Galoisdarstellungen auf den Torsionspunkten von Drinfeld-Moduln des Rangs zwei

Dissertation
zur Erlangung des Grades
des Doktors der Naturwissenschaften
der Naturwissenschaftlich-Technischen Fakultät I
der Universität des Saarlandes

von
Maximilian Gebhardt

Saarbrücken
2003

Tag des Kolloquiums:	24. Juli 2003
Dekan:	Prof. Dr. Philipp Slusallek
Berichterstatter:	Prof. Dr. Ernst-Ulrich Gekeler
	Prof. Dr. Rainer Schulze-Pillot-Ziemen

Inhaltsverzeichnis

[Number theory] shares in common with the natural sciences the property that it is a strongly experimental subject.

Henri Cohen, Computational Aspects of Number Theory

Einleitung

Seit der Dissertation von Emil Artin im Jahre 1923 stellen Funktionenkörper ein zentrales Gebiet der Algebra und Zahlentheorie dar. (Hier und im folgenden verstehe ich unter einem Funktionenkörper eine algebraische Erweiterung von $\mathbb{F}_q(T)$ mit vollem Konstantenkörper $\mathbb{F}_q$.) Ersetzt man das Paar $(\mathbb{Q}, \mathbb{Z})$ durch $(\mathbb{F}_q(T), \mathbb{F}_q[T])$, so ergeben sich tiefe Parallelen zwischen der klassischen Zahlentheorie und der Theorie der Funktionenkörper. Es seien nur Klassenkörpertheorie, Modulformen und die Arithmetik von Zeta- und L-Funktionen erwähnt. Daher erfordert das Verständnis der "zahlentheoretischen" Situation ein gutes Verständnis der Funktionenkörpersituation und umgekehrt. Dabei ist die Funktionenkörpersituation in vielen Fällen einfacher, da es keine nichtarchimedischen Stellen gibt und viele Informationen aus der Untersuchung des Frobeniusendomorphismus $x \mapsto x^q$ gewonnen werden können. Viele berühmte Vermutungen der klassischen Zahlentheorie sind für Funktionenkörper bewiesen.

Weiterhin sind gerade in den letzten Jahren die Funktionenkörper durch ihre Anwendungen in der Kodierungstheorie [Sti93] und Kryptographie [SSW96] ins Zentrum des Interesses gerückt.

In all diesen Zusammenhängen stellen die von V.G. Drinfeld in seiner folgenreichen Arbeit [Dri74] eingeführten Drinfeld-Moduln ein zentrales Werkzeug zur Untersuchung der Arithmetik solcher Funktionenkörper dar. Ausgangspunkt ist die Beobachtung, daß die additive Gruppe $\mathbb{G}_a(L)$ eines Körpers L der Charakteristik p "viele" Endomorphismen besitzt und deshalb nichttriviale Modulstrukturen zuläßt. Grob gesagt ist ein Drinfeld A-Modul (für einen geeigneten Ring A der Charakteristik p) über L eine A-Modul-Struktur (mit einigen zusätzlichen Eigenschaften) der additiven Gruppe von L. Der Rang eines Drinfeld-Moduls ist eine natürliche Zahl, welche die Torsionsstruktur von $\mathbb{G}_a(\bar{L})$ beschreibt ($\bar{L}$ ist der algebraische Abschluß von L). In vielerlei Hinsicht entspricht das Konzept des Drinfeld-Moduls dem Konzept der elliptischen Kurve (bzw. der irreduziblen abelschen Varietät) in der Zahlentheorie über $\mathbb{Q}$. Im weiteren werden wir uns auf den einfachsten Fall $A = \mathbb{F}_q[T]$ beschränken.

Der einfachste Drinfeld-Modul wurde schon in den 30er Jahren von Leonard Carlitz eingeführt und trägt daher heute den Namen Carlitz-Modul. Mit seiner Hilfe können unter anderem galoissche Körpererweiterungen von $\mathbb{F}_q(u)$ explizit konstruiert werden, deren Struktur analog zur Struktur der Kreisteilungserweiterun-

gen über $\mathbb{Q}$ ist. Zum Beispiel ist die Galoisgruppe solcher ,,Carlitz-Erweiterungen" von der Form $(\mathbb{F}_q[T]/\mathfrak{n}(T))^*$ in Analogie zur Galoisgruppe einer Kreisteilungserweiterung $(\mathbb{Z}/n)^*$.
In den letzten Jahren wurden solche Carlitz-Erweiterungen verwendet, um explizit globale Funktionenkörper über $\mathbb{F}_q$ zu konstruieren, für die der Quotient $\frac{N}{g}$ zwischen Anzahl der Stellen vom Grad 1 und dem Geschlecht sehr groß ist. Man vergleiche zum Beispiel die Arbeiten [NX97, Kel01, Geb02] oder [vdGvdV00, vdGvdV03]. Explizit bedeutet in diesem Zusammenhang immer, daß man Polynome angeben kann, deren Nullstellen die Funktionenkörper erzeugen. Solche Funktionenkörper und ihre explizite Beschreibung sind in der Kodierungstheorie von Interesse. Nun besagt aber ein Resultat von Frey, Perret und Stichtenoth [FPS92], daß in jedem abelschen, unendlichen Turm $K_1 \subset K_2 \subset K_3 \ldots$ von Funktionenkörpern über $\mathbb{F}_q$ für den Quotienten $\lim_{i\to\infty} \frac{N(K_i)}{g(K_i)} = 0$ gilt. Da die Torsionserweiterungen von Rang-1 Drinfeld-Moduln immer abelsch sind [Hay79], besagt das obige Theorem, daß diese Klasse von Erweiterungen ein asymptotisch schlechtes Verhalten aufweist. Andererseits besagt ein Resultat von Serre [Ser83], daß es einen unendlichen (notwendigerweise nichtabelschen) Körperturm und eine Konstante $c(q) > 0$ gibt mit $\liminf \frac{N(K_i)}{g(K_i)} \geq c(q)$. Deshalb bietet es sich an, nichtabelsche Torsionserweiterungen zu betrachten, d.h. Torsionserweiterungen von Drinfeld-Moduln vom Rang echt größer eins.
Richard Pink hat in [Pin97] gezeigt, daß für einen Rang-r Drinfeld-Modul ϕ "generisch" die Galoisgruppe der Torsionserweiterung $\mathrm{Gal}(L({}_{\mathfrak{l}^\infty}\phi)|L)$ offen in der Gruppe $\mathrm{GL}(r, A_{\mathfrak{l}})$ ist, wobei $A_{\mathfrak{l}}$ die Komplettierung von A an einer Primstelle $\mathfrak{l}$ bezeichnet. Sein Schüler Francis Gardeyn hat diese Aussage in seiner Dissertation im Fall $\mathrm{rang}(\phi) = 2$ von der Komplettierung $A_{\mathfrak{l}}$ auf den Adelring übertragen. Meistens wird die Galoisgruppe einer $\mathfrak{l}$-Torsionserweiterung also gleich $\mathrm{GL}(r, A/\mathfrak{l})$ sein.
Die Beweise sind aber nicht konstruktiv, so daß für einen konkret gegebenen Drinfeld-Modul ϕ und $\mathfrak{l} \in \mathbb{F}_q[T]$ keine Aussagen gemacht werden können. Daher beschäftigt sich die vorliegende Arbeit mit der Berechnung der Galoisgruppe einer $\mathfrak{l}$-Torsionserweiterung eines Rang-2 Drinfeld-Moduls. Um explizit rechnen zu können, beschränken wir uns dabei auf Drinfeld-Moduln über dem Ring $A = \mathbb{F}_q[T]$, die über dem rationalen Funktionenkörper $\mathbb{F}_q(u)$ definiert sind.
In diesem Fall kann ein Rang-2 Drinfeld-Modul ϕ durch die Daten

$$\phi = (\mathbb{F}_q, \mathbb{F}_q(u), i_\phi(T), i_\phi(T) + g\tau + \Delta\tau^2)$$

beschrieben werden, wobei $i_\phi : \mathbb{F}_q[T] \to \mathbb{F}_q(u)$ der Strukturmorphismus, $\tau : x \mapsto x^q$ die Frobeniusabbildung und $i_\phi(T) + g\tau + \Delta\tau^2 \in \mathbb{F}_q(u)\{\tau\}$ das Bild ϕ_T von T im getwisteten Polynomring ist. Die von ϕ auf $\mathbb{F}_q(u)^{sep}$ induzierte $\mathbb{F}_q[T]$-Modulstruktur wird mit $*_\phi$ bezeichnet. Zu einem irreduziblen $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ bildet die $\mathfrak{l}$-Torsion ${}_{\mathfrak{l}}\phi = \{\alpha \in \mathbb{F}_q(u)^{sep} \mid \mathfrak{l} *_\phi \alpha = 0\}$ einen $\mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u))$-invarianten $\mathbb{F}_q[T]$-Untermodul von $\mathbb{F}_q(u)^{sep}$, der als $\mathbb{F}_{\mathfrak{l}} := \mathbb{F}_q[T]/\mathfrak{l}$ Vektorraum

Dimension 2 hat. Da $*_\phi$ mit der Galoisoperation kommutiert, induziert letztere die $\mathfrak{l}$-Torsionsdarstellung

$$\rho_{\phi,\mathfrak{l}}^{red} : \mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u)) \to \mathrm{Aut}_{\mathbb{F}_\mathfrak{l}}({}_\mathfrak{l}\phi) \cong \mathrm{GL}(2, \mathbb{F}_\mathfrak{l}) \ .$$

Nach Wahl einer Basis des freien zweidimensionalen Moduls ${}_\mathfrak{l}\phi$ betrachten wir den letzten Isomorphismus als Identifikation. Dann ist die folgende Frage zu klären: Gilt die Gleichheit

$$\boxed{\mathrm{Im}(\rho_{\phi,\mathfrak{l}}^{red}) \stackrel{?}{=} \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})}$$

Da

$$\begin{aligned} \mathrm{Im}(\rho_{\phi,\mathfrak{l}}^{red}) &\cong \mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u))/\mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u)[{}_\mathfrak{l}\phi]) \\ &\cong \mathrm{Gal}\,(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) \end{aligned}$$

gilt, kann man die Frage umformulieren zu:
Entscheide, ob

$$\boxed{\mathrm{Gal}\,(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) \stackrel{?}{=} \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})}$$

gilt. Der Körper $\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]$ ist der Zerfällungskörper des Polynoms

$$\phi_\mathfrak{l}(x) \in \mathbb{F}_q(u)[x] \ .$$

Es ist also die Galoisgruppe eines Polynoms in x auszurechnen. Da aber $\deg_x(\phi_\mathfrak{l}) = q^{2\deg_T(\mathfrak{l})}$ ist, wird der Grad solcher Polynome sehr schnell sehr groß, so daß eine Berechnung der Galoisgruppe ohne Berücksichtigung der speziellen Struktur (z.B. Additivität) der Polynome aussichtslos ist.
Wir haben einen Algorithmus $\mathcal{A}$ entwickelt und im Computer-Algebra-System Simath [Sim] implementiert, der entscheidet, ob $\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]\,, \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ gilt (s. Kapitel 5).
Indem wir eine schwache (aber explizite) Abschätzung der Differenten von $\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]|\mathbb{F}_q(u)$ herleiten, liefert uns die explizite Version des Satzes von Chebotarev eine Schranke $N \in \mathbb{N}$, die die maximale Anzahl von Schritten bis zur Terminierung abschätzt. Insgesamt erhalten wir dann:

$$\begin{array}{c}\text{Der Algorithmus terminiert} \\ \text{in } N \text{ Schritten}\end{array} \iff \Big(\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]\,, \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})\Big)$$

Konkrete Rechnungen lassen vermuten, daß die Schranke N um mehrere Größenordnungen zu schlecht ist. Daher haben wir für konkrete Berechnungen ein $N_1 \ll N$ gewählt, und den Algorithmus nach N_1 Schritten abgebrochen. In diesem Fall gilt natürlich nur noch die Implikation "$\Rightarrow$".
Dem Algorithmus $\mathcal{A}$ liegt folgende Idee zu Grunde:

(i) Wir beschaffen uns Informationen über einige Elemente in der Galoisgruppe. Dazu müssen wir die Elemente nicht exakt berechnen. Zu einigen Stellen $\mathfrak{p}(u)$ aus $\mathbb{P}_{\mathbb{F}_q[u]}$ ermitteln wir das charakteristische Polynom und die Ordnung des zugehörigen Frobenius $\mathrm{Frob}(\mathfrak{p}, \mathbb{F}_q(u)[_\mathfrak{l}\phi]|\mathbb{F}_q(u)) \in \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$. Diese sind wohldefiniert, obwohl der Frobenius selbst nur bis auf Konjugation bestimmt ist. Im Fall der $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ genügen diese beiden Daten, um den Konjugationstyp zu bestimmen.

(ii) Wir betrachten die kanonische Abbildung

$$P : \mathrm{GL}(2, \mathbb{F}_\mathfrak{l}) \to \mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$$

und die Klassifikation der maximalen Untergruppen von $\mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$. Unter Verwendung der Informationen aus (i) zeigen wir für jede maximale Untergruppe U von $\mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$

$$P(\mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u))) \nsubseteq U$$

und erhalten damit $P(\mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u))) = \mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$.

(iii) Wir zeigen

$$\det(\mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u))) = \mathbb{F}_\mathfrak{l}^* .$$

(iv) Aus (ii) und (iii) folgern wir

$$\mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l}) .$$

Im Fall von elliptischen Kurven $E|\mathbb{Q}$ wird ähnlich vorgegangen, um zu einem $l \in \mathbb{P}$ die Galoisgruppe der l-Torsionserweiterung $\mathbb{Q}(_lE)|\mathbb{Q}$ zu untersuchen. In Abschnitt 1.11 gehen wir genauer auf die Analogie zwischen Drinfeld-Moduln und elliptischen Kurven ein.

Die Arbeit gliedert sich wie folgt auf:
Im 1. Kapitel wird ein kurzer Abriß der Theorie der Drinfeld-Moduln gegeben. Dabei beschränken wir uns von Anfang an auf den Fall $A = \mathbb{F}_q[T]$. Resultate werden nicht in ihrer allgemeinsten Form zitiert, sondern so, wie sie für die späteren konkreten Rechnungen benötigt werden.
In Kapitel 2 betrachten wir endliche Drinfeld-Moduln. Einem endlichen Rang-r Drinfeld-Modul $\bar{\phi}$ kann ein charakteristisches Polynom $\mathcal{P}_{\bar{\phi}}(X) \in (\mathbb{F}_q[T])[X]$ vom Grad r zugeordnet werden. Dies ist das Analogon zum Polynom $X^2 + (p+1-\#E(\mathbb{F}_p))\,X + p \in \mathbb{Z}[X]$ im Fall einer endlichen elliptischen Kurve $E|\mathbb{F}_p$. Wir geben an, wie man $\mathcal{P}_{\bar{\phi}}(X)$ im Fall $r = 2$ unter Verwendung der Deligne-Kongruenz für Drinfeld-Moduln schnell berechnen kann. Im Fall eines globalen Drinfeld-Moduls ϕ erhalten wir dann zu Stellen $\mathfrak{p} \neq \mathfrak{l}$ guter Reduktion mittels

$$\mathrm{charpol}\big(\mathrm{Frob}(\mathfrak{p}, \mathbb{F}_q(u)[_\mathfrak{l}\phi]|\mathbb{F}_q(u))\big) = \mathcal{P}_{\mathrm{Dred}(\phi,\mathfrak{p})} \bmod \mathfrak{l}$$

das charakteristische Polynom des Frobenius zur Stelle $\mathfrak{p}$.
Die Gruppen $\mathrm{GL}(2, \mathbb{F}_r)$ und $\mathrm{PGL}(2, \mathbb{F}_r)$ über einem beliebigen endlichen Körper $\mathbb{F}_r$ werden in Kapitel 3 genauer beleuchtet. Die dortigen Untersuchungen sind rein gruppentheoretischer Natur, die Theorie der Drinfeld-Moduln geht nicht ein. Wir benutzen die Konjugationstypen in der $\mathrm{GL}(2, \mathbb{F}_r)$, um ein Vertretersystem der Konjugationstypen der $\mathrm{PGL}(2, \mathbb{F}_r)$ zu erhalten. Unter Verwendung der Klassifikation der maximalen Untergruppen der $\mathrm{PGL}(2, \mathbb{F}_r)$ geben wir Kriterien an, mit denen man jeweils ausschließen kann, daß ein Element $[M] \in \mathrm{PGL}(2, \mathbb{F}_r)$, das nur bis auf Konjugation bekannt ist, in einer vorgegebenen maximalen Untergruppe liegt. Unsere Resultate gelten in jeder Charakteristik und schließen auch die Fälle von kleinen endlichen Körpern ($\mathrm{PGL}(2, \mathbb{F}_2), \mathrm{PGL}(2, \mathbb{F}_3)$ etc.) ein.
In Kapitel 4 wenden wir uns der Körpererweiterung $\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]|\mathbb{F}_q(u)$ zu. Wir geben eine (sehr schwache, aber explizite) obere Abschätzung für Differente und Geschlecht der Erweiterung an. Weiter zeigen wir, daß Torsionserweiterungen mit maximaler Galoisgruppe $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ im Fall $\mathbb{F}_{\mathfrak{l}} \neq \mathbb{F}_2$ keine Konstantenerweiterungen enthalten. Wir beleuchten Situationen (rationale Isogenien, Drinfeld-Moduln mit komplexer Multiplikation), in denen die Torsionserweiterung nicht maximal sein kann. In diesem Zusammenhang leiten wir eine Weil-Paarung für Drinfeld-Moduln her. Mit ihrer Hilfe bringen wir die Galoisoperation auf der $\mathfrak{l}(T)$-Torsion eines Rang-2 Drinfeld-Moduls $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ mit der zugehörigen Operation auf der $\mathfrak{l}$-Torsion des Rang-1 Moduls $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau)$ in Verbindung. Insbesonders folgern wir, daß immer $\mathbb{F}_q(u)[_{\mathfrak{l}}\psi] \subseteq \mathbb{F}_q(u)[_{\mathfrak{l}}\phi]$ gilt. Dies liefert uns ein einfaches Kriterium (Satz 4.4.11), das in vielen Fällen zeigt, daß $\det(\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))) = \mathbb{F}_{\mathfrak{l}}{}^*$ gilt.
Unter Verwendung der Tate-Uniformisierung von Drinfeld-Moduln können wir zeigen, daß in Abhängigkeit vom Verhalten an Stellen schlechter Reduktion Elemente der Form $\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ mit $a \neq 0$ in der Galoisgruppe liegen.
In diesem Zusammenhang tritt der häufig zu beobachtende Effekt auf, daß unter der Analogie zwischen $\mathbb{Q}$ und $\mathbb{F}_q(u)$ ein Objekt über $\mathbb{Q}$ zu mehreren Objekten über $\mathbb{F}_q(u)$ korrespondiert. Klassisch wird eine elliptische Kurve $E|\mathbb{Q}$ sowohl über die Weil-Paarung als auch über die Tate-Uniformisierung zur $\mathbb{Z}$-Modulstruktur $z * q := q^z$ von $\overline{\mathbb{Q}}^*$ in Verbindung gebracht. Demgegenüber liefert im Fall von Drinfeld-Moduln die Weil-Paarung einen Zusammenhang zwischen den Moduln $(\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ und $(\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau)$, während die Tate-Uniformisierung eine Verbindung zwischen $(\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ und $(\mathbb{F}_q, \mathbb{F}_q(u), u, u + \tau)$ herstellt.
Im 5. Kapitel setzten wir die Ergebnisse aus den vorherigen Kapiteln zum Algorithmus $\mathcal{A}$ zusammen, der zu vorgegebenem $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ und $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ entscheidet, ob $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ gilt. Dazu führen wir den Begriff eines Schaltgraphen ein und definieren einen speziellen Schaltgraphen, in dem wir die gruppentheoretischen Ergebnisse aus Kapitel 3 kodieren. Dadurch sind im Algorithmus die gruppentheoretischen Anteile von denen aus der Theorie der Drinfeld-Moduln getrennt. Dies erhöht die Übersichtlichkeit des

Algorithmus, da für die $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ einige Sonderfälle beachtet werden müssen ($\#\mathbb{F}_\mathfrak{l}$ klein oder $\mathrm{char}(\mathbb{F}_q) = 2$), während die Resultate über Drinfeld-Moduln (Berechnung des charakteristischen Polynoms eines Frobeniuselements etc.) unabhängig von diesen sind.
Im 6. Kapitel geben wir die Resultate einiger Beispielrechnungen an. Diese haben wir mit einer Modifikation $\mathcal{A}'$ von $\mathcal{A}$ durchgeführt, in der wir die maximale Anzahl der betrachteten $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$ auf 60 beschränkt haben. $\mathcal{A}'$ ist schneller als $\mathcal{A}$, kann aber nicht mehr beweisen, daß $\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ ist. Mit $\mathcal{A}'$ haben wir für $\mathbb{F}_q = \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_4, \mathbb{F}_5$ größere Parameterbereiche abgesucht. Die Rechnungen zeigten, daß der Algorithmus i.a. nur wenige unverzweigte Stellen von $\mathbb{F}_q(u)$ (weniger als 10) berechnen muß, um die Maximalität der Galoisgruppe zu zeigen. Im Fall von $\mathbb{F}_q = \mathbb{F}_3$ haben wir in den Fällen, in denen die Maximalität nicht gezeigt werden konnte, die Galoisgruppe ,,von Hand" bestimmt. In diesen Fällen war die Gruppe immer echt kleiner als $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$. Der Übergang von $\mathcal{A}$ zu $\mathcal{A}'$ hat also in diesen Fällen zu keiner Verschlechterung der Ergebnisse geführt. Die gefundenen nichtmaximalen Fälle sind in Tabelle 6.2 zusammengefaßt. In Abschnitt 6.3 werden kurz mögliche Verallgemeinerungen des hier behandelten Problems angesprochen.

Herrn Prof. Dr. E.-U. Gekeler gilt mein Dank für das interessante Thema und die gute Betreuung. Auch Frau Dipl. Math. Alice Keller möchte ich für die jahrelange gute Zusammenarbeit danken. Ein besonderer Dank gilt Frau Dipl. Math. Ute Staemmler, nicht nur für die viele Zeit, die sie zum Korrekturlesen dieser Arbeit verwendet hat.

Kapitel 1

Grundlagen

In diesem Kapitel stellen wir kurz den für diese Arbeit relevanten Teil der Theorie der Drinfeld-Moduln dar. Da der algorithmische Aspekt später eine große Rolle spielen wird, definieren wir Drinfeld-Moduln nur für den Ring $\mathbb{F}_q[T]$. Für allgemeinere Ordnungen A ist die Repräsentation eines Drinfeld-Moduls bereits ein nichttriviales Problem. Außerdem ist in vielen Computeralgebrasystemen zwar die Arithmetik von $\mathbb{F}_q[T]$ implementiert, nicht aber die Arithmetik solcher allgemeinerer „Drinfeld-Ringe".
Wenn wir Resultate (insbesondere zu Drinfeld-Moduln) anderer Mathematiker zitieren, so geben wir sie nicht unbedingt in ihrer allgemeinsten Form an, sondern so konkret, wie wir die Ergebnisse benötigen. Zum Beispiel werden wir häufig Aussagen zu Rang-2 Drinfeld-Moduln zitieren, die für beliebige Rang-r Drinfeld-Moduln gelten.
Umfassendere Einführungen in die Theorie der Drinfeld-Moduln finden sich in vielen der im Literaturverzeichnis angegebenen Arbeiten, z.B. in [Hay92], [Ros02] oder [Gos96].

1.1 Notation

Wir werden in der ganzen Arbeit die folgende Notation verwenden:

$\mathbb{Z}$	:	Menge der ganzen Zahlen,
$\mathbb{N}_0$	:	Menge der natürlichen Zahlen einschließlich der Null,
$\mathbb{N}$	:	$\mathbb{N}_0 - \{0\}$,
$\mathbb{P}$	:	$\{2, 3, 5, 7, \ldots\}$ Menge der Primzahlen,
$\mathbb{F}_q$	:	der endliche Körper mit q Elementen,
$\mathbb{F}_q[T]$	:	der Polynomring über $\mathbb{F}_q$ in der Unbestimmten T,
$\mathfrak{n}$	:	ein beliebiges Polynom aus $\mathbb{F}_q[T]$,
$\mathbb{F}_q(T)$	:	der rationale Funktionenkörper in der Unbestimmten T,

$\mathbb{P}_{\mathbb{F}_q[T]}$	:	die Menge der nichtkonstanten normierten irreduziblen Polynome in $\mathbb{F}_q[T]$,
$\mathfrak{l}$	:	ein Element von $\mathbb{P}_{\mathbb{F}_q[T]}$,
$\mathrm{v}_{\mathfrak{l}}$	:	die normierte Bewertung an $\mathfrak{l}$,
$\mathbb{F}_{\mathfrak{l}}$	:	der endliche Körper $\mathbb{F}_q[T]/\mathfrak{l}$,
$\mathbb{F}_q[T]_{\mathfrak{l}}$	:	die Komplettierung von $\mathbb{F}_q[T]$ an $\mathfrak{l}$,
$\mathbb{F}_q(T)_{\mathfrak{l}}$	:	der Quotientenkörper von $\mathbb{F}_q[T]_{\mathfrak{l}}$,
$\mathrm{Gal}(L,K)$	:	die Galoisgruppe einer galoisschen Körpererweiterung $L\|K$,
$\bar{L}$	:	der algebraische Abschluß eines Körpers L,
L^{sep}	:	der separable Abschluß eines Körpers L.

Im weiteren werden wir die Primideale von $\mathbb{F}_q[T]$ mit ihren Erzeugern aus $\mathbb{P}_{\mathbb{F}_q[T]}$ identifizieren.
Sei $f(v) = \sum_{i=0}^{n} a_i v^i$ ein Polynom in der Variablen v. Dann bezeichnet

$$\mathrm{coeff}_v(k, f) := a_k$$

den k-ten Koeffizienten.
Sei K ein beliebiger Körper. Dann heißt eine Körpererweiterung $L|K$ mit Transzendenzgrad größer oder gleich eins *Funktionenkörper*. Ist der Transzendenzgrad genau Eins, so heißt $L|K$ *algebraischer Funktionenkörper*. Ein *globaler Funktionenkörper* ist ein algebraischer Funktionenkörper $L|K$, bei dem K endlich ist. Globale Funktionenkörper werden auch *Kongruenzfunktionenkörper* genannt. Die Grundlagen der Theorie der algebraischen Funktionenkörper unter besonderer Berücksichtigung der globalen Funktionenkörper werden z.B. in [Sti93] oder [Ros02] dargestellt. Die Stellenmenge eines algebraischen Funktionenkörpers $L|K$ werden wir mit S_L bezeichnen. Zum Beispiel ist

$$S_{\mathbb{F}_q(T)} = \mathbb{P}_{\mathbb{F}_q[T]} \,\dot{\cup}\, \{T^{-1}\} \ .$$

1.2 Der getwistete Polynomring

Sei im weiteren L ein Erweiterungskörper von $\mathbb{F}_q$ und

$$M := \left\{ \sum_{i=0}^{n} c_i x^{q^i} \mid n \in \mathbb{N}_0, c_i \in L \right\} \quad .$$

Dann ist M zwar unter der Addition von $L[x]$ abgeschlossen, nicht aber unter der Multiplikation von Polynomen. Also ist M kein Teilring des Polynomrings $(L[x], +, \cdot)$.
Es gilt aber

Lemma 1.2.1. *Mit den Verknüpfungen*

$$\begin{array}{rcrcl} + & : & (P+H)(x) & := & P(x)+H(x) \\ \circ & : & (P\circ H)(x) & := & P(H(x)) \end{array}$$

ist $(M,+,\circ)$ *ein nicht-kommutativer Ring mit Eins-Element* $1_M = x$.

M heißt der *Ring der absolut* $\mathbb{F}_q$*-linearen Polynome* über L.
Weiter sei zu einer Unbestimmten τ

$$L\{\tau\} := \left\{ \sum_{i=0}^{n} b_i\tau^i \mid n \in \mathbb{N}_0,\, b_i \in L \right\} .$$

Dann gilt

Lemma 1.2.2. *Mit den Verknüpfungen*

$$\begin{array}{rclclcl} + & : & \sum_{i=0}^{n} a_i\tau^i & + & \sum_{j=0}^{n} b_j\tau^j & := & \sum_{i=0}^{n}(a_i+b_i)\tau^i \\ \circ & : & \sum_{i=0}^{n} a_i\tau^i & \circ & \sum_{j=0}^{m} b_j\tau^j & := & \sum_{k=0}^{n+m}(\sum_{i+j=k} a_i b_j^{q^i})\tau^k \end{array}$$

ist $(L\{\tau\},+,\circ)$ *ein nicht-kommutativer Ring mit Eins-Element* $1_{L\{\tau\}} = 1$.

Für $(L\{\tau\},+,\circ)$ schreiben wir auch

$$L\{\tau\} = \left\{ \sum_{i=0}^{n} a_i\tau^i \mid \tau b = b^q\tau \ \forall b \in L \right\} ,$$

um auszudrücken, daß $L\{\tau\}$ der Polynomring in τ, ergänzt um die obige Kommutatorrelation ist. $L\{\tau\}$ heißt der *getwistete Polynomring*, die Elemente werden als *Frobenius-Polynome* bezeichnet.
Die Multiplikation in $L\{\tau\}$ ist $\mathbb{F}_q$-bilinear, und daher ist $(L\{\tau\},+,\circ)$ sogar eine $\mathbb{F}_q$-Algebra.
Die beiden Algebren $L\{\tau\}$ und M werden durch folgendes Lemma in Verbindung gebracht:

Lemma 1.2.3. *Die Abbildung*

$$L\{\tau\} \to M, \quad \sum_{i=0}^{n} a_i\tau^i \mapsto \sum_{i=0}^{n} a_i x^{q^i}$$

ist ein $\mathbb{F}_q$*-Algebren-Isomorphismus zwischen* $(L\{\tau\},+,\circ)$ *und* $(M,+,\circ)$.

Daher werden wir sie identifizieren. D.h., ist $P(\tau)$ aus $L\{\tau\}$, so bezeichnet $P(x)$ das zugehörige Polynom in M und umgekehrt. Insbesondere ist

$$\mathrm{coeff}_\tau(k,P) = \mathrm{coeff}_x(q^k,P) .$$

Sind $P(\tau) \in L\{\tau\}$ und $\beta \in L$ gegeben, so ist

$$L \ni P(\beta) := subs(x=\beta, P(x))$$

durch das Einsetzen in das zugehörige Polynom definiert.

Definition 1.2.4. *Ein Frobenius-Polynom $P(\tau) = \sum_{i=0}^{n} a_i\tau^i \in L\{\tau\}$ heißt* separabel, *falls $a_0 \neq 0$ gilt.*

Das Frobenius-Polynom $P(\tau) \in L\{\tau\}$ ist also genau dann separabel, wenn das zugehörige Polynom $P(x) \in M$ separabel ist.

Definition 1.2.5. *Die* Höhe *eines $P(\tau) = \sum_{i=0}^{n} a_i\tau^i \in L\{\tau\} - \{0\}$ ist definiert als*

$$ht(P) := \min\{i \mid a_i \neq 0\} \ .$$

1.3 Drinfeld-Moduln

Definition 1.3.1. *Ein $\mathbb{F}_q[T]$-*Körper *(L, i_ϕ) ist ein Erweiterungskörper L von $\mathbb{F}_q$, versehen mit einem $\mathbb{F}_q$-Algebren-Homomorphismus*

$$i_\phi : \mathbb{F}_q[T] \to L \ .$$

Die $\mathbb{F}_q[T]$-Charakteristik *von (L, i_ϕ) ist definiert als*

$$\mathrm{char}(L, i_\phi) := \begin{cases} \infty & ; \ i_\phi \textit{ injektiv} \\ \ker(i_\phi) & ; \ i_\phi \textit{ nicht injektiv} \end{cases} \ .$$

Es sei daran erinnert, daß wir die Primideale von $\mathbb{F}_q[T]$ mit ihren normierten Erzeugern (d.h. den irreduziblen Polynomen) identifizieren.

Definition 1.3.2. *Sei (L, i_ϕ) ein $\mathbb{F}_q[T]$-Körper. Ein* Drinfeld-Modul *ist ein $\mathbb{F}_q$-Algebren-Homomorphismus*

$$\begin{array}{cccc} \phi : & \mathbb{F}_q[T] & \to & L\{\tau\} \\ & \mathfrak{n} & \mapsto & \phi_\mathfrak{n} \end{array}$$

mit

$$\phi_T = i_\phi(T) + \textit{ höhere Terme in } \tau$$

und

$$\deg_\tau(\phi_T) \geqslant 1 \ .$$

Ist L ein endlicher Körper, so heißt der Drinfeld-Modul endlich.

Bemerkung 1.3.3. Wegen

$$\phi_{\sum_{i=0}^{n} c_i T^i} = \sum_{i=0}^{n} \phi_{c_i T^i} = \sum_{i=0}^{n} c_i \phi_T^i \in L\{\tau\}$$

ist der Drinfeld-Modul ϕ durch die Angabe von

$$\phi_T = i_\phi(T) + \sum_{i=1}^{r} a_i \tau^i$$

eindeutig bestimmt. Wir werden einen Drinfeld-Modul ϕ oft durch das Tupel

$$(\mathbb{F}_q, L, i_\phi(T), \phi_T)$$

beschreiben. Die Information zu $i_\phi(T)$ ist zwar bereits in ϕ_T enthalten. Diese Redundanz nehmen wir aber in Kauf, um die Struktur von L als $\mathbb{F}_q[T]$-Körper zu betonen.

Man überlegt sich leicht, daß umgekehrt jedes solche Tupel einen Drinfeld-Modul beschreibt. Es gilt also das folgende Lemma:

Lemma 1.3.4. *Ein Tupel $(\mathbb{F}_q, L, \alpha, P(\tau))$ definiert genau dann einen Drinfeld-Modul, wenn folgende Aussagen erfüllt sind*

(i) L ist Erweiterungskörper von $\mathbb{F}_q$,

(ii) $\alpha \in L$ beliebig,

(iii) $P(\tau) \in L\{\tau\}$ mit $\deg_\tau(P(\tau)) \geqslant 1$,

(iv) $\mathrm{coeff}_\tau(0, P) = \alpha$.

Weiter definieren wir

Definition 1.3.5. *(i) Der* Rang *eines Drinfeld-Moduls ϕ ist definiert als*

$$rg(\phi) := \deg_\tau(\phi_T) .$$

(ii) Die Charakteristik *eines Drinfeld-Moduls ϕ ist definiert als*

$$\mathrm{char}(\phi) := \mathrm{char}(L, i_\phi) .$$

(iii) Als Höhe *von ϕ wird der Wert*

$$ht(\phi) := \begin{cases} 0 & ; \quad \mathrm{char}(\phi) = \infty \\ \frac{1}{\deg_T(\mathfrak{p})} ht(\phi_\mathfrak{p}) & ; \quad \mathrm{char}(\phi) = \mathfrak{p} \end{cases}$$

bezeichnet. Die Höhe eines Drinfeld-Moduls ist immer eine nichtnegative ganze Zahl.

Bemerkung 1.3.6. (i) Ein Drinfeld-Modul hat genau dann die Charakteristik ∞, wenn das Element $i_\phi(T) \in L$ transzendent über $\mathbb{F}_q$ ist.

(ii) Ist $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ ein Drinfeld-Modul und $M|L$ eine Körpererweiterung, so ist auch $(\mathbb{F}_q, M, \alpha, \phi_T)$ ein Drinfeld-Modul. Falls wir im weiteren von Eigenschaften eines Drinfeld-Moduls über Erweiterungen $M|L$ sprechen, so meinen wir immer den wie oben auf M fortgesetzten Drinfeld-Modul.

(iii) Ein Drinfeld-Modul $(\mathbb{F}_q, L, i_\phi(T), \phi_T)$ induziert auf jeder Erweiterung M von L durch

$$\mathfrak{n} *_\phi \beta := \phi_\mathfrak{n}(\beta) = subs(x = \beta, \phi_\mathfrak{n}(x)), \quad \mathfrak{n} \in \mathbb{F}_q[T],\ \beta \in M$$

eine $\mathbb{F}_q[T]$-Modul-Struktur. Dies erklärt auch die zweite Hälfte des Begriffs Drinfeld-Modul.

1.4 Beispiele für Drinfeld-Moduln

Beispiel 1.4.1. Betrachten wir einmal den Drinfeld-Modul

$$\phi = (\mathbb{F}_3, \mathbb{F}_3[w]/(w^2 + w + 2), w, w + w\tau^5)$$

genauer. Es ist

$$rg(\phi) = 5 \qquad \text{und} \qquad \mathrm{char}(\phi) = T^2 + T + 2 \quad .$$

Weiter ergibt sich

$$\begin{aligned} \phi_1(\tau) &= 1 \\ \phi_T(\tau) &= w + w\tau^5 \\ \phi_{T^2}(\tau) &= (w + w\tau^5) \cdot (w + w\tau^5) \\ &= w^2 + w^2\tau^5 + w\tau^5 w + w\tau^5 w\tau^5 \\ &= w^2 + w^2\tau^5 + w\ w^{3^5}\tau^5 + w\ w^{3^5}\tau^{10} \\ &= w^2 + (2 + w^2)\tau^5 + 2\tau^{10} \quad . \end{aligned}$$

Es ist also

$$\begin{aligned} \phi_{T^2+T+2}(\tau) &= \phi_{T^2}(\tau) + \phi_T(\tau) + 2\phi_1(\tau) \\ &= (w^2 + w + 2) + (w^2 + w + 2)\tau^5 + 2\tau^{10} = 2\tau^{10} \end{aligned}$$

und damit

$$ht(\phi) = \frac{10}{2} = 5 \quad .$$

Betrachten wir nun die Operation von $\mathbb{F}_3[T]$ mittels ϕ auf $\mathbb{F}_9 = \mathbb{F}_3[w]/(w^2+w+2)$. Es ist zum Beispiel

$$\begin{aligned} T *_\phi 1 &= \phi_T(1) = 2w \\ T *_\phi w &= w^2 + w\ w^{3^5} = 2w \\ T^2 *_\phi w &= T *_\phi T *_\phi w = T *_\phi 2w = w \\ (T + 1) *_\phi w &= T *_\phi w + 1 *_\phi w = 2w + w = 0 \quad . \end{aligned}$$

Insbesondere gilt

$$(T^2+T)*_\phi 1 = T^2 *_\phi 1 + T *_\phi 1 = w + 2w = 0$$
$$(T^2+T)*_\phi w = T *_\phi (T+1) *_\phi w = T *_\phi 0 = 0$$

Da $\{1, w\}$ eine $\mathbb{F}_q$-Basis von $\mathbb{F}_3[w]/(w^2+w+2)$ ist, ist damit $(T^2+T)*_\phi \alpha = 0$ für alle $\alpha \in \mathbb{F}_3[w]/(w^2+w+2)$. Wir erhalten eine Isomorphie von $\mathbb{F}_q[T]$-Moduln

$$\mathbb{F}_3[w]/(w^2+w+2) \cong {}^{\mathbb{F}_3[T]}/_{(T)} \times {}^{\mathbb{F}_3[T]}/_{(T+1)} \quad .$$

Dabei ist der Modul links des Isomorphiezeichens ein $\mathbb{F}_3[T]$-Modul bezüglich $*_\phi$, der rechte Modul bezüglich der üblichen Multiplikation in $\mathbb{F}_3[T]$. In der Notation von Kapitel 2 heißt dies, daß ϕ die Euler-Poincaré-Charakteristik T^2+T hat. □

Wir geben noch einige weitere Beispiele für Drinfeld-Moduln an.

Beispiel 1.4.2.

$(\mathbb{F}_q, L, \alpha, \phi_T)$	$\mathrm{char}(\phi)$	$[L : i_\phi(\mathbb{F}_q(T))]$
$(\mathbb{F}_q, \mathbb{F}_q, 0, \tau)$	$T \cdot \mathbb{F}_q[T]$	1
$(\mathbb{F}_q, \mathbb{F}_q, 1, 1+\tau)$	$(T-1)\cdot \mathbb{F}_q[T]$	1
$(\mathbb{F}_q, \mathbb{F}_{q^2}, 0, \tau)$	$T \cdot \mathbb{F}_q[T]$	2
$(\mathbb{F}_3, \mathbb{F}_3[w]/(w^2+w+2), w, w+w\tau^3)$	$(T^2+T+2)\cdot \mathbb{F}_q[T]$	1
$(\mathbb{F}_3, \mathbb{F}_3[w]/(w^2+1), w, w+w\tau^3)$	$(T^2+1)\cdot \mathbb{F}_q[T]$	1
$(\mathbb{F}_q, \mathbb{F}_q(u), u, u+u^4\tau+(u^2-1)\tau^5)$	∞	1
$(\mathbb{F}_q, \mathbb{F}_q(u), u^2, u^2+u^4\tau+(u^2-1)\tau^5)$	∞	2
$(\mathbb{F}_q, \mathbb{F}_q(u), 0, u^4\tau+(u^2-1)\tau^5)$	$T \cdot \mathbb{F}_q[T]$	∞
$(\mathbb{F}_q, \mathbb{F}_q((u)), u, u+u^4\tau+(u^2-1)\tau^5)$	∞	∞
$(\mathbb{F}_q, \mathbb{F}_q(u,v), u, u+u^4\tau+(v^2-u)\tau^5)$	∞	∞
$(\mathbb{F}_5, \mathbb{F}_5(u,y)/(y^2-u^3-1)\ , u, u+\tau)$	∞	2

□

1.5 Morphismen von Drinfeld-Moduln

Definition 1.5.1. *Seien* $\phi := (\mathbb{F}_q, L, \alpha_1, \phi_T)$ *und* $\psi := (\mathbb{F}_q, L, \alpha_2, \psi_T)$ *Drinfeld-Moduln.*

(i) Die Menge der L-Homomorphismen *von* ϕ *nach* ψ *ist definiert als*

$$\mathrm{Hom}_L(\phi, \psi) := \{u \in L\{\tau\} \mid u \cdot \phi_T = \psi_T \cdot u\} \ .$$

Sie ist eine Untergruppe von $(L\{\tau\}, +)$. *Elemente ungleich Null aus* $\mathrm{Hom}_L(\phi, \psi)$ *werden auch* L-Isogenien *genannt.*

(ii) Die L-Isomorphismen, *d.h. die invertierbaren* L*-Homomorphismen von* ϕ *nach* ψ, *sind die Elemente von* $\mathrm{Hom}_L(\phi, \psi) \cap L^*$, *die wir mit* $\mathrm{Isom}_L(\phi, \psi)$ *bezeichnen.*

(iii) Die L-Endomorphismen *von* ϕ *sind die Elemente aus* $\mathrm{Hom}_L(\phi, \phi)$.

(iv) Die L-Automorphismen *von* ϕ *sind die Elemente aus* $\mathrm{Isom}_L(\phi, \phi)$, *d.h. die Einheiten des Rings* $\mathrm{Hom}_L(\phi, \phi)$.

Bemerkung 1.5.2. (i) Sind $u \in \mathrm{Hom}_L(\phi, \psi), v \in \mathrm{Hom}_L(\psi, \gamma)$, so ist $v \cdot u \in \mathrm{Hom}_L(\phi, \gamma)$. Die Drinfeld-Moduln über L und ihre Homomorphismen bilden eine Kategorie.

(ii) Falls $\mathrm{Isom}_L(\phi, \psi)$ nicht leer ist, schreiben wir auch $\phi \cong_L \psi$.

(iii) Sei $\phi_T = \sum_{i=0}^r b_i \tau^i$, $\psi_T = \sum_{i=0}^r c_i \tau^i$ und $0 \neq \alpha \in \mathrm{Hom}_L(\phi, \psi)$. Dann ist

$$\phi_T = \alpha^{-1} \psi_T \alpha = \sum_{i=0}^{r} c_i \alpha^{q^i - 1} \ \tau^i \quad .$$

Für die Koeffizienten folgt daraus

$$b_i = c_i \ \alpha^{q^i-1} \qquad \forall 0 \leqslant i \leqslant r \quad .$$

(iv) Aus (iii) folgt, daß Homomorphismen zwischen ϕ und ψ höchstens dann existieren, falls $rg(\phi) = rg(\psi)$ und $i_\phi = i_\psi$ gilt.

Da jedes Element $\mathfrak{n}(T) \in \mathbb{F}_q[T]$ einen Endomorphismus $\phi_{\mathfrak{n}}(\tau) \in L\{\tau\}$ induziert, ist $\phi(\mathbb{F}_q[T]) \subset L\{\tau\}$ immer ein Unterring des Endomorphismenrings $\mathrm{Hom}_L(\phi, \phi)$. Drinfeld-Moduln, deren Endomorphismenring echt größer ist, sind besonders ausgezeichnet.

Definition 1.5.3. *Seien die Bezeichnungen wie oben und* $\bar{L}$ *der algebraische Abschluß von L. Falls* $\mathrm{End}_{\bar{L}}(\phi) \neq \mathbb{F}_q[T]$ *gilt, sagen wir, daß* ϕ komplexe Multiplikation *hat.*

1.6 Teilungspunkte

Wir kommen nun zu einem der zentralen Objekte dieser Arbeit.

Definition 1.6.1. *Sei* $\mathfrak{n} \in \mathbb{F}_q[T]$ *beliebig,* $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ *ein Drinfeld-Modul und* L' *ein Erweiterungskörper von* L*. Dann heißt*

$$_{\mathfrak{n}}\phi(L') := \{\alpha \in L' \mid \mathfrak{n} *_{\phi} \alpha = \phi_{\mathfrak{n}}(\alpha) = 0\}$$

die $\mathfrak{n}$-Torsion *von* ϕ *in* L'*. Wir kürzen* $_{\mathfrak{n}}\phi(\bar{L})$ *durch* $_{\mathfrak{n}}\phi$ *ab. Elemente von* $_{\mathfrak{n}}\phi$ *heißen* $\mathfrak{n}$-Teilungspunkte *oder* $\mathfrak{n}$-Torsionspunkte*. Das Polynom* $\mathfrak{n}(T)$ *wird auch der* Führer *genannt.*

Bemerkung 1.6.2. Die $\mathfrak{n}$-Teilungspunkte eines Drinfeld-Moduls sind also die Nullstellen des Polynoms $\phi_{\mathfrak{n}}(x)$.

Es gilt der folgende Struktursatz für die Teilungspunkte (s. [GS97, Prop.2.1]).

