Def (2.3.5, 2.3.6) R Komm. Ring mit Eins

Polynom über R:

$$\sum_{i=0}^{n} a_i t^i = a_0 + a_1 \cdot t + a_2 \cdot t^2 + \ldots + a_n t^n$$

mit $n \in \mathbb{N}$, $a_i \in R$

t: Unbestimmte

a_i: Koeffizienten ($a_i := 0$ für $i > n$)

$$\sum_{i=0}^{n} a_i t^i = \sum_{i=0}^{m} b_i t^i \quad :\Leftrightarrow \quad a_i = b_i \;\forall i \in \mathbb{N}$$

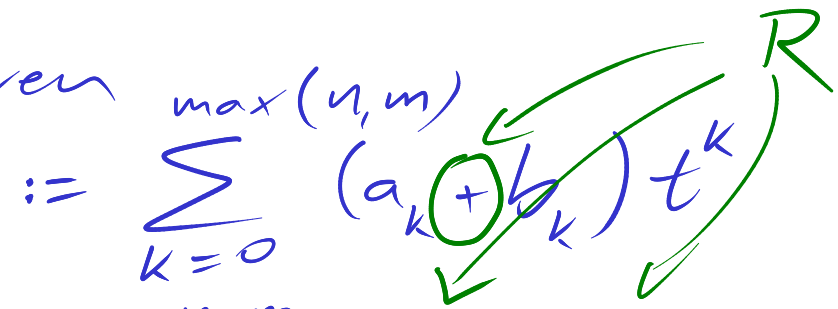
Für $f = a_0 + a_1 t + a_2 t^2 + \ldots + a_n t^n$

$g = b_0 + b_1 t + b_2 t^2 + \ldots + b_m t^m$

definieren

$$f +_p g := \sum_{k=0}^{\max(n,m)} (a_k \oplus b_k) t^k$$

$$f \cdot_p g := \sum_{k=0}^{n \cdot m} \left(\sum_{\substack{i,j: \\ i+j=k}} a_i \odot b_j \right) t^k$$



$R[t]$:= Menge aller Polynome über R

Satz (2.3.6) $(R[t], +_p, \cdot_p)$ ist ein kommutativer Ring mit Eins (Polynomring).

Ab jetzt: $(R[t], +, \cdot)$

Def (2.3.5) **Grad** von $f = \sum a_i t^i \neq 0$

$$\deg(f) := \max\{i \mid a_i \neq 0\}$$

$a_{\deg(f)}$ **Leitkoeffizient**

$$\deg(0) := -\infty$$

Satz (2.3.6) (Gradformel):

$f \neq 0$ Polynom mit Leithoeffizient $a_n \neq 0$
$g \neq 0$ Polynom mit Leithoeffizient $b_m \neq 0$
Falls $a_n \cdot b_m \neq 0$ in R, so ist
$f \cdot g \neq 0$ in $R[t]$, und
$\deg(f \cdot g) = \deg(f) + \deg(g)$.

Korollar (2.3.6):

Für jeden <u>nullteilerfreien</u> Komm. Ring mit Eins R ist auch $R[t]$ nullteilerfrei.

z.B. $R = \mathbb{Z}$

R Körper

$R = \{0\}$ ⇕

Def. (2.3.8) R Ring mit Eins, $1 \neq 0$.

Ein Element $a \in R$ ist eine <u>Einheit</u>, falls es ein multiplikatives Inverses besitzt.

$(\exists a' \in R : a' \cdot a = 1)$

$R^\times :=$ Menge aller Einheiten

$(R^\times, \cdot)$ <u>Einheitengruppe</u>

Satz (2.3.7) (Division mit Rest)

R kommutativer Ring mit Eins

$f, g \in R[t]$

Falls $g \neq 0$ mit Leitkoeff. $b_m \in R^\times$,

so existieren eindeutig bestimmte

$q, r \in R[t]$, für die gilt:

$$f = q \cdot g + r$$

und $\deg(r) < \deg(g)$.

