Lineare Algebra algebraische Strukturen 2

Reinhold Hübl

Wintersemester 2020/21



Definition

Eine Gruppe (G, \circ) heißt **kommutativ** oder **abelsch** wenn für je zwei Elemente $g, h \in G$ gilt:

$$g \circ h = h \circ g$$

Beispiel

 $(\mathbb{Z},+),(\mathbb{R},+)$ und $(\mathbb{Q},+)$ sind kommutative Gruppen.

 $(\mathbb{R}\setminus\{0\},\cdot)$ und $(\mathbb{Q}\setminus\{0\},\cdot)$ sind kommutative Gruppen

Definition

Eine Gruppe (G, \circ) heißt **kommutativ** oder **abelsch** wenn für je zwei Elemente $g, h \in G$ gilt:

$$g \circ h = h \circ g$$

Beispiel

 $(\mathbb{Z},+),(\mathbb{R},+)$ und $(\mathbb{Q},+)$ sind kommutative Gruppen.

 $(\mathbb{R}\setminus\{0\},\cdot)$ und $(\mathbb{Q}\setminus\{0\},\cdot)$ sind kommutative Gruppen

Beispiel

Ist G die Gruppe der bijektiven Abbildungen von $\mathbb R$ in sich, so ist G nicht kommutativ.



Definition

Eine Gruppe (G, \circ) heißt **kommutativ** oder **abelsch** wenn für je zwei Elemente $g, h \in G$ gilt:

$$g \circ h = h \circ g$$

Beispiel

 $(\mathbb{Z},+),(\mathbb{R},+)$ und $(\mathbb{Q},+)$ sind kommutative Gruppen.

 $(\mathbb{R}\setminus\{0\},\cdot)$ und $(\mathbb{Q}\setminus\{0\},\cdot)$ sind kommutative Gruppen

Beispiel

Ist G die Gruppe der bijektiven Abbildungen von $\mathbb R$ in sich, so ist G nicht kommutativ.



Übung

Überprüfen Sie, ob die Gruppe S_3 der Permutationen der Zahlen 1,2 und 3 kommutativ ist.

Übung

Überprüfen Sie, ob die Gruppe S_3 der Permutationen der Zahlen 1,2 und 3 kommutativ ist.

Lösung:

Die Gruppe S_3 ist nicht kommutativ. Generell ist für $n \ge 3$ die Gruppe S_n der Permuationen nicht kommutativ.

Übung

Überprüfen Sie, ob die Gruppe S_3 der Permutationen der Zahlen 1,2 und 3 kommutativ ist.

Lösung:

Die Gruppe S_3 ist nicht kommutativ. Generell ist für $n \ge 3$ die Gruppe S_n der Permuationen nicht kommutativ.

So ist etwa

$$\langle 1 \ 2 \rangle \circ \langle 1 \ 3 \rangle \neq \langle 1 \ 3 \rangle \circ \langle 1 \ 2 \rangle.$$



Übung

Überprüfen Sie, ob die Gruppe S_3 der Permutationen der Zahlen 1,2 und 3 kommutativ ist.

Lösung:

Die Gruppe S_3 ist nicht kommutativ. Generell ist für $n \ge 3$ die Gruppe S_n der Permuationen nicht kommutativ.

So ist etwa

$$\langle 1 \ 2 \rangle \circ \langle 1 \ 3 \rangle \neq \langle 1 \ 3 \rangle \circ \langle 1 \ 2 \rangle.$$



Für ein Element $g \in (G, \circ)$ mit neutralem Element e setzen wir $g^0 = e$, $g^2 = g \circ g$, und allgemein für $n \ge 1$:

$$g^{n} = \underbrace{g \circ g \circ \cdots \circ g}_{\substack{n--\text{mal} \\ n--\text{mal}}}$$

(so dass also $g^n \circ g^m = g^{n+m}$ für alle $n, m \in \mathbb{Z}$).

Lemma

Ist G eine endliche Gruppe und $g \in G$, so gibt es ein $n \ge 1$ mit $g^n = e$.

Für ein Element $g \in (G, \circ)$ mit neutralem Element e setzen wir $g^0 = e$, $g^2 = g \circ g$, und allgemein für $n \ge 1$:

$$g^{n} = \underbrace{g \circ g \circ \cdots \circ g}_{\substack{n--\text{mal} \\ n--\text{mal}}}$$

(so dass also $g^n \circ g^m = g^{n+m}$ für alle $n, m \in \mathbb{Z}$).

Lemma

Ist G eine endliche Gruppe und $g \in G$, so gibt es ein $n \ge 1$ mit $g^n = e$.

Definition

Ist G eine endliche Gruppe und $g \in G$, so heißt

$$\operatorname{ord}(g) := \min\{n \geq 1 : g^n = e\}$$

die Ordnung von g.

Bemerkung

Für eine endliche Gruppe *G* gilt:

Definition

Ist G eine endliche Gruppe und $g \in G$, so heißt

$$\operatorname{ord}(g) := \min\{n \geq 1 : g^n = e\}$$

die **Ordnung** von g.

Bemerkung

Für eine endliche Gruppe *G* gilt:

① Genau dann gilt ord(g) = 1, wenn g = e.

Definition

Ist G eine endliche Gruppe und $g \in G$, so heißt

$$\operatorname{ord}(g) := \min\{n \geq 1 : g^n = e\}$$

die **Ordnung** von g.

Bemerkung

Für eine endliche Gruppe *G* gilt:

- **1** Genau dann gilt ord(g) = 1, wenn g = e.
- ② Für alle $1 \le i < j \le \operatorname{ord}(g)$ gilt: $g^i \ne g^j$.



