Westfälische Wilhelms-Universität Münster
Mathematisches Institut

Über die Entscheidbarkeit gewisser Prädikate in der Theorie der C^*-Algebren

Diplomarbeit

Stephan Rave
30. Juli 2007

Inhaltsverzeichnis

1 Einleitung

In dieser Arbeit wollen wir uns mit Fragen der Berechenbarkeit in der Theorie der C^*-Algebren befassen. Im Wesentlichen wird es also um zwei Dinge gehen: C^*-Algebren und Berechenbarkeitstheorie.

C^*-Algebren sind gerade die unter der Operatornorm und Bildung des adjungierten Operators abgeschlossenen Unteralgebren der beschränkten Operatoren auf einem Hilbertraum. Äquivalent hierzu lassen sie sich intrinsisch als involutive Banachalgebren beschreiben, die zusätzlich der C^*-Bedingung

$$\|x^*x\| = \|x\|^2 \qquad \forall x$$

genügen. Einer der Gründe, weshalb C^*-Algebren interessante mathematische Objekte sind, ist, dass sie eine nichtkommutative Verallgemeinerung des Begriffs des topologischen Raums darstellen, also topologische Strukturen beschreiben, die in einem gewissen Sinne nichtkommutativ sind. Daher sind sie ein zentrales Element der so genannten nichtkommutativen Geometrie. Solche nichtkommutativen Strukturen treten z. B. natürlich bei der Mathematisierung der Quantentheorie auf.

In Kapitel 2 werden wir einen kurzen Überblick über die Theorie der C^*-Algebren geben. Dabei werden wir auf zwei der wichtigsten Resultate (Satz von Gelfand-Naimark, GNS-Konstruktion) hinsteuern und im Vorübergehen alle Begriffe, die wir im Folgenden benötigen werden, einführen. Es erschien uns sinnvoll, dabei ein wenig mehr zu erwähnen, als wir im Folgenden benötigen werden, um wenigstens einen kleinen Eindruck von den größeren Zusammenhängen zu vermitteln.

Da die Theorie komplex ist, wird die Darstellung meist skizzenhaft sein, sodass einiges unklar bleiben wird, so es nicht schon vorher bekannt war. Im weiteren Verlauf der Arbeit wird jedoch meist ein grobes Verständnis der Grundbegriffe ausreichen.

Die Berechenbarkeitstheorie untersucht die Frage nach der prinzipiellen Berechenbarkeit von Funktionen oder Teilmengen natürlicher Zahlen, also die Frage nach der Existenz eines Rechenverfahrens, wie z.B. eines Computerprogramms, das zu gegebenen Argumenten den Funktionswert einer gegebenen Funktion bestimmt, bzw. entscheidet, ob das Argument in einer gegebenen Menge liegt. Man zeigt dabei recht leicht, dass es Funktionen geben muss, die nicht berechenbar sind, darunter auch solche, deren Berechenbarkeit vielleicht sehr wünschenswert wäre (Halteproblem).

Kapitel 3 beinhaltet eine kurze Einführung in die Berechenbarkeitstheorie, in der wir mathematisch exakt und voraussetzungsfrei alle im Folgenden benötigten Begriffe und Resultate bereitstellen werden, was jedoch mit einem recht großen, leider unvermeidbaren technischen Aufwand verbunden sein wird. Dafür werden wir allerdings anders als im ersten Kapitel auch nur wenig mehr sagen als das, was wirklich unabdingbar sein wird. Wer bereits mit Registermaschinen vertraut ist, möchte vielleicht dennoch einen kurzen Blick in Abschnitt 3.7 werfen.

C^*-Algebren sind mathematisch komplexe Objekte, und wenn schon in der Theorie der natürlichen Zahlen interessante Funktionen existieren, die nicht berechenbar sind, so erscheint es, ohne dies hier näher zu präzisieren, nicht verwunderlich, dass dies auch für C^*-Algebren der Fall sein wird.

Daher wollen wir uns in dieser Arbeit daher der Untersuchung der Entscheidbarkeit besonders einfach definierter Teilmengen von C^*-Algebren widmen, die möglichst natürlichen Fragestellungen über C^*-Algebren entsprechen. Genauer werden wir uns für die Entscheidbarkeit von Mengen der Form

$$\left\{x \;\middle|\; \lim_{n\to\infty} a^n x = 0\right\} \tag{1.0.1}$$

oder

$$\left\{x \;\middle|\; \exists n : a^n x = 0\right\} \tag{1.0.2}$$

interessieren.

Als Hauptresultat werden wir zeigen, dass die Algebra $\mathcal{O}_2$ einerseits so einfach strukturiert ist, dass alle Algebrenoperationen auf ihr[†] problemlos berechenbar sind, sich andererseits jedoch Elemente a finden lassen, für die diese Mengen nicht entscheidbar sind. Unser Existenzbeweis wird konstruktiv geführt werden und das Element a von einfacher Form und insbesondere in „berechenbarer Weise“ approximierbar sein. Reizvoll an der Konstruktion von a wird dabei sein, dass Linksmultiplikation mit a gerade einem Rechenschritt einer Registermaschine entspricht und die Unentscheidbarkeit der Mengen (1.0.1) und (1.0.2) aus der Unentscheidbarkeit des Halteproblems für Registermaschinen folgen wird.

Bevor wir zu diesem Resultat gelangen, werden wir in Kapitel 4 zunächst klären müssen, was wir darunter verstehen wollen, dass eine Menge von Elementen einer C^*-Algebra nicht entscheidbar ist. Dies bedarf Erklärung, da wir in Kapitel 3 nur von der Unentscheidbarkeit von Teilmengen von $\mathbb{N}_0^k$ sprechen werden.

In Kapitel 5 werden wir nach Definition und Studium der wichtigsten Eigenschaften von $\mathcal{O}_2$, bzw. allgemeiner von beliebigen von zwei Isometrien mit orthogonalem Bild erzeugten C^*-Algebren, das Hauptresultat unserer Arbeit präsentieren.

Schließlich werden wir in Kapitel 6 die Entscheidbarkeit der Mengen (1.0.1) und (1.0.2) für andere einfache Klassen von C^*-Algebren studieren und dabei sowohl auf positive wie auch negative Resultate stoßen. Dies wird es uns schließlich auch ermöglichen, unser Hauptresultat auf von nur einer echten Isometrie erzeugten C^*-Algebren zu verallgemeinern.

[†] genauer auf einer dichten Unteralgebra

Im Schlussteil in Kapitel 7 werden wir schließlich innehalten und versuchen unsere Resultate einzuordnen, sowie Perspektiven für sich aus ihnen ergebende weitere Fragestellungen aufzuzeigen.

1.1 Konventionen und Bezeichnungsweisen

Üblicherweise setzt man in der Berechenbarkeitstheorie $0 \in \mathbb{N}$, während es in der Funktionalanalysis allgemein gebräuchlich ist, 0 keine natürliche Zahl sein zu lassen. An letztere Gewohnheit werden wir uns halten und setzen also

$$\mathbb{N} := \{1, 2, 3, \dots\} \quad \text{und} \quad \mathbb{N}_0 := \mathbb{N} \cup \{0\}.$$

Mit $\mathbb{Q}(i)$ bezeichnen wir den kleinsten Teilkörper von $\mathbb{C}$, der $\mathbb{Q}$ und i enthält, also $\mathbb{Q}(i) = \{a + ib \mid a, b \in \mathbb{Q}\}$.

Wenn wir von einem lokalkompakten bzw. kompakten topologischen Raum sprechen, meinen wir dabei stets einen lokalkompakten bzw. kompakten *Hausdorffraum*.

Skalarprodukte werden wir stets mit $(\cdot \mid \cdot)$ notieren und sie antilinear in der zweiten Komponente sein lassen.

Für eine nichtleere Menge Ω bezeichne $\Omega^* := \bigcup_{i=0}^{\infty} \Omega^i$ die Menge der Worte über Ω, wobei $\Omega^0 := \{\sqcup\}$ und $\sqcup$ das leere Wort sei. Weiter bezeichne $\Omega^+ := \bigcup_{i=1}^{\infty} \Omega^i$ die Menge der nichtleeren Worte über Ω. Für ein $\omega \in \Omega^*$ bezeichne $|\omega|$ dasjenige $k \in \mathbb{N}_0$ mit $\omega \in \Omega^k$, also die Länge des Worts ω. Sind $\omega_1 = (x_1, \dots, x_m)$ und $\omega_2 = (y_1, \dots, y_n)$ Worte, so sei die Konkatenation $\omega_1\omega_2$ das Wort $(x_1, \dots, x_m, y_1, \dots, y_n)$.

2 C^*-Algebren

Es folgt ein kurzer Überblick über die Theorie der C^*-Algebren, in dem wir auf zwei grundlegende, zentrale Resultate über die Struktur von kommutativen C^*-Algebren (Satz von Gelfand-Naimark) und allgemein von nicht notwendig kommutativen C^*-Algebren (GNS-Konstruktion) eingehen werden. Diese werden auch erhellen, weshalb man in Verbindung mit C^*-Algebren von nichtkommutativer Geometrie spricht und in welcher Weise eine natürliche Verbindung zur Quantentheorie besteht.

Dabei werden wir jedoch viel zu rasch vorgehen und zu vieles auslassen, als dass wir eine solide Basis für die Arbeit mit C^*-Algebren schaffen könnten. Hierfür verweisen wir auf Lehrbücher wie z. B. [Mur]. Dennoch hoffen wir, dass dieses Kapitel genug Grundlage für das Verständnis dieser Arbeit liefern wird.

2.1 Grundbegriffe der Funktionalanalysis

Wir erinnern zunächst kurz an einige grundlegende Begriffe der Funktionalanalysis, gehen auf diese jedoch nicht näher ein. Gute Lehrbücher der Funktionalanalysis sind z. B. [HS], das ausführliche [Wer] oder das recht anspruchsvolle [Rud].

2.1.1 Definition (normierter Raum, Banachraum)**.** Unter einer *Halbnorm* auf einem $\mathbb{K}$-Vektorraum $\mathcal{V}$ mit $\mathbb{K} = \mathbb{R}, \mathbb{C}$ verstehen wir eine Abbildung

$$\begin{aligned} \|\cdot\| : \mathcal{V} &\longrightarrow \mathbb{R} \\ \xi &\longmapsto \|\xi\| \end{aligned}$$

mit folgenden Eigenschaften:

1. $\|\xi\| \geq 0 \qquad \forall \xi \in \mathcal{V}$,
2. $\|\lambda\xi\| = |\lambda| \, \|\xi\| \qquad \forall \xi \in \mathcal{V}, \forall \lambda \in \mathbb{K}$,
3. $\|\xi + \eta\| \leq \|\xi\| + \|\eta\| \qquad \forall \xi, \eta \in \mathcal{V}$.

Gilt zusätzlich

$$\|\xi\| = 0 \Leftrightarrow \xi = 0 \qquad \forall \xi \in \mathcal{V}$$

so heißt $\|\cdot\|$ *Norm*. Ein *normierter Raum* ist ein Vektorraum zusammen mit einer Norm. Eine Norm $\|\cdot\|$ auf $\mathcal{V}$ induziert eine Metrik auf $\mathcal{V}$ vermöge $d(\xi, \eta) := \|\xi - \eta\|$.

Ein normierter Raum heißt *Banachraum*, falls die von der Norm induzierte Metrik vollständig ist. $\mathcal{V}$ heißt separabel, falls eine abzählbare dichte Teilmenge in $\mathcal{V}$ existiert.

Addition und skalare Multiplikation sind in normierten Räumen stetig.

2.1.2 Definition (Hilbertraum)**.** Ein *Skalarprodukt* auf einem $\mathbb{C}$-Vektorraum $\mathcal{H}$ ist eine Abbildung

$$\begin{aligned}(\cdot \mid \cdot) : \mathcal{H} \times \mathcal{H} &\longrightarrow \mathbb{C} \\ (\xi, \eta) &\longmapsto (\xi \mid \eta)\end{aligned}$$

mit folgenden Eigenschaften:

1. $(\cdot \mid \cdot)$ ist linear in der ersten und antilinear in der zweiten Komponente.
2. $(\cdot \mid \cdot)$ ist hermitesch, d.h. $(\xi \mid \eta) = \overline{(\eta \mid \xi)} \qquad \forall \xi, \eta \in \mathcal{H}$.
3. $(\cdot \mid \cdot)$ ist positiv definit, d.h. $(\xi \mid \xi) \geq 0 \quad \forall \xi \in \mathcal{H}$ und

$$(\xi \mid \xi) = 0 \quad \Longrightarrow \quad \xi = 0 \qquad \forall \xi \in \mathcal{H}.$$

Wir nennen zwei Vektoren $\xi, \eta \in \mathcal{H}$ *orthogonal*, wenn $(\xi \mid \eta) = 0$. Ein System paarweise orthogonaler, von 0 verschiedener Vektoren ist linear unabhängig.

Ein Skalarprodukt induziert eine Norm auf $\mathcal{H}$ vermöge $\|\xi\| := \sqrt{(\xi \mid \xi)}$. Ist $\mathcal{H}$ mit dieser Norm ein Banachraum, so heißt $\mathcal{H}$ *Hilbertraum.*

2.1.3 Definition (Orthonormalbasis)**.** Ein System von Vektoren $(\xi_i),\ i \in I$ in einem Hilbertraum $\mathcal{H}$ nennen wir ein *Orthonormalsystem*, falls die ξ_i normiert und paarweise orthogonal sind. Wir nennen (ξ_i) eine *Orthonormalbasis*, falls

$$\mathcal{H} = \overline{\operatorname{span}\left(\{\xi_i\}\right)}.$$

Falls I abzählbar ist, so ist $\mathcal{H}$ separabel.

2.1.4 Definition (beschränkte lineare Abbildung, Operator)**.** Eine lineare Abbildung $T : \mathcal{V} \longrightarrow \mathcal{W}$ zwischen normierten Räumen heißt *beschränkt*, wenn es ein $C \geq 0$ gibt mit

$$\|T(\xi)\| \leq C \|\xi\| \qquad \forall \xi \in \mathcal{V}.$$

T ist genau dann beschränkt, wenn T stetig ist. Gilt

$$\|T(\xi)\| = \|\xi\| \qquad \forall \xi \in \mathcal{V},$$

so heißt T *Isometrie*. Wir schreiben auch $T\xi$ statt $T(\xi)$.

Ein *(beschränkter) Operator* T auf einem normierten Raum $\mathcal{V}$ ist eine (beschränkte) lineare Abbildung $T : \mathcal{V} \longrightarrow \mathcal{V}$. Mit $\mathcal{B}(\mathcal{V})$ bezeichnen wir die Menge der beschränkten Operatoren auf $\mathcal{V}$.

2.1.5 Definition (Operator-Norm einer beschränkten Abbildung)**.** Sei $T : \mathcal{V} \longrightarrow \mathcal{W}$ eine beschränkte lineare Abbildung zwischen normierten Räumen. Setze

$$\|T\| := \sup_{\substack{\xi \in \mathcal{V} \\ \|\xi\|=1}} \|T\xi\| .$$

Für beschränkte lineare Abbildungen T und S, sodass $T \circ S$ existiert, gilt stets $\|T \circ S\| \leq \|T\| \, \|S\|$. $\|\cdot\|$ ist eine Norm auf $\mathcal{B}(\mathcal{V})$.

2.1.6 Definition (Dualraum, schwach-$*$-Topologie)**.** Sei $\mathcal{V}$ ein normierter Raum. Eine *stetiges lineares Funktional f* auf $\mathcal{V}$ ist eine beschränkte lineare Abbildung $f : \mathcal{V} \longrightarrow \mathbb{K}$. Die Menge aller stetigen linearen Funktionale auf $\mathcal{V}$ sei mit $\mathcal{V}'$ bezeichnet und ist mit der Operator-Norm ein Banachraum.

Unter der Schwach-$*$-Topologie auf $\mathcal{V}'$ verstehen wir die Topologie punktweiser Konvergenz auf $\mathcal{V}'$, also diejenige Topologie, die von der Basis

$$\left\{ U_{f,\xi_1,\ldots,\xi_n,\varepsilon} \;\middle|\; f \in \mathcal{V}', n \in \mathbb{N}, \xi_i \in \mathcal{V}, \varepsilon > 0 \right\}$$

mit

$$U_{f,\xi_1,\ldots,\xi_n,\varepsilon} := \left\{ g \in \mathcal{V}' \;\middle|\; |f(\xi_i) - g(\xi_i)| < \varepsilon \text{ für } i = 1, \ldots, n \right\}$$

erzeugt wird.

2.2 Topologische Algebren

Wir erinnern zunächst an die Definition einer Algebra.

2.2.1 Definition (Algebra)**.** Eine $\mathbb{K}$-*Algebra* über einem Körper $\mathbb{K}$ ist ein Quadrupel $(\mathcal{A}, +, \cdot, \odot)$, wobei $\mathcal{V} := (\mathcal{A}, +, \cdot)$ ein $\mathbb{K}$-Vektorraum und $\odot$ eine bilineare, assoziative Verknüpfung

$$\odot : \mathcal{V} \times \mathcal{V} \longrightarrow \mathcal{V}, \;\; (x, y) \longmapsto x \odot y$$

ist. Wir nennen $\mathcal{A}$ *kommutativ*, falls die Verknüpfung $\odot$ kommutativ ist. $\mathcal{A}$ heißt *unital*, falls es ein neutrales Element 1 für $\odot$ gibt, d. h.

$$1 \odot x = x \odot 1 = x \qquad \forall x \in \mathcal{A}.$$

Üblicherweise wird für $\cdot$ und $\odot$ dasselbe Symbol, bzw. überhaupt kein Symbol verwendet.

2.2.2 Definition (Unteralgebra, Ideal, Erzeuger)**.** Sei $\mathcal{A}$ eine $\mathbb{K}$-Algebra. Eine Teilmenge $\mathcal{J} \subseteq \mathcal{A}$ heißt *Unteralgebra* von $\mathcal{A}$, falls $\mathcal{J}$ selber wieder mit den Verknüpfungen von $\mathcal{A}$ eine $\mathbb{K}$-Algebra ist. $\mathcal{J}$ heißt *Ideal*, wenn zusätzlich $\mathcal{A}\mathcal{J} \subseteq \mathcal{J}$ und $\mathcal{J}\mathcal{A} \subseteq \mathcal{J}$ gilt.

Sei $\mathcal{M}$ eine Teilmenge von $\mathcal{A}$. Die von den Elementen von $\mathcal{M}$ *erzeugte* $\mathbb{K}$-*Unteralgebra* ist der Schnitt über alle $\mathbb{K}$-Unteralgebren von $\mathcal{A}$, die $\mathcal{M}$ enthalten. Die Elemente von $\mathcal{M}$ werden *Erzeuger* dieser Algebra genannt. Die von $\mathcal{M}$ erzeugte $\mathbb{K}$-Unteralgebra ist gerade die Algebra der nichtkommutativen Polynome in den Elementen von $\mathcal{M}$:

$$\left\{ \sum_{i=1}^{k} \lambda_i x_{i,1} x_{i,2} \cdots x_{i,l_i} \;\middle|\; k, l_i \in \mathbb{N}, x_{i,j} \in \mathcal{M}, \lambda_i \in \mathbb{K} \right\}.$$

Ist insbesondere die von $\mathcal{M}$ erzeugte Unteralgebra ganz $\mathcal{A}$, so nennen wir auch $\mathcal{A}$ von $\mathcal{M}$ erzeugt.

In der Kategorie der $\mathbb{K}$-Algebren betrachten wir folgende Morphismen:

2.2.3 Definition (Algebrenhomomorphismus)**.** Eine Abbildung $\varphi : \mathcal{A} \longrightarrow \mathcal{B}$ zwischen $\mathbb{K}$-Algebren $\mathcal{A}$ und $\mathcal{B}$ heißt *(Algebren-)Homomorphismus*, falls φ mit den Operationen der Algebren verträglich ist, d.h. φ ist $\mathbb{K}$-linear und es gilt

$$\varphi(xy) = \varphi(x)\varphi(y) \qquad \forall x, y \in \mathcal{A}.$$

Ist φ zusätzlich bijektiv, so nennen wir φ einen *Isomorphismus* sowie $\mathcal{A}$ und $\mathcal{B}$ *isomorph.*

Einen Homomorphismus zwischen unitalen Algebren nennen wir *unital*, falls zusätzlich

$$\varphi(1_{\mathcal{A}}) = 1_{\mathcal{B}}.$$

Im Folgenden betrachten wir in der Regel komplexe Algebren, also $\mathbb{C}$-Algebren.

Eine charakteristische Eigenschaft eines Elements einer (unitalen) komplexen Algebra ist sein Spektrum:

2.2.4 Definition (Invertierbares Element, Spektrum, Spektralradius)**.** Sei $\mathcal{A}$ eine komplexe, unitale Algebra. Ein Element $x \in \mathcal{A}$ heißt *invertierbar*, falls ein Element $x^{-1} \in \mathcal{A}$ existiert mit $xx^{-1} = x^{-1}x = 1$. Das *Spektrum* von x ist definiert als

$$\mathrm{sp}(x) := \{\lambda \in \mathbb{C} \mid \lambda \cdot 1 - x \text{ ist nicht invertierbar}\}.$$

Der *Spektralradius* $\rho(x)$ von x ist der kleinste Radius einer abgeschlossenen Kreisscheibe um 0 in $\mathbb{C}$ die $\mathrm{sp}(x)$ ganz enthält:

$$\rho(x) := \sup_{\lambda \in \mathrm{sp}(x)} |\lambda|.$$

2.2.5 Bemerkung. Für die Algebra der komplexen $n \times n$-Matrizen $M_n(\mathbb{C})$ gilt, dass für jede Matrix $A \in M_n(\mathbb{C})$ das Spektrum $\mathrm{sp}(A)$ von A gerade die Menge der Eigenwerte (Spektralwerte) von A ist.

Im Folgenden werden wir uns stets für Algebren mit topologischer Struktur interessieren.

2.2.6 Definition (normierte Algebra, Banachalgebra)**.** Eine *normierte komplexe Algebra* ist eine komplexe Algebra $\mathcal{A}$ zusammen mit einer Norm $\|\cdot\|$ auf $\mathcal{A}$, die in folgendem Sinne mit der Algebren-Multiplikation verträglich ist:

$$\|xy\| \leq \|x\| \|y\| \qquad \forall x, y \in \mathcal{A}. \tag{2.2.1}$$

Falls $\mathcal{A}$ mit dieser Norm Banachraum ist, so nennen wir $\mathcal{A}$ eine *Banachalgebra.*

Aus (2.2.1) folgt sofort, dass die Multiplikation in normierten Algebren stetig ist.

Wenn wir eine Teilmenge $\mathcal{J} \subseteq \mathcal{A}$ ein *Ideal* von $\mathcal{A}$ nennen, dann meinen wir dabei stets zusätzlich, dass $\mathcal{J}$ abgeschlossen in der Topologie der Algebra ist.

Sei $\mathcal{M}$ eine Teilmenge einer Banachalgebra $\mathcal{A}$. Die von $\mathcal{M}$ *erzeugte Banach-Unteralgebra* ist der Abschluss der von $\mathcal{M}$ erzeugten Unteralgebra, d.h. der Abschluss der Algebra der nichtkommutativen Polynome in $\mathcal{M}$, oder der Schnitt über alle abgeschlossenen Unteralgebren von $\mathcal{A}$.

Als Verallgemeinerung der entsprechenden Resultate für $M_n(\mathbb{C})$, erhalten wir für Banachalgebren:

2.2.7 Theorem. *Sei $\mathcal{A}$ eine unitale Banachalgebra, $x \in \mathcal{A}$. Dann gilt:*

1. $\rho(x) \leq \|x\|$.
2. $\operatorname{sp}(x)$ *ist kompakt.*
3. $\operatorname{sp}(x)$ *ist nicht leer.*
4. $\rho(x) = \lim_{n\to\infty} \sqrt[n]{\|x^n\|}$.

Beweis. Skizze.

1. Für $\|x\| < 1$ ist $\sum_{k=0}^{\infty} \left\|x^k\right\|$ endlich. Daher konvergiert die Neumannsche Reihe
$$\sum_{k=0}^{\infty} x^k.$$
Der Grenzwert ist das inverse Element zu $1 - x$. (Teleskopsumme!) Damit ist für $|\lambda| > \|x\|$
$$\lambda \cdot 1 - x = \lambda\left(1 - \frac{x}{\lambda}\right)$$
invertierbar.

2. Nach 1. ist $\operatorname{sp}(x)$ beschränkt. Aus der Konvergenz der Neumannschen Reihe für Elemente von Norm kleiner 1 folgt weiter, dass die Menge der invertierbaren Elemente von $\mathcal{A}$ offen ist. Denn für x invertierbar und y mit $\|y\| < \frac{1}{\|x^{-1}\|}$ ist auch
$$x - y = x\left(1 - x^{-1}y\right)$$

invertierbar. $\operatorname{sp}(x)$ ist das Komplement des Urbilds der invertierbaren Elemente von $\mathcal{A}$ unter der stetigen Abbildung $\lambda \longmapsto \lambda \cdot 1 - x$.

3. Angenommen, dass $\operatorname{sp}(x) = \emptyset$, und sei f ein stetiges lineares Funktional auf $\mathcal{A}$. Dann ist die Funktion
$$\varphi_f(\lambda) := f\left((\lambda \cdot 1 - x)^{-1}\right) \tag{2.2.2}$$
auf ganz $\mathbb{C}$ holomorph und verschwindet im Unendlichen. Nach dem Satz von Liouville ([Jä], Satz 6) ist also φ_f konstant 0, im Widerspruch dazu, dass die stetigen linearen Funktionale auf normierten Räumen punktetrennend sind ([Wer], Korollar III.1.6).

4. Man prüft leicht, dass aus $\lambda \in \operatorname{sp}(x)$ folgt, dass $\lambda^n \in \operatorname{sp}(x^n)$. (Eigenvektoren zum Eigenwert λ werden Eigenvektoren zum Eigenwert λ^n.) Damit folgt $\operatorname{sp}(x)^n \subseteq \operatorname{sp}(x^n)$, also $\rho(x)^n \leq \rho(x^n) \leq \|x^n\|$, was
$$\rho(x) \leq \liminf_{n\to\infty} \sqrt[n]{\|x^n\|}$$
liefert. Für die umgekehrte Abschätzung bedenke man, dass für jedes stetige lineare Funktional f auf $\mathcal{A}$ die Funktion (2.2.2) auf dem Komplement von $\operatorname{sp}(x)$ holomorph ist und für $|\lambda| > \|x\|$ durch die Laurentreihe
$$\varphi_f(\lambda) = \frac{1}{\lambda}\sum_{k=0}^{\infty} \frac{f(x^k)}{\lambda^k} \tag{2.2.3}$$
dargestellt wird. Aus dem Satz über die Laurentreihen-Entwicklung ([Jä], Satz 12, Satz 16) folgt, dass (2.2.3) bereits für alle λ mit $|\lambda| > \rho(x)$ gelten muss. Aus der Konvergenz der Reihe folgt nun, dass für alle f die Menge
$$\left\{ \left| \frac{f(x^k)}{\lambda^k} \right| \,\middle|\, k \in \mathbb{N}_0 \right\}$$
beschränkt ist. Mit dem Prinzip der gleichmäßigen Beschränktheit ([Wer] Korollar IV.2.2) erhalten wir, dass dann auch die Menge
$$\left\{ \left\| \frac{x^k}{\lambda^k} \right\| \,\middle|\, k \in \mathbb{N}_0 \right\}$$
für $|\lambda| > \rho(x)$ beschränkt ist, woraus wir
$$\rho(x) \geq \limsup_{n\to\infty} \sqrt[n]{\|x^n\|}$$
erhalten.

Siehe [Mur], Lemma 1.2.4, Theorem 1.2.5, Theorem 1.2.7 . $\square$

2.3 Algebren über topologischen Räumen

Sei nun X ein lokalkompakter topologischer Raum. Wir betrachten die Menge der komplexwertigen stetigen Funktionen auf X, die im Unendlichen verschwinden:

$$\mathcal{C}_0(X) := \left\{ f : X \longrightarrow \mathbb{C} \text{ stetig} \;\middle|\; \forall \varepsilon > 0 \; \exists K \subseteq X \text{ kompakt} : |f(X \setminus K)| \subset (-\varepsilon, \varepsilon) \right\}$$

Mittels punktweiser Addition und Multiplikation der Funktionen wird diese Menge zur komplexen kommutativen Algebra.

Falls X sogar kompakt ist, stimmt $\mathcal{C}_0(X)$ mit

$$\mathcal{C}(X) := \{ f : X \longrightarrow \mathbb{C} \mid f \text{ ist stetig} \}$$

überein und die Einsfunktion ist ein Einselement in $\mathcal{C}(X)$, d.h. $\mathcal{C}(X)$ ist unital.

Für die Supremumsnorm

$$\|f\|_\infty := \sup_{x \in X} |f(x)|$$

gilt

$$|(fg)(x)| = |f(x)g(x)| = |f(x)|\,|g(x)| \le \|f\|_\infty \, \|g\|_\infty \qquad \forall x \in X,$$

also

$$\|fg\|_\infty \le \|f\|_\infty \, \|g\|_\infty \, ,$$

d. h. $\mathcal{C}_0(X)$ ist mit der Supremumsnorm eine normierte Algebra.[†] Tatsächlich gilt sogar

2.3.1 Satz. *Sei X ein lokalkompakter topologischer Raum, dann ist $\mathcal{C}_0(X)$ mit der Supremumsnorm eine kommutative Banachalgebra. Ist X kompakt, so ist $\mathcal{C}_0(X) = \mathcal{C}(X)$ unital.*

Beweis. Es ist nur die Vollständigkeit zu zeigen. Sei dazu (f_n) eine Cauchy-Folge in $\mathcal{C}_0(X)$. Dann ist insbesondere für jedes $x \in X$ auch $(f_n(x))$ eine Cauchy-Folge in $\mathbb{C}$. Das heißt gerade, dass (f_n) punktweise gegen eine Funktion f auf X konvergiert. Wegen

$$\begin{aligned} |f(x) - f_n(x)| &\le |f(x) - f_m(x)| + |f_m(x) - f_n(x)| \\ &\le |f(x) - f_m(x)| + \|f_m - f_n\|_\infty \qquad \forall m \in \mathbb{N}, \end{aligned}$$

folgt aus der punktweisen Konvergenz und der Tatsache, dass (f_n) eine Cauchy-Folge ist, dass (f_n) auch in Supremumsnorm gegen f konvergiert. Hieraus folgt weiter die Stetigkeit von f aus der Stetigkeit der f_n und f verschwindet im Unendlichen, da die f_n im Unendlichen verschwinden. □

[†] Die Supremumsnorm ist auf $\mathcal{C}_0(X)$ stets endlich, da stetige Funktionen auf kompakten Räumen beschränkt sind, und die Elemente von $\mathcal{C}_0(X)$ im Unendlichen verschwinden.

2.4 Kommutative C^*-Algebren

Als weitere Operation auf $\mathcal{C}_0(X)$ können wir einer Funktion f ihre komplex konjugierte Funktion $\overline{f}$ mit

$$\overline{f}(x) := \overline{f(x)} \qquad \forall x \in X$$

zuordnen. Es gilt $\overline{\overline{f}} = f$, $\left\|\overline{f}\right\|_\infty = \|f\|_\infty$, sowie $\overline{fg} = \overline{g}\,\overline{f}$. Damit hat die Abbildung

$$\begin{aligned} \bar{\cdot} : \mathcal{C}_0(X) &\longrightarrow \mathcal{C}_0(X) \\ f &\longmapsto \overline{f} \end{aligned}$$

alle Eigenschaften einer stetigen Involution auf $\mathcal{C}_0(X)$:

2.4.1 Definition (Banach-$*$-Algebra)**.** Eine *stetige Involution* $*$ auf einer Banach-Algebra $\mathcal{A}$ ist eine stetige antilineare Abbildung

$$\begin{aligned} (\cdot)^* : \mathcal{A} &\longrightarrow \mathcal{A} \\ x &\longmapsto x^* \end{aligned}$$

mit

$$(\cdot)^* \circ (\cdot)^* = \mathrm{id}_{\mathcal{A}}$$

und

$$(xy)^* = y^* x^* \qquad \forall x, y \in \mathcal{A}.$$

Ein Element $x \in \mathcal{A}$ mit $x^* = x$ nennen wir *selbstadjungiert*. Eine Banach-Algebra mit stetiger Involution heißt *Banach-$*$-Algebra*.

Sei $\mathcal{M}$ eine Teilmenge von $\mathcal{A}$. Die von $\mathcal{M}$ *erzeugte Banach-$*$-Unteralgebra* ist die von $\mathcal{M} \cup \mathcal{M}^*$ erzeugte Banach-Unteralgebra, oder der Schnitt über alle Banach-$*$-Unteralgebren, die $\mathcal{M}$ enthalten.

Zwischen komplexer Konjugation und Betragsbildung einer komplexen Zahl besteht bekanntlich der Zusammenhang

$$\overline{x} \cdot x = |x|^2 .$$

Folglich gilt auch

$$\left\|\overline{f} f\right\|_\infty = \|f\|_\infty^2 .$$

Dies nennen wir die C^*-Eigenschaft einer Involution auf einer Banachalgebra:

2.4.2 Definition (C^*-Algebra)**.** Eine Involution $*$ auf einer Banach-$*$-Algebra erfüllt die *C^*-Bedingung*, falls gilt:

$$\|x^* x\| = \|x\|^2 \qquad \forall x \in \mathcal{A}.$$

Eine Banach-$*$-Algebra, deren Norm die C^*-Bedingung erfüllt, heißt *C^*-Algebra*, und wir nennen eine (Halb-)Norm, die die C^*-Bedingung erfüllt, *C^*-(Halb)-Norm*.

