7 Polynome

7.1 Polynome einer Variablen

Sei R ein kommutativer unitärer Ring, und sei X ein noch nicht verwendetes Symbol.

Definition: Eine Abbildung der Form $f\colon R \to R$, $x \mapsto f(x) = \sum'_{i \geqslant 0} a_i x^i$, mit Koeffizienten $a_i \in R$ und fast allen $a_i = 0$, heisst eine *Polynomfunktion.*

Definition: Ein „formaler Ausdruck“ der Form $F(X) = \sum'_{i \geqslant 0} a_i X^i$, mit Koeffizienten $a_i \in R$ und fast allen $a_i = 0$, heisst ein *Polynom in X über R.* Für jedes solche F, jeden kommutativen unitären Ring R', der R enthält, und jedes Element $x \in R'$, ist der *Wert von F an der Stelle x* das Element

$$F(x) \;:=\; \boxed{\sum_{i \geqslant 0}{}' a_i x^i} \in R'.$$

Insbesondere induziert F eine Polynomfunktion $R' \to R'$, $x \mapsto F(x)$.

$f \rightsquigarrow \mathbb{R} \to \mathbb{R},\ x \mapsto f(x)$

Beispiel: Ein Polynom mit reellen Koeffizienten kann man auf ganz $\mathbb{C}$ auswerten.

$\mathbb{C} \to \mathbb{C},\ x \mapsto f(x).$

Vorsicht: Ist R endlich, so können verschiedene Polynome über R dieselbe Polynomfunktion $R \to R$ induzieren, z.B. die beiden Polynome 0 und $X^2 - X$ über $\mathbb{F}_2$. Es gibt aber immer einen R umgebenden Ring R', auf dem die induzierten Polynomfunktionen verschieden sind.

Definition: Für je zwei Polynome $F(X) = \sum'_{i\geqslant 0} a_i X^i$ und $G(X) = \sum'_{i\geqslant 0} b_i X^i$ und jedes $\lambda \in R$ setzen wir

$$\begin{array}{rcccl}
(F+G)(X) & := & F(X)+G(X) & := & \sum'_{i\geqslant 0} (a_i+b_i)\cdot X^i, \\
(F\cdot G)(X) & := & F(X)\cdot G(X) & := & \sum'_{i\geqslant 0} \left(\sum_{j=0}^{i} a_{i-j}b_j\right)\cdot X^i \\
(\lambda\cdot F)(X) & := & \lambda\cdot F(X) & := & \sum'_{i\geqslant 0} \lambda a_i X^i.
\end{array}$$

Proposition: Diese Operationen sind verträglich mit der Auswertung, das heisst, für alle $x \in R'$ wie oben gilt $(F+G)(x) = F(x)+G(x)$ und so weiter.

$F(x)\cdot G(x) = \sum_i a_i x^i \cdot \sum_k b_k x^k = \sum_{i,k} a_i b_k x^{i+k} = \sum_d \left(\sum_i a_i b_{d-i}\right)\cdot x^d$

Proposition-Definition: Die Menge $R[X]$ aller Polynome in X über R mit den obigen Operationen, dem *Nullpolynom* $0 = \sum'_{i\geqslant 0} 0\cdot X^i$ und dem *Einspolynom* $1 = \sum'_{i\geqslant 0} \delta_{i,0}\cdot X^i$ ist ein kommutativer unitärer Ring, genannt der *Polynomring in X über R.*

Ü.

Konstruktion: Ein Polynom $\sum'_{i\geqslant 0} a_i X^i$ anzugeben ist nach Definition äquivalent dazu, seine Koeffizienten anzugeben. Man kann den Polynomring daher konkret realisieren als die Menge aller Folgen $(a_i)_{i\geqslant 0}$ in R, die schliesslich Null werden, mit komponentenweiser Addition und skalarer Multiplikation sowie dem Produkt $(a_i)_i\cdot(b_i)_i := \left(\sum_{j=0}^{i} a_{i-j}b_j\right)_i$. Dabei repräsentieren die Folge $(0,0,\ldots)$ das Nullelement, die Folge $(1,0,0,\ldots)$ das Einselement, und die Folge $(0,1,0,0,\ldots)$ das Variablensymbol X.

$R[X] \cong R^{(\mathbb{Z}^{\geq 0})}$