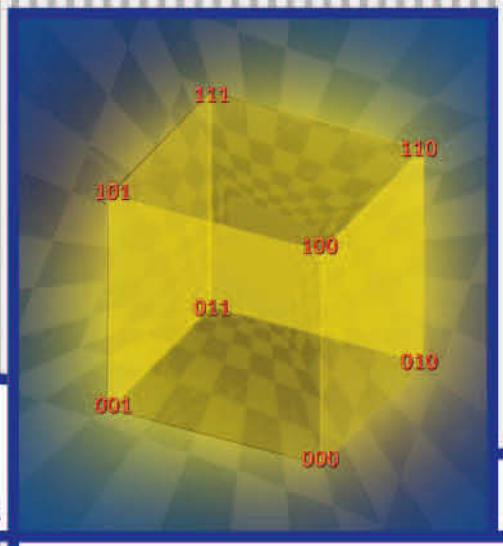


it informatik

Dirk Hachenberger

Mathematik für Informatiker

2., aktualisierte Auflage

PEARSON Studium

Dirk Hachenberger

Mathematik für Informatiker

2., aktualisierte Auflage

PEARSON Studium

ein Imprint von Pearson Education
München • Boston • San Francisco • Harlow, England
Don Mills, Ontario • Sydney • Mexico City
Madrid • Amsterdam

Zu den Distributivgesetzen wäre noch zu sagen, dass wir die Multiplikationsbezeichnung $\cdot$ der Einfachheit halber weggelassen haben. Ferner bedeutet etwa $ab + ac$ eigentlich $(ab) + (ac)$. Da aber (wie aus der Schule beim Rechnen mit reellen Zahlen bekannt) der Multiplikation auch bei abstrakten Ringen eine höhere Priorität als der Addition eingeräumt wird, können diese Klammern weggelassen werden. Im Term $(a + b)c$ sind Klammern freilich notwendig, um der Addition von a und b eine höhere Priorität als der Multiplikation mit c einzuräumen.

Beispiel 6.4.2 **Zahlbereiche**

Wir betrachten die natürlichen, die ganzen, die rationalen und die reellen Zahlen zusammen mit der üblichen Addition und der üblichen Multiplikation. Es ist $(\mathbb{N}, +, \cdot, 0, 1)$ kein Ring, weil $(\mathbb{N}, +, 0)$ keine Gruppe ist. Die folgenden drei Zahlbereiche sind aber allesamt Ringe:

$$(\mathbb{Z}, +, \cdot, 0, 1), \quad (\mathbb{Q}, +, \cdot, 0, 1), \quad (\mathbb{R}, +, \cdot, 0, 1)$$

B Allgemeine Rechengesetze bei Ringen Wir kommen nun zu den wichtigsten Rechengesetzen bei Ringen, welche uns durch den Umgang mit ganzen, rationalen oder reellen Zahlen sehr vertraut vorkommen werden. Der Grund, warum wir einen Nachweis führen ist der, dass diese Gesetze sich allein als Folgerungen der Ring-Axiome ergeben und daher in einem jeden (Modell für einen) Ring gelten, insbesondere bei den Zahlbereichen $\mathbb{Z}$ und $\mathbb{Q}$ und $\mathbb{R}$.

Satz 6.4.3 In einem Ring $(R, +, \cdot, 0, 1)$ gelten die folgenden Gesetze:

(1) $a \cdot 0 = 0 = 0 \cdot a$ für jedes $a \in R$

(2) $a(-b) = (-a)b = -(ab)$ für alle $a, b \in R$

(3) $(-a)(-b) = ab$ für alle $a, b \in R$

Beweis

(1) Da 0 das neutrale Element bzgl. der Addition ist, gilt $0 + 0 = 0$ und daher ist $0 \cdot a = (0 + 0) \cdot a$ für jedes $a \in R$. Das Distributivgesetz liefert somit $0 \cdot a = 0 \cdot a + 0 \cdot a$. Nun addiert man auf beiden Seiten mit $-(0 \cdot a)$, dem additiven Inversen von $0 \cdot a$, und erhält aufgrund der Neutralität von 0 sogleich $0 = 0 \cdot a$. Ganz analog zeigt man die Gültigkeit von $a \cdot 0 = 0$ für jedes $a \in R$.

