Lösungen linearer Polynomgleichungen in Funktionenkörpern und Uniformisierbarkeit von t-Moduln

Dissertation zur Erlangung des akademischen Grades
eines Doktors der Naturwissenschaften (Dr. rer. nat.)
am Fachbereich Mathematik und Naturwissenschaften
der Universität Kassel

vorgelegt von

Dipl.-Math. Dominik Wulf

geboren in Marsberg

4. Januar 2018

Institut für Mathematik
Universität Kassel

Tag der mündlichen Prüfung

31.01.2018

Erstgutachter

Prof. Dr. Hans-Georg Rück

Zweitgutachter

PD Dr. Sebastian Petersen

Für Laura und meine Eltern.

Inhaltsverzeichnis

Vorwort

Diese Arbeit beschäftigt sich mit den Eigenschaften von Lösungen $\mathbb{F}_q$-linearer Polynomgleichungen über Funktionenkörpern, die sich aus der Untersuchung der Kriterien für die Uniformisierbarkeit von abelschen t-Moduln ergeben.

Die heutige Theorie der t-Moduln hat ihren Ursprung in der Arbeit [Drinfeld; 1974], in dem Drinfeld-Moduln eingeführt und untersucht wurden. In dieser zeigt sich, dass Drinfeld-Moduln, die von Drinfeld selbst noch elliptische Moduln genannt wurden, eine Analogie in Funktionenkörpern zu den klassischen elliptischen Kurven darstellen. Diese Analogie ist insbesondere dadurch gekennzeichnet, dass sich sowohl Drinfeld-Moduln als auch elliptische Kurven einem geeigneten Gitter und dessen Exponentialfunktion zuordnen lassen, und dass diese Zuordnung auch umgekehrt gilt.
Der Fall der elliptischen Kurven stellt sich so dar, dass diese isomorph zu einem Torus $\mathbb{C}/\Lambda$ sind, wobei Λ ein $\mathbb{Z}$-Gitter vom Rang 2 ist. Dabei ist $\mathbb{R}$ die Vervollständigung von $\mathbb{Q} = \mathrm{Quot}(\mathbb{Z})$, dem Quotientenkörper des euklidischen Rings $\mathbb{Z}$ bezüglich des Absolutbetrags (der zur Stelle ∞ gehört); weiter ist $\mathbb{C}$ der algebraische Abschluss von $\mathbb{R}$.
Die Situation bei den Drinfeld-Moduln verhält sich ganz entsprechend. Im Quotientenkörper $\mathbb{F}_q(t) = \mathrm{Quot}(\mathbb{F}_q[t])$ des euklidischen Rings $\mathbb{F}_q[t]$ ist ein Absolutbetrag gegeben durch $\left|\frac{f(t)}{g(t)}\right| = q^{\deg(g(t)-\deg(f(t))}$. Die Vervollständigung bezüglich dieses Betrags (der auch hier zur Stelle ∞ gehört) ist dann der Körper der formalen Laurent-Reihen $K_\infty = \mathbb{F}_q((\frac{1}{t}))$. Der algebraische Abschluss $\overline{K_\infty} = \overline{\mathbb{F}_q((\frac{1}{t}))}$ ist in diesem Fall jedoch nicht vollständig, so dass erst die Vervollständigung bezüglich des fortgesetzten Betrags, die wir mit C_∞ bezeichnen, dem Körper $\mathbb{C}$ entspricht. Damit erhalten wir die folgende Analogie zwischen Zahlkörpern und Funktionenkörpern:

$$\mathbb{F}_q[t] \sim \mathbb{Z}, \quad \mathbb{F}_q(t) \sim \mathbb{Q}, \quad K_\infty \sim \mathbb{R}, \quad \overline{K_\infty} \subset C_\infty \sim \mathbb{C}.$$

In der Arbeit [Drinfeld; 1974] wird entsprechend gezeigt, dass Drinfeld-Moduln isomorph zu einem analytischen Torus C_∞/Λ sind, wobei Λ ein $\mathbb{F}_q[t]$-Gitter ist.
Für mehrdimensionale Verallgemeinerungen von elliptischen Kurven und von Drinfeld-Moduln gilt diese Entsprechung von Tori und algebraischen Objekten im Allgemeinen jedoch nicht. Ein analytischer Torus $\mathbb{C}^d/\Lambda$, der durch ein Gitter vollen Rangs Λ in $\mathbb{C}^d$ gegeben ist, lässt sich nur dann einer abelschen Varietät (eine algebraische Varietät mit einer Gruppenstruktur) zuordnen, wenn das Gitter zusätzliche Eigenschaften besitzt.
In der Arbeit [Anderson; 1986] wird mit den t-Moduln eine mehrdimensionale Verallgemeinerung der Drinfeld-Moduln als algebraische Objekte eingeführt (womit diese eine Analogie zu abelschen Varietäten sind). Durch ein Gegenbeispiel wird gezeigt, dass sich t-Moduln nicht immer ein analytischer Torus $\overline{K}_\infty/\Lambda$ mit einem $\mathbb{F}_q[t]$-Gitter Λ in $\overline{K}_\infty$ zuordnen lässt. (Die Betrachtung von $\overline{K}_\infty$ anstatt C_∞ reicht an dieser Stelle aus.) Diejenigen t-Moduln, für die diese Zuordnung möglich ist (dies ist der Fall, wenn die eindeutige Exponentialfunktion des t-Moduls surjektiv ist), werden uniformisierbar genannt. Zudem werden t-Motive, die zu t-Moduln ein duales Konzept darstellen, eingeführt. Ihre Betrachtung (anstelle des zugehörigen t-Moduls) bietet oft gewisse Vorteile. In einem wichtigen Satz, dem Satz von Anderson, wird ein Zusammenhang zwischen Uniformisierbarkeit, Eigenschaften des t-Moduls und Eigenschaften des t-Motivs bewiesen.

Die Frage, welche genauen Kriterien entscheidend dafür sind, wann ein t-Modul uniformisierbar ist und wann nicht, ist ein offenes Problem. Es gibt einige Untersuchungen, die diese Frage in Teilen beantworten, wobei die von [Böckle und Hartl; 2007] und [Bangert; 2011] für diese Arbeit am wichtigsten sind.
In [Böckle und Hartl; 2007] wird gezeigt, dass die Menge der t-Moduln, die zu uniformisierbaren t-Motiven gehören, innerhalb der Menge der τ-Garben, einer Verallgemeinerung der t-Motive, eine Berkovich-offene Menge bilden. Weiterhin werden die Ergebnisse an Beispielen von Rang 2 in der Dimension 2 angewendet.
In [Bangert; 2011] wird eine Beispielserie von t-Moduln von Rang 4 in der Dimension 2 untersucht, wobei diese durch die Form

$$t = I_2\tau^2 + A\tau + \theta I_2\tau^0$$

mit einer Matrix $A \in \mathrm{Mat}_{2\times 2}(\overline{K}_\infty)$ charakterisiert sind. (I_2 bezeichnet hier die Einheitsmatrix, τ den Frobenius-Endomorphismus von $\mathbb{F}_q$ und θ eine Konstante mit $|\theta| = q$.)

Es wird gezeigt, dass die Uniformisierbarkeit eines t-Moduls abhängig von der Lösbarkeit einer rekursiv definierten Folge von speziellen $\mathbb{F}_q$-linearen Polynomgleichungen in zwei Variablen ist, so dass die Folge der Lösungen gegen 0 konvergiert. Diese Gleichungen werden durch elementare Umformungen in eine Polynomgleichung in einer Komponente von einer der Variablen aufgelöst, wozu das zugehörige Newton-Polygon untersucht wird. In der Beispielfamilie wird dann eine Teilfamilie ausgemacht, für die es hinreichende Kriterien für die Lösbarkeit (mit Konvergenz gegen 0) der rekursiven Gleichungen gibt, und eine weitere Teilfamilie, für die es notwendige Bedingungen gibt. Dabei überschneiden sich diese Teilfamilien nicht; sie entstammen jeweils den einfachsten Formen des Newton-Polygons, dessen Untersuchung ansonsten durch die Vielzahl der Terme in den Koeffizienten des aufgelösten Polynoms zu viele Fallunterscheidungen benötigt.

Die Beispielfamilie von t-Moduln aus [Bangert; 2011] ist der Ausgangspunkt dieser Arbeit, wobei wir diese in höhere Dimensionen verallgemeinern, indem wir Matrizen A und $I_d \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)$ mit beliebigem $d \geq 2$ zulassen. Eine Auflösung der linearen Polynomgleichungen in eine Komponente von einer der Variablen und eine Untersuchung des zugehörigen Newton-Polygons führen bereits in Dimension $d = 2$, dazu, dass Einschränkungen nötig sind, um konkrete hinreichende oder notwendige Bedingungen für die Uniformisierbarkeit der zugehörigen t-Moduln herleiten zu können. Die Vielzahl der Fallunterscheidungen macht es schwierig, eine vollständige Analyse durchzuführen, wie aus den Ergebnissen von [Bangert; 2011] ersichtlich ist.

Das Ziel dieser Arbeit ist es, andere Methoden zu entwickeln, mit denen sich die speziellen rekursiv voneinander abhängigen linearen Polynomgleichungen, die die Uniformisierbarkeit von t-Moduln charakterisieren, untersuchen lassen.
Das Problem besteht konkret darin, notwendige und hinreichende Bedingungen zu finden, unter denen es zu der linearen Polynomgleichung

$$f(x,y) := \begin{pmatrix} x_1^{q^2} \\ \vdots \\ x_d^{q^2} \end{pmatrix} + A^T \begin{pmatrix} x_1^{q} \\ \vdots \\ x_d^{q} \end{pmatrix} + \theta \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} - \theta^{-q} \begin{pmatrix} y_1^{q^2} \\ \vdots \\ y_d^{q^2} \end{pmatrix}$$

in den Unbestimmten $x = (x_1, \ldots, x_d)^T$ und $y = (x_1, \ldots, x_d)^T \in \overline{K}_\infty^{\,d}$ für einen gegebenen

Folgenanfang $\underline{x}_0, \ldots, \underline{x}_k \in \overline{K}_\infty^d$ unter der Konvention $\underline{x}_{-1} := 0$ mit

$$f(\underline{x}_i, \underline{x}_{i-1}) = 0 \quad \text{für} \quad k \geq i \geq 0$$

eine Fortsetzung $\underline{x}_0, \ldots, \underline{x}_k, \ldots \underline{x}_{k+l}$ mit $l \in \mathbb{N}_0$ gibt, so dass gilt:

1. $f(\underline{x}_i, \underline{x}_{i-1}) = 0$ gilt für alle i mit $k + l \geq i \geq 0$,
2. $v_\infty(\underline{x}_{k+l}) \geq v_\infty(\underline{x}_{k-1}) + c$ für eine fest vorgegebene Konstante $c > 0$?

Anstatt die Gleichung $f(x, y)$ zu gegebenem y in eine Komponente der Variable x aufzulösen, ist die Grundidee dieser Arbeit, die besondere Struktur als lineare Polynomgleichung zu nutzen. Die gesuchten Ergebnisse sollen dabei möglichst Bedingungen an A als Matrix und y als Vektor sein und nicht Bedingungen an die einzelnen Komponenten von A und y. Ein erster entsprechender Ansatz ist dabei die Verwendung des Henselschen Lemmas, das eine ähnliche Funktion wie das Newton-Polygon hat, aber direkt in höheren Dimensionen anwendbar ist. Eine weitere Idee ist es, die rekursive Abhängigkeit der Lösungen zu untersuchen. Diese beiden Ansätze hatten nur bedingten Erfolg. Ein besseres Ergebnis liefert in dieser Arbeit der Ansatz, die Linearität der Polynomgleichung zu verwenden, um Probleme zu formulieren, deren Bedingungen für ihre Lösbarkeit äquivalente (oder zumindest hinreichende) Kriterien für die Lösbarkeit von $f(x, y)$ darstellen.

Die Arbeit ist wie folgt gegliedert:

In Kapitel 1 führen wir die wichtigsten Grundlagen über additive und $\mathbb{F}_q$-lineare Polynome, Funktionenkörper und die wichtigsten Werkzeuge aus der nicht-archimedischen Analysis ein, die wir in den späteren Kapiteln benötigen. Zudem erklären wir den Begriff des projektiven Limes, mit dem sich das Hauptproblem dieser Arbeit formulieren lässt.

In Kapitel 2 fassen wir die Teile der Theorie der t-Moduln zusammen, die für diese Arbeit wichtig sind. Wir beschreiben Drinfeld-Moduln und die Zuordnung zu Gittern. Dann definieren wir t-Motive, t-Moduln und den Begriff der Uniformisierbarkeit. Wir verwenden dann den an dieser Stelle wichtigen Satz von Anderson, um äquivalente Bedingungen für die Uniformisierbarkeit von t-Moduln zu erhalten.

In Kapitel 3 gehen wir auf die Beispielfamilie von t-Moduln aus der Arbeit [Bangert; 2011] ein und verallgemeinern diese in höhere Dimensionen $d \geq 2$. Wir stellen die Frage nach der Uniformisierbarkeit dieser t-Moduln als Problem von speziellen linearen Polynomgleichungen, die rekursiv voneinander abhängen, dar, die der Satz von Anderson für die diese Beispielfamilie impliziert. Wir erklären dabei die algebraischen Objekte, bestimmte $\mathbb{F}_q[t]$- und $\mathbb{F}_q[[t]]$-Moduln, die in diesem Zusammenhang wichtig sind, und ihre Eigenschaften. Anschließend formulieren wir entsprechende Probleme spezieller Polynomgleichungen, unabhängig von der Frage nach Kriterien für die Uniformisierbarkeit der t-Moduln.

In Kapitel 4 erforschen wir systematisch mit verschiedenen Mitteln die in Kapitel 3 motivierten Probleme spezieller Polynomgleichungen. Wir fassen die wichtigsten Resultate der einzelnen Abschnitte hier kurz zusammen:

4.1 Wir zeigen, dass eine Auflösung der beliebiger Polynomgleichungen in eine Komponente einer der Variablen auch in höheren Dimensionen stets möglich ist, wodurch eine Betrachtung des Newton-Polygons prinzipiell möglich ist.

4.2 Mit dem Henselschen Lemma weisen wir nach, dass es immer eine Fortsetzung zu einer Folge von Lösungen gibt, die gegen 0 konvergiert, falls der Betrag einer einzigen Lösung in einem Folgenanfang klein genug ist.

4.3 Wir untersuchen die rekursive Folge von linearen Polynomgleichungen, die sich ergibt, wenn man die rekursive Abhängigkeit der speziellen Polynomgleichungen ausnutzt und beschreiben ihre Lösungen.

4.4 Wir zeigen, dass die Bedingung für die Lösbarkeit der speziellen Polynomgleichungen, zusammen mit einer geeigneten Konvergenzeigenschaft der Folge der Lösungen, hinreichend erfüllt ist, wenn zwei lineare Polynomgleichungen der Form

$$\begin{pmatrix} z_1^{q^2} \\ \vdots \\ z_d^{q^2} \end{pmatrix} - M \begin{pmatrix} z_1 \\ \vdots \\ z_d \end{pmatrix} = a$$

für gewisse $M \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)$ und $a \in \overline{K}_\infty^d$ mit $|z| \leq 1$ lösbar sind.

Mit Hilfe des Satzes von Lang-Steinberg leiten wir dann für beliebige invertierbare Matrizen M unter der Voraussetzung $|a| < 1$ hinreichende Bedingungen für die Lösbarkeit dieses Teilproblems her.

4.5 Wir erweitern die Ergebnisse aus Abschnitt 4.4 für den wichtigen Spezialfall der Antidiagonalmatrizen der Dimension $d = 2$ (ohne weitere Einschränkungen an den Betrag von a) und stellen Bedingungen für die Lösbarkeit dieses Problems fest, die gleichzeitig notwendig und hinreichend sind.

In Kapitel 5 erklären wir die Bedeutungen der Resultate aus Kapitel 4 für die Untersuchung von Kriterien für die Uniformisierbarkeit von t-Moduln.

Danksagung

Ich möchte mich an dieser Stelle bei allen bedanken, die mich während der Entstehung dieser Arbeit unterstützt und motiviert haben.

An erster Stelle bedanke ich mich bei Herrn Prof. Dr. Hans-Georg Rück für die hervorragende und umfangreiche Betreuung dieser Arbeit, für seine zahlreichen Anregungen und seine Unterstützung.

Ebenfalls möchte ich mich bei Matthias Fetzer, Robin Göller, John Abbott und Jennylee Müller für die vielen Gespräche und ihre Hilfsbereitschaft bedanken. Außerdem bedanke ich mich bei Herrn Prof. Dr. Peter Dräxler für seinen Rat und sein offenes Ohr.

Ein besonders herzlicher Dank gebührt Laura Marschollek vor allem für ihren Rückhalt, ihre Unterstützung und ihre Geduld, aber auch für das Korrekturlesen und die hilfreichen Anmerkungen.

Zu guter Letzt möchte ich meiner Familie für ihren Rückhalt danken.

Dominik Wulf
Kassel, Januar 2018

1 Grundlagen

Wir führen in diesem Kapitel die grundlegenden Begriffe dieser Arbeit ein und stellen ihre wichtigsten Eigenschaften vor.

1.1 Additive Polynome

Additive Polynome spielen in der Theorie der t-Moduln eine zentrale Rolle, wodurch die Untersuchungen spezieller additiver Polynome im Verlauf dieser Arbeit motiviert werden. Die Einführung folgt dem Aufbau von [Goss; 1996, Kapitel 1]; dort werden jedoch zunächst die additiven Polynome noch von absolut additiven Polynomen unterschieden, worauf wir bereits von Vornherein verzichten wollen.

Es sei K ein Körper der Charakteristik p und $\overline{K}$ ein fest gewählter algebraischer Abschluss von K. Wir betrachten Polynome $P(x) \in K[x]$, so dass für alle $\alpha, \beta \in K$ gilt:

$$P(\alpha + \beta) = P(\alpha) + P(\beta).$$

Wenn zwei Polynome $P(x), Q(x) \in K[x]$ diese additive Eigenschaft über K haben, dann gilt dies für die Polynome $P(x) + Q(x)$, $\alpha P(x)$ mit $\alpha \in K$ und $P(Q(x))$ ebenfalls.

1.1.1 Definition. *$P(x) \in K[x]$ heißt additiv, falls $P(\alpha + \beta) = P(\alpha) + P(\beta)$ für alle $\alpha, \beta \in \overline{K}$ gilt (das heißt, die additive Eigenschaft gilt sogar über $\overline{K}$).*

Das wichtigste Beispiel eines additiven Polynoms ist der Frobenius-Homomorphismus τ_p zur Charakteristik p mit $\tau_p(x) = x^p$. Weiter schreiben wir $\tau_p^i(x) := x^{p^i}$.

1.1.2 Definition. *Es sei $K\{\tau_p\} := \{\sum_{i=0}^{k} \alpha_k \tau_p^i \mid \alpha_i \in K\}$ die Teilmenge der Polynome von $K[x]$, die sich als K-Linearkombinationen von $\{\tau_p^k \mid k \in \mathbb{N}_0\}$ darstellen lässt.*

Die Monome $\tau_p^i(x)$ und alle Polynome, die durch diese aufgespannt werden, sind additiv. Mit den bisherigen Beobachtungen bildet damit $K\{\tau\}$ unter den Verknüpfungen Addition und Komposition einen Ring (auch Kompositionsring genannt).

1.1.3 Bemerkung. *Wenn $K \neq \mathbb{F}_p$ ist, dann ist der Ring $K\{\tau_p\}$ nicht kommutativ, denn für alle $\alpha \in K$ gilt der "Twist"*

$$\tau_p \alpha = \alpha^p \tau_p.$$

Falls der Körper K endlich ist, kann für gewisse $P(x) \in K[x]$ die additive Eigenschaft $P(\alpha) + P(\beta) = P(\alpha + \beta)$ für alle $\alpha, \beta \in K$ gelten, auch wenn $P(x) \notin K\{\tau_p\}$ ist.
Ein Beispiel ist das Polynom $P(x) = x + (x^3 - x)^2 = x^6 + x^4 + x^2 + x$ über $\mathbb{F}_3$; hier ist sogar $P(\alpha) = \alpha$ für alle $\alpha \in \mathbb{F}_3$, aber $P(x) \notin \mathbb{F}_3\{\tau_p\}$.

Falls K dagegen nicht endlich ist, können solche Polynome nicht auftreten. In dieser Situation lässt sich $K\{\tau_p\}$ durch das folgende Resultat charakterisieren.

1.1.4 Proposition. *Sei K nicht endlich und $P(x) \in K[x]$. Dann ist $P(x) \in K\{\tau_p\}$ genau dann, wenn $P(\alpha) + P(\beta) = P(\alpha + \beta)$ für alle $\alpha, \beta \in K$ gilt.*

Beweis. Siehe [Goss; 1996, Proposition 1.1.5]. □

Insbesondere ist $\overline{K}$ nicht endlich, da der algebraische Abschluss eines Körpers stets unendlich viele Elemente enthält, und wir erhalten:

1.1.5 Folgerung. *$K\{\tau_p\}$ ist gleich der Menge der additiven Polynome aus $K[x]$.*

Von nun an sei stets $q = p^r$. Wir nehmen weiter an, dass $\mathbb{F}_q \subseteq K$ gilt. Die folgende Definition wird im Laufe dieser Arbeit immer wieder auftauchen.

1.1.6 Definition. *Es sei $\tau := \tau_p^r$ und $K\{\tau\}$ der Kompositionsring der Polynome in τ. Wir nennen $K\{\tau\}$ den Ring der q-Polynome (oder "Twist"-Polynome).*

Wir sehen, dass $K\{\tau\}$ gleich der $\mathbb{F}_q$-Algebra der $\mathbb{F}_q$-linearen Polynome aus $K[x]$ ist.

1.1.7 Bemerkung.

1. *$P(\tau) = \sum_{i=0}^k \alpha_k \tau^i \in K\{\tau\}$ wird in $K[x]$ repräsentiert durch*

$$P(\tau(x)) = \sum_{i=0}^{k} \alpha_k x^{q^i} \in K[x];$$

diese Repräsentation von $P(\tau) \in K\{\tau\}$ durch $P(\tau(x)) \in K[x]$ ist eindeutig, sie entspricht aber nicht der formalen Substitution von x durch τ.

2. *Mit der Multiplikation "$P(\tau) \cdot Q(\tau)$" ist stets die multiplikative Verknüpfung in $K\{\tau\}$, also die Komposition der Abbildungen und nicht die Multiplikation der Darstellungen als Polynome in $K[x]$ gemeint.*

Die Darstellung $P(\tau(x)) \in K[x]$ als Polynom erlaubt es uns, einige Eigenschaften auf $P(\tau)$ in $K\{\tau\}$ zu übertragen.

1.1.8 Definition.

1. *$P(\tau) \in K\{\tau\}$ heißt normiert genau dann, wenn $P(\tau(x))$ normiert ist.*

2. *Wenn $P(\tau) = \sum_{i=0}^{k} \alpha_i \tau^i$ mit $\alpha_k \neq 0$ ist, bezeichnen wir $\deg(P(\tau)) := k$ als q-Grad von $P(\tau)$. Es gilt dabei*
$$q^{\deg(P(\tau))} = \deg(P(\tau(x))).$$

3. *Wir bezeichnen mit $D_\tau \in \mathrm{Hom}_K(K\{\tau\}, K)$ die formale Ableitung in $K\{\tau\}$. Für $f(\tau) = \sum_{i=0}^{k} \alpha_k \tau_p^i \in K\{\tau\}$ gilt dann wegen der Eigenschaft als q-Polynom (es gilt hier $\tau^0(x) = x^{q^0} = x$) in der Charakteristik q:*
$$D_\tau f := f'(\tau) = \alpha_0.$$

Aus den bisherigen Überlegungen ist klar, dass die Nullstellenmenge eines additiven Polynoms $P(x)$ sicherlich eine additive Gruppe in $\overline{K}$ ist. Die folgende Umkehrung ist nun der sogenannte "Hauptsatz der additiven Polynome".

1.1.9 Satz. *Sei $P(x) \in K[x]$ ein separables Polynom. Dann ist $P(x)$ genau dann additiv (bzw. $\mathbb{F}_q$-linear), wenn seine Nullstellenmenge $\{w_1, \ldots, w_k\} \subset \overline{K}$ eine Untergruppe (bzw. ein $\mathbb{F}_q$-Vektorraum in $\overline{K}$) ist.*

Beweis. Siehe [Goss; 1996, Theorem 1.2.1 und Folgerung 1.2.2]. □

Wir erläutern nun die Struktur von $K\{\tau\}$. Dazu stellen wir zunächst die Division mit Rest im Sinne der üblichen Divisionsalgorithmen fest.

1.1.10 Proposition. *Seien $f(\tau), g(\tau) \in K\{\tau\}$ und $g(\tau) \neq 0$, dann gibt es eindeutig bestimmte $a(\tau), r(\tau) \in K\{\tau\}$ mit*

$$f(\tau) = a(\tau) \cdot g(\tau) + r(\tau) \quad \textit{und} \quad \deg(r(\tau)) < \deg(g(\tau)).$$

1.1.11 Folgerung. *Jedes Linksideal in $K\{\tau\}$ ist ein Hauptideal.*

Wir nennen einen Körper K perfekt, falls $\tau(K) = K$ ist. Dies ist gleichbedeutend damit, dass jedes $\alpha \in K$ eine eindeutig bestimmte q-te Wurzel besitzt (denn $x \mapsto \tau(x)$ ist stets injektiv). In diesem Fall können wir dann auch in $K\{\tau\}$ von rechts (mit Rest) dividieren.

1.1.12 Proposition. *Sei K perfekt, dann gibt es zu $f(\tau), g(\tau) \in K\{\tau\}$ mit $g(\tau) \neq 0$ eindeutig bestimmte $b(\tau), r(\tau) \in K\{\tau\}$ mit*

$$f(\tau) = g(\tau) \cdot b(\tau) + r(\tau) \quad \textit{und} \quad \deg(r(\tau)) < \deg(g(\tau)).$$

1.1.13 Folgerung. *Jedes Rechtsideal in $K\{\tau\}$ ist ein Hauptideal, falls K perfekt ist.*

Wir erklären nun noch die Wirkung von τ auf Objekte höherer Dimensionen.

1.1.14 Definition. *Wir definieren für $i \in \mathbb{N}_0$:*

$$\begin{aligned}
x^{(i)} &:= \tau^i(x) := \begin{pmatrix} x_1^{q^i} \\ \vdots \\ x_d^{q^i} \end{pmatrix} \quad \textit{für} \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_d \end{pmatrix} \in K^d \quad \textit{und} \\
A^{(i)} &:= \tau^i(A) := \begin{pmatrix} a_{1,1}^{q^i} & \dots & a_{1,n}^{q^i} \\ \vdots & & \vdots \\ a_{m,1}^{q^i} & \dots & a_{m,n}^{q^i} \end{pmatrix} \quad \textit{für} \quad A = \begin{pmatrix} a_{1,1} & \dots & a_{1,n} \\ \vdots & & \vdots \\ a_{m,1} & \dots & a_{m,n} \end{pmatrix} \in \mathrm{Mat}_{m\times n}(K).
\end{aligned}$$

Dies entspricht der Wirkung von τ^i komponentenweise auf K^n und $\mathrm{Mat}_{m\times n}(K)$.

Falls K perfekt ist, sind analog die eindeutig bestimmten Elemente $x^{(-i)} \in K^n$ und $A^{(-i)} \in \mathrm{Mat}_{m\times n}(K)$ definiert, indem komponentenweise die q^i-te Wurzel gezogen wird.

Für zwei Matrizen $A, B \in \mathrm{Mat}_{d\times d}(K)$ folgt nun analog zum "Twist" in $K\{\tau\}$:

$$A\tau^i \cdot B\tau^j = AB^{(i)}\tau^{i+j}.$$

1.1.15 Proposition. *Es gilt die Gleichheit der Ringe* $\mathrm{Mat}_{d\times d}(K\{\tau\}) = \mathrm{Mat}_{d\times d}(K)\{\tau\}$.

Dabei stellen wir einige Eigenschaften von Matrizen über $K\{\tau\}$ fest.

1.1.16 Definition.

1. *Wir bezeichnen analog zu Definition 1.1.8 mit* $D \in \mathrm{Hom}_K(\mathrm{Mat}_{d\times d}(K)\{\tau\}, \mathrm{Mat}_{d\times d}(K))$ *die formale Ableitung in* $\mathrm{Mat}_{d\times d}(K)\{\tau\}$. *Für* $f(\tau) = \sum_{i=0}^{k} A_i\tau^i \in \mathrm{Mat}_{d\times d}(K)\{\tau\}$ *ist diese gegeben durch:*
$$D_\tau f(\tau) = A_0.$$

2. *Eine Matrix* $A \in \mathrm{Mat}_{d\times d}(K\{\tau\})$ *ist invertierbar, das heißt* $A \in GL_d(K\{\tau\})$, *falls es Matrizen* U *und* $V \in \mathrm{Mat}_{d\times d}(K\{\tau\})$ *gibt, so dass gilt:*
$$UA = I_d = AV$$
In diesem Fall gilt $U, V \in GL_d(K\{\tau\})$ *und es folgt* $U = V$.

1.1.17 Proposition. *Sei* K *perfekt und* $Q \in \mathrm{Mat}_{m\times n}(K\{\tau\})$, *dann gibt es Matrizen* $G \in \mathrm{GL}_m(K\{\tau\})$ *und* $H \in \mathrm{GL}_n(K\{\tau\})$, *so dass alle Einträge außerhalb der Diagonalen (das heißt alle Einträge mit Indizes* $i \neq j$*) von* GQH *verschwinden.*

Beweis. Die Einträge außerhalb der Diagonalen können reihen- und spaltenweise sukzessive mit den Divisionsalgorithmen von links und (da K perfekt ist) auch von rechts eliminiert werden. Siehe [Goss; 1996, Proposition 5.4.8]. □

Additive Gruppenschemata

Wir führen noch eine weitere Betrachtungsweise für $K\{\tau\}$ an, die im Hinblick auf die "Geometrie" der t-Moduln in Kapitel 2 eine wichtige Rolle spielt.

1.1.18 Bemerkung. *Der Ring $K\{\tau\}$ kann nach Satz 1.1.9 auf natürliche Weise als Kompositionsring $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})$ der $\mathbb{F}_q$-linearen Endomorphismen des additiven Gruppenschemas $\mathbb{G}_{a,K}$ über K verstanden werden; dabei ist τ^0 die Identität in $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K})$.*

Im Weiteren sei E eine algebraische Gruppe, die zu dem d-dimensionalen additiven Gruppenschema $\mathbb{G}_{a,K}^d$ mit $d \in \mathbb{N}$ isomorph ist. Wir können also stets Koordinaten wählen, so dass sich E über K^d darstellen lässt. Weiter bezeichnen wir mit $\mathrm{End}_{\mathbb{F}_q}(E)$ den Ring der $\mathbb{F}_q$-linearen Endomorphismen von $E \cong \mathbb{G}_{a,K}^d$ in diesen Koordinaten über K^d.

Wir stellen fest, dass sich mit Definition 1.1.14 Endomorphismen aus $\mathrm{End}_{\mathbb{F}_q}(E)$ durch Elemente in $\mathrm{Mat}_{d\times d}(K)\{\tau\}$ darstellen lassen.

1.1.19 Proposition. $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,K}^d)$ *ist in natürlicher Weise isomorph zu* $\mathrm{Mat}_{d\times d}(K)\{\tau\}$.

Beweis. Siehe [Humphreys; 1975, Kapitel 20.3] □

Das heißt, nach Wahl von Koordinaten gibt es zu jedem $f \in \mathrm{End}_{\mathbb{F}_q}(E)$ eindeutig bestimmte Matrizen $A_i \in \mathrm{Mat}_{d\times d}(K)$, so dass $f = \sum_{i=0}^{k} A_i\tau^i \in \mathrm{Mat}_{d\times d}(K)\{\tau\}$ die entsprechende Darstellung von f ist.

