Prof. Dr. H. Brenner **Osnabrück SS 2017**

Grundkurs Mathematik II

Vorlesung 50

Durch starkes Denken kann man ein Kamel zu Fall bringen.

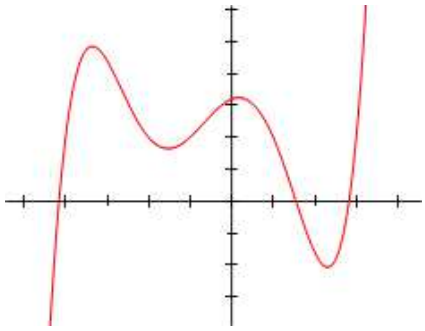
Ibn Sina

Polynomfunktionen

In ein Polynom $P \in K[X]$ kann man ein Element $z \in K$ *einsetzen*, indem man die Variable X an jeder Stelle durch z ersetzt. Dies führt zu einer Abbildung

$$K \longrightarrow K,\ z \longmapsto P(z),$$

die die durch das Polynom definierte *Polynomfunktion* heißt.



Der Graph einer Polynomfunktion von $\mathbb{R}$ nach $\mathbb{R}$ vom Grad 5.

Diese Abbildungen gehören zu den wichtigsten Funktionen. Die konstanten Polynome a_0 führen zu den konstanten Abbildungen mit dem Wert a_0, lineare Polynome der Form $a_1X + a_0$ führen zu affin-linearen Funktionen, insbesondere entspricht die Variable der Identität. Quadratische Polynome $a_2X^2 + a_1X + a_0$ führen auf quadratische Funktionen, die Potenzen der Variablen, also X^k, führen auf die Potenzfunktionen $z \mapsto z^k$.

LEMMA 50.1. *Es sei K ein Körper und $z \in K$ ein fixiertes Element. Dann ist die Abbildung*

$$K[X] \longrightarrow K,$$

die einem Polynom P die Einsetzung $P(z)$ zuordnet, ein Ringhomomorphismus. Für beliebige Polynome $P, Q \in K[X]$ gilt also

(1)
$$(P+Q)(z) \;=\; P(z)+Q(z).$$

(2)
$$(P\cdot Q)(z) \;=\; P(z)\cdot Q(z).$$

(3)
$$1(z) \;=\; 1.$$

Beweis. Es seien $P = \sum_i a_i X^i$ und $Q = \sum_j b_j X^j$.

(1) Es ist
$$P+Q \;=\; \sum_i \left(a_i+b_i\right) X^i$$
und somit ist unter Verwendung des Distributivgesetzes für K
$$\begin{aligned}
(P+Q)(x) &= \left(\sum_i \left(a_i+b_i\right) X^i\right)(z)\\
&= \sum_i \left(a_i+b_i\right) z^i\\
&= \sum_i a_i z^i + \sum_i b_i z^i\\
&= \left(\sum_i a_i X^i\right)(z) + \left(\sum_i b_i X^i\right)(z)\\
&= P(z)+Q(z).
\end{aligned}$$

(2) Es ist
$$P\cdot Q \;=\; \sum_k \left(\sum_{i+j=k} a_i\cdot b_j\right) X^k$$
und somit ist unter Verwendung des Distributivgesetzes und der Potenzgesetze für K
$$\begin{aligned}
(P\cdot Q)(z) &= \left(\sum_k \left(\sum_{i+j=k} a_i\cdot b_j\right) X^k\right)(z)\\
&= \sum_k \left(\sum_{i+j=k} a_i\cdot b_j\right) z^k\\
&= \sum_{i,j} a_i\cdot b_j z^{i+j}\\
&= \left(\sum_i a_i z^i\right)\cdot\left(\sum_j b_j z^j\right)\\
&= \left(\sum_i a_i X^i\right)(z)\cdot\left(\sum_j b_j X^j\right)(z)\\
&= P(z)\cdot Q(z).
\end{aligned}$$

(3) Für jedes konstante Polynom a_0 gilt $a_0(z) = a_0$, da nicht eingesetzt werden kann.

