Stetigkeitsfragen rund ums 17. Hilbertsche Problem

Diplomarbeit von Sabine Cornelsen

Universität Konstanz
Fakultät für Mathematik und Informatik

3. März 1998

Inhaltsverzeichnis

Einleitung

Auf dem internationalen Mathematikerkongreß in Paris im Jahre 1900 hielt der Mathematiker David Hilbert einen Vortrag mit dem Titel "Mathematische Probleme". Er formulierte zur Jahrhundertwende aus verschiedenen mathematischen Bereichen 23 Probleme, "von deren Behandlung eine Förderung der Wissenschaft sich erwarten läßt." Beim 17. Problem handelt es sich um eine Fragestellung, die — wie man in [17] §37 nachlesen kann — bei der Charakterisierung der mit Lineal und Eichmaß konstruierbaren Elemente auftaucht. Sie lautet,

> "ob nicht jede definite Form als Quotient von Summen von Formenquadraten dargestellt werden kann"

und

> "ob die Koeffizienten der bei der Darstellung zu verwendenden Formen stets in demjenigen Rationalitätsbereich angenommen werden dürfen, der durch die Koeffizienten der dargestellten Form gegeben ist."

Dabei heißt eine rationale Funktion $f \in K(X)$ in n Variabeln definit (im Folgenden positiv semidefinit) über K, wenn $f(x) \geq 0$ für alle $x \in K^n$ gilt.

Dieses Problem wurde 1927 von Emil Artin in [2] in folgender Form positiv beantwortet:

> Ist K ein reeller Zahlkörper und $f \in K(X_1, \ldots, X_n)$ positiv semidefinit, so gibt es $e_i \in K$ mit $e_i \geq 0$ und $g_i \in K(X_1, \ldots, X_n)$ mit
>
> $$f = \sum e_i g_i^2$$

Später stellte sich heraus, daß man die Eigenschaft, daß K ein Zahlkörper ist, durch die Forderung, daß f über dem reellen Abschluß von K positiv semidefinit ist, ersetzen kann.

In den 50ern versuchte man das 17. Hilbertsche Problem konstruktiv zu lösen, was auf eine stückweise polynomiale Lösung führte. Diese war insofern unbefriedigend, als daß man, um eine Quadratsummendarstellung zu berechnen, zunächst einmal feststellen mußte, in welchem Bereich der Koeffizienten man sich befindet. Leider kann die stückweise polynomiale Lösung — wie Delzell in [11] zeigt — nicht zu einer polynomialen verbessert werden. Immerhin ist aber eine stetige Abhängigkeit der Koeffizienten möglich.

In dieser Diplomarbeit sollen nun einige Stetigkeitsaussagen rund um das 17. Hilbertsche Problem gesammelt und teilweise verallgemeinert werden. Die Arbeit ist in 5 Kapitel unterteilt. Im ersten Kapitel werden — neben einigen algebraischen — modelltheoretische Hifsmitteln zur Verfügung gestellt. Insbesondere wird in Abschnitt 2 der Endlichkeitssatz bewiesen, der in den drei Hauptsätzen in den Kapiteln 3 und 4 eine wichtige Rolle spielen wird. In Kapitel 2 werden Ergebnisse über Präpositivbereiche und Positivbereiche höherer Stufe auf Körpern und Ringen zusammengetragen. Das Kapitel gipfelt in einem Positivstellensatz, der in Kapitel 3 zwei Anwendungen in Verallgemeinerungen des 17. Hilbertschen Problems findet. Zum einen wird der Fall betrachtet, daß $f \geq 0$ auf einer basisoffenen semialgebraischen Menge gilt, zum andern werden Darstellungen als Summen höherer Potenzen untersucht. In beiden Fällen wird die Stetigkeit — auf geeigneten Teilmengen der Koeffizienten — bewiesen. Im vierten Kapitel werden zunächst gewöhnliche quadratische Formen und dann T-Formen zu einem Präpositivbereich T eingeführt und ein Repräsentationssatz dazu bewiesen. Der Hauptsatz in diesem Kapitel ist die stetige schwache Isotropie hyperbolischer quadratischer Formen. Betrachtet man dabei die Form $< 1, -f >$, so erhält man als Spezialfall wieder die Stetigkeit des 17. Hilbertschen Problems. In Kapitel 5 wird schließlich noch ein konstruktiver Beweis der Stetigkeit des 17. Hilbertschen Problems in einer Unbestimmten über den reellen Zahlen angegeben.

Herzlich danken möchte ich an dieser Stelle meinem Betreuer Prof. Dr. A. Prestel für die vielfache Hilfe und Unterstützung beim Entstehen dieser Arbeit, sowie T. Jacobi, der sich meine Arbeit durchgelesen hat und mir so einige nützliche Hinweise geben konnte.

Kapitel 1

Vorbemerkungen

1.1 Modelltheoretische Hilfsmittel

Die modelltheoretischen Begriffe und Symbole werden wie in [27] verwendet und daher nicht noch einmal im Einzelnen eingeführt. Zwischen den Elementen eines Modells und den entsprechenden Konstanten in der dazugehörenden Sprache wird allerdings in der Schreibweise nicht unterschieden.

Im Folgenden sei

$$L = (+, -, \cdot, <, 0, 1)$$

die Sprache der angeordneten Körper und R ein reell abgeschlossener Körper, d.h. eine L-Struktur, in der die Körperaxiome gelten, $<$ eine mit der Addition und Multiplikation verträgliche lineare Ordnung auf R ist, jedes Polynom ungeraden Grades eine Nullstelle in R hat und alle positiven Zahlen Quadrate sind.

Es gelten folgende zwei nützlichen Sätze, deren Beweis man z.B. in [27] Kapitel 4.2 findet:

Satz 1.1.1 (Quantorenelimination)
Zu jeder L-Formel φ gibt es eine quantorenfreie L-Formel ψ, deren freie Variabeln in denen von φ enthalten sind, so daß

$$R \models \forall(\varphi \leftrightarrow \psi)$$

gilt. D.h. die Theorie der reell abgeschlossenen Körper erlaubt Quantorenelimination.

Die Quantorenelimination ist äquivalent zur Substrukturvollständigkeit:

Satz 1.1.2 (Tarskiprinzip)
Sind R_1 und R_2 zwei reell abgeschlossene Körper, $A \subset R_1 \cap R_2$ eine Substruktur und ist φ eine L_A-Aussage, so gilt

$$R_1 \models \varphi \iff R_2 \models \varphi$$

Da sich $\mathbb{Q}$ in jeden reell abgeschlossenen Körper einbetten läßt, folgt daraus, daß die Theorie der reell abgeschlossenen Körper vollständig ist.

Bemerkung 1.1.3 Als eine weitere Konsequenz aus der Quantorenelimination erhält man, daß es zu jeder L_R-Formel φ mit freien Variabeln $x = (x_1, \ldots, x_n)$ Indizes $k, l \in \mathbb{N}$ und Elemente $q_i, p_{ij} \in R[X]$ gibt so daß

$$R \models \forall x(\varphi(x) \leftrightarrow \bigvee_{i=1}^{k} \left(q_i(x) = 0 \wedge \bigwedge_{j=1}^{l} p_{ij}(x) < 0 \right))$$

Denn: Jede quantorenfreie Formel kann man als endliche Disjunktion von Konjunktionen von Primformeln und negierten Primformeln schreiben. Da die L_R-Terme gerade in Polynome mit Koeffizienten in R umwandelbar sind, können die Primformeln in der Form

$$q(x) = 0 \qquad \text{oder} \qquad p(x) < 0$$

mit $p, q \in R[X]$ geschrieben werden. Die negierten Primformeln haben dann die äquivalente Gestalt

$$q(x) < 0 \vee -q(x) < 0 \qquad \text{oder} \qquad -p(x) < 0 \vee p(x) = 0$$

Berücksichtigt man nun noch, daß $q_1(x) = 0 \wedge \cdots \wedge q_k(x) = 0$ äquivalent ist zu $(q_1^2 + \cdots + q_k^2)(x) = 0$, so erhält man durch Ausklammern die gewünschte Form.

Definiert φ eine offene Teilmenge des R^n, so erhält man durch Komplementbildung aus dem im Folgenden beschriebenen Endlichkeitssatz, daß man sogar auf die q_i verzichten kann.

1.2 Endlichkeitssatz

Satz 1.2.1 (Endlichkeitssatz)
Ist $\varphi(x)$ eine L_R-Formel mit den freien Variabeln $x = (x_1, \ldots, x_n)$ und ist die Teilmenge $\{a \in R^n; R \models \varphi(a)\}$ in R^n abgeschlossen, so gibt es $k, l \in \mathbb{N}$ und $p_{ij} \in R[X]$ mit:

$$R \models \forall x(\varphi(x) \leftrightarrow \bigvee_{i=1}^{k} \bigwedge_{j=1}^{l} p_{ij}(x) \geq 0)$$

Zum Beweis des Satzes werden noch zwei Lemmata benötigt:

Lemma 1.2.2
Sei L eine Sprache, φ eine L-Aussage und seien Γ und Σ L-Aussagenmengen, so daß es $\gamma_0, \gamma_1 \in \Gamma$ mit der Eigenschaft

$$\Sigma \vdash \neg\gamma_0 \qquad \text{und} \qquad \Sigma \vdash \gamma_1$$

gibt. Gilt außerdem für alle Modelle $\mathfrak{A}, \mathfrak{B}$ von Σ, daß

$$\mathfrak{A} \overset{\Gamma}{\rightsquigarrow} \mathfrak{B} \quad \Longrightarrow \quad \mathfrak{A} \overset{\varphi}{\rightsquigarrow} \mathfrak{B}$$

dann ist φ modulo Σ äquivalent zu einer endlichen Disjunktion von Konjunktionen von Elementen aus Γ.

Einen Beweis dazu findet man in [27] Lemma 3.4.

Lemma 1.2.3
Seien R ein reell abgeschlossener Körper, $\mathcal{O}$ ein konvexer Bewertungsring von R mit maximalem Ideal $\mathfrak{M}$ und $\sigma : \mathcal{O} \to \mathcal{O}/\mathfrak{M}$ die Projektion. Ist dann $b \in \mathcal{O}^m$ ein Element mit $\mathbb{Z}[b] \overset{\sigma}{\cong} \mathbb{Z}[\overline{b}]$, so gibt es einen Schnitt $\rho : \mathcal{O}/\mathfrak{M} \to \mathcal{O}$, d.h. ρ ist ein ordnungserhaltender Monomorphismus mit $\sigma \circ \rho = \mathrm{id}_{\mathcal{O}/\mathfrak{M}}$, für den außerdem $\rho(\overline{b}) = b$ gilt.

Beweis: Jedes $\rho : \mathcal{O}/\mathfrak{M} \to \mathcal{O}$ mit $\sigma \circ \rho = \mathrm{id}_{\mathcal{O}/\mathfrak{M}}$ ist ordnungserhaltend, es bleibt also noch die Homomorphieeigenschaft zu zeigen. Da $\mathcal{O}$ ein konvexer Bewertungsring ist, ist $\mathbb{Q}(b) \subset \mathcal{O}$. Sei $\mathbb{Q}(\overline{b}) \subset K \subset \mathcal{O}/\mathfrak{M}$ ein maximaler Teilkörper, für den es einen Schnitt ρ gibt.
Ann: $K \neq \mathcal{O}/\mathfrak{M}$.
Sei dann $r \in \mathcal{O}$ mit $\overline{r} \in \mathcal{O}/\mathfrak{M} \setminus K$.

1. Fall: $\overline{r}$ ist transzendent über K. Dann ist auch r transzendent über $\rho(K)$ und man kann $\rho(\overline{r}) := r$ setzen.

2. Fall: $\overline{r}$ ist algebraisch über K. Sei dann $f \in \mathcal{O}[X]$, so daß $\overline{f}$ das Minimalpolynom von $\overline{r}$ über K ist. Wegen $\mathrm{char} K = 0$ hat $\overline{f}$ nur einfache Nullstellen, also wechselt $\overline{f}$ an der Stelle $\overline{r}$ im reell abgeschlossenen Körper $\mathcal{O}/\mathfrak{M}$ das Vorzeichen. In einer Umgebung von $\overline{r}$ gilt daher ohne Einschränkung $f(\overline{s}) < 0$ für $\overline{s} < \overline{r}$ und $f(\overline{t}) > 0$ für $\overline{t} > \overline{r}$, woraus $f(s) < 0$ und $f(t) > 0$ folgt. Nach dem Zwischenwertsatz gibt es dann ein $r' \in r + \mathfrak{M}$ mit $f(r') = 0$. Man setze also $\rho(\overline{r}) := r'$.

Damit ist eine Erweiterung von ρ auf $K(\overline{r})$ gefunden worden im Widerspruch zur Maximalität von K. □

Damit kann nun der Endlichkeitssatz bewiesen werden:

Beweis: von Satz 1.2.1.
Zunächst wird die L_R-Formel $\varphi(x)$ durch eine L-Formel $\varphi(x,y)$ ersetzt, wobei $y = (y_1, \ldots, y_m)$ für die endlich vielen in φ vorkommenden Konstanten aus R steht. Mit $z = (z_1, \ldots, z_n)$ sei

$$\psi(y) := \forall x(\neg\varphi(x,y) \to \exists\epsilon(\epsilon > 0 \wedge \forall z(||x - z||^2 < \epsilon \to \neg\varphi(z,y))))$$

Dann drückt $\psi(b)$ aus, daß die durch $\varphi(x,b)$ definierte Menge abgeschlossen ist. Sei

$$\Gamma(x,y) = \{0 \leq p(x,y); p \in \mathbb{Z}[X,Y]\} \cup \{0 \neq q(y); q \in \mathbb{Z}[Y] \setminus \{0\}\}$$

Nun soll Lemma 1.2.2 auf folgende Situation angewandt werden:

- Die Sprache sei $L(a,b)$ mit $a \in R^n$ und $b \in R^m$.
- In Σ seien die Axiome eines reell abgeschlossenen Körpers zusammen mit $\psi(b)$.
- $\Gamma = \Gamma(a,b)$ mit $\gamma_0 : 0 \neq 0$ und $\gamma_1 : 0 \neq 1$
- $\varphi = \varphi(a,b)$

Um die Voraussetzungen von Lemma 1.2.2 nachzuprüfen, seien (R,a,b) und (R',a',b') zwei Modelle von Σ und es gelte sowohl $(R,a,b) \overset{\Gamma}{\rightsquigarrow} (R',a',b')$ als auch $(R,a,b) \models \varphi$. Dann bleibt noch zu zeigen: $(R',a',b') \models \varphi$.

Dazu sei $A \subset R$ der von a und b und $A' \subset R'$ der von a' und b' erzeugte Ring. Wegen $(R,a,b) \overset{\Gamma}{\rightsquigarrow} (R',a',b')$ wird durch $a \mapsto a', b \mapsto b'$ ein ordnungstreuer Ringhomomorphismus $\sigma : A \to A'$ induziert, der eingeschränkt auf $\mathbb{Z}[b]$ einen Isomorphismus auf $\mathbb{Z}[b']$ liefert.

Sei $\mathfrak{P}$ der Kern von σ und $\mathcal{O}$ die konvexe Hülle von $A_\mathfrak{P}$ in R. Dann ist $\mathcal{O}$ ein Bewertungsring von R. Sei ferner $\mathfrak{M}$ das maximale Ideal von $\mathcal{O}$ und $R'' = \mathcal{O}/\mathfrak{M}$. Dann ist R'' reell abgeschlossen und es wird sich folgende Situation ergeben:

$$\begin{tikzcd}
(R,a,b) \arrow[d, dash] & & (R',a',b') \\
\mathcal{O} \arrow[d, dash] & R'' = \mathcal{O}/\mathfrak{M} \arrow[l, hook', "\rho"'] \arrow[d, dash] & \\
A_\mathfrak{P} \arrow[d, dash] \arrow[r, two heads, "\sigma"] & \mathrm{Quot}(A') \arrow[d, dash] & \\
(A,a,b) \arrow[d, dash] \arrow[r, two heads, "\sigma"] & (A',a',b') \arrow[d, dash] \arrow[uuur, dash] & \\
\mathbb{Z}[b] \arrow[r, "\cong"] & \mathbb{Z}[b'] &
\end{tikzcd}$$

A' läßt sich in R'' einbetten: Dazu ist zu zeigen, daß die Projektion von $\mathcal{O}$ auf $\mathcal{O}/\mathfrak{M}$ eine Fortsetzung von σ ist. Zunächst läßt sich σ durch $\sigma\left(\frac{r}{s}\right) := \frac{\sigma(r)}{\sigma(s)}$ für $r \in A$ und $s \in A \setminus \mathfrak{P}$ auf $A_\mathfrak{P}$ fortsetzen und es gilt $\sigma(A_\mathfrak{P}) = \mathrm{Quot}(A')$ und $\ker\sigma = \mathfrak{P}A_\mathfrak{P}$. Es bleibt also $\mathfrak{M} \cap A_\mathfrak{P} = \mathfrak{P}A_\mathfrak{P}$ zu zeigen, woraus nach dem Homomorphiesatz die Isomorphie $A_\mathfrak{P}/\mathfrak{M} \cong \mathrm{Quot}A'$ folgt.

"$\subset$" Da $\mathfrak{M}$ keine Einheiten enthalten kann, ist $\mathfrak{M} \cap A_\mathfrak{P} \subsetneq A_\mathfrak{P}$. Da $\mathfrak{P}A_\mathfrak{P}$ das einzige maximale Ideal von $A_\mathfrak{P}$ ist, muß also $\mathfrak{M} \cap A_\mathfrak{P}$ darin enthalten sein.

"$\supset$" Sei $p \in \mathfrak{P}, r \in A \setminus \mathfrak{P}$ und sei ohne Einschränkung $0 < p, r$.
Ann: $\frac{p}{r} \notin \mathfrak{M}$.
Dann ist $\frac{r}{p} \in \mathcal{O}$, d.h. es gibt $s \in A$ und $t \in A \setminus \mathfrak{P}$ mit $0 < s, t$ und $0 < \frac{r}{p} \leq \frac{s}{t}$, woraus

$$0 < rt \leq ps \in \mathfrak{P}$$

folgt. Da σ ordnungserhaltend ist, ist $\mathfrak{P}$ aber konvex, also gilt $rt \in \mathfrak{P}$, woraus $r \in \mathfrak{P}$ oder $t \in \mathfrak{P}$ folgt, im Widerspruch zur Wahl von r und t.

Sei nun nach Lemma 1.2.3 ρ ein Schnitt zu σ.

Ann.: $(R', a', b') \models \neg\varphi$.
Mit dem Tarskiprinzip folgt dann $(R'', a', b') \models \neg\varphi$ und man erhält durch Anwenden von ρ auch $(\rho(R''), \rho(a'), b) \models \neg\varphi$. Da (R', a', b') ein Modell von Σ und damit von $\psi(b')$ ist, folgt analog $(\rho(R''), \rho(a'), b) \models \psi(b)$. Also gibt es ein $\epsilon \in R''$ mit $\epsilon > 0$ und

$$\rho(R'') \models \forall x(||x - \rho(a')|| < \rho(\epsilon) \to \neg\varphi(x, b))$$

Nach dem Tarskiprinzip erhält man dann auch

$$R \models \forall x(||x - \rho(a')|| < \rho(\epsilon) \to \neg\varphi(x, b))$$

Da außerdem $R \models \varphi(a, b)$ gilt, folgt damit $R \models ||a - \rho(a')|| \geq \rho(\epsilon)$, woraus man durch Anwenden von σ

$$||\sigma(a) - a'|| \geq \epsilon > 0$$

erhält im Widerspruch zu $a' = \sigma(a)$.

□

Einen anderen Beweis des Endlichkeitssatzes findet man in [8] Kapitel 2.7 Theorem 2.7.1.

1.3 Weitere Hilfsmittel

In diesem Abschnitt werden in loser Folge noch einige weitere Sätze und Lemmata erwähnt, die später benötigt werden.

Lemma 1.3.1
Sei A ein kommutativer Ring und S eine multiplikativ abgeschlossene Teilmenge von A. Ist dann $\mathfrak{A}$ ein Ideal von A, das im Komplement von S enthalten ist, so gibt es ein Primideal $\mathfrak{P}$ von A mit $A \setminus S \supset \mathfrak{P} \supset \mathfrak{A}$.

Beweis: Sei $\mathfrak{P}$ ein maximales Ideal mit der Eigenschaft $A \setminus S \supset \mathfrak{P} \supset \mathfrak{A}$ (die Existenz liefert Zorns Lemma).
Beh: $\mathfrak{P}$ ist ein Primideal.
Ann: Es gibt $a, b \in A \setminus \mathfrak{P}$ mit $ab \in \mathfrak{P}$.
Wegen der Maximalität von $\mathfrak{P}$ gilt dann $(\mathfrak{P} + aA) \cap S \neq \emptyset$ und $(\mathfrak{P} + bA) \cap S \neq \emptyset$.
Seien also $a_1, b_1 \in \mathfrak{P}$ und $a_2, b_2 \in A$ mit $s := a_1 + aa_2 \in S$ und $r := b_1 + bb_2 \in S$.
Dann gilt $rs = a_1a_2 + aa_2b_1 + bb_2a_1 + aba_2b_2 \in \mathfrak{P}$ im Widerspruch zu S multiplikativ abgeschlossen und $\mathfrak{P} \subset A \setminus S$. □

Lemma 1.3.2
Für einen kommutativen Ring A mit Eins und eine ganze Ringerweiterung B über A gilt:

1. $B^\times \cap A \subset A^\times$
2. *Ist B ein lokaler Ring mit maximalem Ideal $\mathfrak{M}$ und $\mathfrak{A} \subsetneqq A$ ein Ideal von A, so gilt $\mathfrak{A} \subset \mathfrak{M}$.*

Beweis:

1. Seien $a \in B^\times \cap A$ und $b \in B$ mit $ab = 1$, sowie $a_0, \ldots, a_{n-1} \in A$ mit $b^n + a_{n-1}b^{n-1} + \cdots + a_0 = 0$. Multiplikation mit a^{n-1} und auflösen nach b liefert $b = -a_{n-1} - \cdots - a_0 a^{n-1} \in A$.
2. Sei $a \in \mathfrak{A}$, so ist $a \notin A^\times$. Wegen dem eben bewiesenen ist dann auch $a \notin B^\times$. Da B ein lokaler Ring ist, gilt $\mathfrak{M} = B \setminus B^\times$ also folgt $a \in \mathfrak{M}$.

□

Bemerkung 1.3.3 Sei K ein Körper mit einem Absolutbetrag $|\ |$ und sei $f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in K[X]$ ein normiertes Polynom vom Grad n. Sei ferner $a \in K$ eine Nullstelle von f mit $|a| \geq 1$. Dann gilt

$$|a| \leq \sum_{i=0}^{n-1} |a_i|$$

Denn: $0 = a^{-(n-1)} f(a) = a + \sum_{i=0}^{n-1} a_i \frac{1}{a^{n-1-i}}$. Daraus folgt:

$$\begin{aligned} |a| &= |-\sum_{i=0}^{n-1} a_i \frac{1}{a^{n-1-i}}| \\ &\leq \sum_{i=0}^{n-1} |a_i| |\frac{1}{a^{n-1-i}}| \\ &\leq \sum_{i=0}^{n-1} |a_i| \end{aligned}$$

da mit $|a| \geq 1$ auch $|\frac{1}{a^{n-1-i}}| \leq 1$ für $0 \leq i \leq n-1$.

Satz 1.3.4
Die Nullstellen eines Polynoms über $\mathbb{C}$ hängen stetig von dessen Koeffizienten ab, d.h. ist $\sim$ die durch

$$(a_1, \ldots, a_n) \sim (b_1, \ldots, b_n) :\Longleftrightarrow \exists \sigma \in S_n \bigwedge_{i=1}^{n} a_i = b_{\sigma i}$$

definierte Äquivalenzrelation auf $\mathbb{C}^n$ *und bezeichnet* $[(a_1, \ldots, a_n)]$ *die Äquivalenzklasse von* $(a_1, \ldots, a_n) \in \mathbb{C}^n$, *so ist die Abbildung*

$$\begin{array}{rcl} \{(a_0, \ldots, a_n) \in \mathbb{C}^{n+1}; a_n \neq 0\} & \longrightarrow & \mathbb{C}^n / \sim \\ (a_0, \ldots, a_n) & \longmapsto & [(\lambda_1, \ldots, \lambda_n)] \end{array}$$

mit $\sum_{i=0}^n a_i X^i = a_n \prod_{i=1}^n (X - \lambda_i)$ *stetig.*

Einen Beweis dazu findet man zum Beispiel in [9] oder in [31] Theorem 4.5.

