Lineare Algebra und analytische Geometrie I

4. Algebraische Grundbegriffe.

Mengen mit Verknüpfungen

Definition (Def. 4.1.)

Eine Verknüpfung $\star$ auf einer Menge M ist eine Abbildung

$$\begin{aligned}&\mu\colon M \times M \to M \text{ mit } \mu((x,y)) = \mu(x,y) = x\star y\\ &(x,y) \mapsto x\star y\end{aligned}$$

die jedem geordneten Paar (x,y) mit $x,\ y \in M$ ein Element $x\star y \in M$ zuordnet.

Formall muss man $\mu((x,y))$ schreiben, $\mu(x,y)$ und $x\star y$ sind Abkürzungen.
Das Symbol "$\star$" ist ein Vertreter für z.B. "$+$" oder "$\cdot$".
Erste Beispiele:

$M = \mathbb{Z}, \star = +$	$M = \mathbb{Z}, \star = \cdot$	$M = \mathbb{Z}, \star = -$
$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$	$\mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$
$(m,n) \mapsto m+n$	$(m,n) \mapsto m\cdot n$	$(m,n) \mapsto m-n$

$\mu\colon M \times M \to M$
$(x, y) \mapsto x \star y$

Weitere Beispiele: min und max.

Für $m, n \in \mathbb{Z}$ setzen wir

$$\min(m,n) = \begin{cases} m, \text{ falls } m \leqslant n, \\ n, \text{ falls } n < m. \end{cases} \qquad \max(m,n) = \begin{cases} m, \text{ falls } m \geqslant n, \\ n, \text{ falls } n > m. \end{cases}$$

So bekommen wir noch zwei Verknüpfungen:

$$\begin{array}{c|c} \text{min}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} & \text{max}\colon \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z} \\ (m,n) \mapsto \min(m,n) & (m,n) \mapsto \max(m,n) \end{array}$$

Die Verknüpfungstafel der Verknüpfung “min"

Man kann eine Verknüpfung auf einer endlichen Menge durch ihre **Verknüpfungstafel** darstellen.
Sei $M = \{0, 1, 2, 3, 4, 5\} \subseteq \mathbb{Z}$ und $\mu\colon M \times M \to M$ die Abbildung min, also $\mu(m, n) = \min(m, n)$. Wir bilden eine Tafel, indem wir im Kästchen aus der Zeile “m” und der Spalte “n" $\min(m, n)$ stellen.

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	1	1	1	1
2	0	1	2	2	2	2
3	0	1	2	3	3	3
4	0	1	2	3	4	4
5	0	1	2	3	4	5

Logische Operationen als Verknüpfungen

Die logischen Operationen wie “und" können als Verknüpfungen auf $M = \{\text{wahr}, \text{falsch}\}$ aufgefasst werden.
Verknüpfungstafeln:

$\wedge$:

	wahr	falsch
wahr	wahr	falsch
falsch	falsch	falsch

$\vee$:

	wahr	falsch
wahr	wahr	wahr
falsch	wahr	falsch

$(\Rightarrow)$:

	wahr	falsch
wahr	wahr	falsch
falsch	wahr	wahr

Merken, dass die Tafel von $(\Rightarrow)$ nicht symmetrisch ist!

Definition (Def. 4.2.)

Eine Verknüpfung $(m, n) \mapsto m \star n$ auf einer Menge M heißt **kommutativ** genau dann, wenn gilt $m \star n = n \star m \quad \forall m, n \in M$.

Welche den Verknüpfungen "$+$", "$\cdot$", "$-$" auf $\mathbb{Z}$ sind kommutative?
Antwort: "$+$" und "$\cdot$".

Welche den Verknüpfungen $\wedge$, $\vee$, $(\Rightarrow)$ auf $M = \{\text{wahr}, \text{falsch}\}$ sind kommutative?
Antwort: $\wedge$ und $\vee$.

Definition (Def. 4.3.)

Eine Verknüpfung $(m, n) \mapsto m \star n$ auf einer Menge M heißt **assoziativ** genau dann, wenn gilt $(m \star n) \star k = m \star (n \star k) \quad \forall m, n, k \in M$.

