

Alle Strukturen der linearen Algebra bauen auf „Körpern“ auf; diese sind aber nicht der eigentliche Untersuchungsgegenstand der linearen Algebra (dies sind die Vektorräume, die wir im nächsten Kapitel behandeln). Ein „Körper“ ist nicht nur eine Menge, sondern diese Menge trägt zusätzlich eine Struktur: Auf einer Menge sind zwei Operationen (nämlich $+$ und \cdot) erklärt. Grob gesagt, sind Körper algebraische Strukturen, in denen man so rechnen (d. h. addieren und multiplizieren) kann wie mit rationalen oder reellen Zahlen.

2.1 Die Definition

Ein **Körper** besteht aus einer Menge K von Elementen zusammen mit zwei Verknüpfungen $+$ und \cdot , die je zwei Elementen $x, y \in K$ wieder ein Element $x + y$ bzw. $x \cdot y$ von K zuordnen. Damit eine solche Struktur Körper genannt wird, müssen die folgenden drei Gruppen von Gesetzen für alle $x, y, z \in K$ erfüllt sein:

2.1.1 Gesetze der Addition

- *Assoziativität:*

$$(x + y) + z = x + (y + z) .$$

- *Existenz und Eindeutigkeit des neutralen Elements:* Es gibt genau ein Element von K , das wir 0 („Nullelement“) nennen, für das gilt

$$0 + x = x .$$

- *Existenz und Eindeutigkeit inverser Elemente:* Zu jedem x gibt es genau ein Element, das wir $-x$ nennen, für das gilt

$$x + -x = 0 .$$

- *Kommutativität:*

$$x + y = y + x .$$

2.1.2 Gesetze der Multiplikation

- *Assoziativität:*

$$x \cdot (y \cdot z) = (x \cdot y) \cdot z$$

- *Existenz und Eindeutigkeit des neutralen Elements:* Es gibt genau ein vom Nullelement verschiedenes Element, das wir 1 („Einselement“) nennen, für das gilt:

$$1 \cdot x = x \cdot 1 = x .$$

- *Existenz und Eindeutigkeit inverser Elemente:* Zu jedem $x \neq 0$ existiert genau ein Element, das wir x^{-1} nennen, für das gilt:

$$x \cdot x^{-1} = 1 = x^{-1} \cdot x .$$

- *Kommutativität:*

$$x \cdot y = y \cdot x .$$

2.1.3 Distributivgesetz

$$x \cdot (y + z) = x \cdot y + x \cdot z .$$

Wenn Sie nachweisen wollen, dass eine gegebene Struktur ein Körper ist, so müssen Sie (solange keine anderen Charakterisierungen zur Verfügung stehen) *alle* genannten Eigenschaften verifizieren.

Statt $x \cdot y$ werden wir in Zukunft oft einfach xy schreiben.

Um uns an die Definition zu gewöhnen, beweisen wir zwei ganz einfache, aber nützliche Eigenschaften, die für alle Körper gelten und die auf den ersten Blick so unscheinbar sind, dass Sie diese vermutlich übersehen hätten.

1. Multiplikation mit 0

Für jedes x aus K gilt $x \cdot 0 = 0$.

Zum *Beweis* gehen wir wie folgt vor: Wir verwenden zweimal die Tatsache, dass 0 neutrales Element bezüglich der Addition ist, und erhalten

$$x \cdot 0 + 0 = x \cdot 0 = x \cdot (0 + 0) = x \cdot 0 + x \cdot 0 .$$

Wenn wir jetzt auf beiden Seiten $x \cdot 0$ abziehen (das ist eine abkürzende Sprechweise für „ $-x \cdot 0$ addieren“), so ergibt sich $0 = x \cdot 0$. \square

2. (Nullteilerfreiheit)

Sind $x, y \in K$ und gilt $x \neq 0, y \neq 0$, so ist auch $x \cdot y \neq 0$.

Beweis Sei $x \neq 0$ und $xy = 0$. Da $x \neq 0$ ist, existiert das zu x inverse Element x^{-1} . Indem wir die Gleichung $xy = 0$ auf beiden Seiten mit x^{-1} multiplizieren, erhalten wir aufgrund der ersten Eigenschaft

$$y = (x^{-1}x) \cdot y = x^{-1} \cdot (xy) = x^{-1} \cdot 0 = 0,$$

also $y = 0$. Damit ist diese Behauptung gezeigt. \square

Auf *eine* Forderung, die unscheinbar formuliert ist, weise ich besonders hin; es handelt sich darum, dass sowohl „+“ als auch „ \cdot “ *Verknüpfungen* auf K sein müssen.

Was bedeutet das? Eine **Verknüpfung** (genauer gesagt: eine „binäre“ Verknüpfung) auf K ist eine Abbildung, die jedem Paar von Elementen von K ein Element von K zuordnet. Ganz vornehm ausgedrückt ist eine Verknüpfung also eine Abbildung von $K \times K$ in K . Die Addition und Multiplikation eines Körpers K sind Abbildungen

$$(x, y) \mapsto x + y \quad \text{und} \quad (x, y) \mapsto x \cdot y.$$

Entscheidend ist, dass das Bild (in unserem Fall also $x + y$ und $x \cdot y$) wieder ein Element von K ist; diese Forderung bezeichnet man auch als **Abgeschlossenheit**.

Um diesen Begriff klar zu machen, betrachten wir einige *Beispiele* von Verknüpfungen und von Abbildungen, die keine Verknüpfungen sind. Als Grundmenge wählen wir die Menge \mathbf{N} der natürlichen Zahlen. Die gewöhnliche Addition und Multiplikation sowie die Exponentiation sind Verknüpfungen, da $x + y$, $x \cdot y$ und x^y natürliche Zahlen sind, falls x, y natürliche Zahlen sind. Demgegenüber ist aber weder die Subtraktion noch die Division eine Verknüpfung, denn im Allgemeinen ist $x - y$ und x/y keine natürliche Zahl für $x, y \in \mathbf{N}$.

Ein weiteres Beispiel ist folgendes: Wenn K ein Körper ist, so ist das Produkt zweier von Null verschiedener Elemente von K , wie wir wissen, ebenfalls verschieden von Null. Dies kann man auch wie folgt ausdrücken: Die Multiplikation ist auf der Menge $K \setminus \{0\}$ abgeschlossen.

Die ersten *Beispiele* für Körper sind offensichtlich: Sowohl die Menge \mathbf{Q} der rationalen Zahlen als auch die Menge \mathbf{R} und \mathbf{C} der reellen Zahlen bilden, jeweils zusammen mit der gewöhnlichen Addition und Multiplikation, einen Körper. (In diesen Strukturen gelten noch viel mehr arithmetische Gesetze; zum Beispiel kann man bei den rationalen und reellen Zahlen zwischen positiven und negativen Zahlen unterscheiden und beliebig kleine Zahlen betrachten – beides Möglichkeiten, die in Körpern im allgemeinen nicht vorhanden sind.)

Bevor wir weitere Beispiele diskutieren, einige Bemerkungen zur Definition eines Körpers, genauer gesagt einige Bemerkungen dazu, was *nicht* in der Definition eines Körpers steht:

- Wir haben auch für die Multiplikation das Kommutativgesetz gefordert. Dies ist zwar üblich – aber man könnte die elementare Körpertheorie auf weite Strecken auch ohne entwickeln. Wenn in einer algebraischen Struktur alle Axiome eines Körpers gelten, nur das Kommutativgesetz für die Multiplikation nicht, so heißt diese Struktur ein Schiefkörper. Man muss dann auch noch das zweite Distributivgesetz (das bei Körpern aufgrund der Kommutativität der Multiplikation automatisch folgt) fordern, nämlich

$$(x + y) \cdot z = x \cdot z + y \cdot z$$

für alle $x, y, z \in K$. Also: Ein **Schiefkörper** ist eine Menge zusammen mit einer Addition und einer Multiplikation, so dass alle Körperaxiome – mit Ausnahme der Kommutativität der Multiplikation – und beide Distributivgesetze gelten.

Wenn wir die Kommutativität der Multiplikation besonders hervorheben wollen, werden wir auch von einem „kommutativen Körper“ sprechen. Dies bedeutet aber für uns nichts anderes als einfach „Körper“.

Auch Schiefkörper sind hochinteressante algebraische Strukturen; einer der Höhepunkte dieses Kapitels wird die Konstruktion des „Quaternionenschiefkörpers“ sein.

- Mit unseren Axiomen (das heißt: Grundgesetzen) können wir nichts über die „Größe“ (etwa den Absolutbetrag) einzelner Elemente aussagen.

Wir können auch keine Aussage über eine **Anordnung** eines Körpers K (also über eine \leq -Beziehung) machen.

Aus den Körperaxiomen folgen auch keine Axiome über die Stetigkeit der Operationen von K ; wir können also beispielsweise keine Konvergenzaussagen verwenden.

- Man könnte die Körperaxiome auch abschwächen, indem man zum Beispiel nur die Existenz (und nicht die Eindeutigkeit) der neutralen und inversen Elemente fordert. Die Eindeutigkeit kann man nämlich daraus beweisen. Um uns diese Beweise zu ersparen, haben wir ein etwas stärkeres Axiomensystem gewählt. (Wir werden solche Beweise später, in Kap. 9, exemplarisch im Zusammenhang mit der Untersuchung von „Gruppen“ kennen lernen.)

Dieses Kapitel hat zwei größere Abschnitte. Im ersten konstruieren wir wichtige Beispiele von Körpern, im zweiten betrachten wir Automorphismen von Körpern.

