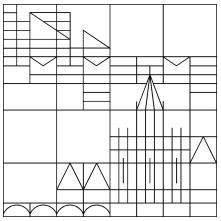
Claus Scheiderer

Reelle algebraische Geometrie II



Vorlesung SS 2016

Universität Konstanz

Inhaltsverzeichnis

Kapitel IV. Positive Polynome und Quadratsummen 5
1. Summen von Quadraten von Polynomen 5
2. Hilberts Theorem über Quadratsummen von Polynomen 11
3. Semiringe und Moduln 17
4. Einführung in Semiordnungen 21
5. Archimedizität 24
6. Der archimedische Positivstellensatz 28
7. Erste Anwendungen: Sätze von Pólya und Handelman 31
8. Schmüdgens Theorem und Folgerungen 33

Kapitel V. Ergänzungen zur kommutativen Algebra 39
1. Primvermeidung, Nakayama Lemma, Krullscher Hauptidealsatz 39
2. Reguläre lokale Ringe 41
3. Reguläre und singuläre Punkte von Varietäten 43
4. Komplettierung 47
5. Potenzreihenringe 56

Kapitel VI. Nichtnegativstellensätze 61
1. Saturierte Präordnungen 61
2. Quadratsummen in lokalen Ringen 65
3. Zweidimensionale lokale Ringe 70
4. Globale Resultate 73

Kapitel VII. Einige Anwendungen von Quadratsummen 77
1. Lokalkonvexe Vektorräume 77
2. Das Momentenproblem 79
3. Stabilität 83
4. Beschreibung konvexer Mengen durch Lasserre-Relaxierung 89

KAPITEL IV

Positive Polynome und Quadratsummen

1. Summen von Quadraten von Polynomen

1.1 Lemma. *Sei K ein Körper, seien $f_1, \dots, f_r \in K$, und sei v eine Bewertung von K. Gibt es eine mit v verträgliche Anordnung P von K mit $f_1 \geq_P 0, \dots, f_r \geq_P 0$, so ist*

$$v(f_1 + \cdots + f_r) \;=\; \min\{v(f_1), \dots, v(f_r)\}.$$

Beweis. $\geq$ gilt ohnehin. Umgekehrt sei etwa $v(f_1) \leq v(f_i)$ für alle i. Dann ist $f_1 + \cdots + f_r = f_1(1 + g_2 + \cdots + g_r)$, wobei die $g_i := \frac{f_i}{f_1}$ im Bewertungsring $\mathcal{O}_v$ von v liegen. Nach Voraussetzung ist $g_i \geq_P 0$ für alle i. Da $\mathcal{O}_v$ P-konvex in K ist, induziert P auf dem Restklassenkörper κ eine Anordnung $\overline{P}$, und es gilt $\overline{g}_i \geq_{\overline{P}} 0$ für alle i. Insbesondere ist $1 + \overline{g}_2 + \cdots + \overline{g}_r >_{\overline{P}} 0$, also $1 + g_2 + \cdots + g_r \in \mathcal{O}_v^*$, woraus die Behauptung folgt. □

1.2 Beispiel.

1. Für jede reelle Bewertung v von K (also Bewertung mit reellem Restklassenkörper) gilt $v(f_1^2 + \cdots + f_r^2) = 2 \min_i v(f_i)$. Denn nach Baer-Krull (II.5.8) hat K eine mit v verträgliche Anordnung.

2. Sei k ein Körper, seien $f_1, \dots, f_r \in k[\mathtt{x}]$ und $f = \sum_i f_i^2$. Sei $p \in k[\mathtt{x}]$ ein irreduzibler Teiler von f. Ist $\operatorname{Quot} k[\mathtt{x}]/(p)$ reell, so ist $m := v_p(f)$ gerade, und $p^{m/2} \mid f_i$ für alle i. (Folgt aus der vorigen Bemerkung, angewandt auf die diskrete Bewertung v_p.)

3. Ist der Körper k reell, so ist $\deg(\sum_i f_i^2) = 2 \max_i \deg(f_i)$ für beliebige Polynome $f_i \in k[\mathtt{x}] = k[x_1, \dots, x_n]$. (Betrachte die durch $v(f) = -\deg(f)$, $f \in k[\mathtt{x}]$, definierte diskrete Bewertung von $k(\mathtt{x})$. Ihr Restklassenkörper ist ein rationaler Funktionenkörper über k in $n-1$ Variablen.)

Im folgenden sei A ein (kommutativer) Ring.

1.3 Definition. Ein Element $f \in A$ ist *sos* (sum of squares, Quadratsumme), wenn $f \in \Sigma A^2$ ist, und ist *psd* (positiv semidefinit), wenn $f \geq_\alpha 0$ für alle $\alpha \in \operatorname{Sper}(A)$ gilt. Wir bezeichnen die Menge aller psd Elemente von A mit A_+.

1.4 Definition. Die *sos-Länge* (oder Quadratsummenlänge) von $f \in A$ (in A) ist definiert als

$$\ell(f) \;=\; \ell_A(f) \;=\; \inf\{r \geq 0 \colon \exists\, f_1, \dots, f_r \in A \text{ mit } f = f_1^2 + \cdots + f_r^2\}$$

(insbesondere $\ell(f) = \infty$ falls $f \notin \Sigma A^2$ ist). Die *Pythagoraszahl* von A ist

$$p(A) \;:=\; \sup\big\{\ell_A(f) \colon f \in \Sigma A^2\big\} \;\in \mathbb{Z} \cup \{\infty\}.$$

1.5 Bemerkungen.

1. Für jeden Ring A gilt $\Sigma A^2 \subseteq A_+$. Ist $A = k$ ein Körper mit $\operatorname{char}(k) \neq 2$, so gilt Gleichheit (Artins Theorem, I.30). Ebenso gilt Gleichheit, wenn A nicht reell (d.h.

$\mathrm{Sper}(A) = \varnothing$, II.2.14) und $\frac{1}{2} \in A$ ist, wegen $-1 \in \Sigma A^2$ und $x = \left(\frac{x+1}{2}\right)^2 - \left(\frac{x-1}{2}\right)^2$. Für die meisten reellen Ringe A ist $\Sigma A^2 \neq A_+$. Für den Polynomring $A = R[x, y]$ haben wir das in Aufgabe 13 gesehen.

2. Nach dem abstrakten Nichtnegativstellensatz (II.2.8) ist

$$A_+ \;=\; \bigcup_{m \geq 0} \Big\{ f \in A \colon \exists\, s,\, t \in \Sigma A^2 \text{ mit } sf = f^{2m} + t \Big\}.$$

Wir zeigen jetzt, daß die Frage nach sos-Darstellungen "linearisiert" werden kann. Zunächst einige Vorbereitungen über symmetrische Matrizen. Sei weiter A ein (kommutativer) Ring, und sei stets $\frac{1}{2} \in A$.

1.6 Für $S = (a_{ij}) \in \mathrm{Sym}_n(A)$ sei

$$q_S \;=\; q_S(\mathtt{x}) \;=\; \mathtt{x}^t S \mathtt{x} \;=\; \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

die zugehörige quadratische Form. (Fasse $\mathtt{x}$ stets auf als *Spaltenvektor* der Variablen.) Die Matrix S, oder die quadratische Form q_S, heißt *psd* (positiv semidefinit) *über* A, wenn für alle $\alpha \in \mathrm{Sper}(A)$ die Matrix S psd über $R(\alpha)$ ist. Nach Definition bedeutet das $u^t \phi(S) u \geq 0$ für jeden Homomorphismus $\phi \colon A \to R$ in einen reell abgeschlossenen Körper R und jedes $u \in R^n$. Gilt stets sogar $u^t \phi(S) u > 0$ für $u \neq 0$, so heißt A positiv definit über A. Man schreibt $S \succeq 0$ bzw. $S \succ 0$, falls S psd bzw. positiv definit ist. Wir setzen

$$\mathrm{Sym}_n^+(A) \;:=\; \big\{ S \in \mathrm{Sym}_n(A) \colon S \succeq 0 \big\},$$
$$\mathrm{Sym}_n^{++}(A) \;:=\; \big\{ S \in \mathrm{Sym}_n(A) \colon S \succ 0 \big\}.$$

1.7 Bemerkungen.

1. Sei $A = R$ ein reell abgeschlossener Körper. Dann ist $\mathrm{Sym}_n^+(R)$ ein volldimensionaler, basisch abgeschlossener (semialgebraischer) konvexer Kegel in $\mathrm{Sym}_n(R)$. Sei $S = (a_{ij}) \in \mathrm{Sym}_n(R)$, sei $p_S(t) = t^n + a_1 t^{n-1} + \cdots + a_n$ das charakteristische Polynom von S. Dann sind äquivalent:

(i) $S \succeq 0$,
(ii) $(-1)^i a_i \geq 0$ für $i = 1, \ldots, n$,
(iii) alle symmetrischen Minoren $\det\big(a_{ij}\big)_{i,j \in I} \geq 0$ (für $\varnothing \neq I \subseteq \{1, \ldots, n\}$).

In der Tat, $p_S(t)$ zerfällt über R, und (i) $\Leftrightarrow$ (ii) folgt somit aus Aufgabe 11. Für $S \succ 0$ hat man eine entsprechende Charakterisierung.

2. Ist A beliebiger Ring und $S \in \mathrm{Sym}_n(A)$ mit charakteristischem Polynom $p(t) = t^n + a_1 t^{n-1} + \cdots + a_n$, so gilt also:

$$S \succeq 0 \quad \Leftrightarrow \quad (-1)^i a_i \in A_+ \;\; (i = 1, \ldots, n).$$

1.8 Lemma. *Für jede Matrix $S \in \mathrm{Sym}_n(A)$ und jedes $r \geq 1$ sind äquivalent:*

(i) *$q_S(\mathtt{x})$ ist Summe von r Quadraten von Linearformen in $A[\mathtt{x}]$;*
(ii) *es gibt (Spalten-) Vektoren $u_1, \ldots, u_r \in A^n$ mit $S = \sum_{i=1}^r u_i u_i^t$;*
(iii) *es gibt $T \in M_{n \times r}(A)$ mit $S = TT^t$.*

Gelten diese Eigenschaften für ein $r \geq 1$, so sagen wir, daß S eine Quadratsumme *(kurz:* sos*) ist. In diesem Fall ist $S \succeq 0$.*

1.9 Definition. Für $S \in \mathrm{Sym}_n(A)$ ist die *(sos-) Länge* von S definiert als

$$\ell_A(S) \;=\; \ell(S) \;:=\; \inf\big\{ r \geq 0 \colon \exists\, T \in M_{n \times r}(A) \text{ mit } S = TT^t \big\}.$$

(Es ist also $\ell_A(S) = \infty$, falls S nicht sos ist.)

1.11 Betrachte nun Polynome von höherem Grad. Sei im folgenden k ein *reeller* Körper, und sei weiter $\mathtt{x} = (x_1, \dots, x_n)$. Für $f \in k[\mathtt{x}]$ sei stets $\deg(f)$ der Totalgrad von f, also

$$\deg\Big(\sum_{\alpha\in\mathbb{Z}_+^n} c_\alpha\, \mathtt{x}^\alpha\Big) := \sup\big\{|\alpha|\colon c_\alpha \neq 0\big\}.$$

Wegen k reell gilt $\deg(f_1^2 + \cdots + f_r^2) = 2\max_i \deg(f_i)$ für beliebige Polynome $f_1, \dots, f_r \in k[\mathtt{x}]$ (siehe auch 1.2). Für $d \geq 0$ sei

$$k[\mathtt{x}]_{\leq d} := \big\{f \in k[\mathtt{x}]\colon \deg(f) \leq d\big\}.$$

Mit

$$J_d := \{\alpha \in \mathbb{Z}_+^d\colon |\alpha| \leq d\}$$

ist $(\mathtt{x}^\alpha)_{\alpha\in J_d}$ eine Basis des k-Vektorraums $k[\mathtt{x}]_{\leq d}$. Insbesondere ist $\dim(k[\mathtt{x}]_{\leq d}) = |J_d| = \binom{n+d}{d}$. Wir schreiben im folgenden

$$\mathtt{X} := (\mathtt{x}^\alpha)_{\alpha\in J_d} \in k[\mathtt{x}]^{J_d},$$

ein mit J_d indizierter (Spalten-) Vektor, dessen Einträge die Monome vom Grad $\leq d$ sind. Die Abbildung

$$k^{J_d} \to k[\mathtt{x}]_{\leq d}, \quad u = (u_\alpha)_{\alpha\in J_d} \mapsto \mathtt{X}^t \cdot u = \sum_{\alpha\in J_d} u_\alpha \mathtt{x}^\alpha$$

ist ein Vektorraum-Isomorphismus.

1.12 Sei $\mathrm{Sym}_{J_d}(k)$ der Raum der symmetrischen Matrizen, deren Zeilen und Spalten mit J_d indiziert sind. Die lineare Abbildung

$$\gamma\colon \mathrm{Sym}_{J_d}(k) \to k[\mathtt{x}]_{\leq 2d}, \quad \gamma(S) = \mathtt{X}^t S \mathtt{X}$$

heißt die *Gramabbildung*. Für eine symmetrische $J_d \times J_d$-Matrix $S = \big(a_{\alpha\beta}\big)_{\alpha,\beta\in J_d}$ ist also

$$\gamma(S) = \sum_{\alpha,\beta\in J_d} a_{\alpha\beta}\, \mathtt{x}^{\alpha+\beta}.$$

Es ist klar, daß γ surjektiv ist. Für $f \in k[\mathtt{x}]_{\leq 2d}$ sei

$$G_f := \gamma^{-1}(f) = \{S \in \mathrm{Sym}_{J_d}(k)\colon f = \mathtt{X}^t S \mathtt{X}\},$$

ein (nichtleerer) affin-linearer Unterraum des k-Vektorraums $\mathrm{Sym}_{J_d}(k)$. Die Matrizen in G_f heißen die *Grammatrizen* von f. Die Dimension von G_f ist gleich $\dim \mathrm{Sym}_{J_d}(k) - \dim k[\mathtt{x}]_{\leq 2d}$, also

$$\dim(G_f) = \frac{1}{2}\binom{n+d}{n}\left(1 + \binom{n+d}{n}\right) - \binom{n+2d}{n}.$$

1.13 Satz. *Sei k ein reeller Körper. Ein Polynom $f \in k[\mathtt{x}]$ ist genau dann eine Summe von Quadraten von Polynomen, wenn f eine positiv semidefinite Grammatrix hat. Ist dies der Fall, so ist*

$$l(f) = \min\{l(S)\colon S \in G_f,\ S \succeq 0\}.$$

Ist $k = R$ reell abgeschlossen, so ist insbesondere $l(f) = \min\{\mathrm{rk}(S)\colon S \in G_f, S \succeq 0\}$.

Beweis. Schreibe $J = J_d$. Ist $f = \sum_{j=1}^r f_j^2$, so ist $\deg(f_j) \leq d$ für alle j. Sei $B \in M_{J\times r}(k)$ die durch

$$(f_1, \dots, f_r) = \mathtt{X}^t B$$

eindeutig bestimmte Matrix. (Die j-te Spalte von B ist also der Koeffizientenvektor von f_j, für $j = 1, \ldots, r$.) Dann folgt

$$f = (\mathtt{X}^t B)(\mathtt{X}^t B)^t = \mathtt{X}^t (BB^t)\mathtt{X},$$

also ist BB^t eine psd Grammatrix von f, und $l(BB^t) \leq r$. Ist umgekehrt $A \in G_f$ psd, und ist $r = l(A)$, so gibt es $B \in M_{J\times r}(k)$ mit $A = BB^t$. Es folgt $f = \mathtt{X}^t A \mathtt{X} = \sum_{j=1}^r (\mathtt{X}^t B_j)^2$, wobei B_j die j-te Spalte von B ist ($j = 1, \ldots, r$). □

1.14 Definition. Ist $f \in k[\mathtt{x}]$, ist $f = f_1^2 + \cdots + f_r^2$ mit $f_i \in k[\mathtt{x}]$, und ist B die $J \times r$-Matrix mit $\mathtt{X}^t B = (f_1, \ldots, f_r)$, so heißt die symmetrische $J \times J$-Matrix $A = BB^t$ die zur Darstellung $f = \sum_i f_i^2$ *gehörende Grammatrix* von f.

1.15 Bemerkungen.

3. Jede sos-Darstellung von f gibt also eine psd Grammatrix von f, und umgekehrt kommt jede psd Grammatrix von f von einer solchen Darstellung. Es stellt sich also die Frage, wann haben zwei sos Darstellungen dieselbe Grammatrix? Ist

$$f \;=\; f_1^2 + \cdots + f_r^2, \tag{$*$}$$

und ist $U = (u_{ij}) \in O_r(k)$ eine orthogonale Matrix (also $UU^t = I$), so ist auch

$$f \;=\; \Big(\sum_i u_{i1} f_i\Big)^2 + \cdots + \Big(\sum_i u_{ir} f_i\Big)^2, \tag{$**$}$$

und beide Darstellungen ($*$) und ($**$) haben dieselbe Grammatrix. Denn ist etwa $(f_1, \ldots, f_r) = \mathtt{X}^t B$, so hat ($*$) die Grammatrix BB^t, und zu ($**$) korrespondiert $\mathtt{X}^t BU$ mit Grammatrix $(BU)(BU)^t = BB^t$.

1.16 Definition. Zwei Darstellungen

$$f_1^2 + \cdots + f_r^2 \;=\; g_1^2 + \cdots + g_r^2$$

als Summen von r Quadraten (mit f_i, $g_i \in k[\mathtt{x}]$) heißen *orthogonal äquivalent*, wenn $U = (u_{ij}) \in O_r(k)$ existiert mit $g_j = \sum_i u_{ij} f_i$ $(j = 1, \ldots, r)$.

Äquivalente Darstellungen haben dieselbe Grammatrix, wie gerade gesehen. Davon gilt auch die Umkehrung:

1.17 Satz. *Sei k ein reeller Körper. Zwei Darstellungen $f_1^2 + \cdots + f_r^2 = g_1^2 + \cdots + g_r^2$ (mit f_i, $g_i \in k[\mathtt{x}]$) sind genau dann orthogonal äquivalent, wenn sie dieselbe Grammatrix haben.*

1.18 Korollar. *Die psd Grammatrizen von $f \in k[\mathtt{x}]$ stehen in Bijektion zu den orthogonalen Äquivalenzklassen von Darstellungen von f als Summe von Quadraten von Polynomen.* □

Satz 1.17 folgt aus dem folgenden Lemma:

1.19 Lemma. *Sei k ein reeller Körper, seien B, $C \in M_{n\times r}(k)$. Dann sind äquivalent:*

(i) *$BB^t = CC^t$;*
(ii) *es gibt eine orthogonale Matrix $U \in O_r(k)$ mit $C = BU$.*

Beweis. (ii) ⇒ (i) ist trivial. Umgekehrt gelte (i). Für x, $y \in k^r$ sei $\langle x, y\rangle = \sum_{i=1}^r x_i y_i$. Seien V bzw. W die Unterräume von k^r, die von den Zeilen $b_1, \ldots, b_N$

von B bzw. $c_1, \dots, c_n$ von C aufgespannt werden. Nach Voraussetzung gilt $\langle b_i, b_j\rangle = \langle c_i, c_j\rangle$ für alle $i, j = 1, \dots, n$. Sind $\lambda_i \in k$ $(i = 1, \dots, n)$ mit $\sum_i \lambda_i b_i = 0$, so ist

$$\langle \sum_i \lambda_i c_i,\ c_j\rangle = \sum_i \lambda_i \langle c_i, c_j\rangle = \sum_i \lambda_i \langle b_i, b_j\rangle = \langle \sum_i \lambda_i b_i,\ b_j\rangle = 0$$

für $j = 1, \dots, n$. Daraus folgt $\langle \sum_i \lambda_i c_i, \sum_i \lambda_i c_i\rangle = 0$, und daraus $\sum_i \lambda_i c_i = 0$ wegen k reell. Somit gibt es eine lineare Abbildung $\phi_0 \colon V \to W$ mit $\phi_0(b_i) = c_i$ $(i = 1, \dots, n)$, und ϕ_0 ist eine Isometrie von V auf W bezüglich der kanonischen Bilinearform $\langle x, y\rangle = \sum_i x_i y_i$. Wähle eine beliebige Isometrie $\phi_1 \colon V^\perp \to W^\perp$. Dann ist $\phi := \phi_0 \oplus \phi_1$ eine Isometrie von k^r auf sich, welche b_i auf c_i abbildet. Ist $U \in O_r(k)$ die Matrix mit $\phi(x) = Ux$ für alle $x \in k^r$, so folgt $BU^t = C$. □

Für k nichtreell ist Lemma 1.19 falsch.

Für einige Folgerungen setzen wir der Einfachheit halber voraus, daß $k = R$ reell abgeschlossen ist.

1.20 Korollar. *Sei $U \subseteq R[\mathtt{x}]$ ein m-dimensionaler linearer Unterraum, und sei $f \in R[\mathtt{x}]$ eine Summe von Quadraten von Elementen aus U. Dann ist f eine Summe von m Quadraten von Elementen aus U.*

Beweis. Der Rang der zugehörigen psd Grammatrix von f ist $\leq \dim(U) = m$. □

1.21 Korollar. *Jede Quadratsumme f in $R[x_1, \dots, x_n]$ mit $\deg(f) \leq 2d$ ist eine Summe von $\binom{n+d}{n}$ Quadraten.* □

Jetzt betrachten wir Newtonpolytope von Polynomen und wenden sie auf Quadratsummen an.

1.23 Definition. Sei k ein Körper, sei $f = \sum_{\alpha \in \mathbb{Z}_+^n} a_\alpha\, \mathtt{x}^\alpha$ ein Polynom in $k[\mathtt{x}] = k[x_1, \dots, x_n]$. Der *Träger* von f ist die Menge

$$\operatorname{supp}(f) \ :=\ \{\alpha \in \mathbb{Z}_+^n \colon a_\alpha \neq 0\}$$

der in f vorkommenden Monome (bzw. ihrer Exponententupel). Das *Newtonpolytop* von f ist

$$\operatorname{New}(f) \ :=\ \operatorname{conv}(\operatorname{supp}(f)),$$

die konvexe Hülle von $\operatorname{supp}(f)$ in $\mathbb{R}^n$.

1.24 Bemerkungen.

2. Als konvexe Hülle endlich vieler Punkte im $\mathbb{R}^n$ ist $\operatorname{New}(f)$ ein Polytop, also ein kompakter Durchschnitt von endlich vielen abgeschlossenen affin-linearen Halbräumen. Für $0 \neq u \in \mathbb{R}^n$ und $c \in \mathbb{R}$ sei im folgenden

$$H_{u,c} \ :=\ \big\{x \in \mathbb{R}^n \colon \langle x, u\rangle \leq c\big\}.$$

Jeder abgeschlossene Halbraum hat so eine Form. (Hier ist wie üblich $\langle u, x\rangle = \sum_{i=1}^n u_i x_i$.)

1.25 Jeder feste Vektor $0 \neq u \in \mathbb{R}^n$ definiert eine Graduierung des Polynomrings $k[\mathtt{x}]$ dadurch, daß man die Variable x_i als homogen vom Grad u_i definiert $(i = 1, \dots, n)$. Das Monom $\mathtt{x}^\alpha$ ist also homogen vom Grad $\langle \alpha, u\rangle$. Die Graduierungsgruppe ist die von $u_1, \dots, u_n$ erzeugte Untergruppe G von $\mathbb{R}$. Es ist

$$k[\mathtt{x}] \ =\ \bigoplus_{g \in G} k[\mathtt{x}]_g,$$

und jede homogene Komponente $k[\mathrm{x}]_g$ ist ein von Monomen aufgespannter k-Vektorraum. Nenne ein Polynom u-homogen, wenn es homogen bezüglich dieser Graduierung ist.

Sei $0 \neq f \in k[\mathrm{x}]$, schreibe $f = \sum_{g\in G} f_g$ mit $f_g \in k[\mathrm{x}]_g$ für $g \in G$. Der u-Grad von f ist

$$\deg_u(f) \;=\; \max\{g \in G\colon f_g \neq 0\} \;=\; \max\{\langle \alpha, u\rangle \colon \alpha \in \operatorname{supp}(f)\}.$$

Sei $\deg_u(f) = g$, dann heißt $L_u(f) := f_g$ die *u-Leitform* von f. Die u-Leitform ist $\neq 0$ und u-homogen. Für Polynome $f_1, f_2 \neq 0$ gilt $\deg_u(f_1 f_2) = \deg_u(f_1) + \deg_u(f_2)$ und $L_u(f_1 f_2) = L_u(f_1)\, L_u(f_2)$.

Genau dann gilt demnach $\operatorname{New}(f) \subseteq H_{u,c}$, wenn $\deg_u(f) \leq c$ ist. Denn $\operatorname{New}(f) \subseteq H_{u,c}$ bedeutet $\langle \alpha, u\rangle \leq c$ für alle $\alpha \in \operatorname{supp}(f)$.

1.27 Satz. *Sei $0 \neq f \in R[\mathrm{x}]$. Für $u = (u_1, \ldots, u_n) \in \mathbb{Q}^n$ und $c \in \mathbb{Q}$ sind äquivalent:*

(i) $\operatorname{New}(f) \subseteq H_{u,c}$;
(ii) *für alle $\xi \in R^n$ bleibt $t^{-c} \cdot f\big(\xi_1 t^{u_1}, \ldots, \xi_n t^{u_n}\big)$ beschränkt für $t \to \infty$, $t \in R$.*

Beweis. Sei $f = f_{g_1} + \cdots + f_{g_r}$ die Zerlegung in u-homogene Komponenten $\neq 0$, mit $\deg_u(f) = g_1 > \cdots > g_r$. Bedingung (i) bedeutet $g_1 \leq c$ (siehe 1.25). Fixiere $\xi \in R^n$ und setze $\eta_t := \big(\xi_1 t^{u_1}, \ldots, \xi_n t^{u_n}\big)$ für $t > 0$. Nach Beispiel 1.26.2 ist

$$f(\eta_t) \;=\; \sum_{i=1}^{r} f_{g_i}(\xi)\, t^{g_i}. \qquad (*)$$

Aus (i) folgt $g_i \leq c$ für alle i, also bleibt dann $t^{-c} f(\eta_t)$ beschränkt für $t \to \infty$. Für die Umkehrung wähle $\xi \in R^n$ mit $f_{g_1}(\xi) \neq 0$. Die höchste Potenz von t in $t^{-c} f(\eta_t)$ ist dann $t^{g_1 - c}$. Aus (ii) folgt also $g_1 - c \leq 0$, also (i). □

1.28 Satz. *Seien $0 \neq f, g \in R[\mathrm{x}]$.*

(a) $\operatorname{New}(fg) = \operatorname{New}(f) + \operatorname{New}(g)$.
(b) *Sind f, g psd, so ist* $\operatorname{New}(f+g) = \operatorname{conv}(\operatorname{New}(f) \cup \operatorname{New}(g))$.

Hierbei ist $C_1 + C_2 = \{x + y\colon x \in C_1,\, y \in C_2\}$, die *Minkowskisumme* von C_1 und C_2. Sind C_1 und C_2 kompakt oder konvex, so gilt dasselbe auch für $C_1 + C_2$.

Beweis. (a) Jedes Monom von fg ist Produkt eines Monoms von f und eines Monoms von g. Also gilt $\operatorname{supp}(fg) \subseteq \operatorname{supp}(f) + \operatorname{supp}(g)$, und daher $\operatorname{New}(fg) \subseteq \operatorname{New}(f) + \operatorname{New}(g)$. Für die Umkehrung genügt es, zu zeigen: Sind $0 \neq u \in \mathbb{R}^n$ und $c \in \mathbb{R}$ mit $\operatorname{New}(fg) \subseteq H_{u,c}$, so ist auch $\operatorname{New}(f) + \operatorname{New}(g) \subseteq H_{u,c}$. Die Voraussetzung sagt $\deg_u(fg) \leq c$. Sei $a = \deg_u(f)$ und $b = \deg_u(g)$. Es ist also $a + b = \deg_u(fg) \leq c$ und $\operatorname{New}(f) \subseteq H_{u,a}$, $\operatorname{New}(g) \subseteq H_{u,b}$. Es folgt $\operatorname{New}(f) + \operatorname{New}(g) \subseteq H_{u,a} + H_{u,b} = H_{u,a+b} \subseteq H_{u,c}$ wie gewünscht.

(b) Wegen $\operatorname{supp}(f+g) \subseteq \operatorname{supp}(f) \cup \operatorname{supp}(g)$ ist $\subseteq$ klar. Es bleibt $\operatorname{New}(f) \cup \operatorname{New}(g) \subseteq \operatorname{New}(f+g)$ zu zeigen. Dafür genügt, daß aus $\operatorname{New}(f+g) \subseteq H_{u,c}$ auch $\operatorname{New}(f) \cup \operatorname{New}(g) \subseteq H_{u,c}$ folgt. Dazu benutzen wir Satz 1.27. Sei $\xi \in R^n$ und $\eta_t = (\xi_1 t^{u_1}, \ldots, \xi_n t^{u_n})$ $(t > 0)$. Die Voraussetzung sagt, daß $t^{-c}\big(f(\eta_t) + g(\eta_t)\big)$ für $t \to \infty$ beschränkt ist. Wegen f, g psd folgt daraus die Beschränktheit von $t^{-c} f(\eta_t)$ und von $t^{-c} g(\eta_t)$, also die Behauptung nach dem Satz. □

1.29 Bemerkung. Ist $C \subseteq \mathbb{R}^n$ eine konvexe Menge, so ist die m-fache Minkowskisumme $C + \cdots + C$ gleich $mC = \{mx\colon x \in C\}$. Aus Satz 1.28(a) folgt also $\operatorname{New}(f^m) = m \operatorname{New}(f)$ für alle $m \geq 1$.

1.30 Korollar. *Sei $f = f_1^2 + \cdots + f_r^2$ mit Polynomen $f_i \in R[\mathbf{x}]$. Dann gilt* $\mathrm{New}(f_i) \subseteq \frac{1}{2}\,\mathrm{New}(f)$ *für* $i = 1, \ldots, r$.

1.31 Korollar. *Sei $f \in R[\mathbf{x}]$ eine Quadratsumme. Ist N die Anzahl der in* $\frac{1}{2}\,\mathrm{New}(f)$ *enthaltenen Gitterpunkte, so ist jede Quadratsummendarstellung von f äquivalent zu einer Summe von N Quadraten.*

1.32 Beispiele.

1. Das Motzkinpolynom $f = x^4y^2 + x^2y^4 - 3x^2y^2 + 1$ ist psd, wie aus der arithmetisch-geometrischen Ungleichung folgt:

$$\frac{1}{3}\Big(1 + x^4y^2 + x^2y^4\Big) \;\geq\; \sqrt[3]{1 \cdot x^4y^2 \cdot x^2y^4}.$$

Andererseits ist f nicht sos, wie man durch Terminspektion einer hypothetischen sos-Darstellung sieht (Aufgabe 13). Die Argumentation vereinfacht sich, wenn man das Newtonpolytop benutzt: $\frac{1}{2}\mathrm{New}(f)$ ist die konvexe Hülle von $(2,1)$, $(1,2)$, $(1,1)$ und $(0,0)$. Nur diese vier Gitterpunkte sind darin enthalten. Wäre f sos, so müßte

$$f \;=\; \sum_i (a_i x^2 y + b_i x y^2 + c_i x y + d_i)^2$$

sein. Dann aber ist der Koeffizient von x^2y^2 gleich $\sum_i c_i^2 \geq 0$, kann also nicht -3 sein.

2. Das Motzkinpolynom hat vier Nullstellen in R^2, nämlich $(\pm 1, \pm 1)$. Für jedes $c > 0$ in R ist $f_c := f + c$ strikt positiv auf R^2, und ist nicht sos, denn an dem gerade gegebenen Argument ändert sich nichts.

3. Das folgende Beispiel stammt von Choi und Lam: Die Form

$$f \;=\; w^4 + x^2y^2 + x^2z^2 + y^2z^2 - 4wxyz$$

in $R[w,x,y,z]$ ist psd, wieder nach der arithmetisch-geometrischen Ungleichung, angewandt auf w^4, x^2y^2, x^2z^2 und y^2z^2. Und f ist nicht sos, denn $\frac{1}{2}\mathrm{New}(f)$ ist die konvexe Hülle von

$$(2,0,0,0),\;\; (0,1,1,0),\;\; (0,1,0,1),\;\; (0,0,1,1).$$

Die einzigen Gitterpunkte in $\frac{1}{2}\mathrm{New}(f)$ sind diese vier Punkte. Wäre f sos, so müßte also

$$f \;=\; \sum_i (a_i w^2 + b_i xy + c_i xz + d_i yz)^2$$

sein, was nicht der Fall ist. Also ist f nicht sos.

2. Hilberts Theorem über Quadratsummen von Polynomen

2.1 Sei k ein Körper. Ist $f \in k[x_0, \ldots, x_n]$ homogen, so sei $\widetilde{f} \in k[x_1, \ldots, x_n]$ die Dehomogenisierung von f bezüglich x_0, also

$$\widetilde{f} \;=\; f(1, x_1, \ldots, x_n).$$

Für $g \in k[x_1, \ldots, x_n]$ sei umgekehrt g^h die Homogenisierung von g, also

$$g^h \;=\; x_0^{\deg(g)}\, g\Big(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}\Big)$$

(für $g \neq 0$, und $0^h = 0$), wobei $\deg(g)$ der Totalgrad von g ist. Es ist also $g^h \in k[x_0, \ldots, x_n]$ homogen vom Grad $\deg(g)$, und $g = \widetilde{g^h}$ ist die Dehomogenisierung von g^h. Für $0 \neq f \in k[x_0, \ldots, x_n]$ homogen ist andererseits $f = x_0^m \cdot (\widetilde{f})^h$, wobei $m \geq 0$ maximal mit $x_0^m \mid f$ ist.

2.2 Lemma. *Sei k reell. Ein homogenes (bzw. beliebiges) Polynom über k ist genau dann psd, wenn seine Dehomogenisierung (bzw. seine Homogenisierung) dies ist. Dieselbe Aussage gilt mit sos statt psd.*

Wir können also wahlweise über homogene Polynome in $n+1$ Variablen oder über beliebige Polynome in n Variablen reden. Wir nehmen hier den homogenen Standpunkt ein, wie es auch Hilbert getan hat. Ist ein homogenes Polynom eine Quadratsumme von Polynomen, so sind bei reellem Grundkörper die Summanden automatisch selbst homogen:

2.3 Lemma. *Sei k ein reeller Körper, seien $f_1, \dots, f_r \in k[\mathtt{x}]$ Polynome, und sei $f = f_1^2 + \cdots + f_r^2$ homogen vom Grad d. Dann ist d gerade, und die f_i sind homogen vom Grad $\frac{d}{2}$.*

2.4 Sei im weiteren R ein reell abgeschlossener Körper, und sei $n \geq 1$. Wir betrachten homogene Polynome (Formen) $f \in R[\mathtt{x}]$ in n Variablen $\mathtt{x} = (x_1, \dots, x_n)$. Für $d \geq 0$ sei $R[\mathtt{x}]_d$ der R-Vektorraum aller solchen Formen vom Grad d. Es sei weiter

$$P_{n,d} \;=\; \{f \in R[\mathtt{x}]_d \colon f \text{ ist psd}\}$$

die Menge aller psd Formen vom Grad d, und

$$\Sigma_{n,d} \;=\; \Big\{ f \in R[\mathtt{x}]_d \colon \exists\, r \geq 0,\ \exists\, f_1, \dots, f_r \in R[\mathtt{x}] \text{ mit } f = \sum_{i=1}^{r} f_i^2 \Big\}$$

die Menge aller Formen vom Grad d, welche eine Quadratsumme von Polynomen (notwendig von Formen vom Grad $\frac{d}{2}$) sind. Offensichtlich gilt $\Sigma_{n,d} \subseteq P_{n,d}$.

2.5 Satz. *Die Teilmengen $P_{n,d}$ und $\Sigma_{n,d}$ von $R[\mathtt{x}]_d$ sind abgeschlossene konvexe semialgebraische Kegel mit nichtleerem Innerem (für d gerade).*

Beweis. Beide Mengen $P_{n,d}$ und $\Sigma_{n,d}$ sind konvexe Kegel, d.h. sie enthalten mit f_1, f_2 auch $f_1 + f_2$ und af_1 (für $a \geq 0$). Für die Aussage, daß $\Sigma_{n,d}$ nichtleeres Inneres hat, siehe RAG II (SS 2016), Aufgabe 1.

$P_{n,d}$ läßt sich durch eine Formel in den Koeffizienten beschreiben, ist also eine semialgebraische Menge. Die Abgeschlossenheit von $P_{n,d}$ ist trivial, denn für jeden Punkt $\xi \in R^n$ ist die Auswertungsabbildung $R[\mathtt{x}]_d \to R$, $f \mapsto f(\xi)$ linear, und insbesondere stetig.

Sei $d = 2e$, und sei $N = \dim R[\mathtt{x}]_e$ (also $N = \binom{n-1+e}{e}$). Nach 1.20 ist $\Sigma_{n,d}$ das Bild der Abbildung

$$\phi \colon (R[\mathtt{x}]_e)^N \to R[\mathtt{x}]_d, \quad (f_1, \dots, f_N) \mapsto f_1^2 + \cdots + f_N^2,$$

und ist daher eine semialgebraische Menge. Die Abbildung ϕ ist polynomial und homogen vom Grad 2, und es gilt $\phi^{-1}(0) = \{0\}$. Nach dem folgenden Lemma ist deshalb $\mathrm{im}(\phi) = \Sigma_{n,d}$ abgeschlossen in $R[\mathtt{x}]_d$.

2.6 Lemma. *Sei $f \colon R^m \to R^n$ eine semialgebraische Abbildung. Es sei f homogen von geradem Grad d, d.h. es gelte $f(ax) = a^d f(x)$ für alle $x \in R^m$ und $a \in R$. Außerdem sei $f^{-1}(0) = \{0\}$. Sei $M \subseteq R^m$ eine abgeschlossene semialgebraische Menge mit $x \in M \Rightarrow ax \in M$ für alle $a \geq 0$. Dann ist auch die Menge $f(M)$ abgeschlossen in R^n.*

Beweis. Sei $S^{n-1} \subseteq R^n$ die Einheitssphäre, und sei

$$p \colon R^n \smallsetminus \{0\} \to S^{n-1}, \quad p(\xi) = \frac{\xi}{|\xi|} \quad (0 \neq \xi \in R^n).$$

Ist $B \subseteq S^{n-1}$ eine abgeschlossene Teilmenge, so ist die Menge $\widehat{B} := p^{-1}(B) \cup \{0\}$ abgeschlossen in R^n. Für $A := M \cap S^{m-1}$ ist $0 \notin f(A)$ nach Voraussetzung, also ist $p \circ f(A) \subseteq S^{n-1}$ eine abgeschlossene Menge. Es gilt $f(M) = \widehat{p \circ f(A)}$, also ist $f(M)$ abgeschlossen in R^n. □

Damit ist Satz 2.5 bewiesen. □

Angeregt durch Minkowski überlegte Hilbert, ob jede psd Form $f \in P_{n,d}$ eine Quadratsumme von Formen ist. Es gibt einige einfache Fälle, wo die Antwort ja ist:

2.7 Lemma. *Sei* $\mathtt{x} = (x_1, \ldots, x_n)$*, sei* $f \in P_{n,d} \subseteq R[\mathtt{x}]$*.*

(a) *Ist* $n = 1$*, so ist* f *ein Quadrat.*
(b) *Ist* $n = 2$*, so ist* f *Summe von zwei Quadraten.*
(c) *Ist* $d = 2$*, so ist* f *Summe von* n *Quadraten.*

2.8 Theorem. (Hilbert 1888) *Seien* $n \geq 1$ *und* $d \geq 0$ *mit* d *gerade. Ist* $n \leq 2$ *oder* $d \leq 2$*, oder ist* $(n, d) = (3, 4)$*, so ist* $\Sigma_{n,d} = P_{n,d}$*. In allen anderen Fällen ist die Inklusion* $\Sigma_{n,d} \subseteq P_{n,d}$ *strikt.*

Beweis. Die offensichtlichen Fälle ($n \leq 2$ oder $d \leq 2$) haben wir gerade diskutiert. Das Motzkinpolynom f liegt in $P_{3,6} \smallsetminus \Sigma_{3,6}$ (Aufgabe 7, oder 1.32), und damit auch in $P_{n,6} \smallsetminus \Sigma_{n,6}$ für alle $n \geq 3$. Für alle $k \geq 0$ und $n \geq 3$ liegt deshalb auch $x_1^{2k} f$ in $P_{n,6+2k} \smallsetminus \Sigma_{n,6+2k}$. Das Choi-Lam Polynom aus 1.32.3 liegt in $P_{4,4} \smallsetminus \Sigma_{4,4}$, also auch in $P_{n,4} \smallsetminus \Sigma_{n,4}$ für alle $n \geq 4$.

Zu zeigen bleibt $P_{3,4} = \Sigma_{3,4}$. Hier hat Hilbert sogar eine noch stärkere Aussage gezeigt: Jede psd ternäre Form vom Grad 4 ist eine Summe von drei Quadraten von quadratischen Formen. Mit elementaren Argumenten zeigen wir eine etwas schwächere Aussage:

2.9 Satz. *Sei* $f \in R[x, y, z]$ *eine psd Form vom Grad* 4*.*

(a) *Hat* f *eine nichttriviale reelle Nullstelle, so ist* f *eine Summe von* 3 *Quadraten.*
(b) *Stets ist* f *eine Summe von* 4 *Quadraten.*

Beweis. (b) folgt aus (a). Sei nämlich $a := \min f(S^2)$ das Minimum von f auf der Einheitssphäre. Die quartische Form

$$g \;:=\; f(x, y, z) - a(x^2 + y^2 + z^2)^2$$

erfüllt dann $g \geq 0$ auf S^2, also ist auch g psd. Nach Voraussetzung hat g eine Nullstelle in S^2, ist also nach (a) eine g Summe von 3 Quadraten. Daher ist f Summe von 4 Quadraten.

Es bleibt (a) zu zeigen. Der folgende Beweis stammt von Pfister.

2.10 Definition. Eine Form $p \in R[x_0, \ldots, x_n]$ heißt *positiv definit*, wenn $p(\xi) > 0$ für alle $0 \neq \xi \in R^n$ gilt.

2.11 Lemma. *Sei* $q \in R[s, t]$ *eine binäre positiv definite Form mit* $\deg(q) = 2$*. Für jede psd Form* $f \in R[s, t]$ *gibt es Formen* g*,* $h \in R[s, t]$ *mit*

$$f \;=\; g^2 + qh^2. \tag{1}$$

Beweis. Wir beweisen die Version für inhomogene univariate Polynome. Sei also $q \in R[t]$ mit $\deg(q) = 2$ und $q(t) > 0$ für alle $t \in R$. Wir können q mit jeder positiven Zahl in R skalieren. Es ist $q = (at+b)^2+c^2$ mit $ac \neq 0$, also $q = c^2(u^2+1)$ mit $u = c^{-1}(at + b)$. Wegen $R[t] = R[u]$ können wir also annehmen $q = t^2 + 1$.

Sei $f \in R[t]$ psd, und sei zunächst $\deg(f) = 2$, etwa $f = (t+a)^2 + b^2$ mit $a, b \in R$. Ist $a = 0$, so ist $f = (b^2-1) + q$ (falls $b^2 \geq 1$) bzw. $f = (1-b^2)t^2 + b^2 q$ (falls $b^2 \leq 1$) eine Darstellung wie gewünscht. Sei jetzt $a \neq 0$. Wir suchen $\lambda \in R$ mit $\lambda \geq 0$, so daß

$$f - \lambda q \;=\; f - \lambda(t^2+1) \;=\; (1-\lambda)t^2 + 2at + (a^2+b^2-\lambda)$$

ein Quadrat ist. Dafür genügt, daß $0 \leq \lambda < 1$ ist und die Diskriminante

$$\delta(\lambda) \;:=\; 4a^2 - 4(1-\lambda)(a^2+b^2-\lambda) \;=\; -4\Big(\lambda^2 - (a^2+b^2+1)\lambda + b^2\Big)$$

verschwindet. Wegen $\delta(0) = -4b^2 \leq 0$ und $\delta(1) = 4a^2 > 0$ hat δ eine Nullstelle λ mit $0 \leq \lambda < 1$.

Ein beliebiges psd Polynom $f \in R[t]$ ist ein Produkt von quadratischen psd Polynomen. Aus dem gerade behandelten Fall folgt wegen

$$(a^2+b^2q)(c^2+d^2q) \;=\; (ac+bdq)^2 + (ad-bc)^2 q,$$

daß f eine Darstellung (1) hat. □

2.12 Wir beweisen nun Satz 2.9(a). Sei $f = f(x,y,z)$ eine psd Form vom Grad 4 mit einer nichttrivialen reellen Nullstelle. Nach einem linearen Koordinatenwechsel erreichen wir $f(0,0,1) = 0$, also

$$f \;=\; f_2(x,y)\cdot z^2 + f_3(x,y)\cdot z + f_4(x,y), \tag{2}$$

wobei $f_j = f_j(x,y)$ eine binäre Form vom Grad j ist ($j = 2,3,4$). Wegen f psd ist jede der drei binären Formen

$$f_2,\; f_4,\; 4f_2f_4 - f_3^2$$

selbst psd, also eine Summe von zwei Quadraten. Ist $f_2 = 0$, so auch $f_3 = 0$, also ist $f = f_4$ eine Summe von zwei Quadraten. Ist $f_2 = l^2$ Quadrat einer Linearform $l \neq 0$, so folgt $l \mid f_3$ (Lemma 1.1 auf $4f_2f_4 - f_3^2$ anwenden), etwa $f_3 = 2lg_2$. Da $4f_2f_4 - f_3^2 = 4l^2(f_4 - g_2^2)$ Summe von zwei Quadraten ist, ist auch $f_4 - g_2^2$ eine Summe von zwei Quadraten. Also ist $f = (lz+g_2)^2 + (f_4 - g_2^2)$ eine Summe von drei Quadraten.

Jetzt sei f_2 positiv definit. Nach Lemma 2.11 existieren binäre Formen $p = p(x,y)$ und $q = q(x,y)$ mit $4f_2f_4 - f_3^2 = q^2 + p^2 f_2$, also

$$q^2 + f_3^2 \;=\; f_2(4f_4 - p^2). \tag{3}$$

Dabei ist $\deg(p) = 2$ und $\deg(q) = 3$. Wegen f_2 psd gibt es Linearformen l_1, $l_2 \in R[x,y]$ with $f_2 = l_1^2 + l_2^2 = (l_1 + il_2)(l_1 - il_2)$ (und $i = \sqrt{-1}$). Aus (3) folgt also, daß $l_1 + il_2$ eine der beiden Formen $q \pm if_3$ teilt. Indem wir gegebenenfalls l_2 durch $-l_2$ ersetzen, können wir annehmen

$$(l_1 + il_2) \;\mid\; (q + if_3).$$

Damit ist f_2 ein Teiler von $(q+if_3)(l_1 - il_2) = (ql_1 + f_3l_2) + i(f_3l_1 - ql_2)$, also auch von Real- und Imaginärteil dieser Form. Die Brüche

$$h_1 \;:=\; \frac{f_3l_1 - ql_2}{2f_2}, \qquad h_2 \;:=\; \frac{ql_1 + f_3l_2}{2f_2}$$

sind also binäre quadratische Formen (mit Koeffizienten in R), und aus (3) folgt

$$h_1^2 + h_2^2 \;=\; \frac{(q^2+f_3^2)(l_1^2+l_2^2)}{4f_2^2} \;=\; \frac{q^2+f_3^2}{4f_2} \;=\; f_4 - \frac{1}{4}p^2.$$

Wegen

$$h_1l_1 + h_2l_2 \;=\; \frac{f_3(l_1^2+l_2^2)}{2f_2} \;=\; \frac{1}{2}\,f_3$$

ist also

$$f \;=\; \Big(\frac{p}{2}\Big)^2 + (h_1 + l_1 z)^2 + (h_2 + l_2 z)^2$$

eine Summe von drei Quadraten quadratischer Formen. □

Damit ist Theorem 2.8 bewiesen. □

Die Frage, wann jedes psd Polynom eine Darstellung als Quadratsumme hat, hat weitreichende Verallgemeinerungen in viele Richtungen, und hat wichtige Anwendungen in der Optimierung. Für den Moment geben wir zwei weitere Fälle an, wo alle nichtnegativen Polynome durch Quadratsummen beschrieben werden.

2.14 Betrachte allgemeiner eine affine R-Varietät V und eine basisch abgeschlossene semialgebraische Teilmenge $K \subseteq V(R)$, etwa

$$K \;=\; \big\{\xi \in V(R)\colon g_1(\xi) \geq 0, \ldots, g_r(\xi) \geq 0\big\}$$

mit $g_1, \ldots, g_r \in R[V]$. Sei $f \in R[V]$ mit $f(\xi) \geq 0$ für alle $\xi \in K$. Unter welchen Voraussetzungen kann man folgern, daß f in der Präordnung $PO(g_1, \ldots, g_r) \subseteq R[V]$ liegt, also eine gewichtete Quadratsummendarstellung

$$f \;=\; \sum_{e_1=0}^{1} \cdots \sum_{e_r=0}^{1} s_e\, g_1^{e_1} \cdots g_r^{e_r}$$

mit $s_e \in \Sigma R[V]^2$ für alle $e = (e_1, \ldots, e_r) \in \{0,1\}^r$ hat?

Die Frage ist im allgemeinen schwierig. Hier ein erstes explizites Beispiel:

2.15 Sei $K \subseteq R$ eine abgeschlossene semialgebraische Menge, $K \neq \varnothing$, R. Dann hat K die Gestalt

$$K \;=\;]-\infty, b_0] \cup [a_1, b_1] \cup \cdots \cup [a_m, b_m] \cup [a_{m+1}, \infty[$$

mit $m \geq 0$ und

$$-\infty \leq b_0 < a_1 \leq b_1 < \cdots < a_m \leq b_m < a_{m+1} \leq \infty.$$

(Dabei sei $]-\infty, -\infty] := [\infty, \infty[:= \varnothing$.) Die Polynome

$$p_i \;:=\; (x - b_i)(x - a_{i+1}) \quad (i = 0, \ldots, m)$$

(mit $x - b_0 := 1$ falls $b_0 = -\infty$, und $x - a_{m+1} := -1$ falls $a_{m+1} = \infty$) heißen die *natürlichen Erzeuger* von K. Es ist $K = \{t \in R\colon p_0(t) \geq 0, \ldots, p_m(t) \geq 0\}$. Sei

$$\mathcal{P}(K) \;=\; \{f \in R[x]\colon f|_K \geq 0\},$$

die Präordnung aller auf K nichtnegativen Polynome in $R[x]$.

2.16 Satz. *Seien K und die natürlichen Erzeuger $p_0, \ldots, p_m$ wie oben.*

(a) *Es ist $\mathcal{P}(K) = PO(p_0, \ldots, p_m)$.*
(b) *Ist umgekehrt $P \subseteq \mathcal{P}(K)$ eine Teilmenge mit $\mathcal{P}(K) = PO(P)$, und ist K unbeschränkt, so gibt es $c_0, \ldots, c_m > 0$ in R mit $c_0 p_0, \ldots, c_m p_m \in P$.*

Beweis. (a) Wir zeigen (a) nur unter der Annahme, daß K keinen isolierten Punkt hat, d.h. daß $a_i < b_i$ für $i = 1, \ldots, m$ gilt. Sei $f \in R[x]$ ein Polynom mit $f|_K \geq 0$. Wir können annehmen, daß alle komplexen Nullstellen von f reell und einfach sind. In jedem der Intervalle $[b_1, a_2], \ldots, [b_{m-1}, a_m]$ hat f eine gerade Anzahl von Nullstellen. Deshalb genügt es, zu zeigen:

(1) Für $b \leq \alpha < \beta \leq a$ ist $(x - \alpha)(x - \beta) \in PO((x - b)(x - a))$;
(2) für $\alpha \leq a$ ist $x - \alpha \in PO(x - a)$, für $\beta \geq b$ ist $\beta - x \in PO(b - x)$.

Die Aussagen (2) sind offensichtlich. Für (1) siehe Aufgabe 52.

(b) Sei K unbeschränkt, sei $p = p_i$ für ein $i \in \{0, \dots, m\}$. Behaupte: Ist $p = q_1 + q_2$ mit $q_1, q_2 \geq 0$ auf K, so ist $q_j = c_j p$ mit $c_j \geq 0$ (und $c_1 + c_2 = 1$). (Anders gesagt, p erzeugt einen Extremalstrahl des konvexen Kegels $\mathcal{P}(K)$.) Denn wegen K unbeschränkt ist $\deg(q_j) \leq \deg(p)$ (≤ 2) für $j = 1, 2$. Da die q_i in den Nullstellen von p verschwinden müssen, folgt die Behauptung. Sind also $f_1, \dots, f_r \in \mathcal{P}(K)$, und ist

$$p \;=\; \sum_{e \in \{0,1\}^r} s_e \cdot f_1^{e_1} \cdots f_r^{e_r}$$

mit Quadratsummen s_e in $R[x]$, so liegt jeder Summand in R_+p, und es folgt $f_j \in R_+p$ für ein $j \in \{1, \dots, r\}$. (Denn aus der expliziten Gestalt von p sieht man, daß p nicht Produkt von zwei nichtkonstanten Faktoren aus $\mathcal{P}(K)$ ist.) □

2.17 Bemerkungen.

1. Seien $g_1, \dots, g_r \in R[x]$, sei $K = \{g_1 \geq 0, \dots, g_r \geq 0\} \subseteq R$. Ob die Inklusion

$$PO(g_1, \dots, g_r) \;\subseteq\; \mathcal{P}(K)$$

eine Gleichheit ist, hängt stark von der Wahl der Ungleichungen g_i ab, wie man aus Satz 2.16 sieht. Sind $p_0, \dots, p_m$ die natürlichen Erzeuger und $p = p_0 \cdots p_m$, so ist auch $K = \{p \geq 0\}$, aber $PO(p) \neq \mathcal{P}(K)$ gilt fast immer, wenn K unbeschränkt ist (nämlich wenn $m \geq 1$ ist).

2. Ist dagegen $R = \mathbb{R}$ und $K \subseteq \mathbb{R}$ kompakt, so wird $\mathcal{P}(K)$ von zwei Polynomen erzeugt, und sogar von einem einzigen, z.B. von $p_0 \cdots p_m$, falls K keine isolierten Punkte enthält. Das zeigen wir später.

