muss man steigende Zinsen fürchten.

13 Wurzeln im Nenner

Wir betrachten noch einmal den geometrischen Quotienten für rationale Exponenten. Dabei zeigt sich, dass wir eine Möglichkeit haben, in speziellen Fällen auch Wurzeln mit größerem Index im Nenner eines Bruches zu beseitigen. Darüber hinaus lässt sich die Verallgemeinerung zu einer universellen Methode, mit der man jede beliebige Wurzelkonstruktion im Nenner auflösen kann, erkennen.

13.1 Algebraischer Hintergrund

In den Schulbüchern dient die Rationalisierung des Nenners der Anwendung von binomischen Formeln. Über die mathematischen Zusammenhänge erfährt man nichts. Dabei sind bei kaum einer anderen Übung algebraische Strukturen so klar zu erkennen. Man begnügt sich mit vagen Hinweisen. Die Wurzel aus dem Nenner müsse verschwinden, dann sei der Bruch besser zu handhaben. Mit der Wurzel rechne man wie mit jeder anderen Zahl auch.

13.1.1 Irrationalität von $\sqrt{2}$

Zuerst zeigen wir, dass $\sqrt{2}$ nicht im Körper $\mathbb{Q}$ vorhanden ist. Der Beweis erfolgt indirekt. Wir nehmen an, $\sqrt{2}$ wäre in $\mathbb{Q}$ enthalten und zeigen, dass daraus ein Widerspruch folgt.

Jedes Element aus $\mathbb{Q}$ kann als Bruch dargestellt werden, wobei Zähler und Nenner als ganzzahlig und teilerfremd angenommen werden können. Der Bruch ist also optimal gekürzt.

$$\frac{z}{n} = \sqrt{2}$$

Dann folgt daraus

$$z^2 = 2n^2$$

Die rechte Seite enthält also den Faktor 2, also muss z gerade sein. Dann enthält z ebenfalls den Faktor 2.

$$z = 2z_1 \Rightarrow z^2 = 2^2 z_1^2 \Rightarrow 2z_1^2 = n^2$$

Damit haben wir den gewünschten Widerspruch. Denn n müsste nun ebenfalls gerade sein, wodurch der Bruch mit 2 gekürzt werden könnte.

13.1.2 Erweiterungskörper

Zum uneingeschränkten Rechnen brauchen wir einen Körper, insbesondere zum Dividieren. $\mathbb{Q}$ ist zwar ein Körper, er enthält jedoch nicht $\sqrt{2}$. Durch die formale Erweiterung von $\mathbb{Q}$ um alle Summen und Produkte mit $\sqrt{2}$ erhalten wir einen sogenannten Erweiterungskörper K, in dem wir wieder uneingeschränkt rechnen können, also auch dividieren. Alle Elemente von K können in der Form

$$a + b\sqrt{2}$$

dargestellt werden. Damit ist klar, dass die Wurzel im Nenner beseitigt werden kann, denn der Bruch ist eine Division. Aus der Abgeschlossenheit von K ergibt sich, dass der Kehrwert des Nenners existiert. Erweitern wir den Bruch nun mit diesem Kehrwert, dann haben wir den Nenner 1.

$$\frac{1}{-1+\sqrt{2}} = \frac{1}{-1+\sqrt{2}} \cdot \frac{1+\sqrt{2}}{1+\sqrt{2}} = 1+\sqrt{2}$$

Das Problem besteht daher darin, eine geeignete Erweiterung des Bruches zu finden.

13.2 Umformung mit der geometrischen Reihe

Wir beginnen mit einem Beispiel:

$$\frac{1}{1-\sqrt[5]{2}}$$

Durch Umformen überzeugen wir uns, dass wir es mit dem geometrischen Quotienten zu tun haben.

$$\frac{1}{1-\sqrt[5]{2}} = -\frac{1-2}{1-2^{\frac{1}{5}}} = -\frac{1-2^{\frac{5}{5}}}{1-2^{\frac{1}{5}}} = -\frac{1-(2^{\frac{1}{5}})^5}{1-2^{\frac{1}{5}}} = -G(1, 2^{\frac{1}{5}}, 5)$$

Da der geometrische Quotient eine geometrische Reihe darstellt, erhalten wir

$$\frac{1}{1-\sqrt[5]{2}} = -2^{\frac{4}{5}} - 2^{\frac{3}{5}} - 2^{\frac{2}{5}} - 2^{\frac{1}{5}} - 1 = -\sqrt[5]{16} - \sqrt[5]{8} - \sqrt[5]{4} - \sqrt[5]{2} - 1$$

Diese Überlegungen lassen sich auf einen beliebigen Wurzelindex verallgemeinern.

$$\frac{1}{1-\sqrt[n]{2}} = -\sum_{0}^{n-1} 2^{\frac{i}{n}}$$

13.3 Die beiden Strukturen des Erzeugnisses

Wir lösen offenbar eine Divisionsaufgabe. Das bedeutet, wir müssen die Division ausführen können. Die passende algebraische Struktur ist der Körper. Wenn wir zum Körper der rationalen Zahlen die 5. Wurzel aus zwei hinzufügen und ebenso alle Summen und Produkte aus dieser Wurzel und den rationalen Zahlen, dann erhalten wir das sogenannte Erzeugnis.

$$K = \left\langle \mathbb{Q}, \sqrt[5]{2} \right\rangle$$

Dieses Erzeugnis hat zwei Strukturen, deren Zusammenwirken unser Problem allgemein löst. Zum einen ist es ein Körper, was uns garantiert, das wir zu jedem von 0 verschiedenen Element auch den Kehrwert als Element von K vorfinden.

Zum zweiten ist es ein Oberkörper zu $\mathbb{Q}$. Also ist es auch ein Vektorraum über $\mathbb{Q}$. Dieser hat eine Basis, die es gestattet, jedes Element als Linearkombination darzustellen. Im vorliegenden Beispiel hat der Vektorraum die Dimension 5. Stellen wir nun den Kehrwert in dieser Basis dar, so haben wir keine Wurzeln mehr im Nenner.

Die Basis ist nicht eindeutig bestimmt. Es genügt irgendeine Basis zu finden. Dazu betrachten wir die Potenzen des Nenners. Sind sie alle linear unabhängig, so ist der Nenner transzendent. Gibt es aber eine Potenz, die linear abhängig von den niedrigeren Potenzen ist, dann haben wir mit diesen eine Basis gefunden.

13.4 Einfaches Beispiel

Wir vereinfachen unser Beispiel noch einmal.

$$\frac{1}{1 - \sqrt[3]{2}}$$

Wir setzen

$$s = 1 - \sqrt[3]{2}$$

und erhalten

$$\begin{aligned} s^0 &= 1 \\ s^1 &= 1 - \sqrt[3]{2} \\ s^2 &= 1 - 2\sqrt[3]{2} + \sqrt[3]{4} \\ s^3 &= -1 - 3\sqrt[3]{2} + 3\sqrt[3]{4} \end{aligned}$$

Offenbar ist s^3 linear abhängig von s^2, s^1 und s^0.

$$s^3 = 3s^2 - 3s - 1$$

Daran ist zu erkennen, dass s Nullstelle des Polynoms

$$y = x^3 - 3x^2 + 3x + 1$$

ist. Dieses Polynom heißt Minimalpolynom von s, weil es von allen Polynomen, die s als Nullstelle haben, dasjenige mit dem kleinsten Grad ist.
Darüber hinaus haben wir eine Basis von

$$K = \left\langle \mathbb{Q}, \sqrt[3]{2} \right\rangle$$

gefunden

$$B_s = \{s^2, s^1, s^0\}$$

K ist demnach ein dreidimensionaler Vektorraum über $\mathbb{Q}$.

Wir bestimmen jetzt die Darstellung des Kehrwertes von s in dieser Basis.
Sei

$$s^{-1} = as^2 + bs + c \quad \text{mit } a, b, c \in \mathbb{Q}$$

Dann gilt

$$ss^{-1} = 1 = as^3 + bs^2 + cs = a(3s^2 - 3s - 1) + bs^2 + cs$$

Daraus ergibt sich

$$(3a + b)s^2 + (-3a + c)s - a = 1$$

Es ist also

$$a = -1,\ b = 3,\ c = -3$$

und damit

$$s^{-1} = -s^2 + 3s - 3$$

Damit ist die Aufgabe gelöst, denn wir haben für den Kehrwert von s eine Darstellung in $\mathbb{Q}$ gefunden, bei der es keinen Nenner mehr gibt.

Meistens wünscht man sich aber eine Darstellung in der Standardbasis

$$B_0 = \{1, \sqrt[3]{2}, \sqrt[3]{4}\}$$

Dieses Ziel kann man auf zwei Wegen erreichen. Da K ein Körper ist, gelten die Rechengesetze und wir können mit Hilfe des Assoziativgesetzes die Klammern auflösen.

$$s^{-1} = -(1 - 2\sqrt[3]{2} + \sqrt[3]{4}) + 3(1 - \sqrt[3]{2}) - 3 = -1 - \sqrt[3]{2} - \sqrt[3]{4}$$

Da K aber auch ein Vektorraum ist, kann man das Gleiche durch einen Basiswechsel erreichen. Dazu bildet man aus den Koordinaten der Basiselemente von B_s in der Standardbasis B_0 eine Matrix

$$\begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Durch Transponieren erhalten wir die gesuchte Transformationsmatrix T.

$$\begin{pmatrix} 1 & -2 & 1 \\ 1 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}^T = \begin{pmatrix} 1 & 1 & 1 \\ -2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$$

Damit erhalten wir

$$\begin{pmatrix} 1 & 1 & 1 \\ -2 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} -1 \\ 3 \\ -3 \end{pmatrix} = \begin{pmatrix} -1 \\ -1 \\ -1 \end{pmatrix}$$

Als Ergebnis erhalten wir natürlich dieselben Koordinaten wie durch das Ausmultiplizieren.

Dieses Beispiel zeigt, wie man sich beide Strukturen eines Erweiterungskörpers zunutze machen kann.

