WS 2003/04

Diskrete Strukturen I

Ernst W. Mayr

mayr@in.tum.de
Institut für Informatik
Technische Universität München

11-18-2004

Definition

Sei R ein (kommutativer) Ring. Ein Polynom über R in der Variablen x ist eine Funktion p der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

wobei $n \in \mathbb{N}_0$, $a_i \in R$ und $a_n \neq 0$.
n heißt der Grad des Polynoms, $a_0, \ldots, a_n$ seine Koeffizienten.
$R[x]$ bezeichnet die Menge der Polynome über dem Ring R in der Variablen x.

Definition

Sei R ein (kommutativer) Ring. Ein Polynom über R in der Variablen x ist eine Funktion p der Form

$$p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \ ,$$

wobei $n \in \mathbb{N}_0$, $a_i \in R$ und $a_n \neq 0$.
n heißt der Grad des Polynoms, $a_0, \ldots, a_n$ seine Koeffizienten.
$R[x]$ bezeichnet die Menge der Polynome über dem Ring R in der Variablen x.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom
   $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

Bemerkungen:

1. Das Nullpolynom $p(x) = 0$ hat Grad 0.
2. Formal kann das Polynom $p(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ auch mit der Folge $(a_0, a_1, \ldots, a_n)$ gleichgesetzt werden.

Beispiel

- $p(x) = x^2 - 2x + 1$ ist ein Polynom vom Grad 2.
- Eine lineare Funktion $f(x) = ax + b$ mit $a \neq 0$ ist ein Polynom vom Grad 1.
- Konstante Funktionen $f(x) = c$ sind Polynome vom Grad 0.

Berechnung des Funktionswertes

Um den Wert eines Polynoms an einer bestimmten Stelle x_0 zu bestimmen, verwendet man besten das sogenannte Hornerschema:

$$\begin{aligned} p(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \\ &= ((\ldots(((a_n x + a_{n-1})x + a_{n-2})x + \ldots.)x + a_1)x + a_0. \end{aligned}$$

Hat man die Koeffizienten in einem Array $a[0..n]$ abgespeichert, kann man den Funktionswert $p(x_0)$ daher wie folgt berechnen:

>0 $p \leftarrow a[n]$
>0 **for** i = n-1 **downto** 0 **do**
>0 $p \leftarrow p \cdot x_0 + a[i]$
>0 **end**
>0 **return**(p)
>0 **end**

Beobachtung:

Für die Auswertung eines Polynoms vom Grad n genügen $O(n)$ Multiplikationen und Additionen.

Hat man die Koeffizienten in einem Array $a[0..n]$ abgespeichert, kann man den Funktionswert $p(x_0)$ daher wie folgt berechnen:

>0 $p \leftarrow a[n]$
>0 <u>for</u> i = n-1 <u>downto</u> 0 <u>do</u>
>0 $p \leftarrow p \cdot x_0 + a[i]$
>0 <u>end</u>
>0 <u>return</u>(p)
>0 <u>end</u>

Beobachtung:

Für die Auswertung eines Polynoms vom Grad n genügen $O(n)$ Multiplikationen und Additionen.

Addition

Die Summe zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_n x^n + \cdots + b_1 x + b_0$ ist definiert durch

$$(a+b)(x) = c_n x^n + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = a_i + b_i \,.$$

Bemerkungen:

- An sich fehlende Koeffizienten sind gleich 0 gesetzt.
- Für den Grad des Summenpolynoms gilt

$$\operatorname{grad}(a+b) \leq \max\{\operatorname{grad}(a), \operatorname{grad}(b)\} \,.$$

Addition

Die Summe zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_n x^n + \cdots + b_1 x + b_0$ ist definiert durch

$$(a+b)(x) = c_n x^n + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = a_i + b_i\ .$$

Bemerkungen:

- An sich fehlende Koeffizienten sind gleich 0 gesetzt.
- Für den Grad des Summenpolynoms gilt

$$\operatorname{grad}(a+b) \leq \max\{\operatorname{grad}(a), \operatorname{grad}(b)\}\ .$$

Addition

Die Summe zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_n x^n + \cdots + b_1 x + b_0$ ist definiert durch

$$(a+b)(x) = c_n x^n + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = a_i + b_i\ .$$

Bemerkungen:

- An sich fehlende Koeffizienten sind gleich 0 gesetzt.
- Für den Grad des Summenpolynoms gilt

$$\operatorname{grad}(a+b) \leq \max\{\operatorname{grad}(a), \operatorname{grad}(b)\}\ .$$

Beispiel

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich
   $(a + b)(x) = x^2 + x + 7$.
   Hier gilt $\operatorname{grad}(a + b) = 2 = \operatorname{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen
   $(a + b)(x) = 2$ und somit
   $\operatorname{grad}(a + b) = 0 < 3 = \max\{\operatorname{grad}(a), \operatorname{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\le n$ lässt sich in Zeit $O(n)$ berechnen.