1.2 Funktionenkörper

In diesem Abschnitt fassen wir die Resultate der nicht-archimedischen Analysis, die wir im Laufe der Arbeit benötigen, zusammen. Wir halten uns dabei an den Aufbau von [Neukirch; 1992, Kapitel II] und [Goss; 1996, Kapitel 2].

Wir werden mit Funktionenkörpern in dieser Arbeit durchgehend nicht-archimedische Körper betrachten. Dies sind in der Regel die Körper $\mathbb{F}_q((\frac{1}{t}))$, endliche algebraische Erweiterungen L von $\mathbb{F}_q((\frac{1}{t}))$ und ein fest gewählter algebraischer Abschluss $\overline{\mathbb{F}_q((\frac{1}{t}))}$.

Es sei zunächst K ein beliebiger Körper der Charakteristik p, der bezüglich einer reellwertigen Bewertung v vollständig ist. Das heißt genauer, dass es eine Bewertungsfunktion $v : K \to \mathbb{R} \cup \{\infty\}$ gibt, so dass für alle $x, y \in K$ gilt:

1. $v(x) = \infty \Longleftrightarrow x = 0$,
2. $v(x \cdot y) = v(x) + v(y)$,
3. $v(x + y) \geq \min\{v(x), v(y)\}$.

Wir nennen v diskret, wenn $v : K \to \mathbb{Z} \cup \{\infty\}$ surjektiv ist.

Es sei $c \in \mathbb{R}$ mit $0 < c < 1$, dann erhalten wir durch die Definition $|x|_v := c^{v(x)}$ für $x \neq 0$ und $|0|_v := 0$ eine Betragsfunktion $|\cdot|_v : K \to \mathbb{R}_0^+$. Das heißt also, dass der Betrag $|x|_v$ von x klein ist genau dann, wenn $v(x)$ groß ist. Dies erlaubt es, die Vollständigkeit von K bezüglich v im üblichen Sinn von Cauchy-Folgen zu betrachten.
Wegen 3. wird die Topologie auf K also durch einen Betrag $|\cdot|_v$ geliefert, der zusätzlich zur normalen Dreiecksungleichung die sogenannte ultrametrische Ungleichung

$$|x + y|_v \leq \max\{|x|_v, |y|_v\}$$

erfüllt. Folglich gilt für den Körper K nicht die archimedische Eigenschaft, die besagt, dass zu jedem $x \in K$ eine natürliche Zahl n existiert, so dass $|\underbrace{1 + \ldots + 1}_{n\text{-mal}}|_v > |x|_v$ ist.

1.2.1 Definition. *Der Körper K sei bezüglich einer diskreten Bewertung v vollständig. K heißt dann lokaler Körper, wenn K bezüglich der von v induzierten Topologie lokal kompakt ist.*

Der Ganzheitsring $\mathcal{O}$ von K ist gegeben durch

$$\mathcal{O} := \mathcal{O}_K := \{x \in K \mid |x|_v \leq 1\} = \{x \in K \mid v(x) \geq 0\},$$

dabei ist $\mathcal{O}$ ein lokaler Ring zu dem maximalen Ideal $\mathfrak{m} \subset \mathcal{O}$ mit

$$\mathfrak{m} := \mathfrak{m}_K := \{x \in K \mid |x|_v < 1\} = \{x \in K \mid v(x) > 0\}.$$

Es lässt sich zeigen, dass ein Körper K genau dann ein lokaler Körper ist, wenn $\mathcal{O}$ kompakt und damit der Restklassenkörper $\mathcal{O}/\mathfrak{m}$ endlich ist.

Wir führen in dem folgenden Beispiel die eingangs erwähnten Funktionenkörper, die für diese Arbeit eine ganz wesentliche Bedeutung haben, als lokale Körper ein.

1.2.2 Beispiel. *Es sei $K := \mathbb{F}_q(t) = \mathrm{Quot}(\mathbb{F}_q[t])$, der Quotientenkörper des euklidischen Rings $\mathbb{F}_q[t]$ zusammen mit der folgenden Bewertung v_∞ (zur Stelle ∞):*

> *Zu $x \in \mathbb{F}_q(t)^\times$ betrachten wir die (nicht notwendigerweise gekürzte) Darstellung $x = \frac{f(t)}{g(t)}$ mit $f(t), g(t) \in \mathbb{F}_q[t]$. Wir definieren dann:*
>
> $$v_\infty(x) := \deg(g(t)) - \deg(f(t)) \text{ für } x \in \mathbb{F}_q(t)^\times; \quad \text{und } v_\infty(0) := \infty.$$

$K_\infty := \mathbb{F}_q((\frac{1}{t}))$, der Körper der formalen Laurent-Reihen in $1/t$, ist die Vervollständigung des Körpers K bezüglich der Bewertung v_∞.

Wir nehmen nun an, dass K ein lokaler Körper ist, wobei $|\mathcal{O}/\mathfrak{m}| = p^r = q$ gilt. Wir setzen dann $c := 1/q$. In diesem Fall ist v diskret und der durch v definierte Betrag $|\cdot|_v$ normiert. Es gilt also:

$$|x|_v = (1/q)^{v_\infty(x)}.$$

Für eine Einheit $u \in \mathcal{O}^\times$ gilt $|x|_v = 1$ bzw. $v(x) = 0$, damit ist $\mathfrak{m} = \mathcal{O} \backslash \mathcal{O}^\times$. Ein Element $\pi \in \mathcal{O}$ mit $v(\pi) = 1$ nennen wir Primelement; es gibt für jedes $x \in K^\times$ eine eindeutige Darstellung $x = u\pi^m$ mit $m \in \mathbb{Z}$ und $u \in \mathcal{O}^\times$.

1.2.3 Satz. *Ein Körper K ist genau dann ein lokaler Körper, wenn K eine endliche Erweiterung von $\mathbb{Q}_p$ oder $\mathbb{F}_q((\frac{1}{t}))$ ist.*

Beweis. Siehe [Neukirch; 1992, Satz II.5.2]. □

Im nicht-archimedischen Fall ist die endliche Erweiterung eines vollständigen Körpers bezüglich der (eindeutigen) fortgesetzten Bewertung wieder vollständig (siehe [Neukirch; 1992, Theorem II.4.8]). Jedoch gilt dies nicht für den algebraischen Abschluss $\overline{K}$ von K, so dass wir die Vervollständigung $\hat{\overline{K}}$ von $\overline{K}$ betrachten.

1.2.4 Proposition. *Sei K ein vollständiger Körper bezüglich der Bewertung v. Weiter sei $\overline{K}$ ein fest gewählter algebraischer Abschluss von K. Dann ist auch die Vervollständigung $\hat{\overline{K}}$ von $\overline{K}$ bezüglich der kanonischen Erweiterung von v algebraisch abgeschlossen.*

Beweis. Siehe [Goss; 1996, Proposition 2.1]. □

Der größte Unterschied zur klassischen Analysis ergibt sich für die Konvergenz von Reihen in K, für die sich ein vergleichsweise einfaches Kriterium angeben lässt.

1.2.5 Proposition. *Sei K ein vollständiger Körper bezüglich der Bewertung v.*

1. *Eine Reihe $\sum_{i=0}^{\infty} a_i$ mit Koeffizienten $a_i \in K$ konvergiert genau dann in K, wenn $\lim\limits_{i\to\infty} a_i = 0$ gilt (das heißt $\lim\limits_{i\to\infty} v(a_i) = \infty$).*
2. *Es sei $f(x) \in K[[x]]$ eine Potenzreihe und $\rho(f) := -\lim\limits_{i\to\infty} \frac{v(a_i)}{i}$, dann konvergiert $f(\alpha)$ für $\alpha \in K$ mit $v(\alpha) > \rho(f)$; und divergiert, falls $v(\alpha) < \rho(f)$ ist. Also ist $\rho(f)$ der Konvergenzradius von f.*

Beweis. Die Aussagen folgen aus der ultrametrischen Dreiecksungleichung. □

Entsprechend nennen wir eine Potenzreihe $f(x) \in K[[x]]$ ganz in K, falls $\rho(f) = -\infty$ ist (das heißt, dass $f(\alpha)$ für alle $\alpha \in K$ konvergiert).

1.2.6 Bemerkung. *Sei K vollständig, aber nicht algebraisch abgeschlossen und $f(x) \in K[[x]]$. Falls $v(\alpha) > \rho(\alpha)$ für $\alpha \in \overline{K}$ ist, dann konvergiert $f(\alpha)$ in $K(\alpha)$.*

Potenzreihen mit Koeffizienten in einer endlichen Erweiterung von K bilden somit Cauchy-Folgen, die in $\overline{K}$ konvergieren, wieder auf konvergente Cauchy-Folgen in $\overline{K}$ ab. Folglich können wir in $K(\alpha)$ arbeiten und müssen nicht zu $\hat{\overline{K}}$ übergehen, wenn wir die Konvergenz von Potenzreihen in $\alpha \in \overline{K}$ benötigen.

Das Henselsche Lemma

Ein wichtiges Mittel zur Bestimmung von Nullstellen von Polynomen und ihrer Bewertungen in nicht-archimedischen Körpern ist das Henselsche Lemma.

Es sei K ein Körper, der bezüglich der Bewertung v vollständig ist. Weiter seien $\mathcal{O}$ der Ganzheitsring und $\mathfrak{m}$ das maximale Ideal bezüglich v in K.

Ähnlich zum Newton-Verfahren in der klassischen Analysis lässt sich das folgende Resultat herleiten:

1.2.7 Satz. *Sei $\widetilde{f} \in \mathcal{O}[x]$ ein Polynom und für ein $a \in \mathcal{O}$ gelte $\widetilde{f}(a) \equiv 0 \bmod \mathfrak{m}$, dann gibt es genau genau ein $\widetilde{\xi} \in \mathcal{O}$, so dass gilt:*

$$\widetilde{f}(\widetilde{\xi}) = 0 \quad \textit{und} \quad \widetilde{\xi} \equiv a \bmod \mathfrak{m}.$$

Falls $\widetilde{f}'(a) \neq 0$ gilt, ist $\widetilde{\xi}$ eindeutig bestimmt.

In mehreren Variablen ist eine Verallgemeinerung dieser Version des Henselschen Lemmas wie folgt gegeben.

1.2.8 Satz. *Die Funktion $\widetilde{f} = (\widetilde{f}_1, \ldots, \widetilde{f}_d)^T : \mathcal{O}^d \to \mathcal{O}^d$ sei gegeben durch Polynome $\widetilde{f}_i \in \mathcal{O}[X]$ in den Unbestimmten $x = (x_1, \ldots, x_d)^T$. Weiter sei $J_{\widetilde{f}}(x)$ die Jacobi-Matrix von $\widetilde{f}$ an der Stelle x. Falls für ein $a = (a_1, \ldots, a_d)^T \in \mathcal{O}^d$ gilt:*

$$\widetilde{f}(a) \equiv \Big(\det(J_{\widetilde{f}}(a))\Big)^2 \bmod \mathfrak{m}^d,$$

dann existiert ein $\widetilde{\xi} = (\widetilde{\xi}_1, \ldots, \widetilde{\xi}_d)^T \in \mathcal{O}^d$, mit folgenden Eigenschaften:

$$\widetilde{f}(\widetilde{\xi}) = 0 \quad \textit{und} \quad \widetilde{\xi} \equiv a \bmod J_{\widetilde{f}}(a)\mathfrak{m}^d.$$

Falls $J_{\widetilde{f}}(a)$ invertierbar ist, ist $\widetilde{\xi}$ eindeutig bestimmt.

Beweis. Siehe [Fisher; 1997, Theorem 1]. □

Newton-Polygone

Ein weiteres wichtiges Werkzeug zur Untersuchung der Bewertung von Nullstellen eines Polynoms in einer Variable über einem nicht-archimedischen Körper K ist das Newton-Polygon. Dieses wollen wir hier wie in [Neukirch; 1992, Kapitel II.6] vorstellen.

Im Folgenden sei K ein Körper zusammen mit einer Bewertung v, wobei K bezüglich v vollständig ist.

1.2.9 Definition. *Sei $f(x) = \sum_{i=0}^{k} a_i x^i \in K[x]$ ein Polynom mit $a_0 \neq 0$ und $a_n \neq 0$. Jedem der Monome $a_i x^i$ ordnen wir den Punkt $(i, v(a_i)) \in \mathbb{R}^2$ zu, wobei im Fall $a_i = 0$ der Punkt (i, ∞) ignoriert wird. Das Newton-Polygon von $f(x)$ ist dann die untere konvexe Hülle der Punktmenge*

$$\{(0, v(a_0)), (1, v(a_1)), \ldots, (k, v(a_k)).$$

Als untere konvexe Hülle besteht das Newton-Polygon stets aus einer endlichen Folge von Strecken, deren Steigungen von links nach rechts (mit anwachsendem i) streng monoton steigend sind. Die Steigungen dieser Strecken stehen in einer erstaunlichen Beziehung zu den Bewertungen der Nullstellen des zugehörigen Polynoms.

1.2.10 Satz. *Sei $f(x) = \sum_{i=0}^{k} a_i x^i \in K[x]$ ein Polynom mit $a_0 \neq 0$ und $a_n \neq 0$. Weiter sei $L \subseteq \overline{K}$ der Zerfällungskörper von $f(x)$ und w sei eine Fortsetzung von v auf L.*

Die Punkte $(i, v(a_i))$ und $(j, v(a_j)$ mit $j > i$ seien die Endpunkte einer Strecke S des Newton-Polygons von $f(x)$ und weiter sei $-m$ die Steigung von S. Dann besitzt $f(x)$ genau $j - i$ Nullstellen $\alpha_i, \ldots, \alpha_j \in L$ mit den Werten

$$w(\alpha_i) = \ldots = w(\alpha_j) = m.$$

Beweis. Die Nullstellen von $f(x)$ werden nach der Größe ihrer Bewertungen sortiert. Die Darstellung der Koeffizienten von a_i von $f(x)$ als elementarsymmetrische Funktionen in den Nullstellen und ein sorgfältiger Vergleich liefern dann die Aussage. Für Details siehe [Neukirch; 1992, Satz II.6.3]. □

1.2.11 Folgerung. *Falls es eine Strecke S im Newton-Polygon von $f(x)$ gibt, deren Projektion auf die x-Achse die Länge 1 hat, dann ist die zugehörige Nullstelle α von $f(x)$ bereits in K selbst enthalten.*

1.3 Projektive Limites

Das zentrale Problem dieser Arbeit lässt sich mit Hilfe projektiver Limites von Vektorräumen formulieren. Wir stellen daher diesen kurz vor.

Es sei K ein Körper und für jedes $k \in \mathbb{N}_0$ (oder aus einer beliebigen anderen halbgeordneten Menge I) sei V_i ein K-Vektorraum. Weiter sei für je zwei Indizes $i > j > 0$ ein Homomorphismus

$$\varphi_{i,j} : V_i \longrightarrow V_j$$

gegeben, so dass für $i > j > k \in \mathbb{N}_0$ gilt: $\varphi_{i,k} = \varphi_{j,k} \circ \varphi_{i,j}$.

1.3.1 Definition. *Der projektive Limes* $\varprojlim V_i \subset \left(\prod_{i\in\mathbb{N}_0} V_i\right)$ *sei gegeben durch*

$$\varprojlim V_i := \varprojlim_{i\in\mathbb{N}_0} V_i := \{(\underline{x}_i)_{i\in N_0} \in \prod_{i\in\mathbb{N}_0} V_i \mid \varphi_{i,j}(\underline{x}_i) = \underline{x}_j \textit{ für } i > j > 0\}.$$

(Im Fall der Indexmenge $I = \mathbb{N}_0$ *nennen wir* $(\underline{x}_i)_{i\in N_0}$ *eine Folge.)*

Durch die K-Vektorraumstruktur der Komponenten V_i lassen sich Addition und Skalarmultiplikation auf $\varprojlim V_i$ komponentenweise definieren. Dadurch wird der projektive Limes selbst zu einem K-Vektorraum, der die folgende universelle Eigenschaft besitzt:

1.3.2 Proposition. *Sei* W *ein Vektorraum und seien* $\psi_i : W \to V_i$ *für* $i \in \mathbb{N}_0$ *Homomorphismen, so dass* $\psi_j = \varphi_{i,j} \circ \psi_i$ *für alle* $i > j > 0$ *gilt. Dann existiert ein eindeutig bestimmter Homomorphismus* $\chi : W \to \varprojlim V_i$*, so dass* $\psi_i = \mathrm{pr}_i \circ \chi$ *für alle* $i \in \mathbb{N}_0$ *gilt.*

Beweis. Folgt aus der Definition. □

1.3.3 Proposition. $\varprojlim V_i$ *ist bis auf Isomorphie eindeutig bestimmt.*

Beweis. Folgt aus der universellen Eigenschaft. □

2 t-Moduln und Uniformisierbarkeit

Wir erläutern in diesem Kapitel die grundlegende Theorie der t-Moduln und erklären den Begriff der Uniformisierbarkeit, da dieser den Ausgangspunkt der Fragestellungen dieser Arbeit darstellt. Der Aufbau entspricht dabei [Goss; 1996, Kapitel 4 und 5], bzw. [Bangert; 2011, Kapitel 1]. t-Moduln lassen sich als eine mehrdimensionale Verallgemeinerung von Drinfeld-Moduln verstehen, die wir für ein besseres Verständnis kurz thematisieren, deren Beschreibung wir aber auf das Wesentliche beschränken. Eine ausführliche Einführung dieser findet sich in [Goss; 1996, Kapitel 3].

Wir werden in dieser Arbeit ausschließlich den Ring $\mathbb{F}_q[t]$ als Grundlage der Drinfeld- und t-Moduln verwenden und auf Betrachtungen allgemeinere Ringe verzichten. Für die Fragestellungen dieser Arbeit ist diese Vereinfachung ausreichend, zudem erleichtert sie die Theorie und Notationen.

Nach dem Vorgehen in Beispiel 1.2.2 erhalten wir die Funktionenkörper $K := \mathbb{F}_q(t)$, $K_\infty := \mathbb{F}_q((\frac{1}{t}))$ und $C_\infty := \hat{\overline{K}}$. Für die (fortgesetzte) Bewertung v_∞ gilt $v_\infty(t) = -1$ und für den normierten nicht-archimedischen Absolutbetrag ist damit $|t|_{v_\infty} = q$.

2.1 Drinfeld-Moduln und Gitter

Wir werden zunächst Drinfeld-Moduln und ihre wichtigsten Eigenschaften vorstellen, bevor wir uns mit ihrer Verallgemeinerung, den t-Moduln, befassen. Wir werden sehen, dass sich Drinfeld-Moduln eindeutig Gittern und der zugehörigen Exponentialfunktion zuordnen lassen und diese Zuordnung auch umgekehrt gilt.

2.1.1 Definition. *Ein Erweiterungskörper L von $\mathbb{F}_q$ heißt $\mathbb{F}_q[t]$-Körper, wenn er zusammen mit einem $\mathbb{F}_q$-Algebra-Homomorphismus $\iota : \mathbb{F}_q[t] \to L$ ausgezeichnet ist.*

Das Primideal $\wp := \mathrm{Kern}(\iota)$ *heißt Charakteristik von* L*. Falls* $\wp = \{0\}$ *ist, nennen wir* L *von generischer Charakteristik, andernfalls von endlicher Charakteristik.*

Wir betrachten nun die Wirkung des q-Frobenius-Endomorphismus τ auf L und erhalten so den Schiefpolynomring der q-Polynome $L\{\tau\}$ mit der Multiplikation $\tau\alpha = \alpha^q\tau$ für $\alpha \in L$. Wie wir in Abschnitt 1.1 gesehen haben, besitzt $L\{\tau\}$ Links- und Rechts-Divisionsalgorithmen, falls L perfekt ist. Siehe dazu [Goss; 1996, Abschnitt 1.6].

Wir führen zunächst den abstrakten Begriff des Drinfeld-Moduls ein.

2.1.2 Definition. *Ein* $\mathbb{F}_q$*-Algebra-Homomorphismus* $\phi : \mathbb{F}_q[t] \to L\{\tau\}, a \mapsto \phi_a$ *über einem* $\mathbb{F}_q[t]$*-Körper* L *heißt Drinfeld-Modul, falls gilt:*

1. $D_\tau \circ \phi = \iota$*, das heißt:* $D_\tau(\phi_a) = \iota(a)\tau^0$ *für* $\phi_a = \sum_{i=0}^{k} \alpha_i \tau^i \in L\{\tau\}$.
2. $\phi(\mathbb{F}_q[t]) \not\subseteq L$*, das heißt: für ein* $a \in \mathbb{F}_q[t]$ *gilt* $\phi_a \neq \iota(a)\tau^0$.

Ein Morphismus zwischen zwei Drinfeld-Moduln ϕ *und* ψ *ist ein q-Polynom* $P \in L\{\tau\}$*, so dass* $P\phi_a = \psi_a P$ *für alle* $a \in A$ *gilt. Im Fall* $P \neq 0$ *wird dies Isogenie genannt.*
Der Rang eines Drinfeld-Moduls ist durch die eindeutige Zahl $r \in \mathbb{N}$ *definiert, für die* $\deg_\tau(\phi_a) = r\deg(a)$ *für alle* $a \in \mathbb{F}_q[t]$ *gilt; siehe dazu [Goss; 1996, Definition 4.5.4].*

Wir sehen also, dass ein Drinfeld-Modul von folgender Gestalt ist:

2.1.3 Bemerkung. *Sei* ϕ *ein Drinfeld-Modul vom Rang* r*, dann gibt es* $g_1, \ldots, g_r \in L$ *mit* $g_r \neq 0$*, so dass für* $t \in \mathbb{F}_q[t]$*:* $\phi_t = \iota(t)\tau^0 + g_1\tau + \ldots + g_r\tau^r \in L\{\tau\}$.
Umgekehrt ist so zu gegebenen $g_1, \ldots, g_r \in L$ *mit* $g_r \neq 0$ *ein Drinfeld-Modul definiert.*

Die folgende "geometrische Betrachtungsweise" ist später hinsichtlich der Verallgemeinerung von Drinfeld-Moduln zu t-Moduln relevant.

2.1.4 Bemerkung. *Nach Bemerkung 1.1.18 ist ersichtlich, dass sich ein Drinfeld-Modul als das additive Gruppenschema* $\mathbb{G}_{a,L}$ *zusammen mit einem* $\mathbb{F}_q$*-linearen Endomorphismus* $t \in L\{\tau\} = \mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a,L})$ *verstehen lässt, so dass* $D_\tau(t(\tau)) = \iota(t)\tau^0$ *und* $t \neq \iota(t)\tau^0$ *gilt.*

Wir werden nun zeigen, dass wir einem Drinfeld-Modul ein Gitter in C_∞ zuordnen können und umgekehrt einem Drinfeld-Modul ein Gitter. Von nun an sei L stets ein vollständiger Körper mit $K_\infty \subseteq L \subseteq C_\infty$ und $\iota : \mathbb{F}_q[t] \to L$ eine Einbettung. Damit ist L etwa eine endliche Erweiterung von K_∞ (oder $L = C_\infty$).

2.1.5 Definition. *Ein $\mathbb{F}_q[t]$-Untermodul $\Lambda \subset C_\infty$ heißt L-Gitter, falls gilt:*

1. *Λ ist ein endlich erzeugter $\mathbb{F}_q[t]$-Modul.*
2. *Λ ist diskret in der Topologie von C_∞, das heißt, eine beschränkte Umgebung in C_∞ enthält nur endliche viele Elemente aus Λ.*
3. *Sei L^{sep} der separable Abschluss von L, dann gilt $\Lambda \subseteq L^{\text{sep}}$ und Λ ist stabil unter der Wirkung von $\mathrm{Gal}(L^{\text{sep}}/L)$.*

Ein Morphismus zwischen zwei L-Gittern Λ und Λ' gleichen Ranges ist ein Element $c \in L$, für das $c\Lambda \subseteq \Lambda'$ gilt. Im Fall $c \neq 0$ wird dies Homothetie genannt.
Der Rang eines L-Gitters sei sein Rang als endlich erzeugter projektiver Untermodul von C_∞; zwischen zwei L-Gittern unterschiedlichen Ranges ist nur $0 \in L$ ein Morphismus.

Zu einem L-Gitter definieren wir wie folgt eine Exponentialfunktion (ähnlich der Weierstraßschen σ-Funktion für Gitter über $\mathbb{C}$ in der Theorie der klassischen elliptischen Kurven; siehe [Washington; 2003, Proposition 9.5]):

$$\exp_\Lambda(x) := x \cdot \prod_{\alpha \in \Lambda \setminus \{0\}} \left(1 - \frac{x}{\alpha}\right).$$

Nach [Goss; 1996, Proposition 4.2.4]) konvergiert e_Λ für alle $x \in C_\infty$ und ist ganz mit einer Potenzreihenentwicklung $\exp_\Lambda = \sum_{i=0}^\infty e_i \tau^i$, deren Koeffizienten e_i in L liegen. Weiter nach [Goss; 1996, Proposition 4.2.5]) ist $\exp_\Lambda : C_\infty \to C_\infty$ eine $\mathbb{F}_q$-lineare Abbildung mit Kern Λ. Folglich ist $\exp_\Lambda$ ein Isomorphismus abelscher Gruppen:

$$C_\infty/\Lambda \cong C_\infty.$$

Mit den Eigenschaften ganzer $\mathbb{F}_q$-linearer Funktionen lässt sich dann zeigen, dass die folgende Identität erfüllt ist; siehe [Goss; 1996, Theorem 4.3.1]:

$$\exp_\Lambda(ax) = a \exp_\Lambda(x) \cdot \prod_{\alpha \in (a^{-1}\Lambda/\Lambda), \alpha \neq 0} (1 - \exp_\Lambda(x)/\exp_\Lambda(\alpha)).$$

Aus dem Beweis dieser Aussage wird klar, dass $\phi_a := ax \cdot \prod_\alpha (1 - x/\exp_\Lambda(\alpha)) \in L\{\tau\}$ für alle $a \in \mathbb{F}_q$ ist. Mit dieser Notation erhalten wir die Funktionalgleichung

$$\exp_\Lambda(ax) = \phi_a(\exp_\Lambda(x)).$$

Entsprechend liefert die $\mathbb{F}_q$-lineare Abbildung $a \mapsto \phi_a$ für $a \in \mathbb{F}_q[t]$ einen Drinfeld-Modul ϕ vom gleichen Rang wie Λ; wir nennen daher ϕ zu Λ assoziiert. Die Wirkung von $a \in A$ durch ϕ_a können wir in dem folgenden kommutativen Diagramm wie in [Goss; 1996, Bemerkung 4.3.6] zusammenfassen:

$$\begin{tikzcd} C_\infty/\Lambda \arrow[r, "a"] \arrow[d, "\exp_\Lambda"', "\cong"] & C_\infty/\Lambda \arrow[d, "\exp_\Lambda"', "\cong"] \\ C_\infty \arrow[r, "\phi_a"] & C_\infty \end{tikzcd}$$

Umgekehrt lässt sich einem Drinfeld-Modul auch ein L-Gitter zuordnen. Es sei nun ein Drinfeld-Modul $\phi_a = \sum_{i=0}^r a_i\tau^i$ vom Rang r über einem vollständigen Körper L gegeben. Aus dem Ansatz $\exp(x) = \sum_{i=0}^\infty e_i\tau^i(x)$ mit $e_0 = 1$ und $\exp(ax) = \phi_a(\exp(x))$ folgen durch Koeffizientenvergleich für $k > 1$ die folgenden rekursiven Bedingungen:

$$e_k = \frac{1}{a^{q^r} - a} \sum_{i=0}^{k} a_i e_{k-i}^{q^i}.$$

Weiter erhalten wir damit, dass die Reihe $\exp(x)$ eindeutig definiert ist. Also gilt:

$$\lim_{k\to\infty} |e_k|^{1/q^k} = 0.$$

Also konvergiert $\exp(x)$ für alle $x \in L$ und folglich ist $\exp : L \to L$ eine ganze $\mathbb{F}_q$-lineare Funktion. Aus der Funktionalgleichung $\exp(ax) = \phi_t(\exp(x))$ sieht man, dass ihr Kern ein $\mathbb{F}_q[t]$-Modul ist, von dem sich wiederum zeigen lässt, dass er ein L-Gitter vom Rang r in C_∞ ist, zu dem ϕ assoziiert ist.

Wir halten fest, dass es eine eindeutige Zuordnung zwischen L-Gittern und Drinfeld-Moduln gibt. Diese Zuordnung ist zudem verträglich mit den jeweiligen Morphismen.

2.1.6 Satz. *Die Kategorie der Drinfeld-Moduln vom Rang r über einem vollständigen Körper L mit $K_\infty \subseteq L \subseteq C_\infty$ äquivalent zur Kategorie der L-Gitter vom Rang r.*

Beweis. Siehe [Goss; 1996, Theorem 4.6.9]. □

2.2 t-Moduln und t-Motive

Wir führen in diesem Abschnitt mit den (abelschen) t-Moduln eine mehrdimensionale Verallgemeinerung der Drinfeld-Moduln ein, die auf die Arbeit von [Anderson; 1986] zurückgeht. So wie Drinfeld-Moduln im Sinne von Abschnitt 2.1 den elliptischen Kurven der klassischen Theorie entsprechen, lassen sich abelsche t-Moduln über Funktionenkörpern als Analogie zu abelschen Varietäten über $\mathbb{C}^n$ auffassen.

Zu t-Moduln gibt es mit den t-Motiven, die wir ebenfalls vorstellen, ein wichtiges duales Konzept, das für gewisse Betrachtungsweisen große Vorteile bietet. Wir beginnen damit, t-Motive zu Drinfeld-Moduln zu definieren und werden dann daraus Definitionen für allgemeine t-Motive und t-Moduln ableiten.

Im Folgenden sei L ein perfekter $\mathbb{F}_q[t]$-Körper und $\iota : \mathbb{F}_q[t] \mapsto L$ eine Einbettung. Weiter sei mit $\phi : \mathbb{F}_q[t] \mapsto L\{\tau\}$ ein Drinfeld-Modul über L gegeben.

Im Mittelpunkt unserer Betrachtungen steht $L\{\tau\}$, der Ring der q-Polynome über L. Weiter sei $L[t,\tau] := L\{\tau\}[t]$ der Ring mit den folgenden Rechenregeln:

$$t\tau = \tau t, \qquad t\alpha = \alpha t \quad \text{und} \quad \tau\alpha = \alpha^q \tau \quad \text{für } \alpha \in L.$$

Wir machen nun $M := M(\phi) := L\{\tau\}$ zu einem $L[t,\tau]$-Linksmodul durch die Wirkung der beiden folgenden nicht-kommutativen Operationen von $\mathbb{F}_q[t]$ auf M:

1. $\mathbb{F}_q[t]$ operiere auf $L\{\tau\}$ vermöge ι als Skalarmultiplikation, das heißt

$$\iota(a) \cdot m := \iota(a) m(\tau) \in L\{\tau\} \quad \text{für } a \in \mathbb{F}_q[t] \text{ und } m \in L\{\tau\}.$$

2. $\mathbb{F}_q[t]$ operiere auf $L\{\tau\}$ vermöge des Drinfeld-Moduls ϕ, das heißt

$$a \cdot m := m(\tau)\phi_a \in L\{\tau\} \quad \text{für } a \in \mathbb{F}_q[t] \text{ und } m \in L\{\tau\}.$$

Beide Operationen von $\mathbb{F}_q[t]$ auf $L\{\tau\}$ werden also bereits durch die Wirkung von t, einmal "t als Operator" und einmal "t als Skalar", beschrieben. Um dies besser unterscheiden zu können, definieren wir $\theta := \iota(t) \in L$.

2.2.1 Bemerkung.

1. *Es ist* $L\{\tau\} \cong L[\tau] \subset L[t,\tau]$ *nach Bemerkung 1.1.7 und wir können somit* $L[t,\tau]$ *auffassen als* $L[t,\tau] = L\{\tau\}[t] \cong L[\tau][t]$.

