universität wien

DIPLOMARBEIT / DIPLOMA THESIS

Titel der Diplomarbeit / Title of the Diploma Thesis

„Algebren- und Körpererweiterungen der reellen Zahlen“

verfasst von / submitted by

Andrea Krenn

angestrebter akademischer Grad / in partial fulfilment of the requirements for the degree of

Magistra der Naturwissenschaften (Mag. rer. nat.)

Wien, 2018 / Vienna, 2018

Studienkennzahl lt. Studienblatt / degree programme code as it appears on the student record sheet:	A 190 412 406
Studienrichtung lt. Studienblatt / degree programme as it appears on the student record sheet:	Lehramtsstudium, UF Physik, UF Mathematik
Betreut von / Supervisor:	ao. Univ.-Prof. Mag. Dr. Günther Hörmann

Zusammenfassung

Für die Entwicklung der gesamten Mathematik, so wie wir sie heute kennen, waren Zahlenbereichserweiterungen von größter Relevanz. In Disziplinen wie Physik und Technik, hätten niemals die heutigen Entwicklungsstände erreicht werden können, wäre der Zahlenbereich nicht stets weiterentwickelt worden.
Ausgehend von den natürlichen Zahlen $\mathbb{N}$, wurden die Zahlenmengen nach und nach immer weiter fortgesetzt. Der geschichtliche Weg von den positiven ganzen Zahlen, über die negativen, rationalen, reellen und komplexen Zahlen, bis hin zu Konstrukten wie den vierdimensionalen Quaternionen, war lange, und oftmals mit großen Schwierigkeiten und Unklarheiten verbunden.

Das Ziel dieser Diplomarbeit ist es, mögliche Erweiterungen, ausgehend von den reellen Zahlen $\mathbb{R}$, genauer unter die Lupe zu nehmen und chronologisch zu beschreiben.
Zunächst wird ein allgemeiner Einblick in den Begriff „Körpererweiterungen“ gegeben. Anschließend wird die Körpererweiterung der reellen Zahlen $\mathbb{R}$ zu den komplexen Zahlen $\mathbb{C}$ beschrieben und die wichtigsten Eigenschaften letzterer werden dargelegt. Ausgehend von dem Körper $\mathbb{C}$, werden dann die vierdimensionalen Quaternionen, sowie die Quaternionenalgebra $\mathbb{H}$ eingeführt.
Zum Abschluss wird noch ein Ausblick über eine mögliche Erweiterung von den Quaternionen, zu den sogenannten Cayley-Zahlen angeschnitten.

Abstract

For the evolution of mathematics like we know it today, the role of extending the range of numbers was of particular importance. Disciplines like physics and engineering wouldn't have reached today's state of the art, without constant development and evolution of the range of numbers.
Beginning with the natural numbers $\mathbb{N}$, the sets of numbers gradually grew. Seen from a historical perspective, the journey of whole numbers to negative, rational, real and complex numbers all the way to the four-dimensional quaternions has been long and troubled with uncertainty and major difficulties.

Purpose of this thesis is to observe possible extensions from the real numbers $\mathbb{R}$ more precisely and describe them chronological.
Starting with an introduction and overview to field extensions, it continuous describing the extension of real numbers $\mathbb{R}$ to complex numbers $\mathbb{C}$. The most important characteristics of complex numbers will be described in detail. Based on the field $\mathbb{C}$, the four-dimensional quaternions as well as the algebra of quaternions $\mathbb{H}$ will be introduced.
In conclusion, there will be a prospect to a possible extension of the quaternions, the Caylay-numbers.

Danksagung

An dieser Stelle möchte ich die Gelegenheit nutzen, um einigen Personen meinen herzlichsten Dank auszusprechen.

In erster Linie möchte ich mich bei meinem Diplomarbeitsbetreuer ao. Univ.-Prof. Mag. Dr. Günther Hörmann für die außerordentlich kompetente und stets motivierende Unterstützung bedanken. Ohne Ihr rasches Korrekturlesen und Ihre konstruktiven Hilfestellungen, wäre es mir niemals möglich gewesen, diese Arbeit in solch einer kurzen Zeit zu verfassen.

Außerdem möchte ich auch meinem Partner René von ganzem Herzen danken. Ohne dich hätte ich die Nerven im Laufe des Studiums unzählige Male geschmissen. Danke, dass du immer mit voller Zuversicht an mich glaubst und die wichtigste Stütze für mich darstellst.

Zu guter Letzt möchte ich mich natürlich auch bei meinen Eltern (Maria und Peter) bedanken. Von Anfang an habt ihr mich in jedem meiner Schritte unterstützt. Ihr habt mir immer wieder das Gefühl vermittelt, dass ich alles schaffen könnte und habt keine Sekunde an mir gezweifelt. Danke für alles!

Inhaltsverzeichnis

Kapitel 1

Körpererweiterungen im Allgemeinen

In der Algebra stellt die Frage nach dem Auffinden von Nullstellen von Polynomen ein grundlegendes Problem dar. Man möchte herausfinden, ob Polynome Nullstellen besitzen und wenn ja, wie man diese bestimmen kann.
Hier möchte ich gleich mit einem Beispiel starten:

Beispiel 1.1 *Sei $K = \mathbb{Q}$ der Körper der rationalen Zahlen und $f(x) = x^2 - 2$ ein Polynom, so sieht man auf den ersten Blick, dass das Polynom keine Nullstellen in $\mathbb{Q}$ hat, da $\sqrt{2}$ eine irrationale Zahl ist. Um die Nullstellen dieses Polynoms trotzdem bestimmen zu können, gibt es nun die Möglichkeit, den Körper $\mathbb{Q}$ zum Körper $\mathbb{R}$ der reellen Zahlen zu erweitern. Wenn man das macht, so hat das angeführte Polynom $f(x) = x^2 - 2$ die Nullstellen $\pm\sqrt{2}$ (vgl. [3]S.291).*

Diese Erweiterung zum Lösen des Problems nennt man **Körpererweiterung**. Um den Begriff „Körpererweiterung“ jedoch in seinen vollen Ausmaßen verstehen zu können, sollten nun einige Definitionen und Begrifflichkeiten eingeführt werden.
In diesem ersten Kapitel stellt das "Lehrbuch der Algebra"von Gerd Fischer (vgl. Quelle [3]) die Hauptliteraturquelle dar, da es einen gut strukturierten Einblick in das Thema „Körpererweiterungen“ bietet.

1.1 Körper

Zur Erinnerung wird zunächst auch noch die Definition eines Körpers gegeben (vgl. [3], S.174), da es für das Verständnis dieser Arbeit unumgänglich ist, diesen Begriff exakt zu kennen .

Definition 1.1 *Ein Körper ist eine Menge K, die zusammen mit den beiden Abbildungen $+ : K \times K \to K$ und $\cdot : K \times K \to K$, den sogenannten Verknüpfungen in K, folgendes erfüllt:*

- *(K,+) ist eine abelsche Gruppe mit 0 als neutralem Element und Inversem $-a$ von a.*
- *$K \setminus \{0\}$ ist bezüglich der Multiplikation eine abelsche Gruppe mit 1 als neutralem Element und a^{-1} als Inversem von a.*
- *Es gilt das Distributivgesetz: $a, b, c \in K$, also $a \cdot (b + c) = a \cdot b + a \cdot c$*

Körper werden stets als Tripel $(K, +, \cdot)$ angeschrieben. Beispiele für Körper stellen $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$ und $(\mathbb{C}, +, \cdot)$ dar.
Wenn die Kommutativität bezüglich der Multiplikation nicht gewährleistet ist, die restlichen Anforderungen an einen Körper jedoch erfüllt sind, so nennt man die Struktur einen **Schiefkörper** (vgl.[3] S.174). Der Begriff des Schiefkörpers wird uns in Kapitel 4 bei den Quaternionen noch begegnen.

1.2 Körpererweiterungen

Nun wollen wir aber tatsächlich zum Begriff „Körpererweiterungen“ kommen. In Gerd Fischers „Lehrbuch der Algebra“ (vgl. [3] S.293) wird der Begriff Körpererweiterung folgendermaßen definiert:

Definition 1.2 *Ist $L \subset K$ ein Unterkörper, so spricht man aus der Sicht von L von einer **Körpererweiterung**.*

Dabei wird der Begriff Unterkörper so beschrieben:

Definition 1.3 *Ist K ein Körper und $S \subset K$ eine Teilmenge, dann nennt man S Unterkörper von K, falls folgendes gilt:*

- *Für $a, b \in S$ ist auch $a + b \in S$ und $a \cdot b \in S$.*
- *S bildet mit den Verknüpfungen $+$ und $\cdot$ ebenfalls einen Körper.*

Es gibt für Körpererweiterungen verschiedene Schreibweisen, die in dieser Arbeit verwendete ist $K \supset L$. Man nennt hierbei L den Unterkörper und K den Oberkörper der Körpererweiterung.

Beispiel 1.2 *Vom Körper der rationalen Zahlen $\mathbb{Q}$ ist der Körper der reellen Zahlen $\mathbb{R}$ ein Oberkörper, es gilt also $\mathbb{R} \supset \mathbb{Q}$ ist eine Körpererweiterung.*

Enthält ein Körper K keinen Unterkörper, welcher eine echte Teilmenge von K ist, so nennt man diesen Körper K einen **Primkörper**. Diese Primkörper sind die „elementaren Bausteine“ für alle anderen Körper (vgl.[1]). Der Primkörper wird in Quelle [6] mit Hilfe des Durchschnittes aller Teilkörper eines Körpers K angegeben. Denn damit kann man den kleinsten Teilkörper, also den Primkörper, von K finden.

$$P = \bigcap \{U : U \text{ ist Teilkörper von K}\}$$

Aufgrund der Benennung (Oberkörper und Unterkörper) erscheint es nicht überraschend, dass es auch **Zwischenkörper** geben kann. Zwischenkörper werden in [3] folgendermaßen beschrieben:

Definition 1.4 *Man nennt einen Körper F Zwischenkörper von L und K, wenn $L \subset F \subset K$ gilt. L und F sind also Unterkörper von K und L ist ebenfalls Unterkörper von F.*

Die reellen Zahlen sind beispielsweise ein Zwischenkörper zwischen den rationalen und den komplexen Zahlen. Später werden wir zeigen, dass es keinen Zwischenkörper zwischen den reellen und komplexen Zahlen geben kann.

Charakteristik

Sei R ein Ring mit 1 und

$$\varphi : \mathbb{Z} \to R,\ n \mapsto n \cdot 1,$$

ein Ringhomomorphismus mit $n \in \mathbb{N}$. Weiters sei $a \in R$. Dann definiert man $n \cdot a := a + ... + a$ (n-mal) und $(-n) \cdot a := n \cdot (-a)$. Da $\varphi : \mathbb{Z} \to \mathbb{R}$ ein Ringhomomorphismus ist, ist Ker(φ) ein Unterring und damit gibt es ein $m \in \mathbb{N}$ mit Ker(φ) = $m\mathbb{Z}$. Falls $m > 0$, dann gilt $m = min\{n \in \mathbb{N} \setminus \{0\} : n \cdot 1 = 0\}$.

Definition 1.5 *Man nennt $char(K) := m$ die Charakteristik des Körpers K.*

Ist die Charakteristik char(K)=0, dann ist $\varphi : \mathbb{Z} \to R$ injektiv.

Satz 1.1 *Die Charakteristik eines endlichen Körpers ist entweder 0 oder eine Primzahl. Also $char(K) = 0$ oder $char(K) \in P$*

Beweis Sei m=char(K) und $m \geq 2$ ($m = 1$ würde 1=0 implizieren, was für einen Körper nicht möglich ist).
Nimm an m wäre nicht prim: Dann existiert eine Zerlegung $k, l \in \mathbb{N} : m = k \cdot l$ mit $1 < k, l < m$. Daher $0 = m \cdot 1 = (kl) \cdot 1 = (k \cdot 1) \cdot (l \cdot 1)$. Somit gilt $k \cdot 1 = 0$ oder $l \cdot 1 = 0$ und das ist ein Widerspruch zur Minimalität der Charakteristik m (vgl. [3] S.292).

□

Grad der Körpererweiterung

Die „Größe“ einer Körpererweiterung kann man mit Hilfe des Grades der Erweiterung angeben. Dabei muss man bei einer Körpererweiterung $K \supset L$ den Oberkörper K als Vektorraum über L betrachten (vgl. [3] S.293).

Definition 1.6 *Die Dimension $dim_L(K)$ des L Vektorraums K heißt Grad der Körpererweiterung $K \supset L$, geschrieben [K:L]. Ist [K:L] endlich, dann nennt man die Körpererweiterung $K \supset L$ endlich.*

(vgl. [8] S. 250)

Das für diese Arbeit wichtigste Beispiel, ist dabei der Grad der Erweiterung von den reellen zu den komplexen Zahlen.

Beispiel 1.3 *Da $\{1, i\}$ eine $\mathbb{R}$-Basis von $(\mathbb{C}, +)$ darstellt, gilt $[\mathbb{C} : \mathbb{R}] = 2$*

(vgl. [6], S.210).

Im Zusammenhang mit dem Körpergrad, ist der folgende Satz äußerst bedeutsam (vgl. [3],S.294):

Satz 1.2 (Gradsatz) *Sei F ein Zwischenkörper der Körpererweiterung von L und K, also $L \subset F \subset K$ dann gilt: $[K : L] = [K : F] \cdot [F : L]$.*

Beweis (vgl.[6], S.211) Es ist zu zeigen: Wenn $(v_i)_{i\in I}$ eine Basis von K über F und $(w_j)_{j\in J}$ eine Basis von F über L ist, dann ist $(w_j v_i)_{(j,i)\in J\times I}$ eine Basis von K über L.

