

2.2.3 Bem. $\text{grad}(f+g) \leq \max\{\text{grad } f, \text{grad } g\}$

$$(*) \quad \text{grad}(fg) \leq \text{grad } f + \text{grad } g$$

Wir vereinbaren für $a \in \mathbb{Z}$: $-\infty < a$, $-\infty + a = -\infty + -\infty = -\infty$.

2.2.4 Satz Sei R Integritätsring. Dann

(i) Es gilt Gleichheit in (*) (ii) $R[X]$ Integritätsring

$$(iii) R[X]^* = R^*$$

Beweis(i) Seien $f = a_0 + a_1 X + \dots + a_n X^n$, $g = b_0 + b_1 X + \dots + b_m X^m$ mit $a_n \neq 0$, $b_m \neq 0$ d.h. $\text{grad } f = n$, $\text{grad } g = m$. Dann $fg = a_n b_m X^{m+n} + \dots$ mit $a_n b_m \neq 0$, also $\text{grad}(fg) \geq m+n = \text{grad } f + \text{grad } g$.

(ii) $f \neq 0, g \neq 0 \leadsto \text{grad } f \geq 0, \text{grad } g \geq 0 \leadsto \text{grad}(fg) \geq 0 \Rightarrow fg \neq 0$

(iii) $f \in R[X]$ Einheit $\leadsto \exists g \in R[X]$ mit $fg = 1 \leadsto \text{grad } f + \text{grad } g = 0$
 $\leadsto \text{grad } f, \text{grad } g \leq 0 \leadsto f, g \in R \leadsto f \in R^*$. $\square$

2.2.5 Satz (Teilen mit Rest) R Ring, $f, g \in R[X]$ mit $g = \sum_{i=0}^d a_i X^i$, $a_d \in R^*$ (insb. $\text{grad } g = d$). Dann $\exists! q, r \in R[X]$ mit $f = gq + r$, $\text{grad } r < \text{grad } g$.

Beweis Existenz: Induktion nach $\text{grad } f$: Falls $\text{grad } f < d$.

so setze $q=0, r=f$. Falls $\text{grad } f = n \geq d$, $f = \sum_{i=0}^n c_i X^i$, $c_n \neq 0$.

Setze $f_1 := f - c_n a_d^{-1} X^{n-d} g = f - (c_n X^n + \dots)$ also $\text{grad } f_1 < \text{grad } f$

Ind. Vor. $\leadsto \exists q_1, r_1 : f_1 = q_1 g + r_1$, $\text{grad } r_1 < d$. Also

$$f = c_n a_d^{-1} X^{n-d} g + q_1 g + r_1 = (c_n a_d^{-1} X^{n-d} + q_1) g + r_1.$$

Eindeutigkeit Wegen $a_d \in R^*$ insb. a_d kein Nullteiler, gilt $\text{grad}(qg) = \text{grad } q + \text{grad } g$ für alle $q \neq 0$.

$$\text{Ist } f = q_1 g + r_1, \text{grad } r_1 < d \leadsto (q - q_1)g = r_1 - r$$

$$\text{grad}(r_1 - r) < d \leadsto \text{grad}(q - q_1)g < d \text{ Aber } \text{grad}(q - q_1)g =$$

$$= \text{grad}(q - q_1) + \text{grad } g = \text{grad}(q - q_1) + d \leadsto \text{grad}(q - q_1) = -\infty \leadsto q - q_1 = 0$$

$$\leadsto r = r_1 \quad \square$$

2.2.6 Bsp. (i) Setze $R[[X]] = (R^{\mathbb{N}_0}, +, \cdot)$ mit der Addition und Multiplikation wie bei Polynomen.

Wir fordern aber nicht, dass fast alle Folgenglieder eines Elem. $(a_i)_{i \in \mathbb{N}_0} \in R[[X]]$ verschwinden.

Es gilt $(a_i)_{i \in \mathbb{N}_0} = \sum_{i \geq 0} a_i X^i$: eine formale Reihe in der Unbestimmte X .

(ii) $\mathbb{C} = \left\{ \sum_{i \geq 0} a_i X^i \in R[[X]] : \begin{array}{l} \text{der Konvergenzradius von} \\ \sum_{i \geq 0} a_i x^i \text{ ist } > 0 \end{array} \right\}$

(iii) $R \text{ Ring} \rightsquigarrow R[X_1, \dots, X_n] = R[X_1, \dots, X_{n-1}][X_n]$
Polynomring in n Unbestimmten über R .

§ 2.3 Ideale und Faktorringer

Die Ideale wurden von Ernst Kummer als "ideale Zahlen" eingeführt (1847, Journal de Crelle) und von Richard Dedekind weiterentwickelt. Man versucht damit die Eindeutigkeit der Primfaktorzerlegung in manchen Ringe zu sichern. Weiterhin sind alle Ringe kommutativ.

2.3.1 Def Sei R Ring. Eine Teilmenge $\mathcal{O} \subset R$ heißt Ideal in R , falls $(\mathcal{O}, +) < (R, +)$ und $\forall a \in \mathcal{O}, r \in R: ar \in \mathcal{O}$. $\{0\}$ heißt Nullideal.

Ein Ideal ist ein Unterring, aber nicht umgekehrt (z.B. $\mathbb{Z} \subset \mathbb{Z}[X]$ ist Unterring aber kein Ideal). R und $\{0\}$ sind Ideale in R ; $n\mathbb{Z} \subset \mathbb{Z}$ sind die einzigen Ideale von $\mathbb{Z}$.