Beispiel

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich
   $(a + b)(x) = x^2 + x + 7$.
   Hier gilt $\mathrm{grad}(a + b) = 2 = \mathrm{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen
   $(a + b)(x) = 2$ und somit
   $\mathrm{grad}(a + b) = 0 < 3 = \max\{\mathrm{grad}(a), \mathrm{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\le n$ lässt sich in Zeit $O(n)$ berechnen.

Beispiel

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich $(a + b)(x) = x^2 + x + 7$.
   Hier gilt $\mathrm{grad}(a + b) = 2 = \mathrm{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen $(a + b)(x) = 2$ und somit
   $\mathrm{grad}(a + b) = 0 < 3 = \max\{\mathrm{grad}(a), \mathrm{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n)$ berechnen.

Beispiel

1. Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich
   $(a + b)(x) = x^2 + x + 7$.
   Hier gilt $\operatorname{grad}(a + b) = 2 = \operatorname{grad}(a)$.
2. Für $a(x) = x^3 + 1$ und $b(x) = -x^3 + 1$ ergibt sich hingegen
   $(a + b)(x) = 2$ und somit
   $\operatorname{grad}(a + b) = 0 < 3 = \max\{\operatorname{grad}(a), \operatorname{grad}(b)\}$.

Beobachtung:
Die Summe (und natürlich auch die Differenz) zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n)$ berechnen.

Multiplikation

Das Produkt zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ erhält man durch Ausmultiplizieren und anschliessendes Sortieren und Zusammenfassen der Koeffizienten. Also

$$(a \cdot b)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Für den Grad des Produktpolynoms gilt

$$\operatorname{grad}(a \cdot b) = \operatorname{grad}(a) + \operatorname{grad}(b)\,.$$

Multiplikation

Das Produkt zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ erhält man durch Ausmultiplizieren und anschliessendes Sortieren und Zusammenfassen der Koeffizienten. Also

$$(a \cdot b)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0, \quad \text{wobei } c_i = \sum_{j=0}^{i} a_j b_{i-j}.$$

Für den Grad des Produktpolynoms gilt

$$\mathrm{grad}(a \cdot b) = \mathrm{grad}(a) + \mathrm{grad}(b)\ .$$

Beispiel

Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + ((-3) \cdot 2 + 5 \cdot 4)x + 5 \cdot 2 \\ &= 4x^3 - 10x^2 + 14x + 10\ .\end{aligned}$$

Man sagt auch, dass die Koeffizienten

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

des Produktpolynoms durch Faltung der Koeffizientenfolgen von $a(x)$ und $b(x)$ entstehen.

Beispiel

Für $a(x) = x^2 - 3x + 5$ und $b(x) = 4x + 2$ ergibt sich

$$\begin{aligned}(a \cdot b)(x) &= (1 \cdot 4)x^3 + (1 \cdot 2 + (-3) \cdot 4)x^2 + ((-3) \cdot 2 + 5 \cdot 4)x + 5 \cdot 2 \\ &= 4x^3 - 10x^2 + 14x + 10\ .\end{aligned}$$

Man sagt auch, dass die Koeffizienten

$$c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

des Produktpolynoms durch Faltung der Koeffizientenfolgen von $a(x)$ und $b(x)$ entstehen.

Beobachtung:
Die Multiplikation zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.
Es gibt dafür aber auch schnellere Algorithmen!

Beobachtung:

Die Multiplikation zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Es gibt dafür aber auch schnellere Algorithmen!