(2) Aufgrund des Distributivgesetzes gilt $ab + a(-b) = a(b + (-b)) = a \cdot 0$. Nach (1) ist dies gleich 0. Das bedeutet aber, dass $a(-b)$ additiv invers zu ab und daher gleich $-(ab)$ ist. Ebenso gilt $ab + (-a)b = (a + (-a))b = 0 \cdot b = 0$, weshalb auch $(-a)b$ additiv

invers zu ab ist. Aufgrund der Eindeutigkeit von (additiven) Inversen folgt somit die Behauptung.[5]

(3) Unter erneuter Verwendung des Distributivgesetzes und (1) gilt $(-a)(-b) + (-a)b = (-a)((-b) + b) = (-a) \cdot 0 = 0$. Also ist $(-a)(-b)$ additiv invers zu $(-a)b$. Da Letzteres nach (2) aber gleich $-ab$ ist, folgt $(-a)(-b) = -(-ab) = ab$, die Behauptung. ■

Es folgen einige Bemerkungen zu ▶Satz 6.4.3:

1. Wählt man in (2) speziell $a = 1$, so folgt $-b = 1 \cdot (-b) = (-1) \cdot b$ für alle $b \in R$.
2. Sind $a = 1$ und $b = 1$, so erhält man $(-1)^2 = 1$ aus (3).
3. Ist $R = \{x\}$ eine Menge, welche nur ein einziges Element x enthält, so sind trivialerweise durch $x \cdot x = x$ und $x + x = x$ zwei Verknüpfungen gegeben, welche alle Axiome aus ▶Definition 6.4.1 erfüllen. Hierbei ist x sowohl neutral bzgl. der Addition als auch neutral bzgl. der Multiplikation. Um diesen langweiligen Fall auszuschließen, haben wir in ▶Definition 6.4.1 gefordert, dass ein Ring wenigstens zwei verschiedene Elemente haben soll.
4. Ist also R ein Ring, so gibt es ein $a \in R$ mit $a \neq 0$. Aufgrund der Neutralität von 1 ist $1 \cdot a = a$. Wegen ▶Satz 6.4.3 ist weiter $0 \cdot a = 0$. Wegen $0 \neq a$ ist daher $1 \cdot a \neq 0 \cdot a$ und und die beiden neutralen Elemente, nämlich 0 und 1, müssen verschieden sein, i. e. $0 \neq 1$.

Ab jetzt bezeichne (ähnlich wie bei den Zahlbereichen) R^* die Teilmenge der von 0 verschiedenen Elemente aus R. Es ist also $1 \in R^* = R \setminus \{0\}$.

C Integritätsbereiche Wir werden im Verlaufe dieses Buches noch viele wichtige Beispiele von Ringen kennenlernen, u. a. sind Restklassenringe, Matrizenringe, Polynomringe und formale Potenzreihenringe zu nennen. Bevor wir zu einigen einfachen Beispielen kommen, fahren wir an dieser Stelle mit zwei Definitionen fort, um spezielle Ringe hervorzuheben.

Definition 6.4.4 Es sei $(R, +, \cdot, 0, 1)$ ein Ring. Ist $(R^*, \cdot, 1)$ ein Teilmonoid von $(R, \cdot, 1)$, so nennt man R einen **Integritätsbereich** (kurz: **Bereich**, engl.: *domain*).

Will man von einem Ring zeigen, dass es sich um einen Integritätsbereich handelt, so muss man nur nachweisen, dass $R^* = R \setminus \{0\}$ bzgl. der Multiplikation abgeschlossen ist (siehe ▶Definition 6.3.1, wir haben ja soeben gesehen, dass wegen $0 \neq 1$ das Element 1

[5] Man schreibt daher auch einfach $-ab$ für $-(ab)$.

in R^* enthalten ist). Das bedeutet wiederum: Sind $x, y \in R^*$, so ist auch $xy \in R^*$, d. h., ist $x \neq 0$ und ist $y \neq 0$, so ist auch $xy \neq 0$. Nochmals anders ausgedrückt bedeutet die Eigenschaft „Integritätsbereich“:

- *Sind* $a, b \in R$ *mit* $ab = 0$*, so folgt* $a = 0$ *oder* $b = 0$, i. e., „ein Produkt ist genau dann gleich null, wenn wenigstens ein Faktor gleich null ist“.

