2. Axiomatische Charakterisierung der reellen Zahlen

2.1 Die Körperaxiome

Def.: M sei eine Menge. Eine Abbildung

$\circ : M \times M \to M, \quad (m_1, m_2) \mapsto m_1 \circ m_2$

heißt eine innere Verknüpfung von M.

Bsp.: Die Addition $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \ (n,m) \mapsto n+m$ und die Multiplikation $\cdot : \mathbb{N} \times \mathbb{N} \to \mathbb{N}, \ (n,m) \mapsto n \cdot m$ sind innere Verknüpfungen von $\mathbb{N}$. Desgl. f. $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

Manche Mengen mit inneren Verknüpfungen sind durch eine besondere Struktur ausgezeichnet:

Def.: Ein Paar $(G, \circ)$ aus einer Menge $G \neq \emptyset$ und einer inneren Verknüpfung $\circ$ von G heißt eine Gruppe, falls gilt

(G1) $(a \circ b) \circ c = a \circ (b \circ c)$ für alle $a, b, c \in G$ (Assoziativität).

(G2) Es gibt $e \in G$ mit $e \circ a = a$ für alle $a \in G$ (neutrales El.).

(G3) Zu jedem $a \in G$ existiert ein $b \in G$ mit $b \circ a = e$ (inverses Element).

Eine Gruppe heißt kommutativ (oder abelsch), falls zusätzlich gilt

(G4) $a \circ b = b \circ a$ für alle $a, b \in G$.

Bem. zu Bsp.: (i) abkürzende Schreibweise: G statt $(G, \circ)$ und ab statt $a \circ b$ (wenn klar ist, welche innere Verknüpfung $\circ$ gemeint ist).

(ii) Für die Analysis I sind fast ausschließlich die abelschen Gruppen von Belang.

(iii) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ sind abelsche Gruppen; $(\mathbb{N}, +)$ nicht: hier fehlen das neutrale und folglich auch die inversen Elemente.

(iv) $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ [1] sind ebenfalls abelsche Gruppen. $(\mathbb{Z}^*, \cdot)$ hingegen nicht – wieder fehlen die Inversen.

<u>Lemma 1</u>: Es sei G eine abelsche Gruppe. Dann gelten:

1. Das neutrale Element e ist eindeutig bestimmt.
2. Zu $a \in G$ existiert genau ein $b \in G$ mit $ab = ba = e$. Dieses wird mit a^{-1} bezeichnet (Eindeutigkeit des Inversen).
3. Für alle $a, b \in G$ ist $(ab)^{-1} = b^{-1}a^{-1}$.
4. $(a^{-1})^{-1} = a$, $e^{-1} = e$
5. Für $a, x, y \in G$ gilt $ax = ay \Leftrightarrow x = y$
6. Zu $a, b \in G$ existiert genau ein $x \in G$, so daß $ax = b$. (Die Gleichung $ax = b$ ist also in einer abelschen Gruppe stets eindeutig lösbar.)

Bem.: Lemma gilt in vollem Umfang auch in nicht-abelschen Gruppen.

---

1) allgemein: $M^* = M \setminus \{0\}$, wenn M eine Menge ist, die eine Null enthält.

Bew.: Zu 1.: Seien e und e' neutrale Elemente.
Dann folgt $e = e'e = ee' = e'$.

Zu 2.: Hier ist nur die Eindeutigkeit zu zeigen. Dazu seien
$ba = e = b'a$. Dann ist
$b = eb = b'ab = b'ba = b'e = eb' = b'$.

Zu 3. Es gilt $(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}b = e$. Damit ist $b^{-1}a^{-1}$ invers zu ab. Nach 2 also $b^{-1}a^{-1} = (ab)^{-1}$.

Zu 4. Es ist $a \cdot a^{-1} = a^{-1}a = e$, also a invers zu a^{-1}.
$\underset{2.}{\Longrightarrow} (a^{-1})^{-1} = a$. Ebenso folgt aus $ee = e$, daß $e = e^{-1}$.

Zu 5. "$\Longleftarrow$" klar (einsetzen)
"$\Longrightarrow$" $ax = ay \Rightarrow a^{-1}(ax) = a^{-1}(ay) \Rightarrow (a^{-1}a)x = (a^{-1}a)y$
$\Rightarrow ex = ey \Rightarrow x = y$.