Nun diskutieren wir ein klassisches Resultat, nämlich die nichtnegativen Polynome auf der Kreislinie. Sei C die affine Kurve $x^2 + y^2 = 1$ über R, es ist also $C(R) = \{(s,t) \in R^2 \colon s^2 + t^2 = 1\}$. Der Koordinatenring von C ist $R[C] = R[x,y]/(x^2 + y^2 - 1)$.

2.18 Satz. *Jedes psd Element in $R[C]$ ist eine Summe von zwei Quadraten in $R[C]$.*

Hier ist eine andere Version des Satzes. Betrachte den Ring $\mathbb{C}[z, z^{-1}]$ der Laurentpolynome, zusammen mit der $\mathbb{C}/\mathbb{R}$-Involution $f \mapsto f^*$ mit $a^* = \overline{a}$ ($a \in \mathbb{C}$), $z^* = z^{-1}$ (also auch $(z^{-1})^* = z$). Für $f = \sum_{n \in \mathbb{Z}} a_n z^n \in \mathbb{C}[z, z^{-1}]$ ist also $f^* = \sum_n \overline{a}_n z^{-n}$, und für $0 \neq \alpha \in \mathbb{C}$ folgt $\overline{f^*(\alpha)} = f(\overline{\alpha}^{-1})$. Ist insbesondere $f = f^*$, so ist $f(\alpha) \in \mathbb{R}$ für alle $|\alpha| = 1$.

2.19 Theorem. (Fejér-Riesz) *Sei $f \in \mathbb{C}[z, z^{-1}]$ mit $f = f^*$. Ist $f \geq 0$ auf $S = \{u \in \mathbb{C} \colon |u| = 1\}$, so gibt es $g \in \mathbb{C}[z]$ mit $f = gg^*$. Genauer gilt: Ist $n \in \mathbb{N}$ mit $z^n f \in \mathbb{C}[z]$, so gibt es ein solches g mit $\deg(g) = n$.*

Beweis. Sei $0 \neq f \in \mathbb{C}[z, z^{-1}]$ mit $f = f^*$ und $z^n f \in \mathbb{C}[z]$. Wir können annehmen $z^{n-1} f \notin \mathbb{C}[z]$. Dann hat f die Gestalt $f = \sum_{j=-n}^{n} c_j z^j$ mit $c_{-j} = \overline{c}_j$ für alle j. Also ist

$$f \;=\; c z^{-n} \prod_{j=1}^{2n} (z - \alpha_j)$$

mit $c \in \mathbb{C}^*$, wobei $\alpha_1, \dots, \alpha_{2n}$ die Nullstellen von f in $\mathbb{C} \setminus \{0\}$ sind. Wegen $f = f^*$ existiert eine Permutation σ von $1, \dots, 2n$ mit $\alpha_j \overline{\alpha_{\sigma(j)}} = 1$ für alle j. Für die Konstante c gilt $\overline{c} = c \prod_j \alpha_j$.

Sei α eine Nullstelle von f mit $|\alpha| = 1$, sei m die Vielfachheit von α. Die Restriktion $f|_S$ wechselt in α genau dann das Vorzeichen, wenn m ungerade ist (lokale Überlegung, Übung). Ist also $f|_S \geq 0$, so kommt jede Nullstelle in S mit gerader Vielfachheit vor. Also kann man n Nullstellen $\beta_1, \ldots, \beta_n$ aus den $2n$ Nullstellen von f so auswählen, daß

$$f \;=\; cz^{-n} \prod_{j=1}^{n} (z - \beta_j)(z - \overline{\beta}_j^{-1})$$

ist. Die Konstante c erfüllt $\overline{c} = c \prod_j \frac{\beta_j}{\overline{\beta}_j}$, also $c = s \prod_j \overline{\beta}_j$ mit $0 \neq s \in \mathbb{R}$. Also ist f Produkt von n Faktoren der Form

$$\frac{\overline{\beta}}{z}(z - \beta)\Big(z - \frac{1}{\overline{\beta}}\Big) \;=\; -(z - \beta)(z^{-1} - \overline{\beta}) \;=\; -(z - \beta)(z - \beta)^*.$$

Es folgt $f = tgg^*$ mit $0 \neq t \in \mathbb{R}$ und $g = \prod_{j=1}^{n}(z - \beta_j)$. Wegen $f \geq 0$ auf S muß dabei $t > 0$ sein. □

2.20 Bemerkung. Der Zusammenhang mit der Formulierung 2.18 wird wie folgt hergestellt: Durch

$$\mathbb{C}[z, z^{-1}] \to \mathbb{C}[x, y]/(x^2 + y^2 - 1), \quad z \mapsto x + iy$$

ist ein Isomorphismus der $\mathbb{C}$-Algebren gegeben, mit inversem Homomorphismus $x \mapsto \frac{1}{2}(z + z^{-1})$, $y \mapsto \frac{1}{2i}(z - z^{-1})$. Überträgt man die Involution $*$ mit diesem Isomorphismus vom linken Ring auf den rechten, so bleiben x und y fix. Deshalb ist der Fixring von $*$ in $\mathbb{C}[z, z^{-1}]$ isomorph zur $\mathbb{R}$-Algebra $\mathbb{R}[x, y]/(x^2 + y^2 - 1)$. Für $g \in \mathbb{C}[z]$ können wir g schreiben als

$$g \;=\; g_0 + ig_1, \quad g_0 = \frac{1}{2}(g + g^*), \quad g_1 = \frac{1}{2i}(g - g^*),$$

und dabei sind g_0, g_1 fix unter $*$. In der Situation von Theorem 2.19 ist also $f = gg^* = g_0^2 + g_1^2$ Summe von zwei Quadraten $*$-invarianter Laurentpolynome.

3. Semiringe und Moduln

Sei A stets ein Ring (kommutativ mit Eins, stets mit $\frac{1}{2} \in A$).

3.1 Definition. Sei A ein Ring.

(a) Eine Teilmenge S von A heißt ein *Semiring* von A (in der älteren Literatur auch *Präprimstelle*, engl. *preprime*), falls gelten $0, 1 \in A$ und $S + S \subseteq S$, $SS \subseteq S$.

(b) Sei S ein Semiring von A. Ein *S-Modul* von A ist eine Teilmenge M von A mit $1 \in M$, $M + M \subseteq M$ und $SM \subseteq M$.

(c) Ein *quadratischer Modul* in A ist eine Teilmenge $M \subseteq A$ mit $1 \in M$, $M + M \subseteq M$ und mit $a^2 M \subseteq M$ für jedes $a \in A$.

3.2 Definition. Sei M ein Modul über dem Semiring $S \subseteq A$.

(a) Der Modul M heißt *echt*, falls $-1 \notin M$ ist.

(b) M heißt *erzeugend*, falls $M - M = A$ ist.

(c) Der *Träger* von M ist $\operatorname{supp}(M) := M \cap (-M)$.

Der Träger $\operatorname{supp}(M)$ ist stets eine additive Untergruppe von A. Weiter gilt:

3.3 Lemma. *Sei A ein Ring und $S \subseteq A$ ein erzeugender Semiring. Für jeden S-Modul M in A ist* $\operatorname{supp}(M)$ *ein Ideal von A. Der einzige unechte S-Modul ist $M = A$.*

BEWEIS. Sei M ein S-Modul. Klar ist, daß $\mathrm{supp}(M)$ eine additive Untergruppe von A mit $S \cdot \mathrm{supp}(M) \subseteq \mathrm{supp}(M)$ ist. Ist also $S - S = A$, so ist $\mathrm{supp}(M)$ ein Ideal von A. Ist $-1 \in M$, so ist $1 \in \mathrm{supp}(M)$, also $\mathrm{supp}(M) = A$, also $M = A$. □

3.4 Bemerkungen.

1. Die Präordnungen von A sind genau die Semiringe $S \subseteq A$, welche alle Quadrate enthalten. Insbesondere ist $S = \Sigma A^2$ ein Semiring von A. Dieser ist erzeugend wegen $\frac{1}{2} \in A$ und $x = (\frac{x+1}{2})^2 - (\frac{x-1}{2})^2$. Die quadratischen Moduln in A sind gerade die ΣA^2-Moduln in A. Der Träger jedes quadratischen Moduls in A ist also ein Ideal von A.

2. Jede Präordnung ist ein quadratischer Modul, aber nicht umgekehrt: Für $A = R[x, y]$ etwa ist der quadratische Modul $M := \Sigma A^2 + x\Sigma A^2 + y\Sigma A^2$ keine Präordnung. Denn $xy \notin M$, d.h. es gibt keine Identität $xy = s_0 + s_1 x + s_2 y$ mit $s_i \in \Sigma A^2$. (Beweis?) Für ein anderes Beispiel siehe auch Aufgabe 3.

3. Hier sind andere Beispiele von Semiringen. Ist etwa A eine $\mathbb{R}$-Algebra, und sind $p_1, \ldots, p_r \in A$ fixiert, so kann man den von $\mathbb{R}_+$ und $p_1, \ldots, p_r$ erzeugten Semiring S in A betrachten. Es ist

$$S \;=\; \Big\{ \sum_{\alpha \in \mathbb{Z}_+^r} c_\alpha\, p_1^{\alpha_1} \cdots p_r^{\alpha_r} : 0 \le c_\alpha \in \mathbb{R},\ c_\alpha = 0 \text{ für fast alle } \alpha \Big\}.$$

Wird A von $p_1, \ldots, p_r$ als $\mathbb{R}$-Algebra erzeugt, so ist S ein erzeugender Semiring von A (und umgekehrt).

4. Semiringe höherer Stufe, etwa der von allen n-ten Potenzen in A erzeugte Semiring ΣA^n (bestehend aus den endlichen Summen von n-ten Potenzen in A). Ist $\frac{1}{n!} \in A$, so ist der Semiring ΣA^n erzeugend, wegen der Identität

$$n!\, x \;=\; \sum_{i=0}^{n-1} (-1)^{n-1-i} \binom{n-1}{i} \Big((x+i)^n - i^n \Big).$$

(Aufgabe ?) Ist dabei n ungerade, so ist also jedes Element in A eine Summe von n-ten Potenzen. Das zeigt, warum in der Regel nur Summen von geraden Potenzen interessant sind.

5. Sei $\mathtt{z} = (z_1, \ldots, z_n)$. Ein Polynom der Form

$$f \;=\; \sum_{j=1}^{r} |p_j(\mathtt{z})|^2 \;=\; \sum_{j=1}^{r} p_j(\mathtt{z}) \cdot \overline{p_j(\mathtt{z})} \;\in \mathbb{C}[\mathtt{z}, \overline{\mathtt{z}}]$$

mit komplexen Polynomen $p_1, \ldots, p_r \in \mathbb{C}[\mathtt{z}]$ heißt eine *hermitesche Quadratsumme*. (Es ist f ein Polynom in $\mathtt{z}$ und in $\overline{\mathtt{z}}$.) Schreibt man $z_j = x_j + iy_j$, $\overline{z}_j = x_j - iy_j$ $(j = 1, \ldots, n)$, so liegt jedes solche f in

$$A \;:=\; \mathbb{R}[\mathtt{x}, \mathtt{y}] \;=\; \mathbb{R}[x_1, y_1, \ldots, x_n, y_n].$$

Die hermiteschen Quadratsummen bilden einen erzeugenden Semiring $\Sigma_h^2 A$ von A, und es gilt $\Sigma_h^2 A \subsetneq \Sigma A^2$ (strikte Inklusion). Siehe Aufgabe 7.

3.5 Bemerkungen.

1. Hat A einen echten quadratischen Modul, so ist A reell. Denn für nichtreelles A ist $-1 \in \Sigma A^2$, also liegt dann -1 in jedem quadratischen Modul.

2. Jeder echte S-Modul ist in einem maximalen echten S-Modul enthalten. Das folgt aus dem Zornschen Lemma, denn eine aufsteigende Vereinigung von S-Moduln ist selbst ein S-Modul.

3. Jeder Durchschnitt von Semiringen von A ist wieder ein Semiring. Ist S ein fester Semiring von A, so sind jeder Durchschnitt und jede Summe von S-Moduln wieder S-Moduln. Der von $f_1, \dots, f_r \in A$ erzeugte S-Modul ist $M = S + Sf_1 + \cdots + Sf_r$. Besonders häufig brauchen wir den Fall $S = \Sigma A^2$: Den von $f_1, \dots, f_r$ erzeugten quadratischen Modul von A bezeichnen wir mit

$$QM(f_1, \dots, f_r) := QM_A(f_1, \dots, f_r) := \Sigma A^2 + f_1 \Sigma A^2 + \cdots + f_r \Sigma A^2.$$

4. Für jedes $f \in A$ ist $QM(f)$ (nur ein Erzeuger) eine Präordnung. Allgemeiner ist für $f_1, \dots, f_r \in A$

$$PO(f_1, \dots, f_r) = QM(f_1, \dots, f_r, f_1f_2, f_1f_3, \dots, f_1 \cdots f_r)$$

($2^r - 1$ Erzeuger rechts).

Einige Allgemeinheiten über quadratische Moduln:

3.6 Bemerkung. Sei $\varphi\colon A \to B$ ein Ringhomomorphismus. Für jeden quadratischen Modul N von B ist $\varphi^{-1}(N)$ ein quadratischer Modul von A. Ist N eine Präordnung, so auch $\varphi^{-1}(N)$. Ist umgekehrt M ein quadratischer Modul von A, so können wir den von $\varphi(M)$ in B erzeugten quadratischen Modul M_B betrachten, genannt die *Erweiterung* von M nach B. Es besteht M_B aus allen endlichen Summen $\sum_i b_i^2 \varphi(x_i)$ mit $x_i \in M$ und $b_i \in B$. Ist M eine Präordnung, so auch M_B. Auch wenn M echt ist, braucht M_B nicht echt zu sein.

Im Fall, wo φ surjektiv ist, gilt genauer:

3.7 Lemma. *Sei I ein Ideal von A, sei $\pi\colon A \to A/I$ der natürliche Epimorphismus. Es besteht eine natürliche Bijektion zwischen den quadratischen Moduln M von A mit $I \subseteq \operatorname{supp}(M)$ und den quadratischen Moduln N von A/I, gegeben durch $M \rightsquigarrow \pi(M)$ bzw. durch $N \rightsquigarrow \pi^{-1}(N)$. Dabei ist* $\operatorname{supp}(\pi(M)) = \pi(\operatorname{supp}(M))$ *und* $\operatorname{supp}(\pi^{-1}(N)) = \pi^{-1}(\operatorname{supp}(N))$.

Sei S eine multiplikative Teilmenge von A, sei M ein quadratischer Modul von A. Die Erweiterung von M nach A_S ist der quadratische Modul

$$M_S = \left\{ \frac{x}{s^2} \colon x \in M,\ s \in S \right\}$$

von A_S. Wieder hat man eine Bijektion zwischen den quadratischen Moduln von A_S und gewissen quadratischen Moduln von A. Es gilt (Aufgabe 4):

3.8 Lemma. *Genau dann ist der quadratische Modul M_T echt, wenn $T \cap \operatorname{supp}(M) = \varnothing$ ist.* □

3.9 Bemerkung. Sei $S \subseteq A$ eine Semiring und M ein S-Modul. Wie in II § 5 verwende die durch

$$f \leq_M g \quad :\Leftrightarrow \quad g - f \in M \quad (f, g \in A)$$

definierte Relation $\leq_M$ auf A. Dies ist eine partielle Ordnungsrelation modulo $\operatorname{supp}(M)$, und es gelten die folgenden Rechenregeln:

(1) $a \leq_M b$ und $a' \leq_M b' \ \Rightarrow\ a + a' \leq_M b + b'$;
(2) $a \leq_M b$ und $s \in S \ \Rightarrow\ as \leq_M bs$.

Eine Untergruppe $I \subseteq A$ heißt *M-konvex*, falls die folgenden äquivalenten Bedingungen erfüllt sind (siehe II.5.11):

(i) Aus $a \leq_M c \leq_M b$ und $a, b \in I$, $c \in A$ folgt $c \in I$;
(ii) aus $a, b \in M$ und $a + b \in I$ folgt $a, b \in I$;
(iii) $\operatorname{supp}(M + I) = I$.

Jeder echte S-Modul in einem maximalen echten S-Modul M enthalten (3.5.2). Dabei gilt:

3.10 Satz. *Ist $S \subseteq A$ ein erzeugender Semiring, und ist M ein maximaler echter S-Modul in A, so ist $M \cup (-M) = A$.*

Anders gesagt, $\leq_M$ ist eine *totale* Anordnung modulo $\operatorname{supp}(M)$.

Beweis. Angenommen, es gebe $a \in A$ mit $\pm a \notin M$. Wegen der Maximalität von M ist $-1 \in (M + Sa) \cap (M - Sa)$. Es gibt also $x, y \in M$ und $s, t \in S$ mit

$$-1 = x + sa \quad \text{und} \quad -1 = y - ta.$$

Multipliziere die Gleichungen mit t bzw. s und addiere, das gibt

$$-s \;=\; t + sy + tx,$$

also ist $-s \in M$, und somit $s \in \operatorname{supp}(M)$. Wegen S erzeugend ist $\operatorname{supp}(M)$ ein Ideal von A (Lemma 3.3). Aus $-1 = x + sa$ folgt also $-1 \in M$, Widerspruch. □

Aus Lemma II.5.12 folgt:

3.11 Satz. *Sei S ein Semiring von A, sei M ein S-Modul in A mit $M \cup (-M) = A$. Dann besteht eine inklusionstreue Bijektion zwischen*

1. *den S-Moduln N in A mit $M \subseteq N$, und*
2. *den M-konvexen Untergruppen $I \subseteq A$ mit $SI \subseteq I$,*

gegeben durch $N \mapsto \operatorname{supp}(N)$ bzw. $I \mapsto M + I = M \cup I$. Jede der beiden Mengen 1. bzw. 2. bildet eine Kette bezüglich Inklusion.

3.12 Korollar. *Sei M ein Modul über einem erzeugenden Semiring S mit $M \cup (-M) = A$. Dann ist $I \mapsto M + I$ eine Bijektion zwischen den M-konvexen Idealen I von A und den S-Obermoduln N von M in A, mit Umkehrabbildung $N \mapsto \operatorname{supp}(N)$. (Beide Mengen bilden jeweils eine Kette bezüglich Inklusion.)*

In der Situation von Satz 3.11 gibt es eine größte M-konvexe und S-stabile Untergruppe I von A mit $1 \notin I$, nämlich die Vereinigung aller solchen Untergruppen, da diese eine Kette bilden. Wir können sie wie folgt beschreiben:

3.13 Satz. *Sei S ein Semiring mit $\frac{1}{2} \in S$, sei M ein echter S-Modul mit $M \cup (-M) = A$. Die größte 1 nicht enthaltende S-stabile und M-konvexe Untergruppe von A ist*

$$I \;=\; \big\{a \in A \colon \forall\, s \in S \;\; 1 \pm sa \in M\big\}.$$

Der größte M enthaltende echte S-Modul ist $M + I$.

Beweis. Die zweite Behauptung folgt aus der ersten wegen Satz 3.11. Die im Satz angegebene Menge ist

$$I \;=\; \{a \in A \colon \text{für alle } s \in S \text{ ist } \; -1 \leq_M sa \leq_M 1\}.$$

Klar ist $SI \subseteq I$. Aus $a_1,\ a_2 \in I$ folgt $a_1 - a_2 \in I$. Denn für $s \in S$ gilt auch $-1 \leq_M 2sa_i \leq_M 1$ $(i = 1, 2)$, also auch $\pm s(a_1 - a_2) \leq_M 1$. Also ist I eine additive Untergruppe, und ist nach Definition S-stabil. Wegen $-1 \notin M$ ist $1 \notin I$. Jede M-konvexe S-stabile Untergruppe J von A mit $1 \notin J$ ist in I enthalten. Denn ist $a \in J$ und $s \in S$, so würde aus $sa \geq_M 1 \geq_M 0$ folgen $1 \in J$, wegen $sa \in J$ und der M-Konvexität von J. Auf der anderen Seite ist I selbst M-konvex. Denn seien f, $g \in M$ mit $f + g \in I$. Für $s \in S$ ist $0 \leq_M sf + sg \leq_M 1$. Wegen $sf,\ sg \geq_M 0$ folgt daraus $0 \leq_M sf,\ sg \leq_M 1$. Dies für alle $s \in S$ zeigt $f,\ g \in I$. □

3.14 Bemerkung. Ist S erzeugend in Satz 3.13, so ist I ein Ideal von A, und ist das größte von (1) verschiedene M-konvexe Ideal von A. Es ist dann also

$$I = \{a \in A \colon \forall\, b \in A\ ab \leq_M 1\}.$$

4. Einführung in Semiordnungen

Zuletzt haben wir allgemein maximale echte S-Moduln betrachtet. Der Fall $S = \Sigma A^2$, also maximale echte quadratische Moduln, führt auf Semiordnungen (Definition siehe 4.2 unten).

4.1 Satz. *Sei M ein echter quadratischer Modul von A, und sei $\mathfrak{p}$ ein minimaler Primteiler von* $\operatorname{supp}(M)$*. Dann ist das Ideal $\mathfrak{p}$ M-konvex, und $M + \mathfrak{p}$ ist ein quadratischer Modul mit Träger $\mathfrak{p}$.*

Insbesondere ist auch $M + \mathfrak{p}$ ein echter quadratischer Modul.

Beweis. Es genügt zu zeigen, daß das Ideal $\mathfrak{p}$ M-konvex ist, denn das bedeutet $\operatorname{supp}(M+\mathfrak{p}) = \mathfrak{p}$ (siehe 3.9), und insbesondere $-1 \notin M+\mathfrak{p}$. Da $S = \Sigma A^2$ erzeugend ist, ist $\operatorname{supp}(M)$ ein Ideal von A (3.3). Seien f, $g \in M$ mit $f + g \in \mathfrak{p}$, wir müssen zeigen, daß f, g in $\mathfrak{p}$ liegen. Der Ring $A_{\mathfrak{p}}/\operatorname{supp}(M)A_{\mathfrak{p}}$ hat nur ein einziges Primideal, nämlich das von $\mathfrak{p}$ erzeugte Ideal. In diesem Ring ist also $f + g$ nilpotent. Deshalb gibt es $n \in \mathbb{N}$ und $u \in A$ mit $u \notin \mathfrak{p}$ und mit $u(f + g)^n \in \operatorname{supp}(M)$. Wir können n ungerade annehmen und haben also

$$u^2 \sum_{i=0}^{n} \binom{n}{i} f^i g^{n-i} \ \in\ \operatorname{supp}(M).$$

Jeder einzelne Summand liegt in M, wegen n ungerade, und liegt daher auch in $-M$. Insbesondere ist $u^2 f^n \in \operatorname{supp}(M) \subseteq \mathfrak{p}$, und daher $f \in \mathfrak{p}$. Analog folgt $g \in \mathfrak{p}$. □

4.2 Definition. Eine *Semiordnung* von A ist ein quadratischer Modul M von A derart, daß $M \cup (-M) = A$ und $\operatorname{supp}(M)$ ein Primideal von A ist.

4.3 Korollar. *Jeder maximale echte quadratische Modul von A ist eine Semiordnung von A.*

Beweis. Nach Satz 3.10 ist $M \cup (-M) = A$. Wäre $\operatorname{supp}(M)$ kein Primideal, so gäbe es einen minimalen Primteiler $\mathfrak{p} \neq \operatorname{supp}(M)$ von $\operatorname{supp}(M)$. Nach Satz 4.1 wäre dann $M + \mathfrak{p}$ ein strikt größerer echter quadratischer Modul. □

4.5 Sei K ein Körper, sei M eine fixierte Semiordnung von K. Der Körper K ist also reell. Wir bezeichnen die durch M definierte totale Anordnung $\leq_M$ auf der Menge K einfach mit $\leq$. Nach Definition gilt also

$$a \leq b \quad \Leftrightarrow \quad b - a \in M.$$

Für alle a, b, $c \in K$ gilt:

(1) $a \leq b \ \Rightarrow\ a + c \leq b + c$,
(2) $a \geq 0 \ \Rightarrow\ ab^2 \geq 0$,
(3) $0 \leq 1$.

Für a, $b > 0$ kann aber $ab < 0$ sein. Umgekehrt definiert jede totale Ordnung $\leq$ auf K mit (1)–(3) eine Semiordnung M auf K, nämlich $M = \{a \in K \colon a \geq 0\}$. Wir bezeichnen daher auch jede totale Ordnung $\leq$ mit (1)–(3) als Semiordnung von K.

4.6 Lemma. *Sei $\leq$ eine Semiordnung auf dem Körper K. Dann ist die Einschränkung von $\leq$ auf $\mathbb{Q}$ die übliche Anordnung von $\mathbb{Q}$. Für alle a, $b \in K$ gilt:*

(a) $a \le b \;\Rightarrow\; ac \le bc$ *für alle* $c \in \Sigma K^2$*;*
(b) $a > 0 \;\Rightarrow\; \frac{1}{a} > 0$*;*
(c) $0 < a \le b \;\Rightarrow\; 0 < \frac{1}{b} \le \frac{1}{a}$*;*
(d) *ist* $0 \le a \le b$*, und ist* $a \in \Sigma K^2$ *oder* $b \in \Sigma K^2$*, so folgt* $0 \le a^2 \le b^2$*.*

BEWEIS. Die erste Aussage ist klar, denn jede positive rationale Zahl ist eine Summe von Quadraten. (a) ist klar, und (b) folgt durch Multiplikation mit $\frac{1}{a^2}$. Wegen

$$\frac{1}{a} - \frac{1}{b} \;=\; \frac{1}{a^2} \cdot \frac{a(b-a)}{b} \;=\; \frac{1}{a^2} \cdot \frac{1}{\frac{1}{a} + \frac{1}{b-a}}$$

für $a \neq b$ folgt (c) aus (b). Für (d) sei etwa $b \in \Sigma K^2$, und sei o.E. $a \neq 0$. Dann ist $ab \le b^2$ nach (a). Aus (b) folgt weiter $\frac{1}{b} \le \frac{1}{a}$, und Multiplikation mit $a^2 b \in \Sigma K^2$ gibt $a^2 \le ab$. Also ist $a^2 \le b^2$. Der Fall $a \in \Sigma K^2$ geht analog, oder folgt aus dem soeben bewiesenen Fall mit Hilfe von (c). □

4.7 Definition. Eine Semiordnung $\le$ von K heißt *archimedisch*, wenn gilt:

$$\forall\, a \in K \;\; \exists\, n \in \mathbb{Z} \;\; a \le n.$$

Dies verallgemeinert den Begriff der archimedischen Anordnungen (I.1.16). Wir werden den Begriff archimedisch bald in größerer Allgemeinheit studieren.

4.8 Satz. *Sei* K *ein Körper. Jede archimedische Semiordnung von* K *ist eine Anordnung von* K*.*

BEWEIS. Sei $\le$ eine archimedische Semiordnung von K. Zunächst zeigen wir, daß $\mathbb{Q}$ dicht in K bezüglich der durch $\le$ definierten Ordnungstopologie ist. Seien $a < b$ in K. Wähle $n \in \mathbb{N}$ mit $\frac{1}{b-a} < n$, dann ist $\frac{1}{n} < b - a$ (nach 4.6(b) und (c)), also $1 < n(b-a)$, d.h. $na < nb - 1$. Wähle $m \in \mathbb{Z}$ minimal mit $nb - 1 \le m$. Dann ist $na < m < nb$, und Division durch n gibt $a < \frac{m}{n} < b$.

Für a, $b \in K$ mit $a > 0$, $b > 0$ müssen wir $ab > 0$ zeigen. Sei o.E. $b < a$, dann gilt $0 < a - b < a + b$. Wähle $q \in \mathbb{Q}$ mit $a - b < q < a + b$. Wegen $q \in \Sigma K^2$ folgt aus 4.6(d) $(a-b)^2 < q^2 < (a+b)^2$, und daraus $4ab > 0$, also $ab > 0$. □

Studiere nun das Zusammenspiel zwischen Semiordnungen und Bewertungen.

4.9 Lemma. *Sei* B *ein Bewertungsring von* K *mit zugehöriger Bewertung* v *von* K*, und sei* M *eine Semiordnung von* K*. Folgende Bedingungen sind äquivalent:*

(i) $(1 + \mathfrak{m}_B)M \subseteq M$*;*
(ii) *aus* $a, b \in K$ *mit* $a >_M 0$ *und* $v(b) > v(a)$ *folgt* $b <_M a$*.*

Sind diese erfüllt, so heißen M *und* B verträglich*.*

BEWEIS. (i) $\Rightarrow$ (ii): Es ist $a \in M$ und $-\frac{b}{a} \in \mathfrak{m}_B$. Aus (i) folgt also $(1 - \frac{b}{a})a = a - b \in M$, also $a >_M b$.

(ii) $\Rightarrow$ (i): Sei $0 \neq a \in M$ und $c \in \mathfrak{m}_B$. Für $b := ac$ ist $v(b) > v(a)$, also gilt $b <_M -a$ nach (iv), d.h. $a + b = (1 + c)a \in M$. □

Ist M eine Anordnung von K, so ist (i) äquivalent zu $1 + \mathfrak{m}_B \subseteq M$, also zu $-1 <_M b <_M 1$ für alle $b \in \mathfrak{m}_B$. Für Anordnungen stimmt gemäß Korollar II.5.5 also die neue Definition von verträglich mit der früheren überein.

4.10 Satz. *Sei* B *ein Bewertungsring von* K *und* M *eine Semiordnung von* K*. Die folgenden vier Bedingungen sind zueinander äquivalent:*

(i) B *ist* M*-konvex in* K*;*

(ii) $\mathfrak{m}_B$ *ist* M*-konvex in* K*;*
(iii) $-1 <_M a <_M 1$ *für alle* $a \in \mathfrak{m}_B$*;*
(iv) $[-1,1]_M \subseteq B$.

Sind B *und* M *verträglich, so sind (i)–(iv) erfüllt. Ist* M *eine Anordnung von* K*, und gelten (i)–(iv), so sind umgekehrt auch* B *und* M *verträglich.*

BEWEIS. Sei M eine Semiordnung von K, sei $\leq \;=\; \leq_M$, und sei $\mathfrak{m} = \mathfrak{m}_B$.

(i) $\Rightarrow$ (ii): Sei B M-konvex, sei $0 < a < b$ mit $b \in \mathfrak{m}$. Wegen B M-konvex ist $a \in B$. Wäre $a \notin \mathfrak{m}$, so wäre $\frac{1}{a} \in B$, und $0 < \frac{1}{b} < \frac{1}{a}$ nach 4.6(c), ein Widerspruch zur M-Konvexität von B wegen $\frac{1}{b} \notin B$.

(ii) $\Rightarrow$ (iii): Sei $a \in K$ mit $a \geq 1$. Wegen $\mathfrak{m}$ M-konvex und $0 < 1 \leq a$ ist dann $a \notin \mathfrak{m}$.

(iii) $\Rightarrow$ (iv): Aus $0 < a < 1$ folgt $\frac{1}{a} > 1$ (4.6(c)), also $\frac{1}{a} \notin \mathfrak{m}$ nach (iii), also $a \in B$.

(iv) $\Rightarrow$ (i): Sei $[-1,1]_M \subseteq B$, seien $0 < a < b$ mit $b \in B$, zu zeigen ist $a \in B$. Ist $a \leq 1$, so gilt dies nach Voraussetzung. Sei $a > 1$, also auch $b > 1$, also $0 < \frac{1}{b} < 1$ (4.6(c)). Division von $0 < a < b$ durch b^2 gibt $0 < \frac{a}{b^2} < \frac{1}{b} < 1$. Nach Voraussetzung ist also $\frac{a}{b^2} \in B$, also $a \in b^2 B \subseteq B$.

Sind B und M verträglich, so ist $1 + \mathfrak{m} \subseteq M$, d.h. es gilt (iii). Ist M eine Anordnung, so folgt aus $1 + \mathfrak{m} \subseteq M$ auch $(1 + \mathfrak{m})M \subseteq M$, also die Verträglichkeit von B und M. □

4.12 Lemma. *Sei* M *eine Semiordnung von* K *und* B *ein* M*-konvexer Teilring von* K*. Dann ist* B *ein Bewertungsring von* K*, und*

$$\overline{M} \;:=\; \big\{\overline{a} \colon a \in B \cap M\big\}$$

ist eine Semiordnung von $\kappa = B/\mathfrak{m}_B$*, genannt die von* M *auf* κ induzierte Semiordnung.

(Dies verallgemeinert die Definition der induzierten Anordnung im Fall, wo M eine Anordnung ist, siehe II.5.6.)

BEWEIS. Sei $a \in K$, etwa $a \geq_M 0$. Ist $a \leq_M 1$, so ist $a \in B$ wegen der M-Konvexität von B. Ist $a \notin B$, so ist also $a >_M 1$, und daher $0 <_M \frac{1}{a} <_M 1$ (4.6(c)), also $\frac{1}{a} \in B$. Also ist B ein Bewertungsring von K. Es ist klar, daß $\overline{M}$ ein quadratischer Modul von κ mit $\overline{M} \cup (-\overline{M}) = \kappa$ ist. Zu zeigen bleibt $-1 \notin \overline{M}$. Wäre $-1 \in \overline{M}$, so gäbe es $a \in B \cap M$ mit $-1 = \overline{a}$, d.h. mit $a + 1 \in \mathfrak{m}$. Wegen $a + 1 \geq_M 1$ ist das ein Widerspruch zu 4.10(iii). □

4.13 Satz. *Sei* M *eine Semiordnung von* K*, sei* B *die* M*-konvexe Hülle von* $\mathbb{Z}$ *in* K*. Dann ist* B *ein Bewertungsring von* K*, und die von* M *auf dem Restklassenkörper* κ_B *induzierte Semiordnung ist eine archimedische Anordnung.*

BEWEIS. Schreibe wieder $\leq \;=\; \leq_M$, es ist also $B = \{a \in K \colon \exists\, n \in \mathbb{N}$ mit $n \pm a \geq 0\}$. Klar ist, daß B eine Untergruppe von $(K,+)$ ist und daß $\mathbb{Q}B \subseteq B$ gilt (wegen 4.6(a)). Aus $0 \leq a \leq n$ und $n \in \mathbb{N}$ folgt $0 \leq a^2 \leq n^2$ nach 4.6(d). Also gilt $a \in B \Rightarrow a^2 \in B$. Wegen

$$ab \;=\; \Big(\frac{a+b}{2}\Big)^2 - \Big(\frac{a-b}{2}\Big)^2$$

ist B also ein Teilring von K. Nach 4.12 ist B ein Bewertungsring von K, und $\overline{M}$ ist eine Semiordnung auf κ. Nach Konstruktion ist $\overline{M}$ archimedisch. Nach Satz 4.8 ist $\overline{M}$ also eine Anordnung von κ. □

5. Archimedizität

Die folgende Definition verallgemeinert Definition 4.7:

5.1 Definition. Sei A ein Ring. Eine additive Unterhalbgruppe $M \subseteq A$ mit $1 \in M$ heißt *archimedisch*, falls gilt:

$$\forall\, f \in A \;\; \exists\, n \in \mathbb{N} \;\; n - f \;\in\; M.$$

5.3 Definition. Sei $M \subseteq A$ eine Unterhalbgruppe mit $1 \in M$. Wir setzen

$$O(M) \;=\; O_A(M) \;:=\; \{f \in A\colon \exists\, n \in \mathbb{N} \;\; n \pm f \;\in\; M\}.$$

Die Elemente von $O(M)$ heißen die *M-beschränkten Elemente* von A.

5.4 Bemerkung. Die Definition von $O(M)$ kann man auch schreiben als

$$O(M) \;=\; \{f \in A\colon \exists\, n \in \mathbb{N} \;\; -n \leq_M f \leq_M n\}.$$

Es ist also $O(M)$ die konvexe Hülle von $\mathbb{Z}$ in A bezüglich der (i.a. nicht totalen) Relation $\leq_M$.

5.5 Lemma. *Sei $M \subseteq A$ eine Unterhalbgruppe mit $1 \in M$. Dann ist $O(M) = \operatorname{supp}(M + \mathbb{Z})$. Insbesondere ist $O(M)$ eine Untergruppe von A. Genau dann ist M archimedisch, wenn $O(M) = A$ ist.*

Beweis. Es ist $O(M) = \{f \in A\colon \pm f \in M + \mathbb{Z}\} = \operatorname{supp}(M + \mathbb{Z})$. □

5.6 Satz. *Ist M ein Semiring oder ein quadratischer Modul in A, so ist $O(M)$ eine Teilring von A.*

Beweis. Zunächst sei M ein Semiring. Seien m, $n \in \mathbb{N}$ und f, $g \in A$ mit $m \pm f \in M$ und $n \pm g \in M$. Für $\varepsilon = \pm 1$ ist

$$(m + f)(n + \varepsilon g) + n(m - f) + m(n - \varepsilon g) \;=\; 3mn + \varepsilon fg.$$

Die linke Seite liegt offensichtlich in M, also folgt $fg \in O(M)$.

Jetzt sei M ein quadratischer Modul in A. Sei $f \in O(M)$, etwa $n \pm f \in M$ mit $n \in \mathbb{N}$. Verwendet man die Identität

$$(m - 4f)^2(n + f) + (m + 4f)^2(n - f) = 2nm^2 - 16(m - 2n)f^2$$

für hinreichend großes $m \in \mathbb{N}$ (es genügt $m = 2n + 1$), so folgt $f^2 \in O(M)$. Da $O(M)$ eine additive Gruppe ist, ergibt sich die Behauptung aus der Identität $fg = (\frac{f+g}{2})^2 - (\frac{f-g}{2})^2$. □

5.7 Satz. *Sei A eine $\mathbb{R}$-Algebra, erzeugt von $x_1, \ldots, x_n$.*

(a) *Sei $S \subseteq A$ ein Semiring mit $\mathbb{R}_+ \subseteq S$. Gibt es $c \in \mathbb{R}$ mit $c \pm x_i \in S$ $(i = 1, \ldots, n)$, so ist S archimedisch.*

(b) *Sei $M \subseteq A$ ein quadratischer Modul. Gibt es $c \in \mathbb{R}$ mit $c - (x_1^2 + \cdots + x_n^2) \in M$, so ist M archimedisch.*

(Die jeweiligen Umkehrungen gelten natürlich ohnehin.)

Beweis. (a) Nach Satz 5.6, und wegen $\mathbb{R}_+ \subseteq S$, ist $O(S)$ eine $\mathbb{R}$-Teilalgebra von A. Die angegebene Bedingung impliziert $x_1, \ldots, x_n \in O(S)$, und damit $O(S) = A$.

(b) Wieder ist $O(M)$ eine $\mathbb{R}$-Teilalgebra von A, nach Satz 5.6. Sei $c \in \mathbb{R}$ mit $f := c - \sum_i x_i^2 \in M$. Für jedes $i = 1, \ldots, n$ ist auch $c - x_i^2 = f + \sum_{j \neq i} x_j^2$ in M, und damit auch

$$\left(c - x_i^2\right) + \left(x_i \pm \frac{1}{2}\right)^2 \;=\; \left(c + \frac{1}{4}\right) \pm x_i \in M.$$

Das zeigt $x_i \in O(M)$, also $O(M) = A$. □

5.8 Lemma. (Brumfiel) *Sei A eine Ring, sei $f(t) \in A[t]$ ein normiertes Polynom von geradem Grad. Dann gibt es ein $a \in A$, so daß $f(t) + a$ eine Summe von Quadraten in $A[t]$ ist.*

BEWEIS. Sei $\deg(f) = 2d$, Beweis per Induktion nach d. Für $2d = 2$ ist die Behauptung klar:

$$t^2 + at + b \;=\; \Big(t + \frac{a}{2}\Big)^2 + \Big(b - \frac{a^2}{4}\Big).$$

Sei jetzt $f = t^{2d} + at^{2d-1} + bt^{2d-2} + \cdots$ mit $2d \geq 4$, und sei die Aussage für kleinere gerade Grade schon gezeigt. Mache den Ansatz

$$f \;=\; \big(t^d + \alpha t^{d-1} + \beta t^{d-2} + \cdots\big)^2 + \big(t^{2d-2} + \cdots\big)$$

mit unbekannten Koeffizienten $\alpha, \beta \in A$, wobei $\cdots$ jeweils kleinere Grade bedeutet. Das zeigt, was man machen muß: Setze $\alpha := \frac{a}{2}$, und wähle β so, daß $\alpha^2 + 2\beta = b - 1$ ist. Dann ist

$$f(t) \;=\; \big(t^d + \alpha t^{d-1} + \beta t^{d-2}\big)^2 + g(t)$$

mit einem normierten Polynom $g(t)$ vom Grad $2d-2$. Nach Induktion gibt es $c \in A$, so daß $g(t) + c$ eine Summe von Quadraten in $A[t]$ ist. Also ist auch $f(t) + c$ eine Summe von Quadraten in $A[t]$. □

5.10 Satz. *Sei M ein quadratischer Modul in A. Dann ist der Ring $O_A(M)$ ganz abgeschlossen in A.*

BEWEIS. Sei $a \in A$ ganz über $O(M) = O_A(M)$, etwa $f(a) = 0$ mit einem normierten Polynom $f(t) \in O(M)[t]$ vom Grad n. Wir können $n \geq 2$ gerade annehmen. Nach Lemma 5.8 gibt es Elemente v, $w \in O(M)$ und Quadratsummen g, h in $O(M)[t]$ so, daß $f(t) + t = v + g(t)$ und $f(t) - t = w + h(t)$ ist. Nach Definition von $O(M)$ gibt es $N \in \mathbb{N}$ mit $N + v$, $N + w \in M$. Substitution $t := a$ gibt $N + a = N + f(a) + a = N + v + g(a) \in M$ und $N - a = N + f(a) - a = N + w + h(a) \in M$. Also ist $a \in O(M)$. □

5.11 Korollar. *Sei $A \to B$ ein ganzer Ringhomomorphismus, und sei M ein archimedischer quadratischer Modul in A. Dann ist auch der von M in B erzeugte quadratische Modul M_B archimedisch.*

BEWEIS. Wegen M archimedisch ist $O_A(M) = A$. Der Teilring $O_B(M_B)$ von B enthält $O_A(M) = A$, und ist ganz abgeschlossen in B nach Satz 5.10, ist also gleich B. □

Das folgende Theorem wird beim Beweis des archimedischen Positivstellensatzes eine entscheidende Rolle spielen.

5.12 Theorem. *Sei M ein echter Modul über einem erzeugenden Semiring S von A. Ist M archimedisch, so ist M in einem Positivkegel von A enthalten.*

BEWEIS. M ist in einem maximalen echten S-Modul M_1 enthalten (Bemerkung 3.5.2), und M_1 ist archimedisch. Wir können M durch M_1 ersetzen, also annehmen, daß M selbst ein maximaler echter S-Modul ist, und müssen dann zeigen, daß M ein Positivkegel ist. Nach Satz 3.10 gilt $M \cup (-M) = A$. Für den Träger von M gilt

$$\operatorname{supp}(M) \;=\; \{a \in A\colon \forall\, b \in A\ ab <_M 1\} \;=\; \{a \in A\colon \forall\, s \in S\ -1 <_M sa <_M 1\},$$

und dies ist ein Ideal von A. Denn die rechte Menge I ist das größte echte M-konvexe Ideal von A, und $M+I$ ist selbst ein echter S-Modul, siehe Satz 3.13 und Bemerkung 3.14. Wegen der Maximalität von M ist also $I \subseteq M$. Wir beweisen nun in mehreren Schritten.

(1) *Für alle $a, b \in A$ mit $a \geq_M 1$ und $b \geq_M 1$ gibt es eine natürliche Zahl $n \geq 1$ mit $nab \geq_M 1$.*

In der Tat, seien $s, t \in S$ mit $a = s-t$. Wegen M archimedisch gibt es $k \in \mathbb{N}$ mit $t \leq_M k$. Fixiere $n \in \mathbb{N}$ mit $n > k$. Es gibt ein maximales $m \in \mathbb{N}$ mit $m \leq_M nb$, und wegen $n \leq_M nb$ ist dabei $m \geq n \geq k+1$. Wegen $M \cup (-M) = A$ ist $nb \leq_M m+1$. Es folgt

$$nab \;=\; nsb - ntb \;\geq_M\; ms - (m+1)t \;=\; ma - t \;\geq_M\; m - t \;\geq_M 1,$$

wie behauptet.

(2) *M ist eine Präordnung in A.*

Es genügt, für $a, b \in M$ zu zeigen, daß auch $ab \in M$ ist. Denn wegen $M \cup (-M) = A$ folgt daraus auch, daß M alle Quadrate enthält. Seien also $a, b \in M$. Da $\operatorname{supp}(M)$ ein Ideal ist, können wir annehmen $a,\ b \notin \operatorname{supp}(M)$. Nach obiger Beschreibung von $\operatorname{supp}(M)$ gibt es also $s,\ t \in S$ mit $sa \geq_M 1$ und $tb \geq_M 1$. Nach (1) gibt es $n \in \mathbb{N}$ mit $nstab \geq_M 1$. Wäre $ab \notin M$, so wäre $ab \leq_M 0$, also auch $nstab \leq_M 0$, Widerspruch. Also ist $ab \in M$.

(3) *M ist ein Positivkegel von A.*

Es bleibt zu zeigen, daß $\operatorname{supp}(M)$ ein Primideal von A ist. Es ist M ein maximaler echter quadratischer Modul, denn andernfalls gäbe es (nach 3.12) ein echt größeres M-konvexes Ideal als $\operatorname{supp}(M)$. Nach Korollar 4.3 ist M also eine Semiordnung, d.h. $\operatorname{supp}(M)$ ist ein Primideal. □

Das Beispiel aus Aufgabe 6 zeigt, daß man auf die Voraussetzung archimedisch in Theorem 5.12 nicht verzichten kann.

Zu jeder Teilmenge $M \subseteq A$ habe die abgeschlossene Menge

$$X(M) \;=\; \{\xi \in \operatorname{Sper}(A) \colon \forall\, f \in M\ f(\xi) > 0\}$$

in $\operatorname{Sper}(A)$ (II.1.4).

5.13 Definition. Für jede Teilmenge $M \subseteq A$ setzen wir

$$X_M \;=\; \{\alpha \in \operatorname{Hom}(A, \mathbb{R}) \colon \alpha(M) \subseteq \mathbb{R}_+\},$$

die Menge aller Ringhomomorphismen $A \to \mathbb{R}$, die auf M nichtnegative Werte haben. Wir versehen X_M mit der Topologie, die von der Inklusion

$$X_M \;\subseteq\; \operatorname{Hom}(A, \mathbb{R}) \;\subseteq\; \mathbb{R}^A = \prod_A \mathbb{R}, \quad \alpha \mapsto \big(\alpha(f)\big)_{f \in A}$$

und der Produkttopologie auf $\mathbb{R}^A$ induziert wird.

5.14 Lemma. *X_M ist eine abgeschlossene Teilmenge von $\mathbb{R}^A$.*

Beweis. $\operatorname{Hom}(A, \mathbb{R})$ ist ein abgeschlossener Teilraum von $\mathbb{R}^A$. Das sieht man mit einem Argument wie im Beweis von Theorem II.4.5 (Kompaktheit der konstruierbaren Topologie von $\operatorname{Sper}(A)$). Andererseits ist klar, daß X_M abgeschlossen in $\operatorname{Hom}(A, \mathbb{R})$ ist. □

5.15 Beispiel. Der einzige Ringhomomorphismus $\mathbb{R} \to \mathbb{R}$ ist die Identität (Korollar I.1.21). Ist also A eine $\mathbb{R}$-Algebra, so ist $\operatorname{Hom}(A, \mathbb{R}) = \operatorname{Hom}_{\mathbb{R}}(A, \mathbb{R})$. Ist V eine affine $\mathbb{R}$-Varietät und $A = \mathbb{R}[V]$ ihr Koordinatenring, so ist $\operatorname{Hom}(A, \mathbb{R}) = V(\mathbb{R})$.

Diese Identifikation stimmt nicht nur als Menge, sondern als topologische Räume (klar, siehe auch I.7.5). Für jede Teilmenge $M \subseteq A$ ist alsdann $X_M = S(M) = \{\xi \in V(\mathbb{R})\colon \forall\, f \in M\ f(\xi) \geq 0\}$ in der Bezeichnung aus II.3.2. Ist etwa M eine endliche Menge, oder etwa ein endlich erzeugter quadratischer Modul, so ist die Menge $X_M \subseteq V(\mathbb{R})$ basisch abgeschlossen semialgebraisch.

5.16 Sei $M \subseteq A$ eine Teilmenge. Jedes $f \in A$ definiert eine Abbildung

$$\widehat{f}\colon X_M \to \mathbb{R}, \quad \widehat{f}(\alpha) = \alpha(f) \quad (\alpha \in X_M).$$

Die Abbildung $\widehat{f}$ ist stetig. Außerdem gelten $\widehat{f+g} = \widehat{f} + \widehat{g}$ und $\widehat{fg} = \widehat{f}\,\widehat{g}$ für $f, g \in A$, sowie $\widehat{1} = 1$. Also haben wir einen Ringhomomorphismus

$$\Phi_M\colon A \to C(X_M, \mathbb{R}), \quad f \mapsto \widehat{f}$$

in den Ring der stetigen $\mathbb{R}$-wertigen Funktionen auf X_M.

5.17 Satz. *Sei $M \subseteq A$ eine Teilmenge. Die natürliche Abbildung*

$$X_M \to \operatorname{Sper}(A), \quad \alpha \mapsto \alpha^{-1}(\mathbb{R}_+)$$

ist eine topologische Einbettung, und identifiziert die Menge X_M mit der Menge $X(M)_{\mathrm{arch}}$ aller Punkte $\xi \in X(M)$, für die der angeordnete Restklassenkörper $\kappa(\xi)$ archimedisch ist. Es gilt $X(M)_{\mathrm{arch}} \subseteq X(M)^{\max}$.

(Erinnerung: $X(M)^{\max}$ ist die Menge der abgeschlossenen Punkte von $X(M)$. Topologische Einbettung heißt Homöomorphismus aufs Bild.)

Beweis. Für $\alpha \in \operatorname{Hom}(A, \mathbb{R})$ sei $\xi_\alpha \in \operatorname{Sper}(A)$ der durch α repräsentierte Punkt (entsprechend dem Positivkegel $\alpha^{-1}(\mathbb{R}_+)$). Für $\alpha \in X_M$ ist $\xi_\alpha \in X(M)$, und umgekehrt. Der angeordnete Körper

$$\kappa(\xi_\alpha) = \big(\operatorname{Quot}(A/\ker(\alpha)),\ \xi_\alpha\big)$$

ist archimedisch (als angeordneter Teilkörper von $\mathbb{R}$). Daher ist insbesondere $\xi_\alpha \in \operatorname{Sper}(A)^{\max}$ (Satz II.5.15). Ist umgekehrt $\xi \in X(M)_{\mathrm{arch}}$, so gibt es nach dem Satz von Hölder (I.1.18) eine eindeutige ordnungstreue Einbettung $\kappa(\xi) \hookrightarrow \mathbb{R}$, also ein eindeutiges $\alpha \in \operatorname{Hom}(A, \mathbb{R})$ mit $\xi_\alpha = \xi$.

Zu zeigen bleibt, daß die Abbildung $X_M \to \operatorname{Sper}(A)$, $\alpha \mapsto \xi_\alpha$ eine topologische Einbettung ist. Die Stetigkeit ist klar, denn für $f \in A$ ist das Urbild der Harrison-offenen Menge $U(f)$ gleich $\{\alpha\colon \widehat{f}(\alpha) > 0\}$, eine in X_M offene Menge. Es genügt, für $f \in A$ und *rationale* ε, $t \in \mathbb{Q}$ mit $\varepsilon > 0$ zu zeigen, daß die Menge

$$\{\xi_\alpha\colon \alpha \in X_M,\ |\alpha(f) - t| < \varepsilon\}$$

relativ offen in $X(M)_{\mathrm{arch}}$ ist. Denn die endlichen Durchschnitte von Mengen $\{\alpha \in X_M\colon |\alpha(f) - t| < \varepsilon\}$ (mit $f \in A$ und ε, $t \in \mathbb{Q}$) bilden eine Basis der Topologie von X_M. Nun bedeutet $|\alpha(f) - \frac{m}{n}| < \frac{1}{n}$, daß $|\alpha(nf - m)| < 1$, also $\alpha(1 \pm (nf - m)) > 0$ ist. Wir können uns also auf Mengen der Form

$$\{\xi_\alpha\colon \alpha \in X_M,\ \alpha(1 \pm f) > 0\}$$

mit $f \in A$ beschränken. Diese Menge ist gleich $U(1 + f, 1 - f) \cap X(M)_{\mathrm{arch}}$. □

5.18 Satz. *Sei M eine archimedische Halbgruppe in A. Dann ist $X(M)_{\mathrm{arch}} = X(M)^{\max}$, und die Abbildung aus 5.17 ist ein Homöomorphismus $X_M \to X(M)^{\max}$ kompakter topologischer Räume.*

Beweis. $X(M)_{\mathrm{arch}} \subseteq X(M)^{\max}$ gilt ohnehin (Satz 5.17). Umgekehrt sei ξ ein abgeschlossener Punkt in $X(M)$, sei $\mathfrak{p} = \operatorname{supp}(\xi)$. Nach Satz II.5.15 ist die Ringerweiterung $A/\mathfrak{p} \subseteq \kappa(\mathfrak{p})$ archimedisch bezüglich ξ. Wegen M archimedisch gibt

es zu jedem $f \in A$ ein $n \in \mathbb{N}$ mit $n \pm f \in M$. Wegen $\xi \in X(M)$ ist insbesondere $\pm f \leq_\xi n$. Also ist der angeordnete Körper $(\kappa(\mathfrak{p}), \xi)$ archimedisch, d.h. es ist $\xi \in X(M)_{\mathrm{arch}}$. Damit ist $X(M)_{\mathrm{arch}} = X(M)^{\max}$ gezeigt. Die Teilmenge $X(M)^{\max}$ von $\mathrm{Sper}(A)$ ist kompakt, siehe Satz II.4.16(b).

Tatsächlich gibt es für die Kompaktheit von X_M ein noch einfacheres Argument. Denn für jedes $f \in A$ gibt es ein $N_f \in \mathbb{N}$ mit $N_f \pm f \in M$. Somit ist

$$X_M \subseteq \prod_{f \in A} [-N_f, N_f] \subseteq \mathbb{R}^A.$$

Der rechte Raum ist kompakt (Satz von Tykhonov), und X_M ist darin abgeschlossen (Lemma 5.14), also selbst kompakt. □

5.19 Bemerkung. Für die Aussage des Satzes ist die Archimedizität von M nicht notwendig. Es genügt vielmehr folgende Beschränktheitseigenschaft der abgeschlossenen Menge $X(M) \subseteq \mathrm{Sper}(A)$: Zu jedem $f \in A$ gibt es ein $N \in \mathbb{N}$ mit $N - f \geq 0$ auf $X(M)$. Das ist eine geometrische Bedingung. Ist etwa $A = \mathbb{R}[V]$ der Koordinatenring einer affinen $\mathbb{R}$-Varietät V, so bedeutet dies gerade, daß die abgeschlossene Teilmenge X_M von $V(\mathbb{R})$ kompakt ist. Hingegen ist die Archimedizität von M eine feinere Bedingung von arithmetischer Natur.

