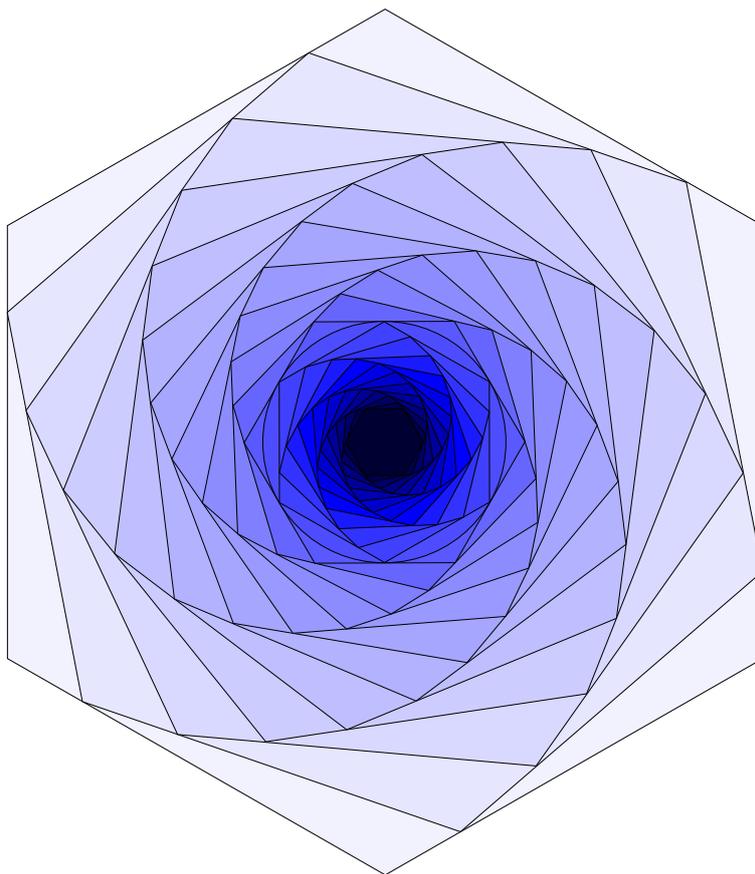




TECHNISCHE
UNIVERSITÄT
DARMSTADT

Approximation projektiver Tensornormen mit konvexer algebraischer Geometrie

*Approximation of Projective Tensor Norms
with Convex Algebraic Geometry*



Masterthesis von Sandra Lang

Technische Universität Darmstadt
Fachbereich Mathematik

Masterthesis

Name: Sandra Lang

Studiengang: Master Mathematik

Betreuer: Prof. Dr. Burkhard Kümmerer

Arbeitsgruppe: Operatoralgebren
und Quantenstochastik

Ausfertigung: 16. Februar 2015

Titelbild: Eine Kette von Polygonen
und ihre Polaren

Approximation projektiver Tensornormen mit konvexer algebraischer Geometrie

Masterarbeit von Sandra Lang

Betreuer: Prof. Dr. Burkhard Kümmerer

URN: [urn:nbn:de:tuda-tuprints-224970](https://nbn-resolving.org/urn:nbn:de:tuda-tuprints-224970)
<https://tuprints.ulb.tu-darmstadt.de/22497/>

Ausfertigung vom 16. Februar 2015

Veröffentlicht von tuprints im Jahr 2023

Published by tuprints in 2023

Dieses Dokument wird bereitgestellt von tuprints,
E-Publishing-Service der TU Darmstadt

This document is provided by tuprints,
e-publishing service of TU Darmstadt

<http://tuprints.ulb.tu-darmstadt.de>
tuprints@ulb.tu-darmstadt.de

Diese Veröffentlichung steht unter folgender Creative-Commons-Lizenz:
Namensnennung 4.0 International, CC BY 4.0
<https://creativecommons.org/licenses/by/4.0/deed.de>

This thesis is licensed under a Creative Commons License:
Attribution 4.0 International, CC BY 4.0
<https://creativecommons.org/licenses/by/4.0/>

Abstract

The aim of this thesis is to investigate a method to approximate the projective norm of multipartite tensor products by the concept of so-called theta bodies. These objects were proposed earlier in order to approximate the convex hull of a real algebraic variety by a chain of convex semialgebraic supersets. We first show that the unit product vectors of a multiple tensor product, whose convex hull equals the unit sphere of the projective norm, form a real algebraic variety. Afterwards, we show that the theta bodies associated to this variety converge to the unit sphere of the projective norm. We arrive at the conclusion that already the first theta body constitutes the unit sphere in case of bipartite tensor products. For the derivation of this result, we tried to give an in-depth introduction to the mathematical concepts, namely, Groebner bases, real algebraic geometry, convex geometry, and multipartite tensor products. In conclusion, we gain an advanced understanding of the set of the product vectors as a variety and obtain different representations of theta bodies as projected spectrahedra or as indicators for positivity. In order to deal with the general case of multipartite tensor products, we develop a software to approximate the projective norm by theta norms.

Vorwort

Der Zustand eines quantenmechanischen Vielteilchensystems wird durch das Tensorprodukt der zugehörigen Einteilchensysteme beschrieben. In diesem Bild entsprechen voneinander unabhängige Teilchen den Produktzuständen. Die konvexe Hülle der Produktzustände nennt man die separablen Zustände. Deren Komplement in der Zustandsmenge bilden die verschränkten Zustände. Sie besitzen im Vergleich zu den separablen Zuständen einige Eigenschaften, die charakteristisch für die Quantenmechanik und damit grundlegendend für die Quantenkryptographie, die Quantenteleportation oder die Quanteninformati­onstheorie sind. Auch quantenmechanische Algorithmen wie zum Beispiel der Shor-Algorithmus zur Primfaktorzerlegung basieren auf diesen Eigenschaften.

Ein Separabilitätskriterium für Zustände stellen projektive Tensornormen dar. Die projektive Norm eines Zustands ist genau dann eins, wenn der Zustand separabel ist. Projektive Normen sind weiterhin ein Verschränkungsmaß: Je verschränkter der Zustand, desto größer ist die projektive Norm.

Der klassische Rahmen, in den projektive Tensornormen eingebettet sind, ist die Theorie topologischer Tensorprodukte. Während zahlreiche formale Eigenschaften solcher Normen bekannt sind, ist es eine Herausforderung, die projektive Norm eines gegebenen Tensors konkret zu bestimmen. Für ein zweifaches Tensorprodukt ist dies zwar mit elementaren Methoden durch die sogenannte Schmidt-Zerlegung möglich, doch bereits für drei Tensorfaktoren ist ein Konzept dieser Art nicht mehr vorhanden.

In dieser Arbeit studieren wir einen alternativen Zugang, die projektive Norm mehrfacher Tensorprodukte von endlicher Dimension zu bestimmen.

Die projektive Norm einer Bestimmung zu unterziehen, reduziert sich auf die Untersuchung ihrer Einheitssphäre. Diese ist als konvexe Hülle der Einheitsproduktvektoren ein Schnitt von Halbräumen. Hier möchten wir nicht alle, sondern nur spezielle Halbräume zur Bestimmung heranziehen. Damit erhalten wir konvexe Obermengen, die bei sukzessiver Verfeinerung gegen die Einheitssphäre konvergieren. So ist es möglich, die projektive Norm im Mindesten einzugrenzen, ferner zu approximieren, und im besten Fall exakt zu bestimmen.

Die Menge der Produktvektoren bildet eine reelle algebraische Varietät. Die Einheitssphäre der projektiven Norm ist also die konvexe Hülle einer Varietät. Die reelle algebraische Geometrie liefert einen vielversprechenden Ansatz, solche konvexe Hüllen durch sogenannte Thetakörper zu approximieren.

Das Ziel dieser Arbeit ist es, die projektive Norm durch Thetakörper zu beschreiben. Im Fall zweifacher Tensorprodukte erhalten wir ein positives Resultat: Der erste Thetakörper bildet die Einheitssphäre der projektiven Norm. Es ist also möglich, Verschränkung von der Warte der reellen algebraischen Geometrie zu messen.

Das erste Kapitel führt in die Theorie der Gröbnerbasen ein. Diese erlauben es, für Koordinatenringe auf kanonische Weise Basen zu bestimmen. Von welcher Gestalt reelle Polynome sind, die auf einer gegebenen Menge einer Vorzeichenbedingung genügen, ermitteln wir im zweiten Kapitel. Darin beweisen wir reelle Positivstellen- und Nullstellensätze. Von speziellen konvexen Objekten wie Kegeln und Spektraedern handelt das dritte Kapitel. Das vierte Kapitel stellt Thetakörper und ihre verschiedenen Darstellungsmöglichkeiten vor. Im fünften Kapitel führen wir mehrfache Tensorprodukte ein und klassifizieren Einheitsproduktvektoren als reelle algebraische Varietät. Schließlich untersuchen wir die Möglichkeit, die Einheitssphäre projektiver Normen durch Thetakörper zu approximieren, im sechsten Kapitel. Kapitel sieben ist eine Dokumentation des Programms PINORM, welches wir zur numerischen Bestimmung der projektiven Norm nach der vorgestellten Methode entwickelt haben. Alle Kapitel außer den ersten drei, die eigenständig und voneinander unabhängig sind, bauen thematisch auf die vorangehenden auf.

Darüber hinaus ist diese Arbeit ein Streifzug durch die Welt der Positivität und der Dualität in ihrem funktionalanalytischen und in ihrem algebraischen Sinne.

An dieser Stelle möchte ich meinen Dank an alle aussprechen, die mich bei der Anfertigung dieser Thesis unterstützt haben. Zunächst danke ich Herrn Professor Kümmerer dafür, dass er mir dieses spannende und weitreichende mathematische Gebiet anvertraut hat. Besonders bedanken möchte ich mich für die großzügige Bereitstellung eines Arbeitsplatzes innerhalb der Arbeitsgruppe, die Mitnahme zur Studienexkursion nach Gersfeld und die Möglichkeit, in zahlreichen „C*-AG“-Treffen über mein Thema zu referieren. Florian Sokoli danke ich für die kompetente thematische Unterstützung, seine konstruktiven Vorschläge und die Einführung in die C*-AG. Für die gründliche Durchsicht der Rohschrift möchte ich mich herzlich bei Felix Voigt bedanken. Andreas Gärtner konnte mir bei vielen Fragen zum Textsatz praktisch behilflich sein. Der gesamten C*-AG sei für ihre konstruktive Rückmeldung zu meinen Vorträgen gedankt. Zu guter Letzt bedanke ich mich bei meiner Familie für ihr Dahinterstehen.

Allen Interessierten wünsche ich eine anregende Lektüre.

Darmstadt, den 16. Februar 2015

Sandra Lang

Inhaltsverzeichnis

1	Gröbnerbasen	1
1.1	Das Idealzugehörigkeitsproblem	2
1.2	Das Idealgleichheitsproblem	9
1.3	Eine Basis für den Koordinatenring	14
2	Reelle Algebraische Geometrie	21
2.1	Reell abgeschlossene Körper	23
2.2	Das Transferprinzip	36
2.3	Positivstellensätze und der reelle Nullstellensatz	45
2.4	Der Satz von Schmüdgen	53
3	Konvexe Geometrie	61
3.1	Polyeder, Spektraeder und Kegel	62
3.2	Duale Kegel und das relative Innere	69
4	Thetakörper	79
4.1	Thetakörper als Kette konvexer Mengen	81
4.2	Thetakörper als projizierte duale Kegel	84
4.3	Thetakörper als projizierte Spektraeder	89
4.4	Thetakörper als Maß für Positivität	92
5	Mehrfache Tensorprodukte	101
5.1	Konstruktion mehrfacher Tensorprodukte	102
5.2	Normen auf Tensorprodukten	106
5.3	Produktvektoren als Varietät	112
6	Approximation der Pi-Norm-Einheitssphäre	123
6.1	Thetakörper induzieren Normen	123
6.2	Polaren und ihre maximalen Seiten	131
6.3	Der erste Thetakörper	146

7 Numerische Simulation	159
7.1 Thetakörper als Lösungen semidefiniter Programme	160
7.2 „Pinorm“ - Ein Programm zur Berechnung von Thetanormen . . .	164
8 Fazit und Ausblick	173
Literaturverzeichnis	176
Notationsverzeichnis	178
Stichwortverzeichnis	185

1 Gröbnerbasen

Wann ist ein Polynom Element eines gegebenen Ideals?

Falls ein Polynom bereits als Polynomkombination von Erzeugern des Ideals geschrieben werden kann, ist die Frage leicht zu bejahen. Dies ist jedoch ein Spezialfall, der im Allgemeinen nicht gegeben ist. Trotzdem kann eine Antwort gefunden werden. Ähnlich verhält es sich mit der Frage:

Wann sind zwei Ideale gleich?

Dieses Kapitel soll der Lösung der beiden Probleme dienen.

Im ersten Abschnitt werden *Gröbnerbasen* als Erzeugendensysteme von Idealen vorgestellt. Eine Gröbnerbasis liefert einen eindeutigen Rest, die *Normalform*, bei Division eines Polynoms durch die Elemente dieses Systems. Dieser Rest verschwindet genau dann, wenn das Polynom bereits im Ideal liegt.

Um die Konstruktion von Gröbnerbasen geht es im zweiten Abschnitt. Hier zeigen wir, dass reduzierte Gröbnerbasen eindeutig sind und sich damit die Frage nach der Gleichheit zweier Ideale beantworten lässt.

Im letzten Abschnitt soll dieses Ergebnis zur Anwendung kommen. Betrachten wir den *Koordinatenring* $\mathbb{R}[X_1, \dots, X_n]/I$ für ein Ideal $I \subseteq \mathbb{R}[X_1, \dots, X_n]$ als \mathbb{R} -Vektorraum, so stellt sich die Frage nach einer Basis. Diese ist durch Normalformen gegeben.

Bei der Behandlung von *Thetakörpern* in Kapitel 4 wird in Abschnitt 4.3 von der hier vorgestellten Theorie Gebrauch gemacht. Da wir auch eine Implementierung der Spektraedarstellung eines Thetakörpers in MATLAB vorstellen, werden wir am Ende des zweiten Abschnitts auf Möglichkeiten eingehen, eine Gröbnerbasis schnell und effizient mit Hilfe von Computeralgebrasystemen zu berechnen.

In diesem Kapitel wird darauf verzichtet, alle Beweise vollständig durchzuführen. Die zentralen Aussagen der ersten beiden Abschnitte sind der Publikation *Ideals*,

Varieties, and Algorithms von Cox, Little und O’Shea, siehe [CLS], entnommen. Sie sind in Kapitel 2, *Groebner Bases*, aufgeführt. Bei Bedarf können fehlende Beweisteile dort nachgeschlagen werden. Die Publikation [BPT] liefert die Motivation für den dritten Abschnitt.

Mit K sei ein Körper bezeichnet.

1.1 Das Idealzugehörigkeitsproblem

Es werden Tupel $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ mit Monomen $X_1^{\alpha_1} \cdot \dots \cdot X_n^{\alpha_n} \in K[X_1, \dots, X_n]$ identifiziert.

Monomordnungen, Multigrad und Litterme

Definition 1.1.1 - Monomordnung

Eine Ordnungsrelation \geq auf \mathbb{N}_0^n heißt *Monomordnung*, falls sie die folgenden Eigenschaften erfüllt:

- (i) Die Ordnung \geq ist total,
- (ii) Für $c \in \mathbb{N}_0^n$ und $a \geq b$ gilt: $(a + c) \geq (b + c)$,
- (iii) Jede nichtleere Teilmenge von \mathbb{N}_0^n besitzt ein kleinstes Element, das heißt, die Relation ist eine Wohlordnung. □

Die letzte Bedingung ist äquivalent dazu, dass jede strikt abfallende Folge

$$a_1 > a_2 > a_3 > \dots$$

von Elementen $(a_i)_{i \in \mathbb{N}} \subseteq \mathbb{N}_0^n$ terminiert.

Im folgenden Beispiel stellen wir mehrere Monomordnungen vor.

Beispiel 1.1.2

- (1) Die *lexikographische Ordnung* \geq_{lex} ist eine Wohlordnung: Für $a, b \in \mathbb{N}_0^n$ mit $a \neq b$ gelte genau dann $a \geq_{lex} b$, falls der erste Eintrag in der Differenz $a - b$, der nicht Null ist, positiv ist. Auf $K[X_1, \dots, X_n]$ ist eine lexikographische Ordnung durch eine Anordnung der Variablen X_1, \dots, X_n gegeben. Es existieren also genau $n!$ lexikographische Ordnungen

auf $K[X_1, \dots, X_n]$. Beispielsweise gelten im Polynomring $K[x, y, z]$ die folgenden Ungleichungen:

$$\begin{aligned} x^2yz &>_{lex} x^2z, \\ x &>_{lex} y^7z^9, \\ y^5 &>_{lex} y^4z^2, \end{aligned}$$

wobei $x > y > z$ sei.

(2) Mit

$$\begin{aligned} \mathcal{F}(\mathbb{N}) &:= \{(a_i)_{i \in \mathbb{N}} \mid a_i = 0 \text{ für fast alle } i \in \mathbb{N}\} \\ &\subseteq \{(a_i)_{i \in \mathbb{N}} \mid a_i \in \mathbb{N}_0 \text{ für alle } i \in \mathbb{N}\} \end{aligned}$$

sei der Raum der endlichen Folgen mit Einträgen aus den natürlichen Zahlen und der Null bezeichnet. Wir betrachten eine Verallgemeinerung der lexikographischen Ordnung durch Definition einer Ordnungsrelation auf ähnliche Weise wie in (1): Sind $a, b \in \mathcal{F}(\mathbb{N})$ verschieden, dann sei $a \geq b$ genau dann, wenn der letzte Eintrag in $a - b$, der nicht Null ist, positiv ist. Diese Ordnung spielt eine Rolle im Beweis von Proposition 2.2.5 auf Seite 41.

(3) Die vorherigen Beispiele haben gezeigt, dass die lexikographische Ordnung keine Rücksicht auf die Summe der Einträge $\alpha_1 + \dots + \alpha_n$ für Tupel $(\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n$ nimmt. Alternativ sei die *graduierte lexikographische Ordnung* \geq_{grlex} definiert: Für $a, b \in \mathbb{N}_0^n$ sei $a \geq_{grlex} b$ genau dann, wenn entweder die Summe der Einträge von a echt größer ist als die von b oder, wenn beide Summen gleich sind, $a \geq_{lex} b$ erfüllt ist. Beispielsweise gelten die Ungleichungen

$$\begin{aligned} x^2yz &>_{grlex} x^2z, \\ x &<_{grlex} y^7z^9, \\ y^5 &<_{grlex} y^4z^2, \\ y^4 &>_{grlex} y^3z \end{aligned}$$

im Polynomring $(K[x, y, z], \geq_{grlex})$.

□

Wenn wir von „der“ lexikographischen Ordnung sprechen, verstehen wir darunter die, die Monome X_1, \dots, X_n absteigend nach ihrem Index anordnet. In $K[x, y, z]$ sei $x > y > z$. Das gleiche gilt für die gradierte lexikographische Ordnung.

Definition 1.1.3 - Grad und Leitterm

Ein Polynom $f := \sum_{\alpha \in \mathbb{N}_0^n} a_\alpha X^\alpha \in K[X_1, \dots, X_n] \setminus \{0\}$ sei gegeben. Auf \mathbb{N}_0^n sei eine Monomordnung festgelegt.

(i) Der *Multigrad* von f sei

$$\text{multideg}(f) := \max(\alpha \in \mathbb{N}_0^n \mid a_\alpha \neq 0).$$

(ii) Der *Grad* von f sei

$$\text{deg}(f) := \max\left(\sum_{i=1}^n \alpha_i \mid \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n, a_\alpha \neq 0\right).$$

(iii) Das *Leitmonom* von f sei $\text{LM}(f) := X^{\text{multideg}(f)}$.

(iv) Der *Leitkoeffizient* von f sei $\text{LC}(f) := a_{\text{multideg}(f)} \in K$.

(v) Der *Leitterm* von f sei $\text{LT}(f) := \text{LC}(f) \cdot \text{LM}(f)$.

Das Polynom f heißt *affin-linear*, falls $\text{deg}(f) \leq 1$ beziehungsweise falls f von der Gestalt $f = a_0 + a_1 X_1 + a_2 X_2 + \dots + a_n X_n$ mit $a_i \in K$, $i = 0, \dots, n$, ist. \square

Bemerkung 1.1.4 Es ist leicht einzusehen, dass für $f, g \in K[X_1, \dots, X_n]$ gilt:

$$\text{multideg}(f + g) \leq \max(\text{multideg}(f), \text{multideg}(g)),$$

$$\text{deg}(f + g) \leq \max(\text{deg}(f), \text{deg}(g)),$$

$$\text{deg}(f \cdot g) = \text{deg}(f) + \text{deg}(g). \quad \square$$

Beispiel 1.1.5

(1) Seien $f, g \in (\mathbb{R}[x, y, z], \geq_{lex})$ mit

$$f := 5x^2y - xy^4z + 3z^2 \quad \text{und}$$

$$g := 1 + 3x - 7y + 9z + y^2z^3 + z^4,$$

dann gilt:

$$\text{multideg}(f) = (2, 1, 0),$$

$$\text{multideg}(g) = (1, 0, 0),$$

$$\text{deg}(f) = 6,$$

$$\text{deg}(g) = 5,$$

$$\text{LT}(f) = 5x^2y,$$

$$\text{LT}(g) = 3x.$$

Es ist auffällig, dass der Grad $\text{deg}(g)$ anzeigt, dass g nicht affin-linear ist. Der Multigrad liefert jedoch keinen Hinweis dafür.

(2) Betrachten wir ein Polynom $f \in (K[X_1, \dots, X_n], \geq_{grlex})$, dann gilt:

$$\text{deg}(f) = \sum_{i=1}^n \alpha_i$$

für $(\alpha_1, \dots, \alpha_n) = \text{multideg}(f)$. \square

Ein Divisionsalgorithmus für Polynome in mehreren Variablen

Notation. Einführend stellen wir eine Notation für Teilbarkeit von Leitertermen vor: Für $g, h \in K[X_1, \dots, X_n]$ mit $g \neq 0$ gelte

$$\text{LT}(g) \mid \text{LT}(h)$$

genau dann wenn ein Monom $p \in K[X_1, \dots, X_n]$ und ein Faktor $k \in K$ existieren mit

$$k \cdot p \cdot \text{LT}(g) = \text{LT}(h).$$

Wir bezeichnen h dann als durch g teilbar.

Satz 1.1.6 - Divisionsalgorithmus

Auf \mathbb{N}_0^n sei eine Monomordnung \geq festgelegt. Weiterhin sei ein s -Tupel $(f_1, \dots, f_s) \in (K[X_1, \dots, X_n] \setminus \{0\})^s$ gegeben. Dann kann $f \in K[X_1, \dots, X_n]$ geschrieben werden als

$$f = a_1 f_1 + \dots + a_s f_s + r,$$

wobei $a_i \in K[X_1, \dots, X_n]$ ein Polynom ist mit

$$\text{multideg}(f) \geq \text{multideg}(a_i f_i)$$

für $i = 1, \dots, s$ und $r = 0$ oder $r \in K[X_1, \dots, X_n] \setminus \{0\}$, wobei dann r eine Linearkombination von Monomen, die jeweils durch keines der Polynome in F teilbar sind, ist. Das Polynom r bezeichnen wir als einen *Rest* der Division von f durch F . \square

Beweisidee. Zunächst stellen wir das Prinzip der Polynomdivision dar.

Dazu seien $g, g', h, h' \in K[X_1, \dots, X_n]$ Polynome mit $\text{multideg}(gg') > \text{multideg}(h)$ und $\text{multideg}(g) > \text{multideg}(h')$. Dann gilt $\text{LT}(g + h') \mid \text{LT}(gg' + h)$ und wir können das Polynom $gg' + h$ durch das Polynom $g + h'$ „teilen“:

$$\begin{aligned} f &:= gg' + h = g'(g + h') + (h - g'h') \quad \text{mit:} \\ \text{multideg}(f) &> \text{multideg}(h - g'h') \quad \text{und} \\ \text{multideg}(f) &= \text{multideg}(g'(g + h')). \end{aligned}$$

Falls $h - g'h'$ durch g teilbar und nicht Null ist, ist es möglich, eine weitere Division von $h - g'h'$ durch $g + h'$ durchzuführen.

Im Folgenden sei ein Algorithmus zur Konstruktion der Divisoren und des Restes angegeben. In der ersten Schleife wird die Variable p mit dem aktuellen Restpolynom belegt. Die zweite Schleife steht für die Division des Restpolynoms p durch

```

Polynome des Systems  $(f_1, \dots, f_s)$ .
IN:  $f, f_1, \dots, f_s$ 
OUT:  $a_1, \dots, a_s, r$ 
 $a_1 := 0; \dots; a_s := 0; r := 0; p := f;$ 
WHILE  $p \neq 0$ 
   $i := 1;$ 
   $d := \text{FALSE};$ 
  WHILE  $i \leq s$  AND  $d = \text{FALSE}$ 
    IF  $\text{LT}(f_i) \mid \text{LT}(p)$ 
       $a_i := a_i + \text{LT}(p) / \text{LT}(f_i);$ 
       $p := p - (\text{LT}(p) / \text{LT}(f_i)) \cdot f_i;$ 
       $d := \text{TRUE};$ 
    ELSE
       $i := i + 1;$ 
    END
  END
  IF  $d = \text{FALSE}$ 
     $r := r + \text{LT}(p);$ 
     $p := p - \text{LT}(p);$ 
  END
END

```

END

Es bleibt zu zeigen, dass der Algorithmus terminiert. Dabei spielt die Bedingung (iii) aus Definition 1.1.1 eine zentrale Rolle. ■

Eine solche Darstellung von f ist sowohl von der Reihenfolge der Divisoren als auch von der gewählten Monomordnung abhängig.

Beispiel 1.1.7 Der Rest ist nicht eindeutig!

Die Division von $x^2y + xy^2 + y^2$ durch die Divisoren $(xy - 1, y^2 - 1)$ ergibt einen anderen Rest als die Division durch $(y^2 - 1, xy - 1)$:

$$\begin{aligned} x^2y + xy^2 + y^2 &= (x + y) \cdot (xy - 1) + 1 \cdot (y^2 - 1) + (x + y + 1) \\ &= (x + 1) \cdot (y^2 - 1) + x \cdot (xy - 1) + (2x + 1) \end{aligned}$$

Ein weiteres Beispiel:

$$\begin{aligned} xy^2 - x &= y \cdot (xy + 1) + 0 \cdot (y^2 - 1) + (-x - y) \\ &= x \cdot (y^2 - 1) + 0 \cdot (xy + 1) + 0 \end{aligned}$$

Ein verschwindender Rest ist also hinreichend dafür, dass ein Polynom im aufgespannten Ideal der Divisoren enthalten ist, aber keine notwendige Bedingung. □

Es ist möglich, Erzeugendensysteme für Ideale zu finden, für die eine Division durch das System unabhängig von der Reihenfolge ist. Davon handelt der nächste Unterabschnitt.

Gröbnerbasen, Normalformen und Idealzugehörigkeit

Existiert für ein Ideal in $K[X_1, \dots, X_n]$ ein Erzeugendensystem aus Monomen, so liegt ein Monom in $K[X_1, \dots, X_n]$ genau dann in diesem Ideal, wenn es durch ein Monom des Erzeugendensystems teilbar ist. In solchen Fällen ist die Idealzugehörigkeit leicht nachzuweisen. Im allgemeinen Fall kommen wir auf diese Idee zurück, indem wir Erzeugendensysteme für Leitmonome betrachten:

Definition 1.1.8 - Gröbnerbasis

Sei $I \subseteq K[X_1, \dots, X_n]$, $I \neq \{0\}$, ein Ideal. Eine Teilmenge $G := \{g_1, \dots, g_k\} \subseteq I \setminus \{0\}$ heißt *Gröbnerbasis*, falls gilt:

$$\langle \text{LT}(I) \rangle = \langle \text{LT}(g_1), \dots, \text{LT}(g_k) \rangle. \quad \square$$

Mit der Notation von eben ist G genau dann eine Gröbnerbasis, falls für alle $f \in I$ ein $i \in \{1, \dots, k\}$ existiert, sodass $\text{LT}(g_i) \mid \text{LT}(f)$.

Bemerkung 1.1.9 Wir beachten, dass eine Gröbnerbasis die Null nicht enthält. Insbesondere besitzt das Ideal $\{0\}$ keine Gröbnerbasis. \square

Proposition 1.1.10 - Jedes Ideal $I \subseteq K[X_1, \dots, X_n]$, $I \neq \{0\}$, besitzt eine Gröbnerbasis. Eine Gröbnerbasis von I ist ein Erzeugendensystem von I . \square

Beweisidee. Für den Beweis benötigen wir *Dicksons Lemma*, siehe [CLS]:

„Ist ein Ideal in $K[X_1, \dots, X_n]$ von Monomen erzeugt,
existiert ein Erzeugendensystem aus endlich vielen Monomen“.

Es existiert also eine Teilmenge $G := \{g_1, \dots, g_k\} \subseteq I$, sodass $\langle \text{LT}(I) \rangle = \langle \text{LT}(G) \rangle$ gilt. Dies zeigt die Existenz einer Gröbnerbasis.

Sei $f \in I \setminus \{0\}$, dann ergibt eine Division von f durch die Gröbnerbasis (g_1, \dots, g_k) eine Darstellung $f = \sum_{i=1}^k a_i g_i + r$ mit Polynomen $a_1, \dots, a_k, r \in K[X_1, \dots, X_n]$, die die Bedingungen aus Satz 1.1.6 erfüllen. Umstellen der Gleichung nach r ergibt, dass $r \in I$ ist. Also ist r durch ein Polynom aus G teilbar, was aber nur möglich ist, wenn $r = 0$ gilt. \blacksquare

Proposition 1.1.11 - Eindeutigkeit des Restes

Sei $I \subseteq K[X_1, \dots, X_n]$ ein Ideal, G eine Gröbnerbasis für I und $f \in K[X_1, \dots, X_n]$. Dann ist der Rest bei Division von f durch G eindeutig, also nicht von der Reihenfolge der Divisoren abhängig. \square

Beweis. Es seien zwei Darstellungen $f = g + r = g' + r'$ gegeben mit $g, g' \in I$ und Resten r, r' . Dann ist $r - r' = g' - g \in I$. Falls $r \neq r'$, ist $r - r'$ teilbar durch ein Element aus G . Allerdings ist keines der Monome von r und r' durch irgendeinen Leitterm $\text{LT}(g_i)$ für $i \in \{1, \dots, k\}$ teilbar. Dies führt zu einem Widerspruch. Also ist $r = r'$. \blacksquare

Definition 1.1.12 - Normalform

Sei $I \subseteq K[X_1, \dots, X_n]$ ein Ideal und $f \in K[X_1, \dots, X_n]$. Wir bezeichnen den Rest r von $f \in K[X_1, \dots, X_n]$ bei Division durch eine Gröbnerbasis G von I als $\bar{f}^G := r$, beziehungsweise als *Normalform* von f . \square

Jetzt ist das Idealzugehörigkeitsproblem gelöst:

Korollar 1.1.13 - Idealzugehörigkeit

Sei $I \subseteq K[X_1, \dots, X_n]$ ein Ideal, G eine Gröbnerbasis für I und $f \in K[X_1, \dots, X_n]$. Dann sind äquivalent:

- (a) Für die Normalform von f gilt: $\bar{f}^G = 0$.
- (b) Es gilt: $f \in I$.

Insbesondere ist ein verschwindender Rest von der gewählten Gröbnerbasis unabhängig. \square

Beweis. Die Implikation (a) \Rightarrow (b) ist klar.

Die andere Implikation sehen wir so: Der Rest \bar{f}^G ist in keinem Monom teilbar durch ein Element von G , aber Element von I , also gilt: $\bar{f}^G = 0$. \blacksquare

1.2 Das Idealgleichheitsproblem

Auf $K[X_1, \dots, X_n]$ sei eine Monomordnung festgelegt.

Zur Konstruktion von Gröbnerbasen

Die Existenz einer Gröbnerbasis für ein gegebenes Ideal wurde im vorherigen Abschnitt gezeigt. Darüber hinaus ist es möglich, eine Gröbnerbasis zu konstruieren. Dazu stellen wir Vorüberlegungen an.

Zunächst ist es möglich, die Erzeuger des Ideals als Prototyp der Gröbnerbasis aufzustellen. Im Allgemeinen wird dies jedoch noch nicht ausreichend sein. Dies ist dann der Fall, wenn die Erzeuger so polynomial kombiniert werden können, dass die Leiterterme verschwinden. Dann ergeben sich neue Leiterterme, die auch in der Gröbnerbasis berücksichtigt werden müssen. Solche Elemente des Ideals werden wir im Folgenden untersuchen:

Definition 1.2.1 - Kleinste gemeinsame Vielfache und S-Polynome

Seien $f, g \in K[X_1, \dots, X_n]$, $\alpha := \text{multideg}(f)$ und $\beta := \text{multideg}(g)$. Es sei $\gamma \in \mathbb{N}_0^n$ mit $\gamma_i := \max(\alpha_i, \beta_i)$. Dann bezeichnet

$$\text{LCM}(\text{LM}(f), \text{LM}(g)) := X^\gamma$$

das *kleinste gemeinsame Vielfache* von $\text{LM}(f)$ und $\text{LM}(g)$.

Weiterhin bezeichne

$$S(f, g) := \frac{X^\gamma}{\text{LT}(f)} \cdot f - \frac{X^\gamma}{\text{LT}(g)} \cdot g$$

das *S-Polynom* von f und g . □

Jetzt kommen wir zu einem Kriterium, wann ein gegebenes System von Polynomen eine Gröbnerbasis ist:

Satz 1.2.2 - Das Kriterium von Buchberger

Sei $I \subseteq K[X_1, \dots, X_n]$, $I \neq \{0\}$, ein Ideal und $G := \{g_1, \dots, g_k\} \subseteq I \setminus \{0\}$ ein Erzeugendensystem von I . Dann sind die folgenden Aussagen äquivalent:

- (a) G ist eine Gröbnerbasis.
- (b) Für alle $i, j \in \{1, \dots, k\}$, $i \neq j$, gilt: $\overline{S(g_i, g_j)}^G = 0$. □

Beweisidee. Die Implikation $(a) \Rightarrow (b)$ ergibt sich aus Korollar 1.1.13.

$(b) \Rightarrow (a)$: Sei $f \in I \setminus \{0\}$. Zu zeigen ist, dass $\text{LT}(f) \in \langle \text{LT}(G) \rangle$ gilt. Wir wählen eine Darstellung $f = \sum_{i=1}^k a_i g_i$ für Polynome $a_1, \dots, a_k \in K[X_1, \dots, X_n]$ und

$$\text{multideg}(f) \leq \max(\text{multideg}(a_i g_i) \mid i = 1, \dots, k) =: \delta,$$

sodass δ minimal ist. Es ist möglich, zu zeigen, dass $\text{multideg}(f) = \delta$ gilt. In diesem Fall ist $\text{LT}(f)$ durch einen Leitterm $\text{LT}(g_i)$, $i \in \{1, \dots, k\}$, teilbar und die Aussage ist bewiesen. Die Details dieses Schrittes werden hier ausgespart. ■

Es ist möglich, eine Gröbnerbasis zu konstruieren, indem sukzessive Reste von S-Polynomen bei Division durch bereits ermittelte Elemente der Gröbnerbasis hinzugefügt werden.

Satz 1.2.3 - Der Algorithmus von Buchberger

Sei $I = \langle f_1, \dots, f_s \rangle \subseteq K[X_1, \dots, X_n]$ ein Ideal und $G := \{g_1, \dots, g_k\} \subseteq I$ durch den angegebenen Algorithmus ermittelt. Dann ist G eine Gröbnerbasis für I .

IN: $F := (f_1, \dots, f_s)$

OUT: $G = (g_1, \dots, g_k)$

$G := F$;

$i := 1$;

WHILE $i \neq 0$

$i = 0$;

$G' = G$;

FOR jedes Paar $p, q \in G'$, $p \neq q$

$S := \overline{S(p, q)}^{G'}$;

IF $S \neq 0$

$G := G \cup \{S\}$;

$i := i + 1$;

END

END

END

□

Beweis. Falls der Algorithmus terminiert, ist die Aussage wegen des Kriteriums von Buchberger Satz 1.2.2 wahr. Zu zeigen bleibt also noch, dass der Algorithmus terminiert.

Seien G und G' nach einer endlichen Anzahl von Durchgängen des Algorithmus

ermittelt und $G' \subsetneq G$. Dann gibt es Polynome $p, q \in G'$, $p \neq q$, sodass $\overline{S(p, q)}^{G'}$ nicht Null ist. Wegen der Eigenschaften der Normalform gilt weiterhin:

$$\begin{aligned} \text{LT}\left(\overline{S(p, q)}^{G'}\right) &\notin \langle \text{LT}(G') \rangle, \text{ aber} \\ \text{LT}\left(\overline{S(p, q)}^{G'}\right) &\in \langle \text{LT}(G) \rangle. \end{aligned}$$

Es folgt: $\langle \text{LT}(G') \rangle \subsetneq \langle \text{LT}(G) \rangle$.

Die Ideale $\langle \text{LT}(G') \rangle$, die sukzessive mit jedem Durchgang des Algorithmus gebildet werden, bilden eine aufsteigende Kette. Diese muss stationär werden. Es gilt also nach endlich vielen Schritten: $\langle \text{LT}(G') \rangle = \langle \text{LT}(G) \rangle$. Nach den eben angestellten Überlegungen gilt dann $G = G'$. ■

Es gibt Möglichkeiten, den Algorithmus effizienter zu gestalten. Zum Beispiel muss das S-Polynom zweier Polynome nicht noch einmal ermittelt werden, wenn die Basis um dem Rest der Division des S-Polynoms bereits vergrößert wurde. Desweiteren sind auf diese Weise ermittelte Gröbnerbasen im Allgemeinen sehr groß. Eine Möglichkeit, die Größe der Basis wieder zu reduzieren, stellen wir im nächsten Unterabschnitt vor.

Wann sind zwei Ideale gleich?

Definition 1.2.4 - Reduzierte Gröbnerbasis

Sei $I \subseteq K[X_1, \dots, X_n]$ ein Ideal. Eine Gröbnerbasis G für I heißt *reduziert*, falls für alle $p \in G$ gilt:

- (i) $\text{LC}(p) = 1$,
- (ii) Kein Monom von p liegt in der Menge $\text{LT}(G \setminus \{p\})$. □

Proposition 1.2.5 - Ein Ideal $I \subseteq K[X_1, \dots, X_n]$, $I \neq \{0\}$, besitzt eine eindeutige reduzierte Gröbnerbasis. □

Beweis. Die Bedingung (i) ist leicht durch Normierung der Leitkoeffizienten zu erfüllen. Sie sei im Folgenden bereits erfüllt.

Behauptung 1: Sei G eine Gröbnerbasis für I und $p \in G$ mit $\text{LT}(p) \in \langle \text{LT}(G \setminus \{p\}) \rangle$. Dann ist $G \setminus \{p\}$ ebenfalls eine Gröbnerbasis für I .

Beweis: Es gilt:

$$\langle \text{LT}(I) \rangle = \langle \text{LT}(G) \rangle = \langle \text{LT}(G \setminus \{p\}) \rangle,$$

also folgt die Behauptung bereits aus Definition 1.1.8. \diamond

Behauptung 2: Es existiert eine Gröbnerbasis G_0 für I , sodass für alle $p \in G_0$ gilt, dass $\text{LT}(p) \notin \langle \text{LT}(G_0 \setminus \{p\}) \rangle$.

Beweis: Die Existenz einer Gröbnerbasis G folgt aus Satz 1.2.3.

Ist $\text{LT}(p) \in \langle \text{LT}(G \setminus \{p\}) \rangle$ für ein $p \in G$ erfüllt, ist nach der vorherigen Behauptung die Menge $G' := G \setminus \{p\}$ wieder eine Gröbnerbasis für I . Existiert ein weiteres Element $p' \in G'$ mit $\text{LT}(p') \in \langle \text{LT}(G' \setminus \{p'\}) \rangle$, ist $G'' := G' \setminus \{p'\}$ wieder eine Gröbnerbasis. So verfahren wir weiter. Da G nur endlich viele Elemente enthält, erhalten wir eine Gröbnerbasis G_0 , die die Forderung erfüllt. \diamond

Behauptung 3: Es existiert eine reduzierte Gröbnerbasis für I .

Beweis: Eine Gröbnerbasis G erfülle die Bedingung aus der vorherigen Behauptung. Sei $p \in G$ und $p' := \overline{p}^{G \setminus \{p\}}$. Der Fall $p' = 0$ ist nach Voraussetzung ausgeschlossen. Wir setzen: $G' := (G \setminus \{p\}) \cup \{p'\}$. Wenn wir p durch $G \setminus \{p\}$ teilen, ist nach Voraussetzung der Leitterm von p durch keinen Leitterm $\text{LT}(g)$, $g \in G \setminus \{p\}$, teilbar. Daher sind die Leitterme von p und p' gleich. Es folgt:

$$\langle \text{LT}(G) \rangle = \langle \text{LT}(G') \rangle.$$

Da $G' \subseteq I \setminus \{0\}$, ist G' auch eine Gröbnerbasis für I und p' reduziert in G' . Dieser Schritt wird wiederholt. Ist ein Element bereits reduziert, bleibt es reduziert. Dies liegt daran, dass die Leitterme erhalten bleiben. \diamond

Behauptung 4: Erfüllen Gröbnerbasen G , G' die Bedingung aus Behauptung 2, gilt: $\text{LT}(G) = \text{LT}(G')$.

Beweis: Angenommen, es gibt ein Element $p \in G$ mit $\text{LT}(p) \notin \text{LT}(G')$. Es ist

$$\text{LT}(p) \in \langle \text{LT}(G) \rangle = \langle \text{LT}(G') \rangle,$$

also existiert ein $p' \in G'$, sodass gilt: $\text{LT}(p') \mid \text{LT}(p)$. Der Fall $\text{LM}(p) = \text{LM}(p')$ führt zu einem Widerspruch. Der Fall $\text{LM}(p) \neq \text{LM}(p')$ ist allerdings auch ausgeschlossen, wie wir im Folgenden zeigen wollen: Es ist $\text{LT}(p') \in \langle \text{LT}(G) \rangle$. Also existiert ein $g \in G \setminus \{p\}$, sodass $\text{LT}(p')$ und damit auch $\text{LT}(p)$ durch $\text{LT}(g)$ teilbar ist. Dies ist jedoch ausgeschlossen. \diamond

Behauptung 5: Eine reduzierte Gröbnerbasis ist eindeutig.

Beweis: Sind G und G' zwei reduzierte Gröbnerbasen, gilt $\text{LT}(G) = \text{LT}(G')$ nach Behauptung 4. Für $p \in G$ existiert also ein $p' \in G'$ mit $\text{LT}(p) = \text{LT}(p')$. Es gilt die Gleichung $0 = \overline{p - p'}^G$, da $p, p' \in I$. Bildung der Differenz $p - p'$ tilgt den Leitterm von p . Die Differenz besteht also nur noch aus Monomen, welche durch keinen der Leitterme $\text{LT}(G) = \text{LT}(G')$ teilbar sind. Also gilt: $0 = \overline{p - p'}^G = p - p'$. Daraus folgt: $p = p'$. \diamond

Damit sind Existenz und Eindeutigkeit der reduzierten Gröbnerbasis bewiesen. \blacksquare

Wann sind zwei gegebene Ideale gleich? Diese Frage ist im Allgemeinen nicht durch die Angabe zweier Erzeugendensysteme gelöst. Das vorige Resultat liefert jedoch eine Antwort auf diese Frage:

Korollar 1.2.6 - Idealgleichheit

Seien $I, J \subseteq K[X_1, \dots, X_n]$, $I \neq \{0\}$, $J \neq \{0\}$, zwei Ideale. Dann sind äquivalent:

- (a) Beide Ideale sind gleich.
- (b) Die reduzierten Gröbnerbasen sind gleich. □

Beweis. Dies folgt direkt aus der Eindeutigkeit der reduzierten Gröbnerbasis, siehe Proposition 1.2.5. ■

Beispiel 1.2.7 Wir betrachten den Ring $\mathbb{R}[a, b, c, d]$ mit der lexikographischen Ordnung oder der graduierten lexikographischen Ordnung, sodass $a > b > c > d$ gilt. Es sei J das Ideal, welches von den Polynomen

$$\begin{aligned} p_1 &:= a \cdot d - b \cdot c \quad \text{und} \\ p_2 &:= a^2 + b^2 + c^2 + d^2 - 1 \end{aligned}$$

erzeugt wird. Dann ist

$$\{p_1, p_2, abc + d(b^2 + c^2 + d^2 - 1), b^2c^2 + d^2(b^2 + c^2 + d^2 - 1)\}$$

eine reduzierte Gröbnerbasis für J . Für die Berechnung haben wir MUPAD genutzt. □

Zur Implementierung von Gröbnerbasen in Computeralgebrasystemen

In dieser Arbeit wurde vor allem auf MUPAD, ein inzwischen fest in MATLAB integriertes System zum symbolischen Rechnen, zurückgegriffen, um Gröbnerbasen zu berechnen. Ein weiteres Programm, SAGE, siehe [Sage], besitzt Implementierungen zum Berechnen von reduzierten Gröbnerbasen. Die deutsche Version ist frei erhältlich unter <http://www.sagemath.org/de/>. Weiterhin werden in Anhang C von [CLS] mehrere Computeralgebrasysteme diskutiert. Insbesondere werden die wichtigsten Befehle zum allgemeinen Umgang mit dem Programm und im Speziellen zum Berechnen von Gröbnerbasen vorgestellt. Es handelt sich hierbei um die Programme AXIOM (frei erhältlich, siehe [Axi]), MAPLE, MATHEMATICA und REDUCE

(frei erhältlich, siehe [Gra]). Nach [BPT], S. 461f, gibt es noch zwei weitere geeignete Programme: SINGULAR und MACAULAY2. Beide sind frei erhältlich. SINGULAR liefert Algorithmen, um die Standardbasis eines reduzierten Polynomrings zu berechnen, siehe http://www.singular.uni-kl.de/Manual/4-0-0/sing_303.htm oder [DGPS]. Die Gröbnerbasen, die mittels MACAULAY2, siehe [GSM], ermittelt wurden, sind im Allgemeinen reduziert.

1.3 Eine Basis für den Koordinatenring

Es sei $I \subseteq K[X_1, \dots, X_n]$, $I \neq \{0\}$, ein Ideal und G eine Gröbnerbasis von I bezüglich einer Monomordnung auf $K[X_1, \dots, X_n]$.

Im Folgenden wollen wir den K -Vektorraum $K[X_1, \dots, X_n]/I$ betrachten. Zunächst stellen wir einen sinnvollen Begriff auf, der Aussagen über den Grad eines reduzierten Polynoms macht, dann bestimmen wir eine Basis.

Der Grad eines reduzierten Polynoms

Definition 1.3.1 - Koordinatenring und Grad

Den K -Vektorraum $K[X_1, \dots, X_n]/I$ bezeichnen wir als den *Koordinatenring* des Ideals I . Für ein Polynom $f \in K[X_1, \dots, X_n]$ definiert

$$\deg(p + I) := \min(\deg(q) \mid p - q \in I, q \in K[X_1, \dots, X_n])$$

den *Grad* der Äquivalenzklasse von f . □

Proposition 1.3.2 - Für $p \in K[X_1, \dots, X_n]$ gilt:

$$\deg(p + I) \leq \deg(\bar{p}^G).$$

Falls p affin-linear ist, gilt die Gleichheit und $\deg(p + I) \leq 1$. Enthält I noch dazu keine nicht-trivialen affin-linearen Polynome, gilt sogar: $p = \bar{p}^G$. Die Gleichheit gilt immer, falls die Gröbnerbasis bezüglich der Ordnung \geq_{grlex} gebildet wurde. □

Beweis. Da ein $q \in I$ existiert, sodass $\bar{p}^G = p + q$ gilt, ist \bar{p}^G ein Repräsentant der Äquivalenzklasse $f + I$ und die Ungleichung ergibt sich aus der Definition des Grades. Sei nun p affin-linear. Ist $\deg(\bar{p}^G) = 0$, ergibt sich sofort die Gleichheit. Ist $\deg(\bar{p}^G) = 1$, folgt $\deg(p + I) \neq 0$, da sonst eine Konstante $c \in K$ existieren

würde, sodass $f + c \in I$ ist. Dies ist jedoch wegen der Eindeutigkeit der Normalform unmöglich. Weiterhin ist $\deg(p + I) \leq 1$. Falls I keine nicht-trivialen affin-linearen Polynome enthält, ist $p = \bar{p}^G$. Betrachten wir die Ordnung \geq_{grlex} auf $K[X_1, \dots, X_n]$ und ist $h \in I$, so ist der Leitterm von h nicht durch den Leitterm von \bar{p}^G teilbar. Also ist $\deg(\bar{p}^G) \leq \deg(\bar{p}^G + h)$. Es folgt die Gleichung $\deg(\bar{p}^G) = \deg(p + I)$. ■

Bemerkung 1.3.3 Im Allgemeinen ist die Behauptung

$$\deg(p + I) = \deg(\bar{p}^G)$$

falsch. Wir liefern ein Gegenbeispiel. Sei $I := \langle xy^2 - y^4 \rangle \subseteq (\mathbb{R}[x, y, z], \geq_{lex})$, dann ist das Polynom y^4 gleich seiner Normalform, aber $\deg(y^4 + I) = \deg(xy^2 + I) = 3$. □

Proposition 1.3.4 - Gradungleichungen

Für $p, q \in K[X_1, \dots, X_n]$ gilt:

- (i) $\deg(p + q + I) \leq \max(\deg(p + I), \deg(q + I))$,
- (ii) $\deg(p \cdot q + I) \leq \deg(p + I) + \deg(q + I)$. □

Beweis. Es seien Polynome $p', q' \in K[X_1, \dots, X_n]$ mit $p' + I = p + I$ und $q' + I = q + I$ so gewählt, dass $\deg(p + I) = \deg(p')$ und $\deg(q + I) = \deg(q')$ gilt. Dann gilt wegen Bemerkung 1.1.4:

$$\begin{aligned} \deg(p + q + I) &\leq \deg(p' + q') \leq \max(\deg(p'), \deg(q')) \\ &= \max(\deg(p + I), \deg(q + I)), \\ \deg(p \cdot q + I) &= \deg(p' \cdot q' + I) \leq \deg(p' \cdot q') \\ &= \deg(p') + \deg(q') = \deg(p + I) + \deg(q + I). \end{aligned}$$

Da $K[X_1, \dots, X_n]/I$ kein Integritätsring sein muss, gilt die Gleichheit in (ii) im Allgemeinen nicht. ■

Beispiel 1.3.5 Wir betrachten das Ideal $I := \langle x^2 - y^3, z^3 + x \rangle \subseteq (\mathbb{R}[x, y, z], \geq_{lex})$ und reduzierte Polynome

$$\begin{aligned} p &:= y^3 + I \quad \text{und} \\ q &:= 5 + x + 3y + I. \end{aligned}$$

Betrachten wir den möglichen Grad der Monome, die ein Polynom in I bilden, folgt: $\deg(p) = 2$, $\deg(q) = 1$, $\deg(p + q + I) = 2$ und $\deg(p \cdot q) = 3$. □

Notation. Sei $M \subseteq K[X_1, \dots, X_n]$ eine Teilmenge. Wir bezeichnen für $k \in \mathbb{N}_0$

$$M_k := \{p \in M \mid \deg(p) \leq k\}$$

als die Menge aller Elemente in M , deren Grad kleiner gleich k ist. Insbesondere bezeichnet

$$K[X_1, \dots, X_n]_1 = \left\{ p \in K[X_1, \dots, X_n] \mid \text{Es gibt } a_0, \dots, a_n \in K \text{ mit } p = a_0 + \sum_{i=1}^n a_i X_i \right\}$$

die Menge der affin-linearen Polynome. Weiterhin bezeichne

$$(M/I)_k := \{p + I \in M/I \mid \deg(p + I) \leq k\}$$

die Menge der reduzierten Polynome in M/I , deren Grad kleiner gleich k ist.

Proposition 1.3.6 - Sei $M \subseteq K[X_1, \dots, X_n]$ eine Teilmenge. Dann gilt:

- (i) $M_k/I \subseteq (M/I)_k$,
- (ii) $K[X_1, \dots, X_n]_k/I = (K[X_1, \dots, X_n]/I)_k$.

Insbesondere gilt: $K[X_1, \dots, X_n]_1/I = (K[X_1, \dots, X_n]/I)_1$. □

Beweis. (i): Ist $p \in M_k$, so gilt: $\deg(p + I) \leq k$.

(ii): Gilt $\deg(p + I) \leq k$, besitzt $p + I$ einen Repräsentanten $g \in K[X_1, \dots, X_n]_k$. ■

Bemerkung 1.3.7 Die Gleichheit in Proposition 1.3.6, (i), gilt im Allgemeinen nicht. Sei $I := \langle x - y^2 \rangle \subseteq \mathbb{R}[x, y, z]$ und $M := \langle y \rangle$. Dann ist $y^2 + I = x + I \in (M/I)_1$, aber $y^2 + I \notin M_1/I$. □

Eine Basis für den Koordinatenring

Wir definieren die Mengen

$$\mathcal{B}_0 := \{p \in K[X_1, \dots, X_n] \mid p \text{ ist Monom und kein LT}(g), g \in G, \text{ teilt } p\} \quad \text{und} \\ \mathcal{B} := \mathcal{B}_0/I.$$

Satz 1.3.8 - **Standardbasis**

Eine Basis des K -Vektorraums $K[X_1, \dots, X_n]/I$ ist gegeben durch \mathcal{B} . Wir nennen sie die *Standardbasis* für I und G . □

Beweis. *Schritt 1:* Die Menge \mathcal{B} ist ein Erzeugendensystem.

Sei $p \in K[X_1, \dots, X_n]$. Die Normalform \bar{p}^G ist in keinem Monom durch einen Leitterm $\text{LT}(g)$, $g \in G$, teilbar. Sie ist daher Linearkombination von endlich vielen Elementen aus \mathcal{B}_0 .

Schritt 2: Das System ist linear unabhängig.

Ist $p := \sum_{b \in \mathcal{B}_0} a_b b \in I$ mit $a_b \in K$ für alle $b \in \mathcal{B}_0$ und $a_b = 0$ für fast alle $b \in \mathcal{B}_0$, dann gilt: $\text{LT}(p) \in \text{LT}(I) = \langle \text{LT}(G) \rangle$. Im Fall $p \neq 0$ existiert ein Monom $b \in \mathcal{B}_0$, sodass $\text{LM}(p) = \text{LM}(b) = b$ gilt. Also ist $b \in \langle \text{LT}(G) \rangle$ und damit ist b durch einen Leitterm $\text{LT}(g)$, $g \in G$, teilbar. Dies ist aber nach Voraussetzung unmöglich. Also ist $p = 0$. ■

Bemerkung 1.3.9 Enthält I keine nicht-trivialen affin-linearen Polynome, gilt:

$$\{1 + I, X_1 + I, \dots, X_n + I\} \subseteq \mathcal{B}. \quad \square$$

Ein Ideal, welches aus affin-linearen Polynomen besteht, kann ersetzt werden:

Proposition 1.3.10 - Affin-lineare Polynome

Ist $p \in K[X_1, \dots, X_n]_1$ affin-linear mit $\deg(p) = 1$, dann gilt:

$$(K[X_1, \dots, X_n]/\langle p \rangle) \cong K[Y_1, \dots, Y_{n-1}]$$

im Vektorraumsinn, wobei Y_1, \dots, Y_{n-1} transzendent über dem Körper K sind. □

Beweis. Es sei $p := \sum_{i=0}^n a_i X_i \in K[X_1, \dots, X_n]$ mit Koeffizienten $a_0, \dots, a_n \in K$. Es sei o.B.d.A. $a_1 \neq 0$. Andernfalls ist eine Permutation der Variablen möglich. Das Leitmonom von p ist $\text{LM}(p) = X_1$, also ist \mathcal{B} mit $I := \langle p \rangle$ und

$$\mathcal{B}_0 = \{X^\alpha \mid \alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}_0^n, \alpha_1 = 0\}$$

die Standardbasis für I bezüglich der Gröbnerbasis $\{p\}$. Die Variablen Y_1, \dots, Y_n seien transzendent über K . Da lineare Abbildungen durch die Bilder der Basisvektoren eindeutig bestimmt sind, ist

$$\begin{aligned} K[X_1, \dots, X_n]/\langle p \rangle &\rightarrow K[Y_2, \dots, Y_n] \\ X^\alpha + I &\mapsto Y^{(\alpha_2, \dots, \alpha_n)} \quad \text{für } \alpha \in \mathbb{N}_0^n, \alpha_1 = 0 \end{aligned}$$

ein K -Vektorraum-Isomorphismus. Es gilt: $K[Y_2, \dots, Y_n] \cong K[Y_1, \dots, Y_{n-1}]$. ■

Definition 1.3.11 - Theta-Basis

Eine K -Vektorraum-Basis Θ von $K[X_1, \dots, X_n]/I$ heißt *Theta-Basis*, falls gilt:

- (i) $\{1 + I, X_1 + I, \dots, X_n + I\} \subseteq \Theta$,
- (ii) Für alle $k \in \mathbb{N}_0$ gilt: Sind $p, q \in \Theta_k$, dann ist $p \cdot q \in \text{span}_K(\Theta_{2k})$. \square

Diese Definition entnehmen wir [BPT]. Aus Eigenschaft (ii) folgt, dass Theta-Basen nicht endlich sind.

Proposition 1.3.12 - Standardbasen sind Theta-Basen

Falls das Ideal I keine nicht-trivialen affin-linearen Polynome enthält, ist die Standardbasis \mathcal{B} bezüglich einer zur Ordnung \geq_{grlex} gebildeten Gröbnerbasis eine Theta-Basis. Weiterhin ist dann \mathcal{B}_k eine Basis für $\mathbb{R}[X_1, \dots, X_n]_k/I$. \square

Beweis. Die erste Bedingung folgt aus Bemerkung 1.3.9. Nun zeigen wir die zweite Bedingung. Es seien $p, q \in \mathcal{B}_0$ Monome mit $p + I, q + I \in \mathcal{B}_k$. Dann existieren Polynome $p', q' \in K[X_1, \dots, X_n]$, sodass $p - p' \in I$ und $q - q' \in I$ ist und die Ungleichungen $\deg(p') \leq k$, $\deg(q') \leq k$ gelten. Dann ist

$$\deg(\overline{p \cdot q}) = \deg(p \cdot q + I) \leq \deg(p' \cdot q') \leq 2k.$$

Damit wird $\overline{p \cdot q}$ von Monomen vom Grad kleiner gleich $2k$ aufgespannt.

Nun zeigen wir die letzte Behauptung. Es sei $p \in \mathbb{R}[X_1, \dots, X_n]_k$. Dann haben alle Monome von p einen Grad, der kleiner gleich k ist. Es reicht also, zu zeigen, dass ein Monom vom Grad kleiner gleich k in der linearen Hülle von \mathcal{B}_k liegt. Dies liegt aber daran, dass die Normalform eines Monoms vom Grad kleiner gleich k aus reduzierten Monomen vom gleichen oder niedrigeren Grad besteht. \blacksquare

In diesem Fall sind die Koeffizienten bezüglich einer Entwicklung zur Standardbasis durch die Koeffizienten der Normalform gegeben.

Die Ordnung auf $K[X_1, \dots, X_n]$ ist maßgeblich für die Thetabaseneigenschaft der Standardbasis. Betrachten wir zum Beispiel das Ideal $I := \langle xy - y^4 \rangle \subseteq (\mathbb{R}[x, y], \geq_{lex})$, dann gilt: $x + I, y + I \in \mathcal{B}_1$, aber $xy + I = y^4 + I \notin \mathcal{B}_2$.

Es gibt allerdings auch Standardbasen bezüglich der lexikographischen Ordnung, die Theta-Basen sind, obwohl es Polynome gibt, deren Normalformen einen größeren Grad besitzen. Dies wollen wir illustrieren:

Beispiel 1.3.13 Wir betrachten das Ideal in $(\mathbb{R}[x, y], \geq_{lex})$, welches von den Polynomen

$$x^3 - y^4, xy^4 - z^4, y^5, y^4z, x^2z^4, yz^4, z^5$$

erzeugt wird. Diese Polynome bilden auch eine Gröbnerbasis des Ideals. Weiterhin bestimmen wir die zugehörige Standardbasis \mathcal{B} . Die Normalform von x^3 ist y^4 , also ist x^3 in \mathcal{B}_4 , aber nicht in \mathcal{B}_3 . Trotzdem bildet \mathcal{B} eine Theta-Basis. Dies sehen wir ein, indem wir Eigenschaft (ii) einer Theta-Basis für Monome mit geradem Grad, die durch x^3 teilbar sind, nachrechnen:

$$x^3x \equiv xy^4 \equiv z^4, x^3y \equiv y^5 \equiv 0, x^3z \equiv y^4z \equiv 0.$$

In allen anderen Fällen ergibt Reduktion einen kleineren Grad. □

Gewährleistet die Eigenschaft einer Basis Θ von $\mathbb{R}[X_1, \dots, X_n]/I$, Theta-Basis zu sein, dass Θ_{2k} eine Basis für $\mathbb{R}[X_1, \dots, X_n]_{2k}/I$ für alle $k \in \mathbb{N}$ ist? Es ist des Nachdenkens wert, dies zu prüfen. Am obigen Beispiel sehen wir, dass Θ_k im Allgemeinen keine Basis für $\mathbb{R}[X_1, \dots, X_n]_k/I$ ist. Weiterhin sehen wir schnell ein, dass die Aussage zumindest für Zweierpotenzen wahr ist: Da ein Monom vom Grad 2^k als Produkt zweier Monome vom Grad 2^{k-1} geschrieben werden kann, folgt die Aussage induktiv, da sie für den Wert 2 wahr ist. Allerdings liegt die Hürde darin, die Aussage für Produkte von Monomen vom Grad $2k + 1$, die selbst im Allgemeinen nicht in der linearen Hülle von Θ_{2k+1} liegen, zu zeigen.

2 Reelle Algebraische Geometrie

In diesem Kapitel stellen wir einige Ergebnisse der *reellen algebraischen Geometrie* vor. Dieser Zweig der Mathematik befasst sich mit der Struktur polynomialer Ungleichungen.

Über den Inhalt dieses Kapitels

Eines der interessantesten Probleme der Mathematik ist die Lösbarkeit von algebraischen Gleichungen. Während es selbst für nur eine Variable nicht immer möglich ist, eine konkrete Formel zur Bestimmung der Verschwindemenge eines Polynoms anzugeben, ist es möglich, die Verschwindemenge von Idealen zu charakterisieren. *Hilberts Nullstellensatz* setzt die Verschwindemenge von Polynomen eines Ideals mit seinem Radikal und den maximalen Idealen des gesamten Polynomrings in Verbindung, siehe [Hul] oder [Har]. Betrachtet man eine Menge von Polynomen mit reellen Koeffizienten, stellt sich die Frage nach den Eigenschaften der größten Menge, auf der alle Polynome nicht negativ sind. Umgekehrt ist die Frage nach der Gestalt von Polynomen, welche auf einer gegebenen Menge nicht negativ sind, interessant. Hier widmen wir uns diesen Fragen.

Die Tatsache, dass Polynome mit reellen Koeffizienten, die als Summe von Quadraten geschrieben werden, keine negativen Werte annehmen können, wenn sie an reellen Zahlen ausgewertet werden, zeigt, dass diese Polynome eine besondere Rolle bei der Betrachtung spielen. Ihre Struktur ist die eines *Kegels* in einem Ring. Darüber hinaus wird es notwendig sein, eine Verallgemeinerung der reellen Zahlen zu betrachten. Dies führt zur Theorie der *reell abgeschlossenen Körper* im ersten Abschnitt.

Verschwindet eine Familie von Polynomen auf einer Menge, so auch alle Polynome des erzeugten Ideals. Ist die Familie auf einer Menge nicht negativ, so auch der erzeugte Kegel. Ist sie ungleich Null, sind auch alle Produkte von Polynomen aus der Familie ungleich Null. Das Zusammenspiel zwischen *Nullstellen*, *Summen von Quadraten* und *Produkten* führt zu Aussagen über *Ideale*, *Kegel* und *Monoide* und

damit zum *formalen Positivstellensatz*, siehe Abschnitt 2.3. Mit dem *Transferprinzip von Tarski-Seidenberg*, von welchem der zweite Abschnitt handelt, sind wir in der Lage, diesen Satz auch zu konkretisieren und den *konkreten Positivstellensatz* aus dem formalen zu folgern.

Die Betrachtungen der ersten drei Abschnitte entnehmen wir der Publikation *Real Algebraic Geometry* von Bochnak, Coste und Roy, siehe [BCR]. Sie stammen aus den Kapiteln 1, *Ordered Fields*, *Real Closed Fields*, und 4, *Real Algebra*. Wir ergänzen sie um eine Einführung zu *semialgebraischen Mengen*, die [BPT] und [BCR] entlehnt ist. Weiterhin beweisen wir das Pendant zum Hilbertschen Nullstellensatz im reellen Fall, den *reellen Nullstellensatz*.

Schließlich zeigen wir mit dem *Satz von Schmüdgen* in Abschnitt 2.4, dass positive Polynome auf beschränkten Mengen eine quadratische Struktur aufweisen, also im Wesentlichen Elemente eines Kegels sind. Wir entnehmen die Ausführungen dieses Abschnitts dem Vorlesungsskript *Reelle algebraische Geometrie 1 & 2* von Netzer, siehe [Net].

Zur Anwendung der Erkenntnisse

Der Inhalt dieses Kapitels ist grundlegend für die Betrachtungen in Kapitel 4, in dem *Thetakörper* als Menge reeller Zahlentupel, auf der bestimmte Polynome, die als Summe von Quadraten geschrieben werden können, nicht negativ sind, studiert werden. An dieser Stelle möchten wir Anwendungsmöglichkeiten der reellen algebraischen Geometrie auf die Untersuchung von Thetakörpern vorstellen. Sie finden sich in den Abschnitten 4.1 und 4.3. Das Ziel ist es, die Ergebnisse dieses Kapitels gewinnbringend hinsichtlich der folgenden Frage einzusetzen:

Von welcher Gestalt sind Thetakörper und wann konvergieren sie?