Zu 6. $ax = b \underset{5.}{\Longleftrightarrow} a^{-1}ax = a^{-1}b \Longleftrightarrow x = a^{-1}b$. $\square$

Def.: Ein Tripel $(K, +, \cdot)$ bestehend aus einer Menge K und zwei inneren Verknüpfungen heißt ein **Körper**, falls gilt

(K1) $x + (y + z) = (x + y) + z$ (Assoziativität) $\;\; \forall x, y, z \in K$
(K2) $x + y = y + x$ (Kommutativität)
(K3) Es gibt $0 \in K$ mit $x + 0 = x$ für alle $x \in K$ (Nullelement)
(K4) Zu $x \in K$ ex. $-x \in K$, so daß $x + (-x) = 0$ (negatives)
(K5) $x \cdot (y \cdot z) = (x \cdot y) \cdot z$ (Ass.) $\;\; \forall x, y, z \in K$
(K6) $x \cdot y = y \cdot x$ (Komm.)
(K7) Es gibt $1 \in K$ mit $1 \cdot x = x$ für alle $x \in K$ (Einselement)
(K8) Zu $x \in K^*$ ex. $x^{-1} \in K^*$, so daß $x^{-1}x = 1$ (inverses).
(K9) $x \cdot (y + z) = x \cdot y + x \cdot z$ $\forall x, y, z \in K$ (Distributivgesetz)

Bem.:

(i) Schreibweise: xy statt $x \cdot y$, $x-y$ statt $x+(-y)$,

falls $y \neq 0$: $\frac{x}{y}$ statt $y^{-1}x$

(ii) Die Axiome (K1) bis (K4) heißen Axiome der Addition. Sie sind gleichbedeutend damit, dass $(K,+)$ eine abelsche Gruppe ist.

(iii) (K5) bis (K8) sind die Axiome der Multiplikation. Sie enthalten die Aussage, dass $(K^*, \cdot)$ eine abelsche Gruppe ist.

Die einfachen Eigenschaften abelscher Gruppen (Lemma 1) haben daher in Körpern die folgenden Entsprechungen:

Folgerung 1. Sei $(K,+,\cdot)$ ein Körper. Dann gelten:

1. 0 und 1 sind eindeutig bestimmt.
2. Negatives $(-x)$ und Inverses (x^{-1}) sind eindeutig bestimmt.
3. $-(x+y) = -x-y$ und, falls $x,y \in K^*$, $(xy)^{-1} = y^{-1}x^{-1}$.
4. $-(-x) = x$, $-0 = 0$, $(x^{-1})^{-1} = x$, $1^{-1} = 1$.
5. $a+x = a+y \Leftrightarrow x=y$ und, falls $a \neq 0$, $ax = ay \Leftrightarrow x=y$
6. Die Gleichung $a+x=b$ und, falls $a \neq 0$, $ax=b$ sind eindeutig lösbar.

Zieht man zusätzlich das Distributivgesetz heran, erhält man weitere einfache Folgerungen aus den Körperaxiomen:

<u>Lemma 2:</u> Sei $(K, +, \cdot)$ ein Körper und $x, y, z \in K$.

Dann gelten:

1. $(x+y)z = xz + yz$,
2. $x \cdot 0 = 0$,
3. $xy = 0 \iff x = 0$ oder $y = 0$ (Nullteilerfreiheit),
4. $(-x)y = -xy$, insbes. $-y = (-1)y$,
5. $(-x)(-y) = xy$.

<u>Bew.:</u> zu 1.: $(x+y)z \underset{(K6)}{=} z(x+y) \underset{(K9)}{=} zx + zy \underset{(K6)}{=} xz + yz$

zu 2.: Aus $0 = 0 + 0$ folgt mit dem Distributivges. (K9)

$x \cdot 0 = x(0+0) \underset{(K9)}{=} x \cdot 0 + x \cdot 0$. Teil 5. der vorangegangenen Folgerung 1 ergibt $0 = x \cdot 0$.

zu 3.: Sei $xy = 0$ und $x \neq 0 \underset{\substack{\text{Folg. 1,} \\ \text{Teil 5}}}{\Longrightarrow} y = x^{-1} \cdot 0 \underset{2.}{=} 0$.

