§ 13 Polynomringe

Gv: K ein Körper (teils genügt auch: K ein kommutativer Ring mit $1 \neq 0$, aber Vorsicht!)

(13.1) Def

a) Eine K-Algebra ist ein Ring R mit 1, der gleichzeitig ein VR über K ist und für den gilt: $\forall a \in K \; \forall r, s \in R: \; a(rs) = (ar)s = r(as)$

[Bspl: $\mathbb{H}$ ist eine $\mathbb{R}$-Algebra]

Ein K-Algebrenhomomorphismus ist eine Abb $\varphi: R \to S$ zwischen K-Algebren, die zugleich ein Ringhomomorphismus und eine K-lineare Abb ist; letzteres bedeutet: $\forall a \in K \; \forall r_1, r_2 \in R:$

$$(ar_1 + r_2)\varphi = a(r_1\varphi) + r_2\varphi.$$

b) Eine K-Algebra R heißt Polynomring in der Unbestimmten X über K, falls es $X \in R$ gibt und sich jedes $f \in R$ eindeutig schreiben läßt als

$$f = f_0 \cdot \underbrace{X^0}_{=1} + f_1 \cdot \underbrace{X^1}_{=X} + f_2 X^2 + \ldots + f_n X^n \qquad (*)$$

mit $n \in \{-\infty\} \cup \mathbb{N}_0$ und $f_0, f_1, \ldots, f_n \in K$, $f_n \neq 0$.

Für $f \in R$ wie in $(*)$ heißt

$$\operatorname{grad}(f) = n \in \{-\infty\} \cup \mathbb{N}_0$$

der Grad von f (bzgl X).

Ein K-Algebrenisomorphismus zw R und S ist ein bijektiver K-Algebrenhomomorphismus von R auf S; vgl (12.2).

Bem
- $X^0 = 1$ ist das Einselement von R
- Es ex genau ein $f \in R$ mit $\operatorname{grad}(f) = -\infty$, nämlich $f = 0$.
- $X^0 = 1, X^1 = X, X^2, X^3, \ldots$ bilden eine Basis für den K-VR R
- R ist kommutativ:

$$f g = \Big(\sum_{i=0}^{m} f_i X^i\Big)\Big(\sum_{j=0}^{n} g_j X^j\Big) = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} f_i g_j\Big) X^k$$

$$= \ldots = g f.$$

(13.2) Satz Sei R ein Polynomring in der Unbest X über K. Dann besitzt R die „universelle Eigenschaft“:
Ist S eine beliebige K-Algebra und $A \in S$, so gibt es genau einen K-Algebrenhomom $\varphi : R \to S$ mit $X\varphi = A$.

Bem: Dieser K-Algebrenhomom heißt Einsetzungshomom, und das Bild von $f = \sum f_i X^i \in R$ unter φ wird gewöhnlich mit $f(A) = \sum f_i A^i$ bezeichnet.
[Die Schreibweise hängt implizit von der Wahl von X ab!]

Bew: Ist $\varphi : R \to S$ ein K-Algebrenhomom mit $X\varphi = A$, so gilt für beliebiges $f = \sum f_i X^i \in R$:

$$f\varphi = \Big(\sum f_i X^i\Big)\varphi = \sum f_i (X\varphi)^i = \sum f_i A^i.$$

Dies beweist die Eindeutigkeit.

Sei nun S eine K-Algebra und $A \in S$.

Leichte Rechnungen zeigen, daß

$$\varphi : R \to S, \quad \sum f_i X^i \mapsto \sum f_i A^i$$

den gewünschten K-Algebrenhomom darstellt.