13.4.1 Beispiel aus dem Schulbuch

Zunächst wenden wir binomische Formeln an.

$$\frac{1}{1+\sqrt{2}+\sqrt{3}} = \frac{1-\sqrt{2}-\sqrt{3}}{1-(5+2\sqrt{6})} = -\frac{1}{2}\cdot\frac{1-\sqrt{2}-\sqrt{3}}{2+\sqrt{6}} =$$

$$= -\frac{1}{2}\cdot\frac{(1-\sqrt{2}-\sqrt{3})(2-\sqrt{6})}{-2} = \frac{1}{2}+\frac{1}{4}\sqrt{2}-\frac{1}{4}\sqrt{6}$$

alternativ gehen wir den Weg über den vektorraum un bestimmen eine Basis.

$$\begin{aligned} s^0 &= 1 \\ s^1 &= 1+\sqrt{2}+\sqrt{3} \\ s^2 &= 6+2\sqrt{2}+2\sqrt{3}+2\sqrt{6} \\ s^3 &= 16+14\sqrt{2}+12\sqrt{3}+6\sqrt{6} \\ s^4 &= 80+48\sqrt{2}+40\sqrt{3}+32\sqrt{6} \end{aligned}$$

Die lineare Abhängigkeit ist

$$s^4 = 4s^3+4s^2-16s+8$$

Das Minimalpolynom ist entsprechend

$$x^4-4x^3-4x^2+16x-8$$

Wir haben also mit $B=\{s^3,s^2,s,1\}$ eine Basis für

$$K=\left\langle \mathbb{Q},\sqrt{2},\sqrt{3}\right\rangle$$

gefunden. Da K ein Vektorraum ist, muss es für das Inverse zu s eine Darstellung in dieser Basis geben.

$$s^{-1} = as^3+bs^2+cs+d$$

Multiplikation mit s auf beiden Seiten liefert

$$1 = as^4+bs^3+cs^2+ds = 4as^3+4as^2-16as+8a+bs^3+cs^2+ds$$

Durch Koeffizientenvergleich erhalten wir daraus

$$a=\frac{1}{8},\ b=-\frac{1}{2},\ c=-\frac{1}{2},\ d=2$$

Damit ist

$$s^{-1} = \frac{1}{8}s^3 - \frac{1}{2}s^2 - \frac{1}{2}s + 2 = \frac{1}{2} + \frac{1}{4}\sqrt{2} - \frac{1}{4}\sqrt{6}$$

Die Abbildung der Basis B in die Standardbasis $B_0 = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ vermittelt

$$\begin{pmatrix} 16 & 6 & 1 & 1 \\ 14 & 2 & 1 & 0 \\ 12 & 2 & 1 & 0 \\ 6 & 2 & 0 & 0 \end{pmatrix} \begin{pmatrix} 1/8 \\ -1/2 \\ -1/2 \\ 2 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/4 \\ 0 \\ -1/4 \end{pmatrix}$$

13.5 Kehrwert einer komplexen Zahl

Die dargestellte Methode lässt sich auch bei komplexen Zahlen anwenden, da hier ebenfalls eine Körpererweiterung vorliegt. Der Grundkörper ist der der reellen Zahlen. Hinzu kommt die imaginäre Einheit i. Dann ist das Erzeugnis der Körper der komplexen Zahlen.

$$\mathbb{C} = \langle \mathbb{R}, i \rangle$$

Das Auffinden des Kehrwertes betrachten wir am Beispiel der Zahl $z = 1 - i$.
Mit Hilfe der binomischen Formel erhalten wir

$$\frac{1}{1-i} = \frac{1+i}{(1-i)(1+i)} = \frac{1+i}{2} = \frac{1}{2} + \frac{1}{2}i$$

Der geometrische Quotient G(1,i,2) liefert

$$\frac{1}{1-i} = \frac{1}{2} \cdot \frac{2}{1-i} = \frac{1}{2} \cdot \frac{1-i^2}{1-i} = \frac{1}{2} + \frac{1}{2}i$$

Schließlich finden wir über eine Basis von $\mathbb{C}$ als Vektorraum

$$
\begin{aligned}
s^0 &= 1 \\
s^1 &= 1 - i \\
s^2 &= -2i
\end{aligned}
$$

Die lineare Abhängigkeit ist

$$s^2 = 2s - 2$$

Dann hat der Kehrwert die Darstellung

$$s^{-1} = as + b \quad \text{mit} \quad a, b \in \mathbb{R}$$

Daraus folgt

$$1 = as^2 + bs = a(2s - 2) + bs \;\Rightarrow\; a = -\frac{1}{2}, \quad b = 1$$

Es ist also

$$s^{-1} = -\frac{1}{2}s + 1 = \frac{1}{2} + \frac{1}{2}i$$

Die Transformationsmatrix ist

$$\begin{pmatrix} 1 & 1 \\ -1 & 0 \end{pmatrix} \begin{pmatrix} -1/2 \\ 1 \end{pmatrix} = \begin{pmatrix} 1/2 \\ 1/2 \end{pmatrix}$$

13.6 Der Körper der komplexen Zahlen

Wir betrachten hier noch kurz die Erweiterung von $\mathbb{R}$ mit i zu $\mathbb{C}$. Bekanntlich legt man als imaginäre Einheit i die Lösung der Gleichung

$$x^2 + 1 = 0$$

fest. Mit dieser Festlegung sind alle quadratischen Gleichungen lösbar in $\mathbb{C}$. Dennoch scheint in dieser Festlegung eine gewisse Willkür zu liegen.

Betrachten wir eine Alternative. Wir definieren eine andere imaginäre Einheit j als Lösung der Gleichung

$$x^2 + 2x + 3$$

Deren Diskriminante ist ebenfalls negativ.

Dann gilt

$$j^2 + 2j + 3 = 0 \quad \Rightarrow \quad j^2 = -2j - 3$$

Wir zeigen jetzt, dass sich mit dem so definierten j die Gleichung $x^2 + 1 = 0$ lösen lässt. Dazu bilden wir eine komplexe Zahl $a + bj$ mit reellen Koeffizienten a und $b \neq 0$ und bestimmen diese.

$$(a+bj)^2+1 = 0 \quad \Rightarrow \quad a^2+b^2j^2+2abj+1 = 0 \quad \Rightarrow \quad a^2+b^2(-2j-3)+2abj+1 = 0$$

Durch Koeffizientenvergleich erhalten wir

$$-2b^2 + 2ab = 0 \quad \Rightarrow \quad a = b$$

$$a^2 - 3b^2 + 1 = 0 \quad \Rightarrow \quad b^2 = \frac{1}{2}$$

Damit haben wir

$$(\frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}})^2 = \frac{1}{2} + \frac{j^2}{2} + j = \frac{1}{2} - \frac{2j}{2} - \frac{3}{2} + j = -1$$

Offenbar lässt sich die übliche imaginäre Einheit i durch die alternative Einheit j ausdrücken.

$$i = \frac{1}{\sqrt{2}} + \frac{j}{\sqrt{2}}$$

Daraus folgt

$$\langle \mathbb{R}, j \rangle = \langle \mathbb{R}, i \rangle = \mathbb{C}$$

Da $\mathbb{C}$ auch ein zweidimensionaler Vektorraum ist, gibt es eine Transformation der Basis $\{1, j\}$ in die Basis $\{1, i\}$, die durch eine Matrix vermittelt wird.

$$\begin{pmatrix} -1/\sqrt{2} & 1/\sqrt{2} \\ 1/\sqrt{2} & 1/\sqrt{2} \end{pmatrix} \begin{pmatrix} 1/\sqrt{2} \\ 1/\sqrt{2} \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

13.7 Die Gauß'sche Zahlenebene

Wie bei den algebraischen Körpererweiterungen haben wir hier mit $\mathbb{C}$ auch einen zweidimensionalenn Vektorraum. Mit der Gauß'schen Zahlenebene tritt noch eine dritte Struktur in derselben Menge hinzu, nämlich der zweidimensionale affine Raum. In diesem gibt es Punkte und Geraden, sowie Lagebeziehungen.

Ein und dasselbe Element von $\mathbb{C}$ kann daher als Punkt im affinen Raum, als Vektor im Vektorraum oder als Zahl im Körper aufgefasst werden.

Dadurch wird die Gauß'sche Zahlenebene zu einem hocheffizienten Konzept.

13.8 Endliche Körper

13.8.1 Restklassenkörper

Die Restklassen modulo 5

$+$	0	1	2	3	4	Permutation
0	0	1	2	3	4	(1)
1	1	2	3	4	0	(12345)
2	2	3	4	0	1	(13524)
3	3	4	0	1	2	(14253)
4	4	0	1	2	3	(15432)

$\cdot$	0	1	2	3	4	Permutation
0	0	0	0	0	0	
1	0	1	2	3	4	(1)
2	0	2	4	1	3	(1243)
3	0	3	1	4	2	(1342)
4	0	4	3	2	1	(14)(23)

bilden einen Körper mit 5 Elementen. Die Restklassen modulo 4 bilden dagegen keinen Körper, wie man an der Multiplikationstabelle sehen kann.

$+$	0	1	2	3	Permutation
0	0	1	2	3	(1)
1	1	2	3	0	(1234)
2	2	3	0	1	(13)(24)
3	3	0	1	2	(1432)

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Die Additionsgruppen sind zyklisch und isomorph zu C_5 bzw C_4.

Die Restklassen modulo 4 bilden einen Ring. Wie E. Galois gezeigt hat, kann man

jedoch einen Körper mit vier Elementen konstruieren, eben nur nicht mit Restklassen. Die Konstruktion geht wie folgt.Da jeder Körper die Elemente 0 und 1 enthalten muss, gibt es zwei weitere Elemente zu bestimmen. Wir bezeichnen den Körper mit $\mathbb{F}_4$. Die Bezeichnung $GF(4)$ ist ebenfalls verbreitet.

$$\mathbb{F}_4 = \{0, 1, a, b\}$$

Offenbar muss $a^2 = b$ und $b^2 = a$ sein, da die anderen Möglichkeiten ausscheiden. Dann folgt $ab = 1$. Damit wäre die Multiplikation definiert.

Für die Addition gehen wir zunächst davon aus, dass alle vier Elemente selbstinvers sind. Dann muss $a + 1 = b$ und $b + 1 = a$ sein. Dann ergibt sich folgendes Tabellenbild.

$+$	0	1	a	b	Permutation
0	0	1	a	b	(1)
1	1	0	b	a	(12)(34)
a	a	b	0	1	(13)(24)
b	b	a	1	0	(14)(23)

$\cdot$	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

Die Additionstabelle zeigt, dass die Addition nicht mehr nach C_4 definiert ist, sondern nach $C_2 \times C_2$, der Klein'schen Vierergruppe.

Dieser Körper kann auch, genau wie $\mathbb{C}$ durch Einführen eines imaginären Elements i, welches über eine unlösbare quadratische Gleichung definiert ist, aus $\mathbb{F}_2$ gewonnen werden.

Die einzige der vier quadratischen Gleichungen in $\mathbb{F}_2$, die dort keine Lösung hat, ist

$$x^2 + x + 1 = 0$$

Dann ist

$$i^2 + i + 1 = 0$$

und damit $a = i$ und $b = i + 1$ oder, was auf dasselbe hinausläuft, $b = i^2$.

Mit $b = i + 1$ kommt am besten zum Vorschein, dass es sich um einen zweidimensionalen Vektorraum über $\mathbb{F}_2$ handelt.

$$\mathbb{F}_4 \simeq V^2_{\mathbb{F}_2}$$

Eine weitere, sehr schöne Realisierung erhält man mit vier zweireihigen Matrizen, denen nichts Imaginäres anhaftet. Addition und Multiplikation erfolgen wie üblich. Die Elemente stammen aus $\mathbb{F}_2$.

$$\mathbb{F}_4 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

Im Gegensatz zur Gauß'schen Zahlenebene kann hier nicht noch ein affiner Raum hinzu gefügt werden, so dass es hier keine Geometrie gibt.

13.8.2 Die Potenzmenge

Die Potenzmenge ist die Menge aller Teilmengen einer Menge. Als Modell betrachten wir einen minimalistischen Modeladen, der nur zwei verschiedene Kleidermodelle führt, ein rotes und ein blaues. Die Potenzmenge ist hier die Menge aller Einkaufsmöglichkeiten, die dieser Laden zu bieten hat. Wir bezeichnen sie mit

$$\mathcal{P}(2)$$

Lara betritt zusammen mit ihrer Freundin Pia den Laden und will etwas kaufen. Sie verlässt sich auf ihren schlechten Geschmack und den noch schlechteren von Pia. Daher

trifft jede für sich eine Auswahl. An der Kasse werden die beiden Auswahlen zusammen geführt und Lara entfernt alles, was in beiden Auswahlen vorhanden ist. Damit ist eine Verknüpfung auf der Potenzmenge definiert. Wir sagen, wir haben eine Addition eingeführt. In der Mengenlehre heißt diese Verknüpfung symmetrische Differenz.

$$A \circ B = (A \setminus B) \cup (B \setminus A)$$

Jede der beiden Frauen hat vier Möglichkeiten der Auswahl. Die entsprechende Verknüpfungstabelle ist:

$\circ$	$\{\}$	$\{R\}$	$\{B\}$	$\{R,B\}$	Permutation
$\{\}$	$\{\}$	$\{R\}$	$\{B\}$	$\{R,B\}$	(1)
$\{R\}$	$\{R\}$	$\{\}$	$\{R,B\}$	$\{B\}$	(12)(34)
$\{B\}$	$\{B\}$	$\{R,B\}$	$\{\}$	$\{R\}$	(13)(24)
$\{R,B\}$	$\{R,B\}$	$\{B\}$	$\{R\}$	$\{\}$	(14)(23)

Wie wir an der Spalte der Permutationen erkennen können ist die Potenzmenge mit dieser Vernüpfung isomorph zur Klein'schen Vierergruppe.