Das zeigt "$\Rightarrow$". "$\Leftarrow$" folgt aus 2.

zu 4.: $0 \underset{2.}{=} 0 \cdot y \underset{(K3,4)}{=} (x + (-x))y \underset{(K9)}{=} xy + (-x)y$.

Mit der Eindeutigkeit des Negativen folgt $(-x)y = -xy$.

zu 5.: $(-x)(-y) \underset{4}{=} -x(-1)y \underset{(K6)}{=} -(-1)(xy) \underset{4}{=} -(-xy) = xy$

Folgerung 1,4.

$\square$

Bsp.: (i) $(\mathbb{Z},+,\cdot)$ ist kein Körper, hier fehlen die inversen Elemente der Multiplikation. Nimmt man solche hinzu, entsteht der Körper $(\mathbb{Q},+,\cdot)$ der rationalen Zahlen.

(ii) Die reellen Zahlen fassen wir auf als einen Körper $(\mathbb{R},+,\cdot)$, in dem noch weitere Axiome gelten (s.u.) und in den $\mathbb{Q}$ und damit auch $\mathbb{Z}$ und $\mathbb{N}$ eingebettet sind.

(iii) Endliche Körper gibt es auch, ein Bsp. werden wir in den Übungen oder im Tutorium diskutieren. → Algebra!

(iv) Ein für die Analysis sehr wichtiger Körper ist der Körper $\mathbb{C} = (\mathbb{C},+,\cdot)$ der komplexen Zahlen, der folgendermaßen definiert wird:

Def.: Für $(x,y) \in \mathbb{R}\times\mathbb{R} =: \mathbb{R}^2$ und $(u,v) \in \mathbb{R}^2$ definieren wir

$$(x,y) + (u,v) := (x+y,\ u+v) \qquad \text{(Addition)}$$

und

$$(x,y)\,(u,v) := (xu - yv,\ xv + yu) \qquad \text{(Multiplikation)}$$

(Auf der rechten Seite sind $+$ und $\cdot$ die Addition bzw. Multiplikation in den reellen Zahlen!)

Durch diese Definitionen wird auf der Ebene $\mathbb{R}^2$ tatsächlich eine Körperstruktur gegeben. Genauer gilt:

Satz 1: $(\mathbb{R}^2, +, \cdot)$ ist ein Körper mit Nullelement $0 := (0,0)$ und Einselement $1 := (1,0)$. Das Negative von $z = (x,y)$ ist $-z := (-x,-y)$. Für $z = (x,y) \neq 0$ ist das Inverse

$$z^{-1} := \frac{1}{z} := \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2} \right).$$

Bez.: Der auf diese Weise definierte Körper wird mit $(\mathbb{C}, +, \cdot)$ oder kurz mit $\mathbb{C}$ bezeichnet, seine Elemente heißen <u>komplexe Zahlen</u>.

Bew.: Die geforderten Axiome werden auf die entsprechenden Eigenschaften der reellen Zahlen zurückgeführt. Diskussion (zum Teil) in den Üb.

Bem. zur Einbettung von $(\mathbb{R}, +, \cdot)$ in $(\mathbb{C}, +, \cdot)$:

$(\{(x,0) : x \in \mathbb{R}\}, +, \cdot)$ ist ein Teilkörper von $(\mathbb{C}, +, \cdot)$, denn

$$(x,0) + (u,0) = (x+u, 0); \quad (x,0)(u,0) = (xu, 0),$$

d.h. er ist abgeschlossen unter $+$ und $\cdot$. Durch

$$I : \mathbb{R} \to \{(x,0) : x \in \mathbb{R}\}, \quad x \mapsto I(x) := (x,0)$$

wird $\mathbb{R}$ isomorph auf $\{(x,0) : x \in \mathbb{R}\}$ abgebildet. Isomorph heißt hier bijektiv und verträglich mit der Körperstruktur, d.h. $I(x+u) = I(x) + I(u)$ und $I(xu) = I(x)\,I(u)$. Wir nennen daher die Zahlen $(x,0)$ reell und schreiben kurz x statt $(x,0)$.

Def.: Die Zahl $i := (0,1)$ heißt imaginäre Einheit.

