Zu §13: Polynomringe

Wir alle "kennen" Polynome der Form

$$f = a_0 + a_1 T^1 + a_2 T^2 + \ldots + a_m T^m$$

mit reellen Koeffizienten a_k und einer "Unbestimmten" T, für die wir reelle (und sogar komplexe) Zahlen einsetzen können. Polynome lassen sich addieren und multiplizieren, sie bilden einen Ring. Bei zwei gleichen Polynomen können wir Koeffizientenvergleich vornehmen, d.h. ein Polynom ist eindeutig durch die Folge $(a_0, a_1, \ldots, a_m)$ der Koeffizienten bestimmt. Wir wollen im folgenden Polynome mit Koeffizienten aus einem beliebigen kommutativen Ring definieren und zeigen, daß sie wieder einen Ring bilden.

Es sei $R \neq 0$ ein kommutativer Ring und

$$F(R) := \{\, (a_k)_{k\in\mathbb{N}_0} \,|\, \forall\, k \in \mathbb{N}_0 : a_k \in R \,\}$$

die Menge aller abzählbaren Folgen $(a_0, a_1, a_2, \ldots)$ von Elementen aus R. Die Gleichheit zweier solcher Folgen ist "gliedweise" erklärt, d.h.

$$(a_k) = (b_k) \;:\; \Longleftrightarrow \quad a_k = b_k \;\text{ für alle } k \in \mathbb{N}_0$$

Da ein Polynom immer nur endlich viele Koeffizienten $\neq 0$ besitzt, betrachten wir in $F(R)$ die Teilmenge der "endlichen" Folgen:

$$F^e(R) := \{\, (a_k)_{k\in\mathbb{N}_0} \,|\, (a_k)_{k\in\mathbb{N}_0} \in F(R), a_k = 0_R \text{ für fast alle } k \in \mathbb{N}_0 \,\}$$

Für $f = (a_k)_{k\in\mathbb{N}_0}$ definieren wir den **Träger** $I(f)$ durch

$$I(f) := \{\, k \,|\, k \in \mathbb{N}_0, a_k \neq 0_R \,\} \subseteq \mathbb{N}_0$$

Dann gilt für $f \in F(R)$: $f \in F^e(R) \iff I(f)$ ist endlich. Bezeichnet $0 = (0_R, 0_R, 0_R, \ldots)$ die konstante Folge Null, so gilt für $f \in F(R)$: $f = 0 \iff I(f) = \emptyset$

Im folgenden wollen wir auf $F^e(R)$ eine Ringstruktur definieren:

1.) Für $f \in F^e(R), f \neq 0$ existiert $\mathbf{grad}(f) := \max(I(f))$. Damit gilt

$$\forall\, k \in \mathbb{N}_0 \,:\, k > \operatorname{grad}(f) \quad \Longrightarrow \quad a_k = 0_R$$

2.) Definition einer Addition: Für $f = (a_k) \in F^e(R)$ und $g = (b_k) \in F^e(R)$ ist die Summe $f + g$ ("gliedweise") definiert durch

$$f + g := (a_k + b_k)$$

Man muß sich nun überlegen, daß $f + g$ wieder in $F^e(R)$ liegt:

Klar ist $f+g \in F(R)$. Es genügt zu zeigen, daß $I(f+g) \subseteq I(f) \cup I(g)$ gilt; denn dann ist $I(f+g)$ als Teilmenge einer endlichen Menge wieder endlich. Sei $k \in \mathbb{N}_0$ und gelte $k \notin I(f) \cup I(g)$. Dann folgt: $k \notin I(f)$ und $k \notin I(g) \implies a_k = 0_R$ und $b_k = 0_R \implies a_k + b_k = 0_R \implies k \notin I(f+g)$, d.h. $I(f + g) \subseteq I(f) \cup I(g)$.

Man erkennt nun leicht, daß $(F^e(R),+)$ eine abelsche Gruppe ist. Dabei ist die konstante Folge $0 \in F^e(R)$ das Nullelement, und das Negative von $f = (a_k) \in F^e(R)$ ist die Folge $-f = (-a_k) \in F^e(R)$. Außerdem ist die Addition assoziativ und kommutativ.

