Mathematik für Informatiker
Teil 1

Dirk Hachenberger
Institut für Mathematik der Universität Augsburg
Wintersemester 2020/21

Kapitel III

ALGEBRAISCHE GRUNDSTRUKTUREN

Die Materialien der ursprünglichen ersten beiden Kapitel, nämlich **I. Grundlagen über Zahlen** und **II. Abbildungen und Mengen** sind im Rahmen des *Vorkurses Mathematik für Informatiker* verarbeitet worden. Um weniger Arbeit mit der Umnummerierung zu haben, starten wir hier mit Kapitel III.

Grundlage für dieses Skript ist unser Lehrbuch

Dirk Hachenberger,
Mathematik für Informatiker,
Pearson Studium, München, 2008 (2. Aufl.),
ISBN 978-3-8273-7320-5.

Siehe die dortigen Abschnitte 6.1, 6.2 und 6.4.

Date: 1. Oktober 2020.

Zusammenfassung

1. **Grundlagen über Monoide**
2. **Über die Invertierbarkeit in Monoiden zu Gruppen**
3. **Ergänzung: Monoidstrukturen bei Abbildungen**
4. **Grundlagen über Ring**e
5. **Über die Invertierbarkeit in Ringen zu Schiefkörpern und Körpe**rn
6. **Ergänzung: Potenzgesetze bei natürlichen und ganzzahligen Exponenten**
7. **Quadratische Gleichungen**

1. Grundlagen über Monoide

Wir starten mit einer nicht-leeren Menge M. Eine **Verknüpfung** (auch **binäre Operation**) auf M ordnet jedem Paar (a, b) mit $a, b \in M$ in *eindeutiger* Weise ein Element aus M zu. Als abstraktes Verknüpfungssymbol verwenden wir $*$ und schreiben die Verknüpfung von a mit b entsprechend als

$$a * b.$$

In konkreten Situationen (etwa bei bestimmten Zahlbereichen) verwendet man sowohl das *Additionssymbol* $+$ als auch das *Multiplikationssymbol* $\cdot$ (Letzteres wird üblicherweise ganz weggelassen). Man unterscheidet in diesem Zusammenhang in *additive* und *multiplikative* Schreibweise.

Bemerkung 1.1. Die grundlegende Eigenschaft einer binären Operation $*$, die oben im Wort „eindeutig“ versteckt ist, bedeutet, dass $*$ eine Abbildung von $M \times M$ nach M ist.

Definition 1.2. Eine Verknüpfung $*$ auf einer Menge M heißt **assoziativ**, falls das **Assoziativgesetz** erfüllt ist:

(AG) $a * (b * c) = (a * b) * c$ für alle $a, b, c \in M$.

Definition 1.3. Es sei M eine Menge mit einer assoziativen Verknüpfung $*$. Dann nennt man das Paar $(M, *)$ ein **Monoid**, wenn Folgendes gilt:

(NE) Es gibt ein Element $e \in M$ mit $e * a = a = a * e$ für jedes $a \in M$.

Ein Element $e \in M$, welches (NE) erfüllt, nennt man ein **neutrales Element**.

Satz 1.4. *Ist $(M, *)$ ein Monoid, so hat M genau ein neutrales Element.*

Beweis. Annahme, e ist ein neutrales Element von $(M, *)$. Weiterhin sei $e' \in M$ ein Element mit der Eigenschaft $y * e' = y$ für jedes $y \in M$. Speziell mit $y = e$ ergibt sich dann $e * e' = e$. Andererseits ist aber $e * x = x$ für jedes $x \in M$, und die spezielle Wahl $x = e'$ liefert $e * e' = e'$. Insgesamt erhalten wir somit $e = e * e' = e'$, also $e' = e$. □

Zur Kennzeichnung des neutralen Elementes e eines Monoids, werden wir ab jetzt häufig die Tripelschreibweise verwenden:

$$(M, *, e).$$

In der additiven Schreibweise verwendet man für das neutrale Element eines Monoids die Bezeichnung 0; das **Nullelement**. Bei der multiplikativen Schreibweise verwendet man hingegen die Bezeichnung 1 und nennt es das **Einselement**.

Definition 1.5. Eine Verknüpfung $*$ auf einer Menge M heißt **kommutativ**, falls das **Kommutativgesetz** erfüllt ist:

(KG) $a * b = b * a$ für alle $a, b \in M$.

Ist $(M, *, e)$ ein Monoid und ist $*$ kommutativ, so spricht man von einem **kommutativen Monoid**.

Die folgenden Beispiele belegen, dass (kommutative) Monoide in zahlreichen Variationen auftreten.

Beispiel 1.6. (Zahlbereiche) Bei jedem der folgenden Tripel handelt es sich um ein kommutatives Monoid.

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

Beispiel 1.7. (Verknüpfungen bei Mengensystemen) Es sei S eine Menge, in diesem Kontext die sog. *Grundmenge*. Davon ausgehend betrachten wir die Potenzmenge von S, also $\mathcal{P}(S)$. Als konkretes Beispiel denke man etwa an eine dreielementige Menge $S = \{u, v, w\}$ (also $u \neq v$ und $u \neq w$ und $v \neq w$). Dann ist

$$\mathcal{P}(S) = \{\emptyset, \{u\}, \{v\}, \{w\}, \{u, v\}, \{u, w\}, \{v, w\}, \{u, v, w\}\}.$$

Nun zu den Verknüpfungen auf $\mathcal{P}(S)$:

(1) Die **Schnittbildung** $\cap$ ist eine assoziative und kommutative Verknüpfung auf $\mathcal{P}(S)$ (siehe Lehrbuch, Definition 1.17.1, Satz 1.17.4). Weiter gilt $X \cap S = X$ für alle $X \subseteq S$, weshalb die Menge S hier als neutrales Element fungiert. Also ist $(\mathcal{P}(S), \cap, S)$ ein kommutatives Monoid.

(2) Ebenso ist auch die **Mengenvereinigung** $\cup$ eine assoziative und kommutative Verknüpfung auf $\mathcal{P}(S)$ (siehe Lehrbuch, Definition 1.17.1, Satz 1.17.4). Hierbei ist $X \cup \emptyset = X$ für alle $X \subseteq S$, weshalb die **leere Menge** $\emptyset$ das neutrale Element bzgl. der Vereinigung ist. Also ist auch $(\mathcal{P}(S), \cup, \emptyset)$ ein kommutatives Monoid.

(3) Die **symmetrische Differenz** zweier Mengen $X, Y \subseteq S$ ist durch

$$X \triangle Y := (X \cup Y) \setminus (X \cap Y)$$

bzw. äquivalent durch

$$X \triangle Y := (X \setminus Y) \cup (Y \setminus X)$$

erklärt (siehe Lehrbuch, Definition 1.17.1). Diese Verknüpfung ist offensichtlich kommutativ. Zum Nachweis der (nicht offensichtlichen) Assoziativität von $\triangle$ bedienen wir uns einer **Wahrheitstafel**. Ausgehend von drei beliebigen Teilmengen X, Y und Z von S codieren wir die insgesamt acht Möglichkeiten für Elemente a aus S hinsichtlich ihrer Zugehörigkeit zu X, Y bzw. Z durch **binäre Tripel**: Beispielsweise bedeutet $(1, 0, 1)$, dass $a \in X$ und $a \notin Y$ und $a \in Z$ gilt. Daraus folgt dann $a \in X \Delta Y$ (gekennzeichnet durch 1) und $a \in Y \Delta Z$ (gekennzeichnet durch 1) sowie $a \notin (X \Delta Y) \Delta Z$ und $a \notin X \Delta (Y \Delta Z)$, jeweils gekennzeichnet durch 0.