Lemma 1.3.5
Sei $\sim$ *wie in Satz 1.3.4 definiert. Dann ist die Quotientenabbildung*

$$\begin{array}{rccc} \pi: & \mathbb{C}^n & \longrightarrow & \mathbb{C}^n / \sim \\ & (a_1, \ldots, a_n) & \longmapsto & [(a_1, \ldots, a_n)] \end{array}$$

eine abgeschlossene Abbildung.

Beweis: Sei $A \subset \mathbb{C}^n$ abgeschlossen. Für $x = (x_1, \ldots, x_n) \in \mathbb{C}^n$ und $\sigma \in S_n$ sei $\sigma x := (x_{\sigma 1}, \ldots, x_{\sigma n})$. Dann ist σ ein Vektorraumisomorphismus auf einem endlichdimensionalen Vektorraum über $\mathbb{R}$ und damit ein Homöomorphismus. Folglich ist mit A auch σA umd damit $\pi^{-1}\pi(A) = \bigcup_{\sigma \in S_n} \sigma A$ in $\mathbb{C}^n$ abgeschlossen, was die Abgeschlossenheit von $\pi(A)$ in $\mathbb{C}^n / \sim$ impliziert. $\square$

Kapitel 2

Positivbereiche höherer Stufe

In diesem Kapitel werden die grundlegenden Definitionen und Sätze im Zusammenhang mit Präpositivbereichen und Positivbereichen (höherer Stufe) eingeführt. Dabei ist Abschnitt 2 eine Vorbereitung für Satz 2.3.7 in Abschnitt 3, der im Beweis der stetigen Darstellung als Summen $2m$-ter Potenzen Verwendung findet. Die Abschnitte 4 und 5 sind eine Vorbereitung für den in Abschnitt 6 bewiesenen Positivstellensatz.

Die Abschnitte 1 bis 3 sind an den Abschnitten 1 und 2 von [4] orientiert. Die Abschnitte 4 und 5 sind an die Abschnitte 1 und 2 von [5] angelehnt und Abschnitt 6 ist [7] entnommen.

2.1 Summen 2m-ter Potenzen

Definition 2.1.1
Eine Teilmenge P eines Ringes A mit Eins heißt **Präprimstelle**, wenn folgende Bedingungen erfüllt sind:

$$\begin{aligned} P + P &\subset P \\ P \cdot P &\subset P \\ 0, 1 \in P, -1 &\notin P \end{aligned}$$

Definition 2.1.2
Eine Präprimstelle P eines Körpers K heißt **Präpositivbereich n-ter Stufe** für ein $n \in \mathbb{N}$, falls gilt:

$$K^n \subset P$$

P heißt **vollständig**, falls

$$a^2 \in P \Rightarrow a \in P \cup -P$$

Bemerkung 2.1.3 Es gibt nur Präpositivbereiche gerader Stufe und nur von Körpern mit char$K = 0$.

Denn: Ist n ungerade, so müßte gleichzeitig $-1 \notin P$ und $-1 = (-1)^n \in P$ gelten. Ist char$K = p$, so müßte ebenfalls $-1 = (p-1)1^n \in P$ gelten.

Bemerkung 2.1.4 Ist P ein Präpositivbereich n-ter Stufe eines Körpers K, so ist $P^\times := P \setminus \{0\}$ eine Untergruppe von $K^\times$.

Denn: Ist $a \in P^\times$, so folgt

$$\frac{1}{a} = a^{n-1}\left(\frac{1}{a}\right)^n \in P$$

Bemerkung 2.1.5 Ist P ein Präpositivbereich n-ter Stufe eines Körpers K und $a \in K$ ein Element für das $a^2 \in P$ und $a \notin -P$ gilt, so ist $P[a] := P + Pa$ wieder ein Präpositivbereich n-ter Stufe.

Denn: $P[a]$ ist ein Halbring mit $0, 1 \in P \subset P[a]$ und $K^n \subset P \subset P[a]$.
Ann: $-1 \in P[a]$. Seien also $u, v \in P$ mit $-1 = u + va$. Dann folgt $v \neq 0$, da sonst schon $-1 \in P$ gelten würde. Nach der letzten Bemerkung folgt daraus $v^{-1} \in P$ und damit $a = -v^{-1}(1+u) \in -P$ im Widerspruch zur Voraussetzung.

Lemma 2.1.6
Ist P ein Präpositivbereich n-ter Stufe eines Körpers K und gibt es ein $x \in K$ mit $x \notin P \cup -P$ und $x^2 \in P$, so gilt:

$$P = \bigcap_{\substack{a \notin P \cup -P \\ a^2 \in P}} P[a]$$

Beweis:
"$\subset$": klar
"$\supset$": Sei $b \in \bigcap P[a]$. Gilt $a \notin P \cup -P$ und $a^2 \in P$ für ein $a \in K$, so gilt dies auch für $-a$. Damit folgt also $b \in P[a] \cap P[-a]$ für alle $a \notin P \cup -P$ mit $a^2 \in P$. Sei also nun so ein a gewählt und seien dazu $\alpha, \beta, \gamma, \delta \in P$ mit

$$b = \alpha + \beta a \tag{2.1}$$
$$b = \gamma - \delta a \tag{2.2}$$

$\gamma\delta\ (2.1)^2 + \alpha\beta\ (2.2)^2$ ergibt dann:

$$\gamma\delta b^2 + \alpha\beta b^2 = \gamma\delta(\alpha^2 + \beta^2 a^2) + \alpha\beta(\gamma^2 + \delta^2 a^2) \in P$$

1. Fall: $\gamma\delta + \alpha\beta = 0$
   Wegen $\gamma\delta, \alpha\beta \in P$,$-1 \notin P$ und Bemerkung 2.1.4 folgt dann $\gamma\delta = \alpha\beta = 0$. Daraus ergeben sich die vier Fälle:

$$\begin{aligned}
\alpha = \gamma = 0 &\implies b \in Pa \cap -Pa \\
\beta = \gamma = 0 &\implies b \in P \ \cap -Pa \\
\alpha = \delta = 0 &\implies b \in Pa \cap \ P \\
\beta = \delta = 0 &\implies b \in P \ \cap \ P
\end{aligned}$$

Damit ist $b \in (Pa \cap -Pa) \cup (P \cap -Pa) \cup (Pa \cap P) \cup (P \cap P) = P$, da $P \cap -P = \{0\}$ und $a \notin P \cup -P$.

2. Fall: $\gamma\delta + \alpha\beta \neq 0$
Dann folgt mit Bemerkung 2.1.4 daß $b^2 \in P$.
Ann: $b \notin P$. Sowieso gilt $b \notin -P$, denn sonst wäre $\delta a = \gamma - b \in P$ und damit auch $a \in P$ im Widerspruch zur Wahl von a. Also gilt $b \notin P \cup -P$ und $b^2 \in P$. Wie oben gilt dies dann auch für $-b$ und damit folgt

$$b \in \bigcap_{\substack{a \notin P \cup -P \\ a^2 \in P}} P[a] \subset P[-b]$$

Es gibt also $\alpha, \beta \in P$ mit $b = \alpha - \beta b$. Daraus folgt $b(1+\beta) = \alpha$ und mit $1 + \beta \in P^\times$ schließlich $b \in P$ im Widerspruch zur Annahme.

In beiden Fällen hat man damit $b \in P$. □

Satz 2.1.7
Sei $m \in \mathbb{N}$ und P' ein Präpositivbereich $2m$-ter Stufe eines Körpers K. Dann gilt:

1. *Es gibt einen vollständigen Präpositivbereich $2m$-ter Stufe P von K mit $P' \subset P$.*

2. *Sei $\mathcal{P} = \{P \subset K; P$ vollständiger Präpositivbereich $2m$ - ter Stufe mit $P' \subset P\}$. Dann gilt:*

$$P' = \bigcap \mathcal{P}$$

Beweis:

1. Sei $P \subset K$ ein maximaler Präpositivbereich $2m$-ter Stufe mit der Eigenschaft $P' \subset P$. (Die Existenz garantiert Zorns Lemma).
Beh: P ist vollständig.
Ann: Es gibt ein $a \in K$ mit $a^2 \in P$ und $a \notin P \cup -P$.
Mit Bemerkung 2.1.5 folgt dann, daß $P[a]$ ein Präpositivbereich $2m$-ter Stufe ist. Wegen $a \notin P$ folgt aber $P[a] \supsetneqq P$ im Widerspruch zur Maximalität von P.

2. Wegen Punkt 1 ist $\mathcal{P}$ nicht leer.
"$\subset$": klar
"$\supset$": Sei $T = \bigcap \mathcal{P}$
Ann: Es gibt ein $a \in T$ mit $a \notin P'$.
Sei $P' \subset R \subset K$ ein maximaler Präpositivbereich $2m$-ter Stufe mit der Eigenschaft $a \notin R$ (Seine Existenz liefert wieder Zorns Lemma). Dann

gibt es ein $b \in R$ mit $b^2 \in R$ und $b \notin R \cup -R$ (Sonst wäre R vollständig, d.h. $R \in \mathcal{P}$. Also gilt $a \notin R \supset T$ im Widerspruch zu $a \in T$.)
Damit sind die Voraussetzungen von Lemma 2.1.6 erfüllt und es gilt

$$R = \bigcap_{\substack{b \notin R \cup -R \\ b^2 \in R}} R[b]$$

Wegen $R \subsetneqq R[b]$ und Bemerkung 2.1.5 folgt aus der Maximalität von R, daß $a \in R[b]$ für alle diese b gilt. Daraus folgt

$$a \in \bigcap_{\substack{b \notin R \cup -R \\ b^2 \in R}} R[b] = R$$

im Widerspruch zur Wahl von R.

□

Korollar 2.1.8
Ist P' ein Präpositivbereich $2m$ - ter Stufe eines Körpers K und $a \in K$ ein Element mit $a \notin P'$, dann gibt es einen vollständigen Präpositivbereich $2m$-ter Stufe P mit $P' \subset P$ und $a \notin P$.

Beweis: Sei $\mathcal{P} = \{P \subset K; P$ ein vollständiger Präpositivbereich $2m$ - ter Stufe mit $P' \subset P\}$ wie in Satz 2.1.7.
Ann: $a \in P$ für alle $P \in \mathcal{P}$.
Dann wäre $a \in \bigcap \mathcal{P} = P'$ (wobei das letzte Gleichheitszeichen aus Satz 2.1.7 (2) folgt) im Widerspruch zu $a \notin P'$. □

2.2 Stone - Ringe

Definition 2.2.1
Sind A ein Ring mit Eins und $P \subset A$ eine Teilmenge, so heißt das Paar (A, P) **Stone-Ring**, falls es folgende Eigenschaften erfüllt:

1. P ist eine Präprimstelle von A
2. $P \cap -P = \{0\}$
3. $\bigwedge_{a \in A} \bigvee_{n \in \mathbb{N}} n \cdot 1 - a \in P$
4. $\bigwedge_{a \in A} [\bigwedge_{n \in \mathbb{N}} 1 + na \in P \Rightarrow a \in P]$

Definition 2.2.2
Sind (A_1, P_1), (A_2, P_2) zwei Stone-Ringe so heißt ein injektiver Ringhomomorphismus

$$\phi : A_1 \longrightarrow A_2$$

Einbettung von (A_1, P_1) in (A_2, P_2), falls $P_1 = \phi^{-1}(P_2)$ gilt.

Satz 2.2.3 (Darstellungssatz von Kadison-Dubois)
Für jeden Stone-Ring (A, P) gibt es einen kompakten Hausdorffraum X, so daß man (A, P) in $(C(X), C(X)^+)$ einbetten kann. Dabei sind:

$$\begin{aligned} C(X) &= \{f : X \longrightarrow \mathbb{R}; f \text{ stetig}\} \\ C(X)^+ &= \{f \in C(X); \bigwedge_{x \in X} f(x) \geq 0\} \end{aligned}$$

Beweis siehe [14]. Einen rein algebraischen Beweis findet man auch in [6].

Korollar 2.2.4
In einem Stone-Ring (A, P) gilt:

1. *Die Quadrate liegen in P.*
2. *Für $n \in \mathbb{N}$ ungerade gilt $a^n \in P \Rightarrow a \in P$.*
3. *Es gibt keine nilpotenten Elemente außer 0.*

Beweis: Sei nach 2.2.3 X ein kompakter Hausdorffraum und ϕ eine Einbettung von (A, P) in $((C(X), C(X)^+)$.

1. Sei $a \in A$. Dann gilt $\phi(a^2)(x) = (\phi(a))^2(x) \geq 0$ für alle $x \in X$. D.h. $\phi(a^2) \in C(X)^+$ und damit $a^2 \in \phi^{-1}(C(X)^+) = P$.

Mit den gleichen Argumenten lassen sich auch 2 und 3 beweisen. □

2.3 Bewertungsringe und Präprimstellen

Definition 2.3.1
Ein Bewertungsring $\mathcal{O}$ eines Körpers K heißt mit einer Präprimstelle P des Körpers **verträglich**, falls für das maximale Ideal $\mathfrak{M}$ von $\mathcal{O}$ gilt:

$$1 + \mathfrak{M} \subset P$$

Definition 2.3.2
Sei P ein vollständiger Präpositivbereich $2m$ -ter Stufe eines Körpers K. Dann seien

$$\begin{aligned} \mathcal{O}(P) &:= \{a \in K; \bigvee_{n \in \mathbb{N}} n \pm a \in P\} \\ \mathfrak{M}(P) &:= \{a \in K; \bigwedge_{n \in \mathbb{N}} \frac{1}{n} \pm a \in P\} \\ \mathrm{Arch}(P) &:= \{a \in \mathcal{O}(P); \bigwedge_{n \in \mathbb{N}} \frac{1}{n} + a \in P\} \end{aligned}$$

Ist klar welcher Präpositivbereich gemeint ist, so bezeichnen $\mathcal{O}$, $\mathfrak{M}$ und Arch die Mengen $\mathcal{O}(P)$, $\mathfrak{M}(P)$ und $\mathrm{Arch}(P)$.

Ziel dieses Abschnittes ist es nun zu zeigen, daß $\mathcal{O}(P)$ ein mit P verträglicher Bewertungsring ist und die von P auf $\mathcal{O}/\mathfrak{M}$ induzierte Ordnung sogar archimedisch ist. Dies wird in Satz 2.3.7 geschehen. Zunächst sind dazu aber noch einige Vorbereitungen nötig.

Lemma 2.3.3
Für einen vollständigen Präpositivbereich $2m$-ter Stufe P eines Körpers K gilt

1. *$\mathcal{O}(P)$ ist ein Ring mit $\mathbb{Q} \subset \mathcal{O}(P)$.*
2. *$\mathfrak{M}(P)$ ist ein Ideal von $\mathcal{O}(P)$.*
3. *$\mathrm{Arch}(P)$ ist eine Präprimstelle von $\mathcal{O}(P)$.*
4. *$x \in \mathcal{O}(P)$, $x + \mathfrak{M} \in \{a + \mathfrak{M}; a \in \mathrm{Arch}(P)\} \Rightarrow x \in \mathrm{Arch}(P)$.*

Beweis:

1. Seien $n_i \in \mathbb{N}$, $a_i \in K$ mit $n_i \pm a_i \in P$ für $i = 1, 2$. Dann gilt:

   $+$: $(n_1 + n_2) \pm (a_1 + a_2) \in P$
   $\cdot$: $n_1 n_2 \pm a_1 a_2 = \frac{1}{2}((n_1 + a_1)(n_2 \pm a_2) + (n_1 - a_1)(n_2 \mp a_2)) \in P$
   $-$: klar
   0,1 : $1 \pm 0 = 1 \in P$, $2 \pm 1 = 3$ bzw $1 \in P$
   $\mathbb{Q} \subset \mathcal{O}$: Aus $1 \in \mathcal{O}$ folgt $\mathbb{Z} \subset \mathcal{O}$ und für $k \in \mathbb{N}$ gilt $1 \pm \frac{1}{k} \in \mathbb{Q}^+ \subset P$. Also folgt $\mathbb{Q} \subset \mathcal{O}$.

2. Für $i = 1, 2$ seien $a_i, a \in K$ und $n_0 \in \mathbb{N}$ so daß $\frac{1}{n} \pm a_i \in P$ für alle $n \in \mathbb{N}$ und $n_0 \pm a \in P$ gilt. Damit erhält man für alle $n \in \mathbb{N}$

   $+$: $\frac{1}{n} \pm (a_1 + a_2) = \frac{1}{2n} \pm a_1 + \frac{1}{2n} \pm a_2 \in P$
   $\cdot$: $\frac{1}{n} \pm a_1 a = \frac{1}{2}((\frac{1}{n_0 n} + a_1)(n_0 \pm a) + (\frac{1}{n_0 n} - a_1)(n_0 \mp a)) \in P$

$\mathfrak{M} \subset \mathcal{O}$: Gilt $\frac{1}{n} \pm a \in P$ für alle $n \in \mathbb{N}$, so insbesondere auch für 1, d.h. $1 \pm a \in P$.

3. Für $i = 1,2$ seien $a_i \in K$ und $n_i \in \mathbb{N}$ so daß $\frac{1}{n} + a_i \in P$ für alle $n \in \mathbb{N}$ und $n_i \pm a_i \in P$ gilt. Dann:

   $+$: Für alle $n \in \mathbb{N}$ gilt $\frac{1}{n} + (a_1 + a_2) = \frac{1}{2n} + a_1 + \frac{1}{2n} + a_2 \in P$

   $\cdot$: Sei $r \in \mathbb{N}$ mit $\frac{1}{n} > \frac{n_1 n_2}{r^2} + \frac{2n_1 n_2}{r}$. Sei also $q = \frac{1}{n} - \frac{n_1 n_2}{r^2} + \frac{2n_1 n_2}{r} \in \mathbb{Q}^+$. Dann gilt $\frac{1}{n} + a_1 a_2 = \frac{n_1 n_2}{r^2} + \frac{2n_1 n_2}{r} + q + a_1 a_2 = (\frac{n_1}{r} + a_1)(\frac{n_2}{r} + a_2) + \frac{n_1}{r}(n_2 - a_2) + \frac{n_2}{r}(n_1 - a_1) + q \in P$

   0,1 : Für alle $n \in \mathbb{N}$ gilt $\frac{1}{n} + 0$, $\frac{1}{n} + 1 \in \mathbb{Q}^+ \subset P$

   -1 : Wäre $-1 \in$ Arch, so wäre $2(\frac{1}{2} + (-1)) = -1 \in P$ im Widerspruch zu P Präpositivbereich.

4. Sei $a \in$ Arch, d.h. für alle $n \in \mathbb{N}$ gelte $\frac{1}{n} + a \in P$. Sei $x \in \mathcal{O}$ mit $x + \mathfrak{M} = a + \mathfrak{M}$, d.h. für alle $n \in \mathbb{N}$ sei $\frac{1}{n} \pm (x - a) \in P$. Dann folgt für alle $n \in \mathbb{N}$, daß $\frac{1}{n} + x = (\frac{1}{2n} + a) + (\frac{1}{2n} + (x - a)) \in P$. Also folgt $x \in$ Arch.

□

Lemma 2.3.4
Zu einem vollständigen Präpositivbereich 2m-ter Stufe P eines Körpers K ist

$$(\mathcal{O}(P)/\mathfrak{M}(P), \mathrm{Arch}(P)/\mathfrak{M}(P))$$

ein Stone-Ring.

Beweis: Es müssen noch die Eigenschaften 2 - 4 eines Stone-Rings nachgeprüft werden:

2. Arch $\cap$ -Arch $\subset \mathfrak{M}$ ist klar nach Definition von Arch und $\mathfrak{M}$.

3. Sei $a \in \mathcal{O}$, d.h. es gibt ein $n_0 \in \mathbb{N}$ mit $n_0 \pm a \in P$. Dann gilt $\frac{1}{n} + n_0 - a \in P$ für alle $n \in \mathbb{N}$, also $n_0 - a \in$ Arch.

4. Sei $a \in \mathcal{O}$ und für alle $n \in \mathbb{N}$ sei $1 + na \in$ Arch. Dann folgt $\frac{1}{n} + a = \frac{1}{1+n}(\frac{1}{n} + (1 + (n+1)a)) \in P$, und damit $a \in$ Arch.

□

Korollar 2.3.5
Für einen vollständigen Präpositivbereich 2m-ter Stufe P eines Körpers K gilt:

$$\bigwedge_{a \in \mathcal{O}(P)} \bigwedge_{n \in \mathbb{N}} \frac{1}{n} + a^2 \in P \tag{2.3}$$

$$\bigwedge_{a \in \mathcal{O}(P)} [\bigvee_{n \in \mathbb{N}} n \text{ ungerade}, a^n \in \mathrm{Arch}(P) \Rightarrow a \in \mathrm{Arch}(P)] \tag{2.4}$$

$$\mathfrak{M}(P) = \mathrm{Rad}(\mathfrak{M}(P)) \tag{2.5}$$

Beweis: Das Korollar folgt sofort aus Lemma 2.3.4 und Korollar 2.2.4 unter Berücksichtigung von 4 in Lemma 2.3.3. □

Lemma 2.3.6 (vgl. [15] Theorem 402 auf Seite 325)
Es gilt:

$$n!X = \sum_{h=0}^{n-1} (-1)^{n-1-h} \binom{n-1}{h} [(X+h)^n - h^n] \tag{2.6}$$

Beweis: Zu einem Polynom $q(X) = a_n X^n + \cdots + a_0$ sei die Differenz $\Delta q(X) := q(X+1) - q(X)$ definiert. Durch Induktion über k folgt dann, daß $\Delta^k q(X) = n \cdot \cdots \cdot (n-k+1) a_n X^{n-k} + q_k(X)$ mit $\deg q_k < n-k$ gilt. Ist nun speziell $q(X) = X^n$, so sieht man wieder durch Induktion über k, daß $\Delta^k q(X) = \sum_{h=0}^{k-1} (-1)^{k-1-h} \binom{k-1}{h} (X+h)^k$ ist. Insgesamt erhält man also:

$$\sum_{h=0}^{n-1} (-1)^{n-1-h} \binom{n-1}{h} (X+h)^n = \Delta^k X^n = n!X + c$$

mit einer Konstanten c. Bringt man nun noch den Ausdruck für c, den man durch $X = 0$ erhält, auf die linke Seite, so erhält man die behauptete Gleichung. □

Satz 2.3.7
Zu einem vollständigen Präpositivbereich 2m-ter Stufe P eines Körpers K ist $\mathcal{O}(P)$ ein mit P verträglicher Bewertungsring und $\overline{P} := (P \cap \mathcal{O}(P))/\mathfrak{M}(P)$ ist ein archimedischer Positivbereich von $k := \mathcal{O}(P)/\mathfrak{M}(P)$.

Beweis: Der Beweis ist in 5 Behauptungen unterteilt.

1. Beh: $\mathcal{O} = \text{Arch} \cup \text{-Arch}$
   "$\supset$": klar
   "$\subset$": Sei $a \in \mathcal{O}$
   1. Fall: $a \in P \cup -P$.
   Wegen $\mathcal{O} \cap P \subset \text{Arch}$ folgt dann auch $a \in \text{Arch} \cup \text{-Arch}$.

   2. Fall: $a \notin P \cup -P$.

   (a) Sei zunächst a so gewählt, daß es ein $r \geqq 1$ gibt mit $a^{2^r} \in P$. Da P vollständig ist folgt $a^{2^{r-1}} \in P \cup -P$. Angenommen für alle $1 \leqq k \leqq r$ gilt $a^{2^k} \in P$. Dann würde insbesondere $a \in P \cup -P$ folgen, im Widerspruch zur Wahl von a. Sei also $k \in \mathbb{N}$ mit $a^{2^k} \in -P$. Damit folgt $\frac{1}{n} - a^{2^k} \in P$ für alle $n \in \mathbb{N}$. Außerdem folgt aus (2.3) sowieso $\frac{1}{n} + a^{2^k} \in P$ für alle $n \in \mathbb{N}$, insgesamt also $a^{2^k} \in \mathfrak{M}$ und mit (2.5) daher $a \in \mathfrak{M} \subset \text{Arch}$.