2.4.3 Bemerkung. Aus der C^*-Bedingung folgt insbesondere sofort, dass $*$ isometrisch ist,

$$\|x\| = \|x^*\| \qquad \forall x \in \mathcal{A},$$

und

$$\|1\| = 1.$$

2.4.4 Satz. *Sei X ein lokalkompakter (kompakter) Raum, dann ist $\mathcal{C}_0(X)$ eine kommutative (unitale) C^*-Algebra.*

In vielen Fällen können wir uns bei der Untersuchung eines Problems ohne Einschränkung auf unitale C^*-Algebren beschränken, indem wir ggf. ein Einselement an die Algebra hinzuadjungieren.

2.4.5 Satz und Definition. *Sei $\mathcal{A}$ eine nicht unitale komplexe Algebra. Dann ist die Menge*

$$\widetilde{\mathcal{A}} = \mathcal{A} \times \mathbb{C}$$

vermöge komponentenweiser Addition und skalarer Multiplikation sowie der Algebren-Multiplikation

$$(x, \lambda) \cdot (y, \mu) := (xy + \mu x + \lambda y, \lambda\mu)$$

eine unitale Algebra, die wir als die Unitalisierung *von $\mathcal{A}$ bezeichnen.*

Falls $\mathcal{A}$ eine C^*-Algebra ist, so existiert auf $\widetilde{\mathcal{A}}$ eine C^*-Norm, die die C^*-Norm auf $\mathcal{A}$ fortsetzt.

Beweis. Skizze. Es ist klar, dass $\widetilde{\mathcal{A}}$ wieder eine Algebra ist. Man prüft recht leicht, dass

$$\|(x, \lambda)\| := \sup_{\substack{y \in \mathcal{A} \\ \|y\| \leq 1}} \|xy + \lambda y\|$$

eine C^*-Norm auf $\widetilde{\mathcal{A}}$ ist, die die Norm auf $\mathcal{A}$ fortsetzt, und dass $\widetilde{\mathcal{A}}$ mit dieser Norm vollständig ist.

Siehe [Dav], Proposition I.1.3 . □

In unitalen C^*-Algebren besteht ein besonders enger Zusammenhang zwischen der Norm und dem Spektrum eines Elements:

2.4.6 Satz. *Sei x ein selbstadjungiertes Element einer unitalen C^*-Algebra. Dann gilt*

$$\rho(x) = \|x\| .$$

Beweis. Folgt sofort aus Satz 2.2.7 und der C^*-Bedingung. □

2.4.7 Korollar. *Auf einer C^*-Algebra $\mathcal{A}$ existiert genau eine Norm, die $\mathcal{A}$ zur C^*-Algebra macht.*

Beweis. Ist $\mathcal{A}$ unital, so erhalten wir sofort für jedes $x \in \mathcal{A}$

$$\|x\|^2 = \|x^*x\| = \rho(x^*x).$$

Der Spektralradius von x^*x ist aber unabhängig von der Norm auf $\mathcal{A}$.
Ist $\mathcal{A}$ nicht unital, so betrachte die Unitalisierung. □

In der Kategorie der C^*-Algebren betrachten wir folgende Morphismen:

2.4.8 Definition ($*$-Homomorphismus)**.** Ein $*$-Homomorphismus zwischen C^*-Algebren $\mathcal{A}$ und $\mathcal{B}$ ist eine Abbildung $\varphi : \mathcal{A} \longrightarrow \mathcal{B}$, die mit den Algebren-Operationen $\mathcal{A}$ und $\mathcal{B}$ verträglich ist, d. h. φ ist ein Algebrenhomomorphismus und es gilt zusätzlich

$$\varphi(x^*) = \varphi(x)^* \qquad \forall x \in \mathcal{A}.$$

Zwei $*$-Algebren heißen isomorph, wenn zwischen ihnen ein bijektiver $*$-Homomorphismus existiert.

Wie der folgende Satz zeigt, ist es tatsächlich unnötig, die Stetigkeit von $*$-Homomorphismen zwischen C^*-Algebren zu fordern, da jeder $*$-Homomorphismus bereits stetig ist.

2.4.9 Satz. *Ist φ ein $*$-Homomorphismus zwischen C^*-Algebren $\mathcal{A}$ und $\mathcal{B}$, so ist φ normvermindernd, insbesondere also stetig.*

Beweis. Nehme zunächst an, dass $\mathcal{A}$ und $\mathcal{B}$ sowie φ unital sind. Dann bildet φ invertierbare Elemente auf invertierbare Elemente ab. Insbesondere haben wir daher zusammen mit Satz 2.4.6 für ein beliebiges $x \in \mathcal{A}$

$$\begin{aligned}\|x\|^2 &= \|x^*x\| = \rho(x^*x)\\ &\geq \rho(\varphi(x^*x)) = \rho(\varphi(x)^*\varphi(x)) = \|\varphi(x)^*\varphi(x)\| = \|\varphi(x)\|^2\end{aligned}$$

Im nicht unitalen Fall setze φ zu einem unitalen $*$-Homomorphismus auf den Unitalisierungen fort. □

Seien X und Y lokalkompakte Räume und $\varphi : X \longrightarrow Y$ eine stetige eigentliche Abbildung (d.h. Urbilder kompakter Mengen sind kompakt). Dann ist

$$\begin{aligned}\mathcal{C}_0(\varphi) : \mathcal{C}_0(Y) &\longrightarrow \mathcal{C}_0(X)\\ f &\longmapsto f \circ \varphi\end{aligned}$$

ein wohldefinierter $*$-Homomorphismus zwischen $\mathcal{C}_0(Y)$ und $\mathcal{C}_0(X)$.† Offensichtlich ist $\mathcal{C}_0(\cdot)$ verträglich mit der Verknüpfung von $*$-Homomorphismen, d. h.

$$\mathcal{C}_0(\psi \circ \varphi) = \mathcal{C}_0(\varphi) \circ \mathcal{C}_0(\psi).$$

†$\mathcal{C}_0(\varphi)(f)$ verschwindet im Unendlichen, weil φ eigentlich ist.

Sind X und Y kompakt, dann ist insbesondere jede stetige Abbildung eigentlich und es gilt

$$\mathcal{C}_0(\varphi)(1_Y) = 1_X,$$

d. h. $\mathcal{C}_0(\varphi)$ ist unital. Damit ist gezeigt:

2.4.10 Satz. $\mathcal{C}_0(\cdot)$ *ist ein kontravarianter Funktor zwischen der Kategorie der lokalkompakten Räume mit eigentlichen Abbildungen als Morphismen und der Kategorie der kommutativen C^*-Algebren mit $*$-Homomorphismen als Morphismen.*

$\mathcal{C}(\cdot) = \mathcal{C}_0(\cdot)$ *ist ein kontravarianter Funktor zwischen der Kategorie der kompakten Räume mit stetigen Abbildungen als Morphismen und der Kategorie der kommutativen unitalen C^*-Algebren mit unitalen $*$-Homomorphismen als Morphismen.*

2.5 Der Satz von Gelfand-Naimark und nichtkommutative Topologie

Könnte es nun sein, dass bereits alle kommutativen C^*-Algebren (bis auf Isomorphie) Funktionen-Algebren auf einem lokalkompakten Raum sind? Der Satz von Gelfand-Naimark bestätigt dies:

2.5.1 Satz und Definition (Spektrum einer C^*-Algebra)**.** *Sei $\mathcal{A}$ eine unitale (kommutative) C^*-Algebra. Die Menge*

$$\operatorname{spec}(\mathcal{A}) := \{\varphi : \mathcal{A} \longrightarrow \mathbb{C} \mid \varphi \textit{ ist unitaler } *\textit{-Homomorphismus}\}$$

ist unter der schwach-$*$-Topologie ein kompakter Raum und heißt das Spektrum *von $\mathcal{A}$.*

Beweis. $\operatorname{spec}(\mathcal{A})$ ist nach Satz 2.4.9 in der Norm-abgeschlossenen Einheitskugel der stetigen linearen Funktionale auf $\mathcal{A}$ enthalten und offensichtlich unter der schwach-$*$-Topologie abgeschlossen. Damit folgt die Behauptung aus dem Satz von Banach-Alaoglu ([Wer], Korollar VIII.3.12), der besagt, dass die Norm-abgeschlossene Einheitskugel der stetigen linearen Funktionale auf einem normierten Raum schwach-$*$-kompakt ist. □

Vermittels Auswertung erhalten wir zu jedem x in $\mathcal{A}$ eine stetige Funktion auf $\operatorname{spec}(\mathcal{A})$:

2.5.2 Satz und Definition (Gelfand-Transformation)**.** *Sei $\mathcal{A}$ eine unitale (kommutative) C^*-Algebra. Dann ist die Abbildung*

$$\begin{aligned} \widehat{\cdot} : \mathcal{A} &\longrightarrow \mathcal{C}(\operatorname{spec}(\mathcal{A})) \\ x &\longmapsto \widehat{x} \end{aligned}$$

mit

$$\widehat{x}(\varphi) := \varphi(x)$$

ein $*$-Homomorphismus.

Beweis. Die Stetigkeit von $\widehat{x}$ folgt gerade aus der Definition der Topologie auf $\mathrm{spec}(\mathcal{A})$. Dass $\widehat{\cdot}$ ein $*$-Homomorphismus ist, ist klar, da jedes $\varphi \in \mathrm{spec}(A)$ ein $*$-Homomorphismus ist. $\square$

Ist $\mathcal{A}$ nicht unital, so setzen wir

$$\mathrm{spec}(\mathcal{A}) := \mathrm{spec}(\widetilde{\mathcal{A}}) \setminus \left\{\widetilde{0}\right\}$$

wobei $\widetilde{0} : \widetilde{\mathcal{A}} \longrightarrow \mathbb{C}$ derjenige $*$-Homomorphismus ist mit $\widetilde{0}\restriction_{\mathcal{A}} \equiv 0$ und $\widetilde{0}(1) = 1$. Mit der von $\mathrm{spec}(\widetilde{A})$ geerbten Topologie ist $\mathrm{spec}(\mathcal{A})$ lokalkompakt und die Einschränkung der Gelfand-Transformierten

$$\widehat{x} := \widehat{\iota(x)}\restriction_{\mathrm{spec}(\mathcal{A})},$$

wobei ι die Inklusion von $\mathcal{A}$ in $\widetilde{\mathcal{A}}$ bezeichne, liefert einen $*$-Homomorphismus

$$\widehat{\cdot} : \mathcal{A} \longrightarrow \mathcal{C}_0(\mathrm{spec}(A)),$$

da $\widetilde{0}(x) = 0$ für alle $x \in \mathcal{A}$.

2.5.3 Theorem (Gelfad-Naimark)**.** *Sei $\mathcal{A}$ eine unitale kommutative C^*-Algebra. Dann ist die Gelfand-Transformation ein isometrischer Isomorphismus:*

$$\mathcal{A} \cong \mathcal{C}(\mathrm{spec}(\mathcal{A})).$$

Ist $\mathcal{A}$ nicht unital, so erhalten wir einen isometrischen Isomorphismus

$$\mathcal{A} \cong \mathcal{C}_0(\mathrm{spec}(\mathcal{A})).$$

Beweis. Skizze. Der nicht unitale Fall folgt leicht aus dem unitalen.

Für unitales $\mathcal{A}$ sieht man sofort, dass das Bild von $\widehat{x}$ eine Teilmenge von $\mathrm{sp}(x)$ ist ($\lambda - \varphi(x) = \varphi(\lambda \cdot 1 - x) \neq 0$, falls $\lambda \cdot 1 - x$ invertierbar). Tatsächlich ist das Bild von $\widehat{x}$ sogar ganz $\mathrm{sp}(x)$. Aus Satz 2.4.6 folgt dann, dass $\widehat{\cdot}$ isometrisch ist. Nach Definition von $\mathrm{spec}(\mathcal{A})$ ist das Bild von $\widehat{\cdot}$ punktetrennend, also nach dem Satz von Stone-Weierstraß ([Wer], Satz VIII.4.7) schon ganz $\mathcal{C}(X)$.

Siehe [Mur], Theorem 2.1.10 . $\square$

Damit hat also jede kommutative C^*-Algebra (bis auf Isomorphie) die Form $\mathcal{C}_0(X)$, d.h. die Zuordnung $X \longmapsto \mathcal{C}_0(X)$ ist (bis auf Isomorphie) surjektiv. Sie ist aber auch injektiv:

2.5.4 Satz. *Sei X ein lokalkompakter Raum. Dann gilt*

$$X \cong \operatorname{spec}(\mathcal{C}_0(X)).$$

Beweis. Idee. O. E. sei X kompakt, sonst betrachte die Einpunktkompaktifizierung von X ([vQ], 8.18). Zeige dass die Abbildung

$$\begin{aligned}\Phi : X &\longrightarrow \operatorname{spec}(\mathcal{C}(X))\\ x &\longmapsto \operatorname{ev}_x\end{aligned}$$

mit $\operatorname{ev}_x(\varphi) := \varphi(x)$ ein Homöomorphismus ist.

Siehe [Mur], Theorem 2.1.15 . □

2.5.5 Korollar. *Ist φ ein injektiver $*$-Homomorphismus zwischen C^*-Algebren, so ist φ isometrisch. Bilder von $*$-Homomorphismen zwischen C^*-Algebren sind C^*-Algebren.*

Beweis. Idee. Wir betrachten ohne Einschränkung den unitalen Fall. Wegen $\|x\|^2 = \|x^*x\|$ reicht es, $\|\varphi(x)\| = \|x\|$ für selbstadjungiertes x zu zeigen. Die von einem solchen x erzeugte unitale C^*-Unteralgebra ist kommutativ, wie auch die von $\varphi(x)$ erzeugte unitale C^*-Unteralgebra. Also reicht es nach Theorem 2.5.3, den Fall

$$\varphi : \mathcal{C}(X) \longrightarrow \mathcal{C}(Y)$$

zu behandeln.

Mit Satz 2.5.4 lässt sich leicht sehen, dass es ein stetiges $\check{\varphi} : Y \longrightarrow X$ gibt, sodass $\varphi(f) = f \circ \check{\varphi}$. Da φ injektiv ist, muss $\check{\varphi}$ surjektiv sein. Damit ist wiederum φ isometrisch.

Die zweite Aussage folgt hieraus, da die Quotientenalgebra einer C^*-Algebra nach einem abgeschlossenen Ideal auf kanonische Weise wieder eine C^*-Algebra ist, sich also ein Homomorphiesatz für C^*-Algebren formulieren lässt, und Bilder vollständiger Räume unter Isometrien vollständig sind.

Siehe [Bla], II.2.2.5 und [Mur], Theorem 3.1.6 . □

Nach Satz 2.5.4 haben wir also bis auf Isomorphie eine funktorielle Eins-zu-Eins-Korrespondenz zwischen lokalkompakten Räumen und kommutativen C^*-Algebren, bzw. kompakten Räumen und unitalen C^*-Algebren.[†] Also ist die Theorie kommutativer C^*-Algebren gerade die Theorie lokalkompakter topologischer Räume. Wenn

[†] Genauer gesagt ist der Funktor $\mathcal{C}_0(\cdot)$ eine natürliche Äquivalenz zwischen der Kategorie der lokalkompakten Räume mit eigentlichen Abbildungen als Morphismen und der Kategorie der kommutativen C^*-Algebren mit $*$-Homomorphismen als Morphismen, bzw. zwischen der Kategorie der kompakten Räume mit stetigen Abbildungen als Morphismen und der Kategorie der kommutativen unitalen C^*-Algebren mit unitalen $*$-Homomorphismen als Morphismen.

wir nichtkommutative C^*-Algebren betrachten, betreiben wir also nichtkommutative Topologie!

Interpretieren wir einen lokalkompakten Raum X als den Zustandsraum eines physikalischen Systems, so können wir $\mathcal{C}_0(X)$ als Algebra der Observablen (Messgrößen) dieses Systems auffassen. (Eine Observable ordnet gerade jedem Zustand eines Systems eine Messgröße zu.) Eine nichtkommutative C^*-Algebra lässt sich dann also als Observablen-Algebra eines „nichtkommutativen" physikalischen Zustandsraums auffassen.

2.6 Darstellungen und GNS-Konstruktion

Wenn wir eine nichtkommutative C^*-Algebra als Algebra der Observablen eines nichtkommutativen Zustandsraums eines physikalischen Systems interpretieren, heißt dies gerade, dass die Observablen dieses Systems (unter Multiplikation) i. Allg. nicht miteinander vertauschen. Solch ein Phänomen ist aber aus der Quantenmechanik, in der die Reihenfolge von Messungen in der Regel nicht vertauschbar ist, wohlbekannt!

Ein quantenmechanisches System lässt sich tatsächlich durch die Algebra seiner Observablen beschreiben, wobei als Observablen Operatoren auf einem geeigneten Hilbertraum $\mathcal{H}$ gewählt werden. Ein Zustand des Systems wird als eindimensionaler Teilraum von $\mathcal{H}$ interpretiert, oder dual hierzu als normiertes positives lineares Funktional auf der Observablenalgebra.[†]

2.6.1 Satz. *Sei $\mathcal{H}$ ein Hilbertraum, dann ist $\mathcal{B}(\mathcal{H})$ mit den üblichen Verknüpfungen und der Bildung des adjungierten Operators als Involution eine C^*-Algebra.*

Beweis. Wir zeigen nur die C^*-Eigenschaft. Dazu reicht es festzustellen, dass einerseits aufgrund der Cauchy-Schwarz-Ungleichung

$$\sup_{\|\xi\|=1} |(T^*T\xi \mid \xi)| \leq \|T^*T\| \, \|\xi\|^2 = \|T^*T\|$$

und andererseits

$$\sup_{\|\xi\|=1} |(T^*T\xi \mid \xi)| = \sup_{\|\xi\|=1} |(T\xi \mid T\xi)| = \sup_{\|\xi\|=1} \|T\xi\|^2 = \|T\|^2$$

gilt. □

Folglich ist jede solche Observablen-Algebra, wenn wir annehmen, dass es sich stets um eine abgeschlossene $*$-Unteralgebra von $\mathcal{B}(\mathcal{H})$ handelt, eine C^*-Algebra. Könnte es nun wieder sein, dass tatsächlich jede C^*-Algebra von dieser Form ist?

[†]Dem Raum span (ξ) wird das Funktional $T \longmapsto (T\xi \mid \xi)$ zugeordnet, falls ξ normiert ist.

2.6.2 Definition (Darstellung)**.** Eine *Darstellung* einer C^*-Algebra $\mathcal{A}$ ist ein Paar $(\pi, \mathcal{H})$, wobei $\mathcal{H}$ ein Hilbertraum und $\pi : \mathcal{A} \longrightarrow \mathcal{B}(\mathcal{H})$ ein $*$-Homomorphismus ist.

Wir nennen π *treu*, falls π injektiv ist.

Da Bilder von $*$-Homomorphismen zwischen C^*-Algebren wieder C^*-Algebren sind (Satz 2.5.5), ist die Frage also, ob jede C^*-Algebra eine treue Darstellung besitzt. Wir übertragen die Definition eines Zustands eines quantenmechanischen Systems auf beliebige C^*-Algebren:

2.6.3 Definition (positives lineares Funktional, Zustand)**.** Ein positives lineares Funktional f auf einer C^*-Algebra $\mathcal{A}$ ist ein lineares Funktional auf $\mathcal{A}$ mit

$$f(x^*x) \geq 0 \qquad \forall x \in \mathcal{A}.$$

f heißt *Zustand*, falls zusätzlich $\|f\| = 1$.

2.6.4 Bemerkung. Ist f ein positives lineares Funktional auf einer C^*-Algebra, so folgt schon, dass f stetig ist.

Beweis. Siehe [Mur], Theorem 3.3.1 . □

Auf C^*-Algebren existieren stets „hinreichend“ viele Zustände.

2.6.5 Satz. *Sei $\mathcal{A}$ eine C^*-Algebra und $x \in \mathcal{A}$ selbstadjungiert. Dann existiert ein Zustand f auf $\mathcal{A}$ mit $|f(x)| = \|x\|$.*

Beweis. Skizze. o.E. sei $\mathcal{A}$ unital. (Sonst unitalisiere.)

Die von x und 1 erzeugte C^*-Unteralgebra $C^*(x, 1)$ ist kommutativ. Folglich enthält $\operatorname{spec}(C^*(x, 1))$ ein φ mit $|\varphi(x)| = \|x\|$. (Die Gelfand-Transformation ist isometrisch.) Setze φ normerhaltend zu einem Funktional auf ganz $\mathcal{A}$ fort. (Satz von Hahn-Banach. [Wer], Theorem III.1.5) Man zeigt leicht, dass aus $\varphi(1) = 1 = \|\varphi\|$ und der Stetigkeit der Fortsetzung bereits folgt, dass diese Fortsetzung positiv ist. ([Mur], Corollary 3.3.4)

Siehe [Mur], Theorem 3.3.6 . □

Zu jedem positiven linearen Funktional können wir eine Darstellung konstruieren:

2.6.6 Theorem (GNS-Konstruktion)**.** *Sei f ein positives lineares Funktional auf einer C^*-Algebra $\mathcal{A}$. Dann existiert eine Darstellung $(\pi_f, \mathcal{H}_f)$ sowie ein Vektor $\xi_f \in \mathcal{H}_f$, so dass*

$$f(x) = (\pi_f(x)\xi_f \mid \xi_f) \qquad \forall x \in \mathcal{A}.$$

ξ_f ist genau dann normiert, wenn f ein Zustand ist.

Ist $f(x) \neq 0$, so folgt insbesondere $\pi_f(x) \neq 0$.

Beweis. Idee. Definiere auf $\mathcal{A}$ die Sesquilinearform

$$<x \mid y>_f := f(y^* x).$$

Aus der Positivität von f folgt, dass $<\cdot \mid \cdot>_f$ hermitesch ist. Also erhalten wir auf $\mathcal{A}/N_f$ mit $N_f := \{x \in \mathcal{A} \mid f(x^* x) = 0\}$ ein Skalarprodukt. Seine Vervollständigung sei $\mathcal{H}_f$.

Die Darstellung π_f erhalten wir, indem wir $\mathcal{A}$ auf $\mathcal{A}/N_f$ durch Linksmultiplikation operieren lassen: $\pi_f(x)\dot{y} := \dot{(xy)}$. Man kann zeigen, dass dies ein beschränkter Operator auf $\mathcal{A}/N_f$ ist, der sich folglich eindeutig auf $\mathcal{H}_f$ fortsetzt.

Falls $\mathcal{A}$ unital ist, so setzen wir $\xi_f := \dot{1}$. Denn dann gilt:

$$<\pi_f(x)\xi_f \mid \xi_f>_f = <\pi_f(x)\dot{1} \mid \dot{1}>_f = <\dot{x} \mid \dot{1}>_f = f(1x) = f(x).$$

Siehe [Dav], Theorem I.9.6 . □

2.6.7 Korollar. *Jede C^*-Algebra besitzt eine treue Darstellung.*

Beweis. Sei $(\pi_i, \mathcal{H}_i), i \in I$ eine Familie von Darstellungen, so erhalten wir eine Darstellung

$$\begin{aligned} \bigoplus_{i \in I} \pi_i : \mathcal{A} &\longrightarrow \bigoplus_{i \in I} \mathcal{H}_i \\ x &\longmapsto \oplus_{i \in I} \pi_i(x) \end{aligned}$$

auf der direkten Summe der Hilberträume $\mathcal{H}_i$. Betrachte insbesondere

$$\pi := \bigoplus_{f \text{ Zustand auf } \mathcal{A}} \pi_f,$$

so folgt aus Satz 2.6.5, dass π treu ist. □

3 Registermaschinen und die Grenzen der Berechenbarkeit

In diesem Kapitel werden wir eine kurze Einführung in die Berechenbarkeitstheorie (Rekursionstheorie) anhand des Modells der Registermaschine geben. Diese Einführung wird insofern vollständig sein, als dass wir alle im Folgenden benötigten Konzepte bereitstellen und sämtliche dabei auftretenden Begriffe exakt definieren werden. Allerdings werden wir dem Leser einige sehr technische Beweise von ohnehin plausiblen Aussagen ersparen.

Darüber hinaus werden wir auch deshalb eine gründliche Einführung in die Berechenbarkeitstheorie nicht ersetzen können, weil wir nur behandeln werden, was im Folgenden unabdingbar sein wird, und wir viele wesentliche Aspekte der Theorie nicht werden beleuchten können. Insbesondere gehen wir auf keine weiteren Modelle der Berechenbarkeit ein, und grundlegende Resultate wie der zweite Rekursionssatz, Normalformtheoreme, der Satz von Post oder Zusammenhänge zwischen Berechenbarkeit und Beweisbarkeit werden keine Erwähnung finden.

Für eine gründliche Einführung in die Berechenbarkeitstheorie verweisen wir auf Lehrbücher wie z. B. [Poh1]. Umfassendere Darstellungen finden sich in [Ler], [Soa] oder [Odi1] und [Odi2]. Im Folgenden werden wir uns im Wesentlichen in verkürzter Form an der Darstellung in [Poh2] orientieren.

3.1 Registermaschinen

Die klassische Berechenbarkeitstheorie untersucht die Frage, welche Funktionen

$$f : \mathbb{N}_0 \longrightarrow \mathbb{N}_0,$$

oder auch allgemeiner Funktionen $f : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0^n$ berechenbar sind. Berechenbar bedeutet, dass ein *endliches*[†] Verfahren (Algorithmus) aus einfachen elementaren Rechenoperationen existiert, das zu jedem $n \in \mathbb{N}_0$ den Wert $f(n)$ berechnet.

[†] „endlich“ meint hier, das nur endlich viele Informationen benötigt werden, um dass Verfahren zu beschreiben. Ließen wir unendliche Algorithmen zu, wäre offensichtlich jede Funktion $f : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ berechenbar, da wir dann schon ihren gesamten Wertverlauf $(f(0), f(1), \dots)$ in dem Algorithmus speichern könnten.

Dabei ist die tatsächliche praktische Durchführbarkeit der Rechnung, also z. B. ob die Rechnung in den nächsten 10^{42} Jahren beendet sein wird oder ob weniger Speichereinheiten während der Rechnung benötigt werden, als Elementarteilchen im Universum existieren, irrelevant. Insbesondere fällt das bekannte $P = NP$-Problem ([Coo]) nicht in die Berechenbarkeitstheorie, sondern ist Gegenstand der so genannten Komplexitätstheorie.

Um uns nun dieser abstrakten Problemstellung anzunähern, wollen wir zunächst überlegen, welche Verfahren zur Berechnung einer Funktion wir bereits kennen:

Heute lassen wir Funktionen $f : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$ in der Regel von Rechenmaschinen, d.h. Computern berechnen. Ein Computer-System besteht aus Hardware, der CPU (Central Processing Unit), Speicher, Laufwerken, der Grafikkarte, etc. , sowie aus Software, also den Programmen, die die einzelnen Arbeitsschritte der Hardware steuern.

Wir wollen dieses Prinzip der Trennung von Hard- oder Software nun in ein mathematisches Modell überführen. Zunächst wenden wir uns der Hardware zu: Dabei ist festzustellen, dass die wesentliche Rechenarbeit eines Computers in seiner CPU zusammen mit dem Arbeitsspeicher durchgeführt wird. Alle weiteren Komponenten dienen letztlich der Ein- und Ausgabe, die wir auf einfache Ein- und Ausgabe-Funktionen reduzieren werden.

In der CPU befinden sich verschiedene Speicher-Register, die jeweils eine natürliche Zahl einer gewissen Größe speichern können. In einer ersten Idealisierung werden wir annehmen, dass unsere Rechenmaschine über q Register verfügt, die jeweils eine *beliebig große* natürliche Zahl speichern können.† Damit können wir in unserem Modell auf Arbeitsspeicher verzichten, da wir, wie sich weiter unten zeigen wird, bereits in den Registern beliebig große Datenmengen speichern können.

Die CPU kann nun diverse Änderungen am Inhalt dieser Register durchführen, wir sprechen von Modifikationsinstruktionen, oder sie auf gewisse Eigenschaften testen, wir sprechen von Testinstruktionen. Moderne CPUs verfügen über einige Hundert dieser Instruktionen. Wir wollen uns hier auf das Nötigste beschränken und definieren:

3.1.1 Definition (Basis-Registermaschine)**.** Die *Basis-Registermaschine* mit q Registern, m-stelliger Input-Funktion und n-stelliger Output-Funktion $(m, n \leq q)$ ist das 5-Tupel

$$\mathcal{R}_q^{m,n} = \big(\mathbb{N}_0^q, \{\mathrm{INC}_i \,|1 \leq i \leq q\} \cup \{\mathrm{DEC}_i \,|1 \leq i \leq q\}, \\ \{\mathrm{EQ0}_i \,|1 \leq i \leq q\}, \mathrm{IN}^m, \mathrm{OUT}^n\big),$$

bestehend aus der Menge der Registerzustände, den Mengen der Modifikations- und Test-Instruktionen, sowie einer Input- und einer Output-Funktion. Dabei ist

†Dies ist zumindest insofern nicht absurd, als dass es theoretisch vorstellbar ist, dass die Register während der Laufzeit der Maschine vergrößert werden könnten, wenn die gespeicherten Zahlen die Kapazität der Register übersteigen sollten. Natürlich existieren dennoch prinzipielle physikalische Grenzen.

- $\mathrm{INC}_i : \mathbb{N}_0^q \longrightarrow \mathbb{N}_0^q,\ (r_1, \dots, r_q) \longmapsto (r_1, \dots, r_{i-1}, r_i + 1, r_{i+1}, \dots, r_q)$
- $\mathrm{DEC}_i : \mathbb{N}_0^q \longrightarrow \mathbb{N}_0^q,\ (r_1, \dots, r_q) \longmapsto (r_1, \dots, r_{i-1}, r_i \dot{-} 1, r_{i+1}, \dots, r_q)$,
  wobei $a \dot{-} b := \begin{cases} a - b & b < a \\ 0 & b \geq a \end{cases}$
- $\mathrm{EQ0}_i : \mathbb{N}_0^q \longrightarrow \{0, 1\},\ (r_1, \dots, r_q) \longmapsto \begin{cases} 0 & r_i > 0 \\ 1 & r_i = 0 \end{cases}$
- $\mathrm{IN}^m : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0^q,\ (x_1, \dots, x_m) \longmapsto (x_1, \dots, x_m, 0, \dots, 0)$
- $\mathrm{OUT}^n : \mathbb{N}_0^q \longrightarrow \mathbb{N}_0^n,\ (r_1, \dots, r_q) \longmapsto (r_1, \dots, r_n)$

Darüber hinaus verfügt die CPU über ein Steuerwerk, welches schrittweise das in die Maschine geladene Programm abarbeitet. Ein Programm ist eine durchnummerierte *endliche* Liste von Anweisungen, die darin bestehen, eine bestimmte Instruktion auszuführen und dann an eine andere Stelle des Programms zu springen. Die Stelle, an die gesprungen wird, hängt dabei im Falle von Test-Instruktionen von dem Ergebnis des Tests ab. Die einzelnen Nummern der Programmstellen werden wir die Zustände des Programms / der Maschine nennen. Im Falle von Modifikations-Instruktionen geht die Maschine in einen festgelegten Folgezustand über, wird eine Test-Instruktion ausgeführt, wechselt sie in einen Folge- oder in einen Verzweigungszustand in Abhängigkeit von dem Ergebnis des Tests. Wir setzen:

3.1.2 Definition (Registermaschinen-Programm)**.** Ein *Registermaschinen-Programm* für eine Basismaschine $\mathcal{R}_q^{m,n}$ ist eine endliche Menge $\mathcal{P}$, für die gilt:

1. Jedes Element $P \in \mathcal{P}$ ist von einer der folgenden Formen:
   - $P = (z, \mathrm{INC}_i, z_f), \quad z, z_f \in \mathbb{N}_0, 1 \leq i \leq q$
   - $P = (z, \mathrm{DEC}_i, z_f), \quad z, z_f \in \mathbb{N}_0, 1 \leq i \leq q$
   - $P = (z, \mathrm{EQ0}_i, z_f, z_v), \quad z, z_f, z_v \in \mathbb{N}_0, 1 \leq i \leq q$
2. Zu jedem $z \in \mathbb{N}_0$ gibt es höchstens ein $P \in \mathcal{P}$ mit $P = (z, \dots)$.
3. Es gibt ein $P \in \mathcal{P}$ der Form $P = (0, \dots)$.

Die Elemente von $\mathcal{P}$ nennen wir *Anweisungen* und die Zahlen z, z_f, z_v, die in den obigen Darstellungen auftreten, den Zustand, Folgezustand bzw. den Verzweigungszustand der Anweisung.

Eine Registermaschine ist nun eine Basis-Registermaschine (die Hardware) zusammen mit einem Registermaschinen-Programm (der Software):

3.1.3 Definition (Registermaschine)**.** Eine *m, n-stellige Registermaschine* mit q Registern ist ein Paar $\mathbb{M} = (\mathcal{R}_q^{m,n}, \mathcal{P})$, mit einem Registermaschinen-Programm $\mathcal{P}$ für $\mathcal{R}_q^{m,n}$.

