Sebastian Thomas

RWTH Aachen, WS 2016/17
23.11.2016–24.11.2016

Diskrete Strukturen

Vorlesungen 10 und 11

9 Der Polynomring

In diesem Abschnitt führen wir Polynome mit Koeffizienten in einem Körper ein. Da sich Polynome addieren und multiplizieren lassen, erhalten wir so für jeden Körper einen kommutativen Ring.
Im Folgenden, bis zum Ende des Abschnitts und mit Ausnahme einiger Beispiele, sei stets ein Körper K gegeben.

Begriffsbildung

Wir beginnen mit der Einführung von Polynomen, wobei wir auf eine Rückführung auf bekannte Konzepte verzichten. Ein Polynom in X soll ein Ausdruck der Form $\sum_{i\in[0,n]} a_i X^i = a_0 + a_1 X + \ldots + a_n X^n$ für ein beliebiges $n \in \mathbb{N}_0$ sein. Führen wir triviale Summanden mit, so können alle Polynome gleich behandelt werden, unabhängig von der Anzahl ihrer jeweiligen nicht-trivialen Summanden. Hierzu betrachten wir im Folgenden die Menge

$$\begin{aligned} K^{(\mathbb{N}_0)} &= \{a \in K^{\mathbb{N}_0} \mid \{i \in \mathbb{N}_0 \mid a_i \neq 0\} \text{ ist endlich}\} \\ &= \{a \in K^{\mathbb{N}_0} \mid \text{es gibt ein } n \in \mathbb{N}_0 \text{ mit } a_i = 0 \text{ für alle } i > n\}. \end{aligned}$$

(9.1) Vorstellung (Polynomring)**.**

(a) Es sei $a \in K^{(\mathbb{N}_0)}$ gegeben. Wir nennen

$$f = \sum_{i\in\mathbb{N}_0} a_i X^i$$

ein *Polynom* in X über K. Die Familie a wird *Koeffizientenfolge*. Für $i \in I$ wird a_i der *Koeffizient* von f an der Stelle i genannt.

(b) Polynome $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$, wobei $a, b \in K^{(\mathbb{N}_0)}$, sind *gleich*, geschrieben $f = g$, falls $a = b$ gilt.

(c) Das Polynom $X = \sum_{i\in\mathbb{N}_0} \delta_{1,i} X^i$ wird *Unbestimmte* genannt.

(d) Der kommutative Ring gegeben durch die Menge der Polynome

$$K[X] := \{\sum_{i\in\mathbb{N}_0} a_i X^i \mid a \in K^{(\mathbb{N}_0)}\}$$

in X über K mit Addition und Multiplikation gegeben durch

$$\begin{aligned} \sum_{i\in\mathbb{N}_0} a_i X^i + \sum_{i\in\mathbb{N}_0} b_i X^i &= \sum_{i\in\mathbb{N}_0} (a_i + b_i) X^i, \\ (\sum_{i\in\mathbb{N}_0} a_i X^i)(\sum_{j\in\mathbb{N}_0} b_j X^j) &= \sum_{k\in\mathbb{N}_0} (\sum_{\substack{i,j\in\mathbb{N}_0 \\ i+j=k}} a_i b_j) X^k \end{aligned}$$

für $a, b \in K^{(\mathbb{N}_0)}$ wird *Polynomring* in X über K genannt.

(e) Wir identifizieren K mit der Teilmenge $\{aX^0 \mid a \in K\}$ von $K[X]$. Das heißt, unter Missbrauch der Notation notieren wir aX^0 für $a \in K$ auch durch a.

Für $a, b \in K^{(\mathbb{N}_0)}$ sind die Polynome $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ in X über K genau dann gleich, wenn $a = b$ gilt, d.h. wenn $a_i = b_i$ für alle $i \in \mathbb{N}_0$ gilt.

(9.2) Beispiel. Es seien $f, g \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$ und $g = -X^3 + 2X^2 + X + 1$. Dann ist

$$\begin{aligned} f + g &= -X^3 + 3X^2 + X, \\ fg &= -X^5 + 2X^4 + 2X^3 - X^2 - X - 1, \\ -2f &= -2X^2 + 2. \end{aligned}$$

Polynomfunktionen

Die wesentliche Eigenschaft eines Polynoms $f \in K[X]$ ist die Möglichkeit, Elemente von K in f „einzusetzen". Hierdurch können wir Polynome als Funktionen auffassen.