1. Konvergenzverhalten von Thetakörpern Die Thetakörper eines Ideals bilden eine Kette von Obermengen der konvexen Hülle der Verschwindemenge des Ideals. Um das Konvergenzverhalten einer solchen Kette zu studieren, ist es hilfreich, eine Aussage über die Gestalt der Polynome machen zu können, die auf der Verschwindemenge nicht negativ sind: Sind diese Polynome schon solche, die Thetakörper bestimmen? Dann wäre Konvergenz gegeben. Nach dem *Satz von Schmüdgen* in Abschnitt 2.4 ist die Konvergenz von Thetakörpern für den Spezialfall einer kompakten Verschwindemenge gegeben.

2. Thetakörper als semialgebraische Menge Die Menge der einen Thetakörper bestimmenden Polynome ist im Allgemeinen nicht endlich. Gleichsam können wir einen Thetakörper als projizierten Spektraeder ansehen. Spektraeder sind semialgebraische Mengen, werden also von endlich vielen Polynomen aufgespannt. Sind projizierte Spektraeder auch semialgebraisch? Welche Polynome spannen die Projektion auf? In diesem Fall könnten wir endlich viele Polynome bestimmen, die einen Thetakörper aufspannen. Wie wir sehen werden, beantwortet das *Transferprinzip von Tarski-Seidenberg* in Abschnitt 2.2 diese Fragen positiv. Nach diesem Prinzip existiert ein algebraisches Ungleichungssystem in n Variablen, das beantwortet, wann ein algebraisches Ungleichungssystem in $n + 1$ Variablen lösbar ist. Gleichzeitig wird eine Methode geliefert, dieses Ungleichungssystem zu bestimmen. Darüber hinaus erlaubt es das Transferprinzip, eine konkrete Version des *formalen Positivstellensatzes*, der in Abschnitt 2.3 vorgestellt wird, zu erhalten. Aus ihm folgt schließlich der Satz von Schmüdgen.

Bei der Untersuchung der Symmetrien von Thetakörpern werden wir auf den reellen Nullstellensatz zurückgreifen.

In diesem Kapitel sei A ein kommutativer Ring. In den letzten drei Abschnitten bezeichnet R einen reell abgeschlossenen Körper.

2.1 Reell abgeschlossene Körper

Zunächst führen wir eine Kegelstruktur auf Ringen ein. Wir stellen danach eine Beziehung zwischen *Primkegeln* und *Anordnungen* auf Körpern her. Die zentralen Aussagen dieses Abschnitts besagen, dass die Körper (oder Ringe), die einen echten Kegel enthalten, die Körper (oder Ringe) sind, in denen die Eins keine Summe von Quadraten ist.

Kegel in Ringen und ihre Erzeuger

Definition 2.1.1 - Kegel kommutativer Ringe

Eine Teilmenge $P \subseteq A$ heißt *Kegel*, falls P die folgenden Eigenschaften erfüllt:

- (i) Sind $a, b \in P$, dann gilt: $a + b \in P$ und $a \cdot b \in P$,
- (ii) Ist $a \in A$, dann gilt: $a^2 \in P$.

Falls $-1 \notin P$ gilt, bezeichnen wir P als *echten Kegel*. □

Vergleichen wir diese Definition mit der eines Kegels in einem Vektorraum, siehe Seite 68, stellen wir fest, dass Bedingung (ii) insoweit anders lautet, als dort das Produkt durch ein Skalarprodukt ersetzt wird. Doch auch für Vektorräume, die Algebren sind, ist die Definition verschieden: der dritte Quadrant der komplexen Zahlenebene ist ein Kegel im \mathbb{R} -Vektorraum \mathbb{C} , aber kein Kegel im Körper \mathbb{C} .

Beispiel 2.1.2

- (1) Die nicht-negativen reellen Zahlen bilden einen echten Kegel im Körper der reellen Zahlen.
- (2) Die Menge aller Polynome in $\mathbb{R}[X]$, die auf einer gegebenen Menge reeller Zahlen nicht negativ ist, bildet einen echten Kegel.
- (3) Die Schnittmenge einer Familie von Kegeln ist wieder ein Kegel.
- (4) Ist $P \subseteq A$ ein Kegel, so ist $n \cdot 1 \in P$ für $n \in \mathbb{N}_0$.
- (5) Ist K ein Körper und $P \subseteq K$ ein Kegel, so ist $\mathbb{Q}_0^+ \subseteq P$, da für $n \in \mathbb{N}$ gilt: $\frac{1}{n} = \frac{1}{n^2} + \dots + \frac{1}{n^2}$. □

Sei $(a_i)_{i \in I} \subseteq A$ eine nichtleere Familie von Elementen. Die Menge

$$\mathcal{M}[(a_i)_{i \in I}] := \left\{ \prod_{i \in I_0} a_i \mid I_0 \subseteq I \text{ endlich} \right\}$$

ist ein multiplikativer Monoid. Es ist $1 \in \mathcal{M}[(a_i)_{i \in I}]$.

Die Summe aller Quadrate von A ist wieder ein Kegel. Wir bezeichnen ihn mit

$$\mathcal{K}_A := \sum A^2 := \left\{ \sum_{i=1}^s a_i^2 \mid a_1, \dots, a_s \in A \right\}.$$

Dieser Kegel ist der Schnitt aller Kegel von A , der *kleinste Kegel von A* .

Sei $M \subseteq A$ eine Teilmenge. Der Schnitt aller Kegel, die M enthalten, ist ein Kegel. Wir bezeichnen ihn mit $\mathcal{K}[M]$ oder als den *erzeugten Kegel* von M . Ist $P \subseteq A$ ein Kegel von A , dann ist leicht einzusehen, dass

$$\mathcal{K}[P, (a_i)_{i \in I}] = \left\{ p + \sum_{i=1}^s q_i b_i \mid p, q_1, \dots, q_s \in P, b_1, \dots, b_s \in \mathcal{M}[(a_i)_{i \in I}] \right\}$$

für den erzeugten Kegel $\mathcal{K}[P, (a_i)_{i \in I}]$ von P und $(a_i)_{i \in I}$ gilt.

Primkegel und ihre Träger

Definition 2.1.3 - Primkegel

Ein echter Kegel $P \subseteq A$ heißt *Primkegel*, falls für alle $a, b \in P$ gilt:

$$\text{Aus } a \cdot b \in P \text{ folgt: } a \in P \text{ oder } -b \in P. \quad \square$$

Ein Primkegel und sein Negatives spannen den Ring A auf:

Proposition 2.1.4 - Primkegel als Erzeuger

Ein Primkegel $P \subseteq A$ ist ein *Erzeuger* von A , das heißt, es gilt:

$$P \cup (-P) = A. \quad \square$$

Beweis. Sei $a \in A$. Es gilt $a^2 \in P$ und per Definition liegt entweder a oder $-a$ im Primkegel P . ■

Beispiel 2.1.5 Es liegt die Überlegung nahe, ob ein echter Kegel $P \subseteq A$, der die Bedingung $P \cup (-P) = A$ erfüllt, Primkegel ist. Dem ist aber nicht so. Das folgende Gegenbeispiel soll dies illustrieren. Im Ring $\mathbb{R}[X]$ betrachten wir den Kegel

$$P := \mathcal{K}[E] \text{ mit} \\ E := \{ \lambda_0, -\lambda_1 X, \lambda_2 (1 + \lambda_3 X), \mu_1 X^2, \mu_2 X^3, \mu_4 X^4, \dots \mid \lambda_0, \dots, \lambda_3 \in \mathbb{R}_0^+, \mu_1, \dots \in \mathbb{R} \}.$$

Behauptung: P ist ein echter Kegel und ein Erzeuger von A .

Beweis: Es ist $-1 \notin P$, also ist P echt. Weiterhin enthält P beliebige Summen der angegebenen Erzeuger. Für ein Polynom $a := \sum_{i=0}^r a_i X^i \in A$ ist $a_0 + a_1 X \in P \cup (-P)$ und $\sum_{i=2}^r a_i X^i \in P \cap (-P)$. Also ist $a \in P \cup (-P)$. ◇

Behauptung: $X \notin P$.

Beweis: Wir nehmen $X \in P$ an. Dann existieren Quadratsummen $p, p_1, \dots, p_s \in \sum A^2$ und $q_1, \dots, q_s \in \mathcal{M}[E]$, sodass $X = p + \sum_{i=1}^s p_i q_i$. Aus dieser Darstellung von X folgt, dass einer der Summanden $p, p_1 q_1, \dots, p_s q_s$ ein Absolutglied besitzt, welches nicht verschwindet. Die Absolutglieder von p, p_1, \dots, p_s sind nicht negativ. Besitzt q_j für $j \in \{1, \dots, s\}$ ein Absolutglied, welches nicht verschwindet, so ist $q_j = \prod_{k=1}^r g_k$ mit affin-linearen Polynomen g_1, \dots, g_r , deren Absolutglied echt positiv ist. Also besitzt auch q_j ein Absolutglied, welches nicht negativ ist. Daraus folgt, dass die Summe $p + \sum_{i=1}^s p_i q_i$ ein Absolutglied besitzt, welches echt positiv ist. Dies ist aber unmöglich. Wir erhalten einen Widerspruch. ◇

Da $-X^2 = X \cdot (-X) \in P$ gilt, ist P kein Primkegel. □

Urbilder von Primkegeln sind Primkegel:

Proposition 2.1.6 - Seien A und B zwei kommutative Ringe, $P \subseteq B$ ein Primkegel und $f : A \rightarrow B$ ein Ringhomomorphismus. Dann ist $f^{-1}(P)$ ein Primkegel von A . \square

Beweis. Die Aussage folgt direkt aus der Definition eines Primkegels. \blacksquare

Die Definitionen von Primkegeln und Primidealen ähneln sich. Die folgende Aussage zeigt eine weitere Analogie auf:

Proposition 2.1.7 - Träger eines Primkegels

Sei $P \subseteq A$ ein Primkegel, dann ist

$$\text{supp}(P) := P \cap (-P)$$

ein Primideal in A , der *Träger* von P . \square

Beweis. *Schritt 1:* $\text{supp}(P)$ ist ein Ideal.

Dass $\text{supp}(P)$ eine additive Untergruppe ist, ist leicht zu sehen. Jetzt zeigen wir, dass das Produkt beliebiger Elemente $a \in A$ und $b \in \text{supp}(P)$ wieder im Träger liegt. Ist $a \in P$, ist $ab \in \text{supp}(P)$. Ist $a \notin P$, ist $-a \in P$ und es folgt: $(-a) \cdot (-b) = ab \in P$ und $(-a) \cdot b = -ab \in P$.

Schritt 2: $\text{supp}(P)$ ist ein Primideal.

Sei $ab \in \text{supp}(P)$ und $a \notin \text{supp}(P)$. Falls $a \notin P$ gilt, ist $b \in \text{supp}(P)$ wegen $ab \in P$ und $a \cdot (-b) \in P$. Falls $a \in P$, ist $b \in P$ und $b \in -P$. \blacksquare

Primkegel induzieren Positivkegel

Jetzt widmen wir uns zunächst Ordnungen auf Körpern.

Definition 2.1.8 - Angeordnete Körper

Ein Körper F heißt *angeordnet*, falls F ein total geordneter Körper ist, d.h. ein Körper, auf dem eine reflexive, antisymmetrische und transitive Relation \leq existiert, bezüglich der alle Elemente vergleichbar sind, und für alle $x, y, c \in F$ gilt:

- (i) Ist $x \leq y$, dann $x + c \leq y + c$,
- (ii) Ist $0 \leq x, 0 \leq y$, dann $0 \leq xy$.

Der *Positivkegel* P von F ist die Menge $P := \{x \in F \mid 0 \leq x\}$. \square

Wir sprechen auch von einer *Anordnung* auf einem Körper und folgern aus den Axiomen:

Proposition 2.1.9 - Sei (F, \leq) ein angeordneter Körper, dann gilt:

- (i) Aus $x \leq y, w \leq z$ folgt: $x + w \leq y + z$,
- (ii) Es ist $0 < 1$,
- (iii) Aus $0 \leq x, 0 \leq y$ und $x + y = 0$ folgt: $x = y = 0$,
- (iv) Der Positivkegel P ist ein Kegel und es gilt: $P \cup (-P) = F$. □

Beweis. Die erste Behauptung folgt aus Definition 2.1.8, (i). Aus Voraussetzung (ii) folgt $0 < 1$, da 1 ein Quadrat ist. Die nächste Behauptung folgt aus der Antisymmetrie von Ordnungsrelationen. Aus (ii) folgt auch, dass der Positivkegel ein Kegel im Sinne von Definition 2.1.1 ist. Da die Ordnung eines angeordneten Körpers total ist, folgt für den Positivkegel P die Gleichung $P \cup (-P) = F$, da je zwei Elemente vergleichbar sind. ■

Beispiel 2.1.10 Der Körper der rationalen oder reellen Zahlen ist angeordnet. Körper der Charakteristik Null können wegen Proposition 2.1.9, (ii), nicht angeordnet werden. Der Körper der komplexen Zahlen kann nicht angeordnet werden, da in einem angeordneten Körper alle Quadrate nicht negativ sind, aber $i^2 = -1 \leq 0$ gilt. Aus dem gleichen Grund kann kein algebraisch abgeschlossener Körper angeordnet werden. Auf $\mathbb{R}[X]$ existiert genau eine Ordnung, sodass X positiv und kleiner als alle positiven reellen Zahlen ist, siehe [BCR], Kapitel 1, Abschnitt 1. □

Primkegel und Positivkegel sind eng verwandt, wie wir im Folgenden sehen werden. Zunächst liefert der folgende Spezialfall Gleichheit:

Proposition 2.1.11 - **Primkegel sind Positivkegel**

Sei F ein Körper, dann gibt es eine Eins-zu-Eins-Beziehung zwischen:

- (a) Primkegeln von F ,
- (b) Positivkegeln einer Anordnung von F . □

Beweis. Ist $P \subseteq F$ ein Primkegel in F , dann definiert $x \leq y := y - x \in P$ eine Anordnung auf F . Umgekehrt ist für eine Anordnung (F, \leq) ein Primkegel von F gegeben durch $\{y - x \mid x, y \in F, x \leq y\}$. Die Abbildung ist eineindeutig. ■

Falls der zu Grunde liegende Ring kein Körper ist, ist der Träger $\text{supp}(P)$ eines Primkegels $P \subseteq A$ im Allgemeinen nicht trivial.

Beispiel 2.1.12 Ein Beispiel dafür ist der Kegel

$$K := \mathcal{K}[\pm X^n \mid n \in \mathbb{N}] \subseteq \mathbb{R}[X].$$

Dieser Kegel besteht aus den Polynomen mit positivem Absolutglied. Daher ist er ein echter erzeugender Kegel mit nicht-trivialem Träger. Sind $a, b \in \mathbb{R}[X]$ zwei Polynome mit $a \notin K$ und $-b \notin K$, so besitzt a ein negatives und b ein positives Absolutglied. Das Produkt $a \cdot b$ besitzt ein negatives Absolutglied, also gilt: $a \cdot b \notin K$. Daraus folgt, dass K ein Primkegel ist. \square

In solch einem Fall ist betrachten wir Positivkegel auf Quotientenkörpern, die von Primkegeln abhängen. Da $\text{supp}(P)$ ein Primideal ist, ist $A/\text{supp}(P)$ ein Integritätsring. Wir können also den Quotientenkörper von $A/\text{supp}(P)$ studieren.

Lemma 2.1.13 - Primkegel induzieren Positivkegel

Sei $P \subseteq A$ ein Primkegel. Wir bezeichnen den Quotientenkörper von $A/\text{supp}(P)$ mit K_P . Seien $\pi : A \rightarrow A/\text{supp}(P)$ und $\Pi : A \rightarrow K_P$ die kanonischen Projektionen. Dann ist

$$P' := \{\pi(a)/\pi(b) \in K_P \mid ab \in P, b \notin \text{supp}(P)\}$$

Positivkegel einer Anordnung auf K_P und $P = \Pi^{-1}(P')$. \square

Beweis. Die Menge P' ist ein Kegel, was durch Nachrechnen der Axiome nachvollzogen werden kann.

Behauptung: Es ist $P = \Pi^{-1}(P')$.

Beweis: Es sei $\pi(c) = \pi(a)/\pi(b) \in P'$ mit $ab \in P$ und $b \notin \text{supp}(P)$. Mit der Annahme $b \in P$ folgt daraus $a \in P$. Nun ist $cb = a + d$ für ein $d \in \text{supp}(P)$. Daraus folgt, dass $c \in P$ ist. Analog ist $c \in P$ im Fall $b \notin P$. Es folgt: $P = \Pi^{-1}(P')$. Wir beachten, dass aus dieser Gleichung $\Pi(P) = P'$ folgt. \diamond

Damit ist P' ein echter Kegel. Aus einer einfachen Rechnung folgt, dass P' auch ein Primkegel ist. Mit Proposition 2.1.11 ist P' Positivkegel einer Ordnung. \blacksquare

Korollar 2.1.14 - Primkegel und Homomorphismen

Sei $P \subseteq A$ eine Teilmenge. Dann sind äquivalent:

- (a) P ist Primkegel.
- (b) Es existiert ein angeordneter Körper F und ein Ringhomomorphismus $f : A \rightarrow F$, sodass gilt: $P = \{a \in A \mid f(a) \geq 0\}$. \square

Beweis. Ist P ein Primkegel, erhalten wir mit Lemma 2.1.13 eine Ordnung auf dem Körper K_P , sodass der Positivkegel das Bild von P unter der kanonischen Projektion ist. Die umgekehrte Aussage folgt aus Proposition 2.1.6. \blacksquare

Nun wieder zu Körpern. Echte Kegel eines Körpers sind in Positivkegeln enthalten:

Lemma 2.1.15 - Kegel im Positivkegel

Sei F ein Körper und $P \subseteq F$ ein echter Kegel. Dann gilt:

- (i) Ist $-a \notin P$, dann ist auch $\mathcal{K}[P, a] = \{x + ay \mid x, y \in P\}$ ein echter Kegel.
- (ii) Es gibt eine Anordnung auf F , deren Positivkegel P enthält. \square

Beweis. (i): Angenommen, es ist $x, y \in P$ mit $-1 = x + ay$, dann ist $y = 0$ ausgeschlossen. Aber auch $y \neq 0$ ist nicht möglich, da dann im Widerspruch zur Annahme $-a = (1/y)^2 \cdot y \cdot (1 + x) \in P$ gilt.

(ii): Das Lemma von Zorn zeigt die Existenz eines maximalen echten Kegels M , in dem P enthalten ist.

Behauptung: Es gilt $M \cup (-M) = F$.

Beweis: Falls $a \in F$ und $a \notin M$ ist, gilt für die Adjungtion $\mathcal{M}[M, -a] = M$ und damit folgt, dass $-a \in M$ ist. \diamond

Damit ist $M \cap (-M)$ ein Ideal in F . Da M ein echter Kegel ist, ist ausgeschlossen, dass $M \cap (-M) = F$ gilt. Es folgt: $M \cap (-M) = \{0\}$.

Behauptung: Der Kegel M ist sogar ein Primkegel.

Beweis: Es sei $ab \in M$ mit $a \notin M$. Angenommen, es ist $(-b) \notin M$. Da der Kegel M ein Erzeuger von F ist, ist $(-a) \in M$ und $b \in M$, also ist $-ab \in M$. Daraus folgt, dass $ab \in M \cap (-M) = \{0\}$ ist. Da ein Körper insbesondere ein Integritätsring ist, folgt, dass $a = 0$ oder $b = 0$ gilt. Beide Fälle sind aber nach Voraussetzung ausgeschlossen. Dies führt zu einem Widerspruch. \diamond

Damit ist M ein Primkegel und damit nach Proposition 2.1.11 der Positivkegel einer Anordnung. \blacksquare

Echte Kegel und Summen von Quadraten

Wir können nun Körper nach ihrer Fähigkeit zur Anordnung klassifizieren:

Satz 2.1.16 - Angeordnete Körper

Sei F ein Körper. Dann sind äquivalent:

- (a) F kann angeordnet werden.
- (b) F besitzt einen echten Kegel.
- (c) Es gilt: $-1 \notin \sum F^2$.
- (d) Für alle $x_1, \dots, x_n \in F$ gilt: Aus $\sum_{i=1}^n x_i^2 = 0$ folgt $x_1 = \dots = x_n = 0$. \square

Beweis. $(a) \Rightarrow (b) \Rightarrow (c) \Leftrightarrow (d)$: Dies erschließt sich mittels früherer Aussagen.

$(c) \Rightarrow (b)$: Ein echter Kegel ist gegeben durch ΣF^2 .

$(b) \Rightarrow (a)$: Lemma 2.1.15. ■

Definition 2.1.17 - Reelle Körper und Ideale

Sei F ein Körper.

- (i) F heißt *reell*, falls F die äquivalenten Bedingungen aus Satz 2.1.16 erfüllt.
- (ii) F heißt *reell abgeschlossen*, falls F ein reeller Körper ist und keine nicht-trivialen algebraischen Erweiterungen, die reell sind und die Anordnung auf F fortsetzen, besitzt.

Ein Ideal $I \subseteq A$ heißt *reell*, falls für $a_1, \dots, a_s \in A$ mit $\sum_{i=1}^s a_i^2 \in I$ gilt, dass $a_i \in I$ für alle $i = 1, \dots, s$ ist. □

Nun klassifizieren wir Ringe, die einen echten Kegel besitzen.

Korollar 2.1.18 - Der Träger eines Primkegels ist ein reelles Primideal. □

Beweis. Sei $P \subseteq A$ ein Primkegel. Nach Proposition 2.1.7 ist der Träger $\text{supp}(P)$ ein Primideal. Sei $a_1, \dots, a_s \in A$ mit $\sum_{i=1}^s a_i^2 = 0$. Übernehmen wir die Notation aus Satz 2.1.13, folgt, dass $\sum_{i=1}^s \Pi(a_i)^2 = 0$ ist. Da K_P ein angeordneter Körper ist, gilt $\Pi(a_i) = 0$ für $i = 1, \dots, s$ und die Aussage folgt. ■

Lemma 2.1.19 - Existenz eines reellen Abschlusses

Ein reeller Körper besitzt eine algebraische Körpererweiterung, die reell abgeschlossen ist. □

Beweis. Sei F ein reeller Körper. Auf der Menge X der reellen algebraischen Körpererweiterungen von F , die die Anordnung auf F fortsetzen, definieren wir eine partielle Ordnung wie folgt:

$$(G, \leq_G) \leq (H, \leq_H) :\Leftrightarrow G \subseteq H \text{ und } \leq_H \text{ setzt } \leq_G \text{ auf } H \text{ fort}$$

für $(G, \leq_G), (H, \leq_H) \in X$. Eine obere Schranke für eine Kette in X ist die Vereinigung aller Elemente der Kette. Mit dem Lemma von Zorn existiert ein maximales Element von X . Dieses ist ein reeller Körper, der keine nicht-trivialen algebraischen Erweiterungen, die reell ist und die Anordnung auf F fortsetzt, besitzt. ■

Satz 2.1.20 - Primkegel in Ringen

Die folgenden Aussagen sind äquivalent:

- (a) A besitzt einen echten Kegel.
- (b) A besitzt einen Primkegel.
- (c) A besitzt ein reelles Primideal.
- (d) Es existiert ein Ringhomomorphismus $f : A \rightarrow K$ in einen reell abgeschlossenen Körper K .
- (e) Es gilt: $-1 \notin \sum A^2$. □

Beweis. (a) \Rightarrow (b): Sei P ein maximaler echter Kegel von A . Ein solcher Kegel existiert nach dem Lemma von Zorn. Wir zeigen, dass P ein Primkegel ist. Seien dazu $a, b \in A$ mit $ab \in P$, $a \notin P$ und $-b \notin P$. Die Kegel $\mathcal{K}[P, a]$ und $\mathcal{K}[P, -b]$ sind nicht echt, also existieren $q_1, q_2, p_1, p_2 \in P$ mit $-1 = p_1 + q_1 a$ und $-1 = p_2 - q_2 b$. Nun ist $1 + p_1 = -q_1 a$ und $1 + p_2 = q_2 b$. Es folgt: $1 + p_1 + p_2 + p_1 p_2 = -q_1 q_2 ab$. Stellen wir die Gleichung nach -1 um, ist die andere Seite der Gleichung ein Element von P , da $ab \in P$ nach Voraussetzung gilt. Dies führt zu einem Widerspruch.

(b) \Rightarrow (d): Korollar 2.1.14.

(d) \Rightarrow (c): Der Kern von f ist ein reelles Primideal.

(c) \Rightarrow (e): Sei I ein reelles Primideal von A . Angenommen, $-1 \in \sum A^2$, dann existiert ein $s \in \sum A^2$ mit $1 + s = 0 \in I$, also folgt $1 \in I$.

(e) \Rightarrow (a): Die Menge $\sum A^2$ ist ein echter Kegel. ■

Charakterisierung reell abgeschlossener Körper

Reell abgeschlossene Körper verhalten sich in vielen Aspekten wie die reellen Zahlen. Hier möchten wir einige Aspekte vorstellen.

Satz 2.1.21 - Reell abgeschlossene Körper

Für einen Körper F sind äquivalent:

- (a) F ist reell abgeschlossen.
- (b) Es gibt genau eine Ordnung auf F . Diese wird durch den Kegel $\sum F^2$ induziert. Weiterhin besitzt jedes Polynom in $F[X]$ von ungeradem Grad eine Nullstelle in F .
- (c) $F[i] = F[X]/(X^2 + 1)$ ist ein algebraisch abgeschlossener Körper. □

Beweis. (a) \Rightarrow (b): Zuerst zeigen wir, dass die Ordnung auf F eindeutig ist.

Behauptung: $\Sigma F^2 \cup (-\Sigma F^2) = F$.

Beweis: Sei $a \in F \setminus \Sigma F^2$. Dann ist $F[\sqrt{a}] = F/(X^2 - a)$ eine nicht-triviale algebraische Erweiterung von F . Jede Anordnung auf $F[\sqrt{a}]$ setzt die Anordnung auf F fort. Nach Voraussetzung folgt, dass $F[\sqrt{a}]$ nicht reell ist. Es existieren also $x_1, \dots, x_r \in F$ und $y_1, \dots, y_n \in F$ mit

$$-1 = \sum_{i=1}^r (x_i + \sqrt{a}y_i)^2.$$

Daraus folgt: $-1 = \sum_{i=1}^r x_i^2 + a \sum_{i=1}^r y_i^2 \in F$. Es folgt weiterhin: $s := \sum_{i=1}^r y_i^2 > 0$. Also ist $s^{-1} = s \cdot (s^{-1})^2 \in \Sigma F^2$ und

$$-a = s^{-1} \left(1 + \sum_{i=1}^r x_i^2 \right) \Sigma F^2.$$

Damit folgt die Aussage. ◇

Ein Element $a \in F$, welches keine Quadratsumme ist, ist negativ. Daraus folgt, dass ein Positivkegel auf F aus den Quadratsummen besteht. Es bleibt zu zeigen, dass jedes Polynom in $F[X]$ von ungeradem Grad eine Nullstelle in F besitzt. Wir nehmen an, dass ein Polynom $f \in F[X]$ von ungeradem Grad $d > 1$ existiert, welches keine Nullstelle in F besitzt, und jedes Polynom in $F[X]$, dessen Grad ungerade und kleiner d ist, eine Nullstelle in F besitzt.

Behauptung: Dies führt zu einem Widerspruch.

Beweis: Da jeder echte irreduzible Faktor von f mit ungeradem Grad eine Nullstelle in F besitzt, ist f irreduzibel. Jede Anordnung auf der algebraischen Erweiterung $F[X]/\langle f \rangle$ setzt die Anordnung auf F fort. Also ist $F[X]/\langle f \rangle$ nicht reell. Es existieren $h_1, \dots, h_r \in F[X]$ und $g \in F[X]$ mit

$$-1 = \sum_{i=1}^r h_i^2 + fg.$$

Wir können annehmen, dass der Grad von h_1, \dots, h_r jeweils echt kleiner d ist, da diese Polynome nach f reduziert werden können. Es folgt, dass g einen ungeraden Grad kleiner gleich $d - 2$ und damit eine Nullstelle in F besitzt. Dies ist allerdings unmöglich. ◇

Also muss jedes Polynom von ungeradem Grad eine Nullstelle besitzen.

(b) \Rightarrow (c): Aus der Voraussetzung folgt einerseits, dass die Charakteristik von F null ist. Andererseits existiert eine Betragsfunktion $\|\cdot\|$ auf F .

Schritt 1: Wir zeigen zunächst, dass jedes Polynom vom Grad zwei in $F[X]$

reduzibel ist.

Behauptung: Für alle $h \in F[\imath]$ existiert ein $w \in F[\imath]$ mit $w^2 = h$.

Beweis: Ist $h \in F$, so ist die Aussage wahr, da $h = \sqrt{\|h\|^2}$ ist. Seien nun $a, b \in F$ mit $b \neq 0$. Dann besitzt die Gleichung

$$a + i \cdot b = (c + i \cdot d)^2 \text{ beziehungsweise}$$

$$c^2 = a + d^2 \quad \text{und} \quad c = \frac{b}{2d}$$

eine Lösung $(c, d) \in F^2$, da nach Voraussetzung das Polynom $d^3 + ad^2 - \frac{1}{4}b^2$ über dem Körper F in Linearfaktoren zerfällt. \diamond

Daraus folgt, dass ein Polynom $X^2 + hX + l$ mit $h, l \in F[\imath]$ zwei Nullstellen in $F[\imath]$ besitzt.

Schritt 2: Sei $f \in F[X]$. Wir zeigen induktiv, dass jedes Polynom in $F[X]$ eine Nullstelle in $F[\imath][X]$ besitzt. Sei $f \in F[X]$ vom Grad $d = 2^m n$, wobei $n \in \mathbb{N}$ ungerade ist. Für $m = 0$ ist die Aussage nach Voraussetzung wahr. Sei nun $m \geq 1$ und die Aussage für $m - 1$ wahr.

Behauptung: f besitzt eine Nullstelle in $F[\imath][X]$.

Beweis: Ist K ein Körper der Charakteristik null und L der Zerfällungskörper einer Familie von Polynomen aus $K[X]$, so ist der Fixkörper der Gruppe der Körperautomorphismen von L über K gleich K . Ist weiterhin L der Zerfällungskörper eines irreduziblen Polynoms $p \in K[X]$, so ist die Automorphismengruppe von L über K eine Untergruppe der Permutationsgruppe der Nullstellen von p . Ein Polynom in $L[X]$, dessen Koeffizienten symmetrisch in den Nullstellen von p sind, kann also als Polynom in $K[X]$ aufgefasst werden. Seien nun z_1, \dots, z_d die Nullstellen von f in einem algebraischen Abschluss von F . Wir betrachten das Polynom

$$g_h := \prod_{i < j} (X - z_i - z_j - h \cdot z_i z_j)$$

für $h \in \mathbb{Z}$. Für jeden Parameter ist es symmetrisch in z_1, \dots, z_d . Wie oben bemerkt, gilt: $g_h \in F[X]$. Der Grad von g_h ist $2^{m-1}(2^m - 1)$. Aus der Induktionsvoraussetzung folgt, dass $i_h, j_h \in \{1, \dots, d\}$ mit $z_{i_h} + z_{j_h} + h \cdot z_{i_h} z_{j_h} \in F[\imath]$ existieren. Ordnen wir Elementen $h \in \mathbb{Z}$ die Indizes (i_h, j_h) zu, so ist diese Abbildung nicht injektiv. Zwei Zahlen $h', h'' \in \mathbb{Z}$ mit $h' \neq h''$ erfüllen also die Gleichungen $i_{h'} = i_{h''}$ und $j_{h'} = j_{h''}$. Daraus folgt:

$$z_{i_{h'}} + z_{j_{h'}} \in F[\imath] \quad \text{und} \quad z_{i_{h'}} z_{j_{h'}} \in F[\imath].$$

Es ist also $g := (X - z_{i_{h'}})(X - z_{j_{h'}}) \in F[\imath][X]$. Nach dem letzten Schritt sind die Nullstellen von g Elemente aus $F[\imath]$. \diamond

Sei nun $f \in F[i][X]$. Mit \bar{f} sei das Polynom in $F[i]$ bezeichnet, welches sich aus f durch Konjugation der Koeffizienten ergibt. Eine einfache Rechnung zeigt, dass das Produkt $f \cdot \bar{f} \in F[X]$ ist. Damit besitzt $f \cdot \bar{f}$ eine Nullstelle z in $F[i]$. Es folgt, dass x oder die Konjugation von x eine Nullstelle von f ist.

(c) \Rightarrow (a): Da $F[i]$ algebraisch abgeschlossen ist, existiert für $a + ib$ mit $a, b \in F$ eine Quadratwurzel $c + id$ mit $c, d \in F$. Es ist also $a^2 + b^2 = (c^2 + d^2)^2$. Damit ist eine Summe von Quadraten in F ein Quadrat. Es folgt, dass F reell ist. Eine algebraische Erweiterung von F hat den Grad zwei. Damit sind jeweils zwei Erweiterungen isomorph und insbesondere nicht reell. ■

Aus diesem Satz folgt, dass \mathbb{R} ein reell abgeschlossener Körper ist.

Das Vorzeichen von Polynomen und deren Ableitungen

Es sind viele Kriterien bekannt, die hinreichend für die Existenz von Nullstellen von Polynomen über dem Körper der reellen Zahlen oder deren Ableitungen sind. Einige davon gelten auch für Polynome über reell abgeschlossenen Körpern. In diesem Unterabschnitt sollen einige angeführt und im nächsten Abschnitt zur Anwendung kommen. Dabei ist es nicht nötig, topologische Begriffe einzuführen.

Es sei R ein reell abgeschlossener Körper.

Korollar 2.1.22 - Der Zwischenwertsatz für Polynome

Es seien $f \in R[X]$ und $a, b \in R$ mit $a < b$. Dann gilt: Ist $f(a)f(b) < 0$, dann existiert ein $c \in R$ mit $a < c < b$ und $f(c) = 0$. □

Beweis. Sei f nicht konstant. Die irreduziblen Faktoren von f sind linear oder von der Form $(X - (a + ib))(X - (a - ib)) = (X - a)^2 + b^2$ für $(a, b) \in F^2$. Da dieser Term immer positiv auf F ist, folgt, dass Vorzeichenwechsel nur in Linearfaktoren von f stattfinden können. ■

Korollar 2.1.23 - Der Mittelwertsatz für formale Ableitungen

Es seien $f \in R[X]$ und $a, b \in R$ mit $a < b$. Dann gilt:

- (i) Ist $f(a) = f(b) = 0$, so hat die formale Ableitung f' von f eine Nullstelle $z \in R$ mit $a < z < b$.
- (ii) Es existiert ein $c \in R$, $a < c < b$, mit $f(b) - f(a) = (b - a)f'(c)$.
- (iii) Verschwindet die Ableitung von f nirgends, besitzt f genau eine Nullstelle in R . □

Beweis. (i): Wir können annehmen, dass f keine Nullstelle zwischen a und b besitzt. Dann existiert ein Polynom $g \in R[X]$, sodass g keine Nullstelle zwischen a und b besitzt und

$$f = (X - a)^m(X - b)^n g$$

gilt. Dann ist

$$\begin{aligned} f' &= (X - a)^{m-1}(X - b)^{n-1}g_0, \\ g_0 &:= m(X - b)g + n(X - a)g + (X - a)(X - b)g'_0. \end{aligned}$$

Es ist $g_0(a) = m(a - b)g$ und $g_0(b) = n(b - a)g$, also hat g_0 einen Vorzeichenwechsel zwischen a und b . Aus Korollar 2.1.22 folgt, dass g_0 und damit auch f' eine Nullstelle $z \in R$ mit $a < z < b$ besitzt.

(ii): Für das Polynom

$$g(X) := f(X) - \left(\frac{f(b) - f(a)}{b - a} X + f(a) - a \frac{f(b) - f(a)}{b - a} \right)$$

gilt: $g(a) = g(b) = 0$. Nach (ii) existiert ein $c \in R$, $a < c < b$, sodass $g'(c) = 0$.

(iii): Aus (i) folgt, dass f höchstens eine Nullstelle besitzt. Angenommen, f besitzt keine Nullstelle in R . Dann ist der Grad von f nach Satz 2.1.21, (b), gerade. Daraus folgt, dass der Grad der Ableitung f' ungerade ist. Diese besitzt dann eine Nullstelle in R . Dies führt zu einem Widerspruch. ■

Abschließend möchten wir noch das Verhalten von Polynomen für hinreichend große oder kleine Werte untersuchen.

Definition 2.1.24 - Divergenz von Folgen

Eine Folge $(x_n)_{n \in \mathbb{N}} \subseteq R$ heißt *divergent*, falls für alle $c \in R$ mit $c > 0$ ein $k_0 \in \mathbb{N}$ existiert, sodass für alle $k > k_0$ gilt: $x_k > c$. □

Proposition 2.1.25 - Divergenz von Polynomen

Sei $f \in R[X]$ normiert und nicht konstant. Weiterhin sei $(x_n)_{n \in \mathbb{N}} \subseteq R$ divergent. Dann gilt:

- (i) $(f(x_n))_{n \in \mathbb{N}}$ ist divergent.
- (ii) Ist der Grad von f gerade, so ist $(f(-x_n))_{n \in \mathbb{N}}$ divergent.
- (iii) Ist der Grad von f ungerade, so ist $-(f(-x_n))_{n \in \mathbb{N}}$ divergent. □

Beweis. Sei $f = \sum_{i=0}^r a_i X^i$ mit $r > 0$ und $a_r = 1$. Wir setzen

$$a := \max \{ \max \{ |a_i| \mid i = 1, \dots, r-1 \}, 2 \}.$$

Sei $c > a^2(r-1)$. Eine einfache Abschätzung zeigt, dass

$$f(c) \geq c^r - c^{r-1}(r-1)a > c^{r-1}(r-1)a(a-1) > c$$

gilt. Damit folgt die erste Aussage. Die weiteren folgen analog. ■

Korollar 2.1.26 - Vorzeichen und formale Ableitungen

Seien $f \in R[X]$ und $a, b \in R$, $f(a) \cdot f(b) \neq 0$, sodass f' auf $(-\infty, a)$ und auf (b, ∞) nicht verschwindet und ein konstantes Vorzeichen hat. Dann gilt:

- (i) Haben $f(a)$ und $f'((-\infty, a))$ die gleichen Vorzeichen, so hat f eine Nullstelle in $(-\infty, a)$.
- (ii) Haben $f(b)$ und $f'((b, \infty))$ verschiedene Vorzeichen, so hat f eine Nullstelle in (b, ∞) . □

Beweis. Es sei o.B.d.A. f normiert. Ist $f'((-\infty, a)) < 0$, so ist der Grad von f' nach Proposition 2.1.25 ungerade. Also ist der Grad von f gerade. Für genügend kleine Werte $c < 0$ ist $f(c) > 0$. Somit besitzt f nach Korollar 2.1.22 eine Nullstelle im Intervall $(-\infty, a)$. Die weiteren Fälle können auf analoge Weise bewiesen werden. ■

2.2 Das Transferprinzip

Das Transferprinzip von Tarski-Seidenberg liefert die Existenz einer Kombination von Polynomgleichungen in Variablen $Y = Y_1, \dots, Y_n$, die als Entscheider darüber fungiert, wann eine Vorzeichenbedingung an ein gegebenes System von Polynomen in den Variablen X, Y eine Lösung X besitzt. Der Beweis stützt sich auf folgende Konstruktion:

Beweiskonstruktion Sind die Polynome nur von einer einzigen Variablen abhängig, ist es möglich, die gesamte Information über ihre Vorzeichen in einer Matrix, der sogenannten *Signaturabbildung*, zu bündeln. Die Signaturabbildung kann sukzessive auf Signaturabbildungen von Polynomen niederen Grades, die durch Ableiten oder Division der ursprünglichen Polynome entstehen, zurückgeführt werden. Schließlich hängt sie von der einfachsten Signaturabbildung, der konstanter Polynome, ab. Sind die Polynome nun von mehreren Variablen abhängig, können

sie als Polynome in einer Variable mit Koeffizientenfunktionen angesehen werden. Die Signaturabbildung kann in Abhängigkeit von den zusätzlichen Polynomen, die die Koeffizienten darstellen, berechnet werden. Dieser Zusatz ist durch Polynomgleichungen, einer sogenannten *boolschen Polynomkombination*, beschreibbar.

Ab jetzt sei mit R ein reell abgeschlossener Körper bezeichnet.

Notation. Für $a \in R$ definieren wir:

$$\text{sign}(a) := \begin{cases} 0, & \text{falls } a = 0, \\ 1, & \text{falls } a > 0, \\ -1, & \text{falls } a < 0. \end{cases}$$

Seien $f_1, \dots, f_s \in R[X] \setminus \{0\}$ Polynome und $\{x_i \mid i = 1, \dots, z\}$ mit

$$-\infty =: x_0 < x_1 < x_2 < \dots < x_z < x_{z+1} := \infty$$

die Menge aller Nullstellen dieser Polynome in R . Für $k = 0, \dots, z$ und $i = 1, \dots, s$ setzen wir

$$I_k := (x_k, x_{k+1}), \\ \text{sign}(f_i(I_k)) := \text{sign}\left(f_i\left(\frac{x_k + x_{k+1}}{2}\right)\right).$$

Die *Signaturabbildung* $\mathcal{S}(f_1, \dots, f_s) \in \mathcal{M}_{s, 2z+1}(\{0, 1, -1\})$ von f_1, \dots, f_s sei gegeben durch

$$\mathcal{S}(f_1, \dots, f_s) := \begin{pmatrix} \dots & \dots & \dots & \dots & \dots & \dots \\ \text{sign}(f_i(I_0)) & \text{sign}(f_i(x_1)) & \text{sign}(f_i(I_1)) & \dots & \text{sign}(f_i(x_z)) & \text{sign}(f_i(I_z)) \\ \dots & \dots & \dots & \dots & \dots & \dots \end{pmatrix},$$

wobei die i -te Zeile mit dem i -ten Polynom korrespondiert. Die Signaturabbildung vereint das Wissen um die Nullstellen und die Vorzeichen der Polynome in sich.

Es sei $m := \max\{\deg f_i \mid i = 1, \dots, s\}$. Die Anzahl der Nullstellen eines Polynoms in $R[X]$ ist kleiner gleich m . Die disjunkte Vereinigung aller Matrizenräume mit höchstens $2sm + 1$ Spalten sei

$$\mathcal{W}_{s,m} := \bigcup_{l=0, \dots, sm} \mathcal{M}_{s, 2l+1}(\{0, 1, -1\}).$$

Die Signaturabbildung

Lemma 2.2.1 - Lösungen durch die Signaturabbildung

Eine Funktion $\varepsilon : \{1, \dots, s\} \rightarrow \{0, 1, -1\}$ sei gegeben. Dann existiert eine Teilmenge $W(\varepsilon) \subseteq \mathcal{W}_{s,m}$, sodass folgende Aussagen äquivalent sind:

(a) Es existiert ein $x \in R$ mit:

$$\left\{ \begin{array}{l} \text{sign}(f_1(x)) = \varepsilon(1) \\ \text{sign}(f_2(x)) = \varepsilon(2) \\ \vdots \\ \text{sign}(f_s(x)) = \varepsilon(s) \end{array} \right\}.$$

(b) $\mathcal{S}(f_1, \dots, f_s) \in W(\varepsilon)$. □

Beweis. Mit der Wahl

$$W(\varepsilon) := \{A \in \mathcal{W}_{s,m} \mid \text{Es existiert eine Spalte von } A, \text{ die } (\varepsilon(1), \dots, \varepsilon(s)) \text{ gleicht}\}$$

ist die Aussage wahr. ■

Lemma 2.2.2 - Lösungen durch Polynome niederen Grades

Seien $f_1, \dots, f_s \in R[X] \setminus \{0\}$, sodass f_s nicht konstant ist. Dann ist $\mathcal{S}(f_1, \dots, f_s)$ komplett aus der Signaturabbildung

$$\mathcal{S}(f_1, \dots, f_{s-1}, f'_s, g_1, \dots, g_s)$$

rekonstruierbar. Dabei ist f'_s die formale Ableitung von f_s und g_1, \dots, g_s sind die jeweiligen Reste von f_s bei Division durch $f_1, \dots, f_{s-1}, f'_s$. □

Beweis. In R gilt der Zwischenwertsatz, siehe Korollar 2.1.22. Mit Korollar 2.1.23 gilt die Aussage, dass die Ableitung eines Polynoms zwischen zwei verschiedenen Nullstellen an mindestens einer Stelle verschwinden muss. Ebenso besitzen Polynome, deren Ableitung keine Nullstelle besitzt, mindestens eine Nullstelle.

Wir setzen $S := \mathcal{S}(f_1, \dots, f_{s-1}, f'_s, g_1, \dots, g_s)$ und $S' := \mathcal{S}(f_1, \dots, f_s)$. Sind $f_1, \dots, f_{s-1}, f'_s$ konstante Polynome, ist ersichtlich, dass S' aus S rekonstruierbar ist. Ab jetzt besitze mindestens eines dieser Polynome eine Nullstelle. Die Nullstellen der Polynome $f_1, \dots, f_{s-1}, f'_s$ und g_1, \dots, g_s seien gegeben durch

$$-\infty := x_0 < x_1 < x_2 < \dots < x_z < x_{z+1} =: \infty.$$

Die Nullstellen von $f_1, \dots, f_{s-1}, f'_s$ bilden eine Teilmenge:

$$-\infty := x_{i_0} < x_{i_1} < \dots < x_{i_w} < x_{i_{w+1}} =: \infty.$$

Wir konstruieren nun eine Funktion $\Theta : \{1, \dots, w\} \rightarrow \{1, \dots, s\}$.

Für $k \in \{1, \dots, w\}$ gibt es ein $t \in \{1, \dots, s\}$, sodass gilt:

$$\begin{cases} f_t(x_{i_k}) = 0, & \text{falls } t \neq s, \\ f'_s(x_{i_k}) = 0, & \text{falls } t = s. \end{cases}$$

Mit der Wahl $\Theta(k) := t$ gilt nun:

$$f_s(x_{i_k}) = g_{\Theta(k)}(x_{i_k}),$$

da per Konstruktion $f_s = h \cdot f_{\Theta(k)} + g_{\Theta(k)}$, $\Theta(k) \neq s$, beziehungsweise $f_s = h \cdot f'_s + g_s$ für ein Restpolynom h gilt. Ziel ist, die Signaturabbildung $\mathcal{S}(f_1, \dots, f_s)$ zu bestimmen. Wir kennen bereits Einträge, deren Zeilenindizes zu f_1, \dots, f_{s-1} gehören und deren Spaltenindizes mit den Nullstellen von f_1, \dots, f_{s-1} korrespondieren. Die Einträge der letzten Zeile (die zu f_s gehört) und die Spalten, die zu den Nullstellen von f_s gehören, sind noch unbekannt. Sie werden jetzt konstruiert.

Schritt 1: Wo liegen die Nullstellen von f_s ?

Wir behaupten, dass die Existenz einer Nullstelle im Intervall I_k , $k \in \{0, \dots, w+1\}$, nur von S abhängt. Das Polynom f_s besitzt eine Nullstelle im Intervall I_k ...

$$\begin{aligned} \dots \text{für } k \in \{1, \dots, w-1\} &\Leftrightarrow \text{sign}(g_{\Theta(k)}(x_{i_k})) \cdot \text{sign}(g_{\Theta(k+1)}(x_{i_{k+1}})) = -1, \\ \dots \text{für } k = 0 &\Leftrightarrow \text{sign}(f'_s(I_0)) \cdot \text{sign}(g_{\Theta(1)}(x_{i_1})) = 1, \\ \dots \text{für } k = w &\Leftrightarrow \text{sign}(f'_s(I_w)) \cdot \text{sign}(g_{\Theta(w)}(x_{i_w})) = -1. \end{aligned}$$

In einem Intervall I_k hat f_s höchstens eine Nullstelle, da ansonsten f'_s weitere Nullstellen besäße. Die Nullstelle x_{i_k} , $k \in \{1, \dots, w\}$, ist auch eine Nullstelle des Polynoms f_s , falls gilt:

$$0 = g_{\Theta(k)}(x_{i_k}).$$

Damit haben wir die Lage der Nullstellen von f_s bestimmt.

Schritt 2: Konstruktion eines Prototyps der Signaturabbildung S' .

Den Prototyp der Signaturabbildung erhalten wir aus S , indem wir alle Spalten, die nicht zu einer Nullstelle von f_1, \dots, f_{s-1} gehören, streichen und die benachbarten Spalten zu einer Spalte zusammenfassen, sowie alle Zeilen, die nicht zu f_1, \dots, f_{s-1} gehören, streichen.

Falls Nullstellen von f_s existieren, bezeichnen wir diese mit $y_1 < y_2 < \dots < y_l$. In diesem Fall erweitern wir die Signaturabbildung. Das Vorgehen wird nun erläutert.

Gilt $y_{\tilde{k}} \in I_k$ für ein $k \in \{0, \dots, w\}$ und ein $\tilde{k} \in \{1, \dots, l\}$, fällt die Spalte für das Intervall I_k weg. Zwischen der zu x_k und der zu x_{k+1} gehörigen Spalte werden drei neue Spalten erzeugt: Jeweils eine für das Intervall $(x_k, y_{\tilde{k}})$, den Punkt $y_{\tilde{k}}$ und das Intervall $(y_{\tilde{k}}, x_{k+1})$.

Schritt 3: Welche Vorzeichen besitzt f_s ?

Die Lage der Nullstellen von f_s in der Signaturabbildung sind bekannt. Alle weiteren Werte werden durch $f'_s(I_0)$ bestimmt:

$$\begin{aligned} f'_s(I_0) < 0 &\Leftrightarrow S'(s, 1) = 1, \\ f'_s(I_0) > 0 &\Leftrightarrow S'(s, 1) = -1, \\ f'_s(I_0) = 0 &\Leftrightarrow S'(s, 1) = 0. \end{aligned}$$

Die restlichen Werte werden alternierend ergänzt. Damit ist die letzte Zeile der Matrix S' bestimmt. Nun gilt es, die Einträge der Spalten zu ermitteln.

Schritt 4: Welche Vorzeichen besitzen f_1, \dots, f_{s-1} an den Nullstellen von f_s ?

Sei $\tilde{k} \in \{1, \dots, l\}$ mit $y_{\tilde{k}} \in I_k$ für ein $k \in \{0, \dots, w\}$. Dann gilt für $m \in \{1, \dots, s-1\}$:

$$\begin{aligned} &\text{sign}(f_m(y_{\tilde{k}})) \\ &= \text{sign}(f_m(y_{\tilde{k}}, x_{k+1})) \\ &= \text{sign}(f_m(x_k, y_{\tilde{k}})) \\ &= \text{sign}(f_m(I_k)) \end{aligned}$$

Jetzt werden nach dem gleichen Prinzip alle Spalten entfernt, die nur zu Nullstellen von f'_s gehören.

Damit ist S' aus S rekonstruierbar. ■

Korollar 2.2.3 - Rekonstruktion der Signaturabbildung

Es existiert eine Abbildung $\varphi : \mathcal{W}_{2s,m} \rightarrow \mathcal{W}_{s,m}$, sodass für alle $f_1, \dots, f_s \in R[X]$, wobei f_1, \dots, f_s nicht Null sind und f_s nicht konstant ist, gilt:

$$\mathcal{S}(f_1, \dots, f_s) = \varphi(\mathcal{S}(f_1, \dots, f_{s-1}, f'_s, g_1, \dots, g_s))$$

Die Signaturabbildung kann also auf eine von Polynomen niederen Grades zurückgeführt werden. □

Beweis. Nach Lemma 2.2.2 ist $\mathcal{S}(f_1, \dots, f_s)$ aus $\mathcal{S}(f_1, \dots, f_{s-1}, f'_s, g_1, \dots, g_s)$ rekonstruierbar. Weiterhin können die Matrizen, die nicht als Signaturabbildung geschrieben werden können, auf eine beliebige Matrix abgebildet werden. Also existiert die Abbildung und ist insbesondere wohldefiniert. ■

Verifizierungen für Signaturabbildungen

Definition 2.2.4 - Boolesche Polynomkombination

Eine *boolesche Polynomkombination* $\mathcal{B}(X)$ in den Variablen X und mit Koeffizienten in R ist eine endliche Kombination von Polynomgleichungen und Polynomungleichungen

$$\mathcal{B}(X) := \left\{ \begin{array}{l} p_1(X) \star 0 \\ p_2(X) \star 0 \\ \vdots \\ p_k(X) \star 0 \end{array} \right\}$$

mit $p_1, \dots, p_k \in R[X_1, \dots, X_n]$ und $\star \in \{=, <, >, \leq, \geq, \neq\}$ (jeweils), wobei die Polynome durch Operatoren aus der Menge $\{\wedge, \vee\}$ miteinander verknüpft sind. \square

Proposition 2.2.5 - Die Signaturabbildung als Polynom

Es seien $f_1, \dots, f_s \in \mathbb{Z}[X, Y_1, \dots, Y_n]$ gegeben. Wir schreiben für $i = 1, \dots, s$:

$$f_i(X, Y) = h_{i, m_i}(Y)X^{m_i} + \dots + h_{i, 0}(Y),$$

wobei $h_{i, m_i} \in \mathbb{Z}[Y_1, \dots, Y_n]$ nicht konstant Null ist. Es sei $m := \max\{m_i \mid i = 1, \dots, s\}$ und $W \subseteq \mathcal{W}_{s, m}$. Dann existiert eine boolesche Polynomkombination $\mathcal{B}(Y)$ mit Koeffizienten in \mathbb{Z} , sodass für jeden reell abgeschlossenen Körper R und $y \in R^n$ äquivalent ist:

- (a) Es ist $\mathcal{S}(f_1(X, y), \dots, f_s(X, y)) \in W$.
- (b) Die Aussage $\mathcal{B}(y)$ ist wahr. \square

Beweis. Mit $\mathcal{F}(\mathbb{N}_0) := \{(a_0, \dots, a_k) \mid a_0, \dots, a_k \in \mathbb{N}_0, k \in \mathbb{N}\}$ sei der Raum der endlichen Folgen mit Einträgen aus den natürlichen Zahlen und der Null bezeichnet. Die Anzahl der Einträge einer Folge mit Wert $s \in \mathbb{N}_0$ bezeichnet $\#s$. Auf $\mathcal{F}(\mathbb{N}_0)$ wird eine Relation \triangleleft eingeführt:

$$a := (a_0, \dots, a_k) \triangleleft b := (b_0, \dots, b_{\bar{k}}),$$

genau dann wenn entweder $a = b$ ist oder ein $r \in \mathbb{N}_0$ existiert, sodass für alle $s \in \mathbb{N}_0$ mit $r < s$ gilt:

- (i) Die Anzahl $\#r$ ist in a (echt) kleiner als die Anzahl $\#r$ in b .
- (ii) Die Anzahl $\#s$ ist in a gleich der Anzahl $\#s$ in b .

Behauptung: Diese Relation ist eine Ordnungsrelation mit den folgenden Eigenschaften:

- (i) Die Ordnung \triangleleft ist total,
- (ii) Für $c \in \mathcal{F}(\mathbb{N}_0)$ und $a \triangleleft b$ gilt: $(a + c) \triangleleft (b + c)$,
- (iii) Jede nichtleere Teilmenge von $\mathcal{F}(\mathbb{N}_0)$ besitzt ein kleinstes Element, das heißt, die Relation ist eine Wohlordnung.

Beweis: Dass die Relation eine Ordnungsrelation ist, kann leicht nachgerechnet werden.

(i): Wenn a und b zwei verschiedene Elemente aus $\mathcal{F}(\mathbb{N}_0)$ sind, können wir r als das größte in a und b vorkommende Element, das in a und b nicht gleich oft vorkommt, wählen. Damit ist die Ordnung total.

(ii): Die Ordnung bleibt unter Summation erhalten.

(iii): Wir identifizieren ein Element $a \in \mathcal{F}(\mathbb{N}_0)$ mit der finiten Folge $\alpha := (\alpha_i)_{i \in \mathbb{N}_0}$, wobei gilt: $\alpha_i = \#i$. Wird b mit β identifiziert, dann ist $a \triangleleft b$, $a \neq b$, genau dann wenn es ein $r \in \mathbb{N}_0$ gibt, sodass $\alpha_r < \beta_r$ und $\alpha_{r+1} = \beta_{r+1} = \alpha_{r+2} = \beta_{r+2} = \dots$ gelten. Wir sehen so leicht ein, dass es nur endlich viele Elemente gibt, die kleiner als ein gegebenes Element sind. \diamond

Nun identifizieren wir f_1, \dots, f_s mit der endlichen Folge $(m_1, \dots, m_s) \in \mathcal{F}(\mathbb{N}_0)$.

Fall 1: $m = 0$.

Dann hängt $\mathcal{S}(f_1, \dots, f_s)$ nur von $h_{1,0}(Y), \dots, h_{s,0}(Y)$ ab.

Fall 2: $m > 0$.

Es sei o.B.d.A. $m_s = m$. Das Urbild von W unter der Abbildung φ , die in Korollar 2.2.3 eingeführt wird, sei bezeichnet mit

$$W' := \varphi^{-1}(W) \subseteq W_{2s,m}.$$

Für $y \in R^n$ gilt die Ungleichung

$$\begin{aligned} & (\deg(f_1(X, y)), \dots, \deg(f'_s(X, y)), \deg(g_1(X, y)), \dots, \deg(g_s(X, y))) \\ & \triangleleft (\deg(f_1(X, y)), \dots, \deg(f_s(X, y))) \end{aligned}$$

und ist echt. Das Ableiten des letzten Polynoms und die anschließende Polynomdivision vermindern den Grad der Polynome bezüglich der Ordnung \triangleleft . Durch sukzessives Vermindern erhalten wir eine Folge von konstanten Polynomen c_1, \dots, c_r . Bilden wir gleichzeitig iterierte Mengen $\varphi^{-1}(W')$, $\varphi^{-1}(\varphi^{-1}(W'))$, ..., so beschreibt die letzte iterierte Menge eine Vorzeichenbedingung an die Signaturabbildung der Konstanten c_1, \dots, c_r . Es existiert also eine Teilmenge $W_0 \subseteq W_{r,m}$, sodass gilt:

$$\mathcal{S}(c_1, \dots, c_r) \in W_0 \Leftrightarrow \mathcal{S}(f_1, \dots, f_s) \in W,$$

wobei $\mathcal{S}(c_1, \dots, c_r)$ polynomial von y abhängt. Die boolsche Polynomkombination ergibt sich aus der Konstruktion von W_0 . Sie besteht aus den möglichen Signaturen der Ableitungen. \blacksquare

Das Transferprinzip von Tarski-Seidenberg

Mit den Vorbereitungen schließen wir:

Satz 2.2.6 - Transferprinzip

Sei $\varepsilon : \{1, \dots, s\} \rightarrow \{0, 1, -1\}$ eine Funktion. Dann gilt:

- (i) Sind $f_1, \dots, f_s \in \mathbb{Z}[X, Y_1, \dots, Y_n]$, dann existiert eine boolsche Polynomkombination $\mathcal{B}(Y)$ mit Koeffizienten in \mathbb{Z} , sodass für jeden reell abgeschlossenen Körper R und $y \in R^n$ äquivalent ist:

- (a) Es existiert ein $x \in R$ mit:

$$\left(\begin{array}{l} \text{sign}(f_1(x, y)) = \varepsilon(1) \\ \text{sign}(f_2(x, y)) = \varepsilon(2) \\ \vdots \\ \text{sign}(f_s(x, y)) = \varepsilon(s) \end{array} \right).$$

- (b) Die Aussage $\mathcal{B}(y)$ ist wahr.

- (iii) Ist F ein angeordneter Körper und $f_1, \dots, f_s \in F[X, Y_1, \dots, Y_n]$, dann existiert eine boolsche Polynomkombination $\mathcal{B}(Y)$ mit Koeffizienten in F , sodass für jeden reell abgeschlossenen Körper R , der F enthält, und $y \in R^n$ äquivalent ist:

- (a) Es existiert ein $x \in R$ mit:

$$\left(\begin{array}{l} \text{sign}(f_1(x, y)) = \varepsilon(1) \\ \text{sign}(f_2(x, y)) = \varepsilon(2) \\ \vdots \\ \text{sign}(f_s(x, y)) = \varepsilon(s) \end{array} \right).$$

- (b) Die Aussage $\mathcal{B}(y)$ ist wahr. □

Beweis. (i): Aus Lemma 2.2.1 und Proposition 2.2.5 folgt die Aussage unmittelbar. (iii): Dazu wenden wir (i) auf $G_i(X, Y, Z^i) := f_i(X, Y)$ an, wobei G_i Koeffizienten in \mathbb{Z} hat und $Z^i := (Z_1^i, \dots, Z_{m_i}^i)$ Variablen sind, die die Koeffizienten von f_i in F repräsentieren, und ergänzen $\mathcal{B}(y)$ um die Restriktionen an Z^i . ■

Das Transferprinzip 2.2.6 gilt auch im geeigneten Sinne für $n = 0$. Dies sehen wir so: Eine Vorzeichenbedingung an Polynome $f_1, \dots, f_s \in R[X]$ kann in eine Vorzeichenbedingung an die Polynome $f_1 \cdot Y, \dots, f_s \cdot Y$ für eine Variable Y umformuliert und $Y = 1$ gesetzt werden.

Jetzt kommen wir zum einem Korollar, welches für den Beweis mehrerer Aussagen im nächsten Abschnitt von Bedeutung sein wird.

Korollar 2.2.7 - Gültigkeit von Gleichungen auf Erweiterungen

Es sei R_1 eine reell abgeschlossene Erweiterung von R , $X := (X_1, \dots, X_n)$ Variablen und $\mathcal{B}(X)$ eine boolsche Polynomkombination mit Koeffizienten in R . Dann sind äquivalent:

- (a) Es existiert ein $y \in R_1^n$, sodass $\mathcal{B}(y)$ wahr ist.
- (b) Es existiert ein $x \in R^n$, sodass $\mathcal{B}(x)$ wahr ist. □

Beweis. Die Implikation $(b) \Rightarrow (a)$ ist klar.

Die Implikation $(a) \Rightarrow (b)$ zeigen wir per Induktion über n .

Induktionsanfang: Im Fall $n = 0$ gilt die Äquivalenz.

Induktionsschritt: Sei nun $n > 0$. Die Aussage:

„Es existiert ein $y \in R_1^n$, sodass $\mathcal{B}(y) = \mathcal{B}(y_1, \dots, y_{n-1}, y_n)$ wahr ist.“

ist äquivalent zu:

„Es existieren $\bar{y} := (y_1, \dots, y_{n-1}) \in R_1^{n-1}$ und $y_n \in R_1$, sodass $\mathcal{B}(\bar{y}, y_n)$ wahr ist.“

Es ist möglich, $\mathcal{B}(X)$ in eine Bedingung an die Vorzeichen der Auswertung von Polynomen in $R[Y_1, \dots, Y_{n-1}, X]$ umzuschreiben. Nach dem Transferprinzip 2.2.6 gilt die folgende Aussage: Es existiert eine boolsche Polynomkombination $\mathcal{C}(Y_1, \dots, Y_{n-1})$ mit Koeffizienten in R , sodass für eine reell abgeschlossene Erweiterung F von R und $\bar{z} \in F^{n-1}$ die beiden folgenden Aussagen äquivalent sind:

„Es existiert ein $z \in F$, sodass $\mathcal{B}(\bar{z}, z)$ wahr ist.“

„Die Aussage $\mathcal{C}(\bar{z})$ ist wahr.“

Sei nun $y \in R_1^n$, sodass $\mathcal{B}(y)$ wahr ist. Mit der Wahl $F := R_1$ und aus den Annahmen folgt, dass $\mathcal{C}(\bar{y})$ wahr ist. Nach der Induktionsvoraussetzung existiert ein $\bar{x} \in R^{n-1}$, sodass $\mathcal{C}(\bar{x})$ wahr ist. Mit der Wahl $F := R$ folgt schließlich, dass ein $x \in R$ existiert, sodass $\mathcal{B}(\bar{x}, x)$ wahr ist. Damit ist die Implikation bewiesen. ■

2.3 Positivstellensätze und der reelle Nullstellensatz

Zunächst führen wir *semialgebraische Mengen* ein. Danach geben wir den reellen Nullstellensatz an. Davon unabhängig widmen wir uns im Folgenden ausführlich der Frage nach der Charakterisierung von Positivstellenmengen in einigen Positivstellensätzen.

Semialgebraische Mengen, Positivstellenmengen und reelle algebraische Varietäten

Definition 2.3.1 - Semialgebraische Mengen

Sei $S \subseteq R^n$ eine Menge, sodass

$$S = \{x \in R^n \mid p_1(x) \star 0, p_2(x) \star 0, \dots, p_k(x) \star 0\}$$

mit $p_i \in R[X_1, \dots, X_n]$, $i = 1, \dots, k$, und $\star \in \{=, <, >, \leq, \geq, \neq\}$ (jeweils). Dann heißt S eine *basissemialgebraische Menge*. Eine endliche Vereinigung von basissemialgebraischen Mengen heißt *semialgebraische Menge*. \square

Mengen der Form

$$\{x \in R^n \mid \text{Die Aussage } \mathcal{B}(x) \text{ ist wahr}\}$$

für boolesche Polynomkombinationen $\mathcal{B}(X_1, \dots, X_n)$ mit Koeffizienten in R sind semialgebraisch. Umgekehrt kann jede semialgebraische Menge so dargestellt werden.

Die Menge aller semialgebraischen Mengen in R^n ist unter endlichen Vereinigungen, Durchschnitten und Komplementbildungen stabil. Ein Hinweis, dass dies nicht für beliebige Durchschnitte zu erwarten ist, gibt folgendes Beispiel:

$$\{(x, y) \in \mathbb{R}_0^+ \times \mathbb{R}_0^+ \mid y - \exp(x) \geq 0\} = \bigcap_{p \in \mathcal{T}} \{z \in \mathbb{R}_0^+ \times \mathbb{R}_0^+ \mid p(z) \geq 0\},$$

wobei \mathcal{T} die Menge der affin-linearen Polynome, die tangential an und positiv über dem Graphen der Exponentialfunktion \exp sind, bezeichnet.