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

Die Gleichheit der beiden Spalten ganz rechts belegt, dass (in allen möglichen Szenarien) ein Element genau dann in $X \Delta (Y \Delta Z)$ enthalten ist, wenn es in $(X \Delta Y) \Delta Z$ enthalten ist, womit die Assoziativität nachgewiesen ist. Wegen

$$X \Delta \emptyset = (X \cup \emptyset) \setminus (X \cap \emptyset) = X \setminus \emptyset = X$$

für jedes $X \subseteq S$ ist $\emptyset$ neutrales Element bzgl. Δ und somit ist $(\mathcal{P}(S), \Delta, \emptyset)$ insgesamt ein kommutatives Monoid.

2. Über die Invertierbarkeit in Monoiden zu Gruppen

Wir bleiben thematisch bei den Monoiden und kommen als Nächstes zu einem überaus wichtigen Aspekt, nämlich der *Invertierbarkeit* gewisser Elemente innerhalb eines Monoids.

Definition 2.1. Ist $(M, *, e)$ ein Monoid und ist $u \in M$, so nennt man u **invertierbar** falls gilt:

Es gibt ein $v \in M$ mit $u * v = e = v * u$.

Satz 2.2. *Es seien $(M, *, e)$ ein Monoid und $u, v, w \in M$. Annahme, es gilt $v * u = e$ und $u * w = e$. Dann folgt $v = w$.*

Beweis. Annahme, e ist ein neutrales Element von $(M, *)$. Wegen der Neutralität von e gilt $v = v * e$. Aufgrund der Annahme $e = u * w$ ergibt sich daraus $v = v * (u * w)$. Eine Anwendung des Assoziativgesetzes liefert sodann $v = (v * u) * w$. Wegen der Annahme $v * u = e$ ergibt sich also $v = e * w$. Schließlich liefert die Neutralität von e die Gleichheit von v und w. □

Bemerkung 2.3. Es sei $(M, *, e)$ ein Monoid. Außerdem sei $u \in M$ ein invertierbares Element. Dann gibt es nach Definition 2.1 ein $v \in M$ mit $u * v = v * u = e$.

(1) Satz 2.2 impliziert, dass dieses v eindeutig bestimmt ist. Man nennt v <u>das</u> **Inverse** zu u.
(2) Je nach Bezeichnung der Verknüpfung verwendet man für das Inverse v von u eine besondere Notation:
   - additiv: $-u$;
   - multiplikativ: u^{-1} bzw. $\frac{1}{u}$.

   Wenn wir abstrakte Monoide betrachten, wollen wir $\overline{u}$ für das Inverse von u schreiben.
(3) Ist v das Inverse zu u, so ist auch v invertierbar, und das zu v gehörende Inverse ist u. Das bedeutet, dass zweifaches Invertieren von u wieder zu u führt, also
$$\overline{(\overline{u})} = u.$$
In der additiven Schreibweise liest sich das als $-(-u) = u$ und in der multiplikativen Schreibweise ergibt sich $(u^{-1})^{-1} = u$ bzw., wenn man Brüche verwendet, $\frac{1}{\frac{1}{u}} = u$. □

Bemerkung 2.4. Das neutrale Element eines Monoids ist stets invertierbar! Es ist wegen $e * e = e$ nämlich zu sich selbst invers.

- abstrakt: $\overline{e} = e$,
- additiv: $-0 = 0$,
- multiplikativ: $1^{-1} = 1$ bzw. $\frac{1}{1} = 1$. □

Wir kommen nun zu einer speziellen Klasse von Monoiden, den sog. *Gruppen*.

Definition 2.5. Es sei $(G, *, e)$ ein Monoid. Dann heißt G eine **Gruppe**, wenn gilt:

(IE) *Jedes* Element von G ist invertierbar.

Ist $*$ zudem kommutativ, so nennt man G eine **kommutative** bzw. eine **abelsche**[a] **Gruppe**.

[a] Niels Henrik Abel (1802-1829)

Beispiel 2.6. (Zahlbereiche)

(1) Im Monoid $(\mathbb{N}, +, 0)$ ist lediglich die Null (additiv) invertierbar, daher handelt es sich nicht um eine Gruppe.
(2) Allerdings sind $(\mathbb{Z}, +, 0)$ und $(\mathbb{Q}, +, 0)$, ebenso $(\mathbb{R}, +, 0)$ (abelsche) Gruppen.
(3) Im Monoid $(\mathbb{N}, \cdot, 1)$ ist lediglich die Eins (multiplikativ) invertierbar. Also ist $(\mathbb{N}, \cdot, 1)$ keine Gruppe.
(4) Im Monoid $(\mathbb{Z}, \cdot, 1)$ ist neben der Eins nur noch -1 (multiplikativ) invertierbar. Also ist $(\mathbb{Z}, \cdot, 1)$ keine Gruppe.
(5) Die Menge der (multiplikativ) invertierbaren Elemente des Monoids $(\mathbb{Q}, \cdot, 1)$ ist $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$. Das heißt, jedes von 0 verschiedene Element ist hier invertierbar. Wegen der Ausnahmesituation bei 0 ist $(\mathbb{Q}, \cdot, 1)$ entsprechend keine Gruppe. Allerdings ist $(\mathbb{Q}^*, \cdot, 1)$ eine (kommutative) Gruppe — auf diesen Sachverhalt kommen wir in Satz 2.9 zurück.
(6) Entsprechend ist $(\mathbb{R}, \cdot, 1)$ keine Gruppe, während $(\mathbb{R}^*, \cdot, 1)$ eine kommutative Gruppe bildet, wobei $\mathbb{R}^* := \mathbb{R} \setminus \{0\}$. □

Beispiel 2.7. (Mengensysteme) Wir betrachten nochmals die Potenzmenge $\mathcal{P}(S)$ einer Menge S.

(1) Das neutrale Element bzgl. der Schnittmengenbildung $\cap$ ist S. Wegen $X \cap Y \subseteq X$ für alle $X, Y \subseteq S$ ist $X \cap Y = S$ nur für $X = S = Y$ erfüllbar, so dass im Monoid $(\mathcal{P}(S), \cap, S)$ lediglich das neutrale Element invertierbar ist.
(2) Das neutrale Element bzgl. der Vereinigungsbildung $\cup$ ist $\emptyset$. Wegen $X \subseteq X \cup Y$ für alle $X, Y \subseteq S$ ist $X \cup Y = \emptyset$ nur für $X = \emptyset = Y$ erfüllbar, weshalb im kommutativen Monoid $(\mathcal{P}(S), \cup, \emptyset)$ ebenfalls lediglich das neutrale Element invertierbar ist.
(3) Betrachten wir abschließend $\mathcal{P}(S)$ zusammen mit der symmetrischen Differenz Δ. Das neutrale Element dieses Monoids ist die leere Menge. Wegen

$$X \Delta X = (X \cup X) \setminus (X \cap X) = X \setminus X = \emptyset$$

ist jedes $X \subseteq S$ bzgl. der symmetrischen Differenz zu sich selbst invers, insbesondere überhaupt invertierbar. Bei $(\mathcal{P}(S), \Delta, \emptyset)$ handelt es sich deshalb stets um eine abelsche Gruppe. □

Die wesentliche Konsequenz des Axioms (IE) ist, dass in Gruppen, im Gegensatz zu allgemeinen Monoiden, uneingeschränkt die sog. *Kürzungsregel* gilt. Genauer:

Satz 2.8. *Es sei $(G, *, e)$ eine Gruppe. Sind $a, b, c \in G$ und gilt $a*b = a*c$ oder $b*a = c*a$, so folgt $b = c$.*

Beweis. Annahme, $a * b = a * c$. Verknüpft man beide Seiten von linke mit dem zu a gehörenden inversen Element, so erhält man

$$\overline{a} * (a * b) = \overline{a} * (a * c).$$

Wegen (AG) und (NE) ergibt sich links $\overline{a} * (a * b) = (\overline{a} * a) * b = e * b = b$ und rechts entsprechend $\overline{a} * (a * c) = (\overline{a} * a) * c = e * c = c$, also $b = c$.

