1.3 Körper

a) Definition

Eine Gruppe besitzt nur eine einzige Verknüpfung. Zum Rechnen und in der linearen Algebra benötigen wir jedoch Addition und Multiplikation.

<u>Def.:</u> Eine Menge K zusammen mit Verknüpfungen $+$ und $\cdot$ auf K heißt Körper, wenn folgendes gilt:

(K1) $(K,+)$ ist eine abelsche Gruppe,
das neutrale Element sei mit 0 bezeichnet.

(K2) Sei $K^* := K \setminus \{0\}$.
Dann gilt für $a, b \in K^*$ auch $a \cdot b \in K^*$,
und $(K^*, \cdot)$ ist eine abelsche Gruppe.

(K3) Es gelten die Distributivgesetze,
d.h. für $a, b, c \in K$ ist

$$a \cdot (b+c) = a \cdot b + a \cdot c \quad \text{und}$$

$$(a+b) \cdot c = a \cdot c + b \cdot c.$$

(Wie immer: Punktrechnung geht vor Strichrechnung.)

<u>Bem.:</u> die beiden Gesetze in (K3) sind wegen der Kommutativität von $\cdot$ äquivalent.

Bem.:

(1) Schreibweise: In $(K,+)$ wird das Neutrale mit 0 und das zu $a \in K$ Inverse mit $-a$ bezeichnet. In $(K \setminus \{0\}, \cdot)$ nennen wir das neutrale Element 1 und schreiben a^{-1} oder $\frac{1}{a}$ für das Inverse von a. Außerdem ist $\frac{b}{a} := a^{-1} b = a b^{-1}$.

(2) Es gelten folgende Rechenregeln:
Seien $a, b, x, \tilde{x} \in K$ beliebig.

i) $1 \neq 0$ (K hat mindestens 2 Elemente.)

ii) $0 \cdot a = a \cdot 0 = 0$

iii) Sei $a \cdot b = 0$. Dann folgt $a = 0$ oder $b = 0$.

iv) $a \cdot (-b) = -(a \cdot b)$ und $(-a) \cdot (-b) = a \cdot b$

v) Seien $x \cdot a = \tilde{x} \cdot a$ und $a \neq 0$. Dann ist $x = \tilde{x}$.

Bew.: i) $1 \in K^*$, aber $0 \notin K^*$

ii) $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$, subtrahiere $0 \cdot a$ auf beiden Seiten.

iii) Umkehrschluß folgt aus (K2):

$$a \neq 0 \text{ und } b \neq 0 \Rightarrow a \cdot b \neq 0$$

iv) $a \cdot b + (-a) \cdot b = (a + (-a)) \cdot b = 0 \cdot b = 0$

$(-a) \cdot (-b) = -((-a) \cdot b) = -(-a \cdot b) = a \cdot b$

v) „Kürzungsregel" gilt in K^*. → Aufgabe 2.2

Für $x = 0$ folgt $\tilde{x} = 0$ (iii), also $x = \tilde{x}$. □

(3) Beispiele für Körper:

i) reelle Zahlen $(\mathbb{R}, +, \cdot)$

ii) rationale Zahlen $(\mathbb{Q}, +, \cdot)$

iii) komplexe Zahlen $(\mathbb{C}, +, \cdot)$ → §1.3b

iv) der kleinste Körper: $\mathbb{F}_2 = \{0, 1\}$

+	0	1
0	0	1
1	1	0

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

$(\mathbb{F}_2, +) \cong C_2$

$(\mathbb{F}_2^*, \cdot) \cong C_1$

zyklische Gruppen

⇒ Bit-Operationen XOR und AND

(4) Auf $\mathbb{R}$ ist eine Ordnungsrelation $\leq$ definiert. Sie hat folgende Eigenschaften $(a, b, c \in \mathbb{R})$:

i) $a \leq a$ (reflexiv)

ii) $a \leq b$ und $b \leq a \Rightarrow a = b$ (antisymmetrisch)

iii) $a \leq b$ und $b \leq c \Rightarrow a \leq c$ (transitiv)

iv) $x \leq y$ oder $y \leq x$ (total)

vgl. Teilmengenrelation $\{1,2\} \not\subset \{2,3\}$ und $\{2,3\} \not\subset \{1,2\}$

v) $a \leq b \Rightarrow a + c \leq b + c$ (monoton bzgl. +)

vi) $a \leq b$ und $0 \leq c \Rightarrow ac \leq bc$ (monoton bzgl. $\cdot$)

Wir sagen, $\mathbb{R}$ ist ein geordneter Körper.

