Mathematische Miniaturen

Vorkurs Mathematik 2014, Woche 4

Dr. Michael H. Mertens

September 2014

Inhaltsverzeichnis

Vorwort

Die vorliegenden Seiten dienen als Grundlage für die fünf Vorlesungen, die ich im Rahmen des Mathematik-Vorkurses am Mathematischen Institut der Universität zu Köln im September 2014 gehalten habe. Der Inhalt ist für angehende Mathematik-Studenten vor dem ersten Semester konzipiert und behandelt verschiedene Themen aus unterschiedlichen Teildisziplinen der Mathematik, wie Zahlentheorie, Algebra, Analysis, etc.

Wegen der Kürze der Zeit können wir nicht alle Resultate, die in dieser Vorlesung behandelt werden, aber die Beweise, die vorgestellt werden, sollen so gestaltet sein, dass sie nur mit Schulmathematik und gelegentlich den vorangegangenen Vorkurs-Vorlesungen auskommen. Vereinzelt wird es vorkommen, dass Resultate aus der Analysis I-Vorlesung benötigt werden, diese werden dann auch nur angegeben. Da man das Beweisen nur dadurch lernt, dass man es selbst tut, sind auch einige Beweise in die Übungen ausgelagert.

In der ersten Vorlesung beschäftigen wir uns mit Primzahlen und ihrer Verteilung und geben u.a. 4 verschiedene Beweise dafür, dass es unendlich viele Primzahlen gibt.

Das nächste Thema werden Polynomgleichungen sein. Wir werden als Lösungsverfahren für kubische Gleichungen die Cardano-Formel behandeln und allgemein hilfreiche algebraische Aussagen über Polynome beweisen, wie z.B. das Lemma von Gauss.

In der dritten Vorlesung beschäftigen wir uns mit Irrationalität und beweisen dort u.a. die Irrationalität von e und π.

Auch in praktischen Anwendungen (Routenplaner, Funknetzwerke,...) ist die Graphentheorie sehr wichtig geworden. In der vierten Vorlesung geben wir eine Einführung und geben einige schöne Resultate an, z.B. die Charakterisierung Eulerscher Graphen, die Eulersche Polyederformel und die Klassifikation der Platonischen Körper.

Zum Abschluss betrachten wir in der letzten Vorlesung die allgemeine harmonische Reihe, die Ihnen später auch in der Analysis I wieder begegnen wird.

Hinweis: Diese Notizen sind trotz eifriger Bemühung vermutlich nicht frei von Tippfehlern u.ä. Korrekturen per E-Mail (`mmertens@math.uni-koeln.de`) sind gerne willkommen.

Köln, im September 2014, Michael H. Mertens

Kapitel 1

Primzahlen und ihre Verteilung

Literaturempfehlung Eine Darstellung zu Abschnitt 1.1 findet sich in jedem Lehrbuch zur elementaren Zahlentheorie, z.B. [RU95]. Eine besonders einfache kann man in Kapitel 2 von [BBC00] finden. Die Beweise aus Abschnitt 1.2 und Abschnitt 1.3 stammen aus den Kapiteln 1 und 2 von [AZ10]. Für einen Beweis des Primzahlsatzes aus Abschnitt 1.4 gibt es leider keine einfache Darstellung, die ohne Analysis oder Funktionentheorie auskommt. Eine Darstellung der Geschichte des Satzes findet man in [RU95].

1.1 Der Fundamentalsatz der Arithmetik

Die Definition einer Primzahl ist sicher hinlänglich bekannt, dennoch möchte ich mit ihr beginnen.

Definition 1.1. *Eine natürliche Zahl $p \in \mathbb{N}$,$p \geq 2$, heißt* Primzahl*, wenn sie außer* 1 *und sich selbst keine (positiven) Teiler besitzt. Falls p andere Teiler besitzt, so heißt p* zusammengesetzt*. Die Menge der Primzahlen bezeichnen wir mit $\mathbb{P}$.*

Unmittelbar hieraus können wir schon eine abgeschwächte Form des Fundamentalsatzes der Arithmetik beweisen, die für das weitere Vorgehen ausreicht.

Satz 1.2. *Jede natürliche Zahl $n \geq 2$ besitzt eine Primfaktorzerlegung*

$$n = p_1^{\nu_1} p_2^{\nu_2} \cdots p_\ell^{\nu_\ell}, \qquad p_1, \ldots, p_\ell \in \mathbb{P},\ \nu_1, \ldots, \nu_\ell \in \mathbb{N}.$$

Beweis. Wir beweisen diesen Satz mittels vollständiger Induktion. Der Induktionsanfang ist leicht, da 2 bereits eine Primzahl ist. Nehmen wir nun an, dass für ein $n \geq 3$ jede Zahl $m < n$ eine Primfaktorzerlegung besitzt. Ist n selbst prim, so sind wir fertig, denn $n = n$ ist eine Primfaktorzerlegung. Ansonsten ist n zusammengesetzt, d.h. es gibt $2 \leq a, b < n$ mit $a \cdot b = n$. Nach Induktionsvoraussetzung haben sowohl a als auch b Primfaktorzerlegungen, sagen wir

$$a = p_1^{a_1} \cdots p_\ell^{a_\ell} \quad \text{und} \quad b = q_1^{b_1} \cdots q_r^{b_r}$$

mit $p_1, \ldots, p_\ell, q_1, \ldots, q_r \in \mathbb{P}$ und $a_1, \ldots, a_\ell, b_1, \ldots, b_r \in \mathbb{N}$. Dann ist aber

$$n = p_1^{a_1} \cdots p_\ell^{a_\ell} \cdot q_1^{b_1} \cdots q_r^{b_r}$$

eine Primfaktorzerlegung von n und die Behauptung folgt nach dem Prinzip der vollständigen Induktion. □

Primzahlen sind also gewissermaßen die Bausteine der natürlichen Zahlen. Es gilt sogar eine stärkere Aussage, der *Fundamentalsatz der Arithmetik*.

Satz 1.3. *Die Primfaktorzerlegung einer natürlichen Zahl $n \geq 2$ ist bis auf Reihenfolge der Faktoren eindeutig.*

Der Beweis hierfür ist zwar nicht kompliziert, nimmt aber viel Zeit in Anspruch, so dass wir ihn hier auslassen.

1.2 Die Unendlichkeit der Primzahlen

In diesem Abschnitt geben wir insgesamt 4 Beweise für folgenden Satz.

Satz 1.4. *Die Menge $\mathbb{P}$ der Primzahlen ist unendlich.*

Zunächst ist dies überhaupt nicht klar, da Primzahlen im Verlauf der Zahlenreihe immer seltener zu werden scheinen und vor allem, da es (bis heute) unmöglich ist für jedes $n \in \mathbb{N}$ die $n$te Primzahl zu konstruieren. Dennoch lässt sich unser Satz im Wesentlichen nur aus Satz 1.2 folgern.

Unser erster Beweis geht auf Euklid zurück und ist vermutlich historisch der älteste.

1. Beweis. Seien $p_1, \ldots, p_n$ irgendwelche Primzahlen. Dann betrachten wir die natürliche Zahl

$$N = p_1 \cdots p_n + 1. \tag{1.1}$$

Diese ist durch keine der Primzahlen $p_1, ..., p_n$ teilbar (sie lässt immer den Rest 1 bei der Division durch p_j, $j = 1, \ldots, n$), hat aber nach Satz 1.2 eine Primfaktorzerlegung, so dass es noch wenigstens eine Primzahl geben muss, die nicht in der endlichen Liste $(p_1, ..., p_n)$ vorkommt. Also ist $\mathbb{P}$ unendlich. □

Euklids Beweis ist insofern von besonderer Genialität, dass er das Problem „die“nächste Primzahl zu konstruieren ignoriert und stattdessen nur *eine* weitere konstruiert.

Bemerkung 1.5. *Es ist bis heute nicht bekannt, ob* Euklids *Vorgehen tatsächlich* alle *Primzahlen liefert. Beginnt man z.B. mit der Primzahl* 2 *und bildet dann sukzessive die Zahl N aus allen gefundenen Primzahlen und fügt ihren kleinsten Primfaktor zur Liste der Primzahlen hinzu, so erhält man folgende Primzahlen,*

$$2, 3, 7, 43, 13, 53, 5, 6221671, 38709183810571, 139, 2801, 11, 17, ...$$

Diese Folge nennt man die Euklid-Mullin-*Folge. Die ersten* 51 *Glieder der Folge sind bekannt, die kleinste Primzahl, die in der Folge bisher nicht auftaucht, ist* 41.

Unser zweiter Beweis stammt von C. GOLDBACH. Er verwendet eine schöne Rekursion für FERMAT-Zahlen

$$F_n := 2^{2^n} + 1, \qquad n \in \mathbb{N}_0. \tag{1.2}$$

Lemma 1.6. *Für jedes $n \in \mathbb{N}$ gilt*

$$\prod_{k=0}^{n-1} F_k = F_n - 2.$$

Der Beweis lässt sich mit vollständiger Induktion führen. Ich verweise dazu auf die Übung.

2. Beweis. Wir zeigen, dass je zwei FERMAT-Zahlen teilerfremd sind, also keine gemeinsamen Primfaktoren besitzen. Das heißt, für jedes $n \in \mathbb{N}$ gibt es eine Primzahl $p \in \mathbb{P}$ mit $p \mid F_n$, aber $p \nmid F_k$ für $k < n$, so dass die Unendlichkeit von $\mathbb{P}$ folgt. Nun zum Beweis der Teilerfremdheit. Aus Lemma 1.6 folgt, dass ein gemeinsamer Teiler d von F_k und F_n $(k < n)$ auch die Zahl 2 teilen muss, also gilt $d \in \{1, 2\}$. Da FERMAT-Zahlen ungerade sind, ist $d = 2$ ausgeschlossen und somit die Behauptung bewiesen. □

Der nächste Beweis erfordert ein weiteres Resultat als Vorbereitung, dass aber auch für sich genommen wichtig ist, den Satz von LAGRANGE aus der Gruppentheorie. Der Vollständigkeit halber erwähnen wir zuvor die Definition einer Gruppe.

Definition 1.7. *Eine Menge G mit einer Abbildung* (Multiplikation)

$$\cdot : G \times G \to G$$

heißt eine Gruppe*, wenn*

(i) für alle $g, h, k \in G$ gilt, dass $(g \cdot h) \cdot k = g \cdot (h \cdot k)$ (Assoziativität)*,*

(ii) es ein Element $1 \in G$ gibt mit $1 \cdot g = g \cdot 1 = g$ für alle $g \in G$ (Existenz der 1)*,*

(iii) für alle $g \in G$ ein $h \in G$ existiert mit $g \cdot h = 1$ (Existenz inverser Elemente)*.*

Eine Teilmenge U von G heißt eine Untergruppe *von G, in Zeichen $U \leq G$, wenn U bezüglich $\cdot$ ebenfalls eine Gruppe ist.*

Man beachte, dass 1 in der obigen Definition lediglich als Symbol gebraucht wird und nicht unbedingt etwas mit der natürlichen Zahl 1 zu tun haben muss. Ebenso ist die Multiplikation als abstrakte Abbildung zu verstehen.

Der Satz von LAGRANGE besagt nun Folgendes.

Satz 1.8. *Sei G eine endliche Gruppe und $U \leq G$, dann ist $|U|$ ein Teiler von $|G|$, wobei $|M|$ die Anzahl der Elemente einer endlichen Menge M bezeichne. Insbesondere teilt die* Ordnung *von $g \in G$ bezeichnet mit* $\operatorname{ord}(g) := |\{g^n | n \in \mathbb{N}\}|$ *die Gruppenordnung $|G|$.*

Beweis. Wir betrachten die Relation

$$g \sim h \;\Leftrightarrow\; gh^{-1} \in U.$$

Aus den Gruppenaxiomen folgt, dass $\sim$ eine Äquivalenzrelation auf G ist, die Äquivalenzklassen sind von der Form $Ua = \{xa \mid x \in U\}$ mit $a \in G$. Offensichtlich haben alle diese Äquivalenzklassen die Mächtigkeit $|U|$. Da sich verschiedene Äquivalenzklassen nicht schneiden und sicherlich $G = \bigcup_{a\in G} Ua$ gilt folgt also, dass $|G|$ durch $|U|$ teilbar ist, wobei der Quotient die Anzahl der verschiedenen Äquivalenzklassen ist.

Wir müssen nun für den zweiten Teil des Satzes noch zeigen, dass für jedes $g \in G$ die (offensichtlich endliche) Menge $C := \{g^n | n \in \mathbb{N}_0\}$ eine Untergruppe von G bildet. Offenbar ist $1 = g^0 \in C$ und Produkte von Elementen in C liegen wieder in C. Da C endlich ist, muss es ein $m \in \mathbb{N}$ geben mit $g^m = 1$, womit für $k \leq m$ die Gleichung $g^{-k} = g^{m-k} \in C$ haben, was wir zeigen wollten. □

Unser dritter Beweis verwendet nun die sogenannten MERSENNE-Zahlen ,

$$M_p := 2^p - 1, \qquad p \in \mathbb{P}. \tag{1.3}$$

3. Beweis. Für jedes $p \in \mathbb{P}$ muss die Zahl M_p einen Primteiler q besitzen. Wir zeigen, dass $q > p$ gelten muss, woraus wieder die Unendlichkeit von $\mathbb{P}$ folgt. Wir verwenden für den Beweis Kongruenzen. Da $q \mid M_p$ folgt die Kongruenz $2^p \equiv 1 \pmod q$, also hat 2 in der Gruppe $G = (\mathbb{Z}/q\mathbb{Z}) \setminus \{0\}$ die Ordnung p, da p eine Primzahl ist. Die Ordnung von G ist $q - 1$, also folgt mit dem Satz von LAGRANGE, dass $p \mid (q - 1)$ gilt, also insbesondere $p < q$, was wir zeigen wollten. □

Unser vierter Beweis ist verglichen mit den bisherigen relativ neu und stammt von H. FÜRSTENBERG aus dem Jahr 1955. Er verwendet die Sprache der *Topologie*. Wir erläutern zunächst die wichtigsten Grundbegriffe.

Definition 1.9. *Sei X eine beliebige Menge. Eine Teilmenge $\mathcal{T} \subseteq \mathfrak{Pot}(X)$ der Potenzmenge von X heißt eine* Topologie*, falls folgende Bedingungen erfüllt sind.*

1. *$X \in \mathcal{T}$ und $\emptyset \in \mathcal{T}$.*
2. *Für beliebig viele (auch unendlich viele) Mengen $T_i \in \mathcal{T}$, $i \in I$, wo I eine beliebige Indexmenge ist, ist die Vereinigung $\bigcup_{i\in I} T_i$ in $\mathcal{T}$ enthalten.*
3. *Für endlich viele Mengen $T_1, ..., T_n \in \mathcal{T}$ ist ihr Durchschnitt $\bigcap_{i=1}^n T_i$ in $\mathcal{T}$ enthalten.*

Die Elemente einer Topologie heißen offene Mengen*, das Komplement $X \setminus T$ einer offenen Menge T heißt* abgeschlossen*.*

Bemerkung 1.10. *Es ist leicht aus der Definition zu sehen, dass beliebige Schnitte und endliche Vereinigungen abgeschlossener Mengen wieder abgeschlossen sind.*

Bemerkung 1.11. *Ein Wort der Warnung: die Begriffe offen und abgeschlossen sind im Allgemeinen weder auf alle Teilmengen anwendbar (d.h. normalerweise gibt es Mengen, die weder offen noch abgeschlossen sind), noch schließen sie sich gegenseitig aus. Die leere Menge ist beispielsweise stets sowohl offen als auch abgeschlossen.*

Beispiel 1.12. *Damit man sich unter diesem abstrakten Begriff etwas vorstellen kann, geben wir ein Standardbeispiel, dass Ihnen in der Vorlesung Analysis I ausführlicher wieder begegnen wird.*

Sei $X = \mathbb{R}$. Wir nennen eine Menge $T \subseteq \mathbb{R}$ offen, wenn für die die folgende Aussage gilt:

$$\forall x \in T \ \exists \varepsilon > 0 \ :]x - \varepsilon, x + \varepsilon[\subseteq T.$$

Dann ist die Menge $\mathcal{T} = \{T \subseteq \mathbb{R} \ : \ T \text{ offen}\}$ eine Topologie auf $\mathbb{R}$.

