# Die Theorie des Anstieges

**Peter Schneider**

Vorlesung in Münster im WS 2006/07

**Zusammenfassung**

So wie Eigenwerte das wesentliche Instrument zur Untersuchung linearer Abbildungen sind, sind es die sogenannten Anstiege für die Theorie der semilinearen Abbildungen.

Der erste Teil der Vorlesung beginnt mit dem Begriff der semilinearen Abbildung und seinen elementaren Eigenschaften. Anschliessend gibt es eine Einführung in die Theorie der diskreten Bewertungsringe. Dabei wird auch ausführlich die Konstruktion der Ringe von Wittvektoren sowie das Konzept der Cohen-Unterringe bei imperfektem Restklassenkörper erklärt. Im letzten Abschnitt wird die klassische Strukturtheorie von semilinearen Abbildungen über vollständig diskret bewerteten Körpern mit perfektem Restklassenkörper entwickelt.

Der zweite Teil der Vorlesung beginnt mit einer eingehenden Untersuchung der Ringe konvergenter Laurentreihen über vollständig diskret bewerteten Körpern. Danach wird der Robba-Ring eingeführt, und seine ringtheoretischen Eigenschaften werden hergeleitet. Der Robba-Ring hat sich als von grundsätzlicher Bedeutung in der modernen $p$-adischen Zahlentheorie herausgestellt. Schließlich wird teilweise ohne Beweise über die Struktur semilinearer Abbildungen über dem Robba-Ring nach Kedlaya berichtet.

# Inhaltsverzeichnis

# Teil I
# Vorbereitungen und klassische Beispiele

## 1 Semilineare Abbildungen

**Erinnerung:** Sei $K$ ein Körper, $V$ ein $K$-Vektorraum, $d := \dim_K V < \infty$ und $f : V \longrightarrow V$ ein linearer Automorphismus.

*Aufgabe der linearen Algebra:* Finde eine Basis von $V$, bzgl. welcher die Matrix $A_f$ von $f$ möglichst einfache Gestalt hat.

Für eine Umformulierung betrachten wir den Isomorphismus von Gruppen

$$\begin{aligned} \mathrm{Aut}_K(V) &\xrightarrow{\cong} GL_d(K) \\ f &\longmapsto A_f \ , \end{aligned}$$

welcher aber von der Basiswahl abhängt. Bei Wahl einer anderen Basis mit Basiswechselmatrix $B$ geht $A_f$ über in $B^{-1}A_fB$. Also ist die Konjugationsklasse von $A_f$ in $GL_d(K)$ unabhängig von der Basiswahl.

*Umformulierte Aufgabe:* Bestimme die Konjugationsklassen in $GL_d(K)$ durch Angabe möglichst einfacher Repräsentanten.

Nach dem Satz von der Jordanschen Normalform besitzt diese Aufgabe (zumindest über algebraisch abgeschlossenem $K$) eine ganz explizite Lösung.

Gegeben sei ein Körper $K$ zusammen mit einem Körperhomomorphismus

$$\sigma : K \longrightarrow K \ .$$

Beachte: $\sigma$ ist notwendigerweise injektiv. Aber wir verlangen nicht, daß $\sigma$ surjektiv, also ein Automorphismus ist. Sei $V$ ein $K$-Vektorraum.

**Definition 1.1.** *Eine Abbildung $f : V \longrightarrow V$ heißt semilinear (genauer $\sigma$-linear), falls gilt:*

*(i)* $f(v_1 + v_2) = f(v_1) + f(v_2)$ *für alle* $v_1, v_2 \in V$

*(ii)* $f(av) = \sigma(a)f(v)$ *für alle* $a \in K$ *und* $v \in V$.

Sei $d := \dim_K V < \infty$, und sei $v_1, \ldots, v_d$ eine fixierte Basis von $V$. Wie bei linearen Abbildungen bilden wir die Matrix $A_f = (a_{ij}) \in M_d(K)$ zur semilinearen Abbildung $f : V \longrightarrow V$ durch

$$f(v_j) = a_{1j}v_1 + \ldots + a_{dj}v_d \ .$$

**Lemma 1.2.** *Die Abbildung*

$$\begin{array}{rl} \textit{Menge aller semilinearen} & \\ \textit{Abbildungen } f : V \longrightarrow V & \stackrel{\cong}{\longrightarrow} M_d(K) \\ f & \longmapsto A_f \end{array}$$

*ist bijektiv.*

*Beweis.* Wie in der linearen Algebra, z. B.: Für $v = c_1v_1 + \ldots + c_dv_d$ ist

$$f(v) = \sum_{j=1}^{d} \sigma(c_j) f(v_j) = \sum_{j=1}^{d} \sigma(c_j) \sum_{i=1}^{d} a_{ij} v_i = \sum_{i=1}^{d} \Big( \sum_{j=1}^{d} a_{ij} \sigma(c_j) \Big) v_i \ .$$

□

**Zusatz 1.3.** *1) Obige Rechnung zeigt:*

$$v \longleftrightarrow \begin{pmatrix} c_1 \\ \vdots \\ c_d \end{pmatrix} \Longrightarrow f(v) \longleftrightarrow A_f \begin{pmatrix} \sigma(c_1) \\ \vdots \\ \sigma(c_d) \end{pmatrix} \ .$$

*2) Die Menge der semilinearen Abbildungen bildet in üblicher Weise einen $K$-Vektorraum, und obige Abbildung ist ein Isomorphismus von $K$-Vektorräumen.*

**Warnung:** 1) $f$ und $g$ sind $\sigma$-linear $\Longrightarrow g \circ f$ ist $\sigma^2$-linear (nicht $\sigma$-linear). 2) Ist $\sigma$ nicht surjektiv, so ist das Bild einer semilinearen Abbildung i. A. kein Untervektorraum.

Für $A = (a_{ij}) \in M_d(K)$ setze $\sigma(A) := (\sigma(a_{ij})) \in M_d(K)$.
Es gilt:
- $\sigma(A + B) = \sigma(A) + \sigma(B)$,
- $\sigma(AB) = \sigma(A)\sigma(B)$,
- $\sigma(E_d) = E_d$ .

Insbesondere ist

$$\begin{array}{rl} \sigma : GL_d(K) & \longrightarrow GL_d(K) \\ A & \longmapsto \sigma(A) \end{array}$$

ein Monomorphismus von Gruppen (ein Automorphismus, falls $\sigma$ bijektiv ist).

Sei $v'_1, \dots v'_d$ eine weitere Basis von $V$, bzgl. welcher $f$ die Matrix $A'_f = (a'_{ij})$ habe. Die Basiswechselmatrix $B = (b_{kl})$ ist gegeben durch

$$v'_l = \sum_{k=1}^{d} b_{kl} v_k \ .$$

**Lemma 1.4.** $A'_f = B^{-1} A \sigma(B)$ .

*Beweis.* Einerseits ist

$$f(v'_j) = \sum_{i=1}^{d} a'_{ij} v'_i = \sum_{i=1}^{d} a'_{ij} \sum_{k=1}^{d} b_{ki} v_k = \sum_{k=1}^{d} \Big( \sum_{i=1}^{d} b_{ki} a'_{ij} \Big) v_k$$

und andererseits

$$\begin{aligned} f(v'_j) &= f\Big( \sum_{l=1}^{d} b_{lj} v_l \Big) = \sum_{l=1}^{d} \sigma(b_{lj}) f(v_l) \\ &= \sum_{l=1}^{d} \sigma(b_{lj}) \Big( \sum_{k=1}^{d} a_{kl} v_k \Big) = \sum_{k=1}^{d} \Big( \sum_{l=1}^{d} a_{kl} \sigma(b_{lj}) \Big) v_k \ . \end{aligned}$$

Der Vergleich ergibt

$$B A'_f = A_f \sigma(B) \ .$$

□

*Offensichtliche analoge Aufgabe:* Bringe $A_f$ durch geeignete Basiswahl auf möglichst einfache Gestalt.

**Übungsaufgabe 1.5.** *Auf $GL_d(K)$ wird durch*

$$A' \sim A, \text{ falls } A' = B^{-1} A \sigma(B) \text{ für ein } B \in GL_d(K)$$

*eine Äquivalenzrelation definiert. Man sagt, $A'$ ist $\sigma$-konjugiert zu $A$. Die zugehörigen Äquivalenzklassen heißen $\sigma$-Konjugationsklassen.*

**Lemma 1.6.**

*i. $A_f$ ist invertierbar $\iff$ $\mathrm{im}(f)$ erzeugt $V$ als $K$-Vektorraum $\implies$ $f$ ist injektiv;*

*ii. ist $\sigma$ bijektiv, so gilt: $A_f$ invertierbar $\iff$ $f$ surjektiv $\iff$ $f$ bijektiv $\iff$ $f$ injektiv.*

*Beweis.* i. Es gilt:

$$A_f \text{ hat Rang } d \Longleftrightarrow f(v_1), \ldots, f(v_d) \text{ ist wieder eine Basis von } V$$
$$\Longleftrightarrow < \mathrm{im}(f) > = V \ .$$

Ist $f(v_1), \ldots, f(v_d)$ eine Basis von $V$, so gilt außerdem für $v = c_1 v_1 + \ldots + c_d v_d$ mit $f(v) = 0$, daß

$$\sigma(c_1) f(v_1) + \ldots + \sigma(c_d) f(v_d) = 0 \text{ und somit } \sigma(c_i) = 0, \text{ also } c_i = 0 \ .$$

Folglich ist $f$ injektiv.

ii. In diesem Falle ist $\mathrm{im}(f)$ ein Untervektorraum. Wegen i. bleibt deswegen nur zu zeigen, daß gilt:

$$f \text{ injektiv} \Longrightarrow f(v_1), \ldots, f(v_d) \text{ sind } K\text{-linear unabhängig.}$$

Sei also $c_1 f(v_1) + \ldots + c_d f(v_d) = 0$. Wegen der Surjektivität von $\sigma$ können wir schreiben $c_i = \sigma(b_i)$. Dann gilt $f(b_1 v_1 + \ldots + b_d v_d) = 0$ und damit wegen der Injektivität von $f$, daß alle $b_i = 0$, also auch alle $c_i = 0$.

□

**Definition 1.7.** *Die semilineare Abbildung $f : V \longrightarrow V$ heißt etal, falls $V = < \mathrm{im}(f) >$ gilt.*

Für etale $f$ ist also obige Aufgabe gleichbedeutend mit der Bestimmung der $\sigma$-Konjugationsklassen in $GL_d(K)$.

## 2 Der einfachste Fall

Sei $p$ eine fixierte Primzahl, $q > 1$ eine fixierte Potenz von $p$ und $K$ ein Körper der Charakteristik $p$, welcher den endlichen Körper $\mathbb{F}_q$ enthält. Dann ist

$$\sigma : K \longrightarrow K$$
$$a \longmapsto a^q$$

ein Körperhomomorphismus - der *Frobenius*. Es gilt:

- $K^{\sigma=\mathrm{id}} := \{a \in K : \sigma(a) = a\} = \mathbb{F}_q$
  (da $a$ Nullstelle von $X^q - X$ ist);

- $K$ algebraisch abgeschlossen $\Longrightarrow \sigma$ ist bijektiv.

Sei $V$ ein $K$-Vektorraum der Dimension $d < \infty$ und $f : V \longrightarrow V$ eine etale semilineare Abbildung. Setze

$$V_1 := \{v \in V : f(v) = v\} \ .$$

Offensichtlich ist $V_1$ ein $\mathbb{F}_q$-Vektorraum.

**Satz 2.1.** *Ist $K$ separabel abgeschlossen (d. h. $K$ besitzt keine echten separablen algebraischen Erweiterungen), so gilt:*

*i.* $\dim_{\mathbb{F}_q} V_1 = \dim_K V$*;*

*ii. die $K$-lineare Abbildung*

$$\begin{aligned} K \otimes_{\mathbb{F}_q} V_1 &\xrightarrow{\cong} V \\ a \otimes v &\longmapsto av \end{aligned}$$

*ist bijektiv.*

*Beweis.* Natürlich können wir $V \neq \{0\}$ annehmen.

*1. Schritt:* Wir zeigen $V_1 \neq \{0\}$. Sei $0 \neq v_0 \in V$ beliebig gewählt und setze $v_i := f^i(v_0)$. Weiter sei $m \geq 1$ minimal, so daß $v_0, \ldots, v_m$ linear abhängig sind (über $K$). Also gibt es bis auf skalare Vielfache genau eine Relation

$$a_0 v_0 + \ldots + a_m v_m = 0 \quad \text{mit } a_i \in K \text{ und } a_m \neq 0 \ .$$

Beachte, daß auch $a_0 \neq 0$; denn mit $v_0, \ldots, v_{m-1}$ sind nach Lemma 1.3.i. auch $v_1 = f(v_0), \ldots, v_m = f(v_{m-1})$ linear unabhängig.
Wir betrachten nun ein beliebiges $v := c_0 v_0 + \ldots + c_{m-1} v_{m-1}$. Dann ist

$$f(v) = c_0^q f(v_0) + \ldots + c_{m-1}^q f(v_{m-1}) = c_0^q v_1 + \ldots + c_{m-1}^q v_m \ ,$$

also

$$v - f(v) = \sum_{i=0}^{m} (c_i - c_{i-1}^q) v_i \quad \text{mit } c_{-1} := c_m := 0 \ .$$

Somit gilt

$$f(v) = v \Longleftrightarrow c_i - c_{i-1}^q = a_i y \quad \text{für ein } y \in K \ .$$

Das Polynom $a_0^{q^m} Y^{q^m} + a_1^{q^{m-1}} Y^{q^{m-1}} + \ldots + a_m Y$ hat die Ableitung $a_m \neq 0$ und ist somit separabel. Da $K$ separabel abgeschlossen ist, finden wir folglich eine Nullstelle $y \neq 0$ in $K$. Bilde nun den Vektor $v$ mit

$$\begin{aligned} c_0 &:= a_0 y, \\ c_1 &:= c_0^q + a_1 y = a_0^q y^q + a_1 y, \\ &\vdots \\ c_{m-1} &:= a_0^{q^{m-1}} y^{q^{m-1}} + \ldots + a_{m-1} y \ . \end{aligned}$$

Wegen $a_0 \neq 0$ ist auch $c_0 \neq 0$ und damit $v \neq 0$. Per Konstruktion ist $v \in V_1$.

*2. Schritt:* Wir zeigen $\dim_{\mathbb{F}_q} V_1 \leq \dim_K V$. Es gelte die gegenteilige Ungleichung $\dim_{\mathbb{F}_q} V_1 > \dim_K V$. Sei $r \geq 2$ minimal, so daß Vektoren $u_1, \ldots, u_r \in V_1$ existieren, welche linear unabhängig über $\mathbb{F}_q$, aber linear abhängig über $K$ sind. Sei etwa

$$b_1 u_1 + \ldots + b_r u_r = 0 \quad \text{und } b_1 \in K^\times \ .$$

Wir können $b_1 = 1$ annehmen. Dann ist

$$0 = f(0) = u_1 + b_2^q u_2 + \ldots + b_r^q u_r$$

und Subtraktion ergibt

$$(b_2 - b_2^q) u_2 + \ldots + (b_r - b_r^q) u_r = 0 \ .$$

Wegen der Minimalität von $r$ muß $b_i = b_i^q$ gelten, was $b_i \in \mathbb{F}_q$ bedeutet und einen Widerspruch darstellt.

*3. Schritt:* Wir zeigen schließlich per Induktion nach $d = \dim_K V$, daß $V_1$ eine $\mathbb{F}_q$-Basis $v_1, \ldots, v_d$ besitzt, welche auch $K$-Basis von $V$ ist. Für den Induktionsanfang sei $d = 1$. Wie im 1. Schritt gezeigt, existiert ein $0 \neq v_1 \in V_1$. Wegen dem 2. Schritt ist dieses $v_1$ eine $\mathbb{F}_q$-Basis von $V_1$. Für den Induktionsschluß sei $d > 1$. Wieder finden wir nach dem 1. Schritt ein $0 \neq v_1 \in V_1$. Dann ist

$$\begin{aligned} \tilde{f} : V/Kv_1 &\longrightarrow V/Kv_1 \\ u + Kv_1 &\longmapsto f(u) + Kv_1 \end{aligned}$$

eine wohldefinierte etale semilineare Abbildung. Die Induktionsannahme für das Paar $(V/Kv_1, \tilde{f})$ liefert Vektoren $v_2', \ldots, v_d' \in V$, so daß gilt:

- $v_1, v_2', \ldots, v_d'$ ist $K$-Basis von $V$,

- $f(v_i') = v_i' + a_i v_1$ für $2 \leq i \leq d$ mit $a_i \in K$.

Sei $c_i \in K$ eine Nullstelle des separablen Polynoms $Y^q - Y + a_i$, und setze $v_i := v_i' + c_i v_1$ für $2 \leq i \leq d$. dann ist $v_1, \ldots, v_d$ natürlich ebenfalls eine $K$-Basis von $V$. Außerdem gilt

$$f(v_i) = f(v_i') + c_i^q v_1 = v_i' + a_i v_1 + c_i^q v_1 = v_i + (a_i + c_i^q - c_i)v_1 = v_i \ ,$$

also $v_1, \ldots, v_d \in V_1$. Auf Grund des 2. Schrittes muß $v_1, \ldots, v_d$ eine $\mathbb{F}_q$-Basis von $V_1$ sein. □

Offensichtlich haben wir das kommutative Diagramm

$$\begin{array}{ccc} K \otimes_{\mathbb{F}_q} V_1 & \xrightarrow{\cong} & V \\ {\scriptstyle \sigma \otimes \mathrm{id}_{V_1}} \downarrow & & \downarrow {\scriptstyle f} \\ K \otimes_{\mathbb{F}_q} V_1 & \xrightarrow{\cong} & V \end{array}$$

**Corollar 2.2.** *Ist $K$ separabel abgeschlossen und $f$ etal, so besitzt $V$ eine $K$-Basis, bzgl. welcher $A_f = E_d$ gilt.*

*Beweis.* Nimm eine $\mathbb{F}_q$-Basis von $V_1$. □

**Corollar 2.3.** *Ist $K$ separabel abgeschlossen, so besteht $GL_d(K)$ aus einer einzigen $\sigma$-Konjugationsklasse.*

# 3 Diskrete Bewertungsringe

**Definition 3.1.** *Ein Hauptidealring $A$ heißt diskreter Bewertungsring, falls er genau ein maximales Ideal $\mathfrak{m} \neq \{0\}$ besitzt. Der Körper $A/\mathfrak{m}$ heißt der Restklassenkörper von $A$.*

Sei $A$ ein diskreter Bewertungsring. Aus dem Satz von der eindeutigen Primfaktorzerlegung folgt dann:

i. $A^\times = A \setminus \mathfrak{m}$;

ii. $\mathfrak{m} = \pi A$ für ein Primelement $\pi$ in $A$;

iii. $\{\pi^n A\}_{n \geq 0}$ ist die Menge der Ideale $\neq 0$ in $A$;

iv. jedes $0 \neq a \in A$ schreibt sich eindeutig als $a = \pi^{v(a)} u$ mit $v(a) \geq 0$ und $u \in A^\times$.

Letzteres definiert eine Funktion $v : A \setminus \{0\} \longrightarrow \mathbb{N} \cup \{0\}$ mit folgenden Eigenschaften

(I) $v$ ist surjektiv und unabhängig von der Wahl von $\pi$,

(II) $v(ab) = v(a) + v(b)$,

(III) $v(a + b) \geq \min(v(a), v(b))$.

**Definition 3.2.** *$v$ heißt die diskrete Bewertung von $A$.*

Sei $K$ der Quotientenkörper von $A$. Wegen (II) erhält man durch

$$v\left(\frac{a}{b}\right) := v(a) - v(b)$$

eine surjektive Abbildung $v : K^\times \longrightarrow \mathbb{Z}$, welche (II) und (III) erfüllt (die diskrete Bewertung von $K$).
Konvention: $v(0) := \infty$.
Es gilt: $A = \{x \in K : v(x) \geq 0\}$, $\mathfrak{m} = \{x \in K : v(x) > 0\}$.

**Lemma 3.3.** *Für $x, y \in K$ mit $v(x) \neq v(y)$ gilt $v(x + y) = \min(v(x), v(y))$.*

*Beweis.* Sei etwa $v(x) > v(y)$. Dann

$$v(x) > v(y) = v(y + x - x) \geq \min(v(x + y), v(-x)) = \min(v(x + y), v(x)) \ ,$$

also $v(x) > v(x + y)$ und somit

$$v(y) \geq v(x + y) \geq \min(v(x), v(y)) = v(y) \ .$$

□

**Lemma 3.4.** *Sei $L$ ein Körper und $v : L^\times \longrightarrow \mathbb{Z}$ eine surjektive Abbildung, welche (II) und (III) erfüllt; dann ist $B := \{x \in L : v(x) \geq 0\}$ ein diskreter Bewertungsring mit Quotientenkörper $L$.*

*Beweis.* Ersichtlich ist $B$ ein Ring mit $B^\times = \{x \in K : v(x) = 0\}$. Wähle ein $\pi \in B$ mit $v(\pi) = 1$. Dann ist $x = \pi^{v(x)}u$ mit $u \in B^\times$. Folglich sind die Ideale $\neq 0$ von $B$ genau die $\pi^n B$ mit $n \geq 0$. □

**Beispiele:** 1) Fixiere eine Primzahl $p$. Die $p$-adische Bewertung von $\mathbb{Q}$ ist definiert durch

$$\begin{aligned} v_p : \mathbb{Q}^\times &\longrightarrow \mathbb{Z} \\ x &\longmapsto n, \text{ falls } x = p^n \frac{a}{b} \text{ mit } p \nmid ab \ . \end{aligned}$$

Der zugehörige Bewertungsring ist $\mathbb{Z}_{(p)} = \{\frac{a}{b} \in \mathbb{Q} : p \nmid b\}$, der Restklassenkörper ist $\mathbb{F}_p$.
2) Sei $k$ ein Körper und $K := k((T))$ der Körper der formalen Laurentreihen über $k$. Dann ist

$$\begin{aligned} v: \quad k((T))^\times &\longrightarrow \mathbb{Z} \\ \sum_{n \geq n_0} a_n T^n &\longmapsto \min\{n : a_n \neq 0\} \end{aligned}$$

eine diskrete Bewertung. Der diskrete Bewertungsring ist der Ring der formalen Potenzreihen $k[[T]]$; der Restklassenkörper ist $k$.
3) Sei $P$ ein Punkt in der komplexen Ebene. Dann ist

$$\mathcal{O}_P := \quad \begin{array}{l} \text{Ring aller Funktionen, welche holomorph in einer} \\ \text{beliebig kleinen Umgebung von } P \text{ sind,} \end{array}$$

ein diskreter Bewertungsring mit

$$v(f) = \text{Nullstellenordnung von } f \text{ in } P$$

und Restklassenkörper $\mathbb{C}$.

Sei weiterhin $A$ ein diskreter Bewertungsring mit Quotientenkörper $K$ und diskreter Bewertung $v$. Für $x \in K$ setze

$$|x| := \begin{cases} e^{-v(x)} & \text{für } x \neq 0, \\ 0 & \text{für } x = 0. \end{cases}$$

Es gilt:

(IV) $|x| \geq 0$,

(V) $|x| = 0 \Longleftrightarrow x = 0$,

(VI) $|xy| = |x| \cdot |y|$,

(VII) $|x + y| \leq \max(|x|, |y|)$.

Also ist $|\ |$ eine Normfunktion auf $K$ mit der "strikten" Dreiecksungleichung (VII). Insbesondere ist $K$ bzgl. $d(x, y) := |x-y|$ ein metrischer Raum. Somit hat man für Folgen in $K$ die üblichen Begriffe:

konvergente Folge, Limes einer konvergenten Folge, Cauchyfolge.

Mit Hilfe der diskreten Bewertung lassen sich diese wie folgt ausdrücken. Sei $(x_n)_{n\in\mathbb{N}}$ eine Folge in $K$. Dann gilt:

- $(x_n)_n$ ist konvergent mit Limes $x \in K$, falls zu jedem $C > 0$ ein $N \in \mathbb{N}$ existiert, so daß $v(x - x_n) \geq C$ für alle $n \in \mathbb{N}$.

- $(x_n)_n$ ist Cauchyfolge, falls zu jedem $C > 0$ ein $N \in \mathbb{N}$ existiert, so daß $v(x_n - x_m) \geq C$ für alle $n, m \geq N$.

Wegen der strikten Dreiecksungleichung (III) vereinfacht sich Letzteres sogar zu:

- $(x_n)_n$ ist Cauchyfolge, falls zu jedem $C > 0$ ein $N \in \mathbb{N}$ existiert, so daß $v(x_{n+1} - x_n) \geq C$ für alle $n \geq N$.

**Definition 3.5.** *Der diskret bewertete Körper $K$ heißt vollständig, falls jede Cauchyfolge in $K$ konvergent ist.*

**Übungsaufgabe 3.6.** *Sei $\pi \in A$ ein Primelement, $a \in K$ und $n \in \mathbb{Z}$. Zeige unter Verwendung der strikten Dreiecksungleichung, daß die Teilmenge $a + \pi^n A$ offen und abgeschlossen in $K$ ist.*

**Satz 3.7.** *Bis auf isometrische Isomorphie gibt es genau einen vollständigen diskret bewerteten Körper $(\hat{K}, \hat{v})$, welcher $K$ als dichten Teilkörper enthält mit $\hat{v}|K^\times = v$.*

*Beweis.* Die Eindeutigkeit ergibt sich durch stetige Fortsetzung der identischen Abbildung auf $K$. Für die Existenz skizzieren wir zwei Strategien.

*Analytische Konstruktion:* Die Menge $\mathcal{C}$ aller Cauchyfolgen in $K$ ist bzgl. komponentenweiser Addition und Multiplikation ein Ring mit Eins. Mittels konstanter Folgen bettet sich $K$ in $\mathcal{C}$ ein. Die Teilmenge $\mathcal{N} \subseteq \mathcal{C}$ aller Nullfolgen ist ein maximales Ideal. Wir definieren

$$\hat{K} := \mathcal{C}/\mathcal{N} \quad \text{und} \quad \hat{v}((x_n)_n + \mathcal{N}) := \lim_{n\to\infty} v(x_n) \ .$$

*Algebraische Konstruktion:* Mit Hilfe des projektiven Limes (siehe unten) konstruiert man den diskreten Bewertungsring

$$\hat{A} := \varprojlim_n A/\mathfrak{m}^n$$

und definiert $\hat{K}$ als den Quotientenkörper von $\hat{A}$. Dazu bemerke man: Ist $a = (a_n + \mathfrak{m}^n)_n \in \hat{A}$, so gilt $a_{n+1} - a_n \in \mathfrak{m}^n$; also ist $(a_n)_n$ eine Cauchyfolge (mit Limes $a$). □

**Definition 3.8.** *$\hat{K}$ bzw. $\hat{A}$ heißt die Komplettierung von $K$ bzw. $A$.*

**Lemma 3.9.** *i. Jedes Primelement $\pi \in A$ ist auch Primelement in $\hat{A}$;*

*ii. $A$ und $\hat{A}$ haben den gleichen Restklassenkörper.*

*Beweis.* Die Eigenschaft i. gilt per Konstruktion. Für ii. erhalten wir aus der Inklusion $A \subseteq \hat{A}$ jedenfalls die Körpereinbettung $A/\pi A \subseteq \hat{A}/\pi\hat{A}$. Sei $\hat{a} \in \hat{A}$. Da einerseits $A$ dicht in $\hat{A}$ ist und andererseits $\hat{a} + \pi\hat{A}$ eine offene Umgebung von $\hat{a}$ in $\hat{A}$ ist, muß es ein $a \in A$ geben mit $a \in \hat{a} + \pi\hat{A}$. Folglich gilt die Gleichheit $A/\pi A = \hat{A}/\pi\hat{A}$. □

**Beispiele:** 1) Die Komplettierung $\mathbb{Q}_p$ von $\mathbb{Q}$ bzgl. der $p$-adischen Bewertung $v_p$ heißt der Körper der $p$-adischen Zahlen und $\mathbb{Z}_p := \hat{\mathbb{Z}}_{(p)}$ der Ring der ganzen $p$-adischen Zahlen.
2) $k((T))$ ist vollständig.

## Anhang: Der projektive Limes

Sei $(I, \leq)$ eine partielle geordnete Menge. Vorgegeben seien weiter

- eine Menge $M_i$ für jedes $i \in I$,
- Abbildungen $\alpha_{ji} : M_i \longrightarrow M_j$ für jedes Paar $i \geq j$ in $I$;

dabei gelte:

i. $\alpha_{ii} = \mathrm{id}_{M_i}$ für alle $i \in I$,

ii. $\alpha_{kj} \circ \alpha_{ji} = \alpha_{ki}$ für alle $i \geq j \geq k$ in $I$.

Man nennt $((M_i)_i, (\alpha_{ji})_{i \geq j})$ ein projektives System (von Mengen). Sein *projektiver Limes* ist definiert als die Menge

$$\varprojlim_{i \in I} M_i := \{(x_i)_i \in \prod_{i \in I} M_i : \alpha_{ji}(x_i) = x_j \text{ für alle } i \geq j\} \ .$$

**Übungsaufgabe 3.10.** *Sind alle $M_i$ Gruppen bzw. Ringe mit Eins und sind alle $\alpha_{ji}$ Gruppen- bzw. Ringhomomorphismen (man spricht dann von einem projektiven System von Gruppen bzw. Ringen), so ist $\varprojlim M_i$ eine Untergruppe bzw. ein Unterring von $\prod_{i \in I} M_i$.*

**Übungsaufgabe 3.11.** *Seien alle $M_i$ Hausdorffsche topologische Räume und alle $\alpha_{ji}$ stetige Abbildungen. Dann ist die Teilmenge $\varprojlim M_i$ in $\prod_{i \in I} M_i$ bzgl. der Produkttopologie abgeschlossen. (Man faßt $\varprojlim M_i$ als topologischen Raum bzgl. der Teilraumtopologie auf.)*

# 4 Erweiterungen diskreter Bewertungsringe

Sei $A$ ein vollständiger diskreter Bewertungsring mit Quotientenkörper $K$. Sei $v$ die diskrete Bewertung, $\mathfrak{m} \subseteq A$ das maximale Ideal, $\pi \in \mathfrak{m}$ ein Primelement und $k = A/\mathfrak{m}$ der Restklassenkörper.

**Satz 4.1.** *(Das Henselsche Lemma)*
*Sei $f \in A[T]$ ein Polynom; es gebe Polynome $g_0, h_0 \in k[T]$, so daß gilt:*
*$g_0$ ist normiert, $g_0$ und $h_0$ sind teilerfremd und $f = g_0 h_0 \bmod \mathfrak{m}$.*
*Dann existieren Polynome $g, h \in A[T]$ mit:*
*$g$ ist normiert, $g \equiv g_0 \bmod \mathfrak{m}$, $h \equiv h_0 \bmod \mathfrak{m}$ und $f = gh$.*

*Beweis.* Zunächst zeigen wir durch Induktion nach $n \in \mathbb{N}_0$, daß Polynome $g_n, h_n \in A[T]$ existieren mit:

$1_n)$ $f \equiv g_n h_n \bmod \mathfrak{m}^{n+1}$,

$2_n)$ $g_n$ ist normiert,

$3_n)$ $\deg(h_n) \leq \deg(f) - \deg(g_0)$,

$4_n)$ $g_n \equiv g_0 \bmod \mathfrak{m}$, $h_n \equiv h_0 \bmod \mathfrak{m}$.

Der Induktionsanfang $n = 0$ ergibt sich sofort aus der Voraussetzung. Seien also $g_0, \ldots, g_n$ und $h_0, \ldots, h_n$ schon konstruiert. Wir definieren

$$g_{n+1} := g_n + u_n \pi^{n+1} \quad \text{und} \quad h_{n+1} := h_n + v_n \pi^{n+1}$$

mit noch zu bestimmenden Polynomen $u_n, v_n \in A[T]$. Dann gilt jedenfalls $4_{n+1})$. Mit $g_0$ und $h_0$ müssen wegen $4_n)$ auch $g_n$ und $h_n$ modulo $\mathfrak{m}$ teilerfremd sein, also

$$k[T] = < g_n \bmod \mathfrak{m},\, h_n \bmod \mathfrak{m} > \ .$$

Wegen $1_n)$ ist $\pi^{-(n+1)}(f - g_n h_n) \in A[T]$. Also finden wir $u_n, v_n \in A[T]$ mit

$$\frac{f - g_n h_n}{\pi^{n+1}} \equiv g_n v_n + h_n u_n \bmod \mathfrak{m} \ . \tag{1}$$

Das bedeutet aber

$$\frac{f - g_{n+1} h_{n+1}}{\pi^{n+1}} \equiv 0 \bmod \mathfrak{m} \ ,$$

was gerade die Bedingung $1_{n+1})$ ist. Man beachte, daß $u_n, v_n$ jederzeit durch $u_n + \phi g_0, v_n - \phi h_0$ mit $\phi \in A[T]$ ersetzt werden können, ohne die Bedingung (1) zu verletzen. Bestimme $\phi$ mittels Division mit Rest ($g_0$ ist normiert!) so, daß $u_n = (-\phi) g_0 + r_0$ mit $\deg(r_0) < \deg(g_0)$. Auf diese Weise erreichen wir

$\deg(u_n) < \deg(g_0)$. Dann folgt $2_{n+1})$ unmittelbar aus $2_n)$. Außerdem folgt aus $3_n)$, daß

$$\begin{aligned} \deg(h_n u_n) &= \deg(h_n) + \deg(u_n) \\ &\leq (\deg(f) - \deg(g_0)) + \deg(g_0) \\ &= \deg(f) \ . \end{aligned} \tag{2}$$

Schließlich ändern wir $v_n$ noch ab, ohne das Bisherige zu verletzen, indem wir alle Koeffizienten $\equiv 0 \bmod \mathfrak{m}$ weglassen. Da $g_n$ normiert ist, folgt dann

$$\begin{aligned} \deg(g_0) + \deg(v_n) &\overset{4_n)}{=} \deg(g_n) + \deg(v_n) = \deg(g_n v_n) = \deg(g_n v_n \bmod \mathfrak{m}) \\ &\overset{(1)}{\leq} \max(\deg(\frac{f - g_n h_n}{\pi^{n+1}} \bmod \mathfrak{m}), \deg(h_n u_n \bmod \mathfrak{m})) \\ &\leq \max(\deg(f - g_n h_n), \deg(h_n u_n)) \\ &\overset{(2)}{\leq} \max(\deg(f - g_n h_n), \deg(f)) \\ &\overset{3_n)}{=} \deg(f) \ . \end{aligned}$$

Mit Hilfe von $3_n)$ erhalten wir schließlich

$$\deg(h_{n+1}) \leq \max(\deg(h_n), \deg(v_n)) \leq \deg(f) - \deg(g_0) \ ,$$

also die Bedingung $3_{n+1})$. Damit ist der Induktionsbeweis abgeschlossen. Wir definieren jetzt

$$g := g_0 + \sum_{n \geq 0} u_n \pi^{n+1}, \qquad h := h_0 + \sum_{n \geq 0} v_n \pi^{n+1} \ .$$

Wegen der Vollständigkeit von $A$ konvergieren diese Reihen koeffizientenweise (vereinfachtes Cauchy-Kriterium) gegen formale Potenzreihen $g, h \in A[[T]]$. Da die Partialsummen $g_n, h_n$ aber nach $2_n) - 4_n)$ unabhängig von $n$ beschränkten Grad haben, gilt schon $g, h \in A[T]$. Offensichtlich ist $g \equiv g_0 \bmod \mathfrak{m}$ und $h \equiv h_0 \bmod \mathfrak{m}$. Wegen $\deg(u_n) < \deg(g_0)$ ist $g$ normiert. Aus $1_n)$ folgt

$$f - gh \equiv f - g_n h_n \equiv 0 \bmod \mathfrak{m}^{n+1} \ ,$$

d. h. die Koeffizienten des Polynoms $f - gh$ liegen in $\bigcap_{n \in \mathbb{N}} \mathfrak{m}^n = \{0\}$. Somit ist $f = gh$. □

**Corollar 4.2.** *Sei $f \in K[T]$ ein normiertes irreduzibles Polynom; dann gilt: $f(0) \in A \Longleftrightarrow f \in A[T]$.*

*Beweis.* Sei $m \in \mathbb{N}_0$ minimal, so daß $\pi^m f \in A[T]$. Wir führen die Annahme, daß $m \geq 1$, zum Widerspruch. Da $f$ normiert und $m \geq 1$ minimal ist, gilt

$$\pi^m f \not\equiv 0 \bmod \mathfrak{m} \quad \text{mit} \quad \deg(\pi^m f \bmod \mathfrak{m}) < \deg(f) \ .$$

Wegen $f(0) \in A$ und $m \geq 1$ ist $\pi^m f(0) \in \mathfrak{m}$. Also

$$\pi^m f \equiv T^r h_0 \bmod \mathfrak{m}$$

für ein $h_0 \in k[T]$ mit $h_0(0) \neq 0$ und $1 \leq r < \deg(f)$. Die Anwendung des Henselschen Lemmas liefert dann eine echte Faktorisierung des Polynoms $\pi^m f$, was im Widerspruch zur Irreduzibilität von $f$ steht. □

Sei $L/K$ eine fixierte endliche Körpererweiterung.

**Satz 4.3.** *Auf $L$ existiert genau eine diskrete Bewertung $v_L$ mit $v_L|K^\times = e(L/K) \cdot v$ für ein eindeutig bestimmtes $e(L/K) \in \mathbb{N}$; dabei ist $e(L/K)$ ein Teiler von $[L:K]$, und der diskret bewertete Körper $(L, v_L)$ ist vollständig.*

*Beweis.* Sei $d := [L:K]$ und $N : L^\times \longrightarrow K^\times$ die Normalabbildung. Wir definieren

$$\tilde{v}_L := v \circ N : L^\times \longrightarrow \mathbb{Z} \ .$$

Die Eigenschaft (II) besitzt $\tilde{v}_L$ per Konstruktion. Die Eigenschaft (III) weisen wir in mehreren Schritten nach.