6) Komplexe Zahlen

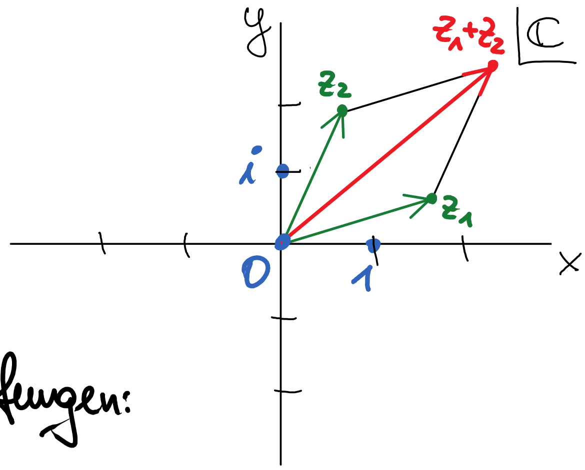
Motivation: $x^2+1=0$ ist für $x\in\mathbb{R}$ nicht lösbar.

Ausweg: Erweiterung der reellen Zahlen auf die komplexen Zahlen $\mathbb{C}$

Darstellung von $\mathbb{C}$ als

Gaußsche Zahlenebene:

$$\mathbb{C} := \{(x,y) \mid x,y\in\mathbb{R}\} = \mathbb{R}^2$$



Wir definieren folgende Verknüpfungen:

(1) Addition $+: \mathbb{C}\times\mathbb{C}\to\mathbb{C}$

Komponentenweise, wie in $\mathbb{R}$:

$$(x_1,y_1)+(x_2,y_2) = (x_1+x_2,\ y_1+y_2), \qquad x_1,x_2,y_1,y_2\in\mathbb{R}$$

($\Rightarrow$ Vektoraddition in $\mathbb{R}^2$)

- Assoziativität überträgt sich von $\mathbb{R}$
- neutrales Element: $0=(0,0)$
- Inverses zu $z=(x,y)$: $\quad -z=(-x,-y)$

$\Rightarrow$ $(\mathbb{C},+)$ ist eine abelsche Gruppe

(2) Multiplikation $\cdot: \mathbb{C}\times\mathbb{C}\to\mathbb{C}$

- neutrales Element: $1=(1,0)$
- imaginäre Einheit $i=(0,1)$ mit $i^2=-1$

- für $\lambda \in \mathbb{R}$ soll gelten: (Skalarmultiplikation in $\mathbb{R}^2$)

$$(\lambda,0)\cdot(x,y) = (\lambda x, \lambda y) = \lambda(x,y)$$

insbesondere: $(\lambda,0)\cdot(x,0) = (\lambda x,0)$

$\Rightarrow$ der Körper $\mathbb{R}$ ist in $\mathbb{C}$ enthalten: $\mathbb{R}\times\{0\} \subset \mathbb{C}$

- damit können wir schreiben:

$$(x,y) = x\cdot 1 + y\cdot i = x + iy$$

Es folgt:

$$(x_1,y_1)\cdot(x_2,y_2) = (x_1+iy_1)\cdot(x_2+iy_2)$$

(Distributivgesetz) $\quad = x_1x_2 + i(x_1y_2+y_1x_2) + i^2 y_1y_2$

$(i^2=-1)$ $\quad = x_1x_2 - y_1y_2 + i(x_1y_2+y_1x_2)$

Ergebnis:

$$(x_1,y_1)\cdot(x_2,y_2) = (x_1x_2-y_1y_2,\ x_1y_2+y_1x_2)$$

- geometrische Interpretation?