2. *Da* L *perfekt ist, besitzt* $L\{\tau\}$ *nach Propositionen 1.1.10 und 1.1.12 sowohl Links- als auch Rechts-Divisionsalgorithmen. Damit ist* $L[t,\tau]$ *nach dem Hilbertschen Basissatz links- und rechts-noethersch.*

Den Zusammenhang zwischen ϕ und $M(\phi)$ erhalten wir, indem wir die wichtigsten Eigenschaften für $M(\phi)$ noch einmal zusammenfassen:

2.2.2 Lemma. *Sei* ϕ *ein Drinfeld-Modul vom Rang* $r > 0$ *über* L *und* $M := M(\phi)$ *das zu* ϕ *assoziierte t-Motiv. Dann gilt:*

1. M *ist als* $L\{\tau\}$*-Modul frei vom Rang* 1.

2. M *wird als* $L[t]$*-Modul frei erzeugt von* $(\tau^0, \tau, \ldots, \tau^{r-1})$.

3. τM *ist ein* $L[t,\tau]$*-Untermodul von* M *und es gilt* $(t-\theta)M/\tau M = \{0\}$.

Beweis. Siehe [Goss; 1996, Lemma 5.4.1]. □

Es ist nun leicht zu zeigen, dass die Umkehrung ebenfalls gilt.

2.2.3 Lemma. *Sei* M *ein* $L[t,\tau]$*-Modul mit den folgenden Eigenschaften:*

1. M *ist als* $L\{\tau\}$*-Modul frei vom Rang* 1.

2. M *wird als* $L[t]$*-Modul ist frei vom Rang* $r > 0$.

3. τM *ist ein* $L[t,\tau]$*-Untermodul von* M *und es gilt* $(t-\theta)M/\tau M = \{0\}$.

Dann existiert einen Drinfeld-Modul ϕ *vom Rang* r *mit* $M \cong M(\phi)$

Beweis. Wir zitieren den Beweis aus [Bangert; 2011, Lemma 1.2.2]. Sei m ein freier Erzeuger von M als $L[\tau]$-Modul, dann lässt sich $t \cdot m$ schreiben als $P(\tau) \cdot m$ für ein $P(\tau) \in L\{\tau\}$. Der Drinfeld-Modul $\phi_t := P(\tau)$ hat dann die gewünschte Eigenschaft. □

Aus dieser Situation lässt sich die folgende Definition allgemeiner t-Motive ableiten, die nicht mehr zu Drinfeld-Moduln assoziiert sein müssen (aber können).

2.2.4 Definition. *Ein t-Motiv M ist ein $L[t,\tau]$-Linksmodul, für den gilt:*

1. *M ist als $L\{\tau\}$-Modul frei und endlich erzeugt.*
2. *Es ist $(t-\theta)^n\,(M/\tau M) = \{0\}$ für fast alle $n \in \mathbb{N}$.*

Ein Morphismus zwischen zwei t-Motiven ist ein $L[t,\tau]$-Linksmodul-Homomorphismus. Falls der $L\{\tau\}$-Rang eines t-Motivs M existiert, definiert dieser die Dimension $\dim(M)$.

Durch die Erweiterung für kleine $n \neq 1$ sind nach [Goss; 1996, Abschnitte 5.5 und 5.7] insbesondere Tensorprodukte von t-Motiven wieder t-Motive, obwohl sich diesen Objekten im Allgemeinen keine Drinfeld-Moduln zuordnen lassen.
Des Weiteren sind die zu Drinfeld-Moduln assoziierten t-Motive ebenfalls t-Motive nach Definition 2.2.4 (mit $n = 1$), da in diesem Fall t als θ auf $M/\tau M$ wirkt.

2.2.5 Bemerkung. *Ein t-Motiv der Dimension d ist natürlich isomorph zu $L\{\tau\}^d$. Damit wirkt $(t-\theta)$ als Element aus $\mathrm{Mat}_{d\times d}(L)\{\tau\}$ auf M. Im Fall $n > 1$ bedeutet $(t-\theta)^n\,(M/\tau M) = \{0\}$ somit, dass $N := D_\tau(t) - \theta \in \mathrm{Mat}_{d\times d}(L)$ nilpotent ist.*

Es sei E eine algebraische Gruppe mit $E \cong \mathbb{G}_{a,L}^d$. Wir können die Endomorphismen $\mathrm{End}_{\mathbb{F}_q}(E)$ nach Proposition 1.1.19 als Elemente in $\mathrm{Mat}_{d\times d}(L)\{\tau\}$ auffassen, wobei wir τ wie in Definition 1.1.14 verstehen.
Mit $\mathrm{Lie}(E)$ bezeichnen wir die Lie-Algebra von E im üblichen Sinn. $\mathrm{Lie}(E)$ ist also der Tangentialraum von $E \cong \mathbb{G}_{a,L}^d$ im Ursprung, damit ist $\mathrm{Lie}(E) \cong L^d$.

Wir werden nun t-Moduln definieren und danach sehen, dass diese ein duales Konzept zu t-Motiven darstellen. t-Moduln können als mehrdimensionale "geometrische Objekte" im Zusammenhang von Bemerkung 2.1.4 verstanden werden.

2.2.6 Definition. *Ein t-Modul E über L ist eine algebraische Gruppe mit $E \cong \mathbb{G}_{a,L}^d$, die mit einem $\mathbb{F}_q$-linearen Endomorphismus $t \in \mathrm{End}_{\mathbb{F}_q}(E)$ versehen ist, so dass gilt:*

$$(t-\theta)^n\,\mathrm{Lie}(E) = 0 \text{ für fast alle } n \in \mathbb{N}.$$

Ein Morphismus zwischen zwei t-Moduln ist ein Homomorphismus der unterliegenden algebraischen Gruppen, der mit der Wirkung von t kommutiert.
Die Dimension $\dim(E)$ *eines t-Moduls E ist durch die Zahl d definiert.*

Wir stellen bereits an dieser Stelle für Dimension $d = 1$ fest, dass diese Definition der t-Moduln eine Verallgemeinerung der Drinfeld-Moduln darstellt.

2.2.7 Bemerkung.

1. *Drinfeld-Moduln zum $\mathbb{F}_q[t]$ sind t-Moduln der Dimension $d = 1$.*
2. *$\mathbb{G}_{a,L}^d$ mit der üblichen Skalarmultiplikation $t(x) = \theta x$ sind t-Moduln. Für $d = 1$ sind diese aber keine Drinfeld-Moduln, da die Nicht-Trivialität der Eigenschaft 2 aus Definition 2.1.2 nicht erfüllt ist.*

Wir werden nun die Dualität zwischen t-Moduln und t-Motiven erklären. Wir bezeichnen im Folgenden mit $\mathrm{Hom}_{\mathbb{F}_q,L}(\cdot,\cdot)$ die Gruppe der $\mathbb{F}_q$-linearen Homomorphismen algebraischer Gruppen über L.

Es sei ein t-Modul E der Dimension d gegeben. Wir definieren dann:

$$M := M(E) := \mathrm{Hom}_{\mathbb{F}_q,L}(E, \mathbb{G}_{a,L}) \cong L\{\tau\}^d,$$

M erhält nun die Struktur eines $L[t,\tau]$-Moduls, indem wir die Verknüpfungen wie folgt als Kompositionen in $L\{\tau\}^d$ definieren:

$$\begin{array}{rcll} \alpha \cdot m & := & \alpha m(\tau) \in L\{\tau\}^d & \text{für } \alpha \in L \text{ und } m \in M, \\ \tau \cdot m & := & \tau m(\tau) \in L\{\tau\}^d & \text{für } m \in M, \\ t \cdot m & := & m(\tau) t \in L\{\tau\}^d & \text{für } m \in M. \end{array}$$

Die Projektion auf die d Koordinaten von M liefert eine $L\{\tau\}$-Basis $(\beta_1, \ldots, \beta_d)$, das heißt, M hat die Dimension d und $m \in M$ lässt sich in $L\{\tau\}^d$ darstellen als Vektor $m(\tau) = (m_1(\tau), \ldots, m_d(\tau))$. Dabei wird die Abbildung $m : \mathbb{G}_{a,L}^d \cong L^d \to \mathbb{G}_{a,L} \cong L$ gerade durch das Einsetzen $x \mapsto m(\tau(x))$ in $m = \sum_{i=1}^d m_i(\tau)\beta_i$ für $x \in L^d$ repräsentiert.

2.2.8 Bemerkung. *Nach Wahl von Koordinaten für $E \cong \mathbb{G}_{a,L}^d$ und $\mathbb{G}_{a,L}$ erhalten wir:*

$$m = \sum_{i=1}^d m_i(\tau)\beta_i = (m_1(\tau), \ldots, m_d(\tau)) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix} = m(\tau) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix} : L^d \to L,$$

t wirkt von rechts auf $m(\tau) \in L\{\tau\}^d$, damit folgt:

$$t \cdot m \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix} = m(\tau) t \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix} = m(\tau) Q_t(\tau) \begin{pmatrix} \beta_1 \\ \vdots \\ \beta_d \end{pmatrix}.$$

Wir sehen also, dass die Darstellung von t als Element $Q_t(\tau) \in \mathrm{Mat}_{d\times d}(L)\{\tau\}$ verträglich mit den obigen Definitionen der Operationen ist.

Folglich ist M ein t-Motiv und $E \mapsto M(E)$ ein kontravarianter Funktor. Weiter gilt an dieser Stelle (siehe [Goss; 1996, Lemma 5.4.7]), dass die Gruppe $\mathrm{Lie}(E)$ durch die Abbildung $x \mapsto (f \mapsto \partial_x f)$ isomorph ist zu

$$\mathrm{Hom}_L(\mathrm{Hom}_{\mathbb{F}_q,L}(E, \mathbb{G}_{a,L})/\tau\,\mathrm{Hom}_{\mathbb{F}_q,L}(E, \mathbb{G}_{a,L}), L) = \mathrm{Hom}_L(M/\tau M, L) \cong L^d.$$

Wir betrachten schließlich die folgende strukturelle Aussage über die Beziehung zwischen $L[t]$-Rang und $L\{\tau\}$-Rang von M.

2.2.9 Lemma. *Sei M ein $L[t,\tau]$-Linksmodul, der sowohl als $L[t]$-Modul als auch als $L\{\tau\}$-Modul endlich erzeugt ist. Dann ist M genau dann frei von endlichem Rang über $L[t]$, wenn M frei von endlichem Rang über $L\{\tau\}$ ist.*

Beweis. Siehe [Goss; 1996, Lemma 5.4.10]. □

2.2.10 Definition. *Ein t-Modul M heißt abelsch, wenn M über $L[t]$ endlich erzeugt ist; und E heißt abelscher t-Modul genau dann, wenn $M(E)$ abelsch ist.*

Wir erhalten die folgende kategorientheoretische Aussage.

2.2.11 Satz. *Über einem perfekten Körper L liefert der Funktor $E \mapsto M(E)$ eine Anti-Äquivalenz zwischen der Kategorie der abelschen t-Moduln und der Kategorie der abelschen t-Motive.*

Beweis. Siehe [Goss; 1996, Theorem 5.4.11]. □

Es bleibt noch die Frage, wie wir den Rang eines t-Moduls E und des zugehörigen t-Motivs $M := M(E)$ so definieren, dass dieser mit dem bekannten Rang der Drinfeld-Moduln übereinstimmt.

Nach Lemma 2.2.9 ist M genau dann abelsch, wenn M als $L[t]$-Modul frei von endlichem Rang ist. In diesem Fall definieren wir den Rang von E und M durch

$$\mathrm{Rang}(E) = \mathrm{Rang}(M(E)) := \mathrm{Rang}_{L[t]}(M).$$

Wir können nun eine allgemeine Charakterisierung der abelschen t-Moduln angeben (wobei die abelschen t-Modul der Dimension $d = 1$ genau die Drinfeld-Moduln sind).

2.2.12 Bemerkung. *Sei $E \cong \mathbb{G}_{a,L}^d$ ein abelscher t-Modul der Dimension d, dann gibt es eindeutig bestimmte Matrizen $G_0, G_1, \ldots, G_k \in \mathrm{Mat}_{d\times d}(L)$, so dass die Wirkung von t gegeben ist durch:*

$$t = G_0\tau^0 + G_1\tau + \ldots + G_k\tau^k \in \mathrm{Mat}_{d\times d}(L)\{\tau\},$$

wobei $N := G_0 - \theta$ nach Bemerkung 2.2.5 nilpotent ist.

Umgekehrt erhalten wir zu gegebenen Matrizen $G_0, G_1, \ldots, G_k \in \mathrm{Mat}_{d\times d}(L)$, wobei $G_0 - \theta$ nilpotent ist, wiederum einen t-Modul der Dimension d durch die Operation:

$$t := G_0\tau^0 + G_1\tau^1 + \ldots + G_k\tau^k \in \mathrm{Mat}_{d\times d}(L)\{\tau\}.$$

(In der Regel werden wir später die Identität τ^0 bei der Notation von t in dieser Darstellung weglassen.)

Die Ähnlichkeit zu der ursprünglichen Definition 2.1.2 der Drinfeld-Moduln wird nun deutlich, wenn wir $\Phi_t := t$ für ein geeignetes $\Phi : \mathbb{F}_q[t] \to L\{\tau\}^d,\ a \mapsto \Phi_a$ betrachten, wobei in diesem Fall $D_\tau(\Phi_a) = (\iota(a) + N)\tau^0$ für eine nilpotente Matrix N gilt.

2.3 Uniformisierbarkeit und der Satz von Anderson

Wir erklären in diesem Abschnitt die Uniformisierbarkeit abelscher t-Moduln (angelehnt an [Goss; 1996, Abschnitt 5.9]). Dabei verallgemeinert der Begriff Uniformisierbarkeit den Sachverhalt aus Satz 2.1.6, dass sich Drinfeld-Moduln durch ein Gitter und dessen Exponentialfunktion darstellen lassen. Wir sehen dann, dass abelsche t-Moduln in diesem Sinne uniformisierbar sein können, aber nicht müssen.

Zunächst werden wir die Exponentialfunktion zu einem t-Modul definieren und feststellen, dass ihre Surjektivität hinreichend für die Uniformisierbarkeit des t-Moduls ist. Anschließend werden wir einen Satz von Anderson [Anderson; 1986, Theorem 2.4] vorstellen, der zeigt, dass Uniformisierbarkeit eines t-Moduls und die Surjektivität der zugehörigen Exponentialfunktion äquivalente Bedingungen sind, die durch eine weitere Bedingung an das zugehörige t-Motiv verbunden werden.

Bei der Einführung der t-Moduln und t-Motive in Abschnitt 2.2 hat die Unterscheidung von "t als Skalar" und "t als Operator" eine wichtige Rolle gespielt. Wir werden im Folgenden analytische Objekte im Funktionenkörper der Skalare betrachten. Wir nehmen daher zunächst an, dass θ eine Unbestimmte ist.
Von nun an schreiben wir $K_\infty := \mathbb{F}_q((\frac{1}{\theta}))$ für die Vervollständigung von $\mathbb{F}_q(\theta) = \mathrm{Quot}(\mathbb{F}_q[\theta])$ bezüglich der diskreten Bewertung v_∞ wie in Beispiel 1.2.2 mit $v_\infty(\theta) = 1$.
Es sei weiter $\overline{K}_\infty = \overline{\mathbb{F}_q((\frac{1}{\theta}))}$ ein fest gewählter algebraischer Abschluss von K_∞ zusammen mit der kanonisch fortgesetzten Bewertung v_∞ auf $\overline{K}_\infty$. Durch die Wahl der natürlichen Einbettung ι mit $\iota(t) = \theta$ werden K_∞ und $\overline{K}_\infty$ zu $\mathbb{F}_q[t]$-Körpern.

Mit $|\cdot|_{v_\infty}$ bezeichnen wir den fortgesetzten normierten Betrag zu v_∞ auf $\overline{K}_\infty$, das heißt $|\theta|_{v_\infty} = q$. Ferner sei $||\cdot||_\infty$ die zugehörige Supremumsnorm auf $\mathrm{Mat}_{m\times n}(\overline{K}_\infty)$.

2.3.1 Definition. *Eine Funktion $f : \overline{K}_\infty^m \to \overline{K}_\infty^n$ heißt ganz $\mathbb{F}_q$-linear, falls es Matrizen $A_i \in \mathrm{Mat}_{m\times n}(\overline{K}_\infty)$ gibt, so dass gilt:*

1. $f(\tau) = \sum_{i=0}^\infty A_i\tau^i \in \mathrm{Mat}_{m\times n}(\overline{K}_\infty)\{\tau\}$,
2. $\lim\limits_{i\to\infty} ||A_i||_\infty^{1/q^i} = 0$,
3. *es ist $\{A_i\} \subset \mathrm{Mat}_{m\times n}(L)$ für eine endliche Erweiterung $L \subset \overline{K}_\infty$ von K_∞.*

Diese Bedingungen stellen nach Bemerkung 1.2.6 sicher, dass für eine ganz $\mathbb{F}_q$-lineare Funktion $f : \overline{K}_\infty^m \to \overline{K}_\infty^n$ die Funktionswerte $f(x) \in \overline{K}_\infty^n$ für alle $x \in \overline{K}_\infty^m$ konvergieren.

Wir können nun die Exponentialfunktion von abelschen t-Moduln als Verallgemeinerung der Exponentialfunktion von Drinfeld-Moduln einführen.

2.3.2 Definition. *Es sei E ein abelscher t-Modul über $\overline{K}_\infty$. Ein $\mathbb{F}_q$-linearer Homomorphismus* $\exp : \mathrm{Lie}(E) \to E$ *heißt Exponentialfunktion, falls gilt:*

1. $\exp$ *erfüllt die Funktionalgleichung* $\exp(D_\tau(t)\, x)) = t \exp(x)$
2. $\exp : \overline{K}_\infty^d \to \overline{K}_\infty^d$ *ist eine ganz $\mathbb{F}_q$-lineare Funktion, deren Potenzreihenentwicklung mit der $d \times d$-Einheitsmatrix I beginnt.*

Im Folgenden sei E ein abelscher t-Modul mit $\Phi : \mathbb{F}_q[t] \to \overline{K}_\infty\{\tau\}^d,\ a \mapsto \Phi_a$ und exp eine Exponentialfunktion. Die erste Bedingung aus Definition 2.3.2 stellt die Verträglichkeit von exp mit Φ sicher, denn durch die Wirkung von t gilt für alle $a \in \mathbb{F}_q[t]$:

$$\exp(D_\tau(\Phi_a)\, z) = \Phi_a(\exp(z)).$$

Die zweite Bedingung ist eine Normierung, wodurch die Eindeutigkeit von exp erreicht wird. Wir schreiben von nun an $\exp_E := \exp$ und erhalten:

2.3.3 Satz. *Sei E ein abelscher t-Modul, dann existiert* $\exp_E$ *und ist eindeutig.*

Beweis. Siehe [Goss; 1996, Theorem 5.9.2 und Theorem 5.9.6]. □

Weiter sehen wir, dass $\mathrm{Kern}(\exp_E)$ durch die Wirkung von t mittels der Funktionalgleichung ein $\mathbb{F}_q[t]$-Modul ist. Das folgende Resultat erklärt die Struktur von $\mathrm{Kern}(\exp_E)$.

2.3.4 Proposition. $\mathrm{Kern}(\exp_E)$ *ist diskret in* $\mathrm{Lie}(E)$ *und es gilt:*

$$\mathrm{Rang}_{\mathbb{F}_q[t]}(\mathrm{Kern}(\exp_E)) \leq \mathrm{Rang}(E).$$

Beweis. Siehe [Goss; 1996, Lemma 5.9.12]. □

Damit ist $\mathrm{Kern}(\exp_E)$ ein $\overline{K}_\infty$-Gitter und falls $\exp_E$ surjektiv ist, induziert dies über $\overline{K}_\infty$ den Isomorphismus

$$\mathrm{Lie}(E)/\,\mathrm{Kern}(\exp_E) \cong E.$$

In diesem Fall folgt dann weiter $\mathrm{Rang}_{\mathbb{F}_q}(\mathrm{Kern}(\exp_E)) = \mathrm{Rang}(E)$.

Entsprechend definieren wir:

2.3.5 Definition. *Ein abelscher t-Modul E heißt uniformisierbar, falls $\exp_E$ surjektiv ist.*

Wir haben in Abschnitt 2.1 gesehen, dass Exponentialfunktionen von Drinfeld-Moduln stets surjektiv sind. Für abelsche t-Moduln gilt dies im Allgemeinen nicht mehr. Das klassische Beispiel, um dies zu zeigen, stammt von Anderson und Coleman. Wir geben es hier in der Form von [Bangert; 2011, Beispiel 4.6.1] an.

2.3.6 Beispiel. *Sei $l \in \overline{K}_\infty$ mit $|l|_{v_\infty} < 1$ und $l + l^{-1} = \theta$ gewählt und weiter sei der t-Modul $E = \mathbb{G}^2_{a,\overline{K}_\infty}$ gegeben durch die Wirkung*

$$t = \tau^2 + \begin{pmatrix} 0 & l^{\frac{1}{q-1}} - l^{\frac{q^2}{q-1}} \\ l^{-\frac{q^2}{q-1}} - l^{-\frac{1}{q-1}} & 0 \end{pmatrix} \tau + \theta.$$

E ist ein abelscher t-Modul der Dimension 2 und von Rang 4, dessen Exponentialfunktion $\exp_E$ injektiv ist und damit nicht surjektiv sein kann (wie in [Goss; 1996, Beispiel 5.9.9.] gezeigt wird).

Im Folgenden werden wir sehen, dass bereits die Erfüllung der Bedingung

$$\mathrm{Rang}_{\mathbb{F}_q}(\mathrm{Kern}(\exp_E)) = \mathrm{Rang}(E)$$

äquivalent zur Surjektivität von $\exp_E$ ist. Dies ist ein Resultat, das auf die Arbeit von Anderson zurückgeht. Der Beweis ist sehr aufwendig und wir müssen dazu einige zusätzliche Begriffe einführen.

2.3.7 Definition. *$\overline{K}_\infty\langle\langle t\rangle\rangle$ sei der Ring der Potenzreihen $\sum_{i=0}^{\infty} a_i t^i$, für die gilt:*

1. *$\lim\limits_{i\to\infty} |a_i| = 0$,*
2. *es ist $\{a_i\} \subset L$ für eine endliche Erweiterung $L \subset \overline{K}_\infty$ von K_∞.*

Wir bemerken, dass diese Bedingungen sicherstellen, dass Potenzreihen aus $\overline{K}_\infty\langle\langle t\rangle\rangle$ auf der abgeschlossenen Einheitsscheibe in $\overline{K}_\infty\langle\langle t\rangle\rangle$ konvergieren.

Es sei E ein abelscher t-Modul über $\overline{K}_\infty$ und $M := M(E)$ sei das zugehörige t-Motiv. Wir definieren ausgehend von M und $\overline{K}_\infty\langle\langle t\rangle\rangle$ den $\overline{K}_\infty[t,\tau]$-Modul

$$M\langle\langle t\rangle\rangle := M \otimes_{\overline{K}_\infty[t]} \overline{K}_\infty\langle\langle t\rangle\rangle,$$

dabei ist die Wirkung von $\overline{K}_\infty[t]$ auf $M\langle\langle t\rangle\rangle$ auf natürliche Weise gegeben. Weiter lassen wir τ diagonal auf $M\langle\langle t\rangle\rangle$ operieren, das heißt:

$$\tau \cdot \left(m \otimes \sum_{i=0}^{\infty} a_i t^i \right) := \tau m \otimes \sum_{i=0}^{\infty} a_i^q t^i \quad \text{für } m \otimes \sum_{i=0}^{\infty} a_i t^i \in M\langle\langle t\rangle\rangle.$$

Im Weiteren spielt der $\mathbb{F}_q[t]$-Modul $M\langle\langle t\rangle\rangle^\tau$ der τ invarianten Elemente von $M\langle\langle t\rangle\rangle$ eine wesentliche Rolle. Wir werden zur besseren Unterscheidbarkeit von nun an konsequent die "Elemente mit Reihen" stets durch Unterstriche kennzeichnen. Wir schreiben also

2.3.8 Definition. $M\langle\langle t\rangle\rangle^\tau := \{\underline{m} \in M\langle\langle t\rangle\rangle \mid \tau(\underline{m}) = \underline{m}\}$.

Die folgende Definition ist grundlegend, da ihre Erfüllung eine weitere äquivalente Bedingung zur Surjektivität von $\exp_E$ darstellt. Sie erlaubt es uns, die Betrachtung auf das t-Motiv M zu richten, was wir in Kapitel 4 häufig nutzen werden.

2.3.9 Definition. *Sei E ein abelscher t-Modul und $M := M(E)$ das zugehörige t-Motiv, dann heißt M rigide analytisch trivial, falls der natürliche Homomorphismus*

$$\pi : \quad M\langle\langle t\rangle\rangle^\tau \otimes_{\mathbb{F}_q[t]} \overline{K}_\infty\langle\langle t\rangle\rangle \ \to M\langle\langle t\rangle\rangle, \quad \underline{m} \otimes \sum_{i=0}^{\infty} a_i t^i \ \mapsto \underline{m} \cdot \sum_{i=0}^{\infty} a_i t^i$$

ein Isomorphismus ist.

Es ist nun eine direkte Folgerung aus dieser Definition, dass für zwei rigide analytische t-Motive M_1 und M_2 das Tensorprodukt $M_1 \otimes M_2$ (mit der diagonalen Operation $\tau(m_1 \otimes m_2) := \tau(m_1) \otimes \tau(m_2)$) wieder rigide analytisch trivial ist.

Die Rolle von $M\langle\langle t\rangle\rangle^\tau$ in $M\langle\langle t\rangle\rangle$ entspricht in dieser Situation der von $\mathrm{Kern}(\exp_E)$ in $\mathrm{Lie}(E)$. Dies wird durch die folgenden Resultate aus [Böckle und Hartl; 2007] ersichtlich, die wir hier zum besseren Verständnis zitieren.

2.3.10 Lemma. *π ist injektiv und $M\langle\langle t\rangle\rangle^{\tau}$ ist endlich erzeugt, dabei gilt:*

$$\mathrm{Rang}_{\mathbb{F}_q[t]}(M\langle\langle t\rangle\rangle^{\tau}) \leq \mathrm{Rang}(E).$$

Beweis. Siehe [Böckle und Hartl; 2007, Lemma 4.2 b)]. □

Falls M rigide analytisch trivial ist, dann zeigt Definition 2.3.9 direkt, dass die Ränge von Definitions- und Bildbereich von π als $\mathbb{F}_q[t]$-Moduln gleich (und damit gleich $\mathrm{Rang}(M) = \mathrm{Rang}(E)$) sein müssen. Die Umkehrung, und damit der folgende Satz, ist dagegen schwieriger zu beweisen. Dabei ist nachzuweisen, dass das Bild von π die richtige Struktur als $L\langle\langle t\rangle\rangle\{\tau\}$-Untermodul von $M\langle\langle t\rangle\rangle$ hat. Für Details dazu verweisen wir auf [Bangert; 2011, Satz 4.1.2].

2.3.11 Lemma. *M ist genau dann rigide analytisch trivial, wenn gilt:*

$$\mathrm{Rang}_{\mathbb{F}_q[t]}(M\langle\langle t\rangle\rangle^{\tau}) = \mathrm{Rang}(E).$$

In diesem Fall ist π surjektiv.

Beweis. Siehe [Böckle und Hartl; 2007, Lemma 4.2 c)]. □

Der Satz von Anderson [Anderson; 1986, Theorem 2.4] zeigt nun den wesentlichen Zusammenhang der einzelnen Bedingungen für die Uniformisierbarkeit.

2.3.12 Satz. *Sei E ein abelscher t-Modul und $M := M(E)$ das zugehörige t-Motiv, dann sind die folgenden Aussagen äquivalent:*

1. $\mathrm{Rang}_{\mathbb{F}_q[t]}(\mathrm{Kern}(\exp_E)) = \mathrm{Rang}(E)$.
2. $\exp_E$ *ist surjektiv.*
3. *$M(E)$ ist rigide analytisch trivial.*

Beweis. Den Schritt von (2) $\Rightarrow$ (1) haben wir bereits gesehen. Die anderen werden in den Schritten (3) $\Rightarrow$ (2) und (1) $\Rightarrow$ (3) gezeigt Richtungen und sind recht aufwendig. Die Surjektivität von $\exp_E$ wird dabei durch homologische Aussagen beschrieben. Siehe dazu [Goss; 1996, Theorem 5.9.14]. □

3 Eine spezielle Familie von t-Moduln

Genaue Kriterien für die Uniformisierbarkeit abelscher t-Modul angeben zu können, ist ein offenes Problem. Das klassische Beispiel eines nicht-uniformisierbaren t-Moduls von Anderson und Coleman (siehe Beispiel 2.3.6) wird in der Arbeit [Bangert; 2011] zu einer ganzen Familie von t-Moduln in der Dimension $d = 2$ erweitert, so dass in dieser auch uniformisierbare t-Moduln enthalten sind. Damit ist diese Beispielfamilie ein guter Ausgangspunkt für die Suche nach notwendigen und hinreichenden Bedingungen für die Uniformisierbarkeit von t-Moduln.

Im Folgenden beschreiben wir eine Verallgemeinerung dieser Familie von t-Moduln in beliebiger Dimension $d \geq 2$. Wir werden aus der Frage der Uniformisierbarkeit dieser t-Moduln die Untersuchung $\mathbb{F}_q$-linearer Polynomgleichungen motivieren.

3.1 Kriterien für die Uniformisierbarkeit spezieller t-Moduln

Nach Satz 2.3.11 ist ein abelscher t-Modul E genau dann uniformisierbar, wenn der $\mathbb{F}_q[t]$-Modul $M\langle\langle t\rangle\rangle^{\tau}$ vollen Rang hat, das heißt, wenn $\mathrm{Rang}_{\mathbb{F}_q[t]}(M\langle\langle t\rangle\rangle^{\tau}) = \mathrm{Rang}(E)$ gilt. Wir wollen in diesem Abschnitt konkretere Kriterien herleiten, anhand derer sich entscheiden lässt, ob ein t-Modul uniformisierbar ist.

Es sei $K_\infty := \mathbb{F}_q((\frac{1}{\theta}))$ und damit $\overline{K}_\infty = \overline{\mathbb{F}_q((\frac{1}{\theta}))}$. Im Weiteren sei E ein t-Modul der Dimension $d \geq 1$ gegeben durch den $\mathbb{F}_q$-linearen Endomorphismus

$$t = \tau^2 + A\tau + \theta\tau^0 \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)\{\tau\}, \tag{3.1}$$

wobei $A = (a_{i,j})_{1\leq,i,j\leq d} \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)$ mit Einträgen $a_{i,j} \in \overline{K}_\infty$ beliebig ist.

Weiter sei $M := M(E)$ das t-Motiv zu E. Wir betrachten im Folgenden den Modul

$$M[[t]] := M \otimes_{\overline{K}_\infty[t]} \overline{K}_\infty[[t]],$$

also die formalen Potenzreihen in t mit Koeffizienten in M, und ferner

$$M[[t]]^\tau := \{\underline{m} \in M[[t]] \mid \tau(\underline{m}) = \underline{m}\},$$

den Untermodul der unter τ invarianten Elemente aus $M[[t]]$. Wir werden nun analog zu [Bangert; 2011, Kapitel 4.1] Kriterien dafür bestimmen, wann Elemente aus $M[[t]]^\tau$ in $M\langle\langle t\rangle\rangle^\tau$ liegen (siehe Definition 2.3.8).

Wir untersuchen zunächst die Struktur von M. Wegen $\dim(M) = \dim(E) = d$ ist $\mathrm{Rang}_{\overline{K}_\infty\{\tau\}}(M) = d$. Demnach ist M als $\overline{K}_\infty\{\tau\}$-Modul isomorph zu $\overline{K}_\infty\{\tau\}^d$ und jedes Element lässt sich als Vektor $m(\tau) = (m_1(\tau), \dots, m_d(\tau))$ schreiben.

