Prof. Dr. H. Brenner **Osnabrück WS 2017/2018**

Lineare Algebra und analytische Geometrie I

Vorlesung 19

In den folgenden Vorlesungen werden wir versuchen, eine quadratische $d \times d$-Matrix M (bzw. einen Endomorphismus) dadurch zu verstehen, dass wir Ausdrücke der Form

$$a_n M^n + a_{n-1} M^{n-1} + \cdots + a_2 M^2 + a_1 M^1 + a_0 M^0$$

untersuchen, wobei M^i als das i-fache Matrixprodukt der Matrix mit sich selbst und M^0 als Einheitsmatrix E_d zu interpretieren ist. Solche Ausdrücke ergeben sich, indem man in Polynome Matrizen einsetzt. In dieser Vorlesung führen wir Polynome und den Polynomring ein.

Der Polynomring über einem Körper

Definition 19.1. Der *Polynomring* über einem Körper K besteht aus allen Polynomen

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

mit $a_i \in K$, $n \in \mathbb{N}$, und mit komponentenweiser Addition und einer Multiplikation, die durch distributive Fortsetzung der Regel

$$X^n \cdot X^m := X^{n+m}$$

definiert ist.

Ein Polynom $P = \sum_{i=0}^{n} a_i X^i = a_0 + a_1 X + \cdots + a_n X^n$ ist formal gesehen nichts anderes als das Tupel $(a_0, a_1, \ldots, a_n)$, die die *Koeffizienten* des Polynoms heißen. Zwei Polynome sind genau dann gleich, wenn sie in allen ihren Koeffizienten übereinstimmen. Der Körper K heißt in diesem Zusammenhang der *Grundkörper* des Polynomrings. Aufgrund der komponentenweisen Definition der Addition liegt unmittelbar eine kommutative Gruppe vor, mit dem *Nullpolynom* (bei dem alle Koeffizienten 0 sind) als neutralem Element. Die Polynome mit $a_i = 0$ für alle $i \geq 1$ heißen *konstante Polynome*, man schreibt sie einfach als a_0.

Die für ein einfaches Tupel zunächst ungewöhnliche Schreibweise deutet in suggestiver Weise an, wie die Multiplikation aussehen soll, das Produkt $X^n \cdot X^m$ ist nämlich durch die Addition der Exponenten, also $X^n \cdot X^m := X^{n+m}$, gegeben. Dabei nennt man X die *Variable* des Polynomrings. Für beliebige Polynome ergibt sich die Multiplikation aus dieser einfachen Multiplikationsbedingung durch distributive Fortsetzung gemäß der Vorschrift, „alles mit

allem“ zu multiplizieren. Die Multiplikation ist also explizit durch folgende Regel gegeben:[1]

$$\left(\sum_{i=0}^{n} a_i X^i\right) \cdot \left(\sum_{j=0}^{m} b_j X^j\right) = \sum_{k=0}^{n+m} c_k X^k \text{ mit } c_k = \sum_{r=0}^{k} a_r b_{k-r} .$$

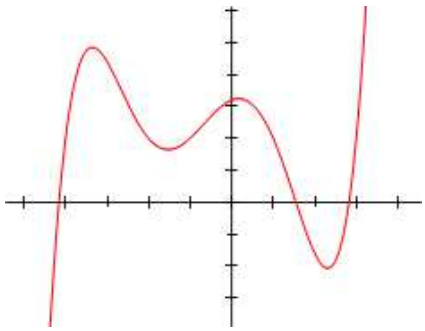
Die Multiplikation ist assoziativ, kommutativ, distributiv und besitzt das konstante Polynom 1 als neutrales Element, siehe Aufgabe 19.3. Insgesamt liegt also ein kommutativer Ring vor.

Definition 19.2. Der *Grad* eines von 0 verschiedenen Polynoms

$$P = a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n$$

mit $a_n \neq 0$ ist n.