Keine der üblichen Mengenverknüpfungen ist jedoch geeignet, als Multiplikation zu fungieren und die Potenzmenge zu einem Körper zu machen. Die Verknüpfungstabelle des Durchschnitts nehmen wir als Beispiel. Das Auftreten der leeren Menge außerhalb von der ersten Zeile und der ersten Spalte steht dem entgegen.

$\cap$	$\{\}$	$\{R\}$	$\{B\}$	$\{R,B\}$
$\{\}$	$\{\}$	$\{\}$	$\{\}$	$\{\}$
$\{R\}$	$\{\}$	$\{R\}$	$\{\}$	$\{B\}$
$\{B\}$	$\{\}$	$\{\}$	$\{B\}$	$\{R\}$
$\{R,B\}$	$\{\}$	$\{B\}$	$\{R\}$	$\{R,B\}$

Wir sehen durch den Vergleich der entsprechenden Tabellen, dass zwar eine Isomorphie zwischen den Additionsgruppen von $\mathcal{P}(2)$ und $\mathbb{F}_4$ besteht, da sie beide zur Klein'schen Vierergruppe isomorph sind, jedoch nicht zwischen den multiplikativen Gruppen.

$\mathcal{P}(2)$	$\mathbb{F}_4$
$\{\}$	0
$\{R,B\}$	1
$\{R\}$	a
$\{B\}$	b

13.8.3 Die symmetrische Gruppe S_3

Wir haben gesehen, dass der Körper $\mathbb{F}_4$ mit 2×2 Matrizen mit Elementen aus $\mathbb{F}_2$ darstellbar ist.

$$\mathbb{F}_4 = \left\{ \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \right\}$$

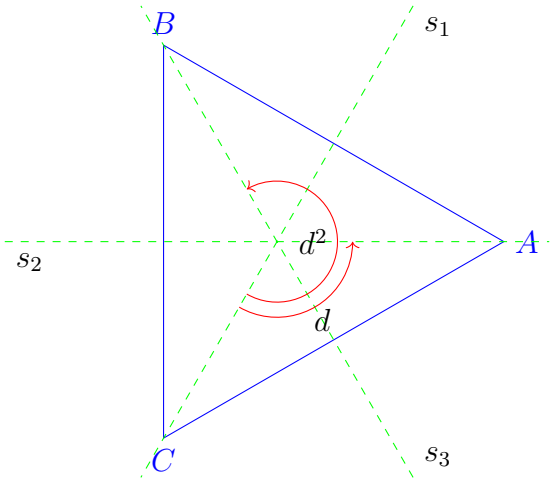
Die drei Matrizen, die von der Nullmatrix verschieden sind, bilden die multiplikative Gruppe des Körpers. Neben der Einheitsmatrix gibt es zwei Matrizen der Ordnung 3. Diese Gruppe ist zyklisch und kommutativ. Sie wird mit C_3 bezeichnet.

Insgesamt gibt es 16 2×2 Matrizen mit Elementen aus $\mathbb{F}_2$. Davon sind 6 regulär und bilden eine Gruppe. Sie wird bezeichnet mit $GL(2,2)$, wobei GL die Abkürzung für general linear group ist. Sie ist isomorph zur symmetrischen Gruppe S_3. Es ist die kleinste Gruppe, die nicht kommutativ ist.

$$GL(2,2) = \left\{ \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\}$$

$$GL(2,2) \simeq S_3$$

13.8.4 Die Symmetriegruppe des gleichseitigen Dreiecks



13.8.5 Gebrochen lineare Funktionen als Gruppe

Die folgenden sechs Funktionen, von denen jeweils nur der Funktionsterm angegeben ist, stellen ebenfalls die symmetrische Gruppe S_3 dar, wobei die Gruppenverknüpfung die Verkettung ist.

$$G = \left\{ x, \frac{x-1}{x}, \frac{1}{1-x}, \frac{1}{x}, 1-x, \frac{x}{x-1} \right\}$$

Diese Funktionen stellen in jedem beliebigen Körper die Gruppe S_3 dar. Betrachten wir sie speziell in $\mathbb{F}_2$, so gibt es keinen Unterschied mehr zwischen $+1$ und -1 und wir erhalten

$$G_2 = \left\{ x, \frac{x+1}{x}, \frac{1}{1+x}, \frac{1}{x}, 1+x, \frac{x}{x+1} \right\}$$

Betrachten wir eine beliebige gebrochen lineare Funktion

$$g = \frac{ax+b}{cx+d}$$

so sehen wir, dass sie auch durch die Matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

dargestellt werden kann, allerdings mit einer wichtigen Einschränkung. Der Funktionsterm ist ein Bruch und kann daher gekürzt und erweitert werden. So stellen etwa

$$\begin{pmatrix} 2 & 1 \\ 3 & 4 \end{pmatrix} \quad \text{und} \quad \begin{pmatrix} 4 & 2 \\ 6 & 8 \end{pmatrix}$$

dieselbe Funktion dar.

Für die Verkettung eines Elements mit sich selbst gilt:

$$g \circ g = g^2 = \frac{(a^2+bc)x + ab + bd}{(ac+cd)x + bc + d^2}$$

Führen wir hier die Kennzahlen der entsprechenden Matrix, nämlich die Spur $S = a+d$ sowie die Determinante $D = ad - bc$ ein, so ergibt sich

$$g^2 = \frac{(aS-D)x + bS}{cSx + dS - D}$$

Die Bedingung dafür, dass g^2 die identische Funktion ist, und g somit die Ordnung 2 hat, lautet

$$S = 0 \quad \text{und} \quad D \neq 0$$

Für g^3 egibt sich entsprechend

$$g^3 = \frac{(a(S^2 - D) - SD)x + b(S^2 - D)}{c(S^2 - D)x + d(S^2 - D) - SD}$$

Daraus folgt, dass g die Ordnung 3 hat, wenn

$$S^2 - D = 0 \quad \text{und} \quad SD \neq 0$$

13.8.6 Die Verknüpfungstabelle von S_3

13.8.7 Die Tafel der Symmetriegruppe

$\cdot$	e	d	d^2	s_1	s_2	s_3
e	e	d	d^2	s_1	s_2	s_3
d	d	d^2	e	s_3	s_1	s_2
d^2	d^2	e	d	s_2	s_3	s_1
s_1	s_1	s_2	s_3	e	d	d^2
s_2	s_2	s_3	s_1	d^2	e	d
s_3	s_3	s_1	s_2	d	d^2	e

Durch die Einfärbung wird die Struktur der symmetrischen Gruppe sichtbar.

Die Elemente e, d, d^2 bilden eine Untergruppe H, die zu C_3 isomorph ist. Diese Untergruppe ist Normalteiler. Die drei Spiegelungen entstehen durch Verknüpfung der drei Elemente von H mit einer der drei Spiegelungen.

$$N = \{se, sd, sd^2\} = \{s_1, s_2, s_3\} = sH = Hs$$

S_3 wird disjunkt zerlegt in den Normalteiler H sowie die sogenannte Nebenklasse N.

Auf der Menge

$$\{H, N\}$$

wird eine Verknüpfung induziert

$\cdot$	H	N
H	H	N
N	N	H

Offenbar ist diese Zerlegung eine Gruppe und als solche isomorph zur zyklischen Gruppe C_2.

Damit hat S_3 insgesamt die Struktur

$$S_3 = C_3 \times C_2$$

13.8.8 Permutationsmatrizen

An dieser Stelle schauen wir uns noch eine etwas andere Form der Darstellung von Permutationen an, nämlich als Permutationsmatrizen.

Neben der zweizeiligen Notation von Permutationen, bei der die erste Zeile die Anordnung vor und die zweite Zeile die Anordnung nach Anwendung angibt, benutzen wir die einzeilige, sogenannte Zyklenschreibweise.

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \longrightarrow (132)$$

Dabei steht die Zyklenschreibweise für die Abbildungskette

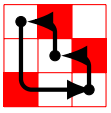
$$(132): \quad 1 \to 3 \to 2 \to 1$$

Wesentlich aufwendiger, aber dafür sehr anschaulich, ist die Darstellung als Permutationsmatrix. Dabei werden aus den beiden Zeilen der Zweizeiligen Darstellung zwei Spalten. Davon ist die eine die Darstellung für die Anordnung vorher, die andere für die Anordnung nachher. Die Spalte für vorher wird als Vektor nach den üblichen Regeln mit einer Matrix multipliziert, so dass das Ergebnis die Spalte für nachher ist. Die Matrix hat in jeder Zeile eine Eins, die restlichen Elemente sind null.

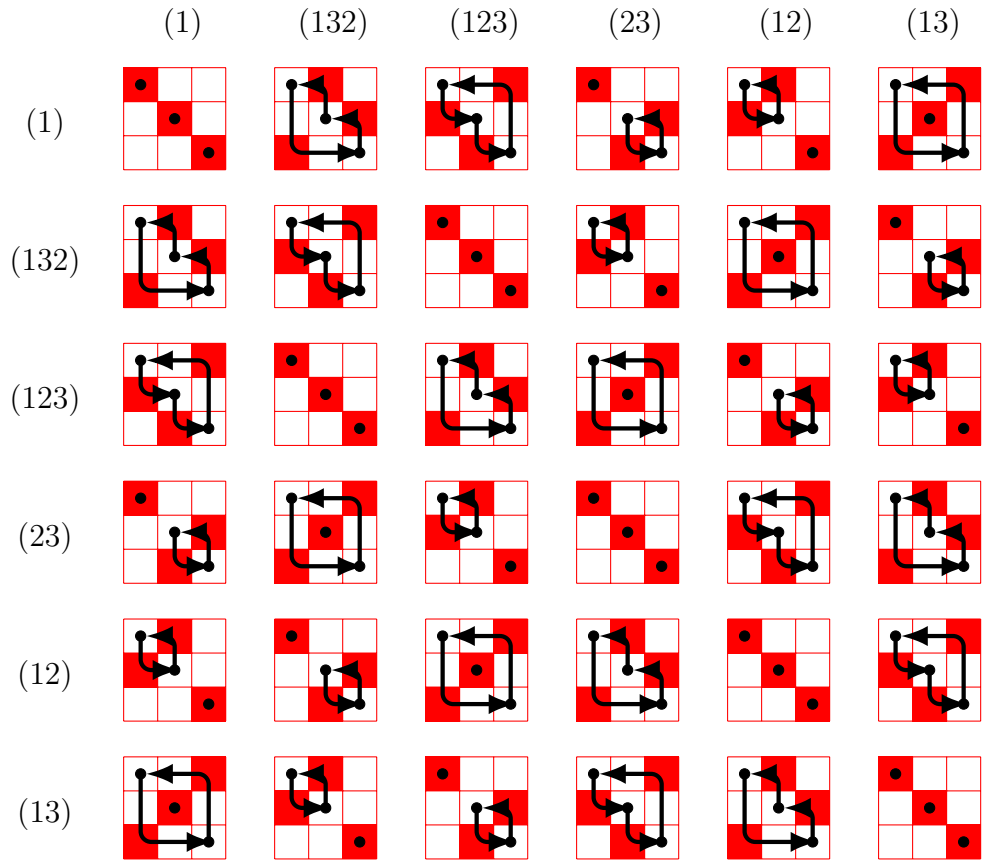
$$\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \quad \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \quad \begin{pmatrix} 3 \\ 1 \\ 2 \end{pmatrix}$$

Die Permutationsmatrizen sind alle regulär und bilden mit der Matrizenmultiplikation eine Gruppe. Es ist nicht weiter verwunderlich, dass diese Gruppe von sechs Matrizen isomorph zu S_3 ist.