Z.B. gilt

$$\Big(\sum_i f_i X^i + \sum_j g_j X^j\Big)\varphi = \Big(\sum_k (f_k + g_k) X^k\Big)\varphi$$

$$= \sum_k (f_k + g_k) A^k = \sum_i f_i A^i + \sum_j g_j A^j,$$

wobei $f_i = 0$ für $i > \operatorname{grad}(f)$ und

$g_j = 0$ für $j > \operatorname{grad}(g)$ zu setzen sind. //

(13.3) Folgerung: Bis auf Isomorphie* gibt es höchstens einen Polynomring in einer Unbest über K.

Bew: Sei R (bzw S) ein Polynomring in der Unbest X (bzw Y) über K. Nach (13.2) ex K-Algebrenhomom $\varphi : R \to S$ mit $X\varphi = Y$ und $\psi : S \to R$ mit $Y\psi = X$. Wir behaupten: φ und ψ sind zueinander invers, dh $\varphi\psi = id_R$ und $\psi\varphi = id_S$.

Offenbar ist $\varphi\psi : R \to R$ ein K-Algebrenhomom mit $X\varphi\psi = Y\psi = X$, ebenso id_R. Aus der Eindeutigkeitsaussage in (13.2) folgt $\varphi\psi = id_R$. Ähnlich erhält man $\psi\varphi = id_S$. //

* Begriffsbildung analog zu (12.2); siehe (13.1)

(13.4) Satz Es ex ein Polynomring R Kloposch
in einer Unbestimmten X über K.

Bew Sei $R = K^{(\mathbb{N}_0)}$ die Menge aller Folgen

$f = (f_0, f_1, \dots)$ in K, die schließlich konstant
0 werden. Dann hat R eine natürliche
VR-Struktur über K (siehe (5.3)):

$$f + g = (f_0 + g_0, f_1 + g_1, f_2 + g_2, \dots) \qquad \text{für } f, g \in R, a \in K$$
$$a f = (a f_0, a f_1, \dots)$$

Weiterhin bildet

$e_0 = (1, 0, \dots)$, $e_1 = (0, 1, 0, \dots)$, ...

eine Basis für R über K:

$f = (f_0, f_1, \dots)$ läßt sich eindeutig als

$f = \sum_{i=0}^{\infty} f_i e_i$ schreiben (mit nur endl vielen
Summanden $\neq 0$).

Def auf R eine Multiplikation, indem
die Vorgabe $e_i \cdot e_j = e_{i+j}$ für $i, j \in \mathbb{N}_0$
linear fortgesetzt wird:

$$f g = \left(\sum f_i e_i\right)\left(\sum g_j e_j\right) = \sum_k \left(\sum_{i+j=k} f_i g_j\right) e_k .$$

Man prüft leicht, daß R dadurch zu einer
K-Algebra mit $1 = e_0$ wird (Übung!).

Setze $X = e_1$. Dann gilt $X^i = e_i$ für $i \in \mathbb{N}_0$,
und R ist ein Polynomring in der Unbest X. //

(13.5) Def Der, nach (13.3) bis auf Isomorphie eind best, Polynomring in einer Unbest X über K wird mit $K[X]$ bezeichnet. Seine Elemente heißen kurz Polynome und werden wahlweise als f oder $f(X)$ geschrieben.

Hat $f = \sum f_i X^i \neq 0$ den Grad n, so heißt $f_n X^n$ der Leitterm und f_n der Leitkoeffizient von f (bzgl X). Ein Polynom $f \in K[X]$ heißt normiert, falls $f \neq 0$ ist und Leitkoeff 1 hat.

Bem ∘ Man kann sich überlegen, daß der Grad eines Polynoms $f \in K[X]$ nicht von der Wahl von X abhängt. [Übung]

∘ Ist S eine K-Algebra und $A \in S$, so wird das Bild von $K[X]$ unter dem Einsetzungshomom $\varphi : K[X] \to S$ mit $X\varphi = A$ durch

$$K[A] = \{ f_0 + f_1 A + \ldots + f_n A^n \mid f = \sum f_i X^i \in K[X] \}$$

bezeichnet.