Das Nullpolynom bekommt keinen Grad. Der Koeffizient a_n, der zum Grad n des Polynoms gehört, heißt *Leitkoeffizient* des Polynoms. Der Ausdruck $a_n X^n$ heißt *Leitterm*. Ein Polynom mit Leitkoeffizient 1 heißt *normiert*.



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

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

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

die die durch das Polynom definierte *Polynomfunktion* heißt. Diese Abbildung ist im Allgemeinen nicht linear, Linearität liegt nur bei $P = a_1 X$ vor.

Die Division mit Rest

Definition 19.3. 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

$$P = TQ$$

[1] Wobei wir natürlich, wie auch bei der Addition oder dem Vergleichen von Polynomen verschiedener Grade, die Polynome für $r > n$ bzw. $k - r > m$ mit den Koeffizienten $a_r = 0$ bzw. $b_{k-r} = 0$ ergänzen können.

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 einen wichtigen Ersatz dafür, die *Division mit Rest*.

Satz 19.4. *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 $P = a_n X^n + \cdots + a_1 X + a_0$ und $T = b_k X^k + \cdots + b_1 X + b_0$ mit $a_n, b_k \neq 0$, $k \leq n$. Dann gilt mit $H = \frac{a_n}{b_k} X^{n-k}$ die Beziehung

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

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 $\operatorname{grad}(T)$ 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 zwei Beispiele, eines über den rationalen Zahlen und eines über den komplexen Zahlen.

Beispiel 19.5. 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 19.6. Wir führen die Polynomdivision

$$P = (4 + 3\mathrm{i})X^3 + X^2 + 5\mathrm{i} \text{ durch } T = (1 + \mathrm{i})X^2 + X - 3 + 2\mathrm{i}$$

aus. Das Inverse zu $1 + \mathrm{i}$ ist $\frac{1}{2} - \frac{1}{2}\mathrm{i}$ und daher ist

$$\begin{aligned}(4 + 3\mathrm{i})(1 + \mathrm{i})^{-1} &= (4 + 3\mathrm{i})\left(\frac{1}{2} - \frac{1}{2}\mathrm{i}\right)\\ &= 2 + \frac{3}{2} - 2\mathrm{i} + \frac{3}{2}\mathrm{i}\\ &= \frac{7}{2} - \frac{1}{2}\mathrm{i}.\end{aligned}$$

Daher beginnt Q mit $\left(\frac{7}{2} - \frac{1}{2}\mathrm{i}\right)X$ und es ist

$$\begin{aligned}&((1 + \mathrm{i})X^2 + X - 3 + 2\mathrm{i})\left(\frac{7}{2} - \frac{1}{2}\mathrm{i}\right)X\\ = \;&(4 + 3\mathrm{i})X^3 + \left(\frac{7}{2} - \frac{1}{2}\mathrm{i}\right)X^2 + \left(-\frac{19}{2} + \frac{17}{2}\mathrm{i}\right)X.\end{aligned}$$

Dies muss man nun von P abziehen und erhält

$$P - \left((4 + 3\mathrm{i})X^3 + \left(\frac{7}{2} - \frac{1}{2}\mathrm{i}\right)X^2 + \left(-\frac{19}{2} + \frac{17}{2}\mathrm{i}\right)X\right)$$

$$= \left(-\frac{5}{2}+\frac{1}{2}\mathrm{i}\right)X^2+\left(\frac{19}{2}-\frac{17}{2}\mathrm{i}\right)X+5\mathrm{i}.$$

Auf dieses Polynom (nennen wir es P') wird das gleiche Verfahren angewendet. Man berechnet

$$\left(-\frac{5}{2}+\frac{1}{2}\mathrm{i}\right)\left(\frac{1}{2}-\frac{1}{2}\mathrm{i}\right) = -1+\frac{3}{2}\mathrm{i}.$$