Die andere Aussage folgt analog durch Verknüpfung von rechts mit $\overline{a}$. □

Wir beenden diesen Abschnitt mit einem weiteren Resultat über abstrakte Monoide.

Satz 2.9. *Zu einem Monoid $(M, *, e)$ bezeichne $E(M)$ die Menge aller seiner invertierbaren Elemente. Dann gelten:*

(1) *Sind $a, b \in E(M)$, so ist auch $a * b \in E(M)$.* [a]

(2) *$(E(M), *, e)$ ist eine Gruppe.*

[a] Also induziert $*$ auch eine Verknüpfung auf $E(M)$; man sagt deshalb auch, dass $E(M)$ bezüglich $*$ **abgeschlossen** ist.

Beweis.

(1) Es sei $x := a * b$ und $\overline{a}$ bzw. $\overline{b}$ seien die zu a bzw. b gehörenden Inversen. Ferner sei $y := \overline{b} * \overline{a}$. Dann gilt aufgrund des Assoziativgesetzes einerseits

$$\begin{aligned} x * y &= (a * b) * y \\ &= a * (b * y) \\ &= a * (b * (\overline{b} * \overline{a})) \\ &= a * ((b * \overline{b}) * \overline{a}) \\ &= a * (e * \overline{a}) \\ &= a * \overline{a} \\ &= e. \end{aligned}$$

Völlig analog ergibt sich $y * x = e$, und damit ist die Invertierbarkeit von $x = a * b$ nachgewiesen, genauer: $\overline{a * b} := \overline{b} * \overline{a}$.[1]

(2) Die Assoziativität braucht man für $(E(M), *)$ nicht extra nachzuweisen, wir müssen uns nur Folgendes klar machen: Da (AG) in $(M, *)$ erfüllt ist und $E(M)$ unter $*$ abgeschlossen ist, **vererbt** sich (AG) auf $E(M)$, denn es gilt ja $a * (b * c) = (a * b) * c$ für *alle* $a, b, c \in M$ und damit erst recht für alle a, b, c aus $E(M)$.
Entsprechend ist klar, dass das neutrale Element e von M, welches ja in $E(M)$ enthalten ist, als neutrales Element von $E(M)$ fungiert. Das alles rechtfertig insbesondere die Schreibweise $(E(M), *, e)$, und wir wissen an dieser Stelle, dass es sich bei $(E(M), *, e)$ um ein Monoid handelt. Gemäß Definition von $E(M)$ ist nun aber *jedes* Element aus $E(M)$ invertierbar und mit $u \in E(M)$ ist auch dessen Inverses $\overline{u}$ in $E(M)$ enthalten. Also bildet $E(M)$ insgesamt eine Gruppe bzgl. $*$.

□

[1] Man achte hier unbedingt auf die umgekehrte Reihenfolge bei der Invertierung.

3. Ergänzung: Monoidstrukturen bei Abbildungen

Wir beginnen mit folgender Überlegung: Es seien M, N und K, sowie L jeweils nicht-leere Mengen. Weiter seien $f : M \to N$ und $g : N \to K$, sowie $h : K \to L$ Abbildungen. Dann gilt

$$h \circ (g \circ f) = (h \circ g) \circ f.$$

Die Verkettung von Abbildungen erfüllt somit das Assoziativgesetz. Um dies einzusehen, ist zuerst zu beachten, dass $h \circ (g \circ f)$ und $(h \circ g) \circ f$ beides Abbildungen von M nach L sind. Ist nun $x \in M$ beliebig, so folgt

$$h \circ (g \circ f)(x) = h(g \circ f(x)) = h(g(f(x))) = h \circ g(f(x)) = (h \circ g) \circ f(x),$$

womit bereits alles gezeigt ist.

Unsere nächste Aufmerksamkeit gilt einer sehr einfachen und dennoch wichtigen Art von Abbildung.

Definition 3.1. Es sei M eine nicht-leere Menge. Die Abbildung

$$\mathrm{id}_M : M \to M, \quad x \mapsto x$$

heißt die **identische Abbildung** auf M.

Satz 3.2. *Zu einer nicht-leeren Menge M sei $\mathrm{Abb}(M)$ die Menge aller Abbildungen von M nach M. Dann ist $(\mathrm{Abb}(M), \circ, \mathrm{id}_M)$ ein Monoid. Dieses ist nicht kommutativ, wenn M wenigstens zwei verschiedene Elemente enthält.*

Beweis. Da es sich bei Definitions- und Wertebereich um die gleiche Menge M handelt, ist $\circ$ eine Verknüpfung auf $\mathrm{Abb}(M)$. Die Assoziativität von $\circ$ folgt aus der einleitenden Bemerkung dieses Abschnitts. Wegen

$$\mathrm{id}_M \circ f(x) = \mathrm{id}_M(f(x)) = f(x) = f(\mathrm{id}_M(x)) = f \circ \mathrm{id}_M(x)$$

für alle $f \in \mathrm{Abb}(M)$ und alle $x \in M$ ist id_M das neutrale Element. Damit ist die Monoid-Eigenschaft nachgewiesen.

Sind nun $u, v \in M$ mit $u \neq v$, so sind $f : M \to M, x \mapsto u$ und $g : M \to M, x \mapsto v$ zwei nicht vertauschbare Abbildungen, denn $f \circ g(u) = f(v) = u$ und $g \circ f(u) = g(u) = v$. □

Bemerkung 3.3. Wir betrachten nochmals das Monoid $(\mathrm{Abb}(M), \circ, \mathrm{id}_M)$, wobei M irgendeine nicht-leere Menge ist. Es sei

$$\mathrm{Sym}(M) := \{f \in \mathrm{Abb}(M) : \ f \text{ ist bijektiv}\}.$$

(1) Dann gilt $f \in \mathrm{Sym}(M)$ genau dann, wenn f innerhalb des Monoids $(\mathrm{Abb}(M), \circ, \mathrm{id}_M)$ *invertierbar* ist. In diesem Falle ist die Umkehrabbildung zu f auch das zu f gehörende Inverse, und das rechtfertigt die Schreibweise f^{-1} für die Umkehrabbildung zu f. Insbesondere gilt

$$f \circ f^{-1} = \mathrm{id}_M = f^{-1} \circ f.$$

(2) Nach Satz 2.9 handelt es sich bei $(\mathrm{Sym}(M), \circ, \mathrm{id}_M)$ um eine Gruppe. Man nennt sie die **symmetrische Gruppe** auf M bzw. auch die **Gruppe aller Permutationen** von M. □

Ist M eine Menge, die wenigstens drei verschiedene Elemente hat, so ist die symmetrische Gruppe von M nicht kommutativ. Den Nachweis überlassen wir als Übungsaufgabe.