Kommen wir nun zu unserem vierten und letzten Beweis von Satz 1.4.

4. Beweis. Wir definieren für $a, b \in \mathbb{Z}$ mit $b > 0$ die Menge

$$N_{a,b} = \{a + nb \ : \ n \in \mathbb{Z}\}$$

und nennen eine Menge $T \subseteq \mathbb{Z}$ offen, wenn sie entweder leer ist oder zu jedem $a \in T$ ein $b \in \mathbb{N}$ existiert mit $N_{a,b} \subseteq T$. Damit ist klar, dass beliebige Vereinigungen offener Mengen wieder offen sind. Weiter gilt für nach dieser Defintion offene Mengen $T_1, T_2 \subseteq \mathbb{Z}$, dass für jedes $a \in T_1 \cap T_2$ ein $b_1 \in T_1$ (bzw. $b_2 \in T_2$) existiert mit $N_{a,b_1} \subseteq T_1$ (bzw. $N_{a,b_2} \subseteq T_2$), so dass $N_{a,b_1 b_2} \subseteq T_1 \cap T_2$ gilt. Damit ist der Durchschnitt endlich vieler offener Mengen wieder offen, so dass die Menge $\mathcal{T}$ aller offenen Mengen eine Topologie auf $\mathbb{Z}$ ist.

Es gilt offenbar, dass jede nicht-leere offene Menge unendlich ist (denn sie muss eine unendliche Menge $N_{a,b}$ enthalten). Außerdem sehen wir, dass sich jede Menge $N_{a,b}$ schreiben lässt als

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b},$$

also als Komplement einer offenen Menge. Dadurch ist $N_{a,b}$ auch abgeschlossen, vgl. Bemerkung 1.11.

Nach dieser Vorbereitung kommen wir nun zu den Primzahlen. Nach Satz 1.2 besitzt jede ganze Zahl $n \neq \pm 1$ einen Primteiler p, ist also in $N_{0,p}$ enthalten. Daher gilt

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Nehmen wir nun an, $\mathbb{P}$ wäre endlich, dann wäre $\bigcup_{p \in \mathbb{P}} N_{0,p}$ als endliche Vereinigung abgeschlossener Mengen abgeschlossen, also auch $\mathbb{Z} \setminus \{-1, 1\}$. Das würde aber bedeuten, dass $\{-1, 1\}$ offen ist, was aber nicht sein kann, da alle nicht-leeren offenen Mengen unendlich sind. Das ist ein Widerspruch, also kann unsere Annahme, dass $\mathbb{P}$ endlich ist nicht richtig gewesen sein, was Satz 1.4 beweist. □

1.3 Das Bertrandsche Postulat

Wir haben uns inzwischen hinlänglich davon überzeugt, dass es unendlich viele Primzahlen gibt. Über ihre Verteilung können wir damit aber noch lange nichts sagen. Mit Euklids Beweismethode können wir dazu sofort folgendes bemerken.

Bemerkung 1.13. *Für jedes $k \in \mathbb{N}$ gibt es k aufeinanderfolgende Zahlen, von denen keine eine Primzahl ist. Anders ausgedrückt gibt es beliebig große Lücken in der Primzahlreihe.*

Beweis. Seien $2, 3, ..., p$ die Primzahlen, die kleiner sind als $k+2$ und $N := 2 \cdot 3 \cdots p$, dann ist jede der k Zahlen

$$N+2,\ N+3,\ ..., N+(k+1)$$

durch mindestens eine Primzahl teilbar, die kleiner ist als $k+2$, also selbst keine Primzahl. □

Andererseits gilt aber das sogenannte Bertrandsche Postulat.

Satz 1.14. *Für jedes $n \geq 1$ gibt es mindestens eine Primzahl $p \in \mathbb{P}$ mit $n < p \leq 2n$.*

Bertrand selbst hat dies nicht bewiesen, aber immerhin (von Hand!) bis $n = 3\,000\,000$ verifiziert, der erste Beweis stammt von Tschebyschew. Ein sehr eleganter Beweis geht auf P. Erdős erste Arbeit aus dem Jahr 1932 zurück, ist aber leider etwas zu umfangreich, um ihn hier vorzustellen.

Wir begnügen uns mit dem folgenden Lemma.

Lemma 1.15. *Das Bertrandsche Postulat ist für $n \leq 4000$ korrekt.*

Beweis. Wir prüfen hierfür nicht 4000 Fälle einzeln nach. Wir bemerken stattdessen, dass

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 631,\ 1259,\ 2503,\ 4001$$

eine Liste von Primzahlen ist, bei der jedes Element weniger als doppelt so groß ist wie sein Vorgänger. Also enthält jede Menge $\{y \in \mathbb{N} \ :\ n < y \leq 2n\}$ für $n \leq 4000$ eine dieser 14 Primzahlen. □

1.4 Der Primzahlsatz

In diesem Abschnitt wollen wir lediglich einige Fakten zusammentragen, den Primzahlsatz formulieren und ein paar Daten präsentieren, die seine Richtigkeit einleuchtend erscheinen lassen.

Die Größe, die uns nun interessieren wird ist die folgende Funktion, die wir für reelle Zahlen $x \geq 0$ erklären durch

$$\pi(x) := |\{p \in \mathbb{P} \ :\ p \leq x\}|.$$

Im Jahre 1792 bzw. 1798 vermuteten C.F. Gauss und A.-M. Legendre unabhängig voneinander eine Beziehung zwischen dieser Funktion und der Funktion $x \mapsto \frac{x}{\log x}$, nämlich dass sie *asymptotisch gleich* sind. Das ist an sich ein ziemlich verblüffendes Resultat, denn das Auftreten von Primzahlen unter den natürlichen Zahlen scheint im großen und ganzen eher chaotisch zu sein, und doch gibt es eine so einfach Annäherung für ihre Anzahl. Dies ist die Aussage des sogenannten großen Primzahlsatzes.

Satz 1.16. *Es gilt*

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

oder in äquivalenter Schreibweise

$$\pi(x) \sim \frac{x}{\log x}.$$

Gauss vermutete eigentlich zunächst dieses Resultat mit einer anderen Funktion statt $\frac{x}{\log x}$, nämlich $\mathrm{Li}(x) := \int_2^x \frac{1}{\log x} dx$. Es ist aber nicht schwer zu sehen, dass beide Behauptungen äquivalent sind. In der Praxis ist jedoch die Annäherung von $\pi(x)$ durch $\mathrm{Li}(x)$ scheinbar besser, wie sich auf den untenstehenden Graphen zeigt. Die grüne Kurve gehört zu $\mathrm{Li}(x)$, die rote zu $\pi(x)$ und die blaue zu $\frac{x}{\log x}$.

Der Primzahlsatz wurde schließlich 1896 von Hadamard und unabhängig auch von de la Vallée-Poussin bewiesen, allerdings mit sehr fortgeschrittenen Methoden der komplexen Analysis, die wir hier nicht andeuten können. Es ist übrigens nicht so, dass $\mathrm{Li}(x) \geq \pi(x)$ stets gilt, wie es die Graphen ja vermuten lassen. Dies wurde allerdings nur abstrakt gezeigt, es ist kein konkretes x bekannt mit $\mathrm{Li}(x) < \pi(x)$.

Auch sonst ist das letzte Wort über den Primzahlsatz noch nicht gesprochen. Der Primzahlsatz gibt eine Abschätzung für $\pi(x)$ durch „einfache“ Funktionen. Eine natürliche Frage ist dann die nach dem Fehler in dieser Abschätzung. Die Riemannsche Vermutung, wahrscheinlich eines der bekanntesten und wichtigsten ungelösten Probleme der gesamten Mathematik, liefert die (zu ihr äquivalente) Aussage, dass der Fehler $|\pi(x) - \frac{x}{\log x}|$ von der Größenordnung $\sqrt{x}\log x$ ist.

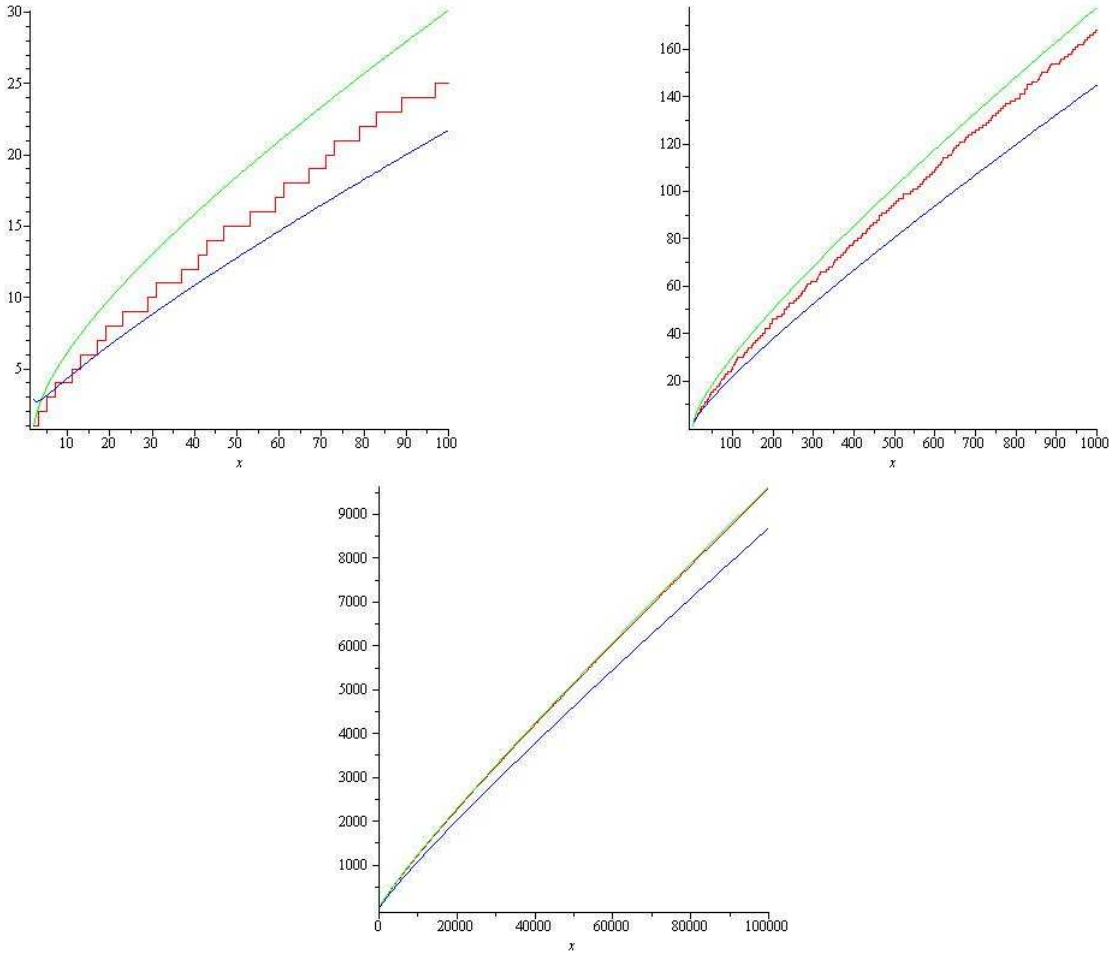


Abbildung 1.1: Graphen von $\mathrm{Li}(x)$, $\pi(x)$ und $\frac{x}{\log x}$ für $x \leq 100,\ 1000,\ 100000$

Kapitel 2

Lösen von Polynomgleichungen

Literaturempfehlungen Die Inhalte von Abschnitte 2.1 and 2.2 sind Standards der Algebra und finden sich in quasi jedem Lehrbuch zur Algebra, z.B. in [Art98]. Für die weiterführende Lektüre zu Satz 2.16 empfehle ich das Buch [Pes05], sowie Kapitel 9 von [Koc04].

2.1 Allgemeine Definitionen

Wir beginnen damit, einige allgemeine Definitionen über Polynome anzugeben. zur Vereinfachung der Notation schreiben wir R stellvertretend für entweder die ganzen Zahlen $\mathbb{Z}$, die rationalen Zahlen $\mathbb{Q}$, die reellen Zahlen $\mathbb{R}$ oder die komplexen Zahlen $\mathbb{C}$. Außerdem bezeichnen wir mit R^* die sogenannte *Einheitengruppe* von R, also $R^* = \{\pm 1\}$ für $R = \mathbb{Z}$ und $R^* = R \setminus \{0\}$ in allen übrigen Fällen.

Definition 2.1. *Ein* Polynom *vom* Grad $n \in \mathbb{N}_0$ *über R ist eine formale Summe*

$$f = a_n X^n + a_{n-1} X^{n-1} + ... + a_1 X + a_0$$

mit einer Unbestimmten X und Koeffizienten $a_n, \ldots, a_0 \in R$ *mit $a_n \neq 0$. Den Grad des Nullpolynoms $f = 0$ definieren wir als $-\infty$. Die Menge aller Polynome über R bezeichnen wir mit $R[X]$.*

Bekannterweise kann man Polynome addieren und multiplizieren, man sagt, dass $R[X]$ ein *Ring* ist. Addition lässt den Grad gleich oder verkleinert ihn, bei der Multiplikation werden die Grade der Faktoren addiert.

Definition 2.2. *(i) Ein Polynom $f \in R[X]$ vom Grad $n \geq 1$ heißt* reduzibel, *falls es Polynome $g, h \in R[X] \setminus R^*$ gibt mit $f = g \cdot h$. Anderenfalls heißt f* irreduzibel.

(ii) Ein Element $\alpha \in R$ heißt eine Nullstelle *eines Polynoms $f \in R[X]$, wenn es ein Polynom $g \in R[X]$ gibt mit $f = (X - \alpha) \cdot g$. Man nennt $X - \alpha$ dann einen* Linearfaktor *von f.*

Bemerkung 2.3. *Man muss an dieser Stelle darauf hinweisen, dass es i.A. von der Wahl von R abhängt, ob ein Polynom irreduzibel ist bzw. eine Nullstelle besitzt. Z.B. hat das Polynom $3X - 5 \in \mathbb{Z}[X]$ keine Nullstelle (über $\mathbb{Z}$), als Polynom in $\mathbb{Q}[X]$ aber sehr wohl, nämlich $\frac{5}{3}$. Ebenso Ist das Polynom $X^2 + 1 \in \mathbb{R}[X]$ irreduzibel, zerfällt aber in $\mathbb{C}[X]$ zu $(X - i) \cdot (X + i)$.*

Bemerkung 2.4. *Dass ein Polynom $f \in R[X]$ keine Nullstelle hat, heißt noch lange nicht, dass es irreduzibel ist. Z.B. ist das Polynom $X^4 + 2X^2 + 1 = (X^2 + 1)^2$ in $\mathbb{R}[X]$ offensichtlich reduzibel, hat aber keine Nullstelle in $\mathbb{R}$.*

Die Definition eines irreduziblen Polynoms erinnert ein wenig an die einer Primzahl. In der Tat kann man zeigen, dass im Polynomring $R[X]$, ähnlich wie in den ganzen Zahlen, eine (bis auf Multiplikation mit Elementen aus R^*) eindeutige Zerlegung in irreduzible Faktoren gibt. Das impliziert folgendes Lemma, das wir aber nicht beweisen.

Lemma 2.5. *Seien $f, g, q \in R[X]$ und q irreduzibel mit $q \mid (f \cdot g)$. Dann gilt $q \mid f$ oder $q \mid g$.*

2.2 Polynome über den ganzen und rationalen Zahlen

Betrachten wir zunächst Polynome mit ganzzahligen Koeffizienten. Aus der Schule kennen Sie vermutlich aus dem Kontext der Polynomdivision die Aufgabe, die Nullstellen eines Polynoms 3. Grades dadurch zu bestimmen, dass man eine Nullstelle α rät, das Polynom durch $X - \alpha$ teilt und die verbleibende quadratische Gleichung mit einem beliebigen Verfahren (pq-Formel, quadratische Ergänzung,...) löst. Das Raten der Nullstelle ist besonders gut möglich, wenn das Polynom *normiert* (also $a_n = 1$ gilt) und ganzzahlig ist. Dann gilt nämlich Folgendes.

