

Wiederholung

- Verknüpfungen auf Menge M : $\cdot : M \times M \rightarrow M$
- (M, \cdot) Monoid, falls Assoziativgesetz
 - assoziativ, d.h. $\forall x, y, z \in M : (AG) \quad x(yz) = (xy)z$
 - $\exists NE \quad e$, d.h. $\forall x \in M$:
neutrales Element $ex = x = xe$
- $x \in M$, $y \in M$ invers zu x : $\Leftrightarrow xy = e = yx$

Inverse sind, falls existent, eindeutig:

Inverse zu x : x^{-1} (bei additiver Schreibweise: $-x$)

~~Wiederholung~~ $x^n := x \cdot x \cdot \dots \cdot x$ (n Faktoren), $n \in \mathbb{N}$ [$x^0 := e$]

- (M, \cdot) abelsch, falls kommutativ, d.h. $\forall x, y \in M: xy = yx$
In diesem Fall oft: $+$ für das Verknüpfungszeichen

• A Menge: $(A^*, *)$ Wort monoid

Elemente: Wörter über A , $a_1 \dots a_n$, $a_i \in A$

Verknüpf. $(a_1 \dots a_n) * (b_1 \dots b_m) = a_1 a_2 \dots a_n b_1 \dots b_m$

ϵ leere Wort
 NE

• M Menge $(A \text{ bb } (M, M), \circ), id_M$

• M^* : Menge der invertierbaren Elemente

$$x, y \in M^* \Rightarrow xy \in M^* \text{ und } (xy)^{-1} = y^{-1} x^{-1}$$

$$x \in M^* \Rightarrow x^{-1} \in M^* \text{ und } (x^{-1})^{-1} = x$$

$$1 \in M^* \Rightarrow 1^{-1} = 1$$

• (G, \cdot) Gruppe, falls (G, \cdot) Monoid, und

$$G^* = G, \text{ d.h. für alle } x \in G, \text{ ex. } y \in G: xy = e = yx.$$

Gruppe der invertierbaren Elemente

Definition

M Monoid

Einheitengruppe von M

(oder *Gruppe der invertierbaren Elemente*):

Gruppe M^\times mit Multiplikation gegeben durch diejenige von M .

Beispiel

► $(\mathbb{Z}, \cdot)^\times = \{1, -1\}$

► $(\mathbb{Q}, \cdot)^\times = \mathbb{Q} \setminus \{0\}$

► A Menge:

$S_A := \text{Abb}(A, A)^\times$, die *symmetrische Gruppe auf A* .

$S_A = \{f \in \text{Abb}(A, A) \mid f \text{ ist invertierbar}\}.$

Untergruppen

Definition

G Gruppe, $U \subseteq G$.

U heißt *Untergruppe* von G , falls gilt:

(a) $\triangleright e \in U$.

U

(b) \triangleright Für alle $x, y \in U$ ist auch $x \cdot y^{-1} \in U$.

U ist abgeschlossen bzgl. \cdot und Invertieren

(b) Ist äquivalent zu: [(b1) und (b2)]

(b1) Für alle $x, y \in U$ ist $x \cdot y \in U$

(b2) Für alle $x \in U$ ist $x^{-1} \in U$

Untergruppen (Forts.)

Beispiele

(a) ► Für $n \in \mathbb{Z}$ ist $(\mathbb{Z}, +)$

$$n\mathbb{Z} := \{nz \mid z \in \mathbb{Z}\} \quad \text{Vielfachenmenge}$$

eine Untergruppe von $(\mathbb{Z}, +)$.

Z.B. ist

- $2\mathbb{Z}$ die Menge der geraden Zahlen.
- $0\mathbb{Z} = \{0\}$.
- $1\mathbb{Z} = \mathbb{Z}$.

(b) ► Sei A eine Menge und $a \in A$. Dann ist

$$S_{A,a} := \{f \in S_A \mid f(a) = a\}$$

eine Untergruppe von S_A .

- $(\mathbb{N}, +)$ ist keine Untergruppe von $(\mathbb{Z}, +)$.