Dabei soll zuerst gezeigt werden, dass $(w_j v_i)_{(j,i)\in J\times I}$ ein Erzeugendensystem ist. Die im Beweis vorkommenden Summen haben nur endlich viele Summanden $\neq 0$. Jedes beliebige $a \in K$ kann geschrieben werden als $a = \sum_{i\in I} f_i v_i$, wobei jedes $f_i \in F$ die Form $f_i = \sum_{j\in J} l_{ij} w_j$ mit $l_{ij} \in L$ aufweist. Damit gilt

$$a = \sum_{(i,j)\in I\times J} l_{ij} w_j v_i.$$

Nun fehlt noch der Beweis, dass $(w_j v_i)_{(ji)\in J\times I}$ linear unabhängig über L ist. Dazu sei für $l_{ij} \in L$ die Summe

$$\sum_{(ij)\in I\times J} l_{ij} w_j v_i = 0.$$

Anders angeschrieben bedeutet das $\sum_{i\in I}(\sum_{j\in J} l_{ij} w_j) v_j = 0$. Weil $(v_i)_{i\in I}$ eine Basis von K über F ist, folgt daraus, dass $\sum_{j\in J} l_{ij} w_j = 0$ ist für alle $i \in I$. Es ist $l_{ji} = 0$ für alle i, j, weil $(w_j)_{j\in J}$ eine Basis von F über L ist.
Damit ist $(w_j v_i)_{(ji)\in J\times I}$ linear unabhängig über L.

□

Aus der Gradformel folgt direkt ein Korollar, mit dessen Hilfe gezeigt werden kann, dass es zwischen den reellen Zahlen und den komplexen Zahlen keine echten Zwischenkörper geben kann. Darauf wird im Kapitel 3 näher eingegangen.

Adjunktion von Elementen

Sei L ein Unterkörper von K. Der kleinste Zwischenkörper, welcher eine bestimmte Teilmenge $A \subset K$ enthält, kann mit folgender Formel angegeben werden:

$$L(A) := \bigcap_{L\cup A\subset F\subset K} F$$

Hierbei durchläuft F alle Unterkörper von K, die sowohl L als auch A beinhalten.

L(A) wird nun der von A über L erzeugte Unterkörper von K genannt. L(A) entsteht durch Adjunktion von A an L, wobei man unter Adjunktion das Hinzufügen von Elementen zu einem Körper versteht.
Für den Fall, dass die Körpererweiterung von nur einem einzigen Element a erzeugt wird, so nennt man a ein primitives Element. Die Körpererweiterung $K \supset L$ wird in diesem Fall **einfache Körpererweiterung** genannt (vgl. [3] S.295,296).

1.3 Algebraische und transzendente Körpererweiterungen

Es gibt verschiedene Arten von Körpererweiterungen . Im kommenden Abschnitt möchte ich zwischen algebraischen und transzendenten Körpererweiterungen unterscheiden und deren Eigenschaften erklären. In diesem Unterkapitel wird bei den Definitionen, Beispielen und Bemerkungen in erster Linie Bezug auf [3] (S.297ff) genommen.

Algebraische Körpererweiterungen

Definition 1.7 *Sei K ein Körper mit dem Unterkörper L. Dann nennt man die Körpererweiterung $K \supset L$ algebraisch, sofern jedes $a \in K$ algebraisch über L ist.*

Ein Element $a \in K$ bezeichnet man dann als **algebraisch über L**, wenn gilt:

$$\exists f \in L[X] \setminus \{0\} : f(a) = 0$$

Hierbei ist L[X] der Ring aller Polynome über dem Körper L.
In Worten ausgedrückt heißt das also, dass a dann ein algebraisches Element ist, wenn a Nullstelle eines Polynoms vom Grad ≥ 0 ist.

Bemerkung 1.1 *$\forall a \in L$: a ist algebraisch über L, denn $f = X - a \in L[X]$ hat eine Nullstelle in a.*

Beispiel 1.4 *Da jede komplexe Zahl der Form $z = a + bi$ Nullstelle des Polynoms*

$$f := (X - z)(X - \bar{z}) = X^2 - 2aX + a^2 + b^2 \in \mathbb{R}[X]$$

ist, ist die Erweiterung $\mathbb{C} \supset \mathbb{R}$ eine algebraische Körpererweiterung.

Es kann gezeigt werden, dass jede endliche Körpererweiterung stets algebraisch ist. Die Umkehrung ist jedoch nicht immer gültig, eine algebraische Körpererweiterung muss also nicht unbedingt endlich sein (vgl. [3], S.307).

Bemerkung 1.2 *Die Eigenschaft „algebraisch“ einer Körpererweiterung ist transitiv. Das heißt:*
Sind die Körpererweiterungen $K \supset L$ und $L \supset F$ algebraisch und ist $K \supset L \supset F$ ein Zwischenkörper, dann ist $K \supset F$ ebenfalls algebraisch (vgl. [6], S.230).

Transzendente Körpererweiterungen

Wenn eine Körpererweiterung nicht algebraisch ist, so ist sie **transzendent**.

Definition 1.8 *Sei K ein Körper mit dem Unterkörper L. Dann nennt man die Körpererweiterung $K \supset L$ transzendent, sofern mindestens eines der Elemente $a \in K$ transzendent (und somit nicht algebraisch) über L ist.*

Ein Element $a \in K$ wird als transzendent über L bezeichnet, wenn

$$\nexists f \in L[X] \setminus \{0\} : f(a) = 0.$$

a ist in diesem Fall also nicht Nullstelle eines Polynoms vom Grad ≥ 0.

Beispiel 1.5 *Als Beispiele für transzendente Elemente in $\mathbb{R}$ über $\mathbb{Q}$ wären e und π zu nennen ([3], S.297). Eine transzendente Körpererweiterung ist die Erweiterung $\mathbb{R} \supset \mathbb{Q}$ ([3], S.306).*

Unterscheidung zwischen algebraischen und transzendenten Elementen

Betrachtet man den Einsetzungshomomorphismus $\sigma_a : L[X] \to K$, $f \mapsto f(a)$, für $a \in K$, so kann man algebraische und transzendente Elemente differenzieren. Es gelten folgende Relationen:

$$\text{a transzendent über L} \Leftrightarrow \text{Ker } \sigma_a = \{0\} \Leftrightarrow \sigma_a \text{ injektiv.}$$

Ist a transzendent über L, so ist das äquivalent zu der Aussage, dass für jedes $n \in \mathbb{N}$ $1,a,a^2,...,a^n$ linear unabhängig über L sind.

$$\text{a algebraisch über L} \Leftrightarrow \text{Ker } \sigma_a \neq \{0\} \Leftrightarrow \sigma_a \text{ nicht injektiv.}$$

Ist a algebraisch über L, so ist das äquivalent zu der Aussage, dass für ein geeignetes $n \in \mathbb{N}$ $1,a,a^2,...,a^n$ linear abhängig über L sind (vgl. [3] S.297).

1.3.1 Minimalpolynom

Sei $K \supset L$ eine Körpererweiterung und $a \in K$ algebraisch über L. Da $L[X]$ ein Hauptidealring ist[1], gibt es ein eindeutig bestimmtes normiertes Polynom $f_a \in L[X]$ vom Grad deg $(f_a) \geq 1$ für das gilt: $\text{Ker}(\sigma_a) = (f_a)$. Man sagt f_a ist das **Minimalpolynom von a über L**.

Eigenschaften des Minimalpolynoms

Satz 1.3 *Für eine Körpererweiterung $K \supset L$ mit $a \in K$ und $f \in Ker(\sigma_a)$ normiert, sind folgende Bedingungen äquivalent (vgl. [3], S.299):*

1) *f ist das Minimalpolynom von a über L.*
2) *Für jedes $0 \neq g \in Ker(\sigma_a)$ gilt $deg(g) \geq deg(f)$*
   (daraus ergibt sich der Name „Minimalpolynom“).
3) *f ist irreduzibel in L[X].*

Diesen Satz wollen wir nun beweisen:

Beweis (Vgl. [3], S.299)
1) $\Rightarrow$ 2):
f ist das Minimalpolynom f_a und $g \in \text{Ker}(\sigma_a) = (f_a)$. Daher gibt es zu g ein $h \in L[X]$

[1] Der Polynomring $K[X]$ über einem Körper K, ist ein Hauptidealring (vgl. [3], S.216).

mit $h \neq 0$, sodass $g = h \cdot f_a$.
Damit ist $\deg(g) = \deg(h \cdot f_a) = \deg(h) + deg(f_a) \geq \deg(f_a)$.

2) $\Rightarrow$ 3):
Es sei $f = g \cdot h$, wobei $g, h \in L[X]$ gilt. Daher gilt $0 = f(a) = g(a) \cdot h(a)$, weshalb entweder $g \in \mathrm{Ker}(\sigma_a)$ oder $h \in \mathrm{Ker}(\sigma_a)$.

Da nun (nach Aussage 2)) $\deg(f) \leq \deg(g)$ oder $\deg(f) \leq \deg(h)$ gelten muss, muss g oder h den Grad 0 haben, dies bedeutet, dass $g \in L^\times$ oder $h \in L^\times$.

3) $\Rightarrow$ 1):
Da $f \in \mathrm{Ker}(\sigma_a) = (f_a)$, gibt es ein $h \in L[X] \neq 0$, sodass $f = h \cdot f_a$ gilt. Da der Grad von $f_a \geq 1$ sein muss, ist $f_a \notin L^\times$. Daher muss (nach Aussage 3)) $h \in L^\times$ gelten. Da sowohl f als auch f_a normiert sind, kann man daraus schließen, dass $h = 1$ und somit $f = f_a$.

□

Eine wichtige Eigenschaft des Minimalpolynoms ist folgende:
Der Grad des Minimalpolynoms $\deg f_a$ kann folgendermaßen angegeben werden:

$$[k(a) : k] = \deg\, f_a.$$

Im Kapitel 3 wird dann das Minimalpolynom für die Körpererweiterung der reellen zu den komplexen Zahlen $\mathbb{C} \supset \mathbb{R}$ beschrieben.

Kapitel 2

Der algebraische Abschluss

Zu Beginn des ersten Kapitels wurde beschrieben, dass das Auffinden von Nullstellen von Polynomen eines der bedeutsamsten Themen in der Algebra darstellt. Beim Beispiel 1.1 wurde das Problem, dass das angegebene Polynom in $\mathbb{Q}$ keine Nullstellen aufweist einfach dadurch behoben, dass der Körper der rationalen Zahlen zum Körper der reellen Zahlen erweitert wurde.
Nun kommt jedoch die Frage auf, ob zu jedem Körper K eine Erweiterung gefunden werden kann, sodass die Nullstellen von vorgegebenen Polynomen in diesem Erweiterungskörper liegen.
In diesem Kapitel soll gezeigt werden, dass es möglich ist, zu jedem Körper eine Erweiterung zu finden, sodass ein beliebiges Polynom aus K[X] in besagtem Erweiterungskörper in Linearfaktoren zerfällt.
Die wichtigste Literatur für dieses Kapitel stellen die Lehrbücher [3](S. 309ff), [4](S.137ff) sowie [6](S.241ff) dar.

2.1 Algebraisch abgeschlossene Körper

Definition 2.1 *Sei K ein Körper. Dann bezeichnet man K als* ***algebraisch abgeschlossen****, wenn jedes nicht konstante Polynom f (grad $f \geq 1$) mit Koeffizienten in K mindestens eine Nullstelle im Körper K aufweist (vgl. [4] S.137).*

Beschreibung für algebraisch abgeschlossene Körper (vgl. [6], S.241):

Lemma 2.1 *Für einen Körper K sind die folgenden Bedingungen äquivalent:*

1) *Der Körper K ist algebraisch abgeschlossen.*
2) *Alle Polynome $P \in K[X]$ zerfallen über K.*
3) *Jedes irreduzible Polynom $P \in K[X]$ hat Grad 1.*
4) *Für eine algebraische Erweiterung von K gilt: es gibt keinen algebraischen Erweiterungskörper $\neq K$.*
5) *Wenn der Grad einer Körpererweiterung $[L : K] \in \mathbb{N}$ ist, so gibt es keinen Erweiterungskörper von K für den $K \neq L$ gilt.*

(Der Beweis hierzu kann in [6], S.241-242 nachgelesen werden.)

Sei nun K ein algebraisch abgeschlossener Körper und f ein Polynom vom Grad $\deg f = n \geq 1$ mit Koeffizienten in K, dann hat f eine Nullstelle in K. Diese Nullstelle wird nun x_1 genannt. Dann kann man f als $f = (X - x_1)g$ darstellen, wobei $g \in K[X]$ und $deg(f) > deg(g)$ ist. Ist der Grad von $g \geq 1$, dann hat auch g eine Nullstelle x_2 im Körper K. Wenn man so weiterhin fortfährt, erhält man nach n Schritten folgende Zerlegung:

$$f = f_0 \cdot (X - x_1) \cdot ... \cdot (X - x_n).$$

Bemerkung 2.1 *Damit kann bewiesen werden, dass jeder algebraisch abgeschlossene Körper unendlich ist, denn:*
Angenommen der Körper wäre endlich, dann wäre $K = a_0, a_1, ..., a_n$. Es wäre dann $f := (X - a_0) \cdot (X - a_1) \cdot ... \cdot (X - a_n) + 1$ ein Polynom, das keine Nullstelle im Körper K hat.

2.1.1 Der Fundamentalsatz der Algebra

Einen äußerst bedeutsamen Satz im Zusammenhang mit algebraisch abgeschlossenen Körpern, stellt der **Fundamentalsatz der Algebra** dar.

Satz 2.1 ***Fundamentalsatz der Algebra:*** *Der Körper der komplexen Zahlen $\mathbb{C}$ ist algebraisch abgeschlossen.*

Die Ironie hinter diesem Satz besteht darin, dass es dafür keinen rein algebraischen Beweis gibt. Dies hängt damit zusammen, dass die komplexen Zahlen eine Körpererweiterung der reellen Zahlen darstellen. Die reellen Zahlen werden jedoch durch Mittel aus der Analysis begründet (vgl. [3], S.310).
Trotzdem soll nun ein Beweis dafür gegeben werden, angelehnt daran, wie er in Quelle [3] (S. 310) geführt wird.