2.2 Beispiele von Körpern

Die neben \mathbf{Q} und \mathbf{R} wichtigsten Körper sind der Körper \mathbf{C} der komplexen Zahlen und der Körper $\text{GF}(2)$ aus 0 und 1. Zuerst behandeln wir \mathbf{C} .

2.2.1 Der Körper der komplexen Zahlen

Wir erhalten die komplexen Zahlen aus den reellen Zahlen, indem wir aus einer reellen Zahl zwei machen. Eine **komplexe Zahl** ist ein Paar $z = (a, b)$ reeller Zahlen; man nennt

$$\mathbf{C} = \{(a, b) \mid a, b \in \mathbf{R}\} (= \mathbf{R} \times \mathbf{R}) .$$

den Körper (noch sollten wir vorsichtig sein und nur sagen: die Menge) der komplexen Zahlen.

Man kann komplexe Zahlen addieren und multiplizieren. Dies geschieht dadurch, dass man diese Operationen auf die entsprechenden Operationen in \mathbf{R} zurückführt: Seien $z = (a, b)$ und $z' = (a', b')$ zwei komplexe Zahlen. Dann ist

$$z + z' := (a, b) + (a', b') := (a + a', b + b') .$$

Man sagt auch, die Addition sei **komponentenweise** definiert.

Die Multiplikation ist *nicht* komponentenweise definiert, sondern auf folgende zunächst kompliziert erscheinende Art und Weise:

$$z \cdot z' = (a, b) \cdot (a', b') := (aa' - bb', ab' + a'b) .$$

Wir werden zeigen, dass \mathbf{C} mit dieser Addition und Multiplikation einen Körper bildet.

Um zu sehen, dass die Multiplikation nicht völlig sinnlos ist, zeigen wir die Eindeutigkeit und Existenz eines Einselements. Dazu setzen wir das neutrale Element (bezüglich der Multiplikation) mit $e = (x, y)$ an und berechnen x und y . Zunächst nutzen wir aus, dass e die Zahl $(1, 0)$ neutralisieren muss; das heißt

$$(1, 0) \cdot (x, y) = (1, 0) .$$

Nach Definition der Multiplikation folgt daraus

$$(x, y) = (1 \cdot x, 1 \cdot y) = (1, 0) \cdot (x, y) = (1, 0) .$$

Das bedeutet, dass $x = 1$ und $y = 0$ sein muss. Also: Wenn es überhaupt ein Element e gibt, das alle Elemente von \mathbf{C} neutralisiert, so muss $e = (1, 0)$ sein. Damit ist die Eindeutigkeit gezeigt. Die Existenz folgt leicht aus der Definition der Multiplikation; es ist nämlich

$$z \cdot e = (a \cdot 1 - b \cdot 0, a \cdot 0 + 1 \cdot b) = (a, b) = z$$

und

$$e \cdot z = (1 \cdot a - 0 \cdot b, 1 \cdot b + a \cdot 0) = (a, b) = z .$$

Also ist e tatsächlich das neutrale Element.

Bevor wir die übrigen Körperaxiome nachweisen, stellen wir eine alternative Darstellung der komplexen Zahlen vor.

Zunächst schreiben wir statt $(a, 0)$ einfach a . Damit können wir die reellen Zahlen als Teil von \mathbb{C} auffassen. Außerdem ergeben sich unmittelbar die folgenden Regeln zur Multiplikation einer reellen Zahl r mit einer komplexen Zahl (a, b) :

$$r \cdot (a, b) = (r, 0) \cdot (a, b) = (r \cdot a, r \cdot b)$$

und

$$(a, b) \cdot r = (a, b) \cdot (r, 0) = (ar, br) = (ra, rb) = r \cdot (a, b) .$$

Insbesondere ist

$$r \cdot (1, 0) = (r, 0) = r \text{ und } r \cdot (0, 1) = (0, r) .$$

Nun kommt der entscheidende Trick: Wir definieren i als $i := (0, 1) \in \mathbb{C}$. Aufgrund der Definition der Multiplikation ergibt sich

$$i^2 = i \cdot i = (0, 1) \cdot (0, 1) = (-1, 0) = -1 .$$

Diese Vereinbarung macht es möglich, dass wir eine beliebige komplexe Zahl $z = (a, b)$ wie folgt ausdrücken können:

$$z = (a, b) = a \cdot (1, 0) + b \cdot (0, 1) = a + b \cdot i = a + ib .$$

Daher schreiben wir statt (a, b) in Zukunft einfach $a + ib$.

Damit können wir das Produkt zweier komplexer Zahlen $z = a + ib$, $z' = a' + ib'$ berechnen:

$$z \cdot z' = (a, b) \cdot (a', b') = (aa' - bb', ab' + a'b) = aa' - bb' + i(ab' + a'b) .$$

Andererseits kann man das Produkt $(a + bi) \cdot (a' + b'i)$ „einfach ausrechnen“ und erhält:

$$\begin{aligned} (a + bi)(a' + b'i) &= aa' + (ab' + ba')i + bi \cdot b'i = aa' + bb'i^2 + (ab' + ba')i \\ &= aa' - bb' + (ab' + ba')i = z \cdot z' . \end{aligned}$$

Die Regel zur Multiplikation komplexer Zahlen wird dadurch denkbar einfach: *Man stelle die komplexen Zahlen in der Form $a + ib$ dar und rechne mit solchen Zahlen „ganz normal“, unter Beachtung der Tatsache $i^2 = -1$.* (In Übungsaufgabe 1 sollen Sie sich überzeugen, dass jedes Gleichheitszeichen in obiger Gleichungskette zu Recht besteht.)

Man nennt a den **Realteil** und b den **Imaginärteil** der komplexen Zahl $z = a + ib$. Die komplexe Zahl i heißt die **imaginäre Einheit** von \mathbb{C} . Komplexe Zahlen sind gleich, wenn

ihre Realteile und ihre Imaginärteile gleich sind. Die reellen Zahlen sind offenbar genau die komplexen Zahlen, deren Imaginärteil gleich Null ist.

Die Einführung des Symbols i geht auf Leonhard Euler (1707–1783) zurück.

Nun weisen wir alle Körperaxiome für \mathbb{C} nach.

Gesetze der Addition Da die Addition komponentenweise erklärt ist, ergeben sich alle Gesetze aus den entsprechenden Gesetzen von \mathbb{R} : Das Nullelement ist $(0, 0)$; das zu (a, b) inverse Element ist $(-a, -b)$.

Gesetze der Multiplikation Wir haben bereits nachgewiesen, dass $(1, 0)$ das Einselement ist. Wir müssen jetzt noch nachweisen, dass jedes Element $(a, b) \neq (0, 0)$ ein Inverses hat; das bedeutet, dass es genau ein Element (a', b') gibt mit $(a + bi) \cdot (a' + b'i) = 1$, also

$$(a, b) \cdot (a', b') = (1, 0) .$$

Das bedeutet

$$1 = (a + bi) \cdot (a' + b'i) = aa' - bb' + (ab' + a'b)i .$$

Also muss

$$1 = aa' - bb'$$

und

$$0 = ab' + a'b$$

gelten. Daraus folgt

$$abb' = a^2a' - a \quad \text{und} \quad abb' = -a'b^2 ,$$

also

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

Das heißt

$$a' = \frac{a}{a^2 + b^2} , \quad b' = \frac{-b}{a^2 + b^2} .$$

Somit ist

$$z' = \left(\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \right)$$

das multiplikative Inverse von $z = (a, b) \neq (0, 0)$. (Beachten Sie, dass in jedem Fall $a^2 + b^2 \neq 0$ ist. Warum? Wegen $z \neq (0, 0)$ ist $a \neq 0$ oder $b \neq 0$ (oder beides). Unabhängig davon, ob $a \neq 0$ positiv oder negativ ist, ist a^2 stets positiv. Also ist $a^2 + b^2$ die Summe der beiden nichtnegativen Zahlen a^2 und b^2 , von denen mindestens eine verschieden von Null ist. Daher ist $a^2 + b^2 > 0$ und insbesondere also $a^2 + b^2 \neq 0$.)

Die Assoziativ- und die Distributivgesetze sollen Sie in den Übungen nachrechnen (siehe Übungsaufgabe 2).

Damit haben wir insgesamt nachgewiesen, dass \mathbf{C} ein Körper ist: der **Körper der komplexen Zahlen**. Man nennt i die imaginäre Einheit; dies ist eine komplexe Zahl, für die $i^2 = -1$ gilt.