Ein direktes Resultat aus dem Transferprinzip von Tarski-Seidenberg ist die auch unter dem Namen *Satz von Tarski-Seidenberg* bekannte Aussage über projizierte semialgebraische Mengen:

Satz 2.3.2 - Projektionen von semialgebraischen Mengen

Sei $S \subseteq R^{n+k}$ eine semialgebraische Menge und

$$\pi : R^{n+k} \rightarrow R^n, (x, y) \mapsto x$$

die Projektion auf die ersten n Koordinaten. Dann ist auch $\pi(S)$ semialgebraisch. \square

Beweis. Es sei zunächst $k = 1$. Die Menge S kann als endliche Vereinigung von Mengen der Form

$$S_0 := \{(x, y) \in R^{n+1} \mid p_1(x, y) \star 0, p_2(x, y) \star 0, \dots, p_r(x, y) \star 0\}$$

mit $p_i \in R[X_1, \dots, X_n, Y]$, $i = 1, \dots, r$, und $\star \in \{=, <, >\}$ (jeweils) geschrieben werden. Jede der Bedingungen $p_i(x, y) \star 0$, $i = 1, \dots, r$, kann in eine Vorzeichenbedingung umformuliert werden. Nach Satz 2.2.6 existiert also eine Boolesche Polynomkombination $\mathcal{C}_0(X_1, \dots, X_n)$ mit Koeffizienten in R , sodass gilt:

$$x \in \pi(S_0) \Leftrightarrow x \in \{z \in R^n \mid \text{Die Aussage } \mathcal{C}_0(z) \text{ ist wahr}\}.$$

Damit ist $\pi(S)$ als endliche Vereinigung semialgebraischer Mengen semialgebraisch. Die Aussage folgt für den allgemeinen Fall $k \geq 1$ induktiv. \blacksquare

Nun möchten wir speziellere Formen semialgebraischer Mengen definieren und im Folgenden genauer untersuchen.

Definition 2.3.3 - Spezielle semialgebraische Mengen

Seien $f_1, \dots, f_s \in R[X_1, \dots, X_n]$ Polynome.

(i) Die *Verschwindemenge* des Ideals $I := \langle f_1, \dots, f_s \rangle$ sei definiert durch

$$\mathcal{Z}(I) := \{x \in R^n \mid f_1(x) = 0, \dots, f_s(x) = 0\}.$$

(ii) Die *Positivstellenmenge* des Kegels $P := \mathcal{K}[f_1, \dots, f_s]$ sei definiert durch

$$\mathcal{W}(P) := \{x \in R^n \mid f_1(x) \geq 0, \dots, f_s(x) \geq 0\}.$$

(iii) Die *Nichtnullmenge* des Monoids $M := \mathcal{M}[f_1, \dots, f_s]$ sei definiert durch

$$\mathcal{N}(M) := \{x \in R^n \mid f_1(x) \neq 0, \dots, f_s(x) \neq 0\}. \quad \square$$

Nach dem *Hilbertschen Basissatz*, siehe [Hul], ist jedes Ideal endlich erzeugt, daher ist es möglich, Verschwindemengen von beliebigen Idealen in $R[X_1, \dots, X_n]$ zu betrachten. Wir bezeichnen eine Menge $V \subseteq R^n$ als *reelle algebraische Varietät* oder als *algebraisch*, falls sie Verschwindemenge eines Ideals ist.

Nichtnullmengen können als Komplemente ausgedrückt werden: $\mathcal{N}(M) = \mathcal{Z}(J)^c$ für das Ideal $J := \langle f_1 \cdot \dots \cdot f_s \rangle$. Verschwindemengen sind Positivstellenmengen: für den Kegel $Q := \mathcal{K}[\pm f_1, \dots, \pm f_s]$ gilt $\mathcal{Z}(I) = \mathcal{W}(Q)$.

Im Fall $R = \mathbb{R}$ sind Verschwinde- und Positivstellenmengen abgeschlossen und Nichtnullmengen offen. Im Folgenden werden wir Aussagen über die Schnitte solcher Mengen aus abstrakteren Aussagen herleiten.

Der formale Positivstellensatz

Lemma 2.3.4 - Formaler Positivstellensatz

Seien $(a_j)_{j \in J}$, $(b_k)_{k \in K}$ und $(c_l)_{l \in L}$ Familien von Elementen eines kommutativen Rings A . Wir definieren $P := \mathcal{K}[(a_j)_{j \in J}]$, $M := \mathcal{M}[(b_k)_{k \in K}]$ und $I := \langle c_l \mid l \in L \rangle$. Dann sind äquivalent:

- (a) Es gibt keinen Primkegel Q von A , sodass
 - Für alle $j \in J$ gilt: $a_j \in Q$,
 - Für alle $k \in K$ gilt: $b_k \notin \text{supp}(Q)$,
 - Für alle $l \in L$ gilt: $c_l \in \text{supp}(Q)$.
- (b) Es gibt keinen Ringhomomorphismus $f : A \rightarrow F$ in einen reell abgeschlossenen Körper F , sodass
 - Für alle $j \in J$ gilt: $f(a_j) \geq 0$,
 - Für alle $k \in K$ gilt: $f(b_k) \neq 0$,
 - Für alle $l \in L$ gilt: $f(c_l) = 0$.
- (c) Es existieren Elemente $a \in P$, $b \in M$, $c \in I$ mit $a + b^2 + c = 0$. □

Beweis. (a) \Leftrightarrow (b): Korollar 2.1.14.

(c) \Rightarrow (b): Angenommen, es gäbe einen solchen Homomorphismus f , dann gilt

$$f(a + b^2 + c) = f(a) + f(b)^2 + f(c) > 0,$$

da $f(a) \geq 0$, $f(b)^2 > 0$ und $f(c) = 0$. Dies ist ein Widerspruch zur Voraussetzung.

(b) \Rightarrow (c): Falls ein Element $b \in M \cap I$ existiert, wählen wir $a = 0$ und $c = -b^2$ und die Aussage ist damit bewiesen. Es sei nun im Folgenden $M \cap I = \emptyset$. Der Beweis gliedert sich in zwei Schritte.

Schritt 1: Konstruktion eines Rings A_2 , auf den Satz 2.1.20 anwendbar ist. Der kanonische Homomorphismus des Rings A in den Quotienten A/I sei mit π bezeichnet. Die Menge $\pi(M) =: \overline{M}$ ist multiplikativ mit $0 \notin \overline{M}$. Zunächst lokalisieren wir den Ring A/I an \overline{M} . Dazu definieren wir auf dem Kreuzprodukt $(A/I) \times \overline{M}$ eine Äquivalenzrelation $\sim_{\overline{M}}$ mit

$$(a, b) \sim_{\overline{M}} (a', b') \Leftrightarrow \text{Es existiert ein } m \in M \text{ mit } m \cdot (ab' - ba') \in I.$$

Die Lokalisierung $(A/I) \times \overline{M} / \sim_{\overline{M}} =: A_1$ wird mit den üblichen Bruchrechnungsregeln zu einem Ring, in dem „Kürzen“ und „Erweitern“ von Brüchen möglich ist. Nun adjungieren wir eine Familie $(T_j)_{j \in J}$ von Unbekannten und betrachten den Ring $A_1[(T_j)_{j \in J}]$. Den Quotienten von $A_1[(T_j)_{j \in J}]$ nach dem Ideal

$$H := \left\langle (T_j^2 - (\pi(a_j), \pi(1)))_{j \in J} \right\rangle$$

bezeichnen wir mit A_2 . Wir definieren ι als Komposition der kanonischen Homomorphismen:

$$\begin{array}{ccccccc} \iota: & A & \rightarrow & A/I & \rightarrow & A_1 & \rightarrow & A_2 \\ & a & \mapsto & \pi(a) & \mapsto & (\pi(a), \pi(1)) & \mapsto & (\pi(a), \pi(1)) + H \end{array}$$

Angenommen, es gibt einen Homomorphismus $g: A_2 \rightarrow F$ in einen reell abgeschlossenen Körper F , dann ist auch $f := g \circ \iota: A \rightarrow F$ ein solcher Homomorphismus und es gelten folgende Aussagen:

Behauptung: Es ist $f(P) \geq 0$.

Beweis: Ein Element $r \in P$ besitzt die Gestalt $r = r_0 + \sum_{i=1}^s r_i m_i$ mit $r_0, \dots, r_s \in \Sigma A^2$ und $m_1, \dots, m_s \in \mathcal{M}[(a_j)_{j \in J}]$. Deshalb wird es auf einen nicht-negativen Wert abgebildet:

$$\begin{aligned} f(r) &= f\left(r_0 + \sum_{i=1}^s r_i m_i\right) \\ &= g\left((\pi(r_0), \pi(1)) + \sum_{i=1}^s (\pi(r_i m_i), \pi(1)) + H\right) \\ &= g((\pi(r_0), \pi(1)) + H) + g\left(\sum_{i=1}^s (\pi(r_i) \pi(m_i), \pi(1)) + H\right) \\ &\geq 0. \end{aligned}$$

Der linke Ausdruck ist eine Summe von Quadraten, da dies bereits für r_0 gilt. Der rechte Ausdruck auch, da r_i eine Summe von Quadraten ist und es gilt: $\pi(a_j) \equiv T_j^2$ in A_2 für $i = 1, \dots, s$. \diamond

Behauptung: Es ist $f(M) \neq 0$ und $f(I) = 0$.

Beweis: Diese Aussagen gelten, da $M \cap I = \emptyset$ und $\iota(I) = 0$. \diamond

Insbesondere sind die Bedingungen aus (b) erfüllt, was nach Voraussetzung aber nicht möglich ist. Es existiert also kein solcher Homomorphismus g .

Nach Satz 2.1.20 gilt: $-1 \in \sum A_2$, also existieren Elemente $\delta_1, \dots, \delta_n \in A_2$, die die Gleichung $-1 = \delta_1^2 + \dots + \delta_n^2$ erfüllen.

Schritt 2: Umformulierung der eben erhaltenen Gleichung.

Die Variablen $T_j, j \in J$, bilden ein Erzeugendensystem des A_1 -Moduls A_2 . Monome in diesen Variablen haben die Gestalt $T_B := \prod_{j \in J} T_j^{B(j)} + H$, wobei $B : J \rightarrow \mathbb{N}_0$ eine Funktion ist mit $B(j) = 0$ für fast alle $j \in J$. Die Menge solcher Monome sei bezeichnet mit \mathcal{B} . Für $B = 0$ ist T_0 konstant. Wir können also δ_i für $i = 1, \dots, n$ in eine Monomdarstellung entwickeln und erhalten

$$\delta_i = \sum_{B \in \mathcal{B}} \gamma_{i,B} T_B$$

mit $\gamma_{i,B} \in A_1$. Es existieren $a_{i,B} \in \pi(A)$ und $m_{i,B} \in \pi(M)$, sodass $\gamma_{i,B} = (a_{i,B}, m_{i,B})$. Also ist

$$\begin{aligned} -1 &= \sum_{\substack{i \in \{1, \dots, n\} \\ B \in \mathcal{B}}} \gamma_{i,B}^2 T_B^2 \\ &= \sum_{i,B} \gamma_{i,B}^2 \prod_{j \in J} (\pi(a_j), \pi(1))^{B(j)} \\ &= \sum_{i,B} (a_{i,B}^2, m_{i,B}^2) \left(\prod_{j \in J} \pi(a_j)^{B(j)}, \pi(1) \right) \end{aligned}$$

und es folgt:

$$0 = \sum_{i,B} \underbrace{\left(\prod_{j \in J} \pi(a_j)^{B(j)} a_{i,B}^2, m_{i,B}^2 \right)}_{\in P} + 1.$$

Multiplizieren wir beide Seiten der Gleichung mit dem kleinsten gemeinsamen Vielfachen der Nenner, also mit einem Produkt solcher Elemente: $(m_{i,B}^2, \pi(1))$, erhalten wir eine Gleichung der Form

$$0 = (a + I) + (b^2 + I)$$

in A/I mit $a \in P$ und $b \in M$. Damit ist $a + b^2 \in I$, das heißt, es existiert ein $c \in I$ mit $a + b^2 + c = 0$. \blacksquare

Bemerkung 2.3.5 Die ersten beiden Aussagen des formalen Positivstellensatzes können auch durch die beiden folgenden Aussagen

(a') Es gibt keinen Primkegel Q von A , sodass

- $P \subseteq Q$,
- $M \cap \text{supp}(Q) = \emptyset$,
- $I \subseteq \text{supp}(Q)$.

(b') Es gibt keinen Ringhomomorphismus $f : A \rightarrow F$ in einen reell abgeschlossenen Körper F , sodass

- $f(P) \geq 0$,
- $f(M) \neq 0$,
- $f(I) = 0$.

ersetzt werden. □

Konkrete Positivstellensätze für Polynome

Satz 2.3.6 - Allgemeiner Positivstellensatz

Es seien $(f_j)_{j \in J}$, $(g_k)_{k \in K}$ und $(h_l)_{l \in L}$ endliche Familien in $R[X_1, \dots, X_n]$. Wir definieren $P := \mathcal{K}[(f_j)_{j \in J}]$, $M := \mathcal{M}[(g_k)_{k \in K}]$ und $I := \langle h_l \mid l \in L \rangle$. Dann sind äquivalent:

- (a) Die Menge $\mathcal{W}(P) \cap \mathcal{N}(M) \cap \mathcal{Z}(I)$ ist leer.
- (b) Es existieren Elemente $f \in P$, $g \in M$, $h \in I$ mit $f + g^2 + h = 0$. □

Beweis. (b) \Rightarrow (a): Die Menge unter (a) hat die folgende Gestalt:

$$\{x \in R^n \mid f_j(x) \geq 0, g_k(x) \neq 0, h_l(x) = 0 \text{ für alle } j \in J, k \in K, l \in L\}.$$

An dieser Gestalt wird deutlich, dass es unter Voraussetzung (b) kein $x \in F^n$ geben kann, welches in der Menge enthalten ist.

(a) \Rightarrow (b): Nach Korollar 2.2.7 ist die Gleichung

$$\{x \in R^n \mid f_j(x) \geq 0, g_k(x) \neq 0, h_l(x) = 0 \text{ für alle } j \in J, k \in K, l \in L\} \neq \emptyset$$

äquivalent zur Aussage:

„Es existiert eine reell abgeschlossene Erweiterung F von R und ein $y \in F^n$ mit $f_j(y) \geq 0, g_k(y) \neq 0, h_l(y) = 0$ für alle $j \in J, k \in K, l \in L$ “.

Durch die Bilder der Variablen X_1, \dots, X_n wird ein Homomorphismus vom Polynomring $R[X_1, \dots, X_n]$ in den Körper F eindeutig festgelegt. Also ist die obige Aussage äquivalent zu:

„Es existiert ein Homomorphismus $\varphi : R[X_1, \dots, X_n] \rightarrow F$
 in eine reell abgeschlossene Erweiterung F von R ,
 sodass $\varphi(f_j) \geq 0, \varphi(g_k) \neq 0, \varphi(h_l) = 0$
 für alle $j \in J, k \in K, l \in L$ gilt“,

da solche Homomorphismen durch Auswertungen an Elementen aus F^n gegeben sind. Lemma 2.3.4 zeigt, dass die Verneinung der letzten Bedingung äquivalent zur Voraussetzung (b) ist. ■

Korollar 2.3.7 - Konkreter Positivstellensatz

Sei I ein Ideal in $R[X_1, \dots, X_n]$. Weiterhin seien Polynome $g_1, \dots, g_s \in R[X_1, \dots, X_n]$ gegeben. Es sei $P := \mathcal{K}[g_1, \dots, g_s]$, $W := \mathcal{Z}(I) \cap \mathcal{W}(P)$ und $P' := P/I$. Dann gilt für ein Polynom $f \in R[X_1, \dots, X_n]$:

- (i) $f(W) \geq 0 \Leftrightarrow$ Es existieren $m \in \mathbb{N}_0$ und $g, h \in P'$ mit $fg = f^{2m} + h$,
- (ii) $f(W) > 0 \Leftrightarrow$ Es existieren $g, h \in P'$ mit $fg = 1 + h$,
- (iii) $f(W) = 0 \Leftrightarrow$ Es existieren $m \in \mathbb{N}_0$ und $g \in P'$ mit $f^{2m} + g = 0$. □

Beweis. Es gibt u_1, \dots, u_k in $R[X_1, \dots, X_n]$ mit $I = \langle u_1, \dots, u_k \rangle$. Es ist

$$W = \{x \in V \mid g_1(x) \geq 0, \dots, g_s(x) \geq 0\}.$$

Mit f sei auch ein Repräsentant von $f + I \in R[X_1, \dots, X_n]/I$ bezeichnet.

(i): Wir definieren

$$S := \{x \in R^n \mid g_i(x) \geq 0, -f(x) \geq 0, f(x) \neq 0, u_l(x) = 0; i = 1, \dots, s; l = 1, \dots, k\}.$$

Die Menge S ist genau dann leer, wenn $f(W) \geq 0$ gilt. Mit Satz 2.3.6 existieren in diesem Fall Polynome $\tilde{f} \in \mathcal{K}[g_1, \dots, g_s, -f]$, $\tilde{g} \in \{f^r \mid r \in \mathbb{N}_0\}$ und $\tilde{h} \in I$ mit

$$\tilde{f} + \tilde{g}^2 + \tilde{h} = 0.$$

Das Polynom \tilde{f} besitzt die Gestalt $\tilde{f} = h + \sum_{i=1}^r g_i \cdot (-f)^i$ mit $h, g_i \in P$. Ist der Exponent i gerade, führen wir den Summanden dem ersten Summanden zu, da er im Kegel ist. Ist er ungerade, multiplizieren wir den ersten Faktor mit $(-f)^{i-1}$ und erhalten so eine Quadratsumme, die im Kegel liegt. Wir können daher o.B.d.A. annehmen, dass $\tilde{f} = h - gf$ mit $g \in P$ ist. Damit ist

$$\tilde{f} + \tilde{g}^2 + \tilde{h} = h - gf + f^{2m} + \tilde{h} = 0.$$

(ii): Wir definieren

$$S := \{x \in R^n \mid g_i(x) \geq 0, -f(x) \geq 0, u_l(x) = 0 \text{ für alle } l = 1, \dots, k; i = 1, \dots, s\}.$$

Hier sei nun \tilde{f} wie oben und $\tilde{g} = 1$. Der Rest folgt analog.

(iii): Definieren wir

$$S := \{x \in R^n \mid g_i(x) \geq 0, f(x) \neq 0, u_l(x) = 0 \text{ für alle } l = 1, \dots, k; i = 1, \dots, s\},$$

so folgt der Rest analog mit $\tilde{f} \in P$ und $\tilde{g} \in \{f^r \mid r \in \mathbb{N}_0\}$. ■

Der reelle Nullstellensatz

In diesem Unterabschnitt bringen wir ein wichtiges Resultat der reellen algebraischen Geometrie an. Mit dem reellen Nullstellensatz charakterisieren wir die Polynome, die auf einer Varietät verschwinden.

Definition 2.3.8 - Verschwindeideal

Sei $V \subseteq R^n$ eine Menge. Das Ideal

$$\mathcal{J}(V) := \{f \in R[X_1, \dots, X_n] \mid f(x) = 0 \text{ für alle } x \in V\}$$

heißt *Verschwindeideal* von V . □

Definition 2.3.9 - Reelles Radikal

Für ein Ideal $I \subseteq A$ sei die Menge

$$\sqrt[R]{I} := \{a \in A \mid a^{2m} + \sum_{i=1}^r b_i^2 \in I \text{ für ein } m \in \mathbb{N} \text{ und } b_1, \dots, b_r \in A\}$$

bezeichnet als das *reelle Radikal* von I . □

Satz 2.3.10 - Reeller Nullstellensatz

Für ein Ideal $I \subseteq R[X_1, \dots, X_n]$ gilt:

$$\mathcal{J}(\mathcal{Z}(I)) = \sqrt[R]{I}.$$

Insbesondere sind äquivalent:

- (a) $\mathcal{J}(\mathcal{Z}(I)) = I$.
- (b) I ist reell. □

Beweis. Es existieren erzeugende Polynome $f_1, \dots, f_m \in R[X_1, \dots, X_n]$ von I . Sei P der Kegel in $R[X_1, \dots, X_n]$, der von den Polynomen $f_1, \dots, f_m, -f_1, \dots, -f_m$ erzeugt wird. Dann ist $\mathcal{W}(P) = \mathcal{Z}(I) =: V$. Sei zunächst $f \in \mathcal{J}(V)$. Dann existieren mit Korollar 2.3.7 $m \in \mathbb{N}_0$ und $g \in P$ mit $f^{2m} + g = 0$. Ist $m = 0$, so ist $1 \in I$ und die Aussage folgt sofort. Im Fall $m > 0$ besitzt g die Form $g = s + h$, wobei s eine Summe von Quadraten und $h \in I$ ist, und es folgt: $f \in \sqrt[m]{I}$.

Sei nun $f \in \sqrt[m]{I}$. Dann existieren $s, h \in R[X_1, \dots, X_n]$, wobei s eine Summe von Quadraten und $h \in I$ ist, mit $(f^2)^m + s + h = 0$. Für $x \in V$ gilt also $f(x) = 0$.

Jetzt zeigen wir die Äquivalenz.

(a) \Rightarrow (b): Ist $\sum_{i=1}^r f_i^2 \in I = \sqrt[m]{I}$, so folgt aus der Definition des reellen Radikals, dass $f_i \in \sqrt[m]{I} = I$ für alle $i = 1, \dots, r$ gilt. Also ist I reell.

(b) \Rightarrow (a): Es ist zu zeigen, dass $\sqrt[m]{I} \subseteq I$ gilt. Sei $f \in \sqrt[m]{I}$. Aus der Definition und der Voraussetzung folgt, dass ein $m \in \mathbb{N}$ existiert, sodass $f^m \in I$ ist. Ist m gerade, so ist $f^{m/2} \in I$. Ist m ungerade, so ist $f^{(m+1)/2} \in I$. Induktiv folgt: $f \in I$. ■

Insbesondere ist das reelle Radikal in diesem Fall ein Ideal.

2.4 Der Satz von Schmüdgen

In diesem Abschnitt stellen wir den *Satz von Schmüdgen* vor. Unter der Voraussetzung, dass R *archimedisch* ist, ist ein auf einer beschränkten semialgebraischen Menge echt positives Polynom $f \in R[X_1, \dots, X_n]$ ein Element aus dem Kegel der aufspannenden Polynome.

Wir entnehmen die Ausführungen dem Vorlesungsskript *Reelle algebraische Geometrie 1 & 2* von Netzer, siehe [Net]. Dabei passen wir die Notation der bisher verwendeten an und beweisen den dort verwendeten Positivstellensatz mittels einer Umformulierung des formalen Positivstellensatzes Lemma 2.3.4.

Auch in diesem Abschnitt sei A ein kommutativer Ring und R ein reell abgeschlossener Körper.

Beweisidee Nach dem konkreten Positivstellensatz ist f genau dann auf der Positivstellenmenge eines Kegels $P \subseteq K[X_1, \dots, X_n]$ positiv, wenn $g, h \in P$ existieren mit $fg = 1 + h$. Wir zeigen, dass im archimedischen Fall $g \in \mathbb{N}$ gewählt werden kann. Dann folgt sofort $f \in P$.

Das reelle Spektrum und der abstrakte Positivstellensatz

Definition 2.4.1 - Reelles Spektrum eines Rings

Die Menge

$$\text{sper}(A) := \{P \subseteq A \mid P \text{ ist Primkegel}\}$$

wird als *reelle Spektrum* von A bezeichnet. □

Für $a \in A$ definieren wir eine Abbildung \hat{a} durch:

$$\begin{aligned} \hat{a}: \text{sper}(A) &\rightarrow \bigcup_{P \in \text{sper}(A)} K_P \\ P &\mapsto a + \text{supp}(P). \end{aligned}$$

Durch einen Kegel $P \subseteq A$ wird auf natürliche Weise nach Lemma 2.1.13 eine Anordnung \geq_P auf K_P definiert.

Bemerkung 2.4.2 Für $a \in A$ und $P \in \text{sper}(A)$ gilt:

$$\begin{aligned} \hat{a}(P) &\geq_P 0, \text{ genau dann wenn } a \in P, \\ \hat{a}(P) &>_P 0, \text{ genau dann wenn } -a \notin P, \\ \hat{a}(P) &=_P 0, \text{ genau dann wenn } a \in \text{supp}(P). \end{aligned}$$

Dies wird an der Konstruktion des Positivkegels von K_P deutlich. □

Ähnlich wie im vorigen Abschnitt definieren wir:

Definition 2.4.3 - Verschwinde- und Positivstellenmengen

Sei weiterhin $U \subseteq A$ eine beliebige Teilmenge. Dann definiert

$$\mathcal{V}(U) := \{P \in \text{sper}(A) \mid \hat{u}(P) =_P 0 \text{ für alle } u \in U\}$$

die *Verschwindemenge* von U und

$$\mathcal{W}(U) := \{P \in \text{sper}(A) \mid \hat{u}(P) \geq_P 0 \text{ für alle } u \in U\}$$

die *Positivstellenmenge* von U . □

Für eine Teilmenge $U \subseteq A$ ist

$$\mathcal{W}(U) = \{P \in \text{sper}(A) \mid U \subseteq P\}.$$

Verschwindemengen können ebenso von den erzeugten Idealen und Positivstellenmengen von den erzeugten Kegeln gebildet werden.

Satz 2.4.4 - Abstrakter Positivstellensatz

Sei $a \in A$ und $P \subseteq A$ ein Kegel. Dann sind jeweils äquivalent:

- (i) (a) Es gilt: $\hat{a} \geq 0$ auf $\mathcal{W}(P)$.
- (b) Für $Q \in \text{sper}(A)$, $P \subseteq Q$ gilt: $a \in Q$.
- (c) Es gibt $m \in \mathbb{N}_0, g, h \in P$ mit $ag = a^{2m} + h$.
- (ii) (a) Es gilt: $\hat{a} > 0$ auf $\mathcal{W}(P)$.
- (b) Für $Q \in \text{sper}(A)$, $P \subseteq Q$ gilt: $-a \notin Q$.
- (c) Es gibt $g, h \in P$ mit $ag = 1 + h$.
- (iii) (a) Es gilt: $\hat{a} = 0$ auf $\mathcal{W}(P)$.
- (b) Für $Q \in \text{sper}(A)$, $P \subseteq Q$ gilt: $a \in \text{supp}(Q)$.
- (c) Es gibt $m \in \mathbb{N}_0, g \in P$ mit $a^{2m} + g = 0$. □

Beweis. Die Äquivalenzen zwischen (a) und (b) folgen aus Bemerkung 2.4.2.

(i): Wir zeigen mit Hilfe von Lemma 2.3.4 die Aussage, indem wir es auf die folgenden Mengen anwenden:

$$\overline{P} := \mathcal{K}[P, -a], \overline{M} := \mathcal{M}[a] \text{ und } \overline{I} := \{0\}.$$

Aussage (b) ist äquivalent zu

$$\text{„Es gibt kein } Q \in \text{sper}(A), \overline{P} \subseteq Q \text{ mit: } a \notin \text{supp}(Q)\text{“}.$$

Mit Lemma 2.3.4 existieren $p \in \overline{P}, b \in \overline{M}, c \in \overline{I}$ mit

$$p + b^2 + c = p + a^{2m} + 0 = 0$$

und damit ergibt sich die Aussage.

(ii): Die Mengen \overline{P} und \overline{I} definieren wir wie oben und $\overline{M} := \{1\}$. Aussage (b) ist äquivalent zu

$$\text{„Es gibt kein } Q \in \text{sper}(A), \overline{P} \subseteq Q \text{ mit: } 1 \notin \text{supp}(Q) \text{ und } 0 \in \text{supp}(Q)\text{“},$$

und mit Lemma 2.3.4 existieren $p \in \overline{P}, b \in \overline{M}$ und $c \in \overline{I}$ mit

$$p + b^2 + c = p + 1^2 + 0 = 0.$$

(iii): Lemma 2.3.4 wenden wir auf die Mengen

$$\overline{P} := P, \overline{M} := \mathcal{M}[a] \text{ und } \overline{I} := \{0\}$$

an. Aussage (b) ist äquivalent zu

„Es gibt kein $Q \in \text{sper}(A), \overline{P} \subseteq Q$ mit: $a \notin \text{supp}(Q)$ “,

also existieren $g \in P, b \in \overline{M}$ und $c \in \overline{I}$ mit

$$g + b^2 + c = g + a^{2m} + 0 = 0$$

und damit folgt die Behauptung. ■

Um den Satz von Schmüdgen zu beweisen, kommen wir auch ohne den Begriff des reellen Spektrums aus, da der abstrakte Positivstellensatz 2.4.7 im Folgenden jeweils nur in der Variante (c) benötigt wird. Beachten wir jedoch die Ähnlichkeit zu Korollar 2.3.7, ist der Zusammenhang zwischen positiven Elementen auf dem Spektrum und positiven Polynomen bemerkenswert. Tatsächlich kann R^n auf geeignete Weise mit dem reellen Spektrum identifiziert werden. Wir verweisen hierzu auf Kapitel 7 in [BCR].

Beschränkte Mengen und archimedische Kegel

Der Satz von Schmüdgen macht eine Aussage über Polynome auf *beschränkten* Mengen. An welcher Stelle geht „Beschränktheit“ ein? Zunächst ist ein sinnvoll auf reell abgeschlossene Körper verallgemeinerter Begriff einzuführen.

Die natürlichen Zahlen fassen wir als Teilmenge eines geordneten Körpers auf.

Definition 2.4.5 - Beschränkte Mengen

Eine Teilmenge $S \subseteq R^n$ heißt *beschränkt*, falls ein $r \in R$ existiert, sodass für alle Elemente $a = (a_1, \dots, a_n) \in S$ gilt: $\sum_{i=1}^n a_i^2 \leq r$. □

Wir werden sehen, dass beschränkte Mengen mit bestimmten Kegeln des Polynomrings identifiziert werden können. Diese werden nun eingeführt:

Definition 2.4.6 - Archimedische Körper und Kegel

Sei (K, \leq) ein total geordneter Körper. K heißt *archimedisch*, falls für alle $a \in K$ ein $r \in \mathbb{N}$ existiert mit $a \leq r$.

Ein Kegel $P \subseteq A$ heißt *archimedisch*, falls für alle $a \in A$ ein $r \in \mathbb{N}$ existiert, sodass gilt: $r - a \in P$. □

Falls für $a \in K$ ein $r \in \mathbb{N}$ existiert mit $a \leq r$, nennen wir a *überschreibbar*.

Wir sehen, dass ein Primkegel $P \subseteq A$ genau dann archimedisch ist, wenn K_P archimedisch ist. Insbesondere ist der Körper der reellen Zahlen archimedisch. Im archimedischen Fall kann der abstrakte Positivstellensatz 2.4.4 konkreter formuliert werden:

Satz 2.4.7 - Archimedischer Positivstellensatz

Sei $P \subseteq A$ ein archimedischer Kegel und $a \in A$. Dann sind äquivalent:

- (a) $\hat{a} > 0$ auf $\mathcal{W}(P)$.
- (b) Es existieren $k \in \mathbb{N}$ und $h \in P$ mit $ka = 1 + h$. □

Beweis. (b) \Rightarrow (a): Satz 2.4.4.

(a) \Rightarrow (b): Nach Satz 2.4.4 gibt es $g, h \in P$ mit $ga = 1 + h$. Nach Voraussetzung wissen wir, dass natürliche Zahlen l, m existieren mit $l - g \in P, a + m \in P$. Sei

$$Q := \{(s, r) \mid s \in \mathbb{N}, r \in \mathbb{Z}, sa + r \in P\}.$$

Für $(s, r) \in Q, r \geq 0$, ist

$$(sl)a + (rl - s) = (l - g)(sa + r) + s(ga - 1) + rg \in P,$$

also ist $(sl, rl - s) \in Q$. Bestimmen wir ausgehend von $(1, m) \in Q$ weitere Elemente in Q , erhalten wir:

$$\begin{aligned} (l, ml - 1) &\in Q, \\ (l^2, ml^2 - 2l) &\in Q, \\ &\vdots \\ (l^e, ml^e - el^{e-1}) &\in Q \end{aligned}$$

für $e \leq ml$. Für $e = ml$ gilt: $ml^e - el^{e-1} = 0$. Also erhalten wir für $e = ml + 1$, dass gilt: $(l^{ml+1}, -l^{ml}) \in Q$. Mit Beispiel 2.1.2 (4) ist $la - 1 \in P$. ■

Lemma 2.4.8 - Archimedische Eigenschaft von Polynomkegeln

Sei K ein archimedischer Körper und $P \subseteq K[X_1, \dots, X_n]$ ein Kegel. Dann sind äquivalent:

- (a) P ist archimedisch.
- (b) Es existiert ein $r \in \mathbb{N}$ mit $r - \sum_{i=1}^n X_i^2 \in P$. □

Beweis. (a) \Rightarrow (b): Per Definition.

(b) \Rightarrow (a): Koeffizienten von Polynomen sind nach Voraussetzung *überschreibbar*, das heißt, die Differenz zu mindestens einer natürlichen Zahl ist Element des Kegels P . Weiterhin gilt:

Schritt 1: Variablen sind überschreibbar.

Für $j = 1, \dots, n$ gilt:

$$(r + 1) \pm X_j = \frac{3}{4} + \left(\frac{1}{2} \pm X_j\right)^2 + \left(r - \sum_{i=1}^n X_i^2\right) + \sum_{\substack{i=1 \\ i \neq j}}^n X_i^2 \in P.$$

Schritt 2: Überschreibbarkeit von Summen und Produkten.

Es seien $f, g \in K[X_1, \dots, X_n]$ überschreibbar und $k, l \in \mathbb{N}$ so gewählt, dass $k \pm f \in P$ und $l \pm g \in P$ sind. Für die Summe und das Produkt gilt:

$$\begin{aligned} (k + l) - (f + g) &\in P, \\ 3kl - fg &= (k + f)(l - g) + k(l + g) + l(k - f) \in P. \end{aligned}$$

Induktiv folgt, dass beliebige Polynome überschreibbar sind. ■

Satz 2.4.9 - Archimedische Kegel

Sei R ein archimedischer reell abgeschlossener Körper und $f_1, \dots, f_s \in R[X_1, \dots, X_n]$. Es sei $P := \mathcal{K}[f_1, \dots, f_s]$. Dann sind äquivalent:

- (a) Der Kegel P ist archimedisches. □
- (b) Die Menge $\mathcal{W}(P)$ ist beschränkt in R^n .

Beweis. (a) \Rightarrow (b): Der Kegel P ist archimedisches. Es existieren daher ein $r \in \mathbb{N}$ und ein $t \in P$ mit $r - \sum_{i=1}^n X_i^2 = t$. Sei $y = (y_1, \dots, y_n) \in \mathcal{W}(P)$, dann gilt die Ungleichung $r - \sum_{i=1}^n y_i^2 = t(y) \geq 0$ und damit ist $r \geq \sum_{i=1}^n y_i^2$.

(b) \Rightarrow (a): Wir werden die Archimedizität von P auf die eines kleineren Kegels zurückführen. Dazu wählen wir zunächst eine Schranke $r \in \mathbb{N}$ mit $r > \sum_{i=1}^n y_i^2$ für alle $y = (y_1, \dots, y_n) \in \mathcal{W}(P)$. Das Polynom $p(X_1, \dots, X_n) := r - \sum_{i=1}^n X_i^2$ ist auf der Menge $\mathcal{W}(P)$ echt positiv.

Mit Korollar 2.3.7 existieren $g, h \in P$ mit $pg = 1 + h$. Da Kegel alle Quadrate enthalten, gilt:

$$(1 + h)p = gp^2 \in P.$$

Bezeichnen wir mit T_0 den Kegel, der von p erzeugt wird, gilt weiterhin:

$$(1 + h)T_0 \subseteq P.$$

Da T_0 nach Lemma 2.4.8 archimedisch ist, existiert ein $s \in \mathbb{N}$ mit $s - h \in T_0$. Damit ist

$$(1 + s)(s - h) = (1 + h)(s - h) + (s - h)^2 \in P,$$

also ist auch $s - h \in P$. Weiterhin ist $p + hr = p + hp + h \sum_{i=1}^n X_i^2 \in P$. Zusammenführen der Ergebnisse ergibt:

$$r(1 + s) - \sum_{i=1}^n X_i^2 = rs + p = (p + hr) + r(s - h) \in P.$$

Damit ist der Kegel P auch archimedisch. ■

Der konkrete archimedische Positivstellensatz

Mit dem Satz von Schmüdgen beschließen wir dieses Kapitel. Er ist ein Pendant zum reellen Nullstellensatz, da er die Polynome charakterisiert, die auf einer Positivstellenmenge echt positiv sind.

Satz 2.4.10 - Schmüdgen; Konkreter archimedischer Positivstellensatz

Sei R ein archimedischer reell abgeschlossener Körper, $f_1, \dots, f_s \in R[X_1, \dots, X_n]$. Die Menge $\mathcal{W}(P)$ mit $P := \mathcal{K}[f_1, \dots, f_s]$ sei beschränkt in R^n . Dann gilt für ein Polynom $p \in R[X_1, \dots, X_n]$: Ist $p > 0$ auf $\mathcal{W}(P)$, dann ist $p \in P$. □

Beweis. Es sei $p > 0$ auf $\mathcal{W}(P)$. Mit Korollar 2.3.7 folgt, dass $g, h \in P$ existieren mit $pg = 1 + h$. Mit Satz 2.4.4 ist $\hat{p} > 0$ auf $\mathcal{W}(P)$. Da P mit Satz 2.4.9 archimedisch ist, folgt aus dem archimedischen Positivstellensatz 2.4.7, dass $k \in \mathbb{N}$ und $t \in P$ existieren mit $kp = 1 + t$. Division durch $\frac{1}{k}$ ergibt:

$$p = \frac{1 + t}{k},$$

und damit ist $p \in P$. ■

3 Konvexe Geometrie

Der Grundbegriff dieses Kapitels ist der der *konvexen Menge* in einem Vektorraum. Wir werden verstehen, welche Strukturen einer beliebigen Menge bei der Bildung der konvexen Hülle erhalten bleiben und wie sich konvexe Mengen unter topologischen Operationen, wie der Bildung eines Abschlusses, verhalten.

Anfangen von der konvexen Hülle von endlich vielen Punkten, den *Polytopen*, über *Polyeder*, die man als Summe von Polytopen mit *Kegeln* schreiben kann, stellen wir den Begriff des *Spektraeders*, die die Charakterisierung von Polyedern über Schnitte von Lösungsmengen affiner Ungleichungen verallgemeinert, vor. Im Speziellen untersuchen wir die Stabilität von Spektraedern unter affinen Transformationen. Wir stellen fest, dass projizierte Spektraeder semialgebraische Mengen sind, sich also als Lösungsmenge endlich vieler polynomialer Ungleichungen schreiben lassen.

Im zweiten Abschnitt befassen wir uns zunächst mit einer verallgemeinerten Darstellung von *dualen Kegeln*. Danach charakterisieren wir die konvexen Mengen, die ein nichtleeres Inneres in einem affinen Teilraum, welches wir *relatives Inneres* nennen, besitzen. Es zeigt sich, dass die Existenz eines nichtleeren relativen Inneren nur in endlichdimensionalen Vektorräumen gesichert werden kann. In diesem Fall können wir Abschlüsse mit der Bildung des relativen Inneren vertauschen. Dies führt zu einem abschließenden Satz, der eine Beziehung zwischen dem Schnitt eines Kegels mit einem Teilraum, dessen Dual und der Projektion auf den topologischen Dual des Teilraums herstellt.

Die Betrachtungen meist struktureller, aber auch technischer Natur werden in Kapitel 4 für den Beweis, dass Thetakörper projizierte Spektraeder sind, benötigt.

In diesem Kapitel bezeichnet V einen Vektorraum über \mathbb{R} .

3.1 Polyeder, Spektraeder und Kegel

In diesem Abschnitt erinnern wir an Grundbegriffe der konvexen Geometrie und führen den Begriff des Spektraeders ein. Dazu notieren wir zunächst grundlegende Definitionen zu symmetrischen und positiven Matrizen. Im Kontext einer kurzen Einführung zu konvexen Mengen bringen wir einige Aussagen zum Abschluss einer konvexen Hülle an. Eingebettet in einen Rahmen aus Aussagen über Polyeder stellen wir danach Spektraeder vor. Zuletzt bringen wir Kegel in Vektorräumen mit Anordnungen in Verbindung. Dies bereitet den nächsten Abschnitt vor.

Die Aussagen zu positiv semidefiniten Matrizen finden sich in [BPT]. Eine gute Referenz hierfür ist [HuWi]. Die Sätze zu konvexen Mengen stammen aus [Sch]. Die Aussagen zu Polyedern und Spektraedern entnehmen wir [BPT]. Die Definition und Beispiele zur allgemeinen Einführung über Kegel und angeordnete Vektorräume sind [BPT] und [GaMa] entlehnt.

Matrizenklassen und Positivität

Eine reellwertige Matrix $A = (a_{i,j})_{1 \leq i,j \leq n} \in \mathcal{M}_n(\mathbb{R})$ heißt *symmetrisch*, falls $a_{i,j} = a_{j,i}$ für alle $1 \leq i, j \leq n$ gilt. Der Raum der symmetrischen Matrizen in $\mathcal{M}_n(\mathbb{R})$ bezeichnen wir mit \mathcal{S}_n . Eine symmetrische Matrix $A \in \mathcal{S}_n$ heißt *positiv semidefinit*, falls für alle $x \in \mathbb{R}^n$ die Ungleichung

$$x^t Ax \geq 0$$

erfüllt ist. Wir schreiben in diesem Fall $A \geq 0$. Den Raum der positiv semidefiniten Matrizen bezeichnen wir mit \mathcal{S}_n^+ . Eine Matrix ist genau dann positiv semidefinit, wenn ihre $2^n - 1$ Hauptminoren nicht negativ sind. Weiterhin heißt eine symmetrische Matrix $A \in \mathcal{S}_n$ *positiv definit*, falls für alle $x \in \mathbb{R}^n$, $x \neq 0$, die Ungleichung

$$x^t Ax > 0$$

erfüllt ist. Wir schreiben dann $A > 0$. Eine Matrix ist genau dann positiv definit, wenn ihre n leitenden Hauptminoren positiv sind. Ferner bezeichnen wir mit \mathcal{O}_n den Raum der orthogonalen $n \times n$ -Matrizen mit reellen Einträgen.

Konvexe Mengen, affine Räume und Polyeder

Eine Teilmenge $C \subseteq V$ heißt *konvex*, falls für alle $v, w \in C$ und $\lambda \in [0, 1]$ die Konvexzerlegung $\lambda v + (1 - \lambda)w$ ebenfalls Element von C ist. Falls $C \subseteq V$ konvex

ist und für ein $v \in C$ gilt, dass v keine echte Konvexzerlegung zweier verschiedener Punkte aus C ist, bezeichnen wir v als *Extremalpunkt* von C . Die Menge aller Extremalpunkte von C wird mit $\text{ext}(C)$ bezeichnet. Ist $S \subseteq V$ eine beliebige Menge, bezeichnen wir den Schnitt aller konvexen Mengen in V , die S enthalten, mit $\text{co}(S)$ beziehungsweise als die *konvexe Hülle* von S .

Nun konzentrieren wir uns auf den Spezialfall $V = \mathbb{R}^n$.

Mengen, die sich als Summe eines linearen Teilraums mit einem Vektor schreiben lassen, also von der Form

$$x_0 + \mathbb{R} \cdot (x_1 - x_0) + \dots + \mathbb{R} \cdot (x_k - x_0) = \left\{ \sum_{i=0}^k \lambda_i x_i \mid \lambda_0 + \dots + \lambda_k = 1 \right\}$$

mit $x_0, x_1, \dots, x_k \in \mathbb{R}^n$ sind, bezeichnen wir als *affine Teilräume* von \mathbb{R}^n . Wenn das System $((x_1 - x_0), \dots, (x_k - x_0))$ linear unabhängig ist, heißt (x_0, x_1, \dots, x_k) *affin unabhängig*. Die Dimension eines affinen Unterraums kann sinnvoll durch die Dimension des linearen Teilraums $\mathbb{R} \cdot (x_1 - x_0) + \dots + \mathbb{R} \cdot (x_k - x_0)$ beschrieben werden.

An dieser Stelle führen wir zwei nützliche Sätze an. Sie erlauben uns, zu charakterisieren, wann die konvexe Hülle von abgeschlossenen Mengen wieder abgeschlossen ist.

Satz 3.1.1 - Carathéodory

Ist $M \subseteq \mathbb{R}^n$ eine Menge und $x \in \text{co}(M)$, so ist x Konvexkombination von affin unabhängigen Punkten von M . Insbesondere ist es möglich, x als Konvexkombination von höchstens $n + 1$ Punkten zu schreiben. □

Beweis. Es existieren $\lambda_0, \dots, \lambda_k > 0$, $\sum_{i=0}^k \lambda_i = 1$, und $x_0, \dots, x_k \in M$ mit $x = \sum_{i=0}^k \lambda_i x_i$. Wir wählen k minimal.

Behauptung: Das System (x_0, \dots, x_k) ist affin unabhängig.

Beweis: Wir nehmen an, dass (x_0, \dots, x_k) affin abhängig ist, und folgern einen Widerspruch. Es ist dann das System $((x_1 - x_0), \dots, (x_k - x_0))$ linear abhängig, das heißt, es existieren $a_0, \dots, a_k \in \mathbb{R}^n \setminus \{0\}$ mit $\sum_{i=0}^k a_i x_i = 0$ und $\sum_{i=0}^k a_i = 0$. Wählen wir $0 \leq s \leq k$ derart, dass λ_s/a_s positiv und kleinstmöglich ist, erhalten wir eine Darstellung von x als Konvexkombination von k Punkten:

$$x = \sum_{i=0}^k \left(\lambda_i - \frac{\lambda_s}{a_s} a_i \right) x_i.$$

Dies ist aber unmöglich. ◇

Damit ist $k \leq n$. ■

Jetzt charakterisieren wir, wie sich Abschlüsse und konvexe Hüllen zueinander verhalten:

Satz 3.1.2 - Abschluss und konvexe Hülle

Für eine Menge $M \subseteq \mathbb{R}^n$ gilt: $\text{co}(\text{cl}(M)) \subseteq \text{cl}(\text{co}(M))$. Ist M beschränkt, gilt die Gleichheit. Insbesondere ist die konvexe Hülle kompakter Mengen kompakt. \square

Beweis. Es sei $x = \sum_{i=1}^k \lambda_i x_i \in \text{co}(\text{cl}(M))$ mit $x_1, \dots, x_k \in \text{cl}(M)$ und geeigneten Faktoren $\lambda_1, \dots, \lambda_k \geq 0, \sum_{i=1}^k \lambda_i = 1$. Sei $\varepsilon > 0$. Es existieren $m_i \in M$ mit $\|x_i - m_i\| < \varepsilon$. Damit ist $m := \sum_{i=1}^k \lambda_i m_i \in \text{co}(M)$ und $\|x - m\| < \varepsilon$. Daraus folgt: $x \in \text{cl}(\text{co}(M))$. Sei nun M beschränkt. Dann ist die Menge

$$K := \left\{ (\lambda_1, \dots, \lambda_{n+1}, x_1, \dots, x_{n+1}) \left| \lambda_1, \dots, \lambda_{n+1} \geq 0, \sum_{i=1}^{n+1} \lambda_i = 1, x_1, \dots, x_{n+1} \in \text{cl}(M) \right. \right\}$$

kompakt und das Bild von K unter der Abbildung

$$\mathbb{R}^{2n+2} \rightarrow \mathbb{R}^n, \quad (\lambda_1, \dots, \lambda_{n+1}, x_1, \dots, x_{n+1}) \mapsto \sum_{i=1}^{n+1} \lambda_i x_i$$

nach Satz 3.1.1 gleich $\text{co}(\text{cl}(M))$. Also ist $\text{co}(\text{cl}(M))$ kompakt. Damit gilt

$$\text{cl}(\text{co}(M)) \subseteq \text{cl}(\text{co}(\text{cl}(M))) = \text{co}(\text{cl}(M))$$

und die Aussage ist bewiesen. ■

Die konvexe Hülle einer abgeschlossenen Menge ist im Allgemeinen nicht abgeschlossen. Als Gegenbeispiel bringen wir die konvexe Hülle einer Geraden und eines Punktes mit echtem Abstand von der Geraden in der Ebene an.

Ein *Polyeder* $P \subseteq \mathbb{R}^n$ ist eine Menge der Form

$$P = \{x \in \mathbb{R}^n \mid \text{Für alle } i = 1, \dots, k \text{ gilt: } \langle y_i, x \rangle \leq b_i\},$$

wobei $y_1, \dots, y_k \in \mathbb{R}^n, b_1, \dots, b_k \in \mathbb{R}$ und $k \in \mathbb{N}$ beliebig gewählt werden können. Aus der Definition folgt, dass Polyeder konvex und abgeschlossen sind. Ist ein Polyeder beschränkt, sprechen wir von einem *Polytop*. Nach dem *Theorem von Minkowski-Weyl* ist ein Polyeder P als Summe einer konvexen Menge und eines Kegels (siehe Definition 3.1.9) endlich erzeugt, siehe [Zie]. Es existiert also eine Darstellung

$$P = \text{co}(x_1, \dots, x_k) + \left\{ \sum_{i=1}^l \lambda_i y_i \left| \lambda_1, \dots, \lambda_l \geq 0 \right. \right\}$$

mit Elementen $x_1, \dots, x_k, y_1, \dots, y_l \in \mathbb{R}^n$. Diese Charakterisierung liefert ein gutes Mittel zum Umgang mit und zur bildlichen Vorstellung von Polyedern. Wir sehen beispielsweise sofort, dass Polytope genau die konvexen Hüllen von endlich vielen Punkten sind.

Wir wollen im Folgenden eine mehr generalisierte Klasse von Teilmengen des Vektorraums \mathbb{R}^n betrachten.

Spektraeder

Jetzt kommen wir zur Definition von Spektraedern.

Definition 3.1.3 - Spektraeder

Eine Teilmenge $S \subseteq \mathbb{R}^n$ heißt *Spektraeder*, falls ein $m \in \mathbb{N}$ existiert mit:

$$S = \left\{ (x_1, \dots, x_n) \in \mathbb{R}^n \mid A_0 + \sum_{i=1}^n A_i x_i \geq 0 \right\},$$

wobei $A_0, \dots, A_n \in \mathcal{S}_m$ sind. Weiterhin bezeichnen wir das Bild $p(S)$ unter einer orthogonalen Projektion $p: \mathbb{R}^n \rightarrow \mathbb{R}^n$ als *projizierten Spektraeder*. \square

Ein Spektraeder ist eine konvexe und abgeschlossene Menge.

Bemerkung 3.1.4 Für $A \in \mathcal{S}_m$ und $B \in \mathcal{S}_k$ sind äquivalent:

- (a) $A \in \mathcal{S}_m^+$ und $B \in \mathcal{S}_k^+$.
- (b) $\begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix} \in \mathcal{S}_{m+k}^+$.

Damit können zwei Matrixungleichungen der Form

$$A_0 + \sum_{i=1}^n A_i x_i \geq 0 \quad \text{und} \quad B_0 + \sum_{i=1}^n B_i x_i \geq 0,$$

mit $A_0, \dots, A_n \in \mathcal{S}_m$ und $B_0, \dots, B_n \in \mathcal{S}_k$, zu einer zusammengefasst werden:

$$\begin{pmatrix} A_0 & 0 \\ 0 & B_0 \end{pmatrix} + \sum_{i=1}^n \begin{pmatrix} A_i & 0 \\ 0 & B_i \end{pmatrix} x_i \geq 0.$$

Spektraeder können also auch als Lösungsmenge endlich vieler Matrixungleichungen geschrieben werden. \square

Beispiel 3.1.5

- (1) Nach der vorangehenden Bemerkung sind Schnitte von Spektraedern wieder Spektraeder. Konvexität ist nicht stabil unter Vereinigungen, daher ist die Vereinigung zweier Spektraeder im Allgemeinen kein Spektraeder mehr.
- (2) Polyeder und insbesondere endlich erzeugte konvexe Mengen sind Spezialfälle von Spektraedern: Definieren die linearen Ungleichungen

$$\langle y_i, x \rangle \leq b_i \quad \text{mit } y_i \in \mathbb{R}^n, b_i \in \mathbb{R}, i = 1, \dots, k,$$

einen Polyeder, wird dieser durch die Matrixungleichung

$$\begin{pmatrix} b_1 & & 0 \\ & \ddots & \\ 0 & & b_k \end{pmatrix} - \sum_{j=1}^n \begin{pmatrix} (y_1)^j & & 0 \\ & \ddots & \\ 0 & & (y_k)^j \end{pmatrix} x_j \geq 0,$$

welche durch diagonale Matrizen gebildet wird, beschrieben.

- (3) Die abgeschlossene Einheitskreisscheibe

$$\left\{ (x, y) \in \mathbb{R}^2 \mid 1 - x^2 - y^2 \geq 0 \right\} = \left\{ (x, y) \in \mathbb{R}^2 \mid \begin{pmatrix} 1-x & y \\ y & 1+x \end{pmatrix} \geq 0 \right\}$$

ist ein Spektraeder. □

Im Folgenden wollen wir die Invarianz von Spektraedern unter affin-linearen Transformationen untersuchen.

Proposition 3.1.6 - Invarianz von Spektraedern

Ist $S \subseteq \mathbb{R}^n$ ein Spektraeder, $A \in \mathcal{M}_n(\mathbb{R})$ invertierbar und $t \in \mathbb{R}^n$, so sind auch die Mengen $A(S)$ und $S + t$ Spektraeder. □

Beweis. Der Spektraeder S sei gegeben wie in Definition 3.1.3, dann ist

$$AS = \left\{ x \in \mathbb{R}^n \mid A_0 + \sum_j \left(\sum_i A_i (A^{-1})_{i,j} \right) x_j \right\},$$

$$S + t = \left\{ x \in \mathbb{R}^n \mid \left(A_0 - \sum_i (A_i t^i) \right) + \sum_i A_i x_i \right\}.$$

Spektraeder sind damit insbesondere unter Drehspiegelungen invariant. ■

Unter beliebigen affin-linearen Transformationen bleiben Spektraeder nicht invariant, da projizierte Spektraeder im Allgemeinen keine Spektraeder sind:

Beispiel 3.1.7 Die Menge

$$\begin{aligned} S &= \left\{ (x, y) \in \mathbb{R}^2 \mid \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} + \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} x + \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} y \geq 0 \right\} \\ &= \left\{ (x, y) \in \mathbb{R}^2 \mid \begin{pmatrix} x & 1 \\ 1 & y \end{pmatrix} \geq 0 \right\} \\ &= \{(x, y) \in \mathbb{R}^2 \mid x \geq 0, xy - 1 \geq 0\} \end{aligned}$$

ist ein Spektraeder, aber das Bild unter der Projektion π auf die erste Koordinate,

$$\begin{aligned} \pi(S) &= \{x \in \mathbb{R} \mid \text{Es gibt ein } y \in \mathbb{R} \text{ mit } x \geq 0, xy - 1 \geq 0\} \\ &= \{x \in \mathbb{R} \mid x > 0\}, \end{aligned}$$

ist nicht abgeschlossen, also kein Spektraeder. □

Da positiv semidefinite Matrizen über ihre Hauptminoren beschrieben werden können, siehe Seite 62, sind Spektraeder semialgebraische Mengen. Für projizierte Spektraeder gilt dies auch. Dies folgt direkt aus einem Korollar des Transferprinzips von Tarski-Seidenberg:

Proposition 3.1.8 - Projizierte Spektraeder sind semialgebraisch

Ist $S \subseteq \mathbb{R}^n$ ein projizierter Spektraeder und $p : \mathbb{R}^n \rightarrow \mathbb{R}^k$ eine orthogonale Projektion, so ist das Bild $p(S)$ eine semialgebraische Menge. □

Beweis. Für eine orthogonale Projektion der Form $\pi : \mathbb{R}^{n+k} \rightarrow \mathbb{R}^k, (x, y) \mapsto x$, folgt die Behauptung direkt aus der Aussage, dass projizierte semialgebraische Mengen selbst wieder semialgebraische Mengen sind, siehe Satz 2.3.2. Nach Proposition 3.1.6 sind Spektraeder unter orthogonalen Transformationen invariant. Eine einfache Überlegung zeigt, dass dies auch für semialgebraische Mengen gilt. Daraus folgt die Aussage für beliebige orthogonale Projektionen. ■

Während die Anzahl der Polynome, die einen Spektraeder als semialgebraische Menge beschreiben, durch die Anzahl der Hauptminoren beschränkt ist, kann die Anzahl der die Projektion beschreibenden Polynome sehr groß werden. Um einen Eindruck zu bekommen, machen wir uns zunächst klar, dass ein Vorgehen wie im Beweis von Satz 2.3.2 auf Seite 46 fordert, dass die Projektion in Hintereinanderausführungen von Projektionen der Kodimension Eins zerlegt wird. Für jede dieser Faktoren ist eine endliche Familie von beschreibenden Polynomen separat zu bestimmen. Selbst diese Bestimmung ist sehr komplex, was in der Komplexität der Signaturabbildung, siehe Korollar 2.2.3 auf Seite 40, begründet ist.

Kegel und angeordnete Vektorräume

Definition 3.1.9 - Kegel in Vektorräumen

Eine Teilmenge $K \subseteq V$ heißt *Kegel*, falls sie die folgenden Eigenschaften erfüllt:

- (i) Sind $v, w \in K$, dann gilt: $v + w \in K$.
- (ii) Ist $v \in K$ und $\lambda \in \mathbb{R}_0^+$, dann gilt: $\lambda v \in K$.

Falls $K \cap (-K) = \{0\}$ gilt, bezeichnen wir K als *echten Kegel*.

Im Fall $K \cup (-K) = V$ bezeichnen wir K als *erzeugenden Kegel*. \square

Der größte Teilraum von V in K ist $K \cap (-K)$ und der kleinste Teilraum über K ist $K - K$.

Das Gegenstück dieser Definition, Kegel kommutativer Ringe, findet sich auf Seite 23 in Kapitel 2. Der Terminus *Kegel* ist somit in dieser Arbeit vom aktuellen Kontext abhängig. Trotz der Unterschiede gibt es strukturelle Gemeinsamkeiten. Auch hier sind Kegel immer als Positivkegel von speziellen Ordnungen zu verstehen:

Definition 3.1.10 - Angeordneter Vektorraum

Ein Vektorraum V heißt *angeordnet*, falls V ein total geordneter Vektorraum ist, d.h. ein Vektorraum, auf dem eine reflexive, antisymmetrische und transitive Relation \leq existiert, sodass alle Elemente vergleichbar sind, und für alle $v, v', w \in V$ gilt:

- (i) Ist $v \leq v'$, dann $v + w \leq v' + w$,
- (ii) Ist $0 \leq v$ und $\lambda \in \mathbb{R}_0^+$, dann $0 \leq \lambda v$.

Der *Positivkegel* P von V ist die Menge $P := \{v \in V \mid 0 \leq v\}$. \square

Wir sprechen auch von einer *Anordnung* auf einen Vektorraum.

Die Bedingung (i) ist äquivalent zu:

$$\text{„Ist } v \leq w, v' \leq w', \text{ dann gilt: } (v + v') \leq (w + w')\text{“}$$

für alle $v, v', w, w' \in V$.

Proposition 3.1.11 - Kegel sind Positivkegel

Es gibt eine Eins-zu-Eins-Beziehung zwischen

- (a) Echten erzeugenden Kegeln von V ,
- (b) Positivkegeln einer Anordnung von V . \square

Beweis. Ist $K \subseteq V$ ein Kegel, dann definiert $v \leq w : \Leftrightarrow w - v \in K$ für $v, w \in V$ eine reflexive und transitive Relation auf V , die die Bedingungen (i) und (ii) erfüllt. Ist K echt, so ist \leq antisymmetrisch. Die Totalität folgt, falls K erzeugend ist. Umgekehrt ist ein echter erzeugender Kegel für eine Anordnung (V, \leq) gegeben durch $\{w - v \mid v, w \in V, v \leq w\}$. Die Abbildung ist eineindeutig. ■

Ist $(v_i)_{i \in I}$ eine Familie von Elementen in V , bezeichnen wir mit $\mathcal{K}((v_i)_{i \in I})$ den Schnitt aller Kegel von V , die $(v_i)_{i \in I}$ enthalten. Es gilt:

$$\mathcal{K}((v_i)_{i \in I}) = \left\{ \sum_{i \in I_0} \lambda_i v_i \mid I_0 \subseteq I, \#I_0 < \infty, \lambda_i > 0 \text{ für alle } i \in I_0 \right\}.$$

Wir nennen $\mathcal{K}((v_i)_{i \in I})$ den *erzeugten Kegel* von $(v_i)_{i \in I}$.

Beispiel 3.1.12

- (1) Die Menge der positiv semidefiniten Matrizen \mathcal{S}_n^+ ist ein echter Kegel in den symmetrischen Matrizen \mathcal{S}_n und induziert die Ordnung \succeq .
- (2) Beliebige Schnitte von Kegeln sind Kegel.
- (3) Endliche Summen von Kegeln sind Kegel.
- (4) Sind $K \subseteq V$ und $L \subseteq W$ Kegel in \mathbb{R} -Vektorräumen V und W , so ist die direkte Summe $K \oplus L$ ein Kegel in $V \oplus W$. □

In den folgenden Kapiteln werden vor allem Kegel, die durch quadratische Polynome erzeugt werden, von Bedeutung sein.

3.2 Duale Kegel und das relative Innere

Das Ziel dieses Abschnitts ist es, Aussagen über den Schnitt von Kegeln mit linearen Teilräumen zu machen. Dazu untersuchen wir die topologischen Eigenschaften konvexer Mengen und übertragen sie auf Kegelschnitte.

Zunächst stellen wir in einem allgemeinen Rahmen *lokalkonvexe Vektorräume* vor, um dann im Speziellen duale Kegel von Teilmengen eines lokalkonvexen Vektorraums zu studieren. Es ist nur dann gesichert, dass konvexe Mengen ein nichtleeres relatives Inneres besitzen, wenn der zu Grunde liegende Vektorraum von endlicher Dimension ist. Diesen Fall betrachten wir näher.

Dieser Abschnitt orientiert sich an den Unterabschnitten 5.2.1 und 7.2.2 der Publikation [BPT]. Hier werden die Begriffe auf duale Kegel in lokalkonvexen

Vektorräumen verallgemeinert. Eine Einführung in die Theorie lokalkonvexer Vektorräume liefert Kapitel VIII in [Wer]. Die Aussagen im vorletzten Unterabschnitt über das relative Innere von konvexen Mengen entnehmen wir im Wesentlichen der Publikation [Roc].

Wie in der Einleitung zu diesem Kapitel bemerkt, bezeichnet V einen Vektorraum über \mathbb{R} . Die Aussagen des ersten Unterabschnitts können problemlos auf einen Vektorraum mit komplexen Skalaren verallgemeinert werden. Aus technischen Gründen setzen wir $V \neq \{0\}$ voraus.

Lokalkonvexe Vektorräume

Im Folgenden sei V *lokalkonvex*, das heißt, V sei ausgestattet mit der durch eine Familie von Halbnormen \mathcal{P} induzierten Topologie $\mathcal{T}_{\mathcal{P}}$. Die Halbnormen \mathcal{P} seien *separierend* beziehungsweise $\mathcal{T}_{\mathcal{P}}$ hausdorffsch.

Eine Umgebungsbasis von $x \in V$ besteht aus endlichen Schnitten von offenen Mengen der Form

$$U_{\varepsilon,p}(x) := \{y \in V \mid p(y-x) < \varepsilon\}$$

für $\varepsilon > 0$ und $p \in \mathcal{P}$. Wir bezeichnen den Schnitt von $U_{\varepsilon,p_1}(x), \dots, U_{\varepsilon,p_k}(x)$ für Halbnormen $p_1, \dots, p_k \in \mathcal{P}$ mit $U_{\varepsilon,p_1, \dots, p_k}(x)$. Da eine Halbnorm eine konvexe Funktion ist, enthält jede Umgebung von x eine konvexe Umgebung. Eine Nullumgebung ist absorbierend.

Mit V^* bezeichnen wir den *topologischen Dual* von V :

$$V^* = \{f : V \rightarrow \mathbb{R} \text{ linear} \mid f \text{ stetig bezüglich } \mathcal{T}_{\mathcal{P}}\}.$$

Nach dem Satz von Hahn-Banach ist V^* eine separierende Menge für V . Damit bildet (V, V^*) ein duales Paar. Auf V^* betrachten wir die lokalkonvexe Topologie, die durch die Auswertungen

$$\hat{v} : V^* \rightarrow [0, \infty), \quad f \mapsto |f(v)|$$

für $v \in V$ induziert wird. Für diese Topologie schreiben wir kurz: $\sigma(V^*, V)$. Wir bezeichnen sie als *schwach-*-Topologie*, falls eine Norm existiert, die $\mathcal{T}_{\mathcal{P}}$ induziert. Es gilt in diesem Fall:

$$(V^*, \sigma(V^*, V))^* = V.$$

Dabei enthält die Menge auf der linken Seite der Gleichung alle linearen Funktionale auf V^* , die stetig bezüglich der Topologie $\sigma(V^*, V)$ sind.

Es sei W ein weiterer lokalkonvexer Vektorraum über \mathbb{K} und $\varphi : V \rightarrow W$ linear und stetig. Dann bezeichnen wir mit

$$\varphi^* : W^* \rightarrow V^*, \quad f \mapsto f \circ \varphi$$

die *Adjungierte* von φ . Es ist leicht zu sehen, dass die Adjungierte stetig ist.