Ist eine Verknüpfung $\star$ auf M assoziativ, so liefern auch ungeklammerte Ausdrücke der Form

$$x_1 \star x_2 \star \ldots \star x_n \quad \text{mit} \quad x_1, x_2, \ldots, x_n \in M$$

wohlbestimmte Elemente von M, das Resultat ist unabhängig davon, wie wir die Klammern setzen. Üblich schreibt man $2 + 7 + 6 + 14 + 21 + 3 + 57$,
weder $(2 + (7 + 6)) + ((14 + 21) + (3 + 57))$ noch
$2 + (7 + ((6 + (14 + 21)) + (3 + 57)))$ noch
$((2 + 7) + (6 + 14)) + ((21 + 3) + 57)$.
Dagegen ist $2 - 8 - 17 - 3$ nicht *wolldefiniert*, denn
$((2 - 8) - 17) - 3 = -26$, $(2 - 8) - (17 - 3) = -20$,
$(2 - (8 - 17)) - 3 = 8$, $2 - ((8 - 17) - 3) = 14$, $2 - (8 - (17 - 3)) = 8$.

Definition (Def. 4.4.)

Sei $(M, \star)$ eine Menge mit Verknüpfung. Ein Element $e \in M$ heißt **neutrales Element** von $(M, \star)$ genau dann, wenn gilt $x \star e = e \star x = x \; \forall x \in M$.

Lemma (Lemma 4.5. Eindeutigkeit neutraler Elemente)

Seien e, e' neutrale Elemente von $(M, \star)$. Dann gilt $e = e'$.

Beweis.

Es gilt $e \star e' = e$, weil e' ein neutrales Element ist, und $e \star e' = e'$, weil e ein neutrales Element ist. Daraus $e = e \star e' = e'$. □

Wir dürfen den bestimmten Artikel verwenden und in einer Menge mit Verknüpfung von dem neutralen Element reden und es mit $e_M = e_{(M,\star)}$ bezeichnen.

Definition (Def. 4.6.)

Ein **Monoid** ist eine Menge mit einer assoziativen Verknüpfung, in der es ein neutrales Element gibt.

Merken, ein Monoid ist nicht leer.
Einige Monodie:

1. $(\mathbb{Z}, +)$, $e_{(\mathbb{Z},+)} = 0$;
2. $(\mathbb{Z}, \cdot)$, $e_{(\mathbb{Z},\cdot)} = 1$;
3. $M = \{\text{wahr}, \text{falsch}\}$, $\star = \wedge$, $e_{(M,\wedge)} = \text{wahr}$;
4. $M = \{\text{wahr}, \text{falsch}\}$, $\star = \vee$, $e_{(M,\vee)} = \text{falsch}$.

Auch $(\mathbb{N} \cup \{0\}, +)$ ist ein Monoid, wo $e = 0$.

Sei X eine Menge und $M = \mathcal{P}(X)$ die Potenzmenge von X, d.h. die Menge aller Teilmengen von X. Das Schneiden und das Vereinigen von Teilmengen sind Verknüpfungen auf $\mathcal{P}(X)$.

$$\begin{array}{l|l} \cap\colon M \times M \to M & \cup\colon M \times M \to M \\ (A, B) \mapsto A \cap B & (A, B) \mapsto A \cup B \end{array}$$

Merken, dass

$$(A \cap B) \cap C = \{x \in M \mid x \in A \wedge x \in B \wedge x \in C\} = A \cap (B \cap C),$$

$$(A \cup B) \cup C = \{x \in M \mid x \in A \vee x \in B \vee x \in C\} = A \cup (B \cup C).$$

Die Verknüpfungen $\cap$ und $\cup$ sind assoziativ.

- $(M, \cap)$ ist ein Monoid, wo $e = M$;
- $(M, \cup)$ ist ein Monoid, wo $e = \varnothing$.

Gruppen

Wir erinnern uns, dass ein Monoid ist eine Menge mit einer assoziativen Verknüpfung, für die es in unserer Menge ein neutrales Element gibt.

Definition (Def. 4.7.)