Zur Geschichte der komplexen Zahlen lesen wir in H. Heusers *Lehrbuch der Analysis I* das folgende:

Komplexe Zahlen verdanken ihr Leben einem Manne, den seine Mutter (wie er selbst berichtet) abtreiben wollte; der sich dann zu einem Wüstling, Streithansl, magisch-mystischen Mathematiker und europaweit gefeierten Arzt entwickelte; ein Mann, der als Student Rektor der Universität Padua und als Greis Insasse des Gefängnisses von Bologna war; der sich erdreistete, das Horoskop Jesu zu stellen und in seinem Buch „Über das Würfelspiel“ Betrugsanleitungen zu geben, und der nebenbei auch noch die „Cardanische Aufhängung“ erfand: Hieronimo Cardano (1501–1576), ein vollblütiger Sohn der italienischen Renaissance. In seiner *Ars magna sive de regulis algebraicis* („Die große Kunst oder über die algebraischen Regeln“, Nürnberg 1545) führt ihn die unverfängliche Aufgabe, eine Strecke der Länge 10 so in zwei Stücke zu zerlegen, dass das aus ihnen gebildete Rechteck die Fläche 40 hat, zu der quadratischen Gleichung $x(10 - x) = 40$ und zu ihren absurden Lösungen $x_{1,2} := 5 \pm \sqrt{-15}$, absurd, weil man aus negativen Zahlen keine (reellen) Quadratwurzeln ziehen kann. Aber nun geschieht etwas Entscheidendes: Cardano setzt die „geistigen Qualen“, die ihm diese Gebilde bereiten, beiseite und findet durch keck-formales Rechnen, dass tatsächlich $x_1 + x_2 = 10$ und $x_1 x_2 = 40$ ist. Sein ironischer Kommentar: „So schreitet der arithmetische Scharfsinn voran, dessen Ergebnis ebenso subtil wie nutzlos ist“. Die „komplexen“ (zusammengesetzten) Ausdrücke $\alpha + \sqrt{-\beta}$ oder $\alpha + i\sqrt{\beta}$ mit der „imaginären Einheit“ $i = \sqrt{-1}$ sind dann nicht mehr aus der Mathematik verschwunden, so sehr sie auch als schein- und gespensterhaft empfunden wurden. Denn sie lieferten nicht nur „Lösungen“ aller quadratischen und kubischen Gleichungen – und zwar solche, die erbaulicherweise den vertrauten Wurzelsätzen des Francois Vieta (1540–1603) genügten –, vielmehr ergab unverdrossenes (und unverstandenes) Rechnen mit diesen windigen „Zahlen“ sogar Sätze „im Reellen“.

2.2.2 Der Quaternionenschiefkörper

Die Mathematiker haben sich (vor allem im letzten Jahrhundert) gefragt, ob man den Prozess der Erweiterung der reellen Zahlen zu den komplexen wiederholen kann. Lange wurde – ohne Erfolg – damit experimentiert, auf der Menge von Tripeln reeller Zahlen eine sinnvolle Multiplikation zu definieren. Der Entdecker der Quaternionen, William Rowan Hamilton (1805–1865), beschreibt die verzweifelten Szenen in einem Brief an seinen Sohn wie folgt:

Every morning, on my coming down to breakfast, you asked me: “Well, Papa, can you multiply triplets?” Whereto I was always obliged to reply, with a sad shake of the head: “No, I can only add and subtract them”.

Schließlich entdeckte Hamilton, nachdem er 13 Jahre lang unermüdlich danach gesucht hatte, wie man auf der Menge aller 4-Tupel (Quadrupel) reeller Zahlen eine Multiplikation so definieren kann, dass man damit wenigstens einen Schiefkörper erhält. Auf Hamilton

geht auch die Bezeichnung Quaternionen für die Elemente dieses Körpers zurück (lateinisch: quattuor: vier). Übrigens stammt Name Quaternion – aus der Bibel; in Apostelgesch. 12, 4 lesen wir in der lateinischen Ausgabe: *[Herodes] misit [Petrum] in carcerem, tradens quattuor quaternionibus militum custodiendum ...* Auf englisch: *[Herodes] put [Peter] in prison, and delivered him to four quaternions of soldiers to keep him ...*

Der Quaternionenschiefkörper wird zu Ehren Hamiltons heute mit \mathbf{H} bezeichnet. Hamilton beschreibt seine Entdeckung äußerst plastisch. Voller Befriedigung berichtet er in einem Brief an seinen Sohn:

On the 16th of October, 1843, – which happened to be a Monday, and a Council day of the Royal Irish Academy – I was walking in to attend and preside, and your mother was walking with me, along the Royal Canal, to which she had perhaps driven; and although she talked with me now and then, yet an under-current of thought was going on in my mind, which gave at last a result, whereof it is not too much to say that I felt at once the importance. An electric circuit seemed to close; and a spark flashed forth, the herald (as I foresaw, immediately) of many long years to come of definitely directed thought and work, by myself it spared, and at all events on the part of others, if I should even be allowed to live long enough distinctly to communicate the discovery. Nor should I resist the impulse – unphilosophically as it may have been – to cut with a knife on a stone at Brougham Bridge, as we passed it, the fundamental formula with the symbols i, j, k ; namely,

$$i^2 = j^2 = k^2 = ijk = -1$$

which contains the Solution of the Problem, but of course the inscription, has long since mouldered away.

Hamilton war besessen von den Quaternionen: Als er im Jahre 1865 starb, gab es bereits 150 Veröffentlichungen über Quaternionen – von denen Hamilton selbst 109 geschrieben hatte. In seinem Nachlass fand man 60 (in Worten: sechzig) Buchmanuskripte zur Mathematik der Quaternionen. Man kann heute aber sicher sagen, dass Hamilton und seine Anhänger die Bedeutung der Quaternionen viel zu hoch eingeschätzt haben.

Wir beschreiben nun den **Quaternionenschiefkörper \mathbf{H}** auf eine sehr übersichtliche Art und Weise, die sich an der Beschreibung der komplexen Zahl in der Form $z = a + ib$ orientiert.

Wir führen dazu drei neue **imaginäre Einheiten** ein, die wir i, j und k nennen. Die Elemente von \mathbf{H} (also die **Quaternionen**) sind alle Ausdrücke der Form

$$h = a + ib + jc + kd \quad \text{mit} \quad a, b, c, d \in \mathbf{R}. \quad (2.1)$$

Die Summe zweier Quaternionen h und $h' = a' + ib' + jc' + kd'$ ist – wie bei den komplexen Zahlen – komponentenweise definiert:

$$h + h' := a + a' + i(b + b') + j(c + c') + k(d + d').$$

Damit ergeben sich die Additionsgesetze von \mathbf{H} wieder ganz einfach aus denen von \mathbf{R} : Das Nullelement ist $0 = 0 + i \cdot 0 + j \cdot 0 + k \cdot 0$, das additive Inverse („Negative“) des Elements

$h = a + ib + jc + kd$ ist

$$-h := -a + i(-b) + j(-c) + k(-d) .$$

Um die Multiplikation in \mathbf{H} zu definieren, definieren wir zuerst die Multiplikationsregeln für die imaginären Einheiten. Es soll sein

$$i^2 := -1, j^2 := -1, k^2 := -1, i \cdot j := k, j \cdot k := i, k \cdot i := j . \quad (2.2)$$

Ferner sollen die folgenden Rechenregeln für die Einheiten i, j und k gelten. Zum einen fordern wir das Assoziativgesetz für die imaginären Einheiten, also

$$j \cdot (j \cdot k) = (j \cdot j) \cdot k, k \cdot (k \cdot i) = (k \cdot k) \cdot i, i \cdot (i \cdot j) = (i \cdot i) \cdot j, i \cdot (j \cdot k) = (i \cdot j) \cdot k, \dots$$

zum zweiten soll jede der imaginären Einheiten i, j, k mit jeder reellen Zahl r vertauschbar sein; das heißt:

$$i \cdot r = r \cdot i, j \cdot r = r \cdot j, k \cdot r = r \cdot k \quad \text{für alle } r \in \mathbf{R} .$$

Daraus ergeben sich alle anderen Gesetze! Zum Beispiel: Sind damit alle Produkte der imaginären Einheiten erklärt? Ja, denn es ergibt sich:

$$j \cdot i = j \cdot (j \cdot k) = (j \cdot j) \cdot k = -1 \cdot k = -k .$$

Entsprechend folgt

$$k \cdot j = -i \text{ und } i \cdot k = -j .$$

Daraus ergibt sich sofort, dass \mathbf{H} in keinem Fall ein *kommutativer* Körper werden kann; denn es ist ja bereits

$$i \cdot j = k \neq -k = j \cdot i .$$

Damit \mathbf{H} zumindest ein Schiefkörper werden kann, müssen wir das Produkt beliebiger Quaternionen erklären. Das ist im Prinzip einfach: Wir multiplizieren die Quaternionen aus und bringen das Produkt auf die Form (2.1), indem wir die Gleichungen (2.2) benutzen.

Sollen wir das einmal mit zwei allgemeinen Quaternionen $h = a + ib + jc + kd$ und $h' = a' + ib' + jc' + kd'$ machen? Ja? Dann holen wir tief Luft und fangen an

$$\begin{aligned} h \cdot h' &= (a + ib + jc + kd) \cdot (a' + ib' + jc' + kd') \\ &= aa' + iab' + jac' + kad' + iba' + i^2bb' + ijb'c' + ikbd' \\ &\quad + jca' + jicb' + j^2cc' + jkcd' + kda' + kidb' + kjdc' + k^2dd' \\ &= aa' - bb' - cc' - dd' + i(ab' + ba' + cd' - dc') \\ &\quad + j(ac' - bd' + ca' + db') + k(ad' + bc' - cb' + da') . \end{aligned} \quad (2.3)$$

Frage Mal ehrlich, hätten Sie weiter gelesen, wenn ich mit dieser Multiplikationsregel angefangen hätte?