*1. Schritt:* Wir zeigen zunächst, daß für ein $x \in L$ mit $\tilde{v}_L(x) \geq 0$ auch $\tilde{v}_L(1+x) \geq 0$ gilt. Sei $p(T)$ das Minimalpolynom von $x$ über $K$. Dann gilt

$$p(0)^{[L:K(x)]} = (-1)^d N(x) \ .$$

Wegen $\tilde{v}_L(x) \geq 0$ gilt $0 \leq v(N(x)) = [L:K(x)] \cdot v(p(0))$ und damit $p(0) \in A$. Nach Cor. 4.2 ist also $p(T) \in A[T]$ und folglich $p(-1) \in A$, d. h. $v(p(-1)) \geq 0$. Aber $p(T-1)$ ist das Minimalpolynom von $1+x$ über $K$. Also

$$p(-1)^{[L:K(x)]} = (-1)^d N(1+x)$$

und somit $\tilde{v}_L(1+x) = v(N(1+x)) = [L:K(x)] \cdot v(p(-1)) \geq 0$.

*2. Schritt:* Sei $x \in L$ mit $\tilde{v}_L(x) \leq 0$. Dann ist $\tilde{v}_L(x^{-1}) \geq 0$ und nach dem ersten Schritt also $\tilde{v}_L(1+x^{-1}) \geq 0$. Hieraus folgt

$$\tilde{v}_L(1+x) = \tilde{v}_L(x(1+x^{-1})) = \tilde{v}_L(x) + \tilde{v}_L(1+x^{-1}) \geq \tilde{v}_L(x) = \min(0, \tilde{v}_L(x)).$$

*3. Schritt:* Seien nun $x, y \in L$. Wir können natürlich $x \neq 0$ annehmen. Dann ist

$$\begin{aligned}\tilde{v}_L(x+y) &= \tilde{v}_L(x) + \tilde{v}_L(1+\frac{y}{x}) \geq \tilde{v}_L(x) + \min(0, \tilde{v}_L(\frac{y}{x})) \\ &= \min(\tilde{v}_L(x), \tilde{v}_L(x) + \tilde{v}_L(\frac{y}{x})) = \min(\tilde{v}_L(x), \tilde{v}_L(y)).\end{aligned}$$

Wegen $\tilde{v}_L|K^\times = d \cdot v$ gilt $d\mathbb{Z} \subseteq \mathrm{im}(\tilde{v}_L) \subseteq \mathbb{Z}$. Folglich existiert genau ein Teiler $c|d$, so daß $\mathrm{im}(\tilde{v}_L) = c\mathbb{Z}$. Dann ist

$$v_L := \frac{1}{c}\tilde{v}_L : L^\times \longrightarrow \mathbb{Z}$$

surjektiv und somit eine diskrete Bewertung von $L$ nach Lemma 3.4, welche $v_L|K^\times = \frac{d}{c} \cdot v$ erfüllt. Setze also $e(L/K) := \frac{d}{c}$.

Um die Vollständigkeit von $(L, v_L)$ einzusehen, benutzen wird die Normfunktion $|\ |$ auf $K$ und fassen $L$ als $K$-Vektorraum auf. Dann ist

$$|x|_L := e^{-v_L(x)/e(L/K)}$$

wegen $|\ |_L|K = |\ |$ eine $K$-Vektorraumnorm auf $L$. Andererseits fixieren wir eine Basis $e_1, \ldots e_d$ von $L$ als $K$-Vektorraum und erhalten durch

$$\left|\sum_{i=1}^{d} a_i e_i\right|' := \max(|a_1|, \ldots, |a_d|)$$

eine zweite $K$-Vektorraumnorm auf $L$. Bzgl. letzterer ist $L$ ersichtlich vollständig.

**Faktum:** *Alle Vektorraumnormen auf einem endlich-dimensionalen $K$-Vektorraum sind äquivalent.*

Folglich ist $L$ auch bzgl. $|\ |_L$ und damit bzgl. $v_L$ vollständig. Es bleibt, die Eindeutigkeit von $v_L$ zu beweisen. Sei $w_L$ eine weitere diskrete Bewertung auf $L$ mit $w_L|K^\times = b \cdot v$ für ein $b \in \mathbb{N}$. Dann sind

$$|x|_L := e^{-v_L(x)/e(L/K)} \qquad \text{und} \quad \|x\|_L := e^{-w_L(x)/b}$$

beides Normfunktionen auf dem Körper $L$, welche die Normfunktion $|\ |$ auf $K$ fortsetzen. Aus obigem Faktum folgt, daß $|\ |_L$ und $\|\ \|_L$ als $K$-Vektorraumnormen äquivalent sind.

**Weiteres Faktum:** *Zu je zwei äquivalenten Normfunktionen $\|\ \|$ und $\|\ \|'$ auf $L$ gibt es ein $\sigma > 0$ mit $\|\ \|' = \|\ \|^\sigma$.*

Da $|\ |_L$ und $\|\ \|_L$ beide $|\ |$ fortsetzen, muß in diesem Falle $\sigma = 1$, also $|\ |_L = \|\ \|_L$ gelten. Es folgt $bv_L = e(L/K)w_L$. Durch Einsetzen eines Primelementes bzgl. $v_L$ erhalten wir $e(L/K)|b$ und aus Symmetriegründen dann $b = e(L/K)$, also $v_L = w_L$. □

Wir halten fest, daß $v_L(\pi) = e(L/K)$ gilt.

**Definition 4.4.** *$e(L/K)$ heißt der Verzweigungsindex von $L/K$.*

Sei $A_L \subseteq L$ der Bewertungsring zu $v_L, \pi_L \in A_L$ ein Primelement und $k_L = A_L/\pi_L A_L$ der Restklassenkörper. Wegen $\pi A_L = \pi_L^{e(L/K)} A_L$ gilt $\mathfrak{m} = \pi A \subseteq \pi_L A_L$. Die Inklusion $A \subseteq A_L$ induziert also eine Inklusion $k \subseteq k_L$ der Restklassenkörper.

**Lemma 4.5.** *$[k_L : k] < \infty$.*

*Beweis.* Seien $\bar{y}_1, \ldots, \bar{y}_n \in k_L$ linear unabhängig über $k$. Wähle $y_1, \ldots, y_n \in A_L$ mit $\bar{y}_i = y_i + \pi_L A_L$. Es genügt zu zeigen, daß $y_1, \ldots, y_n$ linear unabhängig über $K$ sind. Sei also $a_1 y_1 + \ldots + a_n y_n = 0$ mit $a_i \in K$, welche nicht alle $= 0$ sind. Nach Multiplikation mit einer geeigneten Potenz von $\pi$ können wir $a_1, \ldots, a_n \in A$ und etwa $a_1 \in A^\times$ annehmen. Dann läßt sich die Gleichung modulo $\mathfrak{m}$ lesen, und wir erhalten den Widerspruch, daß alle $a_i$ und insbesondere $a_1$ in $\mathfrak{m}$ liegen müssen. □

**Definition 4.6.** *$f(L/K) := [k_L : k]$ heißt der Trägheitsgrad von $L|K$.*

**Übungsaufgabe 4.7.** *Für endliche Erweiterungen $M/L/K$ gilt*

$$e(M/K) = e(M/L)e(L/K) \quad \textit{und} \quad f(M/K) = f(M/L)f(L/K)\ .$$

**Definition 4.8.** *Die Erweiterung $L/K$ heißt*
- *unverzweigt, falls $e(L/K) = 1$ und $k_L/k$ separabel ist,*
- *total-verzweigt, falls $e(L/K) = [L : K]$.*

Für eine unverzweigte Erweiterung $L/K$ ist jedes Primelement für $K$ auch ein Primelement für $L$.

**Lemma 4.9.** *Sei $R \subseteq A$ ein Vertretersystem für $A/\mathfrak{m}$ mit $0 \in R$; weiter seien $\pi_m \in K$ für alle $m \in \mathbb{Z}$ fixierte Elemente mit $v(\pi_m) = m$. Dann gilt:*

*i. Jede Reihe $\sum_{m \geq m_0} a_m \pi_m$ mit $a_m \in R$ konvergiert in $K$;*

*ii. jedes $x \in K$ besitzt eine eindeutig bestimmte Darstellung als Summe $x = \sum_{m \geq m_0} a_m \pi_m$ mit $a_m \in R$; dabei gilt $v(x) = \min\{m : a_m \neq 0\}$.*

*Beweis.* i. Wegen $v(a_m \pi_m) \geq m$ folgt dies sofort aus dem vereinfachten Cauchy-Kriterium. Man beachte, daß alle Elemente $\neq 0$ in $R$ Einheiten in $A$ sind, also Bewertung 0 besitzen. Deswegen haben alle Partialsummen nach Lemma 3.3 und damit auch die konvergente Summe die in ii. angegebene

Bewertung. Insbesondere ist die konvergente Summe $= 0$ genau dann, wenn alle $a_m = 0$ sind.

ii. Es bleibt, die Existenz und Eindeutigkeit der behaupteten Darstellung für ein $x \in K^\times$ zu zeigen. Sei $m_0 := v(x)$. Für die Existenz genügt es, induktiv eine Folge $(a_m)_{m \geq m_0}$ in $R$ zu konstruieren, so daß gilt

$$v(x - s_m) \geq m + 1 \quad \text{für } s_m := \sum_{m_0 \leq \mu \leq m} a_\mu \pi_\mu \ .$$

Aus $v(x) = m_0$ folgt $v(x\pi_{m_0}^{-1}) = 0$. Also existiert ein $a_{m_0} \in R$, so daß $v(x\pi_{m_0}^{-1} - a_{m_0}) > 0$ und somit $v(x - s_{m_0}) > v(\pi_{m_0}) = m_0$. Seien $a_{m_0}, \ldots, a_m$ und damit $s_m$ schon konstruiert. Dann gilt $v((x - s_m)\pi_{m+1}^{-1}) \geq 0$. Folglich existiert ein $a_{m+1} \in R$ mit $v((x - s_m)\pi_{m+1}^{-1} - a_{m+1}) > 0$, was $v(x - s_{m+1}) > v(\pi_{m+1}) = m + 1$ impliziert.
Für die Eindeutigkeit sei $x = \sum_{m \geq m_0} a_m \pi_m = \sum_{n \geq n_0} b_n \pi_n$ mit $a_m, b_n \in R$ und $a_{m_0} \neq 0 \neq b_{n_0}$. Wie schon gezeigt, ist dann $m_0 = v(x) = n_0$ und damit

$$(a_{m_0} - b_{m_0})\pi_{m_0} = \sum_{m > m_0} (b_m - a_m)\pi_m \ ,$$

also $v((a_{m_0} - b_{m_0})\pi_{m_0}) > m_0$. Folglich gilt $v(a_{m_0} - b_{m_0}) > 0$, was $a_{m_0} + \mathfrak{m} = b_{m_0} + \mathfrak{m}$ und dann sogar $a_{m_0} = b_{m_0}$ bedeutet. Dieses Argument induktiv wiederholend erhält man $a_m = b_m$ für alle $m \geq m_0$. □

**Beispiel:** Sei $K = \mathbb{Q}_p$, setze $\pi_m = p^m$ und $R := \{0, 1, \ldots, p-1\}$. Jedes $x \in \mathbb{Q}_p$ besitzt eine eindeutige *p-adische Entwicklung*

$$x = \sum_{m \geq m_0} a_m p^m \quad \text{mit } 0 \leq a_m < p \ .$$

**Übungsaufgabe 4.10.** *Man überlege sich zumindest an Beispielen, daß die p-adischen Entwicklungen im obigen Beispiel nach analogen Regeln addiert und multipliziert werden, wie sie für die Dezimalentwicklung rationaler Zahlen gelten.*

**Satz 4.11.** *i.* $[L : K] = e(L/K)f(L/K)$*;*

*ii.* $A_L$ *ist ein freier* $A$*-Modul vom Range* $[L : K]$*.*

*Beweis.* Wir kürzen ab $e := e(L/K)$ und $f := f(L/K)$. Weiter seien

$$\pi_m := \pi^n \pi_L^i, \text{ falls } m = ne + i \text{ mit } 0 \leq i < e \ ,$$

und $R \subseteq A$ ein fixiertes Vertretersystem für $A/\mathfrak{m}$ mit $0 \in R$. Schließlich fixieren wir Elemente $y_1, \ldots, y_f \in A_L$, deren Restklassen eine $k$-Basis von $k_L$ bilden. Dann ist $\{r_1 y_1 + \ldots + r_f y_f : r_j \in R\} \subseteq A_L$ ein Vertretersystem für $A_L/\pi_L A_L$. Nach Lemma 4.9 besitzt jedes $x \in L$ eine eindeutige Darstellung als konvergente Summe

$$x = \sum_{m \geq m_0} a_m \pi_m \quad \text{mit } a_m = r_1^{(m)} y_1 + \ldots + r_f^{(m)} y_f,\ r_j^{(m)} \in R\ .$$

Durch Einsetzen und Umordnen ergibt sich die eindeutige Darstellung

$$x = \sum_{i=0}^{e-1} \Big( \sum_n a_{ne+i} \pi^n \Big) \pi_L^i = \sum_{i=0}^{e-1} \sum_{j=1}^{f} \Big( \sum_n r_j^{(ne+i)} \pi^n \Big) y_j \pi_L^i\ .$$

Für die Koeffizienten $c_{i,j} := \sum_n r_j^{(ne+i)} \pi^n$ gilt dabei:

- $c_{i,j} \in K$,
- $c_{i,j} \in A$ für alle $i, j \iff x \in A_L$.

Somit ist $\{y_j \pi_L^i\}_{i,j}$ sowohl eine $K$-Basis von $L$ als auch eine $A$-Basis von $A_L$. Insbesondere muß $ef = [L : K]$ gelten. □

Wir sehen insbesondere, daß $L/K$ unverzweigt ist genau dann, wenn $k_L/k$ separabel ist mit $[k_L : k] = [L : K]$.

**Bemerkung 4.12.** *Sei $p(T)$ das Minimalpolynom über $K$ eines Elementes $x \in L$, dann gilt: $x \in A_L \iff p \in A[T]$.*

*Beweis.* Auf Grund der Konstruktion von $v_L$ im Beweis von Satz 4.3 und Satz 4.11.i gilt

$$v_L(x) = \tfrac{[L:K(x)]}{f(L/K)}\, v(p(0))\ .$$

Deswegen folgt die Behauptung aus Cor. 4.2. □

**Satz 4.13.** *Seien $K \subseteq L_1, L_2 \subseteq L$ zwei Teilererweiterungen; mit $L_1/K$ und $L_2/K$ ist auch das Kompositum $L_1 L_2/K$ unverzweigt.*

*Beweis.* Wegen der Multiplikativität der Körpergrade und der Transitivität der Separabilität genügt es zu zeigen, daß mit $L_1/K$ auch $L_1 L_2/L_2$ unverzweigt ist. Nach dem Satz vom primitiven Element existiert ein $\bar{\alpha} \in k_{L_1}$ mit $k_{L_1} = k(\bar{\alpha})$. Wir fixieren ein $\alpha \in A_{L_1}$ mit $\bar{\alpha} = \alpha + \pi_{L_1} A_{L_1}$ und bezeichnen mit

$p(T)$ das Minimalpolynom von $\alpha$ über $K$. Auf Grund der vorausgeschickten Bemerkung liegt $p(T)$ in $A[T]$. Wegen

$$[k_{L_1} : k] \leq \deg(p \bmod \mathfrak{m}) = \deg(p) = [K(\alpha) : K] \leq [L_1 : K] = [k_{L_1} : k]$$

muß $L_1 = K(\alpha)$ gelten und $p \bmod \mathfrak{m}$ das Minimalpolynom von $\bar{\alpha}$ über $k$ sein. Insbesondere ist $L_1 L_2 = L_2(\alpha)$. Das Minimalpolynom $q(T)$ von $\alpha$ über $L_2$ ist ein Teiler von $p(T)$ in $A_{L_2}[T]$ auf Grund des Gaußschen Lemmas. Folglich ist $q \bmod \pi_{L_2} A_{L_2}$ ein Teiler von $p \bmod \mathfrak{m}$, ist somit separabel und muß auf Grund des Henselschen Lemmas dann auch irreduzibel sein (sonst wäre $q$ reduzibel). Also gilt

$$\begin{aligned}[k_{L_1 L_2} : k_{L_2}] &\leq [L_1 L_2 : L_2] = \deg(q) = \deg(q \bmod \pi_{L_2} A_{L_2}) \\ &= [k_{L_2}(\bar{\alpha}) : k_{L_2}] \leq [k_{L_1 L_2} : k_{L_2}],\end{aligned}$$

und es folgt die Separabilität von $k_{L_1 L_2} = k_{L_2}(\bar{\alpha})$ über $k_{L_2}$ mit $[k_{L_1 L_2} : k_{L_2}] = [L_1 L_2 : L_2]$. □

**Definition 4.14.** *Die maximale über $K$ unverzweigte Teilererweiterung von $L/K$ heißt der Trägheitskörper von $L/K$.*

**Übungsaufgabe 4.15.** *Sei $T$ der Trägheitskörper von $L/K$; dann ist $T/K$ separabel, und $k_T/k$ ist die maximale separable Teilererweiterung von $k_L/k$.*

**Bemerkung 4.16.** *Sei $\sigma \in \mathrm{Aut}_K(L)$. Aus der Eindeutigkeitsaussage in Satz 4.3 folgt $v_L \circ \sigma = v_L$ und somit $\sigma(A_L) = A_L$. Folglich induziert $\sigma$ auf den Restklassen einen Automorphismus $\bar{\sigma} \in \mathrm{Aut}_k(k_L)$. Durch $\sigma \longmapsto \bar{\sigma}$ ist ein Gruppenhomomorphismus $\mathrm{Aut}_K(L) \longrightarrow \mathrm{Aut}_k(k_L)$ gegeben.*

# 5 Wittvektoren

Sei $p$ eine ein für alle Mal fixierte Primzahl. Für jede ganze Zahl $n \geq 0$ heißt

$$\Phi_n(X_0, \ldots X_n) := \sum_{i=0}^{n} p^i X_i^{p^{n-i}} = X_0^{p^n} + pX_1^{p^{n-1}} + \ldots + p^n X_n$$

das $n$-te *Wittpolynom*. Es gilt $\Phi_0(X_0) = X_0$ und

$$\begin{aligned}\Phi_{n+1}(X_0, \ldots, X_{n+1}) &= \Phi_n(X_0^p, \ldots, X_n^p) + p^{n+1} X_{n+1} \\ &= X_0^{p^{n+1}} + p\,\Phi_n(X_1, \ldots, X_{n+1})\ .\end{aligned} \tag{3}$$

Sei $A$ ein beliebiger (kommutativer) Ring mit Eins. Wir sagen, daß $p1_A$ kein Nullteiler in $A$ ist, falls die Abbildung $A \xrightarrow{p\cdot} A$ injektiv ist. Im Falle $p1_A \in A^\times$ ist diese Abbildung natürlich sogar bijektiv.

**Lemma 5.1.** *Für $m, n \geq 1$ und $a, b \in A$ gilt:*

$$a \equiv b \bmod p^m A \quad \Longrightarrow a^{p^n} \equiv b^{p^n} \bmod p^{m+n} A \ .$$

*Beweis.* Per Induktion genügt es, den Fall $n = 1$ zu betrachten. Wir benutzen dazu das Polynom

$$P(X, Y) := \sum_{i=0}^{p-1} X^i Y^{p-1-i} \in \mathbb{Z}[X, Y] \ .$$

Aus der Voraussetzung folgt

$$P(a, b) \equiv P(a, a) \equiv p a^{p-1} \bmod p^m A$$

und damit $P(a, b) \in pA$. Wegen $a^p - b^p = (a - b)P(a, b)$ folgt daraus die Behauptung. □

**Lemma 5.2.** *Für $m \geq 1$, $n \geq 0$ und $a_0, \ldots, a_n, b_0, \ldots, b_n \in A$ gilt:*

*i.* $a_i \equiv b_i \bmod p^m A$ *für* $0 \leq i \leq n$

$$\Longrightarrow \Phi_i(a_0, \ldots, a_i) \equiv \Phi_i(b_0, \ldots, b_i) \bmod p^{m+i} A \text{ für alle } 0 \leq i \leq n;$$

*ii. ist $p1_A$ kein Nullteiler in $A$, so gilt in i. auch die Umkehrung.*

*Beweis.* Beide Aussagen werden per Induktion nach $n$ bewiesen. Beide Male ist der Induktionsanfang $n = 0$ trivial. Sei also $n \geq 1$.

i. Nach Voraussetzung und Lemma 5.1 gilt

$$a_i^p \equiv b_i^p \bmod p^{m+1} A \quad \text{für } 0 \leq i \leq n - 1$$

und damit

$$\Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \equiv \Phi_{n-1}(b_0^p, \ldots, b_{n-1}^p) \bmod p^{m+n} A$$

nach Induktionsannahme. Wegen der Rekursionsformel (3) für $\Phi_n$ impliziert Letzteres

$$\Phi_n(a_0, \ldots, a_n) - p^n a_n \equiv \Phi_n(b_0, \ldots, b_n) - p^n b_n \bmod p^{m+n} A \ .$$

Da aber $a_n \equiv b_n \bmod p^m A$, ist $p^n a_n \equiv p^n b_n \bmod p^{m+n} A$ und folglich

$$\Phi_n(a_0, \ldots, a_n) \equiv \Phi_n(b_0, \ldots, b_n) \bmod p^{m+n} A \ .$$

ii. Auf Grund der Induktionsannahme haben wir $a_i \equiv b_i \bmod p^m A$ für $0 \leq i \leq n-1$. Wie eben folgt daraus

$$\Phi_n(a_0, \ldots, a_n) - p^n a_n \equiv \Phi_n(b_0, \ldots, b_n) - p^n b_n \bmod p^{m+n} A \ .$$

Nach Voraussetzung gilt eine solche Kongruenz aber auch schon für die linken Summanden. Also erhalten wir $p^n(a_n - b_n) \in p^{m+n}A$ und damit $a_n - b_n \in p^m A$ wegen der zusätzlichen Voraussetzung. □

Sei

$$A^{\mathbb{N}_0} := \{(a_0, a_1, \ldots) : a_n \in A\}$$

das abzahlbar unendliche direkte Produkt des Ringes $A$ mit sich selbst (Addition und Multiplikation erfolgen also komponentenweise). Wir führen folgende Abbildungen ein:

$$\begin{array}{rccc} f_A : & A^{\mathbb{N}_0} & \longrightarrow & A^{\mathbb{N}_0} \\ & (a_0, a_1, a_2, \ldots) & \longmapsto & (a_1, a_2, \ldots) \end{array}$$

(ein Ringendomorphismus),

$$\begin{array}{rccc} v_A : & A^{\mathbb{N}_0} & \longrightarrow & A^{\mathbb{N}_0} \\ & (a_0, a_1, a_2, \ldots) & \longmapsto & (0, pa_0, pa_1, \ldots) \end{array}$$

(respektiert Addition, aber nicht Multiplikation und das Einselement),

$$\begin{array}{rccc} \Phi_n : & A^{\mathbb{N}_0} & \longrightarrow & A \\ & (a_0, a_1, \ldots) & \longmapsto & \Phi_n(a_0, \ldots, a_n) \end{array}$$

und

$$\begin{array}{rccc} \Phi_A : & A^{\mathbb{N}_0} & \longmapsto & A^{\mathbb{N}_0} \\ & \mathbf{a} & \longmapsto & (\Phi_0(\mathbf{a}), \Phi_1(\mathbf{a}), \Phi_2(\mathbf{a}), \ldots) \ . \end{array}$$

**Lemma 5.3.** *i. Ist $p1_A$ kein Nullteiler in $A$, so ist $\Phi_A$ injektiv;*

*ii. ist $p1_A \in A^\times$, so ist $\Phi_A$ bijektiv.*

*Beweis.* Seien $\mathbf{a} = (a_n)_n$, $\mathbf{u} = (u_n)_n \in A^{\mathbb{N}_0}$. Wegen der Rekursionsformel (3) für die $\Phi_n$ ist die Relation $\Phi_A(\mathbf{a}) = \mathbf{u}$ gleichbedeutend mit dem Gleichungssystem

$$\begin{aligned} & u_0 = a_0, \\ & u_n = \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n a_n \quad \text{für } n \geq 1 \ . \end{aligned} \tag{4}$$

Unter der Voraussetzung in i. bzw. ii. ist somit $\mathbf{a}$ in induktiver Weise durch $\mathbf{u}$ eindeutig bestimmt bzw. kann induktiv aus $\mathbf{u}$ eindeutig berechnet werden. □

**Zusatz 5.4.** *Aus dem Gleichungssystem* (4) *liest man Folgendes ab: Seien* $\mathbf{a} = (a_n)_n, \mathbf{u} = (u_n)_n \in A^{\mathbb{N}_0}$ *mit* $\Phi_A(\mathbf{a}) = \mathbf{u}$. *Sei* $B \subseteq A$ *ein Unterring mit der Eigenschaft, daß die additive Abbildung* $A/B \xrightarrow{p\cdot} A/B$ *injektiv ist. Dann gilt für jedes* $m \geq 0$*:*

$$u_0, \ldots, u_m \in B \Longleftrightarrow a_0, \ldots, a_m \in B \ .$$

**Satz 5.5.** *Der Ring* $A$ *besitze einen Endomorphismus* $\sigma$ *mit*

$$\sigma(a) \equiv a^p \bmod pA \quad \textit{für alle } a \in A \ .$$

*Dann gilt:*

*i. Gegeben* $n \geq 1$ *und* $a_0, \ldots, a_{n-1} \in A$ *setze* $u_i := \Phi_i(a_0, \ldots, a_i)$ *für* $0 \leq i \leq n-1$*; für ein* $u_n \in A$ *gilt dann:*

$$u_n = \Phi_n(a_0, \ldots, a_n) \textit{ für ein } a_n \in A \Longleftrightarrow \sigma(u_{n-1}) \equiv u_n \bmod p^n A \ .$$

*ii.* $A' := \mathrm{im}(\Phi_A)$ *ist ein Unterring von* $A^{\mathbb{N}_0}$*, für welchen gilt:*

- $f_A(A') \subseteq A'$, $v_A(A') \subseteq A'$,
- $A' = \{(u_n)_n \in A^{\mathbb{N}_0} : \sigma(u_n) \equiv u_{n+1} \bmod p^{n+1}A$ *für alle* $n \geq 0\}$.

*Beweis.* i. Nach Voraussetzung an $\sigma$ gilt $\sigma(a_i) \equiv a_i^p \bmod pA$ für alle $0 \leq i \leq n-1$. Die Anwendung von Lemma 5.2.i. mit $m = 1$ liefert

$$\sigma(u_{n-1}) = \Phi_{n-1}(\sigma(a_0), \ldots, \sigma(a_{n-1})) \equiv \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \bmod p^n A \ .$$

Ein $a_n \in A$ mit $u_n = \Phi_n(a_0, \ldots, a_n) = \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) + p^n a_n$ existiert genau dann, wenn $u_n - \Phi_{n-1}(a_0^p, \ldots, a_{n-1}^p) \in p^n A$, also genau dann, wenn $u_n - \sigma(u_{n-1}) \in p^n A$.

ii. Nach i. besitzt $A'$ als Teilmenge von $A^{\mathbb{N}_0}$ die behauptete Beschreibung. Die restlichen Behauptungen lassen sich daraus direkt ablesen.

□

Wir wenden diesen Satz an auf den Polynomring

$$A := \mathbb{Z}[X_0, X_1, \ldots, Y_0, Y_1, \ldots]$$

über $\mathbb{Z}$ in zweimal abzählbar unendlich vielen Variablen. Offensichtlich ist $p1_A$ kein Nullteiler in $A$. Wir betrachten auf $A$ den Ringendomorphismus $\theta$ definiert durch

$$\theta|\mathbb{Z} := \mathrm{id}_{\mathbb{Z}}, \ \theta(X_i) := X_i^p \text{ und } \theta(Y_i) := Y_i^p \text{ für alle } i \geq 0 \ .$$

**Lemma 5.6.** $\theta(a) \equiv a^p \bmod pA$ *für alle* $a \in A$.

*Beweis.* Die Teilmenge $\{a \in A : \theta(a) \equiv a^p \bmod pA\}$ ist ein Unterring von $A$, welcher nach dem kleinen Satz von Fermat $\mathbb{Z}$ und per Definition von $\theta$ alle Variablen $X_i$ und $Y_i$ enthält. Damit muß er aber gleich $A$ sein. □

Setze $\mathbf{X} := (X_0, X_1, \ldots)$ und $\mathbf{Y} := (Y_0, Y_1, \ldots)$ in $A^{\mathbb{N}_0}$. Wegen Lemma 5.3.i. und Satz 5.5.ii. existieren dann eindeutig bestimmte Elemente $\mathbf{S} = (S_n)_n$, $\mathbf{P} = (P_n)_n$, $\mathbf{I} = (I_n)_n$ und $\mathbf{F} = (F_n)_n$ in $A^{\mathbb{N}_0}$ mit

$$\begin{aligned} \Phi_A(\mathbf{S}) &= \Phi_A(\mathbf{X}) + \Phi_A(\mathbf{Y}), \\ \Phi_A(\mathbf{P}) &= \Phi_A(\mathbf{X})\Phi_A(\mathbf{Y}), \\ \Phi_A(\mathbf{I}) &= -\Phi_A(\mathbf{X}), \\ \Phi_A(\mathbf{F}) &= f_A(\Phi_A(\mathbf{X})) \end{aligned}$$

bzw. ausgeschrieben

$$\begin{aligned} \Phi_n(S_0, \ldots, S_n) &= \Phi_n(X_0, \ldots, X_n) + \Phi_n(Y_0, \ldots, Y_n), \\ \Phi_n(P_0, \ldots, P_n) &= \Phi_n(X_0, \ldots, X_n)\Phi_n(Y_0, \ldots, Y_n), \\ \Phi_n(I_0, \ldots, I_n) &= -\Phi_n(X_0, \ldots, X_n), \\ \Phi_n(F_0, \ldots, F_n) &= \Phi_{n+1}(X_0, \ldots, X_{n+1}) \end{aligned} \tag{5}$$

für alle $n \geq 0$. Aus dem Zusatz 5.4 folgt

$$\begin{aligned} S_n, P_n &\in \mathbb{Z}[X_0, \ldots, X_n, Y_0, \ldots, Y_n], \\ I_n &\in \mathbb{Z}[X_0, \ldots, X_n], \\ F_n &\in \mathbb{Z}[X_0, \ldots, X_{n+1}]. \end{aligned}$$

**Lemma 5.7.** $F_n \equiv X_n^p \bmod pA$ *für alle* $n \geq 0$.

*Beweis.* Wir haben

$$\begin{aligned} \Phi_n(F_0, \ldots, F_n) = \Phi_{n+1}(X_0, \ldots, X_{n+1}) &= \Phi_n(X_0^p, \ldots, X_n^p) + p^{n+1}X_{n+1} \\ &\equiv \Phi_n(X_0^p, \ldots, X_n^p) \bmod p^{n+1}A\ . \end{aligned}$$

Damit folgt die Behauptung aus Lemma 5.2.ii. □

Die $S_n, P_n, I_n, F_n$ lassen sich mit Hilfe des Gleichungssystems (4) induktiv explizit berechnen.

**Beispiele:** 1) $S_0 = X_0 + Y_0$, $S_1 = X_1 + Y_1 - \sum_{i=1}^{p-1} \frac{1}{p}\binom{p}{i} X_0^i Y_0^{p-i}$.
2) $P_0 = X_0Y_0$, $P_1 = pX_1Y_1 + X_0^pY_1 + X_1Y_0^p$.
3) $F_0 = X_0^p + pX_1$, $F_1 = X_1^p + pX_2 - \sum_{i=0}^{p-1} \binom{p}{i} p^{p-i-1} X_0^{pi} X_1^{p-i}$.

**Übungsaufgabe 5.8.** *1)* $S_n - X_n - Y_n \in \mathbb{Z}[X_0, \ldots, X_{n-1}, Y_0, \ldots, Y_{n-1}]$. *2) Im Falle* $p \neq 2$ *gilt* $I_n = -X_n$ *für alle* $n \geq 0$.

Sei $B$ ein beliebiger (kommutativer) Ring mit Eins. Einerseits haben wir den als direktes Produkt definierten Ring $(B^{\mathbb{N}_0}, +, \cdot)$. Für jeden Ringhomomorphismus $\rho : B_1 \longrightarrow B_2$ (der stets die Eins respektieren soll) ist

$$\begin{array}{rccc} \rho^{\mathbb{N}_0} : & B_1^{\mathbb{N}_0} & \longrightarrow & B_2^{\mathbb{N}_0} \\ & (b_n)_n & \longmapsto & (\rho(b_n))_n \end{array}$$

ebenfalls ein Ringhomomorphismus. Andererseits definieren wir auf der Menge $W(B) := B^{\mathbb{N}_0}$ eine neue "Addition"

$$(a_n)_n \boxplus (b_n)_n := (S_n(a_0, \ldots, a_n, b_0, \ldots, b_n))_n$$

und eine neue "Multiplikation"

$$(a_n)_n \boxtimes (b_n)_n := (P_n(a_0, \ldots, a_n, b_0, \ldots, b_n))_n \ .$$

Außerdem setzen wir

$$\mathbf{0} := (0, 0, \ldots) \quad \text{und} \quad \mathbf{1} := (1, 0, 0, \ldots) \ .$$

Wegen (5) gelten für die Abbildung

$$\Phi_B : W(B) \longrightarrow B^{\mathbb{N}_0}$$

die Identitäten

$$\begin{aligned} \Phi_B(\mathbf{a} \boxplus \mathbf{b}) &= \Phi_B(\mathbf{a}) + \Phi_B(\mathbf{b}), \\ \Phi_B(\mathbf{a} \boxtimes \mathbf{b}) &= \Phi_B(\mathbf{a}) \cdot \Phi_B(\mathbf{b}) \ . \end{aligned} \tag{6}$$

Zusätzlich sieht man sofort

$$\Phi_B(\mathbf{0}) = 0 \quad \text{und} \quad \Phi_B(\mathbf{1}) = 1 \ . \tag{7}$$

Für jeden Ringhomomorphismus $\rho : B_1 \longrightarrow B_2$ kommutiert $W(\rho) := \rho^{\mathbb{N}_0} : W(B_1) \longrightarrow W(B_1)$ offensichtlich mit $\boxplus$ und $\boxtimes$ und erfüllt $W(\rho)(\mathbf{1}) = \mathbf{1}$ und das kommutative Diagramm

$$\begin{array}{ccc} W(B_1) & \xrightarrow{\Phi_{B_1}} & B_1^{\mathbb{N}_0} \\ {\scriptstyle W(\rho)}\downarrow & & \downarrow{\scriptstyle \rho^{\mathbb{N}_0}} \\ W(B_2) & \xrightarrow{\Phi_{B_2}} & B_2^{\mathbb{N}_0} \ . \end{array}$$

**Satz 5.9.** *i.* $(W(B), \boxplus, \boxtimes)$ *ist ein kommutativer Ring mit Nullelement* $\mathbf{0}$ *und Einselement* $\mathbf{1}$*; das additive Inverse zu* $(b_n)_n$ *ist* $(I_n(b_0, \ldots, b_n))_n$*.*

*ii. Die Abbildung* $\Phi_B : W(B) \longrightarrow B^{\mathbb{N}_0}$ *ist ein Ringhomomorphismus; insbesondere ist*

$$\begin{aligned} \Phi_m : W(B) &\longrightarrow B \\ (b_n)_n &\longmapsto \Phi_m(b_0, \ldots, b_m) \end{aligned}$$

*für jedes* $m \geq 0$ *ein Ringhomomorphismus.*

*iii. Für jeden Ringhomomorphismus* $\rho : B_1 \longrightarrow B_2$ *ist auch* $W(\rho) : W(B_1) \longrightarrow W(B_2)$ *ein Ringhomomorphismus.*

*Beweis.* Auf Grund der Vorüberlegungen genügt es, die Behauptung i. zu beweisen. Dazu betrachten wir den Ring $B_1 := \mathbb{Z}[\{X_b\}_{b \in B}]$ zusammen mit dem surjektiven Ringhomomorphismus $\rho : B_1 \longrightarrow B$ gegeben durch $\rho(X_b) := b$. Der Ring $B_1$ besitzt den durch $\sigma(X_b) := X_b^p$ definierten Endomorphismus $\sigma$ mit der Eigenschaft $\sigma(b) \equiv b^p \bmod pB_1$ für alle $b \in B_1$ (vgl. den Beweis von Lemma 5.6). Ferner ist $p1_{B_1}$ kein Nullteiler in $B_1$. In dieser Situation besagen Lemma 5.3.i. und Satz 5.5.ii., daß

$$\Phi_{B_1} : W(B_1) \xrightarrow{\cong} B_1'$$

eine Bijektion auf den Unterring $B_1'$ in $B_1^{\mathbb{N}_0}$ ist. Wegen (6) und (7) übertragen sich deswegen Assoziativgesetze, Distributivgesetze usw. in $B_1^{\mathbb{N}_0}$ auf die entsprechenden Gesetze für $\boxplus$ und $\boxtimes$ in $W(B_1)$. Somit ist $(W(B_1), \boxplus, \boxtimes)$ ein kommutativer Ring mit Einselement $\mathbf{1}$. Die Formel für das additive Inverse folgt analog aus (5). Da die Abbildung $W(\rho) : W(B_1) \longrightarrow W(B)$ surjektiv ist und $\boxplus, \boxtimes$ und Eins respektiert, folgen die Ringaxiome für $W(B)$ aus denen für $W(B_1)$. □

**Definition 5.10.** $(W(B), \boxplus, \boxtimes)$ *heißt der Ring der Wittvektoren mit Koeffizienten in* $B$*.*

Die $\Phi_n(b_0, \ldots, b_n) \in B$ nennt man auch die *Phantomkomponenten* des Elementes $(b_n)_n \in W(B)$.

