Diplomarbeit
–Charakteristische Polynome von Drinfeld-Moduln–

Florian Jung

Dezember 2000

Ich erkläre hiermit an Eides statt, diese Arbeit selbstständig geschrieben und keine Hilfsmittel außer den angegebenen verwendet zu haben.

Inhaltsverzeichnis

Einleitung **9**

1 Grundlagen **13**

1.1 Grundlagen aus der algebraischen Zahlentheorie und der Theorie der Funktionenkörper . . . 13
1.1.1 Stellen und Bewertungen . . . 13
1.1.2 Norm und Spur über endlichen Körpern . . . 17
1.1.3 Vervollständigung . . . 18
1.1.4 Der rationale Funktionenkörper $\mathbb{F}_q(T)$ . . . 20
1.2 Grundlagen der Theorie der Drinfeld-Moduln . . . 22
1.2.1 Additive Polynome . . . 22
1.2.2 Arithmetik in $L\{\tau\}$ . . . 26
1.2.3 Drinfeld-Moduln . . . 28
1.2.4 Teilungspunkte . . . 30

2 Arithmetik von Drinfeld-Moduln **33**

2.1 Morphismen von Drinfeld-Moduln . . . 33
2.2 Der Endomorphismenring . . . 35
2.3 Der Tate-Modul . . . 38
2.4 Reduktion von Drinfeld-Moduln . . . 40

3 Rang 2 Drinfeld-Moduln **43**

3.1 Isomorphien von Rang 2 Drinfeld-Moduln . . . 43
3.2 Berechnung der Koeffizienten von ϕ_a . . . 49
3.3 Die Hasse-Invariante . . . 52

4 Das charakteristische Polynom **55**

4.1 Theoretische Grundlagen . . . 55
4.2 Berechnung des charakteristischen Polynoms . . . 61
4.2.1 Die Berechnung von ε_ϕ . . . 63
4.2.2 Die Berechnung des maximalen Koeffizienten von a . . . 66
4.2.3 Die Berechnung von a mit Hilfe der Hasse-Invarianten . . . 70

4.2.4 Das Verhalten des charakteristischen Polynoms unter $\overline{L}$-Isomorphie . . . 71

5 Verteilungen von charakteristischen Polynomen **75**
5.1 Umfang und Durchführung der Berechnungen im Fall (a) . . . 76
5.1.1 Übersicht . . . 76
5.1.2 Der Algorithmus . . . 77
5.2 Ergebnisse und Beobachtungen im Fall (a) . . . 80
5.2.1 Verteilungen für festes $\mathfrak{p}$ . . . 80
5.2.2 Verteilungen des Faktors ε_ϕ . . . 82
5.2.3 Verteilungen des Koeffizienten a . . . 82
5.2.4 Verteilungen für alle $\mathfrak{p}$ eines festen Grades . . . 88
Verteilung der Drinfeld-Moduln mit $g = 0$ . . . 91
5.3 Der Fall (b) . . . 93
5.4 Umfang und Durchführung der Berechnungen im Fall (c) . . . 94
5.4.1 Übersicht . . . 94
5.4.2 Der Algorithmus . . . 94
5.5 Ergebnisse und Beobachtungen im Fall (c) . . . 96
5.5.1 Verteilung der Grade für alle $\mathfrak{p}$ eines festen Grades . . . 96
5.5.2 Verteilungen der a für alle $\mathfrak{p}$ eines festen Grades . . . 98
5.6 Implementierung . . . 101

A Tabellen Fall (a) **105**
A.1 Verteilungen für eine feste Stelle $\mathfrak{p}$ . . . 105
A.2 Verteilungen für alle Stellen eines festen Grades . . . 109
A.2.1 Zusammenfassung nach dem maximalen Koeffizienten . . . 114

B Tabellen Fall (b) **119**

C Tabellen Fall (c) **121**
C.1 Verteilungen für alle Stellen eines festen Grades . . . 121

Literaturverzeichnis **129**

Index **131**

Tabellenverzeichnis

5.1 Übersicht der Berechnungen im Fall (a) 76
5.6 Übersicht der Berechnungen im Fall (c) 94
5.7 Werte von $|\mathcal{M}_\phi(d)|$ und $|\mathcal{N}_\phi(d)|$ 97

A.1 Verteilung $q = 3$, $\mathfrak{p}$ vom Grad 4 und 5 105
A.2 Verteilung $q = 5$, $\mathfrak{p}$ vom Grad 4 und 5 107
A.3 Verteilung $q = 2$, alle $\mathfrak{p}$ vom Grad 8 109
A.4 Verteilung $q = 2$, alle $\mathfrak{p}$ vom Grad 9 110
A.5 Verteilung $q = 3$, alle $\mathfrak{p}$ vom Grad 6 111
A.6 Verteilung $q = 3$, alle $\mathfrak{p}$ vom Grad 7 114
A.7 Vergleich von $\mathsf{H}(a, q, d)$ und $\widetilde{\mathsf{C}}(a) \cdot {}_{gl}\mathsf{H}(a, q, d)$ 116

B.1 Verteilung für $\mathbb{F}_{\mathfrak{p}^6}$ und $\mathbb{F}_{\mathfrak{p}^7}$ 119

C.1 Verteilung für $\phi^{(29)}$, alle $\mathfrak{p}$ vom Grad 24 und vom Grad 25 121
C.2 Verteilung für $\phi^{(33)}$, alle $\mathfrak{p}$ vom Grad 14 und vom Grad 15 124
C.3 Verteilung für $\phi^{(23)}$, alle $\mathfrak{p}$ vom Grad 20 und vom Grad 21 126
C.4 Verteilung für $\phi^{(23)}$, alle $\mathfrak{p}$ vom Grad 22 und vom Grad 23 126

Einleitung

Die Theorie der algebraischen Funktionenkörper in endlicher Charakteristik, wie z. B. des rationalen Funktionenkörpers über dem Körper mit q Elementen $\mathbb{F}_q(T)$, weist in vielerlei Hinsicht Analogien zur klassischen Zahlentheorie auf, d. h. der Theorie der Zahlkörper über $\mathbb{Q}$. So lassen sich viele Aussagen direkt in den Kontext der Funktionenkörper übertragen, wenn man die Objekte $\mathbb{Z}$, $\mathbb{Q}$ und $\mathbb{R}$ durch $A = \mathbb{F}_q[T]$, $K = \mathbb{F}_q(T)$ sowie K_∞ (die Komplettierung von K an der Stelle $(\frac{1}{T})$) ersetzt. Ein wesentlicher Unterschied zu $\mathbb{Q}$ besteht jedoch in der durch den Frobeniusendomorphismus gegebenen Struktur im Fall endlicher Charakteristik. Durch dessen Existenz wird die Definition nicht-trivialer A-Modulstrukturen auf K ermöglicht, die keine direkte Analogie in Charakteristik Null besitzen. Solche Modulstrukturen mit gewissen Eigenschaften wurden 1974 von V.G. Drinfeld eingeführt und diese nach ihm benannten *Drinfeld-Moduln* spielen seitdem eine wichtige Rolle in der Arithmetik von Funktionenkörpern.
Schon in den 30er Jahren definierte Carlitz, im Bestreben eine Art von Exponentialfunktion in endlicher Charakteristik einzuführen, den einfachsten Fall eines Drinfeld-Moduls. Die arithmetischen Eigenschaften des *Carlitz-Moduls* ermöglichten es, eine vollständige Analogie der Kreisteilungserweiterungen über $\mathbb{Q}$ und deren Funktion für die Klassenkörpertheorie zu formulieren.

Die vorliegende Arbeit beschäftigt sich mit dem nächst höheren Fall, nämlich mit Drinfeld-Moduln des Ranges 2. Für solche Drinfeld-Moduln über Körpern L endlicher $\mathfrak{p}$-Charakteristik, d. h. L ist eine endliche Erweiterung von $\mathbb{F}_\mathfrak{p} = \mathbb{F}_q[T]/\mathfrak{p}$, wird das charakteristische Polynom des zugehörigen Frobenius $\mathcal{F}_L$ bzgl. ϕ untersucht. Dieses Polynom ist eine Isogenieklasseninvariante und hat die Form $P_\phi(X) = X^2 + aX + b$ mit Koeffizienten a, b aus A. Das Absolutglied b ist bis auf einen Faktor aus $\mathbb{F}_q$ durch $\mathfrak{p}$ gegeben und a hat einen beschränkten Grad.
Es gibt verschiedene Möglichkeiten, Verteilungen von charakteristischen Polynomen zu untersuchen.

Zum einen kann man über dem endlichen Körper L alle Drinfeld Moduln betrachten und miteinander vergleichen. Dies kann man für verschiedene Charakteristiken $\mathfrak{p}$ durchführen (Fall (a)).

Eine zweite Möglichkeit ist, von einem festen Körper $\mathbb{F}_\mathfrak{p}$ auszugehen und dann die charakteristischen Polynome aller Drinfeld-Moduln über den Erweiterungen $\mathbb{F}_{\mathfrak{p}^m}$ zu untersuchen (Fall (b)).

Ein weiterer Ansatz besteht darin, einen globalen Drinfeld-Modul über dem Körper K an allen Stellen mit guten Eigenschaften zu reduzieren und die charakteristischen Polynome der lokalen Drinfeld-Moduln über den endlichen Körpern $\mathbb{F}_{\mathfrak{p}}$ zu berechnen (Fall (c)).

In den Artikeln [Yos73], [Bir68] und [Tat65] werden Untersuchungen im analogen Fall von elliptischen Kurven durchgeführt. Das Absolutglied des dort untersuchten charakteristischen Polynoms ist immer gleich der Primzahl p, an der reduziert wird, und die Frobeniusspur enthält die Information über die Anzahl der Punkte der endlichen Kurve. Es wird die Vermutung aufgestellt und zum Teil bewiesen, dass sich in allen Fällen gleichartige Verteilungen der Frobeniusspuren (nach geeigneter Normierung) ergeben.
Auch in unserem Fall enthält das charakteristische Polynom Informationen über den Körper L, wie z. B. seine Euler-Poincaré-Charakteristik, so dass es bei der Konstruktion von L-Reihen und Zeta-Funktionen eine wichtige Rolle spielt.

Den Ausgangspunkt der Arbeit bilden umfangreiche Berechnungen in den oben beschriebenen Situationen. Anhand derer war es möglich, einen Eindruck über das Verhalten des charakteristischen Polynoms zu gewinnen, bestimmte Aussagen darüber zu beweisen und Vermutungen über Gesetzmäßigkeiten zu formulieren.
Besonders eingehende Berechnungen finden in Fall (a) statt. Hier lassen sich am systematischsten alle Fälle bis zu einer gewissen Stufe ausrechnen und man erhält sehr aussagekräftiges Datenmaterial. In den beiden anderen Fällen muss man sich durch die Wahl eines festen $\mathbb{F}_{\mathfrak{p}}$ bzw. eines festen globalen Drinfeld-Moduls auf Einzelsituationen beschränken, so dass eine Verallgemeinerung der Beobachtungen schwierig ist.

In Kapitel 1 und 2 werden die Grundlagen aus der algebraischen Zahlentheorie bereitgestellt und in die Theorie der Drinfeld-Moduln eingeführt. Kapitel 3 widmet sich den speziellen Eigenschaften von Rang 2 Drinfeld-Moduln und enthält einige grundlegende Sachverhalte, die im weiteren Verlauf sowohl für theoretische Aussagen als auch für die numerischen Untersuchungen, benötigt werden. In Kapitel 4 wird das charakteristische Polynom eingeführt und, den Artikeln [Gek91] und [GS96] folgend, die theoretischen Aussagen über seine Eigenschaften wiedergegeben. Der zweite Abschnitt geht dann der Frage nach, wie es sich berechnen lässt. Es wird eine aus [HY00] abgeleitete Formel für das Signum des Absolutglieds b angegeben und beschrieben, wie man die Frobeniusspur a berechnen kann. Die ebenfalls aus [HY00] bekannte Formel für den „maximal möglichen" Koeffizienten von a im Fall „$\deg \mathfrak{p}$" gerade wird gezeigt und eine analoge Formel für den Fall, dass $\deg \mathfrak{p}$ ungerade ist, bewiesen.
Kapitel 5 beinhaltet die Untersuchungen der oben beschriebenen Verteilungen. Es wird für bestimmte Polynome gezeigt –im Fall (a) und Fall (b) gleichermaßen geltend– dass sie nicht als charakteristische Polynome auftreten können. Danach wird allein der Koeffizient a betrachtet und eine Aussage über das Verhältnis

zwischen den a mit maximalem Grad und denen mit kleinerem Grad gemacht.
Für den Fall (a) wird im Weiteren das Auftreten der Frobeniusspuren unter Einbeziehung aller Primstellen eines festen Grades untersucht und vermutet, dass sich die Häufigkeit eines bestimmten a mit Hilfe einer Konstanten beschreiben lässt, die einzig von der Anzahl der Nullstellen von a über $\mathbb{F}_q$ abhängt.
Die Untersuchungen in Fall (c) zeigen, dass eine Mehrzahl der Beispiele von globalen Drinfeld-Moduln ein „lokal zufälliges" Verhalten zeigen, d. h. die Menge der reduzierten Drinfeld-Moduln verteilt sich analog den Gesetzmäßigkeiten, die in Fall (a) für alle endlichen Drinfeld-Moduln beobachtet wurden. Hierzu Vermutungen allgemeiner Natur aufzustellen, scheint aufgrund der wenigen berechneten Beispiele jedoch sehr gewagt.

An dieser Stelle möchte ich mich bei allen bedanken, die mich beim Anfertigen dieser Arbeit unterstützt haben. Mein großer Dank gilt Herrn Prof. Dr. E.-U. Gekeler für das interessante Thema und die hervorragende Betreuung. Dies gilt in gleichem Maße für alle Mitarbeiter des Lehrstuhls. Insbesondere bedanke ich mich bei Herrn Dipl.-Math M. Gebhardt für die große Hilfe zu Fragen der Programmierung, das Korrekturlesen und den wertvollen fachlichen Gedankenaustausch. Ich bedanke mich außerdem bei meiner Freundin Melanie für fortwährenden Beistand und Ermutigung, sowie bei meiner Familie, von denen ein jeder auf seine Weise zum Gelingen dieser Arbeit beigetragen hat.

Kapitel 1

Grundlagen

1.1 Grundlagen aus der algebraischen Zahlentheorie und der Theorie der Funktionenkörper

In diesem Abschnitt werden die für die Arbeit relevanten Hilfsmittel aus der algebraischen Zahlentheorie bereitgestellt und die grundlegenden Aussagen über die Arithmetik von Funktionenkörpern wiedergeben. Dabei liegt der Schwerpunkt in der Einführung der Bezeichnungen und Definitionen. Es wird nicht versucht, eine umfassende Darstellung dieser Sachverhalte zu geben. Hierzu sei auf die Literatur verwiesen ([Koc97], [Neu92], [Ser79] und [Sti93]).
Die Begrifflichkeit der algebraischen Zahlentheorie wird anhand der Situation erläutert, in deren Rahmen sich die Problemstellungen dieser Arbeit bewegen. Dieses ist die der **algebraischen Funktionenkörper in einer Variablen über einem endlichen Körper der Charakteristik p**.

Sei p eine Primzahl, $q = p^l$ für eine natürliche Zahl l, dann bezeichnet $\mathbb{F}_q$ den endlichen Körper mit q Elementen. Dieser ist vollkommen und hat die Charakteristik p.
Eine Erweiterung $K/\mathbb{F}_q$ heißt *algebraischer Funktionenkörper über* $\mathbb{F}_q$, falls ein transzendentes Element $x \in K$ existiert, so dass K eine endliche, algebraische Erweiterung von $\mathbb{F}_q(x)$ ist.
Ist $K = \mathbb{F}_q(x)$ für ein transzendentes Element $x \in K$, so heißt K *rationaler Funktionenkörper über* $\mathbb{F}_q$.

1.1.1 Stellen und Bewertungen

1.1.1 Definition. *Ein Ring* $\mathcal{O} \subseteq K$ *mit den Eigenschaften*

(i) $\mathbb{F}_q \subsetneqq \mathcal{O} \subsetneqq K$, *und*

(ii) *für alle* $x \in K$ *gilt* $x \in \mathcal{O}$ *oder* $x^{-1} \in \mathcal{O}$, *heißt ein* Bewertungsring *von K.*

Der Bewertungsring $\mathcal{O}$ ist ein lokaler Ring mit dem maximalen Ideal $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^*$. Dieses ist darüber hinaus ein Hauptideal, so dass $\mathcal{O}$ ein *diskreter Bewertungsring ist.*

1.1.2 Definition. (i) *Eine* Stelle $\mathfrak{p}$ *des algebraischen Funktionenkörpers $K/\mathbb{F}_q$ ist das maximale Ideal eines Bewertungsrings $\mathcal{O} \subseteq K$.*

(ii) *Mit $S(K) := \{\mathfrak{p} \mid \mathfrak{p}$ ist eine Stelle von $K/\mathbb{F}_q\}$ wird die Menge der Stellen von $K/\mathbb{F}_q$ bezeichnet.*

(iii) *Ein Element $\pi \in \mathfrak{p}$ mit $\pi\,\mathcal{O} = \mathfrak{p}$ heißt eine* Uniformisierende *von $\mathfrak{p}$.*

(iv) *Der Körper $\mathcal{L}_\mathfrak{p} := \mathcal{O}/\mathfrak{p}$ heißt* Restklassenkörper von $\mathcal{O}$ bzgl. $\mathfrak{p}$.

(v) *Man nennt* $\deg \mathfrak{p} := [\mathcal{L}_\mathfrak{p} : \mathbb{F}_q]$ *den* Grad *der Stelle $\mathfrak{a}$.*

Der Bewertungsring $\mathcal{O}$ mit dem maximalen Ideal $\mathfrak{p}$ ist wegen $\mathcal{O} = \{x \in K| : x^{-1} \notin \mathfrak{p}\}$ durch dieses schon eindeutig bestimmt, so dass die Stellen eineindeutig den Bewertungsringen entsprechen. Deshalb wird $\mathcal{O}_{(\mathfrak{p})} := \mathcal{O}$als der *Bewertungsring zu der Stelle* $\mathfrak{p}$ bezeichnet.

Der Begriff der Stelle lässt sich auch mittels der diskreten Bewertungen einführen.

1.1.3 Definition. *Eine* diskrete Bewertung *von $K/\mathbb{F}_q$ ist eine Funktion $\nu : K \to \mathbb{Z} \cup \{\infty\}$ mit den folgenden Eigenschaften:*

(i) $\nu(x) = \infty \;\Leftrightarrow\; x = 0.$

(ii) $\nu(x\,y) = \nu(x) + \nu(y)$ *für alle $x, y \in K$.*

(iii) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ *für alle $x, y \in K$.*

Eine Bewertung heißt *normiert*, falls $\nu(K^*) = \mathbb{Z}$ ist.

Für eine diskrete Bewertung ν erhält man durch die Definition $|x| := (\frac{1}{q})^{\nu(x)}$ für $x \in K$ eine *Betragsbewertung*, d. h. eine Abbildung $|.| : K \to \mathbb{R}_{\geq 0}$ mit den Eigenschaften:

(i) $|x| = 0 \;\Leftrightarrow\; x = 0.$

(ii) $|x\,y| = |x|\,|y|$ für alle $x, y \in K$.

(iii) $|x + y| \leq |x| + |y|$ für alle $x, y \in K$.

Eine diskrete Bewertung ν heißt *trivial*, falls gilt:

$$\nu(x) = \begin{cases} 0 & \text{für } x \neq 0 \\ \infty & \text{für } x = 0. \end{cases}$$

Sei ν eine diskrete Bewertung von $K/\mathbb{F}_q$, dann ist $\nu_{|\mathbb{F}_q}$ trivial.

Durch die Angabe einer Stelle $\mathfrak{p} \in S(K)$ lässt sich eine diskrete Bewertung $\nu_\mathfrak{p}$ wie folgt definieren.
Sei π eine Uniformisierende von $\mathfrak{p}$, dann hat jedes $x \in K^*$ eine eindeutige Darstellung $x = \pi^{n(x)} \cdot u$ mit $u \in \mathcal{O}^*_{(\mathfrak{p})}$ und $n(x) \in \mathbb{Z}$. Durch die folgende Definition ist eine diskrete Bewertung auf $K/\mathbb{F}_q$ gegeben:

$$\begin{aligned} \nu_\mathfrak{p} :\ K &\longrightarrow \mathbb{Z} \cup \{\infty\} \\ x &\longmapsto \begin{cases} n(x) & x \neq 0 \\ \infty & x = 0. \end{cases} \end{aligned}$$

Umgekehrt erhält man für eine diskrete Bewertung ν einen Bewertungsring $\mathcal{O}_{(\nu)}$ mit maximalem Ideal $\mathfrak{p}$ durch:

$$\begin{aligned} \mathcal{O}_{(\nu)} &:= \{x \in K \mid \nu(x) \geq 0\}, \\ \mathcal{O}^*_{(\nu)} &:= \{x \in K \mid \nu(x) = 0\}, \\ \mathfrak{p} &:= \{x \in K \mid \nu(x) > 0\}. \end{aligned}$$

Diskrete Bewertungen heißen *äquivalent*, wenn sie den gleichen Bewertungsring definieren, und die Äquivalenzklassen werden repräsentiert von den normierten diskreten Bewertungen.
Damit entsprechen die Stellen von K eineindeutig den normierten diskreten Bewertungen, so dass diese Begriffe im Folgenden synonym verwendet werden.

Es gilt die folgende fundamentale Formel für die Stellen von $K/\mathbb{F}_q$:

1.1.4 Proposition. *Sei $\alpha \in K$, dann gilt $\nu_\mathfrak{p}(\alpha) = 0$ für fast alle $\mathfrak{p} \in S(K)$ und zusätzlich*

$$\sum_{\mathfrak{p} \in S(K)} \deg \mathfrak{p}\, \nu_\mathfrak{p}(\alpha) = 0.$$

Beweis. Siehe [Koc97, Satz 5.2.1]. ❑

Durch die Wahl einer beliebigen Stelle $\infty \in S(K)$ definiert man einen Unterring A von K

$$A := \bigcap_{\substack{\mathfrak{p} \in S(K) \\ \mathfrak{p} \neq \infty}} \mathcal{O}_{(\mathfrak{p})} = \{x \in K \mid \nu(x) \geq 0 \text{ für alle } \nu \in S(K) \text{ mit } \nu \neq \nu_\infty\}, \tag{1.1}$$

der die folgenden Eigenschaften besitzt:

(i) A ist Dedekind-Ring.

(ii) K ist der Quotientenkörper von A.

(iii) Die Elemente von $S(K)$ entsprechen eineindeutig denen der Menge $\{\mathfrak{p} \mid 0 \neq \mathfrak{p} \text{ ist Primideal von } A\} \cup \{\infty\}$.

Für die Elemente von A wird auf folgende Weise eine Gradfunktion eingeführt:

$$\begin{aligned} \deg \,:\, A &\longrightarrow \mathbb{Z} \\ a &\longmapsto \log_q |(A/(a)| = -(\deg\infty \cdot \nu_\infty(a)). \end{aligned} \tag{1.2}$$

Es sei nun E/K eine endliche Körpererweiterung von K. Mit $\mathfrak{P} \in S(E)$ sei eine Stelle von E und mit $\mathfrak{p} \in S(K)$ sei eine Stelle von K bezeichnet. Wenn für diese beiden Stellen $\mathcal{O}_{(\mathfrak{p})} \subset \mathcal{O}_{(\mathfrak{P})}$ gilt, dann sagt man „$\mathfrak{P}$ liegt über $\mathfrak{p}$“ bzw. „$\mathfrak{P}$ teilt $\mathfrak{p}$“ und schreibt dies in der Form $\mathfrak{P} \mid \mathfrak{p}$.
Die zugehörige Bewertung $\nu_\mathfrak{P}$ von E heißt dann eine *Fortsetzung* der Bewertung $\nu_\mathfrak{P}$ von K.

1.1.5 Definition. *Sei $\mathfrak{P}$ eine Stelle aus E, die über der Stelle $\mathfrak{p}$ aus K liegt, dann heißt die Zahl $e_\mathfrak{P}(E/K)$, für die gilt*

$$e_\mathfrak{P}(E/K)\nu_\mathfrak{p}(x) = \nu_\mathfrak{P}(x) \quad \textit{für alle } x \in K,$$

der Verzweigungsindex von $\mathfrak{P}$ in E/K.
Der Grad der Erweiterung der Restklassenkörper

$$f_\mathfrak{P}(E/K) := [\mathcal{L}_\mathfrak{P} : \mathcal{L}_\mathfrak{p}] = [\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P} : \mathcal{O}_{(\mathfrak{p})}/\mathfrak{p}]$$

wird als der Trägheitsindex von $\mathfrak{P}$ in E/K *oder auch als der* Restklassengrad von $\mathfrak{P}$ in E/K *bezeichnet.*

Es gilt die folgende fundamentale Beziehung zwischen den Grad einer separablen Körpererweiterung und den Verzweigungsindizes und Trägheitsgraden einer Stelle aus K:

1.1.6 Proposition. *Sei E/K separabel und $\mathfrak{p} \in S(K)$, dann gilt:*

$$[E : K] = \sum_{\mathfrak{P} \mid \mathfrak{p}} e_\mathfrak{P}(E/K) f_\mathfrak{P}(E/K).$$

Beweis. Siehe [Neu92, Satz 8.5]. ❑

1.1.2 Norm und Spur über endlichen Körpern

Für eine endliche Erweiterung E/K führt man die *Spur* und die *Norm* eines Elements $x \in E$ ein, indem man E als K-Vektorraum mit der durch Multiplikation mit x gegebenen Transformation auffasst.

$$\begin{aligned} \mathsf{T}_x \, : \, E &\longrightarrow E \\ \mathsf{T}_x(\alpha) &= x \cdot \alpha. \end{aligned}$$

Man definiert dann

$$\mathrm{N}_K^E(x) := \det(\mathsf{T}_x) \quad \text{und} \quad \mathrm{Tr}_K^E(x) := \mathrm{Tr}(\mathsf{T}_x).$$

Ist E/K separabel vom Grad n und sind $\sigma_1, \ldots, \sigma_n$ die verschiedenen K-Einbettungen von E in $\overline{K}$, dann gilt

$$\begin{aligned} \mathrm{N}_K^E(x) &= \prod_{i=1}^{n} \sigma_i(x), \\ \mathrm{Tr}_K^E(x) &= \sum_{i=1}^{n} \sigma_i(x). \end{aligned}$$

Damit erhält man für die Spur und die Norm in der Situation von endlichen Körpern die folgende Beschreibung.

Sei $E = \mathbb{F}_{q^n}$ und $K = \mathbb{F}_q$, dann ist $\mathbb{F}_{q^n}$ eine zyklische Erweiterung des Grades n von $\mathbb{F}_q$. Diese wird erzeugt von τ, dem Frobenius von $\mathbb{F}_q$, so dass gilt:

$$\begin{aligned} \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) &= x \cdot x^q \cdot \cdots \cdot x^{q-1} = x^{\frac{q^n-1}{q-1}}, \\ \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) &= x + x^q + \cdots + x^{q-1}. \end{aligned}$$

1.1.7 Proposition. *Die Normabbildung über endlichen Körpern hat die folgenden Eigenschaften:*

(i) $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha\,\beta) = \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha)\, \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\beta)$ *für alle* $\alpha, \beta \in \mathbb{F}_{q^n}$.

(ii) *Die Norm bildet* $\mathbb{F}_{q^n}$ *(bzw.* $\mathbb{F}_{q^n}^*$*) surjektiv auf* $\mathbb{F}_q$ *(bzw.* $\mathbb{F}_q^*$*) ab.*

(iii) $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(a) = a^n$ *für alle* $a \in \mathbb{F}_q$.

(iv) $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha^q) = \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha)$ *für alle* $\alpha \in \mathbb{F}_{q^n}$.

Beweis. Siehe [LN94, Theorem 2.23]. ❑

1.1.8 Proposition. *Die Spurabbildung über endlichen Körpern hat die folgenden Eigenschaften:*

(i) $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha+\beta) = \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha) + \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\beta)$ *für alle* $\alpha, \beta \in \mathbb{F}_{q^n}$.

(ii) $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(c\,\alpha) = c\ \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha)$ *für alle* $c \in \mathbb{F}_q, \alpha \in \mathbb{F}_{q^n}$.

(iii) *Die Spur bildet* $\mathbb{F}_{q^n}$ *surjektiv auf* $\mathbb{F}_q$ *ab.*

(iv) $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(a) = n\,a$ *für alle* $a \in \mathbb{F}_q$.

(v) $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha^q) = \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\alpha)$ *für alle* $\alpha \in \mathbb{F}_{q^n}$.

Beweis. Siehe [LN94, Theorem 2.28]. ❑

Da die Norm von $\mathbb{F}_{q^n}^*$ nach $\mathbb{F}_q^*$ und die Spur von $\mathbb{F}_{q^n}$ nach $\mathbb{F}_q$ surjektive Homomorphismen der additiven bzw. der multiplikativen Gruppe sind, gilt für die jeweiligen Urbildmengen unter diesen Abbildungen der folgende Sachverhalt:

$$\begin{aligned} |\,\{x \in \mathbb{F}_{q^n}^* \mid \mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) = a\}\,| &= \frac{q^n-1}{q-1} \quad \text{für alle } \ a \in \mathbb{F}_q^*, \text{ sowie} \\ |\,\{x \in \mathbb{F}_{q^n} \mid \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) = a\}\,| &= q^{n-1} \qquad \text{für alle } \ a \in \mathbb{F}_q. \end{aligned} \tag{1.3}$$

1.1.3 Vervollständigung

So wie sich der Körper $\mathbb{Q}$ bzgl. des Absolutbetrages $|\,.\,|$ zu $\mathbb{R}$ vervollständigen lässt, oder die p-adischen Beträge als Vervollständigungen die kompletten Körper $\mathbb{Q}_p$ liefern, so lassen sich mittels der Bewertungen auch im Funktionenkörperfall Vervollständigungen konstruieren.
Der algebraische Funktionenkörper K sei mit der Bewertung $\nu_\mathfrak{p}$ versehen und $\mathfrak{p}$ sei die zu $\nu_\mathfrak{p}$ gehörige Stelle aus $S(K)$. Durch $\nu_\mathfrak{p}$ ist auf K eine Metrik gegeben, so dass sich auf dem topologischen Raum K der Begriff der Cauchyfolge definieren lässt. Sei $K_\mathfrak{p}$ der Ring der Cauchyfolgen bzgl. $\nu_\mathfrak{p}$ modulo dem maximalen Ideal aller Nullfolgen. Bettet man die Elemente $x \in K$ als die konstanten Folgen $(x, x, \dots)$ in $K_\mathfrak{p}$ ein und definiert auf $K_\mathfrak{p}$ die kanonische Fortsetzung von $\nu_\mathfrak{p}$, die auch mit $\nu_\mathfrak{p}$ bezeichnet wird, und gegeben ist durch

$$\nu_\mathfrak{p}(\overline{(x_n)}_{n\geq 0}) := \lim_{n\to\infty} \nu_\mathfrak{p}(x_n) \quad \text{für } \overline{(x_n)}_{n\geq 0} \in K_\mathfrak{p},$$

so ist $K_\mathfrak{p}$ ein Körper mit den Eigenschaften

(i) K liegt dicht in $K_\mathfrak{p}$, und

(ii) $K_{\mathfrak{p}}$ ist vollständig bzgl. $\nu_{\mathfrak{p}}$.

$K_{\mathfrak{p}}$ heißt die *Vervollständigung von K an der Stelle* $\mathfrak{p}$.
Mit $\mathcal{O}_{\mathfrak{p}} \subset K_{\mathfrak{p}}$ wird der Bewertungsring und mit $\mathfrak{P}$ dessen maximales Ideal von $K_{\mathfrak{p}}$ bzgl. $\nu_{\mathfrak{p}}$ bezeichnet. Ist π eine Uniformisierende von $\mathcal{O}_{(\mathfrak{p})} \subset K$, so lässt sich $\mathcal{O}_{\mathfrak{p}}$ als projektiver Limes schreiben

$$\mathcal{O}_{\mathfrak{p}} = \varprojlim \mathcal{O}_{(\mathfrak{p})}/\pi^n \mathcal{O}_{(\mathfrak{p})}.$$

Außerdem gilt die Isomorphie

$$\mathcal{O}_{(\mathfrak{p})}/\pi^n \mathcal{O}_{(\mathfrak{p})} \simeq \mathcal{O}_{\mathfrak{p}}/\pi^n \mathcal{O}_{\mathfrak{p}} \quad \text{für } n \in \mathbb{N},$$

also insbesondere die Isomorphie der Restklassenkörper

$$\mathcal{L}_{\mathfrak{p}} = \mathcal{O}_{(\mathfrak{p})}/\mathfrak{p} \simeq \mathcal{O}_{\mathfrak{p}}/\mathfrak{P} = \mathcal{L}_{\mathfrak{P}}.$$

Sei $R \subseteq K_{\mathfrak{p}}$ ein Repräsentantensystem für $\mathcal{L}_{\mathfrak{p}}$, dann hat jedes Element von $K_{\mathfrak{p}}$ eine Darstellung

$$x = \sum_{i=n}^{\infty} a_i \pi^i \quad \text{mit } a_i \in R \text{ und } n \in \mathbb{Z}.$$

Der vollständige Körper $K_{\mathfrak{p}}$ hat die Eigenschaft, dass sich $\nu_{\mathfrak{p}}$ auf jede endliche Erweiterung eindeutig fortsetzen lässt und diese Erweiterung dann selbst wieder vollständig ist.

Sei E/K eine endliche Erweiterung vom Grad n und $r_{\mathfrak{p}}(E/K)$ bezeichne die Anzahl der verschiedenen Stellen aus E die über $\mathfrak{p} \in K$ liegen. Für diese Stellen $\mathfrak{P}_1, \ldots, \mathfrak{P}_{r_{\mathfrak{p}}(E/K)}$ seien

$$e_i = e_{\mathfrak{P}}(E/K) \quad \text{und} \quad f_i = f_{\mathfrak{P}}(E/K) \quad \text{für } 1 \leq i \leq r_{\mathfrak{p}}(E/K)$$

jeweils die Verzweigungs- und Trägheitsindizes. Der Körper E lässt sich bzgl. der Stellen $\mathfrak{P}_i$ vervollständigen, und diese Körper werden mit $E_{\mathfrak{P}_i}$ bezeichnet. Für jene Komplettierungen des Erweiterungskörpers gilt:

(i) $E_{\mathfrak{P}_i}$ ist eine Erweiterung von $K_{\mathfrak{p}}$ des Grades $n_i = e_i f_i$.

(ii) Die Bewertung $\nu_{\mathfrak{p}}$ besitzt die eindeutige Fortsetzung $e_i\, \nu_{\mathfrak{P}_i}$ auf $E_{\mathfrak{P}_i}$.

(iii) Der kanonische Homomorphismus

$$\varphi: \quad E \otimes_K K_{\mathfrak{p}} \longrightarrow \prod_{i=1}^{r_{\mathfrak{p}}(E/K)} E_{\mathfrak{P}_i}$$

ist ein Isomorphismus.

(iv) Für die Spur und die Norm eines Elements α aus E gilt:

$$\begin{aligned} \mathrm{Tr}_K^E(\alpha) &= \sum_{i=1}^{r_{\mathfrak{p}}(E/K)} \mathrm{Tr}_{K_{\mathfrak{p}}}^{E_{\mathfrak{P}_i}}(\alpha) \quad \text{und} \\ \mathrm{N}_K^E(\alpha) &= \prod_{i=1}^{r_{\mathfrak{p}}(E/K)} \mathrm{N}_{K_{\mathfrak{p}}}^{E_{\mathfrak{P}_i}}(\alpha). \end{aligned} \tag{1.4}$$

1.1.9 Proposition. *Sei ν eine Fortsetzung der Bewertung eines vollständigen Körpers L auf die endliche Erweiterung E/L vom Grad n. Dann gilt:*

$$n\,\nu(\alpha) = \nu(\mathrm{N}_L^E(\alpha)) \quad \textit{für } \alpha \in E.$$

Beweis. Siehe [Koc97, Satz 4.5.3]. ❑

1.1.4 Der rationale Funktionenkörper $\mathbb{F}_q(T)$

Anhand des für diese Arbeit relevanten (und einfachsten) Falles eines algebraischen Funktionenkörpers, dem rationalen Funktionenkörper über $\mathbb{F}_q$, sollen die eingeführten Begriffe konkretisiert werden. Dieser lässt sich für ein transzendentes Element T darstellen als $K = \mathbb{F}_q(T)$. Der rationale Funktionenkörper bildet in vieler Hinsicht ein Analogon zu dem Körper $\mathbb{Q}$ im Zahlkörperfall. Ein wesentlicher Unterschied besteht darin, dass $\mathbb{Q}$ eine nicht-archimedische Bewertung in Form des Absolutbetrages besitzt. Auf diese Weise wird $\mathbb{Z}$ als der Ring der ganzen Zahlen als Unterring von $\mathbb{Q}$ ausgezeichnet.
Im Funktionenkörperfall sind alle Bewertungen nicht-archimedisch, so dass die Wahl eines Unterrings von K, wie es in (1.1) geschieht, nicht kanonisch ist, sondern von der Wahl der Transzendenten T abhängt.

Die Stellen von $\mathbb{F}_\mathbf{q}(\mathbf{T})$

Die Bewertungsringe von $\mathbb{F}_q(T)$ sind bis auf eine Ausnahme von der Form

$$\mathcal{O}_{(p(T))} := \{\frac{f(T)}{g(T)} \mid f(T), g(T) \in K[T],\ p(T) \nmid g(T)\}, \tag{a}$$

mit dem maximalen Ideal

$$\mathfrak{p}_{(p(T))} = \{\frac{f(T)}{g(T)} \mid f(T), g(T) \in K[T],\ p(T) | f(T), p(T) \nmid g(T)\}$$

und dem Restklassenkörper

$$\mathcal{O}_{(p(T))}/\mathfrak{p}_{(p(T))} = \mathbb{F}_q[T]/p(T) \cong \mathbb{F}_{q^{\deg(p(T))}},$$

wobei $p(T) \in \mathbb{F}_q[T]$ ein irreduzibles Polynom ist.