Beweis 2.1 *Man verwendet hierbei die Theorie von holomorphen Funktionen.* [1]
Angenommen ein Polynom f sei definiert als

$$f := X^n + a_{n-1}X^{n-1} + ... + a_1X + a_0 \in \mathbb{C}[X] \text{ mit } n \geq 1.$$

Wenn $\forall z \in \mathbb{C}$: $f(z) \neq 0$, dann ist $\frac{1}{f}$ holomorph in $\mathbb{C}$. Für X^n gilt folgende Eigenschaft:

$$\exists R > 0 \in \mathbb{R}, \text{ mit } \tfrac{1}{2}|z|^n \leq |f(z)| \leq \tfrac{3}{2}|z|^n \text{ für } |z| \geq R.$$

Somit gilt

$$|\tfrac{1}{f}| \leq \tfrac{2}{R^n} \text{ in } \{z \in \mathbb{C} : |z| \geq R\}.$$

Weiters ist $|\frac{1}{f}|$ beschränkt auf der kompakten Menge $\{z \in \mathbb{C} : |z| \leq R\}$, weil $\frac{1}{f}$ stetig ist. Insgesamt gilt also

$$\tfrac{1}{f} \text{ ist holomorph und } |\tfrac{1}{f}| \text{ ist in } \mathbb{C} \text{ beschränkt.}$$

[1] Als holomorphe Funktion wird in der Funktionentheorie eine (komplexe) Funktion f auf der offenen Menge $U \subset \mathbb{C}$ bezeichnet, wenn f in allen $z_0 \in U$ komplex differenzierbar ist (vgl. [5], S.15).

Laut dem Satz von Liouville[2] *ist* $\frac{1}{f}$ *und somit f konstant. Dies ist ein Widerspruch zu der Annahme, dass der Grad* $deg f \geq 1$ *ist.*

□

2.2 Algebraischer Abschluss

Definition 2.2 *Eine algebraische Körpererweiterung* $\bar{k} \supset k$ *nennt man* ***Algebraischer Abschluss****, falls* $\bar{k}$ *algebraisch abgeschlossen ist (vgl. [3] S.311) .*

hmm Angenommen eine Körpererweiterung $K \supset L$ und eine Menge $\bar{K}$, bestehend aus all jenen Elementen aus K, welche algebraisch über L sind, werden betrachtet. So stellt diese Menge $\bar{K}$ einen Körper dar. Es gilt $K \supset \bar{K} \supset L$ und $\bar{K}$ bildet den algebraischen Abschluss von L in K (vgl. [4], S.137-138).

Existenz des algebraischen Abschlusses

Im Folgenden soll gezeigt werden, dass jeder beliebige Körper einen algebraischen Abschluss besitzt. Hierbei wird auf [6] (S. 243ff) zurückgegriffen.

Satz 2.2 (Satz von Steinitz) *Jeder Körper K besitzt einen algebraischen Abschluss.*

Beweis-Skizze
Für den Beweis wird in [6] das Zorn'sche Lemma vorausgesetzt.[3] Es gibt eine überabzählbare Menge S, für die gilt $K \subseteq S$ und $|K| < |S|$.
Nenne χ die Menge aller Erweiterungskörper L von K, die algebraisch über K sind und für die $L \subseteq S$ gilt. Diese Menge ist offensichtlich nicht leer, da $K \in \chi$ gilt.
Definiere folgende Relation für $L, L' \in \chi$:

$$L \leq L' :\Leftrightarrow L \text{ ist ein Teilkörper von } L'.$$

Diese zweistellige Relation ist transitiv, reflexiv und antisymmetrisch, also eine Ordnung auf χ.

Nun kann man zeigen:

1) **Dass** $(\chi, \leq)$ **induktiv geordnet ist.**
   $\kappa \neq 0$ bezeichne eine Kette in $(\chi, \leq)$ und $T := \bigcup_{L \in \kappa} L$. Für $a, b \in T$ $\exists L := (L, +, \cdot) \in \kappa$, sodass $a, b \in L$. L ist ein Körper. Die folgenden Operationen werden nun definiert: $a \oplus b := a + b$ und $a \odot b := a \cdot b$ für $a, b \in T$, wobei diese Definition unabhängig davon ist, wie man L wählt. Man kann sehr leicht zeigen, dass $(T, \oplus, \odot)$ einen Körper darstellt.
   Beispielsweise kann man die Assoziativität zeigen: $\forall a, b, c \in T$: $\exists E \in \kappa$ mit $a, b, c \in E$, sodass $a \odot (b \odot c) = a \cdot (b \cdot c) = (a \cdot b) \cdot c = (a \odot b) \odot c$. Es können auch alle

[2] Der Satz von Liouville lautet: Jede beschränkte ganze Funktion im $\mathbb{C}^n$ ist konstant (vgl. [5], S. 97).
[3] Zorn'sches Lemma: Jede nichtleere induktiv geordnete Menge hat ein maximales Element (vgl. [6], S.336).

anderen Körperaxiome nachgewiesen werden.
$T \subseteq S$ ist ein Erweiterungskörper für alle $L \in \kappa$. Die Körpererweiterung $T \supset K$ ist algebraisch, weil alle $L \in \kappa$ algebraisch über K sind. Damit folgt $T \in \chi$ und damit ist T eine obere Schranke von κ. Damit ist 1) gezeigt.

- Aus Punkt 1) und dem Zorn'schen Lemma kann gefolgert werden, dass $(\chi, \leq)$ ein maximales Element M besitzt

2) **Dass M algebraisch abgeschlossen ist**.
Dies wird indirekt bewiesen, also nimmt man an, dass M nicht algebraisch abgeschlossen ist. Dann folgt aus dem Lemma 4.2, dass ein algebraischer Erweiterungskörper $M \neq M'$ von M existiert. M' muss nicht unbedingt Teilmenge von S sein, daher muss M' nicht notwendigerweise in χ liegen. Es soll nun ein isomorphes Bild von M' in S gefunden werden. Die Menge S ist als überabzählbar definiert und $|K| < |S|$, daher folgt [4]

$$|M' \setminus M| \leq |M'| < |S| = |S \setminus M|^{5}.$$

Daher gibt es eine injektive Abbildung $\varphi : M' \to S$ wobei $\varphi|_M = Id_M$. Überträgt man die Operationen von $M'(+' \text{ und } \cdot')$ auf $\varphi(M')$, so erhält man $\forall a, b \in M'$:

$$\varphi(a) + \varphi(b) := \varphi(a +' b) \text{ und } \varphi(a) \cdot \varphi(b) := \varphi(a \cdot' b).$$

φ ist ein Isomorphismus von M' auf $\varphi(M')$ und $\varphi(M')$ ist ein algebraischer Erweiterungskörper von M mit $\varphi(M') \neq M$, denn:

$$\text{Sei } a \in M' \text{ und } m_{a,M} = \textstyle\sum_{i=0}^{n} m_i X^i \text{ ein Polynom aus } M[X] \text{ mit Nullstelle a,}$$
$$\text{dann folgt } 0 = \varphi(\textstyle\sum_{i=0}^{n} m_i a^i) = \sum_{i=0}^{n} m_i \varphi(a)^i.$$

Daher ist $\varphi(M')$ algebraisch über K [6]und $\varphi(M') \in \chi$. Das steht im Widerspruch zur Maximalität von M. Damit ist 2) gezeigt und da $M \supset K$ eine algebraische Körpererweiterung ist, ist der Satz von Steinitz gezeigt.

□

[4]Dies folgt aus einem Lemma: $SeiL \supset K$ eine algebraische Körpererweiterung. Falls K unendlich ist, ist $|L| = |K|$ und falls K endlich ist, ist $|L| \leq |\mathbb{N}|$ (vgl. [6], S.223)

[5]Die Tatsache, dass $|S| = |S \setminus M|$ gilt, kann in [6] nachgelesen werden.

[6]Dies folgt aus einem Lemma: Sind $L \supset E$ und $E \supset K$ beides algebraische Körpererweiterungen, dann ist $L \supset K$ ebenfalls eine algebraische Körpererweiterung (vgl. [6], S.222)

2.3 Zerfällungskörper von Polynomen

Ein Zerfällungskörper ist eine möglichst kleine Körpererweiterung, über der ein vorgegebenes Polynom vollständig in Linearfaktoren zerfällt. Die Definitionen, Sätze und Beweise dieses Abschnittes wurden aus Quelle [3] (S.320ff) entnommen.
Dabei wird ein Zerfällungskörper folgendermaßen definiert:

Definition 2.3 *Sei $K \supset L$ eine Körpererweiterung und $f \in L[X]$ ein Polynom mit Grad $n := \deg f \geq 1$. Man nennt $K \supset L$* ***Zerfällungskörper*** *von f über L, falls:*

1) $\exists\ a, x_1, ..., x_n \in K$ mit

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

Das bedeutet, dass f über K in Linearfaktoren zerfällt.

2) K ist bezüglich 1) minimal. Daher gibt es keinen Zwischenkörper $\tilde{K} \neq K$ über dem f in Linearfaktoren zerfällt.

Beispiel 2.1 *Der Körper $\mathbb{C}$ der komplexen Zahlen ist ein Zerfällungskörper von dem Polynom $X^2 + 1 \in \mathbb{R}[X]$.*

Satz 2.3 *Für einen Körper L und ein Polynom $f \in L[X]$ mit $n := \deg f \geq 1$ gilt:*

1) Es existiert ein Zerfällungskörper K von f über L. Dabei ist der Grad des Zerfällungskörpers $K \supset L$ gegeben durch $[K : L] \leq n!$.

2) Seien zwei Zerfällungskörper $K \supset L$ und $F \supset L$ von f über L gegeben. Dann existiert ein Isomorphismus $\psi : K \to F$, durch welchen die Nullstellen von f in K auf die Nullstellen von f in F abgebildet werden und welcher $\psi|L = id_L$ erfüllt.

Man kann also sagen, dass jedes Polynom einen Zerfällungskörper hat. Dieser Zerfällungskörper ist, bis auf Isomorphie, eindeutig festgelegt.

Ein möglicher Beweis für diesen Satz wird in Gerd Fischers Lehrbuch der Algebra (vgl. [3]) auf Seite 321-322 beschrieben.

Kapitel 3

Die komplexen Zahlen

„*Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk*“ (L. Kronecker, Jahresber. DMV 2, S.19).

Im folgenden Kapitel geht es um die wichtigste Körpererweiterung der reellen Zahlen - die komplexen Zahlen. Dabei wird zuerst ihre geschichtliche Entwicklung geschildert und anschließend werden verschiedene Wege zur Realisierung von $\mathbb{C}$ beschrieben. Des Weiteren werden wesentliche Eigenschaften der komplexen Zahlen geschildert.

3.1 Geschichtliches

Schon in der Unterstufe lernt man in österreichischen Gymnasien heutzutage die komplexen Zahlen kennen. Es wird selbstverständlich gelehrt, dass $i = \sqrt{-1}$ eine Lösung der Gleichung $x^2 + 1 = 0$ ist, doch dies konnte man nicht immer so problemlos einsehen und akzeptieren. Offensichtlich hat die angeführte quadratische Gleichung keine Lösung in den reellen Zahlen, daher wurde erstmals die Notwendigkeit der Erweiterung des Zahlenbereiches $\mathbb{R}$ erkannt. Trotz dieser Erkenntnis, war es ein langer Weg, bis die komplexen Zahlen anerkannt und verstanden wurden. Dieser Weg soll hier skizziert werden, wobei hauptsächlich auf das Lehrbuch [2] (S.46ff) Bezug genommen wird.

1. Cardano (1501-1576):

Girolamo Cardano war ein bekannter Mathematiker und Arzt in der Renaissance. Zu dieser Zeit kam der Begriff „imaginäre Größe“ erstmals vor. Cardano beschreibt in seinem Werk *„Artis magnae sive de regulis algebraicis liber unus“* die Lösungen der Gleichung $x(10-x) = 40$ mit $x = 5 \pm \sqrt{-15}$. Die Lösungen hielt er jedoch für unsinnig, weshalb er $\sqrt{-15}$ als „quantitas sophistica“, was so viel wie „formale Zahl“ bedeutet, bezeichnet. Man weiß nicht, ob Cardano über quadratische oder über kubische Gleichungen zu den komplexen Zahlen gekommen ist.

2. Bombelli (1526-1572):

Rafael Bombelli entwickelte die Algebra von Cardano weiter. Er stellte acht Rechenregeln für komplexe Zahlen zusammen. Unter anderem die Regel $(-i)(-i) = -1$ stammt von Bombelli. Er war der erste Mathematiker, welcher das Rechnen mit komplexen Zahlen korrekt lehrte.

3. Descartes (1596-1650), Newton (1643-1727), Leibniz (1646-1716):

René Descartes beschreibt in seinem Werk „*La Géométrie*“ den Unterschied zwischen reell und imaginär.

Laut **Isaac Newton** waren komplexe Wurzeln ein Anzeichen für die Unlösbarkeit einer Gleichung.

Gottfried Wilhelm Leibniz wird die Erkenntnis folgender Beziehung zugeschrieben:

$$\sqrt{1+\sqrt{-3}} + \sqrt{1-\sqrt{-3}} = \sqrt{6}.$$

In der wissenschaftlichen Zeitschrift „Leipiziger Acta Eruditorum“ nennt Leibniz imaginäre Wurzeln eine *„feine und wunderbare Zuflucht des göttlichen Geistes, beinahe ein Zwitterwesen zwischen Sein und Nichtsein"*.