Satz 1.6.3. *Für einen Drinfeld-Modul* ϕ *und ein nichtkonstantes* $\mathfrak{n}$ *aus* $\mathbb{F}_q[T]$ *gilt:*

(i) Die $\mathfrak{n}$*-Torsion* $_{\mathfrak{n}}\phi$ *ist via* ϕ *ein projektiver* $\mathbb{F}_q[T]/\mathfrak{n}$*-Modul vom Rang kleiner oder gleich* $rg(\phi)$*.*

(ii) Ist $\mathrm{ggT}(\mathfrak{n}, \mathfrak{m}) = 1$*, so folgt*

$$_{\mathfrak{n}\cdot\mathfrak{m}}\phi = {_{\mathfrak{n}}\phi} \oplus {_{\mathfrak{m}}\phi} \ .$$

(iii) Ist $\mathrm{char}(\phi) = \infty$ *oder* $\mathrm{ggT}(\mathfrak{n}, \mathrm{char}(\phi)) = 1$*, so ist* $_{\mathfrak{n}}\phi$ *über* $\mathbb{F}_q[T]/\mathfrak{n}$ *frei vom Rang* $rg(\phi)$*.*

(iv) Ist $\mathrm{char}(\phi) = \mathfrak{p} \neq \infty$*, so ist* $_{\mathfrak{p}^i}\phi$ *für alle* $i \in \mathbb{N}$ *frei über* $\mathbb{F}_q[T]/(\mathfrak{p}^i)$ *vom Rang* $rg(\phi) - ht(\phi)$*.*

Lemma 1.6.4. *Sei* $(\mathbb{F}_q, L, \alpha, \phi_T)$ *ein Drinfeld-Modul. Dann kommutiert die Operation von* $\mathrm{Gal}(L^{sep}, L)$ *auf* L^{sep} *mit der durch* ϕ *induzierten* $\mathbb{F}_q[T]$*-Operation auf* L^{sep}*.*

Beweis: Sei σ ein beliebiges Element von $\mathrm{Gal}(L^{sep}, L)$ und $\mathfrak{m} \in \mathbb{F}_q[T]$. Da das additive Polynom $\phi_{\mathfrak{m}}(x)$ über L definiert ist, gilt $\phi_{\mathfrak{m}}(\sigma(x)) = \sigma(\phi_{\mathfrak{m}}(x))$. Also gilt für alle $\beta \in L^{sep}$

$$\sigma(\mathfrak{m} *_{\phi} \beta) = \sigma(\phi_{\mathfrak{m}}(\beta)) = \phi_{\mathfrak{m}}(\sigma(\beta)) = \mathfrak{m} *_{\phi} \sigma(\beta) \ .$$

Damit ist die Aussage gezeigt. □

Korollar 1.6.5. *Seien* $(\mathbb{F}_q, L, \alpha, \phi_T)$ *ein Drinfeld-Modul,* $\mathfrak{n} \in \mathbb{F}_q[T]$ *und* ${}_{\mathfrak{n}}\phi \subseteq L^{sep}$*. Dann ist* ${}_{\mathfrak{n}}\phi$ *ein* $\mathrm{Gal}(L^{sep}, L)$*-invarianter* $\mathbb{F}_q[T]$*-Untermodul von* L^{sep}*.*

Beweis: Es ist klar, daß ${}_{\mathfrak{n}}\phi$ ein Untermodul ist. Sei nun α aus ${}_{\mathfrak{n}}\phi$ und σ ein beliebiges Element von $\mathrm{Gal}(L^{sep}, L)$. Dann gilt

$$\mathfrak{n} *_\phi \sigma(\alpha) = \sigma(\mathfrak{n} *_\phi \alpha) = \sigma(0) = 0 \; .$$

Also liegt $\sigma(\alpha)$ in ${}_{\mathfrak{n}}\phi$, und die Aussage folgt. □

Bemerkung 1.6.6. (i) Die Bedingung ${}_{\mathfrak{n}}\phi \subseteq L^{sep}$ ist nicht automatisch erfüllt. Zum Beispiel liegt für den Drinfeld-Modul $(\mathbb{F}_q, \mathbb{F}_q(u), 0, 0 + u\tau + \tau^2)$ die T-Torsion ${}_T\phi$ (d.h. die Nullstellen von $u \cdot x^q + x^{q^2}$) nicht in $\mathbb{F}_q(u)^{sep}$.

(ii) Das Polynom $\phi_{\mathfrak{n}}(x)$ muß nicht immer separabel sein. Zum Beispiel ist im Fall des Drinfeld-Moduls $(\mathbb{F}_q, \mathbb{F}_q(u), 0, \tau)$ das Polynom $\phi_T(x) = x^q$ nicht separabel, aber ${}_T\phi = \{0\}$ ist Teilmenge von $\mathbb{F}_q(u)^{sep}$.

(iii) Für jeden Drinfeld-Modul $(\mathbb{F}_q, L, \alpha, \phi_T)$ über einem endlichen Körper L liegt für jedes $\mathfrak{n} \in \mathbb{F}_q[T]$ der Torsionsmodul ${}_{\mathfrak{n}}\phi$ in $L^{sep} = \overline{L}$, obwohl das Polynom $\phi_{\mathfrak{n}}(x) \in L[x]$ mehrfache Nullstellen haben kann.

(iv) Für weiterführende Aussagen über Nullstellen von additiven Polynomen über endlichen Körpern sei auf [LN94, Kap. 3] verwiesen.

Aus Lemma 1.6.4 und Korollar 1.6.5 erhalten wir

Satz 1.6.7. *Seien* $(\mathbb{F}_q, L, \alpha, \phi_T)$ *ein Drinfeld-Modul,* $\mathfrak{n} \in \mathbb{F}_q[T]$ *und* ${}_{\mathfrak{n}}\phi \subseteq L^{sep}$*. Dann induziert die Operation von* $\mathrm{Gal}(L^{sep}, L)$ *auf* ${}_{\mathfrak{n}}\phi$ *eine Darstellung*

$$\rho^{red}_{\phi,\mathfrak{n}} : \mathrm{Gal}(L^{sep}, L) \to \mathrm{Aut}_{(\mathbb{F}_q[T]/\mathfrak{n})}({}_{\mathfrak{n}}\phi) \; ,$$

die sogenannte reduzierte Darstellung *oder* Torsionsdarstellung*.*

Diese Darstellung wird später das Hauptobjekt unserer Untersuchung sein.
Das folgende Lemma zeigt, daß in vielen Fällen die Bedingung

$${}_{\mathfrak{n}}\phi \subseteq L^{sep}$$

automatisch erfüllt ist. Insbesondere deckt das Lemma genau die Fälle ab, die uns in dieser Arbeit interessieren werden.

Lemma 1.6.8. *Sei* $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ *ein Rang-r Drinfeld-Modul. Ist L endlich oder* $\mathrm{char}(\phi) = \infty$*, so gilt*

$${}_{\mathfrak{n}}\phi(\bar{L}) \subseteq L^{sep} \; .$$

Beweis: Es ist

$$\phi_{\mathfrak{n}}(x) = i_\phi(\mathfrak{n}) + \sum_{i=1}^{r \deg_T(\mathfrak{n})} a_i x^{q^i} \quad .$$

Deshalb ist die Ableitung $\frac{d}{dx}\phi_{\mathfrak{n}}(x) = i_\phi(\mathfrak{n})$ konstant. Ist $\mathrm{char}(\phi) = \infty$, so ist i_ϕ injektiv und damit $i_\phi(\mathfrak{n}) \neq 0$. Also ist $\mathrm{ggT}(\phi_{\mathfrak{n}}(x), \frac{d}{dx}\phi_{\mathfrak{n}}(x)) = 1$, und $\phi_{\mathfrak{n}}(x)$ ist ein separables Polynom.
Ist L endlich, so gilt $\bar{L} = L^{sep}$, und damit ist die Aussage trivialerweise korrekt. □

1.7 Beispiele für Torsionserweiterungen

Um ein besseres Gefühl für die Situation zu bekommen, werden wir nun an einigen Beispielen die Galoisgruppe einer Torsionserweiterung als Untergruppe einer $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ explizit berechnen.

Beispiel 1.7.1. Sei

$$\phi = (\mathbb{F}_2, \mathbb{F}_2, 0, \tau + \tau^2)$$

und

$$\mathfrak{l}(T) = T^2 + T + 1 \quad .$$

Dann ist

$$\phi_{T^2}(\tau) = \phi_T(\tau) \cdot \phi_T(\tau) = (\tau + \tau^2) \cdot (\tau + \tau^2) = \tau^2 + \tau^4 \quad .$$

Damit ist

$$\phi_{T^2+T+1} = \tau^4 + \tau + 1 = x^{16} + x^2 + x = x(x^{15} + x + 1) \quad .$$

Da $x^{15} + x + 1$ in $\mathbb{F}_2[x]$ irreduzibel ist, ist $\mathbb{F}_{2^{15}}$ der $(T^2 + T + 1)$-Torsionskörper von ϕ. Diesen repräsentieren wir als

$$\mathbb{F}_{2^{15}} := \mathbb{F}_2[\alpha] / (\alpha^{15} + \alpha + 1) \quad .$$

Damit ergibt sich

$$_{T^2+T+1}\phi = \{0, \alpha, \alpha^2, \alpha^{2^2}, \ldots, \alpha^{2^{14}}\} \quad .$$

Explizit ausgeschrieben lauten die Torsionspunkte

$$\begin{array}{cccccccc}
0 & , & \alpha & , & \alpha^2 & , & \alpha^4 & , \\
\alpha^8 & , & \alpha^2 + \alpha & , & \alpha^4 + \alpha^2 & , & \alpha^8 + \alpha^4 & , \\
\alpha^8 + \alpha^2 + \alpha & , & \alpha^4 + \alpha & , & \alpha^8 + \alpha^2 & , & \alpha^4 + \alpha^2 + \alpha & , \\
\alpha^8 + \alpha^4 + \alpha^2 & , & \alpha^8 + \alpha^4 + \alpha^2 + \alpha & , & \alpha^8 + \alpha^4 + \alpha & , & \alpha^8 + \alpha & ,
\end{array} \quad .$$

Diese Menge ist abgeschlossen unter der Operation $*_\phi$. Zum Beispiel erhält man aus dem Torsionspunkt $\alpha^8+\alpha^4$ durch

$$\begin{aligned}(T^3+T^2)*_\phi(\alpha^8+\alpha^4) &= (T(T^2+T+1)+T)*_\phi(\alpha^8+\alpha^4)\\ &= (T(T^2+T+1))*_\phi(\alpha^8+\alpha^4)+T*_\phi(\alpha^8+\alpha^4)\\ &= \big(T*_\phi((T^2+T+1)*_\phi(\alpha^8+\alpha^4)\big)+T*_\phi(\alpha^8+\alpha^4)\\ &= T*_\phi 0+T*_\phi(\alpha^8+\alpha^4)=T*_\phi(\alpha^8+\alpha^4)\\ &= (\alpha^8+\alpha^4)^2+(\alpha^8+\alpha^4)^4=\alpha^{16}+\alpha^8+\alpha^{32}+\alpha^{16}\\ &= \alpha^8+\alpha^{32}=\alpha^8+\alpha^4+\alpha^2\end{aligned}$$

den Torsionspunkt $\alpha^8+\alpha^4+\alpha^2$. Nach Satz 1.6.3 ist ${}_{T^2+T+1}\phi$ ein 2-dimensionaler Vektorraum über dem 4-elementigen Körper $\mathbb{F}_{\mathfrak{l}} := \mathbb{F}_2[T]/(T^2+T+1)$. Von diesem Vektorraum wollen wir nun eine Basis bestimmen. Als ersten Basisvektor wählen wir die Nullstelle α. Da $\phi_T(x)=x^2+x^4$ ist, ist $T*_\phi\alpha=\alpha^4+\alpha^2$, und wir erhalten

$$\mathbb{F}_2[T]\big/(T^2+T+1)*_\phi\alpha=\{0,\alpha,\alpha^4+\alpha^2,\alpha^4+\alpha^2+\alpha\}$$

als den von α erzeugten Unterraum. Da der Torsionspunkt α^2 nicht in diesem Unterraum liegt, können wir ihn als zweiten Basisvektor wählen. Es ist

$$\mathbb{F}_2[T]\big/(T^2+T+1)*_\phi\alpha^2=\{0,\alpha^2,\alpha^8+\alpha^4,\alpha^8+\alpha^4+\alpha^2\}\quad,$$

und wir erhalten

$${}_{T^2+T+1}\phi=\mathbb{F}_{\mathfrak{l}}*_\phi\alpha\oplus\mathbb{F}_{\mathfrak{l}}*_\phi\alpha^2\quad.$$

Wir untersuchen nun, wie sich die Galoisgruppe der Erweiterung $\mathbb{F}_2({}_{T^2+T+1}\phi)|\mathbb{F}_2$ in die $\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})$ einbettet. Da es sich um eine Erweiterung von endlichen Körpern handelt, wird die Galoisgruppe vom Frobenius-Automorphismus $y\mapsto y^2$ erzeugt. Dieser operiert auf der von uns gewählten Basis wie folgt:

$$\begin{array}{rcl}\alpha & \mapsto & \alpha^2=0*_\phi\alpha+1*_\phi\alpha^2\\ \alpha^2 & \mapsto & \alpha^4=(\alpha^4+\alpha^2)+\alpha^2=T*_\phi\alpha+1*_\phi\alpha^2\end{array}\quad.$$

Daher korrespondiert der Frobenius zur Matrix

$$\begin{pmatrix}\bar{0} & \bar{T}\\ \bar{1} & \bar{1}\end{pmatrix}\quad,$$

und wir erhalten (bzgl. der gewählten Basis der (T^2+T+1)-Torsion)

$$\mathrm{Gal}(\mathbb{F}_2({}_{T^2+T+1}\phi),\mathbb{F}_2)=\langle\begin{pmatrix}\bar{0} & \bar{T}\\ \bar{1} & \bar{1}\end{pmatrix}\rangle\leqslant\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})$$

und

$$\mathrm{ord}_{\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})}(\begin{pmatrix}\bar{0} & \bar{T}\\ \bar{1} & \bar{1}\end{pmatrix})=15\quad.$$

$\square$

Beispiel 1.7.2. Wir wählen nun

$$\phi = (\mathbb{F}_2, \mathbb{F}_2, 0, \tau^2)$$

und wieder

$$\mathfrak{f}(T) = T^2 + T + 1 \quad .$$

Dann ist

$$\phi_{\mathfrak{f}}(x) = x^{16} + x^4 + x = x(x^3 + x + 1)(x^6 + x^3 + 1)(x^6 + x^4 + x^2 + x + 1) \quad .$$

Der $(T^2 + T + 1)$-Torsionskörper ist also in diesem Fall $\mathbb{F}_{2^6}$. Sei nun

$$\mathbb{F}_{2^6} := \mathbb{F}_2[\alpha]/(\alpha^6 + \alpha^3 + 1) \quad .$$

Dann haben die einzelnen Faktoren die folgenden Nullstellen

$$\begin{gathered} 0 \\ \alpha^4 + \alpha^2 + \alpha,\ \alpha^5 + \alpha^4,\ \alpha^5 + \alpha^2 + \alpha, \\ \alpha,\ \alpha^2,\ \alpha^4,\ \alpha^5 + \alpha^2,\ \alpha^4 + \alpha,\ \alpha^5, \\ \alpha^5 + \alpha, \alpha^2 + \alpha,\ \alpha^4 + 2\alpha^3 + \alpha^2, \alpha^5 + \alpha^4 + \alpha^2,\ \alpha^5 + \alpha^4 + \alpha^2 + \alpha,\ \alpha^5 + \alpha^4 + \alpha, \end{gathered}$$

wobei in jeder Zeile eine Nullstelle das Quadrat ihrer linken Nachbarin ist. Wieder ist ${}_{T^2+T+1}\phi$ ein 2-dimensionaler Vektorraum über $\mathbb{F}_{\mathfrak{f}} := \mathbb{F}_2[T]/(T^2 + T + 1)$. Es ist

$$\mathbb{F}_{\mathfrak{f}} *_\phi \alpha = \{0, \alpha, \alpha^4, \alpha^4 + \alpha\}$$

und

$$\mathbb{F}_{\mathfrak{f}} *_\phi \alpha^2 = \{0, \alpha^2, \alpha^5 + \alpha^2, \alpha^5\} \quad ,$$

und wir können wieder α und α^2 als Basis von ${}_{T^2+T+1}\phi$ wählen. Der Frobenius $y \mapsto y^2$ operiert auf dieser Basis durch

$$\begin{aligned} \alpha &\mapsto \alpha^2 = 0 *_\phi \alpha + 1 *_\phi \alpha^2 \\ \alpha^2 &\mapsto \alpha^4 = T *_\phi \alpha + 0 *_\phi \alpha^2 \end{aligned} \quad .$$

Damit wird $y \mapsto y^2$ bezüglich der gewählten Basis durch

$$\begin{pmatrix} \bar{0} & \bar{T} \\ \bar{1} & \bar{0} \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_{\mathfrak{f}})$$

beschrieben. Nachdem man diese Matrix in ihre Jordansche Normalform konjugiert hat, erhält man (bis auf Konjugation)

$$\mathrm{Gal}(\mathbb{F}_2({}_{T^2+T+1}\phi), \mathbb{F}_2) = \langle \begin{pmatrix} \overline{T+1} & \bar{1} \\ \bar{0} & \overline{T+1} \end{pmatrix} \rangle \leqslant \mathrm{GL}(2, \mathbb{F}_{\mathfrak{f}}) \quad .$$

□

Beispiel 1.7.3. Nun betrachten wir ein Beispiel in Charakteristik 3. Es sei

$$\phi = (\mathbb{F}_3, \mathbb{F}_3, 1, 1 + 2\tau + \tau^2)$$

und

$$\mathfrak{l}(T) = T^2 + 1 \quad .$$

Es ist $\phi_{T^2}(\tau) = 1 + \tau + \tau^3 + \tau^4$ und daher

$$\phi_{T^2+1}(x) = 2x + x^3 + x^{27} + x^{81} \quad .$$

Mit Hilfe eines Computeralgebrasystems erhält man, daß der Zerfällungskörper dieses Polynoms Grad 8 über $\mathbb{F}_3$ hat. Repräsentieren wir $\mathbb{F}_{3^8}$ durch

$$\mathbb{F}_{3^8} := {}^{\mathbb{F}_3[\alpha]}\!\big/_{(\alpha^8 + \alpha^2 + 2)} \quad ,$$

so ist α einer der 81 Torsionspunkte, die wieder einen 2-dimensionalen Vektorraum über dem Restkörper $\mathbb{F}_{\mathfrak{l}} = \mathbb{F}_3[T]/(T^2 + 1)$ bilden. Mittels

$$T *_\phi \alpha = \alpha^9 + 2\alpha^3 + \alpha = \alpha^3 + 2\alpha$$

und

$$(aT + b) *_\phi \alpha = a \cdot (T *_\phi \alpha) + b \cdot \alpha, \qquad \forall a, b \in \mathbb{F}_3$$

berechnet sich nun das Erzeugnis $\mathbb{F}_{\mathfrak{l}} *_\phi \alpha$ leicht zu

$g \in \mathbb{F}_{\mathfrak{l}}$	0	1	2	T	$T+1$	$T+2$	$2T$	$2T+1$	$2T+2$
$g *_\phi \alpha$	0	α	2α	$\alpha^3 + 2\alpha$	α^3	$\alpha^3 + \alpha$	$2\alpha^3 + \alpha$	$2\alpha^3 + 2\alpha$	$2\alpha^3$

.

Als zweiten Basisvektor wählen wir $\alpha^4 + 2\alpha^2$. Dessen Erzeugnis ist

$g \in \mathbb{F}_{\mathfrak{l}}$	0	1	2	T	$T+1$	$T+2$	$2T$	$2T+1$	$2T+2$
$g *_\phi \alpha$	0	$\alpha^4 + 2\alpha^2$	$2\alpha^4 + \alpha^2$	$2\alpha^6 + 2\alpha^4$	$2\alpha^6 + 2\alpha^2$	$2\alpha^6 + \alpha^4 + \alpha^2$	$\alpha^6 + \alpha^4$	$\alpha^6 + 2\alpha^4 + 2\alpha^2$	$\alpha^6 + \alpha^2$

.

Der Frobenius $y \mapsto y^3$ operiert hier durch

$$\begin{array}{rcl} \alpha & \mapsto & \alpha^3 = (T+1) *_\phi \alpha + 0 *_\phi (\alpha^4 + 2\alpha^2) \\ \alpha^4 + 2\alpha^2 & \mapsto & \alpha^6 + \alpha^4 = 0 *_\phi \alpha + 2T *_\phi (\alpha^4 + 2\alpha^2) \end{array} \quad .$$

Damit entspricht dem Frobenius die Matrix

$$\begin{pmatrix} \overline{T+1} & \overline{0} \\ \overline{0} & \overline{2T} \end{pmatrix} \quad ,$$

und damit ist (wieder bis auf Konjugation)

$$\mathrm{Gal}(\mathbb{F}_3({}_{T^2+1}\phi), \mathbb{F}_3) = \langle \begin{pmatrix} \overline{T+1} & \overline{0} \\ \overline{0} & \overline{2T} \end{pmatrix} \rangle \leqslant \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) \quad .$$

□

Beispiel 1.7.4. Wir betrachten nun einen globalen Drinfeld-Modul. Dieser liefert ein Beispiel für eine nicht-zyklische Galoiserweiterung. Sei

$$\phi = (\mathbb{F}_3, \mathbb{F}_3(u), u, u - \tau^2)$$

und

$$\mathfrak{l}(T) = T \quad .$$

Dann ist

$$\phi_{\mathfrak{l}}(x) = ux - x^9 = x(u - x^8) \quad .$$

Damit können wir die T-Torsionserweiterung als Kummererweiterung auffassen (vgl. [Sti93, III.7.3, VI.3.1]).
Sei $\mathbb{F}_9$ repräsentiert als

$$\mathbb{F}_9 := {}^{\mathbb{F}_3[\lambda]}\big/_{(\lambda^2 + 2\lambda + 2)} \quad .$$

Dann erzeugt λ die multiplikative Gruppe $\mathbb{F}_9^*$. Ist η eine fest gewählte Nullstelle von $x^8 - u$, so gilt

$$x^9 - ux = x \prod_{i=0}^{7} (x - \lambda^i \eta) \quad ,$$

und damit

$$\mathbb{F}_3(u)[{}_T\phi] = \mathrm{ZerfKp}(x^8 - u) = \mathbb{F}_3(u)[\eta, \lambda] = \mathbb{F}_9(u)[\eta] = \mathbb{F}_9(\eta) \quad .$$

Die Galoisgruppe der Erweiterung $\mathbb{F}_9(\eta)|\mathbb{F}_3(u) = \mathbb{F}_9(\eta)|\mathbb{F}_3(\eta^8)$ wird von den beiden Automorphismen

$$\sigma = \begin{pmatrix} \eta & \mapsto & \lambda \cdot \eta \\ \lambda & \mapsto & \lambda \end{pmatrix} \qquad \text{und} \qquad \xi = \begin{pmatrix} \eta & \mapsto & \eta \\ \lambda & \mapsto & \lambda^3 \end{pmatrix}$$

erzeugt. Man rechnet leicht nach, daß $\xi\sigma\xi = \sigma^3$ gilt, und daher ist

$$\mathrm{Gal}(\mathbb{F}_3(u)[{}_T\phi], \mathbb{F}_3(u)) = \langle \sigma, \xi \mid \sigma^8 = 1 = \xi^2 \ , \ \sigma\xi = \xi\sigma^3 \rangle \quad .$$

Insbesondere gilt

$$\#\mathrm{Gal}(\mathbb{F}_3(u)[{}_T\phi], \mathbb{F}_3(u)) = 16 \quad .$$

Wir untersuchen nun, wie die Galoisgruppe als Untergruppe von $\mathrm{GL}(2, \mathbb{F}_T) = \mathrm{GL}(2, \mathbb{F}_3)$ aussieht. Dazu zerlegen wir

$${}_T\phi = \{0, \eta, \lambda\eta, \ldots, \lambda^7\eta\} = \langle \eta \rangle_{\mathbb{F}_T} \oplus \langle \lambda\eta \rangle_{\mathbb{F}_T} = \{0, \eta, 2\eta\} \oplus \{0, \lambda\eta, 2\lambda\eta\}$$

in die direkte Summe von 1-dimensionalen $\mathbb{F}_T$-Untervektorräumen. Wir wählen als $\mathbb{F}_T$-Basis $\{\eta, \ \lambda\eta\}$. Bezüglich dieser Basis ist

$$\begin{aligned} \sigma(\eta) &= \lambda\eta = 0 *_\phi \eta + 1 *_\phi \lambda\eta \\ \sigma(\lambda\eta) &= \lambda^2\eta = (\lambda + 1)\eta = 1 *_\phi \eta + 1 *_\phi \lambda\eta \end{aligned}$$

und

$$\begin{aligned} \xi(\eta) &= \eta = 1 *_\phi \eta + 0 *_\phi \lambda\eta \\ \xi(\lambda\eta) &= \lambda^3\eta = (2\lambda+1)\eta = 1 *_\phi \eta + 2 *_\phi \lambda\eta \quad . \end{aligned}$$

Daher erhalten wir die Beschreibungen

$$\sigma \leftrightarrow \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \quad \text{und} \quad \xi \leftrightarrow \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix}$$

und

$$\mathrm{Gal}(\mathbb{F}_3(u)[{}_T\phi], \mathbb{F}_3(u)) = \langle \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} , \begin{pmatrix} 1 & 1 \\ 0 & 2 \end{pmatrix} \rangle \leqslant \mathrm{GL}(2, \mathbb{F}_3) \quad .$$

□

1.8 Der Tate-Modul

Um die Darstellung auf den Torsionspunkten zu untersuchen, betrachten wir eine „Verfeinerung" dieser Darstellung, d.h. die zugehörige Darstellung auf dem Tate-Modul.

Definition 1.8.1. *Sei $(\mathbb{F}_q, L, \alpha, \phi_T)$ ein Drinfeld-Modul und $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$. Dann bilden die Moduln $({}_{\mathfrak{l}^i}\phi)_{i=1}^\infty$ mit den Verbindungsmorphismen*

$$mult_{\phi,k} : {}_{\mathfrak{l}^{i+k}}\phi \to {}_{\mathfrak{l}^i}\phi, \qquad \alpha \mapsto \mathfrak{l}^k *_\phi \alpha$$

ein projektives System. Der projektive Limes über dieses System

$$T_{\mathfrak{l}}(\phi) := \lim_{\leftarrow} {}_{\mathfrak{l}^i}\phi$$

heißt der Tate-Modul *zu ϕ und $\mathfrak{l}$.*

Der Struktursatz für die $\mathfrak{n}$-Torsion 1.6.3 überträgt sich auf den Tate-Modul, und es ergibt sich:

Satz 1.8.2. *Mit den Bezeichnungen von oben gilt:*

$$T_{\mathfrak{l}}(\phi) \cong \begin{cases} \mathbb{F}_q[T]_{\mathfrak{l}}^{rg(\phi)} & ; \quad \mathfrak{l} \neq \mathrm{char}(\phi) \\ \mathbb{F}_q[T]_{\mathfrak{l}}^{rg(\phi)-ht(\phi)} & ; \quad \mathfrak{l} = \mathrm{char}(\phi) \end{cases}$$

Da die Verbindungsmorphismen mit der Galoisoperation kommutieren, erhalten wir auch eine Darstellung auf der Automorphismengruppe des Tate-Moduls.

Satz 1.8.3. *Sei* $(\mathbb{F}_q, L, \alpha, \phi_T)$ *ein Drinfeld-Modul,* $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$ *und* ${}_{\mathfrak{l}^i}\phi \subseteq L^{sep}$ *für alle i. Dann induziert die Operation von* $\mathrm{Gal}(L^{sep}, L)$ *auf* ${}_{\mathfrak{l}^i}\phi$ *eine Darstellung*

$$\rho_{\phi,\mathfrak{l}}^{Tate} : \mathrm{Gal}(L^{sep}, L) \to \mathrm{Aut}_{\mathbb{F}_q[T]_\mathfrak{l}}(T_\mathfrak{l}(\phi)) \ ,$$

die sogenannte Tate-Darstellung.

Es sei darauf hingewiesen, daß nach Wahl einer Basis

$$\mathrm{Aut}_{\mathbb{F}_q[T]_\mathfrak{l}}(T_\mathfrak{l}(\phi)) \cong \begin{cases} \mathrm{GL}(rg(\phi), \mathbb{F}_q[T]_\mathfrak{l}) & ; \quad \mathfrak{l} \neq \mathrm{char}(\phi) \\ \mathrm{GL}(rg(\phi) - ht(\phi), \mathbb{F}_q[T]_\mathfrak{l}) & ; \quad \mathfrak{l} = \mathrm{char}(\phi) \end{cases}$$

gilt.

Bemerkung 1.8.4. Alle Drinfeld-Moduln, die wir später betrachten werden, sind entweder endlich oder haben Charakteristik ∞. In beiden Fällen gilt nach Lemma 1.6.8 immer ${}_\mathfrak{n}\phi \subseteq L^{sep}$, so daß die Einschränkung in Satz 1.8.3 nicht von Bedeutung sein wird.

Für Darstellungen dieser Art wurde von Pink in [Pin97] der folgende fundamentale Satz gezeigt.

Satz 1.8.5 (Pink). *Sei* $L|\mathbb{F}_q$ *ein algebraischer Funktionenkörper,* $\alpha \in L$ *transzendent über* $\mathbb{F}_q$ *und* $\phi := (\mathbb{F}_q, L, \alpha, \alpha + \sum_{i=1}^r a_i\tau^i)$ *ein Rang-r Drinfeld-Modul. Weiter habe* ϕ *keine komplexe Multiplikation. Dann gilt:*
Die Darstellung

$$\rho_{\phi,\mathfrak{l}}^{Tate} : \mathrm{Gal}(L^{sep}, L) \to \mathrm{Aut}_{\mathbb{F}_q[T]_\mathfrak{l}}(T_\mathfrak{l}(\phi))$$

hat offenes Bild in der $\mathfrak{l}$*-adischen Topologie. Da* $\mathrm{Aut}_{\mathbb{F}_q[T]_\mathfrak{l}}(T_\mathfrak{l}(\phi))$ *eine kompakte Gruppe ist, hat das Bild insbesondere endlichen Index.*

In seiner Dissertation [Gar01] verallgemeinert Francis Gardeyn das Resultat 1.8.5 von Pink. Unter anderem zeigt er, daß im Rang-2 Fall das Bild der Darstellung

$$\mathrm{Gal}(L^{sep}, L) \to \prod_{\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}} \mathrm{GL}(2, \mathbb{F}_q[T]_\mathfrak{l}), \quad \sigma \mapsto \left(\rho_{\phi,\mathfrak{l}}^{Tate}(\sigma)\right)_{\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}}$$

immer noch offen ist, falls der Drinfeld-Modul ϕ keine komplexe Multiplikation hat. Um dies zu tun, benutzt und beweist er folgende für uns interessante Aussage, ohne sie explizit zu benennen (vgl. [Gar01, S.77–80]).

Satz 1.8.6. *Sei* $L|\mathbb{F}_q$ *ein globaler Funktionenkörper,* $\alpha \in L$ *transzendent über* $\mathbb{F}_q$ *und* $\phi := (\mathbb{F}_q, L, \alpha, \alpha + g\tau + \Delta\tau^2)$ *ein Rang-2 Drinfeld-Modul. Weiter habe* ϕ *keine komplexe Multiplikation. Dann gilt*

$$\#\{\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]} \mid \mathrm{Im}(\rho_{\phi,\mathfrak{l}}^{red}) \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})\} < \infty \quad .$$

Allerdings liefert der Beweis keine Informationen über solche Primstellen $\mathfrak{l}(T)$. Daher hilft er uns nicht weiter, wenn wir für konkret gegebene ϕ und $\mathfrak{l}(T)$ die Maximalität entscheiden sollen. Das Resultat von Gardeyn sagt uns allerdings, daß unsere Galoiserweiterungen nur in seltenen Fällen nicht maximal sind.

1.9 Reduktionstheorie von Drinfeld-Moduln

Sei L ein $\mathbb{F}_q[T]$-Körper, und v sei eine nichttriviale diskrete Bewertung auf L (z.B. $L = \mathbb{F}_q(u)$ oder $L = \mathbb{F}_q((u))$ ein Laurentreihenkörper und $v = v_u$). Für die Strukturabbildung $i_\phi : \mathbb{F}_q[T] \to L$ gelte

$$v(i_\phi(\mathfrak{n})) \geqslant 0 \qquad \forall \mathfrak{n} \in \mathbb{F}_q[T] .$$

Weiter sei $O_v := \{\alpha \in L \mid v(\alpha) \geqslant 0\}$, $M_v := \{\alpha \in L \mid v(\alpha) > 0\}$ und $O_v^* := O_v - M_v$.

Definition 1.9.1. *Seien die Notation und die Voraussetzungen wie oben. Weiter sei $\phi = (\mathbb{F}_q, L, i_\phi(T), \phi_T)$ ein Rang-r Drinfeld-Modul mit $\phi_T = i_\phi(T) + \sum_{i=1}^r a_i \tau^i$.*

(i) ϕ heißt ganz *an v, falls alle a_i in O_v liegen und mindestens ein a_i in O_v^* liegt.*

(ii) ϕ hat stabile Reduktion *an v über L, falls ein Drinfeld-Modul ψ über L existiert, der L-isomorph zu ϕ und ganz an v ist.*

(iii) ϕ hat gute Reduktion *an v über L, falls er stabile Reduktion an v hat und der Leitkoeffizient von ψ_T in O_v^* liegt.*

(iv) ϕ heißt instabil *an v über L, falls ϕ keine stabile Reduktion an v über L hat.*

Bemerkung 1.9.2. Ist ϕ ganz an v, so definiert

$$\tilde{\phi} := \left(\mathbb{F}_q,\ O_v/M_v,\ \overline{i_\phi(T)},\ \overline{i_\phi(T)} + \sum_{i=1}^r \overline{a_i} \tau^i \right)$$

einen neuen Drinfeld-Modul vom Grad kleiner oder gleich r. Dieser reduzierte Drinfeld-Modul wird mit

$$\mathrm{Dred}(\phi, v)$$

bezeichnet.

Da in der weiteren Arbeit nur der Fall $L = \mathbb{F}_q(u)$ und $i_\phi(T) = u$ betrachtet wird, konkretisieren wir die obigen Begriffe in dieser Situation noch weiter.

Definition 1.9.3. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \sum_{i=1}^r a_i \tau^i)$ ein Rang-r Drinfeld-Modul. Dann heißt ϕ* minimal, *falls alle $a_1, \ldots, a_r$ in $\mathbb{F}_q[u]$ liegen und falls kein $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]}$ existiert, so daß für alle $1 \leqslant i \leqslant r$ die Ungleichung $v_\mathfrak{p}(a_i) \geqslant q^i - 1$ gilt.*

Nach Bemerkung 1.5.2 besagt die obige Bedingung, daß kein $\alpha \in \mathbb{F}_q(u)$ existiert, so daß die Koeffizienten von $\alpha^{-1}\phi_T(\tau)\alpha$ noch ganz sind und kleinere Bewertung an allen endlichen Stellen haben. Ein Drinfeld-Modul heißt also minimal, falls er „minimal" in seiner $\mathbb{F}_q(u)$-Isomorphieklasse ist.

Satz 1.9.4. *Sei* $(\mathbb{F}_q, \mathbb{F}_q(u), u, \phi_T)$ *ein Rang-r Drinfeld-Modul. Dann existiert genau ein minimaler Drinfeld-Modul* ψ*, der* $\mathbb{F}_q(u)$*-isomorph zu* ϕ *ist. Dieser wird mit* $\min(\phi)$ *bezeichnet.*

Beweis: Wir zeigen zuerst die Existenz. Sei dazu $\phi_T = u + \sum_{i=1}^r a_i\tau^i$. Die a_i sind aus $\mathbb{F}_q(u)$ mit normierten Nennern. Wir definieren $m \in \mathbb{F}_q[u]$ als das kgV über die Nenner aller a_i. Dann ist

$$\psi_T := m^{-1} \cdot \phi_T \cdot m = u + \sum_{i=1}^r b_i\tau^i$$

ein $\mathbb{F}_q(u)$-isomorpher Drinfeld-Modul, der an allen endlichen Stellen ganz ist. Ist nun $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$ ein Polynom mit

$$v_{\mathfrak{p}}(b_i) \geqslant q^i - 1, \qquad \forall 1 \leqslant i \leqslant r\ ,$$

so ersetzen wir ψ_T durch $\mathfrak{p}^{-1}\psi_T\mathfrak{p}$. Dabei nimmt die $\mathfrak{p}$-Bewertung des i-ten Koeffizienten um $q^i - 1 > 0$ ab, alle anderen endlichen Bewertungen verändern sich nicht. Da die Koeffizienten nur endlich viele Teiler haben, erhält man durch Iteration nach endlich vielen Schritten einen minimalen Drinfeld-Modul. (Es ist zu beachten, daß in den Beweis entscheidend eingeht, daß $\mathbb{F}_q[u]$ die Klassenzahl Eins hat, daß also Primideale und Primelemente bis auf Einheiten „dasselbe" sind.) Kommen wir nun zur Eindeutigkeit. Seien ψ und χ zwei $\mathbb{F}_q(u)$-isomorphe minimale Drinfeld-Moduln des vorausgesetzten Typs und $c \in \mathbb{F}_q(u)^*$ mit $c^{-1}\psi_T c = \chi_T$. Dann gilt für alle $i \in \{0, \ldots, r\}$

$$\mathrm{coeff}_\tau(i, \chi_T) = c^{q^i-1} \cdot \mathrm{coeff}_\tau(i, \psi_T)\ .$$

Aufgrund der Bedingung an die Bewertung der Koeffizienten von minimalen Drinfeld-Moduln muß daher $c \in {\mathbb{F}_q}^*$ gelten. Dann folgt aus

$$c^{q^i-1} = (c^{q-1})^{\frac{q^i-1}{q-1}} = 1^{\frac{q^i-1}{q-1}} = 1 \quad ,$$

daß $\psi_T = \chi_T$ und damit $\psi = \chi$ gilt. Also ist der minimale Drinfeld-Modul zu ϕ auch eindeutig. □

Wir formulieren Definition 1.9.1 mit Hilfe des minimalen Drinfeld-Moduls neu.

Lemma 1.9.5. *Sei* $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, \phi_T)$ *ein Rang-r Drinfeld-Modul,* $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]}$*,* $v = v_{\mathfrak{p}}$*,* $\psi = \min(\phi)$ *und* $\psi_T = u + \sum_{i=1}^r b_i\tau^i$*. Dann gilt:*

(i)

$$\phi \text{ ganz an } v \iff \left\{ \begin{array}{ll} \forall i \in \{1, \ldots, r\}: & v(\mathrm{coeff}_\tau(i, \phi_T)) \geqslant 0 \\ \exists j \in \{1, \ldots, r\}: & v(\mathrm{coeff}_\tau(j, \phi_T)) = 0 \end{array} \right\}$$

(ii)

$$\phi \textit{ hat stabile Reduktion an } v \iff \min(\phi) \textit{ ganz an } v$$

(iii)

$$\phi \textit{ hat gute Reduktion an } v \iff \left\{ \begin{array}{c} \min(\phi) \textit{ ganz an } v \\ \textit{und } v(b_r) = 0 \end{array} \right\}$$

(iv)

$$\phi \textit{ instabil an } v \iff \forall i \in \{1, \ldots, r\} \textit{ gilt } v(b_i) > 0$$

Zur Verdeutlichung der Begriffe geben wir das folgende Beispiel.

Beispiel 1.9.6. Seien $\mathfrak{p}(u), \mathfrak{q}(u), \mathfrak{l}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$ paarweise verschieden. Wir betrachten

$$\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \mathfrak{p}(u)\ \mathfrak{l}(u)^{q-1}\ \mathfrak{q}(u)^{q-1}\ \tau + \mathfrak{p}(u)\ \mathfrak{l}(u)^{q^2-1}\ \mathfrak{q}(u)^{q^2}\ \tau^2) \quad .$$

Dann ist

$$\min(\phi) = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \mathfrak{p}(u)\ \tau + \mathfrak{p}(u)\ \mathfrak{q}(u)\ \tau^2) \quad .$$

Damit folgt

- ϕ ist nicht ganz an $\mathfrak{p}(u), \mathfrak{q}(u), \mathfrak{l}(u)$,
- ϕ hat für alle Stellen aus $\mathbb{P}_{\mathbb{F}_q[u]} - \{\mathfrak{p}(u)\}$ stabile Reduktion,
- ϕ ist nur an $\mathfrak{p}(u)$ instabil,
- die Menge der Stellen guter Reduktion ist $\mathbb{P}_{\mathbb{F}_q[u]} - \{\mathfrak{p}(u), \mathfrak{q}(u)\}$.

□

1.10 Rang-2 Drinfeld-Moduln

In dieser Arbeit werden wir uns hauptsächlich mit Rang-2 Drinfeld-Moduln beschäftigen. Daher werden nun einige Definitionen und Aussagen für diese Drinfeld-Moduln zusammengefaßt. Im ganzen Abschnitt seien die Rang-2 Drinfeld-Moduln $\phi = (\mathbb{F}_q, L, \alpha, \alpha + g\tau + \Delta\tau^2)$ und $\tilde{\phi} = (\mathbb{F}_q, L, \alpha, \alpha + \tilde{g}\tau + \tilde{\Delta}\tau^2)$ fest. Zuerst werden wir die Isomorphieklassen von Rang-2 Drinfeld-Moduln genauer beschreiben.

Definition 1.10.1. *Die* j-Invariante *von* ϕ *ist definiert als*

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

Es gilt:

Satz 1.10.2. *Die Drinfeld-Moduln ϕ und $\tilde{\phi}$ sind genau dann L-isomorph, wenn ein $u \in L^*$ existiert mit*

$$\tilde{g} = u^{q-1} g \qquad \textit{und} \qquad \tilde{\Delta} = u^{q^2-1} \Delta \quad .$$

Beweis: Es sind ϕ und $\tilde{\phi}$ genau dann L-isomorph, wenn ein $u \in L^*$ existiert mit $u\tilde{\phi}_T = \phi_T u$. Also genau dann, wenn

$$u\alpha + u\tilde{g}\tau + u\tilde{\Delta}\tau^2 = \alpha u + g u^q \tau + \Delta u^{q^2} \tau^2$$

gilt. Durch Koeffizientenvergleich folgt damit die Aussage. □

Korollar 1.10.3. *Mit der Notation von oben gelten die folgenden Implikationen:*

(i)
$$\phi \cong_L \tilde{\phi} \quad \Rightarrow \quad j(\phi) = j(\tilde{\phi})$$

(ii)
$$\phi \cong_{\bar{L}} \tilde{\phi} \quad \Longleftrightarrow \quad j(\phi) = j(\tilde{\phi})$$

Wir kommen nun zu einer Invarianten, die insbesondere für endliche Drinfeld-Moduln von Bedeutung ist.

Definition 1.10.4. *Sei ϕ ein Rang-2 Drinfeld-Modul wie oben, und es sei* $\mathrm{char}(\phi) = \mathfrak{p} \neq \infty$. *Dann heißt*

$$\mathrm{H}(\phi) := \mathrm{coeff}_\tau(\deg_T \mathfrak{p}, \phi_{\mathfrak{p}}) \in L$$

die Hasse-Invariante *von ϕ.*

Man rechnet leicht nach (vgl. [Jun00, Abschnitt 3.3]):

Satz 1.10.5. *Sei ϕ ein Drinfeld-Modul wie oben,* $\mathrm{char}(\phi) = \mathfrak{p} \neq \infty$, *$d = \deg_T \mathfrak{p}$ und $\phi_{\mathfrak{p}}(\tau) = \sum_{i=0}^{n} a_i \tau^i$. Dann gilt:*

(i) $n = deg_\tau(\phi_{\mathfrak{p}}) = 2d$,

(ii) $a_0 = a_1 = \ldots = a_{d-1} = 0$,

(iii) $\phi_{\mathfrak{p}}(\tau) = a_{2d}\, \tau^{2d}$, *falls* $a_d = a_{\deg_T \mathfrak{p}} = \mathrm{H}(\phi) = 0$ *gilt.*

1.11 Vergleich zur klassischen Situation

Vergleichen wir nun die klassische (Zahlentheorie über $\mathbb{Q}$) mit unserer Situation (Zahlentheorie über $\mathbb{F}_q(u)$). In der klassischen Situation ist man an der Struktur der absoluten Galoisgruppe $\mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q})$ interessiert. Dazu studiert man Darstellungen

$$\mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \to \mathrm{GL}(k, \mathbb{Z}/n) \quad .$$

Diese erhält man, indem man $\mathbb{Z}$-Modul-Strukturen auf Varietäten V über $\mathbb{Q}$ untersucht, die mit der Operation der Galoisgruppe verträglich sind. Dies ist insbesondere dann der Fall, wenn die $\mathbb{Z}$-Modul-Struktur induziert wird von einer Struktur als kommutative algebraische Gruppe auf V, wenn also V eine abelsche Varietät ist. Zu einem $n \in \mathbb{N}$ betrachtet man dann die Menge der n-Torsionspunkte

$${}_nV := \{a \in V | n \cdot a = 1_V\} \quad ,$$

die wegen der vorausgesetzten Verträglichkeit auch abgeschlossen unter der Galoisoperation ist. Ist ${}_nV$ ein freier $\mathbb{Z}/n$-Modul vom Rang k, so induziert die Galoisoperation auf ${}_nV$ eine Darstellung

$$\varphi : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \to \mathrm{GL}(k, \mathbb{Z}/n) \quad .$$

Das Bild unter dieser Darstellung ist

$$\mathrm{Im}\varphi \cong {}^{\mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q})}/_{\ker\varphi} \cong \mathrm{Gal}(\mathbb{Q}({}_nV), \mathbb{Q}) \quad ,$$

wobei

$$\mathbb{Q}({}_nV) := \mathbb{Q}\big(a_1, \ldots, a_k \mid (a_1, \ldots, a_k) \in {}_nV\big)$$

der von den Koordinaten der Punkte aus ${}_nV$ erzeugte Körper ist. Zu dieser Konstruktion geben wir nun die drei einfachsten Beispiele an.
Das erste Beispiel ist zwar trivial, wird aber aus Gründen der Systematik trotzdem erwähnt. Dazu betrachtet man die Gruppe $(\mathbb{C}, +)$ und die dadurch induzierte $\mathbb{Z}$-Modul-Struktur

$$mult: \ \mathbb{Z} \times \mathbb{C} \to \mathbb{C}, \quad (n, z) \mapsto n \cdot z \quad .$$

Dann ist für jedes $n \in \mathbb{N}$

$${}_nmult = \{z \in \mathbb{C} \mid n \cdot z = 0\} = \{0\}$$

ein Rang-0 Modul über $\mathbb{Z}/n$, es ist $\mathbb{Q}({}_nmult) = \mathbb{Q}$, und man erhält eine (nicht besonders interessante) Darstellung in die Gruppe mit nur einem Element

$$\varphi : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \to \mathrm{GL}(0, \mathbb{Z}/n) \quad .$$

Deutlich interessanter ist das nächste Beispiel. Die Gruppe $(\mathbb{C}^*, \cdot)$ induziert den $\mathbb{Z}$-Modul

$$pow: \ \mathbb{Z} \times \mathbb{C}^* \to \mathbb{C}^*, \quad (n, z) \mapsto z^n \quad .$$

Die n-Torsion dieses Moduls

$$_n pow = \{z \in \mathbb{C}^* \mid z^n = 1\}$$

sind die n-ten Einheitswurzeln, die einen freien Rang-1 Modul über $\mathbb{Z}/n$ bilden. Der zugehörige Torsionskörper $\mathbb{Q}(_n pow)$ ist der n-te Kreisteilungskörper. Man erhält eine Darstellung

$$\varphi : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \to \mathrm{GL}(1, \mathbb{Z}/n) \quad ,$$

deren Bild $\mathrm{Gal}(\mathbb{Q}(_n pow), \mathbb{Q})$ bekanntermaßen schon ganz $\mathrm{GL}(1, \mathbb{Z}/n) = (\mathbb{Z}/n)^*$ ist.