Ein weiterer Bewertungsring ist gegeben durch:

$$\mathcal{O}_\infty := \{\frac{f(T)}{g(T)} \mid f(T), g(T) \in K[T],\ \deg f(T) \leq \deg g(T)\}, \tag{b}$$

mit dem maximalen Ideal

$$\mathfrak{p}_\infty = \{\frac{f(T)}{g(T)} \mid f(T), g(T) \in K[T],\ \deg f(T) < \deg g(T)\}$$

und dem Restklassenkörper

$$\mathcal{O}_\infty/\mathfrak{p}_\infty \cong \mathbb{F}_q.$$

Die Stellen von $\mathbb{F}_q(T)$ entsprechen also eineindeutig den normierten Primelementen von $\mathbb{F}_q[T]$ im Fall (a) und dem Element $(\frac{1}{T})$ im Fall (b). Dies sind zugleich auch Uniformisierende der jeweiligen Stellen. Im Fall (a) heißen die Stellen *endlich*, die zu $(\frac{1}{T})$ gehörige Stelle wird als ∞-*Stelle* bezeichnet.

Der Unterring A von $\mathbb{F}_q(T)$, den man aufgrund dieser Wahl der ∞-Stelle durch die Konstruktion in (1.1) erhält, ist der Polynomring in T, denn

$$A := \bigcap_{\substack{\mathfrak{p} \in S(K) \\ \mathfrak{p} \neq \infty}} \mathcal{O}_{(\mathfrak{p})} = \bigcap_{\substack{f(T) \in \mathbb{F}_q[T] \\ f(T) \text{prim}}} \mathcal{O}_{(p(T))} = \mathbb{F}_q[T]. \tag{1.5}$$

Die in (1.2) eingeführte Gradfunktion stimmt mit der üblichen Gradfunktion auf $\mathbb{F}_q[T]$ überein.

Den Stellen vom Typ (a) entsprechen die durch die irreduziblen Polynome gegebenen diskreten Bewertungen:

$$\begin{aligned} \nu_{p(T)} \, : \, \mathbb{F}_q(T) &\longrightarrow \mathbb{Z} \\ x &\longmapsto \begin{cases} i - j & \text{falls } x = \frac{p(T)^i f(T)}{p(T)^j g(T)} \text{ mit } p(T) \nmid f(T), g(T) \\ \infty & \text{falls } x = 0. \end{cases} \end{aligned}$$

Der ∞-Stelle entspricht die negative Gradbewertung, d. h.

$$\begin{aligned} \nu_\infty \, : \, \mathbb{F}_q(T) &\longrightarrow \mathbb{Z} \\ x &\longmapsto \begin{cases} \deg g(T) - \deg f(T) & \text{falls } x = \frac{f(T)}{g(T)} \\ \infty & \text{falls } x = 0. \end{cases} \end{aligned}$$

Die Vervollständigung von $\mathbb{F}_q(T)$ an der ∞-Stelle

Vervollständigt man $\mathbb{F}_q(T)$ an der ∞-Stelle, so erhält man den Körper der formalen Laurent-Reihen in $\frac{1}{T}$, d. h.

$$\mathbb{F}_q(T)_\infty = \mathbb{F}_q((\tfrac{1}{T})) = \{f(T) = \textstyle\sum_{i=-\infty}^{n} a_i T^i, \mid n \in \mathbb{Z} \text{ und } a_i \in \mathbb{F}_q\}.$$

$\mathbb{F}_q(T)_\infty$ ist ein lokaler Körper, d. h. er ist vollständig diskret bewertet mit endlichem Restkörper.

Der algebraische Abschluss von $\mathbb{F}_q(T)_\infty$ ist –im Gegensatz zu dem Körper der komplexen Zahlen als Abschluss von $\mathbb{R}$– nicht mehr vollständig. Die Komplettierung von $\widehat{\overline{\mathbb{F}_q(T)}_\infty}$ wird in Analogie zu $\mathbb{C}$ mit C bezeichnet. Der Körper C ist aufgrund des Lemmas von Krassner algebraisch abgeschlossen.

1.2 Grundlagen der Theorie der Drinfeld-Moduln

Im Folgenden sei L ein Körper mit $char(L) = p \neq 0$. $\overline{L}$ sei ein fixierter algebraischer Abschluss von L.
Für jede Erweiterung $L' \subseteq \overline{L}$ von L bezeichnet $\mathbb{G}_a(L') := (L', +)$ die additive Gruppe von L'.

1.2.1 Additive Polynome

1.2.1 Definition. *Ein Polynom $P(X) \in L[X]$ heißt* additiv *genau dann, wenn für alle $\alpha, \beta \in L$ gilt:*

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

P heißt absolut additiv*, falls P additiv ist über $\overline{L}$.*

Aus dieser Definition folgt sofort:

1.2.2 Proposition. *Seien $P(X), H(X) \in L[X]$ additive Polynome, dann sind auch die Polynome*

(i) $P(X) + H(X)$,

(ii) $P(H(X))$ *und*

(iii) $\alpha P(X)$ *für* $\alpha \in L$

additiv.

Sei $\tau_p(X) := X^p \in L[X]$. Da für das Erheben in die p-te Potenz in Charakteristik p gilt

$$(\alpha + \beta)^p = \alpha^p + \beta^p \qquad \text{für alle} \quad \alpha, \beta \in \overline{L},$$

ist $\tau_p(X)$ ein absolut additives Polynom.
Es zeigt sich, dass die Potenzen von τ_p gerade die Teilmenge der absolut additiven Polynome in $L[X]$ aufspannen, denn es gilt:

1.2.3 Proposition. *Sei $P(X) \in L[X]$ ein absolut additives Polynom, dann ist $P(X)$ von der Form:*

$$P(X) = \sum_{i=0}^{d} a_i X^{p^i}.$$

Beweis. Siehe [Gos96, Corollary 1.1.6]. ❑

Für die Menge

$$\mathrm{End}_L(\mathbb{G}_a(L)) := \{P(X) \in L[X] \mid P(X) \text{ ist absolut additiv}\}$$

gilt also die folgende

1.2.4 Proposition.

(i)
$$\mathrm{End}_L(\mathbb{G}_a(L)) = \{\sum_{i=0}^{d} a_i X^{p^i} \mid d \in \mathbb{N}_0,\ a_i \in L\}$$

(ii) *$End_L(\mathbb{G}_a(L))$ wird durch die Verknüpfungen $+$ und $\circ$, definiert durch*

$$\begin{aligned} + &: \quad (P + H)(X) := P(X) + H(X) \\ \circ &: \quad (P \circ H)(X) := P(H(X)), \end{aligned}$$

zu einem nicht-kommutativen Ring mit Eins-Element X.

Ersetzt man $X^p \in End_L(\mathbb{G}_a(L))$ durch τ_p und entsprechend

$$\begin{aligned} \tau_p^0 &= X \\ \tau_p^i &= \underbrace{\tau_p \circ \ldots \circ \tau_p}_{i \text{ Faktoren}} = X^{p^i}, \end{aligned}$$

dann folgt

$$End_L(\mathbb{G}_a(L)) = \{\sum_{i=0}^{d} a_i \tau_p^i \mid d \in \mathbb{N}_0,\ a_i \in L\}.$$

In der τ_p-Notation haben die Verknüpfungen aus 1.2.4 die folgende Form:

$$
\begin{aligned}
+ : \quad & \Big(\sum_{i=0}^{d} a_i\tau_p^i\Big) + \Big(\sum_{j=0}^{d'} b_j\tau_p^j\Big) = \sum_{k=0}^{max(d,d')} (a_k + b_k)\,\tau_p^k \\
\circ : \quad & \Big(\sum_{i=0}^{d} a_i\tau_p^i\Big) \cdot \Big(\sum_{i=0}^{d'} b_i\tau_p^i\Big) = \sum_{k=0}^{d+d'}\Big(\sum_{i+j=k} (a_i\, b_j^{q^i})\Big)\tau_p^k
\end{aligned}
$$

1.2.5 Definition. *Die Menge* $L\{\tau_p\} = (End_L(\mathbb{G}_a(L)), +, \circ)$ *wird als der* getwistete Polynomring in τ_p *bezeichnet.*

1.2.6 Bemerkung: Alternativ kann man $L\{\tau_p\}$ einführen als den Polynomring in τ_p mit links stehenden Koeffizienten, wobei die Multiplikation von Elementen $\alpha \in L$ und τ_p folgender Kommutatorregel genügt:

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

Es wird im Folgenden vorausgesetzt, dass L den Körper $\mathbb{F}_q$ mit $q = p^l$ als Unterkörper enthält.

1.2.7 Definition. *Ein Polynom* $P(X) \in L[X]$ *heißt* $\mathbb{F}_q$-linear *genau dann, wenn* P *absolut additiv ist und für alle* $a \in \mathbb{F}_q$ *gilt:*

$$P(a \cdot X) = a \cdot P(X).$$

1.2.8 Proposition. $P(X) \in L[X]$ *ist* $\mathbb{F}_q$*-linear genau dann, wenn* $P(X)$ *von der Form*

$$P(X) = \sum_{i=0}^{d} a_i X^{q^i} \quad \textit{mit}\; a_i \in L$$

ist. Für die Menge

$$End_{L,\mathbb{F}_q}(\mathbb{G}_a(L)) := \{P(X) \in L[X] \mid P(X) \textit{ ist } \mathbb{F}_q\textit{-linear}\}$$

gilt:

(i)
$$End_{L,\mathbb{F}_q}(\mathbb{G}_a(L)) = \{\sum_{i=0}^{d} a_i X^{q^i} \mid d \in \mathbb{N}_0,\ a_i \in L\}.$$

(ii) *Sei* $P(X) \in End_{L,\mathbb{F}_q}(\mathbb{G}_a(L))$, *so ist* $\ker(P(X))$ *ein* $\mathbb{F}_q$*-Untervektorraum von* $\overline{L}$.

(iii) *Ist umgekehrt* $H \subset \overline{L}$ *ein endlichdimensionaler* $\mathbb{F}_q$*-Untervektorraum, so ist das Polynom*

$$f_H := \prod_{h \in H} (X - h)$$

$\mathbb{F}_q$*-linear.*

Es folgen nun einige Aussagen im Zusammenhang mit additiven Polynomen und $\mathbb{F}_q$-Untervektorräumen von $\overline{L}$, die für spätere Beweise gebraucht werden. Es wird zunächst der Begriff der *Moore-Determinanten* eingeführt, die ein Analogon zur *Vandermondeschen Determinante* im klassischen Fall darstellt. Mit deren Hilfe wird dann die benötigte Aussage von Proposition 1.2.12 bewiesen. Eine ausführlichere Darstellung findet sich in [Gos96, Chapter 1.3].

1.2.9 Definition. *Für die Menge* $\{w_1, \ldots, w_n\} \subset \overline{L}$ *definiert man die* Moore-Determinante *durch*

$$\Delta(w_1, \ldots, w_n) := \det \begin{pmatrix} w_1 & \ldots & w_n \\ w_1^q & \ldots & w_n^q \\ \vdots & & \vdots \\ w_1^{q^{n-1}} & \ldots & w_n^{q^{n-1}} \end{pmatrix}.$$

Man benötigt die folgende Eigenschaft der Moore-Determinante:

1.2.10 Lemma. *Sei* $\mathbf{C} \in \mathrm{Mat}(d \times d, \mathbb{F}_q)$ *und* $\{w_1, \ldots, w_n\} \subset \overline{L}$*, dann gilt:*

$$\Delta(\mathbf{C} \begin{pmatrix} w_1 \\ \vdots \\ w_n \end{pmatrix}) = \det(\mathbf{C}) \cdot \Delta(w_1, \ldots, w_n).$$

1.2.11 Proposition. *Sei* H *ein* $\mathbb{F}_q$*-Untervektorraum von* $\overline{L}$ *der Dimension* l*, und* $\{h_1, \ldots, h_l\}$ *sei eine Basis von* H*. Dann gilt:*

$$\prod_{\substack{h \in H \\ h \neq 0}} h = (-1)^l \Delta(h_1, \ldots, h_l)^{q-1}.$$

Beweis. Dies ist Corollary 1.3.8 aus [Gos96]. ❏

1.2.12 Proposition. *Sei* L *vom Grad* n *über* $\mathbb{F}_q$ *und* H *ein endlichdimensionaler* $\mathbb{F}_q$*-Untervektorraum von* $\overline{L}$*, der stabil ist unter der Abbildung* $\mathcal{F} : x \mapsto x^{q^n}$*, welche durch den Frobenius von* L *gegeben ist. Weiter sei* $\{h_1, \ldots, h_l\}$ *eine Basis von* H *und* $a_0 := \prod_{\substack{h \in H \\ h \neq 0}} h$*, dann gilt:*

$$\det(\mathcal{F}|_H) = \mathrm{N}^L_{\mathbb{F}_q}((-1)^l \, a_0).$$

Beweis. Nach Proposition 1.2.11 gilt:

$$\Delta(h_1, \ldots, h_l)^{q-1} = (-1)^l \, a_0,$$

und somit

$$\begin{aligned}\Delta(h_1, \ldots, h_l)^{q^n-1} &= ((-1)^l \, a_0)^{\frac{q^n-1}{q-1}} \\ &= \mathrm{N}^L_{\mathbb{F}_q}((-1)^l \, a_0). \end{aligned} \tag{1.6}$$

Sei $\mathbf{C}$ die Abildungsmatrix der $\mathbb{F}_q$-linearen Abbildung $\mathcal{F}$ bzgl. der Basis $\{h_1, \ldots, h_l\}$, dann gilt einerseits mit Lemma 1.2.10

$$\begin{aligned}\Delta(\mathcal{F}\begin{pmatrix} h_1 \\ \vdots \\ h_l \end{pmatrix}) = \Delta(\mathbf{C}\begin{pmatrix} h_1 \\ \vdots \\ h_l \end{pmatrix}) &= \det(\mathbf{C}) \cdot \Delta(h_1, \ldots, h_l) \\ &= \det(\mathcal{F}|_H) \cdot \Delta(h_1, \ldots, h_l),\end{aligned}$$

andererseits gilt aber auch

$$\Delta(\mathcal{F}\begin{pmatrix} h_1 \\ \vdots \\ h_l \end{pmatrix}) = \Delta(h_1, \ldots, h_l)^{q^n}.$$

Zusammen mit (1.6) erhält man

$$\begin{aligned}\det(\mathcal{F}|_H) &= \Delta(h_1, \ldots, h_l)^{q^n-1} \\ &= \mathrm{N}^L_{\mathbb{F}_q}((-1)^l \, a_0),\end{aligned}$$

womit die Behauptung gezeigt ist. ❏

1.2.2 Arithmetik in $L\{\tau\}$

1.2.13 Notation: Ab jetzt gelte immer $\boldsymbol{\tau} := \boldsymbol{\tau}_{\mathbf{p}}^{\mathbf{l}}$ für eine feste Primpotenz q der Form $q = p^l$, das heißt im Ring $L\{\tau\}$ wird für $a \in L$ bzgl. der Kommutatorregel

$$\tau \, a = a^q \, \tau$$

multipliziert.

Sei $P \in L\{\tau\}$ von der Form

$$P = \sum_{i=0}^{d} a_i \tau^i \qquad \text{mit} \quad a_i \in L, a_d \neq 0,$$

dann definiert man:

$\deg_\tau(P) := d$ der *Grad in* τ, wobei $\deg_\tau(0) := -\infty$ gesetzt wird, und

$$D(f) := a_0.$$

Für alle $P, Q \in L\{\tau\}$ gilt:

$$\begin{aligned} \deg_\tau(P+Q) &\leq \deg_\tau(P), \deg_\tau(Q) \\ \deg_\tau(P \cdot Q) &\leq \deg_\tau(P) \cdot \deg_\tau(Q) \end{aligned} \quad \text{und} \quad \begin{aligned} D(P+Q) &\leq D(P) + D(Q) \\ D(P \cdot Q) &\leq D(P) \cdot D(Q). \end{aligned}$$

Der nichtkommutative Ring $L\{\tau\}$ ist nullteilerfrei, d. h. für $f, g \in L\{\tau\}$ folgt aus $f \circ g = 0$, dass entweder $f = 0$ oder $g = 0$ sein muss. Die Einheiten von $L\{\tau\}$ sind die Elemente von L^*.
$L\{\tau\}$ ist *rechtseuklidisch*, d. h. für alle $f, g \in L\{\tau\}$, $g \neq 0$ existieren $h, r \in L\{\tau\}$ mit

$$\begin{gathered} \deg_\tau(r) < \deg_\tau(g) \quad \text{und} \\ f = h \circ g + r. \end{gathered}$$

Hieraus resultiert ein rechtseuklidischer Algorithmus, mit dessen Hilfe man zeigen kann, dass jedes Linksideal ein Hauptideal ist. $L\{\tau\}$ ist somit ein *Linkshauptidealring*, und für zwei Elemente $f, g \in L\{\tau\}$ gibt es deshalb immer ein linkes kleinstes gemeinsames Vielfaches, d. h. es existieren Elemente $u, v \in L\{\tau\}$ mit

$$k = u \circ f = v \circ g.$$

Die Existenz dieses linken kgV ist das entscheidende Argument für den Beweis der folgenden Aussage.

1.2.14 Proposition. *Der Ring $L\{\tau\}$ besitzt einen linken Quotientendivisionsring, d. h. es existiert ein injektiver Ringhomomorphismus $L\{\tau\} \hookrightarrow D_l$, für einen Divisionsring D_l, dessen Elemente eine Darstellung der Form $Q^{-1}P$ mit $P, Q \in L\{\tau\}$ besitzen.*

Beweis. Siehe [Gos96, Paragraph 1.6 und Paragraph 4.11]. ❑

Ein solcher linker Quotientendivisionsring von $L\{\tau\}$, wie er in [Gos96, Definition 4.11.2] explizit konstruiert wird, sei mit $L(\tau)$ bezeichnet.

1.2.15 Bemerkung: (i) Ist L ein perfekter Körper, so ist $L\{\tau\}$ auch ein Rechtshauptidealring, und ganz analog existiert ein rechtes kgV und ein rechter Quotientendivisionsring D_r, der kanonisch isomorph zu D_l ist.

(ii) Die Existenz eines Quotientendivisionsringes folgt nicht automatisch für alle nicht-kommutativen, nullteilerfreien Ringe, ebenso wenig die Isomorphie zwischen D_r und D_l, falls sie existieren.

1.2.3 Drinfeld-Moduln

Nachdem $L\{\tau\}$ als der Ring der Endomorphismen der additiven Gruppe des Körpers L identifiziert und seine grundlegenden Eigenschaften dargelegt wurden, soll in diesem Abschnitt der zentrale Begriff des Drinfeld-Moduls eingeführt werden.

Sei K ein algebraischer Funktionenkörper über $\mathbb{F}_q$. Aus $S(K)$, der Menge der Stellen von K, zeichnet man willkürlich eine davon als die ∞-Stelle v_∞ aus und definiert

$$A := \{x \in K \mid \forall\, v \in S(K) \text{ mit } v \neq v_\infty \text{ ist } v(x) \geq 0\}.$$

Wir wissen, dass für A gilt:

- A ist Dedekind-Ring.
- K ist der Quotientenkörper von A.
- Die Elemente von $S(K)$ entsprechen eineindeutig denen der Menge $\{\mathfrak{p} \mid \mathfrak{p} \text{ ist Primideal von } A\} \cup \{\infty\}$.

1.2.16 Definition. *Einen Körper L bezeichnet man als einen A-*Körper*, wenn er versehen ist mit einem Ringhomomorphismus*

$$\gamma : \quad A \to L.$$

*Die A-*Charakteristik $\operatorname{char}_A(L)$ *des A-Körpers L wird definiert als*

$$\begin{array}{ll} \operatorname{char}_A(L) := \mathfrak{p} & \textit{falls } \ker(\gamma) = \mathfrak{p} \\ \operatorname{char}_A(L) := \infty & \textit{falls } \ker(\gamma) = \{0\}. \end{array}$$

Im Fall $\operatorname{char}_A(L) := \mathfrak{p}$ *für ein* $\mathfrak{p} \subseteq A$ *hat* A endliche Charakteristik. *Im zweiten Fall hat* L generische A-Charakteristik *und für alle Ideale* $\mathfrak{q} \subseteq A$ *definiert man in dieser Situation* $(\mathfrak{q}, \operatorname{char}_A(L)) := 1$.

1.2.17 Bemerkung: (i) Falls keine Verwechslung möglich ist, wird A mit $\gamma(A)$ identifiziert.

(ii) Da γ den Körper $\mathbb{F}_q$ in L einbettet, kann man $\mathbb{F}_q$ vermöge γ als Unterkörper von L auffassen. Der Kern von γ ist ein Primideal von A. Der Ringhomomorphismus γ ist also im Fall $\operatorname{char}_A(L) = \infty$ eine Einbettung von A in L und im Fall $\operatorname{char}_A(L) = \mathfrak{p}$ im Wesentlichen die Reduktionsabbildung modulo dem Primideal $\mathfrak{p}$ von A.

In dieser Situation

K	algebraischer Funktionenkörper in einer Variablen über $\mathbb{F}_q$,
$A = \bigcap_{\substack{\mathfrak{p}\in S(K)\\ \mathfrak{p}\neq\infty}} \mathcal{O}_{(\mathfrak{p})}$	Ring der Elemente aus K, die bzgl. aller $\mathfrak{p} \neq \infty$ ganz sind,
L	ein A-Körper vermöge γ,
$L\{\tau\} = End_{L,\mathbb{F}_q}(\mathbb{G}_a(L))$	der Ring der $\mathbb{F}_q$-Endomorphismen von $\mathbb{G}_a(L)$,

definiert man:

1.2.18 Definition. *Ein* Drinfeld A-Modul über L *ist eine A-Modulstruktur auf $L\{\tau\}$, gegeben durch einen Ringhomomorphismus*

$$\begin{aligned} \phi : A &\to L\{\tau\} \\ a &\mapsto \phi_a \end{aligned}$$

mit den Eigenschaften

(i) *ϕ ist $\mathbb{F}_q$-linear, das heißt für alle $c \in \mathbb{F}_q$, $a \in A$ gilt:* $\phi_{ca} = c \cdot \phi_a$.

(ii) *$D \circ \phi = \gamma$, das heißt es ist* $\phi_a = \gamma(a)\tau^0 +$ *höhere Terme in τ für alle $a \in A$.*

(iii) *Es gibt ein $a \in A$ mit $\phi_a \neq \gamma(a)\tau^0$, m. a. W. ϕ ist nicht trivial.*

1.2.19 Proposition. (i) *Ist ϕ ein Drinfeld A-Modul über L, dann existiert eine ganze Zahl $r \geq 0$, so dass gilt:*

$$\deg_\tau \phi_a = r \deg a \quad \textit{für alle } a \in A.$$

Diese Zahl r wird als der Rang *des Drinfeld-Moduls ϕ bezeichnet und* $\mathrm{rg}(\phi)$ *geschrieben.*

(ii) *Die Abbildung $\phi : A \to L\{\tau\}$ ist injektiv.*

Beweis. Siehe [Gos96, Corollary 4.5.2]. ❑

1.2.20 Beispiel: Die Standardsituation ist dadurch gegeben, dass A der Polynomring in einer Variablen über $\mathbb{F}_q$ ist, d. h.

$$\begin{aligned} A &= \mathbb{F}_q[T], \\ K &= \mathbb{F}_q(T), \\ \infty &\approx (\tfrac{1}{T}). \end{aligned}$$

Als A-Körper L wird entweder eine endliche Erweiterung von $\mathbb{F}_q(T)$ betrachtet, wobei $\mathrm{char}_A(L) = \infty$ gilt, oder L ist eine endliche Erweiterung von $\mathbb{F}_q[T] / \mathfrak{p}$, so dass $\mathrm{char}_A(L) = \mathfrak{p}$ gilt.
Der A-Drinfeld-Modul ϕ über dem Körper L ist dann vollständig bestimmt durch die Angabe von

$$\phi_T = \gamma(T) + \sum_{i=1}^{r} g_i \tau^i \quad \text{mit } g_i \in L, g_r \neq 0 \text{ und } r \geq 1.$$

Für alle $a \in A$ gilt $\deg_\tau(\phi_a) = r \deg(a)$, so dass die Zahl r, die hier auftritt, der in 1.2.19 definierte Rang von ϕ ist.

Der einfachste Fall eines Drinfeld-Moduls ist ein Rang 1 Drinfeld-Modul, der sogenannte *Carlitz-Modul*. Dieser wird definiert als

$$\begin{aligned} A = \mathbb{F}_q[T], \quad L = K = \mathbb{F}_q(T) \\ \gamma = \mathrm{id} : A \hookrightarrow K \\ \phi_T := T + \tau. \end{aligned}$$

Gegenstand dieser Arbeit werden Drinfeld-Moduln des Rangs 2 über einem $\mathbb{F}_q[T]$-Körper L sowohl generischer als auch endlicher Charakteristik sein. Diese sind vollständig bestimmt durch die Angabe von

$$\phi_T := \gamma(T) + g\tau + \Delta\tau^2 \quad \text{mit } g, \Delta \in L \text{ und } \Delta \neq 0.$$

Für den Fall, dass K nicht der rationale Funktionenkörper, sondern eine endliche, algebraische Erweiterung von diesem ist, führt schon die explizite Darstellung eines Drinfeld-Moduls zu nicht-trivialen Problemen. Ist A von der Form $A = \mathbb{F}_q[T, Y]$ mit $\psi(Y) = 0$ für ein $\psi(X) \in \mathbb{F}_q[T][X]$, so erhält man durch den Ansatz

$$\begin{aligned} \phi_T = \gamma(T) + \sum_{i=1}^{r} g_i \tau^i \\ \phi_Y = \gamma(Y) + \sum_{j=1}^{r'} h_j \tau^j \end{aligned}$$

komplizierte nichtlineare Gleichungssysteme für die Koeffizienten g_i und h_j (siehe z.B. [Hay91] oder [Dum92]).

1.2.4 Teilungspunkte

Sei ϕ ein A-Drinfeld-Modul über dem A-Körper L und L' eine Erweiterung von L. Dann operiert ein $a \in A$ auf $x \in L'$ durch

$$a \underset{\phi}{*} x := \phi_a(x) = \gamma x + g_1 x^q + \ldots + g_{r \deg(a)} x^{r \deg(a)}.$$

Auf diese Art induziert ϕ auf allen Erweiterungen L' von L eine A-Modulstruktur.

1.2.21 Definition. *Sei $a \in A$. Ein $x \in \overline{L}$, für das gilt*

$$a \underset{\phi}{*} x = 0,$$

heißt ein a-Teilungs- *bzw.* a-Torsionspunkt. *Die a-Torsionspunkte sind also genau die Nullstellen von $\phi_a(X) \in L[X]$ aus $\overline{L}$.*
Man definiert:

$$_a\phi(L') := \{x \in L' \mid {_a\phi}(x) = 0\}.$$

Die Menge $_a\phi(L')$ heißt der Modul der L'-wertigen a-Teilungspunkte. *Für ein Ideal $\mathfrak{a} \subseteq A$ sei*

$$_\mathfrak{a}\phi(L') := \bigcap_{a \in \mathfrak{a}} {_a\phi}(L').$$

Für den Modul der $\overline{L}$-wertigen a-Teilungspunkte verzichtet man auf die Angabe des Körpers und schreibt einfach $_a\phi$ bzw. $_\mathfrak{a}\phi$ im Fall des Ideals.

Es gelten die folgenden Aussagen:

(i) Ist $\mathfrak{a} = (a)$ ein Hauptideal, dann ist $_\mathfrak{a}\phi = {_a\phi}$.

(ii) Jedes $_\mathfrak{a}\phi$ ist sogar ein $A/\mathfrak{a}$-Modul.

(iii) Für alle Erweiterungen L' von L und alle $\mathfrak{a} \neq \{0\}$ ist $_\mathfrak{a}\phi(L')$ endlich.

Neben diesen Eigenschaften, die unmittelbar aus der Definition folgen, kann man für den Modul der $\mathfrak{a}$-Teilungspunkte folgende Aussage beweisen:

1.2.22 Proposition. *Sei ϕ ein A-Drinfeld-Modul vom Rang r über L und $\mathfrak{a}$ ein von $\{0\}$ verschiedenes Ideal von A, dann gilt für den A-Modul $_\mathfrak{a}\phi(\overline{L})$:*

(i) *Ist $(\mathfrak{a}, \mathrm{char}_A(\overline{L})) = 1$, dann ist $_\mathfrak{a}\phi(\overline{L})$ frei über $A/\mathfrak{a}$ vom Rang r.*

(ii) *Falls $(\mathfrak{a}, \mathrm{char}_A(\overline{L})) = \mathfrak{p}$ für ein Primideal $\mathfrak{p} \neq \{0\}$ ist, so existiert ein $h \in \mathbb{N}$ mit $1 \leq h \leq r$, so dass gilt:*

   Für alle $\mathfrak{a} \subseteq A$ von der Form $\mathfrak{a} = \mathfrak{p}^e$ ist $_\mathfrak{a}\phi(\overline{L})$ frei über $A/\mathfrak{p}^e$ vom Rang $r - h$.

   Die Zahl $h =: \mathrm{ht}(\phi)$, die hier auftritt, wird als die Höhe *von ϕ bezeichnet.*

Beweis. (i) Siehe [Gos96, Remarks 4.5.5] bzw. [DH87, Chapter I 3.3]
(ii) Siehe [DH87, Chapter I 3.4]. ❏

1.2.23 Proposition. *Sei $(\mathfrak{a}, \mathrm{char}_A(\overline{L})) = 1$, dann ist der Modul $_\mathfrak{a}\phi$ der $\mathfrak{a}$-Teilungspunkte invariant unter der A-linearen Operation der Gruppe* $\mathrm{Gal}(L^{\mathrm{sep}}/L)$.

Beweis. Sei $\sigma \in \mathrm{Gal}(L^{\mathrm{sep}}/L)$, $x \in {}_{\mathfrak{a}}\phi$ und $a \in \mathfrak{a}$, dann gilt:

$$\phi_a(\sigma(x)) = \sigma(\phi_a(x)) = \sigma(0) = 0.$$

Damit ist $\sigma(x)$ wieder ein $\mathfrak{a}$-Teilungspunkt.
Für ein $a \in A$ gilt:

$$\sigma(a \underset{\phi}{*} x) = \sigma(\phi_a(x)) = \phi_a(\sigma(x)) = a \underset{\phi}{*} \sigma(x).$$

Die mittlere Gleichung gilt, da ϕ_a Koeffizienten in L hat. Damit folgt die A-Linearität der Operation von σ. ❑

Kapitel 2

Arithmetik von Drinfeld-Moduln

Dieses Kapitel enthält wichtige Aussagen zur Arithmetik von Drinfeld-Moduln. Homomorphismen von Drinfeld-Moduln, der Endomorphismenring sowie der Tate-Modul werden eingeführt. Insbesondere wird an vielen Stellen auf die wichtige Situation von Drinfeld-Moduln über endlichen Körpern eingegangen.
Eine ausführlichere Darstellung dieser Themen findet sich zum Beispiel in [Gos96, Chapter 4], [Gek83] oder in [Hay92]. Die Ausführungen zur Theorie der endlichen Drinfeld-Moduln folgen im Wesentlichen [GS96].

Es gelten die Bezeichnungen aus dem 1. Kapitel.

K	Funktionenkörper in einer Variablen über $\mathbb{F}_q$,
$A = \bigcap_{\substack{\mathfrak{p}\in S(K)\\ \mathfrak{p}\neq\infty}} \mathcal{O}_\mathfrak{p}$	Ring der Elemente aus K, die bzgl. aller $\mathfrak{p} \neq \infty$ ganz sind,
L	ein A-Körper vermöge γ.

2.1 Morphismen von Drinfeld-Moduln

2.1.1 Definition. *Es seien ϕ und ψ zwei A-Drinfeld-Moduln über dem A-Körper L. Ein* Morphismus *von ϕ nach ψ über L ist ein Element $u \in L\{\tau\}$ mit der Eigenschaft*

$$\psi_a \circ u = u \circ \phi_a \qquad \textit{für alle } a \in A.$$

Entsprechend sind Endomorphismen von ϕ *Morphismen von ϕ nach ϕ,* Isomorphismen von ϕ nach ψ *sind Morphismen, die eine Inverse v besitzen, so dass gilt $v \circ u = \mathrm{id}_\phi$ und $u \circ v = \mathrm{id}_\psi$. Ein* Automorphismus von ϕ *ist ein Isomorphismus von ϕ nach ϕ.*

Die Menge der Morphismen von ϕ nach ψ bildet bzgl. der Addition in $L\{\tau\}$ einen A-Modul, der mit $\mathrm{Hom}_L(\phi, \psi)$ bezeichnet wird. Ist u ein Morphismus von ϕ nach ψ und v ein Morphismus von ψ nach θ, so ist die Komposition $v \circ u$ ein

Morphismus von ϕ nach θ. Auf diese Weise wird $\mathrm{Hom}_L(\phi, \phi)$ zu einem Unterring von $L\{\tau\}$, der als $\mathrm{End}_L(\phi)$ bezeichnet wird.

2.1.2 Proposition. *Sei $u \in L\{\tau\}$ ein Morphismus. Dann ist u genau dann ein Isomorphismus, wenn $\deg_\tau(u) = 0$ ist.*

Beweis. Der Morphismus u ist genau dann ein Isomorphismus, wenn es ein $v \in L\{\tau\}$ gibt mit $u \circ v = \tau^0$. Damit folgt die Behauptung. ❑

Ein nicht-verschwindender Morphismus zwischen zwei Drinfeld-Moduln ϕ und ψ hat einen endlichen Kern und wird als *Isogenie* bezeichnet.
Es gilt die folgende

2.1.3 Proposition. *Seien ϕ und ψ zwei A-Drinfeld-Moduln, $\mathrm{rg}(\phi)$ und $\mathrm{rg}(\psi)$ jeweils der Rang, sowie $\mathrm{ht}(\phi)$ und $\mathrm{ht}(\psi)$ die Höhe von ϕ bzw. ψ, dann gilt:*

(i) *Sind ϕ und ψ isogen, so folgt:*

$$\mathrm{rg}(\phi) = \mathrm{rg}(\psi) \quad \textit{und} \quad \mathrm{ht}(\phi) = \mathrm{ht}(\psi).$$

(ii) *Zu jeder Isogenie $u : \phi \to \psi$ existiert eine Isogenie $v : \psi \to \phi$, so dass gilt $v \circ u = \phi_a$ und $u \circ v = \psi_a$ für ein geeignetes $a \in A$.*
Insbesondere wird durch „Isogenie“ eine Äquivalenzrelation auf der Menge der Drinfeld-Moduln definiert.

(iii) *Sei $u \in L\{\tau\}$ mit $H = \ker(u)$, dann ist u eine Isogenie genau dann, wenn gilt:*

(a) *H ist ein A-Untermodul von $(\overline{L}, \phi)$ und*

(b)

$$\mathrm{ht}(\phi) \begin{cases} = 0 & \textit{falls } \mathrm{char}_A(L) = \infty, \\ \equiv 0 \mod d & \textit{falls } \mathrm{char}_A(L) = \mathfrak{p} \textit{ ein Primideal vom Grad } d \textit{ ist.} \end{cases}$$

Beweis. (i) Siehe [Gos96, Corollary 4.7.16].
(ii) Siehe [Gos96, Proposition 4.7.13, Corollary 4.7.14].
(iii)Siehe [GS96, Poposition 2.5]. ❑

2.2 Der Endomorphismenring

Wie in Kapitel 1 wird aus der Menge der Stellen von K eine Stelle ν_∞ ausgezeichnet. Mit K_∞ sei die Vervollständigung von K bzgl. ν_∞ bezeichnet.

Der folgende Satz fasst die wichtigsten Strukturaussagen über den Endomorphismenring eines Drinfeld-Moduls über einem beliebigen Körper zusammen.

2.2.1 Proposition. *Sei ϕ ein Drinfeld-Modul vom Grad r über dem A-Körper L. Dann gilt:*

(i) $\mathrm{End}(\phi)$ *ist ein projektiver A-Modul vom Rang $\leq r^2$.*

(ii) *Hat L generische Charakteristik, so ist* $\mathrm{End}(\phi)$ *kommutativ vom Rang $\leq r$.*

(iii) $\mathrm{End}(\phi) \otimes_A K_\infty$ *ist eine endlichdimensionale Divisionsalgebra über K_∞.*

Beweis. (i) und (ii) Siehe [Gek83, Proposition 2.3] bzw. [Gos96, Theorem 4.7.8, Proposition 4.7.6] ([DH87, Chapter 1 4.10] für die Aussage „$< r$" in (ii)).
(iii) Siehe [Gos96, Proposition 4.7.17] bzw. [Gek83, Korollar 2.5]. ❑

Es folgen nun einige weitere Aussagen über den Endomorphismenring, für den Fall, dass der A-Körper L endliche Charakteristik besitzt.
Die Theorie der Endomorphismenringe von Drinfeld Moduln über endlichen Körpern steht in engem Zusammenhang mit der Theorie der zentralen einfachen Algebren. Einen Überblick der hierzu relevanten Aussagen gibt z.B. [Gos96, S. 93-102]. Der hier zitierte Satz zeigt, dass mit Hilfe von Drinfeld-Moduln über endlichen Körpern wichtige Beispiele für Vertreter dieser Klasse von Algebren angegeben werden können und bestätigt ein weiteres Mal die Analogie zu der Situation der elliptischen Kurven.
Die Aussagen des Abschnitts 4.1 schließen sich direkt an die Ausführungen dieses Paragraphen an.

Der Begriff der zentral-einfachen Algebra soll in aller Kürze eingeführt werden.

2.2.2 Definition. (i) *Sei M ein Ring mit Eins. M heißt* einfach *genau dann, wenn M kein nicht-triviales zweiseitiges Ideal besitzt.*

(ii) *Das* Zentrum *von M wird definiert als die Menge*

$$\mathrm{Zentr}(M) := \{x \in M \mid xm = mx, \forall m \in M\}.$$

2.2.3 Definition. *Sei L ein Körper und M eine L-Algebra, d. h. es existiert ein Ring-Homomorphismus von L nach* $\mathrm{Zentr}(M)$*.*
M heißt zentral-einfach*, falls gilt:*

(i) *M ist einfach.*

(ii) $\mathrm{Zentr}(M) = L$.

Es gelten die folgenden Aussagen:

(i) Es gibt einen Divisionsring D/L, so dass M isomorph ist zu $M_n(D)$.

(ii) Sei E mit $L \subseteq E \subseteq M$ ein maximaler Unterkörper von M, dann gibt es einen Isomorphismus $\iota : M \otimes E \xrightarrow{\sim} M_n(E)$.