(b) Seien nun a allgemein und $r, s \in \mathbb{N}$, s ungerade mit $m = s2^{r-1}$. Da P ein Präpositvbereich $2m$-ter Stufe ist, gilt dann $(a^s)^{2^r} = a^{2m} \in P$. Ist $a^s \in P \cup -P \subset \text{Arch} \cup \text{-Arch}$, so folgt aus (2.4) $a \in \text{Arch} \cup \text{-Arch}$. Sonst kann man Fall 1a anwenden und es folgt $a^s \in \mathfrak{M}$ und mit (2.5) also wieder $a \in \mathfrak{M} \subset \text{Arch}$.

2. Beh: $\mathcal{O}$ ist ein lokaler Ring mit maximalem Ideal $\mathfrak{M}$.
z.z.: $\mathcal{O} \setminus \mathfrak{M} \subset \mathcal{O}^\times$, wobei $\mathcal{O}^\times$ die Einheiten von $\mathcal{O}$ sind.
Sei $a \in \mathcal{O} \setminus \mathfrak{M}$ und $b = a^{2m}$. Dann gilt $b \in P$, da P ein Präpositivbereich $2m$-ter Stufe ist. Wegen (2.5) gilt aber auch $b \notin \mathfrak{M}$. Da mit b auch $\frac{1}{n} + b \in P$ für alle $n \in \mathbb{N}$ gilt, gibt es also ein $n \in \mathbb{N}$ mit $\frac{1}{n} - b \notin P$. Dies impliziert auch $\frac{1}{2n} - b \notin P$. Es kann aber auch nicht $\frac{1}{2n} - b \in \text{Arch}$ gelten, da sonst $\frac{1}{n} - b = \frac{1}{2n} + \frac{1}{2n} - b \in P$ gelten müßte im Widerspruch zur Wahl von n. Wegen Behauptung 1 folgt dann $b - \frac{1}{2n} \in \text{Arch}$ und damit $b - \frac{1}{4n} = \frac{1}{4n} + (b - \frac{1}{2n}) \in P$. Da mit b auch $b + \frac{1}{4n} \in P$ liegt, folgt durch Multiplikation mit $4nb^{-1}$ die Beziehung $4n \pm b^{-1} \in P$, also $b^{-1} \in \mathcal{O}$. Damit gilt aber auch $a^{-1} = \frac{1}{a^{2m}} \cdot a^{2m-1} \in \mathcal{O}$.

3. Beh: $\mathcal{O}$ ist Bewertungsring

(a) Sei zunächst $a \in P$. Dann gilt $a \in \mathcal{O}$ oder $a^{-1} \in \mathfrak{M}$:
Aus $1 - \frac{a}{1+a} = \frac{1}{1+a} \in P$ folgt $\frac{a}{1+a}, \frac{1}{1+a} \in \mathcal{O}$. Dies ergibt zwei Fälle:
- $\frac{1}{1+a} \in \mathcal{O}^\times \Longrightarrow a = \frac{a}{1+a} \cdot (1+a) \in \mathcal{O}$
- $\frac{1}{1+a} \in \mathfrak{M}$. Wegen $1 = \frac{a}{1+a} + \frac{1}{1+a}$ kann dann nicht $\frac{a}{1+a} \in \mathfrak{M}$ gelten, d.h. wegen Behauptung 2 ist $\frac{a}{1+a} \in \mathcal{O}^\times$. Daraus folgt $a^{-1} = \frac{1+a}{a} \cdot \frac{1}{1+a} \in \mathfrak{M}$.

(b) Sei nun $a \in K$ beliebig und $\widetilde{\mathcal{O}}$ der ganze Abschluß von $\mathcal{O}$ in K. Da P ein vollständiger Präpositivbereich $2m$-ter Stufe ist, folgt dann $a^{2m} \in P$ und mit Behauptung 3a auch $a^{2m} \in \mathcal{O}$ oder $a^{-2m} \in \mathfrak{M}$. Dadurch ist $a \in \widetilde{\mathcal{O}}$ oder $a^{-1} \in \widetilde{\mathcal{O}}$, d.h. $\widetilde{\mathcal{O}}$ ist ein Bewertungsring von K. Noch z.z.: $\mathcal{O} = \widetilde{\mathcal{O}}$:
Sei $\widetilde{\mathfrak{M}}$ das maximale Ideal von $\widetilde{\mathcal{O}}$. Wegen Lemma 1.3.2 gilt dann $\mathfrak{M} \subset \widetilde{\mathfrak{M}}$. Sei $a \in \widetilde{\mathcal{O}}$. Angenommen $a^{2m} \notin \mathcal{O}$. Wie oben gilt dann $a^{-2m} \in \mathfrak{M} \subset \widetilde{\mathfrak{M}}$, woraus $a^{-1} \in \widetilde{\mathfrak{M}}$ folgt, im Widerspruch zu $\widetilde{\mathfrak{M}}$ maximales Ideal. Mit (2.6) folgt dann $a \in \mathcal{O}$.

4. Beh: $\mathcal{O}$ ist mit P verträglich
Dies ist klar nach Definition von $\mathfrak{M}$. (wähle $n = 1$)

5. Beh: $\text{Arch} = (\mathcal{O} \cap P) \cup \mathfrak{M}$
"$\supset$": klar
"$\subset$": Sei $a \in \text{Arch} \setminus P$. Dann gilt $a - \frac{1}{k} \notin \text{Arch}$ für alle $k \in \mathbb{N}$, mit Behauptung 1 also $\frac{1}{k} - a \in \text{Arch}$. Daraus folgt $\frac{1}{k} - a = \frac{1}{2k} + (\frac{1}{2k} - a) \in P$. Da $a \in \text{Arch}$, gilt sowieso $\frac{1}{k} + a \in P$, insgesamt also $a \in \mathfrak{M}$.

Letzteres zeigt, daß $\overline{P} = \overline{\text{Arch}}$ gilt und $\overline{P}$ daher einen Positivbereich auf k definiert. Daß dieser archimedisch ist folgt aus der Eigenschaft 3 eines Stone-Rings.

□

2.4 Positivbereiche höherer Stufe auf Körpern

Definition 2.4.1
Sei K ein Körper und P ein Präpositivbereich $2m$-ter Stufe auf K, so daß $K^\times/P^\times$ zyklisch ist, so heißt P **Positivbereich $2m$-ter Stufe** auf K.

Bemerkung 2.4.2

- $[K^\times : P^\times] = 2s$ mit $s|m$
- Ist keine Stufe angegeben, so ist immer $m = 1$ gemeint. Die Eigenschaft, daß $K^\times/P^\times$ zyklisch ist, kann dann durch $P \cup -P = K$ ersetzt werden.
- Ist m eine Zweierpotenz, so ist jeder vollständige Präpositivbereich $2m$-ter Stufe ein Positivbereich $2m$-ter Stufe.

In Analogie zu Satz 2.1.7 gilt auch für Positivbereiche:

Satz 2.4.3
Sei S ein Präpositivbereich $2m$-ter Stufe auf einem Körper K. Dann gilt:

1. *Es gibt einen Positivbereich $2m$-ter Stufe P von K mit $S \subset P$.*
2. *Sei $\mathcal{P} = \{P \supset T; P \text{ Positivbereich } 2m\text{-ter Stufe auf } K\}$. Dann gilt:*

$$S = \bigcap \mathcal{P}$$

Der Beweis ist hier allerdings etwas komplizierter. Man findet ihn in [4] Satz 2.17.

2.5 Positivbereiche höherer Stufe auf Ringen

Definition 2.5.1
Sei A ein kommutativer Ring mit Eins und $S \subset A$ eine Präprimstelle mit

$$A^{2m} \subset S$$

Dann heißt S **Präpositivbereich $2m$-ter Stufe** auf A.

Definition 2.5.2
Sei A ein kommutativer Ring mit Eins und P ein Präpositivbereich $2m$-ter Stufe auf A mit den Eigenschaften

1. $P \cap -P =: \mathfrak{P}$ ist ein Primideal von A.

2. $a, b \in A, \quad ab^{2m} \in P \quad \Longrightarrow \quad a \in P \quad \vee \quad b \in \mathfrak{P}$
3. $\overline{P} := \{\frac{\overline{p}}{\overline{a}^{2m}}; p \in P, a \in A \setminus \mathfrak{P}\}$ ist ein Positivbereich $2m$-ter Stufe auf dem Quotientenkörper $k(\mathfrak{P})$ von $A/\mathfrak{P}$.

Dann nennt man P einen **Positivbereich** $2m$**-ter Stufe** auf A.

Bemerkung 2.5.3

- Ist keine Stufe angegeben, so ist immer $m = 1$ gemeint. Die Eigenschaften 2 und 3 können dann durch $P \cup -P = K$ ersetzt werden.
- Ist A ein Körper, so gilt $k(\mathfrak{P}) = A$ und obige Definition eines Positivbereiches ist konform mit derjenigen für Körper.

Satz 2.5.4
Sei S ein Präpositivbereich $2m$-ter Stufe eines kommutativen Rings A mit Eins. Dann gibt es einen Positivbereich $2m$-ter Stufe P von A mit $S \subset P$.

Beweis: $1 + S$ ist multiplikativ abgeschlossen und enthält wegen $-1 \notin S$ die Null nicht. Sei nun $\mathfrak{P}$ ein Ideal von A, das maximal ist mit der Eigenschaft $\mathfrak{P} \cap (1 + S) = \phi$. Wegen Lemma 1.3.1 auf Seite 8 muß dann $\mathfrak{P}$ ein Primideal sein. Sei $K := k(\mathfrak{P})$ und $\overline{S} := \sum \overline{S} K^{2m}$. Dann ist $\overline{S}$ unter Multiplikation und Addition abgeschlossen und enthält K^{2m}. Also bleibt noch zu zeigen:

$-1 \notin \overline{S}$**:** Sonst seien $s_i \in S, a_i \in A$, und $b_i \in A \setminus \mathfrak{P}$ mit

$$-1 = \sum \overline{s_i} \left(\frac{\overline{a_i}}{\overline{b_i}} \right)^{2m}$$

D.h. $-b^{2m} \equiv \sum s_i a_i^{2m} \mod \mathfrak{P}$ für ein $b \in A \setminus \mathfrak{P}$. Wegen der Maximalität von $\mathfrak{P}$ folgt aus $b \notin \mathfrak{P}$, daß $(bA + \mathfrak{P}) \cap (1 + S) \neq \phi$. Seien also $a \in A$, $p \in \mathfrak{P}$ und $s \in S$ mit $ba + p = 1 + s$. Sei weiter $s' := (1 + s)^{2m} - 1 (\in S)$. Dann gilt:

$$-(1 + s') = -(1 + s)^{2m} \equiv -(ba)^{2m} \equiv \sum s_i (a_i a)^{2m} \mod \mathfrak{P}$$

Also folgt

$$1 + \underbrace{s' + \sum s_i (a_i a)^{2m}}_{\in S} \in \mathfrak{P}$$

im Widerspruch zu $(1 + S) \cap \mathfrak{P} = \phi$.

Also ist $\overline{S}$ ein Präpositivbereich $2m$-ter Stufe auf K und es gibt nach Satz 2.4.3 einen Positivbereich $2m$-ter Stufe von K mit $\overline{S} \subset P$. Das Urbild von P unter $A \to k(\mathfrak{P})$ ist dann ein Positivbereich $2m$-ter Stufe auf A der S enthält. □

Man könnte nun vermuten, daß analog zu Satz 2.4.3 auch ein Präpositivbereich eines kommutativen Rings mit Eins Durchschnitt aller über ihm liegenden Positivbereiche ist. Dies muß aber nicht der Fall sein. Der im nächsten Abschnitt beschriebene Positivstellensatz 2.6.8 wird jedoch eine Charakterisierung für die Elemente in diesem Durchschnitt geben.

2.6 Ein Positivstellensatz

Definition 2.6.1
Sei A ein kommutativer Ring mit Eins, S ein Präpositivbereich $2m$-ter Stufe von A und $M \subset A$ eine Teilmenge mit

$$M + M \subset M, \quad S \cdot M \subset M, \quad 1 \in M, \quad -1 \notin M$$

Dann heißt M ein S**-Modul**.

Definition 2.6.2
Ein Ideal $\mathfrak{A}$ von A heißt M**-konvex** , falls für alle $m, m' \in M$ gilt:

$$m + m' \in \mathfrak{A} \quad \Longrightarrow \quad m, m' \in \mathfrak{A}$$

Lemma 2.6.3
Sei M ein S-Modul und $\mathfrak{A} \subsetneq A$ ein Ideal. Dann sind äquivalent:

1. *$\mathfrak{A}$ ist M-konvex*
2. *$M/\mathfrak{A}$ ist ein $S/\mathfrak{A}$-Modul und $M/\mathfrak{A} \cap -M/\mathfrak{A} = \{0\}$*
3. *$1 + M \cap \mathfrak{A} = \phi$ und $M/\mathfrak{A} \cap -M/\mathfrak{A} = \{0\}$*

Beweis:

1 ⇒ 2: Angenommen es gilt $-1 \in M/\mathfrak{A}$. Dann ist $m + 1 \in \mathfrak{A}$ für ein $m \in M$, woraus $1 \in \mathfrak{A}$ folgen würde, im Widerspruch zu $\mathfrak{A} \neq A$. Also ist $M/\mathfrak{A}$ ein $S/\mathfrak{A}$-Modul. Sei nun $\overline{m} \in M/\mathfrak{A} \cap -M/\mathfrak{A}$, d.h. es gibt ein $m' \in M$ mit $m + m' \in \mathfrak{A}$, woraus $m \in \mathfrak{A}$ folgt. Also ist $\overline{m} = 0$.

2 ⇒ 3: Da $M/\mathfrak{A}$ ein $S/\mathfrak{A}$-Modul ist, gilt $-1 \notin M/\mathfrak{A}$, woraus $1 + M \cap \mathfrak{A} = \phi$ folgt.

3 ⇒ 1: Seien $m, m' \in M$ mit $m + m' \in \mathfrak{A}$. Dann gilt im Restklassenmodul $\overline{m} = -\overline{m'} \in M/\mathfrak{A} \cap -M/\mathfrak{A} = \{0\}$, woraus $m, m' \in \mathfrak{A}$ folgt.

□

Zur nächsten Definition und Bemerkung vgl. [25] Paragraph 1.

Definition 2.6.4
Zu einem Präpositivbereich $2m$-ter Stufe S eines kommutativen Ringes A mit Eins und einem S-Modul M sei

$$\widetilde{M} := \{x \in A;\ \text{es gibt } n \in \mathbb{N} \text{ mit } ((2m)!)^n x \in M\}$$

Bemerkung 2.6.5 Es gilt:

1. $M \subset \widetilde{M}$
2. $\widetilde{M}$ ist ein $\widetilde{S}$-Modul.
3. $\widetilde{S} - \widetilde{S} = A$.

   Denn: Sei $x \in A$. Dann gibt es nach Gleichumg (2.6) auf Seite 18 Elemente $y, z \in \sum A^{2m}$ mit $(2m)!x = y - z$. Wegen $(2m)!(x+z) = y + ((2m)! - 1)z \in \sum A^{2m} \subset S$ ist dann $x + z \in \widetilde{S}$ und damit $x = (x+z) - z \in \widetilde{S} - \widetilde{S}$.
4. $\widetilde{M} \cap -\widetilde{M}$ ist ein Ideal von A.

   Denn: Daß $\widetilde{M} \cap -\widetilde{M}$ eine additive Gruppe ist, ist klar. Sei also $a \in A$ und $m \in \widetilde{M} \cap -\widetilde{M}$. Nach Punkt 3 dieser Bemerkung gibt es dann $s, t \in \widetilde{S}$ mit $a = s - t$. Wegen Punkt 2 folgt daher $am = sm - tm \in \widetilde{M} \cap -\widetilde{M}$.

Lemma 2.6.6
Sei S ein Präpositivbereich $2m$-ter Stufe, M ein S-Modul und $\mathfrak{P} \subset A$ ein Ideal, das maximal ist mit der Eigenschaft $1 + M \cap \mathfrak{P} = \phi$. Dann ist $\mathfrak{P}$ ein M-konvexes Primideal.

Beweis:

M-konvex: Seien $m', m'' \in M$ mit $m' + m'' \in \mathfrak{P}$. Sei $M' := M + \mathfrak{P}$ und $\mathfrak{P}' := \widetilde{M'} \cap -\widetilde{M'}$. Dann gilt $m', m'' \in (-M + \mathfrak{P}) \cap M \subset \mathfrak{P}'$ und es folgt:

- Wegen $1 + M \cap \mathfrak{P} = \phi$ ist M' ein S-Modul und damit $\widetilde{M'}$ ein $\widetilde{S}$-Modul Dann ist aber auch $1 + \widetilde{M'} \cap \mathfrak{P}' = \phi$, denn sonst wäre $1 + m' = -m''$ für gewisse $m', m'' \in \widetilde{M'}$, woraus $-1 = m' + m'' \in \widetilde{M'}$ folgen würde. Damit ist insbesondere auch $1 + M \cap \mathfrak{P}' = \phi$.
- Nach obiger Bemerkung 2.6.5 ist $\mathfrak{P}'$ ein Ideal von A.

Wegen der Maximalität von $\mathfrak{P}$ ist also $\mathfrak{P} = \mathfrak{P}'$, und damit $m', m'' \in \mathfrak{P}$.

Primideal: Sei $ab \in \mathfrak{P}$ und $b \notin \mathfrak{P}$. Wegen der Maximalität von $\mathfrak{P}$ ist dann $1 + M \cap \mathfrak{P} + bA \neq \phi$, also gibt es $m' \in M$ mit $1 + m' \in bA + \mathfrak{P}$, woraus $a^{2m} + a^{2m}m' \in ba^{2m}A + \mathfrak{P} \subset \mathfrak{P}$ folgt. Da $\mathfrak{P}$ M-konvex ist, erhält man daraus $a^{2m} \in \mathfrak{P}$.

Es bleibt also noch zu zeigen, daß $A/\mathfrak{P}$ keine nilpotenten Elemente enthält. Angenommen es gäbe ein Element $a \in A \setminus \mathfrak{P}$ mit $a^2 \in \mathfrak{P}$. Wegen der

Maximalität von $\mathfrak{P}$ gibt es dann wieder ein $m' \in M$ mit $1+m' \in aA+\mathfrak{P}$, woraus $(1+m')^2 \in a^2A+\mathfrak{P} \subset \mathfrak{P}$ folgt und damit

$$(1-(1+m'))^{2m} \in 1-2m-2mm'+\mathfrak{P}$$

Wegen $2mm'+2(m-1) \in M$ folgt dann auch $-1 \in M/\mathfrak{P}$ im Widerspruch dazu, daß $\mathfrak{P}$ ein M-konvexes Ideal ist und $M/\mathfrak{P}$ daher ein $S/\mathfrak{P}$-Modul.

□

Lemma 2.6.7
Sei S ein Präpositivbereich $2m$-ter Stufe auf A und $a \in A$ in allen Positivbereichen $2m$-ter Stufe $P \supset S$ enthalten. Sei ferner $M := S - Sa$ ein S-Modul. Dann gibt es ein M-konvexes Primideal $\mathfrak{P}$ von A mit $a \in \mathfrak{P}$.

Beweis: Sei $\mathfrak{P}$ ein maximales Ideal von A mit der Eigenschaft $1+M\cap\mathfrak{P} = \phi$. Nach Lemma 2.6.6 ist dann $\mathfrak{P}$ ein M-konvexes Primideal und es bleibt noch $a \in \mathfrak{P}$ zu zeigen.

Dazu sei k der Quotientenkörper von $A/\mathfrak{P}$ und für einen S-Modul M sei

$$\overline{M} := \{\frac{\overline{m'}}{\overline{a}^{2m}}; a \in A \setminus \mathfrak{P}, m \in M\}$$

Da $\mathfrak{P}$ M-konvex ist, ist $\overline{S}$ ein Präpositivbereich $2m$-ter Stufe und $\overline{M}$ ein $\overline{S}$-Modul. Denn wäre $-1 \in \overline{M}$, dann gäbe es ein $m' \in M$ und ein $a' \in A \setminus \mathfrak{P}$ mit $m' + a'^{2m} \in \mathfrak{P}$, woraus $a'^{2m} \in \mathfrak{P}$ und damit auch $a' \in \mathfrak{P}$ folgen würde, im Widerspruch zur Wahl von a'. Wegen Satz 2.4.3 und Punkt 3 aus der Definition eines Positivbereiches auf Ringen gilt:

$$\overline{S} = \bigcap_{\substack{P\supset S \\ \text{Positivbereich} \\ \text{mit } \mathfrak{P}=P\cap -P}} \overline{P}$$

Da $a \in P$ für alle diese Positivbereiche gilt, folgt also $\overline{a} \in \overline{S} \subset \overline{M}$. Andererseits ist aber auch $-a \in M$, also $\overline{a} \in \overline{M} \cap -\overline{M} = \{0\}$, wobei die letzte Gleichung aus der M-Konvexität von $\mathfrak{P}$ folgt. Also ist $a \in \mathfrak{P}$. □

Für den nächsten Satz wird noch eine Bezeichnung eingeführt: Ist P ein Positivbereich $2m$-ter Stufe und $\mathfrak{P} = P \cap -P$, so sei

$$P^+ := P \setminus \mathfrak{P}$$

Satz 2.6.8 (Positivstellensatz)
Sei $S \subset A$ ein Präpositivbereich $2m$-ter Stufe und sei $a \in A$, so daß $a \in P^+$ für alle Positivbereiche $2m$-ter Stufe $P \supset S$ von A gilt. Dann gibt es $s, s' \in S$ mit

$$as = 1 + s'$$

Beweis: Ann: $1 + S \cap aS = \phi$.
Dann ist $M = S - aS$ ein S-Modul. Nach Lemma 2.6.7 gibt es daher ein M-konvexes Primideal $\mathfrak{P}$ mit $a \in \mathfrak{P}$. Insbesondere ist dann $\mathfrak{P}$ auch S-konvex, also ist $-1 \notin S + \mathfrak{P}$ und damit $S + \mathfrak{P}$ ein Präpositivbereich $2m$-ter Stufe von A. Nach Satz 2.5.4 gibt es dann einen Positivbereich $2m$-ter Stufe $P \supset S + \mathfrak{P}$ und es folgt $a \in \mathfrak{P} \subset P \cap -P$ im Widerspruch zu $a \in P^+$. $\square$

Kapitel 3

Zwei Anwendungen des Positivstellensatzes

3.1 Stetigkeit des klassischen 17. Hilbertschen Problems in einer Verallgemeinerung

In diesem Abschnitt wird die Stetigkeit des 17. Hilbertschen Problems in folgender Verallgemeinerung bewiesen:

Für ein Polynom $f \in \mathbb{R}[X]$ soll nicht $f(x) \geq 0$ für alle $x \in \mathbb{R}$, sondern nur auf einer offenen Menge $\{x; \bigwedge_{i=1}^{k} f_i(x) > 0\}$ für Polynome $f_i \in \mathbb{R}[X] \setminus \{0\}$ gelten. Natürlich kann man f dann auch nicht mehr unbedingt als Quadratsumme schreiben, aber man erhält noch, daß f in dem Halbring liegt, der von $f_1, \ldots, f_k$ und $(\mathbb{R}(X))^2$ erzeugt wird. Diese Tatsache — ohne Berücksichtigung der Stetigkeit — wurde 1955 von Abraham Robinson in [32] bewiesen. Die stetige Abhängigkeit der Koeffizienten wird hier allerdings nur auf der Menge $\{(f, f_1, \ldots, f_n); f \neq 0 \wedge \exists x \bigwedge_{i=1}^{k} f_i(x) > 0\}$ gezeigt.

Im Spezialfall $k = 1$ und $f_1 = 1$ ist dies gerade das 17. Hilbertsche Problem.

Der Beweis lehnt sich an den Beweis der Stetigkeit im klassischen Fall wie er in [13] geführt wird und auch in der Vorlesung [30] vorkam.

Für einen Multiindex $\theta \in \mathbb{N}^n$ und ein Tupel $X = (X_1, \ldots, X_n)$ sei

$$\begin{aligned} |\theta| &= \theta_1 + \ldots + \theta_n \\ X^\theta &= X_1^{\theta_1} \cdot \ldots \cdot X_n^{\theta_n} \end{aligned}$$

Um die stetige Abhängigkeit der Koeffizienten, die in den Hauptsätzen dieser Diplomarbeit behandelt wird, zu zeigen, werden die vorkommenden Polynome sowohl als Funktion in ihren Unbestimmten als auch in den Koeffizienten aufgefaßt. Zu diesem Zweck wird das allgemeine Polynom

$$f_d(C, X) := \sum_{|\theta| \leq d} C_\theta X^\theta$$

vom Grad d benutzt, wobei X für die n Unbestimmten und C für die $\binom{n+d}{d}$ Koeffizienten steht. Treten — wie in diesem Fall — mehrere Polynome auf, so werden diese durch Koeffizientenvariabeln C^i unterschieden. Im folgenden Satz steht also $f_d(C^0, X)$ für f und $f_d(C^i, X)$ für f_i.