Bemerkung 2.6. *Sei $f = X^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$ normiert und reduzibel, sagen wir $f = g \cdot h$ mit $g = X^k + b_{k-1}X^{k-1} + ... + b_0 \in \mathbb{Z}[X]$ und $h = X^{n-k} + c_{n-k-1}X^{n-k-1} + ... + c_0 \in \mathbb{Z}[X]$. Dann gilt $a_0 = b_0 \cdot c_0$, insbesondere ist also jede ganzzahlige Nullstelle von f ein Teiler von a_0.*

Um ganzzahlige Nullstellen zu finden ist diese Bemerkung recht praktisch. Aber was kann man über die nicht-ganzzahligen Nullstellen sagen (sagen wir über $\mathbb{C}$)? Es könnte ja sein, dass einige davon immerhin noch rational sind. Dass dem nicht so ist, wollen wir im Folgenden beweisen. Dazu zunächst eine Definition.

Definition 2.7. *Ein Polynom $f = a_nX^n + a_{n-1}X^{n-1} + ... + a_0 \in \mathbb{Z}[X]$ heißt* primitiv, *falls der* ggT *seiner Koeffizienten* 1 *ist, das Polynom also durch keine ganze Zahl (außer ± 1) teilbar ist.*

Lemma 2.8. *Das Produkt von zwei primitiven Polynomen ist selbst wieder primitiv.*

Beweis. Seien $f, g \in \mathbb{Z}[X]$ primitive Polynome. Wäre nun $f \cdot g$ nicht primitiv, dann gäbe es eine Primzahl p, die alle Koeffizienten von $f \cdot g$ teilt, also auch das Polynom. Da p auch als irreduzibles Polynom aufgefasst werden kann, bedeutet dies nach Lemma 2.5, dass auch $p \mid f$ oder $p \mid g$ gilt, was aber nach Voraussetzung nicht sein kann. Also muss, wie behauptet, $f \cdot g$ primitiv sein. □

Dieses Lemma führt nun zum Beweis des Gaussschen Lemmas.

Satz 2.9 (Gausssches Lemma). *Ein normiertes Polynom f mit ganzzahligen Koeffizienten ist genau dann irreduzibel in $\mathbb{Z}[X]$, wenn es irreduzibel in $\mathbb{Q}[X]$ ist.*

Beweis. Wir zeigen beide Richtungen der Äquivalenz durch Kontraposition. Ist f reduzibel in $\mathbb{Z}[X]$, dann ist f offenbar auch reduzibel in $\mathbb{Q}[X]$, denn $\mathbb{Z}[X] \subseteq \mathbb{Q}[X]$.

Ist umgekehrt $f = g \cdot h$ mit $g, h \in \mathbb{Q}[X]$, dann können wir aus g und h jeweils den Hauptnenner der Koeffizienten (sagen wir M und N) ausklammern, so dass wir die Faktorisierung

$$f = \frac{1}{MN}\left(\tilde{g} \cdot \tilde{h}\right)$$

mit $\tilde{g} = Mg$ und $\tilde{h} = Nh$. Da M, N jeweils die Hauptnenner von g und h sind, sind $\tilde{g}$ und $\tilde{h}$ ganzzahlig und primitiv. Nach Lemma 2.8 ist damit auch $\tilde{g} \cdot \tilde{h}$ primitiv, d.h. es muss $M \cdot N = \pm 1$ gelten. □

Das Lemma von Gauss gibt nun sofort folgendes Korollar.

Korollar 2.10. *Sei $a, n \in \mathbb{N}$. Dann ist die Zahl $\sqrt[n]{a}$ entweder ganzzahlig oder irrational.*

Den Beweis führen Sie in der Übung. Erinnern Sie sich in diesem Zusammenhang an den Ihnen wohl bekannten Beweis der Irrationalität von $\sqrt{2}$. Dieser lässt sich nicht ohne weiteres so formulieren, dass er ohne einen Widerspruch auskommt. Mit dem Lemma von Gauss ist dies aber sehr wohl möglich.

2.3 Die Cardano-Formel

Oft möchten wir gerne exakt die Nullstellen eines Polynoms mit komplexen Koeffizienten bestimmen. Im Falle quadratischer Polynome, also Polynomen vom Grad 2, ist Ihnen aus der Schule ein Verfahren bzw. eine Formel für die Lösung bekannt, nämlich die quadratische Ergänzung bzw. die pq-Formel.

Lemma 2.11. *Sei $f = X^2 + pX + q$ ein normiertes quadratisches Polynom mit komplexen Koeffizienten p, q. Dann sind die Nullstellen von f gegeben durch*

$$\alpha_1 = -\frac{p}{2} + \sqrt{\frac{p^2}{4} - q} \quad \textit{und} \quad \alpha_2 = -\frac{p}{2} - \sqrt{\frac{p^2}{4} - q}.$$

Diese Formel war im Wesentlichen bereits in der Antike bekannt.

Bemerkung 2.12. *Beachten Sie, dass der Ausdruck $\sqrt{a}$ für $a \in \mathbb{C}$ zunächst nicht eindeutig definiert ist, da es keine ausgezeichnete Lösung der Gleichung $z^2 = a$ gibt. Für $a \in \mathbb{R}$ und $a > 0$ kann man die positive, reelle Lösung der Gleichung auszeichnen, für komplexe a ergibt dies aber keinen Sinn. Wir legen ab sofort fest, dass für $a = r \cdot e^{i\varphi}$ mit $r > 0$ und $-\pi < \varphi \leq \pi$ die m-te Wurzel ($m \in \mathbb{N}$) definiert ist als*

$$\sqrt[m]{a} := \sqrt[m]{r} e^{i\frac{\varphi}{m}}.$$

Außerdem legen wir an dieser Stelle das Symbol $\zeta_m = e^{\frac{2\pi i}{m}}$ fest. Man nennt ζ_m eine primitive m-te Einheitswurzel.

Eine weitere praktische Beobachtung ist der Satz von VIETA, der Ihnen ebenfalls aus der Schule bekannt sein dürfte.

Lemma 2.13. *Sei $f = X^2 + pX + q$ ein normiertes quadratisches Polynom mit Nullstellen $\alpha_1, \alpha_2 \in \mathbb{C}$. Dann gilt $p = -(\alpha_1 + \alpha_2)$ und $q = \alpha_1\alpha_2$.*

Wie kann man nun beispielsweise kubische Gleichungen lösen? Falls das Polynom ganzzahlige Koeffzienten hat, können wir versuchen mit Bemerkung 2.6 eine (ganzzahlige) Nullstelle zu raten und mittels Polynomdivision das Problem auf die Lösung einer quadratischen Gleichung zurückführen. Was aber, wenn das nicht geht? Wir zitieren zunächst einmal den sogenannten *Fundamentalsatz der Algebra*.

Satz 2.14. *Jedes nicht-konstante Polynom mit komplexen Koeffizienten hat eine Nullstelle in $\mathbb{C}$.*

Es gibt viele schöne Beweise für diesen Satz, insgesamt sind weit über 100 bekannt. Allerdings setzt jeder davon zumindest Resultate aus der Analysis I voraus, so dass wir diesen Satz hier leider nicht beweisen können. Einen einfachen und kurzen Beweis finden Sie beispielsweise in Kapitel 19 des Buches [AZ10].

Immerhin gibt es also immer eine komplexe Nullstelle eines kubischen Polynoms. Wenn das Polynom reelle Koeffizienten hat, gibt es sogar immer eine reelle Nullstelle (das ist viel leichter zu beweisen, erfordert aber auch einen Satz aus der Analysis I, den sogenannten *Nullstellensatz von* BOLZANO).

Die Geschichte der Lösungsformel für quadratische Gleichungen ist nicht einfach. Publiziert wurde sie zuerst von CARDANO, so dass Sie bis heute als die CARDANO-*Formel* bekannt ist, allerdings waren vor ihm nachweislich auch DEL FERRO und TARTAGLIA in Besitz zumindest von Spezialfällen der Lösungsformel.

Bevor wir zur eigentlichen Formel kommen, eine kleine Vorbemerkung.

Bemerkung 2.15. *Sei $f = X^3 + a_2X^2 + a_1X + a_0$ ein normiertes, kubisches Polynom. Durch die Substitution $Y = X + \frac{a_2}{3}$ erhalten wir ein Polynom $g = Y^3 + b_1Y + b_0$, wobei*

$$b_1 = a_1 - \frac{a_2^2}{3},$$
$$b_0 = a_0 + \frac{2a_2^3}{27} - \frac{a_1a_2}{3}.$$

gilt. Wir können also ohne Einschränkung von vornherein annehmen, dass unsere kubischen Polynome keinen quadratischen Term haben.

Sei für den Rest dieses Abschnitts $f = X^3+a_1X+a_0$ ein Polynom 3. Grades mit komplexen Koeffizienten. Der grundlegende Trick bei der Herleitung der CARDANO-Formel ist nun, die Unbestimmte X durch $u + v$ für zwei neue Variablen u, v zu ersetzen.

Damit ergibt sich mithilfe des binomischen Lehrsatzes

$$(u+v)^3 + a_1(u+v) + a_0 = u^3 + v^3 + 3(u+v)\left(uv + \frac{a_1}{3}\right) + a_0.$$

Wir können also die Nullstellen von f bestimmen, indem wir die Lösungen der Gleichungen

$$u^3 + v^3 + a_0 = 0 \quad \text{und} \quad uv + \frac{a_1}{3} = 0$$

bestimmen.

Die zweite der Gleichungen ist insbesondere erfüllt, wenn

$$u^3v^3 = -\frac{a_1^3}{27}$$

gilt. Nach dem Satz von Vieta (Lemma 2.13) Wissen wir also, dass u^3 und v^3 die Nullstellen des quadratischen Polynoms

$$Z^2 + a_0Z - \frac{a_1^3}{27}$$

sind. Daraus folgt dann mit der pq-Formel (Lemma 2.11), dass

$$u^3 = -\frac{a_0}{2} + \sqrt{\frac{a_0^2}{4} + \frac{a_1^3}{27}} \quad \text{und} \quad v^3 = -\frac{a_0}{2} - \sqrt{\frac{a_0^2}{4} + \frac{a_1^3}{27}}.$$

Setzt man also

$$u_0 = \sqrt[3]{-\frac{a_0}{2} + \sqrt{\frac{a_0^2}{4} + \frac{a_1^3}{27}}},$$

und bestimmt v_0 so, dass $u_0v_0 = -\frac{a_1}{3}$ gilt (indem man $\sqrt[3]{-\frac{a_0}{2} - \sqrt{\frac{a_0^2}{4} + \frac{a_1^3}{27}}}$ mit einer geigneten Potenz von ζ_3 multipliziert), dann erhalten wir die CARDANO-Formel.

Satz 2.16. *Sei $f = X^3 + a_1X + a_0$ ein kubisches Polynom mit komplexen Koeffizienten und u_0, v_0 wie oben. Dann sind die drei Nullstellen α_1, α_2 und α_3 von f gegeben durch*

$$\alpha_1 = u_0 + v_0, \quad \alpha_2 = \zeta_3u_0 + \zeta_3^2v_0, \quad \alpha_3 = \zeta_3^2u_0 + \zeta_3v_0.$$

Wir können diese Formel auch geometrisch veranschaulichen (sofern die Koeffizienten von f reell sind). Betrachten wir den Würfel mit Kantenlänge x und unterteilen diese wie oben in $x = u+v$, siehe Abbildung 2.1. Um den gesamten Würfel in Abbildung 2.1 auszufüllen benötigen wir neben dem blauen Würfel mit einem Volumen von u^3 sowie dem roten mit Volumen v^3 noch die drei Quader in grün bzw. gelb, die jeweils das Volumen $uv(u+v)$ haben. Damit gilt also

$$x^3 = u^3 + v^3 + 3(u+v)uv.$$

Abbildung 2.1: Kubische Ergänzung

Etwa zur gleichen Zeit wie Cardano fand Ferrari, ein Schüler Cardanos, eine allgemeine Lösungsformel für Gleichungen 4. Grades durch wiederholtes Wurzelziehen. Dies spornte selbstverständlich die Mathematiker der folgenden Zeit an, auch entsprechende Formeln für Gleichungen 5. und höheren Grades zu finden. Doch alle Bemühungen blieben ohne Ergebnis und es dauerte bis ins 19. Jahrhundert, bis Ruffini - allerdings unvollständig - und später unabhängig der norwegische Mathematiker Abel beweisen konnten, dass es eine solche allgemeine Formel nicht geben kann. Dieses Resultat wird heute meist als *Satz von* Abel-Ruffini bezeichnet. Die Idee des Beweises ist im Wesentlichen die folgende: Die Nullstellen eines Polynoms haben untereinander gewisse Symmetrien. Diese Symmetrien bilden, wie man zeigen kann, eine Gruppe (siehe Definition 1.7). Was Abel und Ruffini bemerkten war nun, dass die Existenz einer allgemeinen Lösungsformel durch das wiederholte Ziehen von Wurzeln eine gewisse Eigenschaft dieser Gruppe erzwingt und ab Grad 5 können Gruppen auftreten, die diese Eigenschaft nicht erfüllen. Also kan es keine allgemeine Lösungsformel geben.

Für eine recht allgemein verständliche Darstellung des Beweises sowie seiner Geschichte empfehle ich das Buch [Pes05].

Kapitel 3

Einige irrationale Zahlen

3.1 Ein geometrischer Irrationalitätsbeweis

Inzwischen habe Sie mehrere Möglichkeiten gesehen, die Irrationalität bestimmter Zahlen zu entscheiden. Hier wollen wir einen elementargeometrischen Beweis für die Irrationalität des sogenannten *goldenen Schnittes* φ geben.

Definition 3.1. *Teilt man eine Strecke AB so in zwei Teilstrecken AC und CB (mit $AC \geq CB$), so dass die Seitenverhältnisse $\frac{AC}{CB}$ und $\frac{AB}{AC}$ gleich sind (siehe Abbildung 3.1), so nennt man dieses Verhältnis φ den* goldenen Schnitt*.*

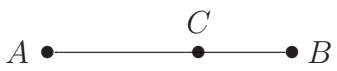


Abbildung 3.1: Der goldene Schnitt

Der goldene Schnitt taucht an vielen Stellen in der Mathematik ganz natürlich auf, so ist φ z.B. genau der Wert des unendlichen *Kettenbruchs*

$$1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{\ddots}}}}$$

oder das Verhältnis der Diagonalenlänge eines regelmäßigen Pentagons zu seiner Seitenlänge. Die Quotienten aufeinanderfolgender FIBONACCI-Zahlen[1] nähern sich ebenfalls

[1]Die ersten beiden FIBONACCI-Zahlen sind 1 und 1 und die nächste ist jeweils die Summe der beiden vorhergehenden. Die ersten FIBONACCI-Zahlen sind also

$$1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, ...$$

dem Wert φ. Da das Seitenverhältnis des goldenen Schnitts als besonders ästhetisch und harmonisch empfunden wird, spielt die Zahl φ auch in der Kunst und Architektur eine wichtige Rolle.

Mit einem einfachen geometrischen Argument können wir nun die Irrationalität von φ herleiten. Wäre nämlich φ rational, sagen wir $\varphi = \frac{m}{n}$ mit $m, n \in \mathbb{N}$, dann könnten wir ein sogenanntes *goldenes Rechteck* mit den ganzzahligen Seitenlängen m und n konstruieren, dessen Seiten genau das Verhältnis φ haben. Nach Definition des Goldenen Schnittes ist aber auch das Rechteck, dass durch Abstreichen eines Quadrates mit Seitenlänge n entsteht, wieder ein Goldenes Rechteck mit ganzzahligen Seitenlängen, siehe Abbildung 3.2.