Wir können jetzt Theorem 5.12 auch wie folgt ausdrücken:

5.20 Korollar. *Sei M ein archimedischer Modul über einem erzeugenden Semiring von A. Ist $X_M = \varnothing$, so ist $-1 \in M$ (also $M = A$).*

Beweis. Wäre $-1 \notin M$, so wäre $X(M) \neq \varnothing$ nach Theorem 5.12, und aus Satz 5.18 (Homöomorphismus $X_M \approx X(M)^{\max}$) würde folgen $X_M \neq \varnothing$. □

6. Der archimedische Positivstellensatz

Wir beweisen den Satz für Moduln über archimedischen Semiringen und für archimedische quadratische Moduln. Der folgende Hilfsbegriff dient nur dazu, einen einheitlichen Beweis zu geben:

6.1 Definition. Ein Semiring S von A heißt eine *Quasipräordnung*, wenn gilt: Zu jedem $f \in A$ gibt es beliebig große Zahlen $m \in \mathbb{N}$ mit $(f + 2^m)^2 \in S$.

Die wesentlichen Beispiele von Quasipräordnungen sind einerseits Präordnungen, andererseits archimedische Semiringe.

6.2 Lemma. *Jede Quasipräordnung S von A ist erzeugend, d.h. es gilt $S - S = A$.*

6.3 Theorem. (Archimedischer Positivstellensatz) *Sei S eine Quasipräordnung in A, und sei M ein archimedischer S-Modul. Für $f \in A$ sind äquivalent:*

(i) *$f > 0$ auf X_M;*
(ii) *es gibt $n \in \mathbb{N}$ mit $nf \in 1 + M$.*

Die beiden wichtigen Fälle, bei denen dieses Theorem greift, sind also einerseits Moduln über archimedischen Semiringen, andererseits archimedische quadratische Moduln.

Beweis. Die Implikation (ii) ⇒ (i) ist klar, denn aus $nf \in 1 + M$ folgt $nf \geq 1$ auf X_M, also $f \geq \frac{1}{n} > 0$ auf X_M. Die nichttriviale Aussage ist also (i) ⇒ (ii). Sei $M' = M - Sf$. Dies ist ein archimedischer S-Modul mit $X_{M'} = \varnothing$. Nach Korollar

5.20 folgt $-1 \in M'$ (beachte, daß S erzeugend ist nach Lemma 6.2). Es gibt also $s \in S$ mit $sf-1 \in M$. Wegen M archimedisch gibt es $k \in \mathbb{N}$ mit $2k-1-s^2f \in M$, und es folgt

$$2k - s \;=\; (2k - 1 - s^2 f) + s(sf-1) + 1 \;\in M.$$

Da S eine Quasipräordnung ist, können wir nach eventuellem Vergrößern von k zusätzlich erreichen, daß $(k-s)^2 \in S$ und k eine 2-Potenz ist. Wegen M archimedisch gibt es $l \in \mathbb{N}$ mit $f + l \in M$. Sei

$$Q \;:=\; \{(m,n) \colon m \in \mathbb{N},\; n \in \mathbb{Z},\; mf + n \in M\}.$$

Es ist also $(1,l) \in Q$. Sei allgemeiner $(m,n) \in Q$ mit $n \geq 0$. Wegen $mf+n \in M$ liegt dann auch

$$k^2 mf + (k^2 n - m) \;=\; (k-s)^2(mf+n) + 2km(sf-1) + ns(2k-s) + m(2k-1-s^2f)$$

in M. Es gilt also

$$(m,n) \in Q \;\text{ und }\; n \geq 0 \quad\Rightarrow\quad (k^2 m,\, k^2 n - m) \in Q.$$

Startend mit $(1,l) \in Q$ erhalten wir also nacheinander $(1,l)$, $(k^2,\, k^2 l - 1)$, $(k^4,\; k^4 l - 2k^2)$, $\ldots \;\in Q$, und zwar so weit, bis erstmals der zweite Eintrag negativ wird. Genauer folgt also

$$k^{2j}(k^2,\, k^2 l - j - 1) \;\in\; Q$$

für $j = 0, 1, \ldots, k^2 l$ (Induktion). Für $j = k^2 l$ ergibt sich insbesondere $(k^{2j+2},\, -k^{2j}) \in Q$. Das bedeutet $k^{2j+2} f - k^{2j} \in M$, und insbesondere $k^{2j+2} f \in 1 + M$. □

6.4 Bemerkungen.

1. Der Beweis hat gezeigt, daß wir die Zahl n in (ii) als 2-Potenz wählen können.

2. Das Schlüsselargument im letzten Beweis wird transparenter, wenn man $\mathbb{Q} \subseteq A$ und $\mathbb{Q}_+ \subseteq S$ annimmt. Dann ist $(m,n) \in Q$ äquivalent zu $f + \frac{n}{m} \in M$, und der entscheidende Schritt besagt: Aus $0 \leq q \in \mathbb{Q}$ und $f + q \in M$ folgt auch $f + q - \frac{1}{k^2} \in M$. Nach endlich vielen Schritten hat man also ein negatives $q \in \mathbb{Q}$ mit $f + q \in M$ gefunden.

Beim archimedischen Positivstellensatz handelt es sich im wesentlichen um einen *nennerfreien* Positivstellensatz. Das wird aus folgender Formulierung deutlich:

6.5 Korollar. *Sei M ein archimedischer Modul über einer Quasipräordnung S mit $\frac{1}{2} \in S$, und sei $f \in A$ mit $f > 0$ auf X_M. Dann ist $f \in M$.*

Beweis. In Theorem 6.3 gibt es ein $m \geq 0$ mit $2^m f \in 1 + M$, siehe Bemerkung 6.4.1. Wegen $\frac{1}{2} \in S$ ergibt Division durch 2^m also $f \in 2^{-m} + M \subseteq M$. □

6.6 Korollar. *Sei $M \subseteq A$ ein archimedischer quadratischer Modul oder ein Modul über einem archimedischen Semiring S mit $\frac{1}{2} \in S$. Jedes $f \in A$ mit $f > 0$ auf X_M liegt in M.* □

6.7 Bemerkungen.

1. Die Aussage (i) ⇒ (ii) des archimedischen Positivstellensatzes 6.3 ist viel stärker als beim Positivstellensatz von Stengle (II.2.7). Auf der anderen Seite wird die Voraussetzung der Archimedizität gebraucht, während Stengles Satz ohne jede Voraussetzung gilt.

2. Im Fall, wo $M = S$ eine (archimedische) Präordnung ist, vereinfacht sich der Beweis von Theorem 6.3 erheblich. Denn wegen S archimedisch folgt aus $f > 0$ auf X_S schon $f > 0$ auf $X(S)$, nach Satz 5.18, und Stengles Positivstellensatz gibt also

ein $s \in S$ mit $sf \in 1+S$ (das ist der erste Schritt im Beweis von 6.3). Man braucht also Korollar 5.20 bzw. Theorem 5.12 nicht zu verwenden, und kann direkt in den Beweis von 6.3 einsteigen.

3. Ist M ein Modul über einem archimedischen Semiring S, so ist M natürlich selbst archimedisch. Für die Aussage von Theorem 6.3 genügt es im allgemeinen aber *nicht*, daß M ein archimedischer Modul über einem erzeugenden Semiring ist. Für ein Beispiel siehe Aufgabe 9.

4. Jacobi hat den Positivstellensatz auch für archimedische Moduln über dem Semiring ΣA^{2n} (mit $n \in \mathbb{N}$) bewiesen (Dissertation, Konstanz 1999).

Die Aussage des archimedischen Positivstellensatzes läßt sich auch als Nichtnegativstellensatz formulieren:

6.8 Korollar. (Archimedischer Nichtnegativstellensatz) *Sei M ein archimedischer Modul über einer Quasipräordnung S von A mit $\frac{1}{2} \in S$. Für jedes $f \in A$ sind dann äquivalent:*

(i) $f \geq 0$ *auf* X_M,
(ii) $\forall\, n \in \mathbb{N} \;\; 1 + nf \in M$.

BEWEIS. (ii) $\Rightarrow$ (i) ist klar: Wäre $f(\alpha) < 0$ für ein $\alpha \in X_M$, so wäre $f(\alpha) < -\frac{1}{n}$ für ein $n \in \mathbb{N}$, und somit $(1+nf)(\alpha) < 0$, also $1+nf \notin M$. Ist umgekehrt $f \geq 0$ auf X_M, und ist $n \in \mathbb{N}$, so ist $1 + nf > 0$ auf X_M. Aus 6.5 folgt also $1 + nf \in M$. □

6.9 Bemerkung. Aus Korollar 6.8 erhält man die Aussage des Positivstellensatzes 6.5 auch wieder zurück. Denn ist $f > 0$ auf X_M, so gibt es $m \geq 0$ mit $f \geq \frac{1}{2^m}$ auf X_M, da X_M kompakt ist. Anwendung von 6.8 auf $f - 2^{-m}$ mit $n = 2^m$ gibt $1 + 2^m(f - 2^{-m}) = 2^m f \in M$, also auch $f \in M$.

Die Archimedizität eines Moduls M ist nicht nur hinreichend für die Aussage des Positivstellensatzes, sondern bei kompaktem X_M auch notwendig:

6.10 Korollar. *Sei M ein Modul über einer Quasipräordnung S mit $\frac{1}{2} \in S$. Genau dann ist M archimedisch, wenn X_M kompakt ist und M jedes $f \in A$ mit $f > 0$ auf X_M enthält.*

BEWEIS. Ist M archimedisch, so ist X_M kompakt (5.18), und M enthält die auf X_M strikt positiven Elemente (6.5). Umgekehrt sei X_M kompakt, und M enthalte jedes auf X_M strikt positive Element. Ist $f \in A$, so gibt es ein $n \in \mathbb{N}$ mit $n \pm f > 0$ auf X_M, wegen X_M kompakt und $\overline{f}$ stetig (5.16). Es folgt $n \pm f \in M$, und somit ist M archimedisch. □

Deshalb ist die Bedingung der Archimedizität von M eine Verschärfung (von arithmetischer Natur) der Kompaktheit von X_M.

In der Literatur werden archimedischer Positiv- bzw. Nichtnegativstellensatz häufig als Darstellungssatz bezeichnet. Zur Erklärung:

Ist X ein topologischer Raum und $B \subseteq C(X, \mathbb{R})$ ein Teilring, so schreibe $B_+ := \{f \in B \colon \forall\, x \in X \;\; f(x) \geq 0\}$. Die Ausgangsfrage des Darstellungssatzes war das Problem, in rein algebraischer Weise zu charakterisieren, wann ein Paar (A, S) aus einem kommutativen Ring A und einem Semiring S in A isomorph ist zu einem Paar (B, B_+) für einen Teilring B von $C(X, \mathbb{R})$ und einen kompakten topologischen Raum X.

6.12 Korollar. *Sei A ein Ring und S ein Semiring in A mit $\frac{1}{2} \in S$. Genau dann gibt es einen kompakten Raum X und einen Teilring B von $C(X,\mathbb{R})$ mit $(A,S) \cong (B,B_+)$, wenn die folgenden Bedingungen erfüllt sind:*

(1) *S ist archimedisch;*
(2) *$S \cap (-S) = \{0\}$;*
(3) *aus $f \in A$ und $1+nf \in S$ für alle $n \in \mathbb{N}$ folgt $f \in S$.*

Tatsächlich läßt sich dann erreichen, daß B ein dichter Teilring von $C(X,\mathbb{R})$ ist.

Dicht bezieht sich auf die Norm $||g|| = \max\{|g(x)|\colon x \in X\}$ der gleichmäßigen Konvergenz für $g \in C(X,\mathbb{R})$.

Beweis. Eigenschaften (1)–(3) sind offensichtlich erfüllt, wenn $(A,S) = (B,B_+)$ mit einem kompakten Raum X und einem Teilring B von $C(X,\mathbb{R})$ ist. Umgekehrt erfülle (A,S) die Bedingungen (1)–(3). Wegen S archimedisch ist der topologische Raum X_S kompakt. Für den Ringhomomorphismus

$$\Phi_S\colon\ A \to C(X_S,\mathbb{R}), \quad f \mapsto \widehat{f}$$

(5.16) gilt $\Phi_S^{-1}(C_+(X_S,\mathbb{R})) = S$ wegen Korollar 6.8 und Bedingung (3). Wegen (2) ist Φ_S injektiv. Aus dem Satz von Stone-Weierstraß folgt, daß $\Phi(A)$ ein dichter Teilring von $C(X_S,\mathbb{R})$ ist: Denn $\Phi(A)$ trennt die Punkte von X_S, und wegen $\frac{1}{2} \in A$ ist $\mathbb{R} \subseteq \overline{\Phi(A)}$, also $\overline{\Phi(A)} = C(X,\mathbb{R})$ nach Stone-Weierstraß. □

7. Erste Anwendungen: Sätze von Pólya und Handelman

7.1 Theorem. (Pólya 1928) *Sei $f \in \mathbb{R}[x_0,\dots,x_n]$ ein homogenes Polynom. Es sind äquivalent:*

(i) *f hat auf $C := \{\xi \in \mathbb{R}^{n+1}\colon \xi_0 \geq 0,\dots,\xi_n \geq 0\} \setminus \{(0,\dots,0)\}$ strikt positive Werte;*
(ii) *es gibt ein $N \geq 1$, so daß alle Koeffizienten der Form $(x_0+\cdots+x_n)^N \cdot f$ strikt positiv sind.*

Beweis. Sei $h = x_0 + \cdots + x_n$. Aus (ii) folgt, daß $h^N f$ auf C strikt positiv ist. Wegen $h|_C > 0$ folgt also $f|_C > 0$. Die wesentliche Aussage ist (i) ⇒ (ii). Sie läßt sich wie folgt durch Anwendung des Positivstellensatzes auf einen geeigneten archimedischen Semiring beweisen. Betrachte das Zariski-offene Komplement $V = \mathbb{P}^n \setminus \mathcal{V}_+(h)$ der Hyperebene $\{h=0\}$ in $\mathbb{P}^n$. Dies ist eine (zu $\mathbb{A}^n$ isomorphe) affine $\mathbb{R}$-Varietät mit Koordinatenring $\mathbb{R}[V] = \mathbb{R}[\frac{x_0}{h},\dots,\frac{x_n}{h}]$. In $\mathbb{R}[V]$ betrachten wir den von $\mathbb{R}_+$ und $\frac{x_0}{h},\dots,\frac{x_n}{h}$ erzeugten Semiring S. Wegen $\frac{x_0}{h}+\cdots+\frac{x_n}{h} = 1$ gilt $1-\frac{x_i}{h} \in S$ für $i = 0,\dots,n$. Nach Satz 5.7(a) ist also S archimedisch. Es gilt

$$X_S \ =\ \big\{(\xi_0 : \cdots : \xi_n) \in V(\mathbb{R})\colon \xi_0 \geq 0,\dots,\xi_n \geq 0\big\}.$$

Sei $d = \deg(f)$. Es ist $\frac{f}{h^d} \in \mathbb{R}[V]$, und nach Voraussetzung ist $\frac{f}{h^d} > 0$ auf X_S. Nach dem Positivstellensatz (siehe 6.6) folgt $\frac{f}{h^d} \in S$. Es ist also $\frac{f}{h^d} \in S$, d.h. es gibt eine Identität

$$\frac{f}{h^d} \ =\ \sum_{e \in \mathbb{Z}_+^{n+1}} c_e \frac{x_0^{e_0}\cdots x_n^{e_n}}{h^{e_0+\cdots+e_n}}$$

mit reellen $c_e \geq 0$ (und $c_e = 0$ für fast alle e). Multiplikation mit h^m für genügend großes $m \in \mathbb{N}$ liefert ein $N \geq 0$, so daß alle Koeffizienten der Form $h^N f$ nichtnegativ sind.

Wir zeigen, daß man die Koeffizienten von $h^N f$ sogar strikt positiv machen kann. Auf dem kompakten Standard n-Simplex

$$\Delta \ :=\ \big\{\xi \in \mathbb{R}^{n+1}\colon \xi_0 \geq 0,\dots,\xi_n \geq 0,\ \sum_i \xi_i = 1\big\}$$

ist $f > 0$, also gibt es $\varepsilon > 0$ mit $f > \varepsilon > 0$ auf Δ. Die Form $f_1 := f - \varepsilon h^d$ ist also strikt positiv auf Δ, und damit wegen Homogenität auf ganz C. Nach der schon bewiesenen Aussage gibt es $N \geq 0$, so daß $h^N f_1$ nichtnegative Koeffizienten hat. Wegen $h^N f = h^N f_1 + \varepsilon h^{N+d}$ sind alle Koeffizienten von $h^N f$ sogar strikt positiv $(\geq \varepsilon)$. □

7.2 Bemerkungen.

1. Die inhomogene Version von Pólyas Satz ist falsch. Siehe Aufgabe 10.

2. Die Aussage von Pólyas Satz läßt sich über jedem reell abgeschlossenen Körper R betrachten. Sie wird aber falsch, wenn R nicht archimedisch ist. Als Beispiel betrachte die quadratische Form

$$f \;=\; (x+y)^2 + c(x-y)^2$$

mit $c \in R$ und $c > n$ für alle $n \in \mathbb{N}$. Siehe Aufgabe 11.

3. An Pólyas Satz schließt sich die Frage nach der Komplexität der Aussage an. Wie groß muß man den Exponenten N wählen, und von welchen Eigenschaften der Form f hängt das ab? Sei $f \in \mathbb{R}[x_0, \ldots, x_n]$ homogen vom Grad d, und schreibe

$$f \;=\; \sum_{|\alpha|=d} \frac{d!}{\alpha_0! \cdots \alpha_n!}\, c_\alpha\, x_0^{\alpha_0} \cdots x_n^{\alpha_n}.$$

Sei $\Delta \subseteq \mathbb{R}^{n+1}$ das Standard n-Simplex wie im vorigen Beweis. Sei $c = \max_\alpha |c_\alpha|$ und $\lambda := \min f(\Delta) > 0$. Powers und Reznick (1999) haben gezeigt: Für

$$N \;>\; \frac{d}{2}\,(d-1)\,\frac{c}{\lambda} - d$$

hat $(x_0 + \cdots + x_n)^N f$ positive Koeffizienten. Diese Schranke hängt nicht ab von der Zahl $n+1$ der Variablen. Im allgemeinen ist die Schranke sogar scharf, siehe Aufgabe 11 für $d = 2$.

Hier ist eine weitere Anwendung des archimedischen Positivstellensatzes:

7.3 Theorem. (Handelman 1988) *Seien $f_1, \ldots, f_r \in \mathbb{R}[x_1, \ldots, x_n]$ lineare Polynome derart, daß das Polyeder $K := \{\xi \in R^n \colon f_i(\xi) \geq 0,\ i = 1 \ldots, r\}$ kompakt und nicht leer ist. Dann gibt es für jedes Polynom f mit $f|_K > 0$ eine endliche Summendarstellung*

$$f \;=\; \sum_{\alpha \in \mathbb{Z}_+^r} c_\alpha\, f_1^{\alpha_1} \cdots f_r^{\alpha_r}$$

mit reellen $c_\alpha \geq 0$.

Für den Beweis brauchen wir:

7.4 Theorem. (Minkowski 1896) *Seien $f, f_1, \ldots, f_r \in \mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1, \ldots, x_n]$ lineare Polynome. Das Polyeder*

$$K \;:=\; \{x \in \mathbb{R}^n \colon f_1(x) \geq 0, \ldots, f_r(x) \geq 0\}$$

sei nicht leer. Dann sind äquivalent:

(i) *$f \geq 0$ auf K;*
(ii) *es gibt $a_0, \ldots, a_r \geq 0$ in $\mathbb{R}$ mit $f = a_0 + a_1 f_1 + \cdots + a_r f_r$.*

Beweis siehe Vorlesung *Konvexität*, Satz 5.16.

7.5 Beweis von Theorem 7.3: In der Situation von Handelmans Satz sei S der von $\mathbb{R}_+$ und $f_1, \ldots, f_r$ erzeugte Semiring in $\mathbb{R}[\mathbf{x}]$. Es ist $X_S = K$, und die Aussage

von 7.3 ist, daß S jedes auf K positive Polynom enthält. Aus Theorem 7.4 folgt, daß S archimedisch ist: Ist $0 < c \in \mathbb{R}$ mit $K \subseteq [-c, c]^n$, so gilt $c \pm x_i \in S$ $(i = 1, \ldots, n)$ nach 7.4, und S ist somit archimedisch nach Satz 5.7(a). Deshalb folgt Theorem 7.3 aus Theorem 7.4 und dem archimedischen Positivstellensatz.

Handelmans Theorem können wir wie folgt verschärfen:

7.6 Korollar. *Seien $f_1, \ldots, f_r$ lineare Polynome in $\mathbb{R}[\mathbf{x}]$, so daß das Polyeder $K = S(f_1, \ldots, f_r)$ kompakt und nicht leer ist. Sei S der von $f_1, \ldots, f_r$ und $\mathbb{R}_+$ erzeugte Semiring in $\mathbb{R}[\mathbf{x}]$. Für beliebige Polynome $g_1, \ldots, g_s \in \mathbb{R}[\mathbf{x}]$ gilt dann: Jedes auf $K \cap S(g_1, \ldots, g_s)$ strikt positive Polynom liegt in*

$$M \;:=\; S + Sg_1 + \cdots + Sg_s.$$

Beweis. Der Semiring S ist archimedisch, wie oben gezeigt. Die Behauptung folgt also aus Korollar 6.6. □

7.7 Bemerkungen.

1. Die Voraussetzung $K \neq \varnothing$ ist notwendig in 7.3 und 7.4, wie das Beispiel $n = 2$ und $f_1 = x_1 - 1$, $f_2 = -x_1$, $f = x_2$ zeigt.

2. Theorem 7.3 bleibt richtig, wenn $\mathbb{R}$ durch einen archimedischen reell abgeschlossenen Körper R ersetzt wird, wird über nicht archimedischem R aber im allgemeinen falsch.

3. Ist $f|_K$ lediglich nichtnegativ in Handelmans Theorem 7.3, so wird die Aussage i.a. falsch. Beispiele (für $n \geq 3$) werden wir später sehen.

4. Die Linearität der f_i in 7.3 ist entscheidend. Betrachte etwa den von x und $1-x^2$ und $\mathbb{R}_+$ erzeugten Semiring S in $\mathbb{R}[x]$. Hier ist $X_S = [0, 1]$ kompakt, aber S ist nicht archimedisch, denn $N - x \notin S$ für alle $N > 0$. (In jedem Produkt $x^i(1-x^2)^j$ hat x einen nichtnegativen Koeffizienten.) Der Positivstellensatz ist also falsch.

Nach einer kleinen Störung eines Erzeugers wird S jedoch archimedisch: Für jedes $a > 0$ ist der von $x - a$ und $1 - x^2$ erzeugte $\mathbb{R}$-Semiring S_a archimedisch, denn

$$(a^2 + 1) - 2ax \;=\; (x - a)^2 + (1 - x^2) \;\in S_a.$$

5. Ein weiteres klassisches Resultat, das mit Hilfe des archimedischen Positivstellensatzes einen einfachen Beweis hat, ist Quillens Theorem: Zu jedem auf der $(2n-1)$-Sphäre

$$|z_1|^2 + \cdots + |z_n|^2 \;=\; 1$$

in $\mathbb{C}^n$ strikt positiven reellen Polynom $f \in \mathbb{C}[z, \overline{z}]$ (mit $f = f^*$, d.h. $f(\overline{z}) = \overline{f(z)}$) gibt es endlich viele holomorphe Polynome $g_1(z), \ldots, g_r(z) \in \mathbb{C}[z]$ mit

$$f(z, \overline{z}) \;=\; \sum_{j=1}^{r} |g_j(z)|^2$$

auf $||z||^2 = \sum_j |z_j|^2 = 1$. Siehe Aufgabe 12.

8. Schmüdgens Theorem und Folgerungen

8.1 Theorem. (Schmüdgen 1991) *Seien $f_1, \ldots, f_r \in \mathbb{R}[x_1, \ldots, x_n]$ Polynome derart, daß die Menge $K = S(f_1, \ldots, f_r) \subseteq \mathbb{R}^n$ kompakt ist. Dann enthält $PO(f_1, \ldots, f_r)$ jedes auf K strikt positive Polynom.*

8.2 Korollar. *Sei V eine affine $\mathbb{R}$-Varietät, und sei $V(\mathbb{R})$ kompakt. Jede auf $V(\mathbb{R})$ strikt positive reguläre Funktion $f \in \mathbb{R}[V]$ ist eine Quadratsumme in $\mathbb{R}[V]$.*

BEWEIS. Sei $V \subseteq \mathbb{A}^n$ abgeschlossen, sei das Verschwindungsideal $I = \mathfrak{I}(V)$ erzeugt von $f_1, \dots, f_r \in \mathbb{R}[\mathbf{x}]$. Für die Präordnung $T = PO(\pm f_1, \dots, \pm f_r)$ in $\mathbb{R}[\mathbf{x}]$ gilt $T = \Sigma\mathbb{R}[\mathbf{x}]^2 + I$, und $S(\pm f_1, \dots, \pm f_r) = V(\mathbb{R})$. Die Aussage ist also ein Spezialfall von 8.1. □

Der folgende Beweis stammt von Wörmann.

8.3 Theorem. *Sei k ein Ring und A eine endlich erzeugte k-Algebra. Sei T eine Präordnung in A derart, daß $T \cap k$ archimedisch in k und X_T kompakt ist. Dann ist T archimedisch.*

Korrektur: Man muß zusätzlich voraussetzen, daß die Präordnung T endlich erzeugt ist. Andernfalls wird die Aussage im allgemeinen falsch. Siehe auch im Beweis unten die Ergänzung in Rot. Herzlichen Dank an Thorsten Mayer, der mich darauf aufmerksam machte, daß hier ein Problem vorliegt! (29. 7. 2016)

BEWEIS. Sei A als k-Algebra erzeugt von $x_1, \dots, x_n$. Betrachte den Teilring $O_A(T)$ von A (5.6). Wegen $T \cap k$ archimedisch in k ist $k \subseteq O_A(T)$. Es genügt deshalb, ein $N \in \mathbb{N}$ mit $N - \sum_i x_i^2 \in T$ zu finden. Denn dann folgt $x_1, \dots, x_n \in O_A(T)$ (wegen $N + 1 \pm 2x_i = (N - x_i^2) + (x_i + 1)^2$), und somit $O_A(T) = A$, d.h. T ist archimedisch.

Wegen X_T kompakt gibt es $c \in \mathbb{N}$ mit $\sum_i x_i^2 < c$ auf X_T. Wir setzen $f := c - \sum_i x_i^2$. Man muß nun argumentieren, daß $f > 0$ nicht nur auf X_T gilt, sondern auch auf $X(T)$. Dazu braucht man die endliche Erzeugtheit von T. Nach Stengles Positivstellensatz II.2.7 gibt es $t \in T$ mit

$$(1 + t)f \in T. \tag{4}$$

Daraus folgt auch

$$(1 + t)f + t \cdot \sum_i x_i^2 \;=\; f + ct \;\in T. \tag{5}$$

Sei $Q = T + fT$, die von T und f erzeugte Präordnung. Nach (4) ist

$$(1 + t)Q \;\subseteq T. \tag{6}$$

Wegen $f \in Q$ und der Bemerkung zu Beginn ist Q archimedisch. Also gibt es $a \in \mathbb{N}$ mit $a - t \in Q$. Aus (6) folgt also

$$c(1 + t)(a - t) \;=\; ca + c(a - 1)t - ct^2 \in T. \tag{7}$$

Schließlich ist

$$c\Big(\frac{a}{2} - t\Big)^2 \;=\; c\frac{a^2}{4} - act + ct^2 \;\in T. \tag{8}$$

Addition von (5), (7) und (8) gibt

$$f + c\Big(a + \frac{a^2}{4}\Big) \;\in T,$$

also

$$c\Big(1 + a + \frac{a^2}{4}\Big) - \sum_i x_i^2 \;\in T,$$

und das Theorem ist bewiesen. □

8.4 Theorem 8.1 folgt aus Theorem 8.3 und dem archimedischen Positivstellensatz: Für die Präordnung $T := PO(f_1, \dots, f_r)$ in $\mathbb{R}[\mathbf{x}]$ ist $X_T = K$ kompakt, also ist T archimedisch nach 8.3. In der Formulierung 8.3 hat das Theorem aber auch andere interessante Anwendungen. Hier nur ein Beispiel:

8.5 Korollar. *Sei $V \subseteq \mathbb{R}^n$ eine durch Polynomgleichungen mit ganzen Koeffizienten definierte und kompakte reell-algebraische Menge. Zu jedem auf V strikt positiven Polynom $f \in \mathbb{Z}[\mathtt{x}]$ gibt es Polynome $g_1, \ldots, g_r \in \mathbb{Z}[\mathtt{x}]$ und $m \geq 0$ mit $2^m f = \sum_{i=1}^r g_i^2$ auf V.*

BEWEIS. Sei V die Nullstellenmenge von $f_1, \ldots, f_r \in \mathbb{Z}[\mathtt{x}]$ in $\mathbb{R}^n$. Sei $k = \mathbb{Z}[\frac{1}{2}]$ und $A = k[x_1, \ldots, x_n]/(f_1, \ldots, f_r)$, sowie $T = \Sigma A^2$. Es ist $X_T = V$ kompakt, und $T \cap k$ ist archimedisch in k (alle positiven Elemente in k sind sos in k). Also ist T archimedisch nach 8.3, und aus dem archimedischen Positivstellensatz folgt $f \in T$. Das ist die Aussage. □

8.8 Nun eine Reihe von Anwendungen von Schmüdgens Satz, zunächst auf Hilberts 17. Problem in der Version für Formen (= homogene Polynome). Sei also R ein reell abgeschlossener Körper und $f \in R[\mathtt{x}] = R[x_0, \ldots, x_n]$ eine psd Form. Wir machen die stärkere Annahme, daß f *positiv definit* ist, d.h. $f(\xi) > 0$ für alle $0 \neq \xi \in R^{n+1}$ gilt. Aus dem Stengleschen Positivstellensatz kann man ableiten:

> *Es gibt eine positiv definite Form h, so daß $h^2 f$ eine Summe von Quadraten (von Formen) ist.*

Siehe Korollar II.3.10, dort im inhomogenen Fall formuliert; daraus kann man auch den homogenen Fall ableiten.

Mit Hilfe von Schmüdgens Theorem können wir ein sehr viel stärkeres Resultat beweisen, *sofern der reell abgeschlossene Grundkörper R archimedisch ist*:

8.9 Theorem. *Seien f, h zwei positiv definite Formen in $\mathbb{R}[x_0, \ldots, x_n]$, und es gelte $\deg(h) \mid \deg(f)$. Dann gibt es ein $N \in \mathbb{N}$ derart, daß $h^N f$ eine Summe von Quadraten von Formen ist.*

8.10 Korollar. *Für jede positiv definite Form $f \in \mathbb{R}[x_0, \ldots, x_n]$ ist*

$$(x_0^2 + \cdots + x_n^2)^N \cdot f$$

eine Quadratsumme für $N \gg 0$. □

BEWEIS VON 8.9. Setze $\mathtt{x} = (x_0, \ldots, x_n)$. Sei m die durch $\deg(f) = m \deg(h)$ bestimmte Zahl. Sei V das Komplement der Hyperfläche $h = 0$ in $\mathbb{P}^n$. Dann ist V eine affine $\mathbb{R}$-Varietät, und $V(\mathbb{R}) = \mathbb{P}^n(\mathbb{R})$ ist kompakt. Der Koordinatenring von V ist der Teilring von $\mathbb{R}[\mathtt{x}]_h$ aus allen Brüchen von Formen gleichen Grades. Nach Voraussetzung ist $\frac{f}{h^m} \in \mathbb{R}[V]$ strikt positiv auf $V(\mathbb{R})$. Nach Schmüdgen ist $\frac{f}{h^m}$ also eine Summe von Quadraten in $\mathbb{R}[V]$. Das bedeutet: Es gibt $k \geq 0$ und Formen $g_1, \ldots, g_r \in \mathbb{R}[\mathtt{x}]$ vom Grad $k \cdot \deg(h)$ mit

$$\frac{f}{h^m} \;=\; \frac{1}{h^{2k}} \sum_{i=1}^r g_i^2.$$

Multiplikation mit h^{2N} für $N \gg 0$ liefert die Behauptung. □

8.11 Bemerkungen.

1. Gemäß Artins Lösung von Hilberts 17. Problem gibt es zu jeder *nichtnegativen* Form $f \in \mathbb{R}[\mathtt{x}]$ eine homogene Quadratsumme $h \neq 0$ derart, daß fh eine Summe von Formenquadraten ist. Korollar 8.10 besagt, daß man h als Potenz von $h_0 := x_0^2 + \cdots + x_n^2$ wählen kann, sofern f positiv definit ist. In diesem Sinn ist h_0 ein *uniformer Nenner* für positiv definite Formen.

2. Für $n \leq 2$ gilt tatsächlich eine noch stärkere Aussage: h_0 ist ein uniformer Nenner für alle *nichtnegativen* Formen. Für $n \geq 3$ gibt es dagegen keinen uniformen Nenner für alle nichtnegativen Formen. Beides werden wir später beweisen.

3. Die Aussage von Theorem 8.9 gilt auch ohne die Voraussetzung $\deg(h) \mid \deg(f)$. In diesem Sinn ist jede positiv definite (nichtkonstante) Form ein uniformer Nenner für positiv definite Formen.

Eine weitere Folgerung aus Schmüdgens Theorem ist folgende Charakterisierung von archimedischen quadratischen Moduln:

8.12 Korollar. *Sei M ein quadratischer Modul in $\mathbb{R}[x_1, \ldots, x_n]$. Dann sind äquivalent:*

(i) *M ist archimedisch;*
(ii) *es gibt ein $c \in \mathbb{R}$ mit $c - \sum_i x_i^2 \in M$;*
(iii) *es gibt ein $f \in M$, so daß die Menge $X_f = \{f \geq 0\}$ in $\mathbb{R}^n$ kompakt ist;*
(iv) *X_M ist kompakt, und M enthält jedes $f \in \mathbb{R}[\mathbf{x}]$ mit $f > 0$ auf X_M.*

Interessant darin ist die Implikation (iii) $\Rightarrow$ (iv) (Putinars Positivstellensatz, 1993).

Beweis. (i) $\Rightarrow$ (ii) $\Rightarrow$ (iii) sind klar, und (i) $\Leftrightarrow$ (iv) wurde schon in 6.10 bemerkt. Gilt (iii), so ist die Präordnung $PO(f)$ archimedisch (Theorem 8.3). Erst recht ist dann M archimedisch, wegen $PO(f) \subseteq M$. □

Für Präordnungen T in $\mathbb{R}[x_1, \ldots, x_n]$ gibt Schmüdgens Satz ein sehr einfaches Kriterium dafür, wann T archimedisch ist, nämlich die Kompaktheit von X_T. Es fragt sich, ob es für quadratische Moduln M in $\mathbb{R}[\mathbf{x}]$ ein ähnliches Kriterium gibt. Die Kompaktheit von M genügt nicht, wie das folgende Beispiel zeigt:

8.13 Beispiel. Sei M der von

$$g_i \;=\; 2x_i - 1 \;\; (i = 1, \ldots, n), \;\; g_{n+1} = 1 - x_1 \cdots x_n$$

in $\mathbb{R}[x_1, \ldots, x_n]$ erzeugte quadratische Modul. Die s.a. Menge

$$K \;=\; X_M \;=\; \Big\{\xi \in \mathbb{R}^n \colon \xi_i \geq \frac{1}{2} \;(i = 1, \ldots, n),\; \xi_1 \cdots \xi_n \leq 1\Big\}$$

ist kompakt, denn $\xi_i \leq 2^{n-1}$ $(i = 1, \ldots, n)$ für jedes $\xi \in K$. (Zeichnung!) Aber für $n \geq 2$ ist M nicht archimedisch. Anders gesagt, für jede reelle Zahl c gilt $c - \sum_i x_i^2 \notin M$.

Wir beweisen das für $n = 2$ mit einem elementaren Argument. Sei $c \in \mathbb{R}$, angenommen es gebe sos Polynome $s_0, \ldots, s_3 \in \mathbb{R}[x, y]$ mit

$$c - (x^2 + y^2) \;=\; s_0 + s_1(2x - 1) + s_2(2y - 1) + s_3(1 - xy).$$

Sei t_i die Leitform von s_i $(i = 0, \ldots, 3)$. Die Leitformen der vier Summanden rechts sind also t_0, $2xt_1$, $2yt_2$, $-xyt_3$. Sei d das Maximum ihrer Grade. Wäre $d \leq 2$, so wären s_1, s_2, s_3 konstant und $\deg(s_0) \leq 2$, und Koeffizientenvergleich bei x^2 (oder y^2) gäbe einen Widerspruch. Also ist $d > 2$, und einige der vier Leitformen müssen sich zu 0 aufsummieren. Ist $d > 2$ gerade, so folgt $t_0 = xyt_3$, ist $d > 2$ ungerade, so folgt $xt_1 + yt_2 = 0$. Beides ist ein Widerspruch dazu, daß die Formen t_i alle psd (sogar sos) sind.

Ist $n \geq 3$, und wäre $c - \sum_{i=1}^n x_i^2 \in M$, so würde durch Substitution $x_3 = \cdots = x_n = 1$ folgen

$$c' - (x_1^2 + x_2^2) \;=\; s_0 + s_1(2x_1 - 1) + s_2(2x_2 - 1) + s_3(1 - x_1x_2)$$

mit $s_i \in \mathbb{R}[x_1, x_2]$ sos. Das widerspricht dem Fall $n = 2$.

8.14 Bemerkungen.

1. Sind $g_1, \dots, g_r \in \mathbb{R}[\mathbf{x}]$ so, daß $K = S(g_1, \dots, g_r)$ kompakt ist, so kann man $f \in \mathbb{R}[\mathbf{x}]$ so wählen, daß $f|_K \geq 0$ und $S(f)$ kompakt ist. Zum Beispiel $f = c^2 - \sum_i x_i^2$, falls $|\xi| \leq c$ für alle $\xi \in K$ ist. Der quadratische Modul $M := QM(g_1, \dots, g_r, f)$ ist dann archimedisch nach 8.12, d.h. jedes $p \in \mathbb{R}[\mathbf{x}]$ mit $p|_K > 0$ hat eine Darstellung

$$p \;=\; s_0 + \sum_{i=1}^{r} s_i g_i + tf$$

mit $s_0, \dots, s_r, t \in \mathbb{R}[\mathbf{x}]$ sos.

Das Beispiel in 8.13 hat Dimension ≥ 2. Tatsächlich gibt es in Dimension 1 kein solches Beispiel, wie wir jetzt zeigen.

8.15 Satz. *Sei $K/\mathbb{R}$ eine Körpererweiterung vom Transzendenzgrad eins. Jede Semiordnung von K ist eine Anordnung von K.*

Beweis. Kann annehmen, daß $K/\mathbb{R}$ endlich erzeugt ist. Sei M eine Semiordnung von K, und sei B die M-konvexe Hülle von $\mathbb{R}$ in K. Nach Satz 4.13 ist B ein Bewertungsring von K mit archimedisch angeordnetem Restklassenkörper. Also ist $B \neq K$, und B hat den Restklassenkörper $\mathbb{R}$. Wegen $\mathbb{R} \subseteq B$ ist B ein diskreter Bewertungsring.

Schreibe wieder $\leq$ für $\leq_M$. Sei t ein Primelement von B mit $t > 0$, wir zeigen zunächst $t(1 + \mathfrak{m}) > 0$. Sei $u = 1 + g$ mit $g \in \mathfrak{m}$. Wegen $\mathfrak{m}$ konvex (4.10) ist $t < u$, und wegen $\frac{t}{g^2} \notin B$ ist $\frac{t}{g^2} > 1$, also $t > g^2$. Es folgt

$$0 \;<\; u - t \;<\; \left(1 + \frac{g}{2}\right)^2 \;<\; u + t,$$

und daraus $0 < (u-t)^2 < (u+t)^2$ nach Lemma 4.6(d), also $tu > 0$ (vgl. mit dem Beweis von Satz 4.8). Da jede positive Einheit in B die Form $v = c^2(1+g)$ mit $c \in \mathbb{R}$ und $g \in \mathfrak{m}$ hat, ist $vt > 0$ für jedes solche v, und somit auch $vt^n > 0$ für alle $n \in \mathbb{Z}$. Folglich ist M eine Anordnung. □

8.16 Satz. *Sei M ein endlich erzeugter quadratischer Modul in $\mathbb{R}[\mathbf{x}]$. Es gelte $\dim \mathbb{R}[\mathbf{x}]/\mathrm{supp}(M) \leq 1$, und es sei X_M kompakt. Dann ist M archimedisch.*

Beweis. Jede Semiordnung N von $A := \mathbb{R}[\mathbf{x}]$ mit $M \subseteq N$ ist ein Positivkegel. Denn der Restklassenkörper des Primideals $\mathrm{supp}(N)$ ist ein Funktionenkörper über $\mathbb{R}$ von Dimension ≤ 1. Die von N darin induzierte Semiordnung ist also eine Anordnung nach Satz 8.15. Folglich ist auch N ein Positivkegel.

Nach Voraussetzung gibt es $c \in \mathbb{R}$ mit $\sum_i x_i^2 < c$ auf X_M. Für $f := c - \sum_i x_i^2 \in A$ und $M_1 := M - f\Sigma A^2$ gilt also $X_{M_1} = \varnothing$. Behaupte, es ist $-1 \notin M_1$. Andernfalls gäbe es nach Korollar 4.3 eine Semiordnung Q von A mit $M_1 \subseteq Q$. Aber Q ist ein Positivkegel nach eben. Es wäre also $X(M_1) \neq \varnothing$. Es ist M_1 endlich erzeugt, also ist $X(M_1)$ eine (basisch abgeschlossene) konstruierbare Menge in $\mathrm{Sper}\,\mathbb{R}[\mathbf{x}]$. Aus $X(M_1) \neq \varnothing$ folgt also auch $X_{M_1} \neq \varnothing$, Widerspruch.

Also ist $-1 \in M$, d.h. es gibt $s \in \Sigma A^2$ und $g \in M$ mit $-1 = g - sf$, also $sf = 1 + g$. Daraus folgt $S(g) \subseteq S(f)$, und insbesondere ist $S(g)$ kompakt. Nach Korollar 8.12 ist M also archimedisch. □

Hier noch eine weitere Anwendung auf archimedische quadratische Moduln. Zunächst zwei Lemmata.

8.17 Lemma. *Seien $g_1, \dots, g_r \in \mathbb{R}[x_0, \dots, x_n]$ Formen von geradem Grad mit $S(g_1, \dots, g_r) = \{0\}$. Dann gibt es sos Formen $s_0, \dots, s_r$ und ein $N \geq 0$ mit*

$$(x_0^2 + \cdots + x_n^2)^N + s_0 + \sum_{i=1}^{r} s_i g_i \;=\; 0$$

derart, daß alle Summanden homogen vom Grad $2N$ sind.

Umgekehrt folgt (für $\deg(g_i)$ gerade) aus einer solchen Identität auch wieder $S(g_1, \dots, g_r) = \{0\}$.

Beweis. Sei $h = x_0^2 + \cdots + x_n^2$, und sei $V = \mathbb{P}^n \smallsetminus V_+(h)$, das Komplement der projektiven Quadrik $h = 0$ wie im Beweis von Satz 8.9. Es ist V eine affine $\mathbb{R}$-Varietät, und $V(\mathbb{R})$ ist kompakt. Insbesondere ist jeder quadratische Modul in $\mathbb{R}[V]$ archimedisch nach Schmüdgen. Sei $\deg(g_i) = 2d_i$ $(i = 1, \dots, r)$, sei M der von den $\frac{g_i}{h^{d_i}}$ $(i = 1, \dots, r)$ in $\mathbb{R}[V]$ erzeugte quadratische Modul. Dann ist $X_M = \varnothing$. Da M archimedisch ist, ist $-1 \in M$ (Korollar 5.20). Das bedeutet eine Gleichung

$$-1 \;=\; \frac{s_0}{h^{2e_0}} + \sum_{i=1}^{r} \frac{s_i g_i}{h^{d_i + 2e_i}}$$

mit sos Formen s_i mit $\deg(s_i) = 4e_i$ $(i = 0, \dots, r)$. Durch Multiplikation mit h^N für $N \gg 0$ folgt eine Identität wie behauptet. □

8.18 Lemma. *Seien $f_1, \dots, f_r \in \mathbb{R}[\mathtt{x}]$, und sei $\tilde{f}_i$ die Leitform von f_i $(i = 1, \dots, r)$. Ist $S(\tilde{f}_1, \dots, \tilde{f}_r) = \{0\}$, so ist die Menge $S(f_1, \dots, f_r)$ kompakt.*

Beweis. Aufgabe 16. □

8.19 Satz. *Seien $g_1, \dots, g_r \in \mathbb{R}[\mathtt{x}] = \mathbb{R}[x_1, \dots, x_n]$ mit $S(\tilde{g}_1, \dots, \tilde{g}_r) = \{0\}$. Ist $\deg(g_i)$ gerade für $i = 1, \dots, r$, so ist der quadratische Modul $QM(g_1, \dots, g_r)$ in $\mathbb{R}[\mathtt{x}]$ archimedisch.*

Beweis. Nach Lemma 8.17 gibt es homogene Quadratsummen $s_0, \dots, s_r$ in $\mathbb{R}[\mathtt{x}]$ mit

$$s_0 + s_1 \tilde{g}_1 + \cdots + s_r \tilde{g}_r \;=\; -(x_1^2 + \cdots + x_n^2)^N,$$

wobei $N \geq 0$ ist und alle Summanden denselben Grad haben. Das Polynom

$$g \;:=\; s_0 + \sum_{i=1}^{r} s_i g_i \;\in\; \mathbb{R}[\mathtt{x}]$$

liegt in $M = QM(g_1, \dots, g_r)$, und die Leitform von g ist $-\big(\sum_i x_i^2\big)^N$, also negativ definit. Nach Lemma 8.18 ist also $S(g)$ kompakt, und aus Korollar 8.12 folgt, daß M archimedisch ist. □

Die Aussage von Satz 8.19 gilt genauso, wenn $\deg(g_i)$ ungerade ist für $i = 1, \dots, r$.

KAPITEL V

Ergänzungen zur kommutativen Algebra

1. Primvermeidung, Nakayama Lemma, Krullscher Hauptidealsatz

1.1 Lemma. *Sei A ein Ring, seien $I_1, \dots, I_r$ und J Ideale von A, und sei $J \subseteq I_1 \cup \dots \cup I_r$. Sind höchstens zwei der I_i nicht prim, so folgt $J \subseteq I_i$ für ein $i \in \{1, \dots, r\}$.*

Beweis. Induktion nach r, wobei der Beginn $r = 1$ trivial ist. Sei $r \geq 2$. Wir beweisen durch Widerspruch, angenommen $J \not\subseteq I_i$ für $i = 1, \dots, r$. Nach Induktionsvoraussetzung ist J nicht in einer Vereinigung von $r-1$ der I_i enthalten. Für $i = 1, \dots, r$ gibt es also ein $x_i \in J$ mit $x_i \notin I_j$ für alle $j \neq i$. Folglich ist $x_i \in I_i$.

Ist $r = 2$, so liegt $x_1 + x_2$ in J, aber nicht in $I_1 \cup I_2$, Widerspruch. Ist $r \geq 3$, so sei etwa I_1 ein Primideal. Dann liegt $x_1 + x_2 \cdots x_r$ in J, aber nicht in $\bigcup_i I_i$, erneut ein Widerspruch. □

1.2 Bemerkungen.

1. Enthält A einen unendlichen Körper k, so ist das Lemma sogar ohne jede Voraussetzung an die Ideale richtig. Denn ein k-Vektorraum ist niemals Vereinigung von endlich vielen echten Untervektorräumen.

2. Das Lemma besagt insbesondere: Ist ein Ideal J in keinem der Primideale $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ enthalten, so gibt es ein $x \in J$ mit $x \notin \mathfrak{p}_i$ $(i = 1, \dots, r)$. Deshalb spricht man von Vermeidung von Primidealen.

1.3 Korollar. *Seien $\mathfrak{p}_1, \dots, \mathfrak{p}_r$ Primideale von A mit $\mathfrak{p}_i \not\subseteq \mathfrak{p}_j$ für $i \neq j$. Sei $S := A \setminus (\mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_r)$, eine multiplikative Menge in A. Der Ring A_S der Brüche hat genau r verschiedene maximale Ideale, nämlich $\mathfrak{p}_i A_S$ für $i = 1, \dots, r$.*

Ein Ring heißt *semilokal*, wenn er nur endlich viele maximale Ideale hat. Der Ring A_S heißt die *Semilokalisierung* von A in $\mathfrak{p}_1, \dots, \mathfrak{p}_r$.

Beweis. Die Primideale von A_S sind genau die $\mathfrak{p}A_S$, wobei $\mathfrak{p}$ ein Primideal von A mit $\mathfrak{p} \subseteq \mathfrak{p}_1 \cup \dots \cup \mathfrak{p}_r$ ist. Nach Lemma 1.1 bedeutet das gerade $\mathfrak{p} \subseteq \mathfrak{p}_i$ für ein i. □

1.4 Definition. Sei A ein Ring. Das Ideal

$$\operatorname{Rad}(A) := \bigcap_{\mathfrak{m} \in \operatorname{Max} A} \mathfrak{m}$$

heißt das *Jacobson-Radikal* von A.

1.5 Bemerkungen.

1. Stets ist $\operatorname{Nil}(A) \subseteq \operatorname{Rad}(A)$. Ist $(A, \mathfrak{m})$ ein lokaler Ring (damit ist gemeint, A ist ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$), so ist $\operatorname{Rad}(A)$ das maximale Ideal von A. Ist A eine endlich erzeugte k-Algebra (k ein Körper), so ist $\operatorname{Rad}(A) = \operatorname{Nil}(A)$. Das folgt aus dem Hilbertschen Nullstellensatz, siehe Aufgabe 19.

2. Es ist $\operatorname{Rad}(A) = \{a \in A \colon 1 + Aa \subseteq A^*\}$.

1.6 Satz. (Nakayama-Lemma) *Sei A ein Ring, I ein Ideal von A und M ein endlich erzeugter A-Modul mit $IM = M$. Dann gibt es ein $a \in I$ mit $(1-a)M = 0$. Ist $I \subseteq \mathrm{Rad}(A)$, so folgt $M = 0$.*

Beweis. Sei $M = Ax_1 + \cdots + Ax_r$. Es gibt eine $r \times r$-Matrix $S = (s_{ij})$ mit Koeffizienten $s_{ij} \in I$ und mit $x_j = \sum_{i=1}^{r} s_{ij}x_i$ $(j = 1, \ldots, r)$. Sei $p_S(t) = t^r + a_1t^{r-1} + \cdots + a_r$ das charakteristische Polynom von S. Es ist $a_i \in I$ für $i = 1, \ldots, r$, und nach Cayley-Hamilton ist $(1 + a_1 + \cdots + a_r)M = 0$. Ist $I \subseteq \mathrm{Rad}(A)$, so ist $1 + I \subseteq A^*$. □

Die wichtigsten Anwendungen des Nakayama-Lemmas beziehen sich auf lokale Ringe.

1.7 Korollar. *Sei $(A, \mathfrak{m})$ ein lokaler Ring und M ein endlich erzeugter A-Modul. Ist $\mathfrak{m}M = M$, so ist $M = 0$.* □

1.8 Satz. *Sei $(A, \mathfrak{m})$ ein lokaler Ring, und sei M ein endlich erzeugter A-Modul. Sei $\kappa = A/\mathfrak{m}$ und $\overline{M} = M \otimes_A \kappa = M/\mathfrak{m}M$, ein endlich-dimensionaler κ-Vektorraum. Für $x_1, \ldots, x_n \in M$ gilt:*

$$x_1, \ldots, x_n \text{ erzeugen } M \text{ (über } A) \;\Leftrightarrow\; \overline{x}_1, \ldots, \overline{x}_n \text{ erzeugen } \overline{M} \text{ (über } \kappa).$$

Aufgrund dieses Satzes versteht man die Erzeugendensysteme von endlich erzeugten Moduln über lokalen Ringen völlig.

1.9 Definition. Sei A ein Ring. Für jeden A-Modul M sei $\mu(M) = \mu_A(M)$ die minimale Erzeugerzahl von M.

Aus Satz 1.8 folgt sofort:

1.10 Korollar. *Ist $(A, \mathfrak{m}, \kappa)$ ein lokaler Ring und M ein endlich erzeugter A-Modul, so ist $\mu_A(M) = \dim_\kappa(M \otimes_A \kappa)$. Jedes nicht verkürzbare Erzeugendensystem von M hat diese Mächtigkeit.* □

1.12 Definition. Sei A ein Ring.

(a) Für $\mathfrak{p} \in \mathrm{Spec}(A)$ heißt $\mathrm{ht}(\mathfrak{p}) := \dim(A_\mathfrak{p})$ die *Höhe* von $\mathfrak{p}$ (in A).

(b) Ist $I \neq (1)$ ein beliebiges Ideal von A, so heißt

$$\mathrm{ht}(I) \;:=\; \min\big\{\mathrm{ht}(\mathfrak{p})\colon \mathfrak{p} \in \mathrm{Spec}(A),\ \mathfrak{p} \supseteq I\big\}$$

die *Höhe* von I.

1.13 Beispiele.

1. Für $\mathfrak{p} \in \mathrm{Spec}(A)$ ist $\mathrm{ht}(\mathfrak{p})$ das Supremum aller Längen von Primidealketten $\mathfrak{p}_0 \subsetneq \mathfrak{p}_1 \subsetneq \cdots \subsetneq \mathfrak{p}_n = \mathfrak{p}$ in A, die mit $\mathfrak{p}$ enden.

2. Jedes Primideal von A ist in einem maximalen Ideal enthalten. Daher ist $\dim(A) = \sup_{\mathfrak{m} \in \mathrm{Max}\, A} \mathrm{ht}(\mathfrak{m})$.