□

Die Division mit Rest für Polynome

DEFINITION 50.2. Es sei K ein Körper. Man sagt, dass ein Polynom $T \in K[X]$ ein Polynom $P \in K[X]$ *teilt*, wenn es ein Polynom $Q \in K[X]$ mit

$$P = TQ$$

gibt.

Wenn P von T geteilt wird, so sagt man auch, dass P ein Vielfaches von T ist. In $K[X]$ ist es, anders wie in einem Körper, aber ähnlich wie in $\mathbb{Z}$, nicht möglich, ein Element durch ein anderes Element $\neq 0$ zu teilen. Es gibt aber, wie bei $\mathbb{Z}$, einen wichtigen Ersatz dafür, die *Division mit Rest*.

SATZ 50.3. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Es seien $P, T \in K[X]$ zwei Polynome mit $T \neq 0$. Dann gibt es eindeutig bestimmte Polynome $Q, R \in K[X]$ mit*

$$P = TQ + R \text{ und mit } \operatorname{grad}(R) < \operatorname{grad}(T) \text{ oder } R = 0\,.$$

Beweis. Wir beweisen die Existenzaussage durch Induktion über den Grad von P. Wenn der Grad von T größer als der Grad von P ist, so ist $Q = 0$ und $R = P$ eine Lösung, so dass wir dies nicht weiter betrachten müssen. Bei $\operatorname{grad}(P) = 0$ ist nach der Vorbemerkung auch $\operatorname{grad}(T) = 0$, also ist T ein konstantes Polynom, und damit ist (da $T \neq 0$ und K ein Körper ist) $Q = P/T$ und $R = 0$ eine Lösung. Sei nun $\operatorname{grad}(P) = n$ und die Aussage für kleineren Grad schon bewiesen. Wir schreiben $P = a_nX^n + \cdots + a_1X + a_0$ und $T = b_kX^k + \cdots + b_1X + b_0$ mit $a_n, b_k \neq 0$, $k \leq n$. Dann gilt mit $H = \frac{a_n}{b_k}X^{n-k}$ die Beziehung

$$\begin{aligned} P' &:= P - TH \\ &= 0X^n + \left(a_{n-1} - \frac{a_n}{b_k}b_{k-1}\right)X^{n-1} + \cdots \\ &\quad + \left(a_{n-k} - \frac{a_n}{b_k}b_0\right)X^{n-k} + a_{n-k-1}X^{n-k-1} + \cdots + a_0. \end{aligned}$$

Dieses Polynom P' hat einen Grad kleiner als n und darauf können wir die Induktionsvoraussetzung anwenden, d.h. es gibt Q' und R' mit

$$P' = TQ' + R' \text{ mit } \operatorname{grad}(R') < \operatorname{grad}(T) \text{ oder } R' = 0\,.$$

Daraus ergibt sich insgesamt

$$P = P' + TH = TQ' + TH + R' = T(Q' + H) + R',$$

so dass also $Q = Q' + H$ und $R = R'$ eine Lösung ist. Zur Eindeutigkeit sei $P = TQ + R = TQ' + R'$ mit den angegebenen Bedingungen. Dann ist $T(Q - Q') = R' - R$. Da die Differenz $R' - R$ einen Grad kleiner als grad (T) besitzt, ist aufgrund der Gradeigenschaften diese Gleichung nur bei $R = R'$ und $Q = Q'$ lösbar. □

Das Polynom T ist genau dann ein Teiler von P, wenn bei der Division mit Rest von P durch T der Rest gleich 0 ist. Der Beweis des Satzes ist konstruktiv, d.h. es wird in ihm ein Verfahren beschrieben, mit der man die Division mit Rest berechnen kann. Dazu muss man die Rechenoperationen des Grundkörpers beherrschen. Wir geben dazu drei Beispiele, zwei über den rationalen Zahlen und eines über einem endlichen Körper.