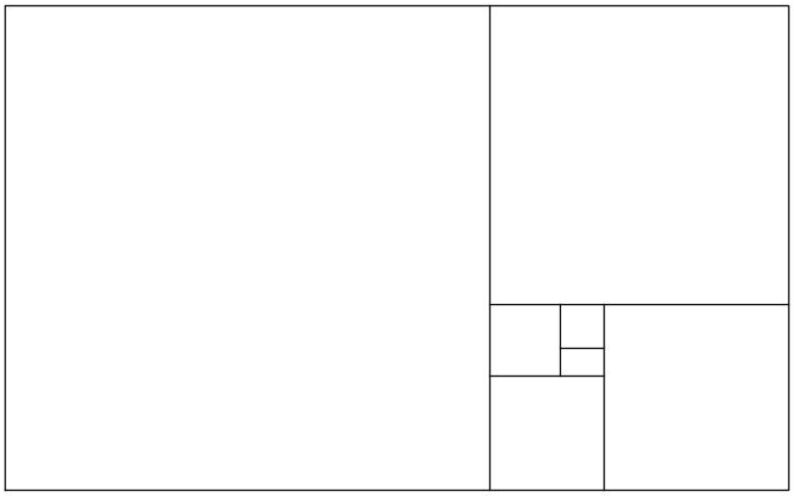


Abbildung 3.2: Goldenes Rechteck

Diesen Prozess kann man beliebig oft wiederholen und immer kleinere Rechtecke mit Seitenlängen in $\mathbb{N}$ konstruieren. Aber eine unendliche absteigende Folge natürlicher Zahlen gibt es nicht, also kann φ nicht rational sein.

3.1.1 Die *descente infinie* und Fermats letzter Satz

Hinter diesem Irrationalitätsbeweis steht ein wichtiges Beweisprinzip aus der Zahlentheorie, das Prinzip der *descente infinie*, der unendlichen absteigenden Folge. Dieses Prinzip, obgleich sicherlich im Wesentlichen seit der Antike bekannt, da sich dieser Irrationalitätsbeweis im Wesentlichen in Euklids *Elemente*, Buch X, finden, wird oft dem französischen Mathematiker Fermat zugeschrieben, da er es wohl als Erster systematisch anwandte. Dies geschah vor allem in Zusammenhang mit dem berühmten *Letzten Satz von* Fermat,

dass für $n \geq 3$ die Gleichung

$$a^n + b^n = c^n$$

nicht von natürlichen Zahlen a, b, c gelöst werden kann. Für $n = 2$ wäre der Satz übrigens falsch, denn z.B. ist $3^2 + 4^2 = 5^2$ und $5^2 + 12^2 = 13^2$ (man kann sogar alle (unendlich vielen) Lösungen der Gleichung für $n = 2$ parametrisieren).

Für $n \geq 3$ behauptete FERMAT in einer Randnotiz in seiner Ausgabe der *Arithmetika* von DIOPHANT, er habe

> „einen wahrhaft hervorragenden Beweis gefunden, doch [sei jener] Rand nicht breit genug, ihn zu fassen."

Ein vollständiger Beweis hat insgesamt fast 350 Jahre auf sich warten lassen, bis er 1994 in zwei Arbeiten von WILES, davon eine gemeinsam mit TAYLOR, veröffentlicht wurde. Er ist allerdings so schwierig und erfordert derart viele sehr neue Techniken, dass es heute als unmöglich angesehen wird, dass FERMAT seinen Satz tatsächlich beweisen konnte. Vermutlich konnte er seine Behauptung für $n = 3$ und $n = 4$ beweisen und schloss voreilig, dass die Behauptung für jedes $n \geq 3$ richtig sein wird.

3.2 Vorbemerkungen

Wir verlassen nun wieder das Reich der elementaren Geometrie und kommen zu ein paar Vorabbemerkungen für das weitere Vorgehen.

Zunächst wenden uns nun der EULERschen Zahl e und der Exponentialfunktion zu.

Sie ist definiert als der Grenzwert

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

und hat in etwa den numerischen Wert

$$e = 2,71828182845904523536028747\ldots .$$

Aus der Schule oder den letzten Wochen des Vorkurses sind Ihnen sicher einige wichtige Eigenschaften der Zahl e bekannt, z.B. ist e die Basis des natürlichen Logarithmus bzw. der Exponentialfunktion, und spielt eine zentrale Rolle in der Darstellung komplexer Zahlen in Polarkoordinaten.

Wir benötigen im Folgenden eine andere Darstellung der Zahl e.

Lemma 3.2. *Die Zahl e lässt sich als Wert der unendlichen Reihe*

$$\sum_{k=0}^{\infty} \frac{1}{k!}$$

darstellen. Allgemeiner gilt für jedes $r \in \mathbb{Q}$ die Gleichung

$$e^r = \sum_{k=0}^{\infty} \frac{r^k}{k!}.$$

Den Beweis hierfür sehen Sie vermutlich in der Vorlesung Analysis I, so dass wir ihn hier auslassen wollen.

Als weiteres Hilfsmittel brauchen wir die *geometrische Reihe*. Dazu sei $x \in \mathbb{R}$ zunächst beliebig und $n \in \mathbb{N}$. Aus der allgemeinen dritten binomischen Formel

$$1 - x^n = (1 - x) \sum_{k=0}^{n-1} x^k$$

folgt sofort die Beziehung

$$\frac{1 - x^{n+1}}{1 - x} = \sum_{k=0}^{n} x^k.$$

Ist nun $|x| < 1$, so wird $|x|^n$ zwar nicht-negativ, aber beliebig klein, wenn n groß wird. Wir können dafür auch schreiben

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

für $|x| < 1$. Daraus folgt dann das überaus praktische Lemma von der geometrischen Reihe.

Lemma 3.3. *Für alle $x \in \mathbb{R}$ mit $|x| < 1$ gilt*

$$\sum_{k=0}^{\infty} x^k = \frac{1}{1 - x}.$$

3.3 Die Irrationalität von e und π

Aus der Definition von e kann man zunächst keinen Anhaltspunkt gewinnen, ob e nun rational oder irrational ist. Ebenso kann man das Problem nicht gut geometrisch angehen. Dennoch ist es nicht schwierig zu beweisen, dass e irrational ist.

Proposition 3.4. *e ist irrational.*

Beweis. Angenommen, e wäre rational, sagen wir $e = \frac{a}{b}$ mit $a, b \in \mathbb{N}$ und $\mathrm{ggT}(a, b) = 1$. Sei zudem $n \in \mathbb{N}$ beliebig. Dann können wir folgendes schreiben,

$$\frac{a}{b} = \sum_{k=0}^{n} \frac{1}{k!} + \sum_{k=n+1}^{\infty} \frac{1}{k!},$$

Multiplizieren wir nun diese Gleichung mit $n!b$, so erhält man

$$n!a = b \sum_{k=0}^{n} n \cdot (n-1) \cdots (n-k+1) + b \sum_{k=n+1}^{\infty} \frac{1}{(n+1) \cdots k}.$$

Die linke Seite ist ofensichtlich eine natürliche Zahl, ebenso der Ausdruck

$$b \sum_{k=0}^{n} n \cdot (n-1) \cdots (n-k+1).$$

Aber der Ausdruck

$$b \sum_{k=n+1}^{\infty} \frac{1}{(n+1)\cdots k} \tag{3.1}$$

kann eben nicht ganzzahlig sein, denn es gilt

$$\begin{aligned} \frac{1}{n+1} &< \frac{1}{n+1} + \frac{1}{(n+1)(n+2)} + \frac{1}{(n+1)(n+2)(n+3)} + ... \\ &< \frac{1}{n+1} + \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} + ... = \frac{(n+1)^{-1}}{1-(n+1)^{-1}} = \frac{1}{n}, \end{aligned}$$

wobei wir für die erste Gleichheit die geometrische Reihe aus Lemma 3.3 benutzt haben. Also liegt der Ausdruck (3.1) echt zwischen $\frac{b}{n+1}$ und $\frac{b}{n}$. Wir können nun also n so groß wählen, dass (3.1) keine ganze Zahl mehr sein kann, was ein Widerspruch ist, so dass die Behauptung folgt. □

Dieser nette Trick stammt von dem französischen Mathematiker FOURIER. Er wirkt im ersten Moment so einfach, dass er wohl nur für diesen einen Beweis gut ist, aber das Gegenteil ist der Fall. Fast ebenso leicht kann man mit einem ähnlichen Argument auch die Irrationalität von e^2 beweisen, was natürlich eine stärkere Aussage ist. Die Idee des Beweises stammt von LIOUVILLE.

Proposition 3.5. *e^2 ist irrational.*

Proof. Nehmen wir wieder an, dass $e^2 = \frac{a}{b}$ gälte mit $a, b \in \mathbb{N}$. Dann können wir diese Gleichung umschreiben in

$$eb = ae^{-1} \tag{3.2}$$

und wieder mit $n!$ für ein beliebiges $n \in \mathbb{N}$ multiplizieren. Die linke Seite von (3.2) kann man dann wie oben schon gesehen behandeln: Mit der Reihendarstellung von e in Lemma 3.2 erhält man, dass

$$n!b \sum_{k=0}^{n} \frac{1}{k!}$$

eine ganze Zahl ist, während der Rest

$$n!b \sum_{k=n+1}^{\infty} \frac{1}{k!}$$

liegt zwischen $\frac{b}{n+1}$ und $\frac{b}{n}$, also ist die linke Seite von (3.2) für große n etwas größer als eine ganze Zahl.

Nun zur rechten Seite von (3.2). Wir erhalten mit der Reihendarstellung von e^{-1} wieder einen ganzzahligen Anteil von

$$n!a \sum_{k=0}^{n} \frac{(-1)^k}{k!}$$

und einen Rest

$$r := (-1)^{n+1} n! a \left(\frac{1}{(n+1)!} - \frac{1}{(n+2)!} + \frac{1}{(n+3)!} \mp \dots \right).$$

Nehmen wir n als gerade an, was wir tun können, da es zunächst beliebig war, so erhalten wir, dass einerseits $r > -\frac{a}{n}$ gilt, andererseits, dass

$$r < -a \left(\frac{1}{n+1} - \frac{1}{(n+1)^2} + \frac{1}{(n+1)^3} \mp \dots \right) = -\frac{a}{n+1} \left(1 - \frac{1}{n} \right) < 0.$$

Damit ist für hinreichendes großes gerades n die rechte Seite von (3.2) etwas *kleiner* als eine ganze Zahl und das ist offenbar absurd. Demnach muss unsere Anfangsannahme, dass e^2 rational ist, falsch sein, also folgt die Behauptung. □

Der Nachteil dieser beiden Beweise ist, dass sie die konkrete Darstellung von e direkt ausnutzen, so dass eine ähnliche Methode wohl für andere Zahlen nicht funktioniert. Deswegen wollen wir nun eine allgemeinere Methode vorstellen, die uns erlauben wird, den folgenden Satz zu beweisen.

Satz 3.6. *Für jedes $r \in \mathbb{Q} \setminus \{0\}$ ist e^r irrational.*

Der Beweis erfordert etwas Vorarbeit, nämlich das

Lemma 3.7. *Sei für $n \in \mathbb{N}$ die Funktion $f : \mathbb{R} \to \mathbb{R}$ definiert durch*

$$f(x) = \frac{x^n (1-x)^n}{n!}.$$

Dann ist Folgendes richtig.

(i) Die Funktion f ist eine Polynomfunktion und es gilt

$$f(x) = \frac{1}{n!} \sum_{j=n}^{2n} c_j x^j,$$

wobei die c_j, $j = n, ..., 2n$, ganze Zahlen sind.

(ii) Für $0 < x < 1$ ist $0 < f(x) < \frac{1}{n!}$.

(iii) Für alle $k \geq 0$ sind die Werte Ableitungen $f^{(k)}(0)$ und $f^{(k)}(1)$ ganze Zahlen.

Beweis. Die Teil (i) folgt unmittelbar aus dem binomischen Lehrsatz.

Zu Teil (ii) bemerken wir, dass für $0 < x < 1$ auch $0 < x^n < 1$ und $0 < (1-x)^n < 1$ gilt, also folgt die Behauptung.

Für Teil (iii) sei zunächst $n \leq k \leq 2n$. Dann ist $f^{(k)}(0) = \frac{k!}{n!} c_k \in \mathbb{Z}$ und für $k < n$ sowie $k > 2n$ gilt $f^{(k)}(0) = 0$. Nun gilt offenbar $f(x) = f(1-x)$, also $f^{(k)}(x) = (-1)^k f^{(k)}(1-x)$, also ist auch $f^{(k)}(1) = (-1)^k f^{(k)}(0)$ eine ganze Zahl. □

Beweis *von Satz 3.6.* Wir können ohne Einschränkung $r \in \mathbb{N}$ annehmen. Wäre nämlich $e^{\frac{s}{t}}$ rational, so wäre auch $e^s = \left(e^{\frac{s}{t}}\right)^t$ rational. Nehmen wir also an, dass $e^r = \frac{a}{b}$ gälte mit $a, b \in \mathbb{N}$. Weiterhin sei $n \in \mathbb{N}$ so groß, dass $n! > ar^{2n+1}$ gilt[2]. Definieren wir nun die Funktion $F : \mathbb{R} \to \mathbb{R}$ durch

$$F(x) = r^{2n} f(x) - r^{2n-1} f'(x) + r^{2n-2} f''(x) \mp ... + f^{(2n)}(x)$$

mit f wie in Lemma 3.7. Da für $k > 2n$ die k-te Ableitung von f identisch Null ist, können wir $F(x)$ auch folgendermaßen schreiben,

$$F(x) = \sum_{k=0}^{\infty} (-1)^k r^{2n-k} f^{(k)}(x).$$

Berechnen wir aus dieser Darstellung die Ableitung von F, so erhalten wir

$$F'(x) = \sum_{k=0}^{\infty} (-1)^k r^{2n-k} f^{(k+1)}(x) = -r \sum_{k=1}^{\infty} (-1)^k r^{2n-k} f^{(k)}(x) = -rF(x) + r^{2n+1} f(x).$$

Eine solche Gleichung nennt man eine *Differentialgleichung*. Nach der Produktregel ergibt sich also

$$\frac{d}{dx}\left[e^{rx} F(x)\right] = re^{rx} F(x) + e^{rx} F'(x) = r^{2n+1} e^{rx} f(x),$$

so dass die Zahl

$$N := b \int_0^1 r^{2n+1} e^{rx} f(x) dx = b\left[e^{rx} F(x)\right]_0^1 = aF(1) - bF(0)$$

gemäß Teil (iii) von Lemma 3.7 eine ganze Zahl ist. Mit Teil (ii) desselben Lemmas erhalten wir aber die Abschätzung

$$0 < N = b \int_0^1 r^{2n+1} e^{rx} f(x) dx < br^{2n+1} e^r \frac{1}{n!} = \frac{ar^{2n+1}}{n!} < 1$$

nach unserer Wahl von n. Ganze Zahlen, die zwischen 0 und 1 liegen, gibt es aber nicht, also haben wir einen Widerspruch und unser Satz 3.6 ist bewiesen. □

Was etwas überraschen mag ist, dass man mit derselben Methode auch folgendes zeigen kann.

Satz 3.8. π^2 *ist irrational.*

Beweis. Wir führen den Beweis wieder durch Widerspruch, nehmen also an, dass $\pi^2 = \frac{a}{b}$ mit für zwei natürliche Zahlen a und b ist. Ähnlich wie im Beweis zu Satz 3.6 definieren wir nun die Polynomfunktion F durch

$$F(x) := b^n \left(\pi^{2n} f(x) - \pi^{2n-2} f^{(2)}(x) + \pi^{2n-4} f^{(4)}(x) \mp ...\right.$$

[2]Dass ein solches n existiert, beweisen Sie in der Übung.

und bemerken durch direktes Nachrechnen, dass F der Differentialgleichung

$$F''(x) = -\pi^2 F(x) + b^n \pi^{2n+2} f(x)$$

genügt. Damit erhalten wir, dass

$$\begin{aligned}\frac{d}{dx}\left[F'(x)\sin(\pi x) - \pi F(x)\cos(\pi x)\right] &= \left(F''(x) + \pi^2 F(x)\right)\sin(\pi x)\\ &= b^n \pi^{2n+2} f(x)\sin(\pi x)\\ &= \pi^2 a^n f(x)\sin(\pi x).\end{aligned}$$

Wieder mit Teil (iii) von Lemma 3.7 sehen wir, dass $F(0)$ und $F(1)$ ganze Zahlen sind, und damit auch

$$N := \pi \int_0^1 a^n f(x)\sin(\pi x)dx = \left[\frac{1}{\pi}F'(x)\sin(\pi x) - F(x)\cos(\pi x)\right]_0^1 = F(0) + F(1).$$

Da die Integrandfunktion in $]0,1[$ positiv ist, ist sicher $N > 0$, aber nach Teil (ii) von Lemma 3.7 haben wir auch die Abschätzung

$$0 < N = \pi \int_0^1 a^n f(x)\sin(\pi x)dx < \frac{\pi a^n}{n!}.$$

Bisher war n noch beliebig, aber wir können genau wie zuvor n nun so groß wählen, dass $\frac{\pi a^n}{n!} < 1$ gilt, und wir haben wieder den erwünschten Widerspruch. □

Auch die Sätze 3.6 and 3.8 sind noch weit von der Wahrheit entfernt, denn mit Mitteln aus der Komplexen Analysis oder auch Funktionentheorie lässt sich der *Satz von* Lindemann-Weierstrass beweisen, aus dem folgt, dass e und π sogar *transzendent* über $\mathbb{Q}$ sind, also keine Nullstellen eines Polynoms mit rationalen Koeffizienten sein können.