4. Euler (1707-1783):

Die imaginären Größen sind für die nach **Leonhard Euler** benannten „Euler'schen Formeln“

$$\cos x = \tfrac{1}{2}(e^{ix} + e^{-ix}) \text{ und } \sin x = \tfrac{1}{2i}(e^{ix} - e^{-ix})$$

äußerst relevant. Euler rechnete jahrelang korrekt mit den imaginären Zahlen, er konnte jedoch keine richtige Erklärung darüber abgeben, was imaginäre Zahlen eigentlich sind.

5. Wallis (1616-1703), Wessel (1745-1818), Argand (1768-1822):

John Wallis und **Caspar Wessel** waren die ersten Wissenschaftler, welche Theorien über den Zusammenhang zwischen komplexen Zahlen und Punkten der Ebene entwickelten. Die Vorstellungen von Wallis blieben jedoch sehr unklar, weshalb die erste relevante Darstellung vom Norweger Caspar Wessel stammt. Wessel stellte gerichtete Strecken durch komplexe Zahlen dar. Senkrecht zur reellen Gerade führte Wessel eine imaginäre Achse ein und Vektoren wurden in der Ebene als komplexe Zahlen beschrieben. Für diese Vektoren wurden Rechenoperationen geometrisch festgelegt.
Jean Rober Argand deutete komplexe Zahlen ebenfalls geometrisch, jedoch etwas anders als Wessel. Argand beschrieb $\sqrt{-1}$ als eine Drehung um 90° in der Ebene und damit $\sqrt{-1}\sqrt{-1} = -1$ als Spiegelung, also eine Drehung um 180°.

Leider blieben die Arbeiten von allen dieser Wissenschaftler weitgehend unbeachtet und die komplexen Zahlen wurden weiterhin als mystisch und unmöglich angesehen.

Im Absatz 3.2 wird die geometrische Darstellung der komplexen Zahlen genauer beschrieben.

6. Gauß (1777-1855):

Erst **Carl Friedrich Gauß** konnte die Denkweisen über komplexe Zahlen revolutionieren und machte „das Unmögliche möglich“. In seiner Dissertation 1799 verwendete Gauß die Auslegung komplexer Zahlen als Punkte in der Zahlenebene. 1811 schreibt Gauß an Bessel, dass man sich die reellen Größen durch eine unendliche gerade Linie und den Zusammenschluss von reellen und imaginären Größen als unendliche Ebene denken kann. Dabei ist jeder Punkt durch Abzisse (a) und Ordinate (b) festgelegt und jeder Punkt repräsentiert a+bi auf dieselbe Art und Weise (vgl. Werke 8, S.90). Heutzutage nennt man das die Darstellung durch reelle Zahlenpaare, worauf im Kapitel 3.2 noch näher eingegangen wird.
Gauß war der Meinung, dass die Benennung „imaginäre Einheit“ zu einem großen Teil dafür verantwortlich war, dass die komplexen Zahlen so lange als unmöglich und geheimnisvoll angesehen wurden. Gauß Deutung der komplexen Zahlen als Punkte der Zahlenebene nahmen ihnen ihre Mystik und somit erlangten sie das gleiche Recht in der Mathematik wie die reellen Zahlen.

7. Cauchy (1789-1857):

Augustin-Louis Cauchy fasste die komplexen Zahlen (im Unterschied zu Gauß) rein algebraisch auf. Das Rechnen mit komplexen Zahlen wurde von Cauchy mit dem Rechnen von reellen Polynomen modulo des Polynoms $X^2 + 1$ beschrieben. Damit deutete Cauchy den Körper $\mathbb{C}$ als Zerfällungskörper von dem Polynom $X^2 + 1$.

8. Hamilton (1805-1865):

Sir William Rowan Hamilton gab sich mit der geometrischen Beschreibung zum Rechnen mit komplexen Zahlen noch nicht zufrieden. Bei seinen Vorarbeiten zu den Quaternionen (vgl. Kapitel 4) gab Hamilton eine formale Definition für die komplexen Zahlen als geordnete Paare reeller Zahlen. Dabei hat er die Rechenoperationen Addition und Multiplikation so festgelegt, dass das Kommutativgesetz, das Assoziativgesetz und die Distributivgesetze weiterhin gültig waren. Die Definition durch reelle Zahlenpaare wird im Absatz 3.2 beschrieben.

9. Ausblick:

Obwohl es immer noch einige Skeptiker gab, was diesen neuen Zahlenbereich anbelangte, erfuhren die komplexen Zahlen im 19. Jahrhundert dann einen wahrhaftigen Aufschwung. **Bernhard Riemann** (1826-1866) sah die komplexen Zahlen schon als selbstverständlich an.
Schnell fanden die komplexen Zahlen Platz in ihrer Anwendung in der Physik, wo sie heutzutage gar nicht mehr wegzudenken sind. 1823 verwendete **Fresnel** sie in seinen Studien zur Totalreflexion. Heute werden diese, einst als unmöglich bezeichneten, Zahlen unter Anderem in der Quantenmechanik und Elektrotechnik völlig bedenkenlos verwendet.

3.2 Realisierungsmethoden der komplexen Zahlen

Die komplexen Zahlen bilden einen Körper - den Körper $\mathbb{C}$. Im vorherigen Absatz wird beschrieben, dass dieser Körper mit reellen Zahlenpaaren definiert werden kann. Dieser Weg zur Realisierung von komplexen Zahlen, sowie auch einige andere Realisierungsmethoden sollen im kommenden Teil dieser Diplomarbeit beschrieben werden. Auch hier dient Quelle [2] als wichtigste Literatur, des Weiteren wird auch auf Quelle [7](S.331ff) Bezug genommen.

3.2.1 Realisierung durch reelle Zahlenpaare

Definition 3.1 *Die Menge $\mathbb{R} \times \mathbb{R}$ der geordneten reellen Zahlenpaare $z := (x, y)$ bildet bezüglich der weiter unten definierten Addition und Multiplikation einen kommutativen Körper. Diesen Körper nennt man den Körper $\mathbb{C}$ der komplexen Zahlen.*

Nun soll gezeigt werden, dass die Menge der komplexen Zahlen $\mathbb{C}$ tatsächlich einen Körper bildet (vgl. [7], S.331-332).
Dazu wird die **Addition in** $\mathbb{R} \times \mathbb{R}$ definiert mit

$$(x_1, x_2) + (y_1, y_2) := (x_1 + y_1, x_2 + y_2).$$

- Das Assoziativgesetz und das Kommutativgesetz bezüglich der Verknüpfung + gelten aufgrund der komponentenweisen Definition der Addition und, weil die Gruppe $(\mathbb{R}, +)$ abelsch ist.
- Das Element (0,0) stellt offensichtlich das neutrale Element bezüglich der Addition dar.
- Ebenso leicht findet man mit $(-x_1, -x_2)$ das inverse Element zu (x_1, x_2) bezüglich der Addition.

Für die **Multiplikation in** $\mathbb{R} \times \mathbb{R}$ gilt:

$$(x_1, x_2) \cdot (y_1, y_2) := (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1),$$

wobei das Assoziativgesetz, das Kommutativgesetz und das Distributivgesetz gelten.

- Die Gültigkeit des Assoziativgesetzes bezüglich der Multiplikation ist durch eine einfache Rechnung zu verifizieren und kann beispielsweise in [7] (S.331) angesehen werden.
- Ebenso leicht überprüfbar ist das Distributivgesetz:

  Wie beim Assoziativgesetz sind wieder (x_1, x_2) , (y_1, y_2) und (z_1, z_2) gegeben.

$$(x_1, x_2)((y_1, y_2) + (z_1, z_2)) = (x_1(y_1 + z_1) - x_2(y_2 + z_2), x_1(y_2 + z_2) + x_2(y_1 + z_1)) =$$

$$= (x_1y_1 - x_2y_2, x_1y_2 + x_2y_1) + (x_1z_1 - x_2z_2, x_1z_2 + x_2z_1) =$$

$$= (x_1, x_2)(y_1, y_2) + (x_1, x_2)(z_1, z_2),$$

  womit die Gültigkeit des Distributivgesetzes gezeigt wurde.

- Da die Gruppe $(\mathbb{R}, \cdot)$ kommutativ ist, und aufgrund der Symmetrie der Verknüpfung $\cdot$, folgt das Kommutativgesetz bezüglich der Multiplikation.

- Offenbar gibt es ein neutrales Element $e := (1, 0)$.
- Es existiert auch ein Inverses $z^{-1} := (\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2})$ von $z = (x, y) \neq 0$.

Damit ist nun klar, dass die komplexen Zahlen tatsächlich einen Körper bilden.

Betrachtet man nun die injektive Abbildung $\mathbb{R} \to \mathbb{C}$, $x \mapsto (x, 0)$, so sieht man, dass die reellen Zahlen $\mathbb{R}$ einen Unterkörper der komplexen Zahlen $\mathbb{C}$ darstellen. Die Abbildung ist also eine Körpereinbettung.
Jede reelle Zahl x kann nun mit einer komplexen Zahl $(x, 0)$ identifiziert werden. Das neutrale Element des Oberkörpers $\mathbb{C}$ von $\mathbb{R}$ ist das Element $e = (1, 0) = 1$.
Wie schon in Beispiel 1.3 erwähnt, ist der Grad der Körpererweiterung $[\mathbb{C} : \mathbb{R}] = 2$. Das liegt daran, dass $\mathbb{C}$ ein zweidimensionaler, reeller Vektorraum ist (vgl. [2], S.54).

3.2.2 Geometrische Realisierung

Sehr oft werden komplexe Zahlen geometrisch dargestellt und beschrieben. Im vorigen Teil wurde beschrieben, dass die geometrische Interpretation auch in der geschichtlichen Entwicklung der komplexen Zahlen schon oftmals eine Rolle spielte.
Um diese Interpretation sinnvoll einführen zu können, sollte erst der Begriff *„imaginäre Einheit“* definiert werden.

Die imaginäre Einheit i

Definition 3.2 *Man nennt $i := (0, 1) \in \mathbb{C}$ die imaginäre Einheit von den komplexen Zahlen $\mathbb{C}$. Dabei gilt, dass $i^2 = -1$.*

Schon mehrmals wurde erwähnt, dass das Polynom $X^2 + 1$ keine reellen Nullstellen aufweist. Im Komplexen können nun, mit Hilfe der imaginären Einheit, die Nullstellen $-i$ und i des Polynoms genannt werden.
Anhand der Definition der komponentenweisen Addition kann eingesehen werden, dass jedes Element $z = (x, y) \in \mathbb{C}$ geschrieben werden kann als $(x, y) = (x, 0) + (0, 1)(y, 0)$ und das wird üblicherweise geschrieben als

$$z = x + iy \quad \text{mit} \quad x, y \in \mathbb{R}.$$

Definition 3.3 *Sei $z = x + iy$ mit $x, y \in \mathbb{R}$. Dann bezeichnet man x als den **Realteil** von z und y als den **Imaginärteil** von z. Dies schreibt man als $x =: Re(z)$ und $y =: Im(z)$.*

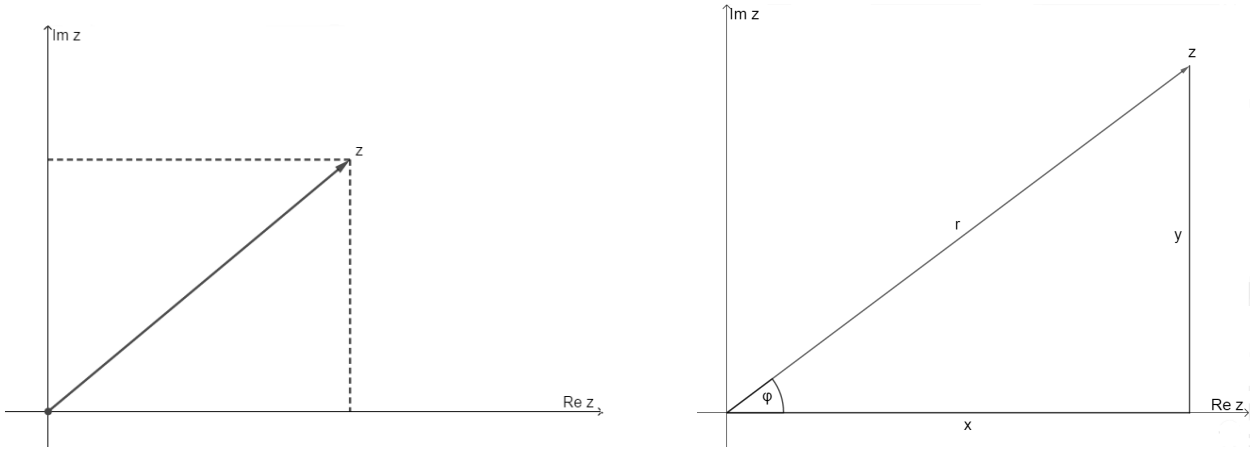
Haben zwei komplexe Zahlen den gleichen Imaginärteil und den gleichen Realteil, so sind diese beiden Zahlen gleich.
Ist der Realteil Re $z = 0$, so nennt man die Zahl **rein imaginär**. Ist der Imaginärteil Im $z = 0$, dann liegt eine **reelle** Zahl vor. Damit ist klar, dass die reellen Zahlen einen Teil der komplexen Zahlen darstellen.

Geometrische Darstellung

Die komplexen Zahlen werden nun in der nach Carl Friedrich Gauß benannten **Gauß'schen Zahlenebene** dargestellt. Dies wird mittels eines Koordinatensystems realisiert, bei welchem auf der x-Achse der Realteil $\mathrm{Re}(z)$ und auf der y-Achse der Imaginärteil $\mathrm{Im}(z)$ aufgetragen wird.

