Torsionskörper eines Rang-2-Drinfeld-Moduls

Diplomarbeit

Enrico Varela Roldán

Saarbrücken, Juni 2009

Betreut von Prof. Dr. Ernst-Ulrich Gekeler

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

Inhaltsverzeichnis

KAPITEL 0

Einleitung

0.1. Vorwort

In der klassischen Situation elliptischer Kurven über den rationalen Zahlen betrachtet man Primstellen p, an denen die untersuchte elliptische Kurve gute Reduktion besitzt. Für solche Primstellen erzeugt die p-Torsion der elliptischen Kurve eine galoissche Körpererweiterung von $\mathbb{Q}$, deren Galois-Gruppe sich in die Gruppe $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$ einbetten lässt. Für einen Überblick über die klassische Theorie, siehe [**Ser73**].

Gegenstand der Untersuchung der Torsionskörper ist unter anderem die Frage, für welche Primstellen die Galois-Gruppe maximal, d.h. die ganze Gruppe $\mathrm{GL}(2, \mathbb{Z}/p\mathbb{Z})$, ist. Es gibt hierfür Aussagen in Form unterer Schranken, so dass diese Eigenschaft für Primstellen erfüllt ist, die jenseits dieser Schranken liegen. Allerdings sind die Schranken im Allgemeinen nicht scharf. In einigen konkreten Beispielen ist es möglich, eine genauere Bestimmung der Primstellen mit maximaler Galois-Gruppe vorzunehmen.

Die Drinfeld-Theorie kann als Analogie dieser klassischen Situation für Funktionenkörper aufgefasst werden. Den Daten $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ und $\mathbb{C}$ der Zahlkörper-Situation entsprechen hier der Polynomring $A = \mathbb{F}_q[T]$, der rationale Funktionenkörper $K = \mathbb{F}_q(T)$, seine Komplettierung an unendlich $K_\infty = \mathbb{F}_q((T^{-1}))$ und der vervollständigte algebraische Abschluss $\mathcal{C}$ von K_∞. Das Analogon zur elliptischen Kurve ist der Drinfeld-Modul vom Rang 2. Davon abgeleitet erhält man für weitere Objekte, wie die Weierstraß-Funktion oder elliptische Modulformen, Entsprechungen auf Seiten der Funktionenkörper.

Torsionskörper von Drinfeld-Moduln können unter ähnlichen Gesichtspunkten untersucht werden wie ihre Gegenstücke im Zahlkörper-Fall. Allerdings verfügt man bisher nicht über vergleichbare Resultate. Dies liegt jedoch nicht in erster Linie daran, dass es sich bei Drinfeld-Moduln um ein neueres Konzept handelt. Vielmehr ist es im Allgemeinen nicht möglich, die klassischen Methoden auf Funktionenkörper zu übertragen. So werden beispielsweise für elliptische Kurven Aussagen der Lie-Theorie verwendet, die in Charakteristik 0 gelten, nicht aber im Fall positiver Charakteristik.

Nur im einfachsten Fall, dem Fall des Drinfeld-Moduls vom Rang 1 (auch bekannt als Carlitz-Modul), ist es bislang gelungen, eine allgemeine Beschreibung der Torsionskörper anzugeben. Diese sind abelsche Körpererweiterungen von K und in ihren Eigenschaften mit Kreisteilungskörpern vergleichbar.

Es existiert kein Drinfeld-Modul höheren Ranges, dessen Torsionskörper vollständig bestimmt sind. In dieser Diplomarbeit wird ein konkreter Drinfeld-Modul des Rangs 2 untersucht. Es gelingt unter Voraussetzung zweier Hypothesen, die Torsionskörper beliebiger quadratfreier Elemente von $A = \mathbb{F}_q[T]$ zu bestimmen. Diese Ergebnisse liefern zugleich Ansätze für weitere Betrachtungen im allgemeinen Fall.

Die vorliegende Diplomarbeit setzt voraus, dass der Leser bereits grundlegend mit Funktionenkörpern vertraut ist. Im Speziellen werden Körpererweiterungen des rationalen Funktionenkörpers $K = \mathbb{F}_q(T)$ betrachtet. Als einführende Literatur

bietet sich beispielsweise [**Sti93**] an. Wichtige Sachverhalte werden jedoch in dieser Arbeit wiederholt bzw. zitiert.

Vorkenntnisse über Drinfeld-Moduln sind nicht notwendig, vielmehr dient hier Kapitel 1 als Einführung. In diesem werden Drinfeld-Moduln definiert und ihre wichtigsten Eigenschaften vorgestellt. Dadurch eignet sich die Arbeit insbesondere als Referenz für Mathematikstudenten, die zuvor noch nicht mit Drinfeld-Moduln gearbeitet haben.

Im zweiten Kapitel wird die zentrale Fragestellung der Diplomarbeit formuliert: Wir betrachten einen konkreten Drinfeld-Modul und definieren die zu bestimmenden Torsionskörper für normierte Primpolynome $\mathfrak{p} \in A$. Erste Überlegungen liefern, dass es in der gegebenen Situation zunächst reicht, das Verhalten an $\mathfrak{p}$ und der unendlichen Stelle zu untersuchen. Dies geschieht in den folgenden beiden Kapiteln.

Nach diesen lokalen Betrachtungen gelingt es uns in Kapitel 5, die gesuchten Eigenschaften des globalen Torsionskörpers zu bestimmen. Abschließend wird in Kapitel 6 gezeigt, wie sich diese Ergebnisse auf die Torsionskörper quadratfreier Elemente von A verallgemeinern lassen. Für den Spezialfall eines Produktes von zwei verschiedenen Primpolynomen wird dies explizit durchgeführt.

Im Anhang der Arbeit sind einige Definitionen und Aussagen aus verschiedenen Bereichen als Referenz zusammengefasst.

0.2. Danksagung

Mein Dank gilt an erster Stelle Herrn Professor Gekeler, der mich auf die interessante Theorie der Drinfeld-Moduln aufmerksam gemacht hat. Er hat sich stets Zeit für die Betreuung meiner Arbeit genommen und mir sowohl bei inhaltlichen als auch stilistischen Fragen sehr geholfen.

Weiter möchte ich mich bei Johannes Lengler und Thorsten Paul bedanken, die mir viele wertvolle Ratschläge gegeben haben.

Nicht zuletzt danke ich meinen Eltern, die es mir überhaupt ermöglicht haben, Mathematik zu studieren, und die mich stets in allen Belangen unterstützt und ermutigt haben.

KAPITEL 1

Drinfeld-Moduln: Definition und Eigenschaften

In diesem Kapitel führen wir den Begriff des Drinfeld-Moduls ein und geben einige grundlegende Eigenschaften an. Auf die Wiedergabe von Beweisen wird in der Regel verzichtet. Diese, sowie weitergehende Ausführungen, können beispielsweise bei [**Gos96**] nachgelesen werden.

Sei p eine Primzahl und q eine Potenz von p. Von nun an bezeichne A den Polynomring $\mathbb{F}_q[T]$ und K seinen Quotientenkörper $\mathbb{F}_q(T)$.

Sei L eine Körpererweiterung von K. Eine **Stelle** eines solchen Körpers L ist das maximale Ideal eines Bewertungsrings von L. Die Menge aller Stellen von L bezeichnen wir mit $\mathbb{P}_L$.

Eine Stelle P von K entspricht eineindeutig entweder einem normierten Primpolynom in A oder es handelt sich um die „unendliche“ Stelle mit Uniformisierender T^{-1}. Die unendliche Stelle wird auch mit ∞ bezeichnet. Stellen vom ersten Typ nennen wir endliche Stellen. Wir unterscheiden im Folgenden nicht zwischen einer endlichen Stelle $\mathfrak{p}$ von K und dem normierten Polynom, das das Ideal erzeugt, da aus dem Kontext deutlich wird, von welchem dieser Konzepte die Rede ist.

Für eine beliebige Stelle P von K bezeichnen wir mit K_P den Körper, den wir erhalten, wenn wir K bezüglich des Absolutbetrages an P vervollständigen. Den Ganzheitsring $\mathcal{O}_{K_P}$ erhalten wir, indem wir den Ring A an P lokalisieren und komplettieren. Mit $\overline{K}$ bezeichnen wir einen beliebigen algebraischen Abschluss von K und mit K^{sep} den separabel algebraischen Abschluss in $\overline{K}$.

1.1. Algebraische Beschreibung von Drinfeld-Moduln

1.1. Definition. Wir bezeichnen mit τ die Abbildung $x \mapsto x^q$. Für den Ring $\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a|L})$ der $\mathbb{F}_q$-Endomorphismen der additiven Gruppe von L gilt

$$\mathrm{End}_{\mathbb{F}_q}(\mathbb{G}_{a|L}) = L\{\tau\},$$

wobei $L\{\tau\}$ der nicht-kommutative Polynomring in τ ist. Die Nicht-Kommutativität erhält man durch die Rechenregel

$$\tau l = l^q \tau, \quad \text{für alle } l \in L.$$

Elemente von $L\{\tau\}$ bezeichnen wir als $\mathbb{F}_q$-additive Polynome oder kurz als **additive Polynome**.

1.2. Bemerkung. Polynome aus $L\{\tau\}$ können mittels der Korrespondenz

$$\tau^i = X^{q^i} \quad \text{für } i \geq 0$$

als $\mathbb{F}_q$-lineare Polynome in $L[X]$ aufgefasst werden und umgekehrt. Wir unterscheiden daher nicht zwischen Polynomen in τ und solchen der Form $\sum_{i=0}^{n} a_i X^{q^i}$ und lassen für ein Polynom $\varphi(X) = \sum_{i=0}^{n} a_i X^{q^i}$ mit Koeffizienten in L die Schreibweise

$$\varphi(X) = \sum_{i=0}^{n} a_i \tau^i \in L\{\tau\}$$

zu. Insbesondere sei darauf hingewiesen, dass aufgrund der Beziehung $\tau^0 = X$ das Absolutglied in τ-Notation dem linearen Term bezüglich X entspricht.

1.3. Definition. Ein **Drinfeld-Modul** auf L wird in der gegebenen Situation definiert durch einen $\mathbb{F}_q$-Ringhomomorphismus

$$\Phi : A \to L\{\tau\}$$

mit der Eigenschaft

$$\delta \circ \Phi = \mathrm{id}_A,$$

wenn $\delta : L\{\tau\} \to L$ die Einsetz-Abbildung $\tau \mapsto 0$ bezeichnet. Das Bild $\Phi(a)$ eines Elementes $a \in A$ unter Φ wird auch mit Φ_a bezeichnet.

1.4. Satz. *Wir bezeichnen mit* $\deg(a)$ *den gewöhnlichen Grad in* T *eines Polynoms* $a \in A$ *und mit* $\deg_\tau(f)$ *den wohlbestimmten Grad in* τ *eines additiven Polynoms* $f \in L\{\tau\}$. *Zu einem Drinfeld-Modul* Φ *existiert eine Zahl* $r \in \mathbb{N}_0$ *mit der Eigenschaft*

$$\deg_\tau(\Phi_a) = r \deg(a), \quad \textit{für alle } a \in A.$$

Die Zahl r *heißt der* ***Rang*** *von* Φ.

1.5. Bemerkung. Die Definition eines Rang-r-Drinfeld-Moduls auf L ist in der betrachteten Situation äquivalent dazu,

$$\Phi_T = T + g_1\tau + \ldots + g_r\tau^r \in L\{\tau\}, \quad g_r \neq 0,$$

anzugeben und auf A zu einem $\mathbb{F}_q$-Algebrenhomomorphismus fortzusetzen.

1.6. Bemerkung. Ein Drinfeld-Modul Φ induziert auf der additiven Gruppe von L und sogar auf jeder L-Algebra M eine neue A-Modulstruktur durch

$$a * x := \Phi_a(x) \quad \text{für alle } a \in A, x \in M.$$

Im Fall eines Rang-0-Drinfeld-Moduls entspricht diese Modulstruktur der tautologischen.

1.7. Definition. Sei $a \in A$. Als **a-Torsion** eines Drinfeld-Moduls bezeichnen wir die Menge

$${}_a\Phi := \ker \Phi_a = \left\{ x \in \overline{L} \mid \Phi_a(x) = 0 \right\}.$$

Ein Element $x \in {}_a\Phi$ wird auch **Torsionspunkt** genannt.

1.8. Satz. *Sei* Φ *ein Rang-*r*-Drinfeld-Modul. Für nicht-konstantes* $a \in A$ *ist die* a*-Torsion* ${}_a\Phi$ *ein freier* $A/(a)$*-Modul vom Rang* r.

1.9. Bemerkung. Bei der hier wiedergegebenen Situation handelt es sich um einen Spezialfall. Das Konzept des Drinfeld-Moduls existiert auch in weiteren Ringen. Im Allgemeinen definiert man einen Drinfeld-Ring als affinen Ring einer Kurve $X \setminus \{\infty\}$ für eine algebraische Kurve X über $\mathbb{F}_q$ und einen abgeschlossenen Punkt $\infty \in X$.

Die angegebenen Definitionen und Eigenschaften übertragen sich sinngemäß auf die allgemeine Situation.

1.2. Analytische Beschreibung

Sei $K_\infty = \mathbb{F}_q((T^{-1}))$ die Komplettierung von K bzgl. des Absolutbetrags $|\cdot| = |\cdot|_\infty$ an ∞. Dieser Absolutbetrag besitzt eine eindeutige Fortsetzung auf den algebraischen Abschluss $\overline{K}_\infty$, da er sich auf jede endliche Teilerweiterung eindeutig fortsetzen lässt. Die Komplettierung $\mathcal{C}$ von $\overline{K}_\infty$ ist wieder algebraisch abgeschlossen, d.h. es handelt sich bei $\mathcal{C}$ um einen algebraisch abgeschlossenen und bzgl. $|\cdot|$ vollständigen Körper (siehe [**BGR84**, S. 146]). Auf einem solchen Körper kann eine analytische Theorie definiert werden.

1.10. Definition. Ein **A-Gitter** in $\mathcal{C}$ ist ein endlich erzeugter A-Untermodul $\Lambda \subset \mathcal{C}$, so dass für jeden Ball $B_s(0)$ um Null mit Radius s gilt, dass $\Lambda \cap B_s(0)$ endlich ist.

Die **Exponentialfunktion** $e_\Lambda : \mathcal{C} \to \mathcal{C}$ eines Gitters ist definiert als das für alle $z \in \mathcal{C}$ konvergente unendliche Produkt

$$e_\Lambda(z) = z \prod_{0 \neq \lambda \in \Lambda} \left(1 - \frac{z}{\lambda}\right).$$

1.11. Bemerkung. Nach Definition gilt für die Exponentialfunktion e_Λ eines Gitters Λ

$$\ker e_\Lambda = \Lambda.$$

Weiter ist e_Λ surjektiv und $\mathbb{F}_q$-linear und lässt sich schreiben als überall konvergente Potenzreihe

$$e_\Lambda(z) = \sum_{i \geq 0} \alpha_i z^{q^i} \quad \text{mit } \alpha_i \in \mathcal{C} \text{ und } \alpha_0 = 1.$$

1.12. Satz. *Es exisistiert eine Bijektion zwischen der Menge der A-Gitter, die als A-Moduln frei vom Rang r sind, und der Menge der Drinfeld-Moduln des Rangs r über $\mathcal{C}$.*

1.13. Bemerkung. Sei Λ ein A-Gitter mit Exponentialfunktion e_Λ und Φ^Λ der zugehörige Drinfeld-Modul über $\mathcal{C}$. Für $a \in A$ ist das Diagramm

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \Lambda & \longrightarrow & \mathcal{C} & \xrightarrow{e_\Lambda} & \mathcal{C} & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle \Phi_a^\Lambda} & & \\ 0 & \longrightarrow & \Lambda & \longrightarrow & \mathcal{C} & \xrightarrow{e_\Lambda} & \mathcal{C} & \longrightarrow & 0 \end{array}$$

kommutativ. Die ersten beiden vertikalen Pfeile bezeichnen hierbei Multiplikation mit a. Insbesondere gilt somit die **Funktionalgleichung**

$$e_\Lambda \circ a = \Phi_a^\Lambda \circ e_\Lambda.$$

1.14. Satz. *In der Situation von Bemerkung 1.13 gilt*

$$a^{-1}\Lambda/\Lambda \xrightarrow{\cong} {}_a\Phi^\Lambda \quad \textit{(kanonisch)}$$

und

$$a^{-1}\Lambda/\Lambda \cong \Lambda/a\Lambda \quad \textit{(unkanonisch).}$$

Beweis. Aus Bemerkung 1.13 folgt direkt, dass

$$e_\Lambda\left(a^{-1}\Lambda\right) = {}_a\Phi^\Lambda$$

ist. Die Abbildung

$$e_\Lambda : a^{-1}\Lambda/\Lambda \longrightarrow {}_a\Phi^\Lambda$$

ist somit ein Isomorphismus, da $\ker e_\Lambda = \Lambda$ ist.

Die Isomorphie von $a^{-1}\Lambda/\Lambda$ und $\Lambda/a\Lambda$ ist im Allgemeinen unkanonisch, da sie durch Multiplikation mit einem beliebigen Erzeuger des Ideals $(a) \subset A$ beschrieben werden kann. Während im betrachteten Fall des Hauptidealrings $A = \mathbb{F}_q[T]$ noch die quasikanonische Wahl eines normierten Erzeugers möglich ist, gilt dies in allgemeineren Situationen nicht mehr. □

1.15. Bemerkung. Es ist möglich, mittels der Funktionalgleichung für einen gegebenen Drinfeld-Modul Φ^Λ die Exponentialfunktion $e_\Lambda = \sum_{i \geq 0} \alpha_i \tau^i$ des zugehörigen Gitters zu berechnen und umgekehrt.

Sei $a \in A \setminus \mathbb{F}_q$. Betrachten wir das Bild

$$\Phi_a^\Lambda = \sum_{i=0}^{r \deg a} s_i \tau^i$$

von a unter Φ, dann genügt α_k für alle $k \geq 1$ der Gleichung

$$(a^{q^k} - a)\alpha_k = \sum_{i=0}^{k-1} s_{k-i} \alpha_i^{q^{k-i}},$$

die sich mit $\alpha_0 = 1$ eindeutig rekursiv lösen lässt. Der Ausdruck $a^{q^k} - a$ ist nach Wahl von a ungleich Null, da $\mathbb{F}_q$ in A algebraisch abgeschlossen ist.

1.16. Satz. *Sei $\Lambda \subset \mathcal{C}$ ein Gitter, dessen Exponentialfunktion $e_\Lambda = \sum_{i \geq 0} \alpha_i \tau^i$ die Bedingung $\alpha_i \in K_\infty$ für alle i erfüllt. Dann gilt*

$$\Lambda \subset K_\infty^{\text{sep}}.$$

Beweis. Da e_Λ eine ganze Funktion ist, gilt

$$|\alpha_i| \, r^{q^i} \to 0 \tag{1.1}$$

für alle $r > 0$. Damit haben fast alle α_i Absolutbetrag < 1. Indem wir gegebenenfalls zu einem geeigneten Gitter $c\Lambda$ mit $c \in K_\infty$ übergehen, können wir sogar annehmen, dass alle Koeffizienten von e_Λ ganz sind. Es folgt nämlich aus der Definition der Exponentialfunktion, dass

$$e_{c\Lambda}(z) = c e_\Lambda(\frac{z}{c}) = \sum_{i \geq 0} c^{1-q^i} \alpha_i z^{q^i}$$

ist. Liegt $c\Lambda$ aber in K_∞^{sep}, so auch Λ.

Da e_Λ ganze Koeffizienten besitzt und so normiert ist, dass $\alpha_0 = 1$ gilt, folgt durch Betrachten des Newtonpolygons von e_Λ (siehe Abschnitt A.2), dass $|\lambda| \geq 1$ ist für jeden Gitterpunkt $0 \neq \lambda \in \Lambda$.

Wir betrachten nun für $k \geq 0$ die additiven Polynome

$$e_k := \sum_{0 \leq i \leq k} \alpha_i \tau^i \in \mathcal{O}_{K_\infty}\{\tau\}.$$

Für die Polynome $e_k(X)$ gilt das Lemma von Hensel in der Fassung von [**Lan70**, S. 42] auch ohne die Voraussetzung, dass ein Startwert x_0 Absolutbetrag ≤ 1 haben muss (siehe Bemerkung 1.17).

Sei nun $\lambda \in \Lambda$ und $0 < \varepsilon < 1$, so existiert wegen (1.1) ein $k = k(\varepsilon)$ derart, dass

$$\left| \alpha_n \lambda^{q^n} \right| \leq \varepsilon \quad \text{für alle } n \geq k \tag{1.2}$$

gilt. Da λ eine Nullstelle von e_Λ ist, erhalten wir

$$e_k(\lambda) = -\sum_{i > k} \alpha_i \lambda^{q^i}.$$

Außerdem gilt nach Defintion $e_k'(z) = \alpha_0 = 1$. Wir können wegen

$$\left| \frac{e_k(\lambda)}{e_k'(\lambda)^2} \right| = \left| \frac{-\sum_{i>k} \alpha_i \lambda^{q^i}}{1} \right| \leq \sup_{i>k} \left| \alpha_i \lambda^{q^i} \right| \leq \varepsilon$$

also das Lemma von Hensel in der oben zitierten Fassung mit Startwert λ anwenden und erhalten eine eindeutig bestimmte Nullstelle λ_k von e_k mit der Eigenschaft $|\lambda - \lambda_k| \leq \varepsilon$. Da wir aber bereits wissen, dass $|\lambda| \geq 1 > \varepsilon$ gilt, muss $|\lambda_k| = |\lambda|$ sein.

Nach Voraussetzung ist auch

$$|e_{k+1}(\lambda_k)| = \left|e_k(\lambda_k) + \alpha_{k+1}\lambda_k^{q^{k+1}}\right| = \left|\alpha_{k+1}\lambda_k^{q^{k+1}}\right| \leq \varepsilon,$$

also existiert nach dem Lemma von Hensel eine eindeutige Nullstelle $\mu_{k+1} \in K_\infty(\lambda_k)$ von e_{k+1} mit der Eigenschaft $|\mu_{k+1} - \lambda_k| \leq \varepsilon$. Wegen der Eindeutigkeit der Konstruktion erhalten wir mit $\mu_{k+1} = \lambda_{k+1}$ eine Folge $(\lambda_i)_{i=k}^{\infty} \subset K_\infty(\lambda_k)$, so dass λ_i Nullstelle von e_i ist. Dann gilt aber

$$|\lambda - \lambda_i| \leq \sup_{n>i}\left|\alpha_n\lambda^{q^n}\right| \overset{i\to\infty}{\longrightarrow} 0,$$

d.h. $\lambda = \lim\limits_{i\to\infty} \lambda_i$ liegt bereits in $K_\infty(\lambda_{k_0})$, wobei k_0 minimal mit der Eigenschaft (1.2) für ein $\varepsilon < 1$ ist. Die Körpererweiterung $K_\infty(\lambda_{k_0})|K_\infty$ ist separabel, da $e_{k_0}(z)$ nach Definition separabel ist. Damit folgt, dass jeder Gitterpunkt λ in einer separablen Erweiterung von K_∞ liegt, also ist $\Lambda \subset K_\infty^{\mathrm{sep}}$. □

1.17. Bemerkung. Der Beweis des Lemmas von Hensel in [**Lan70**, S. 42] vereinfacht sich in unserer Situation durch die Additivität der betrachteten Polynome $e_k(X)$. In Termen der Taylor-Entwicklung bedeutet dies, dass bereits die zweiten Ableitungen verschwinden.

Um die für die Konvergenz erforderlichen Abschätzungen zu zeigen, reicht es dann, dass der Funktionswert im Startwert hinreichend klein im Vergleich zum Wert der Ableitung ist, sofern das betrachtete Polynom ganze Koeffizienten hat. Man kann im Fall eines Startwertes von Betrag > 1 allerdings nicht erwarten, dass die konstruierte Nullstelle ganz ist.

1.18. Bemerkung. Es genügt in Satz 1.16 vorauszusetzen, dass die Koeffizienten von e_Λ in K_∞^{sep} liegen. Der Beweis erfolgt in diesem Fall analog.

1.19. Satz. *Die folgenden Aussagen sind äquivalent:*

(1) *Die Koeffizienten von Φ_T liegen in K_∞^{sep}.*
(2) *Die Exponentialfunktion e_Λ ist Element von $K_\infty^{\mathrm{sep}}\{\{\tau\}\}$.*
(3) *Es gilt: $\Lambda \subset K_\infty^{\mathrm{sep}}$.*

Beweis. Die Äquivalenz der ersten beiden Aussagen ist eine direkte Konsequenz der Rekursionsformel aus Bemerkung 1.15. Dass die zweite Aussage die dritte impliziert, folgt aus Satz 1.16 und Bemerkung 1.18.

Sei also $\Lambda \subset K_\infty^{\mathrm{sep}}$. Da Λ als A-Gitter endlich erzeugt ist, liegt Λ bereits in einer endlichen separablen Erweiterung von K_∞, die somit vollständig ist. Nach Definition ist damit auch jeder Koeffizient von e_Λ in einer separablen Erweiterung von K_∞ enthalten, d.h. $e_\Lambda \in K_\infty^{\mathrm{sep}}\{\{\tau\}\}$. □

1.20. Bemerkung. Man kann in Satz 1.19 den Körper K_∞^{sep} durch den algebraischen Abschluss $\overline{K}_\infty$ von K_∞ ersetzen.

KAPITEL 2

Formulierung der Fragestellungen

In diesem Kapitel beschreiben wir die Fragestellungen, mit denen wir uns im Folgenden befassen werden. Dazu wählen wir zunächst einen konkreten Drinfeld-Modul des Rangs 2:

Wir betrachten im gesamten weiteren Verlauf dieser Arbeit den durch

$$\Phi_T = T + \tau - \tau^2 \in K\{\tau\}$$

gegebenen Drinfeld-Modul. Aufgrund der global gewählten Koeffizienten ist dieser über jeder Körpererweiterung von K definiert.

2.1. Bemerkung. Die Festlegung des betrachteten Drinfeld-Moduls ist nicht zufällig erfolgt. Vielmehr sind die Koeffizienten so gewählt, dass Rechnungen in diesem Drinfeld-Modul möglichst einfach sind.

Sei $\mathfrak{p} \in A$ ein normiertes Primpolynom vom Grad d. Wie erwähnt bezeichnen wir auch die von diesem Polynom erzeugte endliche Stelle des Grades d mit $\mathfrak{p}$. Das additive Polynom $\Phi_\mathfrak{p}$ ist von der Gestalt

$$\Phi_\mathfrak{p} = (-1)^d \tau^{2d} + \sum_{i=1}^{2d-1} a_i \tau^i + \mathfrak{p}\tau^0. \tag{2.1}$$

Dass $\Phi_\mathfrak{p}$ Absolutglied $\mathfrak{p}$ besitzt, folgt aus der in Definition 1.3 angegebenen Eigenschaft des Homomorphismus Φ. Der Leitkoeffizient kann direkt aus der Definition von Φ_T berechnet werden.

Unser Ziel ist es, die Eigenschaften der zugehörigen Torsionskörper, d.h. von Körpererweiterungen der Form

$$K({}_\mathfrak{p}\Phi)|K,$$

zu bestimmen. Wir wissen in jedem Fall:

2.2. Lemma. *Sei $\mathfrak{p} \in A$ ein normiertes Primpolynom vom Grad d. Dann ist die Erweiterung $K({}_\mathfrak{p}\Phi)|K$ galoissch.*

Beweis. Das additive Polynom $\Phi_\mathfrak{p} \in K\{\tau\}$ besitzt als Element von $K[X]$ die Form

$$\Phi_\mathfrak{p}(X) = (-1)^d X^{q^{2d}} + \sum_{i=1}^{2d-1} a_i X^{q^i} + \mathfrak{p}X.$$

Folglich gilt

$$\Phi'_\mathfrak{p}(X) = \mathfrak{p}.$$

Das Polynom $\Phi_\mathfrak{p}(X)$ ist daher separabel. Nach Konstruktion ist die Erweiterung $K({}_\mathfrak{p}\Phi)|K$ normal, da es sich bei ${}_\mathfrak{p}\Phi$ um die Nullstellenmenge des Polynoms $\Phi_\mathfrak{p}(X)$ handelt. Damit ist $K({}_\mathfrak{p}\Phi)|K$ eine Galois-Erweiterung. □

Wir werden Grad, Galois-Gruppe, Verzweigungsverhalten und Geschlecht derartiger Körpererweiterungen berechnen.