Kapitel 4

Graphentheorie

Literaturempfehlung In diesem Kapitel geht es um eine Einführung in elementare Begriffe der Graphentheorie, die im weiteren Verlauf als Hilfsmittel zum Beweis eines klassisch-geometrischen Resultats, nämlich der Klassifikation der PLATONischen Körper. Diese Darstellung lehnt sich locker an diejenige in [RT33], Kapitel 12 an. Außerdem werden EULERsche Graphen behandelt, wobei ich mich hier in der Darstellung im Wesentlichen an [Vol96], Kapitel 3 orientiert habe.

4.1 Einführung

Wir werden keine präzise, formale Definition eines Graphen geben, sondern im Wesentlichen mit anschaulichen Erläuterungen arbeiten. Für uns ist ein *Graph* G eine (endliche) Ansammlung V von sogenannten *Ecken*, die durch *Kanten* miteinander verbunden sind, siehe z.B. die Beispiele in Abbildung 4.1.

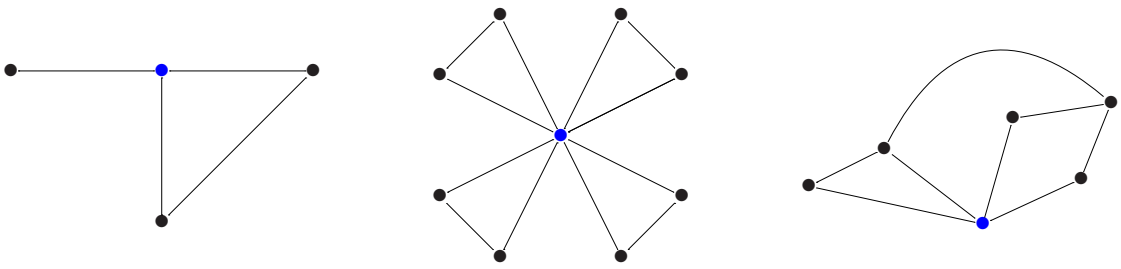


Abbildung 4.1: Graphen

Die Menge der Kanten bezeichnen wir mit E. Zur Vereinfachung schließen wir mehrfache Kanten zwischen denselben Ecken meist aus.

Die Anzahl der Kanten, die an einer Ecke ankommen, nennt man den *Grad* des Knotens. In den obigen Beispielen hat z.B. die blau eingefärbte Ecke den Grad 3, 8, bzw. 4.

Ein *Pfad* von einer Ecke v_0 zu einer Ecke v_n ist eine Folge von Ecken

$$(v_0, v_1, ..., v_n)$$

so dass immer zwischen v_j und v_{j+1} $(j = 0, ..., n-1)$ eine Kante existiert und keine Ecke doppelt vorkommt, außer dass v_0 und v_n gleich sein können, siehe Abbildung 4.2.

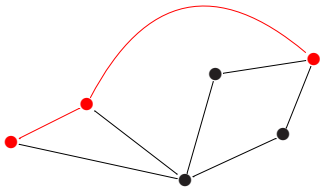


Abbildung 4.2: Pfad

Wenn zwischen zwei beliebigen Ecken eines Graphen immer ein Pfad existiert, so heißt der Graph *zusammenhängend*. Wenn wir es nicht explizit anders fordern, nehmen wir ab sofort alle Graphen als zusammenhängend an.

Ein Pfad von v_0 nach $v_n = v_0$ heißt ein *Kreis*, wenn er mindestens drei verschiedene Kanten enthält (also nicht z.B. über dieselbe Kante hin und zurück läuft).

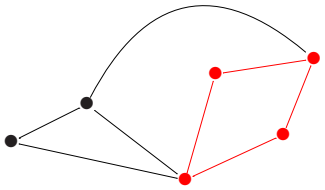


Abbildung 4.3: Kreis

Einen Graphen, der keine Kreise enthält, nennen wir einen *Baum*. Anschaulich ist klar, dass jeder Graph einen sogenannten *Spannbaum* besitzt, also einen Teilgraphen mit denselben Ecken, der zusammenhängend ist und unzusammenhängend wird, wenn man eine beliebige Kante entfernt. In Abbildung 4.4 markieren die roten Ecken *einen* möglichen Spannbaum des angegebenen Graphen.

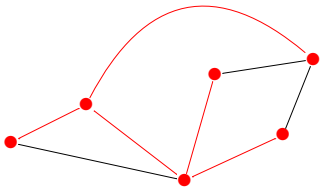


Abbildung 4.4: Spannbaum

Wenn ein Graph in der Ebene (oder äquivalent auf einer Kugeloberfläche) so gezeichnet werden kann, dass sich keine Kanten kreuzen, nennen wir ihn *planar*, eine Eigenschaft, die wir ab sofort ebenfalls stillschweigend von unseren betrachteten Graphen voraussetzen, es sei denn, es wird explizit anders gesagt. Wenn er bereits durch eine solche Zeichnung gegeben ist, nennen wir den Graphen *eben*. Der in Abbildung 4.5 gezeichnete Graph ist z.B. nicht planar, dagegen aber alle Graphen in Abbildung 4.1, diese sind sogar eben.

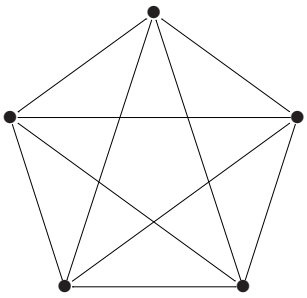


Abbildung 4.5: Ein nicht-planarer Graph

4.2 Das Königsberger Brückenproblem

Die Stadt Königsberg (heute Kaliningrad) liegt am Fluss Pregel und besteht aus mehreren Inseln im Fluss. Im 18. Jahrhundert gab es zwischen den insgesamt 4 Stadtteilen 7 Brücken über den Fluss, siehe Abbildung 4.6.

Es gab nun, wie gesagt im 18. Jahrhundert, ein sehr bekanntes mathematisches Problem über diese Brücken von Königsberg, nämlich ob es von irgendeinem Punkt in der Stadt möglich ist, jede Brücke genau einmal zu überqueren und zum Ausgangspunkt zurückzukehren. Euler bewies im Jahre 1736 einen allgemeinen Satz, der zeigt, dass dies nicht möglich ist. Er erkannte, bevor es die Graphentheorie als eigentliche mathematische Disziplin überhaupt gab, dass das Königsberger Brückenproblem graphentheoretisch zu lösen ist. Dies wird oft als die Geburtsstunde der Graphentheorie und manchmal auch der Topologie angesehen.

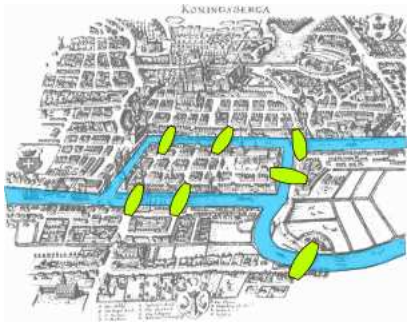
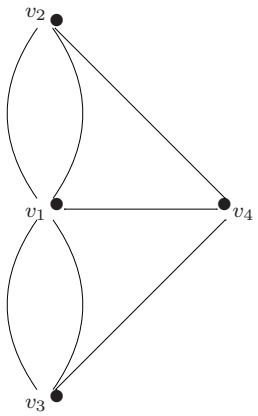


Abbildung 4.6: Die Brücken von Königsberg

Definition 4.1. *Ein (nicht notwendig einfacher) Graph G besitzt einen* Euler-Kreis, *wenn es in ihm einen geschlossenen Pfad gibt, der jede Kante genau einmal enthält. Man nennt G dann auch einen* Eulersch*en Graphen. Man sagt, dass er einen* Euler-Pfad *besitzt, wenn es allgemeiner einen Pfad gibt, der jede Kante genau einmal enthält, aber nicht zum Ausgangspunkt zurückkehrt.*

Die Situation der Königsberger Brücken lässt sich mit folgendem Graphen modellieren.



Euler bewies nun (zumindest teilweise) den folgenden

Satz 4.2. *(i) Ein zusammenhängender Graph enthält genau dann einen* Euler-*Kreis, wenn die Grade aller Ecken gerade sind.*

(ii) Er enthält dann und nur dann einen Euler-*Pfad, wenn er genau 2 Ecken mit ungeradem Grad enthält.*

Für den Beweis brauchen wir ein kleines Lemma.

Lemma 4.3. *Sei G ein zusammenhängender Graph, in dem jede Ecke mindestens Grad 2 hat. Dann enthält G einen Kreis.*

Beweis. Sicherlich enthält G einen längsten Pfad

$$(v_0, v_1, ..., v_n),$$

der nicht mehr um eine Kante verlängert werden kann ohne eine Ecke doppelt zu besuchen. Die Ecke v_0 hat aber mindestens Grad 2, also muss er nach Konstruktion mindestens einen Nachbarn v_k unter den $v_1, ..., v_n$ haben (ansonsten ließe sich der Pfad verlängern). Dann ist aber

$$(v_0, v_1, ..., v_k, v_0)$$

ein Kreis in G. □

Beweis *von Satz 4.2.* Wir zeigen zunächst Teil (i) des Satzes. Dazu ist es leicht einzusehen, dass die Bedingung, dass alle Ecken geraden Grad haben, sicher notwendig für die Existenz eines EULER-Kreises ist. Denn folgt man einem solchen Kreis, so kommt an jeder Ecke eine Kante an und eine andere verlässt ihn wieder, wobei eine Ecke mehrfach besucht werden kann. Da keine Kante doppelt benutzt werden darf, muss also der Grad jeder Ecke gerade sein. Um zu zeigen, dass die Bedingung, nur Ecken mit geradem Grad zu haben, auch hinreichend ist, damit der Graph einen EULER-Kreis enthält, verwenden wir Induktion über die Anzahl der Kanten. Für eine Kante ist die Aussage klar. Für $n \geq 1$ Ecken gibt es nach Lemma 4.3 sicher einen Kreis C in G. Entfernt man nun die Kanten von C aus G, so hat der entstehende Graph G' entweder keine Kanten mehr und ist C somit ein EULER-Kreis, oder er ist ein (möglicherweise unzusammenhängender) nicht-trivialer Teilgraph von G. In den jeweiligen Zusammenhangskomponenten hat nun immernoch jede Ecke geraden Grad, also enthält jede nach Induktionsvoraussetzung einen EULER-Kreis. Da G zusammenhängend war, hat jede Zusammenhangskomponente von G' eine Ecke mit C gemeinsam. Einen EULER-Kreis für G erhält man nun, indem man von einer beliebigen Ecke in C ausgehend startet, bis man an eine Ecke aus einer nicht-trivialen Komponente von G' kommt, dann dem EULER-Kreis dieser Komponente folgt und dann auf C wieder bis zur nächsten Komponente usf.

Teil (ii) folgt nun leicht aus Teil (i). Gibt es in einem Graphen G einen EULER-Pfad mit Anfangsecke v_0 und Endecke v_n, so fügen wir eine weitere Ecke v^* zum Graphen hinzu, der genau mit v_0 und v_n verbunden ist. Nennen wir diesen Graphen G^*. Damit entsteht ein EULER-Kreis, also muss nach (i) in G^* jede Ecke geraden Grad haben. Die Grade von v_0 und v_n in G sind jeweils um eins kleiner als in G^*, alle anderen sind unverändert, also folgt, dass in G genau v_0 und v_n ungeraden Grad haben. Ist umgekehrt G ein Graph mit genau zwei Ecken mit ungeradem Grad, sagen wir wieder v_0 und v_n, so fügen wir eine Kante e^* zwischen v_0 und v_n ein. Damit haben alle Ecken im ergänzten Graphen G^* geraden Grad, es gibt also nach Teil (i) einen EULER-Kreis C in G^*. Indem man aus C die Kante e^* wieder entfernt, entsteht der gewünschte EULER-Pfad. □

4.3 Der EULERsche Polyedersatz

Sei G ein ebener, zusammenhängender Graph. Dann bezeichnen wir die Anzahl seiner Ecken mit e, die Anzahl der Kanten mit k und die Anzahl der vom Graph berandeten

Flächen inklusive der unendlichen äußeren Fläche mit f. Für die Graphen aus Abbildung 4.1 haben wir dann folgende Werte.

Graph	e	k	f
Graph 1	4	4	2
Graph 2	9	12	5
Graph 3	6	8	4

Wir erkennen nun leicht, dass für diese Beispiele stets die Gleichung

$$e + f - k = 2$$

gilt. Dies ist ein allgemeiner Satz, der zuerst von EULER bewiesen wurde und nach ihm der EULER*sche Polyedersatz* genannt wird.

Satz 4.4. *Für jeden ebenen Graphen G mit e Ecken, k Kanten und f Flächen gilt die Beziehung*

$$e + f - k = 2.$$

Beweis. Wir konstruieren einen Spannbaum des Graphen G. Dazu entfernt man für jede Fläche außer der äußeren von G eine sie umrandende Kante, insgesamt also $f - 1$ Stück. Wir wollen uns zunächst überlegen, dass der so konstruierte Teilgraph T ein Spannbaum für G ist. Es ist klar, dass T alle Ecken von G beinhaltet, da wir lediglich Kanten entfernt haben. Außerdem muss T zuammenhängend sein, sonst hätten wir während der Konstruktion von T eine Kante mehr als nötig entfernt. Und enthielte T einen Kreis, so würde dieser eine Fläche einschließen, aber das kann auch nach Konstruktion nicht sein, denn diese Fläche müsste auch eine von G gewesen sein, von der dann in T eine Randkante fehlen würde. Der Teilgraph T selbst hat nun genau $e-1$ Kanten, denn einerseits muss er mindestens $e - 1$ Kanten haben, um alle Ecken zu verbinden, anderseits müsste es unter der Annahme, dass T mehr als $e - 1$ Kanten hätte, notwendig einen Kreis in T geben, was nicht sein kann. Wir haben also von G genau $f - 1$ Kanten entfernt und verbleiben mit $e - 1$ Kanten, also gilt

$$k = (f - 1) + (e - 1),$$

was äquivalent zur Polyederformel ist. □

Zum besseren Verständnis kann man sich folgendes Bild vor Augen halten. Die Kanten stehen für Deiche, und die (inneren) Flächen für trockene Äcker, während die äußere Fläche für umgebendes Gewässer steht. Man will nun durch Niederlegen einiger Deiche alle Äcker unter Wasser setzen und zwar so, dass man immer noch trockenen Fußes auf den Deichen zu jedem Kreuzungspunkt laufen kann.

4.4 Die PLATONischen Körper

Schon seit der Antike sind die fünf sogenannten PLATON*ischen Körper* bekannt, siehe Abbildungen 4.7 bis 4.11. Diese zeichnen sich dadurch aus, dass sie von kongruenten,

Abbildung 4.7: Tetraeder

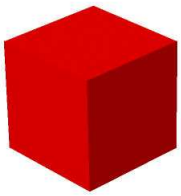


Abbildung 4.8: Hexaeder

Abbildung 4.9: Oktaeder

Abbildung 4.10: Dodekaeder

Abbildung 4.11: Ikosaeder

regelmäßigen Vielecken begrenzt werden und *konvex* sind, d.h. keine einspringenden Ecken haben.

Die Frage, die uns hier interessiert ist die, ob es außer diesen fünf noch andere Platonische Körper geben kann. Wir werden den Eulerschen Polyedersatz verwenden, um folgendes zu zeigen.

Satz 4.5. *Es gibt genau fünf* Platon*ische Körper.*

Proof. Dass es mindestens fünf Platonische Körper geben muss, ist klar, denn wir haben in Abbildungen 4.7 bis 4.11 fünf verschiedene angegeben.