Definition

Ist G eine endliche Gruppe und $g \in G$, so heißt

$$\operatorname{ord}(g) := \min\{n \geq 1 : g^n = e\}$$

die **Ordnung** von g.

Bemerkung

Für eine endliche Gruppe G gilt:

- **1** Genau dann gilt ord(g) = 1, wenn g = e.
- ② Für alle $1 \le i < j \le \operatorname{ord}(g)$ gilt: $g^i \ne g^j$.

Ist G eine endliche Gruppe und $g \in G$, so gilt: $\operatorname{ord}(g) | \operatorname{ord}(G)$.

Definition

Ist G eine endliche Gruppe und $g \in G$, so heißt

$$\operatorname{ord}(g) := \min\{n \geq 1 : g^n = e\}$$

die **Ordnung** von g.

Bemerkung

Für eine endliche Gruppe G gilt:

- **1** Genau dann gilt ord(g) = 1, wenn g = e.
- ② Für alle $1 \le i < j \le \operatorname{ord}(g)$ gilt: $g^i \ne g^j$.

Lemma

Ist G eine endliche Gruppe und $g \in G$, so gilt: $\operatorname{ord}(g) | \operatorname{ord}(G)$.

Speziell gilt also $g^{\operatorname{ord}(G)} = e$.

Definition

Ist G eine endliche Gruppe und $g \in G$, so heißt

$$\operatorname{ord}(g) := \min\{n \geq 1 : g^n = e\}$$

die **Ordnung** von g.

Bemerkung

Für eine endliche Gruppe G gilt:

- Genau dann gilt $\operatorname{ord}(g) = 1$, wenn g = e.
- ② Für alle $1 \le i < j \le \operatorname{ord}(g)$ gilt: $g^i \ne g^j$.

Lemma

Ist G *eine endliche Gruppe und* $g \in G$, *so gilt*: $\operatorname{ord}(g) | \operatorname{ord}(G)$.

Speziell gilt also $g^{\operatorname{ord}(G)} = e$.

Bemerkung

Ist G eine endliche Gruppe und $g \in G$ so schreiben wir

$$\langle g \rangle = \{g = g^1, g^2, g^3, \ldots\}$$

für die Teilmenge von G, die aus den Potenzen von g besteht.

Definition

Eine endliche Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit

$$\langle g \rangle = G$$

In diesem Fall heißt g ein Erzeuger von G.



Bemerkung

Ist G eine endliche Gruppe und $g \in G$ so schreiben wir

$$\langle g \rangle = \{g = g^1, g^2, g^3, \ldots\}$$

für die Teilmenge von G, die aus den Potenzen von g besteht.

Definition

Eine endliche Gruppe G heißt **zyklisch**, wenn es ein $g \in G$ gibt mit

$$\langle g \rangle = G$$

In diesem Fall heißt g ein **Erzeuger** von G.



Beispiel

Die Gruppe $(\mathbb{Z}/n\mathbb{Z},+)$ ist zyklisch mit Erzeuger g=1

Beispiel

Die Gruppe $M = \{1, -1\}$ mit

$$\begin{array}{c|cccc} \circ & 1 & -1, \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array}$$

ist zyklisch mit Erzeuger -1



Beispiel

Die Gruppe $(\mathbb{Z}/n\mathbb{Z},+)$ ist zyklisch mit Erzeuger g=1

Beispiel

Die Gruppe $M = \{1, -1\}$ mit

$$\begin{array}{c|cccc} \circ & 1 & -1, \\ \hline 1 & 1 & -1 \\ -1 & -1 & 1 \end{array}$$

ist zyklisch mit Erzeuger -1

Definition

Ein **Ring** $(R,+,\cdot)$ ist eine nichtleere Menge R mit zwei Verknüpfungen + (Addition) und \cdot (Multiplikation), die zwei Elemente 0,1 enthält, wobei $0 \neq 1$ ist und wobei gilt

- (R, +, 0) ist eine kommutative Gruppe.
- $(R, \cdot, 1)$ ist ein Monoid.
- Es gelten die Distributivgesetze

$$(r+s) \cdot t = r \cdot t + s \cdot t$$
 für alle $r, s, t \in R$
 $r \cdot (s+t) = r \cdot s + r \cdot t$ für alle $r, s, t \in R$

Ist $(R,\cdot,1)$ kommutativ, so nennen wir $(R,+,\cdot)$ einen kommutativen Ring.

Beispiel

 $(\mathbb{Z},+,\cdot)$ ist ein (kommutativer) Ring.

Beispiel

 $(\mathbb{R},+,\cdot)$ und $(\mathbb{Q},+,\cdot)$ sind kommutative Ringe.



Beispiel

 $(\mathbb{Z},+,\cdot)$ ist ein (kommutativer) Ring.

Beispiel

 $(\mathbb{R},+,\cdot)$ und $(\mathbb{Q},+,\cdot)$ sind kommutative Ringe.

Beispiel

 $(\mathbb{N},+,\cdot)$ ist kein Ring.

Beispiel

 $(\mathbb{Z},+,\cdot)$ ist ein (kommutativer) Ring.

Beispiel

 $(\mathbb{R}, +, \cdot)$ und $(\mathbb{Q}, +, \cdot)$ sind kommutative Ringe.

Beispiel

 $(\mathbb{N}, +, \cdot)$ ist kein Ring.