3.) Für $f, g, f+g \in F^e(R) \setminus \{0\}$ gilt $\operatorname{grad}(f+g) \leq \max(\operatorname{grad}(f), \operatorname{grad}(g))$

Setze $m := \operatorname{grad}(f)$ und $n := \operatorname{grad}(g)$. Für einen Index $k > \max(m,n)$ gilt dann $k > m$ und $k > n$. Daraus folgt dann $a_k = b_k = 0_R$ und damit $a_k + b_k = 0_R$, woraus sich die Beh. ergibt.

4.) Definition einer Multiplikation:
Für $f = (a_k) \in F^e(R)$ und $g = (b_k) \in F^e(R)$ ist das **Cauchy–Produkt** definiert durch

$$f \cdot g := (c_k)_{k \in \mathbb{N}_0} \quad \text{mit} \quad c_k = \sum_{\substack{i,j \in \mathbb{N}_0 \\ i+j=k}} a_i b_j \;=\; \sum_{i=0}^{k} a_i b_{k-i}$$

Man muß sich wieder überlegen, daß $f \cdot g$ in $F^e(R)$ liegt:

Klar ist $f \cdot g \in F(R)$. Im Falle $f = 0$ oder $g = 0$ gilt auch $f \cdot g = 0 \in F^e(R)$. Seien deshalb $f \neq 0$ und $g \neq 0$. Setze $m := \operatorname{grad}(f)$, $n := \operatorname{grad}(g)$ und $r := m + n$. Dann folgt $c_k = 0_R$ für alle $k > r$. Aus $i + j = k > r$ ergibt sich nämlich $i > m$ oder $j > n$ und daraus $a_i = 0_R$ oder $b_j = 0_R$, also $a_i \cdot b_j = 0_R$. Damit sind alle Summanden in der Summe für c_k gleich 0_R, c_k selbst ist also Null. Da $I(f \cdot g)$ endlich ist $(|I(f \cdot g)| \leq r = m + n)$, ist $f \cdot g \in F^e(R)$ bewiesen.

Wir halten als Ergebnis fest:

5.) Für $f, g, f \cdot g \in F^e(R) \setminus \{0\}$ gilt $\operatorname{grad}(f \cdot g) \leq \operatorname{grad}(f) + \operatorname{grad}(g)$

Wir führen für einen beliebigen Ring $R \neq 0$ das **Kronecker–Symbol** δ_{ik} ein:

$$\delta_{ik} = \begin{cases} 1_R & \text{für } i = k \\ 0_R & \text{für } i \neq k \end{cases}$$

Dann ist $1 = (1_R, 0_R, 0_R, \ldots) = (\delta_{0k})_{k \in \mathbb{N}_0} \in F^e(R)$ das Einselement; denn
$1 \cdot f = (c_k)$ mit $c_k = \sum_{i+j=k} \delta_{0i} a_j = 1_R a_k = a_k \quad (\forall\, k \in \mathbb{N}_0)$, also $1f = f$ und analog $f1 = f$.
Die Multiplikation ist assoziativ und kommutativ, und es gilt das Distributive Gesetz, so daß $F^e(R)$ insgesamt ein kommutativer Ring ist.

Abschließend untersuchen wir noch den Zusammenhang zwischen R und $F^e(R)$. Dazu stellen wir fest, daß die Abbildung

$$\alpha_R : R \longrightarrow F^e(R) \;,\; a \longmapsto (a, 0_R, 0_R, 0_R, \ldots)$$

ein injektiver Ringhomomorphismus ist. Die Verträglichkeit mit der Addition ist klar, und das Cauchy–Produkt von $\alpha_R(a)$ und $\alpha_R(b)$ ist gerade $\alpha_R(a \cdot b)$. Außerdem ist $\alpha_R(1_R) = 1$. Die Injektivität ergibt sich sofort.

Identifizieren wir $a \in R$ mit $\alpha_R(a) \in F^e(R)$, so können wir R als Unterring von $F^e(R)$ auffassen. Zusammenfassend haben wir bewiesen:

(13.20) SATZ: Für jeden kommutativen Ring $R \neq 0$ ist $F^e(R)$ ein kommutativer Ring, der einen zu R isomorphen Unterring enthält.

Wir werden nun sehen, daß sich die Elemente aus $F^e(R)$ in gewohnter Weise wie Polynome darstellen lassen. Dazu definieren wir:

6.) Das Element $T := (0_R, 1_R, 0_R, 0_R, \ldots) \in F^e(R)$ heißt **Unbestimmte über** R.