(1) Ist $(M, \star)$ ein Monoid und $x \in M$ ein Element, so nennen wir ein weiteres Element $y \in M$ **invers zu** x genau dann, wenn gilt $x \star y = y \star x = e_{(M,\star)}$. Ein Element, das ein Inverses besitzt, heißt **invertierbar**.
(2) Eine **Gruppe** ist ein Monoid, in dem jedes Element ein Inverses besitzt.
(3) Eine **kommutative** Gruppe oder **abelsche** Gruppe ist eine Gruppe, deren Verknüpfung kommutativ ist.

Merken, $(\mathbb{Z}, +)$ ist eine kommutative Gruppe, $-n$ ist invers zu n. Aber in $(\mathbb{Z}, \cdot)$ sind nur 1 und -1 invertierbar. Damit ist $(\mathbb{Z}, \cdot)$ keine Gruppe.

Eine Gruppe, Definition mit Formeln

Eine Gruppe ist eine Menge G mit einer Verknüpfung $(x, y) \mapsto x \star y$, s.d.

(A1) $(x \star y) \star z = x \star (y \star z) \quad \forall x, y, z \in G$;

(A2) $\exists e \in G$, s.d. $e \star x = x \star e = x \quad \forall x \in G$;

(A3) $\forall x \in G \quad \exists y \in G$, s.d. $x \star y = y \star x = e$.

Die kleinste Gruppe ist $(\{e\}, \star)$, wo $e \star e = e$.
Falls eine Gruppe endlich ist, können wie wieder die Verknüpfungstafel betrachten.

Beispiel (Eine Gruppe G mit $|G| = 2$)

Sei es $G = \{e, x\}$ mit $e \neq x$.

	e	x
e	e	x
x	x	e

$x \star e = x \neq e$
e ist nicht invers zu x
Deswegen $x \star x = e$

"Bis auf Isomorphie" existiert höchstens eine Gruppe G mit $|G| = 2$.

Lemma (Lemma 4.8. Eindeutigkeit des Inverses)

Jedes Element eines Monoids besitzt höchstens ein Inverses.

Beweis.

Sei $(M, \star)$ ein Monoid und seien $x, y, y' \in M$ mit $x \star y = y \star x = e$, $x \star y' = y' \star x = e$. Dann

$$y' = e \star y' = (y \star x) \star y' = y \star (x \star y') = y \star e = y.$$

□

Wir dürfen den bestimmten Artikel benutzen und von dem Inversen x^{-1} eines Elements x eines Monoids und insbesondere auch einer Gruppe reden. Das Inverse des Inversen ist stets das ursprüngliche Element, in Formeln $(x^{-1})^{-1} = x$.

Komposition von Abbildungen als Verknüpfung

Sei X eine Menge, sei $M = \mathrm{Abb}(X, X)$ die Menge aller Abbildungen $f: X \to X$. Falls $f, h \in M$, dann ist $f \circ h: X \to X$ eine Abbildung von X nach X, also ein Element von M. Die Verknüpfung $(f, h) \mapsto f \circ h$ auf M ist assoziativ nach dem Satz 3.5. Dazu gilt $f \circ \mathrm{id}_X = f = \mathrm{id}_X \circ f \ \ \forall f \in M$.

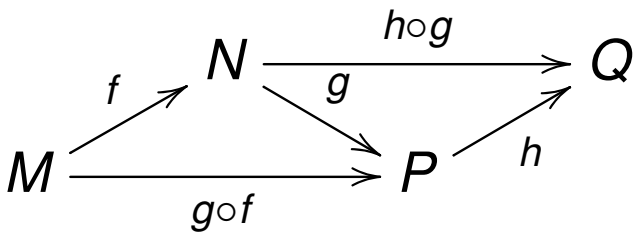
Korollar des Satzes 3.5. $(\mathrm{Abb}(X, X), \circ)$ ist ein Monoid, wo $e = \mathrm{id}_X$.

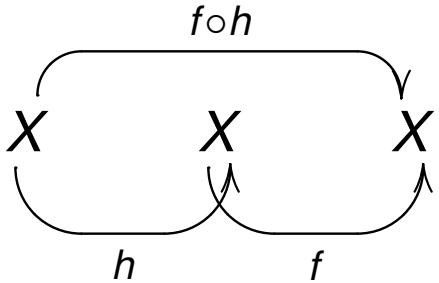
"Korollar" = "Folgerung"

Satz (Satz 3.5.)