4. Grundlagen über Ringe

Wir betrachten in diesem Abschnitt eine nicht-leere Menge R, auf der *zwei* Verknüpfungen definiert sind, eine **Addition** und eine **Multiplikation**. Wichtige Beispiele sind $\mathbb{N}$ bzw. $\mathbb{Z}$ bzw. $\mathbb{Q}$, sowie $\mathbb{R}$ mit den gewöhnlichen Operationen $+$ und $\cdot$. Um nicht von vornherein unbewiesene Dinge hineinzuinterpretieren, schreiben wir zu Beginn die (noch abstrakten) Verknüpfungen als $\oplus$ (Addition) und $\odot$ (Multiplikation). Darüber hinaus sind in R zwei Elemente ausgezeichnet, die **Null** N und die **Eins** E. Später werden wir dafür die üblichen Bezeichnungen 0 bzw. 1 verwenden.

Definition 4.1. Man nennt $(R, \oplus, \odot, N, E)$ einen **Ring**, falls die folgenden Eigenschaften erfüllt sind.

(1) $(R, \oplus, N)$ ist eine kommutative Gruppe.
(2) $(R, \odot, E)$ ist ein Monoid.
(3) Die **Distributivgesetze**:
   (DG_1) $a \odot (b \oplus c) = a \odot b \oplus a \odot c$ für alle $a, b, c \in R$, sowie
   (DG_2) $(a \oplus b) \odot c = a \odot c \oplus b \odot c$ für alle $a, b, c \in R$.

Bemerkung 4.2.

(1) Als kommutative Gruppe erfüllt die additive Struktur $(R, \oplus, N)$ des Ringes R die Axiome (AG), (KG), (NE) und (IE). Für das zu $a \in R$ gehörende **additive Inverse** schreiben wir (vorübergehend) $\ominus a$. Für die Addition $u \oplus (\ominus v)$ schreibt man kurz $u \ominus v$. Die **Subtraktion** $u \ominus v$ ist also nichts anderes als die Addition von u mit dem Inversen von v.
(2) Als Monoid erfüllt die multiplikative Struktur $(R, \odot, E)$ eines Ringes R zunächst lediglich die Axiome (AG) und (NE).
   - Die Multiplikation ist also nicht notwendigerweise kommutativ, was anhand vieler Beispiele im Laufe der Vorlesung belegt werden kann. Gilt innerhalb eines (dann besonderen) Ringes das Kommutativgesetz (KG) bzgl. der Multiplikation, so spricht man von einem **kommutativen Ring**.
   - Ein Element von R kann, muss aber nicht multiplikativ invertierbar sein. Mehr dazu im folgenden Abschnitt 5. □

Beispiel 4.3. (Zahlbereiche)

(1) $(\mathbb{N}, +, \cdot, 0, 1)$ ist kein Ring.
(2) Bei $(\mathbb{Z}, +, \cdot, 0, 1)$ und $(\mathbb{Q}, +, \cdot, 0, 1)$ handelt es sich jeweils um kommutative Ringe. Ebenso ist $(\mathbb{R}, +, \cdot, 0, 1)$ ein kommutativer Ring. □

Beispiel 4.4. (Mengensysteme) Es sei S eine Menge und $\mathcal{P}(S)$ deren Potenzmenge. Dann ist

$$(\mathcal{P}(S), \triangle, \cap, \emptyset, S)$$

ein kommutativer Ring. Der Nachweis des Distributivgesetzes kann man ähnlich zum Assoziativgesetz bzgl. Δ mit einer Wahrheitstafel führen (siehe Lehrbuch, Beispiel 6.17.8). □

Es folgen einige Eigenschaften, die in jedem Ring gelten.

Satz 4.5. *Ist $(R, \oplus, \odot, N, E)$ ein Ring, so gilt $a \odot N = N = N \odot a$ für jedes $a \in R$.*

Beweis. Da N das neutrale Element bzgl. der Addition ist, gilt $N \oplus N = N$ und daher ist $N \odot a = (N \oplus N) \odot a$ für jedes $a \in R$. Das Distributivgesetz liefert $N \odot a = N \odot a \oplus N \odot a$. Nun addiert man auf beiden Seiten $\ominus(N \odot a)$, das additive Inverse von $N \odot a$, und man erhält $N = N \odot a$. Ganz analog zeigt man $a \odot N = N$. □

Satz 4.6. *Ist $(R, \oplus, \odot, N, E)$ ein Ring, so gilt, jeweils für alle $a, b \in R$:*
(1) $a \odot (\ominus b) = (\ominus a) \odot b = \ominus(a \odot b)$,
(2) $(\ominus a) \odot (\ominus b) = a \odot b$.

Beweis.
(1) Aufgrund des Distributivgesetzes und Satz 4.5 gilt
$$a \odot b \oplus a \odot (\ominus b) = a \odot (b \oplus (\ominus b)) = a \odot N = N.$$
Das bedeutet, dass $a \odot (\ominus b)$ additiv invers zu $a \odot b$ ist. Also ist $a \odot (\ominus b)$ gleich $\ominus(a \odot b)$. Der Nachweis der zweiten Gleichung erfolgt analog.
(2) Mit $x = \ominus a$ folgt aus (1), dass $x \odot (\ominus b) = (\ominus x) \odot b$ ist. Wegen $\ominus x = \ominus(\ominus a) = a$ ist dies gleich $a \odot b$.

□

Zur Motivation des nächsten Begriffs betrachten wir nochmals den (kommutativen) Ring
$$(\mathcal{P}(S), \triangle, \cap, \emptyset, S)$$
aus Beispiel 4.4, wobei wir annehmen, dass S *wenigstens zwei* verschiedene Elemente enthält. Nun seien $x, y \in S$ mit $x \neq y$. Dann ist das „Produkt“ $\{x\} \cap \{y\}$ gleich $\emptyset$, also gleich „Null“, obwohl $\{x\} \neq \emptyset$ und $\{y\} \neq \emptyset$ gilt.

Dieses Phänomen führt zu einer wichtigen Differenzierung innerhalb der Klasse aller Ringe.

Definition 4.7. Es sei $(R, \oplus, \odot, N, E)$ ein Ring (mit Null N). Dann nennt man R einen **Integritätsbereich**, falls gilt:
Sind $a, b \in R$ mit $a \odot b = N$, so folgt $a = N$ oder $b = N$.

Innerhalb eines Integritätsbereiches ist ein Produkt also genau dann gleich Null, wenn wenigstens ein Faktor gleich Null ist. Diese entscheidende Bedeutung eines Integritätsbereiches gegenüber allgemeinen Ringen macht sich in der folgenden **Kürzungsregel** bemerkbar.

Satz 4.8. *Es sei $(R, \oplus, \odot, N, E)$ ein Integritätsbereich. Annahme, $a, b, c \in R$ mit $a \neq N$ und mit $a \odot b = a \odot c$. Dann folgt $b = c$.*

Beweis. Die Gleichung $a \odot b = a \odot c$ ist gleichbedeutend mit $a \odot b \ominus a \odot c = N$ (Addition des additiven Inversen von $a \odot c$ auf beiden Seiten). Das Distributivgesetz liefert $a \odot (b \ominus c) = N$. Da R ein Integritätsbereich ist, folgt nun $a = N$ oder $b \ominus c = N$. Der Fall $a = N$ ist nach Voraussetzung ausgeschlossen. Also ergibt sich $b \ominus c = N$. Das ist aber gleichbedeutend mit $b = c$ (Addition von c auf beiden Seiten). □

5. Über die Invertierbarkeit in Ringen zu Schiefkörpern und Körpern

Ist $R = \{x\}$ eine Menge, die nur ein einziges Element x enthält, so sind trivialerweise durch $x \odot x = x$ und $x \oplus x = x$ zwei Verknüpfungen gegeben, welche alle Axiome aus Definition 4.1 erfüllen. Hierbei ist $x = N = E$. Ein solcher Ring ist natürlich nicht besonders interessant, weshalb wir ihn im Folgenden als **trivialen Ring** bezeichnen. Unter einem **nicht-trivialen Ring** versteht man entsprechend einen Ring, der wenigstens zwei verschiedene Elemente enthält.