Wir bilden nun die Potenzen von T bzgl. der Cauchy–Multiplikation:

$$\begin{aligned} T^0 &= (1_R, 0_R, 0_R, 0_R, 0_R, \ldots) \quad = 1 \\ T^1 &= (0_R, 1_R, 0_R, 0_R, 0_R, \ldots) \quad = T \\ T^2 &= (0_R, 0_R, 1_R, 0_R, 0_R, \ldots) \end{aligned}$$

Und allgemein für $n \in \mathbb{N}_0$

7.) $T^n = (0_R, \ldots, 0_R, 1_R, 0_R, 0_R, \ldots) = (\delta_{nk})_{k \in \mathbf{N}_0}$, wobei 1_R an der $(n+1)$–ten Stelle steht.

Für $a \in R$ gilt $\quad aT^k = \alpha(a)T^k \;=\; (a, 0_R, 0_R, 0_R, \ldots) \cdot (\underbrace{0_R, \ldots, 0_R}_{k-mal}, 1_R, 0_R, 0_R, \ldots) =$

$$(\underbrace{0_R, \ldots, 0_R}_{k-mal}, a\,, 0_R, 0_R, \ldots)$$

Sei nun $f = (a_k) \in F^e(R)$. Dann existiert ein $m \in \mathbb{N}_0$ mit $a_k = 0_R$ für alle $k > m$, d.h.

$$\begin{aligned} f = \;& (a_0, a_1, \ldots, a_m, 0_R, 0_R, \ldots) \\ =\; & (a_0, , 0_R, 0_R, \ldots) + (0_R, a_1, 0_R, 0_R, \ldots) + \ldots + (0_R, \ldots, 0_R, a_m, 0_R, 0_R, \ldots) \\ =\; & a_0T^0 + a_1T^1 + a_2T^2 + \ldots + a_mT^m \end{aligned}$$

f läßt sich also in der gewohnten Form darstellen als ein **Polynom**

$$f \;=\; \sum_{k=0}^{m} a_k T^k$$

Die Koeffizienten in dieser Darstellung sind eindeutig bestimmt. Sei zunächst $f \neq 0$ und gelte:

$f = \sum_{i=0}^{m} a_i T^i \;=\; (a_0, a_1, \ldots, a_m, 0_R, 0_R, \ldots)$ mit $a_m \neq 0_R$

$f = \sum_{j=0}^{n} b_j T^j \;=\; (b_0, b_1, \ldots, b_n, 0_R, 0_R, \ldots)$ mit $b_n \neq 0_R$

Dann ergibt sich $m = \operatorname{grad}(f) = n$ und $a_i = b_i$ für alle $i = 0, 1, 2, \ldots, m$.

Im Falle $f = 0$ folgt: $0 = f = \sum_{k=0}^{m} a_k T^k = (a_0, a_1, \ldots, a_m, 0_R, 0_R, \ldots)$ und damit $\quad a_i = 0_R$ für alle $i = 0, 1, ..., m$.

Die Rechenoperationen schreiben sich jetzt in der Form:

$$f = \sum_{i=0}^{m} a_i T^i \quad , \quad g = \sum_{j=0}^{n} b_j T^j$$

8.) $f + g \;=\; \sum\limits_{k=0}^{\max(m,n)} (a_k + b_k)\, T^k$ mit $a_k = 0_R$, falls $k > m$ und $b_k = 0_R$, falls $k > n$.

9.) $f \cdot g \;=\; \sum\limits_{k=0}^{m+n} \left(\sum\limits_{i+j=k} a_i b_j \right) T^k$

Außerdem können wir eine Skalarmultiplikation mit Elementen aus dem Ring R definieren:

10.) $af \;=\; \sum\limits_{i=0}^{m} (aa_i)\, T^i \quad (a \in R)$

Zusammenfassend haben wir bewiesen:

(13.21) SATZ: R sei ein kommutativer Ring $\neq 0$. Dann läßt sich jedes Element $f \in F^e(R) \setminus \{0\}$ in der Form

$$f \;=\; \sum_{k=0}^{m} a_k T^k$$

mit eindeutig bestimmten Koeffizienten $a_k \in R$ $(k = 0, 1, \ldots m)$ und $a_m \neq 0_R$ darstellen. Dabei ist $m = \mathrm{grad}(f)$.