Die Operation von t auf ein Element $m(\tau) \in M$ lässt sich durch die Multiplikation mit der Matrix $Q_t(\tau) = \tau^2 + A\tau + \theta\tau^0$ von rechts darstellen (vergleiche Bemerkung 2.2.8). Wir betrachten nun die Wirkung von t via $Q_t(\tau)$ auf ein Element $(u_1, \dots, u_d)\tau^k$ mit $k \geq 0$ und $u_1, \dots, u_d \in \overline{K}_\infty[t]$ und stellen fest:

$$\begin{aligned} t \cdot (u_1, \dots, u_d)\tau^k &= (u_1, \dots, u_d)\tau^k\,(\tau^2 + A\tau + \theta\tau^0) \\ &= (u_1, \dots, u_d)\tau^{k+2} + (u_1, \dots, u_d)A\tau^{k+1} + \theta\tau^0(u_1, \dots, u_d) \\ \Longleftrightarrow (u_1, \dots, u_d)\tau^{k+2} &= -(u_1, \dots, u_d)A\tau^{k+1} + (t - \theta\tau^0) \cdot (u_1, \dots, u_d)\tau^k. \end{aligned}$$

Durch wiederholte Anwendung dieser Relation können wir den q-Grad von jedem $m(\tau) = (m_1(\tau), \dots, m_d(\tau)^d) \in \overline{K}_\infty\{\tau\}^d$ auf 1 reduzieren, das heißt, $m \in M$ lässt sich schreiben in der Form

$$\begin{aligned} m &= (u_1 + v_1\tau, \dots, u_d + v_d\tau) \\ &= (u_1, \dots, u_d) + (v_1, \dots, v_d)\tau \text{ mit } u_1, \dots, u_d, v_1, \dots, v_d \in \overline{K}_\infty[t]. \end{aligned}$$

Es folgt $\mathrm{Rang}(M) = 2d$, also gilt für M als $\overline{K}_\infty[t]$-Modul:

$$M \;\cong\; \overline{K}_\infty[t]^d + \overline{K}_\infty[t]^d\,\tau \;\cong\; \overline{K}_\infty[t]^{2d}.$$

Die Struktur von M als $\overline{K}_\infty[t]$-Modul können wir auf den $\overline{K}_\infty[[t]]$-Modul $M[[t]]$ auf natürliche Weise fortsetzen, denn wir sehen mit den obigen Argumenten, dass gilt:

$$M[[t]] \;\cong\; \overline{K}_\infty[[t]]^d + \overline{K}_\infty[[t]]^d\,\tau \cong\; \overline{K}_\infty[[t]]^{2d}.$$

Ein Element $\underline{m} \in M[[t]]$ ist also gegeben durch

$$\underline{m} = (\underline{u_1}, \ldots, \underline{u_d}) + (\underline{v_1}, \ldots, \underline{v_d})\tau \text{ mit } \underline{u_1}, \ldots, \underline{u_d}, \underline{v_1}, \ldots, \underline{v_d} \in \overline{K}_\infty[[t]]$$

die Wirkung von τ auf $\underline{m} \in \overline{K}_\infty[[t]]^d + \overline{K}_\infty[[t]]^d\,\tau$ ergibt sich nun wie folgt:

$$\begin{aligned}
\tau \cdot \underline{m} &= \tau \cdot \big(\, (\underline{u_1}, \ldots, \underline{u_d}) + (\underline{v_1}, \ldots, \underline{v_d})\tau\,\big)\\
&= (\underline{u_1}^{(1)}, \ldots, \underline{u_d}^{(1)})\tau + (\underline{v_1}^{(1)}, \ldots, \underline{v_d}^{(1)})\tau^2\\
&= (\underline{u_1}^{(1)}, \ldots, \underline{u_d}^{(1)})\tau + (\underline{v_1}^{(1)}, \ldots, \underline{v_d}^{(1)})\,(t - \theta\tau^0 - A\tau)\\
&= (\underline{v_1}^{(1)}, \ldots, \underline{v_d}^{(1)})\,(t - \theta\tau^0) + \Big(\,(\underline{u_1}^{(1)}, \ldots, \underline{u_d}^{(1)}) - (\underline{v_1}^{(1)}, \ldots, \underline{v_d}^{(1)})A\,\Big)\;\tau.
\end{aligned}$$

Für $m = (\underline{u}, \underline{v}) \in \overline{K}_\infty[[t]]^{2d}$ als $2d$-Zeilenvektor mit $\underline{u}, \underline{v} \in \overline{K}_\infty[[t]]^d$ gilt damit

$$\tau \cdot \underline{m} = \tau(\underline{u}, \underline{v}) = (\underline{u}^{(1)}, \underline{v}^{(1)}) \begin{pmatrix} 0 & I_d \\ t-\theta & -A \end{pmatrix}. \tag{3.2}$$

Wir transponieren diese Gleichung, um die Matrix von links zu multiplizieren:

$$\tau \begin{pmatrix} \underline{u}^T \\ \underline{v}^T \end{pmatrix} = \begin{pmatrix} 0 & t-\theta \\ I_d & -A^T \end{pmatrix} \begin{pmatrix} (\underline{u}^T)^{(1)} \\ (\underline{v}^T)^{(1)} \end{pmatrix}. \tag{3.3}$$

Damit können wir schließlich $M[[t]]^\tau$ in $M[[t]] \cong \overline{K}_\infty[[t]]^{2d}$ bestimmen.

3.1.1 Lemma. *Es gibt einen Isomorphismus von $\mathbb{F}_q[[t]]$-Moduln:*

$$M[[t]]^\tau \cong M[[t]]_1^\tau := \{\underline{v} \in \overline{K}_\infty[[t]]^d \mid \underline{v}^T = (t-\theta^q)I_d(\underline{v}^T)^{(2)} - A^T(\underline{v}^T)^{(1)}\}.$$

Beweis. Sei $\underline{m} = (\underline{u}, \underline{v}) \in M[[t]]^\tau \cong (\overline{K}_\infty[[t]]^{2d})^\tau$, das heißt $(\underline{u}, \underline{v}) = \tau(\underline{u}, \underline{v})$ in Zeilen. Es folgt mit (3.3), dass $\underline{u}^T = (t-\theta)I_d(\underline{v}^T)^{(1)}$ und $\underline{v}^T = (\underline{u}^T)^{(1)} - A^T(\underline{v}^T)^{(1)}$ gilt. Damit ist $\underline{u}^T$ eindeutig bestimmt und nach Einsetzen der ersten in die zweite Gleichung erhalten wir $\underline{v}^T = (t-\theta^q)I_d(\underline{v}^T)^{(2)} - A^T(\underline{v}^T)^{(1)}$. Die Umkehrung folgt analog. $\square$

Wir betrachten den natürlichen Isomorphismus $\overline{K}_\infty[[t]]^d \longrightarrow (\overline{K}_\infty^d)^{\mathbb{N}_0}$, wobei wir die Elemente aus $\overline{K}_\infty[[t]]^d$ als Spaltenvektoren auffassen:

$$\underline{x} = \left(\sum_{k=0}^\infty \underline{x_1}_k t^k, \ldots, \sum_{k=0}^\infty \underline{x_d}_k t^k \right) \longmapsto (\underline{x}_k)_k = \begin{pmatrix} (\underline{x_1}_k)_k \\ \vdots \\ (\underline{x_d}_k)_k \end{pmatrix}. \tag{3.4}$$

Von nun an treffen wir die Konvention $\underline{x}_k := 0 \in \overline{K}_\infty^d$ für $k < 0$, dann operiert t auf $(\overline{K}_\infty^d)^{\mathbb{N}_0}$ auf natürliche Weise von rechts durch Indexverschiebung, das heißt

$$(\underline{x}_k)_k \cdot t := (\underline{x}_{k-1})_k := \begin{pmatrix} (\underline{x_1}_{-1}, \underline{x_1}_0, \underline{x_1}_1, \ldots) \\ \vdots \\ (\underline{x_d}_{-1}, \underline{x_d}_0, \underline{x_d}_1, \ldots) \end{pmatrix} \text{ für } (\underline{x}_k)_k = \begin{pmatrix} (\underline{x_1}_0, \underline{x_1}_1, \underline{x_2}_0, \ldots) \\ \vdots \\ (\underline{x_d}_0, \underline{x_d}_1, \underline{x_2}_0, \ldots) \end{pmatrix}, \tag{3.5}$$

wobei diese Operation wegen (3.4) mit der von t auf $\overline{K}_\infty[[t]]^d$ übereinstimmt. Also sind $\overline{K}_\infty[[t]]^d$ und $(\overline{K}_\infty^d)^{\mathbb{N}_0}$ als $\mathbb{F}_q[[t]]$-Moduln isomorph.

Weiter identifizieren wir die τ-invarianten Elemente in $(\overline{K}_\infty^d)^{\mathbb{N}_0}$. Entsprechend zu Lemma 3.1.1 gilt für eine Folge $(\underline{v}_k)_k \in (\overline{K}_\infty^d)^{\mathbb{N}_0}$, die zu einem Element $\underline{v} \in M[[t]]_1^\tau$ gehört:

$$\begin{aligned} & (\underline{v}_k)_k = (t - \theta^q)(\underline{v}_k)_k^{(2)} - A^T(\underline{v}_k)_k^{(1)} = (\underline{v}_{k-1})_k^{(2)} - \theta^q(\underline{v}_k)_k^{(2)} - A^T(\underline{v}_k)_k^{(1)} \\ \iff \; & \theta^q(\underline{v}_k)_k^{(2)} + A^T(\underline{v}_k)_k^{(1)} + (\underline{v}_k)_k = (\underline{v}_{k-1})_k^{(2)}. \end{aligned}$$

Nach einer Koordinatentransformation $\underline{v}_k \mapsto \theta^{\frac{-1}{q-1}}\underline{v}_k$ ist dies äquivalent zu

$$\theta^{\frac{-q}{q-1}}(\underline{v}_k)_k^{(2)} + A^T\theta^{\frac{-q}{q-1}}(\underline{v}_k)_k^{(1)} + \theta^{\frac{-1}{q-1}}(\underline{v}_k)_k = \theta^{\frac{-q^2}{q-1}}(\underline{v}_{k-1})_k^{(2)}$$

und nach Multiplikation mit der Konstanten $\theta^{\frac{q}{q-1}}$ schließlich äquivalent zu

$$(\underline{v}_k)_k^{(2)} + A^T(\underline{v}_k)_k^{(1)} + \theta(\underline{v}_k)_k = \theta^{-q}(\underline{v}_{k-1})_k^{(2)}. \tag{3.6}$$

Wir betrachten das folgende $\mathbb{F}_q$-lineare Polynom $f(x,y) \in \overline{K}_\infty^d[x,y]$ in den Unbestimmten $x = (x_1, \ldots, x_d)^T$ und $y = (x_1, \ldots, x_d)^T$:

$$f(x,y) := x^{(2)} + A^T x^{(1)} + \theta x - \theta^{-q} y^{(2)}.$$

$f(x, y)$ spielt in den Polynomgleichung, wie wir sie in Kapitel 4 untersuchen werden, eine wesentliche Rolle.

Für $(\underline{v}_k)_k \in (\overline{K}_\infty^d)^{\mathbb{N}_0}$ ist damit Gleichung (3.6) äquivalent dazu, dass für alle $k \in N_0$

$f(\underline{v}_k, \underline{v}_{k-1}) = 0$ gilt, wobei $\underline{v}_{-1} = 0$ ist.

3.1.2 Lemma. *Es gibt einen Isomorphismus von $\mathbb{F}_q[[t]]$-Moduln:*

$$M[[t]]_1^\tau \cong M[[t]]_f^\tau := \{(\underline{v})_k \in (\overline{K}_\infty^d)^{\mathbb{N}_0} \mid \textit{für alle } k \in \mathbb{N}_0 : f(\underline{v}_k, \underline{v}_{k-1}) = 0\}.$$

Beweis. Die Äquivalenz ergibt sich aus den obigen Rechnungen. □

Um festzustellen, ob eine Folge $\underline{v} \in (\overline{K}_\infty^d)^{\mathbb{N}_0}$ in $M[[t]]_f^\tau$ liegt, lassen sich die Gleichungen $f(\underline{x}_k, \underline{x}_{k-1}) = 0$ von $k = 0$ ausgehend, also mit den Startlösungen $f(\underline{v}_0, 0) = 0$ beginnend, iterativ lösen. Wir können dabei im k-ten Schritt die Lösungen des vorhergehenden $(k-1)$-ten Schritts als Konstante auffassen. Folglich gilt es, in jedem Schritt $f(\underline{x}_k, \underline{x}_{k-1}) = 0$ zu überprüfen, ob $\underline{v}_k$ bei festem $\underline{v}_{k-1}$ eine Lösung ist.

3.1.3 Lemma. *Das Polynom $f(x, 0)$ hat q^{2d} verschiedene Nullstellen.*

Beweis. Die Gleichung $f(x, 0) = 0$ ist äquivalent zu der Matrixgleichung $Qx = 0$ für die Matrix $Q \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty\{\tau\})$ mit

$$Q = \begin{pmatrix} \tau^2 + a_{1,1}\tau + \theta\tau^0 & a_{2,1}\tau & \dots & a_{d,1}\tau \\ a_{1,2}\tau & \tau^2 + a_{2,2}\tau + \theta\tau^0 & \dots & a_{d,2}\tau \\ \vdots & & \ddots & \\ a_{1,d}\tau & a_{2,d}\tau & \dots & \tau^2 + a_{d,d}\tau + \theta\tau^0 \end{pmatrix}.$$

Wir sehen, dass die Matrix Q von folgender Form ist:

$$Q = \begin{pmatrix} q_1(\tau) & q_2(\tau) & \dots & q_d(\tau) \\ a_{1,2}\tau & \tau^2 + a_{2,2}\tau + \theta\tau^0 & \dots & a_{d,2}\tau \\ \vdots & & \ddots & \\ a_{1,d}\tau & a_{2,d}\tau & \dots & \tau^2 + a_{d,d}\tau + \theta\tau^0 \end{pmatrix},$$

wobei $\deg_\tau(q_i(\tau)) < \deg_\tau(q_1(\tau))$ für $i = 2, \dots, d$ gilt. Weiter ist die Darstellung von $q_1(\tau)$

als Polynom in einer Variablen separabel, weil $D_\tau(q_1(\tau)) = \theta \neq 0$ ist; die formale Ableitung von $q_1(\tau)$ ist also eine Konstante in dem perfekten Körper $\overline{K}_\infty$ ist und verschwindet nicht (siehe Definition 1.1.8).

Im Weiteren betrachten wir für $1 \leq l \leq d$ allgemein Matrizen $H \in \mathrm{Mat}_{l\times l}(\overline{K}_\infty\{\tau\})$ von dieser speziellen Form, die auch Q besitzt. Genauer sei

$$H := \begin{pmatrix} h_1(\tau) & h_2(\tau) & \dots & h_l(\tau) \\ b_{2,1}\tau & \tau^2 + b_{2,2}\tau + \theta\tau^0 & \dots & b_{2,l}\tau \\ \vdots & & \ddots & \\ b_{l,1}\tau & b_{l,2}\tau & \dots & \tau^2 + b_{l,l}\tau + \theta\tau^0 \end{pmatrix},$$

wobei gelte:

- $b_{i,j} \in \overline{K}_\infty$ für $2 \leq i \leq l$ und $1 \leq j \leq l$,
- $h_i(\tau) \in \overline{K}_\infty\{\tau\}$ für $1 \leq i \leq l$ mit $\deg_\tau(h_1(\tau)) > \deg_\tau(h_i(\tau))$ für $i = 2, \dots, l$,
- die Darstellung von $h_1(\tau)$ als Polynom in einer Variablen ist separabel.

Wir zeigen nun, dass die Gleichung $Hx = 0$ genau $q^{\deg_\tau(h_1(\tau))+2\cdot(l-1)}$ verschiedene Nullstellen $x \in (\overline{K}_\infty)^l$ hat, indem wir diese Aussage induktiv auf ein ähnliches Problem niedrigerer Dimension reduzieren. Für $l = 1$ ist die Aussage offensichtlich wahr. Wir nehmen also an, dass $l > 1$ ist.

Falls $b_{2,1} = \ldots = b_{l,1} = 0$ gilt, hat die $((l-1)\times(l-1))$-Matrix $\widetilde{H}$, die durch Streichen der ersten Spalte und der ersten Zeile von H entsteht, wieder die oben genannte spezielle Form wie H selbst. Da die Darstellung von $h_1(\tau)$ als Polynom in einer Variablen separabel ist, gibt es für jede Nullstelle $\tilde{x} \in (\overline{K}_\infty)^{l-1}$ von $\widetilde{H}\tilde{x} = 0$ genau $q^{\deg_\tau(h_1(\tau))}$ verschiedene Nullstellen für $Hx = 0$. Somit gilt die Aussage in diesem Fall.

Falls $b_{i,1} \neq 0$ für ein $i \in \{2, \dots, l\}$ gilt, können wir ohne Beschränkung der Allgemeinheit annehmen, dass $b_{l,1} \neq 0$ ist, da wir an H von links und von rechts entsprechende Vertauschungsmatrizen multiplizieren können, so dass die spezielle Gestalt von H erhalten bleibt. Insbesondere ändert dies nichts an der Anzahl der Lösungen.

Weiter multiplizieren wir an die Matrix H von links die $(l \times l)$-Matrix

$$G := \begin{pmatrix} \tau & 0 & 0 & \dots & 0 & g(\tau) \\ 0 & 1 & 0 & \dots & 0 & \gamma_2 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ \vdots & & \ddots & \ddots & 0 & \vdots \\ \vdots & & & \ddots & 1 & \gamma_{l-1} \\ 0 & \dots & \dots & \dots & 0 & 1 \end{pmatrix}; \text{ bzw. } G := \begin{pmatrix} 1 & g(\tau) \\ 0 & 1 \end{pmatrix} \text{ im Fall } l = 2,$$

wobei $g(\tau) \in \overline{K}_\infty\{\tau\}$ und $\gamma_2, \dots, \gamma_{l-1} \in \overline{K}_\infty$ im Folgenden geeignet gewählt werden. Dies ändert ebenfalls nicht die Anzahl der Lösungen. Die $(l \times l)$-Matrix GH ist

$$\begin{pmatrix} \tau h_1(\tau) + g(\tau) \cdot b_{l,1}\tau & \tau h_2(\tau) + g(\tau) \cdot b_{l,2}\tau & \tau h_3(\tau) + g(\tau) \cdot b_{l,3}\tau & \dots & \tau h_l(\tau) + g(\tau) \cdot (\tau^2 + b_{l,l}\tau + \theta\tau^0) \\ b_{2,1}\tau + \gamma_2 b_{l,1}\tau & (\tau^2 + b_{2,2}\tau + \theta\tau^0) + \gamma_2 b_{l,2}\tau & b_{2,3}\tau + \gamma_2 b_{l,3}\tau & \dots & b_{2,l}\tau + \gamma_2(\tau^2 + b_{l,l}\tau + \theta\tau^0) \\ b_{3,1}\tau + \gamma_3 b_{l,1}\tau & b_{3,2}\tau + \gamma_3 b_{l,2}\tau & (\tau^2 + b_{3,3}\tau + \theta\tau^0) + \gamma_3 b_{l,3}\tau & \dots & b_{3,l}\tau + \gamma_3(\tau^2 + b_{l,l}\tau + \theta\tau^0) \\ \vdots & \vdots & \ddots & & \\ b_{l-1,1}\tau + \gamma_{l-1} b_{l,1}\tau & b_{l-1,2}\tau + \gamma_{l-1} b_{l,2}\tau & \dots & (\tau^2 + b_{l-1,l-1}\tau + \theta\tau^0) + \gamma_{l-1} b_{l,l-1}\tau & b_{l-1,l}\tau + \gamma_{l-1}(\tau^2 + b_{l,l}\tau + \theta\tau^0) \\ b_{l,1}\tau & b_{l,2}\tau & \dots & b_{l,l-1}\tau & \tau^2 + b_{l,l}\tau + \theta\tau^0 \end{pmatrix}.$$

Wir wählen $g(\tau)$ und $\gamma_2, \dots, \gamma_{l-1}$, so dass gilt:

$$\tau h_1(\tau) + g(\tau) \cdot b_{l,1}\tau = 0 \quad \text{und} \quad b_{i,1}\tau + \gamma_i b_{l,i}\tau = 0 \text{ für alle } i = 2, \dots, l-1.$$

Aus dieser Wahl folgt $\deg_\tau(g(\tau)) = \deg_\tau(h_1(\tau))$ und $D_\tau(g(\tau)) = \frac{\theta}{b_{l,1}} \neq 0$ sowie, dass die erste Spalte von GH bis auf den letzten Eintrag verschwindet.
Wir addieren nun für jedes $i = 2, \dots, l-1$ das $(-\gamma_i)$-fache der i-ten Spalte von GH zu der letzten Spalte von GH. Dies stellte eine Multiplikation mit einer Matrix G' von rechts an die Matrix GH dar und ändert damit auch nicht die Anzahl der Lösungen. Der j-te Eintrag der letzten Spalte von GHG' ist dann

$$\begin{aligned} \text{für } j = 1: \quad & \tau h_1(\tau) + g(\tau) \cdot (\tau^2 + b_{l,l}\tau + \theta\tau^0) - \sum_{i=2}^{l-1} (\tau h_i(\tau) + g(\tau) \cdot b_{l,i}\tau) =: \tilde{h}_1(\tau), \\ \text{für } j = 2, \dots, l-1: \quad & b_{j,l}\tau + \gamma_j(\tau^2 + b_{l,l}\tau + \theta\tau^0) - \gamma_j \left((\tau^2 + b_{j,j}\tau + \theta\tau^0) + \gamma_j b_{l,l}\tau\right) - \sum_{i=2, i\neq j}^{l-1} \gamma_i(b_{j,i}\tau + \gamma_j b_{l,i}\tau) \\ & = \underbrace{\left(b_{j,l} + \gamma_j b_{l,l} - \sum_{i=2}^{l-1} \gamma_i(b_{j,i} + \gamma_j b_{l,i}) \right)}_{=:\tilde{b}_{j,1}} \tau, \\ \text{für } j = l: \quad & \tau^2 + \underbrace{\left(b_{l,l} - \sum_{i=2}^{l-1} \gamma_i b_{l,i} \right)}_{=:\tilde{b}_{l,1}} \tau + \theta\tau^0. \end{aligned}$$

Zuletzt vertauschen wir die Spalten von GHG', so dass die letzte Spalte an die Stelle der zweiten Spalte tritt und für $i = 2, \dots l-2$ die Spalte i an die Stelle der Spalte $i+1$ nach rechts verschoben wird. Dies stellt wiederum eine Multiplikation mit einer Matrix G'' von rechts an die Matrix GHG' dar, was nicht die Anzahl der Lösungen ändert. Wir erhalten insgesamt für $GHG'G''$:

$$\begin{pmatrix} 0 & \tilde{h}_1(\tau) & \tau h_2(\tau) + g(\tau) b_{l,2}\tau & \tau h_3(\tau) + g(\tau) b_{l,3}\tau & \dots & \tau h_{l-1}(\tau) + g(\tau) b_{l,l-1}\tau \\ 0 & \tilde{b}_{j,2}\tau & \tau^2 + (b_{2,2} + \gamma_2 b_{l,2})\tau + \theta\tau^0 & (b_{2,3} + \gamma_2 b_{l,3})\tau & \dots & (b_{2,l-1} + \gamma_2 b_{l,l-1})\tau \\ 0 & \tilde{b}_{j,3}\tau & (b_{3,2} + \gamma_3 b_{l,2})\tau & \tau^2 + (b_{3,3} + \gamma_3 b_{l,3})\tau + \theta\tau^0 & \dots & (b_{3,l-1} + \gamma_3 b_{l,l-1})\tau \\ \vdots & \vdots & & & \ddots & \\ 0 & \tilde{b}_{j,1}\tau & (b_{l-1,2} + \gamma_{l-1} b_{l,2})\tau & (b_{l-1,3} + \gamma_{l-1} b_{l,3})\tau & \dots & \tau^2 + (b_{l-1,l-1} + \gamma_{l-1} b_{l,l-1})\tau + \theta\tau^0\tau \\ b_{l,1}\tau & \tau^2 + \tilde{b}_{l,1}\tau + \theta\tau^0 & b_{l,2}\tau & b_{l,3} & \dots & b_{l,l-1}\tau \end{pmatrix}.$$

Nach Definition von $\tilde{h}_1(\tau)$ ist $D_\tau(\tilde{h}_1(\tau)) = D_\tau(g(\tau)\cdot\theta\tau^0) = \frac{\theta^2}{b_{l,1}} \neq 0$ und weiter gilt

$$\begin{aligned} \deg_\tau(\tilde{h}_1(\tau)) = \deg_\tau(h_1(\tau)) + 2 \quad &> \max_{j=2,\dots,l-1} \{\deg_\tau(\tau h_j(\tau) + g(\tau) b_{l,j}\tau)\} \\ &= \deg_\tau(g(\tau) b_{l,j}\tau)) = \deg_\tau(h_1(\tau)) + 1. \end{aligned}$$

Die $((l-1)\times(l-1))$-Matrix $\widetilde{H}$, die durch Streichen der ersten Spalte und der letzten Zeile von $GHG'G''$ entsteht, hat also die spezielle Form wie H selbst. Durch Induktion folgt schließlich, dass $\widetilde{H}\tilde{x} = 0$ genau $q^{\deg_\tau(\tilde{h}_1(\tau)) + 2\cdot(l-2)} = q^{\deg_\tau(h_1(\tau)) + 2\cdot(l-1)}$ verschiedene Nullstellen $\tilde{x} \in (\overline{K}_\infty)^{l-1}$ hat, die durch Einsetzen dieser Lösungen in die letzte Zeile von $(GHG'G'')x = 0$ genauso viele Nullstellen $x \in (\overline{K}_\infty)^l$ für $Hx = 0$ liefern. □

Das folgende Lemma zeigt nun, dass wir in jedem Schritt ausreichend viele τ-invariante Elemente in $M[[t]]$ finden, wodurch die Möglichkeit grundsätzlich gegeben ist, dass eine Folge aus $(\overline{K}_\infty^d)^{\mathbb{N}_0}$ in $M[[t]]_f^\tau$ liegen kann.

3.1.4 Lemma. *Es gilt* $\operatorname{Rang}_{\mathbb{F}_q[[t]]}(M[[t]]_f^\tau) = \operatorname{Rang}_{\mathbb{F}_q[[t]]}(M[[t]]^\tau) = 2d.$

Beweis. $M[[t]]_f^\tau$ ist ein Untermodul von dem endlich erzeugten $\mathbb{F}_q[[t]]$-Modul $M[[t]]_f$, wobei $M[[t]]_f \cong M[[t]] \cong \overline{K}_\infty[[t]]^{2d}$ gilt. Wir wissen, dass $\mathbb{F}_q[[t]]$ ein lokaler Ring mit dem maximalen Ideal $\mathfrak{m} := t\cdot\mathbb{F}_q[[t]]$ und dem Quotientenkörper $\mathbb{F}_q[[t]]/\mathfrak{m} = \mathbb{F}_q$ ist. Weiter ist $M[[t]]_f^\tau/(\mathfrak{m}\cdot M[[t]]_f^\tau)$ ein $\mathbb{F}_q$-Vektorraum, der mit dem Vektorraum der Startlösungen übereinstimmt. Wir schreiben also entsprechend dieser Überlegungen

$$\mathcal{L} := \{\underline{x}_0 \in \overline{K}_\infty^d \mid f(\underline{x}_0, 0) = 0\} = M[[t]]_f^\tau/(\mathfrak{m}\cdot M[[t]]_f^\tau).$$

Nach Lemma 3.1.3 hat $f(x,0)$ genau q^{2d} verschiedene Nullstellen und wir können darunter $2d$ Nullstellen $\underline{\xi_{(1)}}_0, \ldots, \underline{\xi_{(2d)}}_0 \in \overline{K}_\infty^d$ wählen, die eine $\mathbb{F}_q$-Basis von $\mathcal{L}$ bilden. Wir finden somit zu jedem dieser Basisvektoren $\underline{\xi_{(i)}}_0$ eine Fortsetzung $(\underline{\xi_{(i)}}_k)_k$ in $M[[t]]_f^\tau$ und erhalten mit dem Lemma von Nakayama (siehe [Matsumura; 1986, Theorem 2.3]) schließlich daraus eine Basis $(\underline{\xi_{(1)}}_k)_k, \ldots, (\underline{\xi_{(2d)}}_k)_k$ von $M[[t]]_f^\tau$. □

Wir sehen also, dass die Frage, ob ein t-Modul uniformisierbar ist, gleichbedeutend damit ist, ob es in jedem Schritt genügend τ-invariante Elemente in $M\langle\langle t\rangle\rangle$ gibt. Dieses Problem werden wir im Folgenden genauer betrachten.

In $M\langle\langle t\rangle\rangle^\tau$ sind gerade die Elemente aus $M[[t]]^\tau$ enthalten, die eine Nullfolge bilden und bei denen alle Koeffizienten in einer endlichen Erweiterung $L \subset \overline{K}_\infty$ von K_∞ liegen. Entsprechend beschreiben wir $M\langle\langle t\rangle\rangle^\tau$ als Untermodul von $M[[t]]_f^\tau$ und definieren dazu entsprechend den $\mathbb{F}_q[t]$-Modul

$$M\langle\langle t\rangle\rangle_f^\tau := \left\{ (\underline{v}_k)_k \in M[[t]]_f^\tau \;\middle|\; \begin{array}{l} \lim\limits_{k\to\infty} |\underline{v}_k| = 0 \text{ und die Menge } \{\underline{v}_{i_k}\} \text{ liegt in einer} \\ \text{endlichen algebraischen Erweiterung } L \subset \overline{K}_\infty \text{ von } K_\infty \end{array} \right\}.$$

3.1.5 Lemma. *Es gibt einen Isomorphismus von $\mathbb{F}_q[t]$-Moduln:*

$$M\langle\langle t\rangle\rangle^\tau \cong M\langle\langle t\rangle\rangle_f^\tau.$$

Beweis. Ergibt sich durch die Einschränkung des Isomorphismus aus dem Beweis von Lemma 3.1.2 auf den Untermodul $M\langle\langle t\rangle\rangle^\tau$ von $M[[t]]^\tau$ zusammen mit den Argumenten aus dem Beweis von [Bangert; 2011, Lemma 4.1.9]. □

Schließlich können wir das folgende Resultat festhalten:

3.1.6 Satz. *Sei E ein t-Modul der Dimension d gegeben durch $t = \tau^2 + A\tau + \theta$ mit $A \in \mathrm{Mat}_{d\times d}(L)$ und $M := M(E)$ das zugehörige t-Motiv. Dann ist E ist genau dann uniformisierbar, wenn gilt:*

$$\mathrm{Rang}_{\mathbb{F}_q[t]}\left(M\langle\langle t\rangle\rangle_f^\tau\right) = 2d.$$

Beweis. Folgt aus Lemma 2.3.11 und Lemma 3.1.4. □

Eine geeignete Basis für $M\langle\langle t\rangle\rangle_f^\tau$

Es sei E ein abelscher t-Modul und $M = M(E)$ das zugehörige t-Motiv. Wir wollen in diesem Abschnitt analog zum Beweis von Lemma 3.1.4 eine Basis für $M\langle\langle t\rangle\rangle_f^\tau$ angeben. Im Weiteren sei $r := \mathrm{Rang}_{\mathbb{F}_q[t]}(M\langle\langle t\rangle\rangle_f^\tau) \leq 2d$.

Der $\mathbb{F}_q$-Vektorraum der Startlösungen $\mathcal{L} := \{\underline{x}_0 \in \overline{K}_\infty^d \mid f(\underline{x}_0, 0) = 0\}$ hat die Dimension $2d$, also gibt es eine Basis $(\underline{\xi_{(1)}}_0, \ldots, \underline{\xi_{(2d)}}_0)$ von $\mathcal{L}$.