Beispiel 50.4. Wir führen die Polynomdivision

$$P = X^2 + X + 2 \text{ durch } T = X - 5$$

durch. Es wird also ein quadratisches Polynom durch ein lineares Polynom dividiert, d.h. der Quotient muss vom Grad 1 und der Rest muss vom Grad 0 sein. Im ersten Schritt überlegt man, mit welchem Term man T multiplizieren muss, damit das Produkt mit P im Leitterm übereinstimmt. Das ist offenbar X. Das Produkt ist

$$X\,(X-5) \;=\; X^2 - 5X.$$

Die Differenz von P zu diesem Produkt ist

$$X^2 + X + 2 - \left(X^2 - 5X\right) \;=\; 6X + 2.$$

Mit diesem Polynom, nennen wir es P', setzen wir die Division durch T fort. Um Übereinstimmung im Leitkoeffizienten zu erhalten, muss man T mit 6 multiplizieren, dies ergibt

$$6X - 30\,.$$

Die Differenz zu P' ist somit

$$6X + 2 - (6X - 30) \;=\; 32.$$

Dies ist das Restpolynom und somit ist insgesamt

$$X^2 + X + 2 \;=\; (X+6)\,(X-5) + 32.$$

Beispiel 50.5. Wir führen die Polynomdivision

$$P = 6X^3 + X + 1 \text{ durch } T = 3X^2 + 2X - 4$$

durch. Es wird also ein Polynom vom Grad 3 durch ein Polynom vom Grad 2 dividiert, d.h. dass der Quotient und auch der Rest (maximal) vom Grad 1 sind. Im ersten Schritt überlegt man, mit welchem Term man T multiplizieren muss, damit das Produkt mit P im Leitterm übereinstimmt. Das ist offenbar $2X$. Das Produkt ist

$$2X\left(3X^2 + 2X - 4\right) \;=\; 6X^3 + 4X^2 - 8X.$$

Die Differenz von P zu diesem Produkt ist

$$6X^3+X+1-\left(6X^3+4X^2-8X\right) \;=\; -4X^2+9X+1.$$

Mit diesem Polynom, nennen wir es P', setzen wir die Division durch T fort. Um Übereinstimmung im Leitkoeffizienten zu erhalten, muss man T mit $\frac{-4}{3}$ multiplizieren. Dies ergibt

$$-\frac{4}{3}T \;=\; -\frac{4}{3}\left(3X^2+2X-4\right) \;=\; -4X^2-\frac{8}{3}X+\frac{16}{3}.$$

Die Differenz zu P' ist somit

$$-4X^2+9X+1-\left(-4X^2-\frac{8}{3}X+\frac{16}{3}\right) \;=\; \frac{35}{3}X-\frac{13}{3}.$$

Dies ist das Restpolynom und somit ist insgesamt

$$6X^3+X+1 \;=\; \left(3X^2+2X-4\right)\left(2X-\frac{4}{3}\right)+\frac{35}{3}X-\frac{13}{3}.$$

Beispiel 50.6. Wir führen im endlichen Restklassenkörper $\mathbb{Z}/(7)$ die Polynomdivision

$$P=X^2+3X+5 \text{ durch } T=3X+4$$

durch. Es wird also ein quadratisches Polynom durch ein lineares Polynom dividiert, d.h. der Quotient muss vom Grad 1 und der Rest muss vom Grad 0 sein. Im ersten Schritt überlegt man, mit welchem Term man T multiplizieren muss, damit das Produkt mit P im Leitterm übereinstimmt. Mit was muss man also 3 in $\mathbb{Z}/(7)$ multiplizieren, um 1 zu erhalten? Eine Schreibweise wie $\frac{1}{3}$ ist hier wenig hilfreich, es muss ein Element aus $\mathbb{Z}/(7)$ sein. Wegen $3\cdot 5 \;=\; 15 \;=\; 1 \mod 7$ ist 5 das inverse Element, man muss also mit $5X$ multiplizieren. Das Produkt ist