Zusätzlich haben wir auf $W(B)$ die Abbildungen

$$\begin{aligned} F : \quad W(B) &\longrightarrow W(B) \\ (b_n)_n &\longmapsto (F_n(b_0, \ldots, b_{n+1}))_n \end{aligned}$$

und

$$V: \begin{array}{rl} W(B) & \longrightarrow W(B) \\ (b_n)_n & \longmapsto (0, b_0, b_1, \ldots) \ . \end{array}$$

Aus (5) bzw. (3) folgt die Kommutativität der Diagramme

$$(8) \qquad \begin{array}{ccc} W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}_0} \\ {\scriptstyle F}\downarrow & & \downarrow{\scriptstyle f_B} \\ W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}_0} \end{array} \qquad \text{und} \qquad \begin{array}{ccc} W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}_0} \\ {\scriptstyle V}\downarrow & & \downarrow{\scriptstyle v_B} \\ W(B) & \xrightarrow{\Phi_B} & B^{\mathbb{N}_0} \end{array} \ .$$

**Satz 5.11.** *i. $F$ ist ein Ringendomorphismus von $W(B)$;*

*ii. $V$ ist ein additiver Endomorphismus von $W(B)$;*

*iii. $F(V(\mathbf{b})) = p\mathbf{b}$ für alle $\mathbf{b} \in W(B)$;*

*iv. $V(\mathbf{a} \boldsymbol{\times} F(\mathbf{b})) = V(\mathbf{a}) \boldsymbol{\times} \mathbf{b}$ für alle $\mathbf{a}, \mathbf{b} \in W(B)$;*

*v. $F(\mathbf{b}) \equiv \mathbf{b}^p \bmod pW(B)$ für alle $\mathbf{b} \in W(B)$.*

*Beweis.* (In den Behauptungen beziehen sich Ausdrücke wie $p\mathbf{b}$ und $\mathbf{b}^p$ natürlich auf die neue Ringstruktur in $W(B)$.) Mit dem gleichen Trick wie im Beweis von Satz 5.9 führt man das auf entsprechende Identitäten für $f_B$ und $v_B$ in $B^{\mathbb{N}_0}$ zurück, die leicht nachzuprüfen sind. □

**Definition 5.12.** *$F$ bzw. $V$ heißt der Frobenius bzw. die Verschiebung auf $W(B)$.*

Für jedes $m \geq 0$ sei

$$V_m(B) := \operatorname{im}(V^m) = \{(b_n)_n \in W(B) : b_0 = \ldots = b_{m-1} = 0\} \ .$$

Offensichtlich gilt

$$W(B) = V_0(B) \supset V_1(B) \supset \ldots \quad \text{und} \ \bigcap_m V_m(B) = \{0\} \ .$$

Wegen Satz 5.11.ii. und iv. ist jedes $V_m(B)$ ein Ideal in $W(B)$.

**Definition 5.13.** *$W_m(B) := W(B)/V_m(B)$ heißt der Ring der Wittvektoren der Länge $m$ mit Koeffizienten in $B$.*

**Lemma 5.14.** *i. Für jedes $m \geq 1$ und jedes $(b_n)_n \in W(B)$ gilt*

$$(b_n)_n = (b_0, \ldots, b_{m-1}, 0, \ldots) \dotplus (0, \ldots, 0, b_m, b_{m+1}, \ldots) \ ;$$

*ii. die Abbildung*

$$\begin{aligned} B^m &\longrightarrow W_m(B) \\ (b_0, \ldots, b_{m-1}) &\longmapsto (b_0, \ldots, b_{m-1}, 0, \ldots) \dotplus V_m(B) \end{aligned}$$

*ist für jedes $m \geq 1$ eine mengentheoretische Bijektion.*

*Beweis.* i. Wieder mit Hilfe des Tricks im Beweis von Satz 5.9 genügt es zu zeigen, daß

$$\Phi_k((b_n)_n) = \Phi_k(b_0, \ldots, b_{m-1}, 0, \ldots) + \Phi_k(0, \ldots, 0, b_m, b_{m+1}, \ldots)$$

gilt für alle $k \geq 0$. Dies folgt aber sofort aus

$$\Phi_k(b_0, \ldots, b_{m-1}, 0, \ldots) = \begin{cases} \Phi_k(b_0, \ldots, b_k) & \text{für } 0 \leq k < m, \\ \sum_{i=0}^{m-1} p^i b_i^{p^{k-i}} & \text{für } m \leq k \end{cases}$$

und

$$\Phi_k(0, \ldots, 0, b_m, b_{m+1}, \ldots) = \begin{cases} 0 & \text{für } 0 \leq k < m, \\ \sum_{i=m}^{k} p^i b_i^{p^{k-i}} & \text{für } m \leq k. \end{cases}$$

ii. Die Surjektivität folgt sofort aus i. Für die Injektivität sei

$$(c_0, \ldots, c_{m-1}, 0, \ldots) \dotplus V_m(B) = (b_0, \ldots, b_{m-1}, 0, \ldots) \dotplus V_m(B) \ .$$

Dann gilt wegen i. also $(c_0, \ldots, c_{m-1}, 0, \ldots) = (b_n)_n$ mit einem geeigneten $(0, \ldots, 0, b_m, b_{m+1}, \ldots) \in V_m(B)$. Folglich ist $c_n = b_n$ für alle $0 \leq n < m$. □

**Übungsaufgabe 5.15.** *1) Folgere aus Lemma 5.14, daß*

$$\begin{aligned} W(B) &\xrightarrow{\cong} \varprojlim_m W_m(B) \\ \mathbf{b} &\longmapsto (\mathbf{b} \dotplus V_m(B))_m \end{aligned}$$

*ein Isomorphismus von Ringen ist.*
*2) Die Abbildung $\Phi_0 : W_1(B) \xrightarrow{\cong} B$ ist ein Isomorphismus von Ringen.*

**Lemma 5.16.** *Die Abbildung*

$$\begin{aligned} \tau : \quad B &\longrightarrow W(B) \\ b &\longmapsto (b, 0, \ldots) \end{aligned}$$

*ist multiplikativ.*

*Beweis.* Wir haben $P_0(X_0, Y_0) = X_0 Y_0$. Also ist

$$P_n(X_0, 0, \ldots, 0, Y_0, 0, \ldots, 0) = 0 \quad \text{für alle } n \geq 1$$

zu zeigen. Mit der Abkürzung $\tilde{P}_n(X_0, Y_0) := P_n(X_0, 0, \ldots, Y_0, 0, \ldots)$ folgt aus (5) sofort die Identität

$$\begin{aligned}(X_0Y_0)^{p^n} + \sum_{i=1}^{n} p^i \tilde{P}_i(X_0, Y_0)^{p^{n-i}} &= \Phi_n(\tilde{P}_0, \ldots, \tilde{P}_n) \\ &= \Phi_n(X_0, 0, \ldots)\Phi_n(Y_0, 0, \ldots) \\ &= X_0^{p^n} Y_0^{p^n} \ ,\end{aligned}$$

welche das Gewünschte induktiv liefert. □

**Definition 5.17.** *$\tau(b) \in W(B)$ heißt der Teichmüller-Repräsentant von $b \in B$.*

**Lemma 5.18.** *Für alle $k \geq 1$ gilt $V_1(B)^k = p^{k-1} V_1(B)$.*

*Beweis.* Mit Hilfe der entsprechenden Teilaussagen von Satz 5.11 berechnen wir

$$V(\mathbf{a}) \boldsymbol{\times} V(\mathbf{b}) \overset{iv.}{=} V(\mathbf{a} \boldsymbol{\times} FV(\mathbf{b})) \overset{iii.}{=} V(\mathbf{a} \boldsymbol{\times} p\mathbf{b}) \overset{ii.}{=} pV(\mathbf{a} \boldsymbol{\times} \mathbf{b})$$

für alle $\mathbf{a}, \mathbf{b} \in W(B)$. Daraus folgt $V_1(B)^2 = pV_1(B)$ und dann induktiv die Behauptung. □

Man sagt, der Ring $B$ habe die *Charakteristik* $p$, falls $p1_B = 0$ gilt. In diesem Falle ist der Frobenius

$$\begin{aligned} B &\longrightarrow B \\ b &\longmapsto b^p \end{aligned}$$

ein Ringendomorphismus. Ist diese Abbildung bijektiv, so heißt $B$ *perfekt*.

**Satz 5.19.** *Hat $B$ die Charakteristik $p$, so gilt:*

*i. Für $\mathbf{b} = (b_n)_n \in W(B)$ haben wir*

$$F(\mathbf{b}) = (b_n^p)_n \quad \textit{und} \quad p\mathbf{b} = VF(\mathbf{b}) = FV(\mathbf{b}) = (0, b_0^p, b_1^p, \ldots) \ ;$$

*ii. $V_m(B) \boldsymbol{\times} V_n(B) \subseteq V_{m+n}(B)$ für alle $m, n \geq 0$;*

*iii. $p^k W(B) \subseteq V_1(B)^k \subseteq p^{k-1} W(B)$ für alle $k \geq 1$;*

*iv. der Ringhomomorphismus*

$$\begin{aligned} W(B) &\xrightarrow{\cong} \varprojlim_k W(B)/p^k W(B) \\ \mathbf{b} &\longmapsto (\mathbf{b} + p^k W(B))_k \end{aligned}$$

*ist bijektiv.*

*Beweis.* i. Dies folgt aus Lemma 5.7 und Satz 5.11.iii.

ii. Aus Satz 5.11.iv. ergibt sich induktiv $V^m(\mathbf{a} \boldsymbol{\times} F^m(\mathbf{b})) = V^m(\mathbf{a}) \boldsymbol{\times} \mathbf{b}$ und damit insbesondere

$$V^m(\mathbf{a}) \boldsymbol{\times} V^n(\mathbf{b}) = V^m(\mathbf{a} \boldsymbol{\times} F^m(V^n(\mathbf{b})))$$

bzw.

$$V^n(F^m(\mathbf{b})) \boldsymbol{\times} \mathbf{a} = V^n(F^m(\mathbf{b}) \boldsymbol{\times} F^n(\mathbf{a})) \ .$$

Nach i. haben wir aber $F^m V^n = V^n F^m$. Somit können wir die zweite Gleichung in die rechte Seite der ersten einsetzen und erhalten

$$V^m(\mathbf{a}) \boldsymbol{\times} V^n(\mathbf{b}) = V^{m+n}(F^n(\mathbf{a}) \boldsymbol{\times} F^m(\mathbf{b})) \tag{9}$$

für alle $\mathbf{a}, \mathbf{b} \in W(B)$.

iii. Aus i. folgt $pW(B) = VF(W(B)) \subseteq V_1(B)$. Wegen Lemma 5.18 ergibt sich daraus sofort die Behauptung.

iv. Wegen i. gilt

$$p^k W(B) = \{(0, \ldots, 0, b_k, b_{k+1}, \ldots) \in W(B) : b_n \in B^{p^k} \text{ für alle } n \geq k\} \ .$$

Also ist $\bigcap_{k\geq 1} p^k W(B) = \{\mathbf{0}\}$, was gleichbedeutend mit der Injektivität der betrachteten Abbildung ist. Sei nun $(\mathbf{b}^{(k)} \dotplus p^k W(B))_k \in \varprojlim W(B)/p^k W(B)$. Wegen ii. und iii. gilt

$$p^k W(B) \subseteq V_k(B) \ .$$

Somit ist $(\mathbf{b}^{(k)} \dotplus V_k(B))_k \in \varprojlim W(B)/V_k(B)$. Der Übungsaufgabe 5.15.1) zu Folge existiert dann ein $\mathbf{b} \in W(B)$ mit $\mathbf{b} \dotplus V_k(B) = \mathbf{b}^{(k)} \dotplus V_k(B)$ für alle $k \in \mathbb{N}$. Für alle $j \geq k$ erhalten wir

$$\begin{aligned} \mathbf{b} \dotplus V_j(B) \dotplus p^k W(B) &= \mathbf{b}^{(j)} \dotplus V_j(B) \dotplus p^k W(B) \\ &= \mathbf{b}^{(k)} \dotplus V_j(B) \dotplus p^k W(B) \end{aligned}$$

und damit

$$\mathbf{b} \dotplus \bigcap_{j\geq k} \left[V_j(B) \dotplus p^k W(B)\right] = \mathbf{b}^{(k)} \dotplus \bigcap_{j\geq k} \left[V_j(B) \dotplus p^k W(B)\right] \ .$$

Wir zeigen jetzt aber, daß

$$\bigcap_{j\geq k} \left[V_j(B) \dotplus p^k W(B)\right] = p^k W(B)$$

gilt. Sei dazu $\mathbf{c} = (0, \ldots, 0, c_k, c_{k+1}, \ldots)$ aus dem Durchschnitt auf der linken Seite, etwa

$$\mathbf{c} \in (0, \ldots, 0, a_{j,k}, a_{j,k+1}, \ldots) \dotplus V_j(B) \text{ mit } a_{j,n} \in B^{p^k} \text{ für alle } n \geq k \ .$$

Aus Lemma 5.14 folgt dann

$$c_k = a_{j,k}, c_{k+1} = a_{j,k+1}, \ldots, c_{j-1} = a_{j,j-1}$$

und damit $c_n \in B^{p^k}$ für alle $k \leq n < j$. Da $j$ beliebig war, erhalten wir $\mathbf{c} \in p^k W(B)$ wie behauptet. Folglich ist

$$\mathbf{b} \dotplus p^k W(B) = \mathbf{b}^{(k)} \dotplus p^k W(B) \quad \text{für alle } k \geq 1 \ ,$$

was die Surjektivität der betrachteten Abbildung bedeutet. □

**Satz 5.20.** *Der Ring $B$ habe die Charakteristik $p$ und sei perfekt; dann gilt:*

*i. Für alle $\mathbf{b} = (b_n)_n \in W(B)$ und $m \geq 1$ ist*

$$\mathbf{b} \dotplus V_m(B) = \tau(b_0) \dotplus p\tau(b_1^{p^{-1}}) \dotplus \ldots \dotplus p^{m-1}\tau(b_{m-1}^{p^{-(m-1)}}) \dotplus V_m(B) \ ;$$

*ii. $V_m(B) = p^m W(B) = V_1(B)^m$ für alle $m \geq 0$.*

*Beweis.* i. Wegen Satz 5.19.i. ist

$$\tau(b_0) \dotplus \ldots \dotplus p^{m-1}\tau(b_{m-1}^{p^{-(m-1)}}) \dotplus V_m(B) = (b_0, \ldots, b_{m-1}, 0, \ldots) \dotplus V_m(B) \ ,$$

woraus die Behauptung wegen Lemma 5.14 folgt.

ii. Wegen der Perfektheit von $B$ folgt aus Satz 5.19.i., daß $F$ ein Ringautomorphismus von $W(B)$ ist. Somit gilt

$$p^m W(B) = V^m F^m(W(B)) = V^m(W(B)) = V_m(B)$$

und damit auch

$$V_1(B)^m = (pW(B))^m = p^m W(B) \ .$$

□

**Lemma 5.21.** *Sei $C$ ein Ring mit genau einem maximalen Ideal $\mathfrak{n}$, welches ein Hauptideal $\mathfrak{n} = \pi C$ ist und $\bigcap_{i\geq 1} \mathfrak{n}^i = \{0\}$ erfüllt; dann ist jedes Ideal $\neq \{0\}$ in $C$ von der Form $\pi^k C$ für ein $k \geq 0$.*

*Beweis.* Zunächst sei daran erinnert, daß jede Nichteinheit eines Ringes in einem maximalen Ideal enthalten sein muß. In unserem Falle impliziert dies $C^\times = C \setminus \mathfrak{n}$. Wegen $\bigcap_{i\geq 1} \mathfrak{n}^i = \{0\}$ existiert zu jedem $0 \neq c \in C$ genau ein $v(c) \geq 0$ mit $c \in \mathfrak{n}^{v(c)} \setminus \mathfrak{n}^{v(c)+1}$. Also gilt $c = \pi^{v(c)}u$ für ein $u \in C$. Aber $u \notin \pi C = \mathfrak{n}$; somit ist $u \in C^\times$ eine Einheit. Sei nun $J \neq \{0\}$ ein Ideal in $C$. Wähle $0 \neq c \in J$ so, daß $k := v(c)$ minimal ist. Dann gilt einerseits $J \subseteq \pi^k C$ und andererseits $\pi^k C = cC \subseteq J$. □

**Satz 5.22.** *Sei $B$ ein Körper der Charakteristik $p$; dann gilt:*

*i. $W(B)$ ist ein Integritätsbereich mit genau einem maximalen Ideal, nämlich $V_1(B)$, und $W(B)/V_1(B) \cong B$;*

*ii. der Ringhomomorphismus*

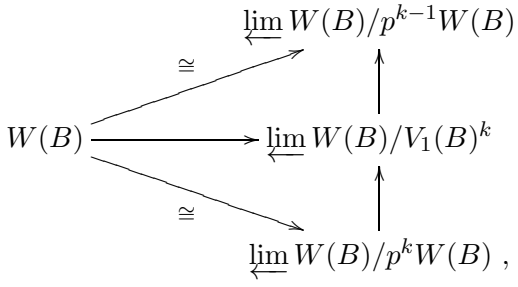
$$\begin{aligned} W(B) &\xrightarrow{\cong} \varprojlim_k W(B)/V_1(B)^k \\ \mathbf{b} &\longmapsto (\mathbf{b} \bmod V_1(B)^k)_k \end{aligned}$$

*ist bijektiv;*

*iii. ist $B$ perfekt, so ist $W(B)$ ein vollständiger diskreter Bewertungsring mit maximalem Ideal $pW(B)$ und Restklassenkörper $B$, und für jedes $\mathbf{b} = (b_n)_n \in W(B)$ gilt*

$$\mathbf{b} = \sum_{n=0}^{\infty} p^n \tau(b_n^{p^{-n}}) \ .$$

*Beweis.* ii. Auf Grund von Satz 5.19.iii. und iv. haben wir das kommutative Diagramm



in welchem die schrägen Pfeile und die Komposition der senkrechten Pfeile bijektiv und die einzelnen senkrechten Pfeile jedenfalls injektiv sind. Dann müssen aber alle Pfeile bijektiv sein.

i. Der Übungsaufgabe 5.15.2) zu Folge ist $W(B)/V_1(B) \cong B$ mittels $\Phi_0$. Also muß $V_1(B)$ ein maximales Ideal sein. Sei $\mathbf{b} \notin V_1(B)$. Zunächst finden wir ein $\mathbf{a} \in W(B)$ mit $\mathbf{a} \boxtimes \mathbf{b} = \mathbf{1} \boxplus \mathbf{c}$ mit $\mathbf{c} \in V_1(B)$.
Wegen ii. existiert

$$(\mathbf{1} \boxplus \mathbf{c})^{-1} = \sum_{i=0}^{\infty} (-1)^i \mathbf{c}^i \in W(B) \ .$$

Also ist $\mathbf{b}$ eine Einheit in $W(B)$. Folglich ist $V_1(B)$ das einzige maximale Ideal in $W(B)$. Schließlich seien $\mathbf{a}, \mathbf{b} \in W(B)$ zwei beliebige Elemente $\neq \mathbf{0}$, etwa $\mathbf{a} = (0, \ldots, 0, a_i, a_{i+1}, \ldots)$ und $\mathbf{b} = (0, \ldots, 0, b_j, b_{j+1}, \ldots)$ mit $a_i, b_j \neq 0$. Wegen Satz 5.19.i. und, da $\Phi_0$ ein Ringhomomorphismus ist, gilt

$$\begin{aligned} F^j((a_i, a_{i+1}, \ldots)) \boxtimes F^i((b_j, b_{j+1}, \ldots)) &= (a_i^{p^j}, a_{i+1}^{p^j}, \ldots) \boxtimes (b_j^{p^i}, b_{j+1}^{p^i}, \ldots) \\ &= (a_i^{p^j} b_j^{p^i}, \ldots) \ . \end{aligned}$$

Zusammen mit (9) erhalten wir

$$\begin{aligned} \mathbf{a} \boxtimes \mathbf{b} &= V^i((a_i, a_{i+1}, \ldots)) \boxtimes V^j((b_j, b_{j+1}, \ldots)) \\ &= V^{i+j}((a_i^{p^j} b_j^{p^i}, \ldots)) = (0, \ldots, 0, a_i^{p^j} b_j^{p^i}, \ldots) \ . \end{aligned}$$

Mit $a_i^{p^j} b_j^{p^i} \neq 0$ ist also auch $\mathbf{a} \boxtimes \mathbf{b} \neq \mathbf{0}$. Folglich ist $W(B)$ ein Integritätsbereich.

iii. Nach Satz 5.20.ii. gilt $V_1(B) = pW(B)$. Wegen i., Satz 5.19.iv. und Satz 5.20.i. bleibt zu zeigen, daß $p\mathbf{1} \neq \mathbf{0}$ und daß jedes Ideal in $W(B)$ ein Hauptideal ist. Nach Satz 5.19.i. gilt

$$p\mathbf{1} = (0, 1, 0, \ldots) \neq \mathbf{0} \ .$$

Aus Satz 5.19.iv. folgt $\bigcap_{k \geq 1} p^k W(B) = \{\mathbf{0}\}$, so daß wir Lemma 5.21 anwenden können. □

**Bemerkung 5.23.** *Ist $B$ ein Körper der Charakteristik $p$, so hat der Quotientenkörper von $W(B)$ die Charakteristik 0.*

*Beweis.* Sei $\ell$ eine Primzahl mit $\ell W(B) = \{0\}$. Wegen $B \cong W(B)/V_1(B)$ ist dann auch $\ell B = \{0\}$. Also muß $\ell = p$ gelten. Aber $p\mathbf{1} = (0, 1, 0, \ldots) \neq \mathbf{0}$. □

Ab dem nächsten Abschnitt benutzen wir auch für Addition und Multiplikation in $W(B)$ die üblichen Standardnotationen (und nicht länger $\boxplus$ und $\boxtimes$).

# 6 Eindeutigkeit von $W(k)$

Zunächst halten wir eine einfache Verallgemeinerung früherer Lemmata fest.

**Lemma 6.1.** *Sei $B$ ein beliebiger Ring und $\mathfrak{a} \subseteq B$ ein beliebiges Ideal mit $p1_B \in \mathfrak{a}$; dann haben wir:*

*i. Für $m, n \geq 1$ und $a, b \in B$ gilt:*

$$a \equiv b \bmod \mathfrak{a}^m \Longrightarrow a^{p^n} \equiv b^{p^n} \bmod \mathfrak{a}^{m+n} \ ;$$

*ii. für $m \geq 1$, $n \geq 0$ und $a_0, \ldots, a_n$, $b_0, \ldots, b_n \in B$ gilt:*

$$a_i \equiv b_i \bmod \mathfrak{a}^m \text{ für } 0 \leq i \leq n \\ \Longrightarrow \Phi_n(a_0, \ldots, a_n) \equiv \Phi_n(b_0, \ldots, b_n) \bmod \mathfrak{a}^{m+n} \ .$$

*Beweis.* Wegen $p1_B \in \mathfrak{a}$ übertragen sich die Beweise von Lemma 5.1 und Lemma 5.2.i. wörtlich. □

Sei nun $k$ ein perfekter Körper der Charakteristik $p > 0$. Weiter sei $A$ ein vollständiger diskreter Bewertungsring und $\alpha : A \longrightarrow k$ ein surjektiver Ringhomomorphismus. Bezeichnet $\mathfrak{m} \subseteq A$ wie immer das maximale Ideal, so induziert $\alpha$ also einen Isomorphismus $\bar{\alpha} : A/\mathfrak{m} \xrightarrow{\cong} k$.

**Satz 6.2.** *Es existiert genau eine multiplikative Abbildung $s : k \longrightarrow A$ mit $\alpha \circ s = \mathrm{id}_k$; sie erfüllt $s(0) = 0$ und $s(1) = 1$.*

*Beweis. Existenz:* Sei $x \in k$. Wegen der Perfektheit von $k$ finden wir induktiv eine Folge $(a_i)_{i \in \mathbb{N}}$ in $A$ mit $\alpha(a_1)^p = x$ und $\alpha(a_{i+1})^p = \alpha(a_i)$ für alle $i \in \mathbb{N}$. Letzteres bedeutet

$$a_{i+1}^p \equiv a_i \bmod \mathfrak{m} \quad \text{und damit} \quad a_{i+1}^{p^{i+1}} \equiv a_i^{p^i} \bmod \mathfrak{m}^{i+1} \quad \text{für alle } i \geq 1$$

nach Lemma 6.1. Folglich ist $(a_i^{p^i})_i$ eine Cauchyfolge und konvergiert gegen ein $s(x) \in A$. Wegen $\alpha(a_i^{p^i}) = x$ gilt $\alpha(s(x)) = x$. Außerdem hängt $s(x)$ nicht von der Wahl der Folge $(a_i)_i$ ab. Sei nämlich $(\tilde{a}_i)_i$ eine weitere Folge in $A$ mit $\alpha(\tilde{a}_i)^p = x$ und $\alpha(\tilde{a}_{i+1})^p = \alpha(\tilde{a}_i)$. Wegen $\alpha(a_i)^{p^i} = x = \alpha(\tilde{a}_i)^{p^i}$ ist dann $\alpha(a_i) = \alpha(\tilde{a}_i)$, also $a_i \equiv \tilde{a}_i \bmod \mathfrak{m}$. Mit Lemma 6.1 folgt $a_i^{p^i} \equiv \tilde{a}_i^{p^i} \bmod \mathfrak{m}^{i+1}$. Also besitzen die Folgen $(a_i^{p^i})_i$ und $(\tilde{a}_i^{p^i})_i$ denselben Limes. Mittels geeigneter Wahl der Folgen ergibt sich nun leicht die Multiplikativität von $s$ sowie $s(0) = 0$ und $s(1) = 1$.

*Eindeutigkeit:* Sei $\tilde{s} : k \longrightarrow A$ eine weitere multiplikative Abbildung mit $\alpha \circ \tilde{s} = \mathrm{id}_k$. Dann gilt $s(x^{p^{-i}}) \equiv \tilde{s}(x^{p^{-i}}) \bmod \mathfrak{m}$ und folglich $s(x) = s(x^{p^{-i}})^{p^i} \equiv \tilde{s}(x^{p^{-i}})^{p^i} = \tilde{s}(x) \bmod \mathfrak{m}^{i+1}$ für alle $i \geq 1$ wegen Lemma 6.1. Das impliziert $s = \tilde{s}$. □

**Beispiel:** Im Falle $A = W(k)$ und $\alpha = \Phi_0$ ist $s = \tau$ (siehe Lemma 5.16).

**Satz 6.3.** *Es existiert genau ein Ringhomomorphismus $\gamma : W(k) \longrightarrow A$ mit $\alpha \circ \gamma = \Phi_0$. Dieser ist stetig und erfüllt*

$$\gamma((x_n)_n) = \sum_{n=0}^{\infty} p^n s(x_n^{p^{-n}}) \qquad \textit{für alle } (x_n)_n \in W(k) \ .$$

*Im Falle $p1_A \neq 0$ ist $\gamma$ injektiv.*

*Beweis. Existenz:* Der Ringhomomorphismus $W(\alpha) : W(A) \longrightarrow W(k)$ ist surjektiv. Sei $(b_n)_n$ aus dem Kern von $W(\alpha)$. Dann gilt $b_n \in \mathfrak{m}$ für alle $n \geq 0$. Folglich ist

$$\begin{aligned} \Phi_m(b_0, \ldots, b_m) &= b_0^{p^m} + pb_1^{p^{m-1}} + \ldots + p^m b_m \\ &\in \mathfrak{m}^{p^m} + p\mathfrak{m}^{p^{m-1}} + \ldots + p^m\mathfrak{m} \\ &\subseteq \mathfrak{m}^{m+1} + p\mathfrak{m}^m + \ldots + p^m\mathfrak{m} \\ &\subseteq \mathfrak{m}^{m+1} \end{aligned}$$

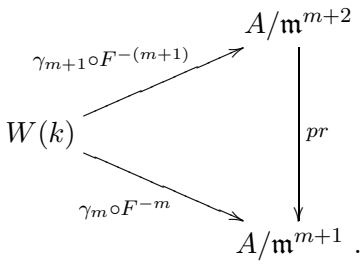
für alle $m \geq 0$. Das impliziert die Existenz von eindeutig bestimmten Ringhomomorphismen $\gamma_m : W(k) \longrightarrow A/\mathfrak{m}^{m+1}$, so daß die Diagramme

$$\begin{array}{ccc} W(A) & \xrightarrow{\Phi_m} & A \\ {\scriptstyle W(\alpha)}\downarrow & & \downarrow{\scriptstyle pr} \\ W(k) & \xrightarrow{\gamma_m} & A/\mathfrak{m}^{m+1} \end{array}$$

kommutativ sind. Wegen (8) haben wir $\Phi_m \circ F = \Phi_{m+1}$, somit $\gamma_m \circ F \circ W(\alpha) = \gamma_m \circ W(\alpha) \circ F = \gamma_{m+1} \circ W(\alpha) \bmod \mathfrak{m}^{m+1}$ und wegen der Surjektivität von $W(\alpha)$ also

$$\gamma_m \circ F \equiv \gamma_{m+1} \bmod \mathfrak{m}^{m+1} \ .$$

Nach Satz 5.19.i. ist aber $F$ auf $W(k)$ invertierbar. Deswegen impliziert die letzte Kongruenz die Kommutativität der Diagramme




Im projektiven Limes erhalten wir also den Ringhomomorphismus

$$\gamma := \varprojlim \gamma_m \circ F^{-m} : W(k) \longrightarrow \varprojlim A/\mathfrak{m}^{m+1} = A \ .$$

Wegen

$$\alpha \circ \gamma \circ W(\alpha) = \bar{\alpha} \circ \gamma_0 \circ W(\alpha) = \alpha \circ \Phi_0 = \Phi_0 \circ W(\alpha)$$

gilt $\alpha \circ \gamma = \Phi_0$.

*Eindeutigkeit und weitere Eigenschaften:* Sei $\tilde{\gamma} : W(k) \longrightarrow A$ ein beliebiger Ringhomomorphismus mit $\alpha \circ \tilde{\gamma} = \Phi_0$. Letzteres impliziert $\tilde{\gamma}(pW(k)) \subseteq \mathfrak{m}$ und dann $\tilde{\gamma}(p^i W(k)) \subseteq \mathfrak{m}^i$ für alle $i \geq 1$. Folglich ist $\tilde{\gamma}$ stetig. Aus Satz 5.22.iii. ergibt sich nun

$$\tilde{\gamma}((x_n)_n) = \sum_{n=0}^{\infty} p^n \tilde{\gamma}(\tau(x_n^{p^{-n}})) \ .$$

Die Eindeutigkeitsaussage im Satz 6.2 impliziert aber $\tilde{\gamma} \circ \tau = s$. Also erhalten wir $\tilde{\gamma} = \gamma$ und

$$\gamma((x_n)_n) = \sum_{n=0}^{\infty} p^n s(x_n^{p^{-n}}) \qquad \text{für alle } (x_n)_n \in W(k) \ .$$

Sei $p1_A \neq 0$. Aus $\gamma((x_n)_n) = 0$ folgt dann wegen Lemma 4.9, daß $s(x_n^{p^{-n}}) = 0$ und damit daß $x_n = 0$ für alle $n \geq 0$. □

**Corollar 6.4.** *Ist $pA$ das maximale Ideal in $A$, so existiert genau ein Ringisomorphismus $\gamma : W(k) \xrightarrow{\cong} A$ mit $\alpha \circ \gamma = \Phi_0$.*

*Beweis.* Der Homomorphismus $\gamma$ aus Satz 6.3 ist injektiv. Auf Grund der Annahme $\mathfrak{m} = pA$ liefern die Reihendarstellungen im Satz 6.3 wegen Lemma 4.9 sämtliche Elemente in $A$. Also ist $\gamma$ auch surjektiv. □

**Beispiel:** $W(\mathbb{F}_p) \cong \mathbb{Z}_p$.

# 7 Cohen-Unterringe

Sei $k$ ein beliebiger Körper der Charakteristik $p > 0$. Dann ist $k^{p^n} = \{x^{p^n} : x \in k\}$ für jedes $n \geq 1$ ein Teilkörper von $k$. Eine Familie $(x_i)_{i\in I}$ von Elementen in $k$ heißt eine *p-Basis* von $k$, falls die Abbildung

$$k^p[\{X_i\}_{i\in I}] \,/ < \{X_i^p - x_i^p\}_{i\in I} > \longrightarrow k$$
$$X_i \longmapsto x_i$$

bijektiv ist. Wir stellen ohne Beweis fest, daß $k$ stets eine $p$-Basis besitzt.

**Übungsaufgabe 7.1.** *Für jede p-Basis $(x_i)_{i\in I}$ von $k$ gilt:*
*1) $k = k^{p^n}(\{x_i\}_{i\in I})$ für alle $n \geq 1$.*
*2) die Elemente $\prod_{i\in I} x_i^{\mu_i}$ mit $0 \leq \mu_i < p^n$ und $\mu_i \neq 0$ für höchstens endlich viele $i \in I$ bilden eine Basis von $k$ als $k^{p^n}$-Vektorraum.*

**Definition 7.2.** *Ein Unterring $C \subseteq W(k)$ heißt Cohen-Unterring, wenn gilt:*
*– $C$ ist ein vollständiger diskreter Bewertungsring mit maximalem Ideal $pC$;*
*– $W(k) = V_1(k) + C$.*

Wegen $C/V_1(k) \cap C \xrightarrow{\cong} W(k)/V_1(k) \xrightarrow{\cong} k$ gilt also $V_1(k) \cap C = pC$, und $k$ ist auch der Restklassenkörper von $C$.

**Satz 7.3.** *Sei $(\mathbf{a}_i)_{i\in I}$ eine Familie von Elementen in $W(k)$, so daß die Familie der $x_i := \Phi_0(\mathbf{a}_i)$ eine p-Basis von $k$ ist; dann existiert genau ein Cohen-Unterring $C \subseteq W(k)$, welcher alle $\mathbf{a}_i$ enthält.*

*Beweis.* Der größeren Klarheit halber benutzen wir in diesem Beweis die Notationen $A := W(k)$, $\mathfrak{m} := V_1(k)$ und $pr := \Phi_0 : A \longrightarrow k$. Außerdem sei $S := \{\mathbf{a}_i : i \in I\} \subseteq A$. Zunächst fixieren wir ein $m \geq 1$. Für jedes $n \geq m-1$ sei

$$C_{n,m} := \text{ der von } S \cup \Phi_n(W(A)) \cup \mathfrak{m}^m \text{ erzeugte Unterring von } A\ .$$

*Behauptung 1: $C_{n,m}$ ist der kleinste Unterring von $A$ mit $C_{n,m} + \mathfrak{m} = A$, welcher $S \cup \mathfrak{m}^m$ enthält.*

Es gilt $\Phi_n(W(A)) = \{a_0^{p^n} + pa_1^{p^{n-1}} + \ldots + p^n a_n : a_0, \ldots, a_n \in A\}$, wegen $pA \subseteq \mathfrak{m}$ also $pr(\Phi_n(W(A))) = k^{p^n}$ und $pr(C_{n,m}) = k^{p^n}(pr(S))$. Die Übungsaufgabe 7.1 impliziert dann $pr(C_{n,m}) = k$, was $C_{n,m} + \mathfrak{m} = A$ bedeutet. Nun sei $A' \subseteq A$ ein Unterring mit $A' + \mathfrak{m} = A$ und $S \cup \mathfrak{m}^n \subseteq A'$. Wir haben zu zeigen, daß $\Phi_n(W(A)) \subseteq A'$ gilt. Seien also $a_0, \ldots, a_n \in A$

beliebige Elemente. Wegen $A' + \mathfrak{m} = A$ existieren $a'_0, \ldots, a'_n \in A'$ mit $a_i \equiv a'_i \bmod \mathfrak{m}$ für alle $0 \leq i \leq n$. Da $n \geq m-1$, impliziert Lemma 6.1, daß $\Phi_n(a_0, \ldots, a_n) \equiv \Phi_n(a'_0, \ldots, a'_n) \bmod \mathfrak{m}^m$. Mit $\Phi_n(a'_0, \ldots, a'_n)$ und $\mathfrak{m}^m$ liegt also auch $\Phi_n(a_0, \ldots, a_n)$ in $A'$.

Damit ist die Behauptung 1 bewiesen, und wir sehen insbesondere, daß der Unterring $C_m := C_{n,m}$ unabhängig von der Wahl von $n$ ist.

*Behauptung 2:* $C_m \cap \mathfrak{m} = p\,C_m + \mathfrak{m}^m$.

Aus $pA \subseteq \mathfrak{m}$ folgt sofort $p\,C_m + \mathfrak{m}^m \subseteq C_m \cap \mathfrak{m}$. Für die umgekehrte Inklusion bezeichne $\Lambda(m)$ die Menge aller Tupel $\mu = (\mu_i)_{i \in I}$ von ganzen Zahlen $0 \leq \mu_i < p^m$ mit $\mu_i \neq 0$ für höchstens endlich viele $i \in I$. Für $\mu \in \Lambda(m)$ setze

$$Z_\mu := \prod_{i \in I} \mathbf{a}_i^{\mu_i} \ .$$

Aus $S^{p^m} = \{\Phi_m(\mathbf{a}_i, 0, \ldots) : i \in I\} \subseteq \Phi_m(W(A))$ folgt, daß $C_m = C_{m,m}$ als Modul über dem Unterring $\Phi_m(W(A)) + \mathfrak{m}^m$ von den $Z_\mu$ erzeugt wird. Wegen $\Phi_m(a_0, \ldots, a_m) = a_0^{p^m} + p\Phi_{m-1}(a_1, \ldots, a_m)$ gilt

$$\Phi_m(W(A)) \subseteq A^{p^m} + pC_{m-1,m} = A^{p^m} + pC_m \ .$$

Jedes $c \in C_m$ läßt sich also schreiben als

$$c = \sum_{\mu \in \Lambda(m)} c_\mu^{p^m} Z_\mu + pc' + c'' \qquad \text{mit } c_\mu \in A, c' \in C_m, c'' \in \mathfrak{m}^m \ .$$

Gelte nun $c \in C_m \cap \mathfrak{m}$. Dann ist

$$0 = pr(c) = \sum_{\mu \in \Lambda(m)} pr(c_\mu)^{p^m} pr(Z_\mu) \ .$$

Nach Übungsaufgabe 7.1 bilden die $pr(Z_\mu)$ aber eine $k^{p^m}$-Basis von $k$. Also muß $pr(c_\mu) = 0$, d. h. $c_\mu \in \mathfrak{m}$ und damit $c_\mu^{p^m} \in \mathfrak{m}^m$ gelten. Folglich ist $c \in pC_m + \mathfrak{m}^m$.