Da $r = \mathrm{Rang}_{\mathbb{F}_q[t]}(M\langle\langle t\rangle\rangle_f^\tau)$ ist, gibt es zu r dieser Basiselemente, seien dies o.B.d.A. die Elemente $\underline{\xi_{(1)}}_0, \ldots, \underline{\xi_{(r)}}_0$, jeweils eine Fortsetzung $\underline{\xi_{(i)}} \in M\langle\langle t\rangle\rangle_f^\tau$.
Das heißt, es ist $f(\underline{\xi_{(i)}}_0, 0) = 0$; die Koeffizienten aller Folgenglieder $\underline{\xi_{(i)}}_k$, $k \in N_0$ liegen in einer endlichen Erweiterung von K_∞ und es gilt:

$$f(\underline{\xi_{(i)}}_{k+1}, \underline{\xi_{(i)}}_k) = 0 \text{ für } k \geq 0 \quad \text{und} \quad \lim_{k\to\infty} |\underline{\xi_{(i)}}_k| = 0.$$

Sei nun $\underline{x}_0 \in \mathcal{L}$ eine beliebige andere Startlösung, dann erhalten wir die Darstellung

$$\underline{x}_0 = \sum_{i=0}^{r} b_i \underline{\xi_{(i)}}_0, \quad \text{mit } b_i \in \mathbb{F}_q.$$

Folglich ist $\sum_{i=0}^r b_i \underline{\xi_{(i)}}$ eine Fortsetzung von $\underline{x}_0$ in $M\langle\langle t\rangle\rangle_f^\tau$, denn mit der $\mathbb{F}_q$-Linearität von f gilt:

$$f\left(\sum_{i=0}^{r} b_i \underline{\xi_{(i)}}_{k+1}, \sum_{i=0}^{r} b_i \underline{\xi_{(i)}}_k)\right) = \sum_{i=0}^{r} b_i \cdot f(\underline{\xi_{(i)}}_{k+1}, \underline{\xi_{(i)}}_k) = 0.$$

Betrachten wir nun die Struktur von $M\langle\langle t\rangle\rangle_f^\tau$ als $\mathbb{F}_q[t]$-Modul. Sei $\sum_{j=0}^n a_j t^j \in \mathbb{F}_q[t]$ beliebig, dann ist zu dem Element $(\sum_{j=0}^n a_j t^j)\underline{x}_0 = (\sum_{j=0}^n a_j t^j) \sum_{i=0}^r b_i \underline{\xi_{(i)}}_0$ eine Fortsetzung in $M\langle\langle t\rangle\rangle_f^\tau$ gegeben durch:

$$\sum_{j=0}^{n} a_j t^j \sum_{i=0}^{r} b_i \underline{\xi_{(i)}} = \sum_{i=0}^{r} \sum_{j=0}^{n} a_j b_i \underline{\xi_{(i)}} t^j.$$

Also ist $(\underline{\xi_{(1)}}, \ldots, \underline{\xi_{(r)}})$ eine $\mathbb{F}_q[t]$-Basis des Moduls $M\langle\langle t\rangle\rangle_f^\tau$.

3.2 Kriterien für Uniformisierbarkeit als Problem linearer Polynomgleichungen

In diesem Abschnitt beschreiben wir die speziellen $\mathbb{F}_q$-linearen Polyomgleichungen, die sich aus der Frage der Uniformisierbarkeit eines t-Moduls in Abschnitt 3.1 ergeben haben, als unabhängiges Problem. Damit motivieren wir die allgemeine Untersuchung der Lösungen spezieller Polynomgleichungen, die wir in Kapitel 4 durchführen werden.

Es sei weiterhin $K_\infty = \mathbb{F}_q((\frac{1}{\theta}))$ und $\overline{K}_\infty = \overline{\mathbb{F}_q((\frac{1}{\theta}))}$. Wir betrachten einen abelschen t-Modul E der Dimension d, der gegeben ist durch den $\mathbb{F}_q$-linearen Endomorphismus

$$t = \tau^2 + A\tau + \theta\tau^0 \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)\{\tau\},$$

wobei $A = (a_{i,j})_{1\leq,i,j\leq d} \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)$ mit den Einträgen $a_{i,j} \in \overline{K}_\infty$ beliebig ist.
Wie wir in Abschnitt 3.1 gesehen haben, stehen bei der Untersuchung der Uniformisierbarkeit dieses t-Moduls die Folgen von Lösungen $(\underline{x}_k)_k \in (\overline{K}_\infty^d)^{\mathbb{N}_0}$ von speziellen rekursiv voneinander abhängigen Polynomgleichungen im Mittelpunkt. Dabei ist das folgende, zu t ähnliche, $\mathbb{F}_q$-lineare Polynom involviert:

$$\widetilde{t} = \tau^2 + A^T\tau + \theta\tau^0 \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)\{\tau\} \tag{3.7}$$

Genauer heißt das (siehe Satz 3.1.6):

3.2.1 Bemerkung. *Es ist $(\underline{x}_k)_k \in M[[t]]_f^\tau$ genau dann, wenn gilt:*

Für $k = 0$ ist $\underline{x}_0 \in \overline{K}_\infty^d$ eine Lösung der Gleichung

$$\widetilde{t}\begin{pmatrix} \underline{x_1}_0 \\ \vdots \\ \underline{x_d}_0 \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Für $k > 0$ ist $\underline{x}_k \in \overline{K}_\infty^d$ jeweils eine Lösung von

$$\widetilde{t}\begin{pmatrix} \underline{x_1}_k \\ \vdots \\ \underline{x_d}_k \end{pmatrix} = \theta^{-q}\tau^2 \begin{pmatrix} \underline{x_1}_{k-1} \\ \vdots \\ \underline{x_d}_{k-1} \end{pmatrix}.$$

Weiter ist $(\underline{x}_k)_k \in M\langle\langle t\rangle\rangle_f^\tau$ *genau dann, wenn* $(\underline{x}_k)_k \in M[[t]]_f^\tau$ *ist und zusätzlich gilt:*

> *Es gibt eine endliche algebraische Erweiterung* $L \subset \overline{K}_\infty$ *von* K_∞*, so dass* $\{\underline{x}_k\} \subset L^d$ *ist und es gilt* $\lim\limits_{k\to\infty} v_\infty(\underline{x}_k) = \infty$*, bzw.* $\lim\limits_{k\to\infty} |\underline{x}_k|_{v_\infty} = 0$.

Indem wir $\underline{x}_k := 0 \in \overline{K}_\infty^d$ für $k < 0$ setzen, können wir somit auf die separate Betrachtung des Sonderfalls $k = 0$ verzichten. Davon ausgehend definieren wir:

3.2.2 Definition. *Es sei* $f(x,y) \in \overline{K}_\infty^d[x,y]$ *in den Unbestimmten* $x = (x_1,\dots,x_d)^T$ *und* $y = (x_1,\dots,x_d)^T$ *gegeben durch:*

$$f(x,y) := x^{(2)} + A^T x^{(1)} + \theta x - \theta^{-q} y^{(2)};$$

dabei ist $f_i(x,y) :=\ x_i^{q^2} + \sum_{j=1}^d a_{j,i} x_j^q + \theta x_i - \theta^{-q} y_i^{q^2} \in L[x,y]$ *für* $i = 1,\dots,d$.

Äquivalent zu $(\underline{x}_k)_k \in M[[t]]_f^\tau$ ist also, falls für alle $k \in \mathbb{N}_0$ gilt:

$$f(\underline{x}_k, \underline{x}_{k-1}) = 0. \tag{3.8}$$

Wir sehen nun weiter, dass $M[[t]]_f^\tau$ auch als projektiver Limes verstanden werden kann. Sei dazu $\varphi : \overline{K}_\infty^d \to \overline{K}_\infty^d$ der $\overline{K}_\infty$-Vektorraumhomomorphismus mit

$$\varphi(x) := \left(\theta^q (x^{(2)} + A^T x^{(1)} + \theta x)\right)^{(-2)},$$

wobei $\varphi(x)$ eindeutig bestimmt ist, da $\overline{K}_\infty$ perfekt ist (siehe Definition 1.1.14).
Weiter definieren wir $\varphi_{i,j} := \varphi^{i-j}$ für $i > j \geq 0$ als die $(i-j)$-fache Hintereinanderausführung von φ. Dann ist durch

$$\varprojlim \overline{K}_\infty^d = \{(\underline{v}_k)_k \in \prod_{i\in\mathbb{N}_0} \overline{K}_\infty^d \mid \varphi_{i,j}(\underline{v}_i) = \underline{v}_j \text{ für } i > j\}$$

ein $\overline{K}_\infty^d[[t]]$-Modul gegeben, wobei t von rechts auf $(\overline{K}_\infty^d)^{\mathbb{N}_0}$ dadurch wirkt, dass 0 als erstes Folgenglied eingefügt wird und die restlichen Folgenglieder nach rechts verschoben werden. Wegen der Konvention $\underline{x}_{-1} = 0$ ist $\underline{x}_{k-1} = (\underline{x}_k)_k \cdot t$ also eine Indexverschiebung. Dabei gilt wegen $f(x, \varphi(x)) = 0$ folglich:

$$\varprojlim \overline{K}_\infty^d = M[[t]]_f^\tau. \tag{3.9}$$

Das Problem, das den Ausgangspunkt für die Untersuchungen in Kapitel 4 darstellt, lässt sich nun wie folgt formulieren:

3.2.3 Problem. *Seien* $\underline{x}_0, \ldots, \underline{x}_k \in \overline{K}_\infty^d$ *mit* $f(\underline{x}_i, \underline{x}_{i-1}) = 0$ *für* $k \geq i \geq 0$ *gegeben. Unter welchen (notwendigen oder hinreichenden) Bedingungen gibt es für* $l \in \mathbb{N}_0$ *eine Fortsetzung* $\underline{x}_0, \ldots, \underline{x}_k, \ldots \underline{x}_{k+l}$*, so dass gilt*

1. $f(\underline{x}_i, \underline{x}_{i-1}) = 0$ *für alle* i *mit* $k + l \geq i \geq 0$,
2. $v_\infty(\underline{x}_{k+l}) \geq v_\infty(\underline{x}_{k-1}) + c$ *für eine fest vorgegebene Konstante* $c > 0$ *?*

Wir werden häufig den Spezialfall $l := 1$ betrachten, auch wenn damit nur noch hinreichende Bedingungen für die Frage angegeben werden können, wann ein Element $(\underline{x}_k)_k \in M[[t]]_f^\tau$ in $M\langle\langle t\rangle\rangle_f^\tau$ liegt. Andererseits führt diese Vereinfachung dazu, dass wir die Wirkung von f bzw. φ nur einmal untersuchen müssen.

3.2.4 Bemerkung. *Wir betrachten den Fall* $d = 1$*. Hier ist ist für* $x, y \in \overline{K}_\infty$

$$f(x, y) := x^{q^2} + ax^q + \theta x - \theta^{-q} y^{q^2}$$

gegeben durch ein $a \in \overline{K}_\infty$*. Wir nehmen nun an, dass* y *fest vorgegeben ist, dann hat die Gleichung* $f(x, y) = 0$ *genau* q^2 *Lösungen* $\xi_1, \ldots \xi_{q^2}$ *für* x*. Es gilt schließlich:*

$$\begin{aligned} \prod_{i=1,\ldots,q^2} \xi_i = \theta^{-q} y^{q^2} \quad &\Longrightarrow \quad v_\infty(\prod_{i=1,\ldots,q^2} \xi_i) = v_\infty(\theta^{-q} y^{q^2}) \\ &\Longrightarrow \quad \sum_{i=1,\ldots,q^2} v_\infty(\xi_i) = q + q^2 v_\infty(y). \end{aligned}$$

Daraus folgt durch Vergleich von linker und rechter Seite, dass es mindestens ein ξ *gibt, für das gilt:*

$$v_\infty(\xi_i) \geq v_\infty(y) + \frac{1}{q},$$

wobei Gleichheit genau dann eintritt, wenn $v_\infty(\xi_1) = \ldots = v_\infty(\xi_{q^2})$ *ist.*

Damit ist Problem 3.2.3 im Fall $d = 1$ gelöst. (Es folgt daraus mit den Argumenten aus Abschnitt 3 die Uniformisierbarkeit aller abelscher t-Moduln der Dimension $d = 1$, was genau der Aussage über Drinfeld-Moduln in 2.1 entspricht).

Aus dieser Beobachtung leiten wir für Problem 3.2.3 ab, dass $c := \frac{1}{q}$ eine mögliche Vereinfachung ist, die wir an einigen Stellen zusätzlich zu $l = 1$ auch für Dimensionen $d > 1$ annehmen werden. Diese Vereinfachung stellt jedoch für sich allein bereits eine Einschränkung dar, durch die nur noch hinreichende Kriterien für die Beantwortung des ursprünglichen Problems untersucht werden können.

3.2.5 Bemerkung. *Einschränkende Annahmen an die Konstanten c und l ermöglichen jeweils nur noch hinreichende Bedingungen für die Lösbarkeit von Problem 3.2.3.*

4 Lösungen spezieller Polynomgleichungen

Wir haben in Kapitel 3 gesehen, dass rekursiv voneinander abhängige $\mathbb{F}_q$-lineare Polynomgleichungen über Funktionenkörpern in der Theorie der t-Moduln eine wesentliche Rolle spielen. Wir werden nun die Probleme, wie in Abschnitt 3.2 beschrieben, unabhängig von t-Moduln untersuchen.

Wir erweitern und systematisieren zunächst die Herangehensweise aus [Bangert; 2011] und entwickeln dann weitere Methoden, mit denen sich die Kriterien für die Lösbarkeit von Problem 3.2.3 in beliebigen Dimensionen erforschen lassen.

4.1 Ein erweitertes Reduktionsverfahren

In [Bangert; 2011, Kapitel 4.1] wird das Problem, wann in Dimension $d = 2$ eine Folge $(\underline{x_k})_k \in M[[t]]_f^\tau$ in $M\langle\langle t\rangle\rangle_f^\tau$ liegt, durch Auflösung der Gleichung $f(x, y) = 0$ in eine Komponente der Variable x und Betrachtung des zugehörigen Newton-Polygons untersucht. Dieser Ansatz lässt sich in höhere Dimensionen $d \geq 2$ übertragen. Wir leiten in diesem Abschnitt ein Reduktionsverfahren für allgemeine $\mathbb{F}_q$-lineare Polynomgleichungen her und zeigen, dass zu gegebenem $y \in \overline{K}_\infty^d$ eine Auflösung von $f(x, y) = 0$ in eine Komponente von x, hier $x_d, \in \overline{K}_\infty$, stets möglich ist.

Es seien $A^T \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty\{\tau\})$ und $y \in \overline{K}_\infty^d$ fest gewählt. Weiter sei $L \subset \overline{K}_\infty$ eine endliche algebraische Erweiterung von K_∞, so dass $A^T \in \mathrm{Mat}_{d\times d}(L)$ und $y \in L^d$ gelten.

Weiter sei nun $f(x, y) \in L^d[x, y]$ aus Definition 3.2.2 entsprechend

$$f(x, y) = x^{(2)} + A^T x^{(1)} + \theta x - \theta^{-q} y^{(2)},$$

dann lässt sich dies darstellen als $f(x,y) = Q\begin{pmatrix} x \\ y \end{pmatrix}$ mit der Blockmatrix $Q \in \mathrm{Mat}_{d\times 2d}(L\{\tau\})$, die gegeben ist durch:

$$Q = \begin{pmatrix} \tau^2 + A^T\tau + \theta\tau^0 & -\theta^{-q}\tau^2 \end{pmatrix}$$

$$= \begin{pmatrix} \tau^2 + a_{1,1}\tau + \theta & a_{2,1}\tau & \dots & a_{d,1}\tau & -\theta^{-q}\tau^2 & & 0 \\ a_{1,2}\tau & \tau^2 + a_{2,2}\tau + \theta & \dots & a_{d,2}\tau & & -\theta^{-q}\tau^2 & \\ \vdots & & \ddots & & & & \ddots & \\ a_{1,d}\tau & a_{2,d}\tau & \dots & \tau^2 + a_{d,d}\tau + \theta & 0 & & -\theta^{-q}\tau^2 \end{pmatrix}.$$

Wir werden im Folgenden zeigen, dass es ein Reduktionsverfahren analog zur Hermite-Normalform für Matrizen über $\mathbb{Z}$ (siehe z.B. [Cohen; 1993, Theorem 2.4.3]) für beliebige Matrizen $Q \in \mathrm{Mat}_{m\times n}(L\{\tau\})$ gibt. Da wir nur die Auflösbarkeit in eine Variable zeigen wollen und in unserem Fall $m > n$ gilt, reicht es, wenn wir eine Matrix G aus $\mathrm{GL}_m(L\{\tau\})$ konstruieren, so dass alle Elemente von GQ, deren Zeilenindex größer als ihr Spaltenindex ist, verschwinden.

4.1.1 Definition. *Sei $GQ \in \mathrm{Mat}_{m\times n}(L\{\tau\})$ mit $m > n$, dann nennen wir die Matrix GQ in aufgelöster Form, falls sie die folgende Gestalt hat:*

$$GQ = \begin{pmatrix} * & * & \dots & * & * & \dots & * \\ 0 & * & \dots & * & * & \dots & * \\ \vdots & \ddots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 0 & * & * & \dots & * \end{pmatrix}.$$

Wir gehen bei dem Reduktionsverfahren iterativ vor; das folgende Lemma liefert dazu einen Schritt.

4.1.2 Lemma. *Sei $Q \in \mathrm{Mat}_{m\times n}(L\{\tau\})$, m, n beliebig, dann gibt es eine invertierbare Matrix $G \in \mathrm{GL}_m(L\{\tau\})$, so dass in der ersten Spalte von GQ alle Einträge unterhalb der ersten Zeile verschwinden.*

Beweis. Wir nehmen an, dass es Nicht-Nulleinträge in der ersten Spalte gibt. Dann gibt es eine invertierbare Matrix T, so dass in der ersten Spalte der Eintrag mit dem kleinsten q-Grad in der ersten Zeile von TQ steht. Sei $p_1(\tau) \in L\{\tau\}$ dieser Eintrag. Wir eliminieren nun sukzessive in allen anderen Einträgen der ersten Spalte alle Monome, deren q-Grad größer als $\deg(p_1(\tau))$ ist, durch Addition entsprechender Vielfacher der ersten Zeile.

Eliminationsschritt: Für $i \in \{2, \ldots, m\}$ wenden wir den Links-Divisions-Algorithmus auf die Einträge $p_i(\tau)$ an. Nach Proposition 1.1.10 finden wir $a_i(\tau), r_i(\tau) \in L\{\tau\}$ mit:

$$p_i(\tau) = s_i(\tau)p_1\tau + r_i(\tau),$$

wobei $\deg(r_i(\tau)) < \deg(p_1(\tau))$ ist. Wir erhalten so die invertierbare Matrix

$$S = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ -s_2(\tau) & 1 & & 0 \\ \vdots & & \ddots & \\ -s_n(\tau) & 0 & & 1 \end{pmatrix} \in \mathrm{GL}_m(L\{\tau\}).$$

Die erste Spalte von STQ ist dann der Spaltenvektor $(p_1(\tau), r_2(\tau), \ldots, r_n(\tau))^T$.

Vertauschungsschritt: Wir wählen aus $(p_1(\tau), r_2(\tau), \ldots, r_n(\tau))^T$ den Nicht-Nulleintrag aus, der den kleinsten q-Grad hat. Sollte dies $p_1(\tau)$ selbst sein, so wurden alle anderen Einträge der ersten Spalte von STQ eliminiert; falls nicht, so vertauschen wir die Zeile dieses Eintrags mit der ersten Zeile durch eine invertierbare Matrix und wiederholen den Eliminationsschritt.

Nach jedem Eliminationsschritt ist der q-Grad aller anderen Einträge der ersten Spalte um mindestens Eins kleiner als der q-Grad des ersten Eintrags. Daher reichen endlich viele Anwendungen von Vertauschungs- und Eliminationsschritten aus, deren Produkt die invertierbare Matrix G liefert, so dass in der ersten Spalte von GQ alle Einträge unterhalb der ersten Zeile verschwinden. □

4.1.3 Satz. *Sei $Q \in \mathrm{Mat}_{m\times n}(L\{\tau\})$ mit $m > n$, dann gibt es eine invertierbare Matrix $G \in \mathrm{GL}_m(L\{\tau\})$, so dass GQ in aufgelöster Form ist.*

Beweis. Wir wenden Lemma 4.1.2 iterativ an, wobei wir nach jedem Schritt die Untermatrix betrachten, die durch Streichen der ersten Zeile und Spalte entsteht. Die invertierbaren Matrizen, die dabei gewonnen werden, ergänzen wir entsprechend mit 1-Einträgen auf der Hauptdiagonalen zur Dimension d. □

Sei G zu Q mit Satz 4.1.3 berechnet. Wir bezeichnen im Weiteren mit $f_*(x_d) = 0$ die Gleichung, die sich für den (d, d)-ten Eintrag von GQ durch Auflösung von $f(x)$ nach

x_d ergibt; diese ist abhängig von A und y.

In aufgelöster Form können wir also zu gegebenen A^T und y die möglichen Bewertungen aller Nullstellen von $f_*(x_d)$ durch Auswertung des zugehörigen Newton-Polygons (siehe Definition 1.2.9) bestimmen. Durch Rückwärtselimination (Einsetzen der k-ten Komponente der Lösung in die $(k-1)$-te Gleichung) lassen sich damit schließlich untere Schranken für die Bewertungen aller Einträge von x finden.

Für Dimension $d = 2$ werden wir nun die Reduktion aus Satz 4.1.3 konkret bestimmen.

4.1.4 Beispiel. *Das Polynomgleichungssystem für $d = 2$ lautet*

$$Q\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} x_1^{q^2} + a_{1,1}x_1^q + a_{2,1}x_1^q + \theta x_1 - \theta^{-q}y_1^{q^2} \\ x_2^{q^2} + a_{1,2}x_1^q + a_{2,2}x_2^q + \theta x_2 - \theta^{-q}y_2^{q^2} \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}.$$

Wir betrachten zur Auflösung zunächst nur den vorderen Teil Q der Blockmatrix Q:

$$Q = \begin{pmatrix} \tau^2 + a_{1,1}\tau + \theta & a_{2,1}\tau \\ a_{1,2}\tau & \tau^2 + a_{2,2}\tau + \theta \end{pmatrix} \in \mathrm{Mat}_{d\times d}(L\{\tau\}).$$

Wir tauschen die Zeilen und führen den ersten Eliminationsschritt durch, das heißt, wir multiplizieren an Q von links die Matrix

$$S_1 \cdot T_1 := \begin{pmatrix} 1 & 0 \\ -\frac{1}{a_{1,2}^q}\tau - \frac{a_{1,1}}{a_{1,2}} & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

und erhalten

$$\begin{pmatrix} a_{1,2}\tau & \tau^2 + a_{2,2}\tau + \theta \\ \theta & -\frac{1}{a_{1,2}^q}\tau^3 + \left(-\frac{a_{2,2}^q}{a_{1,2}^q} - \frac{a_{1,1}}{a_{1,2}}\right)\tau^2 + \left(-\frac{a_{1,1}a_{2,2}}{a_{1,2}} + a_{2,1}\right)\tau - \frac{a_{1,1}}{a_{1,2}} \end{pmatrix}.$$

Wir tauschen noch einmal die Zeilen und führen den zweiten Eliminationsschritt durch, indem wir von links an S_1T_1Q die folgende Matrix multiplizieren

$$S_2 \cdot T_2 := \begin{pmatrix} 1 & 0 \\ -\frac{a_{1,2}}{\theta^q}\tau & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix};$$

dies liefert das Ergebnis

$$\begin{pmatrix} \theta & -\frac{1}{a_{1,2}^{q}}\tau^3 + \left(-\frac{a_{2,2}^{q}}{a_{1,2}^{q}} - \frac{a_{1,1}}{a_{1,2}}\right)\tau^2 + \left(-\frac{a_{1,1}a_{2,2}}{a_{1,2}} + a_{2,1}\right)\tau - \frac{a_{1,1}}{a_{1,2}} \\ 0 & \frac{1}{a_{1,2}^{q^2-1}\theta^q}\tau^4 + \left(\frac{a_{2,2}^{q^2}}{a_{1,2}^{q^2-1}\theta^q} + \frac{a_{1,1}^{q}}{a_{1,2}^{q-1}\theta^q}\right)\tau^3 + \left(\frac{a_{1,1}^{q}a_{2,2}^{q}}{a_{1,2}^{q-1}\theta^q} + \frac{\theta^{q^2-q}}{a_{1,2}^{q^2-1}} - \frac{a_{1,2}a_{2,1}^{q}}{\theta^q} + 1\right)\tau^2 + \left(\frac{a_{1,1}^{q}}{a_{1,2}^{q-1}} + a_{2,2}\right)\tau + \theta \end{pmatrix}.$$

Die aufgelöste Form von Q ergibt sich nun, indem wir noch $S_2T_2S_1T_1(\theta^{-q}I_d\tau^2)$ berechnen.

Nach Vertauschung der symmetrischen Variablen $a_{1,1} \leftrightarrow a_{2,2}$ und $a_{1,2} \leftrightarrow a_{2,1}$ (was eine Auflösung nach x_1 anstatt x_2 bedeutet) und Normierung der letzten Zeile durch Multiplikation mit $a_{1,2}^{q^2-1}\theta^q$ entspricht dies dem Resultat aus [Bangert; 2011, Kapitel 4.1].

Im Fall $d = 2$ reicht eine Ausführung des Induktionsschritts aus Lemma 4.1.2 aus, um GQ in aufgelöste Form zu bringen. Wie man bereits für $d = 3$ leicht sieht, steigt mit anwachsender Dimension der q-Grad an und die Anzahl der Terme (Summen und Differenzen) in den Koeffizienten nimmt exponentiell zu, da bei jedem Schritt des Reduktionsverfahrens mehr Eliminationsmatrizen verwendet werden müssen.

Wir werden dieses Problem in Abschnitt 5 weiter diskutieren.

4.2 Anwendung des Henselschen Lemmas

Wir nutzen in diesem Abschnitt eine erweiterte Version des mehrdimensionalen Henselschen Lemmas, um zu einem fest gegebenen $y \in \overline{K}_\infty$ die Bewertung von Nullstellen der Polynomgleichung $f(x,y)$ aus Definition 3.2.2 untersuchen zu können. Wir wollen diese Methode hinsichtlich der Frage anwenden, wann eine Folge $(\underline{x_k})_k \in M[[t]]_f^\tau$ in $M\langle\langle t\rangle\rangle_f^\tau$ liegt und leiten daraus ein hinreichendes Kriterium ab, wann dies der Fall ist.

Seien $A^T \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)$ und $y \in \overline{K}_\infty^d$ fest gewählt und dazu sei $L \subseteq \overline{K}_\infty$ eine endliche algebraische Erweiterung von K_∞, so dass $A^T \in \mathrm{Mat}_{d\times d}(L)$ und $y \in L^d$ sind. Wir setzen die Bewertung v_∞ von K_∞ auf L fort.
Weiter betrachten wir zu L den Bewertungsring $\mathcal{O}_L := \{a \in L \mid v_\infty(a) \geq 0\}$ und das maximale Ideal $\mathfrak{m}_L := \{a \in L \mid v_\infty(a) > 0\}$. Wir schreiben hier in diesem Abschnitt kurz $\mathcal{O}$ und $\mathfrak{m}$, da dies eindeutig ist.

Entsprechend zur Supremumsnorm sei die Bewertung $v_\infty(x)$ für Vektoren $x \in L^d$ und die Bewertung $v_\infty(A)$ für Matrizen $A \in \mathrm{Mat}_{d\times d}(L)$ jeweils als das Minimum der Bewertungen der Einträge. Wir werden im Weiteren das folgende Lemma implizit benutzen.

4.2.1 Lemma. *Seien $A, B \in \mathrm{Mat}_{d\times d}(L)$ und $\det(A) \neq 0$, dann gilt:*

$$v_\infty(A) + v_\infty(B) \;\leq\; v_\infty(A\cdot B) \;\leq\; v_\infty(\det(A)) - (d-1)\cdot v_\infty(A) + v_\infty(B).$$

Beweis. Aus der Definition der Bewertung erhalten wir auf der einen Seite:

$$\begin{aligned} v_\infty(A\cdot B) = & \min_{1\leq i,j\leq d}\left\{v_\infty\left(\textstyle\sum_{k=1}^d a_{i,k}b_{k,j}\right)\right\} & \geq \min_{1\leq i,j\leq d}\left\{\min_{1\leq k\leq d}\{v_\infty(a_{i,k}b_{k,j})\}\right\} \\ \geq & \min_{1\leq i,j\leq d}\{v_\infty(a_{i,j})\} + \min_{1\leq k,l\leq d}\{v_\infty(b_{k,l})\} & = v_\infty(A) + v_\infty(B). \end{aligned}$$

Mit $\det(A) \neq 0$ gilt $B = A^{-1}(A\cdot B)$. Aus der obigen Abschätzung folgt dann weiter $v_\infty(B) \geq v_\infty(A^{-1}) + v_\infty(A\cdot B)$ und wir bekommen damit auf der anderen Seite:

$$\begin{aligned} v_\infty(A\cdot B) \leq & -v_\infty(A^{-1}) + v_\infty(B) & = -v_\infty\left(\det(A)^{-1}\cdot A^{ad}\right) + v_\infty(B) \\ = & \; v_\infty(\det(A)) - v_\infty(A^{ad}) + v_\infty(B) & \leq v_\infty(\det(A)) - (d-1)\cdot v_\infty(A) + v_\infty(B), \end{aligned}$$

dabei ist A^{ad} die Adjunkte zu A, für die $v_\infty(A^{ad}) \geq (d-1)\cdot v_\infty(A)$ gilt. $\square$

Wir wollen nun das Henselsche Lemma (Satz 1.2.8) im Hinblick auf Problem 3.2.3 anwenden, wann sich eine Folge $\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_k \in L^d$ mit $f(\underline{x}_i, \underline{x}_{i-1})$ für $k \geq i \geq 0$ zu einem Element $\underline{x} \in M\langle\langle t\rangle\rangle_f^\tau$ fortsetzen lässt. Dabei wollen wir ausnutzen, dass die Lösungen, die Satz 1.2.8 liefert, bereits im Grundkörper L enthalten sind.

Sowohl die Koeffizienten von $f(x) := f(x, y) \in L[x]$, bei festem $y \in L$, als auch die Nullstellen werden jedoch im Allgemeinen nicht in $\mathcal{O}$ liegen (wodurch sie sich mit Satz 1.2.8 nicht finden lassen). Daher betrachten wir das folgende transformierte Polynom:

$$\widetilde{f}(\widetilde{x}) := \lambda^{q^2} \cdot f\left(\lambda^{-1}\widetilde{x}\right) = \widetilde{x}^{(2)} + A^T \lambda^{q^2-q}\widetilde{x}^{(1)} + \theta\lambda^{q^2-1}\widetilde{x} - \theta^{-q}\lambda^{q^2} y^{(2)},$$

wobei $A^T \in \mathrm{Mat}_{d\times d}(L)$ und $y \in L^d$, wie beschrieben, fest vorgegeben sind.

4.2.2 Lemma. *Sei* $\lambda \in \mathcal{O}$ *mit* $v_\infty(\lambda) \geq \max\left\{\frac{-v_\infty(A)}{q^2-q}, \frac{1}{q^2-1}, -\frac{1}{q} - v_\infty(y)\right\}$, *dann ist* $\widetilde{f}(\widetilde{x}) \in \mathcal{O}^d[\widetilde{x}]$ *und es gilt:* $f(\lambda^{-1}\widetilde{x}) = 0 \iff \widetilde{f}(\widetilde{x}) = 0$.

Beweis. Dies folgt direkt aus der Definition von $\widetilde{f}(\widetilde{x})$. □

Die Voraussetzungen von Satz 1.2.8 sind für $\widetilde{f}$ erfüllt, falls für ein $a \in \mathcal{O}$ gilt:

$$v_\infty(\widetilde{f}(a)) > v_\infty(J_{\widetilde{f}}(a)^2).$$

Als approximierte Lösung von $\widetilde{f}(\widetilde{x})$ wollen wir $a = 0 \in \mathcal{O}^d$ verwenden, damit liefert die Bedingung $v_\infty(\widetilde{f}(0)) = v_\infty(\theta^{-q}\lambda^{q^2} y^{q^2}) > v_\infty(J_{\widetilde{f}}(0)^2) = 2v_\infty(\theta\lambda^{q^2-1})$ eine obere Schranke für $v_\infty(\lambda)$. Um ein geeignetes λ zwischen dieser und der Schranke aus Lemma 4.2.2 wählen können, muss der Abstand zwischen ihnen größer als $\min\{v_\infty(m) \mid m \in \mathfrak{m}\}$ sein.