Beispiel

Für eine ganze Zahl n>1 betrachtenn wir $\mathbb{Z}/n\mathbb{Z}$, also die Menge der Äquivalenzklassen der Äquivalenzrelation "unterscheiden sich um ein Vielfaches von n", dh.

$$a \sim b \iff n | (b - a)$$

Wir definieren auf $\mathbb{Z}/(n)$ Verknüpfungen + und \cdot durch

$$[r] + [s] := [r + s]$$
 für alle $[r], [s] \in \mathbb{Z}/(n)$
 $[r] \cdot [s] := [r \cdot s]$ für alle $[r], [s] \in \mathbb{Z}/(n)$

Beispiel

Für eine ganze Zahl n>1 betrachtenn wir $\mathbb{Z}/n\mathbb{Z}$, also die Menge der Äquivalenzklassen der Äquivalenzrelation "unterscheiden sich um ein Vielfaches von n", dh.

$$a \sim b \iff n | (b-a)$$

Wir definieren auf $\mathbb{Z}/(n)$ Verknüpfungen + und \cdot durch

$$[r] + [s] := [r + s]$$
 für alle $[r], [s] \in \mathbb{Z}/(n)$
 $[r] \cdot [s] := [r \cdot s]$ für alle $[r], [s] \in \mathbb{Z}/(n)$

Dann ist $(\mathbb{Z}/(n), +, \cdot)$ ein kommutativer Ring mit Nullelement [0] und Einselement [1].

Beispiel

Für eine ganze Zahl n>1 betrachtenn wir $\mathbb{Z}/n\mathbb{Z}$, also die Menge der Äquivalenzklassen der Äquivalenzrelation "unterscheiden sich um ein Vielfaches von n", dh.

$$a \sim b \iff n | (b - a)$$

Wir definieren auf $\mathbb{Z}/(n)$ Verknüpfungen + und \cdot durch

$$[r] + [s] := [r + s]$$
 für alle $[r], [s] \in \mathbb{Z}/(n)$
 $[r] \cdot [s] := [r \cdot s]$ für alle $[r], [s] \in \mathbb{Z}/(n)$

Dann ist $(\mathbb{Z}/(n), +, \cdot)$ ein kommutativer Ring mit Nullelement [0] und Einselement [1].

Beispiel

Wir setzen

$$\mathbb{R}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}\$$

und für
$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$$
 und $g(x) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ definieren wir

•
$$(f+g)(X) = a_n X^n + \dots + (a_m + b_m) \cdot X^m + \dots + (a_1 + b_1)X + a_0 + b_0$$

falls $n > m$.

Beispiel

Wir setzen

$$\mathbb{R}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}\$$

und für $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ und $g(x) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ definieren wir

- $(f+g)(X) = a_n X^n + \dots + (a_m + b_m) \cdot X^m + \dots + (a_1 + b_1)X + a_0 + b_0$ falls n > m.
- $(f+g)(X) = b_m X^m + \dots + (a_n + b_n) \cdot X^n + \dots + (a_1 + b_1) X + a_0 + b_0$ falls n < m.

Beispiel

Wir setzen

$$\mathbb{R}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}\$$

und für $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ und $g(x) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ definieren wir

- $(f+g)(X) = a_n X^n + \dots + (a_m + b_m) \cdot X^m + \dots + (a_1 + b_1)X + a_0 + b_0$ falls n > m.
- $(f+g)(X) = b_m X^m + \cdots + (a_n + b_n) \cdot X^n + \cdots + (a_1 + b_1)X + a_0 + b_0$ falls n < m.
- $\bullet (f \cdot g)(X) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) \cdot X^k.$

Beispiel

Wir setzen

$$\mathbb{R}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}\$$

und für $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ und $g(x) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ definieren wir

- $(f+g)(X) = a_n X^n + \cdots + (a_m + b_m) \cdot X^m + \cdots + (a_1 + b_1)X + a_0 + b_0$ falls n > m.
- $(f+g)(X) = b_m X^m + \dots + (a_n + b_n) \cdot X^n + \dots + (a_1 + b_1)X + a_0 + b_0$ falls n < m.
- $\bullet (f \cdot g)(X) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) \cdot X^k.$

Beispiel

Wir setzen

$$\mathbb{R}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}\$$

und für $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ und $g(x) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ definieren wir

- $(f+g)(X) = a_n X^n + \cdots + (a_m + b_m) \cdot X^m + \cdots + (a_1 + b_1)X + a_0 + b_0$ falls n > m.
- $(f+g)(X) = b_m X^m + \dots + (a_n + b_n) \cdot X^n + \dots + (a_1 + b_1)X + a_0 + b_0$ falls n < m.
- $(f \cdot g)(X) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) \cdot X^k$.

Dann ist R[X] ein kommutativer Ring.

Beispiel

Wir setzen

$$\mathbb{R}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}\$$

und für $f(X) = a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0$ und $g(x) = b_m X^m + b_{m-1} X^{m-1} + \dots + b_1 X + b_0$ definieren wir

- $(f+g)(X) = a_n X^n + \dots + (a_m + b_m) \cdot X^m + \dots + (a_1 + b_1)X + a_0 + b_0$ falls n > m.
- $(f+g)(X) = b_m X^m + \dots + (a_n + b_n) \cdot X^n + \dots + (a_1 + b_1)X + a_0 + b_0$ falls n < m.
- $(f \cdot g)(X) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) \cdot X^k$.

Dann ist R[X] ein kommutativer Ring.

Statt \mathbb{R} hätten wir genauso gut \mathbb{Q} oder sogar \mathbb{Z} nehmen können.