Division

Betrachte das Schema

$$
\begin{array}{rcl}
2x^4 + x^3 + x + 3 & \div & x^2 + x - 1 = 2x^2 - x + 3 \\
-\,(2x^4 + 2x^3 - 2x^2) & & \\
\hline
-x^3 + 2x^2 + x + 3 & & \\
-\,(-x^3 - x^2 + x) & & \\
\hline
3x^2 + 3 & & \\
-(3x^2 + 3x - 3) & & \\
\hline
-3x + 6 & &
\end{array}
$$

Division

Betrachte das Schema

$$
\begin{array}{l}
2x^4 + x^3 + \qquad x + 3 \;\div\; x^2 + x - 1 \;=\; 2x^2 - x + 3 \\
-\,(2x^4 + 2x^3 - 2x^2) \\
\hline
\qquad -x^3 + 2x^2 + x + 3 \\
\qquad -\,(-x^3 - x^2 + x) \\
\hline
\qquad\qquad 3x^2 + \qquad 3 \\
\qquad\qquad -(3x^2 + 3x - 3) \\
\hline
\qquad\qquad\qquad -3x + 6
\end{array}
$$

Division

Betrachte das Schema

$$
\begin{array}{rrrrrl}
2x^4 + & x^3 + & & x + 3 & \div\ x^2 + x - 1 = & 2x^2 - x + 3 \\
-\,(2x^4 + & 2x^3 - & 2x^2) & & & \\ \hline
& -x^3 + & 2x^2 + & x + 3 & & \\
& -\,(-x^3 - & x^2 + & x) & & \\ \hline
& & 3x^2 + & 3 & & \\
& & -(3x^2 + & 3x - 3) & & \\ \hline
& & & -3x + 6 & &
\end{array}
$$

Division

Betrachte das Schema

$$
\begin{array}{rrrrrl}
 & 2x^4 + & x^3 + & & x + 3 & \div\ x^2 + x - 1 \ = \ 2x^2 - x + 3 \\
 - & (2x^4 + & 2x^3 - & 2x^2) & & \\
\hline
 & & -x^3 + & 2x^2 + & x + 3 & \\
 & - & (-x^3 - & x^2 + & x) & \\
\hline
 & & & 3x^2 + & 3 & \\
 & & & -(3x^2 + & 3x - 3) & \\
\hline
 & & & & -3x + 6 &
\end{array}
$$

Division

Betrachte das Schema

$$
\begin{array}{rrrrrl}
2x^4 + & x^3 + & & x + 3 & \div & x^2 + x - 1 = 2x^2 - x + 3 \\
-\,(2x^4 + & 2x^3 - & 2x^2) & & & \\
\hline
 & -x^3 + & 2x^2 + & x + 3 & & \\
 & -\,(-x^3 - & x^2 + & x) & & \\
\hline
 & & 3x^2 + & 3 & & \\
 & & -(3x^2 + & 3x - 3) & & \\
\hline
 & & & -3x + 6 & &
\end{array}
$$

Division

Betrachte das Schema

$$\begin{array}{rcl}
2x^4 + x^3 + \phantom{2x^2 +{}} x + 3 & \div & x^2 + x - 1 \;=\; 2x^2 - x + 3 \\
-\,(2x^4 + 2x^3 - 2x^2) \phantom{{}+ x + 3} & & \\
\hline
-x^3 + 2x^2 + x + 3 & & \\
-\,(-x^3 - x^2 + x) \phantom{{}+ 3} & & \\
\hline
3x^2 + \phantom{x +{}} 3 & & \\
-(3x^2 + 3x - 3) & & \\
\hline
-3x + 6 & &
\end{array}$$

Division

Betrachte das Schema

$$\begin{array}{rrrrrl}
2x^4 + & x^3 + & & & x+3 & \div\ x^2+x-1 \ = \ 2x^2 - x + 3 \\
-\ (2x^4 + & 2x^3 - & 2x^2) & & & \\
\hline
& -x^3 + & 2x^2 + & & x+3 & \\
& -\ (-x^3 - & x^2 + & & x) & \\
\hline
& & 3x^2 + & & 3 & \\
& & -(3x^2 + & 3x - & 3) & \\
\hline
& & & -\ 3x & +\ 6 &
\end{array}$$

Satz

5 Zu je zwei Polynomen $a(x)$ und $b(x)$, $b \neq 0$, gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, so dass

$$a(x) = q(x)b(x) + r(x) \qquad \textit{und} \qquad r = 0 \;\; \textit{oder} \;\; \mathrm{grad}(r) < \mathrm{grad}(b).$$

Beispiel

Im vorhergehenden Schema war das

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = (\underbrace{2x^2 - x + 3}_{q(x)}) \cdot (\underbrace{x^2 + x - 1}_{b(x)}) + (\underbrace{-3x + 6}_{r(x)})$$