Die Komposition von Abbildungen ist **assoziativ**, *es gilt* $(h \circ g) \circ f = h \circ (g \circ f)$ *für alle Abbildungen* $f: M \to N$, $g: N \to P$, $h: P \to Q$.

Bilder:





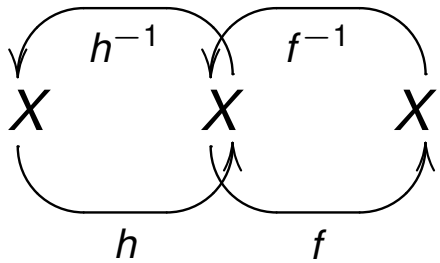
Korollar des Satzes 3.5. $(\mathrm{Abb}(X,X),\circ)$ ist ein Monoid, wo $e=\mathrm{id}_X$.

Übung (Blatt 2): $f\in\mathrm{Abb}(X,X)$ besitzt die inverse Abbildung $\Leftrightarrow$ f ist bijektiv.
Sei $\mathrm{Ab}(X)^\times$ die Menge aller bijektiven Abbildungen $f\colon X\to X$.
Seien $f,h\in\mathrm{Ab}(X)^\times$. Dann haben wir

$$(f\circ h)\circ(h^{-1}\circ f^{-1})=f\circ\underbrace{h\circ h^{-1}}_{\mathrm{id}_X}\circ f^{-1}=f\circ\mathrm{id}_X\circ f^{-1}=f\circ f^{-1}=\mathrm{id}_X.$$

Und ebenfalls $(h^{-1}\circ f^{-1})\circ(f\circ h)=\mathrm{id}_X$. Das heißt, $f\circ h\in\mathrm{Ab}(X)^\times$.

Das Bild:



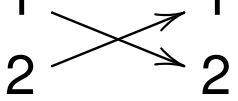
Zusammenfassung und die Hauptaussage

- $M = \mathrm{Abb}(X, X) = \{f : X \to X \mid f \text{ ist eine Abbildung}\}$.
- $\circ : M \times M \to M$ mit $(f, h) \mapsto f \circ h$, "$\circ$" ist assoziativ.
- $(M, \circ)$ ist ein Monoid, wo $e = \mathrm{id}_X$.
- $\mathrm{Ab}(X)^\times \subseteq M$, $\mathrm{Ab}(X)^\times = \{f \in M \mid f \text{ ist bijektiv}\}$.
- $f \circ h \in \mathrm{Ab}(X)^\times$, falls $f, h \in \mathrm{Ab}(X)^\times$.

Man sagt, dass die Teilmenge $\mathrm{Ab}(X)^\times$ **abgeschlossen unter der Verknüpfung** "$\circ$" ist.
Merken noch, dass $f^{-1} \in \mathrm{Ab}(X)^\times$, falls $f \in \mathrm{Ab}(X)^\times$.

- $(\mathrm{Ab}(X)^\times, \circ)$ ist eine Gruppe.

Beispiel: $X = \{1, 2\}$. Hier ist $G = \mathrm{Ab}(X)^\times = \{\mathrm{id}_X, (12)\}$,

wo (12): 

, eine Gruppe mit $|G| = 2$, $(12) \circ (12) = \mathrm{id}_X$.

Die Verknüpfungstafel der Gruppe aller Permutationen der Menge $\{1, 2, 3\}$

$X = \{1, 2, 3\}$. Die Elemente der Menge $G = \mathrm{Ab}(X)^{\times}$ sind Permutationen der Menge X. Eine solche Permutation σ stellen wir durch das geordnete Zahlentripel $\sigma(1)\sigma(2)\sigma(3)$ dar. Zum Beispiel, id_X ist durch 123 dargestellt. Nach dem Satz 1.2. gilt es $|G| = 3! = 6$.

	123	213	312	321	132	231
123	123	213	312	321	132	231
213	213	123	321	312	231	132
312	312	132	231	213	321	123
321	321	231	132	123	312	213
132	132	312	213	231	123	321
231	231	321	123	132	213	312

Jede Zeile und jede Spalte enthält alle 6 verschiedene Reihenfolge.

Homomorphismen

Seien $(M, \star)$, $(M', \star')$ Mengen mit Verknüpfungen.