(13.22) Bezeichnungen: a) Die Elemente aus $F^e(R)$ heißen **Polynome in einer Unbestimmten T über dem Ring** R.

b) Der Ring $F^e(R)$ heißt **Polynomring in einer Unbestimmten T über dem Ring** R und wird mit $\boldsymbol{R[T]}$ bezeichnet.

c) Ein Polynom, dessen sämtliche Koeffizienten 0_R sind, heißt das **Nullpolynom**. Es hat **keinen** Grad.

d) Ist $f \neq 0$ ein Polynom vom Grade m, so heißt der Koeffizient a_m von T^m der **Leitkoeffizient** von f. Ein Polynom, dessen Leitkoeffizient 1_R ist, heißt **normiert**.

Bemerkung: Die Bildung des Polynomringes läßt sich iterieren: Ist R ein kommutativer Ring, so ist auch $S := R[T_1]$ ein kommutativer Ring mit $1_S \neq 0_S$ (Hier ist die Unbestimmte mit T_1 bezeichnet). Über diesem Ring S können wir nun wieder den Polynomring in einer Unbestimmten T_2 bilden:

$$S[T_2] \;=\; (R[T_1])[T_2] \;=:\; R[T_1, T_2]$$

$R[T_1, T_2]$ heißt Polynomring in zwei Unbestimmten über dem Ring R. Die Elemente von $S[T_2]$ sind Polynome in T_2 mit Koeffizienten aus dem Ring $S = R[T_1]$. Allgemein ist

$$R[T_1, T_2, \ldots, T_{n-1}, T_n] := (R[T_1, T_2, \ldots, T_{n-1}])[T_n]$$

der Polynomring in den n Unbestimmten $T_1, T_2, \ldots, T_{n-1}, T_n$.

(13.23) LEMMA: R sei ein kommutativer Ring mit $1_R \neq 0_R$. Dann gilt für Polynome $f, g \in R[T] \setminus \{0_R\}$:

a) $\text{grad}(f+g) \leq \max(\text{grad}(f), \text{grad}(g))$, falls $f+g \neq 0$.

b) $\text{grad}(f \cdot g) \leq \text{grad}(f) + \text{grad}(g)$, falls $f \cdot g \neq 0$

c) Ist R ein **IB**, so folgt $\text{grad}(f \cdot g) = \text{grad}(f) + \text{grad}(g)$

d) R IB $\iff$ $R[T]$ IB

e) R IB $\implies$ $(R[T])^\star = R^\star$.

Bew: **a)** folgt aus 3.) **b)** folgt aus 5.)

c) Seien $f = \sum_{i=0}^{m} a_i T^i$, $g = \sum_{k=0}^{n} b_k T^k$ mit $a_m \neq 0, b_n \neq 0$, also $\text{grad}(f) = m, \text{grad}(g) = n$. Nach 5.) ist dann

$$f \cdot g \;=\; a_0 b_0 + \ldots + (a_m b_n) T^{m+n}$$

Da R nach Voraussetzung ein IB ist, folgt $a_m b_n \neq 0$.
Damit ist $\text{grad}(f \cdot g) = m + n = \text{grad}(f) + \text{grad}(g)$.

d) "$\Longrightarrow$" Seien $f, g \in R[T] \setminus \{0\}$. Dann ist nach c) $\text{grad}(f \cdot g) = \text{grad}(f) + \text{grad}(g) \geq 0$, also $f \cdot g \neq 0$. Damit ist $R[T]$ ein IB.

