- Ring, $(R,+)$ abelsche Gruppe, $(R,\cdot)$ Monoid

$$\left.\begin{aligned} x(y+z) &= xy + xz \\ (x+y)z &= xz + yz \end{aligned}\right\} \quad \forall\, x,y,z \in R$$

Distributivgesetze

<u>kommutativer Ring</u>, falls $(R,\cdot)$ abelsch

- K Kp.: komm. Ring mit $1 \neq 0$ und $K^\times = K \setminus \{0\}$. ~~(1 ≠ 0)~~

- R Ring:
$$\left.\begin{aligned} a\cdot 0 &= 0 = 0\cdot a \\ a\cdot(-b) &= -(ab) = (-a)b \\ (-a)(-b) &= ab \end{aligned}\right\} \quad \forall\, a,b \in R$$

- R komm. Ring heißt <u>Integritätsbereich</u>, falls $1 \neq 0$ und $\forall\, a,b \in R$ gilt: $ab = 0 \Rightarrow a = 0$ oder $b = 0$.

- Beispiel: $\mathbb{R} \times \mathbb{R}$ mit ~~komp. Add~~
komponentenweiser Add. u. Mult.

$$(x,y) \overset{+}{\cdot} (x',y') := (x \overset{+}{\cdot} x', y \overset{+}{\cdot} y')$$ komm. Ring

Nullel. $(0,0)$, Einsel. $(1,1)$

Aber $(0,1) \cdot (1,0) = (0,0)$.

- K Kp., $K[X]$ Menge der Polynome über K in Unbestimmter X

$$f = \sum_{i=0}^{n} a_i X^i = \underbrace{a_0 X^0}_{} + \dots + a_n X^n, \quad a_i \in K$$

a_0, $a_1 X^1 = a_1 X$

Koeff. von f

a_0 konstanter Koeff. von f.

$\deg f := \max\{i \mid a_i \neq 0\}$ falls $f \neq 0$, $\deg 0 = -\infty$

$n = \deg f$, a_n Leitkoeff. von f

f normiert, falls — " ——— $= 1$.

f linear, (quadratisch), falls $\deg f = 1$ ($\deg f = 2$).

- Polynomfunktion zu f: $K \to K$

$$x \mapsto f(x) := \sum_{i=0}^{n} a_i x^i$$ Konvention ($x^0 = 1 \ \forall x \in K$)

Insbesondere: Ist $\deg f = 0$, d.h. $f = a_0 X^0 = a_0$ für ein $a_0 \in K \setminus \{0\}$, dann ist $f(x) = a_0 \ \forall x \in K$.

Der Polynomring (Forts.)

Kopie von K in K[X]

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

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

$$(-X^3+2X^2+X+1)(X^2-1) = -X^5+2X^4+X^3+X^2$$
$$+X^3-2X^2-X-1$$
$$= -X^5+2X^4+2X^3-X^2-X-1$$

Beispiele

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

$$f + g = -X^3 + 3X^2 + X$$
$$fg = -X^5 + 2X^4 + 2X^3 - X^2 - X - 1$$
$$-2f = -2X^2 + 2$$

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 $c_0 = a_0 b_0$ und $c_{n+m} = a_n b_m$).

NE bzgl. $+$: 0 Nullpolynom NE bzgl $\cdot$: $1 = 1 X^0$.

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

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

Grad eines Polynoms (Forts.)

(1) **Korollar**
$K[X]^\times = K^\times$

(2) **Korollar**
$K[X]$ ist Integritätsbereich

<u>Beweis von (1),(2)</u>: Sei $f \in K[X]^\times$. Dann ex. $g \in K[X]$ mit $f \cdot g = 1$.

$\Rightarrow f \cdot g \neq 0$ und $\deg f + \deg g = \deg 1 = 0$

$\Rightarrow \deg f = 0 = \deg g$, d.h. $f \in K^\times$.

<u>Beweis von (2)</u>: ~~Sei $f \in K[X]$, $g \in K[X]$ mit $f \cdot g$~~ $= 0$

~~Wäre $f \neq 0$, L.k. $f = a_n$, $g \neq 0$ L.k. $g = b_m$~~, da

Teilbarkeit

R kommutativer Ring

Definition

$a, b \in R$

$$a \mid b \quad :\Leftrightarrow \quad a \text{ teilt } b$$

(oder b ist <u>Vielfaches von a</u>)

$$:\Leftrightarrow \quad \text{es gibt } q \in R: \quad b = qa$$

Beispiele

- $R = \mathbb{Z}$:
  - $3 \mid 6$
  - $4 \nmid 6$
- $R = Rationals[X]$:
  - $X - 1 \mid X^2 - 1$
  - $X \nmid X^2 - 1$ ⊗

$$X^2 - 1 = (X-1)(X+1)$$

⊗ Sei $f = \sum_{i=0}^{n} a_i X^i$

$$\Rightarrow X f = \sum_{i=0}^{n} a_i X^{i+1}$$

hat konst. ~~Ter~~ Koeff. 0.