∘ In $K[X]$ bilden die konstanten Polynome $f_0 X^0 = f_0$ einen Unterring von $K[X]$, der zu K isomorph ist. Wir unterscheiden in unserer Notation nicht zwischen diesen Kopien von K.

(13.6) Lemma Für $f, g \in K[X]$ gilt:

(1) $\operatorname{grad}(f+g) \leq \max\{\operatorname{grad}(f), \operatorname{grad}(g)\}$,
mit Gleichheit, falls $\operatorname{grad}(f) \neq \operatorname{grad}(g)$

(2) $\operatorname{grad}(fg) = \operatorname{grad}(f) + \operatorname{grad}(g)$

Bem: Hierbei ist $-\infty \leq k$ und $-\infty + k = -\infty$ für alle $k \in \{-\infty\} \cup \mathbb{N}_0$.

Bew: Seien $f = \sum f_i X^i$, $g = \sum g_j X^j \in K[X]$.
Ist $f=0$ oder $g=0$, so gelten die Behauptungen trivialerweise. Seien nun $f, g \neq 0$, also

$m = \operatorname{grad}(f)$, $n = \operatorname{grad}(g) \geq 0$.

Aussage (1) folgt aus

$$f+g = \sum_{k=0}^{\max\{m,n\}} (f_k + g_k) X^k,$$

wobei $f_k = 0$ für $k > m$, $g_k = 0$ für $k > n$ zu setzen sind.

Wegen

$$fg = \sum_{k=0}^{m+n} \Big(\sum_{i+j=k} f_i g_j \Big) X^k \quad \text{mit Leitterm}$$

$\underbrace{f_m}_{\neq 0} \underbrace{g_n}_{\neq 0} X^{m+n}$ ist $\operatorname{grad}(fg) = m+n$.
(K ist nullteilerfrei!)

Also gilt (2). //

(13.7) Folgerung: $K[X]$ ist ein Integritätsbereich mit Einheitengruppe $K[X]^* = \{f \in K[X] \mid \operatorname{grad}(f) = 0\} \cong K^*$.

Jedes $f \in K[X] \setminus \{0\}$ ist zu genau einem normierten Polynom assoziiert.

Bew: Offenbar ist $K[X]$ ein kommutativer Ring mit 1.

Sind $f, g \in K[X] \setminus \{0\}$, so ist nach (13.6)(2)

$$\operatorname{grad}(fg) = \underbrace{\operatorname{grad}(f)}_{\in \mathbb{N}_0} + \underbrace{\operatorname{grad}(g)}_{\in \mathbb{N}_0} \neq -\infty, \text{ also } fg \neq 0.$$

Somit ist $K[X]$ nullteilerfrei und ein Integritätsbereich.

Offenbar ist $\{f \in K[X] \mid \operatorname{grad}(f) = 0\} = \{f_0 \mid f_0 \in K^*\}$ in $K[X]^*$ enthalten. Umgekehrt zeigt (13.6)(2), daß Einheiten in $K[X]$ stets Grad 0 haben.

Ist $f \in K[X] \setminus \{0\}$ mit Leitkoeff $f_m \neq 0$, so ist $f_m^{-1} \cdot f$ das eindeutige normierte Polynom in der Assoziiertenklasse $K[X]^* \cdot f = K^* \cdot f$ von f. //

(13.8) Satz (Division mit Rest)

Seien $f, g \in K[X]$ und $f \neq 0$. Dann ex eindeutig bestimmte Polynome $q, r \in K[X]$ mit

$$g = qf + r \quad \text{und} \quad \operatorname{grad}(r) < \operatorname{grad}(f).$$

Bew (analog zu (11.8)!)