Nach Satz 1.8 ist ${}_{\mathfrak{p}}\Phi$ ein $A/\mathfrak{p}$-Vektorraum der Dimension 2. Diese Eigenschaft wird sich als hilfreich bei der Konstruktion der Torsionskörper erweisen. Der Restkörper $A/\mathfrak{p}$ wird im Folgenden kurz mit $\mathbb{F}_{\mathfrak{p}}$ bezeichnet. Es gilt

$$\#\mathbb{F}_{\mathfrak{p}} = q^d.$$

Eine weitere Konsequenz von Satz 1.8 ist die Tatsache, dass sich die Galois-Gruppe $G := \mathrm{Gal}(K({}_{\mathfrak{p}}\Phi)|K)$ in die Gruppe $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}})$ der invertierbaren 2×2-Matrizen über $\mathbb{F}_{\mathfrak{p}}$ einbetten lässt.

Für die Bestimmung des Geschlechts von $K({}_{\mathfrak{p}}\Phi)|K$ erinnern wir an die Riemann-Hurwitz-Formel:

2.3. Satz (Riemann-Hurwitz-Formel). *Sei F ein algebraischer Funktionenkörper mit Konstantenkörper k und $F'|F$ eine endliche separable Erweiterung mit Konstantenkörpererweiterung $k'|k$. Bezeichne mit $g_{F'}$ und g_F das Geschlecht von $F'|k'$ bzw. $F|k$. Dann gilt*

$$2g_{F'} - 2 = \frac{[F' : F]}{[k' : k]}(2g_F - 2) + \deg \mathcal{D}_F^{F'},$$

wobei $\mathcal{D}_F^{F'}$ die Differente von F' über F ist.

Beweis. Siehe [**Sti93**, Theorem III.4.12]. □

2.4. Bemerkung. Für die in dieser Arbeit verwendeten Notationen zu Differente und Diskriminante, sowie einige Eigenschaften, siehe Abschnitt A.1.

Wir wollen die Riemann-Hurwitz-Formel nun auf die konkrete Situation anwenden, d.h. wir setzen $F = K$ und $F' = K({}_{\mathfrak{p}}\Phi)$. In Kapitel 5 werden wir sehen, dass in diesem Fall die Konstantenerweiterung trivial ist. Weiter wissen wir für den rationalen Funktionenkörper K bereits, dass

$$g_K = 0$$

gilt.

2.5. Lemma. *Die Erweiterung $K({}_{\mathfrak{p}}\Phi)|K$ kann nur an den Stellen $\mathfrak{p}$ und ∞ verzweigt sein.*

Beweis. Sei $\mathfrak{q}$ eine endliche Stelle von K und $\mathfrak{Q}$ eine Stelle in $K({}_{\mathfrak{p}}\Phi)$ über $\mathfrak{q}$. Da es sich bei $K({}_{\mathfrak{p}}\Phi)|K$ um eine Galois-Erweiterung handelt, hängt das Verhalten einer über $\mathfrak{q}$ liegenden Stelle von $K({}_{\mathfrak{p}}\Phi)$ nicht davon ab, welche dieser Fortsetzungen von $\mathfrak{q}$ wir betrachten. Das Verzweigungsverhalten von $\mathfrak{Q}|\mathfrak{q}$ können wir in der lokalisierten und komplettierten Situation bestimmen. In diesem Fall gilt

$$\left(K({}_{\mathfrak{p}}\Phi)\right)_{\mathfrak{Q}} = K_{\mathfrak{q}}({}_{\mathfrak{p}}\Phi),$$

wir betrachten also die Erweiterung lokaler Körper $K_{\mathfrak{q}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{q}}$.

Da das additive Polynom $\Phi_{\mathfrak{p}}$ Absolutglied $\mathfrak{p}$ besitzt, hat $\Phi_{\mathfrak{p}}$ an jeder endlichen Stelle $\mathfrak{q} \neq \mathfrak{p}$ gute Reduktion, d.h. $\Phi_{\mathfrak{p}}$ reduziert modulo $\mathfrak{q}$ zu einem separablen Polynom $\overline{\Phi}_{\mathfrak{p}}$ gleichen Grades. Nach dem trivialen Fall des Lemmas von Hensel (siehe Satz A.15) kann daher jede Nullstelle von $\overline{\Phi}_{\mathfrak{p}}$ zu einer Nullstelle von $\Phi_{\mathfrak{p}}$ geliftet werden.

Es genügt also, die durch $\overline{\Phi}_{\mathfrak{p}}$ beschriebene Restkörpererweiterung vorzunehmen, um den Torsionskörper $K_{\mathfrak{q}}({}_{\mathfrak{p}}\Phi)$ zu erzeugen. Damit ist die Erweiterung $K_{\mathfrak{q}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{q}}$ unverzweigt, d.h. $\mathfrak{q}$ ist unverzweigt in $K({}_{\mathfrak{p}}\Phi)|K$. □

2.6. Bemerkung. Wir vereinfachen nun die Riemann-Hurwitz-Formel für den betrachteten Torsionskörper unter der Voraussetzung, dass die Körpererweiterung $K({}_{\mathfrak{p}}\Phi)|K$ triviale Konstantenerweiterung besitzt.

Für die Bestimmung des Grades der Differente genügt es, die lokalen Diskriminantenexponenten zu berechnen. Es gilt nach Definition des Grades eines Divisors

$$\deg \mathcal{D}_K^{K({}_\mathfrak{p}\Phi)} = \sum_{P \in \mathbb{P}_K} \sum_{\mathfrak{P}|P} d(\mathfrak{P}|P) \deg \mathfrak{P},$$

wobei der Ausdruck $\sum_{\mathfrak{P}|P}$ bedeutet, dass über alle Stellen $\mathfrak{P}$ in $K({}_\mathfrak{p}\Phi)$ summiert wird, die über der Stelle P von K liegen.

Weiter sei $f_{\mathfrak{P}|P}$ der Trägheitsindex von $\mathfrak{P}|P$. Dann ist nach Definition des Grades einer Stelle

$$\deg \mathfrak{P} = f_{\mathfrak{P}|P} \deg P.$$

Die Trägheitsindizes und Differentenexponenten sind hierbei unabhängig von der konkreten Stelle $\mathfrak{P}$ über gegebenem P, da die Erweiterung $K({}_\mathfrak{p}\Phi)|K$ galoissch ist. Es reicht also, die Betrachtungen in der lokalisierten Situation durchzuführen. Die Formel lautet damit

$$\deg \mathcal{D}_K^{K({}_\mathfrak{p}\Phi)} = \sum_{P \in \mathbb{P}_K} \#\{\mathfrak{P}|P\}\, d(K_P({}_\mathfrak{p}\Phi)|K_P) f_{K_P({}_\mathfrak{p}\Phi)|K_P} \deg P,$$

wobei $\#\{\mathfrak{P}|P\}$ die Anzahl der Stellen von $K({}_\mathfrak{p}\Phi)$ über P bezeichnet. Der Ausdruck

$$d(K_P({}_\mathfrak{p}\Phi)|K_P) f_{K_P({}_\mathfrak{p}\Phi)|K_P}$$

ist nach Definition nichts anderes als der lokale Diskriminantenexponent $D_{K_P({}_\mathfrak{p}\Phi)|K_P}$ (siehe Bemerkung A.4).

Aus Lemma 2.5 wissen wir, dass nur die Diskriminantenexponenten an den Stellen $\mathfrak{p}$ und ∞ ungleich Null sein können. Die Riemann-Hurwitz-Formel lässt sich damit schließlich auf die Form

$$2g_L - 2 = -2[K({}_\mathfrak{p}\Phi) : K] + \deg \mathfrak{p}\, \#\{\mathfrak{p}'|\mathfrak{p}\}\, D_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}} + \#\{\infty'|\infty\}\, D_{K_\infty({}_\mathfrak{p}\Phi)|K_\infty}$$

vereinfachen.

Wir werden aufgrund dieser Überlegungen die Körpererweiterung $K({}_\mathfrak{p}\Phi)|K$ zunächst in der an $\mathfrak{p}$ bzw. ∞ lokalisierten Situation untersuchen, um die lokalen Diskriminantenexponenten zu berechnen. Die Eigenschaften des globalen Torsionskörpers können wir anschließend aus den lokalen Daten bestimmen.

KAPITEL 3

Die endliche Stelle $\mathfrak{p}$

Wir untersuchen in diesem Kapitel das Verhalten von $K({}_{\mathfrak{p}}\Phi)$ an der endlichen Stelle $\mathfrak{p}$. Sei $K_{\mathfrak{p}}$ die Komplettierung von K an $\mathfrak{p}$ und $\mathcal{O}_{K_{\mathfrak{p}}}$ der (lokale) Ganzheitsring von $K_{\mathfrak{p}}$ mit normierter Bewertung v. Das normierte Primpolynom $\mathfrak{p} \in A \subset \mathcal{O}_{K_{\mathfrak{p}}}$ ist eine Uniformisierende von $K_{\mathfrak{p}}$. Für den Restkörper gilt ${}^{\mathcal{O}_{K_{\mathfrak{p}}}}\!/_{\mathfrak{p}} = \mathbb{F}_{\mathfrak{p}}$.

Wir betrachten die Erweiterung $K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}$ (vgl. dazu Lemma 2.5) und definieren die lokale Galois-Gruppe

$$G_{\mathfrak{p}} := \mathrm{Gal}(K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}).$$

Diese lässt sich in die globale Galois-Gruppe $G = \mathrm{Gal}(K({}_{\mathfrak{p}}\Phi)|K)$ einbetten und ist isomorph zur Zerlegungsgruppe einer Stelle $\mathfrak{P}$ von $K({}_{\mathfrak{p}}\Phi)$ über $\mathfrak{p}$ (siehe [**Lan70**, S. 13]).

Indem wir die eindeutigen Fortsetzungen von v auf endliche algebraische Erweiterungen von $K_{\mathfrak{p}}$ so normieren, dass eine Uniformisierende von $K_{\mathfrak{p}}$ weiterhin Bewertung 1 besitzt, erhalten wir Bewertungen, die bestimmte Nenner zulassen. Auf diese Weise lässt sich eine eindeutige Fortsetzung von v auf einen algebraischen Abschluss $\overline{K}_{\mathfrak{p}}$ definieren, die $\mathbb{Q} \cup \{\infty\}$ als Bild besitzt. Da diese Fortsetzung eingeschränkt auf $K_{\mathfrak{p}}$ mit der ursprünglichen Bewertung v übereinstimmt, bezeichnen wir sie ebenfalls mit v. Ist im Folgenden nichts anderes angegeben, so beziehen wir uns stets auf diese Bewertung.

Insbesondere entspricht dies der Bewertung, die in Satz A.9 für die Aussage des Newton-Polygons verwendet wird.

Zunächst bestimmen wir die Reduktion von $\Phi_{\mathfrak{p}}$ modulo $\mathfrak{p}$. Wir werden sehen, dass hierbei zwei Fälle möglich sind, die ein unterschiedliches Vorgehen bei den weiteren Betrachtungen erfordern.

Wie bereits in Kapitel 2 erwähnt, gilt die Isomorphie von $\mathbb{F}_{\mathfrak{p}}$-Vektorräumen

$${}_{\mathfrak{p}}\Phi \cong \mathbb{F}_{\mathfrak{p}} \times \mathbb{F}_{\mathfrak{p}}.$$

Dies ist ein Spezialfall des folgenden allgemeineren Sachverhalts:

3.1. Bemerkung. Da Φ_T Koeffizienten in A besitzt, erzeugt der Drinfeld-Modul Φ nicht nur A-Modulstrukturen auf Körpererweiterungen von $K_{\mathfrak{p}}$, sondern auch auf Ringerweiterungen von $\mathcal{O}_{K_{\mathfrak{p}}}$, dem Ideal $\mathfrak{p}$ und ${}_{\mathfrak{p}}\Phi$ selbst.

Wir behalten die Notation aus (2.1) bei und schreiben

$$\Phi_{\mathfrak{p}} = \mathfrak{p}\tau^0 + a_1\tau + \ldots + a_d\tau^d + \ldots + (-1)^d\tau^{2d}$$

mit Koeffizienten in A, also insbesondere in $\mathcal{O}_{K_{\mathfrak{p}}}$. Die Reduktion des additiven Polynoms $\Phi_{\mathfrak{p}}$ modulo $\mathfrak{p}$ hat die Form

$$\overline{\Phi}_{\mathfrak{p}} \equiv 0\tau^0 + \overline{a_1}\tau + \ldots + \overline{a_d}\tau^d + \ldots + (-1)^d\tau^{2d} \mod \mathfrak{p}.$$

3.2. Bemerkung. Wir können die Reduktion $\overline{\Phi} : A \to \mathbb{F}_{\mathfrak{p}}\{\tau\}$ von Φ modulo $\mathfrak{p}$ als Drinfeld-Modul auf Erweiterungen von $\mathbb{F}_{\mathfrak{p}} = A/\mathfrak{p}$ betrachten (vgl. zum Beispiel [**Gek91**, Abschnitt 1]). Da Φ_T Leitkoeffizient -1 besitzt, gilt

$$\deg_\tau \overline{\Phi}_T = 2,$$

also ist auch $\overline{\Phi}$ ein Drinfeld-Modul des Rangs 2.

Nach Bemerkung 3.1 wird durch Φ eine $\mathbb{F}_\mathfrak{p}$-Vektorraumstruktur auf ${}_\mathfrak{p}\Phi$ induziert. Ebenso ist durch $\overline{\Phi}$ eine $\mathbb{F}_\mathfrak{p}$-Vektorraumstruktur auf $\ker \overline{\Phi}_\mathfrak{p}$ gegeben. Das reduzierte Polynom $\overline{\Phi}_\mathfrak{p}(X)$ ist vom Grad q^{2d}, besitzt auf Grund der oben gezeigten Gestalt aber die mindestens q-fache Nullstelle 0. Wegen $\#\mathbb{F}_\mathfrak{p} = q^d$ muss daher entweder

$$\ker \overline{\Phi}_\mathfrak{p} \cong \{0\} \tag{3.1}$$

oder

$$\ker \overline{\Phi}_\mathfrak{p} \cong \mathbb{F}_\mathfrak{p} \tag{3.2}$$

gelten.

Andererseits ist eine direkte Folge aus der Definition von Ganzheitsringen, dass die Nullstellen von $\Phi_\mathfrak{p} \in \mathcal{O}_{K_\mathfrak{p}}\{\tau\}$ in $K_\mathfrak{p}({}_\mathfrak{p}\Phi)$ ganz sind, d.h. dass

$${}_\mathfrak{p}\Phi \subset \mathcal{O}_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)}$$

gilt. Bezeichnen wir das maximale Ideal von $\mathcal{O}_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)}$ mit $\mathfrak{P}$, können wir also die Reduktion ${}_\mathfrak{p}\overline{\Phi}$ von ${}_\mathfrak{p}\Phi$ modulo $\mathfrak{P}$ betrachten.

Da ${}_\mathfrak{p}\Phi$ die Nullstellenmenge von $\Phi_\mathfrak{p}$ ist, gilt im Restkörper von $\mathcal{O}_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)}$

$$\ker \overline{\Phi}_\mathfrak{p} = {}_\mathfrak{p}\overline{\Phi},$$

d.h. die Reduktionsabbildung von der $\mathfrak{p}$-Torsion des Drinfeld-Moduls Φ in die $\mathfrak{p}$-Torsion von $\overline{\Phi}$ ist surjektiv und besitzt als Kern $\mathbb{F}_\mathfrak{p} \times \mathbb{F}_\mathfrak{p}$ im ersten, bzw. $\mathbb{F}_\mathfrak{p}$ im zweiten Fall.

Fall (3.1) bedeutet

$$\overline{\Phi}_\mathfrak{p}(X) \equiv (-1)^d X^{q^{2d}} \mod \mathfrak{p},$$

da $\overline{\Phi}_\mathfrak{p}(X)$ die q^{2d}-fache Nullstelle 0 besitzt. Diesen Fall nennen wir in Anlehnung an die klassische Situation **supersingulär**.

Im Fall (3.2) hat die Nullstelle 0 von $\overline{\Phi}_\mathfrak{p}(X)$ Vielfachheit q^d, es gilt also

$$\overline{\Phi}_\mathfrak{p}(X) \equiv X^{q^d}\left(\overline{a}_d + \ldots + (-1)^d X^{q^{2d}-q^d}\right) \mod \mathfrak{p}, \quad \overline{a}_d \not\equiv 0 \bmod \mathfrak{p}. \tag{3.3}$$

Dies ist der **ordinäre** Fall.

Die obigen Überlegungen erlauben es uns, ein Kriterium dafür zu formulieren, wann eine Stelle supersingulär ist.

3.3. Satz. *Sei $\mathfrak{p} \in A$ ein normiertes Primpolynom vom Grad d. Die Stelle $\mathfrak{p}$ ist genau dann supersingulär, wenn für den d-Koeffizienten a_d von $\Phi_\mathfrak{p}$ die Kongruenz*

$$a_d \equiv 0 \mod \mathfrak{p}$$

gilt.

3.4. Korollar. *Sei $\mathfrak{p}$ eine Stelle vom Grad $d = 1$. Dann ist $\mathfrak{p}$ ordinär.*

Beweis. In der betrachteten Situation gilt

$$\Phi_\mathfrak{p} = -\tau^2 + \tau + \mathfrak{p},$$

d.h. es ist

$$a_1 = 1 \not\equiv 0 \mod \mathfrak{p}.$$

Mit Satz 3.3 folgt die Behauptung. □

3.5. Bemerkung. Für einen beliebigen Drinfeld-Modul ist der überwiegende Anteil der Stellen ordinär. Supersingularität stellt die Ausnahme dar.

Zwar weiß man, dass es unendlich viele supersinguläre Stellen gibt, bis jetzt konnte allerdings nur gezeigt werden, dass die Anzahl der supersingulären Stellen des Grades n mindestens so schnell wächst wie $\log\log n$.

Im Falle des hier betrachteten Drinfeld-Moduls gilt: Für Stellen des Grades 2 tritt Supersingularität nur in Charakteristik 2 auf. Eine Stelle vom Grad 3 kann nur in Charakteristik 3 supersingulär sein.

3.6. Beispiel. Für die folgende Auswahl von Grundkörpern konnten die Anteile supersingulärer Stellen kleiner Grade des betrachteten Drinfeld-Moduls berechnet werden. Dabei bezeichnet S_d die Anzahl der supersingulären Stellen des Grades d. Zum Vergleich ist mit P_d die Anzahl aller endlichen Stellen vom Grad d angegeben. Einträge, die mit „−“ bezeichnet sind, konnten nicht berechnet werden.

	P_2	S_2	P_3	S_3	P_4	S_4	P_5	S_5
$\mathbb{F}_2$	1	1	2	0	3	1	6	0
$\mathbb{F}_4$	6	2	20	0	60	4	204	0
$\mathbb{F}_8$	28	4	168	0	1 008	16	6 552	0
$\mathbb{F}_{16}$	120	8	1 360	0	16 320	64	209 712	0
$\mathbb{F}_{32}$	496	16	10 912	0	261 888	256	6 710 880	−
$\mathbb{F}_{64}$	2 016	32	87 360	0	4 193 280	−	214 748 352	−
$\mathbb{F}_3$	3	0	8	3	18	0	48	0
$\mathbb{F}_9$	36	0	240	27	1620	0	11 808	0
$\mathbb{F}_{27}$	351	0	6 552	243	132 678	0	2 869 776	−
$\mathbb{F}_{81}$	3 240	0	177 120	2 187	10 760 040	−	697 356 864	−
$\mathbb{F}_5$	10	0	40	0	150	0	624	30
$\mathbb{F}_{25}$	300	0	5 200	0	97 500	0	1 953 120	3250
$\mathbb{F}_7$	21	0	112	0	588	0	3 360	0
$\mathbb{F}_{11}$	55	0	440	0	3 630	0	32 208	0
$\mathbb{F}_{13}$	78	0	728	0	7 098	0	74 256	0
$\mathbb{F}_{17}$	136	0	1 632	0	20 808	0	283 968	0
$\mathbb{F}_{19}$	171	0	2 280	0	32 490	0	495 216	0
$\mathbb{F}_{23}$	253	0	4 048	0	69 828	0	1 287 264	0
$\mathbb{F}_{29}$	406	0	8 120	0	176 610	0	4 102 224	−

Wir beginnen unsere weiteren Untersuchungen in beiden Fällen jeweils damit, das Newton-Polygon von

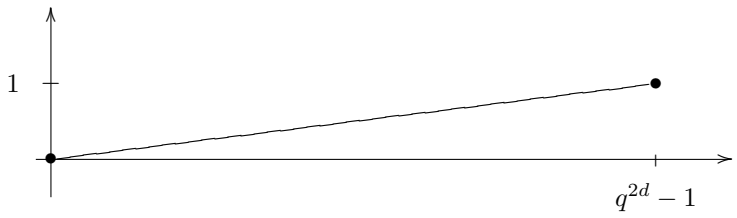
$$f(X) := \frac{\Phi_{\mathfrak{p}}(X)}{X} = \mathfrak{p} + a_1 X^{q-1} + \ldots + a_{2d-1} X^{q^{2d-1}-1} + (-1)^d X^{q^{2d}-1}$$

über $K_{\mathfrak{p}}[X]$ zu bestimmen.

3.7. Bemerkung. Im Weiteren legen wir für das Newton-Polygon eines Polynoms immer die Beschreibung aus Definition A.8 zugrunde, d.h. der äußerste linke Punkt des Newton-Polygons korrespondiert zum Leitkoeffizienten, während der äußerste rechte Punkt durch das Absolutglied bestimmt wird.

3.1. Der supersinguläre Fall

Für die Bewertungen der Koeffizienten von f gilt: Das Absolutglied $\mathfrak{p}$ hat Bewertung 1 und der Leitterm hat Bewertung 0. Die anderen Koeffizienten besitzen echt positive Bewertung. Das Newton-Polygon von f sieht daher wie folgt aus:



Die Nullstellen von f besitzen bezüglich eingangs definierter Bewertung v Bewertung $\frac{1}{q^{2d}-1}$. Darüber hinaus kann man ablesen, dass f über $K_\mathfrak{p}$ irreduzibel ist (siehe Bemerkung A.10).

3.8. Lemma. *Der Zerfällungskörper $K_\mathfrak{p}({}_\mathfrak{p}\Phi)$ enthält die $q^{2d}-1$-ten Einheitswurzeln.*

Beweis. Sei $0 \neq x \in {}_\mathfrak{p}\Phi$. Dann ist

$$[K_\mathfrak{p}(x) : K_\mathfrak{p}] = q^{2d} - 1,$$

da f über $K_\mathfrak{p}$ irreduzibel ist. Andererseits muss aus Bewertungsgründen aber für den Verzweigungsindex der Erweiterung $K_\mathfrak{p}(x)|K_\mathfrak{p}$

$$q^{2d} - 1 \mid e_{K_\mathfrak{p}(x)|K_\mathfrak{p}}$$

gelten. Somit ist $K_\mathfrak{p}(x)|K_\mathfrak{p}$ zahm und voll verzweigt. Nach Satz A.13 existiert eine Uniformisierende $\pi \in K_\mathfrak{p}$, so dass $K_\mathfrak{p}(x)$ von einer Nullstelle des Polynoms

$$X^{q^{2d}-1} - \pi$$

erzeugt wird. Also enthält die galoissche Hülle von $K_\mathfrak{p}(x)$ über $K_\mathfrak{p}$ die $q^{2d}-1$-ten Einheitswurzeln. Damit liegen diese auch in $K_\mathfrak{p}({}_\mathfrak{p}\Phi)$. □

Wir wissen also: Ist ω eine primitive $q^{2d}-1$-te Einheitswurzel, so ist die Körpererweiterung $K_\mathfrak{p}(\omega)|K_\mathfrak{p}$ enthalten in $K_\mathfrak{p}({}_\mathfrak{p}\Phi)$. Die Adjunktion der $q^{2d}-1$-ten Einheitswurzeln an $K_\mathfrak{p}$ entspricht einer quadratischen Erweiterung des Restkörpers $\mathbb{F}_\mathfrak{p}$, das heißt, $K_\mathfrak{p}(\omega)|K_\mathfrak{p}$ ist unverzweigt vom Grad 2.

3.9. Satz. *Sei x_1 eine Nullstelle von f, d.h. ein von Null verschiedener $\mathfrak{p}$-Torsionspunkt. Dann ist die voll verzweigte Erweiterung $K_\mathfrak{p}(\omega)(x_1)|K_\mathfrak{p}(\omega)$ eine Kummer-Erweiterung, also galoissch vom Grad $q^{2d}-1$ mit zyklischer Galois-Gruppe.*

Beweis. Da die Erweiterung $K_\mathfrak{p}(\omega)|K_\mathfrak{p}$ unverzweigt ist, besitzt das Newton-Polygon von f über $K_\mathfrak{p}(\omega)$ die gleiche Gestalt wie über $K_\mathfrak{p}$. Wie in Lemma 3.8 folgt damit, dass die Erweiterung $K_\mathfrak{p}(\omega)(x_1)|K_\mathfrak{p}(\omega)$ voll und zahm verzweigt vom Grad $q^{2d}-1$ ist. Es existiert also eine geeignete Uniformisierende $\pi' \in K_\mathfrak{p}(\omega)$, so dass eine Nullstelle des Polynoms $X^{q^{2d}-1} - \pi'$ die Erweiterung $K_\mathfrak{p}(\omega)(x_1)|K_\mathfrak{p}(\omega)$ erzeugt. Weiter ist

$$\pi' \neq u^m, \quad \text{für alle } u \in K_\mathfrak{p}(\omega), m \mid q^{2d}-1, m > 1,$$

da π' eine Uniformisierende von $K_\mathfrak{p}(\omega)$ ist. Andererseits enthält $K_\mathfrak{p}(\omega)$ nach Konstruktion die $q^{2d}-1$-ten Einheitswurzeln. Die Voraussetzungen von Satz A.16 sind damit erfüllt. Demzufolge ist die betrachtete Erweiterung eine Kummer-Erweiterung und besitzt eine zyklische Galois-Gruppe. □

3.10. Satz. *Es gilt*

$$K_\mathfrak{p}(\omega)(x_1) = K_\mathfrak{p}({}_\mathfrak{p}\Phi),$$

d.h. $\Phi_\mathfrak{p}$ zerfällt über $K_\mathfrak{p}(\omega, x_1)$ vollständig.