Der *Annihilator* eines abgeschlossenen linearen Teilraums $L \subseteq V$ ist

$$L^\perp := \{f \in V^* \mid \text{Für alle } l \in L \text{ gilt: } f(l) = 0\}.$$

Es gilt:

$$(L^*, \sigma(L^*, L)) \cong (V^*/L^\perp, \sigma(V^*, V)^\sim) \quad (3.2.1)$$

wobei \cong die Gleichheit der beiden topologischen Vektorräume und $\sigma(V^*, V)^\sim$ die durch $\sigma(V^*, V)$ induzierte Topologie auf V^*/L^\perp , definiert durch die separierende Familie von Halbnormen

$$\hat{v} : V^*/L^\perp \rightarrow [0, \infty), \quad f + L^\perp \mapsto |f(v)|$$

für $v \in L$, bezeichnet.

Proposition 3.2.1 - Adjungierte der Inklusion

Ist $L \subseteq V$ ein abgeschlossener linearer Teilraum und $\iota : L \rightarrow V$ die Inklusion, dann ist die Adjungierte ι^* gleich der Projektion $\pi_L : V^* \rightarrow V^*/L^\perp$. \square

Beweis. Die Adjungierte

$$\iota^* : V^* \rightarrow L^*, \quad f \mapsto [f \circ \iota : L \rightarrow \mathbb{R}, \quad l \mapsto f|_L(l)]$$

bildet $f \in V^*$ auf $f|_L \in L^*$ ab. Dieser Abbildung entspricht $f + L^\perp \in V^*/L^\perp$ gemäß Gleichung 3.2.1. \blacksquare

Bidualität von dualen Kegeln

An dieser Stelle führen wir eine Verallgemeinerung von Annihilatoren ein:

Definition 3.2.2 - Duale Kegel

Für eine beliebige Menge $M \subseteq V$ bezeichnet

$$M^\star := \{f \in V^* \mid \text{Für alle } m \in M \text{ gilt: } f(m) \geq 0\}$$

den zu M *dualen Kegel*. \square

Duale Kegel sind abgeschlossene Kegel in V^* . Der duale Kegel eines abgeschlossenen linearen Teilraums $L \subseteq V$ ist der Annihilator L^\perp .

Weiterhin können duale Kegel als Positivstellenmenge einer beliebigen Teilmenge des Duals $(V^*)^* = V$ interpretiert werden. Im Kontext der algebraischen Geometrie lässt die Bildung von Verschwindemengen der Verschwindeideale alle Zariski-abgeschlossenen Mengen invariant. Für den Dual eines dualen Kegels gilt ein vergleichbares Resultat:

Proposition 3.2.3 - Bidualität

Für eine Menge $M \subseteq V$ gilt:

- (i) $(\mathcal{K}(M))^\star = M^\star$,
- (ii) $(\text{cl}(M))^\star = M^\star$,
- (iii) $\text{cl}(\mathcal{K}(M)) = (M^\star)^\star$. □

Beweis. (i), (ii): Die Menge, auf der ein Element in V^* nicht negativ ist, bildet einen abgeschlossenen Kegel in V .

(iii): Wir zeigen die Aussage: $K = (K^\star)^\star$, falls K ein abgeschlossener Kegel in V ist. Die allgemeine Aussage folgt dann aus (i) und (ii). Zunächst gilt: $K \subseteq (K^\star)^\star$, da $k \in K$ eindeutig mit dem stetig linearen Funktional

$$\hat{k}: V^* \rightarrow \mathbb{R}, \quad f \mapsto f(k),$$

identifiziert werden kann und $\hat{k} \in (K^\star)^\star$ ist. Es bleibt die andere Inklusion zu zeigen. Sei $K \neq V$ und $x \in V \setminus K$. Nach einem funktionalanalytischen Trennungssatz gilt, dass $t \in \mathbb{R}$ und $\varphi \in V^*$ existieren mit

$$\varphi(x) < t < \varphi(k)$$

für alle $k \in K$. Da $0 \in K$ ist, folgt: $t < 0$. Es gilt also die Ungleichung

$$\hat{x}(\varphi) = \varphi(x) < 0 \leq \varphi(k).$$

Daraus folgt: $\hat{x} \notin (K^\star)^\star$. ■

Abgeschlossene Kegel sind also unter der Bildung des Duals invariant.

Das relative Innere

Das Innere einer konvexen Menge ist leer, wenn es einen echten affinen Teilraum gibt, in dem sie enthalten ist. Um in einem solchen Fall dennoch von einem „Inneren“ sprechen zu können, führen wir den Begriff des *relativen Inneren* ein:

Definition 3.2.4 - Relatives Inneres

Für eine Menge $M \subseteq V$ bezeichnet

$$V_M := \bigcap_{\substack{L \subseteq V \\ L \text{ ist abg. affiner Teilraum}}} L$$

die *affine Hülle* von M . Die affine Hülle sei mit der Teilraumtopologie ausgestattet. Weiterhin sei

$$\text{relin}(M) := \{m \in M \mid \text{Es gibt eine Umgebung } U \subseteq V_M \text{ von } m \text{ mit } U \subseteq M\}$$

das *relative Innere* von M . □

Proposition 3.2.5 - Ist $M \subseteq V$ eine Menge, dann gilt:

- (i) Die affine Hülle von M ist abgeschlossen und affin. Im Fall $0 \in M$ ist $V_M = \text{cl}(\text{span}(M))$, also insbesondere linear.
- (ii) Das relative Innere ist translationsinvariant: $\text{relin}(M) + v = \text{relin}(M + v)$ für $v \in V$.
- (iii) Falls $\text{relin}(M) \neq \emptyset$, enthält M ein Geradenstück.
- (iv) Ist M offen und nichtleer, gilt $V_M = V$.
- (v) Ist $\text{relin}(M) \neq \emptyset$, so ist $V_M = V$ genau dann wenn $\text{relin}(M) = \text{in}(M)$.
- (vi) Ist $\text{relin}(M) \neq \emptyset$ oder $M = \emptyset$, gilt $V_M = V_{\text{relin}(M)}$. □

Beweis. (i), (ii): Aus der Definition folgt, dass $(V_M) + v = V_{M+v}$ gilt. Ein affiner Teilraum ist genau dann ein linearer Teilraum, wenn die Null enthalten ist. Andernfalls betrachten wir $M' := M - m$ für ein $m \in M$ und benutzen die Translationsinvarianz.

(iii): Dies folgt aus (i).

(iv): Wir nehmen an, dass M eine Nullumgebung ist. Da M absorbierend ist, gibt es für $v \in V$ einen Faktor $\lambda \in \mathbb{R}$, $\lambda \neq 0$, mit $\lambda v \in M \subseteq V_M$. Also ist $V \subseteq V_M$.

(v): Die erste Implikation folgt direkt aus der Definition. Falls $\text{relin}(M) = \text{in}(M)$ nichtleer ist, enthält M eine offene Menge. Damit gilt nach (iv): $V_M = V$.

(vi): Ist M leer, folgt die Aussage sofort. Es habe nun M ein nichtleeres relatives

Inneres. Im Fall $V_M = V$ gilt $\text{relin}(M) = \text{in}(M) \neq \emptyset$. Das Innere von M enthält also eine in V nichtleere und offene Menge. Mit (iv) folgt, dass $V_{\text{relin}(M)} = V_{\text{in}(M)} = V$. Im allgemeinen Fall ist das relative Innere von M gleich dem Inneren $\text{in}_{V_M}(M)$ von M bezüglich der Teilraumtopologie auf V_M . Dieses enthält eine bezüglich V_M nichtleere offene Menge. Also ist $V_{\text{relin}(M)} = V_{\text{in}_{V_M}(M)} = (V_M)_{\text{in}_{V_M}(M)} = V_M$. ■

Das relative Innere konvexer Mengen

Der Abschluss einer konvexen Menge $C \subseteq V$ ist als Schnitt von Summen konvexer Mengen konvex:

$$\text{cl}(C) = \bigcap_{\substack{\varepsilon > 0 \\ p_1, \dots, p_k \in \mathcal{P}}} C + \varepsilon B_{1,p_1, \dots, p_k}(0).$$

Das relative Innere ist auch konvex:

Lemma 3.2.6 - Konvexität des relativen Inneren

Sei $C \subseteq V$ eine konvexe Menge, $x \in \text{relin}(C)$ und $y \in \text{cl}(C)$. Dann gilt:

$$(1 - \lambda)x + \lambda y \in \text{relin}(C)$$

für $0 \leq \lambda < 1$. □

Beweis. Nach Proposition 3.2.5 genügt es, den Fall $V_C = V$ zu betrachten. Dann gilt: $\text{relin}(C) = \text{in}(C)$. Sei $\lambda \in [0, 1)$, $x \in \text{relin}(C)$ und $y \in \text{cl}(C)$. Wir wählen eine Teilmenge $p_1, \dots, p_k \in \mathcal{P}$ und $\delta > 0$, sodass $B_{\delta, p_1, \dots, p_k}(x) \subseteq \text{relin}(C)$. Da y im Abschluss liegt, ist in jeder Umgebung von y ein Element von C enthalten. Es gilt insbesondere $y \in C + \varepsilon B$ für alle $\varepsilon > 0$ und $B := B_{1, p_1, \dots, p_k}(0)$. Also ist

$$\begin{aligned} (1 - \lambda)x + \lambda y + \varepsilon B &\subseteq (1 - \lambda)x + \lambda(C + \varepsilon B) + \varepsilon B \\ &= (1 - \lambda)(x + \varepsilon(1 + \lambda)(1 - \lambda)^{-1}B) + \lambda C \\ &\subseteq (1 - \lambda)C + \lambda C = C \end{aligned}$$

für einen genügend kleinen Wert von ε . Also ist $(1 - \lambda)x + \lambda y \in \text{relin}(C)$. ■

Diese Folgerung ergänzt die Überlegung, dass konvexe Hüllen abgeschlossene Mengen im Allgemeinen nicht invariant lassen, siehe Abschnitt 3.1, um eine positive Aussage für offene Mengen:

Korollar 3.2.7 - Die konvexe Hülle einer offenen Menge ist offen. □

Beweis. Sei $U \subseteq V$ offen und nichtleer. Dann ist $V_U = V$ und $\text{co}(U) = R \cup \text{in}(\text{co}(U))$, wobei $R := \text{co}(U) \setminus \text{in}(\text{co}(U))$ den Rand der konvexen Hülle von U bezeichnet. Es seien $x, y \in \text{co}(U)$ und $0 < \lambda < 1$, sodass $\lambda x + (1 - \lambda)y \in R$. Nach Lemma 3.2.6 muss sowohl x als auch y Element des Randes sein. Damit ist $\text{co}(U) \setminus R$ wieder eine konvexe Obermenge von U . Es folgt: $R = \emptyset$. ■

Lemma 3.2.8 - Eine nichtleere konvexe Menge in \mathbb{R}^n besitzt ein nichtleeres relatives Inneres. □

Beweis. Wir nehmen zunächst wieder an, dass $V = V_C$ gilt, und führen den allgemeinen Fall auf diesen zurück. Es existiert eine Teilmenge $c_0, c_1, \dots, c_n \in C$, sodass das System $c_1 - c_0, \dots, c_n - c_0$ linear unabhängig ist. Die konvexe Hülle der Punkte c_0, c_1, \dots, c_n ist wieder in C enthalten. Wenden wir eine geeignete affine Transformation $x \mapsto Ax + b$ für $A \subseteq \mathcal{M}_n(\mathbb{R})$, $b \in \mathbb{R}^n$, auf diese Menge an, können wir annehmen, dass die Ecken dieser konvexen Menge mit den kanonischen Einheitsvektoren übereinstimmen. Daran sehen wir leicht, dass die Menge ein nichtleeres Inneres besitzt. ■

Diese Aussage gilt im Allgemeinen nicht mehr, wenn der Vektorraum nicht von endlicher Dimension ist. Konvexe Mengen können also in gewisser Weise „ausgedünnt“ werden:

Beispiel 3.2.9 Wir setzen $V := \ell^2(\mathbb{N})$ als den Raum der reellwertigen quadratsummierbaren Folgen, versehen mit der 2-Norm $\|\cdot\|_2$, und $C := \mathcal{F}(\mathbb{N})$ als den Unterraum der finiten Folgen. Dann ist $\text{cl}(C) = V$, also $V_C = V$.

Behauptung: Es ist $\text{in}(C) = \emptyset$.

Beweis: Für $f = (f_n)_{n \in \mathbb{N}} \in C$ und $\varepsilon > 0$ existiert eine Folge $\tilde{f} := \left(f_n + \varepsilon \cdot \frac{\sqrt{6}}{\pi} \cdot \frac{1}{n}\right)_{n \in \mathbb{N}}$, sodass \tilde{f} keine finite Folge ist, aber $\|f - \tilde{f}\|_2 = \varepsilon$ gilt. ◇

Da $\text{relin}(C) = \text{in}(C)$ gilt, ist das relative Innere der finiten Folgen leer. □

In speziellen Fällen kann jedoch gesichert werden, dass ein Element im Inneren existiert. Nach [Bro] folgt aus dem Baireschen Kategoriensatz, dass eine absolutkonvexe, abgeschlossene und absorbierende Teilmenge eines Banachraums zumindest den Nullpunkt im Inneren besitzt. Wir benötigen dennoch stärkere Resultate.

Satz 3.2.10 - Abschluss und relatives Inneres

Für eine konvexe Menge $C \subseteq \mathbb{R}^n$ gilt:

- (i) $\text{cl}(\text{relin}(C)) = \text{cl}(C)$,
- (ii) $\text{relin}(\text{cl}(C)) = \text{relin}(C)$. □

Beweis. (i): Die Inklusion $\text{cl}(\text{relin}(C)) \subseteq \text{cl}(C)$ ist klar. Es bleibt die umgekehrte Inklusion zu zeigen. Wir nehmen an, dass C nicht leer ist. Es sei $y \in \text{cl}(C)$. Nach Lemma 3.2.8 existiert ein $x \in \text{relin}(C)$. Alle Konvexkombinationen der Form

$$\lambda y + (1 - \lambda)x, \quad 0 \leq \lambda < 1,$$

sind nach Lemma 3.2.6 im relativen Inneren enthalten. Damit ist y im Abschluss des relativen Inneren.

(ii): Die Inklusion $\text{relin}(\text{cl}(C)) \supseteq \text{relin}(C)$ ist klar. Wir zeigen die umgekehrte Inklusion. Es besitze C mindestens zwei Punkte. Dann können wir annehmen, dass $z \in \text{relin}(\text{cl}(C))$ und $x \in \text{relin}(C)$ existieren mit $x \neq z$. Weiterhin sei $\mu > 1$ so gewählt, dass

$$y := (1 - \mu)x + \mu z = z - (\mu - 1)(x - z) \in \text{relin}(\text{cl}(C))$$

gilt. Dies ist möglich, wenn $\mu - 1$ genügend klein ist. Mit der Wahl $\lambda := \mu^{-1}$ ist nun

$$z = (1 - \lambda)x + \lambda y$$

und $0 < \lambda < 1$. Damit ist $z \in \text{relin}(C)$ nach Lemma 3.2.6. ■

Es existieren normierte Räume, für die diese Aussage nicht mehr gültig ist. Wie Beispiel 3.2.9 zeigt, kann das relative Innere leer sein, obwohl die betrachtete konvexe Menge nicht leer ist.

Korollar 3.2.11 - Schnitte von konvexen Mengen mit Teilräumen

Ist $C \subseteq \mathbb{R}^n$ konvex und $L \subseteq \mathbb{R}^n$ ein affiner Teilraum, sodass $\text{relin}(C) \cap L \neq \emptyset$ ist, dann gilt:

- (i) $\text{relin}(C \cap L) = \text{relin}(C) \cap L$,
- (ii) $\text{cl}(C \cap L) = \text{cl}(C) \cap L$. □

Beweis. Es sei $x \in \text{relin}(C) \cap L$ und $y \in \text{cl}(C) \cap L$. Nach Lemma 3.2.6 ist für jeden Faktor $0 \leq \lambda < 1$ die Konvexkombination $(1 - \lambda)x + \lambda y$ Element von $\text{relin}(C) \cap L$. Also ist $y \in \text{cl}(\text{relin}(C) \cap L)$ und es gilt

$$\text{cl}(C) \cap L \subseteq \text{cl}(\text{relin}(C) \cap L) \subseteq \text{cl}(C \cap L) \subseteq \text{cl}(C) \cap L.$$

Damit ist die zweite Aussage gezeigt und wir wissen, dass $\text{relin}(C) \cap L$ und $C \cap L$ den gleichen Abschluss besitzen. Nach Satz 3.2.10 besitzen sie auch das gleiche relative Innere. Es gilt also

$$\text{relin}(C \cap L) = \text{relin}(\text{relin}(C) \cap L) \subseteq \text{relin}(C) \cap L.$$

Um schließlich die Inklusion $\text{relin}(C) \cap L \subseteq \text{relin}(C \cap L)$ zu zeigen, wählen wir eine Umgebung U_x um x in $(\mathbb{R}^n)_C$ mit $U_x \subseteq C$. Es gilt insbesondere $x \in (\mathbb{R}^n)_{C \cap L}$. Die Menge $U_x \cap (\mathbb{R}^n)_{C \cap L}$ ist eine Umgebung um x in $C \cap L \subseteq (\mathbb{R}^n)_{C \cap L}$. ■

Beispiel 3.2.12 Wie in Beispiel 3.2.9 seien $V := \ell^2(\mathbb{N})$ und $C := \mathcal{F}(\mathbb{N})$. Weiterhin sei $L := \text{span}\left(\left(\frac{1}{n}\right)_{n \in \mathbb{N}}\right) \subseteq V$. Dann ist $\text{cl}(C \cap L) = \{0\} \neq L = \text{cl}(C) \cap L$. \square

Kegelschnitte

Satz 3.2.13 - Kegelschnitte und deren projizierte Duale

Es sei $V := \mathbb{R}^n$, $L \subseteq V$ ein abgeschlossener linearer Teilraum und $K \subseteq V$ ein Kegel mit $L \cap \text{relin}(K) \neq \emptyset$. Dann gilt:

- (i) $(K \cap L)^\star = \text{cl}(K^\star + L^\perp) \subseteq V^\star$,
- (ii) $\text{cl}(\pi_L((K \cap L)^\star)) = \text{cl}(\pi_L(K^\star)) \subseteq V^\star/L^\perp$. \square

Beweis. (i): Der Bidual von V ist V selbst. Weiterhin gibt es für ein $x \in V \setminus L$ ein Funktional $l \in L^\perp$ mit $l(x) \neq 0$. Also existiert für $f \in K^\star$ ein Element des Annihilators $\tilde{l} \in L^\perp$ mit $f(x) + \tilde{l}(x) < 0$. Damit erhalten wir mit Proposition 3.2.3 die Gleichung

$$\begin{aligned} (\text{cl}(K^\star + L^\perp))^\star &= \{x \in V \mid f(x) + l(x) \geq 0 \text{ für alle } f \in K^\star, l \in L^\perp\} \\ &= \{x \in L \mid f(x) \geq 0 \text{ für alle } f \in K^\star\} \\ &= (K^\star)^\star \cap L = \text{cl}(K) \cap L \\ &= \text{cl}(K \cap L). \end{aligned}$$

Die letzte Gleichung folgt mit Korollar 3.2.11.

(ii): Zu zeigen ist mit (i): $\text{cl}(\pi_L(\text{cl}(K^\star + L^\perp))) = \text{cl}(\pi_L(K^\star))$. Da die Projektion auf L^\perp stetig ist, ist die Menge auf der linken Seite der Gleichung in der auf der rechten Seite enthalten. Es bleibt die umgekehrte Inklusion zu zeigen. Ist $x \in K^\star$, so ist $\pi_L(x) = \pi_L(x + l)$ für alle $l \in L^\perp$. \blacksquare

Die Forderung, dass der lineare Teilraum und das relative Innere des Kegels mindestens einen Punkt gemeinsam haben müssen, ist berechtigt:

Beispiel 3.2.14 Es seien $V := \mathbb{R}^3$ und $L := \text{span}(e_1, e_2)$. Dann ist $L^\perp = \text{span}(e_3)$. Es sei ein Kegel gegeben durch

$$\begin{aligned} K &:= \{(k_1, k_2, 0) \in \mathbb{R}^3 \mid k_1 > 0, k_2 > 0\} \cup \{(0, 0)\}, \text{ dann ist} \\ K^\star &= \{(x, y, z) \in \mathbb{R}^3 \mid \langle (x, y, z), (k_1, k_2, 0) \rangle \geq 0 \text{ für alle } k_1 \geq 0, k_2 \geq 0\} \\ &= \{(x, y, z) \in \mathbb{R}^3 \mid xk_1 \geq -yk_2 \text{ für alle } k_1 \geq 0, k_2 \geq 0\} \\ &= \mathbb{R}_0^+ e_1 + \mathbb{R}_0^+ e_2 + \mathbb{R} e_3, \end{aligned}$$

also ist

$$K^\star + L^\perp = K^\star = (K \cap L)^\star.$$

Wählen wir $L' := \text{span}(e_1, e_3)$, ist $K \cap L' = \{0\}$ und

$$K^\star + L'^\perp = \mathbb{R}_0^+ e_1 + \mathbb{R} e_2 + \mathbb{R} e_3 \neq \mathbb{R}^3 = (K \cap L')^\star.$$

Hier wurde die Voraussetzung verletzt. Es gilt allerdings

$$K^\star + L'^\perp = (\text{cl}(K) \cap L')^\star$$

nach dem nächsten Korollar. □

Korollar 3.2.15 - Projektionen von Kegelschnitten

Ist V ein lokalkonvexer Vektorraum, $L \subseteq V$ ein abgeschlossener linearer Teilraum und $K \subseteq V$ ein Kegel, so gilt:

- (i) $\text{cl}(\pi_L((\text{cl}(K) \cap L)^\star)) = \text{cl}(\pi_L(K^\star))$,
- (ii) $\pi_L((K \cap L)^\star) = \{l \in L^\star \mid l(x) \geq 0 \text{ für alle } x \in K \cap L\}$. □

Beweis. Wir lehnen den Beweis von (i) an den Beweis von Satz 3.2.13 an, indem wir geringfügige Änderungen vornehmen. Zunächst stellen wir fest, dass wir die Gleichungsfolge in (i) bis auf die letzte Gleichung übernehmen können. Wir erhalten:

$$\text{cl}(K^\star + L^\perp) = (\text{cl}(K) \cap L)^\star.$$

Auch die Argumentation in (ii) kann übernommen werden. Es gilt also:

$$\text{cl}(\pi_L(\text{cl}(K^\star + L^\perp))) = \text{cl}(\pi_L(K^\star)).$$

Die erste Gleichung ergibt sich, indem wir die Ergebnisse zusammenbringen. Aus der Identifikation der beiden Räume V^\star/L^\perp und L^\star ergibt sich sofort die zweite Gleichung unter (ii). ■

Es bleibt anzumerken, dass die Summe zweier abgeschlossener Mengen nicht immer abgeschlossen ist:

Die Mengen $A_1 := \{(x, 1/x) \mid x > 0\}$ und $A_2 := \{(x, -1/x) \mid x < 0\}$ sind abgeschlossen in \mathbb{R}^2 . Der Punkt $(0, 0)$ ist durch die Folge $((0, 1/n))_{n \in \mathbb{N}} \subseteq (A_1 + A_2)$ approximierbar, aber in der Summe nicht enthalten.

4 Thetakörper

Die konvexe Hülle einer Menge ist ein Schnitt von affinen Halbräumen. Durch Bestimmung dieser Halbräume kann geprüft werden, ob ein Element zur konvexen Hülle gehört oder nicht. Kann ein Halbraum gefunden werden, in dem es nicht liegt, ist eine Zugehörigkeit ausgeschlossen. Im anderen Fall kann jedoch nach endlich vielen Schritten keine hinreichende Aussage getroffen werden.

Ziel dieses Kapitels ist, eine Methode zu finden, die das Ausschlusskriterium für die konvexe Hülle einer reellen algebraischen Varietät vereinfacht. Wir finden eine Kette von konvexen Obermengen der Varietät, sodass der Schnitt aller dieser Mengen die konvexe Hülle ergibt. Falls ein fest gewähltes Element außerhalb einer solchen Menge liegt, kann gleichzeitig ausgeschlossen werden, dass es zur Hülle gehört. Dabei stellt es sich als praktikabel heraus, zu überprüfen, ob es in einer der Obermengen liegt.

Die Methode basiert darauf, nur bestimmte affine Halbräume zu schneiden. Für einen fixen Wert k betrachten wir die Polynome, die affin-linear sind und als Summe von Quadraten von Polynomen bis zum Grad k plus einem Element aus der Verschwindemenge geschrieben werden können. Diese sind auf der Varietät auf jeden Fall nicht negativ. Dadurch erhalten wir eine Obermenge der konvexen Hülle der Varietät, den sogenannten *k-ten Thetakörper*.

Im Folgenden sehen wir, dass die Polynome, die Thetakörper ausschneiden, bestimmte Strukturen und Eigenschaften besitzen, die den Umgang mit ihnen erleichtern.

Im ersten Abschnitt führen wir Thetakörper ein. Im Anschluss arbeiten wir eine Darstellung von Thetakörpern als projizierte Spektraeder aus.

Elemente in einem Thetakörper vom Grad k sind Elemente eines Duals: Sie wirken durch Auswertung auf die Polynome, die affin-linear und eine Summe von Quadraten bis zum Grad k sind, als duale Abbildung. Dabei ergibt sich ein positiver Wert. Thetakörper sind also Teilmengen des dualen Kegels dieser Polynome.

Im zweiten Abschnitt betrachten wir Polynome, die als eine Summe von quadratischen Polynomen geschrieben werden können, die sogenannten *Sos-Polynome*. Das Ziel dieses Abschnittes ist, den erwähnten Dual als Projektion von Elementen aus dem Dual der Sos-Polynome bis zum Grad $2k$ zu schreiben. Dieser duale Kegel hat die Eigenschaft, dass er als Spektraeder geschrieben werden kann, da die Positivität der dualen Abbildung in Positivität von Matrizen übertragen werden kann. Es stellt sich also die Frage, ob Elemente des dualen Kegels der affin-linearen Sos-Polynome, und damit insbesondere Elemente des Thetakörpers, auf den Dual der Sos-Polynome fortgesetzt werden können.

Wir sehen, dass dies in speziellen Fällen möglich ist. Haben wir die Fortsetzbarkeit im zweiten Abschnitt untersucht, werden wir die Spektraederdarstellung im dritten Abschnitt konstruieren.

Im vierten Abschnitt beleuchten wir die Fortsetzbarkeit von Elementen eines Thetakörpers näher. Wir sehen, dass konvergente Thetakörper folgende Eigenschaft besitzen: Je näher ein Element an der konvexen Hülle der Varietät liegt, desto größer kann der Grad k gewählt werden, sodass es im k -ten Thetakörper liegt, und desto größer ist der Teilraum, für den das Element zum dualen Kegel der Sos-Polynome gehört. Die Elemente, die in allen Thetakörpern liegen, können zu *Zuständen* auf den stetigen Funktionen über der Varietät fortgesetzt werden. Wir beleuchten die Fortsetzbarkeit näher und bringen sie in Zusammenhang mit verschiedenen Begriffen der „Positivität“.

Die Betrachtungen der ersten drei Abschnitte entnehmen wir [BPT]. Der letzte Abschnitt enthält ein Resultat aus [Tak], Kapitel IV. Der Inhalt dieses Kapitels baut auf den Inhalt aller drei vorangehenden, einführenden Kapitel auf.

4.1 Thetakörper als Kette konvexer Mengen

Im Folgenden sei $I \subseteq \mathbb{R}[X_1, \dots, X_n]$ ein Ideal.

Konvexe Mengen und Trennung durch Halbräume

Funktionalanalytische Trennungssätze lehren uns, dass konvexe Mengen Schnitte von Halbräumen sind. Ist $S \subseteq \mathbb{R}^n$ eine Menge, gilt:

$$\begin{aligned} \text{cl}(\text{co}(S)) &= \bigcap_{\substack{l \in \mathbb{R}[X_1, \dots, X_n]_1 \\ l(S) \geq 0}} \{x \in \mathbb{R}^n \mid l(x) \geq 0\} \\ &= \bigcap_{\substack{l \in \mathbb{R}[X_1, \dots, X_n]_1 \\ l(S) > 0}} \{x \in \mathbb{R}^n \mid l(x) \geq 0\}, \end{aligned}$$

wobei $\mathbb{R}[X_1, \dots, X_n]_1$ die Menge aller affin-linearen Polynome in n Variablen bezeichnet, siehe Abschnitt 1.3.

Betrachtungen über das Innere und den Abschluss konvexer Hüllen, die wir in Kapitel 3 angestellt haben, führen zu spezifischeren Darstellungen. Ist S kompakt, dann auch $\text{co}(S)$. Wir können in diesem Fall in der vorigen Gleichung auf die Bildung des Abschluss verzichten. Ist S offen, ist auch $\text{co}(S)$ offen und es gilt:

$$\text{co}(S) = \bigcap_{\substack{l \in \mathbb{R}[X_1, \dots, X_n]_1 \\ l(S) > 0}} \{x \in \mathbb{R}^n \mid l(x) > 0\}.$$

Es ist also möglich, die konvexe Hülle der reellen algebraischen Varietät $\mathcal{Z}(I)$ durch affin-lineare Polynome auszuschneiden. Dafür werden jedoch *alle* Polynome benötigt, die affin-linear und nicht negativ auf $\mathcal{Z}(I)$ sind. Stellen wir noch stärkere Restriktionen an die Polynome, ergibt der Schnitt eine Obermenge des ursprünglichen Schnittes. Im Folgenden überlegen wir, welche affin-linearen Polynome nicht negativ auf $\mathcal{Z}(I)$ sind, um sinnvolle Restriktionen zu finden.

Summen von Quadraten und das Verschwindeideal

Die Auswertung eines quadratischen Polynoms f^2 für $f \in \mathbb{R}[X_1, \dots, X_n]$ ist nicht negativ auf \mathbb{R}^n . Auch eine Summe von quadratischen Polynomen ist nicht negativ. Sie heißt eine *Summe von Quadraten* (englisch: *sum of squares*) oder *Sos-Polynom*. Die Menge aller Summen von Quadraten ist ein Kegel im Vektorraum $\mathbb{R}[X_1, \dots, X_n]$ und bildet den kleinsten Kegel des Rings $\mathbb{R}[X_1, \dots, X_n]$. Siehe hierzu Abschnitt 3.1, Seite 68, und Abschnitt 2.1, Seite 24.

Eine Summe von Quadraten ist nicht negativ auf $\mathcal{Z}(I)$. Weiterhin sind Polynome, die im Verschwindeideal $\{f \in \mathbb{R}[X_1, \dots, X_n] \mid f(v) = 0 \text{ für alle } v \in \mathcal{Z}(I)\}$ von $\mathcal{Z}(I)$ liegen, nicht negativ auf $\mathcal{Z}(I)$. Insbesondere gilt dies für Polynome in I . Im Allgemeinen ist ein Polynom in allen diesen Fällen nicht affin-linear. Die Summe zweier solcher Polynome kann jedoch affin-linear sein. Diesen Fall betrachten wir näher.

Definition 4.1.1 - Summe von Quadraten modulo einem Ideal

Es sei $k \in \mathbb{N}$. Ein Polynom $l \in \mathbb{R}[X_1, \dots, X_n]$ heißt *k-sos-mod I*, falls l von der Form

$$l = \sum_{i=1}^r h_i^2 + h$$

ist mit $h_1, \dots, h_r \in \mathbb{R}[X_1, \dots, X_n]_k$ und $h \in I$. □

Beispiel 4.1.2 Das Polynom $X^2 + X^5 \in \mathbb{R}[X]$ ist 1-sos-mod $\langle X^4 \rangle$. □

Thetakörper als Schnitte von Halbräumen

Die Menge aller Punkte, auf der affin lineare *k-sos-mod I*-Polynome nicht negativ sind, stellen wir heraus:

Definition 4.1.3 - Thetakörper

Es sei $k \in \mathbb{N}$. Der *k-te Thetakörper* von I ist die Menge

$$\mathcal{T}_k := \{x \in \mathbb{R}^n \mid l(x) \geq 0 \text{ für alle } l \in \mathbb{R}[X_1, \dots, X_n]_1, l \text{ ist } k\text{-sos-mod } I\}.$$

Die Zahl k bezeichnet den *Grad* des Thetakörpers. □

Ein Thetakörper bildet eine abgeschlossene und konvexe Obermenge von $\mathcal{Z}(I)$. Ist ein Polynom k -sos-mod I , so ist es auch $(k + 1)$ -sos-mod I . Entsprechend ist

$$\mathcal{T}_1 \supseteq \mathcal{T}_2 \supseteq \dots \supseteq \mathcal{T}_k \supseteq \mathcal{T}_{k+1} \supseteq \dots \supseteq \text{cl}(\text{co}(\mathcal{Z}(I)))$$

eine absteigende Kette von Obermengen der reellen algebraischen Varietät $\mathcal{Z}(I)$.

Definition 4.1.4 - Konvergenz von Thetakörpern

Falls

$$\bigcap_{k=1}^{\infty} \mathcal{T}_k = \text{cl}(\text{co}(\mathcal{Z}(I)))$$

gilt, sprechen wir von der *Konvergenz der Thetakörper* von I . □

Die Frage nach der Konvergenz von Thetakörpern läuft im Allgemeinen auf die Frage hinaus, ob genügend viele Polynome, die affin-linear und auf der Varietät nicht negativ sind, als Summe von Quadraten geschrieben werden können. Im Falle der Beschränktheit der Varietät kann als direktes Resultat des Satzes von Schmüdgen, siehe Kapitel 2, die Konvergenz gezeigt werden. Es gibt jedoch auch Fälle, in denen keine Konvergenz gegeben ist. Ein Beispiel dafür gibt [BPT] an.

Satz 4.1.5 - Konvergenz von Thetakörpern

Ist $\mathcal{Z}(I)$ kompakt, so gilt:

$$\bigcap_{k=1}^{\infty} \mathcal{T}_k = \text{co}(\mathcal{Z}(I)).$$

□

Beweis. Nach dem Basissatz von Hilbert gibt es Polynome $f_1, \dots, f_r \in R[X_1, \dots, X_n]$ mit $I = \langle f_1, \dots, f_r \rangle$. Anlehnend an die Notation aus Kapitel 2 bezeichnen wir mit P den Kegel (siehe Abschnitt 2.1), der von den Polynomen $f_1, \dots, f_r, -f_1, \dots, -f_r$ erzeugt wird, und mit $\mathcal{W}(P)$ die Positivstellenmenge von P . Nach den Überlegungen, die wir am Anfang dieses Abschnitts angestellt haben, gibt es für $y \notin \text{co}(\mathcal{Z}(I))$ ein affin lineares Polynom, welches auf $\text{co}(\mathcal{Z}(I))$ echt positiv und auf y echt negativ ist. Sei $x \in \bigcap_{k \in \mathbb{N}} \mathcal{T}_k$ und $l \in \mathbb{R}[X_1, \dots, X_n]_1$, sodass l auf $\text{co}(\mathcal{Z}(I))$ echt positiv ist. Dann ist l insbesondere auf $\mathcal{Z}(I) = \mathcal{W}(P)$ echt positiv. Nach dem Satz von Schmüdgen, Satz 2.4.10 auf Seite 59, ist $l \in P$ und insbesondere k -sos-mod I für ein $k \in \mathbb{N}$. Nach Voraussetzung gilt also $l(x) \geq 0$. Es folgt: $x \in \text{co}(\mathcal{Z}(I))$. ■

Zum Abschluss illustrieren wir ein einfaches Beispiel. In Kapitel 6 behandeln wir interessante Beispiele.

Beispiel 4.1.6 Die Verschwindemenge des Ideals $I := \langle X^2 + 1 \rangle \subseteq \mathbb{R}[X]$ ist leer. Für jeden Wert $a \in \mathbb{R}$ ist

$$(X + a)^2 = 2aX + a^2 - 1 + (X^2 + 1).$$

Damit ist $l_a := 2aX + a^2 - 1$ ein Polynom, welches 1-sos-mod I ist. Die Positivstellenmenge von $l_0 = -1$ ist leer. Damit gilt: $\mathcal{T}_1 = \emptyset$. \square

4.2 Thetakörper als projizierte duale Kegel

In diesem Abschnitt sei $I \subseteq \mathbb{R}[X_1, \dots, X_n]$ ein Ideal, welches keine nicht-trivialen affin-linearen Polynome enthält, und $k \in \mathbb{N}$ fest gewählt.

Kegel aus Summen von Quadraten im Polynomring

Notation. Der wichtigste Kegel, mit dem wir uns in diesem Kapitel beschäftigen, ist der Kegel der quadratischen Polynome. Wir schreiben daher:

$$\mathcal{K} := \mathcal{K}_{\mathbb{R}[X_1, \dots, X_n]} = \{f \in \mathbb{R}[X_1, \dots, X_n] \mid f \text{ ist Sos-Polynom}\}$$

und erinnern dabei an die Notation in Kapitel 2, Abschnitt 2.1. Der Kegel, der von den quadratischen Polynomen, die sich mit Polynomen vom Grad kleiner gleich k bilden lassen, erzeugt wird, sei bezeichnet durch

$$\begin{aligned} \mathcal{K}^k &:= \left\{ f \in \mathbb{R}[X_1, \dots, X_n] \mid f = \sum_{i=1}^r h_i^2 \text{ mit } h_1, \dots, h_r \in \mathbb{R}[X_1, \dots, X_n]_k \right\} \\ &= \{f \in \mathbb{R}[X_1, \dots, X_n] \mid f \text{ ist Sos-Polynom und } \deg(f) \leq 2k\} = \mathcal{K}_{2k}, \end{aligned}$$

siehe Kapitel 1, Abschnitt 1.3. Betrachten wir Polynome in \mathcal{K}^k modulo I , erhalten wir die Menge

$$\mathcal{K}^k(I) := \mathcal{K}^k/I = \{f + I \mid f \in \mathbb{R}[X_1, \dots, X_n], f \text{ ist } k\text{-sos-mod } I\}.$$

Eine Teilmenge davon ist die Menge

$$\begin{aligned} \mathcal{K}^{k,1}(I) &:= \{f + I \mid f \in \mathbb{R}[X_1, \dots, X_n]_1 \text{ ist } k\text{-sos-mod } I\} \\ &= \mathcal{K}^k(I) \cap \mathbb{R}[X_1, \dots, X_n]_1/I. \end{aligned}$$

Die affin-linearen Polynome und ihr Dual

Wir können $\mathbb{R}[X_1, \dots, X_n]/I$ im Sinne von Kapitel 1, Abschnitt 1.3, als Vektorraum mit Standardbasis \mathcal{B} auffassen. Hat die Basis eine unendliche Länge, identifizieren wir $\mathbb{R}[X_1, \dots, X_n]/I$ mit den finiten Folgen $\mathcal{F}(\mathbb{N})$ als Unterraum des Hilbertraums der reellwertigen quadratsummierbaren Folgen $\ell^2(\mathbb{N})$, versehen mit der 2-Norm. Hat die Basis eine endliche Länge, identifizieren wir $\mathbb{R}[X_1, \dots, X_n]/I$ mit dem euklidischen Vektorraum \mathbb{R}^m . Ein Polynom $\sum_{b \in \mathcal{B}} f_b b \in \mathbb{R}[X_1, \dots, X_n]/I$ identifizieren wir mit den Koordinaten $(f_b)_{b \in \mathcal{B}} \subseteq \mathbb{R}$ bezüglich dieser Basis.

Es bezeichne $V := \mathbb{R}[X_1, \dots, X_n]_{2k}/I$ den Raum der Polynome bis zum Grad $2k$ modulo I .

Der Unterraum $L := \mathbb{R}[X_1, \dots, X_n]_1/I$ von V ist isomorph zu \mathbb{R}^{n+1} , da I nach Voraussetzung keine nicht-trivialen affin-linearen Polynome enthält. Siehe hierzu Bemerkung 1.3.9 auf Seite 17. Ein Element $\varphi \in L^*$ ist mit dem Vektor

$$v_\varphi := (\varphi(1+I), \varphi(X_1+I), \dots, \varphi(X_n+I)) \in \mathbb{R}^{n+1}$$

identifizierbar. Die duale Abbildung φ ist also von der Gestalt

$$\begin{aligned} \varphi &= \langle v_\varphi, \cdot \rangle: L \rightarrow \mathbb{R}, \\ \varphi(f) &= \langle v_\varphi, (f_{1+I}, f_{X_1+I}, \dots, f_{X_n+I}) \rangle \\ &= \bar{f}^G(\varphi(X_1+I), \dots, \varphi(X_n+I)) + f_{1+I} \cdot (\varphi(1+I) - 1) \end{aligned}$$

für alle $f = f_{1+I}(1+I) + f_{X_1+I}(X_1+I) + \dots + f_{X_n+I}(X_n+I) \in \mathbb{R}[X_1, \dots, X_n]_1/I$ und eine Gröbnerbasis G von I nach Proposition 1.3.2. Im Fall $\varphi(1+I) = 1$ gilt die Gleichung $\varphi(f) = \bar{f}^G(\varphi(X_1+I), \dots, \varphi(X_n+I))$.

Zusammenfassend erhalten wir folgende Inklusionen:

$$\begin{array}{ccc} V = \mathbb{R}[X_1, \dots, X_n]_{2k}/I & \xrightarrow{\pi} & \mathbb{R}[X_1, \dots, X_n]_1/I = L \\ \cup & & \cup \\ C := \mathcal{K}^k(I) & & \mathcal{K}^{k,1}(I) = C \cap L \end{array}$$

Dabei bezeichnet $\pi: \mathbb{R}[X_1, \dots, X_n]/I \rightarrow L$ die orthogonale Projektion auf L .

Bemerkung 4.2.1 Im Allgemeinen ist die Inklusion $C \cap L \subseteq \pi(C)$ echt. Betrachten wir das Ideal $I := \{0\} \subseteq \mathbb{R}[X]$ und das quadratische Polynom $f := (X+2)^2 \in \mathcal{K}^1$, so ist $\pi(f) = 4X+4$ nicht 1-sos-mod I . \square

Duale Kegel von Summen von Quadraten

Notation. Den dualen Kegel von $\mathcal{K}^{k,1}(I) = C \cap L$ in L bezeichnen wir mit

$$\mathcal{D} := \{\varphi \in L^* \mid \varphi(f) \geq 0 \text{ für alle } f \in C \cap L\}$$

und den dualen Kegel von $\mathcal{K}^k(I) = C$ in V mit

$$\hat{\mathcal{D}} := \{\varphi \in V^* \mid \varphi(f) \geq 0 \text{ für alle } f \in C\}.$$

Wie im zweiten Teilabschnitt bemerkt, sind Elemente in $\hat{\mathcal{D}}$, die das erste Basiselement auf Eins abbilden, Punktauswertungen, wenn man sie als Elemente von L^* auffasst. Sie sind bezeichnet durch

$$\hat{\mathcal{D}}_A := \left\{ (\varphi(X_1 + I), \dots, \varphi(X_n + I)) \mid \varphi \in \hat{\mathcal{D}}, \varphi(1 + I) = 1 \right\}.$$

Es ist zu beachten, dass die dualen Kegel bezüglich verschiedener Räume gebildet werden. Daher verzichten wir auf das Symbol \star , das wir in Kapitel 3 für den dualen Kegel eingeführt haben.

Thetakörper als projizierte Kegel

Es ist möglich, Elemente des Thetakörpers \mathcal{T}_k als duale Abbildung auf $\mathcal{K}^{k,1}(I) \subseteq L$ aufzufassen. Ist $x \in \mathcal{T}_k$, so gilt für $\langle (1, x), \cdot \rangle \in L^*$:

$$\langle (1, x), f \rangle = \bar{f}^G(x) \geq 0 \text{ für alle } f \in \mathcal{K}^{k,1}(I).$$

Sie sind also Auswertungsabbildungen, die auf den k -sos-mod I -Polynomen positiv sind. Diese dualen Abbildungen können zu Elementen des dualen Kegels der Sos-Polynome $\mathcal{K}^k(I)$ in V fortgesetzt werden:

Satz 4.2.2 - Thetakörper sind projizierte Elemente eines dualen Kegels

Falls $L \cap \text{relin}(\mathcal{K}^k(I)) \neq \emptyset$ ist, gilt:

$$\mathcal{T}_k = \text{cl}(\hat{\mathcal{D}}_A). \quad \square$$

Beweis. Es sei $H := \{(1, x) \mid x \in \mathbb{R}^n\} \subseteq \mathbb{R}^{n+1} \cong L^*$. Wie eben bereits angemerkt, ist ein Element des k -ten Thetakörpers ein duales Element auf $C \cap L$. Umgekehrt ist jedes duale Element von $C \cap L$, welches eine Auswertung ist, im Thetakörper. Es gilt also:

$$\{1\} \times \mathcal{T}_k = \mathcal{D} \cap H.$$

Nach Satz 3.2.13 auf Seite 77 gilt, da $L \cap \text{relin}(\mathcal{K}^k(I)) \neq \emptyset$ ist:

$$\text{cl}\left(\pi_L\left(\left(\mathcal{K}^k(I) \cap L\right)^\star\right)\right) = \text{cl}\left(\pi_L\left(\mathcal{K}^k(I)^\star\right)\right)$$

und nach Korollar 3.2.15 gilt:

$$\pi_L\left(\left(\mathcal{K}^k(I) \cap L\right)^\star\right) = \{\varphi \in L^* \mid \varphi(f) \geq 0 \text{ für alle } f \in \mathcal{K}^k(I) \cap L\} = \mathcal{D}.$$

Dabei sind die dualen Kegel bezüglich des Vektorraums V gebildet. Bringen wir diese beiden Aussagen zusammen, erhalten wir

$$\mathcal{D} = \text{cl}\left(\pi_L\left(\hat{\mathcal{D}}\right)\right),$$

da \mathcal{D} als dualer Kegel abgeschlossen ist. Weiterhin ist

$$\{1\} \times \hat{\mathcal{D}}_A = \pi_L\left(\hat{\mathcal{D}}\right) \cap H$$

nach der Definition von $\hat{\mathcal{D}}_A$. Im Folgenden ist nur noch zu zeigen, dass diese beiden Ausdrücke gleich sind:

$$\begin{aligned} \{1\} \times \mathcal{T}_k &= \mathcal{D} \cap H = \text{cl}\left(\pi_L\left(\hat{\mathcal{D}}\right)\right) \cap H \text{ und} \\ \{1\} \times \text{cl}\left(\hat{\mathcal{D}}_A\right) &= \text{cl}\left(\{1\} \times \hat{\mathcal{D}}_A\right) = \text{cl}\left(\pi_L\left(\hat{\mathcal{D}}\right) \cap H\right). \end{aligned}$$

Da die obere Menge Obermenge der unteren ist, gilt die Gleichheit, falls \mathcal{T}_k leer ist. Es sei im Folgenden \mathcal{T}_k nicht leer. Zunächst zwei Vorüberlegungen.

Behauptung: Es sei M ein Kegel. Für $x \in \text{relin}(K)$ ist $\lambda x \in \text{relin}(K)$ für alle $\lambda > 0$. Ist M nicht leer, ist die Bedingung $M = \text{cl}(\mathcal{K}(\text{relin}(M \cap E)))$ hinreichend dafür, dass ein affiner Teilraum E das relative Innere von M schneidet.

Beweis: Die erste Aussage folgt aus der Definition des relativen Inneren durch Skalierung einer relativ offenen Menge um x . Ist weiterhin der Schnitt von $\text{relin}(M)$ mit E leer, so ist $M \cap E$ und damit auch $\text{relin}(M \cap E)$ eine konvexe Teilmenge des Randes von M . Der Kegel $\mathcal{K}(\text{relin}(M \cap E))$ entsteht aus $\text{relin}(M \cap E)$ durch Multiplikation mit nicht-negativen Faktoren. Mit der ersten Aussage folgt, dass

auch $\mathcal{K}(\text{relin}(M \cap E))$ im Rand enthalten ist. \diamond

Behauptung: $\text{relin}(\mathcal{D}) \cap H \neq \emptyset$.

Beweis: Den Kegel über dem relativen Inneren von $\mathcal{D} \cap H$ bezeichnen wir mit K . Wir beweisen, dass $\mathcal{D} = \text{cl}(K)$ gilt, indem wir jeweils zeigen, dass eine Menge in der anderen enthalten ist. Da \mathcal{T}_k nach Voraussetzung nicht leer ist, ist der Kegel \mathcal{D} auch nicht leer. Daraus folgt die Aussage. Den Beweis gliedern wir in zwei Schritte.

Schritt 1: Nach Konstruktion besitzen die Elemente in K eine explizite Darstellung durch Elemente des Thetakörpers: $K = \{ \langle (\lambda, \lambda x), \cdot \rangle \mid \lambda > 0, x \in \text{relin}(\mathcal{T}_k) \}$. Für ein Element $x \in \text{relin}(\mathcal{T}_k)$ ist $\langle (1, x), \cdot \rangle \in \mathcal{D}$, also ist auch $\langle (\lambda, \lambda x), \cdot \rangle \in \mathcal{D}$ für beliebige Skalare $\lambda > 0$. Also ist $K \subseteq \text{cl}(K) \subseteq \mathcal{D}$.

Schritt 2: Angenommen, es gibt ein Element $y = \langle (y_0, y_1, \dots, y_n), \cdot \rangle \in \mathcal{D} \setminus \text{cl}(K)$. Dann ist $y_0 \geq 0$, da $1 \in \mathcal{K}^{k,1}(I)$ gilt. Da die Menge \mathcal{T}_k nicht leer ist, besitzt sie ein echtes relatives Inneres. Folglich existiert ein $x \in \text{relin}(\mathcal{T}_k)$ mit $\langle (1, x), \cdot \rangle \in K$. Nach Annahme existiert ein $\varepsilon > 0$, sodass $y + \varepsilon \langle (1, x), \cdot \rangle \in \mathcal{D} \setminus \text{cl}(K)$ ist. Die erste Komponente $y_0 + \varepsilon$ ist positiv. Skalierung zeigt, dass ein Element in $\mathcal{D} \setminus \text{cl}(K)$ existiert, dessen erste Komponente eins ist. Der Vektor, den die letzten Komponenten dieses Elements bilden, liegt aber im Thetakörper. Dies ist ein Widerspruch. \diamond

Es gilt $\text{relin}(\mathcal{D}) = \text{relin}(\pi_L(\hat{\mathcal{D}}))$ nach Satz 3.2.10 auf Seite 75. Daraus folgt mit Korollar 3.2.11:

$$\text{cl}(\pi_L(\hat{\mathcal{D}})) \cap H = \text{cl}(\pi_L(\hat{\mathcal{D}}) \cap H).$$

Damit ist die Aussage bewiesen. \blacksquare

Im Allgemeinen gilt die Inklusion $\text{cl}(\hat{\mathcal{D}}_A) \subseteq \mathcal{T}_k$, da für $x \in \hat{\mathcal{D}}_A$ gilt:

$$\langle (1, x), f \rangle = \bar{f}^G(x) \geq 0$$

für alle $f \in \mathcal{K}^{k,1}(I)$.

Die Elemente in $\hat{\mathcal{D}}$ sind genau die Elemente, für die bestimmte Matrizen positiv sind. Wie diese Identifikation vorgenommen werden kann, zeigen wir im nächsten Abschnitt.

4.3 Thetakörper als projizierte Spektraeder

Dem letzten Abschnitt zufolge können die Funktionale auf den affin-linearen Polynomen, die k -sos-mod I sind, zu Funktionalen auf den Sos-Polynomen vom Grad kleiner gleich $2k$ fortgesetzt werden. Diese Fortsetzungen sind genau die Funktionale, die alle quadratischen Polynome auf positive Werte abbilden. Wir zeigen, dass dies gleichbedeutend damit ist, dass eine bestimmte Matrix, die sogenannte *Momentmatrix*, positiv semidefinit ist. Da Elemente im Thetakörper Funktionale auf affin-linearen k -sos-mod I -Polynomen sind, folgt, dass diese als projizierte Spektraeder geschrieben werden können.

In diesem Abschnitt sei $I \subseteq \mathbb{R}[X_1, \dots, X_n]$ ein Ideal, welches keine affin-linearen Polynome enthält, und $k \in \mathbb{N}$ fest gewählt.

Weiterhin benötigen wir eine Theta-Basis Θ für $\mathbb{R}[X_1, \dots, X_n]/I$, siehe Kapitel 1. Diese soll die Bedingung, dass Θ_l eine Basis für $\mathbb{R}[X_1, \dots, X_n]_l/I$ für alle $l \in \mathbb{N}$ ist, erfüllen. In Abschnitt 1.3 machen wir deutlich, dass die Standardbasis bezüglich einer Gröbnerbasis für I , die bezüglich der graduierten lexikographischen Ordnung auf $\mathbb{R}[X_1, \dots, X_n]$ gebildet wird, eine solche Theta-Basis ist. Wir fixieren daher diese.

Positive Funktionale induzieren positive Momentmatrizen

Wir betrachten den Vektor

$$[x]_{\Theta_k} := (1 + I, X_1 + I, \dots, X_n + I, \dots, b, \dots) \in (\mathbb{R}[X_1, \dots, X_n]/I)^{\#\Theta_k},$$

der alle Elemente $b \in \Theta_k$ der Theta-Basis bis zum Grad k genau einmal enthält, wobei die Normalformen zunächst aufsteigend nach ihrem Grad und im Feineren absteigend nach ihrem Multigrad angeordnet sind.

Nach Voraussetzung kann das Produkt von $p, q \in \Theta_k$ auf diese Weise dargestellt werden:

$$p \cdot q = \sum_{b \in \Theta_{2k}} \lambda_{p,q}^b \cdot b$$

für Koeffizienten $\lambda_{p,q}^b \in \mathbb{R}$, da Θ eine Theta-Basis ist.

Definition 4.3.1 - Momentmatrizen

Die k -te *Momentmatrix* ist

$$\mathcal{M}_{\Theta_k} := [x]_{\Theta_k} \cdot [x]_{\Theta_k}^t = (p \cdot q)_{p,q \in \Theta_k} = \sum_{b \in \Theta_{2k}} b \cdot (\lambda_{p,q}^b)_{p,q \in \Theta_k}.$$

Ist $y = (y_b)_{b \in \Theta_{2k}} \in \mathbb{R}^{2^k}$, wird

$$\mathcal{M}_{\Theta_k}(y) := \sum_{b \in \Theta_{2k}} y_b \cdot (\lambda_{p,q}^b)_{p,q \in \Theta_k}$$

als die k -te Momentmatrix zu y bezeichnet. □

Ein Vektor $y = (y_b)_{b \in \Theta_{2k}} \in \mathbb{R}^{\#\Theta_{2k}}$ definiert ein lineares Funktional auf $\mathbb{R}[X_1, \dots, X_n]_{2k}/I$:

$$\langle y, \cdot \rangle : \mathbb{R}[X_1, \dots, X_n]_{2k}/I \rightarrow \mathbb{R}, \quad f \mapsto \sum_{b \in \Theta_{2k}} y_b \cdot f_b$$

für $f = \sum_{b \in \Theta_{2k}} f_b \cdot b \in \mathbb{R}[X_1, \dots, X_n]_{2k}/I$, $f_b \in \mathbb{R}$. Mit der Abbildung

$$\pi_{\mathbb{R}^n} : \mathbb{R}^{\#\Theta_{2k}} \rightarrow \mathbb{R}^n, \quad y \mapsto (y(X_1 + I), \dots, y(X_n + I))$$

bezeichnen wir die Einschränkung von y auf den linearen Teilraum \mathbb{R}^n .

Lemma 4.3.2 - Positive Momentmatrizen und positive Funktionale

Für $y = (y_b)_{b \in \Theta_{2k}}$ gilt:

- (i) Für $p, q \in \Theta_k$ gilt: $(\mathcal{M}_{\Theta_k}(y))_{p,q} = \langle y, p \cdot q \rangle$,
- (ii) Die k -te Momentmatrix zu y ist genau dann positiv semidefinit, wenn für alle $f \in \mathbb{R}[X_1, \dots, X_n]_k/I$ gilt: $\langle y, f^2 \rangle \geq 0$. □

Beweis. (i): Das Produkt $p \cdot q \in \text{span}_K(\Theta_{2k})$ kann auf eindeutige Weise so dargestellt werden: $p \cdot q = \sum_{b \in \Theta_{2k}} \lambda_{p,q}^b \cdot b$ für Koeffizienten $\lambda_{p,q}^b \in \mathbb{R}$. Also ist:

$$\langle y, p \cdot q \rangle = \left\langle y, \sum_{b \in \Theta_{2k}} \lambda_{p,q}^b \cdot b \right\rangle = \sum_{b \in \Theta_{2k}} \lambda_{p,q}^b \langle y, b \rangle = \sum_{b \in \Theta_{2k}} y_b \cdot \lambda_{p,q}^b.$$

Dies entspricht dem Eintrag $(\mathcal{M}_{\Theta_k}(y))_{p,q}$ in der Momentmatrix zu y .

(ii): Für $f \in \mathbb{R}[X_1, \dots, X_n]_k/I$, $f = \sum_{b \in \Theta_k} f_b \cdot b$ mit $f_b \in \mathbb{R}$, setzen wir $\hat{f} := (f_b)_{b \in \Theta_k}$. Proposition 1.3.12 zeigt, dass diese Basisdarstellung möglich ist. Dann ist

$$\begin{aligned} \hat{f}^t \cdot \mathcal{M}_{\Theta_k}(y) \cdot \hat{f} &= \hat{f}^t \cdot \left(\sum_{q \in \Theta_k} \langle y, p \cdot q \rangle \cdot f_q \right)_{p \in \Theta_k} = \sum_{p,q \in \Theta_k} f_p \cdot f_q \cdot \langle y, p \cdot q \rangle \\ &= \left\langle y, \sum_{p,q \in \Theta_k} f_p \cdot f_q \cdot p \cdot q \right\rangle = \langle y, f^2 \rangle. \quad \blacksquare \end{aligned}$$

Thetakörper als Projektionen von Spektraedern

Jetzt kommen wir zum abschließenden Resultat:

Satz 4.3.3 - Thetakörper als projizierte Spektraeder

Falls $L \cap \text{relin}(\mathcal{K}^k(I)) \neq \emptyset$, gilt:

$$\mathcal{T}_k = \text{cl} \left(\pi_{\mathbb{R}^n} \left(\left\{ y = (y_b)_{b \in \Theta_{2k}} \mid \mathcal{M}_{\Theta_k}(y) \geq 0, y(1+I) = 1 \right\} \right) \right).$$

Damit ist \mathcal{T}_k der Abschluss eines projizierten Spektraeders. Insbesondere ist \mathcal{T}_k der Abschluss einer semialgebraischen Menge. \square

Beweis. Wir zeigen die Gleichung:

$$\hat{\mathcal{D}}_A = \pi_{\mathbb{R}^n} \left(\left\{ y = (y_b)_{b \in \Theta_{2k}} \mid \mathcal{M}_{\Theta_k}(y) \geq 0, y(1+I) = 1 \right\} \right),$$

dann folgt die Aussage mit Satz 4.2.2. Zunächst halten wir fest, dass die Menge der Sos-Polynome vom Grad kleiner gleich $2k$ der von den Polynomen vom Grad kleiner gleich k erzeugte Kegel ist. Es gilt also $\mathcal{K}^k(I) = \mathcal{K}_{\mathbb{R}[X_1, \dots, X_n]_k} / I$. Wir zeigen nun, dass der duale Kegel dieser Polynome als Spektraeder ausgedrückt werden kann. Es ist

$$\begin{aligned} \hat{\mathcal{D}} &= \{ \varphi \in V^* \mid \varphi(f) \geq 0 \text{ für alle } f \in \mathcal{K}^k(I) \} \\ &= \{ \varphi \in V^* \mid \varphi(f^2 + I) \geq 0 \text{ für alle } f \in \mathbb{R}[X_1, \dots, X_n]_k \} \\ &= \{ y = (y_b)_{b \in \Theta_{2k}} \in \mathbb{R}^{\#\Theta_{2k}} \mid \langle y, f^2 + I \rangle \geq 0 \text{ für alle } f \in \mathbb{R}[X_1, \dots, X_n]_k \} \\ &= \{ y = (y_b)_{b \in \Theta_{2k}} \in \mathbb{R}^{\#\Theta_{2k}} \mid \mathcal{M}_{\Theta_k}(y) \geq 0 \} \quad \text{und} \\ \hat{\mathcal{D}}_A &= \{ (y(X_1 + I), \dots, y(X_n + I)) \in \mathbb{R}^n \mid y = (y_b)_{b \in \Theta_{2k}}, \mathcal{M}_{\Theta_k}(y) \geq 0, y(1+I) = 1 \} \\ &= \pi_{\mathbb{R}^n} \left(\left\{ y = (y_b)_{b \in \Theta_{2k}} \mid \mathcal{M}_{\Theta_k}(y) \geq 0, y(1+I) = 1 \right\} \right). \end{aligned}$$

Der Kegel $\hat{\mathcal{D}}$ ist ein Spektraeder, da die k -te Momentmatrix zu y von der Gestalt

$$\mathcal{M}_{\Theta_k}(y) = \sum_{b \in \Theta_{2k}} y_b \cdot (\lambda_{p,q}^b)_{p,q \in \Theta_k}$$

ist mit symmetrischen Matrizen $(\lambda_{p,q}^b)_{p,q \in \Theta_k} \in \mathcal{S}_{\#\Theta_k}$. Da Spektraeder unter Schnitten stabil sind, ist $\hat{\mathcal{D}}_A$ ein projizierter Spektraeder. Nach Proposition 3.1.8 ist $\hat{\mathcal{D}}_A$ semialgebraisch. \blacksquare

Im Allgemeinen ist \mathcal{T}_k eine Obermenge des projizierten Spektraeders.

Beispiel 4.3.4 Wir betrachten das Ideal $J \subseteq \mathbb{R}[a, b, c, d]$ aus Beispiel 1.2.7. Die Leit-
terme der angegebenen Gröbnerbasis für J sind gegeben durch $\{ad, a^2, abc, b^2c^2\}$.
Also ist $[x]_{\Theta_1} = (1, a, b, c, d)$ und $[x]_{\Theta_2} = (1, a, b, c, d, ab, ac, b^2, bc, bd, c^2, cd, d^2)$.
Durch Reduktion der Produkte ist die zweite Momentmatrix von dieser Gestalt:

$$\mathcal{M}_{\Theta_2} = \begin{pmatrix} 1 & a & b & c & d & ab & ac & b^2 & bc & bd & c^2 & cd & d^2 \\ a & \blacktriangle & ab & ac & bc & \blacktriangle b & \blacktriangle c & ab^2 & \blacktriangle d & b^2c & ac^2 & bc^2 & bcd \\ b & ab & b^2 & bc & bd & ab^2 & \blacktriangle d & b^3 & b^2c & b^2d & bc^2 & bcd & bd^2 \\ c & ac & bc & c^2 & cd & \blacktriangle d & ac^2 & b^2c & bc^2 & bcd & c^3 & c^2d & cd^2 \\ d & bc & bd & cd & d^2 & b^2c & bc^2 & b^2d & bcd & bd^2 & c^2d & cd^2 & d^3 \\ ab & \blacktriangle b & ab^2 & \blacktriangle d & b^2c & \blacktriangleright & \blacktriangledown & ab^3 & \blacktriangle bd & b^3c & \blacktriangle cd & \blacktriangle d^2 & b^2cd \\ ac & \blacktriangle c & \blacktriangle d & ac^2 & bc^2 & \blacktriangledown & \blacktriangleleft & \blacktriangle bd & \blacktriangle cd & \blacktriangle d^2 & ac^3 & bc^3 & bc^2d \\ b^2 & ab^2 & b^3 & b^2c & b^2d & ab^3 & \blacktriangle bd & b^4 & b^3c & b^3d & \blacktriangle d^2 & b^2cd & b^2d^2 \\ bc & \blacktriangle d & b^2c & bc^2 & bcd & \blacktriangle bd & \blacktriangle cd & b^3c & \blacktriangle d^2 & b^2cd & bc^3 & bc^2d & bcd^2 \\ bd & b^2c & b^2d & bcd & bd^2 & b^3c & \blacktriangle d^2 & b^3d & b^2cd & b^2d^2 & bc^2d & bcd^2 & bd^3 \\ c^2 & ac^2 & bc^2 & c^3 & c^2d & \blacktriangle cd & ac^3 & \blacktriangle d^2 & bc^3 & bc^2d & c^4 & c^3d & c^2d^2 \\ cd & bc^2 & bcd & c^2d & cd^2 & \blacktriangle d^2 & bc^3 & b^2cd & bc^2d & bcd^2 & c^3d & c^2d^2 & cd^3 \\ d^2 & bcd & bd^2 & cd^2 & d^3 & b^2cd & bc^2d & b^2d^2 & bcd^2 & bd^3 & c^2d^2 & cd^3 & d^4 \end{pmatrix},$$

wobei die symbolischen Einträge durch die Ausdrücke

$$\begin{aligned} \blacktriangle &:= -b^2 - c^2 - d^2 + 1, \\ \blacktriangledown &:= -b^3c - bc^3 - bcd^2 + bc, \\ \blacktriangleleft &:= b^2d^2 - c^4 + d^4 + c^2 - d^2 \quad \text{und} \\ \blacktriangleright &:= c^2d^2 - b^4 + d^4 + b^2 - d^2 \end{aligned}$$

ersetzt werden. Der obere 5×5 -Block von \mathcal{M}_{Θ_2} ist \mathcal{M}_{Θ_1} . □

4.4 Thetakörper als Maß für Positivität

Die Zugehörigkeit eines Elements zu einem Thetakörper sagt etwas über seine Fähigkeit, so fortgesetzt zu werden, dass die Momentmatrix zur Fortsetzung positiv ist, aus. Je größer der Raum ist, auf dem ein Element fortgesetzt werden kann, desto näher liegt es an der konvexen Hülle der Varietät. Hier möchten wir untersuchen, wie die *Fortsetzungen* eines Elements zu positiven Funktionalen auf den Sos-Polynomen zu Zuständen auf den stetigen Funktionen auf der Varietät führen

und von welcher Gestalt diese Zustände sind. Wir stellen fest, dass die *Schwerpunkte* der Zustände mit den fortgesetzten Punkten korrespondieren. Dies liefert Informationen über die Art möglicher Fortsetzungen. Punkte der Varietät besitzen genau eine Fortsetzung zu einem Punktmaß, während echte Konvexkombinationen aus diesen Punkten mehrere Fortsetzungen besitzen.