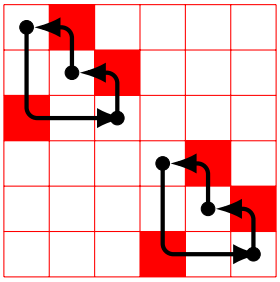
Die Permutationsmatrizen können mit der Zyklendarstellung kombiniert werden. Dazu verwandeln wir die Matrix in ein quadratisches Gitter und färben alle Felder ein, die einer Eins entsprechen. Dazu gibt es für jedes Element aus der Hauptdiagonalen einen Pfeil, der anzeigt, wohin es abgebildet wird.



Damit erhalten wir für die Multiplikationstabelle die folgende Darstellung.



Da in dieser Tabelle jede Permutation von S_3 vorkommt, sind die sechs Zeilen ihrerseits Permutationen der ersten Zeile. Betrachten wir als Beispiel die zweite Zeile.



Diese sechs Permutationen sind natürlich ebenfalls eine Gruppe und isomorph zu S_3.

13.8.9 Die symmetrische Gruppe S_3 als Faktorgruppe

Die symmetrische Gruppe S_4 hat bekanntlich 24 Elemente. Von den zahlreichen Untergruppen ist die Klein'sche Vierergruppe vielleicht die interessanteste, denn sie ist ein sogenannter Normalteiler.

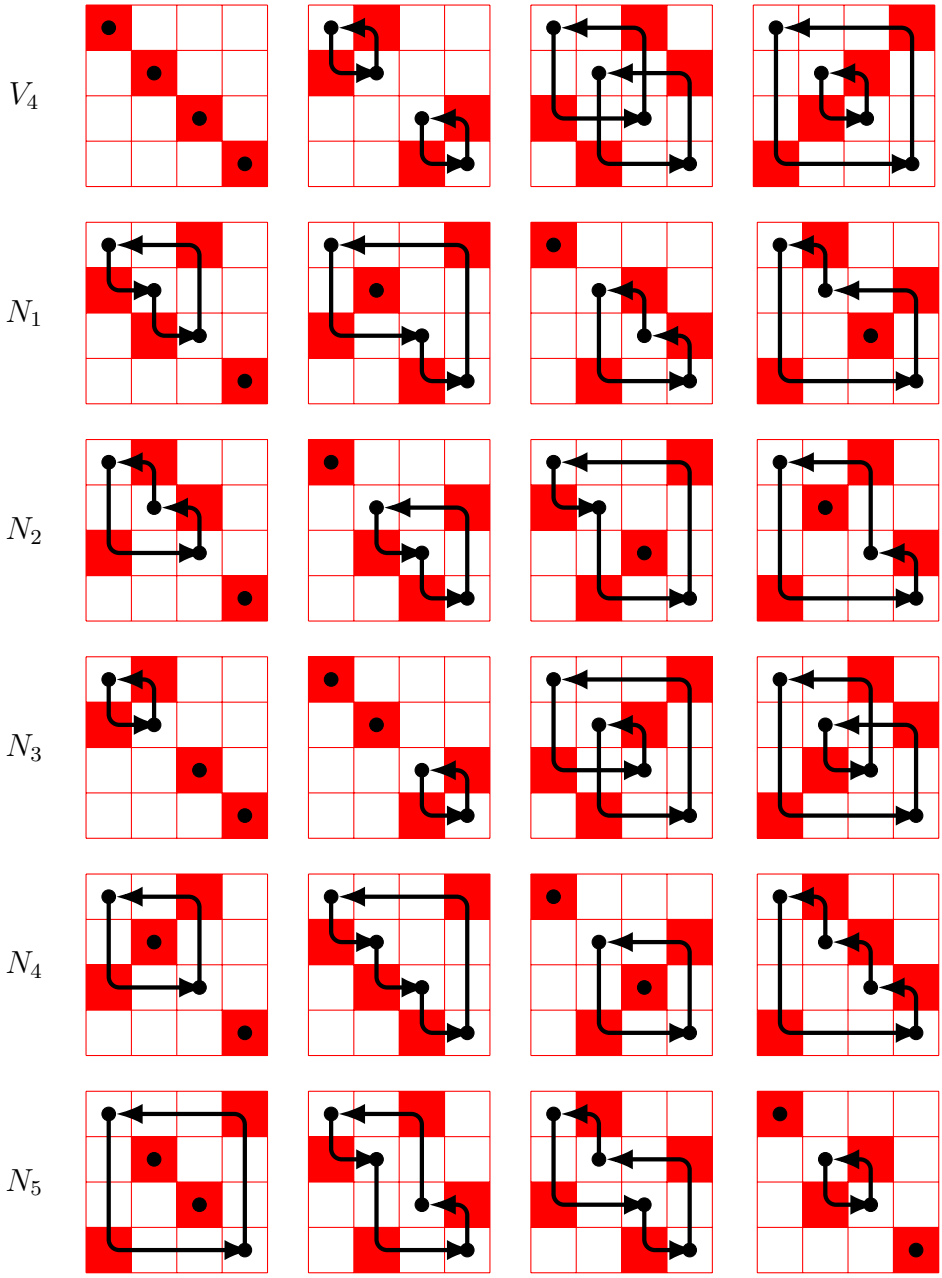
Dieser Begriff hat eine gewisse Analogie zum 5. Axiom von Euklid, dem Parallelenaxiom. Verallgemeinernd könnte man die Situation so beschreiben, dass es in einer großen Welt (Ebene) eine kleinere (Gerade) gibt, die in sich abgeschlossen ist. Findet man nun innerhalb der großen, aber außerhalb der kleinen ein Element (Punkt), so gibt es eine weitere kleine Welt von gleicher Struktur, die dieses Element enthält, aber kein Element mit der ersteren gemeinsam hat. Die beiden kleinen Welten sind disjunkt. Wir wollen sie als Parallelwelten bezeichnen.

Eine Entsprechung dieses Konzepts gibt es auch bei Gruppen, die nichttriviale Untergruppen haben. Dazu betrachten wir eine solche Untergruppe als kleine Welt in der großen Welt der Gruppe. Ein Element der Gruppe, welches nicht in der Untergruppe liegt, verknüpfen wir jetzt mit allen Elementen der Untergruppe. Auf diese Weise erhalten wir genau so viele Produkte, wie die Untergruppe Elemente hat. Wegen der Abgeschlossenheit der Untergruppe liegen alle diese Produkte außerhalb von ihr. Damit haben wir eine Parallelwelt gefunden. Da die Gruppenverknüpfung nicht kommutativ zu sein braucht, kann es zwei solcher Parallelwelten geben, je nach dem, ob man von links oder von rechts verknüpft.

Wir nennen diese Parallelwelten bei den Gruppen Nebenklassen. Dann gibt es Linksnebenklassen und Rechtsnebenklassen. Von besonderer Bedeutung sind die Untergruppen, bei denen die Links- und die Rechtsnebenklassen zusammen fallen. Diese besonderen Untergruppen heißen Normalteiler.

Die Klein'sche Vierergruppe erzeugt nun in der symmetrischen Gruppe S_4 fünf dieser Nebenklassen.

In der nachfolgenden Tabelle sind diese Nebenklassen als Permutationsmatrizen dargestellt.



Je nachdem, ob wir die Multiplikation eines festen Elements mit allen vier Elementen der Klein'schen Gruppe von links oder von rechts durchführen, erhalten wir dieselben vier Produkte. Da diese Multiplikation nicht kommutativ ist, erhalten wir diese Produkte aber in unterschiedlicher Anordnung. Das bedeutet, dass die Linksnebenklassen durch Permutationen aus den Rechtsnebenklassen hervorgehen. Im vorliegenden Fall bilden diese fünf Permutationen zusammen mit der Identität eine zu S_3 isomorphe Gruppe.

Die Gruppenmultiplikation erzeugt aber auch auf der Menge

$$\{N_0 = V_4, N_1 \dots N_5\}$$

eine Verknüpfung. Das Produkt zweier Nebenklassen erhalten wir, indem wir aus jedem der beiden Faktoren einen Repräsentanten wählen und diese mit der vorhandenen Gruppenmultiplikation verknüpfen. Als Ergebnis oder Produkt erklären wir diejenige Nebenklasse, die das Produkt der Repräsentanten enthält.

$$N_2 \circ N_3 \to (132) \cdot (12) = (13) \to N_4$$
$$N_2 \circ N_3 \to (234) \cdot (12) = (1234) \to N_4$$
$$\vdots$$

Diese Verknüpfung ist unabhängig von der Wahl der Repräsentanten. Sie ist also wohldefiniert.

Dadurch wird die Menge zur Gruppe, da auch die übrigen Axiome erfüllt sind. Diese Gruppe heißt Faktorgruppe. Sie ist in diesem Fall isomorph zur symmetrischen Gruppe S_3.

$$S_4/V_4 \cong S_3$$

14 Die Mittelwertsätze der Analysis

14.1 Steigung und Stetigkeit

Betrachten wir einen Polygonzug durch die Punkte mit den Koordinaten

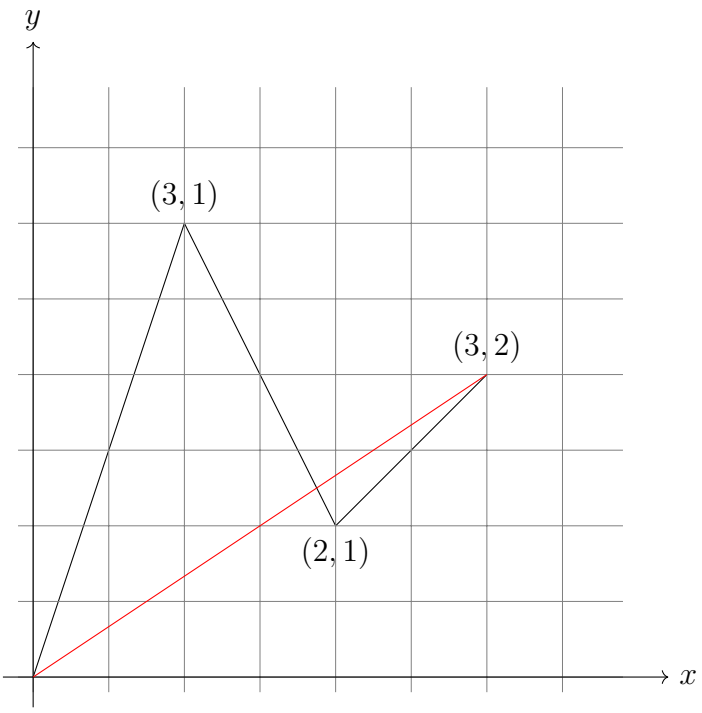
$$(0;0),\ (1;3),\ (2;1),\ (3;2)$$

so hat dieser drei Steigungen aufzuweisen, nämlich

$$m_1 = 3,\ m_2 = -2 \quad \text{und} \quad m_3 = 1$$

Die durchschnittliche Steigung ist daher

$$\overline{m} = \frac{2}{3}$$



Dieser Wert entspricht der Steigung des direkten Weges von $(0,0)$ nach $(3;2)$. Wie man es vom arithmetischen Mittel her kennt, braucht dieses keineswegs unter den Ausgangszahlen vorzukommen.