3.2 Rechenschritts- und Resultats-Funktion

Wir benötigen noch einige weitere Begriffe.

3.2.1 Definition. Sei $\mathbb{M} = (\mathcal{R}_q^{m,n}, \mathcal{P})$ eine Registermaschine. Mit

$$\begin{aligned} Z(\mathbb{M}) := Z(\mathcal{P} := \{z \mid \exists P \in \mathcal{P} : P = (z, \dots)\} \cup \\ \{z_f \mid \exists P \in \mathcal{P} : P = (\dots, z_f, \dots)\} \cup \{z_v \mid \exists P \in \mathcal{P} : P = (\dots, z_v)\} \end{aligned}$$

bezeichnen wir die Menge der Zustände von $\mathbb{M}$.

Weiter sei $E(\mathbb{M}) := E(\mathcal{P}) := Z(\mathbb{M}) \setminus \{z \mid \exists P \in \mathcal{P} : P = (z, \dots)\}$ die Menge der Endzustände, sowie $K(\mathbb{M}) := Z(\mathbb{M}) \times \mathbb{N}_0^q$ die Menge der Konfigurationen von $\mathbb{M}$.

Nach dem bisher Erläuterten sollte die folgende Definition der Rechenschrittfunktion einleuchtend sein.

3.2.2 Definition (Rechenschrittfunktion)**.** Die Rechenschrittfunktion einer Registermaschine $\mathbb{M}$ ist definiert als:

$$\mathrm{RS}_{\mathbb{M}} : K(\mathbb{M}) \longrightarrow K(\mathbb{M})$$

$$(z, \overrightarrow{r}) \longmapsto \begin{cases} (z_f, \mathrm{INC}_i(\overrightarrow{r})) & (z, \mathrm{INC}_i, z_f) \in \mathcal{P} \\ (z_f, \mathrm{DEC}_i(\overrightarrow{r})) & (z, \mathrm{DEC}_i, z_f) \in \mathcal{P} \\ (z_f, \overrightarrow{r}) & (z, \mathrm{EQ0}_i, z_f, z_v) \in \mathcal{P} \text{ und } \mathrm{EQ0}_i(\overrightarrow{r}) = 1 \\ (z_v, \overrightarrow{r}) & (z, \mathrm{EQ0}_i, z_f, z_v) \in \mathcal{P} \text{ und } \mathrm{EQ0}_i(\overrightarrow{r}) = 0 \\ (z, \overrightarrow{r}) & z \in E(\mathbb{M}) \end{cases}$$

Es ist klar, dass $\mathrm{RS}_{\mathbb{M}}$ wohldefiniert ist, denn nach der Definition von Registermaschinen-Programmen trifft stets genau einer der aufgeführten Fälle ein.

Das Anwenden der Rechenschrittfunktion auf eine Konfiguration $(z, \overrightarrow{r})$ von $\mathbb{M}$ liefert gerade die Konfiguration $(z', \overrightarrow{r}')$ von $\mathbb{M}$, die $\mathbb{M}$ einnimmt, nachdem $\mathbb{M}$ in der Konfiguration $(z, \overrightarrow{r})$ einen Rechenschritt durchgeführt hat.

Der Lauf einer Registermaschine $\mathbb{M}$ beginnt nun, indem der Input $\overrightarrow{x}$ mittels IN^m in die Register geladen wird und $\mathbb{M}$ in den Anfangszustand 0 versetzt wird. Daraufhin beginnt $\mathbb{M}$, Rechenschritte durchzuführen. Nach k Rechenschritten befindet sich $\mathbb{M}$ angesetzt auf $\overrightarrow{x}$ also in der Konfiguration

$$\mathrm{RS}_{\mathbb{M}}^k \,(0, \mathrm{IN}^m(\overrightarrow{x}))\,.$$

Die Rechnung läuft so lange, bis M einen Endzustand erreicht. Wir definieren daher:

3.2.3 Definition (Rechenzeitfunktion)**.**

$$\mathrm{RZ}_{\mathbb{M}} : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0 \cup \{\uparrow\}$$

$$\overrightarrow{x} \longmapsto \begin{cases} \min \left\{ k \in \mathbb{N}_0 \;\middle|\; \mathrm{RZ}^k\,(0, \mathrm{IN}^m(\overrightarrow{x})) = (z_e, \overrightarrow{r}), z_e \in E(\mathbb{M}) \right\} & \text{min existiert} \\ \uparrow & \text{sonst} \end{cases}$$

$\mathrm{RZ}_{\mathbb{M}}(\overrightarrow{x})$ bezeichnet also die Anzahl der Rechenschritte, die $\mathbb{M}$ benötigt, um bei der Eingabe $\overrightarrow{x}$ die Rechnung abzuschließen. Falls $\mathbb{M}$ in eine Endlosschleife gerät, nimmt RZ den Wert $\uparrow$ an, was für „nicht definiert“ stehen soll.

Ist schließlich die Rechnung von $\mathbb{M}$ abgeschlossen, wird die Ausgabe mittels OUT^n ausgelesen. Wir definieren die Resultatsfunktion also als:

3.2.4 Definition (Resultatsfunktion)**.**

$$\mathrm{RES}_{\mathbb{M}} : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0^n \cup \{\uparrow\}$$
$$\overrightarrow{x} \longmapsto \begin{cases} \mathrm{OUT}^n \left(\mathrm{RS}^{\mathrm{RZ}(\overrightarrow{x})}\left(0, \mathrm{IN}^m(\overrightarrow{x})\right)\right) & \mathrm{RZ}(\overrightarrow{x}) \neq \uparrow \\ \uparrow & \text{sonst} \end{cases}$$

3.2.5 Beispiele. 1. Sei

$$\mathcal{ADD}_{a,b} = \{(0, \mathrm{EQ0}_a, 3, 1), (1, \mathrm{INC}_b, 2), (2, \mathrm{DEC}_a, 0)\}$$

und

$$\mathbb{ADD} = \left(\mathcal{R}_2^{2,1}, \mathcal{ADD}_{2,1}\right).$$

Dann ist $\mathrm{RES}_{\mathbb{ADD}}$ auf $\mathbb{N}_0^2$ definiert und es gilt

$$\mathrm{RES}_{\mathbb{ADD}}(x, y) = x + y.$$

2. Sei

$$\begin{aligned} \mathcal{MULT} = \{ & (0, \mathrm{EQ0}_1, 9, 1), (1, \mathrm{EQ0}_2, 5, 2), (2, \mathrm{INC}_3, 3), \\ & (3, \mathrm{INC}_4, 4), (4, \mathrm{DEC}_2, 1), (5, \mathrm{EQ0}_4, 8, 6), \\ & (6, \mathrm{INC}_2, 7), (7, \mathrm{DEC}_4, 5), (8, \mathrm{DEC}_1, 0), \\ & (9, \mathrm{EQ0}_3, 42, 10), (10, \mathrm{INC}_1, 11), (11, \mathrm{DEC}_3, 9)\} \end{aligned}$$

und

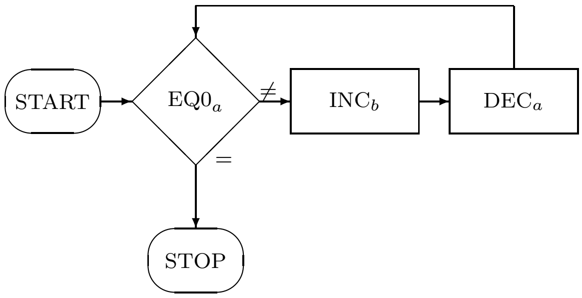
$$\mathbb{MULT} = \left(\mathcal{R}_4^{2,1}, \mathcal{MULT}\right).$$

Dann ist $\mathrm{RES}_{\mathbb{MULT}}$ auf $\mathbb{N}_0^2$ definiert und es gilt

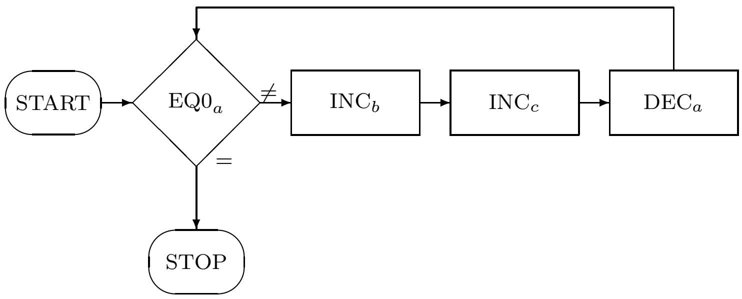
$$\mathrm{RES}_{\mathbb{MULT}}(x, y) = x \cdot y.$$

Beweis. Man zeigt diese Aussagen, die klar sind, sobald man die Struktur des jeweiligen Programms durchschaut hat, durch eine im Grunde einfache, jedoch mühselige doppelte Induktion entlang der Argumente der Resultatsfunktionen. □

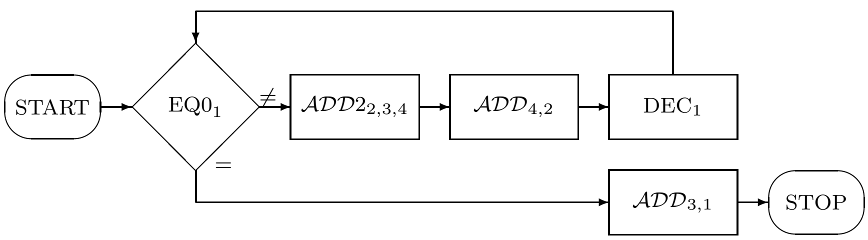
3.2.6 Bemerkung. Spätestens das zweite Beispiel macht klar, dass die direkte Angabe eines Registermaschinen-Programms in der Regel nicht sinnvoll ist. Da die Benennung der einzelnen Zustände jedoch keinerlei Rolle spielt, sondern nur die Verknüpfungen zwischen den einzelnen Anweisungen, die durch die Zustände vermittelt werden, kann man statt der direkten Auflistung des Programms auch ein *Flussdiagramm* angeben, um den Programmablauf durchschaubarer zu gestalten. Im Falle von $\mathcal{ADD}_{a,b}$ hätte dieses beispielsweise die Form



Desweiteren können wir bei größeren Programmen immer wiederkehrende Programmteile als einen einzelnen Block des Flussdiagramms, also als <u>*Unterprogramm*</u> verwenden. Wenn wir z. B. für das $\mathcal{ADD}_{a,b}$ Programm kurz $\longrightarrow \boxed{\mathcal{ADD}_{a,b}} \longrightarrow$ schreiben und zusätzlich das Diagramm



mit $\longrightarrow \boxed{\mathcal{ADD}2_{a,b}} \longrightarrow$ abkürzen, so können wir für $\mathcal{MULT}$ ein recht übersichtliches Flussdiagramm angeben:



3.3 Berechenbarkeit von Funktionen und Prädikaten

3.3.1 Definition (Registermaschinen-berechenbare Funktionen)**.**

$$\mathbb{PF}^{m,n} := \{f : \mathbb{N}_0^m \longrightarrow \mathbb{N}_0^n \cup \{\uparrow\} \mid f = \mathrm{RES}_{\mathbb{M}}, \mathbb{M} \text{ Registermaschine}\}$$

bezeichne die Menge der m-stelligen *Registermaschinen*-partiell-*berechenbaren Funktionen* mit Werten in $\mathbb{N}_0^n$.

$$\mathbb{F}^{m,n} := \{f \in \mathbb{PF}^{m,n} \mid \uparrow \notin \operatorname{im} f\}$$

ist die Menge der m-stelligen *Registermaschinen-berechenbaren Funktionen* mit Werten in $\mathbb{N}_0^n$.

Außerdem sei

$$\mathbb{PF}^m := \mathbb{PF}^{m,1} \quad \text{und} \quad \mathbb{F}^m := \mathbb{F}^{m,1}.$$

Eine partiell berechenbare Funktion f ist also insofern berechenbar, als dass eine Register-Maschine existiert, die für die Inputs $\overrightarrow{x}$, für die $f(\overrightarrow{x})$ definiert ist, gerade $f(x)$ berechnet, sonst jedoch in eine Endlosschleife gerät. Insbesondere muss zu keinem Zeitpunkt des Laufs der Maschine bekannt sein, ob sie zu dem gegebenen Input terminieren wird oder nicht. Ist f berechenbar, so wissen wir schon, dass der Lauf einer Maschine, die f berechnet, schließlich enden muss. Jedoch muss auch hier zu keinem Zeitpunkt im Lauf der Maschine bekannt sein, wie viele weitere Rechenschritte benötigt werden, bis die Maschine terminiert.

Im Folgenden wird die Berechenbarkeit von Prädikaten eine besondere Rolle spielen.

3.3.2 Definition (Prädikat)**.** Ein m-stelliges *Prädikat* P (auf dem Träger der Natürlichen Zahlen) ist eine Menge

$$P \subseteq \mathbb{N}_0^m.$$

Man schreibt

$$P(x_1, \ldots, x_m) \quad :\Longleftrightarrow \quad (x_1, \ldots, x_m) \in P.$$

Wir wollen ein Prädikat berechenbar nennen, wenn es seine charakteristische Funktion ist.

3.3.3 Definition (Registermaschinen-berechenbare Prädikate)**.**

$$\mathbb{PP}^m := \left\{P \subset \mathbb{N}_0^m \;\middle|\; \exists f \in \mathbb{PF}^m : P = f^{-1}(\{1\})\right\}$$

ist die Menge der m-stelligen *Registermaschinen*-partiell-*berechenbaren Prädikate*. Mit

$$\mathbb{P}^m := \left\{P \subset \mathbb{N}_0^m \;\middle|\; \exists f \in \mathbb{F}^m : P = f^{-1}(\{1\})\right\}$$

bezeichnen wir die Menge der m-stelligen *Registermaschinen-berechenbaren Prädikate*.

3.3.4 Bemerkung. Sei P ein m-stelliges Prädikat und bezeichne χ_P seine charakteristische Funktion, d.h. $\chi_P : \mathbb{N}_0^m \longrightarrow \{0,1\}$ und

$$\chi_P(x_1, \ldots, x_m) = 1 \Longleftrightarrow P(x_1, \ldots, x_m).$$

Dann gilt

$$P \in \mathbb{P}^m \Longleftrightarrow \chi_P \in \mathbb{F}^m.$$

Beweis. Ist $P = f^{-1}(\{1\})$ mit $f \in \mathbb{F}^m$, so hänge an jeden Endzustand einer Maschine, die f berechnet, ein Programm an, das in Register 1 den Wert 0 schreibt, falls sein Inhalt nicht 1 ist. □

Wir haben nun definiert, was es bedeutet, dass sich eine Funktion oder ein Prädikat auf einer Registermaschine berechnen lässt. Dabei haben wir viele Idealisierungen und Vereinfachungen gegenüber des Ausgangsmodells des modernen Computers gemacht. Schon daher ist es überhaupt nicht klar, ob es nicht Funktionen gibt, die zwar in einem intuitiven Sinne berechenbar sind, die jedoch nicht von einer Registermaschine berechnet werden können. Dabei ist es allerdings mehr ein empirisches wie auch ein philosophisches und weniger ein mathematisches Problem, festzulegen, was wir unter dem Ausdruck „intuitiv“ hier verstehen wollen.

Ohne dies hier näher rechtfertigen zu können, schließen wir uns folgender üblichen Annahme an:

3.3.5 Definition (Church-Turing-These)**.** Die Klassen der Registermaschinen-berechenbaren Funktionen und Prädikate sind genau die Klassen der intuitiv berechenbaren Funktionen und Prädikate.

Hier sei zu dieser These nur angemerkt, dass alle bis heute entwickelten Modelle von Berechenbarkeit, wie z.B. Turing-Maschinen, μ-rekursive Funktionen oder λ-Kalkül sich als äquivalent zur Registermaschinen-Berechenbarkeit herausgestellt haben, also die gleichen Funktionen und Prädikate berechnen, was die Church-Turing-These zumindest sehr plausibel erscheinen lässt.†

Wir vereinbaren folgende

3.3.6 Redeweisen.

1. Im Folgenden werden wir aufgrund der Church-Turing-These $\mathbb{PF}^m, \mathbb{F}^m, \mathbb{PP}^m, \mathbb{P}^m$ nur noch als die Klassen der berechenbaren bzw. partiell berechenbaren Funktionen oder Prädikate bezeichnen, ohne Hinweis auf das zugrunde liegende Berechenbarkeits-Modell.

2. Statt von „berechenbaren“ oder „partiell berechenbaren“ Funktionen oder Prädikaten, wird auch von „rekursiven“ bzw. „partiell rekursiven“ Funktionen oder Prädikaten gesprochen.

†Auch Quantencomputer berechnen keine größere Klasse von Funktionen.

3. Ein berechenbares Prädikat wird auch „entscheidbar“ genannt. Dementsprechend wird bei einem „Entscheidungsproblem“ die Frage nach der Berechenbarkeit eines Prädikats gestellt.

4. Ein partiell berechenbares Prädikat wird auch „rekursiv aufzählbar“ genannt.

3.3.7 Bemerkung. Die letzte Redeweise ist durch folgende Äquivalenz begründet:

$$P \in \mathbb{PP}^m \quad \Longleftrightarrow \quad \exists f \in \mathbb{F}^{1,m} : P = \mathrm{im}(f).$$

3.3.8 Bemerkung. Die CHURCH-TURING-These hat dramatische Konsequenzen für unsere folgende Arbeit! Aufgrund ihrer reicht es zum Beweis der Berechenbarkeit einer Funktion bzw. der Entscheidbarkeit eines Prädikats, lediglich ein Verfahren anzugeben, von dem klar ist, dass es sich zum Beispiel auf einem normalen Computer (der zudem über potentiell unendlich viel Speicher verfügt) durchführen lässt. Wir sind also insbesondere nicht gezwungen, Registermaschinen-Programme anzugeben, was meist ein sehr aufwendiges Unterfangen werden würde. Im Verlauf dieser Arbeit werden wir sehr regen Gebrauch von dieser Tatsache machen, **indem wir Berechnungsverfahren stets nur so genau umschreiben, dass klar wird, dass sie sich z.B. in ein Java-Programm umsetzen ließen**.

Wenn wir hingegen zeigen wollen, dass eine Funktion nicht berechenbar oder ein Prädikat nicht entscheidbar ist, brauchen wir dank der CHURCH-TURING-These umgekehrt nur zu zeigen, dass keine Registermaschine existiert, die die Funktion berechnet oder das Prädikat entscheidet.

Schließlich stellen wir noch einige einfache Eigenschaften der $\mathbb{P}^m$ fest:

3.3.9 Satz. *Die Mengen $\mathbb{P}^m$ sind abgeschlossen unter Vereinigung, Schnitt und Komplement-Bildung. Sie bilden also eine Mengen-Algebra.*

Beweis. (*Abschluss unter Schnitten*). Seien $A, B \in \mathbb{P}^m$ und $\mathcal{P}_A, \mathcal{P}_B$ Programme, die χ_A und χ_B berechnen und die ohne Einschränkung beide auf einer Basismaschine mit q Registern laufen. Modifiziere $\mathcal{P}_A$ so, dass $\mathcal{P}_A$ auf einer Basismaschine mit $q+1$ Registern läuft und zunächst den Inhalt von Register 1 in Register $q+1$ kopiert, bevor es mit der Rechnung beginnt.

Dann erhalten wir ein Programm, das $\chi_{A\cap B}$ berechnet, indem wir an jeden Endzustand des modifizierten $\mathcal{P}_A$ ein Programm anhängen, das testet, ob Register 1 leer ist. Ist dies der Fall, soll es in einen Endzustand übergehen, ansonsten soll es Register 1 leeren, mit dem Wert von Register $q+1$ füllen und dann Programm $\mathcal{P}_B$ laufen lassen. □

3.3.10 Satz. *Sei $B \in \mathbb{P}^n$ und $f \in \mathbb{F}^{m,n}$. Dann gilt für alle $A \subset \mathbb{N}_0^m$ mit*

$$f(\overrightarrow{x}) \in B \quad \Longleftrightarrow \quad \overrightarrow{x} \in A$$

schon, dass

$$A \in \mathbb{P}^m.$$

Beweis. Seien $\mathcal{P}_{\chi_B}, \mathcal{P}_f$ ohne Einschränkung $\mathcal{R}_q^{n,1}$- bzw. $\mathcal{R}_q^{m,n}$-Programme, die χ_B und f berechnen. Dann erhalten wir ein $\mathcal{R}_q^{m,1}$-Programm, das χ_A berechnet, indem wir an jeden Endzustand von $\mathcal{P}_f$ ein Programm anhängen, das die Register $q-n+1,\dots,q$ leert, und dann $\mathcal{P}_{\chi_B}$ laufen lässt. Dieses Programm berechnet

$$\chi_B \circ f = \chi_A.$$

□

3.4 Kodierung

Wir werden nun die wichtige Beobachtung machen, dass es möglich ist, Programme von Registermaschinen in eine natürliche Zahl zu kodieren. Das Hauptproblem besteht dabei darin, eine endliche Folge natürlicher Zahlen in eine natürliche Zahl zu kodieren.

3.4.1 Lemma. *Es gibt für alle $k \in \mathbb{N}$ injektive berechenbare Funktionen*

$$<\cdot>_k \colon \mathbb{N}_0^k \longrightarrow \mathbb{N}_0$$

und berechenbare Funktionen $(\cdot).: \mathbb{N}_0^2 \longrightarrow \mathbb{N}_0$, $\mathrm{lh}: \mathbb{N}_0 \longrightarrow \mathbb{N}_0$*, sowie ein berechenbares einstelliges Prädikat* Seq*, sodass gilt:*

1. $\bigcup_{k\in\mathbb{N}} \mathrm{im}(<\cdot>_k) = \mathrm{Seq}$
2. $\forall k\ \forall \overrightarrow{x} \in \mathbb{N}_0^k:\ \mathrm{lh}(<\overrightarrow{x}>_k) = k$
3. $\forall k\ \forall \overrightarrow{x} \in \mathbb{N}_0^k:\ \overrightarrow{x} = ((<\overrightarrow{x}>_k)_1, \dots (<\overrightarrow{x}>_k)_k)$

$<\cdot>_k$ *heißt Kodierungsfunktion,* $(\cdot).$ *Dekodierungsfunktion und Zahlen x mit* $\mathrm{Seq}(x)$ *heißen Folgennummern. Für Folgennummern x ist* $\mathrm{lh}(x)$ *die Länge von x.*

Beweis. Sei $p_1, p_2, p_3 \dots$ die Aufzählung aller Primzahlen. Setze

$$<x_1,\dots,x_k>_k := p_1^{x_1+1} \cdots p_k^{x_k+1}.$$

Aufgrund der Eindeutigkeit der Primfaktorzerlegung ist klar, dass dies ein solches Kodierungsschema liefert.

Die Berechenbarkeit wird durch explizite Angabe von Programmen, die die gegebenen Funktionen und Prädikate berechnen, gezeigt. Man mache sich dafür zunächst klar, dass es ein Programm gibt, das Division mit Rest durchführt. Dann können wir aber auch ein Programm finden, das testet, ob eine Zahl eine Primzahl ist, und dann gibt es auch ein Programm, das die n-te Primzahl berechnet. Aus diesen Programmen lassen sich die benötigten Programme schließlich leicht konstruieren. □

3.4.2 Bemerkung. Im Lichte der CHURCH-TURING-These ist sicherlich klar, dass die Funktionen und Prädikate in Lemma 3.4.1 berechenbar sind. Jedoch gleicht es einem Zirkelschluss, sich an dieser Stelle auf die CHURCH-TURING-These zu berufen, da sich ihre Gültigkeit gerade darauf stützt, dass man beweisen kann, dass alle bekannten Modelle der Berechenbarkeit höchstens so stark wie das der Registermaschinen sind. Dafür ist es aber gerade u.a. wesentlich, dass wir auf Registermaschinen Folgen natürlicher Zahlen zu Zahlen kodieren können.

3.4.3 Korollar (Kodierung von Programmen)**.** *Es gibt eine injektive Funktion*

$$<\cdot>\colon \{\textit{Registermaschinen-Programme}\} \longrightarrow \mathbb{N}_0,$$

sodass folgende Funktionen und Prädikate berechenbar sind

1. $\mathrm{im}(<\cdot>)$

2. $\{(x,z) \mid x = <\mathcal{P}>, z \in Z(\mathcal{P})\}$

3. $\{(x,z_e) \mid x = <\mathcal{P}>, z_e \in E(\mathcal{P})\}$

4. $(x,z) \longmapsto \begin{cases} (i,z_f) & x = <\mathcal{P}>, (z, \mathrm{DEC}_i, z_f) \in \mathcal{P} \\ (0,0) & \textit{sonst} \end{cases}$

5. $(x,z) \longmapsto \begin{cases} (i,z_f) & x = <\mathcal{P}>, (z, \mathrm{INC}_i, z_f) \in \mathcal{P} \\ (0,0) & \textit{sonst} \end{cases}$

6. $(x,z) \longmapsto \begin{cases} (i,z_f,z_v) & x = <\mathcal{P}>, (z, \mathrm{EQ0}_i, z_f, z_v) \in \mathcal{P} \\ (0,0,0) & \textit{sonst} \end{cases}$

Beweis. Es sind nur alle Anweisungen des Programms geeignet zusammenzukodieren. Z. B. können wir setzen

1. $<(z, \mathrm{INC}_i, z_f)> := <0, z, i, z_f>$, $\;<(z, \mathrm{DEC}_i, z_f)> := <1, z, i, z_f>$
2. $<(z, \mathrm{EQ0}_i, z_f, z_v)> := <2, z, i, z_f, z_v>$
3. $<\mathcal{P}> := <P_1, \dots, P_m>$, wobei die P_i gerade die Elemente von $\mathcal{P}$ sind, die so angeordnet sind, dass die Ausgangszustände der P_i streng monoton wachsen.

Die Berechenbarkeit wird wieder durch Angabe von Programmen gezeigt. □

Auch wenn die Möglichkeit der Kodierung von Programmen in natürliche Zahlen im Computerzeitalter selbstverständlich erscheint, ist sie doch von fundamentaler und tiefer Bedeutung für die Berechenbarkeitstheorie. Durch Kodierung wird es möglich, Programme mit Programmen rechnen zu lassen. Aus dieser Vermischung von Objekt-Ebene und Meta-Ebene ist es möglich, Varianten der bekannten Lügnerparadoxie „Dieser Satz ist nicht wahr.“ zu konstruieren, aus denen sich viele elementare Resultate der Berechenbarkeitstheorie ergeben.

3.5 Das Halteproblem

Als eine einfache Anwendung des Prinzips der Kodierung können wir die Existenz interessanter[†] nicht entscheidbarer Prädikate anhand des Halteproblems für Registermaschinen zeigen:

3.5.1 Definition (Halteproblem für Registermaschinen)**.**

$$H := \Big\{(x,y) \in \mathbb{N}_0^2 \;\Big|\; x = <\mathcal{P}>, \mathcal{P} \text{ Registermaschinen-Programm für } \mathcal{R}_q^{1,1}, \mathrm{RES}_{(\mathcal{R}_q^{1,1},\mathcal{P})}(y) \neq\uparrow \Big\}$$

ist das *Halteproblem für Registermaschinen.*

$$H^1 := \{x \in \mathbb{N}_0 \mid (x,x) \in H\}$$

nennen wir das *diagonalisierte Halteproblem.*

Ein Paar (x,y) liegt also in H, wenn x eine Registermaschine kodiert, die, angesetzt auf die Zahl y, hält, also nicht in eine Endlosschleife gerät. Das Halteproblem ist nicht entscheidbar:

3.5.2 Satz. *$H \notin \mathbb{P}^2$ und $H^1 \notin \mathbb{P}^1$.*

Beweis. Ist $H \in \mathbb{P}^2$, so auch offensichtlich $H^1 \in \mathbb{P}^1$, also reicht es $H^1 \notin \mathbb{P}^1$ zu zeigen.

Angenommen also, $H^1 \in \mathbb{P}^1$. Dann ist nach Satz 3.3.9 auch

$$\check{H}^1 := \mathbb{N}_0 \setminus H^1 = \{x \in \mathbb{N}_0 \mid (x,x) \notin H\} \in \mathbb{P}^1,$$

und somit

$$\chi_{\check{H}^1} \in \mathbb{F}^1.$$

Offensichtlich ist dann auch

$$\begin{aligned} f : \mathbb{N}_0 &\longrightarrow \mathbb{N}_0 \cup \{\uparrow\} \\ x &\longmapsto \begin{cases} \uparrow & \chi_{\check{H}^1}(x) = 0 \\ 1 & \chi_{\check{H}^1}(x) = 1 \end{cases} \end{aligned}$$

partiell berechenbar. (Hänge an das Programm, das $\chi_{\check{H}^1}$ berechnet, ein Programm an, das, falls Register 1 leer ist, in eine Endlosschleife gerät und sonst in einen Endzustand übergeht.)

[†]Die bloße Existenz nicht entscheidbarer Prädikate folgt sofort aus Kardinalitäts-Gründen!

Sei also $(\mathcal{R}_q^{1,1}, \mathcal{P}_f)$ eine Registermaschine, die f berechnet und sei $x = <\mathcal{P}_f>$. Dann gilt:

$$\begin{aligned} x \in \check{H}^1 &\Leftrightarrow (x,x) \notin H \\ &\Leftrightarrow \mathrm{RES}_{(\mathcal{R}_q^{1,1}, \mathcal{P}_f)}(x) \notin \mathbb{N}_0 \\ &\Leftrightarrow f(x) = \uparrow \\ &\Leftrightarrow x \notin \check{H}^1. \end{aligned}$$

Widerspruch! □

3.6 Die universelle Registermaschine

Wir wollen nun zeigen, dass H und H^1 jedoch rekursiv aufzählbar sind. Dies ist klar, wenn es möglich ist, den Lauf einer beliebigen Registermaschine durch eine feste Registermaschine zu simulieren.

3.6.1 Satz (Universelle Registermaschine)**.** *Die Funktion*

$$U : \mathbb{N}_0^2 \longrightarrow \mathbb{N}_0 \cup \{\uparrow\}$$

$$(x,y) \longmapsto \begin{cases} \mathrm{RES}_{(\mathcal{R}_q^{m,1}, \mathcal{P})}(y_1, \ldots, y_m) & x = <\mathcal{P}>, \mathcal{P} \textit{ ist } \mathcal{R}_q^{m,1}\textit{-Programm und} \\ & y = <y_1, \ldots, y_m> \\ \uparrow & \textit{sonst} \end{cases}$$

ist partiell berechenbar.

Beweis. Mit einiger Mühe, aber ohne wesentliche Schwierigkeiten, können wir auch hier ein Programm finden, das U berechnet. Dafür reicht es im Wesentlichen, zunächst zu prüfen, ob x ein gültiges Programm kodiert und dann ggf. den Lauf dieses Programms zu simulieren. Dazu speichere man kodiert in einem Register die aktuelle Konfiguration der zu simulierenden Maschine und führe an dieser Konfiguration immer wieder die Rechenschrittfunktion der simulierten Maschine aus. Weiter ist dann nur zu erkennen, wann die Maschine eine Endkonfiguration erreicht, und dann das Resultat auszulesen. □

3.6.2 Korollar.

$$H \in \mathbb{PP}^2 \quad \textit{und} \quad H^1 \in \mathbb{PP}^1.$$

Beweis. Es ist nur $H \in \mathbb{P}^2$ zu zeigen. Da U partiell-berechenbar ist, ist auch

$$U' : \mathbb{N}_0^2 \longrightarrow \mathbb{N}_0 \cup \{\uparrow\}$$

$$(x,y) \longmapsto \begin{cases} 1 & U(x,y) \in \mathbb{N}_0 \\ \uparrow & U(x,y) = \uparrow \end{cases}$$

partiell berechenbar. (Füge an die Endzustände eines Programms, welches U berechnet, Anweisungen an, die zu der Ausgabe von 1 führen.) Es ist aber nach Definition von U

$$H = U'^{-1}(\{1\}).$$

□

3.6.3 Korollar.

$$P \in \mathbb{P}^m \iff P \in \mathbb{PP}^k \wedge (\mathbb{N}^m \setminus P) \in \mathbb{PP}^m.$$

Beweis. Seien $P, (\mathbb{N}_0^m \setminus)P \in \mathbb{PP}^m$. Dann sind die charakteristischen Funktionen dieser Prädikate partiell berechenbar. Seien $\mathbb{M}_1$ und $\mathbb{M}_2$ Maschinen, die diese Funktionen berechnen. Wie im Beweis zu 3.6.1 lässt sich eine Registermaschine $\mathbb{M}$ angeben, die zu einem Input $\overrightarrow{x}$ *simultan* die Läufe von $\mathbb{M}_1$ und $\mathbb{M}_2$ simuliert. Da jedoch stets

$$\overrightarrow{x} \in P \vee \overrightarrow{x} \in (\mathbb{N}_0^m \setminus P)$$

gilt, muss die Rechnung einer der Maschinen $\mathbb{M}_1, \mathbb{M}_2$ schließlich terminieren, worauf $\mathbb{M}$ entweder 0 oder 1 ausgeben soll, womit $\mathbb{M}$ die charakteristische Funktion von P berechnet. □

3.6.4 Korollar.

$$\mathbb{P}^m \subsetneq \mathbb{PP}^m \subsetneq \mathcal{P}ow(\mathbb{N}_0).$$

Beweis. Dass die zweite Inklusion echt ist, folgt entweder aus Kardinalitäts-Gründen oder aus Korollar 3.6.3 zusammen mit $\mathbb{P}^m \subsetneq \mathbb{PP}^m$. □

3.7 Berechenbarkeit relativ zu einer Teilmenge von $\mathbb{N}_0^m$

In der Praxis wird uns häufig als Trägermenge einer Funktion oder eines Prädikates nicht $\mathbb{N}_0^m$ sondern eine Teilmenge begegnen. (Zum Beispiel, wenn wir Funktionen $f : \mathbb{N} \longrightarrow \mathbb{N}$ betrachten.) Dennoch wollen wir auch in solchen Fällen ohne größere Komplikationen von Berechenbarkeit oder Entscheidbarkeit sprechen können. Wir setzen daher:

3.7.1 Definition (Berechenbarkeit auf Teilmengen von $\mathbb{N}_0^m$)**.** Sei $\mathcal{M}$ eine beliebige Teilmenge von $\mathbb{N}^m$. Eine Funktion $f : \mathcal{M} \longrightarrow \mathbb{N}^n$ heißt dann *als auf $\mathcal{M}$ definierte Funktion berechenbar*, falls eine Funktion $\tilde{f} \in \mathbb{PF}^{m,n}$ existiert, mit $f = \tilde{f}\restriction_{\mathcal{M}}$.