Beispiel

Wir setzen

$$\mathbb{R}[X] = \{a_n X^n + a_{n-1} X^{n-1} + \dots + a_1 X + a_0 \mid n \in \mathbb{N}, a_i \in \mathbb{R}\}\$$

und für $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ und $g(x) = b_m X^m + b_{m-1} X^{m-1} + \cdots + b_1 X + b_0$ definieren wir

- $(f+g)(X) = a_n X^n + \cdots + (a_m + b_m) \cdot X^m + \cdots + (a_1 + b_1)X + a_0 + b_0$ falls n > m.
- $(f+g)(X) = b_m X^m + \cdots + (a_n + b_n) \cdot X^n + \cdots + (a_1 + b_1) X + a_0 + b_0$ falls n < m.
- $\bullet (f \cdot g)(X) = \sum_{k=0}^{n+m} \left(\sum_{i=0}^{k} a_i \cdot b_{k-i} \right) \cdot X^k.$

Dann ist R[X] ein kommutativer Ring.

Statt \mathbb{R} hätten wir genauso gut \mathbb{Q} oder sogar \mathbb{Z} nehmen können.

Beispiel

Für
$$f(X) = X^3 + X + 1$$
 und $g(X) = 3X^2 + 5X + 2$ gilt
$$(f \cdot g)(X) = (X^3 + X + 1) \cdot (3X^2 + 5X + 2)$$

$$= 3X^5 + 5X^4 + 2X^3 + 3X^3 + 5X^2 + 2X + 3X^2 + 5X + 2$$

$$= 3X^4 + 5X^4 + 5X^3 + 8X^2 + 7X + 2$$

Definition

 $\mathbb{R}[X]$ heißt **Polynomring über** \mathbb{R} .



Beispiel

Für
$$f(X) = X^3 + X + 1$$
 und $g(X) = 3X^2 + 5X + 2$ gilt

$$(f \cdot g)(X) = (X^3 + X + 1) \cdot (3X^2 + 5X + 2)$$

= $3X^5 + 5X^4 + 2X^3 + 3X^3 + 5X^2 + 2X + 3X^2 + 5X + 2$
= $3X^4 + 5X^4 + 5X^3 + 8X^2 + 7X + 2$

Definition

 $\mathbb{R}[X]$ heißt **Polynomring über** \mathbb{R} .

Definition

Ist $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ ein Polynom in $\mathbb{R}[X]$, und ist $a_n \neq 0$, so heißt

$$\deg(f(X)) = n$$

der **Grad** von f(X).

Beispiel

Für
$$f(X) = X^3 + X + 1$$
 und $g(X) = 3X^2 + 5X + 2$ gilt

$$(f \cdot g)(X) = (X^3 + X + 1) \cdot (3X^2 + 5X + 2)$$

= $3X^5 + 5X^4 + 2X^3 + 3X^3 + 5X^2 + 2X + 3X^2 + 5X + 2$
= $3X^4 + 5X^4 + 5X^3 + 8X^2 + 7X + 2$

Definition

 $\mathbb{R}[X]$ heißt **Polynomring über** \mathbb{R} .

Definition

Ist $f(X) = a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$ ein Polynom in $\mathbb{R}[X]$, und ist $a_n \neq 0$, so heißt

$$\deg(f(X)) = n$$

der **Grad** von f(X).

Übung

Wir betrachten $M = \mathbb{R} \times \mathbb{R}$ mit der Addition

$$(a,b)+(c,d)=(a+c,b+d)$$

und der Multiplikation

$$(a,b)\cdot(c,d)=(ac,ad+bc)$$

Überprüfen Sie, ob *M* dadurch zum kommutativen Ring wird.



Übung

Wir betrachten $M = \mathbb{R} \times \mathbb{R}$ mit der Addition

$$(a,b)+(c,d)=(a+c,b+d)$$

und der Multiplikation

$$(a,b)\cdot(c,d)=(ac,ad+bc)$$

Überprüfen Sie, ob M dadurch zum kommutativen Ring wird.

Übung

Wir betrachten $M = \mathbb{R} \times \mathbb{R}$ mit der Addition

$$(a,b)+(c,d)=(a+c,b+d)$$

und der Multiplikation

$$(a,b)\cdot(c,d)=(ac,ad+bc)$$

Überprüfen Sie, ob M dadurch zum kommutativen Ring wird.

Lösung:

 $(M, +, \cdot)$ ist ein kommutativer Ring.



Übung

Wir betrachten $M = \mathbb{R} \times \mathbb{R}$ mit der Addition

$$(a,b)+(c,d)=(a+c,b+d)$$

und der Multiplikation

$$(a,b)\cdot(c,d)=(ac,ad+bc)$$

Uberprüfen Sie, ob M dadurch zum kommutativen Ring wird.

Lösung:

 $(M, +, \cdot)$ ist ein kommutativer Ring.



Definition

Es sei $(R, +, \cdot)$ ein kommutativer Ring. Ein Element $r \in R \setminus \{0\}$ heißt **Nullteiler** von R wenn es ein $s \in R \setminus \{0\}$ gibt mit $r \cdot s = 0$. Ein kommutativer Ring, in dem es keine Nullteiler gibt, heißt **nullteilerfrei** oder **Integritätsbereich**

Definition

Es sei $(R,+,\cdot)$ ein kommutativer Ring. Ein Element $r\in R\setminus\{0\}$ heißt **Nullteiler** von R wenn es ein $s\in R\setminus\{0\}$ gibt mit $r\cdot s=0$. Ein kommutativer Ring, in dem es keine Nullteiler gibt, heißt **nullteilerfrei** oder **Integritätsbereich**

Beispiel

Die Ringe \mathbb{R} , \mathbb{Q} und \mathbb{Z} sind nullteilerfrei.

Definition

Es sei $(R,+,\cdot)$ ein kommutativer Ring. Ein Element $r\in R\setminus\{0\}$ heißt **Nullteiler** von R wenn es ein $s\in R\setminus\{0\}$ gibt mit $r\cdot s=0$. Ein kommutativer Ring, in dem es keine Nullteiler gibt, heißt **nullteilerfrei** oder **Integritätsbereich**

Beispiel

Die Ringe \mathbb{R} , \mathbb{Q} und \mathbb{Z} sind nullteilerfrei.