Lemma 3: Es ist $i^2 = -1$ und $(x,y) = x + iy \quad \forall x,y \in \mathbb{R}$.

Bew.: $i^2 = (0,1)(0,1) = (0-1, 0+0) = (-1,0) = -1$.

$$x + iy = (x,0) + (0,1)(y,0) = (x,0) + (0,y) = (x,y). \quad \square$$

Mit dieser Schreibweise gehen $+$ und $\cdot$ über in:

$$x+iy + u+iv = (x+u) + i(y+v)$$
$$(x+iy)(u+iv) = (xu - yv) + i(xv + yu)$$

(Man rechnet also wie im reellen und beachtet $i^2 = -1$!)

Def.: Es sei $z = x+iy \in \mathbb{C}$ mit $x,y \in \mathbb{R}$. Dann heißen

$\operatorname{Re} z := x$ der Realteil,

$\operatorname{Im} z := y$ der Imaginärteil von z und

$\overline{z} := x - iy$ die zu z konjugiert komplexe Zahl.

Es gelten die folgenden Rechenregeln:

Lemma 4: Für $z = x+iy \in \mathbb{C}$ und $w = u+iv \in \mathbb{C}$

mit $x,y,u,v \in \mathbb{R}$ gelten:

1. $\overline{z+w} = \overline{z} + \overline{w}$, $\overline{zw} = \overline{z} \cdot \overline{w}$;
2. $\frac{1}{2}(z+\overline{z}) = x$, $\frac{1}{2i}(z-\overline{z}) = y$;
3. $z = \overline{z} \iff z$ reell (wie oben erklärt);
4. $z\overline{z} = x^2+y^2$, $z^{-1} = \dfrac{\overline{z}}{z\overline{z}} = \dfrac{x-iy}{x^2+y^2} \quad (z \neq 0)$.

(Beweis zur Übung empfohlen.)

Für den Rest dieses Abschnitts sei $K=(K,+,\cdot)$ ein Körper.

Bem. / Def.: Aufgrund der Assoziativgesetze

$$x_1+(x_2+x_3)=(x_1+x_2)+x_3 \quad ; \quad x_1(x_2x_3)=(x_1x_2)x_3 \quad (x_{1,2,3}\in K)$$

können wir $x_1+x_2+x_3 := (x_1+x_2)+x_3$ und $x_1x_2x_3 := (x_1x_2)x_3$ definieren. Auch für mehr als drei Summanden bzw. Faktoren sind die Ausdrücke

$$\sum_{k=1}^{n} x_k := x_1+\dots+x_n \quad \text{und} \quad \prod_{k=1}^{n} x_k := x_1\cdots x_n \quad (x_k\in K)$$

wohldefiniert. Allgemeiner setzen wir für $n,m\in\mathbb{Z}$, $x_k\in K$:

$$\sum_{k=m}^{n} x_k := \begin{cases} x_m+\dots+x_n & , \text{ falls } n\ge m \\ 0 & , \text{ falls } n<m \text{ („leere Summe")} \end{cases}$$

und

$$\prod_{k=m}^{n} x_k := \begin{cases} x_m\cdots x_n & , \text{ falls } n\ge m \\ 1 & , \text{ falls } n<m \text{ („leeres Produkt")}, \end{cases}$$

wobei Null und ~~und~~ Eins die Körperelemente sind.

Mit diesen Bezeichnungen gelten die folgenden Verallgemeinerungen der Kommutativgesetze und des Distributivgesetzes:

Lemma 5: Für $m\le k\le n$, $m'\le j\le n'$ seien $x_k, y_j\in K$. Ferner sei $(i_m,\dots,i_n)$ eine Umordnung von $(m,\dots,n)$. Dann gelten

1. $\displaystyle\sum_{k=m}^{n} x_{i_k} = \sum_{k=m}^{n} x_k$ und $\displaystyle\prod_{k=m}^{n} x_{i_k} = \prod_{k=m}^{n} x_k$,
2. $\displaystyle\left(\sum_{k=m}^{n} x_k\right)\left(\sum_{j=m'}^{n'} y_j\right) = \sum_{k=m}^{n}\sum_{j=m'}^{n'} x_k y_j$.