Definition (Def. 4.9.)

Eine Abbildung $f : M \to M'$ ist ein **Homomorphismus von Mengen mit Verknüpfung**, falls $f(x \star y) = f(x) \star' f(y) \ \ \forall x, y \in M$. Wenn $(M, \star)$, $(M', \star')$ Gruppen sind, spricht man von **Gruppenhomomorphismen**.

Beispiele.

1. Sei $(M, \star) = (M', \star') = (\mathbb{Z}, +)$. Dann ist $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(n) = -n$ $\forall n \in \mathbb{Z}$ ein Gruppenhomomorphismus. Ebenfalls jede Abbildung $n \mapsto d \cdot n$ mit $d \in \mathbb{Z}$, $d \cdot (n + m) = d \cdot n + d \cdot m$.
2. Sei $(M, \star) = (M', \star') = (\mathbb{Z}, \cdot)$. Dann ist $f : \mathbb{Z} \to \mathbb{Z}$ mit $f(n) = n^2 = n \cdot n$ $\forall n \in \mathbb{Z}$ ein Homomorphismus von Mengen mit Verknüpfung, $f(n \cdot m) = (n \cdot m)^2 = n^2 \cdot m^2$.

Körper

Definition (Def. 4.10.)

Ein **Körper** $(\mathbb{K}, +, \cdot)$ ist eine Menge mit zwei kommutativen assoziativen Verknüpfungen, derart dass die folgenden drei Bedingungen erfüllt sind:

(A1) $(\mathbb{K}, +)$ ist eine Gruppe, die additive Gruppe des Körpers;

(A2) die Teilmenge $\mathbb{K}^\times = \mathbb{K} \setminus \{0_\mathbb{K}\}$, wo $0_\mathbb{K} = e_{(\mathbb{K},+)}$ ist unter "$\cdot$" abgeschlossen und $(\mathbb{K}^\times, \cdot)$ ist eine Gruppe, die multiplikative Gruppe des Körpers;

(A3) Es gilt das Distributivgesetz $a\cdot(b+c) = (a\cdot b) + (a\cdot c) \quad \forall a, b, c, \in \mathbb{K}$.

Beispiele: $(\mathbb{R}, +, \cdot)$ ist ein Körper, wo $e_{(\mathbb{R}^\times,\cdot)} = 1$, auch die Rationale Zahlen $\mathbb{Q} = \left\{ \frac{n}{m} \mid n, m \in \mathbb{Z}, m \neq 0 \right\}$ bilden einen Körper mit $e_{(\mathbb{Q}^\times,\cdot)} = 1$.

Die Menge $\mathbb{K}^\times$ ist eine Gruppe bezüglich "$\cdot$". Insbesondere ist sie nicht leer, es existiert ein neutrales Element $e_{(\mathbb{K}^\times,\cdot)}$, das mann mit $1 = 1_\mathbb{K}$ bezeichnet.

Also $1 \neq e_{(\mathbb{K},+)}$.

Körper, Notation und erste Eigenschaften

$(\mathbb{K}, +, \cdot)$: Die Verknüpfungen "$+$", "$\cdot$" sind kommutative und assoziativ,

(A1) $(\mathbb{K}, +)$ ist eine Gruppe,

(A2) $(\mathbb{K}^\times, \cdot)$ ist eine Gruppe, $\mathbb{K}^\times = \mathbb{K} \setminus \{0_\mathbb{K}\}$,

(A3) $a \cdot (b + c) = (a \cdot b) + (a \cdot c) \quad \forall a, b, c, \in \mathbb{K}$.

$e_{(\mathbb{K},+)}$ bezeichnet man mit $0 = 0_\mathbb{K}$. Es gilt immer $0_\mathbb{K} \neq 1_\mathbb{K}$. Sei $a \in \mathbb{K}$. Das Inverse von a bezüglich "$+$" bezeichnet man mit $-a$. Falls $a \neq 0$, ist $a^{-1} = \frac{1}{a} = 1/a$ das Inverse von a bezüglich "$\cdot$".

Merken $0 \cdot a = (0 + 0) \cdot a = (0 \cdot a) + (0 \cdot a)$ und

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

Also $0 \cdot a = 0 \quad \forall a \in \mathbb{K}$, analog $a \cdot 0 = 0$.