Beweis. Nach der Charakterisierung des supersingulären Falls gilt

$$\overline{\Phi}_\mathfrak{p} \equiv (-1)^d \tau^{2d} \mod \mathfrak{p}.$$

Mit der üblichen Bezeichnung für die Koeffizienten von $\Phi_\mathfrak{p}$ gilt also

$$v(a_i) \geq 1, \quad \text{für alle } 0 \leq i < 2d.$$

Das Absolutglied von $\Phi_\mathfrak{p}$ ist $\mathfrak{p}$ und hat damit Bewertung 1. Mit f bezeichnen wir weiterhin das Polynom $\dfrac{\Phi_\mathfrak{p}(X)}{X}$. Betrachte das Polynom

$$\varphi(X) := \frac{f(x_1X)}{x_1^{q^{2d}-1}} = (-1)^d X^{q^{2d}-1} + \sum_{1\le i<2d} \frac{a_i}{x_1^{q^{2d}-q^i}} X^{q^i-1} + \frac{\mathfrak{p}}{x_1^{q^{2d}-1}}.$$

Dann gilt für das Absolutglied φ_0 von $\varphi(X)$

$$v(\varphi_0) = v\left(\frac{\mathfrak{p}}{x_1^{q^{2d}-1}}\right) = 1 - (q^{2d}-1)v(x_1) = 0 \tag{3.4}$$

und für die weiteren Koeffizienten $\varphi_i := \dfrac{a_i}{x_1^{q^{2d}-q^i}}$ mit $1 \le i < 2d$

$$\begin{aligned} v(\varphi_i) = v\left(\frac{a_i}{x_1^{q^{2d}-q^i}}\right) &= v(a_i) - v\left(x_1^{q^{2d}-q^i}\right) \\ &\ge 1 - \frac{q^{2d}-q^i}{q^{2d}-1} > 0. \end{aligned}$$

Sei $\mathfrak{m} = (x_1)$ das maximale Ideal des Ganzheitsrings von $K_\mathfrak{p}(\omega)(x_1)$ und $\overline{\varphi}_0$ die Reduktion von φ_0 modulo $\mathfrak{m}$, dann gilt

$$\overline{\varphi}(X) \equiv (-1)^d X^{q^{2d}-1} + \overline{\varphi}_0 \mod \mathfrak{m}.$$

Wegen Gleichung (3.4) ist $\overline{\varphi}_0 \neq 0$ im Restkörper von $K_\mathfrak{p}(\omega)(x_1)$. Damit sind sowohl das Polynom $\varphi(X)$ als auch seine Reduktion modulo $\mathfrak{m}$ separabel. Nach Konstruktion hat $\varphi(X)$ die Eigenschaft

$$\varphi(1) = \frac{f(x_1)}{x_1^{q^{2d}-1}} = 0,$$

also besitzt auch $\overline{\varphi}(X)$ eine Nullstelle im Restkörper von $K_\mathfrak{p}(\omega)(x_1)$. Dieser ist wegen der vorgenommenen Restkörpererweiterung der Körper mit q^{2d} Elementen, enthält also die $q^{2d}-1$-ten Einheitswurzeln. Damit zerfällt $\overline{\varphi}(X)$ vollständig über dem Restkörper und nach dem trivialen Fall des Lemmas von Hensel (siehe Satz A.15) zerfällt auch $\varphi(X)$ über $K_\mathfrak{p}(\omega)(x_1)$.

Durch Rücktransformation folgt, dass auch alle Nullstellen von f bzw. $\Phi_\mathfrak{p}$ in $K_\mathfrak{p}(\omega)(x_1)$ liegen. Nach Konstruktion ist dies aber der kleinste Körper mit dieser Eigenschaft. Damit folgt die Behauptung. □

Wir erhalten für den Zerfällungskörper $K_\mathfrak{p}({}_\mathfrak{p}\Phi)$ von $\Phi_\mathfrak{p}$ über $K_\mathfrak{p}$ das Diagramm:

$$\begin{array}{c} K_\mathfrak{p}({}_\mathfrak{p}\Phi) = K_\mathfrak{p}(\omega, x_1) \\ | \\ K_\mathfrak{p}(\omega) \\ | \\ K_\mathfrak{p} \end{array}$$

3.11. Korollar. *Es gilt* $[K_\mathfrak{p}({}_\mathfrak{p}\Phi) : K_\mathfrak{p}] = 2(q^{2d}-1)$.

3.12. Bemerkung. Die lokale Galois-Gruppe $G_\mathfrak{p} = \mathrm{Gal}(K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p})$ besitzt $2(q^{2d}-1)$ Elemente. Es handelt sich bei $G_\mathfrak{p}$ um das semidirekte Produkt von $C_{q^{2d}-1}$ und C_2. Hierbei bezeichnet C_n die zyklische Gruppe mit n Elementen. Für eine Beschreibung der Gruppe $C_{q^{2d}-1}$, siehe Bemerkung A.23.

Die Gruppe C_2 operiert (anders als bei einer Diedergruppe) nicht durch Inversenbildung auf $C_{q^{2d}-1}$ sondern durch Erheben in die q^d-te Potenz. Dies entspricht dem Frobenius-Endomorphismus.

Die Gruppe $G_{\mathfrak{p}}$ ist der Normalisator einer nicht-zerfallenden Cartan-Gruppe.

3.13. Satz. *Für den lokalen Diskriminantenexponenten $D_{K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}}$ gilt*

$$D_{K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}} = 2(q^{2d}-2).$$

Beweis. Da die Erweiterung $K_{\mathfrak{p}}(\omega)|K_{\mathfrak{p}}$ unverzweigt ist, besitzt sie trivialen Diskriminantenexponenten. Die Erweiterung $K_{\mathfrak{p}}(\omega,x_1)|K_{\mathfrak{p}}(\omega)$ ist voll und zahm verzweigt. Wegen Bemerkung A.4 stimmen hier also Differentenexponent und Diskriminantenexponent überein und können mit Satz A.7 berechnet werden. Es gilt insgesamt:

$$D_{K_{\mathfrak{p}}(\omega)|K_{\mathfrak{p}}} = 0,$$
$$D_{K_{\mathfrak{p}}(\omega,x_1)|K_{\mathfrak{p}}(\omega)} = q^{2d}-2.$$

Durch Einsetzen dieser Diskriminantenexponenten in die Formel für die Diskriminante in Körpertürmen (siehe Lemma A.6) erhalten wir

$$D_{K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}} = [K_{\mathfrak{p}}(\omega,x_1):K_{\mathfrak{p}}(\omega)]D_{K_{\mathfrak{p}}(\omega)|K_{\mathfrak{p}}} + 2D_{K_{\mathfrak{p}}(\omega,x_1)|K_{\mathfrak{p}}(\omega)} = 2(q^{2d}-2).$$

Dabei haben wir verwendet, dass die unverzweigte Erweiterung $K_{\mathfrak{p}}(\omega)|K_{\mathfrak{p}}$ quadratisch ist, also Trägheitsindex 2 besitzt. □

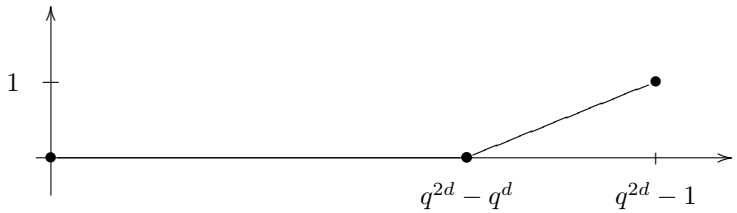
3.2. Der ordinäre Fall

In diesem Abschnitt sei $\mathfrak{p}$ eine ordinäre Stelle des Grades d. Wir fordern zusätzlich, dass $\mathfrak{p}$ die folgende Hypothese erfüllt:

Hypothese 1. Es existiert kein Torsionspunkt $0 \neq z \in {}_{\mathfrak{p}}\Phi$, der in einer unverzweigten Galois-Erweiterung von $K_{\mathfrak{p}}$ liegt.

3.14. Bemerkung. Eine Beschreibung der Stellen, für die bereits nachgewiesen werden konnte, dass sie die Hypothese erfüllen, ist in Abschnitt 3.3 angegeben.

Das Absolutglied von $f = \dfrac{\Phi_{\mathfrak{p}}(X)}{X}$ hat nach der Charakterisierung des ordinären Falls in (3.3) Bewertung 1, die Koeffizienten $a_1,\ldots,a_{d-1}$ von f besitzen echt positive Bewertung und a_d hat Bewertung 0. Da die übrigen Koeffizienten ganz sind, genügt dies, um das Newton-Polygon von f über $K_{\mathfrak{p}}$ zu bestimmen:



$\Phi_{\mathfrak{p}}$ besitzt somit q^d-1 Nullstellen mit Bewertung $\dfrac{1}{q^d-1} > 0$ und $q^{2d}-q^d$ Nullstellen mit Bewertung 0, zusätzlich zur einfachen Nullstelle 0. Die Nullstellen mit echt positiver Bewertung korrespondieren zu einem irreduziblen Teiler von f in $K_{\mathfrak{p}}[X]$.

Sei $x \in {}_{\mathfrak{p}}\Phi$ eine dieser Nullstellen mit echt positiver Bewertung. Wir wissen bereits, dass

$$\mathbb{F}_{\mathfrak{p}} * x \subset {}_{\mathfrak{p}}\Phi$$

gilt, wobei die Schreibweise „$*$“ verdeutlicht, dass es sich hierbei um die durch die Drinfeld-Modulstruktur induzierte nicht-triviale Multiplikation handelt.

Sei also $c \in \mathbb{F}_{\mathfrak{p}}^* = (A/\mathfrak{p})^*$ gegeben durch ein Element von A vom Grad $< d$. Für das Bild von c unter dem Drinfeld-Modul Φ gilt damit

$$\Phi_c = \sum_{i=0}^{2d-2} c_i \tau^i \quad \text{mit } c_i \in A.$$

Insbesondere ist $v(c_i) \geq 0$ für $i = 0, \ldots, 2d-2$. Nach Definition der nicht-trivialen Multiplikation ist

$$c * x = \Phi_c(x) = \sum_{i=0}^{2d-2} c_i x^{q^i}.$$

Daraus folgt

$$v(c * x) = v\left(\sum_{i=0}^{2d-2} c_i x^{q^i}\right) \geq \min_{i=0,\ldots,2d-2} \left\{ v(c_i x^{q^i}) \right\} \geq v(x) > 0.$$

Die Bewertung von x ist aber maximal unter den Nullstellen von f, somit gilt

$$v(c * x) = v(x).$$

Wir fassen dieses Resultat zusammen:

3.15. Lemma. *Die $q^d - 1$ Nullstellen mit Bewertung $\dfrac{1}{q^d - 1}$ bilden zusammen mit 0 einen eindimensionalen Galois-stabilen $\mathbb{F}_{\mathfrak{p}}$-Unterraum von ${}_{\mathfrak{p}}\Phi$.*

Das Polynom

$$\alpha(X) := \prod_{c \in \mathbb{F}_{\mathfrak{p}}} (X - c * x)$$

ist daher $\mathbb{F}_q$-additiv mit Koeffizienten in $K_{\mathfrak{p}}$ und liegt somit in $K_{\mathfrak{p}}[X]$. Da der Kern von $\alpha(X)$ ein eindimensionaler $\mathbb{F}_{\mathfrak{p}}$-Unterraum von ${}_{\mathfrak{p}}\Phi$ ist, ist $\alpha(X)$ auch in $K_{\mathfrak{p}}\{\tau\}$ ein rechter Teiler

$$\alpha = \tau^d + \sum_{i=0}^{d-1} \alpha_i \tau^i, \quad \alpha_i \in K_{\mathfrak{p}} \text{ für alle } i = 0, \ldots, d-1,$$

von $\Phi_{\mathfrak{p}}$. Es existiert also ein additives Polynom

$$\beta = (-1)^d \tau^d + \sum_{i=0}^{d-1} \beta_i \tau^i \in K_{\mathfrak{p}}\{\tau\}$$

mit der Eigenschaft

$$\Phi_{\mathfrak{p}} = \beta \circ \alpha.$$

Der Kern von β ist dann ebenfalls ein eindimensionaler $\mathbb{F}_{\mathfrak{p}}$-Vektorraum. Die Eigenschaften von α und β wollen wir in folgendem Lemma zusammenfassen.

3.16. Lemma. *Seien α und β definiert wie zuvor. Dann besitzen beide Polynome Koeffizienten in $\mathcal{O}_{K_{\mathfrak{p}}}$. Weiter gilt*

$$\overline{\alpha} \equiv \tau^d \mod \mathfrak{p}$$

und

$$\overline{\beta} \equiv (-1)^d \tau^d + \sum_{i=0}^{d-1} \overline{a}_{d+i} \tau^i \mod \mathfrak{p}.$$

BEWEIS. Die Nullstellen von α sind nach Voraussetzung Elemente des Ganzheitsrings $\mathcal{O}_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)}$. Damit liegen aber auch alle Koeffizienten von α im Ganzheitsring von $K_\mathfrak{p}$, da diese sich durch die Nullstellen ausdrücken lassen. Aus der Ganzheit der Koeffizienten von $\Phi_\mathfrak{p}$ folgt nun, dass auch $\beta \in \mathcal{O}_{K_\mathfrak{p}}\{\tau\}$ gilt.

Aus Bedingung (3.3) folgt die Kongruenz

$$\overline{\Phi}_\mathfrak{p} \equiv (-1)^d\tau^{2d} + \ldots + \overline{a}_d\tau^d \equiv \left((-1)^d\tau^d + \ldots + \overline{a}_d\right) \circ \tau^d \mod \mathfrak{p}$$

mit $\overline{a}_d \not\equiv 0 \bmod \mathfrak{p}$. Andererseits ist aber

$$v(\alpha_0) = v\left(\prod_{c\in\mathbb{F}_\mathfrak{p}^*} c * x\right) = \sum_{c\in\mathbb{F}_\mathfrak{p}^*} v(c*x) = 1.$$

Somit muss bereits

$$\overline{\alpha} \equiv \tau^d \mod \mathfrak{p}$$

und

$$\overline{\beta} \equiv (-1)^d\tau^d + \sum_{i=0}^{d-1} \overline{a}_{d+i}\tau^i \mod \mathfrak{p}$$

gelten. □

Mit der Eigenschaft $\overline{a}_d \not\equiv 0 \bmod \mathfrak{p}$ aus der Definition des ordinären Falls folgt direkt das

3.17. KOROLLAR. *Die Reduktion $\overline{\beta}(X)$ von $\beta(X)$ modulo $\mathfrak{p}$ ist über $\mathbb{F}_\mathfrak{p}[X]$ separabel und hat Grad q^d.*

Mithilfe von α und β können wir eine neue Beschreibung von ${}_\mathfrak{p}\Phi$ angeben, denn es gilt

$$\begin{aligned} {}_\mathfrak{p}\Phi &= \left\{z \in \overline{K}_\mathfrak{p} \mid \Phi_\mathfrak{p}(z) = (\beta\circ\alpha)(z) = 0\right\} \\ &= \left\{z \in \overline{K}_\mathfrak{p} \mid \alpha(z) \in \ker\beta\right\}. \end{aligned} \tag{3.5}$$

3.18. LEMMA. *Es gilt*

$$K_\mathfrak{p}(\ker\beta) \subset K_\mathfrak{p}({}_\mathfrak{p}\Phi).$$

BEWEIS. Betrachte ein Element $y \in {}_\mathfrak{p}\Phi \setminus \ker\alpha$, dann ist $(\beta\circ\alpha)(y) = 0$ und $\alpha(y) \neq 0$. Also gilt

$$\alpha(y) \in \ker\beta,$$

und als von Null verschiedenes Element erzeugt $\alpha(y)$ den Kern von β als eindimensionalen $\mathbb{F}_\mathfrak{p}$-Vektorraum. Da $\alpha(X)$ in $K_\mathfrak{p}[X]$ liegt, folgt andererseits

$$\alpha(y) \in K_\mathfrak{p}({}_\mathfrak{p}\Phi),$$

und damit ist $\ker\beta$ in $K_\mathfrak{p}({}_\mathfrak{p}\Phi)$ enthalten. □

Sei also $b \in \overline{K}_\mathfrak{p}$ mit $\mathbb{F}_\mathfrak{p} * b = \ker\beta$ und $u \in \overline{K}_\mathfrak{p}$ ein Element, das die Gleichung

$$\alpha(u) = b$$

erfüllt, so wird ${}_\mathfrak{p}\Phi$ als $\mathbb{F}_\mathfrak{p}$-Vektorraum von x und u erzeugt.

Wir betrachten nun zunächst die durch Adjunktion von $\ker\alpha$ bzw. $\ker\beta$ entstehenden Galois-Erweiterungen von $K_\mathfrak{p}$. Da es sich bei diesen Kernen um eindimensionale $\mathbb{F}_\mathfrak{p}$-Vektorräume handelt, genügt es, eine von Null verschiedene Nullstelle von α bzw. β zu adjungieren.

3.19. SATZ. *Die Erweiterung*

$$K_\mathfrak{p}(b) = K_\mathfrak{p}(\ker\beta)|K_\mathfrak{p}$$

ist unverzweigt.

BEWEIS. Nach Korollar 3.17 und dem Lemma von Hensel genügt es, eine geeignete Restkörpererweiterung vorzunehmen. □

Für eine genaue Bestimmung des Körpergrades dieser Erweiterung benötigen wir das Konzept der Euler-Charakteristik:

3.20. DEFINITION. Durch die folgenden Eigenschaften ist eine wohldefinierte Abbildung χ von der Menge der Isomorphieklassen endlich erzeugter Torsionsmoduln über einem Dedekindring A in die Menge der Ideale $\neq 0$ von A gegeben:

(1) Für einen endlich erzeugten Torsionsmodul M über A hängt $\chi(M)$ nur von der Isomorphieklasse von M ab.
(2) Für ein Primideal $\mathfrak{p}$ von A gilt $\chi(A/\mathfrak{p}) = \mathfrak{p}$.
(3) Die Abbildung χ ist multiplikativ in kurzen exakten Sequenzen. Das heißt, ist die Sequenz von endlich erzeugten A-Torsionsmoduln

$$0 \longrightarrow X \longrightarrow Y \longrightarrow Z \longrightarrow 0$$

exakt, so gilt

$$\chi(Y) = \chi(X)\chi(Z).$$

Das Ideal $\chi(M)$ heißt die **Euler-Charakteristik** des endlich erzeugten Torsionsmoduls M.

3.21. SATZ. *Sei a_d wie bisher der d-Koeffizient von $\Phi_\mathfrak{p}$ und* ord $\overline{a}_d$ *die multiplikative Ordnung von $\overline{a}_d$ in $\mathbb{F}_\mathfrak{p}^*$. Dann gilt*

$$[K_\mathfrak{p}(\ker \beta) : K_\mathfrak{p}] = \text{ord } \overline{a}_d.$$

BEWEIS. Da die betrachtete Erweiterung unverzweigt ist, genügt es, die Situation über dem Restkörper zu betrachten, d.h. den Grad $[\mathbb{F}_\mathfrak{p}(\ker \overline{\beta}) : \mathbb{F}_\mathfrak{p}]$ zu bestimmen.

Sei $\overline{\Phi}$ die Reduktion von Φ modulo $\mathfrak{p}$. Nach [**Gek08**, Theorem 1.8 und 2.11] existiert ein wohlbestimmtes Element $a \in A$ mit $\deg a \leq \frac{d}{2}$, so dass

$$P(X) = X^2 - aX + \mathfrak{p}$$

das charakteristische Polynom des Frobenius $F = F_\mathfrak{p} = \tau^d$ von $\overline{\Phi}$ ist. Das Element a heißt die Frobenius-Spur von $\overline{\Phi}$. Es gilt also

$$F^2 - \overline{\Phi}_a F + \overline{\Phi}_\mathfrak{p} = 0 \quad \text{in } \mathbb{F}_\mathfrak{p}\{\tau\}.$$

Nach Definition des ordinären Falls ist aber

$$\overline{\Phi}_\mathfrak{p} \equiv \overline{\beta} \circ \overline{\alpha} \equiv \overline{\beta} \circ \tau^d \equiv \overline{\beta} \circ F \mod \mathfrak{p}.$$

Zusammen ergibt dies

$$0 = F^2 - \overline{\Phi}_a F + \overline{\Phi}_\mathfrak{p} = (F - \overline{\Phi}_a + \overline{\beta})F,$$

woraus wegen der Nullteilerfreiheit von $\mathbb{F}_\mathfrak{p}\{\tau\}$ folgt, dass

$$F - \overline{\Phi}_a + \overline{\beta} = 0$$

ist. Koeffizientenvergleich liefert, dass a modulo $\mathfrak{p}$ kongruent ist zum Absolutglied von β. Nach Lemma 3.16 gilt daher

$$\overline{a} \equiv \overline{a}_d \mod \mathfrak{p}. \tag{3.6}$$

Wir bezeichnen mit $\chi(\mathbb{F}_\mathfrak{p}, \overline{\Phi})$ die Euler-Charakteristik des A-Moduls $(\mathbb{F}_\mathfrak{p}, \overline{\Phi})$, d.h. wir betrachten $\mathbb{F}_\mathfrak{p}$ bezüglich der durch $\overline{\Phi}$ induzierten A-Modulstruktur. Nach Definition ist die Euler-Charakteristik ein wohlbestimmtes Ideal von A, genauer gilt wegen [**Gek91**, Theorem 5.1]

$$\chi(\mathbb{F}_\mathfrak{p}, \overline{\Phi}) = (P(1)).$$

Die Z-Funktion (definiert in [**Gek91**, Definition 5.7]) von Φ lautet für den gegebenen Drinfeld-Modul

$$Z_\Phi(t) = \frac{1 - at + \mathfrak{p}t^2}{(1-t)(1-\mathfrak{p}t)}.$$

Wir betrachten die Potenzreihenentwicklung

$$\left(t\frac{d}{dt}\log\right) Z_\Phi(t) = t\frac{Z'_\Phi(t)}{Z_\Phi(t)} = \sum_{m\geq 1} z_m t^m \in A[[t]],$$

wobei $\frac{d}{dt}\log$ die logarithmische Ableitung bezeichnet. Wie in [**Gek91**, Korollar 5.9] gezeigt, gilt für die Erweiterung $\mathbb{F}_\mathfrak{p}^{(m)}$ des Grades m von $\mathbb{F}_\mathfrak{p}$

$$\chi(\mathbb{F}_\mathfrak{p}^{(m)}, \overline{\Phi}) = (z_m). \tag{3.7}$$

Betrachtung modulo $\mathfrak{p}$ liefert

$$t\frac{Z'_\Phi(t)}{Z_\Phi(t)} \equiv \sum_{m\geq 1} (1 - \overline{a}^m) t^m \in \mathbb{F}_\mathfrak{p}[[t]]. \tag{3.8}$$

Da $\overline{\Phi}_\mathfrak{p} \equiv \overline{\beta} \circ F \bmod \mathfrak{p}$ ist, stimmen die Nullstellenmengen von $\overline{\Phi}_\mathfrak{p}$ und $\overline{\beta}$ wegen der Injektivität von F überein. Wir erhalten also

$$\mathbb{F}_\mathfrak{p}(\ker\overline{\beta}) = \mathbb{F}_\mathfrak{p}({}_\mathfrak{p}\overline{\Phi}).$$

Es existiert eine eindeutige Zahl $m_0 \in \mathbb{N}$ mit

$$\mathbb{F}_\mathfrak{p}({}_\mathfrak{p}\overline{\Phi}) = \mathbb{F}_\mathfrak{p}^{(m_0)}.$$

Nach Konstruktion gilt

$${}_\mathfrak{p}\overline{\Phi} \subset \mathbb{F}_\mathfrak{p}({}_\mathfrak{p}\overline{\Phi})$$

und ${}_\mathfrak{p}\overline{\Phi}$ ist im ordinären Fall als A-Modul isomorph zu $A/\mathfrak{p}$. Nach Eigenschaft 2 der Euler-Charakteristik muss daher $\mathfrak{p}$ in $\chi(\mathbb{F}_\mathfrak{p}({}_\mathfrak{p}\overline{\Phi}), \overline{\Phi}) = \chi(\mathbb{F}_\mathfrak{p}^{(m_0)}, \overline{\Phi})$ enthalten sein. Wegen (3.7) ist m_0 also minimal mit der Eigenschaft

$$z_{m_0} \equiv 0 \mod \mathfrak{p}.$$

Aus der Kongruenz (3.8) folgt, dass m_0 die multiplikative Ordnung von $\overline{a}$ in $\mathbb{F}_\mathfrak{p}$ ist. Wegen der Beziehung (3.6) ist dies aber auch die multiplikative Ordnung des Absolutglieds von $\overline{\beta}$ bzw. des d-Koeffizienten von $\overline{\Phi}_\mathfrak{p}$. Damit ist die Behauptung gezeigt. □

3.22. Korollar. *Die Galois-Gruppe* $\mathrm{Gal}(K_\mathfrak{p}(\ker\beta)|K_\mathfrak{p})$ *ist isomorph zu einer Untergruppe von* $\mathbb{F}_\mathfrak{p}^*$.

Beweis. Die Gestalt der Galois-Gruppe erhält man mithilfe der Kummer-Theorie (siehe Satz A.16): Die Erweiterung $K_\mathfrak{p}(\ker\beta)|K_\mathfrak{p}$ ist unverzweigt vom Grad $n_\beta \mid q^d - 1$. Damit entsteht die Erweiterung durch Ziehen einer n_β-ten Wurzel aus einem geeigneten Element von $K_\mathfrak{p}$. Da $K_\mathfrak{p}$ primitive n_β-te Einheitswurzeln enthält, handelt es sich um eine Kummer-Erweiterung, die zyklisch der Ordnung n_β ist. □

3.23. Korollar. *Sei* $\deg\mathfrak{p} = 1$. *Dann ist die Erweiterung* $K_\mathfrak{p}(\ker\beta)|K_\mathfrak{p}$ *trivial.*

Beweis. Ist $\mathfrak{p} = T - c$ mit $c \in \mathbb{F}_q$, so gilt

$$\Phi_\mathfrak{p} = T - c + \tau - \tau^2.$$

Damit ist nach Satz 3.21

$$[K_\mathfrak{p}(\ker\beta) : K_\mathfrak{p}] = \mathrm{ord}\ \overline{a}_d = \mathrm{ord}\ 1 = 1.$$

□

3.24. Bemerkung. Um im Beweis von Satz 3.21 das charakteristische Polynom des Frobenius $F_\mathfrak{p}$ als $P(X) = X^2 - aX + \mathfrak{p}$ zu bestimmen, haben wir Gebrauch von der Gestalt des betrachteten Drinfeld-Moduls gemacht: Es liegt an der Wahl der Koeffizienten von Φ_T, dass wir gerade $\mathfrak{p}$ als Absolutglied erhalten (das negative Vorzeichen des Leitterms von Φ_T ist an dieser Stelle entscheidend).

Im Fall eines beliebigen Drinfeld-Moduls ist der Ausdruck im Absolutglied komplizierter.

Wir betrachten nun den Zerfällungskörper von α.

3.25. Satz. *Die Erweiterung*

$$K_\mathfrak{p}(x) = K_\mathfrak{p}(\ker \alpha)|K_\mathfrak{p}$$

ist voll verzweigt vom Grad $q^d - 1$. *Die Galois-Gruppe* $\mathrm{Gal}(K_\mathfrak{p}(x)|K_\mathfrak{p})$ *ist isomorph zu* $\mathbb{F}_\mathfrak{p}^*$.

Beweis. Nach Lemma 3.16 ist $v(\alpha_i) \geq v(\alpha_0) = 1$ für $i = 1, \ldots, d-1$. Das Polynom $\alpha(X) = X^{q^d} + \sum_{i=0}^{d-1} \alpha_i X^{q^i}$ erfüllt damit die Bedingungen des ersten Falls von Satz A.12, der als Verallgemeinerung des Eisensteinkriteriums die Aussage über Grad und Verzweigungsverhalten der betrachteten Erweiterung liefert.

Die Gestalt der Galois-Gruppe folgt aus der Definition von α. □

Aus den bisherigen Überlegungen folgt direkt das

3.26. Korollar. *Die Erweiterungen* $K_\mathfrak{p}(x)$ *und* $K_\mathfrak{p}(b)$ *sind über* $K_\mathfrak{p}$ *linear disjunkt.*

Allerdings ist das Kompositum dieser Körper noch nicht der Zerfällungskörper von $\Phi_\mathfrak{p}$ über $K_\mathfrak{p}$, wie der folgende Satz zeigt.

3.27. Satz. *Ist Hypothese 1 erfüllt, so existiert kein Torsionspunkt* $u \in {}_\mathfrak{p}\Phi$ *in* $K_\mathfrak{p}(b, x)$, *der nicht im Kern von* α *liegt.*

Beweis. Als Folge von Korollar 3.26 und Satz 3.25 ist die Galois-Gruppe

$$H := \mathrm{Gal}(K_\mathfrak{p}(b, x)|K_\mathfrak{p}(b))$$

isomorph zu $\mathrm{Gal}(K_\mathfrak{p}(x)|K_\mathfrak{p})$ und zyklisch der Ordnung $q^d - 1$. Sei σ ein Erzeuger von H, dann gilt $\sigma(z) = c * z$ für alle $z \in \ker \alpha$ und ein Element $c \in \mathbb{F}_\mathfrak{p}^*$ der Ordnung $q^d - 1$.