(iii) Die endlichdimensionale E-Algebra $M_n(E)$ ist versehen mit der Norm- und Spurabbildung $\mathrm{N}_E^{M_n} : M_n(E) \to E$ und $\mathrm{Tr}_E^{M_n} : M_n(E) \to E$, definiert als die Determinante und Spur des durch Linksmultiplikation definierten Endomorphismus von $M_n(E)$. Für die zentral-einfache L-Algebra M lässt sich damit

$$\begin{aligned} \mathrm{N}_E^{M_n} \circ \iota &: M \longrightarrow E \quad \text{und} \\ \mathrm{Tr}_E^{M_n} \circ \iota &: M \longrightarrow E \end{aligned}$$

definieren.
Diese Abbildungen werden als *reduzierte Norm* und *reduzierte Spur* bezeichnet, und es zeigt sich, dass sie unabhängig von der Wahl des maximalen Zwischenkörpers E sind und die Werte schon in L liegen. Man hat also die Abbildungen

$$\begin{aligned} {}_{\mathrm{red}}\mathrm{N}_E^{M_n} &: M \longrightarrow L \quad \text{und} \\ {}_{\mathrm{red}}\mathrm{Tr}_E^{M_n} &: M \longrightarrow L. \end{aligned}$$

Nun zurück zur Ausgangssituation:

Es seien A, K wie bisher und L eine endlicher A-Körper der Charakteristik $\mathfrak{p}$. D. h. L ist ein endliche Erweiterung von $\mathbb{F}_\mathfrak{p} := A/\mathfrak{p}$. Mit d sei der Grad von $\mathfrak{p}$ und mit m der Grad von L über $\mathbb{F}_\mathfrak{p}$ bezeichnet, d. h. $L \cong \mathbb{F}_{q^n}$ für $n = d \cdot m$. Die zu $\mathfrak{p}$ gehörige Stelle aus $S(K)$ sei $\nu_\mathfrak{p}$.

$$\left.\begin{array}{r} m\left\{\begin{array}{c} L \\ | \\ \mathbb{F}_\mathfrak{p} \end{array}\right. \\ d\left\{\begin{array}{c} | \\ \mathbb{F}_q \end{array}\right. \end{array}\right\} n$$

Mit τ sei das Frobenius-Element von $\mathbb{F}_q$ (also die Abbildung $x \mapsto x^q$) und mit $\mathcal{F} := \tau^n$ das Frobenius-Element von L bezeichnet.

Für einen Drinfeld-Modul ϕ des Ranges r über L gilt $\mathcal{F} \circ \phi(a) = \phi(a) \circ \mathcal{F}$, für alle $a \in A$, d. h. $\mathcal{F}$ ist ein Element aus $\mathrm{End}(\phi)$.
Man betrachtet die Einbettung $\phi : A \hookrightarrow L\{\tau\}$ von A in $L\{\tau\}$ und erweitere diese zu einer Einbettung von $K = \mathrm{Quot}(A)$ in $L(\tau)$, den Quotientendivisionsring von $L\{\tau\}$. Sei $D := \mathrm{End}(\phi) \otimes K$ und E bezeichne den Körper $K(\mathcal{F}) \subseteq D$. Mit $\mathbb{F}_q(\mathcal{F})$ werde der Körper der rationalen Funktionen in $\mathcal{F}$ bezeichnet.

$$\begin{tikzcd}
& L(\tau) \arrow[d, dash] & \\
& D = \mathrm{End}(\phi) \otimes K \arrow[d, dash] & \\
& E = K(\mathcal{F}) \arrow[dl, dash] \arrow[dr, dash] & \\
K & & \mathbb{F}_q(\mathcal{F})
\end{tikzcd}$$

Mit diesen Bezeichnungen werden nun die wesentlichen Aussagen aus dem Beweis der nachfolgenden Proposition [Gek91, Theorem 2.9] bzw. [GS96, Theorem 3.8] zusammengefasst. Für eine ausführliche Darstellung wird auf diese Stellen oder auf [Yu95, Theorem 1] verwiesen.

(2.1) Der Divisionsring $L(\tau)$ ist eine zentral einfache Algebra vom Grad n^2 über $\mathbb{F}_q(\mathcal{F})$.

(2.2) $\mathrm{Zentr}_{L(\tau)}(K) = \mathrm{Zentr}_{L(\tau)}(E) = \mathrm{End}(\phi) \otimes_A K$.

(2.3) Die Stellen $\mathcal{F} = 0$ und $\mathcal{F} = \infty$ haben für alle Zwischenkörper $\mathbb{F}_q(\mathcal{F}) \subseteq H \subseteq L(\tau)$ eine eindeutige Fortsetzung (insbesondere also auf den Körper E), die mit ω und ∞_E bezeichnet werden. Die Stelle ω liegt über $\nu_{\mathfrak{p}}$ von K und ∞_E ist die eindeutige Fortsetzung der ∞-Stelle von K.
Sei $\nu_\infty : E \to \mathbb{Q} \cup \{\infty\}$ die dadurch eindeutig bestimmte Fortsetzung der normalisierten Bewertung $\nu_\infty : K \to \mathbb{Z} \cup \{\infty\}$. Aus $\deg_\tau(\phi_a) = r \cdot \deg(a) = -r \cdot \deg\infty \cdot \nu_\infty(a)$ folgt

$$\nu_\infty(\mathcal{F}) = -\frac{n}{r \cdot \deg\infty}\,. \tag{2.4}$$

(2.5) $E_\infty = E \otimes_K K_\infty$ ist ein Körper.

(2.6) $L(\tau) = L\{\tau\} \otimes_{\mathbb{F}_q\{\mathcal{F}\}} \mathbb{F}_q(\mathcal{F})$.

Es gilt:

2.2.4 Proposition. *Sei E der Unterkörper von $D = \mathrm{End}(\phi) \otimes K$, der von $\mathcal{F}$ über K erzeugt wird und $r_1 = [E : K]$ sein Grad. Es gilt:*

(i) *D ist eine zentrale Divisionsalgebra über E mit $\dim_E D = (r_2)^2$, mit der ganzen Zahl $r_2 := r/r_1$.*

(ii) *Es gibt eine eindeutig bestimmte Stelle ω von E, die $\mathcal{F}$ teilt und diese liegt über der Stelle $\nu_{\mathfrak{p}}$ von K. Die Stelle ν_∞ von K hat eine eindeutige Fortsetzung ω_∞ nach E.*

Beweis. Siehe [GS96, 3.8] bzw. [Yu95, Theorem 1]. ❑

2.3 Der Tate-Modul

In diesem Abschnitt der Tate-Modul eingeführt. Einem fest gewählten Drinfeld-Modul ϕ wird an jeder Primstelle $\mathfrak{q} \in S(K)$ ein freier $A_{\mathfrak{q}}$-Modul zugeordnet. Dieser liefert die Möglichkeit einer $\mathfrak{q}$-adischen Darstellung sowohl des Endomorphismenrings $\mathrm{End}(\phi)$ als auch der absoluten Galois-Gruppe $\mathrm{Gal}(L^{\mathrm{sep}}/L)$.

Für eine Stelle $\nu = \nu_{\mathfrak{q}}$ aus $S(K)$ sei mit K_ν die Vervollständigungen an dieser Stelle und mit ${}_{\mathfrak{q}^k}\phi$ die Menge der $\mathfrak{q}^k$-Teilungspunkte bezeichnet. Man definiert

$$ {}_\nu\phi := \varinjlim {}_{\mathfrak{q}^k}\phi, $$

d. h. als den induktiven Limes über die Teilungspunkte aller $\mathfrak{q}$-Potenzen.

2.3.1 Definition. *Der* $\mathfrak{q}$-adische Tate-Modul *eines A-Drinfeld-Moduls ϕ über L wird definiert als*

$$ T_\nu(\phi) := \mathrm{Hom}_{A_\nu}(K_\nu/A_\nu, {}_\nu\phi). $$

2.3.2 Proposition. *Sei ϕ ein A-Drinfeld-Modul vom Rang r, $\nu = \nu_{\mathfrak{q}}$ für $\mathfrak{q} \in S(K)$ und $r' = r - \mathrm{ht}(\phi)$.*
Dann gilt:

$$ T_\nu(\phi) \cong A_\nu^{r'}. $$

Beweis. Siehe [GS96, Corollary 2.3]. ❑

2.3.3 Bemerkung: (i) Sei $\mathfrak{q} \subset A$ ein Primideal mit $\mathfrak{q} \neq \mathrm{char}_A(L)$ und $\nu = \nu_{\mathfrak{q}}$. Nach Proposition 1.2.23 operiert $\mathrm{Gal}(L^{\mathrm{sep}}/L)$ auf ${}_{\mathfrak{q}^n}\phi$ für alle $n \in \mathbb{N}$, was zur $\mathfrak{q}$-adischen Darstellung

$$ \rho_{\mathfrak{q}} : \ \mathrm{Gal}(L^{\mathrm{sep}}/L) \longrightarrow \mathrm{Aut}_{A_\nu}(T_\nu(\phi)) \cong \mathrm{GL}(\mathrm{rg}(\phi), A_\nu) $$

führt.
(ii) Im Fall, dass $\mathfrak{q}$ ein Hauptideal ist, insbesondere in der Standardsituation $A = \mathbb{F}_q[T]$, gilt

$$T_\nu(\phi) \cong \varprojlim \, {}_{\mathfrak{q}^k}\phi,$$

mit den Projektionen gegeben durch

$$\begin{aligned} {}_{\mathfrak{q}^{k+1}}\phi &\to {}_{\mathfrak{q}^k}\phi \\ x &\mapsto \phi_{\mathfrak{q}}(x), \end{aligned}$$

bzw. $T_\nu(\phi)$ wird direkt auf diese Weise definiert.

2.3.4 Proposition. *Sei ϕ ein A-Drinfeld-Modul vom Rang r und $\nu = \nu_{\mathfrak{q}}$ eine Stelle aus K für $\mathfrak{q} \in S(K)$, wobei $\mathfrak{q} \neq \mathrm{char}_A(L)$ ist.*
Dann ist die Darstellung

$$i_{\mathfrak{q}}: \ \mathrm{End}(\phi) \otimes_\nu A_\nu \longrightarrow \mathrm{End}_{A_\nu}(T_\nu(\phi)) \cong \mathrm{Mat}(\mathrm{rg}(\phi), A_\nu)$$

injektiv.

Beweis. Siehe [GS96, Corollary 2.9]. ❏

2.4 Reduktion von Drinfeld-Moduln

Sei L ein A-Körper, der mit einer nicht-trivialen diskreten Bewertung ν versehen ist. Mit $\mathcal{O}_{(\nu)} \subset L$ sei der Bewertungsring von ν, mit $\mathfrak{P}$ dessen maximales Ideal und mit $\mathcal{L}_\nu$ der Restklassenkörper bezeichnet, d. h.

$$\begin{aligned}\mathcal{O}_{(\nu)} &= \{x \in L \mid \nu(x) \geq 0\},\\ \mathfrak{P} &= \{x \in L \mid \nu(x) > 0\},\\ \mathcal{L}_\nu &= \mathcal{O}_{(\nu)}/\mathfrak{P}.\end{aligned}$$

Der Bewertungsring $\mathcal{O}_{(\nu)}$ heißt *endlich*, falls er A enthält, also falls $\nu(A) \geq 0$ ist. Es werden im Folgenden nur endliche $\mathcal{O}_{(\nu)}$ betrachtet.

$L\{\tau\}$ enthält als Unterring $\mathcal{O}_{(\nu)}\{\tau\}$ den getwisteten Polynomring über $\mathcal{O}_{(\nu)}$, und dieser ist versehen mit der kanonischen Reduktionsabbildung

$$\mathrm{red}_{\mathfrak{P}}: \ \mathcal{O}_{(\nu)}\{\tau\} \longrightarrow (\mathcal{O}_{(\nu)}/\mathfrak{P})\{\tau\} = \mathcal{L}_\nu\{\tau\}.$$

2.4.1 Definition. *Es sei $\phi : A \to L\{\tau\}$ ein A-Drinfeld-Modul vom Rang $r > 0$ über L, dann hat ϕ* ganze Koeffizienten, *falls $\phi_a \in \mathcal{O}_{(\nu)}\{\tau\}$ für alle $a \in A$ und die Verknüpfung*

$$\begin{aligned}\mathrm{red}_{\mathfrak{P}} \circ \phi : \ &\longrightarrow \mathcal{L}_\nu\{\tau\}\\ a \ &\longmapsto \mathrm{red}_{\mathfrak{P}}(\phi_a)\end{aligned}$$

einen A-Drinfeld-Modul über dem Körper $\mathcal{L}_\nu$ vom Rang r' mit $0 < r' \leq r$ definiert.

2.4.2 Definition. *(i) Der Drinfeld-Modul ϕ hat* stabile Reduktion bzgl. ν, *falls es einen zu ϕ isomorphen Drinfeld-Modul ϕ' gibt, der ganze Koeffizienten hat, d. h. falls ein $\xi \in L^*$ existiert, so dass $\phi'_a = \xi\phi_a\xi^{-1} \in \mathcal{O}_{(\nu)}\{\tau\}$ für alle $a \in A$ und* $\mathrm{red}_{\mathfrak{P}} \circ \phi'$ *einen Drinfeld-Modul definiert.*

(ii) Man sagt, ϕ hat gute Reduktion bzgl. ν, *falls ϕ stabile Reduktion hat und zusätzlich* $\mathrm{rg}(\mathrm{red}_{\mathfrak{P}} \circ \phi) = \mathrm{rg}(\phi)$ *gilt.*

(iii) Die Teilmenge von $S(K)$, die die Stellen enthält, an denen ϕ gute Reduktion hat, sei mit $S_\phi(K)$ bezeichnet.

Falls ϕ keine stabile (bzw. gute) Reduktion über L besitzt, kann es eine endliche Erweiterung L' von L geben, mit einer über ν liegenden Stelle ν', so dass ϕ als Drinfeld-Modul über L' stabile (bzw. gute) Reduktion an ν' hat.

Diese Möglichkeit bezeichnet man auf folgende Weise:

2.4.3 Definition. *Ein Drinfeld-Modul ϕ hat* potenziell stabile (gute) Reduktion über L bzgl. ν, *falls es eine endliche Erweiterung L' gibt, so dass ϕ stabile (gute) Reduktion über L' bzgl. ν' hat, für eine Stelle ν' mit $\nu \mid \nu'$.*

2.4.4 Proposition. *(i) Jeder Drinfeld-Modul ϕ über L hat potenziell stabile Reduktion über L bzgl. ν.*

(ii) Jeder Rang 1 Drinfeld-Modul hat potenziell gute Reduktion über L bzgl. ν.

Beweis. Siehe [Gos96, Corollary 4.10.4]. ❑

Kapitel 3

Rang 2 Drinfeld-Moduln

Dieser Abschnitt befasst sich mit einigen speziellen Eigenschaften von Drinfeld-Moduln des Ranges 2 und enthält Aussagen, die später für explizite Berechnungen benötigt werden.

Drinfeld-Moduln vom Rang 1, wie der auf Seite 30 definierte Carlitz-Modul, spielen eine wichtige Rolle für die Arithmetik von algebraischen Funktionenkörpern endlicher Charakteristik, da er z.B.– genau wie die Einheitswurzeln über $\mathbb{Q}$ im klassischen Fall – die Konstruktion der maximalen abelschen Erweiterung ermöglichen.
Über $\mathbb{Q}$ erhält man diese durch die Adjunktion der Einheitswurzeln, also den Lösungen der Gleichung $X^n - 1 = 0$.
Analog dazu stellt die Adjunktion der $\mathfrak{a}$-Teilungspunkte eines Rang 1 Drinfeld-Moduls eine galois'sche Erweiterung mit den gleichen Eigenschaften bzgl. der Galois-Gruppe und des Verzweigungsverhaltens wie die Kreisteilungskörper $\mathbb{Q}(\xi_n)/\mathbb{Q}$ dar (vgl. [Hay74]).

Drinfeld-Moduln von höherem Rang, insbesondere die des Ranges 2, stellen in vieler Hinsicht ein Analogon zu elliptischen Kurven im klassischen Fall dar.

Im Folgenden sei $K = \mathbb{F}_q(T)$ der rationale Funktionenkörper und ν_∞ sei die zu $(\frac{1}{T})$ korrespondierende Stelle aus $S(K)$, so dass A der Polynomring $\mathbb{F}_q[T]$ ist. L sei vorläufig ein beliebiger A-Körper.

3.1 Isomorphien von Rang 2 Drinfeld-Moduln

Es seien zwei Drinfeld-Moduln vom Rang 2 gegeben durch

$$\begin{aligned} \phi:\ A = \mathbb{F}_q[T] &\longrightarrow L\{\tau\} \\ \phi_T &\longmapsto \gamma(T) + g\tau + \Delta\tau^2 \end{aligned}$$

und

$$\begin{aligned} \phi' :\ A = \mathbb{F}_q[T] &\longrightarrow L\{\tau\} \\ \phi_T &\longmapsto \gamma(T) + g'\tau + \Delta'\tau^2. \end{aligned}$$

Nach Proposition 2.1.2 sind ϕ und ϕ' isomorph, wenn es ein $u \in L\{\tau\}^* = L^*$ gibt mit $u \circ \phi_a = \phi'_a \circ u$ für alle $a \in A$. Im Fall des Polynomrings ist dies gleichbedeutend mit $u \circ \phi_T = \phi'_T \circ u$, was sich auch durch folgende Beziehungen für g, g', Δ und Δ' beschreiben lässt.

3.1.1 Lemma. *Die Drinfeld-Moduln ϕ und ϕ' sind isomorph über L genau dann, wenn es ein $u \in L^*$ gibt mit*

$$\begin{aligned} g' &= u^{q-1} g \quad \textit{und} \\ \Delta' &= u^{q^2-1}\Delta. \end{aligned} \tag{3.1}$$

3.1.2 Definition. *Die j-*Invariante*des Drinfeld-Moduls $\phi_T = \gamma(T) + g\tau + \Delta\tau^2$ wird definiert als*

$$j(\phi) := \frac{g^{q+1}}{\Delta}.$$

3.1.3 Proposition. (i) *Sind zwei Drinfeld-Moduln ϕ und ϕ' isomorph zueinander, so gilt*

$$j(\phi) = j(\phi').$$

(ii) *Ist L algebraisch abgeschlossen, so gilt auch die umgekehrte Richtung, d. h.*

$$j(\phi) = j(\phi') \quad \Longrightarrow \quad \phi \textit{ ist isomorph zu } \phi' \textit{ über } L.$$

Beweis. (i) Falls ϕ isomorph ist zu ϕ', so gibt es ein $u \in L^*$ mit (3.1) und somit

$$j(\phi') = \frac{g'^{q+1}}{\Delta'} = \frac{(u^{q-1}g)^{q+1}}{u^{q^2-1}\Delta} = \frac{g^{q+1}}{\Delta} = j(\phi).$$

(ii) Es gelte $j(\phi') = j(\phi)$, d. h.:

$$\begin{aligned} \frac{g^{q+1}}{\Delta} &= \frac{g'^{q+1}}{\Delta'} \quad \text{bzw.} \\ \left(\frac{g'}{g}\right)^{q+1} &= \frac{\Delta'}{\Delta}. \end{aligned}$$

Da L algebraisch abgeschlossen ist, existiert ein $u \in L^*$ mit $u^{q-1} = \frac{g'}{g}$. Man erhält

$$u^{q-1}g = \frac{g'}{g} \cdot g = g' \quad \text{und}$$
$$u^{q^2-1}\Delta = \frac{g'}{g}^{q+1} \cdot \Delta = \left(\frac{\Delta'}{\Delta}\right)\Delta = \Delta'.$$

Damit sind ϕ und ϕ' wegen (3.1) isomorph über L. ❑

3.1.4 Bemerkung: Über einem algebraisch abgeschlossenen Körper sind Drinfeld-Moduln bis auf Isomorphie durch ihre j-Invariante charakterisiert. Ist L nicht algebraisch abgeschlossen, so gibt es Drinfeld-Moduln, die isomorph sind über einer Erweiterung von L, ohne es über L zu sein.

Sei L nun ein endlicher Körper mit q^n Elementen.

$$\left.\begin{array}{r} m\left\{\begin{array}{c} L \\ | \\ \mathbb{F}_{\mathfrak{p}} \end{array}\right. \\ d\left\{\begin{array}{c} | \\ \mathbb{F}_q \end{array}\right. \end{array}\right\} n$$

Über L gibt es $q^n\,(q^n-1)$ verschiedene Drinfeld-Moduln. Sei ϕ gegeben durch (g,Δ), dann sind alle zu ϕ isomorphen Drinfeld-Moduln gegeben durch die Paare $(a^{q-1}g, a^{q^2-1}\Delta)$, wobei a durch L^* läuft.

Die Isomorphieklassen entsprechen also eineindeutig den Bahnen der Gruppe L^* auf $L \times L^*$, wobei die Gruppenaktion von L^* gegeben ist durch

$$a(g,\Delta) := (a^{q-1}g, a^{q^2-1}\Delta).$$

Damit lässt sich ein Repräsentantensystem, sowie eine Formel für die Anzahl und die Mächtigkeiten der Isomorphieklassen, explizit angeben.

3.1.5 Proposition. (i) *Die Anzahl der Isomorphieklassen von Rang 2 Drinfeld-Moduln über dem endlichen Körper L ist gegeben durch*

$$(q-1)\,(q^n-1) + (q-1) = q^n\,(q-1) \qquad \textit{falls } n \textit{ ungerade ist,}$$
$$(q-1)\,(q^n-1) + (q^2-1) = (q^n+q)\,(q-1) \qquad \textit{falls } n \textit{ gerade ist.}$$

(ii) *Sei a ein Erzeuger der multiplikativen Gruppe L^*. Ein Repräsentantensystem der Isomorphieklassen ist gegeben durch*

***n* ungerade:**

$$\{\,(a^i,a^j)\mid 1\le i\le q-1,\ 1\le j\le q^n-1\}\cup\{\,(0,a^j)\mid 1\le j\le q-1\},$$

***n* gerade:**

$$\{\,(a^i,a^j)\mid 1\le i\le q-1,\ 1\le j\le q^n-1\}\cup\{\,(0,a^j)\mid 1\le j\le q^2-1\}.$$

(iii) *Die Mächtigkeit der Isomorphieklassen ist gegeben durch*

***n* ungerade:**

$$\frac{q^n-1}{q-1}\quad \textit{für alle Klassen.}$$

***n* gerade:**

$$\frac{q^n-1}{q^2-1}\quad \textit{falls die Klasse aus Drinfeld-Moduln mit } g=0 \textit{ besteht, bzw.}$$
$$\frac{q^n-1}{q-1}\quad \textit{falls die Klasse aus Drinfeld-Moduln mit } g\neq 0 \textit{ besteht.}$$

Beweis. (i) Folgt zum einen direkt aus der Formel für die Anzahl der Isomorphieklassen eines Drinfeld-Moduls des Ranges r für allgemeines r in Proposition 4.1.1 aus [Pot96], oder aus der Konstruktion des Repräsentantensystems im folgenden Beweis von (ii).

(ii) Mit

$$[(g,\Delta)] := \{\, a^i\,(g,\Delta)\mid 1\le i\le q^n-1\}$$

sei die Bahn von (g,Δ) unter der Aktion von L^* bezeichnet, und für (g,Δ) und (g',Δ') definiert man

$$(g,\Delta)\sim(g',\Delta')\ :\Leftrightarrow\ (g,\Delta) \text{ und } (g',\Delta') \text{ sind Vertreter der gleichen Bahn.}$$

Sei g = 0:

Sei ϕ ein Drinfeld-Modul mit $g=0$, dann muss aufgrund von (3.1) für einen isomorphen Drinfeld-Modul auch $g'=0$ gelten. D. h. eine Klasse enthält entweder nur Drinfeld-Moduln mit $g=0$ oder nur solche mit $g\neq 0$.

Sei

$$[(0,\Delta)] := \{\, a^i\,(0,\Delta)\mid 1\le i\le q^n-1\}$$

die Bahn eines Drinfeld-Moduls mit $g = 0$. Es gilt:

$$\begin{aligned} & a^i\,(0,\Delta) = a^j\,(0,\Delta) \\ \iff\quad & a^{i(q^2-1)}\Delta = a^{j(q^2-1)}\Delta \\ \iff\quad & (q^2-1)(i-j) \equiv 0\ (q^n-1) \\ \iff\quad & i-j \equiv 0 \begin{cases} \left(\frac{q^n-1}{q-1}\right) & \text{falls } n \text{ ungerade,} \\ \left(\frac{q^n-1}{q^2-1}\right) & \text{falls } n \text{ gerade.} \end{cases} \end{aligned}$$

Damit folgt

$$|\,[(0,\Delta)]\,| = \begin{cases} \left(\frac{q^n-1}{q-1}\right) & \text{falls } n \text{ ungerade,} \\ \left(\frac{q^n-1}{q^2-1}\right) & \text{falls } n \text{ gerade.} \end{cases}$$

Da es $q^n - 1$ Drinfeld-Moduln mit $g = 0$ gibt, existieren also $q - 1$ Klassen, falls n ungerade ist, und $q^2 - 1$ Klassen, falls n gerade ist.

Sei $\Delta = a^k$ und $\Delta' = a^l$ mit $\Delta \neq \Delta'$, dann gilt:

$$\begin{aligned} & (0,\Delta) \sim (0,\Delta') \\ \iff\quad & \exists\, i \in \{0,\dots,q^n-2\} \text{ mit } \quad \frac{\Delta}{\Delta'} = a^{i(q^2-1)} \\ \iff\quad & \exists\, i \in \{0,\dots,q^n-2\} \text{ mit } \quad \frac{a^k}{a^l} = a^{i(q^2-1)} \\ \iff\quad & \exists\, i \in \{0,\dots,q^n-2\} \text{ mit } \quad a^{(k-l)-i(q^2-1)} = 1 \\ \overset{a \text{ ist Erzeuger}}{\iff}\quad & \exists\, i \in \{0,\dots,q^n-2\} \text{ mit } \quad (k-l) - i(q^2-1) \equiv 0 \quad (q^n-1) \\ \iff\quad & \exists\, i \in \{0,\dots,q^n-2\} \text{ und } j \in \mathbb{Z} \text{ mit } \quad (k-l) = i(q^2-1) + j(q^n-1). \end{aligned}$$

Damit folgt $(k-l) \geq ggT(q^2-1, q^n-1)$ für isomorphe Drinfeld-Moduln. Deshalb liegen die Elemente der Mengen

$$\{\,(0,a^i) \mid 1 \leq i \leq q-1\} \quad \text{falls } n \text{ ungerade bzw.}$$
$$\{\,(0,a^i) \mid 1 \leq i \leq q^2-1\} \quad \text{falls } n \text{ gerade}$$

in unterschiedlichen Bahnen und bilden damit ein Repräsentantensystem für die Isomorphieklassen von Drinfeld-Moduln mit $g = 0$.

Ganz analog zeigt man für

$\mathbf{g \neq 0}$:

Sei

$$[(g,\Delta)] = \{\,a^i\,(g,\Delta) \mid 1 \leq i \leq q^n-1\}$$

die Bahn des Drinfeld-Moduls (g, Δ). Für zwei Vertreter dieser Bahn gilt:

$$
\begin{aligned}
& a^i\,(g,\Delta) = a^j\,(g,\Delta) \\
\iff\quad & \begin{cases} a^{i(q-1)}g = a^{j(q-1)}g & \text{und} \\ a^{i(q^2-1)}\Delta = a^{j(q^2-1)}\Delta \end{cases} \\
\iff\quad & \begin{cases} (q-1)\,(i-j) \equiv 0 \quad (q^n-1) & \text{und} \\ (q^2-1)\,(i-j) \equiv 0 \quad (q^n-1) \end{cases} \\
\iff\quad & (i-j) \equiv 0 \quad \left(\frac{q^n-1}{q-1}\right).
\end{aligned}
$$

Damit folgt

$$|\,[(g,\Delta)]\,| = \frac{q^n-1}{q-1}.$$

Es existieren $(q^n-1)\,(q^n-1)$ verschiedene Drinfeld-Moduln mit $g \neq 0$ und diese verteilen sich damit auf $(q^n-1)\,(q-1)$ Klassen.
Sei $g = a^u$, $g' = a^v$, $\Delta = a^k$ und $\Delta' = a^l$, dann gilt

$$
\begin{aligned}
& (g,\Delta) \sim (g',\Delta') \\
\iff\quad & \exists\, i \in \{0,\ldots,q^n-2\} \text{ mit } \begin{cases} \frac{g}{g'} = a^{i(q-1)} \\ \frac{\Delta}{\Delta'} = a^{i(q^2-1)} \end{cases} \\
\iff\quad & \exists\, i \in \{0,\ldots,q^n-2\} \text{ mit } \begin{cases} \frac{a^u}{a^v} = a^{i(q-1)} \\ \frac{a^k}{a^l} = a^{i(q^2-1)} \end{cases} \\
\overset{a \text{ ist Erzeuger}}{\iff}\quad & \exists\, i \in \{0,\ldots,q^n-2\} \text{ mit } \begin{cases} (u-v) - i(q-1) \equiv 0 \quad (q^n-1) \\ (k-l) - i(q^2-1) \equiv 0 \quad (q^n-1) \end{cases} \\
\iff\quad & \exists\, i \in \{0,\ldots,q^n-2\} \text{ und } j \in \mathbb{Z} \text{ mit } \begin{cases} (u-v) = i(q-1) + j(q^n-1) & ① \\ (k-l) = i(q^2-1) + j(q^n-1) & ② \end{cases}
\end{aligned}
$$

Aus ① folgt, dass zwei Elemente $(a^u, *)$ und $(a^v, *)$ mit $1 \leq u, v \leq q-1$ und $u \neq v$ nicht in der gleichen Bahn liegen können.

Falls sie in der 1. Komponente übereinstimmen, folgt aus ① für Vertreter der gleichen Bahn (g, a^k) und (g, a^l), dass $i = 0$ sein muss und zusammen mit ②, dass $(k-l)$ ein Vielfaches von q^n-1 ist. Dies bedeutet aber, dass $a^k = a^l$ ist. Somit stimmen sie auch in der 2. Komponente überein.

Damit ist gezeigt, dass die $(q^n-1)\,(q-1)$ Elemente von

$$\{\,(a^i, a^j) \mid 1 \leq i \leq q-1, 1 \leq j \leq q^n-1\}$$

in verschiedenen Bahnen liegen und damit ein Repräsentantensystem für die Isomorphieklassen der Drinfeld-Moduln mit $g \neq 0$ bilden.

Damit hat man die Aussage (ii) bewiesen. Die Formeln aus (i) und (iii) folgen direkt aus dieser Konstruktion. ❑

3.2 Berechnung der Koeffizienten von ϕ_a

Sei L wieder ein beliebiger A-Körper und ϕ ein Rang 2 Drinfeld-Modul über L, der gegeben ist durch die Angabe von $g \in L$ und $\Delta \in L^*$, so dass

$$\phi_T = \gamma(T) + g\,\tau + \Delta\,\tau^2$$

ist.

3.2.1 Notation: An dieser Stelle soll eine Schreibweise eingeführt werden, die des öfteren Verwendung findet. Sei ϕ ein A-Drinfeld-Modul. Für ein $a \in A$ wird mit $\mathrm{k}^{\phi}_{a,i}$, bzw. $\mathrm{k}_{a,i}$ wenn keine Verwechslung bzgl. des Drinfeld-Moduls entstehen kann, der Koeffizient von τ^i in $\phi_a \in L\{\tau\}$ bezeichnet.
Es gilt also

$$\phi_a = \sum_{i=0}^{\mathrm{rg}(\phi)\cdot \deg a} \mathrm{k}_{a,i}\tau^i.$$

Die beiden folgenden Lemmata erweisen sich als nützlich für die explizite Berechnung der Werte $\phi_a = \sum_{i=0}^{2\cdot \deg a} \mathrm{k}_{a,i}\tau^i$.

3.2.2 Lemma. *Sei $a \in A = \mathbb{F}_q[T]$ und $\phi_a := \sum_{i=0}^{2\cdot \deg a} \mathrm{k}_{a,i}\tau^i$. Dann genügen die Koeffizienten $\mathrm{k}_{a,i}$ der folgenden Rekursion:*

$$\begin{aligned}
\mathrm{k}_{a,0} &= \gamma(a), \\
\mathrm{k}_{a,1} \cdot \gamma(T^q - T) &= \mathrm{k}_{a,0}^q\, g - \mathrm{k}_{a,0}\, g, \\
\mathrm{k}_{a,i} \cdot \gamma(T^{q^i} - T) &= \mathrm{k}_{a,i-1}^q\, g - \mathrm{k}_{a,i-1}\, g^{q^{i-1}} + \mathrm{k}_{a,i-2}^{q^2}\, \Delta - \mathrm{k}_{a,i-2}\, \Delta^{q^{i-2}}
\end{aligned}$$

$$\textit{für } i = 2, 3, \ldots, 2 \cdot \deg a.$$

Beweis. Für $a \in A$ gelten die Äquivalenzen

$$\begin{aligned}
& & \phi_{a\cdot T} &= \phi_{T\cdot a} \\
&\iff & \phi_a \circ \phi_T &= \phi_T \circ \phi_a
\end{aligned}$$

$$\iff \Big(\sum_{i=0}^{2\cdot \deg a} \mathrm{k}_i\,\tau^i\Big) \circ \big(\gamma(T) + g\tau + \Delta\tau^2\big) = \big(\gamma(T) + g\tau + \Delta\tau^2\big) \circ \Big(\sum_{i=0}^{2\cdot \deg a} \mathrm{k}_i\,\tau^i\Big).$$

Definiert man $\mathrm{k}_{a,i}{:=}0$ für $i<0$ und $i>r\cdot\deg a$, dann folgt (aus der Kommutatorregel $\tau\alpha=\alpha^q\tau$ für $\alpha\in L$) die Gleichung

$$\sum_{i=0}^{2\cdot\deg a+2}(\mathrm{k}_{a,i}\,\gamma(T)^{q^i}+\mathrm{k}_{a,i-1}\,g^{q^{i-1}}+\mathrm{k}_{a,i-2}\,\Delta^{q^{i-2}})\tau^i$$
$$=\sum_{i=0}^{2\cdot\deg a+2}(\mathrm{k}_{a,i}\,\gamma(T)+\mathrm{k}_{a,i-1}^q g+\mathrm{k}_{a,i-2}^{q^2}\,\Delta)\tau^i.$$

Für den Koeffizienten $\mathrm{k}_{a,0}$ gilt:

$$\mathrm{k}_{a,0}=\gamma(a).$$

Der Koeffizientenvergleich von τ liefert dann

$$\mathrm{k}_{a,1}\cdot\gamma(T^q-T)=\mathrm{k}_{a,0}^q\,g-\mathrm{k}_{a,0}\,g.$$

Der Koeffizientenvergleich von τ^i für $2\leq i\leq 2\cdot\deg a$ führt zu

$$\mathrm{k}_{a,i}\cdot\gamma(T^{q^i}-T)=\mathrm{k}_{a,i-1}^q\,g-\mathrm{k}_{a,i-1}\,g^{q^{i-1}}+\mathrm{k}_{a,i-2}^{q^2}\,\Delta-\mathrm{k}_{a,i-2}\,\Delta^{q^{i-2}}.$$

Damit ist die Behauptung gezeigt. ❑

Das nächste Lemma liefert eine geschlossene Formel für die beiden führenden Koeffizienten $\mathrm{k}_{a,2\cdot\deg a}$ und $\mathrm{k}_{a,2\cdot\deg a-1}$ von $\phi_a=\sum_{i=0}^{2\cdot\deg a}\mathrm{k}_{a,i}\,\tau^i$. Für ein normiertes a sind sie nur abhängig von dessen Grad und ϕ, und es zeigt sich, dass der Leitkoeffizient sogar unabhängig von g berechnet werden kann.

3.2.3 Lemma. *Sei $a\in A=\mathbb{F}_q[T]$ ein normiertes Polynom vom Grad d und $\phi: A\to L\{\tau\}$ ein Drinfeld-Modul vom Rang 2, gegeben durch $\phi_T:=\gamma(T)+g\,\tau+\Delta\,\tau^2$. Weiter seien $\mathrm{k}_{a,1},\ldots,\mathrm{k}_{a,2d}$ die Koeffizienten von*

$$\phi_a=\gamma(a)+\mathrm{k}_{a,1}\,\tau+\cdots+\mathrm{k}_{a,2d-1}\,\tau^{2d-1}+\mathrm{k}_{a,2d}\,\tau^{2d}.$$

Dann gilt für die beiden führenden Koeffizienten:

(i)
$$\mathrm{k}_{a,2d}=\Delta^{\frac{q^{2d}-1}{q^2-1}}\qquad \textit{und}$$

(ii)
$$\mathrm{k}_{a,2d-1}=\Delta^{\frac{q^{2d}-1}{q^2-1}}\sum_{i=o}^{d-1}g^{q^{2i}}\Delta^{-\frac{q^{2d-1}+q^{2i}}{q+1}}.$$

Beweis. (i) Sei $a = \sum_{j=0}^{d} a_j T^j$, dann gilt

$$\gamma(a) + \mathrm{k}_{a,1}\,\tau + \cdots + \mathrm{k}_{a,2d}\,\tau^{2d} \;= \phi_a = \;\phi_{\sum_{j=0}^{d} a_j T^j} = \sum_{j=0}^{d} (a_j\;\phi_{T^j}).$$

Zum Koeffizienten von τ^{2d} trägt nur der Summand $a_d \phi_{T^d} = \phi_{T^d}$ etwas bei. Wegen $\phi_{T^d} = (\phi_T)^d$ und der Kommutatorregel $\tau^2 a = a^{q^2}\tau$ folgt demnach:

$$\begin{aligned}
\mathrm{k}_{a,2d}\,\tau^{2d} &= \textstyle\prod_{j=1}^{d} \Delta\tau^2 && \text{da dies der einzige Term ist,}\\
& && \text{in dem } \tau \text{ den Grad } 2d \text{ hat}\\
&= \Delta^{\sum_{j=0}^{d-1}(q^2)^j}\;\tau^{2d}\\
&= \Delta^{\frac{q^{2d}-1}{q^2-1}}\;\tau^{2d}
\end{aligned}$$

und damit die Behauptung (i).