Damit ist Behauptung 2 bewiesen. Aus der Minimalitätseigenschaft der $C_m$ folgt sofort

$$C_m = C_{m+1} + \mathfrak{m}^m \quad \text{für alle } m \geq 1 \ . \tag{10}$$

Wir definieren nun

$$C := \bigcap_{m \geq 1} C_m \ .$$

Offensichtlich ist $S$ in diesem Unterring $C$ von $A$ enthalten. In dem projektiven System von Ringen $(A/\mathfrak{m}^m)_m$ enthalten ist das projektive System

von Unterringen $(C_m/\mathfrak{m}^m)_m$. Auf Grund des Satzes 5.22.ii. sind also in dem kommutativen Diagramm

$$\begin{array}{ccc} A & \xrightarrow{\cong} & \varprojlim A/\mathfrak{m}^m \\ \subseteq\uparrow & & \uparrow\subseteq \\ C & \xrightarrow{\cong} & \varprojlim C_m/\mathfrak{m}^m \end{array}$$

beide horizontale Abbildungen Isomorphismen. Wegen (10) sind alle Übergangsabbildungen $C_{m+1}/\mathfrak{m}^{m+1} \longrightarrow C_m/\mathfrak{m}^m$ und damit auch alle Projektionsabbildungen $C \longrightarrow C_m/\mathfrak{m}^m$ surjektiv. Insbesondere ist

$$C/C \cap \mathfrak{m} \xrightarrow{\cong} C_1/\mathfrak{m} = A/\mathfrak{m} \xrightarrow{\cong} k$$

ein Isomorphismus und somit $C \cap \mathfrak{m}$ ein maximales Ideal in $C$. Genauso wie im Beweis von Satz 5.22.i. ergibt sich (mit Hilfe der geometrischen Reihe), daß alle Elemente in $C \setminus C \cap \mathfrak{m}$ Einheiten in $C$ sind, also daß $C \cap \mathfrak{m}$ das einzige maximale Ideal in $C$ ist. Aus Behauptung 2 folgt

$$\begin{aligned} C \cap \mathfrak{m} &= \bigcap_{m\geq 1} C_m \cap \mathfrak{m} = \bigcap_{m\geq 1} [p\, C_m + \mathfrak{m}^m] \\ &= \bigcap_{m\geq 1} \bigcap_{j\geq m} [p\, C_m + \mathfrak{m}^j] \ . \end{aligned}$$

Aus dem Beweis von Satz 5.19 wissen wir

$$\bigcap_{j\geq m} [p\, C_m + \mathfrak{m}^j] \subseteq \bigcap_{j\geq m} [p\, W(k) + V_j(k)] = pW(k) \ .$$

Sei also $p\,\mathbf{c} \in \bigcap_{j\geq m}[p\, C_m + \mathfrak{m}^j]$, etwa $p\,\mathbf{c} \in p\,\mathbf{c}^{(j)} + \mathfrak{m}^j$ mit $\mathbf{c}^{(j)} \in C_m$. Wegen Satz 5.19.iii. haben wir dann $p(\mathbf{c} - \mathbf{c}^{(m+2)}) \in \mathfrak{m}^{m+2} \subseteq p^{m+1}W(k)$. Da $W(k)$ nach Satz 5.22.i. ein Integritätsbereich ist, folgt $\mathbf{c} - \mathbf{c}^{(m+2)} \in p^m W(k) \subseteq \mathfrak{m}^m$. Also ist $\mathbf{c} \in C_m + \mathfrak{m}^m = C_m$. Wir erhalten

$$\bigcap_{j\geq m} [p\, C_m + \mathfrak{m}^j] = p\, C_m$$

und

$$C \cap \mathfrak{m} = \bigcap_{m\geq 1} p\, C_m = p\big(\bigcap_{m\geq 1} C_m\big) = p\, C \ ,$$

für die mittlere Identität wieder benutzend, daß $A$ ein Integritätsbereich ist. Mit $A$ ist natürlich auch $C$ ein Integritätsbereich mit $p\, 1_C = p\, \mathbf{1} \neq 0$. Ferner

gilt $\bigcap_{m\geq 1} p^m C \subseteq \bigcap_{m\geq 1} \mathfrak{m}^m = \{0\}$ wegen Satz 5.22.ii. Also folgt aus Lemma 5.21, daß $C$ ein diskreter Bewertungsring (mit maximalem Ideal $p\,C$ und Restklassenkörper $k$) ist.

Wir haben

$$C \xrightarrow{\cong} \varprojlim C/C \cap \mathfrak{m}^m \xrightarrow{\cong} \varprojlim C_m/\mathfrak{m}^m \ .$$

Da die Ideale $\neq \{0\}$ in $C$ gerade die $p^j C$ sind, existiert zu jedem $m \geq 1$ ein $j(m) \geq 1$ mit $C \cap \mathfrak{m}^m = p^{j(m)}C$. Wegen $\bigcap_m C \cap \mathfrak{m}^m = \{0\}$ geht $j(m)$ mit $m$ gegen unemdlich. Also ist

$$C \xrightarrow{\cong} \varprojlim_m C/p^{j(m)}C \xrightarrow{\cong} \varprojlim_j C/p^j C$$

und $C$ folglich vollständig.

Für die Eindeutigkeit sei $C' \subseteq A$ ein weiterer Cohen-Unterring mit $S \subseteq C'$. Wegen $C' + \mathfrak{m} = A$ ist $C' \cap \mathfrak{m} = p\,C'$ das maximale Ideal in $C'$. Also existiert wiederum zu jedem $m \geq 1$ ein $j(m) \geq m$, so daß $C' \cap \mathfrak{m}^m = p^{j(m)}C'$. Andererseits impliziert die Behauptung 1, daß $C' + \mathfrak{m}^m \supseteq C_m$ gilt für alle $m \geq 1$. Aus dem kommutativen Diagramm

$$\begin{array}{ccccc}
C' & \xrightarrow{\cong} & \varprojlim C'/p^{j(m)}C' & \xrightarrow{=} & \varprojlim C'/C' \cap \mathfrak{m}^m \\
 & & & & \downarrow \cong \\
\uparrow \subseteq & & & & \varprojlim C' + \mathfrak{m}^m/\mathfrak{m}^m \\
 & & & & \uparrow \subseteq \\
C & & \xrightarrow{\qquad\cong\qquad} & & \varprojlim C_m/\mathfrak{m}^m
\end{array}$$

wird dann die Inklusion $C \subseteq C'$ ersichtlich. Aber $p\,\mathbf{1}$ ist ein Primelement sowohl in $C$ wie in $C'$. Außerdem ist insbesondere der senkrechte Pfeil in dem kommutativen Diagramm

$$\begin{array}{ccc}
C'/p\,C' & & \\
\uparrow \cong & \searrow \cong & \\
 & & A/\mathfrak{m} \\
C/p\,C & \nearrow \cong &
\end{array}$$

bijektiv. Deswegen folgt die Gleichheit $C = C'$ aus Lemma 4.9. □

# 8 Das Theorem von Dieudonné-Manin

Sei $A$ ein diskreter Bewertungsring mit maximalem Ideal $\mathfrak{m} = \pi A$ und Quotientenkörper $K$. Wir fixieren einen Ringautomorphismus $\sigma$ von $A$ und bezeichnen seine (multiplikative) Fortsetzung zu einem Körperautomorphismus von $K$ ebenfalls mit $\sigma$.

**Beispiel:** $A := W(k)$ für ein perfekten Körper $k$ der Charakteristik $p > 0$ und $\sigma := F$ (siehe Satz 5.19.i.).

**Definition 8.1.** *Sei $a \in \mathbb{Z}$. Ein $\sigma^a$-Isokristall ist ein Paar $(V, f)$ bestehend aus einem endlich-dimensionalen $K$-Vektorraum $V \neq \{0\}$ und einer bijektiven $\sigma^a$-linearen Abbildung $f : V \longrightarrow V$. Die Zahl*

$$h(V, f) := \dim_K V$$

*heißt die Höhe von $(V, f)$.*

Für $a = 1$ sprechen wir im Folgenden einfach von einem Isokristall. Sei also $(V, f)$ ein Isokristall. Ein *Gitter* $M$ in $V$ ist ein $A$-Untermodul $M \subseteq V$ mit der Eigenschaft, daß eine $K$-Basis $v_1, \ldots, v_h$ von $V$ existiert mit $M = Av_1 + \ldots + Av_h$. Insbesondere ist also $M$ ein freier $A$-Modul vom Rang $h$.

**Lemma 8.2.** *Für zwei Gitter $M$ und $M'$ in $V$ gilt:*

*i. Zu jedem Vektor $v \in V$ existiert ein $n \geq 0$ mit $\pi^n v \in M$;*

*ii. es existiert ein $n \geq 0$ mit $\pi^n M' \subseteq M$;*

*iii. $M \cap M'$ ist ein Gitter in $V$;*

*iv. $f(M)$ ist ein Gitter in $V$.*

*Beweis.* i. Dies gilt offensichtlich.

ii. Sei $v'_1, \ldots, v'_h$ eine $K$-Basis von $V$ mit $M' = \sum_{i=1}^h Av'_i$. Nach i. finden wir ein $n \geq 0$ mit $\pi^n v'_i \in M$ für alle $1 \leq i \leq h$. Dann ist $\pi^n M' \subseteq M$.

iii. Auf Grund des Elementarteilersatzes existiert eine $K$-Basis $v'_1, \ldots, v'_h$ von $V$ und Elemente $a_1, \ldots, a_h \in A$, so daß $M' = \sum_{i=1}^h Av'_i$ und $M \cap M' = \sum_{i=1}^h Aa_i v'_i$. Mit $n \geq 0$ wie in ii. gilt aber

$$\pi^n M' = \sum_{i=1}^h A\pi^n v'_i \subseteq M \cap M' = \sum_{i=1}^h Aa_i v'_i \ .$$

Folglich ist $a_i \neq 0$ für alle $1 \leq i \leq h$. Somit ist $a_1 v'_1, \ldots, a_h v'_h$ eine $K$-Basis von $V$, welche $M \cap M'$ als Gitter ausweist.

iv. Sei $M = Av_1 + \ldots + Av_h$. Dann ist $f(M) = \sigma^a(A)f(v_1) + \ldots + \sigma^a(A)f(v_h) = Af(v_1) + \ldots + Af(v_h)$. Nach Lemma 1.6 ist $f(v_1), \ldots, f(v_h)$ ebenfalls eine $K$-Basis von $V$. □

Da $\pi A$ das einzige maximale Ideal von $A$ ist, ist $A/\pi A$ bis auf Isomorphie der einzige einfache $A$-Modul. Offensichtlich ist $A/\pi^n A$ für jedes $n \geq 0$ ein $A$-Modul der Länge $n$. Für jedes Gitter $M$ in $V$ ist also $M/\pi^n M \cong \oplus_{i=1}^{h} A/\pi^n A$ ein $A$-Modul der Länge $hn$. Wegen Lemma 8.2 ist für je zwei Gitter $M$ und $M'$ in $V$ der Quotient $M/M \cap M'$ jedenfalls ein $A$-Modul endlicher Länge. Wir setzen

$$[M : M'] := \text{ Länge}_A M/M \cap M' - \text{ Länge}_A M'/M \cap M' \ .$$

**Übungsaufgabe 8.3.** *Für drei Gitter $M, M'$ und $M''$ in $V$ gilt*

$$[M : M''] = [M : M'] + [M' : M''] \ .$$

**Lemma 8.4.** *Die Zahl $[M : f(M)]$ ist unabhängig von der Wahl des Gitters $M$ in $V$.*

*Beweis.* Sei $M'$ ein weiteres Gitter in $V$. Dann gilt

$$[M' : f(M')] = [M' : M] + [M : f(M)] + [f(M) : f(M')] \ .$$

Aber $[f(M) : f(M')] = [M : M'] = -[M' : M]$. □

**Definition 8.5.** *Die Zahl $d(V, f) := [M : f(M)]$ (für ein beliebiges Gitter $M$ in $V$) heißt die Dimension von $(V, f)$.*

Im Folgenden kürzen wir ab $h := h(V, f)$ und $d := d(V, f)$. Für ein Gitter $M$ in $V$ setzen wir

$$\operatorname{ord}_M f := \max \{n \in \mathbb{Z} : f(M) \subseteq \pi^n M\}$$

(beachte Lemma 8.2).

**Lemma 8.6.** *Sei $M$ ein beliebiges Gitter in $V$; dann gilt:*

*i. Für jedes $m \in \mathbb{N}$ ist $\operatorname{ord}_M f \leq \frac{1}{m} \operatorname{ord}_M f^m \leq \frac{d}{h}$;*

*ii. existiert ein $m \in \mathbb{N}$ mit $\operatorname{ord}_M f \neq \frac{1}{m} \operatorname{ord}_M f^m$, so ist*

$$\operatorname{ord}_M f + \frac{1}{h} \leq \frac{1}{h} \operatorname{ord}_M f^h \ .$$

*Beweis.* i. Aus $f(M) \subseteq \pi^n M$ folgt induktiv

$$\begin{aligned} f^m(M) &\subseteq f^{m-1}(\pi^n M) = f^{m-1}(\sigma^{-(m-1)}(\pi)^n M) = \pi^n f^{m-1}(M) \\ &\subseteq \ldots \subseteq \pi^{mn} M \end{aligned}$$

und damit $m \cdot \operatorname{ord}_M f \leq \operatorname{ord}_M f^m$. Andererseits sei $f^m(M) \subseteq \pi^n M$. Dann gilt

$$\begin{aligned} md = m[M : f(M)] &= [M : f^m(M)] \\ &= [M : \pi^n M] + [\pi^n M : f^m(M)] \\ &\geq [M : \pi^n M] = nh \end{aligned}$$

und somit $\operatorname{ord}_M f^m \leq m \cdot \frac{d}{h}$.

ii. Sei $n := \operatorname{ord}_M f$ und $f^m(M) \subseteq \pi^{mn+1} M$ für ein $m \in \mathbb{N}$. Für $i \geq 0$ setze $M_i := \{v \in M : f^i(v) \in \pi^{in+1} M\}$. Aus $f(M) \subseteq \pi^n M$ folgt

$$\pi M = M_0 \subseteq M_1 \subseteq \ldots \subseteq M_m = M \ .$$

Auf Grund des Elementarteilersatzes sind alle $M_i$ Gitter in $V$. Wegen $h = [M : \pi M] = [M_1 : M_0] + [M_2 : M_1] + \ldots + [M : M_{m-1}]$ kann es in dieser Gitterfolge höchstens $h$ echt aufsteigende Schritte geben.

*Zwischenbehauptung: Aus $M_i = M_{i+1}$ folgt $M_i = M_j$ für alle $j > i$.*

Sei $v \in M_j$, also $v \in M$ mit $f^j(v) \in \pi^{jn+1} M$. Schreibe

$$f^{j-(i+1)}(v) = \pi^{(j-(i+1))n} v' \quad \text{mit } v' \in M \ .$$

Dann gilt $\pi^{(j-(i+1))n} f^{i+1}(v') \in A^\times f^j(v) \subseteq \pi^{jn+1} M$ und somit $f^{i+1}(v') \in \pi^{(i+1)n+1} M$. Nach Voraussetzung erhalten wir $f^i(v') \in \pi^{in+1} M$ und folglich $f^{j-1}(v) = f^i(f^{j-(i+1)}(v)) = \sigma^{-(j-(i+1))n}(\pi) f^i(v') \in \pi^{(j-1)n+1} M$, d. h. $v \in M_{j-1}$.

Damit ist die Zwischenbehauptung gezeigt, und wir sehen, daß $M_h = M$, also $f^h(M) \subseteq \pi^{hn+1} M$ bzw. $\operatorname{ord}_M f^h \geq h \cdot \operatorname{ord}_M f + 1$ gelten muß. □

**Definition 8.7.** *Die Zahl*

$$\operatorname{Newton}(V, f) := \sup \left\{ \tfrac{1}{m} \operatorname{ord}_M f^m : m \in \mathbb{N}, M \text{ Gitter in } V \right\}$$

*heißt der erste Anstieg von $(V, f)$.*

Nach Lemma 8.6.i. gilt

$$\operatorname{Newton}(V, f) \leq \frac{d}{h} \ .$$

**Lemma 8.8.** *Für ein beliebiges Gitter $M$ in $V$ gilt*

$$\mathrm{Newton}(V,f) = \lim_{m\to\infty} \tfrac{1}{m} \operatorname{ord}_M(f^m) \ .$$

*Beweis.* Sei $M'$ ein weiteres Gitter in $V$. Nach Lemma 8.2.ii. existieren $n, n' \geq 0$ mit $\pi^n M \subseteq M'$ und $\pi^{n'} M' \subseteq M$. Dann gilt

$$f(M) \subseteq \pi^{-n} f(M') \subseteq \pi^{\operatorname{ord}_{M'} f - n} M' \subseteq \pi^{\operatorname{ord}_{M'} f - n - n'} M$$

und damit $\operatorname{ord}_M f \geq \operatorname{ord}_{M'} f - n - n'$. Für jedes $i \in \mathbb{N}$ erhalten wir dann

$$\begin{aligned}
\sup_m \tfrac{1}{m} \operatorname{ord}_M f^m &\geq \sup_j \tfrac{1}{ij} \operatorname{ord}_M f^{ij} \\
&\geq \sup_j \tfrac{1}{ij} (\operatorname{ord}_{M'} f^{ij} - n - n') \\
&\geq \sup_j \left[ \tfrac{1}{i} \operatorname{ord}_{M'} f^i - \tfrac{n+n'}{ij} \right] \\
&= \tfrac{1}{i} \operatorname{ord}_{M'} f^i \ ,
\end{aligned}$$

wobei in der vorletzten Zeile Lemma 8.6.i. benutzt wurde. Somit ist

$$\lambda := \mathrm{Newton}(V,f) = \sup_m \tfrac{1}{m} \operatorname{ord}_M f^m$$

gezeigt. Nun sei $\varepsilon > 0$. Wir finden ein $m_0 \in \mathbb{N}$ mit

$$\operatorname{ord}_M f^{m_0} > m_0 \left( \lambda - \frac{\varepsilon}{2} \right) \ .$$

Für beliebige ganze Zahlen $r \geq 1$ und $0 \leq s < m_0$ gilt dann

$$\operatorname{ord}_M f^{m_0 r + s} > m_0 r \left( \lambda - \frac{\varepsilon}{2} \right) + s \cdot \operatorname{ord}_M f \ .$$

Wir wählen nun $r_0 \in \mathbb{N}$ derart, daß

$$\operatorname{ord}_M f - \left( \lambda - \frac{\varepsilon}{2} \right) > -\frac{\varepsilon}{2}(r_0 + 1) \ .$$

Für alle ganzen $r \geq r_0$ und $0 \leq s < m_0$ gilt dann

$$s \left( \operatorname{ord}_M f - \left( \lambda - \frac{\varepsilon}{2} \right) \right) / m_0 r + s > -\frac{\varepsilon}{2} \ .$$

Jedes $m > m_0 r_0$ schreibt sich als $m = m_0 r + s$ mit ganzen $r \geq r_0$ und $0 \leq s < m_0$. Also

$$\begin{aligned}
\lambda \geq \frac{1}{m} \operatorname{ord}_M f^m &> \frac{m_0 r}{m_0 r + s} \left( \lambda - \frac{\varepsilon}{2} \right) + \frac{s}{m_0 r + s} \operatorname{ord}_M f \\
&> \frac{m_0 r}{m_0 r + s} \left( \lambda - \frac{\varepsilon}{2} \right) + \frac{s}{m_0 r + s} \left( \lambda - \frac{\varepsilon}{2} \right) - \frac{\varepsilon}{2} \\
&= \left( \lambda - \frac{\varepsilon}{2} \right) - \frac{\varepsilon}{2} = \lambda - \varepsilon \ .
\end{aligned}$$

Daraus folgt $\lambda = \lim_{m\to\infty} \frac{1}{m} \operatorname{ord}_M f^m$. □

**Übungsaufgabe 8.9.** *Sei $\sigma = \mathrm{id}$, also $f$ $K$-linear. Der Einfachheit halber sei angenommen, daß sämtliche Nullstellen $a_1, \ldots, a_r$ des charakteristischen Polynoms von $f$ in $K$ liegen. Dann gilt*

$$\mathrm{Newton}(V, f) = \min(v(a_1), \ldots, v(a_r)) \ ,$$

*wobei $v$ die diskrete Bewertung von $A$ bezeichnet.*

**Lemma 8.10.** *Für beliebige $s \in \mathbb{Z}$ und $r \in \mathbb{N}$ gilt*

$$\mathrm{Newton}(V, \pi^s f^r) = r\,\mathrm{Newton}(V, f) + s \ .$$

*Beweis.* Die Identität

$$\mathrm{Newton}(V, \pi^s f) = \mathrm{Newton}(V, f) + s$$

ist offensichtlich. Außerdem haben wir

$$\mathrm{Newton}(V, f^r) = \lim_{m\to\infty} \tfrac{1}{m} \mathrm{ord}_M\, f^{rm} = \lim_{m\to\infty} \tfrac{r}{m} \mathrm{ord}_M\, f^m = r\,\mathrm{Newton}(V, f) \ .$$

□

**Lemma 8.11.** *Existiert ein Gitter $M$ in $V$ mit $f^{h+1}(M) \subseteq \pi^{-1}M$, so existiert auch ein Gitter $M''$ in $V$ mit $f(M'') \subseteq M''$.*

*Beweis.* Auf Grund des Elementarteilersatzes ist $M' := M + f(M) + \ldots + f^h(M)$ ein Gitter in $V$. Es gilt

$$\sum_{j=0}^{h+1} f^j(M') = \sum_{j=0}^{2h+1} f^j(M) = M' + \sum_{j=0}^{h} f^j(f^{h+1}(M)) \subseteq \pi^{-1}M' \ .$$

Betrachte die aufsteigende Gitterfolge

$$M' \subseteq M' + f(M') \subseteq \ldots \subseteq \sum_{j=0}^{h+1} f^j(M') \subseteq \pi^{-1}M' \ .$$

Wegen $\dim_{A/\pi A} \pi^{-1}M'/M' = h$ muß ein $0 \le i \le h$ existieren mit

$$M'' := \sum_{j=0}^{i} f^j(M') = \sum_{j=0}^{i+1} f^j(M') \ .$$

Offensichtlich gilt $f(M'') \subseteq M''$. □

**Satz 8.12.** *Es existieren ein Gitter $M$ in $V$ und ganze Zahlen $1 \leq r \leq h$ und $s \leq d$, so daß*

$$\operatorname{ord}_M f^r = s \qquad \textit{und} \qquad \operatorname{Newton}(V, f) = \frac{s}{r} \ .$$

*Beweis.* Setze $\lambda := \operatorname{Newton}(V, f)$.

*1. Schritt:* Wir zeigen die Existenz von ganzen Zahlen $1 \leq r \leq h$ und $s$ mit

$$\left|\lambda - \frac{s}{r}\right| \leq \frac{1}{r(h+1)} \ .$$

Zu jedem $r \in \mathbb{Z}$ findet man ein $t_r \in \mathbb{R}$ mit

$$s_r := r\lambda - t_r \in \mathbb{Z} \qquad \text{und} \qquad -\frac{1}{h+1} \leq t_r < 1 - \frac{1}{h+1} \ .$$

Wir zeigen, daß ein $1 \leq r \leq h$ existiert mit $t_r \leq \frac{1}{h+1}$. Ein solches $r$ zusammen mit $s := s_r$ leistet das Gewünschte. Wir nehmen an, daß $t_r > \frac{1}{h+1}$ für alle $1 \leq r \leq h$. Dann finden wir $1 \leq r_1 < r_2 \leq h$ mit $|t_{r_1} - t_{r_2}| \leq \frac{1}{h+1}$. Aber $1 \leq r_2 - r_1 \leq h$ und

$$(r_2 - r_1)\lambda - (t_{r_2} - t_{r_1}) = s_{r_2} - s_{r_1} \in \mathbb{Z} \ ,$$

was ein Widerspruch ist.

*2. Schritt:* Wir zeigen die Existenz eines Gitter $M$ in $V$ mit $f^r(M) \subseteq \pi^s M$. Setze

$$f' := \pi^{-s} f^r \qquad \text{und} \qquad f'' := \pi^{1+(h+1)} f'^{(h+1)^2} \ .$$

Wegen Lemma 8.10 gilt

$$|\operatorname{Newton}(V, f')| = |r\lambda - s| \leq \frac{1}{h+1}, \text{ also } \lambda' := \operatorname{Newton}(V, f') \geq -\frac{1}{h+1} \ ,$$

und

$$\operatorname{Newton}(V, f'') = (h+1)^2\lambda' + 1 + (h+1) \geq 1 \ .$$

Also finden wir ein Gitter $M_1$ in $V$ und ein $m \in \mathbb{N}$ mit $f''^m(M_1) \subseteq M_1$. Für $M_2 := M_1 + f''(M_1) + \ldots + f''^{m-1}(M_1)$ gilt dann $f''(M_2) \subseteq M_2$ und folglich $(\pi f'^{h+1})^{h+1}(M_2) \subseteq \pi^{-1} M_2$. Eine zweimalige Anwendung von Lemma 8.11 liefert zuerst ein Gitter $M'$ in $V$ mit $(\pi f'^{h+1})(M') \subseteq M'$ bzw. $f'^{h+1}(M') \subseteq \pi^{-1} M'$ und dann ein Gitter $M$ in $V$ mit $f'(M) \subseteq M$ bzw. $f^r(M) \subseteq \pi^s M$.

*3. Schritt:* Wegen $|\lambda'| \leq \frac{1}{h+1}$ haben wir nun

$$\operatorname{ord}_M f' \geq 0 > \lambda' - \frac{1}{h} \geq \frac{1}{h} \operatorname{ord}_M f'^h - \frac{1}{h} \ .$$

Aus Lemma 8.6.ii. folgt deswegen $\operatorname{ord}_M f' = \frac{1}{m} \operatorname{ord}_M f'^m$ für alle $m \geq 1$. Also gilt $\lambda' = \operatorname{ord}_M f' \in \mathbb{Z}$, damit $\lambda' = 0$, $\lambda = \frac{s}{r}$ und $\operatorname{ord}_M f^r = s + \operatorname{ord}_M f' = s$. Wegen $\frac{s}{r} = \lambda \leq \frac{d}{h}$ ergibt sich schließlich $s \leq \frac{dr}{h} \leq d$. □

Der gleiche Trick wie im 2. Schritt des vorstehenden Beweises liefert das folgende allgemeine Kriterium.

**Lemma 8.13.** *Seien $r \in \mathbb{N}$ und $s \in \mathbb{Z}$ mit $\operatorname{Newton}(V, f) \geq \frac{s}{r}$; dann existiert ein Gitter $M$ in $V$ mit $f^r(M) \subseteq \pi^s M$.*

*Beweis.* Setze $f' := \pi^{1-s(h+1)} f^{r(h+1)}$. Wegen Lemma 8.10 gilt dann

$$\operatorname{Newton}(V, f') = r(h+1) \operatorname{Newton}(V, f) + 1 - s(h+1) \geq 1 \ .$$

Also existiert ein Gitter $M_1$ in $V$ und ein $m \in \mathbb{N}$ mit $f'^m(M_1) \subseteq M_1$. Für $M_2 := M_1 + f'(M_1) + \ldots + f'^{m-1}(M_1)$ gilt dann $f'(M_2) \subseteq M_2$ und folglich $(\pi^{-s} f^r)^{h+1}(M_2) \subseteq \pi^{-1} M_2$. Nach Lemma 8.11 existiert schließlich ein Gitter $M$ in $V$ mit $\pi^{-s} f^r(M) \subseteq M$ bzw. $f^r(M) \subseteq \pi^s M$. □

**Definition 8.14.** *Das Isokristall $(V, f)$ heißt isoklin, wenn gilt*

$$\operatorname{Newton}(V, f) = \frac{d(V, f)}{h(V, f)} \ .$$

**Lemma 8.15.** *Äquivalent sind:*

*i. $(V, f)$ ist isoklin;*

*ii. es existiert ein Gitter $M$ in $V$ mit $f^h(M) = \pi^d M$;*

*iii. es existiert ein Gitter $M$ in $V$ und Zahlen $r \in \mathbb{N}$ und $s \in \mathbb{Z}$ mit*

$$f^r(M) = \pi^s M \ .$$

*Für jedes Paar $(r, s)$ wie in iii. gilt $\operatorname{Newton}(V, f) = \frac{s}{r}$.*

*Beweis.* i. $\Longrightarrow$ ii. Nach Lemma 8.13 finden wir ein Gitter $M$ in $V$ mit $f^h(M) \subseteq \pi^d M$. Dann gilt

$$[\pi^d M : f^h(M)] = [M : f^h(M)] - [M : \pi^d M] = h[M : f(M)] - dh = 0 \ ,$$

d. h. $f^h(M) = \pi^d M$.

ii. $\Longrightarrow$ iii. Diese Implikation ist trivial.

iii. $\Longrightarrow$ i. Aus

$$\begin{aligned} 0 &= [\pi^s M : f^r(M)] = [M : f^r(M)] - [M : \pi^s M] \\ &= r[M : f(M)] - hs = rd - hs \end{aligned}$$

folgt

$$\frac{d}{h} = \frac{s}{r} = \frac{1}{r} \operatorname{ord}_M f^r \leq \operatorname{Newton}(V, f) \leq \frac{d}{h}$$

und damit $\operatorname{Newton}(V, f) = \frac{d}{h} = \frac{s}{r}$. □

Zu $r \in \mathbb{N}$ und $s \in \mathbb{Z}$ ist das *Standardisokristall* $V_{s,r} = (K^r, f_{s,r})$ definiert durch

$$f_{s,r}(e_i) := \begin{cases} e_{i+1} & \text{für } 1 \leq i < r \ , \\ \pi^s e_1 & \text{für } i = r \ . \end{cases}$$

Für das Gitter $A^r = \sum_{i=1}^r Ae_i$ gilt $f_{s,r}(A^r) = A\pi^s e_1 + \sum_{i=2}^r Ae_i$. Also

$$h(V_{s,r}) = r, \ d(V_{s,r}) = s \quad \text{und } f_{s,r}^r(A^r) = \pi^s A^r \ .$$

Somit ist $V_{s,r}$ isoklin mit $\operatorname{Newton}(V_{s,r}) = \frac{s}{r}$.

Ein Homomorphismus $\alpha : (V, f) \longrightarrow (V', f')$ von $\sigma^a$-Isokristallen ist eine $K$-lineare Abbildung $\alpha : V \longrightarrow V'$ mit $f' \circ \alpha = \alpha \circ f$.

**Lemma 8.16.** *i. Sei* $0 \to (V_1, f_1) \xrightarrow{\alpha} (V, f) \xrightarrow{\beta} (V_2, f_2) \to 0$ *eine kurze exakte Sequenz von Isokristallen; dann gilt*

$$\operatorname{Newton}(V, f) \leq \min(\operatorname{Newton}(V_1, f_1), \operatorname{Newton}(V_2, f_2)) \ ;$$

*ist* $(V, f)$ *isoklin, so auch* $(V_1, f_1)$ *und* $(V_2, f_2)$ *mit*

$$\operatorname{Newton}(V_1, f_1) = \operatorname{Newton}(V_2, f_2) = \operatorname{Newton}(V, f) \ .$$

*ii. Sei* $(V, f)$ *isoklin, und sei* $(V', f')$ *ein weiteres Isokristall mit*

$$\operatorname{Newton}(V, f) < \operatorname{Newton}(V', f') \ ;$$

*dann gibt es keine Homomorphismen* $\neq 0$ *zwischen* $(V, f)$ *und* $(V', f')$ *(in beiden Richtungen).*

*Beweis.* i. Nach Satz 8.12 existiert ein Gitter $M$ in $V$ und Zahlen $r \in \mathbb{N}$ und $s \in \mathbb{Z}$ mit $f^r(M) \subseteq \pi^s M$ und $\text{Newton}(V,f) = \frac{s}{r}$. Dann sind $M_1 := \alpha^{-1}(M)$ und $M_2 := \beta(M)$ Gitter in $V_1$ bzw. $V_2$ (**Übungsaufgabe**) mit $f_i^r(M_i) \subseteq \pi^s M_i$. Somit gilt $\text{Newton}(V,f) = \frac{s}{r} \leq \frac{1}{r}\,\text{ord}_{M_i} f_i^r \leq \text{Newton}(V_i, f_i)$.

Ist $(V,f)$ isoklin, so können wir wegen Lemma 8.15 annehmen, daß $f^r(M) = \pi^s M$ und damit auch $f_i^r(M_i) = \pi^s M_i$ gilt. Wieder aus Lemma 8.15 folgt, daß die $(V_i, f_i)$ isoklin sind mit $\text{Newton}(V_i, f_i) = \frac{s}{r} = \text{Newton}(V,f)$.

ii. Sei $\alpha \neq 0$ ein solcher Homomorphismus. Wir betrachten das Isokristall $(V_1 := \text{im}(\alpha), f_1 := f'|V_1)$ bzw. $(V_1 := \text{im}(\alpha), f_1 := f|V_1)$. Aus i. folgt dann $\text{Newton}(V,f) = \text{Newton}(V_1, f_1) \geq \text{Newton}(V', f')$, was im Widerspruch zur Voraussetzung steht. □

**Lemma 8.17.** *Für teilerfremde $r \in \mathbb{N}$ und $s \in \mathbb{Z}$ (insbesondere $r = 1$ im Falle $s = 0$) besitzt das Standardisokristall $V_{s,r}$ keine echten Unterisokristalle.*

*Beweis.* Sei $(V,f)$ ein Unterisokristall von $V_{s,r}$ der Höhe $1 \leq h \leq r$ und der Dimension $d$. Nach Lemma 8.16.i. ist $(V,f)$ isoklin mit

$$\frac{d}{h} = \text{Newton}(V,f) = \text{Newton}(V_{s,r}) = \frac{s}{r}\ .$$

Wegen der Teilerfremdheit von $r$ und $s$ muß $r$ ein Teiler von $h$ sein, also $r = h$ und damit $V = V_{s,r}$ gelten. □

Von jetzt ab werden wir $A$ als vollständig voraussetzen. Für jedes Gitter $M$ in $V$ ist dann die natürliche Abbildung $M \xrightarrow{\cong} \varprojlim_k M/\pi^k M$ ein Isomorphismus.

**Satz 8.18.** *Sei $A$ vollständig; es existieren eindeutig bestimmte isokline Unterisokristalle $(V_1, f_1), \ldots, (V_r, f_r) \subseteq (V,f)$ mit*

$$V = \bigoplus_{i=1}^{t} V_i,\ \ f = \bigoplus_{i=1}^{t} f_i$$

*und*

$$\text{Newton}(V,f) = \text{Newton}(V_1, f_1) < \text{Newton}(V_2, f_2) < \ldots < \text{Newton}(V_t, f_t)\ .$$

*Beweis.* Per Induktion genügt es, die Existenz einer eindeutig bestimmten Zerlegung

$$V = V_1 \oplus V_1'$$

in $f$-invariante Unterräume zu zeigen, so daß $(V_1, f|V_1)$ isoklin ist und

$$\text{Newton}(V, f) = \text{Newton}(V_1, f|V_1) < \text{Newton}(V_1', f|V_1')$$

gilt.

*Existenz:* Sei $\text{Newton}(V, f) = \frac{s}{r}$ mit $r \in \mathbb{N}$ und $s \in \mathbb{Z}$, und sei $M$ ein Gitter in $V$ mit $f^r(M) \subseteq \pi^s M$ (siehe Satz 8.12). Die Abbildung $g := \pi^{-s} f^r$ erfüllt dann $g(M) \subseteq M$ und induziert somit für jedes $k \in \mathbb{N}$ eine semilineare Abbildung

$$g_k : M/\pi^k M \longrightarrow M/\pi^k M \ .$$

Zunächst fixieren wir ein $k$. Da $M/\pi^k M$ endliche Länge hat, müssen die Ketten von $A$-Untermoduln

$$\text{im}(g_k) \supseteq \text{im}(g_k^2) \supseteq \ldots \supseteq \text{im}(g_k^i) \supseteq \ldots$$

und

$$\ker(g_k) \subseteq \ker(g_k^2) \subseteq \ldots \subseteq \ker(g_k^i) \subseteq \ldots$$

in $M/\pi^k M$ stationär werden. Also existiert ein $j = j(k) \geq 1$ mit

$$M_{k,1} := \text{im}(g_k^j) = \text{im}(g_k^i) \quad \text{und} \quad M_{k,1}' := \ker(g_k^j) = \ker(g_k^i)$$

für alle $i \geq j$. Es ergeben sich sofort folgende Eigenschaften:

a. $g_k(M_{k,1}) = g_k(\text{im}(g_k^j)) = \text{im}(g_k^{j+1}) = M_{k,1}$.

b. $g_k^j(M_{k,1}') = g_k^j(\ker(g_k^j)) = \{0\}$;

c. $g_k(M_{k,1}') = g_k(\ker(g_k^{j+1})) \subseteq \ker(g_k^j) = M_{k,1}'$;

Da $M_{k,1}$ endliche Länge hat, folgt aus a., daß

$$g_k : M_{k,1} \xrightarrow{\cong} M_{k,1}$$

bijektiv ist. Wegen b. erhalten wir insbesondere

$$M_{k,1} \cap M_{k,1}' = \{0\} \ .$$

Sei $\bar{v} \in M/\pi^k M$ ein beliebiges Element. Dann ist $g_k^j(\bar{v}) = g_k^{2j}(\bar{\bar{v}})$ für ein $\bar{\bar{v}} \in M/\pi^k M$ und damit

$$\bar{v} = g_k^j(\bar{\bar{v}}) + (\bar{v} - g_k^j(\bar{\bar{v}})) \in M_{k,1} + M_{k,1}' \ .$$

Folglich gilt

$$M/\pi^k M = M_{k,1} \oplus M'_{k,1} \ .$$

Wenn $k$ nun variiert, prüft man leicht nach, daß diese Zerlegungen unter den Projektionsabbildungen $M/\pi^{k+1}M \longrightarrow M/\pi^k M$ kompatibel sind. Setzen wir

$$M_1 := \varprojlim_k M_{k,1} \quad \text{und} \quad M'_1 := \varprojlim_k M'_{k,1} \ ,$$

so erhalten wir also eine Zerlegung

$$M = M_1 \oplus M'_1$$

in $g$-invariante $A$-Untermoduln. Dabei gilt

d. $g(M_1) = M_1$;

e. $g^{j(1)}(M'_1) \subseteq \pi M'_1$.