Beweis von (a): NE: $e = 0$

• $0 \in n\mathbb{Z}$ ✓ Weil $0 = n \cdot 0$

• Seien $nx, ny \in n\mathbb{Z}$ ($x, y \in \mathbb{Z}$)

Zu zeigen: $nx + (-ny) \in n\mathbb{Z}$

Klar: $nx + (-ny) = n(x + (-y))$ DG: Distributivgesetz ✓

Beweis von (b):

- $\text{id}_M \in S_{A,a}$: Klar, da $\text{id}_M(a) = a$ ✓
- Seien $f, g \in S_{A,a}$. Zu zeigen: $f \circ g^{-1} \in S_{A,a}$.

Zeige zuerst: $g^{-1}(a) = a$.

Dann: $a = g(a) \Rightarrow g^{-1}(a) = g^{-1}(g(a)) = a$ ✓

Damit: $(f \circ g^{-1})(a) = f(g^{-1}(a)) = f(a) = a$ ✓ □

Ringe und Körper

Definition

Ring: Menge R mit zwei Verknüpfungen $+$ und \cdot , so dass gilt:

- ▶ $(R, +)$ abelsche Gruppe $\forall x \in R \text{ bzgl. } + : 0, \exists x: -x$
- ▶ (R, \cdot) Monoid $\forall x \in R \text{ bzgl. } \cdot : 1$
- ▶ für alle $x, y, z \in R$ gilt:

$$\left. \begin{array}{l} x \cdot (y + z) = (x \cdot y) + (x \cdot z) \\ (x + y) \cdot z = (x \cdot z) + (y \cdot z) \end{array} \right\}$$

Die letzten beiden Axiome heißen die *Distributivgesetze*.

DG

Ringe und Körper (Forts.)

- ▶ R Ring

R kommutativ: \cdot kommutativ

- ▶ K Körper: kommutativer Ring K mit

- ▶ $1 \neq 0$

- ▶ jedes Element von $K \setminus \{0\}$ ist invertierbar, d.h. $K^\times = K \setminus \{0\}$

Beispiel: $R = \{0\}$ ist Ring mit $1=0$

Ringe und Körper (Forts.)

Beispiele

► \mathbb{Z} mit üblicher Addition und Multiplikation: *Komm. Ring*

► \mathbb{Q} mit üblicher Addition und Multiplikation: *Körper*

► \mathbb{R}, \mathbb{C} ———— : *Körper*

Ringe und Körper (Forts.)

Beispiel

Körper mit genau zwei Elementen: $\mathbb{F}_2 = \{0, 1\}$

xor	+	0	1
	0	0	1
	1	1	0

1 .	.	0	1
	0	0	0
	1	0	1

$$1 = -1$$

$$1+1 = 0$$

Ringe und Körper (Forts.)

Beispiel

Die Menge $\mathbb{F}_4 := \{0, 1, a, b\}$ mit den Verknüpfungstabellen

+	0	1	a	b
0	0	1	a	b
1	1	0	b	a
a	a	b	0	1
b	b	a	1	0

·	0	1	a	b
0	0	0	0	0
1	0	1	a	b
a	0	a	b	1
b	0	b	1	a

bildet einen Körper.

Es gilt: Ist $q := p^f$ eine Primzahlpotenz (d.h. p Primzahl),
dann ex. Körper \mathbb{F}_q mit genau q Elementen, z.B. \mathbb{F}_2 .

Ringe und Körper (Forts.)

Proposition

R Ring

(a) ► für $a \in R$: $a \cdot 0 = 0 \cdot a = 0$

(b) ► für $a, b \in R$: $a(-b) = (-a)b = -ab$

(c) ► für $a, b \in R$: $(-a)(-b) = ab$

Beweis: (a) $a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 + a \cdot 0$ | Addiere $-a \cdot 0$

$$\Rightarrow -a \cdot 0 + a \cdot 0 = -a \cdot 0 + a \cdot 0 + a \cdot 0$$

$$\Rightarrow 0 = a \cdot 0 \quad \checkmark$$

(b) $ab + a(-b) = a(b + (-b)) = a(b - b) = a \cdot 0 = 0 \quad \checkmark$

~~(a)~~ $\Rightarrow a(-b) = -ab$

(c) $(-a)(-b) \stackrel{(b)}{=} -((-a)b) \stackrel{(b)}{=} -(-ab) = ab \quad \checkmark$

Integritätsbereiche

Definition

R kommutativer Ring.