Liegt jedoch statt eines Polygonzuges eine stetige und differenzierbare Funktion vor, sagt der Mittelwertsatz der Differentialrechnung, dass die Steigung des direkten Weges an mindestens einer Stelle im Intervall vorkommt.

Das bedeutet etwas Tröstliches. Wenn wir unser Ziel erreicht haben, können wir sicher sein, dass wir wenigstens einmal unterwegs die richtige Richtung hatten.

14.2 Der Mittelwertsatz der Differentialrechnung

Für die Potenzfunktionen besagt dieser Satz, dass unser Quotient die Steigung dieser Funktion an einer Stelle im betreffenden Intervall ist.

$$\frac{x_2^n - x_1^n}{x_2 - x_1} = n\xi^{n-1} \;\; \xi \in [x_1; x_2]$$

oder anders ausgedrückt

$$G(n, x_2, x_1) = n\xi^{n-1}$$

14.2.1 Einige spezielle Potenzen

Das bedeutet für einige spezielle Werte von n, z.B. $n = 2$

$$G(2, x_2, x_1) = 2\xi$$

$$\frac{x_2^2 - x_1^2}{x_2 - x_1} = 2\xi$$

$$\xi = \frac{x_1 + x_2}{2}$$

Wir erhalten also auf diese Weise den arithmetischen Mittelwert.

Für $n = -1$ erhalten wir

$$\frac{\frac{1}{x_2} - \frac{1}{x_1}}{x_2 - x_1} = -\frac{1}{\xi^2}$$

oder

$$G(-1, x_2, x_1) = -\frac{1}{\xi^2}$$

und daraus den geometrischen Mittelwert.

$$\xi = \sqrt{x_1 x_2}$$

14.2.2 Eine Besonderheit des arithmetischen Mittelwertes

Betrachten wir noch einmal den Fall $n = 2$ und statt der reinen Potenzfunktion eine beliebige quadratische Funktion.

$$f(x) = \alpha x^2 + \beta x + \gamma \quad \alpha, \beta, \gamma \in \mathbb{R}$$

Wegen

$$f'(x) = 2\alpha x + \beta$$

ergibt sich aus dem Mittelwertsatz

$$2\alpha\xi + \beta = \frac{\alpha x_2^2 + \beta x_2 + \gamma - \alpha x_2^2 - \beta x_2 - \gamma}{x_2 - x_1}$$

Das vereinfacht sich zu

$$2\alpha\xi + \beta = \frac{\alpha(x_2^2 - x_1^2) + \beta(x_2 - x_1)}{x_2 - x_1}$$

Hieraus gewinnen wir für $x_2 \neq x_1$

$$2\alpha\xi + \beta = \alpha(x_2 + x_1) + \beta$$

und daraus

$$\xi = \frac{x_2 + x_1}{2}$$

Das bedeutet, dass der arithmetische Mittelwert unabhängig von den Koeffizienten α, β und γ ist, oder anders ausgedrückt:

jede quadratische Funktion liefert denselben Mittelwert.

Leider trifft diese Aussage für andere Potenzen nicht zu.

14.3 Der Mittelwertsatz der Integralrechnung

Der Mittelwertsatz der Integralrechnung lautet

$$\overline{y} = \frac{1}{x_2 - x_1} \int_{x_1}^{x_2} y \, dx$$

Betrachten wir zunächst als Integranden eine beliebige Potenz von x, die ungleich -1 ist..

$$\overline{y} = \frac{1}{x_2 - x_1} \int_{x_1}^{x_2} x^n \, dx$$

Mit den in den vorigen Abschnitten gewonnenen Erkenntnissen ist das

$$\overline{y} = \frac{1}{x_2 - x_1} \cdot \frac{1}{n+1}(x_2^{n+1} - x_1^{n+1}) = \frac{1}{n+1} \cdot \frac{x_2^{n+1} - x_1^{n+1}}{x_2 - x_1} = \frac{G(n+1, x_2, x_1)}{n+1}$$

Dieser Mittelwert ist offenbar ein symmetrisches Polynom in x_1 und x_2. Außerdem wird dieser Wert im Intervall auch angenommen.

$$\overline{y} = \xi^n \quad \xi \in [x_1; x_2]$$

Somit erhalten wir

$$\xi^n = \frac{1}{n+1} \cdot \frac{x_2^{n+1} - x_1^{n+1}}{x_2 - x_1}$$

und daraus

$$\xi = \sqrt[n]{\frac{1}{n+1} \cdot \frac{x_2^{n+1} - x_1^{n+1}}{x_2 - x_1}}$$

Für $n = 1$ erhalten wir den arithmetischen Mittelwert.

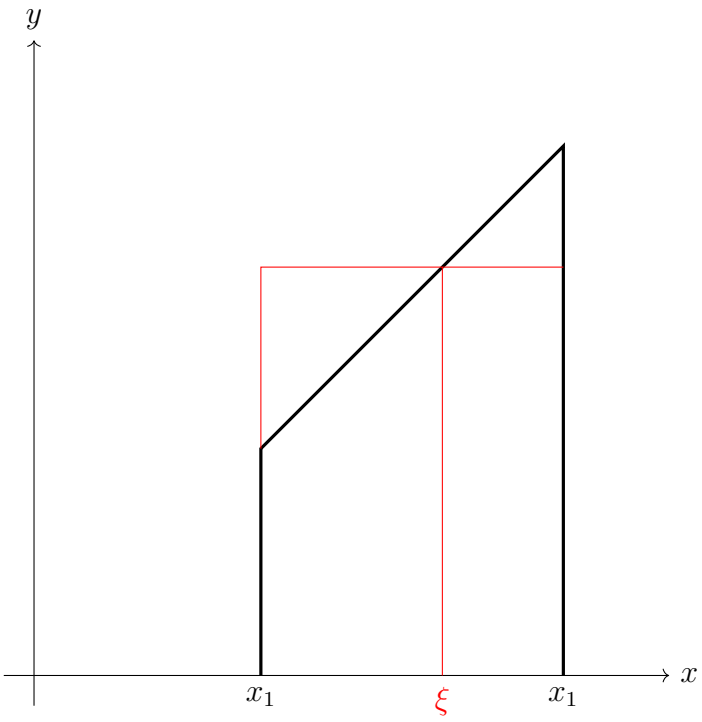
$$\xi = \frac{x_1 + x_2}{2}$$

Für $n = 2$ ergibt sich

$$\xi = \sqrt{\frac{1}{3}(x_1^2 + x_1 x_2 + x_2^2)}$$

Dieser Mittelwert löst das folgende Problem.

Ein rechtwinkliges Trapez rotiert entsprechend der Abbildung um die x-Achse und erzeugt so einen Kegelstumpf. Welchen Radius hat ein Zylinder gleichen Volumens und gleicher Höhe?



Das Rotationsvolumen des Kegelstumpfes erhalten wir mit

$$V_K = 3.141592 \int_{x_1}^{x_2} x^2 \, dx = \frac{3.141592}{3}(x_2^3 - x_1^3)$$

Das Volumen des gesuchten Zylinders ist

$$V_Z = 3.141592\xi^2(x_2 - x_1)$$

Wenn diese beiden Volumina gleich sein sollen, erhalten wir aus dieser Bedingung für ξ den oben erhaltenen Mittelwert für $n = 2$.

$$\xi = \sqrt{\frac{1}{3}(x_1^2 + x_1 x_2 + x_2^2)}$$

Dieser Mittelwert ist, wenn x_1 und x_2 verschieden sind, stets größer als der arithmetische Mittelwert. Zum Beweis gehen wir aus von

$$
\begin{aligned}
0 &\leq (x_1 - x_2)^2 \\
0 &\leq x_1^2 - 2x_1x_2 + x_2^2 \\
3x_1^2 + 6x_1x_2 + 3x_2^2 &\leq 4x_1^2 + 4x_1x_2 + 4x_2^2 \\
\frac{x_1^2 + 2x_1x_2 + x_2^2}{4} &\leq \frac{x_1^2 + x_1x_2 + x_2^2}{3} \\
\frac{x_1 + x_2}{2} &\leq \sqrt{\frac{x_1^2 + x_1x_2 + x_2^2}{3}}
\end{aligned}
$$

und sehen, wie die Behauptung daraus folgt.
Da wir an anderer Stelle schon gesehen haben, dass für n auch negative Werte eingesetzt werden können, betrachten wir noch den Fall $n = -2$.

In diesem Fall geht die Mittelwertformel über in

$$\xi^{-2} = \frac{1}{x_1x_2}$$

Daraus folgt

$$\xi = \sqrt{x_1x_2}$$

Das ist der bekannte geometrische Mittelwert.

Damit haben wir eine Verallgemeinerung des arithmetischen Mittelwertes gefunden. Diese lässt sich aber weiter verallgemeinern, denn für jedes Polynom in x als Integrand liefert der Mittelwertsatz ein symmetrisches Polynom.

15 Primzahlen

Eine sehr schöne weitere Anwendung findet der Quotient

$$m = \frac{a^n - 1}{a - 1} = G(n, a, 1)$$

in der Zahlentheorie.

15.1 Nur primes n kann primes m erzeugen

Zunächst definieren wir die Menge $\mathbb{N}_2$.

$$\mathbb{N}_2 = \mathbb{N} \setminus \{1\}$$

Mit $\mathbb{P}$ bezeichnen wir die Menge aller Primzahlen. Als Primalität bezeichnen wir die Eigenschaft einer natürlichen Zahl, Primzahl zu sein.
Die im obigen Quotienten vorkommenden Parameter a und n sollen Elemente aus $\mathbb{N}_2$ sein. Man sieht sofort, dass m ebenfalls aus $\mathbb{N}_2$ ist.
Es stellt sich nun die Frage, ob dieser Quotient Primzahlen liefern kann. Wenn m Primzahl sein soll, dann muss bereits n Primzahl sein. Der Beweis erfolgt indirekt. Wir zeigen, dass m nicht prim sein kann, wenn n es nicht ist. Wenn n nicht prim ist, dann kann es als Produkt zweier Elemente j, k von $\mathbb{N}_2$ geschrieben werden.

$$m = \frac{a^{j \cdot k} - 1}{a - 1} = \frac{(a^j)^k - 1}{a - 1} = \frac{(a^j)^k - 1}{a^j - 1} \cdot \frac{a^j - 1}{a - 1}$$

Ganz rechts stehen zwei Faktoren aus $\mathbb{N}_2$, weshalb m nicht prim sein kann.
Beispiele:

$$m = \frac{2^6-1}{2-1} = \frac{63}{1} = 7 \cdot 9 \quad \notin \mathbb{P}$$

$$m = \frac{2^5-1}{2-1} = \frac{31}{1} = 31 \quad \in \mathbb{P}$$

15.2 Mersenne-Zahlen und vollkommene Zahlen

Wenn $a = 2$ ist, dann hat der Nenner des Geometrischen Quotienten den Wert 1, so dass er auch weggelassen werden kann. Wenn n eine Primzahl ist, dann nennt man die so entstandene Zahl

$$M_p = 2^p - 1 \quad p \in \mathbb{P}$$

oder anders ausgedrückt

$$M_p = G(p, 2, 1)$$

eine Mersenne-Zahl.
Schon Mersenne selbst (17.Jhd) wusste, dass manche dieser Zahlen Primzahlen sind, andere wiederum nicht. $M_2 = 3$, $M_3 = 7$, $M_5 = 31$ und $M_7 = 127$ sind prim, $M_{11} = 2047 = 23 \cdot 89$ dagegen ist nicht prim.
Es gibt einen interessanten Zusammenhang zwischen den Mersenne-Zahlen und den vollkommenen Zahlen. Vollkommen nennt man eine Zahl, wenn sie mit der Summe ihrer Teiler übereinstimmt, wobei sie selbst als Teiler nicht mitgerechnet wird. Beispiele

$$6=1+2+3$$

$$28=1+2+4+7+14$$

$$496=1+2+4+8+16+31+62+124+248$$

Die vollkommenen Zahlen kommen schon bei Euklid vor (Elemente Buch IX, Satz 36). Er zeigte, dass, wenn q und $2^q - 1$ prim sind, $2^{q-1}(2^q - 1)$ vollkommen ist. Daran erkennt man, dass alle so gefundenen vollkommenen Zahlen gerade sind. Die Frage, ob es ungerade vollkommene Zahlen gibt, ist ungelöst. Von Euler gibt es einen Beweis für die Umkehrung des Euklidischen Satzes, so dass jeder primen Mersenne-Zahl eine vollkommene gerade Zahl entspricht und umgekehrt jeder vollkommenen geraden Zahl eine prime Mersenne-Zahl.