Damit kommen wir zum dritten Beispiel. Wir betrachten eine elliptische Kurve $E|\mathbb{Q}$, die durch eine kurze Weierstraßgleichung $f(x, y) = y^2 - ax^3 - bx - c \in \mathbb{Q}[x, y]$ gegeben ist. Dann ist $E(\mathbb{C}) = \{(x, y) \in \mathbb{C}^2 \mid f(x, y) = 0\} \cup \{0_E\}$. Die Punktgruppe $(E(\mathbb{C}), +)$ ist eine abelsche algebraische Gruppe und induziert die $\mathbb{Z}$-Modul-Struktur

$$*_E : \ \mathbb{Z} \times E(\mathbb{C}) \to E(\mathbb{C}), \quad (n, \alpha) \mapsto \underbrace{\alpha + \ldots + \alpha}_{n-\mathrm{mal}} \quad .$$

Zu $n \in \mathbb{N}$ betrachtet man nun die n-Torsion

$$_n E = \{\alpha \in E(\mathbb{C}) \mid n *_E \alpha = 0_E\} \quad ,$$

die einen freien Rang-2 Modul über $\mathbb{Z}/n$ bildet. Man kann zeigen, daß $_n E \cap \bar{\mathbb{Q}}^2 = {_n E} - \{0_E\}$ ist. Die Koordinaten der Torsionspunkte sind also algebraisch über $\mathbb{Q}$, und man erhält eine Darstellung

$$\varphi_{E,n} : \mathrm{Gal}(\bar{\mathbb{Q}}, \mathbb{Q}) \to \mathrm{GL}(2, \mathbb{Z}/n) \quad .$$

Im Gegensatz zu den vorherigen Beispielen kann das Bild dieser Darstellung (d.h. $\mathrm{Gal}(\mathbb{Q}(_n E), \mathbb{Q})$) eine echte Untergruppe von $\mathrm{GL}(2, \mathbb{Z}/n)$ sein. Die Größe dieses Bildes ist, beginnend mit den Arbeiten von Serre [Ser68, Ser72], intensiv untersucht worden. Zu einer fest gewählten elliptischen Kurve $E|\mathbb{Q}$ und einer Untergruppe H von $\mathrm{GL}(2, \mathbb{Z}/l)$ definieren wir, dem Artikel [Che02] folgend,

$$S_E := \{l \in \mathbb{P} \mid \mathrm{Gal}(\mathbb{Q}(_l E), \mathbb{Q}) \neq \mathrm{GL}(2, \mathbb{Z}/l)\}$$

und

$$S_E^H := \{l \in \mathbb{P} \mid \exists \sigma \in \mathrm{GL}(2, \mathbb{Z}/l) : \sigma^{-1} \mathrm{Gal}(\mathbb{Q}(_l E), \mathbb{Q}) \sigma \leqslant H\} \quad .$$

Dabei ist die letzte Menge so zu verstehen, daß die Galoisgruppen in Untergruppen vom Typ H liegen, wobei die konkrete Gruppe natürlich mit dem l variiert. Mit Hilfe der Klassifikation der maximalen Untergruppen von $\mathrm{GL}(2, \mathbb{Z}/l)$ kann man dann zeigen, daß

$$S_E = S_E^B \cup S_E^N \cup S_E^{N'} \cup S_E^D$$

gilt. Dabei bezeichnet B eine Borelgruppe in $\mathrm{GL}(2, \mathbb{Z}/l)$, N den Normalisator einer zerfallenden Cartanuntergruppe, N' den Normalisator einer nichtzerfallenden Cartanuntergruppe und D eine Untergruppe von $\mathrm{GL}(2, \mathbb{Z}/l)$, deren Bild in der $\mathrm{PGL}(2, \mathbb{Z}/l)$ in einer Untergruppe vom Typ S_4 liegt. Für genauere Definitionen sei auf Kapitel 3 verwiesen. Folgende Resultate zur Größe der Galoisgruppe wurden bisher gezeigt:

Wo	Voraussetzung an $E\vert\mathbb{Q}$	Aussage
[Maz78]	keine	$S_E^B \subset \{p \in \mathbb{P} \mid p \leqslant 37\}$
[Maz78]	keine	$S_E^D \subset \{p \in \mathbb{P} \mid p \leqslant 13\}$
[Ser72]	$E\vert\mathbb{Q}$ hat keine CM	$\#S_E < \infty$
[Ser72]	$E\vert\mathbb{Q}$ hat CM	$\mathbb{P} - \{2\} \subset S_E$
[Ser79]	$E\vert\mathbb{Q}$ hat überall gute oder multiplikative Reduktion	$S_E \subset \{2, 3, 5, 7\}$
[Ser72]	$E\vert\mathbb{Q}$ instabil, $r, \tilde{p}, l \in \mathbb{P}$, $\mathrm{v}_r(j(E)) < 0$, $\Delta(E) \not\equiv 0 \bmod l$, $\tilde{p} = \min\{p \in \mathbb{P} \mid \Delta(E) \not\equiv 0 \bmod p\}$, $\mathrm{v}_r(j(E)) \not\equiv 0 \bmod l$, $l > (\sqrt{\tilde{p}} + 1)^8$	$l \notin S_E$
[Lud95]	keine	$2 \notin S_E \iff \Delta(E) \notin \mathbb{Q}^2$ und $\psi_2(x) \in \mathbb{Q}[x]$ irreduzibel
[Lud95]	keine	$3 \notin S_E \iff \Delta(E) \notin \mathbb{Q}^3$ und $\psi_3(x) \in \mathbb{Q}[x]$ irreduzibel

Dabei bezeichnet $\Delta(E)$ die Diskriminante des minimalen Modells von E, $j(E)$ die j-Invariante und ψ_n das n-Teilungspolynom von E.

In der Tabelle fällt auf, daß das Reduktionsverhalten von E an Stellen $p \in \mathbb{P}$ von großer Bedeutung ist. Es ist also zu berücksichtigen, ob die von der reduzierten Kurve $E(\mathbb{Z}/p)$ induzierte $\mathbb{Z}$-Modul-Struktur vom Typ "*mult*" (additive Reduktion), "*pow*" (multiplikative Reduktion) oder "$*_E$" (gute Reduktion) ist.

Die auf einer additiv geschriebenen abelschen Gruppe induzierte $\mathbb{Z}$-Modulstruktur ist die Multiplikation. Eine multiplikativ geschriebene Gruppe kann durch Exponentiation als $\mathbb{Z}$-Modul betrachtet werden. Daher korrespondiert die additive Reduktion zu "*mult*" und die multiplikative zu "*pow*".

In ihrer Diplomarbeit [Lud95] hat Andrea Ludwig einen Algorithmus entwickelt, der beweist, daß für $l \in \mathbb{P}$

$$\mathrm{Gal}(\mathbb{Q}({}_lE), \mathbb{Q}) = \mathrm{GL}(2, \mathbb{Z}/l)$$

gilt, sofern er terminiert. Rechnungen zeigen, daß er im allgemeinen sehr schnell terminiert, falls Gleichheit gilt.
Wir haben in dieser Arbeit den Algorithmus von A. Ludwig auf Rang-2 Drinfeld-Moduln $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ übertragen. Rang-2 Drinfeld-Moduln werden als das Analogon zu elliptischen Kurven in Kongruenzfunktionenkörpern (Funktionenkörpern mit endlichem Konstantenkörper) betrachtet. In Kongruenzfunktionenkörpern spielt $\mathbb{F}_q[T]$ die gleiche Rolle, die $\mathbb{Z}$ in Zahlkörpern spielt. Da ein Rang-2 Drinfeld-Modul eine $\mathbb{F}_q[T]$-Modul-Struktur induziert und für $\mathfrak{n}(T) \in \mathbb{F}_q[T]$ die $\mathfrak{n}$-Torsion einen freien Rang-2 Modul über $\mathbb{F}_q[T]/\mathfrak{n}$ bildet, verhalten sich elliptische Kurven über Zahlkörpern und Rang-2 Drinfeld-Moduln über $\mathbb{F}_q(u)$ sehr ähnlich.
Den von uns erwähnten $\mathbb{Z}$-Moduln stehen die folgenden Drinfeld-Moduln gegenüber:

$\mathbb{Z}$	$\mathbb{F}_q[T]$
mult	$(\mathbb{F}_q, \mathbb{F}_q(u), u, u\tau^0)$
pow	$(\mathbb{F}_q, \mathbb{F}_q(u), u, u + \tilde{\Delta}\tau)$
$*_E$	$(\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$

mit $\Delta \neq 0 \neq \tilde{\Delta}$. Hierbei waren wir nicht ganz exakt, da $(\mathbb{F}_q, \mathbb{F}_q(u), u, u\tau^0)$ per Definition kein Drinfeld-Modul ist. Um die Analogie zu verdeutlichen, haben wir ihn trotzdem in die Tabelle aufgenommen.
Folgende Probleme treten bei der Übertragung des Algorithmus auf. Dabei bezeichnet $l \in \mathbb{P}$ immer den Führer und $p \in \mathbb{P}$ eine Stelle, an der die elliptische Kurve reduziert wird.
Im Fall der elliptischen Kurven treten nach Reduktion lediglich endliche Primkörper $\mathbb{Z}/p$ auf. Auch das Bild der Galoisdarstellung liegt in der GL(2) über einem endlichen Primkörper. In diesem Fall sind die Charakteristik und die Mächtigkeit des endlichen Körpers gleich.
Für Drinfeld-Moduln treten allerdings sowohl nach Reduktion als auch im Bild der $\mathfrak{l}$-Torsionsdarstellung beliebige endliche Körper auf. Dadurch wird die Untergruppenstruktur von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$, in der ja die Galoisgruppe liegt, komplexer. Außerdem muß bei solchen Körpern zwischen Charakteristik und Mächtigkeit unterschieden werden.
Häufig wird bei elliptischen Kurven $p, l > 5$ vorausgesetzt. Damit werden sowohl die Fälle, daß $\#\mathrm{GL}(2, \mathbb{Z}/l)$ klein ist (und Sonderfälle auftreten), als auch die für elliptische Kurven immer speziellen Charakteristiken 2 und 3 ausgeschlossen. Im Fall der Drinfeld-Moduln kann $\#\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ auch in Charakteristik $2, 3$ beliebig groß werden.

Will man das Verhalten einer fest gewählten elliptischen Kurve $E|\mathbb{Q}$ untersuchen, reicht es meist, sie an fast allen Stellen zu untersuchen. In diesem Fall ist die Einschränkung $p > 5$ nicht relevant. Insbesondere kann jede elliptische Kurve unter dieser Einschränkung behandelt werden.
Demgegenüber schließt die Forderung $\mathrm{char}(\mathbb{F}_{\mathfrak{l}}) > 5$ die Untersuchung aller Drinfeld-Moduln $(\mathbb{F}_q, \mathbb{F}_q(u), u, \phi_T)$ mit $\mathrm{char}(\mathbb{F}_q) \in \{2,3,5\}$ aus. Daher müssen zur Untersuchung der Torsion alle Charakteristiken zugelassen werden.
Weiterhin enthält für nichtprime Körper $\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})$ die Untergruppe $\mathrm{GL}(2,\mathbb{F}_r)$ mit $\mathbb{F}_r \subsetneq \mathbb{F}_{\mathfrak{l}}$. Diese Gruppen können unter Umständen auch als Galoisgruppen auftreten.
Ein weiterer Unterschied tritt im Zusammenspiel von Rang-1 und Rang-2 Strukturen auf.
Im Fall von elliptischen Kurven werden mittels der Weil-Paarung die Galoisgruppen $\mathrm{Gal}(\mathbb{Q}({}_nE),\mathbb{Q})$ und $\mathrm{Gal}(\mathbb{Q}({}_npow),\mathbb{Q})$ in Verbindung gebracht. Für die letztere gilt immer $\mathrm{Gal}(\mathbb{Q}({}_npow),\mathbb{Q}) = \mathrm{GL}(1,\mathbb{Z}/n) = (\mathbb{Z}/n)^*$. Daraus folgt dann, daß für alle E und n

$$\mathrm{Gal}(\mathbb{Q}({}_nE),\mathbb{Q}) \nleq \mathrm{SL}(2,\mathbb{Z}/n)$$

gilt. Dabei ist zu betonen, daß der Modul “*pow*” unabhängig von der gewählten Kurve E ist.
Im Fall von Drinfeld-Moduln wird mit analogen Argumenten der Rang-2 Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u+g\tau+\Delta\tau^2)$ mit dem Rang-1 Modul $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u-\Delta\tau)$ in Verbindung gebracht. Hierbei hängt ψ von ϕ ab. Ein solches ψ kann an manchen Stellen schlechte Reduktion haben. Damit kann im Fall $\mathrm{ggT}(\mathfrak{n},\Delta) \neq 1$ die $\mathfrak{n}$-Torsionserweiterung kleiner werden. Z.B. ist im Fall von $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u-u\tau)$ die T-Torsion gerade $\mathbb{F}_q$, und damit ist

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_T\psi]\,, \mathbb{F}_q(u)) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \right\} \quad .$$

Da eine $\mathfrak{l}$-Torsionserweiterung von ψ nicht maximal sein muß, gibt es Beispiele (vgl. Tabelle Seite 151) für

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u)) \leqslant \mathrm{SL}(2,\mathbb{F}_{\mathfrak{l}}) \quad .$$

Kapitel 2

Endliche Drinfeld-Moduln

Wir werden später globale (über $\mathbb{F}_q(u)$ definierte) Rang-2 Drinfeld-Moduln untersuchen, indem wir sie an endlichen Stellen reduzieren und die zugehörigen endlichen Drinfeld-Moduln betrachten. Daher werden in diesem Kapitel die wichtigsten Tatsachen zu endlichen Drinfeld-Moduln dargestellt. Insbesondere wird die effiziente Berechnung des zugehörigen charakteristischen Polynoms behandelt.
Die Darstellung folgt den Arbeiten [Gek91] bzw. [Gos96, Abschnitt 4.12].

2.1 Das charakteristische Polynom

Analog zu elliptischen Kurven über endlichen Körpern ordnet man auch endlichen Drinfeld-Moduln ein charakteristisches Polynom zu.
Sei also L ein endlicher Körper und $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ ein Rang-r Drinfeld-Modul. Dann ist $\mathfrak{p} := \mathrm{char}(\phi)$ endlich und kann daher als normiertes Primpolynom in $\mathbb{F}_q[T]$ aufgefaßt werden. Das Bild des Polynomrings $\mathbb{F}_q[T]$ unter der Abbildung i_ϕ ist ein Teilkörper von L, den wir mit $\mathbb{F}_{\mathfrak{p}}$ bezeichnen. Es ist klar, daß $\mathbb{F}_{\mathfrak{p}}$ isomorph zu ${}^{\mathbb{F}_q[T]}/_{\mathfrak{p}}$ ist. Weiter definieren wir $m := [L : \mathbb{F}_{\mathfrak{p}}]$, $d := [\mathbb{F}_{\mathfrak{p}} : \mathbb{F}_q]$ und $n := [L : \mathbb{F}_q]$.

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

Sei $\mathcal{F}_L : x \to x^{\#L}$ der Frobenius zu L. Wir haben τ mit dem Frobenius $x \to x^q$ von $\mathbb{F}_q$ identifiziert und erhalten $\mathcal{F}_L = \tau^n \in L\{\tau\}$. Da $\mathcal{F}_L$ mit ϕ_T kommutiert, ist $\mathcal{F}_L$ ein Element von $\mathrm{End}_L(\phi)$. Sei nun $\mathfrak{q} \neq \mathrm{char}(\phi)$ aus $\mathbb{P}_{\mathbb{F}_q[T]}$. Dann operiert $\mathrm{End}_L(\phi)$ auf dem Tate-Modul $T_{\mathfrak{q}}(\phi)$, und wir erhalten eine injektive Abbildung (vgl. [Gek91, S.190])

$$i_{\mathfrak{q}} : \mathrm{End}_L(\phi) \otimes_{\mathbb{F}_q[T]} (\mathbb{F}_q[T])_{\mathfrak{q}} \hookrightarrow \mathrm{End}_{(\mathbb{F}_q[T])_{\mathfrak{q}}}(T_{\mathfrak{q}}(\phi)) \ ,$$

und nach Satz 1.8.2 gilt

$$\mathrm{End}_{(\mathbb{F}_q[T])_\mathfrak{q}}(T_\mathfrak{q}(\phi)) \cong \mathrm{Mat}(rg(\phi), (\mathbb{F}_q[T])_\mathfrak{q}) \ .$$

Betrachtet man nun das Bild $i_\mathfrak{q}(\mathcal{F}_L \otimes 1)$ des Frobenius unter dieser Abbildung, so erhält man das folgende interessante Resultat.

Satz 2.1.1. *Sei $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ ein endlicher Rang-r Drinfeld-Modul. Es seien $\mathfrak{q}, \mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$, und $\mathfrak{q}, \mathfrak{l}, \mathrm{char}(\phi)$ seien paarweise verschieden. Dann gilt*

$$\det(X - i_\mathfrak{q}(\mathcal{F}_L \otimes 1)) = \det(X - i_\mathfrak{l}(\mathcal{F}_L \otimes 1))$$

und

$$\det(X - i_\mathfrak{q}(\mathcal{F}_L \otimes 1)) \in (\mathbb{F}_q[T])[X] \ .$$

Beweis: [Gek91, Corollary 3.4] □

Das charakteristische Polynom von $\mathcal{F}_L$ unter der $\mathfrak{q}$-adischen Darstellung $i_\mathfrak{q}$ hat also Koeffizienten, die nicht nur in der Lokalisierung $(\mathbb{F}_q[T])_\mathfrak{p}$, sondern bereits in $\mathbb{F}_q[T]$ selbst liegen und unabhängig von $\mathfrak{q}$ sind. Der obige Satz erlaubt nun die folgende Definition.

Definition 2.1.2. *Sei $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ ein endlicher Rang-r Drinfeld-Modul, $\mathfrak{q} \in \mathbb{P}_{\mathbb{F}_q[T]}$ und $\mathfrak{q} \neq \mathrm{char}(\phi)$. Dann heißt*

$$\mathcal{P}_\phi := \det(X - i_\mathfrak{q}(\mathcal{F}_L \otimes 1))$$

das charakteristische Polynom *des Drinfeld-Moduls ϕ. Es ist ein Polynom in $(\mathbb{F}_q[T])[X]$.*

Das charakteristische Polynom ist eine Isogenie-Invariante, denn es gilt

Proposition 2.1.3. *Seien $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ und $\psi = (\mathbb{F}_q, L, \alpha, \psi_T)$ zwei endliche Rang-r Drinfeld-Moduln. Dann ist ϕ genau dann L-isogen zu ψ, wenn $\mathcal{P}_\phi = \mathcal{P}_\psi$ gilt.*

Für weiterführende Aussagen über $\mathcal{P}_\phi$ sei auf [HY00] verwiesen.
Wir kommen nun zur Definition der Euler-Poincaré-Charakteristik. Wir betrachten einen endlichen Rang-r Drinfeld-Modul $\phi = (\mathbb{F}_q, L, \alpha, \phi_T)$ und einen $*_\phi$ - Untermodul $M \neq 0$ von L. Da M ein endlicher Modul über dem Hauptidealring $\mathbb{F}_q[T]$ ist, existieren $\mathfrak{q}_1, \ldots, \mathfrak{q}_k \in \mathbb{P}_{\mathbb{F}_q[T]}$ (nicht notwendig paarweise verschieden) und $e_1, \ldots, e_k \in \mathbb{N}$, so daß

$$M \cong_\phi \prod_{i=1}^{k} \mathbb{F}_q[T] / \mathfrak{q}_i^{e_i}$$

gilt.

Definition 2.1.4. *Mit den Bezeichnungen von oben heißt das Polynom*

$$\mathrm{EP}(M,\phi) := \prod_{i=1}^{k} \mathfrak{q}_i^{e_i} \in \mathbb{F}_q[T]$$

die Euler-Poincaré-Charakteristik *des endlichen $*_\phi$ -Moduls M.*

Es gilt nun der Satz

Satz 2.1.5. *Es ist*

$$\mathcal{P}_\phi(0) = c \cdot \mathrm{char}(\phi)^{[L:i_\phi(\mathbb{F}_q[T])]}$$

und

$$\mathcal{P}_\phi(1) = c \cdot \mathrm{EP}(L,\phi)\ ,$$

wobei c in ${\mathbb{F}_q}^*$ liegt.

2.2 Das charakteristische Polynom im Rang-2 Fall

Sei wieder $\phi = (\mathbb{F}_q, L, \alpha, \alpha + g\tau + \Delta\tau^2)$ ein endlicher Rang-2 Drinfeld-Modul mit Charakteristik $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[T]}$. Dann gilt (vgl. z.B. [Gek91]), daß für passende $A(T) \in \mathbb{F}_q[T]$ und $\epsilon_\phi \in {\mathbb{F}_q}^*$

$$\mathcal{P}_\phi = X^2 + A(T)\cdot X + \epsilon_\phi \mathfrak{p}^{[L:i_\phi(\mathbb{F}_q[T])]} \in \mathbb{F}_q[T][X]$$

ist. Nach dem „Satz von Hasse" für Drinfeld-Moduln (siehe [GS97, Theorem 4.4]) ist

$$\deg_T(A) \leqslant \frac{\deg_T(\mathfrak{p})}{2} \cdot [L : i_\phi(\mathbb{F}_q[T])]\ .$$

Bemerkung 2.2.1. Der Satz von Hasse gilt in einer weit allgemeineren Situation. In unserem konkreten Fall erhält man die Aussage direkt, indem man in

$$\mathcal{F}_L^2 + A(T) *_\phi \mathcal{F}_L + \epsilon_\phi \mathfrak{p}^{[L:i_\phi(\mathbb{F}_q[T])]} = 0$$

mit $\mathcal{F}_L = \tau^{[L:\mathbb{F}_q]}$ Koeffizientenvergleich nach τ durchführt.

Der Wert von ϵ_ϕ wird in [Jun00, Prop. 4.2.5] explizit angegeben. Es gilt:

Lemma 2.2.2. *In der Situation von oben ist*

$$\epsilon_\phi = (\mathrm{Norm}^L_{\mathbb{F}_q}(-\Delta))^{-1} \in {\mathbb{F}_q}^*\ .$$

Um $A(T)$ schnell zu berechnen, nutzen wir die folgende Proposition aus [Jun00, S.70].

Proposition 2.2.3. *In der Situation von oben gilt*

$$i_\phi(A(T)) = -\epsilon_\phi \cdot \mathrm{Norm}^L_{\mathbb{F}_\mathfrak{p}}(\mathrm{H}(\phi)) \in \mathbb{F}_\mathfrak{p} \ .$$

Dabei bezeichnet $\mathrm{H}(\phi)$ *die Hasse-Invariante von* ϕ.

Wir betrachten nun den Spezialfall

$$L = \mathbb{F}_\mathfrak{p} = \mathbb{F}_q[u]/\mathfrak{p}(u) = \left\{ \overline{h(u)} \mid h(u) \in \mathbb{F}_q[u] \right\}$$

und

$$\phi = (\mathbb{F}_q,\ \mathbb{F}_q[u]/\mathfrak{p}(u)\ , \overline{u}, \overline{u} + g\tau + \Delta\tau^2) \quad .$$

Dieser Fall tritt insbesondere immer dann auf, wenn der endliche Drinfeld-Modul durch Reduktion eines globalen Drinfeld-Moduls der Form $(\mathbb{F}_q, \mathbb{F}_q(u), u, \phi_T)$ entsteht. Wir erhalten aus Proposition 2.2.3

$$i_\phi(A(T)) = \overline{A(u)} = -\epsilon_\phi \cdot \mathrm{H}(\phi) \ .$$

Es existiert genau ein Element $B(T) \in \mathbb{F}_q[T]$ mit $\deg_T(B) < \deg_T(\mathfrak{p})$ und Bild $i_\phi(B) = \mathrm{H}(\phi) \in \mathbb{F}_\mathfrak{p}$. Da nach dem Satz von Hasse $\deg_T(A) \leqslant \frac{\deg_T(\mathfrak{p})}{2}$ ist, folgt aus 2.2.3 $A(T) = -\epsilon_\phi \cdot B(T) \in \mathbb{F}_q[T]$. Wir schreiben (nicht ganz korrekt, aber suggestiv)

$$A(T) = -\epsilon_\phi \cdot \mathrm{H}(\phi) \ .$$

Weiterhin verwenden wir folgendes Resultat aus [Gek88], das wir nach [Cor99] als Delignes Kongruenz bezeichnen.

Satz 2.2.4 (Delignes Kongruenz). *Seien* $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[T]}$ *und* $\phi = (\mathbb{F}_q, \mathbb{F}_\mathfrak{p}, \overline{u}, \overline{u} + g\tau + \Delta\tau^2)$ *ein Rang-2 Drinfeld-Modul. Sei weiter* $c_0 = 0$, $c_1 = g$ *und* $c_k = -(\overline{u}^{q^{k-1}} - \overline{u}) \cdot c_{k-2} \cdot \Delta^{q^{k-2}} + c_{k-1} \cdot g^{q^{k-1}}$. *Dann ist*

$$c_{\deg_T(\mathfrak{p})} = \mathrm{H}(\phi) \ .$$

Wir fassen den Absatz in dem folgenden Satz zusammen, der es uns erlaubt, das charakteristische Polynom $\mathcal{P}_\phi$ effizient zu berechnen.

Satz 2.2.5. *Seien* $\mathfrak{p}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, $d = \deg_T(\mathfrak{p})$, $g \in \mathbb{F}_\mathfrak{p}$, $\Delta \in \mathbb{F}_\mathfrak{p}^*$, *und* $\phi = (\mathbb{F}_q, \mathbb{F}_\mathfrak{p}, \overline{u}, \overline{u} + g\tau + \Delta\tau^2)$. *Dann ist*

$$\mathcal{P}_\phi = X^2 - \epsilon_\phi \cdot i_\phi^{-1}(c_d)\ X + \epsilon_\phi \mathfrak{p}(T) \ \in \mathbb{F}_q[T][X] \ .$$

Dabei ist

$$\epsilon_\phi = (-1)^d \cdot \Delta^{\frac{q^d-1}{q-1}} \in \mathbb{F}_q{}^* \ ,$$

und c_d *genügt der Rekursion*

$$\begin{aligned} c_0 &= 0 \ , \\ c_1 &= g \ , \\ c_k &= -(\overline{u}^{q^{k-1}} - \overline{u}) \cdot c_{k-2} \cdot \Delta^{q^{k-2}} + c_{k-1} \cdot g^{q^{k-1}} \ . \end{aligned}$$

Weiter bezeichnet $i_\phi^{-1}(c_d)$ *das eindeutig bestimmte Urbild von* c_d *in* $\mathbb{F}_q[T]$ *vom Grad echt kleiner* $\deg_T(\mathfrak{p})$.

Kapitel 3

Die Gruppen $\mathrm{GL}(2, \mathbb{F}_r)$ und $\mathrm{PGL}(2, \mathbb{F}_r)$

Da die von uns untersuchte Galoisgruppe $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$ eine Untergruppe der endlichen linearen Gruppe $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ ist, werden wir diese im vorliegenden Kapitel genauer beleuchten. In unseren Untersuchungen treten endliche Körper in verschiedenen Bedeutungen auf ($\mathbb{F}_p, \mathbb{F}_q, \mathbb{F}_{\mathfrak{l}}$ oder $\mathbb{F}_{\mathfrak{p}}$). Daher werden wir in diesem Kapitel den zugrundeliegenden Körper $\mathbb{F}_r$ nennen, wobei $\#\mathbb{F}_r = r$ gelten soll. Die Charakteristik von $\mathbb{F}_r$ ist p. Untergruppen der GL werden wir mit großen Frakturbuchstaben bezeichnen. Das neutrale Element in der $\mathrm{GL}(2, \mathbb{F}_r)$ nennen wir E.
Die Untersuchungen in diesem Kapitel sind rein gruppentheoretischer Natur und sind völlig unabhängig von der Theorie der Drinfeld-Moduln. Die Verbindung wird erst in den nächsten Kapiteln hergestellt. Insbesondere interessieren uns die maximalen Untergruppen der $\mathrm{GL}(2, \mathbb{F}_r)$ und wie man ausschließt, daß ein bis auf Konjugation gegebenes Element in einer vorgegebenen maximalen Untergruppe liegt. Da die maximalen Untergruppen der $\mathrm{PGL}(2, \mathbb{F}_r)$ in der Literatur (vgl. [Hup67] oder [VM80]) besser untersucht sind, werden wir dazu unsere Elemente in die $\mathrm{PGL}(2, \mathbb{F}_r)$ abbilden und die Information danach wieder auf $\mathrm{GL}(2, \mathbb{F}_r)$ hochliften. Eine nützliche Untersuchung der Gruppe $\mathrm{GL}(2, \mathbb{F}_r)$ ist auch in [Lan76] zu finden.
Wir stellen in diesem Kapitel die Aussagen über $\mathrm{GL}(2, \mathbb{F}_r)$ und $\mathrm{PGL}(2, \mathbb{F}_r)$ zusammen, die wir später im Algorithmus verwenden werden. Bei einigen Aussagen wird daher erst in Kapitel 5 klar werden, warum wir sie hier betonen.

3.1 Die Konjugationsklassen von $\mathrm{GL}(2, \mathbb{F}_r)$

Es ist bekannt, daß die Konjugationsklassen in der $\mathrm{GL}(2, K)$ über einem Körper K durch die Jordanschen Normalformen bestimmt werden. Dies gilt nach [Lan93, S.557f] sinngemäß auch für nicht algebraisch abgeschlossene Körper. Wir geben nun kurz für die $\mathrm{GL}(2,\mathbb{F}_r)$ die Konjugationstypen, deren Anzahl, Größe und die Ordnung der jeweiligen Vertreter an.

$\mathrm{GL}(2,\mathbb{F}_r)$			
Klassentyp	Anzahl der Klassen	Elemente je Klasse	Ordnung
$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ $_{a\neq b,\ ab\neq 0}$	$\frac{1}{2}(r-1)(r-2)$	$r(r+1)$	$\mathrm{kgV}(\mathrm{ord}(a),\mathrm{ord}(b))$
$\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$	$(r-1)$	1	$\mathrm{ord}(a)$
$\begin{pmatrix} a & 1 \\ 0 & a \end{pmatrix}$	$(r-1)$	$(r-1)(r+1)$	$p\ \mathrm{ord}(a)$
$\begin{pmatrix} 0 & a \\ 1 & b \end{pmatrix}$ $_{(x-\gamma)(x-\gamma^r) = x^2-bx-a\in\mathbb{F}_r[x]\ \mathrm{prim}}$	$\frac{1}{2}\ r\ (r-1)$	$r(r-1)$	$\mathrm{ord}_{\mathbb{F}^*_{r^2}}(\gamma)$

Eine Matrix M heißt *halbeinfach*, falls sie nicht den Konjugationstyp $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$ hat. Aus der obigen Tabelle ergibt sich direkt das folgende Lemma.

Lemma 3.1.1. *Sei $M \in \mathrm{GL}(2,\mathbb{F}_r)$. Dann sind äquivalent:*

(i) $\mathrm{v}_p(\mathrm{ord}_{\mathrm{GL}}(M)) > 0$,

(ii) $\mathrm{v}_p(\mathrm{ord}_{\mathrm{GL}}(M)) = 1$,

(iii) M ist nicht halbeinfach,

(iv) M hat den Konjugationstyp $\left(\begin{smallmatrix} a & 1 \\ 0 & a \end{smallmatrix}\right)$.

3.2 Untergruppen von $\mathrm{GL}(2,\mathbb{F}_r)$

Definition 3.2.1. *(i) Die Gruppe* $\mathrm{SL}(2,\mathbb{F}_r) := \{M \in \mathrm{GL}(2,\mathbb{F}_r) \,|\, \det(M) = 1\}$ *heißt* spezielle lineare Gruppe.

(ii) Die Gruppe $B := \{\left(\begin{smallmatrix} a & b \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_r)\}$ heißt die Standard-Borelgruppe. *Eine Gruppe heißt* Borelgruppe, *wenn sie zu B konjugiert ist. Solche Untergruppen werden mit $\mathfrak{B}$ bezeichnet.*

(iii) Die Gruppe $\mathfrak{S} := \{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_r)\}$ heißt die Skalargruppe.

(iv) Die Gruppe $\mathfrak{D} := \{\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_r)\}$ heißt die Diagonalgruppe.

(v) Eine Untergruppe heißt zerfallende Cartanuntergruppe, *wenn sie zu $\mathfrak{D}$ konjugiert ist. Solche Untergruppen werden mit $\mathfrak{Z}$ bezeichnet.*

(vi) *Eine Untergruppe heißt* nichtzerfallende Cartanuntergruppe*, falls sie isomorph zu* $\mathbb{F}_{r^2}^*$ *ist. Solche Untergruppen werden mit* $\mathfrak{T}$ *bezeichnet.*

Bemerkung 3.2.2. Nichtzerfallende Cartanuntergruppen werden in $\mathrm{GL}(2,\mathbb{F}_r)$ wie folgt realisiert. Man betrachtet den Körper $\mathbb{F}_{r^2}$ als 2-dimensionalen $\mathbb{F}_r$-Vektorraum. Zu einem Element $\alpha \in \mathbb{F}_{r^2}^*$ betrachtet man die durch Multiplikation mit α induzierte $\mathbb{F}_r$-lineare Abbildung auf $\mathbb{F}_{r^2}$. Diese Abbildung ist ein Automorphismus des $\mathbb{F}_r$-Vektorraums $\mathbb{F}_{r^2}$. Nach Wahl einer Basis erhält man so eine Einbettung von $\mathbb{F}_{r^2}^*$ in $\mathrm{GL}(2,\mathbb{F}_r)$. Die Bilder unter diesen Einbettungen (die ja von der Wahl der Basis abhängen) sind genau die nichtzerfallenden Cartanuntergruppen.

Bemerkung 3.2.3. Da wir uns in diesem Kapitel stark auf das Buch [Hup67] von Huppert stützen, stellen wir seine Bezeichnungen unseren gegenüber. Ein Element heißt dort *Transvektion* , falls es zu einer Matrix der Form $\left(\begin{smallmatrix}1 & a\\ 0 & 1\end{smallmatrix}\right)$ konjugiert ist. Mit $\mathfrak{T}(H)$ bezeichnet er die zu $\left(\begin{smallmatrix}1 & *\\ 0 & 1\end{smallmatrix}\right)$ konjugierten Untergruppen. Demgegenüber bezeichnet $\mathfrak{T}$ eine nichtzerfallende Cartanuntergruppe. Erzeugende Elemente von $\mathfrak{T}$ werden manchmal auch *Singer-Zykel* genannt. Singer-Zykel sind also genau die Elemente der Ordnung r^2-1 in $\mathrm{GL}(2,\mathbb{F}_r)$.

Die Normalisatoren von Cartanuntergruppen sind maximale Untergruppen in $\mathrm{GL}(2,\mathbb{F}_r)$. Ihre Größe liefert das folgende Lemma.

Lemma 3.2.4. *Sei* $C \leqslant \mathrm{GL}(2,\mathbb{F}_r)$ *eine Cartanuntergruppe und* $\mathrm{Norm}(C)$ *ihr Normalisator. Dann gilt:*

$$[\mathrm{Norm}(C):C] = \begin{cases} 6 \;;\; \mathbb{F}_r = \mathbb{F}_2 \textit{ und } C \textit{ ist zerfallend} \\ 2 \;;\; \textit{sonst} \end{cases}$$

Beweis: Der nichtzerfallende Fall wird in Satz 7.3 in [Hup67, S.187] bewiesen. Ist C zerfallend, so können wir o.B.d.A. $C = \mathfrak{D}$ annehmen. Indem wir für allgemeines $M = \left(\begin{smallmatrix} m_{11} & m_{12}\\ m_{21} & m_{22}\end{smallmatrix}\right)$ und $a \neq b$

$$M^{-1}\begin{pmatrix} a & 0\\ 0 & b\end{pmatrix} M = \begin{pmatrix} a' & 0\\ 0 & b'\end{pmatrix}$$

ansetzen, erhalten wir für $\mathbb{F}_r \neq \mathbb{F}_2$

$$\mathrm{Norm}(C) = \left\{ \begin{pmatrix} 0 & a\\ b & 0\end{pmatrix}, \begin{pmatrix} a & 0\\ 0 & b\end{pmatrix} \mid a,b \in {\mathbb{F}_r}^* \right\} \quad .$$

In $\mathbb{F}_2^*$ können wir nicht $a \neq b$ wählen. In diesem Fall ist $C = \{1\}$ und $\mathrm{Norm}(C) = \mathrm{GL}(2,\mathbb{F}_2) = S_3$. □

Der Normalisator einer zerfallenden Cartanuntergruppe kann immer auf die Form

$$\left\{ \begin{pmatrix} a & 0\\ 0 & b\end{pmatrix} \;,\; \begin{pmatrix} 0 & a\\ b & 0\end{pmatrix} \mid a,b \in {\mathbb{F}_r}^* \right\}$$

konjugiert werden. In ungerader Charakteristik kann der Normalisator einer nichtzerfallenden Cartangruppe nach Wahl eines Nichtquadrats $\lambda \in {\mathbb{F}_r}^*$ auf die Form

$$\left\{ \begin{pmatrix} a & \lambda b \\ b & a \end{pmatrix} , \begin{pmatrix} a & \lambda b \\ -b & -a \end{pmatrix} \mid a, b \in \mathbb{F}_r, (a,b) \neq (0,0) \right\}$$

konjugiert werden. Abstrakt schreibt sich ein solcher Normalisator einer nichtzerfallenden Cartangruppe als

$$\langle \alpha, \beta \mid \alpha^{r^2-1} = 1 = \beta^2,\ \alpha\beta = \beta\alpha^r \rangle \quad .$$

Später werden wir uns damit beschäftigen, was man über die Größe einer Untergruppe G von $\mathrm{GL}(2,\mathbb{F}_r)$ sagen kann, wenn man Informationen über einige Elemente in G besitzt. In diesem Zusammenhang wird uns der folgende Satz von Nutzen sein:

Satz 3.2.5. *Sei K ein Körper und G eine Untergruppe von $\mathrm{GL}(2,K)$. Weiter sei*

$$U = \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in K \right\}$$

in G enthalten. Existiert dann eine Matrix A in G mit (über K) irreduziblem charakteristischen Polynom, so gilt bereits

$$\mathrm{SL}(2,K) \leqslant G \quad .$$

Beweis: Sei $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine Matrix aus G mit irreduziblem charakteristischen Polynom. Dann ist insbesondere a_{21} ungleich 0. Damit liegt auch die Matrix

$$A_2 := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} 1 & -\frac{a_{22}}{a_{21}} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a_{11} & -\frac{\det(A)}{a_{21}} \\ a_{21} & 0 \end{pmatrix}$$

in G. Dann können wir in G auch

$$A_2^{-1} \begin{pmatrix} 1 & -\frac{\det(A)}{a_{21}^2} \\ 0 & 1 \end{pmatrix} A_2 = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

und

$$\begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

bilden. Somit liegt für jedes $b \in K$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^{-1} \cdot \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ -b & 1 \end{pmatrix}$$

in G. Nach [Lan76, S.178] erzeugen die Untergruppen $\left(\begin{smallmatrix} 1 & K \\ 0 & 1 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 1 & 0 \\ K & 1 \end{smallmatrix}\right)$ bereits die ganze $\mathrm{SL}(2,K)$, und damit ist die Aussage gezeigt. $\square$

3.3 Die Gruppe $\mathrm{PGL}(2,\mathbb{F}_r)$

Im weiteren bezeichnet

$$\begin{array}{rcccc} \mathrm{P} & : & \mathrm{GL}(2,\mathbb{F}_r) & \to & \mathrm{PGL}(2,\mathbb{F}_r) \\ & & M & \mapsto & \{\lambda\, M \mid \lambda \in {\mathbb{F}_r}^*\} \end{array}$$

die kanonische Restklassenabbildung. Die Bilder von Objekten aus $\mathrm{GL}(2,\mathbb{F}_r)$ werden durch ein vorgestelltes P bezeichnet. Zu einer Untergruppe $G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$ bezeichnet $\mathrm{P}G$ das Bild in $\mathrm{PGL}(2,\mathbb{F}_r)$. Ist $M = \left(\begin{smallmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_r)$, so schreiben wir $\mathrm{P}M$ als $\begin{bmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{bmatrix}$ bzw. $[M] \in \mathrm{PGL}(2,\mathbb{F}_r)$.
Wir werden später Aussagen über Untergruppen der $\mathrm{PGL}(2,\mathbb{F}_r)$ machen, indem wir charakteristische Polynome von Elementen aus $\mathrm{GL}(2,\mathbb{F}_r)$ berechnen. Daher vergleichen wir im folgenden Lemma die charakteristischen Polynome von Matrizen M, die in $\mathrm{PGL}(2,\mathbb{F}_r)$ dasselbe Element $[M]$ liefern. Das charakteristische Polynom einer Matrix M werden wir mit $\mathrm{charpol}_M(x)$ bezeichnen.

Lemma 3.3.1. *Sei K ein Körper, $M \in \mathrm{GL}(2,K)$ und $\lambda \in K^*$. Dann gilt:*

(i)
$$\mathrm{charpol}_{\lambda M}(x) = \lambda^2 \; \mathrm{charpol}_M(\frac{x}{\lambda}) \quad ,$$

(ii)
$$\mathrm{charpol}_{\lambda M}(x) = x^2 - \lambda \mathrm{Tr}(M)\; x + \lambda^2 \det(M) \quad ,$$

(iii)
$$\frac{\mathrm{Tr}(M)^2}{\det(M)} = \frac{\mathrm{Tr}(\lambda M)^2}{\det(\lambda M)} \quad ,$$

(iv)
$$\mathrm{charpol}_{\lambda M}(x) \textit{ irreduzibel } \iff \mathrm{charpol}_M(x) \textit{ irreduzibel} \quad .$$

Beweis: Klar. □

Wir untersuchen nun die Ordnungen und Konjugationsklassen von Elementen in $\mathrm{PGL}(2,\mathbb{F}_r)$. Dabei kürzen wir $\mathrm{ord}_{\mathrm{GL}(2,\mathbb{F}_r)}(M)$ durch $\mathrm{ord}_{\mathrm{GL}}(M)$ und $\mathrm{ord}_{\mathrm{PGL}(2,\mathbb{F}_r)}([M])$ durch $\mathrm{ord}_{\mathrm{PGL}}([M])$ ab. Sind $[M]$ und $[N]$ konjugiert, so schreiben wir $[M] \sim [N]$.
Wir betrachten auf

$$\mathcal{CP} := \{x^2 + ax + b \mid a, b \in \mathbb{F}_r, b \neq 0\} = \{\mathrm{charpol}_M(x) \mid M \in \mathrm{GL}(2,\mathbb{F}_r)\}$$

die Operation

$$\begin{array}{rcccc} \diamond & : & {\mathbb{F}_r}^* \times \mathcal{CP} & \to & \mathcal{CP} \\ & & (\lambda,\; x^2 + ax + b) & \mapsto & x^2 + \lambda a\; x + \lambda^2 b \end{array} \quad .$$

Es ist also

$$\mathrm{charpol}_{\lambda M}(x) = \lambda \diamond \mathrm{charpol}_M(x) \quad .$$

Den Schlüssel zur Bestimmung der Konjugationsklassen liefert uns der folgende Satz.

Lemma 3.3.2. *Seien* $[A] \neq [E] \neq [B]$ *in* $\mathrm{PGL}(2,\mathbb{F}_r)$. *Dann gilt*

$$[A] \sim [B] \iff \mathrm{charpol}_A(x) \in {\mathbb{F}_r}^* \diamond \mathrm{charpol}_B(x) \,.$$

Beweis: Die Richtung von links nach rechts ergibt sich leicht. Seien $A, B, C \in \mathrm{GL}(2,\mathbb{F}_r)$ mit $[A] = [C^{-1}][B][C] \in \mathrm{PGL}(2,\mathbb{F}_r)$. Dann existiert ein $\lambda \in {\mathbb{F}_r}^*$ mit $A = \lambda C^{-1}BC$. Damit folgt

$$\mathrm{charpol}_A(x) = \mathrm{charpol}_{\lambda C^{-1}BC}(x) = \lambda \diamond \mathrm{charpol}_{C^{-1}BC}(x) = \lambda \diamond \mathrm{charpol}_B(x) \quad .$$

Kommen wir nun zur Folgerung von rechts nach links. Sei $\lambda \in {\mathbb{F}_r}^*$ mit

$$\mathrm{charpol}_A(x) = \lambda \diamond \mathrm{charpol}_B(x) = \lambda^2 \ \mathrm{charpol}_B\left(\frac{x}{\lambda}\right) \quad .$$

Da $[A]$ und $[B]$ ungleich $[E]$ sind, liefert Konjugation in $\mathrm{GL}(2,\mathbb{F}_r)$

$$[A] \sim \begin{bmatrix} 0 & -\det(A) \\ 1 & \mathrm{Tr}(A) \end{bmatrix}$$

und

$$[B] \sim \begin{bmatrix} 0 & -\det(B) \\ 1 & \mathrm{Tr}(B) \end{bmatrix} \,.$$

Wählen wir nun

$$M := \begin{pmatrix} 0 & -\lambda\det(B) \\ 1 & \mathrm{Tr}(B) \end{pmatrix} \in \mathrm{GL}(2,\mathbb{F}_r)$$

so erhalten wir unter Verwendung von $\mathrm{Tr}(A) = \lambda\mathrm{Tr}(B)$ und $\det(A) = \lambda^2\det(B)$

$$[M]^{-1} \begin{bmatrix} 0 & -\det(A) \\ 1 & \mathrm{Tr}(A) \end{bmatrix} [M] = \begin{bmatrix} 0 & -\det(B) \\ 1 & \mathrm{Tr}(B) \end{bmatrix} \,.$$

□

Wir erhalten folgendes Korollar.

Korollar 3.3.3. *Seien* $[A] \neq [E] \neq [B]$ *in* $\mathrm{PGL}(2,\mathbb{F}_r)$. *Dann sind äquivalent:*

(i) Es gilt $[A] \sim [B]$.

(ii) Es existiert ein $\lambda \in {\mathbb{F}_r}^*$ *mit* $\mathrm{charpol}_A(x) = \lambda^2\mathrm{charpol}_B(\frac{x}{\lambda})$.

(iii) Es existiert ein $\lambda \in {\mathbb{F}_r}^*$ *mit* $\mathrm{Tr}(A) = \lambda\mathrm{Tr}(B)$ *und* $\det(A) = \lambda^2\det(B)$.

(iv) Es ist

$$\begin{array}{rlll} & \mathrm{Tr}(A) \neq 0 \neq \mathrm{Tr}(B) & \textit{und} & \frac{\mathrm{Tr}(A)^2}{\det(A)} = \frac{\mathrm{Tr}(B)^2}{\det(B)} \\ \textit{oder} & \mathrm{Tr}(A) = 0 = \mathrm{Tr}(B) & \textit{und} & \frac{\det(A)}{\det(B)} \in ({\mathbb{F}_r}^*)^2 \end{array} .$$

Beweis: Klar. □

Damit erhalten wir aus dem Vertretersystem von Seite 44 der Konjugationsklassen in $\mathrm{GL}(2,\mathbb{F}_r)$ das folgende Vertretersystem der Konjugationsklassen in $\mathrm{PGL}(2,\mathbb{F}_r)$.

