$$\underset{\text{Ring}}{R} \overset{\text{Unterring}}{\subseteq} \underset{\text{Ring}}{S}, \quad s_1,\dots,s_n \in S$$

$$R[x_1,\dots,x_n] = \left\{ \sum_{(i_1,\dots,i_n)\in\mathbb{N}_o^n}^{\text{endlich}} \underbrace{r_{i_1,\dots,i_n} X_1^{i_1}\dots X_n^{i_n}}_{\downarrow\varphi} \,\middle|\, r_1,\dots,r_n \in R \right\}$$

$$R[s_1,\dots,s_n] = \left\{ \sum_{(i_1,\dots,i_n)\in\mathbb{N}_o^n}^{\text{endlich}} \overbrace{r_{i_1\dots i_n} s_1^{i_1}\dots s_n^{i_n}} \,\middle|\, r_1,\dots,r_n \in R \right\}$$

universelle Eigenschaft des Polynomring

$R=\mathbb{Z},\ S=\mathbb{Q}$

$s = s_1 = \frac{1}{2}$

$$\mathbb{Z}\left[\frac{1}{2}\right] = \left\{ \sum_i z_i \left(\frac{1}{2}\right)^i \right\}$$

$R=Q,\ S=\mathbb{R},\ s=\sqrt{2}$

$$Q\left[\sqrt{2}\right] = \left\{ 9+\sqrt{2} \,\middle|\, a,b\in Q \right\}$$

$R=\mathbb{Z},\ S=\mathbb{C},\ s=i$

$$\mathbb{Z}[i] = \left\{ a+ib \,\middle|\, a,b\in\mathbb{Z} \right\}$$

3. Die Teilbarkeit in $K[X]$ (und in $\mathbb{Z}$)

Sei U Unterraum des K-Vektorraums $K[X]$:

$$A,B\in U \ \Rightarrow\ \lambda A+\mu B\in U$$

Sei $U\neq 0$ $\quad m := \min\{\operatorname{grad} A \,|\, A\neq 0 \text{ aus } U\}$

3.1. In U existiert genau ein Polynom M

a) $\operatorname{grad} M = m$

b) M ist normiert

Beweis: $A,B\in U$ mit

$\operatorname{grad} A = m = \operatorname{grad} B$

λ_1 Leitkoeffiezient von A

λ_2 Leitkoeffizient von B

$\Rightarrow$ $\lambda_1\lambda_2$ Leitkoeffiezient von $\lambda_1 B$

$\lambda_1\lambda_2$ Leitkoeffizient von $\lambda_2 A$

$\Rightarrow \operatorname{grad}\underbrace{\left(\lambda_1 B - \lambda_2 A\right)}_{\in u} < M$

$\lambda_1 B = \lambda_2 A$

$\frac{\lambda_1}{\lambda_2} B = A$

$\min U := M$

Ist $U = 0$

$\min U := 0$

Definition: Eine Untermenge U eines (kommutativen) Rings R heißt **Ideal**, wenn

I1) U ist Untergruppe von $R(+)$: $a, b \in U \rightarrow a - b \in U$

I2) $a \in R,\ u \in U \ \Rightarrow\ a \cdot u \in U$

Bemerkung: Sei $R = \mathbb{Z}$

1.1 Untergruppe von $\mathbb{Z}(+)$ $\Rightarrow$ U ist Ideal in $\mathbb{Z}$

Sei $R = K[X]$: U Ideal $\Rightarrow$ U ist Unterraum des Vektorraums $K[X]$

$\lambda \in K,\ A \in U \ \Rightarrow\ \lambda A \in U$

3.2. Für $U \subseteq K[X]$ ist äquivalent:

i) U Ideal

ii) U ist Unterraum von $K[X]$

$P \in K[X],\ A \in U \ \Rightarrow\ PA \in U$

Es genügt zu fordern: $A \in U \ \Rightarrow\ XA \in U$

$\left.\begin{array}{l} X(X)A \in U \\ X^2 A \in U \end{array}\right\}$ alle Linearkombinationen $\in U$

3.3. Satz

Sei U Ideal in $K[X]$ und sei $M := \min U \ \Rightarrow\ U = \langle M \rangle = \{PM \mid P \in K[X]\}$

U Untergruppe von $\mathbb{Z}(+)$ (Vgl. 1.2.)