(ii) Wie in (i), kann auch zum Koeffizienten k_{2d-1} nur $\phi_{T^d} = (\phi_T)^d$ einen Betrag leisten. Multipliziert man diesen Term nach der Kommutatorregel aus und sortiert nach Potenzen von τ, so ist der Koeffizient von τ^{2d-1} eine Summe von Termen K_i mit

$$\mathrm{K}_i\,\tau^{2d-1} = \underbrace{\underset{0}{\Delta}\tau^2 \cdots \Delta\,\tau^2\,\underset{i-1}{g\,\tau}\,\Delta\,\tau^2 \cdots \underset{d-1}{\Delta}\,\tau^2}_{d \text{ Faktoren, } g\,\tau \text{ steht an der } i-1\text{-ten Stelle}} \quad \text{für } 1 \le i \le d$$

und somit ist

$$\begin{aligned}
\mathrm{K}_i &= g^{q^{2i}}\,\underbrace{\Delta^{\sum_{j=1}^{i-1} q^{2j}}}_{\Delta\text{'s vor } g}\underbrace{\Delta^{\sum_{j=i+1}^{d-1} q^{2j-1}}}_{\Delta\text{'s nach } g}\\
&= g^{q^{2i}}\,\Delta^{\sum_{j=0}^{d-1} q^{2j} + \frac{1}{q}\sum_{j=i+1}^{d-1} q^{2j} - \sum_{j=i+1}^{d-1} q^{2j} - q^{2i}}\\
&= g^{q^{2i}}\,\Delta^{\frac{q^{2d}-1}{q^2-1}}\,\Delta^{\frac{1-q}{q}\left(\frac{q^{2d}-1}{q^2-1} - \frac{q^{2(i+1)}-1}{q^2-1}\right)}\,\Delta^{-q^{2i}}\\
&= g^{q^{2i}}\,\Delta^{\frac{q^{2d}-1}{q^2-1}}\,\Delta^{-\frac{q^{2d-1}+q^{2i}}{q+1}}.
\end{aligned}$$

Insgesamt folgt damit (ii), da

$$\begin{aligned}
\mathrm{k}_{a,2d-1} &= \sum_{i=0}^{d-1} \mathrm{K}_i\\
&= \Delta^{\frac{q^{2d}-1}{q^2-1}} \sum_{i=0}^{d-1} g^{q^{2i}}\,\Delta^{-\frac{q^{2d-1}+q^{2i}}{q+1}}
\end{aligned}$$

ist. ❑

3.3 Die Hasse-Invariante

Sei L eine endliche Erweiterung von $\mathbb{F}_\mathfrak{p}$ und $\mathcal{P}$ ein normierter Erzeuger von $\mathfrak{p}$ mit Grad d.
Betrachtet man

$$\phi_\mathcal{P} = \sum_{i=0}^{2\cdot d} \mathrm{k}_{\mathcal{P},i}\tau^i,$$

so kann man mit Hilfe der Formeln aus dem vorangegangenen Abschnitt einige Aussagen über die Koeffizienten $\mathrm{k}_{\mathcal{P},i}$ machen.

Es gilt ([Gos96, Proposition 3.1.6]):

$$T^{q^i} - T = \prod_{\substack{h \in A \\ h \text{ normiert und prim} \\ \deg h | i}} h.$$

Damit folgt die Äquivalenz

$$\gamma(T^{q^i} - T) = 0 \iff i \equiv 0\ (d).$$

Da $\mathrm{k}_{\mathcal{P},0} = \gamma(f) = 0$ ist und $\gamma(T^{q^i} - T) \neq 0$ für $0 < i < d$ ist, folgt mit der Rekursion aus Lemma 3.2.2, dass alle Koeffizienten bis $\mathrm{k}_{\mathcal{P},d}$ verschwinden müssen, d. h. es folgt

$$\phi_\mathcal{P} = \sum_{i=d}^{2\cdot d} \mathrm{k}_{\mathcal{P},i}\tau^i. \tag{3.2}$$

3.3.1 Definition. *Der Koeffizient* $\mathrm{k}_{\mathcal{P},d}$ *von* $\phi_\mathcal{P}$ *heißt die* Hasse-Invariante von ϕ *und wird mit* $\mathrm{H}(\phi)$ *bezeichnet.*

3.3.2 Proposition. *Die folgenden Aussagen sind äquivalent:*

(i) $\mathrm{H}(\phi) = 0$.

(ii) $\phi_\mathcal{P}$ *ist rein inseparabel.*

(iii) ${}_\mathcal{P}\phi(\overline{L}) = \{0\}$.

(iv) $\mathrm{ht}(\phi) = \mathrm{rg}(\phi)$.

Beweis. Die Implikation (i) $\Rightarrow$ (ii) folgt wieder aus Lemma 3.2.2. Ist $\mathrm{H}(\phi) = \mathrm{k}_{\mathcal{P},d} = 0$, so müssen wegen

$$\gamma(T^{q^i} - T) \neq 0 \quad \text{für } d < i < 2d$$

die Koeffizienten $\mathrm{k}_{\mathcal{P},d+1}, \dots \mathrm{k}_{\mathcal{P},2d-1}$ gleich Null sein und damit ist

$$\phi_{\mathcal{P}} = \mathrm{k}_{\mathcal{P},2d}\tau^{2d}.$$

Die restlichen Folgerungen sind offensichtlich. ❑

3.3.3 Definition. *Ein Drinfeld-Modul heißt* supersingulär*, wenn er die Bedingungen aus Proposition* 3.3.2 *erfüllt.*

Ob Drinfeld-Moduln supersingulär sind hängt, nur von ihrer $\overline{L}$-Isomorphieklasse, d. h. von ihrer j-Invariante ab. Außerdem zeigt Proposition 2.1.3, dass Supersingularität eine Eigenschaft der Isogenieklasse ist.

3.3.4 Lemma. *Sei ϕ ein Drinfeld-Modul über L mit* $\mathrm{j}(\phi) = 0$*, d. h. ϕ ist gegeben durch $\phi_T = \gamma(T) + \Delta\,\tau^2$, dann ist*

ϕ supersingulär, falls $\deg \mathfrak{p}$ *ungerade ist, und*

ϕ ist nicht supersingulär, falls $\deg \mathfrak{p}$ *gerade ist.*

Beweis. Siehe [Gek83, Lemma 5.8 und Satz 5.9] zusammen mit Proposition 3.3.2. ❑

Sind ϕ und ϕ' isomorph über L, d. h. falls ein $\xi \in L^*$ existiert mit $\phi_T = \xi^{-1} \circ \phi'_T \circ \xi$, dann ergibt sich damit für die Koeffizienten von

$$\phi_{\mathcal{P}} = \sum_{i=d}^{2\cdot d} \mathrm{k}_{\mathcal{P},i}\,\tau^i \quad \text{und}$$
$$\phi'_{\mathcal{P}} = \sum_{i=d}^{2\cdot d} k'_{\mathcal{P},i}\,\tau^i$$

die folgende Beziehung:

$$k'_{\mathcal{P},i} = \xi^{q^i-1}\,\mathrm{k}_{\mathcal{P},i} \quad \text{für } d \leq i \leq 2\,d.$$

Also gilt insbesondere $\mathrm{H}(\phi') = \xi^{q^d-1}\ \mathrm{H}(\phi)$, und damit ist

$$\mathrm{N}^L_{\mathbb{F}_\mathfrak{p}}(\mathrm{H}(\phi')) = \mathrm{N}^L_{\mathbb{F}_\mathfrak{p}}(\xi^{q^d-1}\ \mathrm{H}(\phi)) = \mathrm{N}^L_{\mathbb{F}_\mathfrak{p}}(\mathrm{H}(\phi)).$$

Die Norm von L nach $\mathbb{F}_\mathfrak{p}$ der Hasse-Invariante ist also nur von der L-Isomorphieklasse des Drinfeld-Moduls abhängig.

Kapitel 4

Das charakteristische Polynom

4.1 Theoretische Grundlagen

Sei ϕ ein Drinfeld-Modul über dem endlichen A-Körper L. Der Frobenius $\mathcal{F}$ von L ist ein Element von $L\{\tau\}$ und kommutiert für alle $a \in A$ mit ϕ_a. Damit liegt $\mathcal{F}$ in dem Endomorphismenring von ϕ und besitzt ein Bild unter der Darstellung

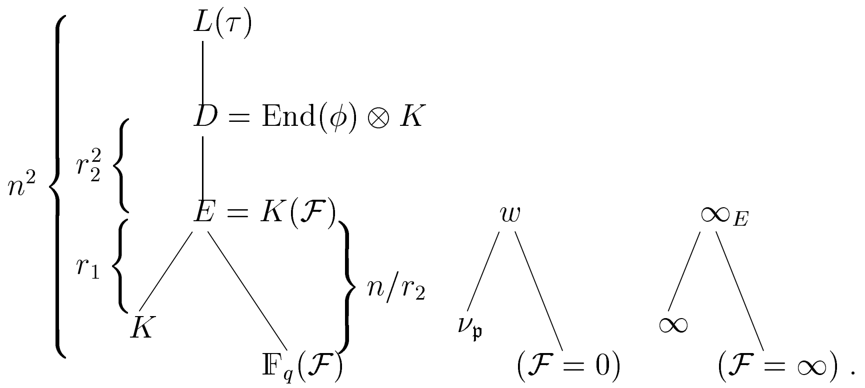
$$i_{\mathfrak{q}} : \operatorname{End}(\phi) \otimes_\nu A_\nu \hookrightarrow \operatorname{End}_{A_\nu}(T_\nu(\phi)) \cong \operatorname{Mat}(\operatorname{rg}(\phi), A_\nu).$$

Auf diese Weise wird dem Drinfeld-Modul ϕ das charakteristische Polynom $P_{\phi,\mathfrak{q}}$ von $i_{\mathfrak{q}}(\mathcal{F})$ zugeordnet. Aus [Gek91] weiß man, dass die Koeffizienten von $P_{\phi,\mathfrak{q}}$ schon in A liegen, d. h. $P_{\phi,\mathfrak{q}} = P_\phi$ ist unabhängig von der Wahl der Stelle $\mathfrak{q}$. Das Absolutglied ist bis auf einen Faktor aus $\mathbb{F}_q^*$ festgelegt. Des Weiteren ist P_ϕ eine Invariante der Isomorphieklasse von ϕ.
Der folgende Abschnitt enthält diese grundlegenden Aussagen aus [Gek91] bzw. [GS96] und gibt im Wesentlichen die dort geführten Beweise wieder.

Die Ausführungen stehen in engem Zusammenhang mit denen über den Endomorphismenring von Drinfeld-Moduln über endlichen Körpern aus Paragraph 2.2, und es gelten die an dieser Stelle eingeführten Bezeichnungen. D. h.: L ist ein endlicher A-Körper der Charakteristik $\mathfrak{p}$ und ϕ ein Rang r Drinfeld-Modul.

$$\left.\begin{array}{r} m\left\{\begin{array}{c} L \\ | \\ \mathbb{F}_{\mathfrak{p}} \end{array}\right. \\ d\left\{\begin{array}{c} | \\ \mathbb{F}_q \end{array}\right. \end{array}\right\} n$$

K wird via ϕ in $L(\tau)$ eingebettet und $\mathcal{F}$ ist der Frobenius des endlichen Körpers L. Die folgende Situation ist also gegeben ([GS96, Seite 73]):



Als Erzeuger der Erweiterung E/K besitzt $\mathcal{F}$ das Minimalpolynom $M_\phi(X)$ des Grades r_1 über A. Des Weiteren hat man für jede Stelle $\nu \in S(K)$ mit $\nu \neq \nu_\mathfrak{p}$ die Einbettung

$$i_\mathfrak{q} : \mathrm{End}(\phi) \otimes_\nu A_\nu \hookrightarrow \mathrm{End}_{A_\nu}(T_\nu(\phi)) \cong \mathrm{Mat}(r, A_\nu) \quad \text{(siehe 2.3.4).}$$

Sei $P_\phi(X)$ das charakteristische Polynom von $i_\mathfrak{q}(\mathcal{F}) \in \mathrm{End}_{A_\nu}(T_\nu(\phi))$ vom Grad r über A_ν. Das folgende Lemma zeigt den Zusammenhang zwischen $M_\phi(X)$ und $P_\phi(X)$.
Sei $\mathrm{N} : D \to K$ die Hintereinanderausführung der reduzierten Norm ${}_{\mathrm{red}}\mathrm{N}_E^D$ und der Norm N_K^E von E nach K.

$$\begin{tikzcd}
D = \mathrm{End}(\phi) \otimes K \arrow[r, hook, "i_\mathfrak{q}"] \arrow[d, "{}_{\mathrm{red}}\mathrm{N}_E^D"] \arrow[dd, bend right, "\mathrm{N}"'] & \mathrm{End}_{A_\nu}(T_\nu(\phi)) \arrow[ddl, "\det"] \\
E = K(\mathcal{F}) \arrow[d, "\mathrm{N}_K^E"] & \\
K &
\end{tikzcd}$$

4.1.1 Lemma. *Sei $u \in \mathrm{End}(\phi)$. Es gilt:*

(i) $\mathrm{N}(u) = \det(i_\nu(u))$.

(ii) $P_\phi(X) = M(X)_\phi^{r_2}$. *Insbesondere hat P_ϕ also Koeffizienten in A unabhängig von der Wahl von $\nu \neq \nu_\mathfrak{p}$.*

Beweis. (i) Die Abbildung N stimmt auf maximalen Unterkörpern $H \subseteq D$ mit der Körpernorm N_K^H überein.
Für alle $\mathfrak{q} \neq \mathfrak{p}$ ist $i_{\nu_\mathfrak{q}}(H) \otimes K_\mathfrak{q}$ eine maximale $K_\mathfrak{q}$-Unteralgebra von $\mathrm{End}_{K_\mathfrak{q}}(T_\mathfrak{q}(\phi) \otimes K_\mathfrak{q})$, deren Norm nach $K_\mathfrak{q}$ durch die Determinantenabbildung gegeben ist.
Somit gilt

$$\mathrm{N}\,|_H = (\det \circ\, i_\nu)|_H$$

für alle maximalen Unterkörper H von $\mathrm{End}(\phi) \otimes K$, so dass

$$N = \det \circ\, i_\nu$$

ist.

(ii) Sei $t \in E$. Dann folgt die Behauptung, falls $P_\phi(t) = M_\phi(t)^{r_2} gilt.$

$$\begin{aligned}
P_\phi(t) &= \det(i_\nu(t - \mathcal{F})) \stackrel{\text{(i)}}{=} \mathrm{N}((t - \mathcal{F}) \\
&= \mathrm{N}_K^E \circ_{\mathrm{red}} \mathrm{N}_E^D(t - \mathcal{F}) && \text{und mit } t - \mathcal{F} \in E \\
&= \mathrm{N}_K^E(t - \mathcal{F})^{r_2} \\
&= (\mathrm{N}_K^E(t - \mathcal{F}))^{r_2} && \text{und mit } E = K(\mathcal{F}) \\
&= (M_\phi(t))^{r_2}.
\end{aligned}$$

Damit stimmen die Polynome überein. Da $M_\phi(X)$ Koeffizienten in A hat und unabhängig von der Wahl der Stelle ν ist, gilt dies auch für $P_\phi(X)$. ❏

Damit lässt sich nun zeigen, dass das charakteristische Polynom den Drinfeld-Modul bis auf Isogenie eindeutig bestimmt.

4.1.2 Proposition. *Für zwei Drinfeld-Moduln ϕ und ψ des Ranges r über L sind die folgenden Aussagen äquivalent:*

(i) *ϕ und ψ sind isogen über L.*

(ii) $\mathrm{End}(\phi) \otimes K$ *und* $\mathrm{End}(\psi) \otimes K$ *sind $\mathcal{F}$-isomorphe K-Algebren, d. h. es existiert ein K-Isomorphismus, der mit den jeweiligen Aktionen der Frobenius-Elemente verträglich ist.*

(iii) *Die Unterkörper $E_\phi \hookrightarrow \mathrm{End}(\phi) \otimes K$ und $E_\psi \hookrightarrow \mathrm{End}(\psi) \otimes K$ sind $\mathcal{F}$-isomorph.*

(iv) $P_\phi(X) = P_\psi(X)$.

(v) $M_\phi(X) = M_\psi(X)$.

Beweis. Die Äquivalenz (iv) $\Leftrightarrow$ (v) folgt sofort aus Lemma 4.1.1.

(ii) $\Leftrightarrow$ (iii) $\Leftrightarrow$ (v):

Die Folgerung (ii) $\Rightarrow$ (iii) gilt trivialerweise, denn wenn $\mathrm{End}(\phi) \otimes K$ und $\mathrm{End}(\psi) \otimes K$ $\mathcal{F}$-isomorph sind, dann erst recht die Unterkörper E_ϕ und E_ψ.
Genauso folgt die Äquivalenz (iii) $\Leftrightarrow$ (v) sofort.
Aus Proposition 2.2.4 folgt, dass sich ein $\mathcal{F}$-Isomorphismus von E_ϕ und E_ψ eindeutig zu einem $\mathcal{F}$-Isomorphismus von $\mathrm{End}(\phi) \otimes K$ und $\mathrm{End}(\psi) \otimes K$ fortsetzen lässt, und damit die Implikation (iii) $\Rightarrow$ (ii) folgt.

(i) $\Rightarrow$ (v):

Sei $u : \phi \to \psi$ eine Isogenie von ϕ nach ψ, d. h. $u \in L\{\tau\}$ mit $u \circ \phi_a = \psi_a \circ u$ für alle $a \in A$. Sei $M_\phi(X) = \sum a_i X^i$ das Minimalpolynom von $\mathcal{F}$ bzgl. der Einbettung $\phi : K \hookrightarrow L\{\tau\}$.
Es gilt:

$$\begin{aligned} 0 = u \circ M_\phi(\mathcal{F}) &= u \circ \sum \phi_{a_i} \circ \mathcal{F}^i \\ &= u \circ \sum \mathcal{F}^i \circ \phi_{a_i} = \sum u \circ \mathcal{F}^i \circ \phi_{a_i} \\ &= \sum \mathcal{F}^i \circ u \circ \phi_{a_i} = \sum \mathcal{F}^i \circ \psi_{a_i} \circ u \\ &= \sum \psi_{a_i} \circ \mathcal{F}^i \circ u. \end{aligned}$$

Damit folgt $\sum \psi_{a_i} \mathcal{F}^i = 0$, so dass gilt $M_\phi | M_\psi$ und damit schon $M_\phi = M_\psi$.

Schließlich noch (ii) $\Rightarrow$ (i):

Sei $\alpha : \mathrm{End}(\phi) \otimes K \to \mathrm{End}(\psi) \otimes K$ ein $\mathcal{F}$-Isomorphismus. Aus dem Theorem von Skolem-Noether ([Gos96, Theorem 4.11.12]) folgt, dass ein Isomorphismus einer zentral einfachen Algebra durch einen inneren Isomorphismus induziert wird. Hieraus folgt die Existenz eines invertierbaren $u \in L(\tau)$ mit der Eigenschaft $\alpha(f) = u \circ f \circ u^{-1}$ für $f \in \mathrm{End}(\phi) \otimes K$.
Da aber $L(\tau) = L\{\tau\} \otimes_{\mathbb{F}_q\{\mathcal{F}\}} \mathbb{F}_q(\mathcal{F})$ und $\mathrm{Zentr}(\mathrm{End}(\phi) \otimes K) = \mathbb{F}_q(\mathcal{F})$ ist, lässt sich u aus $L\{\tau\}$ wählen. Da α ein K-Algebraisomorphismus ist, gilt für alle $k \in K$

$$u \circ \phi_k \circ u^{-1} = \alpha(\phi_k) = \alpha(\phi(k)) = \psi(k) = \psi_k.$$

Insbesondere $u \circ \phi_a = \psi_a \circ u$ für alle $a \in A$, d. h. u ist eine Isogenie, womit die Proposition bewiesen ist. ❑

Die folgende Proposition beschriebt das Absolutglied des charakteristischen Polynoms:

4.1.3 Proposition. *Es gilt:*

$$(P_\phi(0)) = \mathfrak{p}^m.$$

Beweis. Nach Lemma 4.1.1 folgt

$$P_\phi(0) = M_\phi(0)^{r_2} = \mathrm{N}_K^E(\mathcal{F})^{r_2}. \tag{4.1}$$

Nach Proposition 2.2.4 gibt es eine eindeutig bestimmte Stelle von E, die $\mathcal{F}$ teilt, und diese liegt über $\mathfrak{p}$. Somit ist $\mathfrak{p}$ die einzige Stelle, die $(P_\phi(0))$ teilt. Mit Proposition 1.1.4 folgt:

$$\begin{aligned}\nu_\mathfrak{p}(\mathrm{N}_K^E(\mathcal{F})) &= -\frac{1}{\deg \mathfrak{p}} \sum_{\substack{\mathfrak{q}\in S(K)\\ \mathfrak{q}\neq\mathfrak{p}}} \deg \mathfrak{q} \cdot \nu_\mathfrak{q}(\mathrm{N}_K^E(\mathcal{F})) \\ &= -\frac{\deg \infty}{\deg \mathfrak{p}} \cdot \nu_\infty(\mathrm{N}_K^E(\mathcal{F})).\end{aligned} \tag{4.2}$$

Aus (1.4) erhält man

$$\mathrm{N}_K^E(\mathcal{F}) = \mathrm{N}_{K_\infty}^{E_\infty}(\mathcal{F}). \tag{4.3}$$

Damit lässt sich nun der Exponent berechnen:

$$\begin{aligned}\nu_\mathfrak{p}(P_\phi(0)) &= \nu_\mathfrak{p}(\mathrm{N}_K^E(\mathcal{F}))^{r_2}) \\ &= r_2 \cdot \nu_\mathfrak{p}(\mathrm{N}_K^E(\mathcal{F})) && \text{mit (4.2)} \\ &= -r_2 \cdot \frac{\deg \infty}{\deg \mathfrak{p}} \cdot \nu_\infty(\mathrm{N}_K^E(\mathcal{F})) && \text{mit (4.3)} \\ &= -r_2 \cdot \frac{\deg \infty}{\deg \mathfrak{p}} \cdot \nu_\infty(\mathrm{N}_{K_\infty}^{E_\infty}(\mathcal{F})) && \text{mit Proposition 1.1.9} \\ &= -r_2 \cdot \frac{\deg \infty}{\deg \mathfrak{p}} \cdot [E_\infty : K_\infty] \cdot \nu_\infty(\mathcal{F}).\end{aligned}$$

Mit $[E_\infty : K_\infty] = [E : K]$, $\deg \mathfrak{p} = d$, $r_2 = r/[E : K]$ und $\nu_\infty(\mathcal{F}) = -\frac{n}{r\cdot\deg\infty}$ (2.4) folgt

$$\begin{aligned}\nu_\mathfrak{p}(P_\phi(0)) &= \frac{n}{d} \\ &= m.\end{aligned}$$

Also gilt die Behauptung. ❏

4.1.4 Korollar. *Existiert ein Drinfeld-Modul beliebigen Ranges über dem Körper L des Grades m über $A/\mathfrak{p}$, so folgt, dass $\mathfrak{p}^m$ ein Hauptideal ist.*

Umgekehrt werden durch Proposition 4.1.3 die Möglichkeiten für die Wahl des Körpers L, über dem sich Drinfeld-Moduln definieren lassen, durch die notwendige Bedingung, dass $\mathfrak{p}^m$ ein Hauptideal sein muss, eingeschränkt.

4.1.5 Proposition. *Sei x eine Nullstelle von $P_\phi(X)$ in einer Erweiterung von K_∞. Dann gilt:*

$$\nu_\infty(x) = -\frac{n}{r \cdot \deg \infty}.$$

Beweis. Aufgrund von Proposition 4.1.1 genügt es wieder, die Aussage für M_ϕ zu zeigen. Das Polynom M_ϕ ist aber auch das Minimalpolynom der Erweiterung E_∞/K_∞. Das Newtonpolygon besitzt daher eine einzige Strecke. Aus Proposition 4.1.3 folgt

$$\begin{aligned}\nu_\infty(P_\phi(0)) &= -\frac{\deg \mathfrak{p}}{\deg \infty} \cdot m \\ &= -\frac{n}{\deg \infty},\end{aligned}$$

so dass diese Strecke die Steigung $\frac{n}{\deg \infty \cdot r}$ hat. Damit gilt die Behauptung. ❑

4.2 Berechnung des charakteristischen Polynoms

Von nun an sei K der rationale Funktionenkörper $\mathbb{F}_q(T)$ und A der Polynomring in T. Der A-Körper L sei wie im vorherigen Abschnitt eine endliche Erweiterung vom Grad m über $A/\mathfrak{p}$. Die Stelle $\mathfrak{p}$ habe den Grad d und es sei $n = m \cdot d$.

Im Folgenden soll das charakteristische Polynom $P_\phi(X)$ eines Rang 2 Drinfeld-Moduls ϕ über L berechnet werden. $P_\phi(X) \in L\{\tau\}[X]$ ist von der Form

$$P_\phi(X) = X^2 + aX + b,$$

mit $a, b \in A$.

Aus dem vorherigen Abschnitt sind die folgenden Eigenschaften bekannt:

(i) Sei $f = \mathcal{P}^m$ ein normierter Erzeuger von $\mathfrak{p}^m = (\mathcal{P})^m$, dann folgt aus Proposition 4.1.3, dass b bis auf einen Faktor aus $\mathbb{F}_q^*$ dem Erzeuger f entspricht, d. h. es gilt:

$$b = \varepsilon_\phi \cdot f \qquad \text{mit } \varepsilon_\phi \in \mathbb{F}_q^*. \tag{4.4}$$

(ii) Für a die Spur des Frobenius folgt aus Proposition 4.1.5 die Abschätzung $\nu_\infty(a) \geq -\frac{n}{r \cdot \deg \infty} = -\frac{n}{2}$, so dass

$$\deg(a) \leq \lfloor \frac{n}{2} \rfloor \tag{4.5}$$

sein muss.

Also ist $a = \sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} a_i T^i$ und $b = \varepsilon_\phi \cdot f = \varepsilon_\phi \sum_{j=0}^{n} f_j T^j$, mit $a_i, f_j \in \mathbb{F}_q$.

Für das Frobeniuselement $\mathcal{F}$ des Körpers L gilt:

$$P_\phi(\mathcal{F}) = \mathcal{F}^2 + \phi_a \cdot \mathcal{F} + \phi_b = 0. \tag{4.6}$$

Dies lässt sich schreiben als

$$\tau^{2n} + \phi_{(\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} a_i T^i)} \, \tau^n + \phi_{(\varepsilon_\phi \sum_{j=0}^{n} f_j T^j)} = 0,$$

was äquivalent ist zu

$$\tau^{2n} + (\sum_{i=0}^{\lfloor \frac{n}{2} \rfloor} a_i \phi_T^i) \, \tau^n + \varepsilon_\phi \sum_{j=0}^{n} f_i \phi_T^j = 0. \tag{4.7}$$

Die Werte von $f_0, \ldots, f_n$ sind bekannt und der Koeffizientenvergleich von $\tau^0, \ldots, \tau^{2n}$ liefert $2n + 1$ Gleichungen für die Unbekannten $a_0, \ldots, a_{\lfloor \frac{n}{2} \rfloor}$ und ε_ϕ.

Wie das folgende Beispiel verdeutlicht, hat das hieraus resultierende Gleichungssystem eine besonders einfache Gestalt.

4.2.1 Beispiel: Sei $n = 6$, und mit $\mathrm{k}_{x,i}$ werde der Koeffizient von τ^i in ϕ_x bezeichnet, dann liefert (4.7) das folgende Gleichungssystem:

$$\begin{array}{lllllllllll}
\mathrm{k}_{T^3,6}\cdot a_3 & & & & & & & + & \mathrm{k}_{f,12}\cdot\varepsilon_\phi & = & -1\\
\mathrm{k}_{T^3,5}\cdot a_3 & & & & & & & + & \mathrm{k}_{f,11}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,4}\cdot a_3 & + & \mathrm{k}_{T^2,4}\cdot a_2 & & & & & + & \mathrm{k}_{f,10}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,3}\cdot a_3 & + & \mathrm{k}_{T^2,3}\cdot a_2 & & & & & + & \mathrm{k}_{f,9}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,2}\cdot a_3 & + & \mathrm{k}_{T^2,2}\cdot a_2 & + & \mathrm{k}_{T^1,2}\cdot a_1 & & & + & \mathrm{k}_{f,8}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,1}\cdot a_3 & + & \mathrm{k}_{T^2,1}\cdot a_2 & + & \mathrm{k}_{T^1,1}\cdot a_1 & & & + & \mathrm{k}_{f,7}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,0}\cdot a_3 & + & \mathrm{k}_{T^2,0}\cdot a_2 & + & \mathrm{k}_{T^1,0}\cdot a_1 & + & \mathrm{k}_{T^0,0}\cdot a_0 & + & \mathrm{k}_{f,6}\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0
\end{array}$$

Dass die Koeffizienten $\mathrm{k}_{f,0}, \ldots \mathrm{k}_{f,n-1}$ verschwinden müssen, folgt aus (3.2). Denn es gilt

$$\phi_f = \phi_{\mathcal{P}^m} = (\phi_{\mathcal{P}})^m = (\sum_{i=d}^{2d} \mathrm{k}_{\mathcal{P},i}\, \tau^i)^m,$$

mit dem normierten Erzeuger $\mathcal{P}$ von $\mathfrak{p}$. Deshalb ist der Koeffizient von τ^{md} der erste Koeffizient, der von Null verschieden sein kann.

Im Fall, dass n ungerade ist, verschieben sich die Koeffizienten von $a_0, \ldots, a_{\lfloor \frac{n}{2} \rfloor}$ um eine Position nach unten. Sei $n = 7$, dann erhält man diese Gleichungen:

$$\begin{array}{lllllllllll}
 & & & & & & & + & \mathrm{k}_{f,14}\cdot\varepsilon_\phi & = & -1\\
\mathrm{k}_{T^3,6}\cdot a_3 & & & & & & & + & \mathrm{k}_{f,13}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,5}\cdot a_3 & & & & & & & + & \mathrm{k}_{f,12}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,4}\cdot a_3 & + & \mathrm{k}_{T^2,4}\cdot a_2 & & & & & + & \mathrm{k}_{f,11}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,3}\cdot a_3 & + & \mathrm{k}_{T^2,3}\cdot a_2 & & & & & + & \mathrm{k}_{f,10}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,2}\cdot a_3 & + & \mathrm{k}_{T^2,2}\cdot a_2 & + & \mathrm{k}_{T^1,2}\cdot a_1 & & & + & \mathrm{k}_{f,9}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,1}\cdot a_3 & + & \mathrm{k}_{T^2,1}\cdot a_2 & + & \mathrm{k}_{T^1,1}\cdot a_1 & & & + & \mathrm{k}_{f,8}\cdot\varepsilon_\phi & = & 0\\
\mathrm{k}_{T^3,0}\cdot a_3 & + & \mathrm{k}_{T^2,0}\cdot a_2 & + & \mathrm{k}_{T^1,0}\cdot a_1 & + & \mathrm{k}_{T^0,0}\cdot a_0 & + & \mathrm{k}_{f,7}\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0\\
 & & & & & & & & 0\cdot\varepsilon_\phi & = & 0
\end{array}$$

Die Leitkoeffizienten $\mathrm{k}_{T^i,2i}$ für $i = 1, \dots, \lfloor \frac{n}{2} \rfloor$ und $i = n$ sind Potenzen von Δ (vgl. Lemma 3.2.3) und somit von Null verschieden. Daraus folgt, dass mit der Kenntnis von ε_ϕ das Gleichungssystem und damit a eindeutig bestimmt ist.
Im nächsten Abschnitt wird eine explizite Formel für ε_ϕ bewiesen, so dass man in der Lage ist, mit Hilfe des Gleichungssystems die Koeffizienten a und b des charakteristische Polynom zu berechnen.

4.2.1 Die Berechnung von ε_ϕ

Die Hauptaussage dieses Paragraphen ist die Formel für den Faktor ε_ϕ im Absolutglied des charakteristischen Polynoms, für den gilt:

$$P_\phi(X) = X^2 + a\,X + \varepsilon_\phi \cdot f.$$

Eine solche Formel findet man in [HY00] für Drinfeld-Moduln von beliebigem Rang r über dem A-Körper L, wobei A nicht der Polynomring über T sein muss. Der dortige Beweis wird mit einigen Veränderungen für die Situation eines Rang 2 Drinfeld-Moduls über dem $\mathbb{F}_q[T]$-Körper L vereinfacht.

Dafür müssen zunächst einige Begriffe eingeführt werden.

4.2.2 Definition. *Eine* Signum-Funktion *auf K_∞ ist ein Homomorphismus*

$$\mathrm{sgn}: \; K_\infty^* \longrightarrow \mathbb{F}_q^*,$$

der eingeschränkt auf $\mathbb{F}_q^*$ die Identität ist.

Eine solche Funktion lässt sich durch die Definition $\mathrm{sgn}(0) := 0$ auf ganz K_∞ erweitern. Im Folgenden sei sgn eine festgewählte Funktion mit der obigen Eigenschaft.

4.2.3 Definition. *Für eine Stelle $\mathfrak{p} \in S(K)$ und ein Element $b \in A/\mathfrak{p}$ wird das* $(q-1)$-Potenzrestsymbol *als jenes Element $\{\frac{a}{\mathfrak{p}}\}$ aus $\mathbb{F}_q^*$ definiert, welches durch die Kongruenz*

$$\left\{\frac{b}{\mathfrak{p}}\right\} \equiv b^{\frac{q^{\deg \mathfrak{p}}-1}{q-1}} \pmod{\mathfrak{p}}$$

eindeutig bestimmt ist.

Für ein beliebiges Ideal $\mathfrak{a} = (a)$ und ein Element $b \in A$, das prim zu $\mathfrak{a}$ ist, erweitert man die obige Definition auf die folgende Weise:

$$\left\{\frac{b}{a}\right\} := \left\{\frac{b}{\mathfrak{a}}\right\} := \left\{\frac{b}{\mathfrak{p}_1}\right\}^{e_1} \cdots \left\{\frac{b}{\mathfrak{p}_n}\right\}^{e_n},$$

wobei $\mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_n^{e_n}$ die Zerlegung von $\mathfrak{a}$ in Primfaktoren ist.

Für das Potenzrestsymbol gilt das folgende Reziprozitätsgesetz.

4.2.4 Proposition. *Für zwei zueinander prime Elemente a und b aus $\mathbb{F}_q[T]$ gilt:*

$$\left\{\frac{a}{b}\right\}\left\{\frac{b}{a}\right\}^{-1} = \operatorname{sgn}\left((-1)^{\deg a \cdot \deg b}\,\frac{a^{\deg b}}{b^{\deg a}}\right).$$

Beweis. Folgt aus [Neu86, Chapter IV, Theorem 9.3 und Chapter III, Theorem 5.4] angewendet auf diese spezielle Situation. ❏

Damit stehen alle Mittel zur Verfügung, um die folgende Aussage zu beweisen.

4.2.5 Proposition. *Sei $A = \mathbb{F}_q[T]$, $\mathfrak{p}$ eine Stelle von A mit normiertem Erzeuger f vom Grad d. Der Körper L sei eine endliche Erweiterung von $\mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}$ des Grades m und $n = m \cdot d$. Der Rang 2 Drinfeld-Modul ϕ über L sei gegeben durch $\phi_T = \gamma(T) + g\,\tau + \Delta\,\tau^2$ mit $g \in L, \Delta \in L^*$. Für das charakteristische Polynom in der Form $P_\phi(X) = X^2 + a\,X + b$, mit $b = \varepsilon_\phi\, f$ gilt:*

$$\varepsilon_\phi = (-1)^n \left(\Delta^{\frac{q^n-1}{q-1}}\right)^{-1}. \tag{4.8}$$

Beweis. Man kann ohne Beschränkung der Allgemeinheit voraussetzen, dass $(\mathfrak{p}, T) = 1$ gilt. Wäre dies nicht der Fall, würde man T durch $T' = T + 1$ ersetzen.

Der Modul der T-Torsionspunkte ${}_T\phi$ ist ein zwei-dimensionaler Vektorraum über $\mathbb{F}_T := \mathbb{F}_q[T]/(T)$. Der Frobenius $\mathcal{F}$ des Körpers L, gegeben durch

$$\mathcal{F}:\ x \mapsto x^{q^n},$$

operiert als $\mathbb{F}_q$-linearer Automorphismus auf ${}_T\phi$. Die Determinante dieses Automorphismus ist

$$\det_{\mathbb{F}_T}(\mathcal{F}) = b \pmod{T} = \left\{\frac{b}{T}\right\}. \tag{4.9}$$

Um die Behauptung zu erhalten, wird diese Determinante mit einer anderen Methode ein zweites Mal berechnet.

Dazu schreibt man $\phi_T \in L\{\tau\}$ in der Form

$$\phi_T = \gamma(T) + g\,\tau + \Delta\,\tau^2 = \Delta(\tau^2 + \frac{g}{\Delta}\tau + \frac{\gamma(T)}{\Delta}\tau^0).$$

Das Polynom $\frac{\phi_T}{\Delta}$ ist, wenn man es als Element von $L[X]$ auffasst, ein normiertes, $\mathbb{F}_q$-lineares Polynom, welches sich über $\overline{L}$ zerlegen lässt in

$$X^{q^2} + \frac{g}{\Delta} X^q + \frac{\gamma(T)}{\Delta} X = \prod_{h \in {}_T\phi} (X - h).$$

Auf den $\mathcal{F}$-stabilen Vektorraum ${}_T\phi$ lässt sich mit den Bezeichnungen $H = {}_T\phi$ und $a_0 = \frac{\gamma(T)}{\Delta}$ Proposition 1.2.12 anwenden, so dass folgt:

$$\begin{aligned} \det_{\mathbb{F}_T}(\mathcal{F}) &= \mathrm{N}^L_{\mathbb{F}_q}(\frac{\gamma(T)}{\Delta}) \\ &= \mathrm{N}^L_{\mathbb{F}_q}(\gamma(T)) \cdot \mathrm{N}^L_{\mathbb{F}_q}(\frac{1}{\Delta}). \end{aligned} \tag{4.10}$$

Da $\gamma(T)$ in $\mathbb{F}_\mathfrak{p}$ liegt, berechnet sich seine Norm als

$$\begin{aligned} \mathrm{N}^L_{\mathbb{F}_q}(\gamma(T)) &= \mathrm{N}^{\mathbb{F}_\mathfrak{p}}_{\mathbb{F}_q}(\gamma(T))^m \\ &= \gamma(T^{\frac{q^d-1}{q-1}})^m \\ &= \left\{\frac{T}{\mathfrak{p}}\right\}^m \qquad \text{mit } \mathfrak{p}^m = (b) \text{ (Proposition 4.1.3)} \\ &= \left\{\frac{T}{b}\right\}. \end{aligned} \tag{4.11}$$

Der Vergleich der beiden Beschreibungen von $\det_{\mathbb{F}_T}(\mathcal{F})$ in (4.9) und (4.10) liefert zusammen mit (4.11)

$$\begin{aligned} \left\{\frac{b}{T}\right\} &= \det_{\mathbb{F}_T}(\mathcal{F}) \\ &= \mathrm{N}^L_{\mathbb{F}_q}(\gamma(T))\, \mathrm{N}^L_{\mathbb{F}_q}(\frac{1}{\Delta}) \\ &= \left\{\frac{T}{b}\right\} \mathrm{N}^L_{\mathbb{F}_q}(\frac{1}{\Delta}). \end{aligned}$$

Hierauf lässt sich das Reziprozitätsgesetz aus Proposition 4.2.4 anwenden, und man erhält mit

$$\begin{aligned} \mathrm{N}^L_{\mathbb{F}_q}(\frac{1}{\Delta}) &= \left\{\frac{b}{T}\right\} \left\{\frac{T}{b}\right\}^{-1} \\ &= \operatorname{sgn}\left((-1)^{\deg b \cdot \deg T} \frac{b^{\deg T}}{T^{\deg b}}\right) \\ &= (-1)^n \operatorname{sgn}(b) \end{aligned}$$

die Behauptung

$$\varepsilon_\phi = \operatorname{sgn}(b) = (-1)^n \left(\Delta^{\frac{q^n-1}{q-1}}\right)^{-1}.$$

❑

4.2.6 Bemerkung: Im Fall, dass n ungerade ist, folgt die Aussage auch direkt aus der ersten Gleichung des Gleichungssystems. Auch falls n gerade ist, kann man, wenn $\mathrm{k}_{T^n,2n-1}$ (der zweit-höchste Koeffizient von $\phi_{\mathfrak{p}}$) nicht verschwindet, die Werte von ε_ϕ und $a_{\frac{n}{2}}$ direkt anhand der beiden ersten Gleichungen ermitteln. Wenn dies jedoch der Fall ist, kann nicht ausgeschlossen werden, dass jede zweite Gleichung nur die Information $0 = 0$ enthält, so dass das System ohne die Kenntnis von ε_ϕ unterbestimmt wäre.