Wir definieren schließlich $V_1 := KM_1$ und $V'_1 := KM'_1$, was zu der Zerlegung

$$V = V_1 \oplus V'_1$$

in $g$-invariante Unterräume führt. Offensichtlich ist $M_1$ bzw. $M'_1$ ein Gitter in $V_1$ bzw. $V'_1$. Wegen d. und Lemma 8.15 ist $(V_1, g|V_1)$ isoklin mit erstem Anstieg $= 0$; wegen e. gilt

$$\mathrm{Newton}(V'_1, g|V'_1) \geq \frac{1}{j(1)} > 0 = \mathrm{Newton}(V_1, g|V_1) \ .$$

Nun ist aber

$$V = f(V_1) \oplus f(V'_1)$$

eine weitere Zerlegung in $g$-invariante Unterräume, wobei $(f(V_1), g|f(V_1))$ ebenfalls isoklin ist mit

$$\mathrm{Newton}(f(V'_1), g|f(V'_1)) > 0 = \mathrm{Newton}(f(V_1), g|f(V_1)) \ .$$

Aus Lemma 8.16 folgt dann, daß die zusammengesetzten Abbildungen

$$(V_1, g|V_1) \xrightarrow{\subseteq} (V, g) \xrightarrow{pr} (f(V'_1), g|f(V'_1))$$

und

$$(V'_1, g|V'_1) \xrightarrow{\subseteq} (V, g) \xrightarrow{pr} (f(V_1), g|f(V_1))$$

die Nullabbildungen sein müssen. Das bedeutet, daß $V_1$ und $V_1'$ sogar $f$-invariant sind. Aus d. und e. ergibt sich jetzt

$$f^r(M_1) = \pi^s M_1 \quad \text{und} \quad f^{rj(1)}(M_1') \subseteq \pi^{sj(1)+1} M_1' \ .$$

Wieder wegen Lemma 8.15 ist also $(V_1, f|V_1)$ isoklin mit

$$\text{Newton}(V,f) = \frac{s}{r} = \text{Newton}(V_1, f|V_1) < \frac{sj(1)+1}{rj(1)} \leq \text{Newton}(V_1', f|V_1') \ .$$

*Eindeutigkeit:* Das folgt aus Lemma 8.16 in der gleichen Weise wie eben die $f$-Invarianz von $V_1$ und $V_1'$. □

**Definition 8.19.** *Die Zahlen* $\text{Newton}(V_1, f_1), \ldots, \text{Newton}(V_t, f_t)$ *aus Satz 8.18 heißen die Anstiege des Isokristalls* $(V, f)$.

Mit den Bezeichnungen aus Satz 8.18 setze

$$\lambda_i := \text{Newton}(V_i, f_i),\ h_i := h(V_i, f_i),\ d_i := d(V_i, f_i) \ .$$

Es gilt

$$\lambda_i = \frac{d_i}{h_i}$$

und

$$h_1 + \ldots + h_t = h,\ d_1 + \ldots + d_t = d \ .$$

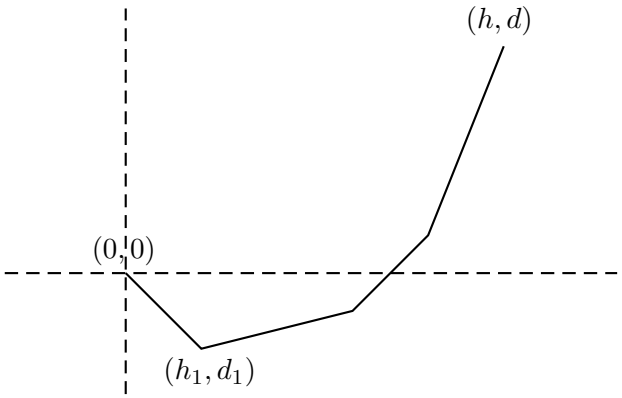
Man benutzt jetzt die Zahlenfolge

$$(\mu_1, \ldots, \mu_h) := (\lambda_1, \ldots, \lambda_1, \lambda_2, \ldots, \lambda_2, \ldots, \lambda_t, \ldots, \lambda_t) \ ,$$

wobei jedes $\lambda_i$ genau $h_i$-mal wiederholt wird, zur Definition der Funktion

$$\text{Newton}_{(V,f)}(i) := \begin{cases} 0 & \text{für } i = 0 \ , \\ \sum_{j=1}^{i} \mu_j & \text{für } 1 \leq i \leq h \ . \end{cases}$$

Durch lineares Verbinden der Punkte $(i, \text{Newton}_{(V,f)}(i))$ in der Ebene $\mathbb{R}^2$ ergibt sich das *Newton-Polygon* von $(V, f)$. Es beginnt im Punkt $(0, 0)$ und endet im Punkt $(h, d)$. Offensichtlich lassen sich alle Zahlen $h_i, d_i, \lambda_i$ aus diesem Polynom ablesen. Zum Beispiel sind die $\lambda_i$ genau die Steigungen der sukzessiven Geradenstücke:




Um auch die Struktur der isoklinen Isokristalle bestimmen zu können, müssen wir weitere Voraussetzungen machen:

(DM)
- $A$ ist vollständig mit algebraisch abgeschlossenem Restklassenkörper $A/\mathfrak{m}$ der Charakteristik $p > 0$;
- $\sigma(a) \equiv a^q \bmod \mathfrak{m}$ für alle $a \in A$ und eine feste $p$-Potenz $q > 1$;
- es existiert ein Primelement $\pi \in A$ mit $\sigma(\pi) = \pi$ .

**Satz 8.20.** *Es gelte* (DM)*; ist $(V, f)$ ein isoklines $\sigma$-Isokristall mit Anstieg $= 0$, so existiert eine $K$-Basis $v_1, \ldots, v_h$ von $V$ mit $f(v_j) = v_j$ für alle $1 \leq j \leq h$.*

*Beweis.* Sei $M$ ein Gitter in $V$ mit $f(M) = M$. Wir konstruieren die gewünschte Basis als $A$-Basis von $M$. Wegen $M \xrightarrow{\cong} \varprojlim_k M/\pi^k M$ genügt es, die gesuchten Basisvektoren als Elemente in $\varprojlim M/\pi^k M$ anzugeben. Dementsprechend werden wir induktiv eine Folge $\{(v_1^{(k)}, \ldots, v_h^{(k)})\}_k$ in $M^h$ konstruieren mit den Eigenschaften:

1. $\{v_1^{(k)} \bmod \pi M, \ldots, v_h^{(k)} \bmod \pi M\}$ ist eine $A/\mathfrak{m}$-Basis von $M/\pi M$;
2. $f(v_j^{(k)}) \equiv v_j^{(k)} \bmod \pi^k M$ für alle $1 \leq j \leq h$;
3. $v_j^{(k+1)} \equiv v_j^{(k)} \bmod \pi^k M$ für alle $1 \leq j \leq h$.

Der Induktionsanfang, also die Existenz von $v_1^{(1)}, \ldots, v_h^{(1)}$ mit 1. - 3. folgt sofort aus Satz 2.1. Seien nun $v_1^{(k)}, \ldots, v_h^{(k)}$ mit 1. - 3. schon konstruiert.

Man überlege sich (**Übungsaufgabe**) zunächst, daß $v_1^{(k)}, \dots, v_h^{(k)}$ wegen 1. eine $A$-Basis von $M$ ist. Also haben wir

$$f(v_j^{(k)}) - v_j^{(k)} = \pi^k \sum_{i=1}^{h} a_{ij} v_i^{(k)} \qquad \text{mit } a_{ij} \in A \ .$$

Da der Restklassenkörper algebraisch abgeschlossen ist, finden wir Elemente $b_{ij} \in A$ mit

$$a_{ij} + \sigma(b_{ij}) - b_{ij} \equiv a_{ij} + b_{ij}^q - b_{ij} \equiv 0 \bmod \mathfrak{m} \ .$$

Setze

$$v_j^{(k+1)} := v_j^{(k)} + \pi^k \sum_{i=1}^{h} b_{ij} v_i^{(k)} \ .$$

Ersichtlich sind dann 1. und 3. per Konstruktion erfüllt. Für 2. berechnen wir

$$\begin{aligned} & f(v_j^{(k+1)}) - v_j^{(k+1)} \\ & \quad = f(v_j^{(k)}) - v_j^{(k)} + \sigma(\pi)^k \sum_{i=1}^{h} \sigma(b_{ij}) f(v_i^{(k)}) - \pi^k \sum_{i=1}^{h} b_{ij} v_i^{(k)} \\ & \quad = \pi^k \sum_{i=1}^{h} (a_{ij} + \sigma(b_{ij}) - b_{ij}) v_i^{(k)} + \pi^{2k} \sum_{i=1}^{h} \sum_{\ell=1}^{h} \sigma(b_{ij}) a_{\ell i} v_\ell^{(k)} \\ & \quad \equiv 0 \bmod \pi^{k+1} M \ . \end{aligned}$$

Wegen 3. sind die Vektoren $v_j := (v_j^{(k)} + \pi^k M)_k$ in $M \cong \varprojlim M/\pi^k M$ wohldefiniert, wegen 1. bilden sie eine $A$-Basis von $M$ und damit eine $K$-Basis von $V$ und wegen 2. erfüllen sie $f(v_j) = v_j$. □

**Satz 8.21.** *Es gelte* (DM)*; sei* $(V, f)$ *ein isoklines* $\sigma$*-Isokristall, und schreibe* $\mathrm{Newton}(V, f) = \frac{s}{r}$ *mit teilerfremden* $r \in \mathbb{N}$ *und* $s \in \mathbb{Z}$*; dann ist* $(V, f)$ *isomorph zu einer (endlichen) direkten Summe von Standardisokristallen* $V_{s,r}$*.*

*Beweis.* Nach Lemma 8.13 finden wir ein Gitter $M$ in $V$ mit $f^r(M) \subseteq \pi^s M$. Aus $\frac{s}{r} = \frac{d}{h}$ folgt

$$[\pi^s M : f^r(M)] = [M : f^r(M)] - [M : \pi^s M] = rd - sh = 0$$

und damit $f^r(M) = \pi^s M$. Durch Anwendung von Satz 8.20 auf das Isokristall $(V, \pi^{-s} f^r)$, welches wegen Lemma 8.15 und Lemma 8.10 isoklin mit

Anstieg $= 0$ ist, finden wir eine Basis $v_1, \ldots, v_h$ von $V$ mit $f^r(v_j) = \pi^s v_j$. Wir setzen $V_j := \sum_{i=0}^{r-1} K f^i(v_j)$. Dann definiert

$$\begin{aligned} V_{s,r} &\longrightarrow (V_j, f|V_j) \\ e_i &\longmapsto f^{i-1}(v_j) \end{aligned}$$

einen surjektiven Homomorphismus von Isokristallen, der wegen Lemma 8.17 sogar ein Isomorphismus sein muß. Also haben wir

$$V = \sum_{j=1}^{h} V_j \quad \text{mit } (V_j, f|V_j) \cong V_{s,r} \ .$$

Wieder wegen Lemma 8.17 gilt entweder $V_j \subseteq \sum_{i \neq j} V_i$ oder $V_j \cap \sum_{i \neq j} V_i = \{0\}$. Durch eventuelles Weglassen einiger Summanden läßt sich deswegen obige Summendarstellung von $V$ zu einer direkten Summe verkürzen. $\square$

# Teil II
# Semilineare Algebra über dem Robba-Ring

Wie bisher fixieren wir einen vollständigen diskreten Bewertungsring $A$ mit maximalem Ideal $\mathfrak{m} = \pi A$, Restklassenkörper $k = A/\mathfrak{m}$ und Quotientenkörper $K$. Bezeichne $|x| := e^{-v(x)}$ die zur diskreten Bewertung $v$ von $A$ gehörige Normfunktion auf $K$. Wir fixieren auch einen algebraischen Abschluß $\bar{K}$ von $K$. Nach Satz 4.3 setzt sich $|\ |$ in eindeutiger Weise zu einer Normfunktion auf $\bar{K}$ fort, die wir ebenfalls mit $|\ |$ bezeichnen.

## 9 Laurentreihen

Eine *Laurentreihe* (mit Koeffizienten in $K$) ist eine formale Reihe

$$F(T) = \sum_{n\in\mathbb{Z}} a_n T^n \qquad \text{mit } a_n \in K\ .$$

Für gegebene reelle Zahl $0 < \delta \leq \varepsilon$ heißt sie $[\delta,\varepsilon]$-*konvergent*, falls gilt

$$\lim_{n\to\infty} |a_{-n}|\delta^{-n} = \lim_{n\to\infty} |a_n|\varepsilon^n = 0\ .$$

Offensichtlich bilden die $[\delta,\varepsilon]$-konvergenten Laurentreihen über $K$ einen $K$-Vektorraum $\mathcal{A}_{[\delta,\varepsilon]}(K)$. Es gilt

$$\mathcal{A}_{[\delta,\varepsilon]}(K) \subseteq \mathcal{A}_{[\delta'\varepsilon']}(K) \qquad \text{für } \delta \leq \delta' \leq \varepsilon' \leq \varepsilon$$

und

$$\mathcal{A}_{[\delta,\varepsilon]}(K) = \bigcap_{\delta\leq\rho\leq\varepsilon} \mathcal{A}_{[\rho,\rho]}(K)\ .$$

Auf $\mathcal{A}_{[\rho,\rho]}(K)$ haben wir die Vektorraumnorm

$$\|F\|_\rho := \max_{n\in\mathbb{Z}} |a_n|\rho^n\ .$$

**Übungsaufgabe 9.1.** *Für jedes $x \in \bar{K}$ mit $\delta \leq |x| \leq \varepsilon$ ist die Reihe $F(x) := \sum_{n\in\mathbb{Z}} a_n x^n$ konvergent in $\bar{K}$.*

**Lemma 9.2.** *$\mathcal{A}_{[\delta,\varepsilon]}(K)$ ist ein Integritätsbereich bzgl. der Multiplikation*

$$\Big(\sum_{n\in\mathbb{Z}} b_n T^n\Big)\Big(\sum_{n\in\mathbb{Z}} c_n T^n\Big) := \sum_{n\in\mathbb{Z}} \Big(\sum_{k+\ell=n} b_k c_\ell\Big) T^n\ ;$$

*dabei gilt $\|FG\|_\rho = \|F\|_\rho \cdot \|G\|_\rho$ für alle $F, G \in \mathcal{A}_{[\delta,\varepsilon]}(K)$ und alle $\delta \leq \rho \leq \varepsilon$.*

*Beweis.* Es genügt, den Fall $\delta = \rho = \varepsilon$ zu betrachten. Wir setzen $F(T) := \sum_{n\in\mathbb{Z}} b_n T^n$, $G(T) := \sum_{n\in\mathbb{Z}} c_n T^n$ und $a_n := \sum_{k+\ell=n} b_k c_\ell$. Offensichtlich können wir $\|F\|_\rho \neq 0$ und $\|G\|_\rho \neq 0$ annehmen. Zu jedem $C > 0$ existiert dann ein $N \in \mathbb{N}$ mit

$$|b_i|\rho^i < \frac{C}{\|G\|_\rho} \quad \text{und} \quad |c_i|\rho^i < \frac{C}{\|F\|_\rho}$$

für alle $i \in \mathbb{Z}$ mit $|i| \geq N$. Für $n \in \mathbb{Z}$ mit $|n| \geq 2N$ ergibt sich

$$|a_n|\rho^n \leq \max_{k+\ell=n} |b_k|\rho^k \cdot |c_\ell|\rho^\ell < C \ .$$

Also ist $(FG)(T)$ wieder $[\rho,\rho]$-konvergent. Assoziativgesetz und Distributivgesetz folgen unmittelbar aus der Definition der Multiplikation. Ebenso ist die Ungleichung $\|FG\|_\rho \leq \|F\|_\rho \cdot \|G\|_\rho$ eine direkte Folge der strikten Dreiecksungleichung für $|\ |$. Für die umgekehrte Ungleichung seien $k_0$ und $\ell_0$ die kleinsten Indizes mit

$$|b_{k_0}|\rho^{k_0} = \|F\|_\rho \quad \text{und} \quad |c_{\ell_0}|\rho^{\ell_0} = \|G\|_\rho \ .$$

Wir setzen $n_0 := k_0 + \ell_0$. Für $n_0 = k + \ell$ gilt $k \leq k_0$ oder $\ell \leq \ell_0$. Ist $k \neq k_0$ und $\ell \neq \ell_0$, so folgt

$$|b_k|\rho^k < \|F\|_\rho \text{ oder } |c_\ell|\rho^\ell < \|G\|_\rho \text{ und damit } |b_k c_\ell|\rho^{n_0} < \|F\|_\rho \cdot \|G\|_\rho \ .$$

Also ist

$$\|FG\|_\rho \geq |a_{n_0}|\rho^{n_0} = |b_{k_0}|\rho^{k_0} \cdot |c_{\ell_0}|\rho^{\ell_0} = \|F\|_\rho \cdot \|G\|_\rho \ .$$

Schließlich muß $\|FG\|_\rho \neq 0$ und somit $FG \neq 0$ gelten. Das bedeutet, daß $\mathcal{A}_{[\rho,\rho]}(K)$ nullteilerfrei ist. □

Wir fixieren nun ein $0 \neq F(T) = \sum_{n\in\mathbb{Z}} a_n T^n$ in $\mathcal{A}_{[\delta,\varepsilon]}(K)$ und betrachten die Funktion

$$\begin{aligned} [\delta,\varepsilon] &\longrightarrow \mathbb{R}_{>0} \\ \rho &\longmapsto \|F\|_\rho \ . \end{aligned}$$

Auf Grund des nachfolgenden Lemmas beschreibt sie sozusagen das Wachstum der Funktion $x \longmapsto F(x)$ auf $\bar{K}$.

**Lemma 9.3.** *(Das Maximumprinzip)*
*Für $\rho \in |\bar{K}^\times| \cap [\delta,\varepsilon]$ gilt*

$$\|F\|_\rho = \max\{|F(x)| : x \in \bar{K}, |x| = \rho\} \ .$$

*Beweis.* Ersichtlich können wir $K$ durch eine endliche Erweiterung ersetzen, ohne die Behauptung zu ändern. Deswegen können wir annehmen, daß ein $c \in K^\times$ existiert mit $|c| = \rho$. Dann ist auch $0 \neq \|F\|_\rho = |a|$ für ein $a \in K^\times$. Die Laurentreihe

$$G(T) := \sum_{n\in\mathbb{Z}} c_n T^n \qquad \text{mit } c_n := a^{-1}a_n c^n$$

ist $[1,1]$-konvergent mit $\|G\|_1 = 1$. Insbesondere liegen alle Koeffizienten $c_n$ in $A$ mit $c_{n_0} \in A^\times$ für mindestens ein $n_0 \in \mathbb{Z}$. Wegen $v(c_n) \longrightarrow \infty$ für $n \longrightarrow \pm\infty$ ist somit $G(T) \bmod \mathfrak{m}$ ein *Laurentpolynom* $\neq 0$ über $k$, d. h. es existiert ein $m \in \mathbb{N}$ mit

$$0 \not\equiv T^m G(T) \bmod \mathfrak{m} \in k[T] \ .$$

Der Restklassenkörper von $\bar{K}$ ist ein algebraischer Abschluß $\bar{k}$ des Restklassenkörpers $k$ (**Übungsaufgabe**). Weil $\bar{k}$ stets unendlich ist, finden wir ein $b \in \bar{K}$ mit $|b| = 1 = |G(b)|$. Das bedeutet

$$1 = |G(b)| \leq \max\{|G(x)| : x \in \bar{K}, |x| = 1\} \leq \|G\|_1 = 1$$

und damit

$$\begin{aligned} \|F\|_\rho = |a| \cdot \|G\|_1 &= \max\{|aG(x)| : x \in \bar{K}, |x| = 1\} \\ &= \max\{|\sum_{n\in\mathbb{Z}} a_n (cx)^n| : x \in \bar{K}, |x| = 1\} \\ &= \max\{|F(x)| : x \in \bar{K}, |x| = \rho\} \ . \end{aligned}$$

□

**Definition 9.4.** *Ein $\rho \in [\delta, \varepsilon]$ heißt kritischer Radius für $F$, falls mindestens zwei verschiedene Indizes $n_1, n_2 \in \mathbb{Z}$ existieren mit*

$$\|F\|_\rho = |a_{n_1}|\rho^{n_1} = |a_{n_2}|\rho^{n_2} \ .$$

**Lemma 9.5.** *$F$ besitzt höchstens endlich viele kritische Radien.*

*Beweis.* Seien $M, N \geq 0$ mit

$$|a_{-M}|\delta^{-M} = \max_{n\leq 0} |a_n|\delta^n \quad \text{und} \quad |a_N|\varepsilon^N = \max_{n\geq 0} |a_n|\varepsilon^n \ .$$

Sei $\delta < \rho < \varepsilon$. Für $n > N$ haben wir $|a_n|\varepsilon^n \leq |a_N|\varepsilon^N$ und damit im Falle $a_N \neq 0$, daß

$$a_n = 0 \text{ oder } \frac{|a_n|}{|a_N|}\rho^{n-N} < \frac{|a_n|}{|a_N|}\varepsilon^{n-N} \leq 1, \quad \text{also stets} \quad |a_n|\rho^n < |a_N|\rho^N \ .$$

Analog ergibt sich im Falle $a_{-M} \neq 0$, daß

$$|a_{-n}|\rho^{-n} < |a_{-M}|\rho^{-M} \quad \text{für} \quad n > M \ .$$

Für kritisches $\delta < \rho < \varepsilon$ muß also gelten

$$0 \neq \|F\|_\rho = |a_{n_1}|\rho^{n_1} = |a_{n_2}|\rho^{n_2} \ \text{ mit geeigneten } \ -M \leq n_1 < n_2 \leq N \ .$$

Folglich liegen die kritischen Radien $\neq \delta, \varepsilon$ in der endlichen Menge $\{\rho : \rho^{n_2-n_1} = |a_{n_1}|/|a_{n_2}|, -M \leq n_1 < n_2 \leq N, a_{n_1}, a_{n_2} \neq 0\}$. □

Seien nun $\delta < \rho_1 < \ldots < \rho_k < \varepsilon$ sämtliche kritischen Radien von $F$ in dem offenen Intervall $(\delta, \varepsilon)$. Wir setzen außerdem $\rho_0 := \delta$ und $\rho_{k+1} := \varepsilon$. Das Argument im Beweis von Lemma 9.5 liefert die Existenz von ganzen Zahlen $M \leq N$, so daß für alle $\rho \in [\delta, \varepsilon]$ gilt

$$\|F\|_\rho = \max_{M \leq n \leq N} |a_n|\rho^n > |a_{n'}|\rho^{n'} \ \text{ für alle } \ n' < M \text{ oder } > N \ . \tag{11}$$

**Lemma 9.6.** *Zu jedem $0 \leq i \leq k$ existiert (genau) ein $n_i \in \mathbb{Z}$ mit*

$$\|F\|_\rho = |a_{n_i}|\rho^{n_i} \quad \textit{für alle} \quad \rho_i < \rho < \rho_{i+1} \ .$$

*Beweis.* Zu jedem $n \in \mathbb{Z}$ sei $U_n := \{\rho_i < \rho < \rho_{i+1} : \|F\|_\rho = |a_n|\rho^n\}$. Wegen (11) bilden die $U_M, \ldots, U_N$ eine disjunkte Überdeckung des zusammenhängenden Intervalls $(\rho_i, \rho_{i+1})$. Ebenso folgt aus (11) leicht, daß jedes $U_n$ eine offene Menge ist. Folglich muß $(\rho_i, \rho_{i+1}) = U_{n_i}$ für ein geeignetes $n_i$ gelten. □

Die Formel (11) zeigt, daß es zweckmäßig ist, die logarithmische Version

$$\begin{aligned} w_F : [\log\delta, \log\varepsilon] &\longrightarrow \mathbb{R} \\ t &\longmapsto \log\|F\|_{e^t} = \max_{n\in\mathbb{Z}}(nt - v(a_n)) \end{aligned}$$

der Funktion $\rho \longmapsto \|F\|_\rho$ zu betrachten. Dann ist

$$w_F(t) = \max_{M \leq n \leq N}(nt - v(a_n))$$

das Maximum von endlich vielen affin-linearen Funktionen. Folglich ist $w_F$ stetig, konvex und stückweise linear. Wegen Lemma 9.6 ändert sich die Steigung von $w_F$ genau an den Stellen $\log\rho_1, \ldots, \log\rho_k$. Wir setzen

$$n(F, \rho) := \min\{n \in \mathbb{Z} : \|F\|_\rho = |a_n|\rho^n\}$$

und

$$N(F,\rho) := \max\{n \in \mathbb{Z} : \|F\|_\rho = |a_n|\rho^n\} \ .$$

Aus der Formel (11) folgt, daß die links- bzw. rechtsseitige Steigung der Funktion $w_F$ im Punkte $\log \rho$ gleich $n(F,\rho)$ bzw. $N(F,\rho)$ ist. Ferner impliziert die Konvexität von $w_F$ dann die Ungleichung

$$N(F,\rho) \leq n(F,\rho') \qquad \text{für alle } \delta \leq \rho < \rho' \leq \varepsilon.$$

**Übungsaufgabe 9.7.** *Für $F, G \neq 0$ in $\mathcal{A}_{[\rho,\rho]}(K)$ gilt*

$$n(FG,\rho) = n(F,\rho) + n(G,\rho) \quad \textit{und} \quad N(FG,\rho) = N(F,\rho) + N(G,\rho)$$

*(vgl. das Argument im Beweis von Lemma 9.2).*

**Definition 9.8.** *Ein Polynom $0 \neq P \in K[T]$ heißt $\rho$-dominant bzw. $\rho$-extremal, falls $N(P,\rho) = \deg(P)$ bzw. $n(P,\rho) = 0$ und $N(P,\rho) = \deg(P)$ gilt.*

**Lemma 9.9.** *Für $0 \neq P \in K[T]$ sind äquivalent:*

*i. $P$ ist $\rho$-dominant bzw. $\rho$-extremal;*

*ii. alle Nullstellen $x \in \bar{K}$ von $P$ erfüllen $|x| \leq \rho$ bzw. $|x| = \rho$.*

*Beweis.* Sei $d := \deg(P)$ und

$$P(T) = b_0 + \ldots + b_d T^d = b_d(T - x_1)\ldots(T - x_d) \ .$$

Insbesondere ist $b_0 = (-1)^d b_d x_1 \ldots x_d$.

ii. $\Longrightarrow$ i. Aus $|x_i| \leq \rho$ folgt $|b_j| \leq |b_d|\rho^{d-j}$, also $|b_j|\rho^j \leq |b_d|\rho^d$, was $N(P,\rho) = d$ bedeutet. Gilt sogar $|x_i| = \rho$, so ergibt sich zusätzlich $|b_0| = |b_d|\rho^d$ und damit $n(P,\rho) = 0$.

i. $\Longrightarrow$ ii. Der Übungsaufgabe 9.7 zu Folge sind ein einer Zerlegung $P = P_1 P_2$ mit $P$ auch beide Faktoren $P_i$ $\rho$-dominant bzw. $\rho$-extremal. Da außerdem eine endliche Erweiterung des Körpers $K$ keinen Einfluß auf die Behauptung hat, können wir also annehmen, daß $\deg(P) = 1$ gilt. In diesem Falle ist die Implikation wegen $b_0 = -b_1 x_1$ offensichtlich. □

**Satz 9.10.** *(1. Divisionssatz)*
*Seien $F(T) = \sum_{n\geq 0} a_n T^n$ eine Potenzreihe in $\mathcal{A}_{[\rho,\rho]}(K)$ und $P(T) = b_0 + \ldots + b_d T^d$ ein $\rho$-dominantes Polynom vom Grade $d > 0$ in $K[T]$; dann*

*existieren eine eindeutig bestimmte Potenzreihe* $G \in \mathcal{A}_{[\rho,\rho]}(K)$ *und ein eindeutig bestimmtes Polynom* $Q$ *vom Grade* $< d$ *mit*

$$F = PG + Q \ ;$$

*darüberhinaus gilt*

$$\|F\|_\rho = \max(\|Q\|_\rho, \|P\|_\rho \cdot \|G\|_\rho) \ .$$

*Beweis. Eindeutigkeit:* Es gelte $F = PG_1 + Q_1 = PG_2 + Q_2$ und damit $P(G_1 - G_2) = Q_2 - Q_1$. Im Falle $G_1 \neq G_2$ folgt aus der Übungsaufgabe 9.7

$$\begin{aligned} d &> \deg(Q_2 - Q_1) \geq N(Q_2 - Q_1, \rho) = N(P(G_1 - G_2), \rho) \\ &= N(P, \rho) + N(G_1 - G_2, \rho) = d + N(G_1 - G_2, \rho) \\ &\geq d \ , \end{aligned}$$

da die Potenzreihe $G_1 - G_2$ natürlich $N(G_1 - G_2, \rho) \geq 0$ erfüllt. Dies ist ein Widerspruch. Also muß $G_1 = G_2$ und dann auch $Q_1 = Q_2$ gelten.

*Existenz: 1. Fall:* Zunächst sei $F$ ein Polynom vom Grade $h$. Wir beweisen die Existenz per Induktion nach $h$. Für $h < d$ ist nichts zu zeigen (setze $G := 0$ und $Q := F$). Für $h \geq d$ setze $G_0(T) := a_h b_d^{-1} T^{h-d}$. Dann ist $F_0 := F - PG_0$ ein Polynom vom Grade $< h$. Nach Induktionsannahme finden wir Polynome $G_1$ und $Q$, letzteres vom Grade $< d$, mit

$$F_0 = PG_1 + Q \quad \text{und} \quad \|F_0\|_\rho = \max(\|Q\|_\rho, \|P\|_\rho \cdot \|G_1\|_\rho) \ .$$

Für $G := G_0 + G_1$ gilt dann $F = PG + Q$ und

$$\begin{aligned} \max(\|Q\|_\rho, \|P\|_\rho \cdot \|G\|_\rho) &\leq \max(\|Q\|_\rho, \|P\|_\rho \cdot \|G_0\|_\rho, \|P\|_\rho \cdot \|G_1\|_\rho) \\ &= \max(\|F_0\|_\rho, \|P\|_\rho \cdot \|G_0\|_\rho) \\ &\leq \max(\|F\|_\rho, \|P\|_\rho \cdot \|G_0\|_\rho) \\ &= \max(\|F\|_\rho, |b_d|\rho^d \cdot |a_h b_d^{-1}|\rho^{h-d}) \\ &= \max(\|F\|_\rho, |a_h|\rho^h) \\ &= \|F\|_\rho \ , \end{aligned}$$

wobei in der zweiten Ungleichung die Multiplikativität von $\| \ \|_\rho$ aus Lemma 9.2 verwendet wird. Die strikte Dreiecksungleichung für $\| \ \|_\rho$ zusammen mit der Multiplikativität liefert direkt die umgekehrte Ungleichung.

*2. Fall :* Nun sei $F$ eine beliebige Potenzreihe. Den 1. Fall anwendend schreiben wir

$$a_n T^n = PG_n + Q_n \text{ mit } \deg(Q_n) < d \text{ und } |a_n|\rho^n = \max(\|Q_n\|_\rho, \|P\|_\rho \|G_n\|_\rho)$$

für jedes $n \geq 0$. Die letztere Normgleichung impliziert, daß

$$G := \sum_{n\geq 0} G_n \quad \text{und} \quad Q := \sum_{n\geq 0} Q_n$$

bzgl. $\| \ \|_\rho$ konvergente Reihen sind und unsere Behauptung erfüllen. □

**Satz 9.11.** *(2. Divisionssatz)*
*Seien $F \in \mathcal{A}_{[\delta,\varepsilon]}(K)$, $\rho \in [\delta, \varepsilon]$ und $P$ ein $\rho$-extremales Polynom vom Grade $d > 0$; dann existieren eindeutig bestimmte $G \in \mathcal{A}_{[\delta,\varepsilon]}(K)$ und $Q \in K[T]$ vom Grade $< d$ mit*

$$F = PG + Q \ ;$$

*darüberhinaus gilt*

$$\|F\|_\rho = \max(\|Q\|_\rho, \|P\|_\rho \cdot \|G\|_\rho) \ .$$

*Beweis. Eindeutigkeit:* Es gelte $F = PG_1 + Q_1 = PG_2 + Q_2$ mit $Q_1 \neq Q_2$. Aus $P(G_1 - G_2) = Q_2 - Q_1$ folgt dann unter Benutzung der Übungsaufgabe 9.7 der Widerspruch

$$\begin{aligned} d &> \deg(Q_2 - Q_1) \geq N(Q_2 - Q_1, \rho) - n(Q_2 - Q_1, \rho) \\ &= N(P(G_1 - G_2), \rho) - n(P(G_1 - G_2), \rho) \\ &= N(P, \rho) - n(P, \rho) + N(G_1 - G_2, \rho) - n(G_1 - G_2, \rho) \\ &\geq N(P, \rho) - n(P, \rho) \\ &= d \ . \end{aligned}$$

*Existenz:* Sei $F = F_- + F_+$ mit

$$F_-(T) = \sum_{n<0} a_n T^n \qquad \text{und} \qquad F_+(T) = \sum_{n\geq 0} a_n T^n \ .$$

Für jedes $\mu \in [\delta, \varepsilon]$ gilt $F_\pm \in \mathcal{A}_{[\mu,\mu]}(K)$ mit $\|F\|_\mu = \max(\|F_+\|_\mu, \|F_-\|_\mu)$. Per Konstruktion ist $F_+$ eine Potenzreihe. Zunächst sei $\mu \in [\rho, \varepsilon]$ beliebig. Wegen Lemma 9.9 ist $P$ $\mu$-dominant. Wir können also den 1. Divisionssatz 9.10 anwenden und erhalten

$$F_+ = PG_+ + Q_+$$

mit einer Potenzreihe $G_+$ in $\mathcal{A}_{[\mu,\mu]}(K)$ und einem Polynom $Q_+$ vom Grade $< d$; dabei gilt

$$\|F_+\|_\mu = \max(\|Q_+\|_\mu, \|P\|_\mu \cdot \|G_+\|_\mu) \ .$$

Als Potenzreihe muß $G_+$ sogar in $\mathcal{A}_{[\delta,\mu]}(K)$ liegen. Aus der Eindeutigkeitsaussage im 1. Divisionssatz folgt dann, daß $G_+$ und $Q_+$ nicht von $\mu$ abhängen. Insbesondere liegt $G_+$ in $\mathcal{A}_{[\delta,\varepsilon]}(K)$ mit

$$\|F_+\|_\rho = \max(\|Q_+\|_\rho, \|P\|_\rho \cdot \|G_+\|_\rho) \ .$$

Nun betrachten wir die Potenzreihe $F_-^*(T) := T^{d-1}F_-(T^{-1})$ in $\mathcal{A}_{[\varepsilon^{-1},\delta^{-1}]}(K)$ und das Polynom $P^*(T) := T^dP(T^{-1})$. Da die Nullstellen von $P^*$ genau die Inversen der Nullstellen von $P$ sind (aus der $\rho$-Extremalität von $P$ folgt $P(0) \neq 0$ und $P^*(0) \neq 0$), ist $P^*$ $\mu$-dominant für jedes $\mu \in [\rho^{-1}, \delta^{-1}]$ nach Lemma 9.9. Ganz analog wie eben erhalten wir also aus dem 1. Divisionssatz

$$F_-^* = P^*G_-^* + Q_-^*$$

mit einer Potenzreihe $G_-^*$ in $\mathcal{A}_{[\varepsilon^{-1},\delta^{-1}]}(K)$ und einem Polynom $Q_-^*$ vom Grade $< d$; zudem gilt

$$\begin{aligned}\rho^{1-d} \cdot \|F_-\|_\rho = \|F_-^*\|_{\rho^{-1}} &= \max(\|Q_-^*\|_{\rho^{-1}}, \|P^*\|_{\rho^{-1}} \cdot \|G_-^*\|_{\rho^{-1}}) \\ &= \max(\|Q_-^*\|_{\rho^{-1}}, \rho^{-d} \cdot \|P\|_\rho \cdot \|G_-^*\|_{\rho^{-1}}) \ .\end{aligned}$$

Sicherlich ist $Q_-(T) := T^{d-1}Q_-^*(T^{-1})$ ein Polynom vom Grade $< d$ mit $\|Q_-\|_\rho = \rho^{d-1} \cdot \|Q_-^*\|_{\rho^{-1}}$ und $G_-(T) := T^{-1}G_-^*(T^{-1}) \in \mathcal{A}_{[\delta,\varepsilon]}(K)$ mit $\|G_-\|_\rho = \rho^{-1} \cdot \|G_-^*\|_{\rho^{-1}}$. Also haben wir

$$\|F_-\|_\rho = \max(\|Q_-\|_\rho, \|P\|_\rho \cdot \|G_-\|_\rho)$$

und per Konstruktion

$$F_- = PG_- + Q_- \ .$$

Setzen wir schließlich $G := G_- + G_+$ und $Q := Q_- + Q_+$, so erhalten wir $F = PG + Q$ mit

$$\begin{aligned}\|F\|_\rho &= \max(\|F_+\|_\rho, \|F_-\|_\rho) \\ &= \max(\|Q_+\|_\rho, \|P\|_\rho \cdot \|G_+\|_\rho, \|Q_-\|_\rho, \|P\|_\rho \cdot \|G_-\|_\rho) \\ &\geq \max(\|Q\|_\rho, \|P\|_\rho \cdot \|G\|_\rho)\end{aligned}$$

und

$$\|F\|_\rho \leq \max(\|Q\|_\rho, \|PG\|_\rho) = \max(\|Q\|_\rho, \|P\|_\rho \cdot \|G\|_\rho) \ .$$

□

**Satz 9.12.** *Für $0 \neq F \in \mathcal{A}_{[\delta,\varepsilon]}(K)$ gilt:*

*i.* $F \in \mathcal{A}_{[\delta,\varepsilon]}(K)^\times \iff n(F,\delta) = N(F,\varepsilon)$*;*

*ii. es existiert ein Polynom* $P$ *vom Grade* $N(F,\varepsilon) - n(F,\delta)$ *und eine Einheit* $u \in \mathcal{A}_{[\delta,\varepsilon]}(K)^\times$*, so daß* $F = Pu$*; dabei gilt:*

*a.* $P$ *und* $u$ *sind bis auf Skalarfaktoren eindeutig bestimmt;*

*b. sämtliche Nullstellen* $x \in \bar{K}$ *von* $P$ *erfüllen* $\delta \leq |x| \leq \varepsilon$*.*

*Beweis.* i. Zuerst sei $F$ eine Einheit. Aus der Konvexität der Funktion $w_F$ folgt $n(F,\delta) \leq N(F,\varepsilon)$. Die Gleichheit ergibt sich dann unmittelbar mit Hilfe der Übungsaufgabe 9.7.