3. Sei A ein faktorieller Ring. Für alle $0 \neq f \in A$, $f \notin A^*$ ist $\mathrm{ht}(Af) = 1$.

Der Krullsche Hauptidealsatz verallgemeinert diese Aussage auf beliebige noethersche Ringe:

1.14 Theorem. ((Verallgemeinerter) Krullscher Hauptidealsatz) *Sei A ein noetherscher Ring, seien $a_1, \ldots, a_n \in A$ und $I = (a_1, \ldots, a_n)$. Für jeden minimalen Primteiler $\mathfrak{p}$ von I ist $\mathrm{ht}(\mathfrak{p}) \leq n$. Insbesondere ist $\mathrm{ht}(I) \leq \mu(I)$.*

Aus Zeitmangel leider kein Beweis.

1.15 Korollar. *Jeder lokale noethersche Ring hat endliche Dimension.*

BEWEIS. Es ist $\dim(A) = \mathrm{ht}(\mathfrak{m}) \leq \mu(\mathfrak{m})$ $(< \infty)$ nach Theorem 1.14. □

2. Reguläre lokale Ringe

2.1 Definition. Sei A ein Ring und $\mathfrak{m}$ ein maximales Ideal von A. Ein Ideal I von A heißt $\mathfrak{m}$-*primär*, wenn $\sqrt{I} = \mathfrak{m}$ ist.

2.2 Bemerkungen.

1. Jedes Ideal $I \neq (1)$ mit $\mathfrak{m}^n \subseteq I$ für ein $n \geq 1$ ist $\mathfrak{m}$-primär. Ist A noethersch, so gilt auch die Umkehrung.

2. Für jedes $\mathfrak{m}$-primäre Ideal I von A hat man einen natürlichen Isomorphismus $A/I \cong A_{\mathfrak{m}}/IA_{\mathfrak{m}}$ (Aufgabe 18).

Aus dem verallgemeinerten Krullschen Hauptidealsatz ergibt sich die folgende Charakterisierung der Dimension von lokalen noetherschen Ringen:

2.3 Theorem. *Sei $(A, \mathfrak{m})$ ein lokaler noetherscher Ring. Dann ist*

$$\dim(A) \;=\; \min\big\{\mu(I)\colon I \text{ ist ein } \mathfrak{m}\text{-primäres Ideal von } A\big\}.$$

Anders gesagt: $\dim(A)$ ist das minimale $d \geq 0$, so daß $a_1, \ldots, a_d \in \mathfrak{m}$ existieren mit $\mathfrak{m} = \sqrt{(a_1, \ldots, a_d)}$.

BEWEIS. Sei $\dim(A) = d$. Für jedes $\mathfrak{m}$-primäre Ideal I ist $\mathfrak{m}$ ein minimaler Primteiler von I. Also ist $d = \mathrm{ht}(\mathfrak{m}) \leq \mu(I)$ nach Krull 1.14. Umgekehrt zeigen wir $d \geq \min_I \mu(I)$ durch Induktion nach d. Für $d = 0$ ist es klar, denn (0) ist ein $\mathfrak{m}$-primäres Ideal. Sei $d \geq 1$, sei $\mathrm{Min}(A) = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$. Nach Lemma 1.1 gibt es ein $a_1 \in \mathfrak{m}$ mit $a_1 \notin \mathfrak{p}_1 \cup \cdots \cup \mathfrak{p}_r$. Es folgt $\dim\big(A/(a_1)\big) \leq d - 1$. Nach Induktionsvoraussetzung für $A/(a_1)$ gibt es $d - 1$ Elemente $a_2, \ldots, a_d \in \mathfrak{m}$ mit $\sqrt{(a_1, a_2, \ldots, a_d)} = \mathfrak{m}$. □

2.4 Definition. Sei $(A, \mathfrak{m})$ ein d-dimensionaler lokaler noetherscher Ring. Eine *Parameterfolge* von A ist eine Folge $a_1, \ldots, a_d \in \mathfrak{m}$ von d Elementen mit $\sqrt{(a_1, \ldots, a_d)} = \mathfrak{m}$.

Nach Theorem 2.3 hat jeder lokale noethersche Ring eine Parameterfolge.

2.5 Korollar. *Ist A ein beliebiger noetherscher Ring und $\mathfrak{p} \in \mathrm{Spec}(A)$ mit $\mathrm{ht}(\mathfrak{p}) = r$, so gibt es r Elemente $a_1, \ldots, a_r \in \mathfrak{p}$, so daß $\mathfrak{p}$ ein minimaler Primteiler von $(a_1, \ldots, a_r)$ ist.*

BEWEIS. Aus Theorem 2.3, angewandt auf $A_{\mathfrak{p}}$, erhalten wir eine Parameterfolge $\frac{a_1}{s_1}, \ldots, \frac{a_r}{s_r}$ von $A_{\mathfrak{p}}$. Damit haben $a_1, \ldots, a_r$ die gewünschte Eigenschaft. □

2.6 Satz. *Sei $(A, \mathfrak{m})$ ein lokaler noetherscher Ring und sei $a_1, \ldots, a_d$ eine Parameterfolge von A. Dann ist $\dim A/(a_1, \ldots, a_i) = d - i$ für $i = 1, \ldots, d$.*

BEWEIS. Sei $\overline{A} = A/(a_1, \ldots, a_i)$, $e = \dim(\overline{A})$, und sei $\overline{b}_1, \ldots, \overline{b}_e$ eine Parameterfolge von $\overline{A}$. Dann ist $(a_1, \ldots, a_i, b_1, \ldots, b_e)$ ein $\mathfrak{m}$-primäres Ideal in A. Nach 2.3 ist also $i + e \geq d$, also $e \geq d - i$. Umgekehrt erzeugen $\overline{a}_{i+1}, \ldots, \overline{a}_d$ ein $\overline{\mathfrak{m}}$-primäres Ideal in $\overline{A}$. Also ist $e \leq d - i$, wieder nach 2.3. □

2.7 Definition. Sei $(A, \mathfrak{m})$ ein lokaler noetherscher Ring, $\kappa = A/\mathfrak{m}$. Die *Einbettungsdimension* von A ist

$$\operatorname{edim}(A) := \mu_A(\mathfrak{m}) = \dim_\kappa(\mathfrak{m}/\mathfrak{m}^2).$$

Die Gleichheit folgt aus dem Nakayama-Lemma (Korollar 1.10).

Aus Theorem 2.3 folgt sofort:

2.8 Korollar. *Für jeden lokalen noetherschen Ring A ist* $\operatorname{edim}(A) \geq \dim(A)$. □

2.9 Definition. Ein lokaler noetherscher Ring A heißt *regulär*, wenn $\operatorname{edim}(A) = \dim(A)$ ist. Ist A regulär mit $d = \dim(A)$, so heißt jedes Erzeugendensystem $a_1, \ldots, a_d$ der Länge d von $\mathfrak{m}$ eine *reguläre Parameterfolge* von A.

2.10 Bemerkungen.

1. Jede reguläre Parameterfolge von A ist auch eine Parameterfolge von A.

2. Sei A ein lokaler noetherscher Ring, sei $d = \dim(A)$. Genau dann ist A regulär, wenn $\dim_\kappa(\mathfrak{m}/\mathfrak{m}^2) = d$ ist. Alsdann ist $a_1, \ldots, a_d$ genau dann eine reguläre Parameterfolge von A, wenn $\overline{a}_1, \ldots, \overline{a}_d$ eine κ-Basis von $\mathfrak{m}/\mathfrak{m}^2$ ist. (Nakayama Lemma, Korollar 1.8.)

2.11 Satz. *Sei $(A, \mathfrak{m})$ ein regulärer lokaler Ring,* $\dim(A) = d$*, seien $a_1, \ldots, a_r \in \mathfrak{m}$. Es sind äquivalent:*

(i) *$a_1, \ldots, a_r$ kann zu einer regulären Parameterfolge ergänzt werden;*
(ii) *$\overline{a}_1, \ldots, \overline{a}_r \in \mathfrak{m}/\mathfrak{m}^2$ sind linear unabhängig über κ;*
(iii) *der lokale Ring $A/(a_1, \ldots, a_r)$ ist regulär und hat Dimension $d - r$.*

Beweis. Sei $\overline{A} = A/(a_1, \ldots, a_r)$. Die Äquivalenz (i) $\Leftrightarrow$ (ii) ist klar nach Bemerkung 2.10.2.

(i) $\Rightarrow$ (iii): Sei $a_1, \ldots, a_r, \ldots, a_d$ eine reguläre Parameterfolge von A. Nach Satz 2.6 ist $\dim(\overline{A}) = d - r$. Das maximale Ideal von $\overline{A}$ wird von $\overline{a}_{r+1}, \ldots, \overline{a}_d$ erzeugt. Also ist $\overline{A}$ regulär (und $\overline{a}_{r+1}, \ldots, \overline{a}_d$ ist eine reguläre Parameterfolge von $\overline{A}$).

(iii) $\Rightarrow$ (i): Sei $\overline{b}_1, \ldots, \overline{b}_{d-r}$ eine reguläre Parameterfolge von $\overline{A}$. Dann ist

$$a_1, \ldots, a_r, b_1, \ldots, b_{d-r}$$

eine reguläre Parameterfolge von A. □

2.12 Satz. *Jeder reguläre lokale Ring ist nullteilerfrei.*

Beweis. Induktion nach $d = \dim(A)$. Für $d = 0$ ist A ein Körper. $d = 1$: Sei $\mathfrak{m} = (x)$, sei $\mathfrak{p} \neq \mathfrak{m}$ ein Primideal. Für $a \in \mathfrak{p}$ gibt es $b \in A$ mit $a = bx$, und $b \in \mathfrak{p}$ wegen $x \notin \mathfrak{p}$. Also ist $\mathfrak{p} = x\mathfrak{p}$, also $\mathfrak{p} = (0)$ nach Nakayama.

Sei $d > 1$. Für jedes $x \in \mathfrak{m} \setminus \mathfrak{m}^2$ ist $A/(x)$ ein regulärer lokaler Ring mit $\dim A/(x) = d - 1$ (Korollar 2.11). Nach Induktionsvoraussetzung ist also (x) ein Primideal von A. Nach Lemma 1.1 (angewandt auf $\mathfrak{m}^2$ und die minimalen Primideale von A) gibt es $x \in \mathfrak{m} \setminus \mathfrak{m}^2$, welches in keinem minimalen Primideal von A liegt. Also gibt es ein (minimales) Primideal $\mathfrak{p} \subseteq (x)$ mit $\mathfrak{p} \neq (x)$. Wie im Fall $d = 1$ folgt $\mathfrak{p} = x\mathfrak{p}$, und daraus $\mathfrak{p} = (0)$, also die Nullteilerfreiheit von A. □

2.13 Satz. *Die regulären lokalen Ringe von Dimension* 0 *(bzw. von Dimension* 1*) sind genau die Körper (bzw. genau die diskreten Bewertungsringe).*

BEWEIS. Für $\dim = 0$ ist die Aussage klar. Jeder diskrete Bewertungsring ist ein eindimensionaler regulärer lokaler Ring, klar. Umgekehrt sei A regulär lokal mit $\dim(A) = 1$. Dann ist A integer (2.12), und $\mathfrak{m} = (t)$ ist ein Hauptideal. Sei $0 \neq a \in \mathfrak{m}$. Wegen $\sqrt{(a)} = \mathfrak{m}$ gibt es ein minimales $n \geq 1$ mit $a \mid t^n$, etwa $t^n = ab$. Dabei ist $b \notin (t) = \mathfrak{m}$ wegen n minimal, also ist $b \in A^*$. Also hat jedes Element $a \neq 0$ in A die Form $a = ut^n$ mit $u \in A^*$ und $n \geq 0$, d.h. A ist ein diskreter Bewertungsring. □

2.14 Bemerkungen. Man kann zeigen:

1. Jeder reguläre lokale Ring ist faktoriell.

2. Für jeden regulären lokalen Ring A und jedes Primideal $\mathfrak{p}$ von A ist auch der lokale Ring $A_\mathfrak{p}$ regulär.

Hier eine wichtige Folgerung für das reelle Spektrum von regulären lokalen Ringen.

2.15 Satz. *Sei $(A, \mathfrak{m})$ ein regulärer lokaler Ring, sei $\dim(A) = d$. Zu jedem $\alpha \in \mathrm{Sper}(A)$ mit $\mathrm{supp}(\alpha) = \mathfrak{m}$ gibt es eine Spezialisierungskette $\alpha_0 \rightsquigarrow \alpha_1 \rightsquigarrow \cdots \rightsquigarrow \alpha_d = \alpha$ der Länge d (mit $\alpha_{i-1} \neq \alpha_i$ für alle i) in $\mathrm{Sper}(A)$ mit $\alpha_d = \alpha$.*

BEWEIS. Induktion nach d. Für $d = 0$ ist nichts zu zeigen. Sei $d \geq 1$, sei $x \in \mathfrak{m} \setminus \mathfrak{m}^2$. Der lokale Ring A/Ax ist regulär mit $\dim(A/Ax) = d - 1$ (2.11), und $\mathfrak{p} = Ax$ ist ein Primideal von A. Der lokale Ring $A_\mathfrak{p}$ ist integer, kein Körper, und sein maximales Ideal ist ein Hauptideal. Also ist $A_\mathfrak{p}$ ein diskreter Bewertungsring nach Satz 2.13. Nach Induktion, angewandt auf $A/\mathfrak{p}$, gibt es eine Kette $\alpha_1 \rightsquigarrow \cdots \rightsquigarrow \alpha_d = \alpha$ in $\mathrm{Sper}(A)$ der Länge $d-1$ mit $\mathrm{supp}(\alpha_1) = \mathfrak{p}$. Nach Baer-Krull, angewandt auf $A_\mathfrak{p}$ und α_1, hat α_1 eine Generalisierung α_0 in $\mathrm{Sper}(A)$ mit $\mathrm{supp}(\alpha_0 = (0)$. □

2.16 Beispiel. In Aufgabe 26 (WS) wurde eine solche Kette für den lokalen Ring $A = \mathbb{R}[x_1, \ldots, x_d]_{(x_1,\ldots,x_d)}$ (regulär von Dimension d, siehe 3.8 unten) explizit konstruiert, zum Beispiel so: Ordne $\mathrm{Quot}(A) = R(x_1, \ldots, x_d)$ an gemäß

$$0 < x_1 \ll x_2 \ll \cdots \ll x_n \ll 1.$$

Das gibt den Positivkegel P von A mit $\mathrm{supp}(P) = (0)$. Jetzt hat man die Spezialisierungskette von Positivkegeln

$$P \subsetneq P + (x_1) \subsetneq P + (x_1, x_2) \subsetneq \cdots \subsetneq P + (x_1, \ldots, x_n)$$

in A, und der Träger von $P + (x_1, \ldots, x_k)$ ist $(x_1, \ldots, x_k)$.

3. Reguläre und singuläre Punkte von Varietäten

3.1 Definition. Sei k ein Körper, sei X eine (quasiprojektive) k-Varietät mit Garbe $U \mapsto \mathcal{O}_X(U)$ der regulären Funktionen (d.h., für offenes $U \subseteq X$ ist $\mathcal{O}_X(U)$ der Ring der regulären Funktionen auf U). Sei $\xi \in X(k)$ ein k-rationaler Punkt. Der *lokale Ring* von X in ξ ist der Ring

$$\mathcal{O}_{X,\xi} := \varinjlim_{U} \mathcal{O}_X(U),$$

induktiver Limes über die Zariski-offenen Umgebungen U von ξ in X. Die Übergangsabbildungen sind dabei die Restriktionsabbildungen.

Das bedeutet: Die Elemente von $\mathcal{O}_{X,\xi}$ sind Äquivalenzklassen von Paaren (U, f) mit $U \subseteq X$ offene Umgebung von ξ und $f \in \mathcal{O}_X(U)$, mit $(U, f) \sim (U', f')$ falls es eine Umgebung $U'' \subseteq U \cap U'$ von ξ gibt mit $f|_{U''} = f'|_{U''}$. Die Ringstruktur auf $\mathcal{O}_{X,\xi}$ ist durch die Ringstruktur auf den $\mathcal{O}_X(U)$ induziert.

3.2 Bemerkungen.

1. Nach Definition gilt $\mathcal{O}_{X,\xi} = \mathcal{O}_{U,\xi}$ für jede offene Umgebung U von ξ. Für das Studium von $\mathcal{O}_{X,\xi}$ kann man also X durch jede offene affine Umgebung von ξ ersetzen. Ist X affin, so ist $\mathcal{O}_{X,\xi} = k[X]_{\mathfrak{m}_\xi}$, wobei $\mathfrak{m}_\xi = \mathcal{I}(\{x\})$ das maximale Ideal von $k[X]$ zum Punkt $\xi \in X(k)$ ist. Denn jede offene Umgebung von ξ in X enthält eine Menge der Form $D_X(s)$ mit $s \in k[X] \setminus \mathfrak{m}_\xi$. Insbesondere ist $\mathcal{O}_{X,\xi}$ stets ein lokaler noetherscher Ring. Das maximale Ideal von $\mathcal{O}_{X,\xi}$ bezeichnen wir bei Bedarf mit $\mathfrak{m}_{X,\xi}$.

2. Sei $\xi \in X(k)$. Die Primideale von $\mathcal{O}_{X,\xi}$ sind in Bijektion zu den abgeschlossenen irreduziblen Untervarietäten $Z \subseteq X$ mit $\xi \in Z$. Insbesondere korrespondieren die minimalen Primideale von $\mathcal{O}_{X,\xi}$ genau zu den irreduziblen Komponenten X' von X mit $\xi \in X'$. Genau dann ist also $\mathcal{O}_{X,\xi}$ ein integrer Ring, wenn ξ nur auf einer einzigen irreduziblen Komponente von X liegt.

3.3 Sei $\xi \in X$ ein Punkt. Die *lokale Dimension* von X in ξ ist

$$\dim_\xi(X) := \min_U \dim(U),$$

Minimum über alle (in der k-Zariskitopologie) offenen Umgebungen U von ξ. Sind $X_1, \ldots, X_r$ die durch ξ gehenden irreduziblen Komponenten von X, so ist $\dim_\xi(X) = \max_{i=1,\ldots,r} \dim(X_i)$.

Die algebraische Dimension der lokalen Ringe ist gleich der (lokalen) geometrischen Dimension:

3.4 Satz. *Für $\xi \in X(k)$ ist $\dim(\mathcal{O}_{X,\xi}) = \dim_\xi(X)$.*

Für den Beweis braucht man einen anderen wichtigen Satz:

3.5 Satz. (Going-down) *Sei $A \subseteq B$ eine ganze Erweiterung integrer Ringe, und sei A ganz abgeschlossen. Dann gilt Going-down: Zu jedem $\mathfrak{q}' \in \operatorname{Spec}(B)$ und jedem $\mathfrak{p} \in \operatorname{Spec}(A)$ mit $\mathfrak{p} \subseteq \mathfrak{q}'$ gibt es ein $\mathfrak{q} \in \operatorname{Spec}(B)$ mit $\mathfrak{q} \subseteq \mathfrak{q}'$ und $\mathfrak{p} = \mathfrak{q} \cap A$.*

Beweis. Sei $S := A \setminus \mathfrak{p}$ und $T := B \setminus \mathfrak{q}'$. Dann sind S, T und ST multiplikative Teilmengen von B. Wir zeigen $\mathfrak{p}B \cap ST = \varnothing$. Dann folgt, daß es ein $\mathfrak{q} \in \operatorname{Spec}(B)$ gibt mit $\mathfrak{p}B \subseteq \mathfrak{q}$ und $\mathfrak{q} \cap ST = \varnothing$. Also ist $\mathfrak{q} \cap A = \mathfrak{p}$ und $\mathfrak{q} \subseteq \mathfrak{q}'$.

Angenommen $y \in \mathfrak{p}B \cap ST$, etwa $y = st$ mit $s \in S$, $t \in T$. Sei $K = \operatorname{Quot}(A)$, sei $f := \operatorname{MinPol}(y/K) = x^n + a_1 x^{n-1} + \cdots + a_n$. Die Koeffizienten a_i von f liegen in A, wegen y ganz über A (siehe meine Vorlesung B4, Satz ...). Behaupte, es gilt sogar $a_i \in \mathfrak{p}$ $(i = 1, \ldots, n)$. Sei C der ganze Abschluß von A in $\overline{K}$. Es gilt also $B \subseteq C$ und $y \in \mathfrak{p}C$. Da $\mathfrak{p}C$ unter $\operatorname{Aut}(\overline{K}/K)$ invariant ist und diese Gruppe transitiv auf den Nullstellen von f operiert, liegen alle Nullstellen in $\mathfrak{p}C$, und somit ist $a_i \in \mathfrak{p}C \cap A$ für alle i (die a_i sind die symmetrischen Polynome in den Nullstellen). Da $A \subseteq C$ eine ganze Erweiterung integrer Ringe ist, gibt Going-up ein Primideal $\mathfrak{P} \in \operatorname{Spec}(C)$ mit $\mathfrak{P} \cap A = \mathfrak{p}$. Wegen $\mathfrak{p}C \subseteq \mathfrak{P}$ folgt also $\mathfrak{p}C \cap A = \mathfrak{p}$.

Division durch s^n zeigt, daß das Minimalpolynom von $t = \frac{y}{s}$ über K gleich

$$x^n + \frac{a_1}{s}\, x^{n-1} + \cdots + \frac{a_n}{s^n}$$

ist. Für die Koeffizienten $c_i := \frac{a_i}{s^i}$ gilt $c_i \in A$, aus demselben Grund wie oben. Wegen $s^i c_i = a_i \in \mathfrak{p}$ und $s \notin \mathfrak{p}$ folgt sogar $c_i \in \mathfrak{p}$ $(i = 1, \ldots, n)$. Also ist $t^n \in \mathfrak{p}B \subseteq \mathfrak{q}'$, Widerspruch zu $t \in T$. □

3.6 Beweis von Satz 3.4: Wir können annehmen, daß X affin und $\dim_\xi(X) = \dim(X) = d$ ist. Wegen $\mathcal{O}_{X,\xi} = k[X]_{\mathfrak{m}_\xi}$ ist $\dim(\mathcal{O}_{X,\xi}) \leq d$ klar. Für die Umkehrung

können wir X irreduzibel annehmen. Sei $X \to \mathbb{A}^d$ eine Noether Normalisierung, entsprechend einer endlichen Ringerweiterung $k[\mathtt{x}] = k[x_1, \ldots, x_d] \subseteq k[X]$. Wir können annehmen $\mathfrak{m}_\xi \cap k[\mathtt{x}] = (x_1, \ldots, x_d)$. Wähle eine Primidealkette der Länge d in $k[\mathtt{x}]$, die in $(x_1, \ldots, x_d)$ endet, z.B. $(0) \subseteq (x_1) \subseteq \cdots \subseteq (x_1, \ldots, x_d)$. Schrittweises Anwenden von Going-down 3.5 gibt eine Primidealkette der Länge d in $k[X]_{\mathfrak{m}_\xi}$. Also ist $\dim(\mathcal{O}_{X,\xi}) \geq d$.

Wir definieren das Konzept von regulären bzw. singulären Punkten nur für k-rationale Punkte:

3.7 Definition. $\xi \in X(k)$ heißt ein *regulärer* (oder *nichtsingulärer*) Punkt von X, wenn der lokale Ring $\mathcal{O}_{X,\xi}$ regulär ist. Andernfalls heißt ξ ein *singulärer* Punkt von X.

3.8 Beispiele.

1. Für $X = \mathbb{A}^n$ oder $\mathbb{P}^n$ ist jeder Punkt $\xi \in X(k)$ regulär. Denn nach einer Translation kann man annehmen $\xi = (0, \ldots, 0) \in \mathbb{A}^n$. Dann ist $\mathcal{O}_{\mathbb{A}^n,\xi} = A_{\mathfrak{m}}$ mit $A = k[x_1, \ldots, x_n]$ und $\mathfrak{m} = (x_1, \ldots, x_n)$. Es ist $\dim(A_{\mathfrak{m}}) = n$ nach Satz 3.4, und es ist $\mathfrak{m}A_{\mathfrak{m}}/\mathfrak{m}^2A_{\mathfrak{m}} \cong \mathfrak{m}/\mathfrak{m}^2 = kx_1 \oplus \cdots \oplus kx_n$ (Aufgabe 17), also ist $\operatorname{edim}(A_m) = n$. Der kanonische Isomorphismus $\mathfrak{m}/\mathfrak{m}^2 \xrightarrow{\sim} \bigoplus_{i=1}^n kx_i$ bildet $f = \sum_{i=1}^n c_i x_i + \sum_{|\alpha|\geq 2} c_\alpha \mathtt{x}^\alpha$ aus $\mathfrak{m}$ ab auf

$$\sum_{i=1}^n c_i x_i \;=\; \sum_{i=1}^n \frac{\partial f}{\partial x_i}(\xi)\, x_i.$$

2. Sei $\xi = (0, \ldots, 0)$ und $\mathfrak{m} = (x_1, \ldots, x_n)$ wie eben, sei $0 \neq f \in \mathfrak{m}$. Für die Hyperfläche $X = \mathcal{V}(f) \subseteq \mathbb{A}^n$ gilt dann $\dim(\mathcal{O}_{X,\xi}) = \dim(X) = n - 1$. Ist $f \notin \mathfrak{m}^2$, so ist $\operatorname{edim}(\mathcal{O}_{X,\xi}) = n - 1$, für $f \in \mathfrak{m}^2$ ist dagegen $\operatorname{edim}(\mathcal{O}_{X,\xi}) = n$. Also ist ξ genau dann ein regulärer Punkt der Hyperfläche X, wenn $\nabla f(\xi) \neq 0$ ist.

Wir zeigen jetzt, daß die nichtsingulären Punkte einer Varietät "eine Zariski-offene Teilmenge bilden".

3.9 Theorem. (Jacobi-Kriterium) *Sei $X \subseteq \mathbb{A}^n$ eine abgeschlossene k-Varietät mit Verschwindungsideal $\mathcal{I}(X) = (f_1, \ldots, f_r)$. Sei $\xi \in X(k)$. Genau dann ist ξ ein nichtsingulärer Punkt von X, wenn für die Jacobimatrix*

$$J \;=\; \Big(\partial f_i/\partial x_j\Big)_{1\leq i\leq r,\ 1\leq j\leq n}$$

gilt $\operatorname{rk} J(\xi) \geq n - \dim_\xi(X)$.

Hier ist $J(\xi)$ also eine $r \times n$-Matrix mit Koeffizienten in k. Die Ungleichung $\operatorname{rk} J(\xi) \leq n - \dim_\xi(X)$ gilt immer.

Beweis. Sei $d = \dim_\xi(X)$, sei $\xi = 0 \in X(k) \subseteq k^n$, und sei $A := k[\mathtt{x}]_{(\mathtt{x})}$ mit maximalem Ideal $\mathfrak{m} = (x_1, \ldots, x_n)$. Es ist also $\mathcal{O}_{X,\xi} = A/(f_1, \ldots, f_r)$, und dieser lokale Ring hat Dimension d nach Satz 3.4. Der k-Vektorraum $\mathfrak{m}_{X,\xi}/\mathfrak{m}_{X,\xi}^2$ ist der Quotient von $\mathfrak{m}/\mathfrak{m}^2$ nach dem linearen Erzeugnis der $f_i + \mathfrak{m}^2$ $(i = 1, \ldots, r)$. Unter dem natürlichen Isomorphismus $\mathfrak{m}/\mathfrak{m}^2 \cong k^n$ (3.8.1) ist also

$$\mathfrak{m}_{X,\xi}/\mathfrak{m}_{X,\xi}^2 \;=\; k^n/\operatorname{span}(\nabla f_1(\xi),\, \ldots,\, \nabla f_r(\xi)).$$

Also ist $\operatorname{edim}(\mathcal{O}_{X,\xi}) = n - \operatorname{rk} J(\xi)$. Das zeigt, daß stets $n - \operatorname{rk} J(\xi) \geq d$ stets gilt, mit Gleichheit genau dann, wenn ξ ein regulärer Punkt von X ist. □

Daraus folgt, daß die regulären Punkte von X "eine Zariski-offene Teilmenge von X bilden". Genauer:

3.10 Theorem. *Sei* $\mathrm{char}(k) = 0$*, sei* X *eine beliebige (quasiprojektive)* k*-Varietät. Es gibt eine eindeutig bestimmte offene Zariski-dichte Teilmenge* $X_{\mathrm{reg}} \subseteq X$ *derart, daß für jede Körpererweiterung* K/k *und jeden Punkt* $\xi \in X(K)$ *gilt: Genau dann ist* ξ *ein regulärer Punkt von* X_K*, wenn* $\xi \in X_{\mathrm{reg}}(K)$ *ist.*

Die Voraussetzung $\mathrm{char}(k) = 0$ kann nicht gestrichen werden (k vollkommener Körper würde genügen).

Beweis. (Skizze) Wir können $X \subseteq \mathbb{A}^n$ affin annehmen. Sind $X_1, \ldots, X_r$ die irreduziblen Komponenten von X, so sind Punkte in $\bigcup_{i<j} X_i \cap X_j$ stets singulär, da ein regulärer lokaler Ring integer ist (siehe 3.2.2, 2.12). Wir können also X irreduzibel annehmen. Dann wird X_{reg} durch die Rangbedingung im Jacobi-Kriterium beschrieben, und das ist eine offene Bedingung an ξ (Nichtverschwinden eines Minors). Man muß aber noch zeigen, daß für K/k das Ideal von X_K in $K[\mathtt{x}]$ von den f_i erzeugt wird. Für $\mathrm{char}(k) = 0$ ist das richtig, für $\mathrm{char}(k) = p > 0$ nicht unbedingt. Weiter bleibt zu zeigen, daß $X_{\overline{k}}$ mindestens einen regulären Punkt hat. □

3.11 Sei X eine k-Varietät. Man setzt $X_{\mathrm{sing}} = X \smallsetminus X_{\mathrm{reg}}$, eine abgeschlossene Teilmenge von X, und nennt X_{reg} (bzw. X_{sing}) den *regulären* (bzw. *singulären*) *Ort* von X. Die Varietät X heißt *nichtsingulär*, wenn $X_{\mathrm{reg}} = X$ ist, andernfalls *singulär*.

Genau dann ist also die Varietät X nichtsingulär, wenn für alle $\xi \in X(\overline{k})$ der lokale Ring von $X_{\overline{k}}$ in ξ regulär ist. Für X affin kann man zeigen, daß dies äquivalent dazu ist, daß für jedes maximale Ideal $\mathfrak{m}$ von $k[X]$ die Lokalisierung $k[X]_{\mathfrak{m}}$ ein regulärer lokaler Ring ist. Man muß also nicht erst nach $\overline{k}$ erweitern. (Eine analoge Bedingung gilt natürlich auch für X nicht affin.)

Besonders einfach ist die Bestimmung der Singularitäten einer Hyperfläche (Spezialfall von Theorem 3.9):

3.12 Korollar. *Sei* $0 \neq f \in k[\mathtt{x}]$ *ohne mehrfache Faktoren, betrachte die Hyperfläche* $X = \mathcal{V}(f)$ *in* $\mathbb{A}^n$*. Dann ist*

$$X_{\mathrm{sing}} \;=\; \mathcal{V}\Big(f,\, \frac{\partial f}{\partial x_1},\, \ldots,\, \frac{\partial f}{\partial x_n}\Big).$$

Genau dann ist X *nichtsingulär, wenn* $(f,\, \frac{\partial f}{\partial x_1},\, \ldots,\, \frac{\partial f}{\partial x_n}) = (1)$ *ist.*

Beweis. Kann annehmen $k = \overline{k}$. Für alle $\xi \in X(k)$ ist $\dim_\xi(X) = n - 1$. Also ξ singulär $\Leftrightarrow \frac{\partial f}{\partial x_i}(\xi) = 0$ für alle i. □

Sei R ein reell abgeschlossener Körper. Der folgende Satz ist eine wichtige Ergänzung zur semialgebraischen Geometrie:

3.13 Theorem. (Artin-Lang) *Sei* X *eine irreduzible* R*-Varietät, und sei* M *eine offene semialgebraische Teilmenge von* $X(R)$*. Genau dann ist* M *Zariski-dicht in* X*, wenn* M *einen nichtsingulären Punkt aus* $X(R)$ *enthält.*

Beweis. Wir können X affin annehmen. Sei M Zariski-dicht in X. Wäre $M \cap X_{\mathrm{reg}}(R) = \varnothing$, so wäre $M \subseteq X_{\mathrm{sing}}(R)$, also wäre der Zariskiabschluß von M enthalten in X_{sing}, Widerspruch zu M Zariski-dicht.

Sei $\xi \in M$ ein nichtsingulärer Punkt von X, dh der lokale Ring $\mathcal{O}_{X,\xi} = R[X]_{\mathfrak{m}_\xi}$ ist regulär. Nach Satz 2.15 gibt es $\alpha \in \operatorname{Sper} R[X]$ mit $\mathrm{supp}(\alpha) = (0)$ und $\alpha \rightsquigarrow \xi$. Wegen M offen in $X(R)$ ist auch $\widetilde{M}$ offen in $\operatorname{Sper} R[X]$ (Endlichkeitssatz III.2.3). Also ist $\alpha \in \widetilde{M}$. Für das Ideal $I \subseteq R[X]$ des Zariskiabschlusses von M gilt also $I \subseteq \mathrm{supp}(\alpha)$, und es folgt $I = (0)$. Also ist M Zariski-dicht in X. □

3.14 Beispiel. Ist X singulär, so kann es nichtleere offene Teilmengen M von $X(R)$ geben, die nicht Zariski-dicht in X sind, also (3.13) nur singuläre Punkte von X enthalten. Betrachte etwa die ebene affine Kurve $X = \mathcal{V}(x^2+y^2-x^3)$ und $M = \{(0,0)\}$, oder der "Whitney-Schirm" $X = \mathcal{V}(y^2z - x^2)$ und $M = \{(0,0,a)\colon a < 0\}$.

4. Komplettierung

4.1 Sei A ein Ring und M ein A-Modul. Eine *(absteigende) Filterierung* von M ist eine absteigende Kette

$$M = M_0 \supseteq M_1 \supseteq M_2 \supseteq \cdots$$

von Untermoduln. Die Filtrierung heißt *separiert*, wenn $\bigcap_{n\geq 0} M_n = \{0\}$ ist.

Sei $(M_n)_{n\geq 0}$ eine feste Filtrierung von M. Dann wird eine Topologie auf M dadurch definiert, daß man für jedes $x \in M$ die Familie der Mengen $x + M_n$ $(n \geq 0)$ als Umgebungsbasis von x definiert. Dies macht M zu einer topologischen abelschen Gruppe, d.h. die Abbildung $M \times M \to M$, $(x,y) \mapsto x - y$ ist stetig. Die Topologie ist genau dann Hausdorff, wenn die Filtrierung separiert ist.

Nach Definition der Topologie konvergiert eine Folge $(x_i)_{i\geq 1}$ genau dann gegen $x \in M$, wenn gilt:

$$\forall\, n \in \mathbb{N}\ \ \exists\, i_0 \in \mathbb{N}\ \ \forall\, i \geq i_0\ \ x_i - x \in M_n.$$

Die Folge heißt eine *Cauchyfolge*, wenn gilt:

$$\forall\, n \in \mathbb{N}\ \ \exists\, i_0 \in \mathbb{N}\ \ \forall\, i, j \geq i_0\ \ x_i - x_j \in M_n.$$

Der Modul M (mit der durch die Filtrierung gegebenen Topologie) heißt *vollständig*, wenn M separiert ist und jede Cauchyfolge in M einen (eindeutigen) Limes in M hat.

4.2 Fixiere eine Filtrierung $(M_n)_{n\geq 0}$ von M und betrachte die Folge

$$M/M_0 \xleftarrow{\varphi_1} M/M_1 \xleftarrow{\varphi_2} M/M_2 \xleftarrow{\varphi_3} \cdots$$

der kanonischen Epimorphismen. Der A-Modul

$$\widehat{M} := \varprojlim_n M/M_n = \Big\{(\xi_n) \in \prod_{n=0}^{\infty} M/M_n \colon \forall\, n \geq 1\ \varphi_n(\xi_n) = \xi_{n-1}\Big\}$$

(ein Untermodul des direkten Produktmoduls $\prod_{n\geq 0} M/M_n$) heißt die *Komplettierung* (oder *Vervollständigung*) des filtrierten Moduls M. Für jedes $n \geq 0$ ist die kanonische Abbildung $\pi_n \colon \widehat{M} \to M/M_n$ surjektiv. Sei $\widehat{M}_n := \ker(\pi_n)$ $(n \geq 0)$. Dann ist $\widehat{M} = \widehat{M}_0 \supseteq \widehat{M}_1 \supseteq \cdots$ eine Filtrierung von $\widehat{M}$ (die *kanonische Filtrierung*), und diese ist vollständig. Die kanonische Abbildung $i\colon M \to \widehat{M}$, $x \mapsto (x + M_n)_n$ hat $\ker(i) = \bigcap_n M_n$, und $i(M)$ ist dicht in $\widehat{M}$. Man sieht leicht: Genau dann ist M vollständig, wenn i ein Isomorphismus ist.

4.3 Satz. *(Universelle Eigenschaft) Seien M, N filtrierte A-Moduln, und sei $N = \widehat{N}$ vollständig. Sei $f\colon M \to N$ eine stetige (A-) lineare Abbildung. Dann gibt es genau eine stetige A-lineare Fortsetzung $\widehat{f}\colon \widehat{M} \to N$ von f, d.h. $f = \widehat{f} \circ i$.*

4.4 Sei $(M_n)_{n\geq 0}$ eine Filtrierung von M, und sei $L \subseteq M$ ein Untermodul. Die auf L induzierte Filtrierung ist definiert durch $L_n = L \cap M_n$ $(n \geq 0)$. Die auf M/L induzierte Filtrierung ist definiert durch $(M/L)_n = (M_n + L)/L$ $(n \geq 0)$.

4.5 Satz. *Sei M ein filtrierter A-Modul, sei L ein Untermodul von M, und seien L und M/L mit der induzierten Filtrierung versehen. Dann besteht eine kanonische exakte Sequenz*

$$0 \to \widehat{L} \to \widehat{M} \to \widehat{M/L} \to 0$$

von A-Moduln.

Beweis. Sei $N := M/L$. Für alle n ist die natürliche Sequenz

$$0 \to \frac{L}{L \cap M_n} \to \frac{M}{M_n} \to \frac{M}{M_n + L} \to 0$$

exakt, und identifiziert sich mit der Sequenz $0 \to L/L_n \to M/M_n \to N/N_n \to 0$. Daher ist $0 \to (L/L_n)_n \to (M/M_n)_n \to (N/N_n)_n \to 0$ eine exakte Sequenz von projektiven Systemen von A-Moduln, im offensichtlichen Sinn. Die Behauptung folgt deshalb aus dem nächsten Lemma. □

4.6 Lemma. *Ist $0 \to (U_n) \to (V_n) \to (W_n) \to 0$ eine exakte Sequenz projektiver Systeme von A-Moduln, so ist die Sequenz*

$$0 \to \varprojlim U_n \to \varprojlim V_n \to \varprojlim W_n$$

exakt. Ist dabei $U_n \to U_{n-1}$ surjektiv für alle $n \geq 1$, so ist sogar

$$0 \to \varprojlim U_n \to \varprojlim V_n \to \varprojlim W_n \to 0$$

exakt.

Beweis. Die Voraussetzung besagt ein kommutatives Diagramm

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U_0 & \longrightarrow & V_0 & \longrightarrow & W_0 & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \varphi_1} & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & U_1 & \longrightarrow & V_1 & \longrightarrow & W_1 & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \varphi_2} & & \uparrow & & \uparrow & & \\
0 & \longrightarrow & U_2 & \longrightarrow & V_2 & \longrightarrow & W_2 & \longrightarrow & 0 \\
 & & \uparrow{\scriptstyle \varphi_3} & & \uparrow & & \uparrow & &
\end{array}$$

mit exakten Zeilen. Sei $U = \prod_{n \geq 0} U_n$, und sei $d_U \colon U \to U$ die durch

$$d_U(u_0, u_1, \dots) := \big(u_0 - \varphi_1(u_1),\, u_1 - \varphi_2(u_2),\, \dots\big)$$

definierte A-lineare Abbildung. Es ist $\ker(d_U) = \varprojlim U_n$. Wir schreiben $\varprojlim{}^1 U_n := \operatorname{coker}(d_U)$, und verwenden analoge Bezeichnungen für die projektiven Systeme (V_n) und (W_n). Aus dem kommutativen Diagramm mit exakten Zeilen

$$\begin{array}{ccccccccc}
0 & \longrightarrow & U & \longrightarrow & V & \longrightarrow & W & \longrightarrow & 0 \\
 & & \downarrow{\scriptstyle d_U} & & \downarrow{\scriptstyle d_V} & & \downarrow{\scriptstyle d_W} & & \\
0 & \longrightarrow & U & \longrightarrow & V & \longrightarrow & W & \longrightarrow & 0
\end{array}$$

und dem Schlangenlemma (Aufgabe 20) folgt die exakte Sequenz

$$0 \to \varprojlim U_n \to \varprojlim V_n \to \varprojlim W_n \to \varprojlim{}^1 U_n \to \varprojlim{}^1 V_n \to \varprojlim{}^1 W_n \to 0.$$

Sind alle Übergangsabbildungen $\varphi_n \colon U_n \to U_{n-1}$ surjektiv, so ist $d_U \colon U \to U$ surjektiv, und somit $\varprojlim{}^1 U_n = 0$. Daraus folgen die Behauptungen. □

4.7 Fixiere jetzt ein Ideal $I \subseteq A$ und versehe A-Moduln M mit der *I-adischen Filtrierung* $M_n := I^n M$ $(n \geq 0)$. Die zugehörige Topologie auf M heißt die *I-adische Topologie*, und

$$\widehat{M} \;=\; \varprojlim M/I^n M$$

heißt die *I-adische Komplettierung* von M. Insbesondere ist $\widehat{A} = \varprojlim A/I^n$, die *$I$-adische Komplettierung* von A, ein topologischer Ring, und $\widehat{M}$ ist in kanonischer Weise ein topologischer $\widehat{A}$-Modul, via

$$(\overline{a}_n) \cdot (\overline{x}_n) \;:=\; (\overline{a_n x_n}).$$

Die Stetigkeit der Multiplikation $\widehat{A} \times \widehat{M} \to \widehat{M}$ folgt dabei aus $I^m \cdot I^n M \subseteq I^{m+n} M$. Jeder Homomorphismus $f\colon M \to N$ von A-Moduln induziert einen Homomorphismus $\widehat{f}\colon \widehat{M} \to \widehat{N}$ der I-adischen Komplettierungen.

4.8 Beispiele.

1. Ist $A = \mathbb{Z}$ und $I = p\mathbb{Z}$ für eine Primzahl p, so ist die $p\mathbb{Z}$-adische Komplettierung von $\mathbb{Z}$ gleich $\mathbb{Z}_p$, der Ring der ganzen p-adischen Zahlen.

2. Ist $A[\mathtt{x}] = A[x_1, \ldots, x_n]$ der Polynomring über A und $I = (x_1, \ldots, x_n)$ (Ideal in $A[\mathtt{x}]$), so ist die I-adische Komplettierung von $A[\mathtt{x}]$ der Ring $A[\![x_1, \ldots, x_n]\!]$ der formalen Potenzreihen in $x_1, \ldots, x_n$ über A.

3. Ist A ein lokaler Ring und $I = \mathfrak{m}$ das maximale Ideal, so bezeichnet man die $\mathfrak{m}$-adische Komplettierung von A meist einfach als die Komplettierung $\widehat{A}$ von A.

4.9 Der zum filtrierten A-Modul M *assoziierte graduierte A-Modul* ist definiert durch

$$\mathrm{Gr}(M) \;:=\; \bigoplus_{n \geq 0} \mathrm{Gr}_n(M), \quad \text{mit} \;\; \mathrm{Gr}_n(M) \;=\; M_n/M_{n+1} \quad (n \geq 0).$$

Sei $I \subseteq A$ ein fixiertes Ideal und M ein A-Modul. Wir versehen A und M mit ihrer I-adischen Filtrierung. Dann ist

$$\mathrm{Gr}^I(A) \;:=\; \bigoplus_{n \geq 0} I^n/I^{n+1}$$

(mit $I^0 := A$) ein graduierter Ring, und

$$\mathrm{Gr}^I(M) \;:=\; \bigoplus_{n \geq 0} I^n M/I^{n+1} M$$

ist ein graduierter Modul über $\mathrm{Gr}^I(A)$.

Ist $I = (a_1, \ldots, a_r)$, so wird $\mathrm{Gr}^I(A)$ als Algebra über $\mathrm{Gr}^I_0(A) = A/I$ erzeugt von den $a_i + I^2 \in \mathrm{Gr}^I_1(A)$ $(i = 1, \ldots, r)$. Ist also A noethersch, so ist also $\mathrm{Gr}^I(A)$ noethersch (Hilbert Basissatz). Wird der A-Modul M erzeugt von $x_1, \ldots, x_m$, so wird $\mathrm{Gr}^I(M)$ als $\mathrm{Gr}^I(A)$-Modul erzeugt von den $x_i + IM \in Gr^I_0(M) = M/IM$ $(i = 1, \ldots, m)$.

4.10 Sei $I \subseteq A$ ein Ideal. Eine Filtrierung (M_n) auf einem A-Modul M heißt eine *I-Filtrierung*, falls für alle $n \geq 0$ gilt $IM_n \subseteq M_{n+1}$. Sie heißt eine *stabile I-Filtrierung*, falls zusätzlich $IM_n = M_{n+1}$ für alle hinreichend großen n gilt.

4.11 Lemma. *Ist (M_n) eine stabile I-Filtrierung auf M, so gibt es einen Index $k \geq 0$ mit*

$$M_{n+k} \;\subseteq\; I^n M$$

für alle $n \geq 0$.

BEWEIS. Ist $IM_n = M_{n+1}$ für $n \geq k$, so folgt $M_{n+k} = I^n M_k \subseteq I^n M$ für $n \geq 0$. □

4.12 Korollar. *Je zwei stabile I-Filtrierungen (M_n) und (M'_n) auf M induzieren auf M dieselbe Topologie, und daher einen Isomorphismus der Komplettierungen.* □

4.13 Definition. Sei I ein Ideal in A. Der graduierte Ring $B_I(A) := \bigoplus_{n\geq 0} B_n$ mit $B_n := I^n$ $(n \geq 0)$ heißt der *Aufblasungsring* von A zum Ideal I.

Beachte, $B_I(A)$ ist kanonisch isomorph zum (graduierten) Teilring von $A[t]$, der von A und tI erzeugt wird:

$$B_I(A) \;=\; A \oplus tI \oplus t^2 I^2 \oplus \cdots$$

Es besteht also $B_I(A)$ aus allen Polynomen in $A[t]$, für die der Koeffizient von t^n in I^n liegt für jedes $n \geq 0$. Ist A noethersch, so ist auch $B_I(A)$ noethersch (Hilbert Basissatz).

4.14 Lemma. *Sei A noethersch, M ein endlich erzeugter A-Modul und $(M_n)_{n\geq 0}$ eine I-Filtrierung auf M. Sei $M^* := \bigoplus_{n\geq 0} M_n$, aufgefaßt als graduierter Modul über $A^* := B_I(A)$. Es sind äquivalent:*

(i) *Die I-Filtrierung (M_n) von M ist stabil;*
(ii) *M^* ist endlich erzeugt als A^*-Modul.*

BEWEIS. Für $i \geq 0$ sei

$$M^*(i) \;:=\; M_0 \oplus \cdots \oplus M_i \oplus IM_i \oplus I^2 M_i \oplus \cdots ,$$

der graduierte A^*-Untermodul von M^* mit $M^*(i)_n = M_n$ für $n \leq i$ und $M^*(i)_n = I^{n-i}M_i$ für $n \geq i$. Es gilt $M^*(0) \subseteq M^*(1) \subseteq \cdots \subseteq \bigcup_{i\geq 0} M^*(i) = M^*$, und jedes $M^*(i)$ ist endlich erzeugt als A^*-Modul. Denn der A^*-Modul $M^*(i)$ wird erzeugt von $M_0 \oplus \cdots \oplus M_i$, und jedes M_k ist endlich erzeugt als A-Modul. Deshalb ist M^* genau dann endlich erzeugt als A^*-Modul, wenn es ein $i \geq 0$ mit $M^*(i) = M^*$ gibt. Letzteres ist äquivalent dazu, daß die I-Filtrierung (M_n) stabil ist. □

4.15 Satz. (Artin-Rees Lemma) *Sei A ein noetherscher Ring, $I \subseteq A$ ein Ideal, M ein endlich erzeugter A-Modul und $N \subseteq M$ ein Untermodul. Ist (M_n) eine stabile I-Filtrierung von M, so ist auch die induzierte I-Filtrierung $(N \cap M_n)$ von N stabil.*

BEWEIS. Nach Lemma 4.14 ist der A^*-Modul $M^* = \bigoplus_{n\geq 0} M_n$ endlich erzeugt. Da $N^* = \bigoplus_{n\geq 0}(N \cap M_n)$ ein A^*-Untermodul von M^* und A^* noethersch ist, ist auch der A^*-Modul N^* endlich erzeugt. Wiederum nach 4.14 ist also die I-Filtrierung $(N \cap M_n)_n$ von N stabil. □

Die wichtigste Anwendung von Artin-Rees besagt, daß die I-adische Topologie von M auf jedem Untermodul von M dessen I-adische Topologie induziert:

4.16 Korollar. *Ist A noethersch und $I \subseteq A$ ein Ideal, und sind $N \subseteq M$ endlich erzeugte A-Moduln, so gibt es ein $k \geq 0$ mit*

$$I^n(N \cap I^k M) \;=\; N \cap I^{n+k} M$$

für alle $n \geq 0$. Insbesondere induzieren die beiden Filtrierungen $N_n = N \cap I^n M$ und $N'_n = I^n N$ auf N dieselbe Topologie. □

Nun eine Reihe wichtiger Folgerungen.

4.17 Korollar. *Sei A ein noetherscher Ring, sei $I \subseteq A$ ein Ideal, und sei $\widehat{\ }$ die I-adische Komplettierung. Für jede exakte Sequenz $M' \xrightarrow{g} M \xrightarrow{f} M''$ aus endlich erzeugten A-Moduln ist auch die komplettierte Sequenz $\widehat{M'} \xrightarrow{\widehat{g}} \widehat{M} \xrightarrow{\widehat{f}} \widehat{M''}$ exakt.*

Beweis. Es genügt, eine kurze exakte Sequenz $0 \to M' \to M \to M'' \to 0$ zu betrachten. Die Behauptung folgt aus Satz 4.5, wenn man beachtet: 1) Die I-adische Filtrierung von M induziert auf M'' die I-adische Filtrierung von M''; 2) auf M' induziert sie eine Filtrierung, die für die Komplettierung zur I-adischen Filtrierung von M' äquivalent ist, nach Korollar 4.16 und Korollar 4.12. □

4.18 Sei $I \subseteq A$ ein Ideal und $\widehat{A} = \varprojlim A/I^n$ die I-adische Komplettierung, sei M ein A-Modul. Dann hat man eine natürliche $\widehat{A}$-lineare Abbildung $\widehat{A} \otimes_A M \to \widehat{M} = \varprojlim M/I^n M$, gegeben durch

$$(a_0 + I,\, a_1 + I^2,\, \dots) \otimes x \;\mapsto\; (a_0 x + IM,\, a_1 x + I^2 M,\, \dots).$$

I.a. ist diese Abbildung weder injektiv noch surjektiv. Jedoch gilt:

4.19 Theorem. *Sei A ein noetherscher Ring und $I \subseteq A$ ein Ideal, und sei $\widehat{\ }$ die I-adische Komplettierung.*

(a) *Für jeden endlich erzeugten A-Modul M ist die Abbildung $\widehat{A} \otimes_A M \to \widehat{M}$ aus 4.18 ein Isomorphismus.*
(b) *$i\colon A \to \widehat{A}$ ist flach.*

Beweis. (a) Sei $G \xrightarrow{q} F \xrightarrow{p} M \to 0$ eine exakte Sequenz von A-Moduln mit F und G frei von endlichem Rang. Dann hat man das kommutative Diagramm

$$\begin{array}{ccccccc}
\widehat{A} \otimes_A G & \xrightarrow{1\otimes q} & \widehat{A} \otimes_A F & \xrightarrow{1\otimes p} & \widehat{A} \otimes_A M & \longrightarrow & 0 \\
\downarrow\sim & & \downarrow\sim & & \downarrow & & \\
\widehat{G} & \xrightarrow{\widehat{q}} & \widehat{F} & \xrightarrow{\widehat{p}} & \widehat{M} & \longrightarrow & 0
\end{array}$$

Die obere Zeile ist exakt wegen der Rechtsexaktheit des Tensorprodukts, die untere nach Korollar 4.17. Die beiden ersten senkrechten Pfeile sind bijektiv, da die I-adische Komplettierung mit endlichen direkten Summen vertauscht. Aus Diagrammjagd folgt, daß auch der dritte senkrechte Pfeil bijektiv ist.

(b) Es genügt, für jede Inklusion $N \subseteq M$ von endlich erzeugten A-Moduln zu zeigen, daß die induzierte Abbildung $N \otimes_A \widehat{A} \to M \otimes_A \widehat{A}$ injektiv ist. Nach (a) identifiziert sich diese Abbildung mit der von $N \subseteq M$ induzierten Abbildung $\widehat{N} \to \widehat{M}$, und ist daher injektiv nach Korollar 4.17. □

4.20 Korollar. *Sei A ein noetherscher Ring und $I \subseteq A$ ein Ideal, und sei $\widehat{A}$ die I-adische Komplettierung von A. Sei $J = \ker(\widehat{A} \to A/I)$.*

(a) *$J = I\widehat{A}$, und $J \subseteq \operatorname{Rad}(\widehat{A})$.*
(b) *Für jedes $n \geq 1$ ist $\ker(\widehat{A} \to A/I^n) = J^n$ $(= I^n\widehat{A})$, und $A/I^n \to \widehat{A}/J^n$ ist ein Isomorphismus.*
(c) *$\operatorname{Gr}^J(\widehat{A}) = \operatorname{Gr}^I(A)$.*

Man schreibt meistens $\widehat{I}$ für $J = I\widehat{A}$. (In der Tat ist auch $J = \varprojlim I/I^n$ die I-adische Komplettierung von I.)