Nun zu den Körperaxiomen. Was ist das Einselement? Nach den Erfahrungen mit \mathbf{C} ist es verführerisch, das Element $1 (= 1 + i \cdot 0 + j \cdot 0 + k \cdot 0)$ zu probieren. Geben wir dieser Verführung nach; es ist:

$$1 \cdot h = 1 \cdot (a + ib + jc + kd) = a + ib + jc + kd = h$$

und

$$h \cdot 1 = (a + ib + jc + kd) \cdot 1 = a + ib + jc + kd = h.$$

Was ist das zu $h = a + ib + jc + kd$ inverse Element? Wir setzen dies als $h' = a' + ib' + jc' + kd'$ an und werten die Gleichung $h \cdot h' = 1$ aus. Gemäß (2.3) ergeben sich daraus die folgenden vier Gleichungen in den Unbekannten a', b', c', d' :

$$\begin{aligned} aa' - bb' - cc' - dd' &= 1, \\ ab' + ba' + cd' - dc' &= 0, \quad ac' - bd' + ca' + db' = 0, \\ ad' + bc' - cb' + da' &= 0. \end{aligned}$$

Daraus ergibt sich nach einigen Versuchen und nach höchstens dreimaligem Verrechnen die erstaunlich einfache Beziehung

$$h' = \left(\frac{a}{a^2 + b^2 + c^2 + d^2}, \frac{-b}{a^2 + b^2 + c^2 + d^2}, \frac{-c}{a^2 + b^2 + c^2 + d^2}, \frac{-d}{a^2 + b^2 + c^2 + d^2} \right).$$

Wir werden in Kap. 4 eine Methode kennen lernen, die solche Gleichungssysteme automatisch löst.

Nun zur Assoziativität der Multiplikation. Wir haben gefordert, dass das Assoziativgesetz jedenfalls für die Einheiten gilt. Nun kommt der Trick: Da wir die Multiplikation über die Multiplikation der Symbole i, j, k definiert haben, folgt die Assoziativität von \mathbf{H} aus der Assoziativität der imaginären Einheiten!

Das ist Mathematik: Wir haben das Problem der Verifizierung unendlich vieler Gleichungen darauf reduziert, überschaubar viele Gleichungen zu verifizieren!

In Übungsaufgabe 5 sollen Sie einen ähnlichen Trick für den Nachweis der *Distributivgesetze entwickeln*.

Insgesamt haben wir jetzt gezeigt, dass die Quaternionen einen echten Schiefkörper bilden! Die Konstruktion des Quaternionenschiefkörpers ist ein Stück klassischer Mathematik, das zur mathematischen Allgemeinbildung gehört. Studieren Sie es entsprechend gründlich.

Man könnte eine ganze Vorlesung über diesen Körper halten. Wir machen hier nur noch zwei kleine Bemerkungen.

1. Der Körper \mathbf{R} der reellen Zahlen ist in \mathbf{H} enthalten. Die reellen Zahlen sind nämlich genau die Quaternionen $a + ib + jc + kd$, bei denen die Koeffizienten b, c, d der imaginären Einheiten Null sind.
2. Auch der Körper \mathbf{C} der komplexen Zahlen ist in \mathbf{H} enthalten. Die komplexen Zahlen sind genau die Quaternionen $h = a + ib + jc + kd$, bei denen die Koeffizienten von j und k verschwinden.

Weitere Information über die Geschichte der Quaternionen und ihre mathematischen Eigenschaften findet man in [Ebbl], Kap. 6.

2.2.3 Einige endliche Körper

Zwar ist die Menge \mathbf{Z} aller ganzen Zahlen kein Körper (warum?), aber man kann aus \mathbf{Z} eine äußerst wichtige Klasse von Körpern gewinnen. Die Grundlage hierfür ist der **euklidische Algorithmus**.

Division mit Rest

Sei a eine ganze Zahl und b eine natürliche Zahl mit $b \geq 1$. Dann gibt es eindeutig bestimmte ganze Zahlen q und r mit folgenden Eigenschaften

$$a = q \cdot b + r \text{ und } 0 \leq r < b .$$

Man nennt r den **Rest**, der bei Division von a durch b entsteht.

Wir werden diesen Satz hier nicht beweisen; Sie sind im ersten Projekt des Kapitels 6 eingeladen, einen Beweis zu liefern. □

Einige *Beispiele*:

- $a = 13, b = 3$: $13 = 4 \cdot 3 + 1$, also $q = 4, r = 1$;
- $a = -13, b = 3$: $-13 = (-5) \cdot 3 + 2$, also $q = -5, r = 2$.

Für uns ist der Rest einer Division besonders wichtig; deshalb hat er eine wichtige Bezeichnung erhalten. Man bezeichnet ihn mit

$$a \bmod b \quad (\text{gesprochen „}a \text{ modulo } b\text{“}).$$

Tab. 2.1 Addition und Multiplikation in \mathbb{Z}_5

$+_5$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

\cdot_5	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Tab. 2.2 Addition und Multiplikation in \mathbb{Z}_6

$+_6$	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

\cdot_6	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Beispiele $13 \bmod 3 = 1$, $-13 \bmod 3 = 2$.

Wir schreiben

$$a \equiv b \pmod{n} \quad (\text{gesprochen „}a \text{ kongruent } b \text{ modulo } n\text{“}),$$

falls $a \bmod n = b \bmod n$ ist, d. h. falls a und b bei Division durch n den gleichen Rest ergeben.

Mit diesem Hilfsmittel können wir zu jeder natürlichen Zahl n eine algebraische Struktur \mathbb{Z}_n mit Addition und Multiplikation erklären, indem wir definieren:

\mathbb{Z}_n besteht aus den ganzen Zahlen $0, 1, \dots, n-1$; die Addition $+_n$ in \mathbb{Z}_n ist definiert durch

$$a +_n b := (a + b) \bmod n;$$

schließlich ist die Multiplikation \cdot_n in \mathbb{Z}_n definiert durch

$$a \cdot_n b := (a \cdot b) \bmod n.$$

In \mathbb{Z}_n werden also alle durch n teilbaren ganzen Zahlen mit 0 identifiziert; alle Zahlen, die bei Division durch n den Rest 1 ergeben, mit 1 usw. Die Addition und Multiplikation erfolgt „modulo n “. Wir schreiben den Index n an das Plus- und Malzeichen, um es nicht mit den Plus- und Malzeichen für ganze Zahlen zu verwechseln. Wenn keine Verwechslungsgefahr mehr besteht, werden wir den Index großzügig weglassen. Wir betrachten nun zwei Beispiele, nämlich \mathbb{Z}_5 und \mathbb{Z}_6 ; wir geben die Addition und die Multiplikation jeweils in einer Tabelle an (Tab. 2.1 und 2.2).

Was erkennen wir an diesen Beispielen? Sind diese Strukturen Körper? Schon auf den ersten Blick erkennen wir, dass die additiven Strukturen zwar sehr ähnlich, die multiplikativen Strukturen aber grundsätzlich verschieden sind. Bei \mathbb{Z}_5 ist zunächst kein Grund

zu erkennen, weshalb diese Struktur kein Körper sein sollte. Aber \mathbf{Z}_6 ? Hier sieht die Multiplikationstabelle schon sehr merkwürdig aus. Zwar ist 1 offenbar ein Einselement, aber das Element 2 hat kein Inverses (denn es gibt kein Element x mit $2 \cdot x = 1$)! Also kann \mathbf{Z}_6 bestimmt kein Körper sein.

Wir beantworten die Frage, ob überhaupt und wenn ja, welche \mathbf{Z}_n Körper sind, in drei Schritten.

1. Etappe

Für jede natürliche Zahl n erfüllt \mathbf{Z}_n alle Axiome eines kommutativen Körpers – bis möglicherweise auf die Existenz eines multiplikativen Inversen.

Dies ergibt sich daraus, dass sich die arithmetischen Gesetze von \mathbf{Z} auf \mathbf{Z}_n übertragen. Ganz einfach sind die Existenz der neutralen Elemente und des negativen Elements einzusehen: Da $a + 0 = a$ ist, ist auch $a +_n 0 = (a + 0) \bmod n = a + 0 = a$. Ebenso folgt $a \cdot 1 \bmod n = a$ für alle Elemente a von \mathbf{Z}_n . Das zu $a \in \mathbf{Z}_n$ negative Element ist $n - a$; denn es ist

$$a +_n (n - a) = (a + (n - a)) \bmod n = n \bmod n = 0.$$

Auch Assoziativ- und Distributivgesetz in \mathbf{Z}_n folgen aus den entsprechenden Gesetzen in \mathbf{Z} . Zum Beispiel ist für Elemente a, b, c von \mathbf{Z}_n :

$$\begin{aligned} (a +_n b) +_n c &= (a + b) \bmod n +_n c = ((a + b) \bmod n + c) \bmod n \\ &= (a + b + c) \bmod n = \dots = a +_n (b +_n c). \end{aligned}$$

Der Nachweis der Assoziativität der Multiplikation und des Distributivgesetzes ist Thema der Übungsaufgabe 11. \square

Der Beweis der ersten Etappe ist ein Beispiel für ein wichtiges Prinzip in der Mathematik, das *Homomorphieprinzip*: Eigenschaften gehen von einer ‚großen‘ Struktur (in unserem Fall \mathbf{Z}) durch eine geeignete Abbildung (einen „Homomorphismus“) auf eine kleine Struktur (in unserem Fall \mathbf{Z}_n) über. Wir werden solche Homomorphiephänomene in Abschn. 2.3 und ausführlich in Kap. 5 studieren. Es ist nicht erstaunlich, dass die „kleine“ Struktur entsprechende Eigenschaften wie die „große“ hat. Es ist aber zunächst nicht einsichtig, weshalb \mathbf{Z}_n (unsere „kleine“ Struktur) ein Körper sein soll (also zusätzliche Eigenschaften haben soll).

Der nächste Schritt gibt dafür auch keine zusätzlichen Indizien her.