Umgekehrt sei nun $m := N(F,\varepsilon) = n(F,\delta)$. Wir schreiben $F = aT^m(1 - G)$ mit $a \in K^\times$ und $G(T) = \sum_{n\neq 0} b_n T^n \in \mathcal{A}_{[\delta,\varepsilon]}(K)$. Sicherlich ist $aT^m \in \mathcal{A}_{[\delta,\varepsilon]}(K)^\times$. Andererseits folgt aus der Voraussetzung und der Konvexität von $w_F$, daß $F$ keine kritischen Radien in $[\delta,\varepsilon]$ besitzt und deswegen gilt $\max(\|G\|_\delta, \|G\|_\varepsilon) < 1$. Das übliche Argument mit der geometrischen Reihe liefert dann das Inverse $\sum_{n\geq 0} G^n$ von $1 - G$ in $\mathcal{A}_{[\delta,\varepsilon]}(K)$.

ii. Wir führen den Beweis der Existenz mit Induktion nach $d := N(F,\varepsilon) - n(F,\delta)$. Der Induktionsanfang $d = 0$ wurde in i. gezeigt. Sei also $d > 0$. Weiter sei $\rho \in [\delta,\varepsilon]$ ein kritischer Radius für $F$ und

$$0 < h := N(F,\rho) - n(F,\rho) \leq d \ .$$

*Zwischenbehauptung:* $F = \bar{P}G$ *in* $\mathcal{A}_{[\delta,\varepsilon]}(K)$ *mit einem* $\rho$*-extremalen Polynom* $\bar{P}$ *vom Grade* $h$*.*

Durch Multiplikation mit $T^{-n(F,\rho)}$ können wir $n(F,\rho) = 0$ und $N(F,\rho) = h$ annehmen. Wir konstruieren nun induktiv eine bestimmte Folge von Polynomen $(P_m)_{m\in\mathbb{N}}$ mit

$$\deg(P_m) = h \quad \text{und} \quad \|F - P_m\|_\rho < \|F\|_\rho \ .$$

Wegen unseren Annahmen über $n(F,\rho)$ und $N(F,\rho)$ folgt aus diesen Bedingungen sofort:

$$P_m \text{ ist } \rho\text{-extremal mit } \|F\|_\rho = \|P_m\|_\rho \ .$$

Sei $F(T) = \sum_{n\in\mathbb{Z}} a_n T^n$. Wir setzen $P_1(T) := \sum_{n=0}^{h} a_n T^n$. Aus unseren Annahmen über $n(F,\rho)$ und $N(F,\rho)$ folgt $\deg(P_1) = h$ und $\|F - P_1\|_\rho < \|F\|_\rho$. Jetzt nehmen wir an, daß $P_1, \ldots, P_m$ schon wie gewünscht konstruiert seien. Durch Anwendung des 2. Divisionssatzes 9.11 erhalten wir

$$F = P_m G_m + Q_m$$

mit $G_m \in \mathcal{A}_{[\delta,\varepsilon]}(K)$ und einem Polynom $Q_m$ vom Grade $< h$. Also hat

$$P_{m+1} := P_m + Q_m$$

ebenfalls den Grad $h$. Durch Anwendung der Eindeutigkeitsaussage im 2. Divisionssatz auf die Identität

$$F - P_m = P_m(G_m - 1) + Q_m$$

erhalten wir ferner

$$\|F - P_m\|_\rho = \max(\|Q_m\|_\rho, \|P_m\|_\rho \cdot \|G_m - 1\|_\rho) \ .$$

Also ist

$$\|F - P_{m+1}\|_\rho \leq \max(\|F - P_m\|_\rho, \|Q_m\|_\rho) = \|F - P_m\|_\rho < \|F\|_\rho \ .$$

Ferner ergibt sich

$$\|F - P_m\|_\rho \leq \|F - P_1\|_\rho$$

und

$$\|G_m - 1\|_\rho \cdot \|F\|_\rho = \|G_m - 1\|_\rho \cdot \|P_m\|_\rho \leq \|F - P_m\|_\rho \leq \|F - P_1\|_\rho < \|F\|_\rho,$$

also

$$\|G_m - 1\|_\rho \leq \frac{\|F - P_1\|_\rho}{\|F\|_\rho} < 1$$

für alle $m \in \mathbb{N}$. Ebenso können wir die Eindeutigkeitsaussage im 2. Divisionssatz auf die Identität

$$Q_m(G_{m+1} - 1) = P_m(G_m - G_{m+1}) - Q_{m+1}$$

anwenden und erhalten

$$\begin{aligned} \|Q_m\|_\rho \cdot \frac{\|F - P_1\|_\rho}{\|F\|_\rho} &\geq \|Q_m\|_\rho \cdot \|G_{m+1} - 1\|_\rho \\ &= \max(\|Q_{m+1}\|_\rho, \|P_m\|_\rho \cdot \|G_m - G_{m+1}\|_\rho) \\ &= \max(\|Q_{m+1}\|_\rho, \|F\|_\rho \cdot \|G_m - G_{m+1}\|_\rho) \ . \end{aligned}$$

Induktiv folgt daraus

$$\|Q_m\|_\rho \leq \|F - P_1\|_\rho \cdot \left(\frac{\|F - P_1\|_\rho}{\|F\|_\rho}\right)^{m-1}$$

und

$$\|G_m - G_{m+1}\|_\rho \leq \left(\frac{\|F - P_1\|_\rho}{\|F\|_\rho}\right)^{m+1}$$

für alle $m \in \mathbb{N}$. Ersteres besagt, daß $(Q_m)_{m\in\mathbb{N}}$ bzgl. $\| \ \|_\rho$ eine Nullfolge ist. Also konvergiert die Folge $(P_m)_{m\in\mathbb{N}}$ bzgl. $\| \ \|_\rho$ gegen ein $\rho$-extremales Polynom $\bar{P}$ vom Grade $h$. Letzteres bedeutet, daß die Folge $(G_m)_{m\in\mathbb{N}}$ in $\mathcal{A}_{[\rho,\rho]}(K)$ gegen eine Laurentreihe $G$ konvergiert. Aus den Relationen $F = P_m G_m + Q_m$ folgt im Limes die Relation

$$F = \bar{P}G$$

in $\mathcal{A}_{[\rho,\rho]}(K)$. Da $\bar{P}$ $\rho$-extremal ist, können wir die Eindeutigkeitsaussage im 2. Divisionssatz ein drittes Mal anwenden um zu sehen, daß $G$ in $\mathcal{A}_{[\delta,\varepsilon]}(K)$ liegen muß. Damit ist die Zwischenbehauptung bewiesen.

Unter Benutzung der Übungsaufgabe 9.7 haben wir

$$\begin{aligned} N(G,\varepsilon) - n(G,\delta) &= N(F,\varepsilon) - n(F,\delta) - (N(\bar{P},\varepsilon) - n(\bar{P},\delta)) \\ &= d - h < d \ . \end{aligned}$$

Also können wir die Induktionsannahme auf $G$ anwenden und erhalten so die Existenz von $P$ und $u$. Die Eigenschaft b. besitzt das Polynom $P$ per Konstruktion. Für die in a. behauptete Eindeutigkeit sei nun

$$F = Qv$$

eine weitere Zerlegung mit einem Polynom $Q$ vom Grade $\deg(Q) = \deg(P)$ und einer Einheit $v \in \mathcal{A}_{[\delta,\varepsilon]}(K)^\times$. Sei $L/K$ ein Zerfällungskörper für $PQ$. Da $\mathcal{A}_{[\delta,\varepsilon]}(L)$ ein Integritätsbereich ist, folgt aus der Identität $Puv^{-1} = Q$ in $\mathcal{A}_{[\delta,\varepsilon]}(K) \subseteq \mathcal{A}_{[\delta,\varepsilon]}(L)$, daß ein $x \in \bar{K}$ mit $\delta \leq |x| \leq \varepsilon$ mit der gleichen Multiplizität als Nullstelle von $P$ wie von $Q$ auftritt. Wegen b. ist $P$ also ein Teiler von $Q$ in $K[T]$. Die Gradgleichheit impliziert schließlich $Q = aP$ für ein $a \in K^\times$ und folglich ($\mathcal{A}_{[\delta,\varepsilon]}(K)$ ist ein Integritätsbereich) $v = a^{-1}u$. □

**Corollar 9.13.** *$\mathcal{A}_{[\delta,\varepsilon]}(K)$ ist ein Hauptidealring.*

*Beweis.* Wegen Satz 9.12.ii. gilt für jedes Ideal $J \subseteq \mathcal{A}_{[\delta,\varepsilon]}(K)$, daß

$$J = \mathcal{A}_{[\delta,\varepsilon]}(K)(J \cap K[T]) \ .$$

Aber $J \cap K[T] = K[T]P$ ist ein Hauptidealring in $K[T]$. □

**Bemerkung 9.14.** *Aus dem Satz 9.12.ii. folgt auch, daß jedes $0 \neq F \in \mathcal{A}_{[\delta,\varepsilon]}(K)$ höchstens endlich viele Nullstellen in $\bar{K}$ besitzt.*

**Übungsaufgabe 9.15.** *Durch*

$$\begin{aligned}\|F\|_{\delta,\varepsilon} &:= \max\{\|F\|_\rho : \delta \le \rho \le \varepsilon\} \\ &= \max(\|F\|_\delta, \|F\|_\varepsilon) \\ &= \max(\max_{n<0} |a_n|\delta^n, \max_{n\ge 0} |a_n|\varepsilon^n)\end{aligned}$$

*wird auf* $\mathcal{A}_{[\delta,\varepsilon]}(K)$ *eine Vektorraumnorm definiert; dabei gilt:*

a. $\mathcal{A}_{[\delta,\varepsilon]}(K)$ *ist vollständig (also ein Banachraum) bzgl.* $\| \ \|_{\delta,\varepsilon}$*;*

b. $\|FG\|_{\delta,\varepsilon} \le \|F\|_{\delta,\varepsilon} \cdot \|G\|_{\delta,\varepsilon}$ *für alle* $F, G \in \mathcal{A}_{[\delta,\varepsilon]}(K)$*;*

c. *die Laurentpolynome bilden einen bzgl.* $\| \ \|_{\delta,\varepsilon}$ *dichten Unterraum in* $\mathcal{A}_{[\delta,\varepsilon]}(K)$*.*

Als nächstes setzen wir $0 < \delta < \varepsilon$ voraus und studieren den Ring

$$\mathcal{A}_{[\delta,\varepsilon)}(K) := \bigcap_{\delta\le\rho<\varepsilon} \mathcal{A}_{[\rho,\rho]}(K) = \bigcap_{\delta\le\varepsilon'<\varepsilon} \mathcal{A}_{[\delta,\varepsilon']}(K) \ .$$

Einerseits ist dies natürlich ebenfalls ein Integritätsbereich. Andererseits trägt er auch eine natürliche Vektorraumtopologie, nämlich die gröbste Vektorraumtopologie, bzgl. welcher aller Normen $F \longmapsto \|F\|_\rho$ für $\rho \in [\delta, \varepsilon)$ stetig sind. Eine Folge $(F_i)_{i\in\mathbb{N}}$ in $\mathcal{A}_{[\delta,\varepsilon)}(K)$ konvergiert gegen ein $F \in \mathcal{A}_{[\delta,\varepsilon)}(K)$ genau dann, wenn $\lim_{i\to\infty} \|F - F_i\|_\rho = 0$ gilt für alle $\rho \in [\delta, \varepsilon)$. Aus der Übungsaufgabe 9.15.a. folgt, daß $\mathcal{A}_{[\delta,\varepsilon)}(K)$ ebenfalls vollständig (also ein *Fréchetraum*) ist. Allerdings läßt sich diese Topologie nicht durch eine einzelne Vektorraumnorm beschreiben.

**Bemerkung 9.16.** *i. In* $\mathcal{A}_{[\delta,\varepsilon)}(K)$ *ist jedes Hauptideal* $F\mathcal{A}_{[\delta,\varepsilon)}(K)$ *abgeschlossen;*

*ii. in* $\mathcal{A}_{[\delta,\varepsilon]}(K)$ *ist jedes Ideal abgeschlossen.*

*Beweis.* i. Wir können sicherlich $F \neq 0$ annehmen. Sei $\tilde{G} = \lim_{i\to\infty} FG_i$ in $\mathcal{A}_{[\delta,\varepsilon)}(K)$. Dann gilt $\lim_{i\to\infty} \|FG_i - FG_{i+1}\|_\rho = 0$ für alle $\rho \in [\delta, \varepsilon)$. Die Multiplikativität von $\| \ \|_\rho$ impliziert $\lim_{i\to\infty} \|G_i - G_{i+1}\|_\rho = 0$. Also ist $(G_i)_i$ eine Cauchyfolge und konvergiert wegen der Vollständigkeit von $\mathcal{A}_{[\delta,\varepsilon)}(K)$ gegen ein $G \in \mathcal{A}_{[\delta,\varepsilon)}(K)$. Es folgt $\tilde{G} = \lim_{i\to\infty} FG_i = F \cdot \lim_{i\to\infty} G_i = FG \in F\mathcal{A}_{[\delta,\varepsilon)}(K)$.

ii. Wegen Corollar 9.13 läßt sich obiges Argument jetzt für jedes Ideal durchführen. □

Aus beweistechnischen Gründen ist es zweckmäßig, eine Folge $(\varepsilon_j)_{j\in\mathbb{N}}$ mit $\delta < \varepsilon_1 < \ldots < \varepsilon_j < \ldots < \varepsilon$ und $\lim_{j\to\infty} \varepsilon_j = \varepsilon$ zu wählen. Dann gilt

$$\ldots \subseteq \mathcal{A}_{[\delta,\varepsilon_j]}(K) \subseteq \ldots \subseteq \mathcal{A}_{[\delta,\varepsilon 1]}(K) \quad \text{und} \quad \mathcal{A}_{[\delta,\varepsilon)}(K) = \bigcap_{j\in\mathbb{N}} \mathcal{A}_{[\delta,\varepsilon_j]}(K) \ .$$

Die Topologie auf $\mathcal{A}_{[\delta,\varepsilon)}(K)$ wird durch die abzählbar vielen Normen $\| \ \|_\delta$ und $\| \ \|_{\varepsilon_j}$ für $j \geq 1$ definiert.

**Lemma 9.17.** *Ein $0 \neq F(T) = \sum_{n\in\mathbb{Z}} a_n T^n \in \mathcal{A}_{[\delta,\varepsilon)}(K)$ ist eine Einheit genau dann, wenn ein $n_0 \in \mathbb{Z}$ existiert mit*

$$|a_n|\delta^n < |a_{n_0}|\delta^{n_0} \quad \textit{und} \quad |a_n|\varepsilon^n \leq |a_{n_0}|\varepsilon^{n_0} \quad \textit{für alle} \quad n \neq n_0 \ .$$

*Beweis.* Offensichtlich ist $F$ eine Einheit in $\mathcal{A}_{[\delta,\varepsilon)}(K)$ genau dann, wenn es eine Einheit in allen $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ ist. Wegen Satz 9.12.i. ist Letzteres gleichbedeutend mit der Existenz eines $n_0 \in \mathbb{Z}$, so daß gilt

$$|a_n|\rho^n < |a_{n_0}|\rho^{n_0} \qquad \text{für alle } n \neq n_0 \text{ und alle } \rho \in [\delta, \varepsilon) \ .$$

Es ist schließlich leicht zu sehen, daß diese Ungleichungen äquivalent zu den behaupteten sind. □

**Satz 9.18.** *Jedes abgeschlossene Ideal $J \subseteq \mathcal{A}_{[\delta,\varepsilon)}(K)$ ist ein Hauptideal $J = F\mathcal{A}_{[\delta,\varepsilon)}(K)$ erzeugt von einer Potenzreihe $F$.*

*Beweis.* Es bezeichne $J_j$ das von $J$ in $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ erzeugte Ideal. Also

$$J \subseteq \ldots \subseteq J_{j+1} \subseteq J_j \subseteq \ldots \subseteq J_1 \ .$$

*1. Schritt:* Es gilt $J = \bigcap_{j\in\mathbb{N}} J_j$. Wegen der Abgeschlossenheit von $J$ genügt es zu zeigen, daß $J$ dicht in $\bigcap_j J_j$ ist. Zunächst folgt aus der Übungsaufgabe 9.15.c., daß $J$ dicht ist in jedem $J_j$: Ein beliebiges Element in $J_j$ schreibt sich nämlich als $F_1G_1 + \ldots + F_mG_m$ mit $F_i \in J$ und $G_i \in \mathcal{A}_{[\delta,\varepsilon_j]}(K)$. Sei $G_i = \lim_{n\to\infty} G_{i,n}$ mit $G_{i,n} \in \mathcal{A}_{[\delta,\varepsilon)}(K)$. Dann gilt $H_n := F_1G_{1,n} + \ldots + F_mG_{m,n} \in J$ und $F_1G_1 + \ldots + F_mG_m = \lim_{n\to\infty} H_n$. Ist nun $H \in \bigcap_j J_j$ ein beliebiges Element, so finden wir, wie eben gezeigt, zu jedem $j \geq 1$ ein $H_j \in J$ mit $\|H - H_j\|_{\delta,\varepsilon_j} < \frac{1}{j}$. Dann gilt

$$\|H - H_{j'}\|_{\delta,\varepsilon_j} \leq \|H - H_{j'}\|_{\delta,\varepsilon_{j'}} < \frac{1}{j'} \leq \frac{1}{j} \qquad \text{für alle } j' \geq j \ .$$

Das bedeutet $H = \lim_{j\to\infty} H_j$ in $\mathcal{A}_{[\delta,\varepsilon)}(K)$.

*2. Schritt:* Wir können natürlich $J \neq \{0\}$ annehmen. Wegen Corollar 9.13 und Satz 9.12.ii. gilt dann für alle $j \geq 1$, daß

$$J_j = P_j \mathcal{A}_{[\delta,\varepsilon_j]}(K)$$

mit einem Polynom $P_j \in K[T]$, dessen sämtliche Nullstellen $x \in \bar{K}$ die Bedingung $\delta \leq |x| \leq \varepsilon_j$ erfüllen. Wir können ferner $P_j(0) = 1$ voraussetzen. Wegen $P_{j+1}\mathcal{A}_{[\delta,\varepsilon_j]}(K) = P_j \mathcal{A}_{[\delta,\varepsilon_j]}(K)$ zeigt das Argument für die Eindeutigkeit im Beweis von Satz 9.12.ii., daß $P_j$ in $K[T]$ ein Teiler von $P_{j+1}$ ist. Sämtliche Nullstellen $x \in \bar{K}$ des Polynoms $Q_j := \frac{P_{j+1}}{P_j}$ erfüllen $\varepsilon_j < |x| \leq \varepsilon_{j+1}$. Außerdem ist $Q_j(0) = 1$. Eine besonders einfache Situation liegt vor, falls ein $j_0 \in \mathbb{N}$ existiert mit $Q_j = 1$ für alle $j \geq j_0$. Dann ist $P_{j_0} = P_{j_0+1} = P_{j_0+2} = \ldots$ und damit

$$\begin{aligned} J &= \bigcap_{j\in\mathbb{N}} J_j = \bigcap_{j\geq j_0} J_j = \bigcap_{j\geq j_0} P_{j_0}\mathcal{A}_{[\delta,\varepsilon_j]}(K) \\ &= P_{j_0} \cdot \bigcap_{j\geq j_0} \mathcal{A}_{[\delta,\varepsilon_j]}(K) = P_{j_0}\mathcal{A}_{[\delta,\varepsilon]}(K) \ . \end{aligned}$$

Dabei wird in der vierten Identität benutzt, daß alle $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ Integritätsbereiche sind. Im Folgenden werden wir deswegen annehmen, daß $\deg(Q_j) > 0$ für unendlich viele $j \in \mathbb{N}$ gilt. In der Tat können wir dann durch Übergang zu einer Teilfolge von $(\varepsilon_j)_j$ sogar voraussetzen, daß $\deg(Q_j) > 0$ für alle $j \in \mathbb{N}$ gilt. Ziel dieses Schrittes ist es, die $P_j$ zu Polynomen $P_j^*$ mit noch "besseren" Eigenschaften abzuändern.

*Zwischenbehauptung 1: Seien $Q \in K[T]$ mit $Q(0) = 1$ und $\nu > 0$, so daß sämtliche Nullstellen $x \in \bar{K}$ von $Q$ die Bedingung $|x| > \nu$ erfüllen; dann gilt $\|Q\|_\nu = 1$ und $Q \in \mathcal{A}_{[\mu,\nu]}(K)^\times$ für alle $0 < \mu \leq \nu$.*

Daß $Q$ eine Einheit in $\mathcal{A}_{[\mu,\nu]}(K)$ sein muß, ergibt sich durch Anwendung von Satz 9.12.ii. Ist $Q(T) = c_0 + c_1 T + \ldots$, so folgt dann auch Satz 9.12.i. die Existenz eines $n_0 \geq 0$ mit

$$|c_n|\rho^n < |c_{n_0}|\rho^{n_0} \quad \text{für alle} \quad 0 < \rho \leq \nu \ .$$

Wäre $n_0 > 0$, so würden wir aber den Widerspruch $1 < |c_{n_0}|\rho^{n_0}$, also $|c_{n_0}| > \rho^{-n_0}$ für alle $0 < \rho \leq \nu$ erhalten. Damit ist die Zwischenbehauptung gezeigt.

Wir erhalten also

$$Q_j \in \mathcal{A}_{[\mu,\varepsilon_j]}(K)^\times \qquad \text{für alle } 0 < \mu \leq \varepsilon_j \ .$$

Wegen $Q_j(0) = 1$ muß außerdem $Q_j^{-1}(T) = \sum_{n\geq 0} a_{n,j} T^n$ eine Potenzreihe sein mit $a_{0,j} = 1$. Da $Q_j$ eine Nullstelle $x \in \bar{K}$ mit $0 < |x| < \varepsilon$ besitzt, kann

$Q_j^{-1}$ aber nicht $|x|$-konvergent sein. Somit existiert

$$n(j) := \min\{n \in \mathbb{N} : |a_{n,j}|\varepsilon^n > 1\}$$

(denn sonst wäre $|a_{n,j}||x|^n = |a_{n,j}|\varepsilon^n \cdot \left(\frac{|x|}{\varepsilon}\right)^n \leq \left(\frac{|x|}{\varepsilon}\right)^n$ eine Nullfolge). Also

$$|a_{n,j}|\varepsilon^n \leq 1 \quad \text{für alle} \quad 0 \leq n < n(j) \ .$$

Wir setzen

$$\bar{Q}_j(T) := \sum_{n=0}^{n(j)-1} a_{n,j}T^n \in K[T] \ .$$

Aus Lemma 9.17 folgt $\bar{Q}_j \in \mathcal{A}_{[\mu,\varepsilon)}(K)^\times$. Wir definieren

$$Q_j^* := Q_j\bar{Q}_j \in K[T] \cap \mathcal{A}_{[\mu,\varepsilon_j]}(K)^\times \ .$$

*Zwischenbehauptung 2:* $\|Q_j^* - 1\|_\rho \leq \left(\frac{\rho}{\varepsilon_j}\right)^{n(j)}$ *für alle* $0 < \rho \leq \varepsilon_j$.
Zunächst stellen wir fest, daß wegen

$$Q_j^* - 1 = Q_j\bar{Q}_j - 1 = Q_j(\bar{Q}_j - Q_j^{-1})$$

das Polynom $Q_j^*$ von der Form

$$Q_j^*(T) = 1 + b_{n(j),j}T^{n(j)} + b_{n(j)+1,j}T^{n(j)+1} + \ldots$$

ist. Andererseits ist $Q_j^*(0) = 1$ und $Q_j^* \in \mathcal{A}_{[\mu,\varepsilon_j]}(K)^\times$ für alle $0 < \mu \leq \varepsilon_j$. Die Zwischenbehauptung 1 impliziert deswegen $|b_{n,j}|\varepsilon_j^n \leq 1$ für alle $n \geq 0$. Somit folgt

$$\begin{aligned}\|Q_j^* - 1\|_\rho &= \max_{n \geq n(j)} |b_{n,j}|\rho^n = \max_{n \geq n(j)} |b_{n,j}|\varepsilon_j^n \cdot \left(\frac{\rho}{\varepsilon_j}\right)^n \\ &\leq \max_{n \geq n(j)} \left(\frac{\rho}{\varepsilon_j}\right)^n = \left(\frac{\rho}{\varepsilon_j}\right)^{n(j)}\end{aligned}$$

für alle $0 < \rho \leq \varepsilon_j$.

*Zwischenbehauptung 3: Die Folge* $(n(j))_{j\in\mathbb{N}}$ *geht gegen* $\infty$.
Mit Hilfe der Zwischenbehauptung 1 folgt

$$|a_{n,j}|\varepsilon_j^n \leq \|Q_j^{-1}\|_{\varepsilon_j} = \|Q_j\|_{\varepsilon_j}^{-1} = 1$$

für alle $n \geq 0$ und $j \geq 1$. Das ist gleichbedeutend mit

$$v(a_{n,j}) - n\log\varepsilon_j \geq 0 \quad \text{bzw.} \quad v(a_{n,j}) \geq n\log\varepsilon_j \ .$$

Sei nun ein beliebiges $N \in \mathbb{N}$ vorgegeben. Sei

$$d_n := \text{ größte ganze Zahl } < n \log \varepsilon \ .$$

Dann existiert ein $j_0 \geq 1$ mit

$$d_n < n \log \varepsilon_j < n \log \varepsilon \qquad \text{für alle } j \geq j_0 \text{ und } 0 < n < N \ .$$

Wegen $v(a_{n,j}) \in \mathbb{Z}$ folgt aus $v(a_{n,j}) \geq n \log \varepsilon_j$ dann aber

$$v(a_{n,j}) \geq n \log \varepsilon \qquad \text{für alle } j \geq j_0 \text{ und } 0 \leq n < N \ .$$

Letztere Ungleichung ist äquivalent zu $|a_{n,j}|\varepsilon^n \leq 1$. Also erhalten wir

$$n(j) \geq N \quad \text{für alle} \quad j \geq j_0 \ .$$

Damit sind die Zwischenbehauptungen 2 und 3 gezeigt.

Wir definieren nun die Polynome

$$P_j^* := P_1 Q_1^* \cdot \ldots \cdot Q_{j-1}^* \ .$$

Wegen $\bar{Q}_j \in \mathcal{A}_{[\delta,\varepsilon)}(K)^\times$ gilt

$$P_j^* \mathcal{A}_{[\delta,\varepsilon)}(K) = P_1 Q_1 \cdot \ldots \cdot Q_{j-1} \mathcal{A}_{[\delta,\varepsilon)}(K) = P_j \mathcal{A}_{[\delta,\varepsilon)}(K) \ .$$

Wir haben also neue Polynome $P_j^*$ mit

$$J_j = P_j^* \mathcal{A}_{[\delta,\varepsilon_j]}(K)$$

für alle $j \geq 1$ konstruiert.

*3. Schritt:* Die Folge $(P_j^*)_{j\in\mathbb{N}}$ konvergiert in $\mathcal{A}_{[\delta,\varepsilon)}(K)$ gegen eine Potenzreihe $F$. Seien also $\rho \in [\delta, \varepsilon)$ und $C > 0$ vorgegeben. Wähle $j_0 = j_0(\rho)$ mit $\rho < \varepsilon_{j_0}$. Die Zwischenbehauptung 2 impliziert dann $\|Q_j^* - 1\|_\rho < 1$ und damit $\|Q_j^*\|_\rho = 1$ für alle $j \geq j_0$. Auf Grund der Zwischenbehauptungen 2 und 3 zusammen finden wir außerdem ein $j_1 \geq j_0$, so daß

$$\|Q_j^* - 1\|_\rho < \frac{C}{\|P_{j_0}^*\|_\rho} \qquad \text{für alle } j \geq j_1 \ .$$

Es folgt

$$\|P_{j+1}^* - P_j^*\|_\rho = \|Q_j^* - 1\|_\rho \cdot \|Q_{j-1}^*\|_\rho \cdot \ldots \cdot \|Q_{j_0}^*\|_\rho \cdot \|P_{j_0}^*\|_\rho < C$$

für alle $j \geq j_1$. Somit ist $(P_j^*)_{j\in\mathbb{N}}$ eine Cauchyfolge in $\mathcal{A}_{[\delta,\varepsilon)}(K)$, welche wegen der Vollständigkeit konvergent ist gegen ein $F$ mit $\|F\|_\rho = \|P_{j_0(\rho)}^*\|_\rho \neq 0$.

Ebenso konvergiert für jedes $j \geq 1$ die Folge $(Q_j^* Q_{j+1}^* \dots Q_{j+i}^*)_{i \geq 0}$ gegen ein $0 \neq F_j \in \mathcal{A}_{[\delta,\varepsilon)}(K)$, und es gilt

$$F = P_j^* F_j \ .$$

Alle $Q_{j+i}^*$ für $i \geq 0$ sind Einheiten in $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$. Aus der Multiplikativität der $\| \ \|_\rho$ folgt, daß der Limes einer Folge von Einheiten entweder $= 0$ oder ebenfalls eine Einheit ist. Also gilt $F_j \in \mathcal{A}_{[\delta,\varepsilon_j]}(K)^\times$ und damit

$$F\mathcal{A}_{[\delta,\varepsilon_j]}(K) = P_j^* \mathcal{A}_{[\delta,\varepsilon_j]}(K) = J_j \ .$$

Wir erhalten schließlich

$$J = \bigcap_j J_j = \bigcap_j F\mathcal{A}_{[\delta,\varepsilon_j]}(K) = F \cdot \bigcap_j \mathcal{A}_{[\delta,\varepsilon_j]}(K) = F\mathcal{A}_{[\delta,\varepsilon)}(K) \ .$$

□

**Lemma 9.19.** *Sei $F \in \mathcal{A}_{[\delta,\varepsilon)}(K)$, und seien $G_j \in \mathcal{A}_{[\delta,\varepsilon_j]}(K)$ mit*

$$G_{j+1} - G_j \in F\mathcal{A}_{[\delta,\varepsilon_j]}(K) \qquad \textit{für alle } j \geq 1;$$

*dann existiert ein $G \in \mathcal{A}_{[\delta,\varepsilon)}(K)$ mit*

$$G - G_j \in F\mathcal{A}_{[\delta,\varepsilon_j]}(K) \qquad \textit{für alle } j \geq 1 \ .$$

*Beweis.* Die Annahme besagt

$$G_{j+1} + F\mathcal{A}_{[\delta,\varepsilon_{j+1}]}(K) \subseteq G_j + F\mathcal{A}_{[\delta,\varepsilon_j]}(K)$$

für alle $j \geq 1$. Auf Grund der Übungsaufgabe 9.15 und der Bemerkung 9.16.ii. ist jedes $G_j + F\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ ein vollständiger metrischer Raum (bzgl. der von $\| \ \|_{\delta,\varepsilon_j}$ induzierten Metrik), und obige Inklusionen sind stetig mit dichtem Bild. In dieser Situation sagt der *Satz von Mittag-Leffler* aus der allgemeinen Topologie, daß der Durchschnitt $\bigcap_{j \in \mathbb{N}} G_j + F\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ nicht leer ist. Jedes $G$ aus diesem Durchschnitt erfüllt die Behauptung. □

**Satz 9.20.** *Jedes endlich-erzeugte Ideal $J \subseteq \mathcal{A}_{[\delta,\varepsilon)}(K)$ ist ein Hauptideal.*

*Beweis.* Per Induktion können wir annehmen, daß $J = < F, G >$ von zwei Elementen $F, G \neq 0$ erzeugt wird. Nach Satz 9.18 ist der Abschluß von $J$ ein Hauptideal $< H >$. Es genügt zu zeigen, daß $H \in J$. Zunächst gilt jedenfalls $F = HF_0$ und $G = HG_0$ mit $F_0, G_0 \in \mathcal{A}_{[\delta,\varepsilon)}(K)$. Das von $F$ und

$G$ in $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ erzeugte Ideal ist nach Bemerkung 9.16.ii. abgeschlossen in $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$. Für jedes $j \geq 1$ können wir also schreiben

$$H = A_j F + B_j G \quad \text{mit} \quad A_j, B_j \in \mathcal{A}_{[\delta,\varepsilon_j]}(K) \ .$$

In dem Integritätsbereich $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ gilt dann

$$A_{j+1}F_0 + B_{j+1}G_0 = 1 = A_j F_0 + B_j G_0 \ ,$$

also

$$(B_{j+1} - B_j)G_0 = (A_j - A_{j+1})F_0$$

und damit

$$\begin{aligned} B_{j+1} - B_j &= (B_{j+1} - B_j)A_j F_0 + (B_{j+1} - B_j)B_j G_0 \\ &= (B_{j+1} - B_j)A_j F_0 + (A_j - A_{j+1})B_j F_0 \\ &\in F_0 \mathcal{A}_{[\delta,\varepsilon_j]}(K) \ . \end{aligned}$$

Gemäß Lemma 9.19 finden wir ein $B \in \mathcal{A}_{[\delta,\varepsilon)}(K)$ mit

$$B - B_j = C_j F_0 \quad \text{und} \quad C_j \in \mathcal{A}_{[\delta,\varepsilon_j]}(K)$$

für alle $j \geq 1$. Es folgt

$$\begin{aligned} BG - H &= H(BG_0 - 1) = H((B - B_j)G_0 - A_j F_0) \\ &= H(C_j G_0 - A_j)F_0 = (C_j G_0 - A_j)F \end{aligned}$$

für alle $j \geq 1$. Da die $\mathcal{A}_{[\delta,\varepsilon_j]}(K)$ Integritätsbereiche sind, hängt $D := C_j G_0 - A_j$ nicht von $j$ ab und liegt in $\mathcal{A}_{[\delta,\varepsilon)}(K)$. Wir erhalten schließlich

$$H = -DF + BG \in < F, G > = J \ .$$

□

Integritätsbereiche, in denen jedes endlich-erzeugte Ideal ein Hauptideal ist, nennt man *Bezoutringe*.

Für jedes $0 \neq F(T) = \sum_{n\in\mathbb{Z}} a_n T^n \in \mathcal{A}_{[\delta,\varepsilon)}(K)$ haben wir die stückweise lineare, stetige, konvexe Funktion

$$\begin{aligned} w_F : [\log\delta, \log\varepsilon) &\longrightarrow \mathbb{R} \\ t &\longmapsto \max_{n\in\mathbb{Z}}(nt - v(a_n)) \end{aligned}$$

(deren Einschränkung auf jedes $[\log\delta, \log\varepsilon'] \subseteq [\log\delta, \log\varepsilon)$ mit der zuvor betrachteten Funktion $w_F$ zu $F \in \mathcal{A}_{[\delta,\varepsilon']}(K)$ übereinstimmt).

Im Folgenden interessieren wir uns besonders für den Fall $\varepsilon = 1$.

**Lemma 9.21.** *Für* $0 \neq F(T) = \sum_{n\in\mathbb{Z}} a_n T^n \in \mathcal{A}_{[\delta,1)}(K)$ *sind äquivalent:*

*i. Die Funktion* $\rho \longmapsto \|F\|_\rho$ *auf* $[\delta, 1)$ *ist (nach oben) beschränkt;*

*ii. die Funktion* $w_F$ *auf* $[\log\delta, 0)$ *ist (nach oben) beschränkt;*

*iii.* $\lim_{\rho\to 1} \|F\|_\rho < \infty$ *bzw.* $\lim_{t\to 0} w_F(t) < \infty$ *existiert;*

*iv.* $w_F$ *besitzt nur endlich viele Steigungen;*

*v. es existiert ein* $C > 0$ *mit* $|a_n| \leq C$ *für alle* $n \in \mathbb{Z}$.

*In diesem Falle gilt* $\|F\|_1 := \sup_{n\in\mathbb{Z}} |a_n| = \max_{n\in\mathbb{Z}} |a_n|$.