Anstelle der kartesischen Koordinaten können für die komplexen Zahlen auch **Polarkoordinaten** verwendet werden (vgl. [7], S.336). Damit kann jede komplexe Zahl $z = x+iy$ geschrieben werden als: $z = r(\cos\varphi + i\sin\varphi)$.
Dabei ist der Radius r gegeben durch $r = \sqrt{x^2+y^2}$, was aus dem Satz von Pythagoras folgt. Für den Winkel φ gilt: $\tan\varphi = \frac{y}{x}$ mit $\varphi \in [0, 2\pi)$. Dabei nennt man φ das Argument von z (vgl. [7], S.336).

In der Abbildung 3.1 werden diese beiden Möglichkeiten der Darstellung graphisch veranschaulicht.



(a) Komplexe Zahl in der Gauß'schen Zahlenebene

(b) Komplexe Zahlen mit Polarkoordinaten

Abbildung 3.1: Geometrische Darstellung komplexer Zahlen

Man kann mit komplexen Zahlen auch graphisch rechnen. Die Addition wird mit klassischer Vektoraddition gemacht.
In Abbildung 3.2 wird ein Beispiel zur Addition zweier komplexer Zahlen z_1 und z_2 dargestellt.

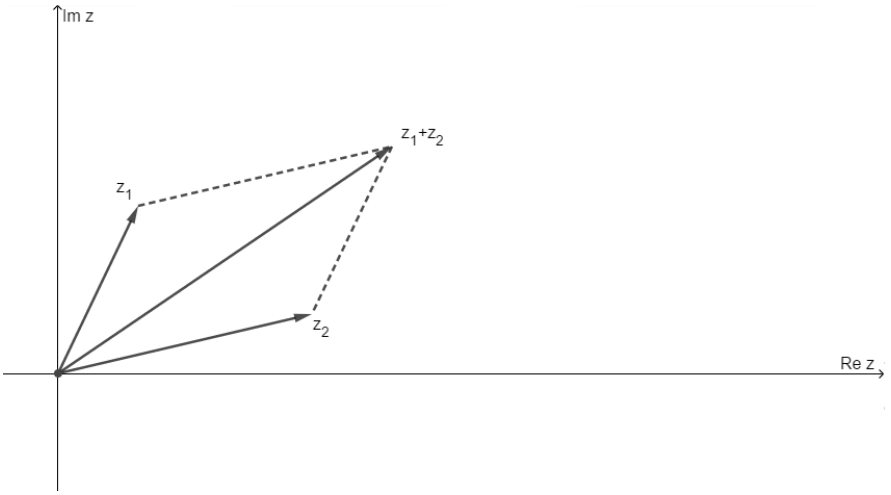


Abbildung 3.2: Geometrische Addition komplexer Zahlen

Man sieht also, dass man komplexe Zahlen $z = x+iy$ geometrisch eindeutig festlegen kann. Gemeinsam mit der Beziehung $i^2 = -1$ folgt daraus, dass die komplexen Zahlen eine zweidimensionale Körpererweiterung der reellen Zahlen sind. $\mathbb{C}$ ist isomorph zum Zerfällungskörper von $X^2 + 1 \in \mathbb{R}[X]$ (vgl. [2], S.55).

3.2.3 Realisierung durch reelle 2×2 Matrizen

Eine andere Methode komplexe Zahlen der Form $z = x + iy$ zu definieren, sind reelle 2×2 Matrizen. Diese Art der Realisierung wird in Lehrbüchern jedoch normalerweise nicht zur Einführung der komplexen Zahlen genutzt.
Hierbei wird allen komplexen Zahlen der Form $c = a + ib$ eine Abbildung

$$T : \mathbb{C} \to \mathbb{C} \quad , \quad z \mapsto cz = ax - by + i(bx + ay)$$

zugeschrieben. Diese Abbildung ist $\mathbb{C}$-linear.

Beschreibt man die komplexen Zahlen $\mathbb{C}$ mittels $\mathbb{R}^2$ und $z = x + iy = \binom{x}{y}$, dann folgt

$$T\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax - by \\ bx + ay \end{pmatrix} = \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}.$$

Nun soll gezeigt werden, dass die Menge $M := \{\begin{pmatrix} a & -b \\ b & a \end{pmatrix} : a, b \in \mathbb{R}\}$ bezüglich der Matrizenaddition und der Matrizenmultiplikation ein kommutativer Körper mit Eins ist.
Dazu betrachtet man nun die $\mathbb{R}$-lineare Abbildung

$$F : \mathbb{C} \to \mathrm{Mat}(2, \mathbb{R}) \ , \ c = a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix},$$

wobei $\mathrm{Mat}(2, \mathbb{R})$ der nicht-kommutative Ring der reellen 2×2 Matrizen ist. Nun sieht man, dass für alle $r, r' \in \mathbb{R}$ und $c, c' \in \mathbb{C}$ folgendes gilt

$$F(rc + r'c') = rF(c) + r'F(c') \quad \text{und} \quad F(cc') = F(c)F(c').$$

Außerdem gilt

$$F(1) = E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

wobei man das Einselement E als Einheitsmatrix bezeichnet. Damit ist die Menge M ein kommutativer Körper mit Eins.

Betrachtet man nun die $\mathbb{R}$-lineare Abbildung

$$F : \mathbb{C} \to M \quad , \quad a + bi \mapsto \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \quad \text{mit} \quad I := F(i) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad , \quad I^2 = -E,$$

wobei I die imaginäre Einheit darstellt, so sieht man, dass F ein Körperhomomorphimus ist.

3.2.4 Isomorphismus $\mathbb{C} \cong \mathbb{R}[X]/(X^2 + 1)$

Es kann gezeigt werden, dass der Quotientenring $\mathbb{R}[X]/(X^2 + 1)$ isomorph zum Körper der komplexen Zahlen $\mathbb{C}$ ist.
Dabei wird wie in [3] (S.211-212) vorgegangen.
Zunächst wird der Ringhomomorphismus $\sigma : \mathbb{R}[X] \to \mathbb{C}$, $f \mapsto \sigma(f) := f(i)$ betrachtet, wobei $\sigma(a + bX) = a + bi$ surjektiv ist. Nun soll gezeigt werden, dass $\text{Ker}\sigma = (X^2 + 1)$ gilt. Dazu wird jedes f mit Rest durch $X^2 + 1$ geteilt:

$$f = (X^2 + 1) \cdot q + r \text{ mit } \deg r \leq 1 \text{ und } r = a + bX,\ a, b \in R.$$

Es folgt, wegen $i^2 + 1 = 0$, dass $f(i) = r(i) = a + bi$ ist. Da $r(i) = 0 \Leftrightarrow r = 0$, folgt

$$\sigma(f) = 0 \Leftrightarrow f = (X^2 + 1)q.$$

Der erste Isomorphiesatz besagt (vgl. [3], S.209):

Satz 3.1 *Wenn $\varphi : R \to R'$ ein Ringhomomorphismus ist, dann ist $\overline{\varphi} : R/Ker\varphi \to \varphi(R)$, $x + Ker\varphi \mapsto \varphi(x)$ ein Isomorphismus. Aus φ ist surjektiv folgt $R' \cong R/Ker\varphi$.*

Nach diesem Satz gilt:

$\overline{\sigma} : \mathbb{R}[X]/(X^2 + 1) \to \mathbb{C}$, $f + (X^2 + 1) \mapsto \sigma(f) = f(i) = r(i)$, ist ein Isomorphismus.

3.3 Körpererweiterung $\mathbb{C} \supset \mathbb{R}$

In Kapitel 1.3 wurde bereits begründet, dass die Körpererweiterung $\mathbb{C} \supset \mathbb{R}$ eine algebraische Körpererweiterung ist. Gleichzeitig ist $\mathbb{C} = \mathbb{R}(i) \supset \mathbb{R}$ ebenfalls das wichtigste Beispiel für eine einfache Körpererweiterung, also eine Körpererweiterung, welche von einem primitiven Element erzeugt wird (vgl. „Adjunktion von Elementen“, Kapitel 1.2). Es gilt $i^2 = -1$ und $X^2 + 1$ ist das Minimalpolynom von i über $\mathbb{R}$.
Für das irreduzible Polynom $f = X^2 + 1 \in \mathbb{Q}[X]$ gilt, dass

$$x := X + (X^2 + 1) \in \mathbb{Q}[X]/(X^2 + 1) =: K,$$

eine Nullstelle ist, weil

$$f(x) = x^2 + 1 = (X^2 + (X^2 + 1)) + (1 + (X^2 + 1)) = X^2 + 1 + (X^2 + 1) = 0 + (X^2 + 1).$$

Ebenso kann man sehen, dass $-x$ auch eine Nullstelle von f in K ist. Der Zerfällungskörper K ist isomorph zum Zerfällungskörper $\mathbb{Q}(i) \subset \mathbb{C}$.
Da $x \in K$, sowie i und $-i$ dasselbe Minimalpolynom $X^2+1 \in \mathbb{Q}[X]$ aufweisen, existieren zwei Isomorphismen

$$\varphi_1, \varphi_2 : K \to \mathbb{Q}(i)$$

für die gilt $\varphi_1(x) = i$ und $\varphi_2(x) = -i$.

Es gibt keinen Körper zwischen $\mathbb{R}$ und $\mathbb{C}$

Schon bei der Einführung des Begriffes Zwischenkörper (Definition 1.4) wurde erwähnt, dass es keinen echten Zwischenkörper zwischen den reellen Zahlen $\mathbb{R}$ und den komplexen Zahlen $\mathbb{C}$ geben kann. Diese Aussage soll im kommenden Absatz bewiesen werden. Dabei wird auf Quelle [3] (S.) Bezug genommen.

Aus der Gradformel (vgl. Satz 1.2) folgt dieses Korollar:

Korollar 3.1 *Sei $L \subset F \subset K$ ein Zwischenkörper und der Grad $[K : L] < \infty$, dann gelten:*

1) *Ist $[K : L] = [K : F]$, dann ist $L = F$.*
2) *Wenn $[K : L]$ prim ist, dann ist $L = F$ oder $F = K$.*

Daraus folgt, dass es keinen echten Zwischenkörper von $\mathbb{C} \supset \mathbb{R}$ gibt.

3.4 Eigenschaften der komplexen Zahlen

3.4.1 Die komplexen Zahlen sind ungeordnet

Um diese Eigenschaft einzuführen, wird zunächst der Begriff „geordneter Körper“ definiert (vgl. [7], S.299-300).

Definition 3.4 *Ist K ein Körper und auch eine totalgeordnete Menge $(K, \leq)$, dann nennt man K **geordneter Körper**, falls für alle $q, r, s \in K$ folgende Bedingungen erfüllt sind:*

- $q \leq r \Rightarrow q + s \leq r + s$
- $q > 0 \wedge r > 0 \Rightarrow qr > 0$

Ist K ein geordneter Körper, so schreibt man $(K, +, \cdot, \leq)$.

Für geordnete Körper gelten die folgenden Rechenregeln:

1) $x \leq y \Leftrightarrow y - x \geq 0$.
2) $-x \geq 0 \Leftrightarrow x \leq 0$.
3) Für $x \geq 0$ und $y \leq z \Rightarrow xy \leq xz$.
4) Für $x < 0$ und $y \leq z \Rightarrow xy \geq xz$.
5) Ist $x \neq 0$, dann ist $x^2 > 0$ und somit $1 > 0$.
6) Aus $0 < x < y$ folgt $0 < y^{-1} < x^{-1}$.

Die Rechenregeln, sowie ein Beweis für ihre Gültigkeit, sind in Quelle [7] (S.300) nachzulesen.

In Quelle [2] (S.56) wird gezeigt, dass die komplexen Zahlen keinen geordneten Körper bilden:

Satz 3.2 *Es existiert keine Ordnungsrelation auf den komplexen Zahlen, womit* $(\mathbb{C}, +, \cdot)$ *zu einem geordneten Körper wird. Das bedeutet, es gibt keine Relation, sodass folgende Bedingungen gelten:*

- $\forall z \in \mathbb{C}$ *gilt* $z > 0$, $z = 0$ *oder* $-z > 0$.
- *Ist* $w > 0$ *und* $z > 0$, *dann gilt* $wz > 0$ *und* $w + z > 0$.

Beweis Gäbe es eine Ordnungsrelation auf den komplexen Zahlen, so würde, analog zu den reellen Zahlen, gelten: $z^2 > 0 \; \forall z \neq 0$. Daher wären somit $1^2 > 0$ und $i^2 > 0$. Insbesondere wäre dann $i^2 + 1 > 0$, was ein Widerspruch ist, da $i^2 + 1 = 0$ gilt.

□

Die Nichtanordenbarkeit der komplexen Zahlen war unter anderem ein Grund dafür, warum sie in ihrer geschichtlichen Entwicklung so lange große Probleme bereitet haben.

3.4.2 Die komplexen Zahlen sind einzigartig

Obwohl die komplexen Zahlen einst als willkürlich und unmöglich angesehen wurden, kann man zeigen, dass sie ganz und gar nicht willkürlich sind. Im Folgenden werden verschiedene Wege aufgezeigt, um zu beweisen, dass die komplexen Zahlen einzigartig sind. Hierbei wird ebenfalls auf Quelle [2] Bezug genommen.

Satz 3.3 *Alle zweidimensionalen, kommutativen, nullteilerfreien Oberringe K von den reellen Zahlen* $\mathbb{R}$ *mit Eins sind isomorph zum Körper der komplexen Zahlen* $\mathbb{C}$.

Beweis (Vgl. [2], S.56) Da $\dim_{\mathbb{R}} K = 2$ gibt es ein $u \in K \setminus \mathbb{R}$. K ist ein reeller Vektorraum und u bildet gemeinsam mit $1 \in \mathbb{R} \subset K$ eine Basis über K. Es gibt $c, d \in \mathbb{R}$, sodass

$u^2 = 1c + (2d)u = c + 2du$, weil $u^2 \in K = \text{span}\{1, u\}$. Sei $v := u - d$, dann ist $v \notin \mathbb{R}$ und $r := c + d^2 \in \mathbb{R}$. Damit ist $v^2 = r$. Für r muss $r < 0$ gelten, da sonst $\sqrt{r} \in \mathbb{R}$ und somit $v = \pm\sqrt{r} \in \mathbb{R}$ wäre. Daher existiert ein $s \in \mathbb{R}$ mit $s^2 = -r^{-1}$ und ein $w := sv \in K \setminus \mathbb{R}$ mit $w^2 = -1$.
Damit ist die Abbildung $\mathbb{C} \to K, \;\; x + iy \mapsto x + wy$ ein Körperisomorphismus.