Eine Prädikat $P \subseteq \mathcal{M}$ heißt *als Teilmenge von $\mathcal{M}$ entscheidbar* bzw. *relativ zu $\mathcal{M}$ entscheidbar*, falls seine charakteristische Funktion χ_P als auf $\mathcal{M}$ definierte Funktion berechenbar ist.

Eine Funktion f ist also als auf $\mathcal{M}$ definierte Funktion berechenbar, falls wir eine Registermaschine angeben können, die zu einem Input $\overrightarrow{x}$ *aus* $\mathcal{M}$ den Funktionswert von f berechnet. Liegt $\overrightarrow{x}$ nicht in $\mathcal{M}$, so kann sich die Maschine beliebig verhalten, insbesondere in eine Endlosschleife geraten.

Beachte, dass wir für jede Teilmenge $P \subseteq \mathcal{M}$ zwei Begriffe von Entscheidbarkeit haben: Entscheidbarkeit als Prädikat auf $\mathbb{N}_0^m$ und Entscheidbarkeit als Prädikat relativ zu $\mathcal{M}$. Ist P entscheidbar, so auch als Teilmenge von $\mathcal{M}$. Ist jedoch $\mathcal{M}$ selber nicht entscheidbar, so ist nicht jedes relativ zu $\mathcal{M}$ entscheidbare P schon entscheidbar. Es gilt jedoch:

3.7.2 Bemerkung. Ist $\mathcal{M}$ entscheidbar und P als Teilmenge von $\mathcal{M}$ entscheidbar, so ist P entscheidbar.

Beweis. Wir können P entscheiden, indem wir von jedem $\overrightarrow{x}$ zunächst entscheiden, ob $\overrightarrow{x} \in \mathcal{M}$. Wenn nein, so liegt $\overrightarrow{x}$ nicht in P. Falls ja, so können wir das Entscheidungsverfahren für P als Teilmenge von $\mathcal{M}$ anwenden, um $\overrightarrow{x} \in P$ zu entscheiden. □

3.7.3 Bemerkung. Offensichtlich lassen sich die Sätze 3.3.9 und 3.3.10 problemlos wie folgt verallgemeinern:

1. Die Klasse der relativ zu $\mathcal{M}$ entscheidbaren Prädikate ist unter Vereinigung, Schnitt und Komplement-Bildung in $\mathcal{M}$ abgeschlossen.

2. Sei $B \subseteq \mathcal{N} \subset \mathbb{N}_0^n$ entscheidbar als Teilmenge von $\mathcal{N}$ und $f : \mathcal{M} \longrightarrow \mathcal{N}$ berechenbar. Dann gilt für alle $A \subseteq \mathbb{N}_0^m$ mit

$$f(\overrightarrow{x}) \in B \quad \Longleftrightarrow \quad \overrightarrow{x} \in A$$

   schon, dass A als Teilmenge von $\mathcal{M}$ berechenbar ist.

4 Berechenbarkeit und C^*-Algebren

4.1 Zulässige Abzählungen

Im Folgenden wollen wir Berechenbarkeitsfragen in der Theorie der C^*-Algebren untersuchen. Genauer wollen wir uns mit der Entscheidbarkeit gewisser Teilmengen von C^*-Algebren (dabei wollen wir wieder von Prädikaten sprechen) beschäftigen. Da wir bisher lediglich über Berechenbarkeit von Funktionen und Prädikaten auf den natürlichen Zahlen gesprochen haben, ist zunächst zu klären, was wir im Falle von C^*-Algebren unter Berechenbarkeit verstehen wollen.

Um mit Registermaschinen mit Elementen von C^*-Algebren zu rechnen, werden wir diesen Elementen natürliche Zahlen zuordnen, die diese repräsentieren. (Wir kodieren also Elemente von C^*-Algebren in natürliche Zahlen.) Damit ist jedoch klar, dass wir stets nur über eine abzählbare Teilmenge einer C^*-Algebra $\mathcal{A}$ sprechen können. Im Folgenden werden wir daher stets nur separable[†] C^*-Algebren $\mathcal{A}$ mit einer abzählbaren dichten $\mathbb{Q}(i)$-$*$-Unteralgebra $\widehat{\mathcal{A}}$ betrachten. Diese werden wir so wählen, dass wir die Elemente von $\widehat{\mathcal{A}}$ auf natürliche Weise durch eine Funktion $\varphi : \mathbb{N}_0 \longrightarrow \widehat{\mathcal{A}}$ so abzählen können, dass die Algebren-Verknüpfungen von $\widehat{\mathcal{A}}$ berechenbar werden:

4.1.1 Definition (zulässige Abzählung)**.** Sei $\mathcal{A}$ eine C^*-Algebra und $\widehat{\mathcal{A}}$ eine abzählbare dichte $\mathbb{Q}(i)$-$*$-Unteralgebra von $\mathcal{A}$. Wir nennen eine Abzählung (Bijektion) $\varphi : \mathbb{N}_0 \longrightarrow \widehat{\mathcal{A}}$ *zulässig*, wenn folgende Abbildungen berechenbar sind:

- $f_1 : \mathbb{N}_0^2 \longrightarrow \mathbb{N}_0,\ (x,y) \longmapsto \varphi^{-1}\left(\varphi(x) + \varphi(y)\right)$
- $f_2 : \mathbb{N}_0^2 \longrightarrow \mathbb{N}_0,\ (x,y) \longmapsto \varphi^{-1}\left(\varphi(x) \cdot \varphi(y)\right)$
- $f_3 : \mathbb{N}_0^6 \longrightarrow \mathbb{N}_0,$

$$(x_1, x_2, y_1, y_2, s, z) \longmapsto \begin{cases} \varphi^{-1}\left((-1)^s \frac{x_1 + i x_2}{y_1 + i y_2} \cdot \varphi(z)\right) & y_1 + i y_2 \neq 0 \\ 0 & \text{sonst} \end{cases}$$

- $f_4 : \mathbb{N}_0 \longrightarrow \mathbb{N}_0,\ x \longmapsto \varphi^{-1}\left(\varphi(x)^*\right)$

Für $a \in \widehat{\mathcal{A}}$ werden wir $\varphi^{-1}(a)$ auch den Kode von a nennen.

[†]Eine C^*-Algebra heißt separabel, wenn sie als Banachraum separabel ist.

Es wird in allen von uns betrachteten Fällen klar sein, dass eine solche zulässige Abzählungen stets existiert.

Von einer zulässigen Abzählung φ ausgehend, können wir Teilmengen oder Folgen[†] von Elementen von $\widehat{\mathcal{A}}$ Berechenbarkeit oder Unberechenbarkeit zuschreiben, indem wir eine Teilmenge oder Folge von Elementen von $\widehat{\mathcal{A}}$ (un)berechenbar nennen, falls ihre Urbilder unter φ (un)berechenbar sind:

4.1.2 Definition. Sei $\widehat{\mathcal{A}}$ durch eine zulässige Abzählung φ abgezählt. Wir nennen eine Abbildung $f : \widehat{\mathcal{A}}^m \longrightarrow \widehat{\mathcal{A}}^n$ *berechenbar bezüglich* φ, falls ${\varphi^{(n)}}^{-1} \circ f \circ \varphi^{(m)}$ berechenbar ist.[‡] Analog nennen wir eine Abbildung $g : \mathbb{N}_0^m \longrightarrow \widehat{\mathcal{A}}^n$ *berechenbar bezüglich* φ, falls ${\varphi^{(n)}}^{-1} \circ g$ berechenbar ist.

Ein Prädikat $P \subseteq \widehat{\mathcal{A}}^m$ heiße *entscheidbar bezüglich* φ, falls ${\varphi^{(m)}}^{-1}(P)$ entscheidbar ist.

Analog ist Berechenbarkeit von Funktionen und Prädikaten auf $\widehat{\mathcal{A}}$ relativ zu einer Teilmenge $\mathcal{M} \subseteq \widehat{\mathcal{A}}^m$ zu verstehen.

Ist klar, auf welche zulässige Abzählung wir uns beziehen, so werden wir einfach von berechenbaren Funktionen und Prädikaten sprechen.

Ist nun die Entscheidbarkeit von Teilmengen von $\widehat{\mathcal{A}}$ von der gewählten zulässigen Abzählung abhängig? Dies ist jedenfalls nicht der Fall, wenn $\widehat{\mathcal{A}}$ endlich erzeugt ist!

4.1.3 Satz. *Sei $\mathcal{A}$ eine C^*-Algebra, $\widehat{\mathcal{A}}$ eine endlich erzeugte dichte $\mathbb{Q}(i)$-$*$-Unteralgebra und φ, ψ zulässige Abzählungen von $\widehat{\mathcal{A}}$. Dann sind*

$$\psi^{-1} \circ \varphi : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$

und

$$\varphi^{-1} \circ \psi : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$

berechenbar, und somit sind Funktionen und Prädikate genau dann bezüglich φ berechenbar, wenn sie bezüglich ψ berechenbar sind.

Beweis. Sei $v_1, \ldots, v_n$ ein Erzeugendensystem von $\widehat{\mathcal{A}}$, das ohne Einschränkung unter $*$ abgeschlossen sei. Dann lässt sich jedes Element von $\widehat{\mathcal{A}}$ schreiben als

$$\sum_{i=1}^{k} \lambda_i v_{m_{i,1}} v_{m_{i,2}} \cdots v_{m_{i,l_i}} \qquad k, l_i \in \mathbb{N}, m_{i,j} \in \{1, \ldots n\}, \lambda_i \in \mathbb{Q}(i). \tag{4.1.1}$$

Somit berechnet folgendes Verfahren $\psi^{-1} \circ \varphi(n)$:

[†] Dabei fassen wir eine Folge natürlicher Zahlen als eine Abbildung $\mathbb{N}_0 \to \mathbb{N}_0$ auf.

[‡] $\varphi^{(m)}$ bezeichne die Abbildung $\varphi^{(m)} : \mathbb{N}_0^m \longrightarrow \widehat{\mathcal{A}}^m, \ (x_1, \ldots, x_m) \longmapsto (\varphi(x_1), \ldots, \varphi(x_m))$.

Gehe systematisch alle Summen a der Form (4.1.1) durch.[†] Da φ und ψ zulässig sind, und in diesen Summen nur die endlich vielen Algebren-Elemente $v_1, \ldots, v_n$ vorkommen, deren Kodes bezüglich φ und ψ wir in das Programm hineinkodieren können, lassen sich jeweils $\varphi^{-1}(a)$ und $\psi^{-1}(a)$ berechnen. Da jedes Element von $\widehat{\mathcal{A}}$ von der Form (4.1.1) ist, kommen wir schließlich zu einem $a \in \widehat{\mathcal{A}}$, sodass $\varphi^{-1}(a) = n$ ist. Dann ist aber $\psi^{-1} \circ \varphi(n) = \psi^{-1}(a)$. Analoges gilt für $\varphi^{-1} \circ \psi$.

Dass in dieser Situation die φ-berechenbaren Funktionen und Prädikate mit den ψ-berechenbaren Funktionen und Prädikaten übereinstimmen, folgt sofort aus der Definition und Satz 3.3.10 bzw. Bemerkung 3.7.3 . □

In vielen Fällen müssen wir uns also nicht um die Wahl der zulässigen Abzählung φ sorgen.

Bezüglich der Frage, inwiefern unsere Begriffsbildung von Berechenbarkeit in C^*-Algebren sinnvoll ist, verweisen wir auf die abschließende Diskussion in Kapitel 7.

Wie schon in Bemerkung 3.3.8 angemerkt, werden wir beim Beweis der Entscheidbarkeit eines Prädikats auf einer C^*-Algebra großzügig damit sein, einer gewissen Operation Berechenbarkeit zuzuschreiben, insofern, als dass wir Verfahren zu ihrer Durchführung nur soweit spezifizieren werden, dass ihre Umsetzbarkeit in ein Computerprogramm klar wird, ohne dass wir jedoch ein konkretes Programm angeben werden. Etwa sind aus der Linearen Algebra Verfahren bekannt, die lineare Unabhängigkeit von Vektoren des $\mathbb{Q}(i)^n$ zu prüfen, derer wir uns ohne nähere Angabe eines konkreten Computer- oder gar Registermaschinen-Programms bedienen werden, von denen jedoch klar ist, dass eine solche Umsetzung ohne Probleme möglich ist.

Dies gilt auch, wenn wir von der Existenz von zulässigen Abzählungen sprechen. Folgende Bemerkung zeigt dabei, dass wir in vielen Fällen auf kanonische Weise ähnlich zu dem Vorgehen in Satz 4.1.3 eine zulässige Abzählung erhalten können:

4.1.4 Bemerkung. Sei $\widehat{\mathcal{A}}$ dichte $\mathbb{Q}(i)$-$*$-Unteralgebra einer C^*-Algebra $\mathcal{A}$ sowie (v_i), $i \in I$ ein endliches oder abzählbar unendliches System von Erzeugern von $\widehat{\mathcal{A}}$, von dem wir wieder ohne Einschränkung annehmen können, dass es $*$-abgeschlossen ist. Dann lässt sich wie folgt eine zulässige Abzählung φ von $\widehat{\mathcal{A}}$ finden.

Definiere $\varphi(n)$ rekursiv:

Seien $\varphi(m)$ für $m < n$ schon definiert. Um $\varphi(n)$ zu definieren, gehe (nach dem

[†]Damit meinen wir genauer Folgendes: Repräsentiere Summen der Form (4.1.1) durch bestimmte endliche Folgen natürlicher Zahlen (welche sich wiederum vermittels Kodierung als eine natürliche Zahl schreiben lassen) so, dass sich diese Folgen in berechenbarer Weise aufzählen lassen und des Weiteren die *formalen* Algebrenoperationen auf diesen Ausdrücken in dieser Repräsentation berechenbar sind. (D. h. es sollen nicht die möglichen zusätzliche Relationen in $\widehat{\mathcal{A}}$ gelten. Anders gesagt, wir rechnen in der von den Erzeugern erzeugten *freien* $*$-Algebra)

immer gleichen System) systematisch alle Ausdrücke der Form

$$\sum_{i=1}^{k} \lambda_i v_{m_{i,1}} v_{m_{i,2}} \cdots v_{m_{i,l_i}} \qquad k, l_i \in \mathbb{N}, m_{i,j} \in I, \lambda_i \in \mathbb{Q}(i) \tag{4.1.2}$$

durch.[†] Für jeden Ausdruck a dieser Form prüfe für jedes $m < n$:

1. Sei a_m derjenige Ausdruck, der nach diesem Verfahren für $\varphi(m)$ bereits ausgewählt wurde ($\varphi(m) = a_m$).

2. Gilt in $\widehat{\mathcal{A}}$, dass $a = a_m$? Falls ja, verwerfe a, sonst weiter mit $m + 1$, falls $m + 1 < n$.

Wurde a nicht verworfen, so setze $\varphi(n) := a$.

Offensichtlich definiert dies eine Abzählung $\varphi : \mathbb{N}_0 \longrightarrow \widehat{\mathcal{A}}$. Diese Abzählung ist zulässig, falls es zu $\widehat{\mathcal{A}}$ ein Entscheidungsverfahren gibt, dass für einen Ausdruck a der Form (4.1.2), also unter Kenntnis der λ_i und $m_{i,j}$ prüft, ob $a = 0$ in $\widehat{\mathcal{A}}$ gilt.

Wir zeigen dies für den Fall der Addition: Es ist also $f_1(x, y) = \varphi^{-1}(\varphi(x) + \varphi(y))$ zu berechnen. Dies leistet das folgende Verfahren.

1. Bestimme ein a der Form (4.1.2), sodass $\varphi(x) = a$. Dies ist möglich, indem wir obige rekursive Definition von $\varphi(x)$ als Berechnungsverfahren verwenden. (Dazu müssen wir nach dem gleichen Verfahren also zunächst $\varphi(0), \varphi(1), \dots, \varphi(x-1)$ bestimmen.) Für Schritt 2 ist wesentlich, dass wir nach Voraussetzung gerade ein Entscheidungsverfahren haben, um $a = a_n \;\Leftrightarrow\; a - a_n = 0$ in $\widehat{\mathcal{A}}$ zu testen.

2. Bestimme ein b der Form (4.1.2), sodass $\varphi(y) = b$.

3. Ermittle die Form des Ausdrucks $a+b$, also die zugehörigen λ_i und $m_{i,j}$ in (4.1.2.

4. Für jedes n bestimme bei 0 beginnend, wie oben einen Ausdruck c, sodass $\varphi(n) = c$. Falls $c - (a + b) \neq 0$ in $\widehat{\mathcal{A}}$, so fahre bei $n + 1$ fort. Andernfalls ist $\varphi^{-1}(\varphi(x) + \varphi(y)) = n$.

Mit Hilfe des Verfahrens aus dieser Bemerkung erhalten wir in allen von uns untersuchten Fällen zulässige Abzählungen. Außer für die Algebra $\mathcal{O}_2$ werden wir dabei allerdings nicht näher darauf eingehen, wie zu entscheiden ist, ob ein Ausdruck der Form (4.1.2) gleich 0 ist, da dies sonst stets direkt klar sein wird.

[†]Siehe Fußnote zu 4.1.3.

5 Von zwei Isometrien erzeugte C^*-Algebren

5.1 Isometrien

Im Folgenden werden wir uns besonders für C^*-Algebren interessieren, die von Isometrien erzeugt werden.

5.1.1 Definition (Isometrie, Projektion)**.** Ein Element s einer unitalen C^*-Algebra heißt *Isometrie*, falls gilt

$$s^*s = 1.$$

s heißt *echte* Isometrie, falls $ss^* \neq 1$, ansonsten heißt s *unitär*. Ein Element p einer C^*-Algebra heißt *Projektion*, falls

$$p^* = p \quad \text{und} \quad p^2 = p.$$

Zwei Projektionen p, q heißen *orthogonal*, falls

$$pq = 0.$$

5.1.2 Bemerkung. Ist s eine Isometrie, so gilt $\|s\| = 1$ und ss^* ist eine Projektion, die als *Bildprojektion* bezeichnet wird. Produkte von Isometrien sind Isometrien.

Beweis. Es gilt

$$\|s\|^2 = \|s^*s\| = \|1\| = 1$$

und $(ss^*)^* = ss^*$, sowie

$$(ss^*)(ss^*) = s\underbrace{(s^*s)}_{1}s^* = ss^*.$$

Ist t eine weitere Isometrie, so gilt auch

$$(st)^*(st) = t^*s^*st = t^*1t = 1.$$

□

5.1.3 Bemerkung. Isometrien und Projektionen von dargestellten C^*-Algebren sind gerade Isometrien und orthogonale Projektionen im Sinne der Funktionalanalysis, und der Projektionsraum der Bildprojektion einer Isometrie ist das Bild der Isometrie. Zwei Projektionen sind orthogonal genau dann, wenn ihre Projektionsräume orthogonal sind.

Beweis. Alle Aussagen folgen leicht aus der Tatsache, dass

$$(S\xi \mid \eta) = (\xi \mid S^*\eta) \qquad \forall \xi, \eta \in \mathcal{H}.$$

Siehe [Wer], Lemma V.5.4 und Satz V.5.9 . □

Wird eine C^*-Algebra $\mathcal{A}$ von zwei Isometrien mit orthogonalen Bildprojektionen s_1, s_2 erzeugt, so hat die von s_1, s_2 erzeugte $\mathbb{Q}(i)$-$*$-Unteralgebra eine besonders einfache Form.

Sei dazu für $\mu = (k_1 k_2 \dots k_m) \in \{1,2\}^+$

$$s_\mu := s_{k_1} s_{k_2} \dots s_{k_m} \qquad \text{und also} \qquad s_\mu^* = s_{k_m}^* s_{k_{m-1}}^* \dots s_{k_1}^*,$$

sowie $s_{\sqcup} = 1$.

5.1.4 Lemma. *Sei $\mathcal{A}$ eine von Isometrien s_1, s_2 mit orthogonalen Bildprojektionen erzeugte C^*-Algebra. Dann gilt*

$$s_1^* s_2 = 0 \quad \textit{und} \quad s_2^* s_1 = 0.$$

Beweis. Um die erste Gleichung einzusehen, multipliziere die nach Voraussetzung geltende Gleichung

$$s_1 s_1^* s_2 s_2^* = 0$$

von links mit s_1^* und von rechts mit s_2. Die zweite Gleichung wird analog gezeigt. □

5.1.5 Korollar. *Sei $\widehat{\mathcal{A}}$ die von s_1, s_2 erzeugte $\mathbb{Q}(i)$-$*$-Unteralgebra von $\mathcal{A}$. Es gilt*

1. *Sei $s_\mu^* s_\nu \neq 0$. Dann gilt*

   a) *Falls $|\mu| = |\nu|$, dann $\mu = \nu$ und $s_\mu^* s_\nu = 1$.*

   b) *Falls $|\mu| < |\nu|$, so gibt es ein $\nu' \in \{1,2\}^{|\nu|-|\mu|}$ mit $\nu = \mu\nu'$ und $s_\mu^* s_\nu = s_{\nu'}$.*

   c) *Falls $|\nu| < |\mu|$, so gibt es ein $\mu' \in \{1,2\}^{|\mu|-|\nu|}$ mit $\mu = \nu\mu'$ und $s_\mu^* s_\nu = s_{\mu'}^*$.*

2. *Jedes $x \in \widehat{\mathcal{A}}$ ist von der Form*

$$x = \sum_{i=1}^{k} \lambda_i s_{\mu_i} s_{\nu_i}^* \qquad \lambda_i \in \mathbb{Q}(i), \mu_i, \nu_i \in \{1,2\}^*. \tag{5.1.1}$$

Beweis. Der erste Teil folgt leicht durch Induktion nach der Länge von μ und η aus Lemma 5.1.4.

Der zweite Teil folgt dann aus 1. und daraus, dass jedes Element von $\widehat{\mathcal{A}}$ in der Form (4.1.2) geschrieben werden kann. □

5.1.6 Beispiel. Sei $\mathcal{H}$ ein separabler Hilbertraum mit Orthonormalbasis $(\xi_i)_{i\in\mathbb{N}}$. Die Operatoren S_1 und S_2, erklärt durch

$$\begin{aligned} S_1 : \mathcal{H} &\longrightarrow \mathcal{H} \\ \xi_i &\longmapsto \xi_{2i-1} \end{aligned}$$

und

$$\begin{aligned} S_2 : \mathcal{H} &\longrightarrow \mathcal{H} \\ \xi_i &\longmapsto \xi_{2i} \end{aligned}$$

sind Isometrien mit orthogonalen Bildern.

Zusätzlich ist die orthogonale Summe der Bildräume von S_1 und S_2 schon ganz $\mathcal{H}$, d.h. es gilt

$$S_1S_1^* + S_2S_2^* = 1. \tag{5.1.2}$$

Wir bezeichnen die von S_1 und S_2 erzeugte C^*-Algebra mit $\mathcal{O}_2$.

5.1.7 Bemerkung. Die Algebra $\mathcal{O}_2$ hat viele interessante Eigenschaften und spielt eine wichtige Rolle in der Theorie der C^*-Algebren. Insbesondere gilt, dass $\mathcal{O}_2$ einfach und rein unendlich ist, und dass jede von Isometrien s_1, s_2 erzeugte C^*-Algebra mit

$$s_1s_1^* + s_2s_2^* = 1$$

bereits isomorph zu $\mathcal{O}_2$ ist. Somit lässt sich $\mathcal{O}_2$ also auch als die von den Relationen

$$s_1^*s_1 = 1 \qquad s_2^*s_2 = 1 \qquad s_1s_1^* + s_2s_2^* = 1$$

erzeugte unitale *universelle C^*-Algebra* definieren. (Dies ist die übliche Definition.) Siehe [Cun] oder [Dav], Kapitel V.

5.1.8 Bemerkung. Für $\mathcal{A} = \mathcal{O}_2$ existiert eine zulässige Abzählung der von S_1, S_2 erzeugten $\mathbb{Q}(i)$-$*$-Algebra $\widehat{\mathcal{A}}$.

Beweis. Aufgrund von Bemerkung 4.1.4 reicht es zu entscheiden, wann ein $A \in \widehat{\mathcal{A}}$ der Form (5.1.1) gleich 0 ist. (Wir durchlaufen also nur Elemente der spezielleren Form (5.1.1) statt der Form (4.1.2), was jedoch sicherlich kein Problem darstellt.)

Nun folgt aus (5.1.2) leicht durch Induktion nach k, dass auch

$$\sum_{\mu\in\{1,2\}^k} s_\mu s_\mu^* = 1. \tag{5.1.3}$$

Sei n die maximale Länge der Worte der ν_i die in der Darstellung von a auftreten. Dann können wir durch Einfügen von Summen der Form (5.1.3) eine Darstellung für a erhalten, in der alle ν_i die Länge n haben:

$$a = \sum_{i=1}^{k} \lambda_i s_{\mu_i} s_{\nu_i}^* = \sum_{i=1}^{k} \lambda_i s_{\mu_i} \Big(\sum_{\eta \in \{1,2\}^{n-|\nu_i|}} s_\eta s_\eta^* \Big) s_{\nu_i}^*.$$

Die neue Darstellung ergibt sich offensichtlich in berechenbarer Weise aus der alten Darstellung.

Es gelte also ohne Einschränkung $|\nu_i| = n$ für alle i, und weiter können wir durch Zusammenfassen annehmen, dass für $i \neq j$ gilt, dass $\nu_i = \nu_j \Rightarrow \mu_i \neq \mu_j$. Wir behaupten, dass dann $a = 0$ in $\mathcal{O}_2$ genau dann gilt, wenn $\lambda_i = 0 \ \forall i$, womit wir das gesuchte Entscheidungsverfahren gefunden hätten.

Sei $a = 0$ in $\mathcal{O}_2$ und es gebe ein i mit $\lambda_i \neq 0$. Sei i_0 so, dass μ_{i_0} von maximaler Länge unter allen μ_i mit $\lambda_i \neq 0$ ist. Da alle ν_i die gleiche Länge haben, ergibt Rechtsmultiplikation mit $s_{\nu_{i_0}}$ nach Korollar 5.1.5

$$0 = a s_{\nu_{i_0}} = \sum_{\nu_i = \nu_{i_0}} \lambda_i s_{\mu_i}.$$

Hat μ_{i_0} die Länge 0, so erhalten wir aufgrund der Maximalität der Länge den Widerspruch $0 = a s_{\nu_{i_0}} = \lambda_{i_0} 1 \implies \lambda_{i_0} = 0$. Also hat μ_{i_0} mindestens die Länge 1.

Linksmultiplikation mit $s_{\mu_{i_0}}^*$ ergibt weiter

$$0 = s_{\mu_{i_0}}^* a s_{\nu_{i_0}} = \sum_{\substack{\nu_i = \nu_{i_0} \\ \mu_{i_0} = \mu_i \eta_i}} \lambda_i s_{\eta_i}^*,$$

denn μ_{i_0} hat maximale Länge, und es ist nur dann $s_{\mu_{i_0}}^* s_{\mu_i} \neq 0$, wenn μ_i ein Anfangsstück von μ_{i_0} ist.

Habe μ_{i_0} die Form $(x_1 x_2 \ldots x_l)$. Setze $y := 1$, falls $x_l = 2$, und $y := 2$, falls $x_l = 1$. Dann gilt

$$0 = s_{\mu_{i_0}}^* a s_{\nu_{i_0}} s_y^l = \lambda_{i_0} s_y^l,$$

denn falls η_i ein Endstück von μ_{i_0} einer Länge größer 0 ist (und dies ist genau dann der Fall, wenn $i \neq i_0$), so gilt $s_{\eta_i}^* s_y^l = 0$.

Also gilt $\lambda_{i_0} = 0$. Widerspruch! □

Die Existenz einer zulässigen Abzählung und auch z. B. das gerade angegebene Verfahren, um $a = 0$ in $\widehat{\mathcal{A}}$ zu entscheiden, zeigen, dass wir die Struktur von $\widehat{\mathcal{A}}$ recht gut im Griff haben. Im Kontrast dazu stehen die Ergebnisse des nächsten Abschnitts.

5.2 Das Hauptresultat

Die interessanten kombinatorischen Eigenschaften der Multiplikation von Worten in den Erzeugern von C^*-Algebren, die von zwei Isometrien mit orthogonalen Bildern erzeugt werden, und die Möglichkeit, durch Grenzübergang unendliche Produkte zu betrachten, lassen es vorstellbar erscheinen, dass sich in solchen Algebren die Rechnung einer Registermaschine simulieren lässt, wobei Multiplikation mit einem gewissen Element der Algebra als ein Rechenschritt und der Grenzübergang zu einem unendlichen Produkt als der Gesamtlauf des Programms zu interpretieren wäre. Dann würden in natürlicher Weise unentscheidbare, durch Multiplikation und Grenzwertbildung definierte Prädikate in der Algebra auftreten.

Dass dies tatsächlich so ist, zeigt der folgende

5.2.1 Satz. *Sei $\mathcal{A}$ eine von Isometrien s_1, s_2 mit orthogonalem Bild erzeugte C^*-Algebra und $\widehat{\mathcal{A}}$ die von s_1 und s_2 erzeugte $\mathbb{Q}(i)$-$*$-Unteralgebra, sowie φ eine zulässige Abzählung von $\widehat{\mathcal{A}}$. Weiter sei*

$$\mathcal{S} := \left\{ \lambda s_1^z s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2 \middle| \lambda \in \mathbb{Q}(i)\ z, r_1, \ldots, r_q \in \mathbb{N}_0 \right\}.$$

Dann existieren Elemente $a, b \in \mathcal{A}$, sodass gilt:

1. *Es gibt berechenbare Folgen $(a_k), (b_k)$ aus $\widehat{\mathcal{A}}$, die gegen a bzw. b konvergieren, mit $\|a - a_k\| \leq \frac{1}{k}\ \forall k$ und $\|b - b_k\| \leq \frac{1}{k}\ \forall k$.*

2. *$ax, bx \in \mathcal{S}\ \ \forall x \in \mathcal{S}$, und die Abbildungen*

$$M_a : \mathcal{S} \longrightarrow \mathcal{S},\ x \longmapsto ax$$

und

$$M_b : \mathcal{S} \longrightarrow \mathcal{S},\ x \longmapsto bx$$

sind berechenbar.

3. *Die Prädikate*

$$\left\{ x \in \mathcal{S} \;\middle|\; \lim_{n\to\infty} a^n x = 0 \right\} \subseteq \mathcal{S} \tag{5.2.1}$$

und

$$\left\{ x \in \mathcal{S} \;\middle|\; \exists n \in \mathbb{N} : b^n x = 0 \right\} \subseteq \mathcal{S} \tag{5.2.2}$$

sind als Teilmengen von $\mathcal{S}$ nicht entscheidbar.

Beweis. Im Folgenden werden wir ein Element a von $\mathcal{A}$ mit den gewünschten Eigenschaften konstruieren, indem wir die Elemente von $\mathcal{S}$ als Konfigurationen einer Registermaschine $\mathbb{M}$ interpretieren und a so definieren, dass Linksmultiplikation mit a an ein Element von $\mathcal{S}$ gerade einem Rechenschritt von $\mathbb{M}$ entspricht und dabei gilt, dass

$a^n x$ genau dann gegen 0 konvergiert, wenn $\mathbb{M}$, auf die x entsprechende Konfiguration angesetzt, in eine Endlosschleife gerät.

Nun ist nach Korollar 3.6.2 das diagonalisierte Halteproblem H^1 rekursiv aufzählbar und also die Funktion

$$f : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$
$$x \longmapsto \begin{cases} 1 & x \in H^1 \\ \uparrow & x \notin H^1 \end{cases}$$

partiell berechenbar. Wählen wir $\mathbb{M} := \left(\mathcal{R}_q^{1,1}, \mathcal{P}_f\right)$ als eine Registermaschine, die f berechnet, so ist nach Satz 3.5.2 nicht entscheidbar, für welchen Input x die Maschine $\mathbb{M}$ in eine Endlosschleife gerät. (Denn dies ist gerade das Komplement von H^1 und $\mathbb{P}^1$ ist unter Komplementen abgeschlossen.) Dann kann aber auch das Prädikat (5.2.1) als Teilmenge von $\mathcal{S}$ nicht entscheidbar sein …

Ohne Einschränkung habe $\mathcal{P}_f$ genau einen Endzustand z_e. (Ansonsten ersetze alle Endzustände in $\mathcal{P}_f$ durch einen festen Endzustand z_e.)