Somit sind die Zahlbereiche $(\mathbb{Z}, +, \cdot, 0, 1)$ und $(\mathbb{Q}, +, \cdot, 0, 1)$ sowie $(\mathbb{R}, +, \cdot, 0, 1)$ allesamt Integritätsbereiche. Wir werden später sowohl kommutative als auch nichtkommutative Ringe kennenlernen, die keine Bereiche sind.

Liegt ein Integritätsbereich zugrunde, so kann man aus $a \neq 0$ und der Gleichung $ab = ac$ folgern, dass $b = c$ ist. Diesen Vorgang bezeichnet man auch als **Kürzungsregel**. Es ist nämlich $ab = ac$ äquivalent zu $ab - ac = 0$, also zu $a(b - c) = 0$. Ist also $a \neq 0$, so muss $b - c = 0$ sein, was wiederum $b = c$ bedeutet. Liegt hingegen ein allgemeiner Ring zugrunde, so kann man aus $a \neq 0$ und $ab = ac$ nicht unbedingt $b = c$ folgern!

D Die Einheitengruppe eines Ringes, Schiefkörper und Körper Der Begriff „Einheitengruppe eines Ringes“ bezieht sich auf die multiplikative Struktur.

Definition 6.4.5 Die **Einheitengruppe** $E(R)$ eines Ringes $(R, +, \cdot, 0, 1)$ ist die Menge der Elemente, die bzgl. der Multiplikation invertierbar sind, also

$$E(R) := \{x \in R: \text{ es gibt ein } y \in R \text{ mit } xy = 1 = yx\}.$$

In diesem Zusammenhang nennt man die multiplikativ invertierbaren Elemente von R auch **Einheiten** von R.

Ist x eine Einheit von R, so ist x von 0 verschieden. Ist nämlich y multiplikativ invers zu x, so folgte aus $x = 0$ durch Multiplikation beider Seiten mit y, dass $xy = 0 \cdot y = 0$ ist. Nun ist aber $xy = 1$ sowie $0 \neq 1$, was einen Widerspruch liefert. Insofern ist die Einheitengruppe $E(R)$ eines Ringes stets eine Teilmenge von R^*.

So wie die vollkommensten Monoide die Gruppen sind, spielen die Ringe, in denen man (wie eben gesehen mit der notwendigen Ausnahme der Null) uneingeschränkt multiplikativ invertieren kann, eine wichtige Rolle. Es sind dies die Schiefkörper und, im kommutativen Fall, die Körper.

Definition 6.4.6 Es sei $(K, +, \cdot, 0, 1)$ ein Ring. Annahme, jedes $x \in K^*$ ist multiplikativ invertierbar,[6] was damit gleichbedeutend ist, dass $(K^*, \cdot, 1)$ eine Gruppe ist. Dann nennt man K einen **Schiefkörper**. Ist K zudem ein kommutativer Ring, was damit gleichbedeutend ist, dass $(K^*, \cdot, 1)$ eine kommutative bzw. abelsche Gruppe ist, so nennt man K einen **Körper**.

Es ist $(\mathbb{Z}, +, \cdot, 0, 1)$ kein Körper, da lediglich 1 und -1 Einheiten in $\mathbb{Z}$ sind. Allerdings bilden die rationalen Zahlen $(\mathbb{Q}, +, \cdot)$ ebenso wie die reellen Zahlen $(\mathbb{R}, +, \cdot)$ jeweils Körper. Mit den komplexen Zahlen $\mathbb{C}$ werden wir im nächsten Abschnitt einen weiteren Körper kennenlernen; es handelt sich dabei um eine Erweiterung der reellen Zahlen. Des Weiteren werden wir im übernächsten Abschnitt die komplexen Zahlen ihrerseits zum Zahlbereich der Quaternionen erweitern. Diese Quaternionen bilden einen Schiefkörper, welcher kein Körper ist; in einem solchen Fall spricht man von einem **echten Schiefkörper**.

E Grundlegende Beispiele von Ringen Nachdem wir nun alle wichtigsten grundlegenden Definitionen von Ringen beisammen haben, werden wir uns einigen einfachen Beispielen widmen.