*Beweis.* Die Implikation iv. $\Longrightarrow$ iii. ist offensichtlich. Die Bedingung iii. bedeutet, daß sich $\rho \longmapsto \|F\|_\rho$ und $w_F$ zu stetigen Funktionen auf den abgeschlossenen Intervallen $[\delta, 1]$ bzw. $[\log\delta, 0]$ fortsetzen. Also gilt dann i. und ii. Die Äquivalenz i. $\Longleftrightarrow$ ii. ist wiederum offensichtlich. (Man beachte übrigens, daß $w_F$ als stückweise lineare und konvexe Funktion stets nach unten beschränkt ist.)

i. $\Longrightarrow$ v. Nach Annahme existiert ein $C > 0$ mit $\|F\|_{\varepsilon_j} \leq C$ für alle $j \geq 1$, d. h. $|a_n|\varepsilon_j^n \leq C$ für alle $n \in \mathbb{Z}$ und $j \geq 1$. Durch Limesübergang erhalten wir $|a_n| \leq C$ für alle $n \in \mathbb{Z}$.

v. $\Longrightarrow$ iv. Die Menge der Steigungen von $w_F$ ist die nach unten durch $N(F, \delta)$ beschränkte Menge der ganzen Zahlen $n(F, \rho) \leq N(F, \rho)$ für $\rho \in (\delta, 1)$. Es genügt also zu zeigen, daß die Menge der $N(F, \rho)$ nach oben beschränkt ist. Nach Annahme existiert ein $C > 0$ mit $v(a_n) \geq -\log C$ für alle $n \in \mathbb{Z}$. Da die $v(a_n)$ ganze Zahlen sind, folgt $\inf_{n\in\mathbb{Z}} v(a_n) = \min_{n\in\mathbb{Z}} v(a_n)$. Das beweist den Zusatz. Man beachte zusätzlich, daß wegen der $\delta$-Konvergenz von $F$ natürlich $\lim_{n\to-\infty} |a_n| = 0$ gilt. Sei nun $n_0 \in \mathbb{Z}$ minimal mit $|a_{n_0}| \geq |a_n|$ für alle $n \in \mathbb{Z}$. Für jedes $\rho \in [\delta, 1)$ und jedes $n > n_0$ haben wir dann

$$a_n = 0 \text{ oder } \frac{|a_n|}{|a_{n_0}|}\rho^{n-n_0} < \frac{|a_n|}{|a_{n_0}|} \leq 1, \text{ also stets } |a_n|\rho^n < |a_{n_0}|\rho^{n_0} \ .$$

Daraus folgt $N(F, \rho) \leq n_0$. □

Aus Lemma 9.21.v. folgt leicht, daß

$$\mathcal{A}^b_{[\delta,1)}(K) := \{F \in \mathcal{A}_{[\delta,1)}(K) : w_F \text{ hat nur endlich viele Steigungen}\}$$

ein Unterring von $\mathcal{A}_{[\delta,1)}(K)$ ist, welcher $\mathcal{A}_{[\delta,1]}(K)$ enthält.

**Bemerkung 9.22.** $\| \ \|_1$ *ist eine Vektorraumnorm auf* $\mathcal{A}^b_{[\delta,1)}(K)$ *mit*

$$\|FG\|_1 = \|F\|_1 \cdot \|G\|_1$$

*für alle* $F, G \in \mathcal{A}^b_{[\delta,1)}(K)$.

*Beweis.* Aus Lemma 9.21 folgt, daß $\| \ \|_1$ eine Vektorraumnorm ist, für welche

$$\|F\|_1 = \lim_{\rho \longrightarrow 1} \|F\|_\rho$$

gilt. Also ist die Multiplikativität von $\| \ \|_1$ eine Konsequenz der Multiplikativität der $\| \ \|_\rho$. □

**Lemma 9.23.** $\mathcal{A}^b_{[\delta,1)}(K)^\times = \mathcal{A}_{[\delta,1)}(K)^\times$.

*Beweis.* Dies folgt unmittelbar aus Lemma 9.17. □

**Satz 9.24.** $\mathcal{A}^b_{[\delta,1)}(K)$ *ist ein Hauptidealring, in dem jedes Ideal von einem Polynom erzeugt wird.*

*Beweis.* Als Unterring des Integritätsbereiches $\mathcal{A}_{[\delta,1)}(K)$ ist $\mathcal{A}^b_{[\delta,1)}(K)$ natürlich ebenfalls ein Integritätsbereich. Wir betrachten zunächst ein Hauptideal $J = < F >$ in $\mathcal{A}^b_{[\delta,1)}(K)$. Da $w_F$ nur endlich viele Steigungen hat, folgt aus Satz 9.12.ii., daß ein $j_0 \geq 1$ existiert, so daß $F$ keine Nullstellen $x \in \bar{K}$ mit $\varepsilon_{j_0} < |x| < 1$ besitzt. Mit dieser Information gehen wir in den 2. Schritt des Beweises von Satz 9.18 und sehen, daß wir in dem einfachen Fall sind, wo (mit den dortigen Bezeichnungen) $Q_j = 1$ für alle $j \geq j_0$ gilt. Es folgt

$$F\mathcal{A}_{[\delta,1)}(K) = P_{j_0}\mathcal{A}_{[\delta,1)}(K)$$

und wegen Lemma 9.23 also

$$J = F\mathcal{A}^b_{[\delta,1)}(K) = P_{j_0}\mathcal{A}^b_{[\delta,1)}(K) \ .$$

Ein beliebiges Ideal $J \subseteq \mathcal{A}^b_{[\delta,1)}(K)$ erfüllt deswegen

$$J = (J \cap K[T])\mathcal{A}^b_{[\delta,1)}(K)$$

und muß also ein von einem Polynom erzeugtes Hauptideal sein. □

# 10 Der Robba-Ring

Für $0 < \delta' < \delta < 1$ ist

$$\mathcal{A}_{[\delta',1)}(K) \subseteq \mathcal{A}_{[\delta,1)}(K)$$

eine Inklusion von Integritätsbereichen. Deswegen ist

$$\mathcal{R}_K := \bigcup_{0<\delta<1} \mathcal{A}_{[\delta,1)}(K)$$

ebenfalls ein Integritätsbreich. Man nennt $\mathcal{R}_K$ den *Robba-Ring* (über $K$).

**Satz 10.1.** *$\mathcal{R}_K$ ist ein Bezoutring.*

*Beweis.* Sei $J \subseteq \mathcal{R}_K$ ein Ideal, daß von endlich vielen Elementen $F_1, \ldots, F_m$ erzeugt wird. Dann existiert ein $0 < \delta < 1$ mit $F_1, \ldots, F_m \in \mathcal{A}_{[\delta,1)}(K)$. Nach Satz 9.20 gilt

$$\sum_{i=1}^{m} F_i \mathcal{A}_{[\delta,1)}(K) = F\mathcal{A}_{[\delta,1)}(K)$$

und damit auch $J = < F >$. □

Analog bilden wir die Unterringe

$$\begin{aligned}\mathcal{R}_K^b &:= \bigcup_{0<\delta<1} \mathcal{A}_{[\delta,1)}^b(K) \\ &= \Big\{ \sum_{n\in\mathbb{Z}} a_n T^n \in \mathcal{R}_K : \{|a_n|\}_{n\in\mathbb{Z}} \text{ ist beschränkt} \Big\}\end{aligned}$$

und

$$\mathcal{R}_K^{\text{int}} := \Big\{ \sum_{n\in\mathbb{Z}} a_n T^n \in \mathcal{R}_K : |a_n| \leq 1 \text{ für alle } n \in \mathbb{Z} \Big\} .$$

Also

$$\mathcal{R}_K^{\text{int}} \subseteq \mathcal{R}_K^b \subseteq \mathcal{R}_K .$$

**Satz 10.2.** *$\mathcal{R}_K^b$ ist ein Körper.*

*Beweis.* Sei $0 \neq F(T) = \sum_{n\in\mathbb{Z}} a_n T^n \in \mathcal{R}_K^b$. Auf Grund von Lemma 9.21.iv. existiert ein $0 < \delta < 1$, so daß $F \in \mathcal{A}_{[\delta,1)}^b(K)$ mit $n_0 := n(F,\delta) = N(F,\rho)$ für alle $\delta \leq \rho < 1$. Also gilt $|a_n|\rho^n < |a_{n_0}|\rho^{n_0}$ für alle $n \neq n_0$ und alle $\delta \leq \rho < 1$. Durch Limesübergang folgt $|a_n| \leq |a_{n_0}|$ für alle $n \in \mathbb{Z}$. Nach Lemma 9.17 ist $F$ somit eine Einheit in $\mathcal{A}_{[\delta,1)}(K)$, wegen Lemma 9.23 also schon eine Einheit in $\mathcal{A}_{[\delta,1)}^b(K)$ und damit in $\mathcal{R}_K^b$. □

**Bemerkung 10.3.** $\mathcal{R}_K^\times = (\mathcal{R}_K^b)^\times$.

*Beweis.* Dies folgt aus Lemma 9.23. □

Offensichtlich existiert für jedes $F \in \mathcal{R}_K^b$ eine geeignete Potenz $\pi^m$, so daß $\pi^m F$ in $\mathcal{R}_K^{\text{int}}$ liegt. Insbesondere ist $\mathcal{R}_K^b$ der Quotientenkörper von $\mathcal{R}_K^{\text{int}}$. Aus Bemerkung 9.22 folgt, daß

$$\begin{aligned} \omega : \ \mathcal{R}_K^b \setminus \{0\} &\longrightarrow \mathbb{Z} \\ \sum_{n\in\mathbb{Z}} a_n T^n &\longmapsto \min_{n\in\mathbb{Z}} v(a_n) \end{aligned}$$

eine diskrete Bewertung ist, d. h. die Eigenschaften (I) - (III) aus Abschnitt 3 besitzt. Offensichtlich ist $\mathcal{R}_K^{\text{int}}$ der zugehörige diskrete Bewertungsring (vgl. Lemma 3.4). Jedes Primelement von $A$ ist auch ein Primelement für $\mathcal{R}_K^{\text{int}}$. Einerseits erfüllen alle Laurentreihen $\sum_{n\in\mathbb{Z}} a_n T^n$ in $\mathcal{R}_K$ die Bedingung $\lim_{n\to-\infty} v(a_n) = \infty$. Andererseits ist jede Laurentreihe der Form $\sum_{n\geq n_0} a_n T^n$ mit beschränkter Menge $\{|a_n|\}_{n\geq n_0}$ in $\mathcal{R}_K^b$ enthalten. Deswegen ist der Restklassenkörper von $\mathcal{R}_K^{\text{int}}$ gleich $k((T))$. Der diskrete Bewertungsring $\mathcal{R}_K^{\text{int}}$ ist nicht vollständig. Die Komplettierung von $\mathcal{R}_K^{\text{int}}$ bzw. $\mathcal{R}_K^b$ wird mit $\mathcal{E}_K^{\text{int}}$ bzw. $\mathcal{E}_K$ bezeichnet.

**Lemma 10.4.** *$\mathcal{E}_K$ ist der Körper aller Laurentreihen $\sum_{n\in\mathbb{Z}} a_n T^n$, deren Koeffizienten $a_n \in K$ eine beschränkte Menge bilden und $\lim_{n\to-\infty} v(a_n) = \infty$ erfüllen; die diskrete Bewertung $\omega$ von $\mathcal{E}_K$ ist gegeben durch*

$$\omega\Big(\sum_{n\in\mathbb{Z}} a_n T^n\Big) := \min_{n\in\mathbb{Z}} v(a_n) \ .$$

*Beweis.* Dis Existenz des Minimums in der Formel für $\omega$ folgt aus der Tatsache, daß die $v(a_n)$ ganze Zahlen sind. Offensichtlich bilden die in der Behauptung genannten Laurentreihen einen $K$-Vektorraum $\tilde{\mathcal{E}}_K$ der durch

$$\|F\|_1 := e^{-\omega(F)}$$

normiert ist. Es ist auch klar, daß $\tilde{\mathcal{E}}_K$ den Körper $\mathcal{R}_K^b$ enthält. Sei $F(T) = \sum_{n\in\mathbb{Z}} a_n T^n \in \tilde{\mathcal{E}}_K$ ein beliebiges Element. Die $F_i(T) := \sum_{n\geq -i} a_n T^n$ liegen für jedes $i \in \mathbb{N}$ in $\mathcal{R}_K^b$. Wegen

$$\lim_{i\to\infty} \|F - F\|_1 = \lim_{i\to\infty} \max_{n<-i} |a_n| = 0$$

liegt $\mathcal{R}_K^b$ also dicht in $\tilde{\mathcal{E}}_K$. Um $\mathcal{E}_K = \tilde{\mathcal{E}}_K$ zu beweisen, bleibt also nur noch zu zeigen, daß $\tilde{\mathcal{E}}_K$ bzgl. $\| \ \|_1$ vollständig ist. Sei $(G_i)_{i\in\mathbb{N}}$ mit $G_i(T) =$

$\sum_{n\in\mathbb{Z}} a_{n,i}\, T^n$ eine Cauchyfolge in $\tilde{\mathcal{E}}_K$. Dann ist $(a_{n,i})_{i\in\mathbb{N}}$ für jedes $n \in \mathbb{Z}$ eine Cauchyfolge in $K$, welche also gegen ein $a_n \in K$ konvergiert. Wir setzen $G(T) := \sum_{n\in\mathbb{Z}} a_n T^n$. Sei $C > 0$ vorgegeben. Es existiert ein $i_0 \in \mathbb{N}$ mit

$$\|G_{i+1} - G_i\|_1 \leq C \text{ und damit } \|G_j - G_i\|_1 \leq C \text{ für alle } j > i \geq i_0 \ .$$

Aus $\max_{n\in\mathbb{Z}} |a_{n,j} - a_{n,i}| \leq C$ für alle $j > i \geq i_0$ folgt durch Übergang zum Limes bzgl. $j \longrightarrow \infty$, daß auch

$$\sup_{n\in\mathbb{Z}} |a_n - a_{n,i}| \leq C \qquad \text{für alle } i \geq i_0 \tag{12}$$

gilt. Wegen $\lim_{n\to-\infty} |a_{n,i_0}| = 0$ existiert außerdem ein $n_0 \leq 0$ mit

$$|a_{n,i_0}| \leq C \qquad \text{für alle } n \leq n_0 \ . \tag{13}$$

Insbesondere impliziert (12), daß

$$|a_n| \leq \max(|a_n - a_{n,i_0}|, |a_{n,i_0}|) \leq \max(C, \|G_{i_0}\|_1) \qquad \text{für alle } n \in \mathbb{Z},$$

und (12) und (13) zusammen, daß

$$|a_n| \leq \max(|a_n - a_{n,i_0}|, |a_{n,i_0}|) \leq C \qquad \text{für alle } n \leq n_0 \ .$$

Ersteres bedeutet, daß die Koeffizienten $a_n$ eine beschränkte Menge in $K$ bilden, und Letzteres, daß $\lim_{n\to-\infty} |a_n| = 0$. Also liegt $G$ in $\tilde{\mathcal{E}}_K$. Wiederum aus (12) folgt nun, daß die Folge $(G_i)_{i\in\mathbb{N}}$ bzgl. $\| \ \|_1$ gegen $G$ konvergiert. □

Ein diskreter Bewertungsring, der die Behauptung des Henselschen Lemmas 4.1 erfüllt, wird *henselsch* genannt. In der kommutativen Algebra beweist man das folgende Resultat.

**Lemma 10.5.** *(Nagata)*
*Für einen diskreten Bewertungsring $B$ mit maximalem Ideal $\mathfrak{n}$ sind äquivalent:*

*i. $B$ ist henselsch;*

*ii. jedes normierte Polynom $T^d + b_{d-1}T^{d-1} + \ldots + b_1 T + b_0$ in $B[T]$ mit $b_0 \in \mathfrak{n}$ und $b_1 \notin \mathfrak{n}$ besitzt eine Nullstelle in $\mathfrak{n}$;*

*iii. jedes normierte Polynom $T^d + b_{d-1}T^{d-1} + \ldots + b_0$ in $B[T]$ mit $b_{d-1} \notin \mathfrak{n}$ und $b_{d-2}, \ldots, b_0 \in \mathfrak{n}$ besitzt eine Nullstelle in $-b_{d-1} + \mathfrak{n}$.*

**Satz 10.6.** *$\mathcal{R}_K^{\mathrm{int}}$ ist henselsch.*

*Beweis.* Wir wollen das Lemma 10.5 benutzen. Sei also $P(Z) = Z^d + b_{d-1}Z^{d-1} + \ldots + b_0$ ein Polynom in $\mathcal{R}_K^{\text{int}}[Z]$ mit $b_{d-1} \not\equiv 0 \bmod \pi$ und $b_{d-2} \equiv \ldots \equiv b_0 \equiv 0 \bmod \pi$. Wir haben zu zeigen, daß ein $x \in \mathcal{R}_K^{\text{int}}$ existiert mit $P(x) = 0$ und $x \equiv -b_{d-1} \bmod \pi$. Durch Übergang von $P(Z)$ zu dem Polynom $(-b_{d-1})^{-d}P(-b_{d-1}Z)$ können wir $b_{d-1} = -1$ annehmen. Auf Grund des Henselschen Lemmas 4.1 existiert jedenfalls genau ein $x \in \mathcal{E}_K^{\text{int}}$ mit $P(x) = 0$ und $x \equiv 1 \bmod \pi$. Um zu zeigen, daß $x$ schon in $\mathcal{R}_K^{\text{int}}$ liegt, verwenden wir das Newtonsche Approximationsverfahren. Zunächst halten wir fest, daß für jedes $y \in \mathcal{R}_K^{\text{int}}$ mit $y \equiv 1 \bmod \pi$ gilt

$$P'(y) \equiv dy^{d-1} - (d-1)y^{d-2} \equiv 1 \bmod \pi \ .$$

Durch die rekursive Definition

$$x_1 := 1 \quad \text{und} \quad x_{i+1} := x_i - \tfrac{P(x_i)}{P'(x_i)}$$

erhalten wir also eine Folge $(x_i)_{i\geq 1}$ in $1 + \pi\mathcal{R}_K^{\text{int}}$. Induktiv zeigen wir, daß

$$P(x_i) \equiv 0 \bmod \pi^i \quad \text{und} \quad x_{i+1} \equiv x_i \bmod \pi^i$$

gilt. Letzteres folgt unmittelbar aus Ersterem. Aus der binomischen Formel ergibt sich leicht

$$P(Z_0 + Z_1\pi^i) \equiv P(Z_0) + P'(Z_0)Z_1\pi^i \bmod \pi^{i+1} \ .$$

Insbesondere erhalten wir

$$\begin{aligned} P(x_{i+1}) &= P\big(x_i - \tfrac{P(x_i)}{P'(x_i)}\big) = P\big(x_i + \tfrac{-P(x_i)}{\pi^i P'(x_i)}\pi^i\big) \\ &\equiv P(x_i) - \tfrac{P(x_i)}{\pi^i}\pi^i \equiv 0 \bmod \pi^{i+1} \ . \end{aligned}$$

Also ist $(x_i)_{i\geq 1}$ eine Cauchyfolge, welche in $\mathcal{E}_K^{\text{int}}$ gegen $x$ konvergiert.

Nach Annahme gilt $\|b_j\|_1 \leq |\pi| < 1$ für $0 \leq j \leq d-2$. Wegen Lemma 9.21.iii. finden wir deswegen ein $0 < \delta_1 < 1$ mit $b_j \in \mathcal{A}^b_{[\delta_1,1)}(K)$ und $\|b_j\|_\rho < 1$ für alle $0 \leq j \leq d-2$ und alle $\rho \in [\delta_1, 1)$. Sämtliche Koeffizienten $b$ der Polynome $P(Z)$ und $P'(Z)$ erfüllen dann $b \in \mathcal{A}^b_{[\delta_1,1)}(K)$ mit $\|b\|_\rho \leq 1$ für alle $\rho \in [\delta_1, 1)$. Wir fixieren eine strikt aufsteigende Folge $\delta_1 < \ldots < \delta_i < \ldots < \delta < 1$ und zeigen induktiv, daß

$$x_i \in \mathcal{A}^b_{[\delta_i,1)}(K) \quad \text{mit} \quad \|x_i\|_\rho \leq 1 \quad \text{für alle} \quad \rho \in [\delta_i, 1)$$

gilt. Trivialerweise hat $x_1 = 1$ diese Eigenschaften. Aus der Induktionsannahme folgt

$$P(x_i), P'(x_i) \in \mathcal{A}^b_{[\delta_i,1)}(K) \text{ mit } \|P(x_i)\|_\rho, \|P'(x_i)\|_\rho \leq 1 \text{ für alle } \rho \in [\delta_i, 1) \ .$$

Andererseits impliziert die Kongruenz $P'(x_i) \equiv 1 \bmod \pi$ aber $\|P'(x_i)\|_\rho \geq 1$ für alle $\rho \in [\delta_i, 1)$. Es folgt $\|P'(x_i)\|_\rho = 1$ für alle $\rho \in [\delta_i, 1)$ was bedeutet, daß die Funktion $w_{P'(x_i)}$ auf $[\log \delta_i, 0)$ konstant gleich 0 ist. Mit Satz 9.12.i. und Lemma 9.23 erhalten wir $P'(x_i) \in \mathcal{A}_{[\delta_{i+1},1)}(K)^\times = \mathcal{A}^b_{[\delta_{i+1},1)}(K)^\times$. Mit $x_i$ liegt dann auch $x_{i+1}$ in $\mathcal{A}^b_{[\delta_{i+1},1)}(K)$ und erfüllt

$$\|x_{i+1}\|_\rho \leq \max(\|x_i\|_\rho, \frac{\|P(x_i)\|_\rho}{\|P'(x_i)\|_\rho}) \leq 1$$

für alle $\rho \in [\delta_{i+1}, 1)$. Insgesamt ist also $(x_i)_{i\geq 1}$ jedenfalls eine Folge in $\mathcal{A}^b_{[\delta,1)}(K)$ mit $\|x_i\|_\delta \leq 1$ für alle $i \geq 1$. Sei $x_i(T) = \sum_{n\in\mathbb{Z}} a_{n,i}T^n$ und $x(T) = \sum_{n\in\mathbb{Z}} a_n T^n$. Aus

$$1 \geq \|x_i\|_\delta \geq |a_{n,i}|\delta^n = |a_{n,i}|\rho^n \cdot \left(\tfrac{\delta}{\rho}\right)^n$$

folgt im Limes bzgl. $i$ die Ungleichung

$$|a_n|\rho^n \leq \left(\tfrac{\delta}{\rho}\right)^{-n}$$

und damit

$$\lim_{n\to-\infty} |a_n|\rho^n = 0 \qquad \text{für alle } \delta < \rho < 1 \ .$$

Andererseits folgt aus $|a_n| \leq 1$ natürlich $\lim_{n\to\infty} |a_n|\rho^n = 0$ für alle $0 < \rho < 1$. Für alle $\delta < \rho < 1$ ist $x$ also $\rho$-konvergent und liegt damit in $\mathcal{R}^{\mathrm{int}}_K$. □

**Satz 10.7.** *Sei $A = W(k)$ der Ring der Wittvektoren mit Koeffizienten in einem perfekten Körper $k$ der Charakteristik $p > 0$; dann ist $\mathcal{E}^{\mathrm{int}}_K$ isomorph zum Cohen-Unterring von $W(k((T)))$ zur Liftung $\{\tau(T)\}$ der $p$-Basis $\{T\}$ des Körpers $k((T))$.*

*Beweis.* Wir können den Beweis weitestgehend axiomatisch führen. Der vollständige diskrete Bewertungsring $B := \mathcal{E}^{\mathrm{int}}_K$ hat das maximale Ideal $pB$. Es bezeichne $\sigma_0 := F$ den Frobenius-Automorphismus von $A = W(k)$. Wie wir im Abschnitt 12 ausführlich besprechen werden, ist dann

$$\begin{aligned} \sigma : \qquad B &\longrightarrow B \\ \sum_{n\in\mathbb{Z}} a_n T^n &\longmapsto \sum_{n\in\mathbb{Z}} \sigma_0(a_n) T^{pn} \end{aligned}$$

ein Ringendomorphismus von $B$ mit den Eigenschaften

$$\sigma(b) \equiv b^p \bmod pB \qquad \text{für alle } b \in B$$

und

$$\omega \circ \sigma = \omega \ .$$

Somit erfüllt $B$ insbesondere die Voraussetzungen von Lemma 5.3.i. und Satz 5.5. Zusammen mit Satz 5.9.ii. erhalten wir die Ringmonomorphismen

$$\begin{array}{ccc} & & B \\ & & \Big\downarrow{\scriptstyle b\mapsto(b,\sigma(b),\sigma^2(b),\ldots)} \\ W(B) & \xrightarrow[\cong]{\Phi_B} & B' \qquad\quad \subseteq B^{\mathbb{N}_0} \ . \end{array}$$

Also gibt es genau einen Ringmonomorphismus

$$\begin{aligned} s : B &\longrightarrow W(B) \\ b &\longmapsto (b_0, b_1, \ldots) \text{ mit } \sigma^n(b) = \Phi_n(b_0, \ldots, b_n) \text{ für alle } n \geq 0 \ . \end{aligned}$$

Das Kompositum

$$s_0 : B \xrightarrow{s} W(B) \xrightarrow{\mathrm{pr}} W(B/pB)$$

ist immer noch injektiv. Sei nämlich $s_0(b) = 0$ und $s(b) = (b_0, b_1, \ldots)$. Dann gilt $b_n \in pB$ und wegen Lemma 5.2.i.

$$\sigma^n(b) = \Phi_n(b_0, \ldots, b_n) \equiv \Phi_n(0, \ldots, 0) = 0 \bmod p^{n+1}B$$

für alle $n \geq 0$. Es folgt $\omega(b) = \omega(\sigma^n(b)) > n$ für alle $n \geq 0$ und damit $b = 0$. Offensichtlich ist das Diagramm

$$\begin{array}{ccc} B & \xrightarrow{\qquad s_0 \qquad} & W(B/pB) \\ & {\scriptstyle \mathrm{pr}} \searrow \quad \swarrow {\scriptstyle \Phi_0} & \\ & B/pB & \end{array}$$

kommutativ. Also ist $s_0(B)$ ein Cohen-Unterring von $W(B/pB)$. Andererseits ist $\{T\}$ eine $p$-Basis von $B/pB = k((T))$. Wegen

$$\sigma^n(T) = T^{p^n} = \Phi_n(T, 0, \ldots, 0)$$

gilt $s_0(T) = \tau(T)$. Die behauptete Charakterisierung des Cohen-Unterringes $s_0(B)$ folgt deswegen aus Satz 7.3. $\square$

# 11 HN-Anstiege

In diesem Abschnitt wollen wir der Einfachheit halber die Angabe des Körpers $K$ in unseren Notationen weglassen. Wir haben also die beiden Ringe

$$\mathcal{R}^b \subseteq \mathcal{R} \ .$$

Dabei ist $\mathcal{R}$ ein Bezoutring und $\mathcal{R}^b$ ein diskret bewerteter Körper mit diskreter Bewertung $\omega$ und diskretem Bewertungsring $\mathcal{R}^{\text{int}}$. Wichtig im Folgenden ist die Eigenschaft (Bemerkung 10.3)

$$\mathcal{R}^\times = (\mathcal{R}^b)^\times \ . \tag{14}$$

Für diesen Abschnitt sei $\sigma : \mathcal{R} \longrightarrow \mathcal{R}$ ein beliebiger injektiver Ringendomorphismus mit

$$\sigma(\mathcal{R}^b) \subseteq \mathcal{R}^b \qquad \text{und} \qquad \omega \circ \sigma = \omega \ .$$

Allerdings wollen wir das folgende Axiom fordern: Für jedes $n \in \mathbb{N}$ und jede Matrix $A \in M_n(\mathcal{R}^{\text{int}})$ ist die Abbildung

$$\begin{aligned} (\mathcal{R}/\mathcal{R}^b)^n &\xrightarrow{\cong} (\mathcal{R}/\mathcal{R}^b)^n \\ \mathbf{v} + (\mathcal{R}^b)^n &\longmapsto \mathbf{v} - A\sigma(\mathbf{v}) + (\mathcal{R}^b)^n \end{aligned} \tag{Bij}$$

bijektiv. Wie üblich ist hier die Anwendung von $\sigma$ auf einen Spaltenvektor (bzw. später ebenso auf eine Matrix) komponentenweise zu verstehen.

**Bemerkung 11.1.** *Mit $\sigma$ erfüllt auch $\sigma^r$ für alle $r \in \mathbb{N}$ das Axiom* (Bij).

*Beweis.* Das Axiom (Bij) angewendet auf die $nr \times nr$-Matrix

$$\tilde{A} := \begin{pmatrix} 0 & & & & A \\ E_n & 0 & & & \\ & \ddots & & & \\ & & & 0 & \\ 0 & & & E_n & 0 \end{pmatrix}$$

ergibt die Bijektivität der Abbildung

$$(\mathbf{v}_0, \ldots, \mathbf{v}_{r-1}) \longmapsto (\mathbf{v}_0 - A\sigma(\mathbf{v}_{r-1}), \mathbf{v}_1 - \sigma(\mathbf{v}_0), \mathbf{v}_2 - \sigma(\mathbf{v}_1), \ldots, \mathbf{v}_{r-1} - \sigma(\mathbf{v}_{r-2}))$$

auf $(\mathcal{R}/\mathcal{R}^b)^{nr}$. Sei nun $\mathbf{v} \in \mathcal{R}^n$ mit $\mathbf{v} - A\sigma^r(\mathbf{v}) \in (\mathcal{R}^b)^n$. Wir setzen $\mathbf{v}_i := \sigma^i(\mathbf{v})$ für $0 \leq i \leq r-1$. Dann ist

$$\mathbf{v}_0 - A\sigma(\mathbf{v}_{r-1}) \in (\mathcal{R}^b)^n, \mathbf{v}_1 - \sigma(\mathbf{v}_0) = \mathbf{v}_2 - \sigma(\mathbf{v}_1) = \ldots = \mathbf{v}_{r-1} - \sigma(\mathbf{v}_{r-2}) = 0 \ .$$

Also folgt $\mathbf{v}_0, \ldots, \mathbf{v}_{r-1} \in (\mathcal{R}^b)^n$ und insbesondere $\mathbf{v} \in (\mathcal{R}^b)^n$. Andererseits sein ein $\mathbf{w} \in \mathcal{R}^n$ vorgegeben. Wir finden $\mathbf{v}_0, \ldots, \mathbf{v}_{r-1} \in \mathcal{R}^n$ mit

$$\mathbf{w} \equiv \mathbf{v}_0 - A\sigma(\mathbf{v}_{r-1}) \bmod (\mathcal{R}^b)^n$$

und

$$\mathbf{v}_1 - \sigma(\mathbf{v}_0) \equiv \mathbf{v}_2 - \sigma(\mathbf{v}_1) \equiv \ldots \equiv \mathbf{v}_{r-1} - \sigma(\mathbf{v}_{r-2}) \equiv 0 \bmod (\mathcal{R}^b)^n \ .$$

Letzteres bedeutet

$$\mathbf{v}_{r-1} \equiv \sigma^{r-1}(\mathbf{v}_0) \bmod (\mathcal{R}^b)^n \ .$$

Also erhalten wir

$$\mathbf{w} \equiv \mathbf{v}_0 - A\sigma^r(\mathbf{v}_0) \bmod (\mathcal{R}^b)^n \ .$$

□

Im Abschnitt 1 haben wir den Begriff der etalen $\sigma$-linearen Abbildung über dem Körper $\mathcal{R}^b$ eingeführt. Über dem Ring $\mathcal{R}$ tun wir das in ganz analoger Weise. Sei $V$ ein freier $\mathcal{R}$-Modul von endlichem Rang $h := \mathrm{rank}(V)$. Eine additive Abbildung $f : V \longrightarrow V$ heißt *$\sigma$-linear* wenn gilt

$$f(av) = \sigma(a)f(v) \qquad \text{für alle } a \in \mathcal{R} \text{ und } v \in V \ .$$

Bzgl. jeder Basis von $V$ können wir dann wie zuvor die Matrix $A_f \in M_h(\mathcal{R})$ zu $f$ bilden. Bei Übergang zu einer anderen Basis mit Basiswechselmatrix $B \in GL_h(\mathcal{R})$ geht $A_f$ über in $B^{-1}A_f\sigma(B)$. Die Abbildung $f$ heißt *etal*, wenn $A_f \in GL_h(\mathcal{R})$ invertierbar ist.

**Definition 11.2.** *Ein $\sigma$-Modul ist ein Paar $(V, f)$ bestehend aus einem freien $\mathcal{R}$-Modul $V$ von endlichem Rang und einer etalen $\sigma$-linearen Abbildung $f : V \longrightarrow V$.*

Für jeden $\sigma$-Modul $(V, f)$ ist $\det(A_f)$ wegen (14) eine Einheit in $\mathcal{R}^\times = (\mathcal{R}^b)^\times$, und wir können die von der Basiswahl unabhängige ganze Zahl

$$\deg(V, f) := \omega(\det(A_f))$$

bilden; sie heißt der *Grad* von $(V, f)$.

**Definition 11.3.** *Für einen $\sigma$-Modul $(V, f)$ mit $V \neq \{0\}$ heißt*

$$\mu(V, f) := \frac{\deg(V, f)}{\mathrm{rank}(V)}$$

*der HN-Anstieg von $(V, f)$.*

Wenn aus dem Zusammenhang klar ist, welche Abbildung $f$ gemeint ist, schreiben wir manchmal einfach $\deg(V)$ bzw. $\mu(V)$ statt $\deg(V,f)$ bzw. $\mu(V,f)$.

Sei $(V,f)$ ein $\sigma$-Modul. Ein *$\sigma$-Untermodul* von $(V,f)$ ist ein $\mathcal{R}$-Untermodul $V' \subseteq V$ mit $f(V') \subseteq V'$ und so, daß $(V', f|V')$ wieder ein $\sigma$-Modul ist.

**Definition 11.4.** *Ein $\sigma$-Modul $(V,f)$ mit $V \neq \{0\}$ heißt semistabil, wenn für jeden $\sigma$-Untermodul $V' \neq \{0\}$ von $(V,f)$ gilt*

$$\mu(V', f|V') \geq \mu(V,f) \ .$$

Das Axiom (Bij) geht ein in den Beweis der folgenden grundlegenden Tatsache.

**Lemma 11.5.** *Sei $(V,f)$ ein $\sigma$-Modul $\neq \{0\}$ und $V' \subset V$ ein echter $\sigma$-Untermodul mit $\operatorname{rank}(V') = \operatorname{rank}(V)$; dann gilt*

$$\mu(V', f|V') > \mu(V,f) \ .$$

*Beweis.* Sei $v_1, \ldots, v_h$ bzw. $v'_1, \ldots, v'_h$ eine Basis von $V$ bzw. $V'$; sei $A_f$ bzw. $A'_f$ die zugehörige Matrix zu $f$ bzw. $f|V'$. Wir haben

$$\omega(\det(A'_f)) > \omega(\det(A_f))$$

zu zeigen. Bezeichne $B \in M_h(\mathcal{R})$ die Matrix, welche die $v'_i$ durch die Basis $v_1, \ldots, v_h$ ausdrückt. Dann gilt $\det(B) \neq 0$ und $A_f \sigma(B) = B A'_f$, also

$$\det(B) - \left[\det(A_f) \cdot \det(A'_f)^{-1}\right] \sigma(\det(B)) = 0 \ .$$

Ist $\omega(\det(A'_f)) \leq \omega(\det(A_f))$, so folgt $\det(A_f) \cdot \det(A'_f)^{-1} \in \mathcal{R}^{\mathrm{int}}$. Der Fall $n = 1$ des Axioms (Bij) impliziert dann $\det(B) \in \mathcal{R}^b \setminus \{0\} \subseteq \mathcal{R}^\times$. Also ist $B \in GL_h(\mathcal{R})$ invertierbar und folglich $V' = V$ im Widerspruch zur Voraussetzung. □

Ist für einen freien $\mathcal{R}$-Untermodul $U \subseteq V$ mit $f(U) \subseteq U$ auch der Faktormodul $V/U$ frei, so sind sowohl $(U, f|U)$ als auch $V/U$ mit der von $f$ induzierten $\sigma$-linearen Abbildung $\bar{f}$ wiederum $\sigma$-Moduln. Dabei gilt

$$\operatorname{rank}(V) = \operatorname{rank}(U) + \operatorname{rank}(V/U)$$

und

$$\deg(V,f) = \deg(U, f|U) + \deg(V/U, \bar{f}) \ ,$$

folglich

$$\mu(V) = \mu(U)\frac{\operatorname{rank}(U)}{\operatorname{rank}(V)} + \mu(V/U)\frac{\operatorname{rank}(V/U)}{\operatorname{rank}(V)} \ .$$

**Lemma 11.6.** *Sei $V$ ein freier Modul von endlichem Rang über einem beliebigen Bezoutring $R$; für einen $R$-Untermodul $U \subseteq V$ sind äquivalent*

*i. $U$ und $V/U$ sind freie $R$-Moduln;*

*ii. $U$ ist saturiert, d. h. jedes $v \in V$ mit $av \in U$ für ein $0 \neq a \in R$ liegt selbst schon in $U$.*

*Beweis.* i. $\Longrightarrow$ ii. Da $V/U$ frei ist, ist es in einem Vektorraum über dem Quotientenkörper von $R$ enthalten und kann somit keine Elemente $\bar{v} \neq 0$ mit $a\bar{v} = 0$ für ein $0 \neq a \in R$ enthalten. Folglich ist $U$ saturiert.

ii. $\Longrightarrow$ i. Zunächst beweisen wir per Induktion nach $n$ folgende

*Zwischenbehauptung: Zu vorgegebenen Elementen $c_1, \ldots, c_n \in R$ mit $\sum_{i=1}^n Rc_i \neq \{0\}$ wähle ein $c \in R$, so daß $\sum_{i=1}^n Rc_i = Rc$; dann existiert eine Matrix $B \in GL_n(R)$, deren erste Spalte gerade $(c_1/c, \ldots, c_n/c)$ ist.*

Der Fall $n = 1$ sowie der Fall $c_1 = \ldots c_{n-1} = 0$ sind beide offensichtlich. Existiere also ein $0 \neq d \in R$ mit $Rd = \sum_{i=1}^{n-1} Rc_i$. Per Induktionsannahme gibt es eine Matrix $B_0 \in GL_{n-1}(R)$ mit erster Spalte $(c_1/d, \ldots, c_{n-1}/d)$. Wir setzen $B_1 := \left(\begin{smallmatrix} B_0 & 0 \\ 0 & 1 \end{smallmatrix}\right) \in GL_n(R)$. Wegen $Rd + Rc_n = Rc$ finden wir $a, b \in R$ mit $ad - bc_n = c$. Die Matrix

$$B := B_1 \begin{pmatrix} d/c & 0 & \ldots & 0 & b \\ 0 & 1 & & 0 & 0 \\ \vdots & & \ddots & & \vdots \\ 0 & 0 & & 1 & 0 \\ c_n/c & 0 & \ldots & 0 & a \end{pmatrix}$$

ist invertierbar und hat die gewünschte erste Zeile. Damit ist die Zwischenbehauptung gezeigt.