2. Etappe

Wenn n eine zusammengesetzte ganze Zahl ist, also $n = ab$ mit $a > 1$ und $b > 1$, dann ist \mathbf{Z}_n bestimmt kein Körper.

Dies ergibt sich ohne große Schwierigkeiten: Ist $n = a \cdot b$ mit $a > 1$ und $b > 1$, so sind a und b Elemente von \mathbf{Z}_n mit

$$a \cdot_n b = (a \cdot b) \mod n = 0.$$

Dies ist aber in einem Körper unmöglich, da das Produkt je zweier von Null verschiedener Elemente ein von Null verschiedenes Element ergibt (Nullteilerfreiheit). \square

Damit können höchstens die Strukturen \mathbf{Z}_n Körper sein, für die n eine Primzahl ist. (Eine **Primzahl** ist eine ganze Zahl $p > 1$, die nur von 1 und p geteilt wird.)

Nun die Überraschung:

3. Etappe (Existenz von Körpern mit Primzahlordnung)

Wenn p eine Primzahl ist, dann ist \mathbf{Z}_p ein kommutativer Körper mit genau p Elementen.

Beweis Es ist klar, dass \mathbf{Z}_p genau p Elemente hat. Also ist nur zu zeigen, dass jedes Element $a \neq 0$ ein multiplikatives Inverses hat. Im Gegensatz zu den vorigen Untersuchungen werden wir das zu a inverse Element nicht explizit angeben, sondern nur seine Existenz zeigen. Wir brauchen dazu folgenden Hilfssatz über ganze Zahlen (den wir hier nicht beweisen):

Teilt die Primzahl p ein Produkt $a \cdot b$ ganzer Zahlen a und b , so teilt p mindestens eine der Zahlen a oder b .

Zum Beispiel folgt aus der Tatsache, dass eine Primzahl p die Zahl 35 teilt, dass p eine der Zahlen 5 oder 7 teilt, also dass $p = 5$ oder $p = 7$ ist. (Wenn p keine Primzahl ist, dann gilt diese Aussage nicht: 4 teilt $60 = 6 \cdot 10$, aber 4 teilt weder 6 noch 10.) Wir werden diesen Hilfssatz hier *nicht* beweisen, aber in Kap. 6 in allgemeinerem Rahmen ausführlicher darauf eingehen.

Nun ans Werk: Sei p eine Primzahl, sei a eine natürliche Zahl mit $1 \leq a < p$. Es ist zu zeigen, dass es eine natürliche Zahl $a' < p$ gibt mit $a \cdot_p a' = 1$, das heißt

$$a \cdot a' \mod p = 1.$$

Dazu betrachten wir die Produkte

$$0 \cdot_p a, 1 \cdot_p a, 2 \cdot_p a, 3 \cdot_p a, \dots, (p-1) \cdot_p a. \quad (*)$$

Behauptung Diese Zahlen sind paarweise verschieden „modulo p “.

Angenommen, es wäre $h \cdot_p a \bmod p = k \cdot_p a \bmod p$ mit $h \neq k$. Das bedeutet, dass $h \cdot a$ und $k \cdot a$ den gleichen Rest bei Division durch p haben. Also ist $h \cdot a - k \cdot a = (h - k) \cdot a$ durch p teilbar. Da p das Produkt $(h - k) \cdot a$ teilt, muss p einen der Faktoren teilen.

Kann p die Zahl a teilen? Nein. Denn a ist kleiner als p . Also muss p die Zahl $h - k$ teilen. Ferner liegt diese Zahl zwischen $-(p - 1)$ und $+(p - 1)$ (denn es ist $h \leq p - 1$ und $k \geq 0$). Die einzige Zahl in diesem Intervall, die durch p teilbar ist, ist aber – die Zahl 0. Daher muss $h - k = 0$, also $h = k$ sein: ein Widerspruch!

Was wissen wir jetzt? Die Elemente von $(\mathbb{Z}_p \setminus \{0\})$, die verschieden von $0 (= 0 \cdot_p a)$ sind, sind verschiedene Elemente von $\mathbb{Z}_p \setminus \{0\}$. Da dies $p - 1$ Elemente sind, und da $\mathbb{Z}_p \setminus \{0\}$ nur $p - 1$ Elemente hat, müssen das alle Elemente von $\mathbb{Z}_p \setminus \{0\}$ sein!

Was nützt uns dies? Viel! Daraus folgt nämlich, dass jedes Element aus $\mathbb{Z}_p \setminus \{0\}$ eine Darstellung der Form $(*)$ hat. Insbesondere hat die Zahl 1 eine solche Darstellung. Daher muss es eine Zahl $h \in \{1, \dots, p - 1\}$ geben mit

$$1 = h \cdot_p a.$$

Dann ist aber dieses Element $h \in \mathbb{Z}_p \setminus \{0\}$ invers zu a . □

2.2.4 Konstruktion eines Körpers mit vier Elementen

Wir stellen uns vor, dass es einen Körper K mit genau vier Elementen gibt. Wir werden sukzessiv die Elemente und die Operationen von K bestimmen. Dadurch wird dieser Körper so klar vor uns stehen, dass wir von seiner Existenz überzeugt sind.

Ein Körper K mit vier Elementen enthält – wie jeder Körper – die Elemente $0, 1, 1 + 1$ (das wir 2 taufen können), $1 + 1 + 1, \dots$. Diese Elemente müssen aber nicht notwendig verschieden sein. Im Gegenteil: Da K nur endlich viele Elemente hat, muss irgendwann

$$\underbrace{1 + 1 + \dots + 1}_{n \text{ mal}} = \underbrace{1 + 1 + \dots + 1}_{n \text{ mal}}$$

mit $n > m$ sein. Daraus ergibt sich

$$\underbrace{1 + 1 + \dots + 1}_{(n-m) \text{ mal}} = 0$$

Insbesondere ist 0 eine Summe von Einsen. Indem wir 1 subtrahieren, erhalten wir

$$\underbrace{1 + 1 + \dots + 1}_{(n-m-1) \text{ mal}} = -1$$

Insbesondere halten wir die erstaunliche Tatsache fest, dass das Element -1 von der Form $1 + 1 + \dots + 1$ ist.

Tab. 2.3 Die Addition in $\text{GF}(4)$

+	0	1	a	$a+1$
0	0	1	a	$a+1$
1	1	0	$a+1$	a
a	a	$a+1$	0	1
$a+1$	$a+1$	a	1	0

Wir wissen, dass \mathbb{Z}_4 kein Körper ist. Das bedeutet, dass K – falls ein solcher Körper überhaupt existiert! – nicht nur aus den Elementen $0, 1, 1+1, 1+1+1, \dots$ bestehen kann. Es muss also ein Element a von K geben, das nicht von der Form $0, 1, 1+1, \dots$ ist. Welche Elemente muss K enthalten?

Sicherlich – wie jeder Körper – die Elemente 0 und 1 . Außerdem a , also auch $a+1$. Kann $a+1$ eines der Elemente sein, die wir schon aufgelistet haben? Nein: Wäre $a+1 = a$, so folgte $1 = 0$; wäre $a+1 = 1$, so folgte $a = 0$; wäre $a+1 = 0$, so folgte $a = -1$, also von der Form $1+1+\dots+1$: In jedem Fall ein Widerspruch.

Also besteht der Körper K mit vier Elementen genau aus den Elementen $0, 1, a$ und $a+1$. Damit kann man die Additions- und Multiplikationstabelle leicht aufstellen.

Zunächst zur *Addition*: Da die Addition kommutativ ist, gilt $1+a = a+1$. Als nächstes folgt $1+1 = 0$, denn sowohl $1+1 = 1$ als auch $1+1 = a$ als auch $1+1 = a+1$ führen auf einen Widerspruch; also muss $1+1$ das vierte Element, also gleich 0 sein. Daraus folgt auch

$$a+a = a \cdot (1+1) = a \cdot 0 = 0$$

und

$$(a+1) + (a+1) = (a+1) \cdot (1+1) = (a+1) \cdot 0 = 0.$$

Damit ergeben sich alle anderen Summen:

$$(a+1) + 1 = a = 1 + (a+1) \text{ und } (a+1) + a = a + a + 1 = 1.$$

Die Additionstabelle sieht also wie folgt aus (Tab. 2.3).

Man sieht mit einem Blick, dass 0 das Nullelement ist und dass jedes Element genau eine additive Inverse hat. Mit etwas mehr Mühe zeigt man auch das Assoziativgesetz.

Nun zur *Multiplikation*: Alle Produkte, in denen 0 oder 1 als Faktor vorkommt, sind klar. Wir müssen also nur noch $a \cdot a$, $(a+1) \cdot a$, $a \cdot (a+1)$ und $(a+1) \cdot (a+1)$ bestimmen. Was kann $a \cdot (a+1)$ sein? Weder 0 (sonst wäre $a=0$ oder $a+1=0$), noch a (sonst wäre $a+1=1$), noch $a+1$ (sonst wäre $a=1$). Also muss $a \cdot (a+1) = 1$ sein. Entsprechend ergibt sich $(a+1) \cdot a = 1$. Daraus folgt

$$a^2 = a(a+1) + a = 1 + a = a+1 \text{ und } (a+1)^2 = (a+1)a + a+1 = 1 + a+1 = a.$$

Somit hat die Multiplikationstabelle folgendes Aussehen (Tab. 2.4).