BEWEIS. Die exakte Sequenz $0 \to I^n \to A \to A/I^n \to 0$ von A-Moduln gibt folgendes kommutative Diagramm:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & I^n \otimes \widehat{A} & \longrightarrow & \widehat{A} & \longrightarrow & \widehat{A}/I^n\widehat{A} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} & & \downarrow{\scriptstyle\sim} & & \\ 0 & \longrightarrow & \widehat{I^n} & \longrightarrow & \widehat{A} & \longrightarrow & A/I^n & \longrightarrow & 0 \end{array}$$

Die obere Zeile entsteht durch Tensorierung mit $\widehat{A}$ und ist exakt nach 4.19(b). Die untere Zeile ist die I-adische Komplettierung, und ist exakt nach Korollar 4.17. Die vertikalen Pfeile sind bijektiv nach 4.19(a). Daraus folgen die Aussagen (b) und (c). Für (a) ist noch zu zeigen $1 - x \in (\widehat{A})^*$ für jedes $x \in J$. Die geometrische Reihe $\sum_{n\geq 0} x^n$ konvergiert in $\widehat{A}$ wegen $x^n \in J^n$, und $(1-x)\sum_n x^n = 1$. □

4.21 Korollar. *Für jeden lokalen noetherschen Ring $(A, \mathfrak{m})$ ist $\widehat{A} = \varprojlim A/\mathfrak{m}^n$ ein lokaler Ring mit maximalem Ideal $\widehat{\mathfrak{m}} = \mathfrak{m}\widehat{A}$ und mit Restklassenkörper $\widehat{A}/\widehat{\mathfrak{m}} = A/\mathfrak{m}$.* □

Wir zeigen nun, daß die Komplettierung eines noetherschen Rings wieder noethersch ist. Dazu betrachten wir assoziierte graduierte Ringe und Moduln.

4.22 Lemma. *Sei A ein Ring und $f\colon M \to N$ ein Homomorphismus von filtrierten A-Moduln, d.h. es gelte $f(M_n) \subseteq N_n$ für alle n. Seien $\mathrm{Gr}(f)\colon \mathrm{Gr}(M) \to \mathrm{Gr}(N)$ bzw. $\widehat{f}\colon \widehat{M} \to \widehat{N}$ die induzierten Abbildungen. Ist $\mathrm{Gr}(f)$ injektiv bzw. surjektiv, so gilt dasselbe für $\widehat{f}$.*

BEWEIS. Für $n \geq 1$ sei $f_n\colon M/M_n \to N/N_n$ die von f induzierte Abbildung. Es ist $f_1 = \mathrm{Gr}_0(f)$. Aus den kommutativen Diagrammen mit exakten Zeilen

$$\begin{array}{ccccccccc} 0 & \longrightarrow & M_n/M_{n+1} & \longrightarrow & M/M_{n+1} & \longrightarrow & M/M_n & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle \mathrm{Gr}_n(f)} & & \downarrow{\scriptstyle f_{n+1}} & & \downarrow{\scriptstyle f_n} & & \\ 0 & \longrightarrow & N_n/N_{n+1} & \longrightarrow & N/N_{n+1} & \longrightarrow & N/N_n & \longrightarrow & 0 \end{array}$$

sieht man induktiv: Ist $\mathrm{Gr}(f)$ injektiv (bzw. surjektiv), so ist f_n injektiv (bzw. surjektiv) für alle n. Im ersten Fall ist $\widehat{f} = \varprojlim f_n$ injektiv nach Lemma 4.6. Im zweiten Fall ist $\ker(f_{n+1}) \to \ker(f_n)$ surjektiv für alle n (Schlangenlemma). Anwendung von Lemma 4.6 auf die exakte Sequenz

$$0 \;\to\; (\ker f_n) \;\to\; (M/M_n) \;\xrightarrow{(f_n)}\; (N/N_n) \;\to\; 0$$

von projektiven Systemen zeigt dann, daß $\widehat{f}$ surjektiv ist. □

Der wesentliche Schritt im Beweis ist das folgende Lemma:

4.23 Lemma. *Sei A ein Ring, I ein Ideal in A und M ein A-Modul mit einer separierten I-Filtrierung (M_n). Es sei A I-adisch vollständig, und $\mathrm{Gr}(M)$ sei endlich erzeugt als Modul über $\mathrm{Gr}(A) = \mathrm{Gr}^I(A)$. Dann ist der A-Modul M endlich erzeugt.*

BEWEIS. Der $\mathrm{Gr}(A)$-Modul $\mathrm{Gr}(M)$ wird von endlich vielen homogenen Elementen $\xi_1, \ldots, \xi_r$ erzeugt, etwa mit $\deg(\xi_i) = n_i$. Es ist also $\xi_i = x_i + M_{n_i+1}$ mit

$x_i \in M_{n_i}$ $(i = 1, \ldots, r)$. Sei $F(i)$ gleich A, versehen mit der I-Filtrierung

$$F(i)_n := \begin{cases} A, & \text{falls } n \leq n_i, \\ I^{n-n_i}, & \text{falls } n \geq n_i, \end{cases}$$

und sei $F = F(1) \oplus \cdots \oplus F(r)$, aufgefaßt als filtrierter A-Modul mit $F_n = \bigoplus_i F(i)_n$ für alle n. Wegen A vollständig sind auch die filtrierten A-Moduln $F(i)$, und somit F, vollständig. Die Abbildung

$$f\colon F \to M, \quad f(a_1, \ldots, a_r) = a_1 x_1 + \cdots + a_r x_r$$

ist ein Homomorphismus von filtrierten A-Moduln, denn

$$f(F(i)_n) = \begin{cases} Ax_i & n \leq n_i, \\ I^{n-n_i} x_i & n \geq n_i \end{cases}$$

ist in M_n enthalten, für alle $i = 1, \ldots, r$. Die von f induzierte Abbildung

$$\mathrm{Gr}(f)\colon \mathrm{Gr}(F) \to \mathrm{Gr}(M)$$

ist ein Homomorphismus von graduierten $\mathrm{Gr}(A)$-Moduln. Für $i = 1, \ldots, r$ ist $\mathrm{Gr}_{n_i} F(i) = A/I$, und der Erzeuger $\overline{1}$ darin wird durch $\mathrm{Gr}(f)$ auf $\xi_i = \overline{x}_i \in \mathrm{Gr}_{n_i}(M)$ abgebildet. Also ist $\mathrm{Gr}(f)$ surjektiv. Nach Lemma 4.22 ist also auch $\widehat{f}\colon \widehat{F} \to \widehat{M}$ surjektiv. Im kommutativen Diagramm

$$\begin{array}{ccc} F & \xrightarrow{f} & M \\ {\scriptstyle\sim}\downarrow & & \downarrow{\scriptstyle i_M} \\ \widehat{F} & \xrightarrow{\widehat{f}} & \widehat{M} \end{array}$$

ist also i_M surjektiv. Wegen M separiert ist i_M auch injektiv, also bijektiv, und daher ist f surjektiv. Also wird M erzeugt von $x_1, \ldots, x_r$. □

4.24 Theorem. *Ist A ein noetherscher Ring und I ein Ideal von A, so ist auch die I-adische Komplettierung $\widehat{A}$ von A noethersch.*

Beweis. Versehe $\widehat{A}$ mit der kanonischen, also der $\widehat{I}$-adischen Filtrierung (4.20). Diese ist separiert. Außerdem ist $\mathrm{Gr}^{\widehat{I}}(\widehat{A}) = \mathrm{Gr}^I(A)$ (Korollar 4.20(c)), und dieser Ring ist noethersch, siehe 4.9. Sei M ein Ideal von $\widehat{A}$. Versehe M mit der I-Filtrierung $M_n = M \cap \widehat{I}^n$ $(n \geq 0)$. Dann ist $\mathrm{Gr}(M)$ ein Ideal in $\mathrm{Gr}(\widehat{A})$, ist also als solches endlich erzeugt. Nach Lemma 4.23 (angewandt auf den Ring $\widehat{A}$) ist das Ideal M von $\widehat{A}$ endlich erzeugt. □

Wir wollen jetzt zeigen, daß für die I-adische Komplettierung $\widehat{A}$ von A gilt $\dim(\widehat{A}) = \dim(A)$. Es stimmt für jeden noetherschen Ring A und jedes Ideal I, aber wir beweisen es nur im Spezialfall, wo A lokal und $I = \mathfrak{m}$ das maximale Ideal von A ist.

4.25 Im folgenden sei stets $(A, \mathfrak{m})$ ein lokaler noetherscher Ring. Ist M ein endlich erzeugter A-Modul mit $\mathfrak{m}^n M = 0$ für ein $n \geq 0$, so gibt es eine endliche Folge

$$\{0\} = M_0 \subsetneq M_1 \subsetneq \cdots \subsetneq M_r = M$$

von Untermoduln mit $M_i/M_{i-1} \cong A/\mathfrak{m}$ $(i = 1, \ldots, r)$ als A-Moduln. Jede solche Folge heißt eine *Kompositionsreihe* von M. Wie bei endlichen Gruppen gilt der Satz von Jordan-Hölder: Je zwei Kompositionsreihen von M haben dieselbe Länge r. Man nennt r die *Länge* des A-Moduls M und schreibt $l(M) = r$.

Die Länge ist additiv in exakten Sequenzen: Ist $0 \to M' \to M \to M'' \to 0$ eine kurze exakte Sequenz von A-Moduln und $\mathfrak{m}^n M = 0$ für ein $n \geq 0$, so ist $l(M) = l(M') + l(M'')$. Enthält A einen Körper k mit $k \cong A/\mathfrak{m}$, so ist einfach $l(M) = \dim_k(M)$.

4.26 Satz. *Sei I ein $\mathfrak{m}$-primäres Ideal von A, und sei $(M_n)_{n\geq 0}$ eine stabile I-Filtrierung auf A.*

(a) *Es gibt (genau) ein Polynom $g(t) \in \mathbb{Q}[t]$ mit $l(A/M_n) = g(n)$ für alle $n \gg 0$.*
(b) *Es ist* $\deg g(t) \leq \mu(I)$.
(c) *Grad und Leitkoeffizient von $g(t)$ hängen nur von I ab (nicht von der Filtrierung).*

Beweis. (Skizze) Betrachte den graduierten Ring $G = \mathrm{Gr}^I(A)$. Ist $r = \mu(I)$ und $I = (a_1, \ldots, a_r)$, so hat man einen Isomorphismus $(A/I)[x_1, \ldots, x_r]/J \cong G$ graduierter Ringe (mit $\deg(x_i) = 1$), für ein geeignetes homogenes Ideal J (siehe auch 4.9). Ähnlich wie in B5 zeigt man die Existenz eines Polynoms $q \in \mathbb{Q}[t]$ mit $l(A/I^i) = g(i)$ für $i \gg 0$, und mit $\deg(g) \leq r$. Das gibt die Behauptungen (a) und (b) für die I-adische Filtrierung $M_n = I^n$.

(c) Seien (M_n), (M'_n) zwei stabile I-Filtrierungen auf A. Dann sind sie im folgenden Sinn vergleichbar: Nach 4.11 gibt es $n_0, n_1 \geq 0$ mit $M_{n+n_0} \subseteq I^n$, $M'_{n+n_1} \subseteq I^n$ für alle $n \geq 0$. Es folgt für $n \geq 0$:

$$M'_{n_0+n_1+n} \subseteq I^{n+n_0} \subseteq M_{n+n_0} \subseteq I^n \subseteq M'_n$$

Also ist $g'(t) \leq g(t + n_0) \leq g'(t + n_0 + n_1)$ für $t \gg 0$, also haben g und g' gleichen Grad und Leitkoeffizient. □

Bezeichne den Grad aus 4.26 mit $d_I(A) := \deg g(t)$.

4.27 Lemma. *Für je zwei $\mathfrak{m}$-primäre Ideale I, J von A ist $d_I(A) = d_J(A)$.*

Beweis. Versehe A mit der I-adischen bzw. J-adischen Filtrierung, dann haben wir entsprechende Polynome $g_I(t)$ bzw. $g_J(t) \in \mathbb{Q}[t]$ gemäß 4.26(a). Ist $I \subseteq J$, so ist $l(A/I^n) \geq l(A/J^n)$ für alle n, also $\deg(g_I) \geq \deg(g_J)$. Andererseits ist $g_{I^r}(n) = l(A/I^{rn}) = g_I(rn)$ für $n \gg 0$, also $g_{I^r}(t) = g_I(rt)$, also $\deg(g_{I^r}) = \deg(g_I)$. Es gibt Indizes r, s mit $I^r \subseteq J^s \subseteq I$, also folgt die Behauptung. □

Wir schreiben $d(A) := d_I(A)$, für I ein beliebiges primäres Ideal von A.

4.28 Lemma. *Ist $x \in \mathfrak{m}$ ein Nichtnullteiler von A, so ist $d(A/x) < d(A)$.*

Beweis. Sei $B = A/Ax$. Sei I ein primäres Ideal von A mit $x \in I$, z.B. $I = \mathfrak{m}$, und sei $J = I/Ax$, ein primäres Ideal von B. Für alle n haben wir die exakte Sequenz

$$0 \to \frac{Ax}{Ax \cap I^n} \to \frac{A}{I^n} \to \frac{B}{J^n} \to 0.$$

Durch $(Ax \cap I^n)_{n\geq 0}$ wird eine stabile I-Filtrierung auf $Ax \cong A$ gegeben, nach dem Artin-Rees Lemma 4.15. Wegen

$$l(B/J^n) = l(A/I^n) - l(Ax/Ax \cap I^n),$$

und weil die Hilbertpolynome zu beiden Summanden auf der rechten Seite gleichen Grad $d(A)$ und Leitkoeffizient haben nach 4.26, hat das Polynom zur linken Seite kleineren Grad. □

4.29 Korollar. *Für jeden noetherschen lokalen Ring A ist $d(A) = \dim(A)$.*

BEWEIS. Sei $\dim(A) = d$. Es gibt ein primäres Ideal I mit $\mu(I) = d$ (Theorem 2.3). Nach Satz 4.26(b) ist also $d(A) = d_I(A) \leq d$. Die Umkehrung zeigen wir durch Induktion nach d, wobei der Beginn $d = 0$ trivial ist. Es gibt ein Primideal $\mathfrak{p}$ von A mit $\dim(A/\mathfrak{p}) = d$, dann ist $d(A) \geq d(A/\mathfrak{p})$. Kann also annehmen, daß A integer ist. Wähle $x \in \mathfrak{m}$ mit $\dim(A/Ax) = d - 1$. Nach Induktion ist dann $d(A/Ax) = d - 1$, und aus 4.28 folgt $d(A) > d(A/Ax)$, also $d(A) \geq d$. □

Die wichtigste Folgerung ist:

4.30 Theorem. *Für jeden noetherschen lokaler Ring $(A, \mathfrak{m})$ mit Komplettierung $\widehat{A}$ und graduiertem Ring $\mathrm{Gr}(A) = \mathrm{Gr}^{\mathfrak{m}}(A)$ ist*

$$\dim(A) \;=\; \dim(\widehat{A}) \;=\; \dim \mathrm{Gr}(A).$$

BEWEIS. Es gibt ein Polynom $g \in \mathbb{Q}[t]$ mit $l(A/\mathfrak{m}^n) = g(n)$ für alle $n \gg 0$, und es ist $\dim(A) = \deg(g)$ (Korollar 4.29). Nach Korollar 4.20 und Theorem 4.24 ist auch $(\widehat{A}, \widehat{\mathfrak{m}})$ ein noetherscher lokaler Ring mit $\widehat{A}/\widehat{\mathfrak{m}}^n \cong A/\mathfrak{m}^n$ für alle $n \geq 0$. Korollar 4.29 gibt also $\dim(A) = \dim(\widehat{A})$. Andererseits ist $\mathrm{Gr}(A)$ eine endlich erzeugte graduierte Algebra über $k = A/\mathfrak{m}$. Nach B5 ist also auch $\dim \mathrm{Gr}(A) = \deg(g) = \dim(A)$. □

4.31 Korollar. *Für jeden Körper k ist $k[\![x_1, \ldots, x_d]\!]$ ein regulärer lokaler Ring von Dimension d.*

BEWEIS. Das ist die Komplettierung von $k[x_1, \ldots, x_d]_{(x_1,\ldots,x_d)}$, einem regulären lokalen Ring von Dimension d. Die Aussage folgt also aus 4.24 und 4.30. □

4.32 Theorem. *Sei $(A, \mathfrak{m})$ ein lokaler noetherscher Ring, sei $k = A/\mathfrak{m}$. Es sind äquivalent:*

(i) *A ist regulär von Dimension d;*
(ii) *$\widehat{A}$ ist regulär von Dimension d;*
(iii) $\mathrm{Gr}(A) \cong k[x_1, \ldots, x_d]$.

Enthält A einen zu k isomorphen Teilkörper, so ist auch

(iv) $\widehat{A} \cong k[\![x_1, \ldots, x_d]\!]$

äquivalent. (Die Implikation (iv) ⇒ (i) gilt stets.)

BEWEIS. Wegen $\widehat{A}$ lokal (Korollar 4.21) und noethersch (Theorem 4.24) und $\dim(\widehat{A}) = \dim(A)$ (Theorem 4.30) folgt (i) ⇔ (ii) aus $A/\mathfrak{m}^2 \cong \widehat{A}/\widehat{\mathfrak{m}}^2$ (Korollar 4.20).

(i) ⇒ (iii): Eine reguläre Parameterfolge $a_1, \ldots, a_d$ von A ($d = \dim(A)$) gibt einen surjektiven Homomorphismus $k[\mathtt{x}] \twoheadrightarrow \mathrm{Gr}(A)$ graduierter Ringe ($\mathtt{x} = (x_1, \ldots, x_d)$), siehe Beweis von 4.26. Wegen $\dim \mathrm{Gr}(A) = d$ (Theorem 4.30) ist dieser auch injektiv. Umgekehrt folgt aus (iii) wegen diesem Theorem, daß $\dim(A) = d$ und $\mathfrak{m}/\mathfrak{m}^2 \cong k^d$, also A regulär ist.

Genauso sieht man (iv) ⇒ (i). Sei jetzt A regulär mit $k \subseteq A$. Die reguläre Folge $a_1, \ldots, a_d$ gibt dann sogar einen lokalen Homomorphismus $k[\mathtt{x}]_{(\mathtt{x})} \to A$, $x_i \mapsto a_i$ ($i = 1, \ldots, d$) der lokalen Ringe. Die Komplettierung $k[\![\mathtt{x}]\!] \to \widehat{A}$ ist ein Isomorphismus nach Lemma 4.22, denn die zugehörige Abbildung der graduierten Ringe ist ein Isomorphismus nach dem Argument eben. □

Die Äquivalenz von (iv) mit (i) ist allgemeiner richtig unter der viel schwächeren Bedingung, daß der reguläre lokale Ring A lediglich irgend einen Körper enthält. Man sieht direkt, daß dies zu $\mathrm{char}(\mathrm{Quot}(A)) = \mathrm{char}(k)$ äquivalent ist. Der Beweis

ist deshalb viel schwieriger, weil man vor allem zeigen muß, daß $\widehat{A}$ eine Kopie von k enthält (Struktursatz von Cohen).

Ist dagegen $\operatorname{char}(\operatorname{Quot}(A)) = 0$ und $\operatorname{char}(k) = p > 0$, so kann $\widehat{A}$ kein Potenzreihenring sein. (Beispiel $A = \mathbb{Z}_{p\mathbb{Z}}$ (p prim) und $\widehat{A} = \mathbb{Z}_p$, der Ring der ganzen p-adischen Zahlen.)

5. Potenzreihenringe

5.1 Ist A ein Ring und $\mathtt{x} = (x_1, \dots, x_n)$, so bezeichent $A[\![\mathtt{x}]\!] = A[\![x_1, \dots, x_n]\!]$ den Ring der formalen Potenzreihen in $\mathtt{x}$ mit Koeffizienten in A. Der Ring $A[\![\mathtt{x}]\!]$ besteht also aus den formalen unendlichen Reihen

$$f \;=\; \sum_{\alpha \in \mathbb{Z}_+^n} a_\alpha \, \mathtt{x}^\alpha$$

mit $a_\alpha \in A$ für alle α, versehen mit der offensichtlichen Addition und Multiplikation. Für $n \geq 1$ gilt

$$A[\![x_1, \dots, x_n]\!] \;=\; A[\![x_1, \dots, x_{n-1}]\!]\,[\![x_n]\!]$$

kanonisch.

Sei jetzt $A = k$ ein Körper. Die *Ordnung* von $f \in k[\![\mathtt{x}]\!]$ ist definiert durch

$$\omega(f) \;:=\; \min\{|\alpha| \colon \alpha \in \mathbb{Z}_+^n,\ c_\alpha \neq 0\}$$

für $f \neq 0$, sowie $\omega(0) := \infty$). Es gilt $\omega(fg) = \omega(f) + \omega(g)$ und $\omega(f+g) \geq \min\{\omega(f), \omega(g)\}$ für alle $f, g \in k[\![\mathtt{x}]\!]$. Anders gesagt, ω setzt sich zu einer diskreten Bewertung des Quotientenkörpers $k(\!(\mathtt{x})\!) := \operatorname{Quot} k[\![x]\!]$ fort. Der Ring $k[\![\mathtt{x}]\!]$ ist integer und lokal mit maximalem Ideal

$$\mathfrak{m} \;=\; \{f \in k[\![\mathtt{x}]\!] \colon \omega(f) \geq 1\}$$

und Restklassenkörper k. Tatsächlich ist $k[\![\mathtt{x}]\!]$ $\mathfrak{m}$-adisch vollständig, und ist ein regulärer lokaler Ring von Dimension n (Theorem 4.31). Für $f \in \mathfrak{m}$ ist $1 - f$ eine Einheit, nämlich

$$(1-f)^{-1} \;=\; 1 + f + f^2 + \cdots .$$

Die Reihe konvergiert wegen $\omega(f^r) \geq r$. Es ist $\mathfrak{m}^r = \{f \colon \omega(f) \geq r\}$ für alle r.

5.2 Der Quotientenkörper von $k[\![x_1, \dots, x_n]\!]$ wird mit $k(\!(x_1, \dots, x_n)\!)$ bezeichnet. Für $n = 1$ ist $k(\!(x)\!)$ der Körper aller formalen Laurentreihen

$$f \;=\; \sum_{i \in \mathbb{Z}} a_i x^i, \quad a_i = 0 \text{ für alle } i \ll 0.$$

Die diskrete Bewertung auf $k(\!(x)\!)$ ist gegeben durch

$$\omega(f) \;=\; \min\{i \in \mathbb{Z} \colon a_i \neq 0\}$$

für $f \neq 0$. Für $n = 2$ hat man die Inklusion $k[\![x_1, x_2]\!] = k[\![x_1]\!][\![x_2]\!] \subseteq k(\!(x_1)\!)[\![x_2]\!]$, und daher auch die Inklusion von Körpern

$$k(\!(x_1, x_2)\!) \;\subseteq\; k(\!(x_1)\!)(\!(x_2)\!).$$

Diese Inklusion ist *strikt* (Aufgabe 25). Entsprechend sind für mehrere Variablen alle Inklusionen in der Kette

$$k(\!(x_1, \dots, x_n)\!) \;\subseteq\; k(\!(x_1)\!)(\!(x_2, \dots, x_n)\!) \;\subseteq \cdots \subseteq\; k(\!(x_1)\!) \cdots (\!(x_n)\!)$$

von Körpern strikt.

Sei weiter $\mathtt{x} = (x_1, \dots, x_n)$.

5.3 Definition. Die Potenzreihe $f \in k[\![\mathtt{x}]\!]$ heißt *regulär bezüglich x_n (von Ordnung p)*, wenn $f(0,\dots,0,x_n) \in k[\![x_n]\!]$ nicht identisch Null ist (und Ordnung p hat). Äquivalent ist also, daß das Monom x_n^r in f vorkommt für ein $r \geq 0$ (und daß p das kleinste solche r ist).

5.4 Lemma. *Sei $|k| = \infty$, sei $0 \neq f \in k[\![\mathtt{x}]\!]$ mit $\omega(f) = p$. Nach einem geeigneten linearen Koordinatenwechsel über k wird f regulär bezüglich x_n von Ordnung p.*

Beweis. Sei $f = f_p + g$ mit einer Form $f_p \neq 0$ vom Grad p und mit $g \in k[\![\mathtt{x}]\!]$ mit $\omega(g) \geq p+1$. Wähle $v \in k^n$ mit $f_p(v) \neq 0$ und wechsle die Variablen so, daß $v = e_n$ wird. □

5.5 Im weiteren werden wir stets eine der Variablen auszeichnen. Wir setzen daher $A := k[\![\mathtt{x}]\!] = k[\![x_1,\dots,x_n]\!]$ mit $n \geq 0$, und arbeiten in $A[\![y]\!] = k[\![x_1,\dots,x_n,y]\!]$, dem Potenzreihenring über k in den $n+1$ Variablen $x_1,\dots,x_n,y$.

Eine Reihe $f = \sum_{i\geq 0} a_i y^i \in A[\![y]\!]$ (mit $a_i \in A$) ist also genau dann regulär von Ordnung p bezüglich y, wenn $a_p \in A^*$ und $a_i \in \mathfrak{m}_A$ für $0 \leq i < p$ ist. Das Element f heißt ein *Weierstraß-Polynom* (bezüglich y), wenn

$$f \;=\; y^p + a_{p-1}\,y^{p-1} + \cdots + a_1 y + a_0$$

mit $p \geq 0$ und $a_0,\dots,a_{p-1} \in \mathfrak{m}_A$ ist. Das bedeutet also: Die Potenzreihe $f \in k[\![\mathtt{x},y]\!]$ ist regulär bezüglich y von Ordnung p, und ist gleichzeitig ein normiertes Polynom vom Grad p in y, mit Koeffizienten in $A = k[\![\mathtt{x}]\!]$.

5.6 Theorem. (Divisionssatz, Weierstraß) *Sei $A = k[\![\mathtt{x}]\!]$, seien $f, g \in A[\![y]\!]$, und sei $g \in A[\![y]\!]$ regulär von Ordnung p bezüglich y.*

(a) *Es gibt eindeutig bestimmte $q \in A[\![y]\!]$ und $r \in A[y]$ mit $f = qg + r$ und $\deg_y(r) < p$.*
(b) *Sind dabei $f, g \in A[y]$, und ist $\deg_y(g) = p$, so ist auch $q \in A[y]$.*

Die Voraussetzungen an g für (b) (also $g \in A[y]$ mit $\deg_y(g) = p$, und g regulär von Ordnung p bezüglich y) sind zusammen äquivalent dazu, daß ug ein Weierstraß-Polynom vom Grad p bezüglich y ist, für eine Einheit $u \in A^*$.

Beweis. Für jede Potenzreihe $f = \sum_{i\geq 0} a_i y^i$ in $A[\![y]\!]$ (mit $a_i \in A$) sei

$$v(f) \;:=\; \min\{\omega(a_i)\colon\; i \geq 0\}.$$

Es gelten die Eigenschaften einer diskreten Bewertung, also

(1) $v(f) = \infty \;\Leftrightarrow\; f = 0$,
(2) $v(f+g) \;\geq\; \min\{v(f), v(g)\}$,
(3) $v(fg) \;=\; v(f) + v(g)$

für $f, g \in A[\![y]\!]$. Dabei sind (1), (2) klar, ebenso wie $v(fg) \geq v(f) + v(g)$. Um $\leq$ zu zeigen, sei $f = \sum_i a_i y^i$, $g = \sum_i b_i y^i$ und $fg = \sum_i c_i y^i$, und seien $r, s \geq 0$ jeweils minimal mit $v(f) = \omega(a_r)$ bzw. $v(g) = \omega(b_s)$. Dann ist

$$c_{r+s} \;=\; a_r b_s + \sum_{i=1}^{r} a_{r-i} b_{s+i} + \sum_{i=1}^{s} a_{r+i} b_{s-i}.$$

Darin haben alle Summanden außer dem ersten einen ω-Wert $> v(f) + v(g)$. Also ist $\omega(c_{i+j}) = v(f) + v(g)$, und somit folgt $v(fg) \leq v(f) + v(g)$.

Die durch v definierte Topologie macht den Ring $A[\![y]\!]$ vollständig. Ist also (f_i) eine Folge in $A[\![y]\!]$ mit $v(f_{i+1} - f_i) \to \infty$ für $i \to \infty$, so gibt es eindeutig $f \in A[\![y]\!]$ mit $v(f - f_i) \to \infty$ für $i \to \infty$. Das ist klar, denn die Folge der Potenzreihen f_i in der Variablen y konvergiert koeffizientenweise, wegen A vollständig.

Wir beweisen nun den Divisionssatz. Sei $\overline{g}$ das Bild von g in $(A/\mathfrak{m}_A)[\![y]\!] = k[\![y]\!]$. Nach Voraussetzung gilt $\omega(\overline{g}) = p$ für Wir können also (eindeutig) schreiben

$$g \;=\; cy^p + a_0 + a_1 y + \cdots + a_p y^p + y^{p+1} b$$

mit $c \in k^*$, $a_0, \ldots, a_p \in \mathfrak{m}_A$ und $b \in A[\![y]\!]$. Wir setzen

$$h \;:=\; a_0 + a_1 y + \cdots + a_p y^p \in A[y],$$

es ist also $g = h + y^p(c + by)$. Wir definieren die Abbildung $\phi\colon A[\![y]\!] \to A[\![y]\!]$ durch

$$f - qh \;=\; r + y^p(c + by) \cdot \phi(q) \quad (q \in A[\![y]\!])$$

mit $r \in A[y]$ und $\deg_y(r) < p$. Das ist wohldefiniert, denn es ist r die Trunkierung der Potenzreihe $f - qh$ ab der Potenz y^p, und der Rest schreibt sich eindeutig als Produkt $y^p(c+by)\phi(q)$, wegen $c + by \in A[\![y]\!]^*$. Ein Fixpunkt der Abbildung ϕ, also ein $q \in A[\![y]\!]$ mit $\phi(q) = q$, ist ein $q \in A[\![y]\!]$ mit $f = qg + r$ für ein $r \in A[y]$ mit $\deg_y(r) < p$. Wir müssen also zeigen, daß ϕ genau einen Fixpunkt hat.

Das Argument ist analog zum Beweis des Banachschen Fixpunktsatzes. Man zeigt also, daß ϕ "strikt kontrahierend" ist. Für q, $q' \in A[\![y]\!]$ gilt

$$f - qh \;=\; r + y^p(c + by) \cdot \phi(q), \quad f - q'h \;=\; r' + y^p(c + by) \cdot \phi(q')$$

mit r, $r' \in A[y]$ und $\deg(r)$, $\deg(r') < p$. Es folgt

$$(q' - q)h \;=\; (r - r') + y^p(c + by) \cdot \big(\phi(q) - \phi(q')\big).$$

Der v-Wert der rechten Seite ist gleich dem Minimum der beiden Zahlen $v(r - r')$ und $v(y^p(c + by)(\phi q - \phi q'))$, da $r - r'$ ein Polynom vom Grad $< p$ und der Rest durch y^p teilbar ist. Wegen $v(y) = v(c + by) = 0$ folgt insbesondere

$$v\big(\phi(q) - \phi(q')\big) \;\geq\; v\big(h(q' - q)\big).$$

Nach Konstruktion gilt $v(h) \geq 1$, und somit gilt

$$v\big(\phi(q) - \phi(q')\big) \;\geq\; 1 + v(q - q')$$

für alle q, $q' \in A[\![y]\!]$. Damit ist schon klar, daß es höchstens einen Fixpunkt gibt. Ist andererseits $q_0 \in A[\![y]\!]$ beliebig gewählt, so hat die Folge $\phi^i(q_0)$, $i \geq 0$, einen Limes q in $A[\![y]\!]$, denn $v(\phi^{i+1}q_0 - \phi^i q_0) \geq i$ (Cauchyfolge). Dieser Limes ist ein Fixpunkt von ϕ.

Damit ist (a) bewiesen. Sind unter der Voraussetzung des Satzes f, $g \in A[y]$, und ist $\deg_y(g) = p$, so ist der Leitkoeffizient von g eine Einheit in A. Wir können also f auch in $A[y]$ durch g mit Rest dividieren (gewöhnliche Division mit Rest im Polynomring $A[y]$), und erhalten q', $r' \in A[y]$ mit $\deg_y(r') < p$ und mit $f = q'g + r'$. Aus der schon bewiesenen Eindeutigkeit in (a) folgt $q' = q$. □

5.8 Korollar. *Sei $g \in A[y]$ ein Weierstraß-Polynom bezüglich y. Dann ist der kanonische Ringhomomorphismus*

$$A[y]/(g) \;\to\; A[\![y]\!]/(g)$$

ein Isomorphismus.

Beweis. Surjektiv folgt aus 5.6(a), injektiv aus 5.6(b). □

Weiter sei $A = k[\![\mathbf{x}]\!]$.

5.9 Theorem. (Vorbereitungssatz, Weierstraß) *Sei $f \in A[\![y]\!]$ regulär von Ordnung p in y. Dann gibt es eine Einheit u in $A[\![y]\!]$ und ein Weierstraß-Polynom $g \in A[y]$ vom Grad p mit $f = ug$. Dadurch sind u und g eindeutig bestimmt.*

BEWEIS. Nach dem Divisionssatz gibt es eine Identität

$$y^p \;=\; fq + \sum_{i=0}^{p-1} a_i y^i$$

mit $q \in A[\![y]\!]$ und $a_0, \ldots, a_{p-1} \in A$. Nach Anwenden des Homomorphismus $A[\![y]\!] \to (A/\mathfrak{m}_A)[\![y]\!] = k[\![y]\!]$, $g \mapsto \overline{g}$ geht sie über in

$$y^p \;=\; \overline{f} \cdot \overline{q} + \sum_{i=0}^{p-1} \overline{a}_i\, y^i.$$

Dabei ist $\omega(\overline{f}) = p$. Es folgt $\overline{a}_0 = \cdots = \overline{a}_{p-1} = 0$ und $\overline{q} \in k[\![y]\!]^*$, und somit $q \in A[\![y]\!]^*$. Es ist also $g := y^p - \sum_{i=0}^{p-1} a_i y^i$ ein Weierstraß-Polynom in $A[y]$, und es gilt $f = q^{-1}g$. Die Eindeutigkeit folgt aus der Eindeutigkeit im Divisionssatz: Ist $f = u_1 g_1 = u_2 g_2$ mit Einheiten u_i und Weierstraß-Polynomen g_i, und ist dabei $g_i = y^p + r_i$ mit $r_i \in A[y]$ und $\deg_y(r_i) < p$ $(i = 1, 2)$, so folgt $y^p = u_i^{-1} f - r_i$ für $i = 1, 2$, und daraus $u_1 = u_2$ und $r_1 = r_2$ nach 5.6. □

5.11 Theorem. *Der Potenzreihenring $k[\![x_1, \ldots, x_n]\!]$ ist faktoriell.*

BEWEIS. (Für $|k| = \infty$) Wieder sei $n \geq 0$ und $A = k[\![x_1, \ldots, x_n]\!]$. Wir setzen voraus, daß A bereits als faktoriell erkannt ist, und zeigen, daß dann auch $A[\![y]\!]$ faktoriell ist. Da $A[\![y]\!]$ noethersch ist, ist noch zu zeigen, daß jedes irreduzible Element in $A[\![y]\!]$ prim ist.

Sei also $g \in A[\![y]\!]$ irreduzibel. Nach einem Koordinatenwechsel erreichen wir, daß g regulär bezüglich y ist (Lemma 5.4). Nach dem Vorbereitungssatz 5.9 können wir g so mit einer Einheit multiplizieren, daß g ein Weierstraß-Polynom vom Grad p in y wird.

Wir zeigen zunächst, daß g auch in $A[y]$ irreduzibel ist. Sei also $g = g_1 g_2$ mit $g_i \in A[y]$. Nach eventuellem Vertauschen der Faktoren ist dann g_1 eine Einheit in $A[\![y]\!]$. Aus $g_2 = g \cdot g_1^{-1}$ und $g, g_2 \in A[y]$ folgt aber $g_1^{-1} \in A[y]$ nach Aussage (b) in Theorem 5.6. Also ist g_1 eine Einheit in $A[y]$, und daher g in $A[y]$ tatsächlich irreduzibel.

Jetzt seien f_1, $f_2 \in A[\![y]\!]$, und es gelte $g \mid f_1 f_2$ in $A[\![y]\!]$. Nach dem Divisionssatz können wir schreiben

$$f_1 \;=\; q_1 g + r_1, \quad f_2 \;=\; q_2 g + r_2$$

mit $q_i \in A[\![y]\!]$, $r_i \in A[y]$ und $\deg(r_i) < p$ für $i = 1, 2$. Es folgt $r_1 r_2 = gh$ mit $h \in A[\![y]\!]$. Wieder folgt aus 5.6(b), daß $h \in A[y]$ sein muß. Es gilt also $g \mid r_1 r_2$ in $A[y]$. Da g in $A[y]$ irreduzibel und dieser Ring faktoriell ist (nach Induktionsvoraussetzung und Gaußschem Lemma), folgt $g \mid r_i$ in $A[y]$ für ein i, und damit auch $g \mid f_i$ in $A[\![y]\!]$. Also ist $A[\![y]\!]$ faktoriell. □

Das folgende Korollar ist eine Version der henselschen Eigenschaft von Potenzreihenringen.

5.12 Korollar. *Sei $A = k[\![\mathtt{x}]\!] = k[\![x_1, \ldots, x_n]\!]$ mit $n \geq 0$, sei $\mathfrak{m}$ das maximale Ideal von A. Sei $f \in A[y]$ ein normiertes Polynom, und sei $a \in k$ eine Nullstelle der Vielfachheit $p \geq 1$ von $\overline{f}(y) \in (A/\mathfrak{m})[y] = k[y]$. Dann gibt es normierte Polynome $g, h \in A[y]$ mit $f = gh$ und mit $\overline{g} = (y - a)^p$. Dabei sind g und h durch diese Bedingung eindeutig bestimmt.*

BEWEIS. Wir können annehmen $a = 0$ (ersetze y durch $y' = y - a$). Dann ist f regulär von Ordnung p bezüglich y. Nach dem Vorbereitungssatz (Theorem 5.9) ist also $f = ug$ mit $u \in A[\![y]\!]^*$ und einem Weierstraß-Polynom $g \in A[y]$ vom

Grad p (bezüglich y). Es ist also insbesondere $\overline{g} = y^p$, und es gilt $u \in A[y]$ nach Teil (b) des Divisionssatzes 5.6. Die Eindeutigkeit folgt aus der Eindeutigkeit im Vorbereitungssatz. Denn sind g, h wie in 5.12, so ist $h(0) \in A^*$, also ist h eine Einheit in $A[\![y]\!]$. □

5.13 Theorem. (Puiseux) *Sei k ein algebraisch abgeschlossener Körper mit* $\mathrm{char}(k) = 0$. *Dann ist auch der Körper*

$$k(\!(x^{1/\infty})\!) \;:=\; \bigcup_{q\geq 1} k(\!(x^{1/q})\!)$$

algebraisch abgeschlossen.

Man bezeichnet $k(\!(x^{1/\infty})\!)$ als Körper der *(formalen) Puiseuxreihen* über k. Die Elemente von $k(\!(x^{1/\infty})\!)$ sind die formalen unendlichen Reihen

$$f \;=\; \sum_{n\in\mathbb{Z}} a_n x^{n/q}$$

mit $q \in \mathbb{N}$ und $a_n \in k$ $(n \in \mathbb{Z})$, $a_n = 0$ für alle $n \ll 0$. Nach dem Theorem ist also $k(\!(x^{1/\infty})\!)$ ein algebraischer Abschluß des Körpers $k(\!(x)\!)$ der formalen Laurentreihen.

5.14 Korollar. *Ist R ein reell abgeschlossener Körper, und ist P die Anordnung von $R(\!(x)\!)$ mit $x >_P 0$, so ist $R(\!(x^{1/\infty})\!)$ der reelle Abschluß von $(R(\!(x)\!), P)$.*

Beweis. Sei $S = R(\!(x^{1/\infty})\!) = \bigcup_q R(\!(x^{1/q})\!)$. Die Erweiterung $S/R(\!(x)\!)$ ist algebraisch, und S hat eine P fortsetzende Anordnung (das Vorzeichen einer Puiseuxreihe ist das Vorzeichen des Koeffizienten des Monoms von kleinstem Grad). Nach Theorem 5.13 ist der Körper $S(\sqrt{-1})$ algebraisch abgeschlossen. Daraus folgt die Behauptung. □

Beweis von Theorem 5.13. Sei $F = k(\!(x^{1/\infty})\!)$, sei $f \in F[t]$ ein normiertes Polynom vom Grad $n > 1$. Wir zeigen, daß f reduzibel über F ist. Es gibt ein $q \geq 1$, so daß f Koeffizienten in $k(\!(x^{1/q})\!)$ hat. Wir ersetzen $x^{1/q}$ durch x und nehmen deshalb an

$$f(t) \;=\; t^n + a_1(x)t^{n-1} + \cdots + a_n(x)$$

mit $a_i(x) \in k(\!(x)\!)$. Indem wir t durch $t + \frac{1}{n}a_1(x)$ ersetzen, erreichen wir auch $a_1(x) = 0$. Sei

$$r \;=\; \min\Big\{\frac{\omega(a_i)}{i} \colon a_i \neq 0,\ i = 1,\ldots,n\Big\},$$

und sei $r = \frac{p}{q}$ mit $q \in \mathbb{N}$ und $p \in \mathbb{Z}$. Die Substitutionen $x = y^q$ und $t = y^p u$ geben

$$\begin{aligned} f &= y^{np}u^n + a_1(y^q)y^{(n-1)p}\,u^{n-1} + \cdots + a_n(y^q) \\ &= y^{np}\Big(u^n + y^{-p}a_1(y^q)\,u^{n-1} + \cdots + y^{-np}a_n(y^q)\Big) \\ &= y^{np}\,g(u). \end{aligned}$$

Die Koeffizienten $b_i = y^{-ip}a_i(y^q)$ von $g(u)$ liegen in $k(\!(y)\!)$ und erfüllen

$$\omega(b_i) \;=\; -ip + q\omega(a_i) \;=\; iq\Big(\frac{\omega(a_i)}{i} - \frac{p}{q}\Big) \;\geq\; 0.$$

Also ist $g(u) = u^n + b_1u^{n-1} + \cdots + b_n$ ein normiertes Polynom in $k[\![y]\!][u]$. Dabei ist $b_1 = 0$, und mindestens einer der Koeffizienten $b_2, \ldots, b_n$ ist eine Einheit. Also hat $\overline{g}(u) \in k[u]$ mindestens zwei verschiedene Nullstellen in k. Nach Korollar 5.12 ist $g(u)$ reduzibel in $k[\![y]\!][u]$. Das bedeutet, daß $f(t)$ reduzibel über $k(\!(x^{1/q})\!)$, also auch über F, ist. □

KAPITEL VI

Nichtnegativstellensätze

1. Saturierte Präordnungen

Sei A stets ein beliebiger Ring ($\frac{1}{2} \in A$). Für jede Teilmenge $M \subseteq A$ schreibe weiter

$$X(M) \;=\; X_A(M) \;=\; \{\alpha \in \operatorname{Sper}(A) \colon \forall\, f \in M \;\; f(\alpha) \geq 0\},$$
$$Z(M) \;=\; Z_A(M) \;=\; \{\alpha \in \operatorname{Sper}(A) \colon \forall\, f \in M \;\; f(\alpha) = 0\}$$

(abgeschlossene Teilmengen von $\operatorname{Sper}(A)$).

1.2 Notation. Ist $Z \subseteq \operatorname{Sper}(A)$ eine Teilmenge, so schreiben wir

$$\mathcal{P}(Z) \;:=\; \{f \in A \colon f|_Z \geq 0\} = \bigcap_{P \in Z} P$$

(Präordnung der auf Z nichtnegativen Elemente von A).

1.3 Bemerkung. Die Operatoren X und $\mathcal{P}$ sind inklusionsumkehrend, und für alle Teilmengen $M \subseteq A$ und $Z \subseteq \operatorname{Sper}(A)$ gilt:

$$Z \subseteq X(M) \quad \Leftrightarrow \quad M \subseteq \mathcal{P}(Z).$$

1.4 Lemma. *Für jede Präordnung T sind äquivalent:*

(i) *T ist Durchschnitt von Positivkegeln von A;*
(ii) *$T = \mathcal{P}(X(T))$;*
(iii) *aus $f \in A$ und $sf = f^{2m} + t$ mit $s, t \in T$ und $m \geq 0$ folgt $f \in T$.*

Sind diese Eigenschaften erfüllt, so heißt T saturiert.

(Siehe Aufgabe 30.)

1.5 Korollar. *Zu jeder Präordnung T von A gibt es eine eindeutig bestimmte kleinste saturierte Präordnung S von A mit $T \subseteq S$. Man schreibt* $\operatorname{Sat}(T) := S$ *und nennt* $\operatorname{Sat}(T)$ *die* Saturierung *von T. Es ist*

$$\operatorname{Sat}(T) \;=\; \mathcal{P}(X(T)) \;=\; \{f \in A \colon \exists\, m \in \mathbb{N} \;\exists\, s,\, t \in T \;\; sf = f^{2m} + t\}.$$

1.6 Beispiele.

1. Ist $A = R[\mathbf{x}]$ und $T = PO(f_1, \ldots, f_r)$, so ist $\operatorname{Sat}(T) = \mathcal{P}(K) = \{f \in R[\mathbf{x}]\colon f|_K \geq 0\}$ für $K = S(f_1, \ldots, f_r)$.

2. Die kleinste saturierte Präordnung in A ist

$$A_+ \;=\; \operatorname{Sat}(\Sigma A^2) \;=\; \{f \in A \colon \forall\, \xi \in \operatorname{Sper}(A)\;\; f(\xi) \geq 0\},$$

die Präordnung der *psd Elemente* von A. Daß die Präordnung ΣA^2 saturiert ist bedeutet also $A_+ = \Sigma A^2$. Sage dafür kurz, im Ring A gilt psd = sos.

3. Ist A nicht reell, d.h. ist $\operatorname{Sper}(A) = \varnothing$, so ist $\Sigma A^2 = A$ (II.2.14). Es gilt dann also psd = sos aus trivialen Gründen.

4. Ist $A = K$ ein Körper, so ist jede Präordnung in K saturiert (I.28). In den meisten anderen Ringen ist das falsch. Ist $R[\mathbf{x}] = R[x_1, \ldots, x_n]$ der Polynomring

über einem reell abgeschlossenen Körper R, so gilt psd = sos in $R[\mathbf{x}]$ nur für $n \leq 1$ (Hilbert, IV.2.8). Auch für $n = 1$ gibt es nichtsaturierte Präordnungen in $R[x]$, z.B. $T = PO(x^3)$.

5. Nach dem Satz von Fejér-Riesz (IV.2.19) gilt psd = sos in $R[x, y]/(x^2+y^2-1)$.

6. Für jede (abgeschlossene) semialgebraische Teilmenge K von R ist die saturierte Präordnung $\mathcal{P}(K)$ in $R[x]$ endlich erzeugt (von den "natürlichen Erzeugern"), IV.2.16.

In den obigen Beispielen sind saturierte Präordnungen jeweils endlich erzeugt. Im allgemeinen ist das jedoch die Ausnahme. Tatsächlich gilt das folgende allgemeine negative Resultat:

1.7 Theorem. *Sei V eine affine R-Varietät, seien $f_1, \ldots, f_r \in R[V]$, und sei $K = S(f_1, \ldots, f_r) \subseteq V(R)$. Ist $\dim(K) \geq 3$, so gibt es ein $p \in R[V]$ mit $p \geq 0$ auf $V(R)$, aber $p \notin PO(f_1, \ldots, f_r)$.*

Insbesondere ist eine endlich erzeugte Präordnung in $R[\mathbf{x}]$ niemals saturiert, wenn sie eine Menge von Dimension ≥ 3 beschreibt.

1.8 Sei $(A, \mathfrak{m})$ ein regulärer lokaler Ring mit $k = A/\mathfrak{m}$, sei $\mathrm{Gr}(A) = \bigoplus_{n\geq 0} \mathrm{Gr}_n(A)$ der zu A assoziierte graduierte Ring, mit $\mathrm{Gr}_n(A) = \mathfrak{m}^n/\mathfrak{m}^{n+1}$ $(n \geq 0)$. Sei $d = \dim(A)$, und sei $a_1, \ldots, a_d$ ein reguläres Parametersystem von A. Nach Theorem V.4.32 ist $\mathrm{Gr}(A)$ der Polynomring über k in den d Variablen $\xi_i = a_i + \mathfrak{m}^2 \in \mathrm{Gr}_1(A)$ $(i = 1, \ldots, d)$. Insbesondere ist der Ring $\mathrm{Gr}(A)$ nullteilerfrei. Für $0 \neq f \in A$ sei

$$\omega(f) \;:=\; \max\{n \geq 0 \colon f \in \mathfrak{m}^n\}.$$

Das Maximum ist wohldefiniert nach dem Krullschen Durchschnittssatz (Aufgabe 21). Es gilt

$$\omega(f+g) \;\geq\; \min\{\omega(f), \omega(g)\}$$

und

$$\omega(fg) \;=\; \omega(f) + \omega(g)$$

für alle $f, g \in A$, letzteres da der Ring $\mathrm{Gr}(A)$ integer ist. Es ist ω also die Restriktion einer diskreten Bewertung von $K = \mathrm{Quot}(A)$ auf A.

Ist $0 \neq f \in A$ und $n := \omega(f)$, so definiere die *Leitform* von f als das Element

$$L(f) \;:=\; f + \mathfrak{m}^{n+1} \;\in\; \mathfrak{m}^n/\mathfrak{m}^{n+1} = \mathrm{Gr}_n(A).$$

Es ist also $L(f) \neq 0$ eine Form vom Grad n in den Erzeugern $\xi_i = L(a_i)$ von $\mathrm{Gr}(A)$.

1.9 Lemma. *Sei A ein regulärer lokaler Ring, mit reellem Restklassenkörper k. Ist $0 \neq f \in A$ eine Summe von r Quadraten in A, so ist $\omega(f) = 2s$ gerade, und $L(f) \in \mathrm{Gr}_{2s}(A)$ ist eine Summe von r Quadraten von Elementen in $\mathrm{Gr}_s(A)$.*

Beweis. Wir zeigen zunächst, daß der Restklassenkörper der diskreten Bewertung ω von $K = \mathrm{Quot}(A)$ (definiert durch $\omega(\frac{a}{b}) = \omega(a) - \omega(b)$ für $0 \neq a, b \in A$) reell ist. Das bedeutet, für $x_1, \ldots, x_n \in K$ mit $\omega(x_i) \geq 0$ und $\omega(\sum x_i^2) > 0$ gilt $\omega(x_i) > 0$ für alle i. Schreibe $x_i = \frac{a_i}{b_i}$ mit $0 \neq a_i, b_i \in A$ und $\omega(a_i) \geq \omega(b_i)$. Indem wir die Gleichung mit $\prod_i b_i^2$ multiplizieren, sehen wir, daß es genügt, zu zeigen: Aus $y_1, \ldots, y_n \in A$ mit $\omega(y_i) \geq r$ und $\omega(\sum y_i^2) > 2r$ folgt $\omega(y_i) > r$ für alle i. Anders gesagt, aus $p_1, \ldots, p_n \in \mathrm{Gr}_r(A)$ und $\sum p_i^2 = 0$ in $\mathrm{Gr}_{2r}(A)$ folgt $p_i = 0$ für alle i. Aber das ist klar, denn $\mathrm{Gr}(A)$ ist ein Polynomring über dem reellen Körper k (Theorem V.4.32).

Ist jetzt $f = \sum_{i=1}^r f_i^2$ mit $f_i \in A$, und ist $s = \min_i \omega(f_i)$, so ist $\omega(f) = 2s$ (IV.1.1). Also ist $L(f)$ die Summe der $L(f_j)^2$ für diejenigen Indices j, für welche $\omega(f_j) = s$ ist. □

1.10 Korollar. *Sei A ein regulärer lokaler Ring mit $\dim(A) \geq 3$ und mit reellem Restklassenkörper k. Dann gilt* psd $\neq$ sos *in A.*

Beweis. Sei $a_1, \ldots, a_d$ ein reguläres Parametersystem ($d = \dim(A) \geq 3$), sei

$$M(x_1, x_2, x_3) \;=\; x_1^4 x_2^2 + x_1^2 x_2^4 + x_3^6 - 3x_1^2 x_2^2 x_3^2$$

die Motzkin-Form, und sei $f := M(a_1, a_2, a_3)$. Dann ist f psd in A (als Bild des psd Elements $M \in \mathbb{Z}[x_1, x_2, x_3]$ unter dem Homomorphismus $x_i \mapsto a_i$ nach A). Es ist $\omega(f) = 6$, und die Leitform $L(f) = M(\xi_1, \xi_2, \xi_3)$ ist die Motzkinform in den Erzeugern $\xi_i = L(a_i)$ des Polynomrings $\mathrm{Gr}(A) \cong k[\xi_1, \ldots, \xi_d]$. Da $L(f)$ nicht sos in $\mathrm{Gr}(A)$ ist, ist f nicht sos in A. □

1.11 Beweis von Theorem 1.7. Zur Vereinfachung nehmen wir an, daß K in V Zariski-dicht und V irreduzibel (mit $\dim(V) = d \geq 3$) ist. O.E. seien $f_1, \ldots, f_r \neq 0$. Wegen K Zariski-dicht in V ist auch die basisch offene Menge $\{\xi \in V(R) \colon f_i(\xi) > 0 \ (i = 1, \ldots, r)\}$ Zariski-dicht in V. Also gibt es $\xi \in V_{\mathrm{reg}}(R)$ mit $f_i(\xi) > 0$ für $i = 1, \ldots, r$ (Artin-Lang, siehe Theorem V.3.13). Seien $a_1, \ldots, a_d \in R[V]$ derart, daß die a_i das maximale Ideale des lokalen Rings $A := \mathcal{O}_{V,\xi} = \mathbb{R}[V]_{\mathfrak{m}_\xi}$ erzeugen. Sei

$$p \;:=\; M(a_1, a_2, a_3) \;\in R[V]$$

(mit M die Motzkin-Form). Dann ist $p \geq 0$ auf $V(R)$. Behaupte, $p \notin T = PO(f_1, \ldots, f_r)$. Sei dazu $\widehat{A}$ die Komplettierung von A. Wäre $p \in T$, so wäre p sos in $\widehat{A}$, denn wegen $f_i(\xi) > 0$ sind die f_i Quadrate in $\widehat{A}$. Nach dem Argument im Beweis von Korollar 1.10 ist jedoch p nicht sos in $\widehat{A}$. □

Ist K eine basisch abgeschlossene Menge mit $\dim(K) \geq 3$, so ist die saturierte Präordnung $\mathcal{P}(K)$ niemals endlich erzeugt nach Theorem 1.7. Es bleibt die Frage in Dimension ≤ 2. Wir werden sie in typischen Fällen beantworten.

