Notizen zum ersten Tutorium

Jendrik Stelzner

25. Mai 2017

1 Zur Definition des Polynomrings

Es sei R ein kommutativer Ring. Auf der Menge der endlichen Folgen auf R

$$R[\mathbb{N}] \coloneqq \{(a_n)_{n\in\mathbb{N}} \mid a_i \in R \text{ für alle } i \in \mathbb{N}\,, a_i = 0 \text{ für fast alle } i \in \mathbb{N}\,\} \tag{D}$$

wird eine Addition

$$(a_n)_{n\in\mathbb{N}} + (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}} \quad \text{mit} \quad c_i = a_i + b_i \text{ für alle } i \in \mathbb{N} \tag{A}$$

und eine Multiplikation

$$(a_n)_{n\in\mathbb{N}} \cdot (b_n)_{n\in\mathbb{N}} = (c_n)_{n\in\mathbb{N}} \quad \text{mit} \quad c_i = \sum_{j=0}^{i} a_j b_{i-j} \text{ für alle } i \in \mathbb{N} \tag{M}$$

definiert. Zusammen mit dieser Addition und Multiplikation ist $R[\mathbb{N}]$ ein kommutativer Ring. Das Einselement ist gegeben durch $1_{R[\mathbb{N}]} = (1, 0, 0, \dots)$.

Wir führen nun die Notation $t \coloneqq (0, 1, 0, 0, \dots)$ ein. Induktiv ergibt sich für alle $n \geq 0$, dass

$$\begin{aligned}
t^0 &= (1, 0, 0, \dots), \\
t^1 &= (0, 1, 0, 0, \dots), \\
t^2 &= (0, 0, 1, 0, 0, \dots), \\
&\vdots \\
t^n &= (0, \dots, 0, 1, 0, 0, \dots),
\end{aligned}$$

dass also $t^n = (\delta_{ni})_{i\in\mathbb{N}}$. Für alle $r, s \in R$ gilt

$$(r, 0, 0, \dots) + (s, 0, 0, \dots) = (r + s, 0, 0, \dots)$$

und

$$(r, 0, 0, \dots) \cdot (s, 0, 0, \dots) = (r \cdot s, 0, 0, \dots).$$

Wir können deshalb R mit dem Unterring

$$\{(r, 0, 0, \dots) \mid r \in R\} \subseteq R[\mathbb{N}]$$

identifzieren. Für alle $r \in R$ und $(a_0, \dots, a_n, 0, 0, \dots) \in R[\mathbb{N}]$ git dann, dass

$$\begin{aligned} r \cdot (a_0, a_1, \dots, a_n, 0, 0, \dots) &= (r, 0, 0, \dots) \cdot (a_0, \dots, a_n, 0, 0, \dots) \\ &= (ra_0, \dots, ra_n, 0, 0, \dots). \end{aligned} \tag{S}$$

Damit ergibt sich nun für jedes $(a_0, \dots, a_n, 0, 0, \dots) \in R[\mathbb{N}]$, dass

$$\begin{aligned} &(a_0, a_1, \dots, a_n, 0, 0, \dots) \\ &= (a_0, 0, 0, \dots) + (0, a_1, 0, 0, \dots) + \dots + (0, \dots, 0, a_n, 0, 0, \dots) \\ &= a_0(1, 0, 0, \dots) + a_1(0, 1, 0, 0, \dots) + \dots + a_n(0, \dots, 0, 1, 0, 0, \dots) \\ &= a_0 t^0 + a_1 t^1 + \dots + a_n t^n = \sum_{i=0}^{n} a_i t^i. \end{aligned}$$

Da $a_i = 0$ für alle $i > n$ gilt, lässt sich statt $\sum_{i=0}^{n} a_i t^i$ auch $\sum_{i=0}^{\infty} a_i t^i$ schreiben. Anstelle von (D) schreibt man nun

$$R[t] = \left\{ \sum_{i=0}^{\infty} a_i t^i \;\middle|\; a_i \in R \text{ für alle } i \in \mathbb{N}\,, a_i = 0 \text{ für fast alle } i \in \mathbb{N} \right\}. \tag{D'}$$