Annahme: Es existiert $u \in K_\mathfrak{p}(b, x)$ mit $\Phi_\mathfrak{p}(u) = 0$ und $\alpha(u) \neq 0$. Nach Hypothese 1 ist $u \notin K_\mathfrak{p}(b)$, d.h. $\sigma(u) \neq u$. Allerdings liegt $\alpha(u)$ im Kern von β und somit in $K_\mathfrak{p}(b)$. Da σ Elemente von $K_\mathfrak{p}(b)$ festhält, gilt

$$\alpha(u) = \sigma(\alpha(u)) = \alpha(\sigma(u)),$$

d.h. es ist

$$0 \neq \sigma(u) - u \in \ker \alpha.$$

Setzen wir $x' := \sigma(u) - u$, so lässt sich direkt nachrechnen, dass das Element $y := (c-1)^{-1} * x' \in \ker \alpha$ die Gleichung

$$\sigma(u) - u = \sigma(y) - y$$

erfüllt. Hierbei ist y wohldefiniert, da c nach Definition ungleich 1 ist. Wir erhalten durch Äquivalenzumformung

$$\begin{aligned} & \sigma(u) - u = \sigma(y) - y \\ \Leftrightarrow \quad & \sigma(u - y) = u - y \\ \Leftrightarrow \quad & \rho(u - y) = u - y \quad \text{für alle } \rho \in H \\ \Leftrightarrow \quad & u - y \in K_\mathfrak{p}(b). \end{aligned}$$

Nach Konstruktion ist $u - y$ ein Element von ${}_{\mathfrak{p}}\Phi$, liegt andererseits aber in der unverzweigten Erweiterung $K_{\mathfrak{p}}(b)$ von $K_{\mathfrak{p}}$ im Widerspruch zur Hypothese. □

Es muss somit noch eine weitere Körpererweiterung vorgenommen werden, um die Körpererweiterung $K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}$ zu erzeugen. Diese wird durch das folgende Lemma beschrieben.

3.28. Lemma. *Sei $u \in \overline{K}_{\mathfrak{p}}$ eine Lösung der Gleichung $\alpha(u) = b$. Dann ist die Körpererweiterung $K_{\mathfrak{p}}(x,u) = K_{\mathfrak{p}}(x,b)(u)$ von $K_{\mathfrak{p}}(x,b)$ der Zerfällungskörper von $\Phi_{\mathfrak{p}}$.*

Beweis. Dass tatsächlich

$$K_{\mathfrak{p}}(x,u) = K_{\mathfrak{p}}(x,b)(u)$$

gilt, folgt direkt aus der Definition von u. Nach Konstruktion ist in jedem Fall

$$K_{\mathfrak{p}}(x,u) \subset K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi).$$

Da mit einer Lösung von

$$\alpha(u) = b$$

auch alle weiteren Lösungen in $K_{\mathfrak{p}}(x,u)$ liegen (weil $\ker\alpha$ in $K_{\mathfrak{p}}(x,u)$ enthalten ist), folgt mit der in (3.5) angegebenen Beschreibung der $\mathfrak{p}$-Torsion die Behauptung. □

3.29. Satz. *In der Situation von Lemma 3.28 gilt: Die Erweiterung $K_{\mathfrak{p}}(x,u)$ von $K_{\mathfrak{p}}(x,b)$ ist voll verzweigt vom Grad q^d.*

Die Galois-Gruppe $\mathrm{Gal}(K_{\mathfrak{p}}(x,u)|K_{\mathfrak{p}}(x,b))$ *ist isomorph zu $\mathbb{F}_{\mathfrak{p}}$. Für den lokalen Differentenexponenten gilt*

$$d(K_{\mathfrak{p}}(x,u)|K_{\mathfrak{p}}(x,b)) = 2(q^d - 1).$$

Beweis. Da die Erweiterung $K_{\mathfrak{p}}(b)|K_{\mathfrak{p}}$ unverzweigt ist, bezeichnen wir das maximale Ideal von $K_{\mathfrak{p}}(b)$ ebenfalls mit $\mathfrak{p}$. Das maximale Ideal von $K_{\mathfrak{p}}(x,b)$ nennen wir $\mathfrak{P}$.

Wir finden $u_0 \in \mathcal{O}_{K_{\mathfrak{p}}(b)}$ mit $\alpha(u_0) \equiv b \bmod \mathfrak{p}$. Ist nämlich $n_\beta := [K_{\mathfrak{p}}(b) : K_{\mathfrak{p}}]$, so ist nach Satz 3.19

$$\#\left(\mathcal{O}_{K_{\mathfrak{p}}(b)}/\mathfrak{p}\right) = (\#\mathbb{F}_{\mathfrak{p}})^{n_\beta} = q^{dn_\beta}.$$

Zusammen mit der Kongruenz

$$\alpha(X) \equiv X^{q^d} \mod \mathfrak{p}$$

folgt, dass das Element

$$u_0 = b^{q^{d(n_\beta - 1)}}$$

das Gewünschte leistet. Es gilt also

$$b' := \alpha(u_0) - b \in \mathfrak{p},$$

d.h.

$$v(b') \geq 1.$$

Als Element der unverzweigten Erweiterung $K_{\mathfrak{p}}(b)$ von $K_{\mathfrak{p}}$ besitzt b' ganzzahlige Bewertung bezüglich v.

Da α ein additives Polynom ist, erhalten wir die gleiche Körpererweiterung, wenn wir in der Gleichung

$$\alpha(u) = b$$

die rechte Seite um ein Element des Bildes $\alpha\left(K_{\mathfrak{p}}(x,b)\right)$ abändern.

Somit ist $K_{\mathfrak{p}}(x,b)(u) = K_{\mathfrak{p}}(x,b)(u')$, wenn u' eine Lösung von

$$\alpha(u') = b' \tag{3.9}$$

ist. Zusätzlich nehmen wir nun eine Renormierung von α vor. Wir setzen

$$\widetilde{\alpha}(X) := \frac{\alpha(xX)}{x^{q^d}} = X^{q^d} + \sum_{i=0}^{d-1} \widetilde{\alpha}_i X^{q^i}.$$

Da α über $K_{\mathfrak{p}}(x,b)$ zerfällt, gilt dies auch für $\widetilde{\alpha}$. Die Koeffizienten von $\widetilde{\alpha}$ sind von der Form

$$\widetilde{\alpha}_i = \frac{\alpha_i}{x^{q^d-q^i}} \quad \text{für} \quad 0 \leq i \leq d-1$$

und besitzen daher nach Lemma 3.16 nicht-negative Bewertung. Insbesondere ist

$$v(\widetilde{\alpha}_0) = v(\alpha_0) - (q^d-1)v(x) = 0,$$

d.h. die Reduktion von $\widetilde{\alpha}$ modulo $\mathfrak{P}$ ist separabel und zerfällt über dem Restkörper von $K_{\mathfrak{p}}(x,b)$.

Eine Lösung u' von (3.9) erzeugt die gleiche Körpererweiterung wie eine Nullstelle $\widetilde{u}'$ von

$$\widetilde{\alpha}\,(X) - \widetilde{b}'$$

mit $\widetilde{u}' = \dfrac{u'}{x}$ und $\widetilde{b}' = \dfrac{b'}{x^{q^d}}$.

Wir bezeichnen mit w die auf $K_{\mathfrak{p}}(x,b)$ normierte diskrete Bewertung, d.h. für $y \in K_{\mathfrak{p}}(x,b)$ gilt

$$w(y) = (q^d-1)v(y).$$

Annahme: Es gilt $v(b') > 1$. Dann ist

$$\begin{aligned} w\left(\widetilde{b'}\right) = w\left(\frac{b'}{x^{q^d}}\right) &= (q^d-1)v(b') - q^d w(x) \\ &\geq 2(q^d-1) - q^d > 0. \end{aligned}$$

Betrachten wir also die Reduktion des Polynoms $\widetilde{\alpha}\,(X) - \widetilde{b}'$ modulo $\mathfrak{P}$, so ist diese kongruent zu $\widetilde{\alpha}$ modulo $\mathfrak{P}$ und zerfällt damit über dem Restkörper von $K_{\mathfrak{p}}(x,b)$. Mithilfe des trivialen Falls des Lemmas von Hensel folgt, dass das Polynom $\widetilde{\alpha}\,(X) - \widetilde{b}'$ eine Nullstelle in $K_{\mathfrak{p}}(x,b)$ besitzt. Das bedeutet, dass die gesuchte Körpererweiterung $K_{\mathfrak{p}}(x,b)(u)$ von $K_{\mathfrak{p}}(x,b)$ trivial ist, im Widerspruch zu Satz 3.27.

Also ist $v(b') = 1$. Dann gilt

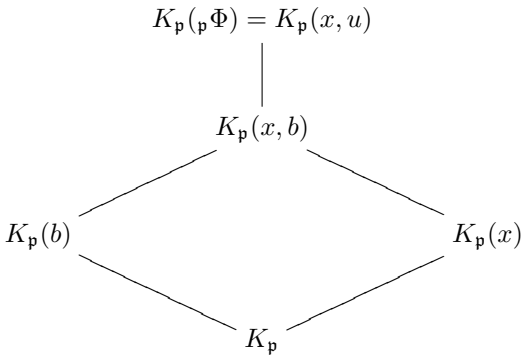
$$w\left(\widetilde{b'}\right) = w\left(\frac{b'}{x^{q^d}}\right) = (q^d-1)v(b') - q^d w(x) = q^d - 1 - q^d = -1.$$

Damit genügt das Polynom

$$\widetilde{\alpha}(X) - \widetilde{b'}$$

den Bedingungen von Satz A.21, der die Erweiterung beschreibt, die von einer Nullstelle eines solchen Polynoms erzeugt wird. Bei der Bestimmung der Galois-Gruppe nutzen wir aus, dass die additive Gruppe von $\mathbb{F}_{\mathfrak{p}}$ isomorph ist zu $\ker \alpha$. $\square$

Die Körpererweiterung $K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}$ besitzt damit die Gestalt:



Aus den bisherigen Überlegungen erhalten wir folgende Resultate:

3.30. Korollar. *Sei $n_\beta = [K_\mathfrak{p}(b) : K_\mathfrak{p}]$. Es gilt*

$$[K_\mathfrak{p}({}_\mathfrak{p}\Phi) : K_\mathfrak{p}] = n_\beta(q^d - 1)q^d.$$

3.31. Korollar. *Fixiere die $\mathbb{F}_\mathfrak{p}$-Basis $\{x, u\}$ von ${}_\mathfrak{p}\Phi$. Die lokale Galois-Gruppe*

$$G_\mathfrak{p} = \mathrm{Gal}(K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p})$$

lässt sich bezüglich dieser Basis in der Form

$$G_\mathfrak{p} = \left\{ \begin{pmatrix} a & b \\ 0 & c \end{pmatrix} \middle| a \in \mathbb{F}_\mathfrak{p}^*, b \in \mathbb{F}_\mathfrak{p}, c \in G_u \right\} \subset \mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$$

darstellen, wobei $G_u \subset \mathbb{F}_\mathfrak{p}^*$ isomorph zur Galois-Gruppe der unverzweigten Erweiterung $K_\mathfrak{p}(b)|K_\mathfrak{p}$ ist.

Des Weiteren können wir nun den lokalen Diskriminantenexponenten berechnen.

3.32. Satz. *Sei $n_\beta = [K_\mathfrak{p}(b) : K_\mathfrak{p}] = [K_\mathfrak{p}(x,b) : K_\mathfrak{p}(x)]$. Für den lokalen Diskriminantenexponenten $D_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}}$ gilt*

$$D_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}} = n_\beta(q^{2d} - 2).$$

Beweis. Wir verwenden die Formel aus Lemma A.6 um aus den Diskriminantenexponenten der Teilerweiterungen den gesamten Diskriminantenexponenten zu berechnen. Im Einzelnen gilt:

Nach Satz 3.29 gilt in der wild verzweigten Erweiterung $K_\mathfrak{p}(x,u)|K_\mathfrak{p}(x,b)$ für den lokalen Differentenexponenten

$$d(K_\mathfrak{p}(x,u)|K_\mathfrak{p}(x,b)) = 2(q^d - 1).$$

Weiter liefert Satz A.7 für den Differentenexponenten der voll und zahm verzweigten Erweiterung $K_\mathfrak{p}(x)|K_\mathfrak{p}$

$$d(K_\mathfrak{p}(x)|K_\mathfrak{p}) = q^d - 2.$$

Da beide Teilerweiterungen voll verzweigt sind, folgt mit Bemerkung A.4, dass die Differentenexponenten mit den Diskriminantenexponenten der jeweiligen Erweiterungen übereinstimmen.

In der unverzweigten Erweiterung $K_\mathfrak{p}(x,b)|K_\mathfrak{p}(x)$ gilt

$$D_{K_\mathfrak{p}(x,b)|K_\mathfrak{p}(x)} = 0.$$

Wir wenden nun zweimal Lemma A.6 an. Im ersten Schritt erhalten wir zunächst

$$\begin{aligned} D_{K_\mathfrak{p}(x,u)|K_\mathfrak{p}(x)} &= [K_\mathfrak{p}(x,u) : K_\mathfrak{p}(x,b)] D_{K_\mathfrak{p}(x,b)|K_\mathfrak{p}(x)} + n_\beta D_{K_\mathfrak{p}(x,u)|K_\mathfrak{p}(x,b)} \\ &= 2n_\beta(q^d - 1), \end{aligned}$$

da n_β nach Definition der Trägheitsindex der Erweiterung $K_\mathfrak{p}(x,b)|K_\mathfrak{p}(x)$ ist. Damit können wir im zweiten Schritt den lokalen Diskriminantenexponenten von $K_\mathfrak{p}(x,u)|K_\mathfrak{p}$ berechnen. Es gilt

$$D_{K_\mathfrak{p}(x,u)|K_\mathfrak{p}} = [K_\mathfrak{p}(x,u) : K_\mathfrak{p}(x)]D_{K_\mathfrak{p}(x)|K_\mathfrak{p}} + D_{K_\mathfrak{p}(x,u)|K_\mathfrak{p}(x)},$$

wobei wir ausgenutzt haben, dass die Erweiterung $K_\mathfrak{p}(x)|K_\mathfrak{p}$ voll verzweigt ist, und damit Trägheitsindex 1 besitzt. Insgesamt ist also

$$D_{K_\mathfrak{p}(x,u)|K_\mathfrak{p}} = n_\beta q^d(q^d-2) + 2n_\beta(q^d-1) = n_\beta(q^2d-2).$$

□

3.3. Die Hypothese im ordinären Fall

In diesem Abschnitt wollen wir auf die zuvor im ordinären Fall formulierte Hypothese 1 zurückkommen. Wir beweisen, dass die Hypothese für alle Stellen des Grades 1 und 2 erfüllt ist.

3.33. Bemerkung. Weiter hat die Untersuchung sämtlicher normierter Primpolynome vom Grad 3 über endlichen Körpern $\mathbb{F}_q$, wobei $q \leq 32$ und char $\mathbb{F}_q \neq 3$ ist, keine Beispiele für ordinäre Stellen geliefert, an denen die Hypothese verletzt ist.

Ob es tatsächlich endliche Stellen gibt, die die Hypothese nicht erfüllen, ist offen.

3.34. Bemerkung. Es sei darauf hingewiesen, dass wir nur in Satz 3.27 direkten Gebrauch von der Hypothese gemacht haben. Wir können daher auch im Fall, dass eine ordinäre Stelle die Hypothese nicht erfüllt, Resultate formulieren, die von diesem Satz unabhängig sind.

Für den Beweis in den bisher gelösten Fällen verwenden wir folgendes

3.35. Lemma. *Die Hypothese ist für eine endliche Stelle $\mathfrak{p}$ von K erfüllt, wenn das additive Polynom $\Phi_\mathfrak{p}$ keine Zerlegung der Form*

$$\Phi_\mathfrak{p} = \delta \circ \gamma$$

mit additiven Polynomen $\gamma, \delta \in \mathcal{O}_{K_\mathfrak{p}}\{\tau\}$ besitzt, die die Eigenschaften

$$\delta \equiv (-1)^d \tau^d \mod \mathfrak{p}$$

bzw.

die Reduktion von γ modulo $\mathfrak{p}$ ist separabel

erfüllen.

Beweis. Wir zeigen die Kontraposition der Aussage. Sei also $z \in {}_\mathfrak{p}\Phi$ enthalten in einer unverzweigten Galois-Erweiterung L von $K_\mathfrak{p}$. Nach Lemma 3.15 kann z keine der Nullstellen mit echt positiver Bewertung sein, also hat z Bewertung 0 in $K_\mathfrak{p}({}_\mathfrak{p}\Phi)$. Mit z liegen auch alle $\mathbb{F}_\mathfrak{p}$-Vielfachen von z in L. Andererseits kann kein Torsionspunkt $z' \in {}_\mathfrak{p}\Phi$ in L enthalten sein, der $\mathbb{F}_\mathfrak{p}$-linear unabhängig von z ist, da sonst $\{z, z'\} \subset L$ eine Basis von ${}_\mathfrak{p}\Phi$ wäre. Dann aber ließe sich x in dieser Basis darstellen und L enthielte eine voll verzweigte Körpererweiterung von $K_\mathfrak{p}$.

Die Elemente von $\mathbb{F}_\mathfrak{p} * z$ werden somit unter der Galois-Gruppe von $K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}$ aufeinander abgebildet, d.h.

$$\gamma(X) := \prod_{c \in \mathbb{F}_\mathfrak{p}} (X - c * z)$$

liegt bereits in $K_\mathfrak{p}[X]$ und wegen der Ganzheit der Nullstellen sogar in $\mathcal{O}_{K_\mathfrak{p}}[X]$. Da $\ker\gamma$ ein $\mathbb{F}_\mathfrak{p}$-Unterraum von ${}_\mathfrak{p}\Phi$ ist, ist

$$\gamma(X) = X^{q^d} + \sum_{i=0}^{d-1} \gamma_i X^{q^i} \in \mathcal{O}_{K_\mathfrak{p}}\{\tau\}$$

ein rechter Teiler von $\Phi_\mathfrak{p}$, d.h. wir erhalten die Faktorisierung $\Phi_\mathfrak{p} = \delta \circ \gamma$ mit einem additiven Polynom $\delta \in \mathcal{O}_{K_\mathfrak{p}}\{\tau\}$. Weiter gilt

$$v(\gamma_0) = v\left(\prod_{c\in\mathbb{F}_\mathfrak{p}^*} (c * z)\right) = 0.$$

Damit erfüllt γ die verlangten Bedingungen. Die Eigenschaften von δ folgen wie in Lemma 3.16 aus der Charakterisierung von $\overline{\Phi}_\mathfrak{p}$ im ordinären Fall. □

3.36. Satz. *Sei $\mathfrak{p} \in A$ ein normiertes Primpolynom des Grades 1. Dann erfüllt die Stelle $\mathfrak{p}$ Hypothese 1.*

Beweis. Es genügt, den Fall $\mathfrak{p} = T$ zu betrachten. Die Aussage für allgemeine Stellen $\mathfrak{p} = T - c$, $c \in \mathbb{F}_q$, folgt durch Koordinatentransformation.

Annahme: Es existieren $\gamma_0 \in \mathcal{O}_{K_\mathfrak{p}}^*$ und $\delta_0 \in \mathfrak{p}$ mit

$$\Phi_T = (-\tau + \delta_0)(\tau + \gamma_0).$$

Durch Koeffizientenvergleich folgt

$$\gamma_0\delta_0 = T \tag{3.10}$$

und

$$\delta_0 - {\gamma_0}^q = 1. \tag{3.11}$$

Umstellen von (3.11) liefert, dass

$$\delta_0 = (1 + {\gamma_0}^q) = (1 + \gamma_0)^q$$

eine q-te Potenz in $\mathcal{O}_{K_\mathfrak{p}}$ ist. Andererseits ist nach (3.10)

$$\delta_0 = {\gamma_0}^{-1} T$$

eine Uniformisierende von $\mathfrak{p}$. Dies ist ein Widerspruch. Mit Lemma 3.35 folgt die Behauptung. □

3.37. Satz. *Sei $\mathfrak{p} = T^2 + uT + v \in A$ eine ordinäre Stelle des Grades 2, $u, v \in \mathbb{F}_q$. Dann ist Hypothese 1 für $\mathfrak{p}$ erfüllt.*

Beweis. Annahme: Es existieren additive Polynome $\gamma = \tau^2 + \gamma_1\tau + \gamma_0$ und $\delta = \tau^2 + \delta_1\tau + \delta_0$ in $\mathcal{O}_{K_\mathfrak{p}}\{\tau\}$ mit den Eigenschaften

$$\Phi_\mathfrak{p} = \delta \circ \gamma$$

und

$$\delta_0 \equiv \delta_1 \equiv 0 \mod \mathfrak{p}$$

bzw.

$$\gamma_0 \in \mathcal{O}_{K_\mathfrak{p}}^*.$$

Koeffizientenvergleich liefert die Bedingungen

$$\mathfrak{p} = \delta_0\gamma_0 \tag{3.12}$$

$$u + T + T^q = \delta_1{\gamma_0}^q + \delta_0\gamma_1 \tag{3.13}$$

$$1 - u - T - T^{q^2} = {\gamma_0}^{q^2} + \delta_1{\gamma_1}^q + \delta_0 \tag{3.14}$$

$$-2 = {\gamma_1}^{q^2} + \delta_1. \tag{3.15}$$

Aus Gleichung (3.12) folgt, dass δ_0 eine Uniformisierende von $\mathfrak{p}$ ist. Gleichung (3.15) liefert, dass δ_1 eine q-te Potenz ist. Zusammen mit (3.13) und (3.14) ergibt sich, dass $\delta_0 + \delta_0\gamma_1 = \delta_0(1+\gamma_1)$ eine q-te Potenz ist. Da $\#\left(\mathcal{O}_{\kappa_\mathfrak{p}}/\mathfrak{p}\right) = q^2$ gilt, ist nach Gleichung (3.15) aber

$$\gamma_1 \equiv {\gamma_1}^{q^2} \equiv -2 \mod \mathfrak{p},$$

so dass $1+\gamma_1$ eine Einheit in $\mathcal{O}_{K_\mathfrak{p}}$ ist. Also ist auch $\delta_0(1+\gamma_1)$ eine Uniformisierende, im Widerspruch dazu, dass es sich bei diesem Element um eine q-te Potenz handeln soll. Mit Lemma 3.35 folgt die Behauptung. □

KAPITEL 4

Die unendliche Stelle ∞

In diesem Kapitel betrachten wir die lokale Körpererweiterung $K_\infty({}_\mathfrak{p}\Phi)|K_\infty$ mit Galois-Gruppe

$$G_\infty := \mathrm{Gal}(K_\infty({}_\mathfrak{p}\Phi)|K_\infty).$$

Wie in Kapitel 3 für die lokale Galois-Gruppe an der endlichen Stelle beschrieben, lässt sich auch G_∞ nach $G = \mathrm{Gal}(K({}_\mathfrak{p}\Phi)|K)$ einbetten.

Das Element T^{-1} ist eine Uniformisierende von K_∞, wir erhalten also die Darstellung $K_\infty = \mathbb{F}_q((T^{-1}))$. Der Restkörper von K_∞ ist $\mathbb{F}_q$.

Wir bezeichnen mit v die normierte diskrete Bewertung auf K_∞ und mit $|\cdot|$ den zugehörigen Absolutbetrag. Wie in Kapitel 3 normieren wir die Fortsetzungen von v so, dass wir auf dem algebraischen Abschluss $\overline{K}_\infty$ eine eindeutige (wieder mit v bezeichnete) Bewertung mit Bild $\mathbb{Q} \cup \{\infty\}$ erhalten, bezüglich der eine Uniformisierende von K_∞ Bewertung 1 hat.

Unsere Vorgehensweise an der unendlichen Stelle unterscheidet sich wesentlich von der an der endlichen Stelle $\mathfrak{p}$. Durch Betrachtung der analytischen Eigenschaften des gegebenen Drinfeld-Moduls gelingt es uns, zu zeigen, dass das lokale Verhalten an ∞ nicht von der Wahl von $\mathfrak{p}$ abhängt.

4.1. Analytische Vorüberlegungen

Sei $\mathcal{C}$ die in Abschnitt 1.2 eingeführte Komplettierung von $\overline{K}_\infty$. Sei Λ das durch unseren Drinfeld-Modul Φ definierte Gitter in $\mathcal{C}$ und e_Λ die zugehörige Exponentialfunktion. Es gilt

$$e_\Lambda(X) = \sum_{i \geq 0} \alpha_i X^{q^i} \in K_\infty[[X]].$$

Dies folgt direkt aus den Berechnungsvorschriften für e_Λ in Bemerkung 1.15 unter Verwendung der Tatsache, dass die Koeffizienten von Φ_T bereits über K definiert sind.

Wir wollen das Newton-Polygon zu e_Λ konstruieren, um eine genauere Beschreibung der Nullstellenmenge Λ zu erhalten. Wir benötigen dazu Aussagen über die Bewertungen der Koeffizienten der Exponentialfunktion. Diese liefert das folgende

4.1. Lemma. *Für die Bewertungen der Koeffizienten α_k von e_Λ gilt*

$$v(\alpha_k) \begin{cases} = \frac{k}{2} q^k & \text{für } k \text{ gerade,} \\ = q & \text{für } k = 1, \\ \geq \frac{k+1}{2} q^k & \text{für } k > 1 \text{ ungerade.} \end{cases}$$

Beweis. Für $k = 0$ und $k = 1$ rechnet man die Behauptung direkt nach: Nach Bemerkung 1.15 ist $\alpha_0 = 1$ und $\alpha_1 = (T^q - T)^{-1}$, d.h. $v(\alpha_0) = 0$ und $v(\alpha_1) = q$.

Für $k \geq 2$ existiert die Formel

$$\alpha_k = (T^{q^k} - T)^{-1}(\alpha_{k-1}^q - \alpha_{k-2}^{q^2}),$$

die man ebenfalls aus Bemerkung 1.15 erhält, indem man dort $a = T$ wählt und die Koeffizienten des gegebenen Drinfeld-Moduls einsetzt. Da T^{-1} eine Uniformisierende von K_∞ ist, gilt

$$v\left((T^{q^k} - T)^{-1}\right) = q^k.$$

Wir zeigen nun die Aussage für $k \geq 2$ durch Induktion.
Induktionsanfang: $k = 2$. Es ist

$$\alpha_2 = (T^{q^2} - T)^{-1}(\alpha_1^q - 1),$$

d.h.

$$v(\alpha_2) = q^2.$$

$k = 3$. Dann ist

$$\alpha_3 = (T^{q^3} - T)^{-1}(\alpha_2^q - \alpha_1^{q^2})$$

und damit folgt

$$v(\alpha_3) \geq q^3 + \min\{q^3, q^3\} = 2q^3.$$

Induktionsvoraussetzung: Sei die Behauptung gezeigt für k und $k-1$ mit $k-1 \geq 2$.
Induktionsschritt: $k-1, k \to k+1$.

Erster Fall: k ist gerade. Es ist nach Induktionsvoraussetzung

$$v(\alpha_k) = \frac{k}{2}q^k \quad \text{und} \quad v(\alpha_{k-1}) \geq \frac{k}{2}q^{k-1}.$$

Also gilt

$$v(\alpha_k^q) = \frac{k}{2}q^{k+1} \quad \text{bzw.} \quad v(\alpha_{k-1}^{q^2}) \geq \frac{k}{2}q^{k+1},$$

woraus mittels der rekursiven Formel folgt

$$v(\alpha_{k+1}) \geq q^{k+1} + \frac{k}{2}q^{k+1} = \frac{(k+1)+1}{2}q^{k+1}.$$

Dies zeigt den ersten Fall.