Beispiel

Die Ringe $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind nullteilerfrei.

Definition

Es sei $(R,+,\cdot)$ ein kommutativer Ring. Ein Element $r\in R\setminus\{0\}$ heißt **Nullteiler** von R wenn es ein $s\in R\setminus\{0\}$ gibt mit $r\cdot s=0$. Ein kommutativer Ring, in dem es keine Nullteiler gibt, heißt **nullteilerfrei** oder **Integritätsbereich**

Beispiel

Die Ringe \mathbb{R} , \mathbb{Q} und \mathbb{Z} sind nullteilerfrei.

Beispiel

Die Ringe $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind nullteilerfrei.

Beispiel

Dre Ring $M = \mathbb{R} \times \mathbb{R}$ von oben ist nicht nullteilerfrei.

Definition

Es sei $(R,+,\cdot)$ ein kommutativer Ring. Ein Element $r\in R\setminus\{0\}$ heißt **Nullteiler** von R wenn es ein $s\in R\setminus\{0\}$ gibt mit $r\cdot s=0$. Ein kommutativer Ring, in dem es keine Nullteiler gibt, heißt **nullteilerfrei** oder **Integritätsbereich**

Beispiel

Die Ringe \mathbb{R} , \mathbb{Q} und \mathbb{Z} sind nullteilerfrei.

Beispiel

Die Ringe $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind nullteilerfrei.

Beispiel

Dre Ring $M = \mathbb{R} \times \mathbb{R}$ von oben ist nicht nullteilerfrei.

Übung

Überprüfen Sie, ob der Ring $\mathbb{Z}/6\mathbb{Z}$ nullteilerfrei ist.

Lösung:

Der Ring ist nicht nullteilerfrei, denn es gilt

$$[2] \cdot [3] = [0]$$

und $[2] \neq [0]$, $[3] \neq [0]$.



Definition

Ein Körper $(K, +, \cdot)$ ist eine nichtleere Menge K mit zwei Verknüpfungen + und \cdot , die zwei Elemente 0, 1 enthält, wobei $0 \neq 1$ ist und wobei gilt (K, +, 0) ist eine kommutative Gruppe.

Definition

Ein **Körper** $(K,+,\cdot)$ ist eine nichtleere Menge K mit zwei Verknüpfungen + und \cdot , die zwei Elemente 0,1 enthält, wobei $0 \neq 1$ ist und wobei gilt

- (K, +, 0) ist eine kommutative Gruppe.
- $(K \setminus \{0\}, \cdot, 1)$ ist eine kommutative Gruppe.

Definition

Ein **Körper** $(K,+,\cdot)$ ist eine nichtleere Menge K mit zwei Verknüpfungen + und \cdot , die zwei Elemente 0,1 enthält, wobei $0 \neq 1$ ist und wobei gilt

- (K, +, 0) ist eine kommutative Gruppe.
- \bullet ($K \setminus \{0\}, \cdot, 1$) ist eine kommutative Gruppe.
- Es gilt das Distributivgesetz

$$(r+s) \cdot t = r \cdot t + s \cdot t$$
 für alle $r, s, t \in R$

Definition

Ein **Körper** $(K,+,\cdot)$ ist eine nichtleere Menge K mit zwei Verknüpfungen + und \cdot , die zwei Elemente 0,1 enthält, wobei $0 \neq 1$ ist und wobei gilt

- (K, +, 0) ist eine kommutative Gruppe.
- $(K \setminus \{0\}, \cdot, 1)$ ist eine kommutative Gruppe.
- Es gilt das Distributivgesetz

$$(r+s) \cdot t = r \cdot t + s \cdot t$$
 für alle $r, s, t \in R$

Beispie

 $(\mathbb{R},+,\cdot)$ und $(\mathbb{Q},+,\cdot)$ sind Körper.



Definition

Ein **Körper** $(K,+,\cdot)$ ist eine nichtleere Menge K mit zwei Verknüpfungen + und \cdot , die zwei Elemente 0,1 enthält, wobei $0 \neq 1$ ist und wobei gilt

- (K, +, 0) ist eine kommutative Gruppe.
- $(K \setminus \{0\}, \cdot, 1)$ ist eine kommutative Gruppe.
- Es gilt das Distributivgesetz

$$(r+s) \cdot t = r \cdot t + s \cdot t$$
 für alle $r, s, t \in R$

Beispiel

 $(\mathbb{R},+,\cdot)$ und $(\mathbb{Q},+,\cdot)$ sind Körper.

Beispie

 $(\mathbb{Z},+,\cdot)$ ist kein Körper.

Definition

Ein **Körper** $(K, +, \cdot)$ ist eine nichtleere Menge K mit zwei Verknüpfungen + und \cdot , die zwei Elemente 0, 1 enthält, wobei $0 \neq 1$ ist und wobei gilt

- (K, +, 0) ist eine kommutative Gruppe.
- $(K \setminus \{0\}, \cdot, 1)$ ist eine kommutative Gruppe.
- Es gilt das Distributivgesetz

$$(r+s) \cdot t = r \cdot t + s \cdot t$$
 für alle $r, s, t \in R$

Beispiel

 $(\mathbb{R},+,\cdot)$ und $(\mathbb{Q},+,\cdot)$ sind Körper.

Beispiel

 $(\mathbb{Z},+,\cdot)$ ist kein Körper.

Bemerkung

Jeder Körper ist ein nullteilerfreier kommutativer Ring. Die Umkehrung gilt nicht.

Ein nullteilerfreier kommutativer Ring R ist erst dann ein Körper, wenn es zu jedem $x \in R$ ein inverses Element gibt, also ein Element $y \in R$ mit $x \cdot y = 1$.