Die Addition (A) ist in dieser Schreibweise durch

$$\left(\sum_{i=0}^{\infty} a_i t^i \right) + \left(\sum_{i=0}^{\infty} b_i t^i \right) = \sum_{i=0}^{\infty} (a_i + b_i) t^i \tag{A'}$$

gegeben, und die Multiplikation (M) durch

$$\left(\sum_{i=0}^{\infty} a_i t^i \right) \cdot \left(\sum_{i=0}^{\infty} b_i t^i \right) = \sum_{i=0}^{\infty} \left(\sum_{j=0}^{i} a_i b_{j-i} \right) t^i = \sum_{i,j=0}^{\infty} a_i b_j t^{i+j}. \tag{M'}$$

Für $r \in R$ und $\sum_{i=0}^{\infty} a_i t^i \in R[t]$ ist (S) gegeben durch

$$r \cdot \left(\sum_{i=0}^{\infty} a_i t^i \right) = \sum_{i=0}^{\infty} (r a_i) t^i. \tag{S'}$$

Bemerkung. • Man bezeichnet das obige Element t as „Variable“.

- Statt „t“ lassen sich auch andere Buchstaben verwenden; beliebt sind T, x, X, y und Y.
- Die Multiplikation auf $R[t]$ ist eindeutig dadurch bestimmt, dass
  1. $t^i \cdot t^j = t^{i+j}$ für alle $i, j \in \mathbb{N}$,

2. $r \cdot (f \cdot g) = (r \cdot f) \cdot g = f \cdot (r \cdot g)$ für alle $r \in R$ und $f, g \in R[t]$,
3. Die Multiplikation ist distributiv in beiden Argumenten.

- Ist K ein Körper, so definiert (S') eine Skalarmultiplikation von K auf $K[t]$, die zu einer K-Vektorraumstruktur auf $K[t]$ führt. Eine K-Basis von $K[t]$ ist dann durch die Familie $(t^n)_{n\in\mathbb{N}}$ gegeben.

2 Polynomdivision, Hauptideale und größte gemeinsame Teiler

2.1 Teilbarkeit

Definition 1. Es sei R ein kommutativer Ring und es seien $a, b \in R$. Dann ist a ein *Teiler* von b, bzw. *a teilt b*, falls es $c \in R$ mit $b = ac$ gibt. Man schreibt dann $a \mid b$.

Definition 2. Es sei R eine kommutativer Ring, und es seien $a, b \in R$. Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* von a und b, falls

1. d ist ein gemeinsamer Teiler von a und b, d.h. es gilt $d \mid a$ und $d \mid b$ und

2. für jedes $d' \in R$ mit $d' \mid a$ und $d' \mid b$ gilt $d' \mid d$.

2.2 Polynomdivision

Von nun an sei K ein Körper.

Satz 3 (Polynomdivision, bzw. Teilen mit Rest). Es seien $f, g \in K[t]$ mit $g \neq 0$. Dann gibt es eindeutige Polynome $q, r \in K[t]$ mit

1. $\deg(r) < \deg(g)$ und

2. $f = qg + r$.

Beweis. • Wir zeigen zunächst die Eindeutigkeit:
Es seien $q, q', r, r' \in K[t]$ mit $\deg(r), \deg(r') < \deg(g)$ und $qg + r = f = q'g + r'$. Dann gilt

$$(q - q')g = r' - r, \tag{1}$$

Zum einen gilt dabei, dass

$$\deg(r' - r) \leq \max\{\deg(r'), \deg(-r)\} = \max\{\deg(r'), \deg(r)\} < \deg(g),$$

und zum anderen gilt

$$\deg((q - q')g) = \deg(q - q')\deg(g).$$

Daraus folgt, dass $\deg(q - q')\deg(g) < \deg(g)$ gilt. Somit muss $\deg(q - q') < 0$ gelten, also $\deg(q - q') = -\infty$ und deshalb $q - q' = 0$. Aus (1) folgt damit, dass auch $r' - r = 0$ gilt.

- Wir zeigen nun die Existenz per Induktion über $n \coloneqq \deg f$. Dabei gilt $m \coloneqq \deg g \geq 0$, da $g \neq 0$ gilt.