15.3 Test auf Primalität

Da nun leider nicht jedes $p \in \mathbb{P}$ automatisch eine Primzahl liefert, muss das Ergebnis auf Primalität getestet werden. Dazu gibt es ein Iterationsverfahren von Lukas, mit dem Mersenne-Zahlen getestet werden können. Daher sind auch bis jetzt alle bekannten, sehr großen Primzahlen Mersenne-Zahlen.
Unter http://www.mersenne.org findet sich im Internet eine Plattform zur Suche nach primen Mersenne-Zahlen. An dieser Suche kann sich jedermann beteiligen. Zur Zeit (im Jahr 2006) sind 44 Mersenne-Primzahlen bekannt, die größte hat etwas weniger als 10 Millionen Dezimalstellen. Die nächste dürfte die 10 Millionen-Stellen-Grenze überschreiten, womit ein Preis von $100000 fällig wird. Einzelheiten finden sich auf der genannten Website.

15.4 Es gibt keine größte Primzahl

Die Jagd nach immer größeren Primzahlen wäre ziemlich unwitzig, wenn es eine größte Primzahl gäbe. Man weiß jedoch, dass es unendlich viele Primzahlen gibt. Einen Beweis dafür liefern die Mersenne-Zahlen selbst. Zunächst ist klar, dass $M_p > p$ ist. Das brauchen wir noch nicht einmal zu beweisen, denn es gilt allgemeiner:
Jeder Primteiler q von M_p ist größer als p. Es gilt dann nämlich

$$2^p - 1 \mod 0q$$

und damit

$$2^p \mod 1q$$

Da p Primzahl ist, bilden die Restklassen von p einen Körper $\mathbb{F}_p$, in dessen multiplikativer Gruppe
$mathbbF_p \setminus \{0\}$ die 2, wie oben gesehen, die Ordnung p hat. Nach dem Satz von Lagrange teilt diese Ordnung die Ordnung der Gruppe, welche $q - 1$ ist, und

$$p \mid q - 1 \Rightarrow p < q$$

Wenn wir also annehmen, dass es eine größte Primzahl p gibt, dann können wir mit Hilfe der Mersenne-Zahl M_p die Existenz einer noch größeren Primzahl nachweisen, was einen offensichtlichen Widerspruch ergibt. Es kann also, wie allgemein bekannt, keine größte Primzahl geben und die Jagd kann weitergehen.

15.5 Der Beweis von Kummer

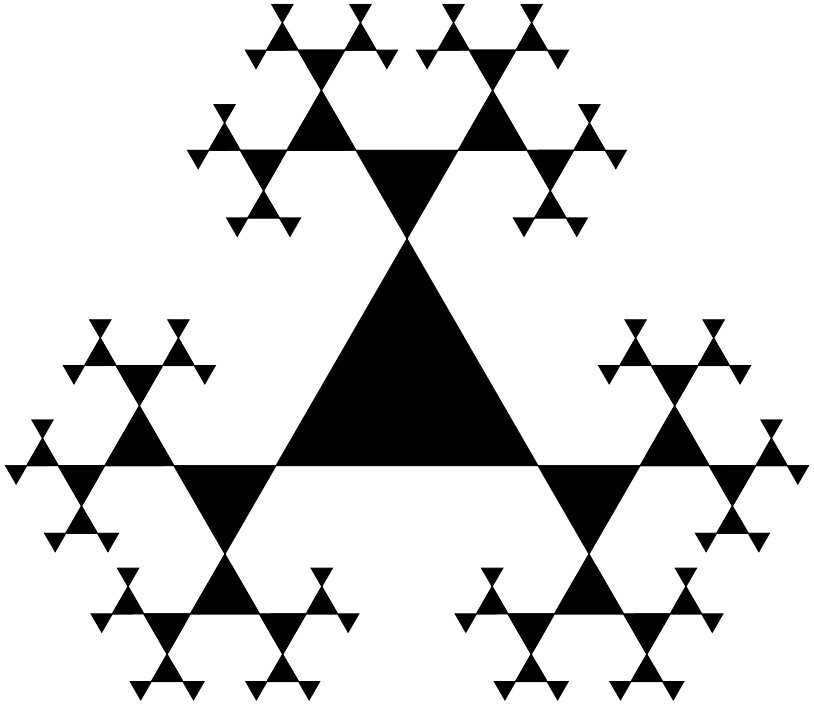
Obwohl es nicht direkt mit unserem Quotienten zu tun hat, möchte ich an dieser Stelle ein mathematisches Kleinod vorstellen.
Schon bei Euklid finden wir als Argument für einen Widerspruchsbeweis, dass man, wenn es nur endlich viele Primzahlen gibt, deren Produkt bilden kann. Nennen wir es PaP, Produkt aller Primzahlen.
Natürlich kommt jetzt das Inkrement: was ist mit $PaP + 1$?
Das kann ja keine Primzahl sein, dazu ist es zu groß. Also muss es Teiler haben. Die stecken jedoch auch in PaP. Das Distributivgesetz verlangt aber, dass ein gemeinsamer Teiler von Minuend und Subtrahend auch die Differenz teilt.
Da die Differenz jedoch 1 ist, geht das nicht, und wir haben den gewünschten Widerspruch.

16 Der Goldene Schnitt

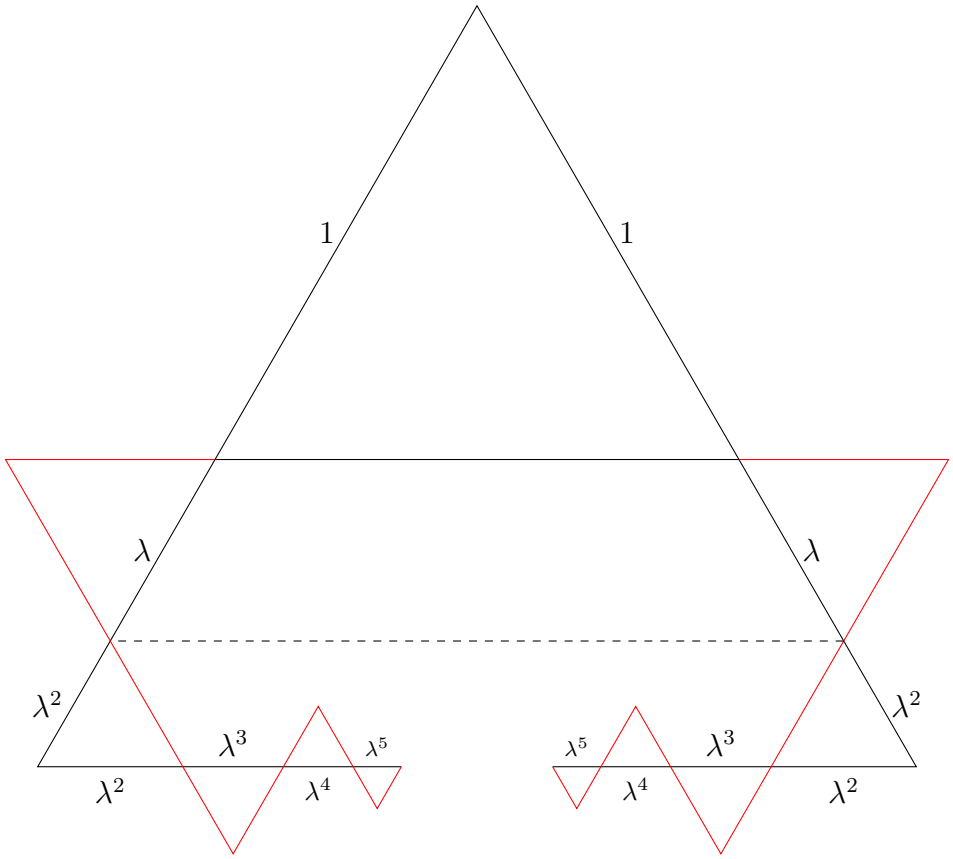
Die geometrische Reihe führt uns, wie wir gleich sehen werden, auch zum Goldenen Schnitt. Die Verbindung ergibt sich dadurch, dass die geometrische Reihe ein Konvergenzintervall hat. An zwei Beispielen soll das gezeigt werden.

16.1 Goldene Fraktale

Wir betrachten eine einfache geometrische Figur, nämlich ein gleichseitiges Dreieck, welches in die euklidische Ebene eingebettet ist. Daraus konstruieren wir eine Füllung der Ebene, indem wir an den Ecken dieses Dreiecks durch Punktspiegelung und gleichzeitige Verkleinerung neue gleichseitige Dreiecke anfügen.
Bezeichnen wir den Verkleinerungsfaktor mit λ und setzen wir $\lambda = \frac{1}{2}$, so ergibt sich eine sehr „luftige“ Füllung, wie die folgende Abbildung zeigt.



Daher ist es naheliegend, einen Verkleinerungsfaktor zu wählen, der eine dichtere Füllung ergibt. Dieser müßte offenbar größer als $\frac{1}{2}$ sein. Wenn er zu groß ist, sind jedoch Überschneidungen zu befürchten. Dadurch ergibt sich die Frage, bei welchem Wert für λ haben wir die größte Dichte ohne Überschneidungen.