Bemerkung

Jeder Körper ist ein nullteilerfreier kommutativer Ring. Die Umkehrung gilt nicht.

Ein nullteilerfreier kommutativer Ring R ist erst dann ein Körper, wenn es zu jedem $x \in R$ ein inverses Element gibt, also ein Element $y \in R$ mit $x \cdot y = 1$.

Beispiel

Die Ringe $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind Körper.



Bemerkung

Jeder Körper ist ein nullteilerfreier kommutativer Ring. Die Umkehrung gilt nicht.

Ein nullteilerfreier kommutativer Ring R ist erst dann ein Körper, wenn es zu jedem $x \in R$ ein inverses Element gibt, also ein Element $y \in R$ mit $x \cdot y = 1$.

Beispiel

Die Ringe $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind Körper.

Beispie

Der Ring $\mathbb{Z}/6\mathbb{Z}$ ist kein Körper.



Bemerkung

Jeder Körper ist ein nullteilerfreier kommutativer Ring. Die Umkehrung gilt nicht

Ein nullteilerfreier kommutativer Ring R ist erst dann ein Körper, wenn es zu jedem $x \in R$ ein inverses Element gibt, also ein Element $y \in R$ mit $x \cdot y = 1$.

Beispiel

Die Ringe $\mathbb{Z}/2\mathbb{Z}$ und $\mathbb{Z}/3\mathbb{Z}$ sind Körper.

Beispiel

Der Ring $\mathbb{Z}/6\mathbb{Z}$ ist kein Körper.



Übung

Überprüfen Sie, ob der Ring $\mathbb{Z}/15\mathbb{Z}$ ein Körper ist.



Übung

Überprüfen Sie, ob der Ring $\mathbb{Z}/15\mathbb{Z}$ ein Körper ist.

Dieser Ring ist kein Körper, denn er ist nicht nullteilerfrei.



Übung

Überprüfen Sie, ob der Ring $\mathbb{Z}/15\mathbb{Z}$ ein Körper ist.

Lösung:

Dieser Ring ist kein Körper, denn er ist nicht nullteilerfrei.

Bemerkung

Ist $(R,+,\cdot)$ ein kommutativer Ring, so heißt ein $r\in R$ **Einheit**, wenn es ein $s\in R$ gibt mit $r\cdot s=1$. Die Einheiten von R bilden eine Gruppe (bezüglich \cdot), die **Einheitengruppe** E(R) von R.

Regel

Ein kommutativer Ring R ist genau dann ein Körper, wenn $E(R) = R \setminus \{0\}.$



Bemerkung

Ist $(R, +, \cdot)$ ein kommutativer Ring, so heißt ein $r \in R$ **Einheit**, wenn es ein $s \in R$ gibt mit $r \cdot s = 1$. Die Einheiten von R bilden eine Gruppe (bezüglich \cdot), die **Einheitengruppe** E(R) von R.

Regel

Ein kommutativer Ring R ist genau dann ein Körper, wenn $E(R) = R \setminus \{0\}.$

Beispiel

Der Polynomoring $\mathbb{R}[X]$ ist kein Körper.



Bemerkung

Ist $(R, +, \cdot)$ ein kommutativer Ring, so heißt ein $r \in R$ **Einheit**, wenn es ein $s \in R$ gibt mit $r \cdot s = 1$. Die Einheiten von R bilden eine Gruppe (bezüglich \cdot), die **Einheitengruppe** E(R) von R.

Regel

Ein kommutativer Ring R ist genau dann ein Körper, wenn $E(R) = R \setminus \{0\}.$

Beispiel

Der Polynomoring $\mathbb{R}[X]$ ist kein Körper.



Der Körper $\mathbb C$ der komplexen Zahlen ist ein Erweiterungskörper von $\mathbb R$, der wie folgt konstruiert wird:

Wir definieren \mathbb{C} als die Menge alle Zahlenpaare $(x,y) \in \mathbb{R}^2$ und mit der folgenden Addtion und Multiplikation.

Der Körper $\mathbb C$ der komplexen Zahlen ist ein Erweiterungskörper von $\mathbb R$, der wie folgt konstruiert wird:

Wir definieren \mathbb{C} als die Menge alle Zahlenpaare $(x,y) \in \mathbb{R}^2$ und mit der folgenden Addtion und Multiplikation.

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

Der Körper $\mathbb C$ der komplexen Zahlen ist ein Erweiterungskörper von $\mathbb R$, der wie folgt konstruiert wird:

Wir definieren \mathbb{C} als die Menge alle Zahlenpaare $(x,y) \in \mathbb{R}^2$ und mit der folgenden Addtion und Multiplikation.

- $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$
- $(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2 y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1).$



Der Körper $\mathbb C$ der komplexen Zahlen ist ein Erweiterungskörper von $\mathbb R$, der wie folgt konstruiert wird:

Wir definieren \mathbb{C} als die Menge alle Zahlenpaare $(x,y) \in \mathbb{R}^2$ und mit der folgenden Addtion und Multiplikation.

•
$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1).$$

Wir benutzen die folgende Notation:

$$0 = (0,0)$$
 (das Nullelement).
 $1 = (1,0)$ (das Einselement).
 $i = (0,1)$.
 $(x,y) = x + i \cdot y$.