Tab. 2.4 Die Multiplikation in $\text{GF}(4)$

\cdot	0	1	a	$a + 1$
0	0	0	0	0
1	0	1	a	$a + 1$
a	0	a	$a + 1$	1
$a + 1$	0	$a + 1$	1	a

Auch bei dieser Tabelle sieht man unschwer, dass jedes von Null verschiedene Element genau ein multiplikatives Inverses hat (denn in jeder von 0 verschiedenen Zeile und Spalte kommt das Element 1 genau einmal vor). Wie üblich sind das Assoziativ- und die Distributivgesetze zwar prinzipiell sehr einfach, in Wahrheit aber relativ mühsam nachzuweisen.

Wenn dies alles geleistet ist, dann haben wir bewiesen: Es gibt einen endlichen Körper mit genau 4 Elementen.

Schlussbemerkungen Endliche Körper mit q Elementen werden oft mit \mathbb{F}_q oder $\text{GF}(q)$ bezeichnet. („GF“ steht für „Galoisfeld“ nach Evariste Galois (1811–1832). Das Wort „Feld“ steht dabei für „Körper“; im Englischen heißt ein (mathematischer) Körper bis heute „field“.)

Evariste Galois hat (um das mindeste zu sagen) ein äußerst interessantes Leben geführt. Sie sollten nicht versäumen, in einem Buch über Geschichte der Mathematik (etwa [Wu-ßA]) den Roman seines Lebens nachzulesen.

Wir haben uns klargemacht, dass es endliche Körper $\text{GF}(p)$ gibt, wenn p eine Primzahl ist. In der Algebra zeigt man, dass es einen endlichen Körper $\text{GF}(q)$ genau dann gibt, wenn q eine Primzahlpotenz, also von der Form $q = p^n$ mit p Primzahl und n natürliche Zahl, ist. Jeder solche Körper ist bis auf Isomorphie (siehe den folgenden Abschnitt) eindeutig bestimmt. Das heißt: Für jede Primzahlpotenz q gibt es genau einen Körper mit q Elementen. In den Übungen (siehe Übungsaufgabe 14) wird $\text{GF}(9)$ konstruiert werden.

2.3 Automorphismen von Körpern

Es hat sich in der Mathematik als außerordentlich nützlich erwiesen, zu jeder Struktur die zugehörigen strukturerhaltenden Abbildungen (Homomorphismen, Automorphismen) zu betrachten. Wir untersuchen die Automorphismen von einigen der in Abschn. 2.2 konstruierten Körper; dies dient hauptsächlich dem Zweck, an substantiellem, aber technisch nicht zu schwierigem Stoff Mathematik zu üben.

2.3.1 Die Definitionen

Seien K und L Körper; wir bezeichnen in beiden Körpern die Addition mit $+$ und die Multiplikation mit \cdot .

Ein **Homomorphismus** von K nach L ist eine Abbildung f von K nach L , für die

$$f(x + y) = f(x) + f(y) \text{ und } f(x \cdot y) = f(x) \cdot f(y)$$

für alle $x, y \in K$ gilt und folgende Eigenschaft erfüllt ist:

$$f(1) \neq 0.$$

Anschaulich bedeutet dies: Die arithmetische Struktur von K (das heißt „ $x + y$ “, „ $x \cdot y$ “) wird durch f auf die arithmetische Struktur von L (also „ $f(x) + f(y)$ “, „ $f(x) \cdot f(y)$ “) übertragen.

Das Konzept der Homomorphie ist zentral in der Mathematik; es tritt bei allen Strukturen (algebraisch, geometrisch, topologisch, ...) auf. Wir werden es später im Rahmen der linearen Abbildungen ausführlich studieren.

Jeder Homomorphismus zwischen Körpern ist automatisch injektiv (siehe Übungsaufgabe 21). Ein Homomorphismus zwischen Körpern heißt ein **Isomorphismus**, falls er bijektiv ist. Wenn es einen Isomorphismus zwischen zwei Strukturen gibt, sagt man, sie sind **isomorph**.

Isomorphe Strukturen sind „strukturgleich“; das bedeutet, dass sie – bis auf eventuelle andere Namen für die Elemente und Verknüpfungen – gleich sind. Für die Isomorphie zweier Strukturen gebraucht man häufig das Symbol \cong .

Ein Isomorphismus einer Struktur auf sich selbst heißt **Automorphismus**. Jede Struktur hat mindestens einen Automorphismus, nämlich die identische Abbildung; diesen bezeichnet man auch als den **trivialen** Automorphismus.

In diesem Abschnitt werden wir die Automorphismen einiger der in Abschn. 2.2 konstruierten Körper studieren. Es ist leider aber so, dass die meisten dieser Körper nur den trivialen Automorphismus haben. Wir werden bis zu \mathbb{C} vorstoßen müssen, um einen – allerdings sehr wichtigen – nichttrivialen Automorphismus zu sehen.

2.3.2 Der Körper der rationalen Zahlen

In diesem Abschnitt beweisen wir den folgenden Satz.

Starrheit von \mathbb{Q}

Der Körper der rationalen Zahlen besitzt nur den trivialen Automorphismus.

Dazu überlegen wir uns zunächst zwei ganz einfache Hilfstatsachen, nämlich die Invarianz der neutralen Elemente und die Invarianz der negativen Elemente („Invarianz“ bedeutet Unveränderlichkeit).

Invarianz der neutralen Elemente

Jeder Automorphismus f eines beliebigen Körpers K führt das Nullelement 0 und Einselement 1 in sich über. Das heißt, es ist $f(0) = 0$ und $f(1) = 1$.

Zum Beweis schreiben wir

$$0 = 0 + 0$$

(dies folgt aus $a = a + 0$ für alle $a \in K$). Wenn wir auf beide Seiten f anwenden, ergibt sich

$$f(0) = f(0 + 0) = f(0) + f(0) .$$

Nun subtrahieren wir auf beiden Seiten $f(0)$ und erhalten

$$0 = f(0) - f(0) = f(0) + f(0) - f(0) = f(0) ,$$

d. h. $f(0) = 0$.

Damit folgt auch $f(1) \neq 0$. (Denn sonst wäre $f(1) = 0 = f(0)$, und f wäre nicht injektiv.) Nun wenden wir den entsprechenden Trick auf die Gleichung $1 = 1 \cdot 1$ an:

$$f(1) = f(1 \cdot 1) = f(1) \cdot f(1) .$$

Da $f(1) \neq 0$ ist, existiert $f(1)^{-1}$, und wir erhalten

$$1 = f(1) \cdot f(1)^{-1} = f(1) \cdot f(1) \cdot f(1)^{-1} = f(1) ,$$

also $f(1) = 1$. □

Die zweite einfache Tatsache ist die folgende:

Invarianz der negativen Elemente

Jeder Automorphismus f eines beliebigen Körpers K erfüllt

$$f(-a) = -f(a) \text{ für alle } a \in K .$$

Insbesondere ist stets

$$f(-1) = -f(1) = -1.$$

Es ist zu zeigen, dass $f(-a) + f(a) = 0$ ist:

$$f(-a) + f(a) = f((-a) + a) = f(0) = 0.$$

Nun zu **Q**: Sei f ein beliebiger Automorphismus des Körpers **Q**. Wir müssen zeigen, dass f jedes Element von **Q** fest lässt. Dazu schalten wir einen Schritt vor:

Invarianz der ganzen Zahlen

Jeder Automorphismus f von **Q** lässt jede ganze Zahl fest:

Beweis Sei zunächst n eine natürliche Zahl. Dann ist

$$n = \underbrace{1 + 1 + \dots + 1}_{n \text{ mal}}.$$

Da $f(1) = 1$ ist, ergibt sich daraus

$$f(n) = f(1 + 1 + \dots + 1) = f(1) + f(1) + \dots + f(1) = 1 + 1 + \dots + 1 = n.$$

Wenn $-n$ eine negative ganze Zahl ist, dann ist

$$-n = (-1) + (-1) + \dots + (-1) \quad (n \text{ mal}).$$

Da $f(-1) = -f(1) = -1$ ist, folgt

$$\begin{aligned} f(-n) &= f((-1) + (-1) + \dots + (-1)) = f(-1) + f(-1) + \dots + f(-1) \\ &= (-1) + (-1) + \dots + (-1) = -n. \end{aligned}$$

Daraus folgt, dass jede rationale Zahl $q = r/s$ festbleibt:

$$f(q) = f(r/s) = f(r \cdot s^{-1}) = f(r) \cdot f(s^{-1}) = f(r) \cdot f(s)^{-1} = r \cdot s^{-1} = q,$$

da $r, s \in \mathbb{Z}$.

(Die Gleichung $f(s^{-1}) = f(s)^{-1}$ ist Gegenstand von Übungsaufgabe 16.)

Damit haben wir gezeigt, dass der Körper **Q** nur den trivialen Automorphismus besitzt; man sagt dazu auch: **Q** ist **starr**.

2.3.3 Der Körper der reellen Zahlen

Nun zeigen wir, dass auch der Körper \mathbf{R} starr ist.

Dazu stellen wir uns wieder einen beliebigen Automorphismus f des Körpers \mathbf{R} vor und zeigen, dass f jede reelle Zahl auf sich abbildet. Genau so wie im vorigen Abschnitt zeigt man, dass f jede rationale Zahl wieder auf eine rationale Zahl abbildet (das Bild von r/s ist $f(r)/f(s)$). Also wissen wir, dass f einen Automorphismus von \mathbf{Q} „induziert“. Das Ergebnis des vorigen Abschnitts sagt also, dass f alle rationalen Zahlen festlassen muss. Daher brauchen wir uns nur noch zu überzeugen, dass f an keiner irrationalen Zahl „wackeln“ kann.

