3. Polynome

3.1 Definition und Grundlagen

Definition 131

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.
Die Funktion p ordnet jedem Wert $x_0 \in R$ den Wert $p(x_0) \in R$ zu, ist also eine Funktion von R nach R.
$R[x]$ 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 132

- $p(x) = x^2 - 2x + 1$ 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.

3.2 Rechnen mit Polynomen

Berechnung des Funktionswertes

Um den Wert eines Polynoms an einer bestimmten Stelle $x_0 \in R$ zu bestimmen, verwendet man am 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:

$\underline{\texttt{begin}}$
  $p \leftarrow a[n]$
  $\underline{\texttt{for}}$ i = n-1 $\underline{\texttt{downto}}$ 0 $\underline{\texttt{do}}$
    $p \leftarrow p \cdot x_0 + a[i]$
  $\underline{\texttt{end}}$
  $\underline{\texttt{return}}(p)$
$\underline{\texttt{end}}$

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

Addition

Die Summe zweier Polynome $a(x) = a_n x^n + \cdots + a_1 x + a_0$ und $b(x) = b_m x^m + \cdots + b_1 x + b_0$ ist (sei o.B.d.A. $m \leq n$) 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 133

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 $O(n)$ arithmetischen Schritten 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

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

falls R nullteilerfrei sowie $a \neq 0 \neq b$ ist, ansonsten

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

Beispiel 134

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

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

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:
Das Produkt zweier Polynome vom Grad $\leq n$ lässt sich in Zeit $O(n^2)$ berechnen.

Es gibt dafür aber auch schnellere Algorithmen!

Division

Für diesen Abschnitt setzen wir voraus, dass der Koeffizientenring ein Körper ist. Betrachte das Schema

$$
\begin{array}{rl}
2x^4 + x^3 + \qquad x + 3 & \text{div} \;\; x^2 + x - 1 \;=\; 2x^2 - x + 3 \\
\underline{-\,(2x^4 + 2x^3 - 2x^2)} & \\
-x^3 + 2x^2 + x + 3 & \\
\underline{-\,(-x^3 - x^2 + x)} & \\
3x^2 + \qquad 3 & \\
\underline{-(3x^2 + 3x - 3)} & \\
-\,3x + 6 &
\end{array}
$$

Satz 135

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

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

Beispiel 136

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 $\mathrm{grad}(a) < \mathrm{grad}(b)$, 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.

Beweis (Forts.):

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 $\mathrm{grad}(\tilde{r}) < \mathrm{grad}(b)$ (falls $m = n$, wird $\tilde{q}(x) = 0$ und $\tilde{r}(x) = \tilde{a}(x)$). Es gilt

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

Beweis (Forts.):

Um die Eindeutigkeit zu beweisen, nehmen wir an, es gäbe 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 $r = \hat{r}$.

$\square$

Beobachtung:

Für zwei Polynome a und b von Grad höchstens n kann man die Polynome q und r aus Satz 135 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.

Beobachtung:

Falls der führende Koeffizient des Divisorpolynoms gleich 1 ist, lässt sich die Division auch über einem Ring R durchführen.

3.3 Nullstellen von Polynomen

Definition 137

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

Lemma 138

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 135 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., $p(x) = q(x) \cdot (x - x_0)$. □

Satz 139 (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 138 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. $\square$

Beispiele 140

- 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.

3.4 Partialbruchzerlegung

Beispiel 141

Finde zu $\frac{g}{f} = \frac{x^2+1}{(x-1)^2(x-2)}$ Polynome p, q mit $\mathrm{grad}(p) < 2$, $\mathrm{grad}(q) < 1$ und

$$\frac{x^2+1}{(x-1)^2(x-2)} = \frac{p}{(x-1)^2} + \frac{q}{x-2}. \qquad (*)$$

Die r.S. von (*) heißt Partialbruchzerlegung von $\frac{g}{f}$.

Ansatz: $p(x) = ax + b$, $q(x) = c$.

$$\frac{p}{(x-1)^2} + \frac{q}{x-2} = \frac{(x-2)\cdot p + (x-1)^2 \cdot q}{(x-1)^2(x-2)}.$$

Durch Vergleich mit (*) erhält man

$$\begin{aligned} x^2+1 &= (ax+b)(x-2)+c(x-1)^2 \\ &= (a+c)x^2+(b-2a-2c)x+c-2b. \end{aligned}$$

Koeffizientenvergleich liefert folgendes lineares Gleichungssystem:

$$\begin{aligned} a+c &= 1 \\ b-2a-2c &= 0 \\ c-2b &= 1 \end{aligned}$$

Dieses hat die eindeutige Lösung $a=-4, \quad b=2, \quad c=5$. Somit gilt:

$$\frac{x^2+1}{(x-1)^2(x-2)} = \frac{-4x+2}{(x-1)^2} + \frac{5}{x-2}.$$