2.3.2 Lemma Sei $\mathcal{O} \subset R$ Ideal. Dann gilt: $\mathcal{O} = R \Leftrightarrow \mathcal{O} \cap R^* \neq \emptyset$.
 R Körper $\Leftrightarrow$ Die einzigen Ideale von R sind $\{0\}$ und R .

Beweis Sei $u \in \mathcal{O} \cap R^* \leadsto 1 = u \cdot u^{-1} \in \mathcal{O} \leadsto \forall a \in R \ a = a \cdot 1 \in \mathcal{O}$

Ang. $\mathcal{O} \subset R$ Ideal, $\mathcal{O} \neq \{0\} \Rightarrow \mathcal{O} = R$. Sei $a \in R \setminus \{0\}$.

Dann ist $\mathcal{O} := Ra := \{ra : r \in R\}$ ein Ideal, $Ra \neq \{0\}$

Also $Ra = R \leadsto \exists b \in R$ mit $ab = 1 \leadsto a \in R^* \leadsto R \setminus \{0\} = R^* \quad \square$

2.3.3 Lemma (i) Sind $(\mathcal{O}_i)_{i \in I}$ Ideale von R , so ist $\bigcap_{i \in I} \mathcal{O}_i$ Ideal.

(ii) Ist $\varphi: R \rightarrow R'$ Homom, $\mathfrak{b} \subset R'$ Ideal, so ist $\varphi^{-1}(\mathfrak{b}) \subset R$ Ideal.
 Insb ist $\text{Ker } \varphi$ ein Ideal.

(iii) Ist $\varphi: R \rightarrow R'$ surj. Homom, $\mathcal{O} \subset R$ Ideal, so ist $\varphi(\mathcal{O})$ Ideal.

(iv) $\mathcal{O}, \mathfrak{b} \subset R$ Ideale, so sind $\mathcal{O} + \mathfrak{b} := \{a + b : a \in \mathcal{O}, b \in \mathfrak{b}\}$
 $\mathcal{O}\mathfrak{b} := \langle \{ab : a \in \mathcal{O}, b \in \mathfrak{b}\} \rangle$ (Erzeugnis in $(R, +)$) Ideale
 und $\mathcal{O}\mathfrak{b} \subset \mathcal{O} \cap \mathfrak{b}$.

2.3.4 Def Sei $M \subset R$. Das von M erzeugte Ideal (M) ist das kleinste Ideal, das M enthält: $(M) := \bigcap \{ \mathcal{O} : M \subset \mathcal{O} \}$

2.3.5 Lemma $(M) = \left\{ \sum_{i=1}^n r_i m_i : r_i \in R, m_i \in M, n \in \mathbb{N} \right\}$

Insb. $(a_1, \dots, a_m) = Ra_1 + \dots + Ra_m = \left\{ \sum_{i=1}^m r_i a_i : r_i \in R \right\}$
und $(a) = Ra$ für $a_1, \dots, a_m, a \in R$.

2.3.6 Bem. R Integritätsring. Dann gilt: $(a) = (b) \Leftrightarrow \exists c \in R^*, b = ac$

Beweis: " $\Rightarrow$ " Ist $a = 0$, so $b \in (0) = \{0\}$ also $b = 0 \leadsto$ Beh.

Ang. $a, b \in R \setminus \{0\}$. Dann $a \in (b)$, $b \in (a) \leadsto \exists c, d$ $a = bc$, $b = ad$

$\leadsto a = adc \leadsto a(1 - dc) = 0 \leadsto 1 - dc = 0 \leadsto d, c \in R^*$.
R Int'ring

" $\Leftarrow$ " $ax = ac \cdot c^{-1}x = b(c^{-1}x) \in Rb = (b)$ für alle $x \in R$, also
 $(a) = Ra \subset Rb = (b)$. Genauso auch $(b) \subset (a)$. $\square$

2.3.7 Def. Ein Ideal $\mathcal{O} \subset R$ heißt Hauptideal, falls $\exists a \in R$ mit $\mathcal{O} = (a)$. R heißt Hauptidealring, falls R Integritätsring ist und jedes Ideal ein Hauptideal ist.

2.3.8 Bsp. (i) $\mathbb{Z}$ ist Hauptidealring: $\mathcal{O} \subset \mathbb{Z}$ Ideal $\leadsto (\mathcal{O}, +) < (\mathbb{Z}, +)$
 $\leadsto \exists m \in \mathbb{Z}$ mit $\mathcal{O} = m\mathbb{Z}$. (ii) R Körper $\Rightarrow R[X]$ Hauptidealring,
(iii) R Körper $\Rightarrow R$ Hauptidealring (einzige Ideale $(0), (1) = R$).

2.3.9 Def. R Ring, $\mathcal{O} \subset R$ Ideal. Definiere der Quotientenring $R/\mathcal{O}$ durch: (i) $(R/\mathcal{O}, +)$ ist die Quotientengruppe

(ii) $(a + \mathcal{O})(b + \mathcal{O}) = ab + \mathcal{O}$

Dann ist $R/\mathcal{O}$ ein Ring (Einselem $1 + \mathcal{O}$) und die kanonische Projektion $\pi: R \rightarrow R/\mathcal{O}$, $\pi(a) = a + \mathcal{O}$ ist ein Ringhomom.

(Wohldefiniertheit: $a - a' = x \in \mathcal{O} \leadsto (a + \mathcal{O})(b + \mathcal{O}) =$
 $= (xc + a' + \mathcal{O})(b + \mathcal{O}) = \underbrace{xb}_{\in \mathcal{O}} + a'b + \mathcal{O} = a'b + \mathcal{O}$)
 $\in \mathcal{O}$, da $\mathcal{O}$ Ideal