Satz 3.3.4. *Wir betrachten auf* ${\mathbb{F}_r}^* - \{1,-1\}$ *die Äquivalenzrelation*

$$\alpha \approx \beta :\Longleftrightarrow (\alpha = \beta \textit{ oder } \alpha = \beta^{-1}) \quad .$$

Sei V_1 ein Vertretersystem von ${\mathbb{F}_r}^* - \{1,-1\}/\approx$. Im Fall von $\mathrm{char}(\mathbb{F}_r) \neq 2$ *sei außerdem $c \in \mathbb{F}_r - (\mathbb{F}_r)^2$ ein fest gewähltes Nichtquadrat. Dann haben die Konjugationsklassen von* $\mathrm{PGL}(2,\mathbb{F}_r)$ *folgendes Vertretersystem:*

$\mathrm{PGL}(2,\mathbb{F}_r)$		
Klassentyp	*Anzahl der Klassen*	*Ordnung*
$\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}$	1	1
$\underset{1\neq -1}{\begin{bmatrix}1 & 0\\0 & -1\end{bmatrix}}$	$\begin{cases}1 & ; \quad r \equiv 1 \bmod 2\\ 0 & ; \quad r \equiv 0 \bmod 2\end{cases}$	2
$\underset{a\in V_1}{\begin{bmatrix}1 & 0\\0 & a\end{bmatrix}}$	$\begin{cases}\frac{r-3}{2} & ; \quad r \equiv 1 \bmod 2\\ \frac{r-2}{2} & ; \quad r \equiv 0 \bmod 2\end{cases}$	$\mathrm{ord}(a)$
$\begin{bmatrix}1 & 1\\0 & 1\end{bmatrix}$	1	$p = \mathrm{char}(\mathbb{F}_r)$
$\begin{bmatrix}0 & c\\1 & 0\end{bmatrix}$	$\begin{cases}1 & ; \quad r \equiv 1 \bmod 2\\ 0 & ; \quad r \equiv 0 \bmod 2\end{cases}$	2
$\underset{\substack{(x-\gamma)(x-\gamma^r)\\ =x^2-x-a \text{ prim}}}{\begin{bmatrix}0 & a\\1 & 1\end{bmatrix}}$	$\begin{cases}\frac{r-1}{2} & ; \quad r \equiv 1 \bmod 2\\ \frac{r}{2} & ; \quad r \equiv 0 \bmod 2\end{cases}$	$\mathrm{ord}_{\mathbb{F}^*_{r^2}}(\gamma^{r-1})$

Beweis: Das Bild des Standardvertretersystems der $\mathrm{GL}(2,\mathbb{F}_r)$ in der $\mathrm{PGL}(2,\mathbb{F}_r)$ ist

$$\left\{\begin{bmatrix}1 & 0\\0 & 1\end{bmatrix}\right\} \cup \left\{\begin{bmatrix}1 & 0\\0 & a\end{bmatrix} \mid a \in {\mathbb{F}_r}^* - \{1\}\right\} \cup \left\{\begin{bmatrix}a & 1\\0 & a\end{bmatrix} \mid a \in {\mathbb{F}_r}^*\right\}$$
$$\cup \left\{\begin{bmatrix}0 & a\\1 & b\end{bmatrix} \mid x^2 - bx - a \in \mathbb{F}_r[x] \text{ prim}\right\} \quad .$$

Wir haben gesehen, daß das Verhalten von $[M] \in \mathrm{PGL}(2,\mathbb{F}_r)$ davon abhängt, ob $\mathrm{Tr}(M) = 0$ oder $\mathrm{Tr}(M) \neq 0$ gilt. Daher teilen wir die obigen Mengen entsprechend auf und erhalten

$$\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right\} \cup \left\{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \mid 1 \neq -1\right\} \cup \left\{\begin{bmatrix}1 & 0\\ 0 & a\end{bmatrix} \mid a \in \mathbb{F}_r{}^* - \{-1,1\}\right\}$$
$$\cup \left\{\begin{bmatrix}a & 1\\ 0 & a\end{bmatrix} \mid a \in \mathbb{F}_r{}^*\right\} \cup \left\{\begin{bmatrix}0 & a\\ 1 & 0\end{bmatrix} \mid x^2 - a \in \mathbb{F}_r[x] \text{ prim }\right\}$$
$$\cup \left\{\begin{bmatrix}0 & a\\ 1 & b\end{bmatrix} \mid x^2 - bx - a \in \mathbb{F}_r[x] \text{ prim }, b \neq 0\right\} \quad .$$

Betrachtet man nun, welche dieser Matrizen in $\mathrm{PGL}(2,\mathbb{F}_r)$ konjugiert sind, so erhält man das im Satz angegebene minimale Vertretersystem

$$\left\{\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}\right\} \cup \left\{\begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \mid 1 \neq -1\right\} \cup \left\{\begin{bmatrix}1 & 0\\ 0 & a\end{bmatrix} \mid a \in V_1\right\} \cup \left\{\begin{bmatrix}1 & 1\\ 0 & 1\end{bmatrix}\right\}$$
$$\cup \left\{\begin{bmatrix}0 & c\\ 1 & 0\end{bmatrix}\right\} \cup \left\{\begin{bmatrix}0 & a\\ 1 & 1\end{bmatrix} \mid x^2 - x - a \in \mathbb{F}_r[x] \text{ prim }\right\} \quad .$$

Die Anzahlen der verschiedenen Typen sind weitgehend klar. Nur zum letzten Typ in der Tabelle ist etwas zu sagen.
Ist $r \equiv 0 \bmod 2$, so ist die Abbildung $\varphi : \mathbb{F}_r \to \mathbb{F}_r,\ x \mapsto x^2 - x$ ein $\mathbb{F}_2$-Vektorraumendomorphismus mit $\ker(\varphi) = \{0,1\}$. Daher ist $\#\varphi(\mathbb{F}_r) = \frac{r}{2}$, und für alle $a \in \mathbb{F}_r - \varphi(\mathbb{F}_r)$ ist das Polynom $x^2 - x - a$ prim.
Ist $r \equiv 1 \bmod 2$, so ergibt quadratische Ergänzung, daß das Polynom $x^2 - x - a$ genau dann prim ist, wenn $a \notin -\frac{1}{4} + (\mathbb{F}_r{}^*)^2$ gilt. Da $\#(\mathbb{F}_r{}^*)^2 = \frac{r-1}{2}$ ist, ist das Polynom für $(r-1) - \frac{r-1}{2} = \frac{r-1}{2}$ Wahlen von a prim.
Auch die jeweiligen Elementordnungen sind klar. Im letzten Fall benutzt man, daß

$$\mathrm{ord}_{\mathrm{PGL}(2,\mathbb{F}_r)}(\begin{bmatrix}0 & a\\ 1 & b\end{bmatrix}) = \mathrm{ord}_{\mathrm{PGL}(2,\mathbb{F}_{r^2})}(\begin{bmatrix}0 & a\\ 1 & b\end{bmatrix}) = \mathrm{ord}_{\mathrm{PGL}(2,\mathbb{F}_{r^2})}(\begin{bmatrix}\gamma & 0\\ 0 & \gamma^r\end{bmatrix})$$

gilt. □

Aus der obigen Tabelle ergibt sich direkt das folgende Korollar.

Korollar 3.3.5. *Die Anzahl der Konjugationsklassen in* $\mathrm{PGL}(2,\mathbb{F}_r)$ *ist*

$$\begin{cases} r+2 & ; \quad r \equiv 1 \bmod 2 \\ r+1 & ; \quad r \equiv 0 \bmod 2 \end{cases} \quad .$$

Da für alle $[M],[N] \in \mathrm{PGL}(2,\mathbb{F}_r)$ immer $\mathrm{ord}_{\mathrm{PGL}}([M]) = \mathrm{ord}_{\mathrm{PGL}}([N]^{-1}[M][N])$ gilt, haben wir die Ordnungen aller Elemente in $\mathrm{PGL}(2,\mathbb{F}_r)$ bestimmt. Insbesondere erhalten wir:

Lemma 3.3.6. *(i) Es existiert ein* $[M] \in \mathrm{PGL}(2, \mathbb{F}_r)$ *mit* $\mathrm{ord}_{\mathrm{PGL}}([M]) = r+1$.

(ii) Es existiert ein $[M] \in \mathrm{PGL}(2, \mathbb{F}_r)$ *mit* $\mathrm{ord}_{\mathrm{PGL}}([M]) = r-1$.

(iii) Für alle $M \in \mathrm{GL}(2, \mathbb{F}_r)$ *gilt* $\mathrm{v}_p(\mathrm{ord}_{\mathrm{GL}}(M)) = \mathrm{v}_p(\mathrm{ord}_{\mathrm{PGL}}([M]))$.

Beweis:

(i) Sei γ ein Erzeuger von $\mathbb{F}_{r^2}^*$ und $(x-\gamma)(x-\gamma^r) = x^2 - ax - b$. Wähle $M = \begin{bmatrix} 0 & a \\ 1 & b \end{bmatrix}$.

(ii) Wähle $M = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$, wobei a ein Erzeuger von ${\mathbb{F}_r}^*$ ist.

(iii) Klar.

□

Für die späteren Rechnungen ist folgendes wichtig:

Lemma 3.3.7. *Sei* $M \in \mathrm{GL}(2, \mathbb{F}_r)$*. Dann kann man aus der Kenntnis des Minimalpolynoms und des charakteristischen Polynoms von* M *die Ordnung* $\mathrm{ord}_{\mathrm{PGL}(2,\mathbb{F}_r)}([M])$ *bestimmen. Hat das charakteristische Polynom keine doppelte Nullstelle in* $\overline{\mathbb{F}_r}$*, so genügt die Kenntnis des charakteristischen Polynoms.*

Beweis: Das Minimalpolynom und das charakteristische Polynom bestimmen den Konjugationstyp von M in $\mathrm{GL}(2, \mathbb{F}_r)$. Daher kann man den Standardvertreter der Konjugationsklasse von M in $\mathrm{GL}(2, \mathbb{F}_r)$ und damit auch den Standardvertreter der Konjugationsklasse von $[M]$ in $\mathrm{PGL}(2, \mathbb{F}_r)$ angeben. Dessen Ordnung können wir aus der obigen Tabelle ablesen. Hat das charakteristische Polynom verschiedene Nullstellen im algebraischen Abschluß, so ist das Minimalpolynom gleich dem charakteristischen. □

3.4 Die maximalen Untergruppen von $\mathrm{PGL}(2, \mathbb{F}_r)$

Bevor wir nun zu den maximalen Untergruppen der $\mathrm{PGL}(2, \mathbb{F}_r)$ kommen, zeigen wir noch, wie wir Informationen von der $\mathrm{PGL}(2, \mathbb{F}_r)$ auf die $\mathrm{GL}(2, \mathbb{F}_r)$ hochliften.

Satz 3.4.1. *Sei* $G \leqslant \mathrm{GL}(2, \mathbb{F}_r)$ *und* $\mathrm{P}G = \mathrm{PGL}(2, \mathbb{F}_r)$*. Dann ist* $G \geqslant \mathrm{SL}(2, \mathbb{F}_r)$.

Beweis: Da $\#\ker(\mathrm{P}) = (r-1)$ und $\mathrm{ggT}(r-1, p) = 1$ ist, gilt $\mathrm{v}_p(\#G) = \mathrm{v}_p(\#\mathrm{P}G) = \mathrm{v}_p(\#\mathrm{PGL}(2, \mathbb{F}_r)) = \mathrm{v}_p(\#\mathrm{GL}(2, \mathbb{F}_r))$. Betrachten wir die p-Sylowgruppe $U = \left\{ \begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} \mid a \in \mathbb{F}_r \right\}$ in $\mathrm{PGL}(2, \mathbb{F}_r)$, so muß

$$G \cap \mathrm{P}^{-1}(U) \geqslant \left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in \mathbb{F}_r \right\}$$

gelten. Mit dem gleichen Argument erhält man, daß die Untergruppe $\left\{\begin{pmatrix}1 & 0\\ a & 1\end{pmatrix} \mid a \in \mathbb{F}_r\right\}$ in G liegt. Nach [Lan76, S.178] erzeugen diese beiden Dreiecksgruppen bereits die $\mathrm{SL}(2,\mathbb{F}_r)$. Damit ist die Aussage gezeigt. □

Lemma 3.4.2. *Sei* $\mathrm{SL}(2,\mathbb{F}_r) \leqslant G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$ *und* $\det(G) = {\mathbb{F}_r}^*$. *Dann ist* G *schon ganz* $\mathrm{GL}(2,\mathbb{F}_r)$.

Beweis: Aus dem Isomorphiesatz

$${\mathbb{F}_r}^* = {}^{G}/_{G \cap \mathrm{SL}(2,\mathbb{F}_r)} = {}^{G}/_{\mathrm{SL}(2,\mathbb{F}_r)}$$

folgt $\#G = (r-1)\ \#\mathrm{SL}(2,\mathbb{F}_r) = \#\mathrm{GL}(2,\mathbb{F}_r)$. □

Die beiden obigen Ergebnisse setzen sich zu folgendem Kriterium zusammen.

Kriterium 3.4.3. *Sei* $G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$, $\mathrm{P}G = \mathrm{PGL}(2,\mathbb{F}_r)$ *und* $\det(G) = {\mathbb{F}_r}^*$. *Dann gilt*

$$G = \mathrm{GL}(2,\mathbb{F}_r)\ .$$

Die Aussagen, die wir später im Algorithmus verwenden werden, werden wir im weiteren als Kriterien bezeichnen.
Von entscheidender Bedeutung ist die Klassifizierung der maximalen Untergruppen der $\mathrm{PGL}(2,\mathbb{F}_r)$. Die maximalen Untergruppen der $\mathrm{PSL}(2,\mathbb{F}_r)$ wurden bereits von Dickson in [Dic01] um 1900 untersucht und sind auch in [Hup67] zu finden. Daraus lassen sich natürlich die maximalen Untergruppen der $\mathrm{PGL}(2,\mathbb{F}_r)$ ableiten. Diese wurden aber in [VM80, Theorem 3] explizit angegeben, so daß wir auf diese Quelle verweisen.

Satz 3.4.4. *Sei* $G \lneqq \mathrm{PGL}(2,\mathbb{F}_r)$. *Dann ist* G *in einer der folgenden Gruppen enthalten:*

(i) $\mathrm{PSL}(2,\mathbb{F}_r)$,

(ii) $\mathrm{PGL}(2,\mathbb{F}_s)$, *für einen Zwischenkörper* $\mathbb{F}_p \subseteq \mathbb{F}_s \subsetneqq \mathbb{F}_r$,

(iii) $\mathrm{D}_{2(r+1)}$,

(iv) $\mathrm{D}_{2(r-1)}$,

(v) $\mathrm{P}\mathfrak{B}$, *dem Bild einer Borelgruppe von* $\mathrm{GL}(2,\mathbb{F}_r)$,

(vi) A_4,

(vii) S_4,

(viii) A_5 .

Dabei bezeichnet D_n *die Diedergruppe mit* n *Elementen und* S_n *(bzw.* A_n*) die symmetrische (bzw. alternierende) Gruppe mit* $n!$ *(bzw.* $\frac{n!}{2}$*) Elementen.*

Die Gruppen $\mathrm{D}_{2(r+1)}$ und $\mathrm{D}_{2(r-1)}$ sind die Bilder der Normalisatoren von Cartanuntergruppen unter der Abbildung P. Bei den Gruppen A_4, S_4 und A_5 handelt es sich um Ausnahmefälle, die auch nicht in jeder $\mathrm{PGL}(2,\mathbb{F}_r)$ auftreten.
Um später Ausnahmefälle abzufangen, überlegen wir uns noch, unter welchen Bedingungen die angegebenen Untergruppen keine echten Untergruppen sind.

Bemerkung 3.4.5. An dieser Stelle wollen wir den Begriff der *echten Untergruppe* klären. Sind U, G endliche Gruppen, so heißt U echte Untergruppe von G, falls $\#U < \#G$ ist und G eine zu U isomorphe Untergruppe besitzt. In diesem Sinne ist $\mathrm{GL}(2,\mathbb{F}_2)$ echte Untergruppe von S_4, S_4 ist keine echte Untergruppe von S_4, und S_5 ist ebenfalls keine echte Untergruppe von S_4.

Satz 3.4.6. *(i) Die Gruppe* $\mathrm{PSL}(2,\mathbb{F}_r)$ *ist genau dann gleich* $\mathrm{PGL}(2,\mathbb{F}_r)$*, wenn* $p = \mathrm{char}(\mathbb{F}_r) = 2$ *gilt.*

(ii) Die Gruppe $\mathrm{PGL}(2,\mathbb{F}_s)$ *mit* $\mathbb{F}_p \subseteq \mathbb{F}_s \subsetneq \mathbb{F}_r$ *ist immer eine echte Untergruppe von* $\mathrm{PGL}(2,\mathbb{F}_r)$*.*

(iii) Die Gruppe $\mathrm{D}_{2(r+1)}$ *ist genau dann gleich* $\mathrm{PGL}(2,\mathbb{F}_r)$*, wenn* $\mathbb{F}_r = \mathbb{F}_2$ *ist.*

(iv) Die Gruppe $\mathrm{D}_{2(r-1)}$ *ist immer eine echte Untergruppe von* $\mathrm{PGL}(2,\mathbb{F}_r)$*.*

(v) Die Borelgruppe $\mathrm{P}\mathfrak{B}$ *ist immer eine echte Untergruppe von* $\mathrm{PGL}(2,\mathbb{F}_r)$*.*

(vi) Ist $\mathbb{F}_r = \mathbb{F}_2$*, so ist* A_4 *keine echte Untergruppe von* $\mathrm{PGL}(2,\mathbb{F}_r)$*.*

(vii) Ist $r \leqslant 3$*, so ist* S_4 *keine echte Untergruppe von* $\mathrm{PGL}(2,\mathbb{F}_r)$*.*

(viii) Ist $r \leqslant 4$*, so ist* A_5 *keine echte Untergruppe von* $\mathrm{PGL}(2,\mathbb{F}_r)$*.*

Beweis: Man vergleicht die Mächtigkeiten der jeweiligen Gruppen mit $\#\mathrm{PGL}(2,\mathbb{F}_r) = (r-1)r(r+1)$. □

Wir geben nun die Ausschlußkriterien an.

Kriterium 3.4.7. *Sei* $G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$*,* $\mathbb{F}_s \subseteq \mathbb{F}_r$ *ein Teilkörper,* $M \in G$ *und* $m = \mathrm{ord}_{\mathrm{PGL}}([M])$*. Dann gelten folgende Implikationen:*

(i) $\det(M) \notin (\mathbb{F}_r{}^*)^2 \Rightarrow \mathrm{P}G \nleq \mathrm{PSL}(2,\mathbb{F}_r)$,

(ii) $\frac{\mathrm{Tr}(M)^2}{\det(M)} \notin \mathbb{F}_s \Rightarrow \mathrm{P}G \nleq \mathrm{PGL}(2,\mathbb{F}_s)$,

(iii) $2(r+1) \not\equiv 0 \bmod m \Rightarrow \mathrm{P}G \nleq \mathrm{D}_{2(r+1)}$,

(iv) $2(r-1) \not\equiv 0 \bmod m \Rightarrow \mathrm{P}G \nleq \mathrm{D}_{2(r-1)}$,

(v) $\mathrm{charpol}_M(x)$ *ist irreduzibel* $\Rightarrow \mathrm{P}G \nleq \mathrm{P}\mathfrak{B}$,

(vi) $\left.\begin{cases} 12 \not\equiv 0 \bmod m \\ \textit{oder} \quad (r = 3 \textit{ und } \det(M) \notin (\mathbb{F}_3^*)^2) \end{cases}\right\} \Rightarrow PG \not\leq A_4,$

(vii) $24 \not\equiv 0 \bmod m \Rightarrow PG \not\leq S_4,$

(viii) $\left.\begin{cases} 60 \not\equiv 0 \bmod m \\ \textit{oder} \quad (r = 5 \textit{ und } \det(M) \notin (\mathbb{F}_5^*)^2) \end{cases}\right\} \Rightarrow PG \not\leq A_5.$

Beweis: Die Fälle $(i), (iii), (iv), (vii)$ sind klar. In (vi) und $(viii)$ wird verwendet, daß $\mathrm{PSL}(2,\mathbb{F}_3) \cong A_4$ und $\mathrm{PSL}(2,\mathbb{F}_5) \cong A_5$ ist (vgl. [Hup67, S.183]). Die Fälle (ii) und (v) folgen aus Lemma 3.3.1. □

Die beiden Spezialfälle $r = 3, 5$ müssen berücksichtigt werden, da in diesen Fällen die Mächtigkeit der $\mathrm{PGL}(2,\mathbb{F}_r)$ gleich 24 bzw. 120 ist. Diese Zahlen besitzen nur die Primteiler $2, 3$ und 5, und nach unserer Untersuchung der Elementordnungen in $\mathrm{PGL}(2,\mathbb{F}_r)$ existieren keine Elemente, deren Ordnung nicht 12 bzw. 60 teilt. Zur Analyse unseres Algorithmus werden wir später folgenden Satz verwenden:

Satz 3.4.8. *Sei $U \lneq \mathrm{GL}(2,\mathbb{F}_r)$, und $\mathrm{P}U$ sei eine maximale, echte Untergruppe von $\mathrm{PGL}(2,\mathbb{F}_r)$. Dann existiert ein $M \in \mathrm{GL}(2,\mathbb{F}_r)$, das die Voraussetzungen des zugehörigen Kriteriums aus 3.4.7 erfüllt.*

Beweis: Die Numerierung folgt der Numerierung der maximalen Untergruppen in 3.4.7.

(i) Ist $\mathrm{PSL}(2,\mathbb{F}_r) \neq \mathrm{PGL}(2,\mathbb{F}_r)$, so ist $\mathrm{char}(\mathbb{F}_r) \neq 2$, und damit existiert ein $M \in \mathrm{GL}(2,\mathbb{F}_r)$ mit $\det(M) \notin ({\mathbb{F}_r}^*)^2$.

(ii) Klar.

(iii) Ist $p \neq 2$, so wähle M mit $\mathrm{ord}_{\mathrm{PGL}}([M]) = p$. Ist $p = 2$, so wähle M mit $\mathrm{ord}_{\mathrm{PGL}}([M]) = r - 1$.

(iv) Analog zum obigen Fall wählen wir für $p \neq 2$ ein Element M mit $\mathrm{ord}_{\mathrm{PGL}}([M]) = p$, sonst mit $\mathrm{ord}_{\mathrm{PGL}}([M]) = r + 1$.

(v) Klar.

(vi) Für $r \geqslant 4$ wählen wir M mit $\mathrm{ord}_{\mathrm{PGL}}([M]) = (r + 1)$. Für $r = 2$ ist A_4 keine Untergruppe, und für $r = 3$ ist $A_4 = \mathrm{PSL}(2,\mathbb{F}_3)$.

(vii) Da S_4 als echte Untergruppe vorausgesetzt ist, ist $r \geqslant 4$, und wir wählen M mit $\mathrm{ord}_{\mathrm{PGL}}([M]) = (r + 1)$.

(viii) Da A_5 als echte Untergruppe vorausgesetzt ist, ist $r \geqslant 5$. Im Fall $r \geqslant 6$ wählen wir M mit $\mathrm{ord}_{\mathrm{PGL}}([M]) = (r+1)$. Im Fall $r = 5$ ist $A_5 = \mathrm{PSL}(2,\mathbb{F}_5)$.

□

Nehmen wir an, daß die Untergruppe G bereits ganz $\mathrm{GL}(2,\mathbb{F}_r)$ ist, daß wir dies allerdings nicht wissen. Dann besagt der obige Satz, daß die in 3.4.7 angegebenen Kriterien genügen, um zu zeigen, daß $\mathrm{P}G = \mathrm{PGL}(2,\mathbb{F}_r)$ gilt, wenn wir alle Minimalpolynome und charakteristischen Polynome von Elementen aus G verwenden. Wir werden nun weitere Kriterien herleiten, die wir benutzen werden, um unseren Algorithmus effizienter zu machen.

Lemma 3.4.9. *Sei* $C \leqslant \mathrm{GL}(2,\mathbb{F}_r)$ *eine (zerfallende oder nichtzerfallende) Cartanuntergruppe. Dann enthält* $\mathrm{Norm}(C)$ *genau dann nicht-halbeinfache Elemente, wenn* $p = 2$ *ist.*

Beweis: Für $\mathbb{F}_r = \mathbb{F}_2$ und C zerfallend ist das klar. Ansonsten ist nach Lemma 3.2.4 die Mächtigkeit $\#\mathrm{Norm}(C) \in \{2(r-1), 2(r+1)\}$. Daher ist $\mathrm{v}_p(\#\mathrm{Norm}(C))$ genau dann größer Null, wenn $p = 2$ ist. Da ein Element in $\mathrm{GL}(2,\mathbb{F}_r)$ genau dann halbeinfach ist, wenn seine Ordnung prim zu p ist, ist damit die Aussage gezeigt. □

Da die p-Bewertungen der GL-Ordnung und der PGL-Ordnung gleich sind, erhalten wir nun ein weiteres Kriterium.

Kriterium 3.4.10. *Sei* $p \neq 2$ *und* $M \in G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$. *Ist* $\mathrm{v}_p(\mathrm{ord}_{\mathrm{GL}}(M)) > 0$, *so ist* $\mathrm{P}G \nleqslant \mathrm{D}_{2(r-1)}$ *und* $\mathrm{P}G \nleqslant \mathrm{D}_{2(r+1)}$.

Wir kommen zu weiteren Kriterien für die Diedergruppen. Diese Kriterien haben sich im Algorithmus als sehr effizient erwiesen, um die Diedergruppen auszuschließen.

Lemma 3.4.11. *Sei* $\mathrm{D}_{2m} = \langle \sigma, \tau \mid \sigma^2 = \tau^m = 1, \sigma\tau = \tau^{-1}\sigma \rangle$ *eine Untergruppe von* $\mathrm{PGL}(2,\mathbb{F}_r)$, $M \in \mathrm{GL}(2,\mathbb{F}_r)$ *und* $[M] \in \mathrm{D}_{2m} - \langle\tau\rangle$. *Dann gilt*

$$\mathrm{Tr}(M) = 0 \quad .$$

Beweis: Sei $[M] = \sigma\tau^\alpha$ aus $\mathrm{D}_{2m} - \langle\tau\rangle$. Dann ist $(\sigma\tau^\alpha)^2 = \sigma\tau^\alpha\tau^{(m-1)\alpha}\sigma = 1$. Also ist $[M]^2 = [E]$ bzw. $M^2 = \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right)$ für ein $a \in \mathbb{F}_r$. Damit ist $M^2 - \left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) = 0$. Also ist $x^2 - a$ das charakteristische Polynom von M. Da der Koeffizient von x^1 im Polynom Null ist, ist damit die Aussage gezeigt. □

Wir erhalten direkt zwei weitere Kriterien:

Kriterium 3.4.12. *Sei* $M \in G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$. *Ist* $\mathrm{Tr}(M) \neq 0$ *und* $\mathrm{charpol}_M(x)$ *irreduzibel, so ist*

$$\mathrm{P}G \nleqslant \mathrm{D}_{2(r-1)} \; .$$

Beweis: Seien $\sigma, \tau \in \mathrm{D}_{2(r-1)}$ wie oben. Dann ist $\mathrm{P}^{-1}(\langle\tau\rangle)$ eine zerfallende Cartanuntergruppe. Diese enthält aber nur Matrizen mit zerfallenden charakteristischen Polynomen. Da $\mathrm{charpol}_M(x)$ irreduzibel ist, ist daher $[M] \notin \langle\tau\rangle$. Andererseits ist $[M] \notin \mathrm{D}_{2(r-1)} - \langle\tau\rangle$, da $\mathrm{Tr}(M) \neq 0$ ist. □

Kriterium 3.4.13. *Sei $M \in G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$. Ist $\mathrm{charpol}_M(x) = (x-a)(x-b)$ mit $a, b \in \mathbb{F}_r$, $a \neq b$ und $\mathrm{Tr}(M) \neq 0$, so ist*

$$\mathrm{P}G \nleqslant \mathrm{D}_{2(r+1)} \,.$$

Beweis: In diesem Fall ist $\mathrm{P}^{-1}(\langle\tau\rangle)$ eine nichtzerfallende Cartanuntergruppe. Diese ist isomorph zu $\mathbb{F}_{r^2}^*$. Daher haben die charakteristischen Polynome von Elementen aus $\mathrm{P}^{-1}(\langle\tau\rangle)$ entweder eine doppelte Nullstelle in $\mathbb{F}_r$ oder sind irreduzibel.
Daher schließt die Bedingung an $\mathrm{charpol}_M(x)$ aus, daß $[M]$ in $\langle\tau\rangle$ liegt. Wie oben schließt $\mathrm{Tr}(M) \neq 0$ aus, daß $[M]$ in $\mathrm{D}_{2(r+1)} - \langle\tau\rangle$ liegt. □

Wir geben noch einige weitere (triviale) Kriterien an, die wir später benutzen werden.

Kriterium 3.4.14. *Sei $M \in G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$. Ist $\mathrm{ord}_{\mathrm{PGL}}([M]) \geqslant 6$, so ist $\mathrm{P}G \nleqslant A_4, S_4, A_5$.*

Beweis: Die Ordnung der Elemente dieser Gruppen ist immer kleiner oder gleich 5. □

Kriterium 3.4.15. *Sei $M \in G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$ nicht halbeinfach, und sei $\mathrm{char}(\mathbb{F}_r) \geqslant 5$. Dann ist $\mathrm{P}G \nleqslant A_4, S_4, A_5$.*

Beweis: Ist M nicht halbeinfach, so ist seine Ordnung durch $\mathrm{char}(\mathbb{F}_r)$ teilbar. Dann ist auch $\mathrm{ord}_{\mathrm{PGL}}([M])$ durch $\mathrm{char}(\mathbb{F}_r)$ teilbar, und aus dem Kriterium 3.4.14 folgt dann die Aussage. □

Kriterium 3.4.16. *Sei $p = \mathrm{char}(\mathbb{F}_r) \neq 2$, $G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$ und $\det(G) = {\mathbb{F}_r}^*$. Dann ist $\mathrm{P}G \nleqslant \mathrm{PSL}(2,\mathbb{F}_r)$.*

Beweis: Klar. □

Aus [VM80, Theorem 3] erhalten wir noch folgendes Kriterium:

Kriterium 3.4.17. *(i) Ist $p = 2$ und $\mathrm{v}_p(r) \equiv 1 \bmod 2$, so ist A_4 keine Untergruppe von $\mathrm{PGL}(2,\mathbb{F}_r)$.*

(ii) Ist $p = 2$, so ist S_4 keine Untergruppe von $\mathrm{PGL}(2,\mathbb{F}_r)$.

(iii) Ist $p \neq 5$ und $r^2 \not\equiv 1 \bmod 5$, so ist A_5 keine Untergruppe von $\mathrm{PGL}(2,\mathbb{F}_r)$.

Da nach [Hup67, S.183] die Gruppen A_4 und $\mathrm{PSL}(2,\mathbb{F}_3)$ (bzw. A_5 und $\mathrm{PSL}(2,\mathbb{F}_5)$) isomorph sind, erhalten wir noch:

Kriterium 3.4.18. *Sei* $G \leqslant \mathrm{GL}(2,\mathbb{F}_r)$.

(i) *Ist* $r = 3$ *und* $\mathrm{P}G \nleq A_4$, *so folgt* $\mathrm{P}G \nleq \mathrm{PSL}(2,\mathbb{F}_r)$.

(ii) *Ist* $r = 3$ *und* $\mathrm{P}G \nleq \mathrm{PSL}(2,\mathbb{F}_r)$, *so folgt* $\mathrm{P}G \nleq A_4$.

(iii) *Ist* $r = 5$ *und* $\mathrm{P}G \nleq A_5$, *so folgt* $\mathrm{P}G \nleq \mathrm{PSL}(2,\mathbb{F}_r)$.

(iv) *Ist* $r = 5$ *und* $\mathrm{P}G \nleq \mathrm{PSL}(2,\mathbb{F}_r)$, *so folgt* $\mathrm{P}G \nleq A_5$.

Kapitel 4

Die Torsionsdarstellung

Wir werden uns nun die Erweiterung

$$\mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)$$

in unserer Situation genauer ansehen. Es bezeichne $O_{\mathfrak{l}}$ den ganzen Abschluß von $\mathbb{F}_q[u]$ in $\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]$, $e(\mathfrak{P},\mathfrak{p})$ den Verzweigungsindex und $f(\mathfrak{P},\mathfrak{p})$ den Trägheitsindex.
Für eine kurze Zusammenfassung des Verhaltens von Idealen in Galoiserweiterungen verweisen wir auf [FJ86, Kap. 5].
Für eine unverzweigte Stelle $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]}$ betrachten wir das Diagramm

$$\begin{array}{ccccc} \mathfrak{P} & \hookrightarrow & O_{\mathfrak{l}} & \hookrightarrow & \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \\ & & | & & | \\ \mathfrak{p} & \hookrightarrow & \mathbb{F}_q[u] & \hookrightarrow & \mathbb{F}_q(u) \end{array} ,$$

wobei $\mathfrak{P}$ eine Stelle über $\mathfrak{p}$ bezeichnet. Dieser Stelle wird durch die Bedingung

$$\mathrm{Frob}_{\mathfrak{P}}(\alpha) \equiv \alpha^{\#\mathbb{F}_{\mathfrak{P}}} \bmod \mathfrak{P} \qquad \forall \alpha \in O_{\mathfrak{l}}$$

ein eindeutiges Element $\mathrm{Frob}_{\mathfrak{P}} \in \mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$ (der *Frobenius* zur Stelle $\mathfrak{P}$) zugeordnet. Die Menge

$$(\mathfrak{p}, \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)) := \{\mathrm{Frob}_{\mathcal{Q}} \mid \mathcal{Q} \text{ teilt } \mathfrak{p}\}$$

bildet eine volle Konjugationsklasse in $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$, es ist also

$$(\mathfrak{p}, \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)) = \{\sigma^{-1}\mathrm{Frob}_{\mathfrak{P}}\, \sigma \mid \sigma \in \mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))\} .$$

Wir werden nun $\mathrm{Frob}_{\mathfrak{P}}$ als Element in $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ untersuchen. In manchen Fällen werden wir Sätze für Drinfeld-Moduln von beliebigem Rang r zeigen, obwohl wir später nur den Rang-2 Fall benötigen werden.
Die Menge der unverzweigten Stellen wird in Korollar 4.5.4 genauer charakterisiert werden.

4.1 Der Konjugationstyp von $\mathrm{Frob}_{\mathfrak{P}}$

Da die Reduktion von Polynomen mit der Komposition kommutiert, identifizieren sich $O_{\mathfrak{l}}/\mathfrak{P}$ und $\mathbb{F}_{\mathfrak{p}}\left({}_{\mathfrak{l}}\mathrm{Dred}(\phi,\mathfrak{p})\right)$ als $(\mathbb{F}_q[T],\phi)$-Moduln. Via dieser Identifikation können wir $\mathrm{Frob}_{\mathfrak{P}}$ als den Erzeuger der Galoisgruppe von

$$\mathbb{F}_{\mathfrak{p}}\left({}_{\mathfrak{l}}\mathrm{Dred}(\phi,\mathfrak{p})\right) \mid \mathbb{F}_{\mathfrak{p}}$$

auffassen. (Es sei daran erinnert, daß $\mathrm{Dred}(\phi,\mathfrak{p})$ den an $\mathfrak{p}(u)$ reduzierten Drinfeld-Modul ϕ bezeichnet.) In 2.1 haben wir für endliche Drinfeld-Moduln bereits das charakteristische Polynom der Operation des Frobenius auf dem Tate-Modul $T_{\mathfrak{l}}(\phi)$ untersucht. Der folgende Satz bringt dies in Zusammenhang mit unserer Situation:

Satz 4.1.1. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \sum_{i=1}^{r} a_i\tau^i)$ ein Rang-r Drinfeld-Modul, $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$. Weiter habe ϕ gute Reduktion an $\mathfrak{p}(u)$, und es sei $\mathfrak{p}(T) \neq \mathfrak{l}(T)$. Dann gilt für alle $i \in \mathbb{N}$: Die Reduktion induziert einen Isomorphismus von $\mathbb{F}_q[T]$-Moduln*

$${}_{\mathfrak{l}^i}\phi \cong {}_{\mathfrak{l}^i}\mathrm{Dred}(\phi,\mathfrak{p})$$

und damit

$$T_{\mathfrak{l}}(\phi) \cong T_{\mathfrak{l}}(\mathrm{Dred}(\phi,\mathfrak{p}))\ .$$

Beweis: Die Reduktion ist für jedes $\mathfrak{n}(T) \in \mathbb{F}_q[T]$ ein $\mathbb{F}_q[T]$-Modul-Homomorphismus auf der $\mathfrak{n}$-Torsion, da das Auswerten von Abbildungen mit Reduktion kommutiert.
Sei $i \in \mathbb{N}$ beliebig. Wir beachten, daß $\mathrm{char}(\mathrm{Dred}(\phi,\mathfrak{p}(u))) = \mathfrak{p}(T)$ ist. Daher ist das Polynom $(\mathrm{Dred}(\phi,\mathfrak{p}))_{\mathfrak{l}^i}(x) \in \mathbb{F}_{\mathfrak{p}}(x)$ separabel, und jede der Lösungen aus ${}_{\mathfrak{l}^i}\mathrm{Dred}(\phi,\mathfrak{p})$ kann mit dem Henselschen Lemma eindeutig zu einer Lösung von $\phi_{\mathfrak{l}^i}(x)$ im separablen Abschluß der Komplettierung $(\mathbb{F}_q(u))_{\mathfrak{p}}$ geliftet werden. Da $(\mathbb{F}_q(u))_{\mathfrak{p}}$ den Körper $\mathbb{F}_q(u)$ enthält, können wir die Menge dieser Lösungen mit ${}_{\mathfrak{l}^i}\phi$ identifizieren. Damit haben wir gezeigt, daß die Reduktionsabbildung von ${}_{\mathfrak{l}^i}\phi$ auf ${}_{\mathfrak{l}^i}\mathrm{Dred}(\phi,\mathfrak{p})$ surjektiv ist.
Da ϕ gute Reduktion an $\mathfrak{p}$ hat, ist $\deg_x((\mathrm{Dred}(\phi,\mathfrak{p}))_{\mathfrak{l}^i}) = \deg_x(\phi_{\mathfrak{l}^i}(x))$. Außerdem sind beide Polynome separabel. Daher ist $\#_{\mathfrak{l}^i}\phi = \#_{\mathfrak{l}^i}\mathrm{Dred}(\phi,\mathfrak{p})$. Die Reduktion ist also sogar eine Bijektion auf den Torsionspunkten und liefert damit für jedes $i \in \mathbb{N}$ einen $\mathbb{F}_q[T]$-Modul-Isomorphismus von ${}_{\mathfrak{l}^i}\phi$ nach ${}_{\mathfrak{l}^i}\mathrm{Dred}(\phi,\mathfrak{p})$.
Da diese Isomorphismen mit den von ϕ bzw. $\mathrm{Dred}(\phi,\mathfrak{p})$ bestimmten $\mathbb{F}_q[T]$-Moduloperationen kommutieren, liefert dies auch einen Isomorphismus der Tate-Moduln. □

Die Operation von $\mathrm{Frob}_{\mathfrak{P}}$ auf $T_{\mathfrak{l}}(\mathrm{Dred}(\phi,\mathfrak{p}))$ haben wir bereits im Abschnitt 2.1 betrachtet. Damit erhalten wir direkt das Korollar

Korollar 4.1.2. *Seien die Voraussetzungen wie im Satz 4.1.1. Dann gilt für das charakteristische Polynom*

$$\mathrm{charpol}(\mathrm{Frob}_{\mathfrak{P}}) = \mathit{red}(\mathcal{P}_{\mathrm{Dred}(\phi,\mathfrak{p})}, \mathfrak{l}) \in (\mathbb{F}_q[T]/\mathfrak{l}(T))[X]\ ,$$

wobei $\mathcal{P}_{\mathrm{Dred}(\phi,\mathfrak{p})} \in (\mathbb{F}_q[T])[X]$ *das charakteristische Polynom des reduzierten Drinfeld-Moduls bezeichnet.*

Bemerkung 4.1.3. Obwohl es aus dem Kontext immer klar sein sollte, sei explizit darauf hingewiesen, daß $red(f,g)$ das am Polynom g reduzierte Polynom f bezeichnet, während $\mathrm{Dred}(\phi, g)$ für einen an g reduzierten Drinfeld-Modul ϕ steht. Es ist also zwischen $red(\phi_T, \mathfrak{p})$ und $\mathrm{Dred}(\phi, \mathfrak{p})$ zu unterscheiden.

Im Fall eines Rang-2 Drinfeld-Moduls können wir $\mathrm{Gal}(\mathbb{F}_q(u)[\mathfrak{l}\phi], \mathbb{F}_q(u))$ als Untergruppe von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ auffassen. Insbesondere ist $\mathrm{charpol}(\mathrm{Frob}_\mathfrak{P})$ das charakteristische Polynom einer Matrix aus $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$.
An dieser Stelle wollen wir noch einmal daran erinnern, daß es uns genügt, $\mathrm{Frob}_\mathfrak{P}$ bis auf Konjugation zu bestimmen, da wir in unseren späteren Berechnungen keine der Stellen über $\mathfrak{p}$ auszeichnen können.
Wie wir in Abschnitt 3.1 gesehen haben, legt das charakteristische Polynom bereits die Konjugationsklasse fest, falls es keine doppelte Nullstelle hat. Falls $\mathrm{charpol}(\mathrm{Frob}_\mathfrak{P}) = (X-\alpha)^2 \in \mathbb{F}_\mathfrak{l}[X]$ ist, so kann $\mathrm{Frob}_\mathfrak{P}$ zu

$$\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix} \qquad \text{oder} \qquad \begin{pmatrix} \alpha & 1 \\ 0 & \alpha \end{pmatrix}$$

konjugiert sein. Diese beiden Fälle können durch die Ordnung von $\mathrm{Frob}_\mathfrak{P}$ in $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ unterschieden werden. Es gilt allgemein

Lemma 4.1.4. *Sei* $M \in \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ *und* $p = \mathrm{char}(\mathbb{F}_\mathfrak{l})$. *Dann ist* M *genau dann zu einer Matrix der Form* $\left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)$ *konjugiert, wenn* $\mathrm{ord}(M) \equiv 0 \bmod p$ *gilt.*

Beweis: Dies folgt direkt aus der Klassifikation der Konjugationstypen durch ihre Jordansche Normalform und der Tatsache, daß $\left(\begin{smallmatrix} \alpha & 1 \\ 0 & \alpha \end{smallmatrix}\right)^n = \left(\begin{smallmatrix} \alpha^n & n\cdot\alpha^{n-1} \\ 0 & \alpha^n \end{smallmatrix}\right)$ ist (vgl. Abschnitt 3.1). □

Bevor wir zur Berechnung von $\mathrm{ord}(\mathrm{Frob}_\mathfrak{P})$ kommen, werden wir noch kurz die Berechnung der Größe des Zerfällungskörpers eines Polynoms aus $\mathbb{F}_r[x]$ untersuchen. Sei also $f(x) \in \mathbb{F}_r[x]$. Falls $f(x)$ nicht separabel ist, können wir es in $\mathrm{ggT}(f, f') \cdot \frac{f}{\mathrm{ggT}(f,f')}$ zerlegen, und die Zerfällungskörper der beiden Faktoren berechnen. Daher können wir o.B.d.A. annehmen, daß $f(x)$ separabel ist. Dann gilt:

Lemma 4.1.5. *Sei* $f(x) \in \mathbb{F}_r[x]$ *normiert und separabel. Dann ist*

$$[\mathrm{ZerfKp}(f) : \mathbb{F}_r] = \min\{n \in \mathbb{N} \mid x^{r^n} \equiv x \bmod f(x)\} \quad .$$

Beweis: Da $f(x)$ normiert und separabel ist, zerfällt es im Körper $\mathbb{F}_{r^n}$ genau dann in Linearfaktoren, wenn $f(x)$ das Polynom $x^{r^n} - x$ teilt. □

Wir können also den Grad des Zerfällungskörpers berechnen, ohne f zu faktorisieren. Das obige n kann man mit Hilfe des folgenden Lemmas effizienter berechnen.

Lemma 4.1.6. *Sei $f(x) \in \mathbb{F}_r[x]$ normiert und separabel. Sei weiter*

$$M := \{\bar{x}^{r^m} \in \mathbb{F}_r[x]/_{f(x)} \mid m \in \mathbb{N}\}$$

und

$$* : \left(\mathbb{F}_r[x]/_{f(x)}\right) \times \left(\mathbb{F}_r[x]/_{f(x)}\right) \to \mathbb{F}_r[x]/_{f(x)}, \quad (\alpha(x), \beta(x)) \mapsto \alpha(\beta(x)) \quad .$$

Dann ist $(M, *)$ eine abelsche Gruppe.

Beweis: Es gilt $\bar{x}^{r^m} * \bar{x}^{r^n} = (\bar{x}^{r^n})^{r^m} = \bar{x}^{r^{n+m}}$, also ist M unter der Verknüpfung abgeschlossen, und die Verknüpfung ist kommutativ. Es ist klar, daß $*$ assoziativ ist. Das neutrale Element ist $\bar{x}$, und nach dem obigen Lemma liegt $\bar{x}$ in M. Da M endlich ist, liegt dann zu jedem Element auch sein Inverses in M. □

Da der Grad des Zerfällungskörpers von f die Ordnung von $\bar{x}^r$ in der abelschen Gruppe $(M, *)$ ist, können wir $[\mathrm{ZerfKp}(f) : \mathbb{F}_r]$ mit Hilfe eines Baby-Step-Giant-Step-Algorithmus ermitteln, ohne alle Potenzen $\bar{x}^{q^i}$ für $1 \leqslant i \leqslant [\mathrm{ZerfKp}(f) : \mathbb{F}_r]$ berechnen zu müssen.
Kommen wir nun zur Berechnung von $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}})$ zurück. Wir benutzen, daß $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}}) = \#\mathrm{Gal}(\mathbb{F}_{\mathfrak{p}}\left({}_{\mathfrak{l}}\mathrm{Dred}(\phi, \mathfrak{p})\right), \mathbb{F}_{\mathfrak{p}})$ ist.

Satz 4.1.7. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \sum_{i=1}^{r} a_i \tau^i)$ ein Rang-r Drinfeld-Modul, $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$. Weiter habe ϕ gute Reduktion an $\mathfrak{p}(u)$, und es sei $\mathfrak{p}(T) \neq \mathfrak{l}(T)$. Es sei $g(x) := \mathrm{Dred}(\phi, \mathfrak{p})_{\mathfrak{l}}(x) \in \mathbb{F}_{\mathfrak{p}}(x)$ und $f(x) = (\mathrm{coeff}_x(q^{r \cdot \deg_T(\mathfrak{l})}, g(x)))^{-1} \cdot g(x)$ das zugehörige normierte Polynom. Dann gilt*

$$\mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}}) = \min\{n \in \mathbb{N} \mid x^{(\#\mathbb{F}_{\mathfrak{p}})^n} \equiv x \bmod f(x)\} \, .$$

Beweis: Das Polynom $\phi_{\mathfrak{l}}(x)$ hat die Form

$$\phi_{\mathfrak{l}}(x) = \mathfrak{l}(u) \cdot x + \sum_{i=1}^{r \cdot \deg_T(\mathfrak{l})} b_i \cdot x^{q^i} \in \mathbb{F}_q(u)[x] \quad .$$

Da ϕ gute Reduktion an $\mathfrak{p}$ hat, ist $b_{r \cdot \deg_T(\mathfrak{l})} \not\equiv 0 \bmod \mathfrak{p}$. Es ist $\frac{d}{dx}(\phi_{\mathfrak{l}}(x)) = \mathfrak{l}(u) \not\equiv 0 \bmod \mathfrak{p}$, und damit sind die Polynome $g(x)$ und $f(x)$ separabel. Da $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}})$ der Grad des Zerfällungskörpers von $f(x)$ (bzw. $g(x)$) ist, folgt die Aussage. □

Im Rang-2 Fall erhalten wir daraus das folgende Korollar:

Korollar 4.1.8. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul, $\mathfrak{p}, \mathfrak{P}, \mathfrak{l}, f(x)$ wie oben und $\mathfrak{l}(T) \neq \mathfrak{p}(T)$. Sei $\alpha \in \mathbb{F}_{\mathfrak{p}}^*$, $p = char(\mathbb{F}_q)$ und $\mathrm{charpol}(\mathrm{Frob}_{\mathfrak{P}}) = (X - \alpha)^2 \in \mathbb{F}_{\mathfrak{l}}[X]$. Dann sind äquivalent*

(i) $\mathrm{Frob}_{\mathfrak{P}}$ *ist konjugiert zu* $\begin{pmatrix} \alpha & 0 \\ 0 & \alpha \end{pmatrix}$,

(ii) $\mathrm{ord}(\mathrm{Frob}_{\mathfrak{P}}) \not\equiv 0 \bmod p$,

(iii) $x^{(\#\mathbb{F}_\mathfrak{p})^{\mathrm{ord}(\alpha)}} \equiv x \bmod f(x)$,

(iv) $x^{\#\mathbb{F}_\mathfrak{p}^{(\#\mathbb{F}_\mathfrak{l}-1)}} \equiv x \bmod f(x)$.