Um nun a zu konstruieren, müssen wir 1. Konfigurationen von $\mathbb{M}$ Elemente von $\mathcal{S}$ zuordnen, 2. Modifikations- und Testinstruktionen, sowie 3. Anweisungen als Elemente von $\mathcal{A}$ interpretieren und schließlich 4. aus diesen einzelnen Anweisungen a konstruieren. Im Folgenden werden wir dabei regen Gebrauch von Korollar 5.1.5 machen, ohne allerdings darauf jedes Mal explizit zu verweisen.

1. Wir übertragen Konfigurationen von $\mathbb{M}$ auf Elemente von $\mathcal{S}$ vermittels:

$$\phi : K(\mathbb{M}) \longrightarrow \mathcal{S}$$
$$(z, (r_1, \ldots, r_q)) \longmapsto s_1^z s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2$$

2. Für die Instruktionen INC_m von $\mathcal{R}_q^{1,1}$ setzen wir

$$\overline{\mathrm{INC}}_1 := \frac{1}{2} s_1,$$

sowie für $m = 2, \ldots, q$ und $n \in \mathbb{N}_0$

$$\overline{\mathrm{INC}}_{m,n} := \sum_{i_1+\ldots+i_{m-1}=n} (s_1^{i_1} s_2 \ldots s_1^{i_{m-1}} s_2) s_1 (s_2^* s_1^{*i_{m-1}} s_2^* \ldots s_2^* s_1^{*i_1}).$$

Dabei entspricht die Linksmultiplikation eines Summanden

$$(s_1^{i_1} s_2 \ldots s_1^{i_{m-1}} s_2) s_1 (s_2^* s_1^{*i_{m-1}} s_2^* \ldots s_2^* s_1^{*i_1})$$

an ein Element der Form

$$x = \lambda s_1^{r_1} s_2 \cdots s_1^{r_q} s_2{}^{\dagger}$$

gerade der Ausführung der Instruktion INC_m, falls

$$x = \lambda s_1^{i_1} s_2 \cdots s_1^{i_{m-1}} s_2 x',$$

also x einem Registerstand $\overrightarrow{r}$ von $\mathbb{M}$ entspricht mit $r_1 = i_1, \ldots, r_{m-1} = i_{m-1}$. Andernfalls ist das Produkt mit diesem Summanden 0. Um alle möglichen Registerinhalte von $\mathbb{M}$ abzudecken, muss noch über n summiert werden:

$$\overline{\mathrm{INC}}_m := \sum_{n=0}^{\infty} \frac{1}{2^{n+1}(n+1)^{m-1}} \overline{\mathrm{INC}}_{m,n}.$$

Die Koeffizienten $\frac{1}{2^{n+1}(n+1)^{m-1}}$ sind so gewählt, dass die Reihe absolut konvergiert und jeder Summand eine Norm echt kleiner 1 hat. Denn es gilt

$$\left\| (s_1^{i_1} s_2 \ldots s_1^{i_{m-1}} s_2) s_1 (s_2^* s_1^{*i_{m-1}} s_2^* \ldots s_2^* s_1^{*i_1}) \right\| \leq 1,$$

also

$$\begin{aligned} \left\|\overline{\mathrm{INC}}_{m,n}\right\| \leq \left|\left\{(i_1, \ldots, i_{m-1}) \in \mathbb{N}_0^{m-1} \;\middle|\; i_1 + \cdots + i_{m-1} = n\right\}\right| \cdot 1 \\ < (n+1)^{m-1}. \end{aligned}$$

Analog setzen wir für für die Instruktionen DEC_m

$$\overline{\mathrm{DEC}}_1 := \frac{1}{2} s_1^* + \frac{1}{2} s_2 s_2^*,$$

und für $m = 2, \ldots, q, n \in \mathbb{N}_0$

$$\begin{aligned} \overline{\mathrm{DEC}}_{m,n} := & \sum_{i_1 + \ldots + i_{m-1} = n} (s_1^{i_1} s_2 \ldots s_1^{i_{m-1}} s_2) s_1^* (s_2^* s_1^{*i_{m-1}} s_2^* \ldots s_2^* s_1^{*i_1}) + \\ & \sum_{i_1 + \ldots + i_{m-1} = n} (s_1^{i_1} s_2 \ldots s_1^{i_{m-1}} s_2) s_2 s_2^* (s_2^* s_1^{*i_{m-1}} s_2^* \ldots s_2^* s_1^{*i_1}) \end{aligned}$$

sowie

$$\overline{\mathrm{DEC}}_m := \sum_{n=0}^{\infty} \frac{1}{2^{n+1}(n+1)^{m-1}} \overline{\mathrm{DEC}}_{m,n}.$$

Hier treten jeweils zwei Summanden auf, da die Fälle $r_m \neq 0$ (1. Summand) und $r_m \neq 0$ (2. Summand) zu unterscheiden sind. Das Produkt mit dem jeweils anderen Summanden ergibt 0.

† Gegenüber den Elementen von $\mathcal{S}$ fehlt hier also $s_1^z s_2$!

Schließlich definieren wir für die Instruktionen $\mathrm{EQ0}_m$

$$\overline{\mathrm{EQ0}}_1 := \frac{1}{2} s_2 s_2^* \qquad \overline{\mathrm{EQ0}}'_1 := \frac{1}{2}(1 - s_2 s_2^*),$$

sowie für $m = 2, \dots, q, n \in \mathbb{N}_0$

$$\overline{\mathrm{EQ0}}_{m,n} := \sum_{i_1+\ldots+i_{m-1}=n} (s_1^{i_1} s_2 \dots s_1^{i_{m-1}} s_2) s_2 s_2^* (s_2^* s_1^{*i_{m-1}} s_2^* \dots s_2^* s_1^{*i_1}),$$

$$\overline{\mathrm{EQ0}}_m := \sum_{n=0}^{\infty} \frac{1}{2^{n+1}(n+1)^{m-1}} \overline{\mathrm{EQ0}}_{m,n},$$

$$\overline{\mathrm{EQ0}}'_{m,n} := \sum_{i_1+\ldots+i_{m-1}=n} (s_1^{i_1} s_2 \dots s_1^{i_{m-1}} s_2)(1 - s_2 s_2^*)(s_2^* s_1^{*i_{m-1}} s_2^* \dots s_2^* s_1^{*i_1}),$$

$$\overline{\mathrm{EQ0}}'_m := \sum_{n=0}^{\infty} \frac{1}{2^{n+1}(n+1)^{m-1}} \overline{\mathrm{EQ0}'}_{m,n}.$$

$\overline{\mathrm{EQ0}}_m$ und $\overline{\mathrm{EQ0}}'_m$ sind jeweils so gewählt, dass Linksmultiplikation an ein x wie oben dieses x unverändert lässt, falls $r_m = 0$, jedoch 0 ergibt, falls $r_m \neq 0$ (für $\overline{\mathrm{EQ0}}_m$), bzw. umgekehrt 0 ergibt, falls $r_m = 0$, und x unverändert lässt, falls $r_m \neq 0$ (für $\overline{\mathrm{EQ0}}'_m$).

3. Die verschiedenen Typen von Anweisungen, die in $\mathcal{P}_f$ auftreten können, übersetzen wir wie folgt:

$$\overline{(z, \mathrm{INC}_m, z_f)} := s_1^{z_f} s_2 \overline{\mathrm{INC}}_m s_2^* s_1^{*z},$$

$$\overline{(z, \mathrm{DEC}_m, z_f)} := s_1^{z_f} s_2 \overline{\mathrm{DEC}}_m s_2^* s_1^{*z},$$

$$\overline{(z, \mathrm{EQ0}_m, z_f, z_v)} := \left(s_1^{z_f} s_2 \overline{\mathrm{EQ0}}_m + s_1^{z_v} s_2 \overline{\mathrm{EQ0}}'_m \right) s_2^* s_1^{*z}.$$

4. Schließlich sei

$$a := \sum_{P \in \mathcal{P}} \overline{P} + s_1^{z_e} s_2 s_2^* s_1^{*z_e}.$$

Zunächst zeigen wir, dass a Aussage 1 erfüllt. Dazu setzen wir:

$$\begin{aligned}
\overline{(z,\mathrm{INC}_1,z_f)}_k &:= \overline{(z,\mathrm{INC}_1,z_f)} \\
\overline{(z,\mathrm{INC}_m,z_f)}_k &:= (s_1^{z_f}s_2)\sum_{i=0}^{k}\frac{1}{2^{n+1}(n+1)^{m-1}}\overline{\mathrm{INC}}_{m,n}(s_2^* s_1^{*z}) && m=2,\dots,q \\
\overline{(z,\mathrm{DEC}_1,z_f)}_k &:= \overline{(z,\mathrm{DEC}_1,z_f)} \\
\overline{(z,\mathrm{DEC}_m,z_f)}_k &:= (s_1^{z_f}s_2)\sum_{i=0}^{k}\frac{1}{2^{n+1}(n+1)^{m-1}}\overline{\mathrm{DEC}}_{m,n}(s_2^* s_1^{*z}) && m=2,\dots,q \\
\overline{(z,\mathrm{EQ0}_1,z_f,z_v)}_k &:= \overline{(z,\mathrm{EQ0}_1,z_f,z_v)} \\
\overline{(z,\mathrm{EQ0}_m,z_f,z_v)}_k &:= \Bigg((s_1^{z_f}s_2)\sum_{i=0}^{k}\frac{1}{2^{n+1}(n+1)^{m-1}}\overline{\mathrm{EQ0}}_{m,n}+ \\
&\qquad (s_1^{z_v}s_2)\sum_{i=0}^{k}\frac{1}{2^{n+1}(n+1)^{m-1}}\overline{\mathrm{EQ0}'}_{m,n}\Bigg)s_2^* s_1^{*z} && m=2,\dots,q
\end{aligned}$$

Nun ist es aufgrund der Wahl der Koeffizienten in den Summen, die $\overline{\mathrm{INC}}_m$, $\overline{\mathrm{DEC}}_m$, $\overline{\mathrm{EQ0}}_m$ und $\overline{\mathrm{EQ0}}'_m$ definieren, klar, dass es ein $K \in \mathbb{N}$ gibt, sodass für jede Anweisung $P \in \mathcal{P}$

$$\left\|\overline{P} - \overline{P}_{k+K}\right\| \leq \frac{1}{|\mathcal{P}_f| \cdot k}$$

ist. Dann folgt für $a_k := \sum_{P \in \mathcal{P}_f} \overline{P}_{k+K} + s_1^{z_e} s_2 s_2^* s_2^{*z_e}$

$$\|a - a_k\| \leq \frac{1}{k}.$$

Es bleibt zu verifizieren, dass die Folge $\varphi^{-1}(a_n)$ berechenbar ist. Dies ist jedoch klar aufgrund der Zulässigkeit von φ und der Tatsache, dass wir $\varphi^{-1}(s_1)$ und $\varphi^{-1}(s_2)$ in das Programm zur Berechnung von $\varphi^{-1}(a_n)$ hineinkodieren können. (Denn die Form der *endlichen* Mehrfachsumme a_k hängt in berechenbarer Weise von k ab.)

Als Nächstes wollen wir prüfen, ob unsere Definition von a unser Ziel verwirklicht, dass Linksmultiplikation von a an ein $x \in \mathcal{S}$ einem Rechenschritt von $\mathbb{M}$ entspricht. Damit meinen wir, dass das Diagramm

$$\begin{tikzcd}
K(\mathbb{M}) \arrow[r, "\phi"] \arrow[d, "\mathrm{RS}_{\mathbb{M}}"'] & \mathcal{S} \arrow[d, "M_a"] \\
K(\mathbb{M}) \arrow[r, "\phi"] & \mathcal{S}
\end{tikzcd} \tag{5.2.3}$$

kommutiert.

Sei dazu $(z, \overrightarrow{r})$ eine beliebige Konfiguration von $\mathbb{M}$ und setze

$$x := \phi\,(z, \overrightarrow{r}) = s_1^z s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2.$$

Nun ist z entweder der Endzustand z_e von $\mathbb{M}$, oder nicht:

1. $z = z_e$. Sei $P \in \mathcal{P}_f$ beliebig. Dann hat $\overline{P}$ die Form $\overline{P} = Q s_2^* s_1^{*z'}$ mit $z' \neq z$. Also gilt
$$\overline{P}x = Q(s_2^* s_1^{*z'})(s_1^z s_2) s_1^{r_1} s_2 \cdots s_1^{r_q} s_2 = 0.$$
Daher:
$$\begin{aligned} ax &= \left(\sum_{P \in \mathcal{P}_f} \overline{P} + s_1^{z_e} s_2 s_2^* s_1^{*z_e} \right) (s_1^{z_e} s_2) s_1^{r_1} s_2 \cdots s_1^{r_q} s_2 \\ &= 0 + s_1^{z_e} s_2 (s_2^* s_1^{*z_e})(s_1^{z_e} s_2) s_1^{r_1} s_2 \cdots s_1^{r_q} s_2 \\ &= s_1^{z_e} s_2 s_1^{r_1} \cdots s_1^{r_q} s_2 = x. \end{aligned}$$
Da weiter $(z_e, \overrightarrow{r})$ eine Endkonfiguration von $\mathbb{M}$ ist, gilt nach Definition von $\mathrm{RS}_{\mathbb{M}}$, dass $\mathrm{RS}_{\mathbb{M}}\,(z_e, \overrightarrow{r}) = (z_e, \overrightarrow{r})$. Somit kommutiert Diagramm 5.2.3.

2. $z \neq z_e$. Da z kein Endzustand ist, existiert genau ein $P \in \mathcal{P}_f$ mit z als Ausgangszustand. Wie in 1. folgt für jedes andere $P' \in \mathcal{P}_f$
$$\overline{P'}x = 0,$$
sowie
$$s_1^{z_e} s_2 s_2^* s_1^{*z_e} x = 0,$$
also
$$ax = \overline{P}x.$$
Die Anweisung P kann drei verschiedene Typen von Instruktionen beinhalten: $\mathrm{INC}_m, \mathrm{DEC}_m, \mathrm{EQ0}_m$. Wir unterscheiden diese drei Fälle:

   a) $P = (z, \mathrm{INC}_m, z_f)$. Nach Definition von $\overline{P}$ und $\overline{\mathrm{INC}}_m$, sowie wieder Korollar 5.1.5, haben wir für $m = 1$
$$\begin{aligned} \overline{P}x &= \left(s_1^{z_f} s_2 \overline{\mathrm{INC}}_1 s_2^* s_1^{*z}\right) \left(s_1^z s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2\right) \\ &= s_1^{z_f} s_2 \overline{\mathrm{INC}}_1 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2 \\ &= \frac{1}{2} s_1^{z_f} s_2 s_1^{r_1+1} s_2 \cdots s_1^{r_q} s_2 \\ &= \frac{1}{2} \phi(z_f, (r_1+1, r_2, \ldots, r_q)) \end{aligned}$$

und für $m = 2, \ldots, q$

$$\begin{aligned}
\overline{P}x &= \left(s_1^{z_f} s_2 \overline{\mathrm{INC}}_m s_2^* s_1^{*z}\right) \left(s_1^z s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2\right) \\
&= s_1^{z_f} s_2 \overline{\mathrm{INC}}_m s_1^{r_1} s_2 \cdots s_1^{r_q} s_2 \\
&= s_1^{z_f} s_2 \sum_{n=0}^{\infty} \frac{1}{2^{n+1}(n+1)^{m-1}} \quad \cdot \\
&\qquad \sum_{i_1+\ldots+i_{m-1}=n} \Big[(s_1^{i_1} s_2 \ldots s_1^{i_{m-1}} s_2) s_1 (s_2^* s_1^{*i_{m-1}} s_2^* \ldots s_2^* s_1^{*i_1}) \cdot \\
&\qquad\qquad (s_1^{r_1} s_2 \cdots s_1^{r_{m-1}} s_2) s_1^{r_m} s_2 (s_1^{r_{m+1}} \cdots s_1^{r_q} s_2) \Big] .
\end{aligned}$$

In dieser Doppelsumme ist erneut nach Korollar 5.1.5 jeder Summand 0, außer für $n = r_1 + \cdots + r_{m-1}$ und $i_1 = r_1, \ldots, i_{m-1} = r_{m-1}$:

$$\begin{aligned}
&= \mu s_1^{z_f} s_2 (s_1^{r_1} s_2 \cdots s_1^{r_{m-1}} s_2) s_1 s_1^{r_m} s_2 (s_1^{r_{m+1}} \cdots s_1^{r_q} s_2) \\
&= \mu s_1^{z_f} s_2 s_1^{r_1} s_2 \cdots s_1^{r_{m-1}} s_2 s_1^{r_m+1} s_2 s_1^{r_{m+1}} \cdots s_1^{r_q} s_2 \\
&= \mu \phi \left(z_f, (r_1, \ldots, r_{m-1}, r_m + 1, r_{m+1}, \ldots, r_q)\right)
\end{aligned}$$

mit $\mu = \frac{1}{2^{r_1+\cdots+r_q+1}(r_1+\cdots+r_q+1)^{m-1}}$. Nach Definition von $RS_{\mathbb{M}}$ ist aber

$$RS_{\mathbb{M}}\left(z, (r_1, \ldots, r_q)\right) = (z_f, r_1, \ldots, r_{m-1}, r_m + 1, r_{m+1}, \ldots, r_q).$$

Wir haben also hier

$$\mu \phi \left(\mathrm{RS}\left(z, \overrightarrow{r}\right)\right) = a \phi \left(z, \overrightarrow{r}\right),$$

d.h. Diagramm 5.2.3 kommutiert bis auf den Faktor μ. Außerdem ist

$$0 < \mu = \frac{1}{2^{r_1+\cdots+r_q+1}(r_1 + \cdots + r_q + 1)^{m-1}} \leq \frac{1}{2}.$$

b) $P = (z, \mathrm{DEC}_m, z_f)$. Die Rechnung verläuft analog zu a). Dabei müssen die Fälle $r_m \neq 0$ und $r_m = 0$ unterschieden werden, denen die zwei Summanden in der Definition von $\overline{\mathrm{DEC}}_{m,n}$ entsprechen. Statt dies noch einmal durchzurechnen, wollen wir lieber noch den Verzweigungsfall näher betrachten:

c) $P = (z, \mathrm{EQ0}_m, z_f, z_v)$. Wie in a) erhalten wir

$$\begin{aligned}
\overline{P}x &= \left(s_1^{z_f} s_2 \overline{\mathrm{EQ0}}_m + s_1^{z_v} s_2 \overline{\mathrm{EQ0}'}_m\right) s_1^{r_1} s_2 \cdots s_1^{r_q} s_2 \\
&= \mu (s_1^{z_f} s_2)(s_1^{r_1} s_2 \cdots s_1^{r_{m-1}} s_2)(s_2 s_2^*)(s_1^{r_m} s_2 \cdots s_1^{r_q} s_2) + \\
&\qquad \mu (s_1^{z_v} s_2)(s_1^{r_1} s_2 \cdots s_1^{r_{m-1}} s_2)(1 - s_2 s_2^*)(s_1^{r_m} s_2 \cdots s_1^{r_q} s_2)
\end{aligned}$$

mit $\mu \leq \frac{1}{2}$. Ist nun $r_m = 0$, so wird der zweite Summand 0 und der erste liefert das gewünschte Ergebnis

$$\overline{P}x = \mu s_1^{z_f} s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2,$$

denn $\mathbb{M}$ geht in diesem Fall in den Folgezustand z_f über. Oder aber es ist $r_m \neq 0$, dann verschwindet der erste Summand und wir erhalten

$$\overline{P}x = \mu s_1^{z_v} s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2,$$

in Übereinstimmung damit, dass $\mathbb{M}$ in den Verzweigungszustand z_v übergeht. Auch hier haben wir also

$$\mu\phi\left(\mathrm{RS}\left(z, \overrightarrow{r}\right)\right) = a\phi\left(z, \overrightarrow{r}\right),$$

sowie

$$0 < \mu \leq \frac{1}{2}.$$

Insgesamt haben wir also gezeigt:

Feststellung. Das Diagramm 5.2.3 kommutiert bis auf einen Skalar μ. D.h. für alle Konfigurationen $(z, \overrightarrow{r})$ von $\mathbb{M}$ gibt es ein $\mu \in \mathbb{Q}$, sodass

$$\mu\phi\left(\mathrm{RS}_{\mathbb{M}}\left(z, \overrightarrow{r}\right)\right) = a\phi\left(z, \overrightarrow{r}\right). \tag{5.2.4}$$

Ist dabei z der Endzustand z_e von $\mathbb{M}$, so gilt

$$\mu = 1, \tag{5.2.5}$$

ist jedoch $z \neq z_e$, dann gilt

$$0 < \mu \leq \frac{1}{2}. \tag{5.2.6}$$

Außerdem hat μ die Form $\mu = \frac{1}{\nu}$ mit $\nu \in \mathbb{N}$ und ν hängt in berechenbarer Weise von $r_1, \ldots, r_q$ ab.

Damit ist insbesondere gezeigt, dass $ax \in \mathcal{S}\ \forall x \in \mathcal{S}$, denn $\mathcal{S} = \mathbb{Q}(i) \cdot \operatorname{im}\phi$. Sei nun $\hat{x} \in \mathbb{N}_0$ mit $\varphi(\hat{x}) \in \mathcal{S}$ beliebig. Dann können wir $\varphi^{-1}\left(M_a(\varphi(\hat{x}))\right) = \varphi^{-1}(a\varphi(\hat{x}))$ wie folgt berechnen:

1. Finde $x_1, x_2, y_1, y_2, s, z, r_1, \ldots, r_q \in \mathbb{N}_0$ mit

$$\hat{x} = \varphi^{-1}\left((-1)^s \frac{x_1 + ix_2}{y_1 + iy_2} s_1^z s_2 s_1^{r_1} s_2 \cdots s_1^{r_q} s_2\right).$$

   Dies ist möglich, da aufgrund der Zulässigkeit von φ die rechte Seite der Gleichung eine berechenbare Funktion in $x_1, x_2, y_1, y_2, s, z, r_1, \ldots, r_q$ ist, und wir daher lediglich diesen Ausdruck systematisch für alle $x_1, x_2, y_1, y_2, s, z, r_1, \ldots, r_q$ berechnen müssen, bis wir das Ergebnis $\hat{x}$ erhalten.

2. Bestimme
$$\left(z', r'_1, \ldots, r'_q\right) := \mathrm{RS}_{\mathbb{M}}\left(z, (r_1, \ldots, r_q)\right).$$
Dies lässt sich berechnen, da sich die Rechnung einer Registermaschine simulieren lässt (universelle Registermaschine). Berechne die Konstante ν aus obiger Feststellung zu der Konfiguration $(z, \overrightarrow{r})$.

3. Berechne
$$\varphi^{-1}\left(M_a(\varphi(\hat{x}))\right) = \varphi^{-1}\left((-1)^s \frac{x_1 + ix_2}{y_1 + iy_2} \cdot \frac{1}{\nu} \cdot s_1^{z'} s_2 s_1^{r'_1} s_2 \cdots s_1^{r'_q} s_2\right),$$
was wiederum aufgrund der Zulässigkeit von φ möglich ist.

Damit ist Aussage 2 des Satzes für M_a gezeigt.

Um Aussage 3 einzusehen, sei eine beliebige Ausgangskonfiguration $(0, \overrightarrow{r})$ von $\mathbb{M}$ gegeben. Wir unterscheiden, ob $\mathbb{M}$ angesetzt auf $(0, \overrightarrow{r})$ in eine Endlosschleife gerät oder nicht:

1. $\mathbb{M}$ *gerät in eine Endlosschleife.* Dies ist äquivalent dazu, dass $\mathbb{M}$ nie den Endzustand z_e annimmt. Mit (5.2.4) folgt durch Iteration
$$a^n \phi\left(0, \overrightarrow{r}\right) = \mu_1 \cdots \mu_n \phi\left(\mathrm{RS}^n\left(0, \overrightarrow{r}\right)\right),$$
und wegen (5.2.6)
$$\left\|a^n \phi\left((0, \overrightarrow{r})\right)\right\| \leq \frac{1}{2^n} \cdot 1.$$
Also
$$\lim_{n \to \infty} a^n \phi\left(0, \overrightarrow{r}\right) = 0.$$

2. $\mathbb{M}$ *gelangt nach N Rechenschritten in den Endzustand z_e.* Für die ersten N Rechenschritte gilt wie oben
$$a^N \phi\left(0, \overrightarrow{r}\right) = \mu_1 \cdots \mu_N \phi\left(\mathrm{RS}^N\left(0, \overrightarrow{r}\right)\right).$$
Da sich nun aber $\mathbb{M}$ im Endzustand befindet, verringert sich wegen (5.2.5) die Norm nicht weiter:
$$\begin{aligned} a^{N+m} \phi\left(0, \overrightarrow{r}\right) &= \mu_1 \cdots \mu_N \phi\left(\mathrm{RS}^{N+m}\left(0, \overrightarrow{r}\right)\right) \\ &= \mu_1 \cdots \mu_N \phi\left(\mathrm{RS}^N\left(0, \overrightarrow{r}\right)\right), \end{aligned}$$
also $\left\|a^{N+m} \phi\left(0, \overrightarrow{r}\right)\right\| = \mu_1 \cdots \mu_n \cdot 1 > 0$, d. h.
$$a^n \phi\left(0, \overrightarrow{r}\right) \quad \text{konvergiert nicht gegen } 0.$$

Damit ist das Halteproblem für $\mathbb{M}$ auf die Entscheidbarkeit von Prädikat (5.2.1) reduziert:

$$\lim_{n\to\infty} a^n \phi\,(0,(x,0,\dots,0)) = 0 \iff \mathrm{RES}_{\mathbb{M}}(x) = \uparrow \iff x \in (\mathbb{N}_0 \setminus H^1). \tag{5.2.7}$$

Da aber nach Voraussetzung φ zulässig und somit

$$x \longmapsto \varphi^{-1}\,(\phi\,(0,(x,0,\dots,0)))$$

berechenbar ist, würde ein Entscheidungsverfahren für (5.2.1) nach Bemerkung 3.7.3 auch ein Entscheidungsverfahren für $(\mathbb{N}_0 \setminus H^1)$ liefern, im Widerspruch zur Unentscheidbarkeit von H^1.

Um schließlich die Aussagen 1 bis 3 für b zu zeigen, setze

$$b := \sum_{P\in\mathcal{P}_f} \overline{P},$$

und zeige alles analog. Dabei stellt sich heraus, dass $b\,\phi\,(z,\overrightarrow{r}) = 0$, gdw. z der Endzustand z_e ist, und daher weiter

$$\exists n : b^n \phi\,(0,(x,0,\dots,0)) = 0 \iff \mathrm{RES}_{\mathbb{M}}(x) \neq \uparrow \iff x \in H^1. \tag{5.2.8}$$

□

5.2.2 Bemerkung. Man macht sich recht leicht klar, dass die im Beweis des Satzes definierte Menge $\mathcal{S}$ bezüglich φ entscheidbar ist. (Sowohl $\mathcal{S}$ als auch das Komplement von $\mathcal{S}$ sind rekursiv aufzählbar.)

5.2.3 Bemerkung. Der Beweis von Satz 5.2.1 zeigt, dass $\mathcal{O}_2$ und andere von Isometrien mit orthogonalen Bildprojektionen erzeugten C^*-Algebren in gewisser Weise „Turing-vollständig"[†] sind: Wenn wir die Konstruktion im Beweis für eine beliebige Registermaschine $\mathbb{M}$ durchführen, erhalten wir $\mathrm{RES}_{\mathbb{M}}(\overrightarrow{x})$ in Form von

$$\mathrm{RES}_{\mathbb{M}}(\overrightarrow{x}) \quad \widehat{=} \quad \lim_{n\to\infty} a^n \phi(0,(x_1,\dots,x_m,0,\dots,0)).$$

Zusätzlich ist der Limes 0, falls $\mathbb{M}$ in eine Endlosschleife geraten sollte.

5.2.4 Bemerkung. Später werden wir diesen Satz auf jede C^*-Algebra $\mathcal{A}$ mit dichter Unteralgebra $\widehat{\mathcal{A}}$, sodass $\widehat{\mathcal{A}}$ eine echte Isometrie enthält, verallgemeinern können!

[†]Man nennt ein Berechenbarkeits-Modell Turing-vollständig, falls es alle Funktionen berechnet, die eine Registermaschine berechnet.

6 Andere Algebren

Es ist naheliegend zu untersuchen, ob die beobachteten Phänomene auch bei anderen C^*-Algebren auftreten und inwiefern sie mit der Komplexität der Algebren zusammenhängen. So würde man sich wünschen, dass die betrachteten Prädikate weder bei endlichdimensionalen noch bei kommutativen C^*-Algebren unentscheidbar werden. Auch wäre es wünschenswert, dass es hinreichend einfache nichtkommutative unendlichdimensionale C^*-Algebren gibt, in denen keine solchen Beobachtungen zu machen sind.

6.1 Endlichdimensionale C^*-Algebren

Endlichdimensionale C^*-Algebren haben eine einfache Struktur:

6.1.1 Satz. *Ist $\mathcal{A}$ eine endlichdimensionale C^*-Algebra mit* $\dim \mathcal{A} > 0$*, so ist $\mathcal{A}$ schon endliche direkte Summe von vollen Matrixalgebren, d.h. es gibt ein $k \in \mathbb{N}$ und $d_1, \dots, d_k \in \mathbb{N}$ mit*

$$\mathcal{A} = M_{d_1}(\mathbb{C}) \oplus \cdots \oplus M_{d_k}(\mathbb{C}),$$

wobei $M_d(\mathbb{C})$ die Algebra der komplexwertigen $d \times d$-Matrizen bezeichnet.

Beweis. Siehe [Mur], Theorem 6.3.8 . □

Zerlegen wir nun $\mathcal{A}$ auf diese Weise, so gilt für Elemente $A, X \in \mathcal{A}$

$$A^n X = (A_1 \oplus \cdots \oplus A_k)^n (X_1 \oplus \cdots \oplus X_k) = A_1^n X_1 \oplus \cdots \oplus A_k^n X_k.$$

Da die direkte Summe von C^*-Algebren die Produkt-Topologie der einzelnen Faktoren trägt, können wir sowohl die Frage nach Nilpotenz wie auch die Frage nach Nullkonvergenz entscheiden, indem wir diese für jeden Summanden einzeln entscheiden. Daher werden wir uns im Folgenden auf die Untersuchung von vollen Matrixalgebren $M_d(\mathbb{C})$ beschränken.

Sei also $\mathcal{A} := M_d(\mathbb{C})$ und als dichte Unteralgebra $\widehat{\mathcal{A}} := M_d(\mathbb{Q}(i))$ gewählt.

Da $\widehat{\mathcal{A}}$ endlich erzeugt ist, sind nach Satz 4.1.3 alle zulässigen Abzählungen von $\widehat{\mathcal{A}}$ äquivalent. Daher lassen sich aus dem Kode einer Matrix A aus $\widehat{\mathcal{A}}$ die Koeffizienten von A berechnen, da es sicherlich eine zulässige Abzählung gibt, bei der dies möglich ist.

Es ist sofort klar, dass für die von uns untersuchten Prädikate Entscheidungsverfahren existieren. Genauer:

6.1.2 Satz. *Für $A \in M_d(\mathbb{C})$ sind die Prädikate*

$$\left\{X \in M_d(\mathbb{Q}(i)) \;\middle|\; \lim_{n\to\infty} A^n X = 0\right\} \tag{6.1.1}$$

und

$$\left\{X \in M_d(\mathbb{Q}(i)) \;\middle|\; \exists n : A^n X = 0\right\} \tag{6.1.2}$$

für jede zulässige Abzählung von $M_d(\mathbb{Q}(i))$ entscheidbar.

Beweis. Beide Prädikate sind $\mathbb{Q}(i)$-Untervektorräume von $M_d(\mathbb{Q}(i))$. Da $M_d(\mathbb{Q}(i))$ endlichdimensional ist, gilt dies auch für die Prädikate. Man wähle eine beliebige Basis für (6.1.1) bzw. (6.1.2). Ein Entscheidungsverfahren für die Prädikate (6.1.1) bzw. (6.1.2) besteht dann darin, zu prüfen, ob der vorgegebene Vektor X linear unabhängig von diesen Basisvektoren ist. Aus der linearen Algebra sind hierfür einfache Entscheidungsverfahren bekannt. Die *endlich vielen* Basisvektoren von (6.1.1) bzw. (6.1.2) können in das Programm hineinkodiert werden. □

Unbefriedigend an diesem Ergebnis ist, dass es nicht konstruktiv ist, da keine Aussage gemacht wird, wie eine Basis des gegebenen Prädikats zu finden ist. – Wir wollen daher im Folgenden untersuchen, ob auch die Prädikate

$$\left\{(A, X) \in M_d(\mathbb{Q}(i)) \times M_d(\mathbb{Q}(i)) \;\middle|\; \lim_{n\to\infty} A^n X = 0\right\} \tag{6.1.3}$$

und

$$\left\{(A, X) \in M_d(\mathbb{Q}(i)) \times M_d(\mathbb{Q}(i)) \;\middle|\; \exists n : A^n X = 0\right\} \tag{6.1.4}$$

entscheidbar sind.