Vielfache und Potenzen werden folgendermaßen erklärt:

Def.: Für $n \in \mathbb{N}_0$ und $x \in K$ setzen wir

$$n \cdot x := \sum_{k=1}^{n} x = \underbrace{x + \ldots + x}_{n\text{-mal}} \quad ; \quad x^n := \prod_{k=1}^{n} x = \underbrace{x \cdot \ldots \cdot x}_{n\text{-mal}}$$

$$(-n)x := -nx \qquad ; \quad x^{-n} = (x^{-1})^n \quad (x \neq 0).$$

Bem.: (i) $0 \cdot x = 0$, $x^0 = 1$ in Übereinstimmung mit der Def. der leeren Summe bzw. des leeren Produkts.

(ii) $n \notin K$ ist möglich (endliche Körper!), insofern läßt sich die Def. des Vielfachen nicht aus den Axiomen folgern.

(iii) Es gelten die üblichen Rechenregeln:

- $(n+m)x = nx + mx$ • $x^{n+m} = x^n x^m$
- $n(x+y) = nx + ny$ • $(xy)^n = x^n y^n$
- $n(mx) = (n \cdot m)x$ • $x^{n \cdot m} = (x^m)^n$

(Auch dies ohne Beweis.)

Es sollen nun zwei einfache, aber wichtige Identitäten gezeigt werden, die in jedem Körper gelten:

Satz 2 (geometrische Summenformel): Es sei $x \in K \setminus \{1\}$ und $n \in \mathbb{N}_0$. Dann gilt

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

Bew.: $$(x-1)\sum_{k=0}^{n} x^k = x^{n+1} + x^n + \ldots + x - x^n - \ldots - x - 1 = x^{n+1} - 1.$$ $\square$

Da $x \neq 1$ $\Rightarrow$ Beh.

Satz 3 (Binomischer Lehrsatz): Es sei $x \in K$ und $n \in \mathbb{N}_0$. Dann gilt

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k.$$

Bew.: Ind. über n, beginnend mit

$n = 0$: $(1+x)^0 = 1 = \sum_{k=0}^{0} \binom{0}{k} x^0 \; (= x^0)$.

$n \to n+1$: $(1+x)^{n+1} = (1+x)^n (1+x)$

$$\overset{\text{I.V.}}{=} \left(\sum_{k=0}^{n} \binom{n}{k} x^k\right)(1+x) = \sum_{k=0}^{n} \binom{n}{k} x^k + \sum_{k=0}^{n} \binom{n}{k} x^{k+1}$$

$$= \sum_{k=0}^{n+1} \binom{n}{k} x^k + \sum_{\substack{k=1 \\ (k=0)}}^{n+1} \binom{n}{k-1} x^k \leftarrow \text{(Indexverschiebung!)}$$

$$= \sum_{k=0}^{n+1} \underbrace{\left(\binom{n}{k} + \binom{n}{k-1}\right)}_{=\binom{n+1}{k}} x^k = \sum_{k=0}^{n+1} \binom{n+1}{k} x^k.$$ $\square$

Folgerungen:

1. Für $a, b \in K$ ist $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k$.

Das ist klar für $a = 0$ und für $a \neq 0$ haben wir:

$$(a+b)^n = a^n \left(1 + \frac{b}{a}\right)^n \underset{\substack{\text{Satz 3,} \\ x = \frac{b}{a}}}{=} a^n \sum_{k=0}^{n} \binom{n}{k} \left(\frac{b}{a}\right)^k$$

$$= \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k.$$

2. $\sum_{k=0}^{n} \binom{n}{k} = 2^n$, $\sum_{k=0}^{n} \binom{n}{k} (-1)^k = \begin{cases} 1 & \text{für } n = 0 \\ 0 & \text{für } n \geq 1 \end{cases}$

(Setze $x = 1$ bzw. $x = -1$ in Satz 3!)

3. $\# M = n \Rightarrow \# \mathcal{P}(M) = 2^n$

Denn: $\# \mathcal{P}(M) = \sum_{k=0}^{n} \# \{ N \subset M : \# N = k \}$

$$\underset{\text{Bsp. aus 1.2}}{=} \sum_{k=0}^{n} \binom{n}{k} \underset{2.}{=} 2^n.$$