VL #5

(3) Betrag von $z\in\mathbb{C}$:

Norm (Länge) des Vektors $z=(x,y)$: $|z| := \sqrt{x^2+y^2}$

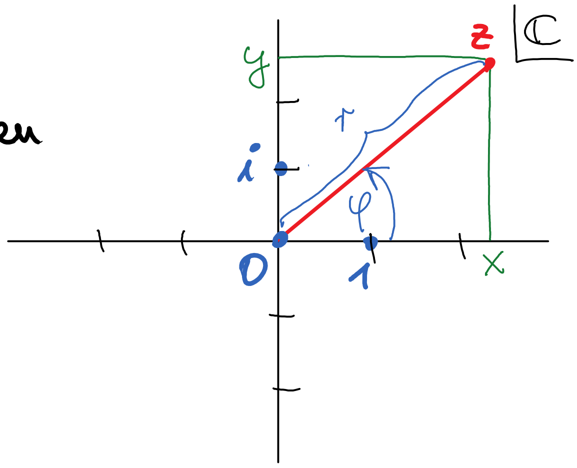
Es gilt $|z|\geq 0$, und $|z|=0 \Leftrightarrow z=0$.

(4) Polarform: Übergang zu Polarkoordinaten in $\mathbb{R}^2$

$$r := \sqrt{x^2+y^2} = |z|$$

Für $r>0$ $(z\neq 0)$ gibt es einen eindeutig bestimmten Winkel $\varphi\in[0,2\pi)$, so daß

$$x = r\cos(\varphi),\quad y = r\sin(\varphi).$$



Aus der Analysis: $\cos(\varphi) + i\sin(\varphi) = e^{i\varphi}$

(Beweis mittels Reihendarstellungen von cos, sin, exp.)

$\Rightarrow$ $z \in \mathbb{C} \setminus \{0\}$ hat die eindeutige Darstellung

$z = r e^{i\varphi}$ mit $r = |z| > 0$, $\varphi \in [0, 2\pi)$

$z = (r\cos(\varphi), r\sin(\varphi))$ „Argument von z"

- Multiplikation: Sei $z = r e^{i\varphi}$, $z' = r' e^{i\varphi'}$.

Dann ist $z \cdot z' = r r' e^{i(\varphi+\varphi')}$ (Drehstreckung)

Bew.: Additionstheoreme für cos, sin. Sei $r = r' = 1$.

$z \cdot z' = (\cos(\varphi)\cos(\varphi') - \sin(\varphi)\sin(\varphi'), \cos(\varphi)\sin(\varphi') + \sin(\varphi)\cos(\varphi'))$

$= (\cos(\varphi+\varphi'), \sin(\varphi+\varphi'))$ $\square$

(5) Komplex Konjugiertes von $z = (x, y) \in \mathbb{C}$:

(oder: z^*) $\bar{z} := (x, -y) = x - iy$ (Spiegelung an x-Achse)

- Regel: ersetze alle i durch $-i$
- es gilt: $z\bar{z} = (x+iy)\cdot(x-iy) = x^2 - i^2y^2 = x^2 + y^2$

also: $|z|^2 = z\bar{z}$

(6) multiplikative Gruppe $(\mathbb{C} \setminus \{0\}, \cdot)$

- Assoziativität: $(z \cdot z') \cdot z'' = (r r') r'' e^{i[(\varphi+\varphi')+\varphi'']} = z \cdot (z' \cdot z'')$
- Neutrales bzgl. $\cdot$: $r = 1, \varphi = 0 \Rightarrow (1, 0)$
- Inverses von $z \in \mathbb{C} \setminus \{0\}$: $z^{-1} = \frac{1}{|z|^2} \bar{z}$

(Reellmachen des Nenners durch Erweitern mit $\bar{z}$.)

Bew.: $z^{-1} z = \frac{1}{|z|^2} \bar{z} \cdot z = 1$ $\square$

$z = (x, y) = r e^{i\varphi} \Rightarrow z^{-1} = \left(\frac{x}{x^2+y^2}, \frac{-y}{x^2+y^2}\right) = \frac{1}{r} e^{-i\varphi}$

- Kommutativ: $z \cdot z' = z' \cdot z$

(7) das Distributivgesetz wurde für die Konstruktion der Multiplikation verwendet $\Rightarrow$ ist erfüllt

Check: $z_1 = (x_1, y_1) \in \mathbb{C}$, usw.

$$z_1 \cdot (z_2 + z_3)$$
$$= (x_1(x_2+x_3) - y_1(y_2+y_3),\ x_1(y_2+y_3) + y_1(x_2+x_3))$$
$$= (x_1x_2 - y_1y_2,\ x_1y_2 + y_1x_2) + (x_1x_3 - y_1y_3,\ x_1y_3 + y_1x_3)$$
$$= z_1 \cdot z_2 + z_1 \cdot z_3 \qquad \square$$

(8) aus (1,2,6,7) folgt: $\mathbb{C}$ ist ein Körper.
Aber $\mathbb{C}$ ist kein geordneter Körper. Es gibt keine mit $\leq$ vergleichbare Ordnungsrelation.