□

Mit Hilfe des Fundamentalsatzes der Algebra (vgl. Absatz 2.1.1) in Form eines Faktorisierungssatzes, kann ein allgemeinerer **Einzigkeitssatz** für die komplexen Zahlen gezeigt werden (vgl. [2], S.96).

Satz 3.4 *Jeder nullteilerfreie, kommutative Oberring K von $\mathbb{R}$ mit Eins, für den alle Elemente aus K algebraisch über $\mathbb{R}$ sind, ist isomorph zum Körper $\mathbb{R}$ oder zum Körper $\mathbb{C}$.*

Für den nachfolgenden Beweis dieses Satzes, wird der Faktorisierungssatz für reelle Polynome benötigt (vgl. [2], S.94), der wiederrum auf dem Fundamentalsatz der Algebra beruht:

Satz 3.5 *Alle reellen Polynome f mit grad $f = n \geq 1$ im Polynomring $\mathbb{R}[X]$ können eindeutig als*

$$f(X) = a(X - c_1)^{m_1} \cdot \ldots \cdot (X - c_s)^{m_s} q_1(X)^{n_1} \cdot \ldots \cdot q_t(X)^{n_t}$$

geschrieben werden.
Dabei gilt:

- $a \neq 0 \in \mathbb{R}$
- *Für $s, t \in \mathbb{N}$ sind $c_1, \ldots, c_s \in \mathbb{R}$ paarweise verschieden und $m_1, \ldots, m_s, n_1, \ldots, n_t \in \mathbb{N}\backslash\{0\}$ mit $m_1 + \ldots + m_s + 2n_1 + \ldots + 2n_t = n$.*
- *Für $j = 1, \ldots, t$ und $q_1, \ldots, q_t$ sind $q_j(X) = X^2 - b_j X - a_j$ mit $b_j^2 + 4a_j < 0$ paarweise verschieden.*

Der Beweis für den Faktorisierungssatz ist ebenfalls in [2] (S. 94) nachzulesen.

Beweis von Satz 3.4 (Vgl. [2], S.96) Da alle Elemente aus K algebraisch über $\mathbb{R}$ sind, gibt es zu jedem $v \in K \setminus \mathbb{R}$ ein reelles Polynom f mit $f(v) = 0$. Der Oberring K ist nach Definition nullteilerfrei und v annulliert ein Polynom p mit $\deg(p) = 1$ oder $\deg(p) = 2$. Dies folgt aus dem Faktorisierungssatz für reelle Polynome (vgl. Satz 3.5). Das Polynom p ist nicht linear, weil $v \notin \mathbb{R}$ und somit ist $p(X) = X^2 - bX - a$ und damit $v^2 = a + bv$.

Sei nun der Oberring $K \neq \mathbb{R}$ und $v \in K \setminus \mathbb{R}$. Der zweidimensionale reelle Vektorraum $V = \mathbb{R} + \mathbb{R}v$ wird von 1 und v erzeugt, wobei für v, wie oben gezeigt, $v^2 = a + bv$ gilt.

Damit gilt für $x_1 + y_1 v$ und $x_2 + y_2 v \in V$:

$$(x_1 + y_1 v)(x_2 + y_2 v) = (x_1 x_2 + y_1 y_2 a) + (x_1 y_2 + y_1 x_2 + y_1 y_2 b)v \in V.$$

Da V ein nullteilerfreier, kommutativer, zweidimensionaler Oberring von $\mathbb{R}$ ist, ist V isomorph zum Körper $\mathbb{C}$ der komplexen Zahlen (vgl. Satz 3.3).
Nun muss noch die Gleichheit $K = V$ nachgewiesen werden. Dazu wählt man $u \in K \setminus \mathbb{R}$ beliebig. Es existiert ein Polynom $f \in \mathbb{R}[X] \setminus \{0\}$ für das $f(u) = 0$ gilt. Über $\mathbb{C} \simeq V \subset K$ zerfällt das Polynom f in Linearfaktoren $X - c$, $c \in V$. Ein Faktor dieser Art wird von u annulliert, weil K nullteilerfrei ist. Damit ist $u = c \in V$ und somit wurde $K = V \simeq \mathbb{C}$ gezeigt.

□

Aus Satz 3.4 folgt direkt, dass der Körper der komplexen Zahlen $\mathbb{C}$ der einzige echte kommutative algebraische Erweiterungskörper der reellen Zahlen $\mathbb{R}$ ist (bis auf Isomorphie) (vgl. [2], S.97).

Es gibt zwar keinen kommutativen algebraischen Oberkörper $\neq \mathbb{C}$ von den komplexen Zahlen, jedoch konnte Hamilton einen nicht kommutativen Oberkörper der reellen Zahlen beschreiben, nämlich die vierdimensionalen Quaternionen. Auf dieses System wird im Kapitel 4 eingegangen.
Außerdem gibt es noch das System der achtdimensionalen Cayley-Zahlen über $\mathbb{R}$, welche weder die Kommutativität noch die Assoziativität erfüllen, aber noch nullteilerfrei sind.

Bemerkung 3.1 *In [2] (S.42) wird gezeigt, dass auch die reellen Zahlen eindeutig festgelegt sind. Eine Menge $(K, +, \cdot, \leq)$, wobei $+$ und $\cdot$ die inneren Verknüpfungen sind und $\leq$ eine zweistellige Relation ist, nennt man die Menge der reellen Zahlen, genau dann, wenn die folgenden drei Axiome zutreffen (vgl. [2], S.30):*

1) *$(K, +, \cdot)$ ist ein Körper.*
2) *Die lineare Anordnung $\leq$ auf K ist mit Addition und Multiplikation verträglich.*
3) *Alle nichtleeren und nach unten beschränkten Teilmengen $M \subset K$ haben in K ein Infimum.*

Die Menge der rationalen Nullfolgen (also der rationalen Folgen r_n für die $\lim r_n = 0$ gilt) wird N genannt und ist ein Ideal in der Menge F aller rationalen Fundamentalfolgen[1]*. Das bedeutet:*

1) *Sind (r_n) und (s_n) Nullfolgen, ist ist auch $(s_n + r_n)$ eine Nullfolge.*
2) *Ist (r_n) eine Nullfolge und (s_n) eine Fundamentalfolge, dann ist $(r_n \cdot s_n)$ eine Nullfolge.*

Ist die Differenz zweier Fundamentalfolgen gleich Null, so sind die beiden Fundamentalfolgen äquivalent. Die Äquivalenzklasse von (r_n) ist $(r_n) + N := \{(r_n + h_n) : (h_n) \in \mathbb{N}\}$ und wird als Restklasse von r_n modulu N bezeichnet. Da N ein Ideal ist, können Restklassen addiert und multipliziert werden, womit die Menge F/N der Restklassen zu einem kommutativen Ring mit Eins wird.
Es kann gezeigt werden, dass die Restklassen der Fundamentalfolgen modulo den Nullfolgen einen Körper F/N bilden (vgl. [2], S.35).

[1] Man nennt eine rationale Folge r_n Fundamentalfolge oder Cauchyfolge, wenn $\forall \varepsilon > 0$ $\exists$ Index k, sodass $\forall m, n \geq k$ stets $|r_m - r_n| < \varepsilon$ gilt (vgl. [2], S.34)

Sei nun F/N der Cantorsche Körper der Fundamentalfolgen modulo den Nullfolgen, dann gilt folgender Satz:

Satz 3.6 *Jeder angeordnete K, für den die drei oben angeführten Axiome gelten, ist isomorph zu F/N.*

Der Beweis zu diesem Satz kann in [2] (S. 42) nachgelesen werden.

Kapitel 4

Quaternionen

Es hat sich schon im Absatz zur Einzigkeit der komplexen Zahlen (vgl. Kapitel 3.4.2) herauskristallisiert, dass es keinen kommutativen algebraischen Oberkörper $\neq \mathbb{C}$ der komplexen Zahlen gibt. Es gibt jedoch einen nicht kommutativen Oberkörper von $\mathbb{C}$ und zwar die so genannten **Quaternionen**. Auf diese Struktur wird im folgenden Kapitel näher eingegangen.

4.1 Geschichtliches

In der Mathematik waren nun schon viele Zahlenbereichserweiterungen möglich. Die natürlichen Zahlen konnten um die negativen Zahlen erweitert werden, so wie die reellen Zahlen zu den komplexen erweitert wurden.
Mitte des 19. Jahrhunderts stellte sich der Mathematiker und Physiker **Sir William Rowan Hamilton** die Frage, ob es noch eine weitere Vervollständigung der Zahlenbereiche geben kann.
Diese Suche, nach einer Erweiterung der komplexen Zahlen, wird im folgenden Teil dieser Diplomarbeit geschildert. Dabei wird auf die Quellen [2], [7] und [9] Bezug genommen.

In Absatz 3.1 wurde bereits erwähnt, dass Hamilton herausfand, dass komplexe Zahlen durch reelle Zahlenpaare beschrieben werden können. Als nächsten Schritt wollte der Mathematiker dann die zweidimensionalen, komplexen Zahlen zu einem dreidimensionalen Konstrukt erweitern (vgl.[9], S.51).
Das heißt er wollte der Frage nachgehen, ob es eine Körperstruktur auf $\mathbb{R} \times \mathbb{R} \times \mathbb{R} = \mathbb{R}^3$ bzw. sogar auf $\mathbb{R} \times ... \times \mathbb{R} = \mathbb{R}^n$ geben kann (vgl. [7], S.344).

Dazu versuchte Hamilton über viele Jahre hinweg eine Möglichkeit zur Multiplikation reeller Tripel zu finden, doch der Erfolg bei seiner Suche blieb stets aus.
Im Jahr 1843, nach vielen Rückschlägen, wurde Hamilton schließlich klar, dass er von Anfang an einem falschen Ansatz nachging. Anstelle einer dreidimensionalen Struktur, hätte er stets nach einer vierdimensionalen suchen sollen. Noch im Oktober desselben Jahres, stellte Hamilton bei einer Sitzung der Royal Irish Academy seine neue Entdeckung vor.

Er nannte dieses vierdimensionale Konstrukt, welches im folgenden Kapitel noch näher beschrieben werden soll, **Quaternionen**. Hamilton verbrachte seine komplette restliche Laufbahn als Wissenschaftler damit, diese genauer zu studieren und ihre Eigenschaften herauszufinden.

Tatsächlich gelang es Hamilton die Gültigkeit der Produktformel für die Quaternionenmultiplikation zu beweisen. Erst viel später wurde herausgefunden, dass Leonhard Euler die Rechenregeln und insbesondere die Produktformel der Quaternionen schon im Jahr 1748 kannte. Euler erwähnte diese in einem Brief an Goldbach und nannte sie „Vier-Quadrate-Satz".
Auch in einem Werk von Carl Friedrich Gauß aus dem Jahr 1819, welches zur Zeit Hamiltons noch nicht veröffentlicht war, werden die Rechengesetze für Quaternionen bereits beschrieben (vgl. [2], S.157-158).

Hamilton wollte die Quaternionen stets überall verbreiten und war sicher, dass er damit die mathematische Physik revolutionieren könnte.
Oftmals wurde Hamilton als starrsinnig und eingebildet bezeichnet und trotzdem, oder genau deshalb, schaffte er es, dass die Quaternionen im wissenschaftlichen Bereich in aller Munde waren. An der Yale Universität (USA) wurde 1895 sogar eine Vereinigung zur Erforschung der Quaternionen gegründet und wichtige Politiker, wie der ehemalige irische Präsident, besuchten Vorträge zu diesem Thema.
Heutzutage werden die Quaternionen nicht mehr gar so hoch gelobt, wie in damaligen Zeiten, da klar wurde, dass die Quaternionenalgebra nichts anderes ist, als ein Spezialfall der Algebra komplexer 2×2 Matrizen.

Bemerkung 4.1 *(Vgl. [2], S.155)*
Mit dem heutigen mathematischen Wissensstand ist es leicht einzusehen, warum Hamiltons Erfolg bei der Suche nach einer $\mathbb{R}$-linearen Fortsetzung der Multiplikation der Tupel (α, β) von $\mathbb{C} = \mathbb{R}^2$ für die reellen Tripel (α, β, γ) im $\mathbb{R}^3$ ausblieb, denn:

Sei die kanonische Basis des $\mathbb{R}^3$ bezeichnet durch: $e := (1,0,0)$, $i := (0,1,0)$, $j := (0,0,1)$, wobei e das neutrale Element ist. Dann gilt:

$$ij := \rho e + \sigma i + \tau j \text{ mit geeigneten Zahlen } \rho, \sigma, \tau \in \mathbb{R}.$$

Ist nun $i(ij) = (ii)j = -j$ und $i^2 = -e$, dann gilt:

$$-j = i(ij) = i(\rho e + \sigma i + \tau j) = \rho i - \sigma e + \underbrace{\tau ij}_{=\tau(\rho e + \sigma i + \tau j)} = (\tau\rho - \sigma)e + (\tau\sigma + \rho)i + \tau^2 j.$$

Aufgrund dessen, dass e, i, j linear unabhängig sind, ist dann $\tau^2 = -1$ und damit $\tau \notin \mathbb{R}$.

4.2 Definition der Quaternionen

Im Folgenden soll das Konstrukt der Quaternionen allgemein definiert und beschrieben werden.
Die herangezogenen Quellen für diesen Teil sind [2], [6] und [7].