Der Trick besteht darin, eine irrationale Zahl zwischen rationalen Zahlen so einzuschachteln, dass sie nicht aus diesem Intervall entweichen kann. Dazu müssen wir nachweisen, dass f die Ordnungsrelation „ \leq “ respektiert:

Invarianz der Ordnungsrelation

Wenn $a < b$ ist, dann gilt $f(a) < f(b)$.

Das zunächst unlösbar scheinende Problem hierbei ist, dass nicht zu sehen ist, wie man f auf eine *Ungleichung* anwenden kann. Man könnte natürlich „ $a < b$ “ so in eine Gleichung verwandeln, dass man „ $a + c = b$ (mit positivem c)“ schreiben kann. Wenn man darauf f anwendet, erhält man

$$f(a) + f(c) = f(b) .$$

Da man aber nicht kontrollieren kann, ob $f(c)$ positiv oder negativ ist, nützt einem diese Gleichung wenig. Also muss man anders vorgehen. Hier kommt der folgende Trick zur Anwendung:

Aus $a < b$ folgt $b - a > 0$. Da jede positive reelle Zahl eine reelle Quadratwurzel hat, gibt es eine reelle Zahl r mit $b - a = r^2$. Damit sind wir in der Lage, mit f zu operieren:

$$f(b) - f(a) = f(b - a) = f(r^2) = f(r) \cdot f(r) > 0 ,$$

da das Quadrat einer jeden reellen Zahl nichtnegativ ist.

Das bedeutet

$$f(b) > f(a) .$$

Hieraus ergibt sich nun leicht, dass \mathbf{R} starr ist: Angenommen, es gäbe eine reelle Zahl r mit $f(r) \neq r$. Sei o. B. d. A. $r < f(r)$. („O. B. d. A.“ ist eine Abkürzung für „ohne Beschränkung der Allgemeinheit“; dies bedeutet in unserem Fall, dass der Fall „ $f(r) < r$ “ genauso funktioniert.)

Wir wählen eine rationale Zahl q mit

$$r < q < f(r) .$$

Wegen der Invarianz der Ordnungsrelation folgt aus $r < q$ aber

$$f(r) < f(q) = q .$$

Dies ist ein Widerspruch. Also bleibt jede reelle Zahl unter f fest. Somit gilt:

Starrheit von \mathbb{R}

Der Körper der reellen Zahlen besitzt nur den trivialen Automorphismus.

Nun kommen wir endlich zu einem Körper mit einem nichttrivialen Automorphismus.

2.3.4 Konjugiert-komplexe Zahlen

Der Körper \mathbb{C} der komplexen Zahlen hat zwar – man glaubt es kaum – überabzählbar viele Automorphismen (siehe etwa [Hun, S. 317, Exercise 6]), *ein* Automorphismus spielt aber eine ganz besondere Rolle; diesen behandeln wir hier.

Für eine komplexe Zahl $z = a + ib$ sei

$$\bar{z} = a - ib$$

Diese Zahl heißt die zu z **konjugiert-komplexe Zahl**.

Satz über konjugiert-komplexe Zahlen

Die Abbildung f von \mathbb{C} in sich, die definiert ist durch

$$f(z) = f(a + ib) := a - ib = \bar{z} ,$$

ist ein Automorphismus von \mathbb{C} .

Beweis Offenbar ist f surjektiv und injektiv. Sind $z = a + ib$ und $z' = a' + ib'$ zwei beliebige komplexe Zahlen, so gilt:

$$f(z + z') = f(a + a' + i(b + b')) = a + a' - i(b + b') = a - ib + a' - ib' = f(z) + f(z') ,$$

und

$$\begin{aligned} f(z z') &= f((a + ib)(a' + ib')) = f(aa' - bb' + i(ab' + a'b)) \\ &= aa' - bb' - i(ab' + a'b) = (a - ib)(a' - ib') = f(z)f(z') . \end{aligned}$$

Hurra! Die Abbildung f ist ein Automorphismus von \mathbf{C} , der nicht alle Elemente fest lässt!

Apropos: Welche Elemente von \mathbf{C} bleiben unter f fest? Das sind diejenigen Elemente, für die gilt

$$f(z) = z,$$

also

$$a - ib = a + ib, \quad \text{d. h.} \quad 0 = 2ib, \quad \text{also} \quad b = 0.$$

Das sind also genau die Elemente von \mathbf{C} , deren Imaginärteil gleich Null ist, also genau die reellen Zahlen.

2.4 Verständnisfragen, Übungen und Tipps

Richtig oder falsch?

1. Thema: Komplexe Zahlen

- ☐ i ist die einzige komplexe Zahl, deren Quadrat gleich -1 ist.
- ☐ 1 ist die einzige komplexe Zahl, die zu sich selbst (multiplikativ) invers ist.
- ☐ Die multiplikative Inverse einer Zahl aus $\mathbf{C} \setminus \mathbf{R}$ ist nicht reell.
- ☐ Das Produkt je zweier Zahlen aus $\mathbf{C} \setminus \mathbf{R}$ ist in $\mathbf{C} \setminus \mathbf{R}$.

2. Thema: Automorphismen von Körpern.

Sei K ein Körper.

- ☐ Die Identität ist immer ein Automorphismus von K .
- ☐ Die Identität ist nie ein Automorphismus von K .
- ☐ Jeder Körper hat nur die Identität als Automorphismus.
- ☐ Jeder Körper hat mindestens zwei Automorphismen, nämlich die Identität und die **Nullabbildung** (das ist diejenige Abbildung, die jedes Element auf 0 abbildet).
- ☐ Kein Automorphismus $\neq \text{id}$ bildet ein Element von K auf sich ab.
- ☐ Jeder Automorphismus von K lässt mindestens zwei Elemente von K fest.
- ☐ $\text{GF}(4)$ hat nur die Identität als Automorphismus.

Übungsaufgaben

1. Überzeugen Sie sich, dass jedes der Gleichheitszeichen in folgender Gleichungskette im Körper \mathbf{C} der komplexen Zahlen zu Recht besteht (das heißt, auf die Definition zurückgeführt werden kann).

$$\begin{aligned} (a + bi)(a' + b'i) &= aa' + ab'i + bia' + bi \cdot b'i \\ &= aa' + bb'i^2 + (ab' + ba')i \\ &= aa' - bb' + (ab' + ba')i = z \cdot z'. \end{aligned}$$

2. Zeigen Sie, dass in \mathbf{C} die Assoziativgesetze und das Distributivgesetz gelten.
3. Berechnen Sie die multiplikativen Inversen der folgenden komplexen Zahlen:

$$5 + 2i, 7 - i, 1 + 2i.$$

4. Zeigen Sie, dass für die Einheiten von \mathbf{H} das Assoziativgesetz gilt, falls man (neben den anderen Festlegungen, die wir in Abschn. 2.2 für die Einheiten getroffen haben) nur die folgenden Gesetze fordert:

$$j \cdot (j \cdot k) = (j \cdot j) \cdot k, k \cdot (k \cdot i) = (k \cdot k) \cdot i, i \cdot (i \cdot j) = (i \cdot i) \cdot j.$$

5. (a) Zeigen Sie: Man kann die Gültigkeit der Distributivgesetze in \mathbf{H} auf die Gültigkeit der Distributivgesetze für die Einheiten zurückführen.
(b) Weisen Sie die Distributivgesetze für die Einheiten von \mathbf{H} nach.
6. Führen Sie den Quaternionenschiefkörper nach der Art und Weise ein, in der wir die komplexen Zahlen eingeführt haben. Also etwa so: Die Quaternionen sind die 4-Tupel (a, b, c, d) reeller Zahlen. Speziell setzen wir fest: $i := (0, 1, 0, 0)$, $j := (0, 0, 1, 0)$, $k := (0, 0, 0, 1)$. Die Addition wird komponentenweise definiert.
(a) Definieren Sie die Multiplikation.
(b) Zeigen Sie, dass man auf diese Weise einen Schiefkörper erhält.
7. Sei n eine natürliche Zahl. Zeigen Sie: Wenn a, b, a', b' natürliche Zahlen sind mit

$$a' \equiv a \pmod{n} \text{ und } b' \equiv b \pmod{n},$$

so gilt auch

$$a' + b' \equiv a + b \pmod{n} \text{ und } a' \cdot b' \equiv a \cdot b \pmod{n}.$$

8. Lösen Sie die folgenden Gleichungen „modulo 11“ (das heißt in \mathbf{Z}_{11}):

$$6 \cdot x = 2, 2 \cdot x + 4 = 9, 3 \cdot x - 9 = 5, 7 \cdot x = 1.$$

9. Welche der folgenden Gleichungen sind „modulo 12“ (das heißt in \mathbf{Z}_{12}) lösbar? Geben Sie gegebenenfalls eine Lösung an:

$$6 \cdot x = 2, 2 \cdot x + 4 = 9, 3 \cdot x - 9 = 5, 7 \cdot x = 1.$$

10. Warum ist \mathbf{Z}_{ab} für $a > 1$ und $b > 1$ kein Körper?
Ist es möglich, dass eine Teilmenge $U \subseteq \mathbf{Z}_{ab}$ (mit der Addition und Multiplikation von \mathbf{Z}_{ab} !) ein Körper ist?
11. Zeigen Sie, dass in \mathbf{Z}_n das Assoziativ- und das Distributivgesetz gelten.