Zweiter Fall: k ist ungerade. Nach Induktionsvoraussetzung ist dann

$$v(\alpha_k) \geq \frac{k+1}{2}q^k \quad \text{und} \quad v(\alpha_{k-1}) = \frac{k-1}{2}q^{k-1}.$$

Damit gilt

$$v(\alpha_k^q) \geq \frac{k+1}{2}q^{k+1} \quad \text{bzw.} \quad v(\alpha_{k-1}^{q^2}) = \frac{k-1}{2}q^{k+1}.$$

Die rekursive Formel liefert in diesem Fall

$$v(\alpha_{k+1}) = q^{k+1} + \frac{k-1}{2}q^{k+1} = \frac{k+1}{2}q^{k+1}$$

und die Behauptung ist auch im zweiten Fall bewiesen. □

4.2. Bemerkung. Beachte im Folgenden, dass dem Newton-Polygon für Potenzreihen gemäß Bemerkung A.11 eine andere Normierung zugrunde liegt als im Polynomfall: Die Bewertungen der Koeffizienten werden von links nach rechts in aufsteigender Ordnung eingetragen, beginnend beim Absolutglied der Potenzreihe. Als Konsequenz daraus entspricht die Bewertung der Nullstellen auf einem Geradenstück nicht der Steigung des Geradenstücks sondern dem Negativen der Steigung.

Wir können nun zeigen, dass das Gitter in der gegebenen Situation über die folgende Eigenschaft verfügt, die Rechnungen im Gitter vereinfacht:

4.3. Satz. *Es existiert eine A-Basis $\{\omega_1, \omega_2\} \subset \mathcal{C}$ von Λ, d.h. $\Lambda = A\omega_1 \oplus A\omega_2$, mit der Eigenschaft*

$$|\omega_1| = |\omega_2| \quad \textit{ist minimal in } \Lambda.$$

BEWEIS. Der Beweis erfolgt über das Newton-Polygon von e_Λ. Wir zeigen, dass die in Lemma 4.1 bewiesenen Eigenschaften der Bewertungen der Koeffizienten von e_Λ ausreichen, um das Newton-Polygon zu bestimmen.

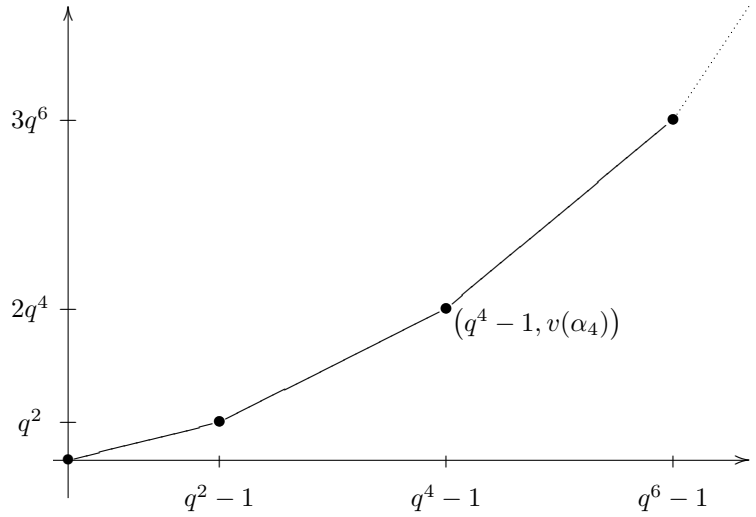
Zunächst bilden wir die konvexe Hülle zu den Koeffizienten mit geradem Index, an denen wir die exakte Bewertung kennen, d.h. wir verwenden die Stützstellen

$$(q^{2k}-1, v(\alpha_{2k})) = (q^{2k}-1, kq^{2k}) \quad \text{mit } k \geq 0.$$

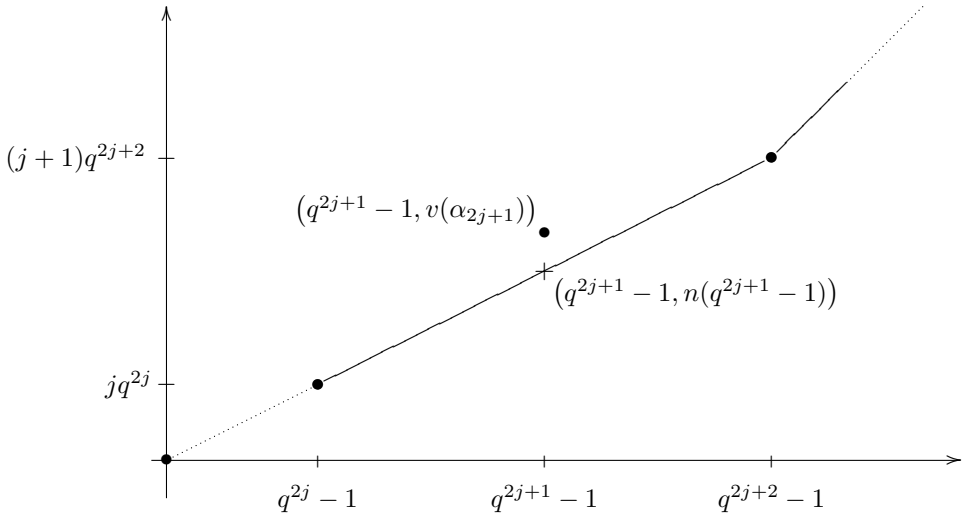
Bezeichnen wir die Steigung der Verbindungsstrecke der Stützstellen im Intervall $[q^{2k}-1, q^{2k+2}-1]$ mit m_k, so ist

$$m_k = \frac{(k+1)q^{2k+2} - kq^{2k}}{q^{2k+2}-1-(q^{2k}-1)} = k + \frac{q^2}{q^2-1}.$$

Es gilt also $m_0 < m_1 < m_2 < \ldots$ und damit erzeugen die Verbindungsstrecken der Stützstellen die konvexe Hülle bezüglich der geraden Indizes.



Wir betrachten nun den Wert der durch diesen Polygonzug gegebenen Funktion n in $q^{2j+1}-1$ mit $j \in \mathbb{N}_0$. Ist dieser Wert kleiner als die untere Schranke für $v(\alpha_{2j+1})$, so ist die im ersten Schritt berechnete konvexe Hülle tatsächlich das Newton-Polygon von e_Λ.



Die Funktion n hat in $q^{2j+1}-1$ nach Definition Steigung m_j. Daraus folgt

$$n\left(q^{2j+1}-1\right) = jq^{2j} + m_j\left(q^{2j+1}-q^{2j}\right) = jq^{2j} + \left(j+\frac{q^2}{q^2-1}\right)\left(q^{2j+1}-q^{2j}\right).$$

Da $q>1$ ist, gilt folgende Rechnung

$$\begin{aligned}
& q^2-q < q^2-1 \\
\Leftrightarrow \quad & \left(q^2-q\right)q^{2j+1} < \left(q^2-1\right)q^{2j+1} \\
\Leftrightarrow \quad & \frac{1}{q^2-1}\left(q^{2j+3}-q^{2j+2}\right) < q^{2j+1} \\
\Leftrightarrow \quad & jq^{2j+1} + \frac{q^2}{q^2-1}\left(q^{2j+1}-q^{2j}\right) < (j+1)q^{2j+1} \\
\Leftrightarrow \quad & jq^{2j} + \left(j+\frac{q^2}{q^2-1}\right)\left(q^{2j+1}-q^{2j}\right) < (j+1)q^{2j+1} \\
\Leftrightarrow \quad & n\left(q^{2j+1}-1\right) < (j+1)q^{2j+1} \le v(\alpha_{2j+1}).
\end{aligned}$$

Die Gitterpunkte mit den kleinsten Absolutbeträgen entsprechen den Nullstellen von e_Λ, die zum ersten Teilstück des Newton-Polygons gehören, da dieses die geringste Steigung hat. Dieses Teilstück hat die horizontale Länge q^2-1. Da in $A\setminus\{0\}$ aber nur die $q-1$ Elemente von $\mathbb{F}_q^*$ Betrag kleiner oder gleich 1 besitzen, existieren A-linear unabhängige Elemente ω_1 und ω_2 in $\mathcal{C}$, die den gleichen (minimalen) Betrag haben und Λ somit als A-Modul erzeugen. □

4.4. Korollar. *Betrachte einen Gitterpunkt $\lambda = a\omega_1 + b\omega_2 \in \Lambda$ mit $a,b\in A$. Dann ist*

$$|\lambda| = \max\{|a|,|b|\}\,|\omega_1|\,(=\max\{|a|,|b|\}\,|\omega_2|).$$

Wir zeigen nun zunächst ein weiteres

4.5. Lemma. *Sei $a\in A\setminus\mathbb{F}_q$. Die a-Torsion ${}_a\Phi$ ist in $K_\infty(\Lambda)$ enthalten und die Körpererweiterung $K_\infty(\Lambda)|K_\infty({}_a\Phi)$ ist galoissch.*

Beweis. Aus der in Satz 1.14 gezeigten Beziehung

$$e_\Lambda : a^{-1}\Lambda/\Lambda \xrightarrow{\cong} {}_a\Phi$$

folgt, dass $K_\infty({}_a\Phi)$ in $K_\infty(\Lambda) = K_\infty(a^{-1}\Lambda)$ enthalten ist. Weiter liefert Satz 1.16, dass

$$\Lambda \subset K_\infty^{\mathrm{sep}}$$

gilt. Damit lässt sich die gegebene Situation wie folgt darstellen

$$\begin{array}{c} K_\infty^{\mathrm{sep}} \\ | \\ K_\infty(\Lambda) \\ | \\ K_\infty({}_a\Phi) \\ | \\ K_\infty. \end{array}$$

Insbesondere ist die Körpererweiterung $K_\infty(\Lambda)|K_\infty$ separabel. Sie ist sogar endlich, da Λ als A-Modul von zwei Elementen erzeugt wird.

Sei nun σ ein K_∞-Homomorphismus von $K_\infty(\Lambda)$ in den separabel algebraischen Abschluss K_∞^{sep}. Dann gilt für jedes Element $\lambda \in \Lambda$ unter Verwendung der Stetigkeit von σ

$$e_\Lambda(\sigma(\lambda)) = \sigma(e_\Lambda(\lambda)) = \sigma(0) = 0,$$

da wir bereits wissen, dass e_Λ Koeffizienten in K_∞ besitzt. Das heißt, das Gitter Λ wird unter jedem K_∞-Homomorphismus $K_\infty(\Lambda) \longrightarrow K_\infty^{\text{sep}}$ in sich überführt; ein solcher Homomorphismus beschränkt sich also zu einem Automorphismus von $K_\infty(\Lambda)$. Damit ist die Erweiterung $K_\infty(\Lambda)|K_\infty$ normal und sogar galoissch.

Im Speziellen ist auch $K_\infty(\Lambda)|K_\infty({}_a\Phi)$ galoissch. □

Damit gelingt es uns, folgende zentrale Aussage zu beweisen.

4.6. Satz. *Sei $a \in A \setminus \mathbb{F}_q$. Dann ist*

$$K_\infty({}_a\Phi) = K_\infty(\Lambda).$$

Beweis. Annahme: $\#\text{Gal}(K_\infty(\Lambda)|K_\infty({}_a\Phi)) > 1$. Dann existiert ein nichttriviales Element $\sigma \in \text{Gal}(K_\infty(\Lambda)|K_\infty({}_a\Phi))$. Nach Satz 1.14 ist $e_\Lambda(a^{-1}\omega_1) \in {}_a\Phi$, also gilt

$$e_\Lambda(a^{-1}\omega_1) = \sigma\left(e_\Lambda(a^{-1}\omega_1)\right) = e_\Lambda(\sigma(a^{-1}\omega_1)).$$

Daraus folgt

$$\sigma(a^{-1}\omega_1) - a^{-1}\omega_1 \in \ker e_\Lambda = \Lambda,$$

was äquivalent ist zu

$$\sigma(\omega_1) \equiv \omega_1 \mod a\Lambda.$$

Folglich ist

$$\sigma(\omega_1) = \omega_1 + a\lambda \quad \text{für ein } \lambda \in \Lambda$$

und, da $|\omega_1|$ nach Definition minimal ist in Λ, und $|a| > 1$ gilt, erhalten wir

$$|\sigma(\omega_1)| = |\omega_1 + a\lambda| \geq |a|\,|\omega_1| > |\omega_1|.$$

Nach Voraussetzung ist aber $|\sigma(\omega_1)| = |\omega_1|$, da σ als Galois-Automorphismus isometrisch auf dem Gitter Λ operiert. Dies ist ein Widerspruch. □

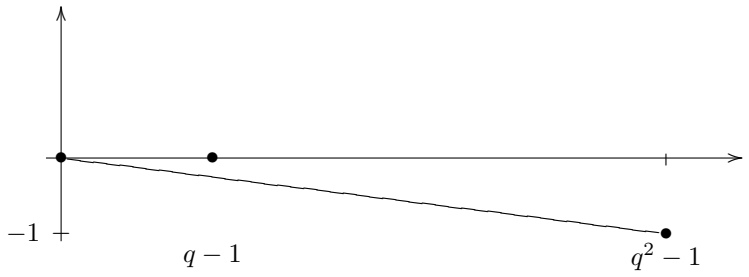
In der an ∞ lokalisierten Situation erhalten wir also für jedes nicht-konstante Polynom $a \in A$ den gleichen Torsionskörper. Wir werden uns daher im Folgenden darauf beschränken, die Stelle $\mathfrak{p} = T$ zu betrachten, um die Rechnungen möglichst weit zu vereinfachen.

4.2. Betrachtung von Φ_T

Wir bestimmen zunächst das Newton-Polygon von $f(X) := \dfrac{\Phi_T(X)}{X}$ über K_∞. Da f von der Form

$$f(X) = T + X^{q-1} - X^{q^2-1}$$

ist und für die Bewertungen der Koeffizienten $v(T) = (-1)$ und $v(1) = v(-1) = 0$ gilt, besitzt das Newton-Polygon folgende Gestalt:



Daraus folgt, dass jede Nullstelle von f im Zerfällungskörper von f Bewertung $-\frac{1}{q^2-1}$ besitzt. Des Weiteren ist f irreduzibel über $K_\infty[X]$; die zugehörige Galois-Gruppe operiert transitiv auf den Nullstellen von f.

Die Situation an der unendlichen Stelle ähnelt damit dem supersingulären Fall an der endlichen Stelle. In der Tat erhalten wir die folgenden Versionen dort gezeigter Aussagen:

4.7. Lemma. *Der Zerfällungskörper $K_\infty({}_T\Phi)$ von Φ_T enthält die q^2-1-ten Einheitswurzeln.*

Beweis. Der Beweis erfolgt analog zum Beweis von Lemma 3.8. □

Wir können daher wiederum zunächst die q^2-1-ten Einheitswurzeln zu K_∞ adjungieren, bevor wir Nullstellen von f adjungieren. Dies erlaubt es uns, folgende Aussage zu formulieren:

4.8. Satz. *Sei ω eine primitive q^2-1-te Einheitswurzel und x_1 eine Nullstelle von f. Die voll verzweigte Körpererweiterung*

$$L_\infty := K_\infty(\omega)(x_1)|K_\infty(\omega)$$

ist eine Kummer-Erweiterung, d.h. sie ist galoissch vom Grad q^2-1 mit zyklischer Galois-Gruppe.

Beweis. Analog zum Beweis von Satz 3.9. □

Damit gelingt es uns, zu zeigen:

4.9. Satz. *Das Polynom $\Phi_T(X)$ zerfällt über L_∞.*

Beweis. Die T-Torsion ${}_T\Phi$ ist ein zweidimensionaler $\mathbb{F}_q$-Vektorraum. Es ist also zu zeigen, dass x_1 in L_∞ zu einer Basis von ${}_T\Phi$ ergänzt werden kann.

Mit $\alpha := x_1^{q-1}$ ist das Polynom

$$\prod_{c\in\mathbb{F}_q}(X-cx_1) = X^q - \alpha X = \tau - \alpha\tau^0$$

ein rechter Teiler von Φ_T in $L_\infty\{\tau\}$, da sein Kern einen $\mathbb{F}_q$-Unterraum von ${}_T\Phi$ bildet. Es existiert also $\beta \in L_\infty$ mit $\Phi_T = (-\tau+\beta)(\tau-\alpha)$. Koeffizientenvergleich liefert die Bedingungen

$$\begin{aligned} \alpha^q + \beta &= 1 \\ -\alpha\beta &= T. \end{aligned} \tag{4.1}$$

Für die Bewertungen gilt

$$v(\alpha) = (q-1)v(x_1) = -\frac{q-1}{q^2-1}$$

und

$$v(\beta) = v(-T\alpha^{-1}) = -1 - v(\alpha) = -\frac{q(q-1)}{q^2-1}.$$

Ist $0 \neq x_2 \in \overline{K}_\infty$ eine weitere Nullstelle von Φ_T, die $x_2 \neq cx_1$ für alle $c \in \mathbb{F}_q^*$ erfüllt, so ist $x_2 \notin \ker(\tau-\alpha)$. Wir definieren

$$u := x_2^q - \alpha x_2 \in \ker(-\tau+\beta)\setminus\{0\}.$$

Dann ist $-u^q + \beta u = 0$ bzw. $-u^{q-1}+\beta = 0$. Notwendige Bedingung dafür, dass x_2 in L_∞ liegt, ist also, dass β in L_∞ eine $q-1$-te Potenz ist. Umstellen von (4.1) liefert die Gleichung

$$\frac{\beta}{\alpha} = -\alpha^{q-1} + \frac{1}{\alpha}.$$

Da α eine $q-1$-te Potenz ist, folgt: Das Element β ist genau dann eine $q-1$-te Potenz, wenn $-\alpha^{q-1}+\frac{1}{\alpha}$ eine ist. Dies zeigen wir mithilfe des trivialen Falls des Lemmas von Hensel. Gesucht ist eine Lösung der Gleichung

$$\begin{aligned} & X^{q-1}+\alpha^{q-1}-\frac{1}{\alpha}=0 \\ \Leftrightarrow\ & \frac{1}{\alpha^{q-1}}X^{q-1}+1-\frac{1}{\alpha^q}=0. \end{aligned}$$

Mit der Substitution $X=\alpha Y$ lautet die zu lösende Gleichung

$$h(Y):=Y^{q-1}+1-\frac{1}{\alpha^q}=0.$$

Da α echt negative Bewertung besitzt, verschwindet $\frac{1}{\alpha^q}$ modulo des maximalen Ideals $\mathfrak{m}$ von L_∞. Über dem Restkörper $\mathbb{F}_{q^2}$ von L_∞ gilt somit

$$\overline{h}(Y)\equiv Y^{q-1}+1 \mod \mathfrak{m}.$$

Das reduzierte Polynom $\overline{h}$ ist separabel und besitzt Nullstellen über $\mathbb{F}_{q^2}$. Diese können nach dem Lemma von Hensel zu Nullstellen von h in L_∞ geliftet werden. Rücksubstitution liefert die Existenz von $b\in L_\infty$ mit $b^{q-1}=\beta$. Es bleibt zu zeigen, dass die Gleichung

$$X^q-\alpha X=b$$

in L_∞ eine Lösung besitzt. Unter Ausnutzung von $\alpha=x_1^{q-1}$ lässt sich diese Gleichung mit der Substitution $X=x_1Z$ in die Gestalt

$$Z^q-Z=x_1^{-q}b \tag{4.2}$$

überführen. Wegen

$$v(b)=\frac{1}{q-1}v(\beta)=-\frac{q}{q^2-1}$$

gilt

$$v(x_1^{-q}b)=0.$$

Wir betrachten nun eine Erweiterung $L'_\infty:=L_\infty(y)$ von L_∞, wobei y ein Element von $\overline{K}_\infty$ ist, das der Gleichung (4.2) genügt. Da $Z^q-Z-x_1^{-q}b$ ein separables Polynom in $L_\infty[Z]$ ist, dessen Reduktion im Restkörper ebenfalls separabel und vom Grad q ist, ist diese Erweiterung unverzweigt. Sie ist also insbesondere trivial, wenn die Reduktion der Gleichung (4.2) modulo $\mathfrak{m}$ eine Lösung im Restkörper von L_∞ besitzt, d.h. wenn in $\mathbb{F}_{q^2}$ gilt

$$\overline{x_1^{-q}b}\in \mathrm{Im}(F-id)$$

mit dem Frobenius-Automorphismus $F:\mathbb{F}_{q^2}\to\mathbb{F}_{q^2}, x\mapsto x^q$. Lemma A.14 liefert die Beziehung

$$\mathrm{Im}(F-id)=\ker(F+id)$$

und somit reicht es zu zeigen:

$$\overline{x_1^{-q}b}\in\ker(F+id),$$

was jedoch äquivalent ist zu

$$(x_1^{-q}b)^q+x_1^{-q}b\in\mathfrak{m}.$$

Dies erhalten wir mit folgender Rechnung

$$\begin{aligned}
& v\left((x_1^{-q}b)^q + x_1^{-q}b\right) \\
&= v\left(x_1^{-q^2}b\left[b^{q-1} + x_1^{q^2-q}\right]\right) \\
&= v(x_1^{-q^2+q}) + \underbrace{v(x_1^{-q}b)}_{=0} + v(b^{q-1} + (x_1^{q-1})^q) \\
&= v(x_1^{-q^2+q}) + v(\beta + \alpha^q) \\
&\overset{(4.1)}{=} v(x_1^{-q^2+q}) + v(1) \\
&= \frac{q^2-q}{q^2-1} \\
&= \frac{q}{q+1} > 0.
\end{aligned}$$

Die Erweiterung $L'_\infty \mid L_\infty$ ist daher trivial; wir finden also bereits in L_∞ ein geeignetes Element, mit dem wir x_1 zu einer Basis von ${}_T\Phi$ ergänzen können. Damit ist die Behauptung gezeigt. □

Der Zerfällungskörper $K_\infty({}_T\Phi)$ von Φ_T über K_∞ lässt sich beschreiben durch das Diagramm:

$$\begin{array}{c} K_\infty({}_T\Phi) = K_\infty(\omega, x_1) \\ | \\ K_\infty(\omega) \\ | \\ K_\infty \end{array}$$

4.10. Korollar. *Es gilt* $[K_\infty({}_T\Phi) : K_\infty] = 2(q^2-1)$.

4.11. Bemerkung. Die lokale Galois-Gruppe $G_\infty = \mathrm{Gal}(K_\infty({}_\mathfrak{p}\Phi)|K_\infty)$ besitzt $2(q^2-1)$ Elemente. Wie im supersingulären Fall an der endlichen Stelle ist die Gruppe G_∞ Normalisator einer nicht-zerfallenden Cartan-Gruppe.

Mit den Bezeichnungen aus Bemerkung 3.12 lässt sich G_∞ beschreiben als das semidirekte Produkt von C_{q^2-1} und C_2, wobei die Gruppe C_2 durch Erheben in die q-te Potenz auf C_{q^2-1} operiert. Die zyklische Untergruppe C_{q^2-1} von $\mathrm{GL}(2, \mathbb{F}_q)$ ist vom in Bemerkung A.23 angegebenen Typ.

4.12. Satz. *Für den lokalen Diskriminantenexponenten* $D_{K_\infty({}_\mathfrak{p}\Phi)|K_\infty}$ *gilt*

$$D_{K_\infty({}_\mathfrak{p}\Phi)|K_\infty} = 2(q^2-2).$$

Beweis. Die Berechnung des lokalen Diskriminantenexponenten erfolgt wie in Satz 3.13. Wir erhalten für den lokalen Diskriminantenexponenten der zahm und voll verzweigten Erweiterung $K_\infty(\omega, x_1)|K_\infty(\omega)$ nach Satz A.7

$$D_{K_\infty(\omega,x_1)|K_\infty(\omega)} = q^2 - 2$$

und wissen, dass in der unverzweigten quadratischen Erweiterung $K_\infty(\omega)|K_\infty$

$$D_{K_\infty(\omega)|K_\infty} = 0$$

gilt. Durch Einsetzen dieser Diskriminantenexponenten in die Formel aus Lemma A.6 folgt die Behauptung. □

KAPITEL 5

Die globale Situation

In den vorangegangenen Kapiteln haben wir unter anderem die lokalen Galois-Gruppen $G_\mathfrak{p}$ und G_∞ an $\mathfrak{p}$ bzw. ∞ bestimmt. Die angegebenen Darstellungen sind jedoch abhängig von jeweils geeignet gewählten Basen von ${}_\mathfrak{p}\Phi$.

Wollen wir aus den lokalen Galois-Gruppen Schlüsse über die globale Galois-Gruppe $G = \mathrm{Gal}(K({}_\mathfrak{p}\Phi|K)$ ziehen, so müssen wir zunächst bestimmen, in welchem Verhältnis die Gruppen $G_\mathfrak{p}$ und G_∞ als Untergruppen von G zueinander stehen.

5.1. Die globale Galois-Gruppe

Wir wissen bislang, dass G eine Untergruppe von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$ ist und Untergruppen besitzt, die zu $G_\mathfrak{p}$ bzw. G_∞ isomorph sind. Sei $C \subset G$ eine zyklische Untergruppe von G_∞ mit $q^2 - 1$ Elementen.

5.1. Bemerkung. Da G_∞ bereits für $d = 1$ realisiert wird, lässt sich C in $\mathrm{GL}(2, \mathbb{F}_q)$ einbetten. Elemente von C besitzen somit charakteristische Polynome im Polynomring in einer Variablen über $\mathbb{F}_q$.

5.2. Satz. *Sei $\mathbb{F}_q[C]$ der Gruppenring zur betrachteten Gruppe C. Dann ist ${}_\mathfrak{p}\Phi$ ein halbeinfacher $\mathbb{F}_q[C]$-Modul.*

Beweis. Eine $\mathbb{F}_q[C]$-Modulstruktur auf einem $\mathbb{F}_q$-Vektorraum M ist gegeben, wenn C auf M $\mathbb{F}_q$-linear operiert. Dies ist für die Torsion ${}_\mathfrak{p}\Phi$ in der Tat der Fall, da C Untergruppe der Galois-Gruppe G ist. Da $\#C = q^2 - 1$ teilerfremd zur Charakteristik von $\mathbb{F}_q$ ist, ist jeder $\mathbb{F}_q[C]$-Modul halbeinfach. □

In diesem Kapitel bezeichne $\Lambda = A\omega_1 \oplus A\omega_2$ weiterhin das in Abschnitt 4.1 beschriebene Gitter, das zum betrachteten Drinfeld-Modul gehört.

5.3. Bemerkung. Das Gitter Λ induziert auf ${}_\mathfrak{p}\Phi$ durch die in Satz 1.14 hergeleitete Darstellung

$$ {}_\mathfrak{p}\Phi \cong \mathfrak{p}^{-1}\Lambda/\Lambda = \left\{ \frac{a_1}{\mathfrak{p}}\omega_1 + \frac{a_2}{\mathfrak{p}}\omega_2 \,\middle|\, a_i \in A, \deg a_i < d, i = 1, 2 \right\} $$

eine Filtrierung von $\mathbb{F}_q$-Vektorräumen

$$ {}_\mathfrak{p}\Phi \cong V_d \supset V_{d-1} \supset \ldots \supset V_1 \supset V_0 = \{0\} \tag{5.1} $$

mit

$$ V_j := \left\{ \frac{a_1}{\mathfrak{p}}\omega_1 + \frac{a_2}{\mathfrak{p}}\omega_2 \,\middle|\, a_i \in A, \deg a_i < j, i = 1, 2 \right\}, \quad j = 1, \ldots, d. $$

5.4. Lemma. *Die Operation von C auf ${}_\mathfrak{p}\Phi$ respektiert die Filtrierung* (5.1).

Beweis. Da die betrachtete Filtrierung eine Bedingung an die Absolutbeträge bezüglich ∞ ausdrückt, folgt die Behauptung aus Satz 4.6. Wegen

$$ |\sigma(\omega_1)|_\infty = |\omega_1|_\infty \quad \text{für } \sigma \in G_\infty $$

operiert C nämlich isometrisch auf dem Gitter, bildet also jedes der V_i auf sich ab. □

Es handelt sich somit bei (5.1) um eine Filtrierung von C-Untermoduln. Es gilt

$$\dim_{\mathbb{F}_q}(V_j/V_{j-1}) = 2, \quad j = 1, \ldots, d.$$

Da V_d als $\mathbb{F}_q[C]$-Modul halbeinfach ist, existiert ein C-Untermodul $W_d \subset V_d$, so dass $V_d = V_{d-1} \oplus W_d$ gilt, d.h. $W_d \cong V_d/V_{d-1}$. Induktiv erhält man

$$V_d = \bigoplus_{i=1}^{d} W_i, \quad \dim W_i = 2, \quad i = 1, \ldots, d.$$

5.5. Lemma. *Es existiert kein eindimensionaler C-stabiler $\mathbb{F}_q$-Untervektorraum von ${}_{\mathfrak{p}}\Phi$.*

Beweis. Sei γ ein Erzeuger von C. Für den Beweis des Lemmas genügt es, zu zeigen, dass γ keinen Eigenwert in $\mathbb{F}_q^*$ besitzt.