Satz 3.1.1 (Hauptsatz)
Sei $f_d(C,X) := \sum_{|\theta|\le d} C_\theta X^\theta$ das allgemeine Polynom vom Grad d in n Variabeln $X = (X_1,\dots,X_n)$, mit den $m = \binom{n+d}{d}$ Koeffizientenvariabeln $C = (C_1,\dots,C_m)$ und sei $\mathbf{C} = (C^0,\dots,C^k)$. Seien

$$B = \{\max_i \min_j p_{ij}(\mathbf{C}) : p_{ij} \in \mathbb{Z}[\mathbf{C}]\} \quad \text{und} \quad A = B[X]$$

Dann gibt es $l_0,\dots,l_k,\sigma',\sigma'' \in \mathbb{N}$ und $\epsilon_1^{(i)},\dots,\epsilon_k^{(i)},\delta_1^{(j)},\dots,\delta_k^{(j)} \in \{0,1\}$, sowie $\alpha_i,\beta_j \in B$ und $g_i,h_j \in A$ für alle $1 \le i \le \sigma'$, $1 \le j \le \sigma''$ so daß

$$f_d(C^0,X)\left(\sum_{i=1}^{\sigma'} \alpha_i g_i^2 \prod_{\nu=1}^{k} f_d(C^\nu,X)^{\epsilon_\nu^{(i)}}\right) = \left(\prod_{\nu=0}^{k} f_d(C^\nu,X)^{l_\nu}\right)^2 + \sum_{j=1}^{\sigma''} \beta_j h_j^2 \prod_{\nu=1}^{k} f_d(C^\nu,X)^{\epsilon_\nu^{(j)}} \tag{3.1}$$

Ist R ein reell abgeschlossener Körper in dem für $\mathbf{a} = (a^{(0)},\dots,a^{(k)})$ gilt

$$R \models \forall x \left(\bigwedge_{\nu=1}^{k} f_d(a^{(\nu)},x) > 0 \to f_d(a^{(0)},x) \ge 0\right)$$

so sind $\alpha_i(\mathbf{a}),\beta_j(\mathbf{a}) \ge 0$ für alle $1 \le i \le \sigma'$, $1 \le j \le \sigma''$.

Bemerkung 3.1.2 $B = \{\max_i \min_j p_{ij};\ p_{ij} \in \mathbb{Z}[\mathbf{C}]\}$ ist ein Ring. (vgl. [10] Seite 655.)

In der folgenden Bemerkung werden nun einige Definitionen gemacht, um den Satz in den etwas handlicheren Satz 3.1.4 umzuformulieren und so den Positivstellensatz anwenden zu können. Am Ende des Abschnitts, im eigentlichen Beweis von 3.1.1, muß dann nur noch erklärt werden, warum es sich bei 3.1.4 tatsächlich nur um eine Umformulierung handelt.

Bemerkung 3.1.3 Sei $\varphi(\mathbf{C}) := \forall x \left(\bigwedge_{\nu=1}^{k} f_d(C^{(\nu)},x) > 0 \to f_d(C^{(0)},x) \ge 0\right)$ und R ein reell abgeschlossener Körper. Dann gilt:

$$\begin{aligned}\{\mathbf{a} \in R^{(k+1)m}; \varphi(\mathbf{a})\} = \bigcap_{x\in R} \Bigg(&\left(\bigcup_{\nu=1}^{k} R^{\nu m} \times \{a \in R^m; f_d(a,x) \le 0\} \times R^{(k-\nu)m}\right) \\ &\cup \left(\{a \in R^m; f_d(a,x) \ge 0\} \times R^{km}\right)\Bigg) \\ \subset\ & R^{(k+1)m} \quad \text{abgeschlossen}\end{aligned}$$

Wendet man den Endlichkeitssatz 1.2.1 an, so erhält man endlich viele Polynome $p_{ij} \in \mathbb{Z}[\mathbf{C}]$ mit

$$R \models \varphi(\mathbf{C}) \longleftrightarrow \bigvee_i \bigwedge_j p_{ij}(\mathbf{C}) \geq 0$$

Seien

$$p_i(\mathbf{a}) := \min_j p_{ij}(\mathbf{a}) \quad \text{und} \quad p(\mathbf{a}) := \max_i p_i(\mathbf{a})$$

Dann gilt:

$$R \models \bigvee_i \bigwedge_j p_{ij}(\mathbf{a}) \geq 0 \longleftrightarrow p(\mathbf{a}) \geq 0 \tag{3.2}$$

Seien nun A und B wie im Satz beschrieben und sei $S \subset A$ der Halbring, der von A^2, $f_d(C^1, X), \ldots, f_d(C^k, X)$, p, $p - p_i$ und $p_{ij} - p_i$ erzeugt wird. Sei $F := \{\prod_{\nu=0}^k f_d(C^\nu, X)^{l_\nu}; l_\nu \in \mathbb{N}\}$ und seien

$$\begin{aligned} A_F &:= \{\frac{a}{f}; a \in A, f \in F\} \\ S_F &:= \{\frac{s}{f^2}; s \in S, f \in F\} \end{aligned}$$

Dann gilt:

Satz 3.1.4
Es gibt $s_1, s_2 \in S_F$ mit $f_d(C^0, X)\ s_1 = 1 + s_2$

Wegen seiner Bedeutung für andere Beweise sei zunächst ein Teil des Beweises in ein Lemma ausgelagert.

Lemma 3.1.5
Seien A ein kommutativer Ring mit Eins und $p_{ij} \in \mathbb{Z}[X]$ endlich viele Polynome, sowie $p_i(x) = \min_j p_{ij}(x)$ und $p(x) = \max_i p_i(x)$. Sei ferner S ein Präpositivbereich von A mit $p, p - p_i, p_{ij} - p_i \in S$ und sei $\mathfrak{P}$ ein Primideal von A, so daß $S/\mathfrak{P}$ ein Präpositivbereich von $A/\mathfrak{P}$ ist. Dann gilt bezüglich eines über $S/\mathfrak{P}$ liegenden Positivbereiches von $A/\mathfrak{P}$:

$$\overline{p} = \max_i \min_j \overline{p_{ij}} \in S/\mathfrak{P}$$

Beweis: Aus $\prod(p - p_i) = 0$ folgt $\prod(\overline{p} - \overline{p_i}) = 0$ im Integritätsring $A/\mathfrak{P}$. Es gibt also ein i_0 mit $\overline{p} = \overline{p_{i_0}}$. Ebenso folgt aus $\prod(p_{ij} - p_i) = 0$, daß es ein j_0 mit $\overline{p_i} = \overline{p_{ij_0}}$ gibt. Außerdem gilt $\overline{p - p_i} \in S/\mathfrak{P}$, d.h. $\overline{p_{i_0}} = \overline{p} = \max_i \overline{p_i}$ und $\overline{p_{ij} - p_i} \in S/\mathfrak{P}$. Daher ist $\overline{p_{ij_0}} = \overline{p_i} = \min_j \overline{p_{ij}}$ bzgl. jedem über $S/\mathfrak{P}$ liegenden Positivbereich. Also folgt

$$\overline{p} = \max_i \overline{p_i} = \max_i \min_j \overline{p_{ij}}$$

Da außerdem $p \in S$ gilt, folgt die Behauptung. $\square$

Beweis: von Satz 3.1.4.

1. Fall: $-1 \in S_F$: Dann gilt $4f = (f+1)^2+(-1)(f-1)^2 \in S_F$ für alle $f \in A_F$. Also erfüllt $s_1 = 4$ und $s_2 = (f_d(C^0, X) + 1)^2 + (-1)(f_d(C^0, X) - 1)^2$ die gewünschten Eigenschaften.

2. Fall: $-1 \notin S_F$: Dann ist S_F ein Präpositivbereich von A_F. Es soll der Positivstellensatz 2.6.8 angewandt werden. Dazu ist zu zeigen: Ist $P \supset S_F$ ein Positivbereich von A_F, $\mathfrak{P} = P \cap -P$ das zugehörige Primideal und seien $\overline{A_F} = A_F/\mathfrak{P}$, $\overline{P} = P/\mathfrak{P}$ und $\overline{f} = f + \mathfrak{P}$ für $f \in A_F$, dann gilt $\overline{f_d(C^0, X)} \in \overline{P} \setminus \{0\}$.
   Wegen $f_d(C^0, X) \in A_F^\times$ folgt $f_d(C^0, X) \notin \mathfrak{P}$ und damit $\overline{f_d(C^0, X)} \neq 0$. Da $f_d(C^0, X) \in \mathbb{Z}[\mathbf{C}, X]$, gilt außerdem $\overline{f_d(C^0, X)} = f_d(\overline{C^0}, \overline{X})$.
   Ann: $f_d(\overline{C^0}, \overline{X}) \notin \overline{P}$.
   Für $\nu = 1, \ldots, k$ gilt $f_d(C^\nu, X) \in S_F \cap A_F^\times$. Also ist $f_d(\overline{C^\nu}, \overline{X}) \in \overline{P} \setminus \{0\}$. Aus Lemma 3.1.5 erhält man außerdem $\bigvee_i \bigwedge_j p_{ij}(\overline{\mathbf{C}}) \in \overline{P}$. Sei nun R' der Quotientenkörper von $\overline{A_F}$ bezüglich des von $\overline{P}$ induzierten Positivbereichs. Die Annahme impliziert also:

$$R' \models \exists \mathbf{C}, X \quad \underbrace{f_d(C^0, X) < 0}_{\neg\beta} \wedge \underbrace{\bigwedge_{i=1}^{k} f_d(C^i, X) > 0}_{\alpha} \wedge \underbrace{\bigvee_i \bigwedge_j p_{ij}(\mathbf{C}) \geq 0}_{\gamma}$$

   Nach dem Tarskiprinzip gilt die Aussage dann auch in R. Da die Formel $\neg\forall x((\alpha \to \beta) \leftrightarrow \gamma)$ äquivalent zu $\exists x((\neg\alpha \wedge \neg\gamma) \vee (\beta \wedge \neg\gamma) \vee (\neg\beta \wedge \alpha \wedge \gamma))$ ist, folgt also

$$R \models \neg\forall \mathbf{C}, X \left(\left(\bigwedge_{i=1}^{k} f_d(C^i, X) > 0 \ \to f_d(C^0, X) \geq 0 \right) \leftrightarrow \bigvee_i \bigwedge_j p_{ij}(\mathbf{C}) \geq 0 \right)$$

   im Widerspruch zur Wahl der p_{ij}.
   Der Positivstellensatz liefert also $s_1, s_2 \in S_F$ mit $f_d(C^0, X)\ s_1 = 1 + s_2$.

$\square$

Beweis: von Satz 3.1.1.
Multipliziert man in Satz 3.1.4 die Nenner hoch, so hat die Gleichung die Gestalt von (3.1). Die α_i und β_j bestehen dann aus Summen von Produkten in p,

$p - p_i$ und $p_{ij} - p_i$. Außer p nehmen diese Elemente sowieso auf ganz $R^{(k+1)m}$ nur nichtnegative Werte an. Nach Formel (3.2) folgt aber $p(\mathbf{a}) \geq 0$ aus $R \models \varphi(\mathbf{a})$. □

Korollar 3.1.6
Es sei $\mathbf{a} \in R^{(k+1)m}$ *mit* $R \models \varphi(\mathbf{a})$. *Gilt* $f_d(a^0, X) \neq 0$ *und* $\exists x \bigwedge_{i=1}^k f_d(a^i, x) > 0$, *so gibt es* $\sigma \in \mathbb{N}$, $s, r_i \in A$, *und* $\gamma_i \in B$ *für* $i = 1, \ldots, \sigma$ *mit* $\gamma_i(\mathbf{a}) \geq 0$ *und*

$$f_d(a^0, X) = \sum_{i=1}^{\sigma} \gamma_i(\mathbf{a}) \left(\frac{r_i(\mathbf{a}, X)}{s(\mathbf{a}, X)} \right)^2 \prod_{\nu=1}^{k} f_d(a^\nu, X)^{\epsilon_\nu^{(i)}}$$

Beweis: Sei $s(\mathbf{C}, X) = \sum_{i=1}^{\sigma'} \alpha_i \prod_{\nu=1}^k f_d(C^\nu, X)^{\epsilon_\nu^{(i)}} g_i^2$ und sei $x_0 \in R^n$ mit $\bigwedge_{i=1}^k f_d(a^i, x_0) > 0$. Dann gilt $\bigwedge_{i=1}^k f_d(a^i, x) > 0$ auch auf einer Umgebung U von x_0. Daher folgt aus $f_d(a^\nu, X) \neq 0$ und $R \models \varphi(\mathbf{a})$ schon $s(\mathbf{a}, X) \neq 0$. (Denn ist $s(\mathbf{a}, X) = 0$, so folgt mit Gleichung (3.1) auch

$$\left(\prod_{\nu=0}^{k} f_d(a^\nu, X)^{l_\nu} \right)^2 + \underbrace{\sum_{j=1}^{\sigma''} \beta_j h_j^2 \prod_{\nu=1}^{k} f_d(a^\nu, X)^{\epsilon_\nu^{(j)}}}_{=:h(X)} = 0$$

Ferner kann aus $\bigwedge_{i=1}^k f_d(a^i, x) > 0$ auf $h(x) \geq 0$ und damit auf $f_d(a^0, x) = 0$ für alle $x \in U$ geschlossen werden. Daraus folgt aber schon $f_d(a^0, X) = 0$.) Dividiert man nun Gleichung (3.1) durch s und erweitert die rechte Seite mit s, so erhält man eine Gleichung der gewünschten Form. □

Bemerkung 3.1.7

- Gibt es kein x mit $\bigwedge_{i=1}^k f_d(a^i, x) > 0$, so kann man nicht so einfach auf $s(\mathbf{a}, X) \neq 0$ schließen. Ist z.B. $f_1 = -X^2$, so erfüllt

  $$f \cdot 0 = f_1^2 + X^2 f_1$$

  Gleichung (3.1) auch dann, wenn $f \neq 0$ ist.

- Aus $\gamma_i(\mathbf{a}) \geq 0$ folgt im reell abgeschlossenen Körper R schon, daß $\gamma_i(\mathbf{a})$ ein Quadrat ist. Daher kann man γ_i noch zu $\frac{r_i(\mathbf{a},X)}{s(\mathbf{a},X)}$ schlagen und erhält damit tatsächlich eine Darstellung von $f_d(a^0, X) \neq 0$ im Halbring, der von $(R(X))^2$ und $f_d(a^1, X), \ldots, f_d(a^k, X)$ erzeugt wird.

- Im Spezialfall $k = 1$ und $f_1 = 1$ lassen sich die Terme $\gamma_i \frac{r_i}{s}$ durch 0 stetig auf $a \in R^m$ mit $f(a, X) = 0$ fortsetzen, so daß man auf diese Weise im klassischen 17.Hilbertschen Problem überall Stetigkeit erhält.

3.2 Stetige Darstellung positv-semidefiniter Polynome in einer Variabeln als Summe $2m$ - ter Potenzen

In diesem Abschnitt wird das 17. Hilbertsche Problem in einer anderen Hinsicht verallgemeinert. Es interessiert nun nicht mehr, wann ein Polynom als Quadratsumme dargestellt werden kann, sondern als Summe $2m$-ter Potenzen. Es wird allerdings nur eine hinreichende Bedingung dafür angegeben und die stetige Abhängigkeit der Koeffizienten in diesem Fall gezeigt.

Die Argumentation ist [28] entnommen und mit Hilfe des Positivstellensatzes 2.6.8 für alle geraden Potenzen verallgemeinert. (Die Formulierung des aus [28] verwendeten Satzes ohne Beweis findet man auch in [29]. Dort wird außerdem ein Beispiel für eine Darstellung als Summe 2^m-ter Potenzen angegeben, deren Darstellung nicht stetig möglich ist.)

Satz 3.2.1
Seien (K, P_0) ein angeordneter Körper und $m, d \in \mathbb{N}$ mit $2m \mid d$,

$$f = f_d(\mathbf{a}, X) = a_d X^d + \ldots + a_0 \in K[X]$$

Seien ferner $N, M \in \mathbb{N}$ mit folgenden Eigenschaften:

(i) $|a_i| \leq N$ für $0 \leq i \leq d$ und $\frac{1}{N} \leq a_d$

(ii) Sei R der reelle und $\widetilde{K}$ der algebraische Abschluß von (K, P_0) und gelte für $x \in \widetilde{K}$ mit $f(x) = 0$

(a) $x \in R \Longrightarrow 2m \mid$ Multiplizität von x in f

(b) $x \notin R \Longrightarrow \frac{1}{M} \leq |\mathrm{Im}(x)|$

Dann gilt:

$$f \in \sum P_0 K(X)^{2m}$$

Beweis: Seien $F = K(X)$ und $P' = \sum P_0 F^{2m}$. Dann ist P' ein Präpositivbereich $2m$-ter Stufe von F.

Ann.: $f \notin P'$.

Nach Korollar 2.1.8 gibt es dann einen vollständigen Präpositivbereich $2m$-ter Stufe P von F, so daß $f \notin P$ gilt. Seien $\mathcal{O} = \mathcal{O}(P)$ der Bewertungsring von F und $\mathfrak{M}$ das zugehörige maximale Ideal wie sie in Definition 2.3.2 definiert wurden und v die zugehörige Bewertung. Hat man die Aussage

(iii) Es gibt $a \in P_0$ und $g \in F$ so daß $v(fag^{2m}) = 0$ und $\overline{fag^{2m}} > 0$

gezeigt, so kann man auf ein $p \in P \setminus \mathfrak{M}$ mit $\overline{fag^{2m}} = \overline{p}$ schließen. D.h. $fag^{2m}p^{-1} \in 1 + \mathfrak{M}$. Da $\mathcal{O}$ ein mit P verträglicher Bewertungsring ist, gilt aber auch $1 + \mathfrak{M} \subset P$, insgesamt also $f \in P$ im Widerspruch zur Wahl von P.

Es bleibt also noch (iii) zu zeigen:
Seien $a = a_d^{-1}$ und $c_i = a_i a_d^{-1}$ für $0 \le i \le d$. Dann gilt $|c_i| = |a_i||a_d^{-1}| \le N^2$. Sei weiter

$$af = f_1 \cdot \ldots \cdot f_r$$

die Zerlegung von af in irreduzible normierte Polynome $f_i \in K[X]$. Dann haben die f_i die folgenden Eigenschaften:

- Die Beträge der Nullstellen von af und also auch die der f_i sind durch $\max\{1, \sum_{i=0}^{d-1} |c_i|\} \le \max\{1, dN^2\}$ beschränkt (vgl. Bemerkung 1.3.3). Damit sind aber auch die Koeffizienten der f_i als elementarsymmetrische Funktionen ihrer Nullstellen durch eine natürliche Zahl beschränkt.

- Hat f_i eine Nullstelle in R so gilt wegen (ii), daß es ein $k_i \in \mathbb{N}$ gibt, so daß x eine $2mk_i$-fache Nullstelle von f ist. Da K angeordnet ist, gilt $\mathrm{char} K = 0$, also ist K vollkommen und es muß in der Zerlegung von af genau $2mk_i$ viele f_i geben mit $f_i(x) = 0$. Diese sind alle gleich, denn seien $f_i(x) = f_j(x) = 0$; dann gilt $f_i = \mathrm{Irr}(x, K) = f_j$.

Seien nun ohne Einschränkung die f_i so angeordnet, daß die ersten s diejenigen mit reellen Nullstellen sind. Sei dann

$$g^{-1} := \prod_{i=1}^{s} f_i^{\frac{1}{k_i}}$$

Nach obiger Überlegung gilt somit $g \in K(X)$ und $f_0 := afg^{2m} \in K[X]$ hat folgende Eigenschaften:

- f_0 hat keine Nullstelle in R.
- $2m \mid \deg f_0 =: d_0$.
- Die nichtreellen Nullstellen von f_0 sind die gleichen (evtl. nicht alle) wie die von f und ihr Betrag ist also größer oder gleich $\frac{1}{M}$. Da f_0 höchstens die Nullstellen von f hat gilt wie oben, daß auch die Koeffizienten von f_0 durch eine natürliche Zahl beschränkt sind.

Nach der Definition von $\mathcal{O}$ und weil $P_0 = P \cap K$ ein Positivbereich ist, ist $\mathcal{O} \cap K$ die konvexe Hülle von $\mathbb{Q}$ in K. Sei $\mathcal{O}'$ die konvexe Hülle von $\mathbb{Q}$ in R und sei $\mathfrak{M}'$ das maximale Ideal von $\mathcal{O}'$. Dann ist $\mathcal{O}'$ eine Fortsetzung von $\mathcal{O} \cap K$ auf R und es gilt:

- Die Koeffizienten von f_0 liegen in $\mathcal{O} \cap K$. Damit ist $\overline{f_0} \in \overline{K}[X]$ wohldefiniert.

- $\overline{f_0}$ ist normiert und vom Grad d_0.

- $\overline{f_0}$ hat keine Nullstellen in $\overline{R}$.

  Denn: Da f_0 keine reellen Nullstellen hat, gilt $f_0 = \prod(X - a_k)^2 + b_k^2$ mit $a_k, b_k \in R$. Im algebraischen Abschluß von R hat f_0 daher genau die Nullstellen $a_k \pm ib_k$. Einerseits gilt dann wie oben, daß die Beträge von a_k und b_k durch natürliche Zahlen beschränkt sind, d.h. $a_k, b_k \in \mathcal{O}'$ und außerdem folgt wegen (ii), daß $|b_k| \geq \frac{1}{M}$, d.h. $b_k \notin \mathfrak{M}'$. Damit gilt aber auch $\prod(x - a_k)^2 + b_k^2 \notin \mathfrak{M}'$ für alle $x \in \mathcal{O}'$.

- Da $\overline{f_0}$ normiert ist, nimmt es für große x positive Werte an, also ist $\overline{f_0}$ auf ganz $\overline{R}$ streng positiv.

- Da $\overline{K} \subset \overline{F} \subset \mathbb{R}$ und $\overline{R}$ reell abgeschlossen ist, folgt aus dem Tarskiprinzip, daß $\overline{f_0}$ auch auf ganz $\mathbb{R}$ streng positiv ist.

Um den Beweis von (iii) nun zu Ende zu bringen, seien zwei Fälle unterschieden:

1. Fall: $v(X) \geq 0$. Dann gilt $\overline{f_0} \in \overline{K}[\overline{X}] \subset \overline{K[X]} \subset \mathbb{R}$. Ist α das Bild von $\overline{X}$ in $\mathbb{R}$, so gilt $\overline{f_0}(\alpha) > 0$, da $\overline{f_0}$ streng positiv auf $\mathbb{R}$ ist. Also folgt auch $\overline{f_0} = \overline{f_0}(\overline{X}) > 0$.

2. Fall: $v(X) < 0$. Sei $f_0 = \sum b_i X^i$. Dann gilt

$$X^{-d_0} f_0 - 1 = \underbrace{X^{-1}}_{\in \mathfrak{M}} \underbrace{\sum_{i=0}^{d_0-1} b_i X^{i-d_0+1}}_{\in \mathcal{O}} \in \mathfrak{M}$$

   Es ist also $\overline{X^{-d_0} f_0} = 1 > 0$. Sei $d_0 = 2mk$. Dann ist (iii) mit $X^{-k}g$ statt dem ursprünglich gewählten g erfüllt.

Damit ist (iii) und somit Satz 3.2.1 gezeigt. □

Es soll nun die stetige Darstellung von Polynomen als Summen $2m$-ter Potenzen in folgendem Sinne gezeigt werden:

Satz 3.2.2 (Hauptsatz)
Seien $m, d \in \mathbb{N}$ mit $2m \mid d$ und sei $f_d(C, X) = C_d X^d + \cdots + C_0 \in \mathbb{Z}[C, X]$. Seien weiter $N, M \in \mathbb{N}$ und

$$B = \{\max_i \min_j p_{ij}; p_{ij} \in \mathbb{Z}[C]\}$$

Abhängig von m, d, N und M gibt es dann $l, k', k'' \in \mathbb{N}$ und $\alpha_i, \beta_j \in B$ und $g_i, h_j \in B[X]$ für alle $1 \leq i \leq k'$, $1 \leq j \leq k''$, so daß

$$f \cdot \sum_{j=1}^{k''} \beta_j h_j^{2m} = f^{2ml} + \sum_{i=1}^{k'} \alpha_i g_i^{2m} \tag{3.3}$$

Erfüllt $f_d(\mathbf{a}, X)$ die Bedingungen (i) und (ii) aus Satz 3.2.1, so folgt außerdem $\alpha_i(\mathbf{a}), \beta_j(\mathbf{a}) \geq 0$.