Definition 5.1. Wir betrachten das multiplikative Monoid $(R, \odot, E)$ eines Ringes $(R, \oplus, \odot, N, E)$. In diesem Zusammenhang nennt man $u \in R$ eine **Einheit**, falls u *multiplikativ invertierbar* ist, falls also gilt:

Es gibt ein $v \in R$ mit $u \odot v = E = v \odot u$.

Die Menge $E(R)$ aller multiplikativ invertierbaren Elemente eines Ringes nennt man die **Einheitengruppe** von R.

Der Name **Einheitengruppe** ist gerechtfertigt, weil es sich nach Satz 2.8 bei $(E(R), \odot, E)$ um eine eigenständige Gruppe handelt. Sind $x, y \in E(R)$, so gilt

$$(x \odot y)^{-1} = y^{-1} \odot x^{-1} \quad bzw. \quad \frac{1}{x \odot y} = \frac{1}{y} \odot \frac{1}{x}.$$

Satz 5.2. *Es sei $(R, \oplus, \odot, N, E)$ ein nicht-trivialer Ring. Die Menge seiner von Null verschiedenen Elemente sei stets mit R^* bezeichnet.*[a] *Dann gilt:*

(1) $E \neq N$.
(2) $E(R) \subseteq R^*$.

[a] Es ist also $R^* = R \setminus \{N\}$.

Beweis.

(1) Nach Voraussetzung gibt es ein $a \in R$ mit $a \neq N$. Wäre $N = E$, so folgte $a = a \odot E = a \odot N = N$, ein Widerspruch. Also ist $N \neq E$.
(2) Ist speziell $a \in E(R)$, so ist einerseits $a^{-1} \odot a = E$ und andererseits $a^{-1} \odot N = N$ (nach Satz 4.5). Also kann nicht $a = N$ gelten. Das zeigt $N \notin E(R)$.[2]

□

Definition 5.3. Einen nicht-trivialen Ring, in dem *jedes* von Null verschiedene Element multiplikativ invertierbar ist, nennt man einen **Schiefkörper**. Einen kommutativen Schiefkörper nennt man einen **Körper**.

Körper spielen im weiteren Verlauf dieser Vorlesung eine wichtige Rolle! Als Bezeichnung für einen abstrakten Körper verwenden wir meist das Symbol $\mathbb{K}$. Einen Schiefkörper, der kein Körper ist, wollen wir einen **echten Schiefkörper** nennen. Dort gibt es demnach Elemente a, b mit $a \odot b \neq b \odot a$.

Beispiel 5.4. (Zahlbereiche)

(1) $(\mathbb{Z}, +, \cdot, 0, 1)$ ist **kein** Körper, aber $(\mathbb{Q}, +, \cdot, 0, 1)$ ist ein Körper.

[2] Das bedeutet im Endeffekt, dass man innerhalb eines nicht-trivialen Ringes nicht durch die Null dividieren kann bzw. darf!

(2) Ebenso ist $(\mathbb{R}, +, \cdot, 0, 1)$ ein Körper. □

Wir werden neben dem Körper $\mathbb{Q}$ der rationalen Zahlen und dem Körper $\mathbb{R}$ der reellen Zahlen noch weitere Beispiele für Körper kennenlernen, die allesamt sehr wichtig sind: Zum einen den Körper $\mathbb{C}$ der **komplexen Zahlen**, und zum anderen die **Restklassenkörper** $\mathbb{Z}_p$ (dabei ist p eine Primzahl). Außerdem werden wir später auch einen echten Schiefkörper vorstellen, nämlich den Schiefkörper $\mathbb{H}$ der **Quaternionen**.

Satz 5.5. *Jeder Schiefkörper ist ein Integritätsbereich.*

Beweis. Annahme, $(R, \oplus, \odot, N, E)$ ist ein Schiefkörper. Es seien $a, b \in R$ mit $a \odot b = N$. Falls $a = N$, so ist nichts zu zeigen. Falls $a \neq N$, so hat a ein zugehöriges multiplikatives Inverses a^{-1}. Wir multiplizieren die Gleichung $a \odot b = N$ von links mit a^{-1} und erhalten

$$a^{-1} \odot (a \odot b) = a^{-1} \odot N.$$

Nach Satz 4.5 ergibt sich auf der rechten Seite N. Mit dem Assoziativgesetz erhält man links $(a^{-1} \odot a) \odot b = E \odot b = b$. Insgesamt zeigt dies $b = N$. □

Wir beenden diesen Abschnitt mit zwei wichtigen Beispielen von Körpern.

Beispiel 5.6. (Binärer Körper) Ausgangspunkt ist eine Menge S mit *nur einem* Element, sagen wir x. Dann ist $\mathcal{P}(S) = \{\emptyset, \{x\}\} = \{\emptyset, S\}$. Als Verknüpfungstafeln für die Operationen des Ringes $(\mathcal{P}(S), \triangle, \cap, \emptyset, S)$ ergeben sich

$\triangle$	$\emptyset$	S
$\emptyset$	$\emptyset$	S
S	S	$\emptyset$

und

$\cap$	$\emptyset$	S
$\emptyset$	$\emptyset$	$\emptyset$
S	$\emptyset$	S

.

Übersetzt man das wie folgt:

Mengelehre:	S	$\emptyset$	$\triangle$	$\cap$
Aussagenlogik:	wahr	falsch	XOR	$\wedge$
vereinfachte Symbole:	1	0	$+$	$\cdot$

,

so ergibt sich (u.a.)

$+$	0	1
0	0	1
1	1	0

und

$\cdot$	0	1
0	0	0
1	0	1

.

Es sind alle Anforderungen an einen Körper erfüllt. Man nennt dieses Verknüpfungsgebilde den **binären Körper** (da er genau zwei Elemente enthält). Als Bezeichnung für den binären Körper verwendet man $\mathbb{Z}_2$ oder auch $\mathbb{F}_2$. □

Beispiel 5.7. (Ternärer Körper) Wir wollen untersuchen, ob es einen Körper mit **drei** Elementen gibt. Neben der Null (0) und der Eins (1) sei a das dritte, verbleibende Element.

Wäre $a + 1 = 1$, so folgte $a = 0$; wäre $a + 1 = a$, so folgte $1 = 0$. Beides sind Widersprüche, und deshalb muss $a + 1 = 0$ gelten, also ist a das additive Inverse zu 1, das heißt: $a = -1$.[3] Die Multiplikationstafel ergibt sich nun zwangsweise aus den bereits hergeleiteten allgemeinen Gesetzen:

$\cdot$	0	1	-1
0	0	0	0
1	0	1	-1
-1	0	-1	1

[3] Im Gegensatz zum binären Körper ist die 1 also nicht zu sich selbst additiv invers, es gilt also nicht $1 + 1 = 0$.

Die Additionstafel sieht (notwendigerweise) wie folgt aus:

$+$	0	1	-1
0	0	1	-1
1	1	-1	0
-1	-1	0	1

.

Es gilt nämlich $1+1=-1$, da $1+1=0$ und $1+1=1$ wegen $1\neq -1$ und $1\neq 0$ auszuschließen sind. Sodann erhält man $(-1)+(-1)=(-1)\cdot(1+1)=(-1)\cdot(-1)=1$.