Annahme: γ hat einen Eigenwert in $\mathbb{F}_q^*$. Dann liegt nach Bemerkung 5.1 auch der zweite Eigenwert in $\mathbb{F}_q^*$. Wir können somit die Jordan-Normalform von γ in $\mathrm{GL}(2, \mathbb{F}_q)$ bilden. Diese ist entweder eine Diagonalmatrix oder besteht aus einem 2×2-Jordan-Block J der Form

$$J = \begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix},$$

wenn a der Eigenwert von γ ist. Ein solches Element J von $\mathrm{GL}(2, \mathbb{F}_q)$ hat als Ordnung jedoch ein Vielfaches der Charakteristik von $\mathbb{F}_q$, kann also nicht die zyklische Gruppe C mit $q^2 - 1$ Elementen erzeugen.

Also ist γ diagonalisierbar in $\mathrm{GL}(2, \mathbb{F}_q)$ und somit gilt bereits $\gamma^{q-1} = 1$ im Widerspruch zu $\langle \gamma \rangle = \mathrm{C}$. □

Mit diesem Lemma beweisen wir folgenden

5.6. Satz. *Das Polynom $\dfrac{\Phi_{\mathfrak{p}}(X)}{X}$ ist über $K[X]$ irreduzibel.*

Beweis. Annahme: Es existiert ein nicht-trivialer Teiler g' von $\dfrac{\Phi_{\mathfrak{p}}(X)}{X}$ in $K[X]$. Dieser ist mit der auf ${}_{\mathfrak{p}}\Phi$ durch den Drinfeld-Modul induzierten $\mathbb{F}_{\mathfrak{p}}$-Vektorraumstruktur verträglich, so dass $\ker g' \cup \{0\}$ ein $\mathbb{F}_{\mathfrak{p}}$-Untervektorraum von ${}_{\mathfrak{p}}\Phi$ ist. Wegen der Nicht-Trivialität des Teilers handelt es sich dabei um einen eindimensionalen $\mathbb{F}_{\mathfrak{p}}$-Vektorraum.

Wir erhalten unter der Annahme also in $K\{\tau\}$ eine Zerlegung

$$\Phi_{\mathfrak{p}} = f \circ g$$

mit $\deg_\tau f = \deg_\tau g = d$. Der eindimensionale $\mathbb{F}_{\mathfrak{p}}$-Unterraum $H := \ker g$ von ${}_{\mathfrak{p}}\Phi$ ist Galois-stabil.

Wir betrachten für die $\mathfrak{p}$-Torsion wieder die Darstellung

$$\mathfrak{p}^{-1}\Lambda/\Lambda \xrightarrow{\cong} {}_{\mathfrak{p}}\Phi$$

mit einem Obergitter $\mathfrak{p}^{-1}\Lambda$ von Λ. In Termen von A-Basen lassen sich die Gitter beschreiben durch

$$\Lambda = \langle \omega_1, \omega_2 \rangle,$$
$$\mathfrak{p}^{-1}\Lambda = \langle \mathfrak{p}^{-1}\omega_1, \mathfrak{p}^{-1}\omega_2 \rangle.$$

Als Konsequenz aus der Annahme existiert nun ein weiteres A-Gitter Γ, ebenfalls vom Rang 2, mit

$$\Gamma/\Lambda \cong H$$

und

$$\Lambda \subset \Gamma \subset \mathfrak{p}^{-1}\Lambda.$$

Nach dem Elementarteilersatz existiert eine neue Basis $\{\eta_1, \eta_2\}$ von Λ bzw. eine Basis $\left\{\mathfrak{p}^{-1}\eta_1, \mathfrak{p}^{-1}\eta_2\right\}$ von $\mathfrak{p}^{-1}\Lambda$, so dass gilt

$$\Gamma = A\eta_1 + A\mathfrak{p}^{-1}\eta_2.$$

Dies liefert für H die Beschreibung

$$H \cong \left\{ \frac{a}{\mathfrak{p}}\eta_2 \,\middle|\, a \in A, \deg a < d \right\}. \tag{5.2}$$

Schneiden von (5.1) mit H liefert eine neue Filtrierung

$$(V_d \cap H) \supset (V_{d-1} \cap H) \supset \ldots \supset (V_1 \cap H) \supset (V_0 \cap H) = \{0\},$$

bzw. mit $U_i := V_i \cap H$ für alle $i = 0, \ldots, d$,

$$U_d \supset U_{d-1} \supset \ldots \supset U_1 \supset U_0 = \{0\}. \tag{5.3}$$

Die Galois-Stabilität von H gewährleistet, dass auch (5.3) eine Filtrierung von C-Moduln ist. Aus (5.2) folgt

$$\dim_{\mathbb{F}_q}(U_j/U_{j-1}) = 1, \quad j = 1, \ldots, d.$$

Damit ist U_1 ein eindimensionaler C-stabiler Untermodul von V_d im Widerspruch zu Lemma 5.5. □

Die Irreduzibilität von $\dfrac{\Phi_{\mathfrak{p}}(X)}{X}$ liefert direkt die folgende Aussage:

5.7. Korollar. *Die Operation von G auf ${}_{\mathfrak{p}}\Phi \setminus \{0\}$ ist transitiv.*

Für den Beweis des nächsten Satzes verwenden wir folgenden Spezialfall eines allgemeineren Sachverhalts aus der Gruppentheorie.

5.8. Lemma. *Sei $d > 1$ oder $q > 3$. Für einen Normalteiler N von $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}})$ gilt*

$$\mathrm{SL}(2, \mathbb{F}_{\mathfrak{p}}) \subset N$$

oder

$$N \subset Z,$$

wobei $Z := \left\{aI \mid a \in \mathbb{F}_{\mathfrak{p}}^*\right\}$ das Zentrum von $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}})$ ist.

Beweis. Nach Voraussetzung ist $\#\mathbb{F}_{\mathfrak{p}} = q^d > 3$. Damit folgt die Behauptung direkt aus Satz A.22. □

5.9. Satz. *Sei $\mathfrak{p}$ eine endliche Stelle, an der der ordinäre Fall vorliegt. Dann gilt: Erfüllt die Stelle $\mathfrak{p}$ Hypothese 1, so ist*

$$G = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}}).$$

Beweis. Wir behandeln zunächst die Fälle $\#\mathbb{F}_{\mathfrak{p}} = 2$ und $\#\mathbb{F}_{\mathfrak{p}} = 3$ gesondert. In den übrigen Fällen können wir Lemma 5.8 anwenden.

Sei $\mathbb{F}_{\mathfrak{p}}$ der Körper mit zwei Elementen, d.h. $q = 2$ und $d = 1$. Aus der Betrachtung an der unendlichen Stelle folgt

$$\#G_\infty = 2(q^2 - 1) = 2 \cdot 3 = 6.$$

Andererseits ist aber

$$\#\mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}}) = q(q-1)(q^2-1) = 2 \cdot 3 = 6.$$

Da G die lokale Galois-Gruppe G_∞ umfasst, folgt die Behauptung.

Sei nun $\#\mathbb{F}_{\mathfrak{p}} = 3$, d.h. $q = 3$ und $d = 1$. In diesem Fall gilt

$$\#\mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}}) = 48$$

und

$$\#G_\infty = 2(q^2 - 1) = 16.$$

Da die Stelle $\mathfrak{p}$ ordinär ist, existieren in der lokalen Galois-Gruppe $G_\mathfrak{p}$ Elemente der Ordnung 3; bei Wahl der in Kapitel 3 konstruierten $\mathbb{F}_\mathfrak{p}$-Basis von ${}_\mathfrak{p}\Phi$ beispielsweise das Element

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Somit enthält G ein Element der Ordnung 3 und eine Untergruppe mit 16 Elementen. Diese erzeugen aus Ordnungsgründen aber bereits die Gruppe $\mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$.

Sei schließlich $\#\mathbb{F}_\mathfrak{p} > 3$. Wir betrachten die Untergruppe

$$G' = \left\langle gG_\mathfrak{p}g^{-1} \mid g \in \mathrm{GL}(2, \mathbb{F}_\mathfrak{p}) \right\rangle$$

von $GL(2, \mathbb{F}_\mathfrak{p})$. Nach Konstruktion ist G' Normalteiler in $\mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$.

Behauptung: Die Gruppe G' ist eine Untergruppe von G. Um dies zu sehen, zeigen wir: Zu beliebigem $g \in \mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$ existiert $\widetilde{g} \in G$ mit der Eigenschaft

$$\widetilde{g}G_\mathfrak{p}\widetilde{g}^{-1} = gG_\mathfrak{p}g^{-1}.$$

Diese Bedingung ist äquivalent zu

$$G_\mathfrak{p} = \widetilde{g}^{-1}gG_\mathfrak{p}g^{-1}\widetilde{g}\,.$$

Wie in Korollar 3.31 angegeben, existiert im ordinären Fall eine Basis von ${}_\mathfrak{p}\Phi$, in der jedes Element von $G_\mathfrak{p}$ obere Dreiecksgestalt besitzt. Insbesondere ist dann $G_\mathfrak{p}$ bezüglich dieser Basis Normalteiler der Borelgruppe B aller oberen Dreiecksmatrizen in $\mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$. Finden wir also zu beliebigem $g \in \mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$ ein Element $\widetilde{g} \in G$, das die Bedingung

$$\widetilde{g}^{-1}g \in B$$

erfüllt, so ist die Behauptung bewiesen. Nun lässt sich B aber charakterisieren durch

$$B = \{\gamma \in GL(2, \mathbb{F}_\mathfrak{p}) \mid \gamma \text{ hat den Eigenvektor } v\}$$

mit einem geeigneten Element $v \neq 0$ von ${}_\mathfrak{p}\Phi$. Wir setzen

$$w := g(v) \in {}_\mathfrak{p}\Phi \setminus \{0\}$$

und nach Korollar 5.7 existiert ein Element $\widetilde{g} \in G$ mit der Eigenschaft

$$\widetilde{g}^{-1}(w) = v.$$

Somit besitzt $\widetilde{g}^{-1}g$ den Eigenvektor v und liegt daher in B.

Nach Lemma 5.8 gilt, dass die Normalteiler von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$ entweder im Zentrum liegen oder die Untergruppe $\mathrm{SL}(2, \mathbb{F}_\mathfrak{p})$ umfassen. Da $G_\mathfrak{p} \subset G'$ nicht in die Skalarmatrizen eingebettet werden kann, liegt G' allerdings nicht im Zentrum und enthält somit die Untergruppe $\mathrm{SL}(2, \mathbb{F}_\mathfrak{p})$. Zusammen mit der Surjektivität der Determinantenabbildung auf $G_\mathfrak{p}$ liefert dies

$$G' = \mathrm{GL}(2, \mathbb{F}_\mathfrak{p}).$$

Andererseits ist G' aber in $G \subset \mathrm{GL}(2, \mathbb{F}_\mathfrak{p})$ enthalten, es gilt also schließlich

$$G = \mathrm{GL}(2, \mathbb{F}_\mathfrak{p}).$$

□

Der Beweis ist wegen des direkten Bezugs auf die Beschreibung der lokalen Galoisgruppe in Kapitel 3 in der angegebenen Form tatsächlich nur auf den ordinären Fall anwendbar. Formulieren wir die Aussage des Satzes jedoch im supersingulären Fall als Hypothese, so können wir für Stellen, die sie erfüllen, auch in diesem Fall weitere Ergebnisse herleiten.

Hypothese 2. Die supersinguläre Stelle $\mathfrak{p}$ von K besitze die Eigenschaft

$$\mathrm{Gal}(K({}_\mathfrak{p}\Phi)|K) = \mathrm{GL}(2, \mathbb{F}_\mathfrak{p}).$$

5.10. Bemerkung. Vor dem Hintergrund des seltenen Auftretens des supersingulären Falls fällt diese Einschränkung bei der Beurteilung der Resultate nicht allzu sehr ins Gewicht. Die überwiegende Anzahl der betrachteten Stellen wird ordinär sein, so dass wir diese zusätzliche Annahme in den meisten Fällen nicht benötigen werden.

5.2. Eigenschaften des globalen Torsionskörpers

Im Folgenden sei $\mathfrak{p}$ eine Stelle, die Hypothese 1 im ordinären bzw. Hypothese 2 im supersingulären Fall erfüllt.

Aus den bekannten Formeln für die Größe der allgemeinen linearen Gruppe über endlichen Körpern erhalten wir die folgende Aussage:

5.11. Korollar. *Für den Grad des globalen Torsionskörper $K({}_{\mathfrak{p}}\Phi)$ über K gilt unter Voraussetzung der Hypothesen*

$$[K({}_{\mathfrak{p}}\Phi) : K] = (q^{2d} - 1)(q^{2d} - q^d).$$

In dieser Situation können wir nun die folgende Aussage beweisen, auf die bereits in Kapitel 2 hingewiesen wurde.

5.12. Satz. *Die Erweiterung $K({}_{\mathfrak{p}}\Phi)|K$ enthält keine nicht-triviale Konstantenerweiterung.*

Beweis. Annahme: Die Behauptung ist falsch. Aus der Betrachtung an der Stelle ∞ folgt, dass eine im Torsionskörper $K({}_{\mathfrak{p}}\Phi)$ enthaltene Konstantenerweiterung L von $K = \mathbb{F}_q(T)$ höchstens Grad 2 besitzen kann. Die Annahme führt also zu der Situation:

$$\begin{array}{c} K({}_{\mathfrak{p}}\Phi) \\ | \\ L = \mathbb{F}_{q^2}(T) \\ | \\ K = \mathbb{F}_q(T) \end{array}$$

Ist $\mathfrak{p}$ eine Stelle vom Grad 1, so liefert Korollar 3.4, dass $\mathfrak{p}$ ordinär ist. Nach Korollar 3.23 ist der Trägheitsindex von $\mathfrak{p}$ in $K_{\mathfrak{p}}({}_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}$ in diesem Fall trivial. Dies steht im Widerspruch zur Existenz von L.

Wir können also ohne Einschränkung annehmen, dass

$$\#\mathbb{F}_{\mathfrak{p}} = q^d > 3$$

gilt. Damit ist im Folgenden Lemma 5.8 anwendbar.

Da $L|K$ galoissch vom Grad 2 ist, ist die Galois-Gruppe $H := \mathrm{Gal}(K({}_{\mathfrak{p}}\Phi)|L)$ ein Normalteiler von $G = \mathrm{Gal}(K({}_{\mathfrak{p}}\Phi)|K) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}})$ mit der Eigenschaft

$$[G : H] = 2.$$

Weiter ist

$$\#H = \frac{\#G}{2} = \frac{(q^{2d} - 1)(q^{2d} - q^d)}{2} = (q^d - 1)\frac{q^d(q^{2d} - 1)}{2} > q^d - 1,$$

so dass H nicht im Zentrum von $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}})$ liegen kann. Nach Lemma 5.8 gilt also

$$\mathrm{SL}(2, \mathbb{F}_{\mathfrak{p}}) \subset H.$$

Aus den vorangegangenen Überlegungen erhalten wir die Gleichung

$$[G : \mathrm{SL}(2, \mathbb{F}_{\mathfrak{p}})] = [G : H][H : \mathrm{SL}(2, \mathbb{F}_{\mathfrak{p}})] = 2[H : \mathrm{SL}(2, \mathbb{F}_{\mathfrak{p}})]. \tag{5.4}$$

Da $\mathrm{SL}(2,\mathbb{F}_\mathfrak{p})$ der Kern der Determinantenabbildung $\det : \mathrm{GL}(2,\mathbb{F}_\mathfrak{p}) \longrightarrow \mathbb{F}_\mathfrak{p}^*$ ist, gilt weiter

$$G/_{\mathrm{SL}(2,\mathbb{F}_\mathfrak{p})} \cong \mathbb{F}_\mathfrak{p}^*. \tag{5.5}$$

Die multiplikative Gruppe $\mathbb{F}_\mathfrak{p}^*$ ist zyklisch der Ordnung $q^d - 1$, also ist

$$[G : \mathrm{SL}(2,\mathbb{F}_\mathfrak{p})] = q^d - 1.$$

Wir führen nun eine Fallunterscheidung durch, um die Annahme zum Widerspruch zu führen.

Fall 1: $\mathrm{char}\, K = 2$. Aus Gleichung (5.4) folgt, dass $[G : \mathrm{SL}(2,\mathbb{F}_\mathfrak{p})]$ gerade ist. Im betrachteten Fall ist aber $q^d - 1$ ungerade. Dies ist ein Widerspruch, also existiert in Charakteristik 2 kein Normalteiler H mit den geforderten Eigenschaften und damit auch keine nicht-triviale Konstantenerweiterung.

Fall 2: $\mathrm{char}\, K \neq 2$. In diesem Fall existiert genau eine Untergruppe H von G mit den verlangten Eigenschaften, nämlich die Untergruppe der Matrizen, deren Determinante ein Quadrat in $\mathbb{F}_\mathfrak{p}^*$ ist, d.h.

$$H = \left\{\gamma \in G \mid \det\gamma \in (\mathbb{F}_\mathfrak{p}^*)^2\right\}.$$

Die Abbildung $G \longrightarrow G/H$ ist gegeben durch

$$\gamma \mapsto (\det\gamma) \mod (\mathbb{F}_\mathfrak{p}^*)^2, \quad \gamma \in G.$$

Wir betrachten nun eine endliche Stelle $\mathfrak{q} \neq \mathfrak{p}$. Nach Lemma 2.5 ist eine solche Stelle unverzweigt in $K({}_\mathfrak{p}\Phi)|K$. Wir können daher den zugehörigen Frobenius-Automorphismus $F_\mathfrak{q}$ bilden. Dieser besitzt nach [**Gek08**, Theorem 2.11] das charakteristische Polynom

$$X^2 - aX + \mathfrak{q} \in \mathbb{F}_\mathfrak{p}[X] \tag{5.6}$$

mit einem Element $a \in \mathbb{F}_\mathfrak{p}$. Da die Determinante des Frobenius $F_\mathfrak{q}$ gemäß (5.6) kongruent ist zu $\mathfrak{q}$ modulo $\mathfrak{p}$, wird $F_\mathfrak{q}$ eingeschränkt auf L beschrieben durch $\left(\frac{\mathfrak{q}}{\mathfrak{p}}\right)$, das quadratische Symbol modulo $\mathfrak{p}$.

Das bedeutet, dass die quadratische Erweiterung $L|K$ mit derjenigen Erweiterung von K übereinstimmt, die man durch Adjunktion einer Quadratwurzel aus $\mathfrak{p}$ erhält. In $K(\sqrt{\mathfrak{p}})|K$ ist die Stelle $\mathfrak{p}$ aber verzweigt. Dies steht im Widerspruch zur Annahme $L = \mathbb{F}_{q^2}(T)$. Damit existiert auch in diesem Fall keine nicht-triviale Konstantenerweiterung. □

5.13. Satz. *Für das Geschlecht $g = g_{K({}_\mathfrak{p}\Phi)}$ des Körpers $K({}_\mathfrak{p}\Phi)$ gilt im ordinären Fall unter Verwendung von Hypothese 1*

$$g = \frac{d}{2}(q^{2d}-1)(q^{2d}-2) - \frac{q^2}{2(q^2-1)}(q^{2d}-1)(q^{2d}-q^d) + 1.$$

Beweis. Nach Bemerkung 2.6 hat die Riemann-Hurwitz-Formel in der gegebenen Situation die Gestalt

$$2g - 2 = -2[K({}_\mathfrak{p}\Phi) : K] + \deg\mathfrak{p}\,\#\{\mathfrak{p}'|\mathfrak{p}\}\,D_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}} + \#\{\infty'|\infty\}\,D_{K_\infty({}_\mathfrak{p}\Phi)|K_\infty}.$$

Wir sind nun in der Lage, die hierbei auftretenden Größen zu bestimmen. Nach Korollar 5.11 ist

$$[K({}_\mathfrak{p}\Phi) : K] = (q^{2d}-1)(q^{2d}-q^d).$$

Die lokalen Diskriminantenexponenten wurden in den Sätzen 3.32 und 4.12 als

$$D_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}} = n_\beta(q^{2d}-2)$$

und

$$D_{K_\infty({}_\mathfrak{p}\Phi)|K_\infty} = 2(q^2-2)$$

bestimmt, wobei n_β den Trägheitsindex von $K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}$ bezeichnet. Der Grad von $\mathfrak{p}$ ist d. Die Kenntnis der Größe der lokalen Galois-Gruppen erlaubt es uns, die Anzahl der Stellen von $K({}_\mathfrak{p}\Phi)$ über einer gegebenen Stelle von K zu berechnen. Es gilt

$$\#\{\mathfrak{p}'|\mathfrak{p}\} = \frac{|G|}{|G_\mathfrak{p}|} = \frac{(q^{2d}-1)(q^{2d}-q^d)}{n_\beta q^d(q^d-1)} = \frac{q^{2d}-1}{n_\beta}$$

und

$$\#\{\infty'|\infty\} = \frac{|G|}{|G_\infty|} = \frac{(q^{2d}-1)(q^{2d}-q^d)}{2(q^2-1)}.$$

Einsetzen in die Riemann-Hurwitz-Formel und Auflösen nach g liefert die Behauptung. □

Unter Voraussetzung der zweiten Hypothese können wir ebenfalls das Geschlecht von $K({}_\mathfrak{p}\Phi)$ im supersingulären Fall berechnen.

5.14. Satz. *Sei $\mathfrak{p}$ eine supersinguläre Stelle, die Hypothese 2 erfüllt. Dann gilt für das Geschlecht $g = g_{K({}_\mathfrak{p}\Phi)}$ von $K({}_\mathfrak{p}\Phi)$*

$$g = \frac{d}{2}(q^{2d}-q^d)(q^{2d}-2) - \frac{q^2}{2(q^2-1)}(q^{2d}-1)(q^{2d}-q^d) + 1.$$

Beweis. Im Vergleich zur Berechnung des Geschlechts im ordinären Fall ändert sich in der Formel aus Bemerkung 2.6 nur der Anteil an der endlichen Stelle. Nach Satz 3.13 ist im supersingulären Fall

$$D_{K_\mathfrak{p}({}_\mathfrak{p}\Phi)|K_\mathfrak{p}} = 2(q^{2d}-2).$$

Weiter gilt

$$\#\{\mathfrak{p}'|\mathfrak{p}\} = \frac{|G|}{|G_\mathfrak{p}|} = \frac{(q^{2d}-1)(q^{2d}-q^d)}{2(q^{2d}-1)} = \frac{(q^{2d}-q^d)}{2}.$$

Wie im Beweis von Satz 5.13 folgt die Behauptung nun durch Einsetzen in die Riemann-Hurwitz-Formel. □

KAPITEL 6

Verallgemeinerung der Resultate

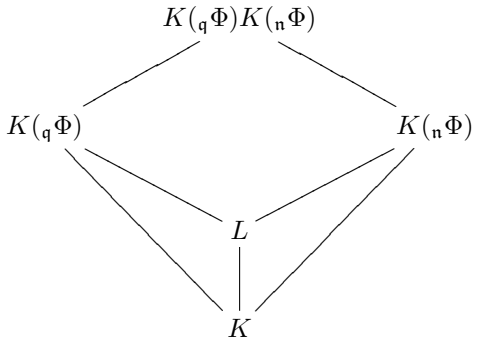
Bei den bisherigen Überlegungen haben wir uns darauf beschränkt, die Torsionskörper $K({}_{\mathfrak{p}}\Phi)$ für Primpolynome $\mathfrak{p} \in A$ zu betrachten. In diesem Kapitel wollen wir die Resultate verallgemeinern. Dies gelingt uns, unter Berücksichtigung der Hypothesen, für quadratfreie Elemente von A.

Wir betrachten dazu in K eine endliche Stelle $\mathfrak{q}$ des Grades t und einen Divisor $\mathfrak{n} = \prod \mathfrak{p}_i$ mit paarweise verschiedenen endlichen Stellen $\mathfrak{p}_i \neq \mathfrak{q}$. Weiter fordern wir, dass für alle auftretenden ordinären Stellen Hypothese 1 und für alle supersingulären Stellen Hypothese 2 erfüllt ist.

Wir wissen bereits, dass $\mathfrak{q}$ verzweigt ist in $K({}_{\mathfrak{q}}\Phi)$ und unverzweigt in $K({}_{\mathfrak{n}}\Phi)$ aufgrund der guten Reduktion von $\Phi_{\mathfrak{n}}$ an $\mathfrak{q}$.

6.1. Satz. *Die Körpererweiterungen $K({}_{\mathfrak{q}}\Phi)$ und $K({}_{\mathfrak{n}}\Phi)$ sind linear disjunkt über K.*

Beweis. Wir bilden zunächst den Durchschnitt L von $K({}_{\mathfrak{q}}\Phi)$ und $K({}_{\mathfrak{n}}\Phi)$.



Die Erweiterung $L|K$ ist als Durchschnitt zweier galoisscher Körpererweiterungen von K selbst eine Galois-Erweiterung. Die Galois-Gruppe $H := \mathrm{Gal}(K({}_{\mathfrak{q}}\Phi)|L)$ ist daher ein Normalteiler von $\mathrm{Gal}(K({}_{\mathfrak{q}}\Phi)|K) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{q}})$.

Da L in $K({}_{\mathfrak{n}}\Phi)$ enthalten ist, ist insbesondere $\mathfrak{q}$ unverzweigt in L. Sei $\mathfrak{Q}$ eine Stelle in L über $\mathfrak{q}$. Betrachten wir die lokale Körpererweiterung $L_{\mathfrak{Q}}|K_{\mathfrak{q}}$, so können wir diese in die in Kapitel 3 beschriebene Erweiterung $K_{\mathfrak{q}}({}_{\mathfrak{q}}\Phi)|K_{\mathfrak{q}}$ einbetten. Genauer liegt der Körper $L_{\mathfrak{Q}}$ nach Wahl einer solchen Einbettung in der unverzweigten Teilerweiterung von $K_{\mathfrak{q}}({}_{\mathfrak{q}}\Phi)|K_{\mathfrak{q}}$.

Die Gestalt dieser unverzweigten Erweiterung von $K_{\mathfrak{q}}$ hängt davon ab, ob die Stelle $\mathfrak{q}$ supersingulär oder ordinär ist. Behalten wir die Notation aus Kapitel 3 bei, so gilt für $H_{\mathfrak{q}} := \mathrm{Gal}(K_{\mathfrak{q}}({}_{\mathfrak{q}}\Phi)|L_{\mathfrak{Q}})$ daher im supersingulären Fall

$$\mathrm{Gal}(K_{\mathfrak{q}}({}_{\mathfrak{q}}\Phi)|K_{\mathfrak{q}}(\omega)) \subset H_{\mathfrak{q}}$$

und im ordinären Fall

$$\mathrm{Gal}(K_{\mathfrak{q}}({}_{\mathfrak{q}}\Phi)|K_{\mathfrak{q}}(\ker \beta)) \subset H_{\mathfrak{q}}.$$

Die lokale Galois-Gruppe $H_{\mathfrak{q}}$ kann wiederum in die globale Galois-Gruppe H eingebettet werden.