Beweis: Die Ordnung von $\left(\begin{smallmatrix}\alpha & 0\\ 0 & \alpha\end{smallmatrix}\right)$ ist $\mathrm{ord}(\alpha)$, und die Ordnung von $\left(\begin{smallmatrix}\alpha & 1\\ 0 & \alpha\end{smallmatrix}\right)$ ist $p \cdot \mathrm{ord}(\alpha)$. Weiter ist $\mathrm{ord}(\alpha)$ ein Teiler von $\#\mathbb{F}_\mathfrak{l} - 1$ und $\mathrm{ggT}(\#\mathbb{F}_\mathfrak{l} - 1, p) = 1$. Mit den Aussagen 4.1.4 und 4.1.7 von oben folgen die Äquivalenzen. $\square$

Bemerkung 4.1.9. (i) Das Polynom

$$\mathrm{Dred}(\phi, \mathfrak{p})_\mathfrak{l}(x) = \sum_{i=0}^{r \deg_T(\mathfrak{l})} b_i x^{q^i} \in \mathbb{F}_\mathfrak{p}[x]$$

ist i.a. ein Polynom hohen Grades. Da aber die meisten Koeffizienten gleich Null sind, kann es mit wenig Speicherplatz repräsentiert werden. Zum Beispiel werden in Simath [Sim] Polynome standardmäßig nur durch ihre Koeffizienten ungleich Null repräsentiert. Berechnet man nun

$$x^{q^m} \bmod \mathrm{Dred}(\phi, \mathfrak{p})_\mathfrak{l}(x) ,$$

so erhält man für $m \geqslant r \cdot \deg_T(\mathfrak{l})$ i.a. weitgehend vollbesetzte Polynome vom Grad $q^{r \deg_T(\mathfrak{l})}$. Diese benötigen viel Speicherplatz und machen die Rechnung zeitintensiv. Es ist wesentlich zeitintensiver, die Ordnung des Frobenius auszurechnen als sein charakteristisches Polynom. Daher ist unser Algorithmus so konzipiert, daß möglichst vermieden wird, den exakten Konjugationstyp zu ermitteln, falls das charakteristische Polynom eine doppelte Nullstelle hat (vgl. Seite 102). Da von den $(\#\mathbb{F}_\mathfrak{l}^2 - \#\mathbb{F}_\mathfrak{l}) \cdot (\#\mathbb{F}_\mathfrak{l}^2 - 1)$ Matrizen in $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ lediglich $(\#\mathbb{F}_\mathfrak{l} - 1) + (\#\mathbb{F}_\mathfrak{l} - 1) \cdot (\#\mathbb{F}_\mathfrak{l}^2 - 1)$ Matrizen ein solches charakteristisches Polynom haben, sollte dieser Fall auch nur etwa in einem von $\#\mathbb{F}_\mathfrak{l} = q^{\deg_T(\mathfrak{l})}$ Fällen auftreten.

(ii) Im Rang-2 Fall kann das charakteristische Polynom einer Stelle $\mathfrak{P}$ mit Satz 2.2.5 schnell berechnet werden, weil es nur von der Stelle $\mathfrak{p}(u) = \mathfrak{P} \cap \mathbb{F}_q(u)$ abhängt. Mit den Ergebnissen aus diesem Abschnitt können wir dann den Konjugationstyp von $\mathrm{Frob}_\mathfrak{P}$ explizit bestimmen. Da wir nur $\mathfrak{p}(u)$ als normiertes Primpolynom in $\mathbb{F}_q[u]$ explizit gegeben haben und wir $\mathfrak{P}$ mit unseren Methoden nicht von den anderen Stellen über $\mathfrak{p}(u)$ unterscheiden können, ist der GL(2)-Konjugationstyp die maximale Information, die wir über $\mathrm{Frob}_\mathfrak{P}$ erhalten können.

4.2 Rationale Isogenien

In den folgenden Abschnitten wollen wir einige Situationen beleuchten, in denen a priori

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$$

gelten muß.

Satz 4.2.1. *Sei* $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ *ein Rang-2 Drinfeld-Modul,* $\mathfrak{n} \in \mathbb{F}_q[T] - \mathbb{F}_q$. *Dann gilt: Ist* ${}_{\mathfrak{n}}\phi\left(\overline{\mathbb{F}_q(u)}\right) \cap \mathbb{F}_q(u) \neq \{0\}$, *so ist*

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{n}}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2,\ \mathbb{F}_q[T]/\mathfrak{n}) .$$

Beweis: Wir halten fest, daß ${}_{\mathfrak{n}}\phi\left(\overline{\mathbb{F}_q(u)}\right) = {}_{\mathfrak{n}}\phi\left(\mathbb{F}_q(u)^{sep}\right)$ gilt, da das Polynom $\phi_{\mathfrak{n}}(x) \in \mathbb{F}_q(u)[x]$ separabel ist. Sei nun $0 \neq \alpha \in {}_{\mathfrak{n}}\phi\left(\overline{\mathbb{F}_q(u)}\right) \cap \mathbb{F}_q(u)$. Dann gilt $\sigma(\alpha) = \alpha$ für alle σ aus $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{n}}\phi], \mathbb{F}_q(u))$. Da aber $\mathrm{GL}(2, \mathbb{F}_q[T]/\mathfrak{n})$ transitiv auf $(\mathbb{F}_q[T]/\mathfrak{n})^2 - \{(0,0)\}$ operiert, können die beiden Gruppen nicht gleich sein. □

Ist ${}_{\mathfrak{n}}\phi\left(\overline{\mathbb{F}_q(u)}\right) \cap \mathbb{F}_q(u) \neq \{0\}$, so sagen wir, daß der Drinfeld-Modul *rationale* $\mathfrak{n}$-*Torsion* hat.

Lemma 4.2.2. *Ist im obigen Satz* $\mathfrak{n} = \mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$ *irreduzibel, so ist die Gruppe* $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$ *konjugiert zu einer Untergruppe von* $\left(\begin{smallmatrix} 1 & \mathbb{F}_{\mathfrak{l}} \\ 0 & \mathbb{F}_{\mathfrak{l}}{}^* \end{smallmatrix}\right)$.

Beweis: Sei wie im obigen Beweis $0 \neq \alpha \in {}_{\mathfrak{l}}\phi\left(\overline{\mathbb{F}_q(u)}\right) \cap \mathbb{F}_q(u)$. Dann ist ${}_{\mathfrak{l}}\phi$ ein zweidimensionaler Vektorraum über dem Körper $\mathbb{F}_{\mathfrak{l}} = \mathbb{F}_q[T]/\mathfrak{l}$. Daher können wir α zu einer geordneten Basis $\{\alpha, \beta\}$ ergänzen. Da alle Elemente der Galoisgruppe α fixieren, haben sie bezüglich der obigen Basis die Form $\left(\begin{smallmatrix} 1 & * \\ 0 & * \end{smallmatrix}\right)$. Damit ist das Lemma gezeigt. □

Im nächsten Beispiel werden wir eine Familie von Drinfeld-Moduln konstruieren, die rationale T-Torsionspunkte besitzen.

Beispiel 4.2.3. Zu einem $h \in \mathbb{F}_q(u)^*$ betrachten wir den Rang-2 Drinfeld-Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u(1 - h\tau)(1 - \tau))$. Dann ist

$$\phi_T(x) = u\big((x - x^q) - h \cdot (x - x^q)^q\big) = u \cdot (x - x^q) \cdot \big(1 - h\ (x - x^q)^{q-1}\big) .$$

Daher gilt

$$\big({}_T\phi \cap \mathbb{F}_q(u)\big) \supset \mathbb{F}_q .$$

Damit haben alle diese Drinfeld-Moduln rationale T-Torsion. Wählen wir noch $h = \frac{1}{(u-u^q)^{q-1}}$, so ist auch u ein T-Torsionspunkt von ϕ, und wir erhalten

$${}_T\phi = \mathbb{F}_T *_\phi 1 + \mathbb{F}_T *_\phi u = \mathbb{F}_q *_\phi 1 + \mathbb{F}_q *_\phi u = \{\alpha + \beta u \mid \alpha, \beta \in \mathbb{F}_q\} .$$

Für diesen Modul ist damit sogar die ganze T-Torsion rational. □

Bemerkung 4.2.4. Ist $\mathfrak{n} \in \mathbb{F}_q[T]$ ein nichtkonstantes nichtprimes Polynom und $A_{\mathfrak{n}} := \mathbb{F}_q[T]/\mathfrak{n}$, so existieren Punkte $P \in A_{\mathfrak{n}} \times A_{\mathfrak{n}}$, für die der Stabilisator

$Stab_{\mathrm{GL}(2,A_{\mathfrak{n}})}(P)$ nicht zu einer Gruppe der Form $\begin{pmatrix}1 & * \\ 0 & *\end{pmatrix}$ konjugiert ist. Sei z.B. $\mathfrak{n} = \mathfrak{p} \cdot \mathfrak{q}$ das Produkt zweier verschiedener Primpolynome und $P = (\overline{\mathfrak{p}}, \overline{0}) \in A_{\mathfrak{n}} \times A_{\mathfrak{n}}$. Dann ist nach dem Chinesischen Restsatz

$$\mathrm{GL}(2, A_{\mathfrak{n}}) \cong \mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}}) \times \mathrm{GL}(2, \mathbb{F}_{\mathfrak{q}}) \; .$$

Da sich dabei P in der Form $(0,0) \times (\mathfrak{p}, 0) \in \mathbb{F}_{\mathfrak{p}}^2 \times \mathbb{F}_{\mathfrak{q}}^2$ zerlegt, ist

$$Stab_{\mathrm{GL}(2,A_{\mathfrak{n}})}(P) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{p}}) \times \begin{pmatrix}1 & \mathbb{F}_{\mathfrak{q}} \\ 0 & \mathbb{F}_{\mathfrak{q}}^*\end{pmatrix} \qquad .$$

Vergleicht man nun die Mächtigkeiten der beiden Gruppen

$$\begin{aligned}
\#Stab_{\mathrm{GL}(2,A_{\mathfrak{n}})}(P) &= (\#\mathbb{F}_{\mathfrak{p}}{}^2 - 1)\,(\#\mathbb{F}_{\mathfrak{p}}{}^2 - \#\mathbb{F}_{\mathfrak{p}})\,(\#\mathbb{F}_{\mathfrak{q}} - 1)\,\#\mathbb{F}_{\mathfrak{q}} \\
&\neq (\#\mathbb{F}_{\mathfrak{p}} - 1)(\#\mathbb{F}_{\mathfrak{q}} - 1)\,\#\mathbb{F}_{\mathfrak{p}}\#\mathbb{F}_{\mathfrak{q}} \\
&= (\#A_{\mathfrak{n}}^*) \cdot (\#A_{\mathfrak{n}}) \\
&= \#\begin{pmatrix}1 & A_{\mathfrak{n}} \\ 0 & A_{\mathfrak{n}}^*\end{pmatrix} \; ,
\end{aligned}$$

so sieht man, daß sie nicht konjugiert sind.

Kommen wir nun zu weiteren nichtmaximalen Erweiterungen.

Satz 4.2.5. *Seien $w \in \mathbb{F}_q(u)\{\tau\}$ separabel, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, \phi_T)$, $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, \psi_T)$ zwei Rang-2 Drinfeld-Moduln, und es sei $\{0\} \subsetneq \ker(w) \subsetneq {}_{\mathfrak{l}}\psi(\overline{\mathbb{F}_q(u)})$. Gilt $w \circ \phi_T = \psi_T \circ w$ (d.h. $w \in \mathrm{Hom}_{\mathbb{F}_q(u)}(\phi, \psi)$), so ist bis auf Konjugation*

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u)) \leqslant \begin{pmatrix}\mathbb{F}_{\mathfrak{l}}{}^* & \mathbb{F}_{\mathfrak{l}} \\ 0 & \mathbb{F}_{\mathfrak{l}}{}^*\end{pmatrix} \; .$$

Beweis: Da $w(x)$ ein Polynom mit Koeffizienten in $\mathbb{F}_q(u)$ ist, gilt

$$\sigma(\ker(w)) = \ker(w) \quad \forall \sigma \in \mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u)) \; .$$

Für ein $\mathfrak{m} \in \mathbb{F}_q[T]$ und ein $\alpha \in \ker(w)$ gilt

$$w(\mathfrak{m} *_{\phi} \alpha) = w\,(\phi_{\mathfrak{m}}(\alpha)) = \psi_{\mathfrak{m}}(w(\alpha)) = 0 \; .$$

Daher ist $\ker(w)$ auch ein $(\mathbb{F}_q[T], *_{\phi})$-Untermodul von $\mathbb{F}_q(u)^{sep}$. Aufgrund der Voraussetzung ist $\ker(w)$ sogar ein galoisinvarianter Untermodul von ${}_{\mathfrak{l}}\phi$. Da $\mathfrak{l}$ prim ist, sind ${}_{\mathfrak{l}}\phi$ und $\ker(w)$ dann $(\mathbb{F}_{\mathfrak{l}}, *_{\phi})$-Vektorräume. Man kann ihre Dimension betrachten und erhält $0 < \dim_{\mathbb{F}_{\mathfrak{l}}}(\ker(w)) < 2$. Also existiert eine Basis $\{\alpha, \beta\}$ von ${}_{\mathfrak{l}}\phi$ mit $\alpha \in \ker(w)$, $\beta \in {}_{\mathfrak{l}}\phi$. Da $\ker(w)$ galoisinvariant ist, lassen sich alle Elemente der Galoisgruppe bezüglich dieser Basis durch obere Dreiecksmatrizen darstellen. □

4.3 Komplexe Multiplikation

Wir werden nun eine weitere Situation betrachten, in der $\mathrm{Gal}(\mathbb{F}_q(u)[\imath\phi], \mathbb{F}_q(u))$ nicht maximal ist. Um diese zu untersuchen, werden wir in einigen Argumenten benutzen, daß man Drinfeld-Moduln auf allgemeineren Ringen als $\mathbb{F}_q[T]$ definieren kann. Diese allgemeineren Drinfeld-Moduln treten allerdings nur in diesem Abschnitt auf. Daher werden wir sie hier nicht exakt definieren und verweisen stattdessen auf Kapitel 4 aus [Gos96] und die Arbeit [Hay79].
Sei also $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ unser Rang-2 Drinfeld-Modul. Er habe komplexe Multiplikation durch die Ordnung A. Weiter sei $K = Quot(A)$ der Quotientenkörper und O_K der ganze Abschluß von A in K (der mit dem ganzen Abschluß von $\mathbb{F}_q[T]$ übereinstimmt).

$$\begin{array}{ccccc} A & \hookrightarrow & O_K & \hookrightarrow & K \\ & & | & & | \\ & & \mathbb{F}_q[T] & \hookrightarrow & \mathbb{F}_q(T) \end{array}$$

Dann ist $K|\mathbb{F}_q(T)$ eine imaginär-quadratische Erweiterung von globalen Funktionenkörpern (d.h. die unendliche Stelle von $\mathbb{F}_q(T)$ zerfällt nicht in K). Die Abbildung $i_\phi : T \mapsto u$ legt eine Einbettung

$$\mathbb{F}_q(T) \hookrightarrow \mathbb{F}_q(u)$$

fest und läßt sich auf zwei Weisen zu Einbettungen

$$\imath_1, \imath_2 : K \hookrightarrow \overline{\mathbb{F}_q(u)}$$

fortsetzen. (Außer im Fall $\mathrm{char}(\mathbb{F}_q) = 2$ und $K = \mathbb{F}_q(\sqrt{T})$. In diesem Fall gelten die folgenden Aussagen trivialerweise.)
Für einen fest gewählten algebraischen Abschluß $\overline{\mathbb{F}_q(u)}$ gilt

$$\imath_1(K) = \imath_2(K)\ .$$

Wir wählen im weiteren eine der Einbettungen fest und bezeichnen sie mit $\imath$. Das Bild von K unter $\imath$ wird mit $\tilde{K}$ bezeichnet.
Für einen gegebenen Drinfeld-Modul können wir leicht testen, ob er komplexe Multiplikation hat. Es gilt der folgende Satz von Schweizer aus [Sch96, Theorem 3.2.7].

Satz 4.3.1. *Ein Rang-2 Drinfeld-Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ hat genau dann komplexe Multiplikation, wenn $j(\phi) = \frac{g^{q+1}}{\Delta}$ bereits in $\mathbb{F}_q[u]$ liegt und* *in der folgenden Liste vorkommt:*

q	$j = j(\phi)$	*Gleichung für* ω	$\mathfrak{f}$	g
bel.	0	$\omega = \gamma$	1	0
bel.	$j_\beta = (u^q - u)(1 - (u-\beta)^{q^2-q})$	$\omega = \gamma(u-\beta)$	$T - \beta$	0
2	$j_\square = u^3(u+1)^3(u^2+u+1)$	$\omega = \gamma(u^2+u+1)$	T^2+T+1	0
$2 \not\mid q$	$(u-\beta)^{\frac{q+1}{2}}((u-\beta)^{\frac{q-1}{2}}+1)^{q+1}$	$\omega^2 = u - \beta$	1	0
$2 \not\mid q$	$-(u-\beta)^{\frac{q+1}{2}}((u-\beta)^{\frac{q-1}{2}}-1)^{q+1}$	$\omega^2 = \varepsilon(u-\beta)$	1	0
2^n	$\alpha^{-1}(\ell^{2^{n-1}} + \ell^{2^{n-2}} + \ldots + \ell + 1)^{q+1}$	$\omega^2 + \omega = \alpha u + \beta = \ell$	1	0
2	$(u+1)^6$	$\omega^2 + u\omega = u^3$	T	0
2	u^6	$\omega^2 + (u+1)\omega = (u+1)^3$	$T+1$	0
2	$u^3(u+1)^3$	$\omega^2 + \omega = u^3 + u + 1$	1	1
2	$u^6(u+1)^6$	$\omega^2 + \omega = u^5 + u^3 + 1$	1	2
3	$u^4(u+1)^4(u-1)^4(u^3-u-1)^2$	$\omega^2 = u^3 - u - 1$	1	1
3	$-u^4(u+1)^4(u-1)^4(u^3-u+1)^2$	$\omega^2 = -u^3 + u - 1$	1	1
4	$(u^4+u)^{10}$	$\omega^2 + \omega = u^3 + \delta$	1	1

Dabei ist $\alpha \in \mathbb{F}_q{}^*$, $\beta \in \mathbb{F}_q$, $\ell = \alpha u + \beta$, δ *eine Primitivwurzel in* $\mathbb{F}_4^*$, $\mathbb{F}_{q^2} = \mathbb{F}_q(\gamma)$ *und* $\varepsilon \in \mathbb{F}_q{}^*$ *kein Quadrat. Außerdem ist* $K = \big(\mathbb{F}_q(u)\big)(\omega)$, $A = (\mathbb{F}_q[T])[\omega]$, *und* $\mathfrak{f}$ *bezeichnet den Führer der Ordnung* A *(d.h.* $A = \mathbb{F}_q[T] + \mathfrak{f}O_K$*). Ferner bezeichnet* g *das Geschlecht des Funktionenkörpers* K.

Wir sehen, daß in 9 der 13 Fälle A gleich der Maximalordnung O_K ist. In diesen Fällen existiert nun ein Rang-1 Drinfeld-Modul

$$\psi : O_K \mapsto \overline{\mathbb{F}_q(u)}\{\tau\}$$

mit

$$\psi\,|_{\mathbb{F}_q[T]} = \phi\ .$$

(Hier verwenden wir, daß man Drinfeld-Moduln auf allgemeineren Ringen als $\mathbb{F}_q[T]$ definieren kann.) Wir betrachten nun das folgende Körperdiagramm:

$$\begin{tikzcd}[column sep=small]
 & \tilde{K}[{}_{\mathfrak{f}}\phi] \arrow[dl, dash] \arrow[dr, dash] & \\
\tilde{K} \arrow[dr, dash] & & \mathbb{F}_q(u)[{}_{\mathfrak{f}}\phi] \arrow[dl, dash] \\
 & \tilde{K} \cap \mathbb{F}_q(u)[{}_{\mathfrak{f}}\phi] \arrow[d, dash] & \\
 & \mathbb{F}_q(u) &
\end{tikzcd}$$

Nach der Theorie für allgemeine Rang-1 Drinfeld-Moduln ist

$$\mathrm{Gal}(\tilde{K}[{}_{\mathfrak{f}}\psi], \tilde{K}) \leqslant \left({}^{O_K}\!/_{\mathfrak{f}}\right)^* = \mathrm{GL}(1, {}^{O_K}\!/_{\mathfrak{f}})\ , \qquad (*)$$

wobei zu beachten ist, daß das Ideal $\mathfrak{l}(u)\cdot O_K$ unter Umständen nicht prim ist. Da

$$\tilde{K}[{}_{\mathfrak{l}}\phi]=\tilde{K}[{}_{\mathfrak{l}}\psi]$$

ist, folgt dann mit dem Verlagerungssatz der Galoistheorie

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi],\tilde{K}\cap\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi])\leqslant\left({}^{O_K}/_{\mathfrak{l}}\right)^*.$$

Den Quotienten kann man wie folgt beschreiben:

$$\left({}^{O_K}/_{\mathfrak{l}}\right)^*\cong\begin{cases}(\mathbb{F}_{\mathfrak{l}}\times\mathbb{F}_{\mathfrak{l}})^* & ;\ \mathfrak{l}\text{ zerfällt in }K\\ \mathbb{F}^*_{q^{2\deg_T(\mathfrak{l})}} & ;\ \mathfrak{l}\text{ ist träge in }K\\ \left({}^{\mathbb{F}_q[T]}/_{\mathfrak{l}^2}\right)^* & ;\ \mathfrak{l}\text{ ist verzweigt in }K\end{cases}$$

Für Stellen $\mathfrak{l}$ guter Reduktion liefert uns das folgende Lemma von Bae [Bae95b, Theorem 1.5], daß der dritte Fall nicht auftreten kann.

Lemma 4.3.2. *Der Rang-2 Drinfeld-Modul $\phi=(\mathbb{F}_q,\mathbb{F}_q(u),u,u+g\tau+\Delta\tau^2)$ habe komplexe Multiplikation durch die Ordnung A. Weiter sei $K=Quot(A)$ und $\mathfrak{l}(T)\in\mathbb{P}_{\mathbb{F}_q[T]}$. Ist dann $\mathfrak{l}(T)$ in $K|\mathbb{F}_q(T)$ verzweigt, so hat ϕ schlechte Reduktion an $\mathfrak{p}(u)$.*

Wir können die Aussage des Lemmas auch direkt erhalten, indem wir die endlich vielen Fälle aus der Liste 4.3.1 von Schweizer Fall für Fall durchgehen.
Wir sind nun in der Lage, genauere Aussagen über die auftretenden Galoisdarstellungen zu machen.

Satz 4.3.3. *Seien die Bezeichnungen wie oben. Insbesondere sei ϕ ein Rang-2 Drinfeld-Modul mit komplexer Multiplikation durch A. Weiter seien $A=O_K$, $\mathfrak{l}\in\mathbb{P}_{\mathbb{F}_q[T]}$, $\mathrm{Gal}:=\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi],\mathbb{F}_q(u))$, $\mathfrak{Z}$ eine zerfallende Cartanuntergruppe und $\mathfrak{T}$ eine nichtzerfallende Cartanuntergruppe von $\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})$. Sei weiter $\mathbb{F}_{\mathfrak{l}}\neq\mathbb{F}_2$, und ϕ habe gute Reduktion an $\mathfrak{l}(u)$. Dann gilt bis auf Konjugation in $\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})$:*

(i)

$$\left\{\begin{array}{rc} & \mathfrak{l}\textit{ zerfällt in }K|\mathbb{F}_q(T)\\ \textit{und} & \tilde{K}\cap\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]=\mathbb{F}_q(u)\end{array}\right\}\Rightarrow(\mathrm{Gal}\leqslant\mathfrak{Z})$$

(ii)

$$\left\{\begin{array}{rc} & \mathfrak{l}\textit{ zerfällt in }K|\mathbb{F}_q(T)\\ \textit{und} & \tilde{K}\cap\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]=\tilde{K}\end{array}\right\}\Rightarrow(\mathrm{Gal}\not\leqslant\mathfrak{Z}\textit{ und }\mathrm{Gal}\leqslant\mathrm{Norm}(\mathfrak{Z}))$$

(iii)

$$\left\{\begin{array}{rc} & \mathfrak{l}\textit{ träge in }K|\mathbb{F}_q(T)\\ \textit{und} & \tilde{K}\cap\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]=\mathbb{F}_q(u)\end{array}\right\}\Rightarrow(\mathrm{Gal}\leqslant\mathfrak{T})$$

(iv)

$$\left.\begin{array}{rc} & \mathfrak{l} \textit{ träge in } K|\mathbb{F}_q(T) \\ \textit{und} & \tilde{K} \cap \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] = \tilde{K} \end{array}\right\} \Rightarrow (\mathrm{Gal} \not\leqslant \mathfrak{T} \textit{ und } \mathrm{Gal} \leqslant \mathrm{Norm}(\mathfrak{T}))$$

Beweis: Nach Lemma 4.3.2 ist $\mathfrak{l}(T)$ in $K|\mathbb{F}_q(T)$ unverzweigt. Daher bettet sich $({}^{O_K}/_{\mathfrak{l}})^*$ in eine zerfallende (bzw. nichtzerfallende) Cartanuntergruppe der $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ ein, falls $\mathfrak{l}$ in K zerfällt (bzw. nicht zerfällt).
Sei nun $\tilde{L} := \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \cap \tilde{K}$. Dann ist

$$\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u)) = \mathrm{Gal}(\tilde{L}, \mathbb{F}_q(u)) \ltimes \mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \tilde{L})\ .$$

Da $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \tilde{L}) \leqslant ({}^{O_K}/_{\mathfrak{l}})^*$ normal in $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u))$ ist, folgt die Aussage mit Lemma 3.2.4. □

Damit erhalten wir, daß Drinfeld-Moduln mit komplexer Multiplikation durch eine Maximalordnung fast nie maximale Torsionserweiterungen haben.

Satz 4.3.4. *Seien die Voraussetzungen wie in Satz 4.3.3. Insbesondere sei ϕ ein Rang-2 Drinfeld-Modul mit komplexer Multiplikation durch $A = O_K$ und $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$. Ist dann $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u))$ gleich $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$, so ist*

$$\mathbb{F}_{\mathfrak{l}} = \mathbb{F}_2 \quad , \quad \tilde{K} \subset \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \quad \textit{und} \quad \mathfrak{l} \textit{ in } \tilde{K}|\mathbb{F}_q(u) \textit{ träge}\ .$$

Beweis: Im Beweis des letzten Satzes haben wir gesehen, daß

$$\#\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u)) = \#\mathrm{Gal}(\tilde{L}, \mathbb{F}_q(u)) \cdot \#\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \tilde{L})$$

ist. Dabei ist $\#\mathrm{Gal}(\tilde{L}, \mathbb{F}_q(u)) \leqslant 2$ und $\#\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \tilde{L})$ ein Teiler von $\#\mathbb{F}_{\mathfrak{l}}{}^2 - 1$ oder $(\#\mathbb{F}_{\mathfrak{l}} - 1)^2$. Daher kann die Gleichheit

$$\#\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) = (\#\mathbb{F}_{\mathfrak{l}}{}^2 - 1) \cdot (\#\mathbb{F}_{\mathfrak{l}}{}^2 - \#\mathbb{F}_{\mathfrak{l}}) = \#\mathrm{Gal}(\tilde{L}, \mathbb{F}_q(u)) \cdot \#\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \tilde{L})$$

nur gelten, falls $\#\mathrm{Gal}(\tilde{L}, \mathbb{F}_q(u)) = 2$, $\#\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \tilde{L}) = \#\mathbb{F}_{\mathfrak{l}}{}^2 - 1$ und $\#\mathbb{F}_{\mathfrak{l}} = 2$ gilt. □

Die nächsten Beispiele zeigen, daß in der obigen Aussage keine Äquivalenz gilt.

Beispiel 4.3.5. (i) Sei $\phi = (\mathbb{F}_2, \mathbb{F}_2(u), u, u + \tau^2)$. Dann ist $\phi_T(x) = x(u + x^3)$, $K = \mathbb{F}_4(T)$, $\tilde{K} = \mathbb{F}_4(u)$ und T in $K|\mathbb{F}_2(T)$ träge. Nach Kummertheorie ist $\mathbb{F}_2(u)[_T\phi] = \mathbb{F}_4(\sqrt[3]{u})$, und wir erhalten

$$[\mathbb{F}_2(u)[_T\phi] : \mathbb{F}_2(u)] = 6 = \#\mathrm{GL}(2, \mathbb{F}_T) = \#\mathrm{GL}(2, \mathbb{F}_2)\ ,$$

also

$$\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})\ .$$

(ii) Sei nun $\phi = (\mathbb{F}_2, \mathbb{F}_2(u), u, u + u\tau^2)$. Dann ist $\phi_T(x) = ux(1+x)(1+x+x^2)$, $K = \mathbb{F}_4(T)$, $\tilde{K} = \mathbb{F}_4(u)$ und T in $K|\mathbb{F}_2(T)$ träge. Es ist $\mathbb{F}_2(u)[_T\phi] = \mathbb{F}_4(u)$. Beschreiben wir nun die T-Torsion $\mathbb{F}_4$ als $\mathbb{F}_2[\alpha]/(\alpha^2+\alpha+1)$, so operiert das nichttriviale Galoiselement auf der $\mathbb{F}_2$-Basis $\{1, \alpha\}$ durch

$$1 \mapsto 1 \quad , \quad \alpha \mapsto \alpha + 1 \; .$$

Bzgl. dieser Basis gilt dann

$$\mathrm{Gal}(\mathbb{F}_2(u)[_T\phi], \mathbb{F}_2(u)) = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \; ,$$

also

$$\mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l}) \; .$$

□

Ist A keine Maximalordnung (dies tritt in 4 Fällen auf), so können die obigen Argumente analog durchgeführt werden. Allerdings erhält man dann keinen Rang-1 Drinfeld-Modul, sondern einen Modul

$$\psi : A \mapsto \overline{\mathbb{F}_q(u)}\{\tau\} \quad .$$

Wie in [Hay79] gezeigt, verhalten sich solche Moduln wie Rang-1 Drinfeld-Moduln. Ersetzt man die Ungleichung $(*)$ durch

$$\mathrm{Gal}(\tilde{K}[_\mathfrak{l}\psi], \tilde{K}) \leqslant \left({}^{A}/_{\mathfrak{l}}\right)^* \leqslant \left({}^{O_K}/_{\mathfrak{l}}\right)^* = \mathrm{GL}(1, {}^{O_K}/_{\mathfrak{l}}) \; ,$$

so erhält man analoge Resultate, sofern $\mathfrak{l}(T)$ teilerfremd zum Führer von A ist.

4.4 Die Rang-1 Teilerweiterung

Um die Erweiterung

$$\mathbb{F}_q(u)[_\mathfrak{l}\phi] \mid \mathbb{F}_q(u)$$

in unserer Situation (ϕ ein Rang-2 Drinfeld-Modul über $\mathbb{F}_q(u)$ etc.) zu beschreiben, ist es hilfreich, wenn man Zwischenerweiterungen unter Kontrolle hat. Eine solche Zwischenerweiterung werden wir in diesem Abschnitt angeben.

Dazu müssen wir allerdings das äußere Produkt von ϕ mit sich in der Kategorie der Drinfeld-Moduln bilden. Leider ist es aber in dieser Kategorie nicht möglich, zu tensorieren oder Quotienten zu bilden. Daher wurde von Anderson in [And86] der Begriff des t-Moduls (einer Verallgemeinerung eines Drinfeld-Moduls) eingeführt. Diese t-Moduln bilden mit passend definierten Morphismen eine Kategorie, die unter Tensorierung und Quotientenbildung abgeschlossen ist und die Drinfeld-Moduln als Teilkategorie enthält.

In unserem speziellen Fall ergibt sich, daß das äußere Produkt von ϕ (als t-Modul) mit sich doch wieder ein Drinfeld-Modul ist. Und zwar gilt (vgl. [Ham93])

$$\phi \wedge \phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau) \ .$$

Daher nennen wir $(\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau)$ den zum Rang-2 Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ *assoziierten* Drinfeld-Modul. Nach [Ham93, Theorem 4.5] gilt:

Satz 4.4.1. *Sei* $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, $\Delta \in \mathbb{F}_q(u)^*$. *Dann existiert ein* $\mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u))$*-linearer Isomorphismus*

$$T_{\mathfrak{l}}(\phi) \wedge T_{\mathfrak{l}}(\phi) \xrightarrow{\cong} T_{\mathfrak{l}}(\phi \wedge \phi)$$

von $(\mathbb{F}_q[T])_{\mathfrak{l}}$*-Moduln.*

Korollar 4.4.2. *Sei* $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$, $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau)$ *und* $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$. *Dann existiert eine surjektive,* $\mathbb{F}_q[T]$*-bilineare und mit der Operation von* $\mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u))$ *verträgliche Paarung*

$$\mathcal{W} : {}_{\mathfrak{l}}\phi \times {}_{\mathfrak{l}}\phi \to {}_{\mathfrak{l}}\psi \ .$$

Beweis: Sei φ der Isomorphismus aus Satz 4.4.1 und proj die kanonische Projektionsabbildung vom Tate-Modul auf die $\mathfrak{l}$-Torsion. Zu $\alpha, \beta \in {}_{\mathfrak{l}}\phi$ seien $\tilde{\alpha}, \tilde{\beta} \in T_{\mathfrak{l}}(\phi)$ mit $\mathrm{proj}(\tilde{\alpha}) = \alpha$, $\mathrm{proj}(\tilde{\beta}) = \beta$. Dann definieren wir

$$\mathcal{W}(\alpha, \beta) := \mathrm{proj}(\varphi(\tilde{\alpha} \wedge \tilde{\beta})) \ .$$

Die Abbildung $\mathcal{W}$ hängt nicht von der speziellen Wahl von $\tilde{\alpha}$ und $\tilde{\beta}$ ab. Surjektivität, Bilinearität und Verträglichkeit mit der Galoisoperation folgen aus den entsprechenden Eigenschaften von φ. □

Bemerkung 4.4.3. Die Abbildung $\mathcal{W}$ ist das Analogon zur Weil-Paarung auf der Torsion von elliptischen Kurven (vgl. [Sil86]). Die Rolle des $\mathbb{Z}$-Moduls

$$\begin{array}{lcccc} pow & : & \mathbb{Z} \times \mathbb{C}^* & \to & \mathbb{C}^* \\ & & (z, \alpha) & \mapsto & \alpha^z \end{array} ,$$

wird hier vom Rang-1 Drinfeld-Modul

$$\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau)$$

übernommen. Allerdings ist im klassischen Fall der Modul *pow* unabhängig von der betrachteten elliptischen Kurve, während in unserem Fall ψ über das Δ vom Rang-2 Drinfeld-Modul ϕ abhängt.

Korollar 4.4.4. *In der Situation von oben gilt*

$$_{\mathfrak{l}}\psi \subset \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \ .$$

Beweis: Seien $\sigma \in \mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u)[_{\mathfrak{l}}\phi])$ und $\zeta \in {}_{\mathfrak{l}}\psi$ beliebig. Da $\mathcal{W}$ surjektiv ist, existieren $\alpha, \beta \in {}_{\mathfrak{l}}\phi$ mit $\mathcal{W}(\alpha,\beta) = \zeta$. Mit der Galoislinearität folgt dann

$$\sigma(\zeta) = \sigma(\mathcal{W}(\alpha,\beta)) = \mathcal{W}(\sigma(\alpha),\sigma(\beta)) = \mathcal{W}(\alpha,\beta) = \zeta \ .$$

Da dies für alle $\sigma \in \mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u)[_{\mathfrak{l}}\phi])$ gilt, folgt $\zeta \in \mathbb{F}_q(u)[_{\mathfrak{l}}\phi]$. □

Weiter induziert eine n-dimensionale lineare Darstellung auf dem n-fachen äußeren Produkt genau die Determinantendarstellung. Es gilt also:

Satz 4.4.5. *Sei* $\sigma \in \mathrm{Gal}(\mathbb{F}_q(u)^{sep}, \mathbb{F}_q(u))$ *und* $a \in \mathbb{F}_q(u)[_{\mathfrak{l}}\psi]$. *Dann ist*

$$\sigma(a) = \det(\rho_{\phi,\mathfrak{l}}^{red}(\sigma)) *_\psi a \ ,$$

wobei die rechte Seite wegen $\det(\rho_{\phi,\mathfrak{l}}^{red}(\sigma)) \in \mathbb{F}_{\mathfrak{l}}^{\ *}$ *und* $a \in {}_{\mathfrak{l}}\psi$ *wohldefiniert ist.*

Korollar 4.4.6. *Es ist*

$$\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u)[_{\mathfrak{l}}\psi]) = \mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\, , \mathbb{F}_q(u)) \cap \mathrm{SL}(2, \mathbb{F}_{\mathfrak{l}}).$$

Damit ergibt sich

$$\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\psi], \mathbb{F}_q(u)) = {}^{\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\, , \mathbb{F}_q(u))}\big/_{\left(\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\, , \mathbb{F}_q(u)) \cap \mathrm{SL}(2, \mathbb{F}_{\mathfrak{l}})\right)},$$

und es folgt:

Korollar 4.4.7. *Es gilt*

$$\{\det(M) \mid M \in \mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\, , \mathbb{F}_q(u))\} = \mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\psi], \mathbb{F}_q(u)) \ .$$

Damit erhalten wir eine weitere Familie von nichtmaximalen Erweiterungen.

Korollar 4.4.8. *Seien* $\alpha \in \mathbb{F}_q$, $g, h \in \mathbb{F}_q(u)$, $h \neq 0$ *beliebig. Weiter sei* $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + (u+\alpha)h^{q-1}\tau^2)$ *und* $\mathfrak{l}(T) = T + \alpha \in \mathbb{P}_{\mathbb{F}_q[T]}$. *Dann ist* $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\, , \mathbb{F}_q(u))$ *eine Untergruppe der* $\mathrm{SL}(2, \mathbb{F}_q)$.

Beweis: Zu ϕ ist der Rang-1 Drinfeld-Modul $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - (u+\alpha)h^{q-1}\tau)$ assoziiert. Dessen minimales Modell $(\mathbb{F}_q, \mathbb{F}_q(u), u, u - (u+\alpha)\tau)$ erhalten wir durch Konjugation mit h^{-1}. Damit ist $\psi_{T+\alpha}(x) = (u+\alpha)(x - x^q)$ und ${}_{T+\alpha}\psi = \mathbb{F}_q$. Daher ist $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\psi], \mathbb{F}_q(u)) = \{1\}$. Mit $\mathbb{F}_{T+\alpha} = \mathbb{F}_q$ folgt die Aussage. □

Analog zum Vorgehen im obigen Beweis erhält man zu jeder nichtmaximalen Rang-1 Erweiterung eine Familie von nichtmaximalen Rang-2 Erweiterungen. Allerdings zeigen die folgenden Resultate, daß Rang-1 Erweiterungen meist maximal sind.

Lemma 4.4.9. *Sei $\gamma = (\mathbb{F}_q, \mathbb{F}_q(u), u, u+\tau)$ der Carlitz-Modul und $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u+a\tau)$ ein beliebiger Rang-1 Drinfeld-Modul. Sei weiter $\mathfrak{n} \in \mathbb{F}_q[T]$ und $\gamma_\mathfrak{n}(\tau) = \sum_{i=0}^d c_i\,\tau^i$. Dann ist*

$$\psi_\mathfrak{n}(\tau) = \sum_{i=0}^d a^{\frac{q^i-1}{q-1}} c_i\,\tau^i\ .$$

Dabei ist zu beachten, daß die Exponenten $\frac{q^i-1}{q-1}$ immer ganzzahlig sind.

Beweis: Sei $\beta \in \overline{\mathbb{F}_q(u)}$ mit $\psi_T = \beta^{-1}\gamma_T\beta$, d.h. $\beta^{q-1} = a$. Dann gilt $\psi_\mathfrak{n} = \beta^{-1}\gamma_\mathfrak{n}\beta$. Also

$$\psi_\mathfrak{n} = \beta^{-1}\left(\sum_{i=0}^d c_i\,\tau^i\right)\beta = \sum_{i=0}^d \beta^{q^i-1} c_i\,\tau^i = \sum_{i=0}^d a^{\frac{q^i-1}{q-1}} c_i\,\tau^i\ .$$

□

Nun erhalten wir direkt:

Satz 4.4.10. *Sei $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u+a\tau)$ ein Rang-1 Drinfeld-Modul, $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$, und ψ habe gute Reduktion an $\mathfrak{l}(u)$. Dann gilt:*

(i)

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\psi]\,, \mathbb{F}_q(u)) = \mathbb{F}_\mathfrak{l}{}^*$$

(ii) Der volle Konstantenkörper von $\mathbb{F}_q(u)[{}_\mathfrak{l}\psi]$ ist $\mathbb{F}_q$.

Beweis: Da ψ gute Reduktion an $\mathfrak{l}(u)$ hat, ist für das minimale Modell $\min(\psi) = \tilde{\psi} = (\mathbb{F}_q, \mathbb{F}_q(u), u, u+\tilde{a}\tau)$ die Bewertung $v_\mathfrak{l}(\tilde{a}) = 0$. Sei γ wieder der Carlitz-Modul. Dann haben nach Lemma 4.4.9 die Polynome $\tilde{\psi}_\mathfrak{l}(x)$ und $\gamma_\mathfrak{l}(x)$ das gleiche Newton-Polygon an $\mathfrak{l}(u)$. Damit übertragen sich die entsprechenden Beweise aus [Hay74] von $\gamma_\mathfrak{l}(x)$ auf $\tilde{\psi}_\mathfrak{l}(x)$. Insbesondere ist $\frac{\tilde{\psi}_\mathfrak{l}(x)}{x} \in \mathbb{F}_q(u)[x]$ irreduzibel, und damit $[\mathbb{F}_q(u)[{}_\mathfrak{l}\psi] : \mathbb{F}_q(u)] \geqslant q^{\deg_T \mathfrak{l}} - 1$. Da aber $\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\psi]\,, \mathbb{F}_q(u)) \leqslant \mathbb{F}_\mathfrak{l}{}^*$ gilt, folgt Gleichheit. Weiter erhält man wie beim Carlitz-Modul, daß der Trägheitsindex der ∞-Stelle in $\mathbb{F}_q(u)[{}_\mathfrak{l}\psi]|\mathbb{F}_q(u)$ gleich Eins ist. Daher ist $\mathbb{F}_q$ der volle Konstantenkörper. □

In Verbindung mit Korollar 4.4.7 erhalten wir den folgenden Satz.

Satz 4.4.11. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u+g\tau+\Delta\tau^2)$ ein Rang-2 Drinfeld-Modul und $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$. Weiter sei $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u-\Delta\tau)$ der zugehörige Rang-1 Drinfeld-Modul mit minimalem Modell $\tilde{\psi} = (\mathbb{F}_q, \mathbb{F}_q(u), u, u-\tilde{\Delta}\tau)$. Ist dann $\tilde{\Delta} \not\equiv 0 \bmod \mathfrak{l}(u)$, so gilt*

$$\{\det(M) \mid M \in \mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]\,, \mathbb{F}_q(u))\} = \mathbb{F}_\mathfrak{l}{}^*\ .$$

Bemerkung 4.4.12. Das Beispiel $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \tau - h^{q-1}\tau^2)$ mit h aus $\mathbb{F}_q(u)^*$ macht klar, daß sich im obigen Satz die $\mathfrak{l}$-Bewertungen von Δ und $\tilde{\Delta}$ unterscheiden können.

Abschließend geben wir ein Beispiel für eine weder triviale noch maximale Torsionserweiterung im Rang-1 Fall an.

Beispiel 4.4.13. Sei $\mathrm{char}(\mathbb{F}_q) \neq 2$ und $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + u\tau)$. Dann ist $\psi_T(x) = u(x + x^q)$. Da $\mathrm{ggT}(x^q - x, x^q + x) = x$ ist, ist Null die einzige Nullstelle von $x^q + x$ in $\mathbb{F}_q$. Es ist $\frac{x^{q^2}-x}{x^q+x} = (x^q + x)^{q-1} - 1 \in \mathbb{F}_q[x]$, und daher teilt $x^q + x$ das Polynom $x^{q^2} - x$. Damit liegen alle von 0 verschiedenen Nullstellen in $\mathbb{F}_{q^2} - \mathbb{F}_q$. Also zerfällt $\frac{\phi_T(x)}{x}$ in $\mathbb{F}_q(u)[x]$ in quadratische irreduzible Faktoren. Insgesamt erhalten wir

$$\mathbb{F}_q(u)[{}_T\psi] = \mathbb{F}_{q^2}(u) .$$

□

4.5 Differente, Geschlecht, Verzweigung

Um Geschlecht und Verzweigung in der Erweiterung $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)$ zu untersuchen, betrachten wir die zugehörige Differente.
Wir wiederholen kurz die wichtigsten Begriffe, wobei wir uns am Buch [Sti93] orientieren. Seien $L|K$ eine Erweiterung von algebraischen Funktionenkörpern, S_K bzw. S_L die jeweiligen Stellenmengen (inklusive der ∞-Stellen), $P \in S_K$ und $P' \in S_L$. Weiter sei O_P der Ganzheitsring an P, $O'_P = \bigcap_{P'|P} O_{P'}$ der ganze Abschluß von O_P in L und $\mathrm{v}_{P'}$ die Fortsetzung der normierten diskreten Bewertung v_P. Sei weiter $C_P := \{z \in L \mid \mathrm{Tr}_{L|K}(z \cdot O'_P) \subset O_P\}$ der komplementäre Modul und $t \in L$ mit $C_P = t \cdot O'_P$. Dann ist der Differentenexponent

$$d(P', P) := -\mathrm{v}_{P'}(t)$$

wohldefiniert, nichtnegativ und fast immer gleich Null. Weiter definieren wir die Differenten

$$\mathit{Diff}\,(P) := \sum_{P'|P,\ P' \in S_L} d(P', P) \cdot P'$$

und

$$\mathit{Diff}\,(L, K) := \sum_{P \in S_K} \mathit{Diff}\,(P) .$$

Nach dem Dedekindschen Differentensatz gilt für den Verzweigungsindex $e(P', P)$

$$e(P', P) - 1 \leqslant d(P', P) ,$$

wobei Gleichheit genau im Fall zahmer Verzweigung gilt. Daher können wir einerseits mit Hilfe der Differenten die Verzweigung abschätzen. Andererseits können wir sie auch dazu benutzen, mittels der Hurwitz-Formel das Geschlecht abzuschätzen. In diesem Zusammenhang wollen wir daran erinnern, daß für ein $\alpha \in O_P$

$$0 \leqslant \mathrm{v}_{P'}(\alpha) = e(P', P) \cdot \mathrm{v}_P(\alpha) \leqslant [L : K] \cdot \mathrm{v}_P(\alpha)$$

gilt.
Da unsere Erweiterung $\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]|\mathbb{F}_q(u)$ von einem additiven Polynom erzeugt wird, zeigen wir zuerst das folgende Lemma.