Definition 4.1 *(vgl. [7], S.345)*
Sei $\mathbb{H} := \mathbb{C} \times \mathbb{C}$. *Mit den beiden Verknüpfungen* $+$ *und* $\cdot$, *wird* $\mathbb{H}$ *die Menge der Quaternionen genannt. Die beiden Verknüpfungen werden wie folgt definiert:*

$$(z_0, z_1) + (w_0, w_1) := (z_0 + w_0, z_1 + w_1)$$

$$(z_0, z_1)(w_0, w_1) := (z_0 w_0 - z_1 \overline{w_1}, z_0 w_1 + z_1 \overline{w_0})$$

Schon im ersten Kapitel dieser Diplomarbeit wurde erwähnt, dass die Quaternionen einen sogenannten Schiefkörper bilden.

Definition 4.2 *(Vgl. [6], S.139).*

Ein Ring mit Eins wird als ***Schiefkörper*** *bezeichnet, falls alle Elemente* $\neq 0$ *invertierbar sind. Es muss also* $R^\times = R \setminus \{0\}$ *gelten.*
Ist der Ring mit Eins zusätzlich kommutativ, so spricht man von einem Körper.

Nun soll erklärt werden, warum $(\mathbb{H}, +, \cdot)$ tatsächlich einen Schiefkörper bildet (vgl. [7], S.345):

- $(H, +)$ ist eine abelsche Gruppe, was aus der komponentenweisen Addition folgt.
- Die Quaternionen sind bezüglich der Multiplikation assoziativ, was leicht nachgerechnet werden kann:

$$((z_0, z_1)(w_0, w_1))(v_0, v_1) = (z_0 w_0 - z_1 \overline{w_1}, z_0 w_1 + z_1 \overline{w_0})(v_0, v_1) =$$

$$= (z_0 w_0 v_0 - z_1 \overline{w_1} v_0 - z_0 w_1 \overline{v_1} - z_1 \overline{w_0 v_1}, z_0 w_0 v_1 - z_1 \overline{w_1} v_1 + z_0 w_1 \overline{v_0} + z_1 \overline{w_0 v_0}) =$$

$$= (z_0, z_1)(w_0 v_0 - w_1 \overline{v_1}, w_0 v_1 + w_1 \overline{v_0}) = (z_0, z_1)((w_0, w_1)(v_0, v_1))$$

- Die Distributivgesetze sind ebenfalls gültig, was gleichfalls durch eine Rechnung verifiziert werden kann.
- Die Quaternionen sind bezüglich der Multiplikation jedoch **nicht** kommutativ. Dies wird vor allem anhand von Tabelle 4.1 in Absatz 4.3.1 klar.
- Das neutrale Element bezüglich der Verknüpfung $\cdot$ ist durch $(1, 0)$ gegeben.
- Jedes Element $\neq 0$ in $\mathbb{H}$ besitzt ein Inverses, welches folgendermaßen definiert ist:

$$(z_0, z_1)^{-1} = \left(\frac{z_0}{|z_0|^2 + |z_1|^2}, \frac{-z_1}{|z_0|^2 + |z_1|^2}\right).$$

Aufgrund all dieser algebraischen Eigenschaften, bilden die Quaternionen einen Schiefkörper.

4.3 Realisierungsmethoden der Quaternionen

Wie auch bei den komplexen Zahlen in Kapitel 3.2, gibt es auch für die Quaternionen verschiedene Möglichkeiten, um sie einzuführen.
Zuerst werden sie mittels einer Multiplikationstabelle nach den Hamiltonischen Bedingungen realisiert. Anschließend werden die Quaternionen mittels komplexer 2×2 Matrizen eingeführt. Dabei wird Bezug genommen auf [2] (S.159ff.).

4.3.1 Realisierung mittels Multiplikationstabelle

Eine Basis des $\mathbb{R}^4$ wird gegeben durch

$$e_1 : (1,0,0,0),\ e_2 := (0,1,0,0),\ e_3 := (0,0,1,0) \text{ und } e_4 := (0,0,0,1),$$

wobei e_1 das neutrale Element, also das Einselement bezüglich der Multiplikation darstellt.
In der folgenden Tabelle 4.1 wird die Multiplikation nach den Hamilton'schen Bedingungen angeführt. Anhand dieser Tabelle wird die Quaternionenalgebra definiert.

$\cdot$	e_2	e_3	e_4
e_2	$-e_1$	e_4	$-e_3$
e_3	$-e_4$	$-e_1$	e_2
e_4	e_3	$-e_2$	$-e_1$

Tabelle 4.1: Hamilton'sche Multiplikationstabelle

Mit Hilfe der Tabelle sieht man offensichtlich, dass die Quaternionenmultiplikation nicht kommutativ ist, wie schon in Absatz 4.2 angesprochen wurde.
Beispielsweise ist

$$e_2e_3 = e_4 \text{ und } e_3e_2 = -e_4, \text{ womit } e_2e_3 \neq e_3e_2 \text{ gilt.}$$

Um die Quaternionenalgebra zu beschreiben, wird zunächst der Begriff „$\mathbb{R}$-Algebra" definiert (vgl.[2], S.151):

Definition 4.3 *Sei V ein Vektrorraum über $\mathbb{R}$ mit einer zusätzlich definierten Multiplikation $V \times V \to V$, $(x,y) \mapsto xy$. Der Vektorraum V wird als* ***reelle Algebra****, oder* ***$\mathbb{R}$-Algebra****, bezeichnet, wenn die Bilinearität des Produktes erfüllt ist. Es muss also für jedes $\alpha, \beta \in \mathbb{R}$ und für alle $x, y, z \in V$ gelten:*

$$x(\alpha y + \beta z) = \alpha \cdot xy + \beta \cdot xz \quad \textit{und} \quad (\alpha x + \beta y)z = \alpha \cdot xz + \beta \cdot yz.$$

Insbesondere gilt $\alpha(xy) = (\alpha x)y = x(\alpha y)$.

Besitzt eine Algebra ein Einselement $e \in V$*, so gilt* $ex = xe = x \ \forall x \in V$.

Allgemein ist eine reelle Algebra nicht kommutativ bzw. assoziativ. Von einer ***kommutativen Algebra*** *ist die Rede, wenn das Kommutativgesetz* $xy = yx \ \forall x, y \in V$ *gilt. Analog wird eine* ***assoziative Algebra*** *durch Gültigkeit des Assoziativgesetzes* $x(yz) = (xy)z \ \forall x, y, z \in V$ *festgelegt.*

Beispiel 4.1 *Ein Beispiel für eine reelle Algebra bildet der Körper der komplexen Zahlen* $\mathbb{C}$*. Genauer gesagt ist* $\mathbb{C}$ *eine kommutative, assoziative und nullteilerfreie* $\mathbb{R}$*-Algebra mit Eins.*

Die Quaternionenalgebra ist eine vierdimensionale $\mathbb{R}$-Algebra und wird mit $\mathbb{H}$ benannt. Die Quaternionen bezeichnen hierbei die Elemente dieser assoziativen Algebra.

Zur Beschreibung der Quaternionenalgebra werden die Quadrupel e_1, e_2, e_3, e_4 neu benannt:

$$e_1 =: e,\ e_2 =: i,\ e_3 =: j,\ e_4 =: k,$$

wobei

$$i^2 = j^2 = k^2 = ijk = -e \ \text{ und } \ ij = -ji = k$$

gelten.
Für die Multiplikation gilt hierbei die **Produktformel**:

$$\begin{gathered}(\alpha e + \beta i + \gamma j + \delta k)(\alpha' e + \beta' i + \gamma' j + \delta' k) = \\ = e(\alpha\alpha' - \beta\beta' - \gamma\gamma' - \delta\delta') + i(\alpha\beta' + \beta\alpha' + \gamma\delta' - \delta\gamma') + \\ j(\alpha\gamma' - \beta\delta' + \gamma\alpha' + \delta\beta') + k(\alpha\delta' + \beta\gamma' - \gamma\beta' + \delta\alpha'),\end{gathered}$$

welche durch zyklisches Vertauschen von i, j, k und distributives Ausrechnen erhalten wird.

4.3.2 Realisierung durch komplexe 2×2 Matrizen

Eine andere Art die Quaternionen zu realisieren, sind komplexe 2×2 Matrizen. Diese Methode kannte bereits Arthur Cayley im Jahr 1858.
Dabei wird eine Unteralgebra[1] $\mathcal{H}$ von $\mathrm{Mat}(2, \mathbb{C})$ und ein Isomorphismus der Quaternionenalgebra auf diese Unteralgebra, also $F : \mathbb{H} \to \mathcal{H}$ konstruiert.
Es gilt folgender Satz (vgl.[2], S.160):

Satz 4.1 *Durch die Menge* $\mathcal{H} := \{\begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} : w, z \in \mathbb{C}\}$ *wird eine reelle Unteralgebra von Mat*$(2, \mathbb{C})$ *konstruiert.* $\mathcal{H}$ *ist dabei eine Matrixalgebra. Hierbei stellt* $E := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$

[1] Wenn für alle Elemente x, y eines reellen Untervektorraums U einer reellen Algebra $\mathcal{A} = (V, \cdot)$ gilt: $xy \in U$, dann bezeichnet U eine reelle Unteralgebra von $\mathcal{A}$ (vgl. [2], S.152).

das neutrale Element dar.
Nun gilt für alle Matrizen der Form $A = \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} \in \mathcal{H}$ *über* $\mathbb{R}$ *die Gleichung*

$$A^2 - (SpurA)A + (\det A)E = 0 \text{ mit } SpurA = 2Re\ w,\ \det A = |w|^2 + |z^2|.$$

Dabei ist $\mathcal{H}$ *eine assoziative, vierdimensionale Divisionsalgebra.*

An dieser Stelle soll nun der Begriff „Divisionsalgebra“ definiert werden (vgl.[2], S.153):

Definition 4.4 *Sei* V *ein reeller Vektorraum. Sind die Gleichungen* $ax = b$ *und* $ya = b$ *für alle Elemente* $a \neq 0 \in V$ *und* $b \in V$ *in* $\mathcal{A}$ *eindeutig lösbar für* x *und* y*, so wird die Algebra* $\mathcal{A}$ *als Divisionsalgebra bezeichnet.*

Nun kann der oben angeführte Satz 4.1 bewiesen werden (vgl. [2], S.160):

Beweis Im ersten Schritt soll gezeigt werden, dass $\mathcal{H}$ einen vierdimensionalen, reellen Untervektorraum von $\mathrm{Mat}(2, \mathbb{C})$ darstellt, welcher bezüglich der Matrizenmultiplikation abgeschlossen ist. Dies kann durch unmittelbares Rechnen nachgewiesen werden.
Ebenfalls durch eine direkte Rechnung verifiziert werden, kann die Gleichung
$A^2 - (\mathrm{Spur}A)A + (\det A)E = 0$.

Im nächsten Schritt wird begründet, warum $\mathcal{H}$ eine assoziative Divisionsalgebra bildet. Nachdem $\mathrm{Mat}(2, \mathbb{C})$ assoziativ ist, gilt dies auch für $\mathcal{H}$.

Für jede endlich-dimensionale Algebra $\mathcal{A}$ sind die folgenden Aussagen äquivalent (vgl. [2], S.154):

- $\mathcal{A}$ ist nullteilerfrei
- $\mathcal{A}$ ist eine Divisionsalgebra.

Damit lässt sich einsehen, dass $\mathcal{H}$ eine Divisionsalgebra ist. Seien $A, B \in \mathcal{H}$ mit $AB = 0$, so gilt $\det A \cdot \det B = 0$ mit $\det A = 0$ oder $\det B = 0$. Die Determinante
$\det \begin{pmatrix} w & -z \\ \overline{z} & \overline{w} \end{pmatrix} = |w|^2 + |z|^2$ ist genau dann Null, wenn $w = 0$ und $z = 0$ gilt.

Damit ist der Satz gezeigt.

□

Nun soll noch verifiziert werden, dass die Hamilton'sche Algebra $\mathbb{H}$ eine assoziative Divisionsalgebra darstellt. Hierzu wird das folgende Lemma benötigt (vgl. [2], S.153):

Lemma 4.1 *Sei* $\mathcal{A}$ *eine assoziative Divisionsalgebra. Dann bildet* $G := \mathcal{A} \setminus \{0\}$ *eine Gruppe bzgl. der Multiplikation in* $\mathcal{A}$*, wobei das neutrale Element von* G *dem Einselement von* $\mathcal{A}$ *entspricht.*

Beweis Dieses Lemma ist gültig, weil jede Gleichung der Form $ax = b$ und $ya = b$ in G eindeutig lösbar ist und G damit eine Gruppe ist.

□

Nun ist klar, dass $\mathcal{H} \setminus \{0\}$ eine Gruppe bezüglich der Multiplikation darstellt. Man sieht, dass durch die Menge der unten definierten Elemente $\{E, -E, I, -I, J, -J, K, -K\}$ eine nicht-kommutative Untergruppe der Gruppe $\mathcal{H} \setminus \{0\}$ gebildet wird. Alle Elemente dieser Menge, außer $\pm E$, haben die Ordnung 4.
Dabei sind E, I, J, K in folgendem Lemma festgelegt (vgl. [2],S.160-161):

Lemma 4.2 *Durch*

$$F : \mathbb{H} \to \mathcal{H},\ (\alpha, \beta, \gamma, \delta) \mapsto \begin{pmatrix} \alpha + \beta i & -\gamma - \delta i \\ \gamma - \delta i & \alpha - \beta i \end{pmatrix}$$

wird ein $\mathbb{R}$-Algebra-Isomorphismus definiert, für welchen

$$F(e_1) := E, \qquad F(e_2) = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix} := I$$

$$F(e_3) = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} := J, \quad F(e_4) = \begin{pmatrix} 0 & -i \\ -i & 0 \end{pmatrix} := K \text{ gilt.}$$

Beweis-Skizze Der Beweis zu Lemma 4.2 wird angelehnt an [2] (S.161) skizziert.
F ist eine bijektive, $\mathbb{R}$-lineare Abbildung. Nun soll gezeigt werden, dass für $\mu, v = 1, 2, 3, 4$ gilt: $F(e_\mu)F(e_v) = F(e_\mu e_v)$ (vgl. [3], S.154). Da die Matrizen E, I, J, K genau die F-Bilder von e_1, e_2, e_3, e_4 sind sie und den gleichen Multiplikationsregeln folgen, ist auch das ersichtlich.
Es gelten: $I^2 = J^2 = -E$, $IJ = -JI = K$. Aus dem Assoziativgesetz folgen die restlichen Beziehungen, wie beispielsweise $K^2 = (IJ) = (-JI) = -IJ^2I = I^2 = -E$.