Wir zeigen nun zunächst in beiden Fällen, dass die Determinantenabbildung auf H surjektiv ist, sowie dass H nicht in das Zentrum von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$ eingebettet werden kann.

1. Fall: Die Stelle $\mathfrak{q}$ ist supersingulär. In diesem Fall liefert Satz 3.9, dass

$$\mathrm{Gal}(K_\mathfrak{q}({}_\mathfrak{q}\Phi)|K_\mathfrak{q}(\ker\beta)) = C \subset H$$

gilt, wobei C eine zyklische Untergruppe von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$ der Ordnung $q^{2t} - 1$ ist.

Sei $\mathbb{F}_\mathfrak{q}^{(2)}$ die quadratische Erweiterung von $\mathbb{F}_\mathfrak{q}$. Nach Bemerkung A.23 kann die Gruppe C aufgefasst werden als Einbettung der multiplikativen Gruppe von $\mathbb{F}_\mathfrak{q}^{(2)}$ nach $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$. Damit entspricht die Determinantenabbildung auf C der Normabbildung $\mathbb{F}_\mathfrak{q}^{(2)} \longrightarrow \mathbb{F}_\mathfrak{q}$, deren Surjektivität aber bekannt ist (siehe z.B. [**LN97**, Theorem 2.28]).

Andererseits kann C nicht in das Zentrum von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$ eingebettet werden, da dieses nur $q^t - 1$ Elemente enthält.

2. Fall: Die Stelle $\mathfrak{q}$ ist ordinär. Wir bezeichnen die in Satz 3.29 bestimmte Galois-Gruppe der wild verzweigten Teilerweiterung an der endlichen Stelle mit H_1 und die Galois-Gruppe, die bei der Adjunktion der Torsionspunkte mit echt positiver Bewertung auftritt (siehe Satz 3.25), mit H_2.

Wählen wir eine $\mathbb{F}_\mathfrak{q}$-Basis von ${}_\mathfrak{q}\Phi$ wie in Korollar 3.31, so besitzen H_1 und H_2 bezüglich dieser Basis die Gestalt

$$H_1 = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \middle| \, b \in \mathbb{F}_\mathfrak{q} \right\}$$

bzw.

$$H_2 = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \middle| \, a \in \mathbb{F}_\mathfrak{q}^* \right\}$$

und liegen nach unseren Vorüberlegungen in H.

Da H_1 in H enthalten ist, kann H nicht ins Zentrum von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$ eingebettet werden. Mit $H_2 \subset H$ folgt, dass die Determinantenabbildung auf H surjektiv ist.

Wir haben damit in beiden Fällen die behaupteten Eigenschaften der Gruppe H gezeigt und sind fertig, falls

$$\#\mathbb{F}_\mathfrak{q} > 3$$

gilt. Da H nämlich nicht im Zentrum von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$ liegt, umfasst die Gruppe H dann nach Lemma 5.8 die Untergruppe $\mathrm{SL}(2, \mathbb{F}_\mathfrak{q})$. Andererseits ist aber die Determinantenabbildung auf H surjektiv. Damit gilt

$$H = \mathrm{GL}(2, \mathbb{F}_\mathfrak{q}).$$

Ist $\#\mathbb{F}_\mathfrak{q} = 2$, so ist $\mathfrak{q}$ eine Stelle vom Grad 1. Nach Korollar 3.4 ist $\mathfrak{q}$ ordinär und die oben definierte Untergruppe H_1 von H hat Ordnung 2. Allerdings ist in diesem Fall $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$ isomorph zu S_3, der symmetrischen Gruppe vom Grad 3. Diese besitzt als einzigen nicht-trivialen Normalteiler A_3, die alternierende Gruppe vom Grad 3. Da diese kein Element der Ordnung 2 enthält, folgt

$$H = \mathrm{GL}(2, \mathbb{F}_\mathfrak{q}).$$

Sei also $\mathbb{F}_\mathfrak{q}$ der Körper mit drei Elementen. Dann sind die drei nicht-trivialen Normalteiler von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$ das Zentrum von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{q})$, die Quaternionengruppe Q_8 mit 8 Elementen, sowie die Gruppe $\mathrm{SL}(2, \mathbb{F}_\mathfrak{q})$. Als Stelle des Grades 1 ist $\mathfrak{q}$ ordinär. Wir haben bereits gesehen, dass H nicht ins Zentrum eingebettet werden kann. Da die Determinantenabbildung auf H_2 surjektiv ist, folgt aus $H_2 \subset H$, dass

$$H \neq \mathrm{SL}(2, \mathbb{F}_\mathfrak{q}),$$

gilt. Schließlich enthält H_1 mit

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

ein Element der Ordnung 3, das also auch in H liegt. Wegen $\#Q_8 = 8$ ist somit

$$H \neq Q_8.$$

Wir erhalten wiederum

$$H = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{q}}).$$

In jedem Fall gilt also, dass die Körpererweiterung $L|K$ trivial ist, das bedeutet

$$K({}_{\mathfrak{q}}\Phi) \cap K({}_{\mathfrak{n}}\Phi) = K.$$

Die Erweiterungen $K({}_{\mathfrak{q}}\Phi)$ und $K({}_{\mathfrak{n}}\Phi)$ sind damit linear disjunkt über K. □

Es ist somit möglich, aus den Ergebnissen für $K({}_{\mathfrak{q}}\Phi)$ und $K({}_{\mathfrak{n}}\Phi)$ die entsprechenden Daten der Erweiterung

$$K({}_{\mathfrak{q}}\Phi)K({}_{\mathfrak{n}}\Phi) = K({}_{\mathfrak{q}}\Phi, {}_{\mathfrak{n}}\Phi) = K({}_{\mathfrak{qn}}\Phi)$$

zu bestimmen. Wir werden dies exemplarisch für den Fall zweier endlicher Stellen $\mathfrak{p} \neq \mathfrak{q}$, die die Hypothesen erfüllen, durchführen. Zunächst halten wir eine direkte Konsequenz der oben gezeigten linearen Disjunktheit fest.

6.2. Lemma. *Seien $\mathfrak{p}$ und $\mathfrak{q}$ zwei verschiedene endliche Stellen von K. Dann gilt unter Voraussetzung der Hypothesen*

$$\mathrm{Gal}(K({}_{\mathfrak{pq}}\Phi)|K) \cong \mathrm{Gal}(K({}_{\mathfrak{p}}\Phi)|K) \times \mathrm{Gal}(K({}_{\mathfrak{q}}\Phi)|K) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}}) \times \mathrm{GL}(2, \mathbb{F}_{\mathfrak{q}}).$$

Zur Vereinfachung der Notation setzen wir

$$n_{\mathfrak{p}} := [K({}_{\mathfrak{p}}\Phi) : K] = [K({}_{\mathfrak{pq}}\Phi) : K({}_{\mathfrak{q}}\Phi)]$$

und

$$n_{\mathfrak{q}} := [K({}_{\mathfrak{q}}\Phi) : K] = [K({}_{\mathfrak{pq}}\Phi) : K({}_{\mathfrak{p}}\Phi)].$$

Um das Geschlecht $g_{K({}_{\mathfrak{pq}}\Phi)}$ von $K({}_{\mathfrak{pq}}\Phi)$ zu berechnen, verwenden wir wieder die Riemann-Hurwitz-Formel. Da die Erweiterung $K({}_{\mathfrak{pq}}\Phi)|K$ keine Konstantenerweiterung enthält, besitzt die Formel die Gestalt

$$2g_{K({}_{\mathfrak{pq}}\Phi)} - 2 = -2[K({}_{\mathfrak{pq}}\Phi) : K] + \deg \mathcal{D}_K^{K({}_{\mathfrak{pq}}\Phi)}.$$

Wie in Bemerkung 2.6 gezeigt, gilt auch in dieser Situation

$$\deg \mathcal{D}_K^{K({}_{\mathfrak{pq}}\Phi)} = \sum_{P \in \mathbb{P}_K} \deg P \, \#\{P'|P\} \, D_{K_P({}_{\mathfrak{pq}}\Phi)|K_P}$$

mit den lokalen Diskriminantenexponenten $D_{K_P({}_{\mathfrak{pq}}\Phi)|K_P}$. Nach der Definition von Differente und Diskriminante ist

$$D(P) := \#\{P'|P\} \, D_{K_P({}_{\mathfrak{pq}}\Phi)|K_P}$$

der globale Diskriminantenexponent der Stelle P in $K({}_{\mathfrak{pq}}\Phi)|K$. Wir werden diese Größen im Folgenden bestimmen. Dazu betrachten wir zunächst das Verzweigungsverhalten der Erweiterung $K({}_{\mathfrak{pq}}\Phi)|K$.

6.3. Bemerkung. In $K({}_{\mathfrak{pq}}\Phi)|K$ können höchstens die Stellen $\mathfrak{p}$, $\mathfrak{q}$ und ∞ verzweigt sein. Aufgrund der linearen Disjunktheit wissen wir weiterhin: Verzweigte Stellen von $K({}_{\mathfrak{pq}}\Phi)|K({}_{\mathfrak{p}}\Phi)$ liegen über verzweigten Stellen von $K({}_{\mathfrak{q}}\Phi)|K$, d.h. über $\mathfrak{q}$ oder der Stelle ∞. Entsprechend gilt dies auch für das Verzweigungsverhalten von $K({}_{\mathfrak{pq}}\Phi)|K({}_{\mathfrak{q}}\Phi)$.

6.4. Lemma. *Sei $\mathfrak{d}(\mathfrak{p})$ der globale Diskriminantenexponent von $\mathfrak{p}$ in $K({}_{\mathfrak{p}}\Phi)|K$. Dann gilt*

$$D(\mathfrak{p}) = n_{\mathfrak{q}}\mathfrak{d}(\mathfrak{p}).$$

BEWEIS. Wir betrachten in $K(_{\mathfrak{pq}}\Phi)|K$ die Zwischenerweiterung $K(_{\mathfrak{p}}\Phi)$ und wenden die Formel für die Diskriminante in Körpertürmen aus Lemma A.5 an:

$$\begin{array}{c} K(_{\mathfrak{pq}}\Phi) \\ | \\ K(_{\mathfrak{p}}\Phi) \\ | \\ K \end{array}$$

Nach Bemerkung 6.3 ist eine Stelle von $K(_{\mathfrak{p}}\Phi)$, die über $\mathfrak{p}$ liegt, unverzweigt in der Erweiterung $K(_{\mathfrak{pq}}\Phi)|K(_{\mathfrak{p}}\Phi)$. Wir erhalten also für den Diskriminantenexponenten von $\mathfrak{p}$ in $K(_{\mathfrak{pq}}\Phi)|K$ keinen Anteil durch die obere Teilerweiterung. Damit ist

$$D(\mathfrak{p}) = [K(_{\mathfrak{pq}}\Phi) : K(_{\mathfrak{p}}\Phi)]\mathfrak{d}(\mathfrak{p}) = n_{\mathfrak{q}}\mathfrak{d}(\mathfrak{p}).$$

□

Analog erhält man für $D(\mathfrak{q})$ die folgende Aussage:

6.5. LEMMA. *Sei $\mathfrak{d}(\mathfrak{q})$ der globale Diskriminantenexponent von $\mathfrak{q}$ in $K(_{\mathfrak{q}}\Phi)|K$. Dann gilt*

$$D(\mathfrak{q}) = n_{\mathfrak{p}}\mathfrak{d}(\mathfrak{q}).$$

Die hierbei auftretenden Diskriminantenexponenten $\mathfrak{d}(\mathfrak{p})$ und $\mathfrak{d}(\mathfrak{q})$ können wir konkret angeben:

6.6. BEMERKUNG. Sei $\mathfrak{p}$ eine endliche Stelle vom Grad d. Ist $\mathfrak{p}$ ordinär, so sei Hypothese 1 erfüllt, andernfalls Hypothese 2. Für den globalen Diskriminantenexponenten $\mathfrak{d}(\mathfrak{p})$ von $\mathfrak{p}$ in $K(_{\mathfrak{p}}\Phi)|K$ gilt in der Notation von Bemerkung 2.6

$$\mathfrak{d}(\mathfrak{p}) = \#\{\mathfrak{p}'|\mathfrak{p}\}D_{K_{\mathfrak{p}}(_{\mathfrak{p}}\Phi)|K_{\mathfrak{p}}}.$$

Mit den Resultaten aus Satz 5.13 und 5.14 bedeutet das

- $\mathfrak{d}(\mathfrak{p}) = (q^{2d}-1)(q^{2d}-2)$ im ordinären Fall, bzw.
- $\mathfrak{d}(\mathfrak{p}) = (q^{2d}-q^d)(q^{2d}-2)$ im supersingulären Fall.

6.7. BEMERKUNG. Für den globalen Diskriminantenexponenten $D(\infty)$ können wir ausnutzen, dass nach Satz 4.6

$$K_\infty(_{\mathfrak{pq}}\Phi) = K_\infty(_{\mathfrak{p}}\Phi) = K_\infty(_{\mathfrak{q}}\Phi) = K_\infty(_T\Phi)$$

gilt. Der lokale Diskriminantenexponent in $K_\infty(_{\mathfrak{pq}}\Phi)|K_\infty$ stimmt daher mit dem in Satz 4.12 bestimmten überein. Bezeichnen wir die lokale Galois-Gruppe an ∞ weiter mit G_∞, dann gilt insbesondere sowohl

$$\#G_\infty \mid n_{\mathfrak{p}}$$

als auch

$$\#G_\infty \mid n_{\mathfrak{q}}.$$

Wir erhalten damit das

6.8. LEMMA. *Es ist*

$$D(\infty) = \frac{n_{\mathfrak{p}}n_{\mathfrak{q}}}{\#G_\infty} D_{K_\infty(_{\mathfrak{pq}}\Phi)|K_\infty}.$$

Wir können nun das Geschlecht von $K(_{\mathfrak{pq}}\Phi)$ berechnen.

6.9. Satz. *Für das Geschlecht $g_{K(\mathfrak{p}\mathfrak{q}\Phi)}$ von $K(\mathfrak{p}\mathfrak{q}\Phi)$ gilt unter Voraussetzung der Hypothesen*

$$\begin{aligned} g_{K(\mathfrak{p}\mathfrak{q}\Phi)} &= n_{\mathfrak{q}} \left(g_{K(\mathfrak{p}\Phi)} - 1\right) + \frac{n_{\mathfrak{p}}}{2}\mathfrak{d}(\mathfrak{q}) \deg \mathfrak{q} + 1 \\ &= n_{\mathfrak{p}} \left(g_{K(\mathfrak{q}\Phi)} - 1\right) + \frac{n_{\mathfrak{q}}}{2}\mathfrak{d}(\mathfrak{p}) \deg \mathfrak{p} + 1. \end{aligned}$$

Beweis. Durch Einsetzen der Resultate für die globalen Diskriminantenexponenten in die Riemann-Hurwitz-Formel erhalten wir

$$\begin{aligned} 2g_{K(\mathfrak{p}\mathfrak{q}\Phi)} - 2 &= -2n_{\mathfrak{p}}n_{\mathfrak{q}} + n_{\mathfrak{q}}\mathfrak{d}(\mathfrak{p}) \deg \mathfrak{p} + n_{\mathfrak{p}}\mathfrak{d}(\mathfrak{q}) \deg \mathfrak{q} + \frac{n_{\mathfrak{p}}n_{\mathfrak{q}}}{\#G_\infty} D_{K_\infty(\mathfrak{p}\mathfrak{q}\Phi)|K_\infty} \\ &= n_{\mathfrak{q}} \left(-2n_{\mathfrak{p}} + \mathfrak{d}(\mathfrak{p}) \deg \mathfrak{p} + \frac{n_{\mathfrak{p}}}{\#G_\infty} D_{K_\infty(\mathfrak{p}\mathfrak{q}\Phi)|K_\infty}\right) + n_{\mathfrak{p}}\mathfrak{d}(\mathfrak{q}) \deg \mathfrak{q}. \end{aligned}$$

Auflösen nach $g_{K(\mathfrak{p}\mathfrak{q}\Phi)}$ liefert

$$\begin{aligned} g_{K(\mathfrak{p}\mathfrak{q}\Phi)} &= n_{\mathfrak{q}} \left[\frac{1}{2}\left(-2n_{\mathfrak{p}} + \mathfrak{d}(\mathfrak{p}) \deg \mathfrak{p} + \frac{n_{\mathfrak{p}}}{\#G_\infty} D_{K_\infty(\mathfrak{p}\mathfrak{q}\Phi)|K_\infty}\right)\right] + \frac{n_{\mathfrak{p}}}{2}\mathfrak{d}(\mathfrak{q}) \deg \mathfrak{q} + 1 \\ &= n_{\mathfrak{q}} \left[g_{K(\mathfrak{p}\Phi)} - 1\right] + \frac{n_{\mathfrak{p}}}{2}\mathfrak{d}(\mathfrak{q}) \deg \mathfrak{q} + 1. \end{aligned}$$

Im letzten Schritt haben wir dabei die Beschreibung des Geschlechts von $K(\mathfrak{p}\Phi)$ aus Satz 5.13 bzw. Satz 5.14 verwendet. Der zweite Teil der Aussage folgt analog durch Ausklammern von $n_{\mathfrak{p}}$ im ersten Schritt. □

Entsprechend lassen sich diese Rechnungen nun fortsetzen, um die Daten für eine Erweiterung $K(\mathfrak{n}\Phi)$ mit einem beliebigen quadratfreien Divisor $\mathfrak{n}$ zu berechnen.

6.10. Beispiel. Unter Voraussetzung der Hypothesen können wir für Stellen kleiner Grade die in Satz 5.13, Satz 5.14 bzw. Satz 6.9 bestimmten Geschlechter der Torsionskörper als Polynome in q angeben.

Sei $\mathfrak{p}$ ein normiertes Primpolynom in $A = \mathbb{F}_q[T]$ des Grades d. Wir setzen voraus, dass die Stelle $\mathfrak{p}$ im ordinären Fall Hypothese 1 und im supersingulären Fall Hypothese 2 erfüllt. Für $d \leq 3$ haben wir für das Geschlecht $g_{K(\mathfrak{p}\Phi)}$ von $K(\mathfrak{p}\Phi)$ die folgenden Formeln:

1. Fall: Die Stelle $\mathfrak{p}$ ist ordinär.

d	$g_{K(\mathfrak{p}\Phi)}$
1	$\frac{1}{2}\left(q^3 - 3q^2\right) + 2$
2	$\frac{1}{2}\left(q^8 - 5q^4\right) + 3$
3	$\frac{1}{2}\left(q^{12} - q^{10} + q^9 - q^8 + q^7 - 9q^6 + q^5\right) + 4$

Anmerkung: Für $d = 1$ und $d = 2$ haben wir in Abschnitt 3.3 bewiesen, dass $\mathfrak{p}$ die Hypothese erfüllt.

2. Fall: Die Stelle $\mathfrak{p}$ ist supersingulär.

d	$g_{K(\mathfrak{p}\Phi)}$
2	$\frac{1}{2}\left(q^8 - 2q^6 - 3q^4 + 4q^2\right) + 1$
3	$\frac{1}{2}\left(2q^{12} - q^{10} - 2q^9 - q^8 + q^7 - 6q^6 + q^5 + 6q^3\right) + 1$

Anmerkung: Nach Korollar 3.4 kann eine Stelle des Grades 1 nicht supersingulär sein.

Sei $\mathfrak{q} \in A$ ein weiteres normiertes Primpolynom des Grades t. Ist auch $t \leq 3$, so erhalten wir unter Voraussetzung der Hypothesen die folgenden Formeln für das Geschlecht $g_{K(\mathfrak{p}\mathfrak{q}\Phi)}$ von $K(\mathfrak{p}\mathfrak{q}\Phi)$:

1. Fall: Beide Stellen sind ordinär.

d	t	$g_{K(\mathfrak{p}\mathfrak{q}\Phi)}$
1	1	$\frac{1}{2}\left(q^8 - 8q^6 + 6q^5 + 11q^4 - 10q^3 - 4q^2 + 4q\right) + 1$
1	2	$\frac{1}{2}\left(2q^{12} - q^{11} - 5q^{10} + q^9 - q^8 + 5q^7 + 7q^6 - 5q^5 - q^4 - 4q^3 - 2q^2 + 4q\right) + 1$
1	3	$\frac{1}{2}\left(3q^{16} - 2q^{15} - 6q^{14} + 3q^{13} + q^{12} + 3q^{11} - 9q^{10} + 6q^9 + 12q^8 - 9q^7 - q^6 - 3q^5 + 6q^4 - 4q^3 - 6q^2 + 6q\right) + 1$
2	2	$\frac{1}{2}\left(3q^{16} - 3q^{14} - 14q^{12} + 14q^{10} + 19q^8 - 19q^6 - 8q^4 + 8q^2\right) + 1$
2	3	$\frac{1}{2}\left(4q^{20} - 3q^{18} - q^{17} - 8q^{16} - 7q^{14} + 5q^{13} + 13q^{12} + q^{11} + 14q^{10} - 4q^9 - 3q^8 - 5q^7 - 10q^6 - 6q^4 + 4q^3 + 6q^2\right) + 1$
3	3	$\frac{1}{2}\left(5q^{24} - q^{22} - 4q^{21} - q^{20} + 2q^{19} - 24q^{18} + 2q^{17} + 22q^{15} - 2q^{13} + 31q^{12} - 2q^{11} + q^{10} - 30q^9 + q^8 - 12q^6 + 12q^3\right) + 1$

2. Fall: Beide Stellen sind supersingulär.

d	t	$g_{K(\mathfrak{p}\mathfrak{q}\Phi)}$
2	2	$\frac{1}{2}\left(3q^{16} - 7q^{14} - 6q^{12} + 22q^{10} - 5q^8 - 15q^6 + 8q^4\right) + 1$
2	3	$\frac{1}{2}\left(4q^{20} - 5q^{18} - 4q^{17} - 6q^{16} + 5q^{15} + 6q^{13} + 8q^{12} + 9q^{10} - 8q^9 - 10q^8 - 9q^7 + 10q^5\right) + 1$
3	3	$\frac{1}{2}\left(5q^{24} - q^{22} - 10q^{21} - q^{20} + 2q^{19} - 12q^{18} + 2q^{17} + 34q^{15} - 2q^{13} - 5q^{12} - 2q^{11} + q^{10} - 24q^9 + q^8 + 12q^6\right) + 1$

3. Fall: Die Stelle $\mathfrak{p}$ ist ordinär, die Stelle $\mathfrak{q}$ ist supersingulär.

d	t	$g_{K(\mathfrak{p}\mathfrak{q}\Phi)}$
1	2	$\frac{1}{2}\left(2q^{12} - q^{11} - 7q^{10} + 3q^9 + 3q^8 + q^7 + 9q^6 - 7q^5 - 9q^4 + 4q^3 + 2q^2\right) + 1$
1	3	$\frac{1}{2}\left(3q^{16} - 2q^{15} - 6q^{14} + 4q^{12} + 6q^{11} - 9q^{10} + 3q^9 + 9q^8 - 7q^6 - 9q^5 + 6q^4 + 2q^3\right) + 1$
2	2	$\frac{1}{2}\left(3q^{16} - 5q^{14} - 10q^{12} + 18q^{10} + 7q^8 - 17q^6 + 4q^2\right) + 1$
2	3	$\frac{1}{2}\left(4q^{20} - 3q^{18} - 4q^{17} - 8q^{16} + 3q^{15} - 4q^{14} + 8q^{13} + 10q^{12} + 4q^{11} + 11q^{10} - 10q^9 - 6q^8 - 11q^7 - 4q^6 + 6q^5 + 4q^3\right) + 1$
3	2	$\frac{1}{2}\left(4q^{20} - 5q^{18} - q^{17} - 6q^{16} + 2q^{15} - 3q^{14} + 3q^{13} + 11q^{12} - 3q^{11} + 12q^{10} - 2q^9 - 7q^8 - 3q^7 - 6q^6 + 4q^5 - 6q^4 + 6q^2\right) + 1$
3	3	$\frac{1}{2}\left(5q^{24} - q^{22} - 7q^{21} - q^{20} + 2q^{19} - 18q^{18} + 2q^{17} + 28q^{15} - 2q^{13} + 13q^{12} - 2q^{11} + q^{10} - 27q^9 + q^8 + 6q^3\right) + 1$

Für alle in diesem Beispiel angegebenen Formeln gilt: Obwohl in bestimmten Koeffizienten der Polynome Nenner auftreten, nehmen die Polynome für beliebige Primzahlpotenzen q Werte in den natürlichen Zahlen an.

KAPITEL 7

Fazit

Als erste Erkenntnis der vorliegenden Arbeit können wir festhalten, dass selbst im Fall des „einfachsten“ Drinfeld-Moduls des Rangs 2 über dem Körper $K = \mathbb{F}_q(T)$ die untersuchten Probleme über eine hohe Komplexität verfügen. Bis jetzt ist es noch nicht gelungen, die Beschreibung der Torsionskörper des betrachteten Drinfeld-Moduls vollständig abzuschließen.

Dennoch liefert die Arbeit relevante Ergebnisse: Die Bestimmung der $\mathfrak{p}$-Torsionskörper für Primstellen $\mathfrak{p}$ hängt nur noch von den im Hauptteil formulierten Hypothesen ab. Eine Untersuchung des Gültigkeitsbereichs der Hypothesen wäre ein möglicher Gegenstand weiterer Forschungen. Das Hauptaugenmerk liegt hierbei wegen des häufigeren Auftretens auf dem ordinären Fall.

Keinen Einschränkungen durch die Hypothese unterliegen die Ergebnisse für ordinäre Stellen des Grades 1 und 2, da wir für diese nachgewiesen haben, dass die Hypothese erfüllt ist.

Ausgehend von den numerischen Rechnungen, die Beispiel 3.6 zugrunde liegen, bieten sich jedoch auch nähere Betrachtungen der supersingulären Stellen an. Neben der noch offenen Frage, welche supersingulären Stellen der zweiten Hypothese genügen, geht es hierbei auch zunächst um eine Klassifikation der supersingulären Stellen. Die bisherigen Ergebnisse legen zwar einen Zusammenhang zwischen Charakteristik und Grad der betrachteten Stelle nahe, dieser ist allerdings zu überprüfen, da es sich hierbei auch um eine mehr oder weniger zufällige Erscheinung handeln kann. Als mögliche Ursache dafür käme in Betracht, dass die bisher betrachteten Grade relativ klein sind und zudem Primzahlen bzw. Primzahlpotenzen.

Schließlich ist für den betrachteten Drinfeld-Modul noch eine Verallgemeinerung der Resultate von quadratfreien auf beliebige Elemente von $A = \mathbb{F}_q[T]$ durchzuführen.

Abgesehen von Aussagen über den konkreten Drinfeld-Modul liefert die vorliegende Arbeit auch Ansätze für die Betrachtung weiterer Drinfeld-Moduln, da sich einige der verwendeten Argumente auf allgemeinere Situationen übertragen lassen. So könnten in einem nächsten Schritt beispielsweise zunächst solche Drinfeld-Moduln betrachtet werden, deren Verhalten an der unendlichen Stelle ebenfalls unabhängig von der Wahl der betrachteten Torsion ist (im Sinne von Abschnitt 4.1).

Insbesondere sei darauf hingewiesen, dass die vorliegenden Ergebnisse konstruktiv sind. So gibt es zwar bei [**Pin97**] allgemeine Aussagen über die Einbettung der Galois-Gruppen der Torsionskörper in die adelische lineare Gruppe (die Bilder unter der Einbettung sind offen, haben also endlichen Index), diese Resultate sind jedoch nicht effektiv und können daher für konkrete Rechnungen nicht verwendet werden.