Lemma 4.5.1. *Seien die Bezeichnungen wie oben, $p = \mathrm{char}(K)$ und*

$$f(x) = \sum_{i=0}^{n} a_i x^{p^i} \in O_P[x]$$

mit $a_0 \cdot a_n \neq 0$. Weiter sei $\eta \in \overline{K}$ eine Nullstelle von $f(x)$ und $L = K(\eta)$. Dann gilt

$$d(P', P) \leqslant \mathrm{v}_{P'}(a_0 \cdot {a_n}^{p^n - 2}) \ .$$

Beweis: Zuerst transformieren wir f in ein normiertes Polynom.

$$f(\frac{x}{a_n}) = {a_n}^{1-p^n} \sum_{i=0}^{n} a_i {a_n}^{p^n - p^i - 1} x^{p^i} =: {a_n}^{1-p^n} g(x) \ .$$

Da $K(\eta)$ gleich $K(a_n \cdot \eta)$ ist, können wir statt $f(x)$ das normierte Polynom $g(x)$ mit der Nullstelle $\tilde{\eta} = a_n \eta$ betrachten. Ist nun $m(x)$ das Minimalpolynom von $\tilde{\eta}$, so existiert ein $h(x) \in K(x)$ mit $g(x) = h(x) \cdot m(x)$. Da $g(x)$ und $m(x)$ normiert und ganz an P sind, gilt nach dem Lemma von Gauß sogar $h(x) \in O_P(x)$. Dann folgt für die Ableitung

$$a_0 {a_n}^{p^n - 2} = g'(x) = h'(x) m(x) + h(x) m'(x) \ ,$$

und daher

$$a_0 {a_n}^{p^n - 2} = g'(\tilde{\eta}) = h(\tilde{\eta}) m'(\tilde{\eta}) \ .$$

Nach [Sti93, III.5.10] gilt dann

$$d(P', P) \leqslant \mathrm{v}_{P'}(m'(\tilde{\eta})) = \mathrm{v}_{P'}(g'(\tilde{\eta})) - \mathrm{v}_{P'}(h(\tilde{\eta})) \leqslant \mathrm{v}_{P'}(a_0 {a_n}^{p^n - 2}) \ .$$

□

Betrachten wir nun das $\mathfrak{n}$-Torsionspolynom $\phi_\mathfrak{n}(x)$.

Lemma 4.5.2. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$, $\mathfrak{n}(T) \in \mathbb{F}_q[T]$ beliebig und $\phi_\mathfrak{n}(\tau) = \sum_{i=0}^{d} a_i \tau^i$. Dann gilt*

$$d = 2 \deg_T(\mathfrak{n}), \qquad a_0 = \mathfrak{n}(u), \qquad a_d = \Delta^{\frac{q^d - 1}{q^2 - 1}} \ .$$

Beweis: Sei $\mathfrak{n}(T) = \sum_{i=0}^{n} c_i T^i$. Dann gilt

$$\phi_{\mathfrak{n}(T)} = \sum_{i=0}^{n} c_i(u + g\tau + \Delta\tau^2)^i = \sum_{i=0}^{2n} a_i\tau^i \ .$$

Vernachlässigt man die τ-Anteile, so erhält man $a_0 = \sum_{i=0}^{n} c_i u^i$. Der höchste auftretende τ-Grad ist $2n$. Zum Monom τ^{2n} trägt nur der Term $(\Delta\tau^2)^n$ bei. Multiplizieren wir diesen im nichtkommutativen Ring $\mathbb{F}_q(u)\{\tau\}$ aus, so erhalten wir

$$\begin{aligned}
(\Delta\tau^2)^n &= \Delta\tau^2\Delta\tau^2\Delta\tau^2 \ldots \Delta\tau^2\Delta\tau^2 \\
&= \Delta^{1+q^2}\tau^4\Delta\tau^2 \ldots \Delta\tau^2\Delta\tau^2 \\
&= \Delta^{1+q^2+q^4}\tau^6\Delta \ldots \Delta\tau^2\Delta\tau^2 \\
&= \Delta^{1+q^2+q^4+\ldots+q^{2(n-1)}}\tau^{2n} \\
&= \Delta^{\frac{q^{2n}-1}{q^2-1}}\tau^{2n} \quad .
\end{aligned}$$

Damit ist das Lemma gezeigt. □

Wir können nun die Differente an den endlichen Stellen von $\mathbb{F}_q(u)$ wie folgt abschätzen.

Satz 4.5.3. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$, $\mathfrak{P}$ eine Stelle von $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$, die $\mathfrak{p}(u)$ teilt. Weiter sei $\phi = \min(\phi)$ und damit g und Δ aus $\mathbb{F}_q[u]$. Dann gilt*

$$d(\mathfrak{P}, \mathfrak{p}) \leqslant 2\ e(\mathfrak{P}, \mathfrak{p}) \cdot \left(\mathrm{v}_{\mathfrak{p}}(\mathfrak{l}(u)) + \frac{(q^{2\deg_T \mathfrak{l}} - 2)(q^{2\deg_T \mathfrak{l}} - 1)}{q^2 - 1} \mathrm{v}_{\mathfrak{p}}(\Delta) \right) \ .$$

Beweis: Wir wählen eine Basis $\{\lambda_1, \lambda_2\}$ des 2-dimensionalen $\mathbb{F}_{\mathfrak{l}}$-Vektorraums ${}_{\mathfrak{l}}\phi = {}_{\mathfrak{l}}\min(\phi)$ und betrachten die Erweiterungen $\mathbb{F}_q(u)(\lambda_1)|\mathbb{F}_q(u)$ und $\mathbb{F}_q(u)(\lambda_1, \lambda_2)|\mathbb{F}_q(u)(\lambda_1)$. Auf beide können wir Lemma 4.5.1 und Lemma 4.5.2 anwenden. Da $\mathbb{F}_q(u)(\lambda_1, \lambda_2) = \mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$ ist, erhalten wir aus der Transitivität der Differente in Körpertürmen die Ungleichung

$$d(\mathfrak{P}, \mathfrak{p}) \leqslant 2 \left(\mathrm{v}_{\mathfrak{P}}(\mathfrak{l}(u)) + \frac{(q^{2\deg_T \mathfrak{l}} - 2)(q^{2\deg_T \mathfrak{l}} - 1)}{q^2 - 1} \mathrm{v}_{\mathfrak{P}}(\Delta) \right) \quad .$$

Für alle $\alpha \in \mathbb{F}_q(u)$ gilt $\mathrm{v}_{\mathfrak{P}}(\alpha) = e(\mathfrak{P}, \mathfrak{p}) \cdot \mathrm{v}_{\mathfrak{p}}(\alpha)$, und damit folgt die Aussage. □

Korollar 4.5.4. *In $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)$ sind höchstens die ∞-Stelle und die Teiler von $\mathfrak{l}(u) \cdot \Delta$ verzweigt.*

Beweis: Nach dem Dedekindschen Differentensatz kommen alle verzweigten Stellen in der Differente *Diff* $(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]|\mathbb{F}_q(u))$ vor. Die Anteile zu den endlichen Stellen können wir durch den obigen Satz nach oben abschätzen, und zur ∞-Stelle haben wir bisher keine Aussage gemacht. □

Bemerkung 4.5.5. (i) Die obigen Beweise und die Aussage 4.5.4 übertragen sich direkt auf beliebige Rang-r Drinfeld-Moduln $(\mathbb{F}_q, \mathbb{F}_q(u), u, u + \sum_{i=1}^r c_i\ \tau^i)$.

(ii) Die im Korollar 4.5.4 angegebenen Stellen müssen nicht verzweigt sein. Zum Beispiel ist die T-Torsionserweiterung des Drinfeld-Moduls $(\mathbb{F}_q, \mathbb{F}_q(u), u, u + \sum_{i=1}^r u\ \tau^i)$ eine Konstantenerweiterung, und daher ist keine Stelle verzweigt.

In vielen Fällen können wir die verzweigten Stellen genauer angeben.

Satz 4.5.6. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul und $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$. Hat ϕ gute Reduktion an $\mathfrak{l}(u)$, so sind die endlichen verzweigten Stellen in $\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]|\mathbb{F}_q(u)$ genau*

$$\{\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]} \mid \phi \textit{ hat keine gute Reduktion an } \mathfrak{p}\} \cup \{\mathfrak{l}(u)\} \quad .$$

Beweis: Es sei o.B.d.A. $\phi = \min(\phi)$, d.h., die Stellen schlechter Reduktion seien genau die Teiler von Δ. Nach [Tak82] ist die Menge der endlichen verzweigten Stellen ungleich $\mathfrak{l}(u)$ genau

$$\{\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]} \mid \phi \text{ hat keine gute Reduktion an } \mathfrak{p}\} \quad .$$

Es ist also noch die Stelle $\mathfrak{l}(u)$ zu untersuchen. Dazu betrachten wir den assoziierten Rang-1 Modul

$$\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau) \quad .$$

Dann gilt nach Korollar 4.4.4

$$\mathbb{F}_q(u) \subseteq \mathbb{F}_q(u)[{}_\mathfrak{l}\psi] \subseteq \mathbb{F}_q(u)[{}_\mathfrak{l}\phi] \quad .$$

Da $\mathrm{ggT}(\mathfrak{l}, \Delta) = 1$ ist, hat das Polynom $\psi_\mathfrak{l}(x) \in \mathbb{F}_q(u)[x]$ an $\mathfrak{l}$ das gleiche Newton-Polygon wie $\gamma_\mathfrak{l}(x)$, wobei $\gamma = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \tau)$ den Carlitz-Modul bezeichnet. Damit erhält man mit den gleichen Argumenten wie in [Hay74], daß $\mathfrak{l}(u)$ in $\mathbb{F}_q(u)[{}_\mathfrak{l}\psi]|\mathbb{F}_q(u)$ voll verzweigt ist. Daher ist $\mathfrak{l}(u)$ auch in $\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]|\mathbb{F}_q(u)$ verzweigt. □

Die ∞-Stelle kann sowohl verzweigt als auch unverzweigt sein, wie die folgenden beiden Beispiele zeigen.

Beispiel 4.5.7. Der Rang-2 Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau - \tau^2)$ besitzt als assoziierten Rang-1 Modul den Carlitz-Modul $\gamma = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \tau)$. Da für jedes $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ die ∞-Stelle in $\mathbb{F}_q(u)[{}_\mathfrak{l}\gamma]|\mathbb{F}_q(u)$ verzweigt ist, ist ∞ auch in jeder Erweiterung $\mathbb{F}_q(u)[{}_\mathfrak{l}\phi]|\mathbb{F}_q(u)$ verzweigt. □

Beispiel 4.5.8. Wir können bestimmte Kummererweiterungen als T-Torsions-Erweiterungen interpretieren. Dazu betrachten wir das Polynom

$$f(x) = x^{q^2-1} - a\sum_{i=1}^{s} \mathfrak{p}_i(u)^{n_i} \in \mathbb{F}_q(u)[x] \quad .$$

Dabei sei $a \in \mathbb{F}_q{}^*$, $s \geqslant 1$, und die $\mathfrak{p}_i(u)$ seien paarweise verschiedene, irreduzible und normierte Polynome. Weiter sei $\mathrm{ggT}(q^2-1, n_i) = 1$ für alle $1 \leqslant i \leqslant s$, und es gelte

$$\mathrm{ggT}\left(\sum_{i=1}^{s} n_i \cdot \deg_u(\mathfrak{p}_i)\ ,\ q^2-1\right) = q^2-1 \quad .$$

Sei η eine Nulstelle von $f(x)$. Da $\mathbb{F}_{q^2}$ der Zerfällungskörper des Polynoms $x^{q^2-1} - 1 \in \mathbb{F}_q[x]$ ist, ist

$$\mathrm{ZerfKp}(f) = \mathbb{F}_{q^2}(u, \eta) \quad .$$

In der Konstantenerweiterung $\mathbb{F}_{q^2}(u)|\mathbb{F}_q(u)$ ist ∞ unverzweigt. Nach [Sti93, Prop. VI.3.1.] gilt dies auch für die Erweiterung $\mathbb{F}_{q^2}(u,\eta)|\mathbb{F}_{q^2}(u)$. Also ist die ∞-Stelle im Zerfällungskörper von $f(x)$ unverzweigt. Schreiben wir nun mit $\mathfrak{n}(u) := a\sum_{i=1}^{s} \mathfrak{p}_i(u)^{n_i}$

$$f(x) = \frac{\mathfrak{n}(u)}{ux}\left(\frac{u}{\mathfrak{n}(u)}x^{q^2} - ux\right) \quad ,$$

so erhälten wir, daß die T-Torsionserweiterung des Moduls

$$\phi = \left(\mathbb{F}_q, \mathbb{F}_q(u), u, u - \frac{u}{\mathfrak{n}(u)}\tau^2\right)$$

an der ∞-Stelle unverzweigt ist. Je nach Wahl der $\mathfrak{p}_i(u)^{n_i}$ hat ϕ gute oder schlechte Reduktion an T.
Wählen wir $\mathfrak{n}$ so, daß

$$\mathrm{ggT}(\deg_u(\mathfrak{n}), q^2-1) = \mathrm{ggT}\left(\sum_{i=1}^{s} n_i \cdot \deg_u(\mathfrak{p}_i)\ ,\ q^2-1\right) \neq q^2-1$$

ist, dann liefert die obige Konstruktion Drinfeld-Moduln, in deren T-Torsionserweiterungen ∞ verzweigt. $\square$

Die ∞-Stelle macht uns auch bei der Berechnung der Differenten Probleme, da dort wilde Verzweigung auftreten kann. Dies illustriert das folgende Beispiel von Taguchi aus [Tag92], dessen Hauptaussagen wir hier ohne Beweis wiedergeben.

Beispiel 4.5.9. Sei $n \in \mathbb{N}$ und

$$\phi^{(n)} := (\mathbb{F}_q, \mathbb{F}_q(u), u, u + u^{n(q^2-q)-1}\tau + \tau^2) \ .$$

Dann ist die Erweiterung $\mathbb{F}_q(u)[_T\phi^{(n)}]|\mathbb{F}_q(u)$ an der ∞-Stelle wild verzweigt, und für eine Stelle ∞' über ∞ ist $d(\infty', \infty) \geqslant n$. Die Differente an ∞ wird also mit wachsendem n beliebig groß, obwohl $\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi^{(n)}], \mathbb{F}_q(u))$ immer eine Untergruppe von $\mathrm{GL}(2, \mathbb{F}_q)$ ist. Es ist also nicht möglich, die Differente durch den Grad der Erweiterung abzuschätzen. $\square$

Im gleichen Artikel [Tag92] zeigt Taguchi, daß für einen festen Drinfeld-Modul ϕ und eine fest gewählte Stelle $\mathfrak{l}(T)$ die Differente $\mathit{Diff}\,(P_\infty)$ im unendlichen Körperturm

$$\mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \subset \mathbb{F}_q(u)[_{\mathfrak{l}^2}\phi] \subset \ldots \subset \mathbb{F}_q(u)[_{\mathfrak{l}^i}\phi] \subset \ldots$$

unabhängig von $i \in \mathbb{N}$ beschränkt ist. Allerdings folgt diese Schranke aus der analytischen Beschreibung des Drinfeld-Moduls und ist nicht ohne weiteres explizit berechenbar.
Wir wollen nun die Differente an der ∞-Stelle analog zu den endlichen Stellen abschätzen. Dabei haben wir das Problem, daß das Polynom $\phi_{\mathfrak{l}}(x) \in \mathbb{P}_{\mathbb{F}_q[T]}[x]$ dort nicht ganz ist. Um es passend zu transformieren, benötigen wir das folgende Lemma.

Lemma 4.5.10. *Sei K ein globaler Körper, $\mathfrak{p} \in S_K$, $\beta \in K$ mit $\mathrm{v}_{\mathfrak{p}}(\beta) = 1$, $h : \mathbb{N}_0 \to \mathbb{N}$ eine beliebige Funktion und $f(x) = \sum_{i=0}^n a_i x^{h(i)}$. Ist dann*

$$t := \left\lceil \max\left\{ -\frac{\mathrm{v}_{\mathfrak{p}}(a_i)}{h(i)} \mid i = 0, \ldots, n \right\} \right\rceil ,$$

so gilt

$$f(\beta^t x) \in O_{\mathfrak{p}}[x] .$$

Für ein $\alpha \in \mathbb{R}$ bezeichnet $\lceil \alpha \rceil := \min\{z \in \mathbb{Z} \mid \alpha \leqslant z\}$ die Gaußklammer.

Beweis: Die Aussage folgt aus den folgenden Äquivalenzen:

$$\begin{aligned} f(\beta^t x) \in O_{\mathfrak{p}}[x] \quad &\Longleftrightarrow \quad \sum_{i=0}^n a_i \beta^{t \cdot h(i)} x^{h(i)} \in O_{\mathfrak{p}}[x] \\ &\Longleftrightarrow \quad \mathrm{v}_{\mathfrak{p}}(a_i \beta^{t \cdot h(i)}) \geqslant 0 \quad \forall 0 \leqslant i \leqslant n \\ &\Longleftrightarrow \quad t \geqslant -\frac{\mathrm{v}_{\mathfrak{p}}(a_i)}{h(i)} \qquad \forall 0 \leqslant i \leqslant n \end{aligned}$$

□

Nun können wir die Differente an der ∞-Stelle abschätzen.

Satz 4.5.11. *Seien die Bezeichnungen wie in Satz 4.5.3, $n := 2\deg_T(\mathfrak{l})$ und*

$$\phi_{\mathfrak{l}}(x) = \sum_{i=0}^n a_i \; x^{q^i} \in \mathbb{F}_q[u][x] .$$

Weiter sei ∞' eine Stelle von $\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]$ über ∞. Dann gilt

$$d(\infty', \infty) \leqslant 2 \; e(\infty', \infty) \left(\mathrm{v}_\infty(\mathfrak{l}(u)) + \frac{(q^n-2)(q^n-1)}{q^2-1} \mathrm{v}_\infty(\Delta) + t(q^n-1)^2 \right)$$

mit

$$t := \left\lceil \max\left\{ -\frac{\mathrm{v}_\infty(a_i)}{q^i} \mid i = 0, \ldots, \; n \right\} \right\rceil .$$

Beweis: Wir werden wie an den endlichen Stellen argumentieren. Dazu muß allerdings $\phi_{\mathfrak{l}}(x)$ erst in ein Polynom aus $O_\infty[x]$ transformiert werden. Dazu verwenden wir das Lemma 4.5.10 mit $h(i) = q^i$ und $\beta = \frac{1}{u}$. Dann ergibt sich t als $t = \lceil \max\{-\frac{\mathrm{v}_\infty(a_i)}{q^i} \mid i = 0, \ldots, 2\deg_T(\mathfrak{l})\}\rceil$, und wir betrachten im weiteren das Polynom

$$g(x) := \phi_{\mathfrak{l}}(u^{-t}x) = \sum_{i=0}^{2\deg_T(\mathfrak{l})} a_i u^{-t\cdot q^i}\, x^{q^i} \in O_\infty[x]\ ,$$

das den gleichen Zerfällungskörper wie $\phi_{\mathfrak{l}}(x)$ hat. Mit Lemma 4.5.2 erhalten wir für $i = 0$

$$a_0 \cdot u^{-t} = \mathfrak{l}(u) \cdot u^{-t}$$

und für $i = n = 2\deg_T(\mathfrak{l})$

$$a_n \cdot u^{-t\cdot q^n} = \Delta^{\frac{q^n-1}{q^2-1}} \cdot u^{-t\cdot q^n}\ .$$

Wie im Beweis von Satz 4.5.3 folgt daraus

$$\begin{aligned} d(\infty', \infty) &\leqslant 2\ e(\infty', \infty) \cdot \mathrm{v}_\infty\left(\mathfrak{l}(u) \cdot u^{-t} \cdot \left(\Delta^{\frac{q^n-1}{q^2-1}} \cdot u^{-t\cdot q^n}\right)^{q^n-2}\right) \\ &= 2\ e(\infty', \infty)\left(\mathrm{v}_\infty(\mathfrak{l}(u)) + \frac{(q^n-2)(q^n-1)}{q^2-1}\mathrm{v}_\infty(\Delta) - t\ \mathrm{v}_\infty(u)\ (1 + (q^n-2)q^n)\right) \\ &= 2\ e(\infty', \infty)\left(\mathrm{v}_\infty(\mathfrak{l}(u)) + \frac{(q^n-2)(q^n-1)}{q^2-1}\mathrm{v}_\infty(\Delta) + t(q^n-1)^2\right) \qquad . \end{aligned}$$

□

Bemerkung 4.5.12. Es ist offensichtlich, daß für $t = 0$ die obige Formel mit der Abschätzung aus Satz 4.5.3 übereinstimmt. Außerdem ist $-\frac{\mathrm{v}_\infty(a_0)}{q^0} = -\mathrm{v}_\infty(\mathfrak{l}(u)) \geqslant 0$. Damit ist der Wert von t immer nichtnegativ.

Wir können nun daran gehen, den Grad der Differenten abzuschätzen.

Lemma 4.5.13. *Seien die Bezeichnungen wie oben, $K = \mathbb{F}_q(u)$, $L = \mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$, $\mathfrak{p} \in S_K$, und $\mathfrak{P}$ bezeichne Stellen von L über $\mathfrak{p}$. Dann gilt*

$$\sum_{\mathfrak{P}|\mathfrak{p}} d(\mathfrak{P}, \mathfrak{p}) \deg(\mathfrak{P}) \leqslant \begin{cases} 2\,[L:K]\left(\mathrm{v}_\infty(\mathfrak{l}(u)) + \frac{(q^n-2)(q^n-1)}{q^2-1}\mathrm{v}_\infty(\Delta)\right) & ;\ \mathfrak{p} \mid \mathfrak{l}\cdot\Delta \\ 2\,[L:K]\left(\mathrm{v}_\infty(\mathfrak{l}(u)) + \frac{(q^n-2)(q^n-1)}{q^2-1}\mathrm{v}_\infty(\Delta) + t(q^n-1)^2\right) & ;\ \mathfrak{p} = \infty \\ 0 & ;\ \textit{sonst} \end{cases}\ .$$

Beweis: Da $L|K$ galoissch ist, sind $e(\mathfrak{P}, \mathfrak{p})$, $\deg(\mathfrak{P}) = f(\mathfrak{P}, \mathfrak{p})$ und $d(\mathfrak{P}, \mathfrak{p})$ unabhängig von der Wahl der Stelle über $\mathfrak{p}$. Daher kürzen wir die Indizes durch $e(\mathfrak{p})$, $f(\mathfrak{p})$ und $d(\mathfrak{p})$ ab. Weiter bezeichne $g(\mathfrak{p})$ die Anzahl der Stellen von L über $\mathfrak{p}$. Dann gilt

$$\sum_{\mathfrak{P}|\mathfrak{p}} d(\mathfrak{P}, \mathfrak{p}) \deg(\mathfrak{P}) = \sum_{\mathfrak{P}|\mathfrak{p}} d(\mathfrak{p}) \frac{[L:K]}{g(\mathfrak{p})e(\mathfrak{p})} = [L:K]\frac{d(\mathfrak{p})}{e(\mathfrak{p})}\ .$$

Mit den Sätzen 4.5.3 und 4.5.11 folgt nun die Aussage. □

Satz 4.5.14. *Mit dem obigen Lemma können wir den Grad der Differenten*

$$\deg\left(\mathit{Diff}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi],\mathbb{F}_q(u))\right) = \sum_{\mathfrak{p}\mid\mathfrak{l}(u)\cdot\Delta(u)} \left(\sum_{\mathfrak{P}\mid\mathfrak{p}} d(\mathfrak{P},\mathfrak{p})\deg(\mathfrak{P})\right) + \sum_{\infty'\mid\infty} d(\infty',\infty)\deg(\infty')$$

explizit nach oben abschätzen.

Nun können wir mit Hilfe der Hurwitz-Formel das Geschlecht der Torsionserweiterung abschätzen.

Satz 4.5.15. *Seien die Bezeichnungen wie oben und $g(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi])$ das Geschlecht des Funktionenkörpers. Dann gilt*

$$g(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]) \leqslant 1 + \frac{1}{2}\deg\left(\mathit{Diff}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi],\mathbb{F}_q(u))\right),$$

wobei der Grad der Differenten durch die Resultate von oben explizit nach oben abgeschätzt werden kann.

Beweis: Nach der Hurwitz-Formel ist

$$g(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]) = 1 + \frac{[\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]:\mathbb{F}_q(u)]}{[F:\mathbb{F}_q]}(g(\mathbb{F}_q(u))-1) + \frac{1}{2}\deg\left(\mathit{Diff}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi],\mathbb{F}_q(u))\right),$$

wobei F den Konstantenkörper von $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$ bezeichnet. Da der rationale Funktionenkörper Geschlecht Null hat, folgt daraus bereits die Aussage. □

Bemerkung 4.5.16. Die obige Abschätzung des Geschlechts ist sehr grob. Einerseits können wir nicht genau sagen, welchen Fehler wir bei der Abschätzung der Differenten machen. Andererseits ist die Abschätzung des Quotienten $\frac{[\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]:\mathbb{F}_q(u)]}{[F:\mathbb{F}_q]}$ sehr ungenau. Wir haben ihn nämlich gegen Null abgeschätzt und werden später sehen (vgl. Satz 4.6.4), daß in den meisten Fällen

$$\frac{[\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]:\mathbb{F}_q(u)]}{[F:\mathbb{F}_q]} = \#\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}}) \approx q^{4\deg_T(\mathfrak{l})} \gg 0$$

gilt.

4.6 Konstantenerweiterung

Wir werden nun den vollen Konstantenkörper von $\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]$ untersuchen.
Im ganzen Abschnitt gelten die folgenden Bezeichnungen:
$g, \Delta \in \mathbb{F}_q(u)$, $\Delta \neq 0$, $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$, $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau)$, $\tilde{\psi} = \min(\psi) = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \tilde{\Delta}\tau)$, $\gamma = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \tau)$ der Carlitz-Modul, $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$, K_ϕ der volle Konstantenkörper von $\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]$ und K_ψ der volle Konstantenkörper von $\mathbb{F}_q(u)[_{\mathfrak{l}}\psi]$.
Eine qualitative Beschreibung der Konstantenerweiterungen liefert das folgende Lemma aus [Dav01].

Lemma 4.6.1. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + a_1\tau + \ldots + a_r\tau^r)$ ein Rang-r Drinfeld-Modul,* Tors $= \{\alpha \in \overline{\mathbb{F}_q(u)} \mid \exists \mathfrak{n} \in \mathbb{F}_q[T]$ *mit* $\phi_{\mathfrak{n}}(\alpha) = 0\}$ *und* $\mathbb{F}_{\text{Tors}}$ *der volle Konstantenkörper von* $\mathbb{F}_q(u)(\text{Tors})$. *Dann gilt*

$$[\mathbb{F}_{\text{Tors}} : \mathbb{F}_q] < \infty \quad .$$

Zum Beweis: Die Aussage folgt aus der analytischen Beschreibung von Drinfeld-Moduln durch Gitter, auf die wir hier nicht eingehen wollen. Daher sei auf die Arbeit [Dav01] verwiesen. □

Das Lemma legt nahe, daß im allgemeinen in $\mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)$ keine Konstantenerweiterung auftreten sollte. Allerdings liefert der Beweis des Lemmas kein einfaches Kriterium, um zu entscheiden, ob bei fest gewähltem ϕ und $\mathfrak{l}$ eine Konstantenerweiterung vorliegt.
Im folgenden werden wir daher die konkrete Situation etwas genauer beleuchten. Dazu benutzen wir, daß zu Konstantenerweiterungen normale Untergruppen von $\text{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$ korrespondieren. Außerdem sind Konstantenerweiterungen abelsch, so daß diese normalen Untergruppen den Kommutator der Galoisgruppe enthalten müssen. Da $\text{GL}(2, \mathbb{F}_l)$ nur sehr wenige Normalteiler enthält und wir den Kommutator leicht angeben können, erhalten wir im Fall $\text{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \text{GL}(2, \mathbb{F}_l)$ starke Einschränkungen an ϕ, falls eine Konstantenerweiterung vorliegt.
Diesen Ansatz fassen wir nochmal in dem folgenden Lemma zusammen.

Lemma 4.6.2. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + a_1\tau + \ldots + a_r\tau^r)$ ein Rang-r Drinfeld-Modul,* $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$ *und* Kom *der Kommutator von* $\text{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$. *Dann gilt*

$$\text{Kom} \quad \trianglelefteq \quad \text{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], K_\phi(u)) \quad \trianglelefteq \quad \text{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) \quad .$$

Damit können wir den Grad der Konstantenerweiterung durch

$$\begin{aligned}
[K_\phi : \mathbb{F}_q] \quad &\leqslant \quad \max\{[\text{Gal} : N] \mid N \trianglelefteq \text{Gal}, {}^{\text{Gal}}/_{N} \text{ abelsch } \} \\
&\leqslant \quad \max\{[U : N] \mid U \leqslant \text{GL}(2, \mathbb{F}_{\mathfrak{l}}), N \trianglelefteq U, {}^{U}/_{N} \text{ abelsch } \}
\end{aligned}$$

abschätzen, wobei Gal für $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$ steht. Wählt man für U eine nichtzerfallende Cartanuntergruppe und $N = \{1\}$, so erhält man

$$q^{2\deg_T(\mathfrak{l})} - 1 \leqslant \max\{[U : N] \mid U \leqslant \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}), N \trianglelefteq U, {}^{U}/_{N} \text{ abelsch } \} \ .$$

Es ist zu vermuten, daß in der obigen Ungleichung sogar Gleichheit gilt. Das folgende Lemma liefert die Kommutatoren der $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$.

Lemma 4.6.3. *Es gilt:*

$$\mathrm{Kom}(\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})) = \mathrm{SL}(2, \mathbb{F}_{\mathfrak{l}}) \iff \mathbb{F}_{\mathfrak{l}} \neq \mathbb{F}_2$$

Beweis:

(i) '$\Leftarrow$': Für $\#\mathbb{F}_{\mathfrak{l}} > 3$ ist die Aussage in [Hup67, S.181] zu finden. Im Fall von $\mathrm{GL}(2, \mathbb{F}_3)$ berechnet man (z.B. unter Verwendung eines Computer-Algebra-Systems), daß $\#\{A^{-1}B^{-1}AB \mid A, B \in \mathrm{GL}(2, \mathbb{F}_3)\} = 24$ ist. Da der Kommutator in der $\mathrm{SL}(2, \mathbb{F}_3)$ enthalten sein muß und $\#\mathrm{SL}(2, \mathbb{F}_3) = 24$ ist, folgt $\mathrm{Kom}(\mathrm{GL}(2, \mathbb{F}_3)) = \mathrm{SL}(2, \mathbb{F}_3)$.

(ii) '$\Rightarrow$': Es ist $\mathrm{GL}(2, \mathbb{F}_2) = \mathrm{SL}(2, \mathbb{F}_2) \cong \mathrm{S}_3$, und diese Gruppe hat den abelschen Quotienten $\mathbb{Z}/2\mathbb{Z}$.

□

Damit erhalten wir für maximale Erweiterungen das folgende Resultat.

Satz 4.6.4. *Seien die Bezeichnungen wie auf Seite 81, $q^{\deg_T(\mathfrak{l})} \neq 2$ und $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$. Dann gilt für die Konstantenkörper*

$$K_\phi = K_\psi \ .$$

Beweis: Wegen der Maximalität der Erweiterung ist $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)[{}_{\mathfrak{l}}\psi]) = \mathrm{SL}(2, \mathbb{F}_{\mathfrak{l}})$. Weiter ist nach unseren obigen Überlegungen $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], K_\phi(u))$ ein Normalteiler, der den Kommutator von $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ enthält. Nach Lemma 4.6.3 ist der Kommutator genau $\mathrm{SL}(2, \mathbb{F}_{\mathfrak{l}})$. Insgesamt erhalten wir $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)[{}_{\mathfrak{l}}\psi]) \leqslant \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], K_\phi(u))$ bzw. $K_\phi(u) \subset \mathbb{F}_q(u)[{}_{\mathfrak{l}}\psi]$. Damit ist die Aussage gezeigt. □

In Satz 4.4.10 haben wir bereits die Konstantenerweiterungen von Rang-1 Drinfeld-Moduln untersucht und erhalten daraus den folgenden Satz.

Satz 4.6.5. *Seien die Bezeichnungen wie auf Seite 81, $q^{\deg_T(\mathfrak{l})} \neq 2$, $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ und $\tilde{\Delta} \not\equiv 0 \bmod \mathfrak{l}(u)$. Dann gilt*

$$K_\phi = \mathbb{F}_q \ .$$

Über den Fall

$$\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi]\,,\mathbb{F}_q(u)) \neq \mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})$$

können wir nicht viel aussagen. Daher beenden wir den Abschnitt mit einigen Beispielen, die verdeutlichen, welche Phänomene auftreten können.

Beispiel 4.6.6. Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + u\,\alpha\tau + u\,\beta\tau^2)$ mit $\alpha \in \mathbb{F}_q$, $\beta \in {\mathbb{F}_q}^*$. Dann ist $\mathbb{F}_q(u)[_T\phi]|\mathbb{F}_q(u)$ eine Konstantenerweiterung, also $\mathbb{F}_q(u)[_T\phi] = K_\phi(u)$. Da Konstantenerweiterungen abelsch sind, ist in diesen Fällen immer $\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,,\mathbb{F}_q(u)) \neq \mathrm{GL}(2,\mathbb{F}_T)$. Unter Verwendung der Theorie q-linearer Polynome über $\mathbb{F}_q$ (vgl. [LN94, Theorem 3.63]) läßt sich zeigen, daß $[\mathbb{F}_q(u)[_T\phi] : \mathbb{F}_q(u)]$ ein Teiler von $q^2 - 1$ ist. □

Beispiel 4.6.7. Wir betrachten nun ein Beispiel, das sowohl als Drinfeld-Modul mit komplexer Multiplikation als auch als Kummererweiterung interpretiert werden kann. Dabei handelt es sich um eine Verallgemeinerung von Beispiel 1.7.4 von $\mathbb{F}_3$ zu $\mathbb{F}_q$. Wir werden sehen, wie sich in diesem Beispiel unsere Strukturaussagen über Drinfeld-Moduln in bekannte Aussagen über Kummererweiterungen (vgl. [Sti93]) übersetzen. Wir betrachten den Drinfeld-Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \tau^2)$ und seine T-Torsion, d.h., wir untersuchen den Zerfällungskörper des Polynoms $\phi_T(x) = ux - x^{q^2} \in \mathbb{F}_q(u)[x]$. Sei η eine fest gewählte Nullstelle von $x^{q^2-1} - u$ und $\lambda \in \mathbb{F}_{q^2}$ mit $\mathbb{F}_{q^2}^* = \langle\lambda\rangle$. Dann ist $_T\phi = \{\lambda^i\eta \mid 0 \leqslant i < q^2 - 1\} \cup \{0\}$. Kummertheorie liefert uns, daß $\mathbb{F}_q(u)[_T\phi] = \mathbb{F}_{q^2}(\eta)$ ist. Insbesondere ist $\mathbb{F}_{q^2}$ der volle Konstantenkörper der Torsionserweiterung. Die Galoisgruppe ergibt sich zu

$$\begin{aligned}\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,,\mathbb{F}_q(u)) =& \langle \begin{pmatrix} \eta & \mapsto & \lambda\cdot\eta \\ \lambda & \mapsto & \lambda \end{pmatrix} , \begin{pmatrix} \eta & \mapsto & \eta \\ \lambda & \mapsto & \lambda^q \end{pmatrix} \rangle \\ =& \langle \alpha, \beta \mid \beta^2 = \alpha^{q^2-1} = 1\ ,\ \alpha\beta = \beta\alpha^q \rangle \quad .\end{aligned}$$

Mit der Theorie der Drinfeld-Moduln erhalten wir folgendes: Der Drinfeld-Modul ϕ hat komplexe Multiplikation durch $\mathbb{F}_{q^2}[T]$. Da $\mathbb{F}_q(u)[_T\phi]$ den Körper $\mathbb{F}_{q^2}(u)$ enthält, folgt aus Satz 4.3.3, daß

$$\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,,\mathbb{F}_q(u)) \leqslant \mathrm{Norm}(\mathfrak{T})$$

und

$$\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,,\mathbb{F}_q(u)) \not\leqslant \mathfrak{T}$$

ist. Da

$$\mathrm{Norm}(\mathfrak{T}) \cong \langle \alpha, \beta \mid \alpha^{q^2-1} = 1 = \beta^2,\ \alpha\beta = \beta\alpha^q \rangle$$

ist (s. Seite 46), stimmt dies mit dem Ergebnis aus der Kummertheorie überein. Weiter ist der ϕ zugeordnete Rang-1 Modul der Carlitz-Modul $\gamma = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + \tau)$, und daher ist

$$\mathrm{Gal}(\mathbb{F}_q(u)[_T\gamma]\,,\mathbb{F}_q(u)) \cong {\mathbb{F}_q}^*$$

und

$$\mathbb{F}_q(u)[{}_T\gamma] \cap \mathbb{F}_{q^2} = \mathbb{F}_q \ .$$

Wir fassen die Situation in einem Diagramm zusammen.

$$\begin{tikzcd}
& \mathbb{F}_q(u)[{}_T\phi] \arrow[dl, dash, "\mathrm{Norm}(\mathfrak{T}) \cap \mathrm{SL}(2, \mathbb{F}_T)"'] \arrow[dr, dash, "\mathfrak{T} \cong \langle\alpha\rangle"] & \\
\mathbb{F}_q(u)[{}_T\gamma] \arrow[dr, dash, "{\mathbb{F}_T}^*"'] & & \mathbb{F}_{q^2}(u) \arrow[dl, dash, "\langle\beta\rangle \cong \langle x \mapsto x^q\rangle \cong \mathrm{Norm}(\mathfrak{T})/\mathfrak{T}"] \\
& \mathbb{F}_q(u) &
\end{tikzcd}$$

Es sei nochmal darauf hingewiesen, daß in diesem Beispiel

$$K_\psi = \mathbb{F}_q \quad \text{und} \quad K_\phi \neq \mathbb{F}_q$$

gilt. □

4.7 Die verzweigten Stellen

Wir werden nun Informationen über Elemente der Galoisgruppe gewinnen, indem wir die endlichen verzweigten Stellen untersuchen. Diese unterteilen sich nach Korollar 4.5.4 in die Stellen, an denen der Drinfeld-Modul schlechte Reduktion hat, und die Stelle $\mathfrak{l}(u)$, die als Bild des Führers unter i_ϕ auftritt.
Wenden wir uns zuerst den Stellen schlechter Reduktion zu. Indem wir den entsprechenden Beweis für elliptische Kurven (vgl. [Sil94, Kapitel V]) auf Drinfeld-Moduln übertragen, können wir in vielen Fällen zeigen, daß nicht-halbeinfache Matrizen in der Galoisgruppe einer Torsionserweiterung liegen. Die Hauptingredienzen des Beweises sind von Bae und Kang in den Arbeiten [BK92], [BK93], [Bae95a] bewiesen worden. In diesen Arbeiten haben sie die Theorie der in [Gek88] definierten Tate-Drinfeld-Moduln ausgearbeitet. Wir stellen hier kurz die zentralen Ergebnisse zusammen.
Sei $K|\mathbb{F}_q$ ein lokaler Funktionenkörper mit normierter Bewertung $\mathrm{v} : K \to \mathbb{Z} \cup \{\infty\}$, O_K der Ganzheitsring und $|\cdot|$ die zugehörige Norm. Diese kann eindeutig auf den algebraischen Abschluß $\bar{K}$ fortgesetzt werden.
Weiter sei K durch den injektiven $\mathbb{F}_q$-Algebren-Homomorphismus $i : \mathbb{F}_q[T] \to K$ ein $\mathbb{F}_q[T]$-Körper, und für das Bild gelte $\mathrm{Bild}(i) \subseteq O_K$. Es seien

$$\gamma := (\mathbb{F}_q, K, i(T), i(T) + \tau)$$

der Carlitz-Modul und $s, t \in \bar{K}$ mit $t^{q-1} = s$ und $|s| < 1$.
Die Koeffizienten g und Δ des generischen Rang-2 Drinfeld-Moduls können als formale Potenzreihen mit Koeffizienten in $i(\mathbb{F}_q[T])$ in einem formalen Parameter t, der Uniformisierenden der Spitze ∞ (vgl. [Gek88]) aufgefaßt werden. Einsetzen von $t \in \bar{K}$ wie oben liefert den Drinfeld-Modul

$$\phi^{\langle s\rangle} := (\mathbb{F}_q, K, i(T), i(T) + g(t)\tau + \Delta(t)\tau^2) \quad ,$$

den *Tate-Drinfeld-Modul* zu s. Dieser ist wohldefiniert, da nach [Gek88, Abschnitt 6] die Werte $g(t), \Delta(t)$ in K liegen und unabhängig von der Wahl der Nullstelle von $Y^{q-1} - s \in K[Y]$ sind. Für einen Tate-Drinfeld-Modul gilt immer $|j(\phi^{\langle s\rangle})| = |s|^{-1}$.
Durch

$$e_t(z) := z \cdot \prod_{\mathfrak{m} \in \mathbb{F}_q[T]-\{0\}} (1 - \frac{z}{\gamma_{\mathfrak{m}}(t^{-1})})$$

wird eine Funktion auf ganz $\bar{K}$ definiert.
Diese Funktion ist ein $\mathbb{F}_q[T]$-Modul-Homomorphismus des $*_\gamma$-Moduls $\bar{K}$ in den $*_{\phi^{\langle s\rangle}}$-Modul $\bar{K}$, d.h., für alle $\alpha, \beta \in \bar{K}$, $\mathfrak{m} \in \mathbb{F}_q[T]$ gilt

$$\begin{aligned} e_t(\alpha + \beta) &= e_t(\alpha) + e_t(\beta) \\ e_t(\mathfrak{m} *_\gamma \alpha) &= \mathfrak{m} *_{\phi^{\langle s\rangle}} e_t(\alpha) \quad . \end{aligned}$$

Der Kern von e_t ist

$$D_t := \mathbb{F}_q[T] *_\gamma t^{-1} \quad .$$

Zu einem beliebigen nichtkonstanten Polynom $\mathfrak{n}$ aus $\mathbb{F}_q[T]$ wählen wir ein $\eta \in K^{sep}$ mit

$$\mathbb{F}_q[T] *_\gamma \eta = {}_{\mathfrak{n}}\gamma \quad .$$

Sei nun $\omega \in \bar{K}$ mit $\gamma_{\mathfrak{n}}(\omega) = \mathfrak{n} *_\gamma \omega = t^{-1}$. Dann liegt ω bereits in K^{sep}, und die Nullstellen des „Kummer-Polynoms" $\gamma_{\mathfrak{n}}(x) - t^{-1}$ (vgl. [Sch90]) sind

$$\begin{aligned} \{\alpha \in \bar{K} \mid \gamma_{\mathfrak{n}}(\alpha) - t^{-1} = 0\} &= \{\omega + \tilde{\eta} \mid \tilde{\eta} \in {}_{\mathfrak{n}}\gamma\} \\ &= \omega + \mathbb{F}_q[T] *_\gamma \eta \quad . \end{aligned}$$

Damit folgt

$$\begin{aligned} \mathcal{W}(\mathfrak{n}) &:= \{\alpha \in \bar{K} \mid \exists \mathfrak{m} \in \mathbb{F}_q[T] \text{ mit } \mathfrak{n} *_\gamma \alpha = \mathfrak{m} *_\gamma t^{-1}\} \\ &= \mathbb{F}_q[T] *_\gamma \omega + \mathbb{F}_q[T] *_\gamma \eta \subset K^{sep} \quad . \end{aligned}$$

Es gilt der Satz:

Satz 4.7.1. *Die Abbildung e_t induziert einen* $\mathrm{Gal}(K^{sep}, K)$*-linearen* $\mathbb{F}_q[T]$*-Modul-Isomorphismus zwischen dem $*_\gamma$-Modul $\mathcal{W}(\mathfrak{n})/D_t$ und dem $*_{\phi^{\langle s\rangle}}$-Modul der $\mathfrak{n}$-Torsion ${}_{\mathfrak{n}}\phi^{\langle s\rangle}$. Es ist*

$$\mathcal{W}(\mathfrak{n})/D_t \;\cong\; {}_{\mathfrak{n}}\gamma \times \left(\mathbb{F}_q[T] *_\gamma \omega / D_t\right) \;\cong\; \mathbb{F}_q[T]/\mathfrak{n} \times \mathbb{F}_q[T]/\mathfrak{n} \quad ,$$

und $\mathcal{W}(\mathfrak{n})/D_t$ wird als $*_\gamma$-Modul erzeugt von den Restklassen von η und ω.

Beweis: Siehe [BK92]. □

Weiter gilt nach [Bae95a]:

Satz 4.7.2. *Sei $\phi = (\mathbb{F}_q, K, i(T), i(T)+g\tau+\Delta\tau^2)$ ein beliebiger Rang-2 Drinfeld-Modul. Genau dann existiert ein $s \in K$ mit $|s| < 1$ und*

$$\phi \cong_K \phi^{\langle s \rangle} \quad ,$$

falls $|j(\phi)| = |\frac{g^{q+1}}{\Delta}| > 1$ ist und die Gleichung $Y^{q-1} - g \in K[Y]$ eine Lösung in K hat.

Nun können wir den für uns in diesem Zusammenhang zentralen Satz beweisen:

Satz 4.7.3. *Seien K, O_K, i, v wie oben und $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$. Sei weiter $\phi = (\mathbb{F}_q, K, i(T), i(T) + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul mit $|j(\phi)| = |\frac{g^{q+1}}{\Delta}| > 1$. Dann existiert eine Untergruppe $(H, +)$ von $(\mathbb{F}_{\mathfrak{l}}, +)$ der Mächtigkeit $\frac{\#\mathbb{F}_{\mathfrak{l}}}{\mathrm{ggT}(\#\mathbb{F}_{\mathfrak{l}}, \mathrm{v}(j(\phi)))}$, so daß*

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in H \right\} \leqslant \mathrm{Verzw}(K({}_{\mathfrak{l}}\phi), K)$$

ist, wobei $\mathrm{Verzw}(K({}_{\mathfrak{l}}\phi), K)$ *die Verzweigungsgruppe der Erweiterung bezeichnet.*

Beweis: Es sei γ der Carlitz-Modul und $\eta \in {}_{\mathfrak{l}}\gamma$ ein fest gewählter Erzeuger der $\mathfrak{l}$-Torsion. Da $|j(\phi)| > 1$ ist, existiert im Körper $K(\sqrt[q-1]{g})$ ein s mit $|s| < 1$, so daß der zugehörige Tate-Drinfeld-Modul $\phi^{\langle s \rangle}$ über $K(\sqrt[q-1]{g})$ isomorph zu ϕ ist. Sei weiter $t \in K^{sep}$ eine fest gewählte Lösung der Gleichung $Y^{q-1} - s$ und

$$L := K(\sqrt[q-1]{g}\ ,\ {}_{\mathfrak{l}}\gamma, t) \quad .$$

Da $\mathbb{F}_q{}^* \subset K$ ist, ist

$$L \supseteq K(\sqrt[q-1]{g}\ ,\ t) \supseteq K(\sqrt[q-1]{g}) \supseteq K$$

ein Turm von Galoiserweiterungen, und wir halten fest, daß $\mathrm{ggT}([L : K], q) = 1$ ist. Weiter betrachten wir die durch

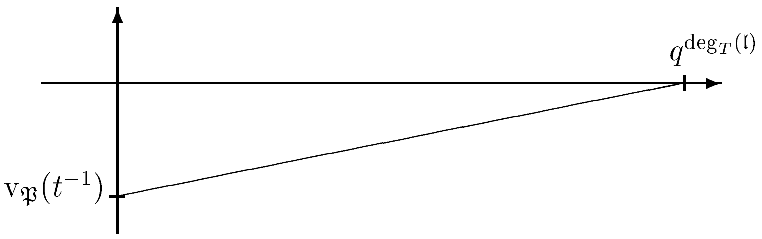
$$W := \{\alpha \in K^{sep} \mid \gamma_{\mathfrak{l}}(\alpha) - t^{-1}\} = 0$$

definierte Carlitz-Kummer-Erweiterung $L(W)|L$.