Existenz (per Induktion nach $\operatorname{grad}(g)$): Ist $\operatorname{grad}(g) < \operatorname{grad}(f)$, so wähle $q = 0$ und $r = g$. Sei nun $n = \operatorname{grad}(g) \geq \operatorname{grad}(f) = m$. Dann hat g (bzw f) den Leitterm $g_n X^n$ (bzw $f_m X^m$). Für $h = g - \frac{g_n}{f_m} X^{n-m} f \in K[X]$ gilt: $\operatorname{grad}(h) < \operatorname{grad}(g)$. Per Induktion ex $q', r' \in K[X]$ mit $h = q'f + r'$ und $\operatorname{grad}(r') < \operatorname{grad}(f)$.

Dann erfüllen $q = q' + \frac{g_n}{f_m} X^{n-m}$

und $r = r'$ die gewünschten Bedingungen:

$$g = h + \frac{g_n}{f_m} X^{n-m} f = qf + r \text{ und } \operatorname{grad}(r) < \operatorname{grad}(f).$$

Eindeutigkeit: Seien auch $\tilde{q}, \tilde{r} \in K[X]$ mit den gewünschten Eigenschaften. Dann gilt

$$(q - \tilde{q}) f = (g - r) - (g - \tilde{r}) = \tilde{r} - r,$$

also $\operatorname{grad}(q - \tilde{q}) + \operatorname{grad}(f) = \operatorname{grad}(\tilde{r} - r) < \operatorname{grad}(f)$.

Das ergibt $\operatorname{grad}(q - \tilde{q}) = -\infty$, also $q = \tilde{q}$ und $r = \tilde{r}$. //

Folgerung: Die Ergebnisse aus §11 für $\mathbb{Z}$ übertragen sich nun „mutatis mutandis" auf $K[X]$:

a) Je zwei Elemente in $K[X]$ haben einen größten gemeinsamen Teiler, und dieser ist bis auf Multiplikation mit einer Einheit eindeutig. Es gibt daher genau eine Abb

$$ggT: K[X] \times K[X] \to \{0\} \cup \{f \in K[X] \mid f \text{ normiert}\},$$

so daß $ggT(g,h)$ für alle $g, h \in K[X]$ ein gr gem Teiler von g, h ist.

Sind $g, h \in K[X]$, dann ex Bézout-Koeffizienten $s, t \in K[X]$ mit $sg + th = ggT(g,h)$. Der gr gem Teiler und Bézout-Koeffizienten können effektiv mit dem euklidischen Algorithmus berechnet werden.

b) In $K[X]$ fallen die Begriffe „unzerlegbar" und „prim" zusammen; man spricht meist von

irreduziblen Polynomen. Mit etwas Geschick beweist man die eindeutige Primfaktorzerlegung:

Sei $f \in K[X] \setminus \{0\}$. Dann besitzt f eine Faktorisierung

$$f = a \cdot g_1 \cdots g_r ,$$

wobei $a \in K^* \ (= K[X]^*)$, $r \in \mathbb{N}_0$ sind und $g_1, \dots, g_r \in K[X]$ normiert und irreduzibel (über K) sind. Diese Zerlegung ist - bis auf die Reihenfolge der Faktoren - eindeutig.

c) Sei $f \in K[X]$. Die Relation

$$g \equiv_f h \quad \text{gdw} \quad f \mid (g-h), \text{ d.h.}$$

$$g - h \in fK[X] = \{ f \cdot t \mid t \in K[X] \}$$

ist eine Äquivalenz auf $K[X]$. Auf

$K[X]/fK[X] = K[X]/\equiv_f$ wird durch

$$(g + fK[X]) + (h + fK[X]) = (g+h) + fK[X]$$

$$(g + fK[X]) \cdot (h + fK[X]) = g \cdot h + fK[X]$$

eine Ringstruktur definiert; $K[X]/fK[X]$ heißt Restklassenring. Es gilt: $K[X]/fK[X]$ ist ein Körper gdw f irreduzibel in $K[X]$ ist.