Analog zum letzten Abschnitt wird dieser Satz zunächst wieder in eine handlichere Form umformuliert.

Bemerkung 3.2.3

1. Fixiert man in Satz 3.2.1 die natürlichen Zahlen m, d, N und M, so daß $2m \mid d$ gilt, so können (i) und (ii) als Formel $\varphi(\mathbf{a})$ der Logik erster Stufe in der Sprache der angeordneten Körper über dem reellen Abschluß R von K_0 ausgedrückt werden.

   Denn: Beachtet man, daß eine natürliche Zahl n die n-fache Summation von 1 bedeutet, so können die vorkommenden Begriffe folgendermaßen formuliert werden:

   - $|a| \leq N$: $\quad a \leq N \wedge -a \leq N$
   - $2m|\mu$: $\quad \bigvee_{i=0}^{\mu} 2mi = \mu$
   - Multiplizität der reellen Nullstelle x von f ist μ: $\bigwedge_{i=1}^{\mu} f_d^{(i-1)}(\mathbf{a}, x) = 0 \wedge f_d^{(\mu)}(\mathbf{a}, x) \neq 0$, wobei $f^{(k)}$ die k-te Ableitung von f bedeutet.
   - y ist Imaginärteil einer nicht-reellen Nullstelle $x + iy$ von f: $y \neq 0 \wedge \exists b_0, \ldots, b_{d-2} \quad (X^2 - 2xX + x^2 + y^2) \sum_{i=0}^{d-2} b_i X^i = f_d(\mathbf{a}, X)$

2. Die Menge $\{\mathbf{a} \in R^{d+1}; R \models \varphi(\mathbf{a})\}$ ist eine abgeschlossene Teilmenge von R^{d+1}.

   Denn: Wegen des Tarskiprinzips 1.1.2 genügt es dies für $R = \mathbb{R}$ zu zeigen. Sei

$$\mathfrak{Z} := \{(x_1, \ldots, x_d) \in \mathbb{C}^d; \bigwedge_{i=1}^{d-1} |\mathrm{Im} x_i| \leq |\mathrm{Im} x_{i+1}| \\ \bigwedge_{i=0}^{d/2m-1} \left(\mathrm{Im} x_{2mi+1} = 0 \rightarrow \bigwedge_{j=1}^{2m} x_{2mi+1} = x_{2mi+j} \right) \wedge \\ \bigwedge_{i=1}^{d} \left(\mathrm{Im} x_i \neq 0 \rightarrow \frac{1}{M} \leq |\mathrm{Im} x_i| \right) \}$$

$$=\{(x_1,\dots,x_d)\in\mathbb{C}^d;\ \bigwedge_{i=1}^{d-1}|\mathrm{Im}x_i|\le|\mathrm{Im}x_{i+1}|$$

$$\bigwedge_{i=0}^{d/2m-1}\left(\mathrm{Im}x_{2mi+1}\neq 0\vee\underbrace{\bigwedge_{j=1}^{2m}x_{2mi+1}=x_{2mi+j}}_{\alpha_{2mi+1}}\right)\wedge$$

$$\bigwedge_{i=1}^{d}\left(\underbrace{\mathrm{Im}x_i=0}_{\beta_i}\vee\underbrace{\frac{1}{M}\le|\mathrm{Im}x_i|}_{\gamma_i}\right)\}$$

$$\stackrel{!}{=}\{(x_1,\dots,x_d)\in\mathbb{C}^d;\ \bigwedge_{i=1}^{d-1}|\mathrm{Im}x_i|\le|\mathrm{Im}x_{i+1}|$$

$$\bigwedge_{i=0}^{d/2m-1}\left((\mathrm{Im}x_{2mi+1}=0\wedge\bigwedge_{j=1}^{2m}x_{2mi+1}=x_{2mi+j})\vee\frac{1}{M}\le|\mathrm{Im}x_{2mi+1}|\right)$$

$$\bigwedge_{i=1}^{d}\left(\mathrm{Im}x_i=0\vee\frac{1}{M}\le|\mathrm{Im}x_i|\right)\}$$

$\subset\mathbb{C}^d$ abgeschlossen

Dabei ergibt sich die letzte Gleichung folgendermaßen: Die Konjunktionsglieder haben für $i\in 2m\mathbb{Z}+1$ die Form $(\neg\beta\vee\alpha)\wedge(\beta\vee\gamma)$. Berücksichtigt man, daß aus γ sowieso β folgt, liefert Ausklammern, daß diese Bedingung äquivalent ist zu $\gamma\vee(\alpha\wedge\beta)$.

Sei π wie in Lemma 1.3.5 die abgeschlossene Quotientenabbildung. Die durch φ definierte Menge ist gerade der Schnitt des Urbildes von $\pi(\mathfrak{Z})$ unter der in Satz 1.3.4 angegebenen stetigen Abbildung mit $\mathbb{R}^{d+1}$ und der abgeschlossenen Menge aller Koeffizienten, so daß (i) erfüllt ist. Sie ist damit abgeschlossen.

3. Aus dem Endlichkeitssatz 1.2.1 folgt also, daß es endlich viele Polynome $p_{ij}\in\mathbb{Z}[C_0,\dots,C_d]$ gibt, so daß φ äquivalent zur Formel $\bigvee_i\bigwedge_j p_{ij}(\mathbf{a})\ge 0$ ist, d.h. für alle $\mathbf{a}\in K_0^{d+1}$ gilt:

$$(K_0,P_0)\models\bigvee_i\bigwedge_j p_{ij}(\mathbf{a})\ge 0\Longrightarrow f_d(\mathbf{a},X)\in\sum P_0K_0(X)^{2m}$$

Seien nun

$$p_i(\mathbf{a}):=\min_j p_{ij}(\mathbf{a})\quad\text{und}\quad p(\mathbf{a}):=\max_i p_i(\mathbf{a})$$

und $A \subset B[X]$ der Ring erzeugt durch

$$\mathbb{Z}[C,X], p_i, p \text{ und } \frac{1}{f}$$

und $S \subset A$ der Halbring, der durch

$$\mathbb{Z}[C]^2, A^{2m}, p - p_i, p_{ij} - p_i \text{ und } p$$

erzeugt wird. Dann gilt der folgende Satz:

Satz 3.2.4
Es gibt $s, t \in S$, so daß $ft = 1 + s$.

Beweis: Ist $-1 \in S$, so folgt $f \cdot 0 = 1 + (-1)$. Ansonsten ist S ein Präpositivbereich $2m$-ter Stufe und der Positivstellensatz kann angewendet werden:

Sei $P \supset S$ ein Positvbereich $2m$-ter Stufe auf A und $\mathfrak{P} = P \cap -P$. Da $f \in A^\times$ gilt, folgt $f \notin \mathfrak{P}$.
Ann: $f \notin P$.

- Einerseits folgt dann $\overline{f} \notin \overline{P}$. Denn sonst wäre $p \equiv fa^{2m} \bmod \mathfrak{P}$ für ein $p \in P$ und $a \in A \setminus \mathfrak{P}$. Dann folgt $fa^{2m} \in P$ und mit Bedingung 2 der Definition eines Positivbereichs $2m$-ter Stufe auf einem Ring also $f \in P \vee a \in \mathfrak{P}$ im Widerspruch zur Annahme.

- Andererseits gilt aber auch $\overline{f} \in \overline{P}$:

  - Sei $K_0 := \mathbb{Q}(\overline{C})$. Dann ist $P_0 := K_0 \cap \overline{P}$ ein Positivbereich von K_0. Denn mit $\mathbb{Z}[\overline{C}]^2 \subset P_0$ ist auch $K_0^2 \subset P_0$ (Für $a, b \in \mathbb{Z}[\overline{C}], b \neq 0$ gilt nämlich $(\frac{a}{b})^2 = a^2(b^{m-1})^2 b^{-2m} \in P_0$).
  - Außerdem erhält man nach Lemma 3.1.5

  $$\overline{p} = \max_i \min_j \overline{p_{ij}} \in P$$

  Damit gelten für $f_d(\overline{C}, X) \in K_0[X]$ die Bedingungen (i) und (ii) aus Satz 3.2.1 und es gibt also $n \in \mathbb{N}$, $p_i \in P_0$ und Polynome $g_1, \ldots, g_n, h \in K_0[X]$ ohne gemeinsamen Teiler mit

  $$f_d(\overline{C}, X) = \frac{\sum_{i=1}^n p_i g_i(X)^{2m}}{h(X)^{2m}}$$

  Dann gilt $h(\overline{X}) \neq 0$. Denn sonst erhält man durch Hochmultiplizieren des Nenners – unter Berücksichtigung der Tatsache, daß alle Summanden nicht negativ bzüglich $\overline{P}$ sind – aus $h(\overline{X}) = 0$ auch $g_i(\overline{X}) = 0$ für alle i. Damit wäre aber das Minimalpolynom von $\overline{X}$ über K_0 ein gemeinsamer Teiler von h und $g_1, \ldots, g_n$ im Widerspruch zur Wahl dieser Polynome.

  Man kann also X durch $\overline{X}$ ersetzen und erhält

  $$\overline{f} = f_d(\overline{C}, \overline{X}) \in \sum P_0 K_0(\overline{X})^{2m} \subset \overline{P}$$

Damit ist die Annahme zum Widerspruch geführt worden und es gilt $f \in P$. Der Positivstellensatz liefert nun t, s mit $ft = 1 + s$. □

Beweis: des Hauptsatzes 3.2.2.
Multipliziert man in Satz 3.2.4 die Nenner hoch (Potenzen von f), so hat die Gleichung die Gestalt (3.3). Die α_i und β_j bestehen dann aus Summen von Produkten in p, $p - p_i$, $p_{ij} - p_i$ und Elementen aus $\mathbb{Z}[C]^2$. Außer p nehmen diese Elemente sowieso auf ganz R^{d+1} nur nichtnegative Werte an und es folgt $p(\mathbf{a}) \geq 0$, wenn $f_d(\mathbf{a}, X)$ die Bedingungen (i) und (ii) erfüllt. □

Korollar 3.2.5
Gelten für $\mathbf{a} \in K^{d+1}$ die Bedingungen (i) und (ii) aus Satz 3.2.1, so gibt es $\sigma \in \mathbb{N}$, $s, r_i \in B[X]$ und $\gamma_i \in B$ für $i = 1, \ldots, \sigma$ mit $\gamma_i(\mathbf{a}) \geq 0$ und

$$f_d(\mathbf{a}, X) = \sum_{i=1}^{\sigma} \gamma_i(\mathbf{a}) \left(\frac{r_i(\mathbf{a}, X)}{s(\mathbf{a}, X)} \right)^{2m}$$

Dabei hängen σ, s, r_i und γ_i von m, d, N und M ab.

Beweis: Sei $s = \sum_{j=1}^{k''} \beta_j h_j^{2m}$. Wegen (i) gilt $f_d(\mathbf{a}, X) \neq 0$. Also ist auch $s(\mathbf{a}, X) \neq 0$. Dividiert man nun Gleichung (3.3) durch s, so erhält man nach Erweitern der rechten Seite mit s die gewünschte Form. □

Kapitel 4

Quadratische Formen

4.1 Quadratische Formen und Bilinearformen

In diesem Abschnitt werden die grundlegenden Begriffe im Zusammenhang mit quadratischen Formen eingeführt Die Definitionen und Sätze entstammen im Wesentlichen [19] Kapitel 1 und [33] Abschnitt 1.

Definition 4.1.1
Eine **Quadratische Form** der Dimension n über einem Körper K ist ein homogenes Polynom q vom Grad 2 in n Unbestimmten mit Koeffizienten aus K, d.h.

$$q := \sum_{1\leq i\leq j\leq n} a_{ij} X_i X_j \quad \text{mit} \quad a_{ij} \in K$$

Mit $< a_1, \ldots, a_n >$ sei eine quadratische Form $q = \sum_{i=1}^{n} a_i X_i^2$ in Diagonalform bezeichnet.

Sei nun $\mathrm{char} K \neq 2$ und $q_{ji} = q_{ij} = \frac{1}{2} a_{ij}$ für $i > j$, sowie $q_{ii} = a_{ii}$, dann definiert $Q := (q_{ij})_{1\leq i,j\leq n}$ eine symmetrische Matrix und man kann q mit der Abbildung

$$\begin{array}{rccc} q: & K^n & \longrightarrow & K \\ & v & \longmapsto & v^t Q v \end{array}$$

identifizieren. Gilt $q(v) = 0$ für ein $v \in K^n$, so heißt v **isotrop**, sonst heißt v **anisotrop**. Eine quadratische Form q heißt **isotrop**, falls es ein isotropes $v \in K^n \setminus \{0\}$ gibt. Sonst heißt q **anisotrop**. Ist $\det Q \neq 0$, so heißt q **regulär**, sonst **singulär**.

Zwei Quadratische Formen q_1 und q_2 heißen **isometrisch** ($q_1 \cong q_2$), wenn es einen Vektorraumisomorphismus φ auf K^n mit $q_1 = q_2 \circ \varphi$ gibt. D.h. zwei isometrische Formen beschreiben die gleiche Abbildung bzgl. unterschiedlicher Basen. Die unter Isometrie invariante Größe $\det Q \cdot (K^\times)^2$ wird als **Determinante** $\det q$ der quadratischen Form q bezeichnet.

Ist q eine n-dimensionale und p eine m-dimensionale quadratische Form, so wird durch

$$\begin{array}{rccc} q\perp p: & K^n \oplus K^m & \longrightarrow & K \\ & (v,w) & \longmapsto & q(v)+p(w) \end{array}$$

die **orthogonale Summe** und durch

$$\begin{array}{rccc} q\otimes p: & K^n \otimes K^m & \longrightarrow & K \\ & v\otimes w & \longmapsto & q(v)\cdot p(w) \end{array}$$

das **Tensorprodukt** auf q und p definiert. Dies sind quadratische Formen der Dimension $n+m$ bzw. $n\cdot m$. Für die n-fache orthogonale Summe der gleichen quadratischen Form q wird auch nq geschrieben. Für $a \in K$ wird $< a > \otimes q$ auch durch aq abgekürzt.

Jeder quadratischen Form wird durch

$$\begin{array}{rccc} B_q: & K^n \times K^n & \longrightarrow & K \\ & (v,w) & \longmapsto & \frac{1}{2}(q(v+w)-q(v)-q(w)) = v^tQw \end{array}$$

eine symmetrische Bilinearform zugeordnet. Umgekehrt wird jeder symmetrischen Bilinearform auf einem endlichdimensionalen Vektorraum nach Basiswahl durch $q_B(v) := B(v,v)$ eine quadratische Form zugeordnet. Die für quadratische Formen definierten Begriffe wie isometrisch, isotrop, Dimension oder regulär können so auch auf Bilinearformen bzw bilineare Räume übertragen werden. Dabei versteht man unter einem bilinearen Raum das Paar (V,B), wobei B eine symmetrische Bilinearform auf dem Vektorraum V ist. Ist U ein Untervektorraum des bilinearen Raums (V,B), so heißt

$$U^\perp := \{v \in V; B(v,U)=0\}$$

das **orthogonale Komplement** von U. Dabei bedeutet $B(v,U)=0$, daß $B(v,w)=0$ für alle $w \in U$ gilt. $V^\perp$ heißt das **Radikal** von V.

Bemerkung 4.1.2 Ist B eine Bilinearform auf V und $U \subset V$ ein Untervektorraum für den $U \oplus V^\perp = V$ gilt, so folgt

$$U \perp V^\perp \cong V$$

vermöge der Abbildung $(u,v) \longmapsto u+v$.

Es gibt also immer eine orthogonale Zerlegung eines bilinearen Raums in sein Radikal und einen regulären Anteil.

Bemerkung 4.1.3 Ist B eine Bilinearform auf V, so gilt

$$B \text{ regulär} \Longleftrightarrow V^\perp = \{0\}$$

Denn ist $(e_1, \ldots, e_n)$ eine Basis von V, so ist die Tatsache, daß B regulär ist, gleichbedeutend mit $\det(B(e_i, e_j))_{1 \le i,j \le n} \neq 0$. Das Gleichungssystem

$$\sum x_i B(e_i, e_j) = 0 \quad (j = 1, \ldots, n)$$

besitzt also nur die triviale Lösung. Dies bedeutet gerade $V^\perp = \{0\}$.

Lemma 4.1.4
Ist (V, B) ein regulärer bilinearer Raum mit Teilraum U, so gilt:

1. $\dim U + \dim U^\perp = \dim V$
2. $U^{\perp\perp} = U$
3. *Ist U regulär, so folgt:*
   (a) $V = U \perp U^\perp$
   (b) $\det V = \det U \cdot \det U^\perp$, *insbesondere ist $U^\perp$ regulär.*

Beweis:

1. Sei $(e_1, \ldots, e_r)$ eine Basis von U. Dann ist

$$U^\perp = \{\sum \lambda_i e_i; \sum \lambda_i B(e_i, e_j) = 0 \text{ für alle } j = 1, \ldots, r\}$$

   Da V regulär ist, hat dieses Gleichungssystem vollen Rang r, und der Lösungsraum hat daher die Dimension $\dim V - r$.

2. Wendet man (1) auf U und $U^\perp$ an und subtrahiert die beiden Gleichungen, so erhält man $\dim U = \dim U^{\perp\perp}$. Außerdem gilt per Definition für alle $u \in U$, daß $B(u, v) = 0$ für alle $v \in U^\perp$ gilt, also ist $U \subset U^{\perp\perp}$.

3. (a) Ist U regulär, so gilt $U \cap U^\perp = \{0\}$. Jetzt folgt die Behauptung mit (1).
   (b) Sei $(e_{r+1}, \ldots, e_n)$ eine Basis von $U^\perp$. Wegen (a) ist dann $(e_1, \ldots, e_n)$ eine Basis von V und es gilt:

$$(B(e_i, e_j))_{1 \le i,j \le n} = \begin{pmatrix} (B(e_i, e_j))_{1 \le i,j \le r} & 0 \\ 0 & (B(e_i, e_j))_{r+1 \le i,j \le n} \end{pmatrix}$$

   woraus die Behauptung folgt.

□

Bemerkung 4.1.5 Zu jeder regulären Form gibt es ein anisotropes Element.

Denn: Sei q eine reguläre Form. Dann gibt es $u, v \in K^n$ mit $B_q(u, v) \neq 0$. Wegen $4B_q(u, v) = q(u + v) - q(u - v)$ und $\mathrm{char} K \neq 2$ muß dann entweder $u + v$ oder $u - v$ anisotrop sein.

Satz 4.1.6
Jeder bilineare Raum hat eine orthogonale Zerlegung in eindimensionale Unterräume.

Ist speziell $v_1 \in V$ mit $q(v_1) \neq 0$, so gibt es $v_2, \ldots, v_n \in V$ mit

$$V = Kv_1 \perp Kv_2 \perp \ldots \perp Kv_n$$

$(v_1, \ldots, v_2)$ heißt dann **orthogonale Basis** *von V.*

Beweis: Da in $V^\perp$ jede direkte Summenzerlegung eine orthogonale Zerlegung ist, genügt es wegen Bemerkung 4.1.2 zu zeigen, daß jeder reguläre Raum eine solche Zerlegung hat. Dies wird durch Induktion über die Dimension n des Raumes V gezeigt:

Induktionsanfang: n=1 : klar

Induktionsschritt: Da V regulär ist gibt es nach Bemerkung 4.1.5 ein $v_1 \in V$ mit $q(v_1) \neq 0$. Nach Lemma 4.1.4 (3) folgt dann $V = Kv_1 \perp (Kv_1)^\perp$. Da mit Kv_1 auch $(Kv_1)^\perp$ regulär ist, kann die Induktionsvoraussetzung angewandt werden, die eine orthogonale Zerlegung von $(Kv_1)^\perp$ in 1-dimensionale Unterräume liefert. □

Definition 4.1.7
$H :=< 1, -1 >$ heißt **hyperbolische Ebene**. Eine quadratische Form q für die es ein $r \in \mathbb{N}$ gibt, so daß $q \cong rH$ ist, heißt **hyperbolisch**.

Bemerkung 4.1.8

1. Jede zwei-dimensionale reguläre isotrope quadratische Form ist isometrisch zur hyperbolischen Ebene.

   Denn: Sei q eine solche Form und $u \neq 0$ ein isotropes Element. Da q regulär ist gibt es dazu ein w mit $B_q(u, w) = 1$. Sei $v = 2w - q(w)u$. Dann gilt $q(v) = 0$ und $B_q(u, v) = 2$. Seien nun $u' = \frac{1}{4}u + v$ und $v' = -\frac{1}{4}u + v$ Dann hat B_q bezüglich der Basis (u', v') die Gestalt einer hyperbolischen Ebene.

2. Ist q eine quadratische Form, so ist $q \perp -q$ hyperbolisch.

   Denn: Sei ohne Einschränkung der Allgemeinheit $q \cong< a_1, \ldots, a_n >$. Dann gilt $q \perp -q \cong< a_1, -a_1 > \perp \ldots \perp < a_n, -a_n > \overset{1.}{\cong} nH$.

Lemma 4.1.9
Sei q eine quadratische Form und seien $u, w \in V = K^n$ mit $q(u) = q(w) \neq 0$. Dann gilt $(Ku)^\perp \cong (Kw)^\perp$.

Beweis: Sei zunächst q regulär und sei $V' = Ku + Kw$. Es werden drei Fälle unterschieden:

1. Fall: $\dim V' = 1$. Dann gilt $Ku = Kw$ und damit $(Ku)^\perp = (Kw)^\perp$.

2. Fall: $\dim V' = 2$ und V' ist regulär. Dann folgt $V = V' \perp V'^\perp$ mit Lemma 4.1.4 (3) und es gibt Unterräume U und W von V (die orthogonalen Komplemente von Ku bzw Kw in V') mit $V' = Ku \perp U = Kv \perp W$. Für diese Räume gilt einerseits $\det U = \frac{\det V'}{\det Ku} = \frac{\det V'}{q(u)} = \frac{\det V'}{q(w)} = \det W$ und andererseits $\dim U = 1 = \dim V$, woraus $U \cong W$ folgt. Damit erhält man:

$$(Ku)^\perp = U \perp V'^\perp \cong W \perp V'^\perp = (Kw)^\perp$$

3. Fall: $\dim V' = 2$ und $\det V' = 0$. V' wird nun zu einem regulären 3-dimensionalen Raum ergänzt: v_0 ergänze u nach Satz 4.1.6 zu einer orthogonalen Basis von V'. Da V regulär ist, gibt es ein $v_1 \in V$ mit $B(v_0, v_1) = 1$. Sei $V'' = Kv_0 + Ku + Kv_1$. Dann hat V'' bezüglich der Basis (v_0, u, v_1) die Darstellung:

$$\begin{pmatrix} 0 & 0 & 1 \\ 0 & q(u) & * \\ 1 & * & * \end{pmatrix}$$

woraus $\det V'' = q(u) \neq 0$ folgt. Also ist V'' ein 3-dimensionaler regulärer Raum. Seien U und W die orthogonalen Komplemente von Ku und Kw, dann folgt wieder mit Lemma 4.1.4: $V'' = Ku \perp U = Kw \perp W$ und $V = V'' \perp V''^\perp$. Außerdem gilt $v_0 \in U \cap W$ ($v_0 \in U$: klar. $v_0 \in W$: Sei $w = \lambda u + \beta v_0 \in W$. Dann folgt $B(v_0, w) = \lambda B(v_0, u) + \beta B(v_0, v_0) = 0$). Da $q(v_0) = 0$ gilt, folgt $U \cong W$ mit Bemerkung 4.1.8 und damit

$$(Ku)^\perp = U \perp V''^\perp \cong W \perp V''^\perp = (Kw)^\perp$$

Sei nun q allgemein und sei $V = V^\perp \perp V_0$ eine Zerlegung von V in sein Radikal und einen regulären Anteil. Für Unterräume $U \subset V_0$ gilt dann $U^\perp = V^\perp \perp U^{\perp_0}$, wobei $U^{\perp_0}$ das orthogonale Komplement von U in V_0 bezeichnet. Da wegen eben bewiesenem $(Ku)^{\perp_0} \cong (Kw)^{\perp_0}$ gilt, folgt damit auch $(Ku)^\perp \cong (Kw)^\perp$. □

Satz 4.1.10 (Kürzungssatz von Witt)
Seien q_1, q_2, p quadratische Formen und sei p regulär. Dann gilt

$$q_1 \perp p \cong q_2 \perp p \quad \Longrightarrow \quad q_1 \cong q_2$$

Beweis: Der bequemeren Notation wegen verläuft der Beweis wieder über den Begriff des bilinearen Raumes. Es wird also gezeigt: Sind V_1, V_2, W bilineare Räume und W regulär, so folgt aus $V_1 \perp W \cong V_2 \perp W$ die Isometrie von V_1 und V_2.