12. Die **Ordnung** eines Elements $a \neq 0$ aus \mathbf{Z}_n ist die kleinste natürliche Zahl i mit $a^i = 1$ (in \mathbf{Z}_n). Bestimmen Sie die Ordnung in folgenden Fällen:

$$a = 5, n = 7; a = 10, n = 17; a = 8, n = 15; a = 2, n = 7.$$

13. Überlegen Sie, dass es keinen Körper mit genau 6 Elementen gibt.
 14. Konstruieren Sie einen Körper, der genau 9 Elemente hat.
 15. Sei K ein Körper, in dem es kein Element a gibt, für das $a^2 = -1$ gilt. Wir definieren auf der Menge $K \times K$ die Addition komponentenweise und eine Multiplikation durch folgende Vorschrift:

$$(x, y) \cdot (x', y') := (xx' - yy', xy' + x'y).$$

- (a) Zeigen Sie, dass die so definierte Struktur ein Null- und ein Einselement besitzt.
 (b) Zeigen Sie, dass jedes von 0 verschiedene Element ein multiplikatives Inverses besitzt.
 (c) Ist $K \times K$ mit den oben definierten Verknüpfungen ein Körper?
 16. Zeigen Sie: Wenn f ein Automorphismus eines Körpers K ist, dann gilt $f(k^{-1}) = f(k)^{-1}$ für alle $k \in K \setminus \{0\}$.
 17. Sei K ein endlicher Körper.
 (a) Dann gibt es eine natürliche Zahl n derart, dass

$$n \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{n \text{ mal}} = 0.$$

gilt.

- (b) Sei p die kleinste natürliche Zahl mit $p \cdot 1 = 0$. Zeigen Sie: p ist eine Primzahl.
 [Man nennt p die **Charakteristik** des Körpers K]
 18. (a) Sei p eine Primzahl. Zeigen Sie: \mathbf{Z}_p hat die Charakteristik p .
 (b) Sei K ein Körper mit Charakteristik p . Dann enthält K einen Körper, der isomorph zu \mathbf{Z}_p ist.
 (c) Sei K ein Körper der Charakteristik p , und sei K nicht isomorph zu \mathbf{Z}_p . Dann gilt $|K| \geq p^2$.
 19. Bestimmen Sie alle Automorphismen der Körper $\text{GF}(2)$, $\text{GF}(3)$, $\text{GF}(4)$.
 20. Bestimmen Sie alle Automorphismen des Körpers $\text{GF}(p)$ ($= \mathbf{Z}_p$), wobei p eine Primzahl ist.
 21. Sei $f: K \rightarrow L$ ein Homomorphismus des Körpers K in den Körper L . Zeigen Sie:
 (a) Das Element $0 \in K$ ist das einzige Element, das auf $0 \in L$ abgebildet wird.
 (b) Die Abbildung f ist injektiv.

Projekt: Die Gaußsche Zahlenebene

Ein „Projekt“ ist eine große Übungsaufgabe. Sie sollten versuchen, nachdem Sie den Stoff verstanden haben, ein Projekt zu bearbeiten. Nehmen Sie sich dazu eine Woche

Zeit, lösen Sie pro Tag eine Teilaufgabe. Versuchen Sie, Ihre Erkenntnisse sauber aufzuschreiben.

Erschrecken Sie nicht vor der Länge der Aufgabenstellung. Diese dient nur dazu, Ihnen zu helfen und Ihnen genau zu sagen, was Sie im nächsten Teilschritt tun sollten.

Carl Friedrich Gauß (1777–1855), einer der bedeutendsten Mathematiker aller Zeiten, hat mit seiner geometrischen Interpretation der komplexen Zahlen wesentlich dazu beigetragen, dass man allgemein an die Existenz der komplexen Zahlen „glaubte“. (Diese Interpretation war allerdings schon zuvor von John Wallis (1616–1703) erahnt und von Caspar Wessel (1745–1818) präzise formuliert worden.)

Der erste Schritt ist ganz einfach: Wir identifizieren die komplexe Zahl $a + ib$ mit dem Punkt $P = (a, b)$ der kartesischen Ebene (siehe Abb. 2.1). Zum Beispiel wird die Zahl 0 mit dem Koordinatenursprung $O = (0, 0)$ identifiziert. Umgekehrt nennt man die kartesische Ebene, bei der jeder Punkt als komplexe Zahl interpretiert wird, die **Gaußsche Zahlenebene** (Abb. 2.1).

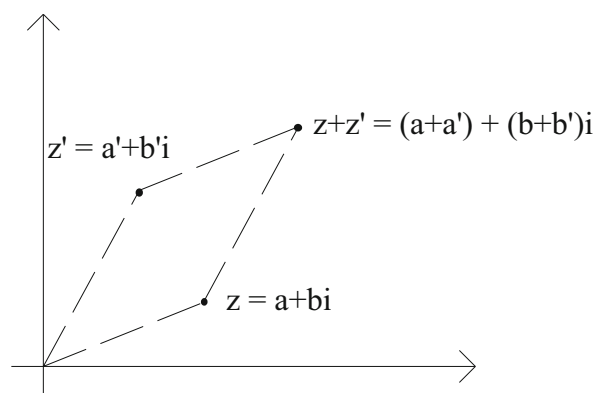


Abb. 2.1 Die Gaußsche Zahlenebene

Die Frage ist jetzt, ob sich die Addition und die Multiplikation im Körper \mathbb{C} geometrisch deuten lassen. Wir setzen für dieses Projekt einige elementare Kenntnisse der ebenen Geometrie voraus. Als einführende und vertiefende Literatur empfehle ich [Cox], Kap. 9.

1. Zeigen Sie, dass die Summe der Elemente $a + ib, c + id \in \mathbb{C}$ der Summe der Punkte (a, b) und (c, d) entspricht. Die **Summe** zweier Punkte P und Q ist dabei erklärt als der vierte Punkt des Parallelogramms, das die Punkte O, P und Q als Ecken hat.

Nun zur Multiplikation. Die Multiplikation eines Punktes mit einer reellen Zahl ist einfach zu beschreiben.

2. Auf welchen Punkt wird ein Punkt A abgebildet, wenn er mit 2 multipliziert wird? Gibt es einen Punkt, der bei dieser Abbildung unverändert bleibt? (Einen solchen Punkt nennt man **Fixpunkt**.) Welche Geraden bleiben fest?

Eine **Streckung** ist eine Abbildung der Ebene \mathbf{R}^2 in sich, die Geraden in Geraden überführt, genau einen Fixpunkt P (das **Zentrum**) hat, so dass jede Gerade durch diesen Fixpunkt in sich überführt wird.

3. Zeigen Sie: Die Abbildung der Gaußschen Zahlenebene in sich, die durch Multiplikation mit einer reellen Zahl $\neq 0$ beschrieben wird, ist eine Streckung mit Zentrum O .

Nun zur Multiplikation mit echt komplexen Zahlen.

4. Zeichnen Sie ein Dreieck mit den Eckpunkten $A = (a, a')$, $B = (b, b')$ und $C = (c, c')$ in die Ebene (wählen Sie konkrete Werte für a, a', b, b', c, c'). Multiplizieren Sie jeden Punkt mit i . (Das heißt: Bilden Sie die Punkte $A^* = (a + ia')i$, $B^* = \dots$) Beschreiben Sie die geometrische Operation, die das Ausgangsdreieck vollzogen hat.
5. Welchen Effekt beobachten Sie, wenn Sie die Punkte A, B, C mit der komplexen Zahl $z = \cos 45^\circ + i \cdot \sin 45^\circ$ multiplizieren.
6. Zeigen Sie: Die Multiplikation mit der komplexen Zahl $z = \cos \varphi + i \cdot \sin \varphi$ beschreibt eine Drehung um den Ursprung um den Winkel φ .
Für welchen Winkel φ erhält man eine Punktspiegelung?
7. Beschreiben Sie die geometrische Operation, die durch die Multiplikation mit einer komplexen Zahl $c + id$ beschrieben wird, indem Sie diese als Hintereinanderausführung einer Drehung und einer Streckung („Drehstreckung“) beschreiben.

Es gibt noch weitere geometrisch interessante Abbildungen, zum Beispiel die Spiegelungen an einer Achse. Kann man auch diese in der Gaußschen Zahlenebene darstellen? Nichts leichter als das:

8. Zeigen Sie: Die Abbildung $\sigma: z \rightarrow \bar{z}$ beschreibt eine Spiegelung an der x -Achse. (Dafür müssen Sie zeigen, dass σ Punkte in Punkte, Geraden in Geraden überführt, dass jeder Punkt der x -Achse festbleibt und dass jede Gerade senkrecht zur x -Achse in sich überführt wird.)

Sie sollten mit folgenden Begriffen umgehen können

Körper, neutrales Element, inverses Element, Assoziativität, Distributivität, Kommutativität, Schiefkörper, \mathbf{R} , \mathbf{C} , i , imaginäre Einheit, Realteil, Imaginärteil, \mathbf{H} , Quaternionen, $a \bmod b$, \mathbf{Z}_n , $\text{GF}(q)$, Homomorphismus, Isomorphismus, isomorph, Automorphismus, starrer Körper, konjugiert komplex



Lineare Algebra

Eine Einführung in die Wissenschaft der Vektoren,
Abbildungen und Matrizen

Beutelspacher, A.

2014, XIV, 368 S. 13 Abb., 10 Abb. in Farbe., Softcover

ISBN: 978-3-658-02412-3