Teilbarkeit (Forts.)

R kommutativer Ring

Präordnung: reflexiv $a \mid a$ OK für $q=1$

transitiv: $a \mid b$ und $b \mid c \Rightarrow a \mid c$

$b = q_1 a$, $c = q_2 b \Rightarrow c = q_2 b = (q_2 q_1) a$ ✓

Proposition

$\mid$ ist Präordnung auf R

Proposition

- (a) für $a, b, c \in R$: $a \mid b$ und $a \mid c \Rightarrow a \mid b + c$
- (b) für $a \in R$: $a \mid 0$
- (c) für $a, b, c \in R$: $a \mid b \Rightarrow a \mid cb$

Beweis von (a): Seien $q_1, q_2 \in R$ mit $b = q_1 a$ und $c = q_2 a$

$\Rightarrow b + c = q_1 a + q_2 a = (q_1 + q_2) a$ ✓

Beweis der Proposition:

„$\Rightarrow$" $b = ua$ für ein $u \in R^\times$ $\Rightarrow$ $a | b$

$a = u^{-1} b$ $\Rightarrow$ $b | a$

„$\Leftarrow$" $b = xa$, $a = yb$ für geeignete $x, y \in R$

$\Rightarrow$ $a = yb = yxa$

$\Rightarrow$ $(1 - yx)a = 0$

$\overset{RIB}{\Rightarrow}$ $a = 0$ oder $1 - yx = 0$

$a = 0$ $\Rightarrow$ $b = 0$ und $a = b$ ✓

$1 - yx = 0$ $\Rightarrow$ $yx = 1$ d.h. $x \in R^\times$ und a, b assoziiert. $\blacksquare$

Assoziiertheit

R kommutativer Ring

Definition

$a, b \in R$

a assoziiert zu b $:\Leftrightarrow$ es existiert $u \in R^\times$ mit $b = ua$

Beispiele

- $R = \mathbb{Z}$: 3 assoziiert zu -3
- $R = \mathbb{Q}[X]$: $X - 1$ assoziiert zu $2X - 2$ $= 2(X-1)$, $2 \in \mathbb{Q}^\times = \mathbb{Q}[X]^\times$

Assoziiertheit (Forts.)

Proposition

Sei R Integritätsbereich, $a, b \in R$.

Dann sind äquivalent:

- a assoziiert zu b
- $a \mid b$ und $b \mid a$

Beispiele

- im Fall $R = \mathbb{Z}$: $|a| = |b|$
- im Fall $R = K[X]$: $a = b = 0$ oder $\text{L.k.}(a)^{-1} a = \text{L.k.}(b)^{-1} b$

Ideale

R kommutativer Ring

$\{0\}$ ist Ideal

R ist Ideal

Definition

$I \subseteq R$ heißt *Ideal* von R, falls gilt:

- $I \neq \emptyset$
- $a + b \in I$ für alle $a, b \in I$ abgeschlossen bzgl. $+$
- $ar \in I$ für alle $r \in R$, $a \in I$ absorbiert beliebige Faktoren

$\Rightarrow 0 = a \cdot 0 \in I$ für ein beliebiges $a \in I$.

Beispiele

- Für $a \in R$ ist $(a) := aR := \{ar \mid r \in R\}$ ein Ideal. Menge aller Vielfachen von a.
  Ideale dieser Form heißen *Hauptideale*. z. B. $n\mathbb{Z}$, $n \in \mathbb{Z}$
- Für $a, b \in R$ ist $(a, b) := \{\lambda a + \mu b \mid \lambda, \mu \in R\}$ ein Ideal,
  das kleinste Ideal von R, das a und b enthält.

Ideale (Forts.)

Beispiele

- $R = \mathbb{Z}$: $3\mathbb{Z} = \{3z \mid z \in \mathbb{Z}\}$
- $R = \mathbb{Z}$: $(2,3) = \mathbb{Z}$: $1 = 3 + (-1)2 \in (2,3) \Rightarrow z = 1z \in (2,3) \; \forall z \in \mathbb{Z}$
- $R = \mathbb{Z}$: $(6,9) = (3)$
- $R = K[X]$: $XK[X] = \{f \in K[X] \mid X \text{ teilt } f\} =$
  $= \{f \in K[X] \mid \text{konst. Koeff. von } f = 0\} = \{f \in K[X] \mid f(0) = 0\}$

Bemerkung

Sei R kommutativer Ring und $a, b \in R$

(a) ► $a \mid b \Leftrightarrow (b) \subseteq (a)$. Teilen heißt Umfassen.