Der Beweis erfolgt durch Induktion über die Dimension n von W:

Induktionsanfang: $n = 1$
Sei w eine Basis von W, $V := V_2 \perp W$, $\varphi : V_1 \perp W \longrightarrow V$ eine Isometrie und sei $u = \varphi(w)$. Dann folgt $q(u) = q(w) \neq 0$ und man erhält

$$V_1 \overset{\varphi}{\cong} (Ku)^{\perp} \overset{4.1.9}{\cong} (Kw)^{\perp} = W^{\perp} = V_2$$

Induktionsschritt: Sei $w \in W$ mit $q(w) \neq 0$. Dann gilt $W = Kw \perp (Kw)^{\perp}$ und aus der Induktionsvoraussetzung folgt

$$V_1 \perp (Kw)^{\perp} \cong V_2 \perp (Kw)^{\perp}$$

Da $\dim\,(Kw)^{\perp} < \dim W$ gilt, folgt $V_1 \cong V_2$ wieder aus der Induktionsvoraussetzung. □

Satz 4.1.11 (Zerlegungssatz von Witt)
Jede reguläre quadratische Form q hat eine orthogonale Zerlegung

$$q \quad \cong \quad q_0 \perp rH$$

in einen bis auf Isomorphie eindeutig bestimmten anisotropen Teil q_0, genannt der **Kern** *von q und einen hyperbolischen Teil. Dabei heißt das eindeutig bestimmte $r \in \mathbb{N}$ der* **Index** *von q. Eine solche Zerlegung heißt* **Wittzerlegung**.

Beweis: Der Beweis erfolgt durch Induktion über die Dimension n von q.
Induktionsanfang: n = 1: Da q regulär ist, ist q anisotrop , also gilt $q = q_0$.
Induktionsschritt: Ist q anisotrop, so folgt $q = q_0$. Ansonsten sei $u \neq 0$ ein isotropes Element und $v \in K^n$ mit $B(u, v) = 1$. Dann gilt $\det(q|Ku + Kv) = \det \begin{pmatrix} 0 & 1 \\ 1 & * \end{pmatrix} = -1 \neq 0$, also ist $q|Ku + Kv$ eine zwei-dimensionale reguläre isotrope Form und nach Bemerkung 4.1.8 isometrisch zur hyperbolischen Ebene. Sei außerdem noch $q' = q|(Ku + Kv)^{\perp}$, dann folgt $q \cong H \perp q'$. Ist q'' eine weitere Form mit $q \cong H \perp q''$ so folgt aus dem Kürzungssatz $q' \cong q''$. Aus der Induktionsvoraussetzung folgt nun die gewünschte eindeutige Zerlegung von q'. □

Definition 4.1.12
Zwei quadratische Formen q_1 und q_2 heißen **wittäquivalent** ($q_1 \sim q_2$), falls ihre Kerne äquivalent sind. Die Äquivalenzklasse einer Form q wird mit $[q]$, oder auch nur mit q bezeichnet.

Bemerkung 4.1.13 Die Äquivalenzklassen wittäquivalenter quadratischer Formen über einem Körper K zusammen mit den induzierten Operationen $\perp$ als Addition und $\otimes$ als Multiplikation bilden einen kummutativen Ring mit Eins, den sogenannten **Witt-Ring** $W(K)$. Dabei ist $0 := [H]$ das Nullelement und $1 := [< 1 >]$ das Einselement.

4.2 Pfister-Formen

In diesem Abschnitt wird der Begriff der Pfisterformen eingeführt und gezeigt, daß diese Formen immer multiplikativ sind, insbesondere ist also jede isotrope Pfisterform hyperbolisch. Diese Tatsache wird dann im nächsten Abschnitt Verwendung finden.

Die auftauchenden Sätze und Definitionen sind im Wesentlichen [20] Paragraph 3 entnommen.

Definition 4.2.1
Eine n-fache **Pfisterform** über einem Körper K ist eine Quadratische Form der Gestalt

$$\bigotimes_{i=1}^{n} < 1, a_i > \qquad \text{mit } a_i \in K^\times$$

und wird mit $\ll a_1, \ldots, a_n \gg$ bezeichnet.

Definition 4.2.2
Ist q eine quadratische Form, so **repräsentiert** q ein $\alpha \in K^\times$, wenn es ein $v \in V$ gibt mit $q(v) = \alpha$ und

$$D(q) := \{\alpha \in K^\times; \exists v \in V \quad q(v) = \alpha\}$$

heißt die **Wertemenge** von q. Falls $\alpha q \cong q$ für ein $\alpha \in K^\times$ gilt, so bezeichnet man α als **Ähnlichkeitsfaktor** von q, und mit

$$G(q) := \{\alpha \in K^\times; \alpha q \cong q\}$$

sei die Menge der Ähnlichkeitsfaktoren bezeichnet.

Bemerkung 4.2.3 $G(q)$ ist eine Gruppe und es gilt $(K^\times)^2 \subset G(q)$.

Definition 4.2.4
Eine quadratische Form q heißt **multiplikativ**, wenn sie

- anisotrop ist und $D(q) = G(q)$ gilt oder
- hyperbolisch ist, d.h. es gilt $[q] = 0$.

Bemerkung 4.2.5

1. $1 \in D(q) \Rightarrow G(q) \subset D(q)$.
   Denn: Sei $\alpha \in G(q)$, außerdem $v \in V$ mit $q(v) = 1$ und sei $\varphi : \alpha q \cong q$. Dann gilt $\alpha = \alpha q(v) = q(\varphi(v))$. Also folgt $\alpha \in D(q)$.
2. $< 1 >$ ist multiplikativ
   Denn: $q :=< 1 >$ ist anisotrop. Wegen $D(q) = (K^\times)^2 \subset G(q)$ und $1 \in D(q)$ folgt die Multiplikativität.

3. $< 1, a >$ ist für alle $a \in K^\times$ multiplikativ.
Denn: Ist die Form $q :=< 1, a >$ isotrop, so ist sie nach Bemerkung 4.1.8 hyperbolisch. Sei nun q anisotrop. Da $1 \in D(q)$, ist nur noch $D(q) \subset G(q)$ zu zeigen. Sei $\alpha \in D(q)$. Dann gibt es $\beta, \gamma \in K$ mit $\alpha = \beta^2 + a\gamma^2$. Hat q bzgl. (u, v) die Gestalt $< 1, a >$, so hat q bezüglich $(\beta u + \gamma v, -a\gamma u + \beta v)$ die Gestalt $< \beta^2 + a\gamma^2, a\beta^2 + a^2\gamma^2 >= \alpha < 1, a >$.

Lemma 4.2.6
Ist q eine multiplikative quadratische Form, so ist auch $q \otimes < 1, a >$ multiplikativ.

Beweis:

1. Fall: q isotrop.
Da q multiplikativ ist, muß $[q] = 0$ gelten, woraus $[q\otimes < 1, a >] = 0$ folgt.

2. Fall: q anisotrop und

(a) $q\otimes < 1, a >$ isotrop.
Da $q\otimes < 1, a >= q\perp aq$ gilt, gibt es $\alpha, \beta \in D(q)$ mit $\alpha + a\beta = 0$. Da q anisotrop und multiplikativ ist, gilt $D(q) = G(q)$ und daher folgt:

$$q\perp aq \cong \alpha q\perp a\beta q = \alpha q\perp -\alpha q$$

Mit Bemerkung 4.1.8 folgt daraus, daß $q\otimes < 1, a >$ hyperbolisch ist.

(b) $q\otimes < 1, a >$ anisotrop.
Da $1 \in D(q\otimes < 1, a >)$ liegt, genügt es wegen Bemerkung 4.2.5 zu zeigen, daß $D(q\otimes < 1, a >) \subset G(q\otimes < 1, a >)$ gilt. Sei also $\alpha \in D(q\otimes < 1, a >)$. Seien dazu $\beta, \gamma \in D(q) \cup \{0\}$ mit $\alpha = \beta + a\gamma$. Dann können folgende drei Fälle auftreten:
Ist $\gamma = 0$, d.h. $\alpha \in D(q) = G(q)$, dann folgt

$$\alpha(q\perp aq) = \alpha q\perp a\alpha q \cong q\perp aq$$

Ist $\beta = 0$, d.h. $\gamma \in D(q) = G(q)$, dann folgt

$$\alpha(q\perp aq) = a\gamma q\perp a^2\beta q \cong aq\perp q \cong q\perp aq$$

Ist schließlich $\beta, \gamma \neq 0$. Dann folgt

$$\begin{aligned}
\alpha(q\perp aq) &= (\beta + a\gamma)(q\perp aq) \\
&= \beta((1 + a\frac{\gamma}{\beta})(< 1, a > \otimes q)) \\
&\overset{4.2.3}{\cong} \beta((1 + a\frac{\gamma}{\beta})(< 1, a\frac{\gamma}{\beta} > \otimes q)) \\
&\overset{4.2.5(3)}{\cong} \beta(< 1, a\frac{\gamma}{\beta} > \otimes q)
\end{aligned}$$

$$\begin{aligned} &\cong \beta(q\perp a\frac{\gamma}{\beta}q) \\ &= \beta q\perp a\gamma q \\ &\cong q\perp aq \end{aligned}$$

□

Satz 4.2.7
Jede Pfisterform ist multiplikativ.

Beweis: Beweis durch Induktion über n:
Induktionsanfang: $n = 1$: siehe Bemerkung 4.2.5
Induktionsschritt: $\ll a_1, \ldots, a_n \gg = \ll a_1, \ldots, a_{n-1} \gg \otimes < 1, a_n >$ ist nach Induktionsvoraussetzung und obigem Lemma multiplikativ. □

Korollar 4.2.8
Jede isotrope Pfisterform ist hyperbolisch.

4.3 Quadratische Formen bzgl. Präpositivbereichen

Ziel dieses Abschnittes ist es, den Repräsentationssatz für T-Formen zu beweisen, d.h. ist T ein Präpositivbereich und sind $a_1, \ldots, a_n \in K^\times$, so gilt $b \in \sum_{i=1}^n T \cdot a_i \setminus \{0\}$ genau dann, wenn es $b_2, \ldots, b_n \in K^\times$ gibt, so daß $< a_1, \ldots, a_n >$ und $< b, b_2, \ldots, b_n >$ für alle Positivbereiche, die T enthalten, die gleiche Signatur haben. Der Repräsentationssatz wird dann im Beweis von Satz 4.4.1 - dem Ziel dieses Kapitels - Verwendung finden.

Die in diesem Abschnitt vorkommenden Definitionen und Sätze entstammen [23] Kapitel 1.

Definition 4.3.1
Sei T ein Präpositivbereich eines Körpers K und seien $a_1, \ldots, a_n \in K^\times$. Dann heißt der formale Ausdruck

$$q =< a_1, \ldots, a_n >_T$$

eine (diagonale) T-**Form** der Dimension n.

Definition 4.3.2
Ist $q =< a_1, \ldots, a_n >_T$ eine T-Form und $P \supset T$ ein Positivbereich, so ist die P-**Signatur** von q definiert durch

$$\operatorname{sgn}_P(q) := \sum_{i=1}^n \operatorname{sgn}_P(a_i)$$

mit

$$\mathrm{sgn}_P(a_i) := \begin{cases} 1 & \text{,falls } a_i \in P^\times \\ -1 & \text{,falls } a_i \notin P^\times \end{cases}$$

Definition 4.3.3
Für zwei T-Formen $< a_1, \ldots, a_n >_T$ und $< b_1, \ldots, b_n >_T$ ist die **orthogonale Summe** definiert durch

$$< a_1, \ldots, a_n >_T \perp < b_1, \ldots, b_n >_T := < a_1, \ldots, a_n, b_1, \ldots, b_n >_T$$

und das **Tensorprodukt** durch

$$< a_1, \ldots, a_n >_T \otimes < b_1, \ldots, b_n >_T := < \ldots, a_i b_j, \cdots >$$

Bemerkung 4.3.4 Für zwei T-Formen q und p und einen Positivbereich $P \supset T$ gilt:

$$\begin{aligned} \mathrm{sign}_P(q) &\equiv \dim q \quad (\mathrm{mod} 2) \\ \mathrm{sign}_P(q \perp p) &= \mathrm{sign}_P(q) + \mathrm{sign}_P(p) \\ \mathrm{sign}_P(q \otimes p) &= \mathrm{sign}_P(q) \cdot \mathrm{sign}_P(p) \end{aligned}$$

Definition 4.3.5
Zwei T-Formen heißen **T-isometrisch**, falls sie die gleiche Dimension und für alle Positivbereiche $P \supset T$ die gleiche Signatur haben. Sind q und p T-isometrisch so schreibt man $q \cong_T p$.

Bemerkung 4.3.6 Aus der Definition von T-isometrisch folgt:

$$< a_1, \ldots, a_n >_T \cong_T < a_1 t_1, \ldots, a_n t_n >_T \quad \text{für } a_i \in K^\times, t_i \in T^\times \tag{4.1}$$
$$< a, b >_T \cong_T < a + b, ab(a + b) >_T \quad \text{für } a, b, a + b \in K^\times \tag{4.2}$$

Definition 4.3.7
Eine T-Form q heißt **T-hyperbolisch** , falls $\mathrm{sgn}_P(q) = 0$ für alle Positivbereiche $P \supset T$ gilt. $q =< a_1, \ldots, a_n >_T$ heißt **T-isotrop**, falls es $(t_1, \ldots, t_n) \in T^n \setminus \{0\}$ mit $\sum_{i=1}^n a_i t_i = 0$ gibt. Sonst heißt q **T-anisotrop**. Ist speziell $T = \sum K^2$, so heißt eine T-isotrope Form **schwach isotrop**.

$$D_T(q) := \sum_{i=1}^n T \cdot a_i \setminus \{0\}$$

heißt die **T-Wertemenge** von q. Ist $\alpha \in D_T(q)$, so nennt man α auch **T-repräsentiert** durch q.

Lemma 4.3.8
Sei $q =< a_1, \ldots, a_n >_T$. Dann gilt:

1. *Für alle $r \in \mathbb{N}$ und $t_1, \ldots, t_r \in T^\times$ ist*
$$D_T(< t_1, \ldots, t_r > \otimes q) \overset{(a)}{=} D_T(q) \overset{(b)}{=} D_T(r \cdot q)$$
2. *Für alle $r \in \mathbb{N}$ gilt: q T-isotrop $\Leftrightarrow rq$ T-isotrop*
3. *q T-isotrop $\Leftrightarrow$ es gibt $t_1, \ldots, t_r \in T^\times$ so daß $< t_1, \ldots, t_r > \otimes < a_1, \ldots, a_n >$ isotrop ist.*

Beweis:

1. (a) **"$\subset$":** Sei $b \in D_T(< t_1, \ldots, t_r > \otimes q)$. D.h. es gibt $s_{ij} \in T$ mit
$$b = \sum_{i,j} s_{ij} t_i a_j = \sum_j \underbrace{(\sum_i s_{ij} t_i)}_{\in T} a_j$$
Also ist $b \in D_T(q)$.
"$\supset$": Sei umgekehrt $b \in D_T(q)$. Seien also $s_j \in T$ mit
$$b = \sum_j s_j a_j = \sum_j \underbrace{s_j t_j^{-1}}_{\in T} t_j a_j + \sum_{i \neq j} \underbrace{0}_{\in T} \cdot t_i a_j$$
Also ist $b \in D_T(< t_1, \ldots, t_r > \otimes q)$.
(b) Da $r \cdot q =< 1, \ldots, 1 > \otimes q$ folgt die Behauptung mit (a).

2. "$\Rightarrow$" klar
"$\Leftarrow$" Sei rq T-isotrop. Seien also $t_i^{(j)} \in T$ nicht alle Null, so daß
$$0 = \sum_{j=1}^r \sum_{i=1}^n t_i^{(j)} a_i = \sum_{i=1}^n \underbrace{\sum_{j=1}^r t_i^{(j)}}_{\in T} a_i$$
Ist $t_{i_0}^{(j_0)} \neq 0$, so ist auch $\sum_{j=1}^r t_{i_0}^{(j)} \neq 0$, also q T-isotrop.

3. "$\Rightarrow$" Sei $0 = \sum t_i a_i$ und $r \leq n$, so daß ohne Einschränkung $t_1, \ldots, t_r \neq 0$ und $t_{r+1}, \ldots, t_n = 0$ gilt. Dann ist $< t_1, \ldots, t_r > \otimes < a_1, \ldots, a_n >=$ $< t_1 a_1, \ldots t_r a_r, \ldots, t_i a_j, \cdots >$ isotrop.
"$\Leftarrow$" Ist $< t_1, \ldots, t_r > \otimes < a_1, \ldots, a_n >$ isotrop, so gibt es $q_{ij} \in K^2 \subset T$, die nicht alle Null sind, so daß
$$0 = \sum_{ij} q_{ij} t_i a_j = \sum_j \underbrace{\sum_i q_{ij} t_i}_{\in T} a_j$$
Wieder können nicht alle Summen Null sein. Also ist q T-isotrop.

□

Lemma 4.3.9 (Witt-Formel)
Für $a_1, \ldots, a_n \in T^\times$ gilt:

$$2^n < a_1, \ldots, a_n > \quad \sim \sum_{\substack{(\epsilon_1,\ldots,\epsilon_n) \\ \in \\ \{\pm 1\}^n}} < \epsilon_1, \ldots, \epsilon_n > \otimes \ll \epsilon_1 a_1, \ldots, \epsilon_n a_n \gg$$

Beweis: Es gilt $< \epsilon_i > \otimes \ll \epsilon_i a_i \gg \; = \; < \epsilon_i, \epsilon_i^2 a_i > \; \cong \; < \epsilon_i, a_i > \; \cong \; < a_i, \epsilon_i > \; \cong$ $< a_i, \epsilon_i a_i^2 > \; = \; < a_i > \otimes \ll \epsilon_i a_i \gg$, woraus $< \epsilon_1, ..., \epsilon_n > \otimes \ll \epsilon_1 a_1, ..., \epsilon_n a_n \gg$ $\cong < a_1, ..., a_n > \otimes \ll \epsilon_1 a_1, ..., \epsilon_n a_n \gg$ folgt. Damit genügt es zu zeigen, daß für alle $a_i \in K^\times$ gilt:

$$\sum_{\epsilon} \ll \epsilon_1 a_1, \ldots, \epsilon_n a_n \gg \sim 2^n < 1 >$$

Dies wird durch Induktion über n gezeigt:

Induktionsanfang: $n = 1$:
$\ll a_1 \gg \perp \ll -a_1 \gg \cong < 1, 1 > \perp < a_1, -a_1 > \sim < 1, 1 > = 2 < 1 >$.

Induktionsschritt:

$$\begin{aligned}
& \sum_{\epsilon \in \{\pm 1\}^n} \ll \epsilon_1 a_1, \ldots, \epsilon_n a_n \gg \\
= \; & \sum_{\epsilon \in \{\pm 1\}^{n-1}} (\ll \epsilon_1 a_1, \ldots, \epsilon_{n-1} a_{n-1}, a_n \gg \perp \ll \epsilon_1 a_1, \ldots, \epsilon_{n-1} a_{n-1}, -a_n \gg) \\
\cong \; & \sum_{\epsilon \in \{\pm 1\}^{n-1}} \ll \epsilon_1 a_1, \ldots, \epsilon_{n-1} a_{n-1} \gg \otimes (\ll a_n \gg \perp \ll -a_n \gg) \\
\overset{IV}{\sim} \; & 2^{n-1} < 1 > \otimes 2 < 1 > \\
= \; & 2^n < 1 >
\end{aligned}$$

□

Satz 4.3.10
Für ein T-Form $q = < a_1, \ldots, a_n >_T$ sind äquivalent:

1. *q ist T-hyperbolisch.*
2. *es gibt $t_1, \ldots, t_r \in T^\times$ mit $[\ll t_1, \ldots, t_r \gg \otimes < a_1, \ldots, a_n >] = 0$*
3. *es gibt $t_1, \ldots, t_r \in T^\times$ mit $[\, < t_1, \ldots, t_r > \otimes < a_1, \ldots, a_n >] = 0$*

Beweis:

"$2 \Rightarrow 3$": Es ist $\ll t_1, \ldots, t_r \gg = < u_1, \ldots u_s >$ mit $u_i = \prod t_j^{\epsilon_j}$ und $\epsilon_j \in \{0, 1\}$. Da $T^\times$ multiplikativ abgeschlossen ist, sind also auch die u_i aus $T^\times$ und $< u_1, \ldots, u_s >$ erfüllt die Anforderungen in (3).

"$3 \Rightarrow 1$": Sei $q = < a_1, \ldots, a_n >$. Dann bedeutet $[< t_1, \ldots, t_r > \otimes q] = 0$, daß es $s \in \mathbb{N}$ mit $< t_1, \ldots, t_r > \otimes q \cong s < -1, 1 >$ gibt. Dann muß aber $\mathrm{sgn}_P(< t_1, \ldots, t_r >) \cdot \mathrm{sgn}_P q = \mathrm{sgn}_P(< t_1, \ldots, t_r > \otimes q) = 0$ für jeden Positivbereich $P \supset T$ gelten. Mit $\mathrm{sgn}_P(< t_1, \ldots, t_r >) = r \neq 0$ folgt also $\mathrm{sgn}_P q = 0$.

"$1 \Rightarrow 2$": Sei $q = < a_1, \ldots, a_n >_T$ hyperbolisch und $\epsilon := (\epsilon_1, \ldots, \epsilon_n) \in \{\pm 1\}^n$. Sei ferner $T_\epsilon := T[\epsilon_1 a_1, \ldots, \epsilon_n a_n]$.

1. Fall: $-1 \notin T_\epsilon$. Dann gibt es einen Positivbereich $P \supset T_\epsilon$. Für dieses P gilt $\epsilon_i a_i \in P$ für alle $i = 1, \ldots, n$, was gleichbedeutend ist mit $\mathrm{sgn}_P \epsilon_i = \mathrm{sgn}_P a_i$. Daraus folgt $\mathrm{sgn}_P < \epsilon_1, \ldots, \epsilon_n > = \mathrm{sgn}_P q = 0$ und wegen $\epsilon_i \in \{\pm 1\}$ bedeutet dies gerade $< \epsilon_1, \ldots, \epsilon_n > \cong \frac{n}{2} H$, also $[< \epsilon_1, \ldots, \epsilon_n >] = 0$.
2. Fall: $-1 \in T_\epsilon$. Sei $q_\epsilon := \ll \epsilon_1 a_1, \ldots, \epsilon_n a_n \gg$. Dann gilt $D_T(q_\epsilon) = T_\epsilon \setminus \{0\}$. Insbesondere gilt also $\pm 1 \in D_T(q_\epsilon)$ und damit ist $2 q_\epsilon$ eine T-isotrope Form. Wegen Lemma 4.3.8 (2) ist dann auch q_ϵ eine T-isotrope Form und mit Lemma 4.3.8 (3) gibt es $t_1^\epsilon, \ldots, t_m^\epsilon \in T^\times$, so daß $< t_1^\epsilon, \ldots, t_m^\epsilon > \otimes q_\epsilon$ isotrop ist. Dann ist $\ll t_1^\epsilon, \ldots, t_m^\epsilon \gg \otimes q_\epsilon$ erst recht isotrop. Da dies eine Pfisterform ist muß sie laut Korollar 4.2.8 schon hyperbolisch sein.

Setzt man $\ll t_1, \ldots, t_r \gg := \bigotimes_{-1 \in T_\epsilon} \ll t_1^\epsilon, \ldots, t_m^\epsilon \gg$ und multipliziert dies mit der Witt-Formel 4.3.9, so erhält man $[\ll t_1, \ldots, t_r \gg \otimes q] = 0$.