(9.3) Definition (Polynomfunktion)**.** Es seien $f \in K[X]$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben. Die Abbildung

$$K \to K,\ x \mapsto \sum_{i\in\mathbb{N}_0} a_i x^i$$

heißt *Polynomfunktion* zu f und wird unter Missbrauch der Notation wieder als f notiert.

(9.4) Beispiel. Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$. Dann ist $f(5) = 24$.

Beweis. Es gilt $f(5) = 5^2 - 1 = 24$. □

Wir betonen, dass Polynome keine Funktionen *sind*, sondern nur zugehörige Polynomfunktionen *liefern*. So gibt es etwa über dem Körper $\mathbb{F}_2$ unendlich viele Polynome, aber lediglich vier Polynomfunktionen (alle vier Funktionen von $\mathbb{F}_2$ nach $\mathbb{F}_2$ sind Polynomfunktionen).

Grad eines Polynoms

Es seien $f \in K[X]\setminus\{0\}$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben. Wegen $f \neq 0$ ist $a \neq 0$ und wegen $a \in K^{(\mathbb{N}_0)}$ gibt es ein $n \in \mathbb{N}_0$ mit $a_n \neq 0$ und $a_i = 0$ für $i > n$. Somit ist

$$f = \sum_{i\in[0,n]} a_i X^i.$$

Wir wollen nun etwas Terminologie für diese endliche Darstellung eines Polynoms festlegen.

(9.5) Definition (Grad, Leitkoeffizient, normiertes Polynom)**.** Es seien $f \in K[X] \setminus \{0\}$ und $a \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ gegeben.

(a) Der *Grad* von f ist definiert als

$$\deg f := \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\}.$$

(b) Der Koeffizient $\mathrm{lc}(f) := a_{\deg f}$ von f heißt *Leitkoeffizient* von f.

(c) Wir sagen, dass f ein *normiertes* Polynom ist, falls $\mathrm{lc}(f) = 1$ ist.

Wir betonen, dass das Nullpolynom keinen Grad hat.

(9.6) Beispiel.

(a) Das Polynom $X^2 - 1$ über $\mathbb{Q}$ hat den Grad 2 und den Leitkoeffizienten 1 und ist daher normiert.

(b) Das Polynom $-X^3 + 2X^2 + X + 1$ über $\mathbb{Q}$ hat den Grad 3 und den Leitkoeffizienten -1 und ist daher nicht normiert.

(9.7) Bemerkung. Es seien $f, g \in K[X] \setminus \{0\}$ gegeben.

(a) Wenn $f + g \neq 0$ ist, gilt

$$\deg(f+g) \leq \max(\deg f, \deg g).$$

Wenn $\deg f \neq \deg g$ ist, gilt

$$\deg(f+g) = \max(\deg f, \deg g).$$

(b) Es gilt $fg \neq 0$ und

$$\deg(fg) = \deg f + \deg g.$$

Beweis. Es seien $a, b \in K^{(\mathbb{N}_0)}$ mit $f = \sum_{i\in\mathbb{N}_0} a_i X^i$ und $g = \sum_{i\in\mathbb{N}_0} b_i X^i$ gegeben.

(a) Es ist $f + g = \sum_{i\in\mathbb{N}_0}(a_i + b_i)X^i$. Für $i \in \mathbb{N}_0$ mit $a_i + b_i \neq 0$ gilt auch $a_i \neq 0$. Folglich ist

$$\deg(f+g) = \max\{i \in \mathbb{N}_0 \mid a_i + b_i \neq 0\} \leq \max\{i \in \mathbb{N}_0 \mid a_i \neq 0\} = \deg f.$$

Analog lässt sich $\deg(f+g) \leq \deg g$ zeigen.

Nun gelte $\deg f \neq \deg g$. Wir nehmen o.B.d.A. an, dass $\deg f < \deg g$ ist. Für $i \in \mathbb{N}_0$ mit $i \geq \deg g$ gilt dann $a_i = 0$ und damit

$$a_i + b_i = \begin{cases} b_{\deg g}, & \text{falls } i = \deg g, \\ 0, & \text{falls } i > \deg g. \end{cases}$$

Folglich ist $\deg(f+g) = \deg g = \max(\deg f, \deg g)$.