Wir untersuchen nun die Galoisgruppen im folgenden Körperdiagramm:

$$\begin{tikzcd}
 & K^{sep} \arrow[dl, dash] \arrow[dd, dash] \\
L(W) \arrow[dd, dash] & \\
 & L({}_{\mathfrak{l}}\phi) = L({}_{\mathfrak{l}}\phi^{\langle s \rangle}) \arrow[dd, dash] \\
L \arrow[ur, dash] \arrow[dd, dash] & \\
 & K({}_{\mathfrak{l}}\phi) \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Sei ω ein Element aus W, so ist $W = \omega + \mathbb{F}_q[T] *_{\gamma\,\mathfrak{l}}\gamma$. Untersuchen wir nun das Newton-Polygon des Polynoms $\gamma_{\mathfrak{l}}(x) - t^{-1} \in L(x)$, wobei wir das Bewertungsideal von L mit $\mathfrak{P}$ und das von K mit $\mathfrak{p}$ bezeichnen. Wegen $|t^{q-1}| = |s| = |j(\phi)|^{-1}$ ist $\mathrm{v}_{\mathfrak{P}}(t^{-1}) < 0$. Da das Bild von $i : \mathbb{F}_q[T] \to K$ in O_K liegt, sind alle Koeffizienten des Polynoms $\gamma_{\mathfrak{l}}(x)$ ganz an $\mathfrak{P}$, und da $\gamma_{\mathfrak{l}}(x)$ normiert ist, hat das Newton-Polygon von $\gamma_{\mathfrak{l}}(x) - t^{-1}$ an $\mathfrak{P}$ die Form



Untersucht man nun, wo das Newton-Polygon das Gitter $\mathbb{Z} \times \mathbb{Z}$ schneidet, so erhält man, daß das Polynom in $L(x)$ in höchstens $\mathrm{ggT}(\mathrm{v}_{\mathfrak{P}}(t^{-1}), q^{\deg_T(\mathfrak{l})})$ irreduzible Polynome vom Grad größer oder gleich $\frac{q^{\deg_T(\mathfrak{l})}}{\mathrm{ggT}(q^{\deg_T(\mathfrak{l})}, \mathrm{v}_{\mathfrak{P}}(t^{-1}))}$ zerfällt. Da der Körpergrad von L über K prim zu q ist, gilt dies auch für den Verzweigungsindex. Daher ist

$$\mathrm{ggT}(q^{\deg_T(\mathfrak{l})}, \mathrm{v}_{\mathfrak{P}}(t^{-1})) = \mathrm{ggT}(q^{\deg_T(\mathfrak{l})}, \mathrm{v}_{\mathfrak{p}}(t^{-1})) \quad .$$

Wegen

$$(q-1)\mathrm{v}_{\mathfrak{p}}(t) = \mathrm{v}_{\mathfrak{p}}(t^{q-1}) = -\mathrm{v}_{\mathfrak{p}}(j(\phi))$$

ist dann die Länge der Bahn von ω unter der Verzweigungsgruppe von $K^{sep}|L$ ein Vielfaches von

$$\frac{q^{\deg_T(\mathfrak{l})}}{\mathrm{ggT}(q^{\deg_T(\mathfrak{l})}, \mathrm{v}_{\mathfrak{p}}(j(\phi)))} \quad .$$

Sei nun $\tilde{\omega}$ ein Element aus dieser Bahn und σ ein zugehöriges Element aus der Verzweigungsgruppe mit $\sigma(\omega) = \tilde{\omega}$. Dann existiert ein $\mathfrak{n} \in \mathbb{F}_q[T]$ mit

$$\sigma(\omega) = \omega + \mathfrak{n} *_{\gamma} \eta \quad .$$

Wir untersuchen nun, wie σ auf ${}_{\mathfrak{l}}\phi^{\langle s\rangle}$ operiert. Dazu verwenden wir die Uniformisierung

$$e_t : {K^{sep}}/{D_t} \to K^{sep}$$

von oben. Nach Satz 4.7.1 bilden $e_t(\eta)$ und $e_t(\omega)$ eine $\mathbb{F}_{\mathfrak{l}}$-Basis von ${}_{\mathfrak{l}}\phi^{\langle s\rangle}$. Auf dieser Basis operiert σ wie folgt:

$$\begin{aligned} \sigma(e_t(\eta)) &= e_t(\sigma(\eta)) \overset{\eta \in L}{=} e_t(\eta) \\ \sigma(e_t(\omega)) &= e_t(\sigma(\omega)) = e_t(\omega + \mathfrak{n} *_{\gamma} \eta) = e_t(\omega) + \mathfrak{n} *_{\phi^{\langle s\rangle}} e_t(\eta) \end{aligned}$$

Also induziert σ auf ${}_{\mathfrak{l}}\phi^{\langle s\rangle}$ eine lineare Abbildung, die bzgl. der obigen Basis durch die Matrix

$$\begin{pmatrix} 1 & \bar{\mathfrak{n}} \\ 0 & 1 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$$

repräsentiert wird. So erhält man zu jedem Element aus der Bahn von ω unter der Verzweigungsgruppe eine Matrix der obigen Form, und diese Matrizen sind paarweise verschieden. Da die Verzweigungsgruppe von $L({}_{\mathfrak{l}}\phi)|L$ Untergruppe der Verzweigungsgruppe von $K({}_{\mathfrak{l}}\phi)|K$ ist, folgt die Aussage. $\square$

Bemerkung 4.7.4. Der obige Satz schließt die Möglichkeit

$$\#(\mathrm{Verzw}(K({}_{\mathfrak{l}}\phi), K) \cap \begin{pmatrix} 1 & \mathbb{F}_{\mathfrak{l}} \\ 0 & 1 \end{pmatrix}) > \frac{\#\mathbb{F}_{\mathfrak{l}}}{\mathrm{ggT}(\#\mathbb{F}_{\mathfrak{l}}, \mathrm{v}(j(\phi)))}$$

nicht aus.

Da für Galoiserweiterungen von globalen Körpern die Galoisgruppe der Komplettierung an einer Stelle $\mathfrak{q}$ gerade die Zerlegungsgruppe von $\mathfrak{q}$ ist, liefert uns der obige Satz das folgende Resultat für Torsionserweiterungen von globalen Körpern.

Satz 4.7.5. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$. Ist dann $\mathrm{v}_{\mathfrak{p}}(j(\phi)) = (q+1)\mathrm{v}_{\mathfrak{p}}(g) - \mathrm{v}_{\mathfrak{p}}(\Delta) < 0$, so existiert eine Untergruppe $(H, +)$ von $(\mathbb{F}_{\mathfrak{l}}, +)$ der Mächtigkeit $\frac{\#\mathbb{F}_{\mathfrak{l}}}{\mathrm{ggT}(\#\mathbb{F}_{\mathfrak{l}}, \mathrm{v}_{\mathfrak{p}}(j(\phi)))}$, so daß für eine Stelle $\mathfrak{P}$ von $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$ über $\mathfrak{p}$*

$$\left\{ \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \mid a \in H \right\} \leqslant \mathrm{Verzw}(\mathfrak{P}, \mathbb{F}_q(u)({}_{\mathfrak{l}}\phi)|\mathbb{F}_q(u)) \leqslant \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$$

gilt, wobei $\mathrm{Verzw}(\mathfrak{P}, \mathbb{F}_q(u)({}_{\mathfrak{l}}\phi)|\mathbb{F}_q(u))$ die Verzweigungsgruppe der Stelle $\mathfrak{P}$ bezeichnet.

Beweis: Die Aussage folgt direkt aus Satz 4.7.3, indem man $\mathbb{F}_q(u)$ an $\mathfrak{p}$ komplettiert. $\square$

Wir erhalten das folgende Korollar:

Korollar 4.7.6. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$ mit $\mathrm{v}_{\mathfrak{p}}(j(\phi)) = (q+1)\mathrm{v}_{\mathfrak{p}}(g) - \mathrm{v}_{\mathfrak{p}}(\Delta) < 0$.*
Dann gilt:

(i) Ist $\mathrm{ggT}(q^{\deg_T(\mathfrak{l})}, \mathrm{v}_{\mathfrak{p}}(j(\phi))) \neq q^{\deg_T(\mathfrak{l})}$, so existiert ein Element der Ordnung $p = \mathrm{char}(\mathbb{F}_q)$ in $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) \leqslant \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$.

(ii) Ist $\mathrm{ggT}(q^{\deg_T(\mathfrak{l})}, \mathrm{v}_{\mathfrak{p}}(j(\phi))) = 1$, so gilt sogar (bis auf Konjugation)

$$\begin{pmatrix} 1 & \mathbb{F}_{\mathfrak{l}} \\ 0 & 1 \end{pmatrix} \leqslant \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) \quad .$$

Nachdem wir die Stellen schlechter Reduktion abgehandelt haben, werden wir nun noch das Verhalten der Galoisgruppe an der Stelle $\mathfrak{l}(u)$ untersuchen.

Satz 4.7.7. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul, $\phi = \min(\phi)$, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ und $\Delta \not\equiv 0 \bmod \mathfrak{l}(u)$. Weiter sei $H := \mathrm{H}(\mathrm{Dred}(\phi, \mathfrak{l}(u))) \in \mathbb{F}_\mathfrak{l}$ die Hasse-Invariante des an $\mathfrak{l}(u)$ reduzierten Drinfeld-Moduls, und $\mathfrak{P}$ sei eine Stelle von $\mathbb{F}_q(u)[_\mathfrak{l}\phi]$ über $\mathfrak{l}(u)$. Dann existiert ein Element $\sigma \in \mathrm{Verzw}(\mathfrak{P}) \leqslant \mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u))$ mit*

$$\mathrm{ord}(\sigma) = \begin{cases} q^{\deg_T(\mathfrak{l})} - 1 & ; \quad H \neq 0 \\ q^{2\deg_T(\mathfrak{l})} - 1 & ; \quad H = 0 \end{cases} .$$

Dabei bezeichnet $\mathrm{Verzw}(\mathfrak{P})$ *die Verzweigungsgruppe der Stelle* $\mathfrak{P}$.

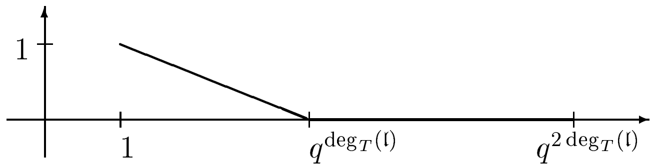
Beweis: Wir erhalten die Aussage, indem wir das Newton-Polygon von $\phi_\mathfrak{l}(x) \in \mathbb{F}_q(u)[x]$ an der Stelle $\mathfrak{l}(u)$ betrachten.
Sei

$$\phi_\mathfrak{l}(x) = \sum_{i=0}^{q^{2\deg(\mathfrak{l})}} a_i x^i \quad .$$

Es ist klar, daß $a_i = 0$ gilt, falls i keine q-Potenz ist. Betrachten wir die Bewertung der Koeffizienten an $\mathfrak{l}(u)$, so erhalten wir mit Satz 1.10.5

$$\begin{aligned} \mathrm{v}_\mathfrak{l}(a_1) &= \mathrm{v}_\mathfrak{l}(\mathfrak{l}(u)) = 1, \\ \mathrm{v}_\mathfrak{l}(a_i) &\geqslant 1 \qquad \forall\ 2 \leqslant i \leqslant q^{\deg(\mathfrak{l})} - 1 \\ \mathrm{v}_\mathfrak{l}(a_i) &\geqslant 0 \qquad \forall\ q^{\deg(\mathfrak{l})} \leqslant i \leqslant q^{2\deg(\mathfrak{l})} - 1 \\ \mathrm{v}_\mathfrak{l}(a_{q^{2\deg(\mathfrak{l})}}) &= \mathrm{v}_\mathfrak{l}(\Delta^{q^{2\deg(\mathfrak{l})}}) = 0. \end{aligned}$$

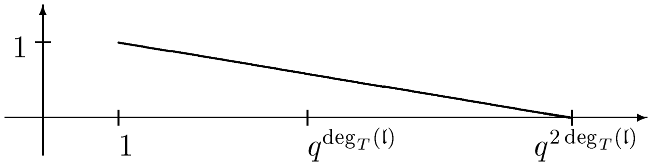
Da die Hasse-Invariante H gerade $red(a_{q^{\deg(\mathfrak{l})}}, \mathfrak{l}(u))$ ist, erhalten wir im Fall $0 \neq H \in \mathbb{F}_\mathfrak{l}$ das Newton-Polygon



Der erste Streckenzug im Newton-Polygon hat also Steigung $\frac{1}{1-q^{\deg(\mathfrak{l})}}$, und daher existiert ein Element der Ordnung $q^{\deg(\mathfrak{l})} - 1$ in der zugehörigen Verzweigungsgruppe.
Ist $0 = H \in \mathbb{F}_\mathfrak{l}$, so gilt nach Satz 1.10.5 auch für die folgenden Koeffizienten

$$\mathrm{v}_\mathfrak{l}(a_i) \geqslant 1 \qquad \forall\ q^{\deg(\mathfrak{l})} \leqslant i \leqslant q^{2\deg(\mathfrak{l})} - 1 \quad .$$

Das Newton-Polygon hat in diesem Fall die Form



.

Es hat die Steigung $\frac{1}{1-q^{2\deg(\mathfrak{l})}}$. Infolgedessen existiert ein Element der Ordnung $q^{2\deg(\mathfrak{l})}-1$ in der Verzweigungsgruppe. $\square$

Kapitel 5

Der Algorithmus

Wir kommen nun zu dem auf Seite 9 angekündigten Algorithmus. Dieser entscheidet zu vorgegebenem Rang-2 Drinfeld-Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ und $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ in endlicher Zeit, ob

$$\mathrm{Gal}\,(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$$

gilt. Die Idee des Algorithmus haben wir bereits auf Seite 9 beschrieben. In 5.3 geben wir die Basisversion des Algorithmus an und zeigen, daß er immer terminiert. Im darauf folgenden Abschnitt werden wir einige Resultate aus den vorherigen Kapiteln benutzen, um die Effizienz des Algorithmus zu erhöhen.

5.1 Die Chebotarev-Schranke

In diesem Abschnitt werden wir die Schranke aus der expliziten Version des Satzes von Chebotarev nach oben abschätzen. Die explizite Version für globale Funktionenkörper wird in [FJ86] angegeben. Allerdings fehlt dort in einigen Aussagen ein Parameter, der auftritt, wenn der zugrundeliegende Funktionenkörper kein rationaler Funktionenkörper ist. Dies wird im Anhang von [GJ98] korrigiert. Daher werden wir uns hier immer auf diesen Artikel beziehen, obwohl wir nur mit $\mathbb{F}_q(u)$ arbeiten und in diesem Fall die Formeln in [FJ86] korrekt sind.
Wir verwenden die folgende Notation. Es sei $\mathcal{C}$ eine Konjugationsklasse in $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u))$, $K_{\phi,\mathfrak{l}}$ der Konstantenkörper von $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$, $n := [K_{\phi,\mathfrak{l}} : \mathbb{F}_q]$, $K_{\phi,\mathfrak{l}}(u) = \mathbb{F}_q(u, K_{\phi,\mathfrak{l}})$ und $m := [\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi] : K_{\phi,\mathfrak{l}}(u)]$.
Ein Element $\sigma \in \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]\,, \mathbb{F}_q(u))$ induziert eine Abbildung

$$\tilde{\sigma} : K_{\phi,\mathfrak{l}} \to K_{\phi,\mathfrak{l}} \quad , \qquad x \mapsto x^{q^a} \; .$$

Die induzierte Abbildung $\tilde{\sigma}$ ist eine Potenz des Frobenius $x \mapsto x^q$, diese Potenz wird mit $a_\sigma \in \mathbb{N}_0$ bezeichnet. Die in Satz 4.5.15 angegebene obere Abschätzung für das Geschlecht g von $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$ bezeichnen wir mit $\tilde{g}$. Wir definieren

$$C_k(\mathcal{C}) := \left\{ \mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]} \mid \begin{array}{c} \deg_u(\mathfrak{p}) = k, \\ \mathfrak{p} \text{ in } \mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]|\mathbb{F}_q(u) \text{ unverzweigt}, \\ (\mathfrak{p}, \mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)) = \mathcal{C} \end{array} \right\} .$$

Die folgenden Ungleichungen werden wir verwenden. Dabei legen wir wenig Wert darauf, ob die oberen Schranken gut sind. Es ist lediglich wichtig, daß sie explizit berechenbar sind.

$$\begin{gathered} 1 \leqslant m \leqslant \#\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) < q^{4 \deg_T(\mathfrak{l})} \\ 1 \leqslant n \leqslant \#\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) < q^{4 \deg_T(\mathfrak{l})} \\ 1 \leqslant a_\sigma \leqslant n < q^{4 \deg_T(\mathfrak{l})} \\ 0 \leqslant g \leqslant \tilde{g} \end{gathered}$$

Lemma 5.1.1. *Es existiert ein $\tilde{k}$ (abhängig von $\mathcal{C}$) im Bereich*

$$2 \log_q(2 + 2q^{4 \deg_T(\mathfrak{l})} + 2\tilde{g}) < \tilde{k} \leqslant n + 2 \log_q(2 + 2q^{4 \deg_T(\mathfrak{l})} + 2\tilde{g}) ,$$

für das

$$C_{\tilde{k}}(\mathcal{C}) \neq \emptyset$$

gilt.

Beweis: Sei $k \in \mathbb{N}$ beliebig. Nach [GJ98, Korollar 13.5] ist $C_k(\mathcal{C}) \neq \emptyset$, falls ein $\sigma \in \mathcal{C}$ existiert, so daß die folgenden Bedingungen erfüllt sind:

$$\begin{aligned} & k \equiv a_\sigma \bmod n \quad , \\ & k \geqslant 2 \log_q(g + m) \quad , \\ & 0 < \frac{\#\mathcal{C}}{km} q^k - \frac{\#\mathcal{C}}{km} 2(m + g + 1) q^{\frac{k}{2}} \quad . \end{aligned}$$

Die unterste Formel können wir wie folgt umformen:

$$\begin{array}{cccl} & \frac{\#\mathcal{C}}{km} q^{\frac{k}{2}} (q^{\frac{k}{2}} - 2(m + g + 1)) & > 0 \\ \Longleftrightarrow & q^{\frac{k}{2}} - 2(m + g + 1) & > 0 \\ \Longleftrightarrow & k & > 2 \log_q(2 + 2m + 2g) \end{array}$$

Aus

$$2 \log_q(2 + 2m + 2g) > 2 \log_q(m + g)$$

folgt dann, daß das Ungleichungssystem von oben äquivalent ist zu

$$\begin{aligned} & k \equiv a_\sigma \bmod n \quad , \\ & k > 2 \log_q(2 + 2m + 2g) \quad . \end{aligned}$$

Da mit den oben angegebenen Abschätzungen

$$2\log_q(2+2q^{4\deg_T(\mathfrak{l})}+2\tilde{g}) > 2\log_q(2+2m+2g)$$

gilt, existiert ein $\tilde{k}$ im Bereich

$$2\log_q(2+2q^{4\deg_T(\mathfrak{l})}+2\tilde{g}) < \tilde{k} \leqslant n + 2\log_q(2+2q^{4\deg_T(\mathfrak{l})}+2\tilde{g}) ,$$

das sowohl die Ungleichung als auch die Kongruenz erfüllt. □

Wir können die Aussage mittels $n < q^{4\deg_T(\mathfrak{l})}$ unabhängig von n machen und erhalten:

Satz 5.1.2. *Es existiert ein $\tilde{k}$ im Bereich*

$$2\log_q(2+2q^{4\deg_T(\mathfrak{l})}+2\tilde{g}) < \tilde{k} < q^{4\deg_T(\mathfrak{l})} + 2\log_q(2+2q^{4\deg_T(\mathfrak{l})}+2\tilde{g}) ,$$

für das

$$C_{\tilde{k}}(\mathcal{C}) \neq \emptyset$$

gilt.

Es ist klar, daß die obige Abschätzung extrem grob ist. Zum Beispiel haben wir n gegen $q^{4\deg_T(\mathfrak{l})}$ abgeschätzt, während nach unseren Überlegungen in Abschnitt 4.6 in den meisten Fällen $n = 1$ gelten wird. Auch bei der Herleitung von $\tilde{g}$ haben wir einige nicht besonders scharfe Abschätzungen verwendet.
Daher werden wir den Satz in folgender Formulierung benutzen:

Korollar 5.1.3. *Sei $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ ein Rang-2 Drinfeld-Modul und $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$. Dann gibt es eine explizit berechenbare Schranke $t \in \mathbb{N}$, so daß gilt:*
Für jede Konjugationsklasse $\mathcal{C}$ in $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$ existiert ein $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$ mit $\deg_u(\mathfrak{p}) \leqslant t$ und $(\mathfrak{p}, \mathbb{F}_q(u)[_{\mathfrak{l}}\phi] \mid \mathbb{F}_q(u)) = \mathcal{C}$.

Bemerkung 5.1.4. Im obigen Beweis darf die Bedingung $k \equiv a_\sigma \bmod n$ nicht vernachlässigt werden. Es gilt nämlich nicht, daß man immer ein einziges k finden kann, so daß man für alle Konjugationsklassen einen Frobenius findet, wenn man über alle Stellen vom Grad k läuft. Betrachtet man z.B. die Körpererweiterung $\mathbb{F}_{q^2}(u)|\mathbb{F}_q(u)$ und als σ das nichttriviale Galoiselement, so ist $a_\sigma = 1$, und die Konstantenerweiterung hat Grad 2. Aus dem Zerfallen von irreduziblen Polynomen in Erweiterungen endlicher Körper folgt dann

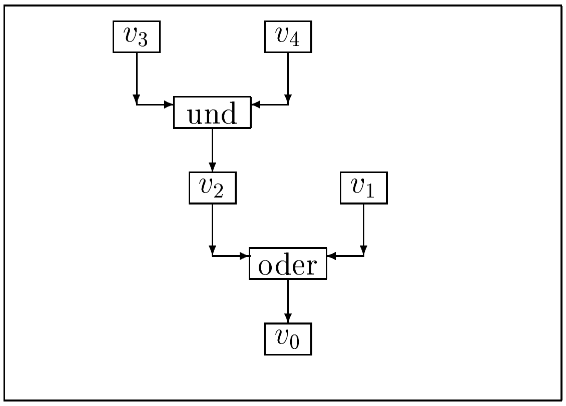
$$C_k(\{\sigma\}) = \begin{cases} \emptyset & , \quad k \equiv 0 \bmod 2 \\ \{\mathfrak{p}(u) \mid \deg_u(\mathfrak{p}) = k\} & , \quad k \equiv 1 \bmod 2 \end{cases}$$

Für $C_k(\{id\})$ gilt entsprechend

$$C_k(\{id\}) = \{\mathfrak{p}(u) \mid \deg_u(\mathfrak{p}) = k\} - C_k(\{\sigma\}) .$$

5.2 Schaltgraphen

Bevor wir den Algorithmus angeben, werden wir nun noch die für uns zentrale Datenstruktur beschreiben.
In dieser Datenstruktur wird ein Schaltplan der Form



.

als ein System von Aussagen

$$\begin{aligned} v_3 \wedge v_4 &\Rightarrow v_2 \\ v_2 &\Rightarrow v_0 \\ v_1 &\Rightarrow v_0 \end{aligned}$$

dargestellt. Weiter wird formalisiert, wie man aus der Korrektheit bestimmter Aussagen mittels der erlaubten Folgerungen auf die Korrektheit weiterer Aussagen schließen kann.

Definition 5.2.1. *Sei V eine endliche Menge,* $\mathrm{Pot}(V)$ *die Potenzmenge von V, $R \subset \mathrm{Pot}(V) \times V$ und $f : V \to \{0,1\}$. Dann heißt das Tripel $S := (V, R, f)$ ein* Schaltgraph. *Die Menge V heißt* Knotenmenge, *R heißt die* Schaltrelation *und f die* Belegungsfunktion. *Die Menge $I(S) := \{v \in V \mid f(v) = 1\}$ heißt die* Information *von S.*

Definition 5.2.2. *Sei $S = (V, R, f)$ ein Schaltgraph und $(M, w) \in R$. Dann definieren wir einen neuen Schaltgraphen $\tilde{S} = (\tilde{V}, \tilde{R}, \tilde{f})$ durch $\tilde{V} := V$, $\tilde{R} := R$ und*

$$\tilde{f}(v) = \begin{cases} f(v) & , \quad v \neq w \\ 1 & , \quad v = w \text{ und } f(w) = 1 \\ 1 & , \quad v = w \text{ und } f(w) = 0 \text{ und } \forall\ s \in M \text{ ist } f(s) = 1 \\ 0 & , \quad v = w \text{ und } f(w) = 0 \text{ und } \exists\ s \in M \text{ mit } f(s) = 0 \end{cases} .$$

Wir sagen, $\tilde{S}$ entsteht aus S durch innere Transformation *(oder* innere Schaltung*) entlang (M, w), und schreiben*

$$S \stackrel{(M,w)}{\longrightarrow} \tilde{S} .$$

Definition 5.2.3. *Sei $S = (V, R, f)$ ein Schaltgraph und $w \in V$. Dann definieren wir einen neuen Schaltgraphen $\tilde{S} = (\tilde{V}, \tilde{R}, \tilde{f})$ durch $\tilde{V} := V$, $\tilde{R} := R$ und*

$$\tilde{f}(v) = \begin{cases} f(v) & , \quad v \neq w \\ 1 & , \quad v = w \end{cases} \quad .$$

Wir sagen, $\tilde{S}$ entsteht aus S durch äußere Transformation *(oder* äußere Schaltung*) an w, und schreiben*

$$S \xrightarrow{w} \tilde{S} \,.$$

Nach einer Transformation gilt immer $I(\tilde{S}) = I(S)$ oder $I(\tilde{S}) = I(S) \cup \{w\}$, die Information nimmt also nie ab. Insbesondere gilt immer $I(S) \subseteq I(\tilde{S})$.

Definition 5.2.4. *Ein Schaltgraph S heißt* saturiert*, wenn für jede innere Schaltung $S \xrightarrow{(M,w)} \tilde{S}$ die Information gleich bleibt (d.h. $I(\tilde{S}) = I(S)$).*

Lemma 5.2.5. *Jeder Schaltgraph kann durch endlich viele innere Schaltungen in einen saturierten Schaltgraphen überführt werden. Dieser ist eindeutig bestimmt.*

Beweis: Sei $S = (V, R, f)$ ein Schaltgraph. Da V eine endliche Menge ist und die Information durch Anwendung von inneren Schaltungen nie abnimmt, ist klar, daß man S in endlich vielen Schritten in einen saturierten Schaltgraphen überführen kann.
Es bleibt noch die Eindeutigkeit zu zeigen. Wir führen den Beweis durch Widerspruch. Seien $\tilde{S}$ und $\hat{S}$ zwei verschiedene Saturierungen von S. Dann gilt für die zugehörigen Informationen $I(\tilde{S}) \neq I(\hat{S})$. Seien $\tilde{S}$ und $\hat{S}$ durch die beiden folgenden Ketten von inneren Transformationen aus S hervorgegangen:

$$S = \tilde{S}_0 \xrightarrow{(N_0,v_0)} \tilde{S}_1 \xrightarrow{(N_1,v_1)} \ldots \xrightarrow{(N_{n-2},v_{n-2})} \tilde{S}_{n-1} \xrightarrow{(N_{n-1},v_{n-1})} \tilde{S}_n = \tilde{S}$$

und

$$S = \hat{S}_0 \xrightarrow{(M_0,w_0)} \hat{S}_1 \xrightarrow{(M_1,w_1)} \ldots \xrightarrow{(M_{m-2},w_{m-2})} \hat{S}_{m-1} \xrightarrow{(M_{m-1},w_{m-1})} \hat{S}_m = \hat{S} \quad .$$

Wir können (evtl. nach Vertauschung von $\tilde{S}$ und $\hat{S}$) o.B.d.A. annehmen, daß

$$\mathcal{N} := I(\hat{S}) - I(\tilde{S}) \neq \emptyset$$

gilt. $\mathcal{N}$ enthält also genau die Knoten, deren Belegung im Verlauf der zweiten Kette von 0 auf 1 ansteigt und deren Belegung in der ersten Kette auf 0 bleibt. Sei nun

$$i := \min\{k \in \mathbb{N}_0 \mid I(\hat{S}_k) \cap \mathcal{N} \neq \emptyset\} \quad .$$

Da $\mathcal{N} \neq \emptyset$ ist, ist $i > 0$, und wir können den Schritt

$$\hat{S}_{i-1} \xrightarrow{(M_{i-1},w_{i-1})} \hat{S}_i$$

betrachten. Nach Konstruktion ist $w_i \in I(\hat{S})$ und $w_i \notin I(\tilde{S})$. Wegen der Minimalität von i liegt kein Knoten aus M_{i-1} in $\mathcal{N}$. Aus $M_{i-1} \subseteq I(\hat{S}_{i-1}) \subseteq I(\hat{S})$ folgt dann

$$\begin{aligned}\emptyset &= M_{i-1} \cap \mathcal{N} = M_{i-1} \cap (I(\hat{S}) - I(\tilde{S})) \\ &= (M_{i-1} \cap I(\hat{S})) - I(\tilde{S}) = M_{i-1} - I(\tilde{S})\end{aligned}$$

bzw.

$$M_{i-1} \subseteq I(\tilde{S}) \quad .$$

Da $\tilde{S}$ saturiert ist und die Schaltrelation (M_{i-1}, w_{i-1}) auch in $R(\tilde{S}) = R(S)$ liegt, ist dann

$$w_{i-1} \in I(\tilde{S})$$

im Widerspruch zur Konstruktion von w_{i-1}. Daher muß $I(\tilde{S}) = I(\hat{S})$ sein. Dies ist äquivalent zu $\tilde{S} = \hat{S}$. □

Wir können einen Schaltgraphen durch den folgenden Algorithmus saturieren.

SATURIERE
Eingabe: Ein Schaltgraph $S = (V, R, f)$. Ausgabe: Der zugehörige saturierte Schaltgraph $\bar{S} = (\bar{V}, \bar{R}, \bar{f})$.
1) $\tilde{S} := S$ 2) $n := \#I(\tilde{S})$ 3) Führe für alle $(M, w) \in R$ die innere Transformation $\tilde{S} \overset{(M,w)}{\longrightarrow} \tilde{S}$ aus. 4) Ist $\#I(\tilde{S}) \neq n$, so gehe zu Schritt 2. Ansonsten gebe $\tilde{S}$ aus und beende den Algorithmus.

Bemerkung 5.2.6. (i) Eine Schaltung verringert nie die Information eines Schaltgraphen.

(ii) Statt $(\{a_1, \ldots, a_n\}, w) \in R$ schreiben wir auch

$$\big((a_1 = 1) \wedge \ldots \wedge (a_n = 1)\big) \Rightarrow (w = 1)$$

oder

$$\big(a_1 \wedge \ldots \wedge a_n\big) \Rightarrow w \quad .$$

(iii) Der Schaltplan von Seite 94 wird durch $V = \{v_0, \ldots, v_4\}$ und

$$R = \big\{(\{v_3, v_4, \}, v_2),\ (\{v_2\}, v_0),\ (\{v_1\}, v_0)\big\}$$

repräsentiert. Ist $f = (v_0, \ldots, v_4) = (1, 0, 0, 1, 1)$, so ist nach $S \overset{(\{v_3,v_4\},v_2)}{\longrightarrow} \tilde{S}$ die Belegung $\tilde{f} = (1, 0, 1, 1, 1)$, während nach $S \overset{(\{v_1\},v_0)}{\longrightarrow} \tilde{S}$ die Belegung $\tilde{f} = (1, 0, 0, 1, 1) = f$ ist. Ist $f = (0, 0, 0, 1, 1)$, so ist die zugehörige saturierte Belegung $(1, 0, 1, 1, 1)$.

(iv) Falls für alle $(M, w) \in R$ die Menge M nur aus einem Element besteht, so läßt sich (V, R) als gerichteter Graph interpretieren.

5.3 Der Basisalgorithmus

Kommen wir nun zur Beschreibung des Algorithmus. Dazu definieren wir uns erst einen Schaltgraphen (V, R, f). Die Knoten aus $V = \{v_0, \ldots, v_n\}$ repräsentieren dabei Aussagen, z.B.

$$v_0 : \qquad G = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) \ .$$

Die Belegungsfunktion beschreibt den Wahrheitsgehalt der Aussage in unserer Situation.

$$f(v_i) = \begin{cases} 1 & , \quad \text{die durch } v_i \text{ repräsentierte Aussage ist wahr.} \\ 0 & , \quad \text{der Wahrheitswert der Aussage } v_i \text{ ist } \textit{unbekannt.} \end{cases}$$

Die Relationen in R beschreiben Implikationen zwischen den verschiedenen Aussagen. Die v_i repräsentieren nur gruppentheoretische Aussagen über $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ und $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$. Damit beschreiben die Relationen lediglich gruppentheoretische Zusammenhänge. Die Relationen gewinnen wir aus den Kriterien aus Kapitel 3. Weder in V noch in R wird Bezug auf Drinfeld-Moduln genommen.
Die durch die v_i repräsentierten Aussagen sehen wie folgt aus:

v_0 : $G = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$
v_1 : $\det(G) = \mathbb{F}_{\mathfrak{l}}{}^*$
v_2 : $\mathrm{P}G = \mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$
v_3 : $\mathrm{P}G \not\leq \mathrm{PSL}(2, \mathbb{F}_{\mathfrak{l}})$ oder $\mathrm{PSL}(2, \mathbb{F}_{\mathfrak{l}})$ ist keine echte Untergruppe von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$
v_4 : $\mathrm{P}G \not\leq \mathrm{PGL}(2, \mathbb{F}_n)$ für alle $\mathbb{F}_p \subseteq \mathbb{F}_n \subsetneq \mathbb{F}_{\mathfrak{l}}$.
v_5 : $\mathrm{P}G \not\leq \mathrm{D}_{2(\#\mathbb{F}_{\mathfrak{l}}+1)}$ oder $\mathrm{D}_{2(\#\mathbb{F}_{\mathfrak{l}}+1)}$ ist keine echte Untergruppe von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$
v_6 : $\mathrm{P}G \not\leq \mathrm{D}_{2(\#\mathbb{F}_{\mathfrak{l}}-1)}$
v_7 : $\mathrm{P}G \not\leq \mathrm{P}\mathfrak{B}$
v_8 : $\mathrm{P}G \not\leq A_4$ oder A_4 ist keine echte Untergruppe von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$
v_9 : $\mathrm{P}G \not\leq S_4$ oder S_4 ist keine echte Untergruppe von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$
v_{10} : $\mathrm{P}G \not\leq A_5$ oder A_5 ist keine echte Untergruppe von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$
v_{11} : $\exists M \in G$ mit $\langle \det(M) \rangle = \mathbb{F}_{\mathfrak{l}}{}^*$.
v_{13} : $\exists M \in G$ mit $\det(M) \notin (\mathbb{F}_{\mathfrak{l}}{}^*)^2$
v_{14} : $\exists M \in G$ mit $\frac{\mathrm{Tr}(M)^2}{\det(M)} \notin \mathbb{F}_n$, für alle $\mathbb{F}_p \subseteq \mathbb{F}_n \subsetneq \mathbb{F}_{\mathfrak{l}}$.
v_{15} : $\exists M \in G$ mit $2(\#\mathbb{F}_{\mathfrak{l}} + 1) \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M])$
v_{16} : $\exists M \in G$ mit $2(\#\mathbb{F}_{\mathfrak{l}} - 1) \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M])$
v_{17} : $\exists M \in G$ mit $\mathrm{charpol}_M(x) \in \mathbb{F}_{\mathfrak{l}}[x]$ irreduzibel
v_{18} : $\exists M \in G$ mit $12 \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M])$
v_{19} : $\exists M \in G$ mit $24 \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M])$
v_{20} : $\exists M \in G$ mit $60 \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M])$
v_{21} : $\#\mathbb{F}_{\mathfrak{l}} \equiv 0 \bmod 2$
v_{22} : $\#\mathbb{F}_{\mathfrak{l}} = 2$
v_{23} : $\#\mathbb{F}_{\mathfrak{l}} = 3$

Fortsetzung auf nächster Seite

Fortsetzung		
v_{24}	:	$\#\mathbb{F}_{\mathfrak{l}} = 4$
v_{25}	:	$\#\mathbb{F}_{\mathfrak{l}} = 5$

Da die Numerierung der v_i zu korrespondierenden Aussagen passen soll, ist v_{12} undefiniert. In Satz 3.4.6 haben wir bereits geklärt, unter welchen Bedingungen an $\mathbb{F}_{\mathfrak{l}}$ mögliche maximale Untergruppen von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$ (siehe 3.4.4) keine echten Untergruppen sind.
Dies liefert uns folgende Implikationen:

$$\begin{array}{lllclllclll}
v_{21} & \Rightarrow & v_3 & , & v_{22} & \Rightarrow & v_5 & , & v_{22} & \Rightarrow & v_8 \\
v_{22} & \Rightarrow & v_9 & , & v_{22} & \Rightarrow & v_{10} & , & v_{23} & \Rightarrow & v_9 \\
v_{23} & \Rightarrow & v_{10} & , & v_{24} & \Rightarrow & v_{10} & , & & &
\end{array}$$

Das Ausschlußkriterium 3.4.7 für die maximalen Untergruppen liefert:

$$\begin{array}{rllclllclll}
v_{13} & \Rightarrow & v_3 & , & v_{14} & \Rightarrow & v_4 & , & v_{15} & \Rightarrow & v_5 \\
v_{16} & \Rightarrow & v_6 & , & v_{17} & \Rightarrow & v_7 & , & v_{18} & \Rightarrow & v_8 \\
v_{23} \wedge v_{13} & \Rightarrow & v_8 & , & v_{19} & \Rightarrow & v_9 & , & v_{20} & \Rightarrow & v_{10} \\
v_{25} \wedge v_{13} & \Rightarrow & v_{10} & , & & & & & & &
\end{array}$$

Weiter verwenden wir

$$v_{11} \Rightarrow v_1 \quad .$$

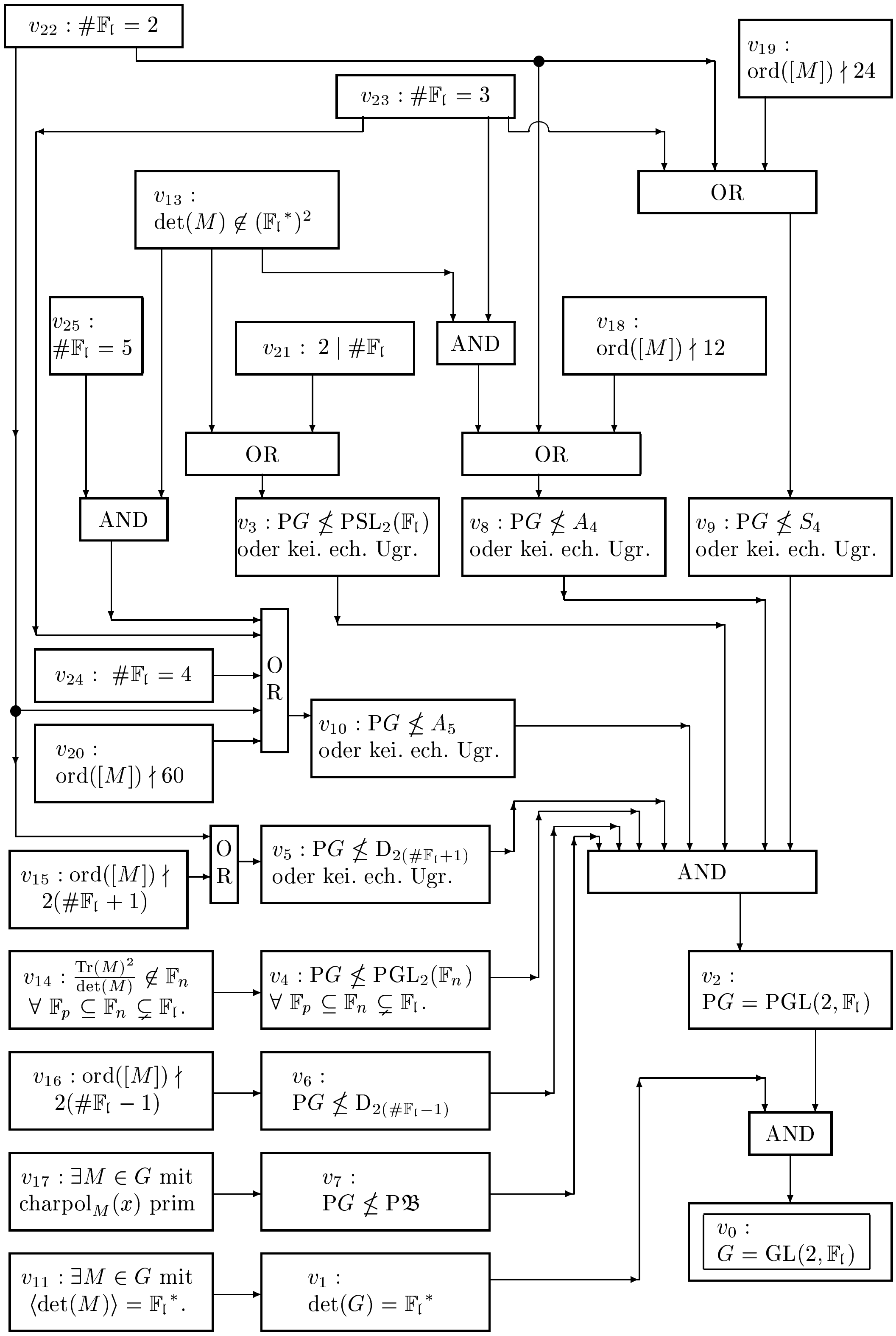
Dies setzen wir alles durch

$$v_3 \wedge v_4 \wedge v_5 \wedge v_6 \wedge v_7 \wedge v_8 \wedge v_9 \wedge v_{10} \quad \Rightarrow \quad v_2$$

und

$$v_2 \wedge v_1 \quad \Rightarrow \quad v_0$$

zusammen.
Zur besseren Veranschaulichung der Knoten und Implikationen geben wir auf Seite 99 ein Bild des Schaltgraphen an.
Da wir Polynome in $\mathbb{F}_q[u]$ aufzählen wollen, wählen wir uns noch eine Numerierung $\mathrm{Nr} : \mathbb{F}_q[u] \to \mathbb{N}_0$. Diese soll bijektiv sein, und für zwei Polynome mit $\deg_u(g) < \deg_u(f)$ soll $\mathrm{Nr}(g) < \mathrm{Nr}(f)$ gelten. Die von uns in der Implementierung gewählte Aufzählung wird auf Seite 104 beschrieben. Zu einem $f(u) \in \mathbb{F}_q[u]$ sei $Nextprime(f)$ das in der obigen Numerierung nächste normierte irreduzible Polynom in $\mathbb{P}_{\mathbb{F}_q[u]}$. Insbesondere ist für $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$ immer $\mathfrak{p} \neq Nextprime(\mathfrak{p})$.
Damit erhalten wir nun den Algorithmus:



Der Schaltgraph von Seite 97

ENTSCHEIDUNGSALGORITHMUS	
Eingabe: Ein Schaltgraph $S = (V, R, f)$, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ und ein Rang-2 Drinfeld-Modul $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$.	
Ausgabe: Die Aussage $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ bzw. $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$	
1)	Setze $\phi := \min(\phi)$
2)	Setze $m := q^{4\deg_T(\mathfrak{l})} + 2\log_q(2 + 2q^{4\deg_T(\mathfrak{l})} + 2\tilde{g})$ (vgl. Satz 5.1.2)
3)	Setze $f(v) := 0$ für alle $v \in V$.
4)	(Verwende Drinfeldtheorie) Berechne $\#\mathbb{F}_{\mathfrak{l}} = q^{4\deg_T(\mathfrak{l})}$ und setze für die entsprechenden Knoten $w \in \{v_{21}, \ldots, v_{25}\}$ die Belegungsfunktion $f(w) := 1$.
5)	$S := SATURIERE(S)$
6)	$\mathfrak{p}(u) := u$
7)	Falls $\Delta \equiv 0 \bmod \mathfrak{p}$ oder $\mathfrak{l}(u) = \mathfrak{p}(u)$ ist, gehe zu Schritt 12.
8)	Berechne das charakteristische Polynom $\mathrm{charpol}_{\mathrm{Frob}_{\mathfrak{p}}}(x) \in \mathbb{F}_{\mathfrak{l}}[x]$.
9)	Berechne $n := \mathrm{ord}_{\mathrm{PGL}(2,\mathbb{F}_{\mathfrak{l}})}([\mathrm{Frob}_{\mathfrak{p}}])$
10)	Setze in Abhängigkeit von $\mathrm{charpol}_{\mathrm{Frob}_{\mathfrak{p}}}(x)$ und n für die entsprechenden v_i die Funktionswerte $f(v_i) := 1$.
11)	$S := SATURIERE(S)$
12)	Setze $\mathfrak{p} := Nextprime(\mathfrak{p})$.
13)	Falls $f(v_0) = 0$ und $\deg_u(\mathfrak{p}) \leqslant m$ ist, gehe zu Schritt 7.
14)	Falls $f(v_0) = 1$ ist, gib aus: $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$. Ist $f(v_0) = 0$, so gib aus: $\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$.

Es sei daran erinnert, daß wir aus der Kenntnis des charakteristischen Polynoms und des Minimalpolynoms von $M \in \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ die Ordnung von $[M]$ in $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$ berechnen können (vgl. Lemma 3.3.7).
Zur Notation im Algorithmus ist zu bemerken, daß wir eigentlich $\mathrm{Frob}_{\mathfrak{P}}$ für eine Stelle $\mathfrak{P}$ von $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]$ über $\mathfrak{p}$ definiert haben. Wir verwenden allerdings nur Eigenschaften von $\mathrm{Frob}_{\mathfrak{P}}$, die lediglich vom Konjugationstyp in $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ abhängen. Daher schreiben wir statt $\mathrm{Frob}_{\mathfrak{P}}$ einfach $\mathrm{Frob}_{\mathfrak{p}}$.
Der Algorithmus erzeugt eine Folge von Schaltgraphen

$$S_i = (V_i, R_i, f_i) \quad ,$$

wobei V_i und R_i sich nicht verändern und die Belegungsfunktion f_i unser Wissen im Schritt i repräsentiert. Die S_{i+1} gehen durch innere oder äußere Transformationen aus den S_i hervor. Die inneren Transformationen treten in den Schritten 5 und 11 auf, die äußeren in den Schritten 4 und 10. Dabei korrespondieren innere Transformationen zu Informationsgewinn, den man durch Verwendung der Untergruppenstruktur von $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ bzw. $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$ erhält. Äußere Transformationen beschreiben den Informationsgewinn, den man aus der Theorie der Drinfeld-Moduln (insbesondere der berechneten Frobeniuselemente) erhält.