  Als Induktionsanfang dient der Fall $n < m$. Dann lässt sich $q = 0$ und $r = f$ wählen.

  Es sei nun $n \geq m$, und es seien $f = a_n t^n + \sum_{i=0}^{n-1} a_i t^i$ und $g = b_m t^m + \sum_{j=0}^{m-1} b_j t^j$, wobei $b_m \neq 0$. Die beiden Polynome f und $\frac{a_n}{b_m} t^{n-m} g$ haben dann den gleichen Grad (hierfür sorgt der Faktor t^{n-m}) sowie den gleichen Leitkoeffizienten (hierfür sorgt der Faktor $\frac{a_n}{b_m}$). In der Differenz $f - \frac{a_n}{b_m} t^{n-m} g$ löschen sich diese Leitkoeffizieten daher aus, weshalb

  $$\deg\left(f - \frac{a_n}{b_m} t^{n-m} g\right) < \deg(f)$$

  gilt. Nach Induktionsvoraussetzung gibt es deshalb $q, r \in K[t]$ mit $\deg(r) < \deg(g)$, so dass

  $$f - \frac{a_n}{b_m} t^{n-m} g = qg + r,$$

  gilt, und somit auch

  $$f = \left(\frac{a_n}{b_m} t^{n-m} + q\right) g + r.$$

  Dies zeigt die Existenz. □

Bemerkung 4. Der obige Beweis von Satz 3 liefert ein konstruktives Verfahren zur Berechnung von q und r.

2.3 Hauptideale

Wir zeigen im Folgenden mithilfe der Polynomdivision den folgenden Satz:

Satz 5. Je zwei Polynome $f, g \in K[t]$ besitzen einen größten gemeinsamen Teiler $d \in K[t]$, und es gibt $a, b \in K[t]$ mit $d = af + bg$.

Wir führen einen Beweis mithilfe von Idealen.

Definition 6. Eine Teilmenge $I \subseteq R$ eines kommutativen Rings R heißt *Ideal* falls I eine Untergruppe der additiven Gruppe von R ist, und $rx \in I$ für alle $r \in R$ und $x \in I$ gilt.

Beispiel 7. Es sei R ein kommutativer Ring.

1. Für jedes $a \in R$ ist $(a) = Ra \coloneqq \{ra \mid r \in R\}$ ein Ideal in R. Man bezeichnet ein Ideal dieser Form als *Hauptideal*.

2. Sind $I, J \subseteq R$ zwei Ideale, so ist auch $I + J \coloneqq \{x + y \mid x \in I, y \in J\}$ ein Ideal in R. Dies ist das kleinste Ideal in R, dass die beiden Ideale I und J enthält.

3. Induktiv folgt, dass für alle Ideale $I_1, \dots, I_n \subseteq R$ auch

$$I_1 + \dots + I_n = \{x_1 + \dots + x_n \,|\, x_1 \in I_1, \dots, x_n \in I_n\}$$

   ein Ideal in R ist.

   (Alternativ lässt sich auch direkt Nachrechnen, dass für jede Familie $(I_\lambda)_{\lambda\in\Lambda}$ von Idealen $I_\lambda \subseteq R$ die Summe

$$\sum_{\lambda\in\Lambda} I_\lambda = \left\{ \sum_{\lambda\in\Lambda} x_\lambda \,\middle|\, x_\lambda \in I_\lambda \text{ für alle } \lambda \in \Lambda, x_\lambda = 0 \text{ für fast alle } \lambda \in \Lambda \right\}$$

   ein Ideal in R ist. Dies ist das kleinste Ideal in R, dass alle I_λ enhält.)

4. Für alle $a_1, \dots, a_n$ ist

$$(a_1, \dots, a_n) \coloneqq (a_1) + \dots + (a_n) = \{r_1 a_1 + \dots + r_n a_n \,|\, r_1, \dots, r_n \in R\}$$

   ein Ideal in R.

Proposition 8. Jedes Ideal $I \subseteq K[t]$ ist von der Form $I = (f)$ für ein $f \in I$, d.h. jedes Ideal in $K[t]$ ist ein Hauptideal.