In diesem Abschnitt sei $I \subseteq \mathbb{R}[X_1, \dots, X_n]$ ein Ideal, welches keine affin-linearen Polynome enthält, $V := \mathcal{Z}(I)$ kompakt und nicht leer sowie $V = \text{ext}(\text{co}(V))$. Wir setzen weiterhin $K := \text{co}(V)$.

Positive Momentmatrizen durch Auswertungsfunktionale

Zunächst betrachten wir ein Element $y \in V$. Die Auswertung von y an einem Basiselement $b \in \Theta$ ist wohldefiniert. Setzen wir

$$\tilde{y}_k := (b(y))_{b \in \Theta_{2k}}$$

für $k \in \mathbb{N}$, so ist \tilde{y}_k ein lineares Funktional auf $\mathbb{R}[X_1, \dots, X_n]_{2k}/I$ und es gilt:

Proposition 4.4.1 - Auswertungsfunktionale

Die k -te Momentmatrix zu \tilde{y}_k ist positiv semidefinit. □

Beweis. Es ist

$$\begin{aligned} \mathcal{M}_{\Theta_k}(\tilde{y}_k) &= \sum_{b \in \Theta_{2k}} b(y) \cdot (\lambda_{p,q}^b)_{p,q \in \Theta_k} = \left(\left(\sum_{b \in \Theta_{2k}} b \cdot \lambda_{p,q}^b \right) (y) \right)_{p,q \in \Theta_k} \\ &= ((p \cdot q)(y))_{p,q \in \Theta_k} = ((p(y) \cdot q(y)))_{p,q \in \Theta_k} \\ &= (p(y))_{p \in \Theta_{2k}} \cdot (q(y))_{q \in \Theta_{2k}}^t \geq 0. \end{aligned}$$

Daraus folgt die Aussage. ■

Also ist \tilde{y}_k eine geeignete Fortsetzung von y , um die Zugehörigkeit von y zu \mathcal{T}_k aufzuzeigen.

Betrachten wir nun ein Element z der konvexen Hülle K von V , so sind geeignete Fortsetzungen durch Konvexkombinationen der Auswertungsfunktionale gegeben:

$$\tilde{z}_k := \left(\sum_{i=1}^{n+1} \lambda_i b(v_i) \right)_{b \in \Theta_{2k}}$$

setzt z geeignet fort, wobei $z = \sum_{i=1}^{n+1} \lambda_i v_i$ ist mit $\lambda_i \geq 0$, $\sum_{i=1}^{n+1} \lambda_i = 1$, und $v_i \in V$.

Fortsetzungen der Auswertungsfunktionale zu Zuständen

Es sei $X \subseteq \mathbb{R}^n$ kompakt. Die stetigen reellwertigen Funktionen auf X bezeichnen wir mit $\mathcal{C}(X)$. Vershen mit der Supremumsnorm ist $\mathcal{C}(X)$ ein Banachraum. Eine Funktion $f \in \mathcal{C}(X)$ heißt *positiv*, falls die Auswertung an allen Punkten in X nicht negativ ist. Ein Funktional $\varphi \in \mathcal{C}(X)^*$ heißt *positiv*, falls die Auswertung von φ an allen positiven Funktionen nicht negativ ist. Ist $\varphi \in \mathcal{C}(X)^*$ positiv mit Operatornorm eins, heißt φ *Zustand*. Ein Zustand heißt *rein*, falls er ein Extrempunkt der konvexen Menge $\rho(X)$ aller Zustände auf $\mathcal{C}(X)$ ist.

Für $y \in X$ ist die Punktauswertung

$$\begin{aligned} \delta_y: \mathcal{C}(X) &\rightarrow \mathbb{R} \\ f &\mapsto f(y) \end{aligned}$$

ein multiplikatives stetiges lineares Funktional. Umgekehrt sind alle stetigen linearen Funktionale auf $\mathcal{C}(X)$, die multiplikativ sind, durch Punktauswertungen gegeben. Sie bilden die Menge der reinen Zustände auf $\mathcal{C}(X)$.

Nach dem Satz von Stone-Weierstrass ist $\mathbb{R}[X_1, \dots, X_n]/I$ dicht in $\mathcal{C}(V)$ bezüglich der Supremumsnorm.

Definition 4.4.2 - Fortsetzungen

Ein Funktional $\varphi \in \mathcal{C}(V)^*$ heißt *Fortsetzung* von $x \in \mathbb{R}^n$, falls

$$(\varphi(1+I), \varphi(X_1+I), \dots, \varphi(X_n+I)) = (1, x)$$

gilt und

$$\mathcal{M}_{\Theta_k} \left((\varphi(b))_{b \in \Theta_{2k}} \right) \geq 0$$

für alle $k \in \mathbb{N}$ ist. In diesem Fall heißt x *fortsetzbar*. □

Für $y \in V$ ist $\delta_y \in \mathcal{C}(V)^*$ eine Fortsetzung von y . Es gilt:

$$\delta_y(f) = \tilde{y}_k(f)$$

für alle $f \in \mathbb{R}[X_1, \dots, X_n]_{2k}/I$ und für alle $k \in \mathbb{N}$. Eine Fortsetzung mit dieser Eigenschaft ist eindeutig. Es ist $\delta_y \in \mathcal{K}^\star$, dem dualen Kegel der Sos-Polynome.

Satz 4.4.3 - Fortsetzungen und Zustände

Es sei $x \in \mathbb{R}^n$. Dann gilt:

- (i) Eine Fortsetzung von x ist ein Zustand auf $\mathcal{C}(V)$.
- (ii) Es ist x genau dann fortsetzbar, wenn $x \in K$ gilt.

Weiterhin ist jeder Zustand auf $\mathcal{C}(V)$ Fortsetzung eines Elements in K . □

Beweis. (i): Sei φ eine Fortsetzung von x . Da $\mathbb{R}[X_1, \dots, X_n]/I$ dicht in $\mathcal{C}(V)$ ist, ist φ positiv. In diesem Fall ist $\varphi(1 + I)$ gleich der Operatornorm von φ . Aus der Voraussetzung $\varphi(1 + I) = 1$ folgt, dass φ ein Zustand ist.

(ii): Es sei x fortsetzbar. Dann gilt insbesondere, dass $x \in \mathcal{T}_k$ für alle $k \in \mathbb{N}$ ist. Nach Satz 4.1.5 folgt, dass $x \in K$ ist. Gilt umgekehrt $x \in K$, so ist $x = \sum_{i=1}^r \lambda_i v_i$ mit $\lambda_i \geq 0$, wobei $\sum_{i=1}^r \lambda_i = 1$ ist, und $v_i \in V$ darstellbar. Also wird x durch das Funktional

$$\varphi := \sum_{i=1}^r \lambda_i \delta_{v_i}$$

fortgesetzt, da $(\varphi(X_1 + I), \dots, \varphi(X_n + I)) = x$ gilt.

Die letzte Behauptung folgt aus den vorigen Überlegungen, da ein Zustand $\psi \in \rho(V)$ das Element $(\psi(X_1 + I), \dots, \psi(X_n + I))$ fortsetzt, und Lemma 4.3.2. ■

Die konvexe Hülle der Punktauswertungen bezeichne $\tilde{K} := \text{co}(\{\delta_y \mid y \in V\})$. Die Menge der Fortsetzungen in \tilde{K} zu einem Element $x \in K$ ist konvex. Ist $x \in V$, so besitzt x genau eine Fortsetzung in \tilde{K} , da nach Voraussetzung $V = \text{ext}(K)$ gilt. Im Allgemeinen besitzt ein Element in $K \setminus V$ mehrere Fortsetzungen in \tilde{K} , da sich Funktionale zu unterschiedlichen Konvexzerlegungen unterscheiden.

Der schwach- \star -Abschluss von $\text{co}(\{\delta_y \mid y \in X\}) \subseteq \mathcal{C}(X)^*$ ist $\rho(X)$, die Menge der Zustände. Es ist möglich, zu beweisen, dass jeder Zustand $\varphi \in \rho(X)$ durch ein *Wahrscheinlichkeitsmaß*, das heißt, durch ein reguläres Borelmaß μ auf X mit der Eigenschaft $\mu(X) = 1$, gegeben ist. Für $f \in \mathcal{C}(X)$ ist dann

$$\varphi(f) = \int_X f \, d\mu.$$

Wir schreiben in diesem Fall $\varphi_\mu := \varphi$.

Nun geben wir für eine Fortsetzung in $\rho(V) \setminus \tilde{K}$ ein Beispiel an.

Beispiel 4.4.4 Es sei $I := \langle X_1^2 + X_2^2 - 1 \rangle \subseteq \mathbb{R}[X_1, X_2]$ und $V := \mathcal{Z}(I) \subseteq \mathbb{R}^2$ der Einheitskreis. Dann ist das positive Funktional

$$\varphi_\lambda: \mathcal{C}(V) \rightarrow \mathbb{R}, \quad f \mapsto \int_V f \, d\lambda$$

wobei λ das Lebesgue-Maß bezeichnet, ein Zustand. Es ist

$$\begin{aligned} \varphi_\lambda(X_1 + I) &= \int_V X_1 \, d\lambda = \int_0^{2\pi} \cos \alpha \, d\alpha = 0, \\ \varphi_\lambda(X_2 + I) &= \int_V X_2 \, d\lambda = \int_0^{2\pi} \sin \alpha \, d\alpha = 0. \end{aligned}$$

Der Punkt $(0,0)$ besitzt also die Fortsetzungen $\varphi_\lambda, \frac{1}{2}\delta_{(-1,0)} + \frac{1}{2}\delta_{(1,0)}$ und viele weitere. \square

Diese Beobachtungen erlauben es, folgende Analogien herzustellen. Elemente in der konvexen Hülle K von V besitzen Fortsetzungen zu Zuständen auf $\mathcal{C}(V)$. Umgekehrt liefert jeder Zustand eine Fortsetzung eines Elements in K . Ein Element im Thetakörper \mathcal{T}_k ist immer noch zu einem positiven Funktional auf $\mathbb{R}[X_1, \dots, X_n]_{2k}/I$ fortsetzbar. Es ist also möglich, für $x \in \mathbb{R}^n$ einen *Grad an Positivität* zu betrachten: Es ist x umso „positiver“, je größer der Grad der Thetakörper ist, in denen x enthalten ist.

In Kapitel 6 untersuchen wir die konvexe Hülle der Produkteinheitsvektoren. In der Literatur beschreibt sie einen „Zustandsraum“. Dieser Abschnitt rechtfertigt auf eine andere Weise, diese konvexe Hülle einen „Zustandsraum“ zu nennen.

Zustände und Schwerpunkte

In diesem letzten Unterabschnitt wollen wir die Anzahl der Fortsetzungen untersuchen. Dabei konzentrieren wir uns auf folgenden dualen Zusammenhang: Elemente in K sind genau die *Schwerpunkte* ihrer Fortsetzungen. Das Wissen über die Schwerpunkte liefert Informationen über mögliche Fortsetzungen.

Die Theorie zu Schwerpunkten von Zuständen entnehmen wir [Tak], Kapitel IV, Abschnitt 6.

Lemma 4.4.5 - Schwerpunkte von Wahrscheinlichkeitsmaßen

Es sei $C \subseteq \mathbb{R}^n$ eine kompakte konvexe Menge und μ ein Wahrscheinlichkeitsmaß auf C . Dann existiert genau ein $y \in C$ mit der Eigenschaft

$$l(y) = \int_C l(x) d\mu(x)$$

für alle $l \in \mathbb{R}[X_1, \dots, X_n]_1$. In diesem Fall heißt y *Schwerpunkt* von μ . Es gilt:

$$y = (\varphi_\mu(X_1 + I), \dots, \varphi_\mu(X_n + I)). \quad \square$$

Beweis. Die Abbildung

$$\varphi: \mathbb{R}^n \rightarrow \mathbb{R}, \quad l \mapsto \int_C \langle l, x \rangle d\mu(x)$$

wird durch ein eindeutiges Element $y \in \mathbb{R}^n$ repräsentiert. Angenommen, $y \notin C$. Dann existiert nach funktionalanalytischen Trennungssätzen ein $l \in \mathbb{R}^n$ mit

$$\varphi(l) = \langle l, y \rangle > \sup\{\langle l, x \rangle \mid x \in K\} =: \alpha,$$

woraus folgt:

$$\varphi(l) = \int_C \langle l, x \rangle d\mu(x) \leq \int_C \alpha d\mu(x) = \alpha < \varphi(l).$$

Dies ist ein Widerspruch. Also folgt: $y \in K$. Da $\mu(C) = 1$, gilt die Aussage auch für affin-lineare Funktionale. Die letzte Aussage folgt direkt aus den Definitionen. ■

Lemma 4.4.6 - Extrempunkte als Schwerpunkte

Es sei $C \subseteq \mathbb{R}^n$ eine kompakte konvexe Menge und μ ein Wahrscheinlichkeitsmaß auf C mit Schwerpunkt $x \in \text{ext}(C)$. Dann ist μ das Punktmaß zu x , also $\varphi_\mu = \delta_x$. □

Beweis. Nach funktionalanalytischen Trennungssätzen existiert ein affin-lineares Funktional $l \in \mathbb{R}[X_1, \dots, X_n]_1$ mit $l(y) = 0$ und $l(x) > 0$ für alle $x \in \text{relin}(C)$. Wir setzen

$$C_0 := \{x \in C \mid l(x) = 0\}.$$

Diese Menge ist ebenfalls kompakt und konvex und es gilt: $y \in \text{ext}(C_0)$.

Behauptung: $\mu(C \setminus C_0) = 0$.

Beweis: Es ist $l(x) > 0$ auf $C \setminus C_0$ und

$$0 = l(y) = \int_C l(x) d\mu(x).$$

Daraus folgt, dass l auf $C \setminus C_0$ fast überall null ist. \diamond

Es ist möglich, ein affin-lineares Funktional zu finden, welches auf y verschwindet und auf $\text{relin}(C_0)$ echt positiv ist. Die Verschwindemenge auf C_0 heiße C_1 . Auf die gleiche Weise bilden wir induktiv Mengen C_2, C_3, \dots . Da sich die Dimension des kleinsten affinen Unterraums $(\mathbb{R}^n)_{C_s}$, in dem C_s enthalten ist, bei jedem Schritt verringert, gibt es ein $0 \leq s \leq n$ mit $C_s = \{y\}$. Das Wahrscheinlichkeitsmaß μ konzentriert sich daher auf den Punkt y . Für eine ausführlichere Einführung zu den hier vorgebrachten Argumenten siehe Abschnitt 3.2 oder Abschnitt 6.2. \blacksquare

Ein Wahrscheinlichkeitsmaß μ auf V kann zu einem Wahrscheinlichkeitsmaß $\tilde{\mu}$ auf K fortgesetzt werden. Dies geschieht so: Für eine messbare Menge $A \subseteq K$ sei

$$\tilde{\mu}(A) := \mu(A \cap V).$$

Abschließend stellen wir fest, dass Punkte der konvexen Hülle von V die Schwerpunkte ihrer Fortsetzungen sind:

Satz 4.4.7 - Schwerpunkte von Fortsetzungen

Es sei $y \in K$ und $\varphi \in \rho(V)$ eine Fortsetzung von y . Weiterhin sei μ das Wahrscheinlichkeitsmaß auf V , welches φ repräsentiert. Dann gilt:

- (i) Der Schwerpunkt von $\tilde{\mu}$ ist gleich y .
- (ii) Ist $y \in V$, dann ist μ das Punktmaß zu y . \square

Beweis. Die Behauptung (i) folgt direkt aus Lemma 4.4.5. Die zweite Aussage folgt aus Lemma 4.4.6. \blacksquare

Nach Theorem 6.11 in [Tak] kann ein Wahrscheinlichkeitsmaß auf K in geeigneter Weise durch ein *Randmaß*, also durch ein Wahrscheinlichkeitsmaß, für das $K \setminus V$ eine Nullmenge ist, ersetzt werden. Dies ist der Fall, da Randmaße maximal sind in dem Sinne, dass der induzierte Zustand auf konvexen Funktionen aus $\mathcal{C}(K)$ größere Werte erzielt. Um einen Schwerpunkt zu erhalten, reicht es also aus, die Masse auf den Extrempunkten zu konzentrieren. Auf Beispiel 4.4.4 Bezug nehmend, ist der Zustand $\delta_{(0,0)}$ ersetzbar durch die Zustände φ_λ oder $\frac{1}{2}\delta_{(-1,0)} + \frac{1}{2}\delta_{(1,0)}$, die durch Randmaße induziert werden, da alle den Schwerpunkt $(0,0)$ besitzen.

Zum Abschluss eine Übersicht. Für $y \in \mathbb{R}^n$ und $k \in \mathbb{N}$ gilt:

- $y \in V \quad \Leftrightarrow$ Es gibt eine Fortsetzung von y ,
welche Punktauswertung ist
- $y \in K \setminus V \quad \Leftrightarrow$ Es gibt eine Fortsetzung von y ,
welche keine Punktauswertung ist
- $y \in \mathcal{T}_k \quad \Leftrightarrow$ y besitzt eine Fortsetzung in $(\mathcal{K}^k(I))^\star$
- $y \notin K \quad \Leftrightarrow$ Es gibt keine Fortsetzung von y

5 Mehrfache Tensorprodukte

In diesem Kapitel stellen wir *mehrfache Tensorprodukte* als Verallgemeinerung des bekannten zweifachen Tensorprodukts vor. Die konvexe Hülle der *Einheitsproduktvektoren* eines mehrfachen Tensorprodukts bildet die Einheitssphäre der *projektiven Norm*. Das Ziel dieses Kapitels ist es, Produktvektoren als reelle algebraische Varietät zu schreiben. Damit ist die Einheitssphäre der projektiven Norm die konvexe Hülle einer reellen algebraischen Varietät. Es ist also möglich, diese als Schnitt von Thetakörpern zu schreiben, siehe Abschnitt 4.1. Von der Berechnung der projektiven Norm mittels *Thetanormen* handeln die nächsten Kapitel.

Im ersten Abschnitt konstruieren wir das mehrfache Tensorprodukt als Auswertungsabbildung auf Multilinearformen. Hierbei verallgemeinern wir die Theorie, die in der Publikation [Ryan] entwickelt wird. Wir stellen alternative Möglichkeiten, ein mehrfaches Tensorprodukt zu verstehen, vor. Im Anschluss untersuchen wir die Assoziativität wichtiger Eigenschaften.

Der zweite Abschnitt handelt zunächst von der projektiven Norm. Bei der Vorstellung der *injektiven Norm* gehen wir auf die Extrempunkte ihrer Einheitssphäre und auf *duale Normen* ein. Schließlich kann auf dem mehrfachen Tensorprodukt auf natürliche Weise ein Skalarprodukt definiert werden, welches die *Hilbert-Schmidt-Norm* induziert.

Tensoren können mit *mehrstufigen Matrizen* identifiziert werden. Im dritten Abschnitt zeigen wir, dass es eine Familie von 2×2 -Unterdeterminanten eines Tensors gibt, die genau dann alle verschwinden, wenn der Tensor ein Produktvektor ist. Fassen wir diese Determinanten als Polynome vom Grad zwei auf, folgt, dass die Produktvektoren die Verschwindemenge dieser Polynome bilden. Mit dem reellen Nullstellensatz zeigen wir, dass das Verschwindeideal der Produktvektoren von den Determinanten erzeugt wird.

Wenn es möglich ist, verallgemeinern wir die Theorie auf beliebige Vektorräume. Die zentralen Aussagen sind jedoch nur für das mehrfache Tensorprodukt von Vektorräumen endlicher Dimension sinnvoll.

5.1 Konstruktion mehrfacher Tensorprodukte

Im Folgenden seien V_1, \dots, V_m Vektorräume über \mathbb{K} für ein $m \in \mathbb{N}$, $m \geq 2$. Den Raum der Multilinearformen $V_1 \times \dots \times V_m \rightarrow \mathbb{K}$ bezeichnen wir mit $\text{Mult}(V_1, \dots, V_m)$.

Die Abbildung ι bilde einen Vektor $(v_1, v_2, \dots, v_m) \in (V_1 \times \dots \times V_m)$ auf das lineare Funktional

$$\begin{aligned} v_1 \otimes v_2 \otimes \dots \otimes v_m : \text{Mult}(V_1, \dots, V_m) &\rightarrow \mathbb{K} \\ A &\mapsto A(v_1, v_2, \dots, v_m) \end{aligned}$$

ab. Die lineare Hülle des Bildes von ι in $\text{Mult}(V_1, \dots, V_m)'$ bezeichnen wir als das m -fache Tensorprodukt von V_1, \dots, V_m und schreiben dafür $V_1 \otimes V_2 \otimes \dots \otimes V_m$. Ein Erzeugendensystem von $V_1 \otimes V_2 \otimes \dots \otimes V_m$ ist daher gegeben durch

$$\mathcal{P}_{V_1 \otimes V_2 \otimes \dots \otimes V_m} := \{v_1 \otimes \dots \otimes v_m \mid v_1 \in V_1, \dots, v_m \in V_m\},$$

die Menge der *Produktvektoren*. Ein Tensor in $V_1 \otimes \dots \otimes V_m$ *faktoriert*, falls er ein Produktvektor ist.

Für das mehrfache Tensorprodukt gelten im Vergleich zum zweifachen analoge Eigenschaften. Insbesondere ist ι eine multilineare Abbildung. Weiterhin gilt:

Proposition 5.1.1 - Eigenschaften des mehrfachen Tensorprodukts

- (i) Ist jeweils $(e_i^k)_{i \in I_k}$ eine Basis für V_k , $k = 1, \dots, m$, so ist

$$\{e_{i_1}^1 \otimes \dots \otimes e_{i_m}^m \mid i_1 \in I_1, \dots, i_m \in I_m\}$$

eine Basis für $V_1 \otimes V_2 \otimes \dots \otimes V_m$.

- (ii) Ein Tensor $\sum_{i=1}^r v_1^i \otimes \dots \otimes v_m^i$ ist genau dann gleich null, wenn für alle Funktionale $\varphi_k \in V_k'$, $k = 1, \dots, m$, gilt: $\sum_{i=1}^r \varphi_1(v_1^i) \dots \varphi_m(v_m^i) = 0$.
- (iii) (*Alternative Darstellung*)

Die lineare Abbildung $j : V_1 \otimes \dots \otimes V_m \rightarrow \text{Mult}(V_1', \dots, V_m')$ mit

$$\begin{aligned} j(v_1 \otimes v_2 \otimes \dots \otimes v_m) : \quad V_1' \times \dots \times V_m' &\rightarrow \mathbb{K} \\ (\varphi_1, \dots, \varphi_m) &\mapsto \varphi_1(v_1) \dots \varphi_m(v_m) \end{aligned}$$

definiert eine Einbettung von $V_1 \otimes \dots \otimes V_m$ in $\text{Mult}(V_1', \dots, V_m')$.

(iv) (*Universelle Eigenschaft*)

Jede multilineare Abbildung $T : V_1 \times \cdots \times V_m \rightarrow Z$ in einen \mathbb{K} -Vektorraum Z faktorisiert über $V_1 \otimes \cdots \otimes V_m$, das heißt, es existiert genau eine lineare Abbildung $\tilde{T} : V_1 \otimes \cdots \otimes V_m \rightarrow Z$, sodass $T = \tilde{T} \circ \iota$. Insbesondere ist das Tensorprodukt durch diese Eigenschaft bis auf Isomorphie eindeutig bestimmt. \square

Beweis. Zum Beweis verweisen wir auf [Ryan], Kapitel 1. Dort sind die Aussagen für zweifache Tensorprodukte bewiesen. Für mehrfache Tensorprodukte ist eine analoge Beweisführung möglich. \blacksquare

Die universelle Eigenschaft zeigt, dass genau eine lineare Abbildung $\tilde{\beta}$ auf dem Tensorprodukt $V'_1 \otimes \cdots \otimes V'_m$ existiert, die die multilineare Abbildung

$$\begin{aligned} \beta : \quad V'_1 \times \cdots \times V'_m &\rightarrow (V_1 \otimes \cdots \otimes V_m)' \\ (\varphi_1, \dots, \varphi_m) &\mapsto [v_1 \otimes \cdots \otimes v_m \mapsto \varphi_1(v_1) \cdots \varphi_m(v_m)] \end{aligned}$$

faktorisiert.

Proposition 5.1.2 - Funktionale durch das Tensorprodukt der Duale

Die Abbildung $\tilde{\beta} : V'_1 \otimes \cdots \otimes V'_m \rightarrow (V_1 \otimes \cdots \otimes V_m)'$ ist eine Einbettung. \square

Beweis. Es sei $\varphi \in V'_1 \otimes \cdots \otimes V'_m$ mit $\varphi(z) = 0$ für alle $z \in V_1 \otimes \cdots \otimes V_m$ und $\varphi \neq 0$. Dann existiert nach der letzten Proposition eine Darstellung

$$\sum_{i=1}^r \varphi_1^i \otimes \cdots \otimes \varphi_m^i$$

von φ , sodass $(\varphi_j^i)_{i=1, \dots, r}$ für $j = 1, \dots, m$ jeweils linear unabhängig sind. Nach Voraussetzung ist

$$\sum_{i=1}^r \varphi_1^i(v_1) \cdots \varphi_m^i(v_m) = 0$$

für alle $v_k \in V_k$, $k = 1, \dots, m$.

Behauptung: Für alle $v_k \in V_k$, $k = 1, \dots, m-1$, gilt:

$$\sum_{i=1}^r \varphi_1^i(v_1) \cdots \varphi_{m-1}^i(v_{m-1}) = 0.$$

Beweis: Angenommen, das Gegenteil ist der Fall. Dann existiert eine nicht-triviale Linearkombination von $\varphi_m^1, \dots, \varphi_m^r$ zu null. Dies ist ein Widerspruch zur Voraussetzung. \diamond

Induktiv führt dies zu einem Widerspruch, also ist $\varphi = 0$. \blacksquare

Bemerkung 5.1.3 Betrachten wir Banachräume E_1, \dots, E_m , so gilt die Eigenschaft (ii) von Proposition 5.1.1 auch, wenn ausschließlich stetige lineare Funktionale betrachtet werden. Dies folgt aus dem Satz von Hahn-Banach, siehe [Wer]. Somit folgt aus der letzten Proposition, dass *Produktfunktionale*

$$\{\varphi_1 \otimes \dots \otimes \varphi_m \mid \varphi_1 \in (E_1)^*, \dots, \varphi_m \in (E_m)^*\}$$

eine separierende Teilmenge des Duals $(E_1 \otimes \dots \otimes E_m)'$ bilden. □

Charakterisierung von Produktvektoren durch Assoziativität

Proposition 5.1.4 - Assoziativität des Tensorprodukts

Es sind $V_1 \otimes V_2 \otimes V_3$, $(V_1 \otimes V_2) \otimes V_3$ und $V_1 \otimes (V_2 \otimes V_3)$ jeweils isomorph. Weiterhin existiert ein Isomorphismus zwischen $V_1 \otimes \dots \otimes V_m$ und $V_{\sigma(1)} \otimes \dots \otimes V_{\sigma(m)}$ für jede Permutation σ auf $\{1, \dots, m\}$. Insbesondere ist die Bildung des m -fachen Tensorprodukts assoziativ. □

Beweis. Zunächst zeigen wir die erste Aussage. Die zweite folgt aus der Assoziativität und der Isomorphie zwischen $V_1 \otimes V_2$ und $V_2 \otimes V_1$.

Die trilineare Abbildung

$$\begin{aligned} \iota: V_1 \times V_2 \times V_3 &\rightarrow (V_1 \otimes V_2) \otimes V_3 \\ (v, w, z) &\mapsto (v \otimes w) \otimes z \end{aligned}$$

bezeichne die Komposition der kanonischen Abbildungen

$$\iota_1: V_1 \times V_2 \times V_3 \rightarrow (V_1 \otimes V_2) \times V_3 \quad \text{und} \quad \iota_2: (V_1 \otimes V_2) \times V_3 \rightarrow (V_1 \otimes V_2) \otimes V_3.$$

Weiterhin bezeichnen wir die kanonische Abbildung, die jedem Tripel aus $V_1 \times V_2 \times V_3$ einen Tensor aus $V_1 \otimes V_2 \otimes V_3$ zuordnet, mit j . Aus der universellen Eigenschaft folgt nun sofort, dass eine eindeutige lineare Abbildung $\tilde{\sigma}$ mit $\iota = \tilde{\sigma} \circ j$ existiert.

Behauptung: $\sigma_0: (V_1 \otimes V_2) \times V_3 \rightarrow V_1 \otimes V_2 \otimes V_3$, $(\sum_{i=1}^r v_i \otimes w_i, z) \mapsto \sum_{i=1}^r v_i \otimes w_i \otimes z$ definiert eine bilineare Abbildung und es gilt: $j = \sigma_0 \circ \iota_1$.

Beweis: Es sei $\sum_{i=1}^r v_i \otimes w_i = \sum_{j=1}^s \tilde{v}_j \otimes \tilde{w}_j \in V_1 \otimes V_2$ und $z \in V_3$. Dann gilt für jede Trilinearform A auf $V_1 \times V_2 \times V_3$:

$$\left(\sum_{i=1}^r v_i \otimes w_i \otimes z \right) (A) = \sum_{i=1}^r A(v_i, w_i, z) = \sum_{j=1}^s A(\tilde{v}_j, \tilde{w}_j, z) = \left(\sum_{j=1}^s \tilde{v}_j \otimes \tilde{w}_j \otimes z \right) (A),$$

da die Auswertung $A(\cdot, \cdot, z)$ bilinear auf $V_1 \times V_2$ ist. \diamond

Behauptung: Es existiert eine lineare Abbildung σ von $(V_1 \otimes V_2) \otimes V_3$ nach $V_1 \otimes V_2 \otimes V_3$ mit $j = \sigma \circ \iota$.

Beweis: Aus der universellen Eigenschaft des Tensorprodukts folgt, dass genau eine lineare Abbildung σ existiert mit $\sigma_0 = \sigma \circ \iota_2$. Also ist $j = \sigma_0 \circ \iota_1 = \sigma \circ \iota$. \diamond

Behauptung: Es existiert ein Isomorphismus zwischen $(V_1 \otimes V_2) \otimes V_3$ und $V_1 \otimes V_2 \otimes V_3$.

Beweis: Es ist $j = (\sigma \circ \tilde{\sigma}) \circ j = \text{id}_{V_1 \otimes V_2 \otimes V_3} \circ j$. Aufgrund der universellen Eigenschaft folgt: $\sigma \circ \tilde{\sigma} = \text{id}_{V_1 \otimes V_2 \otimes V_3}$. Weiterhin ist $\iota = (\tilde{\sigma} \circ \sigma) \circ \iota$. Wir weisen leicht nach, dass daraus $\iota_2 = (\tilde{\sigma} \circ \sigma) \circ \iota_2$ folgt. Damit ist auch $\tilde{\sigma} \circ \sigma = \text{id}_{(V_1 \otimes V_2) \otimes V_3}$. Es folgt $\tilde{\sigma} = \sigma^{-1}$. \diamond

Analog ist $V_1 \otimes (V_2 \otimes V_3)$ isomorph zu $V_1 \otimes V_2 \otimes V_3$. \blacksquare

Lemma 5.1.5 - Faktorisierung von Produktvektoren

Ein Tensor $v \in V_1 \otimes V_2 \otimes V_3$ faktorisiere jeweils über die ersten beiden und über die letzten beiden Tensorfaktoren. Dann ist v ein Produktvektor. \square

Beweis. Es sei $v \neq 0$. Dann existieren zwei Darstellungen

$$v = \sum_{i=1}^p \sum_{j=1}^q \sum_{k=1}^r \lambda_{j,k} \eta_i(x_i \otimes y_j \otimes z_k) = \sum_{l=1}^s \sum_{m=1}^t \sum_{n=1}^u \tilde{\lambda}_{l,m} \tilde{\eta}_n(x_l \otimes y_m \otimes z_n),$$

wobei $(x_i)_{i=1, \dots, \max(p,s)} \subseteq V_1$, $(y_j)_{j=1, \dots, \max(q,t)} \subseteq V_2$ und $(z_k)_{k=1, \dots, \max(r,u)} \subseteq V_3$ jeweils linear unabhängigen Systeme sind. Wegen Proposition 5.1.1, (ii), können wir annehmen, dass $p = s$, $q = t$ und $r = u$ gilt. Weiterhin können wir annehmen, dass für alle $j \in \{1, \dots, q\}$ ein $k \in \{1, \dots, r\}$ existiert, sodass $\lambda_{j,k} \neq 0$ ist, und dass $\tilde{\eta}_n \neq 0$ für alle $n \in \{1, \dots, u\}$ ist. Dann folgt:

$$v = \sum_{i=1}^p \sum_{j=1}^q \sum_{k=1}^r \tilde{\lambda}_{i,j} \tilde{\eta}_k(x_i \otimes y_j \otimes z_k),$$

also gilt die Gleichung $\lambda_{j,k} \eta_i = \tilde{\lambda}_{i,j} \tilde{\eta}_k$. Da für alle $j \in \{1, \dots, q\}$ ein Index $k \in \{1, \dots, r\}$ mit $\lambda_{j,k} \neq 0$ existiert und $\tilde{\eta}_k \neq 0$ ist, folgt, dass eine Konstante μ_j existiert, sodass für alle $i \in \{1, \dots, p\}$ gilt: $\tilde{\lambda}_{i,j} = \eta_i \mu_j$. Also ist

$$v = \sum_{i=1}^p \sum_{j=1}^q \sum_{k=1}^r \eta_i \mu_j \tilde{\eta}_k(x_i \otimes y_j \otimes z_k) = \left(\sum_{i=1}^p \eta_i x_i \right) \otimes \left(\sum_{j=1}^q \mu_j y_j \right) \otimes \left(\sum_{k=1}^r \tilde{\eta}_k z_k \right),$$

also ein Produktvektor. \blacksquare

5.2 Normen auf Tensorprodukten

Mit E_1, \dots, E_m seien Banachräume bezeichnet.

Eine Norm $\|\cdot\|$ auf dem m -fachen Tensorprodukt $E_1 \otimes \dots \otimes E_m$ heißt *Kreuznorm*, falls für alle Produktvektoren $e_1 \otimes \dots \otimes e_m \in \mathcal{P}_{E_1 \otimes \dots \otimes E_m}$ gilt:

$$\|e_1 \otimes \dots \otimes e_m\| = \|e_1\| \cdots \|e_m\|.$$

Die Menge

$$\mathcal{E}_{E_1 \otimes \dots \otimes E_m} := \{z \mid z = e_1 \otimes \dots \otimes e_m \text{ mit } e_1 \in (E_1)_1, \dots, e_m \in (E_m)_1\}$$

der Produkte aus normierten Vektoren bezeichnen wir als *Einheitsproduktvektoren*. Für Kreuznormen auf $E_1 \otimes \dots \otimes E_m$ ist $\mathcal{E}_{E_1 \otimes \dots \otimes E_m}$ eine Teilmenge des Randes der Einheitssphäre.

Die projektive Norm

Proposition 5.2.1 - Projektive Norm

Die Abbildung

$$\begin{aligned} \|\cdot\|_\pi : E_1 \otimes \dots \otimes E_m &\rightarrow \mathbb{R}_0^+ \\ z &\mapsto \inf\{\sum_{i=1}^r \|x_1^i\| \cdots \|x_m^i\| \mid z = \sum_{i=1}^r x_1^i \otimes \dots \otimes x_m^i\} \end{aligned}$$

ist eine Kreuznorm auf dem m -fachen Tensorprodukt $E_1 \otimes \dots \otimes E_m$. Wir bezeichnen sie als die *projektive Norm* oder als die *Pi-Norm*. \square

Beweis. Analog zur Beweisführung in [Ryan] benutzen wir die universelle Eigenschaft des mehrfachen Tensorproduktes, Proposition 5.1.1, (iii), und die separierende Eigenschaft der Produktfunktionale, siehe Bemerkung 5.1.3. \blacksquare

Proposition 5.2.2 - Assoziativität der projektiven Norm

Sind E, F und G jeweils von endlicher Dimension, so sind die beiden normierten Räume $((E \otimes F, \|\cdot\|_\pi) \otimes G, \|\cdot\|_\pi)$ und $(E \otimes F \otimes G, \|\cdot\|_\pi)$ gleich. \square

Beweis. Zunächst definieren wir die Abbildung

$$\|\cdot\|_{\pi_0} : E \otimes F \otimes G \rightarrow \mathbb{K}, \quad z \mapsto \inf \left\{ \sum_{i=1}^r \|z_i\|_{\pi} \|g_i\| \mid z = \sum_{i=1}^r z_i \otimes g_i, z_i \in E \otimes F, g_i \in G \right\}.$$

Dann gilt für $z \in E \otimes F \otimes G$:

Behauptung: Es ist $\|z\|_{\pi_0} = \|z\|_{\pi}$.

Beweis: Die Ungleichung $\|z\|_{\pi_0} \leq \|z\|_{\pi}$ ist leicht einzusehen. Wir zeigen nun die Ungleichung $\|z\|_{\pi_0} \geq \|z\|_{\pi}$. Sei $\varepsilon > 0$. Dann existiert eine Darstellung $z = \sum_{i=1}^r z_i \otimes g_i$ mit $z_i \in E \otimes F$ und $g_i \in G$, $\|g_i\| = 1$, sodass $\sum_{i=1}^r \|z_i\|_{\pi} \leq \|z\|_{\pi_0} + \varepsilon/2$ gilt. Wir wählen für $i = 1, \dots, r$ eine Darstellung $z_i = \sum_{j \in I_i} e_j^i \otimes f_j^i$ mit endlicher Indexmenge I_i , sodass gilt: $\sum_{j \in I_i} \|e_j^i\| \|f_j^i\| \leq \|z_i\|_{\pi} + \varepsilon/(2r)$. Dann ist

$$\|z\|_{\pi} \leq \sum_{i=1}^r \sum_{j \in I_i} \|e_j^i\| \|f_j^i\| \leq \sum_{i=1}^r (\|z_i\|_{\pi} + \varepsilon/(2r)) = \sum_{i=1}^r \|z_i\|_{\pi} + \varepsilon/2 \leq \|z\|_{\pi_0} + \varepsilon.$$

Da $\varepsilon > 0$ beliebig war, folgt die Aussage. ◇

Auf $E \otimes F \otimes G$ stimmt $\|\cdot\|_{\pi_0}$ also mit der projektiven Norm überein. ■

Gemäß ihrer Konstruktion ist die projektive Norm die größte Kreuznorm auf dem Tensorprodukt $E_1 \otimes \dots \otimes E_m$. Ihre Einheitssphäre ist daher in der Einheitssphäre jeder anderen Kreuznorm enthalten. Umgekehrt enthält sie die konvexe Hülle der normierten Produktvektoren. Es gilt sogar die Gleichheit:

Proposition 5.2.3 - Konvexe Hülle der Einheitsproduktvektoren

Es gilt: $\mathcal{B}_{1,\pi} = \text{cl}(\text{co}(\mathcal{P}_V \cap \mathcal{B}_{1,\pi})) = \text{cl}(\text{co}(\mathcal{E}_V))$ mit $V := E_1 \otimes \dots \otimes E_m$. □

Beweis. Zunächst zeigen wir die letzte Gleichung. Die Inklusion

$$\text{cl}(\text{co}(\mathcal{P}_V \cap \mathcal{B}_{1,\pi})) \supseteq \text{cl}(\text{co}(\mathcal{E}_V))$$

ist schnell einzusehen. Sei nun $e \in \mathcal{P}_V$ mit $\|e\|_{\pi} \leq 1$. Dann ist $\|e/\|e\|_{\pi}\|_{\pi} = 1$ und

$$e = \lambda \left(\frac{e}{\|e\|_{\pi}} \right) + (1 - \lambda) \left(\frac{-e}{\|e\|_{\pi}} \right)$$

mit $0 \leq \lambda := (\|e\|_{\pi} + 1)/2 \leq 1$. Also ist $e \in \text{co}(\mathcal{E}_V)$.

Jetzt zeigen wir die erste Gleichung. Die Inklusion

$$\mathcal{B}_{1,\pi} \supseteq \text{cl}(\text{co}(\mathcal{E}_V))$$

gilt nach einer einführenden Anmerkung. Sei nun $e \in \text{in}(\mathcal{B}_{1,\pi})$. Dann existiert eine Darstellung $e = \sum_{i=1}^r x_1^i \otimes \cdots \otimes x_m^i$ mit $1 > \delta := \sum_{i=1}^r \|x_1^i\| \cdots \|x_m^i\| \geq \|e\|_\pi$. Es ist

$$1 \geq \|e/\delta\|_\pi = \sum_{i=1}^r \|x_1^i \otimes \cdots \otimes x_m^i\|_\pi / \delta \cdot (\|x_1^i \otimes \cdots \otimes x_m^i\|_\pi^{-1} \cdot x_1^i \otimes \cdots \otimes x_m^i).$$

Da nach Konstruktion $1 = \sum_{i=1}^r \|x_1^i \otimes \cdots \otimes x_m^i\|_\pi / \delta$ gilt, folgt, dass $e/\delta \in \text{co}(\mathcal{P}_V \cap \mathcal{B}_{1,\pi})$ ist. Schließlich ist $e \in \delta \cdot \text{co}(\mathcal{P}_V \cap \mathcal{B}_{1,\pi}) \subseteq \text{co}(\mathcal{P}_V \cap \mathcal{B}_{1,\pi})$. ■

Da die konvexe Hülle kompakter Teilmengen endlichdimensionaler Vektorräume wieder kompakt ist, siehe Satz 3.1.2, können wir in diesem Fall in der letzten Proposition auf die Abschlüsse verzichten.

Die injektive Norm

Proposition 5.2.4 - Injektive Norm

Die Abbildung

$$\begin{aligned} \|\cdot\|_\epsilon: E_1 \otimes \cdots \otimes E_m &\rightarrow \mathbb{R}_0^+ \\ z &\mapsto \sup\{ |(\varphi_1 \otimes \cdots \otimes \varphi_m)(z)| \mid \varphi_1 \in (E_1^*)_1, \dots, \varphi_m \in (E_m^*)_1 \} \end{aligned}$$

ist eine Kreuznorm auf dem m -fachen Tensorprodukt $E_1 \otimes \cdots \otimes E_m$. Wir bezeichnen sie als die *injektive Norm*. □

Beweis. Die Abbildung ist positiv. Die Definitheit folgt aus der separierenden Eigenschaft des Duals, siehe Bemerkung 5.1.3. Es ist $\|\lambda z\|_\epsilon = |\lambda| \|z\|_\epsilon$ für alle $\lambda \in \mathbb{R}$ und alle $z \in E_1 \otimes \cdots \otimes E_m$. Für den Absolutbetrag auf \mathbb{K} gilt die Dreiecksungleichung, also auch hier. Dass die injektive Norm eine Kreuznorm ist, sehen wir leicht ein. ■

Die injektive Norm ist schwächer als die projektive: $\|z\|_\epsilon \leq \|z\|_\pi$ für alle $z \in V$.

Proposition 5.2.5 - Duale Normen

Es sei $\|\cdot\|_\alpha$ eine Kreuznorm auf $E_1 \otimes \cdots \otimes E_m$. Für $\varphi \in E_1^* \otimes \cdots \otimes E_m^*$ sei die *duale Norm* $\|\cdot\|_{\alpha^*}$ zu $\|\cdot\|_\alpha$ definiert durch

$$\|\varphi\|_{\alpha^*} = \sup\{ |\varphi(z)| \mid z \in E_1 \otimes \cdots \otimes E_m, \|z\|_\alpha \leq 1 \}.$$

Dann ist die duale Norm genau dann eine Kreuznorm, wenn $\|\cdot\|_\epsilon \leq \|\cdot\|_\alpha \leq \|\cdot\|_\pi$ gilt. □

Beweis. Der Beweis für zweifache Tensorprodukte erfolgt analog für mehrfache Tensorprodukte. ■

Betrachten wir $\mathcal{H} \otimes \mathcal{K}$ als Tensorprodukt reeller Hilberträume \mathcal{H} und \mathcal{K} , so ist ein Tensor $\xi \otimes \eta$ eindeutig mit dem Operator $\langle \cdot, \xi \rangle \cdot \eta \in \mathcal{B}(\mathcal{H}, \mathcal{K})$ isometrisch isomorph identifizierbar. Die Operatornorm des Bildes eines Tensors liefert also seine injektive Norm. Lässt sich eine solche Identifikation auch für mehrfache Tensorprodukte vornehmen? Ohne allzu tief in diese Thematik einzusteigen, wollen wir im Kontext des nächsten Abschnitts eine Idee geben, wie Analogien hergestellt werden können.

Hier halten wir zunächst fest, dass für einen Vektor $v \in \mathbb{R}^n \otimes \mathbb{R}^m$ eine im Wesentlichen eindeutige Darstellung

$$v = \sum_{i=1}^n \lambda_i e_i \otimes f_i$$

mit $\lambda_i \geq 0$ und Orthonormalsystemen $\{e_i\}_{i=1}^n$ in \mathbb{R}^n und $\{f_i\}_{i=1}^m$ in \mathbb{R}^m existiert.

Proposition 5.2.6 - Extremalpunkte und Isometrien

Sei $v \in \mathbb{R}^n \otimes \mathbb{R}^m$ in der Darstellung von oben. Dann gilt:

$$\|v\|_\epsilon = \sup\{\lambda_1, \dots, \lambda_n\}.$$

Insbesondere gibt es eine Eins-zu-Eins-Beziehung zwischen den Extremalpunkten von $\mathcal{B}_{1,\epsilon}$ und den Isometrien in $\mathcal{M}_{m,n}(\mathbb{R})$. □

Beweis. Wir identifizieren v mit der Matrix

$$A := \sum_{i=1}^n \lambda_i \langle \cdot, e_i \rangle \cdot f_i.$$

Dann ist

$$A^t A := \sum_{i=1}^n \lambda_i^2 \langle \cdot, e_i \rangle \cdot e_i.$$

Das Spektrum von $A^t A$ ist $\{\lambda_1^2, \dots, \lambda_n^2\}$. Nach dem Spektralsatz ist die Quadratwurzel aus dem Spektralradius von $A^t A$ gleich der Operatornorm von A . Damit erhalten wir die Gleichung $\|v\|_\epsilon = \sup\{\lambda_1, \dots, \lambda_n\}$. Weiterhin ist v genau dann ein Extremalpunkt von $\mathcal{B}_{1,\epsilon}$, wenn $\lambda_1 = \dots = \lambda_n = 1$ gilt. Dies ist gleichbedeutend damit, dass A eine Isometrie in $\mathcal{M}_{m,n}(\mathbb{R})$ ist. ■

Die Hilbert-Schmidt-Norm

Es seien $\mathcal{H}_1, \dots, \mathcal{H}_m$ Hilberträume und $V := \mathcal{H}_1 \otimes \dots \otimes \mathcal{H}_m$ das algebraische Tensorprodukt. An dieser Stelle möchten wir auf kanonische Weise ein Skalarprodukt auf V definieren, sodass V die Eigenschaften der Faktoren $\mathcal{H}_1, \dots, \mathcal{H}_m$ erbt.

Nach dem Satz von Riesz-Frechet ist ein Hilbertraum \mathcal{L} zu sich selbst dual, das heißt, es existiert ein antilinearer Isomorphismus

$$\begin{aligned} I: \mathcal{L} &\rightarrow \mathcal{L}^* \\ w &\mapsto v \mapsto \langle v, w \rangle. \end{aligned}$$

Somit ist auf kanonische Weise die folgende antilineare Abbildung konstruierbar:

$$\begin{aligned} J: V &\rightarrow V' \\ w_1 \otimes \dots \otimes w_m &\mapsto v \mapsto (\tilde{\beta}(I(w_1) \otimes \dots \otimes I(w_m)))(v). \end{aligned}$$

Entsprechend ist die Abbildung

$$\langle v, w \rangle := (J(w))(v) = \sum_{i=1}^s \sum_{j=1}^t \langle v_1^i, w_1^j \rangle \dots \langle v_m^i, w_m^j \rangle,$$

wobei $v = \sum_{i=1}^s v_1^i \otimes \dots \otimes v_m^i$ und $w = \sum_{j=1}^t w_1^j \otimes \dots \otimes w_m^j$ mit $v_k^i, w_k^j \in \mathcal{H}_k$ sind, wohldefiniert auf $V \times V$. Sie definiert ein Skalarprodukt auf V . Damit wird V zu einem Prä-Hilbertraum. Sind $\mathcal{H}_1, \dots, \mathcal{H}_m$ von endlicher Dimension, ist V ein Hilbertraum.

Definition 5.2.7 - Hilbert-Schmidt-Norm

Mit dem Symbol

$$\|v\|_{\text{HS}} := \sqrt{\langle v, v \rangle}$$

für $v \in V$ sei die *Hilbert-Schmidt-Norm* bezeichnet. □

Die Hilbert-Schmidt-Norm ist eine Kreuznorm. Weiterhin gilt:

Proposition 5.2.8 - Eigenschaften der Hilbert-Schmidt-Norm

Es gilt für $v \in V$:

- (i) $\|v\|_\epsilon \leq \|v\|_{\text{HS}} \leq \|v\|_\pi$.
- (ii) $v \in \text{ext}(\mathcal{B}_{1,\text{HS}})$, genau dann wenn $\|v\|_{\text{HS}} = 1$ gilt. □

Beweis. (i): Da ein Hilbertraum mit seinem Dual identifizierbar und die duale Norm zur Hilbert-Schmidt-Norm gleich der Operatornorm ist, folgt, dass die Hilbert-Schmidt-Norm zu sich selbst dual ist. Insbesondere ist die duale Norm eine Kreuznorm. Damit folgt aus Proposition 5.2.5, dass die Hilbert-Schmidt-Norm zwischen der injektiven und der projektiven Norm liegt.

(ii): Sei $v \in V$ mit $\|v\|_{\text{HS}} = 1$. Angenommen, es existieren $x, y \in V$, $\|x\|_{\text{HS}} = \|y\|_{\text{HS}} = 1$ und $v = \lambda x + (1 - \lambda)y$ mit $0 < \lambda < 1$. Dann gilt: $1 = \|v\|_{\text{HS}} \leq \lambda\|x\|_{\text{HS}} + (1 - \lambda)\|y\|_{\text{HS}} = 1$. Daraus folgt, dass $x = \mu y$ für einen Faktor $\mu \in (\mathbb{K})_1$ ist. Also ist $|\lambda\mu + (1 - \lambda)| = 1$. Da die Einheitskugel von \mathbb{K} strikt konvex ist, folgt $\mu = 1$ und damit $x = y$. ■

Abschließend möchten wir noch auf die Symmetriegruppe der Produktvektoren eingehen. Es sei \mathcal{H} die Vervollständigung des Tensorprodukts V bezüglich der Hilbert-Schmidt-Norm. Dann ist die Abbildung

$$\begin{aligned} \mathcal{B}(\mathcal{H}_1) \otimes \cdots \otimes \mathcal{B}(\mathcal{H}_m) &\rightarrow \mathcal{B}(\mathcal{H}) \\ T_1 \otimes \cdots \otimes T_m &\mapsto [x_1 \otimes \cdots \otimes x_m \rightarrow T_1(x_1) \otimes \cdots \otimes T_m(x_m)] \end{aligned}$$

eine Einbettung. Weiterhin bezeichne \mathcal{U}_i die unitäre Gruppe von \mathcal{H}_i und \mathcal{U} die unitäre Gruppe von \mathcal{H} .

Proposition 5.2.9 - Symmetrien der Produktvektoren

Die Gruppe

$$\mathcal{G}_{\mathcal{H}} := \{U_1 \otimes \cdots \otimes U_m \mid U_i \in \mathcal{U}_i \text{ für } i = 1, \dots, m\} \subseteq \mathcal{U}$$

ist invariant auf den Einheitsproduktvektoren $\mathcal{E}_{\mathcal{H}}$ und wirkt transitiv auf $\mathcal{E}_{\mathcal{H}}$. □

Beweis. Dies ist leicht einzusehen. ■

5.3 Produktvektoren als Varietät

Im vorigen Abschnitt haben wir gezeigt, dass die Einheitskugel der projektiven Norm die abgeschlossene konvexe Hülle der Einheitsproduktvektoren ist. Wie können wir diese konvexe Hülle beschreiben?

Zunächst stellt sich die Frage nach Kriterien dafür, wann ein Vektor ein Produktvektor ist. Das Ziel dieses Abschnitts ist, ein solches Kriterium zu finden. Motivierend ist, dass Produktvektoren der Länge eins in $\mathbb{R}^2 \otimes \mathbb{R}^2$ von der Gestalt

$$\begin{pmatrix} \cos(\varphi) \\ \sin(\varphi) \end{pmatrix} \otimes \begin{pmatrix} \cos(\psi) \\ \sin(\psi) \end{pmatrix}, \quad \varphi \in [0, 2\pi), \quad \psi \in [0, 2\pi)$$

sind. Identifizieren wir Tensoren mit darstellenden Matrizen linearer Abbildungen, also $x \otimes y \in \mathbb{R}^2 \otimes \mathbb{R}^2$ mit $\langle \cdot, y \rangle \cdot x \in \mathcal{M}_2(\mathbb{R})$, so hat ein solcher Produktvektor die Gestalt

$$\begin{pmatrix} \cos(\varphi)\cos(\psi) & \cos(\varphi)\sin(\psi) \\ \sin(\varphi)\cos(\psi) & \sin(\varphi)\sin(\psi) \end{pmatrix}.$$

Ein Vektor ist also genau dann ein Produktvektor, wenn die Determinante der darstellenden Matrix verschwindet. Wir sehen, dass sich diese Beobachtung verallgemeinern lässt. Es ist möglich, Produktvektoren als reelle algebraische Varietät zu schreiben.

Es sei $V := \mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_r}$ für natürliche Zahlen $n_1, \dots, n_r \geq 2$ und $r > 1$. Basisvektoren von \mathbb{R}^n seien gegeben durch $e_i := (\delta_i(k))_{k=1, \dots, n} \in \mathbb{R}^n$ für alle $i = 1, \dots, n$.

Tensoren als mehrstufige Matrizen

Notation. Auf der Menge

$$N := \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_r\}$$

definieren wir die *invers lexikographische Ordnung* \geq_{invlex} : Für zwei verschiedene Elemente $a, b \in N$ gelte genau dann $a \geq_{invlex} b$, falls der erste Eintrag in der Differenz $b - a$, der nicht Null ist, positiv ist. Weiterhin sei mit

$$\mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$$

der Vektorraum aller Abbildungen $N \rightarrow \mathbb{R}$ bezeichnet. Wir nennen ihn den Raum der *r-stufigen Matrizen*. Als Notation für eine *r*-stufige Matrix $N \rightarrow \mathbb{R}$, $i \mapsto \lambda_i$,

verwenden wir die Koeffizientenschreibweise $(\lambda_i)_{i \in N}$. Auf natürliche Weise sind die *Matrixeinheiten*

$$\{E_{k_1, \dots, k_r} := (\delta_{i_1}(k_1) \cdots \delta_{i_r}(k_r))_{i=(i_1, \dots, i_r) \in N} \mid k_1 \leq n_1, \dots, k_r \leq n_r\}$$

eine Basis dieses Vektorraums. Er ist daher isomorph zu $\mathbb{R}^{n_1 \cdots n_r}$. Weiterhin folgt mit Proposition 5.1.1, (i), dass ein Isomorphismus ι durch

$$\begin{aligned} \iota : \quad V &\rightarrow \mathcal{M}_{n_1, \dots, n_r}(\mathbb{R}) \\ e_{i_1} \otimes \cdots \otimes e_{i_r} &\mapsto E_{i_1, \dots, i_r} \end{aligned}$$

gegeben ist. Auf diese Weise ist eine kanonische Identifikation von mehrstufigen Matrizen mit mehrfachen Tensoren möglich. So identifizieren wir einen Produktvektor:

$$\begin{pmatrix} \lambda_1^1 \\ \vdots \\ \lambda_{n_1}^1 \end{pmatrix} \otimes \cdots \otimes \begin{pmatrix} \lambda_1^r \\ \vdots \\ \lambda_{n_r}^r \end{pmatrix} \mapsto (\lambda_{i_1}^1 \cdots \lambda_{i_r}^r)_{i=(i_1, \dots, i_r) \in N}.$$

Proposition 5.3.1 - Der Isomorphismus ι ist eine Isometrie zwischen V , versehen mit der Hilbert-Schmidt-Norm, und $\mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$, versehen mit der 2-Norm. \square

Beweis. Diese Aussage zeigt eine einfache Rechnung. Das Bild eines Einheitsproduktvektors v unter ι ist von der Form $(\lambda_{i_1}^1 \cdots \lambda_{i_r}^r)_{i=(i_1, \dots, i_r) \in N}$ mit $(\lambda_1^k)^2 + \cdots + (\lambda_{n_r}^k)^2 = 1$ für alle $k = 1, \dots, r$. Also gilt für die 2-Norm dieser Matrix:

$$\begin{aligned} \|\iota(v)\|_2^2 &= \sum_{i \in N} (\lambda_{i_1}^1)^2 \cdots (\lambda_{i_r}^r)^2 \\ &= \sum_{i \in \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_{r-1}\}} (\lambda_{i_1}^1)^2 \cdots (\lambda_{i_{r-1}}^{r-1})^2 \cdot \underbrace{((\lambda_1^r)^2 + \cdots + (\lambda_{n_r}^r)^2)}_{=1} \\ &= \sum_{i \in \{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_{r-1}\}} (\lambda_{i_1}^1)^2 \cdots (\lambda_{i_{r-1}}^{r-1})^2 = \dots = (\lambda_1^1)^2 + \cdots + (\lambda_{n_1}^1)^2 = 1. \end{aligned}$$

Die Abbildung bildet insbesondere eine Orthonormalbasis von V aus Produktvektoren normerhaltend auf die Matrixeinheiten von $\mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$ ab. \blacksquare

Die injektive Norm als Operatornorm

Wie im vorigen Abschnitt angekündigt, wollen wir einen Zusammenhang zwischen der injektiven Norm und Operatornormen aufzeigen. Eine mehrstufige Matrix kann

im geeigneten Sinn als Operator verstanden werden. Für $A = (a_i)_{i \in N} \in \mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$ und $b = (b_k)_{k \in \{1, \dots, n_r\}} \in \mathbb{R}^{n_r}$ sei das *Produkt* von A und b gegeben durch:

$$A \star b := \left(\sum_{k=1}^{n_r} a_{i_1, \dots, i_k} \cdot b_k \right)_{(i_1, \dots, i_{r-1}) \in \{1, \dots, n_1\} \times \dots \times \{1, \dots, n_{r-1}\}} \in \mathcal{M}_{n_1, \dots, n_{r-1}}(\mathbb{R}).$$

Die injektive Norm ist als Supremum über mehrfache Anwendungen von Vektoren auf eine mehrstufige Matrix gegeben:

Proposition 5.3.2 - Die injektive Norm als Operatornorm

Es gilt für $v \in V$:

$$\|v\|_\epsilon = \sup\{|\iota(v) \star b_r \star b_{r-1} \star \dots \star b_1| \mid b_i \in (\mathbb{R}^{n_i})_1, i = 1, \dots, r\}. \quad \square$$

Beweis. Es sei $v = x_1 \otimes \dots \otimes x_r \in V$ ein Produktvektor. Bezeichnen wir die k -te Komponente von x_i mit λ_k^i , $k = 1, \dots, n_i$, so ist

$$\begin{aligned} \iota(v) \star b_r \star b_{r-1} \star \dots \star b_1 &= (\lambda_{i_1}^1 \dots \lambda_{i_r}^r)_{i=(i_1, \dots, i_r) \in N} \star b_r \star b_{r-1} \star \dots \star b_1 \\ &= (\lambda_{i_1}^1 \dots \lambda_{i_{r-1}}^{r-1} \cdot \langle x_r, b_r \rangle)_{i=(i_1, \dots, i_{r-1})} \star b_{r-1} \star \dots \star b_1 \\ &= \langle x_r, b_r \rangle \cdot \iota(x_1 \otimes \dots \otimes x_{r-1}) \star b_{r-1} \star \dots \star b_1 = \dots \\ &= \langle x_r, b_r \rangle \langle x_{r-1}, b_{r-1} \rangle \dots \langle x_1, b_1 \rangle. \quad \blacksquare \end{aligned}$$

Beispiel 5.3.3 Mit dieser Darstellung können Normen, die zwischen $\|\cdot\|_\epsilon$ und $\|\cdot\|_\pi$ liegen, konstruiert werden.

Behauptung: Die Norm auf $V := ((\mathbb{R}^{n_1} \otimes \mathbb{R}^{n_2}, \|\cdot\|_\pi) \otimes \mathbb{R}^{n_3}, \|\cdot\|_\epsilon)$ ist gegeben durch:

$$\sup\{\|\iota(v) \star b\|_\pi \mid b \in (\mathbb{R}^{n_3})_1\}$$

für $v \in V$.

Beweis: Es sei $v = \sum_{i=1}^s x_i \otimes y_i \otimes z_i$. Die Norm auf dem Tensorprodukt sei bezeichnet mit $\|\cdot\|_\alpha$. Da die injektive und die projektive Norm für ein zweifaches Tensorprodukt endlichdimensionaler Vektorräume zueinander dual sind, gilt:

$$\begin{aligned} \|v\|_\alpha &= \sup \left\{ \left| \sum_{i=1}^s \psi(x_i \otimes y_i) \langle z_i, b \rangle \right| \mid \|\psi\|_\epsilon \leq 1, b \in (\mathbb{R}^{n_3})_1 \right\} \\ &= \sup \left\{ \left| \psi \left(\sum_{i=1}^s \langle z_i, b \rangle (x_i \otimes y_i) \right) \right| \mid \|\psi\|_\epsilon \leq 1, b \in (\mathbb{R}^{n_3})_1 \right\} \\ &= \sup \{ |\psi(\iota(v) \star b)| \mid \|\psi\|_\epsilon \leq 1, b \in (\mathbb{R}^{n_3})_1 \} \\ &= \sup \{ \|\iota(v) \star b\|_\pi \mid b \in (\mathbb{R}^{n_3})_1 \}. \end{aligned}$$

Daraus folgt die Aussage. ◇

Solch eine Darstellung kann beliebig verallgemeinert werden. □

Ein Kriterium für Produktvektoren

Zunächst zitieren wir ein Resultat aus der algebraischen Geometrie, siehe [Har]:

Lemma 5.3.4 - Satz von Segré

Ein Vektor $v \in \mathbb{R}^m \otimes \mathbb{R}^n$ ist genau dann ein Produktvektor, wenn alle 2×2 -Unterdeterminanten von $\iota(v)$ verschwinden. \square

Beweis. Es sei $v \in \mathbb{R}^m \otimes \mathbb{R}^n$ ein Produktvektor. Dann existieren $x = \sum_{i=1}^m \lambda_i e_i \in \mathbb{R}^m$ und $y = \sum_{j=1}^n \mu_j e_j \in \mathbb{R}^n$ mit $v = x \otimes y = \sum_{i=1}^m \sum_{j=1}^n \lambda_i \mu_j (e_i \otimes e_j)$. Nun ist leicht zu sehen, dass alle 2×2 -Unterdeterminanten von $\iota(v) = (\lambda_i \mu_j)_{i=1, \dots, m; j=1, \dots, n}$ verschwinden. Nun zeigen wir die andere Implikation. Ein Tensor $v \in \mathbb{R}^m \otimes \mathbb{R}^n$ erfülle die Voraussetzung, das heißt, alle 2×2 -Unterdeterminanten von $\iota(v) = (\lambda_{i,j})_{i=1, \dots, m; j=1, \dots, n}$ verschwinden. Falls alle Einträge von $\iota(v)$ verschwinden, ist $v = 0$.

Behauptung: Falls $v \neq 0$ gilt, ist $\iota(v)$ vom Rang eins.

Sei $\lambda_{i,j} \neq 0$. Wir betrachten alle Einträge, die in der gleichen Zeile liegen. Ist ein solcher Eintrag null, folgt aus der Voraussetzung, dass alle Einträge in der gleichen Spalte ebenfalls null sind. Ist ein solcher Eintrag $\lambda_{i,j'} \neq 0$ ungleich null, so gilt für alle nicht verschwindenden Einträge $\lambda_{i',j'} \neq 0$:

$$\frac{\lambda_{i,j}}{\lambda_{i,j'}} = \frac{\lambda_{i',j}}{\lambda_{i',j'}}.$$

Da Verhältnissbildung auf reellen Zahlentupeln mit nicht verschwindender zweiter Komponente transitiv ist, folgt, dass alle Zeilen Vielfache voneinander sind. \diamond

Eine $m \times n$ -Matrix A vom Rang r kann als Produkt einer $m \times r$ -Matrix A_1 und einer $r \times n$ -Matrix A_2 , wobei A_1 und A_2 den Rang r besitzen, geschrieben werden. Daher existieren Vektoren $x \in \mathbb{R}^m$ und $y \in \mathbb{R}^n$ mit $\iota(v) = x \cdot y^t = (x_i y_j)_{i=1, \dots, m; j=1, \dots, n}$ und es ist $v = x \otimes y$. \blacksquare

Jetzt verallgemeinern wir dieses Resultat.

Satz 5.3.5 - Determinantenkriterium für Produktvektoren

Für einen Vektor $v := (\lambda_{i_1, \dots, i_r})_{i=(i_1, \dots, i_r) \in N} \in \mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$ sind äquivalent:

- (a) $\iota^{-1}(v)$ ist ein Produktvektor.
- (b) Es gilt

$$\det \begin{pmatrix} \lambda_{i_1, \dots, i_r} & \lambda_{j_1, \dots, j_r} \\ \lambda_{k_1, \dots, k_r} & \lambda_{l_1, \dots, l_r} \end{pmatrix} = 0$$

für alle Indizes mit den folgenden Eigenschaften: Es existiert ein $t \in \{1, \dots, r\}$, sodass für alle $s \in \{1, \dots, r\}$ die Kriterien

- (i) Ist $s = t$, so gilt: $i_s = k_s$ und $j_s = l_s$.
- (ii) Ist $s \leq t - 1$, so gilt: $i_s = j_s$ und $k_s = l_s$.
- (iii) Ist $s \geq t + 1$, so gilt: $i_s = k_s = j_s = l_s$.

erfüllt sind. □

Beweis. (a) \Rightarrow (b): Dass das Bild eines Produktvektors unter ι diese Eigenschaften erfüllt, ist leicht zu sehen, da es von der Form $(\lambda_{i_1}^1 \cdots \lambda_{i_r}^r)_{i_1 \in \{1, \dots, n_1\}, \dots, i_r \in \{1, \dots, n_r\}}$ ist.