Um zu zeigen, dass es auch nur höchstens fünf geben kann, wollen wir, wie gesagt, die Eulersche Polyederformel verwenden. Dazu stellen wir uns ein beliebiger Platonischer Körper in eine Kugel einbeschrieben vor und projizieren die Ecken und Kanten auf die Kugeloberfläche. dabei bleiben zwar Winkel, Längen und Flächeninhalte nicht erhalten, aber diese sind für die weiteren überlegungen auch nicht von Belang. Wir können uns so nämlich einen Platonischen Körper mit e Ecken, k Kanten und f Flächen als ebenen Graphen (auf einer Kugeloberfläche) vorstellen, so dass nach dem Polyedersatz 4.4 die

Gleichung

$$e + f - k = 2. \tag{4.1}$$

Nun seien die Grenzflächen des Polyeders alles φ-Ecke ($\varphi \in \mathbb{N}$). Dann gilt auf jeden Fall

$$\varphi \geq 3.$$

Ebenso treffen sich in jeder Ecke des Polyeders gleich viele Flächen, sagen wir ε Stück. Dann ist auch klarerweise

$$\varepsilon \geq 3.$$

Da die Begrenzungsflächen unseres Polyeders alles kongruente φ-Ecke sind, haben wir für jede Seitenfläche des Polyeders auch φ Kanten. Jede Kante gehört zu genau zwei Seitenflächen, also haben wir die Beziehung

$$f\varphi = 2k. \tag{4.2}$$

Genauso treffen in jeder Ecke des Polyeders ε Flächen und damit auch ε Kanten aufeinander. Da jede Kante genau zwei Ecken verbindet, haben wir auch hier

$$e\varepsilon = 2k. \tag{4.3}$$

Multiplizieren wir nun (4.1) mit 2ε, so erhalten wir die Gleichung

$$2e\varepsilon + 2f\varepsilon - 2k\varepsilon = 4\varepsilon$$

Nach (4.2) und (4.3) können wir in obiger Gleichung $e\varepsilon$ und $2k$ jeweils durch $f\varphi$ ersetzen, so dass sich Folgendes ergibt,

$$f(2\varphi + 2\varepsilon - \varphi\varepsilon) = 4\varepsilon. \tag{4.4}$$

Da f und 4ε positiv sind, muss dies auch für die Klammer in (4.4) gelten. Dies liefert unmittelbar die Ungleichung

$$\varphi\varepsilon - 2\varphi - 2\varepsilon + 4 = (\varphi - 2)(\varepsilon - 2) < 4.$$

Da φ und ε ganze Zahlen und mindestens 3 sind, kommen nur die folgenden Kombinationen für φ und ε in Frage,

$$(\varphi, \varepsilon) \in \{(3,3), (3,4), (4,3), (3,5), (5,3)\}. \tag{4.5}$$

Daraus folgt dann schließlich, dass es in der Tat höchstens fünf Platonische Körper geben kann. □

Mit (4.5) sehen wir auch, dass die Seitenfläche eines PLATONischen Körpers nur ein Drei-, Vier-, oder Fünfeck sein kann.

Aus (4.4) können wir ableiten, dass

$$f = \frac{4\varepsilon}{2\varphi + 2\varepsilon - \varphi\varepsilon}$$

gilt, woraus mit (4.2) die Gleichung

$$k = \frac{f\varphi}{2} = \frac{\varepsilon\varphi}{2\varphi + 2\varepsilon - \varphi\varepsilon}$$

folgt. Daraus wiederum ergibt sich mit (4.3) die Beziehung

$$e = \frac{2k}{\varepsilon} = \frac{4\varphi}{2\varphi + 2\varepsilon - \varphi\varepsilon}.$$

Wir fassen die möglichen Konfigurationen in der folgenden Tabelle zusammen.

φ	ε	f	k	e	
3	3	4	6	4	Tetraeder
3	4	8	12	6	Oktaeder
4	3	6	12	8	Hexaeder
3	5	20	30	12	Ikosaeder
5	3	12	30	20	Dodekaeder

Kapitel 5

Neue Objekte zum Rechnen

Literaturempfehlung In den meisten Lehrbüchern über Algebra oder Lineare Algebra findet sich ein Abschnitt über die HAMILTON-Quaternionen, z.B. in [Lan02]. Elliptische Kurven werden in den meisten Quellen deutlich abstrakter eingeführt als hier, so dass viele Lehrbücher, die sie behandeln, noch nicht gut für Sie lesbar sind. Eine verhältnismäßig einfache Einführung findet man in [IR90] oder [Wer02].

5.1 Quaternionen

Wie Sie sich aus der vergangenen Woche erinnern werden, können die komplexen Zahlen $\mathbb{C}$ als reelle Ebene anschaulich realisiert werden, wobei Addition komplexer Zahlen der Vektoraddition im $\mathbb{R}^2$ und die Multiplikation komplexer Zahlen einer Drehstreckung entspricht. Diese Interpretation verdanken wir C. F. GAUSS. Man hat darauf lange versucht, mit einer entsprechenden Vorstellung eine Art von *hyperkomplexen Zahlen* einzuführen, die statt mit der Ebene mit dem dreidimensionalen Raum arbeiten. All diese Versuche blieben erfolglos, bis der irische Mathematiker W. R. HAMILTON im Jahre 1843 erkannte, dass eine solche Konstruktion nicht möglich ist, und man statt mit dem dreidimensionalen mit dem vierdimensionalen Raum über $\mathbb{R}$ arbeiten muss. Die so entstehenden Objekte nennt man heute nach ihrem Entdecker die HAMILTON-*Quaternionen*. Diese Objekte wollen wir nun einführen und ein paar ihrer Eigenschaften beleuchten.

Definition 5.1. *Für die Symbole* $\mathbf{i}$, $\mathbf{j}$ *und* $\mathbf{k}$ *legen wir folgende Relationen fest,*

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1, \quad \mathbf{i} \cdot \mathbf{j} = -\mathbf{j} \cdot \mathbf{i} \quad \textit{und} \quad \mathbf{i} \cdot \mathbf{j} = \mathbf{k}.$$

Für ein Quadrupel (a_0, a_1, a_2, a_3) *reeller Zahlen nennt man dann*

$$\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$$

*ein (*HAMILTON-*)*Quaternion*, wobei die Summe rein formal zu verstehen ist. Die Menge der* HAMILTON-*Quaternionen bezeichnen wir mit* $\mathbb{H}$. *Die* Summe *zweier Quaternionen* $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ *und* $\beta = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}$ *ist erklärt durch*

$$\alpha + \beta = (a_0 + b_0) + (a_1 + b_1)\mathbf{i} + (a_2 + b_2)\mathbf{j} + (a_3 + b_3)\mathbf{k},$$

ihr Produkt *ist definiert durch*

$$\begin{aligned}\alpha \cdot \beta = &(a_0b_0 - a_1b_1 - a_2b_2 - a_3b_3)\\ &+ (a_0b_1 + a_1b_0 + a_2b_3 - a_3b_2)\mathbf{i}\\ &+ (a_0b_2 - a_1b_3 + a_2b_0 + a_3b_1)\mathbf{j}\\ &+ (a_0b_3 + a_1b_2 - a_2b_1 + a_3b_0)\mathbf{k}.\end{aligned}$$

Man könnte Quaternionen auch einfach als Quadrupel reeller Zahlen einführen, aber die Schreibweise in obiger Definition erweist sich als intuitiver. Es gilt nämlich folgender

Satz 5.2. *Die* Hamilton-*Quaternionen* $\mathbb{H}$ *mit der Addition und Multiplikation aus Definition 5.1 bilden einen nicht-kommutativen Ring.*

Beweis. Wir erinnern an die verschiedenen Gesetze, die hier gezeigt werden müssen. Seien dazu $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, \beta = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k}, \gamma = c_0 + c_1\mathbf{i} + c_2\mathbf{j} + c_3\mathbf{k} \in \mathbb{H}$ beliebig.

A1 $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$. (Assoziatvität der Addition)

A2 $\alpha + \beta = \beta + \alpha$. (Kommutativität der Addition)

A3 Es gibt ein Element $0 \in \mathbb{H}$ mit $\alpha + 0 = 0 + \alpha = \alpha$ für alle $\alpha \in \mathbb{H}$. (Existenz der Null)

A4 Zu jedem $\alpha \in \mathbb{H}$ existiert ein $\beta \in \mathbb{H}$ mit $\alpha + \beta = 0$. (Existenz inverser Elemente)

M1 $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$. (Assoziativität der Multiplikation)

M2 Es existiert ein Element $1 \in \mathbb{H}$ mit $1 \cdot \alpha = \alpha \cdot 1 = \alpha$ für alle $\alpha \in \mathbb{H}$. (Existenz der Eins)

D1 $\alpha \cdot (\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$. (Distributivität von links)

D2 $(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma$. (Distributivität von rechts)

Da die Addition komponentenweise definiert ist, sind die Axiome A1-A4 klar, wobei das Nullelement gegeben ist durch $0 = 0 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$ und das additive Inverse zu α durch $-\alpha = (-a_0) + (-a_1)\mathbf{i} + (-a_2)\mathbf{j} + (-a_3)\mathbf{k}$. Ebenso ist leicht einzusehen, dass M2 erfüllt ist mit $1 = 1 + 0\mathbf{i} + 0\mathbf{j} + 0\mathbf{k}$. Die restlichen Axiome nachzurechnen ist in dieser Darstellung zwar einfach, aber mühselig, so dass wir dies hier nicht ausführen. In der Übung werden Sie einen eleganteren Weg sehen, um die Axiome nachzurechnen.

Dass die Multiplikation nicht kommutativ ist, ist schon aus den Relationen für $\mathbf{i} = 0+1\mathbf{i}+0\mathbf{j}+0\mathbf{k}$, $\mathbf{j} = 0+0\mathbf{i}+1\mathbf{j}+0\mathbf{k}$ und $\mathbf{k} = 0+0\mathbf{i}+0\mathbf{j}+1\mathbf{k}$ klar, denn z.B. ist $\mathbf{i}\cdot\mathbf{j} = -\mathbf{j}\cdot\mathbf{i}$.□

Bemerkung 5.3. *(i) Man beachte, dass man wegen der Nicht-Kommutativität der Multiplikation tatsächlich* 2 *Distributivgesetze nachrechnen muss.*

(ii) Die reellen Zahlen betten sich auf natürliche Weise in die Quaternionen ein ($a \mapsto a+0\mathbf{i}+0\mathbf{j}+0\mathbf{k}$), sodass wir ein Quaternion auch mit einer reellen Zahl multiplizieren können. Man sieht leicht, dass dann für $a \in \mathbb{R}$ und $\alpha \in \mathbb{H}$ stets $a \cdot \alpha = \alpha \cdot a$ gilt.

(iii) Zur Vereinfachung der Notation schreiben wir Summanden der Form $0\mathbf{j}$ o.ä. im Folgenden nicht mehr aus.

Eine wichtige Eigenschaft der HAMILTON-Quaternionen haben wir bisher nicht erwähnt. Diese bilden nämlich beinahe einen Körper, wie wir im nächsten Satz sehen werden Zuvor aber eine

Definition 5.4. *Für ein Quaternion $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}$ heißt*

$$\overline{\alpha} := a_0 - a_1\mathbf{i} - a_2\mathbf{j} - a_3\mathbf{k}$$

das zu α konjugierte *Quaternion. Die* Spur *von α ist*

$$\mathrm{Spur}(\alpha) = \alpha + \overline{\alpha}$$

und die Norm *von α ist gegeben durch*

$$N(\alpha) = \alpha \cdot \overline{\alpha}.$$

Lemma 5.5. *Seien $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k}, \beta = b_0 + b_1\mathbf{i} + b_2\mathbf{j} + b_3\mathbf{k} \in \mathbb{H}$. Dann gilt*

(i) $\overline{\overline{\alpha}} = \alpha$,

(ii) $\overline{\alpha \cdot \beta} = \overline{\beta} \cdot \overline{\alpha}$,

(iii) $\mathrm{Spur}(\alpha) = 2a_0$,

(iv) $N(\alpha) = a_0^2 + a_1^2 + a_2^2 + a_3^2$,

(v) $N(\overline{\alpha}) = N(\alpha)$,

(vi) $N(\alpha \cdot \beta) = N(\alpha)N(\beta)$.

Insbesondere sind Norm und Spur eines Quaternions stets reelle Zahlen.

Den Beweis führen Sie in der Übung.

Wir erhalten nun den folgenden wichtigen

Satz 5.6. *Sei $\alpha = a_0 + a_1\mathbf{i} + a_2\mathbf{j} + a_3\mathbf{k} \in \mathbb{H} \setminus \{0\}$. Dann existiert ein Element $\alpha^{-1} \in \mathbb{H}$ mit $\alpha \cdot \alpha^{-1} = \alpha^{-1} \cdot \alpha = 1$.*

Proof. Definiere das Quaternion

$$\beta := \frac{1}{N(\alpha)}\overline{\alpha}.$$

Zunächst müssen wir sicherstellen, dass β wohldefiniert ist, also dass $N(\alpha) \neq 0$ gilt. Aus Lemma 5.5 wissen wir nun, dass $N(\alpha)$ eine Summe von Quadraten reeller Zahlen ist. Da $\alpha \neq 0$ vorausgesetzt war, ist mindestens eines dieser Quadrate positiv, die übrigen nicht-negativ, also gilt $N(\alpha) > 0$. Es gilt dann

$$\alpha \cdot \beta = \frac{1}{N(\alpha)}\alpha \cdot \overline{\alpha} = \frac{1}{N(\alpha)}N(\alpha) = 1$$

und

$$\beta \cdot \alpha = \frac{1}{N(\alpha)}\overline{\alpha} \cdot \overline{\overline{\alpha}} = \frac{1}{N(\alpha)}N(\overline{\alpha}) = 1.$$

Damit können wir $\alpha^{-1} = \beta$ wählen. □

Nicht-kommutative Ringe, in denen jedes Element außer 0 multiplikativ invertierbar ist, nennt man *Schiefkörper* oder *Divisionsalgebren*, denn sie unterscheiden sich von Körpern lediglich darin, dass die Multiplikation nicht kommutativ ist.

Bemerkung 5.7. *Man kann mit einer ähnlichen Konstruktion auch die sogebannten* Cayley-Oktaven *oder* Oktonionen $\mathbb{O}$ *einführen, welche dann mit* 8*-Tupeln reeller Zahlen arbeiten. Dort ist dann weiterhin jedes Element multiplikativ invertierbar, allerdings ist die Multiplikation weder kommutativ noch assoziativ. Man kann zeigen, dass damit alle (nicht notwendig assoziativen) reellen Divisionsalgebren gefunden sind. Diese sind*

$$\mathbb{R}, \quad \mathbb{C}, \quad \mathbb{H}, \quad \textit{und} \quad \mathbb{O}.$$

Dies ist allerdings zu fortgeschritten, um es hier anzudeuten.

Bemerkung 5.8. *Die Quaternionen bilden nicht nur eine rein akademische Spielerei, sie haben in vielen Bereichen Anwendungen gefunden. Innermathematisch basiert z.B. ein wesentlicher Schritt im Beweis des berühmten* Vier-Quadrate-Satzes *von* Euler-Lagrange*, der aussagt, dass jede natürliche Zahl als Summe von* 4 *Quadratzahlen geschrieben werden kann, auf der Tatsache, dass die Norm-Abbildung auf den Quaternionen* multiplikativ *ist. Außerdem lassen sich durch Quaternionen z.B. Drehungen im dreidimensionalen Raum leichter beschreiben als durch Drehmatrizen, was in der Computergraphik ausgenutzt wird, und auch die fundamentalen Gleichungen der Elektrodynamik lassen sich durch Quaternionen sehr elegant formulieren.*

5.2 Elliptische Kurven

Von einem anschaulichen Standpunkt haben Sie inzwischen gelernt mit Punkten auf einer Geraden, sprich den reellen Zahlen $\mathbb{R}$, in einer Ebene, also den komplexen Zahlen $\mathbb{C}$, und sogar im vierdimensionalen Raum, also den Hamilton-Quaternionen $\mathbb{H}$, zu rechnen. In diesem Abschnitt werden wir eine bestimmte Sorte von *Kurven* kennenlernen, auf der man in gewisser Weise ebenfalls rechnen kann.

