# Unterlagen zu Polynomringen

Erhard Aichinger

Linz, im November 2005

KAPITEL 1

# Polynome und Körper

## 1. Körper

DEFINITION 1.1. Ein kommutativer Ring mit Eins $\mathbf{R} = (R, +, -, \cdot, 0, 1)$ ist ein *Körper* wenn

(1) $|R| \geq 2$,
(2) Für alle $x \in R \setminus \{0\}$ gibt es ein $y \in R$ mit $x \cdot y = 1$.

ÜBUNGSAUFGABEN 1.2.

(1) Zeigen Sie, dass es in einem Körper für jedes $x$ höchstens ein $y$ mit $x \cdot y = 1$ geben kann.
(2) Zeigen Sie, dass das Produkt zweier Elemente in einem Körper nur dann 0 ist, wenn einer der Faktoren gleich 0 ist.

In einem Körper hat jedes Element $a \neq 0$ genau ein multiplikativ inverses Element; wir bezeichnen es mit $a^{-1}$. Für jede Primzahl $p$ ist der Ring $\mathbb{Z}_p$ ein Körper.

DEFINITION 1.3. Sei $\mathbf{E} = (E, +, -, \cdot, 0, 1)$ ein Körper, und sei $K \subseteq E$. Die Menge $K$ ist dann *Trägermenge eines Unterkörpers* von $\mathbf{E}$, wenn

(1) $0 \in K$, $1 \in K$,
(2) für alle $x, y \in K$ gilt $x + y \in K$, $x - y \in K$, $x \cdot y \in K$,
(3) für alle $x \in K \setminus \{0\}$ gilt $x^{-1} \in K$.

Wenn $K$ Trägermenge eines Unterkörpers von $\mathbf{E}$ ist, so ist $\mathbf{K} = \left(K, +|_{K\times K}, -|_K, \cdot|_{K\times K}, 0, 1\right)$ selbst ein Körper. Wir bezeichnen $\mathbf{K}$ dann als *Unterkörper* von $\mathbf{E}$, und $\mathbf{E}$ als *Erweiterung* von $\mathbf{K}$.

## 2. Polynome

DEFINITION 1.4. Sei $\mathbf{K}$ kommutativer Ring mit Eins. Dann ist $K[x]$ die Menge aller Ausdrücke

$$a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots + a_n x^n$$

mit $n \in \mathbb{N}_0$ und $a_0, a_1, \ldots, a_n \in K$.

DEFINITION 1.5. Addition und Multiplikation auf $K[x]$.

DEFINITION 1.6. Sei $f \in K[x]$. $\deg f := \ldots$, $\deg 0 := -1$.

DEFINITION 1.7. Sei $\mathbf{K}$ Körper, und seien $f, g \in K[x]$.

(1) $f$ *teilt* $g$, wenn es $q \in K[x]$ gibt, sodass $g = q \cdot f$.
(2) $f$ ist *invertierbar*, wenn $\deg f = 0$.
(3) $f$ ist *irreduzibel über* $\mathbf{K}$ (ein irreduzibles Polynom in $K[x]$), wenn $\deg f \geq 1$ und für alle $a, b \in K[x]$ mit $a \cdot b = f$ entweder $a$ oder $b$ Grad 0 hat.
(4) $f$ ist *normiert*, wenn es führenden Koeffizienten 1 hat.

## 3. Teilbarkeit von Polynomen

SATZ 1.8. *Sei* $\mathbf{K}$ *Körper, und seien* $f, g \in K[x]$. *Wenn* $f \neq 0$, *so gibt es* $q, r \in K[x]$ *mit* $g = q \cdot f + r$ *und* $\deg r < \deg f$.

DEFINITION 1.9 (ggT in $\mathbf{K}[x]$). Sei $\mathbf{K}$ ein Körper, und seien $f, g \in K[x]$, nicht beide 0. Dann ist $d \in K[x]$ ein *größter gemeinsamer Teiler* von $f$ und $g$, wenn folgende Bedingungen gelten:

(1) $d | f$ und $d | g$,
(2) Für alle $h \in K[x]$ mit $h | f$ und $h | g$ gilt $\deg(h) \leq \deg(d)$,
(3) $d$ ist normiert.

Wir bezeichnen den Rest von $g$ bei der Division durch $f$ mit $g \bmod f$. Da das Paar $(g, f)$ die gleichen gemeinsamen Teiler wie das Paar $(f, g \bmod f)$ hat, können wir einen größten gemeinsamen Teiler mithilfe des Euklidschen Algorithmus berechnen.