Bspl: • X^2+1 ist ired in $\mathbb{R}[X]$ und $\mathbb{R}[X]/(X^2+1)\mathbb{R}[X]$ liefert ein „Modell" für $\mathbb{C}$

• X^3+X+1 ist ired in $\mathbb{F}_2[X]$ und $\mathbb{F}_2[X]/(X^3+X+1)\mathbb{F}_2[X]$ liefert ein „Modell" für $\mathbb{F}_8$

(13.9) Korollar

Sei $g \in K[X]$ und $a \in K$ eine Nullstelle von g, d.h. $g(a) = 0$. Dann ex $q \in K[X]$ mit $g = (X-a) \cdot q$.

Bew: (13.8), angewandt auf $f = X - a$ ergibt

$g = (X-a)q + r$ für $q, r \in K[X]$ mit $\operatorname{grad}(r) < 1$, d.h. $r = r_0 \in K$.

Einsetzen von a liefert

$$0 = g(a) = 0 \cdot q(a) + r_0 = r_0 = r,$$

also $g = (X-a)q$. ∎

(13.10) Korollar Sei $f \in K[X] \setminus \{0\}$. Dann ex eine Zerlegung

$$f = (X - a_1)^{e_1} \cdots (X - a_r)^{e_r} \cdot g \qquad (*)$$

mit $r \in \mathbb{N}_0$, $e_1, \ldots, e_r \in \mathbb{N}$, $a_1, \ldots, a_r \in K$ und $g \in K[X]$, so daß gilt:

- $\operatorname{grad}(f) = e_1 + \ldots + e_r + \operatorname{grad}(g)$ [insb. $0 \leq r \leq \operatorname{grad}(f)$]
- $a_1, \ldots, a_r$ sind die paarw. versch. Nullstellen von f in K
- g hat keine Nullstellen in K (bzgl. X)

Weiterhin sind die Exponenten e_i den Nullstellen a_i eindeutig zugeordnet (sie heißen Vielfachheiten), und g ist eind. bestimmt.

Bew: Durch Abspalten von Linearfaktoren gemäß (13.9) läßt sich f auf die Form $(*)$ bringen.

Als Nullstellen von f in K (bzgl. X) sind $a_1, \ldots, a_r$ und die Anzahl $r \in \mathbb{N}_0$ eindeutig bestimmt.

Die weiteren Eindeutigkeitsbehauptungen ergeben sich per Induktion, da in dem Integritätsbereich $K[X]$ von 0 verschiedene Faktoren gekürzt werden dürfen. //

(13.11) Korollar Ein Polynom $f \in K[X] \setminus \{0\}$ vom Grad $n = \operatorname{grad}(f) \geq 0$ hat höchstens n Nullstellen in K, inkl. Vielfachheiten.

(13.12) Def Ein Polynom $f \in K[X] \setminus \{0\}$ zerfällt (vollständig) in Linearfaktoren über K, falls

$$f = c(X - a_1) \cdots (X - a_n), \quad n = \operatorname{grad}(f),$$

für geeignete $c, a_1, \ldots, a_n \in K$ gilt:

(nicht notw. pw verschieden!)

Bspl: $X^2 - 2$ zerfällt nicht in Linearfaktoren über $\mathbb{Q}$

$X^2 - 2 = (X - \sqrt{2})(X + \sqrt{2})$ zerfällt voll. in Linfkt über $\mathbb{R}$

(13.13) Fakt (Steinitz 1910)

Jeder Körper besitzt einen algebraisch abgeschlossenen Oberkörper, d.h. einen Oberkörper, über dem jedes Polynom $\neq 0$ in Linearfaktoren zerfällt.

[benutzt Auswahlaxiom]

(13.14) „Fundamentalsatz der Algebra" (d'Alembert 1746, Gauß 1799)

Der Körper $\mathbb{C}$ ist alg. abgeschl., d.h. jedes $f \in \mathbb{C}[X] \setminus \{0\}$ zerfällt über $\mathbb{C}$ in Linearfaktoren.

[beweist man z.B. in der Funktionentheorie- / Algebra-Vorl.]