(b) ► Ist R Integritätsbereich, dann gilt:
a assoziiert zu $b \Leftrightarrow (a) = (b)$.

Beweis der Bemerkung:

(a) „$\Rightarrow$" $b = xa$ für ein $x \in R$

~~(a)~~ Sei $r \in R$. $\Rightarrow rb = rxa \in (a)$

$\Rightarrow (b) \subseteq (a)$

„$\Leftarrow$" $b = 1b \in (b) \subseteq (a)$

$\Rightarrow$ es ex. $x \in R$ mit $b = xa$, d.h. $a \mid b$.

Division mit Rest

Division mit Rest

- $a \in \mathbb{Z}$, $b \in \mathbb{Z} \setminus \{0\}$

  Dann existieren eindeutige $q, r \in \mathbb{Z}$, $0 \leq r < |b|$ mit

  $$a = qb + r$$

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

  Dann existieren eindeutige $q, r \in K[X]$, $\deg r < \deg g$ mit

  $$f = qg + r$$

Bew. für Division mit Rest in $\mathbb{Z}$:

OBdA $b > 0$, denn $a = qb + r \iff a = (-q)(-b) + r$

Setze $q := \left\lfloor \frac{a}{b} \right\rfloor := \max\{ z \in \mathbb{Z} \mid z \leq \frac{a}{b} \}$

größte ganze Zahl $\leq a/b$.

$\Rightarrow a = qb + r$ mit $r = a - qb$, $0 \leq r < b$.

Beweis der Division mit Rest in $K[X]$:

$f = 0$: $\quad f = 0 \cdot g \qquad r = 0$ ✓

$f \neq 0$, $\deg f < \deg g$: $\quad f = 0 \cdot g + f$ ✓

$f \neq 0$, $\deg f \geq \deg g$, $\deg f = n$, $\deg g = m$, $a_n := \text{L.K. } f$, $b_m := \text{L.K. } g$

Setze $\quad f' := f - \dfrac{a_n}{b_m} X^{n-m} g$

$\deg f' < \deg f$

$\xRightarrow[\text{über } \deg f]{\text{Induktion}}$ es ex. $q', r \in K[X]$: $\quad f' = q' \cdot g + r$, $\deg r < \deg g$.

$\Longrightarrow f = \left(q' + \dfrac{a_n}{a_m} X^{n-m}\right) g + r$ und $\deg r < \deg g$. $\blacksquare$

Division mit Rest (Forts.)

$$f = 2X^3 - 9X^2 + 4X, g = X^2 - 3X - 4 \in \mathbb{Q}[X].$$

$$
\begin{array}{l}
2X^3 - 9X^2 + 4X : (X^2 - 3X - 4)(2X - 3) \\
-(2X^3 - 6X^2 - 8X) \\
\hline
\quad -3X^2 + 12X \\
\quad -(-3X^2 + 9X + 12) \\
\hline
\qquad 3X - 12
\end{array}
$$

$$f = \underbrace{(X^2 - 3X - 4)}_{g}\underbrace{(2X - 3)}_{q} + \underbrace{3X - 12}_{r}$$

Teilbarkeit und Nullstellen von Polynomen

Definition

K Körper, $f \in K[X]$

Wert der zu f gehörigen Polynomfunktion an a.

- *Nullstelle* von f: $a \in K$ mit $f(a) = 0$
- *Linearfaktor* von f: $d \in K[X]$ linear mit $d \mid f$

Proposition

K Körper, $f \in K[X]$, $a \in K$

a ist Nullstelle von $f \Leftrightarrow X - a$ ist Linearfaktor von f

Beweis der Proposition:

„$\Rightarrow$" $f = q(X-a) + r$ $\deg r < \deg(X-a) = 1$, d.h.

$r = 0$ oder $\deg r = 0$

$0 = f(a) = q(a)(a-a) + r(a) = r(a) \Rightarrow r = 0$, da r konstant!

Siehe Skript

$\Rightarrow f = (X-a)q$

„$\Leftarrow$" $f = (X-a)g \Rightarrow f(a) = (a-a)g(a) = 0$ $\blacksquare$

Vielfachheiten von Nullstellen

Definition

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

$$\mathrm{m}_a(f) = \max\{k \in \mathbb{N}_0 \mid (X-a)^k \text{ teilt } f\}$$

heißt *Vielfachheit* von a als Nullstelle von f.

Beispiel $2X^2 - 2 = 2(X^2-1) = 2(X-1)(X+1)$

$$\mathrm{m}_a(2X^2-2) = \begin{cases} 1, & \text{für } a \in \{1, -1\} \\ 0 & \text{für } a \in \mathbb{Q} \setminus \{1, -1\} \end{cases}$$

Bemerkung

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

a Nullstelle von $f \Leftrightarrow \mathrm{m}_a(f) \geq 1$