Beispiel 6.4.7 ***n*-Tupel über Ringe**

Es sei $(R, +, \cdot, 0, 1)$ ein Ring und $n \in \mathbb{N}^*$. Versieht man R^n, die Menge aller n-Tupel über R mit der punktweisen Addition $\oplus$ und der punktweisen Multiplikation $\odot$, so erhält man einen Ring $(R^n, \oplus, \odot)$, dessen Null das n-Tupel $(0, 0, \ldots, 0)$ und dessen Eins das n-Tupel $(1, 1, \ldots, 1)$ ist. Mit diesen punktweisen Operationen ist R^n genau dann kommutativ, wenn R kommutativ ist. Wie wir ebenfalls aus dem Abschnitt über Monoide wissen, ist die Einheitengruppe dieses Ringes gleich $E(R)^n$, dem n-fachen kartesischen Produkt der Einheitengruppe von R (versehen mit der punktweisen Multiplikation).

Ist $n \geq 2$, so handelt es sich bei $(R^n, \oplus, \odot)$ nicht um einen Integritätsbereich, selbst wenn R ein Integritätsbereich ist (ja selbst, wenn R ein Körper sein sollte): Ist nämlich e^i das n-Tupel, welches an der i-ten Position eine 1 und an allen anderen Positionen einen 0-Eintrag hat, so gilt $e^i \odot e^j = (0, 0, \ldots, 0)$, falls $i \neq j$, also beispielsweise $e^1 \odot e^2 = (0, 0, \ldots, 0)$. ■

Beispiel 6.4.8 **Ringstrukturen bei Mengensystemen**

Ausgehend von einer nichtleeren Menge N betrachten wir die Potenzmenge $\mathcal{P}(N)$ zusammen mit der symmetrischen Differenz Δ (als Addition) und der Schnittmengen-

[6] In diesem Fall ist, wie man als Übung nachrechnen möge, $(K, +, \cdot, 0, 1)$ automatisch ein Integritätsbereich!

bildung $\cap$ (als Multiplikation). Aufgrund der entsprechenden Beispiele aus den beiden Abschnitten über Monoide und Gruppen wissen wir bereits, dass $(\mathcal{P}(N), \Delta, \emptyset)$ eine kommutative Gruppe und $(\mathcal{P}(N), \cap, N)$ ein kommutatives Monoid darstellen. Durch den nun folgenden Nachweis des Distributivgesetzes $X \cap (Y \Delta Z) = X \cap Y \Delta X \cap Z$ erhalten wir sodann, dass es sich bei $(\mathcal{P}(N), \Delta, \cap, \emptyset, N)$ um einen kommutativen Ring handelt. Dazu bedienen wir uns, ähnlich wie bei der Assoziativität von Δ in ▶Beispiel 6.1.9, einer Wahrheitstafel.

X	Y	Z	$Y \Delta Z$	$X \cap Y$	$X \cap Z$	$X \cap (Y \Delta Z)$	$X \cap Y \Delta X \cap Z$
1	1	1	0	1	1	0	0
1	1	0	1	1	0	1	1
1	0	1	1	0	1	1	1
1	0	0	0	0	0	0	0
0	1	1	0	0	0	0	0
0	1	0	1	0	0	0	0
0	0	1	1	0	0	0	0
0	0	0	0	0	0	0	0

Es ist zu bemerken, dass dieser Ring kein Integritätsbereich ist, wenn N mehr als ein Element enthält. Sind nämlich x und y zwei verschiedene Elemente von N und wählt man beispielsweise $X = \{x\}$ und $Y = \{y\}$, so gilt $X \cap Y = \emptyset$. Das bedeutet, dass das Produkt von X und Y hier gleich null ist, ohne dass einer der Faktoren gleich null ist. Hat N hingegen nur ein Element, so ist $\mathcal{P}(N) = \{\emptyset, N\}$, und in diesem Fall liegt dann ein Körper vor, den wir aufgrund seiner Wichtigkeit als eigenes Beispiel gleich anschließend nochmals betrachten wollen. ■

Beispiel 6.4.9 **Der binäre Körper**

Ausgehend von einer einelementigen Menge N betrachten wir nochmals den Ring $(\mathcal{P}(N), \Delta, \cap, \emptyset, N)$ aus dem letzten Beispiel. (Allgemeiner könnte man, ausgehend von einer beliebigen nichtleeren Menge N, anstatt $\mathcal{P}(N)$ auch das zweielementige Mengensystem $\{\emptyset, N\}$ betrachten.)