(b) \Rightarrow (a): Es sei $r > 1$. Die Determinanten, die das Kriterium für $t = r$ erfüllen, beschreiben die Faktorisierung in der letzten Komponente nach Lemma 5.3.4. Also ist v Produktvektor in $(\mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_{r-1}}) \otimes \mathbb{R}^{n_r}$. Im Fall $v \neq 0$ existiert ein Basisvektor von \mathbb{R}^{n_r} , sodass die letzte Komponente einen echten Anteil daran besitzt. Die Determinanten für $t = r - 1$ und $i_r = i$, wobei v in der letzten Komponente einen echten Anteil an einem Basisvektor $e_i \in \mathbb{R}^{n_r}$ besitzt, beschreiben jeweils die Faktorisierung in den ersten $r - 1$ Komponenten. Die anderen Determinanten sind null. Induktiv folgt mit Lemma 5.1.5, dass v ein Produktvektor ist. ■

Das Determinantenkriterium zeigt, dass die Eigenschaft, Produktvektor zu sein, algebraisiert werden kann. Dies werden wir im nächsten Abschnitt behandeln.

Produktvektoren als Varietät

Den Polynomring $\mathbb{R}[x_i \mid i \in N]$ versehen wir mit der graduierten lexikographischen Ordnung, wobei N und damit alle Monome vom Grad eins wie im letzten Unterabschnitt invers lexikographisch geordnet sind. Verschwindemengen von Polynomen in $\mathbb{R}[x_i \mid i \in N]$ sehen wir ausschließlich als Elemente in $\mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$ an. Es sei

$$f_{i,j,k,l} := x_i x_l - x_j x_k \in \mathbb{R}[x_i \mid i \in N]$$

für jeweils vier Indizes $i, j, k, l \in N$.

Das oben genannte Kriterium erlaubt es, die Menge der Produktvektoren als gemeinsame Verschwindemenge spezieller Determinanten darzustellen. Die Menge

$$P := \{f_{i,j,k,l} \mid i, j, k, l \in N \text{ erfüllen die Bedingung aus Satz 5.3.5, (b) und der Leitterm von } f_{i,j,k,l} \text{ hat ein positives Vorzeichen}\}$$

enthält alle Determinanten, welche zur Charakterisierung von Produktvektoren wesentlich sind. Sie erzeugt die zwei Ideale

$$\mathcal{J}_V := \langle P \rangle \text{ und}$$

$$\mathcal{J}_V := \left\langle \mathcal{J}_V, 1 - \sum_{i \in N} x_i^2 \right\rangle.$$

Korollar 5.3.6 - Produktvektoren als reelle algebraische Varietät

Es gilt: $\iota(\mathcal{P}_V) = \mathcal{Z}(\mathcal{J}_V)$ und $\iota(\mathcal{E}_V) = \mathcal{Z}(\mathcal{J}_V) = \mathcal{Z}(\mathcal{J}_V) \cap \mathcal{Z}(1 - \sum_{i \in N} x_i^2)$. □

Beweis. Die erste Aussage folgt direkt aus Satz 5.3.5. Weiterhin ist ein Produktvektor nach Proposition 5.3.1 genau dann normiert, wenn das Bild unter ι Nullstelle des Polynoms $1 - \sum_{i \in N} x_i^2$ ist. ■

Insbesondere ist die Menge der Einheitsproduktvektoren kompakt.

Wir ergänzen ein technisches Detail. Die Determinanten sind bis auf Vielfache bereits durch ihre Diagonalen bestimmt.

Proposition 5.3.7 - Charakterisierung der Determinanten

Es gilt:

- (i) Sei $(i, l) \in N^2$, sodass sich i und l in mindestens zwei Stellen unterscheiden und $i > l$ gilt. Dann existiert genau ein Paar $(j, k) \in N^2$, sodass $j > k$ und $f_{i,j,k,l} \in P \cup (-P)$.
- (ii) Ist $f \in P$, dann existiert genau ein $(i, j, k, l) \in N^4$ mit $i > j > k > l$, sodass $f = f_{i,j,k,l}$. Insbesondere unterscheiden sich i und l in mindestens zwei Stellen.
- (iii) Es ist

$$\#P = \frac{1}{2} \dim(V) (\dim(V) + r - 1 - (n_1 + \dots + n_r)),$$

wobei $\dim(V) = n_1 \cdot \dots \cdot n_r$ gilt. □

Beweis. (i): Seien $(i, l) \in N^2$ gegeben. Sind alle Stellen von i und l verschieden, existieren eindeutige Indizes $(j, k) \in N^2$, $j > k$, sodass i, j, k, l die Bedingung aus Satz 5.3.5, (b) erfüllen. Weiterhin ist $f_{i,j,k,l} \neq 0$, das heißt, die Aussage ist wahr. Sei nun $t := \max\{s \in \{1, \dots, r\} \mid i_s \neq l_s\}$. Dann ist $t > 1$. Setzen wir nun

$$j := (i_1, \dots, i_{t-1}, l_t, i_{t+1}, \dots, i_r), \quad k := (l_1, \dots, l_{t-1}, i_t, i_{t+1}, \dots, i_r)$$

für $t < r$ und

$$j := (i_1, \dots, i_{r-1}, l_r), \quad k := (l_1, \dots, l_{r-1}, i_r)$$

für $t = r$, so erfüllen i, j, k, l die Bedingung aus Satz 5.3.5, (b). Nach Voraussetzung ist $i \neq j$ und $i \neq k$, also folgt: $f_{i,j,k,l} \in P \cup (-P)$. Es bleibt noch die Eindeutigkeit von (j, k) zu zeigen. Seien $(j', k') \in N^2$ mit $j' > k'$ und $f_{i,j',k',l} \in P \cup (-P)$. Dann existiert ein $t' \in \{1, \dots, r\}$, sodass für alle $s \in \{1, \dots, r\}$ die Kriterien (i), (ii) und (iii) aus Satz 5.3.5, (b) erfüllt sind. Es folgt, dass $t' \geq t$ ist. Angenommen, es ist $t' > t$. Dann ist $a = j'$ oder $a = k'$, was nach Voraussetzung ausgeschlossen ist. Es folgt also $t' = t$ und damit ist $(j', k') = (j, k)$.

(ii): Sei $f \in P$. Dann existieren $(i, l) \in N^2$ mit $i > l$, sodass $\text{LT}(f) = x_i x_l$. Weiterhin existiert ein $t \in \{1, \dots, r\}$, sodass $i_t \neq l_t$ ist und f die Gestalt

$$\begin{aligned} f &= x_i x_l - x_j x_k \quad \text{mit} \\ i &= (i_1, \dots, i_{t-1}, i_t, i_{t+1}, \dots, i_r), \quad j := (i_1, \dots, i_{t-1}, l_t, i_{t+1}, \dots, i_r) \\ k &:= (l_1, \dots, l_{t-1}, i_t, i_{t+1}, \dots, i_r), \quad l = (l_1, \dots, l_{t-1}, l_t, i_{t+1}, \dots, i_r) \end{aligned}$$

für $t < r$ und

$$i = (i_1, \dots, i_r), \quad j := (i_1, \dots, i_{r-1}, l_r), \quad k := (l_1, \dots, l_{r-1}, i_r), \quad l = (l_1, \dots, l_{r-1}, l_r)$$

für $t = r$ besitzt. Da nach Voraussetzung $f \neq 0$ gilt, existiert ein $t'' \in \{1, \dots, t-1\}$ mit $i_{t''} \neq l_{t''}$. Daraus folgt: $(i_1, \dots, i_{t-1}, 1, \dots, 1) > (l_1, \dots, l_{t-1}, 1, \dots, 1)$. Insbesondere ist $i > j > k > l$.

(iii): Sei $d := \dim(V)$. Für alle $i \in N$ gilt

$$\begin{aligned} S_i &:= \#\{j \in N \mid i > j \text{ und } i \text{ und } j \text{ unterscheiden sich an genau einer Stelle}\} \\ &= (n_1 - i_1) + \dots + (n_r - i_r) = (n_1 + \dots + n_r) - (i_1 + \dots + i_r). \end{aligned}$$

Weiterhin ist

$$\begin{aligned} S_2 &:= \#\{(i, j) \in N^2 \mid i > j\} \\ &= (d-1) + (d-2) + \dots + 1 = d(d-1)/2 \quad \text{und} \\ \sum_{i \in N} \sum_{s=1}^r i_s &= (1+2+\dots+n_1) \cdot n_2 \cdot \dots \cdot n_r + (1+2+\dots+n_2) \cdot n_1 \cdot n_3 \cdot \dots \cdot n_r + \dots \\ &\quad + (1+2+\dots+n_r) \cdot n_1 \cdot \dots \cdot n_{r-1} \\ &= \left(\sum_{s=1}^r \frac{n_s(n_s+1)}{2} \right) \cdot \prod_{\substack{t=1, \dots, r \\ t \neq s}} n_t = \frac{d \cdot r}{2} + \frac{d}{2} \cdot \sum_{s=1}^r n_s. \end{aligned}$$

Es folgt:

$$\begin{aligned} \#P &:= S_2 - \sum_{i \in N} S_i = d(d-1)/2 - d(n_1 + \dots + n_r) + \frac{d \cdot r}{2} + \frac{d}{2} \cdot \sum_{s=1}^r n_s \\ &= \frac{1}{2} (d^2 + d(-1 - (n_1 + \dots + n_r) + r)) = \frac{d}{2} (d + r - 1 - (n_1 + \dots + n_r)), \end{aligned}$$

was zu beweisen war. ■

Im Wesentlichen sind damit alle Determinanten durch Angabe ihrer Diagonaleinträge bestimmt. Weiterhin bemerken wir den Zusammenhang zwischen $\#P$ und der maximalen Dimension eines *vollständig verschränkten Unterraums* des Tensorprodukts $\mathbb{C}^{n_1} \otimes \dots \otimes \mathbb{C}^{n_r}$, siehe [Par].

Das Verschwindeideal der Produktvektoren

Im Folgenden untersuchen wir die Polynome, die die Eigenschaft eines Tensors, Produktvektor zu sein, codieren, nach ihrer Eigenschaften als Erzeugendensystem eines Ideals. Erzeugen sie das Verschwindeideal der Produktvektoren? Das Resultat kommt im nächsten Kapitel zur Anwendung.

Lemma 5.3.8 - Produktvektoren und Gröbnerbasen

Es sind äquivalent:

- (a) P ist eine Gröbnerbasis für \mathcal{J}_V .
- (b) $r = 2$.

In diesem Fall ist P sogar eine reduzierte Gröbnerbasis für \mathcal{J}_V . Im Fall $r > 2$ ist das Erzeugendensystem $P \cup \{1 - \sum_{i \in N} x_i^2\}$ keine Gröbnerbasis für \mathcal{J}_V . □

Beweis. Sei $P' := \{f_{i,j,k,l} \mid i, j, k, l \in N \text{ erfüllen die Bedingung aus Satz 5.3.5, (b)}\}$.

(b) \Rightarrow (a): Sei zunächst $r = 2$. Wir zeigen durch Anwendung des Kriteriums von Buchberger, Satz 1.2.2 auf Seite 9, dass P eine Gröbnerbasis von \mathcal{J}_V ist. Es seien zwei Determinanten $f, g \in P$ mit $f := f_{a,b,c,d}$ und $g := f_{k,l,n,m}$ für $(a, b, c, d) \in N^4$ und $(k, l, n, m) \in N^4$ gegeben. Wir nehmen an, dass $a > b > c > d$, $k > l > m > n$ gilt. Weiterhin sei $f \neq g$ und $a \geq k$. Wir zeigen nun, dass der Rest der Division des S-Polynoms von f und g durch P verschwindet. Da f und g beliebig gewählt sind, folgt mit dem Kriterium von Buchberger, dass P eine Gröbnerbasis für \mathcal{J}_V ist.

Zunächst bestimmen wir das kleinste gemeinsame Vielfache des Leitterms $x_a x_d$ von f und des Leitterms $x_k x_n$ von g . Es ist

$$\text{LCM}(x_a x_d, x_k x_n) = \begin{cases} x_a x_d x_k x_n, & a \neq k \text{ und } d \neq n \\ x_a x_d x_n, & a = k \text{ und } d \neq n \\ x_a x_d x_k, & a \neq k \text{ und } d = n \end{cases}$$

Der Fall $a = k$ und $d = n$ tritt nicht auf, da wir $f \neq g$ vorausgesetzt haben.

Fall 1: $a \neq k$ und $d \neq n$.

Es ist

$$\begin{aligned} S(f, g) &= x_k x_n \cdot f - x_a x_d \cdot g = x_a x_d x_l x_m - x_b x_c x_k x_n \\ &= x_l x_m \cdot f - x_b x_c \cdot g. \end{aligned}$$

Da der Leitterm $x_a x_d x_l x_m$ von $S(f, g)$ nicht kleiner als der Grad von $x_l x_m \cdot f$ und von $x_b x_c \cdot g$ ist, folgt, dass der Rest der Division von $S(f, g)$ durch P null ist.

Es existieren Indizes $a', b', c', d' \in N$ und $k', l', n', m' \in N$, sodass alle 2×2 -Untermi-
noren der Matrix

$$M := \begin{pmatrix} x_a & x_b & x_{a'} & x_{b'} \\ x_c & x_d & x_{c'} & x_{d'} \\ x_{k'} & x_{l'} & x_k & x_l \\ x_{m'} & x_{n'} & x_m & x_n \end{pmatrix}$$

Elemente aus P' sind.

Fall 2: $a = k$ und $d \neq n$.

In diesem Fall können wir annehmen, dass $b \geq l$ gilt. Es ist

$$S(f, g) = x_n \cdot f - x_d \cdot g = -x_b x_c x_n + x_d x_l x_m.$$

Im Fall $b = l$ gilt: $S(f, g) = -x_l(x_c x_n - x_d x_m)$. Da $f_{c,n,d,m} \in P'$, folgt die Aussage. Sei nun $b > l$. Der Leitterm von $S(f, g)$ ist $-x_b x_c x_n$. Es ist

$$\begin{aligned} S(f, g) &= -x_c(x_b x_n - x_{n'} x_{b'}) - x_c x_{n'} x_{b'} + x_d x_l x_m \\ &= -x_c(x_b x_n - x_{n'} x_{b'}) - x_{b'}(x_c x_{n'} - x_d x_m), \end{aligned}$$

da $m = m'$ und $l = b'$. Da x_b größer als Einträge der Matrix M außer x_a ist, ist das Monom $x_b x_c x_n$ nicht kleiner als alle Monome der obigen Darstellung von $S(f, g)$. Damit folgt die Aussage.

Fall 3: $a \neq k$ und $d = n$.

Es ist $a > k$, $m = c'$ und $b = b'$. Daraus folgt:

$$\begin{aligned} S(f, g) &= x_k \cdot f - x_a \cdot g = x_a x_l x_m - x_b x_c x_k \\ &= x_m(x_a x_l - x_{b'} x_{k'}) - x_b(x_c x_k - x_m x_{k'}) \\ &= x_m(x_a x_l - x_{b'} x_{k'}) - x_b(x_c x_k - x_{c'} x_{k'}) \end{aligned}$$

mit dem Leitterm $x_a x_l x_m$. Da $f_{a,b',k',l} \in P'$ und $f_{c,c',k',k} \in P'$, folgt die Behauptung. Wir haben nun bewiesen, dass P eine Gröbnerbasis ist. Da alle Leiterterme von Elementen in P ein positives Vorzeichen haben, Monome vom Grad zwei und keine Quadrate sind, ist P reduziert.

Zum Beweis der anderen Implikation und der weiteren Aussagen benutzen wir die Definition einer Gröbnerbasis. Wir geben ein Polynom an, welches im Ideal liegt, dessen Leitterm aber nicht durch den Leitterm eines Erzeugers teilbar ist. Sei zunächst $r = 3$ und $n_1 = n_2 = n_3 = 2$. Es seien die Polynome

$$f := x_{1,1,1}x_{2,2,1} - x_{1,2,1}x_{2,1,1} \in P \quad \text{und} \quad g := x_{1,1,1}x_{1,2,2} - x_{1,1,2}x_{1,2,1} \in P$$

definiert. Das S-Polynom von f und g ist

$$S(f, g) = x_{1,1,2}x_{1,2,1}x_{2,2,1} - x_{1,2,1}x_{1,2,2}x_{2,1,1}.$$

(a) \Rightarrow (b): Der Leitterm von $S(f, g)$ ist $x_{1,1,2}x_{1,2,1}x_{2,2,1}$. Davon sind alle Faktoren vom Grad zwei, $x_{1,2,1}x_{2,2,1}$, $x_{1,1,2}x_{1,2,1}$ und $x_{1,1,2}x_{2,2,1}$, keine Leiterterme eines Polynoms aus P . Da der Leitterm von $S(f, g)$ auch nicht durch den Leitterm des Normierungspolynoms $1 - \sum_{i \in N} x_i^2$ teilbar ist, folgt, dass $P \cup \{1 - \sum_{i \in N} x_i^2\}$ keine Gröbnerbasis für \mathcal{J}_V ist.

In allen anderen Fällen mit $r \geq 3$ sind in analoger Weise Gegenbeispiele konstruierbar. Wir wählen hierfür f und g wie oben und ergänzen die Indizes der Variablen jeweils um $r - 3$ Einsen. Dann folgt die Aussage mit Proposition 5.3.7. \blacksquare

Mit dem reellen Nullstellensatz folgt aus der letzten Aussage, dass Polynome, die auf den Produktvektoren verschwinden, von Determinanten erzeugt werden:

Satz 5.3.9 - Das Verschwindeideal der Produktvektoren

Für $r = 2$ gilt: $\mathcal{J}(\mathcal{Z}(\mathcal{J}_V)) = \mathcal{J}_V$. \square

Beweis. Sei $r = 2$. Wir beweisen, dass das Ideal \mathcal{J}_V reell ist, da daraus nach dem reellen Nullstellensatz 2.3.10 direkt die Aussage folgt. Nach Definition 2.1.17 ist dafür zu zeigen: Aus $a_1, \dots, a_s \in \mathbb{R}[x_i \mid i \in N]$ mit $\sum_{i=1}^s a_i^2 \in \mathcal{J}_V$ folgt, dass $a_i \in \mathcal{J}_V$ für alle $i = 1, \dots, s$ gilt. Wir nehmen das Gegenteil an. Es sei o.B.d.A. $a_1 \notin \mathcal{J}_V$. Weiterhin sei $k \in \{1, \dots, s\}$ so gewählt, dass $a_1, \dots, a_k \notin \mathcal{J}_V$ und $a_i \in \mathcal{J}_V$ für alle $i \in \{1, \dots, s\}$ mit $i > k$ ist. Es ist $-a_i^2 \in \mathcal{J}_V$ für $i \in \{1, \dots, s\}$, $i > k$. Daraus folgt: $a_1^2 + \dots + a_k^2 \in \mathcal{J}_V$. Nach Lemma 5.3.8 ist das Erzeugendensystem P von \mathcal{J}_V eine Gröbnerbasis. Es seien mit r_1, \dots, r_k jeweils die Reste der Division von a_1, \dots, a_k durch P bezeichnet.

Behauptung: Es ist $\text{LT}(r_i)^2 = \text{LT}(r_i^2)$.

Beweis: Der Term $\text{LT}(r_i)^2$ hat unter den Monomen von r_i^2 , die den höchsten Grad besitzen, den größten Multigrad bezüglich der lexikographischen Ordnung. \diamond

Wir nehmen im Folgenden an, dass $\text{LM}(\sum_{i=1}^k r_i^2) = \text{LM}(r_1)^2$ gilt.

Behauptung: $\text{LM}(r_1)^2$ ist reduziert bezüglich P .

Beweis: Das Leitmonom eines Polynoms $p \in P$ besitzt die Form $x_b x_c$ für $b, c \in N$ und $b \neq c$. Angenommen, $\text{LM}(r_1)^2$ ist durch $x_b x_c$ teilbar. Dann folgt, dass $\text{LM}(r_1)$ teilbar durch $x_b x_c$ ist. Dies ist ein Widerspruch zur Annahme, dass r_i reduziert bezüglich P ist. \diamond

Da $r_1^2 + \dots + r_k^2 \in \mathcal{J}_V$ gilt, muss $\text{LM}(r_1)^2$ durch den Leitterm eines Polynoms $p \in P$ teilbar sein. Dies ist aber nach der vorigen Behauptung unmöglich. Dies ist ein Widerspruch zur Annahme, dass $a_1 \notin \mathcal{J}_V$ ist. Es folgt: $a_1, \dots, a_s \in \mathcal{J}_V$. \blacksquare

An dieser Stelle möchten wir anhand eines Beispiels aufzeigen, wie groß eine reduzierte Gröbnerbasis für \mathcal{J}_V werden kann.

Beispiel 5.3.10 Wir stellen natürlichen Zahlen n_1, \dots, n_r mit $V := \mathbb{R}^{n_1} \otimes \dots \otimes \mathbb{R}^{n_r}$ die Länge L der reduzierten Gröbnerbasis für \mathcal{J}_V zur lexikographischen Ordnung gegenüber. Es sei $D := (\#P) + 1$ die Anzahl der im vorigen Unterabschnitt vorgestellten Erzeuger für \mathcal{J}_V , die aus geeigneten Determinanten und dem Normierungspolynom $1 - \sum_{i \in N} x_i^2$ bestehen.

n_1, \dots, n_r	$\dim(V)$	D	L
2, 2	4	2	4
2, 3	6	4	9
3, 3	9	10	23
5, 5	25	101	217
6, 6	36	226	476
2, 2, 2	8	9	22
2, 2, 3	12	22	56
2, 3, 3	18	55	137
3, 3, 3	27	136	371
3, 3, 4	36	253	767
2, 2, 2, 2	16	45	119
2, 2, 2, 2, 2	32	209	645

Durch Adjungtion des Normierungspolynoms zu \mathcal{J}_V entstehen neue Leittermine, die die reduzierte Gröbnerbasis sichtlich vergrößern. Auffällig ist, dass die Werte für $\dim(V)$ und D für $\mathbb{R}^6 \otimes \mathbb{R}^6$ größer als für $\mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2 \otimes \mathbb{R}^2$ sind, dies jedoch nicht für L gilt. Vermutlich ist die Länge der reduzierten Gröbnerbasis für gleichbleibende Werte von $\dim(V)$ desto höher, je größer r ist. \square

6 Approximation der Pi-Norm-Einheitssphäre

In diesem Kapitel untersuchen wir, wie die projektive Norm mittels *Thetanormen* bestimmt werden kann. Wir zeigen, dass der erste Thetakörper im einfachst denkbaren Fall, wenn der zugrunde liegende Vektorraum ein reelles zweifaches Tensorprodukt ist, bereits die Einheitssphäre der projektiven Norm liefert. In diesem Fall ist die projektive Norm gleich der ersten Thetanorm. Diese Thetanorm kann in der Praxis durch die Darstellung des ersten Thetakörpers als projizierter Spektraeder berechnet werden. Methoden hierfür stellen wir im nächsten Kapitel vor.

Im ersten Abschnitt zeigen wir, dass die Einheitssphäre der projektiven Norm als konvexe Hülle der Einheitsproduktvektoren, die eine reelle algebraische Varietät bilden, durch Thetakörper approximierbar ist. Diese Thetakörper bilden eine Kette von Kreuznormen, die zwischen der projektiven und der Hilbert-Schmidt-Norm liegen. Wir liefern verschiedene Ansätze, die Güte der Approximation zu bestimmen. Um diese zu präzisieren, entwickeln wir im zweiten Abschnitt geometrische Methoden, die Größe von Thetakörpern einzuschränken, insbesondere die Theorie der *Polaren* einer kompakten konvexen Menge. So können wir die Ergebnisse des ersten Abschnitts verallgemeinern und folgern das Resultat im dritten Abschnitt.

Es sei $V := \mathbb{R}^{n_1} \otimes \dots \otimes \mathbb{R}^{n_r}$ für natürliche Zahlen $r \geq 2$ und $n_1, \dots, n_r \geq 2$. Wir übernehmen die Notation aus Abschnitt 5.3. Weiterhin seien mit \mathcal{T}_k , $k \in \mathbb{N}$, die zum Ideal $\mathcal{J}_V \subseteq \mathbb{R}[x_i \mid i \in N]$ gebildeten Thetakörper bezeichnet. Im dritten Abschnitt beschränken wir uns auf den Fall $r = 2$.

6.1 Thetakörper induzieren Normen

In den Kapiteln 5, 4 und 2 haben wir Vorarbeit geleistet, sodass dieses zentrale Resultat eine direkte Folgerung aus den Sätzen dieser Kapitel ist:

Korollar 6.1.1 - Pi-Norm-Einheitssphäre als Schnitt von Thetakörpern

Es gilt: $\iota(\mathcal{B}_{1,\pi}) = \bigcap_{k=1}^{\infty} \mathcal{T}_k$. □

Beweis. Nach Proposition 5.2.3 gilt: $\mathcal{B}_{1,\pi} = \text{co}(\mathcal{E}_V)$. Nach Korollar 5.3.6 sind die Einheitsproduktvektoren eine kompakte reelle algebraische Varietät: $\iota(\mathcal{E}_V) = \mathcal{Z}(\mathcal{J}_V)$. Nach Satz 4.1.5 ist $\bigcap_{k=1}^{\infty} \mathcal{T}_k = \text{co}(\mathcal{Z}(\mathcal{J}_V)) = \text{co}(\iota(\mathcal{E}_V)) = \iota(\text{co}(\mathcal{E}_V)) = \iota(\mathcal{B}_{1,\pi})$. ■

Es stellt sich die Frage nach der Güte dieser Konvergenz. Konvergieren die Thetakörper rasch gegen ihren Schnitt? Dies wollen wir im Folgenden untersuchen.

Die Größe von Thetakörpern. Der äußere Radius

In diesem Unterabschnitt bestimmen wir die kleinste skalierte Einheitssphäre zur Hilbert-Schmidt-Norm, welche Obermenge des ersten Thetakörpers von \mathcal{J}_V ist. Den Radius dieser Sphäre bezeichnen wir als den *äußeren Radius*.

Der Rand der Einheitssphäre der Hilbert-Schmidt-Norm ist die zum Ideal

$$I := \left\langle 1 - \sum_{i \in N} x_i^2 \right\rangle$$

gebildete reelle algebraische Varietät. Somit kann sie durch Thetakörper approximiert werden.

Satz 6.1.2 - Die Hilbert-Schmidt-Einheitssphäre

Mit \mathcal{T} sei der erste Thetakörper von I bezeichnet. Dann gilt: $\mathcal{T} = \mathcal{B}_{1,\text{HS}}$. □

Beweis. Es ist $\text{co}(\mathcal{Z}(I)) = \mathcal{B}_{1,\text{HS}}$. Damit ist \mathcal{T} eine Obermenge von $\mathcal{B}_{1,\text{HS}}$. Sei $v \in V$ mit $\|v\|_{\text{HS}} = 1$. Wir setzen: $v_\lambda = \lambda \cdot v$ für $\lambda > 0$. Das Polynom

$$\frac{1}{2} \cdot \sum_{i \in N} (x_i - \iota(v)_i)^2$$

ist eine Summe von Quadraten und kongruent zu dem affin-linearen Polynom

$$l := 1 - \sum_{i \in N} \iota(v)_i \cdot x_i$$

modulo I . Es ist

$$l(v_\lambda) = 1 - \sum_{i \in N} \iota(v)_i \cdot \iota(\lambda v)_i = 1 - \lambda \sum_{i \in N} \iota(v)_i^2 = 1 - \lambda.$$

Damit existiert genau dann ein Polynom, welches 1-sos-mod I und an v_λ negativ ist, wenn $\lambda > 1$ ist. ■

Es ist daher möglich, den ersten Thetakörper von \mathcal{J}_V in die Einheitskugel der Hilbert-Schmidt-Norm einzufassen:

Korollar 6.1.3 - Der äußere Radius

Der äußere Radius von \mathcal{T}_1 ist eins. □

Beweis. Ist ein Polynom 1-sos-mod I , so ist es auch 1-sos-mod \mathcal{J}_V . Es folgt also mit Satz 6.1.2 die Inklusion $\mathcal{T}_1 \subseteq \mathcal{B}_{1,HS}$ für den ersten Thetakörper \mathcal{T}_1 von \mathcal{J}_V . Die Einheitskugel der projektiven Norm berührt den Rand der Hilbert-Schmidt-Einheitskugel an den Einheitsproduktvektoren, da beide Normen Kreuznormen sind. Damit folgt die Aussage. ■

Thetakörper induzieren eine Kette von Normen

Das Minkowskifunktional zu einer konvexen, absorbierenden und kreisförmigen Teilmenge eines Vektorraums, die keine linearen Teilräume enthält, ist eine Norm. Dies ist eine Folgerung aus Lemma III.2.2 in [Wer]. Thetakörper von \mathcal{J}_V sind konvex und absorbierend. Nach Korollar 6.1.3 enthalten sie auch keine linearen Teilräume. Es bleibt die Kreisförmigkeit zu zeigen.

Ein Monom $m \in \mathbb{R}[X_1, \dots, X_n]$ heißt *gerade*, wenn $\deg(m)$ gerade ist. Sonst heißt es *ungerade*. Entsprechend heißt ein Polynom in $\mathbb{R}[X_1, \dots, X_n]$ *gerade* bzw. *ungerade*, wenn es ausschließlich von geraden bzw. ausschließlich von ungeraden Monomen aufgespannt wird. Der Vektorraum $\mathbb{R}[X_1, \dots, X_n]$ ist also die direkte Summe des Vektorraums G_n der geraden und des Vektorraums U_n der ungeraden Polynome.

Lemma 6.1.4 - Kreisförmigkeit der Thetakörper

Sind $f_1, \dots, f_m \in G_n$, so sind die Thetakörper zum Ideal $\langle f_1, \dots, f_m \rangle$ kreisförmig. □

Beweis. Sei $I := \langle f_1, \dots, f_m \rangle$. Ein Polynom $f \in \mathbb{R}[X_1, \dots, X_n]$ zerlegen wir in seinen geraden Anteil f_G und seinen ungeraden Anteil f_U . Es sei auf $\mathbb{R}[X_1, \dots, X_n]$ eine Abbildung φ definiert durch $\varphi(f) := f_G - f_U$. Wir erinnern an die Notation in Kapitel 4, Abschnitt 4.2.

Behauptung: Für alle $p \in \mathcal{K} + I$ existiert ein $q \in \mathcal{K} + I$ mit $\varphi(q) = p$.

Beweis: Sei $p = \sum_{i=1}^s h_i^2 + \sum_{j=1}^n g_j f_j \in \mathcal{K} + I$ mit geeigneten Polynomen h_i, g_j . Mit der Wahl $q := \sum_{i=1}^s \varphi(h_i)^2 + \sum_{j=1}^n \varphi(g_j) f_j$ ist $q \in \mathcal{K} + I$ und es gilt: $q = p_G - p_U = \varphi(p)$. Da φ selbstinvers ist, folgt die Aussage. ◇

Sei nun x im k -ten Thetakörper zu I und $l \in \mathcal{K}^k + I$ affin-linear. Mit der obigen

Behauptung existiert ein $q \in \mathcal{K} + I$ mit $\varphi(q) = l$, sodass q in $\mathcal{K}^k + I$ liegt und affin-linear ist. Es gilt nun: $l(-x) = l_G(x) - l_U(x) = \varphi(l)(x) = q(x) \geq 0$. Daraus folgt, dass $-x$ ebenso im k -ten Thetakörper enthalten ist. ■

Diese Aussage gilt im Allgemeinen nicht für ein Ideal, welches von ungeraden Polynomen erzeugt wird:

Beispiel 6.1.5 Die Verschwindemenge eines affin-linearen Polynoms ist gleich dem ersten Thetakörper zum Ideal, welches dieses Polynom erzeugt. Dies ist leicht einzusehen, da das Polynom selbst und sein Negatives eine Summe von Quadraten, nämlich der Null, modulo dem Ideal sind. Für $I := \langle X + 1 \rangle \subseteq \mathbb{R}[X]$ gilt

$$1 \notin \{-1\} = \mathcal{Z}(I),$$

also ist der erste Thetakörper von I nicht kreisförmig. □

Da das Ideal \mathcal{J}_V von geraden Polynomen erzeugt wird, induzieren die Thetakörper, die zu \mathcal{J}_V gebildet werden, eine Norm.

Definition 6.1.6 - Thetanormen

Die durch das Minkowskifunktional

$$\begin{aligned} \|\cdot\|_{\Theta,k} : V &\rightarrow \mathbb{R}_0^+ \\ z &\mapsto \inf\{\alpha > 0 \mid \iota(z) \in \alpha \mathcal{T}_k\} \end{aligned}$$

zum Thetakörper \mathcal{T}_k definierte Norm heißt k -te Thetanorm. □

Satz 6.1.7 - Eine Kette von Kreuznormen

Die Thetanormen sind Kreuznormen und es gilt:

$$\|\cdot\|_\epsilon \leq \|\cdot\|_{\text{HS}} \leq \|\cdot\|_{\Theta,1} \leq \|\cdot\|_{\Theta,2} \leq \dots \leq \|\cdot\|_{\Theta,k} \leq \|\cdot\|_{\Theta,k+1} \leq \dots \leq \|\cdot\|_\pi. \quad \square$$

Beweis. Die Kette folgt aus Abschnitt 4.1 und der Inklusion $\mathcal{B}_{1,\pi} \subseteq \mathcal{T}_k \subseteq \mathcal{B}_{1,\text{HS}}$. Sie zeigt, dass die k -te Thetanorm eines Einheitsproduktvektors eins ist. Daraus folgt, dass die Thetanormen Kreuznormen sind. ■

Die Größe von Thetakörpern. Der innere Radius

Im vorigen Unterabschnitt haben wir eine obere Schranke für die Größe eines Thetakörpers zum Ideal \mathcal{J}_V ermittelt. Hier charakterisieren wir untere Schranken.

Definition 6.1.8 - Innerer Radius eines Thetakörpers

Für $k \in \mathbb{N}$ definiere

$$r(\mathcal{T}_k) := \sup\{r > 0 \mid r \cdot \mathcal{B}_{1,\text{HS}} \subseteq \mathcal{T}_k\}$$

den *inneren Radius* von \mathcal{T}_k . □

Ein Ansatz zur Ermittlung oberer Schranken an den inneren Radius von \mathcal{T}_k ist, nach Polynomen, welche affin-linear und k -sos-mod \mathcal{J}_V sind sowie an einem Element auf dem Rand von $\text{co}(\mathcal{Z}(\mathcal{J}_V))$ verschwinden, zu suchen. Das folgende Lemma liefert notwendige und hinreichende Bedingungen an ein solches Polynom und charakterisiert den inneren Radius von \mathcal{T}_1 im einfachsten Fall.

Lemma 6.1.9 - Innerer Radius des ersten Thetakörpers

In $\mathbb{R}^2 \otimes \mathbb{R}^2$ gilt:

$$r(\mathcal{T}_1) = \inf \left(\left(\sup\{r > 0 \mid \text{Es ex. } m \in \mathbb{N} \text{ und } f, g \in \mathcal{P}_s^r : fl_s = (l_s)^{2m} + g\} \right)_{s \in \mathbb{N}} \right),$$

wobei \mathcal{P}_s^r der von den Polynomen

$$\begin{aligned} p^r &:= r^2 - x_{11}^2 - x_{12}^2 - x_{21}^2 - x_{22}^2, \\ p_0 &:= \sum_{k=1}^s (a_{11}^k \cdot a_{22}^k - a_{12}^k \cdot a_{21}^k), -p_0, \\ p_{ij} &:= 1 - \sum_{k=1}^s (a_{ij}^k)^2, -p_{ij}, \\ p_{ijvw} &:= \sum_{k=1}^s a_{ij}^k \cdot a_{vw}^k \text{ und } -p_{ijvw}, \end{aligned}$$

wobei $i, j, v, w \in \{1, 2\}$ und $i + j + v + w$ ungerade sind, erzeugte Kegel und

$$l_s := 1 + \sum_{k=1}^s (a_0^k)^2 + 2 \sum_{i,j \in \{1,2\}} \left(\sum_{k=1}^s a_0^k \cdot a_{ij}^k \right) \cdot x_{ij}$$

ist, wobei $x_{i,j}$, a_0^k und $a_{i,j}^k$ Variablen für $i, j, v, w \in \{1, 2\}$ und $k = 1, \dots, s$ sind. □

Beweis. Es ist $\mathcal{J}_V = \langle x_{11} \cdot x_{22} - x_{12} \cdot x_{21}, 1 - x_{11}^2 - x_{12}^2 - x_{21}^2 - x_{22}^2 \rangle$. Wir zeigen die Aussage mit Hilfe des konkreten Positivstellensatzes 2.3.7 auf Seite 51.

Ein Polynom $l' \in \mathbb{R}[x_{11}, x_{12}, x_{21}, x_{22}]$, welches 1-sos-mod \mathcal{J}_V ist, ist von der Gestalt

$$l' := \sum_{k=1}^s h_k^2 + h$$

mit $h \in \mathcal{J}_V$ und $h_k = \left(\sum_{i,j \in \{1,2\}} a_{ij}^k \cdot x_{ij} \right) + a_0^k$, wobei $a_{ij}^k \in \mathbb{R}$ und $a_0^k \in \mathbb{R}$ für $k = 1, \dots, s$ gilt. Also ist

$$\begin{aligned} l' &= \sum_{i,j \in \{1,2\}} \left(\sum_{k=1}^s (a_{ij}^k)^2 \right) \cdot x_{ij}^2 + 2 \sum_{\substack{i,j,v,w \in \{1,2\} \\ (i,j) \neq (v,w)}} \left(\sum_{k=1}^s a_{ij}^k \cdot a_{vw}^k \right) \cdot x_{ij} \cdot x_{vw} \\ &+ 2 \sum_{i,j \in \{1,2\}} \left(\sum_{k=1}^s a_0^k \cdot a_{ij}^k \right) \cdot x_{ij} + \sum_{k=1}^s (a_0^k)^2 + h. \end{aligned}$$

Wir fordern nun zusätzlich, dass l' affin-linear ist. Eine reduzierte Gröbnerbasis G von \mathcal{J}_V ist in Beispiel 1.2.7 gegeben. Leitertme von G , deren Grad zwei ist, sind x_{11}^2 und $x_{11}x_{22}$. Alle anderen Leitertme haben einen höheren Grad. Mit Korollar 1.1.13 ergeben sich drei notwendige Bedingungen an die Koeffizienten $a_{ij} := (a_{ij}^1, \dots, a_{ij}^s)$ mit $i, j \in \{1, 2\}$:

- (i) $\langle a_{11}, a_{12} \rangle = \langle a_{11}, a_{21} \rangle = \langle a_{12}, a_{22} \rangle = \langle a_{21}, a_{22} \rangle = 0$,
- (ii) $\langle a_{11}, a_{22} \rangle = -\langle a_{12}, a_{21} \rangle$,
- (iii) $\sum_{k=1}^s (a_{11}^k)^2 = \sum_{k=1}^s (a_{12}^k)^2 = \sum_{k=1}^s (a_{21}^k)^2 = \sum_{k=1}^s (a_{22}^k)^2$.

Diese Bedingungen sind auch hinreichend dafür, dass es ein $h \in \mathcal{J}_V$ gibt, sodass l' affin-linear ist. Sind die drei Bedingungen erfüllt, ist

$$l_s := 1 + \sum_{k=1}^s (a_0^k)^2 + 2 \sum_{i,j \in \{1,2\}} \left(\sum_{k=1}^s a_0^k \cdot a_{ij}^k \right) \cdot x_{ij}$$

in der gleichen Restklasse wie l' modulo \mathcal{J}_V . Wir betrachten l_s im Folgenden als ein Polynom in den Variablen $x := (x_{11}, x_{12}, x_{21}, x_{22})$, $a_0 := (a_0^1, \dots, a_0^s)$ und $a_{i,j}$ für alle $i, j \in \{1, 2\}$. Jetzt setzen wir formal

$$l := 1 + \sum_{k=1}^{\infty} (a_0^k)^2 + 2 \sum_{i,j \in \{1,2\}} \left(\sum_{k=1}^{\infty} a_0^k \cdot a_{ij}^k \right) \cdot x_{ij}.$$

Dann ist l ein Polynom in den Variablen $x := (x_{11}, x_{12}, x_{21}, x_{22})$ und unendlich vielen Koeffizienten $(a_0^1, \dots, a_0^s, a_0^{s+1}, \dots)$, $(a_{ij}^1, \dots, a_{ij}^s, a_{ij}^{s+1}, \dots)$, $i, j \in \{1, 2\}$, die wir zusammenfassend mit a bezeichnen. Wir betrachten nur Koeffizienten von l , die fast

überall null sind. Weiterhin reicht es im Folgenden aus, Polynome zu betrachten, die keine Konstanten sind. Für die Lösungsmenge L_r des Ungleichungssystems

$$l(x, a) < 0; x, a \text{ erfüllen (i), (ii), (iii), } \langle x, x \rangle \leq r^2 \text{ und } \sum_{k=1}^{\infty} (a_{11}^k)^2 = 1$$

gilt nach den einführenden Überlegungen:

$$\pi_{\mathbb{R}^4}(L_r) = \{x \in r\mathcal{B}_{1,\text{HS}} \mid x \notin \mathcal{T}_1\}.$$

Eine Lösung (x, a) erfüllt genau dann die Voraussetzungen des Ungleichungssystems, wenn ein $s \in \mathbb{N}$ existiert, sodass die Auswertung eines jeden Polynoms in \mathcal{P}_s^r an (x, a) einen Wert ergibt, der nicht negativ ist. Definieren wir $\mathcal{W}(\mathcal{P}_s^r)$ als die Positivstellenmenge von \mathcal{P}_s^r , gilt die Äquivalenz

$$r\mathcal{B}_{1,\text{HS}} \setminus \mathcal{T}_1 \neq \emptyset.$$

\Leftrightarrow Es existiert ein s , sodass $l_s(x, a) < 0$ für ein $(x, a) \in \mathcal{W}(\mathcal{P}_s^r)$ ist.

\Leftrightarrow Es existiert ein s , sodass $l_s(\mathcal{W}(\mathcal{P}_s^r)) \geq 0$ falsch ist.

\Leftrightarrow Es existiert ein s , sodass für alle m und $f, g \in \mathcal{P}_s^r$ gilt: $fl_s \neq (l_s)^{2m} + g$.

Dass die letzte Zeile äquivalent zur vorletzten ist, folgt aus Satz 2.3.7. Wir setzen:

$$R := \inf \left(\left(\sup \{r > 0 \mid \text{Es existieren } m \in \mathbb{N} \text{ und } f, g \in \mathcal{P}_s^r : fl_s = (l_s)^{2m} + g\} \right)_{s \in \mathbb{N}} \right).$$

Behauptung: $R = r(\mathcal{T}_1)$.

Beweis: Sei $r > r(\mathcal{T}_1)$. Dann existiert ein $x \in r\mathcal{B}_{1,\text{HS}}$ mit $x \notin \mathcal{T}_1$. Also ist $R < r$ und damit $R \leq r(\mathcal{T}_1)$. Ist stattdessen $r \leq r(\mathcal{T}_1)$, so gilt die Negation der obigen Aussage, das heißt, für alle $s \in \mathbb{N}$ existiert eine Polynomgleichung wie oben für r . Also ist $r \leq R$ und damit $r(\mathcal{T}_1) \leq R$. \diamond

Damit ist die Aussage bewiesen. \blacksquare

Besitzt ein Tensor Hilbert-Schmidt-Norm r und existiert ein k -sos-mod \mathcal{J}_V -Polynom, sodass die Auswertung daran negativ ist, so ist r eine obere Schranke für den inneren Radius von \mathcal{T}_k . Da die Einheitsproduktvektoren Extrempunkte der Pi-Norm-Einheitssphäre sind, bietet sich als Kandidat für ein solches Element mit Hilbert-Schmidt-Norm eins ein „(maximal) verschränkter“ Vektor an, zum Beispiel ein Bell-Zustand:

$$y := \frac{1}{\sqrt{2}}(e_1 \otimes e_1 + e_2 \otimes e_2).$$

Mit dieser Wahl ist $\|y\|_{\text{HS}} = 1$ und $\iota(y) = \frac{1}{\sqrt{2}}(1, 0, 0, 1)$.

Beispiel 6.1.10 Wir zeigen, dass der innere Radius von \mathcal{T}_1 echt kleiner eins ist. Zunächst gehen wir davon aus, dass der zu Grunde liegende Raum $\mathbb{R}^2 \otimes \mathbb{R}^2$ ist, und wählen y wie oben.

Behauptung: $y \notin \mathcal{T}_1$.

Beweis: Die Auswertung des Polynoms

$$l := 3 - 2\sqrt{2}(x_{11} + x_{22})$$

an y ergibt -1 . Weiterhin ist

$$l = (x_{12} - x_{21})^2 + (x_{11} + x_{22} - \sqrt{2})^2 + h$$

für das Polynom $h := 1 - \sum_{i,j=1}^2 x_{ij}^2 - 2(x_{11}x_{22} - x_{12}x_{21}) \in \mathcal{J}_V$, also ist l ein Polynom, welches 1-sos-mod \mathcal{J}_V ist. \diamond

Das Beispiel ist auf den allgemeinen Fall $\mathbb{R}^{n_1} \otimes \dots \otimes \mathbb{R}^{n_r}$ übertragbar. Die Summe von Quadraten ist dann um die Terme x_{ij}^2 für $(i, j) \notin \{1, 2\} \times \{1, 2\}$ zu ergänzen. \square

Eine weitere Eingrenzung liefert das folgende Resultat:

Satz 6.1.11 - Schranken an den inneren Radius

Es gilt für $k \in \mathbb{N}$: $r(\mathcal{T}_k) \leq \frac{1}{\sqrt{2}}$. Für $\mathbb{R}^2 \otimes \mathbb{R}^2$ ist $r(\mathcal{T}_k) = \frac{1}{\sqrt{2}}$. \square

Beweis. Für Vektoren $z \in \mathbb{R}^2 \otimes \mathbb{R}^2$, die bezüglich der projektiven Norm normiert sind, gibt es eine im Wesentlichen eindeutige Darstellung $z = \lambda v \otimes w + (1 - \lambda)v' \otimes w'$ mit Orthonormalbasen $\{v, v'\}$ und $\{w, w'\}$ von \mathbb{R}^2 und $\lambda \in [0, 1]$. Die Hilbert-Schmidt-Norm eines solchen Vektors nimmt für $\lambda = 1/2$ ein Minimum von $1/\sqrt{2}$ an. Da $\mathcal{B}_{1,\pi} \subseteq \mathcal{T}_k$ gilt, folgt die Ungleichung $1/\sqrt{2} \leq r(\mathcal{T}_k)$ für $\mathbb{R}^2 \otimes \mathbb{R}^2$.

Wie im vorigen Beispiel betrachten wir $y \in \mathbb{R}^2 \otimes \mathbb{R}^2$ und verallgemeinern das Resultat. Sei $r > 0$. Das Polynom

$$\frac{1}{2}((-1 + x_{11} + x_{22})^2 + (x_{12} - x_{21})^2)$$

ist eine Summe von Quadraten. Eine einfache Rechnung zeigt, dass es kongruent zu dem affin-linearen Polynom

$$l := 1 - (x_{11} + x_{22})$$

modulo \mathcal{J}_V ist. Die Auswertung von l an $r \cdot y$ ergibt

$$l(ry) = 1 - r\sqrt{2}.$$

Dieser Ausdruck ist genau dann negativ, wenn $r > 1/\sqrt{2}$ ist. \blacksquare

Der skalierte Bell-Zustand $\frac{1}{2}(e_1 \otimes e_1 + e_2 \otimes e_2)$ liegt also auf dem Rand des ersten Thetakörpers. Dies gilt auch für die anderen Bell-Zustände, was eine Permutation der Variablen deutlich macht. Setzen wir im Polynom

$$\frac{1}{2}((-1 + \diamond + \diamond)^2 + (\diamond + \diamond)^2)$$

die Variablen wie in der Tabelle angegeben, ist es kongruent zu

$$l := 1 - (\diamond + \diamond)$$

modulo \mathcal{J}_V und der Wert dieses affin-linearen Polynoms am entsprechenden, mit einem Faktor $r > \frac{1}{\sqrt{2}}$ skalierten Bell-Zustand ist negativ.

Bell-Zustand	\diamond	\diamond	\diamond	\diamond
$\frac{1}{\sqrt{2}} \cdot (e_1 \otimes e_1 + e_2 \otimes e_2)$	x_{11}	x_{22}	x_{12}	$-x_{21}$
$\frac{1}{\sqrt{2}} \cdot (e_1 \otimes e_1 - e_2 \otimes e_2)$	x_{11}	$-x_{22}$	x_{12}	x_{21}
$\frac{1}{\sqrt{2}} \cdot (e_1 \otimes e_2 + e_2 \otimes e_1)$	x_{12}	x_{21}	x_{11}	$-x_{22}$
$\frac{1}{\sqrt{2}} \cdot (e_1 \otimes e_2 - e_2 \otimes e_1)$	x_{12}	$-x_{21}$	x_{11}	x_{22}

Wir untersuchen im Folgenden, ob diese Polynome ausreichen, um den ersten Thetakörper zu bestimmen.

6.2 Polaren und ihre maximalen Seiten

Im letzten Abschnitt haben wir festgestellt, dass der Rand des ersten Thetakörpers den Rand der Einheitskugel der projektiven Norm an den Einheitsproduktvektoren und auch an den mit $\frac{1}{\sqrt{2}}$ skalierten Bell-Zuständen berührt. Um zu wissen, ob wir aus diesen Informationen schließen können, dass der erste Thetakörper mit der Einheitskugel übereinstimmt, benötigen wir Kenntnisse über deren Geometrie.

Die Geometrie kompakter konvexer Mengen ist im Wesentlichen durch ihre *Seiten* bestimmt. Wir werden sehen, dass es eine Hierarchie unter den Seiten gibt, und dass maximale Vektoren innere Punkte von *maximalen Seiten* sind.

In diesem Abschnitt möchten wir zunächst Seiten konvexer Mengen charakterisieren, danach die Polare als duales Objekt einer kompakten konvexen Menge einführen und schließlich das Verhältnis zwischen *dualen Seiten* untersuchen.

Maximale und annullierte Seiten konvexer Mengen

In diesem Unterabschnitt sei $K \subseteq \mathbb{R}^n$ eine kompakte und konvexe Menge, die nicht leer ist. Die Randpunkte und das Innere von K betrachten wir relativ zur affinen Hülle von K .

Definition 6.2.1 - Seiten kompakter konvexer Mengen

Eine Teilmenge $S \subseteq K$, die nicht leer ist, heißt *Seite* von K , wenn für alle $z \in S$ gilt: Ist $z = \lambda x + (1 - \lambda)y$ mit $\lambda \in (0, 1)$ und $x, y \in K$, so folgt, dass $x, y \in S$. Für $k \in K$ bezeichnen wir eine Seite S mit $k \in S$ als *minimale Seite* für k , falls jede Seite F mit $k \in F$ Obermenge von S ist. Eine echte Seite S von K heißt *maximal*, wenn es keine Seiten F von K mit $S \subsetneq F \subsetneq K$ gibt. Falls ein affin-lineares Funktional existiert, welches sein Minimum über K exakt an einer Seite S annimmt, bezeichnen wir S als *annulliert*. Als *Dimension* $\dim(S)$ einer Seite S bezeichnen wir die Dimension ihrer affinen Hülle. \square

Seiten sind konvexe Mengen. Ist der Schnitt beliebig vieler Seiten nicht leer, so ist er eine Seite. Insbesondere existieren minimale Seiten von $k \in K$ als Schnitt aller Seiten von K , die k enthalten.

Beispiel 6.2.2 Extremalpunkte sind Seiten. Die Seiten eines Polyeders in \mathbb{R}^3 sind seine Ecken, Kanten und Flächen sowie der Polyeder selbst. \square

Die Teilmenge von K , auf der ein affin-lineares Funktional sein Minimum annimmt, ist eine Seite. Nimmt ein affin-lineares Funktional sein Minimum über K exakt an einer Seite S an, so sagen wir, dass es S *annulliert*. Wir machen zunächst Aussagen über das Schnittverhalten von Seiten, um zu charakterisieren, welche Seiten annulliert werden können.

Proposition 6.2.3 - Maximale und minimale Seiten

Für Seiten $S, S_1, S_2 \subseteq K$ gilt:

- (i) $S = K$ oder S ist Teilmenge des Randes von K .
- (ii) S ist kompakt.
- (iii) Ist $S_1 \subsetneq S_2$, so ist $\dim(S_1) < \dim(S_2)$ und S_1 Teilmenge des Randes von S_2 .
- (iv) Ist $S_1 \cap S_2 \neq \emptyset$, so ist $S_1 \cap S_2$ eine Seite und es gilt:

$$\dim(S_1 \cap S_2) \leq \min(\dim(S_1), \dim(S_2)).$$

Die Gleichheit gilt dabei genau dann, wenn eine der beiden Mengen S_1 und S_2 in der anderen enthalten ist.

- (v) Ist $\text{relin}(S_1) \cap S_2 \neq \emptyset$, so gilt: $S_1 \subseteq S_2$.
- (vi) Ist der Schnitt beliebig vieler annullierter Seiten nicht leer, so ist er eine annullierte Seite.
- (vii) S ist genau dann maximal, wenn jedes auf K nicht-triviale affin-lineare Funktional, welches über K an S minimal ist, sein Minimum exakt an S annimmt. Insbesondere sind maximale Seiten annulliert und es gilt entweder $S = K$ oder S ist in einer maximalen Seite enthalten. \square

Beweis. Nach Satz 3.2.10 gilt $\text{cl}(\text{relin}(C)) = \text{cl}(C)$ für eine konvexe Menge $C \subseteq \mathbb{R}^n$. Daraus folgt, dass eine konvexe Teilmenge des Randes von K eine niedrigere Dimension als K besitzt.

(i): Falls $k \in S$ ein innerer Punkt von K ist, existiert eine konvexe Umgebung U von k , die in K enthalten ist. Wir schließen nun aus der Definition einer Seite, dass U in S enthalten ist. Sei nun $z \in K$. Dann existiert ein Faktor $\lambda \in (0, 1)$, sodass $\lambda z + (1 - \lambda)k \in U$ ist. Es folgt: $z \in S$. Damit ist $S = K$.

(ii): Der Schnitt von K mit der affinen Hülle von S ist kompakt, konvex und nicht leer. Mit (i) folgt, dass S keine echte Teilmenge dieses Schnittes sein kann.

(iii),(iv): Aus (i) folgt, dass die affinen Hüllen von Seiten, die echte Teilmengen voneinander sind, ebenso echte Teilmengen voneinander sind.

(v): Der Schnitt $S_1 \cap S_2$ ist nicht leer und damit nach (iv) eine Seite von K und damit auch von S_1 . Mit (i) folgt aus der Voraussetzung, dass $S_1 \cap S_2 = S_1$ gilt. Daraus folgt die Behauptung.

(vi): Wir zeigen zunächst, dass der Schnitt zweier annullierter Seiten annulliert wird. Das affin-lineare Funktional φ_i annulliere S_i für $i = 1, 2$. Dann annulliert $\varphi_1 + \varphi_2$ den Schnitt $S_1 \cap S_2$. Dies zeigt, dass ein Schnitt endlich vieler annullierter Seiten, der nicht leer ist, eine annullierte Seite ist. Sei F ein System von annullierten Seiten, sodass der Schnitt aller Seiten in F nicht leer ist. Die Menge X aller endlichen Schnitte von annullierten Seiten aus F ist durch Inklusion gerichtet. Aus (iii) folgt, dass jede Kette von X beschränkt ist. Nach dem Lemma von Zorn existiert ein maximales Element in X . Demnach terminiert die Schnittbildung nach endlich vielen echten Schnitten.

(vii): Funktionalanalytische Trennungssätze und ein Dimensionsargument, welches nach (iii) besagt, dass eine aufsteigende Kette echter annullierter Seiten stationär wird, zeigen, dass jede konvexe Teilmenge des Randes von K in einer maximalen annullierten Seite M von K enthalten ist. Da jede Seite, die Teilmenge des Randes von K ist, eine Teilmenge einer echten annullierten Seite ist, ist M auch eine maximale Seite. \blacksquare

Maximale Seiten sind also annullierte Seiten. Für minimale Seiten muss dies nicht gelten, da für $k \in K$ zwar eine eindeutig bestimmte *minimale annullierte Seite* als Schnitt aller annullierter Seiten von K , die k enthalten, existiert, diese allerdings im Allgemeinen von der minimalen Seite verschieden ist.

Beispiel 6.2.4 Der Graph der Funktion

$$f: [-1, 1] \rightarrow \mathbb{R} \\ x \mapsto \begin{cases} 1, & x < 0 \\ \sqrt{1-x^2}, & x \geq 0 \end{cases}$$

berandet das konvexe Gebiet

$$K := \{(x, y) \in [-1, 1] \times [-1, 1] \mid y \leq f(x)\}$$

in der Zahlenebene. Der Punkt $e := (0, 1)$ ist ein Extrempunkt von K . Die minimale annullierte Seite zu e ist $\{\lambda(-1, 1) + (1 - \lambda)(0, 1) \mid \lambda \in [0, 1]\}$, aber die minimale Seite zu e ist $\{e\}$. \square

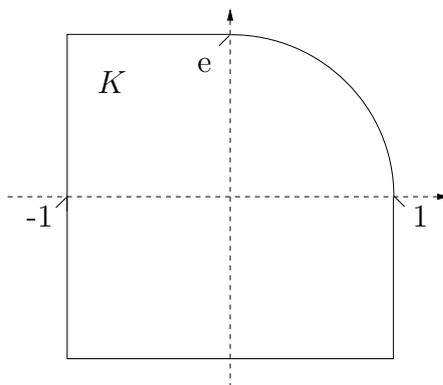


Abbildung 6.1: Visualisierung der Menge K aus Beispiel 6.2.4

Falls jeder Randpunkt von K Extrempunkt ist, heißt K *strikt konvex*. Wird ein Randpunkt von K durch Elemente von K nicht-trivial konvex kombiniert, so folgt aus Lemma 3.2.6, dass auch diese Randpunkte sind. Also ist K genau dann strikt konvex, wenn kein Randpunkt von K nicht-triviale Konvexkombination von Randpunkten ist. In diesem Fall bestehen die echten Seiten von K aus den Extrempunkten.

Proposition 6.2.5 - Strikt konvexe Mengen und Annullierung

Ist K strikt konvex, dann werden alle Seiten annulliert. Insbesondere ist dann jeder Extrempunkt einer kompakten und konvexen Teilmenge L von K , der auf dem Rand von K liegt, eine annullierte Seite von L . \square

Beweis. Die minimale annullierte Seite zu einem Randpunkt von K ist eine konvexe Teilmenge des Randes. \blacksquare

Beispielsweise sind Sphären oder Ellipsen strikt konvex.

Polaren und Bipolaren

Polaren verwirklichen eine duale Beziehung zwischen kompakten konvexen Mengen. Die Menge der affin-linearen Funktionale, durch die eine konvexe Menge eindeutig bestimmt ist, bildet ihre Polare. Nutzen wir sie, um Seiten zu annullieren, überträgt sich die Geometrie der Polaren auf die Geometrie der Seiten.

Definition 6.2.6 - Polare

Für eine Menge $A \subseteq \mathbb{R}^n$ bezeichne

$$A^\circ := \{y \in \mathbb{R}^n \mid \text{Für alle } x \in A \text{ gilt: } \langle x, y \rangle \leq 1\}$$

die *Polare* von A . \square

Der Bipolarensatz, siehe [Wer], besagt:

$$(A^\circ)^\circ = \text{cl}(\text{co}(A \cup \{0\})).$$

Insbesondere ist eine kompakte konvexe Nullumgebung gleich ihrer Bipolaren.

Beispiel 6.2.7

- (1) Die Polare ist konvex und abgeschlossen. Insbesondere bleiben kompakte konvexe Nullumgebungen unter Polarenbildung invariant. Dies gilt auch für Kreisförmigkeit.
- (2) Die Polare der Einheitssphäre zur 1-Norm ist die Einheitssphäre der Supremumsnorm.
- (3) Die Einheitssphäre zur 2-Norm ist zu sich selbst polar.

(4) Die Polare zu einer Ellipse

$$E := \left\{ (x, y) \in \mathbb{R}^2 \mid \left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 \leq 1 \right\}$$

für $a, b > 0$ ist

$$E^\circ = \left\{ (x, y) \in \mathbb{R}^2 \mid (ax)^2 + (by)^2 \leq 1 \right\},$$

eine Ellipse mit den Radien $1/a$ und $1/b$. Dies sieht man leicht ein, da

$$\|(x, y)\| \leq 1 \Leftrightarrow (ax, by) \in E \Leftrightarrow \left(\frac{x}{a}, \frac{y}{b}\right) \in E^\circ.$$

Polaren von Ellipsen sind durch die Inversen der Radien bestimmt.

(5) Die Polare zu $x \in \mathbb{R}^n$ ist

$$\{x\}^\circ = \{y \in \mathbb{R}^n \mid \langle x, y \rangle \leq 1\}.$$

Dies ist ein affiner Halbraum, welcher durch eine Hyperebene, die senkrecht auf x mit Abstand $\|x\|^{-1}$ zum Ursprung steht, begrenzt wird.

(6) Die Polare einer beliebigen Vereinigung von Mengen ist der Schnitt der Polaren. Insbesondere sind Polaren von Punktfolgen Schnitte von Halbräumen. □

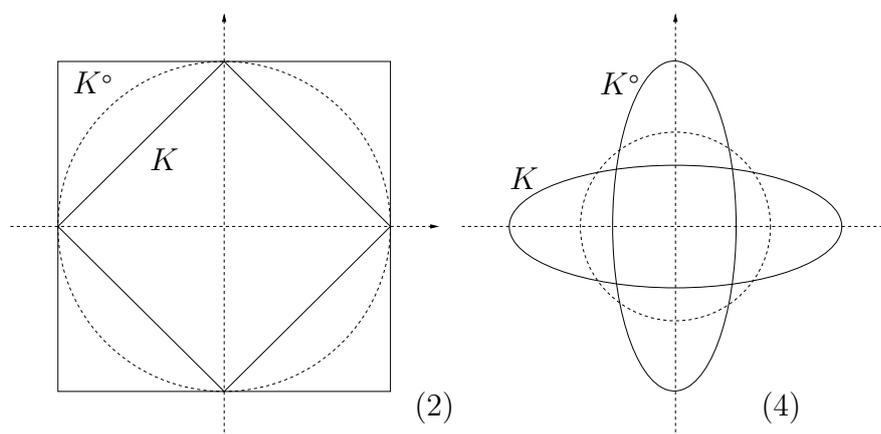


Abbildung 6.2: Visualisierung der Polaren aus Beispiel 6.2.7

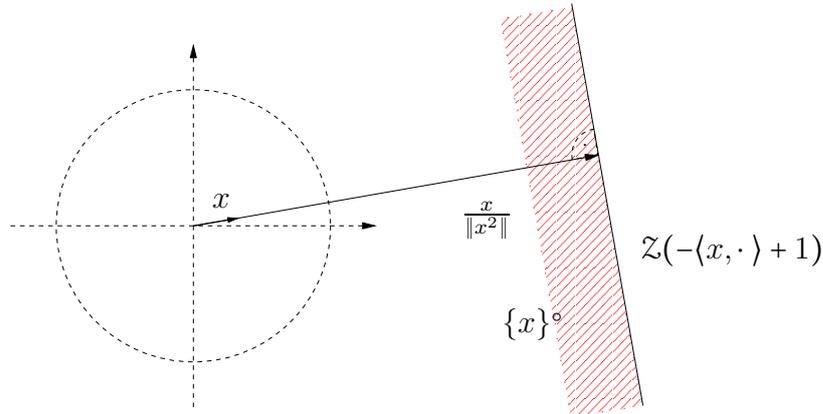


Abbildung 6.3: Die Polare zu einem Punkt; siehe 6.2.7, (5)

Durch Polaren induzierte Normen und der innere Radius

In den folgenden Unterabschnitten bis zum Ende des Abschnitts sei K eine kompakte und konvexe Nullumgebung von \mathbb{R}^n , die auch eine kreisförmige Teilmenge der Einheitssphäre \mathcal{B}_1 ist.

Definition 6.2.8 - Innerer Radius

Der *innere Radius* von K sei bezeichnet durch

$$r(K) := \sup\{r > 0 \mid r \cdot \mathcal{B}_1 \subseteq K\}. \quad \square$$

Die Minkowskifunktionale zu K und der Polaren K° induzieren Normen. Es gilt für $v \in \mathbb{R}^n$:

$$\begin{aligned} \|v\|_K &:= \inf\{\alpha > 0 \mid v \in \alpha K^\circ\} = \inf\{\alpha > 0 \mid \text{Für alle } w \in K \text{ gilt: } \langle w, v \rangle \leq \alpha\} \\ &= \sup\{\langle w, v \rangle \mid w \in K\} \leq \|v\|, \\ \|v\|^K &:= \inf\{\alpha > 0 \mid v \in \alpha K = \alpha(K^\circ)^\circ\} = \sup\{\langle w, v \rangle \mid w \in K^\circ\} \\ &= \sup\{\langle w, v \rangle \mid \|w\|_K \leq 1\} \geq \|v\|. \end{aligned}$$

Es ist $\mathcal{B}_{1, \|\cdot\|_K} = K^\circ$ und $\mathcal{B}_{1, \|\cdot\|^K} = K$. Aus Theorem 3.2 in [Arv] folgt, dass die beiden Normen den inneren Radius charakterisieren:

$$\inf\{\|v\|_K \mid \|v\| = 1\} = r(K) \quad \text{und} \quad \sup\{\|v\|^K \mid \|v\| = 1\} = \frac{1}{r(K)}.$$

Definition 6.2.9 - Maximale Vektoren

Ein Vektor $v \in K$ mit $\|v\| = 1$ heißt *maximal*, falls $\|v\|_K = r(K)$. □

Ein Vektor ist genau dann maximal, wenn die Norm $\|\cdot\|^K$ an ihm den maximalen Wert $1/r(K)$ annimmt. Dies zeigt Theorem 4.2 in [Arv]. Es ist leicht zu sehen, dass $\sup\{\|v\|^K \mid \|v\| = r(K)\} = 1$ und $\inf\{\|v\|_K \mid \|v\| = 1/r(K)\} = 1$. Dies zeigt, dass der *äußere Radius* von K° als Schnitt aller skalierten Einheitssphären, die Obermengen von K° sind, gleich $1/r(K)$ ist.