Die Umkehrung "$\Longleftarrow$" ist klar, da R als Unterring eines IB's selbst wieder ein IB ist.

e) $R^\star \subseteq (R[T])^\star$ ist klar, da R ein Unterring von $R[T]$ ist. Sei umgekehrt $f \in (R[T])^\star$. Dann gibt es ein $g \in R[T]$ mit $f \cdot g = 1$. Mit c) folgt $0 = \text{grad}(1) = \text{grad}(f \cdot g) = \text{grad}(f) + \text{grad}(g)$, also $\text{grad}(f) = \text{grad}(g) = 0$, d.h. $f, g \in R$ und $f \in R^\star$. □

(13.24) SATZ: Division mit Rest in $R[T]$

R sei ein kommutativer Ring mit $1_R \neq 0_R$ und $g \in R[T]$ ein Polynom, dessen Leitkoeffizient eine Einheit in R ist. Dann gibt es zu jedem Polynom $f \in R[T]$ eindeutig bestimmte Polynome $q, r \in R[T]$, wobei gilt:

$$f = qg + r \;\text{ mit }\; r = 0 \text{ oder } \text{grad}(r) < \text{grad}(g)$$

Bew: Existenz:
Im Falle $f = 0$ setze man $q = r = 0$. Für den Fall $f \neq 0$ seien

$$f = \sum_{i=0}^{m} a_i T^i \;\; (a_m \neq 0) \;,\; g = \sum_{k=0}^{n} b_k T^k \;\; (b_n \in R^\star)$$

Wir führen nun Induktion nach $m = \text{grad}(f)$:

$m = 0$ $f = a_0 \neq 0$

1. Fall $\text{grad}(g) = 0 \implies f = \underbrace{(a_0 b_0^{-1})}_{=q} \underbrace{b_0}_{=g} + \underbrace{0}_{=r}$

2. Fall $\text{grad}(g) > 0 \implies f = 0 \cdot g + f$ mit $\text{grad}(f) = 0 < \text{grad}(g)$

(IV) Sei $m > 0$ beliebig und die Behauptung richtig für alle Polynome vom Grade $< m$

Sei $f \in R[T]$ mit $\text{grad}(f) = m$. Zu zeigen: f läßt sich durch g mit Rest teilen.

1. Fall $m = \text{grad}(f) < \text{grad}(g) = n$: $\quad f = 0g + f$

2. Fall $m = \text{grad}(f) \geq \text{grad}(g) = n$:

Sei

$$f_1 := (a_m b_n^{-1}) T^{m-n} g \in R[T]$$

Der Leitkoeffizient von f_1 ist $(a_m b_n^{-1}) b_n = a_m \neq 0$, daher $\text{grad}(f_1) = m$. Folglich $f - f_1 = 0$ oder $f - f_1$ hat einen Grad $< m$. Im ersten Fall sind wir fertig, im zweiten Fall gilt nach (IV)

$$f - f_1 \;=\; g \cdot q_1 + r \qquad (q_1, r \in R[T], r = 0 \text{ oder } \text{grad}(r) < \text{grad}(g))$$

$$f \;=\; f_1 + gq_1 + r \;=\; (\underbrace{a_m b_n^{-1} T^{m-n} + q_1}_{=:q \in R[T]}) \cdot g + r$$

Eindeutigkeit:

Es gelte außerdem $f = g \cdot \tilde{q} + \tilde{r}$ mit $\tilde{r} = 0$ oder $\text{grad}(\tilde{r}) < \text{grad}(g)$. Dann folgt

$$(q - \tilde{q})g = \tilde{r} - r$$

Annahme: $q - \tilde{q} \neq 0$. Da der Leitkoeffizient von g eine Einheit, und damit kein Nullteiler ist, folgt $(q - \tilde{q})g \neq 0$ und

$$\text{grad}((q - \tilde{q})g) = \text{grad}(q - \tilde{q}) + \text{grad}(g) \geq \text{grad}(g)$$

Also $\tilde{r} - r \neq 0$ und $\text{grad}(\tilde{r} - r) \geq \text{grad}(g)$. Ist eines der Polynome r oder $\tilde{r}$ das Nullpolynom (etwa $r = 0$), so folgt mit $\text{grad}(\tilde{r} - r) = \text{grad}(\tilde{r}) < \text{grad}(g)$ ein **Widerspruch**, sind dagegen beide Polynome $\neq 0$, so folgt mit $\text{grad}(\tilde{r} - r) \leq \max(\text{grad}(\tilde{r}), \text{grad}(r)) < \text{grad}(g)$ ein **Widerspruch**. Beide Polynome können wegen $\tilde{r} - r \neq 0$ nicht 0 sein.

Folglich $q - \tilde{q} = 0 \implies \tilde{q} = q$ und damit $\tilde{r} - r = 0$, also $\tilde{r} = r$.

Damit ist alles bewiesen. □