4.2.2 Die Berechnung des maximalen Koeffizienten von a

In (4.5) wurde schon gezeigt, dass a höchstens den Grad $\lfloor \frac{n}{2} \rfloor$ besitzt. Falls n gerade ist, lässt sich aus [HY00, Theorem 4.5] eine Formel für den „maximal möglichen“ Koeffizienten $a_{\frac{n}{2}}$ von $a = \sum_{i=0}^{\frac{n}{2}} a_i T^i$ ableiten. Es zeigt sich, dass $a_{\frac{n}{2}}$ nur von Δ abhängt.

Diese Formel wird hier mittels des Gleichungssystems und der Aussage über ε_ϕ bewiesen, und zusätzlich wird eine ähnliche Formel im Fall „n ungerade“ für den Koeffizienten $a_{\frac{n-1}{2}}$ gezeigt. In diesem Fall ist der maximal mögliche Koeffizient nicht mehr allein von Δ abhängig, er kann jedoch durch eine geschlossene Formel in g und $\mathrm{j}(\phi)$ beschrieben werden.

4.2.7 Proposition. *Für den maximal möglichen Koeffizienten der Spur des Frobenius gelten die folgenden Formeln:*

(i) ***n gerade:***

$$a_{\frac{n}{2}} = -\operatorname{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}((\Delta^{\frac{q^n-1}{q^2-1}})^{-1}).$$

(ii) ***n ungerade:*** *Falls $g \neq 0$ ist, gilt:*

$$a_{\frac{n-1}{2}} = (g^{\frac{q^n-1}{q-1}})^{-1} \ \operatorname{Tr}_{\mathbb{F}_q}^{L}(\mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1}).$$

Beweis. (i) Durch Vergleich der Koeffizienten von τ^n in (4.7) erhält man die Gleichheit

$$a_{\frac{n}{2}} \cdot \mathrm{k}_{T^{\frac{n}{2}},n} + \varepsilon_\phi \cdot \mathrm{k}_{T^n,2n} = -1. \tag{4.12}$$

Dabei treten die Leitkoeffizienten von $\phi_{T^{\frac{n}{2}}}$ und ϕ_{T^n} auf, die sich mittels Lemma 3.2.3 berechnen lassen. Es gilt:

$$\mathrm{k}_{T^{\frac{n}{2}},n} = \Delta^{\frac{q^n-1}{q^2-1}}, \quad \text{sowie}$$
$$\mathrm{k}_{T^n,2n} = \Delta^{\frac{q^{2n}-1}{q^2-1}}.$$

Für ε_ϕ gilt aufgrund von Proposition 4.2.5, dass

$$\varepsilon_\phi = (\Delta^{\frac{q^n-1}{q-1}})^{-1}$$

ist, so dass sich $a_{\frac{n}{2}}$ bestimmen lässt, indem man diese Werte in (4.12) einsetzt:

$$\begin{aligned}
& a_{\frac{n}{2}} \cdot \Delta^{\frac{q^n-1}{q^2-1}} + (\Delta^{\frac{q^n-1}{q-1}})^{-1} \cdot \Delta^{\frac{q^{2n}-1}{q^2-1}} = -1 \\
\iff \quad & a_{\frac{n}{2}} \cdot \Delta^{\frac{q^n-1}{q^2-1}} + (\Delta^{\frac{q^n-1}{q^2-1}})^{-(q+1)} \cdot (\Delta^{\frac{q^n-1}{q^2-1}})^2 = -1 \\
\iff \quad & a_{\frac{n}{2}} = -((\Delta^{\frac{q^n-1}{q^2-1}})^{-1} + (\Delta^{\frac{q^n-1}{q^2-1}})^{-q}) \\
\iff \quad & a_{\frac{n}{2}} = -\operatorname{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}((\Delta^{\frac{q^n-1}{q^2-1}})^{-1}).
\end{aligned}$$

Damit ist Teil (i) bewiesen.

(ii) Aufgrund der nachfolgenden Proposition 4.2.11 kann hier angenommen werden, dass $g = 1$ ist, da jeder Drinfeld-Modul (falls $g \neq 0$) isomorph zu einem solchen ist.

Der Koeffizientenvergleich von τ^{2n-1} in (4.7) liefert die Gleichung

$$a_{\frac{n-1}{2}} \cdot \mathrm{k}_{T^{\frac{n-1}{2}},n-1} + \varepsilon_\phi \cdot \mathrm{k}_{T^n,2n-1} = 0. \tag{4.13}$$

Lemma 3.2.3 ergibt:

$$\begin{aligned}
\mathrm{k}_{T^{\frac{n-1}{2}},n-1} &= \Delta^{\frac{q^{n-1}-1}{q^2-1}}, \\
\mathrm{k}_{T^n,2n-1} &= \Delta^{\frac{q^{2n}-1}{q^2-1}} \sum_{i=0}^{n-1} g^{q^{2i}} \Delta^{-\frac{q^{2n-1}+q^{2i}}{q+1}} = \Delta^{\frac{q^{2n}-1}{q^2-1}} \sum_{i=0}^{n-1} \Delta^{-\frac{q^{2n-1}+q^{2i}}{q+1}}.
\end{aligned}$$

Nach Proposition 4.2.5 folgt

$$\varepsilon_\phi = -(\Delta^{\frac{q^n-1}{q-1}})^{-1}.$$

Behauptung: Für $x \in L$ und ungerades n gilt:

$$x^{\frac{q^{2n}-1}{q^2-1}} = x^{\frac{q^n-1}{q-1}}. \tag{4.14}$$

Beweis.

$$\begin{aligned}
x^{\frac{q^{2n}-1}{q^2-1}} &= x^{\frac{q^n-1}{q-1}\frac{q^n+1}{q+1}} \\
&= x^{(\frac{q^n-1}{q-1})(1+(q-1)\frac{(q^{n-1}-1)q}{q^2-1})} \\
&= x^{\frac{q^n-1}{q-1}} \quad \underbrace{x^{(q^n-1)\frac{(q^{n-1}-1)q}{q^2-1}}}_{=1,\text{ da } n \text{ ungerade und } x\in L} \\
&= x^{\frac{q^n-1}{q-1}}.
\end{aligned}$$

Insgesamt folgt damit aus Gleichung (4.13)

$$\begin{aligned}
a_{\frac{n-1}{2}} &= (\Delta^{\frac{q^{n-1}-1}{q^2-1}})^{-1} \sum_{i=0}^{n-1} \Delta^{-\frac{q^{2n-1}+q^{2i}}{q+1}} \\
&= \sum_{i=0}^{n-1} \Delta^{-\frac{q^{2n-1}+q^{2i}}{q+1}-\frac{q^{n-1}-1}{q^2-1}} \\
&=: \sum_{i=0}^{n-1} h_i.
\end{aligned}$$

Für die rechte Seite von (ii) gilt:

$$\begin{aligned}
\mathrm{Tr}_{\mathbb{F}_q}^{L}(\mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1}) &= \sum_{i=0}^{n-1}((\frac{1}{\Delta})^{\frac{q^n-q}{q^2-1}+1})^{q^i} \\
&= \sum_{i=0}^{n-1} \Delta^{-(\frac{q^n-q}{q^2-1}+1)q^i} \\
&= \sum_{i=0}^{n-1} \mathrm{k}_i,
\end{aligned} \tag{4.15}$$

mit

$$\mathrm{k}_i := \Delta^{-(\frac{q^n-q}{q^2-1}+1)q^i} \quad \text{für } i \geq 0.$$

Die rechte Seite von Gleichung (4.15) zeigt, dass $\mathrm{k}_{i+n} = \mathrm{k}_i$ gilt.

Behauptung: Es gilt:

$$h_i = \mathrm{k}_{2i+n-1} \quad \text{für } 0 \leq i \leq n-1,$$

und damit ist

$$\sum_{i=0}^{n-1} h_i = \sum_{i=0}^{n-1} \mathrm{k}_{2i+n-1} = \sum_{i=0}^{n-1} \mathrm{k}_i.$$

Beweis. Betrachtet man den Exponenten von Δ in

$$\begin{aligned}
h_i &= \Delta^{-\frac{q^{2n-1}+q^{2i}}{q+1}-\frac{q^{n-1}-1}{q^2-1}} \\
&= \Delta^{e_{\Delta,h_i}}
\end{aligned}$$

und

$$\begin{aligned}
\mathrm{k}_{2i+n-1} &= \Delta^{-(\frac{q^n-q}{q^2-1}+1)q^{2i+n-1}} \\
&= \Delta^{e_{\Delta,\mathrm{k}_{2i+n-1}}},
\end{aligned}$$

so ergibt sich

$$
\begin{aligned}
&e_{\Delta,h_i} - e_{\Delta,\mathrm{k}_{2i+n-1}} \\
&= -\frac{q^{2n-1}+q^{2i}}{q+1} - \frac{q^{n-1}-1}{q^2-1} + (\frac{q^n-q}{q^2-1}+1)q^{2i+n-1} \\
&= \frac{-q^{2n}+q^{2n-1}-q^{2i+1}+q^{2i}-q^{n-1}+1+q^{2i+2n-1}-q^{2i+n}-q^{2i+n-1}+q^{2i+n+1}}{q^2-1} \\
&= \frac{-(q^n+1)(q^n-1)+q^{n-1}(q^n-1)+q^{2i+n-1}(q^n-1)+q^{2i+1}(q^n-1)-q^{2i}(q^n-1)}{q^2-1} \\
&= \frac{-(q^n+1)+q^{n-1}+q^{2i+n-1}+q^{2i+1}-q^{2i}}{q^2-1}(q^n-1) \\
&= \Big(\frac{q^{n-1}-1}{q^2-1}+\frac{q^{2i+1}-q^n}{q^2-1}+\frac{q^{2i+n-1}-q^{2i}}{q^2-1}\Big)(q^n-1) \\
&\equiv 0\ (q^n-1).
\end{aligned}
$$

Damit gilt die Behauptung und insgesamt folgt (ii). ❑

Mit Hilfe dieser Proposition ist es in einigen Fällen möglich, einem Drinfeld-Modul anzusehen, ob der Koeffizient a des charakteristischen Polynom maximalen Grad besitzt.

4.2.8 Korollar. *Sei ϕ ein Drinfeld-Modul mit $g \neq 0$. Wenn gilt*

(i) *n ist gerade,* $\mathrm{char}(L) \neq 2$ *und*

$$\mathrm{j}(\phi)^{\frac{q^n-1}{q^2-1}} \in \mathbb{F}_q,$$

bzw.

(ii) *n ist ungerade,* $\mathrm{char}(L) \nmid n$ *und*

$$\mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1} \in \mathbb{F}_q,$$

dann nimmt a den maximal möglichen Grad an, ist also insbesondere nicht supersingulär.

Beweis. (i) Wenn g ungleich Null ist, dann lässt sich Proposition 4.2.7 umformen zu

$$
\begin{aligned}
a_{\frac{n}{2}} &= -\,\mathrm{Tr}^{\mathbb{F}_{q^2}}_{\mathbb{F}_q}((\Delta^{\frac{q^n-1}{q^2-1}})^{-1}) \\
&= -(g^{\frac{q^n-1}{q-1}})^{-1}\ \mathrm{Tr}^{\mathbb{F}_{q^2}}_{\mathbb{F}_q}((\frac{g^{q+1}}{\Delta})^{\frac{q^n-1}{q^2-1}}) \\
&= -(g^{\frac{q^n-1}{q-1}})^{-1}\ \mathrm{Tr}^{\mathbb{F}_{q^2}}_{\mathbb{F}_q}(\mathrm{j}(\phi)^{\frac{q^n-1}{q^2-1}}).
\end{aligned}
$$

Liegt $\mathrm{j}(\phi)^{\frac{q^n-1}{q^2-1}}$ schon in $\mathbb{F}_q$, dann ist unter den gemachten Voraussetzungen

$$\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(\mathrm{j}(\phi)^{\frac{q^n-1}{q^2-1}}) = 2 \cdot \mathrm{j}(\phi)^{\frac{q^n-1}{q^2-1}} \neq 0,$$

und damit verschwindet der maximale Koeffizient $a_{\frac{n}{2}}$ nicht.

(ii) Wieder gilt: Liegt $\mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1}$ schon in $\mathbb{F}_q$, so ist nach Voraussetzung

$$\mathrm{Tr}_{\mathbb{F}_q}^{L}(\mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1}) = n \cdot \mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1} \neq 0,$$

und der maximale Koeffizient

$$a_{\frac{n-1}{2}} = (g^{\frac{q^n-1}{q-1}})^{-1}\ \mathrm{Tr}_{\mathbb{F}_q}^{L}(\mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1})$$

muss von Null verschieden sein. ❑

4.2.3 Die Berechnung von a mit Hilfe der Hasse-Invarianten

Eine andere Möglichkeit, das charakteristische Polynom zu bestimmen, ist mittels der in Abschnitt 3.3 eingeführten Hasse-Invariante. Die Gleichung (4.6) liefert durch Vergleich der Koeffizienten von τ^n die folgende Aussage:

$$\mathrm{k}_{a,0} = -\mathrm{k}_{b,n}.$$

Daraus ergibt sich:

4.2.9 Proposition. *Sei $P_\phi(X) = X^2 + aX + b$ das charakteristische Polynom von $\mathcal{F}$ und ε_ϕ der Leitkoeffizient von b, dann gilt:*

$$\gamma(a) = -\varepsilon_\phi\, \mathrm{N}_{\mathbb{F}_\mathfrak{p}}^{L}(\mathrm{H}(\phi)).$$

Beweis.

$$\begin{aligned}
\gamma(a) &= \mathrm{k}_{a,0} = -\mathrm{k}_{b,n} && \text{mit } b = \varepsilon_\phi \cdot f\\
&= -\varepsilon_\phi\, \mathrm{k}_{f,n}\\
&= -\varepsilon_\phi\, \mathrm{k}_{\mathcal{P}^m,n} && \text{mit (3.2)}\\
&= -\varepsilon_\phi \prod_{i=0}^{m-1} \mathrm{k}_{\mathcal{P},d}^{q^{d\,i}}\\
&= -\varepsilon_\phi\, \mathrm{N}_{\mathbb{F}_\mathfrak{p}}^{L}(\mathrm{k}_{\mathcal{P},d})\\
&= -\varepsilon_\phi\, \mathrm{N}_{\mathbb{F}_\mathfrak{p}}^{L}(\mathrm{H}(\phi)).
\end{aligned}$$

❑

4.2.10 Korollar. *Ist $L = \mathbb{F}_\mathfrak{p}$, dann gilt:*

$$a = -\varepsilon_\phi \, \mathrm{H}(\phi), \tag{4.16}$$

mit der Darstellung von $\mathrm{H}(\phi)$ *als Element von* $\mathbb{F}_q[T]/\mathfrak{p}$.

Beweis. Die Strukturabbildung γ ist durch die Reduktion modulo $\mathfrak{p}$ vom Grad d gegeben. Der Koeffizient a hat nach (4.5) höchstens den Grad $\lfloor \frac{d}{2} \rfloor$, so dass er durch die Kongruenz

$$a \equiv -\varepsilon_\phi \, \mathrm{H}(\phi) \quad (\mathfrak{p})$$

eindeutig charakterisiert ist. ❑

Damit kennt man das charakteristische Polynom im Fall $L = \mathbb{F}_\mathfrak{p}$ schon, wenn man die Werte ε_ϕ und $\mathrm{H}(\phi)$ berechnet hat.
Ist L eine echte Erweiterung von $\mathbb{F}_\mathfrak{p}$ ist, so trifft dies nicht mehr zu, denn a kann dann auch vom Grad d oder größer sein, so dass es durch Lemma 4.2.9 nicht eindeutig festgelegt wird.

4.2.4 Das Verhalten des charakteristischen Polynoms unter $\overline{L}$-Isomorphie

Zwei Drinfeld-Moduln, die über L isogen sind, besitzen nach Proposition 4.1.2 das gleiche charakteristische Polynom. Insbesondere gilt diese Aussage für zwei L-isomorphe Drinfeld-Moduln. Es gibt aber Drinfeld-Moduln, die nicht zueinander isomorph sind über L, es jedoch werden, wenn man sie über $\overline{L}$ betrachtet (vgl. Bemerkung 3.1.4). Die nächste Proposition zeigt, wie sich die charakteristischen Polynome solcher Drinfeld-Moduln zueinander verhalten.

4.2.11 Proposition. *Sei ϕ ein Drinfeld-Modul über L, gegeben durch*

$$\phi_T = \gamma(T) + g\,\tau + \Delta\,\tau^2.$$

Für ein Element $\xi \in \overline{L}^*$ gelte $c := \xi^{q-1} \in L$, und man definiert

$$\phi_T^{(c)} := \xi^{-1} \circ \phi \circ \xi,$$

so dass

$$\phi_T^{(c)} = \gamma(T) + c \cdot g\,\tau + c^{q+1} \cdot \Delta\,\tau^2$$

ist. Es gelten die folgenden Aussagen:

(i) *Die Drinfeld-Moduln ϕ und $\phi^{(c)}$ haben die gleiche j-Invariante.*

(ii) *Sei $P_\phi(X) = X^2 + a\,X + b$ das charakteristische Polynom bzgl. ϕ, dann hat $\phi^{(c)}$ das charakteristische Polynom*

$$P_{\phi^{(c)}}(X) = X^2 + (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot a\,X + (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot b.$$

Beweis. (i) Für die j-Invariante von $\phi^{(c)}$ gilt:

$$\mathrm{j}(\phi^{(c)}) = \frac{(c\cdot g)^{q+1}}{c^{q+1}\cdot\Delta} = \frac{g^{q+1}}{\Delta} = \mathrm{j}(\phi).$$

(ii) Der konstante Term von $P_{\phi^{(c)}}(X)$ ist $\varepsilon_{\phi^{(c)}} \cdot f$ und $\varepsilon_{\phi^{(c)}}$ wird mit Hilfe von (4.8) berechnet. Man erhält:

$$\begin{aligned}\varepsilon_{\phi^{(c)}} &= (-1)^n \left((c^{q+1}\,\Delta)^{\frac{q^n-1}{q-1}}\right)^{-1}\\ &= \left(c^{\frac{q^n-1}{q-1}}\right)^{q+1} \cdot (-1)^n \left(\Delta^{\frac{q^n-1}{q-1}}\right)^{-1}\\ &= (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot \varepsilon_\phi.\end{aligned} \tag{4.17}$$

Also ist $\varepsilon_{\phi^{(c)}} \cdot f = (\frac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot \varepsilon_\phi \cdot f$, so dass die die Behauptung aus (ii) bzgl. des Absolutgliedes gezeigt ist.

Im Fall $L = \mathbb{F}_\mathfrak{p}$ ließe sich die Aussage über den linearen Term direkt aus der Formel (4.16) herleiten.
Für ein allgemeineres L betrachtet man die Gleichung (4.6) in der Form

$$P_\phi(\mathcal{F}) = \mathcal{F}^2 + (\sum_{i=0}^{n} \mathrm{k}^\phi_{a,i}) \cdot \mathcal{F} + (\sum_{i=0}^{2\cdot n} \mathrm{k}^\phi_{b,i}) = 0.$$

Der Koeffizientenvergleich von $\tau^n, \ldots, \tau^{2n}$ liefert die Beziehungen

$$\begin{aligned}\mathrm{k}^\phi_{a,i} &= -\mathrm{k}^\phi_{b,n+i} \quad \text{für } i = 0,\ldots,(n-1) \quad \text{und}\\ \mathrm{k}^\phi_{a,n} &= -\mathrm{k}^\phi_{b,2n} - 1.\end{aligned} \tag{4.18}$$

Auf die gleiche Weise erhält man für das charakteristische Polynom von $\mathcal{F}$ bzgl. $\phi^{(c)}$ mit den Koeffizienten a' und b'

$$P_{\phi^{(c)}}(\mathcal{F}) = \mathcal{F}^2 + (\sum_{i=0}^{n} \mathrm{k}^{\phi^{(c)}}_{a',i}) \cdot \mathcal{F} + (\sum_{i=0}^{2\cdot n} \mathrm{k}^{\phi^{(c)}}_{b',i}) = 0$$

die Gleichungen

$$\begin{aligned}\mathrm{k}^{\phi^{(c)}}_{a',i} &= -\mathrm{k}^{\phi^{(c)}}_{b',n+i} \quad \text{für } i = 0,\ldots,(n-1) \quad \text{und}\\ \mathrm{k}^{\phi^{(c)}}_{a',n} &= -\mathrm{k}^{\phi^{(c)}}_{b',2n} - 1.\end{aligned} \tag{4.19}$$

Wegen (4.17) gilt $b' = (\frac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot b$, und für ein beliebiges $x \in \mathbb{F}_q[T]$ folgt aus der Definition von $\phi^{(c)}$:

$$\phi^{(c)}_x = \xi^{-1} \circ \phi_x \circ \xi \quad \text{und deshalb}$$
$$\mathrm{k}^{\phi^{(c)}}_{x,i} = \xi^{q^i-1} \mathrm{k}^{\phi}_{x,i} = c^{\frac{q^i-1}{q-1}} \mathrm{k}^{\phi}_{x,i} \quad \text{für } i = 0, \ldots, 2 \cdot \deg x. \tag{4.20}$$

Insgesamt erhält man mit (4.17) - (4.20), dass für $i = 0, \ldots, (n-1)$ gilt

$$\begin{aligned}
& & \mathrm{k}^{\phi^{(c)}}_{a',i} &= -\mathrm{k}^{\phi^{(c)}}_{b',n+i} \\
&\Longleftrightarrow & \mathrm{k}^{\phi^{(c)}}_{a',i} &= -(\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot \mathrm{k}^{\phi^{(c)}}_{b,n+i} \\
&\Longleftrightarrow & c^{\frac{q^i-1}{q-1}} \cdot \mathrm{k}^{\phi}_{a',i} &= -(\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot c^{\frac{q^{n+i}-1}{q-1}} \cdot \mathrm{k}^{\phi}_{b,n+i} \\
&\Longleftrightarrow & \mathrm{k}^{\phi}_{a',i} &= -(\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot c^{\frac{q^i(q^n-1)}{q-1}} \cdot \mathrm{k}^{\phi}_{b,n+i} \\
&\Longleftrightarrow & \mathrm{k}^{\phi}_{a',i} &= -(\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot (\mathrm{N}^L_{\mathbb{F}_q}(c))^{q^i} \cdot \mathrm{k}^{\phi}_{b,n+i} \\
&\Longleftrightarrow & \mathrm{k}^{\phi}_{a',i} &= -(\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot \mathrm{k}^{\phi}_{b,n+i} \\
&\Longleftrightarrow & \mathrm{k}^{\phi}_{a',i} &= (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot \mathrm{k}^{\phi}_{a,i}.
\end{aligned}$$

Ganz analog folgert man

$$\begin{aligned}
& & \mathrm{k}^{\phi^{(c)}}_{a',n} &= -\mathrm{k}^{\phi^{(c)}}_{b',2n} - 1 \\
&\Longleftrightarrow & c^{\frac{q^n-1}{q-1}} \cdot \mathrm{k}^{\phi}_{a',n} &= -(\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot c^{\frac{q^{2n}-1}{q-1}} \cdot \mathrm{k}^{\phi}_{b,2n} - 1 \\
&\Longleftrightarrow & (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot \mathrm{k}^{\phi}_{a',n} &= -\mathrm{k}^{\phi}_{b,2n} - 1 \\
&\Longleftrightarrow & \mathrm{k}^{\phi}_{a',n} &= (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot \mathrm{k}^{\phi}_{a,n}.
\end{aligned}$$

Es gilt also für alle $i = 0, \ldots, n$

$$\mathrm{k}^{\phi}_{a',i} = (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot \mathrm{k}^{\phi}_{a,i},$$

und damit

$$\phi_{a'} = \phi_{(\frac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot a}\,,$$

so dass aus der Injektivität von ϕ die Gleichheit

$$a' = (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot a$$

folgt. Zusammen mit (4.17) liefert dies die Behauptung

$$P_{\phi^{(c)}}(X) = X^2 + (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)}) \cdot a\, X + (\tfrac{1}{\mathrm{N}^L_{\mathbb{F}_q}(c)})^2 \cdot b.$$

❑

Kapitel 5

Verteilungen von charakteristischen Polynomen

Nachdem wir in der Lage sind, das charakteristische Polynom zu berechnen, soll jetzt die Verteilung von charakteristischen Polynomen in den folgenden drei Situationen untersucht werden.

Fall (a)	$A = \mathbb{F}_q[T],\ K = \mathbb{F}_q(T),\ L = \mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}$ mit $\mathfrak{p} \in S(K)$ Berechnet werden die charakteristischen Polynome aller Drinfeld-Moduln vom Rang 2 über dem endlichen Körper L. Dies wird für alle $\mathfrak{p}$ bis zu einem gewissen Grad durchgeführt.

Fall (b)	$A = \mathbb{F}_q[T],\ K = \mathbb{F}_q(T),\ L = \mathbb{F}_{\mathfrak{p}^m}$ für ein festes $\mathfrak{p} \in S(K)$ Berechnet werden die charakteristischen Polynome aller Drinfeld-Moduln vom Rang 2 über dem endlichen Körper L. Die Stelle $\mathfrak{p}$ wird fest gewählt, während m wächst.

Fall (c)	$A = \mathbb{F}_q[T],\ K = \mathbb{F}_q(T),\ L = K$ Der Rang 2 Drinfeld-Modul ϕ über K wird an den Stellen $\mathfrak{p} \in S_\phi(K)$ reduziert und das charakteristische Polynom für $\mathrm{red}_{\mathfrak{p}} \circ \phi$ bestimmt. Dies geschieht für alle $\mathfrak{p}$ bis zu einem gewissen Grad.

Im analogen Fall von elliptischen Kurven wurden entsprechende Untersuchungen durchgeführt in [Tat65](Fall (c)), [Bir68](Fall (a)) und [Yos73](Fall (b)). Ähnlich der dortigen Situation interessieren wir uns für das statistische Verhalten der auftretenden Frobeniuselemente bzw. ihrer charakteristischen Polynome.

5.1 Umfang und Durchführung der Berechnungen im Fall (a)

5.1.1 Übersicht

Berechnet werden die charakteristischen Polynome für alle Rang 2 Drinfeld-Moduln über dem endlichen Körper $\mathbb{F}_{\mathfrak{p}} = \mathbb{F}_q[T]/\mathfrak{p}$ für alle $\mathfrak{p}$ bis zu einem gewissen Grad. Für diese Situation fanden die umfangreichsten Untersuchungen statt und die nachfolgende Tabelle zeigt, welche Fälle ausgewertet wurden.

Tabelle 5.1: Übersicht der Berechnungen im Fall (a)

q	**Grad**	**Anzahl der primen $\mathfrak{p}$ vom Grad d**	**Anzahl der Drinfeld-Moduln über $\mathbb{F}_{\mathfrak{p}}$**	**Anzahl der Isomorphieklassen von Drinfeld-Moduln über $\mathbb{F}_{\mathfrak{p}}$**
2	1	2	2	2
	2	1	12	6
	3	2	56	8
	4	3	240	18
	5	6	992	32
	6	9	4032	66
	7	18	16256	128
	8	30	65280	258
	9	56	261632	512
	10	99	1047552	1026
	11	186	4192256	2048
	12	335	16773120	4098
	13	630	67100672	8192
	14	1161	268419072	16386
	15	2182	1073709056	32768
4	1	4	12	12
	2	6	240	60
	3	20	4032	192
	4	60	65280	780
	5	204	1047552	3072
	6	670	16773120	12300

Fortsetzung auf der nächsten Seite

Fortsetzung				
	7	2340	268419072	49152
3	1	3	6	6
	2	3	72	24
	3	8	702	54
	4	18	6480	168
	5	48	58806	486
	6	116	530712	1464
	7	312	4780782	4374
	8	810	43040160	13128
	9	2184	387400806	39366
9	1	9	72	72
	2	36	6480	720
	3	240	530712	5832
	4	1620	43040160	52560
5	1	5	20	20
	2	10	600	120
	3	40	15500	500
	4	150	390000	2520
	5	624	9762500	12500
	6	2580	244125000	62520
7	1	7	42	42
	2	21	2352	336
	3	112	117306	2058
	4	588	5762400	14448
	5	3360	282458442	100842

5.1.2 Der Algorithmus

Der Algorithmus, mit dem Fall (a) berechnet wird, wird kurz erläutert. Zu konkreteren Fragen der Implementierung und des Laufzeitverhaltens sei auf Abschnitt 5.6 verwiesen.

Obwohl L im Fall (a) der Körper $\mathbb{F}_{\mathfrak{p}}$ selbst ist, wird der Algorithmus hier mit den Bezeichnungen des allgemeinen Falles einer endlichen Erweiterung vom Grad m über $\mathbb{F}_{\mathfrak{p}}$ beschrieben. Auf diese Weise lässt er sich direkt auf den Fall (b) übertragen.

$$\left.\begin{array}{r} m\left\{\begin{array}{c} L \\ | \\ \mathbb{F}_{\mathfrak{p}} \end{array}\right. \\ d\left\{\begin{array}{c} | \\ \mathbb{F}_q \end{array}\right. \end{array}\right\} n$$

Proposition 4.1.2, aus der folgt, dass isogene Drinfeld-Moduln das gleiche charakteristische Polynom besitzen, erlaubt es, die Berechnungen in einem ersten Schritt zu vereinfachen. Dies gilt insbesondere für isomorphe Drinfeld-Moduln. In Proposition 3.1.5 wird gezeigt, wie ein Repräsentantensystem der Isomorphieklassen endlicher Drinfeld-Moduln vom Rang 2 aussieht, und welche Mächtigkeiten die einzelnen Klassen besitzen.

Durch Ausprobieren wird ein Erzeuger a der multiplikativen Gruppe L^* bestimmt. Anschliesend wird ein Repräsentantensystem der Isomorphieklassen von Rang 2 Drinfeld-Moduln über L durchlaufen, und für diese das charakteristische Polynom berechnet. Der nachstehende Algorithmus illustriert dieses Verfahren.

5.1.1 Algorithmus.

```
begin
  bestimme Erzeuger a von L
  if n gerade then for i := 0 to q − 2 do
                      g := a^i
                      for j := 0 to q^n − 2 do
                          Δ := a^j;
                          berechne das charakteristische Polynom von φ_{g,Δ};
                      od
                   od
                   g := 0;
                   for j := 0 to q^2 − 2 do
                      Δ := a^j;
                      berechne das charakteristische Polynom von φ_{g,Δ};
                   od
              else
                   for i := 0 to q − 2 do
                      g := a^i
                      for j := 0 to q^n − 2 do
                          Δ := a^j;
                          berechne das charakteristische Polynom von φ_{g,Δ};
                      od
                   od
                   g := 0;
                   for j := 0 to q − 2 do
                      Δ := a^j;
                      berechne das charakteristische Polynom von φ_{g,Δ};
                   od
  fi
end
```

Aufgrund dieser Vorgehensweise muss das charakteristische Polynom nur für $(q-1)\,q^n$ Drinfeld-Moduln, falls n gerade ist, und für $(q-1)\,(q^n+q)$ Drinfeld-

Moduln, falls n ungerade ist, berechnet werden. Im Gegensatz dazu stehen $q^n\,(q^n-1)$ Fälle, würde man es für jeden Drinfeld-Modul einzeln berechnen.

Da der Grad von $a_{\phi_{g,\Delta}}$ kleiner oder gleich $\lfloor\frac{n}{2}\rfloor$ ist und $\varepsilon_{\phi_{g,\Delta}}$ in $\mathbb{F}_q^*$ liegt, gibt es für das charakteristische Polynom

$$P_{\phi_{g,\Delta}} = X^2 + a_{\phi_{g,\Delta}}\,X + \varepsilon_{\phi_{g,\Delta}}\cdot f$$

nur endlich viele Möglichkeiten. Die Häufigkeiten der einzelnen charakteristischen Polynome beim Durchlaufen des Repräsentantensystems lassen sich in einem $q^{\lfloor\frac{n}{2}\rfloor+2}$ Zellen großen Feld abspeichern.
Um die absolute Anzahl von Drinfeld-Moduln zu ermitteln, muss jede Isomorphieklasse mit ihrer Mächtigkeit (siehe Proposition 3.1.5 (iii)) gewichtet werden. Im Fall „n ungerade" sind alle Klassen gleichmächtig mit $\frac{q^n-1}{q-1}$ Elementen pro Klasse. Für „n gerade" haben die q^2-1 Klassen der Drinfeld-Moduln mit $g=0$ die Mächtigkeit $\frac{q^n-1}{q^2-1}$ im Gegensatz zu der Größe $\frac{q^n-1}{q-1}$ der anderen Klassen, so dass diese etwas stärker gewichtet werden.

Die Berechnung des charakteristischen Polynoms für einen einzelnen Vertreter ϕ einer Isomorphieklasse geschieht auf die folgende Weise:

- Berechne den Leitkoeffizienten ε_ϕ von b mittels der Formel aus Proposition 4.2.5
$$\varepsilon_\phi = (-1)^n\left(\Delta^{\frac{q^n-1}{q-1}}\right)^{-1}.$$
- Löse für die Koeffizienten $a_0,\dots,a_{\lfloor\frac{n}{2}\rfloor}$ von $a=\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor} a_iT^i$ das Gleichungssystem, welches der Koeffizientenvergleich von $\tau^n,\dots,\tau^{2n}$ aus der Gleichung (4.7)
$$\tau^{2n} + (\sum_{i=0}^{\lfloor\frac{n}{2}\rfloor} a_i\phi_T^i)\,\tau^n + \varepsilon_\phi\phi_f = 0$$
liefert.

Wie Beispiel 4.2.1 illustriert, hat dieses Gleichungssystem eine besonders einfache Gestalt. Aus Lemma 3.2.3 folgt, dass für die Leitkoeffizienten $\mathrm{k}_{T^j,2j}$ von ϕ_{T^j} gilt

$$\mathrm{k}_{T^j,2j} = \Delta^{\frac{q^{2j}-1}{q^2-1}} \quad \text{für } j=0,\dots,\lfloor\frac{n}{2}\rfloor.$$

Diese Koeffizienten sind insbesondere von Null verschieden.
Damit lassen sich $a_0,\dots,a_{\lfloor\frac{n}{2}\rfloor}$ durch die folgende Vorschrift berechnen.

5.1.2 Algorithmus.

begin berechne $\phi_f = \sum_{l=0}^{2n} \mathrm{k}_{f,l}\, \tau^l$;
for $i := 0$ to $\lfloor \frac{n}{2} \rfloor$ do
berechne $\phi_{T^i} = \sum_{l=0}^{2l} \mathrm{k}_{T^i,l}\, \tau^l$;
od
if n gerade then
$a_{\lfloor \frac{n}{2} \rfloor} := -\varepsilon_\phi \cdot \mathrm{k}_{f,2n} - 1$;
else
$a_{\lfloor \frac{n}{2} \rfloor} := -\varepsilon_\phi \cdot \mathrm{k}_{f,2n-1}$;
fi
for $i := \lfloor \frac{n}{2} \rfloor - 1$ to 0 do
$a_i := -\frac{\varepsilon_\phi \cdot \mathrm{k}_{f,2i+n} + \sum_{l=i+1}^{\lfloor \frac{n}{2} \rfloor} a_l \mathrm{k}_{T^l,2i}}{\mathrm{k}_{T^i,2i}}$;
od
end

Um die Koeffizienten zu bestimmen, genügt es also, die $\lfloor \frac{n}{2} \rfloor$ Gleichungen, die durch den Vergleich von $\tau^n, \tau^{n+2}, \ldots, \tau^{n+2\lfloor \frac{n}{2} \rfloor}$ gegeben sind, zu berücksichtigen.

5.2 Ergebnisse und Beobachtungen im Fall (a)

5.2.1 Verteilungen für festes $\mathfrak{p}$

In diesem Abschnitt wird die Verteilung aller $(q^d - 1)\, q^d$ charakteristischen Polynome über dem Körper $\mathbb{F}_\mathfrak{p}$ für ein festes $\mathfrak{p}$ des Grades d untersucht. Die Tabellen A.1 und A.2 zeigen zwei solche Verteilungen ausschnittsweise.

Eine erste Auffälligkeit sind die großen Unterschiede in den Verteilungen abhängig von der Parität von $\deg \mathfrak{p}$. Ist der Grad der Stelle ungerade und größer als Eins, so ist unter den berechneten Fällen kein einziger, in dem ein mögliches charakteristisches Polynom nicht auch auftritt.
Ein ganz anderes Verhalten zeigen die Fälle mit geradem d. Hier gibt es viele Fälle, in denen ein charakteristisches Polynom, gegeben durch die Werte a und ε_ϕ, nicht als charakteristisches Polynom eines Drinfeld-Moduls über $\mathbb{F}_\mathfrak{p}$ vorkommt. Dies lässt sich für bestimmte Situationen mit der folgenden Aussage erklären:

5.2.1 Proposition. *Ist* $\mathrm{char}(\mathbb{F}_\mathfrak{p}) \neq 2$, $\deg \mathfrak{p}$ *gerade und* $P_\phi(X) = X^2 + aX + \varepsilon_\phi \mathfrak{p}$ *das charakteristische Polynom von* $\mathcal{F}$ *bzgl.* ϕ*, dann gilt:*

Hat a nicht den maximal möglichen Grad $\frac{d}{2}$, so folgt, dass

ε_ϕ ein Quadrat ist, falls $q \equiv 3\ (4)$ gilt, bzw.