Anhang: Definitionen und verwendete Aussagen

Dieser Anhang enthält einige Definitionen sowie allgemeine Aussagen, die in dieser Arbeit verwendet werden. In einigen Fällen dient die Angabe an dieser Stelle dazu, Notationen festzulegen. In anderen Fällen erschien es sinnvoll, in den Beweisen verwendete Sachverhalte nicht im Hauptteil der Arbeit zu wiederholen, um den Lesefluss nicht zu unterbrechen. Andererseits sollte aber eine gewisse Geschlossenheit der Arbeit erhalten bleiben, so dass die wichtigsten Aussagen an dieser Stelle nachgeschlagen werden können.

Die meisten zahlentheoretischen Aussagen sind im Folgenden für die allgemeine Situation von Quotientenkörpern von Dedekindringen oder diskreten Bewertungsringen formuliert. Die hierbei übliche Voraussetzung, alle Restkörpererweiterungen seien separabel, ist bei den in dieser Arbeit betrachteten Funktionenkörpern erfüllt, da in diesem Fall die Restkörper endlich und damit perfekt sind.

A.1. Differente und Diskriminante

In diesem Abschnitt sei K der Quotientenkörper eines Dedekindrings A und $L|K$ eine endliche separable Körpererweiterung. Weiter setzen wir voraus, dass alle auftretenden Restkörpererweiterungen separabel sind. Es werden Begriffe und Schreibweisen im Zusammenhang mit Differente und Diskriminante einer solchen Erweiterung festgelegt. Des Weiteren werden Aussagen zu ihrer Berechnung wiederholt, die in dieser Arbeit verwendet werden.

Beweise und weitere Eigenschaften können beispielsweise bei [**Neu99**, III, Paragraph 2] nachgelesen werden.

A.1. Definition. Die **Differente** von L über K ist ein Divisor $\mathcal{D}_K^L$ in L. Sie ist definiert als das Inverse des dualen A-Moduls des Ganzheitsrings von L. Die in der multiplikativen Schreibweise des Divisors auftretenden Exponenten bezeichnen wir mit $d(\mathfrak{P}|\mathfrak{p})$, wenn $\mathfrak{P}$ eine Stelle von L über einer Stelle $\mathfrak{p}$ von K ist.

Wir nennen $d(\mathfrak{P}|\mathfrak{p})$ den **Differentenexponenten** von $\mathfrak{P}|\mathfrak{p}$.

A.2. Definition. Die **Diskriminante** $\mathfrak{D}_K^L$ von $L|K$ ist ein Divisor von K und ist definiert durch

$$\mathfrak{D}_K^L = N(\mathcal{D}_K^L),$$

wobei $N = N_K^L$ die Normabbildung von L nach K bezeichnet. Die Diskriminantenexponenten $\mathfrak{d}(\mathfrak{p})$ sind in der offensichtlichen Weise definiert.

A.3. Bemerkung. Der Diskriminantenexponent einer Stelle $\mathfrak{p}$ von K ist genau dann ungleich Null, wenn $\mathfrak{p}$ in $L|K$ verzweigt ist.

A.4. Bemerkung. Setzen wir zusätzlich voraus, dass die Körper L und K lokal sind mit maximalen Idealen $\mathfrak{P}|\mathfrak{p}$, so schreiben wir für den Differentenexponenten auch

$$d(\mathfrak{P}|\mathfrak{p}) = d(L|K).$$

Für den lokalen Diskriminantenexponenten $D_{L|K}$ gilt in diesem Fall

$$D_{L|K} = fd(L|K),$$

wenn $f = f_{L|K}$ den Trägheitsindex von $L|K$ bezeichnet.

A.5. Lemma. *Sei $M|L$ eine weitere endliche separable Körpererweiterung. Wir bezeichnen mit N_K^L die Normabbildung von L nach K. Dann erfüllen die Diskriminanten folgende Beziehung*

$$\mathfrak{D}_{M|K} = \mathfrak{D}_{L|K}^{[M:L]} N_K^L \left(\mathfrak{D}_{M|L}\right).$$

A.6. Lemma. *In der Situation von Lemma A.5 seien die betrachteten Körper lokal. Sei $f = f_{L|K}$ der Trägheitsindex von L über K. Dann gilt für die Diskriminantenexponenten*

$$D_{M|K} = [M : L]D_{L|K} + fD_{M|L}.$$

A.7. Satz. *Sei $\mathfrak{P}$ eine Stelle von L mit $K \cap \mathfrak{P} =: \mathfrak{p}$. Sei $e_{\mathfrak{P}|\mathfrak{p}}$ der Verzweigungsindex von $\mathfrak{P}|\mathfrak{p}$. Für den Differentenexponenten gilt genau dann*

$$d(\mathfrak{P}|\mathfrak{p}) = e_{\mathfrak{P}|\mathfrak{p}} - 1,$$

wenn $e_{\mathfrak{P}|\mathfrak{p}}$ teilerfremd ist zur Charakteristik von K.

A.2. Das Newton-Polygon

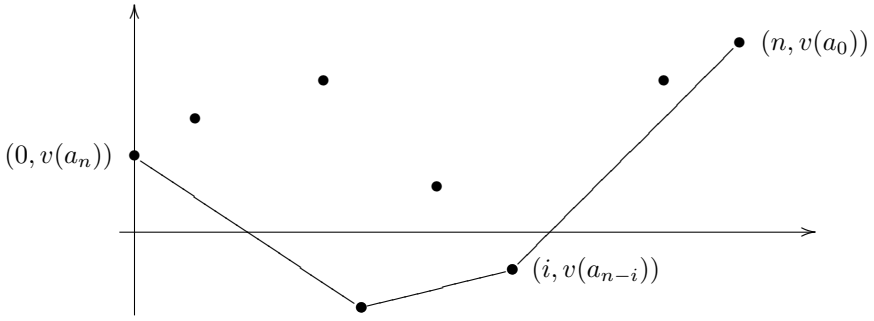
Das Newton-Polygon stellt ein Hilfsmittel dar, das es erlaubt, Aussagen über die Bewertungen der Nullstellen von Polynomen und Potenzreihen über vollständigen Körpern zu formulieren.

Die Eigenschaften im Polynomfall sind beispielsweise bei [**Neu99**, S. 145] gezeigt (allerdings in vertauschter Normierung). Weiter lassen sich die Aussagen, die in [**Kob84**, IV, Paragraph 4] für Potenzreihen über Komplettierungen von Zahlkörpern formuliert sind, direkt auf die Situation über beliebigen vollständig diskret bewerteten Körpern verallgemeinern.

A.8. Definition. Sei K ein vollständig diskret bewerteter Körper mit normierter Bewertung v und sei

$$f(X) = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in K[X]$$

ein Polynom mit $a_0 \neq 0 \neq a_n$. Für jeden Koeffizienten $a_i \neq 0$ tragen wir den Punkt $(i, v(a_{n-i})) \in \mathbb{R}^2$ in ein zweidimensionales Koordinatensystem ein. Anschließend bilden wir die untere konvexe Hülle dieser Punkte. Der entstehende Polygonzug heißt das **Newton-Polygon** von $f(X)$.



A.9. Satz. *In der Situation von Definition A.8 sei L der Zerfällungskörper von f über K. Die eindeutige Fortsetzung w von v auf L sei dabei so normiert, dass sie auf K mit v übereinstimmt.*

Ist das Geradenstück $[(i, v(a_{n-i})) : (j, v(a_{n-j}))]$ der Teil des Newton-Polygons mit Steigung m, so besitzt f genau $j-i$ Nullstellen $\alpha_1, \ldots, \alpha_{j-i}$ mit der Eigenschaft

$$w(\alpha_1) = \ldots = w(\alpha_{j-i}) = m.$$

A.10. Bemerkung. Anschaulich sagt Satz A.9 aus, dass jeder „Knick“ des Newton-Polygons einem Teiler von f in $K[X]$ entspricht, da die zugehörige Nullstellenmenge invariant unter der Operation der Galois-Gruppe ist. Umgekehrt kann jeder solche Teiler nur dann weiter zerfallen, wenn das zugehörige Teilstück des Newton-Polygons einen Punkt von $\mathbb{Z} \times \mathbb{Z}$ durchläuft, vergleiche dazu Satz A.12.

A.11. Bemerkung. Das Newton-Polygon lässt sich auch für Potenzreihen definieren. Seien K und v wie zuvor und

$$f(X) = 1 + \sum_{i \geq 1} a_i X^i \in K[[X]].$$

Das Newton-Polygon von f ist die untere konvexe Hülle der Punkte

$$(0,0), (a_1, v(a_1)), (a_2, v(a_2)), \ldots$$

wobei wiederum die Koeffizienten mit Bewertung ∞ ausgelassen werden. Dann gilt: Hat das Geradenstück des Newton-Polygons mit Steigung m die horizontale Länge l, so besitzt f genau l Nullstellen mit Bewertung $-m$.

Beachte an dieser Stelle die im Vergleich zum Polynomfall umgedrehte Reihenfolge der Knoten und das daraus resultierende vertauschte Vorzeichen der Bewertung.

A.3. Zur Beschreibung von Körpererweiterungen

Dieser Abschnitt enthält einige Aussagen, die im Hauptteil der Arbeit verwendet werden, um die Eigenschaften von Körpererweiterungen zu bestimmen.

Der folgende Satz stellt eine Verallgemeinerung des Irreduzibilitätskriteriums von Eisenstein dar.

A.12. Satz. *Sei K Quotientenkörper eines Dedekindrings. Alle Restkörpererweiterungen seien separabel. Betrachte ein Polynom*

$$f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$$

in $K[X]$. Existiert eine Stelle $\mathfrak{p}$ von K mit zugehöriger normierter Bewertung v, so dass eine der Bedingungen

(1) $v(a_n) = 0, \quad v(a_i) \geq v(a_0) > 0 \quad$ *für alle* $i = 1, \ldots, n-1$
und $ggT(n, v(a_0)) = 1$,

(2) $v(a_n) = 0, \quad v(a_i) \geq 0 \quad$ *für alle* $i = 1, \ldots, n-1, \quad v(a_0) < 0$
und $ggT(n, v(a_0)) = 1$

erfüllt ist, so ist $f(X)$ in $K[X]$ irreduzibel. In einer Körpererweiterung $K(u)|K$, die durch Adjunktion einer Nullstelle u von f entsteht, ist $\mathfrak{p}$ voll verzweigt.

Beweis. Der Beweis von [**Sti93**, Proposition III.1.14] gilt auch in der hier wiedergegebenen allgemeineren Situation. □

A.13. Satz. *Sei K Quotientenkörper eines vollständigen diskreten Bewertungsrings A. Der Restkörper von K sei perfekt. Betrachte eine endliche separable Körpererweiterung $L|K$ vom Grad n. Ist $L|K$ voll und zahm verzweigt, so existiert eine Uniformisierende ω von L, so dass $\pi := \omega^n$ eine Uniformisierende von K ist. Es gilt*

$$L = K(\omega).$$

Beweis. Siehe [**Lan70**, II, §5, Proposition 12]. □

A.14. Lemma. *Betrachte die Abbildung*

$$F : \mathbb{F}_{q^2} \longrightarrow \mathbb{F}_{q^2} \quad . \\ x \mapsto x^q$$

Dann gilt

$$\ker(F + id) = \mathrm{Im}(F - id).$$

Beweis. Im Ring der $\mathbb{F}_q$-Endomorphismen von $\mathbb{F}_{q^2}$ gilt

$$0 = F^2 - id = (F + id)(F - id).$$

Ist $u \in \mathrm{Im}(F - id)$, so existiert $v \in \mathbb{F}_{q^2}$ mit der Eigenschaft $v^q - v = u$. Da aber

$$(F + id)\left((F - id)(v)\right) = 0$$

gilt, liegt u in $\ker(F + id)$. Dies zeigt

$$\mathrm{Im}(F - id) \subset \ker(F + id). \tag{A.1}$$

Andererseits gilt nach dem Dimensionssatz für endlichdimensionale Vektorräume

$$\begin{aligned} \dim_{\mathbb{F}_q} \mathbb{F}_{q^2} &= \dim_{\mathbb{F}_q} \ker(F - id) + \dim_{\mathbb{F}_q} \mathrm{Im}(F - id) \\ &= \dim_{\mathbb{F}_q} \mathbb{F}_q + \dim_{\mathbb{F}_q} \mathrm{Im}(F - id), \end{aligned}$$

d.h. $\dim_{\mathbb{F}_q} \mathrm{Im}(F - id) = 1$. Also muss wegen (A.1) die Eigenschaft

$$\dim_{\mathbb{F}_q} \ker(F + id) \geq 1$$

erfüllt sein. Da $\ker(F + id)$ aber eine echte Teilmenge von $\mathbb{F}_{q^2}$ ist, folgt

$$\dim_{\mathbb{F}_q} \ker(F + id) = 1.$$

Somit gilt in (A.1) Gleichheit. □

A.15. Satz (Trivialer Fall des Lemmas von Hensel). *Sei K ein Körper, der bezüglich eines nicht-archimedischen Absolutbetrags $|.|$ vollständig ist. Sei A der zugehörige Bewertungsring mit maximalem Ideal $\mathfrak{p}$ und Restkörper $k = A/\mathfrak{p}$. Sei $f(X) \in A[X]$ ein Polynom, dessen Reduktion modulo $\mathfrak{p}$ nicht verschwindet. Das Polynom $f(X)$ besitze modulo $\mathfrak{p}$ eine Faktorisierung*

$$f(X) \equiv \overline{g}_1(X)\overline{g}_2(X) \mod \mathfrak{p}$$

mit teilerfremden Polynomen $\overline{g}_1(X), \overline{g}_2(X) \in k[X]$. Dann zerfällt auch f in ein Produkt

$$f(X) = g_1(X)g_2(X)$$

von Polynomen $g_1, g_2 \in A[X]$, die die Eigenschaften $\deg g_1 = \deg \overline{g}_1$ und

$$g_i(X) \equiv \overline{g}_i(X) \mod \mathfrak{p}, \quad i = 1, 2,$$

besitzen.

Beweis. Zum Beispiel [**Neu99**, II, Hensel's Lemma 4.6]. □

Die folgende Aussage gilt auch in allgemeineren Situationen, ist hier aber für den in der Arbeit verwendeten Funktionenkörper-Fall formuliert.

A.16. Satz (Kummer-Erweiterungen). *Sei L ein algebraischer Funktionenkörper mit Konstantenkörper k. Sei $n > 1$ eine natürliche Zahl, die teilerfremd zur Charakteristik von k ist. Sei $u \in L$ ein Element mit der Eigenschaft*

$$u \neq w^d \quad \text{für alle } w \in L \text{ und } d \mid n, d > 1.$$

Eine Erweiterung L' von L der Form

$$L' = L(y) \quad \text{mit } y^n = u$$

*heißt eine **Kummer-Erweiterung** von L.*

Es gilt: Das Polynom $\varphi(T) = T^n - u$ ist das Minimalpolynom von y über K. Die Erweiterung $L'|L$ ist galoissch vom Grad n mit zyklischer Galois-Gruppe.

BEWEIS. Siehe [**Sti93**, Proposition III.7.3]. □

A.4. Höhere Verzweigungstheorie

In diesem Abschnitt sei K ein lokaler vollständig diskret bewerteter Körper mit normierter Bewertung v_K, maximalem Ideal $\mathfrak{p}$ und Ganzheitsring $\mathcal{O}$. Wir setzen voraus, dass der Restkörper $\mathcal{O}/\mathfrak{p}$ perfekt ist.

Wir erinnern zunächst an das Konzept der höheren Verzweigungsgruppen, siehe dazu [**Ser79**, Kap. IV]. Anschließend werden wir mithilfe des Newton-Polygons und der in diesem Abschnitt wiederholten Eigenschaften der höheren Verzweigungsgruppen eine Beschreibung für Körpererweiterungen eines bestimmten Typs angeben.

A.17. DEFINITION (Höhere Verzweigungsgruppen). Sei $L|K$ eine galoissche Körpererweiterung mit Galois-Gruppe G. Sei v_L die normierte Fortsetzung von v_K auf L und x eine Uniformisierende von L. Das maximale Ideal von L bezeichnen wir mit $\mathfrak{P}$. Für $i \geq -1$ definieren wir

$$\begin{aligned} G_i &:= \{\sigma \in G \mid v_L(\sigma(x) - x) \geq i + 1\} \\ &= \left\{\sigma \in G \mid \sigma(x) \equiv x \bmod \mathfrak{P}^{i+1}\right\}. \end{aligned}$$

A.18. SATZ. *In der Situation von Definition A.17 gilt:*

(1) *Die Gruppen G_i bilden eine absteigende Folge von Normalteilern von G.*
(2) *Es ist $G_{-1} = G$ und G_0 ist die Trägheitsgruppe von $L|K$.*
(3) *Für hinreichend großes i ist G_i die triviale Gruppe.*

Insgesamt erhalten wir also

$$G = G_{-1} \supset G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_j = G_{j+1} = \ldots = \{1\}.$$

BEWEIS. Siehe [**Ser79**, IV, §1, Proposition 1]. □

A.19. LEMMA. *Der Index von G_1 in G_0 ist teilerfremd zur Charakteristik des Restkörpers von L.*

BEWEIS. Siehe [**Ser79**, IV, §2, Korollar 1]. □

A.20. SATZ. *Für den Differentenexponenten $d(L|K)$ gilt*

$$d(L|K) = \sum_{i=0}^{\infty} (\#G_i - 1).$$

Die Summe ist dabei endlich, da $\#G_i - 1 = 0$ gilt, wenn i hinreichend groß ist.

BEWEIS. Siehe [**Ser79**, IV, §1, Proposition 4]. □

A.21. SATZ. *Es gelte zusätzlich* $\operatorname{char} K = p > 0$. *Sei α ein normiertes separables $\mathbb{F}_p$-additives Polynom des Grades p^n in $\mathcal{O}[X]$, dessen Reduktion modulo $\mathfrak{p}$ separabel ist. Weiter sei* $\ker \alpha$ *in K enthalten. Für ein $b \in K$ mit $v_K(b) = -1$ betrachten wir eine Erweiterung L von K der Form*

$$L = K(y) \quad \text{mit } \alpha(y) = b.$$

Es gilt: Die Erweiterung $L|K$ ist galoissch und voll verzweigt vom Grad p^n. Die Galois-Gruppe ist kanonisch isomorph zu $\ker \alpha \cong (\mathbb{Z}/p\mathbb{Z})^n$. *Für den lokalen Differentenexponenten $d(L|K)$ gilt*

$$d(L|K) = 2p^n - 2.$$

BEWEIS. Das separable Polynom $\alpha(X) - b \in K[X]$ genügt den Bedingungen des zweiten Falls von Satz A.12. Dies liefert die Aussage über den Grad und das Verzweigungsverhalten von $L|K$. Sei $\mathfrak{P}$ das maximale Ideal in L. Bezeichnen wir mit v_L die normierte Fortsetzung von v_K auf L, so erhalten wir aus dem Newton-Polygon von $\alpha(X) - b$, dass

$$v_L(y) = -1$$

gilt. Das Element $x := y^{-1}$ ist somit eine Uniformisierende von L.

Wegen der Additivität von α unterscheiden sich zwei Nullstellen des Polynoms $\alpha(X) - b$ um ein Element von $\ker \alpha$. Da dieser Kern aber in K enthalten ist, ist L der Zerfällungskörper von $\alpha(X) - b$ über K und daher galoissch.

Die auf diese Weise erhaltene Beschreibung der Galois-Gruppe $G := \mathrm{Gal}(L|K)$ hängt nicht von den getroffenen Wahlen ab, sondern liefert die kanonische Beziehung

$$G = \ker \alpha.$$

Für $a \in \ker \alpha$ ist der zugehörige Galois-Automorphismus $\sigma_a \in G$ bestimmt durch

$$\sigma_a(y) = y + a.$$

Aus dem Newton-Polygon von α folgt wegen der Separabilität von $\alpha \bmod \mathfrak{p}$, dass jede Nullstelle von α Bewertung 0 besitzt.

Um den Differentenexponenten zu berechnen, bestimmen wir zunächst die höheren Verzweigungsgruppen. Da die Erweiterung $L|K$ voll verzweigt ist, gilt

$$G_{-1} = G_0 = G.$$

Nach Lemma A.19 ist der Index $[G_0 : G_1]$ teilerfremd zur Charakteristik p von K. Andererseits besitzt G_0 Ordnung p^n, was zur Folge hat, dass auch

$$G_1 = G$$

ist. Weiter gilt für ein Element $a \in \ker \alpha$ nach oben angegebener Beschreibung der Galois-Automorphismen in G

$$\begin{aligned}\sigma_a(x) = \sigma_a\left(\frac{1}{y}\right) = \frac{1}{y+a} &= \frac{1}{y\left(1+\frac{a}{y}\right)} \\ &= \frac{1}{y}\left(1 - \frac{a}{y} + \left(\frac{a}{y}\right)^2 - \dots\right) \\ &= x\left(1 - ax + a^2x^2 + \dots\right).\end{aligned}$$

Da wir bereits gezeigt haben, dass a Bewertung 0 besitzt, erhalten wir

$$\sigma_a(x) \equiv x - ax^2 \mod \mathfrak{P}^3.$$

Nach Definition der höheren Verzweigungsgruppen ist damit bereits

$$G_2 = \{0\}.$$

Mit Satz A.20 gelingt es uns also, den Differentenexponenten als

$$d(L|K) = (\#G_0 - 1) + (\#G_1 - 1) = 2(\#G - 1) = 2p^n - 2$$

zu bestimmen. □

A.5. Gruppentheorie

A.22. Satz. *Sei K ein Körper. Sei G eine Untergruppe von $\mathrm{GL}(n,K)$ mit $\mathrm{SL}(n,K) \subset G$. Ist $n \geq 3$ oder $\#K > 3$, so gilt für einen Normalteiler N von G*

$$\mathrm{SL}(n,K) \subset N$$

oder

$$N \subset \{aI \mid a \in K^*\} =: Z,$$

wobei I die $n \times n$-Einheitsmatrix bezeichnet, d.h. Z ist das Zentrum von $\mathrm{GL}(n,K)$.

Beweis. Siehe [**Hup67**, S. 185]. □

A.23. Bemerkung. Sei $\mathbb{F}_l$ der endliche Körper mit l Elementen. Es existiert eine (unkanonische) Einbettung der quadratischen Körpererweiterung $\mathbb{F}_{l^2}$ von $\mathbb{F}_l$ in den Ring der 2×2-Matrizen über $\mathbb{F}_l$.

Unter einer solchen Einbettung entspricht die multiplikative Gruppe $\mathbb{F}_{l^2}^*$ einer zyklischen Untergruppe der Ordnung $l^2 - 1$ von $\mathrm{GL}(2, \mathbb{F}_l)$.

Symbolverzeichnis

$\mathbb{N}$	die natürlichen Zahlen $1, 2, 3, \ldots$
$\mathbb{N}_0$	die natürlichen Zahlen mit 0
$\mathbb{Z}$	der Ring der ganzen Zahlen
$\mathbb{Q}$	der Körper der rationalen Zahlen
$\mathbb{R}$	der Körper der reellen Zahlen
$\mathbb{C}$	der Körper der komplexen Zahlen
$R[X]$	der Polynomring über dem Ring R
$R[[X]]$	der Ring der formalen Potenzreihen über dem Ring R
$F(X)$	der rationale Funktionenkörper über dem Körper F
$F((X))$	der Körper der formalen Laurent-Reihen über dem Körper F
$\mathrm{GL}(n, R)$	die Gruppe der invertierbaren $n \times n$-Matrizen über dem Ring R, die „allgemeine lineare Gruppe"
$\mathrm{SL}(n, R)$	die Gruppe der invertierbaren $n \times n$-Matrizen mit Determinante 1 über dem Ring R, die „spezielle lineare Gruppe"
q	eine Primzahlpotenz, Seite 7
$\mathbb{F}_q$	der endliche Körper mit q Elementen, Seite 7
A	der Ring $\mathbb{F}_q[T]$, Seite 7
K	der rationale Funktionenkörper $\mathbb{F}_q(T)$, Seite 7
$\mathbb{P}_L$	die Menge der Stellen eines Körpers L, Seite 7
K_P	die Komplettierung von K an einer Stelle P, Seite 7
$\mathcal{O}_{K_P}$	der Ganzheitsring von K_P, Seite 7
K^{sep}	der separabel algebraische Abschluss von K, Seite 7
τ	die Abbildung $x \mapsto x^q$; entspricht X^q für eine Unbestimmte X, Seite 7
$L\{\tau\}$	der nicht-kommutative Polynomring in τ über L, Seite 7
Φ_a	das Bild von $a \in A$ unter einem Drinfeld-Modul Φ, Seite 8
${}_a\Phi$	$:= \ker \Phi_a$, $a \in A$, die a-Torsion von Φ, Seite 8
$\mathcal{C}$	die Komplettierung eines algebraischen Abschlusses von K_∞, Seite 8
e_Λ	die Exponentialfunktion eines Gitters $\Lambda \subset \mathcal{C}$, Seite 9
$\mathfrak{p}$	eine endliche Stelle von K; entspricht eineindeutig einem normierten Primpolynom in $A[X]$, Seite 13
d	der Grad von $\mathfrak{p}$, Seite 13
$\mathbb{F}_\mathfrak{p}$	der Restkörper $A/\mathfrak{p}$, Seite 14
$G_\mathfrak{p}$	die lokale Galois-Gruppe an $\mathfrak{p}$; im supersingulären Fall, Seite 21 im ordinären Fall, Seite 30
G_∞	die lokale Galois-Gruppe an ∞, Seite 42
$\mathcal{D}_K^L$	die Differente der Erweiterung $L\|K$, Seite 59
$d(\mathfrak{P}\|\mathfrak{p})$	der Differentenexponent einer Stelle $\mathfrak{P}\|\mathfrak{p}$ von L, Seite 59
$\mathfrak{D}_K^L$	die Diskriminante von $L\|K$, Seite 59
$\mathfrak{d}(\mathfrak{p})$	der Diskriminantenexponent einer Stelle $\mathfrak{p}$ von K, Seite 59
$d(L\|K)$	der Differentenexponent einer lokalen Erweiterung $L\|K$, Seite 59
$D_{L\|K}$	der Diskriminantenexponent einer lokalen Erweiterung $L\|K$, Seite 59

Literaturverzeichnis

[BGR84] S. Bosch, U. Güntzer, and R. Remmert, *Non-Archimedean analysis*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 261, Springer-Verlag, Berlin, 1984, A systematic approach to rigid analytic geometry. MR MR746961 (86b:32031)

[Gek91] Ernst-Ulrich Gekeler, *On finite Drinfel′d modules*, J. Algebra **141** (1991), no. 1, 187–203. MR MR1118323 (92e:11064)

[Gek08] ———, *Frobenius distributions of Drinfeld modules over finite fields*, Trans. Amer. Math. Soc. **360** (2008), no. 4, 1695–1721. MR MR2366959 (2008m:11114)

[Gos96] David Goss, *Basic structures of function field arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], vol. 35, Springer-Verlag, Berlin, 1996. MR MR1423131 (97i:11062)

[Hup67] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin, 1967. MR MR0224703 (37 #302)

[Kob84] Neal Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, second ed., Graduate Texts in Mathematics, vol. 58, Springer-Verlag, New York, 1984. MR MR754003 (86c:11086)

[Lan70] Serge Lang, *Algebraic number theory*, Addison-Wesley Publishing Co., Inc., Reading, Mass.-London-Don Mills, Ont., 1970. MR MR0282947 (44 #181)

[LN97] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn. MR MR1429394 (97i:11115)

[Neu99] Jürgen Neukirch, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder. MR MR1697859 (2000m:11104)

[Pin97] Richard Pink, *The Mumford-Tate conjecture for Drinfeld-modules*, Publ. Res. Inst. Math. Sci. **33** (1997), no. 3, 393–425. MR MR1474696 (98f:11062)

[Ser73] J.-P. Serre, *A course in arithmetic*, Springer-Verlag, New York, 1973, Translated from the French, Graduate Texts in Mathematics, No. 7. MR MR0344216 (49 #8956)

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg. MR MR554237 (82e:12016)

[Sti93] Henning Stichtenoth, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993. MR MR1251961 (94k:14016)