

WS 2005/06

Diskrete Strukturen

Ernst W. Mayr

Fakultät für Informatik
TU München

<http://www14.in.tum.de/lehre/2005WS/ds/index.html.de>

29. November 2005

Division

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

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

Satz 132

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

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

Beispiel 133

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

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

so setzen wir

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

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

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 $\text{grad}(\tilde{r}) < \text{grad}(b)$. Es gilt

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

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



Beobachtung:

Für zwei Polynome a und b von Grad höchstens n kann man die Polynome q und r aus Satz 132 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 134

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

Lemma 135

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 132 gibt es Polynome q und r mit

$p(x) = q(x) \cdot (x - x_0) + r(x)$ und $\text{grad}(r) < \text{grad}(x - x_0) = 1$, also $\text{grad}(r) = 0$, 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 136 (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 135 eine Darstellung $p(x) = q(x) \cdot (x - a)$ mit $\text{grad}(q) = n - 1$. Nach Induktionsannahme hat q höchstens $n - 1$ und somit p höchstens n Nullstellen. □

Beispiele 137

- 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 138

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

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

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 $a = -4$, $b = 2$, $c = 5$. Somit gilt:

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

Satz 139 (Partialbruchzerlegung)

Seien $f, g \in K[x]$ ($K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$) Polynome mit $\text{grad}(g) < \text{grad}(f)$, und es gelte

$$f(x) = (x - \alpha_1)^{m_1} \cdot \dots \cdot (x - \alpha_r)^{m_r}$$

mit $\mathbb{N} \ni m_i \geq 1$ und paarweise verschiedenen $\alpha_i \in K$ ($i = 1, \dots, r$). Dann gibt es eindeutig bestimmte Polynome $g_1, \dots, g_r \in K[x]$ mit $\text{grad}(g_i) < m_i$, so dass gilt:

$$\frac{g}{f} = \frac{g_1}{(x - \alpha_1)^{m_1}} + \dots + \frac{g_r}{(x - \alpha_r)^{m_r}}.$$