1.12 Satz. *Sei A ein Ring und T eine saturierte Präordnung in A. Für jede multiplikative Teilmenge S von A ist auch die Präordnung T_S in A_S saturiert.*

(T_S ist die von T in A_S erzeugte Präordnung.)

Beweis. Identifiziere $\mathrm{Sper}(A_S)$ mit einem Teilraum von $\mathrm{Sper}(A)$ wie üblich, und analog für die Zariski-Spektren. Sei $X = X_A(T)$ die zu T gehörende pro-basisch abgeschlossene Menge in $\mathrm{Sper}(A)$, es ist also $T = \mathcal{P}(X)$. Dann ist $X_{A_S}(T_S) = X \cap \mathrm{Sper}(A_S) =: X_S$ die zu T_S in $\mathrm{Sper}(A_S)$ assoziierte Menge. Sei $f \in A_S$ mit $f \geq 0$ auf X_S, wir wollen $f \in T_S$ zeigen. Dafür können wir $f \in A$ annehmen. Sei $W := \{f < 0\} \cap X$. Behaupte, es gibt ein $s \in S$ mit $s \equiv 0$ auf W. In der Tat, zu jedem $\alpha \in W$ gibt es ein $s_\alpha \in S$ mit $s_\alpha(\alpha) = 0$, wegen $\alpha \notin \mathrm{Sper}(A_S)$. Es ist also

$$W \;\subseteq\; \bigcup_{\alpha \in W} Z(s_\alpha).$$

Die Menge W in $\mathrm{Sper}(A)$ ist prokonstruierbar, und die Mengen $Z(s_\alpha)$ sind alle konstruierbar. Da die konstruierbare Topologie kompakt ist, gibt es also endlich viele $\alpha_1, \ldots, \alpha_n \in W$ mit $W \subseteq \bigcup_{i=1}^n Z(s_{\alpha_i})$. Für $s := s_{\alpha_1} \cdots s_{\alpha_n}$ gilt also $s \in S$ und $W \subseteq Z(s)$, wie behauptet. Für $g := s^2 f \in A$ gilt also $g \geq 0$ auf X, also $g \in T$. Somit liegt $f = \frac{g}{s^2}$ in T_S. □

1.13 Lemma. *Sei A ein Ring und $T \subseteq A$ eine Präordnung. Dann ist*

$$\sqrt{\operatorname{supp}(T)} \;=\; \bigcap_{\alpha\in X(T)} \operatorname{supp}(\alpha) \;=\; \operatorname{supp}(\operatorname{Sat}(T)).$$

Beweis. Wegen $\operatorname{Sat}(T) = \bigcap_{\alpha\in X(T)} P_\alpha$ ist $\operatorname{supp}(\operatorname{Sat}(T)) = \bigcap_{\alpha\in X(T)} \operatorname{supp}(\alpha)$. Insbesondere ist dies ein Radikalideal. Wegen $T \subseteq \operatorname{Sat}(T)$ folgt also

$$\sqrt{\operatorname{supp}(T)} \;\subseteq\; \operatorname{supp}(\operatorname{Sat}(T)).$$

Für die Umkehrung sei $f \in \operatorname{supp}(\operatorname{Sat}(T))$, also $f \equiv 0$ auf $X(T)$. Nach dem abstrakten reellen Nullstellensatz II.2.9 folgt dann $f \in \sqrt{\operatorname{supp}(T)}$. □

1.14 Lemma. *Sei $Y \subseteq \operatorname{Sper}(A)$ eine prokonstruierbare Teilmenge, und sei $I = \bigcap_{\alpha\in Y} \operatorname{supp}(\alpha)$. Ist $\mathfrak{p}$ ein Primideal von A mit $I \subseteq \mathfrak{p}$, so gibt es ein $\alpha \in Y$ mit $\operatorname{supp}(\alpha) \subseteq \mathfrak{p}$. Insbesondere ist*

$$\dim(A/I) \;=\; \sup_{\alpha\in Y} \dim(A/\operatorname{supp}(\alpha)).$$

Beweis. Angenommen $\operatorname{supp}(\alpha) \not\subseteq \mathfrak{p}$ für alle $\alpha \in Y$, d.h. zu jedem $\alpha \in Y$ gebe es ein $f_\alpha \in \operatorname{supp}(\alpha)$ mit $f_\alpha \notin \mathfrak{p}$. Dann ist $Y \subseteq \bigcup_{\alpha\in Y} Z(f_\alpha)$. Wegen Y prokonstruierbar, und da alle $Z(f_\alpha)$ konstruierbar sind, folgt aus der Kompaktheit der konstruierbaren Topologie: Es gibt endlich viele $\alpha_1, \ldots, \alpha_n \in Y$ mit $Y \subseteq \bigcup_{i=1}^n Z(f_{\alpha_i})$. Für $f := f_{\alpha_1} \cdots f_{\alpha_n}$ gilt dann $Y \subseteq Z(f)$, d.h. $f \in \bigcap_{\alpha\in Y} \operatorname{supp}(\alpha) = I$. Wegen $f \notin \mathfrak{p}$ ist das ein Widerspruch zu $I \subseteq \mathfrak{p}$. □

1.15 Bemerkungen.

1. Ist $K \subseteq R^n$ eine semialgebraische Menge, und ist $V \subseteq \mathbb{A}^n$ der Zariskiabschluß von K, so gilt für das Verschwindungsideal von V in $R[\mathbf{x}]$:

$$I_V \;=\; \bigcap_{\alpha\in\widetilde{K}} \operatorname{supp}(\alpha).$$

2. Aus Lemma 1.13 folgt daher: Ist T eine endlich erzeugte Präordnung in $R[\mathbf{x}]$ und $K = S(T) \subseteq R^n$, also $\widetilde{K} = X_{R[\mathbf{x}]}(T)$, und ist $V \subseteq \mathbb{A}^n$ der Zariskiabschluß von K, so gilt $\sqrt{\operatorname{supp}(T)} = I_V$. Insbesondere ist also $\dim(K) = \dim R[\mathbf{x}]/I_V = \dim R[\mathbf{x}]/\operatorname{supp}(T)$.

1.17 Bemerkung. Gegeben sei jetzt eine abgeschlossene Untervarietät W einer affinen R-Varietät V und ein $g \in R[W]$ mit $g \geq 0$ auf $W(R)$. Wann läßt sich g zu einem auf ganz $V(R)$ nichtnegativen Polynom fortsetzen, d.h. wann gibt es $f \in R[V]$ mit $g = f|_W$ und $f \geq 0$ auf $V(R)$?

Anders gesagt: Sei A ein Ring, $I \subseteq A$ ein Ideal und $\varphi\colon A \to A/I$ der kanonische Homomorphismus. Es gilt $\varphi(A_+) \subseteq (A/I)_+$. Sei umgekehrt $b \in (A/I)_+$, wann gibt es $a \in A_+$ mit $b = a + I$?

1. Jede Quadratsumme in B läßt sich zu einer Quadratsumme in A liften. Gilt also psd = sos in B, so ist $A_+ \to B_+$ surjektiv.

2. Im allgemeinen ist die Abbildung $A_+ \to B_+$ nicht surjektiv. Beispiel: $A = \mathbb{R}[x, y]$, $B = A/I$ mit $I = (y^2 - x^3)$ (siehe Aufgabe 33).

Wir können immerhin eine hinreichende Bedingung für die Existenz eines psd Lifts formulieren. Im Hinblick auf spätere Anwendung formulieren wir die Aussage in größerer Allgemeinheit:

1.18 Lemma. *Sei A ein Ring und $I \subseteq A$ ein Ideal, sei $Y \subseteq \operatorname{Sper}(A)$ eine abgeschlossene Teilmenge, und sei $f \in A$ mit $f \geq 0$ auf $Y \cap Z(I)$. Für jedes*

$\alpha \in Y \cap Z(I) \cap Z(f)$ gebe es ein $h \in I$ mit $h \geq 0$ auf Y und $f + h \geq 0$ auf einer Umgebung von α in Y. Dann gibt es ein $h \in I$ mit $f + h \geq 0$ auf Y.

BEWEIS. Es genügt, für jedes $\alpha \in Y$ zu zeigen, daß es ein $h_\alpha \in I$ gibt mit $h_\alpha \geq 0$ auf Y und $(f + h_\alpha)(\alpha) \geq 0$. Dann gibt es nämlich endlich viele $\alpha_1, \ldots, \alpha_n \in Y$ mit $Y \subseteq \bigcup_{i=1}^n X(f + h_{\alpha_i})$, denn Y ist kompakt in der konstruierbaren Topologie. Für $h := \sum_{i=1}^n h_{\alpha_i}$ gilt dann $h \in I$ und $f + h \geq 0$ auf Y.

Sei also $\alpha \in Y$. Zunächst habe α eine Spezialisierung β in $Z(I)$. Ist $f(\beta) = 0$, so gibt es nach Voraussetzung ein $h \in I \cap \mathcal{P}(Y)$ mit $f + h \geq 0$ in einer Umgebung von β, und insbesondere $(f + h)(\alpha) \geq 0$. Ist $f(\beta) \neq 0$, so ist $f(\beta) > 0$, und wir können $h = 0$ nehmen. Es bleibt der Fall, wo $\overline{\{\alpha\}} \cap Z(I) = \varnothing$ ist. Das bedeutet $-1 \in P_\alpha + I$, d.h. es gibt $g \in I$ mit $g(\alpha) \geq 1$. Für $h := (1 + f^2)g^2$ gilt dann $h \in I$ und $h(\alpha) > |f(\alpha)|$. Dieses h tut's. □

1.19 Korollar. *Ist $f \in A$ psd in einer Umgebung von $Y \cap Z(I)$, so gibt es $h \in I$ mit $f + h \geq 0$ auf Y.*

BEWEIS. Für jedes α ist die Bedingung aus Lemma 1.18 erfüllt mit $h = 0$. □

1.20 Korollar. *Ist $f \in A$ mit $f > 0$ auf $Y \cap Z(I)$, so gibt es ein $h \in I$ mit $f + h > 0$ auf Y.*

BEWEIS. Die Konstruktion im Beweis von Lemma 1.18 gibt zu jedem $\alpha \in Y$ ein Element $h_\alpha \in I$ mit $h_\alpha \geq 0$ auf Y und mit $(f + h_\alpha)(\alpha) > 0$. Das Kompaktheitsargument aus dem Beweis dort gibt also die gewünschte Folgerung. □

2. Quadratsummen in lokalen Ringen

2.1 Theorem. *Sei A ein lokaler Ring, sei $u \in A^*$ psd. Dann ist u eine Quadratsumme in A.*

BEWEIS. Für den Ring $B = A[t]/(t^2 + u) = A[\sqrt{-u}]$ gilt $\mathrm{Sper}(B) = \varnothing$. Also ist -1 sos in B. Es gibt also a_i, $b_i \in A$ mit $-1 = \sum_{i=1}^r (a_i + b_i\tau)^2$ in B (mit $\tau = \bar{t}$), also insbesondere mit

$$-1 \;=\; \sum_{i=1}^r a_i^2 - u \sum_{i=1}^r b_i^2. \qquad (*)$$

Das besagt $u \sum_i b_i^2 = 1 + \sum_i a_i^2$. Falls $\sum_{i=1}^r b_i^2$ Einheit in A ist, so ist

$$u \;=\; \Big(\sum_{i=1}^r b_i^2\Big)^{-1} \Big(1 + \sum_{i=1}^r a_i^2\Big)$$

sos in A, und wir sind fertig. Ist der Restklassenkörper $k = A/\mathfrak{m}$ reell, so gilt $\sum_i b_i^2 \in A^*$ automatisch. Für den Rest des Beweises nehmen wir an $\sum_i b_i^2 \in \mathfrak{m}_A$ und zeigen, daß man dann eine andere Identität $(*)$ finden kann, welche die gewünschte Eigenschaft hat.

Für x, $y \in A^r$ sei $\langle x, y\rangle = \sum_{i=1}^r x_i y_i$. Indem wir r notfalls vergrößern, können wir erreichen, daß $b_i \in \mathfrak{m}_A$ für zwei Indices i gilt, etwa b_1, $b_2 \in \mathfrak{m}_A$. Es gibt w_1, $w_2 \in A$ mit $0 \neq \overline{w}_1^2 + \overline{w}_2^2 \neq -\frac{1}{u}$ in k. Sei $w = (w_1, w_2, 0, \ldots, 0) \in A^r$, sowie $a = (a_1, \ldots, a_r)$, $b = (b_1, \ldots, b_r)$. Dann ist $\langle b, w\rangle \in \mathfrak{m}_A$. Wegen $\langle b, b\rangle \in \mathfrak{m}_A$ ist $\langle a, a\rangle \equiv -1 \pmod{\mathfrak{m}_A}$ nach $(*)$. Setze

$$\gamma \;=\; \frac{\langle a, a\rangle - u\langle b, w\rangle}{\langle a, a\rangle - u\langle w, w\rangle} \;\in\; A^*$$

(der Nenner ist eine Einheit wegen $1 + u\langle w, w\rangle \notin \mathfrak{m}_A$). Setze weiter

$$\begin{pmatrix} a' \\ b' \end{pmatrix} := \begin{pmatrix} a \\ b \end{pmatrix} - 2\gamma \begin{pmatrix} a \\ w \end{pmatrix} \in A^r \oplus A^r.$$

Wir berechnen:

$$\begin{aligned} \langle a', a'\rangle - u\langle b', b'\rangle &= (1-2\gamma)^2\langle a, a\rangle - u\langle b - 2\gamma w, b - 2\gamma w\rangle \\ &= \Big(\langle a, a\rangle - u\langle b, b\rangle\Big) + 4\gamma\Big((\gamma-1)\langle a, a\rangle + u(\langle b, w\rangle - \gamma\langle w, w\rangle)\Big) \\ &= -1 + 4\gamma\Big(\gamma\big(\langle a, a\rangle - u\langle w, w\rangle\big) - \big(\langle a, a\rangle - u\langle b, w\rangle\big)\Big) \\ &= -1. \end{aligned}$$

Andererseits ist $\langle b', b'\rangle \in A^*$. Denn wegen $\langle b, b\rangle$, $\langle b, w\rangle \in \mathfrak{m}$ ist

$$\langle b', b'\rangle \equiv \langle b - 2\gamma w,\ b - 2\gamma w\rangle \equiv 4\gamma^2\langle w, w\rangle \not\equiv 0$$

modulo $\mathfrak{m}$. Nach dem Argument zu Beginn ist also $u \in \Sigma A^2$. □

Der Fall von semilokalen Ringen läßt sich auf lokale Ringe zurückführen:

2.2 Satz. *Sei A ein semilokaler Ring und M ein quadratischer Modul in A. Ist $f \in A$, und ist $\frac{f}{1} \in M_{\mathfrak{m}}$ für jedes maximale Ideal $\mathfrak{m}$ von A, so ist $f \in M$.*

($M_{\mathfrak{m}}$ ist der von M in $A_{\mathfrak{m}}$ erzeugte quadratische Modul.)

Beweis. Seien $\mathfrak{m}_1, \ldots, \mathfrak{m}_r$ die maximalen Ideale von A. Nach Voraussetzung gibt es für jedes $i = 1, \ldots, r$ ein $s_i \in A$ mit $s_i \notin \mathfrak{m}_i$ und mit $s_i^2 f \in M$. Nach dem Chinesischen Restsatz gibt es für jedes $i = 1, \ldots, r$ ein $a_i \in A$ mit $a_i \equiv 1 \pmod{\mathfrak{m}_i}$ und mit $a_i \equiv 0 \pmod{\mathfrak{m}_j}$ für alle $j \neq i$ in $\{1, \ldots, r\}$. Dann ist

$$u := \sum_{i=1}^{r} (a_i s_i)^2$$

eine Einheit in A, und es gilt

$$uf = \sum_{i=1}^{r} a_i^2 \cdot s_i^2 f \in M.$$

Wegen u^{-1} sos in A folgt $f \in M$. □

2.3 Korollar. *In einem semilokalen Ring ist jede positiv definite Einheit eine Quadratsumme.*

Beweis. Sei f eine psd Einheit in A. Für jedes $\mathfrak{m} \in \mathrm{Max}(A)$ ist f auch eine psd Einheit in $A_{\mathfrak{m}}$, also sos in $A_{\mathfrak{m}}$ nach Theorem 2.1. Nach Lemma 2.2, angewandt auf $M = \Sigma A^2$, folgt f sos in A. □

Sei A ein Ring, seien $g_1, \ldots, g_r \in A$, und sei $T = PO_A(g_1, \ldots, g_r)$. Wir adjungieren formale Quadratwurzeln der g_i und schreiben

$$B = A[x_1, \ldots, x_r]/(x_i^2 - g_i \colon i = 1, \ldots, r).$$

2.4 Lemma. *Für jedes $f \in A$ gilt:*

(a) *$f \in \mathrm{Sat}(T)$ genau dann, wenn f in B psd ist;*
(b) *$f \in T$ genau dann, wenn f in B sos ist.*

BEWEIS. Das Bild der Restriktionsabbildung $\mathrm{Sper}(B) \to \mathrm{Sper}(A)$ ist die Teilmenge $X_A(T)$ von $\mathrm{Sper}(A)$. Daraus folgt (a). Als A-Modul ist B frei mit den 2^r Produkten

$$x_J := \prod_{i\in J} x_i \quad (J \subseteq [r])$$

als Basis. Sei $s\colon B \to A$ die A-lineare Abbildung mit $s(1) = 1$ und $s(x_J) = 0$ für alle $J \neq \varnothing$. Ist $b = \sum_J a_J x_J \in B$ (mit $a_J \in A$), so ist

$$s(b^2) \;=\; \sum_J a_J^2 g_J$$

mit $g_J := x_J^2 = \prod_{i\in J} g_i \in T$, also ist $s(b^2) \in T$. Ist also $f \in A$ und f sos in B, so ist $f = s(f) \in T$. Die Umkehrung ist ohnehin klar. □

2.5 Satz. *Sei A ein semilokaler Ring und T eine Präordnung in A. Dann gilt* $\mathrm{Sat}(T) \cap A^* \subseteq T$.

BEWEIS. Sei $f \in A^* \cap \mathrm{Sat}(T)$. Wegen $f > 0$ auf $X(T)$ gilt $X(-f) \cap \bigcap_{t\in T} X(t) = \varnothing$. Wegen der Kompaktheit der konstruierbaren Topologie ist schon ein endlicher Teildurchschnitt leer, es gibt also endlich viele $t_1, \ldots, t_r \in T$ mit $f > 0$ auf $X(t_1, \ldots, t_r)$. Betrachte den Ring

$$B \;=\; A[x_1, \ldots, x_r] \,/\, (x_1^2 - t_1,\, \ldots,\, x_r^2 - t_r).$$

Da A semilokal und B eine endliche A-Algebra ist, ist auch B semilokal (going-up). In B ist f eine psd Einheit, also sos nach Korollar 2.3. Nach Lemma 2.4 bedeutet das $f \in T$. □

Nach diesen Allgemeinheiten nun ein Schlüssellemma:

2.6 Lemma. *Sei A ein semilokaler Ring und T eine Präordnung in A, und sei $f \in \mathrm{Sat}(T)$. Ist $f \in T + (f^2)$, so folgt $f \in T$.*

BEWEIS. Nach Satz 2.2 können wir annehmen, daß A lokal ist. Nach Voraussetzung gibt es eine Identität $f = t + f^2 g$ mit $t \in T$ und $g \in A$. Ist $f \in A^*$, so folgt $f \in T$ nach Satz 2.5. Sei also $f \in \mathfrak{m}$. Dann ist $f(1 - fg) = t$ und $1 - fg \in A^*$. Behaupte, es ist $1 - fg \in \mathrm{Sat}(T)$. Denn $f \geq 0$ auf $X(T)$, und auf $X(T) \cap U(f)$ ist $1 - fg \geq 0$, während auf $X(T) \cap Z(f)$ gilt $1 - fg \equiv 1$. Nach Satz 2.5 folgt also $1 - fg \in T$. Somit liegt $f = (1 - fg)^{-1} t$ ebenfalls in T. □

Das folgende Korollar verallgemeinert noch einmal Satz 2.5:

2.7 Korollar. *Ist A semilokal und T eine Präordnung in A, und ist $f \in A$ strikt positiv auf $X(T)$, so ist $f \in T$.*

BEWEIS. Sei $f > 0$ auf $X(T)$. Nach Lemma 2.6 genügt es zu zeigen, daß $f \in T + (f^2)$ ist. Aber es ist $X(T + (f^2)) = X(T) \cap Z(f) = \varnothing$, und somit $T + (f^2) = A$. □

2.8 Satz. *Sei A ein semilokaler Ring und $T \subseteq A$ eine Präordnung, und sei $f \in \mathrm{Sat}(T)$. Ist $f \notin T$, so gibt es ein Ideal J mit $\sqrt{J} = \sqrt{\mathrm{supp}(T + Af)}$ und mit $f \notin T + J$.*

BEWEIS. Wir notieren zunächst eine simple Beobachtung. Ist $f \in \mathrm{Sat}(T)$ und $g \in \mathrm{supp}(T)$, und ist $f \in T + A(f + g)^2$, so folgt $f \in T$. In der Tat, es folgt $f + g \in T + A(f + g)^2$, und daraus wegen $f + g \in \mathrm{Sat}(T)$ auch $f + g \in T$ nach Lemma 2.6. Wegen $-g \in T$ folgt daraus $f \in T$.

Sei jetzt also $f \in \mathrm{Sat}(T)$. Es ist $X(T+Af) = X(T) \cap Z(f) = X(T+Af^2)$. Nach Lemma 1.13 gilt also

$$\sqrt{\mathrm{supp}(T+Af)} \;=\; \sqrt{\mathrm{supp}(T+Af^2)}.$$

Sei $(g_\lambda)_{\lambda\in\Lambda}$ ein Erzeugendensystem des Ideals $\mathrm{supp}(T+Af^2)$, und sei

$$J \;:=\; Af^2 + \sum_{\lambda\in\Lambda} A(f+g_\lambda)^2.$$

Es gilt $\sqrt{J} = \sqrt{\mathrm{supp}(T+Af)}$. Behaupte, aus $f \in T+J$ folgt $f \in T$, womit dann der Satz gezeigt ist. Sei also $f \in T+J$. Es gibt endlich viele unter den g_λ, sagen wir $g_1, \ldots, g_r$, mit

$$f \;\in\; T + \big(f^2,\, (f+g_1)^2,\, \ldots,\, (f+g_r)^2\big).$$

Wir wenden jetzt die zu Beginn des Beweises gemachte Bemerkung an. Es ist $f \in T'+A(f+g_r)^2$ mit $T' = T+(f^2,(f+g_1)^2,\ldots,(f+g_{r-1})^2)$, und es gilt $f \in \mathrm{Sat}(T')$ (wegen $X(T') \subseteq Z(f)$) und $g_r \in \mathrm{supp}(T+Af^2) \subseteq \mathrm{supp}(T')$. Also folgt $f \in T'$. Iteriert man diesen Schritt, so erhält man $f \in T+(f^2)$. Eine weitere Anwendung von 2.6 gibt daher $f \in T$. □

2.9 Notation. Sei $(A,\mathfrak{m})$ ein lokaler noetherscher Ring, und sei T eine Präordnung in A. Mit $\widehat{T}$ bezeichnen wir die von T in der Komplettierung $\widehat{A} = \varprojlim A/\mathfrak{m}^n$ von A erzeugte Präordnung, und nennen $\widehat{T}$ die *Komplettierung* von T. Sei $i\colon A \to \widehat{A}$ der kanonische Homomorphismus.

2.10 Lemma. *Es gilt $i^{-1}(\widehat{T}+\widehat{\mathfrak{m}}^n) = T+\mathfrak{m}^n$ für alle $n \geq 0$.*

Beweis. "$\supseteq$" ist klar. "$\subseteq$": Sei $f \in A$ mit $i(f) \in \widehat{T}+\widehat{\mathfrak{m}}^n$. Habe also

$$i(f) \;\equiv\; g_1^2 t_1 + \cdots + g_r^2 t_r \pmod{\widehat{\mathfrak{m}}^n}$$

mit $t_j \in T$, $g_j \in \widehat{A}$ $(j=1,\ldots,r)$ und $r \geq 1$. Wegen $A/\mathfrak{m}^n \xrightarrow{\sim} \widehat{A}/\widehat{\mathfrak{m}}^n$ (V.4.20) gibt es $h_j \in A$ mit $i(h_j) - g_j \in \widehat{\mathfrak{m}}^n$ $(j=1,\ldots,r)$. Für $t := \sum_j h_j^2 t_j \in T$ gilt dann $i(f) \equiv i(t) \pmod{\widehat{\mathfrak{m}}^n}$. Also ist $f - t \in i^{-1}(\widehat{\mathfrak{m}}^n) = \mathfrak{m}^n$, d.h. $f \in T+\mathfrak{m}^n$. □

2.11 Theorem. *Sei A ein lokaler noetherscher Ring, sei T eine Präordnung in A, und sei $f \in \mathrm{Sat}(T)$. Für jedes $\alpha \in Z(f)\cap X(T)$ sei $\mathrm{supp}(\alpha) = \mathfrak{m}$. Dann sind äquivalent:*

(i) $f \in T$,
(ii) $i(f) \in \widehat{T}$,
(iii) $f \in T+\mathfrak{m}^n$ *für alle $n \geq 0$.*

Bedingungen (i)–(iii) sind insbesondere erfüllt, wenn $\widehat{T}$ (in $\widehat{A}$) saturiert ist.

Beweis. Für die Präordnung $T' := T+Af$ gilt $X(T') = Z(f)\cap X(T)$. Gemäß Lemma 1.13 ist die Voraussetzung äquivalent zu $\mathfrak{m} \subseteq \sqrt{\mathrm{supp}(T')}$. Die Implikation (i) ⇒ (ii) ist trivial, und (ii) ⇒ (iii) folgt aus Lemma 2.10. Es gelte (iii), angenommen $f \notin T$. Nach Satz 2.8 gibt es ein Ideal J mit $\sqrt{J} = \sqrt{\mathrm{supp}(T')}$ und $f \notin T+J$. Also $\mathfrak{m} \subseteq \sqrt{J}$. Wegen A noethersch gibt es $n \geq 0$ mit $\mathfrak{m}^n \subseteq J$, und es folgt $f \notin T+\mathfrak{m}^n$, Widerspruch zur Voraussetzung (iii). Wegen $i(f) \in \mathrm{Sat}(\widehat{T})$ ist (ii) erfüllt, wenn $\widehat{T}$ saturiert ist. □

2.12 Bemerkung. Wir erläutern die Voraussetzung von Theorem 2.11 in einer geometrischen Situation. Seien dazu $h_1,\ldots,h_r \in R[\mathbf{x}] = R[x_1,\ldots,x_n]$ (mit R reell abgeschlossen), sei $K = S(h_1,\ldots,h_r) \subseteq R^n$ die zugehörige basisch abgeschlossene Menge, sei $\xi \in K$, und sei $A = R[\mathbf{x}]_{\mathfrak{m}_\xi}$ der lokale Ring in ξ (mit $\mathfrak{m}_\xi \subseteq R[\mathbf{x}]$ das

maximale Ideal zum Punkt ξ). Sei $T = PO_A(h_1, \ldots, h_r)$, und sei $f \in R[\mathbf{x}]$ mit $f|_K \geq 0$. Dann ist $f \in \mathrm{Sat}(T)$. Sei $f(\xi) = 0$. Die Bedingung

$$\mathrm{supp}(\alpha) \;=\; \mathfrak{m}_A \quad \text{für alle} \quad \alpha \in Z_A(f) \cap X_A(T) \tag{$*$}$$

aus 2.11 ist (zum Beispiel) erfüllt, wenn f in K nur endlich viele Nullstellen hat.

Hier sind erste Anwendungen der bewiesenen Resultate.

2.13 Korollar. *Sei A ein lokaler noetherscher Ring mit $\dim(A) = 1$, sei $T \subseteq A$ eine Präordnung, und sei $f \in \mathrm{Sat}(T)$ ein Nichtnullteiler. Dann gilt $f \in T \Leftrightarrow f \in \widehat{T}$.*

Beweis. Da f kein Nullteiler und $\dim(A) = 1$ ist, ist $\mathfrak{m} \subseteq \sqrt{Af}$, also auch $\mathfrak{m} \subseteq \sqrt{\mathrm{supp}(T + Af)}$. Die Voraussetzungen von Theorem 2.11 sind also erfüllt. □

2.14 Korollar. *Sei A ein diskreter Bewertungsring. Dann gilt* psd = sos *in A.*

Beweis. Sei $0 \neq f \in A_+$. Ist $k = A/\mathfrak{m}$ nicht reell, so ist $f > 0$ auf $\mathrm{Sper}(A)$, und somit f sos (Korollar 2.7). Sei k reell, sei $f = ut^n$ mit $u \in A^*$ und t ein Primelement. Dann ist n gerade, und u ist psd in A, also sos (Theorem 2.1). □

Ist C eine Kurve über dem reell abgeschlossenen Körper R, so gilt also psd = sos in $\mathcal{O}_{C,\xi}$ für jeden nichtsingulären Punkt $\xi \in C(R)$. Aber auch in singulären Punkten kann psd = sos gelten, abhängend von der Natur der Singularität:

2.15 Satz. *Sei C eine irreduzible ebene Kurve über R, sei $\xi \in C(R)$ ein gewöhnlicher Doppelpunkt. Dann gilt* psd = sos *in $\mathcal{O}_{C,\xi}$.*

Beweis. Sei $A = \mathcal{O}_{C,\xi}$. O.E. sei $\xi = (0,0)$, seien (x, y) affine Koordinaten. Die Voraussetzung sagt $C = \mathcal{V}(f)$ mit

$$f \;=\; f_2(x,y) + f_3(x,y) + \cdots \;\in\; R[x,y]$$

mit f_i homogen vom Grad i, und dabei ist f_2 das Produkt von zwei nicht assoziierten Linearformen in $R[x,y]$. Es ist $\widehat{A} = R[\![x,y]\!]/(f)$. Nach dem Vorbereitungssatz können wir annehmen, daß f ein Weierstraßpolynom vom Grad 2 ist, also $f = y^2 + 2a(x)xy + b(x)x^2$ mit $a, b \in R[\![x]\!]$. Somit $f = (y + xa(x))^2 - x^2c(x)$ mit einem $c \in \mathbb{R}[\![x]\!]$, und aus der Voraussetzung folgt $c(0) > 0$. Also $f = g_1g_2$ mit $g_{1,2} = y + x(a(x) \pm c(x))$. Es gibt einen Automorphismus von $R[\![x,y]\!]$ mit $x \mapsto g_1$, $y \mapsto g_2$, siehe Aufgabe .. Es folgt $\widehat{A} = R[\![x,y]\!]/(g_1g_2) \cong R[\![x,y]\!]/(xy)$. In diesem Ring gilt psd = sos nach Aufgabe .. Nach Korollar 2.13 folgt psd = sos also auch in A. □

Für andere Kurvensingularitäten gilt dagegen psd $\neq$ sos, zum Beispiel für die Kuspe $y^2 = x^3$ (siehe Aufgabe 35).

Hier ist eine weitere Illustration:

2.16 Satz. *Sei $f \in R[\mathbf{x}]$ ein psd Polynom. Es sei $f(0) = 0$, und die Hessematrix $\big((\partial^2 f/\partial x_i \partial x_j)(0)\big)$ im Ursprung sei positiv definit. Ist 0 die einzige reelle Nullstelle von f in einer Zariski-Umgebung von 0, so ist f sos im lokalen Ring $R[\mathbf{x}]_{(\mathbf{x})}$.*

Beweis. Sei $\mathfrak{m} = (x_1, \ldots, x_n)$ und $A = R[\mathbf{x}]_{\mathfrak{m}}$, der lokale Ring im Ursprung. Nach linearem Koordinantenwechsel ist $f = \sum_i x_i^2 + g$ mit $g \in \mathfrak{m}^3$. Nach Aufgabe 36 ist f sos in $\widehat{A} = R[\![x_1, \ldots, x_n]\!]$. Wegen f psd und $Z(f)$ endlich ist Theorem 2.11 anwendbar (siehe Bemerkung 2.12) und gibt die Behauptung. □

3. Zweidimensionale lokale Ringe

3.1 Theorem. *Sei k ein Körper. Im Potenzreihenring $k[\![x,y]\!]$ gilt* psd = sos.

Stelle zunächst einige Hilfsmittel bereit. Die beiden folgenden Sätze sind klassisch und stammen von Artin:

3.2 Satz. *Sei k ein Körper, sei $f \in k[t]$ ein normiertes irreduzibles Polynom. Ist der Körper $k[t]/(f)$ nichtreell, so ist f eine Summe von Quadraten in $k[t]$.*

Beweis. Wir können annehmen, daß k reell ist. Nach Voraussetzung gibt es eine Gleichung

$$fh \;=\; \sum_{i=1}^{n} g_i^2 \qquad (*)$$

mit g_i, $h \in k[t]$, wobei $g_i \neq 0$ und $\deg(g_i) < \deg(f)$ für alle i gilt. Es ist also $\deg(h) < \deg(f)$, und wegen k reell ist $h \neq 0$. Wähle eine Identität $(*)$ mit $h \neq 0$ und $\deg(h)$ minimal. Wir zeigen, daß h konstant ist, und sind dann fertig.

Angenommen $\deg(h) \geq 1$. Es gibt einen Index i mit $h \nmid g_i$. Denn wäre $g_i = hg_i'$ für alle i, so $fh = h^2 \sum_i g_i'^2$, also $f = h \sum_i g_i'^2$, Widerspruch wegen f irreduzibel und $1 \leq \deg(h) < \deg(f)$. Schreibe $g_i = q_i h + r_i$ mit q_i, $r_i \in k[t]$ und $\deg(r_i) < \deg(h)$, dann ist $r_i \neq 0$ für ein i. Benutze die Identität

$$\Big(\sum_i g_i^2\Big)\Big(\sum_i r_i^2\Big) \;=\; \Big(\sum_i r_i g_i\Big)^2 + \sum_{i<j}\Big(r_i g_j - r_j g_i\Big)^2. \qquad (**)$$

Wegen $r_i \equiv g_i \pmod h$ für alle i ist $\sum_i r_i^2 \equiv \sum_i r_i g_i \equiv \sum_i g_i^2 \equiv 0 \pmod h$, und weiter $r_i g_j - r_j g_i \equiv 0 \pmod h$ für alle $i < j$. Es folgt einerseits $\sum_i r_i^2 = hh'$ mit $0 \neq h' \in k[t]$, wobei $\deg(h') < \deg(h)$ ist. Andererseits hat die rechte Seite in $(**)$ die Form $h^2 q$ mit $q \in k[t]$ sos. Zusammen folgt $fh^2h' = h^2 q$, und Kürzen gibt $fh' = q$. Wegen $\deg(h') < \deg(h)$ ist das ein Widerspruch zur Minimalität von $\deg(h)$. □

3.3 Korollar. *Sei k ein Körper. Ist $f \in k[t]$ eine Quadratsumme in $k(t)$, so auch in $k[t]$.*

Beweis. Wir können annehmen, daß f keine mehrfachen Faktoren in $k[t]$ hat. Nach Voraussetzung gibt es eine Identität $fh^2 = \sum_{i=1}^n g_i^2$ mit Polynomen h, $g_i \neq 0$. Der Leitkoeffizient von f ist also sos in k. Ist f_1 ein gemeinsamer irreduzibler Teiler von f, $g_1, \ldots, g_n$, etwa $f = f_1 \tilde{f}$ und $g_i = f_1 \tilde{g}_i$, so folgt $h = f_1 \tilde{h}$, also

$$f(f_1\tilde{h})^2 \;=\; f_1^2 \sum_i \tilde{g}_i^2,$$

und Kürzen gibt $f\tilde{h}^2 = \sum_i \tilde{g}_i^2$. Induktiv erreichen wir also $\mathrm{ggT}(f, g_1, \ldots, g_n) = 1$. Damit hat jeder normierte irreduzible Faktor f' von f einen nichtreellen Restklassenkörper. Nach Satz 3.2 ist f' sos in $k[t]$. Somit ist f sos in k. □

3.4 Lemma. *Sei B ein diskreter Bewertungsring mit reellem Restklassenkörper. Im Polynomring $B[t]$ gilt dann* psd = sos.

Beweis. Sei $K = \mathrm{Quot}(B)$, und sei π ein Primelement von B. Sei $f \in B[t]$ psd in $B[t]$. Dann ist f auch psd in $K(t)$, und ist daher sos in $K(t)$. Nach Korollar 3.3 ist f auch sos in $K[t]$. Es gibt also $f_1, \ldots, f_r \in B[t]$ und $n \geq 0$ mit $\pi^{2n} f = f_1^2 + \cdots + f_r^2$. Ist $n \geq 1$, so zeigt Reduktion dieser Identität modulo π, daß π die Koeffizienten von jedem f_i teilt, da der Restklassenkörper von B reell ist. Induktiv folgt, daß f in $B[t]$ sos ist. □

3.5 Lemma. *Für $A = k[\![x,y]\!]$ und $F = \mathrm{Quot}(A) = k(\!(x,y)\!)$ gilt $A_+ = A \cap \Sigma F^2$.*

BEWEIS. $\subseteq$ ist klar wegen $F_+ = \Sigma F^2$. Umgekehrt genügt es zu zeigen, daß jeder Punkt $\alpha \in \mathrm{Sper}(A)$ eine Generalisierung mit Träger (0) hat. Dafür genügt, daß für $\mathfrak{p} = \mathrm{supp}(\alpha)$ der lokale Ring $A_\mathfrak{p}$ selbst regulär ist (dann kann man Satz V.2.15 anwenden). Für $\mathfrak{p} = (0)$ bzw. $\mathfrak{p} = \mathfrak{m}$ ist das trivial bzw. klar. Wegen $\dim(A) = 2$ bleibt der Fall $\mathrm{ht}(\mathfrak{p}) = 1$. Wegen A faktoriell ist dann $\mathfrak{p} = (\pi)$ ein Hauptideal und $A_\mathfrak{p}$ ein diskreter Bewertungsring. □

3.6 Beweis von Theorem 3.1. Sei $A = k[\![x,y]\!]$, sei $0 \neq f \in A$ psd. Wir wollen zeigen, daß f sos in A ist. Nach 2.1 können wir $f \in \mathfrak{m}_A$ annehmen. Wegen A faktoriell können wir schreiben $f = f_1 g^2$ mit f_1, $g \in A$, wobei f_1 keinen mehrfachen Faktor enthält. Dabei ist auch f_1 psd in A, nach Lemma 3.5, und es genügt zu zeigen, daß f_1 sos ist.

Also können wir annehmen, daß f in A keinen mehrfachen Faktor enthält. Nach einem Koordinatenwechsel erreichen wir $f = ug$ mit einer Einheit $u \in A^*$ und einem Weierstraßpolynom $g \in k[\![x]\!][y]$ (Vorbereitungssatz). Setze $B := k[\![x]\!]$ und $K = k(\!(x)\!)$, und schreibe $g = p_1 \cdots p_r$ als Produkt von irreduziblen Faktoren p_i in $B[y]$. Wir können annehmen, daß die p_i normiert in y sind, dann sind die p_i selbst Weierstraßpolynome in y. Es gilt $B[y]/(p_i) \cong A/(p_i)$ für alle i (Korollar V.5.8), also sind die p_i auch irreduzibel in A.

Für jeden Index i ist der Restklassenkörper $\mathrm{Quot}(A/(p_i))$ von p_i nichtreell. Denn sei o.E. $i = 1$, angenommen, es gibt $\alpha \in \mathrm{Sper}(A)$ mit $\mathrm{supp}(\alpha) = (p_1)$. Da $A_{(p_1)}$ ein diskreter Bewertungsring ist, gibt es dann nach dem Satz von Baer-Krull (II.5.8) Anordnungen α_1, $\alpha_2 \in \mathrm{Sper}(A)$ mit $\mathrm{supp}(\alpha_j) = (0)$, mit $\alpha_j \rightsquigarrow \alpha$ $(j = 1, 2)$, und mit $p_1(\alpha_1) > 0$, $p_1(\alpha_2) < 0$. Wegen $f = up_1 \cdots p_r$ psd muß einer der Faktoren $u, p_2, \ldots, p_r$ in α_1 und α_2 verschiedene Vorzeichen haben. Dann ist dieser Faktor aber durch p_1 teilbar, Widerspruch.

Für $i = 1, \ldots, r$ ist $K[y]/(p_i)$ der Quotientenkörper von $B[y]/(p_i) \cong A/(p_i)$. Da dieser Körper nichtreell und $p_i \in B[y]$ normiert ist, ist p_i sos in $K[y]$ nach Satz 3.2. Nach Lemma 3.4 ist p_i also auch sos in $B[y]$. Insbesondere sind die p_i sos in A. Wegen $f = up_1 \ldots p_r$, und nochmals wegen Lemma 3.5, ist u psd in A, also auch sos. Somit ist f sos in A. □

3.7 Korollar. *Ist R ein reell abgeschlossener Körper, so ist jedes psd Element in $R[\![x,y]\!]$ Summe von zwei Quadraten in diesem Ring.*

BEWEIS. Jede psd Einheit in $A = R[\![x,y]\!]$ ist ein Quadrat in A. Nach dem Beweis 3.6 können wir annehmen (mit $B = R[\![x]\!]$ und $K = R(\!(x)\!)$): $f \in B[y]$ ist irreduzibel und normiert und ist sos in $B[y]$. Zu zeigen ist, daß f Summe von zwei Quadraten ist. Der Körper $K[y]/(f) = \mathrm{Quot}(B[y]/(f))$ ist eine nichtreelle endliche Erweiterung von K, enthält also $i = \sqrt{-1}$ nach Aufgabe 29. Also gibt es $p, q \in B[y]$ mit $f \nmid pq$ und $f \mid p^2 + q^2$. Behaupte, f ist reduzibel in $B[i,y]$. Denn wegen $f \mid (p+iq)(p-iq)$ würde sonst etwa folgen $f \mid p + iq$ in $B[i,y]$, also $f \mid p$ und $f \mid q$ in $B[y]$, Widerspruch. Es folgt $f = u(g+ig')(g-ig')$ mit $g, g' \in B[y]$ und $u \in B^*$, also $f = u(g^2 + g'^2)$ (und u ist ein Quadrat). □

Wir dehnen Theorem 3.1 von Potenzreihenringen auf beliebige 2-dimensionale reguläre lokale Ringe aus:

3.8 Theorem. *Sei A ein regulärer lokaler Ring mit* $\dim(A) \leq 2$. *Dann gilt* psd = sos *in A.*

BEWEIS. (Skizze) Der Fall $\dim(A) = 1$ wurde schon bewiesen (Korollar 2.14), sei $\dim(A) = 2$. Jeder reguläre lokale Ring ist faktoriell (Satz von Auslander-Buchsbaum, ohne Beweis). Sei $f \in A$ psd. Wie in 3.6 können wir annehmen, daß f keine mehrfachen Faktoren hat (brauche dabei die zu Lemma 3.5 analoge Aussage, Beweis wie dort). Wie in 3.6 folgt daraus $\mathfrak{m} \subseteq \sqrt[\mathrm{re}]{(f)}$. Nach Theorem 2.11 genügt es zu zeigen, daß f in $\widehat{A}$ sos ist. Ist $k = A/\mathfrak{m}$ nicht reell, so ist $\mathrm{Sper}(\widehat{A}) = \varnothing$ (Aufgabe 24), also ist dann jedes Element in $\widehat{A}$ sos. Ist k reell, so ist $\widehat{A} \cong k[\![x, y]\!]$ (Theorem V.4.32, wir haben das nur im Fall $k \subseteq A$ bewiesen). In $\widehat{A}$ gilt also psd = sos (Theorem 3.1), und wir sind fertig. □

Auch für gewisse Präordnungen in A zeigen wir die Saturiertheit. Dazu als Vorbereitung:

3.9 Satz. *Sei A ein regulärer lokaler Ring mit $\dim(A) = d$, sei $u \in A^*$, und sei $B = A[x]/(x^2 - u)$. Dann ist B ein semilokaler Ring mit höchstens zwei maximalen Idealen, und für jedes $\mathfrak{q} \in \mathrm{Max}(B)$ ist $B_{\mathfrak{q}}$ regulär von Dimension d.*

BEWEIS. Sei $K = \mathrm{Quot}(A)$ und $k = A/\mathfrak{m}_A$. Zunächst sei $u \in K^{*2}$, etwa $u = a^2$. Dann ist $a \in A^*$ (wegen A faktoriell ist A ganz abgeschlossen). Die beiden Hauptideale $(x + a)$ und $(x - a)$ von $A[x]$ sind relativ prim, also ist

$$B \;=\; A[x]/(x^2 - a^2) \;\cong\; \frac{A[x]}{(x-a)} \times \frac{A[x]}{(x+a)} \;\cong\; A \times A$$

(Chinesischer Restsatz). Jetzt sei $u \notin K^{*2}$. Da $A \subseteq B$ eine endliche Ringerweiterung ist, ist $\dim(A) = \dim(B)$, und jedes maximale Ideal von B liegt über $\mathfrak{m}_A$. Es ist

$$B/\mathfrak{m}_A B \;\cong\; k[x]/(x^2 - \overline{u}).$$

Ist $\overline{u} \notin k^{*2}$, so ist $B/\mathfrak{m}_A B$ ein Körper. Also ist dann B ein lokaler Ring, und Erzeuger des Ideals $\mathfrak{m}_A$ in A erzeugen auch das Ideal $\mathfrak{m}_B$ in B. Es bleibt der Fall $u \equiv a^2 \pmod{\mathfrak{m}_A}$ mit $a \in A^*$. Dann hat B zwei maximale Ideale, nämlich $\mathfrak{q}_1 = \mathfrak{m}_A B + (x-a)B$ und $\mathfrak{q}_2 = \mathfrak{m}_A B + (x+a)B$. Wegen $u - (a+y)^2 = u - a^2 - y(2a+y)$ können wir a modulo $\mathfrak{m}_A$ so abändern, daß $u - a^2 = b \notin \mathfrak{m}_A^2$ ist. Dann gibt es $b_2, \ldots, b_d \in \mathfrak{m}_A$ mit $\mathfrak{m}_A = (b, b_2, \ldots, b_d)$ (Satz V.2.11). In B gilt $b = x^2 - a^2$. Also werden $\mathfrak{q}_1 = (x - a, b_2, \ldots, b_d)$ und $\mathfrak{q}_2 = (x + a, b_2, \ldots, b_d)$ von jeweils d Elementen erzeugt. Andererseits haben $\mathfrak{q}_{1,2}$ in B beide Höhe $\geq d$, nach Going-down V.3.5. Also sind $B_{\mathfrak{q}_1}$, $B_{\mathfrak{q}_2}$ beide regulär von Dimension d. □

Ein entsprechendes Resultat gilt auch allgemeiner für

$$B \;=\; A[x_1, \ldots, x_r]/(x_i^2 - u_i \colon\; i = 1, \ldots, r),$$

wobei $u_1, \ldots, u_r$ Einheiten in A sind.

3.10 Satz. *Ist A ein regulärer lokaler Ring, $\dim(A) \leq 2$, und ist $u \in A^*$, so ist die Präordnung $PO_A(u)$ in A saturiert.*

BEWEIS. $B = A[x]/(x^2 - u)$ ist ein semilokaler Ring, und es gilt psd = sos in $B_{\mathfrak{q}}$ für jedes $\mathfrak{q} \in \mathrm{Max}(B)$ (Satz 3.9, Theorem 3.8). Nach Satz 2.2 gilt also psd = sos in B. Sei $T = PO_A(u)$, sei $f \in \mathrm{Sat}(T)$. Dann ist f psd, und damit sos, in B. Gemäß Lemma 2.4 folgt daraus $f \in T$. □

Mit demselben Argument zeigt man, daß $PO_A(u_1, \ldots, u_r)$ saturiert ist für beliebige Einheiten $u_1, \ldots, u_r$ in A (unter Benutzung der erwähnten Verallgemeinerung von 3.9).

3.11 Korollar. *Sei A ein regulärer lokaler Ring mit $\dim(A) = 2$, seien a, $b \in A$ mit $(a, b) = \mathfrak{m}$. Dann sind die Präordnungen $PO(a)$ und $PO(a, b)$ in A saturiert.*

BEWEIS. Die Ringe $B = A[x]/(x^2 - a)$ und $C = A[x, y]/(x^2 - a,\ y^2 - b)$ sind wieder regulär lokal von Dimension 2 (Aufgabe 40). Nach 3.8 gilt psd = sos in B und in C. Sei $T = PO(a)$, sei $f \in \mathrm{Sat}(T)$. Dann ist f psd, und damit sos, in B. Gemäß Lemma 2.4 folgt daraus $f \in T$. Ganz genauso zeigt man, daß $PO(a, b)$ saturiert ist. □

Die zu Korollar 3.11 analoge Aussage für eindimensionale reguläre lokale Ringe (also diskrete Bewertungsringe) wurde in Aufgabe 39 bewiesen.

4. Globale Resultate

Wir beweisen nun globale Nichtnegativstellensätze, indem wir sie auf lokale solche Aussagen zurückführen. Erreicht wird das durch das archimedische Lokal-global Prinzip, das erste Hauptresultat in diesem Abschnitt.

Im folgenden sei A ein beliebiger Ring.

4.1 Eine (abgeschlossene) Teilmenge $X \subseteq \mathrm{Sper}(A)$ heißt *probasisch*, falls es eine Präordnung T in A gibt mit $X = X(T)$ (also falls X ein Durchschnitt von Mengen $\{f_i \geq 0\}$ mit $f_i \in A$ ist). Wir nennen X *beschränkt*, falls zu jedem $f \in A$ ein $N \in \mathbb{N}$ existiert mit $N \pm f \geq 0$ auf X. Anders gesagt, falls die saturierte Präordnung $\mathcal{P}(X)$ archimedisch ist.

4.2 Bemerkung. Ist $X \subseteq \mathrm{Sper}(A)$ eine probasische beschränkte Menge, so ist für jedes $\alpha \in X^{\max}$ der angeordnete Restklassenkörper $\kappa(\alpha)$ archimedisch. Denn $\kappa(\alpha)$ ist relativ archimedisch über A (Satz II.5.15). Man hat den kanonischen Ringhomomorphismus $\Phi\colon A \to C(X^{\max}, \mathbb{R})$, siehe IV.5.16, und $\Phi(A)$ ist ein dichter Teilring von $C(X^{\max}, \mathbb{R})$ (siehe IV.6.12).

Denn sei $M = \mathcal{P}(X)$, also $X = X(M)$. Wegen M archimedisch identifiziert sich $X^{\max} = X(M)^{\max}$ mit $X_M = \{\alpha \in \mathrm{Hom}(A, \mathbb{R})\colon \alpha|_M \geq 0\}$ (Satz IV.5.18). Dabei wird $\Phi\colon X_M \to C(X_M, \mathbb{R})$ die Abbildung $f \mapsto \widehat{f}$ mit $\widehat{f}(\alpha) = \alpha(f)$. Daraus ist klar, daß $\Phi(A)$ die Punkte von $X^{\max}$ trennt.

4.3 Lemma. *Sei X eine probasische beschränkte Teilmenge von $\mathrm{Sper}(A)$, und seien a, $b \in A$ mit $a \geq 0$ auf X und $b < 0$ auf $X \cap Z(a)$. Dann gibt es ein $N \in \mathbb{N}$ mit $Na > b$ auf X.*

BEWEIS. Sei $Y := X \cap \{b \geq 0\}$, und sei $T = \mathcal{P}(Y)$. Nach Voraussetzung gilt $a > 0$ auf $Y = X_T$. Nach dem Positivstellensatz (II.2.7) gibt es $s, t \in T$ mit $as = 1 + t$. Wegen X beschränkt gibt es $m, n \in \mathbb{N}$ mit $m > b$ und $n > s$ auf Y. Dann folgt $mna > mas \geq m > b$ auf Y. Also gilt $mna > b$ auch auf X. □

4.4 Lemma. *Sei $X \subseteq \mathrm{Sper}(A)$ eine beschränkte und probasische Teilmenge von $\mathrm{Sper}(A)$. Seien f, $g \in A$ mit $f \geq 0$ und $g \geq 0$ auf X. Für jedes $h \in Af + Ag$ mit $h > 0$ auf X gibt es dann s, $t \in A$ mit $sf + tg = h$ und mit $s > 0$, $t > 0$ auf X.*

BEWEIS. Seien a, $b \in A$ mit $af + bg = h$. Es gilt $a > 0$ auf $X \cap Z(g)$ und $b > 0$ auf $X \cap Z(f)$. Mit 4.3 finden wir also N_1, $N_2 \in \mathbb{N}$ mit $N_1 g > -a$ und $N_2 f > -b$ auf X. Auf dem kompakten topologischen Raum $X^{\max}$ definieren wir stetige $\mathbb{R}$-wertige Funktionen φ, ψ (punktweise) durch

$$\varphi := \max\Big\{-N_1,\ -\frac{b}{f}\Big\} \quad \text{bzw.} \quad \psi := \min\Big\{N_2,\ \frac{a}{g}\Big\}$$

(außerhalb $Z(f)$ bzw. $Z(g)$), und durch $\varphi \equiv -N_1$ auf $X^{\max} \cap Z(f)$ bzw. $\psi \equiv N_2$ auf $X^{\max} \cap Z(g)$. Dies ist tatsächlich wohldefiniert. Denn $U := \{b > N_1 f\}$ ist eine offene Umgebung von $X \cap Z(f)$. Auf $(U \cap X^{\max}) \setminus Z(f)$ ist $-\frac{b}{f} < -N_1$, dort ist also $\varphi = -N_1$. Analog für ψ: Die Menge $V := \{N_2 g < a\}$ ist eine offene Umgebung von $X \cap Z(g)$. Auf $(V \cap X^{\max}) \setminus Z(g)$ ist $\frac{a}{g} > N_2$, dort ist also $\psi = N_2$.