ε_ϕ kein Quadrat ist, falls $q \equiv 1\ (4)$ gilt.

Beweis. Für $x \in \overline{\mathbb{F}}_q$ gilt das Kriterium: $x \in {\mathbb{F}_q}^2 \Leftrightarrow x^{\frac{q-1}{2}} = 1$.
Es sei $\phi_T = \gamma(T) + g\,\tau + \Delta\,\tau^2$ und $\delta := \Delta^{\frac{q^n-1}{q^2-1}}$. Der maximale Koeffizient von a verschwindet nach Voraussetzung. Zusammen mit Proposition 4.2.7 (i) folgt dann

$$\begin{aligned} 0 = a_{\frac{n}{2}} &= -\operatorname{Tr}^{\mathbb{F}_{q^2}}_{\mathbb{F}_q}((\delta)^{-1}) \\ &= -\delta^{-1} - \delta^{-q}. \end{aligned}$$

Man erhält:

$$\delta^2 = -\delta^{q+1}. \tag{5.1}$$

Der Faktor ε_ϕ berechnet sich nach Formel (4.8), und es gilt

$$\begin{aligned} \varepsilon_\phi &= (\Delta^{\frac{q^n-1}{q-1}})^{-1} \\ &= (\delta^{q+1})^{-1} \\ &= ((\delta^2)^{\frac{q+1}{2}})^{-1} \qquad \text{mit (5.1)} \\ &= ((-\delta^{q+1})^{\frac{q+1}{2}})^{-1} \\ &= (-1)^{\frac{q+1}{2}}((\delta^{q+1})^{-1})^{\frac{q+1}{2}} \\ &= (-1)^{\frac{q+1}{2}}(\varepsilon_\phi)^{\frac{q+1}{2}}. \end{aligned}$$

Somit folgt

$$\varepsilon_\phi^{\frac{q-1}{2}} = (-1)^{\frac{q+1}{2}} = \begin{cases} 1 & \text{falls } q \equiv 3\ (4) \\ -1 & \text{falls } q \equiv 1\ (4). \end{cases}$$

D. h. ε_ϕ ist $\begin{cases} \text{ein Quadrat, falls } q \equiv 3\ (4) \\ \text{kein Quadrat, falls } q \equiv 1\ (4) \end{cases}$ ist. ❑

Die vorangegangene Proposition schließt es, im Fall ungerader Charakteristik und d gerade, für $\frac{(q-1)}{2} q^{\frac{d}{2}}$ Polynome von vornherein aus, als charakteristische Polynome in Frage zu kommen. Dies sind aber nicht die einzigen Polynome, deren Häufigkeit gleich Null ist. Auch Frobeniusspuren von maximalem Grad treten zusammen mit bestimmten Faktoren ε_ϕ nicht auf (vgl. Tabelle A.1 und A.2). Welche a/ε_ϕ-Kombinationen nicht vorkommen, ist hierbei abhängig von $\mathfrak{p}$, so dass kein Kriterium ähnlich zu Proposition 5.2.1 angegeben werden kann.

5.2.2 Verteilungen des Faktors ε_ϕ

Zählt man, wie oft ε_ϕ einen bestimmten Wert aus $\mathbb{F}_q^*$ annimmt, so stellt man fest, dass alle Elemente mit der gleichen Häufigkeit auftreten.

5.2.2 Notation: Mit $\mathcal{D}(L)$ sei die Menge aller Rang 2 Drinfeld-Moduln über dem endlichen Körper$L$ bezeichnet.

5.2.3 Proposition. *Es gilt:*

$$|\{\phi \in \mathcal{D}(L) \mid \varepsilon_\phi = a\}| = \frac{q^n\,(q^n-1)}{q-1} \quad \textit{für alle } a \in \mathbb{F}_q^*.$$

Beweis. Nach Formel (4.8) ist $\varepsilon_\phi = (-1)^n \left(\Delta^{\frac{q^n-1}{q-1}}\right)^{-1} = (-1)^n\,(\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(\Delta))^{-1}$. Berechnet man alle Drinfeld-Moduln über L, so nimmt Δ und damit auch ε_ϕ jeden Wert aus L^* genau q^n-mal an, so dass mit (1.3) die Behauptung folgt. ❑

5.2.3 Verteilungen des Koeffizienten a

Fasst man die Fälle mit gleichem a zusammen, d. h. man zählt das Auftreten einer bestimmten Frobeniusspur, so zeigt sich für Stellen $\mathfrak{p}$ vom Grad kleiner als vier die folgende Verteilung:

5.2.4 Vermutung. *Für $d = \deg \mathfrak{p}$ kleiner als vier verteilen sich die Häufigkeiten der Frobeniusspuren der $q^d\,(q^d-1)$ Drinfeld-Moduln über $\mathbb{F}_\mathfrak{p}$ nach der folgenden Tabelle:*

a	$\deg \mathfrak{p} = 1$	$\deg \mathfrak{p} = 2$	$\deg \mathfrak{p} = 3$
$a = 0$	$q-1$	q^2-1	$(q^3-1)(q+1)$
$a \in \mathbb{F}_q^*$	$q-1$	q^2-q-1	$q^4-(q+1)^2$
$a \in \mathbb{F}_q[T]\backslash\mathbb{F}_q$	$\neg$	q^2	q^4-q

Im Fall $\deg \mathfrak{p} = 1$ ist a aus $\mathbb{F}_q$ gegeben durch $a = \frac{g}{\Delta}$, so dass die angegebene Verteilung direkt folgt.

Ist der Grad von $\mathfrak{p}$ größer, so verteilen sich die a nicht mehr in einer solchen Regelmäßigkeit. Dazu kommt, dass die Verteilung auch nicht mehr unabhängig von $\mathfrak{p}$ ist, wie durch folgendes Beispiel verdeutlicht wird.

5.2.5 Beispiel: Für $q=3$ ergeben sich die folgenden Häufigkeiten von Elementen

$a \in A$ mit $\deg a \leq \lfloor \frac{d}{2} \rfloor$ für die angegebenen $\mathfrak{p}$.

a	$\mathfrak{p} = T^4 + 2T^2 + 2$	$\mathfrak{p} = T^4 + T^3 + 2$	$\mathfrak{p} = T^4 + T^3 + 2T + 1$
0	480	320	320
1	90	80	80
2	90	80	80
T	160	240	90
$T+1$	160	240	240
$T+2$	160	90	240
$2T$	160	240	90
$2T+1$	160	90	240
$2T+2$	160	240	240
T^2	250	240	360
T^2+1	250	330	240
T^2+2	250	360	330
T^2+T	280	330	360
T^2+T+1	280	360	240
T^2+T+2	280	240	330
T^2+2T	280	240	240
T^2+2T+1	280	120	120
T^2+2T+2	280	210	210
$2T^2$	250	240	360
$2T^2+1$	250	360	330
$2T^2+2$	250	330	240
$2T^2+T$	280	240	240
$2T^2+T+1$	280	210	210
$2T^2+T+2$	280	120	120
$2T^2+2T$	280	330	360
$2T^2+2T+1$	280	240	330
$2T^2+2T+2$	280	360	240

Dennoch zeigt auch dieses Beispiel einige Regelmäßigkeiten:

5.2.6 Beobachtung: (i) Das Verhältnis der a mit maximalem Grad zu denen mit kleinerem Grad ist q zu 1, wie schon im Fall, dass $\deg \mathfrak{p} = 2$ ist.

(ii) Die a's, die sich nur um einen Faktor aus $\mathbb{F}_q^*$ unterscheiden, treten mit derselben Häufigkeit auf.

(iii) Für $\mathfrak{p}$'s, die sich nur in T-Potenzen kleiner als $\frac{d}{2}$ unterscheiden, erhält man die gleichen Häufigkeiten in der gleichen Anzahl auf, nur werden diese auf andere a permutiert.

Dies sind keine Zufälligkeiten, sondern Aussagen, die im Folgenden verallgemeinert werden.

Für einen Erweiterungskörper L von $\mathbb{F}_\mathfrak{p}$ definiert man die folgenden Mengen:

$$\begin{aligned}\mathcal{M}(L) &:= \{\phi_{g,\Delta} \in \mathcal{D}(L) \mid a_{\phi_{g,\Delta}} \text{ ist vom Grad } \lfloor \tfrac{n}{2} \rfloor\} \quad \text{und}\\ \mathcal{N}(L) &:= \{\phi_{g,\Delta} \in \mathcal{D}(L) \mid a_{\phi_{g,\Delta}} \text{ ist vom Grad kleiner als } \lfloor \tfrac{n}{2} \rfloor\}.\end{aligned}$$

$\mathcal{D}(L)$ ist die disjunkte Vereinigung von $\mathcal{M}(L)$ und $\mathcal{N}(L)$ und es gilt $|\mathcal{D}| = |\mathcal{M}(L)| + |\mathcal{N}(L)| = q^n\,(q^n - 1)$.

5.2.7 Vermutung. *Es wird vermutet, dass für den Körper L mit q^n Elementen und n ungerade gilt:*

$$|\{x \in L \mid \mathrm{Tr}^L_{\mathbb{F}_q}(x^{\frac{q^n-q}{q^2-1}+1}) = 0\}| = q^{n-1}.$$

Erklärung: Die ist offensichtlich, falls $\mathrm{ggT}(q^n-1, \frac{q^n-q}{q^2-1}+1) = \mathrm{ggT}(\frac{n+1}{2}, q-1)$ den Wert Eins hat.
In den anderen Fällen gilt:

$$\begin{aligned}\mathrm{Tr}^L_{\mathbb{F}_q}(x^{\frac{q^n-q}{q^2-1}+1}) &= x^{(1+q+q^3+\cdots+q^{n-1})} + \cdots + x^{(1+q+q^3+\cdots+q^{n-1})\cdot q^{n-1}}\\ &= x^{1+q+q^3+\cdots+q^{n-1}} + x^{q+q^2+q^4+\cdots+q^{n-1}} + \cdots + x^{1+q^2+\cdots+q^{n-3}+q^{n-2}}.\end{aligned}$$

Dies ist ein Polynom vom Grad $q^{n-1} + \frac{q^n-q}{q^2-1}$ (vorletzter Summand) mit der minimalen x-Potenz $\frac{q^n-q}{q^2-1} + 1$ (erster Summand).
Damit folgt, dass es höchstens

$$(q^{n-1} + \frac{q^n-q}{q^2-1} - \frac{q^n-q}{q^2-1} + 1) + 1 = q^{n-1}$$

Nullstellen besitzt. Damit gilt:

$$|\{x \in L \mid \mathrm{Tr}^L_{\mathbb{F}_q}(x^{\frac{q^n-q}{q^2-1}+1}) = 0\}| \leq q^{n-1}. \tag{5.2}$$

Leider ist es mir nicht mehr gelungen, auch die umgekehrte Richtung zu zeigen. Jedoch wird sie durch alle durchgeführten Berechnungen ($|L| < 50000$) bestätigt.

5.2.8 Proposition. *Die Mengen $\mathcal{M}(L)$ und $\mathcal{N}(L)$ haben die folgenden Mächtigkeiten:*

n gerade:

$$\begin{aligned}|\mathcal{M}(L)| &= q \cdot \frac{q^n\,(q^n-1)}{q+1},\\ |\mathcal{N}(L)| &= \frac{q^n\,(q^n-1)}{q+1}.\end{aligned}$$

n ungerade:

$$|\mathcal{M}(L)| \geq (q-1)\cdot q^{n-1}\,(q^n-1),$$
$$|\mathcal{N}(L)| \leq q^{n-1}\,(q^n-1),$$

bzw. wenn man 5.2.7 *als richtig voraussetzt, oder* $\mathrm{ggT}(\frac{n+1}{2}, q-1) = 1$ *ist*

$$|\mathcal{M}(L)| = (q-1)\cdot q^{n-1}\,(q^n-1),$$
$$|\mathcal{N}(L)| = q^{n-1}\,(q^n-1).$$

Beweis. Ob $\phi_{g,\Delta}$ in $\mathcal{M}(L)$ oder $\mathcal{N}(L)$ liegt, hängt vom Verhalten des maximalen Koeffizienten ab. Ist er Null liegt $\phi_{g,\Delta}$ in $\mathcal{N}(L)$, sonst in $\mathcal{M}(L)$. Mittels Proposition 4.2.7 kann man ihn für n gerade und n ungerade unterschiedlich berechnen.

n gerade:
Für den maximalen Koeffizienten gilt die Gleichung:

$$a_{\frac{n}{2}} = -\operatorname{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}((\Delta^{\frac{q^n-1}{q^2-1}})^{-1}).$$

Es gilt:

$$\begin{aligned} & -\operatorname{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(\alpha) = 0 \\ \iff\quad & \alpha^q + \alpha = 0 \\ \iff\quad & \alpha = 0 \quad \text{oder} \quad \alpha^{q-1} = -1. \end{aligned}$$

Da Δ ungleich Null ist, folgen die Äquivalenzen

$$\begin{aligned} & a_{\frac{n}{2}} = 0 \\ \iff\quad & -\operatorname{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}((\Delta^{\frac{q^n-1}{q^2-1}})^{-1}) = 0 \\ \iff\quad & ((\Delta^{\frac{q^n-1}{q^2-1}})^{-1})^{q-1} = -1 \\ \iff\quad & \Delta^{\frac{q^n-1}{q+1}} = -1. \end{aligned}$$

Sei e ein Erzeuger der multiplikativen Gruppe L^* und $\Delta = e^i$, dann gilt

$$e^{i\cdot\frac{q^n-1}{q+1}} = -1 \quad\iff\quad \begin{cases} i = \frac{q+1}{2} + z\,(q+1),\ \text{mit } z \in \mathbb{Z} & \text{falls } 2 \nmid q, \\ i = z\,(q+1),\ \text{mit } z \in \mathbb{Z} & \text{falls } 2 \mid q. \end{cases}$$

Durchläuft Δ alle Elemente von L, dann verschwindet $a_{\frac{n}{2}}$ in beiden Fällen für $\frac{q^n-1}{q+1}$ Werte von Δ und ist ungleich Null in den restlichen $q\cdot\frac{q^n-1}{q+1}$ Fällen. Multipliziert man dies mit q^n für die möglichen Werte von g, so ist die Behauptung für n gerade gezeigt.

n ungerade:
Für $g = 0$ folgt aus Lemma 3.3.4, dass a gleich Null ist, so dass diese ϕ in $\mathcal{N}(L)$ liegen. Ist $g \neq 0$, dann gilt für den Koeffizienten $a_{\frac{n-1}{2}}$ die Gleichung:

$$a_{\frac{n-1}{2}} = (g^{\frac{q^n-1}{q-1}})^{-1}\ \mathrm{Tr}^L_{\mathbb{F}_q}(\mathrm{j}(\phi)^{\frac{q^n-q}{q^2-1}+1}).$$

Wenn Δ alle Elemente von L durchläuft, dann auch $\mathrm{j}(\phi)$, so dass die Behauptung aus Vermutung 5.2.7 folgt, da $a_{\frac{n-1}{2}}$ für alle Drinfeld-Moduln über L in höchstens (genau)

$$(q^n - 1) \cdot (q^{n-1} - 1) + (q^n - 1) = q^{n-1}(q^n - 1)$$

Fällen, wie behauptet, verschwindet. ❑

5.2.9 Bemerkung: Für n ungerade ist das Verhältnis der Häufigkeiten von Koeffizienten a mit maximalen Grad zu denjenigen mit kleinerem Grad $q-1$ zu 1. Dies entspricht genau dem Verhältnis der jeweiligen Anzahl solcher Polynome über L.

Im Fall n gerade, ist das Verhältnis der Häufigkeiten q zu 1, so dass hier die Polynome mit maximal möglichem Grad verglichen mit ihrer Anzahl überrepräsentiert sind.

Es folgt die Verallgemeinerung von Beobachtung 5.2.6 (ii).

5.2.10 Proposition. *Sei* $\mathrm{H}_L(a)$ *die Häufigkeit, mit der* a *als Frobeniusspur auftritt, wenn man* $P_\phi(X)$ *für alle* ϕ *über* L *berechnet, dann gilt:*

$$(a') = (a) \quad \Longrightarrow \quad \mathrm{H}_L(a') = \mathrm{H}_L(a).$$

D. h. Elemente aus $\mathbb{F}_q[T]$*, die sich nur um einen Faktor aus* $\mathbb{F}_q^*$ *unterscheiden, kommen mit der gleichen Häufigkeit vor.*

Beweis. Man definiert die Menge der Drinfeld-Modul mit gleicher j-Invariante

$$\mathcal{J}_k(L) := \{\, \phi \in \mathcal{D}(L) \mid \mathrm{j}(\phi) = k \,\}.$$

Ein Drinfeld-Modul werde durch ein Paar (g, Δ) dargestellt, dann gilt:

$$\mathcal{J}_k(L) = \begin{cases} \{\, (x, x^{q+1}\, k^{-1}) \mid x \in L^* \,\} & \text{falls } k \neq 0 \\ \{\, (0, x) \mid x \in L^* \,\} & \text{falls } k = 0 \end{cases}$$

Die Menge aller Drinfeld-Moduln über L ist die disjunkte Vereinigung der Mengen $\mathcal{J}_k(L)$, und für alle $k \in L$ gilt $|\mathcal{J}_k(L)| = q^n - 1$.

Nach Proposition 4.2.11 gilt für jede der Mengen $\mathcal{J}_k(L)$ mit $k \neq 0$, dass sich die Frobeniusspuren der Elemente einer solchen Menge nur um einen Faktor aus $\mathbb{F}_q^*$ unterscheiden. Sei $a^{(0)} := a_{\phi_{1,\frac{1}{k}}}$, dann ist

$$a_{\phi_{x,\frac{x^{q+1}}{k}}} = (\mathrm{N}^L_{\mathbb{F}_q}(x))^{-1} \cdot a^{(0)} \quad \text{für alle } x \in L^*.$$

Da x alle Werte aus L^* durchläuft, folgt aus den Eigenschaften der Norm (vgl. (1.3)), dass $(\mathrm{N}^L_{\mathbb{F}_q}(x))^{-1}$ jeden Wert aus $\mathbb{F}_q^*$ gleich oft, d. h. $(\frac{q^n-1}{q-1})$-mal, annimmt.

Die Behauptung gilt demnach für jede Menge $\mathcal{J}_k(L)$ mit $k \neq 0$ einzeln, d. h. wenn man sich auf Drinfeld-Moduln dieser Menge beschränkt, dann verteilen sich deren Frobeniusspuren gleichmäßig auf Elemente, die sich nur um einen Faktor aus $\mathbb{F}_q^*$ unterscheiden. Man muss dies also nur noch für $\mathcal{J}_0(L)$ zeigen.

Falls n ungerade ist, folgt aus Lemma 3.3.4, dass a immer gleich Null ist und damit gilt die Proposition.

Ist n gerade, so zerlegt man $\mathcal{J}_0(L)$ disjunkt in die folgenden Mengen:

$$\mathcal{J}_{0,l}(L) := \{\, (0,x) \mid x = e^{l+i\,(q+1)}, i = 1, \dots, \frac{q^n-1}{q+1} \}, \quad \text{für } l = 0, \dots, q,$$

wobei e ein Erzeuger der multiplikativen Gruppe L^* ist. Es gilt:

$$\mathcal{J}_0(L) = \bigcup_{l=0}^{q} \mathcal{J}_{0,l}(L).$$

Ganz analog zu den Mengen $\mathcal{J}_k(L)$ mit $k \neq 0$ folgt für jede der Mengen $\mathcal{J}_{0,l}(L)$ aus Proposition 4.2.11, dass deren Elemente jeweils bis auf einen Faktor aus $\mathbb{F}_q^*$ die gleiche Frobeniusspur besitzen. Die Faktoren, die hier auftreten sind:

$$(\mathrm{N}^L_{\mathbb{F}_q}(e^i))^{-1} = (\mathrm{N}^L_{\mathbb{F}_q}(e^{-1}))^i \quad \text{für } i = 1, \dots, \frac{q^n-1}{q+1}.$$

Die Norm bildet den Erzeuger e^{-1} auf einen Erzeuger von $\mathbb{F}_q^*$ ab, so dass auch hier gilt: jeder der $q-1$ Faktoren aus $\mathbb{F}_q^*$ tritt gleich oft auf, d. h. $(\frac{q^n-1}{q^2-1})$-mal.

Somit verteilen sich auch die a_ϕ für ϕ aus $\mathcal{J}_0(L)$ gleichmäßig, so dass die Behauptung gezeigt ist. ❑

Auch Beobachtung 5.2.6 (iii) hat zeigt einen allgemeingültigen Charakter, was an dieser Stelle jedoch nicht bewiesen wird.

5.2.4 Verteilungen für alle $\mathfrak{p}$ eines festen Grades

Im nächsten Schritt werden die Häufigkeiten der Frobeniusspuren aller Drinfeld-Moduln über $\mathbb{F}_\mathfrak{p}$ berechnet und dies für alle Primstellen $\mathfrak{p}$ eines bestimmten Grades aufsummiert. Es werden sowohl die absolute Anzahl, als auch die der Isogenieklassen von Drinfeld-Moduln mit dieser Frobeniusspur gezählt. Dies ist äquivalent, falls der untersuchte Grad ungerade ist. Falls er gerade ist, haben die Klassen, die aus Drinfeld-Moduln mit $g = 0$ bestehen, eine geringere Gewichtung, so dass zusätzlich auch die Verteilung dieser Klassen gesondert untersucht wird. Die Spalten zwei, drei und vier in den Tabellen A.3 bis A.6 zeigen Beispiele dieser Verteilungen.

Das Verhältnis von Werten a mit maximal möglichem Grad $\lfloor \frac{d}{2} \rfloor$ zu solchen mit kleinerem Grad, wird in Proposition 5.2.8 für ein einzelnes $\mathfrak{p}$ beschrieben und ist unter Annahme von Vermutung 5.2.7:

$$\begin{array}{rl} \mathbf{q} : \mathbf{1} & \text{falls } d \text{ gerade ist, und} \\ (\mathbf{q}-\mathbf{1}) : \mathbf{1} & \text{falls } d \text{ ungerade ist.} \end{array}$$

Diese Eigenschaft bleibt beim Aufsummieren über alle $\mathfrak{p}$ des gleichen Grades erhalten.

Die Anzahl der Polynome über $\mathbb{F}_q$ eines bestimmten Grades zu denen mit kleinerem Grad ist immer $(q-1):1$. Wenn im Folgenden also von „Gleichverteilung“ gesprochen wird, ist dies im Fall d gerade bzgl. der Gewichtung mit dem Faktor $\frac{q}{q-1}$ zu verstehen ist.
D. h.: Hat ein a vom Grad kleiner als $\lfloor \frac{d}{2} \rfloor$ die Häufigkeit $\mathsf{H}(a)$, dann sollte bei „gleicher“ Verteilung ein a' vom Grad gleich $\lfloor \frac{d}{2} \rfloor$ die Häufigkeit $\mathsf{H}(a') = \frac{q}{q-1}\mathsf{H}(a)$ besitzen, um diese prinzipielle Asymmetrie auszugleichen.

Ist d ungerade, so ist dies nicht nötig, da dann Anzahl und Auftreten der Fälle „a hat Grad kleiner als $\lfloor \frac{d}{2} \rfloor$“ und „$a$ hat Grad gleich $\lfloor \frac{d}{2} \rfloor$“ übereinstimmen, und damit eine echte Gleichverteilung möglich ist.

Sei $\pi_q(d)$ die Anzahl der Primstellen vom Grad d in A und

$$\mathsf{H}(a,q,d) := \Big| \bigcup_{\substack{\mathfrak{p}\in S(K) \\ \deg \mathfrak{p} = d}} \{\, \phi \in \mathcal{D}(L) \mid a_\phi = a \} \Big|,$$

die Häufigkeit von a, dann läge eine Gleichverteilung in dem obigen Sinne vor, wenn folgende Gleichheit

$$\mathsf{H}(a,q,d) = {}_{gl}\mathsf{H}(a,q,d) := \begin{cases} \pi_q(d) \cdot \frac{q^{n-1}(q^n-1)}{q^{\lfloor \frac{d}{2} \rfloor}} & \text{falls } d \text{ ungerade} \\ \begin{cases} \pi_q(d) \cdot \frac{q^{n+1}(q^n-1)}{q^{\lfloor \frac{d}{2} \rfloor}(q^2-1)} & \deg a < \lfloor \frac{d}{2} \rfloor \\ \pi_q(d) \cdot \frac{q^{n}(q^n-1)}{q^{\lfloor \frac{d}{2} \rfloor}(q+1)} & \deg a = \lfloor \frac{d}{2} \rfloor \end{cases} & \text{falls } d \text{ gerade,} \end{cases}$$

für alle $a \in A$ mit $\deg a \leq \lfloor \frac{d}{2} \rfloor$ erfüllt wäre.

Die Terme in q von ${}_{gl}\mathsf{H}$ erhält man durch Teilen der Häufigkeiten, wie sie aufgrund von Proposition 5.2.8 gegeben sind, durch die jeweilige Anzahl der Polynome aus A.

Anhand der berechneten Fälle kann man die folgende Beobachtung machen:

5.2.11 Beobachtung: Die a sind nicht gleichverteilt. Stattdessen gibt es eine begrenzte Anzahl von Häufungspunkten. Dieses Verhalten hängt nicht von d ab, d. h. für wachsendes d ändert sich die Qualität der Verteilung nicht.
Lässt man dagegen q größer werden, dann liegen die Häufungswerte immer näher beieinander, so dass sich die Verteilung für wachsendes q an ${}_{gl}\mathsf{H}$ annähert.

Für $q = 2$ zum Beispiel tritt anstelle der Gleichverteilung ${}_{gl}\mathsf{H}(a, 2, d)$ eine Verteilung mit Häufungswerten $\frac{4}{9} \cdot {}_{gl}\mathsf{H}(a, 2, d)$, $\frac{8}{9} \cdot {}_{gl}\mathsf{H}(a, 2, d)$ und $\frac{16}{9} \cdot {}_{gl}\mathsf{H}(a, 2, d)$ auf.
Die folgende Tabelle zeigt anhand verschiedener Werte von q für ungerades d die durchschnittliche, minimale und maximale Häufigkeit. Der Quotient von minimalem und maximalem Wert liegt immer näher bei Eins, so dass sich vermuten lässt, dass sich für größere q eine annähernde Gleichverteilung einstellt.

	$q = 2$	$q = 3$	$q = 4$	$q = 5$	$q = 7$
Grad	13	9	5	5	5
Durchschnitt	330261160	348124528	3339072	48734400	2766939840
Minimum	142719984	2838931680	3040356	46200836	2699883900
Maximum	652609734	5198409840	4382532	60430656	3218685120
Min/Max	0,218	0,546	0,693	0,765	0,839

Ein weiteres Phänomen wird in der nächsten Tabelle gezeigt.

$q = 2$ alle $\mathfrak{p}$ vom Grad 10 bis Grad 14					
a	$d = 10$	$d = 11$	$d = 12$	$d = 13$	$d = 14$
T^3	962302	10456076	25342590	286652236	697140338
$T^3 + 1$	1040732	11520516	27966120	312077100	767620004
$T^3 + T$	1893232	21141416	50936340	569962544	1420209504
$T^3 + T + 1$	478082	5371328	13033020	144964318	361125008
$T^3 + T^2$	1893232	21141416	50936340	569962544	1420209504
$T^3 + T^2 + 1$	478082	5371328	13033020	144964318	361125008
$T^3 + T^2 + T$	1040732	11520516	27966120	312077100	767620004
$T^3 + T^2 + T + 1$	962302	10456076	25342590	286652236	697140338

Die Werte der Tabelle legen die Existenz eines Proportionalitätsfaktors $\mathsf{C}(a)$ für a nahe, d. h. eines Faktors für den gilt $\mathsf{H}(a, q, d) = \mathsf{C}(a) \cdot {}_{gl}\mathsf{H}(a, q, d)$, der unabhängig ist vom Grad d. Darüber hinaus scheint in diesen Faktor $\mathsf{C}(a)$ einzig und allein das Nullstellenverhalten des Polynoms a einzufließen.

5.2.12 Vermutung. *Für $a \in A$ gibt es eine Konstante $\mathsf{C}(a)$, so dass gilt:*

$$\mathsf{H}(a,q,d) \approx \mathsf{C}(a) \cdot {}_{gl}\mathsf{H}(a,q,d) \quad \textit{für alle } d \geq \lfloor \frac{\deg a}{2} \rfloor.$$

Diese Konstante hängt nur von der Anzahl der Nullstellen von a über $\mathbb{F}_q$ ab.

Sei mit

$$\mathsf{N}_{\mathbb{F}_q}(a) := |\{x \in \mathbb{F}_q \mid a(x) = 0\}|$$

die Anzahl der Nullstellen des Polynoms a über $\mathbb{F}_q$ bezeichnet. Der Wert von $\mathsf{C}(a)$ verhält sich dann annähernd linear in $\mathsf{N}_{\mathbb{F}_q(a)}$, falls $q \neq 2$ ist. Für $q = 2$ zeigen die Daten ein Verhältnis von $4:2:1$ der Häufigkeiten, je nachdem, ob das betreffende a zwei, eine oder keine Nullstelle in $\mathbb{F}_2$ besitzt.

Durch die folgende Definition von $\widetilde{\mathsf{C}}(a)$ erhält man einen Wert, der die berechneten Werte mit einer bemerkenswerten Genauigkeit annähert (siehe Tabelle A.7).

5.2.13 Definition. *Eine Konstante $\mathsf{C}(a)$, wie sie in Vermutung 5.2.12 auftritt, wird in den untersuchten Fällen durch*

$$\widetilde{\mathsf{C}}(a) := \begin{cases} \frac{(q-1)^2+q+\frac{q}{q-1}\mathsf{N}_{\mathbb{F}_q}(a)}{(q-1)^2+q+\frac{q}{q-1}} & \textit{falls } q \neq 2 \\ \frac{q^2 q^{\mathsf{N}_{\mathbb{F}_q}(a)}}{(q+1)^2} & \textit{falls } q = 2 \end{cases}$$

approximiert.

Während kleine Veränderungen an den Parametern der Konstanten $\widetilde{\mathsf{C}}(a)$ diese noch etwas verbessern könnten, sprechen viele Argumente dafür, dass die prinzipielle Struktur von $\mathsf{C}(a)$ in $\widetilde{\mathsf{C}}(a)$ erfasst wird. Denn die besondere Art, in der das Nullstellenverhalten von a Einfluss auf $\widetilde{\mathsf{C}}(a)$ hat, erklärt alle der auftretenden Phänomene des Datenmaterials. Besonders augenfällig ist die folgende Beobachtung:

5.2.14 Beobachtung: Sei $q \neq 2$. Bildet man die Mengen

$$[a]_{\mathsf{abs}} := \{x \in A \mid \deg(a-x) < 1\}$$

der Elemente, die sich nur im Absolutglied unterscheiden, und summiert innerhalb dieser Gruppen die Häufigkeiten auf, so erhält man für jene Summen eine Gleichverteilung (siehe Spalten fünf und sechs in den Tabellen A.3 bis A.5).

Erklärung: Innerhalb dieser Gruppen addiert sich die Anzahl der Nullstellen über $\mathbb{F}_q$ auf genau q, so dass unter der Annahme der Vermutung 5.2.12 und Defintion 5.2.13 gilt:

$$\begin{aligned}
\mathsf{H}([a]_{\mathsf{abs}}, q, d) &:= \sum_{a \in [A]_{\mathsf{abs}}} \mathsf{H}(a, q, d) \\
&= \sum_{a \in [A]_{\mathsf{abs}}} \widetilde{\mathsf{C}}(a) \cdot {}_{gl}\mathsf{H}(a, q, d) \\
&= \left(\sum_{a \in [A]_{\mathsf{abs}}} \frac{(q-1)^2 + q + \frac{q}{q-1}\mathsf{N}_{\mathbb{F}_q}(a)}{(q-1)^2 + q + \frac{q}{q-1}} \right) \cdot {}_{gl}\mathsf{H}(a, q, d) \\
&= q \cdot {}_{gl}\mathsf{H}(a, q, d).
\end{aligned}$$

Da die Gruppen q Elemente enthalten, ergibt sich hieraus die auftretende Gleichverteilung.

5.2.15 Beobachtung: Für den Ausnahmefall „$q = 2$“ erhält man eine solche Gleichverteilung erst nach Gruppierung in Polynome, die sich bis zum linearen Term unterscheiden.

Erklärung: Auch dieses Verhalten lässt sich aus der Struktur von $\widetilde{\mathsf{C}}(a)$ ableiten. Jede dieser Gruppen enthält ein Element mit zwei Nullstellen, zwei Elemente mit einer und ein Element mit keiner Nullstelle, so dass sich die unterschiedlichen Verteilungen innerhalb jeder Gruppe herausmitteln.

Weitere Anhaltspunkte über die Natur einer solchen Konstanten sind die folgenden Auffälligkeiten.

5.2.16 Beobachtung: Alle linearen Polynome haben die gleiche Häufigkeit. Polynome aus A, die keine Nullstelle in $\mathbb{F}_q$ besitzen, wie z. B. die Konstanten ungleich Null, kommen mit der minimalen Häufigkeit vor, während für $a = 0$ das Maximum angenommen wird.

Verteilung der Drinfeld-Moduln mit $g = 0$

Ist d ungerade, so ist es interessant, die Verteilung der Drinfeld-Moduln mit $g = 0$ zu kennen, da deren Isomorphieklassen kleiner sind, und deshalb einen geringeren Beitrag zu der absoluten Anzahl von Drinfeld-Moduln leisten. Somit ist das Zählen, wie häufig ein a als die Frobeniusspur einer Isomorphieklasse auftritt, nicht äquivalent zum Zählen, wie oft dieses a als Spur der einzelnen Drinfeld-Moduln selbst auftritt. Diesbezüglich lässt sich Folgendes beobachten:

5.2.17 Beobachtung: Die Klassen, bestehend aus Drinfeld-Modul mit $g = 0$, verteilen sich auf alle der möglichen a, und zeigen eine umgekehrt proportionale Häufigkeit zu der Gesammtzahl der Klassen mit der jeweiligen Frobeniusspur, falls $a \neq 2$. Auch für $q = 2$ zeigt sich eine ähnlich ausgeglichene Verteilung auf alle a, allerdings lässt sich das antiproportionale Verhältnis zur Zahl aller Klassen nicht durchgängig beobachten.

Es machen sich also keine Häufungen in speziellen a bemerkbar, so dass eine Unterscheidung der Zählweisen unnötig scheint, da beide fast identische Verteilungen liefern.

Alle der aufgeführten Beobachtungen wurden anhand des kompletten Datenmaterials aller berechneten Fälle (siehe Tabelle 5.1) gemacht und verifiziert. Diese Daten, sowie die Berechnungen in den anderen Fällen, werden unter der Internetadresse

http://www.math.uni-sb.de/~ag-gekeler/fjung/index.html

zur vollständigen Einsicht zur Verfügung gestellt.

5.3 Der Fall (b)

Berechnet werden die charakteristischen Polynome aller Drinfeld-Moduln vom Rang 2 über dem endlichen Körper $L = \mathbb{F}_{\mathfrak{p}^m}$. Die Stelle $\mathfrak{p}$ wird fest gewählt, während m wächst. Es zeigt sich jedoch, dass die Komplexität schon für ein $\mathfrak{p}$ vom Grad kleiner gleich zwei mit größer werdendem m zu stark ansteigt, so dass eine umfangreichere Untersuchung nicht möglich ist (vgl. auch Abschnitt 5.6). Die durchgeführten Berechnungen haben also einen eher zufälligen Charakter.

Um die charakteristischen Polynome im Fall (b) zu berechnen, wird derselbe Algorithmus wie in (a) verwendet, d. h. es wird ein Repräsentantensystem der Isomorphieklassen von Drinfeld-Moduln über L durchlaufen, und für jeden Vertreter das charakteristische Polynom mittels Formel (4.8) und Lösen des Gleichungssystems (4.7) ermittelt.

Die wesentlichen Aussagen wurden auch für diese Situation schon im vorherigen Abschnitt gezeigt. So gilt Proposition 5.2.1 genauso, wenn man $\mathbb{F}_{\mathfrak{p}}$ durch L und d durch n ersetzt und Proposition 5.2.8 und Proposition 5.2.10 wurden direkt in dieser Allgemeinheit formuliert.

Tabelle B.1 zeigt ein Beispiel für eine Verteilung der Frobeniusspuren für $q = 3$ $\mathfrak{p} = T + 2$ für gerades und ungerades m. Es werden nur normierte a angeführt, da sich die Häufigkeiten der anderen mit Proposition 5.2.10 ergeben.
Es zeigen sich Muster, die sehr stark von denen abweichen, die man in Fall (a) beobachten kann.
Aufgrund der geringen Aussagekraft, der wenigen berechneten Fälle, wird auf diesen Fall von Verteilung nicht weiter eingegangen.

5.4 Umfang und Durchführung der Berechnungen im Fall (c)

5.4.1 Übersicht

Wir betrachten einen fest gewählten globalen Drinfeld-Modul ϕ über $\mathbb{F}_q(T)$. Dieser wird an den Stellen $\mathfrak{p} \in S_\phi(K)$ reduziert und das charakteristische Polynom des Frobenius von $L = \mathbb{F}_q[T]/\mathfrak{p}$ berechnet. Dies wird für alle $\mathfrak{p}$ bis zu einem bestimmten Grad durchgeführt. Die folgende Tabelle zeigt eine Auflistung der willkürlich gewählten Fälle und gibt an, bis zu welchem Grad gerechnet wurde.