Bemerkung: $\langle A \rangle = \{PA \mid P \in K[X]\}$ ist Ideal

$\lambda(PA) + \mu(QA) = (\lambda P + \mu Q)A$

$X(PA) = (XP)A$

$Q(PA) = (QP)A$

Beweis: klar im Fall $U = 0$

Sei $U \neq 0$

$\langle M \rangle \subseteq U$ klar

$\supseteq$

$A \in U$: $A = PM + R$: $\operatorname{grad} R < \operatorname{grad} M$

$R \subset A - PM \in U$

$\Rightarrow R = 0$

$A, B \neq 0$ aus $K[X]$

Gilt $B = PA$, $P \in K[X]$, so ist A **Teiler** von B ($P = \frac{B}{A}$)

Ist min grad $P = 0$ oder grad $A = 0$, so ist A **trivialer Teiler** von B

Beispiel: $K = \mathbb{R}$

$$\overset{B}{X^2} + 1 = \overset{P}{\frac{1}{3}}\left(3\overset{A}{X^2} + 3\right)$$

Triviale Zerlegung $B = \lambda\left(\frac{1}{2}B\right)$

$K = \mathbb{C}$

$$\left(X^2 + 1\right) = (X - i)(X - i)$$

Nichttriviale Zerlegung

Beachte: Die Polynome vom Grad 0 sind die **Einheiten** des Rings $K[X]$

In $\mathbb{Z}$: 1 und -1 sind die Einheiten

A, B heißen **teilerfremd**, wenn sie keine gemeinsamen Teiler vom Grad >0 besitzen

$$\langle A \rangle + \langle B \rangle = \left\{A_1 + B_1 \middle| A_1 \in \langle A \rangle,\ B_1 \in \langle B \rangle\right\}$$

$$= \left(P_1 A + P_2 B \middle| P_1, P_2 \in K[X]\right)$$

$$\langle A \rangle \cap \langle B \rangle = \left\{PA \middle| P \in K[X], PA \in \langle B \rangle\right\}$$

Unterräume von $K[X]$ und Ideale von $K[X]$

Beispiele in $\mathbb{Z}$:

$a = 8,\ b = 12$ $ggT(8,12) = 4,\ kgV(8,12) = 24$

$\langle a \rangle + \langle b \rangle$ = Alle Vielfachen von A + alle Vielfachen von B

$\langle a \rangle \cap \langle b \rangle$ = Alle Vielfachen von A und zugleich alle Vielfachen von B

3.4. a) $\langle A\rangle + \langle B\rangle$ und $\langle A\rangle \cap \langle B\rangle$ sind Ideale

b) Sei $G = \min\left(\langle A\rangle + \langle B\rangle\right)$, dann ist $\langle G\rangle = \langle A\rangle + \langle B\rangle$ (Vgl. 3.3.)

Insbesondere existiert $P, Q \in K[X]$ mit $G = PA + QB$

c) Sei $K = \min\underbrace{\left(\langle A\rangle \cap \langle B\rangle\right)}_{\neq 0}$, dann $\langle K\rangle = \langle A\rangle \cap \langle B\rangle$ (Vgl. 3.3.)

$G := ggT(A,B)$, $K := kgV(A,B)$

$A, B \in \langle A\rangle + \langle B\rangle$

$\Rightarrow G$ ist Teiler von A und B

Sei H ebenfalls Teiler von A und B

d.h. $\begin{matrix} A \subseteq \langle X\rangle \\ B \subseteq \langle H\rangle \end{matrix} \Rightarrow \langle G\rangle = \langle A\rangle + \langle B\rangle \subseteq \langle H\rangle$

A und B ist Teiler von K
Sei H auch Vielfaches von A und B

d.h. $H \subseteq \langle A\rangle \cap \langle B\rangle = \langle K\rangle$
d.h. K ist Teiler von H

Beispiel:
$i \cdot 8 + j \cdot 12, \quad i, j \in \mathbb{Z}$
$j = 1,\ i = -1: \quad 4 \in \langle 8\rangle + \langle 12\rangle \qquad \text{ggT} = 4$
$4 = \min\langle\langle a\rangle + \langle b\rangle\rangle$
$\left\{i \cdot \left(\middle| i \in \mathbb{Z}\right)\right\} \wedge \left\{j \cdot 12 \middle| j \in \mathbb{Z}\right\}$

3.5. Sei $\text{ggT}(A,B) = 1$, d.h. A und B seien teilerfremd
Sei A, B normiert. Dann gilt:

$\text{kgV}(A,B) = A \cdot B$

Beweis: $K = \text{kgV}(A,B)$

$A \cdot B \in \langle A\rangle \cap \langle B\rangle = \langle K\rangle$

Es existiert $P \in K[X]$ mit $A \cdot B = PK$

$P\left(\frac{K}{A}\right)A = AB = P\left(\frac{K}{B}\right)B$

$B = P\left(\frac{K}{A}\right),\ A = P\left(\frac{K}{B}\right)$

A, B teilerfremd $\Rightarrow \text{grad}\, P = 0 \overset{\text{wg. Normierung}}{\Rightarrow} P = 1$