Diese Kriterien zusammen führen uns zu dem folgenden Resultat:

4.2.3 Satz. *Es sei* $\varepsilon \geq \min\{v_\infty(m) \mid m \in \mathfrak{m}\}$ *und für* $A \in \mathrm{Mat}_{d\times d}(L)$, $y \in L^d$ *gelte:*

$$v_\infty(y) > \max\left\{-\frac{q^2-2}{q^4-q^3} \cdot v_\infty(A) - \frac{q+2}{q^2}, \quad \frac{-q^2-q+1}{q^3-q}\right\} + \frac{q^2-2}{q^2} \cdot \varepsilon,$$

dann existiert ein eindeutig bestimmtes $\xi = (\xi_1, \ldots, \xi_d)^T \in L^d$ *mit*

$$f(\xi) = 0 \quad \textit{und} \quad v_\infty(\xi) \geq 1 + q + q^2 v_\infty(y) > v_\infty(y) + \frac{1}{q}.$$

Beweis. Aus den Voraussetzungen folgern wir:

$$\begin{array}{lll}
1. \quad v_\infty(y) & > & -\frac{q^2-2}{q^4-q^3}\cdot v_\infty(A) - \frac{q+2}{q^2} + \frac{q^2-2}{q^2}\cdot\varepsilon \\
& \Longrightarrow & \frac{-v_\infty(A)}{q^2-q} + \varepsilon \quad < \quad \frac{q^2}{q^2-2}\cdot v_\infty(y) + \frac{q+2}{q^2-2}, \\
2. \quad v_\infty(y) & > & \frac{-q^2-q+1}{q^3-q} + \frac{q^2-2}{q^2}\cdot\varepsilon \quad = \quad \frac{q^2-2}{q^2}\left(\frac{1}{q^2-1} - \frac{q+2}{q^2-2} + \varepsilon\right) \\
& \Longrightarrow & \frac{1}{q^2-1} + \varepsilon \quad < \quad \frac{q^2}{q^2-2}\cdot v_\infty(y) + \frac{q+2}{q^2-2}, \\
3. \quad v_\infty(y) & > & \frac{-q^2-q+1}{q^3-q} + \frac{q^2-2}{q^2}\cdot\varepsilon \quad > \quad \frac{q^2-2}{2(q^2-1)}\cdot\frac{-2q^2-2q+2}{q(q^2-2)} + \frac{q^2-2}{2(q^2-1)}\cdot\varepsilon \\
& \Longrightarrow & \left(\frac{q^2}{q^2-2}+1\right)v_\infty(y) \quad > \quad \frac{-2q^2-2q+2}{q(q^2-2)} + \varepsilon \quad = \quad -\frac{1}{q} - \frac{q+2}{q^2-2} + \varepsilon \\
& \Longrightarrow & -\frac{1}{q} - v_\infty(y) + \varepsilon \quad < \quad \frac{q^2}{q^2-2}\cdot v_\infty(y) + \frac{q+2}{q^2-2}.
\end{array}$$

Das heißt, es gilt die folgende Ungleichung:

$$\max\left\{\frac{-v_\infty(A)}{q^2-q},\quad \frac{1}{q^2-1},\ -\frac{1}{q} - v_\infty(y)\right\} + \varepsilon \ < \ \frac{q^2}{q^2-2}v_\infty(y) + \frac{q+2}{q^2-2}.$$

Wegen $\varepsilon \geq \min\{v_\infty(a) \mid a \in \mathfrak{m}\}$ existiert demnach ein $\lambda \in \mathcal{O}$, so dass gilt:

$$\max\left\{\frac{-v_\infty(A)}{q^2-q},\quad \frac{1}{q^2-1},\quad -\frac{1}{q} - v_\infty(y)\right\} \ \leq v_\infty(\lambda) < \ \frac{q^2}{q^2-2}\cdot v_\infty(y) + \frac{q+2}{q^2-2}.$$

Es sei $\widetilde{\varepsilon} := \frac{q^2}{q^2-2}\cdot v_\infty(y) + \frac{q+2}{q^2-2} - v_\infty(\lambda)$. Wir betrachten das transformierte Polynom

$$\widetilde{f}(\widetilde{x}) := \lambda^{q^2}\cdot f\left(\lambda^{-1}\widetilde{x}\right) = \widetilde{x}^{(2)} + A^T\lambda^{q^2-q}\widetilde{x}^{(1)} + \theta\lambda^{q^2-1}\widetilde{x} - \theta^{-q}\lambda^{q^2}y^{(2)}.$$

Nach Wahl von λ ist $\widetilde{f}(\widetilde{x}) \in \mathcal{O}^d[\widetilde{x}]$ und die Ableitung von $\widetilde{f}$ ist unabhängig von der Stelle $\widetilde{x}$. Wir schreiben daher $J_{\widetilde{f}} := J_{\widetilde{f}}(\widetilde{x}) = \theta\lambda^{q^2-1}\cdot I_d$. Es folgt die Äquivalenz:

$$\begin{aligned}
v_\infty(\lambda) < \frac{q^2}{q^2-2}\cdot v_\infty(y) + \frac{q+2}{q^2-2} \quad &\Longleftrightarrow \quad -(q^2-2)v_\infty(\lambda) > -q-2-q^2v_\infty(y) \\
&\Longleftrightarrow \quad q + q^2v_\infty(\lambda) + q^2v_\infty(y) > 2(-1+(q^2-1)v_\infty(\lambda)) \\
&\Longleftrightarrow \quad v_\infty(\theta^{-q}\lambda^{q^2}y^{q^2}) > 2v_\infty(J_{\widetilde{f}}).
\end{aligned}$$

Für die approximierte Lösung $a = 0 \in \mathcal{O}^d$ erhalten wir also die Ungleichung

$$v_\infty(\widetilde{f}(0)) = v_\infty(\theta^{-q}\lambda^{q^2}y^{q^2}) > 2v_\infty(J_{\widetilde{f}}).$$

Somit sind die Voraussetzungen des verallgemeinerten Henselschen Lemmas (Satz 1.2.8) für $\widetilde{f}(\widetilde{\xi})$ und $a = 0$ erfüllt und es gibt ein eindeutig bestimmtes $\widetilde{\xi} \in \mathcal{O}^d$, für das gilt:

$$\widetilde{f}(\widetilde{\xi}) = 0 \quad \text{und} \quad v_\infty(\widetilde{\xi}) = v_\infty(\widetilde{\xi} - 0) > v_\infty(J_{\widetilde{f}}).$$

Entsprechend ist $\xi := \lambda^{-1}\widetilde{\xi}$ die gesuchte Lösung mit $f(\xi) = 0$ und wir sehen:

$$\begin{aligned} v_\infty(\xi) &= v_\infty(\widetilde{\xi}) - v_\infty(\lambda) > v_\infty(J_{\widetilde{f}}) - v_\infty(\lambda) = -1 + (q^2-2)v_\infty(\lambda) \\ &= -1 + (q^2-2)\left(\frac{q^2}{q^2-2}\cdot v_\infty(y) + \frac{q+2}{q^2-2} - \widetilde{\varepsilon}\right) = 1 + q + q^2 v_\infty(y) - (q^2-2)\widetilde{\varepsilon}. \end{aligned}$$

Durch geeignete Wahl von λ können wir annehmen, dass $\widetilde{\varepsilon} \in L$ möglichst klein ist; somit gilt $v_\infty(\xi) \geq 1 + q + q^2 v_\infty(y)$. Aus der Voraussetzung folgern wir zudem:

$$v_\infty(y) > \frac{-q^2-q+1}{q^3-q} = \frac{-q^2-q}{q^3-q} + \frac{1}{q^3-q} \implies (q^2-1)v_\infty(y) > -(1+q) + \frac{1}{q}.$$

Dies bedeutet schließlich, dass stets $v_\infty(\xi) \geq 1 + q + q^2 v_\infty(y) > v_\infty(y) + \frac{1}{q}$ ist. □

Falls wir Satz 4.2.3 anwenden können, ist die Nullstelle von $f(x)$, die das Henselsche Lemma liefert, stets im Grundkörper L enthalten. Wir stellen somit fest:

4.2.4 Folgerung. *Seien* $\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_k \in L^d$ *mit* $f(\underline{x}_i, \underline{x}_{i-1}) = 0$ *für* $k \geq i \geq 0$ *und für* $\underline{x}_k$ *seien die Voraussetzungen von Satz* 4.2.3 *erfüllt, dann gibt es eine Fortsetzung zu einer Folge* $(\underline{x}_k)_k \in M\langle\langle t\rangle\rangle_f^\tau$.

Beweis. Wenn $\underline{x}_i = y \in L^d$ die Voraussetzungen von Satz erfüllt 4.2.3, dann erfüllt die Lösung $\underline{x}_{i+1} = \xi$ diese ebenfalls. Wir können also den Satz wiederholt anwenden, wobei insbesondere $\{\underline{x}_k\} \subset L^d$ und $\lim\limits_{k\to\infty} v_\infty(\underline{x}_k) = \infty$ gelten. □

4.3 Rekursive Polynomgleichungen

In diesem Abschnitt betrachten wir den $\mathbb{F}_q[[t]]$-Modul $M[[t]]_f^\tau$. Wir beschreiben eine Familie von rekursiv definierten Funktionen einführen, deren Nullstellen gerade eine Folge $(\underline{x}_k)_k \in M[[t]]_f^\tau$ bilden.

Sei $\underline{x} \in M[[t]]_f^\tau$, das heißt, es ist $\underline{x} \in (\overline{K}_\infty^d)^{\mathbb{N}_0}$ und für alle $k \in \mathbb{N}_0$ mit $\underline{x}_{k-1} := 0$ gilt:

$$f(\underline{x}_k, \underline{x}_{k-1}) = \left[\underline{x}_k^{(2)} + A^T \underline{x}_k^{(1)} + \theta \underline{x}_k^{(0)}\right] - \theta^{-q} \underline{x}_{k-1}^{(2)} = 0.$$

Wir stellen die Gleichung nach $\underline{x}_{k-1}$ um und erhalten für $i \geq 0$ durch Potenzieren der Koeffizienten mit q^i die Identitäten

$$\underline{x}_{k-1}^{(i+2)} = \theta^{q^{i+1}} \left[\underline{x}_k^{(i+2)} + (A^T)^{(i)} \underline{x}_k^{(i+1)} + \theta^{q^i} \underline{x}_k^{(i)}\right] = \left(\theta^q \cdot f(\underline{x}_k, 0)\right)^{(i)}.$$

Betrachten wir zunächst $k = 1$. Mit $f(\underline{x}_1, \underline{x}_0) = 0$ ist auch $(f(\underline{x}_1, \underline{x}_0))^{(2)} = 0$. In diese Gleichung können wir die Identitäten für $\underline{x}_1^{(i+2)}$ einsetzen und bekommen dann

$$\begin{aligned}
(f(\underline{x}_1, \underline{x}_0))^{(2)} &= \theta^{q^3} \left[\underline{x}_2^{(4)} + (A^T)^{(2)} \underline{x}_2^{(3)} + \theta^{q^2} \underline{x}_2^{(2)}\right] + (A^T)^{(2)} \theta^{q^2} \left[\underline{x}_2^{(3)} + (A^T)^{(1)} \underline{x}_2^{(2)} + \theta^q \underline{x}_2^{(1)}\right] \\
&\quad + \theta^{q^2+q} \left[\underline{x}_2^{(2)} + A^T \underline{x}_2^{(1)} + \theta \underline{x}_2\right] - \theta^{-q^3} \underline{x}_0^{(4)} \\
&= \theta^{q^3} \underline{x}_2^{(4)} + \left((A^T)^{(2)} \theta^{q^3} + (A^T)^{(2)} \theta^{q^2}\right) \underline{x}_2^{(3)} \\
&\quad + \left(\theta^{q^3+q^2} + (A^T)^{(2)} (A^T)^{(1)} \theta^{q^2} + \theta^{q^2+q}\right) \underline{x}_2^{(2)} \\
&\quad + \left((A^T)^{(2)} \theta^{q^2+q} + A^T \theta^{q^2+q}\right) \underline{x}_2^{(1)} + \theta^{q^2+q+1} \underline{x}_2 - \theta^{-q^3} \underline{x}_0^{(4)} = 0.
\end{aligned}$$

Dies ist ein q-Polynom in zwei Variablen vom q-Grad 4, was wir nach Normierung von $\underline{x}_2^{(4)}$ als $f_{(2)}(x, y)$ in den Unbestimmten x und y bezeichnen. Insbesondere hat dieses Polynom die Nullstelle $(x, y) = (\underline{x}_2, \underline{x}_0^{(2)})$.

Wir setzen $f_{(1)}(x, y) := f(x, y)$ und führen dieses Vorgehen iterativ fort, um $f_{(k)}(x, y)$ für $k > 2$ zu definieren. Dazu potenzieren wir die Koeffizienten des Polynoms $f_{(2)}(x, y)$ wieder mit q^2, setzen dann die obigen Identitäten für $\underline{x}_k^{(i+2)}$ ein und normieren abschließend den höchsten vorkommenden Term von $\underline{x}_k$.

Wir erhalten so die folgende Familie von q-Polynomen, die wir die Folge der iterierten Polynome $(f_{(1)}(x,y), f_{(1)}(x,y), \ldots)$ nennen wollen:

4.3.1 Definition. *Für $k \geq 1$ sei:*

$$f_{(k)}(x,y) = \left[\theta^{-q^{2k-1}} \sum_{i=0}^{2k} a_{(k),i} x^{(i)}\right] - \theta^{-kq^{2k-1}} y^{(2k)} \in \overline{K}_\infty^d[x,y]$$

mit den Koeffizienten $a_{(1),0} := \theta$, $a_{(1),1} := A^T$, $a_{(1),2} := 1$ und für $k > 1$:

$$a_{(k),i} := \begin{cases} \sum_{j=0}^{2} \theta^{q^{1+i-j}} (a_{(k-1),i-j})^{(2)} \cdot (a_{(1),j})^{(i-j)} & \text{für } 0 \leq i \leq 2k \\ 0 & \text{sonst} \end{cases}$$

4.3.2 Bemerkung. *Nach Konstruktion ist $f_{(k)}(x,y)$ vom q-Grad $2k$ in x und in y und hat die Nullstelle $(x,y) = (\underline{x}_k, \underline{x}_0^{(2(k-1))})$.*
Für den Koeffizient von $x^{(2k)}$ gilt $a_{(2k),k} = 1$, da dieser in der Konstruktion normiert wird. Das Monom $\theta^{-kq^{2k-1}} y^{(2k)}$ entsteht dadurch, dass nach dem Einsetzen der Identitäten gilt:

$$(f(\underline{x}_k, \underline{x}_0))^{(2)} = \theta^{q^{2k-1}} \underline{x}_k^{(2k)} + \ldots - (\theta^{(k-1)q^{2(k-1)-1}} \underline{x}_0^{(2(k-1))})^{(2)},$$

wobei durch das Normieren mit $\theta^{-q^{2k-1}}$ zusammen mit dem Koeffizienten $(\theta^{(k-1)q^{2(k-1)-1}})^{q^2}$ aus dem vorherigen Schritt gerade $\theta^{-kq^{2k-1}}$ als Koeffizient vor $y^{(2k)}$ steht.

Aus der Definition der q-Polynome $f_{(k)}(x,y)$ folgt für $k > 1$ die Gleichheit:

$$f_{(k+1)}(x,y) = \left(f_{(k)}\left((f_{(1)}(x,0))^{(-2)}, 0\right)\right)^{(2)} - \theta^{-kq^{2k-1}} y^{(2(k+1))}, \tag{4.1}$$

wobei wir mit $x = (f_{(1)}(x,0))^{(-i)}$ die eindeutig bestimmte Lösung der Gleichung $x^{(i)} = (f_{(1)}(x,0))$ für $i \geq 0$ bezeichnen.

4.3.3 Lemma. *Sei $\underline{x} \in (\overline{K}_\infty^d)^{\mathbb{N}_0}$ mit $f(\underline{x}_0, 0) = 0$, dann gilt:*

$$\underline{x} \in M[[t]]_f^\tau \iff f_{(k)}(\underline{x}_k, \underline{x}_0) = 0 \text{ für alle } k \geq 1.$$

Beweis. Sei $\underline{x} \in M[[t]]_f^\tau$, dann ist $f(\underline{x}_k, \underline{x}_{k-1}) = f_{(1)}(\underline{x}_k, \underline{x}_{k-1}) = 0$ für alle $k \in \mathbb{N}_0$. Dies bedeutet gerade, dass für $i \geq 0$ die folgenden Identitäten gelten:

$$\underline{x}_{k-1}^{(i+2)} = \big(f_{(1)}(\underline{x}_k, 0)\big)^{(i)} = \sum_{j=0}^{2} (a_{(1),j})^{(i)}\, \underline{x}_k^{(i+j)}, \tag{4.2}$$

Nach Voraussetzung ist $(f_{(1)}(\underline{x}_1, \underline{x}_0))^{(2)} = 0$. Wir nutzen damit beginnend induktiv für $k \geq 1$ die Gleichheit (4.1) und sehen, dass $f_{(k+1)}(\underline{x}_{k+1}, \underline{x}_0) = (f_{(k)}(\underline{x}_k, \underline{x}_0))^{(2)} = 0$ gilt.

Sei umgekehrt $f_{(k)}(\underline{x}_k, \underline{x}_0) = 0$ für alle $k \geq 1$, dann bekommen wir daraus direkt die Gleichheit $f_{(k+1)}(\underline{x}_{k+1}, \underline{x}_0) = (f_{(k)}(\underline{x}_k, \underline{x}_0))^{(2)} = 0$. Nach Konstruktion gilt somit:

$$\begin{aligned} 0 &= (f_{(k)}(\underline{x}_k, \underline{x}_0))^{(2)} = \left[\sum_{i=0}^{2k} (a_{(k-1),i})^{(2)} \underline{x}_k^{(i+2)}\right] - \theta^{-kq^{2k-1}} \underline{x}_0^{(2(k+1))} \qquad \text{und} \\ 0 &= f_{(k+1)}(\underline{x}_{k+1}, \underline{x}_0) = \left[\sum_{i=0}^{2(k+1)} \sum_{j=0}^{2} (a_{(k-1),i-j})^{(2)} \cdot (a_{(0),j})^{(i)} \underline{x}_{k+1}^{(i)}\right] - \theta^{-kq^{2k-1}} \underline{x}_0^{(2(k+1))}. \end{aligned}$$

Entsprechend erhalten wir aus der Gleichung (4.1), dass die Identitäten (4.2) gelten. Folglich ist $(f(\underline{x}_{k+1}, \underline{x}_k))^{(2)} = 0$ für alle $k \in \mathbb{N}_0$ und damit auch $f(\underline{x}_{k+1}, \underline{x}_k) = 0$. $\square$

Wir können also die Familie $(f_{(k)}(x, y))_{k \geq 1}$ anstelle einer wiederholten Anwendung von $f(x, y)$ verwenden, um Fortsetzungen in $M[[t]]_f^\tau$ zu finden. $f_{(k)}(x, y)$ hat lediglich q-Grad $2k$ und demnach q^{2kd} Nullstellen in $\overline{K}_\infty$, während $f(x, y)$ dagegen q-Grad 2 und somit q^{2d} Nullstellen in $\overline{K}_\infty$ hat.

Die zusätzlichen Nullstellen von $f_{(k)}(x, y)$ sind alle möglichen Fortsetzungen in $M[[t]]^\tau$, die zu einer gegebenen Startlösung $\underline{x}_0$ möglich sind. Dies sehen wir wie folgt:

4.3.4 Lemma. *Sei $\underline{x} \in M[[t]]_f^\tau$, dann gilt für alle i, k mit $1 \leq i \leq k$:*

$$f_{(k)}(\underline{x_i}, \underline{x_0}) = 0.$$

Beweis. Es ist $f(\underline{x}_k, \underline{x}_{k-1}) = 0$ für alle $k \in \mathbb{N}_0$ und $f_{(k)}(\underline{x}_k, \underline{x_0}) = 0$ für alle $k \geq 1$. Mit Gleichung (4.1) erhalten wir, dass auch $f_{(k)}(\underline{x_i}, \underline{x_0}) = 0$ für $1 \leq i \leq k$ gilt. $\square$

4.4 Zusammensetzungen von Polynomgleichungen

In diesem Abschnitt geben wir eine Möglichkeit an, wie wir zu einem fest gegebenen $y \in \overline{K}_\infty^d$ die Polynomgleichung $f(x) := f(x,y) = 0$ vom q-Grad 2 aus zwei zueinander ähnlichen Polynomgleichungen vom q-Grad 1 zusammensetzen können.
Im Anschluss daran bestimmen wir in beliebiger Dimension $d \geq 2$ Kriterien, die für die Existenz von Lösungen x dieser Teilprobleme mit $v_\infty(x) \geq v_\infty(y) + \frac{1}{q}$ hinreichend sind.

Seien $A^T \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)$ und $y \in \overline{K}_\infty^d$ fest gewählt und weiter sei $L \subseteq \overline{K}_\infty$ eine endliche algebraische Erweiterung von L mit $A^T \in \mathrm{Mat}_{d\times d}(L)$ und $y \in L^d$.

4.4.1 Problem. *Wir betrachten in Dimension $d \geq 1$ die $\mathbb{F}_q$-lineare Polynomgleichung*

$$f(x) := f(x,y) = x^{(2)} + A^T x^{(1)} + \theta x - \theta^{-q} y^{(2)} = 0, \tag{4.3}$$

wobei wir eine Lösung $x \in \widetilde{L}^d$ in einer endlichen algebraischen Erweiterung $\widetilde{L} \subset \overline{K}_\infty$ von L suchen, so dass $v_\infty(x) \geq v_\infty(y) + c$ mit $c > 0$ gilt.

Nach Bemerkung 3.2.4 wissen wir, dass in Dimension $d = 1$ zu gegebenen $y \in L^d$ stets eine Lösung x in einer endlichen Körpererweiterung von $\overline{K}_\infty$ existiert, so dass $v_\infty(x) \geq v_\infty(y) + \frac{1}{q}$ gilt und mit dem Henselschen Lemma (Satz 1.2.8) erhalten wir unter bestimmten Voraussetzungen auch in höheren Dimensionen $d \geq 1$ eine Lösung x, für die der Bewertungsanstieg $v_\infty(x) \geq v_\infty(y) + \frac{1}{q}$ ebenfalls gilt.

Wir vermuten daher, dass, falls eine entsprechende Lösung existiert, der Zuwachs der Bewertung auch in Dimension $d \geq 2$ mindestens $c := \frac{1}{q}$ ist. (Vergleiche die Diskussion zu Problem 3.2.3.)

Wegen $v_\infty(\theta^{-\frac{1}{q}}) = \frac{1}{q}$ wählen wir in diesem Fall Variablen $\lambda_1, \dots \lambda_d \in \overline{K}_\infty$, so dass gilt:

$$x = \theta^{-\frac{1}{q}} \Lambda y \quad \text{mit } \Lambda = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_d \end{pmatrix}, v_\infty(\Lambda) \geq 0.$$

Weiter setzen wir voraus, dass y keine Nulleinträge hat. (Sonst verschwindet auch für die entsprechende Komponente von x.) Dann lässt sich mit dieser Substitution Gleichung

(4.3) umformen zu:

$$
\begin{aligned}
& \theta^{-q}\Lambda^{q^2}y^{(2)} + A^T(\theta^{-1}\Lambda^q y^{(1)}) + \theta^{1-\frac{1}{q}}\Lambda = \theta^{-q}y^{(2)} \\
\iff\ & \theta^{-q}\begin{pmatrix} \lambda_1^{q^2}y_1^{q^2} \\ \vdots \\ \lambda_j^{q^2}y_d^{q^2} \end{pmatrix} + \theta^{-1}\begin{pmatrix} \sum_{j=1}^d a_{j,1}\lambda_j^q y_j^q \\ \vdots \\ \sum_{j=1}^d a_{j,n}\lambda_j^q y_j^q \end{pmatrix} + \theta^{1-\frac{1}{q}}\begin{pmatrix} \lambda_1 y_1 \\ \vdots \\ \lambda_d y_d \end{pmatrix} = \theta^{-q}\begin{pmatrix} y_1^{q^2} \\ \vdots \\ y_d^{q^2} \end{pmatrix} \\
\iff\ & \begin{pmatrix} \lambda_1^{q^2} \\ \vdots \\ \lambda_d^{q^2} \end{pmatrix} + \theta^{q-1}\begin{pmatrix} \sum_{j=1}^d a_{j,1}\frac{y_j^q}{y_1^{q^2}}\lambda_j^q \\ \vdots \\ \sum_{j=1}^d a_{j,n}\frac{y_j^q}{y_d^{q^2}}\lambda_j^q \end{pmatrix} + \theta^{q+1-\frac{1}{q}}\begin{pmatrix} \lambda_1 y_1^{1-q^2} \\ \vdots \\ \lambda_d y_d^{1-q^2} \end{pmatrix} = \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix},
\end{aligned}
$$

wobei wir definieren:

$$
B := \theta^{q-1}\begin{pmatrix} a_{1,1}\cdot\frac{y_1^q}{y_1^{q^2}} & \dots & a_{n,1}\cdot\frac{y_d^q}{y_1^{q^2}} \\ \vdots & & \vdots \\ a_{1,n}\cdot\frac{y_1^q}{y_d^{q^2}} & \dots & a_{n,n}\cdot\frac{y_d^q}{y_d^{q^2}} \end{pmatrix} = \theta^{q-1}\begin{pmatrix} y_1^{-q^2} & & 0 \\ & \ddots & \\ 0 & & y_d^{-q^2} \end{pmatrix}\cdot A^T\cdot\begin{pmatrix} y_1^q & & 0 \\ & \ddots & \\ 0 & & y_d^q \end{pmatrix},
$$

$$
C := \theta^{q+1-\frac{1}{q}}\begin{pmatrix} y_1^{1-q^2} & & 0 \\ & \ddots & \\ 0 & & y_d^{1-q^2} \end{pmatrix}, \quad \lambda := \begin{pmatrix} \lambda_1 \\ \vdots \\ \lambda_d \end{pmatrix} \quad \text{und} \quad \mathbb{1} := \begin{pmatrix} 1 \\ \vdots \\ 1 \end{pmatrix}.
$$

Damit ist das Ausgangsproblem 4.4.1 für $c = \frac{1}{q}$ äquivalent zu:

4.4.2 Problem. *Wir betrachten zu gegebenen $B, C \in \mathrm{Mat}_{d\times d}(L)$ die Polynomgleichung*

$$
\lambda^{(2)} + B\lambda^{(1)} + C\lambda = \mathbb{1}, \tag{4.4}
$$

wobei wir eine Lösung $\lambda \in \widetilde{L}^d$ mit $v_\infty(\lambda) \geq 0$ in einer endlichen algebraischen Erweiterung $\widetilde{L} \subset \overline{K}_\infty$ von L suchen.

Wir werden nun zeigen, dass sich die Polynomgleichung 4.4 vom Grad q^2 durch zwei zueinander ähnliche Polynomgleichungen vom Grad q zusammensetzen lässt.
Dazu bestimmen wir zwei Matrizen M_1 und $M_2 \in \mathrm{Mat}_{d\times d}(\overline{K}_\infty)$, so dass für diese gilt:

$$
M_1^{(1)} + M_2 = -B, \qquad M_2 \cdot M_1 = C, \tag{4.5}
$$

wobei wir weiter voraussetzen, dass M_1 und M_2 invertierbar sind. (Was gegeben ist, wenn y keine Nulleinträge hat.)

Es gibt eine endliche algebraische Erweiterung von L, so dass die Koeffizienten von M_1, M_2 und ihrer Inversen in dieser enthalten sind. Wir nehmen an dieser Stelle an, dass L diese Erweiterung bereits selbst ist. Folglich ist Gleichung (4.4) äquivalent zu

$$(\lambda^{(1)} - M_1\lambda)^{(1)} - M_2(\lambda^{(1)} - M_1\lambda) \;=\; \mathbb{1}. \tag{4.6}$$

Die Lösbarkeit von Problem 4.4.2 ist somit hinreichend erfüllt, wenn wir zwei entsprechende Probleme der folgenden Form (für M_1 und M_2) lösen können:

4.4.3 Problem. *Zu $M \in \mathrm{GL}_d(L)$ und $a \in L^d$ mit $v_\infty(a) \geq 0$ betrachten wir*

$$z^{(1)} - Mz = a, \tag{4.7}$$

wobei wir eine Lösung $z \in \widetilde{L}^d$ mit $v_\infty(z) \geq 0$ in einer endlichen algebraischen Erweiterung $\widetilde{L} \subset \overline{K}_\infty$ von L suchen.

Hinsichtlich der Zusammensetzung des Ausgangsproblems 4.4.2 sehen wir, dass es möglich ist, die beiden entsprechenden Teilprobleme ein wenig zu modifizieren:

4.4.4 Bemerkung. *Für das zusammengesetzte Problem 4.4.2 suchen wir insgesamt eine Lösung λ mit $v_\infty(\lambda) \geq 0$, dafür ist die Bedingung $v_\infty(z) \geq 0$ für das "äußere Teilproblem" (4.4.3 mit $M = M_2$) nicht notwendig. Falls wir die Bedingung $v_\infty(z) \geq 0$ für das "äußere Teilproblem" fallen lassen, können wir jedoch für das zugehörige "innere Teilproblem" (4.4.3 mit $M = M_1$) nicht mehr $v_\infty(a) \geq 0$ annehmen.*

Wir wollen auf die Übereinstimmung der Teilprobleme jedoch vorerst nicht verzichten und setzen an dieser Stelle stets $v_\infty(a) \geq 0$ voraus. Wir sehen direkt:

4.4.5 Bemerkung.

a) *Falls $v_\infty(M) \geq 0$ gilt, ist $z^{(1)} - Mz = a$ eine Ganzheitsgleichung. Demnach gilt auch $v_\infty(z) \geq 0$ für jede Lösung $z \in \widetilde{L}^d$, wobei $\widetilde{L} \subset \overline{K}_\infty$ eine geeignete endliche algebraische Erweiterung von L ist.*

b) Falls $v_\infty(M^{-1}) > 0$ und $v_\infty(a) \geq 0$ gilt, substituieren wir $z = M^{-1}\widetilde{z}$ und erhalten aus $z^{(1)} - Mz = a$:

$$\widetilde{f}(\widetilde{z}) = M^{(-1)}\widetilde{z}^{(1)} + \widetilde{z} - a.$$

Die Jacobi-Matrix von $\widetilde{f}$ an der Stelle $a \in \mathcal{O}_L^d$ ist dann $J_{\widetilde{f}}(a) = I_d$ und es gilt:

$$v_\infty(\widetilde{f}(a)) - v_\infty(J_{\widetilde{f}}(a)^2) = v_\infty(\widetilde{f}(a)) = v_\infty(M^{(-1)}a^{(1)}) > 0,$$

nach dem Henselschen Lemma (Satz 1.2.8) existiert somit eine Lösung $\widetilde{\xi}$ in $\mathcal{O}^d$ mit $v_\infty(\widetilde{\xi} - a) > v_\infty(J_{\widetilde{f}}(a)) = 0$, woraus $v_\infty(\xi) > 0$ folgt und wir die Lösung $\xi := M^{-1}\widetilde{\xi}$ mit $v_\infty(\xi) > 0$ erhalten.

Im Weiteren werden wir die Bedingungen für die Lösbarkeit von Problem 4.4.3 genauer untersuchen. Wir wollen dazu Gleichung 4.7 durch eine Transformation so abändern, dass sie die Form $\widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a}$ hat. In diesem Fall können wir die Gleichungen in den einzelnen Komponenten getrennt betrachten, was die Untersuchung der Bewertungen der Lösungen erheblich erleichtert.

Wir verwenden dazu einen Spezialfall des Satzes von Lang und Steinberg.