Definition 5.9. *(i) Sei $f(X)$ ein Polynom mit reellen Koeffizienten. Dann nennen wir die Menge*

$$C = \{(x, y) \in \mathbb{R}^2 \mid y^2 = f(x)\}$$

eine Kurve *über* $\mathbb{R}$.

(ii) Ist $f(X) = X^3 + aX + b$ ein Polynom dritten Grades mit Diskriminante $\Delta = 4a^3 + 27b^2 \neq 0$, *so nennen wir die Kurve*

$$E = \{(x, y) \in \mathbb{R}^2 \mid y^2 = f(x)\}$$

eine elliptische Kurve. *Das Polynom $f(X)$ nennt man das* Weierstrass-Polynom *der elliptischen Kurve E.*

Bemerkung 5.10. *Unsere Definition einer Kurve ist nicht die allgemein übliche, sie reicht aber für unsere Zwecke aus.*

Typische Bilder elliptischer Kurven finden Sie in Abbildung 5.1.

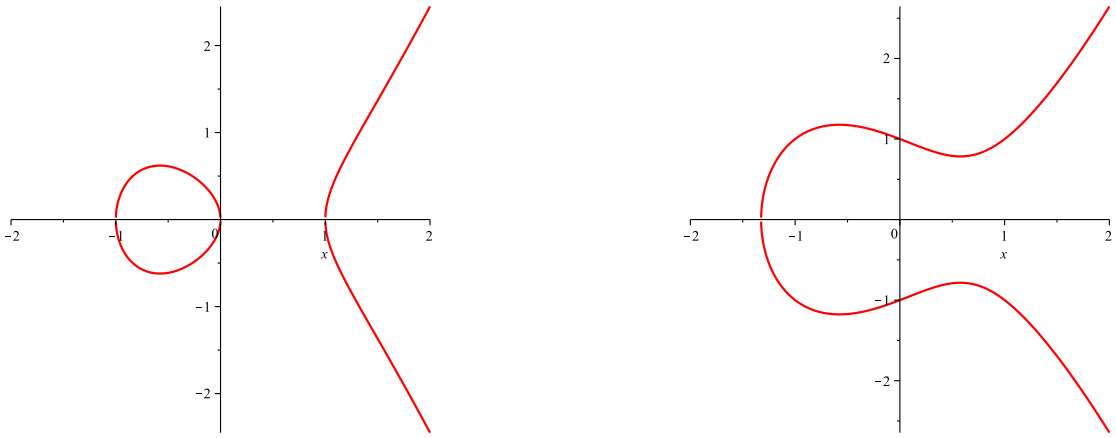


Abbildung 5.1: Elliptische Kurven

In der modernen Mathematik kann die Bedeutung der elliptischen Kurven kaum übertrieben werden. So sind sie z.B. mit die zentralen Objekte in Wiles' Beweis von Fermat's Letztem Satz (siehe Abschnitt 3.1.1), der wesentliche Gegenstand der Birch und Swinnerton-Dyer-Vermutung, eines der 7 Millenniumsprobleme, auf dessen Lösung ein Preisgeld von 1 000 000 $ ausgesetzt ist, und auf ihnen basieren wichtige Verschlüsselungsalgorithmen in der Kryptographie, um nur einige Beispiele zu nennen. Wir wollen uns hier mit einem Phänomen beschäftigen, das elliptische Kurven gegenüber anderen Kurven auszeichnet, nämlich dass man auf ihnen rechnen kann.

Definieren wir dazu zunächst die Addition zweier verschiedener Punkte P und Q auf einer elliptischen Kurve E geometrisch. Die Punkte P und Q legen eine Gerade eindeutig fest, die E in einem Punkt $P*Q$ schneidet. Wir spiegeln diesen Punkt an der horizontalen Achse und erhalten so den Punkt $P \oplus Q$, siehe Abbildung 5.2.

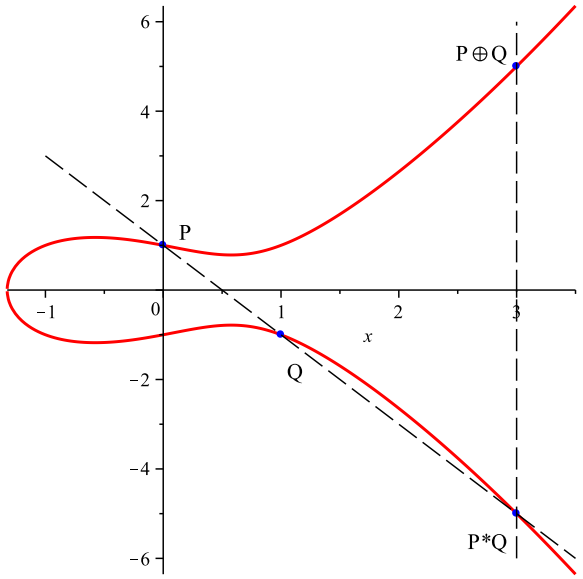


Abbildung 5.2: Addition verschiedener Punkte auf einer elliptischen Kurve

In der Definition einer elliptischen Kurve mit WEIERSTRASS-Polynom $X^3 + aX + b$ haben wir verlangt, dass $\Delta = 4a^3 + 27b^2$ nicht null ist. Dies garantiert uns, dass die *Tangente* an die Kurve E in jedem Punkt existiert. Mittels *projektiver Methoden*, die Sie vermutlich später in der Linearen Algebra lernen werden, könnte man dies recht leicht beweisen, wir nehmen dies jedoch als gegeben hin. Da die Tangente nun immer existiert, können wir auch geometrisch erklären, was wir für einen Punkt P auf der Kurve E mit dem Ausdruck $P \oplus P$ meinen: Wir bestimmen die Tangente an E in P, welche E wiederum in einem Punkt schneidet. Diesen Punkt nennen wir $P * P$. Das Spiegelbild dieses Punktes an der horizontalen Achse ist dann $P \oplus P$, siehe Abbildung 5.3. Man spricht hier auch von der *Verdopplung* des Punktes P und schreibt statt $P \oplus P$ auch einfach $2 \cdot P$.

Diese vorangegangene Erläuterung enthält eine wesentliche Lücke, auf die wir nun zu sprechen kommen. Z.B. würde die durch $P * Q$ und $P \oplus Q$ verlaufende Gerade in Abbildung 5.2 die Kurve E sicher nie schneiden. Dies kann man aber reparieren, indem man einen *unendlich fernen Punkt* $\mathcal{O}$ zu E hinzufügt und festlegt, dass senkrechte Geraden die Kurve E immer im Punkt $\mathcal{O}$ schneiden. Auch die Verbindungsgerade eines beliebigen Punktes $P = (x, y)$ von $E \setminus \{\mathcal{O}\}$ zum Punkt $\mathcal{O}$ ist eine senkrechte Gerade, die mit E den weiteren Schnittpunkt $P * \mathcal{O} = (x, -y)$ hat, so dass

$$P \oplus \mathcal{O} = P$$

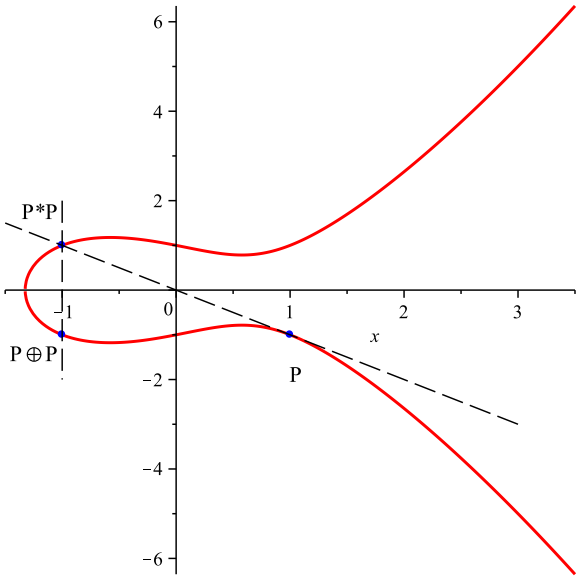


Abbildung 5.3: Verdopplung eines Punktes auf einer elliptischen Kurve

gilt für alle P in $E \setminus \{\mathcal{O}\}$. Wir definieren auch

$$\mathcal{O} \oplus \mathcal{O} = \mathcal{O}.$$

Wir sehen auch sofort, dass für $P = (x, y)$ und $-P := (x, -y)$ stets

$$P \oplus (-P) = \mathcal{O}$$

gilt.

Wir wollen diese anschaulichen Überlegungen nun etwas formalisieren.

Proposition 5.11. *Sei E eine elliptische Kurve mit* Weierstrass*-Polynom $f(X) = X^3 + aX + b$ und $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ seien Punkte von $E \setminus \{\mathcal{O}\}$. Dann gilt*

$$P \oplus Q = (x_3, y_3)$$

mit

$$x_3 = \begin{cases} \lambda^2 - x_1 - x_2, & \text{für } Q \neq \pm P \\ \lambda^2 - 2x_1 & \text{für } P = Q \text{ und } y_1 \neq 0 \end{cases} \quad \text{und} \quad y_3 = \lambda(x_1 - x_3) - y_1,$$

wobei

$$\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2}, & \text{für } P \neq Q \\ \frac{3x_1^2 + a}{2y_1} & \text{für } P = Q \text{ und } y_1 \neq 0. \end{cases}$$

gilt.
Für $P = (x, 0)$ gilt $P \oplus P = \mathcal{O}$.

Der Beweis ist eine etwas aufwendige und nicht sehr erhellende Rechnung, die wir hier nicht ausführen wollen. Man bestimmt die Gleichung der durch P und Q festgelegten Gerade (bzw. der Tangente für $P = Q$) und bestimmt ihren Schnittpunkt mit der Kurve durch Gleichsetzen, was dann die obigen Formeln liefert.

Wir wollen nun die Definition einer ABELschen Gruppe . Eine allgemeine Gruppe haben wir bereits in Definition 1.7 eingeführt.

Definition 5.12. *Eine nicht-leere Menge G mit einer Verknüpfung*

$$+ : G \times G \to G, (g, h) \mapsto g + h$$

heißt eine ABELsche Gruppe*, falls*

1. *für $g, h, k \in G$ stets $(g + h) + k = g + (h + k)$ gilt,*
2. *ein* neutrales Element *Element $0 \in G$ existiert mit $g + 0 = 0 + g = g$ für alle $g \in G$,*
3. *zu jedem $g \in G$ ein* inverses Element *$h \in G$ existiert mit $g + h = h + g = 0$,*
4. *für alle $g, h \in G$ stets $g + h = h + g$ gilt.*

Nur die letzte Bedingung liefert etwas Neues gegenüber Definition 1.7.

Es gilt nun der

Satz 5.13. *Eine elliptische Kurve E zusammen mit der Verknüpfung $\oplus$ ist eine* ABELsche *Gruppe, wobei $\mathcal{O}$ das neutrale Element und $-P = (x, -y)$ das zu $P = (x, y)$ inverse Element ist.*

Beweis. Dass $\mathcal{O}$ das neutrale Element und $-P$ das zu P inverse Element ist, haben wir bereits gesehen. Dass die Verknüpfung $\oplus$ kommutativ ist, ist offensichtlich, weil die Verbindungsgerade von P nach Q dieselbe wie von Q nach P ist, insbesondere ist der dritte Schnittpunkt mit der Kurve gleich, und damit gilt $P \oplus Q = Q \oplus P$. Die Assoziativität nachzurechnen ist wieder nicht ohne eine längliche Rechnung zu bewerkstelligen, die aber nicht viel Einsicht bietet, so dass wir darauf verzichten wollen, sie durchzuführen. □

Bemerkung 5.14. *Für $m \in \mathbb{Z}$ können wir den Punkt $m \cdot P$ für einen Punkt P auf einer elliptischen Kurve E erklären vermöge*

$$m \cdot P := \begin{cases} \underbrace{P \oplus \cdots \oplus P}_{m \text{ Mal}} & \text{für } m > 0 \\ \mathcal{O} & \text{für } m = 0 \\ |m| \cdot (-P) & \text{für } m < 0. \end{cases}$$

Kapitel 6

Die allgemeine harmonische Reihe

Literaturempfehlung Die allgemeine harmonische Reihe ist ein Standardthema in der Vorlesung Analysis I, sie wird dementsprechend in quasi jedem Lehrbuch zur Analysis behandelt, z.B. in [K̈95]. Für den zweiten Teil des Kapitels habe ich mich an Kapitel 8 von [AZ10] orientiert.

6.1 Konvergenz und Divergenz der allgemeinen harmonischen Reihe

Schon in Kapitel 3 haben wir mit unendlichen Reihen gearbeitet, so z.B. der geometrischen Reihe (siehe Lemma 3.3) oder der Exponentialreihe (siehe Lemma 3.2). In dieser Vorlesung werden wir uns mit der *allgemeinen harmonischen Reihe* befassen.

Definition 6.1. *Für $\sigma \in \mathbb{R}$ nennen wir den Ausdruck*

$$\sum_{n=1}^{\infty} \frac{1}{n^\sigma}$$

die allgemeine harmonische Reihe. *Für $\sigma = 1$ spricht man auch von der* harmonischen Reihe.

In diesem Abschnitt wollen wir uns damit beschäftigen, wann diese Reihe einen sinnvollen, endlichen Wert hat. Es ist relativ offensichtlich, dass die allgemeine harmonische Reihe für $\sigma \leq 0$ unendlich würde, denn dann ist für alle $n \in \mathbb{N}$

$$\frac{1}{n^\sigma} \geq \frac{1}{n^0} = 1,$$

und die Summe von unendlich vielen Einsen wäre unendlich, was wir nicht als vernünftigen Wert annehmen. Für $\sigma > 0$ müssen wir aber genauer hinsehen. In der Analysis I-Vorlesuing werden alle diese Betrachtungen noch einmal formal korrekter und v.a. vollständiger angestellt. beispielsweise haben wir hier nicht die Zeit, formal die Begriffe

Konvergenz und *Divergenz* von unendlichen Summen (oder *Reihen*) zu diskutieren. Für den Moment bezeichnen wir eine Reihe $\sum_{n=1}^{\infty} a_n$ über positive reelle Zahlen a_n, $n \in \mathbb{N}$, als *divergent* wenn wir die *Partialsummen* $\sum\limits_{n=1}^{N} a_n$ nach unten gegen eine Größe abschätzen können, die mit N unendlich groß wird. Z.B. ist $\sum_{n=1}^{\infty} 1$ divergent, da

$$\sum_{n=1}^{N} 1 = N$$

gilt, was für große N beliebig groß wird (offensichtlich). Andererseits nennen wir eine Reihe Reihe wie oben *konvergent*, wenn wir die Partialsummen nach oben gegen eine Größe abschätzen können, die für beliebig große N beschränkt bleibt. Z.B. ist die Reihe $\sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n$ konvergent, denn nach der allgemeinen dritten binomischen Formel gilt

$$\sum_{n=1}^{N} \left(\frac{1}{2}\right)^n = \frac{1 - \left(\frac{1}{2}\right)^{N+1}}{1 - \frac{1}{2}} - 1 \leq \frac{1}{1 - \frac{1}{2}} = 2.$$

In der Analysis I zeigen Sie, dass man einer konvergenten Reihe eine reelle Zahl als eindeutigen Wert zuordnen kann. Der Wert der Reihe $\sum_{n=1}^{\infty} \left(\frac{1}{2}\right)^n$ wäre damit z.B. 1, siehe Lemma 3.3.

Ich weise darauf hin, dass unsere „Definition“ für Reihenkonvergenz ausschließlich für Reihen über positive reelle Zahlen funktioniert und auch nicht tatsächlich präzise ist. Für unsere Zwecke reicht Sie aber.