Satz

5 Zu je zwei Polynomen $a(x)$ und $b(x)$, $b \neq 0$, gibt es eindeutig bestimmte Polynome $q(x)$ und $r(x)$, so dass

$$a(x) = q(x)b(x) + r(x) \qquad \text{und} \qquad r = 0 \;\; \text{oder} \;\; \mathrm{grad}(r) < \mathrm{grad}(b).$$

Beispiel

Im vorhergehenden Schema war das

$$\underbrace{2x^4 + x^3 + x + 3}_{a(x)} = (\underbrace{2x^2 - x + 3}_{q(x)}) \cdot (\underbrace{x^2 + x - 1}_{b(x)}) + (\underbrace{-3x + 6}_{r(x)})$$

Beweis:

Gilt $\text{grad}(a) < \text{grad}(b)$, so kann man $q = 0$ und $r = a$ setzen. Sei also $\text{grad}(a) \geq \text{grad}(b)$.

Induktion über $\text{grad}(a)$:

Ist $\text{grad}(a) = 0$, so folgt aus $\text{grad}(a) \geq \text{grad}(b)$, dass a und b beides konstante Funtionen sind. Also $a(x) = a_0$ und $b(x) = b_0$ mit $b_0 \neq 0$. Wir können daher $q(x) = a_0/b_0$ und $r(x) = 0$ setzen.

Beweis:
Gilt $\mathrm{grad}(a) < \mathrm{grad}(b)$, so kann man $q = 0$ und $r = a$ setzen. Sei also $\mathrm{grad}(a) \geq \mathrm{grad}(b)$.
Induktion über $\mathrm{grad}(a)$:
Ist $\mathrm{grad}(a) = 0$, so folgt aus $\mathrm{grad}(a) \geq \mathrm{grad}(b)$, dass a und b beides konstante Funtionen sind. Also $a(x) = a_0$ und $b(x) = b_0$ mit $b_0 \neq 0$. Wir können daher $q(x) = a_0/b_0$ und $r(x) = 0$ setzen.

Ist $\mathrm{grad}(a) = n > 0$ und $\mathrm{grad}(b) = m$, $m \leq n$, und

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \\ b(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0 \end{aligned}$$

so setzen wir

$$\tilde{a}(x) = a(x) - (a_n/b_m) x^{n-m} \cdot b(x) \ .$$

Dann gilt $\mathrm{grad}(\tilde{a}) < \mathrm{grad}(a)$.

Nach Induktionsannahme gibt es daher Polynome $\tilde{q}(x)$ und $\tilde{r}(x)$ mit $\tilde{a}(x) = \tilde{q}(x) \cdot b(x) + \tilde{r}(x)$, mit $\tilde{r}(x) = 0$ oder $\mathrm{grad}(\tilde{r}) < \mathrm{grad}(b)$. Es gilt

$$a(x) \ = \ (a_n/b_m)x^{n-m} b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) \ = \ q(x)b(x) + r(x) \ .$$

$$a(x) \ = \ (a_n/b_m)x^{n-m} b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) \ =: \ q(x)b(x) + r(x) \ .$$

Ist $\operatorname{grad}(a) = n > 0$ und $\operatorname{grad}(b) = m$, $m \leq n$, und

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \\ b(x) &= b_m x^m + b_{m-1}x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0 \end{aligned}$$

so setzen wir

$$\tilde{a}(x) = a(x) - (a_n/b_m)x^{n-m} \cdot b(x) \,.$$

Dann gilt $\operatorname{grad}(\tilde{a}) < \operatorname{grad}(a)$.
Nach Induktionsannahme gibt es daher Polynome $\tilde{q}(x)$ und $\tilde{r}(x)$ mit $\tilde{a}(x) = \tilde{q}(x) \cdot b(x) + \tilde{r}(x)$, mit $\tilde{r}(x) = 0$ oder $\operatorname{grad}(\tilde{r}) < \operatorname{grad}(b)$. Es gilt

$$a(x) \;=\; (a_n/b_m)x^{n-m}b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) \;=\; q(x)b(x) + r(x) \,.$$

$$a(x) \;=\; (a_n/b_m)x^{n-m}b(x) + \tilde{q}(x)b(x) + \tilde{r}(x) \;=:\; q(x)b(x) + r(x) \,.$$