4.4.6 Satz. *Die Abbildung $\mathrm{GL}_d(\overline{K}_\infty) \to \mathrm{GL}_d(\overline{K}_\infty),\ E \mapsto E^{-1}E^{(1)}$ ist surjektiv.*

Beweis. Siehe [Steinberg; 1968]. □

Die Abbildung $E^T \mapsto E^{(1)}E^{-1}$ ist damit ebenfalls surjektiv und wir stellen fest:

4.4.7 Bemerkung. *Sei $M \in \mathrm{GL}_d(L)$, dann gibt es nach Satz 4.4.6 eine invertierbare Matrix $E \in \mathrm{GL}_n(\overline{K}_\infty))$, so dass gilt:*

$$M = E^{(1)}E^{-1}. \tag{4.8}$$

Wir nennen E und E^{-1} in diesem Fall Lang-Steinberg-Matrizen zu M.

Wir bemerken, dass die Matrix E über $\overline{K}_\infty$ durch die Relation

$$M = E^{(1)}E^{-1} \Longleftrightarrow E^{(1)} - ME = 0$$

nicht eindeutig bestimmt ist. Wir gehen an dieser Stelle davon aus, dass wir Lang-Steinberg-Matrizen E und E^{-1} zu M fest gewählt haben. Dann gibt es eine endliche algebraische Erweiterung von L, so dass die Koeffizienten von E und E^{-1} in dieser enthalten sind. Wir nehmen wieder an, dass dies für den Körper L selbst gilt.

Wir werden im Weiteren sehen, dass die Bewertungen der Lösung von Problem 4.5.2 nicht von der konkreten Wahl von E abhängen.

Mit einer Lang-Steinberg-Matrix E zu M können wir Gleichung 4.7 nun umformen, indem wir die Variablentransformation $\widetilde{z} := E^{-1}z$ durchführen. Es gilt mit $M = E^{(1)}E^{-1}$:

$$\begin{aligned} z^{(1)} - Mz = a &\iff z^{(1)} - E^{(1)}E^{-1}z = a \\ &\iff E^{(1)}\widetilde{z}^{(1)} - E^{(1)}E^{-1}E\,\widetilde{z} = a \\ &\iff \widetilde{z}^{(1)} - \widetilde{z} = (E^{(1)})^{-1}a. \end{aligned}$$

Wir definieren $\widetilde{a} := (E^{(1)})^{-1}a$, also ist Gleichung 4.7 äquivalent zu

$$\widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a}; \quad z = E\,\widetilde{z}. \tag{4.9}$$

Wir können an dieser Stelle die Gleichungen in den einzelnen Komponenten unabhängig betrachten. Unser Ziel ist es dabei, durch die Bedingung $v_\infty(z) \geq v_\infty(E) + v_\infty(\widetilde{z}) \geq 0$ geeignete Kriterien an M und a für die Lösbarkeit von Problem 4.4.3 zu finden.

Wir betrachten nun Gleichung (4.9) für $i = 1, \ldots, d$ komponentenweise. Wir unterscheiden dabei die Fälle $v_\infty(\widetilde{a}_i) \leq 0$ und $v_\infty(\widetilde{a}_i) > 0$ und sehen, dass wir Lösungen für $\widetilde{z}$ im Fall $v_\infty(\widetilde{a}_i) \leq 0$ näherungsweise und im Fall $v_\infty(\widetilde{a}_i) > 0$ sogar exakt angeben können.

4.4.8 Bemerkung. *Sei $z \in \overline{K}_\infty$ gegeben, so dass $\widetilde{z}_i^q - \widetilde{z}_i = \widetilde{a}_i$ gilt.*

a) Falls $v_\infty(\widetilde{a}_i) \leq 0$ ist, definieren wir für ein unbestimmtes $k \in \mathbb{N}$ den Fehler

$$\widetilde{\varepsilon}_i := \widetilde{z}_i - \sum_{j=1}^{k} \widetilde{a}_i^{q^{-j}}. \tag{4.10}$$

Es folgt dann durch Einsetzen in die Ausgangsgleichung die Relation

$$\widetilde{z}_i^q - \widetilde{z}_i = \widetilde{a}_i + \widetilde{\varepsilon}_i^q - \widetilde{a}_i^{q^{-k}} - \widetilde{\varepsilon}_i \iff \widetilde{\varepsilon}_i^q - \widetilde{\varepsilon}_i = \widetilde{a}_i^{q^{-k}}$$

und wir sehen mit $v_\infty(\widetilde{a}_i^{q^{-k}}) < 0$, dass für die Bewertung des Fehlers $\widetilde{\varepsilon}_i$ gilt:

$$v_\infty(\widetilde{\varepsilon}_i) = \frac{1}{q^{k+1}} v_\infty(\widetilde{a}_i) \leq 0. \tag{4.11}$$

b) Falls $v_\infty(\widetilde{a}_i) > 0$ ist, konvergiert die Reihe $\sum_{j=0}^{\infty} \widetilde{a}_i^{q^j}$ und wir rechnen nach:

$$\widetilde{z}_i^q - \widetilde{z}_i = \widetilde{a}_i \quad \textit{für} \quad \widetilde{z}_i := -\sum_{j=0}^{\infty} \widetilde{a}_i^{q^j}. \tag{4.12}$$

Wir haben in Bemerkung 4.4.5 gesehen, dass die Bedingungen $v_\infty(M) > 0$ und $v_\infty(M^{-1}) > 0$ hinreichend sind, um Problem 4.4.3 lösen zu können.

Im Folgenden weisen wir die Lösbarkeit mit den (approximierten) Lösungen aus Bemerkung 4.4.8 in diesen Fällen noch einmal explizit nach. Diese Rechnungen helfen uns im anschließenden Abschnitt 4.5, das Vorgehen im Spezialfall der Antidiagonalmatrizen zu erklären.

Wir beginnen mit $v_\infty(M) > 0$:

4.4.9 Proposition. *Seien $a \in L^d$ mit $v_\infty(a) \geq 0$ und $M \in \mathrm{GL}_d(L)$ mit $v_\infty(M) > 0$ gegeben. Weiter sei E eine Lang-Steinberg-Matrix zu M und $\widetilde{a} := (E^{(1)})^{-1}a$. Dann gibt es eine Lösung $z \in \widetilde{L}^d$ (wobei $\widetilde{L} \subset \overline{K_\infty}$ eine geeignete endliche algebraische Erweiterung von L ist) mit $v_\infty(z) \geq$ für die Gleichung*

$$z^{(1)} - Mz = a.$$

Beweis. Wir stellen zunächst fest, dass in diesem Fall wegen $v_\infty(M) > 0$ nach Bemerkung 4.4.5 auch $v_\infty(E) > 0$ gilt.
In $\overline{K_\infty}$ gibt es eine Lösung z; wir wählen eine endliche algebraische Erweiterung $\widetilde{L}$ von L, in der diese enthalten ist. Wir müssen nun $v_\infty(z) \geq$ zeigen und approximieren z dazu durch die Summe $\sum_{j=1}^{k} \widetilde{a}^{(-j)} \in L^d$ mit $k \in \mathbb{N}$, wobei wir die Fehler $\widetilde{\varepsilon}_i$ in den Komponenten wie in Bemerkung 4.4.8 angeben. Wir unterscheiden abhängig von $v_\infty(\widetilde{a}_i)$:

1. Für die Komponenten von $\widetilde{a}_i$ mit $v_\infty(\widetilde{a}_i) \leq 0$ sei aus technischen Gründen $\widetilde{\delta}_i := 0$ und $z_i := \sum_{j=1}^{k} \widetilde{a}_i^{q^{-j}} + \widetilde{\varepsilon}_i + \widetilde{\delta}_i$, wobei $v_\infty(\widetilde{\varepsilon}_i) = \frac{1}{q^{k+1}} v_\infty(\widetilde{a}_i) \leq 0$ durch Formel 4.11

gegeben ist.

2. Für die Komponenten von $\widetilde{a}_i$ mit $v_\infty(\widetilde{a}_i) > 0$ sei $\widetilde{\varepsilon}_i := 0$ und $\widetilde{z}_i := -\sum_{j=0}^{\infty} \widetilde{a}_i^{q^j} + \widetilde{\varepsilon}_i$, wobei wir dies zu $z_i = \sum_{j=1}^{k} \widetilde{a}_i^{q^{-j}} + (-\sum_{j=0}^{k} \widetilde{a}_i^{q^{-j}} - \sum_{j=1}^{\infty} \widetilde{a}_i^{q^j}) + \widetilde{\varepsilon}_i$ umschreiben. In diesem Fall definieren wir dann $\widetilde{\delta}_i := -\sum_{j=1}^{k} \widetilde{a}_i^{q^{-j}} - \sum_{j=0}^{\infty} \widetilde{a}_i^{q^j}$, wobei $v_\infty(\widetilde{\delta}_i) > 0$ wegen $v_\infty(\widetilde{a}_i) > 0$ gilt.

Diese technische Notation wird nun dadurch klar, dass wir den ganzen Vektor $\widetilde{z}$ schreiben können als

$$\widetilde{z} = \sum_{j=1}^{k} \widetilde{a}_i^{(-j)} + \widetilde{\varepsilon} + \widetilde{\delta},$$

wobei $v_\infty(\varepsilon) \geq \frac{1}{q^{k+1}} v_\infty(\widetilde{a})$ und $v_\infty(\widetilde{\delta}) > 0$ gilt. Wir müssen im Weiteren also zeigen, dass $v_\infty(z) = v_\infty(E\ \widetilde{z}) \geq 0$ ist.

Wir wählen dazu $k \in \mathbb{N}$ so, dass $v_\infty(\widetilde{\varepsilon}) = \frac{1}{q^{k+1}} v_\infty(\widetilde{a}) \geq -v_\infty(E)$ ist, damit folgt:

$$v_\infty(E\,\widetilde{\varepsilon}) \geq \underbrace{v_\infty(E)}_{>0} + \underbrace{v_\infty(\widetilde{\varepsilon})}_{\leq 0} \geq 0.$$

Um $v_\infty(E \sum_{j=1}^{k} \widetilde{a}^{(-j)})$ abzuschätzen, berechnen wir für $j \in \{1, \ldots, k\}$:

$$\begin{aligned} E\ \widetilde{a}^{(-j)} &= (E\,(E^{-1})^{(1)} a)^{(-j)} \\ &= E\,(E^{-1})^{(-(j-1))} a^{(-j)}. \end{aligned}$$

Für $j = 1$ ist $E\,(E^{-1})^{(-(j-1))} = I_d$ und für $j \geq 2$ gilt, indem wir mit geeigneten Potenzen von E erweitern:

$$\begin{aligned} E(E^{-1})^{(-(j-1))} &= E(E^{-1})^{(-1)} \cdot E^{(-2)}(E^{-1})^{(-2)} \cdots E^{(-(j-2))}(E^{-1})^{(-(j-1))} \\ &= (E^{(1)}E^{-1})^{(-1)} \cdot (E^{(1)}E^{-1})^{(-2)} \cdots (E^{(1)}E^{-1})^{(-(j-1))} \\ &= M^{(-1)} \cdot M^{(-2)} \cdots M^{(-(j-1))} = \prod_{l=1}^{j-1} M^{(-l)}. \end{aligned}$$

Wir definieren $\prod_{l=1}^{j-1} M^{(-l)} := I_d$ für $j = 1$. Es ist damit $v_\infty(\prod_{l=1}^{j-1} M^{(-l)}) = 1$ für $j = 1$,

$v_\infty(\prod_{l=1}^{j-1} M^{(-l)}) > 0$ für $j \geq 2$ und $v_\infty(a) \geq 0$. Daraus folgt schließlich:

$$\begin{aligned} v_\infty(E \sum_{j=1}^{k} \widetilde{a}^{(-j)}) &= v_\infty(\sum_{j=1}^{k} (\prod_{l=1}^{j-1} M^{(-l)} a^{(-j)})) \\ &\geq \min_{j=1,\dots,k} \{ v_\infty(\prod_{l=1}^{j-1} M^{(-l)} a^{(-j)}) \} \geq 0. \end{aligned}$$

Insgesamt gilt also $v_\infty(z) = v_\infty(E\,\widetilde{z}) = v_\infty(E \sum_{j=1}^{k} \widetilde{a}^{(-j)} + E\,\widetilde{\varepsilon} + E\,\widetilde{\delta}) \geq 0$. □

Den Fall $v_\infty(M^{-1}) \geq 0$ erhalten ganz ähnlich:

4.4.10 Proposition. *Seien $a \in L^d$ mit $v_\infty(a) \geq 0$ und $M \in \mathrm{GL}_d(L)$ mit $v_\infty(M^{-1}) \geq 0$ gegeben. Weiter sei E eine Lang-Steinberg-Matrix zu M und $\widetilde{a} := (E^{(1)})^{-1} a$. Dann ist $\sum_{j=1}^{\infty} \widetilde{a}^{(j)}$ eine Lösung z (mit $v_\infty(z) \geq 0$) der Gleichung*

$$z^{(1)} - Mz = a.$$

Beweis. Nach Bemerkung 4.4.5 gilt in diesem Fall $v_\infty((E)^{-1}) \geq 0$, woraus mit Bemerkung 4.4.8 folgt, dass $v_\infty(\widetilde{z}_i) = v_\infty(\widetilde{a}_i)$ ist. Somit konvergiert die Summe $\widetilde{z} := \sum_{j=1}^{\infty} \widetilde{a}^{(j)}$ und ist nach Bemerkung 4.4.8 eine Lösung, für die wir nun $v_\infty(z) = v_\infty(E\,\widetilde{z}) \geq 0$ zeigen.

Für $j \in \{0, \dots, k\}$ betrachten wir

$$\begin{aligned} E\,\widetilde{a}^{(j)} &= (E\,(E^{-1})^{(1)} a)^{(j)} \\ &= E\,(E^{-1})^{(j+1)} a^{(j)} \end{aligned}$$

und erweitern dies wiederum mit geeigneten Potenzen von E zu:

$$\begin{aligned} E(E^{-1})^{(j+1)} &= E(E^{(1)})^{-1} \cdot E^{(1)}(E^{(2)})^{-1} \cdots E^{(j)}(E^{(j+1)})^{-1} \\ &= M^{-1} \cdot (M^{-1})^{(1)} \cdots (M^{-1})^{(j)} = \prod_{l=0}^{j}((M^{-1})^{(l)}). \end{aligned}$$

Mit $v_\infty(M^{-1}) \geq 0$ und $v_\infty(a) \geq 0$ erhalten wir dann

$$\begin{aligned} v_\infty(E \sum_{j=1}^{k} \widetilde{a}_i^{(j)}) &= v_\infty(\sum_{j=1}^{k}(\prod_{l=0}^{j}(M^{-1})^{(l)} a^{(j)})) \\ &\geq \min_{j=1,\ldots,k}\{ v_\infty(\prod_{l=0}^{j}(M^{-1})^{(l)} a^{(j)}) \} > 0. \end{aligned}$$

Somit gilt hier $v_\infty(z) = v_\infty(E\, \widetilde{z}) = v_\infty(E\ \sum_{j=1}^{k} \widetilde{a}_i^{(j)}) \geq 0.$ □

4.5 Antidiagonalgleichungen in Dimension $d = 2$

Wir führen die Untersuchungen aus Abschnitt 4.4 fort, beschränken uns jetzt aber in Dimension $d = 2$ auf Antidiagonalmatrizen M, also solche Matrizen, deren Nicht-Nulleinträge sich nur auf der Gegendiagonalen befinden.
Für diesen Spezialfall leiten wir im Laufe dieses Abschnitts für allgemeine a (ohne die bisherige Voraussetzung $v_\infty(a) \geq 0$) notwendige und hinreichende Kriterien an M und a für die Lösbarkeit von Problem 4.4.3 her.

Es sei $M = \begin{pmatrix} 0 & m_2 \\ m_3 & 0 \end{pmatrix}$ eine invertierbare Antidiagonalmatrix.

Um eine Lang-Steinberg-Matrix $E = \begin{pmatrix} e_1 & e_2 \\ e_3 & e_4 \end{pmatrix}$ zu M zu bestimmen, berechnen wir:

$$\begin{aligned} M = E^{(1)}E^{-1} &= \begin{pmatrix} e_1^q & e_2^q \\ e_3^q & e_4^q \end{pmatrix} \cdot \left(\frac{1}{\det(E)} \begin{pmatrix} e_4 & -e_2 \\ -e_3 & e_1 \end{pmatrix} \right) \\ &= \frac{1}{e_1e_4 - e_2e_3} \begin{pmatrix} e_1^q e_4 - e_2^q e_3 & e_1 e_2^q - e_1^q e_2 \\ e_3^q e_4 - e_3^q e_4 & e_1 e_4^q - e_2 e_3^q \end{pmatrix}. \end{aligned}$$

Es gilt also $e_1^q e_4 - e_2^q e_3 = 0$ und $e_1 e_4^q - e_2 e_3^q = 0$. Dabei kann E keine Nulleinträge haben, da wir annehmen, dass M invertierbar ist. Also folgen aus diesen beiden Gleichungen die Relationen

$$\frac{e_2^q}{e_1^q} = \frac{e_4}{e_3} \quad \text{und} \quad \frac{e_2}{e_1} = \frac{e_4^q}{e_3^q}.$$

Definieren wir nun $\zeta := \frac{e_4}{e_3}$, muss $\zeta^{q^2} = \zeta$ gelten; es ist also $\zeta \in \mathbb{F}_{q^2}$ und es folgt

$$e_2 = \zeta^q e_1 \quad \text{und} \quad e_4 = \zeta e_3.$$

Wir erhalten durch Einsetzen $\frac{e_1^q}{e_3} = m_2$ und $\frac{e_3^q}{e_1} = m_3$, woraus wir schließen:

$$e_1^{q^2-1} = m_2^q m_3 \quad \text{und} \quad e_3^{q^2-1} = m_2 m_3^q. \tag{4.13}$$

Wir bemerken, dass wir für jedes beliebige $\zeta \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ eine Lang-Steinberg-Matrix E zu

M erhalten, wobei dann gilt:

$$M = \begin{pmatrix} 0 & e_1^q e_3^{-1} \\ e_3^q e_1^{-1} & 0 \end{pmatrix}, \; E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} \text{ und } E^{-1} = \frac{1}{\zeta - \zeta^q} \begin{pmatrix} \zeta e_1^{-1} & -\zeta^q e_3^{-1} \\ -e_1^{-1} & e_3^{-1} \end{pmatrix}.$$

Es sei $a \in L^2$ beliebig. Wir lassen dabei die Forderung $v_\infty(a) > 0$, wie in Bemerkung 4.4.4 beschrieben, im Folgenden fallen. Dann definieren wir

$$\widetilde{a} := (E^{(1)})^{-1} a = \frac{1}{\zeta^q - \zeta} \begin{pmatrix} \zeta^q e_1^{-q} a_1 - \zeta e_3^{-q} a_2 \\ -e_1^{-q} a_1 + e_3^{-q} a_2 \end{pmatrix}. \tag{4.14}$$

Also gilt wegen $v_\infty(\zeta) = 0$ für die Bewertungen der einzelnen Komponenten von $\widetilde{a}$:

$$v_\infty(\widetilde{a}_1), v_\infty(\widetilde{a}_2) \geq \min\{v_\infty(a_1) - q v_\infty(e_1), v_\infty(a_2) - q v_\infty(e_3)\}, \tag{4.15}$$

hier kann nur dann $v_\infty(\widetilde{a}_1) \neq v_\infty(\widetilde{a}_2)$ gelten, wenn $v_\infty(\widetilde{a}_1) - q v_\infty(\widetilde{e}_2) = v_\infty(\widetilde{a}_2) - q v_\infty(\widetilde{e}_4)$ ist (und dabei Terme mit niedrigeren Bewertungen entsprechend ausgelöscht werden).

Wir wollen zunächst die Abhängigkeiten zwischen m_2, m_3 und e_1, e_3 untersuchen.

4.5.1 Bemerkung. *Aus den Beziehungen 4.13) folgt für e_1 und e_3, dass $e_1^{q^2-1} = m_2^q\, m_3$ und $e_3^{q^2-1} = m_2\, m_3^q$ gelten. Das heißt für die entsprechenden Bewertungen:*

$$v_\infty(e_1) = \frac{q\, v_\infty(m_2) + v_\infty(m_3)}{q^2 - 1} \quad \textit{und} \quad v_\infty(e_3) = \frac{v_\infty(m_2) + q\, v_\infty(m_3)}{q^2 - 1}.$$

Dabei gilt insbesondere:

$$\begin{aligned} v_\infty(e_1) \geq 0 &\iff v_\infty(m_2^q\, m_3) \geq 0, \\ v_\infty(e_3) \geq 0 &\iff v_\infty(m_2\, m_3^q) \geq 0. \end{aligned}$$

Wir werden nun aus einer genauen Untersuchung des Falls der Antidiagonalmatrizen notwendige und hinreichende Bedingungen an a und E herleiten, unter denen es eine Lösung z für Problem 4.4.3 mit $v_\infty(z) \geq 0$ gibt, wobei wir keine weiteren Annahmen an die Bewertung von a machen. Durch Bewertungsvergleiche ergeben sich direkt die folgenden notwendigen Bedingungen.

4.5.2 Lemma. *Sei* $M = \begin{pmatrix} 0 & m_2 \\ m_3 & 0 \end{pmatrix}$ *invertierbar und* E *eine Lang-Steinberg-Matrix zu* M *mit*

$$E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} \quad \text{und} \quad M = E^{(1)}E^{-1} = \begin{pmatrix} 0 & e_1^q e_3^{-1} \\ e_3^q e_1^{-1} & 0 \end{pmatrix}.$$

Weiter sei z *eine Lösung* $z \in \overline{K}_\infty^2$ *von* $z^{(1)} - Mz = a$ *mit* $v_\infty(z) \geq 0$*, dann gelten die folgenden Implikationen:*

1. $v_\infty(e_1) \geq 0 \implies v_\infty(m_2^q\, a_2 + a_1^q) \geq 0$,
2. $v_\infty(e_1) < 0 \implies v_\infty(m_3^{-1}\, a_2 + m_2^{-q}\, m_3^{-1}\, a_1^q) > 0$,
3. $v_\infty(e_3) \geq 0 \implies v_\infty(m_3^q\, a_1 + a_2^q) \geq 0$,
4. $v_\infty(e_3) < 0 \implies v_\infty(m_2^{-1}\, a_1 + m_3^{-q}\, m_2^{-1}\, a_2^q) > 0$.

Beweis. Wir nehmen an, dass es eine Lösung $z \in \widetilde{L}^d$ mit $v_\infty(z) \geq 0$ gibt. Dann gilt

$$\begin{aligned} z^{(1)} - Mz = a &\implies z^{(2)} - M^{(1)}z^{(1)} = a^{(1)} \\ &\implies z^{(2)} - M^{(1)}(Mz + a) = a^{(1)} \\ &\implies z^{(2)} - M^{(1)}Mz = M^{(1)}a + a^{(1)} \\ &\implies \begin{pmatrix} z_1^{q^2} \\ z_2^{q^2} \end{pmatrix} - \begin{pmatrix} m_2^q\, m_3 & 0 \\ 0 & m_3^q\, m_2 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} m_2^q\, a_2 + a_1^q \\ m_3^q\, a_1 + a_2^q \end{pmatrix}. \end{aligned}$$

Die Zeilen dieser Gleichung sind wegen der Diagonalgestalt von $M^{(1)}M$ getrennt:

$$\begin{aligned} z_1^{q^2} - m_2^q\, m_3 + z_1 &= m_2^q\, a_2 + a_1^q, \\ z_2^{q^2} - m_3^q\, m_2 + z_2 &= m_3^q\, a_1 + a_2^q. \end{aligned}$$

Wir erhalten die Implikationen 1 und 2 wie folgt aus der ersten Zeile:

1. Nach Bemerkung 4.5.1 ist $v_\infty(e_1) \geq 0$ äquivalent zu $v_\infty(m_2^q\, m_3) \geq 0$. Damit ergibt sich wegen $v_\infty(z_1) \geq 0$ aus der ersten Zeile direkt $v_\infty(m_2^q\, a_2 + a_1^q) \geq 0$.

2. Es ist $v_\infty(e_1) < 0$ äquivalent zu $v_\infty(m_2^q m_3) < 0$. Weiter folgt aus der ersten Zeile

$$\begin{aligned} & v_\infty(m_2^q m_3\ z_1 + m_2^q a_2 + a_1^q) = v_\infty(z_1^q) \geq 0 \\ \implies\ & v_\infty(m_2^q m_3 \cdot (z_1 + m_3^{-1} a_2 + m_2^{-q} m_3^{-1} a_1^q)) \geq 0 \\ \implies\ & v_\infty(m_2^q m_3) + v_\infty(z_1 + m_3^{-1} a_2 + m_2^{-q} m_3^{-1} a_1^q) \geq 0. \end{aligned}$$

Mit $v_\infty(m_2^q m_3) < 0$ und $v_\infty(z_1) \geq 0$ schließen wir: $v_\infty(m_3^{-1} a_2 + m_2^{-q} m_3^{-1} a_1^q) > 0$.

Die Implikationen 3 und 4 ergeben sich aus der zweiten Zeile ganz analog. □

4.5.3 Folgerung. *Aus den Implikationen in Lemma 4.5.2 ergibt sich weiter*

1. $v_\infty(e_1) \geq 0 \implies v_\infty(a_2) \geq qv_\infty(e_3) - q^2 v_\infty(e_1)$ *und* $v_\infty(a_1) \geq 0$,
2. $v_\infty(e_1) < 0 \implies v_\infty(a_2) > qv_\infty(e_3) - v_\infty(e_1)$ *und* $v_\infty(a_1) > \frac{q^2-1}{q} v_\infty(e_1)$,
3. $v_\infty(e_3) \geq 0 \implies v_\infty(a_1) \geq qv_\infty(e_1) - q^2 v_\infty(e_3)$ *und* $v_\infty(a_2) \geq 0$,
4. $v_\infty(e_3) < 0 \implies v_\infty(a_1) > qv_\infty(e_1) - v_\infty(e_3)$ *und* $v_\infty(a_2) > \frac{q^2-1}{q} v_\infty(e_3)$.

Beweis. Folgt direkt durch Einsetzen der Definitionen. □

Lemma 4.5.2 bzw. Folgerung 4.5.3 liefert somit notwendige Bedingungen für die Lösbarkeit von Problem 4.4.3 für Antidiagonalmatrizen. Wir sehen mit Bemerkung 4.5.1, dass diese schwächer als die hinreichenden Bedingungen $v_\infty(M) \geq 0$ oder $v_\infty(M^{-1}) > 0$ für allgemeine Matrizen M sind, die wir in Bemerkung 4.4.5 festgestellt haben. Entsprechend kann für Antidiagonalmatrizen als notwendige Bedingung zusätzlich der Fall auftreten, in dem $v_\infty(M) < 0$ und $v_\infty(M^{-1}) < 0$ gilt.

Wir werden jetzt analog zu Propositionen 4.4.9 und 4.4.10 zeigen, dass die notwendigen Bedingungen aus Folgerung 4.5.3 für Antidiagonalmatrizen auch hinreichend sind.

4.5.4 Proposition. *Sei* $M = \begin{pmatrix} 0 & m_2 \\ m_3 & 0 \end{pmatrix}$ *invertierbar und* E *eine Lang-Steinberg-Matrix zu* M *mit* $v_\infty(E) \geq 0$ *und*

$$E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} \quad \text{und} \quad M = E^{(1)} E^{-1} = \begin{pmatrix} 0 & e_1^q e_3^{-1} \\ e_3^q e_1^{-1} & 0 \end{pmatrix}.$$

Weiter gelte für $a \in L^2$ (dies sind die notwendigen Bedingungen aus Folgerung 4.5.3):

1. $v_\infty(a_2) \geq qv_\infty(e_3) - q^2 v_\infty(e_1)$ *und* $v_\infty(a_1) \geq 0$

sowie

3. $v_\infty(a_1) \geq qv_\infty(e_1) - q^2 v_\infty(e_3)$ *und* $v_\infty(a_2) \geq 0,$

dann gibt es eine Lösung $z \in \widetilde{L}^2$ (wobei $\widetilde{L} \subset \overline{K}_\infty$ eine geeignete endliche algebraische Erweiterung von L ist) mit $v_\infty(z) \geq$ für die Gleichung

$$z^{(1)} - Mz = a \ \left(\Longleftrightarrow \ \widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a};\ \widetilde{z} = E^{-1}z\right).$$

Beweis. Sei $z \in \overline{K}_\infty^2$ eine Lösung. Wir wählen eine endliche algebraische Erweiterung $\widetilde{L}$ von L, so dass $z \in L^2$ ist. Um $v_\infty(z) \geq 0$ zu zeigen, approximieren wir z durch die Summe $\sum_{j=1}^k \widetilde{a}^{(-j)} \in L^d$ mit $k \in \mathbb{N}$ wie in Proposition 4.4.9 und schreiben

$$\widetilde{z} = \sum_{j=1}^{k} \widetilde{a}_i^{(-j)} + \widetilde{\varepsilon} + \widetilde{\delta},$$

dabei gilt $v_\infty(\varepsilon) \geq \frac{1}{q^{k+1}} v_\infty(\widetilde{a})$ und $v_\infty(\widetilde{\delta}) > 0$. Um zu zeigen, dass $v_\infty(z) = v_\infty(E\,\widetilde{z}) \geq 0$ ist, wählen wir $k \in \mathbb{N}$ so, dass $v_\infty(E\,\widetilde{\varepsilon}) > 0$ ist. Wie in Proposition 4.4.9 sehen wir, dass

$$E \sum_{j=1}^{k} \widetilde{a}^{(-j)} = \sum_{j=1}^{k} (\prod_{l=1}^{j-1} M^{(-l)}) a^{(-j)},$$

wobei $\prod_{l=1}^{j-1} M^{(-l)} := I_d$ für $j = 1$ definiert ist. An dieser Stelle rechnen wir nun mittels Induktion nach, dass für $j \geq 1$ gilt:

$$\prod_{l=1}^{j-1} M^{(-l)} = \begin{cases} \begin{pmatrix} 0 & e_1\, e_3^{-q^{-(j-1)}} \\ e_3\, e_1^{-q^{-(j-1)}} & 0 \end{pmatrix}, & \text{falls } (j-1) \text{ ungerade,} \\[2em] \begin{pmatrix} e_1\, e_1^{-q^{-(j-1)}} & 0 \\ 0 & e_3\, e_3^{-q^{-(j-1)}} \end{pmatrix}, & \text{falls } (j-1) \text{ gerade.} \end{cases}$$

Wegen $v_\infty(E) > 0$ ist $v_\infty(e_1), v_\infty(e_3) \geq 0$. Damit erhalten wir weiter:

Falls $(j-1)$ gerade ist, gilt wegen $v_\infty(a_1), v_\infty(a_2) > 0$ direkt:

$$v_\infty((\prod_{l=1}^{j-1} M^{(-l)})a^{(-j)}) \geq 0.$$

Falls $(j-1)$ ungerade ist, gelten für alle $(j-1) \geq 1$ die Abschätzungen

$$v_\infty(e_1\, e_3^{-q^{-(j-1)}} a_2^{q^{-j}}) \overset{j=2}{\geq} v_\infty(e_1\, e_3^{-q^{-1}} a_2^{q^{-2}}) = \frac{1}{q^2}\underbrace{(v_\infty(a_2) + q^2 v_\infty(e_1) - q v_\infty(e_3))}_{\geq 0 \text{ nach Voraussetzung 1}} \geq 0,$$

$$v_\infty(e_3\, e_1^{-q^{-(j-1)}} a_1^{q^{-j}}) \overset{j=2}{\geq} v_\infty(e_3\, e_1^{-q^{-1}} a_1^{q^{-2}}) = \frac{1}{q^2}\underbrace{(v_\infty(a_1) + q^2 v_\infty(e_3) - q v_\infty(e_1))}_{\geq 0 \text{ nach Voraussetzung 3}} \geq 0,$$

woraus wir hier ebenfalls schließen können:

$$v_\infty((\prod_{l=1}^{j-1} M^{(-l)})a^{(-j)}) \geq 0.$$

Insgesamt folgt also $v_\infty(z) = v_\infty(E\,\widetilde{z}) = v_\infty(E\,\sum_{j=1}^{k} \widetilde{a}^{(-j)} + E\,\widetilde{\varepsilon} + E\,\widetilde{\delta}) \geq 0.$ □

Damit ist der Fall $v_\infty(E) \geq 0$ komplett durch notwendige und hinreichende Bedingungen beschrieben. Wir betrachten im Folgenden $v_\infty(E^{-1}) > 0$.