Für uns ist besonders interessant, dass es eine enge Verbindung zwischen den behandelten Normen und projektiver und injektiver Norm auf Tensorprodukten gibt. Wählen wir K als die konvexe Hülle der Einheitsproduktvektoren des Tensorprodukts $\mathbb{R}^{n_1} \otimes \dots \otimes \mathbb{R}^{n_r}$, die der Einheitssphäre der projektiven Norm auf diesem Tensorprodukt gleicht, zeigt Theorem 8.2 in [Arv] auf, dass für alle $v \in K$ gilt:

$$\|v\|_K = \|v\|_\epsilon \quad \text{und} \quad \|v\|^K = \|v\|_\pi.$$

Klassen von affin-linearen Funktionalen

In diesem Unterabschnitt charakterisieren wir affin-lineare Funktionale auf \mathbb{R}^n nach ihren Trennungseigenschaften. Zunächst können wir folgende Identifikation vornehmen:

$$\begin{aligned} \mathbb{R}^{n+1} &\rightarrow \{f : \mathbb{R}^n \rightarrow \mathbb{R} \mid f \text{ affin-linear}\} \\ (\varphi_1, \dots, \varphi_n, d) &\mapsto -\langle(\varphi_1, \dots, \varphi_n), \cdot\rangle + d \end{aligned}$$

Multiplikation eines Funktionals mit einer positiven Konstanten ändert nichts an der Verschwindemenge und auch nichts an der Positivstellenmenge. Die Äquivalenzrelation

$$x \sim y \iff \text{Es existiert ein } \lambda > 0 \text{ mit } x = \lambda y$$

auf $\mathbb{R}[X_1, \dots, X_{n+1}]_1$ reduziert Funktionale nach dieser Eigenschaft. Sie werden so mit Elementen eines projektiven Raums identifiziert. Möchten wir echte Seiten von kompakten konvexen Nullumgebungen annullieren, ist dies nur mit Funktionalen möglich, deren additive Konstante positiv ist, da diese das Ergebnis der Auswertung des Funktionals am Wert Null ist. Ein Repräsentantensystem für diese Funktionale ist demnach gegeben durch

$$\mathcal{R} := \{-\langle\varphi, \cdot\rangle + 1 \mid \varphi \in \mathbb{R}^n, \varphi \neq 0\}.$$

Anschaulich gesehen handelt es sich dabei um Vektoren, die jeweils in Richtung der größten Abnahme ihres induzierten Funktionals zeigen und deren orthogonale Komplemente den Raum durch eine Hyperebene trennen.

Weiterhin möchten wir die Funktionale charakterisieren, die auf K beziehungsweise auf der Polaren K° nicht negativ sind. Es gibt eine Eins-zu-Eins-Beziehung zwischen affin-linearen Funktionalen, welche auf K (oder K°) nicht negativ sind, und Elementen der Polaren K° (oder K):

Proposition 6.2.10 - Nicht negative Funktionale und die Polare

Es sei $L := \{(x_1, \dots, x_{n+1}) \in \mathbb{R}^{n+1} \mid x_{n+1} = 1\}$, dann ist

- (i) $\pi_{\mathbb{R}^n}((-\langle K, \cdot \rangle + 1)^\star \cap L) = K^\circ$,
- (ii) $\pi_{\mathbb{R}^n}((-\langle K^\circ, \cdot \rangle + 1)^\star \cap L) = K$. □

Beweis. Es ist leicht einzusehen, dass für $\Phi := -\langle \varphi, \cdot \rangle + 1 \in \mathcal{R}$ gilt:

$$\begin{aligned} K \subseteq \mathcal{W}(\Phi) &\Leftrightarrow \langle \varphi, v \rangle \leq 1 \text{ für alle } v \in K \\ &\Leftrightarrow \varphi \in K^\circ. \end{aligned}$$

In diesem Fall ist $\mathcal{Z}(\Phi) = \{v \in K \mid \langle \varphi, v \rangle = 1\}$. Ebenso gilt: $K^\circ \subseteq \mathcal{W}(\Phi) \Leftrightarrow \varphi \in K$. ■

Darüber hinaus stellt diese Aussage auch eine Beziehung zwischen dualen Kegeln und der Polaren her.

Annullierende Funktionale, maximale und minimale Seiten der Einheitsphäre und ihrer Polaren

Die auf K nicht negativen Funktionale sind nun bekannt. Die Verschwindemengen dieser Funktionale auf K liefern die annullierten Seiten.

Satz 6.2.11 - Annullierte Seiten der Einheitsphäre und ihrer Polaren

Seien $\varphi \in K^\circ$, $\psi \in K$ und $\Phi := -\langle \varphi, \cdot \rangle + 1$, $\Psi := -\langle \psi, \cdot \rangle + 1$ jeweils die induzierten Funktionale. Dann gilt:

- (i) Es ist $\|\varphi\|_K = 1$ genau dann, wenn $K \cap \mathcal{Z}(\Phi) \neq \emptyset$.
Insbesondere sind die echten annullierten Seiten von K gegeben durch

$$S_v^K := \{k \in K \mid 1 = \|k\|^K = \langle v, k \rangle\}$$

für $v \in K^\circ$ mit $\|v\|_K = 1$.

- (ii) Es ist $\|\psi\|^K = 1$ genau dann, wenn $K^\circ \cap \mathcal{Z}(\Psi) \neq \emptyset$.
 Insbesondere sind die echten annullierten Seiten von K° gegeben durch

$$S_w^{K^\circ} := \{k \in K^\circ \mid 1 = \|k\|_K = \langle w, k \rangle\}$$

für $w \in K$ mit $\|w\|^K = 1$. □

Beweis. (i): Sei $\|\varphi\|_K = 1$. Da die Norm $\|\cdot\|_K$ als Supremum über Auswertungen an Elementen in K geschrieben werden kann, existiert ein $k \in K$ mit $1 = \langle \varphi, k \rangle$. Es ist also $k \in K \cap \mathcal{Z}(\Phi)$. Nun zeigen wir die andere Implikation. Es ist $\|\varphi\|_K \leq 1$. Wir nehmen an, dass $\|\varphi\|_K < 1$ ist. Ein Element $k \in K$ ist genau dann in der Verschwindemenge von Φ , wenn $1 = \langle \varphi, k \rangle$ gilt. In diesem Fall ist $\|k\|^K = 1$ und k nimmt diese Norm am Vektor φ an. Weiterhin ist $\langle \varphi / \|\varphi\|_K, k \rangle = \|\varphi\|_K^{-1} > 1$. Dies ein Widerspruch zur Annahme wegen $\|k\|^K = 1$. Es folgt, dass $\|\varphi\|_K = 1$ ist.

(ii): Der Beweis erfolgt analog. ■

Bemerkung 6.2.12 Manchmal ist es nützlich, die annullierten Seiten in der folgenden Form zu schreiben:

$$S_v^K = \left\{ \frac{k}{\|k\|_K} \mid \|k\| = 1 \text{ mit } \|k\|^K = \langle v, k \rangle \right\} \text{ und}$$

$$S_w^{K^\circ} = \left\{ \frac{k}{\|k\|_K} \mid \|k\| = 1 \text{ mit } \|k\|_K = \langle w, k \rangle \right\}$$

mit $\|v\|_K = 1$ und $\|w\|^K = 1$. Diese Seiten sind also durch die Vektoren charakterisiert, die ihre Norm am gegebenen Vektor annehmen. □

Wir stellen die Vermutung an, dass es duale Beziehungen zwischen den Hierarchien von Seiten gibt. Zur Motivation erinnern wir uns an die Beispiele 6.2.7 und stellen folgenden dualen Bezug zwischen Vektoren her:

Proposition 6.2.13 - Ist $v \in K$ mit $\|v\| = 1$ maximal, so ist $v/\|v\|_K$ ein annullierter Extrempunkt von K° . □

Beweis. Das Funktional $-\langle v/\|v\|_K, \cdot \rangle + 1$ ist nicht negativ auf K° und es gilt für einen Vektor $w \in K$ mit $\|w\| = 1$:

$$1 = \left\langle \frac{v}{\|v\|_K}, \frac{w}{\|w\|_K} \right\rangle \Leftrightarrow \|v\|^K \|w\|_K = \langle v, w \rangle \leq 1$$

Es ist $\|v\|^K \|w\|_K = (1/r(K)) \cdot \|w\|_K \geq (1/r(K)) \cdot r(K) = 1$, also folgt in diesem Fall die Gleichung $v = w$. Damit ist $\{v/\|v\|_K\}$ die Verschwindemenge des Funktionals auf K° . ■

Ein Einheitsvektor v mit $v/\|v\|_K \in \text{ext}(K^\circ)$, sodass $\|\cdot\|_K$ an v minimal ist, ist maximal. Allerdings gilt die Umkehrung von Proposition 6.2.13 im Allgemeinen nicht. Beispiel 6.2.7 zeigt, dass duale Ellipsen inverse Radien besitzen. Alle Randpunkte einer Ellipse sind annullierte Extrempunkte, allerdings sind für ungleiche Radien nur zwei Vektoren maximal.

In einigen Fällen erhalten wir noch stärkere Aussagen über die Art der Seiten:

Satz 6.2.14 - Maximale und minimale Seiten

Sei v ein Einheitsvektor, $S := S_{v/\|v\|_K}^K$ und $S' := S_{v/\|v\|_K}^{K^\circ}$.

- (i) Ist v maximal, so ist S maximal, $v/\|v\|_K \in S$ mit $v \in (S - v/\|v\|_K)^\perp$ und $S' = \{v/\|v\|_K\}$, also insbesondere minimal.
- (ii) Ist $\|v\|_K = 1$, so ist S' maximal, $v \in S'$ mit $v \in (S' - v)^\perp$ und $S = \{v\}$, also insbesondere minimal. □

Beweis. (i): Sei v maximal. Dann ist leicht zu sehen, dass $v/\|v\|_K \in S$ ist.

Behauptung: Ein affin-lineares Funktional Φ , welches nicht negativ auf K ist und eine Nullstelle an $v/\|v\|_K$ hat, ist eindeutig bestimmt und annulliert S .

Beweis: Nach Satz 6.2.11 sind derartige Funktionale gegeben durch

$$-\langle \varphi/\|\varphi\|_K, \cdot \rangle + 1 \quad \text{mit} \quad 1 = \langle \varphi/\|\varphi\|_K, v/\|v\|_K \rangle$$

für einen Einheitsvektor φ . Da $\|v\|_K = 1/r(K)$, $\|\varphi\|_K \geq r(K)$ und $\langle \varphi, v \rangle \leq 1$ gilt, folgt: $\varphi = v$. Es gibt also nur ein einziges Funktional, welches die Voraussetzung erfüllt. Die Verschwindemenge dieses Funktionals auf K besteht aus den Vektoren in K , die ihre $\|\cdot\|_K$ -Norm an $v/\|v\|_K$ annehmen, also genau aus S . ◇

Alle Funktionale, die auf K nicht negativ und auf S null sind, verschwinden insbesondere an $v/\|v\|_K$. Wie eben gezeigt, gibt es genau ein solches Funktional, und dessen Verschwindemenge ist S . Damit ist S eine maximale Seite.

Behauptung: $v \in (S - v/\|v\|_K)^\perp$.

Beweis: Ist $k \in S$, so ist

$$\left\langle k, \frac{v}{\|v\|_K} \right\rangle = 1 = \frac{1}{\|v\|_K \cdot \|v\|_K}, \quad \text{also ist} \quad \langle k, v \rangle = \left\langle \frac{v}{\|v\|_K}, v \right\rangle.$$

Umstellen der Gleichung zeigt die Behauptung. ◇

Behauptung: S' ist minimal.

Beweis: Es ist $S' = K^\circ \cap \mathcal{Z}(\Psi)$ mit $\Psi := -\langle v/\|v\|_K, \cdot \rangle + 1$. Nach dem Beweis von Proposition 6.2.13 wissen wir bereits, dass die Verschwindemenge von Ψ auf K° genau $\{v/\|v\|_K\}$ entspricht. ◇

(ii): Es ist nach Voraussetzung $1 = \|v\| = \|v\|^K$. Wegen $1 \geq \|v\|_K \geq \langle v/\|v\|^K, v \rangle = 1$ folgt die Gleichung $1 = \|v\|^K$. Insbesondere ist $v \in S'$. Wir verfahren hier ähnlich wie im Beweis von (i). Ein affin-lineares Funktional, welches auf K° nicht negativ ist und eine Nullstelle an v hat, ist von der Form

$$\Psi := -\langle \psi/\|\psi\|^K, \cdot \rangle + 1 \quad \text{mit} \quad 1 = \langle \psi/\|\psi\|^K, v \rangle$$

für einen Einheitsvektor ψ . Es ist $\|\psi\|^K \geq 1$, also folgt: $\psi = v$. Die Verschwindemenge von Ψ auf K° ist S' . Damit ist S' maximal. Weiterhin ist für $k \in S'$

$$\langle k, v \rangle = 1 = \langle v, v \rangle,$$

also folgt: $v \in (S' - v)^\perp$. Die Aussage für S folgt sofort aus Bemerkung 6.2.12. ■

Beispiel 6.2.15 Mit Satz 6.2.14 ist die Polare zu regelmäßigen Polyedern leicht zu bestimmen.

- (i) (*Platonische Körper*) Die Flächen eines platonischen Körpers sind seine maximalen Seiten. Die Extrempunkte sind die Ecken und der Schwerpunkt jeder Fläche ist ein maximaler Vektor. Die Symmetriegruppe wirkt transitiv auf Ecken und maximalen Vektoren. Diese Betrachtungen zeigen, dass die Polare eines platonischen Körpers der duale Körper ist.
- (ii) (*Hexagone*) Abbildung 6.4 zeigt eine Kette von zwölf Hexagonen und deren Polaren. □

Grundsätzlich können weitere maximale Seiten existieren, die keinen maximalen Vektor enthalten. Dies sehen wir leicht am Beispiel der Ellipse ein. Ist K unter bestimmten Symmetrien invariant, kann die Symmetriegruppe benutzt werden, um die maximalen Seiten zu bestimmen. Dies werden wir im nächsten Abschnitt im Anwendungsfall konkretisieren.

Duale Seiten und Extrempunkte

Es besteht ein Zusammenhang zwischen maximalen Seiten und annullierten Extrempunkten der Polaren. Dieser ist in [BPT] auf Seite 457 angedeutet. Hier möchten wir ihn ausführen.

Definition 6.2.16 - Duale Seiten

Sei $S \subseteq K$ leer oder eine Seite. Dann definiert

$$S^\wedge := \{v \in K^\circ \mid \text{Für alle } s \in S \text{ gilt: } 1 = \langle v, s \rangle\}$$

die *duale Seite* zu S . □

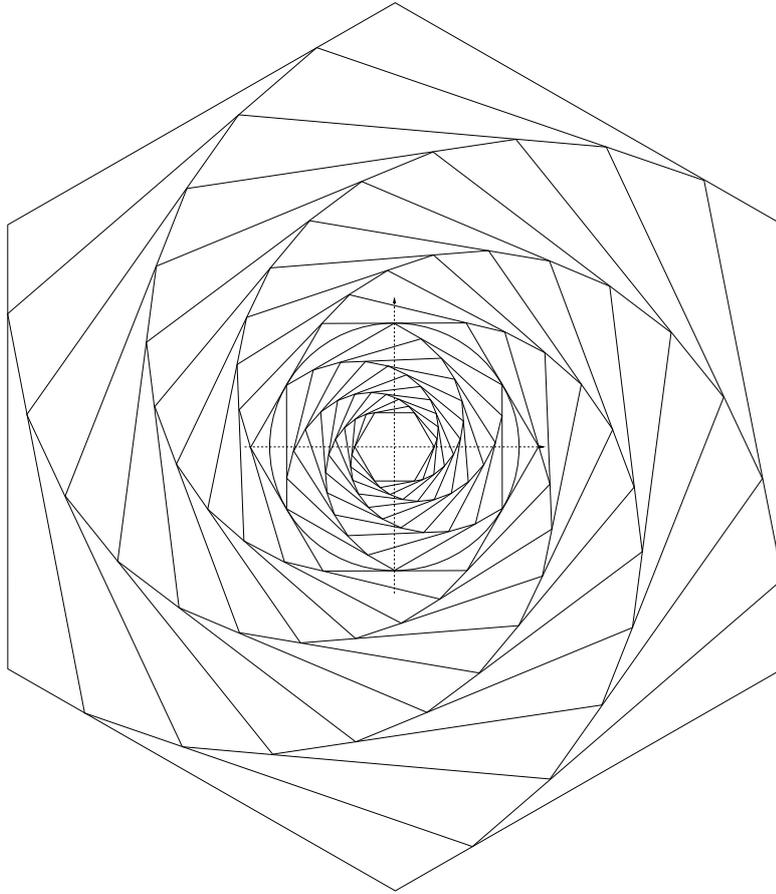


Abbildung 6.4: Die Polaren zu einer Kette von Polygonen

Analog definieren wir die duale Seite in K zu einer Seite von K° .

Es ist $\emptyset^\Delta = K$ und $K^\Delta = \emptyset$. Die duale Seite S^Δ zu einer Seite $S \subseteq K$ ist entweder leer oder eine Seite. Weiterhin ist S^Δ der Schnitt aller durch S in K° ausgeschnittenen Seiten:

$$S^\Delta = \bigcap_{s \in S} S_s^{K^\circ}.$$

Umgekehrt kann S^Δ als die Menge der Funktionale, die durch K° induziert werden und auf S verschwinden, aufgefasst werden. Die dualen Seiten zu einem Punkt haben wir in Satz 6.2.11 als die echten annullierten Seiten der Polaren charakterisiert. Dieser Begriff erlaubt die Dualisierung einer Hierarchie von Seiten:

Proposition 6.2.17 - Annullierte Seiten und echte Seiten

Sei $S \subseteq K$ eine Seite.

- (i) S ist genau dann annulliert, wenn $(S^\Delta)^\Delta = S$ gilt.
- (ii) S ist genau dann echt, wenn S^Δ echt ist. □

Beweis. (i): Sei $S \subseteq K$ eine Seite. Aus $(S^\Delta)^\Delta = S$ folgt, dass S annulliert ist. Wir zeigen nun die andere Implikation. Sei S annulliert. Dann existiert ein $w \in S^\Delta$, sodass aus $1 = \langle w, v \rangle$ für $v \in K$ folgt: $v \in S$. Sei nun $d \in (S^\Delta)^\Delta$. Dann gilt, da $w \in S^\Delta$, insbesondere $1 = \langle w, d \rangle$, woraus folgt: $d \in S$.

(ii): Ist S nicht echt, so ist auch S^Δ nicht echt. Sei nun S echt. Dann ist S in einer maximalen Seite F von K enthalten. Aus $(S^\Delta)^\Delta \subseteq (F^\Delta)^\Delta = F$ folgt, dass S^Δ nicht leer ist. Ist $v \in S^\Delta$, so ist $-v \notin S^\Delta$, also ist S echt. ■

Satz 6.2.18 - Extremalpunkte und maximale Seiten

Sei $S \subseteq K$ eine Seite, die einen annullierten Extremalpunkt von K enthält. Dann sind äquivalent:

- (a) $S = \{e\}$ für einen annullierten Extremalpunkt $e \in K$.
- (b) S^Δ ist eine maximale Seite von K° . □

Beweis. (a) \Rightarrow (b): Sei $e \in K$ ein annullierter Extremalpunkt. Dann ist $\{e\}^\Delta$ eine echte Seite von K° . Angenommen, es gelte die Inklusion $\{e\}^\Delta \subsetneq S \subsetneq K^\circ$ für eine annullierte Seite S von K° , dann ist $\emptyset \subsetneq S^\Delta \subseteq (\{e\}^\Delta)^\Delta = \{e\}$. Daraus folgt die Gleichung $S^\Delta = \{e\}$, also ist $S = (S^\Delta)^\Delta = \{e\}^\Delta$. Dies ist ein Widerspruch zur Voraussetzung. Also ist $\{e\}^\Delta$ maximal.

(b) \Rightarrow (a): Es sei $e \in S$ für einen annullierten Extremalpunkt $e \in K$. Dann gilt die Inklusion $S^\Delta \subseteq \{e\}^\Delta$. Da S^Δ maximal ist, folgt die Gleichheit. Da $\{e\}$ annulliert ist, existiert ein $k \in \{e\}^\Delta$, sodass aus $1 = \langle k, v \rangle$ für $v \in K$ folgt: $v = e$. Ist $s \in S$, so ist die Gleichung $1 = \langle s, k \rangle$ erfüllt. Es folgt $s = e$. ■

Die Menge K , die in Abbildung 6.5 dargestellt wird, zeigt, dass in Satz 6.2.18 nicht auf die Voraussetzung verzichtet werden kann. Die duale Seite der maximalen Seite $\{e\}$ enthält Elemente in K° , deren assoziierte lineare Funktionale die Verschwindemengen φ_1 und φ_2 besitzen. Insbesondere besteht $\{e\}^\Delta$ aus mindestens zwei Elementen.

Bemerkung 6.2.19 Sowohl Proposition 6.2.17 als auch Satz 6.2.18 können gleichermaßen für Seiten der Polaren K° formuliert werden. □

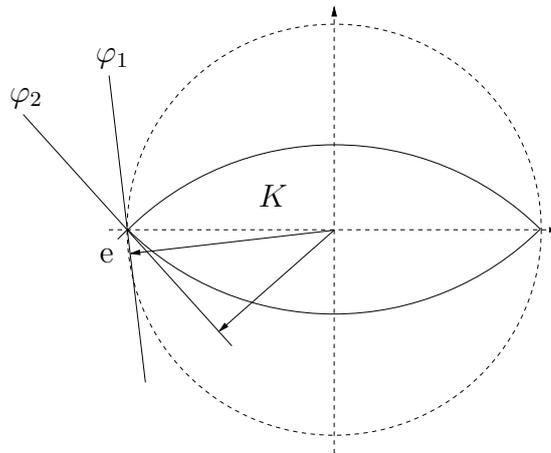


Abbildung 6.5: Ein Extremalpunkt wird von zwei dualen Elementen annulliert

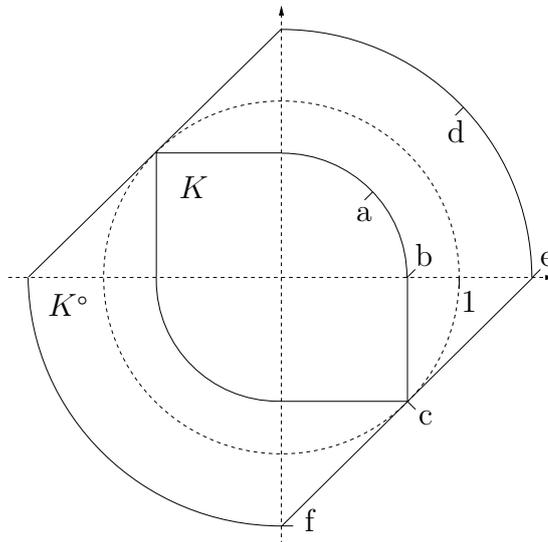


Abbildung 6.6: Visualisierung der Polaren aus Beispiel 6.2.20

Das folgende anschauliche Beispiel illustriert verschiedene duale Zusammenhänge zwischen Seiten.

Beispiel 6.2.20 Skalieren wir das konvexe Gebiet aus Beispiel 6.2.4 mit dem Faktor $1/\sqrt{2}$, erhalten wir eine Menge, deren Vereinigung K mit der dazu kongruenten, um den Winkel π gedrehten Menge in Abbildung 6.6 dargestellt ist. Extremalpunkte von K und K° sind zum Beispiel

$$\begin{aligned} a &:= (0.5, 0.5) \in K, & d &:= (1, 1) \in K^\circ, \\ b &:= (1/\sqrt{2}, 0) \in K, & e &:= (\sqrt{2}, 0) \in K^\circ, \\ c &:= (1/\sqrt{2}, -1/\sqrt{2}) \in K, & f &:= (0, -\sqrt{2}) \in K^\circ. \end{aligned}$$

Die echten Seiten von K werden durch $\{a\}$, $\{b\}$, $\text{co}(b, c)$ und $\{c\}$ repräsentiert. Dabei sind die ersten drei genannten maximal. Die echten Seiten von K° werden durch $\{d\}$, $\text{co}(e, f)$ und $\{e\}$ repräsentiert. Dabei sind die ersten zwei genannten maximal. Die folgende Tabelle zeigt duale Beziehungen zwischen Seiten von K und Seiten von K° auf.

Seite S von K	S^Δ	$(S^\Delta)^\Delta$
$\{a\}$	$\{d\}$	$\{a\}$
$\{b\}$	$\{e\}$	$\text{co}(b, c)$
$\{c\}$	$\text{co}(e, f)$	$\{c\}$
$\text{co}(b, c)$	$\{e\}$	$\text{co}(b, c)$

Die Seite $\{b\}$ ist nicht annulliert, ihre duale Seite nicht maximal und deren duale Seite eine echte Obermenge von $\{b\}$. \square

Abbildung 6.7 veranschaulicht den Einfluss eines maximalen Vektors v und eines Einheitsvektors w mit $w \in K$ auf die Geometrie von K und der Polaren K° .

6.3 Der erste Thetakörper

In diesem Abschnitt zeigen wir, dass der erste Thetakörper für zweifache Tensorprodukte bereits der konvexen Hülle der Produktvektoren entspricht. Zunächst illustrieren wir dies im einfachst denkbaren Fall, dann verallgemeinern wir die Aussage auf beliebige Dimensionen.

Im ersten Abschnitt dieses Kapitels haben wir gezeigt, dass mit dem inneren Radius skalierte Bell-Zustände auf dem Rand des ersten Thetakörpers liegen. Hier werden wir sehen, dass die Polynome, welche wir dazu benutzt haben, 1-sos-mod \mathcal{J}_V sind und die maximalen Seiten, welche zu den Bell-Zuständen gehören, annullieren. Mittels Betrachtungen des letzten Abschnitts schließen wir, dass alle maximalen Seiten der Einheitssphäre der projektiven Norm in $\mathbb{R}^2 \otimes \mathbb{R}^2$ von maximalen Vektoren induziert werden. Weiterhin werden wir zeigen, dass Thetakörper von reellen Radikalen unter Symmetrien ihrer Verschwindemenge invariant bleiben. Dies

Lemma 6.3.1 - Symmetrie reeller algebraischer Varietäten

Sei $Z \subseteq \mathbb{R}^q$ eine reelle algebraische Varietät und $I := \mathcal{J}(Z) \subseteq \mathbb{R}[X_1, \dots, X_q]$. Dann gilt für $O \in \mathcal{O}_q$:

$$\mathcal{J}(O(Z)) = I \circ O^{-1}.$$

Ist Z unter O invariant, gilt sogar: $I = I \circ O^{-1}$. □

Beweis. Es gilt die Äquivalenz

$$\begin{aligned} f \in \mathcal{J}(O(Z)) &\Leftrightarrow f(x) = 0 \text{ für alle } x \in O(Z) \\ &\Leftrightarrow f(O(x)) = 0 \text{ für alle } x \in Z \\ &\Leftrightarrow f \circ O \in \mathcal{J}(Z) = I \\ &\Leftrightarrow f \in I \circ O^{-1}. \end{aligned}$$

Falls $O(Z) = Z$, gilt weiterhin: $I = \mathcal{J}(Z) = \mathcal{J}(O(Z)) = I \circ O^{-1}$. ■

Thetakörper respektieren die Symmetrie ihrer Varietät:

Korollar 6.3.2 - Thetakörper sind symmetrisch

Sei $Z \subseteq \mathbb{R}^q$ eine reelle algebraische Varietät und $I := \mathcal{J}(Z) \subseteq \mathbb{R}[X_1, \dots, X_q]$. Dann gilt für $O \in \mathcal{O}_q$ mit $O(Z) = Z$:

$$\mathcal{T}_k(I) = O(\mathcal{T}_k(I))$$

für alle $k \in \mathbb{N}$. □

Beweis. Sei $O \in \mathcal{O}_q$ mit $O(Z) = Z$. Zunächst zeigen wir eine Hilfsaussage.

Behauptung: Für $f \in \mathbb{R}[X_1, \dots, X_q]$ ist $\deg(f) = \deg(f \circ O)$.

Beweis: Für Monome gilt die Aussage. Das sehen wir so: Sei $p := X_1^{\alpha_1} \dots X_q^{\alpha_q}$ für Exponenten $\alpha_1, \dots, \alpha_q \in \mathbb{N}_0$. Für jeden Teiler X_i , $i \in \{1, \dots, q\}$, bezeichne Y_i das Monom in $(O(X_1, \dots, X_q))_i$ mit dem höchsten Multigrad eins. Dann verschwindet der Anteil von $Y_1^{\alpha_1} \dots Y_q^{\alpha_q}$ in $p \circ O$ nicht. Da die Aussage für Monome gilt, gilt sie auch für beliebige Polynome. ◇

Sei l affin-linear und k -sos-mod I . Dann existiert eine Darstellung

$$l = \sum_{j=1}^r h_j^2 + h$$

mit Polynomen $h_j \in \mathbb{R}[X_1, \dots, X_q]_k$ und $h \in I$. Es ist

$$l \circ O = \sum_{j=1}^r (h_j \circ O)^2 + h \circ O.$$

Da die Grundraumtransformation O den Grad von h_j invariant lässt und $h \circ O \in I$ ist, ist auch $l \circ O$ affin-linear und k -sos-mod I .

Behauptung: Ist $x \in \mathcal{T}_k(I)$, dann ist auch $O(x) \in \mathcal{T}_k(I)$.

Beweis: Sei $x \in \mathcal{T}_k(I)$. Dann ist $l(O(x)) = (l \circ O)(x) \geq 0$ für alle Polynome l , welche affin-linear und k -sos-mod I sind. Daraus folgt: $O(x) \in \mathcal{T}_k(I)$. \diamond

Da die Varietät auch unter O^{-1} invariant bleibt, folgt die Aussage. \blacksquare

Die maximalen Seiten im einfachsten Fall

In diesem Abschnitt betrachten wir den Spezialfall $V := \mathbb{R}^2 \otimes \mathbb{R}^2$. Wir leiten eine Darstellung der maximalen Seiten der projektiven Einheitskugel her und zeigen, dass jede maximale Seite einen mit dem inneren Radius skalierten maximalen Vektor als inneren Punkt besitzt.

Eine Parametrisierung aller orthogonalen Matrizen in $\mathcal{M}_2(\mathbb{R})$ ist gegeben durch

$$U_z^i := \begin{pmatrix} z_1 & -(-1)^i z_2 \\ z_2 & (-1)^i z_1 \end{pmatrix}$$

mit einem Einheitsvektor $z = (z_1, z_2)$ und $i \in \{0, 1\}$, wobei der letztere Parameter modulo zwei gerechnet wird. Drehungen werden durch die Wahl $i = 0$ und Spiegelungen durch die Wahl $i = 1$ repräsentiert. Wir setzen

$$U := U_{e_2}^0 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{und} \quad T := U_{e_1}^1 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Eine einfache Rechnung zeigt, dass

$$U_z^i \cdot U = (-1)^i \cdot U \cdot U_z^i$$

für alle Einheitsvektoren z und $i \in \{0, 1\}$ gilt.

Alle Tensoren in V besitzen eine Darstellung, die die projektive Norm liefert. Es ist möglich, ein Tensor als Linearkombination zweier Einheitsproduktvektoren zu schreiben, wobei die Faktoren jeweils zueinander orthogonal sind. Die Summe der

Koeffizienten ergibt die projektive Norm. Ein Vektor mit projektiver Norm eins besitzt also eine Darstellung der folgenden Art:

$$\begin{aligned}\eta(v, w, \lambda, i+j) &:= \lambda v \otimes w + (1-\lambda)(-1)^{i+j}U(v) \otimes U(w) \\ &= (U_v^i \otimes U_w^j)(\lambda e_1 \otimes e_1 + (1-\lambda)e_2 \otimes e_2)\end{aligned}$$

mit $\lambda \in [0, 1]$, $i, j \in \{0, 1\}$ und zwei Einheitsvektoren v und w .

Für feste Wahlen von v und w wird die Hilbert-Schmidt-Norm für $\lambda = 1/2$ minimal. Entsprechend erhalten wir alle maximalen Vektoren durch die Wahl $\lambda = 1/2$ und eine Skalierung mit $\sqrt{2}$:

$$\begin{aligned}\{\xi \in V \mid \xi \text{ ist maximal}\} &= \left\{ \sqrt{2} \cdot \eta(v, w, 1/2, k) \mid \|v\| = \|w\| = 1, k \in \{0, 1\} \right\} \\ &= \left\{ \frac{1}{\sqrt{2}}(v \otimes w + (-1)^k U(v) \otimes U(w)) \mid \|v\| = \|w\| = 1, k \in \{0, 1\} \right\}.\end{aligned}$$

Die Gruppe \mathcal{G}_V ist sowohl auf den Einheitsproduktvektoren als auch auf den maximalen Vektoren invariant. In beiden Fällen wirkt sie auch transitiv.

Lemma 6.3.3 - Eine maximale Seite

Die maximale Seite zum Bell-Zustand

$$y := \frac{1}{\sqrt{2}}(e_1 \otimes e_1 + e_2 \otimes e_2)$$

ist

$$\begin{aligned}S_y &= \{\eta(v, v, \lambda, 0) \mid \|v\| = 1, \lambda \in [0, 1]\} \\ &= \{\lambda(v \otimes v) + (1-\lambda)U(v) \otimes U(v) \mid \|v\| = 1, \lambda \in [0, 1]\} \\ &= \text{co}(\{v \otimes v \mid \|v\| = 1\}).\end{aligned}$$

□

Beweis. Die maximale Seite zu y ist eine konvexe Menge, die aus bezüglich der projektiven Norm normierten Tensoren besteht. Sei $\eta = \eta(v, w, \lambda, k)$ ein Element dieser Seite. Dann ist

$$\begin{aligned}1 &= \langle y / \|y\|_\epsilon, \eta \rangle = \langle e_1 \otimes e_1 + e_2 \otimes e_2, \lambda(v \otimes w) + (1-\lambda)(-1)^k U(v) \otimes U(w) \rangle \\ &= \langle v, w \rangle \cdot (\lambda + (1-\lambda)(-1)^k).\end{aligned}$$

Im Fall $k = 0$ folgt daraus die Gleichung $v = w$ und wir erhalten: $\eta = \eta(v, v, \lambda, 0)$. Im Fall $k = 1$ ist entweder $v = w$ und $\lambda = 1$, woraus $\eta = \eta(v, v, 1, 0)$ folgt, oder es gilt die Gleichung $v = -w$ mit $\lambda = 0$, woraus $\eta = \eta(U(v), U(v), 1, 0)$ folgt. Wie wir sehen, reduziert sich der Fall $k = 1$ auf den Fall $k = 0$. Daraus folgen die ersten beiden Gleichungen der Behauptung. Die letzte Gleichung folgt aus der Konvexität der maximalen Seite zu y . ■

Die Mengen

$$\begin{aligned}\mathcal{O}^0 &:= \{O \otimes O \mid O \in \mathcal{O}_2, \det(O) = 1\} \quad \text{und} \\ \mathcal{O}^1 &:= \{O \otimes O^t \mid O \in \mathcal{O}_2, \det(O) = 1\}\end{aligned}$$

sind Untergruppen von \mathcal{G}_V .

Satz 6.3.4 - Maximale Seiten der Einheitssphäre

Sei $\xi = \sqrt{2} \cdot \eta(v, w, 1/2, k)$ ein maximaler Vektor. Dann ist die maximale Seite zu ξ gegeben durch

$$\begin{aligned}S_\xi &= \text{co}(\{\tilde{O}(v \otimes w) \mid \tilde{O} \in \mathcal{O}^k\}) \\ &= \{\tilde{O}(\lambda(v \otimes w) + (1 - \lambda)(-1)^k U(v) \otimes U(w)) \mid \tilde{O} \in \mathcal{O}^k, \lambda \in [0, 1]\} \\ &= \{\tilde{O}(\eta(v, w, \lambda, k)) \mid \tilde{O} \in \mathcal{O}^k, \lambda \in [0, 1]\}.\end{aligned}$$

Weiterhin ist in jeder maximalen Seite S von $\mathcal{B}_{1,\pi}$ genau ein skalierter maximaler Vektor $\eta = \eta(v, w, 1/2, k)$ enthalten. Dieser ist ein innerer Punkt von S und Fixpunkt von \mathcal{O}^k . Für alle Tensoren $\tau \in V$ folgt aus $\eta + \tau \in S$, dass $\eta - \tau \in S$ gilt. \square

Beweis. *Schritt 1:* Bestimmung der maximalen Seiten.

Es sei $\xi := \sqrt{2} \cdot \eta(v, w, 1/2, i + j)$ ein maximaler Vektor in der Darstellung von oben.

Behauptung: Es ist

$$\begin{aligned}S_\xi &= \text{co}(\{(U_v^i \otimes U_w^j)(x \otimes x) \mid \|x\| = 1\}) \\ &= (U_v^i \otimes U_w^j)(S_y).\end{aligned}$$

Beweis: Dass die letzte Gleichung der Behauptung wahr ist, zeigt Lemma 6.3.3. Wir zeigen noch die erste Gleichung. Die maximale Seite zu ξ ist durch die Vektoren η mit projektiver Norm eins, die die Gleichung

$$1 = \left\langle \frac{\xi}{\|\xi\|_\epsilon}, \eta \right\rangle$$

erfüllen, gegeben. Wir setzen:

$$S := \text{co}(\{(U_v^i \otimes U_w^j)(x \otimes x) \mid \|x\| = 1\}).$$

Vektoren der Form $(U_v^i \otimes U_w^j)(x \otimes x)$ erfüllen die obige Gleichung nach Lemma 6.3.3. Also gilt: $S \subseteq S_\xi$. Sei nun $\eta \in S_\xi$, dann ist $((U_v^i)^{-1} \otimes (U_w^j)^{-1})(\eta)$ in der maximalen Seite zu y enthalten. Es folgt: $\eta \in S$. \diamond

Behauptung: Für alle Einheitsvektoren x gilt:

$$U_v^i(x) = T^i(U_x^i(v)) \quad \text{und} \quad T^i U_x^i = U_{T^i(x)}^0.$$

Beweis: Es ist

$$U_v^i(x) = \begin{pmatrix} x_1 v_1 - (-1)^i x_2 v_2 \\ x_1 v_2 + (-1)^i x_2 v_1 \end{pmatrix} = \begin{cases} U_x^0(v), & i = 0 \\ T(U_x^1(v)), & i = 1 \end{cases}, \quad \text{wobei}$$

$$U_x^0 = \begin{pmatrix} x_1 & -x_2 \\ x_2 & x_1 \end{pmatrix}, \quad U_x^1 = \begin{pmatrix} x_1 & x_2 \\ x_2 & -x_1 \end{pmatrix} \quad \text{und} \quad T(U_x^1) = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix}$$

gilt. Die letzte Gleichung ist wahr für $i = 0$. Für $i = 1$ ist

$$U_{T(x)}^0 = \begin{pmatrix} x_1 & x_2 \\ -x_2 & x_1 \end{pmatrix} = T(U_x^1) = (U_x^0)^t.$$

Daraus folgt die Behauptung. ◇

Es folgt also, dass die maximale Seite zu ξ auf diese Weise geschrieben werden kann:

$$S_\xi = \text{co} \left(\left\{ \left(U_{T^i(x)}^0 \otimes U_{T^j(x)}^0 \right) (v \otimes w) \mid \|x\| = 1 \right\} \right).$$

Für alle Einheitsvektoren x und $i \in \{0, 1\}$ ist $U_{T^i(x)}^0$ eine Drehung. Falls nun $i + j$ gerade ist, handelt es sich sowohl im vorderen als auch im hinteren Teil um die gleiche Drehung. Im Fall $i + j$ ungerade ist die zweite Drehung die Transponierte der ersten. Es folgt die erste Gleichung der Behauptung.

Schritt 2: Herleiten einer weiteren Darstellung.

Es sei $k := i + j$ und

$$\tilde{S} := \left\{ \tilde{O} \left(\lambda(v \otimes w) + (1 - \lambda)(-1)^k U(v) \otimes U(w) \right) \mid \tilde{O} \in \mathcal{O}^k, \lambda \in [0, 1] \right\}.$$

Wir zeigen zunächst die Inklusion $\tilde{S} \subseteq S_\xi$. Da die maximale Seite S_ξ konvex ist, ist es ausreichend, zu zeigen, dass für alle $\tilde{O} \in \mathcal{O}^k$ die beiden Tensoren $\tilde{O}(v \otimes w)$ und $\tilde{O}((-1)^k U(v) \otimes U(w))$ darin enthalten sind. Für den ersten Tensor folgt dies sofort aus der bereits bekannten Darstellung. Mit $k = 0$ ist der zweite Tensor auch in der maximalen Seite enthalten. Sei nun $k = 1$. Dann ist dieser gegeben durch

$$O \otimes O^t(-U(v) \otimes U(w)) = -OU(v) \otimes O^t U(w) = OU \otimes (OU)^t(v \otimes w)$$

für eine Drehung $O \in \mathcal{O}_2$, da nach einer einführenden Bemerkung in diesem Unterabschnitt O und U kommutieren und damit die Gleichung

$$O^t U = -O^t U^t = -(UO)^t = -(OU)^t$$

gilt. Also ist auch dieser in der maximalen Seite enthalten. Nun zeigen wir die Inklusion $S_\xi \subseteq \tilde{S}$. Nach der ersten Behauptung hat ein Vektor in S_ξ die Form

$$\begin{aligned}
 & (U_v^i \otimes U_w^j)(\lambda(x \otimes x) + (1 - \lambda)U(x) \otimes U(x)) \\
 &= \lambda(U_v^i(x) \otimes U_w^j(x)) + (1 - \lambda)U_v^i U(x) \otimes U_w^j U(x) \\
 &= \lambda \left(U_{T^i(x)}^0(v) \otimes U_{T^j(x)}^0(w) \right) + (1 - \lambda)(-1)^{i+j} U U_v^i(x) \otimes U U_w^j(x) \\
 &= \lambda \left(U_{T^i(x)}^0 \otimes U_{T^j(x)}^0 \right) (v \otimes w) + (1 - \lambda)(-1)^{i+j} (U \otimes U) \left(U_{T^i(x)}^0 \otimes U_{T^j(x)}^0 \right) (v \otimes w) \\
 &= \tilde{O} \left(\lambda(v \otimes w) + (1 - \lambda)(-1)^k U(v) \otimes U(w) \right)
 \end{aligned}$$

für einen Einheitsvektor x , einen Faktor $\lambda \in [0, 1]$ und $\tilde{O} := U_{T^i(x)}^0 \otimes U_{T^j(x)}^0 \in \mathcal{O}^k$. Diese Darstellung zeigt, dass die maximale Seite S_ξ in \tilde{S} enthalten ist. Daraus folgen die zweite und die dritte Gleichung.

Schritt 3: Maximale Seiten beinhalten maximal einen mit dem inneren Radius skalierten maximalen Vektor.

Sind A und B zwei konvexe Mengen mit $A \subseteq B$ und S eine Seite in B , so ist der Schnitt $A \cap S$ eine Seite in A oder leer. Da die Einheitskugel der Hilbert-Schmidt-Norm strikt konvex ist, ist jeder ihrer Extrempunkte auch eine maximale Seite. Eine Seite der Einheitskugel der projektiven Norm besitzt also maximal einen Vektor, der die minimale Hilbert-Schmidt-Norm besitzt. Insbesondere ist ein solcher Vektor invariant unter \mathcal{O}^0 beziehungsweise unter \mathcal{O}^1 , da jede Transformation mit einem solchen Element einen maximalen Vektor liefert, der in der gleichen Seite liegt.

Schritt 4: Maximale Vektoren als innere Punkte.

Sei nun S eine maximale Seite zum Vektor $z := \eta(x, y, 1/2, k) \in S$ mit $\|x\| = \|y\| = 1$ und $k \in \{0, 1\}$.

Behauptung: Für alle $w \in S$ ist $-w + 2z \in S$.

Beweis: Es existiert ein $\tilde{O} \in \mathcal{O}^k$ und ein Faktor $\lambda \in [0, 1]$, sodass $w = \lambda p + (1 - \lambda)q$ gilt, wobei $p := \tilde{O}(x \otimes y)$ und $q := \tilde{O}((-1)^k U(x) \otimes U(y))$ ist. Es ist $z = 1/2(p + q)$. Also folgt: $-w + 2z = (1 - \lambda)p + \lambda q \in S$. \diamond

Ist $w = z + (w - z) \in S$, so gilt auch $z - (w - z) = -w + 2z \in S$. Insbesondere ist z ein innerer Punkt von S . \blacksquare

Bemerkung 6.3.5 Eine maximale Seite S von $\mathcal{B}_{1,\pi}$ enthält also genau einen skalierten maximalen Vektor $\eta = \eta(v, w, 1/2, k)$. Sie ist invariant unter \mathcal{O}^k . Damit ist η als ein innerer Punkt von S und Fixpunkt von \mathcal{O}^k auf zwei Weisen ein „Schwerpunkt“ von S . Um dies zu präzisieren, geben wir die letzten Aussagen des Satzes konkreter wieder:

(i) Ist $\vartheta = \eta(v, w, \lambda, k) \in S$, dann ist $\vartheta = \eta + (\vartheta - \eta)$ und es gilt:

$$\eta - (\vartheta - \eta) = 2\eta - \vartheta = \eta(v, w, 1 - \lambda, k) = (U \otimes (-1)^k U)(\vartheta).$$

Dies zeigt eine einfache Rechnung.

(ii) Die Gruppe \mathcal{O}^k operiert treu auf dem Rand von $\mathcal{B}_{1,\pi}$. Die Menge der Fixpunkte ist

$$\left\{ \eta(x, y, 1/2, k) \mid \|x\| = \|y\| = 1 \right\},$$

besteht also nur aus skalierten maximalen Vektoren. Dies sehen wir so: Eine notwendige Bedingung an einen Fixpunkt $\eta = \eta(x, y, \lambda, \tilde{k})$ ist, dass $(U \otimes (-1)^k U)(\eta) = \eta$ gilt, was nach einer einfachen Rechnung zu den Gleichungen $\lambda = 1/2$ und $\tilde{k} = k$ führt.

Auf Abbildung 6.8 ist dieser Sachverhalt schematisch dargestellt. □

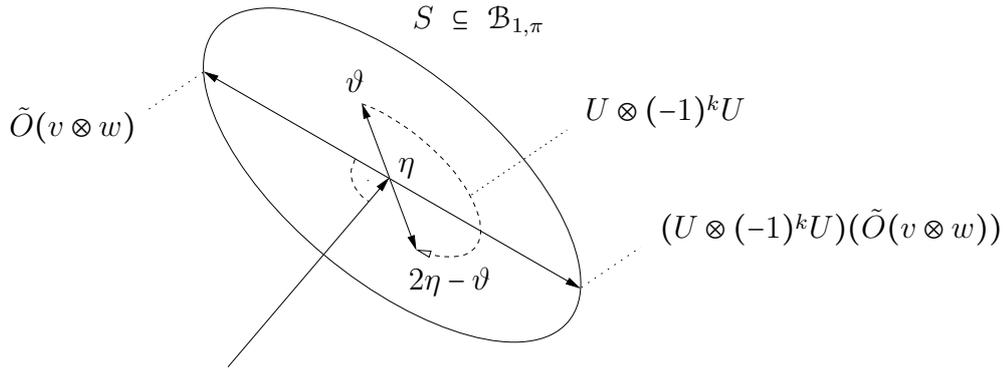


Abbildung 6.8: Maximale Vektoren als Schwerpunkte

Beispiel 6.3.6 Wir bestimmen die maximalen Seiten aller Bell-Zustände. Dazu setzen wir die Variablen, die in der Tabelle

Skalierter Bell-Zustand	\diamond	\diamond
$1/2(e_1 \otimes e_1 + e_2 \otimes e_2) = \eta(e_1, e_1, 1/2, 0)$	$(v_1, v_2) \otimes (v_1, v_2)$	$(-v_2, v_1) \otimes (-v_2, v_1)$
$1/2(e_1 \otimes e_1 - e_2 \otimes e_2) = \eta(e_1, e_1, 1/2, 1)$	$(v_1, v_2) \otimes (v_1, -v_2)$	$(v_2, -v_1) \otimes (v_2, v_1)$
$1/2(e_1 \otimes e_2 + e_2 \otimes e_1) = \eta(e_1, e_2, 1/2, 1)$	$(v_1, v_2) \otimes (v_2, v_1)$	$(-v_2, v_1) \otimes (v_1, -v_2)$
$1/2(e_1 \otimes e_2 - e_2 \otimes e_1) = \eta(e_1, e_2, 1/2, 0)$	$(v_1, v_2) \otimes (-v_2, v_1)$	$(v_2, -v_1) \otimes (v_1, v_2)$

angegeben sind, in diesen Ausdruck ein:

$$\{\lambda(\otimes) + (1 - \lambda)(\otimes) \mid v = (v_1, v_2), \|v\| = 1, \lambda \in [0, 1]\}.$$

Das ergibt die maximale Seite zum entsprechenden Zustand. \square

Die Tatsache, dass eine maximale Seite Tensoren enthält, die von genau zwei Parametern abhängen, legt den Schluss nahe, dass es sich bei den maximalen Seiten von $\mathcal{B}_{1,\pi}$ um zweidimensionale Objekte handelt. Die Ausführung dieses Gedankens soll hier jedoch nicht Gegenstand der Betrachtung werden.

Maximale Vektoren im verallgemeinerten Fall

Es sei nun $V := \mathbb{R}^n \otimes \mathbb{R}^m$ wie oben angegeben.

Für einen Vektor $\xi \in V$ existiert eine im Wesentlichen eindeutige Darstellung

$$\xi = \sum_{i=1}^n \lambda_i e_i \otimes f_i$$

mit $\lambda_i \geq 0$ und Orthonormalsystemen $\{e_i\}_{i=1}^n$ in \mathbb{R}^n und $\{f_i\}_{i=1}^n$ in \mathbb{R}^m . Es ist

$$\|\xi\|_{\pi} = \sum_{i=1}^n \lambda_i.$$

Mit dieser Darstellung lassen sich die maximalen Vektoren leicht ermitteln:

Proposition 6.3.7 - Maximale Vektoren der projektiven Einheitsphäre

Für $\xi \in V$, $\|\xi\| = 1$ sind äquivalent:

- (a) ξ ist maximal.
- (b) Es existiert eine Darstellung

$$\xi = \sum_{i=1}^n \frac{1}{\sqrt{n}} e_i \otimes f_i$$

mit Orthonormalsystemen $\{e_i\}_{i=1}^n$ in \mathbb{R}^n und $\{f_i\}_{i=1}^n$ in \mathbb{R}^m . \square

Beweis. Wir ermitteln alle Randpunkte von $\mathcal{B}_{1,\text{HS}}$, deren projektive Norm maximal ist. Sei $\xi \in \mathcal{B}_{1,\text{HS}}$, $\|\xi\| = 1$, dargestellt wie oben. Dann ist

$$\|\xi\|_{\text{HS}} = \sum_{i=1}^n \lambda_i^2 = 1.$$

Wir minimieren die Funktion

$$\begin{aligned} \|\cdot\|_\pi : \quad (\mathbb{R}_0^+)^n &\rightarrow \mathbb{R}_0^+ \\ (\lambda_1, \dots, \lambda_n) &\mapsto \lambda_1 + \dots + \lambda_n, \end{aligned}$$

unter der Nebenbedingung $\varphi := 1 - \sum_{i=1}^n \lambda_i^2$. Der Gradient von $\|\cdot\|_\pi$ ist konstant eins. Die j -te Komponente des Gradienten von φ ist $-2\lambda_j$ für $j = 1, \dots, n$. Nach der Multiplikatorregel von Lagrange ist eine notwendige Bedingung eines Extrempunktes von $\|\cdot\|_\pi$ im Innern von $(\mathbb{R}_0^+)^n$ unter der Nebenbedingung φ , dass die Gradienten linear abhängig sind. Äquivalent dazu ist die Bedingung $\lambda_1 = \dots = \lambda_n =: \lambda$. Dies ist genau dann der Fall, wenn $\lambda = 1/\sqrt{n}$ gilt.

Jetzt untersuchen wir, ob die Funktion $\|\cdot\|_\pi$ Randmaxima besitzt. Wir nehmen dazu den Fall $\lambda_1, \dots, \lambda_k > 0$ und $\lambda_{k+1}, \dots, \lambda_n = 0$, $k \in \{1, \dots, n-1\}$, an. Dann wird das Maximum von $\|\cdot\|_\pi$ unter dieser Nebenbedingung für $\lambda_1 = \dots = \lambda_k = 1/\sqrt{k}$ angenommen. Dieser Wert ist allerdings echt kleiner als \sqrt{n} und liefert kein globales Extremum. ■

Maximale Vektoren annullieren Extrempunkte der Einheitssphäre der injektiven Norm $\mathcal{B}_{1,\varepsilon}$ nach Proposition 6.2.13. Wie in Proposition 5.2.6 gesehen, sind dies bereits alle Extrempunkte von $\mathcal{B}_{1,\varepsilon}$. Diese liefern nach Satz 6.2.18 Funktionale, welche die zu den maximalen Vektoren gehörigen maximalen Seiten annullieren.

Lemma 6.3.8 - Jede maximale Seite von $\mathcal{B}_{1,\pi}$ wird durch einen maximalen Vektor induziert. □

Beweis. Ist $\xi \in V$ maximal, so annulliert das Funktional

$$\Phi_\xi := -\left\langle \frac{\xi}{\|\xi\|_\varepsilon}, \cdot \right\rangle + 1$$

die durch ξ induzierte maximale Seite S_ξ^V von V . Sei nun $\eta \in V$ mit $\|\eta\|_\pi = 1$.

Behauptung: Es existiert ein maximaler Vektor ξ mit $\Phi_\xi(\eta) = 0$.

Beweis: Es existiert eine Darstellung

$$\eta = \sum_{i=1}^n \mu_i e_i \otimes f_i$$

mit Faktoren $\mu_i \geq 0$, $\mu_1 + \dots + \mu_n = 1$, und ONS $\{e_i\}_{i=1}^n$ in \mathbb{R}^n und $\{f_i\}_{i=1}^n$ in \mathbb{R}^m . Sei

$$\xi := \frac{1}{\sqrt{n}} \sum_{i=1}^n e_i \otimes f_i,$$

dann ist $e_i \otimes f_i \in \mathcal{Z}(\Phi_\xi)$ für alle $i \in \{1, \dots, n\}$. Damit ist

$$\eta \in \text{co}(e_1 \otimes f_1, \dots, e_n \otimes f_n) \subseteq \mathcal{Z}(\Phi_\xi),$$

das heißt, ξ leistet das Gewünschte. \diamond

Damit ist η in der von ξ induzierten Seite enthalten. Es ist also jeder Randpunkt von $\mathcal{B}_{1,\pi}$ in einer von einem maximalen Vektor induzierten maximalen Seite enthalten. Wir zeigen nun, dass alle maximalen Seiten von $\mathcal{B}_{1,\pi}$ von dieser Gestalt sind. Sei S eine maximale Seite. Dann existiert ein innerer Punkt $\tau \in \text{relin}(S)$. Wie oben gezeigt, ist τ in einer von einem maximalen Vektor induzierten maximalen Seite S' enthalten. Mit Proposition 6.2.3, (v) folgt nun, dass $S \subseteq S'$ gilt. Wegen der Maximalität von S folgt die Gleichheit. \blacksquare

Approximation der Einheitssphäre der projektiven Norm durch den ersten Thetakörper

Für zweifache Tensorprodukte ist $\mathcal{B}_{1,\pi}$ der Schnitt aller Halbräume, welche durch Polynome induziert werden, die 1-sos-mod \mathcal{J}_V sind:

Satz 6.3.9 - Approximation durch den ersten Thetakörper

In $\mathbb{R}^n \otimes \mathbb{R}^m$ ist $\mathcal{T}_1 = \mathcal{B}_{1,\pi}$. \square

Beweis. Der Vektor

$$y := \frac{1}{\sqrt{n}} \sum_{i=1}^n e_i \otimes e_i$$

ist maximal und das affin-lineare Polynom

$$l := 1 - \left(\sum_{i=1}^n x_{ii} \right) = -\langle \sqrt{n} \cdot \iota(y), \cdot \rangle + 1$$

annulliert die maximale Seite zu y . Das Polynom

$$h := \frac{1}{2} \left(1 - \sum_{i \in N} x_i^2 - \sum_{\substack{i,j=1,\dots,n \\ i \neq j}} (x_{ii}x_{jj} - x_{ij}x_{ji}) \right)$$

ist im Ideal \mathcal{J}_V enthalten. Eine einfache Rechnung zeigt, dass l kongruent zu der Summe von Quadraten

$$f := \frac{1}{2} \left(\left(-1 + \sum_{i=1}^n x_{ii} \right)^2 + \sum_{\substack{i=1,\dots,n \\ j>n}} x_{ij}^2 + \sum_{\substack{i,j=1 \\ i>j}}^n (x_{ij} - x_{ji})^2 \right)$$

modulo \mathcal{J}_V mit $l = f + h$ ist. Im Beweis von Satz 6.1.11 ist dies bereits für $n = m = 2$ dargelegt. Sei nun v ein maximaler Vektor. Die Gruppe \mathcal{G}_V wirkt transitiv auf allen maximalen Vektoren. Es existiert daher eine Abbildung $A := U_1 \otimes U_2 \in \mathcal{G}_V$ mit $U_1 \in \mathcal{O}_n, U_2 \in \mathcal{O}_m$ und $v = A(y)$. Wir betrachten nun das Funktional

$$\begin{aligned} l \circ A^{-1} &= -\langle \sqrt{n} \cdot \iota(y), A^{-1}(\cdot) \rangle + 1 = -\langle A(\sqrt{n} \cdot \iota(y)), \cdot \rangle + 1 = -\langle \sqrt{n} \cdot \iota(v), \cdot \rangle + 1 \\ &= f \circ A^{-1} + h \circ A^{-1}. \end{aligned}$$

Argumente, die bereits im Beweis von Lemma 6.3.2 verwandt wurden, zeigen, dass der Grad eines Polynoms unter einer Grundraumtransformation invariant bleibt. Insbesondere ist $l \circ A^{-1}$ affin-linear und $f \circ A^{-1}$ quadratisch.

Behauptung: $h \circ A^{-1} \in \mathcal{J}_V$.

Beweis: Das Ideal \mathcal{J}_V wird von \mathcal{J}_V und dem Polynom $g := \sum_{i \in N} x_i^2 - 1$ erzeugt. Daher ist es möglich, h in eine Summe $h = h_I + h_J$, wobei $h_I \in \mathcal{J}_V$ und $h_J \in \langle g \rangle$ ist, zu zerlegen. Nach Satz 5.3.9 ist das Ideal \mathcal{J}_V Verschwindeideal der Menge der Produktvektoren. Da A ein Element der Symmetriegruppe der Produktvektoren ist, gilt mit Lemma 6.3.1: $h_I \circ A^{-1} \in \mathcal{J}_V$. Da ι ein isometrischer Isomorphismus zwischen V und $\mathcal{M}_{n,m}(\mathbb{R})$ ist, folgt

$$\begin{aligned} g \circ A^{-1} &= (\langle \iota(\cdot), \iota(\cdot) \rangle - 1) \circ A^{-1} \\ &= (\langle \iota(A^{-1}(\cdot)), \iota(A^{-1}(\cdot)) \rangle - 1) = \langle \iota(\cdot), \iota(\cdot) \rangle - 1 \\ &= g. \end{aligned}$$

Somit ist g invariant unter A^{-1} , $h_J \circ A^{-1} \in \mathcal{J}_V$ und die Aussage folgt. \diamond

Damit ist auch $l \circ A^{-1}$ affin-linear und 1-sos-mod \mathcal{J}_V . Weiterhin annulliert $l \circ A^{-1}$ die zu v gehörige maximale Seite. Nach Lemma 6.3.8 sind alle maximalen Seiten durch maximale Vektoren gegeben. Daraus folgt die Aussage. \blacksquare

7 Numerische Simulation

Das Ziel dieser Arbeit ist es, die projektive Norm mit einer Methode, die auf dem Konzept der Konvergenz von Thetakörpern beruht, zu berechnen.

In den Kapiteln 5 und 6 haben wir theoretische Methoden dargelegt, wie die Einheitssphäre der projektiven Norm als konvexe Hülle einer Varietät durch Thetakörper beschrieben werden kann. Für zweifache Tensorprodukte haben wir festgestellt, dass bereits der erste Thetakörper mit der Einheitssphäre übereinstimmt. In diesem Fall kann die projektive Norm allerdings vergleichsweise unkompliziert mit elementaren Methoden der linearen Algebra berechnet werden. Diese Methoden greifen nicht mehr im Fall von mehrfachen Tensorprodukten. Wir haben noch keine Aussage gemacht, wie dieser Fall zu behandeln ist, nehmen jedoch an, dass dafür andere Argumente nötig sein werden und sich bei der Verallgemeinerung ähnliche Probleme auftun können, wie es bei der elementaren Methode der Fall ist, nämlich, dass sich viele wichtige Eigenschaften nicht assoziativ verhalten.

Wir finden trotzdem eine Methode, die projektive Norm durch Thetakörper zu berechnen. In diesem Kapitel stellen wir das Programm PINORM vor, welches basierend auf dem Computeralgebrasystem MATLAB in der Lage ist, die Berechnung durchzuführen. Das Programm nutzt die Beschreibung von Thetakörpern als projizierte Spektraeder und eine numerische Methode aus der *semidefiniten Programmierung*, die es erlaubt, Spektraeder als Lösungsmenge *semidefiniter Programme* zu beschreiben.

Ein Überblick über das Programm

Das Programm PINORM approximiert die projektive Norm von Tensoren aus dem reellen Tensorprodukt

$$V := \mathbb{R}^{n_1} \otimes \dots \otimes \mathbb{R}^{n_r}$$

für natürliche Zahlen $n_1, \dots, n_r \geq 2$ und $r > 1$, indem es Thetanormen zu beliebigen Thetakörpern berechnet. Dies geschieht mittels der Darstellung von Thetakörpern als projizierte Spektraeder.

Es sei $n := n_1 \cdots n_r$ die Dimension von V . Aus Kapitel 6 übernehmen wir alle Konventionen und die Notation.

7.1 Thetakörper als Lösungen semidefiniter Programme

In [GaMa] werden semidefinite Programme als Verallgemeinerung linearer Programme eingeführt. Sie erweitern die lineare Optimierung um eine spezielle Klasse nicht-linearer Optimierungsprobleme. Das Ziel dieses Abschnitts ist es, zu zeigen, dass die semidefinite Programmierung zur Bestimmung von Thetanormen herangezogen werden kann.

Symmetrische Matrizen und semidefinite Programmierung

Für eine natürliche Zahl $m \in \mathbb{N}$ ist die Abbildung

$$\langle A, B \rangle := \sum_{i,j=1}^m a_{i,j} b_{i,j}$$

für $A, B \in \mathcal{S}_m$ ein Skalarprodukt auf den symmetrischen $m \times m$ -Matrizen.

Definition 7.1.1 - Semidefinite Programme

Ein Optimierungsproblem der Form

$$\begin{aligned} \max! \quad & \langle C, X \rangle && \text{(Zielfunktion)} \\ \text{mit} \quad & \langle A_1, X \rangle = a_1, && \text{(Nebenbedingungen)} \\ & \langle A_2, X \rangle = a_2, \\ & \vdots \\ & \langle A_s, X \rangle = a_s, \\ & X \geq 0 \end{aligned}$$

in den Variablen $X \in \mathcal{S}_m$ mit Restriktionsmatrizen $C, A_1, \dots, A_s \in \mathcal{S}_m$ sowie Schranken $a_1, \dots, a_s \in \mathbb{R}$ heißt *semidefinites Programm (SDP)*. Das Programm heißt *lösbar*, falls ein $X \in \mathcal{S}_m$ existiert, sodass alle Nebenbedingungen erfüllt sind. In diesem Fall heißt X *Lösung* oder, falls die Zielfunktion an X maximal wird, *optimale Lösung*. \square

In [GaMa] werden Algorithmen zur Lösung von semidefiniten Programmen angegeben. Wir benutzen das Programm SDPT3-4.0, welches von [Toh] bereitgestellt wird.

Approximation der projektiven Norm durch semidefinite Programmierung

Für alle $k \in \mathbb{N}$ ist der k -te Thetakörper \mathcal{T}_k zum Ideal \mathcal{J}_V gleich dem Abschluss der Projektion des Spektraeders

$$S_k := \left\{ \tilde{y} = (\tilde{y}_b)_{b \in \Theta_{2k}} \mid \mathcal{M}_{\Theta_k}(\tilde{y}) \geq 0, \tilde{y}_{1+\mathcal{J}_V} = 1 \right\}$$

auf \mathbb{R}^n , wenn die Voraussetzung von Satz 4.3.3 erfüllt ist. In diesem Fall ist die Projektion $\pi_{\mathbb{R}^n}(S_k)$ dicht in \mathcal{T}_k , also ist das Minkowskifunktional s_k zu $\pi_{\mathbb{R}^n}(S_k)$ gleich der Thetanorm. Ist die Voraussetzung verletzt, ist der Thetakörper immer noch eine echte Obermenge des projizierten Spektraeders $\pi_{\mathbb{R}^n}(S_k)$ und dieser nach Abschnitt 4.4 eine Obermenge von $\mathcal{Z}(\mathcal{J}_V)$. Für alle $y \in \mathbb{R}^{n_1} \otimes \dots \otimes \mathbb{R}^{n_r}$ gilt also:

$$\|y\|_{\Theta,k} \leq s_k(y) \leq \|y\|_{\pi}.$$

Das heißt, dass die Minkowskifunktionale $(s_k)_{k \in \mathbb{N}}$ zum projizierten Spektraeder punktweise gegen die projektive Norm konvergieren. Da wir in diesem Sinne nicht zwischen den Thetanormen und diesen Funktionalen zu unterscheiden brauchen, ist für das Kommende eine Prüfung der Voraussetzung nicht nötig.