- ▶ $a \in R$ heißt *Nullteiler*, falls ein $0 \neq b \in R$ existiert mit $ab = 0$.
- ▶ R heißt *Integritätsbereich*, falls $1 \neq 0$ und R keine Nullteiler außer 0 besitzt
(d.h. für alle $a, b \in R$ gilt: $ab = 0 \Rightarrow a = 0$ oder $b = 0$).

Integritätsbereiche (Forts.)

Beispiel

Ring \mathbb{Z} ist Integritätsbereich

Beispiel

Kommutativer Ring mit genau vier Elementen und Nullteilern:

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

Integritätsbereiche (Forts.)

Proposition

Körper sind Integritätsbereiche.

Bemerkung


R kommutativer Ring mit $1 \neq 0$

Äquivalent sind:

(a) $\blacktriangleright R$ ist Integritätsbereich

(b) \blacktriangleright für $a, x, y \in R$: $ax = ay \Rightarrow a = 0$ oder $x = y$ Kürzungsregel

Beweis: (a) \Rightarrow (b): $ax = ay \Rightarrow a(x - y) = 0$
 $\Rightarrow a = 0$ oder $x - y = 0$
 $\Rightarrow a = 0$ oder $x = y$.

(b) \Rightarrow (a): $ab = 0 \Rightarrow ab = a \cdot 0$
 $\Rightarrow a = 0$ oder $b = 0$. 

Beh.: K Körper $\Rightarrow K$ Integritätsbereich

Bew.: • $1 \neq 0$ ✓

• Seien $a, b \in K$, $ab = 0$ z.z.: $a = 0$ oder $b = 0$.

Sei $a \neq 0$. (sonst fertig)

Mult. mit a^{-1} :

$$\underbrace{a^{-1}(ab)} = a^{-1} \cdot 0 = 0$$

$$(a^{-1}a)b = 1 \cdot b = b, \text{ d.h. } b = 0. \quad \square$$

Polynome

K Körper

Definition

- Polynom in der *Unbestimmten* X : Ausdruck der Form

$$f = \sum_{i=0}^n a_i X^i = a_0 \overset{\circ}{X} + a_1 X + \dots + a_n X^n$$

für ein $n \in \mathbb{N}_0$ mit $a_i \in K$ für $i = 0, \dots, n$ (*beliebig groß*)

- Die $a_i \in K$, $i = 0, \dots, n$ heißen die *Koeffizienten* von f .
- $K[X]$: Menge der Polynome über K in der Unbestimmten X .

Polynome (Forts.)

Bemerkung und Schreibweise

- Koeffizienten gleich 0 können beliebig hinzugefügt oder weggelassen werden.

$$f = \sum_{i=0}^n a_i X^i = a_0 + a_1 X + \dots + a_n X^n + 0X^{n+1} + \dots$$

- Der Kürze halber schreibt man:
 X^i statt $1X^i$, X statt X^1 , a_0 statt $a_0 X^0$,
 $-a_i X^i$ statt $+(-a_i)X^i$ und $0X^i$ lässt man weg.

Beispiel

$$2X^0 + (-1)X + 1X^2 + 0X^3 = 2 - X + X^2. \quad = \quad X^2 - X + 2$$

Polynome (Forts.)

Definitionen

Seien $f = \sum_{i=0}^n a_i X^i$ und $g = \sum_{i=0}^n b_i X^i$ in $K[X]$.

► $f = g :\Leftrightarrow a_i = b_i$ für alle $i = 0, \dots, n$. [Koeffizientenvergleich]

► f heißt das *Nullpolynom*, geschrieben $f = 0$, falls $a_i = 0$ für alle $i = 0, \dots, n$.

► Sei $f \neq 0$. Dann sei $\deg f := \max\{i \mid a_i \neq 0\}$.