Tabelle 5.6: Übersicht der Berechnungen im Fall (c)

q	Bezeichnung	$\boldsymbol{\phi}$	Bis zum Grad
2	$\phi^{(21)}$	$\phi_T = T + \tau + T\,\tau^2$	24
	$\phi^{(22)}$	$\phi_T = T + \tau + T^2\,\tau^2$	24
	$\phi^{(23)}$	$\phi_T = T + \tau + T^3\,\tau^2$	25
	$\phi^{(24)}$	$\phi_T = T + (T^2 + T + 1)\,\tau + \tau^2$	25
	$\phi^{(25)}$	$\phi_T = T + \tau + (T + 1)\,\tau^2$	25
	$\phi^{(26)}$	$\phi_T = T + \tau + (T^2 + 1)\,\tau^2$	25
	$\phi^{(27)}$	$\phi_T = T + \tau + (T^3 + 1)\,\tau^2$	25
	$\phi^{(28)}$	$\phi_T = T + \tau + (T^2 + T)\,\tau^2$	24
	$\phi^{(29)}$	$\phi_T = T + \tau + (T^3 + T + 1)\,\tau^2$	25
3	$\phi^{(31)}$	$\phi_T = T + \tau + T\,\tau^2$	16
	$\phi^{(32)}$	$\phi_T = T + \tau + T^2\,\tau^2$	16
	$\phi^{(33)}$	$\phi_T = T + \tau + (T^2 + 1)\,\tau^2$	16
	$\phi^{(34)}$	$\phi_T = T + \tau + (T^2 + 2)\,\tau^2$	16
5	$\phi^{(51)}$	$\phi_T = T + \tau + T\,\tau^2$	9
	$\phi^{(52)}$	$\phi_T = T + \tau + (T^2 + 2)\,\tau^2$	9

5.4.2 Der Algorithmus

Um das charakteristische Polynom zu bestimmen, wird (wie in den vorangegangenen Fällen) der Faktor $\varepsilon_\phi \in \mathbb{F}_q^*$ nach der Formel aus Proposition 4.2.5 berechnet. Der Koeffizient a wird aber nicht über das Gleichungssystem wie in (a) oder (b), sondern nach Lemma 4.2.9 mittels der Hasse-Invarianten bestimmt.
Die Abbildung γ ist in dieser Situation die Reduktion modulo $\mathfrak{p}$, und Korollar 4.2.10 liefert, wenn man die Elemente aus L in Form von Polynomen über $\mathbb{F}_q[T]$ modulo $\mathfrak{p}$ darstellt, die Gleichheit

$$a = -\varepsilon_\phi\,\mathrm{H}(\phi).$$

Es genügt demnach, zusätzlich zu ε_ϕ noch

$$\mathrm{H}(\mathrm{red}_\mathfrak{p} \circ \phi) = \mathrm{red}_\mathfrak{p}(\mathrm{H}(\phi)) = \mathrm{red}_\mathfrak{p}(k^\phi_{\mathfrak{p},d}),$$

d. h. den d-ten Koeffizienten von $(\mathrm{red}_\mathfrak{p} \circ \phi)(\mathfrak{p})$ bzw. von $\mathrm{red}_\mathfrak{p}(\phi_\mathfrak{p})$ zu berechnen, um das charakteristische Polynom zu bestimmen. Anstatt $\phi_\mathfrak{p}$ auszuwerten, und anschließend den mittleren Koeffizienten modulo $\mathfrak{p}$ zu reduzieren, ist es effizienter, mittels der Rekursionsformel aus Lemma 3.2.2 den d-ten Koeffizienten zu bestimmen. Diese lässt sich außerden so zu modifizieren, dass in jedem Schritt modulo $\mathfrak{p}$ reduziert werden kann.

Die neue Rekursionsformel hat die folgende Gestalt:

5.4.1 Algorithmus.

begin
  $h_{\mathfrak{p},0} := \mathrm{red}_\mathfrak{p}(\,1\,);$
  $h_{\mathfrak{p},1} := \mathrm{red}_\mathfrak{p}(\,-\frac{g}{T^q-T}\,);$
  for $i := 2$ to $d-1$ do
    $h_{\mathfrak{p},i} := \mathrm{red}_\mathfrak{p}(\,-\frac{h_{\mathfrak{p},i-1}g^{q^{i-1}}+h_{\mathfrak{p},i-2}\Delta^{q^{i-2}}}{T^{q^i}-T}\,);$
  od
  $h_{\mathfrak{p},d} := \mathrm{red}_\mathfrak{p}(\,-\frac{h_{\mathfrak{p},d-1}g^{q^{d-1}}+h_{\mathfrak{p},d-2}\Delta^{q^{d-2}}}{(T^{q^d}-T)/\mathfrak{p}}\,);$
end

5.4.1 Lemma. *Es gilt:*

$$\mathrm{red}_\mathfrak{p}(k^\phi_{\mathfrak{p},d}) = h_{\mathfrak{p},d}.$$

Beweis. Für die Koeffizienten $h_{\mathfrak{p},i}$ mit $0 \leq i \leq d-1$ gilt:

$$h_{\mathfrak{p},i} \equiv \frac{k^\phi_{\mathfrak{p},i}}{\mathfrak{p}} \quad (\mathfrak{p}^2).$$

Dies folgt, da aus der ursprünglichen Rekursion der Faktor $\mathfrak{p}$ und alle Terme, von denen man weiß, dass sie kongruent Null modulo $\mathfrak{p}^2$ sind, weggelassen wurden. Das Teilen durch $\mathfrak{p}$ wird für $h_{\mathfrak{p},d}$ wieder rückgängig gemacht, indem der Faktor $\mathfrak{p}$ aus dem Nenner entfernt wird. Damit folgt die Behauptung. ❑

Dies ist eine sehr effizient berechenbare Rekursionsformel für die Hasse-Invariante des reduzierten Drinfeld-Moduls und damit der wesentliche Teil für einen Algorithmus, um die Spur des Frobeniuselements von L zu bestimmen.

5.5 Ergebnisse und Beobachtungen im Fall (c)

In diesen Abschnitt wird untersucht, wie sich ein globaler Drinfeld-Modul

$$\phi : \mathbb{F}_q[T] \longrightarrow \mathbb{F}_q(T)\{\tau\}$$

lokal, d. h. nach Reduktion an den Stellen $\mathfrak{p}$ mit guter Reduktion verhält. Das Interesse dabei gilt dem charakteristischen Polynom des Frobenius $\mathcal{F}$ von $\mathbb{F}_\mathfrak{p}$ bzgl. des endlichen Drinfeld-Moduls

$$\mathrm{red}_\mathfrak{p} \circ \phi : \mathbb{F}_q[T] \longrightarrow \mathbb{F}_\mathfrak{p}\{\tau\}.$$

Dieses wird für alle $\mathfrak{p} \in S_\phi(K)$ eines bestimmten Grades berechnet und die Verteilung der auftretenden Frobeniusspuren $a_{\mathrm{red}_\mathfrak{p} \circ \phi}$ mit den Ergebnissen aus Abschnitt 5.2 verglichen.
Tabelle 5.6 zeigt die zufällig gewählten Beispiele, für die dieses Verfahren durchgeführt wurde.

Im Fall (a) tragen sehr viele Drinfeld-Moduln zur Verteilung bei, so dass spezielle Eigenschaften einzelner beim Betrachten der Gesamtheit aller Drinfeld-Moduln geringen Einfluss auf das Ergebnis haben. In Fall (c) dagegen ist die Wahl des Drinfeld-Moduls ϕ von entscheidender Bedeutung, so dass in Abhängigkeit von ϕ ein sehr unterschiedliches Verhalten zu erwarten ist. Aus diesem Grund sind anhand der wenigen Fälle keine allgemeingültigen Schlüsse geraten, vielmehr geben sie stichprobenartige Eindrücke der Situation wieder.

Theoretische Aussagen zu dieser Problemstellung gibt es über die Häufigkeiten von Primstellen mit supersingulärer Reduktion in [Dav95] und [Dav96], wo das asymptotische Verhalten der Funktion

$$\pi_\phi(x) := |\{\mathfrak{p} \in S_\phi(K) \mid a_{\mathrm{red}_\mathfrak{p} \circ \phi} = 0\}|$$

untersucht wird. Fragestellungen bzgl. des charakteristischen Polynoms in Fall (c) und damit allgemeinerer Frobeniusspuren als nur Null werden in Abschnitt fünf und sechs von [HY00] behandelt. So beschreibt Theorem 5.2 und Example 2 die Verteilung der Faktoren $\varepsilon_{\mathrm{red}_\mathfrak{p} \circ \phi}$ in Abhängigkeit von Δ. Mit Theorem 6.1 werden Aussagen über die Menge der Stellen $\mathfrak{p}$, für die $a_{\mathrm{red}_\mathfrak{p} \circ \phi}$ den Grad $\frac{\deg \mathfrak{p}}{2}$ hat, gemacht. Darauf die im Folgenden näher eingegangen.

5.5.1 Verteilung der Grade für alle $\mathfrak{p}$ eines festen Grades

Es werden nun die Beobachtungen erläutert, die beim Auswerten der Daten gemacht wurden. Dazu definiert man zunächst

$$\mathcal{M}_\phi(d) := \{\mathfrak{p} \in S_\phi(K) \mid \deg \mathfrak{p} = d, \deg a_{\mathrm{red}_\mathfrak{p} \circ \phi} = \lfloor \tfrac{d}{2} \rfloor\} \text{ und}$$
$$\mathcal{N}_\phi(d) := \{\mathfrak{p} \in S_\phi(K) \mid \deg \mathfrak{p} = d, \deg a_{\mathrm{red}_\mathfrak{p} \circ \phi} < \lfloor \tfrac{d}{2} \rfloor\}.$$

Als erstes wird das Verhältnis von $|\mathcal{M}_\phi(d)|$ und $|\mathcal{N}_\phi(d)|$ untersucht. Das oben erwähnte Theorem 6.1 aus [HY00] lässt sich hierfür im Fall „d gerade" anwenden. Demnach ist die Dirichlet-Dichte der Menge der Stellen, für die $a_{\mathrm{red}_\mathfrak{p}\circ\phi}$ den maximal möglichen Grad besitzt, abhängig von der unter L-Isomorphie invarianten natürlichen Zahl s, die definiert ist, als die kleinste Zahl, für die gilt:

$$\Delta^s \in (L^*)^{q^2-1}.$$

Für $q = 2$ folgt z. B.:

$$\text{Liegt } \Delta \text{ in } (L^*)^3, \text{ dann ist } a_{\mathrm{red}_\mathfrak{p}\circ\phi} < \frac{\deg \mathfrak{p}}{2} \text{ für alle } \mathfrak{p} \text{ mit } d \equiv 0\ (2). \tag{5.3}$$

In diesem Fall gibt es keine Stellen $\mathfrak{p}$, für die $a_{\mathrm{red}_\mathfrak{p}\circ\phi}$ den maximalen Grad annimmt.
Ist $s = q^2 - 1$, dann folgt:

Der Anteil der Stellen $\mathfrak{p}$ eines festen, geraden Grades mit $\mathfrak{p} \in \mathcal{M}_\phi(d)$ ist $\frac{q}{q+1}$ (siehe auch [HY00, Example 4]). (5.4)

Die folgende Tabelle zeigt die Werte von $|\mathcal{M}_\phi(d)|$ und $|\mathcal{N}_\phi(d)|$ für alle berechneten ϕ jeweils für ein gerades und ein ungerades d.

Tabelle 5.7:

		d gerade			d ungerade		
q	$\boldsymbol{\phi}$	d	$\|\mathcal{M}_\phi(d)\|$	$\|\mathcal{N}_\phi(d)\|$	d	$\|\mathcal{M}_\phi(d)\|$	$\|\mathcal{N}_\phi(d)\|$
2	$\phi^{(21)}$	22	127100	63457	23	182361	182361
	$\phi^{(22)}$	22	127100	63457	23	182361	182361
	$\phi^{(23)}$	22	0	190557	23	182361	182361
	$\phi^{(24)}$	22	0	190557	23	364722	0
	$\phi^{(25)}$	22	127100	63457	23	182361	182361
	$\phi^{(26)}$	22	127100	63457	23	182361	182361
	$\phi^{(27)}$	22	127038	63519	23	182361	182361
	$\phi^{(28)}$	22	127038	63519	23	182364	182358
	$\phi^{(29)}$	22	127038	63519	23	182584	182138
3	$\phi^{(31)}$	14	256074	85410	15	637728	318848
	$\phi^{(32)}$	14	170664	170820	15	637728	318848
	$\phi^{(33)}$	14	256152	85332	15	637536	319040
	$\phi^{(34)}$	14	256152	85332	15	637920	318656
5	$\phi^{(51)}$	8	40612	8138	9	173600	43400
	$\phi^{(52)}$	8	40612	8138	9	173770	43230

5.5.1 Beobachtung: (i) Das Verhalten im geraden Fall wird vollständig durch [HY00, Theorem 6.1] erklärt. Auf $\phi^{(23)}$ und $\phi^{(24)}$ lässt sich (5.3) anwenden, woraus die Werte Null in der vierten Spalte folgen.

Für alle anderen ϕ bis auf $\phi^{(32)}$ ist die Zahl s gleich q^2-1, d. h. Δ liegt erst durch Potenzieren mit q^2-1 in $(L^*)^{q^2-1}$, so dass (5.4) zum Tragen kommt. In diesen Fällen folgt für $|\mathcal{M}_\phi(d)|$ und $|\mathcal{N}_\phi(d)|$ stets ein Verhältnis von $q:1$ für gerades d.

Für $\phi^{(32)}$ gilt $s=\frac{q^2-1}{2}$, so dass auch hier das abweichende Verhalten durch Theorem 6.1 begründet wird.

(ii) Ist d ungerade, dann gilt für alle ϕ bis auf $\phi^{(23)}$, dass $|\mathcal{M}_\phi(d)|$ und $|\mathcal{N}_\phi(d)|$ im Verhältnis $(q-1):1$ zueinander auftreten.

(iii) Die beobachteten Beziehungen sind unabhängig von d.

5.5.2 Vermutung. *Ist q^2-1 die kleinste natürliche Zahl, so dass gilt $\Delta^{q^2-1}\in(L^*)^{q^2-1}$, dann ist das Verhältnis $|\mathcal{M}_\phi(d)|$ zu $|\mathcal{N}_\phi(d)|$*

$$\begin{array}{ll} q:1 & \textit{wenn } d \textit{ gerade ist, und} \\ (q-1):1 & \textit{wenn } d \textit{ ungerade ist.} \end{array}$$

Dies würde bedeuten, dass Drinfeld-Moduln mit solchem Δ in ihrem lokalen Verhalten eine analoge Verteilung, bzgl. Unterscheidung nach Frobeniusspur mit maximalem Grad und solche mit kleinerem Grad, besäßen, wie sie schon für Fall (a) ausgeführt wurde.

5.5.2 Verteilungen der a für alle $\mathfrak{p}$ eines festen Grades

Es folgt die Untersuchung der Vorkommen einzelner Werte von a als Koeffizient $a_{\mathrm{red}_\mathfrak{p}\circ\phi}$, wieder für alle $\mathfrak{p}\in S_\phi(K)$ eines festen Grades d. Die Tabellen C.1 und C.2 zeigen für den Drinfeld-Modul $\phi^{(29)}$ und $\phi^{(33)}$, wie sich alle Stellen des Grades 24 und 25 bzw. 14 und 15 auf die möglichen Polynome vom Grad kleiner gleich $\lfloor\frac{d}{2}\rfloor$ verteilen. Da die Anzahl dieser Polynome sehr groß ist, werden sie in Gruppen solcher Polynome zusammengefasst, die sich nur bis T^7 bzw. T^4 unterscheiden. An einigen Stellen werden diese Tabellen „auseinandergezogen", um einen Blick auf die Häufigkeiten einzelner bzw. feiner gruppierter a zu ermöglichen.

5.5.3 Beobachtung: Erfüllt ϕ die Bedingungen wie in Vermutung 5.5.2, dann zeigt sich ein zu Fall (a) analoges Verhalten, d. h.:

(i) Nach Zusammenfassen in Gruppen, die sich nur im Absolutglied (bis zum linearen Term für $q=2$) unterscheiden, erhält man eine annähernde Gleichverteilung (mit der üblichen Gewichtung der a mit $\deg a=\lfloor\frac{d}{2}\rfloor$, mit dem

Faktor $\frac{q}{q+1}$, falls d gerade ist, siehe Seite 88), mit einer stetig kleiner werdenden Standardabweichung. Während diese für $\phi^{(29)}$ und $d = 22$ (23) bei etwa 8 (5) Prozent liegt, beträgt sie für $d = 24$ (25) nur noch 5 (4) Prozent.

(ii) Die Häufigkeit eines bestimmten a scheint auch in diesem Fall durch einen Proportionalitätsfaktor, der das Verhältnis zur Gleichverteilung beschreibt und unabhängig von d ist, gegeben zu sein.

(iii) Darüber hinaus unterliegt dieser Proportionalitätsfaktor ähnlichen Gesetzmäßigkeiten wie die in 5.2.12 für den Fall (a) vermutete Konstante $\mathsf{C}(a)$, d. h. der Faktor ist abhängig vom Nullstellenverhalten von a.

Die Stringenz dieser Beobachtungen ist bei weitem nicht so hoch wie in Fall (a), wo das Verhältnis der Ereignisse zu den möglichen Werten, d. h. die Anzahl der betrachteten endlichen Drinfeld-Moduln zu den möglichen Spuren mit dem ungefähren Wert $\frac{q^{3d}}{d\, q^{\lfloor \frac{d}{2} \rfloor + 1}}$ sehr groß ist. Damit sind die Verteilungen sehr stabil. Im Fall (c) beträgt dieses Verhältnis der Anzahl der Stellen vom Grad d zu den möglichen Frobeniusspuren ca. $\frac{q^{d}}{d\, q^{\lfloor \frac{d}{2} \rfloor + 1}}$, so dass man noch größere Grade, als die hier berechneten, betrachten müsste, um ausagekräftigere Ergebnisse zu erhalten.

Jedoch zeigen alle untersuchten Fälle mit $s = q^2 - 1$ die Tendenz zu einem analogen Verhalten wie es in Fall (a) sehr eindeutig festgestellt werden kann. Dies hätte dann auch in diesem Fall die Existenz einer Konstanten $\mathsf{D}(a)$ zur Folge, für die gilt:

$$\mathsf{H}'(a, \phi, q, d) = \mathsf{D}(a) \cdot {}_{gl}\mathsf{H}'(a, \phi, q, d),$$

mit

$$\mathsf{H}'(a, \phi, q, d) := |\{\mathfrak{p} \in S_\phi(K) \mid \deg \mathfrak{p} = d, a_{\mathrm{red}_\mathfrak{p} \circ \phi} = a\}|,$$

sowie der „Gleichverteilung“

$${}_{gl}\mathsf{H}'(a, \phi, q, d) := \begin{cases} \frac{\pi_q(d)}{q^{\lfloor \frac{d}{2} \rfloor + 1}} & \text{falls } d \text{ ungerade} \\ \begin{cases} \frac{q \cdot \pi_q(d)}{(q^2-1)\, q^{\lfloor \frac{d}{2} \rfloor}} & \text{falls } \deg a = \lfloor \frac{d}{2} \rfloor \\ \frac{\pi_q(d)}{(q+1)\, q^{\lfloor \frac{d}{2} \rfloor}} & \text{falls } \deg a < \lfloor \frac{d}{2} \rfloor \end{cases} & \text{falls } d \text{ gerade,} \end{cases}$$

und $\mathsf{D}(a)$ hängt nur von der Anzahl der Nullstellen von a ab.

Auch die Drinfeld-Moduln $\phi^{(23)}$, $\phi^{(24)}$ und $\phi^{(32)}$, die bzgl. des Verhältnises von $|\mathcal{M}_\phi(d)|$ und $|\mathcal{N}_\phi(d)|$ ein abweichendes Verhalten besitzen, zeigen für die a, die als Werte vorkommen, ein sehr regelmäßiges Verhalten. Interessant ist hier das

Verhalten von $\phi^{(23)}$ (siehe Tabelle C.3 und C.4), da hier zum ersten Mal die Abhängigkeit von d über die Parität hinaus geht, wie man für $d = 22$ und $d = 24$ sieht. So treten einmal nur a mit $0 \leq \deg a \leq \lfloor \frac{d}{2} \rfloor - 1$ auf, während für $d = 24$ nur solche mit $\lfloor \frac{d}{2} \rfloor - 1 \leq \deg a \leq \lfloor \frac{d}{2} \rfloor$ vorkommen. Auch für ungerade d zeigen sich an diesen Fall Besonderheiten, die man nur an diesem Beispiel findet.
Weder für $\phi^{(24)}$ noch für $\phi^{(32)}$ lässt sich ein solches Verhalten beobachten.

Wie schon in Fall (a) gilt, dass alle der angeführten Beobachtungen anhand des kompletten Datenmaterials verifiziert wurden. Auch diese Daten stehen unter der Internetadresse

http://www.math.uni-sb.de/∼ag-gekeler/fjung/index.html

zur Verfügung.

5.6 Implementierung

Alle Berechnungen wurden mit Hilfe des Computeralgebrasystems **Simath** durchgeführt. **Simath** erweitert die Programmiersprache **C** um Datentypen und Funktionen für den Umgang mit Objekten der algebraischen Zahlentheorie. So werden Hilfsmittel zum Rechnen in endlichen Körpern, zur Konstruktion von Körpererweiterungen, Datentypen für Polynome usw. zur Verfügung gestellt. Für genauere Informationen über **Simath** und dessen Anwendungsgebiete sei auf die Homepage des **Simath**-Projekts verwiesen:

http://diana.math.uni-sb.de/∼simath/index.html

Die Programme liefen auf verschiedenen Rechnern des Fachbereichs Mathematik an der Universität des Saarlandes. Dies sind zum größten Teil 4×550 MHz Pentium III Maschinen mit einem **Linux** Betriebssystem. Dem jeweiligen Prozessen standen zumeist 99 Prozent der Rechenleistung einer CPU zu Verfügung. Die Berechnungen wurden über das letzte Jahr verteilt durchgeführt. Die Quelldateien umfassen ca. 3000 Zeilen Code, und werden nach Rücksprache gerne zur Einsicht überlassen.

Grundlegend für alle Algorithmen ist das Rechnen in endlichen Körpern. Die **Simath**-Darstellung von Elementen eines endlichen Körpers $\mathbb{F}_q$, mit $q = p^l$, geschieht in Form von Polynomen über dem Primkörper $\mathbb{F}_p$ des Grades kleiner als l.
Betrachtet man eine endliche Erweiterung von $\mathbb{F}_q$ (in unserem Fall zum Beispiel den Körper $\mathbb{F}_\mathfrak{p}$), so gibt es für Elemente dieser Erweiterung zwei mögliche Darstellungen.

(i) Man benutzt die in **Simath** eingebaute Funktion, die einen Erweiterungskörper konstruiert und die Einbettung von $\mathbb{F}_q$ in diesen beschreibt. Die Elemente von $\mathbb{F}_\mathfrak{p}$ sind wieder Polynome über $\mathbb{F}_p$, diesmal vom Grad kleiner als $d \cdot l$. Hierbei ist die Darstellung eines Elements von $\mathbb{F}_q$ nicht identisch mit der Darstellung des gleichen Elements eingebettet in $\mathbb{F}_\mathfrak{p}$.

(ii) Die zweite Möglichkeit besteht darin, mit Polynomen über $\mathbb{F}_q$ modulo dem Primideal $\mathfrak{p}$ zu rechnen. Auf diese Weise haben die Elemente von $\mathbb{F}_\mathfrak{p}$ die Darstellung als Polynome vom Grad kleiner d, deren Koeffizienten Polynome vom Grad kleiner als l über $\mathbb{F}_p$ sind. Die Einbettung von $\mathbb{F}_q$ in $\mathbb{F}_\mathfrak{p}$ geschieht in Form der konstanten Polynome.

Beide Darstellungen haben jeweils Vor- und Nachteile. Die Berechnung der Erweiterung wie in (i) benötigt je nach Grad erhöhte Rechenzeit. Hat man den Körper aber erst konstruiert, so kann man mit seinen Elementen sehr effizient rechnen und hat alle **Simath**-Funktionen für deren Manipulation zur Verfügung.

Bei der Methode in (ii) ist das Rechnen mit den Elementen von $\mathbb{F}_\mathfrak{p}$ etwas langsamer, dafür wird aber keine Rechenzeit zur Beschreibung der Erweiterung –speziell der Einbettung von $\mathbb{F}_q$ nach $\mathbb{F}_\mathfrak{p}$– benötigt.

Darin ist begründet, warum in den Fällen (a) und (b) das charakteristische Polynom mittels des Gleichungssystems und in Fall (c) über die Hasse-Invariante bestimmt wird.
In (a) und (b) berechnet man $P_{\phi_{g,\Delta}}(X)$ für alle endlichen Drinfeld-Moduln über einem festen Körper $\mathbb{F}_\mathfrak{p}$ bzw. L. Dadurch wird die aufwendige Konstruktion dieses Körpers, wie es (i) beschreibt, durch das effizientere Rechnen mit seinen Elementen kompensiert. Des Weiteren sind die Grade der Erweiterung in beiden Fällen sehr klein.

Im Fall (c) wird für den Körper $\mathbb{F}_\mathfrak{p}$ lediglich ein charakteristisches Polynom berechnet und anschließend zum nächsten $\mathfrak{p}$ übergegangen. Zusätzlich haben die Erweiterungen einen höheren Grad, so dass es effizienter ist, nicht jeden Körper einzeln zu erzeugen, sondern mittels der in (ii) beschriebenen Methode, d. h. modulo dem Primideal $\mathfrak{p}$ über $\mathbb{F}_q$ zu rechnen.
Allgemein lässt sich festhalten, dass die Berechnung eines einzelnen charakteristischen Polynoms, nur Sekundenbruchteile an Rechenzeit benötigt. Die Komplexität der Aufgabenstellungen besteht in der rasant wachsenden Zahl der Fälle, die ausgewertet werden müssen.

In Fall (a) und Fall (c) läuft man über alle Primpolynome aus $\mathbb{F}_q[T]$ bis zu einem bestimmten Grad. Deren Anzahl nimmt, wie die dritte Spalte von Tabelle 5.1 verdeutlicht, exponentiell zu und kann mit $\frac{q^d}{d}$ abgeschätzt werden.
In (a) werden jeweils ca. q^{d+1} charakteristische Polynome berechnet. Beispielsweise dauert die Auswertung für ein $\mathfrak{p}$ im Fall $q = 2$ und $\deg \mathfrak{p} = 15$ ungefähr eine Stunde, so dass die Berechnung aller 2182 Stellen des Grades 15 drei Monate Rechenzeit in Anspruch nimmt.
Es ist problemlos möglich, für ein ausgewähltes $\mathfrak{p}$ eines höheren Grades die charakteristischen Polynome aller Drinfeld-Moduln über $\mathbb{F}_\mathfrak{p}$ zu berechnen, doch es ist nicht möglich, dies für alle $\mathfrak{p}$ in einer annehmbaren Zeit zu bewältigen. Solche Einzelfälle sind jedoch für die in dieser Arbeit untersuchten Verteilungen uninteressant.
Somit stellen die in Tabelle 5.1 aufgeführten Grade, bis zu denen Fall (a) berechnet wurde, die Grenze der Fälle dar, die in angemessener Zeit vollständig ausgewertet werden können.

Im Fall (c) wächst die Komplexität der Berechnungen für ein einzelnes $\mathfrak{p}$ nur unwesentlich mit dem Grad von $\mathfrak{p}$ an. Aus diesem Grund liegt die Grenze des Grades, bis zu dem alle Primstellen von $\mathbb{F}_q[T]$ betrachtet werden können, höher.

Fall (b) erfordert die Berechnung einer zweiten Erweiterung L vom Grad m über $\mathbb{F}_\mathfrak{p}$. Der Körper L besitzt q^{dm} Elemente. Man muss $d = \deg \mathfrak{p}$ sehr klein wählen, um die charakteristischen Polynome aller Drinfeld-Moduln über L in vernünftiger Zeit berechnen zu können. Mit m wächst die Mächtigkeit von L sehr stark an, so dass auf umfangreiche Berechnungen in diesem Fall zu Gunsten von (a) und (c) verzichtet wurde.

Anhang A

Tabellen Fall (a)

A.1 Verteilungen für eine feste Stelle $\mathfrak{p}$

Die Tabellen A.1 und A.2 zeigen Beispiele von Verteilungen der charakteristischen Polynome des Frobenius $\mathcal{F}$ von $L = \mathbb{F}_\mathfrak{p} = \mathbb{F}_q[T]/\mathfrak{p}$, für alle Drinfeld-Moduln über L.

In der dritten Spalte stehen die Häufigkeiten für ein zufällig gewähltes $\mathfrak{p}$ vom Grad 4, in der vierten Spalte die einer Stelle $\mathfrak{p}$ vom Grad 5. Ein charakteristisches Polynom $P_\phi(X) = X^2 + a\,X + \varepsilon_\phi\,\mathfrak{p}$ wird durch $a \in \mathbb{F}_q[T]$ und $\varepsilon_\phi \in \mathbb{F}_q^*$ repräsentiert.

Tabelle A.1:

$q = 3$, $\mathfrak{p}$ vom Grad 4 und 5			
a	ε_ϕ	$\mathfrak{p} = T^4 + 2T^3 + 2$	$\mathfrak{p} = T^5 + T^4 + T^2 + 2T + 2$
0	1	320	1331
	2	0	2299
1	1	80	968
	2	0	484
2	1	80	968
	2	0	484
T	1	240	2178
	2	0	484
$T+1$	1	90	605
	2	0	968
$T+2$	1	240	484
	2	0	1815
$2T$	1	240	2178
	2	0	484
$2T+1$	1	240	484
Fortsetzung auf der nächsten Seite			

Fortsetzung $q = 3$, $\mathfrak{p}$ vom Grad 4 und 5			
a	ε_ϕ	$\mathfrak{p} = T^4 + 2T^3 + 2$	$\mathfrak{p} = T^5 + T^4 + T^2 + 2T + 2$
	2	0	1815
$2T + 2$	1	90	605
	2	0	968
T^2	1	160	2178
	2	80	484
$T^2 + 1$	1	80	1210
	2	250	726
$T^2 + 2$	1	120	605
	2	240	2420
$T^2 + T$	1	0	1331
	2	240	968
$T^2 + T + 1$	1	40	968
	2	80	1331
$T^2 + T + 2$	1	50	968
	2	160	968
$T^2 + 2T$	1	240	968
	2	90	605
$T^2 + 2T + 1$	1	40	484
	2	320	1815
$T^2 + 2T + 2$	1	80	1089
	2	160	484
$2T^2$	1	160	2178
	2	80	484
$2T^2 + 1$	1	120	605
	2	240	2420
$2T^2 + 2$	1	80	1210
	2	250	726
$2T^2 + T$	1	240	968
	2	90	605
$2T^2 + T + 1$	1	80	1089
	2	160	484
$2T^2 + T + 2$	1	40	484
	2	320	1815
$2T^2 + 2T$	1	0	1331
	2	240	968
$2T^2 + 2T + 1$	1	50	968
	2	160	968
$2T^2 + 2T + 2$	1	40	968

Fortsetzung auf der nächsten Seite

Fortsetzung $q = 3$, $\mathfrak{p}$ vom Grad 4 und 5			
a	ε_ϕ	$\mathfrak{p} = T^4 + 2T^3 + 2$	$\mathfrak{p} = T^5 + T^4 + T^2 + 2T + 2$
	2	80	1331

Tabelle A.2:

$q = 5$, $\mathfrak{p}$ vom Grad 4 und 5			
a	ε_ϕ	$T^4 + 4T2 + 3T + 1$	$T^5 + T^4 + 2$
0	1	0	8591
	2	1248	55451
	3	1248	55451
	4	0	8591
1	1	0	8591
	2	1560	12496
	3	936	8591
	4	0	55451
2	1	0	55451
	2	936	8591
	3	1560	12496
	4	0	8591
...			
T	1	0	15620
	2	624	23430
	3	1248	15620
	4	0	19525
$T+1$	1	0	15620
	2	936	23430
	3	2496	15620
	4	0	19525
$T+2$	1	0	15620
	2	1872	23430
	3	1560	15620
	4	0	19525
...			
T^2	1	1872	7810
	2	1560	31240
	3	0	11715
	4	0	39050
T^2+1	1	624	17963
	2	936	21087
	3	0	32802
	4	312	10153
Fortsetzung auf der nächsten Seite			

Fortsetzung $q = 5$, $\mathfrak{p}$ vom Grad 4 und 5			
a	ε_ϕ	$T^4 + 4T^2 + 3T + 1$	$T^5 + T^4 + 2$
$T^2 + 2$	1	624	24211
	2	1872	10934
	3	0	18744
	4	156	16401
…			
$T^2 + 2T + 1$	1	624	7810
	2	2184	31240
	3	0	11715
	4	624	39050
$T^2 + 2T + 2$	1	2808	17963
	2	624	21087
	3	0	32802
	4	780	10153
$T^2 + 2T + 3$	1	1560	24211
	2	2184	10934
	3	0	18744
	4	468	16401
…			
$4T^2 + 4T + 2$	1	1248	21087
	2	2184	21868
	3	0	21868
	4	780	9372
$4T^2 + 4T + 3$	1	624	26554
	2	1872	12496
	3	0	12496
	4	936	22649
$4T^2 + 4T + 4$	1	1248	24211
	2	650	10934
	3	0	18744
	4	624	16401

A.2 Verteilungen für alle Stellen eines festen Grades

Die folgenden Tabellen zeigen die Häufigkeiten der Frobeniusspuren, d. h. des Koeffizienten a von $P_\phi(X) = X^2 + a\,X + \varepsilon_\phi\,\mathfrak{p}$, ohne nach ε_ϕ zu unterscheiden. Es werden alle Drinfeld-Moduln über $\mathbb{F}_\mathfrak{p}$ gezählt, und dies wird für alle Stellen $\mathfrak{p}$ eines festen Grades aufsummiert.

Die zweite Spalte gibt die Anzahl aller Drinfeld-Moduln an, während die vierte Spalte die Anzahl der Isomorphieklassen von Drinfeld-Moduln mit dieser Frobeniusspur enthält. Zusätzlich gibt die dritte Spalte die Häufigkeit der Klassen wieder, die aus Drinfeld-Moduln mit $g = 0$ (d. h. mit $\mathrm{j}(\phi) = 0$) bestehen.
Die möglichen Werte von a werden so gruppiert, dass die Elemente, die sich nur im Absolutglied (für $q = 2$) bis zum linearen Term) unterscheiden, zusammengehören.
In den Spalten fünf und sechs sind die Werte der Spalten zwei und vier für diese Gruppen aufsummiert. Über diese Summen wird getrennt für die a mit maximalem Grad und jene mit kleinerem Grad der Durchschnitt gebildet und am Ende der Tabellen zusammen mit der Standardabweichung aufgeführt.