Der Körper $\mathbb C$ der komplexen Zahlen ist ein Erweiterungskörper von $\mathbb R$, der wie folgt konstruiert wird:

Wir definieren \mathbb{C} als die Menge alle Zahlenpaare $(x,y) \in \mathbb{R}^2$ und mit der folgenden Addtion und Multiplikation.

$$(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2).$$

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 \cdot x_2 - y_1 \cdot y_2, x_1 \cdot y_2 + x_2 \cdot y_1).$$

Wir benutzen die folgende Notation:

$$0 = (0,0)$$
 (das Nullelement).

$$1 = (1,0)$$
 (das Einselement).

$$i = (0, 1).$$

$$(x, y) = x + i \cdot y.$$



Addition und Multiplikation der komplexen Zahlen schreiben sich damit wie folgt

•
$$(x_1 + i \cdot y_1) + (x_2 + i \cdot y_2) = (x_1 + x_2 + i \cdot (y_1 + y_2).$$

Addition und Multiplikation der komplexen Zahlen schreiben sich damit wie folgt

- $(x_1 + i \cdot y_1) + (x_2 + i \cdot y_2) = (x_1 + x_2 + i \cdot (y_1 + y_2).$
- $(x_1 + i \cdot y_1) \cdot (x_2 + i \cdot y_2) = x_1 \cdot x_2 y_1 \cdot y_2 + i \cdot (x_1 \cdot y_2 + x_2 \cdot y_1).$

Satz (Der Körper der komplexen Zahlen

Die komplexen Zahlen $\mathbb C$ zusammen mit dieser Addition und Multiplikation bilden einen Körper.

Addition und Multiplikation der komplexen Zahlen schreiben sich damit wie folgt

- $(x_1 + i \cdot y_1) + (x_2 + i \cdot y_2) = (x_1 + x_2 + i \cdot (y_1 + y_2).$
- $(x_1 + i \cdot y_1) \cdot (x_2 + i \cdot y_2) = x_1 \cdot x_2 y_1 \cdot y_2 + i \cdot (x_1 \cdot y_2 + x_2 \cdot y_1).$

Satz (Der Körper der komplexen Zahlen)

Die komplexen Zahlen $\mathbb C$ zusammen mit dieser Addition und Multiplikation bilden einen Körper.

Das inverse Element $\frac{1}{z}$ zu einer komplexen Zahl $z = x + i \cdot y \neq 0$ ist gegeben durch

$$\frac{1}{z} = \frac{x - i \cdot y}{x^2 + y^2}$$

das Nullelement bezüglich der Addition ist $0=0+i\cdot 0$, das Einselemnet bezüglich der Multiplikation ist $1=1+i\cdot 0$.

Addition und Multiplikation der komplexen Zahlen schreiben sich damit wie folgt

- $(x_1 + i \cdot y_1) + (x_2 + i \cdot y_2) = (x_1 + x_2 + i \cdot (y_1 + y_2).$
- $(x_1 + i \cdot y_1) \cdot (x_2 + i \cdot y_2) = x_1 \cdot x_2 y_1 \cdot y_2 + i \cdot (x_1 \cdot y_2 + x_2 \cdot y_1).$

Satz (Der Körper der komplexen Zahlen)

Die komplexen Zahlen $\mathbb C$ zusammen mit dieser Addition und Multiplikation bilden einen Körper.

Das inverse Element $\frac{1}{z}$ zu einer komplexen Zahl $z = x + i \cdot y \neq 0$ ist gegeben durch

$$\frac{1}{z} = \frac{x - i \cdot y}{x^2 + y^2}$$

das Nullelement bezüglich der Addition ist $0=0+i\cdot 0$, das Einselemnet bezüglich der Multiplikation ist $1=1+i\cdot 0$.

Bezeichnung

Ist $z = x + i \cdot y$ eine komplexe Zahl, so heißt x der **Realteil** von z und wird mit $\operatorname{Re}(z)$ bezeichnet und y der **Imaginärteil** von z und wird mit $\operatorname{Im}(z)$ bezeichnet.

Die Zahl $\overline{z} = x - i \cdot y$ heißt die zu z komplex konjugierte Zahl, und

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

heißt der Betrag von z.

Bezeichnung

Ist $z = x + i \cdot y$ eine komplexe Zahl, so heißt x der **Realteil** von z und wird mit $\operatorname{Re}(z)$ bezeichnet und y der **Imaginärteil** von z und wird mit $\operatorname{Im}(z)$ bezeichnet.

Die Zahl $\overline{z} = x - i \cdot y$ heißt die zu z komplex konjugierte Zahl, und

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

heißt der Betrag von z.

Beispiel

 \bullet $i \cdot i = -1$

Bezeichnung

Ist $z = x + i \cdot y$ eine komplexe Zahl, so heißt x der **Realteil** von z und wird mit $\operatorname{Re}(z)$ bezeichnet und y der **Imaginärteil** von z und wird mit $\operatorname{Im}(z)$ bezeichnet.

Die Zahl $\overline{z} = x - i \cdot y$ heißt die zu z komplex konjugierte Zahl, und

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

heißt der Betrag von z.

- \bullet i·i = -1.
- $(2+3 \cdot i) \cdot (1-i) = 5+i$.

Bezeichnung

Ist $z = x + i \cdot y$ eine komplexe Zahl, so heißt x der **Realteil** von z und wird mit $\operatorname{Re}(z)$ bezeichnet und y der **Imaginärteil** von z und wird mit $\operatorname{Im}(z)$ bezeichnet.

Die Zahl $\overline{z} = x - i \cdot y$ heißt die zu z komplex konjugierte Zahl, und

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

heißt der Betrag von z.

- $\mathbf{i} \cdot \mathbf{i} = -1$.
- $(2+3 \cdot i) \cdot (1-i) = 5+i$.
- $\frac{1}{2+i} = \frac{2}{5} \frac{1}{5} \cdot i.$

Bezeichnung

Ist $z = x + i \cdot y$ eine komplexe Zahl, so heißt x der **Realteil** von z und wird mit $\operatorname{Re}(z)$ bezeichnet und y der **Imaginärteil** von z und wird mit $\operatorname{Im}(z)$ bezeichnet.