Die gestrichelte Linie zeigt folgende Gleichheit.

$$1 + \lambda = \lambda^2 + 2\lambda^3 + 2\lambda^4 + 2\lambda^5 + \cdots$$

Durch Faktorisieren erhalten wir

$$1 + \lambda = \lambda^2 + 2\lambda^3(1 + \lambda + \lambda^2 + \cdots)$$

Der Term in der Klammer ist die wohlbekannte Geometrische Reihe. Diese konvergiert wegen $\lambda < 1$ und wir erhalten

$$1 + \lambda = \lambda^2 + 2\lambda^3 \cdot G(\infty, 1, \lambda) = \lambda^2 + 2\lambda^3 \frac{1}{1 - \lambda}$$

Das entspricht der kubischen Gleichung

$$\lambda^3 + 2\lambda^2 - 1 = 0$$

Da die Koeffizientensumme nicht verschwindet, kommt als Teiler des absoluten Gliedes nur -1 in Frage. Das ist zwar eine Lösung der vorliegenden kubischen Gleichung, jedoch kein zulässiger Wert für λ. Spalten wir den Linearfaktor $\lambda + 1$ ab, so sind die restlichen Lösungen in

$$\lambda^2 + \lambda - 1 = 0$$

zu finden. Die einzige positive Lösung dieser quadratischen Gleichung ist

$$-\frac{1}{2} + \frac{1}{2}\sqrt{5}$$

und stellt das Teilungsverhältnis des Goldenen Schnittes dar.
Da das absolute Glied -1 ist, ist die andere Lösung der negative Kehrwert dieses Teilungsverhältnisses. Folgt man einem weitverbreiteten Brauch, die beiden Verhältnisse des Goldenen Schnittes mit τ und $\frac{1}{\tau}$ zu bezeichnen, wobei τ der Wert ist, der größer als 1 ist, so sind im vorliegenden Fall die Lösungen $-\tau$ und $\frac{1}{\tau}$.
Man kann die Lösung auch noch auf eine andere Weise bekommen, die vielleicht interessanter ist, und die uns in ein weiteres Gebiet der Mathematik führt. Da die quadratische Gleichung als Teilterm $x^2 - 1$ enthält und die 1 wegen nichtverschwindender Koeffizientensumme als Lösung ausscheidet, dividieren wir durch $x - 1$ und erhalten

$$\frac{x^2 - 1}{x - 1} + \frac{x}{x - 1} = 0$$

Umformen der beiden Brüche ergibt

$$x + 1 + \frac{1}{1 - \frac{1}{x}} = 0$$

Damit erhalten wir die Beziehung

$$-x = 1 + \frac{1}{1 + \frac{1}{-x}}$$

Damit haben wir eine Rekursion, die zu einem Kettenbruch führt. Man setzt den ganzen Term der rechten Seite innerhalb dieses Terms für $-x$ ein. Das führt im ersten Schritt zu

$$-x = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{-x}}}}$$

und dann weiter zu

$$-x = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{-x}}}}}$$

Es entsteht offenbar ein unendlicher periodischer Kettenbruch aus lauter Einsen. Das ist der Kettenbruch von τ. Wir haben demnach

$$x = -\tau$$

und damit als zweite Lösung

$$x = \frac{1}{\tau}$$

Bricht man den obigen Kettenbruch ab, so entsteht eine rationale Approximation. Die Folge dieser Approximationen ist

$$\frac{1}{1}, \frac{1}{2}, \frac{2}{3}, \frac{3}{5}, \frac{5}{8}, \frac{8}{13}, \frac{13}{21}, \dots$$

Man sieht, dass sowohl die Zähler als auch die Nenner Fibonacci-Zahlen sind. Es gibt lediglich eine Verschiebung der Zählerfolge um eins nach rechts gegenüber der Nennerfolge.
Die Fibonacci-Zahlen bilden eine rekursive Folge, bei der jedes Folgenglied die Summe der beiden vorangehenden Folgenglieder ist. Man braucht dazu zwei Startwerte, z.B. 1 und 1 und erhält dann die Folge

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, \cdots$$

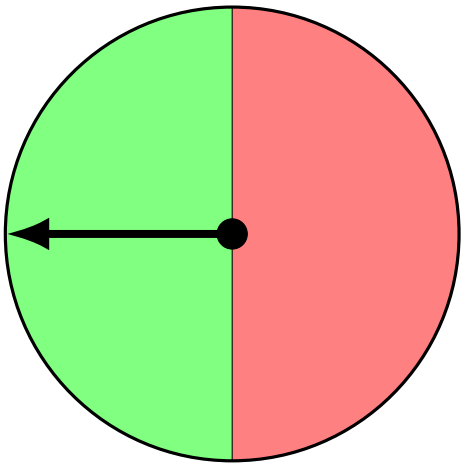
Kehren wir zu unserem Fraktal zurück! Das so entstehende Dreiecksfraktal kann man als Goldenes Fraktal bezeichnen. Nach dem gleichen Rezept erhält man Goldene Fraktale aus anderen Grundfiguren wie Quadrat und Fünfeck. Damit haben wir die Verbindung zum Goldenen Schnitt über die geometrische Reihe gezeigt. Dieser Gedanke lässt sich noch etwas weiter führen, wie später zu sehen sein wird.

16.2 Goldenes Glücksrad

16.3 Goldener Schnitt versus $1:1$

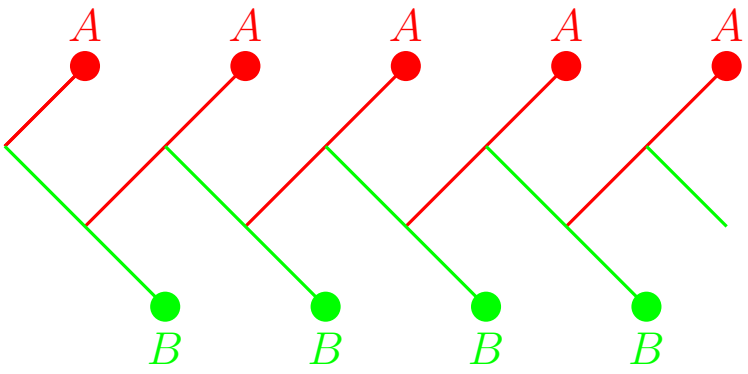
16.3.1 Ein Spiel für zwei Spieler und ein Glücksrad

Zwei Spieler, wir nennen sie A und B, denken sich ein Spiel mit einem Glücksrad aus. Dieses ist eine Drehbare Scheibe. Der Zeiger Z ist fest. Die Spieler drehen abwechselnd die Scheibe. Diese ist in zwei Hälften aufgeteilt, die eine rot gefärbt, die andere grün. Die rote Hälfte gehört zu A, die grüne zu B. Bleibt der Zeiger im roten Feld, wenn A dreht, so hat A gewonnen. Anderenfalls ist B am Zug. Steht der Zeiger dann im grünen Feld, so hat B gewonnen.



16.3.2 Wer anfängt, ist im Vorteil

Nach kurzer Zeit stellen die Spieler fest, dass meistens der gewinnt, der anfängt. Betrachten wir die Situation, wenn A anfängt. Dann ist der Spielverlauf durch den folgenden Baum dargestellt. Jeder Spieler kann nur gewinnen, wenn er am Zug ist.



16.3.3 Berechnung des Vorteils

Damit ergibt sich die Wahrscheinlichkeit P, dass A gewinnt durch

$$P(A\ gewinnt) = \frac{1}{2} + \frac{1}{8} + \frac{1}{32} + \dots$$

oder

$$P(A\ gewinnt) = \sum_{i=1}^{\infty} \frac{1}{2^{2i-1}} = \frac{1}{2} \sum_{i=1}^{\infty} \frac{1}{2^{2i}}$$

Damit haben wir eine unendliche geometrische Reihe.

$$P(A\ gewinnt) = \frac{1}{2} \sum_{i=1}^{\infty} \frac{1}{2^{2i}} = \frac{1}{2} \cdot \frac{1}{1 - \frac{1}{4}}$$

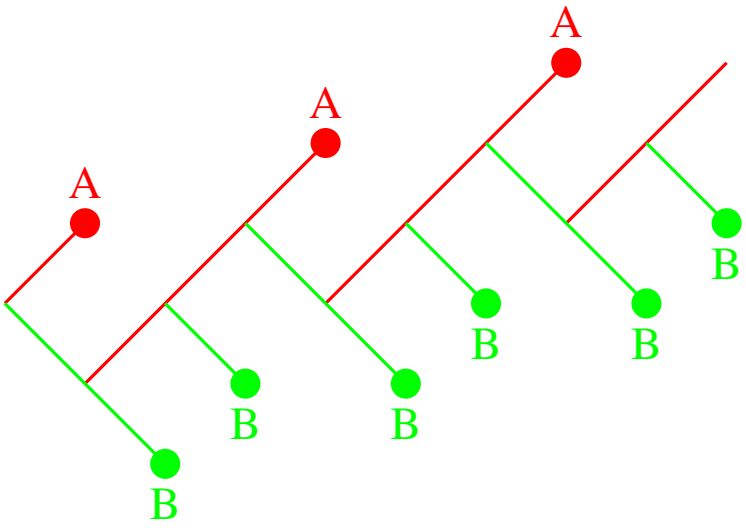
Somit erhalten wir

$$P(A\ gewinnt) = \frac{1}{2} \cdot \frac{1}{1 - \frac{1}{4}} = \frac{2}{3}$$

Damit ist klar, dass das Spiel in dieser Form keinen Spaß macht. Welche Varianten gibt es, die Chancen von B zu verbessern und zu einem Spielverlauf zu kommen, bei dem jeder die gleiche Wahrscheinlichkeit hat, zu gewinnen.

16.3.4 Der Andere darf zweimal drehen

Wir prüfen, ob als Nachteilsausgleich in Frage kommt, den B immer zweimal drehen zu lassen, wenn er dran ist. Dazu betrachten wir den geänderten Ereignisbaum.



16.3.5 Was hat sich geändert?

Wie man sieht, haben sich die Gewinnchancen von A vermindert.

$$P(A\ gewinnt) = \frac{1}{2} + \frac{1}{16} + \frac{1}{128} + \dots$$

oder

$$P(A\ gewinnt) = \sum_{i=1}^{\infty} \frac{1}{2^{3i-2}} = \frac{1}{2} \sum_{i=1}^{\infty} \frac{1}{2^{3i}}$$

In diesem Fall konvergiert die unendliche geometrische Reihe gegen

$$P(A\ gewinnt) = \frac{1}{2} \sum_{i=1}^{\infty} \frac{1}{2^{3i}} = \frac{1}{2} \cdot \frac{1}{1 - (\frac{1}{2})^3}$$

Somit erhalten wir

$$P(A\ gewinnt) = \frac{1}{2} \cdot \frac{1}{1 - \frac{1}{8}} = \frac{4}{7}$$

Dieser Wert ist zwar schon besser als der vorige. Aber trotzdem ist der Spieler A immer noch gegenüber B im Vorteil, da $\frac{4}{7}$ größer ist als $\frac{1}{2}$.

16.3.6 B darf noch öfter hintereinander drehen

Aus dem Vorangegangenen ergibt sich, dass, wenn wir B n mal hintereinander drehen lassen, die Wahrscheinlichkeit so dargestellt werden kann:

$$P(A\ gewinnt) = \frac{1}{2} + \frac{1}{2^{n+1}} + \frac{1}{(2^{n+1})^2} + \dots$$

$$P(A\ gewinnt) = \frac{1}{2} \sum_{i=1}^{\infty} \frac{1}{2^{(n+1)i}} = \frac{1}{2} \cdot \frac{1}{1 - (\frac{1}{2})^{n+1}}$$

Somit erhalten wir

$$P(A\ gewinnt) = \frac{1}{2} \cdot \frac{1}{1 - (\frac{1}{2})^{n+1}} = \frac{2^n}{2^{n+1} - 1}$$

Für wachsendes n konvergiert dieser Ausdruck gegen $\frac{1}{2}$. Das bedeutet, dass B so oft drehen kann, wie er will, ohne je auf die Gewinnwahrscheinlichkeit $\frac{1}{2}$ zu kommen.
Der Ausgleich muss also anders geschaffen werden.
Dazu betrachten wir die Möglichkeit, den Sektor von A auf dem Glücksrad zu verkleinern und den von B entsprechend zu vergrößern.