6.1.3 Satz. *Für $A, X \in M_d(\mathbb{C})$ gilt:*

$$\exists n : A^n X = 0 \quad \Longleftrightarrow \quad A^d X = 0.$$

Beweis. Es ist genau dann $A^n X = 0$, wenn $\operatorname{im} X \subseteq \ker A^n$. Damit folgt die Aussage sofort durch Untersuchung des verallgemeinerten Eigenraums von A zum Eigenwert 0. Wir führen dies zur Erinnerung noch näher aus:

Bezeichnen K_i die Kerne von A^i, so gilt zunächst offensichtlich

$$K_i \subseteq K_{i+1}.$$

Gilt nun für ein k, dass $K_k = K_{k+1}$, so würde folgen dass

$$\begin{aligned} x \in K_{k+m} &\Leftrightarrow A^{k+1} A^{m-1} x = A^{k+m} x = 0 \\ &\Leftrightarrow A^k A^{m-1} x = A^{k+m-1} = 0 \qquad \text{denn } K_{k+1} = K_k \\ &\dots \\ &\Leftrightarrow A^k x = 0 \\ &\Leftrightarrow x \in K_k. \end{aligned}$$

D. h. aber, dass die Folge der K_i streng aufsteigend ist, bis sie schließlich konstant wird. Da die K_i aber Unterräume von $\mathbb{C}^n$ sind, folgt, dass ihre Dimension streng monoton wächst, bis sie konstant wird. Also, da diese Dimension durch d beschränkt ist, folgt $K_{d+1} = K_{d+m}$ $\forall m$. Da aber weiter, falls $K_1 = 0$ ist, A und damit auch jedes A^i invertierbar ist, muss, schon $\dim A_1 \geq 1$ sein, falls die Folge der K_i nicht konstant 0 ist. Also gilt sogar

$$K_d = K_{d+m} \qquad \forall m \in \mathbb{N}.$$

Somit:

$$\begin{aligned} \exists n : A^n X = 0 &\Leftrightarrow \exists n \forall x \in \operatorname{im} X : x \in K_n \\ &\Leftrightarrow \forall x \in \operatorname{im} X : x \in K_d \\ &\Leftrightarrow A^d X = 0. \end{aligned}$$

□

Damit ist also, um die Frage nach Nilpotenz zu klären, nur $A^d X$ zu berechnen, was unter jeder zulässigen Abzählung von $\mathcal{A}$ möglich ist.

Um (6.1.3) zu entscheiden, müssen wir erheblich mehr Aufwand betreiben:

6.1.4 Bemerkung. Für $A, X \in M_d(\mathbb{C})$ gilt

$$\lim_{n\to\infty} A^n X = 0 \quad \Longleftrightarrow \quad \lim_{n\to\infty} A^n (X e_i) = 0 \quad \text{für } i = 1, \dots, d,$$

wobei e_i den i-ten kanonischen Basisvektor des $\mathbb{C}^d$ bezeichnet.

Beweis. Für Operatoren auf endlichdimensionalen Hilberträumen stimmen die Normtopologie und die starke Operator-Topologie[†] überein. □

6.1.5 Satz. *Sei $A \in M_d(\mathbb{C})$. Bezeichnen wir den verallgemeinerten Eigenraum zu $\lambda \in \operatorname{sp}(A)$ von A mit V_λ (d.h. $V_\lambda = \ker(A - \lambda)^d$), so gilt für alle $X \in \mathcal{A}$*

$$\lim_{n\to\infty} A^n X = 0 \quad \Longleftrightarrow \quad \operatorname{im} X \subseteq \bigoplus_{\substack{\lambda \in \operatorname{sp}(A),\\ |\lambda|<1}} V_\lambda.$$

Beweis. Bekanntlich gilt

$$\mathbb{C}^d = \bigoplus_{\lambda \in \operatorname{sp} A} V_\lambda. \tag{6.1.5}$$

Im Folgenden zerlegen wir die V_λ weiter in die zu den Jordankästchen einer Jordanschen Normalform von A gehörigen Teilräume von V_λ, d. h. wir haben eine Zerlegung

$$V_\lambda = V_{\lambda,1} \oplus \cdots \oplus V_{\lambda,k_\lambda} \tag{6.1.6}$$

[†]Topologie der punktweisen Konvergenz

mit Basisvektoren $v_{(\lambda,l,1)}, \dots, v_{(\lambda,l,d_{\lambda,l})}$ von $V_{\lambda,l}$, bezüglich denen die Einschränkung von V auf $V_{\lambda,l}$ die Form

$$A\restriction_{V_{\lambda,l}} \widehat{=} \begin{pmatrix} \lambda & & & & \\ 1 & \lambda & & & \\ & 1 & \lambda & & \\ & & \ddots & \ddots & \\ & & & 1 & \lambda \end{pmatrix} \tag{6.1.7}$$

hat. Außerdem sei $P_{V_{\lambda,l}}$ diejenige Projektion mit

$$\operatorname{im} P_{V_{\lambda,l}} = V_{\lambda,l} \quad \text{und} \quad \ker P_{V_{\lambda,l}} = \bigoplus_{(\lambda',l')\neq(\lambda,l)} V_{\lambda,l}.$$

Es gilt

$$P_{V_{\lambda,l}} A = A P_{V_{\lambda,l}}.$$

(Zur Jordanschen Normalform siehe ein beliebiges Lehrbuch zur linearen Algebra, z. B. [Lor1].) Da auf endlichdimensionalen Vektorräumen alle Normen äquivalent sind ([Wer], Satz I.2.5), können wir im Folgenden als Norm die Summennorm bezüglich der gewählten Basis betrachten, d.h.

$$\left\| \sum_{\lambda,l,i} a_{\lambda,l,i} v_{\lambda,l,i} \right\| = \sum_{\lambda,l,i} |a_{\lambda,l,i}|.$$

Sei nun zunächst

$$\operatorname{im} X \not\subseteq \bigoplus_{\substack{\lambda\in\operatorname{sp}(A),\\ |\lambda|<1}} V_\lambda.$$

Dann gibt es ein i mit $Xe_i \notin \bigoplus_{\substack{\lambda\in\operatorname{sp} A,\\ |\lambda|<1}} V_\lambda$. Also muss es λ, l mit $|\lambda| \geq 1$ geben mit $P_{V_{\lambda,l}} X e_i \neq 0$.

Wegen

$$\|A^n X e_i\| \geq \left\| P_{V_{\lambda,l}} A^n X e_i \right\| = \left\| A^n P_{V_{\lambda,l}} X e_i \right\|$$

reicht es daher zu zeigen, dass $A^n P_{V_{\lambda,l}} X e_i$ nicht gegen 0 konvergiert, um zu sehen, dass $A^n X e_i$ nicht gegen 0 konvergiert.

Sei nun

$$P_{V_{\lambda,l}} X e_i = a_m v_{(\lambda,l,m)} + a_{m+1} v_{(\lambda,l,m+1)} + \cdots + a_{d_{\lambda,l}} v_{(\lambda,l,d_{\lambda,l})} \quad \text{mit } a_m \neq 0,$$

so gilt wegen der Form des Jordankästchens (6.1.7)

$$A^n P_{V_{\lambda,l}} X e_i = a_m \lambda^n v_{(\lambda,l,m)} + a'_{m+1} v_{(\lambda,l,m+1)} + \cdots + a'_{d_{\lambda,l}} v_{(\lambda,l,d_{\lambda,l})} \quad a'_i \in \mathbb{C}.$$

Also
$$\left\| A^n P_{V_{\lambda,l}} X e_i \right\| \geq a_m \lambda^n,$$
und, da $a_m \neq 0$ und $|\lambda| \geq 1$, konvergiert $A^n X e_i$ nicht gegen 0.

Umgekehrt sei nun
$$\operatorname{im} X \subseteq \bigoplus_{\substack{\lambda \in \operatorname{sp} A, \\ |\lambda| < 1}} V_\lambda.$$
Aufgrund der Zerlegungen (6.1.5) und (6.1.6) reicht es wegen Bemerkung 6.1.4, für alle λ, l mit $|\lambda| < 1$ zu zeigen, dass $A^n P_{\lambda,l} X e_i$ für alle i gegen 0 konvergiert, um zu sehen, dass $A^n X$ gegen 0 konvergiert.

Habe $A^n P_{V_{\lambda,l}} X e_i$ die Darstellung
$$A^n P_{V_{\lambda,l}} X e_i = a_1^{(n)} v_{(\lambda,l,1)} + \cdots + a_{d_{\lambda,l}}^{(n)} v_{(\lambda,l,d_{\lambda,l})},$$
dann haben wir zu zeigen:
$$\lim_{n \to \infty} a_j^{(n)} = 0 \qquad j = 1, \ldots, d_{\lambda,l}. \tag{6.1.8}$$
Da A auf $V_{\lambda,l}$ die Form (6.1.7) hat, sind folgende Rekursionsgleichungen gegeben.
$$a_1^{(n+1)} = \lambda a_1^{(n)} \qquad \text{und} \qquad a_{j+1}^{(n+1)} = a_j^{(n)} + \lambda a_{j+1}^{(n)} \quad j = 1, \ldots, d_{\lambda,l} - 1. \tag{6.1.9}$$
Wir zeigen (6.1.8) durch vollständige Induktion nach j.

Induktionsanfang $j = 1$. Aus (6.1.9) erhalten wir sofort $a_1^{(n)} = \lambda^n a_1^{(0)}$ und wegen $|\lambda| < 1$ die Behauptung.

Induktionsschritt. Es gelte (6.1.8) für j. Sei $\varepsilon > 0$. Nach Induktionsvoraussetzung finden wir ein N, so groß, dass
$$\left| a_j^{(n)} \right| < \varepsilon \cdot \frac{1 - |\lambda|}{2} \qquad \text{für } n \geq N.$$
Für $n \geq N$ erhalten wir nun, falls $\left| a_{j+1}^{(n)} \right| \geq \varepsilon$,
$$\begin{aligned}
\left| a_{j+1}^{(n+1)} \right| &\leq \left| a_j^{(n)} \right| + |\lambda| \left| a_{j+1}^{(n)} \right| && \text{nach (6.1.9)} \\
&= \left(\frac{\left| a_j^{(n)} \right|}{\left| a_{j+1}^{(n)} \right|} + |\lambda| \right) \left| a_{j+1}^{(n)} \right| \\
&\leq \left(\frac{\left| a_j^{(n)} \right|}{\varepsilon} + |\lambda| \right) \left| a_{j+1}^{(n)} \right| && \text{Vor. für } \left| a_{j+1}^{(n)} \right| \\
&< \frac{1 + |\lambda|}{2} \left| a_{j+1}^{(n)} \right|. && \text{Wahl von } N
\end{aligned}$$

Ist also $\left|a_{j+1}^{(N)}\right| \geq \varepsilon$, so gibt es ein N' mit $\left|a_{j+1}^{(N')}\right| < \varepsilon$, denn in der obigen Ungleichung ist $\left|\frac{1+|\lambda|}{2}\right| < 1$. (Andernfalls setze $N' := N$) Für jedes $n \geq N$ mit $\left|a_{j+1}^{(n)}\right| < \varepsilon$ gilt außerdem

$$\begin{aligned}
\left|a_{j+1}^{(n+1)}\right| &\leq \left|a_j^{(n)}\right| + |\lambda| \left|a_{j+1}^{(n)}\right| && \text{nach (6.1.9)} \\
&< \left|a_j^{(n)}\right| + \lambda \, |\varepsilon| \\
&< \frac{1-|\lambda|}{2}\varepsilon + |\lambda| \, \varepsilon && \text{Wahl von } N \\
&= \frac{1+|\lambda|}{2}\varepsilon < \varepsilon,
\end{aligned}$$

also ist auch $\left|a_{j+1}^{(n+m)}\right| < \varepsilon$ für jedes m.

Damit ist gezeigt, dass für alle $n \geq N'$ gilt:

$$\left|a_{j+1}^{(n)}\right| < \varepsilon.$$

Also konvergiert $a_{j+1}^{(n)}$ gegen 0. □

Um das Prädikat (6.1.3) zu entscheiden, müssen wir also feststellen, ob Xe_i für alle i nur in verallgemeinerten Eigenräumen von A mit Eigenwerten vom Betrag kleiner 1 Anteile hat. Dies ist jedoch zunächst ein problematisches Unterfangen, da wir sowohl die Eigenwerte als auch die Eigenräume von A im Allgemeinen nur näherungsweise bestimmen können†, und das Konvergenzverhalten von $A^n X$ bei Eigenwertbeträgen von exakt 1 umspringt.

Wir werden zunächst feststellen, dass wir auf die Bestimmung der Eigenräume verzichten können:

6.1.6 Korollar. *Sei $v \in \mathbb{C}^d$. Setze*

$$v_0 := v, \; v_1 := Av, \; \ldots, \; v_{d-1} := A^{d-1}v$$

und sei

$$V := \operatorname{span}(v_0, \ldots, v_{d-1}).$$

Dann schränkt sich A auf einen Endomorphismus von V ein, und es gilt:

$$\lim_{n\to\infty} A^n v = 0 \quad \Longleftrightarrow \quad \forall \lambda \in \operatorname{sp}(A\restriction_V) : |\lambda| < 1.$$

†Die Eigenwerte von A zu bestimmen ist äquivalent dazu, die komplexen Nullstellen des charakteristischen Polynoms von A zu bestimmen, was bekanntlich ab dem fünften Grad algebraisch nicht mehr möglich ist.

Beweis. Es ist offensichtlich, dass sich A zu einem Endomorphismus von V einschränkt. Weiter gilt $\lim_{n\to\infty} A^n v = 0$, gdw. $\lim_{n\to\infty} (A\restriction_V)^n v = 0$. Wenn wir V_λ wie oben für $A\restriction_V$ definieren, erhalten wir nach dem Gezeigten:

$$\lim_{n\to\infty} (A\restriction_V)^n v = 0 \Longleftrightarrow v \in \bigoplus_{\substack{\lambda\in\mathrm{sp}(A\restriction_V),\\ |\lambda|<1}} V_\lambda.$$

Gilt nun $\forall\lambda \in \mathrm{sp}(A\restriction_V) : |\lambda| < 1$, so ist offensichtlich diese Bedingung erfüllt und $(A\restriction_V)^n v$ konvergiert gegen 0.

Gibt es umgekehrt ein $\lambda \in \mathrm{sp}(A\restriction_V)$ mit $|\lambda| \geq 1$, so muss also, soll $A\restriction_V^n v$ gegen 0 gehen,

$$P_{V_\lambda} v = 0$$

gelten. Da wie oben P_{V_λ} mit $A\restriction_V$ vertauscht, folgt:

$$P_{V_\lambda} v_j = P_{V_\lambda} (A\restriction_V)^j v = (A\restriction_V)^j P_{V_\lambda} v = 0 \qquad j = 0, \ldots, n-1.$$

Damit aber

$$V_\lambda = P_{V_\lambda}(V) = P_{V_\lambda}(\mathrm{span}\,(v_0, \ldots, v_{n-1})) = 0.$$

Widerspruch! □

Wir haben somit folgendes Entscheidungsverfahren für das Prädikat (6.1.3): Führe die folgenden Schritte für $i = 1, \ldots, d$ durch.

1. Berechne $Xe_i, AXe_i, \ldots, A^{d-1}Xe_i$.
2. Berechne maximales k, sodass $Xe_i, AXe_i, \ldots, A^k Xe_i$ linear unabhängig sind
3. Berechne die Koordinaten-Matrix von A bzgl. dieser Basis.
4. Berechne das charakteristische Polynom der Matrix.
5. Entscheide, ob dieses Polynom eine Nullstelle vom Betrag größer gleich 1 hat.

$A^n X$ konvergiert genau dann gegen 0, wenn für alle i keine Nullstelle vom Betrag größer gleich 1 gefunden wurde.

Es verbleibt also zu klären, wie von einem gegebenen Polynom zu entscheiden ist, ob es Nullstellen vom Betrag größer gleich 1 besitzt. Dazu zeigen wir folgendes

6.1.7 Lemma. *Es existiert ein Verfahren, das für jedes Polynom $P(X) \in \mathbb{Q}(i)[X]$ entscheidet, ob $P(X)$ in $\mathbb{C}$ eine Nullstelle z mit $|z| \geq 1$ besitzt.*

Beweis. Es ist nicht überraschend, dass eine Vielzahl numerischer Verfahren zur Bestimmung von Nullstellen von Polynomen existieren. Darunter existieren solche Verfahren, die alle Nullstellen von P mit gegebener Genauigkeit bestimmen. Wir sind jedoch mit dem Problem konfrontiert, dass der Fall eintreten kann, dass zu jeder beliebigen Genauigkeit Näherungen für Nullstellen betraglich so nahe an 1 liegen, dass aufgrund des Näherungsfehlers nicht zu entscheiden ist, ob die Nullstelle Betrag kleiner 1 hat oder nicht.

Wüssten wir jedoch, dass P keine Nullstellen mit Betrag 1 hat, so können wir das Problem entscheiden, indem wir das Näherungsverfahren so lange mit gegen 0 konvergierendem Näherungsfehler durchführen, bis für alle Nullstellen von P entschieden ist, ob sie Betrag kleiner 1 haben oder nicht.[†]

Nun ist $z = x + iy$ genau dann eine Nullstelle von P mit Betrag 1, wenn folgendes Gleichungssystem erfüllt ist:

$$\begin{aligned} P(x+iy)\overline{P}(x-iy) &= 0 \\ x^2 + y^2 &= 1 \end{aligned}$$

wobei wir die Gleichung $P(z) = 0$ durch $|P(z)|^2 = 0$ ersetzt haben. Substituieren wir für y^2 in der ersten Gleichung die zweite Gleichung, erhalten wir äquivalent:

$$\begin{aligned} Q(x) + yR(x) &= 0 \\ x^2 + y^2 &= 1 \end{aligned}$$

mit Polynomen $Q, R \in \mathbb{Q}[X]$. Man überzeugt sich sofort, dass dieses System eine Lösung hat, gdw. das in der ersten Gleichung quadrierte System

$$\begin{aligned} y^2R^2(x) &= Q^2(x) \\ x^2 + y^2 &= 1 \end{aligned}$$

eine Lösung besitzt. Substituieren wir schließlich noch einmal die zweite Gleichung für y, so erhalten wir:

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

Dieses System hat genau dann eine Lösung, wenn

$$S(x) := (1-x^2)R^2(x) - Q^2(x) \in \mathbb{Q}[X]$$

[†]Seien $z_1, \dots, z_k$ die Nullstellen von P, von denen keine Betrag 1 habe. Dann gibt es ein $\varepsilon > 0$, sodass für jedes i entweder $B_{2\varepsilon}(z_i) \subset B_1(0)$ oder $B_{2\varepsilon(z_i)} \subset \overline{B_1(0)}^c$. Werden die Nullstellen nun durch $\tilde{z_1}, \dots, \tilde{z_k}$ mit Fehler kleiner ε approximiert, dann gilt auch $B_\varepsilon(\tilde{z}_i) \subset B_1(0)$ oder $B_\varepsilon(\tilde{z}_i) \subset \overline{B_1(0)}^c$.

eine *reelle* Nullstelle vom Betrag kleiner gleich 1 hat.

Nun existieren Algorithmen, die die Anzahl reeller Nullstellen eines Polynoms mit rationalen Koeffizienten exakt bestimmen und ihre Position in beliebiger Näherung ermitteln. Siehe [CL] für einen Überblick.

Also können wir wie folgt vorgehen:

1. Prüfe durch Einsetzen, ob $S(x)$ die Nullstellen -1 oder 1 hat. Wenn ja, besitzt $P(z)$ eine komplexe Nullstelle vom Betrag kleiner gleich 1.

2. Wenn nein, bestimme die Anzahl der reellen Nullstellen von $S(x)$.

3. Nähere diese Nullstellen immer genauer an, bis entschieden werden kann, ob ihr Betrag kleiner oder größer 1 ist.

4. Falls es eine Nullstelle vom Betrag kleiner gleich 1 gibt, hat $P(z)$ eine komplexe Nullstelle vom Betrag kleiner gleich 1, sonst nicht.

Damit haben wir das gesuchte Verfahren gefunden. □

Insgesamt ist damit gezeigt:

6.1.8 Korollar. *Die Prädikate*

$$\Big\{(A,X) \in M_d(\mathbb{Q}(i)) \times M_d(\mathbb{Q}(i)) \;\Big|\; \lim_{n\to\infty} A^n X = 0\Big\}$$

und

$$\Big\{(A,X) \in M_d(\mathbb{Q}(i)) \times M_d(\mathbb{Q}(i)) \;\Big|\; \exists n : A^n X = 0\Big\}$$

sind für jede zulässige Abzählung von $M_d(\mathbb{Q}(i))$ entscheidbar.

Dieses Ergebnis ist insofern schwächer als Satz 6.1.2, als dass wir als Wahlen für A nur Elemente von $M_d(\mathbb{Q}(i))$, also $\widehat{\mathcal{A}}$, zulassen, es in Satz 5.2.1 jedoch gerade wesentlich war, dass A aus der erzeugten C^*-Algebra gewählt wurde. Wir können Korollar 6.1.8 jedoch leicht verallgemeinern:

6.1.9 Korollar. *Sei $\widehat{\mathcal{A}} := M_d(\mathbb{Q}(i))$ mit einer zulässigen Abzählung φ, $\mathcal{S}$ eine beliebige Teilmenge von $\widehat{\mathcal{A}}$, sowie $\mathcal{R}$ eine beliebige, durch ein (nicht notwendig zulässiges) $\psi : \mathbb{N}_0 \longrightarrow \mathcal{R}$ abgezählte Teilmenge von $\mathcal{A} = M_d(\mathbb{C})$, sodass*

$$AX \in \mathcal{S} \qquad \forall A \in \mathcal{R}, \forall X \in \mathcal{S}$$

und die Abbildung

$$M : \mathcal{R} \times \mathcal{S} \longrightarrow \mathcal{S},\ (A,X) \longmapsto AX$$

berechenbar ist.[†] *Dann sind die Prädikate*

$$\left\{(A,X) \in \mathcal{R} \times \mathcal{S} \;\middle|\; \lim_{n\to\infty} A^n X = 0\right\} \tag{6.1.10}$$

und

$$\left\{(A,X) \in \mathcal{R} \times \mathcal{S} \;\middle|\; \exists n : A^n X = 0\right\} \tag{6.1.11}$$

als Teilmengen von $\mathcal{R} \times \mathcal{S}$ entscheidbar.[‡]

Beweis. Die Entscheidbarkeit von (6.1.11) folgt auch hier sofort aus Satz 6.1.3, da $A^k X$ für jedes k berechnet werden kann. Zur Berechenbarkeit von (6.1.10) brauchen wir nur zu bemerken, dass das oben angegebene Entscheidungsverfahren für das Prädikat (6.1.3) auch bereits (6.1.10) entscheidet, denn die Koordinatenmatrix der Einschränkung von A auf den von $Xe_i, AXe_i, \ldots, A^{d-1}Xe_i$ aufgespannten $\mathbb{Q}(i)$-Vektorraum hat auch hier nur Koeffizienten in $\mathbb{Q}(i)$, die sich aus den $A^k X$ berechnen lassen. □

6.2 Kommutative C^*-Algebren

Nach dem Satz von Gelfand-Naimark (Satz 2.5.3) ist jede kommutative C^*-Algebra $\mathcal{A}$ isomorph zu den im Unendlichen verschwindenden Funktionen auf ihrem Spektrum:

$$\mathcal{A} \cong \mathcal{C}_0\left(\operatorname{spec}(\mathcal{A})\right).$$

Nehmen wir an, dass $\mathcal{A}$ schon diese Form hat, und zeigen:

6.2.1 Satz. *Sei $\mathcal{A} = \mathcal{C}_0(X)$ mit X lokalkompakt, sowie $f, g \in \mathcal{A}$. Dann gilt*

$$\exists n : f^n g = 0 \iff fg = 0 \tag{6.2.1}$$

und

$$\lim_{n\to\infty} f^n g = 0 \iff \{x \in X \mid |f(x)| \geq 1\} \subseteq \{x \in X \mid g(x) = 0\}. \tag{6.2.2}$$

Beweis. Die Äquivalenz (6.2.1) gilt offensichtlich, weil

$$\begin{aligned} f^n g = 0 &\Leftrightarrow \forall x \in X : |f(x)|^n \, |g(x)| = 0 \\ &\Leftrightarrow \forall x \in X : |f(x)| \, |g(x)| = 0 \\ &\Leftrightarrow fg = 0. \end{aligned}$$

[†] D. h. $\varphi^{-1}(\psi(x)\varphi(y))$ ist berechenbar.

[‡] D. h. die Urbilder dieser Mengen unter $\psi \times \varphi$ sind als Teilmengen von $(\psi \times \varphi)^{-1}(\mathcal{R} \times \mathcal{S})$ entscheidbar.

Um (6.2.2) einzusehen, nehmen wir zunächst an, dass es ein $x \in X$ gibt mit $|f(x)| \geq 1$ und $g(x) \neq 0$. Dann gilt $|f(x)^n g(x)| \geq |g(x)| > 0$ und somit auch

$$\|f^n g\|_\infty \geq |f^n(x) g(x)| > |g(x)| > 0,$$

also konvergiert $f^n g$ nicht gegen 0.

Gelte umgekehrt, dass $\{x \in X \mid |f(x)| \geq 1\} \subseteq \{x \in X \mid g(x) = 0\}$ und sei $\varepsilon > 0$. Setze

$$A := |g|^{-1}([\varepsilon, \infty)).$$

Da $f \in \mathcal{C}_0(X)$ und A abgeschlossen ist, nimmt $f\restriction_A$ auf A ein Betrags-Maximum, welches nach Definition von A und der Voraussetzung kleiner als 1 sein muss. Also

$$\lim_{n\to\infty} \|(f\restriction_A)^n (g\restriction_A)\|_\infty \leq \lim_{n\to\infty} \|(f\restriction_A)\|_\infty^n \|(g\restriction_A)\|_\infty = 0.$$

Für $x \in X \setminus A$ gilt entweder $g(x) = 0$, also $f^n(x)g(x) = 0$ oder aber $|f(x)| < 1$ und somit $|f^n(x)g(x)| \leq \varepsilon$, d.h.

$$\left\|(f\restriction_{X\setminus A})^n (g\restriction_{X\setminus A})\right\|_\infty \leq \varepsilon.$$

Also gilt schließlich $\|f^n g\|_\infty \leq \varepsilon$. □

6.2.2 Korollar. *Sei $\mathcal{A}$ eine kommutative C^*-Algebra sowie $\widehat{\mathcal{A}}$ eine beliebige abzählbare Unteralgebra mit einer zulässigen Abzählung. Dann ist das Prädikat*

$$\left\{(A, X) \in \widehat{\mathcal{A}} \times \widehat{\mathcal{A}} \;\middle|\; \exists n : A^n X = 0\right\}$$

entscheidbar.

Oder allgemeiner:

6.2.3 Korollar. *Sei $\mathcal{A}$ eine kommutative C^*-Algebra, $\mathcal{R}$,$\mathcal{S}$ Teilmengen mit (nicht notwendig zulässigen) Abzählungen, so dass*

$$AX \in \mathcal{S} \qquad \forall A \in \mathcal{R}, \forall X \in \mathcal{S}$$

und die Abbildung

$$M_a : \mathcal{R} \times \mathcal{S} \longrightarrow \mathcal{S},\ (X, A) \longmapsto XA$$

berechenbar ist. Dann ist das Prädikat

$$\left\{(A, X) \in \mathcal{R} \times \mathcal{S} \;\middle|\; \exists n : A^n X = 0\right\}$$

als Teilmenge von $\mathcal{R} \times \mathcal{S}$ entscheidbar.

Leider ist unklar, wie wir aus Satz (6.2.1) ein ähnlich allgemeines Resultat für den Fall der Konvergenz gegen 0 erhalten sollen. Zwar gibt der Satz eine befriedigende Charakterisierung der Nullkonvergenz, doch ist nicht klar, wie die gefundene Bedingung für eine beliebig gegebene kommutative Algebra $\mathcal{A}$ mit dichter Unteralgebra $\widehat{\mathcal{A}}$ durch einen Algorithmus zu prüfen sein soll.†

Wir werden feststellen, dass dies auch schon für einfache Fälle wie $\mathcal{A} = \mathcal{C}([0,1])$ mit gewissen Aufwand verbunden ist.

6.2.4 Satz. *Betrachte* $\mathcal{A} = \mathcal{C}([0,1])$ *und die dichte Unteralgebra*

$$\widehat{\mathcal{A}} = \{p \in \mathcal{A} \mid p \text{ ist Polynomfunktion mit Koeffizienten aus } \mathbb{Q}(i)\}$$

mit einer zulässigen Abzählung. Dann ist das Prädikat

$$\left\{(f,g) \in \widehat{\mathcal{A}} \times \widehat{\mathcal{A}} \;\middle|\; \lim_{n\to\infty} f^n g = 0\right\}$$

entscheidbar.

Beweis. Zunächst sei bemerkt, dass wir auch hier stets aus dem Kode eines Polynoms $p \in \widehat{\mathcal{A}}$ die Koeffizienten von p bestimmen können, da $\widehat{\mathcal{A}}$ endlich erzeugt ist, und es sicher eine zulässige Abzählung von $\widehat{\mathcal{A}}$ gibt, bezüglich der dies möglich ist (Satz 4.1.3).

Wir geben ein geeignetes Entscheidungsverfahren an, das aus folgenden Schritten besteht:

1. Gegeben seien $f, g \in \widehat{\mathcal{A}}$. Wenn $f = 0$ oder $g = 0$, so gilt $\lim_{n\to\infty} f^n g = 0$. Fertig.

2. Berechne $|f|^2$. Dies ist ein Polynom mit Koeffizienten in $\mathbb{Q}$.

3. Prüfe ob $|f|^2 \equiv 1$. Wenn ja, fertig. $f^n g$ konvergiert nicht gegen 0.

4. Sei m der Grad von $|f|^2$. Prüfe für $i = 1 \dots m+1$, ob $|f|^2\left(\frac{i}{m+1}\right) > 1$. Falls dies wenigstens einmal zutrifft, fertig. $f^n g$ konvergiert nicht gegen 0. (Da sonst f auf einer ganzen offenen Menge Betrag größer 1 hätte, g jedoch nur endlich viele Nullstellen hat.)

5. Zerlege $|f|^2 - 1$ in normierte Primfaktoren

$$|f|^2 - 1 = q f_1^{p_1} \dots f_k^{p_k}$$

mit paarweise verschiedenen f_i. Hierzu existiert eine Vielzahl von Verfahren. Für einen Überblick siehe z. B. [Kal].

6. Prüfe für $i = 1 \dots k$: Ist p_i gerade oder ungerade?

†Siehe auch Kapitel 7.

Ungerade. Hat f_i reelle Nullstelle?† Wenn ja, fertig. $f^n g$ kann nicht gegen 0 konvergieren.

Gerade. Hat f_i reelle Nullstelle? Wenn ja, prüfe ob f_i das Polynom g teilt. (Polynomdivision.) Falls nein, fertig. $f^n g$ konvergiert nicht gegen 0.

7. $f^n g$ konvergiert gegen 0.

Zum Beweis der Korrektheit des Verfahrens prüfen wir das Kriterium von Satz 6.2.1. Nach Definition der Supremums-Norm genügt es offensichtlich, das Konvergenzverhalten von $(|f|^2)^n g$ zu untersuchen.

Zunächst schließt das angegebene Verfahren einige Sonderfälle aus, nämlich dass f oder g konstant 0 werden oder $\forall x \in [0,1] : |f(x)|^2 \geq 1$. (1.-4.) (Denn wäre $|f|^2 \geq 1$, hätte $|f|^2 - 1$ wegen 4. $m+1$ verschiedene Nullstellen, was wegen 3. nicht möglich ist.)

Nun gilt:

(i) Wird $|f|^2$ größer 1, d.h. hat $|f|^2 - 1$ eine Nullstelle mit Vorzeichenwechsel, so kann $f^n g$ nicht gegen 0 konvergieren, denn in diesem Fall würde sofort für unendlich viele x gelten, dass $|f|^2(x) > 0$, g besitzt jedoch nur endlich viele Nullstellen.

(ii) Hat $|f|^2$ bei x das lokale Maximum 1, d.h. hat $|f|^2 - 1$ bei x eine Nullstelle ohne Vorzeichenwechsel, so muss g an dieser Stelle ebenfalls 0 werden, andernfalls konvergiert $f^n g$ nicht gegen 0.

(iii) Da $|f|^2$ nach der Prüfung in 4. wenigstens an einer Stelle kleiner 1 ist, konvergiert $f^n g$ nach Satz 6.2.1 gegen 0, wenn die Fälle (i) und (ii) dies nicht ausschließen.