□

Bemerkung 4.3.11 Aus 4.3.10 (3) und 4.3.8 (3) erhält man:

$$q \quad T-\text{hyperbolisch} \qquad \Longrightarrow \qquad q \quad T-\text{isotrop}$$

Satz 4.3.12 (Repräsentationssatz)
Sei $b_1 \in K^\times$ und $q = < a_1, \ldots, a_n >$. Dann gilt:

$$b_1 \in D_T(q) \Leftrightarrow \exists b_2, \ldots, b_n \in K^\times \quad q \cong_T < b_1, b_2, \ldots, b_n >_T$$

Beweis:

"$\Leftarrow$": Sei $b_1 \in D_T(q)$, seien also $t_1, \dots, t_n \in T$ mit $b_1 = a_1t_1 + \cdots + a_nt_n$. Sei zunächst $a_1t_1 + \cdots + a_it_i \neq 0$ und $t_i \neq 0$ für alle $1 \leq i \leq n$. Wegen (4.2) folgt dann $< a_1, \dots, a_n > \cong_T < a_1t_1, \dots, a_nt_n >$ und durch n-faches Anwenden von (4.2) erhält man $< a_1, \dots, a_n > \cong < b_1, \dots, b_n >$ mit

$$b_k = (a_kt_k \sum_{i=1}^{k-1} a_it_i)(\sum_{i=1}^{k} a_it_i) \quad \text{für } 2 \leq k \leq n$$

Seien nun die t_i allgemein, aber ohne Einschränkung so gewählt, daß es ein $r \in \mathbb{N}$ gibt mit $t_i \neq 0$ für $i \leq r$ und $t_i = 0$ für $i > r$. Gibt es ein i mit $a_it_i + \cdots + a_nt_n = 0$, so sei $s := \min\{i; a_it_i + \cdots + a_nt_n = 0\} - 1$. Dann ist $b_1 \in D_T(< a_1, \dots, a_s >)$ und mit oben Bewiesenem erhält man $b_i \in K^\times$ mit $< a_1, \dots, a_s > \cong < b_1, \dots, b_s >$. Also gilt

$$< a_1, \dots, a_n > \cong < b_1, \dots, b_s, a_{s+1}, \dots, a_n >$$

"$\Rightarrow$": Sei $< a_1, \dots, a_n > \cong < b_1, \dots, b_n >$, dann gilt

$$\begin{aligned} & \operatorname{sign}_P(< a_1, \dots, a_n, -b_1, \dots, -b_n >) \\ = \; & \operatorname{sign}_P(< a_1, \dots, a_n >) - \operatorname{sign}_P(< b_1, \dots, b_n >) \\ = \; & 0 \end{aligned}$$

für alle Positivbereiche $P \supset T$. Also ist $< a_1, \dots, a_n, -b_1, \dots, -b_n >$ eine T-hyperbolische Form und wegen Satz 4.3.10 gibt es $t_1, \dots, t_r \in T^\times$ mit

$$\begin{aligned} 0 &= [< t_1, \dots, t_r > \otimes < a_1, \dots, a_n, -b_1, \dots, -b_n >] \\ &= [< t_1, \dots, t_r >]([< a_1, \dots, a_n >] - [< b_1, \dots, b_n >]) \end{aligned}$$

Also folgt:

$$< t_1, \dots, t_r > \otimes < a_1, \dots, a_n > \sim < t_1, \dots, t_r > \otimes < b_1, \dots, b_n > \tag{4.3}$$

Da die beiden Formen auf der rechten und linken Seite von (4.3) die selbe Dimension haben, müssen sie schon als gewöhnliche quadratische Formen isometrisch sein und es folgt:

$$\begin{aligned} t_1b_1 &\in D(< t_1, \dots, t_r > \otimes < b_1, \dots, b_n >) \\ &= D(< t_1, \dots, t_r > \otimes < a_1, \dots, a_n >) \\ &\subset D_T(< t_1, \dots, t_r > \otimes q) \\ &\overset{4.3.8}{=} D_T(q) \end{aligned}$$

Damit folgt: $b_1 \in t_1^{-1} D_T(q) = D_T(q)$.

$\square$

4.4 Stetige schwache Isotropie quadratischer Formen über reell abgeschlossenen Körpern

In diesem Abschnitt wird nun das Ziel dieses Kapitels erreicht. Es wird gezeigt: Ist R ein reell abgeschlossener Körper und sind $f_1, \ldots, f_k \in R[X_1, \ldots, X_n] \setminus \{0\}$ Polynome, so daß $< f_1(x), \ldots, f_k(x) >$ für alle x mit $\bigwedge f_i(x) \neq 0$ eine $\sum R^2$-hyperbolische Form ist, so ist $< f_1, \ldots, f_k >$ schwach isotrop in $R(X_1, \ldots, X_n)$. Dabei können die Koeffizienten der Polynome, die die schwache Isotropie belegen, in stetiger Abhängigkeit von den Koeffizienten der f_i gewählt werden.

Dieser Abschnitt folgt [3].

Satz 4.4.1 (Hauptsatz)
Sei $f_d(C, X)$ das allgemeine Polynom vom Grad d in den n Variabeln $X = (X_1, \ldots, X_n)$ mit den $m = \binom{n+d}{d}$ Koeffizientenvariabeln $C = (C_1, \ldots, C_m)$. Sei $k \in \mathbb{N}$ gerade und sei $\mathbf{C} = (C^1, \ldots, C^k)$ mit $C^i = (C_1^i, \ldots, C_m^i)$ und $f_i = f_d(C^i, X)$. Sei ferner $B = \{\max\min p_{ij}; p_{ij} \in \mathbb{Z}[\mathbf{C}]\}$. Dann gibt es ein $N \in \mathbb{N}$, sowie $h_{ij} \in \mathbb{Z}[\mathbf{C}, X]$ und $\alpha_{ij} \in B$ für $i = 1, \ldots, k$ und $j = 1, \ldots, N$, so daß gilt:

$$\sum_i f_i \sum_j \alpha_{ij} h_{ij}^2 = 0 \tag{4.4}$$

Ist R ein reell abgeschlossener Körper mit $\mathbf{a} \in R^{km}$, so daß $a^i \neq 0$ für alle $i = 1, \ldots, k$ gilt, so gibt es ein i mit $\sum_j \alpha_{ij}(\mathbf{a}) h_{ij}(\mathbf{a}, X)^2 \neq 0$. Ist außerdem

$$\varphi(\mathbf{a}) = \forall x \quad \left(\bigwedge_{i=1}^{k} f_d(a^i, x) \neq 0 \rightarrow \mathrm{sgn}_P < f_d(a^1, x), \ldots, f_d(a^k, x) >= 0 \right)$$

und gilt $R \models \varphi(\mathbf{a})$, so sind alle $\alpha_{ij}(\mathbf{a}) \geq 0$.

Analog zur Vorgehensweise im letzten Kapitel wird der Satz zunächst in den handlicheren Satz 4.4.4 umformuliert. Dazu dienen die folgenden zwei Bemerkungen.

Bemerkung 4.4.2 Zur einfacheren Schreibweise sei die Indexmenge $I = \{\nu \in \{1, \ldots, k\}^k; \nu_1 < \cdots < \nu_{\frac{k}{2}} \wedge \nu_{\frac{k}{2}+1} < \cdots < \nu_k \wedge (i \neq j \rightarrow \nu_i \neq \nu_j)\}$ definiert. Dann gilt:

$$\begin{aligned} & \{\mathbf{a} \in R^{km}; R \models \varphi(\mathbf{a})\} \\ = \quad & \{\mathbf{a} \in R^{km}; R \models \forall x \quad \left(\bigwedge_{i=1}^{k} f_d(a^i, x) \neq 0 \right. \\ & \left. \rightarrow \bigvee_{\nu \in I} \left(\bigwedge_{i=1}^{\frac{k}{2}} f_d(a^{\nu_i}, x) \leq 0 \wedge \bigwedge_{i=\frac{k}{2}+1}^{k} f_d(a^{\nu_i}, x) \geq 0 \right) \right) \} \end{aligned}$$

$$= \quad \{\mathbf{a} \in R^{km}; R \models \forall x \quad \left(\bigvee_{i=1}^{k} f_d(a^i, x) = 0 \right.$$
$$\left. \vee \bigvee_{\nu \in I} \left(\bigwedge_{i=1}^{\frac{k}{2}} f_d(a^{\nu_i}, x) \leq 0 \wedge \bigwedge_{i=\frac{k}{2}+1}^{k} f_d(a^{\nu_i}, x) \geq 0 \right) \right) \}$$

Setzt man nun

$$\begin{aligned} M_i^{=}(x) &:= R^{(i-1)m} \times \{a \in R^m; f_d(a, x) = 0\} \times R^{(k-i)m} \\ M_i^{\geq}(x) &:= R^{(i-1)m} \times \{a \in R^m; f_d(a, x) \geq 0\} \times R^{(k-i)m} \\ M_i^{\leq}(x) &:= R^{(i-1)m} \times \{a \in R^m; f_d(a, x) \leq 0\} \times R^{(k-i)m} \end{aligned}$$

so kann man dies auch schreiben als

$$\bigcap_{x \in R^n} \left(\bigcup_{i=1}^{k} M_i^{=}(x) \cup \bigcup_{\nu \in I} \left(\bigcap_{i=1}^{\frac{k}{2}} M_{\nu_i}^{\leq}(x) \cap \bigcap_{i=\frac{k}{2}+1}^{k} M_{\nu_i}^{\geq}(x) \right) \right)$$

was die Abgeschlossenheit von $\{\mathbf{a} \in R^{km}; R \models \varphi(\mathbf{a})\}$ in R^{km} impliziert. Unter Verwendung des Endlichkeitssatzes erhält man daher endlich viele Polynome $p_{ij} \in \mathbb{Z}[\mathbf{C}]$ mit

$$R \models \forall \mathbf{C} \quad \varphi(\mathbf{C}) \leftrightarrow \bigvee_i \bigwedge_j p_{ij}(\mathbf{C}) \geq 0$$

Seien

$$p_i(\mathbf{a}) = \min_j p_{ij}(\mathbf{a}) \quad \text{und} \quad p(\mathbf{a}) = \max_i p_i(\mathbf{a})$$

Sei $A \subset B[X]$ der von $\mathbb{Z}[\mathbf{C}, X]$, p_i und p erzeugte Ring und sei $S \subset A$ der Halbring, der von A^2, $p_{ij} - p_i$, $p - p_i$ und p erzeugt wird. Mit der multiplikativ abgeschlossenen Menge $F := \{f_1^{\nu_1} \cdot \ldots \cdot f_k^{\nu_k}; \nu_1, \ldots, \nu_k \in \mathbb{N}\}$ seien

$$\begin{aligned} A_F &:= \{\frac{a}{f}; a \in A, f \in F\} \\ S_F &:= \{\frac{s}{f^2}; s \in S, f \in F\} \end{aligned}$$

Unter Verwendung dieser Bezeichnungen gilt folgende Bemerkung:

Bemerkung 4.4.3 S_F ist ein Präpositivbereich von A_F.
Denn: Ann: $-1 \in S_F$.
Dann gibt es $s \in S$ und $f \in F$ mit $f^2 + s = 0$. Sei nun $\mathbf{a}$ so, daß $f_{2i} = 1$ und $f_{2i+1} = -1$ gilt. Dann ist $\varphi(\mathbf{a})$ erfüllt und es folgt $p(\mathbf{a}) \geq 0$. Somit ist auch $s(\mathbf{a}, x) \geq 0$ und damit $f^2(\mathbf{a}, x) + s(\mathbf{a}, x) \geq 1 > 0$ für alle x. Daher kann $f^2 + s$ nicht die Nullfunktion sein.

Satz 4.4.4
Es gibt $s_1, \ldots, s_k \in S_F$ mit $(1 + s_1)f_1 + \sum_{i=2}^{k} s_i f_i = 0$

Zum Beweis des Satzes wird noch ein Lemma benötigt:

Lemma 4.4.5
Sei A ein kommutativer Ring mit Eins, sei $\mathfrak{A}$ ein Ideal von A und $\mathfrak{P} \supset \mathfrak{A}$ ein minimales Primideal. Sei weiter $a \in \mathfrak{P}$. Dann gilt:
Es gibt ein $b \in A \setminus \mathfrak{P}$ mit $ab \in \mathrm{rad}\mathfrak{A}$, d.h. es gibt ein $n \in \mathbb{N}$ mit $(ab)^n \in \mathfrak{A}$.

Beweis: Sei $V := \{ba^n; b \in A \setminus \mathfrak{P}, \quad n \in \mathbb{N}\}$.
Ann: $V \cap \mathrm{rad}\mathfrak{A} = \phi$.
Wegen Lemma 1.3.1 gibt es dann ein Primideal $\mathfrak{P}' \supset \mathfrak{A}$, so daß $\mathfrak{P}' \cap V = \phi$. Da $a \in V$ gilt, folgt $a \notin \mathfrak{P}'$ und damit $\mathfrak{P} \neq \mathfrak{P}'$. Andererseits gilt aber auch $\mathfrak{P}' \subset \mathfrak{P}$, denn sei $x \notin \mathfrak{P}$, dann folgt $xa \in V$, was $xa \notin \mathfrak{P}'$ und damit $x \notin \mathfrak{P}'$ impliziert. Insgesamt bedeutet dies:

$$\mathfrak{P} \underset{\neq}{\supseteq} \mathfrak{P}' \supset \mathrm{rad}\mathfrak{A} \supset \mathfrak{A}$$

im Widerspruch zur Minimalität von $\mathfrak{P}$.

Seien also $b \in A \setminus \mathfrak{P}$ und $n \in \mathbb{N}$ mit $ba^n \in \mathrm{rad}\mathfrak{A}$. Sei etwa $b^k a^{nk} \in \mathfrak{A}$. Da $\mathfrak{A}$ ein Ideal ist, gilt dann auch $(ba)^{nk} = b^{k(n-1)} b^k a^{nk} \in \mathfrak{A}$ und damit $ba \in \mathrm{rad}\mathfrak{A}$. □

Beweis: von Satz 4.4.4
Sei

$$T := S_F + \sum_{i=2}^{k} S_F a_i \quad \text{mit} \quad a_i = f_i f_1$$

Dann gilt $S_F \cdot T, T + T \subset T$ und $1 \in T$. Im Folgenden soll nun $-1 \in T$ gezeigt werden. Ist das gezeigt, so gibt es $s_1, s_2', \ldots, s_k' \in S_F$ mit

$$-1 = s_1 + \sum_{i=2}^{k} s_i' f_i f_1$$

Die Elemente s_1 und $s_i = s_i' f_1^2$ für $i = 2, \ldots, k$ erfüllen dann die geforderten Eigenschaften.

Sei nun

$$\mathfrak{A} = \{a \in A_F; -a^2 \in T\}$$

Ist $\mathfrak{A} = A_F$, so folgt $-1 \in T$ aus $1 \in A_F$ und es ist alles gezeigt. Sei also das Gegenteil angenommen, d.h.:

Ann: $\mathfrak{A} \neq A_F$

$\mathfrak{A}$ ist ein Ideal von A_F. (Für $a, b \in \mathfrak{A}$, $x \in A_F$ gilt $-(xa)^2 = x^2(-a^2) \in T$, $-(a+b)^2 = (a-b)^2 - 2a^2 - 2b^2 \in T$ und $-(-a)^2 = -a^2 \in T$. Außerdem liegt $0 \in \mathfrak{A}$.) Sei $\mathfrak{P} \supset \mathfrak{A}$ ein minimales Primideal und sei K der Quotientenkörper von $A_F/\mathfrak{P}$.

Es gilt $S_F/\mathfrak{P} \cap -S_F/\mathfrak{P} = \{0\}$: Sonst seien $s_1, s_2 \in S_F \setminus \mathfrak{P}$ mit $s_1 + s_2 \in \mathfrak{P}$. Nach Lemma 4.4.5 gibt es dann ein $b \in A_F \setminus \mathfrak{P}$ mit $b(s_1 + s_2) \in \mathrm{rad}\mathfrak{A}$, d.h. es gibt ein $n \in \mathbb{N}$ mit $b^n(s_1 + s_2)^n \in \mathfrak{A}$, woraus $-b^{2n}(s_1 + s_2)^{2n} \in T$ folgt. Sei $s' = (s_1 + s_2)^{2n} - s_1^{2n}$. Dann ist $s' \in S_F$ und es gilt $-(bs_1)^{2n} = -b^{2n}(s_1 + s_2)^{2n} + b^{2n}s' \in T$ und damit $(bs_1)^n \in \mathfrak{A} \subset \mathfrak{P}$, woraus $b \in \mathfrak{P}$ oder $s_1 \in \mathfrak{P}$ folgt, im Widerspruch zur Wahl von b und s_1 aus $A_F \setminus \mathfrak{P}$.

Also ist $S_F/\mathfrak{P}$ ein Präpositivbereich von $A_F/\mathfrak{P}$, der einen Präpositivbereich S' von K induziert. Da $f_i \in A_F^\times$ gilt, folgt $\overline{f_i} \neq 0$. Es können nun die folgenden zwei Fälle auftreten, die beide noch zu einem Widerspruch geführt werden müssen:

1. Fall: $\mathrm{sgn}_P(\overline{f_1}, \ldots, \overline{f_k}) = 0$ für alle Positivbereiche $P \supset S'$ von K .
Da multiplizieren mit $\overline{f_1}$ alle oder kein Vorzeichen verändert, ist dann auch $\mathrm{sgn}_P(\overline{f_1^2}, \overline{f_1 f_2}, \ldots, \overline{f_1 f_k}) = 0$ und wegen $\overline{f_1^2} \in P^\times$ auch $\mathrm{sgn}_P(1, \overline{a_2}, \ldots, \overline{a_k}) = 0$ für alle Positivbereiche $P \supset S'$. Daraus folgt, daß

$$< 1, \overline{a_2}, \ldots, \overline{a_k} >_{S'} \cong_{S'} < -1, 1, \ldots, -1, 1 >_{S'}$$

Aus dem Repräsentationssatz 4.3.12 folgt daher

$$-1 \in S' + \sum_{i=2}^{k} S'\overline{a_i}$$

Ist s das Produkt der in dieser Gleichung auftretenden Nenner aus S_F, dann ist $s \in S_F \setminus \mathfrak{P}$ und es gibt ein $t \in T$ mit $s + t \in \mathfrak{P}$. Nach Lemma 4.4.5 gibt es dann wieder ein $b \in A_F \setminus \mathfrak{P}$ mit $b(t+s) \in \mathrm{rad}\mathfrak{A}$. Sei $t' = b^2 t$ und $s' = b^2 s$. Dann ist $t' \in T$ und $s' \in S_F \setminus \mathfrak{P}$ und es gilt $t' + s' \in \mathrm{rad}\mathfrak{A}$. Also gibt es ein $n \in \mathbb{N}$ mit $(t' + s')^n \in \mathfrak{A}$. Sei $s'' = s'^n$ und $t'' = (t' + s')^n - s'^n$. Dann gilt wieder $s'' \in S_F \setminus \mathfrak{P}$ und $t'' \in T$. Mit $-t''^2 - 2s''t'' - s''^2 = -(t'' + s'')^2 \in T$ folgt also $-s''^2 \in T$, woraus $s'' \in \mathfrak{A} \subset \mathfrak{P}$ folgt, im Widerspruch zu $s'' \in S_F \setminus \mathfrak{P}$.

2. Fall: $\operatorname{sgn}_P(\overline{f_1}, \ldots, \overline{f_k}) \neq 0$ für einen Positivbereich $P \supset S'$ von K. Sei dann R' der reelle Abschluß von K bzgl. P. Nach Lemma 3.1.5 auf Seite 28 folgt $R' \models \bigvee_i \bigwedge_j p_{ij}(\overline{\mathbf{a}}) \geq 0$, d.h.

$$R' \models \exists \mathbf{C}, X \quad \operatorname{sgn}_{R'^2} \left\langle f_d(C^1, X), \ldots, f_d(C^k, X) \right\rangle \neq 0 \\ \wedge \bigwedge_i f_d(C^i, X) \neq 0 \wedge \bigvee_i \bigwedge_j p_{ij}(\mathbf{C}) \geq 0 \quad (4.5)$$

Nach dem Tarskiprinzip gilt dies dann auch in R, woraus

$$R \models \neg \forall \mathbf{C} \forall X \quad \left(\bigwedge_{i=1}^{k} f_d(C^i, X) \neq 0 \right. \\ \left. \rightarrow \operatorname{sgn}_{R^2} < f_d(C^1, X), \ldots, f_d(C^k, X) >= 0 \right) \\ \leftrightarrow \bigvee_i \bigwedge_j p_{ij}(\mathbf{C}) \geq 0 \quad (4.6)$$

folgt (vgl. den Beweis zu Satz 3.1.1 auf Seite 27) im Widerspruch zur Wahl der p_{ij}.

□

Beweis: von Satz 4.4.1.
Multipliziert man in Satz 4.4.4 die Nenner hoch (dies sind nur Quadrate aus F), so erhält man eine Gleichung in der gewünschten Form. Die α_{ij} sind dabei Summen von Produkten von $p_{ij} - p_i$, $p - p_i$ und p. Dabei sind $p_{ij} - p_i$ und $p - p_i$ auf ganz R^{km} und p auf $\{\mathbf{a} \in R^{km}; \varphi(\mathbf{a})\}$ nicht negativ. Da $-1 \notin S_F$ gilt, garantiert Satz 4.4.4, daß der Faktor mit Index $i = 1$ nicht verschwindet. □

Kapitel 5

Konstruktive stetige Quadratsummendarstellung positiv semidefiniter Polynome in einer Variabeln über den reellen Zahlen

Nach einem Skript von Martin Ziegler (Freiburg) vom 5.9.88.

Die bisherigen Beweise der drei Sätze über stetige Darstellungen verliefen alle nach mehr oder weniger dem selben Muster - und sie enthielten alle einen Widerspruchsbeweis. Daher soll hier noch ein konstruktiver Beweis der stetigen Abhängigkeit der Koeffizienten in einem Spezialfall des 17. Hilbertschen Problems vorgestellt werden.

Definition 5.1.1
Es werden folgende Bezeichnungen eingeführt:

$$\begin{array}{rcl} P_n & := & \{p \in \mathbb{R}[X]; \deg p \leq n\} \\ P_{2n}^+ & := & \{p \in P_{2n}; \forall x \in \mathbb{R} \quad p(x) \geq 0\} \\ P_{2n}^{++} & := & \{\sum a_i X^i \in P_{2n}^+; a_{2n} > 0\} \end{array}$$

Dabei sei P_n durch die kanonische Isomorphie zu $\mathbb{R}^{n+1}$ topologisiert.

Bemerkung 5.1.2 Es gilt:

- $P_{2n}^+ \subset P_{2n}$ abgeschlossen.

  Denn: Für $a \in \mathbb{R}$ ist die Abbildung

$$\begin{array}{rcccc} F_a & : & P_{2n} & \longrightarrow & \mathbb{R} \\ & & p & \longmapsto & p(a) \end{array}$$

stetig und damit ist $P_{2n}^{+} = \bigcap_{a\in\mathbb{R}} F_a^{-1}(\mathbb{R}_0^{+}) \subset P_{2n}$ abgeschlossen.

- $P_{2n}^{++} \subset P_{2n}^{+}$ offen.
  Denn: Die Abbildung
  $$\begin{array}{cccc} F & : & P_{2n}^{+} & \longrightarrow & \mathbb{R} \\ & & \sum a_i X^i & \longmapsto & a_{2n} \end{array}$$
  ist als Projektion auf die $2n$-te Komponente stetig und damit ist das Urbild $P_{2n}^{++} = F^{-1}(\mathbb{R}^{+}) \subset P_{2n}^{+}$ offen.

Bemerkung 5.1.3 Sei $p \in P_{2n}^{++}$ und seien $\lambda_1, \ldots, \lambda_{2n}$ die (möglicherweise komplexen) Nullstellen von p. Dann läßt sich p schreiben als

$$p = a^2 \prod_{i=1}^{2n} (X - \lambda_i)$$

Die Reihenfolge der Nullstellen kann man dabei so wählen, daß $\lambda_{2i-1} = \overline{\lambda_{2i}}$ für alle $i = 1, \ldots, n$ gilt.