Die eigentliche Implikation beweisen wir jetzt ebenfalls per Induktion nach $h := \operatorname{rank}(V)$. Sei $v_1, \ldots, v_h$ eine Basis von $V$. Im Falle $U = \{0\}$ ist nichts zu zeigen. Existiere also ein $0 \neq v = \sum_{i=1}^h c_i v_i \in U$. Sei $0 \neq c \in R$ mit $Rc = Rc_1 + \ldots Rc_h$. Wir setzen $w := \sum_{i=1}^h (c_i/c)v_i \in V$. Da $U$ saturiert ist, gilt aber schon $w \in U$. Der Basiswechsel mit der entsprechenden Matrix aus der Zwischenbehauptung liefert eine Basis von $V$ der Form $w, w_2, \ldots, w_h$. Folglich ist $V/Rw$ ein freier $R$-Modul vom Rang $h - 1$, und wir können die Induktionsannahme auf den saturierten Untermodul $U/Rw$ von $V/Rw$ anwenden. Es folgt, daß $U/Rw$, also auch $U$, und $(V/Rw)/(U/Rw) \cong V/U$ frei sind. □

**Lemma 11.7.** *Für jeden $\sigma$-Modul $(V, f)$ ist die Menge der HN-Anstiege aller $\sigma$-Untermoduln $\neq \{0\}$ nach unten beschränkt.*

*Beweis.* Zuallererst stellen wir fest, daß für jeden $\sigma$-Untermodul $V'$ von $(V, f)$ gilt $\operatorname{rank}(V') \leq \operatorname{rank}(V)$ (betrachte dazu die erzeugten Vektorräume über dem Quotientenkörper von $\mathcal{R}$). Deswegen ist ein Beweis der Behauptung durch vollständige Induktion nach $\operatorname{rank}(V)$ sinnvoll. Besitzt $V$ keine $\sigma$-Untermoduln $\neq \{0\}$ von kleinerem Rang, so folgt die Behauptung aus Lemma 11.5. Damit ist insbesondere der Induktionsanfang gewährleistet. Sei also $U' \neq \{0\}$ ein $\sigma$-Untermodul von $(V, f)$ mit $\operatorname{rank}(U') < \operatorname{rank}(V)$. Man prüft leicht nach, daß

$$U := \{v \in V : av \in U' \text{ für ein } 0 \neq a \in \mathcal{R}\}$$

ein saturierter $\mathcal{R}$-Untermodul von $V$ ist mit $\operatorname{rank}(U) = \operatorname{rank}(U') < \operatorname{rank}(V)$ (wegen Lemma 11.6 ist $U$ frei), für welchen $f(U) \subseteq U$ gilt (die sogenannte *Saturierung* von $U'$). Auf die $\sigma$-Moduln $(U, f|U)$ und $(V/U, \bar{f})$ läßt sich die Induktionsvoraussetzung anwenden: Die Menge der HN-Anstiege ihrer sämtlichen $\sigma$-Untermoduln $\neq \{0\}$ ist durch eine Konstante $C$ nach unten beschränkt. Sei nun $V' \neq \{0\}$ ein beliebiger $\sigma$-Untermodul nach $V$. Wir betrachten die exakte Sequenz

$$0 \longrightarrow V' \cap U \longrightarrow V' \longrightarrow V' + U/U \longrightarrow 0 \ .$$

Offensichtlich ist $V' \cap U$ saturiert in $V'$. Wegen Lemma 11.6 sind also sowohl $V' \cap U$ als auch $V' + U/U$ wiederum $\sigma$-Moduln und zwar $\sigma$-Untermoduln von $U$ bzw. $V/U$. Ist einer von beiden $= \{0\}$, so folgt direkt $\mu(V', f|V') \geq C$. Andernfalls haben wir

$$\begin{aligned}
\mu(V', f|V') &= \frac{\deg(V' \cap U) + \deg(V' + U/U)}{\operatorname{rank}(V')} \\
&= \mu(V' \cap U)\frac{\operatorname{rank}(V' \cap U)}{\operatorname{rank}(V')} + \mu(V' + U/U) \cdot \frac{\operatorname{rank}(V' + U/U)}{\operatorname{rank}(V')} \\
&\geq C \cdot \frac{\operatorname{rank}(V' \cap U) + \operatorname{rank}(V' + U/U)}{\operatorname{rank}(V')} \\
&= C \ .
\end{aligned}$$

□

**Lemma 11.8.** *Sei $(V, f)$ ein $\sigma$-Modul $\neq \{0\}$; unter allen $\sigma$-Untermoduln $\neq \{0\}$ mit kleinstmöglichem HN-Anstieg existiert genau ein größter $V_1$ (der alle anderen enthält), und dieser ist semistabil und saturiert.*

*Beweis.* Nach Lemma 11.7 ist

$$\{\operatorname{rank}(V)! \cdot \mu(V') : \{0\} \neq V' \subseteq V \text{ ein } \sigma\text{-Untermodul}\}$$

eine nach unten beschränkte Menge von ganzen Zahlen. Folglich besitzt die Menge der $\mu(V')$ sogar ein Minimum $\lambda$. Sei $\{0\} \neq U' \subseteq V$ ein $\sigma$-Untermodul mit $\mu(U') = \lambda$. Offensichtlich gilt dann $\mu(U'') \geq \lambda = \mu(U')$ für jedes $\sigma$-Untermodul $\{0\} \neq U'' \subseteq U'$. Also ist $U'$ semistabil. Wie im Beweis von Lemma 11.7 bezeichne $U$ die Saturierung von $U'$. Dann ist einerseits $\mu(U) \geq \lambda = \mu(U')$ und andererseits $\operatorname{rank}(U) = \operatorname{rank}(U')$. Wegen Lemma 11.5 impliziert Letzteres $\mu(U') \geq \mu(U)$. Also gilt $\mu(U) = \lambda$. Seien nun $U_1, U_2 \subseteq V$ zwei saturierte $\sigma$-Untermoduln $\neq \{0\}$ mit $\mu(U_1) = \lambda = \mu(U_2)$. Aus den exakten Sequenzen von $\sigma$-Moduln (benutze Lemma 11.6)

$$0 \longrightarrow U_1 \cap U_2 \longrightarrow U_1 \longrightarrow U_1 + U_2/U_2 \longrightarrow 0$$

und

$$0 \longrightarrow U_2 \longrightarrow U_1 + U_2 \longrightarrow U_1 + U_2/U_2 \longrightarrow 0$$

folgt

$$\begin{aligned}
&\mu(U_1 + U_2) \\
&= \mu(U_2)\frac{\operatorname{rank}(U_2)}{\operatorname{rank}(U_1 + U_2)} + \mu(U_1 + U_2/U_2)\frac{\operatorname{rank}(U_1 + U_2/U_2)}{\operatorname{rank}(U_1 + U_2)} \\
&= \mu(U_2)\frac{\operatorname{rank}(U_2)}{\operatorname{rank}(U_1 + U_2)} + \\
&\qquad \Big(\mu(U_1) - \mu(U_1 \cap U_2)\frac{\operatorname{rank}(U_1 \cap U_2)}{\operatorname{rank}(U_1)}\Big)\frac{\operatorname{rank}(U_1)}{\operatorname{rank}(U_1 + U_2)} \\
&\leq \lambda\frac{\operatorname{rank}(U_2)}{\operatorname{rank}(U_1 + U_2)} + \Big(\lambda - \lambda\frac{\operatorname{rank}(U_1 \cap U_2)}{\operatorname{rank}(U_1)}\Big)\frac{\operatorname{rank}(U_1)}{\operatorname{rank}(U_1 + U_2)} \\
&= \lambda\Big(\frac{\operatorname{rank}(U_2) + \operatorname{rank}(U_1) - \operatorname{rank}(U_1 \cap U_2)}{\operatorname{rank}(U_1 + U_2)}\Big) \\
&= \lambda\ ,
\end{aligned}$$

also $\mu(U_1 + U_2) = \lambda$. Aus der zweiten exakten Sequenz folgt außerdem

$$\operatorname{rank}(U_2) < \operatorname{rank}(U_1 + U_2) \leq \operatorname{rank}(V) \qquad \text{im Falle } U_1 \subsetneqq U_2\ .$$

Das sukzessive Aufsummieren saturierter $\sigma$-Untermoduln mit HN-Anstieg $= \lambda$ muß also nach endlich vielen Schritten zu dem gewünschten maximalen $\sigma$-Untermodul $V_1$ mit $\mu(V_1) = \lambda$ führen. □

Offensichtlich ist $(V, f)$ genau dann semistabil, wenn $V_1 = V$ gilt. Ein Homomorphismus $\alpha : (V', f') \longrightarrow (V, f)$ von $\sigma$-Moduln ist eine $\mathcal{R}$-lineare Abbildung $\alpha : V' \longrightarrow V$ mit $\alpha \circ f' = f \circ \alpha$.

**Lemma 11.9.** *Seien $(V', f')$ und $(V, f)$ semistabile $\sigma$-Moduln $\neq \{0\}$ mit $\mu(V', f') < \mu(V, f)$; dann ist die Nullabbildung der einzige Homomorphismus von $(V', f')$ nach $(V, f)$.*

*Beweis.* Sei $\alpha : (V', f') \longrightarrow (V, f)$ ein Homomorphismus. Wäre $\alpha$ injektiv, so wäre $(\mathrm{im}(\alpha), f|\,\mathrm{im}(\alpha))$ ein $\sigma$-Untermodul von $(V, f)$, und es ergäbe sich der Widerspruch

$$\mu(V) > \mu(V') = \mu(\mathrm{im}(\alpha)) \geq \mu(V) \ .$$

Also ist $\ker(\alpha) \neq \{0\}$. Andererseits ist der $\mathcal{R}$-Untermodul $\ker(\alpha)$ von $V'$ saturiert. Denn aus $av' \in \ker(\alpha)$ für ein $v' \in V'$ und ein $0 \neq a \in \mathcal{R}$ folgt $0 = \alpha(av') = a\alpha(v')$ und damit $\alpha(v') = 0$, da $\mathcal{R}$ ein Integritätsbereich ist, und es deswegen in dem freien Modul $V$ keine Elemente $v \neq 0$ mit $av = 0$ geben kann. Wegen Lemma 11.6 haben wir also die exakte Sequenz von $\sigma$-Moduln

$$0 \longrightarrow \ker(\alpha) \xrightarrow{\subseteq} V' \xrightarrow{\alpha} \mathrm{im}(\alpha) \longrightarrow 0 \ .$$

Wäre $\mathrm{im}(\alpha) \neq \{0\}$, so ergäbe sich der Widerspruch

$$\begin{aligned}
\mu(V') &= \mu(\ker(\alpha))\frac{\mathrm{rank}(\ker(\alpha))}{\mathrm{rank}(V')} + \mu(\mathrm{im}(\alpha))\frac{\mathrm{rank}(\mathrm{im}(\alpha))}{\mathrm{rank}(V')} \\
&\geq \mu(V')\frac{\mathrm{rank}(\ker(\alpha))}{\mathrm{rank}(V')} + \mu(V)\frac{\mathrm{rank}(\mathrm{im}(\alpha))}{\mathrm{rank}(V')} \\
&> \mu(V')\frac{\mathrm{rank}(\ker(\alpha))}{\mathrm{rank}(V')} + \mu(V')\frac{\mathrm{rank}(\mathrm{im}(\alpha))}{\mathrm{rank}(V')} \\
&= \mu(V') \ .
\end{aligned}$$

□

**Satz 11.10.** *Sei $(V, f)$ ein $\sigma$-Modul $\neq \{0\}$; dann existiert genau eine echt aufsteigende Folge $\{0\} = V_0 \subset V_1 \subset \ldots \subset V_\ell = V$ von saturierten $\sigma$-Untermoduln mit:*

*i. die $\sigma$-Moduln $V_1, V_2/V_1, \ldots, V/V_{\ell-1}$ sind semistabil;*

*ii. $\mu(V_1) < \mu(V_2/V_1) < \ldots < \mu(V/V_{\ell-1})$ .*

*Beweis: Existenz:* Sei $V_1$ der in Lemma 11.8 konstruierte $\sigma$-Untermodul. Sei $\{0\} \neq \bar{V}' \subseteq V/V_1$ ein $\sigma$-Untermodul und sei $V'$ sein Urbild in $V$. Aus der exakten Sequenz von $\sigma$-Moduln (Lemma 11.6)

$$0 \longrightarrow V_1 \longrightarrow V' \longrightarrow \bar{V}' \longrightarrow 0$$

folgt

$$\begin{aligned}\mu(\bar{V}') &= \Big(\mu(V') - \mu(V_1)\frac{\operatorname{rank}(V_1)}{\operatorname{rank}(V')}\Big)\frac{\operatorname{rank}(V')}{\operatorname{rank}(\bar{V}')} \\ &= \mu(V')\frac{\operatorname{rank}(V')}{\operatorname{rank}(\bar{V}')} - \mu(V_1)\frac{\operatorname{rank}(V_1)}{\operatorname{rank}(\bar{V}')} \\ &> \mu(V_1)\end{aligned}$$

wegen $\mu(V') > \mu(V_1)$. Folglich können wir $V_2$ so wählen, daß $V_2/V_1 = (V/V_1)_1$ gilt. Iterativ liefert dies die Existenz der gewünschten Folge.

*Eindeutigkeit:* Seien

$$\{0\} \subset V_1 \subset \ldots \subset V_\ell = V \qquad \text{und} \qquad \{0\} \subset V_1' \subset \ldots \subset V_m' = V$$

zwei Folgen mit den behaupteten Eigenschaften. Es gelte etwa $\mu(V_1) \leq \mu(V_1')$. Wegen Lemma 11.9 muß dann das Kompositum

$$V_1 \xrightarrow{\subseteq} V \xrightarrow{\mathrm{pr}} V/V_{m-1}'$$

die Nullabbildung sein. Also gilt $V_1 \subseteq V_{m-1}'$, und wir erhalten genauso, daß das Kompositum

$$V_1 \xrightarrow{\subseteq} V_{m-1}' \xrightarrow{\mathrm{pr}} V_{m-1}'/V_{m-2}'$$

die Nullabbildung ist. Nach endlich vielen Schritten ergibt sich $V_1 \subseteq V_1'$ und $\mu(V_1) = \mu(V_1')$. Also können wir analog mit $V_1'$ und der Folge $V_i$ argumentieren und erhalten schließlich $V_1 = V_1'$. Eine Wiederholung der gesamten Argumentation für $V_2/V_1$ und $V_2'/V_1'$ in $V/V_1 = V/V_1'$ ergibt $V_2 = V_2'$. Induktiv folgt $V_i = V_i'$ für alle $i$. □

Die im Satz 11.10 konstruierte Folge heißt die *HN-Filtrierung* des $\sigma$-Moduls $(V, f)$.

**Definition 11.11.** *Sei $(V, f)$ ein $\sigma$-Modul $\neq \{0\}$ mit $h := \operatorname{rank}(V)$ und $\mu(V, f) = \frac{s}{r}$, wobei $r > 0$ und $s \in \mathbb{Z}$ teilerfremd seien; $(V, f)$ heißt isoklin, falls $V$ eine Basis besitzt, bzgl. welcher die Matrix der $\sigma^r$-linearen Abbildung $\pi^{-s} f^r$ in $GL_h(\mathcal{R}^{\mathrm{int}})$ liegt.*

**Bemerkung 11.12.** *Mit $f$ ist auch $f^r$ für jedes $r \in \mathbb{N}$ etal.*

*Beweis.* Dies folgt sofort aus der Identität $A_{f^r} = A_f \sigma(A_f) \ldots \sigma^{r-1}(A_f)$. □

Als zweite Anwendung des Axioms (Bij) beweisen wir das Folgende.

**Satz 11.13.** *Jeder isokline $\sigma$-Modul $(V, f)$ ist semistabil.*

*Beweis.* Sei $\mu(V) = \frac{s}{r}$ mit teilerfremdem Zahlen $r \geq 1$ und $s \in \mathbb{Z}$. Weiter sei $U \subseteq V$ ein $\sigma$-Untermodul $\neq \{0\}$. Wir müssen zeigen, daß

$$\mu(U) \geq \frac{s}{r}$$

gilt. Wegen Lemma 11.5 können wir $U$ als saturiert annehmen. Sei $v_1, \ldots, v_h$ bzw. $u_1, \ldots, u_m$ eine Basis von $V$ bzw. $U$, und sei $B$ die $h \times m$-Matrix, welche die $u_j$ durch die $v_i$ ausdrückt. Weiter bezeichne $A \in GL_h(\mathcal{R})$ die Matrix zu $f^r$ bzgl. der Basis $v_1, \ldots, v_h$ und $A_0 \in GL_m(\mathcal{R})$ die Matrix zu $f^r|U$ bzgl. der Basis $u_1, \ldots, u_m$. Es gilt

$$BA_0 = A\sigma^r(B) \ .$$

Es bezeichne $\mathcal{I}(m)$ die Menge aller geordneten Tupel $(i_1 < \ldots < i_m)$ von ganzen Zahlen in der Menge $\{1, \ldots, h\}$. Für zwei Elemente $I = (i_1 < \ldots < i_m)$ und $J$ in $\mathcal{I}(m)$ sei $B_I$ bzw. $A_{I,J}$ die $m \times m$-Matrix, die aus den Zeilen $i_1, \ldots, i_m$ von $B$ besteht bzw. die aus $A$ durch Weglassen der Zeilen bzw. Spalten mit Index nicht in $I$ bzw. $J$ entsteht. Dann gilt

$$\det(A_0)\det(B_I) = \sum_{J \in \mathcal{I}(m)} \det(A_{I,J})\sigma^r(\det(B_J)) \ . \tag{15}$$

Da $(V, f)$ isoklin ist, können wir die Basis $v_1, \ldots, v_h$ so wählen, daß $\pi^{-s}A \in GL_h(\mathcal{R}^{\mathrm{int}})$ gilt. Es folgt

$$\det(A_{I,J}) \in \pi^{ms}\mathcal{R}^{\mathrm{int}}, \text{ d. h. } \omega(\det(A_{I,J})) \geq ms$$

für alle $I, J \in \mathcal{I}(m)$. Wir wollen per Widerspruch argumentieren und nehmen jetzt $\mu(U) < \frac{s}{r}$ an. Dann ist

$$\omega(\det(A_0)) = r\deg(U, f|U) = rm\mu(U, f|U) < ms \ .$$

Folglich hat die Matrix $(\det(A_0)^{-1}\det(A_{I,J}))_{I,J \in \mathcal{I}(m)}$ sämtliche Einträge in $\pi\mathcal{R}^{\mathrm{int}}$. Also können wir Bemerkung 11.1 auf die Identität (15) anwenden und erhalten $\det(B_I) \in \mathcal{R}^b$ für alle $I \in \mathcal{I}(m)$. Außerdem folgt dann

$$\begin{aligned}\min_I \omega(\det(B_I)) &\geq \min_{I,J}(\omega(\det(A_0)^{-1}\det(A_{I,J})) + \omega(\det(B_J))) \\ &\geq 1 + \min_J \omega(\det(B_J))\end{aligned}$$

und somit $\det(B_I) = 0$ für alle $I \in \mathcal{I}(m)$. Nach Konstruktion hatte die Matrix $B$ aber den Rang $m$, was den gewünschten Widerspruch liefert. □

Wir halten fest, daß wir bisher nur die Injektivität der Abbildung im Axiom Bij benötigt haben.

# 12 Spezielle Endomorphismen

Wir betrachten ein festes $u \in \mathcal{R}_K^{\mathrm{int}}$ mit der Eigenschaft, daß

$$u \equiv T^q \bmod \pi \qquad \text{für ein } q > 1 \text{ in } \mathbb{N}.$$

Sei etwa $u(T) = \sum_{n\in\mathbb{Z}} c_n T^n$. Es gilt

$$|c_q| = 1 > |\pi| \geq |c_n| \qquad \text{für alle } n \neq q \ .$$

Aus Lemma 9.21.iv. folgt deswegen (vgl. den Beweis von Satz 10.2) die Existenz eines $0 < \delta_0 < 1$ mit $u \in \mathcal{A}^b_{[\delta_0,1)}(K)^\times$ und

$$|c_n|\rho^n < |c_q|\rho^q = \rho^q \qquad \text{für alle } n \neq q \text{ und alle } \rho \in [\delta_0, 1) \ . \tag{16}$$

Insbesondere ist

$$\|u\|_\rho = \rho^q < 1 \qquad \text{für alle } \rho \in [\delta_0, 1) \ .$$

Seien nun $\delta_0 \leq \delta < 1$ und $F \in \mathcal{A}_{[\delta,1)}(K)$ ein beliebiges Element, etwa $F(T) = \sum_{n\in\mathbb{Z}} a_n T^n$. Dann gilt

$$\lim_{n\to\pm\infty} \|a_n u^n\|_\rho = \lim_{n\to\pm\infty} |a_n|\rho^{qn} = 0 \qquad \text{für alle } \rho \in [\delta^{1/q}, 1) \ .$$

Also ist die Reihe

$$F(u) := \sum_{n\in\mathbb{Z}} a_n u^n$$

konvergent in dem Fréchetraum $\mathcal{A}_{[\delta^{1/q},1)}(K)$.

**Lemma 12.1.** *$\|F(u)\|_\rho = \|F\|_{\rho^q}$ für alle $\rho \in [\delta^{1/q}, 1)$.*

*Beweis.* Aus (16) folgt $\|u - c_q T^q\|_\rho < |c_q|\rho^q = \rho^q = \|u\|_\rho$ und damit $\|\frac{u}{c_q T^q} - 1\|_\rho < 1$.

*Zwischenbehauptung: $\|\left(\frac{u}{c_q T^q}\right)^n - 1\|_\rho < 1$ für alle $n \in \mathbb{Z}$.*

Die Ungleichung ist trivial für $n = 0$. Setze $v := \frac{u}{c_q T^q}$. Für $n > 0$ haben wir

$$\begin{aligned} \|v^n - 1\|_\rho = \|((v-1)+1)^n - 1\|_\rho &= \|\sum_{i=1}^{n} \binom{n}{i} (v-1)^i\|_\rho \\ &\leq \max_{1\leq i\leq n} \|v-1\|_\rho^i = \|v-1\|_\rho < 1 \ . \end{aligned}$$

Dies benutzend erhalten wir für $n < 0$ ebenfalls

$$\|v^n - 1\|_\rho = \|v^n\|_\rho \cdot \|v^{-n} - 1\|_\rho < \|v\|_\rho^n = 1 \ .$$

Damit ist die Zwischenbehauptung bewiesen, und es ergibt sich

$$\|u^n - c_q^n T^{qn}\|_\rho < \rho^{qn} = \|u^n\|_\rho \qquad \text{für alle } \rho \in [\delta_0, 1) \ .$$

Für

$$F(u) = \sum_{n\in\mathbb{Z}} a_n u^n = \sum_{n\in\mathbb{Z}} a_n c_q^n T^{qn} + \sum_{n\in\mathbb{Z}} a_n (u^n - c_q^n T^{qn})$$

folgt

$$\|\sum_{n\in\mathbb{Z}} a_n c_q^n T^{qn}\|_\rho = \|F\|_{\rho^q}$$

und

$$\begin{aligned} \|\sum_{n\in\mathbb{Z}} a_n (u^n - c_q^n T^{qn})\|_\rho &\leq \max_{n\in\mathbb{Z}} |a_n| \cdot \|u^n - c_q^n T^{qn}\|_\rho \\ &< \max_{n\in\mathbb{Z}} |a_n| \rho^{qn} \\ &= \|F\|_{\rho^q} \ . \end{aligned}$$

Das bedeutet aber $\|F(u)\|_\rho = \|F\|_{\rho^q}$. □

Für $\delta_0 \leq \delta < 1$ haben wir also den injektiven stetigen Ringhomomorphismus

$$\begin{aligned} \mathcal{A}_{[\delta,1)}(K) &\longrightarrow \mathcal{A}_{[\delta^{1/q},1)}(K) \\ F &\longmapsto F(u) \ . \end{aligned}$$

Durch Übergang zur Vereinigung bzgl. $\delta \longrightarrow 1$ erhalten wir den injektiven Ringendomorphismus

$$\begin{aligned} \mathcal{R}_K &\longrightarrow \mathcal{R}_K \\ F &\longmapsto F(u) \ . \end{aligned}$$

Aus Lemma 12.1 und Lemma 9.21.i. folgt, daß sich ersterer Endomorphismus einschränkt zu einem Ringhomomorphismus

$$\mathcal{A}^b_{[\delta,1)}(K) \longrightarrow \mathcal{A}^b_{[\delta^{1/q},1)}(K) \ ,$$

welcher $\|F(u)\|_1 = \|F\|_1$ erfüllt. Wieder in der Vereinigung ergibt sich ein Körperendomorphismus

$$\mathcal{R}_K^b \longrightarrow \mathcal{R}_K^b \ ,$$

welcher die diskrete Bewertung $\omega$ respektiert und sich insbesondere zu einem Endomorphismus

$$\mathcal{E}_K \longrightarrow \mathcal{E}_K$$

fortsetzt. Letzerer ist wegen Lemma 10.4 nachwievor durch $F \longmapsto F(u)$ gegeben.

Andererseits sei $\sigma_0$ ein Körperendomorphismus von $K$ mit der Eigenschaft $v \circ \sigma_0 = v$. Offensichtlich wird dann durch

$$F(T) = \sum_{n\in\mathbb{Z}} a_n T^n \longmapsto (\sigma_0 F)(T) := \sum_{n\in\mathbb{Z}} \sigma_0(a_n) T^n$$

ein injektiver Ringendomorphismus all der betrachteten Ringe $\mathcal{A}_{[\delta,\varepsilon]}(K)$, $\mathcal{A}_{[\delta,\varepsilon)}(K)$, $\mathcal{A}^b_{[\delta,1)}(K)$, $\mathcal{R}_K, \mathcal{R}_K^b$, $\mathcal{R}_K^{\mathrm{int}}$, $\mathcal{E}_K^{\mathrm{int}}$ und $\mathcal{E}_K$ definiert. Dabei gilt

$$\|\sigma_0(F)\|_\rho = \|F\|_\rho$$

für jedes jeweils zugelassene $\rho$.

**Definition 12.2.** *Ein Ringendomorphismus $\sigma : \mathcal{R}_K \longrightarrow \mathcal{R}_K$ heißt $(\sigma_0-)$ speziell, wenn er von der Form*

$$\sigma(F) = (\sigma_0 F)(u) \qquad \textit{für alle } F \in \mathcal{R}_K$$

*ist für ein $u \in \mathcal{R}_K^{\mathrm{int}}$ mit $u \equiv T^q \bmod \pi$ für ein $q \in \mathbb{N}$.*

**Übungsaufgabe 12.3.** *Das Kompositum zweier spezieller Endomorphismen ist speziell.*

**Satz 12.4.** *Jeder spezielle Endomorphismus $\sigma$ von $\mathcal{R}_K$ erfüllt das Axiom* (Bij) *aus Abschnitt 11.*

*Beweis.* Sei $u := \sigma(T) \equiv T^q \bmod \pi$. Wie zu Beginn diese Abschnittes diskutiert, gilt $u \in \mathcal{A}^b_{[\delta_0,1)}(K)^\times \cap (\mathcal{R}_K^{\mathrm{int}})^\times$ mit $w_u(t) = qt$ auf $[\log \delta_0, 0]$.

Zu gegebener Matrix $A$ über $\mathcal{R}_K^{\mathrm{int}}$ haben wir die Bijektivität des Endomorphismus $\mathbf{v} \longmapsto \mathbf{v} - A\sigma(\mathbf{v})$ von $(\mathcal{R}_K/\mathcal{R}_K^b)^n$ zu zeigen. Für jedes $m \in \mathbb{N}$ ist $\tilde{A} := T^{-m}u^m A$ ebenfalls eine Matrix über $\mathcal{R}_K^{\mathrm{int}}$, und das Diagramm

$$\begin{array}{ccc} (\mathcal{R}_K/\mathcal{R}_K^b)^n & \xrightarrow{\mathbf{v}\mapsto\mathbf{v}-A\sigma(\mathbf{v})} & (\mathcal{R}_K/\mathcal{R}_K^b)^n \\ {\scriptstyle T^{-m}\cdot}\downarrow & & \downarrow{\scriptstyle T^{-m}\cdot} \\ (\mathcal{R}_K/\mathcal{R}_K^b)^n & \xrightarrow{\mathbf{v}\mapsto\mathbf{v}-\tilde{A}\sigma(\mathbf{v})} & (\mathcal{R}_K/\mathcal{R}_K^b)^n \end{array}$$

ist kommutativ. Die Spalten sind offensichtlich bijektiv. Folglich ist die obere Zeile genau dann bijektiv, wenn es die untere ist. Wir finden ein $\delta_0 \leq \delta_1 < 1$, so daß $A$ und damit auch $\tilde{A}$ eine Matrix über $\mathcal{A}^b_{[\delta_1,1)}(K)$ ist.

*Zwischenbehauptung: Zu jedem $F \in \mathcal{R}^{\mathrm{int}}_K \cap \mathcal{A}^b_{[\delta_1,1)}(K)$ existiert ein $\delta_1 \leq \delta < 1$ und ein $m \in \mathbb{N}$, so daß $\|T^{-m}u^m F\|_\rho \leq 1$ für alle $\rho \in [\delta, 1]$ gilt.*

Wir wählen $\delta$ so, daß $w_F$ genau eine Steigung $\lambda$ auf $[\log \delta, 0]$ besitzt. Wegen $w_F(0) = -\omega(F) \leq 0$ und

$$w_{T^{-m}u^m F}(t) = m(q-1)t + w_F(t) = (m(q-1) + \lambda)t$$

genügt es, anschließend $m \geq -\frac{\lambda}{q-1}$ zu wählen.

Die Zwischenbehauptung besagt, daß wir durch geeignete Wahl von $\delta_1 \leq \delta < 1$ und $m$ erreichen können, daß sämtliche Einträge $F$ der Matrix $\tilde{A}$ die Eigenschaft $\|F\|_\rho \leq 1$ für alle $\rho \in [\delta, 1]$ besitzen.

*Injektivität:* Sei $\mathbf{v} = (v_1, \ldots, v_n) \in \mathcal{R}^n_K$ mit $\mathbf{w} = (w_1, \ldots, w_n) := \mathbf{v} - \tilde{A}\sigma(\mathbf{v}) \in (\mathcal{R}^b_K)^n$. Durch Vergrößerung von $\delta$ können wir annehmen, daß $w_1, \ldots, w_n \in \mathcal{A}^b_{[\delta,1)}(K)$ und $\sigma(v_1), \ldots, \sigma(v_n) \in \mathcal{A}_{[\delta,1)}(K)$ gilt. Nach Lemma 9.21 bzw. Übungsaufgabe 9.15 finden wir eine Konstante $C > 0$ mit

$$\|w_1\|_\rho, \ldots, \|w_n\|_\rho \leq C \qquad \text{für alle } \delta \leq \rho < 1$$

und

$$\|\sigma(v_1)\|_\rho, \ldots, \|\sigma(v_n)\|_\rho \leq C \qquad \text{für alle } \delta \leq \rho \leq \delta^{1/q}.$$

Aus $\mathbf{v} = \mathbf{w} + \tilde{A}\sigma(\mathbf{v})$ und der Zusatzeigenschaft der Matrix $\tilde{A}$ folgt dann

$$\|v_1\|_\rho, \ldots, \|v_n\|_\rho \leq C \qquad \text{für alle } \delta \leq \rho \leq \delta^{1/q}.$$

Dies impliziert aber auf Grund von Lemma 12.1, daß

$$\|\sigma(v_1)\|_\rho, \ldots, \|\sigma(v_n)\|_\rho \leq C \qquad \text{für alle } \delta^{1/q} \leq \rho \leq \delta^{1/q^2}.$$

Induktives Wiederholen dieses Argumentes ergibt

$$\|v_1\|_\rho, \ldots, \|v_n\|_\rho \leq C \qquad \text{für alle } \delta \leq \rho < 1$$

und damit $\mathbf{v} \in (\mathcal{R}^b_K)^n$ wegen Lemma 9.21.

*Surjektivität:* Sei $\mathbf{w} = (w_1, \ldots, w_n) \in \mathcal{R}^n_K$. Wieder können wir durch Vergrößerung von $\delta$ annehmen, daß $w_1, \ldots, w_n \in \mathcal{A}_{[\delta,1)}(K)$ gilt. Wir konstruieren induktiv eine Folge $\{\mathbf{w}_l = (w_{l,1}, \ldots, w_{l,n})\}_{l \geq 0}$ in $\mathcal{A}_{[\delta^{1/q},1)}(K)^n$. Sei $\mathbf{w}_0 := \mathbf{w}$. Wir schreiben

$$w_{l,i} = \sum_{j \in \mathbb{Z}} a_{l,i,j} T^j \ ,$$

setzen

$$w_{l,i}^+ := \sum_{j\geq 1} a_{l,i,j}T^j,\ w_{l,i}^- := w_{l,i} - w_{l,i}^+,\ \mathbf{w}_l^\pm := (w_{l,1}^\pm, \ldots, w_{l,n}^\pm)$$

und definieren

$$\mathbf{w}_{l+1} := \tilde{A}\sigma(\mathbf{w}_l^+)\ .$$

Ersichtlich gilt $T^{-1}w_{l,i}^+ \in \mathcal{A}_{[0,1)}(K)$ und damit $\mathbf{w}_{l+1} \in \mathcal{A}_{[\delta^{1/q},1)}(K)^n$ und

$$\begin{aligned}\max_i \|w_{l+1,i}^+\|_\rho &\leq \max_i \|w_{l+1,i}\|_\rho \leq \max_i \|w_{l,i}^+\|_{\rho^q} \\ &= \rho^q \max_i \|T^{-1}w_{l,i}^+\|_{\rho^q} \leq \rho^q \max_i \|T^{-1}w_{l,i}^+\|_\rho \\ &= \rho^{q-1} \max_i \|w_{l,i}^+\|_\rho\end{aligned}$$

für alle $\rho \in [\delta^{1/q}, 1)$. Dabei benutzt der erste Teil der Folgerung sowie die zweite Ungleichung im zweiten Teil die Zusatzeigenschaft der Matrix $\tilde{A}$ und Lemma 12.1. Die dritte Ungleichung ist die offensichtliche Tatsache, daß für alle $F \in \mathcal{A}_{[0,1)}(K)$ und alle $0 \leq \rho_1 \leq \rho_2 < 1$ gilt $\|F\|_{\rho_1} \leq \|F\|_{\rho_2}$. Wir sehen also, daß gilt

$$\lim_{l\to\infty} w_{l,i}^+ = 0 \quad \text{in } \mathcal{A}_{[\rho,\rho]}(K) \text{ für alle } 1 \leq i \leq n \text{ und } 0 \leq \rho < 1.$$

Somit existiert $v_i := \sum_{l=0}^\infty w_{l,i}^+$ in $\mathcal{A}_{[0,1)}(K)$. Wir setzen $\mathbf{v} := (v_1, \ldots, v_n)$. Es folgt

$$\mathbf{w} - \mathbf{v} + \tilde{A}\sigma(\mathbf{v}) = \sum_{l=0}^\infty \mathbf{w}_l^- \qquad \text{in } \mathcal{A}_{[\delta^{1/q},1)}(K).$$

Der Vektor von Laurentreihen auf der rechten Seite enthält keine positiven Potenzen von $T$ und liegt deswegen in $\mathcal{A}^b_{[\delta^{1/q},1)}(K)^n$. □

**Theorem 12.5.** *(Kedlaya)*
*Ist $\sigma$ ein spezieller Endomorphismus von $\mathcal{R}_K$ so ist jeder semistabile $\sigma$-Modul isoklin.*

## Literatur


[1] Bosch S.: Algebra. Springer 1993.

[2] Bourbaki N.: Algebra II, Chap. 4 - 7. Masson 1990.

[3] Bourbaki N.: Commutative Algebra. Hermann 1972.

[4] Bourbaki N.: Algèbre commutative, Chap. 8 - 9. Springer 2006.

[5] Bourbaki N.: General Topology, Chap. 1 - 4. Springer 1989.

[6] Kedlaya K.: Slope filtrations revisited. Documenta Math. 10, 447-525 (2005).

[7] Lazard M.: Les zéros des fonctions analytiques d'une variable sur un corps valué complet. Publ. Math. IHES 14, 47 - 75 (1962).

[8] Lazard M.: Commutative Formal Groups. Springer Lect. Notes Math. 443, 1975.

[9] Nagata M.: Local Rings. J. Wiley 1962.

[10] Neukirch J.: Algebraische Zahlentheorie. Springer 1992.

[11] Robert A.: A Course in $p$-adic Analysis. Springer 2000.

[12] Serre J.-P.: Local Fields. Springer 1979.

[13] Zink, T.: Cartiertheorie kommutativer formaler Gruppen. Teubner, Leipzig 1983.