"Punk vor Strich": $a \cdot c + b \cdot d = (a \cdot c) + (b \cdot d)$.

"Weglassen von Multiplikationssymbolen": $ab = a \cdot b$.

Wenn wir mit Buchstaben rechnen, werden wir meist $a \cdot b := ab$ abkürzen.

Mit durch Ziffern dargestellten Zahlen ist das wenig sinnvoll, $21 = 7 \cdot 3 \neq 73$.

Der Körper $\mathbb{F}_2$

$(\mathbb{K}, +, \cdot)$: Die Verknüpfungen "$+$", "$\cdot$" sind kommutative und assoziativ, $(\mathbb{K}, +)$ ist eine Gruppe, $(\mathbb{K}^\times, \cdot)$ ist eine Gruppe, $K^\times = \mathbb{K} \setminus \{0_\mathbb{K}\}$, $a \cdot (b + c) = ab + ac \ \ \forall a, b, c, \in \mathbb{K}$.

Der kleinste Körper besteht aus zwei Elementen 0 und 1, $\mathbb{F}_2 = \{0, 1\}$. Die Addition und Multiplikation kann man so verstehen, wir addieren (oder multiplizieren) 1 und 0 als ganze Zahlen und nehmen danach den Rest modulo 2, sowie $1 + 1$ ist 2 in $\mathbb{Z}$ und damit 0 in $\mathbb{F}_2$.

Die Verknüpfungen "$+$", "$\cdot$" sind kommutative und assoziativ, weil sie auf $\mathbb{Z}$ diese Eigenschaften erfüllen. Das Distributivgesetz gilt, kann man sogar direkt sehen: $1(a + b) = a + b, \ \ 0(a + b) = 0$.

$(\mathbb{F}_2, +)$ ist eine Gruppe; $(\mathbb{F}_2^\times, \cdot) = (\{1\}, \cdot)$ ist eine Gruppe. Die Verknpfungstafeln auf $\mathbb{F}_2$ sind

"$+$":

	0	1
0	0	1
1	1	0

"$\cdot$":

	0	1
0	0	0
1	0	1

Betrachten wir die folgende Bijektion zwischen $\{0, 1\}$ und $\{$wahr,falsch$\}$

$$0 \longleftrightarrow \text{falsch}$$

$$1 \longleftrightarrow \text{wahr}$$

so entspricht "$\cdot$" der Konjunktion, aber "$+$" der Disjunktion nicht. Vergleichen

"$\cdot$" in $\mathbb{F}_2$:

	0	1
0	0	0
1	0	1

$\wedge$:

	falsch	wahr
falsch	falsch	falsch
wahr	falsch	wahr

"$+$" in $\mathbb{F}_2$:

	0	1
0	0	1
1	1	0

$\vee$:

	falsch	wahr
falsch	falsch	wahr
wahr	wahr	wahr

Lemma (Lemma 4.11)

In jedem Körper $\mathbb{K}$ gilt:

1. $ab = 0 \Rightarrow (a = 0 \vee b = 0)$;
2. $-a = (-1)a \ \forall a \in \mathbb{K}$;
3. $(-1)(-1) = 1$;
4. $(-a)(-b) = ab \ \forall a, b \in \mathbb{K}$;
5. $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \ \forall a, c \in \mathbb{K}, \ \forall b, d \in \mathbb{K}^\times$;
6. $\frac{ac}{bc} = \frac{a}{b} \ \forall a \in \mathbb{K}, \ \forall b, c \in \mathbb{K}^\times$;
7. $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \ \forall a, c \in \mathbb{K}, \ \forall b, d \in \mathbb{K}^\times$;
8. $m(ab) = (ma)b \ \forall m \in \mathbb{Z}, \forall a, b \in \mathbb{K}$.

(1) $ab = 0 \Rightarrow (a = 0 \vee b = 0)$.
(2) $-a = (-1)a \ \ \forall a \in \mathbb{K}$.

Beweis.