Denn:

- Der Leitkoeffizient muß positiv sein, da p sonst für große x negative Werte annehmen würde. Da $\mathbb{R}$ reell abgeschlossen ist, läßt er sich also als Quadrat schreiben.

- Für alle Nullstellen $\lambda \in \mathbb{C}$ von p gilt $p(\overline{\lambda}) = \overline{p(\lambda)} = 0$ und durch sukzessive Polynomdivision von p durch $(X - \lambda)(X - \overline{\lambda})$ erhält man, daß λ und $\overline{\lambda}$ gleiche Vielfachheit haben. Ist $\lambda \notin \mathbb{R}$, dann gilt $\overline{\lambda} \neq \lambda$ und man erhält die Bedingung an die Reihenfolge der Nullstellen, indem man $\overline{\lambda}$ auf λ folgen läßt.

- Für $\lambda \in \mathbb{R}$ gilt, daß 2 die Vielfachheit von λ teilt:
  Denn sei
  $$p = \prod (X - \underbrace{\lambda_i}_{\in\mathbb{R}})^{2\mu_i + \epsilon_i} \prod ((X - \underbrace{\lambda_i}_{\in\mathbb{C}\setminus\mathbb{R}})(X - \overline{\lambda_i}))^{\delta_i}$$
  so daß $\epsilon_i \in \{0, 1\}$ und die λ_i alle verschieden sind. Dann gilt
  $$p(a) = \underbrace{\prod (a - \lambda_i)^{2\mu_i} \prod |a - \lambda_i|^{2\delta_i}}_{\geq 0} \prod (a - \lambda_i)^{\epsilon_i}$$
  für $a \in \mathbb{R}$. Ist $q = \prod (X - \lambda_i)$, so genügt es also zu zeigen, daß es ein $a \in \mathbb{R}$ mit $q(a) < 0$ gibt.
  Es gilt $q'(\lambda_k) = \prod_{i\neq k} (\lambda_k - \lambda_i) \neq 0$. Sei ohne Einschränkung $q'(\lambda_k) > 0$. Dann gilt in einer Umgebung um λ_k
  $$x < \lambda_k \Rightarrow q(x) < q(\lambda_k) = 0$$

Da aber $p(a) \geq 0$ für alle $a \in \mathbb{R}$ ist, müssen zwangsläufig schon alle $\epsilon_i = 0$ gewesen sein.

Lemma 5.1.4
Ist $F : P_{2n}^{+} \longrightarrow P_n$ eine Abbildung für die $(F(p)(x))^2 \leq p(x)$ für alle $x \in \mathbb{R}$ gilt, so bildet F beschränkte Mengen in beschränkte Mengen ab.

Beweis: Sei $\|.\|$ die Maximumsnorm und sei $M \subset P_{2n}^{+}$ beschränkt. Sei also $\mu \in \mathbb{N}$, so daß $\|p\| \leq \mu$ für alle $p \in M$ gilt. Dann gilt für alle $p = \sum a_i X^i$ und für alle $x \in \mathbb{R}$ die Gleichung

$$|F(p)(x)| \leq \sqrt{p(x)} = \sqrt{\sum a_i x^i} \leq \sqrt{\mu}\sqrt{\sum |x|^i}$$

Mit dem Lagrangen-Interpolationspolynom an den Stützstellen $0, \ldots, n$ läßt sich $F(p)$ schreiben als

$$\sum_{k=0}^{n} F(p)(k) \prod_{\substack{j=0 \\ j \neq k}}^{n} \frac{j-X}{j-k} =: \sum_{k=0}^{n} \left(\sum_{j=0}^{n} c_j^{(k)} F(p)(j) \right) X^k$$

wobei die $c_j^{(k)}$ von p unabhängige rationale Zahlen sind. Damit ist

$$\|F(p)\| \leq \max\{\sum_{j=0}^{n} |c_j^{(k)}| \sqrt{\mu} \sqrt{\sum_{i=0}^{n} |j|^i}; 0 \leq k \leq n\} = \text{const}$$

für alle $p \in M$ durch eine Konstante beschränkt. □

Lemma 5.1.5
Für Polynome $p \in \mathbb{R}[X]$ gilt:

$$\|p\| \to 0 \Leftrightarrow \forall x \in \mathbb{R} \quad |p(x)| \to 0.$$

Beweis:

"$\Rightarrow$" Sei $x \in \mathbb{R} \setminus \{0\}$ und sei $\epsilon > 0$. Da $\|p\| \to 0$ geht, können die Koeffizienten von p durch jedes positive δ beschränkt werden. Sei etwa $\delta = \frac{\epsilon}{\sum |x|^i}$. Dann gilt $|p(x)| < \delta \sum |x|^i = \epsilon$. Für $x = 0$ ist $|p(0)|$ der Betrag des konstanten Koeffizienten und man kann $\delta := \epsilon$ setzen.

"$\Leftarrow$" Sei $\epsilon > 0$. Wie in obigem Lemma kann man die Koefizienten b_i von p mit Hilfe des Lagrangen Interpolationspolynoms schreiben als $b_i = \sum c_i^j p(j)$ mit von p unabhängigen c_i^j (insbesondere gilt $\sum |c_i^j| \neq 0$). Da $p(x)$ gegen Null geht, kann man die Werte von p durch jedes positive δ abschätzen. sei etwa $\delta = \frac{\epsilon}{\sum |c_i^j|}$. Dann folgt $|b_i| < \delta \sum |c_i^j| = \epsilon$.

□

Lemma 5.1.6
Es gibt stetige definierbare Abbildungen

$$g_{2n} : P_{2n}^{++} \longrightarrow P_n$$

mit den folgenden Eigenschaften:

1. *für alle* $p \in P_{2n}^{++}$ *gilt* $p - (g_{2n}(p))^2 \in P_{2n-2}^{+}$
2. g_{2n} *bildet beschränkte Mengen auf beschränkte Mengen ab.*

Beweis: Sei $p = a^2 \prod_{i=1}^{2n}(X - \lambda_i)$ wie in Bemerkung 5.1.3 und sei

$$g_{2n}(p) := a \prod_{i=1}^{n}(X - \mathrm{Re}\lambda_{2i}) \quad \text{mit} \quad a > 0$$

Dann erfüllt g_{2n} die Bedingungen 1 und 2:

1. Sei $2m$ die Anzahl der reellen Nullstellen und es gelte ohne Einschränkung $\lambda_1, \dots, \lambda_{2m} \in \mathbb{R}$ und $\lambda_{2m+1}, \dots, \lambda_{2n} \in \mathbb{C} \setminus \mathbb{R}$. Hat p nur reelle Nullstellen, so folgt $p - (g_{2n}(p))^2 = 0 \in P_{2n-2}^{+}$. Sei also $m < n$. Dann gilt:

$$\begin{aligned} p - (g_{2n}(p))^2 &= a^2 \prod_{i=1}^{n}(X - \lambda_{2i})(X - \overline{\lambda_{2i}}) - a^2 \prod_{i=1}^{n}(X - \mathrm{Re}\lambda_{2i})^2 \\ &= a^2 \prod_{i=1}^{m}(X - \lambda_{2i})^2(p_1 - p_2) \end{aligned}$$

mit

$$\begin{aligned} p_1 &:= \prod_{i=m+1}^{n} (X^2 - 2X\mathrm{Re}\lambda_{2i} + (\mathrm{Re}\lambda_{2i})^2 + (\mathrm{Im}\lambda_{2i})^2) \\ &= X^{2(n-m)} + X^{2(n-m)-1} \sum_{i=m+1}^{n} -2\mathrm{Re}\lambda_{2i} \\ &\qquad + \text{kleinere Potenzen von } X \\ p_2 &:= \prod_{i=m+1}^{n} (X^2 - 2X\mathrm{Re}\lambda_{2i} + (\mathrm{Re}\lambda_{2i})^2) \\ &= X^{2(n-m)} + X^{2(n-m)-1} \sum_{i=m+1}^{n} -2\mathrm{Re}\lambda_{2i} \\ &\qquad + \text{kleinere Potenzen von } X \end{aligned}$$

Also ist $p - (g_{2n}(p))^2 \in P_{2n-2}$. Außerdem gilt $p_1(x) \geq p_2(x)$ für alle $x \in \mathbb{R}$ und es folgt insgesamt $p - (g_{2n}(p))^2 \in P_{2n-2}^{+}$.

2. Aus (1) folgt $(g_{2n}(p)(x))^2 \leq p(x)$ für alle $x \in \mathbb{R}$, daher folgt die Behauptung aus Lemma 5.1.4.

Da nach Satz 1.3.4 auf Seite 9 die Nullstellen stetig von den Koeffizienten abhängen und Real- und Imaginärteil als Projektionen auch stetig sind, ist g_{2n} eine stetige Funktion. $\square$

Definition 5.1.7
Für $k = 0, \ldots, n$ seien folgende Funktionen definiert:

$$\begin{array}{rcccc} e_n^k & : & P_n & \longrightarrow & P_n \\ & & p & \longmapsto & X^n \cdot p(\frac{1}{X} + k) \end{array}$$

$$\begin{array}{rcccc} f_n^k & : & P_n & \longrightarrow & P_n \\ & & p & \longmapsto & (X-k)^n p(\frac{1}{X-k}) \end{array}$$

Lemma 5.1.8
Es gilt:

1. e_n^k *und* f_n^k *sind zueinander inverse Automorphismen des Vektorraums* P_n *(und da* $\dim P_n < \infty$ *also stetig).*
2. *Sind* $p, q \in P_n$*, so gilt* $f_{2n}^k(p \cdot q) = f_n^k(p) \cdot f_n^k(q)$.
3. $e_{2n}^k(P_{2n}^+), f_{2n}^k(P_{2n}^+) \subset P_{2n}^+$
4. *Zu jedem* $p \in P_{2n}^+ \setminus \{0\}$ *gibt es ein* $k \in \{0, \ldots, n\}$*, so daß* $e_{2n}^k(p) \in P_{2n}^{++}$ *gilt.*

Beweis:

1. Daß die beiden Funktionen e_n^k und f_n^k wohldefiniert und linear sind ist klar. Bleibt noch zu zeigen, daß sie zueinander invers sind:

$$\begin{aligned} f_n^k e_n^k(p)(X) &= f_n^k(X^n p(\frac{1}{X} + k)) \\ &= (X-k)^n (\frac{1}{X-k})^n p(X-k+k) \\ &= p(X) \\ e_n^k f_n^k(p)(X) &= e_n^k((X-k)^n p(\frac{1}{X-k})) \\ &= X^n(\frac{1}{X} + k - k)^n p(\frac{1}{\frac{1}{X} + k - k}) \\ &= p(X) \end{aligned}$$

2. Seien $p, q \in P_n$. Dann gilt:

$$\begin{aligned} f_{2n}^k(p \cdot q) &= (X-k)^{2n} p(\frac{1}{X-k}) q(\frac{1}{X-k}) \\ &= (X-k)^n p(\frac{1}{X-k})(X-k)^n q(\frac{1}{X-k}) \\ &= f_n^k(p) \cdot f_n^k(q) \end{aligned}$$

3. Seien $x \in \mathbb{R}$ und $p \in P_{2n}^+$. Dann gilt:

$$\begin{aligned} e_{2n}^k(p)(x) &= \left\{ \begin{array}{cc} x^{2n} p(\frac{1}{x}+k) & \text{für} \quad x \neq 0 \\ a_{2n} & \text{für} \quad x = 0 \end{array} \right\} \geq 0, \text{ da } p \in P_{2n}^+ \\ f_{2n}^k(p)(x) &= \left\{ \begin{array}{cc} (x-k)^{2n} p(\frac{1}{x-k}) & \text{für} \quad x \neq k \\ a_{2n} & \text{für} \quad x = k \end{array} \right\} \geq 0, \text{ da } p \in P_{2n}^+ \end{aligned}$$

4. Der $2n$-te Koeffizient von $e_{2n}^k(p)$ ist $p(k)$, denn:

$$X^{2n} \sum_{i=0}^{2n} a_i (\frac{1}{X}+k)^i = X^{2n} \underbrace{(a_0 + k a_1 + \cdots + k^{2n} a_{2n})}_{p(k)} + \text{niedrigere Potenzen von } X \tag{5.1}$$

Da ein Polynom, das auf ganz $\mathbb{R}$ nur nichtnegative Werte annimmt, nur doppelte reelle Nullstellen haben kann, kann $p \in P_{2n}^+$ also höchstens n verschiedene Nullstellen in $\mathbb{R}$ haben und unter den $n+1$ Zahlen $0, \ldots, n$ muß es also ein k geben mit $p(k) \neq 0$. Für dieses k gilt dann $e_{2n}^k(p) \in P_{2n}^{++}$.

□

Bemerkung 5.1.9 Für $q_j \in P_n$ gilt:

$$e_{2n}^k(p) = \sum_j q_j^2 \Longrightarrow p = \sum_j (f_n^k(q_j))^2 \tag{5.2}$$

Denn $p = f_{2n}^k e_{2n}^k(p) = f_{2n}^k(\sum_j q_j^2) = \sum_j f_{2n}^k q_j^2 = \sum_j (f_n^k(q_j))^2$.

Satz 5.1.10
Sei $A_0 = 1$ und $A_n = (n+1)(A_{n-1}+1)$. Dann gibt es zu jedem $n \in \mathbb{N}$ stetige definierbare Funktionen

$$f_j : P_{2n}^+ \longrightarrow P_n \quad (j = 0, \ldots, A_n)$$

so daß für alle $p \in P_{2n}^+$ gilt:

$$p = \sum_{j=0}^{A_n - 1} (f_j(p))^2$$

Beweis: Beweis durch Induktion über n:

Induktionsanfang: Sei $f_0(a_0) = \sqrt{a_0}$. Dann gilt $a_0 = (f_0(a_0))^2$.

Induktionsschritt: Die f_j werden zunächst auf $U_k := (e_{2n}^k)^{-1}(P_{2n}^{++})$ definiert: Sei $p \in P_{2n}^+ \setminus \{0\}$ und sei nach Lemma 5.1.8 ein $k \in \{0, \dots, n\}$ gewählt, so daß $e_{2n}^k(p) \in P_{2n}^{++}$ gilt. Dann ist $e_{2n}^k(p) - (g_{2n} e_{2n}^k(p))^2 \in P_{2n-2}^+$ und nach Induktionsvorraussetzung gibt es dann $f_j : P_{2n-2}^+ \longrightarrow P_{n-1}$ mit

$$e_{2n}^k(p) - (g_{2n} e_{2n}^k(p))^2 = \sum_{j=0}^{A_{n-1}-1} (f_j(e_{2n}^k(p) - (g_{2n} e_{2n}^k(p))^2))^2$$

Mit (5.2) folgt daher

$$p = \sum_{j=0}^{A_{n-1}-1} (\underbrace{f_n^k(f_j(e_{2n}^k(p) - (g_{2n} e_{2n}^k(p))^2))}_{=:F_j^k(p)})^2 + (\underbrace{f_n^k g_{2n} e_{2n}^k(p)}_{=:F_{A_{n-1}}^k(p)})^2$$

Die F_j^k werden nun so gewichtet, daß man sie auf $P_{2n}^+ \setminus U_k$ stetig durch Null fortsetzen kann. Dazu sei $h^k(p)$ der $2n$-te Koeffizient von $e_{2n}^k(p)$. Dann ist h^k die Verknüpfung von e_{2n}^k und der Projektion auf die $2n$-te Komponente und damit stetig. Ist $p \in P_{2n}^+$, so gilt immer $h^k(p) \geq 0$ und außerdem

$$h^k(p) > 0 \Longleftrightarrow e_{2n}^k(p) \in P_{2n}^{++}$$

Seien nun die neuen Funktionen, auf ganz P_{2n}^+ definiert durch:

$$g_j^k(p) = \begin{cases} \sqrt{\frac{h^k(p)}{h^0(p)+\cdots+h^n(p)}} F_j^k(p) & \text{für } h^k(p) > 0 \\ 0 & \text{für } h^k(p) = 0 \end{cases}$$

Wegen Lemma 5.1.8 ist

$$h^0(p) + \cdots + h^n(p) \neq 0 \text{ für } p \in P_{2n}^+ \setminus \{0\} \tag{5.3}$$

und durch Fallunterscheidung über $h^k(p) > 0$ und $h^k(p) = 0$ erhält man

$$\sum_{j=0}^{A_{n-1}} (g_j^k(p))^2 = \frac{h^k(p)}{h^0(p) + \cdots + h^n(p)} \cdot p$$

für alle $k = 0, \dots, n$. Für alle $p \in P_{2n}^+$ gilt also

$$\sum_{k=0}^{n} \sum_{j=0}^{A_{n-1}} (g_j^k(p))^2 = p$$

und die Anzahl der Summanden ist $(n+1)(A_{n-1}+1) = A_n$.

Nun bleibt noch zu zeigen, daß $g_j^k : P_{2n}^+ \longrightarrow P_n$ für alle j und k stetig ist.

Da $\sum_j (F_j^k(p)(x))^2 = p(x)$ ist, gilt $(F_j^k(p)(x))^2 \leq p(x)$ für alle $x \in \mathbb{R}$. Nach Lemma 5.1.4 bildet F_k^j also beschränkte Mengen auf beschränkte Mengen ab.

Liegt p in U_k oder im Innern von $P_{2n}^+ \setminus U_k$, so ist die Stetigkeit von g_j^k in p klar. Sei also p auf dem Rand von U_k, d.h. $g_j^k(p) = 0$.

1. Fall: $p \neq 0$.
   Sei $K = \{q \in P_{2n}^+; \|p - q\| \leq \frac{\|p\|}{2}\}$ und sei (p_i) ein Folge in K mit $p_i \to p$ für $i \to \infty$. Da für $p_i \notin U_k$ sowieso $g_j^k(p_i) = 0$ gilt, seien ohne Einschränkung alle $p_i \in U_k$. Die stetige Funktion $\sqrt{\sum h_i}$ nimmt auf dem Kompaktum K ihr Minimum an, dies sei M. Da $0 \notin K$ liegt, folgt $M \neq 0$ mit Ungleichung (5.3). Außerdem ist mit K auch $F_j^k(K)$ beschränkt (etwa durch μ). Damit gilt:

$$\begin{aligned} \|g_j^k(p_l)\| &= |\sqrt{\frac{h^k(p_l)}{\sum h^i(p_l)}}|\|F_j^k(p_l)\| \\ &\leq \sqrt{h^k(p_l)}\frac{\mu}{M} \\ &\to \sqrt{h^k(p)}\frac{\mu}{M} \end{aligned}$$

   für $i \to \infty$, da h^k stetig ist.

2. Fall: $p = 0$.
   Aus $p(x) = |p(x)| = \sum (g_j^i(p)(x))^2$ für $x \in \mathbb{R}$ folgt $|g_j^i(p)(x)| \leq \sqrt{p(x)} \to 0$ für $p \to 0$ und mit Lemma 5.1.5 folgt dann

$$g_j^k(p) \to 0 \quad \text{für} \quad p \to 0$$

   .

□

Index

Literaturverzeichnis

[1] ALEXANDROV, P. S. *Die Hilbertschen Probleme*, vol. 252 of *Ostwalds Klassiker der exakten Wissenschaften.* Akademische Verlagsgesellschaft Geest & Portig K.-G. Leipzig, 1971.

[2] ARTIN, E. über die Zerlegung definiter Funktionen in Quadrate. *Abhandlungen aus dem Mathematischen Seminar der Hamburgschen Universität 5* (1927), 100 – 115.

[3] BACKMEISTER, T. Stetige schwache Isotropie quadratischer Formen über $R(x_1, ..., x_n)$, R ein reell abgeschlossener Körper. Handschriftliches Manuskript.

[4] BECKER, E. Summen n-ter Potenzen in Körpern. *Journal für die reine und angewandte Mathematik 307/308* (1979), 8 – 30.

[5] BECKER, E., AND GONDARD, D. On rings admitting orderings and 2-primary chains of orderings of higher level. *manuscripta mathematica 65* (1989), 63 – 82.

[6] BECKER, E., AND SCHWARTZ, N. Zum Darstellungssatz von Kadison-Dubois. *Archiv der Mathematik 40* (1983), 421 – 428.

[7] BERR, R. The Intersection Theorem for Orderings of Higher Level. *Manuscripta Mathematica 75* (1992), 273 – 277.

[8] BOCHNAK, J., COSTE, M., AND ROY, M.-F. *Geometrie algebrique reelle*, vol. 3 of *A Series of Modern Surveys in Mathematics.* Springer-Verlag, 1987.

[9] COOLIDGE, J. L. The continuity of the roots of an algebraic equation. *Annales of Mathematics 9* (1908), 116–118.

[10] DELZELL, C. On the Pierce-Birkhoff conjecture over ordered fields. *Rocky Mountain Journal of Mathematics 19* (1989), 651–668.

[11] DELZELL, C. N. Case distinctions are necessary for representing polynomials as sums of squares. *Proceedings of the Herbrand Symposium, Logic Colloquium 107* (1981), 87 – 103.

[12] Delzell, C. N. A continous constractive solution to Hilbert's 17th problem. *Inventiones mathematicae 76* (1984), 365 – 384.

[13] Delzell, C. N. Continous, piecewise-polynomial functions which solve Hilbert's 17th problem. *Journal für die reine und angewandte Mathematik 440* (1993), 157 – 173.

[14] Dubois, D. W. A note on David Harrison's theory of preprimes. *Pacific Journal of Mathamatics 21*, 1 (1967), 15 – 19.

[15] Hardy, G. H., and Wright, E. M. *An introduction to the theory of numbers*, 4 ed. Oxford University Press, Oxford, 1960.

[16] Hilbert, D. Mathematische Probleme. *Archiv der Mathematik und Physik 3.1* (1901), 44 – 63, 213 – 237.

[17] Hilbert, D. *Grundlagen der Geometrie.* B. G. Teubner Stuttgart, 1968.

[18] Kadison, R. V. *A representation theory for commutative topological algebra.* No. 7 in Memoires of the American Mathematical Society. American Mathematical Society, 1951.

[19] Knebusch, M., and Kolster, M. *Wittrings*, vol. 2 of *Aspects of Mathematics.* Vieweg, 1982.

[20] Knebusch, M., and Scharlau, W. *Algebraic Theory of Quadratic Forms, Generic Methods and Pfister Forms*, vol. 1 of *DMV seminar.* Birkhäuser, Boston, 1980.

[21] Knebusch, M., and Scheiderer, C. *Einführung in die reelle Algebra.* Vieweg-Studium; 63: Aufbaukurs Mathematik. Vieweg, 1989.

[22] Lam, T. Y. *The algebraic theory of quadratic forms.* Mathamatic lecture note series. W. A. Benjamin, Inc., 1973.

[23] Lam, T. Y. *Orderings, valuations and quadratic forms.* No. 52 in Conference board of mathematical sciences, regional conference series in mathematics. American Mathamatical Society, 1981.

[24] Lorenz, F. *Quadratische Formen über Körpern.* Lecture Notes in Mathematics. Springer, 1980.

[25] Marshall, M., and Walter, L. Signatures of higher level on rings with many units. *Mathematische Zeitschrift 204* (1990), 129–143.

[26] Prestel, A. *Lectures on formally real fields.* Lecture Notes in Mathematics. Springer, 1984.

[27] Prestel, A. *Einführung in die Mathematische Logik und Modelltheorie*, 1 ed. Vieweg Studium Aufbaukurs Mathematik. Vieweg, 1986.

[28] Prestel, A. Modelltheorie angewandt auf Fragen über Polynome. Vorlesung, Universität von Santiago de Chile, 1989.

[29] Prestel, A. Continous representations of real polynomials as sums of 2^m-th powers. In *Tagungsberichte* (1990), Tagung vom 10.6. - 16.6.1990 über Reelle algebraische Geometrie, Mathematisches Forschungsinstitut Oberwolfach, p. 18.

[30] Prestel, A. Das 17. Hilbertsche Problem. Vorlesung, Universität Konstanz, 1996.

[31] Prestel, A., and Ziegler, M. Model theoretic methods in the theory of topological fields. *Journal für die reine und angewandte Mathematik 299/300* (1978), 318 – 341.

[32] Robinson, A. On ordered fields and definite forms. *Mathematische Annalen 130* (1955), 257 – 271.

[33] Witt, E. Theorie der quadratischen Formen in beliebigen Körpern. *Journal für die reine und angewandte Mathematik 176* (1937), 31 – 44.

[34] Ziegler, M. Stetige Quadratsummendarstellung positiv definiter $p \in \mathbb{R}[x]$. Handschriftliches Manuskript, Sept. 1988.