Wir beweisen nun den folgenden

Satz 6.2. *Für $\sigma > 1$ ist die allgemeine harmonische Reihe konvergent, ansonsten divergent.*

Beweis. Sei zunächst $\sigma = 1 + \varepsilon$ mit $\varepsilon > 0$. Wir verwenden einen kleinen Trick und fassen immer 2^k viele Summanden der Reihe zusammen und schätzen diese nach oben ab. Dann haben wir folgendes

$$\begin{aligned}
&1 + \underbrace{\frac{1}{2^{1+\varepsilon}} + \frac{1}{3^{1+\varepsilon}}}_{\leq 2 \cdot \frac{1}{2^{1+\varepsilon}}} + \underbrace{\frac{1}{4^{1+\varepsilon}} + \frac{1}{5^{1+\varepsilon}} + \frac{1}{6^{1+\varepsilon}} + \frac{1}{7^{1+\varepsilon}}}_{\leq 4 \frac{1}{4^{1+\varepsilon}}} + \underbrace{\frac{1}{8^{1+\varepsilon}} + \ldots + \frac{1}{15^{1+\varepsilon}}}_{\leq 8 \cdot \frac{1}{8^{1+\varepsilon}}} + \ldots \\
\leq & 1 + \frac{1}{2^{\varepsilon}} + \left(\frac{1}{2^{\varepsilon}}\right)^2 + \left(\frac{1}{2^{\varepsilon}}\right)^3 + \ldots \\
= & \frac{2^{\varepsilon}}{2^{\varepsilon} - 1},
\end{aligned}$$

wobei wir in der letzten Zeile die geometrische Reihe verwendet haben. Wir können also für $\sigma > 1$ die allgemeine harmonische Reihe gegen eine konvergente geometrische Reihe nach oben abschätzen, also ist sie selbst konvergent.

Offenbar gilt für jedes $n \in \mathbb{N}$ und $0 < \sigma \leq 1$

$$\frac{1}{n^\sigma} \geq \frac{1}{n},$$

so dass es reicht, die Divergenz der harmonischen Reihe zu beweisen. Dazu fassen wir wieder immer 2^k viele Summanden zusammen, schätzen diesmal aber nach unten ab. So erhalten wir

$$1 + \frac{1}{2} + \underbrace{\frac{1}{3} + \frac{1}{4}}_{\geq 2 \cdot \frac{1}{4} = \frac{1}{2}} + \underbrace{\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}}_{\geq 4 \cdot \frac{1}{8} = \frac{1}{2}} + \underbrace{\frac{1}{9} + ... + \frac{1}{16}}_{\geq 8 \cdot \frac{1}{16} = \frac{1}{2}} + ...,$$

also können wir für $N \in \mathbb{N}$ abschätzen

$$\sum_{n=1}^{2^N} \frac{1}{n} \geq 1 + \frac{N}{2},$$

was mit N gegen unendlich geht, so dass die harmonische Reihe divergiert. □

Bemerkung 6.3. *Die Divergenz der harmonischen Reihe ist sehr langsam. So ist z.B.* $\sum_{n=1}^{1\,000\,000} \frac{1}{n} \approx 14.3927$. *Man kann sogar genau angeben, wie langsam die harmonische Reihe wächst, es gilt nämlich*

$$\lim_{N \to \infty} \left(\sum_{n=1}^{N} \frac{1}{n} - \log(N) \right) = \gamma,$$

wo

$$\gamma = 0.5772156649...$$

die Euler-Mascheroni-*Konstante ist.*

6.2 Spezielle Werte

Wir haben oben gesehen, dass der Reihe

$$\sum_{n=1}^{\infty} \frac{1}{n^2}$$

ein reeller Wert zugeordnet werden kann. Die Bestimmung diese Wertes ist als das *Basel-Problem* bekannt, welches wir in diesem Abschnitt lösen wollen. Dazu müssen wir ein wenig Integralrechnung aus der Schule wiederholen bzw. erweitern.

6.2.1 Die Substitutionsformel

In der Schule lernt man (zumindest im Leistungskurs) die Substitutionsformel für Integrale.

Lemma 6.4. *Seien $f, g : [a, b] \to \mathbb{R}$ stetig-differenzierbare Funktionen (d.h. sie besitzen eine stetige Ableitung) mit $a < b \in \mathbb{R}$. Dann gilt die Gleichheit*

$$\int_a^b f'(g(x))g'(x)dx = f(g(b)) - f(g(a)).$$

Dies ist eine einfache Konsequenz der Kettenregel. Man kann die Substitutionsregel auch wie folgt formulieren, es bleibt aber die selbe Regel.

Lemma 6.5. *Sei $f : [a, b] \to \mathbb{R}$ eine stetig differenzierbare Funktion und $g : [a, b] \to \mathbb{R}$ stetig differenzierbar und injektiv. Dann gilt*

$$\int_a^b f(x)dx = \int_{g^{-1}(a)}^{g^{-1}(b)} f(g(y))g'(y)dy.$$

Diese Substitutionsregeln kann man auch für zweidimensionale Integrale formulieren. Dort integriert man eine Funktion $f : \mathbb{R}^2 \to \mathbb{R}$ nicht über ein Intervall, sondern eher über eine Fläche S im $\mathbb{R}^2$,

$$\int_S f(x, y)dx\,dy,$$

wobei man die Integrationen nach x und y einfach nacheinander ausführt. In manchen Situationen ist es vorteilhaft, evtl. über eine andere Fläche, sagen wir T, zu integrieren. Dazu wählt man eine bijektive, stetig differenzierbare Abbildung, die $(u, v) \in T$ auf $(x, y) = (x(u, v), y(u, v)) \in S$ abbildet (was stetig differenzierbar im $\mathbb{R}^2$ genau heißt, ist zunächst gar nicht so klar, wie man denken könnte, aber das würde uns hier zu weit führen). Dann gilt das

Lemma 6.6. *Mit obigen Bezeichnungen und Voraussetzungen gilt*

$$\int_S (f(x, y)dx\,dy = \int_T f(x(u, v), y(u, v)) \left|\frac{d(x, y)}{d(u, v)}\right| du\,dv,$$

wobei

$$\frac{d(x, y)}{d(u, v)} = \frac{dx}{du}\frac{dy}{dv} - \frac{dx}{dv}\frac{fy}{du}$$

gilt. Der Ausdruck $\frac{dx}{du}$ meint hierbei die Ableitung von $x(u, v)$ nach u, wobei man v als Konstante ansieht.

6.2.2 Das Baselproblem

Mit diesem Handwerkszeug ausgerüstet werden wir nun folgenden Satz mit Hilfe einer einfachen Integraltransformation beweisen.

Satz 6.7. *Es gilt*

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Beweis. Wir werden das Doppelintegral

$$I := \int_0^1 \int_0^1 \frac{1}{1-xy} dx\, dy$$

auf zwei verschiedene Weisen auswerten und so unsere Behauptung beweisen. Wir entwickeln den Integranden in eine geometrische Reihe, was im bereich der Integration tun dürfen, und erhalten so

$$\begin{aligned} I &= \int_0^1 \int_0^1 \sum_{n=0}^{\infty} (xy)^n dx\, dy = \sum_{n=0}^{\infty} \int_0^1 \int_0^1 (xy)^n dx\, dy \\ &= \sum_{n=0}^{\infty} \left(\int_0^1 x^n dx \right) \cdot \left(\int_0^1 y^n dy \right) = \sum_{n=0}^{\infty} \frac{1}{n+1} \cdot \frac{1}{n+1} \\ &= \sum_{n=1}^{\infty} \frac{1}{n^2}. \end{aligned}$$

Es ist hier auch wieder nicht ohne Weiteres klar, dass man die unendliche Summation mit der Integration vertauschen darf. Im Allgemeinen geht das NICHT!

Wir haben das Integral I zunächst über ein achsparalleles Quadrat mit Seitenlänge 1 und der unteren linken Ecke im Koordinatenursprung, siehe Abbildung 6.1. Wir benutzen nun Lemma 6.6, um stattdessen über das Quadrat aus Abbildung 6.2 zu integrieren. Wir definieren

$$u := \frac{y+x}{2} \quad \text{und} \quad v := \frac{y-x}{2},$$

also

$$x = u - v \quad \text{und} \quad y = u + v.$$

Dann gilt

$$\frac{1}{1-xy} = \frac{1}{1-u^2+v^2}$$

und

$$\frac{d(x,y)}{d(u,v)} = 1 \cdot 1 - (-1) \cdot 1 = 2.$$

Wir teilen das Integral entsprechend der Abbildung auf und erhalten

$$I = 4 \int_0^{\frac{1}{2}} \left(\int_0^u \frac{1}{1-u^2+v^2} dv \right) du + 4 \int_{\frac{1}{2}}^1 \left(\int_0^{1-u} \frac{1}{1-u^2+v^2} dv \right) du.$$

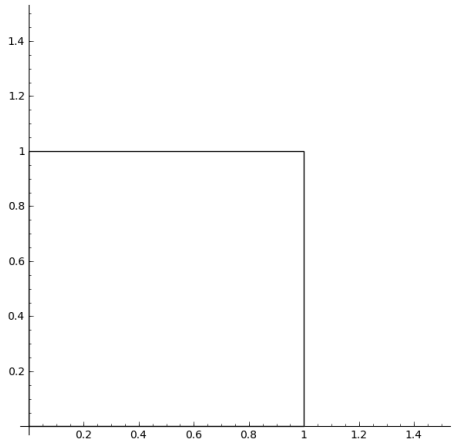


Abbildung 6.1:

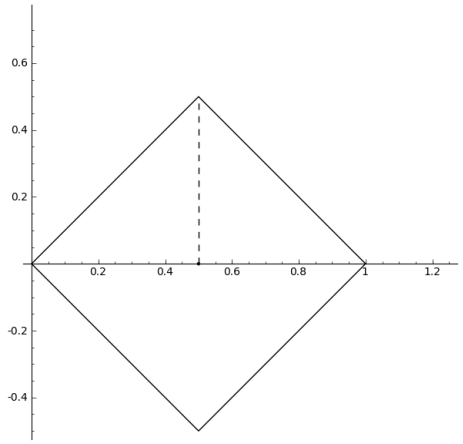


Abbildung 6.2:

Mit dem Standardintegral (vgl. Tafelwerk oder rechnen Sie es nach) $\int \frac{1}{a^2+x^2}dx = \frac{1}{a}\arctan\left(\frac{x}{a}\right)+C$ können wir jeweils die innere Integration (nach v) ausführen und wir haben dann

$$\begin{aligned} I =& 4\int_0^{\frac{1}{2}} \frac{1}{\sqrt{1-u^2}} \arctan\left(\frac{u}{\sqrt{1-u^2}}\right) du \\ &+4\int_{\frac{1}{2}}^1 \frac{1}{\sqrt{1-u^2}} \arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right) du. \end{aligned}$$

Wir bemerken nun (durch direktes Nachrechnen), dass

$$\arctan\left(\frac{u}{\sqrt{1-u^2}}\right)' = \frac{1}{\sqrt{1-u^2}}$$

und

$$\arctan\left(\frac{1-u}{\sqrt{1-u^2}}\right)' = -\frac{1}{2}\frac{1}{\sqrt{1-u^2}}$$

gilt, so dass wir die verbleibenden Integrale mit Lemma 6.4 ausrechnen können. Aus Lemma 6.4 folgt nämlich die allgemeine Integrationsformel

$$\int_a^b f'(x)f(x)dx = \left[\frac{1}{2}f(x)^2\right]_a^b = \frac{1}{2}f(b)^2 - \frac{1}{2}f(a)^2,$$

die uns folgendes liefert ($g(u) := \arctan\left(\frac{u}{\sqrt{1-u^2}}\right)$ und $h(u) := \arctan\left(\frac{u}{\sqrt{1-u^2}}\right)$),

$$\begin{aligned} I =& 4\int_0^{\frac{1}{2}} g'(u)g(u)du + 4\int_{\frac{1}{2}}^1 -2h'(u)h(u) \\ =& 2\left[g\left(\frac{1}{2}\right)^2 - g(0)^2\right] - 4\left[h\left(1\right)^2 - h\left(\frac{1}{2}\right)^2\right] \\ =& 2\left(\frac{\pi}{6}\right)^2 - 0 - 0 + 4\left(\frac{\pi}{6}\right)^2 = \frac{\pi^2}{6}. \end{aligned}$$

Damit folgt die Behauptung. □

Bemerkung 6.8. *Der Wert der Reihe* $\sum_{n=1}^{\infty} \frac{1}{n^2}$ *wurde zuerst von* Euler *im Jahr 1735 bestimmt, während er in Basel arbeitete, daher der Name Basel-Problem. Er berechnete sogar für jedes* $k \in \mathbb{N}$ *die Werte* $\sum_{n=1}^{\infty} \frac{1}{n^{2k}}$*, die immer ein rationales Vielfaches von* π^{2k} *sind. Z.B. gilt*

$$\sum_{n=1}^{\infty} \frac{1}{n^4} = \frac{\pi^4}{90}, \quad \sum_{n=1}^{\infty} \frac{1}{n^6} = \frac{\pi^6}{945}, \quad \sum_{n=1}^{\infty} \frac{1}{n^8} = \frac{\pi^8}{9450}, \ldots$$

Sein Vorgehen war allerdings vollkommen anders als das hier beschriebene.

Symbolverzeichnis

$\mathbb{C}$	Körper der komplexen Zahlen
Δ	Diskriminante einer Kurve mit WEIERSTRASS-Polynom $X^3 + aX + b$, $\Delta = 4a^3 + 27b^2$.
$\exists$	Existenzquantor
$\forall$	Allquantor
γ	EULER-MASCHERONI-Konstante, $\gamma = 0.5772156649...$
ggT	größter gemeinsamer Teiler
log	natürlicher Logarithmus, $\log x := \int_1^x \frac{1}{t} dt$
$\mathbb{N}$	Menge der naturlichen Zahlen, $\mathbb{N} = \{1, 2, 3, \dots\}$
$\mathbb{N}_0$	naturliche Zahlen mit 0
$\oplus$	Additionsoperator auf einer elliptischen Kurve, siehe S. 44
$\mathbb{P}$	Menge der Primzahlen
$\mathfrak{Pot}(X)$	Potenzmenge der Menge X
$\mathbb{Q}$	Körper der rationalen Zahlen
$\mathbb{R}$	Körper der reellen Zahlen
φ	der goldene Schnitt, $\varphi = 1.6180339...$
$\mathbb{Z}$	Ring der ganzen Zahlen
$]a, b[$	offenes Intervall von a bis b, $]a, b[= \{x \in \mathbb{R} \ : \ a < x < b\}$
e	EULERsche Zahl, $e = \lim_{n\to\infty} \left(1 + \frac{1}{n}\right)^n = 2.71828...$
$f^{(k)}(x)$	k-te Ableitung der Funktion f an der Stelle x
F_n	n-te FERMAT-Zahl, $F_n = 2^{2^n} + 1$

M_p	p-te MERSENNE-Zahl, $M_p = 2^p - 1$
R	Ring oder Körper, $R \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}\}$
R^*	Einheitengruppe von R, $\mathbb{Z}^* = \{\pm 1\}$, sonst $R^* = R \setminus \{0\}$

Namensverzeichnis

Literaturverzeichnis

[Art98] Artin, M.: *Algebra*. Grundstudium der Mathematik. Birkhäuser-Verlag, 1998.

[AZ10] Aigner, M. und G. M. Ziegler: *Das BUCH der Beweise*. Springer-Verlag, 3. Auflage Auflage, 2010.

[BBC00] Beck, A., M. N. Bleicher und D. W. Crowe: *Excursions into Mathematics*. A K Peters Ltd., Millennium edition Auflage, 2000.

[IR90] Ireland, K. und M. Rosen: *A Classical Introduction to Modern Number Theory*. Springer-Verlag, 2. Auflage, 1990.

[K̈95] Königsberger, K.: *Analysis 1*. Springer-Verlag, 3 Auflage, 1995.

[Koc04] Koch, H.: *Einführung in die Mathematik*. Springer-Verlag, 2. Auflage Auflage, 2004.

[Lan02] Lang, S.: *Algebra*. Springer-Verlag, 2002.

[Pes05] Pesic, P.: *Abels Beweis*. Springer-Verlag, 2005.

[RT33] Rademacher, H. und O. Toeplitz: *Von Zahlen und Figuren*. Springer-Verlag, 2. Auflage Auflage, 1933. Reprint von 2001.

[RU95] Remmert, R. und P. Ullrich: *Elementare Zahlentheorie*. Grundstudium der Mathematik. Birkhäuser-Verlag, 1995.

[Vol96] Volkmann, L.: *Fundamente der Graphentheorie*. Springer-Verlag, 1996.

[Wer02] Werner, A.: *Elliptische Kurven in der Kryptographie*. Springer-Verlag, 2002.