## Unterringe

**Definition:** Sei $(R, +, \cdot)$ ein Ring mit Eins. Eine Teilmenge $S \subset R$ heißt Unterring von $R$ :$\Leftrightarrow$

a) $1 \in S$

b) $a + b \in S$ für alle $a, b \in S$

c) $-a \in S$ für alle $a \in S$

d) $a \cdot b \in S$ für alle $a, b \in S$

Falls $R$ sogar ein Körper ist und für alle $a \in S \setminus \{0\}$ das Inverse $a^{-1}$ auch in $S$ liegt, so ist $S$ ein Unterkörper (Teilkörper) von $R$.

**Bsp.:** $\mathbb{Z}$ sind Unterringe von $\mathbb{Q}, \mathbb{R}, \mathbb{C}$.
$\mathbb{Q}$ ist Teilkörper von $\mathbb{R}$ und $\mathbb{C}$, $\mathbb{R}$ Teilkörper von $\mathbb{C}$.

**Bemerkung:** Ähnlich wie bei den Gruppen sind Unterringe bzw. Unterkörper selbst Ringe (mit 1) bzw. Körper wenn man die Verknüpfungen $+, \cdot$ entsprechend einschränkt.

## Polynomringe

**Definition:** Sei $R$ ein kommutativer Ring mit Eins.
So nennen wir die Menge aller Polynome in einer Variablen mit Koeffizienten in $R$ Polynomring über $R$.

$$R[t] := \left\{ \sum_{k=0}^{n} a_k t^k \text{ für } n \in \mathbb{N}, a_0, \dots, a_n \in R \right\}$$

**Bemerkung:** Die Polynome kann man als Funktionen in einer Variablen $t$ verstehen. Dies definiert in natürlicher Art die Verknüpfungen $+$ und $\cdot$.

Dies ist nicht die einzige Sichtweise:
Jedes Element von $R[t]$ ist durch $n, a_0, \dots, a_n$ eindeutig festgelegt! $(n, a_0, a_1, a_2 \dots a_n)$

$$+ : \quad \sum_{k=0}^{n} a_k t^k + \sum_{k=0}^{m} b_k t^k = \qquad (o.B.d.A.\ n \le m)$$

$$= \sum_{k=0}^{n} (a_k + b_k) t^k + \sum_{k=n+1}^{m} b_k t^k$$

$$= \sum_{k=0}^{m} (a_k + b_k) t^k \qquad \text{wobei} \quad a_k = 0 \ \forall\, k > n.$$

$$\rightarrow \quad (a_0, a_1, a_2 \dots a_n) + (b_0, b_1 \dots b_m) = (a_0 + b_0 \dots a_m + b_m)$$

$$\cdot : \quad \left(\sum_{k=0}^{n} a_k t^k\right) \cdot \left(\sum_{k=0}^{m} b_k t^k\right) = \sum_{k=0}^{m+n} \left( \sum_{\substack{i=0\dots n \\ j=0\dots m \\ i+j=k}} a_i b_j \right) t^k$$

$$\rightarrow \quad (a_0, a_1, a_2) \cdot (b_0, b_1) = (a_0 b_0,\ a_0 b_1 + a_1 b_0,\ a_1 b_1 + a_2 b_0,\ a_2 b_1)$$

**Satz:** Der Polynomring über einem Ring mit Eins ist in der Tat ein Ring mit Eins.

**Beweis:** $(R[t], +)$ eine abelsche Gruppe ist folgt direkt aus den Gruppenaxiomen für $R$.

Auch das Assoziativgesetz folgt, da bei den Polynomen einfach elementweise gültig:

$$p(t) \cdot \big(q(t) \cdot r(t)\big) = \big(p(t)\, q(t)\big) \cdot r(t) \qquad \forall\, t$$

$\in R$ $\in R$ $\in R$

(Beweis auch über die Formel oben möglich)

Ähnliches gilt für das Distributivgesetz.

**Ex. der Eins:** $\sum_{k=0}^{0} 1 \cdot t^0$ erfüllt die Eigenschaften eines 1-El.

**Definition:** Sei $p = \sum_{j=0}^{n} a_j t^j \in R[t]$. Dann nennt man

$\deg(p) := \max\{j \in \{0,\dots,n\} : a_j \neq 0\}$ den Grad des Polynoms. Das zugehörige $a_j$ den Leitkoeffizienten ($a_j$ für $j = \deg(p)$).

**Satz:** Für jeden kommutativen Ring $R$ mit Eins und zwei Polynome $p, q$ gilt immer:

a) $\deg(p+q) \leq \max\{\deg(p), \deg(q)\}$

b) $\deg(p \cdot q) \leq \deg(p) + \deg(q)$

Die Gleichheit gilt genau dann wenn das Produkt der Leitkoeffizienten $\neq 0$ ist.

**Beweis:** a) $\sum_{j=0}^{n} a_j t^j + \sum_{j=0}^{m} b_j t^j = \sum_{j=0}^{n} (a_j + b_j) t^j$ mit $a_j = 0 \ \forall j > n$ (Fall $m \geq n$)

Man bekommt ein Polynom vom Grad höchstens $n$.

Für $n > m$ analog

b) $\sum_{j=0}^{n} a_j t^j \cdot \sum_{j=0}^{m} b_j t^j = \sum_{j=0}^{m+n} c_j t^j$

$$c_{m+n} = a_n \cdot b_m$$

Man erhält also ein Polynom vom Grad höchstens $m+n$. Falls $a_n b_m \neq 0$ ist, so ist der Grad exakt $m+n$ und umgekehrt. Dann ist $a_n b_m$ auch der Leitkoeffizient des Produkts.