Damit sind wir aber noch nicht am Ende. Wir haben bisher lediglich Folgendes gezeigt: *Wenn* es einen Körper mit drei Elementen gibt, so sehen die Additions- und die Multiplikationstafel *notwendigerweise* so aus, wie dargestellt. Der Körper wäre also eindeutig festgelegt. Wovon wir uns nun noch überzeugen müssten, ist, dass diese Rechenregeln im Einklang mit den Assoiativgesetzen und dem Distributivgesetz stehen, also

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

für jede Wahl von x,y,z aus $\{0,1,-1\}$. Nun gibt es 27 mögliche Belegungen für (x,y,z), und die drei Regeln können mit viel Fleiss für jede dieser Konstellationen nachgeprüft werden. Wir verzichten auf die Vorführung dieser 81 Berechnungen und verkünden lediglich, dass die Assoiativgesetze und das Distributivgesetz tatsächlich gültig sind, so dass mit den obigen Verknüpfungstafeln ein Körper vorliegt. Man nennt ihn den **ternären Körper**. □

An dieser Stelle wird deutlich, dass man zum Auffinden weiterer Beispiele von Körpern geschicktere Methoden verwenden muss, um nicht in uferlose Fallunterscheidungen und Rechnungen zu verfallen. Wie könnte zum Beispiel ein Körper mit 101 Elementen aussehen? Kann es einen Körper mit 100 Elementen geben? Wieviele verschiedene (unterschiedliche Verknüpfungstafeln) von Körpern mit 125 Elementen gibt es?

Wir werden in Abschnitt 8 einen eleganten Zugang zu gewissen kommutativen Ringen und Körpern kennenlernen, von denen der binäre und der ternäre Körper lediglich Spezialfälle sind, und bei dem der Nachweis des Assoziativgesetzes und des Distributivgesetzes obsolet sind.

6. Ergänzung: Potenzgesetze bei natürlichen und ganzzahligen Exponenten

In diesem Abschnitt geht es um weitere wichtige Aspekte in allgemeinen Ringen. Im Folgenden sei daher $(R, +, \cdot, 0_R, 1_R)$ ein Ring. Zur Einstimmung auf die Potenzgesetze definieren zunächst eine sog. *äußere Multiplikation* von natürlichen Zahlen mit Elementen aus R. Zur Unterscheidung von der natürlichen Null (0) und von der natürlichen Eins (1) verwenden wir daher vorübergehend die Bezeichnungen 0_R bzw. 1_R für die Null bzw. die Eins in R. Für die Verknüpfungen verwenden wir allerdings die gleichen Symbole wie bei $\mathbb{N}$, weil aus dem Zusammenhang hervorgeht, welche Objekte miteinander verknüpft werden.

Es sei also a irgendein Element von R.

- Wir definieren $0 \cdot a := 0_R$.
- Ist $m \in \mathbb{N}$ und $m \cdot a \in R$ definiert, so sei

$$(m+1) \cdot a := m \cdot a + a.$$

Aufgrund des Induktionsprinzips ist dann für jedes $n \in \mathbb{N}$ ein Ringelement $n \cdot a \in R$ definiert, das **n-Fache** von a.

Speziell bemerkenswert sind in diesem Zusammenhang folgende Sachverhalte.

(1) Es gilt $1 \cdot a = a$ für jedes $a \in R$, denn: $1 \cdot a = (0+1) \cdot a = 0 \cdot a + a = 0_R + a = a$.
(2) Ausserdem gilt $n \cdot 0_R = 0_R$ für jedes $n \in \mathbb{N}$. (Nachweis mit Induktion: Es ist $0 \cdot 0_R = 0_R$; ist $m \cdot 0_R = 0_R$ für ein $m \in \mathbb{N}$, so ist $(m+1) \cdot 0_R = m \cdot 0_R + 1 \cdot 0_R = 0_R + 0_R = 0_R$.)

Wir verwenden die gleichen Bezeichnungen wie oben und definieren nun *natürliche Potenzen* von Ringelementen.

Definition 6.1. (Potenzen von Ringelementen) Es seien $(R, +, \cdot, 0_R, 1_R)$ ein Ring und a ein Element von R.

- Wir definieren $a^0 := 1_R$.
- Ist $m \in \mathbb{N}$ und $a^m \in R$ definiert, so sei

$$a^{m+1} := a^m \cdot a.$$

Aufgrund des Induktionsprinzips ist dann für jedes $n \in \mathbb{N}$ ein Ringelement $a^n \in R$ definiert, die **n-te Potenz** von a.

Bemerkung 6.2. Speziell bemerkenswert sind in diesem Zusammenhang folgende Sachverhalte.

(1) Es gilt $a^1 = a$ für jedes a aus R, denn $a^1 = a^{0+1} = a^0 \cdot a = 1_R \cdot a = a$.
(2) Ausserdem gilt $1_R^n = 1_R$ für alle $n \in \mathbb{N}$. (Nachweis mit Induktion: Es ist $1_R^0 = 1_R$, und aus $1_R^m = 1_R$ folgt $1_R^{m+1} = 1_R^m \cdot 1_R = 1_R \cdot 1_R = 1_R$.) □

Satz 6.3. *Es seien $(R, +, \cdot, 0_R, 1_R)$ ein Ring und $a \in R$. Für alle $n, m \in \mathbb{N}$ gilt dann:*

(1) $(n+m) \cdot a = n \cdot a + m \cdot a$.
(2) $a^{n+m} = a^n \cdot a^m$.

Beweis. Da es sich bei (1) um das additive Analogon von (2) handelt, führen wir lediglich den Beweis zu (2). Konkret führen wir einen Induktionsbeweis über die Variable m. Es sei

$$L := \{\ell \in \mathbb{N} : a^{n+\ell} = a^n \cdot a^\ell \ \underline{\text{für jedes}}\ n \in \mathbb{N}\}.$$

- Induktionsanfang: Ist $m = 0$, so ist $a^{n+0} = a^n = a^n \cdot 1_R = a^n \cdot a^0$, und zwar für jedes $n \in \mathbb{N}$. Also gilt $0 \in L$.
- Induktionsschritt: Es sei m ein Element von L, es gelte also $a^{n+m} = a^n \cdot a^m$ für jedes $n \in \mathbb{N}$. Dann folgt

  $$a^{n+(m+1)} = a^{(n+1)+m} = a^{n+1} \cdot a^m = (a^n \cdot a) \cdot a^m = a^n \cdot (a \cdot a^m).$$

  Dabei wurde beim zweiten Gleichheitszeichen $m \in L$ verwendet. Nutzt man dies nochmals aus, so erhält man

  $$a \cdot a^m = a^1 \cdot a^m = a^{1+m} = a^{m+1}.$$

  Insgesamt folgt daher $a^{n+(m+1)} = a^n \cdot a^{m+1}$, und dies gilt für jedes $n \in \mathbb{N}$. Damit ist $m + 1 \in L$ gezeigt. Aufgrund des Prinzips der vollständigen Induktion erhalten wir insgesamt $L = \mathbb{N}$.

□

Satz 6.4. *Es seien $(R, +, \cdot, 0_R, 1_R)$ ein Ring und $a, b \in R$, sowie $m, n \in \mathbb{N}$. Dann gilt:*

(1) $n \cdot (a + b) = n \cdot a + n \cdot b$.
(2) *Unter der Annahme $ab = ba$ folgt $(ab)^n = a^n \cdot b^n$.*
(3) $(a^m)^n = a^{m \cdot n}$.

Beweis. Der Beweis sei als Übung gestellt. □

Bemerkung 6.5. Betrachte nochmals einen Ring $(R, +, \cdot, 0_R, 1_R)$. Annahme $a \in R$ ist multiplikativ invertierbar. Dann ist auch jede Potenz a^n von a (mit $n \in \mathbb{N}$) invertierbar und es gilt $(a^n)^{-1} = (a^{-1})^n$. Dafür schreibt man vereinfachend a^{-n}. Daran sieht man, dass es sinnvoll ist, auch negative Exponenten zu betrachten. Sodann bleiben die Gesetze aus Satz 6.3 (2) und Satz 6.4 (3) gültig, wenn m, n sogar beliebige ganze Zahlen sind.