16.3.7 Der Sektor von A wird verkleinert

Kehren wir wieder zu der Situation zurück, wie sie in Abbildung 1 dargestellt ist. Die Spieler drehen abwechselnd, jedoch sind ihre Sektoren nicht mehr gleich groß. A, der anfängt, hat den kleineren Sektor und damit eine kleinere Wahrscheinlichkeit als 50

$$P(A\ gewinnt) = p + p^2q + p^3q^2 + p^4q^3 \dots$$

Nach Distributivgesetz können wir faktorisieren

$$P(A\ gewinnt) = p(1 + pq + (pq)^2 + (pq)^3 \dots)$$

oder

$$P(A\ gewinnt) = p \sum_{i=0}^{\infty} (pq)^i$$

Womit sich durch Grenzübergang ergibt:

$$P(A\ gewinnt) = p \sum_{i=0}^{\infty} (pq)^i = p \cdot \frac{1}{1 - pq}$$

Beide Spieler haben die gleiche Gewinnchance, wenn dieser Wert gleich $\frac{1}{2}$ ist.

$$p \cdot \frac{1}{1-pq} = \frac{1}{2}$$

Berücksichtigt man, dass $p + q = 1$, so führt diese Bedingung zu einer quadratischen Gleichung.

$$2p = 1 - pq \;\Rightarrow\; p^2 - 3p + 1 = 0$$

16.3.8 Die ideale Aufteilung

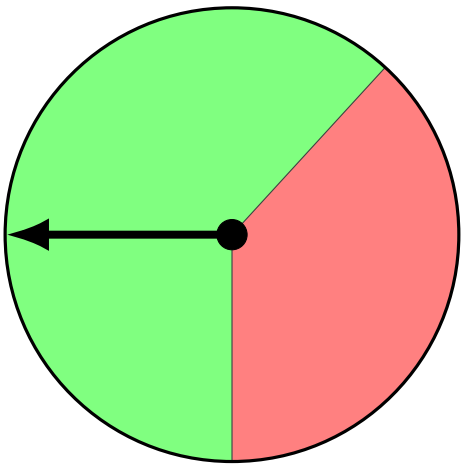
Eine der Lösungen der Gleichung aus dem vorigen Abschnitt ist kleiner als eins, nämlich

$$\frac{3}{2} - \frac{1}{2}\sqrt{5}$$

Das wäre das Maß für den kleineren Sektor. Der größere wäre dementsprechend

$$-\frac{1}{2} + \frac{1}{2}\sqrt{5}$$

Diese beiden Werte erfüllen die Regel des Goldenen Schnitts:
Das Kleine verhält sich zum Großen wie das Große zum Ganzen.
Somit haben wir gefunden, dass die „Goldene Wahrscheinlichkeit“ das Problem löst.



16.3.9 Kombination der beiden Möglichkeiten

Wie gestaltet sich das Spiel, wenn beide Möglichkeiten kombiniert werden? Es ist anzunehmen, dass das Feld von A wieder vergrößert werden muss, wenn B mehr als einmal drehen darf. Betrachten wir den Fall, dass B jedesmal zweimal drehen darf. Wir erhalten dann

$$P(A\ gewinnt) = p + p^3q + p^4q^2 + p^5q^3 \ldots$$

Nach Distributivgesetz können wir faktorisieren

$$P(A\ gewinnt) = p(1 + p^2q + (p^2q)^2 + (p^2q)^3 \ldots)$$

oder

$$P(A\ gewinnt) = p\sum_{i=0}^{\infty}(p^2q)^i$$

Womit sich durch Grenzübergang ergibt:

$$P(A\ gewinnt) = p\sum_{i=0}^{\infty}(p^2q)^i = p \cdot \frac{1}{1-p^2q}$$

Wenn beide Spieler dieselbe Chance haben sollen, ergibt sich

$$p \cdot \frac{1}{1-p^2q} = \frac{1}{2}$$

Die im Intervall $[0;1]$ liegende Lösung ist $p = 0.445$

16.3.10 Der allgemeine Fall

Lässt man den Spieler B n mal drehen, so erhält man

$$p \cdot \frac{1}{1-p^nq} = \frac{1}{2}$$

Wegen

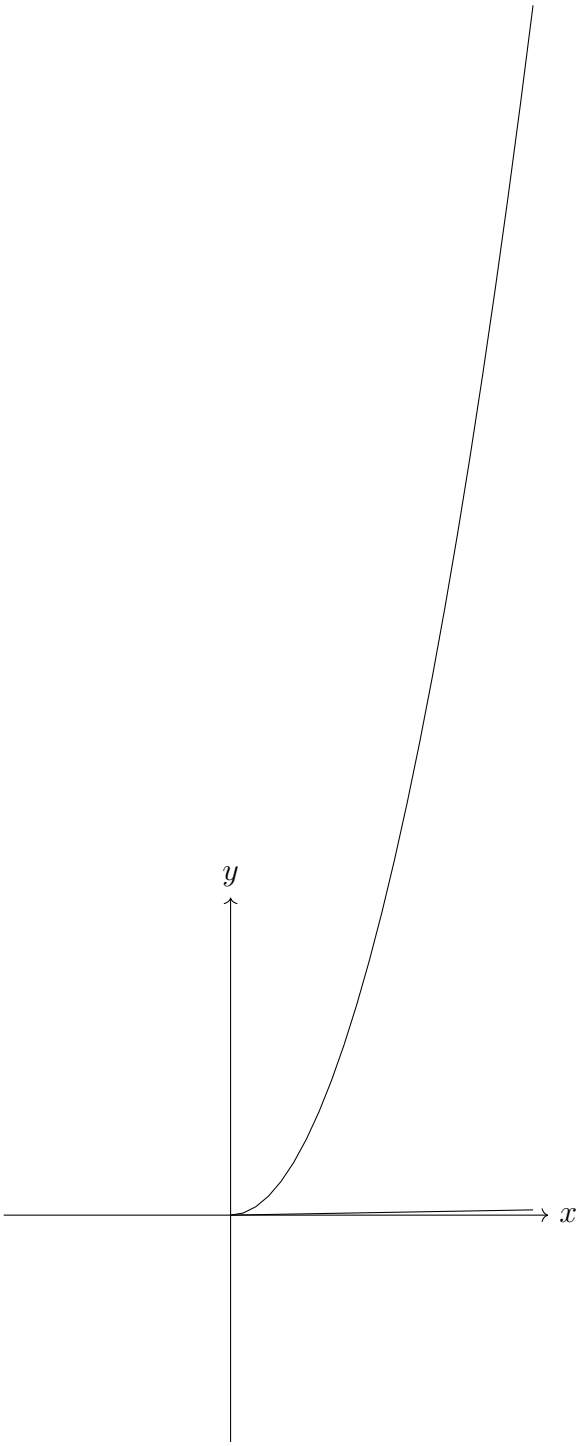
$$\lim_{n\to\infty} p^n = 0$$

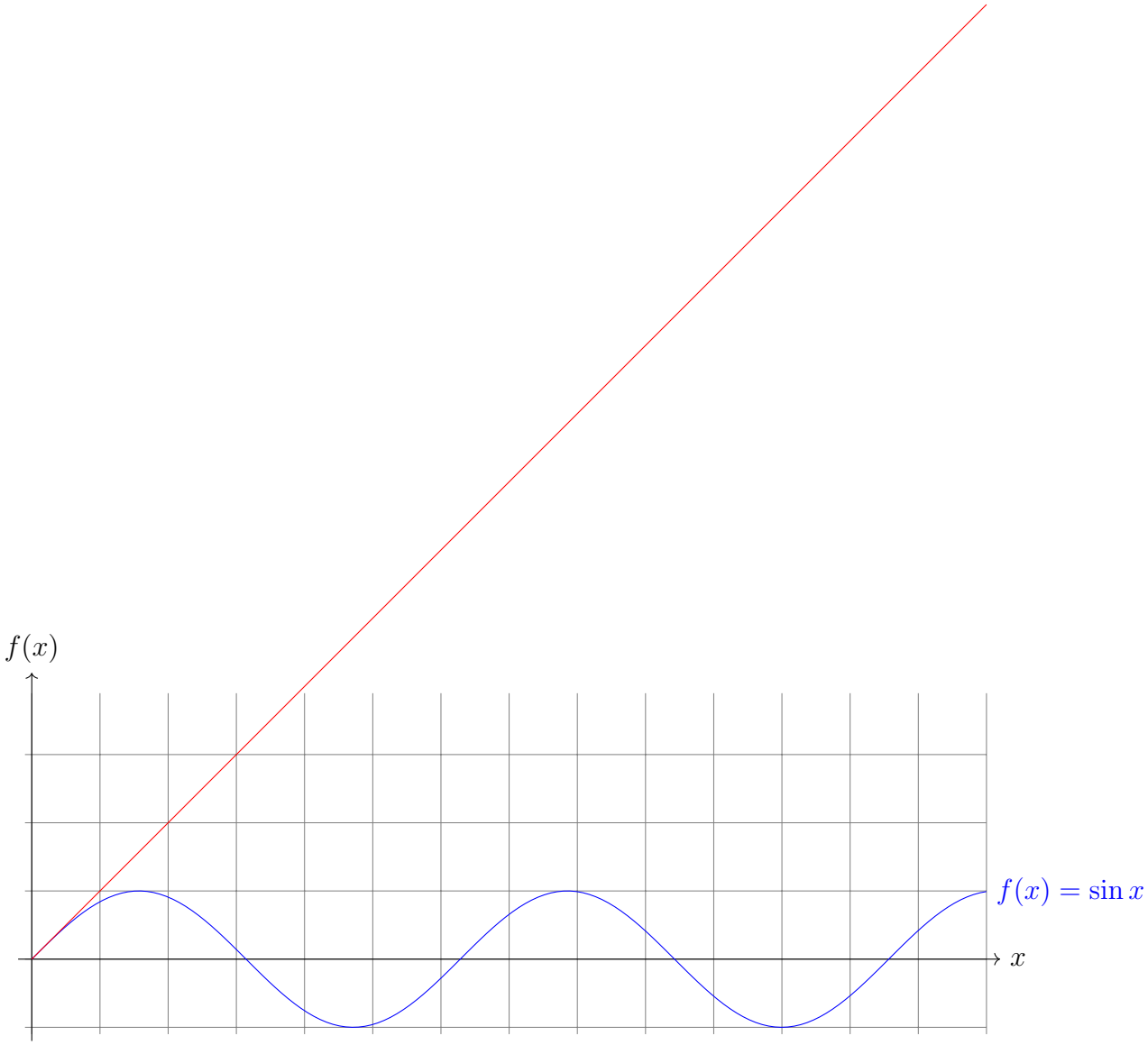
konvergiert die Lösung dieser Gleichung gegen $\frac{1}{2}$.
Wir sehen also auch von dieser Seite, dass die Aufteilung in gleiche Sektoren nur dann Chancengleichheit herstellt, wenn B nur noch alleine drehen darf. Damit haben wir einen Übergang von der Teilung nach dem Goldenen Schnitt zu der Teilung in zwei gleiche Teile.

16.3.11 Goldener Schnitt die bessere Teilung?

Wenn etwas in zwei Teile zu teilen ist, liegt die Teilung in zwei gleiche Teile offenbar am nächsten. So war auch in diesem Fall die Ausgangssituation. Erst wenn sich dieser Ansatz als unbrauchbar erweist, wird Ausschau gehalten nach anderen Möglichkeiten der Aufteilung. Dabei entsteht dann ein kleineres Teil, der sogenannte Minor, und ein größeres Teil, der sogenannte Major. Auffällig häufig löst dann eine Teilung nach der Regel "Minor zu Major wie Major zum Ganzen" das Problem. Wegen dieser Eigenschaft nennt man diese Teilung auch "Goldenen Schnitt".
Es bleibt zu beachten, dass die Teilung in zwei gleiche Teile trotzdem immer noch die erste Wahl ist.
?

17 Taylor




$f(x)$
$f(x) = \sin x$
x