Wird nun $|f|^2 - 1$ wie oben in normierte irreduzible Polynome zerlegt, so folgt aus der Tatsache, dass die Polynome $f_1, \ldots, f_i$ die Minimalpolynome ihrer Nullstellen sind, dass die Nullstellenmengen der f_i disjunkt sein müssen. Außerdem besitzen die f_i nur einfache Nullstellen, denn wäre x eine mehrfache Nullstelle von f_i, so hätte auch die Ableitung f_i' die Nullstelle x im Widerspruch dazu, dass f_i das Minimalpolynom von x ist. Damit ist klar, dass Schritt 5. und 6. gerade die Bedingungen (i) und (ii) prüfen. (Die hier verwendeten algebraischen Begriffe und Argumente finden sich ausführlich in jedem Lehrbuch der Algebra wie [Bos] oder [Lor2].) □

Auch hier stellt sich erneut die Frage, ob die Entscheidbarkeit erhalten bleibt, wenn wir für f Elemente aus ganz $\mathcal{C}[0,1]$ zulassen. Tatsächlich haben wir es aber schon im folgenden Sinne mit dem allgemeinsten Fall zu tun:

†Wie oben bemerkt, existiern hierzu Entscheidungsverfahren. Siehe [CL].

6.2.5 Lemma. *Sei wie oben* $\mathcal{A} = \mathcal{C}([0,1])$ *und* $\widehat{\mathcal{A}}$ *die dichte Unteralgebra der Polynomfunktionen mit Koeffizienten in* $\mathbb{Q}(i)$. *Sei* $\mathcal{S}$ *eine beliebige Teilmenge von* $\widehat{\mathcal{A}}$, *die nicht nur das Nullpolynom enthält. Ist dann* $f \in \mathcal{A}$ *beliebig mit*

$$fg \in \mathcal{S} \qquad \forall g \in \mathcal{S},$$

so folgt schon $f \in \widehat{\mathcal{A}}$.

Beweis. Sei $f \neq 0$. Wähle ein $g \in \mathcal{S}$ mit $g \neq 0$. Dann gibt es nach Voraussetzung ein $h \in \mathcal{S}$ mit

$$fg = h,$$

also

$$\forall x \in [0,1]: \quad g(x) \neq 0 \implies f(x) = \frac{h(x)}{g(x)}$$

Da f stetig ist folgt, dass jede k-fache Nullstelle von g auch k-fache Nullstelle von h sein muss, also dass es in (dem Integritätsring) $\mathbb{Q}(i)[X]$ teilerfremde Polynome $g', h' \in \widehat{\mathcal{A}}$ gibt, die g und h teilen, sodass g' keine Nullstelle in $[0,1]$ besitzt und

$$f = \frac{h'}{g'}.$$

Da nun aber $f^n g = \left(\frac{h'}{g'}\right)^n g \in \widehat{\mathcal{A}}$ und g' und h' teilerfremd sind, folgt schon

$$g'^n \mid g \qquad \forall n \in \mathbb{N}.$$

Dies ist aber nur möglich, wenn $g' \equiv q$ mit $q \in \mathbb{Q}(i)$. Also

$$f = \frac{1}{q} h' \in \widehat{\mathcal{A}}.$$

□

6.3 Die Algebren $\mathcal{C}([0,1], M_d(\mathbb{C}))$

Mit $\mathcal{C}([0,1], M_d(\mathbb{C}))$ bezeichnen wir die C^*-Algebra der stetigen Funktionen

$$f : [0,1] \longrightarrow M_d(\mathbb{C})$$

versehen mit punktweisen Verknüpfungen und dem Supremum der punktweisen Operator-Normen als Norm.

6.3.1 Satz. *Für $\mathcal{A} = \mathcal{C}([0,1], M_d(\mathbb{C}))$,*

$$\widehat{\mathcal{A}} = \left\{ f \in \mathcal{A} \;\middle|\; f = (f_{ij}), f_{ij} \text{ ist Polynom mit Koeffizienten in } \mathbb{Q}(i), i,j = 1, \dots d \right\}$$

mit einer zulässigen Abzählung φ und $f \in \mathcal{A}$ beliebig, sind die Prädikate

$$\left\{ g \in \widehat{\mathcal{A}} \;\middle|\; \lim_{n\to\infty} f^n g = 0 \right\}$$

und

$$\left\{ g \in \widehat{\mathcal{A}} \;\middle|\; \exists n : f^n g = 0 \right\}$$

entscheidbar.

Beweis. Offensichtlich sind beide Prädikate unter Addition und unter Multiplikation mit Funktionen aus $\mathbb{Q}(i)[X]$ abgeschlossen. Damit bilden sie einen $\mathbb{Q}(i)[X]$-Untermodul des $\mathbb{Q}(i)[X]$-Moduls $\widehat{\mathcal{A}}$. $\widehat{\mathcal{A}}$ ist ein freier $\mathbb{Q}(i)[X]$ Modul mit der endlichen Basis $\left(f_{ij}^{(kl)}\right)$, wobei $f_{ij}^{(kl)}(t) := \delta_{ik}\delta_{jl}$, also mit der Basis der matrixwertigen Funktionen, die in einer Komponente konstant 1 und in allen anderen Komponenten konstant 0 sind.

Da $\mathbb{Q}(i)[X]$ ein Hauptidealring ist, sind auch die beiden Prädikate freie, endlich erzeugte Moduln über $\mathbb{Q}(i)[X]$. (Siehe [Lan], Theorem III.7.1)

Damit können wir wie im endlichdimensionalen Fall bei Satz 6.1.2 vorgehen, indem wir die Koordinaten einer $\mathbb{Q}(i)[X]$-Basis des zu entscheidenden Prädikats in das Programm kodieren, und zu einem gegebenen $g \in \widehat{\mathcal{A}}$ nur prüfen müssen, ob es im Erzeugnis dieser Basis liegt.

Dies ist z. B. möglich, indem wir zunächst die lineare Unabhängigkeit von g von dieser Basis statt in $\widehat{\mathcal{A}} \cong (\mathbb{Q}(i)[X])^{d^2}$ in $\mathrm{Quot}(\mathbb{Q}(i)[X])^{d^2}$ entscheiden, im Falle linearer Abhängigkeit g als $\mathrm{Quot}(\mathbb{Q}(i)[X])$-Linearkombination darstellen und entscheiden, ob die Koeffizienten dieser Linearkombination in $\mathbb{Q}(i)[X]$ liegen. ($\mathrm{Quot}(\mathbb{Q}(i)[X])$ bezeichne den Quotientenkörper von $\mathbb{Q}(i)[X]$, also den Körper der gebrochen-rationalen Funktionen mit Koeffizienten in $\mathbb{Q}(i)$.) $\square$

6.4 Die C^*-Algebra der kompakten Operatoren

Im Folgenden sei stets $\mathcal{H}$ ein separabler Hilbertraum mit Orthonormalbasis $(\xi_i)_{i\in\mathbb{N}}$. Wir erinnern an die Definition der kompakten Operatoren:

6.4.1 Definition (kompakte Operatoren)**.** Ein Operator $K : \mathcal{H} \longrightarrow \mathcal{H}$ heißt kompakt, wenn das Bild der abgeschlossenen Einheitskugel $\overline{B}_1(0)$ relativ-kompakt in $\mathcal{H}$ ist, d. h. wenn sein Abschluss in $\mathcal{H}$ kompakt ist. Mit $\mathcal{K}(\mathcal{H})$ bezeichnen wir die Menge der kompakten Operatoren auf $\mathcal{H}$.

Die kompakten Operatoren haben folgende Eigenschaften:

6.4.2 Satz. *1. $\mathcal{K}(\mathcal{H})$ bildet ein (abgeschlossenes beidseitiges) Ideal in $\mathcal{B}(\mathcal{H})$.*

2. Hat ein Operator K endlichen Rang, d. h. ist sein Bild endlichdimensional, so ist K kompakt.

3. Die Operatoren von endlichem Rang sind dicht in $\mathcal{K}(\mathcal{H})$.

4. Sei $(a_k) \in l^\infty(\mathbb{N})$ eine beschränkte Folge komplexer Zahlen. Dann definiert

$$\begin{aligned} M_{(a_k)} : \mathcal{H} &\longrightarrow \mathcal{H} \\ \xi_k &\longmapsto a_k \xi_k \end{aligned}$$

einen beschränkten Operator auf $\mathcal{H}$. $M_{(a_k)}$ ist kompakt genau dann, wenn (a_k) eine Nullfolge ist.

Beweis. 1.-3. Siehe [Wer], Satz II.3.2, Korollar VI.3.7 .
4. folgt leicht aus 3. und der Tatsache, dass $\left\|M_{(a_k)}\right\| = \|(a_k)\|_\infty$. □

Wir vereinbaren folgende Bezeichnungsweise:

6.4.3 Definition. 1. Mit $\mathcal{M}_d$ sei die Menge aller Operatoren $T \in \mathcal{B}(\mathcal{H})$ bezeichnet, für die gilt:

$$\operatorname{span}(\xi_{d+1}, \xi_{d+2}, \dots) \subseteq \ker T \quad \text{und} \quad \operatorname{im} T \subseteq \operatorname{span}(\xi_1, \dots \xi_d) .$$

Weiter sei $\mathcal{M}_\infty$ die Vereinigung aller $\mathcal{M}_d$.

2. Mit $\mathcal{M}_\infty(\mathbb{Q}(i))$ bezeichnen wir die Menge aller $T \in \mathcal{M}_\infty$, für die gilt, dass

$$(T\,\xi_i \mid \xi_j) \in \mathbb{Q}(i) \qquad \forall i,j \in \mathbb{N}.$$

Ferner sei mit $\mathcal{M}_d(\mathbb{Q}(i))$ der Schnitt $\mathcal{M}_d \cap \mathcal{M}_\infty(\mathbb{Q}(i))$ bezeichnet.

Die Mengen $\mathcal{M}_d$ und $\mathcal{M}_\infty$ bzw. $\mathcal{M}_d(\mathbb{Q}(i))$ und $\mathcal{M}_\infty(\mathbb{Q}(i))$ hängen also von der Wahl der Orthonormalbasis $(\xi_i)_{i\in\mathbb{N}}$ von $\mathcal{H}$ ab. Offensichtlich handelt es sich um $*$-Unteralgebren von $\mathcal{K}(\mathcal{H})$, und $\mathcal{M}_d$ und $\mathcal{M}_d(\mathbb{Q}(i))$ sind isomorph zu $M_d(\mathbb{C})$ bzw. $M_d(\mathbb{Q}(i))$. Es gilt:

6.4.4 Lemma. *$\mathcal{M}_\infty$ und $\mathcal{M}_\infty(\mathbb{Q}(i))$ sind dicht in $\mathcal{K}(\mathcal{H})$.*

Beweis. Für $\mathcal{M}_\infty$ folgt dies leicht aus Teil 3 von Satz 6.4.2 und der Tatsache, dass $(\xi_i)_{i\in\mathbb{N}}$ eine Orthonormalbasis von $\mathcal{H}$ ist.
$\mathcal{M}_d(\mathbb{Q}(i))$ liegt dicht in $\mathcal{M}_d$ (genau wie $M_d(\mathbb{Q}(i))$ dicht in $M_d(\mathbb{C})$ liegt), also ist $\mathcal{M}_\infty(\mathbb{Q}(i))$ dicht in $\mathcal{M}_\infty$ und somit auch in $\mathcal{K}(\mathcal{H})$. □

Setze für $i, j \in \mathbb{N}$

$$E_{ij} : \mathcal{H} \longrightarrow \mathcal{H}$$
$$\xi \longmapsto (\xi \mid \xi_j)\, \xi_i$$

Dann sind alle E_{ij} Elemente von $\mathcal{M}_\infty(\mathbb{Q}(i))$ und es gilt

$$E_{ij}^* = E_{ji}, \tag{6.4.1}$$
$$E_{ij}E_{kl} = \delta_{jk}E_{il}, \tag{6.4.2}$$

womit insbesondere die E_{ii} paarweise orthogonale Projektionen (auf span (ξ_i)) sind. Außerdem gilt

$$\mathrm{span}_{\mathbb{Q}(i)}\left(\{E_{ij} \mid i, j \in \mathbb{N}\}\right) = \mathcal{M}_\infty(\mathbb{Q}(i))\,. \tag{6.4.3}$$

Ein System $E_{i,j},\ i, j \in I$ von Elementen von $\mathcal{M}_\infty(\mathbb{Q}(i))$, das die Relationen (6.4.1) und (6.4.2) erfüllt, nennen wir ein System von *Matrixeinheiten* für $\mathcal{M}_\infty(\mathbb{Q}(i))$. Gilt zusätzlich (6.4.3), so nennen wir das System *vollständig*. Die eben definierten E_{ij} nennen wir die kanonischen Matrixeinheiten von $\mathcal{M}_\infty(\mathbb{Q}(i))$.

Leider ist $\mathcal{M}_\infty(\mathbb{Q}(i))$ nicht endlich erzeugt und somit sind nicht notwendig alle zulässigen Abzählungen von $\mathcal{M}_\infty(\mathbb{Q}(i))$ äquivalent.† Wenn wir im Folgenden $\mathcal{M}_\infty(\mathbb{Q}(i))$ als $\widehat{\mathcal{A}}$ wählen, wollen wir jedoch zumindest mit den kanonischen Matrixeinheiten E_{ij} sinnvoll rechnen können. Wir nennen daher eine zulässige Abbildung φ *normal*, wenn die Abbildung

$$\alpha : \mathbb{N}^2 \longrightarrow \mathcal{M}_\infty(\mathbb{Q}(i))$$
$$(i, j) \longmapsto E_{ij}$$

berechenbar ist. Insbesondere können wir dann zu jedem $X \in \mathcal{M}_\infty(\mathbb{Q}(i))$ aus dem Kode von X die Matrixkoeffizienten von X bezüglich der E_{ij} berechnen.

Im Folgenden werden wir uns zunächst nur für normale zulässige Abzählungen interessieren. Es ist klar, dass es solche Abzählungen gibt.

Wir wollen nun das Hauptresultat aus Kapitel 5 auf die C^*-Algebra der kompakten Operatoren übertragen. Dazu erinnern wir daran, dass die C^*-Algebra $\mathcal{O}_2$ (bis auf Isomorphie) von den Isometrien S_1, S_2 mit $S_1(\xi_i) := \xi_{2i-1}$ und $S_2(\xi_i) := \xi_{2i}$ erzeugt wird (Beispiel 5.1.6). Da die Bilder von S_1 und S_2 orthogonal sind, traf Satz 5.2.1 auf $\mathcal{O}_2$ zu.

Wir benötigen zusätzlich folgendes

†Tatsächlich lassen sich leicht nicht äquivalente zulässige Abzählungen von $\mathcal{M}_\infty(\mathbb{Q}(i))$ finden. Sei dazu $\omega : \mathbb{N} \longrightarrow \mathbb{N}$ eine nicht berechenbare Bijektion. Diese liefert eine unitäre Abbildung U_ω auf $\mathcal{H}$ vermittels $U_\omega(\xi_i) := \xi_{\omega(i)}$. Weiter sei φ eine zulässige Abzählung, für die die Abbildung $\alpha : \mathbb{N} \longrightarrow \mathcal{M}_\infty(\mathbb{Q}(i))$, $n \longmapsto E_{nn}$ berechenbar ist. Dann kann man recht leicht sehen, dass $\varphi_\omega := Ad(U_\omega) \circ \varphi$ ebenfalls zulässig ist und α bzgl. φ_ω nicht berechenbar sein kann.

6.4.5 Lemma. *1. Sei (a_k) eine beschränkte Folge komplexer Zahlen, die an keiner Stelle 0 wird. Dann gibt es Folgen $(b_k), (b'_k), (c_k), (c'_k)$, die an keiner Stelle 0 werden mit $\|(b_k)\|_\infty, \|(b'_k)\|_\infty, \|(c_k)\|_\infty, \|(c'_k)\|_\infty \leq \|(a_k)\|_\infty$, sodass*

$$S_1 M_{(a_k)} = M_{(b_k)} S_1 \qquad S_1^* M_{(a_k)} = M_{(b'_k)} S_1^*$$
$$S_2 M_{(a_k)} = M_{(c_k)} S_2 \qquad S_2^* M_{(a_k)} = M_{(c'_k)} S_2^*$$

2. Sei $(a_k)_k$ eine beschränkte Folge komplexer Zahlen, die an keiner Stelle 0 wird. Dann gibt es $(b_k), (b'_k), (c_k), (c'_k)$ wie in 1. mit

$$M_{(a_k)} S_1 = S_1 M_{(b_k)} \qquad M_{(a_k)} S_1^* = S_1^* M_{(b'_k)}$$
$$M_{(a_k)} S_2 = S_2 M_{(c_k)} \qquad M_{(a_k)} S_2^* = S_2^* M_{(c'_k)}$$

3. Sei (a_k) wie in 1. und seien $\mu, \nu \in \{1,2\}^*$. Dann gibt es Folgen $(b_k), (c_k)$, wie oben mit

$$S_\mu S_\nu^* M_{(a_k)} = M_{(b_k)} S_\mu S_\nu^* \qquad M_{(a_k)} S_\mu S_\nu^* = S_\mu S_\nu^* M_{(c_k)}$$

Beweis. 1. Zu gegebenen (a_k) definieren wir die Folgen $(b_k), (b'_k), (c_k), (c'_k)$ wie folgt:

$$b_k := \begin{cases} a_1 & k \text{ gerade} \\ a_{\frac{k+1}{2}} & k \text{ ungerade} \end{cases} \qquad b'_k := a_{2k-1}$$
$$c_k := \begin{cases} a_1 & k \text{ ungerade} \\ a_{\frac{k}{2}} & k \text{ gerade} \end{cases} \qquad c'_k := a_{2k}$$

Die so definierten Folgen werden offensichtlich nirgends 0 und haben kleinere Supremums-Norm als (a_k). Schließlich prüft man sofort anhand der Definitionen von S_1 und S_2, dass die geforderten Relationen für alle ξ_i erfüllt sind. Da diese eine Orthonormalbasis bilden, folgt die Behauptung.

2. Entweder wie in 1., oder Anwenden der Involution auf die geforderten Gleichungen unter Ausnutzung von 1. und der Tatsache, dass $M^*_{(a_k)} = M_{(\overline{a_k})}$.

3. Wiederholte Anwendung von 1. und 2.

□

Wir können nun Satz 5.2.1 auf $\mathcal{K}(\mathcal{H})$ übertragen, indem wir aus dem dort definierten Operator a durch Multiplikation mit einem geeigneten Multiplikationsoperator einen kompakten Operator mit denselben kombinatorischen Eigenschaften gewinnen.

6.4.6 Satz. *Sei $\mathcal{A} = \mathcal{K}(\mathcal{H})$ und $\widehat{\mathcal{A}} = \mathcal{M}_\infty(\mathbb{Q}(i))$ mit zulässiger normaler Abzählung φ. Dann gibt es Operatoren $A, B \in \mathcal{A}$ mit*

1. *Es gibt berechenbare Folgen (A_n) und (B_n) aus $\widehat{\mathcal{A}}$, die gegen A bzw. B konvergieren, mit $\|A - A_n\|, \|B - B_n\| \leq \frac{1}{n}\ \forall n$.*

2. *$AX, BX \in \widehat{\mathcal{A}}\ \ \forall X \in \widehat{\mathcal{A}}$, und die Abbildungen*
$$M_A : \widehat{\mathcal{A}} \longrightarrow \widehat{\mathcal{A}},\ X \longmapsto AX$$
und
$$M_B : \widehat{\mathcal{A}} \longrightarrow \widehat{\mathcal{A}},\ X \longmapsto BX$$
sind berechenbar.

3. *Die Prädikate*
$$\left\{X \in \widehat{\mathcal{A}} \;\middle|\; \lim_{n\to\infty} A^n X = 0\right\}$$
und
$$\left\{X \in \widehat{\mathcal{A}} \;\middle|\; \exists n : B^n X = 0\right\}$$
sind nicht entscheidbar.

Beweis. Wähle wie im Beweis von Satz 5.2.1 eine Registermaschine $\mathbb{M} = \left(\mathcal{R}_q^{1,1}, \mathcal{P}_f\right)$ mit genau einem Endzustand z_e, die die Funktion

$$f : \mathbb{N}_0 \longrightarrow \mathbb{N}_0$$
$$x \longmapsto \begin{cases} 1 & x \in H^1 \\ \uparrow & x \notin H^1 \end{cases}$$

berechnet, sodass also nicht entscheidbar ist, für welche $x \in \mathbb{N}_0$ gilt, dass $\mathbb{M}$ bei Input x in eine Endlosschleife gerät.

Zusätzlich wollen wir annehmen, dass wann immer $\mathbb{M}$ in den Zustand z_e kommt, alle q Register leer sind. Dies ist keine Einschränkung, da wir sonst das Programm mit einem weiteren Programm verknüpfen können, welches nacheinander alle Register von $\mathbb{M}$ leert und dann in den Endzustand z_e übergeht. Weiter können wir, da Zustände beliebig umnummeriert werden können, ohne Einschränkung annehmen, dass $z_e = 1$.

Zu $P \in \mathcal{P}$ sei $\overline{P}$ wie in Satz 5.2.1 mit $s_1 := S_1$ und $s_2 := S_2$ und schließlich

$$a := \sum_{P \in \mathcal{P}} \overline{P} + S_1 S_2 S_2^* S_1^*$$

definiert. (Beachte $z_e = 1$!)

Es sei die Folge (a_k) definiert durch

$$a_k := \begin{cases} 1 & k \leq 2^{q+2} \\ \frac{1}{k} & \text{sonst} \end{cases}$$

Wir erhalten nun aus a nach Satz 6.4.2 einen kompakten Operator, wenn wir a mit dem Multiplikationsoperator $M_{(a_k)}$ verknüpfen:

$$A := aM_{(a_k)}.$$

Um wieder Konfigurationen von $\mathbb{M}$ auf Operatoren in $\widehat{\mathcal{A}}$ zu übertragen, setzen wir:

$$\begin{aligned} \Phi : K(\mathbb{M}) &\longrightarrow \widehat{\mathcal{A}} \\ (z,(r_1,\ldots,r_q)) &\longmapsto S_1^z S_2 S_1^{r_1} S_2 \ldots S_1^{r_q} S_2 E_{11} \end{aligned}$$

Man prüft leicht anhand der Definitionen von S_1, S_2 und E_{11}, dass dieser Ausdruck die Form E_{i1} hat, und somit das Bild von Φ tatsächlich in $\widehat{\mathcal{A}}$ liegt.

Wir zeigen nun durch vollständige Induktion, dass es für alle n eine Folge (b_k) mit $\|(b_k)\|_\infty \leq 1$ gibt, die nirgends 0 wird, sodass

$$A^n \Phi\left(z,(r_1,\ldots,r_q)\right) = \left(a^n \phi\left(z,(r_1,\ldots,r_q)\right)\right) M_{(b_k)} E_{11}, \tag{6.4.4}$$

wobei ϕ die Abbildung aus dem Beweis von Satz 5.2.1 ist.

Induktionsanfang $n = 0$. Klar, setze $b_k \equiv 1$.

Induktionsschritt. Sei (6.4.4) korrekt für n. Für $n+1$ gilt nach Induktionsvoraussetzung

$$\begin{aligned} A^{n+1}\Phi\left(z,(r_1,\ldots,r_q)\right) &= A\left[\left(a^n\phi\left(z,(r_1,\ldots,r_q)\right)\right) M_{(b_k)} E_{11}\right] \\ &= aM_{(a_k)}\left(a^n\phi\left(z,(r_1,\ldots,r_q)\right)\right) M_{(b_k)} E_{11}. \end{aligned}$$

Da nun aber nach dem in Satz 5.2.1 Gezeigten insbesondere $a^n\phi\left(z,(r_1,\ldots,r_q)\right)$ stets von der Form μS_ν ist, gibt es nach Lemma 6.4.5 eine Folge (c_k) mit

$$\|(c_k)\|_\infty \leq \|(a_k)\|_\infty = 1,$$

die nirgends 0 wird, sodass wir weiter umformen können:

$$\begin{aligned} aM_{(a_k)}\left(a^n\phi\left(z,(r_1,\ldots,r_q)\right)\right) M_{(b_k)} E_{11} &= a\left(a^n\phi\left(z,(r_1,\ldots,r_q)\right)\right) M_{(c_k)} M_{(b_k)} E_{11} \\ &= \left(a^{n+1}\phi\left(z,(r_1,\ldots,r_q)\right)\right) M_{(c_k b_k)} E_{11}. \end{aligned}$$

Da aber mit (b_k) und (c_k) auch $(c_k b_k)$ nirgends 0 wird und Supremums-Norm kleiner gleich 1 hat, ist die Behauptung gezeigt.

Wir wollen als nächstes zeigen, dass

$$\lim_{n\to\infty} A^n\Phi\,(0,(x,0,\dots,0)) = 0 \iff \mathrm{RES}_{\mathbb{M}}(x) = \uparrow \iff x \in (\mathbb{N}_0 \setminus H^1). \qquad (6.4.5)$$

Dabei wurde im Beweis von Satz 5.2.1 bereits gezeigt, dass

$$\lim_{n\to\infty} a^n\phi\,(0,(x,0,\dots,0)) = 0 \iff \mathrm{RES}_{\mathbb{M}}(x) = \uparrow \iff x \in (\mathbb{N}_0 \setminus H^1). \qquad (6.4.6)$$

Nehmen wir zunächst an, dass $\mathbb{M}$ bei Input x in eine Endlosschleife gerät. Nach (6.4.6) gilt dann $\lim_{n\to\infty} a^n\phi\,(0,(x,0,\dots,0)) = 0$, und mit (6.4.4) folgt sofort, dass dann auch $\lim_{n\to\infty} A^n\Phi\,(0,(r_1,\dots,r_q)) = 0$, da mit $\|(b_k)\|_\infty \leq 1$ auch $\left\|M_{(b_k)}\right\| \leq 1$.

Gelte nun, dass $\mathbb{M}$ bei Input x den Endzustand $z_e = 1$ erreicht und sei

$$\overrightarrow{r} := (x,0,\dots,0).$$

Dann gibt es nach dem Beweis von 5.2.1 ein N und eine rationale Zahl $\mu > 0$ mit

$$a^N\phi\,(0,\overrightarrow{r}) = \mu\phi\left(1,\overrightarrow{0}\right) = \mu S_1 S_2^{q+1}, \qquad (6.4.7)$$

denn $z_e = 1$ und nach Wahl von $\mathbb{M}$ haben alle q Register von $\mathbb{M}$ im Endzustand den Wert 0. Weiter entnehmen wir dem Beweis von 5.2.1, dass

$$aS_1S_2^{q+1} = a\phi\left(1,\overrightarrow{0}\right) = \phi\left(1,\overrightarrow{0}\right) = S_1S_2^{q+1}. \qquad (6.4.8)$$

Nun folgt aus (6.4.7) mit (6.4.4)

$$A^N\Phi\,(0,\overrightarrow{r}) = \mu S_1 S_2^{q+1} M_{(b_k)} E_{11}. \qquad (6.4.9)$$

Wähle nun eine Folge (c_k) mit $M_{(a_k)}S_1S_2^{q+1} = S_1S_2^{q+1}M_{(c_k)}$. Dann muss insbesondere nach Definition von S_1 und S_2 gelten:

$$a_{2^{q+2}-1}\xi_{2^{q+2}-1} = M_{(a_k)}S_1S_2^{q+1}\,\xi_1 = S_1S_2^{q+1}M_{(c_k)}\,\xi_1 = c_1\xi_{2^{q+2}-1},$$

d. h.

$$c_1 = a_{2^{q+2}-1} = 1. \qquad (6.4.10)$$

Aus (6.4.9) folgt aber mit (6.4.8)

$$\begin{aligned} A^{N+1}\Phi\,(0,\overrightarrow{r}) &= A\left[\mu S_1S_2^{q+1}M_{(b_k)}E_{11}\right] \\ &= \mu a\left[M_{(a_k)}S_1S_2^{q+1}\right]M_{(b_k)}E_{11} \\ &= \mu a S_1S_2^{q+1}M_{(c_kb_k)}E_{11} \\ &= \mu S_1S_2^{q+1}M_{(c_kb_k)}E_{11}, \end{aligned}$$

also nach Iteration:

$$A^{N+m}\Phi\left(0,\overrightarrow{r}\right)=\mu S_1 S_2^{q+1} M_{(c_k^m b_k)} E_{11}.$$

Insbesondere gilt also nach (6.4.10)

$$\left\|A^{N+m}\Phi\left(0,\overrightarrow{r}\right)\xi_1\right\|=\left\|\mu c_1^m b_1 \xi_{2^{q+2}-1}\right\|=\left|\mu b_1\right|,$$

und $A^{N+m}\Phi\left(0,\overrightarrow{r}\right)$ konvergiert nicht gegen 0. Also ist (6.4.5) nachgewiesen.

Aufgrund der Normalität von φ ist aber die Abbildung

$$x\longmapsto\varphi^{-1}\left(\Phi(0,(x,0,\ldots,0))\right)$$

berechenbar, denn

$$\Phi(0,(x,0,\ldots,0))=S_2 S_1^x S_2^q E_{11}=E_{i1},$$

und i hängt berechenbar von x ab. Aus Satz 3.3.10 folgt daher wieder, dass

$$\left\{X\in\widehat{\mathcal{A}}\;\middle|\;\lim_{n\to\infty}A^n X=0\right\}$$

aufgrund der Unentscheidbarkeit von H^1 nicht entscheidbar ist. Aussage 3 ist für A damit gezeigt.

Aussage 1 lässt sich ähnlich wie im Beweis von Satz 5.2.1 zeigen. Wie dort können wir A sicherlich durch

$$A_n:=\left[\sum_{P\in\mathcal{P}}\overline{P}_{n+K}+S_1S_2S_2^*S_1^*\right]M_{(a_k^n)}$$

mit

$$a_k^n:=\begin{cases}a_k & k<2n+K\\ 0 & k\geq 2n+K\end{cases}$$

für geeignetes K so approximieren, dass die Folge dieser A_n der Konvergenzbedingung von Aussage 1 genügt. Weiter gilt nach Definition von $M_{(a_k^n)}$, dass

$$\operatorname{span}\left(\xi_{2n+K},\xi_{2n+K+1},\ldots\right)\subseteq\ker A_n.$$

Außerdem können wir A_n als

$$A_n=\left[\sum_{s=1}^{t}\lambda_s S_{\mu_s}S_{\nu_s}^*\right]M_{(a_k^n)}\qquad\mu_s,\nu_s\in\{1,2\}^*,\lambda_s\in\mathbb{Q}(i)\tag{6.4.11}$$

schreiben, wobei sich geeignete λ_s,μ_s,ν_s aus n berechnen lassen. Für $j<2n+K$ gilt nun

$$S_{\mu_s}S_{\nu_s}^*\xi_j=0\quad\text{oder}\quad S_{\mu_s}S_{\nu_s}^*\xi_j=\xi_{i_{s,j}},\tag{6.4.12}$$

wobei $i_{s,j}$ berechenbar von s und j abhängt. Also gibt es ein $d \geq 2n + K$ mit

$$\operatorname{im} A_n \subseteq \operatorname{span}(\xi_1, \xi_2, \ldots, \xi_d),$$

d. h. es gilt tatsächlich $A_n \in \mathcal{M}_d(\mathbb{Q}(i)) \subseteq \mathcal{M}_\infty(\mathbb{Q}(i))$.

Aus der Darstellung (6.4.11) und aus (6.4.12) folgt weiter, dass sich auch die Koeffizienten der Darstellung

$$A_n = \sum_{i,j \leq d} \lambda_{i,j} E_{ij} \qquad \lambda_{i,j} \in \mathbb{Q}(i)$$

berechnen lassen. Aus der Normalität von φ folgt daher, dass die Folge der A_n berechenbar ist. Damit ist Aussage 1 gezeigt.

Um schließlich Aussage 2 einzusehen, bemerken wir nur, dass für jedes i ein n berechnet werden kann, sodass

$$AE_{ij} = A_n E_{ij} \qquad \forall j \in \mathbb{N}.$$

Denn das Bild von E_{ij} ist $\operatorname{span}(\xi_i)$, und nach Definition von S_1 und S_2 ist stets $S_\nu^* \xi_i = 0$, wenn ν auf 2 endet und $|\nu|$ groß genug wird, wie dies bei allen $\overline{\mathrm{INC}}_{m,n}$, $\overline{\mathrm{DEC}}_{m,n}$, $\overline{\mathrm{EQ0}}_{m,n}$ und $\overline{\mathrm{EQ0}}'_{m,n}$ für hinreichend großes n der Fall ist. Es ist klar, dass sich eine solche Schranke für die Länge von ν aus i berechnen lässt.

Also lässt sich zu jedem $X \in \widehat{\mathcal{A}}$ ein n berechnen, sodass

$$AX = A_n X.$$

Wegen $A_n \in \widehat{\mathcal{A}}$ folgt dann, dass das Bild von M_A tatsächlich in $\widehat{\mathcal{A}}$ liegt, und AX kann berechnet werden, weil wir $A_n X$ berechnen können.

Die Aussagen über B gelten wieder analog mit

$$b = \sum_{P \in \mathcal{P}} \overline{P}$$

und

$$B = bM_{(a_k)}.$$

□

In $\mathcal{M}_\infty(\mathbb{Q}(i))$ können wir jedoch keine solchen Elemente A oder B finden:

6.4.7 Satz. *Für $\mathcal{A} = \mathcal{K}(\mathcal{H})$, $\widehat{\mathcal{A}} = \mathcal{M}_\infty(\mathbb{Q}(i))$ und $A \in \widehat{\mathcal{A}}$ sind die Prädikate*

$$\left\{ X \in \widehat{\mathcal{A}} \;\middle|\; \lim_{n \to \infty} A^n X = 0 \right\}$$

und

$$\left\{ X \in \widehat{\mathcal{A}} \;\middle|\; \exists n : A^n X = 0 \right\}$$

bezüglich jeder zulässigen Abzählung von $\widehat{\mathcal{A}}$ entscheidbar.