$$5X\left(3X+4\right) \;=\; X^2+6X.$$

Die Differenz von P zu diesem Produkt ist

$$X^2+3X+5-\left(X^2+6X\right) \;=\; 4X+5.$$

Mit diesem Polynom, nennen wir es P', setzen wir die Division durch T fort. Um Übereinstimmung im Leitkoeffizienten zu erhalten, muss man T mit 6 multiplizieren, da ja $3\cdot 6 \;=\; 18 \;=\; 4 \mod 7$ ist. Dies ergibt

$$4X+3\,.$$

Die Differenz zu P' ist somit

$$4X+5-\left(4X+3\right) \;=\; 2.$$

Dies ist das Restpolynom und somit ist insgesamt

$$X^2+3X+5 \;=\; \left(5X+6\right)\left(3X+4\right)+2.$$

Nullstellen

Unter einer Nullstelle eines Polynoms P versteht man ein $a \in K$ mit $P(a) = 0$. Ein Polynom muss keine Nullstellen besitzen, ferner hängt dies vom Grundkörper ab.

LEMMA 50.7. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom und $a \in K$. Dann ist a genau dann eine Nullstelle von P, wenn P ein Vielfaches des linearen Polynoms $X - a$ ist.*

Beweis. Wenn P ein Vielfaches von $X - a$ ist, so kann man

$$P = (X - a)Q$$

mit einem weiteren Polynom Q schreiben. Einsetzen ergibt

$$P(a) = (a - a)Q(a) = 0.$$

Im Allgemeinen gibt es aufgrund der Division mit Rest eine Darstellung

$$P = (X - a)Q + R,$$

wobei $R = 0$ oder aber den Grad 0 besitzt, also eine Konstante ist. Einsetzen ergibt

$$P(a) = R.$$

Wenn also $P(a) = 0$ ist, so muss der Rest $R = 0$ sein, und das bedeutet, dass $P = (X - a)Q$ ist. □

KOROLLAR 50.8. *Sei K ein Körper und sei $K[X]$ der Polynomring über K. Sei $P \in K[X]$ ein Polynom ($\neq 0$) vom Grad d. Dann besitzt P maximal d Nullstellen.*

Beweis. Wir beweisen die Aussage durch Induktion über d. Für $d = 0, 1$ ist die Aussage offensichtlich richtig. Sei also $d \geq 2$ und die Aussage sei für kleinere Grade bereits bewiesen. Sei a eine Nullstelle von P. Dann ist $P = Q(X - a)$ nach Lemma 50.7 und Q hat den Grad $d - 1$, so dass wir auf Q die Induktionsvoraussetzung anwenden können. Das Polynom Q hat also maximal $d - 1$ Nullstellen. Für $b \in K$ gilt $P(b) = Q(b)(b - a)$. Dies kann nur dann 0 sein, wenn einer der Faktoren 0 ist, so dass eine Nullstelle von P gleich a ist oder aber eine Nullstelle von Q ist. Es gibt also maximal d Nullstellen von P. □

Der Interpolationssatz

Der folgende Satz heißt *Interpolationssatz* und beschreibt die Interpolation von vorgegebenen Funktionswerten durch Polynome.

Satz 50.9. *Es sei K ein Körper und es seien n verschiedene Elemente $a_1, \ldots, a_n \in K$ und n Elemente $b_1, \ldots, b_n \in K$ gegeben. Dann gibt es ein eindeutiges Polynom $P \in K[X]$ vom Grad $\leq n-1$ derart, dass $P(a_i) = b_i$ für alle i ist.*

Beweis. Wir beweisen die Existenz und betrachten zuerst die Situation, wo $b_j = 0$ ist für alle $j \neq i$. Dann ist

$$(X-a_1)\cdots(X-a_{i-1})(X-a_{i+1})\cdots(X-a_n)$$

ein Polynom vom Grad $n-1$, das an den Stellen $a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n$ den Wert 0 hat. Das Polynom

$$\frac{b_i}{(a_i-a_1)\cdots(a_i-a_{i-1})(a_i-a_{i+1})\cdots(a_i-a_n)} \\ (X-a_1)\cdots(X-a_{i-1})(X-a_{i+1})\cdots(X-a_n)$$

hat an diesen Stellen ebenfalls eine Nullstelle, zusätzlich aber noch bei a_i den Wert b_i. Nennen wir dieses Polynom P_i. Dann ist

$$P = P_1 + P_2 + \cdots + P_n$$

das gesuchte Polynom. An der Stelle a_i gilt ja

$$P_j(a_i) = 0$$

für $j \neq i$ und $P_i(a_i) = b_i$.