Satz 7.1.2 - Thetanormen und Lösungen semidefiniter Programme

Für $k \in \mathbb{N}$ und $y \in \mathbb{R}^n$ existiert ein semidefinites Programm, das genau dann lösbar ist, wenn $y \in \pi_{\mathbb{R}^n}(S_k)$ ist. Insbesondere existiert ein semidefinites Programm, sodass die Lösungsmenge des Programms den Spektraeder S_k bildet. \square

Beweis. Zunächst geben wir für alle $y \in \mathbb{R}^n$ ein semidefinites Programm $(SP(y))$ an, sodass die folgenden Aussagen äquivalent sind:

- (a) $y \in \pi_{\mathbb{R}^n}(S_k)$,
- (b) Es existiert eine Fortsetzung $\tilde{y} = (\tilde{y}_b)_{b \in \Theta_{2k}}$ von y mit $\tilde{y}_{1+\mathcal{J}_V} = 1$, $\tilde{y}_{X_1+\mathcal{J}_V} = y_1, \dots, \tilde{y}_{X_n+\mathcal{J}_V} = y_n$ und $\mathcal{M}_{\Theta_k}(\tilde{y}) \geq 0$,
- (c) Das Programm $(SP(y))$ ist lösbar.

Das Ziel ist es, die Momentmatrix zu einer Fortsetzung von y nach (b) als Lösung von $(SP(y))$ zu schreiben. Lösungen von $(SP(y))$ seien also Matrizen $X \in \mathcal{S}_l$ mit $l := \#\Theta_k$. Die Anforderung an die Restriktionen ist, dass Lösungen Momentmatrizen sind. Die Variablen einer Parametrisierung der Momentmatrizen sind demnach gegeben durch die Basis Θ_{2k} . Klar ist, dass die Zielfunktion von $(SP(y))$ keine Rolle spielt und deshalb auf Null gesetzt werden kann. Nun geben wir einen Algorithmus zur Konstruktion der Restriktionsmatrizen an und zeigen, dass das resultierende semidefinite Programm das Gewünschte leistet.

Schritt 1: Restriktionsmatrizen für y .

Die ersten $n + 1$ Einträge der Momentmatrix einer Fortsetzung sind eindeutig durch y bestimmt. Wir setzen daher:

$$\begin{aligned} A_z &:= 1/2(E_{1,z} + E_{z,1}) \in \mathcal{S}_l \quad \text{und} \\ a_z &:= 1, \quad a_2 = y_1, \quad \dots, \quad a_{n+1} = y_n \end{aligned}$$

für $z = 1, \dots, n + 1$.

Schritt 2: Restriktionsmatrizen zu Beziehungen zwischen Basisvektoren.

Ist das Produkt zweier Basisvektoren aus Θ_k reduzierbar, ergibt dies eine Restriktion an die Momentmatrix. Ist das Produkt dagegen ein Basisvektor in Θ_{2k} , muss der Eintrag zum Produkt gleich dem Wert der Fortsetzung an diesem Basisvektor sein. In dem Fall, dass das Produkt zweier Basisvektoren b_1, b_2 aus Θ_k einen Basisvektor aus Θ_{2k} ergibt, ist es grundsätzlich möglich, dass zwei andere Basisvektoren b_3, b_4 mit $b_1 \neq b_3$ und $b_1 \neq b_4$ das gleiche Produkt ergeben. Dann gilt:

$$\mathcal{M}_{\Theta_k}(b_1, b_2) = \mathcal{M}_{\Theta_k}(b_3, b_4)$$

und wir sagen: b_1 und b_2 sind *doppelt*. Dies ergibt weitere Restriktionen, da die entsprechenden Einträge der Momentmatrix gleich sein müssen. Alle diese Restriktionen ermitteln wir schrittweise durch einen Algorithmus:

- (i) Setze $p = q = 1$.
- (ii) *Fall 1:* Es ist $\Theta_k(p) \cdot \Theta_k(q) \in \Theta_{2k}$, aber $\Theta_k(p)$ und $\Theta_k(q)$ sind nicht doppelt.

In diesem Fall gibt es keine neue Restriktion. Setze formal:

$$M_{p,q} := 0.$$

Fall 2: $\Theta_k(p)$ und $\Theta_k(q)$ sind doppelt.

Falls Indizes $p, q \in \{1, \dots, l\}$ existieren, sodass $p = p'$ und $q > q'$ gilt, oder sodass $p > p'$ gilt, und die Gleichung

$$\Theta_k(p) \cdot \Theta_k(q) = \Theta_k(p') \cdot \Theta_k(q') \in \Theta_{2k}$$

erfüllt ist, so setze:

$$M_{p,q} := E_{p,q} - E_{p',q'}.$$

Andernfalls setze formal $M_{p,q} := 0$.

Fall 3: Ist $\Theta_k(p) \cdot \Theta_k(q) \notin \Theta_{2k}$, so ist $\Theta_k(p) \cdot \Theta_k(q)$ reduzierbar. Es ist

$$\Theta_k(p) \cdot \Theta_k(q) = \sum_{b \in \Theta_{2k}} \lambda_{\Theta_k(p), \Theta_k(q)}^b \cdot b$$

für Koeffizienten $\lambda_{\Theta_k(p), \Theta_k(q)}^b \in \mathbb{R}$. Für $b \in \Theta_{2k}$ mit $\lambda_{\Theta_k(p), \Theta_k(q)}^b \neq 0$ existieren $p_b, q_b \in \{1, \dots, l\}$ mit $b = \Theta_k(p_b) \cdot \Theta_k(q_b)$. Setze:

$$M_{p,q} := -E_{p,q} + \sum_{b \in \Theta_{2k}} \lambda_{\Theta_k(p), \Theta_k(q)}^b E_{p_b, q_b}.$$

- (iii) Im Fall $p = q = l$ ist der Algorithmus beendet. Andernfalls setze $p' := p$ und $q' := q + 1$, falls $q < l$, und $p' := p + 1$ und $q' := 1$, falls $q = l$ gilt, und fahre mit den neuen Werten mit (ii) fort.

Wir definieren:

$$\begin{aligned} (SP(y)) \quad & \max! \langle 0, X \rangle \\ & \text{mit } \langle A_1, X \rangle = a_1, \dots, \langle A_{n+1}, X \rangle = a_{n+1}, \\ & \langle 1/2(M_{p,q} + M_{p,q}^t), X \rangle = 0 \text{ für alle } p, q \in \{1, \dots, l\} \text{ und} \\ & X \geq 0. \end{aligned}$$

Behauptung: Die Projektion der Lösungsmenge von $(SP(y))$ auf \mathbb{R}^n wird durch alle Tensoren $y \in \mathbb{R}^n$, die die obige Äquivalenz erfüllen, gebildet.

Beweis: Dies wird im Wesentlichen an der Konstruktion von $(SP(y))$ deutlich. Wir bemerken noch, dass für alle $p, q \in \{1, \dots, l\}$ und $X \in \mathcal{S}_l$ gilt:

$$\sum_{i,j=1}^n (M_{p,q})_{i,j} X_{i,j} = \langle 1/2(M_{p,q} + M_{p,q}^t), X \rangle,$$

da X symmetrisch ist. ◇

Verzichten wir auf die Restriktionen A_2, \dots, A_{n+1} , so erhalten wir ein semidefinites Programm, welches die zweite Behauptung erfüllt. ■

Beispiel 7.1.3 Die Konstruktion der Restriktionsmatrizen wird an der in 4.3.4 angegebenen Momentmatrix \mathcal{M}_{Θ_2} deutlich. Es sei $k = 2$ und ein semidefinites

Programm zu einem Tensor in $\mathbb{R}^2 \otimes \mathbb{R}^2$ wie im Beweis zu Satz 7.1.2 gebildet. Dann sind

$$(ab, ac, b^2, bc, bd, c^2, cd, d^2)$$

variabel. Beispielsweise ist

$$A_2 = \frac{1}{2}(E_{1,2} + E_{2,1}).$$

Da $\Theta_2(1) \cdot \Theta_2(6) = ab = \Theta_2(2) \cdot \Theta_2(3)$, gilt nach Konstruktion (Fall 2):

$$M_{1,6} = 0 \quad \text{und} \quad M_{2,3} = E_{2,3} - E_{1,6}.$$

Weiterhin ist $\Theta_2(3) \cdot \Theta_2(9) = b^2c = \Theta_2(4) \cdot \Theta_2(8)$ (ebenfalls Fall 2). Somit gilt:

$$M_{3,9} = 0 \quad \text{und} \quad M_{4,8} = E_{4,8} - E_{3,9}.$$

Da die Reduktion von $d \cdot ab = abd$ gleich b^2c ist (Fall 3), können wir

$$M_{5,6} = -E_{5,6} + E_{4,8}$$

setzen. Es ist $a \cdot a = a^2$ kongruent zu $1 - b^2 - c^2 - d^2$ (Fall 3). Also erhalten wir beispielsweise:

$$M_{2,2} = -E_{2,2} + E_{1,1} - E_{3,3} - E_{4,4} - E_{5,5}.$$

Wir sehen anhand dieser Beispiele, dass die Restriktionen alle Beziehungen zwischen den Variablen berücksichtigen. □

7.2 „Pinorm“ - Ein Programm zur Berechnung von Thetanormen

Das Programm PINORM besteht aus in MATLAB ausführbaren Skripten des Datenformats *.m*. Es besitzt mehrere Routinen, die auf den Hauptroutinen MAIN_1.m und MAIN_2.m basieren, und einigen Hilfsfunktionen. Nach rechenintensiven Schritten ist eine Zwischenspeicherung der Daten möglich. Die wesentlichen Schritte sind ausführlich kommentiert. Damit sollte es möglich sein, sich rasch einzufinden.

Die Zwischenschritte zur Berechnung der Thetanormen

Das Programm PINORM folgt in seinem Aufbau diesen Schritten:

- (1) Aufstellen des Verschwindeideals $\mathcal{J}_V \subseteq \mathbb{R}[X_1, \dots, X_n]$, wobei $n := n_1 \cdots n_r$ ist, mittels des Determinantenkriteriums Satz 5.3.5.
- (2) Berechnung der Gröbnerbasis G von \mathcal{J}_V zur graduierten lexikographischen Ordnung.
- (3) Ermittlung der Standardbasis Θ_k von $\mathbb{R}[X_1, \dots, X_n]_k / \mathcal{J}_V$ für G und einen festen Wert $k \geq 1$.
- (4) Aufstellen der Momentmatrix \mathcal{M}_{Θ_k} und der Momentmatrix $\mathcal{M}_{\Theta_k}(\tilde{z})$ zu Fortsetzungen \tilde{z} von Tensoren $z \in V$.
- (5) Aufstellen der Restriktionsmatrizen für das im Beweis von Satz 7.1.2 beschriebene semidefinite Programm.
- (6) Berechnung der k -ten Thetanorm von $y \in V$ durch Skalierung und anschließender Überprüfung der Fortsetzbarkeit zu einer positiv semidefiniten Momentmatrix mittels semidefiniter Programmierung.

Mittels der Hauptroutine `MAIN_1.m` werden die Schritte (1) bis (5) und alle späteren Schritte mittels `MAIN_2.m` durchgeführt. Neben den Hauptroutinen stehen auch einige Routinen für spezielle Berechnungen bereit.

Im Folgenden beschreiben wir die Funktionsweise dieser Routinen. Zur Illustration geben wir beispielhafte Werte an, die sich an Beispiel 4.3.4 anlehnen.

Die Eingabewerte und der Ausgabewert

Funktion	Variable	Beispielwert	Entsprechung	Datentyp
Tensorprodukt	V	[2 2]	$V = \mathbb{R}^2 \otimes \mathbb{R}^2$	array
Thetakörper	K	2	$k = 1$	integer
Tensor	y	[1 0 0 1]	$y = e_1 \otimes e_1 + e_2 \otimes e_2$	array

Die boolsche Variable `ja` gibt an, ob eine Ausgabe in das „Command Window“ gewünscht wird, und durch die Belegung von `gen` ist eine Steuerung der Genauigkeit der SDP-Routine `SDPT3` möglich. Voreingestellt ist `gen = 10^(-12)`.

Der Ausgabewert ist `normy`. Er gibt die k -te Thetanorm von y an.

Die Durchführung der Zwischenschritte

Hier stellen wir die Funktionen vor, mit denen die einzelnen Schritte durchgeführt werden können und auf die die Hauptroutinen zugreifen.

A_1_determinanten.m. Aufstellen des Verschwindeideals der Einheitsproduktvektoren. Dabei sind die Variablen invers lexikographisch geordnet.

Eingabewerte: V, ja.

Ausgabewerte:

Funktion	Variable	Beispiel	Datentyp
Determinanten und Normierungspolynom	p	$\{x_{11}x_{22} - x_{12}x_{21}, x_{11}^2 + x_{12}^2 + x_{21}^2 + x_{22}^2 - 1\}$	array, sym
Variablen	Va	$\{x_{11}, x_{12}, x_{21}, x_{22}\}$	cell array, char

Werte zu den obigen Beispielen sind:

```
p = [ poly(x11*x22 - x12*x21, [x11, x12, x21, x22]),
      poly(x11^2 + x12^2 + x21^2 + x22^2 - 1, [x11, [...] ])],
Va = {'x11' 'x12' 'x21' 'x22'}.
```

A_2_groebner.m. Mittels der Funktion `groebner::gbasis`, die in MUPAD bereitgestellt wird, berechnen wir die Gröbnerbasis von p. Diese Funktion ist sehr rechenintensiv, wenn die Anzahl der Variablen groß wird. Werte für die Größe der Gröbnerbasis in Abhängigkeit von dieser Anzahl liefert Beispiel 5.3.10.

Eingabewerte: V, p, ja.

Ausgabewert:

Funktion	Variable	Beispiel	Datentyp
Gröbnerbasis	GB	$\{x_{11}^2 + x_{12}^2 + x_{21}^2 + x_{22}^2 - 1, x_{11}x_{22} - x_{12}x_{21}, x_{11}x_{12}x_{21} + x_{12}^2x_{22} + x_{21}^2x_{22} + x_{22}^3 - x_{22}, x_{12}^2x_{21}^2 + x_{12}^2x_{22}^2 + x_{21}^2x_{22}^2 + x_{22}^4 - x_{22}^2\}$	wie p

A_3_momentmatrix.m. Aufstellen der Momentmatrix des k -ten Thetakörpers in Basisdarstellung und in Restriktionsform für die semidefinite Programmierung zur Standardbasis Θ .

Eingabewerte: V, K, GB, Va, ja.

Ausgabewerte:

Funktion	Var.	Datentyp	Größe
Basismonome bis zum Grad k	BK	matrix	$t_1 \times n$
Basismonome bis zum Grad $2k$	B2K	matrix	$t_2 \times n$
Positionen Basismonome in Momentmatrix	POS	cell array	$t_2 \times 1$
Koeffizientenmatrizen (Momentmatrix)	MBK	matrix	$t_1 \times t_1 \times t_2$
Reduktions-Restriktionen (SDP)	MBL	matrix	$t_1 \times t_1 \times [\dots]$
Restriktionen für gleiche Produkte (SDP)	MBM	matrix	$t_1 \times t_1 \times [\dots]$

Einträge von Matrizen haben den Datentyp „double“ und der Datentyp der Einträge von POS ist „array“. Es ist $t_1 := \#\Theta_k$ und $t_2 := \#\Theta_{2k}$.

Die Basismonome bis zum Grad $2k$ sind in den Matrizen BK und B2K codiert. Jede Zeile steht für ein Basismonom. Jede Spalte steht für eine Variable, von oben nach unten nach dem Grad geordnet. Die Einträge stehen für die Exponenten. Für die Ausgabe werden die Matrizen transponiert. Beispielsweise werden Θ_1 und Θ_2 durch die folgenden Matrizen repräsentiert:

$$\begin{array}{l}
 \text{BK} = \begin{array}{cccccc} 0 & 1 & 0 & 0 & 0 & \\ 0 & 0 & 1 & 0 & 0 & \\ 0 & 0 & 0 & 1 & 0 & \\ 0 & 0 & 0 & 0 & 1 & \end{array} \quad
 \text{B2K} = \begin{array}{cccccccccccc} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 2 & 1 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 2 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 2.
 \end{array}
 \end{array}$$

Die Momentmatrix ist in der dreistufigen Matrix MBK codiert. Jede Ebene repräsentiert die Koeffizientenmatrix zu einem Basisvektor aus Θ_{2k} . In unserem Beispiel gehören zu den Basismonomen $1, x_{11}, x_{12}^2$ und $x_{12}x_{21} \in \Theta_2$ die folgenden Koeffizientenmatrizen der Momentmatrix \mathcal{M}_{Θ_1} :

$$\begin{array}{l}
 \text{MBK}(:, :, 1) = \begin{array}{ccccc} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \quad
 \text{MBK}(:, :, 2) = \begin{array}{ccccc} 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \\
 \\
 \text{MBK}(:, :, 8) = \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \quad
 \text{MBK}(:, :, 9) = \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0. \end{array}
 \end{array}$$

Die Matrizen MBL und MBM für die semidefinite Programmierung folgen in ihrem Aufbau den Restriktionsmatrizen, die zum Beweis von Satz 7.1.2 konstruiert wurden. Die Matrix MBM gehört zu Restriktionen des Typs, die im Fall 2 auftreten. In unserem Beispiel tritt Fall 2 nicht auf, also ist MBM dann leer. Fall 3 wird durch die Matrix MBL abgedeckt. Diese enthält die Restriktionen, die durch Reduktion von Produkten aus Basisvektoren gebildet werden. Hier besteht MBL nur aus zwei Ebenen, da $x_{11} \cdot x_{11}$ und $x_{11} \cdot x_{22}$ die einzigen Produkte von Basismonomen in Θ_1 sind, die reduzierbar sind:

$$\begin{array}{rcl} \text{MBL}(:, :, 1) & = & \begin{array}{ccccc} 2 & 0 & 0 & 0 & 0 \\ 0 & -2 & 0 & 0 & 0 \\ 0 & 0 & -2 & 0 & 0 \\ 0 & 0 & 0 & -2 & 0 \\ 0 & 0 & 0 & 0 & -2 \end{array} & \text{MBL}(:, :, 2) & = & \begin{array}{ccccc} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & -1 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array} \end{array}$$

Wir beachten, dass die Formulierung des semidefiniten Programms an die für SDPT3 vorgesehene angepasst werden muss. Das bedeutet insbesondere, dass Ebenen in MBL jeweils aus oberen rechten Dreiecksmatrizen bestehen und die Hauptdiagonalen mit zwei multipliziert werden müssen.

Die Matrix POS gibt für jedes Monom aus Θ_{2k} an, welche Positionen oben rechts in der Momentmatrix ausschließlich von ihm besetzt werden. Nach Beispiel 4.3.4 ist für $k = 1$:

$$\text{POS}\{1\} = [1 \ 1] \quad \text{POS}\{2\} = [1 \ 2] \quad \text{POS}\{6\} = [2 \ 3].$$

Setzen wir $k = 2$, so ist $x_{11}x_{12} = x_{11} \cdot x_{12} = 1 \cdot x_{11}x_{12}$ und damit

$$\text{POS}\{6\} = [2 \ 3 \ 1 \ 6].$$

A_3_momentmatrix_sp.m. Der Unterschied dieser Routine zur vorigen ist, dass die Matrizen MBK, MBL und MBM im Datenformat „sparse“ vorliegen. Dieses Format erlaubt einen performanteren Umgang mit Matrizen, deren Einträge überwiegend verschwinden. Einträge, die von null verschieden sind, werden als Tripel gespeichert:

$$A = [1, 0; 0, -6; 0, 0] \quad \text{sparse}(A) = \begin{array}{ll} (1,1) & 1 \\ (2,2) & -6. \end{array}$$

Da es kein „sparse“-Format für dreistufige Matrizen gibt, werden die obigen Matrizen folgendermaßen in zweistufige konvertiert:

MBK: Vertikale Reihung der Ebenen, beginnend mit der ersten Ebene. Dies ergibt eine $(t_1 \cdot t_2) \times t_1$ -Matrix. Die ersten zwei Ebenen unseres Beispiels sehen so aus:

$$\begin{aligned} \text{MBK}(1:10, 1:5) = & \begin{pmatrix} (1,1) & 1 \\ (7,1) & 1 \\ (2,2) & 1 \\ (6,2) & 1. \end{pmatrix} \end{aligned}$$

MBL und MBM: Zunächst wird jede Restriktionsmatrix in einen Vektor konvertiert, indem die Indizes der rechten oberen Dreiecksmatrix von links nach rechts und von oben nach unten spaltenweise linearisiert werden. Dabei wird jeder Eintrag auf der Diagonale (wie oben) mit zwei und alle anderen Einträge mit $\sqrt{2}$ multipliziert. Danach werden die Restriktionsmatrizen beginnend mit der ersten Restriktion horizontal aneinandergereiht. Dies ergibt jeweils eine $(1/2 \cdot t_1 \cdot (t_1 + 1)) \times [\dots]$ -Matrix. Zum Beispiel ist MBL eine 15×2 -Matrix:

$$\begin{aligned} \text{MBL} = & \begin{pmatrix} (1,1) & 2 \\ (3,1) & -2 \\ (6,1) & -2 \\ (10,1) & -2 \\ (15,1) & -2 \\ (9,2) & \text{sqrt}(2) \\ (12,2) & -\text{sqrt}(2). \end{pmatrix} \end{aligned}$$

Die Multiplikation der Einträge mit Konstanten hat den folgenden Grund: In SDPT3-4.0 werden symmetrische Matrizen $X \in \mathcal{S}_l$ mit ihrer Linearisierung

$$\text{svec}(X) := (X_{11}, \sqrt{2} \cdot X_{1,2}, \sqrt{2} \cdot X_{2,2}, \dots, \sqrt{2} \cdot X_{l-1,l}, X_{l,l})$$

identifiziert, wobei die Einträge, die nicht auf der Diagonalen stehen, mit $\sqrt{2}$ multipliziert werden. Dann gilt für zwei symmetrische Matrizen X, \tilde{X} :

$$\langle X, \tilde{X} \rangle = \langle \text{svec}(X), \text{svec}(\tilde{X}) \rangle.$$

Die Multiplikation der Diagonalen mit zwei erklärt sich aus der Symmetrisierung der Restriktionsmatrizen.

A_4_thetakoerper_sdp.m. Validierung, ob ein gegebener Tensor im projizierten Spektraeder S_k enthalten ist oder nicht, über das semidefinite Programm zu den

erstellten Restriktionsmatrizen.

Eingabewerte: **y**, **V**, **MM**, **lk**, **ja**.

In **MM** werden die Matrizen **MBL** und **MBM** zusammengefasst, also je nach Datenformat in der zweiten oder dritten Dimension aneinandergereiht. Der nächste Eingabeparameter **lk** steht für die Anzahl der Elemente in Θ_1 , genauer, für **size(BK,1)**.

Ausgabewerte: Die boolesche Variable **jaa** gibt an, ob der Tensor **y** im projizierten Spektraeder enthalten ist oder nicht.

Funktion	Variable	Datentyp	Größe
Momentmatrix zu einer Fortsetzung	X	matrix, double	$t_1 \times t_1$

Mit den obigen Daten erhalten wir: **jaa** = 1, das heißt, $e_1 \otimes e_1 + e_2 \otimes e_2$ ist nicht im ersten Thetakörper enthalten. Mit **y** = 0.5*[1 0 0 1] erhalten wir dagegen

```
X = 1.000    0.500    0.000    0.000    0.500
      0.500    0.375    0.000    0.000    0.125
      0.000    0.000    0.125    0.125    0.000
      0.000    0.000    0.125    0.125    0.000
      0.500    0.125    0.000    0.000    0.375.
```

Diese Matrix ist eine positiv semidefinite Momentmatrix zur Fortsetzung

$$(1, 1/2, 0, 0, 1/2, 0, 0, 1/8, 1/8, 0, 1/8, 0, 3/8)$$

von $(1/2, 0, 0, 1/2)$.

A_5_thetanorm.m. Berechnung des Minkowskifunktional zu S_k über ein Intervallhalbierungsverfahren.

Eingabewerte: **y**, **V**, **lk**, **MM**, **gen**, **a**, **b**.

Mit den Faktoren **a** und **b** beginnt das Intervallhalbierungsverfahren. Sie dürfen nicht negativ sein und sollten so gewählt sein, dass **a** < **b** gilt und **a*y** im projizierten Spektraeder liegt, **b*y** aber nicht. Sonst werden sie automatisch belegt.

Ausgabewerte: Es ist **X** wie oben eine positive Momentmatrix zu einer Fortsetzung von **t1*y**.

Funktion	Variable	Bedeutung
Untere Grenze	th1	Es ist th1*y fortsetzbar
Obere Grenze	th2	Es ist th2*y nicht fortsetzbar und th2-th1 < gen
Thetanorm	normy	normy = $(1/th1 - 1/th2)/2$

Mit den obigen Daten erhalten wir X wie oben und

`th1 = 0.5000` `th2 = 0.5000` `normy = 1.9999.`

Hinweise zur Benutzung des SDP-Solvers

Zur Benutzung des Solvers SDPT3-4.0 muss der Ordner „SDPT3-4.0“ dem „Current Directory“ hinzugefügt werden, zum Beispiel über „Current Folder → Add to path → Selected Folders and Subfolders“. Informationen zum Aufbau und zum Gebrauch von SDPT3-4.0 entnehmen wir der Dokumentation <http://www.math.nus.edu.sg/~mattohkc/sdpt3/guide4-0-draft.pdf>, oder, für den speziellen Gebrauch, dem Kommentarteil von `A_4_thetakoerper_sdp.m`.

Nützliche Funktionen

`vectomat.m` konvertiert einen Tensor in eine mehrdimensionale Matrix.

`isproductvector.m` prüft, ob ein Tensor ein Produktvektor ist.

`pinorm.m` berechnet die Pinorm von Tensoren eines zweifachen Tensorprodukts.

8 Fazit und Ausblick

Im Fall zweifacher Tensorprodukte ist es uns gelungen, die Einheitssphäre der projektiven Norm durch den ersten Thetakörper zum Ideal, welches von den Determinanten und dem Normierungspolynom erzeugt wird, auszudrücken. Den allgemeinen Fall für Tensorprodukte $\mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_r}$, wobei $r, n_1, \dots, n_r \geq 2$ natürliche Zahlen sind, haben wir zunächst numerisch behandelt. Es liegt die Frage nahe, ob hier auch ein ähnliches konkretes Ergebnis erzielt werden kann. Dem interessierten Leser möchten wir einige Hinweise geben.

Der allgemeine Fall - konkret Kapitel 6 illustriert, dass das Verständnis der Geometrie der Einheitssphäre der projektiven Norm wesentlich dazu beiträgt, die Annullierungsmengen von Funktionalen, die Summen von Quadraten bis auf einen Rest sind, zu berechnen. Bei der Behandlung des multipartiten Falls kann dies sich auch als nützlich herausstellen. Dabei ist Folgendes zu beachten:

- (i) Im bipartiten Fall haben die maximalen Seiten von $\mathcal{B}_{1,\pi}$ eine einheitliche Gestalt. Im multipartiten Fall ist allein die Bestimmung des inneren Radius und damit auch der maximalen Vektoren eine Herausforderung. Entsprechend ist das Wissen über die maximalen Seiten gering. Wir vermuten, dass es verschiedene Klassen von maximalen Seiten gibt, deren Anzahl proportional von r abhängt.
- (ii) Im Allgemeinen werden nicht alle maximalen Seiten von einem maximalen Vektor induziert und ein skaliertes maximaler Vektor ist kein innerer Punkt seiner induzierten Seite.

Wir erwähnen nun einige Ansätze, die es erleichtern, die Geometrie der Einheitssphäre $\mathcal{B}_{1,\pi}$ oder ihrer Polaren zu umreißen.

- (i) Falls ein innerer Punkt einer Seite $S \subsetneq \mathcal{B}_{1,\pi}$ ein Randpunkt des ersten Thetakörpers \mathcal{T}_1 ist, folgt nach Lemma 8.0.1, dass S Teilmenge des Randes von \mathcal{T}_1 ist. Kandidaten für solche inneren Punkte sind Vektoren, deren projektive Norm bekannt ist.
- (ii) Ein weiterer Ansatz ist, die Funktionale, die einen Randpunkt der Einheitssphäre annullieren, genauer zu untersuchen. Wann sind sie

- eine Summe von Quadraten modulo dem Verschwindeideal? Es bietet sich hierfür eine exakte Darstellung der durch maximale Vektoren erzeugten Funktionale an, da dies im bipartiten Fall zielführend war.
- (iii) Vermutlich sind maximale Vektoren dadurch gekennzeichnet, dass die Determinanten aus Satz 5.3.5 an ihnen maximale Werte erzielen, was sich in der Struktur der annullierenden Funktionale als Summe von Quadraten niederschlägt.
 - (iv) Hilfreich ist die Bestimmung der Produktvektoren, die in der maximalen Seite zu einem maximalen Vektor ξ liegen, und des Stabilisators von ξ .
 - (v) Darüber hinaus könnte es sinnvoll sein, Sos-Polynome mit Positivität in Verbindung zu bringen, was wir es bereits in Kapitel 4 versucht haben.
 - (vi) Nach Proposition 3.1.8 sind Thetakörper semialgebraische Mengen. Welche Polynome sind hier bestimmend?

Lemma 8.0.1 - Konvexe Obermengen und innere Punkte

Seien A und B zwei kompakte konvexe Teilmengen von \mathbb{R}^n mit $A \subseteq B$ und $S \subseteq A$ eine echte Seite von A . Dann gilt: Schneidet der Rand von B das relative Innere von S , so ist S Teilmenge des Randes von B . \square

Beweis. Es sei $\xi \in S$ ein innerer Punkt von S . Falls S aus nur einem Element besteht, ist die Aussage wahr. Andernfalls existiert ein weiteres Element $\eta \in S$, sodass $\xi \neq \eta$ ist. Die Menge $I := \{\lambda \in \mathbb{R} \mid \lambda(\eta - \xi) + \xi \in S\}$ ist ein kompaktes Intervall mit $0 \in \text{in}(I)$. Das Intervall

$$I_A := \{\lambda \in \mathbb{R} \mid \lambda(\eta - \xi) + \xi \text{ ist ein Randpunkt von } B\}$$

ist eine abgeschlossene Teilmenge von I . Da $0 \in I_A$, ist I_A nicht leer. Da S eine echte Seite von A ist, existiert ein Vektor $0 \neq v \in \mathbb{R}^n$, sodass $\lambda(\eta - \xi) + \xi + \kappa v \notin S$ für alle $\kappa > 0$ und für alle $\lambda \in I$ gilt und die Funktion

$$\begin{aligned} f: I &\rightarrow \mathbb{R} \\ \lambda &\mapsto \sup\{\kappa \geq 0 \mid \lambda(\eta - \xi) + \xi + \kappa v \in B\} \end{aligned}$$

stetig, positiv und konvex ist.

Behauptung: Das Innere von I enthält keine isolierten Punkte von I_A .

Beweis: Angenommen, $\zeta \in I_A$ ist ein solcher isolierter Punkt, dann existiert ein Faktor $\varepsilon > 0$, sodass $\zeta(\eta - \xi) + \xi$ der einzige Randpunkt von B auf der

Verbindungsstrecke zwischen $(-\varepsilon + \zeta)(\eta - \xi) + \xi$ und $(\varepsilon + \zeta)(\eta - \xi) + \xi$ ist. Es ist also $f((-\varepsilon + \zeta, \varepsilon + \zeta) \setminus \{\zeta\}) > 0$. Mit $m := \min(f(-\varepsilon/2 + \zeta), f(\varepsilon/2 + \zeta)) > 0$ ist

$$0 = f(\zeta) = f\left(\frac{1}{2}\left(-\frac{\varepsilon}{2} + \zeta\right) + \frac{1}{2}\left(\frac{\varepsilon}{2} + \zeta\right)\right) < m \leq \frac{1}{2}f\left(-\frac{\varepsilon}{2} + \zeta\right) + \frac{1}{2}f\left(\frac{\varepsilon}{2} + \zeta\right),$$

was ein Widerspruch zur Konvexität von f ist. \diamond

Behauptung: Das Innere von I enthält keine Randpunkte von I_A .

Beweis: Es sei $\zeta \in I_A$ ein Randpunkt. Dann existieren Faktoren $\varepsilon > 0$ und $\delta > 0$, sodass ohne Beschränkung der Allgemeinheit $f(-\varepsilon + \zeta) > 0$ und $f(\delta + \zeta) = 0$ gilt. Sei nun $\lambda \in (0, 1)$ mit $-\lambda\varepsilon + (1 - \lambda)\delta = 0$, dann ist

$$0 = f(\zeta) = f(\lambda(-\varepsilon + \zeta) + (1 - \lambda)(\delta + \zeta)) < \lambda f(-\varepsilon + \zeta) + (1 - \lambda)f(\delta + \zeta),$$

was ein Widerspruch zur Konvexität von f ist. \diamond

Damit stimmen I und I_A überein. Da η beliebig gewählt war, kann auf diese Weise ganz S ausgeschöpft werden. \blacksquare

Der allgemeine Fall - numerisch Um den Algorithmus für PINORM effizienter zu gestalten, bietet sich eine Strukturanalyse der Gröbnerbasis und der Momentmatrizen an. Die Determinanten, die das Verschwindeideal der Produktvektoren erzeugen, bilden eine Gröbnerbasis. Da das Normierungspolynom symmetrisch ist und die Festlegung einer Ordnung auf den Variablen dieser Symmetrie gegenläufig ist, wird eine Gröbnerbasis des durch die Produkteinheitsvektoren erzeugten Ideals wesentlich größer. Dies zeigt bereits das einfache Beispiel 1.2.7. Den Nachteilen durch eine aufwändigere Bestimmung steht der Vorteil einer kürzeren Standardbasis gegenüber. Vielleicht ist es möglich, zunächst mit den Determinanten zu arbeiten und die Normierung später einfließen zu lassen, auch im Hinblick auf eine mögliche Vereinfachung der Momentmatrizen.

Komplexe Tensorprodukte Wie verallgemeinern wir das Resultat auf Tensorprodukte über den komplexen Zahlen? Durch eine geschickte Umformulierung des Problems könnte dieser Fall aus dem reellen folgen.

Die Einheitsphäre als Mannigfaltigkeit Hier haben wir die Einheitsphäre der projektiven Norm im Allgemeinen und die Menge der Produktvektoren im Speziellen algebraisch betrachtet. Es ist auch möglich, diese beiden Mengen jeweils in ihrer Eigenschaft als Mannigfaltigkeit zu untersuchen. Beispielsweise bilden die Einheitsproduktvektoren in $\mathbb{R}^2 \otimes \mathbb{R}^2$ den sogenannten *Clifford-Torus*, welcher im Sinne der Riemannschen Geometrie in der dreidimensionalen Sphäre flach ist.

Literaturverzeichnis

- [Arv] ARVESON, William: *Maximal vectors in Hilbert space and quantum entanglement*. Journal of Functional Analysis 256, 1476-1510 (2009).
- [Axi] AXIOM. *The Scientific Computation System*. <http://axiom-developer.org/>, Version vom 16. Februar 2015.
- [BCR] BOCHNAK, Jacek; COSTE, Michel; ROY, Marie-Françoise: *Real Algebraic Geometry*. Springer-Verlag, Berlin Heidelberg 1998.
- [BPT] BLEKHERMAN, Grigoriy; PARRILO, Pablo A.; THOMAS, Rekha R. (Hrsg.): *Semidefinite Optimization and Convex Algebraic Geometry*. Cambridge University Press, Cambridge 2013.
- [Bro] BROKATE, Martin: *Konvexe Analysis*. Manuskript zur Vorlesung, München 2008. http://www-m6.ma.tum.de/~brokate/con_ss08.pdf, Version vom 16. Februar 2015.
- [CLS] COX, David; LITTLE, John; O'SHEA, Donal: *Ideals, Varieties, and Algorithms. An Introduction to Computational Algebraic Geometry and Commutative Algebra*. Springer-Verlag, New York 2008.
- [DGPS] DECKER, Wolfram; GREUEL, Gert-Martin; PFISTER, Gerhard; SCHÖNEMANN, Hans: SINGULAR 3-1-6. *A computer algebra system for polynomial computations*. Kaiserslautern 2012. <http://www.singular.uni-kl.de>, Version vom 16. Februar 2015.
- [GaMa] GÄRTNER, Bernd; MATOUŠEK, Jiří: *Approximation Algorithms and Semidefinite Programming*. Springer-Verlag, Berlin Heidelberg 2012.
- [Gra] GRÄBE, Hans-Gert: CALI, *A REDUCE Package for Commutative Algebra, Version 2.2.1*. Leipzig 1995. <http://www.reduce-algebra.com/docs/cali.pdf>, Version vom 16. Februar 2015.
- [GSM] GRAYSON, Daniel R.; STILLMAN, Michael E.: MACAULAY2, *A software system for research in algebraic geometry*. 2014. <http://www.math.uiuc.edu/Macaulay2/>, Version vom 16. Februar 2015.

-
- [Har] HARTSHORNE, Robin: *Algebraic Geometry*. Springer-Verlag, New York 1997.
- [Hul] HULEK, Klaus: *Elementare algebraische Geometrie*. Verlagsgesellschaft Vieweg & Sohn, Braunschweig/Wiesbaden 2000.
- [HuWi] HUPPERT, Bertram; WILLEMS, Wolfgang: *Lineare Algebra*. Teubner-Verlag, Wiesbaden 2006.
- [Net] NETZER, Tim: *Reelle algebraische Geometrie 1 & 2*. Manuskript zur Vorlesung, Leipzig 2013. http://tu-dresden.de/die_tu_dresden/fakultaeten/fakultaet_mathematik_und_naturwissenschaften/fachrichtung_mathematik/institute/geometrie/mitarbeiter/netzer/pdf/RAG.pdf, Version vom 16. Februar 2015.
- [Par] PARTHASARATHY, K. R.: *On the maximal dimension of a completely entangled subspace for finite level quantum systems*. New Delhi 2004. <http://arxiv.org/pdf/quant-ph/0405077v1.pdf>, Version vom 16. Februar 2015.
- [Roc] ROCKAFELLAR, R. Tyrrell: *Convex Analysis*. Princeton University Press, Princeton 1970.
- [Ryan] RYAN, Raymond A.: *Introduction to Tensor Products of Banach Spaces*. Springer-Verlag, London 2002.
- [Sage] SAGE. Open-Source-Mathematiksystem. <http://www.sagemath.org/>, Version vom 16. Februar 2015.
- [Sch] SCHNEIDER, Rolf: *Konvexgeometrie*. Manuskript zur Vorlesung, Freiburg 2005. <http://home.mathematik.uni-freiburg.de/rschnei/Konvexg.15.02..pdf>, Version vom 16. Februar 2015.
- [Tak] TAKESAKI, Masamichi: *Theory of Operator Algebras 1*. Springer-Verlag, Berlin Heidelberg New York 2001.
- [Toh] TOH, Kim-Chuan: *SDPT3, A MATLAB software for semidefinite-quadratic-linear programming*. Singapur 2009. <http://www.math.nus.edu.sg/~mattokkc/sdpt3.html>, Version vom 16. Februar 2015.
- [Wer] WERNER, Dirk: *Funktionalanalysis*. Springer-Verlag, Berlin Heidelberg 2011.
- [Zie] ZIEGLER, Günter M.: *Lectures on Polytopes*. Springer-Verlag, New York 1995.

Notationsverzeichnis

Konventionen

Die Menge der natürlichen Zahlen \mathbb{N} enthält die Null nicht. Ist die Null eingeschlossen, schreiben wir \mathbb{N}_0 . Falls nicht anders vermerkt, bezeichnen n, m, k, l, r und s natürliche Zahlen. Die Menge der rationalen (oder reellen) Zahlen, die nicht negativ sind, bezeichnen wir mit \mathbb{Q}_0^+ (oder mit \mathbb{R}_0^+).

Für eine natürliche Zahl n sei die Abbildung

$$\delta_n : \mathbb{N} \rightarrow \{0, 1\}, \quad m \mapsto \begin{cases} 1, & n = m \\ 0, & n \neq m \end{cases}$$

definiert.

Ist nichts anderes vermerkt, bezeichnet I eine beliebige Indexmenge, ansonsten ein Ideal. Das Symbol i bezeichnet ein Element einer Indexmenge.

Mit \mathbb{K} ist der Körper der reellen oder der komplexen Zahlen bezeichnet.

Sei M eine Menge. Die Anzahl der Elemente von M bezeichnen wir mit $\#M$. Eine Teilmenge T von M heißt *echt*, wenn $T \subsetneq M$ gilt. Die Aussage: „ $x, y \in M$ “ ist gleichbedeutend mit „ $x \in M, y \in M$ “. Ist $f : M \rightarrow N$ eine Abbildung zwischen zwei Mengen M und N und $A \subseteq M, B \subseteq N$, so definieren wir: $f(A) := \{f(x) \mid x \in A\}$ und $f^{-1}(B) := \{x \in M \mid f(x) \in B\}$.

Ist A eine Teilmenge einer Gruppe G , so bezeichnet $-A := \{-a \mid a \in A\} \subseteq G$ die Menge aller Elemente, deren Inverses in A liegt. Ist B eine weitere Teilmenge, bezeichnet $A + B := \{a + b \mid a \in A, b \in B\}$ die Summe aller Elemente in A und B , analog $A + g := \{a + g \mid a \in A\}$ für ein Element $g \in G$.

Ringe besitzen ein Einselement und sind kommutativ. Ist R ein Ring und F eine Familie von Elementen in R , dann wird das von F erzeugte Ideal mit $\langle F \rangle$ bezeichnet. Wird ein Ideal $I \subseteq R$ von F erzeugt, so ist F ein *Erzeugendensystem* von I . In der Literatur wird ein Erzeugendensystem oft *Basis* genannt, siehe beispielsweise [BPT].

Ist V ein Vektorraum über einem Körper K und $M \subseteq V$ eine Teilmenge, so bezeichnet

$$\text{span}_K(M) := \left\{ \sum_{i=1}^k \lambda_i m_i \mid \lambda_i \in K, m_i \in M \text{ für alle } i = 1, \dots, k \right\}$$

die *lineare Hülle* von M . Als *Funktional* bezeichnen wir eine Abbildung von V in seinen Skalarenkörper. Ein Funktional ist meist linear oder affin-linear. Die Menge der linearen Funktionalen bildet den algebraischen Dual von V und ist mit dem Symbol V' bezeichnet. Ist V von endlicher Dimension, werden Vektoren, soweit nicht anders angegeben, als Elemente in \mathbb{R}^n angesehen, und oft unterscheiden wir notationell nicht zwischen Vektoren und ihrer dualen Abbildung. Lineare Abbildungen zwischen \mathbb{R}^m und \mathbb{R}^n identifizieren wir mit ihren darstellenden Matrizen. Für eine Menge N bezeichnet das Symbol

$$\mathcal{M}_{n,m}(N)$$

die Menge der $n \times m$ -Matrizen mit Einträgen aus N . Das Transponieren einer Matrix wird durch ein hochgestelltes t ausgedrückt. Für $r \in \{1, \dots, n\}$ und $s \in \{1, \dots, m\}$ seien die *Matrixeinheiten* von $\mathcal{M}_{n,m}(\mathbb{R})$ mit

$$E_{r,s} := (\delta_i(r)\delta_j(s))_{i=1,\dots,n; j=1,\dots,m}$$

bezeichnet. Den Begriff *Orthonormalsysteme* kürzen wir mit *ONS* ab. Mit dem Symbol $\langle \cdot, \cdot \rangle$ bezeichnen wir das euklidische Skalarprodukt auf \mathbb{R}^n und mit $\|\cdot\|$ die davon induzierte Norm.

Die Abbildung $\pi_{\mathbb{R}^n}$ bezeichnet die orthogonale Projektion des Hilbertraums $\ell(\mathbb{N})$ der quadratsummierbaren Folgen auf die ersten n Koordinaten.

Ist X ein topologischer Raum und $M \subseteq X$ eine beliebige Teilmenge, ist mit $\text{cl}(M)$ den Abschluss von M und mit $\text{in}(M)$ das Innere von M in X bezeichnet.

Ist $(E, \|\cdot\|)$ ein normierter Raum, so bezeichnet $E_1 := \{e \in E \mid \|e\| \leq 1\}$ oder $\mathcal{B}_{1,\|\cdot\|}$ die Einheitskugel von E .

Die Junktoren Konjunktion und Disjunktion werden jeweils durch \wedge und \vee symbolisiert. Mit *entweder ... oder* bezeichnen wir die Kontravalenz.

Spezielle Notation

Die folgenden Einträge sind nach der Reihenfolge ihres Erscheinens sortiert.

1 Gröbnerbasen

K	Körper	1
$K[X_1, \dots, X_n]$	Polynomring über K in n Variablen	2
\geq_{lex}	Lexikographische Ordnung	2
$\mathcal{F}(\mathbb{N}_0)$	Raum der endlichen Folgen mit Werten in \mathbb{N}_0	2
\geq_{grlex}	Graduierte lexikographische Ordnung	2
f, g	Polynome	4
$\text{multideg}(f)$	Multigrad von f	4
$\text{deg}(f)$	Grad von f	4
$\text{LM}(f)$	Leitmonom von f	4
$\text{LC}(f)$	Leitkoeffizient von f	4
$\text{LT}(f)$	Leitterm von f	4
$ $	Teilbarkeitssymbol	5
G	Gröbnerbasis	7
\bar{f}^G	Rest der Division von f durch G	8
LCM	Kleinstes gemeinsames Vielfaches	9
$S(f, g)$	S-Polynom von f und g	9
I	Ideal in $K[X_1, \dots, X_n]$	14
$K[X_1, \dots, X_n]/I$	Koordinatenring	14
$\text{deg}(p + I)$	Grad von $p + I$	14
M	Teilmenge von $K[X_1, \dots, X_n]$	16
M_k	Elemente von M , deren Grad kleiner gleich k ist	16
$(M/I)_k$	Reduzierte Polynome in M/I , deren Grad kleiner gleich k ist	16
\mathcal{B}	Standardbasis für I und G	16
Θ	Theta-Basis für I	18

2 Reelle Algebraische Geometrie

A	Kommutativer Ring mit Eins	23
R	Reell abgeschlossener Körper	23
P	Kegel in A	23
$\mathcal{M}[(a_i)_{i \in I}]$	Erzeugter Monoid einer Familie $(a_i)_{i \in I} \subseteq A$	23
$\mathcal{K}_A, \Sigma A^2$	Kleinster Kegel von A	23
$\mathcal{K}[M]$	Erzeugter Kegel einer Teilmenge $M \subseteq A$	23
$\mathcal{K}[P, (a_i)_{i \in I}]$	Erzeugter Kegel von P und $(a_i)_{i \in I}$	23
$\text{supp}(P)$	Träger eines Primkegels P	26
(F, \leq)	Angeordneter Körper	26
K_P	Quotientenkörper von $A/\text{supp}(P)$	28
π, Π	Projektionen von A nach $A/\text{supp}(P)$ oder nach K_P	28
sign	Funktion, welche Elemente aus R auf ihr Vorzeichen abbildet	37
f_1, \dots, f_s	Polynome aus $R[X]$	37

I_k	Intervalle, welche zu Nullstellen von f_1, \dots, f_s gebildet werden	37
$\mathcal{S}(f_1, \dots, f_s)$	Signaturabbildung von f_1, \dots, f_s	37
$\mathcal{W}_{s,m}$	Disjunkte Vereinigung von Matrizenräumen	37
φ	Abbildung, die die Signaturabbildung rekonstruiert	40
$\mathcal{B}(X)$	Boolsche Polynomkombination in den Variablen X	41
$\mathcal{Z}(I)$	Verschwindemenge eines Ideals $I \subseteq R[X_1, \dots, X_n]$	46
$\mathcal{W}(P)$	Positivstellenmenge eines Kegels $P \subseteq R[X_1, \dots, X_n]$	46
$\mathcal{N}(M)$	Nichtnullmenge eines Monoids $M \subseteq R[X_1, \dots, X_n]$	46
$\mathcal{J}(V)$	Verschwindeideal einer Menge $V \subseteq R^n$	52
$\sqrt[R]{I}$	Reelles Radikal eines Ideals $I \subseteq A$	52
$\text{sper}(A)$	Reelles Spektrum von A	54
\hat{a}	Funktion, welche $P \in \text{sper}(A)$ auf $a + \text{supp}(P)$ abbildet ($a \in A$) . .	54
$\mathcal{V}(U)$	Verschwindemenge einer Teilmenge $U \subseteq A$	54
$\mathcal{W}(U)$	Positivstellenmenge einer Teilmenge $U \subseteq A$	54

3 Konvexe Geometrie

V	Vektorraum über \mathbb{R}	62
\mathcal{S}_n	Raum der symmetrischen Matrizen in $\mathcal{M}_n(\mathbb{R})$	62
\mathcal{S}_n^+	Raum der positiv semidefiniten Matrizen in $\mathcal{M}_n(\mathbb{R})$	62
\geq	Ordnung auf \mathcal{S}_n durch positiv semidefinite Matrizen	62
\mathcal{O}_n	Raum der orthogonalen Matrizen in $\mathcal{M}_n(\mathbb{R})$	62
$\text{ext}(C)$	Menge der Extrempunkte einer konvexen Menge $C \subseteq V$	62
$\text{co}(S)$	Konvexe Hülle von $S \subseteq V$	62
$\mathcal{K}((v_i)_{i \in I})$	Erzeugter Kegel einer Familie $(v_i)_{i \in I} \subseteq V$	69
\oplus	Symbol für die Bildung der direkten Summe	69
V	Lokalkonvexer Vektorraum über \mathbb{R}	70
\mathcal{P}	Familie von Halbnormen	70
$\mathcal{T}_{\mathcal{P}}$	Durch \mathcal{P} induzierte Topologie auf V	70
$U_{\varepsilon,p}(x)$	Element einer Umgebungsbasis von $\mathcal{T}_{\mathcal{P}}$ für $x \in V$ und $p \in \mathcal{P}$	70
V^*	Topologischer Dual von V	70
$\sigma(V^*, V)$	Schwache Topologie auf V^*	70
φ^*	Adjungierte zu $\varphi : V \rightarrow W$	70
L^\perp	Annihilator eines abgeschlossenen linearen Teilraums $L \subseteq V$	70
π_L	Projektion von V^* nach V^*/L^\perp	71
M^\star	Dualer Kegel zu $M \subseteq V$	71
V_M	Affine Hülle von M in V	73
$\text{relin}(M)$	Relatives Inneres von M	73
$\ell^2(\mathbb{N})$	Raum der reellwertigen quadratsummierbaren Folgen	75
$\mathcal{F}(\mathbb{N})$	Raum der reellwertigen finiten Folgen	75

4 Thetakörper

I	Ideal in $\mathbb{R}[X_1, \dots, X_n]$	81
\mathcal{J}_k	k -ter Thetakörper von I für $k \in \mathbb{N}$	82
\mathcal{K}	Kegel der quadratischen Polynome	84
\mathcal{K}^k	Kegel, von den Quadraten vom Grad kleiner gleich $2k$ erzeugt ...	84
$\mathcal{K}^k(I) =: C$	\mathcal{K}^k/I	84
$\mathcal{K}^{k,1}(I)$	Polynome, welche affin-linear und k -sos-mod I sind, modulo I ...	84
V	$\mathbb{R}[X_1, \dots, X_n]_{2k}/I$	85
L	$\mathbb{R}[X_1, \dots, X_n]_1/I$	85
v_φ	Darstellender Vektor von $\varphi \in L^*$	85
\mathcal{D}	Dualer Kegel von $C \cap L$ in L	86
$\hat{\mathcal{D}}$	Dualer Kegel von C in V	86
$\hat{\mathcal{D}}_A$	Elemente in $\hat{\mathcal{D}}$, die die Eins auf eins abbilden, auf \mathbb{R}^n projiziert ..	86
Θ	Theta-Basis für $\mathbb{R}[X_1, \dots, X_n]/I$	89
$[x]_{\Theta_k}$	Vektor, der alle Basiselemente aus Θ_k enthält	89
\mathcal{M}_{Θ_k}	Die k -te Momentmatrix	89
$\mathcal{M}_{\Theta_k}(y)$	Die k -te Momentmatrix zu $y = (y_b)_{b \in \Theta_{2k}}$	89
$\pi_{\mathbb{R}^n}$	Einschränkung von y auf den linearen Teilraum \mathbb{R}^n	89
V	Die kompakte Verschwindemenge $\mathcal{Z}(I) \subseteq \mathbb{R}^n$	92
K	Konvexe Hülle von V	92
\tilde{y}_k	Auswertungsfunktional auf $\mathbb{R}[X_1, \dots, X_n]_{2k}/I$, durch $y \in V$ induziert	93
$\mathcal{C}(X)$	Stetige reellwertige Funktionen auf einer kompakten Menge $X \subseteq \mathbb{R}^n$	94
$\rho(X)$	Menge der Zustände auf $\mathcal{C}(X)$	94
δ_y	Punktauswertung von Funktionen in $\mathcal{C}(X)$ an $y \in X$	94
φ_μ	Durch ein Wahrscheinlichkeitsmaß μ induzierter Zustand auf X ..	95

5 Mehrfache Tensorprodukte

V_1, \dots, V_m	Vektorräume	102
$\text{Mult}(V_1, \dots, V_m)$	Multilinearformen auf $V_1 \times \dots \times V_m$	102
$V_1 \otimes V_2 \otimes \dots \otimes V_m$	m -faches Tensorprodukt	102
$v_1 \otimes v_2 \otimes \dots \otimes v_m$	Produktvektor	102
$\mathcal{P}_{V_1 \otimes V_2 \otimes \dots \otimes V_m}$	Menge der Produktvektoren	102
$\iota, j, \beta, \tilde{\beta}$	Identifikationsabbildungen	102
E_1, \dots, E_m	Banachräume	106
$\mathcal{E}_{E_1 \otimes \dots \otimes E_m}$	Menge der Einheitsproduktvektoren	106
$\ \cdot\ _\pi$	Projektive Norm	106
$\ \cdot\ _\epsilon$	Injektive Norm	108
$\ \cdot\ _{\alpha^*}$	Duale Norm zu einer Norm $\ \cdot\ _{\alpha^*}$	108
$\mathcal{H}_1, \dots, \mathcal{H}_m$	Hilberträume	110
I, J	Antilineare Identifikationsabbildungen	110

$\langle v, w \rangle$	Skalarprodukt auf $V := \mathcal{H}_1 \otimes \cdots \otimes \mathcal{H}_m$ von $v, w \in V$ 110
$\ \cdot \ _{\text{HS}}$	Hilbert-Schmidt-Norm 110
\mathcal{H}	Vervollständigung von $(V, \ \cdot \ _{\text{HS}})$ 111
$\mathcal{U}_1, \dots, \mathcal{U}_m, \mathcal{U}$	Unitäre Gruppen von $\mathcal{H}_1, \dots, \mathcal{H}_m$ und \mathcal{H} 111
$\mathcal{G}_{\mathcal{H}}$	Gruppe der Produktvektoren aus unitären Operatoren 111
V	Mehrfaches Tensorprodukt $\mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_r}$ für $r, n_1, \dots, n_r \geq 2$... 112
$(e_i)_{i=1, \dots, n}$	Kanonische Basisvektoren von \mathbb{R}^n 112
N	Indexmenge $\{1, \dots, n_1\} \times \cdots \times \{1, \dots, n_r\}$ 112
\geq_{invlex}	Invers lexikographische Ordnung auf N 112
$\mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$	Vektorraum der mehrstufigen Matrizen 112
$(\lambda_i)_{i \in N}$	Mehrstufige Matrix 112
E_{k_1, \dots, k_r}	Matrixeinheit für $k_1 \leq n_1, \dots, k_r \leq n_r$ 112
ι	Identifikationsabbildung zwischen $\mathcal{M}_{n_1, \dots, n_r}(\mathbb{R})$ und V 112
\star	Multiplikationsabbildung auf mehrstufigen Matrizen 113
$f_{i,j,k,l}$	Polynom für $i, j, k, l \in N$ 116
P	Menge der Determinanten, die Produktvektoren charakterisieren 116
$\mathcal{I}_V, \mathcal{J}_V$	Ideale, erzeugt von P (und dem Normierungspolynom) 116

6 Approximation der Pi-Norm-Einheitssphäre

V	Mehrfaches Tensorprodukt $\mathbb{R}^{n_1} \otimes \cdots \otimes \mathbb{R}^{n_r}$ für $r, n_1, \dots, n_r \geq 2$... 123
\mathcal{T}_k	k -ter Thetakörper zu \mathcal{J}_V 123
I	Vom Normierungspolynom erzeugtes Ideal 124
G_n, U_n	Gerade und ungerade Polynome in $\mathbb{R}[X_1, \dots, X_n]$ 125
$\ \cdot \ _{\Theta, k}$	k -te Thetanorm 126
$r(\mathcal{T}_k)$	Innerer Radius des Thetakörpers \mathcal{T}_k 127
y	Bell-Zustand 129
K	Kompakte und konvexe Teilmenge von \mathbb{R}^n , die nicht leer ist 132
$\dim(S)$	Dimension einer Seite S von K 132
A°	Polare einer Teilmenge $A \subseteq \mathbb{R}^n$ 135
K	Kompakte, konvexe Nullumgebung in \mathbb{R}^n und Teilmenge von \mathcal{B}_1 137
$r(K)$	Innerer Radius von K 137
\mathcal{R}	Repräsentantensystem der auf K nicht negativen Funktionale ... 138
S_v^K	Annullierte Seite von K , induziert durch $v \in K^\circ$, $\ v\ _K = 1$ 139
S^A	Duale Seite zu einer Seite S von K 142
V	Gleich $\mathbb{R}^n \otimes \mathbb{R}^m$. Im zweiten Unterabschnitt gilt: $n = m = 2$ 146
\mathcal{G}_V	Untergruppe der Symmetriegruppe der Produktvektoren 147
S_ξ	Maximale Seite zu $\xi \in V \setminus \{0\}$ 147
U_z^i	Orthogonale 2×2 -Matrix mit $\ z\ = 1$ und $i \in \{0, 1\}$ 149
U, T	Spezielle orthogonale 2×2 -Matrizen 149
$\eta(v, w, \lambda, i + j)$	Parametrisierung eines Vektors mit projektiver Norm eins 149
$\mathcal{O}^0, \mathcal{O}^1$	Untergruppen von \mathcal{G}_V 151

7 Numerische Simulation

V	Mehrfaches Tensorprodukt $\mathbb{R}^{n_1} \otimes \dots \otimes \mathbb{R}^{n_r}$ für $r, n_1, \dots, n_r \geq 2$...	159
n	Dimension von V	159
$\langle \cdot, \cdot \rangle$	Skalarprodukt auf \mathcal{S}_m	160
$\text{svec}(X)$	Linearisierung von $X \in \mathcal{S}_m$	169

Stichwortverzeichnis

- Äußerer Radius, 124
- Adjungierte, 71
- Affine Hülle, 73
- Affine Unabhängigkeit, 63
- Affiner Teilraum, 63
- Algebraische Gleichung, 21
- Algorithmus von Buchberger, 10
- Angeordneter Vektorraum, 68
- Annihilator, 71
- Anordnung, 27
- Assoziativität, 104, 106
- Banachraum, 94, 106
- Basis
 - Standard-, 16, 85, 89, 165
 - Theta-, 18, 89
- Bell-Zustand, 129
- Bidualität, 72
- Bipolarsatz, 135
- Boolsche Polynomkombination, 37, 41, 45
- Computeralgebrasystem, 1, 13
- Determinantenkriterium, 115, 165
- Dicksons Lemma, 7
- Divergenz, 35
- Divisionsalgorithmus, 5
- Dual
 - topologischer, 70
- Duale Norm, 101, 108
- Einheitsproduktvektoren, 106, 123, 166
- Erzeuger, 1, 25
- Extremalpunkt, 63, 109, 140
- Faktorisierung, 102, 105
- Folgenraum, 75, 85
- Fortsetzung, 93, 94
- Gröbnerbasis, 1, 7, 85, 89, 119, 165
 - reduzierte, 11, 119
- Grad, 4, 14
 - eines Thetakörpers, 83
- Graduierte lexikographische Ordnung, 3, 165
- Gradungleichungen, 15
- Hexagon, 142
- Hilbert-Schmidt-Norm, 110, 124
- Hilbertraum, 110
- Hilbertscher Basissatz, 47
- Ideal, 1
 - reelles, 30
 - Verschwinde-, 52
- Idealgleichheitsproblem, 13
- Idealzugehörigkeitsproblem, 8
- Injektive Norm, 101, 108, 114
- Innerer Radius, 127, 137
- Invers lexikographische Ordnung, 112
- Isometrie, 109
- Körper
 - angeordneter, 27
 - archimedischer, 53, 57
 - reell abgeschlossener, 21, 30
 - reeller, 30
- Kegel, 21, 23, 61, 68

- archimedischer, 57
- dualer, 61, 72, 79, 86
- echter, 68
- erzeugender, 68
- erzeugter, 24, 69
- projizierter, 86
- Kegelschnitt, 77
- Kleinste gemeinsames Vielfaches, 9
- Konvexe Hülle, 63
- Koordinatenring, 1, 14
- Kreuznorm, 106, 123, 126
- Kriterium von Buchberger, 9

- Leitkoeffizient, 4
- Leitmonom, 4
- Leitterm, 4
- Lexikographische Ordnung, 2
- Lineare Optimierung, 160
- Lokalkonvexer Vektorraum, 70

- MATLAB, 164
- Matrix
 - mehrstufige, 101, 112
 - Moment-, 90, 93, 161
 - orthogonale, 62, 149
 - positiv definite, 62
 - positiv semidefinite, 62, 90
 - symmetrische, 62
- Matrizeinheit, 113
- Maximaler Vektor, 138
- Mehrfaches Tensorprodukt, 102
- Mehrstufige Matrix, 101, 112
- Menge
 - beschränkte, 22, 56
 - kompakte, 22, 137
 - konvexe, 61, 63, 81, 137
 - semialgebraische, 22, 45
- Minkowskifunktional, 125, 137, 161
- Mittelwertsatz, 35
- Momentmatrix, 90, 93, 161
- Monoid, 22, 24
- Monomordnung, 2
- Multigrad, 4

- Multilinearform, 102

- Nicht-lineare Optimierung, 160
- Nichtnullmenge, 47
- Norm
 - duale, 101, 108
 - Hilbert-Schmidt-, 110, 124
 - injektive, 101, 108, 114
 - Kreuz-, 106, 123, 126
 - Operator-, 114
 - Pi-, 106, 123, 159
 - projektive, 101, 106, 123, 159
 - Supremums-, 94
 - Theta-, 101, 123, 126, 159
- Normalform, 1, 8
- Nullstellenmenge, 21
- Nullstellensatz
 - Hilberts, 21
 - reeller, 22, 53

- Operatornorm, 114
- Optimierung, 160
- Ordnung
 - graduierte lexikographische, 3, 165
 - invers lexikographische, 112
 - lexikographische, 2
 - Monom-, 2

- Pi-Norm, 106, 123, 159
- PINORM, 159
- Platonischer Körper, 142
- Polare, 123, 135
- Polyeder, 61, 66
- Polynom, 1
 - affin-lineares, 4, 14, 17, 79, 138
 - gerades, 125
 - S-, 9
 - Sos-, 80, 82, 89, 93
 - ungerades, 125
- Polynomdivision, 5
- Polynomungleichung, 21, 36, 41
- Polytop, 61
- Positives Funktional, 94

- Positivkegel, 27, 68
- Positivstellenmenge, 47, 54, 72
- Positivstellensatz
 - abstrakter, 55
 - allgemeiner, 50
 - archimedischer, 57
 - formaler, 22, 47
 - konkreter, 22, 51, 127
- Primkegel, 25
- Produktfunktionale, 104
- Produktvektor, 102, 115
- Projektive Norm, 101, 106, 123, 159
- Punktauswertung, 94

- Radikal, 21
- Radius
 - äußerer, 124
 - innerer, 127, 137
- Reelle algebraische Geometrie, 21
- Reelles Radikal, 52
- Reelles Spektrum, 54
- Relatives Inneres, 61, 73
- Restriktionsmatrix, 161

- S-Polynom, 9
- Satz von Carathéodory, 63
- Satz von Hahn-Banach, 104
- Satz von Riesz-Frechet, 110
- Satz von Schmüdgen, 22, 53, 59
- Satz von Segré, 115
- Satz von Stone-Weierstrass, 94
- Schwach- \ast -Topologie, 70
- Schwache Topologie, 70
- Schwerpunkt, 93, 97
- SDPT3-4.0, 161
- Seite, 132
 - annulierte, 132
 - duale, 143
 - maximale, 132
 - minimale, 132
- Semidefinite Programmierung, 159
- Semidefinites Programm, 159
- Signaturabbildung, 37

- Sos-mod I , 82
- Sos-Polynom, 80, 82, 89, 93
- Spektraeder, 1, 61, 65, 80, 123, 159
- Standardbasis, 16, 85, 89, 165
- Strikte Konvexität, 135
- Sum of squares, 82
- Summe von Quadraten, 21, 24, 79, 82
- Supremumsnorm, 94
- Symmetriegruppe, 111

- Teilbarkeit, 5
- Tensorprodukt
 - mehrfaches, 102
- Theta-Basis, 18, 89
- Thetakörper, 1, 22, 79, 83, 123, 159
 - Konvergenz der, 22, 83, 124
- Thetanorm, 101, 123, 126, 159
- Träger eines Primkegels, 26
- Transferprinzip von Tarski-Seidenberg, 22, 36, 43

- Universelle Eigenschaft, 103

- Varietät
 - reelle algebraische, 47, 79, 112, 117, 123
- Vektorraum
 - angeordneter, 68
 - lokalkonvexer, 70
- Verschwindeideal, 52, 121
- Verschwindemenge, 21, 47, 54
- Vorzeichen, 34

- Wahrscheinlichkeitsmaß, 95

- Zustand, 80, 94
 - Bell-, 129
 - reiner, 94
- Zwischenwertsatz, 34