Beweis. Ist $I = \{0\}$, so lässt sich $f = 0$ wählen. Wir betrachten daher im Folgenden nur den Fall $I \neq \{0\}$.

Es sei $f \in I$ mit $f \neq 0$ von minimalen Grad. Dann gilt auch $af \in I$ für alle $a \in K[t]$, und somit $(f) \subseteq I$. Ist andererseits $g \in I$, so gibt es nach Satz 3 Polynome $q, r \in K[t]$ mit $\deg(r) < \deg(f)$ und $g = qf + r$. Dann gilt $r = g - qf \in I$. Wegen der Gradminimalität von f muss bereits $r = 0$ gelten, und somit $g = qf \in (f)$. □

Bemerkung 9. Für einen kommutativen Ring R sind die folgenden Bedingungen äquivalent:

1. R ist ein Körper.

2. Es gilt $R[t] \neq 0$ und in $R[t]$ ist ein „Teilen mit Rest“ wie in Satz 3 möglich, d.h. für alle $f, g \in R[t]$ mit $g \neq 0$ gibt es $q, r \in R[t]$ mit $\deg(r) < \deg(g)$ und $f = qg + r$ (die Eindeutigkeit von q und r wird hier nicht gefordert).

3. Der Ring $R[t]$ ist ein Integritätsbereich und jedes Ideal $I \subseteq R[t]$ ist ein Hauptideal.

Insbesondere lässt sich an den ringtheoretischen Eigenschaften des Polynomrings $R[t]$ schon erkennen, ob R selbst ein Körper ist.

Wir können nun den größten gemeinsamen Teiler zweier Polynome idealtheoretisch beschreiben, und erhalten als Korollar einen Beweis für Satz 5.

Lemma 10. Es sei R ein kommutativer Ring, und es seien $f, g \in R$. Gibt es $d \in R$ mit $(f, g) = (d)$, so ist d ein größter gemeinsamer Teiler von f und g.

Beweis. Da $f, g \in (f, g) = (d)$ gilt, gibt es $a, b \in R$ mit $f = ad$ und $g = bd$, weshalb $d \mid f$ und $d \mid g$ gilt. Andererseits folgt aus $d \in (d) = (f, g)$, dass es $a, b \in R$ mit $d = af + bg$ gibt. Ist $d' \in R$ mit $d' \mid f$ und $d' \mid g$, so gilt deshalb auch $d' \mid (af + bg) = d$. □

Beweis von Satz 5. Nach Proposition 8 gibt es $d \in K[t]$ mit $(f, g) = (d)$. Nach Lemma 10 ist d ein größter gemeinsamer Teiler von f und g. Da $d \in (d) = (f, g)$ gilt, gibt es $a, b \in K[t]$ mit $d = af + bg$. □

Bemerkung 11. 1. Sind $d, d' \in K[t]$ zwei größte gemeinsame Teiler von $f, g \in K[t]$, so gibt es ein $\lambda \in K$, $\lambda \neq 0$ mit $d' = \lambda d$. Man spricht daher häufig von *dem* größten gemeinsamen Teiler zweier Polynome, und bezeichnet diesen mit $\mathrm{ggT}(f, g)$.

2. Da es in $K[t]$ eine Division mit Rest gibt (Satz 3) lässt sich mithilfe des euklidischen Algorithmus ein größter gemeinsamer Teiler von $f, g \in K[t]$ berechnen, sowie entsprechende $a, b \in K[t]$ mit $\mathrm{ggT}(f, g) = af + bg$.

Bemerkung 12. Auch in $\mathbb{Z}$ ist eine Division mit Rest möglich, d.h. für alle $n, m \in \mathbb{Z}$ mit $m \neq 0$ gibt es eindeutige $q, r \in \mathbb{Z}$ mit $n = qm + r$; dies lässt sich analog zu Satz 3 zeigen, wobei man anstelle des Grades deg mit dem Betrag $|\cdot|$ arbeitet. Analog zu Proposition 8 lässt sich deshalb zeigen, dass jedes Ideal $I \subseteq \mathbb{Z}$ von der Form $I = (n)$ für ein $n \in \mathbb{Z}$ ist.