Schauen wir uns ebenfalls nochmals alternativ die Menge $\{\mathtt{w}, \mathtt{f}\}$ der beiden logischen Wahrheitswerte, versehen mit den Verknüpfungen xor (als Addition) und der Konjunktion $\wedge$ (als Multiplikation), siehe Abschnitt 1.4, an. Wir übersetzen nun Elemente samt Operationen gemäß folgender Tabelle

$\{\mathtt{w}, \mathtt{f}\}$	$\{\emptyset, N\}$	$\mathbb{F}_2$
$\wedge$	$\cap$	$\cdot$
xor	$\triangle$	$+$
$\mathtt{f}$	$\emptyset$	0
$\mathtt{w}$	N	1

und erhalten eine Struktur $(\mathbb{F}_2, +, \cdot, 0, 1)$ mit Verknüpfungen

$$\begin{array}{c|cc} + & 0 & 1 \\ \hline 0 & 0 & 1 \\ 1 & 1 & 0 \end{array} \quad \text{und} \quad \begin{array}{c|cc} \cdot & 0 & 1 \\ \hline 0 & 0 & 0 \\ 1 & 0 & 1 \end{array}, \tag{6.4.1}$$

welche man die **binäre Addition** (bzw. die **Addition modulo 2**) und die **binäre Multiplikation** (bzw. die **Multiplikation modulo 2**) nennt. Diese Struktur ist sicher eine der grundlegendsten Objekte der Informatik. Es handelt sich dabei in der Tat um einen Körper, nämlich den sog. binären Körper bzw. den **Restklassenkörper modulo 2**, welcher uns im nächsten Kapitel 7 u. a. im Rahmen der Grundlagen der Codierungstheorie als Komponentenbereich von (binären) Codes begegnen wird.

Obwohl die Menge $\mathbb{F}_2$ als Grundmenge für einen Körper kleinstmöglich ist, erweist sich das Nachrechnen sämtlicher Axiome der Körpereigenschaft von $\mathbb{F}_2$ allein anhand der obigen Verknüpfungstafeln (6.4.1) als recht mühsam. Glücklicherweise wissen wir aber aufgrund der Herkunft bereits, dass es sich bei $(\mathbb{F}_2, +, \cdot, 0, 1)$ um einen kommutativen Ring handelt, weil dies allgemein bei $(\mathcal{P}(N), \Delta, \cap, \emptyset, N)$ der Fall ist. Ferner ist $\mathbb{F}_2^* = \{1\}$ und die 1 stets invertierbar, womit dann sämtliche Körperaxiome erfüllt sind. ■

In Verallgemeinerung zum binären Körper werden wir im folgenden Kapitel mit der Addition und der Multiplikation modulo $n \in \mathbb{N}$ (mit $n \geq 2$) weitere Ringe kennenlernen, die sog. Restklassenringe.

F Eine Übersicht verschiedener Kategorien von Ringen Zum Ausklang dieses Abschnittes folgt eine kleine Übersicht über die verschiedenen Kategorien von Ringen zusammen mit Beispielklassen, die im weiteren Verlauf des vorliegenden Textes noch vorkommen werden.

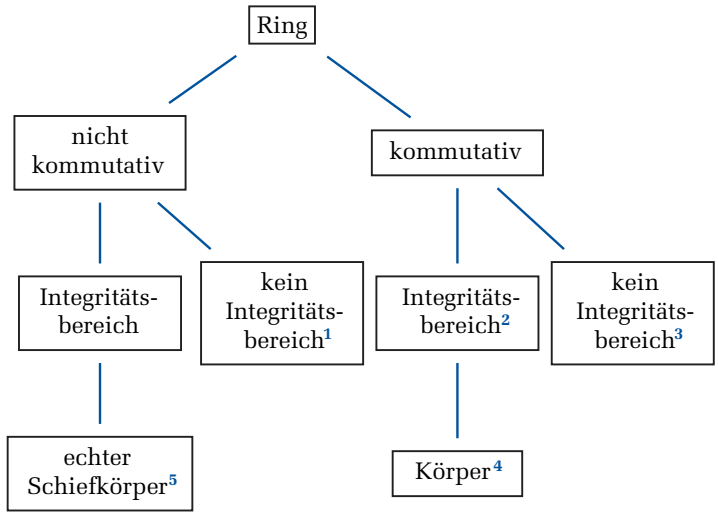
[1]: Matrixringe bzw. Matrixalgebren

[2]: ganze Zahlen,
Polynomringe,
formale Potenzreihenringe

[3]: Restklassenring modulo n, wobei n keine Primzahl,
Folgen über einem Körper mit punktweiser Addition/Multiplikation