Auf $X^{\max}$ gilt (punktweise) $\varphi < \psi$. Denn $-N_1 < \frac{a}{g}$ und $-\frac{b}{f} < N_2$ gelten nach Wahl von N_1, N_2 dort, wo die Nenner nicht verschwinden; und $-\frac{b}{f} < \frac{a}{g}$ gilt dort wegen $h > 0$. Auf $X^{\max} \cap Z(f)$ ist $\varphi = -N_1$, auf $X^{\max} \cap Z(g)$ ist $\psi = N_2$, also gilt $\varphi < \psi$ auch dort. Nach Stone-Weierstraß (vergleiche 4.2) gibt es also ein $c \in A$ mit $(-\frac{b}{f} \leq) \varphi < c < \psi (\leq \frac{a}{g})$ auf $X^{\max}$. Daraus folgen

$$-b \ < \ cf \quad \text{und} \quad cg \ < \ a$$

auf $X^{\max}$, also auch auf X. Für $s := a - cg$ und $t := b + cf \in A$ gelten also $s, t > 0$ auf X und $sf + tg = h$. □

4.5 Satz. *Sei A ein Ring, und sei $X \subseteq \mathrm{Sper}(A)$ eine beschränkte probasische Teilmenge von $\mathrm{Sper}(A)$. Seien $f_1, \ldots, f_r \in A$ mit $f_i \geq 0$ auf X, und sei $h \in Af_1 + \cdots + Af_r$ mit $h > 0$ auf X. Dann gibt es $a_1, \ldots, a_r \in A$ mit*

$$a_1 f_1 + \cdots + a_r f_r \ = \ h$$

und mit $a_i > 0$ auf X $(i = 1, \ldots, r)$.

Beweis. Der Fall $r = 1$ ist trivial, und $r = 2$ ist Lemma 4.4. Sei $r > 2$, und sei der Satz schon für $r - 1$ bewiesen. Setze $\overline{A} = A/(f_r)$ und $\overline{f}_i = f_i + (f_r)$ $(i = 1, \ldots, r-1)$. Die probasische Teilmenge $\overline{X} := X \cap Z(f_r)$ von $\mathrm{Sper}(\overline{A})$ ist beschränkt. Nach Induktionsannahme gibt es $b_1, \ldots, b_{r-1} \in A$ mit $b_i > 0$ auf $X \cap Z(f_r)$ und mit

$$b_1 f_1 + \cdots + b_{r-1} f_{r-1} \ \equiv \ h \pmod{(f_r)}.$$

Nach Korollar 1.20 gibt es $c_1, \ldots, c_{r-1} \in A$ mit $c_i \equiv b_i \bmod (f_r)$ und mit $c_i > 0$ auf X $(i = 1, \ldots, r-1)$. Setze $f := \sum_{i=1}^{r-1} c_i f_i$ und $g := f_r$. Dann sind $f, g \geq 0$ auf X, und es ist $h \in Af + Ag$. Anwendung von Lemma 4.4 auf f und g gibt $s, t \in A$ mit $s > 0$, $t > 0$ auf X und mit $h = sf + tg$. Daraus folgt die Behauptung. □

4.6 Theorem. (Archimedisches Lokal-global Prinzip) *Sei A ein Ring, und sei M ein Modul über einer archimedischen Präordnung T in A. Sei $f \in A$. Für jedes maximale Ideal $\mathfrak{m}$ von A mit $\mathrm{supp}(M) \subseteq \mathfrak{m}$ gelte $f \in M_{\mathfrak{m}}$. Dann ist $f \in M$.*

Beweis. Ist $\mathfrak{p}$ ein Primideal von A mit $\mathrm{supp}(M) \not\subseteq \mathfrak{p}$, so gilt $M_{\mathfrak{p}} = A_{\mathfrak{p}}$. Denn sei $s \in \mathrm{supp}(M)$ mit $s \notin \mathfrak{p}$. Da $\mathrm{supp}(M)$ ein Ideal von A ist, gilt $-s^2 \in M$, und daher ist $-1 \in M_{\mathfrak{p}}$, also $M_{\mathfrak{p}} = A_{\mathfrak{p}}$.

Daher gilt $f \in M_{\mathfrak{m}}$ für jedes maximale Ideal $\mathfrak{m}$ von A. Zu jedem $\mathfrak{m} \in \mathrm{Max}(A)$ gibt es also ein $s \in A \setminus \mathfrak{m}$ mit $s^2 f \in M$. Daher gibt es endlich viele Elemente $s_1, \ldots, s_r \in A$ mit $(s_1, \ldots, s_r) = (1)$, also auch $(s_1^2, \ldots, s_r^2) = (1)$, und mit $s_i^2 f \in M$ für jedes i. Die Menge $X(T) \subseteq \mathrm{Sper}(A)$ ist beschränkt wegen T archimedisch. Nach Satz 4.5 gibt es also $a_1, \ldots, a_r \in A$ mit $\sum_{i=1}^{r} a_i s_i^2 = 1$ und mit $a_i > 0$ auf $X(T)$ für $i = 1, \ldots, r$. Nach dem archimedischen Positivstellensatz gilt $a_i \in T$ für alle i. Somit liegt $f = \sum_{i=1}^{r} a_i s_i^2 f$ in M. □

Für Präordnungen kann man noch schärfer formulieren:

4.7 Theorem. *Sei T eine archimedische Präordnung von A. Sei $f \in \mathrm{Sat}(T)$, und es gelte $f \in T_{\mathfrak{m}}$ für jedes maximale Ideal $\mathfrak{m}$ von A mit $\mathrm{supp}(T + Af) \subseteq \mathfrak{m}$. Dann ist $f \in T$.*

BEWEIS. Wegen Theorem 4.6 genügt es, für jedes maximale Ideal $\mathfrak{m}$ von A mit $\operatorname{supp}(T+Af) \not\subseteq \mathfrak{m}$ zu zeigen $f \in T_{\mathfrak{m}}$. Es gilt jedenfalls $f \in \operatorname{Sat}_{A_{\mathfrak{m}}}(T_{\mathfrak{m}})$. Ist $f \notin \mathfrak{m}$, so ist $f \in (A_{\mathfrak{m}})^*$, und daher $f \in T_{\mathfrak{m}}$ nach Satz 2.5. Sei also $f \in \mathfrak{m}$. Nach Voraussetzung gibt es $t_i \in T$, $a_i \in A$ $(i = 1, 2)$ mit $t_1 + a_1 f = -t_2 + a_2 f \notin \mathfrak{m}$. Es gilt t_1, $t_2 \in A_{\mathfrak{m}}^*$, und aus $t_1 + t_2 = (a_2 - a_1)f$ und $f \in \operatorname{Sat}_{A_{\mathfrak{m}}}(T_{\mathfrak{m}})$ folgt auch $f > 0$ auf $X_{A_{\mathfrak{m}}}(T_{\mathfrak{m}})$. Nach Korollar 2.7 folgt $f \in T_{\mathfrak{m}}$. □

4.8 Korollar. *Sei T eine archimedische Präordnung in A. Ist $T_{\mathfrak{m}}$ saturiert (in $A_{\mathfrak{m}}$) für jedes maximale Ideal $\mathfrak{m}$ von A mit $\operatorname{supp}(T) \subseteq \mathfrak{m}$, so ist T saturiert.*

Die Umkehrung gilt auch ohne jede archimedische Voraussetzung (Satz 1.12).

BEWEIS. Ist $f \in \operatorname{Sat}(T)$, so ist auch $f \in \operatorname{Sat}(T_{\mathfrak{m}})$ für alle $\mathfrak{m}$. Die Aussage folgt also aus 4.7. □

Einige geometrische Anwendungen:

4.9 Korollar. *Sei V eine nichtsinguläre affine $\mathbb{R}$-Varietät mit $V(\mathbb{R})$ kompakt und mit $\dim(V) \leq 2$. Dann gilt $\operatorname{psd} = \operatorname{sos}$ in $\mathbb{R}[V]$.*

Die Aussage für Dimension 2 ist bemerkenswert im Hinblick auf $\operatorname{psd} \neq \operatorname{sos}$ in $\mathbb{R}[x, y]$ (Hilbert).

BEWEIS. Die Präordnung $T = \Sigma\mathbb{R}[V]^2$ in $\mathbb{R}[V]$ ist archimedisch nach Schmüdgen. Ist $\mathfrak{m}$ ein maximales Ideal in $\mathbb{R}[V]$, so ist $\mathbb{R}[V]_{\mathfrak{m}}$ ein regulärer lokaler Ring von Dimension ≤ 2. Nach Korollar 3.8 gilt also $\operatorname{psd} = \operatorname{sos}$ in $\mathbb{R}[V]_{\mathfrak{m}}$. Die Behauptung folgt also aus Korollar 4.8. □

4.10 Satz. *Sei V eine affine $\mathbb{R}$-Varietät, sei $T \subseteq \mathbb{R}[V]$ eine endlich erzeugte Präordnung und $K = S(T)$, und sei $f \in \mathbb{R}[V]$ mit $f \geq 0$ auf K. Ist K kompakt und $Z(f) \cap K$ endlich, und ist $f \in \widehat{T}_{\xi}$ für alle $\xi \in Z(f) \cap K$, so ist $f \in T$.*

BEWEIS. Nach Schmüdgen ist T archimedisch. Gemäß Theorem 4.7 genügt es deshalb, für jedes maximale Ideal $\mathfrak{m}$ von $\mathbb{R}[V]$ mit $\operatorname{supp}(T + (f)) \subseteq \mathfrak{m}$ zu zeigen, daß $f \in T_{\mathfrak{m}}$ ist.

Die Nullstellenvarietät von $\operatorname{supp}(T + (f))$ ist der Zariskiabschluß von $Z(f) \cap K$ in V. Wegen $|Z(f) \cap K| < \infty$ ist dieser Zariskiabschluß gleich $K \cap Z(f)$. Also genügt es, für jedes $\xi \in Z(f) \cap K$ zu zeigen, daß $f \in T_{\mathfrak{m}_\xi}$ ist. Nach Voraussetzung gilt $f \in \widehat{T}_{\mathfrak{m}_\xi}$. Aus 2.11 folgt also $f \in T_{\mathfrak{m}_\xi}$. □

4.11 Korollar. *Sei $T \subseteq \mathbb{R}[x_1, \ldots, x_n]$ eine endlich erzeugte Präordnung, und sei $K = S(T)$ kompakt. Sei $f \in \mathbb{R}[\mathtt{x}]$ mit $f \geq 0$ auf K derart, daß für jedes $\xi \in Z(f) \cap K$ die Hessematrix $D^2 f(\xi) = \left(\partial^2 f(\xi)/\partial x_i\, \partial x_j\right)$ positiv definit ist. Dann ist $f \in T$.*

BEWEIS. Nach Aufgabe 36 ist f sos in $\widehat{\mathbb{R}[\mathtt{x}]_{\mathfrak{m}_\xi}}$ für alle $\xi \in Z(f) \cap K$. Die Menge $Z(f) \cap K$ ist endlich, denn die Nullstellen von f in K sind isoliert. Die Aussage folgt also aus Satz 4.10. □

4.12 Bemerkung. Sei $f \in \mathbb{R}[\mathtt{x}]$, sei $r > 0$ und $g = r^2 - \sum_{i=1}^n x_i^2$, sowie $T = PO(g) \subseteq \mathbb{R}[\mathtt{x}]$. Sei $f_* := \min\{f(\xi) \colon |\xi| \leq r\}$. Für alle $a \in \mathbb{R}$ mit $a < f_*$ gibt es eine Identität

$$f - a \;=\; \sum_i p_i^2 + g \sum_j q_j^2 \qquad (*)$$

mit p_i, $q_j \in \mathbb{R}[\mathbf{x}]$ (archimedischer Positivstellensatz). Beschränkt man die $\deg(p_i)$ und $\deg(q_j)$, so kann man mit semidefiniter Programmierung das sup aller $a \in \mathbb{R}$ finden, für die eine Identität $(*)$ mit den gegebenen Gradschranken existiert. Dieses Supremum ist eine untere Schranke für f_*. Ist $f - f_* \notin T$, so gehen die Grade der p_i, q_j für $a \nearrow f_*$ notwendig gegen ∞. Ist dagegen $f - f_* \in T$, so lassen sich die Grade der p_i, q_j für alle $a \leq f_*$ uniform beschränken. Nach 4.11 tritt der letztere Fall ein, falls $f - f_*$ in allen Nullstellen in $K = B_r(0)$ positiv definite Hessesche hat. Unter der Voraussetzung $f|_{\partial K} > f_*$ kann man zeigen, daß diese Bedingung für generische Wahl von f erfüllt ist.

4.13 Satz. *Seien $p_1, \ldots, p_r \in \mathbb{R}[x, y]$ irreduzibel, sei $K = S(p_1, \ldots, p_r) \subseteq \mathbb{R}^2$ kompakt. Es gelte:*

(1) *Für $i = 1, \ldots, r$ und alle $\xi \in K$ mit $p_i(\xi) = 0$ ist $\nabla p_i(\xi) \neq 0$;*
(2) *ist auch $p_j(\xi) = 0$ mit $j \neq i$, so sind $\nabla p_i(\xi)$ und $\nabla p_j(\xi)$ linear unabhängig;*
(3) *$K \cap Z(p_i, p_j, p_k) = \varnothing$ für je drei verschiedene Indices i, j, k.*

Dann ist $PO(p_1, \ldots, p_r) = \mathcal{P}(K)$, d.h. die Präordnung $PO(p_1, \ldots, p_r)$ in $\mathbb{R}[x, y]$ ist saturiert.

Beispiele sind kompakte Polygone, oder allgemeiner kompakte basisch abgeschlossene Mengen $K \subseteq \mathbb{R}^2$, die durch glatte Randkurven mit transversalen Schnitten begrenzt werden (keine drei durch denselben Randpunkt).

Beweis. Sei $T = PO(p_1, \ldots, p_r)$, es ist $\mathrm{Sat}(T) = \mathcal{P}(K)$. Für alle $\xi \in \partial K$ gibt es $t \leq 2$ Polynome $f_1, \ldots, f_t$ mit $f_i(\xi) = 0$ und mit $\nabla f_1(\xi), \ldots, \nabla f_t(\xi)$ linear unabhängig, so daß $U \cap K = U \cap \{f_1 \geq 0, \ldots, f_t \geq 0\}$ für eine Umgebung U von ξ gilt. Insbesondere ist $\dim_\xi(K) = 2$. Daraus folgt: Sind $f \in \mathbb{R}[x, y]$ und $0 \neq g \in T$, und ist $fg \in \mathcal{P}(K)$, so ist auch $f \in \mathcal{P}(K)$.

Sei $f \in \mathcal{P}(K)$, zu zeigen ist $f \in T$. Nach eben können wir annehmen, daß f nicht durch ein Quadrat und nicht durch eines der p_i teilbar ist. Daraus folgt $|Z(f) \cap K| < \infty$. Nach 4.10 genügt es, $f \in \widehat{T}_\xi$ für alle $\xi \in Z(f) \cap K$ zu zeigen. Sei also $\xi \in Z(f) \cap K$. Nach Umnumerieren der p_i gibt es $0 \leq t \leq 2$ mit $p_i(\xi) = 0$ für $1 \leq i \leq t$ und $p_i(\xi) > 0$ für $t + 1 \leq i \leq r$. Dabei sind die $\nabla p_i(\xi)$ $(1 \leq i \leq t)$ linear unabhängig. Nach Korollar 3.11 ist $\widehat{T}_\xi$ saturiert, und der Beweis ist beendet. □

KAPITEL VII

Einige Anwendungen von Quadratsummen

1. Lokalkonvexe Vektorräume

1.1 Definition. Ein *topologischer Vektorraum* (über $\mathbb{R}$) ist ein $\mathbb{R}$-Vektorraum V mit einer Hausdorff-Topologie derart, daß Addition $V \times V \to V$ und Skalarmultiplikation $\mathbb{R} \times V \to V$ stetige Abbildungen sind. Den Vektorraum aller stetigen Linearformen $V \to \mathbb{R}$ auf V bezeichnen wir mit V'.

1.2 Beispiel. Eine Vektorraumnorm auf dem $\mathbb{R}$-Vektorraum V ist eine Abbildung $V \to \mathbb{R}$, $x \mapsto ||x||$, welche $||x|| > 0$ für $x \neq 0$, $||x+y|| \leq ||x|| + ||y||$ und $||ax|| = |a| \cdot ||x||$ für alle $a \in \mathbb{R}$ und $x, y \in V$ erfüllt. Durch $d(x,y) = ||x-y||$ wird eine Metrik auf V definiert, welche V zu einem topologischen Vektorraum macht. Ein *normierter Vektorraum* ist ein $\mathbb{R}$-Vektorraum V zusammen mit einer Vektorraumnorm.

1.3 Lemma. *Ist* $\dim(V) < \infty$*, so gibt es nur eine Vektorraumtopologie auf* V*.*

Beweis. Übung. □

1.4 Sei V ein $\mathbb{R}$-Vektorraum. Eine Teilmenge $K \subseteq V$ heißt *konvex*, wenn für alle $x, y \in K$ und alle $0 \leq t \leq 1$ gilt $(1-t)x + ty \in K$. Gilt zusätzlich $tK \subseteq K$ für alle $t \geq 0$ und $K \neq \varnothing$, so heißt K ein *konvexer Kegel*. Die konvexe Hülle $\mathrm{conv}(M)$ von $M \subseteq V$ ist der Durchschnitt aller konvexen Obermengen von M und besteht aus allen Konvexkombinationen $\sum_{i=1}^{n} a_i x_i$ mit $n \in \mathbb{N}$, $x_i \in K$, $a_i \geq 0$ mit $\sum_i a_i = 1$. Nun habe V eine Vektorraumtopologie. Ist $K \subseteq V$ konvex, so auch $\overline{K}$ (Übung). Für jede Teilmenge $M \subseteq V$ ist

$$M^* := \{L \in V' \colon L|_M \geq 0\}$$

ein konvexer Kegel in V'.

1.5 Definition. Ein topologischer Vektorraum V heißt *lokalkonvex*, falls es in V eine 0-Umgebungsbasis aus konvexen Mengen gibt.

Zum Beispiel ist jeder normierte Vektorraum lokalkonvex (die offenen Kugeln $B_r(0)$ sind konvex). Der wichtigste Satz über lokalkonvexe Vektorräume ist der Trennungssatz:

1.6 Theorem. (Hahn-Banach) *Sei V ein lokalkonvexer Vektorraum, seien A, B disjunkte konvexe Teilmengen von V mit A kompakt und B abgeschlossen. Dann gibt es eine stetige Linearform $L \in V'$ und ein $c \in \mathbb{R}$ mit $L(b) < c < L(a)$ für alle $a \in A$, $b \in B$.*

(Beweis siehe jedes Buch über Funktionalanalysis) Sei V lokalkonvex. Hier sind direkte Folgerungen:

1.7 Korollar. *Sei $K \subseteq V$ eine konvexe Teilmenge. Dann ist $\overline{K}$ ein Durchschnitt von abgeschlossenen Halbräumen $\{x \in V : L(x) \geq c\}$ (mit $L \in V'$ und $c \in \mathbb{R}$).*

BEWEIS. $\overline{K}$ ist konvex in V. Nach Hahn-Banach gibt es zu jedem $x \in V \setminus \overline{K}$ ein $L \in V'$ und ein $c \in \mathbb{R}$ mit $L|_{\overline{K}} \geq c > L(x)$. □

1.8 Korollar. *Sei $C \subseteq V$ ein konvexer Kegel, sei $C^{**} := \{x \in V : \forall\, L \in C^* \; L(x) \geq 0\}$. Dann ist $C^* = (\overline{C})^*$ und $C^{**} = \overline{C}$.*

BEWEIS. Wegen C^{**} abgeschlossen konvex und $C \subseteq C^{**}$ ist $\overline{C} \subseteq C^{**}$. Ist $L \in V'$ und $a \in \mathbb{R}$ mit $L|_C \geq a$, so ist $a \leq 0$ und $L|_C \geq 0$. Also folgt $C^{**} \subseteq \overline{C}$. □

1.9 Satz. *Sei V ein $\mathbb{R}$-Vektorraum mit einer höchstens abzählbaren linearen Basis. Sei τ die wie folgt auf V definierte Topologie: Eine Teilmenge $X \subseteq V$ ist τ-abgeschlossen, wenn $X \cap W$ abgeschlossen in W ist für jeden endlich-dimensionalen Unterraum $W \subseteq V$. Dann gilt:*

(a) *τ ist eine Vektorraumtopologie auf V, und ist feiner als jede andere Vektorraumtopologie auf V;*
(b) *τ ist lokalkonvex.*

Wir nennen τ die kanonische Topologie *auf V.*

1.10 Lemma. *Seien X, Y Hausdorffräume, sei $W \subseteq X \times Y$ eine offene Menge, sei $y \in Y$, und sei $K \subseteq X$ eine kompakte Teilmenge mit $K \times \{y\} \subseteq W$. Dann gibt es eine Umgebung V von y in Y mit $K \times V \subseteq W$. (Übung)*

BEWEIS VON SATZ 1.9. Kann annehmen, daß V eine lineare Basis $(v_n)_{n\geq 1}$ hat. Sei U eine τ-offene 0-Umgebung in V. Konstruieren induktiv eine Folge $(\varepsilon_n)_{n\geq 1}$ positiver reeller Zahlen. Wähle $\varepsilon_1 > 0$ mit $a_1 v_1 \in U$ für alle $|a_1| \leq \varepsilon_1$. Seien $\varepsilon_1, \ldots, \varepsilon_n > 0$ schon konstruiert mit $\sum_{i=1}^n a_i v_i \in U$ für alle $a = (a_1, \ldots, a_n) \in \prod_{i=1}^n [-\varepsilon_i, \varepsilon_i] \subseteq \mathbb{R}^n$. Nach 1.10 gibt es ein $\varepsilon_{n+1} > 0$ mit $\sum_{i=1}^{n+1} a_i v_i \in U$ für alle $(a_1, \ldots, a_{n+1}) \in \prod_{i=1}^{n+1} [-\varepsilon_i, \varepsilon_i] \subseteq \mathbb{R}^{n+1}$. Sei $\varepsilon = (\varepsilon_n)_{n\geq 1}$ die so konstruierte Folge, und sei

$$B(\varepsilon) := \Big\{ \sum_{n\geq 1} a_n v_n : \forall\, n \geq 1 \; |a_n| < \varepsilon_n,\; a_n = 0 \text{ für fast alle } n \Big\}.$$

Für jeden Unterraum $W \subseteq V$ mit $\dim(W) < \infty$ ist $B(\varepsilon) \cap W$ offen in W, denn $W \subseteq \operatorname{span}(v_1, \ldots, v_n)$ für ein $n \in \mathbb{N}$. Also ist $B(\varepsilon)$ eine τ-offene und konvexe 0-Umgebung in V. Nach Konstruktion gilt $B(\varepsilon) \subseteq U$.

Die Mengen der Form $B(\varepsilon)$, wo $\varepsilon = (\varepsilon_n)_n$ eine Folge positiver reeller Zahlen ist, bilden also eine 0-Umgebungsbasis für die Topologie τ. Damit folgt, daß τ eine Vektorraumtopologie auf V ist (Aufgabe 43). Da die Mengen $B(\varepsilon)$ konvex in V sind, ist τ lokalkonvex.

Ist τ' eine beliebige Vektorraumtopologie auf V, so ist $\tau' \subseteq \tau$. Denn ist $U \subseteq V$ τ'-offen, so ist $U \cap W$ offen in W für jeden Unterraum W von V mit $\dim(W) < \infty$, und somit ist U τ-offen nach Definition von τ. □

1.11 Korollar. *Sei $\dim(V)$ höchstens abzählbar, sei V versehen mit der kanonischen Topologie.*

(a) *Jeder Untervektorraum von V ist abgeschlossen.*
(b) *Jede lineare Abbildung $V \to W$ in einen topologischen Vektorraum W ist stetig. Insbesondere ist jede Linearform auf V stetig.*

BEWEIS. Nach Definition der kanonischen Topologie reduzieren sich beide Aussagen sofort auf den Fall, wo $\dim(V) < \infty$ ist. Hier sind sie klar. □

1.12 Bemerkung. Ist $\dim(V)$ abzählbar unendlich, so gibt es keine abzählbare 0-Umgebungsbasis für die kanonische Topologie. Denn ist $\varepsilon^1, \varepsilon^2, \dots$ eine Folge von Folgen $\varepsilon^i = (\varepsilon^i_n)_{n\in\mathbb{N}}$ positiver reeller Zahlen, und ist $\varepsilon = (\varepsilon_n)_{n\in\mathbb{N}}$ definiert durch $\varepsilon_n := \frac{1}{2}\,\varepsilon^n_n$, so gilt $B(\varepsilon^i) \not\subseteq B(\varepsilon)$ für alle i. Insbesondere ist die kanonische Topologie also nicht metrisierbar.

Als Konsequenz der vorigen Bemerkung ist die Bildung des Abschlusses einer Menge (z.B. eines konvexen Kegels) in V im allgemeinen subtil. Den Folgenabschluß können wir wie folgt charakterisieren:

1.13 Satz. *Eine Folge $(x_i)_{i\geq 1}$ von Vektoren konvergiert in V genau dann, wenn sie ganz in einem endlich-dimensionalen Unterraum von V enthalten ist und in diesem konvergiert.*

BEWEIS. Sei $(x_i)_{i\geq 1}$ eine konvergente Folge in V, sei x der Grenzwert. Wir können annehmen $x = 0$. Sei $(v_n)_{n\geq 1}$ eine Basis von V. Für jedes $i \geq 1$ schreibe $x_i = \sum_{n\geq 1} a_{in} v_n$ mit $a_{in} \in \mathbb{R}$ (und $a_{in} = 0$ für fast alle n). Angenommen, $\operatorname{span}(x_i \colon i \geq 1)$ habe unendliche Dimension. Es gibt also Folgen $n_1 < n_2 < \cdots$ und $i_1 < i_2 < \cdots$ in $\mathbb{N}$ mit $a_{i_k n_k} \neq 0$ für alle $k \geq 1$. Sei $\varepsilon = (\varepsilon_n)_{n\geq 1}$ mit

$$\varepsilon_n \;=\; \begin{cases} |a_{i_k n_k}|/2 & \text{falls } \exists\, k \in \mathbb{N} \text{ mit } n = n_k, \\ 1 & \text{sonst.} \end{cases}$$

Für jedes $k \geq 1$ ist dann $x_{i_k} \notin B(\varepsilon)$, Widerspruch zur Voraussetzung $x_i \to 0$. □

1.14 Korollar. *Für jede Teilmenge M von V ist*

$$M^{\ddagger} \;:=\; \bigcup_{\substack{U\subseteq V \\ \dim(U)<\infty}} \overline{M \cap U}$$

der Folgenabschluß von M (Vereinigung über alle endlich-dimensionalen Unterräume U von V). □

(Der Folgenabschluß von M ist die Menge aller Grenzwerte aller konvergenten Folgen $(x_n)_{n\geq 1}$ mit $x_n \in M$ für alle n.) Aufgabe 44 zeigt, daß im allgemeinen $M^{\ddagger} \neq \overline{M}$ gilt.

2. Das Momentenproblem

2.1 Sei X ein topologischer Raum, sei $\mathcal{B}$ die von den offenen Teilmengen von X erzeugte σ-Algebra. Jedes (positive) Maß auf $(X, \mathcal{B})$ heißt ein *Borelmaß* auf X. Hat X eine abzählbare Basis offener Mengen (z.B. der Fall für $X \subseteq \mathbb{R}^n$), so ist der *Träger* $\operatorname{supp}(\mu)$ von μ definiert als kleinste abgeschlossene Menge $S \subseteq X$ mit $\mu(X \smallsetminus S) = 0$. Für $Z \subseteq X$ abgeschlossen identifizieren sich die Borelmaße auf X mit Träger in Z mit den Borelmaßen auf Z.

2.2 Sei μ ein Borelmaß auf $\mathbb{R}^n$, sei $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{Z}^n_+$. Man nennt

$$m_\alpha(\mu) \;:=\; \int_{\mathbb{R}^n} x^\alpha \,\mu(dx) \;=\; \int_{\mathbb{R}^n} x_1^{\alpha_1} \cdots x_n^{\alpha_n} \,\mu(dx)$$

das *Moment der Ordnung* α von μ, sofern das Integral existiert. Genau dann existieren alle Momente von μ, wenn für jedes $f \in \mathbb{R}[\mathtt{x}]$ das Integral $\int_{\mathbb{R}^n} f(x)\,\mu(dx)$

existiert. Alsdann ist

$$L_\mu\colon \mathbb{R}[\mathtt{x}] \to \mathbb{R}, \quad L_\mu(f) := \int_{\mathbb{R}^n} f(x)\,\mu(dx)$$

eine Linearform.

2.3 Definition. Eine Linearform $L\colon \mathbb{R}[x_1,\dots,x_n] \to \mathbb{R}$ heißt ein *Momentenfunktional*, wenn ein Borelmaß μ auf $\mathbb{R}^n$ existiert mit $L = L_\mu$. Ist $K \subseteq \mathbb{R}^n$ eine abgeschlossene Menge, und existiert solches μ mit $\operatorname{supp}(\mu) \subseteq K$, so heißt L auch ein *K-Momentenfunktional*. Wir schreiben $\mathcal{M}(K)$ für die Menge aller K-Momentenfunktionale.

2.4 Bemerkung. Der $\mathbb{R}$-Vektorraum $\mathbb{R}[\mathtt{x}]$ hat eine abzählbare Basis. Wir versehen $\mathbb{R}[\mathtt{x}]$ im weiteren stets mit der kanonischen Topologie (1.9). Es ist also $\mathbb{R}[\mathtt{x}]'$ der Vektorraum aller Linearformen $\mathbb{R}[\mathtt{x}] \to \mathbb{R}$. Die Menge $\mathcal{M}(K)$ ist ein konvexer Kegel in $\mathbb{R}[\mathtt{x}]'$.

2.5 Sei $K \subseteq \mathbb{R}^n$ eine abgeschlossene Menge. Das *K-Momentenproblem* hat zwei Teile:

1. Charakterisiere die Teilmenge $\mathcal{M}(K)$ von $\mathbb{R}[\mathtt{x}]'$ (*Existenzteil*);
2. charakterisiere bei gegebenem $L \in \mathcal{M}(K)$ die Gesamtheit aller Borelmaße μ mit $L = L_\mu$ (*Eindeutigkeitsteil*).

Wir betrachten nur den Existenzteil. Welche Art von Antwort man erwarten kann, wird aus folgenden klassischen Resultaten deutlich:

2.6 Satz. *Sei $a = (a_0, a_1, \dots)$ eine Folge reeller Zahlen.*

(a) (Hamburger 1921) *Genau dann ist a eine Momentenfolge auf $K = \mathbb{R}$, wenn die Matrix*

$$A = \begin{pmatrix} a_0 & a_1 & a_2 & \cdots \\ a_1 & a_2 & a_3 & \cdots \\ a_2 & a_3 & a_4 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

psd ist.

(b) (Stieltjes 1894) *Genau dann ist a eine Momentenfolge auf $K = \mathbb{R}_+$, wenn A und*

$$B = \begin{pmatrix} a_1 & a_2 & a_3 & \cdots \\ a_2 & a_3 & a_4 & \cdots \\ a_3 & a_4 & a_5 & \cdots \\ \vdots & \vdots & \vdots & \ddots \end{pmatrix}$$

beide psd sind.

(Eine unendliche reelle symmetrische Matrix $C = (c_{ij})_{i,j\ge 0}$ heißt dabei psd, i.Z. $C \succeq 0$, wenn alle endlichen symmetrischen Teilmatrizen psd sind.)

2.7 Bemerkung. Sei $L \in \mathbb{R}[x]'$, sei $a_i = L(x^i)$ $(i \ge 0)$. Für jedes Polynom $p = \sum_{i\ge 0} b_i x^i$ ist dann

$$L(p^2) \;=\; L\Big(\sum_{i,j} b_i b_j\, x^{i+j}\Big) \;=\; \sum_{i,j} b_i b_j a_{i+j} \;=\; b^t A b,$$

wobei b den Spaltenvektor der Koeffizienten von p bezeichnet. Satz 2.6(a) sagt also: $L \in \mathcal{M}(\mathbb{R}) \Leftrightarrow L(p^2) \geq 0$ für alle $p \in \mathbb{R}[x]$. Analog ist $L(xp^2) = b^t Bb$, also sagt 2.6(b): $L \in \mathcal{M}(\mathbb{R}_+) \Leftrightarrow L(p^2) \geq 0$ und $L(xp^2) \geq 0$ für alle $p \in \mathbb{R}[x]$.

2.8 Theorem. (Haviland, 1935/36) *Sei $K \subseteq \mathbb{R}^n$ eine beliebige abgeschlossene Teilmenge, sei*

$$\mathcal{P}(K) \;=\; \big\{f \in \mathbb{R}[\mathbf{x}] \colon f|_K \geq 0\big\}.$$

Dann gilt $\mathcal{M}(K) = \mathcal{P}(K)^*$, d.h. $L \in \mathbb{R}[\mathbf{x}]'$ ist genau dann ein K-Momentenfunktional, wenn $L(f) \geq 0$ für alle $f \in \mathcal{P}(K)$ ist.

Beweis. Ist $L \in \mathcal{M}(K)$ und μ ein Maß auf K mit $L = L_\mu$, dann ist $L(f) = \int_K f(x)\,\mu(dx) \geq 0$ für alle $f \in \mathcal{P}(K)$. Die Umkehrung zeigen wir nur im Fall, wo K kompakt ist. Dann ist $C(K,\mathbb{R})$, versehen mit der sup-Norm $||\cdot||_K$, ein Banachraum. Sei $I = \{f \in \mathbb{R}[\mathbf{x}] \colon f|_K = 0\}$ das Verschwindungsideal von K in $\mathbb{R}[\mathbf{x}]$. Nach Stone-Weierstraß ist $\mathbb{R}[\mathbf{x}]/I \subseteq C(K,\mathbb{R})$ ein dichter Teilring. Sei $L \in \mathbb{R}[\mathbf{x}]'$ mit $L|_{\mathcal{P}(K)} \geq 0$. Dann ist $I \subseteq \ker(L)$, also wird eine Linearform $\bar{L} \colon \mathbb{R}[\mathbf{x}]/I \to \mathbb{R}$ induziert.

Für $p \in \mathbb{R}[\mathbf{x}]$ und $c = ||p||_K$ sind $c \pm p \in \mathcal{P}(K)$, also ist $L(c \pm p) \geq 0$. Somit gilt $|L(p)| \leq ||p||_K \cdot L(1)$ für alle $p \in \mathbb{R}[\mathbf{x}]$. Die Linearform $\bar{L}$ setzt sich deshalb (eindeutig) zu einer stetigen Linearform $\tilde{L} \colon C(K,\mathbb{R}) \to \mathbb{R}$ fort: Ist $f \in C(K,\mathbb{R})$, und ist $(f_i)_{i\geq 1}$ eine Folge in $\mathbb{R}[\mathbf{x}]$ mit $||f - f_i||_K \to 0$, so ist die Folge $(L(f_i))_{i\geq 1}$ in $\mathbb{R}$ eine Cauchyfolge wegen

$$\big|L(f_i) - L(f_j)\big| \;\leq\; ||f_i - f_j||_K \cdot L(1),$$

und wir können $\tilde{L}(f) := \lim_{i\to\infty} L(f_i)$ definieren. Die Linearform $\tilde{L}$ ist wohldefiniert und stetig und erfüllt $\tilde{L}(f) \geq 0$ für $f \geq 0$. Nach dem Rieszschen Darstellungssatz gibt es genau ein Borelmaß μ auf X mit $L(f) = \int f(x)\,\mu(dx)$ für alle $f \in C(X,\mathbb{R})$. □

Das Argument hat gezeigt, daß für kompaktes K jedes $L \in \mathcal{M}(K)$ durch ein eindeutig bestimmtes Borelmaß auf K dargestellt wird. Für nichtkompaktes K ist die Eindeutigkeitsfrage dagegen subtil.

2.10 Bemerkung. Die Sätze von Hamburger und Stieltjes folgen sofort aus dem Satz von Haviland. Denn für $K = \mathbb{R}$ ist $\mathcal{P}(K) = \Sigma\mathbb{R}[x]^2$, für $K = \mathbb{R}_+$ ist $\mathcal{P}(K) = \Sigma\mathbb{R}[x]^2 + x\Sigma\mathbb{R}[x]^2 = PO(x)$ (siehe z.B. Satz IV.2.16).

2.11 Definition. Sei $K \subseteq \mathbb{R}^n$ abgeschlossen, sei $F \subseteq \mathbb{R}[\mathbf{x}]$ eine Teilmenge, und sei $M = QM(F)$ der von M erzeugte quadratische Modul. Wir sagen, daß das K-Momentenproblem durch F *gelöst* wird, wenn $\mathcal{M}(K) = M^*$ ist. Gibt es eine endliche Menge F mit dieser Eigenschaft, so heißt das K-Momentenproblem *endlich lösbar*.

2.12 Bemerkung. Daß das K-Momentenproblem durch $F \subseteq \mathbb{R}[\mathbf{x}]$ gelöst wird bedeutet: $\mathcal{M}(K)$ besteht genau aus allen $L \in \mathbb{R}[\mathbf{x}]'$ mit $L(fp^2) \geq 0$ für alle $f \in F \cup \{1\}$ und $p \in \mathbb{R}[\mathbf{x}]$. Ähnlich wie in 2.6 läßt sich das dadurch ausdrücken, daß gewisse unendliche symmetrische Matrizen psd sind:

Zu $f = \sum_\gamma b_\gamma x^\gamma \in \mathbb{R}[\mathbf{x}]$ und $L \in \mathbb{R}[\mathbf{x}]'$ bilde die unendliche symmetrische Matrix

$$A_L(f) \;:=\; \Big(\sum_\gamma b_\gamma L(x^{\alpha+\beta+\gamma})\Big)_{\alpha,\beta\in\mathbb{Z}_+^n}$$

Für $p = \sum_\alpha a_\alpha x^\alpha$ in $\mathbb{R}[\mathbf{x}]$ ist dann

$$L(fp^2) \;=\; \sum_{\alpha,\beta,\gamma} b_\gamma a_\alpha a_\beta\, L(x^{\alpha+\beta+\gamma}) \;=\; a^t \cdot A_L(f) \cdot a$$

(mit $a = (a_\alpha)$ Spaltenvektor). Deshalb gilt $A_L(f) \succeq 0 \Leftrightarrow L(fp^2) \geq 0$ für alle $p \in \mathbb{R}[\mathtt{x}]$. Wird also das K-Momentenproblem durch $f_1, \ldots, f_r$ gelöst, so folgt

$$\mathcal{M}(K) \;=\; \big\{L \in \mathbb{R}[\mathtt{x}]' \colon A_L(1) \succeq 0,\, A_L(f_1) \succeq 0,\, \ldots,\, A_L(f_r) \succeq 0\big\}.$$

2.13 Satz. *Sei $K \subseteq \mathbb{R}^n$ abgeschlossen, und sei $M \subseteq \mathbb{R}[\mathtt{x}]$ ein konvexer Kegel.*

(a) *$\mathcal{P}(K)$ ist abgeschlossen in $\mathbb{R}[\mathtt{x}]$.*
(b) *Genau dann ist $\mathcal{M}(K) = M^*$, wenn $\overline{M} = \mathcal{P}(K)$ ist.*

Beweis. Für $\xi \in \mathbb{R}^n$ sei $L_\xi \in \mathbb{R}[\mathtt{x}]'$ die Auswertungsabbildung in ξ. Dann ist $\mathcal{P}(K) = \bigcap_{\xi \in K} L_\xi^{-1}(\mathbb{R}_+)$, also abgeschlossen. Wegen $\mathcal{M}(K) = \mathcal{P}(K)^*$ (2.8) folgt aus $\mathcal{M}(K) = M^*$ also $\mathcal{P}(K) = \mathcal{M}(K)^* = M^{**} = \overline{M}$ (siehe 1.8). Aus $\mathcal{P}(K) = \overline{M}$ folgt umgekehrt $\mathcal{P}(K)^* = M^*$. □

Genau dann wird also das K-Momentenproblem durch $f_1, \ldots, f_r$ gelöst, wenn $QM(f_1, \ldots, f_r)$ eine dichte Teilmenge von $\mathcal{P}(K)$ ist.

2.14 Korollar. *Ist $M \subseteq \mathbb{R}[\mathtt{x}]$ ein konvexer Kegel mit $\mathcal{M}(K) = M^*$, so ist $S(M) = \{\xi \in \mathbb{R}^n \colon \forall\, f \in M\ f(\xi \geq 0\} = K$.*

Beweis. Sei $K_1 := S(M)$. Nach 2.13 ist $M \subseteq \mathcal{P}(K)$, also $K = S(\mathcal{P}(K)) \subseteq S(M) = K_1$. Umgekehrt ist $M \subseteq \mathcal{P}(K_1)$, also auch $\overline{M} = \mathcal{P}(K) \subseteq \mathcal{P}(K_1)$, also $K_1 \subseteq K$. □

2.15 Korollar. *Das K-Momentenproblem kann nur dann endlich lösbar sein, wenn K basisch abgeschlossen semialgebraisch ist.* □

Eine große Klasse von endlich lösbaren Momentenproblemen erhalten wir aus dem archimedischen Positivstellensatz:

2.16 Theorem. *Seien $h_1, \ldots, h_r \in \mathbb{R}[\mathtt{x}]$. Ist der quadratische Modul $M = QM(h_1, \ldots, h_r)$ archimedisch, so lösen $h_1, \ldots, h_r$ das Momentenproblem für $K = S(h_1, \ldots, h_r)$.*

Beweis. Es ist $M \subseteq \mathcal{P}(K)$. Ist umgekehrt $f \in \mathcal{P}(K)$, so gilt $f + \varepsilon \in M$ für alle $\varepsilon > 0$. Also folgt $f \in \overline{M}$. Somit ist $\overline{M} = \mathcal{P}(K)$, also fertig nach 2.13. □

Insbesondere gibt Schmüdgens Theorem:

2.17 Korollar. *Für jede basisch abgeschlossene kompakte Menge $K \subseteq \mathbb{R}^n$ ist das K-Momentenproblem endlich lösbar.* □

Ein weiteres Beispiel von gelösten Momentenproblemen:

2.18 Korollar. *Für jede abgeschlossene semialgebraische Menge $K \subseteq \mathbb{R}$ ist das K-Momentenproblem endlich lösbar.*

Beweis. Die saturierte Präordnung $\mathcal{P}(K)$ ist endlich erzeugt (Satz IV.2.16). □

2.19 Lemma. *Sei μ ein Maß auf $\mathbb{R}^n$, dessen Momente existieren. Sei $I \subseteq \mathbb{R}[\mathtt{x}]$ ein Ideal mit $I \subseteq \ker(L_\mu)$. Dann ist* $\operatorname{supp}(\mu) \subseteq Z(I)$.

($Z(I) :=$ Nullstellenmenge von I in $\mathbb{R}^n$)

BEWEIS. Die Behauptung sagt $\mu(\mathbb{R}^n \setminus Z(I)) = 0$. Sei $I = (h_1, \dots, h_m)$, sei $h = h_1^2 + \cdots + h_m^2$. Dann ist $h \geq 0$ auf $\mathbb{R}^n$, und $Z(h) = Z(I)$. Mit $U_k := \{\xi \in \mathbb{R}^n \colon h(\xi) \geq \frac{1}{k}\}$ $(k \geq 1)$ ist $\mathbb{R}^n \setminus Z(I) = \bigcup_{k\geq 1} U_k$. Es genügt also, $\mu(U_k) = 0$ für alle k zu zeigen. Das gilt wegen $L_\mu(h) = 0$ und

$$\mu(U_k) \;=\; \int_{U_k} 1 \, d\mu \;\leq\; k \int_{U_k} h \, d\mu \;\leq\; k \int_{\mathbb{R}^n} h \, d\mu \;=\; k L_\mu(h) \;=\; 0.$$

□

2.20 Satz. *Sei $L \in \mathbb{R}[\mathtt{x}]'$ mit $L(f^2) \geq 0$ für alle $f \in \mathbb{R}[\mathtt{x}]$. Sei I das größte Ideal von $\mathbb{R}[\mathtt{x}]$ mit $I \subseteq \ker(L)$. Dann gilt:*

(a) $I = \{f \in \mathbb{R}[\mathtt{x}] \colon L(f^2) = 0\}$,
(b) $I = \sqrt[\mathrm{re}]{I}$,
(c) *für jedes Maß μ mit $L = L_\mu$ ist $Z(I)$ der Zariskiabschluß von* $\mathrm{supp}(\mu)$ *in* $\mathbb{R}^n$.

BEWEIS. (a) Sei $J = \{f \in \mathbb{R}[\mathtt{x}] \colon L(f^2) = 0\}$. Es gilt $I \subseteq J$, denn aus $f \in I$ folgt $f^2 \in I \subseteq \ker(L)$ wegen I Ideal, also $L(f^2) = 0$. Sei $f \in J$ und $g \in \mathbb{R}[\mathtt{x}]$. Für alle $t \in \mathbb{R}$ ist $0 \leq L((tf + g)^2) = 2t\, L(fg) + L(g^2)$, woraus $L(fg) = 0$ folgt. Insbesondere ist $L(f) = 0$, also gilt $J \subseteq \ker(L)$. Weiter $L((fg)^2) = L(f \cdot fg^2) = 0$ für jedes $g \in \mathbb{R}[\mathtt{x}]$, also $fg \in J$. Ist auch $g \in J$, so ist $L((f + g)^2) = 2L(fg) = 0$, also $f + g \in J$. Somit ist J ein Ideal, also gilt $J \subseteq I$.

(b) Es ist auch $J = \sqrt[\mathrm{re}]{J}$. Denn aus einer Identität $f^{2^m} + a_1^2 + \cdots + a_r^2 \in J$ (mit $f, a_i \in \mathbb{R}[\mathtt{x}]$ und $m \geq 1$) folgt $L(f^{2^m}) = 0$, und daraus induktiv $L(f^2) = 0$, also $f \in J$.

(c) Für den Zariskiabschluß Z' von $\mathrm{supp}(\mu)$ in $\mathbb{R}^n$ gilt $Z' \subseteq Z(I)$ nach 2.19. Ist I' das Verschwindungsideal von Z' in $\mathbb{R}[\mathtt{x}]$, so ist $\int f \, d\mu = 0$ für alle $f \in I'$, also $I' \subseteq \ker(L)$. Nach Definition von I folgt $I' \subseteq I$, und somit $Z(I) \subseteq Z(I') = Z'$. □

2.21 Satz. *Sei $K \subseteq \mathbb{R}^n$ abgeschlossen. Für den konvexen Kegel $M \subseteq \mathbb{R}[\mathtt{x}]$ gelte $M^* = \mathcal{M}(K)$. Sei $I \subseteq \mathbb{R}[\mathtt{x}]$ ein Ideal. Dann ist $(M + I)^* = \mathcal{M}(K \cap Z(I))$.*

BEWEIS. Nach Voraussetzung gilt $\overline{M} = \mathcal{P}(K)$ (Satz 2.13(b)), also insbesondere $M \subseteq \mathcal{P}(K)$. Für $Z := Z(I)$ folgt $M + I \subseteq \mathcal{P}(K \cap Z)$, also folgt $\mathcal{M}(K \cap Z) = \mathcal{P}(K \cap Z)^* \subseteq (M + I)^*$. Umgekehrt sei $L \in (M + I)^*$. Wegen $L \in M^* = \mathcal{M}(K)$ ist $L = L_\mu$ für ein Maß μ auf K. Es ist $I \subseteq \ker(L_\mu)$, also folgt $\mathrm{supp}(\mu) \subseteq Z$ aus Lemma 2.19, und daher $\mathrm{supp}(\mu) \subseteq K \cap Z$, also $L \in \mathcal{M}(K \cap Z)$. □

2.22 Korollar. *Sei $K \subseteq \mathbb{R}^n$ eine abgeschlossene Menge, und sei $Z \subseteq \mathbb{R}^n$ eine Zariski-abgeschlossene Menge. Ist das K-Momentenproblem endlich lösbar, so ist auch das $(K \cap Z)$-Momentenproblem endlich lösbar.* □

BEWEIS. Wird das K-Momentenproblem durch $h_1, \dots, h_r$ gelöst, und ist $Z = Z(g_1, \dots, g_s)$, so wird das $(K \cap Z)$-Momentenproblem nach Satz 2.21 gelöst durch $h_1, \dots, h_r, \pm g_1, \dots, \pm g_s$. □

3. Stabilität

3.1 Sei $\Sigma := \Sigma\mathbb{R}[\mathtt{x}]^2$ der sos-Kegel in $\mathbb{R}[\mathtt{x}]$. Für $d \geq 0$ sei $\mathbb{R}[\mathtt{x}]_d = \{f \in \mathbb{R}[\mathtt{x}] \colon \deg(f) \leq d\}$ (deg := Totalgrad). Für $h_1, \dots, h_r \in \mathbb{R}[\mathtt{x}]$ und $h_0 := 1$ sei

$$\Sigma_d(h_1, \dots, h_r) \;:=\; \Big\{ \sum_{i=0}^{r} s_i h_i \colon \; s_i \in \Sigma, \; \deg(s_i h_i) \leq d \; (i = 0, \dots, r) \Big\}.$$

Sei $M = QM(h_1, \dots, h_r) \subseteq \mathbb{R}[\mathbf{x}]$ und $M_d = M \cap \mathbb{R}[\mathbf{x}]_d$, setze $h_0 := 1$. Dann ist $\Sigma_d(h_1, \dots, h_r) \subseteq M_d$ eine Inklusion von konvexen Kegeln in $\mathbb{R}[\mathbf{x}]_d$, und es ist

$$M \;=\; \bigcup_{d\geq 0} M_d \;=\; \bigcup_{d\geq 0} \Sigma_d(h_1, \dots, h_r).$$

Beides sind aufsteigende Vereinigungen. Die Inklusionen $\Sigma_d(h_1, \dots, h_r) \subseteq M_d$ sind i.a. strikt. (Beispiel $M = QM(h) \subseteq \mathbb{R}[x]$ mit $h = 1 - x^2$, dann $1 + x \in M_1$, aber $1 + x \notin \Sigma_1(h)$.)

3.2 Lemma. *Für $d \geq 0$ und $h_1, \dots, h_r \in \mathbb{R}[\mathbf{x}]$ ist $\Sigma_d(h_1, \dots, h_r)$ ein semialgebraischer konvexer Kegel in $\mathbb{R}[\mathbf{x}]_d$.*

Beweis. Konvexer Kegel ist klar. Kann annehmen $\deg(h_i) \leq d$ für alle i. Für $i = 0, \dots, r$ sei $e_i := \lfloor \frac{1}{2}(d - \deg(h_i)) \rfloor$, und sei $m_i = \dim \mathbb{R}[\mathbf{x}]_{e_i}$. Dann ist $\Sigma_d(h_1, \dots, h_r)$ die Bildmenge der Abbildung

$$\phi\colon \bigoplus_{i=0}^{r} \big(\mathbb{R}[\mathbf{x}]_{e_i}\big)^{m_i} \;\to\; \mathbb{R}[\mathbf{x}]_d, \quad \big(p_{ij}\big)_{\substack{0\leq i\leq r\\ 1\leq j\leq m_i}} \;\mapsto\; \sum_{i=0}^{r}\sum_{j=1}^{m_i} p_{ij}^2 h_i.$$

Denn ist $s_i \in \Sigma$ mit $\deg(s_i h_i) \leq d$, so ist s_i eine Summe von m_i Quadraten von Polynomen vom Grad $\leq e_i$ (siehe IV.1.20 für die Anzahlaussage). Es ist ϕ eine polynomiale Abbildung zwischen $\mathbb{R}$-Vektorräumen von endlicher Dimension, also ist $\mathrm{im}(\phi)$ eine semialgebraische Menge nach Tarski. □

3.3 Definition. Sei $M = QM(h_1, \dots, h_r)$ ein endlich erzeugter quadratischer Modul, sei $h_0 = 1$. Man nennt M *stabil*, wenn es eine Abbildung $\varphi\colon \mathbb{N} \to \mathbb{N}$ gibt, so daß $M_d \subseteq \Sigma_{\varphi(d)}(h_1, \dots, h_r)$ für alle $d \geq 0$ gilt. Solches φ heißt eine *Stabilitätsschranke* für M (bezüglich dem Erzeugendensystem $h_1, \dots, h_r$).

Die Stabibilität hängt nur von M ab, nicht vom gewählten Erzeugendensystem. Das folgt aus dem nächsten Lemma:

3.5 Lemma. *Seien $h_1, \dots, h_r \in \mathbb{R}[\mathbf{x}]$, sei $M = QM(h_1, \dots, h_r)$, sei $g \in M$. Genau dann gibt es für M eine Stabilitätsschranke bezüglich $h_1, \dots, h_r$, wenn es eine solche bezüglich $h_1, \dots, h_r, g$ gibt.*

Beweis. "⇒" ist klar. Umgekehrt sei $\varphi\colon \mathbb{N} \to \mathbb{N}$ eine Abbildung derart, daß es für alle $d \in \mathbb{N}$ und alle $p \in M_d$ eine Darstellung

$$p \;=\; s_0 + s_1 h_1 + \cdots + s_r h_r + tg$$

mit $s_0, \dots, s_r, t \in \Sigma$ und $\deg(s_i h_i) \leq \varphi(d)$ $(i = 0, \dots, r)$, $\deg(tg) \leq \varphi(d)$ gibt. Wegen $g \in M$ gibt es eine Gleichung

$$g \;=\; q_0 + q_1 h_1 + \cdots + q_r h_r$$

mit $q_0, \dots, q_r \in \Sigma$. Sei $e = \max\{\deg(q_i h_i)\colon i = 0, \dots, r\}$. Dann ist

$$p \;=\; (s_0 + tq_0) + (s_1 + tq_1)h_1 + \cdots + (s_r + tq_r)h_r$$

mit $s_i + tq_i \in \Sigma$, und dabei gilt

$$\deg\big((s_i + tq_i)h_i\big) \;\leq\; \varphi(d) + e - \deg(g)$$

für alle i. Also ist $\psi(d) = \varphi(d) + e - \deg(g)$ eine Stabilitätsschranke bezüglich $h_1, \dots, h_r$. □

3.6 Beispiele.

1. $M = \Sigma \subseteq \mathbb{R}[\mathbf{x}]$ ist stabil mit Stabilitätsschranke $\varphi(d) = d$.

2. $M = \Sigma + \Sigma(1-x^2) \subseteq \mathbb{R}[x]$ $(n = 1)$ ist stabil, mit Stabilitätsschranke $\varphi(d) = d+1$ (Aufgabe 47).