(b) Es ist $fg = \sum_{k\in\mathbb{N}_0}(\sum_{\substack{i,j\in\mathbb{N}_0 \\ i+j=k}} a_i b_j)X^k$. Für $k \in \mathbb{N}_0$ mit $k \geq \deg f + \deg g$ gilt dann

$$\sum_{\substack{i,j\in\mathbb{N}_0 \\ i+j=k}} a_i b_j = \begin{cases} a_{\deg f} b_{\deg g}, & \text{falls } k = \deg f + \deg g, \\ 0, & \text{falls } i > \deg f + \deg g. \end{cases}$$

Folglich ist $fg \neq 0$ und $\deg(fg) = \deg f + \deg g$. □

(9.8) Korollar. Es ist

$$K[X]^\times = K^\times.$$

Beweis. Für $f \in K[X]^\times$ gilt

$$\deg f + \deg f^{-1} = \deg(ff^{-1}) = \deg 1 = 0,$$

also $\deg f = \deg f^{-1} = 0$ und damit $f, f^{-1} \in K^\times$. Folglich ist $K[X]^\times \subseteq K^\times$. Da jedes in K invertierbare Element insbesondere in $K[X]$ invertierbar ist, gilt umgekehrt auch $K^\times \subseteq K[X]^\times$. Insgesamt ist also $K[X]^\times = K^\times$. □

(9.9) Korollar. Der Polynomring $K[X]$ ist ein Integritätsbereich.

Beweis. Dies gilt nach Bemerkung (9.7)(b). □

Manchmal betrachten wir nur Polynome bis zum einem gegebenen Grad n. Wir legen eine Schreibweise fest:

(9.10) Notation. Für $n \in \mathbb{N}_0$ setzen wir

$$K[X]_{<n} := \{f \in K[X] \mid f = 0 \text{ oder } \deg f < n\}.$$

(9.11) Bemerkung. Für $n \in \mathbb{N}_0$ ist

$$K[X]_{<n} = \{\sum_{i\in[0,n-1]} a_i X^i \mid a \in K^{[0,n-1]}\}.$$

Insbesondere gilt $K[X]_{<0} = \{0\}$ und $K[X]_{<1} = K$.

(9.12) Definition (konstantes Polynom, lineares Polynom)**.** Es sei $f \in K[X]$ gegeben.

(a) Wir nennen f ein *konstantes* Polynom, falls $f = 0$ oder $\deg f = 0$ ist.

(b) Wir nennen f ein *lineares* Polynom, falls $\deg f = 1$ ist.

(9.13) Beispiel.

(a) Das Polynom 2 über $\mathbb{Q}$ ist konstant.

(b) Das Polynom $2X + 3$ über $\mathbb{Q}$ ist linear.

Nullstellen

Unter allen Körperelementen, die man in ein gegebenes Polynom einsetzen kann, sind diejenigen von besonderem Interesse, welche die Null als Wert annehmen:

(9.14) Definition (Nullstelle)**.** Es sei $f \in K[X]$ gegeben. Eine *Nullstelle* von f ist ein $a \in K$ mit

$$f(a) = 0.$$

(9.15) Beispiel. Es sei $f \in \mathbb{Q}[X]$ gegeben durch $f = X^2 - 1$. Dann sind 1 und -1 Nullstellen von f.

Beweis. Es gilt $f(1) = 1^2 - 1 = 0$ und $f(-1) = (-1)^2 - 1 = 0$. Folglich sind 1 und -1 Nullstellen von f. □

(9.16) Definition (algebraisch abgeschlossen)**.** Wir nennen K *algebraisch abgeschlossen*, falls jedes Polynom über K, welches nicht konstant ist, eine Nullstelle hat.

(9.17) Beispiel. Der Körper der reellen Zahlen $\mathbb{R}$ ist nicht algebraisch abgeschlossen.

Beweis. Für alle $a \in \mathbb{R}$ gilt $a^2 + 1 \geq 0 + 1 = 1 > 0$ und damit insbesondere $a^2 + 1 \neq 0$, d.h. das Polynom $X^2 + 1$ über $\mathbb{R}$ hat keine Nullstelle. Folglich ist $\mathbb{R}$ nicht algebraisch abgeschlossen. □

Der *Fundamentalsatz der Algebra*, welchen wir im Rahmen dieser Vorlesung nicht beweisen können, besagt, dass der Körper der komplexen Zahlen $\mathbb{C}$, siehe Definition (11.25), algebraisch abgeschlossen ist.