[4]: rationale Zahlen,
reelle Zahlen,
komplexe Zahlen,
Restklassenring modulo p mit p Primzahl,
rationale Funktionen

[5]: der Quaternionenschiefkörper



6.5 Der Körper der komplexen Zahlen

In diesem Abschnitt wollen wir zeigen, wie man den Zahlbereich $\mathbb{R}$ der reellen Zahlen zum Zahlbereich $\mathbb{C}$ der komplexen Zahlen erweitern kann. Unter dem Gesichtspunkt dieses Kapitels ist dann $\mathbb{C}$ ein weiteres Beispiel für einen Körper. Im Rahmen der Analysis (Teil IV) werden wir weitere spezifische Eigenschaften von $\mathbb{C}$ kennenlernen und damit unser Wissen über die komplexen Zahlen vertiefen.

A Grundmenge, Verknüpfungen und Nachweis der Körpereigenschaft Wir beginnen mit der Menge $C := \mathbb{R} \times \mathbb{R}$ aller Paare reeller Zahlen. Darauf werden wie folgt zwei Verknüpfungen, eine Addition und eine Multiplikation eingeführt:

$$\textbf{Addition}: \quad (a, b) + (c, d) := (a + c, b + d) \tag{6.5.1}$$

$$\textbf{Multiplikation}: \quad (a, b)(c, d) := (ac - bd, ad + bc) \tag{6.5.2}$$

Bei der Addition handelt es sich um die bereits bekannte komponentenweise Addition. Die Multiplikation sieht auf den ersten Blick etwas merkwürdig aus, wir werden dies aber später rückwirkend motivieren können. Momentan mag der folgende Satz als Existenzberechtigung dieser Multiplikation genügen, wonach es sich bei C zusammen mit diesen beiden Operationen um einen Körper handelt. Man beachte auch, dass die punktweise Multiplikation zwar näherliegt, aber hier nicht zu einem Integritätsbereich und damit auch nicht zu einem Körper führen kann, wie wir anhand von ▶Beispiel 6.4.7 wissen.

Satz 6.5.1 Bezüglich der beiden eben eingeführten Verknüpfungen bildet C einen Körper. Man nennt C den **Körper der komplexen Zahlen**.

Beweis Zum Beweis dieses Satzes sind die drei Bedingungen aus Definition 6.4.1 nachzuweisen.

(1) Wir beginnen mit der additiven Struktur. Wegen $C = \mathbb{R}^2$ handelt es sich bei der Addition (wie gesagt) um die komponentenweise (bzw. punktweise) Addition. Da der Komponentenbereich $(\mathbb{R}, +, 0)$ eine kommutative Gruppe ist, ist auch C bzgl. $+$ eine kommutative Gruppe. Das Nullelement ist $(0, 0)$; das additive Inverse zu (a, b) ist $-(a, b) := (-a, -b)$.

(2) Für die multiplikative Struktur ist nachzuweisen, dass es sich bei $C^* = C \setminus \{(0, 0)\}$ um eine kommutative Gruppe bzgl. der Multiplikation handelt. Im Einzelnen bedeutet das den Nachweis

- des Assoziativgesetzes der Multiplikation,
- des Kommutativgesetzes der Multiplikation,
- der Existenz eines neutralen Elementes bzgl. der Multiplikation,
- der multiplikativen Invertierbarkeit eines jeden Elementes aus C^*.