(1) Die Menge $\mathbb{K} \setminus \{0\}$ ist bezüglich die Multiplikation abgeschlossen. Oder merken, dass

$$a^{-1}ab = b, \text{ falls } a \neq 0.$$

Deswegen, $(a \neq 0 \wedge ab = 0) \Rightarrow b = 0$.

(2) Das inverse Element zu a bezüglich "$+$" ist eindeutig, dieses Element bezeichnet man mit $-a$. Nun

$$(-1)a + a = \underbrace{1a + (-1)a = (1 + (-1))a}_{\text{Distributivgesetz}} = 0a = 0.$$

□

(3) $(-1)(-1) = 1$.
(4) $(-a)(-b) = ab \ \ \forall a, b \in \mathbb{K}$.
(5) $\frac{a}{b}\frac{c}{d} = \frac{ac}{bd} \ \ \forall a, c \in \mathbb{K}, \ \forall b, d \in \mathbb{K}^\times$.

Beweis.

(3) Wir wissen schon, dass $(-1)a = -a$ für alle $a \in \mathbb{K}$. Also $(-1)(-1) = -(-1) = 1$.

(4)

$$(-a)(-b) = (-1)a(-1)b = (-1)(-1)ab = 1ab = ab.$$

(5)

$$\frac{a}{b}\frac{c}{d} = ab^{-1}cd^{-1} = acb^{-1}d^{-1} = ac(db)^{-1} = ac(bd)^{-1} = \frac{ac}{bd}.$$

□

(6) $\frac{ac}{bc} = \frac{a}{b} \quad \forall a \in \mathbb{K},\ \forall b, c \in \mathbb{K}^\times$.

(7) $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd} \quad \forall a, c \in \mathbb{K},\ \forall b, d \in \mathbb{K}^\times$.

Beweis.

(6)

$$\frac{ac}{bc} = ac(bc)^{-1} = acc^{-1}b^{-1} = ab^{-1} = \frac{a}{b}.$$

(7)

$$\frac{a}{b} + \frac{c}{d} = \frac{ad}{bd} + \frac{bc}{bd} = ad \cdot \frac{1}{bd} + bc \cdot \frac{1}{bd} = (ad + bc) \cdot \frac{1}{bd} = \frac{ad + bc}{bd}.$$

□

(8) $m(ab) = (ma)b \quad \forall m \in \mathbb{Z}, \forall a, b \in \mathbb{K}$.
Man definiert

$$na = \underbrace{a + a + \ldots + a}_{n \text{ Stücke } a} \quad \forall n \in \mathbb{N}, \ \forall a \in \mathbb{K}$$

und setzt dazu $0_{\mathbb{Z}} \cdot a = 0_{\mathbb{K}}$, $(-n)a = -na = n(-a)$.

Beweis.

(8) Merken, $0_{\mathbb{Z}} \cdot (ab) = 0_{\mathbb{K}} = 0_{\mathbb{K}} b = (0_{\mathbb{Z}} \cdot a)b$, stimmt. Weiter,

$$n(ab) = \underbrace{ab + ab + \ldots + ab}_{n \text{ Stücke } ab} = (\underbrace{a + a + \ldots + a}_{n \text{ Stücke } a})b = (na)b$$

wegen des Distributivgesetzes.
Dazu $(-n)(ab) = n(-ab) = (n(-a))b = ((-n)a)b$. □

Der Aufbau des Zahlensystems

$$\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$$

- Eine vollständig überzeugende Konstruktion der natürlichen Zahlen $\mathbb{N}$ ist nur im Rahmen der Logik möglich.
- $\mathbb{N} \subset \mathbb{Z}$: Der Begriff von 0 und Lösbarkeit aller Gleichungen des Typs $x + a = b$.
- $\mathbb{Z} \subset \mathbb{Q}$: Lösbarkeit aller Gleichungen des Typs $ax = b$ mit $a \neq 0$.
- $\mathbb{Q} \subset \mathbb{R}$: Jeder unendliche Folge $a_1, a_2, \ldots, a_n, \ldots,$ wo $a_n \in \mathbb{Q}$ und $|a_{n+1} - a_n| < \frac{1}{2}|a_n - a_{n-1}|$ für jede n, besitzt einen Limis.
- $\mathbb{R} \subset \mathbb{C}$: Lösbarkeit aller Gleichungen des Typs $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0 = 0$.