Die Eindeutigkeit folgt aus Korollar 50.8. □

Wenn die Daten $a_1, \ldots, a_n$ und $b_1, \ldots, b_n$ gegeben sind, so findet man das interpolierende Polynom P vom Grad $\leq n-1$, das es nach Satz 50.9 geben muss, folgendermaßen: Man macht den Ansatz

$$P = c_0 + c_1X + c_2X^2 + \cdots + c_{n-2}X^{n-2} + c_{n-1}X^{n-1}$$

und versucht die unbekannten Koeffizienten $c_0, \ldots, c_{n-1}$ zu bestimmen. Jeder Interpolationspunkt (a_i, b_i) führt zu einer linearen Gleichung

$$c_0 + c_1a_i + c_2a_i^2 + \cdots + c_{n-2}a_i^{n-2} + c_{n-1}a_i^{n-1} = b_i$$

über K. Das entstehende lineare Gleichungssystem besitzt genau eine Lösung, die das Polynom bestimmt.

Rationale Funktionen

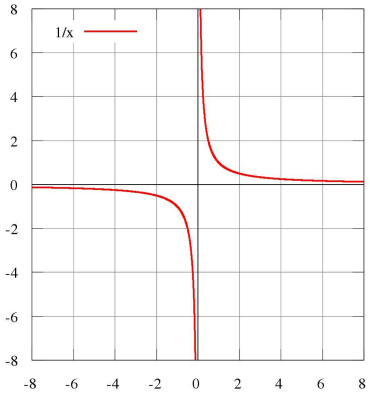
Der Polynomring $K[X]$ ist ein kommutativer Ring, aber kein Körper. Man kann aber mit Hilfe von formal-rationalen Funktionen einen Körper konstruieren, der den Polynomring enthält, ähnlich wie man aus $\mathbb{Z}$ die rationalen Zahlen $\mathbb{Q}$ konstruieren kann. Dazu definiert man

$$K(X) := \left\{ \frac{P}{Q} \mid P, Q \in K[X],\, Q \neq 0 \right\},$$

wobei man wie bei $\mathbb{Q}$ zwei Brüche $\frac{P}{Q}$ und $\frac{P'}{Q'}$ miteinander identifiziert, wenn

$$PQ' = P'Q$$

ist. Auf diese Weise entsteht der *Körper der rationalen Funktionen* (über K).



Man kann Brüche P/Q von Polynomen als Funktionen auffassen, die außerhalb der Nullstellen des Nenners definiert sind. Das Beispiel zeigt den Graphen der rationalen Funktion $1/X$.

Einen formalen Ausdruck P/Q kann man in folgender Weise wieder als eine Funktion auffassen.

DEFINITION 50.10. Zu zwei Polynomen $P, Q \in K[X]$, $Q \neq 0$, heißt die Funktion

$$D \longrightarrow K,\ z \longmapsto \frac{P(z)}{Q(z)},$$

wobei $D \subseteq K$ das Komplement der Nullstellen von Q ist, eine *rationale Funktion*.

Die nach den Polynomfunktionen einfachsten Funktionen sind die rationalen Funktionen.

Abbildungsverzeichnis

Quelle = Polynomialdeg5.svg , Autor = Benutzer Geek3 auf Commons, Lizenz = CC-by-sa 3.0 1

Quelle = Function-1 x.svg , Autor = Benutzer Qualc1 auf Commons, Lizenz = CC-by-sa 3.0 8