12. Polynomringe

Auch in diesem Kapitel sei R stets ein nicht-trivialer kommutativer Ring.

Für Mengen A, B sei ${}^{A}B$ die Menge aller Funktionen $f: A \to B$. Sei R ein Ring und sei

$$\mathcal{F}_R := \{ f \in {}^{\mathbb{N}}R : \exists n_f \in \mathbb{N}\ \forall k \geq n_f\ (f(k) = 0_R) \}.$$

Für $f, g \in \mathcal{F}_R$ definieren wir $f+g, f \cdot g \in \mathcal{F}_R$ wie folgt:

$$(f+g)(k) := f(k) +_R g(k)$$

$$(f \cdot g)(k) := \sum_{i=0}^{k} f(i) \cdot_R g(k-i)$$

Beachte: Für $m := \max\{n_f, n_g\}$ gilt für alle $k \geq 2m$:

$$(f \cdot g)(k) = 0_R, \text{ d.h. } f \cdot g \in \mathcal{F}_R.$$

- Die Funktionen "+" & "·" sind assoz., komm., und es gelten die Distributivgesetze.
- $0_{\mathcal{F}_R}(k) := 0_R$ (für alle k) ist Neutralelem. bzgl. "+".
- $1_{\mathcal{F}_R}(k) := \begin{cases} 1_R & \text{für } k=0, \\ 0_R & \text{sonst,} \end{cases}$ ist Neutralelement bzgl. "·".

Somit ist $(\mathcal{F}_R, 0_{\mathcal{F}_R}, 1_{\mathcal{F}_R}, +, \cdot)$ ein komm. Ring.

Sei nun X ein Symbol, das in R nicht vorkommt. Wir identifizieren nun $f \in \mathcal{F}_R$ mit $\sum_{i=0}^{\infty} f(i) \cdot X^i$, wobei wir üblicherweise nur die endlich vielen Terme $f(i) \cdot X^i$ aufschreiben, für die $f(i) \neq 0_R$ ist; ausser für $0_{\mathcal{F}_R}$, dafür schreiben wir 0_R. Weiter schreiben wir a_i für $f(i)$ und identifizieren X^0 mit 1_R und X^1 mit X.

$\rightsquigarrow$ Damit wird $\mathcal{F}_R$ zum <u>Polynomring</u> $R[X]$ in der <u>Unbestimmten</u> X.

Elemente von $R[X]$ sind somit von der Form

$$a_0 + a_1 \cdot X + a_2 \cdot X^2 + \ldots + a_n X^n \quad (\text{für ein } n \in \mathbb{N}).$$

<u>Bem.</u> Elemente in $R[X]$ werden addiert und multipliziert wie Polynome, denn es sind Polynome! [aber <u>keine</u> Polynomfunktionen!]

<u>Faktum 12.1</u> Die natürliche Inklusion $\iota : R \hookrightarrow R[X]$
$a \longmapsto a + 0 \cdot X + 0 \cdot X^2 + \ldots$
ist ein Ringhomom. und wir können R auffassen als Unterring von $R[X]$.

<u>Bew:</u> $\varphi(a+b) = a + b + 0 \cdot X + \ldots = (a + 0 \cdot X + \ldots) + (b + 0 \cdot X + \ldots)$
$= \varphi(a) + \varphi(b)$

und $\varphi(a \cdot b) = a \cdot b + 0 \cdot X + \ldots = (a + 0 \cdot X + \ldots) \cdot (b + 0 \cdot X + \ldots)$,

und es gilt $\varphi(1_R) = 1_R + 0 \cdot X + \ldots = 1_{R[X]}$

$\dashv$

<u>Def.</u> Ist S komm. Ring, $R \subseteq S$ ein Unterring von S, und $s_0 \in S$, so sei $R[s_0]$ der kleinste Unterring von S der R und s_0 enthält. [Beachte: $R[s_0]$ ist <u>kein</u> Polynomring]

<u>Proposition 12.2</u> $R[s_0] = \{ \tilde{s} \in S : \tilde{s} = a_0 + a_1 s + \ldots + a_n s^n$ mit $n \in \mathbb{N}$ und $a_i \in R \}$.

Damit ist $R[s_0]$ eindeutig bestimmt.

[Im Wesentlichen ersetzen wir im Polynomring $R[X]$ die Unbestimmte X durch s_0 und werten die Ausdrücke in S aus.]

<u>Beweis:</u>
- $R[s_0] \subseteq S$ ist ein Unterring von S der R und s_0 enthält. Beachte: $1_R \in R$ und damit auch $1_R s_0 = s_0 \in R[s_0]$.
- Ist $\tilde{S} \subseteq S$ ein Unterring mit $R \subseteq \tilde{S}$ und $s_0 \in \tilde{S}$, so muss gelten $R[s_0] \subseteq \tilde{S}$.

$\dashv$

<u>Bsp.</u> $\mathbb{Z}[i]$, $\mathbb{Z}[e]$, $\mathbb{Z}[-\frac{1}{2} + i \cdot \frac{\sqrt{3}}{2}]$