Wir rechnen dazu drei Beispiele:

BEISPIEL 1.10. Wir berechnen ein größten gemeinsamen Teiler von $f, g \in \mathbb{R}[x]$ für

$$f = -8x + 4x^2 + 6x^3 - 5x^4 + x^5$$

und

$$g = 4 - 4x - x^2 + x^3.$$

Wir bilden die gleiche Tabelle wie beim Euklidschen Algorithmus für ganze Zahlen und erhalten:

$$\begin{array}{ccc}
-8x + 4x^2 + 6x^3 - 5x^4 + x^5 & 1 & 0 \\
4 - 4x - x^2 + x^3 & 0 & 1 \\
-24 + 32x - 10x^2 & 1 & -6 + 4x - x^2 \\
-\left(\frac{32}{25}\right) + \frac{16x}{25} & \frac{11}{50} + \frac{x}{10} & -\left(\frac{8}{25}\right) + \frac{7x}{25} + \frac{9x^2}{50} - \frac{x^3}{10} \\
0 & &
\end{array}$$

Um einen normierten gemeinsamen Teiler zu erhalten, multiplizieren wir die vorletzte Zeile dieser Tabelle mit $\frac{25}{16}$ und erhalten $-2 + x$ als einen größten gemeinsamen Teiler.

Außerdem gilt

$$-2 + x = (\frac{11}{32} + \frac{5x}{32}) \cdot f + (-\left(\frac{1}{2}\right) + \frac{7x}{16} + \frac{9x^2}{32} - \frac{5x^3}{32}) \cdot g.$$

BEISPIEL 1.11. Wir berechnen den größten gemeinsamen Teiler der Polynome

$$f = 1 + x^3 + x^5$$

und

$$g = 1 + x + x^3$$

in $\mathbb{Z}_2[x]$. Wir erhalten

$$\begin{array}{cccc} 1 + x^3 + x^5 & 1 & 0 \\ 1 + x + x^3 & 0 & 1 \\ 1 + x^2 & 1 & x^2 \\ 1 & x & 1 + x^3 \\ 0 & & \end{array}$$

Daher ist 1 ein größter gemeinsamer Teiler, und es gilt

$$1 = x \cdot f + (1 + x^3) * g.$$

BEISPIEL 1.12. Wir berechnen den größten gemeinsamen Teiler der Polynome

$$f = 1 + x^3 + x^5$$

und

$$g = 1 + x + x^3$$

in $\mathbb{Z}_3[x]$. Wir erhalten

$$\begin{array}{cccc} 1 + x^3 + x^5 & 1 & 0 \\ 1 + x + x^3 & 0 & 1 \\ 1 + 2x^2 & 1 & 2x^2 \\ 1 + 2x & x & 1 + 2x^3 \\ 0 & & \end{array}$$

Daher ist $2 * (1 + 2x) = 2 + x$ ein größter gemeinsamer Teiler, und es gilt

$$2 + x = 2x \cdot f + (2 + x^3) \cdot g.$$

Wir können also einen größten gemeinsamen Teiler mithilfe des Euklidschen Algorithmus bestimmen. Daraus ergibt sich:

SATZ 1.13. *Sei* $\mathbf{K}$ *ein Körper, und seien* $f, g \in K[x]$, *nicht beide* 0. *Dann gibt es einen größten gemeinsamen Teiler* $d$ *von* $f$ *und* $g$, *für den es* $u, v \in K[x]$ *gibt, sodass* $u \cdot f + v \cdot g = d$.

SATZ 1.14. *Sei* $\mathbf{K}$ *ein Körper, und seien* $f, g \in K[x]$, *nicht beide* 0, *und sei* $d \in K[x]$. *Wir nehmen an, dass es* $u, v \in K[x]$ *gibt, sodass* $d = u \cdot f + v \cdot g$. *Dann teilt jeder gemeinsame Teiler von* $f$ *und* $g$ *auch das Polynom* $d$.

*Beweis:* Sei $h$ ein gemeinsamer Teiler von $f$ und $g$. Dann gilt $h | uf + vg$, also $h | d$. ■

KOROLLAR 1.15. *Sei* $\mathbf{K}$ *ein Körper, und seien* $f, g \in K[x]$*, nicht beide* 0*. Seien* $d_1, d_2 \in K[x]$ *beide* ggT *von* $f$ *und* $g$*. Dann gilt* $d_1 = d_2$*.*

*Beweis*: Nach Satz 1.13 gibt es einen größten gemeinsamen Teiler $d$ von $f$ und $g$, der sich als $uf + vg$ mit $u, v \in K[x]$ schreiben lässt. Wegen Satz 1.14 gilt $d_1 | d$. Sowohl $d_1$ als auch $d$ haben den maximal möglichen Grad unter allen gemeinsamen Teilern von $f$ und $g$. Also gilt $\deg(d_1) = \deg(d)$. Somit gibt es ein $\alpha \in K$, sodass $d = \alpha d_1$. Da $d$ und $d_1$ normiert sind, gilt $\alpha = 1$ und somit $d = d_1$. Ebenso gilt $d = d_2$, also $d_1 = d_2$. ■

## 4. Polynomfunktionen und Nullstellen

DEFINITION 1.16. Sei $\mathbf{K}$ ein Körper, und sei $f \in K[x]$. Seien $n \in \mathbb{N}$ und $a_0, a_1, \ldots, a_n \in K$ so, dass

$$f = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n.$$

Dann ist $\overline{f}$ die Funktion, die durch

$$\begin{array}{rccl} \overline{f} & : & K & \longrightarrow & K \\ & & k & \longmapsto & a_0 + a_1 k + a_2 k^2 + \cdots + a_n k^n \end{array}$$

definiert ist. Sie heißt *die von* $f$ *induzierte Polynomfunktion*.