Ist $\mathrm{grad}(a) = n > 0$ und $\mathrm{grad}(b) = m$, $m \leq n$, und

$$\begin{aligned} a(x) &= a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0, \quad a_n \neq 0, \\ b(x) &= b_m x^m + b_{m-1} x^{m-1} + \cdots + b_1 x + b_0, \quad b_m \neq 0 \end{aligned}$$

so setzen wir

$$\tilde{a}(x) = a(x) - (a_n/b_m) x^{n-m} \cdot b(x) \,.$$

Dann gilt $\mathrm{grad}(\tilde{a}) < \mathrm{grad}(a)$.
Nach Induktionsannahme gibt es daher Polynome $\tilde{q}(x)$ und $\tilde{r}(x)$ mit $\tilde{a}(x) = \tilde{q}(x) \cdot b(x) + \tilde{r}(x)$, mit $\tilde{r}(x) = 0$ oder $\mathrm{grad}(\tilde{r}) < \mathrm{grad}(b)$. Es gilt

$$a(x) = (a_n/b_m) x^{n-m} b(x) + \tilde{q}(x) b(x) + \tilde{r}(x) = q(x) b(x) + r(x) \,.$$

$$a(x) = (a_n/b_m) x^{n-m} b(x) + \tilde{q}(x) b(x) + \tilde{r}(x) =: q(x) b(x) + r(x) \,.$$

Um die Eindeutigkeit zu beweisen, nehmen wir an, es gebe für Polynome a und b zwei Darstellungen wie im Satz angegeben. Also $q \cdot b + r = a = \hat{q} \cdot b + \hat{r}$ und somit auch

$$(q - \hat{q}) \cdot b = (r - \hat{r}).$$

Falls $q \neq \hat{q}$, ist die linke Seite ein Polynom vom Grad $\geq \mathrm{grad}(b)$. Da die rechte Seite aus der Differenz zweier Polynome vom Grad kleiner als $\mathrm{grad}(b)$ besteht, Widerspruch! Also ist $q = \hat{q}$ und damit auch $r = \hat{r}$.

q. e. d.

Um die Eindeutigkeit zu beweisen, nehmen wir an, es gebe für Polynome a und b zwei Darstellungen wie im Satz angegeben. Also $q \cdot b + r = a = \hat{q} \cdot b + \hat{r}$ und somit auch

$$(q - \hat{q}) \cdot b = (r - \hat{r}).$$

Falls $q \neq \hat{q}$, ist die linke Seite ein Polynom vom Grad $\geq \mathrm{grad}(b)$. Da die rechte Seite aus der Differenz zweier Polynome vom Grad kleiner als $\mathrm{grad}(b)$ besteht, Widerspruch! Also ist $q = \hat{q}$ und damit auch $r = \hat{r}$.

q. e. d.

Beobachtung:

Für zwei Polynome a und b von Grad höchstens n kann man die Polynome q und r aus Satz 5 wie im Beispiel bestimmen. Da sich der Grad des Polynoms in jeder Zeile verringert, benötigen wir also höchstens n Multiplikationen von Polynomen mit Konstanten und n Subtraktionen von Polynomen vom Grad höchstens n. Insgesamt ergibt sich:

Die Division zweier Polynome vom Grad $\le n$ lässt sich in Zeit $O(n^2)$ berechnen.

Beobachtung:

Für zwei Polynome a und b von Grad höchstens n kann man die Polynome q und r aus Satz 5 wie im Beispiel bestimmen. Da sich der Grad des Polynoms in jeder Zeile verringert, benötigen wir also höchstens n Multiplikationen von Polynomen mit Konstanten und n Subtraktionen von Polynomen vom Grad höchstens n. Insgesamt ergibt sich:

Die Division zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

4.3.3 Nullstellen von Polynomen

Definition

Eine Nullstelle eines Polynoms p ist ein Wert x_0 mit $p(x_0) = 0$.

Lemma

6 Sei $p \in R[x]$, $x_0 \in R$ eine Nullstelle von p. Dann ist $p(x)$ ohne Rest durch $x - x_0$ teilbar.

Beweis.

Nach Satz 5 gibt es Polynome q und r mit
$p(x) = q(x) \cdot (x - x_0) + r(x)$ und $\mathrm{grad}(r) < \mathrm{grad}(x - x_0) = 1$,
also $\mathrm{grad}(r) = 0$, d.h. $r(x) = r_0$. Wegen
$p(x_0) = q(x_0) \cdot (x_0 - x_0) + r_0 = r_0$ muss also r_0 gleich Null sein.
D.h., $p(x) = q(x) \cdot (x - x_0)$. $\square$

4.3.3 Nullstellen von Polynomen

Definition

Eine Nullstelle eines Polynoms p ist ein Wert x_0 mit $p(x_0) = 0$.