$\deg f$ heißt der *Grad* von f . $\deg f = 0 \Leftrightarrow f = a_0 X^0, a_0 \neq 0$
 $\quad \quad \quad = a_0$

Konvention: $\deg 0 := -\infty$.

Polynome (Forts.)

Definitionen

Sei $f = \sum_{i=0}^n a_i X^i \in K[X]$.

- ▶ a_0 heißt der *konstante* oder *absolute Koeffizient* von f .
- ▶ Ist $\deg f = n \geq 0$, so heißt a_n der *Leitkoeffizient* oder *Hauptkoeffizient* von f . Insbesondere: $a_n \neq 0$.
- ▶ Das Polynom heißt *normiert*, wenn der Hauptkoeffizient gleich 1 ist.
- ▶ Das Polynom f heißt *linear*, wenn $\deg f = 1$, und *quadratisch*, wenn $\deg f = 2$ ist.
- ▶ Das Polynom f heißt *konstant*, wenn $\deg f \leq 0$ ist.

Polynome (Forts.)

Beispiele

- ▶ $f = -1 + X^2$
- ▶ $g = X + 2X^2 - X^3$

- ▶ $\deg f = 2$
- ▶ $\deg g = 3$
- ▶ Leitkoeffizient von f : 1
- ▶ Leitkoeffizient von g : -1
- ▶ Konstanter Koeffizient von f : -1
- ▶ Konstanter Koeffizient von g : 0
- ▶ f normiert? Ja
- ▶ g normiert? Nein (falls $1 \neq -1$)

Polynome (Forts.)

Notation

$$K^{(\mathbb{N}_0)} := \{(a_i) \in K^{\mathbb{N}_0} \mid a_i = 0 \text{ für fast alle } i \in \mathbb{N}_0\}.$$

(fast alle: alle, bis auf endlich viele.) $K^{\mathbb{N}_0}$: Menge der Folgen in K indiziert durch \mathbb{N}_0

Bemerkung

Das Polynom $f = \sum_{i=0}^n a_i X^i \in K[X]$ kann durch die Folge seiner Koeffizienten

$$(a_0, a_1, a_2, \dots, a_n, 0, 0, 0, \dots) \in K^{(\mathbb{N}_0)}$$

definiert werden (mathematisch präzise Definition von Polynom.)

Unbestimmte: $X = 1X = 1X^1 = (0, 1, 0, 0, 0, \dots)$.

Konstante Polynome: $a_0 X^0 = (a_0, 0, 0, 0, \dots)$.

Polynomfunktionen

Warnung

Polynome sind *keine* Funktionen

Sei $K = \mathbb{F}_2 = \{0, 1\}$:

- ▶ $\text{Abb}(K, K)$ endlich mit $|\text{Abb}(K, K)| = 4$
- ▶ $K[X]$ unendlich

<u>0, 1</u>	
0	0
0	1
1	0
1	1

Polynomfunktionen (Forts.)

Definition

$$f = \sum_{i=0}^n a_i X^i \in K[X].$$

Polynomfunktion zu f :

$$K \rightarrow K, x \mapsto \sum_{i=0}^n a_i x^i$$

Missbrauch der Notation: notiere Polynomfunktion auch als f

Für $x \in K$ heißt $f(x) \in K$ der *Wert von f an der Stelle x* .

Polynomfunktionen (Forts.)

Beispiele

- $f = -2 + X - \frac{1}{3}X^2 + X^4 \in \mathbb{Q}[X]$ liefert Polynomfunktion

$$f : \mathbb{Q} \rightarrow \mathbb{Q}, \quad a \mapsto -2 + a - \frac{1}{3}a^2 + a^4$$

$$f(5) = -2 + 5 - \frac{1}{3}25 + 625 = \frac{1859}{3}$$

- $f = X + X^2 \in \mathbb{F}_2[X]$

$$f(0) = 0 \qquad 0 + 0 \cdot 0 = 0$$

$$f(1) = 0 \qquad 1 + 1 \cdot 1 = 1 + 1 = 0$$

Hier liefern f und das Nullpolynom 0 die gleiche Polynomfunktion.