Die Zahl $\overline{z} = x - i \cdot y$ heißt die zu z komplex konjugierte Zahl, und

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

heißt der Betrag von z.

- $\mathbf{i} \cdot \mathbf{i} = -1$.
- $(2+3 \cdot i) \cdot (1-i) = 5+i$.
- $\frac{1}{2+i} = \frac{2}{5} \frac{1}{5} \cdot i$.
- $\frac{1+i}{2+i} = \frac{3}{5} + \frac{1}{5} \cdot i$.

Bezeichnung

Ist $z = x + i \cdot y$ eine komplexe Zahl, so heißt x der **Realteil** von z und wird mit $\operatorname{Re}(z)$ bezeichnet und y der **Imaginärteil** von z und wird mit $\operatorname{Im}(z)$ bezeichnet.

Die Zahl $\overline{z} = x - i \cdot y$ heißt die zu z komplex konjugierte Zahl, und

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

heißt der Betrag von z.

- $\mathbf{i} \cdot \mathbf{i} = -1$.
- $(2+3 \cdot i) \cdot (1-i) = 5+i$.
- $\frac{1}{2+i} = \frac{2}{5} \frac{1}{5} \cdot i$.
- $\frac{1+i}{2+i} = \frac{3}{5} + \frac{1}{5} \cdot i$.

Übung

Berechnen Sie

$$z = \frac{2 + 3 \cdot i}{1 - i}$$

Übung

Berechnen Sie

$$z = \frac{2 + 3 \cdot i}{1 - i}$$

$$z = \frac{-1+5 \cdot i}{2} = -\frac{1}{2} + \frac{5}{2} \cdot i$$

Übung

Berechnen Sie

$$z = \frac{2 + 3 \cdot i}{1 - i}$$

$$z = \frac{-1+5 \cdot i}{2} = -\frac{1}{2} + \frac{5}{2} \cdot i$$

Es gilt $i \cdot i = -1$, und damit für jede positive reelle Zahl r:

$$(i \cdot \sqrt{r})^2 = i^2 \cdot \sqrt{r}^2 = -1$$

dh.in den komplexen Zahlen hat jede reelle Zahl eine Quadratwurzel. Es gilt sogar noch mehr:

Satz (Fundamentalsatz der Algebra)

Der Körper C ist algebraisch abgeschlossen, dh. jede Gleichung

$$a_n \cdot x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$$

vom Grad $n \geq 1$ mit $a_l \in \mathbb{C}$ hat eine Lösung, dh. es gibt ein $z_0 \in \mathbb{C}$ mit

$$a_n \cdot z_0^n + a_{n-1} z_0^{n-1} + \dots + a_1 z_0 + a_0 = 0$$



Es gilt $i \cdot i = -1$, und damit für jede positive reelle Zahl r:

$$(i \cdot \sqrt{r})^2 = i^2 \cdot \sqrt{r}^2 = -1$$

dh.in den komplexen Zahlen hat jede reelle Zahl eine Quadratwurzel. Es gilt sogar noch mehr:

Satz (Fundamentalsatz der Algebra)

Der Körper $\mathbb C$ ist algebraisch abgeschlossen, dh. jede Gleichung

$$a_n \cdot x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 = 0$$

vom Grad $n \geq 1$ mit $a_l \in \mathbb{C}$ hat eine Lösung, dh. es gibt ein $z_0 \in \mathbb{C}$ mit

$$a_n \cdot z_0^n + a_{n-1} z_0^{n-1} + \dots + a_1 z_0 + a_0 = 0$$



Beispiel

Es ist

$$\sqrt{-16} = 4 \cdot i$$

und daher hat die Gleichung

$$x^2 + 2x + 5 = 0$$

$$x_{1,2} = \frac{-2 \pm \sqrt{2^2 - 4 \cdot 5}}{2} = \frac{-2 \pm \sqrt{-16}}{2} = \frac{-2 \pm 4 \cdot \mathrm{i}}{2}$$

Beispiel

Es ist

$$\sqrt{-16} = 4 \cdot i$$

und daher hat die Gleichung

$$x^2 + 2x + 5 = 0$$

die beiden Lösungen

$$x_{1,2} = \frac{-2 \pm \sqrt{2^2 - 4 \cdot 5}}{2} = \frac{-2 \pm \sqrt{-16}}{2} = \frac{-2 \pm 4 \cdot i}{2}$$

also

$$x_1 = -1 + 2 \cdot i$$
, $x_2 = -1 - 2 \cdot i$

Beispiel

Es ist

$$\sqrt{-16} = 4 \cdot i$$

und daher hat die Gleichung

$$x^2 + 2x + 5 = 0$$

die beiden Lösungen

$$x_{1,2} = \frac{-2 \pm \sqrt{2^2 - 4 \cdot 5}}{2} = \frac{-2 \pm \sqrt{-16}}{2} = \frac{-2 \pm 4 \cdot i}{2}$$

also

$$x_1 = -1 + 2 \cdot i, \qquad x_2 = -1 - 2 \cdot i$$

Übung

Bestimmen Sie die Lösungen der Gleichung

$$2x^2 - 8x + 10 = 0$$

Übung

Bestimmen Sie die Lösungen der Gleichung

$$2x^2 - 8x + 10 = 0$$

$$x_1 = 2 + i$$
, $x_2 = 2 - i$.

Übung

Bestimmen Sie die Lösungen der Gleichung

$$2x^2 - 8x + 10 = 0$$

$$x_1 = 2 + i$$
, $x_2 = 2 - i$.