□

Die nicht-kommutative Gruppe $\{E, -E, I, -I, J, -J, K, -K\}$ wird endliche **Quaternionengruppe** genannt.
Vorher wurde schon gezeigt, dass $\mathcal{H}$ eine assoziaitve Divisionsalgebra ist (vgl. Satz 4.1). Durch den Isomorphismus $F : \mathbb{H} \to \mathcal{H}$ kann dies auf die Hamilton'sche Algebra $\mathbb{H}$ übertragen werden.

4.4 Eigenschaften der Quaternionen und der Hamilton'schen Algebra

Nun sollen einige algebraische Eigenschaften der Quaternionenalgebra beschrieben werden. Hierbei wird auf Quelle [2] (S.162,167ff) referenziert.

4.4.1 Der Imaginärraum der Hamilton'schen Algebra

Analog zu der imaginären Einheit bei den komplexen Zahlen (vgl. Kapitel 3.2.2), gibt es in der Hamilton'schen Algebra den Imaginärraum von $\mathbb{H}$.
Dieser ist folgendermaßen definiert:

Definition 4.5 *Sei e, i, j, k die Hamilton'sche Standardbasis. Als Imaginärraum von $\mathbb{H}$ wird der dreidimensionale Untervektorraum*

$$Im\ \mathbb{H} := \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

bezeichnet.

$\mathbb{H}$ kann als Summe von Vektorräumen geschrieben werden:

$$\mathbb{H} = \mathbb{R}e \oplus \text{Im } \mathbb{H},$$

wobei e das Einselement ist und $\mathbb{R}e$ invariant definiert wird. Damit auch $\mathbb{H}$ unabhängig von der Wahl der Basis wird, muss beachtet werden, dass eine Quaternion der Form $x = \alpha e + \beta i + \gamma j + \delta k$ der Gleichung

$$x^2 = 2\alpha x - (\alpha^2 + \beta^2 + \gamma^2 + \delta^2)e$$

gehorcht. Ist $\alpha = 0$, so ist $x \in \text{Im}\mathbb{H}$ und somit erhält man eine basisinvariante Darstellung vom Imaginärraum von $\mathbb{H}$:

$$\text{Im}\mathbb{H} = \{x \in \mathbb{H} : x^2 \in \mathbb{R}e \text{ und } x \notin \mathbb{R}e \setminus \{0\}\}.$$

4.4.2 Hamilton'sche Tripel

Hamilton'sche Tripel sind für die allgemeine Theorie von Algebren von äußerster Relevanz und werden in [2] (S.184) wie folgt definiert:

Definition 4.6 *Sei $\mathcal{A}$ eine Algebra mit Einselement e. Falls die unten angeführten Hamilton'schen Bedingungen erfüllt sind, bilden die Elemente u, v, w ein Hamilton'sches Tripel.*

Hamilton'sche Bedingungen:

$$u^2 = v^2 = w^2 = -e, \quad w = uv = -vu, \quad u = wu = -uw, \quad u = vw = -wv$$

Es kann verifiziert werden, dass alle Elemente eines Hamilton'schen Tripels stets reinimaginär sind (vgl. [2], S.185).
Außerdem gilt der **Existenzsatz für Hamilton'sche Tripel** (vgl. Satz 4.2), für den zuerst die folgende Definition von Nöten ist (vgl. [3], S.186):

Definition 4.7 *Eine Algebra $\mathcal{A}$ wird **alternativ** genannt, wenn $\forall x, y \in \mathcal{A}$ gelten:*

- $x(xy) = x^2y$
- $(xy)y = xy^2$
- $(xy)x = x(yx)$

Hierbei gilt, dass eine Algebra $\mathcal{A}$ genau dann alternativ ist, wenn von jeweils zwei Elementen $x, y \in \mathcal{A}$ eine assoziative Unteralgebra erzeugt wird (Satz von E. Artin, vgl. [2], S.187).

Satz 4.2 *(vgl.[3], S.186).*
Sei $\mathcal{A}$ eine nullteilerfreie, alternative Algebra mit e als Einselement. Weiters sei U ein zweidimensionaler Untervektorraum von Im $\mathcal{A}$. Nun gilt: $\forall u \in U$ mit $u^2 = -e$
$\exists v \in U$, sodass u, v, uv ein Hamilton'sches Tripel darstellen.

4.4.3 Satz von Frobenius

An dieser Stelle sei noch ein interessanter Satz erwähnt und zwar der Satz von Frobenius (vgl. [2], S.189):

Satz 4.3 *Für eine nullteilerfreie, assoziative, quadratische, reelle Algebra $\mathcal{A} \neq 0$ sind folgende Möglichkeiten gegeben:*

- *$\mathcal{A}$ ist zu den reellen Zahlen $\mathbb{R}$ isomorph.*
- *$\mathcal{A}$ ist zu den komplexen Zahlen $\mathbb{C}$ isomorph.*
- *$\mathcal{A}$ ist zur Hamilton'schen Algebra $\mathbb{H}$ isomorph.*

Dabei wird eine Algebra $\mathcal{A}$ mit Einselement e als quadratisch bezeichnet, wenn für alle $x \in \mathcal{A}$ die Gleichung $x^2 = \alpha e + \beta x$ mit $\alpha, \beta \in \mathbb{R}$ erfüllt ist (vgl. [2], S.187).

4.4.4 Fundamentalsatz der Algebra für Quaternionen

In Absatz 2.1.1 wurde der Fundamentalsatz der Algebra für komplexe Zahlen behandelt. Nun wird der **Fundamentalsatz der Algebra für Quaternionen** vorgestellt, wobei [2] (S.168-169) als Literaturquelle diente.

Satz 4.4 *Sei p ein Polynom mit deg $p = n > 0$ über $\mathbb{H}$. Dabei habe p die Gestalt $p = m + q$, mit einem Monom m vom Grad n und einem Polynom q von Grad deg $q < n$. Dann gilt, dass $p : \mathbb{H} \to \mathbb{H}$ surjektiv ist. Insbesondere $\exists a \in \mathbb{H} : p(a) = 0$.*

Beweis Der Beweis kann beispielsweise in [2] (S.168) nachgelesen werden.

Kapitel 5

Ausblick - Cayley Zahlen

Dadurch, dass bei der Erfindung der Quaternionen auf die Kommutativität verzichtet wurde, erlebte die Algebra damals ein komplett neues Zeitalter. Nur zwei Monate nach Hamiltons Entdeckung der vierdimensionalen Quaternionenalgebra, wurde ein achtdimensionales Konstrukt entwickelt. Im Dezember 1843 erfand J.T. Graves die so genannten Oktaven oder Okternionen.
Hamilton fand heraus, dass diese Divisionsalgebra nicht mehr assoziativ ist.
Zwei Jahre später entwickelte **Arthur Cayley** die Oktaven weiter und gab ihnen einen neuen Namen - die **Cayley Zahlen**.
Auf dieses Konstrukt soll, mit Hilfe von [2] (S.205ff), in diesem Kapitel überblicksmäßig eingegangen werden.

5.1 Konstruktion der Cayley-Algebra $\mathbb{O}$

Es wurde bereits mehrfach erwähnt, dass die komplexen Zahlen, mittels des kartesischen Produktes $\mathbb{R} \times \mathbb{R}$, aus dem Körper der reellen Zahlen entstanden sind.
Auf ähnliche Art und Weise entstand die Quaternionenalgebra $\mathbb{H}$, mit Hilfe des Produktes $\mathbb{C} \times \mathbb{C}$, aus dem Körper der komplexen Zahlen $\mathbb{C}$.
Nun werden die Cayley-Zahlen, ebenfalls mittels eines Produktes, aus der Quaternionenalgebra gewonnen. Dabei wird das Produkt für zwei Elemente $x = (x_1, x_2)$ und $y = (y_1, y_2)$ wie folgt definiert:

$$xy = (x_1, x_2)(y_1, y_2) := (x_1 y_1 - \overline{y_2}, x_2, x_2 \overline{y_1} + y_2 x_1).$$

Man sieht, dass die Distributivgesetze gelten, womit aus $\mathbb{H} \times \mathbb{H}$ eine achtdimensionale $\mathbb{R}$-Algebra wird, welche Cayley-Algebra $\mathbb{O}$ genannt wird.
Es kann gezeigt werden, dass $\mathbb{O}$ eine quadratische Algebra ist.

5.1.1 Der Imaginärraum der Cayley-Zahlen

Genau wie die Hamilton'sche Algebra, gibt es auch bei der Cayley-Algebra einen Imaginärraum. Dieser ist folgendermaßen definiert:

$$\text{Im } \mathbb{O} = \text{Im } \mathbb{H} \times \mathbb{H}.$$

5.1.2 Multiplikationstabelle für $\mathbb{O}$

Wie in Tabelle 4.1 für die Quaternionen angeführt, gibt es auch für die Cayley-Zahlen eine Multiplikationstabelle .
Eine Basis für den Vektorraum $V := \mathbb{R}^8$ ist durch folgende Elemente gegeben:

$$e_1 := (1, 0, ..., 0), e_2 := (0, 1, 0, ..., 0), ..., e_8 := (0, ..., 0, 1).$$

Dabei ist, wie auch bei der Multiplikation der Quaternionen, e_1 das Einselement.

Durch Tabelle 5.1 ist nun die Oktavenmultiplikation festgelegt (vgl.[2],S.215):

$\cdot$	e_2	e_3	e_4	e_5	e_6	e_7	e_8
e_2	$-e_1$	e_4	$-e_3$	e_6	$-e_5$	$-e_8$	e_7
e_3	$-e_4$	$-e_1$	e_2	e_7	e_8	$-e_5$	$-e_6$
e_4	e_3	e_2	$-e_1$	e_8	$-e_7$	e_6	$-e_5$
e_5	$-e_6$	$-e_7$	$-e_8$	$-e_1$	e_2	e_3	e_4
e_6	e_5	$-e_8$	e_7	$-e_2$	$-e_1$	$-e_4$	e_3
e_7	e_8	e_5	$-e_6$	$-e_3$	e_4	$-e_1$	$-e_2$
e_8	$-e_7$	e_6	e_5	$-e_4$	$-e_3$	e_2	$-e_1$

Tabelle 5.1: Multiplikationstabelle für $\mathbb{O}$

Betrachtet man nun beispielsweise

$$e_3(e_4e_5) = -e_6 \text{ und } (e_3e_4)e_5 = e_6,$$

so ist sofort klar, dass die Cayley-Zahlen nicht assoziativ sind.

5.1.3 Einzigkeit der Cayley-Zahlen

Zu guter Letzt sei nun noch darauf hingewiesen, dass die Cayley-Algebra, ähnlich wie die komplexen Zahlen, einzigartig sind. Der folgende Satz von Zorn aus dem Jahre 1933 soll dies verdeutlichen (vgl. [2], S.216):

Satz 5.1 *Sei $\mathcal{A}$ eine nullteilerfreie, alternative, quadratische, relle, nicht-assoziative Algebra. Dann ist $\mathcal{A}$ isomorph zur Cayley-Algebra $\mathbb{O}$.*

Unter diesem Satz ist in [**2**] ebenfalls ein möglicher Beweis dazu angeführt.

Tabellenverzeichnis

Abbildungsverzeichnis

Quellenverzeichnis

Literatur

[1] Felbert A. *Struktur eines Körpers - algebraische und tranzendente Körpererweiterungen*. Köln, Sep. 2006 (siehe S. 10).

[2] Ebbinghaus et al. *Zahlen*. 3. Aufl. Heidelberg: Springer, 1992 (siehe S. 23, 26, 27, 29, 32–35, 37–45, 47, 48).

[3] Fischer G. *Lehrbuch der Algebra*. 4. Aufl. München und Garching: Springer Spektrum, Juli 2017 (siehe S. 9–14, 17–19, 21, 30, 31, 43, 44).

[4] Wüstholz G. *Algebra - Für Studierende der Mathematik, Physik, Informatik*. 2. Aufl. Wiesbaden: Springer Spektrum, Apr. 2013 (siehe S. 17, 19).

[5] Fischer W.; Lieb I. *Einführung in die Komplexe Analysis. Elemente der Funktionentheorie*. 1. Aufl. Bonn und Bremen: Vieweg+Teubner, 2009 (siehe S. 18, 19).

[6] Karpfinger C.; Mayberg K. *Algebra. Gruppen-Ringe-Körper*. Heidelberg: Spektrum-Akademischer Verlag, 2009 (siehe S. 10–13, 17, 19, 20, 39).

[7] Schichl H.; Steinbauer R. *Einführung in das mathemtaische Arbeiten*. 1. Aufl. Heidelberg: Springer, 2009 (siehe S. 26, 28, 31, 32, 37, 39).

[8] Schulze-Pillot R. *Einführung in Algebra und Zahlentheorie*. Springer Spektrum, Apr. 2014 (siehe S. 11).

[9] Crilly T. *Die großen Fragen. Mathematik*. Heidelberg: Spektrum Akademischer Verlag, 2012 (siehe S. 37).