Beim Nachweis des Assoziativgesetzes der Multiplikation berechnet man zunächst

$$\begin{aligned}((a, b)(c, d))(e, f) &= (ac - bd, ad + bc)(e, f)\\ &= ((ac - bd)e - (ad + bc)f, (ac - bd)f + (ad + bc)e)\\ &= (ace - bde - adf - bcf, acf - bdf + ade + bce)\end{aligned}$$

unter Verwendung der üblichen Rechengesetze reeller Zahlen. Entsprechend gilt aber auch

$$\begin{aligned}(a, b)((c, d)(e, f)) &= (a, b)(ce - df, cf + de)\\ &= (a(ce - df) - b(cf + de), a(cf + de) + b(ce - df))\\ &= (ace - adf - bcf - bde, acf + ade + bce - bdf).\end{aligned}$$

Eine kleine Änderung der Reihenfolge zeigt, dass die beiden Endpaare gleich sind, womit die Gültigkeit des Assoziativgesetzes gezeigt ist. Entsprechend gilt das Kommutativgesetz:

$$(a, b)(c, d) = (ac - bd, ad + bc) = (ca - db, cb + da) = (c, d)(a, b)$$

Wir machen uns als Nächstes auf die Suche nach einem Einselement (u, v). Ein solches Element muss für alle $(a, b) \in C$ die Gleichung $(a, b) = (a, b)(u, v)$ erfüllen (aufgrund der bereits nachgewiesenen Kommutativität ergibt sich dann $(u, v)(a, b) = (a, b)$ für alle

$a, b \in \mathbb{R}$ automatisch). Ausmultiplizieren liefert $(a, b)(u, v) = (au - bv, av + bu)$, was somit zur Bedingung

$$au - bv = a \text{ und } av + bu = b \text{ für alle } a, b \in \mathbb{R}$$

führt. Wählen wir nun speziell $(a, b) = (0, 1)$, so liefert die erste Gleichung $-v = 0$, also $v = 0$, während die zweite Gleichung $u = 1$ ergibt. Demnach ist $(1, 0)$ der einzige Kandidat für eine Eins in C. In der Tat ist

$$(a, b)(1, 0) = (a \cdot 1 - b \cdot 0, a \cdot 0 + b \cdot 1) = (a - 0, 0 + b) = (a, b) \quad \text{für alle } (a, b) \in C,$$

sodass $(C, \cdot, (1, 0))$ insgesamt ein kommutatives Monoid ist.

Als Nächstes zeigen wir, dass jedes $(a, b) \neq (0, 0)$ multiplikativ invertierbar ist. Wir nehmen dazu an, dass (a, b) eine Einheit in C ist, und versuchen über die Beziehung $(a, b)(x, y) = (1, 0)$ einerseits Bedingungen für (a, b) und andererseits Formeln für (x, y) in Abhängigkeit von (a, b) zu finden. (Wegen der Kommutativität der Multiplikation gilt dann automatisch auch $(x, y)(a, b) = (1, 0)$.) Ausmultiplizieren liefert zunächst $(a, b)(x, y) = (ax - by, ay + bx)$, sodass ein komponentenweiser Vergleich mit $(1, 0)$ zu den beiden Gleichungen

$$ax - by = 1 \text{ und } ay + bx = 0$$

führt. An dieser Stelle ist eine Fallunterscheidung sinnvoll.

- Ist $b = 0$, so ist $a \neq 0$ wegen $(a, b) \neq (0, 0)$. Mit $b = 0$ folgt aus der ersten Gleichung dann $ax = 1$, also $x = \frac{1}{a}$. Aus der zweiten Gleichung folgt $ay = 0$ und somit $y = 0$, da ja $a \neq 0$ ist.

- Wir nehmen nun an, dass $b \neq 0$ ist. Dann liefert das Auflösen der zweiten Gleichung $ay + bx = 0$ nach x, dass $x = -\frac{ay}{b}$ ist. Setzt man dies in die erste Gleichung $ax - by = 1$ ein, so ergibt sich $-\frac{a^2y}{b} - by = 1$. Löst man dies wiederum nach y auf, so erhält man:

  $$y = \left(-\frac{a^2}{b} - b\right)^{-1} = \left(-\frac{a^2}{b} - \frac{b^2}{b}\right)^{-1} = (-1)^{-1} \cdot \left(\frac{a^2 + b^2}{b}\right)^{-1} = -\frac{b}{a^2 + b^2}$$

  Dabei erinnere man sich an den aus der Schule bekannten Sachverhalt, wonach u^2 für jede von 0 verschiedene reelle Zahl echt größer als 0 ist, weshalb $a^2 + b^2 \neq 0$ für $(a, b) \neq (0, 0)$ folgt. Setzt man dies wiederum in die erste nach x aufgelöste Gleichung ein, so ergibt sich $x = \frac{a}{a^2+b^2}$. Damit sind die Zahlen x und y ganz in den Eingangszahlen a und b ausgedrückt.