(9) es gilt wie in $\mathbb{R}$ die Dreiecksungleichung:
$$|z_1 + z_2| \leq |z_1| + |z_2| \quad \text{für } z_1, z_2 \in \mathbb{C}$$
Beweis: Übung.

(10) die Komponenten von $z = (x, y) \in \mathbb{C}$ heißen Real- und Imaginärteil:
$$\operatorname{Re} z := \frac{1}{2}(z + \bar{z}) = x$$
$$\operatorname{Im} z := \frac{1}{2i}(z - \bar{z}) = y$$

(11) Sei $z_n = e^{i 2\pi/n}$, $n \in \mathbb{N}$, also $|z| = 1$. Dann ist die Multiplikation mit z_n eine Drehung um $2\pi/n$.
Es gilt $(z_n)^n = 1 \Rightarrow \operatorname{erz}(\{z_n\}) \cong C_n$ (Drehgruppe)

c) Summenzeichen (nur Skript)

<u>Def.:</u> Sei $(A,+)$ eine abelsche Gruppe, und sei $a_k \in A$ für $k = n, n+1, \dots, m$. Dann schreiben wir für die endliche Summe s über die a_k:

$$s = \sum_{k=n}^{m} a_k := a_n + a_{n+1} + \dots + a_m.$$

m ← Ende

k ← Laufindex, n ← Beginn

<u>Bem.:</u>

(1) das Inverse zu $a \in A$ wird nicht benötigt.

(2) Schreibweise mit Indexmengen:

$$\sum_{k=n}^{m} a_k = \sum_{n \le k \le m} a_k = \sum_{k \in I} a_k, \qquad I := \{k \in \mathbb{Z} \mid n \le k \le m\}$$

(3) Analogie zu for-Schleifen, z.B. in C/C++:

```
double s=0;
for (k=n; k<=m; k=k+1)
{
      s = s+ a[k];
}
// die Summe steht in s
```

(4) Doppelsummen:

wegen Kommutativität von + und für endliche Summen gilt:

$$\sum_{i\in I}\Big(\sum_{j\in J} a_{ij}\Big) = \sum_{j\in J}\Big(\sum_{i\in I} a_{ij}\Big) = \sum_{(i,j)\in I\times J} a_{ij} = \sum_{i\in I, j\in J} a_{ij}$$

(5) Rechenregeln: Seien K ein Körper, I eine endliche Indexmenge, und $a_k, b_k, \lambda \in K$ $(k \in I)$. Dann gilt:

- Addition: $$\sum_{k\in I} a_k + \sum_{k\in I} b_k = \sum_{k\in I}(a_k+b_k)$$

- Skalarmultiplikation: $$\lambda \sum_{k\in I} a_k = \sum_{k\in I}(\lambda a_k)$$
  (kleines Distributivgesetz)

- Distributivgesetz: $$\left(\sum_{i\in I} a_i\right)\left(\sum_{j\in J} b_j\right) = \sum_{i\in I}\sum_{j\in J} a_i b_j$$

$$(1+2+3)\cdot(4+5) = 1\cdot 4 + 1\cdot 5 + 2\cdot 4 + 2\cdot 5 + 3\cdot 4 + 3\cdot 5$$

(6) Beispiel: binomische Formel $(n\in\mathbb{N})$

$$(a+b)^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k \qquad \binom{n}{k} = \frac{n!}{k!(n-k)!},\quad 0! = 1$$

$$= \underbrace{\binom{n}{0}}_{1}a^n b^0 + \underbrace{\binom{n}{1}}_{n}a^{n-1}b + \ldots + \underbrace{\binom{n}{n-1}}_{n}a b^{n-1} + \underbrace{\binom{n}{n}}_{1}b^n$$

$$= a^n + n a^{n-1}b + \frac{n(n-1)}{2}a^{n-2}b^2 + \ldots + n a b^{n-1} + b^n$$