Euklidischer Algorithmus

R kommutativer Ring mit Eins, $1 \neq 0$.

Def (2.3.8) Für $a, b \in R$

$b \mid a \quad :\Leftrightarrow \quad \exists c \in R : a = b \cdot c$ "b teilt a"

c ist ein ggT(a,b)

$:\Leftrightarrow$ ① $c \mid a$ und $c \mid b$, und

② $\forall c' \in R$:

$(c' \mid a$ und $c' \mid b)$

$\Rightarrow \boxed{c' \mid c}$

Korrektur!

Notiz:

(i) $(b \mid a$ und $a \mid b) \Leftrightarrow b = x \cdot a$ für $x \in R^\times$

(ii) c, c' ggT$(a,b) \Leftrightarrow c = x \cdot c'$ für ein $x \in R^\times$.

Satz: In $\mathbb{Z}$ und im Polynomring $K[t]$ über einem Körper K existiert zu beliebigen Elementen $a \neq 0, b \neq 0$ stets ein $ggT(a,b)$.

Konstruktiver Beweis:

$$\mathbb{Z} \xrightarrow{\delta} \mathbb{N} \qquad K[t] \xrightarrow{\delta} \mathbb{N}$$
$$c \mapsto |c| \qquad c \mapsto \deg(c)$$

Def.: $a_0 = a$, $a_1 = b$, $\delta(a_0) \geq \delta(a_1)$

Führe nun Teilung mit Rest durch:

$a_0 = q_1 \cdot a_1 + a_2$ $\quad a_k \mid a_0$

$a_1 = q_2 \cdot a_2 + a_3$ $\quad a_k \mid a_1$

$a_2 = q_3 \cdot a_3 + a_4$

$\vdots$ $\quad \vdots$

$a_{k-3} = q_{k-2} \cdot a_{k-2} + a_{k-1}$ $\quad a_k \mid a_{k-3}$

$a_{k-2} = q_{k-1} \cdot a_{k-1} + a_k$ $\quad a_k \mid a_{k-2}$

$a_{k-1} = q_k \cdot a_k + 0$ $\qquad a_k \mid a_{k-1}$

Beh: $a_k \mid a_i \ \forall i$

Also ist a_k g.T. von a, b.

Beh: $(c \mid a_0$ und $c \mid a_1) \Rightarrow c \mid a_k$.

□

Lemma von Bézout (2.3.9)

In $\mathbb{Z}$ und im Polynomring $K[t]$ über einem Körper K gilt:

Ist c ein ggT(a,b) $(a \neq 0, b \neq 0)$ so existieren x, y mit

$$c = x \cdot a + y \cdot b$$

Beweis: $a_0 := a$, $b_0 := b$

$$a_0 = q_1 \cdot a_1 + a_2$$
$$a_1 = q_2 \cdot a_2 + a_3$$
$$\vdots$$
$$a_{k-3} = q_{k-2} a_{k-2} + a_{k-1}$$
$$a_{k-2} = q_{k-1} a_{k-1} + a_k$$
$$a_{k-1} = q_k \cdot a_k + 0$$

Beh: $\exists x_i, y_i$ mit $a_i = x_i a_0 + y_i a_1$

$i=0$: $a_0 = 1 \cdot a_0 + 0 \cdot a_1$

$i=1$: $a_1 = 0 \cdot a_0 + 1 \cdot a_1$

Sind $x_i, x_{i-1}, y_i, y_{i-1}$ konstruiert, folgt aus

$$\boxed{a_{i-1} = q_i \cdot a_i + a_{i+1}}:$$

$$a_{i+1} = -q_i \cdot a_i + a_{i-1}$$

$$= \dots$$

$$= \underbrace{(-q_i x_i + x_{i-1})}_{x_{i+1}} a_0 + \underbrace{(-q_i y_i + y_{i-1})}_{y_{i+1}} a_1$$

□