  Es ist zu erwähnen, dass die beiden eben berechneten Terme auch für $b = 0$ sinnvoll sind, denn dann erhält man $x = \frac{1}{a}$ und $y = 0$ wie im ersten Fall. Rein vom Ergebnis her wäre also keine Fallunterscheidung notwendig gewesen; allein der Rechenweg hat diese benötigt.

Zusammenfassend erhalten wir also: Ist $(a, b) \neq (0, 0)$, so ist (a, b) multiplikativ invertierbar und es gilt

$$(a, b)^{-1} = \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right), \tag{6.5.3}$$

was man im Nachhinein nochmals direkt durch

$$(a, b) \left(\frac{a}{a^2 + b^2}, -\frac{b}{a^2 + b^2} \right) = \left(\frac{a^2 + b^2}{a^2 + b^2}, \frac{-ab + ba}{a^2 + b^2} \right) = (1, 0)$$

verifizieren kann. Damit ist dann insgesamt erkannt, dass $(C^*, \cdot, (1, 0))$ eine kommutative Gruppe ist.

(3) Schließlich rechnet man das Distributivgesetz nach (aufgrund der Kommutativität der Multiplikation genügt es, ein Distributivgesetz zu zeigen). Dazu seien (a, b) und (c, d) sowie (e, f) drei beliebige Paare aus C. Dann gilt (unter Verwendung des Distributivgesetzes in $\mathbb{R}$):

$$\begin{aligned}
(a, b)((c, d) + (e, f)) &= (a, b)(c + e, d + f) \\
&= (a(c + e) - b(d + f), a(d + f) + b(c + e)) \\
&= (ac + ae - bd - bf, ad + af + bc + be) \\
&= ((ac - bd) + (ae - bf), (ad + bc) + (af + be)) \\
&= (ac - bd, ad + bc) + (ae - bf, af + be) \\
&= (a, b)(c, d) + (a, b)(e, f)
\end{aligned}$$

Damit ist alles bewiesen. ■

B Die reellen Zahlen als Teilkörper der komplexen Zahlen Wir haben eingangs bemerkt, dass es sich bei C um eine Erweiterung der reellen Zahlen handelt, was wir nun genauer begründen wollen. Dazu betrachten wir die Abbildung

$$\Psi\colon \mathbb{R} \to C,\ a \mapsto (a, 0). \tag{6.5.4}$$

Diese ist injektiv und darüber hinaus sowohl mit der Addition als auch mit der Multiplikation auf $\mathbb{R}$ vertauschbar, es gilt nämlich $\Psi(a+b) = (a+b, 0) = (a, 0)+(b, 0) = \Psi(a)+\Psi(b)$ sowie $\Psi(ab) = (ab, 0) = (a, 0)(b, 0) = \Psi(a)\Psi(b)$ für alle $a, b \in \mathbb{R}$. Damit überträgt sich bijektiv die Körperstruktur von $\mathbb{R}$ auf die Teilmenge $R := \{(a, 0)\colon a \in \mathbb{R}\}$ von C (welche gleich dem Bild von Ψ ist), weshalb man $\mathbb{R}$ mit R einfach **identifizieren** kann[7]. In diesem Sinne ist dann $\mathbb{R}$ ein **Teilkörper** von C.[8]

C Imaginäre Einheit, Real- und Imaginärteil Ein wesentlicher Unterschied zwischen den reellen Zahlen $\mathbb{R}$ und den komplexen Zahlen C besteht darin, dass man in C (im

[7] Siehe auch Kapitel 8 zum Thema „Homomorphismen".

[8] Unter einem Teilkörper F eines Körpers K versteht man allgemein eine nichtleere Teilmenge F von K, welche unter der Addition und der Multiplikation abgeschlossen ist und diesbezüglich einen eigenständigen Körper bildet.