

A-12 Der Ring der Polynome

Beobachtung:

Die Menge aller Polynome in x über einem Ring \mathcal{R} wird mit $\mathcal{R}[x]$ bezeichnet. Sie bildet selbst einen kommutativen Ring. Hierbei sind Addition und Multiplikation von $C(x) = \sum_{j=0}^n c_j x^j$ und $D(x) = \sum_{j=0}^m d_j x^j$ mit $c_n \neq 0 \neq d_m$ und $m \geq n$ definiert als

$$E(x) = C(x) + D(x) = \sum_{j=0}^m e_j x^j \quad \text{mit} \quad e_j = \begin{cases} c_j + d_j & \text{für } j \leq n \\ d_j & \text{für } n < j \leq m \end{cases}$$

und

$$E(x) = C(x) * D(x) = \sum_{j=0}^{n+m} e_j x^j \quad \text{mit} \quad e_j = \sum_{i=0}^j c_i * d_{j-i}$$

wie zuvor schreiben wir $\deg(C) = n$ und $\deg(D) = m$.



Mit der oben für das Nullpolynom getroffenen Vereinbarung gilt immer:

$$\begin{aligned} \deg(P \pm Q) &\leq \max(\deg(P), \deg(Q)), \\ \deg(P * Q) &= \deg(P) + \deg(Q), \end{aligned}$$

wobei

$$-\infty + n = -\infty = -\infty + (-\infty).$$

Beobachtung:

Ist \mathcal{R} ein Körper, so ist der Polynomring $\mathcal{R}[x]$ ein Integritätsbereich, der sich zum Körper der rationalen Funktionen (d.h. Quotienten von teilerfremden Polynomen) erweitern lässt (vergleiche Übergang $\mathbb{Z} \rightarrow \mathbb{Q}$). Damit ergibt sich die Frage nach der Division von Polynomen.

Von jetzt ab betrachten wir nur noch den Fall, wo \mathcal{R} ein Körper ist.



Lemma A.110

Im Ring $\mathcal{R}[x]$ gilt:

- (i) $P(x) = 0 = 0 \cdot x^0 + 0 \cdot x^1 + \dots$ **Nullelement**
- (ii) $P(x) = 1 = 1 \cdot x^0 + 0 \cdot x^1$ **Einsselement**
- (iii) Den Grad des Nullelementes setzt man zu $\deg(0) = -\infty$
- (iv) $\deg(P(x)) = 0$ genau dann wenn $P(x) = c_0 \in \mathcal{R} \wedge c_0 \neq 0$
- (v) Es gibt keine Nullteiler im Ring $\mathcal{R}[x]$ genau dann wenn \mathcal{R} selbst ein Integritätsbereich ist.



Satz A.111

Für jeden Körper \mathcal{R} ist $\mathcal{R}[x]$ ein **Euklidischer Ring**, d.h. für je zwei Elemente $a(x), b(x) \in \mathcal{R}[x]$ existieren Polynome $q(x) \in \mathcal{R}[x]$ und $r(x) \in \mathcal{R}[x]$, so dass

$$a(x) = b(x)q(x) + r(x) \quad \text{mit} \quad \deg(r(x)) < \deg(b(x))$$

Man schreibt dann wie im Fall $\mathbb{R} = \mathbb{N}$ auch

$$r(x) = a(x) \bmod b(x)$$

Bemerkung

Obiger Satz gilt in \mathbb{Z} mit $\deg(x) = |x|$, der gewöhnliche Betrag.



Beispiel A.112

$$(2x^5 + 5x^3 + x^2 + 7x + 1) = (2x^2 + 1) * (x^3 + 2x + 1/2) + (5x + 1/2)$$

Bemerkung:

Wie die Bezeichnung **Euklidischer Ring** andeutet, lässt sich in jedem solchem Ring der in Sektion **A-8** zunächst für natürliche Zahlen definierte Euklidische Algorithmus ohne jegliche Veränderung einsetzen. Daraus folgt wiederum die Eindeutigkeit der Primfaktorzerlegung.

Lemma A.114

Wie im Ring der ganzen Zahlen gilt für irreduzibles $c(x) \in \mathcal{R}[x]$ die Implikation

$$c(x)|(a(x) * b(x)) \implies c(x)|a(x) \vee c(x)|b(x)$$

Satz A.115

Ist \mathcal{R} ein Körper, so besitzt jedes Polynom $a(x) \in \mathcal{R}[x]$ eine Faktorisierung

$$a(x) = p_1(x) p_2(x) \dots p_m(x)$$

in irreduzible Polynome $p_j(x)$ für $j = 1 \dots m$.

Diese sind eindeutig bis auf konstante Faktoren, d.h. aus

$$a(x) = p'_1(x) \dots p'_m(x)$$

folgt (gegebenenfalls nach Umnummerierung)

$$p'_j(x) = \gamma_j p_j(x) \quad \text{mit} \quad \gamma_j \in \mathcal{R}.$$

Definition A.113 (Teilbarkeit in $\mathcal{R}[x]$)

- (i) Falls ein Polynom $0 \neq c(x) \in \mathcal{R}[x]$ eine Produktdarstellung

$$c(x) = a(x) * b(x) \quad \text{mit} \quad a(x), b(x) \in \mathcal{R}[x]$$

besitzt, heißen $a(x)$ und $b(x)$ **Teiler** von $c(x)$. Man schreibt dann wie üblich $a(x)|c(x)$ und $b(x)|c(x)$.

- (ii) Falls sowohl $a(x)$ wie $b(x)$ nicht konstant sind, d.h.

$$\begin{aligned} 0 < \deg(a(x)) < \deg(c(x)) \\ 0 < \deg(b(x)) < \deg(c(x)), \end{aligned}$$

dann nennt man $a(x)$ und $b(x)$ **echte Teiler** von $c(x)$.

- (iii) Falls $0 \neq c(x) \in \mathcal{R}[x]$ keinerlei echte Teiler besitzt, heißt es **prim** oder **irreduzibel**.

Beispiel A.116

$$x^3 - 1 = (x - 1) * (x^2 + x + 1), \quad \text{da } x^2 + x + 1 \text{ und } x - 1 \text{ irreduzibel.}$$

Beobachtung:

Mit $b(x) = x - x_0$ für $x_0 \in \mathcal{R}$ als lineares Polynom ergibt sich aus Satz A.111 für ein beliebiges Polynom $a(x)$ mit $\deg(a(x)) > 0$ die Darstellung

$$a(x) = q(x) * (x - x_0) + r_0 \quad \text{mit} \quad r_0 = a(x_0) \in \mathcal{R}.$$

Die letzte Aussage folgt durch Einsetzen, da das Residuum r_0 vom Grad $0 < 1 = \deg(b)$ sein muss.