4.5.5 Proposition. *Sei* $M = \begin{pmatrix} 0 & m_2 \\ m_3 & 0 \end{pmatrix}$ *invertierbar und* E *eine Lang-Steinberg-Matrix zu* M *mit* $v_\infty(E^{-1}) > 0$ *und*

$$E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} \quad \textit{und} \quad M = E^{(1)}E^{-1} = \begin{pmatrix} 0 & e_1^q e_3^{-1} \\ e_3^q e_1^{-1} & 0 \end{pmatrix}.$$

Weiter gelte für $a \in L^2$ *(dies sind die notwendigen Bedingungen aus Folgerung 4.5.3):*

$$\mathit{2.}\ v_\infty(a_2) > q v_\infty(e_3) - v_\infty(e_1) \ \textit{und}\ v_\infty(a_1) > \frac{q^2-1}{q} v_\infty(e_1)$$

sowie

$$4.\ v_\infty(a_1) > qv_\infty(e_1) - v_\infty(e_3) \text{ und } v_\infty(a_2) > \frac{q^2-1}{q} v_\infty(e_3),$$

dann gibt es eine Lösung $z \in L^2$ mit $v_\infty(z) \geq$ für die Gleichung

$$z^{(1)} - Mz = a \ \left(\Longleftrightarrow\ \widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a};\ \widetilde{z} = E^{-1}z\right).$$

Beweis. In diesem Fall gelten $v_\infty(e_1) < 0$ und $v_\infty(e_3) < 0$, da $v_\infty(E^{-1}) > 0$ ist. Betrachten wir zunächst $\widetilde{a} := (E^{(1)})^{-1}a$.

Wegen $v_\infty(a_1) > qv_\infty(e_1) - v_\infty(e_3) > qv_\infty(e_1)$ und $v_\infty(a_2) > qv_\infty(e_3) - v_\infty(e_1) > qv_\infty(e_3)$ folgt aus der Abschätzung 4.15, dass $v_\infty(\widetilde{a}_1), v_\infty(\widetilde{a}_2) > 0$ gilt. Somit ist eine Lösung $\widetilde{z} \in L^2$ gegeben durch die folgende konvergente Reihe (siehe Bemerkung 4.4.8):

$$\widetilde{z} := -\sum_{j=0}^{\infty} \widetilde{a}^{(j)}.$$

Wir müssen zeigen, dass $v_\infty(z) = v_\infty(E\,\widetilde{z}) \geq 0$ ist. Wie in Proposition 4.4.9 folgt

$$E\,(-\sum_{j=0}^{\infty} \widetilde{a}^{(j)}) = -\sum_{j=0}^{k} (\prod_{l=0}^{j} (M^{-1})^{(l)}) a^{(j)},$$

und wir erhalten durch Induktion für $j \geq 0$:

$$\prod_{l=0}^{j} (M^{-1})^{(l)} = \begin{cases} \begin{pmatrix} 0 & e_1\, e_3^{-q^{j+1}} \\ e_3\, e_1^{-q^{j+1}} & 0 \end{pmatrix}, & \text{falls } j \text{ gerade}, \\ \\ \begin{pmatrix} e_1\, e_1^{-q^{j+1}} & 0 \\ 0 & e_3\, e_3^{-q^{j+1}} \end{pmatrix}, & \text{falls } j \text{ ungerade}. \end{cases}$$

Wir sehen an dieser Stelle weiter:

Falls j gerade ist, ergeben sich für alle $j \geq 0$ die Abschätzungen

$$v_\infty(e_1\, e_3^{-q^{j+1}} a_2^{q^j}) \overset{j=0}{\geq} v_\infty(e_1\, e_3^{-q^{-1}} a_2^{q^{-2}}) = \frac{1}{q^2}\underbrace{(v_\infty(a_2) + v_\infty(e_1) - q v_\infty(e_3))}_{>0 \text{ nach Voraussetzung 2}} > 0,$$

$$v_\infty(e_3\, e_1^{-q^{j+1}} a_1^{q^j}) \overset{j=0}{\geq} v_\infty(e_3\, e_1^{-q^{-1}} a_1^{q^{-2}}) = \frac{1}{q^2}\underbrace{(v_\infty(a_1) + q^2 v_\infty(e_3) - q v_\infty(e_1))}_{>0 \text{ nach Voraussetzung 4}} > 0;$$

also erhalten wir in diesem Fall:

$$v_\infty((\prod_{l=0}^{j}(M^{-1})^{(l)})a^{(j)}) > 0.$$

Falls j ungerade ist, erhalten wir für $j \geq 1$

$$v_\infty(e_1\, e_1^{-q^{j+1}} a_1^{q^j}) \overset{j=1}{\geq} v_\infty(e_1\, e_1^{-q^{-1}} a_1^{q^{-1}}) = \frac{1}{q^2}\underbrace{(v_\infty(a_1) - \frac{q^2-1}{q} v_\infty(e_1))}_{>0 \text{ nach Voraussetzung 2}} > 0,$$

$$v_\infty(e_3\, e_3^{-q^{j+1}} a_2^{q^j}) \overset{j=1}{\geq} v_\infty(e_3\, e_3^{-q^{-1}} a_2^{q^{-1}}) = \frac{1}{q^2}\underbrace{(v_\infty(a_2) - \frac{q^2-1}{q} v_\infty(e_3))}_{>0 \text{ nach Voraussetzung 4}} > 0;$$

damit folgt auch hier:

$$v_\infty((\prod_{l=0}^{j}(M^{-1})^{(l)})a^{(j)}) > 0.$$

Schließlich haben wir insgesamt $v_\infty(z) = v_\infty(E\,\widetilde{z}) = v_\infty(E\,(-\sum_{j=1}^{k} \widetilde{a}^{(j)})) > 0.$ □

Also sind auch im Fall $v_\infty(E^{-1}) > 0$ die notwendigen Bedingungen aus Folgerung 4.5.3 für die Existenz einer Lösung hinreichend. Es bleibt noch der Fall, in dem

$$v_\infty(E) > 0 \quad \text{und} \quad v_\infty(E^{-1}) > 0$$

gelten. Hier ist $v_\infty(e_1) \geq 0$ und $v_\infty(e_3) < 0$; oder umgekehrt $v_\infty(e_1) < 0$ und $v_\infty(e_3) \geq 0$.

Wir betrachten im Folgenden $v_\infty(e_1) \geq 0$ und $v_\infty(e_3) < 0$. Wir nehmen dabei an, dass für $a \in L^2$ die entsprechenden notwendigen Bedingungen 1 und 4 aus 4.5.3 für die Lösbarkeit von Problem 4.4.3 gelten. Damit gilt insbesondere auch $v_\infty(a_2) \geq \frac{q^2-1}{q} v_\infty(e_3)$ und für $\widetilde{a} := (E^{(1)})^{-1} a$ erhalten wir dann die folgende Abschätzung (analog zu 4.15):

$$v_\infty(\widetilde{a}_1), v_\infty(\widetilde{a}_2) \geq \min\{v_\infty(a_1) - q v_\infty(e_1), \underbrace{v_\infty(a_2) - q v_\infty(e_3)}_{> (\frac{q^2-1}{q} - q)\, v_\infty(e_3) > 0}\}.$$

4.5.6 Bemerkung. *Damit können an dieser Stelle die beiden folgenden Fälle eintreten:*

a) $v_\infty(a_1) - q v_\infty(e_1) \leq 0$, *dann ist* $v_\infty(\widetilde{a}_1) = v_\infty(\widetilde{a}_2) = v_\infty(a_1) - q v_\infty(e_1)$;

b) $v_\infty(a_1) - q v_\infty(e_1) > 0$, *hier gilt dann* $v_\infty(\widetilde{a}_1), v_\infty(\widetilde{a}_2) > 0$.

Wir zeigen nun, falls $z \in \overline{K}_\infty^2$ eine Lösung von Problem 4.4.3 mit $v_\infty(e_1) \geq 0$ und $v_\infty(e_3) < 0$ ist, dass dann notwendigerweise Fall b) eintreten muss und Fall a) somit ausgeschlossen werden kann.
Dabei sehen wir direkt, dass die Bedingung von Fall b) bereits erfüllt ist, wenn der Teil $v_\infty(a_1) > q v_\infty(e_1) - v_\infty(e_3)$ von Bedingung 4 aus Folgerung 4.5.3 gilt.

4.5.7 Lemma. *Sei* $M = \begin{pmatrix} 0 & m_2 \\ m_3 & 0 \end{pmatrix}$ *invertierbar und* E *eine Lang-Steinberg-Matrix zu* M *mit* $v_\infty(e_1) \geq 0$ *und* $v_\infty(e_3) < 0$, *wobei*

$$E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} \quad \text{und} \quad M = E^{(1)} E^{-1} = \begin{pmatrix} 0 & e_1^q e_3^{-1} \\ e_3^q e_1^{-1} & 0 \end{pmatrix}.$$

Weiter sei $a \in L^2$ *mit* $v_\infty(a_2) > 0$ *und* $z \in \overline{K}_\infty^2$ *eine Lösung von* $z^{(1)} - Mz = a$ *mit* $v_\infty(z) \geq 0$, *dann folgt*

$$v_\infty(a_1) - q v_\infty(e_1) > 0.$$

Beweis. Wir nutzen im Folgenden die Ähnlichkeit von E^{-1} und $(E^{(1)})^{-1}$. Es gilt

$$E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} = \begin{pmatrix} e_1 & 0 \\ 0 & e_3 \end{pmatrix} \begin{pmatrix} 1 & \zeta^q \\ 1 & \zeta \end{pmatrix}, \quad E^{-1} = \frac{1}{\zeta - \zeta^q} \begin{pmatrix} -\zeta & \zeta^q \\ 1 & -1 \end{pmatrix} \begin{pmatrix} e_1^{-1} & 0 \\ 0 & e_3^{-1} \end{pmatrix},$$

wir erhalten wegen $\zeta^{q^2} = \zeta \in \mathbb{F}_{q^2}$ die folgenden Darstellungen für $E^{(1)}$ und $(E^{(1)})^{-1}$:

$$\begin{aligned} E^{(1)} &= \begin{pmatrix} e_1^q & 0 \\ 0 & e_3^q \end{pmatrix} \begin{pmatrix} 1 & \zeta \\ 1 & \zeta^q \end{pmatrix} = \begin{pmatrix} e_1^q & 0 \\ 0 & e_3^q \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & \zeta^q \\ 1 & \zeta \end{pmatrix} \quad \text{und} \\ (E^{(1)})^{-1} &= \frac{1}{\zeta - \zeta^q} \begin{pmatrix} -\zeta & \zeta^q \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e_1^{-q} & 0 \\ 0 & e_3^{-q} \end{pmatrix}. \end{aligned}$$

Damit folgt aus der transformierten Gleichung $\widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a}$ mit $\widetilde{z} = E^{-1}z$:

$$\begin{aligned} & \widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a} \\ \iff \quad & (E^{(1)})^{-1} z^{(1)} - E^{-1} z = (E^{(1)})^{-1} a \\ \iff \quad & \frac{1}{\zeta - \zeta^q} \begin{pmatrix} -\zeta & \zeta^q \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e_1^{-q} & 0 \\ 0 & e_3^{-q} \end{pmatrix} z^{(1)} - \frac{1}{\zeta - \zeta^q} \begin{pmatrix} -\zeta & \zeta^q \\ 1 & -1 \end{pmatrix} \begin{pmatrix} e_1^{-1} & 0 \\ 0 & e_3^{-1} \end{pmatrix} z \\ & \qquad = \frac{1}{\zeta - \zeta^q} \begin{pmatrix} -\zeta & \zeta^q \\ 1 & -1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e_1^{-q} & 0 \\ 0 & e_3^{-q} \end{pmatrix} a \\ \iff \quad & \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e_1^{-q} & 0 \\ 0 & e_3^{-q} \end{pmatrix} z^{(1)} - \begin{pmatrix} e_1^{-1} & 0 \\ 0 & e_3^{-1} \end{pmatrix} z = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} e_1^{-q} & 0 \\ 0 & e_3^{-q} \end{pmatrix} a \\ \iff \quad & \begin{cases} e_3^{-q} z_2^q - e_1^{-1} z_1 = e_3^{-q} a_2, \\ e_1^{-q} z_1^q - e_3^{-1} z_2 = e_1^{-q} a_1. \end{cases} \end{aligned}$$

Aus der ersten Zeile ergibt sich dann aus den Voraussetzungen $v_\infty(z_1), v_\infty(z_2), v_\infty(a_2) > 0$ und $v_\infty(e_3) < 0$, dass $v_\infty(e_1^{-1} z_1) > 0$ ist. Somit ist auch $v_\infty(e_1^{-q} z_1^q) > 0$, weshalb aus der zweiten Zeile $v_\infty(e_1^{-q} a_1) > 0$ folgt. □

Mit Lemma 4.5.7 sehen wir, dass in dem Fall, in dem $v_\infty(e_1) \geq 0$ und $v_\infty(e_3) < 0$ gelten, die Erfüllung der Bedingungen 1 und 4 bereits ein notwendiges Kriterium für die Lösbarkeit von Problem 4.4.3 darstellen. Wir werden abschließend beweisen, dass sie auch hinreichend sind, wobei wir das Lemma implizit benutzen.

4.5.8 Proposition. *Sei* $M = \begin{pmatrix} 0 & m_2 \\ m_3 & 0 \end{pmatrix}$ *invertierbar und* E *eine Lang-Steinberg-*

Matrix zu M mit $v_\infty(e_1) \geq 0$ und $v_\infty(e_3) < 0$, wobei

$$E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} \quad \text{und} \quad M = E^{(1)} E^{-1} = \begin{pmatrix} 0 & e_1^q e_3^{-1} \\ e_3^q e_1^{-1} & 0 \end{pmatrix}.$$

Weiter gelte für $a \in L^2$ (dies sind die notwendigen Bedingungen aus Folgerung 4.5.3):

$$\text{1. } v_\infty(a_2) \geq q v_\infty(e_3) - q^2 v_\infty(e_1) \text{ und } v_\infty(a_1) \geq 0$$

sowie

$$\text{4. } v_\infty(a_1) > q v_\infty(e_1) - v_\infty(e_3) \text{ und } v_\infty(a_2) > \frac{q^2-1}{q} v_\infty(e_3),$$

dann gibt es eine Lösung $z \in L^2$ mit $v_\infty(z) \geq 0$ für die Gleichung

$$z^{(1)} - Mz = a \; \left(\Longleftrightarrow \; \widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a};\; \widetilde{z} = E^{-1} z\right).$$

Beweis. Nach Bemerkung 4.5.6 gilt hier $v_\infty(\widetilde{a_1}), v_\infty(\widetilde{a_2}) > 0$. Wir können also analog zum Beweis von Proposition 4.5.4 vorgehen, da (nach Bemerkung 4.4.8) die Reihe

$$\widetilde{z} := -\sum_{j=0}^{\infty} \widetilde{a}^{(j)}$$

konvergiert und eine Lösung ist. Wir müssen nachweisen, dass $v_\infty(z) = v_\infty(E\,\widetilde{z}) \geq 0$ ist. Wie in Proposition 4.4.9 folgt

$$E\,(-\sum_{j=0}^{\infty} \widetilde{a}^{(j)}) = -\sum_{j=0}^{k} (\prod_{l=0}^{j} (M^{-1})^{(l)}) a^{(j)},$$

und für $j \geq 0$ gilt:

$$\prod_{l=0}^{j} (M^{-1})^{(l)} = \begin{cases} \begin{pmatrix} 0 & e_1\, e_3^{-q^{j+1}} \\ e_3\, e_1^{-q^{j+1}} & 0 \end{pmatrix}, & \text{falls } j \text{ gerade,} \\[2ex] \begin{pmatrix} e_1\, e_1^{-q^{j+1}} & 0 \\ 0 & e_3\, e_3^{-q^{j+1}} \end{pmatrix}, & \text{falls } j \text{ ungerade.} \end{cases}$$

Falls j gerade ist, ergibt sich nun für $j \geq 0$

$$\begin{aligned}
v_\infty(e_1 e_3^{-q^{j+1}} a_2^{q^j}) &= v_\infty(e_1) + q^j(-qv_\infty(e_3) + v_\infty(a_2)) \\
&\overset{4}{>} v_\infty(e_1) + q^j\left(-qv_\infty(e_3) + \frac{q^2-1}{q} v_\infty(e_3)\right) = v_\infty(e_1) - q^j v_\infty(e_3) > 0, \\
v_\infty(e_3 e_1^{-q^{j+1}} a_1^{q^j}) &= \underbrace{q^j\left(v_\infty(a_1) + \frac{1}{q^j} v_\infty(e_3) - qv_\infty(e_1)\right)}_{>0 \text{ für alle } j\geq 0 \text{ nach } 4} > 0;
\end{aligned}$$

also gilt:

$$v_\infty((\prod_{l=0}^{j}(M^{-1})^{(l)})a^{(j)}) > 0.$$

Falls j ungerade ist, erhalten wir für $j \geq 1$

$$\begin{aligned}
v_\infty(e_1 e_1^{-q^{j+1}} a_1^{q^j}) &= q^j \underbrace{(v_\infty(a_1) + -qv_\infty(e_1))}_{>0 \text{ nach } 4} > 0, \\
v_\infty(e_3 e_3^{-q^{j+1}} a_2^{q^j}) &= (1 - q^{j+1}) v_\infty(e_3) + q^j v_\infty(a_2) \\
&\overset{4}{>} (1 - q^{j+1}) v_\infty(e_3) + (q^j \cdot \frac{q^2-1}{q}) v_\infty(e_3) = (1 - q^{j-1}) v_\infty(e_3) > 0;
\end{aligned}$$

damit folgt:

$$v_\infty((\prod_{l=0}^{j}(M^{-1})^{(l)})a^{(j)}) > 0.$$

Wir schließen also insgesamt $v_\infty(z) = v_\infty(E\,\widetilde{z}) = v_\infty(E\,(-\sum_{j=1}^{k} \widetilde{a}^{(j)})) > 0$. □

4.5.9 Bemerkung. *Wir haben Bedingung 1 aus Folgerung 4.5.3 für den Beweis von Proposition 4.5.6 nicht benötigt.*

Der Fall, in dem $v_\infty(e_1) < 0$ und $v_\infty(e_3) \geq 0$ gilt, ergibt sich nun aus der Symmetrie der Gleichungen und der Bedingungen ganz analog, wobei hier 2 und 3 aus Folgerung 4.5.3 die notwendigen und hinreichenden Bedingungen zur Lösbarkeit von 4.4.3 sind.

Wir fassen die Ergebnisse noch einmal zusammen.

4.5.10 Satz. *Sei* $M = \begin{pmatrix} 0 & m_2 \\ m_3 & 0 \end{pmatrix}$ *invertierbar und E eine Lang-Steinberg-Matrix zu*

M, so dass gilt:

$$E = \begin{pmatrix} e_1 & \zeta^q e_1 \\ e_3 & \zeta e_3 \end{pmatrix} \quad \text{und} \quad M = E^{(1)} E^{-1} = \begin{pmatrix} 0 & e_1^q e_3^{-1} \\ e_3^q e_1^{-1} & 0 \end{pmatrix}.$$

Dann gibt es eine Lösung $z \in L^2$ mit $v_\infty(z) \geq 0$ für die Gleichung

$$z^{(1)} - Mz = a \; \big(\Longleftrightarrow \; \widetilde{z}^{(1)} - \widetilde{z} = \widetilde{a}; \; \widetilde{z} = E^{-1} z \big)$$

genau dann, wenn die folgenden Bedingungen erfüllt sind:

1. $v_\infty(e_1) \geq 0 \iff v_\infty(a_2) \geq q v_\infty(e_3) - q^2 v_\infty(e_1)$ *und* $v_\infty(a_1) \geq 0$,
2. $v_\infty(e_1) < 0 \iff v_\infty(a_2) > q v_\infty(e_3) - v_\infty(e_1)$ *und* $v_\infty(a_1) > \frac{q^2-1}{q} v_\infty(e_1)$,
3. $v_\infty(e_3) \geq 0 \iff v_\infty(a_1) \geq q v_\infty(e_1) - q^2 v_\infty(e_3)$ *und* $v_\infty(a_2) \geq 0$,
4. $v_\infty(e_3) < 0 \iff v_\infty(a_1) > q v_\infty(e_1) - v_\infty(e_3)$ *und* $v_\infty(a_2) > \frac{q^2-1}{q} v_\infty(e_3)$.

Das heißt, abhängig von den möglichen Bewertungen von E ist die Lösbarkeit gegeben:

- *Im Fall $v_\infty(E) \geq 0$: genau dann, wenn 1 und 3 gelten.*
- *Im Fall $v_\infty((E)^{-1}) > 0$: genau dann, wenn 2 und 4 gelten.*
- *Im Fall $v_\infty(E) < 0$ und $v_\infty((E)^{-1}) < 0$ unterscheiden wir weiter*
  - *falls $v_\infty(e_1) \geq 0$ und $v_\infty(e_3) < 0$: genau dann, wenn 1 und 4 gelten,*
  - *falls $v_\infty(e_1) < 0$ und $v_\infty(e_3) \geq 0$: genau dann, wenn 2 und 3 gelten.*

5 Anwendungen für t-Moduln

Wir fassen in diesem Kapitel die Ergebnisse der Untersuchungen aus Kapitel 4 noch einmal zusammen und stellen sie in Zusammenhang mit den Kriterien für die Uniformisierbarkeit von t-Moduln, wobei wir einfache Beispiele der Dimension $d = 1$ diskutieren.

5.1 Zusammenfassung der Ergebnisse

Im Folgenden sei stets $f(x) := f(x, y)$ wie in Definition 3.2.2, wobei $y \in \overline{K_\infty}$ nicht notwendigerweise fest gewählt ist.

Zu 4.1: Ein erweitertes Reduktionsverfahren

Im Abschnitt 4.1 haben wir ein erweitertes Reduktionsverfahren ähnlich der Hermite-Normalform hergeleitet. Wir zeigen, dass die Auflösbarkeit von $f(x)$ zu gegebenen y in eine Komponente x_d der Variable x auch in höheren Dimensionen immer möglich ist. Dieses Ergebnis ist nur bedingt hilfreich für die Untersuchung der Uniformisierbarkeit von t-Moduln. Zwar ist die Auswertung des Newton-Polygons in einem konkreten Fall möglich, aber umgekehrt ist das Herleiten von notwendigen und hinreichenden Bedingungen nur prinzipiell durchführbar. Selbst in Dimension $d = 2$ ist die Komplexität der Terme in den Koeffizienten der Auflösung $f_*(x_d) = 0$ bereits so hoch, dass in der Arbeit [Bangert; 2011, Kapitel 4] nur entweder notwendige oder hinreichende Bedingungen für die jeweils einfachsten Formen des Newton-Polygons abgeleitet werden konnten.

Eine heuristische Betrachtung zeigt, dass $\deg(f_*(x_d)) = q^{2d}$ ist (was sich ebenfalls aus theoretischen Überlegungen durch Lemma 3.1.4 ergibt), und dass die Anzahl der Summanden in den Koeffizienten exponentiell anwächst.

Zu 4.2: Anwendung des Henselschen Lemmas

Das Henselsche Lemma hat im Vergleich zum Newton-Polygon den Vorteil, dass es sich in mehreren Variablen anwenden lässt. Zudem zeigt Satz 4.2.4, dass sobald ein Folgenglied eines Folgenanfangs $\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_k \in L^d$ die Bedingungen von Satz 4.2.3 erfüllt, sich dieser Folgenanfang zu einem Element in $M\langle\langle t\rangle\rangle_f^\tau$ fortsetzen lässt. Jedoch sind die Bedingungen des Satzes sehr stark. Wir können das Ergebnis wie folgt zusammenfassen:

5.1.1 Bemerkung. *Ein t-Modul E ist genau dann uniformisierbar, wenn es zu jeder Startlösung $\underline{x}_0$ mit $f(\underline{x}_0, 0) = 0$ eine Folge von Fortsetzungen $\underline{x}_0, \underline{x}_1, \ldots, \underline{x}_k$ gibt, so dass $y = \underline{x}_k$ die Voraussetzung von Satz 4.2.3 erfüllt. Unter diesen Bedingungen lässt sich Satz 4.2.3 wiederholt anwenden und garantiert, dass es in jedem Schritt eine Nullstelle $\underline{x}_{k+1}$ im gleichen Körper mit $v_\infty(\underline{x}_{k+1}) \geq v_\infty(\underline{x}_k) + \frac{1}{q}$ gibt.*

Ein Vergleich mit der aufgelösten Gleichung aus Abschnitt 4.1 zeigt, dass sich Satz 4.2.3 nur dann anwenden lässt, wenn das Newton-Polygon eine Strecke mit den Endpunkten $(0, v_\infty(a_0))$ und $(1, v_\infty(a_1))$ hat. Aus dem folgenden Beispiel im eindimensionalen Fall $d = 1$ wird schnell klar, dass die interessanten Fälle, in denen das Newton-Polygon in diesem Bereich nicht abknickt, nicht ohne Weiteres erfasst werden können. Es gibt Fälle, in denen endlich oft ein Anwachsen der Bewertung um $\frac{1}{q}$ eintritt (siehe Bemerkung 3.2.4), ohne dass das Newton-Polygon seine prinzipielle Gestalt ändert.

5.1.2 Beispiel. *Wir betrachten den t-Modul E der Dimension $d = 1$ gegeben durch*

$$t = \tau^2 + a\tau + \theta,$$

das heißt, E ist ein Drinfeld-Modul und damit stets uniformisierbar. Wir wählen a, so dass $v_\infty(a) := -\frac{q^2}{q+1}$ ist, und eine Startlösung $\underline{x}_0$ mit $v_\infty(\underline{x}_0) = -\frac{q}{q^2-1}$. Letztere können wir an dem Newton-Polygon von $f(x, 0)$ ablesen.
Für das nächste Folgenglied hat $f(x, \underline{x}_0)$ dann genau q Fortsetzungen $\underline{x}_1$ mit gleicher Bewertung $v_\infty(\underline{x}_1) > v_\infty(\underline{x}_0)$, was wir an dem Newton-Polygon von $f(\underline{x}_1, \underline{x}_0)$ sehen. Diese Lösungen lassen sich danach eindeutig mit Satz 4.2.3 fortsetzen.

Zu 4.3: Rekursive Polynomgleichungen

Die rekursiv definierten q-Polynome $f_{(k)}(x, y)$ bringen keine Vorteile für die in dieser Arbeit betrachteten Methoden zur Untersuchung der speziellen Polynomgleichungen.

Die Auflösung in eine Variable mit dem Vorgehen in Abschnitt 4.1 ist durch den erhöhten Grad nicht sinnvoll und auch das Henselsche Lemma ist zur Lösung ebenfalls kein geeignetes Mittel, wie das folgende Beispiel zeigt:

5.1.3 Beispiel. *Wir betrachten noch einmal das Beispiel 5.1.2. Wenn wir die iterierten Polynome $f_{(k)}(\underline{x}_k, \underline{x}_0)$ für $k \geq 1$ betrachten, werden wir Satz 4.2.3 nicht direkt anwenden können. Denn für das k-te Folgenglied gibt es nur genau eine Fortsetzung zu jeder der q möglichen Fortsetzungen des $(k-1)$-ten Folgenglieds, wobei diese alle die gleiche Bewertung haben. Damit hat das Newton-Polygon in diesem Fall keine Strecke mit den Endpunkten $(0, v_\infty(a_0))$ und $(1, v_\infty(a_1))$, weshalb sich das Henselsche Lemma nicht anwenden lässt.*

Zu 4.4: Zusammensetzungen von Polynomgleichungen

Die hinreichenden Bedingungen $v_\infty(M) > 0$ bzw. $v_\infty(M^{-1}) > 0$ für die Lösbarkeit von Problem 4.4.3 lassen sich nicht direkt für die Herleitung von Kriterien für die Uniformisierbarkeit eines t-Moduls einsetzen. Jedoch ist dieser Ansatz vielversprechend, was der Spezialfall der Antidiagonalgleichungen zeigt.

Ein prinzipielles Problem ist hierbei, dass die Voraussetzung $v_\infty(a) \geq 0$ und die Annahme, dass der Bewertungsanstieg $c = \frac{1}{q}$ beträgt, nur noch hinreichende Bedingungen erlauben, wie wir in der Diskussion von Problem 3.2.3 gesehen haben.

Zu 4.5: Antidiagonalgleichungen in Dimension $d = 2$

Die notwendigen und hinreichenden Kriterien in Satz 4.5.10 in dem Spezialfall, in dem M eine Antidiagonalmatrix ist, sind ein guter Ausgangspunkt, um Kriterien für die Uniformisierbarkeit eines t-Moduln mit $t = \tau^2 + A\tau + \theta\tau^0$ zu finden, bei denen A eine Antidiagonalmatrix ist. Die Matrix B der transformierten Gleichung in Problem 4.4.2 ist dann ebenfalls eine Antidiagonalmatrix und lässt sich damit als Produkt von Antidiagonalmatrizen M_1 und M_2 der Teilprobleme 4.4.3 darstellen.
Wir bemerken an dieser Stelle noch einmal, dass wir die Voraussetzung $v_\infty(a) \geq 0$ für die notwendigen und hinreichenden Kriterien in diesem Spezialfall nicht benötigt haben. Falls sich zeigen ließe, dass der Bewertungsanstieg hier tatsächlich immer $c = \frac{1}{q}$ beträgt, ist die Zusammensetzung von zwei Problemen 4.4.3 äquivalent zu Problem 4.4.1.

Insbesondere ist das Beispiel von Anderson und Coleman (Beispiel 2.3.6) mit einer Antidiagonalmatrix gegeben, weshalb dies ein guter Ausgangspunkt ist, eine geeignete Beispielfamilie von t-Moduln zu finden, deren Bedingungen für die Uniformisierbarkeit sich durch notwendige und hinreichende Kriterien mit den in Abschnitt 4.5 bewiesenen Ergebnissen beschreiben lassen.

Literaturverzeichnis

[Anderson 1986] ANDERSON, Greg W.: t-Motives. In: *Duke Math. J.* 53 (1986), S. 457–502

[Bangert 2011] BANGERT, Oliver: *Uniformisierbarkeit in Familien von abelschen t-Moduln höheren Ranges*, Universität Kassel, Dissertation, 2011

[Böckle und Hartl 2007] BÖCKLE, Gebhardt ; HARTL, Urs: Uniformizable families of t-motives. In: *Trans. Amer. Math. Soc.* 359(8) (2007), S. 3933–3972

[Cohen 1993] COHEN, Henri: *A Course in Computational Algebraic Number Theory.* Springer, 1993

[Drinfeld 1974] DRINFELD, Vladimir G.: Elliptic modules. In: *Mat. Sb. (N.S.)* 94(136) (1974), S. 594–627,656

[Fisher 1997] FISHER, Benji: A Note on Hensel's Lemma in Several Variables. In: *Proc. Amer. Math. Soc.* 125 (1997)

[Goss 1996] GOSS, David: *Basic Structures of Function Field Arithmetic.* Springer, 1996

[Humphreys 1975] HUMPHREYS, James E.: *Linear Algebraic Groups.* Springer, 1975

[Matsumura 1986] MATSUMURA, Hideyuki: *Commutative ring theory.* Cambridge University Press, 1986

[Neukirch 1992] NEUKIRCH, Jürgen: *Algebraische Zahlentheorie.* Springer, 1992

[Steinberg 1968] STEINBERG, Robert: Endomorphisms of linear algebraic groups. In: *Memoirs of the American Mathematical Society* 80 (1968)

[Washington 2003] WASHINGTON, Lawrence C.: *Elliptic curves. Number theory and cryptography.* CRC Press, 2003