Lemma

6 Sei $p \in R[x]$, $x_0 \in R$ eine Nullstelle von p. Dann ist $p(x)$ ohne Rest durch $x - x_0$ teilbar.

Beweis.

Nach Satz 5 gibt es Polynome q und r mit $p(x) = q(x) \cdot (x - x_0) + r(x)$ und $\mathrm{grad}(r) < \mathrm{grad}(x - x_0) = 1$, also $\mathrm{grad}(r) = 0$, d.h. $r(x) = r_0$. Wegen $p(x_0) = q(x_0) \cdot (x_0 - x_0) + r_0 = r_0$ muss also r_0 gleich Null sein. D.h., $p(x) = q(x) \cdot (x - x_0)$. □

4.3.3 Nullstellen von Polynomen

Definition

Eine Nullstelle eines Polynoms p ist ein Wert x_0 mit $p(x_0) = 0$.

Lemma

6 Sei $p \in R[x]$, $x_0 \in R$ eine Nullstelle von p. Dann ist $p(x)$ ohne Rest durch $x - x_0$ teilbar.

Beweis.

Nach Satz 5 gibt es Polynome q und r mit
$p(x) = q(x) \cdot (x - x_0) + r(x)$ und $\mathrm{grad}(r) < \mathrm{grad}(x - x_0) = 1$,
also $\mathrm{grad}(r) = 0$, d.h. $r(x) = r_0$. Wegen
$p(x_0) = q(x_0) \cdot (x_0 - x_0) + r_0 = r_0$ muss also r_0 gleich Null sein.
D.h., $p(x) = q(x) \cdot (x - x_0)$. $\square$

Satz

7 (Fundamentalsatz der Algebra) Jedes Polynom $p \neq 0$ mit Grad n hat höchstens n Nullstellen.

Beweis.

Wir zeigen den Satz durch Induktion über den Grad des Polynoms. Ist p ein Polynom mit Grad 0, so ist die Aussage wegen der Annahme $p \neq 0$ offenbar richtig. Ist p ein Polynom mit Grad $n > 0$, so hat p entweder keine Nullstelle (und die Aussage ist somit trivialerweise richtig) oder p hat mindestens eine Nullstelle a. Dann gibt es nach Lemma 6 eine Darstellung $p(x) = q(x) \cdot (x - a)$ mit $\mathrm{grad}(q) = n - 1$. Nach Induktionsannahme hat q höchstens $n - 1$ und somit p höchstens n Nullstellen. □

Satz

7 (Fundamentalsatz der Algebra) Jedes Polynom $p \neq 0$ mit Grad n hat höchstens n Nullstellen.

Beweis.

Wir zeigen den Satz durch Induktion über den Grad des Polynoms. Ist p ein Polynom mit Grad 0, so ist die Aussage wegen der Annahme $p \neq 0$ offenbar richtig. Ist p ein Polynom mit Grad $n > 0$, so hat p entweder keine Nullstelle (und die Aussage ist somit trivialerweise richtig) oder p hat mindestens eine Nullstelle a. Dann gibt es nach Lemma 6 eine Darstellung $p(x) = q(x) \cdot (x - a)$ mit $\mathrm{grad}(q) = n - 1$. Nach Induktionsannahme hat q höchstens $n - 1$ und somit p höchstens n Nullstellen. $\square$

Beispiel

- Das Polynom $x^2 - 1 = (x+1)(x-1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.

Beispiel

- Das Polynom $x^2 - 1 = (x+1)(x-1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.

Beispiel

- Das Polynom $x^2 - 1 = (x+1)(x-1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.

Beispiel

- Das Polynom $x^2 - 1 = (x+1)(x-1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.

Beispiel

- Das Polynom $x^2 - 1 = (x+1)(x-1)$ über $\mathbb{R}$ hat zwei Nullstellen $x = +1$ und $x = -1$ in $\mathbb{R}$.
- Das Polynom $x^2 + 1$ hat keine einzige reelle Nullstelle.
- Das Polynom $x^2 + 1$ hat die beiden komplexen Nullstellen $x = i$ und $x = -i$, wobei i die imaginäre Einheit bezeichnet, also $i = \sqrt{-1}$.

Bemerkung: $\mathbb{C}$ ist algebraisch abgeschlossen, da jedes Polynom $\in \mathbb{C}[x]$ vom Grad ≥ 1 mindestens eine Nullstelle $\in \mathbb{C}$ hat; $\mathbb{R}$ und $\mathbb{Q}$ sind nicht algebraisch abgeschlossen.