3. $M = \Sigma + \Sigma h \subseteq \mathbb{R}[x]$ mit $h = (1-x^2)^3$ ist nicht stabil. Für alle $\varepsilon > 0$ ist $1 + \varepsilon - x^2 \in M$. Man kann zeigen: Es gibt eine Konstante $C > 0$ so, daß in jeder Identität

$$1 + \varepsilon - x^2 \;=\; s + t(1-x^2)^3$$

mit s, $t \in \Sigma$ gilt

$$\deg(s) \;\geq\; \frac{C}{\sqrt{\varepsilon}}.$$

4. Das Konzept der Stabilität verallgemeinert sich vom Polynomring auf beliebige endlich erzeugte $\mathbb{R}$-Algebren A. Ein quadratischer Modul $M = \Sigma + \Sigma h_1 + \cdots + \Sigma h_r$ in A heißt stabil, wenn es zu jedem endlich-dimensionalen Unterraum U von A einen endlich-dimensionalen Unterraum W von A gibt mit

$$M \cap U \;\subseteq\; (\Sigma W^2) + (\Sigma W^2)h_1 + \cdots + (\Sigma W^2)h_r$$

(mit ΣW^2 = Menge der Summen von Quadraten von Elementen aus W). Für $A = \mathbb{R}[\mathtt{x}]$ ist dies zur obigen Definition äquivalent. Die Unabhängigkeit von der Wahl der Erzeugendensystems (Lemma 3.5) zeigt man analog. Mit dieser Definition gilt:

3.7 Lemma. *Ist $M \subseteq A$ ein endlich erzeugter quadratischer Modul, und ist $I \subseteq \operatorname{supp}(M)$ ein Ideal, so ist M genau dann stabil in A, wenn M/I stabil in A/I ist.*

Beweis. "$\Rightarrow$" ist klar. Für "$\Leftarrow$" sei $I = (g_1, \ldots, g_s)$. Wähle ein Erzeugendensystem $h = (h_1, \ldots, h_r)$ von M so, daß die $\pm g_j$ unter den h_i sind. Für jeden Unterraum $V \subseteq A$ sei

$$\Sigma_h(V) \;:=\; (\Sigma V^2) + (\Sigma V^2)h_1 + \cdots + (\Sigma V^2)h_r.$$

Sei $U \subseteq A$ ein Unterraum mit $\dim(U) < \infty$. Wegen M/I stabil gibt es einen Unterraum $W \subseteq A$ mit $\dim(W) < \infty$ und mit

$$M \cap U \;\subseteq\; \Sigma_h(W) + I.$$

Sei $L \subseteq A$ ein Unterraum mit $U + \Sigma_h(W) \subseteq L$ und mit $\dim(L) < \infty$. Dann gilt $M \cap U \subseteq (I \cap L) + \Sigma_h(W)$. Sei $V \subseteq A$ ein Unterraum mit $1 \in V$, $\dim(V) < \infty$ und mit $I \cap L \subseteq g_1 V + \cdots + g_s V$. Wegen

$$g_i v \;=\; g_i\Big(\frac{1+v}{2}\Big)^2 - g_i\Big(\frac{1-v}{2}\Big)^2$$

und wegen $\{\pm g_1, \ldots, \pm g_s\} \subseteq \{h_1, \ldots, h_r\}$ folgt $I \cap L \subseteq \Sigma_h(V)$. Also ist $M \cap U \subseteq \Sigma_h(V) + \Sigma_h(W) \subseteq \Sigma_h(V+W)$. □

3.8 Bemerkung. Eine zur Stabilität analoge Eigenschaft kann man auch für Ideale (etwa im Polynomring) untersuchen. Für Ideale ist diese Eigenschaft immer erfüllt: Ist $I = (h_1, \ldots, h_r) \subseteq k[\mathtt{x}]$ ein Ideal, so gibt es zu jedem $d \geq 0$ ein $e \geq 0$ mit

$$I \cap k[\mathtt{x}]_d \;\subseteq\; k[\mathtt{x}]_e\, h_1 + \cdots + k[\mathtt{x}]_e\, h_r.$$

Denn analog zu Lemma 3.5 hängt die Eigenschaft nicht ab vom fixierten Erzeugersystem von I. Wir können deshalb eine Gröbnerbasis von I wählen, und tun dies bezüglich einer deg-verträglichen Monomordnung (also $x^\alpha \preceq x^\beta \Rightarrow |\alpha| \leq |\beta|$). Gemäß Division mit Rest gibt es dann für jedes $f \in I$ Polynome $g_1, \ldots, g_r \in k[\mathtt{x}]$ mit $f = \sum_{i=1}^r g_i h_i$ und mit $LM(g_i h_i) \preceq LM(f)$ für alle i. Insbesondere ist also $\deg(g_i h_i) \leq \deg(f)$ für alle i.

3.9 Satz. *Sei $M \subseteq \mathbb{R}[\mathbf{x}]$ ein endlich erzeugter quadratischer Modul. Die s.a. Menge $K = S(M)$ enthalte einen nichtleeren offenen Kegel im $\mathbb{R}^n$. Dann ist M stabil (mit Stabilitätsschranke $\varphi(d) = d$).*

BEWEIS. Aufgabe 46. □

3.10 Lemma. *Sei A ein Ring, sei $I \subseteq A$ ein Ideal. Dann ist $1 + \sqrt[\mathrm{re}]{I} \subseteq I + \Sigma A^2$.*

BEWEIS. Zeige zunächst induktiv: Für jedes $a \in A$ und jedes $n \geq 1$ ist

$$n - a + \frac{4a^{2^n}}{2^{2^{n+1}}} \;\in\; \Sigma A^2. \tag{$*$}$$

Für $n = 1$ ist das die Identität $1 - a + \frac{a^2}{4} = (1 - \frac{a}{2})^2$. Wegen

$$n + 1 - a + \frac{4a^{2^{n+1}}}{2^{2^{n+2}}} \;=\; \Big(n - a + \frac{4a^{2^n}}{2^{2^{n+1}}}\Big) + \Big(1 - \frac{2a^{2^n}}{2^{2^{n+1}}}\Big)^2$$

ergibt sich der allgemeine Fall. Sei jetzt $a \in \sqrt[\mathrm{re}]{I}$. Nach dem abstrakten reellen Nullstellensatz ist $-a^{2m} \in I + \Sigma A^2$ für ein $m \in \mathbb{N}$. Wähle eine 2-Potenz $n = 2^k$ mit $2^n \geq 2m$. Dann gilt also $-a^{2^n} \in I + \Sigma A^2$. Anwendung von $(*)$ auf na statt a zeigt $n(1 - a) \in I + \Sigma A^2$. Daraus folgt $1 - a \in I + \Sigma A^2$. □

3.11 Korollar. *Für jeden quadratischen Modul $M \subseteq \mathbb{R}[\mathbf{x}]$ und jedes $0 < \varepsilon \in \mathbb{R}$ gilt $\varepsilon + \sqrt{\mathrm{supp}(M)} \subseteq M$. Insbesondere ist $M + \sqrt{\mathrm{supp}(M)} \subseteq M^\ddagger \subseteq \overline{M}$.*

BEWEIS. Erste Aussage sofort aus Lemma 3.10, angewandt auf das Ideal $I = \mathrm{supp}(M)$). Für $f \in M + \sqrt{\mathrm{supp}(M)}$ und alle $n \in \mathbb{N}$ ist also $\frac{1}{n} + f \in M$. Daraus folgt $f \in M^\ddagger$ (Folgenabschluß von M). □

3.12 Korollar. *Für jede endlich erzeugte Präordnung $T \subseteq \mathbb{R}[\mathbf{x}]$ ist $\mathrm{supp}(\overline{T}) = \sqrt{\mathrm{supp}(T)}$.*

BEWEIS. Sei $K = S(T)$. Es ist $\mathrm{Sat}(T) = \mathcal{P}(K)$ abgeschlossen in $\mathbb{R}[\mathbf{x}]$ (2.13(a)), also gilt $\overline{T} \subseteq \mathrm{Sat}(T)$, und wegen $\mathrm{supp}(\mathrm{Sat}(T)) = \sqrt{\mathrm{supp}(T)}$ (VI.1.13) folgt $\mathrm{supp}(\overline{T}) \subseteq \sqrt{\mathrm{supp}(T)}$. Die umgekehrte Inklusion gilt nach Korollar 3.10. □

3.13 Lemma. *Sei M ein quadratischer Modul in einem Ring A, sei $I := \mathrm{supp}(M)$. Dann ist das Ideal $\sqrt{I}$ M-konvex, d.h. es ist $\mathrm{supp}(M + \sqrt{I}) = \sqrt{I}$.*

BEWEIS. Nach IV.4.1 ist jeder minimale Primteiler $\mathfrak{p}$ von I ein M-konvexes Ideal. Als Durchschnitt von M-konvexen Idealen ist also auch $\sqrt{I}$ M-konvex. □

Der folgende Satz bestimmt den Abschluß eines stabilen quadratischen Moduls. Ebenso wichtig ist die Tatsache, daß dieser Abschluß selbst wieder stabil ist:

3.14 Theorem. *Sei M ein stabiler endlich erzeugter quadratischer Modul in $\mathbb{R}[\mathbf{x}]$. Dann ist $\overline{M} = M + \sqrt{\mathrm{supp}(M)}$, und der quadratische Modul $\overline{M}$ ist selbst endlich erzeugt und stabil.*

BEWEIS. Setze $A := \mathbb{R}[\mathbf{x}]$, schreibe $\Sigma = \Sigma A^2$ und $A_m := \mathbb{R}[\mathbf{x}]_m$ für alle $m \geq 0$. Sei $M = \Sigma h_0 + \cdots + \Sigma h_r$, sei $I := \sqrt{\mathrm{supp}(M)}$. Wir fixieren $d \geq 0$ und zeigen, daß $M_d = M \cap A_d$ abgeschlossen (in A_d) ist. Nach Voraussetzung gibt es ein $e \geq 0$, so daß jedes Element in M_d von der Form $\sum_{i=0}^r s_i h_i$ mit $s_i \in \Sigma$ und $\deg(s_i h_i) \leq e$ ist. Sei $e_i = \lfloor \frac{1}{2}(e - \deg(h_i)) \rfloor$ (o.E. sei $e \geq \max_i \deg(h_i)$), und sei $m_i = \deg(A_{e_i})$

$(i = 0, \dots, r)$. Betrachte die Abbildung

$$\phi\colon \bigoplus_{i=0}^{r} A_{e_i}^{m_i} \to A_e, \quad p = \big(p_{ij}\big)_{\substack{0\le i\le r\\ 1\le j\le m_i}} \mapsto \sum_{i=0}^{r}\sum_{j=1}^{m_i} p_{ij}^2\, h_i.$$

Die Abbildung ϕ ist homogen vom Grad 2, und es gilt $M_d = A_d \cap \operatorname{im}(\phi)$.

(1) $\operatorname{im}(\phi) + I$ *ist abgeschlossen in* A.

Setze $J_i := \{f \in A\colon fh_i \in I\}$ $(i = 0, \dots, r)$. Dies ist ein Ideal von A, und wegen $\sqrt{I} = I$ ist $\sqrt{J_i} = J_i$. Die Abbildung ϕ induziert eine Abbildung

$$\overline{\phi}\colon \bigoplus_{i=0}^{r} \big(A_{e_i}/A_{e_i} \cap J_i\big)^{m_i} \to A_e/I_e.$$

Sei $\overline{p} = (\overline{p}_{ij})$ ein Tupel in der linken Menge mit $\overline{\phi}(\overline{p}) = 0$, also mit $\sum_{i,j} p_{ij}^2 h_i \in I$. Nach Lemma 3.13 ist das Ideal I M-konvex. Deshalb folgt $p_{ij}^2 h_i \in I$ für alle i, j, also $p_{ij} \in J_i$. Also ist $\overline{\phi}^{-1}(0) = \{\overline{0}\}$. Nach Lemma IV.2.6 ist deshalb die Bildmenge $\operatorname{im}(\overline{\phi})$ abgeschlossen in $A_e/I_e = (A_e + I)/I$. Somit ist $\operatorname{im}(\phi) + I$ abgeschlossen in $A_e + I$, also auch in A.

(2) $(M + I)_d \subseteq \operatorname{im}(\phi) + I$.

Seien $g \in M$ und $h \in I$, und für $f = g + h$ gelte $\deg(f) \le d$. Nach Korollar 3.11 ist $h + \varepsilon \in M$ für alle $\varepsilon > 0$. Also ist $f + \varepsilon \in M_d$ für alle $\varepsilon > 0$, und somit ist $f \in \overline{M_d}$. Aus $M_d \subseteq \operatorname{im}(\phi) \subseteq \operatorname{im}(\phi)$ und (1) folgt $\overline{M}_d \subseteq \operatorname{im}(\phi) + I$, womit (2) gezeigt ist.

(3) Der quadratische Modul $M + I$ *ist stabil.*

Nach (2) ist $(M+I)_d \subseteq \operatorname{im}(\phi)+I$. Diese Aussage für alle d sagt, daß $(M+I)/I$ stabil in A/I ist. Nach Lemma 3.7 ist also auch $M + I$ stabil in A.

(4) $M + I$ *ist der Abschluß von* M.

Nach (2) ist $(M + I)_d \subseteq (\operatorname{im}(\phi) + I)_d$. Die umgekehrte Inklusion gilt ohnehin, also gilt Gleichheit. Die rechte Menge ist abgeschlossen nach (1), also ist $(M + I)_d$ abgeschlossen. Dies für alle d zeigt, daß $M + I$ abgeschlossen ist. Andererseits ist $M + I \subseteq \overline{M}$ nach Korollar 3.11, woraus (4) folgt. □

3.15 Korollar. *Sei* M *ein stabiler endlich erzeugter quadratischer Modul. Genau dann ist* M *abgeschlossen, wenn* $\operatorname{supp}(M)$ *ein Radikalideal ist.*

Beweis. Wegen M stabil ist $\overline{M} = M + \operatorname{supp}(M)$ (3.14). Daraus sofort die Behauptung. □

Anwendung:

3.16 Korollar. *Ist* M *ein endlich erzeugter quadratischer Modul in* $\mathbb{R}[\mathbf{x}]$*, und enthält* $S(M)$ *einen nichtleeren offenen Kegel, so ist* M *abgeschlossen (und stabil).*

Beweis. Nach Satz 3.9 ist M stabil. Da $S(M)$ Zariski-dicht in $\mathbb{A}^n$ ist, ist $\operatorname{supp}(M) = (0)$. Also ist M abgeschlossen nach Korollar 3.15. □

3.16 verallgemeinert die Abgeschlossenheit des sos-Kegels in $\mathbb{R}[\mathbf{x}]$ (Satz IV.2.5). Das Resultat läßt sich auch vom affinen Raum $\mathbb{A}^n$ auf viele andere affine $\mathbb{R}$-Varietäten verallgemeinern. Andererseits erhalten wir jetzt viele Beispiele von nicht stabilen quadratischen Moduln:

3.17 Korollar. *Sei $M \subseteq \mathbb{R}[\mathbf{x}]$ ein endlich erzeugter und archimedischer quadratischer Modul. Für die Menge $K = S(M) \subseteq \mathbb{R}^n$ gelte $\dim(K) \geq 3$. Dann ist M nicht stabil.*

Beweis. Nach dem archimedischen Positivstellensatz enthält M alle auf K strikt positiven Polynome. Daher ist $\overline{M}$ saturiert, d.h. $\overline{M} = \mathcal{P}(K)$. Wäre M stabil, so wäre $\mathcal{P}(K)$ endlich erzeugt nach 3.14. Das ist aber nicht der Fall, siehe Theorem VI.1.7. □

Die Aussage von Korollar 3.17 bleibt auch für $\dim(K) = 2$ noch richtig (Beweis schwierig). Im speziellen Fall $K \subseteq \mathbb{R}^2$ gibt es einen einfacheren Beweis:

3.18 Theorem. *Sei $n \geq 2$, seien $h_1, \ldots, h_r \in \mathbb{R}[\mathbf{x}] = \mathbb{R}[x_1, \ldots, x_n]$, sei $K = S(h_1, \ldots, h_r) \subseteq \mathbb{R}^n$ und $M = QM(h_1, \ldots, h_r)$. Ist M stabil, und hat K nichtleeres Inneres in $\mathbb{R}^n$, dann gibt es ein auf $\mathbb{R}^n$ strikt positives Polynom, das nicht in M liegt. Insbesondere lösen $h_1, \ldots, h_r$ nicht das K-Momentenproblem.*

Benutze folgenden offensichtlichen

3.19 Hilfssatz. *Sei $d \in \mathbb{N}$, sei $N = \dim \mathbb{R}[\mathbf{x}]_d$. Dann gibt es N Punkte $\xi_1, \ldots, \xi_N \in \mathbb{R}^n$ derart, daß die lineare Abbildung*

$$\mathbb{R}[\mathbf{x}]_d \to \mathbb{R}^N, \quad f \mapsto \big(f(\xi_1), \ldots, f(\xi_N)\big)$$

bijektiv ist.

Beweis von Theorem 3.18. Die letzte Aussage folgt aus der ersten. Denn aus M stabil folgt wegen $\operatorname{supp}(M) = (0)$, daß M abgeschlossen ist (Theorem 3.14). Aus 3.18 folgt, daß M nicht saturiert ist. Also ist $\overline{M} = M \neq \mathcal{P}(K)$.

Für den Beweis der ersten Aussage fixiere $f \in \mathbb{R}[x]$ mit $f > 0$ auf $\mathbb{R}^n$ derart, daß f nicht sos ist (zB $f = g + 1$ mit g das (inhomogene) Motzkinpolynom). Nach einer Translation erreiche $h_i(0) > 0$ für $i = 1, \ldots, r$. Für $0 < c \in \mathbb{R}$ sei $f_c(x) := f(cx)$. Wir zeigen genauer: Für hinreichend großes $c > 0$ ist $f_c \notin M$. Angenommen nämlich, es gebe eine Identität

$$f_c(x) \;=\; \sum_{i=0}^{r} h_i(x) \sum_{j=1}^{N_c} g_{ij}^{(c)}(x)^2 \tag{9}$$

für beliebig große $c > 0$ (mit $h_0 = 1$). Wegen M stabil gibt es dann solche Identitäten auch mit $\deg\big(g_{ij}^{(c)}\big) \leq d$ für ein $d \geq 0$, und für alle i, j und c, und mit $N_c = N < \infty$ für alle c. Ersetze x durch $\frac{x}{c}$ und erhalte dann

$$f(x) \;=\; \sum_{i=0}^{r} h_i\Big(\frac{x}{c}\Big) \sum_{j=1}^{N} g_{ij}^{(c)}\Big(\frac{x}{c}\Big)^2. \tag{10}$$

Wegen $h_i(0) > 0$ für alle i gibt es reelle Zahlen ρ, $\alpha > 0$ mit $h_i(u) \geq \alpha > 0$ für alle $u \in \mathbb{R}^n$ mit $|u| < \rho$. Für jeden Punkt $v \in \mathbb{R}^n$ gibt es deshalb $0 < c_0 \in \mathbb{R}$ so, daß

$$\sup_{c > c_0} \sup_{i,j} \Big| g_{ij}^{(c)}\Big(\frac{v}{c}\Big) \Big| \;<\; \infty$$

ist. In der Tat, für $c > c_0 := \frac{|v|}{\rho}$ ist $\big|\frac{v}{c}\big| < \rho$, also

$$f(v) \;=\; \sum_{i,j} h_i\Big(\frac{v}{c}\Big)\, g_{ij}^{(c)}\Big(\frac{v}{c}\Big)^2 \;\geq\; \alpha \sum_{i,j} g_{ij}^{(c)}\Big(\frac{v}{c}\Big)^2,$$

also ist obiges Supremum höchstens gleich $\sqrt{f(v)/\alpha}$.

Wegen $\deg\big(g_{ij}^{(c)}\big) \le d$ für alle i, j und c ist die Menge aller Polynome $g_{ij}^{(c)}\big(\frac{x}{c}\big)$ im Vektorraum $\mathbb{R}[\mathbf{x}]_d$ beschränkt, nach dem Hilfssatz. Deshalb gibt es eine Folge $c_\nu \to \infty$ derart, daß für jedes Paar i, j von Indices die Folge der Polynome $g_{ij}^{(c_\nu)}\big(\frac{x}{c_\nu}\big)$ $(\nu \to \infty)$ gegen ein Polynom $g_{ij}(x) \in \mathbb{R}[\mathbf{x}]_d$ konvergiert (koeffizientenweise). Betrachtet man Gleichung (10) für $c := c_\nu$ und geht zum Limes $\nu \to \infty$ über, so folgt

$$f(x) \;=\; \sum_{i=0}^{r} h_i(0) \sum_{j=1}^{N} g_{ij}(x)^2.$$

Das widerspricht der Tatsache, daß f nicht sos ist. □

3.20 Korollar. *Sei $n \ge 2$. Ist $M \subseteq \mathbb{R}[\mathbf{x}]$ ein endlich erzeugter archimedischer quadratischer Modul, und hat $K = S(M)$ nichtleeres Inneres in $\mathbb{R}^n$, so ist M nicht stabil.*

Beweis. Folgt sofort aus Theorem 3.18 und dem archimedischen Positivstellensatz. □

3.21 Korollar. *Sei $K \subseteq \mathbb{R}^n$ $(n \ge 2)$ eine abgeschlossene Menge, welche einen nichtleeren offenen Kegel in $\mathbb{R}^n$ enthält, so ist das K-Momentenproblem nicht endlich lösbar.*

Beweis. Sei $K = S(h_1, \ldots, h_r)$ eine beliebige endliche Beschreibung von K, sei $M = QM(h_1, \ldots, h_r)$. Nach Satz 3.9 ist M stabil. Nach Theorem 3.18 ist also $\overline{M} = M \ne \mathcal{P}(K)$. □

4. Beschreibung konvexer Mengen durch Lasserre-Relaxierung

4.1 Sei $\mathrm{Sym}_d(\mathbb{R})$ der Vektorraum der symmetrischen reellen $d \times d$-Matrizen, sei $\mathrm{Sym}_d^+(\mathbb{R}) = \{A \in \mathrm{Sym}_d(\mathbb{R})\colon A \succeq 0\}$, Kegel der psd Matrizen. Bekanntlich ist $A \in \mathrm{Sym}_d(\mathbb{R})$ genau dann psd, wenn für $\det(tI - A) = t^d - s_1 t^{d-1} \cdots + (-1)^d s_d$ gilt $s_i \ge 0$ $(i = 1, \ldots, d)$. Also ist $\mathrm{Sym}_d^+(\mathbb{R})$ ein basisch abgeschlossener semialgebraischer konvexer Kegel in $\mathrm{Sym}_d(\mathbb{R})$.

4.2 Definition. Sei V ein $\mathbb{R}$-Vektorraum, $\dim(V) < \infty$. Ein *Spektraeder* in V ist eine Menge der Form

$$S \;=\; \{x \in V\colon A + L(x) \succeq 0\}$$

in V, wobei $d \ge 1$, $L\colon V \to \mathrm{Sym}_d(\mathbb{R})$ eine lineare Abbildung und $A \in \mathrm{Sym}_d(\mathbb{R})$ ist.

4.3 Beispiele.

1. Ein Spektraeder in $V = \mathbb{R}^n$ ist also eine Menge der Form

$$S \;=\; \{x \in \mathbb{R}^n\colon M(x) \succeq 0\}$$

mit $d \in \mathbb{N}$, $M_0, \ldots, M_n \in \mathrm{Sym}_d(\mathbb{R})$ und $M(x) := M_0 + x_1 M_1 + \cdots + x_n M_n$. Schreibe kurz $S = sp(M(x))$. Eine Ungleichung der Form $M(x) \succeq 0$ mit $M(x)$ wie eben heißt *lineare Matrixungleichung* (LMI).

Sind $M_1, \ldots, M_n \in \mathrm{Sym}_d(\mathbb{R})$ linear unabhängig, so ist $sp(M(x))$ ein affinlinearer Schnitt von $\mathrm{Sym}_d^+(\mathbb{R})$. Sind sie linear abhängig, so ist $sp(M) \cong S \times \mathbb{R}^m$ mit $m \ge 1$ und einem solchen Schnitt S.

2. Jedes Polyeder ist ein Spektraeder. Denn ist $S = \{x \in \mathbb{R}^n\colon \langle x, u_i\rangle \ge a_i$ $(i = 1, \ldots, m)\}$ mit $u_i \in \mathbb{R}^n$, $a_i \in \mathbb{R}$ $(i = 1, \ldots, m)$, so ist $S = sp(M(x))$ für

$$M(x) \;=\; -\mathrm{diag}(a_1, \ldots, a_m) + \sum_{j=1}^{n} x_j \,\mathrm{diag}(u_{1j}, \ldots, u_{mj})$$

Jedes (Hyper-) Ellipsoid ist ein Spektraeder: Ist $A \in \mathrm{Sym}_n(\mathbb{R})$ positiv definit und $S = \{x \in \mathbb{R}^n \colon (x-u)^t A(x-u) \le 1\}$ mit $u \in \mathbb{R}^n$, so ist $S = S(M(x))$ für

$$M(x) \;=\; \begin{pmatrix} 1 & -u^t \\ -u & A^{-1} \end{pmatrix} + \sum_{i=1}^{n} x_i \begin{pmatrix} 0 & e_i^t \\ e_i & 0 \end{pmatrix} \;=\; \begin{pmatrix} 1 & (x-u)^t \\ x-u & A^{-1} \end{pmatrix}$$

in $\mathrm{Sym}_{n+1}(\mathbb{R})$. Denn für $v \in \mathbb{R}^n$ ist $v^t A v \le 1$ äquivalent zu $\begin{pmatrix} 1 & v^t \\ v & A^{-1} \end{pmatrix} \succeq 0$.

3. Spektraeder haben eine sehr restriktive Eigenschaft, sie sind starr konvex. Vermutungsweise sind sie dadurch sogar charakterisiert. Können wir hier nicht diskutieren.

4.4 Satz.

(a) *Jedes Spektraeder ist konvex, basisch abgeschlossen, semialgebraisch.*
(b) *Translationen und lineare Urbilder von Spektraedern sind Spektraeder.*
(c) *Endliche Durchschnitte von Spektraedern sind Spektraeder.*
(d) *Ist $S \subseteq \mathbb{R}^n$ ein Spektraeder und $u \in \mathrm{int(S)}$, so gibt es eine LMI $M(x)$ mit $S = \{x \in \mathbb{R}^n \colon M(x) \succeq 0\}$ und mit $M(u) = I$.*

Die Beweise von (a)-(c) sind klar, (d) ist eine Übungsaufgabe (lineare Algebra).

4.5 Definition. Sei V ein $\mathbb{R}$-Vektorraum, $\dim(V) < \infty$. Eine Menge $K \subseteq V$ heißt *sdp-Menge* (oder *projiziertes Spektraeder*, oder *spektraler Schatten*) in V, wenn $K = f(S)$ ist für eine lineare Abbildung $f \colon W \to V$ (mit $\dim(W) < \infty$) und ein Spektraeder $S \subseteq W$.

4.6 Bemerkungen.

1. Jede sdp-Menge ist konvex und semialgebraisch. Lineare Urbilder und Bilder von sdp-Mengen sind wieder sdp-Mengen, ebenso endliche Durchschnitte.

2. sdp-Mengen sind im allgemeinen nicht abgeschlossen, Beispiel

$$\left\{ x \in \mathbb{R} \colon \exists\, y \in \mathbb{R} \;\; \begin{pmatrix} x & 1 \\ 1 & y \end{pmatrix} \succeq 0 \right\} \;=\;]0, \infty[\,.$$

3. Optimierung von linearen Funktionalen über sdp-Mengen ist praktisch genauso einfach wie über Spektraeder. Daher besteht ein großes Interesse daran zu verstehen, welche konvexen Mengen eine Darstellung als projiziertes Spektraeder erlauben, und wie man solche erhalten kann. Die Helton-Nie Vermutung besagt, daß jede konvexe semialgebraische Menge eine sdp-Menge ist.

Wir diskutieren ein Verfahren von Lasserre. Ist $K \subseteq \mathbb{R}^n$ eine basisch abgeschlossene semialgebraische Menge, so wird eine absteigende Folge $K(1) \supseteq K(2) \supseteq \cdots \supseteq K$ von sdp-Mengen $K(d)$ konstruiert. In günstigen Fällen ist $\bigcap_d K(d) = \mathrm{conv}(K)$, in noch günstigeren ist sogar $\mathrm{conv}(K) = K(d)$ für ein $d \ge 1$. Die Konstruktion benutzt Quadratsummen und hängt eng mit den Konzepten Saturiertheit und Stabilität zusammen.

4.7 Seien $h_1, \ldots, h_r \in \mathbb{R}[\mathbf{x}]$, sei $K = S(h_1, \ldots, h_r) \subseteq \mathbb{R}^n$, und sei

$$M \;=\; \Sigma h_0 + \cdots + \Sigma h_r$$

(mit $h_0 = 1$ und $\Sigma = \Sigma\mathbb{R}[\mathbf{x}]^2$), sowie $I = \mathrm{supp}(M)$. Wir fixieren ein $d \in \mathbb{N}$ mit $d \ge \deg(h_i)$ für alle i, und setzen

$$e_i \;=\; \left\lfloor \frac{1}{2}\big(d - \deg(h_i)\big) \right\rfloor \quad (i = 0, \ldots, r).$$

Sei $U = \mathbb{R}[\mathbf{x}]_d$ und $W_i = \mathbb{R}[\mathbf{x}]_{e_i}$ für $i = 0, \dots, r$, und sei U' bzw. W_i' der lineare Dualraum von U bzw. W_i. Wir schreiben weiter $M_d = M \cap \mathbb{R}[\mathbf{x}]_d$, $M_0(d) := \{\sum_{i=0}^r s_i h_i \colon s_i \in \Sigma, \deg(s_i h_i) \le d \text{ für alle } i\}$ und $M(d) := M_0(d) + I_d$. Weiter sei $M(d)^* = \{\mu \in U' \colon \forall\, f \in M(d)\ \mu(f) \ge 0\}$, der zum Kegel $M(d)$ duale Kegel in U'.

4.8 Lemma. *$M(d)^*$ ist ein Spektraeder in U'.*

Beweis. Es ist $M(d)^* = M_0(d)^* \cap I_d^\perp$. Sei $i \in \{0, \dots, r\}$. Bezeichne den Raum der symmetrischen Bilinearformen auf W_i mit $S^2 W_i'$. Nach Wahl einer Basis von W_i identifiziert sich $S^2 W_i'$ mit $\mathrm{Sym}_N(\mathbb{R})$, dem Raum der symmetrischen Matrizen mit $N = \dim(W_i)$. Für jedes $\mu \in U'$ habe die symmetrische Bilinearform

$$\beta_i(\mu) \colon\ W_i \times W_i \to \mathbb{R}, \quad (p, q) \mapsto \mu(pqh_i)$$

auf W_i. Die Abbildung $\beta_i \colon U' \to S^2 W_i'$, $\mu \mapsto \beta_i(\mu)$ ist linear. Nach Definition ist

$$M_0(d)^* \ = \ \bigcap_{i=0}^r \{\mu \in U' \colon \forall\, p \in W_i\ \mu(p^2 h_i) \ge 0\} \ = \ \bigcap_{i=0}^r \{\mu \in U' \colon \beta_i(\mu) \succeq 0\}.$$

Also ist $M_0(d)^*$, und damit auch $M(d)^*$, ein Spektraeder in U'. □

4.9 Sei $L = \mathbb{R}[\mathbf{x}]_1$, sei L' der Dualraum von L, und sei $\rho \colon U' \to L'$ die Restriktionsabbildung zwischen den Dualräumen. Wir betrachten die affin-linearen Teilräume $U_1' = \{\mu \in U' \colon \mu(1) = 1\}$ von U' und $L_1' = \{\lambda \in L' \colon \lambda(1) = 1\}$ von L'. Dann gilt $\rho(U_1') \subseteq L_1'$. Für jedes $\xi \in \mathbb{R}^n$ sei $\lambda_\xi \in \mathbb{R}[\mathbf{x}]'$ die Auswertungsabbildung in ξ. Via

$$\mathbb{R}^n \xrightarrow{\sim} L_1', \quad \xi \mapsto \lambda_\xi\big|_L$$

(ein affin-linearer Isomorphismus) identifizieren wir L_1' mit $\mathbb{R}^n$. Mittels dieser Identifikation fassen wir $K \subseteq \mathbb{R}^n$ auch als Teilmenge von L_1' auf. (Die Umkehrabbildung $L_1' \to \mathbb{R}^n$ ist $\lambda \mapsto \big(\lambda(x_1), \dots, \lambda(x_n)\big)$.)

Mit $M(d)^*$ ist auch $M(d)^* \cap U_1'$ ein Spektraeder in $U_1' \subseteq U'$. Folglich ist

$$K(d) \ := \ \rho(M(d)^* \cap U_1') \ = \ L_1' \cap \rho(M(d)^*)$$

ein projiziertes Spektraeder in $L_1' = \mathbb{R}^n$. Es ist also $K(d)$ die Menge aller $\xi \in \mathbb{R}^n$, für die eine Linearform $\lambda \in U'$ mit $\lambda|_{M(d)} \ge 0$ und mit $\lambda(f) = f(\xi)$ für alle $f \in L$ existiert. Oder auch

$$K(d) \ = \ \Big\{\big(\mu(x_1), \dots, \mu(x_n)\big) \colon \mu \in M(d)^* \subseteq U',\ \mu(1) = 1\Big\}.$$

4.10 Lemma. *$K \subseteq K(d)$.*

Beweis. Für $\xi \in K$ ist $\lambda_\xi|_U \in U'$ eine Linearform, welche auf $M(d)$ nichtnegativ ist (wegen $M(d) \subseteq M \subseteq \mathcal{P}(K)$). □

Es ist also $K(d)$ ein projiziertes Spektraeder in $\mathbb{R}^n$, welches die konvexe Hülle von K enthält. Dabei gilt:

4.11 Lemma. *Für $d_1 \le d_2$ ist $K(d_2) \subseteq K(d_1)$.*

Beweis. Die Restriktionsabbildung $(\mathbb{R}[\mathbf{x}]_{d_2})' \to (\mathbb{R}[\mathbf{x}]_{d_1})'$ bildet $M(d_2)^*$ nach $M(d_1)^*$ ab, wegen $M(d_1) \subseteq M(d_2)$. □

4.12 Bemerkung. Das Spektraeder $M(d)^*$, und damit auch die sdp-Menge $K(d)$ in $\mathbb{R}^n$, wird durch eine vollkommen explizite lineare Matrixungleichung beschrieben. Für eine einfachere Notation nehme an $\mathrm{supp}(M) = (0)$. Sei $h \in \mathbb{R}[\mathbf{x}]$ mit $\deg(h) \le d$, etwa $h = \sum_{|\alpha| \le \deg(h)} h_\alpha \mathbf{x}^\alpha$, und sei $e = \lfloor \frac{1}{2}(d - \deg(h)) \rfloor$. Sei $U = \mathbb{R}[\mathbf{x}]_d$ und $W = \mathbb{R}[\mathbf{x}]_e$. Als Basis für $U' = \mathbb{R}[\mathbf{x}]_d'$ nehmen wir die μ_α ($|\alpha| \le d$),

definiert durch $\mu_\alpha(x^\beta) = \delta_{\alpha,\beta}$ (für $|\alpha|, |\beta| \le d$). Für $\mu \in U'$ betrachte wie oben die symmetrische Bilinearform $\beta_h(\mu) \in S^2W'$,

$$\beta_h(\mu)\colon\ W \times W \to \mathbb{R}, \quad (p,q) \mapsto \mu(pqh).$$

Für $|\alpha| \le d$ ist also

$$\beta_h(\mu_\alpha)(x^\chi, x^\eta) \ = \ \mu_\alpha\big(x^{\chi+\eta}h\big) \ = \ \sum_\sigma h_\sigma\, \mu_\alpha\big(x^{\chi+\eta+\sigma}\big) \ = \ h_{\alpha-\chi-\eta}.$$

Bezeichne die Matrix von $\beta_h(\mu_\alpha)$ mit

$$S_\alpha(h) \ := \ \big(h_{\alpha-\chi-\eta}\big)_{|\chi|,|\eta|\le e}$$

Setze kurz $S_0(h) := S_{(0,\dots,0)}$ und $S_i(h) := S_{(0,\dots,1,\dots,0)}$ mit 1 an der i-ten Stelle (für $i = 1,\dots,n$). Das durch die lineare Abbildung $\beta_h\colon U' \to S^2W'$ definierte Spektraeder in U' ist damit gleich

$$\Big\{ \sum_{|\alpha|\le d} u_\alpha\mu_\alpha\colon u_\alpha \in \mathbb{R}\ (|\alpha| \le d),\ \sum_{|\alpha|\le d} u_\alpha S_\alpha(h) \succeq 0 \Big\}.$$

Die Projektion nach $\mathbb{R}^n = L_1'$ ist die Menge aller $\xi \in \mathbb{R}^n$, für die reelle Zahlen $u_\alpha \in \mathbb{R}$ $(1 < |\alpha| \le d)$ existieren mit

$$S_0(h) + \sum_{i=1}^n \xi_i S_i(h) + \sum_{1<|\alpha|\le d} u_\alpha S_\alpha(h) \ \succeq \ 0.$$

Bezeichne die linke Matrix mit $S_h(\xi, u)$. Dann ist also

$$K(d) \ = \ \big\{\xi \in \mathbb{R}^n\colon \exists\, u_\alpha \in \mathbb{R}\ (1 < |\alpha| \le d) \text{ mit } S_{h_i}(\xi,u) \succeq 0\ (i = 0,\dots,r)\big\}.$$

Für $d \to \infty$ erhält man eine absteigende Folge von sdp-Obermengen $K(d)$ von K in $\mathbb{R}^n$. Offensichtliche Fragen: Gibt es $d \ge 1$ mit $\mathrm{conv}(K) = K(d)$? Oder ist zumindest $\mathrm{conv}(K) = \bigcap_d K(d)$?

4.13 Lemma. *Sei $K \ne \varnothing$, sei $d \in \mathbb{N}$. Für jedes lineare Polynom $l \in \mathbb{R}[\mathbf{x}]$ gilt:*

$$l \ge 0 \ \ \textit{auf}\ \ K(d) \quad \Leftrightarrow \quad l \in \overline{M(d)}.$$

Beweis. "$\Leftarrow$": Sei $l \in \overline{M(d)}$. Zu jedem $\xi \in K(d)$ gibt es $\lambda \in U'$ mit $\lambda(f) = f(\xi)$ für alle $f \in L$, und mit $\lambda \ge 0$ auf $M(d)$, also auch auf $\overline{M(d)}$. Nimm $f := l$ (liegt in $L \cap \overline{M(d)}$ nach Voraussetzung), dann folgt insbesondere $l(\xi) = \lambda(l) \ge 0$.

"$\Rightarrow$": Sei $l \ge 0$ auf $K(d)$. Wegen $\overline{M(d)} = M(d)^{**}$ ist zu zeigen: Für jede Linearform $\lambda \in U'$ mit $\lambda \ge 0$ auf $M(d)$ ist $\lambda(l) \ge 0$. Sei solches λ fixiert, es ist also $\lambda(1) \ge 0$.

1. Fall: $\lambda(1) > 0$. Nach Skalieren von λ erreichen wir $\lambda(1) = 1$. Sei dann $\xi = (\lambda(x_1),\dots,\lambda(x_n)) \in \mathbb{R}^n$, also $\lambda(f) = f(\xi)$ für alle $f \in L$. Nach Definition von $K(d)$ ist $\xi \in K(d)$, also ist $\lambda(l) = l(\xi) \ge 0$ nach Voraussetzung an l.

2. Fall: $\lambda(1) = 0$. Fixiere einen Punkt $\xi \in K$ und setze $\lambda_t := t^{-1}(\lambda + t\lambda_\xi) \in U'$ für alle $t > 0$. Dann ist $\lambda_t \in U'$ mit $\lambda_t(1) = 1$, und es ist $\lambda_t \ge 0$ auf $\overline{M(d)}$. Sei $\xi_t \in \mathbb{R}^n$ der Punkt mit $\lambda_t(f) = f(\xi_t)$ für alle $f \in L_1$. Dann ist $\xi_t \in K(d)$, und wegen $l \ge 0$ auf $K(d)$ ist somit $\lambda_t(l) = l(\xi_t) \ge 0$, also auch $\lambda(l) + tl(\xi) \ge 0$. Grenzübergang $t \to 0$ zeigt jetzt $\lambda(l) \ge 0$. □

4.14 Zur Vereinfachung machen wir ab jetzt die Annahme, daß ($K \ne \varnothing$ und) $I = \mathrm{supp}(M)$ ein Radikalideal ist. Dann ist $M(d)$ abgeschlossen (in $\mathbb{R}[\mathbf{x}]_d$) für alle d. In der Tat, das wurde in Schritt (1) im Beweis von Theorem 3.14 gezeigt.

4.15 Korollar. *$\overline{K(d)}$ ist die Menge aller $\xi \in \mathbb{R}^n$ mit $f(\xi) \geq 0$ für alle $f \in L \cap M(d)$.*

BEWEIS. Da $K(d) \subseteq \mathbb{R}^n$ konvex ist, ist

$$\overline{K(d)} \;=\; \bigcap_{\substack{l \in L \\ l|K(d) \geq 0}} \big\{\xi \in \mathbb{R}^n \colon l(\xi) \geq 0\big\}$$

nach dem (endlich-dimensionalen) Trennungssatz. Nach Lemma 4.13 (und Voraussetzung 4.14) läuft der Durchschnitt genau über alle $l \in L \cap M(d)$. □

4.16 Korollar. *Genau dann ist $\overline{K(d)} = \overline{\mathrm{conv}(K)}$, wenn $L \cap \mathcal{P}(K) \subseteq M(d)$ gilt.*

BEWEIS. Beide Mengen $K(d)$ bzw. $\mathrm{conv}(K)$ sind konvex in $\mathbb{R}^n$. Nach dem Trennungssatz sind ihre Abschlüsse genau dann gleich, wenn die jeweiligen Kegel der auf diesen Mengen nichtnegativen linearen Polynome übereinstimmen. Diese Kegel sind $L \cap M(d)$ (Lemma 4.13, wegen $M(d)$ abgeschlossen) bzw. $L \cap \mathcal{P}(K)$, und die Inklusion $M(d) \subseteq \mathcal{P}(K)$ gilt ohnehin immer. □

4.17 Satz. *Ist $L \cap \mathcal{P}(K) \subseteq \overline{L \cap M}$, so gilt*

$$\overline{\mathrm{conv}(K)} \;=\; \bigcap_{d>0} \overline{K(d)}.$$

Ist zusätzlich K kompakt, so gilt auch $\mathrm{conv}(K) = \bigcap_{d>0} K(d)$ (und $\mathrm{conv}(K)$ ist kompakt).

BEWEIS. Die Inklusion "$\subseteq$" gilt ohnehin immer. Für die Gleichheit ist also zu zeigen: Ist $l \in L \cap \mathcal{P}(K)$ und $\xi \in \bigcap_d \overline{K(d)}$, so ist $l(\xi) \geq 0$. Nach Voraussetzung ist $l \in \overline{L \cap M}$. Da $L \cap M$ ein konvexer Kegel in L ist, gibt es ein $g \in L \cap M$ mit $l + tg \in M$ für alle $t > 0$. (Tatsächlich kann man jedes g im relativen Inneren von $L \cap M$ nehmen, Übung.) Zu jedem $t > 0$ gibt es also ein $d_t \in \mathbb{N}$ mit $l + tg \in L \cap M(d_t)$. Wegen $\xi \in \overline{K(d_t)}$ folgt also $(l + tg)(\xi) = l(\xi) + tg(\xi) \geq 0$. Durch Grenzübergang $t \to 0$ ergibt sich $l(\xi) \geq 0$.

Ist K kompakt, so ist auch $\mathrm{conv}(K)$ kompakt nach dem Lemma von Carathéodory, und der Zusatz folgt. □

Ist K in 4.17 kompakt, so wird $\mathrm{conv}(K)$ tatsächlich beliebig gut von den sdp-Mengen $K(d)$ approximiert:

4.18 Lemma. *Ist $K_1 \supseteq K_2 \supseteq \cdots \supseteq \bigcap_m K_m = K$ eine Folge abgeschlossener konvexer Mengen in $\mathbb{R}^n$, und ist $K \neq \varnothing$ kompakt, so gibt es zu jedem $\varepsilon > 0$ einen Index m mit $\mathrm{dist}(K, K_m) < \varepsilon$ (dh $\forall\, x \in K_d\ \exists\, y \in K$ mit $|x - y| < \varepsilon$).*

BEWEIS. Für $y \in \mathbb{R}^n$ sei $d_K(y) = \min\{|y - x| \colon x \in K\}$. Die Abbildung $d_K \colon \mathbb{R}^n \to \mathbb{R}$ ist stetig. Sei $\varepsilon > 0$ und $U = \{y \in \mathbb{R}^n \colon d_K(y) < \varepsilon\}$ (eine offene Umgebung von K), angenommen $K_m \not\subseteq U$ für alle m. Für jedes $m \geq 1$ gibt es also $y_m \in K_m$ mit $d_K(y_m) \geq \varepsilon$. Wegen K_m konvex gibt es auch $y_m \in K_m$ mit $d_K(y_m) = \varepsilon$. Die Menge $X := \{y \in \mathbb{R}^n \colon d_K(y) = \varepsilon\}$ ist kompakt, und $X \cap K_m \neq \varnothing$ für alle m. Also folgt $X \cap \bigcap_m K_m \neq \varnothing$, d.h. $X \cap K \neq \varnothing$. Das ist ein Widerspruch. □

Wir halten insbesondere fest:

4.19 Korollar. *Ist der quadratische Modul M archimedisch, so ist*

$$\operatorname{conv}(K) \;=\; \bigcap_{d\geq 1} K(d).$$

Beweis. Für $l \in L \cap \mathcal{P}(K)$ und $\varepsilon > 0$ ist $l + \varepsilon \in M$, also ist $l \in \overline{L \cap M}$. Die Aussage folgt also aus Satz 4.17. □

4.20 Korollar. *Sei K kompakt. Gibt es ein $d \in \mathbb{N}$ mit $L \cap \mathcal{P}(K) \subseteq M(d)$, so ist $\operatorname{conv}(K) = K(d)$: Die Lasserre-Relaxierung ist exakt.*

Beweis. Nach 4.16 gilt $\overline{K(d)} = \overline{\operatorname{conv}(K)}$. Wegen K kompakt ist $\operatorname{conv}(K)$ kompakt, also folgt $K(d) \subseteq \operatorname{conv}(K)$. Die umgekehrte Inklusion gilt sowieso. □

In diesem Fall haben wir also eine explizite Darstellung von K als projiziertes Spektraeder gefunden. Beachte, daß die Voraussetzung einerseits eine partielle Saturiertheit von M bedeutet (saturiert in Grad eins), und andererseits eine partielle Stabilität von M (stabil in Grad eins).

4.21 Beispiel. Betrachte $f = x^2 + y^2 - 1 \in \mathbb{R}[x, y]$, das Ideal $I = (f)$ und den quadratischen Modul $M = \Sigma + I = \Sigma + \Sigma h - \Sigma h$ in $\mathbb{R}[x, y]$. Es ist also $K = C(\mathbb{R})$ die Einheitskreislinie, mit $C = V(f) \subseteq \mathbb{A}^2$. Sei $L = \mathbb{R}[x, y]_1$. Für $d \geq 1$ ist $M(d) = \{s+fh\colon s \in \Sigma,\, h \in \mathbb{R}[x, y],\, \deg(s), \deg(fh) \leq d\}$. Es ist $L \cap \mathcal{P}(K) \subseteq M(2)$. Das folgt aus dem Satz von Fejér-Riesz, oder durch direktes Nachrechnen, z.B. $2(1-x) = (1-x)^2+y^2-f$. Nach Korollar 4.20 ist also $K(2) = \operatorname{conv}(K)$ (Einheitskreisscheibe). Wir berechnen die zugehörige sdp-Darstellung. Verwende die Basis $1, x, y$ von $L = W$ bzw. $1, x, y, x^2, xy, y^2$ von $U = \mathbb{R}[x, y]_2$. Es ist $M(2)^* \cap U_1' \subseteq U'$ die Menge aller $\mu = \mu_1 + \xi\mu_x + \eta\mu_y + a\mu_{x^2} + b\mu_{xy} + c\mu_{y^2}$ mit $\mu(f) = 0$, also $c = 1 - a$, und mit $\mu(l^2) \geq 0$ für jedes $l \in L$, also mit

$$\begin{pmatrix} 1 & \xi & \eta \\ \xi & a & b \\ \eta & b & 1-a \end{pmatrix} \;\succeq\; 0. \qquad (*)$$

Es ist also $\operatorname{conv}(K)$ die Menge aller $(\xi, \eta) \in \mathbb{R}^2$, für die $a, b \in \mathbb{R}$ existieren mit $(*)$.

4.22 Bisher sind wir von einem quadratischen Modul $M \subseteq \mathbb{R}[\mathbf{x}]$ ausgegangen und haben $L = \mathbb{R}[\mathbf{x}]_1$ verwendet. Wir können auch mit einer affinen $\mathbb{R}$-Varietät V und ihrem Koordinatenring $A = \mathbb{R}[V]$ arbeiten und einen beliebigen Unterraum L (mit $\dim(L) < \infty$) nehmen. Zur Vereinfachung erkläre dies nur im Fall, wo $M = \Sigma A^2$ ist. Ist $1, y_1, \ldots, y_r$ eine Basis von L, so wird also versucht, die konvexe Hülle der Bildmenge von

$$\varphi\colon V(\mathbb{R}) \to \mathbb{R}^r, \quad \xi \mapsto (y_1(\xi), \ldots, y_r(\xi))$$

darzustellen. Fixiere L wie eben, sowie Unterräume $W, U \subseteq A$ mit $WW \subseteq U$, $L \subseteq U$ und $\dim(U) < \infty$. Sei $1, y_1, \ldots, y_r, z_1, \ldots, z_s$ eine Basis von U. Habe wieder die lineare Abbildung

$$\beta\colon U' \to S^2W', \quad \beta(\mu)(w_1, w_2) = \mu(w_1w_2),$$

und für $\mu \in U'$ gilt $\mu \in (\Sigma W^2)^* \Leftrightarrow \beta(\mu) \succeq 0$. Die zugehörige sdp-Menge ist also

$$K_W \;=\; \Big\{\xi \in \mathbb{R}^r\colon\; \exists\, b_1, \ldots, b_s \in \mathbb{R} \text{ mit } \beta\Big(\mu_1 + \sum_i \xi_i\mu_{y_i} + \sum_j b_j\mu_{z_j}\Big) \geq 0\Big\},$$

und diese Menge enthält $\varphi(V(\mathbb{R}))$. Ist $V(\mathbb{R})$ kompakt, und ist $L \cap A_+ \subseteq \Sigma W^2$, so ist $K_W = \operatorname{conv}\varphi(V(\mathbb{R}))$, analog wie 4.20.

4.23 Beispiel. Sei $C = V(x^2 + y^2 - 1) \subseteq \mathbb{A}^2$, sei $C_0 \subseteq \mathbb{A}^2$ die Kurve $x^4 + y^2 = x^2$ (eine liegende Acht). Die Kurve C_0 ist rational, man hat den surjektiven Morphismus

$$C \to C_0, \quad (x, y) \mapsto (x, xy).$$

Um $\operatorname{conv} C_0(\mathbb{R}) \subseteq \mathbb{R}^2$ zu beschreiben, müssen wir eine Relaxierung zum Unterraum $L = \operatorname{span}(1, x, xy) \subseteq \mathbb{R}[C]$ durchführen. Wähle $W = \operatorname{span}(1, x, y)$ und $U = WW = \operatorname{span}(1, x, y, x^2, xy)$ in $\mathbb{R}[C]$, dann ist $L \subseteq U$ und

$$K_W \;=\; \Big\{(\xi, \eta) \in \mathbb{R}^2 \colon \exists\, a,\, b \in \mathbb{R} \;\; \begin{pmatrix} 1 & \xi & a \\ \xi & b & \eta \\ a & \eta & 1-b \end{pmatrix} \succeq 0 \Big\}.$$

Tatsächlich ist $K_W = \operatorname{conv} C_0(\mathbb{R})$, d.h. die Relaxierung ist bereits exakt. Diese Menge ist nicht basisch abgeschlossen, also kein Spektraeder.

4.24 Beispiel. Für ein weiteres Beispiel betrachte die kuspische Kurve C_1 mit der Gleichung $x^4 + y^2 = x^3$. Wir haben den surjektiven Morphismus

$$C \to C_1, \quad (x, y) \;\mapsto\; \Big(\frac{1-y}{2},\, \frac{x(1-y)}{4}\Big).$$

Um die konvexe Hülle von $C_1(\mathbb{R})$ zu beschreiben, müssen wir eine Relaxierung zum Unterraum $L = \operatorname{span}(1,\, y,\, x(1-y)) \subseteq \mathbb{R}[C]$ durchführen.

Mache Variablentransformation $u = x$, $w = 1 - y$, schreibe also $\mathbb{R}[C] = \mathbb{R}[u, w]/(u^2 + w^2 - 2w)$, dann ist $L = \operatorname{span}(1, w, uw)$, und die Abbildung $C \to C_1$ ist $(u, w) \mapsto (\frac{w}{2},\, \frac{uw}{4})$. Für $W = \operatorname{span}(1, u, w)$ und $U = WW = \operatorname{span}(1, u, w, u^2, uw)$ in $\mathbb{R}[C]$ ist wieder $L \subseteq U$, und analog zum vorigem Beispiel ergibt sich

$$K_W \;=\; \Big\{(\xi, \eta) \in \mathbb{R}^2 \colon \exists\, a,\, b \in \mathbb{R} \;\; \begin{pmatrix} 1 & a & \xi \\ a & b & \eta \\ \xi & \eta & 2\xi - b \end{pmatrix} \succeq 0 \Big\}.$$

Tatsächlich ist K_W größer als $\operatorname{conv} C_1(\mathbb{R})$, Zeichnung. (Zum Beispiel ist $(2, 0) \in K_W$, für $a = b = 0$.) Um die Approximation zu verbessern, müssen wir W vergrößern. Nimm $W = \operatorname{span}(1, u, w, u^2, uw)$ und $U = WW = \operatorname{span}(1, u, w, u^2, uw, u^3, u^2w, u^4, u^3w)$. Für

$$\mu \;=\; \mu_1 + a\mu_u + \xi\mu_w + b\mu_{u^2} + \eta\mu_{uw} + c\mu_{u^3} + d\mu_{u^2w} + e\mu_{u^4} + f\mu_{u^3w}$$

ergibt sich $\beta(\mu)$ als

$$\begin{pmatrix} 1 & a & \xi & b & \eta \\ a & b & \eta & c & d \\ \xi & \eta & 2\xi - b & d & 2\eta - c \\ b & c & d & e & f \\ \eta & d & 2\eta - c & f & 2d - e \end{pmatrix}.$$

Es ist also K_W die Menge aller (ξ, η), für die $a, \ldots, f$ existieren, so daß obige Matrix psd ist, und man kann zeigen $\operatorname{conv} C_1(\mathbb{R}) = K_W$.