DEFINITION 1.17. Sei $\mathbf{K}$ ein Körper, sei $f \in K[x]$, und sei $\alpha \in K$. Die Zahl $\alpha$ ist eine *Nullstelle* von $f$, wenn $\overline{f}(\alpha) = 0$.

SATZ 1.18. *Sei* $\mathbf{K}$ *ein Körper, sei* $f \in K[x]$*, und sei* $\alpha \in K$*. Dann ist* $\alpha$ *genau dann eine Nullstelle von* $f$*, wenn* $x - \alpha \mid f$ *gilt.*

SATZ 1.19. *Sei* $\mathbf{K}$ *ein Körper, sei* $n \in \mathbb{N}$*, und sei* $f \in K[x]$ *ein Polynom mit* $\deg(f) = n$*. Dann hat* $f$ *höchstens* $n$ *Nullstellen.*

*Beweis:* Die Aussage stimmt für $n = 1$: ein Polynom der Form $\alpha_1 x + \alpha_2$ hat, wenn $\alpha_1 \neq 0$, nur die Nullstelle $-\alpha_2 \cdot (\alpha_1)^{-1}$.

Wir nehmen nun an, dass $n \geq 1$ ist, und dass jedes Polynom vom Grad $n$ höchstens $n$ Nullstellen hat. Wir zeigen, dass dann jedes Polynom vom Grad $n + 1$ höchstens $n + 1$ Nullstellen haben kann. Sei dazu $f$ ein Polynom vom Grad $n + 1$. Wenn $f$ keine Nullstellen hat, dann sind wir fertig, denn"keine Nullstellen" heißt natürlich auch "weniger als $n + 2$ Nullstellen". Wenn $f$ zumindest eine Nullstelle hat, dann wählen wir eine Nullstelle $\alpha$. Wir können dann ein Polynom $g$ vom Grad $n$ finden, sodass

$$f = (x - \alpha) \cdot g.$$

Sei nun $\beta$ eine Nullstelle von $f$ mit $\beta \neq \alpha$. Dann gilt $\overline{f}(\beta) = (\beta - \alpha) \cdot \overline{g}(\beta)$. Also gilt $0 = (\beta - \alpha) \cdot \overline{g}(\beta)$. Wegen $\beta - \alpha \neq 0$ gilt $\overline{g}(\beta) = 0$. Das Element $\beta$ ist daher eine Nullstelle von $g$.

Da wir angenommen haben, dass jedes Polynom vom Grad $n$ höchstens $n$ Nullstellen hat, hat $g$ höchstens $n$ Nullstellen. Jede Nullstelle von $f$ ist entweder gleich $\alpha$ oder unter diesen $n$ Nullstellen von $g$. Somit hat $f$ höchstens $n + 1$ Nullstellen. ■

## 5. Körper aus Polynomringen

Sei $f$ ein Polynom in $K[x]$. Für $a, b \in K[x]$ definieren wir

$$a \equiv b \pmod{f},$$

falls $f | a - b$. Das ist genau dann der Fall, wenn $a \bmod f = b \bmod f$. Wir definieren

$$[a]_f := \{a + q \cdot f \mid q \in K[x]\}.$$

Sei $K[x]/f$ definiert durch

$$K[x]/f := \{[a]_f \mid a \in K[x]\}.$$

Auf $K[x]/f$ definieren wir $+, -, \cdot$ durch

$$\begin{aligned} [a]_f + [b]_f &:= [a + b]_f \\ [a]_f - [b]_f &:= [a - b]_f \\ [a]_f \cdot [b]_f &:= [a \cdot b]_f. \end{aligned}$$

SATZ 1.20. *Sei* $\mathbf{K}$ *ein Körper, und sei* $f \in K[x]$. *Dann ist* $\left(K[x]/f, +, -, \cdot, [0]_f, [1]_f\right)$ *ein Ring mit Eins.*

SATZ 1.21. *Sei* $\mathbf{K}$ *ein Körper,* $f \in K[x]$ *irreduzibel über* $\mathbf{K}$. *Dann ist* $\mathbf{K}[x]/f$ *ein Körper.*