Daher ist der konstante Term von Q gleich $-1+\frac{3}{2}\mathrm{i}$ und es ergibt sich

$$((1+\mathrm{i})X^2+X-3+2\mathrm{i})\left(-1+\frac{3}{2}\mathrm{i}\right) = \left(-\frac{5}{2}+\frac{1}{2}\mathrm{i}\right)X^2+\left(-1+\frac{3}{2}\mathrm{i}\right)X-\frac{13}{2}\mathrm{i}.$$

Dies ziehen wir von P' ab und erhalten

$$P'-\left(\left(-\frac{5}{2}+\frac{1}{2}\mathrm{i}\right)X^2+\left(-1+\frac{3}{2}\mathrm{i}\right)X-\frac{13}{2}\mathrm{i}\right) = \left(\frac{21}{2}-10\mathrm{i}\right)X+\frac{23}{2}\mathrm{i}.$$

Dies ist der Rest R, die vollständige Division mit Rest ist also

$$\begin{aligned}&(4+3\mathrm{i})X^3+X^2+5\mathrm{i}\\ =\ &((1+\mathrm{i})X^2+X-3+2\mathrm{i})\left(\left(\frac{7}{2}-\frac{1}{2}\mathrm{i}\right)X-1+\frac{3}{2}\mathrm{i}\right)+\left(\frac{21}{2}-10\mathrm{i}\right)X+\frac{23}{2}\mathrm{i}.\end{aligned}$$

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. Das Polynom X^2+1 hat keine reelle Nullstelle, dagegen gibt es die komplexen Nullstellen i und $-\mathrm{i}$. Als Element in $\mathbb{R}[X]$ kann man X^2+1 nicht als Produkt von einfacheren Polynomen schreiben, in $\mathbb{C}[X]$ hingegen hat man die Zerlegung

$$X^2+1 = (X-\mathrm{i})(X+\mathrm{i}).$$

Bemerkung 19.7. Es sei K ein Körper, $K[X]$ der Polynomring über K und $a\in K$. Dann ist die Einsetzungsabbildung

$$K[X]\longrightarrow K,\ P\longmapsto P(a),$$

K-linear. Darüber hinaus gilt

$$(PQ)(a) = P(a)Q(a),$$

siehe Aufgabe 19.8.

Lemma 19.8. *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 19.9. *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 (falls P keine Nullstelle besitzt, sind wir direkt fertig), Dann ist $P = Q(X-a)$ nach Lemma 19.8 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 Fundamentalsatz der Algebra

Es gilt der folgende *Fundamentalsatz der Algebra*, den wir hier ohne Beweis erwähnen.

SATZ 19.10. *Jedes nichtkonstante Polynom $P \in \mathbb{C}[X]$ über den komplexen Zahlen besitzt eine Nullstelle.*

Aus dem Fundamentalsatz der Algebra folgt, dass jedes von 0 verschiedene Polynom $P \in \mathbb{C}[X]$ in Linearfaktoren zerfällt, d.h. man kann

$$P = c(X-z_1)(X-z_2)\cdots(X-z_n)$$

mit bis auf die Reihenfolge eindeutig bestimmten komplexen Zahlen $c, z_1, \ldots, z_n$ schreiben (wobei Wiederholungen erlaubt sind).

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

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

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).

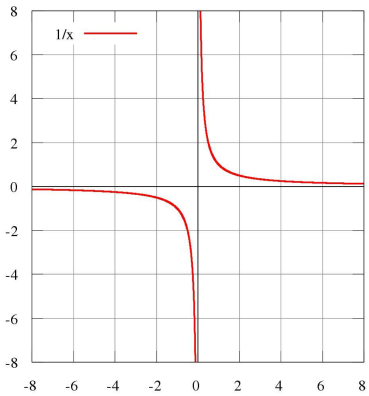
Einen formalen Ausdruck P/Q kann man in folgender Weise wieder als eine Funktion auffassen.

Definition 19.11. 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.



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

Abbildungsverzeichnis