Tabelle A.3:

$q = 2$, alle $\mathfrak{p}$ vom Grad 8					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
0	79050	0	310		
1	19550	2	78		
T	35360	2	140		
$T+1$	35360	2	140	169320	668
T^2	37060	1	146		
T^2+1	37060	1	146		
T^2+T	74800	1	294		
T^2+T+1	19040	5	78	167960	664
T^3	34340	2	136		
T^3+1	38420	2	152		
T^3+T	67660	1	266		
T^3+T+1	17340	3	70	157760	624
T^3+T^2	67660	1	266		
T^3+T^2+1	17340	3	70		
T^3+T^2+T	38420	2	152		
T^3+T^2+T+1	34340	2	136	157760	624
T^4	66980	2	264		
T^4+1	66980	2	264		
Fortsetzung auf der nächsten Seite					

Fortsetzung $q = 2$, alle $\mathfrak{p}$ vom Grad 8					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
$T^4 + T$	157760	2	620		
$T^4 + T + 1$	36720	6	148	328440	1296
$T^4 + T^2$	138040	1	542		
$T^4 + T^2 + 1$	36720	9	150		
$T^4 + T^2 + T$	73440	3	290		
$T^4 + T^2 + T + 1$	73440	3	290	321640	1272
$T^4 + T^3$	141440	2	556		
$T^4 + T^3 + 1$	36720	6	148		
$T^4 + T^3 + T$	73440	3	290		
$T^4 + T^3 + T + 1$	76160	5	302	327760	1296
$T^4 + T^3 + T^2$	76160	5	302		
$T^4 + T^3 + T^2 + 1$	73440	3	290		
$T^4 + T^3 + T^2 + T$	141440	2	556		
$T^4 + T^3 + T^2 + T + 1$	36720	6	148	327760	1296
Durchschnitt der a mit Grad kleiner als 4				163200.0	645.0
Standardabweichung				5461.2	21.0
Durchschnitt der a mit Grad gleich 4				326400.0	1290.0
Standardabweichung				2762.2	10.4

Tabelle A.4:

$q = 2$, alle $\mathfrak{p}$ vom Grad 9					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
0	891184	56	1744		
1	196224	0	384		
T	406756	0	796		
$T + 1$	406756	0	796	1900920	3720
T^2	393470	0	770		
$T^2 + 1$	393470	0	770		
$T^2 + T$	776720	0	1520		
$T^2 + T + 1$	214620	0	420	1778280	3480
T^3	397558	0	778		
$T^3 + 1$	425152	0	832		
$T^3 + T$	797160	0	1560		
$T^3 + T + 1$	203378	0	398	1823248	3568
$T^3 + T^2$	797160	0	1560		
$T^3 + T^2 + 1$	203378	0	398		
$T^3 + T^2 + T$	425152	0	832		
$T^3 + T^2 + T + 1$	397558	0	778	1823248	3568
Fortsetzung auf der nächsten Seite					

Fortsetzung $q = 2$, alle $\mathfrak{p}$ vom Grad 9					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
T^4	398580	0	780		
T^4+1	398580	0	780		
T^4+T	874832	0	1712		
T^4+T+1	188048	0	368	1860040	3640
T^4+T^2	793072	0	1552		
T^4+T^2+1	220752	0	432		
T^4+T^2+T	402668	0	788		
T^4+T^2+T+1	402668	0	788	1819160	3560
T^4+T^3	782852	0	1532		
T^4+T^3+1	202356	0	396		
T^4+T^3+T	402668	0	788		
T^4+T^3+T+1	435372	0	852	1823248	3568
$T^4+T^3+T^2$	435372	0	852		
$T^4+T^3+T^2+1$	402668	0	788		
$T^4+T^3+T^2+T$	782852	0	1532		
$T^4+T^3+T^2+T+1$	202356	0	396	1823248	3568
Durchschnitt der a mit Grad kleiner als 4				1831424.0	3584.0
Standardabweichung				44123.9	86.3
Durchschnitt der a mit Grad gleich 4				1831424.0	3584.0
Standardabweichung				16605.5	32.5

Tabelle A.5:

$q = 3$, alle $\mathfrak{p}$ vom Grad 6					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
0	853216	0	2344		
1	454909	11	1258		
2	454909	11	1258	1763034	4860
T	564200	8	1556		
$T+1$	564200	8	1556		
$T+2$	564200	8	1556	1692600	4668
$2T$	564200	8	1556		
$2T+1$	564200	8	1556		
$2T+2$	564200	8	1556	1692600	4668
T^2	564200	8	1556		
T^2+1	459186	14	1272		
T^2+2	683683	5	1882	1707069	4710
T^2+T	683683	5	1882		
T^2+T+1	564200	8	1556		
Fortsetzung auf der nächsten Seite					

Fortsetzung $q = 3$, alle $\mathfrak{p}$ vom Grad 6					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
T^2+T+2	459186	14	1272	1707069	4710
T^2+2T	683683	5	1882		
T^2+2T+1	564200	8	1556		
T^2+2T+2	459186	14	1272	1707069	4710
$2T^2$	564200	8	1556		
$2T^2+1$	683683	5	1882		
$2T^2+2$	459186	14	1272	1707069	4710
$2T^2+T$	683683	5	1882		
$2T^2+T+1$	459186	14	1272		
$2T^2+T+2$	564200	8	1556	1707069	4710
$2T^2+2T$	683683	5	1882		
$2T^2+2T+1$	459186	14	1272		
$2T^2+2T+2$	564200	8	1556	1707069	4710
T^3	841841	11	2321		
T^3+1	841841	11	2321		
T^3+2	841841	11	2321	2525523	6963
T^3+T	866138	14	2390		
T^3+T+1	866138	14	2390		
T^3+T+2	866138	14	2390	2598414	7170
T^3+2T	1185639	5	3261		
T^3+2T+1	701883	17	1941		
T^3+2T+2	701883	17	1941	2589405	7143
T^3+T^2	1006096	8	2770		
T^3+T^2+1	848666	14	2342		
T^3+T^2+2	707343	17	1956	2562105	7068
T^3+T^2+T	1006096	8	2770		
T^3+T^2+T+1	848666	14	2342		
T^3+T^2+T+2	707343	17	1956	2562105	7068
T^3+T^2+2T	848666	14	2342		
T^3+T^2+2T+1	707343	17	1956		
T^3+T^2+2T+2	1006096	8	2770	2562105	7068
T^3+2T^2	1006096	8	2770		
T^3+2T^2+1	707343	17	1956		
T^3+2T^2+2	848666	14	2342	2562105	7068
T^3+2T^2+T	1006096	8	2770		
T^3+2T^2+T+1	707343	17	1956		
T^3+2T^2+T+2	848666	14	2342	2562105	7068
T^3+2T^2+2T	848666	14	2342		
T^3+2T^2+2T+1	1006096	8	2770		
Fortsetzung auf der nächsten Seite					

Fortsetzung $q = 3$, alle $\mathfrak{p}$ vom Grad 6					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
$T^3 + 2T^2 + 2T + 2$	707343	17	1956	2562105	7068
$2T^3$	841841	11	2321		
$2T^3 + 1$	841841	11	2321		
$2T^3 + 2$	841841	11	2321	2525523	6963
$2T^3 + T$	1185639	5	3261		
$2T^3 + T + 1$	701883	17	1941		
$2T^3 + T + 2$	701883	17	1941	2589405	7143
$2T^3 + 2T$	866138	14	2390		
$2T^3 + 2T + 1$	866138	14	2390		
$2T^3 + 2T + 2$	866138	14	2390	2598414	7170
$2T^3 + T^2$	1006096	8	2770		
$2T^3 + T^2 + 1$	848666	14	2342		
$2T^3 + T^2 + 2$	707343	17	1956	2562105	7068
$2T^3 + T^2 + T$	848666	14	2342		
$2T^3 + T^2 + T + 1$	707343	17	1956		
$2T^3 + T^2 + T + 2$	1006096	8	2770	2562105	7068
$2T^3 + T^2 + 2T$	1006096	8	2770		
$2T^3 + T^2 + 2T + 1$	848666	14	2342		
$2T^3 + T^2 + 2T + 2$	707343	17	1956	2562105	7068
$2T^3 + 2T^2$	1006096	8	2770		
$2T^3 + 2T^2 + 1$	707343	17	1956		
$2T^3 + 2T^2 + 2$	848666	14	2342	2562105	7068
$2T^3 + 2T^2 + T$	848666	14	2342		
$2T^3 + 2T^2 + T + 1$	1006096	8	2770		
$2T^3 + 2T^2 + T + 2$	707343	17	1956	2562105	7068
$2T^3 + 2T^2 + 2T$	1006096	8	2770		
$2T^3 + 2T^2 + 2T + 1$	707343	17	1956		
$2T^3 + 2T^2 + 2T + 2$	848666	14	2342	2562105	7068
Durchschnitt der a mit Grad kleiner als 3				1710072.0	4717.3
Standardabweichung				19634.5	53.3
Durchschnitt der a mit Grad gleich 3				2565108.0	7076.0
Standardabweichung				19208.5	54.2

A.2.1 Zusammenfassung nach dem maximalen Koeffizienten

Die Tabelle A.6 ist analog aufgebaut zu den vorherigen beiden, lediglich die Zusammenfassung in Gruppen erfolgt hier für solche a, die sich nur im maximalen Term $a_{\lfloor \frac{d}{2} \rfloor} T^{\lfloor \frac{d}{2} \rfloor}$ unterscheiden. Der Durchschnitt über die Werte aus den Spalten fünf und sechs, wird getrennt für die a mit Absolutglied Null und die mit Absolutglied ungleich Null berechnet und am Ende zusammen mit der Standardabweichung angegeben.

Tabelle A.6:

$q = 3$, alle $\mathfrak{p}$ vom Grad 7					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
0	27281280	624	24960		
T^3	18113196	0	16572		
$2T^3$	18113196	0	16572	63507672	58104
T^2	18113196	0	16572		
T^3+T^2	21743049	0	19893		
$2T^3+T^2$	21743049	0	19893	61599294	56358
$2T^2$	18113196	0	16572		
T^3+2T^2	21743049	0	19893		
$2T^3+2T^2$	21743049	0	19893	61599294	56358
T	18106638	0	16566		
T^3+T	18355842	0	16794		
$2T^3+T$	26028702	0	23814	62491182	57174
T^2+T	21746328	0	19896		
T^3+T^2+T	21743049	0	19893		
$2T^3+T^2+T$	18405027	0	16839	61894404	56628
$2T^2+T$	21746328	0	19896		
T^3+2T^2+T	21743049	0	19893		
$2T^3+2T^2+T$	18405027	0	16839	61894404	56628
$2T$	18106638	0	16566		
T^3+2T	26028702	0	23814		
$2T^3+2T$	18355842	0	16794	62491182	57174
T^2+2T	21746328	0	19896		
T^3+T^2+2T	18405027	0	16839		
$2T^3+T^2+2T$	21743049	0	19893	61894404	56628
$2T^2+2T$	21746328	0	19896		
T^3+2T^2+2T	18405027	0	16839		
$2T^3+2T^2+2T$	21743049	0	19893	61894404	56628
1	15122748	0	13836		
Fortsetzung auf der nächsten Seite					

Fortsetzung $q = 3$, alle $\mathfrak{p}$ vom Grad 7					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
T^3+1	18113196	0	16572		
$2T^3+1$	18113196	0	16572	51349140	46980
T^2+1	15312930	0	14010		
T^3+T^2+1	18405027	0	16839		
$2T^3+T^2+1$	18405027	0	16839	52122984	47688
$2T^2+1$	21746328	0	19896		
T^3+2T^2+1	15132585	0	13845		
$2T^3+2T^2+1$	15132585	0	13845	52011498	47586
$T+1$	18106638	0	16566		
T^3+T+1	18355842	0	16794		
$2T^3+T+1$	15040773	0	13761	51503253	47121
T^2+T+1	18113196	0	16572		
T^3+T^2+T+1	18405027	0	16839		
$2T^3+T^2+T+1$	15132585	0	13845	51650808	47256
$2T^2+T+1$	15312930	0	14010		
T^3+2T^2+T+1	15132585	0	13845		
$2T^3+2T^2+T+1$	21743049	0	19893	52188564	47748
$2T+1$	18106638	0	16566		
T^3+2T+1	15040773	0	13761		
$2T^3+2T+1$	18355842	0	16794	51503253	47121
T^2+2T+1	18113196	0	16572		
T^3+T^2+2T+1	15132585	0	13845		
$2T^3+T^2+2T+1$	18405027	0	16839	51650808	47256
$2T^2+2T+1$	15312930	0	14010		
T^3+2T^2+2T+1	21743049	0	19893		
$2T^3+2T^2+2T+1$	15132585	0	13845	52188564	47748
2	15122748	0	13836		
T^3+2	18113196	0	16572		
$2T^3+2$	18113196	0	16572	51349140	46980
T^2+2	21746328	0	19896		
T^3+T^2+2	15132585	0	13845		
$2T^3+T^2+2$	15132585	0	13845	52011498	47586
$2T^2+2$	15312930	0	14010		
T^3+2T^2+2	18405027	0	16839		
$2T^3+2T^2+2$	18405027	0	16839	52122984	47688
$T+2$	18106638	0	16566		
T^3+T+2	18355842	0	16794		
$2T^3+T+2$	15040773	0	13761	51503253	47121
T^2+T+2	15312930	0	14010		
Fortsetzung auf der nächsten Seite					

Fortsetzung $q = 3$, alle $\mathfrak{p}$ vom Grad 7					
a	Anzahl	$\mathrm{Kl}_{g=0}$	Klassen	$\sum$ Anzahl	$\sum$ Klassen
$T^3 + T^2 + T + 2$	15132585	0	13845		
$2T^3 + T^2 + T + 2$	21743049	0	19893	52188564	47748
$2T^2 + T + 2$	18113196	0	16572		
$T^3 + 2T^2 + T + 2$	18405027	0	16839		
$2T^3 + 2T^2 + T + 2$	15132585	0	13845	51650808	47256
$2T + 2$	18106638	0	16566		
$T^3 + 2T + 2$	15040773	0	13761		
$2T^3 + 2T + 2$	18355842	0	16794	51503253	47121
$T^2 + 2T + 2$	15312930	0	14010		
$T^3 + T^2 + 2T + 2$	21743049	0	19893		
$2T^3 + T^2 + 2T + 2$	15132585	0	13845	52188564	47748
$2T^2 + 2T + 2$	18113196	0	16572		
$T^3 + 2T^2 + 2T + 2$	15132585	0	13845		
$2T^3 + 2T^2 + 2T + 2$	18405027	0	16839	51650808	47256
Durchschnitt der a mit Absolutglied Null				62140693.3	56853.3
Standardabweichung				571856.2	523.2
Durchschnitt der a mit Grad gleich 3				51796541.3	47389.3
Standardabweichung				311771.9	285.2

Tabelle A.7: Vergleich von $\mathsf{H}(a, q, d)$ und $\widetilde{\mathsf{C}}(a) \cdot {}_{gl}\mathsf{H}(a, q, d)$

a	$\mathsf{H}(a, q, d)$	$\widetilde{\mathsf{C}}(a) \cdot {}_{gl}\mathsf{H}(a, q, d)$
$q = 3, d = 7$		
0	27281280	24914228
1	15122748	15165182
2	15122748	15165182
T	18106638	18414864
$T + 1$	18106638	18414864
$T + 2$	18106638	18414864
$2T$	18106638	18414864
$2T + 1$	18106638	18414864
$2T + 2$	18106638	18414864
T^2	18113196	18414864
$T^2 + 1$	15312930	15165182
$T^2 + 2$	21746328	21664546
$T^2 + T$	21746328	21664546
$T^2 + T + 1$	18113196	18414864
$T^2 + T + 2$	15312930	15165182
$T^2 + 2T$	21746328	21664546
Fortsetzung auf der nächsten Seite		

Fortsetzung		
a	$\mathsf{H}(a,q,d)$	$\breve{\mathsf{C}}(a) \cdot {}_{gl}\mathsf{H}(a,q,d)$
T^2+2T+1	18113196	18414864
T^2+2T+2	15312930	15165182
T^3	18113196	18414864
T^3+1	18113196	18414864
T^3+2	18113196	18414864
T^3+T	18355842	18414864
T^3+T+1	18355842	18414864
T^3+T+2	18355842	18414864
T^3+2T	26028702	24914228
T^3+2T+1	15040773	15165182
T^3+2T+2	15040773	15165182
T^3+T^2	21743049	21664546
T^3+T^2+1	18405027	18414864
T^3+T^2+2	15132585	15165182
T^3+T^2+T	21743049	21664546
T^3+T^2+T+1	18405027	18414864
T^3+T^2+T+2	15132585	15165182
T^3+T^2+2T	18405027	18414864
T^3+T^2+2T+1	15132585	15165182
T^3+T^2+2T+2	21743049	21664546
$q=7, d=5$		
0	3218685120	3205473701
1	2699883900	2693850863
2	2699883900	2693850863
3	2699883900	2693850863
4	2699883900	2693850863
5	2699883900	2693850863
6	2699883900	2693850863
T	2765763420	2766939840
$T+1$	2765763420	2766939840
$T+2$	2765763420	2766939840
$T+3$	2765763420	2766939840
$T+4$	2765763420	2766939840
$T+5$	2765763420	2766939840
$T+6$	2765763420	2766939840
T^2	2765763420	2766939840
T^2+1	2701060320	2693850863
T^2+2	2701060320	2693850863
T^2+3	2833211500	2840028817
T^2+4	2701060320	2693850863
T^2+5	2833211500	2840028817
Fortsetzung auf der nächsten Seite		

Fortsetzung		
a	$\mathsf{H}(a,q,d)$	$\breve{\mathsf{C}}(a) \cdot {}_{gl}\mathsf{H}(a,q,d)$
T^2+6	2833211500	2840028817
T^2+T	2833211500	2840028817
T^2+T+1	2833211500	2840028817
T^2+T+2	2765763420	2766939840
T^2+T+3	2701060320	2693850863
T^2+T+4	2701060320	2693850863
T^2+T+5	2833211500	2840028817
T^2+T+6	2701060320	2693850863
T^2+2T	2833211500	2840028817

Anhang B

Tabellen Fall (b)

Tabelle B.1:

$q = 3$, $\mathfrak{p} = T + 2$		
a	Anzahl über $\mathbb{F}_{\mathfrak{p}^6}$	Anzahl über $\mathbb{F}_{\mathfrak{p}^7}$
0	182	2186
1	11648	61208
2	11648	61208
T	4368	114765
$T+1$	4368	114765
$T+2$	0	0
T^2	4368	91812
T^2+1	10920	68859
T^2+2	0	0
T^2+T	6552	91812
T^2+T+1	0	0
T^2+T+2	8736	91812
T^2+2T	0	0
T^2+2T+1	4368	91812
T^2+2T+2	10920	68859
T^3	8736	91812
T^3+1	8736	91812
T^3+2	273	0
T^3+T	10920	68859
T^3+T+1	0	0
T^3+T+2	10920	68859
T^3+2T	0	0
T^3+2T+1	4368	91812
Fortsetzung auf der nächsten Seite		

Fortsetzung $q = 3$, $\mathfrak{p} = T + 2$		
a	Anzahl über $\mathbb{F}_{\mathfrak{p}^6}$	Anzahl über $\mathbb{F}_{\mathfrak{p}^7}$
$T^3 + 2T + 2$	4368	91812
$T^3 + T^2$	17472	114765
$T^3 + T^2 + 1$	0	0
$T^3 + T^2 + 2$	10920	68859
$T^3 + T^2 + T$	0	0
$T^3 + T^2 + T + 1$	15288	91812
$T^3 + T^2 + T + 2$	6552	91812
$T^3 + T^2 + 2T$	14196	114765
$T^3 + T^2 + 2T + 1$	10920	62301
$T^3 + T^2 + 2T + 2$	0	0
$T^3 + 2T^2$	0	0
$T^3 + 2T^2 + 1$	10920	62301
$T^3 + 2T^2 + 2$	14196	114765
$T^3 + 2T^2 + T$	17472	114765
$T^3 + 2T^2 + T + 1$	10920	68859
$T^3 + 2T^2 + T + 2$	0	0
$T^3 + 2T^2 + 2T$	15288	91812
$T^3 + 2T^2 + 2T + 1$	0	0
$T^3 + 2T^2 + 2T + 2$	6552	91812

Anhang C

Tabellen Fall (c)

C.1 Verteilungen für alle Stellen eines festen Grades

Die folgenden Tabellen zeigen das Auftreten der Frobeniusspuren beim Reduzieren eines Drinfeld-Moduls $\phi : \mathbb{F}_q[T] \to \mathbb{F}_q(T)\{\tau\}$ für alle Stellen $\mathfrak{p} \in S_\phi(\mathbb{F}_q(T))$ eines festen Grades d. Es wird sowohl ein Fall mit d gerade als auch ein Fall mit d ungerade betrachtet. Es erfolgt eine Zusammenfassung der a in Gleichheit bis auf Terme eines gewissen Grades.

Tabelle C.1: Verteilung für $\phi^{(29)}$

$q = 2$, alle $\mathfrak{p}$ vom Grad 24 und vom Grad 25 für $\phi^{(29)}$		
a	Anzahl Grad 24	Anzahl Grad 25
$O(7)$	14506	41909
$T^8 + O(7)$	14331	42023
$T^9 + O(7)$	14433	42068
$T^9 + T^8 + O(7)$	14654	42619
$T^{10} + O(7)$	14581	42034
$T^{10} + T^8 + O(7)$	14466	41962
$T^{10} + T^9 + O(7)$	14690	41826
$T^{10} + T^9 + T^8 + O(7)$	14609	41736
...		
Ausschnitt ohne Zusammenfassung		
T^8	42	136
$T^8 + 1$	47	131
$T^8 + T$	83	318
$T^8 + T + 1$	24	94
$T^8 + T^2$	108	318
$T^8 + T^2 + 1$	19	80
Fortsetzung auf der nächsten Seite		

Fortsetzung $q = 2$, alle $\mathfrak{p}$ vom Grad 22 und vom Grad 23 für $\phi^{(29)}$		
a	Anzahl Grad 24	Anzahl Grad 25
$T^8 + T^2 + T$	55	149
$T^8 + T^2 + T + 1$	56	149
$T^8 + T^3$	90	297
$T^8 + T^3 + 1$	26	79
$T^8 + T^3 + T$	51	166
$T^8 + T^3 + T + 1$	42	133
$T^8 + T^3 + T^2$	52	140
$T^8 + T^3 + T^2 + 1$	49	152
$T^8 + T^3 + T^2 + T$	83	271
$T^8 + T^3 + T^2 + T + 1$	28	62
$T^8 + T^4$	105	263
$T^8 + T^4 + 1$	32	78
$T^8 + T^4 + T$	48	149
$T^8 + T^4 + T + 1$	35	149
$T^8 + T^4 + T^2$	54	156
$T^8 + T^4 + T^2 + 1$	50	140
$T^8 + T^4 + T^2 + T$	114	299
$T^8 + T^4 + T^2 + T + 1$	36	76
$T^8 + T^4 + T^3$	61	168
$T^8 + T^4 + T^3 + 1$	51	134
$T^8 + T^4 + T^3 + T$	87	271
$T^8 + T^4 + T^3 + T + 1$	29	74
$T^8 + T^4 + T^3 + T^2$	93	303
$T^8 + T^4 + T^3 + T^2 + 1$	21	64
$T^8 + T^4 + T^3 + T^2 + T$	54	121
$T^8 + T^4 + T^3 + T^2 + T + 1$	46	184
Ende des Ausschnitts ohne Zusammenfassung		
...		
$T^{11} + O(7)$	14641	41887
$T^{11} + T^8 + O(7)$	14640	42019
$T^{11} + T^9 + O(7)$	14484	41849
$T^{11} + T^9 + T^8 + O(7)$	14401	41692
$T^{11} + T^{10} + O(7)$	14584	41831
$T^{11} + T^{10} + T^8 + O(7)$	14547	41566
$T^{11} + T^{10} + T^9 + O(7)$	14752	42260
$T^{11} + T^{10} + T^9 + T^8 + O(7)$	14519	41705
$T^{12} + O(7)$	29217	41563
$T^{12} + T^8 + O(7)$	28908	41716
$T^{12} + T^9 + O(7)$	29031	42264
$T^{12} + T^9 + T^8 + O(7)$	28962	42068
...		
Fortsetzung auf der nächsten Seite		

Fortsetzung $q=2$, alle $\mathfrak{p}$ vom Grad 22 und vom Grad 23 für $\phi^{(29)}$		
a	Anzahl Grad 24	Anzahl Grad 25
Ausschnitt Zusammenfassung bis zum linearen Term		
$T^{12}+T^9+T^8+O(1)$	424	675
$T^{12}+T^9+T^8+T^2+O(1)$	456	668
$T^{12}+T^9+T^8+T^3+O(1)$	433	659
$T^{12}+T^9+T^8+T^3+T^2+O(1)$	473	697
$T^{12}+T^9+T^8+T^4+O(1)$	465	664
$T^{12}+T^9+T^8+T^4+T^2+O(1)$	417	716
$T^{12}+T^9+T^8+T^4+T^3+O(1)$	440	620
$T^{12}+T^9+T^8+T^4+T^3+T^2+O(1)$	417	662
$T^{12}+T^9+T^8+T^5+O(1)$	460	729
$T^{12}+T^9+T^8+T^5+T^2+O(1)$	444	696
$T^{12}+T^9+T^8+T^5+T^3+O(1)$	502	707
$T^{12}+T^9+T^8+T^5+T^3+T^2+O(1)$	477	643
$T^{12}+T^9+T^8+T^5+T^4+O(1)$	458	641
$T^{12}+T^9+T^8+T^5+T^4+T^2+O(1)$	448	649
$T^{12}+T^9+T^8+T^5+T^4+T^3+O(1)$	467	671
$T^{12}+T^9+T^8+T^5+T^4+T^3+T^2+O(1)$	451	629
Ende des Ausschnitts Zusammenfassung bis zum linearen Term		
…		
$T^{12}+T^{10}+O(7)$	28988	42147
$T^{12}+T^{10}+T^8+O(7)$	29090	41732
$T^{12}+T^{10}+T^9+O(7)$	29233	41896
$T^{12}+T^{10}+T^9+T^8+O(7)$	29350	42117
$T^{12}+T^{11}+O(7)$	29285	41790
$T^{12}+T^{11}+T^8+O(7)$	29384	42187
$T^{12}+T^{11}+T^9+O(7)$	29133	41955
$T^{12}+T^{11}+T^9+T^8+O(7)$	29105	42084
$T^{12}+T^{11}+T^{10}+O(7)$	28996	41875
$T^{12}+T^{11}+T^{10}+T^8+O(7)$	29347	41934
$T^{12}+T^{11}+T^{10}+T^9+O(7)$	29254	42245
$T^{12}+T^{11}+T^{10}+T^9+T^8+O(7)$	28749	41617
Durchschnitt für Grad kleiner als 12	14552.4	41936.6
Standardabweichung	109.3	242.0
Durchschnitt für Grad gleich 12	29127.0	41949.4
Standardabweichung	175.0	214.7

Tabelle C.2: Verteilung für $\phi^{(33)}$

$q = 3$, alle $\mathfrak{p}$ vom Grad 14 und vom Grad 15 für $\phi^{(33)}$		
a	Anzahl Grad 14	Anzahl Grad 15
$O(4)$	9477	35598
$T^5 + O(4)$	9457	35358
$2T^5 + O(4)$	9536	35189
$T^6 + O(4)$	9565	35929
$T^6 + T^5 + O(4)$	9540	35252
…		
Ausschnitt ohne Zusammenfassung		
$T^6 + T^5$	39	180
$T^6 + T^5 + 1$	42	134
$T^6 + T^5 + 2$	36	126
$T^6 + T^5 + T$	56	174
$T^6 + T^5 + T + 1$	37	132
$T^6 + T^5 + T + 2$	40	123
$T^6 + T^5 + 2T$	26	118
$T^6 + T^5 + 2T + 1$	33	115
$T^6 + T^5 + 2T + 2$	44	164
$T^6 + T^5 + T^2$	47	173
$T^6 + T^5 + T^2 + 1$	28	119
$T^6 + T^5 + T^2 + 2$	34	157
$T^6 + T^5 + T^2 + T$	38	184
$T^6 + T^5 + T^2 + T + 1$	26	127
$T^6 + T^5 + T^2 + T + 2$	48	146
$T^6 + T^5 + T^2 + 2T$	27	148
$T^6 + T^5 + T^2 + 2T + 1$	47	160
$T^6 + T^5 + T^2 + 2T + 2$	30	132
$T^6 + T^5 + 2T^2$	32	131
$T^6 + T^5 + 2T^2 + 1$	45	161
$T^6 + T^5 + 2T^2 + 2$	46	156
$T^6 + T^5 + 2T^2 + T$	35	166
$T^6 + T^5 + 2T^2 + T + 1$	45	122
$T^6 + T^5 + 2T^2 + T + 2$	39	146
$T^6 + T^5 + 2T^2 + 2T$	66	185
$T^6 + T^5 + 2T^2 + 2T + 1$	37	121
$T^6 + T^5 + 2T^2 + 2T + 2$	31	125
$T^6 + T^5 + T^3$	54	168
$T^6 + T^5 + T^3 + 1$	37	145
$T^6 + T^5 + T^3 + 2$	33	122
Ende des Ausschnitts ohne Zusammenfassung		
…		
Fortsetzung auf der nächsten Seite		

Fortsetzung $q = 3$, alle $\mathfrak{p}$ vom Grad 14 und vom Grad 15 für $\phi^{(33)}$		
a	Anzahl Grad 14	Anzahl Grad 15
$T^6 + 2T^5 + O(4)$	9279	35294
$2T^6 + O(4)$	9541	35585
$2T^6 + T^5 + O(4)$	9525	35502
$2T^6 + 2T^5 + O(4)$	9412	35333
$T^7 + O(4)$	14139	35482
$T^7 + T^5 + O(4)$	14055	35178
$T^7 + 2T^5 + O(4)$	14309	35573
$T^7 + T^6 + O(4)$	14319	35102
$T^7 + T^6 + T^5 + O(4)$	14324	35599
$T^7 + T^6 + 2T^5 + O(4)$	14289	35697
$T^7 + 2T^6 + O(4)$	14060	35406
$T^7 + 2T^6 + T^5 + O(4)$	14213	35206
$T^7 + 2T^6 + 2T^5 + O(4)$	14342	35531
$2T^7 + O(4)$	14198	35354
$2T^7 + T^5 + O(4)$	14297	35397

...

Ausschnitt Zusammenfassung bis Absolutglied		
$T^6 + T^5 + O(0)$	117	440
$T^6 + T^5 + T + O(0)$	133	429
$T^6 + T^5 + 2T + O(0)$	103	397
$T^6 + T^5 + T^2 + O(0)$	109	449
$T^6 + T^5 + T^2 + T + O(0)$	112	457
$T^6 + T^5 + T^2 + 2T + O(0)$	104	440
$T^6 + T^5 + 2T^2 + O(0)$	123	448
$T^6 + T^5 + 2T^2 + T + O(0)$	119	434
$T^6 + T^5 + 2T^2 + 2T + O(0)$	134	431
Ende Ausschnitt Zusammenfassung bis Absolutglied		

...

$2T^7 + 2T^5 + O(4)$	14200	35097
$2T^7 + T^6 + O(4)$	14149	35660
$2T^7 + T^6 + T^5 + O(4)$	14026	35454
$2T^7 + T^6 + 2T^5 + O(4)$	14099	35491
$2T^7 + 2T^6 + O(4)$	14515	35370
$2T^7 + 2T^6 + T^5 + O(4)$	14265	35537
$2T^7 + 2T^6 + 2T^5 + O(4)$	14353	35402
Durchschnitt für Grad kleiner als 7	9481.3	35448.9
Standardabweichung	85.1	217.6
Durchschnitt für Grad gleich 7	14230.7	35418.7
Standardabweichung	123.9	173.8

Die beiden folgenden Tabellen zeigen die Verteilung für den Drinfeld-Modul $\phi^{(23)}$ für die Grade 20 bis 23.

Tabelle C.3: Verteilung für $\phi^{(32)}$

$q = 2$, **alle $\mathfrak{p}$ vom Grad 20 und vom Grad 21 für** $\phi^{(23)}$		
a	Anzahl Grad 20	Anzahl Grad 21
$O(6)$	9945	0
$T^7 + O(6)$	16320	0
$T^8 + O(6)$	13056	0
$T^8 + T^7 + O(6)$	13056	0
$T^9 + O(6)$	0	0
$T^9 + T^7 + O(6)$	0	0
$T^9 + T^8 + O(6)$	0	0
$T^9 + T^8 + T^7 + O(6)$	0	0
$T^{10} + O(6)$	0	12463
$T^{10} + T^7 + O(6)$	0	12453
$T^{10} + T^8 + O(6)$	0	12463
$T^{10} + T^8 + T^7 + O(6)$	0	12453
$T^{10} + T^9 + O(6)$	0	12598
$T^{10} + T^9 + T^7 + O(6)$	0	12464
$T^{10} + T^9 + T^8 + O(6)$	0	12554
$T^{10} + T^9 + T^8 + T^7 + O(6)$	0	12410

Tabelle C.4: Verteilung für $\phi^{(32)}$

$q = 2$, **alle $\mathfrak{p}$ vom Grad 22 und vom Grad 23 für** $\phi^{(23)}$		
a	Anzahl Grad 22	Anzahl Grad 23
$O(6)$	0	0
$T^7 + O(6)$	0	0
$T^8 + O(6)$	0	0
$T^8 + T^7 + O(6)$	0	0
$T^9 + O(6)$	0	0
$T^9 + T^7 + O(6)$	0	0
$T^9 + T^8 + O(6)$	0	0
$T^9 + T^8 + T^7 + O(6)$	0	0
$T^{10} + O(6)$	23808	0
$T^{10} + T^7 + O(6)$	23808	0
$T^{10} + T^8 + O(6)$	23808	0
$T^{10} + T^8 + T^7 + O(6)$	23808	0
$T^{10} + T^9 + O(6)$	23773	0
$T^{10} + T^9 + T^7 + O(6)$	23744	0
$T^{10} + T^9 + T^8 + O(6)$	24096	0
Fortsetzung auf der nächsten Seite		

Fortsetzung $q = 2$, alle $\mathfrak{p}$ vom Grad 22 und vom Grad 23 für $\phi^{(23)}$		
a	Anzahl Grad 22	Anzahl Grad 23
$T^{10} + T^9 + T^8 + T^7 + O(6)$	23712	0
$T^{11} + O(6)$	0	23018
$T^{11} + T^7 + O(6)$	0	22822
$T^{11} + T^8 + O(6)$	0	22778
$T^{11} + T^8 + T^7 + O(6)$	0	22678
$T^{11} + T^9 + O(6)$	0	22742
$T^{11} + T^9 + T^7 + O(6)$	0	22682
$T^{11} + T^9 + T^8 + O(6)$	0	22886
$T^{11} + T^9 + T^8 + T^7 + O(6)$	0	22755
$T^{11} + T^{10} + O(6)$	0	22742
$T^{11} + T^{10} + T^7 + O(6)$	0	22682
$T^{11} + T^{10} + T^8 + O(6)$	0	22886
$T^{11} + T^{10} + T^8 + T^7 + O(6)$	0	22755
$T^{11} + T^{10} + T^9 + O(6)$	0	22778
$T^{11} + T^{10} + T^9 + T^7 + O(6)$	0	22678
$T^{11} + T^{10} + T^9 + T^8 + O(6)$	0	23018
$T^{11} + T^{10} + T^9 + T^8 + T^7 + O(6)$	0	22822

Literaturverzeichnis

[Bir68] Birch, B. J.: How the number of points of an elliptic curve over a fixed prime field varies. In: *J. London Math. Soc.* (1968), Nr. 43, S. 50–67

[Dav95] David, Chantal: Supersingular Reduktion of Drinfel'd Modules. In: *Duke Mathematical Journal* (1995), Nr. 78, S. 399–412

[Dav96] David, Chantal: Average Distribution of Supersingular Drinfeld Modules. In: *J. Number Theory* (1996), Nr. 56, S. 366–380

[DH87] Deligne, P. ; Husemöller, D.: Survey of Drinfeld modules. In: *Contemp. Math.* (1987), Nr. 67, S. 25–91

[Dum92] Dummit, D. S.: Genus Two Hyperelliptic Drinfeld Modules over $\mathbb{F}_2$. In: D. Goss et al (Hrsg.): *The Arithmetic of Function Fields*, de Gruyter, 1992, S. 117–129

[Gek83] Gekeler, E.-U.: Zur Arithmetik von Drinfeld-Moduln. In: *Math. Ann.* (1983), Nr. 262, S. 167–182

[Gek91] Gekeler, E.-U.: On finite Drinfeld modules. In: *J. Algebra* 141 (1991), S. 187–203

[Gos96] Goss, David: *Basic Structures of Function Field Arithmetic*. Berlin : Springer, 1996

[GS96] Gekeler, E.-U. ; Snyder, Brian A.: Drinfeld modules over finite fields. In: E.-U. Gekeler et al (Hrsg.): *Drinfeld Modules, Modular Schemes and Applications*, World Scientific, 1996, S. 66–87

[Hay74] Hayes, David R.: Explicit class field theory for rational function fields. In: *Trans. Amer. Math. Soc.* (1974), Nr. 189, S. 77–91

[Hay91] Hayes, David R.: On the reduction of rank-one Drinfeld modules. In: *Math. Comp.* (1991), Nr. 57, S. 339–349

[Hay92] Hayes, David R.: A brief introduction to Drinfeld modules. In: D. Goss et al (Hrsg.): *The Arithmetic of Function Fields*, de Gruyter, 1992, S. 1–32

[HY00] Hsia, Liang-Chung ; Yu, Jing: On Charakteristic Polynomials of Geometric Frobenius Associated to Drinfeld Modules. In: *Compositio Mathematica* (2000), Nr. 122, S. 261–280

[Koc97] Koch, Helmut: *Zahlentheorie*. Braunschweig/Wiesbaden : Vieweg, 1997

[LN94] Lidl, Rudolf ; Niederreiter, Harald: *Indroduction to finite fields and their applications*. Cambridge University Press, 1994

[Neu86] Neukirch, Jürgen: *Class Field Theory*. Berlin : Springer, 1986

[Neu92] Neukirch, Jürgen: *Algebraische Zahlentheorie*. Berlin Heidelberg : Springer, 1992

[Pot96] Potemine, Igor: *Arithmétique des corps globaux de fonctions et géométrie des schémas modulaires de Drinfeld*, Grenoble, Dissertation, 1996

[Ser79] Serre, J-P.: *Local Fields*. New York : Springer, 1979

[Sti93] Stichtenoth, Henning: *Algebraic Function Fields and Codes*. Berlin Heidelberg : Springer, 1993

[Tat65] Tate, John T.: Algebraic Cycles and Poles of Zeta Functions. In: *Arithmetical Algebraic Geometry* (1965), S. 93–110

[Yos73] Yoshida, Hiroyuki: On an Analogue of the Sato Conjecture. In: *Inventiones math.* 19 (1973), S. 261–277

[Yu95] Yu, Jiu-Kang: Isogenies of Drinfeld Modules over Finite Fields. In: *J. Number Theory* (1995), Nr. 54, S. 161–171

Index

A, *15*
A-Charakteristik, *28*
A-Körper, *28*
Algebra
  zentral einfache, 35
  zentral-einfache, *35*
${}_a\phi(L')$, *31*

Bewertung
  äquivalente, *15*
  Betrags-, *14*
  diskrete, *14*, 21
  Fortsetzung einer, *16*
  normierte, *14*
  triviale, *15*
Bewertungsring, *14*

Carlitz-Modul, *30*, 43
$\mathrm{char}_A(L)$, *28*
Charakteristik
  endliche, *28*
  generische, *28*

$D(f)$, *27*
$deg_\tau(P)$, *26*
Drinfeldmodul, *29*

einfach, *35*
$\mathrm{End}_L(\mathbb{G}_a(L))$, 23
Endomorphismus, *33*
$\mathrm{End}_L(\phi)$, *34*
$\mathrm{End}(\phi)$, 35
ε_ϕ, *61*, 64

Fall (a), *75*
Fall (b), *75*
Fall (c), *75*
Frobenius, 36
Funktionenkörper
  algebraischer, *13*
  rationaler, *13*, 20–22

γ, *28*
Grad
  einer Stelle, *14*
  in τ, *26*
  in A, 16

Höhe, *31*
Hasse-Invariante, *52*, 70
$\mathrm{Hom}_L(\phi, \psi)$, *33*
$\mathrm{ht}(\phi)$, *31*

Isogenie, *34*
Isomorphieklassen, 45–49
Isomorphismus, *33*

j-Invariante, *44*, 72
$j(\phi)$, *44*

Koeffizient
  maximaler, *66*
Koeffizienten
  ganze, *40*
Kommutatorregel, 24, 26

$L\{\tau\}$, *26*
$L\{\tau_p\}$, *24*

Minimalpolynom, *56*
Moore-Determinante, *25*
Morphismus, *33*
$M_\phi(X)$, *56*

N, *56*

Norm, *17*
  über endlichen Körpern, *17*
  reduzierte, *36*, 56
$_\nu\phi$, *38*

ϕ, *29*
$\phi^{(c)}$, *71*
Polynom
  absolut additives, *22*, 23
  additives, *22*
  charakteristisches, *56*
Polynomring
  getwisteter, *24*
Potenzrestsymbol, *63*
$P_\phi(X)$, *56*, 61
Produktformel, *15*

Quotientendivisionsring, 27

Rang, *29*
rg(ϕ), *29*
$_{\mathrm{red}}\mathrm{N}$, *36*, 56
$_{\mathrm{red}}\mathrm{Tr}$, *36*
Reduktion
  gute, *40*
  potentiell gute, *41*
  potentiell stabile, *41*
  stabile, *40*
Rekursionsformel, 49
Repräsentantensystem, *45*, 78
Restklassengrad, *16*
Restklassenkörper, *14*
Reziprozitätsgesetz, *64*

Signum-Funktion, *63*
sgn, *63*
$S(K)$, *14*
$S_\phi(K)$, *40*
Spur, *17*
  über endlichen Körpern, *17*
  reduzierte, *36*
Standardsituation, 29
Stelle, *14*, 15, 20
supersingulär, 69
supesingulär, *53*

Tate-Modul, *38*
τ, 36
τ_p, *23*
Teilungspunkt, *31*
$T_\nu(\phi)$, *38, 39*
Torsionspunkt, *31*
Trägheitsindex, *16*

Uniformisierende, *14*

Vervollständigung, *19*, 22
Verzweigungsindex, *16*

Zentrum, *35*
Zentr(M), *35*