Beweis. Sei $A \in \mathcal{M}_d(\mathbb{Q}(i))$. Da $\mathcal{M}_d(\mathbb{Q}(i))$ offensichtlich zu der C^*-Algebra der $d \times d$-Matrizen $M_d(\mathbb{Q}(i))$ isomorph ist und da für ein beliebiges $X \in \mathcal{M}_\infty(\mathbb{Q}(i))$

$$AX \in \mathcal{M}_d(\mathbb{Q}(i)),$$

sowie

$$\exists n : A^n X = 0 \quad \Longleftrightarrow \quad \exists n : A^n(AX) = 0$$

und

$$\lim_{n\to\infty} A^n X = 0 \quad \Longleftrightarrow \quad \lim_{n\to\infty} A^n(AX) = 0$$

gilt, folgt die Behauptung aus Satz 6.1.2. □

Wie verhält es sich nun, wenn φ nicht normal ist? Können wir Satz 6.4.6 auch auf diesen Fall übertragen? Es stellt sich heraus, dass jede zulässige Abzählung von $\mathcal{M}_\infty(\mathbb{Q}(i))$ zumindest „quasi“-normal ist:

6.4.8 Lemma. *Sei φ eine zulässige Abzählung von $\mathcal{M}_\infty(\mathbb{Q}(i))$. Dann gibt es ein System von Matrixeinheiten F_{ij}, $i, j \in \mathbb{N}$ von $\mathcal{M}_\infty(\mathbb{Q}(i))$, sodass die Abbildung*

$$\begin{aligned} \alpha : \mathbb{N}^2 &\longrightarrow \mathcal{M}_\infty(\mathbb{Q}(i)) \\ (i, j) &\longmapsto F_{ij} \end{aligned}$$

berechenbar ist. (F_{ij} ist jedoch nicht notwendig vollständig.)

Beweis. Wegen der Eigenschaften (6.4.1) und (6.4.2) und der Zulässigkeit von φ reicht es zu zeigen, dass wir ein System von Matrixeinheiten F_{ij} finden können, sodass die Abbildung

$$\begin{aligned} \beta : \mathbb{N} &\longrightarrow \mathcal{M}_\infty(\mathbb{Q}(i)) \\ i &\longmapsto F_{i1} \end{aligned}$$

berechenbar ist. Wir definieren β rekursiv wie folgt:

1. $\beta(1)$. Setze $F_{11} := E_{11}$, sowie $\beta(1) := F_{11}$.
2. *Seien* $\beta(1), \dots, \beta(n)$ schon definiert. Prüfe für jedes k bei $k = 0$ beginnend:
   a) Ist $\varphi(k)^*\varphi(k) = F_{11}$? Wenn nein, weiter bei $k+1$.
   b) Ist $(\beta(1)\beta(1)^* + \cdots + \beta(n)\beta(n)^*)\varphi(k) = 0$. Wenn ja, setze $F_{(n+1)1} := \varphi(k)$, $\beta(n+1) := F_{(n+1)1}$. Sonst weiter bei $k+1$.

   Man macht sich leicht klar, dass diese Suche schließlich terminieren wird.

Offensichtlich ist dann F_{ij} mit $F_{ij} := F_{i1}{F_{j1}}^*$ ein System von Matrixeinheiten. □

Nun ist das so gewonnene System zwar nicht notwendig vollständig, aber für unsere Belange ist es nicht weniger schlecht als ein vollständiges System, da es eine C^*-Unteralgebra von $\mathcal{K}(\mathcal{H})$ erzeugt, die wiederum isomorph zu $\mathcal{K}(\mathcal{H})$ ist. Es gilt:

6.4.9 Satz. *Sei $\mathcal{A}$ eine C^*-Algebra, $\widehat{\mathcal{A}}$ eine dichte $\mathbb{Q}(i)$-$*$-Unteralgebra, f_{ij} ein System von Matrixeinheiten in $\widehat{\mathcal{A}}$, sowie φ eine zulässige Abzählung, so dass die Abbildung*

$$\begin{aligned} \alpha : \mathbb{N}^2 &\longrightarrow \widehat{\mathcal{A}} \\ (i,j) &\longmapsto f_{ij} \end{aligned}$$

berechenbar ist.

Dann gilt

1. *$\mathcal{A}_f := \overline{\operatorname{span}(\{f_{ij}\})}$ ist eine C^*-Unteralgebra von $\mathcal{A}$, die isomorph zur Algebra der kompakten Operatoren auf einem separablen Hilbertraum ist. $\widehat{\mathcal{A}}_f := \operatorname{span}_{\mathbb{Q}(i)}(\{f_{ij}\})$ ist eine dichte $\mathbb{Q}(i)$-$*$-Unteralgebra von $\mathcal{A}_f$.*
2. *Für jede normale zulässige Abzählung φ' von $\widehat{\mathcal{A}}_f$ sind die Abbildungen $\varphi^{-1} \circ \varphi'$ und $\varphi'^{-1} \circ \varphi\restriction_{\varphi^{-1}(\widehat{\mathcal{A}}_f)}$ berechenbar.*

Beweis. 1. Dass $\operatorname{span}(\{f_{ij}\})$ bzw. $\operatorname{span}_{\mathbb{Q}(i)}(\{f_{ij}\})$ $\mathbb{C}$- bzw. $\mathbb{Q}(i)$-$*$-Unteralgebren von $\mathcal{A}$ bzw. $\widehat{\mathcal{A}}$ sind, ist aufgrund der Eigenschaften von Matrixeinheiten klar. Also ist $\mathcal{A}_f$ eine C^*-Unteralgebra von $\mathcal{A}$. $\widehat{\mathcal{A}}_f$ ist natürlich dicht in $\mathcal{A}_f$.

Um einzusehen, dass $\mathcal{A}_f$ isomorph zu $\mathcal{K}(\mathcal{H})$ ist, beachte, dass

$$\begin{aligned} \alpha : \operatorname{span}(\{f_{ij}\}) &\longrightarrow \mathcal{M}_\infty \\ f_{ij} &\longmapsto E_{ij} \end{aligned}$$

ein bijektiver $*$-Homomorphismus ist, wobei E_{ij} wie oben die kanonischen Matrixeinheiten von $\mathcal{M}_\infty$ bezeichne. Nun erhalten wir aber für jedes d per Einschränkung einen bijektiven $*$-Homomorphismus

$$\alpha\restriction_{\operatorname{span}(\{f_{ij}\,\mid\, i,j\leq d\})} : \operatorname{span}(\{f_{ij} \mid i,j \leq d\}) \longrightarrow \mathcal{M}_d\,.$$

Als endlichdimensionale Teilräume sind $\operatorname{span}(\{f_{ij} \mid i,j \leq d\})$ und $\mathcal{M}_d$ abgeschlossen†, also sind sie C^*-Unteralgebren von $\mathcal{A}$ und $\mathcal{K}(\mathcal{H})$. Damit gilt für alle $d \in \mathbb{N}$, dass $\alpha\restriction_{\operatorname{span}(\{f_{ij}\,\mid\, i,j\leq d\})}$ ein Isomorphismus zwischen C^*-Algebren und nach Satz 2.5.5 also isometrisch ist. Somit ist α isometrisch.

Daher setzt sich α fort zu einem isometrischen (also injektiven) $*$-Homomorphismus $\overline{\alpha} : \mathcal{A}_f \longrightarrow \mathcal{K}(\mathcal{H})$. Da $\mathcal{M}_\infty$ dicht in $\mathcal{K}(\mathcal{H})$ liegt, ist $\overline{\alpha}$ folglich ein Isomorphismus.

† Auf endlichdimensionalen Vektorräumen sind alle Normen äquivalent ([Wer], Satz I.2.5), also sind endlich dim. normierte Räume stets vollständig, also als Teilräume eines Banachraums abgeschlossen.

2. Sei φ' eine normale zulässige Abzählung von $\widehat{\mathcal{A}}_f$. Wir können $\varphi^{-1} \circ \varphi'(n)$ und $\varphi'^{-1} \circ \varphi\restriction_{\varphi^{-1}(\widehat{\mathcal{A}}_f)(n)}$ genauso wie in Satz 4.1.3 wie folgt bestimmen:

   Gehe systematisch alle $\mathbb{Q}(i)$-Linearkombinationen der $f_{i,j}$ durch. Da α bezüglich φ sowie bezüglich φ' berechenbar ist und φ und φ' zulässig sind, können wir dabei die Kodes der Linearkombinationen unter φ und φ' berechnen. Schließlich muss einer dieser Kodes unter φ' die Zahl n sein. Dann ist der Kode dieser Linearkombination unter φ gerade $\varphi^{-1} \circ \varphi'(n)$. Umgekehrt muss schließlich auch der Kode einer Linearkombination unter φ die Zahl n sein, und der Kode dieser Linearkombination unter φ' ist $\varphi'^{-1} \circ \varphi(n)$.

□

6.4.10 Korollar. *Sei $\mathcal{A} = \mathcal{K}(\mathcal{H})$, $\widehat{\mathcal{A}} = \mathcal{M}_\infty(\mathbb{Q}(i))$, sowie φ eine zulässige Abzählung. Dann gibt es Elemente $A, B \in \mathcal{A}$, sowie eine Menge $\mathcal{S} \subseteq \widehat{\mathcal{A}}$ mit*

1. *Es gibt berechenbare Folgen (A_n) und (B_n) aus $\widehat{\mathcal{A}}$, die gegen A bzw. B konvergieren, mit $\|A - A_n\|, \|B - B_n\| \leq \frac{1}{n}$ $\forall n$.*

2. *$AX, BX \in \mathcal{S}$ $\forall x \in \mathcal{S}$, und die Abbildungen*

$$M_A : \mathcal{S} \longrightarrow \mathcal{S},\ X \longmapsto AX$$

   und

$$M_B : \mathcal{S} \longrightarrow \mathcal{S},\ X \longmapsto BX$$

   sind berechenbar.

3. *Die Prädikate*

$$\left\{X \in \mathcal{S} \;\middle|\; \lim_{n\to\infty} A^n X = 0\right\} \subseteq \mathcal{S} \tag{6.4.13}$$

   und

$$\left\{X \in \mathcal{S} \;\middle|\; \exists n : B^n X = 0\right\} \subseteq \mathcal{S} \tag{6.4.14}$$

   sind als Teilmengen von $\mathcal{S}$ nicht entscheidbar.

Beweis. Sei F_{ij} ein bezüglich φ berechenbares System von Matrixeinheiten. Wende Satz 6.4.6 auf $\mathcal{A}_F$, $\widehat{\mathcal{A}}_F$ sowie eine beliebige normale Abzählung φ' von $\widehat{\mathcal{A}}_F$ an. Wir haben also $A, B \in \mathcal{A}_F \subseteq \mathcal{A}$, $(A_n), (B_n) \in \widehat{\mathcal{A}}_F \subseteq \widehat{\mathcal{A}}$ mit den gewünschten Eigenschaften bezüglich φ', wenn wir $\mathcal{S} := \widehat{\mathcal{A}}_F$ setzen.

Nun folgt, da $\varphi^{-1} \circ \varphi'$ und $\varphi'^{-1} \circ \varphi\restriction_{\varphi^{-1}(\widehat{\mathcal{A}}_F)}$ berechenbar sind:

1. $(\varphi^{-1}(A_n)) = ((\varphi^{-1} \circ \varphi')(\varphi'^{-1}(A_n)))$ ist berechenbar, also ist (A_n) berechenbar bzgl. φ. Analog ist (B_n) bzgl. φ berechenbar.

2. Für $n \in \varphi^{-1}(\mathcal{S})$ ist

$$\varphi^{-1}(A \cdot \varphi(n)) = (\varphi^{-1} \circ \varphi') \left[\varphi'^{-1} \left(A \cdot \varphi' \left(\left(\varphi'^{-1} \circ \varphi\restriction_{\varphi^{-1}(\widehat{\mathcal{A}}_F)}\right)(n)\right)\right)\right]$$

   berechenbar, d.h. M_A ist bezüglich φ berechenbar. Analog für M_B.

3. Sei $\mathcal{P}$ das Prädikat (6.4.13) oder das Prädikat (6.4.14). Angenommen, $\mathcal{P}$ ist als Teilmenge von $\mathcal{S}$ bezüglich φ entscheidbar. Das heißt gerade, dass $\varphi^{-1}(\mathcal{P})$ als Teilmenge von $\varphi^{-1}(\mathcal{S})$ entscheidbar ist. Nun gilt

$$(\varphi^{-1} \circ \varphi')(\varphi'^{-1}(\mathcal{P})) = \varphi^{-1}(\mathcal{P})$$

   und

$$(\varphi^{-1} \circ \varphi')(\varphi'^{-1}(\mathcal{S} \setminus \mathcal{P})) = \varphi^{-1}(\mathcal{S} \setminus \mathcal{P}).$$

   Nach Bemerkung 3.7.3 wäre somit $\varphi'^{-1}(\mathcal{P})$ und das heißt gerade $\mathcal{P}$ bezüglich φ' entscheidbar. Widerspruch!

□

Ausgangspunkt unserer Untersuchung war die Beobachtung, dass in von zwei Isometrien mit orthogonalem Bild erzeugten C^*-Algebren die von uns untersuchten Prädikate unentscheidbar wurden, was wir in diesem Abschnitt auf die Algebra der kompakten Operatoren übertragen haben. Wir werden nun sehen, dass sich dieses Ergebnis auf beliebige C^*-Algebren überträgt, die eine echte Isometrie beinhalten.

6.4.11 Satz. *Sei $\mathcal{A}$ eine C^*-Algebra, $\widehat{\mathcal{A}}$ eine dichte $\mathbb{Q}(i)$-$*$-Unteralgebra, sowie φ eine zulässige Abzählung von $\widehat{\mathcal{A}}$. Zusätzlich gelte, dass $\widehat{\mathcal{A}}$ eine echte Isometrie s enthalte. Dann gilt*

1. *Die Elemente der Form*

$$f_{ij} := s^i(1 - ss^*)(s^*)^j \qquad i, j \in \mathbb{N}$$

   bilden ein System von Matrixeinheiten.

2. *Die Abbildung*

$$\begin{aligned} \alpha : \mathbb{N}^2 &\longrightarrow \widehat{\mathcal{A}}_f \\ (i, j) &\longmapsto f_{ij} \end{aligned}$$

   ist berechenbar.

Beweis. 1. Offensichtlich gilt $f_{ij}^* = f_{ji}$. Um (6.4.2) zu prüfen, unterscheiden wir die Fälle $j < k$, $j = k$ und $j > k$:

a) $j < k$. Wir haben

$$f_{ij}f_{kl} = s^i \cdot \underbrace{(1-ss^*)s^{k-j}}_{s^{k-j}-s(s^*s)s^{k-j-1}=0} \cdot (1-ss^*)(s^*)^l = 0.$$

b) $j = k$. Es gilt

$$f_{ij}f_{kl} = s^i(1-ss^*)(1-ss^*)(s^*)^l = f_{il}.$$

c) $j > k$. Analog zum ersten Fall ergibt sich

$$f_{ij}f_{kl} = s^i(1-ss^*) \cdot \underbrace{(s^*)^{j-k}(1-ss^*)}_{(s^*)^{j-k}-(s^*)^{j-k-1}(s^*s)s^*=0} \cdot (s^*)^l = 0.$$

2. Dass α berechenbar ist, folgt aus der Tatsache, dass φ zulässig ist und die Ausdrücke, die die f_{ij} definieren, nur durch (in offensichtlich berechenbarer Weise von i und j abhängenden) Algebren-Operationen aus den Elementen s und 1 gebildet werden. Die Kodes von s und 1 lassen sich wiederum in das Programm zur Berechnung von α hineinkodieren lassen.

□

6.4.12 Korollar. *Sei $\mathcal{A}$ eine C^*-Algebra mit dichter $\mathbb{Q}(i)$-$*$-Unteralgebra $\widehat{\mathcal{A}}$ und zulässiger Abzählung φ, sodass $\widehat{\mathcal{A}}$ eine echte Isometrie s enthält. Dann gibt es Elemente $a, b \in \mathcal{A}$, sowie eine Menge $\mathcal{S} \subseteq \widehat{\mathcal{A}}$ mit*

1. *Es gibt berechenbare Folgen (a_n) und (b_n) aus $\widehat{\mathcal{A}}$, die gegen a bzw. b konvergieren, mit $\|a - a_n\|, \|b - b_n\| \leq \frac{1}{n}$ $\forall n$.*
2. *$ax, bx \in \mathcal{S}$ $\forall x \in \mathcal{S}$, und die Abbildungen*

$$M_a : \mathcal{S} \longrightarrow \mathcal{S},\ x \longmapsto ax$$

und

$$M_b : \mathcal{S} \longrightarrow \mathcal{S},\ x \longmapsto bx$$

sind berechenbar.

3. *Die Prädikate*

$$\left\{x \in \mathcal{S} \;\middle|\; \lim_{n\to\infty} a^n x = 0\right\} \subseteq \mathcal{S}$$

und

$$\left\{x \in \mathcal{S} \;\middle|\; \exists n : b^n x = 0\right\} \subseteq \mathcal{S}$$

sind als Teilmengen von $\mathcal{S}$ nicht entscheidbar.

Beweis. Aufgrund von Satz 6.4.11 folgt dies genau wie in Korollar 6.4.10 aus Satz 6.4.9. □

7 Diskussion der Ergebnisse

Im Laufe unserer Untersuchungen haben wir immer wieder die Frage untersucht, ob in einer C^*-Algebra $\mathcal{A}$ die Prädikate

$$\left\{x \in \mathcal{S} \;\middle|\; \lim_{n\to\infty} a^n x = 0\right\} \tag{7.0.1}$$

und

$$\left\{x \in \mathcal{S} \;\middle|\; \exists n : a^n x = 0\right\} \tag{7.0.2}$$

für ein gegebenes $a \in \mathcal{A}$ und eine gewisse Teilmenge $\mathcal{S} \subseteq \mathcal{A}$ entscheidbar sind. Dabei stellten wir fest, dass für endlichdimensionale C^*-Algebren (7.0.1) und (7.0.2) stets entscheidbar waren, wie auch für die unendlichdimensionalen Algebren der Form $\mathcal{C}([0,1], M_d(\mathbb{C}))$, während sich hingegen für C^*-Algebren, die echte Isometrien enthalten, stets ein a und $\mathcal{S}$ finden lassen, sodass (7.0.1) oder (7.0.2) unentscheidbar werden.†

Dies sind zwar recht weitreichende Ergebnisse, jedoch ist zu beachten, dass wir mehrere *Wahlen* getroffen haben, bevor wir von der Entscheidbarkeit oder Unentscheidbarkeit dieser Prädikate sprechen konnten:

Zunächst mussten wir eine dichte $\mathbb{Q}(i)$-$*$-Unteralgebra $\widehat{\mathcal{A}}$ von $\mathcal{A}$ wählen, da wir mit einem Computer stets nur über abzählbare Mengen sprechen können. Von dieser abzählbaren Menge ist jedoch sicher zu fordern, dass sie möglichst viele Eigenschaften der Algebra $\mathcal{A}$ reflektiert, um sinnvoll mit diesem Modell über $\mathcal{A}$ sprechen zu können. Die Forderung, dass $\mathcal{A}$ eine dichte $\mathbb{Q}(i)$-$*$-Unteralgebra von $\mathcal{A}$ ist, scheint auf der Hand zu liegen.

Zweitens mussten wir neben einer dichten Unteralgebra $\widehat{\mathcal{A}}$ auch festlegen, wie wir die Elemente von $\widehat{\mathcal{A}}$ in natürliche Zahlen (oder, aufgrund von Abschnitt 3.4 hierzu äquivalent, in endliche Folgen natürlicher Zahlen) kodieren wollen, um so in der Rechenmaschine Namen für die Elemente von $\widehat{\mathcal{A}}$ zur Verfügung zu haben. Auch hier scheint der Begriff der zulässigen Abzählung die Minimalanforderungen an eine solche Kodierung zu bestimmen, wenn wir in $\widehat{\mathcal{A}}$ rechnen wollen.

Erfreulicherweise stellte sich aufgrund von Bemerkung 4.1.4 in allen untersuchten Fällen heraus, dass solche zulässigen Abzählungen existieren und sich aufgrund von Satz 4.1.3 stets als äquivalent erwiesen, mit Ausnahme der kompakten Operatoren und der nicht endlich erzeugten Unteralgebra $\widehat{\mathcal{A}} = \mathcal{M}_\infty(\mathbb{Q}(i))$. Aber auch im Falle

† Die Isometrie muss natürlich in $\widehat{\mathcal{A}}$ liegen!

von $\mathcal{M}_\infty(\mathbb{Q}(i))$ stellte uns dies vor keine ernsten Hindernisse. Zudem hätten wir statt $\mathcal{M}_\infty(\mathbb{Q}(i))$ auch die von $M_{\left(\frac{1}{n}\right)}S$ erzeugte $\mathbb{Q}(i)$-$*$-Unteralgebra von $\mathcal{K}(\mathcal{H})$ betrachten können, wobei S den unilateralen Shift auf $\mathcal{H}$ bezeichne. Denn diese Algebra ist endlich erzeugt und enthält $\mathcal{M}_\infty(\mathbb{Q}(i))$, ist also dicht in $\mathcal{K}(\mathcal{H})$. Allerdings wäre dies sicher eine weniger kanonische Wahl für $\widehat{\mathcal{A}}$ gewesen.

Insofern sind unsere Ergebnisse also stets unabhängig von der Wahl einer (geeigneten) Kodierung von $\widehat{\mathcal{A}}$, jedoch setzen sie stets eine konkrete Wahl von $\widehat{\mathcal{A}}$ voraus. Bereits die Argumentation in Satz 6.1.2 versagt, wenn $\widehat{\mathcal{A}} := M_d(\mathbb{K})$ gewählt wird, mit einem Zwischenkörper $\mathbb{K}$ der Erweiterung $\mathbb{C}/\mathbb{Q}(i)$ von unendlichem Grad über $\mathbb{Q}(i)$, da dann $\widehat{\mathcal{A}}$ kein endlichdimensionaler $\mathbb{Q}(i)$-Vektorraum mehr ist.

Sind wir an konkreter symbolischer Rechnung mit Elementen einer C^*-Algebra, ähnlich wie mit einem Computer-Algebra-System, interessiert[†], so stellt dies keine zu gravierende Einschränkung dar, da wir uns dann eben stets, wie wir argumentiert haben, für eine Unteralgebra $\widehat{\mathcal{A}}$ und ein Kodierungsschema für $\widehat{\mathcal{A}}$ entscheiden müssen. Zwar haben wir in dieser Arbeit stets nur eine Wahl für $\widehat{\mathcal{A}}$ getroffen, aber wie wir meinen, die jeweils auf der Hand liegende, und sind bezüglich dieser Wahl unabhängig von der Kodierung zu befriedigenden Ergebnissen gelangt.

Wollen wir jedoch anhand der Unentscheidbarkeit der Prädikate (7.0.1) oder (7.0.2) Informationen über die Struktur oder Komplexität von $\mathcal{A}$ gewinnen – und unsere Ergebnisse scheinen zu suggerieren, dass zumindest grobe Zusammenhänge bestehen – so sind wir mit dem Problem konfrontiert, dass unsere Ergebnisse „koordinatenabhängig“ sind, also von der Wahl von $\widehat{\mathcal{A}}$ abhängen. Um also aus den beobachteten Phänomenen einen Begriff, der eine Eigenschaft von C^*-Algebren kodiert, zu gewinnen, ist noch weitere Arbeit notwendig.

Unmittelbar naheliegende Fragen wären z. B., ob Unentscheidbarkeit im Falle von Algebren wie $\mathcal{O}_2$ oder $\mathcal{K}(\mathcal{H})$ bei jeder Wahl von $\widehat{\mathcal{A}}$ auftreten, oder umgekehrt im Falle der endlichdimensionalen C^*-Algebren oder von $\mathcal{C}([0,1], \mathcal{M}_d(\mathbb{C}))$ niemals auftreten.

Weiterhin denkbar wäre, unser „Rechenwerkzeug“ $(\widehat{\mathcal{A}}, \varphi)$, weiter zu schärfen. Denn mit der in dieser Arbeit entwickelten Terminologie haben wir neben der algebraischen Struktur von $\widehat{\mathcal{A}}$ lediglich die geometrische Information, dass auf $\widehat{\mathcal{A}}$ eine C^*-Norm existiert, bezüglich der $\widehat{\mathcal{A}}$ dicht in $\mathcal{A}$ liegt. Damit ist $\mathcal{A}$ natürlich bei weitem nicht festgelegt. Es wäre naheliegend, zusätzlich die Approximierbarkeit der Normfunktion oder des Spektrums für Elemente aus $\widehat{\mathcal{A}}$ zu fordern. Damit wäre die Klasse der möglichen $(\widehat{\mathcal{A}}, \varphi)$ (wobei der Begriff der zulässigen Abzählung entsprechend zu erweitern wäre) verkleinert und somit der Weg zu koordinatenunabhängigen Ergebnissen einfacher.

Dass eine solche Einschränkung wünschenswert sein könnte, zeigt auch der Fall der kommutativen C^*-Algebren, bei dem wir, auch ohne eine konkrete Algebra zu

[†]Dies wäre zumindest für manche der von uns untersuchten Algebren in Anwendungsfragen denkbar.

betrachten, durch Gelfand-Transformation eine mathematisch befriedigende, einfache Eigenschaft der Elemente von (7.0.1) erhalten haben (Satz 6.2.1), es jedoch völlig unklar war, wie wir anhand von $(\widehat{\mathcal{A}}, \varphi)$ diese Eigenschaft entscheiden sollten.

Insgesamt legt dies alles jedoch die Vermutung nahe, dass, um mit berechenbarkeitstheoretischen Methoden gute Begriffe für C^*-Algebren zu erhalten, ein allgemeinerer, abstrakterer Rahmen gefunden werden muss, in dem diese Fragen behandelt werden, wie durch Untersuchung größerer Klassen von Prädikaten und durch Anwendung abstrakterer Methoden der höheren Rekursionstheorie.

Es bleibt die Frage, inwiefern wir in dieser Arbeit C^*-Algebren-spezifische Aussagen gemacht haben, zumal sich (7.0.2) in jeder Algebra und (7.0.1) in jeder normierten Algebra definieren lässt.

Tatsächlich scheint kein Grund zu bestehen, diese Prädikate nicht auch in beliebigen Banachalgebren zu untersuchen. Der Übergang zu normabgeschlossenen Algebren erscheint jedoch wesentlich, da wir in allen Fällen, in denen wir auf Unentscheidbarkeit gestoßen sind, Elemente aus dem Abschluss der Algebra wählen mussten. Im Falle der kompakten Operatoren konnten wir sogar zeigen, dass in $\mathcal{M}_\infty(\mathbb{Q}(i))$ solche Elemente nicht existieren können. (Und auch für $\mathcal{O}_2$ erscheint diese Vermutung naheliegend.)

Desweiteren lassen sich unsere Hauptresultate, in denen Unentscheidbarkeit auftritt, überhaupt nur in $*$-Algebren formulieren, was vielleicht ein Argument sein mag, gesondert Banach-$*$-Algebren zu untersuchen. Umgekehrt sollte sich allerdings, mit ein wenig Verfeinerung des Beweises, Satz 5.2.1 von C^*-Algebren auch auf beliebige Banach-$*$-Algebren übertragen lassen.

Es soll noch betont sein, dass in den Sätzen 5.2.1, 6.4.6, 6.4.10 und 6.4.12 die Elemente a und b selbst immer in berechenbarer Weise definiert wurden. (Dies sollen gerade die Aussagen 1 und 2 in diesen Sätzen aussagen.) Dies ist wesentlich, da in unendlichdimensionalen Algebren stets unberechenbare Informationen in Elementen „untergebracht“ werden können. Betrachte z. B. in $\mathcal{K}(\mathcal{H})$ den Multiplikationsoperator $M_{\left(\frac{1}{n}\chi(n)\right)}$ wobei χ eine nicht berechenbare charakteristische Funktion ist. Die Existenz solcher Elemente scheint aber wenig mehr auszusagen, als dass die Algebra unendlichdimensional ist.

Schließlich mag es von Interesse sein, zu beobachten, dass in allen untersuchten Fällen (7.0.1) und (7.0.2) immer zugleich entscheidbar wurden oder es zugleich für beide Prädikate Elemente gab, sodass die Prädikate unentscheidbar wurden, umgekehrt jedoch im Falle von Entscheidbarkeit die Charakterisierung von (7.0.1) wesentlich komplexer war und geometrischerere Eigenschaften miteinbezog als die Charakterisierung von (7.0.2). Im endlichdimensionalen Fall waren z. B. für (7.0.1) Kenntnisse über Eigenwerte und Eigenräume nötig, das gefundene Berechnungsverfahren war kompliziert, während um (7.0.2) zu entscheiden nur eine d-fache Potenz gebildet werden musste.

Es liegt die Frage nahe, ob die Unentscheidbarkeit der beiden Prädikate immer zusammenfällt. Zudem ist (7.0.2) offensichtlich stets rekursiv aufzählbar (bilde einfach alle $a^n x$), während die berechenbarkeitstheoretische Komplexität von (7.0.1) a priori unklar ist. Es ist klar, dass (7.0.1) für das in unseren Sätzen konstruierte a rekursiv aufzählbar ist, da dies für H^1 gilt. Gibt es Fälle, in denen H^1 nicht rekursiv aufzählbar ist? Wenn ja, wann?

Literaturverzeichnis

[Bla] Bruce Blackadar. *Operator algebras. Theory of C^*-algebras and von Neumann algebras.* Encyclopaedia of Mathematical Sciences 122. Operator Algebras and Non-Commutative Geometry 3. Berlin: Springer, 2006.

[Bos] Siegfried Bosch. *Algebra. 6th ed.* Springer-Lehrbuch. Berlin: Springer, 2006.

[CL] G.E. Collins und R. Loos. Real zeroes of polynomials. In *Computer algebra, symbolic and algebraic computation, Comput. Suppl. 4, 83-94.* 1982.

[Coo] Stephen Cook. The p versus np problem. *Clay Mathematics Institute. Millenium Problems, Official Problem Description.* `http://claymath.org/millennium/P_vs_NP/pvsnp.pdf`.

[Cun] Joachim Cuntz. Simple c^*-algebras generated by isometries. *Commun. Math. Phys.*, 57:173–185, 1977.

[Dav] Kenneth R. Davidson. *C^*-algebras by example.* Fields Institute Monographs. 6. Providence, RI: American Mathematical Society (AMS), 1996.

[HS] Friedrich Hirzebruch und Winfried Scharlau. *Einführung in die Funktionalanalysis. Unveränd. Nachdr. der 1. Aufl.* BI-Hochschultaschenbücher. 296. Mannheim: BI-Wissenschaftsverlag, 1991.

[Jä] Klaus Jänich. *Funktionentheorie. Eine Einführung. 6. Aufl.* Springer-Lehrbuch. Berlin: Springer, 2004.

[Kal] E. Kaltofen. Factorization of polynomials. Computer algebra, symbolic and algebraic computation, Comput. Suppl. 4, 95-113 (1982)., 1982.

[Lan] Serge Lang. *Algebra. 3rd revised ed.* Graduate Texts in Mathematics. 211. New York, NY: Springer, 2002.

[Ler] Manuel Lerman. *Degrees of unsolvability. Local and global theory.* Perspectives in Mathematical Logic. Berlin etc.: Springer-Verlag, 1983.

[Lor1] Falko Lorenz. *Lineare Algebra II. 3., überarb. Aufl.* Mannheim: B.I. Wissenschaftsverlag, 1992.

[Lor2] Falko Lorenz. *Einführung in die Algebra I. 3. Aufl.* Heidelberg: Spektrum Akademischer Verlag, 1996.

[Mur] Gerard J. Murphy. *C^*-algebras and operator theory.* Boston, MA etc.: Academic Press, Inc, 1990.

[Odi1] P.G. Odifreddi. *Classical recursion theory. The theory of functions and sets of natural numbers.* Studies in Logic and the Foundations of Mathematics, 125. Amsterdam etc.: North-Holland, 1989.

[Odi2] P.G. Odifreddi. *Classical recursion theory. Vol. II.* Studies in Logic and the Foundations of Mathematics. 143. Amsterdam: Elsevier, 1999.

[Poh1] Wolfram Pohlers. *Mathematische Grundlagen der Informatik.* Handbuch der Informatik. München: Oldenbourg., 1993.

[Poh2] Wolfram Pohlers. *Einführung in die Mathematische Logik und Theoretische Informatik.* Vorlesungsmitschrift, 2003.

[Rud] Walter Rudin. *Functional analysis. 2nd ed.* International Series in Pure and Applied Mathematics. New York, NY: McGraw-Hill, 1991.

[Soa] Robert I. Soare. *Recursively enumerable sets and degrees. A study of computable functions and computably generated sets.* Perspectives in Mathematical Logic. Berlin etc.: Springer-Verlag, 1987.

[vQ] Boto von Querenburg. *Mengentheoretische Topologie. 3., neu bearb. und erw. Aufl.* Berlin: Springer., 2001.

[Wer] Dirk Werner. *Funktionalanalysis. 5. erw. Aufl.* Springer-Lehrbuch. Berlin: Springer, 2005.