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:
  $S_A := \mathrm{Abb}(A, A)^\times$, die *symmetrische Gruppe auf* A.
  $S_A = \{f \in \mathrm{Abb}(A, A) \mid f \text{ ist invertierbar}\}$.

Untergruppen

Definition

G Gruppe, $U \subseteq G$.

U heißt *Untergruppe* von G, falls gilt:

- $e \in U$.
- Für alle $x, y \in G$ ist auch $x \cdot y^{-1} \in G$.

Untergruppen (Forts.)

Beispiele

- Für $n \in \mathbb{Z}$ ist

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

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

  Z.B. ist

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

- 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 $(\mathbb{Z}, +)$.

Ringe und Körper

Definition

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

- $(R, +)$ abelsche Gruppe
- $(R, \cdot)$ Monoid
- für alle $x, y, z \in R$ gilt:

$$x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$
$$(x + y) \cdot z = (x \cdot z) + (y \cdot z)$$

Die letzten beiden Axiome heißen die *Distributivgesetze*.

Ringe und Körper (Forts.)

- R Ring

  R *kommutativ*: $\quad\cdot$ kommutativ

- *Körper*: kommutativer Ring K mit
  - $1 \neq 0$
  - jedes Element von $K \setminus \{0\}$ ist invertierbar

Ringe und Körper (Forts.)

Beispiele

- $\mathbb{Z}$ mit üblicher Addition und Multiplikation:
- $\mathbb{Q}$ mit üblicher Addition und Multiplikation:

Ringe und Körper (Forts.)

Beispiel

Körper mit genau zwei Elementen:

$+$	0	1
0	0	1
1	1	0

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

Ringe und Körper (Forts.)

Beispiel

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

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

$\cdot$	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.

Ringe und Körper (Forts.)

Proposition

R Ring

- für $a \in R$: $a \cdot 0 = 0 \cdot a = 0$
- für $a, b \in R$: $a(-b) = (-a)b = -ab$
- für $a, b \in R$: $(-a)(-b) = ab$

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: $\quad ab = 0 \Rightarrow a = 0$ 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

$\cdot$	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:

- R ist Integritätsbereich
- für $a, x, y \in R$: $\quad ax = ay \Rightarrow a = 0$ oder $x = y$

Polynome

K Körper

Definition

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

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

für ein $n \in \mathbb{N}_0$ mit $a_i \in K$ für $i = 0, \ldots, n$..

- Die $a_i \in K$, $i = 0, \ldots, n$ 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.

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

- Der Kürze halber schreibt man:
  X^i statt $1X^i$, X statt X^1, a_0 statt a_0X^0,
  $-a_iX^i$ statt $+(-a_i)X^i$ und $0X^i$ lässt man weg.

Beispiel

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

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 $i = 0, \ldots, n$.
- f heißt das *Nullpolynom*, geschrieben $f = 0$, falls $a_i = 0$ für alle $i = 0, \ldots, n$.
- Sei $f \neq 0$. Dann sei $\deg f := \max\{i \mid a_i \neq 0\}$.

  $\deg f$ heißt der *Grad* von f.

  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.
- 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

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

- $\deg f =$
- $\deg g =$
- Leitkoeffizient von f:
- Leitkoeffizient von g:
- Konstanter Koeffizient von f:
- Konstanter Koeffizient von g:
- f normiert?
- g normiert?

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.)

Bemerkung

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

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

definiert werden (mathematisch präzise Definition von Polynom.)

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

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

Polynomfunktionen

Warnung

Polynome sind *keine* Funktionen

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

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

Polynomfunktionen (Forts.)

Definition

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

Polynomfunktion zu f:

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

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

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

$$f(5) =$$

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

$$f(0) =$$

$$f(1) =$$

Hier liefern f und das Nullpolynom 0 die gleiche Polynomfunktion.

Der Polynomring

Bemerkung

$K[X]$ wird zu einem kommutativen Ring mit Verknüpfungen Addition und Multiplikation wie folgt:

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

$$f + g := \sum_{i=0}^{\max\{n,m\}} (a_i + b_i) X^i,$$

$$f \cdot g := \sum_{i=0}^{n+m} c_i X^i \text{ mit } c_i := \sum_{k=0}^{i} a_k b_{i-k}$$

(insbesondere ist $c_0 =$ und $c_{n+m} =$).

NE bzgl. $+$: NE bzgl $\cdot$:

Der Polynomring (Forts.)

- K wird identifiziert mit $\{aX^0 \mid a \in K\} \subseteq K[X]$

  Missbrauch der Notation: für $a \in K$: notiere aX^0 als a

Beispiele

$f, g \in \mathbb{Q}[X]$, $f = X^2 - 1$, $g = -X^3 + 2X^2 + X + 1$

$$\begin{aligned} f + g &= -X^3 + 3X^2 + X \\ fg &= -X^5 + 2X^4 + 2X^3 - X^2 - X - 1 \\ -2f &= -2X^2 + 2 \end{aligned}$$

Der Polynomring (Forts.)

Bemerkung

$f, g \in K[X] \setminus \{0\}$

- $f + g \neq 0 \Rightarrow$

$$\deg(f+g) \leq \max\{\deg f, \deg g\}$$

  $f + g \neq 0$, $\deg f \neq \deg g \Rightarrow$

$$\deg(f+g) = \max\{\deg f, \deg g\}$$

- Es gilt $fg \neq 0$ und

$$\deg(fg) \quad = \deg f + \deg g$$

Grad eines Polynoms (Forts.)

Korollar
$K[X]^\times = K^\times$

Korollar
$K[X]$ ist Integritätsbereich