Ist schließlich (neben a) auch $b \in R$ multiplikativ invertierbar, und gilt $ab = ba$, so bleibt das Gesetz in Satz 6.4 (2) gültig wenn n sogar eine beliebige ganze Zahl ist. □

7. Quadratische Gleichungen

Wir betrachten in diesem Abschnitt zunächst einen allgemeinen Körper $(\mathbb{K}, +, \cdot, 0, 1)$. Zu jedem fest vorgegebenen Tripel $a, b, c \in \mathbb{K}$ mit $a \neq 0$ ist die **quadratische Gleichung**

$$„ax^2 + bx + c = 0“ \text{ in der Variablen } x$$

assoziiert. Wir fragen nach der Lösung dieser Gleichung durch Elemente aus $\mathbb{K}$. Gesucht ist also die Menge

$$\mathbb{L}_{a,b,c} := \{z \in \mathbb{K} : az^2 + bz + c = 0\}.$$

Bemerkung 7.1. Betrachten wir zunächst den Spezialfall $(a, b, c) = (1, 0, -u)$ für ein $u \in \mathbb{K}$. Die Gleichung „$ax^2 + bx + c = 0$“ ist dann gleichbedeutend mit „$x^2 = u$“. Bezeichnet man mit

$$Q(\mathbb{K}) := \{z^2 : z \in \mathbb{K}\}$$

die Menge aller **Quadrate** in $\mathbb{K}$, so ergibt sich unmittelbar, dass „$x^2 = u$“ genau dann in $\mathbb{K}$ lösbar ist, wenn $u \in Q(\mathbb{K})$ gilt, wenn also u ein Quadrat ist.

Wieviele Lösungen kann es dann insgesamt geben, wenn u ein Quadrat ist?

(1) Ist $u = 0$, so gibt es genau ein $z \in \mathbb{K}$ mit $z^2 = 0$, nämlich $z = 0$.
(2) Annahme $u \neq 0$ und $z \in \mathbb{K}$ ist eine gegebene Lösung. Für jedes $w \in \mathbb{K}$ gilt nun

$$w^2 - u = w^2 - z^2 = (w - z)(w + z).$$

Also ist $w^2 = u$ genau dann, wenn $(w - z)(w + z) = 0$. Da $\mathbb{K}$ als Körper ein Integritätsbereich ist (siehe Satz 5.5), folgt dementsprechend $w = z$ oder $w = -z$. Deshalb gibt es *höchstens* zwei verschiedene Lösungen.

- Dabei kann die Situation $w = z = -z$ trotz $z \neq 0$ mitunter auftreten! Das erfordert allerdings $0 = z + z = (1 + 1) \cdot z$, also $1 + 1 = 0$, was beispielsweise beim binären Körper der Fall ist.
- Ist hingegen $1 + 1 \neq 0$ in $\mathbb{K}$, so hat die Gleichung „$x^2 = u$“ mit $u \neq 0$ im Falle der Lösbarkeit *genau zwei* Lösungen, und diese beiden Lösungen sind dann additiv invers zueinander. □

Definition 7.2. Es sei $(\mathbb{K}, +, \cdot, 0, 1)$ ein Körper mit $1 + 1 \neq 0$. Die zur Gleichung „$ax^2 + bx + c = 0$“ gehörende **Diskriminante** ist die Zahl

$$\Delta := b^2 - 4ac$$

aus $\mathbb{K}$.

In Abhängigkeit der „Lage“ ihrer Diskriminante Δ innerhalb $\mathbb{K}$ kann die Lösbarkeit der zugehörigen quadratischen Gleichung wie folgt vollständig beschrieben werden.

Satz 7.3. *Annahme,* $(\mathbb{K}, +, \cdot, 0, 1)$ *ist ein Körper, in dem* $1 + 1 \neq 0$ *gilt. Es sei* Δ *die Diskriminante der quadratischen Gleichung „*$ax^2 + bx + c = 0$*“, wobei* $a \neq 0$*. Dann gilt:*

(1) *Ist* Δ *kein Quadrat in* $\mathbb{K}$*, so hat die Gleichung* ***keine*** *Lösung in* $\mathbb{K}$*.*

(2) *Ist* $\Delta = 0$*, so hat die Gleichung* ***genau eine*** *Lösung in* $\mathbb{K}$*, nämlich*

$$z = -\frac{b}{2a}.$$

(3) *Ist* Δ *ein von* 0 *verschiedenes Quadrat in* $\mathbb{K}$*, so hat die Gleichung* ***genau zwei*** *verschiedene Lösungen in* $\mathbb{K}$*, nämlich*

$$z_1 = \frac{-b + \Gamma}{2a} \quad \textit{und} \quad z_2 = \frac{-b - \Gamma}{2a}.$$

Dabei ist $\Gamma \in \mathbb{K}$ *irgend eines der beiden Elemente aus* $\mathbb{K}$ *mit* $\Gamma^2 = \Delta$*.*

Bemerkung. Wir weisen zunächst darauf hin, dass die „2“ natürlich für $1 + 1$ steht. Die Situation von Körpern $\mathbb{K}$ mit $1 + 1 = 0$ nimmt daher auch deshalb eine Sonderrolle ein, weil dort eine Division durch 2 nicht erlaubt ist (siehe die Formeln für die Lösungen in der Aussage des Satzes).

Beweis. Starten wir also mit „$ax^2 + bx + c = 0$“. Nach Division durch a erhält man die äquivalente Gleichung „$x^2 + \frac{b}{a}x + \frac{c}{a} = 0$“. Einsetzen eines beliebigen Elementes z aus $\mathbb{K}$ in die linke Seite ergibt $z^2 + \frac{b}{a}z + \frac{c}{a}$. Eine Anwendung der ersten binomischen Formel (innerhalb $\mathbb{K}$)[4] zeigt

$$\left(z + \frac{b}{2a}\right)^2 = z^2 + \frac{b}{a}z + \frac{b^2}{4a^2},$$

und deshalb ist

$$z^2 + \frac{b}{a}z + \frac{c}{a} = \left(z + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}.$$

(Dabei steht „4“ für 2^2, also für $2 \cdot 2$.) Diesen Schritt nennt man *quadratische Ergänzung.* Addition der beiden rechts stehenden Summanden ergibt

$$-\frac{b^2}{4a^2} + \frac{c}{a} = -\frac{b^2 - 4ac}{4a^2}.$$

Wir stellen insgesamt fest: Genau dann ist $z \in \mathbb{K}$ eine Lösung von „$ax^2 + bx + c = 0$“, wenn

$$\left(z + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

gilt. Letzteres kann durch Multiplikation mit $4a^2$ nochmals umgeformt werden zu

$$(*) \qquad \left[2a \cdot \left(z + \frac{b}{2a}\right)\right]^2 = b^2 - 4ac = \Delta.$$

Man sieht nun, warum die Diskriminante für die Lösbarkeit die entscheidende Rolle spielt, und dass der allgemeine Fall der Lösung einer quadratischen Gleichung auf den in Bemerkung 7.1 untersuchten Spezialfall zurückgeführt ist.

Die Lösbarkeit innerhalb $\mathbb{K}$ impliziert also, dass die Diskriminante ein Quadrat in $\mathbb{K}$ ist. Damit ist die erste Behauptung, also (1) bewiesen.

Wir nehmen ab jetzt an, dass Δ ein Quadrat in $\mathbb{K}$ ist. Hierbei gibt es nun (wieder) zwei Fälle zu unterscheiden.

(i) Falls $\Delta = 0$, so ist $(*)$ äquivalent zu $2a \cdot \left(z + \frac{b}{2a}\right) = 0$. Wegen $2a \neq 0$ ergibt sich $z + \frac{b}{2a} = 0$, also eindeutig $z = -\frac{b}{2a}$, womit (2) bewiesen ist.

[4] Für u, v aus $\mathbb{K}$ gilt: $(u + v)^2 = (u + v)(u + v) = u(u + v) + v(u + v) = u^2 + uv + vu + v^2$, und dies ist gleich $u^2 + uv + uv + v^2 = u^2 + (1 + 1)uv + v^2 = u^2 + 2uv + v^2$.

(ii) Falls $\Delta \neq 0$, so gibt es ein $\Gamma \in \mathbb{K}$ mit $\Gamma \neq 0$ und mit $\Gamma^2 = \Delta$. Wir setzen

$$z_1 := \frac{-b+\Gamma}{2a} \quad \text{und} \quad z_2 := \frac{-b-\Gamma}{2a}.$$

Dann sind z_1 und z_2 zwei verschiedene Elemente aus $\mathbb{K}$, weil sonst $\Gamma = -\Gamma$, also $0 = \Gamma + \Gamma = (1+1)\cdot\Gamma$, was wegen $\Gamma \neq 0$ und $1+1 \neq 0$ nicht sein kann.

Wegen Bemerkung 7.1 ist der Beweis von (3) abgeschlossen. Wir wollen aber nochmals detailliert argumentieren, dass es, analog zum Spezialfall aus Bemerkung 7.1, keine weiteren Lösungen mehr geben kann. Ist nämlich w irgendein Element von $\mathbb{K}$, so gilt

$$a\cdot(w-z_1)\cdot(w-z_2) = aw^2 - a(z_1+z_2)w + az_1z_2.$$

Wegen

$$-a(z_1+z_2) = -a\cdot\frac{-b+\Gamma-b-\Gamma}{2a} = b$$

und wegen

$$az_1z_2 = \frac{(-b)^2-\Gamma^2}{4a} = \frac{b^2-\Delta}{4a} = \frac{b^2-b^2+4ac}{4a} = c$$

erhält man dann

$$a\cdot(w-z_1)\cdot(w-z_2) = aw^2+bw+c.$$

Letzteres gilt, wie gesagt für jedes $w \in \mathbb{K}$. Daher ist $w \in \mathbb{K}$ genau dann eine Lösung von „$ax^2+bx+c=0$“, wenn $a\cdot(w-z_1)\cdot(w-z_2)=0$ ist. Da ein Körper ein Integritätsbereich ist (siehe nochmals Satz 5.5), und da $a \neq 0$ vorausgesetzt ist, kann dies nur sein, wenn $w-z_1=0$ oder $w-z_2=0$ gilt, was gleichbedeutend mit $w=z_1$ oder $w=z_2$ ist. Also hat die Gleichung in diesem Fall genau die beiden angegebenen (verschiedenen) Lösungen z_1 und z_2.

□

Es stellt sich nun generell die Frage, wie die Menge der Quadrate innerhalb eines Körpers $\mathbb{K}$ aussieht. Diese Frage ist im allgemeinen sehr schwierig und kann hier nicht erschöpfend beantwortet werden. Betrachten wir stattdessen einige konkrete Situationen.

Beispiel 7.4.

(1) Wir wollen die Gleichung „$x^2-3x+\frac{7}{4}=0$“ über $\mathbb{Q}$ und über $\mathbb{R}$ lösen. Deren Diskriminante ist

$$\Delta = (-3)^2 - 4\cdot 1\cdot\tfrac{7}{4} = 2.$$

Da 2 kein Element von $Q(\mathbb{Q})$ ist, hat diese Gleichung keine Lösung in $\mathbb{Q}$. Über $\mathbb{R}$ hingegen hat sie die beiden Lösungen

$$\frac{3+\sqrt{2}}{2} \quad \text{und} \quad \frac{3-\sqrt{2}}{2}.$$

(2) Im ternären Körper ist 1 das einzige von 0 verschiedene Element, das ein Quadrat ist. Die Gleichung „$x^2+x-1=0$“, deren Diskriminante gleich

$$1^2 - 4\cdot 1\cdot(-1) = 1+4 = 1+1+1+1+1 = 1+1 = -1$$

ist, hat daher keine Lösung im ternären Körper. Natürlich kann man das (hier) auch direkt durch Ausprobieren aller Möglichkeiten zeigen: $1^2+1-1=1$ und $0^2+0-1=-1$ und $(-1)^2+(-1)-1 = 1-1-1 = -1$. □

Wir kommen abschließend zur Betrachtung der rationalen und der reellen Zahlen. Bei $\mathbb{Q}$ und $\mathbb{R}$ handelt es sich um sog. **angeordnete Körper**, ein Phänomen, welches wir im kommenden Semester im Rahmen der Analysis genauer erörtern müssen. An dieser Stelle sei betont, dass das Quadrat einer jeden reellen Zahl *nicht-negativ* ist (kurz: $r^2 \geq 0$ für jedes $r \in \mathbb{R}$).

(1) Innerhalb $\mathbb{Q}$ wissen wir anhand der Zahl 2, dass nicht jede positive Zahl ein Quadrat ist. In der Tat gibt es *unendlich viele* positive rationale Zahlen die kein Quadrat in $\mathbb{Q}$ sind, wie man sich als Übung klar mache. Es gilt

$$Q(\mathbb{Q}) = \left\{ \frac{m^2}{n^2} : m, n \in \mathbb{N}^*,\ \mathrm{ggT}(m,n) = 1 \right\} \cup \{0\}\,.$$

(2) Die Vervollständigung von $\mathbb{Q}$ zu den reellen Zahlen $\mathbb{R}$ (dem Kontinuum) liefert hingegen die folgende befriedigende Situation: Die Gleichung „$x^2 = r$“ ist *für jede positive reelle Zahl* r lösbar. Das bedeutet

$$Q(\mathbb{R}) = \mathbb{R}_0^+.$$

Die *eindeutige positive reelle Zahl* s mit $s^2 = r$ heißt die **Quadratwurzel** von r und wird mit

$$\sqrt{r}$$

bezeichnet.

Wir wollen Satz 7.3 nun abschließend nochmals auf der Grundlage der reellen Zahlen formulieren. Das Folgende sollte unter dem Stichwort „Mitternachtsformel“ selbstverständlich bekannt sein.

Satz 7.5. *Wir betrachten die quadratische Gleichung „$ax^2 + bx + c = 0$“ über dem Körper $\mathbb{R}$ der reellen Zahlen, wobei $a \neq 0$. Es sei $\Delta = b^2 - 4ac$ die Diskriminante dieser Gleichung. Dann gilt:*

(1) *Ist $\Delta < 0$, so hat die Gleichung **keine** Lösung in $\mathbb{R}$.*
(2) *Ist $\Delta = 0$, so hat die Gleichung **genau eine** Lösung in $\mathbb{R}$, nämlich*

$$z = -\frac{b}{2a}.$$

(3) *Ist $\Delta > 0$, so hat die Gleichung **genau zwei** verschiedene Lösungen in $\mathbb{R}$, nämlich*

$$z_1 = \frac{-b + \sqrt{\Delta}}{2a} \quad \textit{und} \quad z_2 = \frac{-b - \sqrt{\Delta}}{2a}.$$

□

Institut für Mathematik, Universität Augsburg, D-86135 Augsburg
Email address: hachenberger@math.uni-augsburg.de