Satz 5.3.1. *Der obige Algorithmus terminiert immer und liefert das richtige Ergebnis.*

Beweis: Die Bedingung an den Grad von $\mathfrak{p}$ sichert, daß der Algorithmus immer terminiert.
Der Algorithmus liefert genau dann das richtige Ergebnis, wenn die Äquivalenz

$$\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) \iff \text{Der Knoten } v_0 \text{ nimmt den Wert 1 an, bevor } \deg_u(\mathfrak{p}) > m \text{ wird.}$$

gilt.
Die Richtung von rechts nach links beruht darauf, daß die verwendeten Implikationen aus R korrekt sind.
Betrachten wir nun die Gegenrichtung und setzen $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ voraus. In Satz 3.4.6 haben wir untersucht, wann mögliche maximale Untergruppen der $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$ keine echten Untergruppen sind. Und der Satz 3.4.7 sichert, daß wir jede vorkommende maximale Untergruppe mit unseren Kriterien ausschließen. Der Schluß von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$ auf $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ durch $v_2 \wedge v_1 \Rightarrow v_0$ ist nach Kriterium 3.4.3 erlaubt. Der Satz 5.1.2 sichert, daß man aus jeder Konjugationsklasse von $\mathrm{Gal}(\mathbb{F}_q(u)[_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$ einen Vertreter findet, wenn man die $\mathrm{Frob}_{\mathfrak{p}}$ zu allen $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[T]}$ mit $\deg_u(\mathfrak{p}) \leqslant m$ durchläuft. Da unsere Kriterien nur von der Kenntnis der Konjugationstypen abhängen, wird daher $f(v_0) = 1$, bevor $\deg(\mathfrak{p}) > m$ wird. $\square$

5.4 Erhöhung der Effizienz

Es gibt verschiedene Möglichkeiten, die Effizienz des Algorithmus zu erhöhen. Man kann zum Beispiel die Anzahl der Schaltrelationen erhöhen. Die Isomorphie von $\mathrm{PSL}(2, \mathbb{F}_3)$ zu A_4 bzw. $\mathrm{PSL}(2, \mathbb{F}_5)$ zu A_5 liefert noch die Relationen (siehe Kriterium 3.4.18)

$$\begin{array}{lcl} v_{23} \wedge v_3 \Rightarrow v_8 & , & v_{23} \wedge v_8 \Rightarrow v_3 \\ v_{25} \wedge v_3 \Rightarrow v_{10} & , & v_{25} \wedge v_{10} \Rightarrow v_3 \end{array} .$$

Aus Kriterium 3.4.17 erhalten wir

$$v_{21} \Rightarrow v_9 .$$

Weiter gelten die trivialen Implikationen

$$v_{20} \Rightarrow v_{18} \quad , \quad v_{19} \Rightarrow v_{18} \quad , \quad v_{24} \Rightarrow v_{21} \quad , \quad v_{22} \Rightarrow v_{21} \quad .$$

Als nächsten Schritt kann man erst die Knotenmenge vergrößern und dann neue Schaltrelationen unter Verwendung der neuen Knoten einfügen. Wir haben zum Beispiel noch die folgenden Knoten

v_{30} : $\#\mathbb{F}_{\mathfrak{l}} \not\equiv 0 \bmod 2$
v_{44} : $\exists M \in G$ mit $\mathrm{charpol}_M(x) \in \mathbb{F}_{\mathfrak{l}}[x]$ irreduzibel und $\mathrm{Tr}(M) \neq 0$.
v_{45} : $\exists M \in G$ mit $\mathrm{charpol}_M(x) = (x-a)(x-b)$, $a, b \in \mathbb{F}_{\mathfrak{l}}$, $a \neq b$ und $\mathrm{Tr}(M) \neq 0$.
v_{46} : $\exists M \in G$ mit $\mathrm{v}_p(\mathrm{ord}_{\mathrm{PGL}}[M]) > 0$.

mit den Schaltrelationen

$$v_{30} \wedge v_{46} \Rightarrow v_{15} \quad , \quad v_{30} \wedge v_{46} \Rightarrow v_{16} \quad , \quad v_{30} \wedge v_1 \Rightarrow v_{13}$$
$$v_{30} \wedge v_{11} \Rightarrow v_{13} \quad , \quad v_{44} \wedge v_{17} \Rightarrow v_{13}$$

ergänzt. Weiter liefert Kriterium 3.4.12

$$v_{44} \Rightarrow v_6$$

und Kriterium 3.4.13

$$v_{45} \Rightarrow v_5 \quad .$$

Die letzten beiden Schaltungen haben den Vorteil, daß wir mit ihnen die Diedergruppen ausschließen können, ohne die Ordnung des Frobeniuselements berechnen zu müssen.
Als dritte Möglichkeit können wir den vierten Schritt im Algorithmus ausbauen. Dort können wir die Resultate über Drinfeld-Moduln aus Kapitel 4 verwenden, um bestimmte Knoten im Schaltgraphen von vorneherein auf Eins zu setzen. Wir haben uns in Satz 4.4.11 bereits überlegt, daß in sehr vielen Fällen die Determinantendarstellung surjektiv ist. Daher ersetzen wir Schritt 4 im Algorithmus durch

Erweiterung von Schritt 4	
4a)	Berechne $\#\mathbb{F}_{\mathfrak{l}}$ und setze die entsprechenden Knoten im Schaltgraph auf Eins.
4b)	Betrachte $\psi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \Delta\tau)$ und berechne $\min(\psi) = (\mathbb{F}_q, \mathbb{F}_q(u), u, u - \tilde{\Delta}\tau)$.
4c)	Falls $\tilde{\Delta} \not\equiv 0 \bmod \mathfrak{l}(u)$, so setze v_1 auf Eins.

Dank der Relationen $v_{30} \wedge v_1 \Rightarrow v_{13}$ und $v_{13} \Rightarrow v_3$ kann dann in ungerader Charakteristik die $\mathrm{PSL}(2, \mathbb{F}_{\mathfrak{l}})$ bereits ausgeschlossen werden, ohne einen Frobenius berechnen zu müssen. Und in gerader Charakteristik ist ja $\mathrm{PSL}(2, \mathbb{F}_{\mathfrak{l}}) = \mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$, was im Schaltgraph durch die Relation $v_{21} \Rightarrow v_3$ repräsentiert wird. Nach Kriterium 3.4.17 können wir noch ergänzen:

Erweiterung von Schritt 4	
4d)	Ist $\mathrm{char}(\mathbb{F}_{\mathfrak{l}}) = 2$ und $\mathrm{v}_p(\#\mathbb{F}_{\mathfrak{l}}) \equiv 1 \bmod 2$, so setze $v_8 = 1$.
4e)	Ist $\mathrm{char}(\mathbb{F}_{\mathfrak{l}}) \neq 5$ und $(\#\mathbb{F}_{\mathfrak{l}})^2 \not\equiv 1 \bmod 5$, so setze $v_{10} = 1$.

Die Tate-Uniformisierung (Korollar 4.7.6) liefert uns weiter

Erweiterung von Schritt 4	
4f)	Falls ein $\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]}$ existiert mit $\mathrm{v}_{\mathfrak{p}}(j(\phi)) < 0$ und $\mathrm{ggT}(\#\mathbb{F}_{\mathfrak{l}}, \mathrm{v}_{\mathfrak{p}}(j(\phi)) \neq \#\mathbb{F}_{\mathfrak{l}}$, so setze $v_{46} = 1$.

5.5 Zur Struktur des Algorithmus

Die Einführung des Begriffs des Schaltgraphen ermöglicht es, die gruppentheoretischen Anteile von denen aus der Theorie der Drinfeld-Moduln zu trennen. Dadurch können neue theoretische Erkenntnisse leicht in den bestehenden Algorithmus integriert werden.
Es ist nicht nötig, daß im Schaltgraphen alle Knoten auf Eins gesetzt werden, um die Surjektivität der Torsionsdarstellung zu zeigen. Dies ist angenehm, da wir nicht sagen können, in welcher Reihenfolge Frobeniuselemente mit bestimmten Eigenschaften auftreten. Der Satz von Chebotarev liefert uns nur eine Heuristik, um die Häufigkeit des Auftretens bestimmter Elemente zu schätzen. Den Informationsstand im Algorithmus kann man in jedem Schritt an der Belegungsfunktion ablesen. Ein weiterer Vorteil des Schaltgraphen ist, daß sich Spezialfälle ($\mathrm{char}(\mathbb{F}_q) = 2$ oder $\#\mathbb{F}_{\mathfrak{l}}$ klein) transparent in den Algorithmus integrieren lassen, ohne die Gesamtstruktur ändern zu müssen. Zum Beispiel ist im allgemeinen das Kriterium zum Knoten

$$v_{45}: \quad \exists M \in G \text{ mit } \mathrm{charpol}_M(x) = (x-a)(x-b), a, b \in \mathbb{F}_{\mathfrak{l}}, a \neq b \text{ und } \mathrm{Tr}(M) \neq 0$$

effizienter als

$$v_{16}: \quad \exists M \in G \text{ mit } 2(\#\mathbb{F}_{\mathfrak{l}} - 1) \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M]) ,$$

um die maximale Untergruppe $\mathrm{D}_{2(\#\mathbb{F}_{\mathfrak{l}}-1)}$ auszuschließen. Allerdings ist im Fall $\mathbb{F}_{\mathfrak{l}} = \mathbb{F}_3$ das Polynom $x^2+2 = (x-1)(x-2)$ das einzige quadratische Polynom mit zwei verschiedenen Nullstellen ungleich Null. Daher erfüllt kein $M \in \mathrm{GL}(2, \mathbb{F}_3)$ die Aussage des Knotens v_{45}. Im Fall $\phi = (\mathbb{F}_3, \mathbb{F}_3(u), u, u+g\tau+\Delta\tau^2)$ und $\deg_T(\mathfrak{l}) = 1$ muß die $\mathrm{D}_{2(\#\mathbb{F}_{\mathfrak{l}}-1)}$ daher mittels v_{16} ausgeschlossen werden.
Auch die Fälle, daß für kleine endliche Körper mögliche maximalen Untergruppen (siehe Satz 3.4.4) keine echten Untergruppen von $\mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$ sind, konnten leicht in den Algorithmus integriert werden.

5.6 Zur Implementierung

Wir haben den Algorithmus im Computeralgebrasystem Simath [Sim] implementiert und verschiedene Berechnungen durchgeführt.
Dabei haben wir folgendes ausgenutzt: Sei ϕ ein fest vorgebener Drinfeld-Modul. Dann kann jeder Stelle $\mathfrak{p}(u) \in \mathbb{P}_{\mathbb{F}_q[u]}$ guter Reduktion das Polynom $\mathcal{P}_{\mathrm{Dred}(\phi,\mathfrak{p})} \in (\mathbb{F}_q[T])[X]$ zugeordnet werden. Zu einem beliebigen $\mathfrak{l}(T)$ aus $\mathbb{P}_{\mathbb{F}_q[T]}$ erhält man

das charakteristische Polynom des Frobenius $\mathrm{Frob}_{\mathfrak{p}}$ zur Stelle $\mathfrak{p}(u) \neq \mathfrak{l}(u)$ in der Erweiterung $\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi]|\mathbb{F}_q(u)$ nach Korollar 4.1.2 durch

$$\mathrm{charpol}(\mathrm{Frob}_{\mathcal{P}}) = red(\mathcal{P}_{\mathrm{Dred}(\phi,\mathfrak{p})}, \mathfrak{l}) \in (\mathbb{F}_q[T]/\mathfrak{l}(T))[X] \; .$$

Will man ganze Serien von Beispielen berechnen, so bietet es sich daher an, zu einem Drinfeld-Modul ϕ zuerst alle $\mathcal{P}_{\mathrm{Dred}(\phi,\mathfrak{p})}$ bis zu einer bestimmten Schranke zu berechnen und erst danach damit anzufangen, die Führer $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ zu durchlaufen.
Wir haben in Bemerkung 4.1.9 bereits darauf hingewiesen, daß es teuer ist, die Ordnung des Frobeniuselements zu berechnen. Daher haben wir meist darauf verzichtet. Dank der auf Seite 102 angegebenen Relationen können für $\#\mathbb{F}_{\mathfrak{l}} > 3$ die Diedergruppen ausgeschlossen werden, ohne Elementordnungen berechnen zu müssen. Um diesen ($\#\mathbb{F}_{\mathfrak{l}} \leqslant 3$) und ähnliche Sonderfälle für kleine Gruppen $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ abzufangen, haben wir für $\#\mathbb{F}_{\mathfrak{l}} < 20$ den Wert von $\mathrm{ord}_{\mathrm{PGL}}(\mathrm{Frob}_{\mathfrak{p}})$ berechnet. In solchen Gruppen sind die Ordnungen noch so klein, daß ihre Berechnung keine Laufzeitprobleme bringt. Für $\#\mathbb{F}_{\mathfrak{l}} > 20$ haben wir der Laufzeit zuliebe auf die Information $\mathrm{ord}_{\mathrm{PGL}}(\mathrm{Frob}_{\mathfrak{p}})$ verzichtet. In diesen Fällen ist die Gruppe $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ bereits so groß, daß genügend viele verschiedene charakteristische Polynome auftreten, um die Knoten zu erfüllen. Daher benötigt der Algorithmus in diesen Fällen keine Elementordnungen.
Lediglich um die Gruppen A_4, S_4, A_5 auszuschließen, werden Teilinformationen über Elementordnungen benötigt. Es müssen Elemente der Ordnung größer $3, 4$ bzw. 6 existieren. Daher haben wir in Abhängigkeit von der Belegung der Knoten v_8, v_9, v_{10} (der Knoten, die zu A_4, S_4, A_5 korrespondieren) getestet, ob die Ordnung eines vorliegenden Elements größer $3, 4$ bzw. 6 ist.
Drinfeld-Moduln mit komplexer Multiplikation haben wir bei unseren Berechnungen von vorneherein ausgespart. Dies ist leicht zu bewerkstelligen, da man nur testen muß, ob die j-Invariante in der Liste 4.3.1 vorkommt.
Wir geben noch die von uns gewählte Ordnung auf $\mathbb{F}_q[T]$ (bzw. $\mathbb{F}_q[u]$) an. Der Primkörper $\mathbb{F}_p$ sei durch die Elemente $\{0, 1, \ldots, p-1\} \subset \mathbb{N}_0$ repräsentiert und durch die übliche Relation “$<$” geordnet. Für $f(y), g(y) \in \mathbb{F}_p[y]$ definieren wir dann

$$f(y) \lessdot g(y) :\Longleftrightarrow \; \mathrm{coeff}_y(\deg_y(f-g), f) < \mathrm{coeff}_y(\deg_y(f-g), g)$$

Ein Polynom vom Grad d ist also immer kleiner als ein Polynom vom Grad $(d+1)$. In $(\mathbb{Z}/7\mathbb{Z})[y]$ gilt zum Beispiel

$$0 \;\lessdot\; 6y^2 \;\lessdot\; y^3 + 3y^2 + 6y \lessdot\; y^3 + 5y^2 + y \lessdot\; 2y^3 \lessdot\; 2y^3 + 1 \quad .$$

Den Körper $\mathbb{F}_q = \mathbb{F}_{p^d}$ repräsentieren wir durch

$$\mathbb{F}_q = {}^{\mathbb{F}_p[y]}\!/_{h(y)} \quad ,$$

wobei $h(y)$ das bezüglich "$\lessdot$" minimale normierte irreduzible Polynom vom Grad d in $\mathbb{F}_p[y]$ bezeichnet. Die Elemente von $\mathbb{F}_q$ sind dann gegeben durch $\{f(y) \mid \deg_y(f) < d\}$ und werden durch "$\lessdot$" linear angeordnet. Seien nun $\alpha(T), \beta(T) \in \mathbb{F}_q[T]$. Dann definieren wir

$$\alpha(T) \prec \beta(T) :\Longleftrightarrow \operatorname{coeff}_T(\deg_T(\alpha-\beta),\alpha) \lessdot \operatorname{coeff}_T(\deg_T(\alpha-\beta),\beta) \quad .$$

Diese Ordnung bezeichnen wir als die lexikographische Ordnung auf dem Polynomring. Wir definieren

$$\operatorname{Nr}(\beta) := \#\{\alpha \in \mathbb{F}_q[T] \mid \alpha \prec \beta\}$$

und

$$\operatorname{Nrred}(\beta) := \#\{\alpha \in \mathbb{F}_q[T] \mid \alpha \in \mathbb{P}_{\mathbb{F}_q[T]}, \alpha \preceq \beta\} \ .$$

Es ist also $\operatorname{Nr}(0) = 0$, $\operatorname{Nr}(T) = q$ und $\operatorname{Nrred}(T) = 1$.
Die Konstante m aus Schritt 2 des Algorithmus ist so groß, daß es nicht praktikabel ist, alle Stellen vom Grad kleiner m zu durchlaufen. In unseren Berechnungen hat sich gezeigt, daß es genügt, eine deutlich kleinere Schranke $\tilde{m}$ (in der Größenordnung von 60) zu wählen. Da die Anzahl der Typen maximaler Untergruppen der $\mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$ (und die Anzahl der Knoten im Schaltgraph) unabhängig von der Größe von $\mathbb{F}_\mathfrak{l}$ ist, überrascht es nicht, daß $\tilde{m}$ in der Praxis auch unabhängig von $\#\mathbb{F}_\mathfrak{l}$ gewählt werden kann. Dabei ist natürlich klar, daß man Drinfeld-Moduln konstruieren kann, die an einer vorgegebenen endlichen Menge von Stellen schlechte Reduktion haben. Solche Drinfeld-Moduln haben aber zwangsläufig Koeffizienten sehr großen Grades. Da wir nur Drinfeld-Moduln mit Koeffizienten kleinen Grades betrachtet haben, haben für uns die 60 Stellen immer genügt. In allen Fällen, in denen der Algorithmus nach 60 Schritten die Maximalität der Galoisgruppe (d.h. die Surjektivität der zugehörigen Torsionsdarstellung) nicht zeigen konnte und die von uns „von Hand" untersucht wurden, konnten wir auch beweisen, daß die Darstellung nicht maximal war (siehe dazu die Einzelbeispiele im nächsten Kapitel). In den nicht-maximalen Fällen konnten wir an der Belegung des Schaltgraphen nach Beendigung des Algorithmus recht genau ablesen, wie die Galoisgruppe aussehen sollte.
Es sei noch einmal betont, daß nach der Wahl eines konstanten Wertes für $\tilde{m}$ anstelle von m der Algorithmus nur noch die Ergebnisse

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$$

oder

> Die Gleichheit von $\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u))$ und $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$
> konnte nicht gezeigt werden.

liefert. Er kann dann nicht zeigen, daß die beiden Gruppen ungleich sind.

Die Berechnungen großer Beispielserien zeigen, daß einige Symmetrien vorliegen. Wir betrachten die affine Gruppe

$$\mathrm{Aff} := \left\{ \begin{array}{cccc} A_{a,b} & : & \mathbb{F}_q & \to & \mathbb{F}_q \\ & & x & \mapsto & ax+b \end{array} \mid a,b \in \mathbb{F}_q,\ a \neq 0 \right\} \quad .$$

Diese operiert auf $\mathbb{F}_q[T]$ durch

$$A_{a,b} \star f(T) := \frac{f(aT+b)}{a^{\deg_T(f)}} \quad .$$

Auf den Drinfeld-Moduln operiert sie durch

$$\begin{aligned} & A_{a,b} \star (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g(u)\tau + \Delta(u)\tau^2) \\ & := \left(\mathbb{F}_q, \mathbb{F}_q(u), u, u + \frac{g(au+b)}{a}\tau + \frac{\Delta(au+b)}{a}\tau^2 \right) \quad . \end{aligned}$$

Aus dem jeweiligen Zusammenhang wird immer klar sein, welche der beiden obigen Operationen durch das Symbol $\star$ bezeichnet wird.
Es gilt:

Lemma 5.6.1. *Sei* $A \in \mathrm{Aff}$, $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g(u)\tau + \Delta(u)\tau^2)$ *und* $\mathfrak{n}(T) \in \mathbb{F}_q[T]$. *Dann ist*

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{n}}\phi], \mathbb{F}_q(u)) = \mathrm{Gal}(\mathbb{F}_q(u)[{}_{A\star\mathfrak{n}}(A\star\phi)], \mathbb{F}_q(u)) \ .$$

Beweis: Es sei $A = A_{a,b}$. Wir betrachten den Koordinatenwechsel

$$\mathbb{F}_q(u) \to \mathbb{F}_q(u), \quad f(u) \mapsto f(au+b)$$

und den dadurch induzierten $\mathbb{F}_q$-Algebren-Homomorphismus

$$\begin{array}{cccc} \varphi : & \mathbb{F}_q(u)\{\tau\} & \to & \mathbb{F}_q(u)\{\tau\} \\ & \sum_{i=0}^n a_i(u)\ \tau^i & \mapsto & \sum_{i=0}^n a_i(au+b)\ \tau^i \end{array} \quad .$$

Die Abbildung φ kommutiert auf $\mathbb{F}_q(u)\{\tau\}$ mit dem Einsetzungshomomorphismus (Einsetzen in x, wobei $\tau = x^q$ ist). Dann ist

$$\begin{aligned} \varphi(\phi_T) &= \varphi(u + g(u)\tau + \Delta(u)\tau^2) \\ &= (au+b) + g(au+b)\tau + \Delta(au+b)\tau^2 \\ &= (A\star\phi)_{aT+b} \quad . \end{aligned}$$

Damit erhalten wir für $\mathfrak{n}(T) = \sum_{i=0}^n c_i T^i$

$$\begin{aligned} \varphi(\phi_{\mathfrak{n}(T)}(\tau)) &= \sum_{i=0}^n \varphi(c_i)\varphi({\phi_T}^i) = \sum_{i=0}^n c_i(\varphi(\phi_T))^i \\ &= \sum_{i=0}^n c_i((A\star\phi)_{aT+b})^i = (A\star\phi)_{\sum_{i=0}^n c_i(aT+b)^i} \\ &= a^{\deg_T(\mathfrak{n})} \cdot (A\star\phi)_{A\star\mathfrak{n}}(\tau) \quad . \end{aligned}$$

Für alle $d \in \mathbb{F}_q{}^*, \mathfrak{m} \in \mathbb{F}_q[T]$ gilt

$$_{d \cdot \mathfrak{m}}(A \star \phi) = {}_{\mathfrak{m}}(A \star \phi) \quad ,$$

so daß der Faktor $a^{\deg_T(\mathfrak{n})}$ keinen Einfluß auf die Torsionserweiterung hat. Da φ den Körper $\mathbb{F}_q(u)$ festläßt, folgt die Aussage. $\square$

Wir haben die Operation $\star$ so normiert, daß die Menge der normierten Polynome von $\mathbb{F}_q[T]$ unter $\star$ abgeschlossen ist. Damit operiert Aff auf den Paaren $(\phi, \mathfrak{l}(T))$ mit $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, und die zugehörigen Torsionserweiterungen sind invariant unter dieser Operation.

Kapitel 6

Beispiele

6.1 Serien

Für $q = 2, 3, 4, 5$ haben wir größere Bereiche von Drinfeld-Moduln ϕ und primen Führern $\mathfrak{l}$ abgesucht. Alle Rechnungen wurden auf einem handelsüblichen PC mit Pentium III Prozessor mit 550 MHz durchgeführt. Die gefundenen Ergebnisse sind in den folgenden Tabellen zusammengefaßt.
Zu jedem q geben wir zwei Tabellen an. In der ersten Tabelle beschreiben wir, welcher Bereich abgesucht wurde und wie sich der Algorithmus verhielt.
In der zweiten Tabelle beleuchten wir die Fälle genauer, in denen die Surjektivität der Galoisdarstellung nicht gezeigt werden konnte. Wir geben an, in wievielen Fällen ein Knoten $[i]$ des Schaltgraphen nach Beendigung des Algorithmus noch den Wert 0 hatte. Dies gibt uns einen Hinweis, wie oft die Galoisgruppe in einer Untergruppe vom betrachteten Typ lag. Zur besseren Lesbarkeit haben wir zu jedem Knoten $[i]$ seine Bedeutung kurz angedeutet. Die exakte Bedeutung der einzelnen Knoten ist in der Definition des Schaltgraphen auf Seite 97 zu finden.
Es sei nochmal darauf hingewiesen, daß die Werte in der Tabelle angeben, in wieviel Fällen der entsprechende Knoten *nicht* erfüllt war.
In den Tabellen fällt auf, daß im allgemeinen sehr wenig Stellen benötigt werden, um die Maximalität der Torsionserweiterung zu zeigen. Dies durch eine genaue Analyse des Algorithmus zu erklären wäre extrem aufwendig, und daher verzichten wir hier darauf. Stattdessen werden wir einige heuristische Argumente anführen, um das Verhalten des Algorithmus zu erklären. Dazu schicken wir das folgende Lemma vorweg.

Lemma 6.1.1. *Es seien* $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$ *und* $M_1, M_2, M_3, M_4 \in \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ *mit*

(i) $\frac{q^{\deg_T(\mathfrak{l})}-1}{q-1}$ *besitzt einen Primteiler ungleich* $2, 3$ *oder* 5*,*

(ii) $\mathrm{charpol}(M_1)$ *ist irreduzibel und* $\mathrm{Tr}(M_1) \neq 0$*,*

(iii) $\mathrm{charpol}(M_2)$ *hat zwei verschiedene Nullstellen in* $\mathbb{F}_\mathfrak{l}$ *und* $\mathrm{Tr}(M_2) \neq 0$*,*

(iv) $\frac{\mathrm{Tr}(M_3)^2}{\det(M_3)}$ *liegt in keinem echten Teilkörper von* $\mathbb{F}_{\mathfrak{l}}$*,*

(v) $\langle \det(M_4) \rangle = {\mathbb{F}_{\mathfrak{l}}}^*$.

Dann zeigt der Algorithmus von Seite 97ff , daß

$$\langle M_1, M_2, M_3, M_4 \rangle = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$$

ist.

Beweis: Wegen (ii) gilt im Schaltgraph $v_{17} = 1$ und $v_{44} = 1$. Mit (v) ergibt sich $v_{11} = 1$ und $v_{13} = 1$. Aus (i) in Verbindung mit (v) folgt $v_{18} = 1$, $v_{19} = 1$, $v_{20} = 1$. Die Bedingung (iii) liefert $v_{45} = 1$, und wegen (iv) ist $v_{14} = 1$. Saturiert man nun den Schaltgraphen, so erhält man $v_0 = 1$. □

Es ist plausibel anzunehmen, daß in den meisten Fällen Bedingung (i) erfüllt ist. Mit Hilfe der Daten über die Konjugationsklassen der $\mathrm{GL}(2, \mathbb{F}_r)$ aus der Tabelle von Seite 44 erhält man direkt:

$$\begin{aligned} &\#\{M \in \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) \mid \mathrm{charpol}(M) \text{ hat zwei verschiedene Nullstellen und } \mathrm{Tr}(M) \neq 0\} \\ &\qquad = \begin{cases} \frac{1}{2}\#\mathbb{F}_{\mathfrak{l}}\ (\#\mathbb{F}_{\mathfrak{l}} - 1)\ (\#\mathbb{F}_{\mathfrak{l}} - 3)\ (\#\mathbb{F}_{\mathfrak{l}} + 1) & ; \quad q \not\equiv 0 \bmod 2 \\ \frac{1}{2}\#\mathbb{F}_{\mathfrak{l}}\ (\#\mathbb{F}_{\mathfrak{l}} - 1)\ (\#\mathbb{F}_{\mathfrak{l}} - 2)\ (\#\mathbb{F}_{\mathfrak{l}} + 1) & ; \quad q \equiv 0 \bmod 2 \end{cases} \\ &\qquad \approx \frac{1}{2}\ (\#\mathbb{F}_{\mathfrak{l}})^4 \end{aligned}$$

$$\begin{aligned} &\#\{M \in \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) \mid \mathrm{charpol}(M) \text{ ist irreduzibel und } \mathrm{Tr}(M) \neq 0\} \\ &\qquad = \begin{cases} \frac{1}{2}\ \#\mathbb{F}_{\mathfrak{l}}\ (\#\mathbb{F}_{\mathfrak{l}} - 1)^3 & ; \quad q \not\equiv 0 \bmod 2 \\ \frac{1}{2}\ {\#\mathbb{F}_{\mathfrak{l}}}^2\ (\#\mathbb{F}_{\mathfrak{l}} - 1)^2 & ; \quad q \equiv 0 \bmod 2 \end{cases} \\ &\qquad \approx \frac{1}{2}\ (\#\mathbb{F}_{\mathfrak{l}})^4 \end{aligned}$$

Weiter ist

$$\begin{aligned} \#\{M \in \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}}) \mid \langle \det(M) \rangle = {\mathbb{F}_{\mathfrak{l}}}^*\} &= \varphi(\#\mathbb{F}_{\mathfrak{l}} - 1) \cdot \#\mathrm{SL}(2, \mathbb{F}_{\mathfrak{l}}) \\ &= \varphi(\#\mathbb{F}_{\mathfrak{l}} - 1) \cdot \#\mathbb{F}_{\mathfrak{l}} \cdot ({\#\mathbb{F}_{\mathfrak{l}}}^2 - 1) \quad , \end{aligned}$$

wobei hier $\varphi(n)$ die Eulersche φ-Funktion bezeichnet. Wir nehmen an, daß ein Element der Form $\frac{\mathrm{Tr}(M_3)^2}{\det(M_3)}$ etwa mit der gleichen Wahrscheinlichkeit in einem echten Teilkörper liegt wie ein beliebig gewähltes Element aus $\mathbb{F}_{\mathfrak{l}}$.
Der Satz von Chebotarev liefert, daß die Wahrscheinlichkeit, an einer Stelle $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$ ein Element einer bestimmten Form zu finden, etwa so hoch ist wie die Wahrscheinlichkeit, ein solches Element zu erhalten, wenn man zufällig aus der $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$ auswählt. Die obigen Überlegungen haben gezeigt, daß zu jeder

Bedingung aus Lemma 6.1.1 in der $\mathrm{GL}(2,\mathbb{F}_{\mathfrak{l}})$ sehr viele Elemente existieren, die diese Bedingung erfüllen. Insbesondere gibt es auch viele Matrizen, die zwei oder drei der Bedingungen gleichzeitig erfüllen.
Daher ist es nicht überraschend, daß meistens nur wenige Frobeniuselemente benötigt werden, um die Surjektivität der Torsionsdarstellung zu zeigen.
Es ist klar, daß die obigen Argumente nur sehr grobe Heuristiken sind, und daß die Argumentation (abgesehen von der Aussage des Lemmas) keinen Anspruch auf mathematische Exaktheit erhebt.
In vielen Fällen reicht sogar die Betrachtung eines einzigen $\mathrm{Frob}_{\mathfrak{p}}$, um die Surjektivität zu zeigen. Dies wollen wir durch das folgende Lemma erklären.

Lemma 6.1.2. *Sei* $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g(u)\tau + \Delta(u)\tau^2)$, $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$, $p = \mathrm{char}(\mathbb{F}_q)$ *und* $M \in \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$. *Weiter gelte:*

(i) $\mathrm{char}(\mathbb{F}_q) \neq 2$,

(ii) $\mathrm{ggT}(\Delta, \mathfrak{l}(u)) = 1$,

(iii) $\exists \mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]}$, *mit* $\mathrm{v}_{\mathfrak{p}}(j(\phi)) < 0$ *und* $\mathrm{ggT}(q^{\deg_T(\mathfrak{l})}, \mathrm{v}_{\mathfrak{p}}(j(\phi))) \neq q^{\deg_T(\mathfrak{l})}$,

(iv) $\mathrm{charpol}_M(x) \in \mathbb{F}_{\mathfrak{l}}[x]$ *irreduzibel,*

(v) $\mathbb{F}_p\left(\frac{\mathrm{Tr}(M)^2}{\det(M)}\right) = \mathbb{F}_{\mathfrak{l}}$,

(vi) $120 \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M])$.

Dann zeigt der Algorithmus, daß

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$$

gilt.

Beweis: Sei $G = \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$. Da $\mathrm{ggT}(\Delta, \mathfrak{l}(u)) = 1$ ist, ist $\det(G) = \mathbb{F}_{\mathfrak{l}}{}^*$ und damit $\mathrm{P}G \not\leq \mathrm{PSL}(2, \mathbb{F}_{\mathfrak{l}})$. Die Tate-Uniformisierung liefert uns, daß wegen *(iii)* ein $N \in G$ mit $\mathrm{ord}_{\mathrm{PGL}}([N]) \equiv 0 \bmod p$ existiert. Mit $\mathrm{char}(\mathbb{F}_q) \neq 2$ folgt daraus $\mathrm{P}G \not\leq \mathrm{D}_{2(\#\mathbb{F}_{\mathfrak{l}}-1)}$ und $\mathrm{P}G \not\leq \mathrm{D}_{2(\#\mathbb{F}_{\mathfrak{l}}+1)}$. Da $\mathrm{charpol}_M(x)$ irreduzibel ist, liegt $\mathrm{P}G$ nicht in einer projektiven Borelgruppe, und $\mathbb{F}_p\left(\frac{\mathrm{Tr}(M)^2}{\det(M)}\right) = \mathbb{F}_{\mathfrak{l}}$ zeigt, daß $\mathrm{P}G$ nicht in einer $\mathrm{PGL}(2, \mathbb{F}_r)$ für einen echten Teilkörper $\mathbb{F}_r$ von $\mathbb{F}_{\mathfrak{l}}$ liegt. Die letzte Bedingung $120 \not\equiv 0 \bmod \mathrm{ord}_{\mathrm{PGL}}([M])$ sichert, daß $\mathrm{P}G$ nicht in A_4, S_4 oder A_5 liegen kann.
Insgesamt folgt, daß $\mathrm{P}G = \mathrm{PGL}(2, \mathbb{F}_{\mathfrak{l}})$ ist, und mit $\det(G) = \mathbb{F}_{\mathfrak{l}}{}^*$ ergibt sich $G = \mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$. $\square$

Für $\mathrm{char}(\mathbb{F}_q) = 2$ läßt sich ein entsprechendes Lemma angeben.

Beispiel 6.1.3.

	$\mathbb{F}_2$
Betrachtete $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ (keine CM)	$0 \leqslant \deg(g) \leqslant 4$, $0 \leqslant \deg(\Delta) \leqslant 8$
Anzahl ϕ mit CM	562
Betrachtete Führer $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$	$1 \leqslant \deg(\mathfrak{l}) \leqslant 6$
Anzahl der Führer	$2+1+2+3+6+9 = 23$
Anzahl der $(\phi, \mathfrak{l})$	363170
Gal $\neq$ GL$(2, \mathbb{F}_\mathfrak{l})$	601
$\deg(\mathfrak{l}) = 1$	574
$\deg(\mathfrak{l}) = 2$	27
Laufzeit	1334 min
Durchschnitt für ein $(\phi, \mathfrak{l})$	0.22 sec
Maximal betrachtete Frob$_\mathfrak{p}$	60
Maximal benötigte Frob$_\mathfrak{p}$	29
$1 - 5$	275 679
$6 - 10$	80 296
$11 - 15$	6164
$16 - 20$	390
$21 - 25$	34
$26 - 30$	6

$q = 2$	Gal$(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq$ GL$(2, \mathbb{F}_\mathfrak{l})$		
	Kurzbeschreibung	$\deg_T(\mathfrak{l}) = 1$	$\deg_T(\mathfrak{l}) = 2$
[0]	$G = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$	574	27
[1]	$\det(G) = \mathbb{F}_\mathfrak{l}^*$	0	0
[2]	$\mathrm{P}G = \mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$	574	27
[3]	$\mathrm{P}G \not\leqslant \mathrm{PSL}(2, \mathbb{F}_\mathfrak{l})$	0	0
[4]	$\mathrm{P}G \not\leqslant \mathrm{PGL}(2, \mathbb{F}_{q^i})$	574	22
[5]	$\mathrm{P}G \not\leqslant D_{2(\#\mathbb{F}_\mathfrak{l}+1)}$	0	5
[6]	$\mathrm{P}G \not\leqslant D_{2(\#\mathbb{F}_\mathfrak{l}-1)}$	574	22
[7]	$\mathrm{P}G \not\leqslant PBorel$	574	22
[8]	$\mathrm{P}G \not\leqslant A_4$	0	22
[9]	$\mathrm{P}G \not\leqslant S_4$	0	0
[10]	$\mathrm{P}G \not\leqslant A_5$	0	0

Es sei noch mal darauf hingewiesen, daß die Werte in der unteren Tabelle angeben, in wievielen Fällen der entsprechende Knoten nicht erfüllt war.

□

Beispiel 6.1.4.

	$\mathbb{F}_4$
Betrachtete $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ (keine CM)	$0 \leqslant \deg(g) \leqslant 1$, $0 \leqslant \deg(\Delta) \leqslant 4$
Anzahl ϕ mit CM	1041
Betrachtete Führer $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$ Anzahl der Führer	$1 \leqslant \deg(\mathfrak{l}) \leqslant 4$ $4 + 6 + 20 + 60 = 90$
Anzahl der $(\phi, \mathfrak{l})$	1 381 050
$\mathrm{Gal} \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ $\deg(\mathfrak{l}) = 1$ $\deg(\mathfrak{l}) = 2$ $\deg(\mathfrak{l}) = 3$ $\deg(\mathfrak{l}) = 4$	1566 504 162 0 900
Laufzeit Durchschnitt für ein $(\phi, \mathfrak{l})$	2207 min 0.09 sec
Maximal betrachtete $\mathrm{Frob}_\mathfrak{p}$	60
Maximal benötigte $\mathrm{Frob}_\mathfrak{p}$ $1 - 5$ $6 - 10$ $11 - 15$ $16 - 20$ $21 - 25$	24 1 164 080 199 819 14 738 790 57

$q = 4$	$\mathrm{Gal}(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$				
	Kurzbeschreibung	$\deg_T(\mathfrak{l}) = 1$	$\deg_T(\mathfrak{l}) = 2$	$\deg_T(\mathfrak{l}) = 3$	$\deg_T(\mathfrak{l}) = 4$
[0]	$G = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$	504	162	0	900
[1]	$\det(G) = {\mathbb{F}_\mathfrak{l}}^*$	300	90	0	900
[2]	$PG = \mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$	216	72	0	0
[3]	$PG \nleqslant \mathrm{PSL}(2, \mathbb{F}_\mathfrak{l})$	0	0	0	0
[4]	$PG \nleqslant \mathrm{PGL}(2, \mathbb{F}_{q^i})$	156	0	0	0
[5]	$PG \nleqslant D_{2(\#\mathbb{F}_\mathfrak{l}+1)}$	60	0	0	0
[6]	$PG \nleqslant D_{2(\#\mathbb{F}_\mathfrak{l}-1)}$	156	72	0	0
[7]	$PG \nleqslant PBorel$	156	72	0	0
[8]	$PG \nleqslant A_4$	156	0	0	0
[9]	$PG \nleqslant S_4$	0	0	0	0
[10]	$PG \nleqslant A_5$	0	0	0	0

Die Tabellen unterstützen die Vermutung, daß nichtmaximale Erweiterungen nur für kleine Grade von $\deg_T(\mathfrak{l})$ auftreten. Die Fälle vom Grad 4 sollten sich dadurch erklären lassen, daß der assoziierte Rang-1 Modul keine maximale $\mathfrak{l}$-Torsionserweiterung besitzt. Es handelt sich also um einen Effekt, der nicht von den Rang-2 Moduln, sondern von den Rang-1 Moduln herrührt. □

Beispiel 6.1.5.

	$\mathbb{F}_3$
Betrachtete $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ (keine CM)	$g = u$, $0 \leqslant \deg(\Delta) \leqslant 8$
Anzahl ϕ mit CM	0
Betrachtete Führer $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$ Anzahl der Führer	$1 \leqslant \deg(\mathfrak{l}) \leqslant 4$ $3 + 3 + 8 + 18 = 32$
Anzahl der $(\phi, \mathfrak{l})$	629824
Gal $\neq$ GL$(2, \mathbb{F}_\mathfrak{l})$ $\deg(\mathfrak{l}) = 1$ $\deg(\mathfrak{l}) = 2$ $\deg(\mathfrak{l}) = 3$	264 155 5 104
Laufzeit Durchschnitt für ein $(\phi, \mathfrak{l})$	1052 min 0.10 sec
Maximal betrachtete Frob$_\mathfrak{p}$	60
Maximal benötigte Frob$_\mathfrak{p}$ $1 - 5$ $6 - 10$ $11 - 15$ $16 - 20$ $21 - 25$	23 599 362 29276 6279 876 6

$q = 3$	Gal$(\mathbb{F}_q(u)[{}_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq$ GL$(2, \mathbb{F}_\mathfrak{l})$			
	Kurzbeschreibung	$\deg_T(\mathfrak{l}) = 1$	$\deg_T(\mathfrak{l}) = 2$	$\deg_T(\mathfrak{l}) = 3$
[0]	$G = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$	155	5	104
[1]	$\det(G) = \mathbb{F}_\mathfrak{l}^*$	120	0	104
[2]	$PG = \mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$	155	5	104
[3]	$PG \nleqslant \mathrm{PSL}(2, \mathbb{F}_\mathfrak{l})$	120	0	104
[4]	$PG \nleqslant \mathrm{PGL}(2, \mathbb{F}_{q^i})$	0	0	0
[5]	$PG \nleqslant D_{2(\#\mathbb{F}_\mathfrak{l}+1)}$	13	0	0
[6]	$PG \nleqslant D_{2(\#\mathbb{F}_\mathfrak{l}-1)}$	4	5	0
[7]	$PG \nleqslant PBorel$	23	5	0
[8]	$PG \nleqslant A_4$	120	0	0
[9]	$PG \nleqslant S_4$	0	0	0
[10]	$PG \nleqslant A_5$	0	0	0

□

Beispiel 6.1.6.

	$\mathbb{F}_3$
Betrachtete $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ (keine CM)	$0 \leqslant \deg(g) \leqslant 3$, $0 \leqslant \deg(\Delta) \leqslant 3$
Anzahl ϕ mit CM	98
Betrachtete Führer $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$	$1 \leqslant \deg(\mathfrak{l}) \leqslant 4$
Anzahl der Führer	$3 + 3 + 8 + 18 = 32$
Anzahl der $(\phi, \mathfrak{l})$	204224
Gal $\neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$	2158
$\deg(\mathfrak{l}) = 1$	1500
$\deg(\mathfrak{l}) = 2$	18
$\deg(\mathfrak{l}) = 3$	640
Laufzeit	407 min
Durchschnitt für ein $(\phi, \mathfrak{l})$	0.12 sec
Maximal betrachtete $\mathrm{Frob}_\mathfrak{p}$	60
Maximal benötigte $\mathrm{Frob}_\mathfrak{p}$	30
$1 - 5$	189 500
$6 - 10$	12 102
$11 - 15$	420
$16 - 20$	40
$21 - 25$	0
$26 - 30$	4

$q = 3$	$\mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$			
	Kurzbeschreibung	$\deg_T(\mathfrak{l}) = 1$	$\deg_T(\mathfrak{l}) = 2$	$\deg_T(\mathfrak{l}) = 3$
[0]	$G = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$	1500	18	640
[1]	$\det(G) = \mathbb{F}_\mathfrak{l}{}^*$	960	0	640
[2]	$\mathrm{P}G = \mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$	1500	18	640
[3]	$\mathrm{P}G \nleq \mathrm{PSL}(2, \mathbb{F}_\mathfrak{l})$	960	0	640
[4]	$\mathrm{P}G \nleq \mathrm{PGL}(2, \mathbb{F}_{q^i})$	0	0	0
[5]	$\mathrm{P}G \nleq D_{2(\#\mathbb{F}_\mathfrak{l}+1)}$	66	0	0
[6]	$\mathrm{P}G \nleq D_{2(\#\mathbb{F}_\mathfrak{l}-1)}$	24	0	0
[7]	$\mathrm{P}G \nleq PBorel$	516	18	0
[8]	$\mathrm{P}G \nleq A_4$	960	0	0
[9]	$\mathrm{P}G \nleq S_4$	0	0	0
[10]	$\mathrm{P}G \nleq A_5$	0	0	0

Wir haben die nichtmaximalen Fälle genauer untersucht und jeweils nachgerechnet, daß die Torsionserweiterung wirklich nicht maximal war. Dies ist im Abschnitt 6.2 zusammengefaßt.
In der obigen Tabelle fällt auf, daß fast immer die Surjektivität mit weniger als 20 Stellen gezeigt werden konnte. In den verbleibenden 4 Beispielen wurden aber 2 mal 29 und 2 mal 30 Stellen benötigt.

Einer dieser ,,Ausreißer" ist das Beispiel

$$\phi = (\mathbb{F}_3, \mathbb{F}_3(u), u + (u^3 + 2u + 2)\tau + (u^3 - u)\tau^2), \qquad \mathfrak{l}(T) = T^3 + 2T + 1 \quad .$$

Betrachtet wir die charpol($\mathrm{Frob}_\mathfrak{p}$) zu den unverzweigten Stellen (d.h. $\mathfrak{p}(u) \notin \{u, u+1, u+2, u^3+2u+1\}$). Dann haben die Polynome charpol($\mathrm{Frob}_\mathfrak{p}$) $\in \mathbb{F}_\mathfrak{l}[x]$ zwei verschiedene Nullstellen in $\mathbb{F}_\mathfrak{l}$ für alle solchen $\mathfrak{p}(u)$ mit $\mathrm{Nrred}(\mathfrak{p}) \leqslant 33$. Erst für $\mathfrak{p}(u) = u^5 + 2u + 2$ ist charpol($\mathrm{Frob}_\mathfrak{p}$) irreduzibel. Daher kann die Borelgruppe in der $\mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$ erst mit Hilfe dieser Stelle ausgeschlossen werden. Da etwa die Hälfte der Elemente in der $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ irreduzibles charakteristisches Polynom haben, ist es ungewöhnlich, daß man erst 29 Elemente mit zerfallendem charakteristischem Polynom erhält.
Wendet man auf die ganze Situation die affine Transformation $u \mapsto 2u$ an (siehe Lemma 5.6.1), so transformiert sich $u^5 + 2u + 2$ in $u^5 + 2u + 1$ und wir erhalten ein Beispiel, in dem die ersten 29 Frobeniuselemente gebraucht werden.
Die anderen beiden Beispiele erklären sich genauso. $\square$

Beispiel 6.1.7.

	$\mathbb{F}_5$
Betrachtete $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u + g\tau + \Delta\tau^2)$ (keine CM)	$0 \leqslant \deg(g) \leqslant 2,\ g \neq 0$ $0 \leqslant \deg(\Delta) \leqslant 2$
Anzahl ϕ mit CM	0
Betrachtete Führer $\mathfrak{l} \in \mathbb{P}_{\mathbb{F}_q[T]}$	$1 \leqslant \deg(\mathfrak{l}) \leqslant 3$
Anzahl der Führer	$5 + 10 + 40 = 55$
Anzahl der $(\phi, \mathfrak{l})$	845 680
Gal $\neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$	3960
$\deg(\mathfrak{l}) = 1$	3760
$\deg(\mathfrak{l}) = 2$	200
Laufzeit	829 min
Durchschnitt für ein $(\phi, \mathfrak{l})$	0.05 sec
Maximal betrachtete $\mathrm{Frob}_\mathfrak{p}$	60
Maximal benötigte $\mathrm{Frob}_\mathfrak{p}$	29
$1 - 5$	814 008
$6 - 10$	25 920
$11 - 15$	1412
$16 - 20$	288
$21 - 25$	68
$26 - 30$	24

$q = 5$	$\mathrm{Gal}(\mathbb{F}_q(u)[_\mathfrak{l}\phi], \mathbb{F}_q(u)) \neq \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$		
	Kurzbeschreibung	$\deg_T(\mathfrak{l}) = 1$	$\deg_T(\mathfrak{l}) = 2$
[0]	$G = \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$	3760	200
[1]	$\det(G) = \mathbb{F}_\mathfrak{l}^*$	1240	0
[2]	$PG = \mathrm{PGL}(2, \mathbb{F}_\mathfrak{l})$	3760	200
[3]	$PG \nleqslant \mathrm{PSL}(2, \mathbb{F}_\mathfrak{l})$	1240	0
[4]	$PG \nleqslant \mathrm{PGL}(2, \mathbb{F}_{q^i})$	0	0
[5]	$PG \nleqslant D_{2(\#\mathbb{F}_\mathfrak{l}+1)}$	260	0
[6]	$PG \nleqslant D_{2(\#\mathbb{F}_\mathfrak{l}-1)}$	200	0
[7]	$PG \nleqslant PBorel$	2440	200
[8]	$PG \nleqslant A_4$	240	0
[9]	$PG \nleqslant S_4$	500	0
[10]	$PG \nleqslant A_5$	1240	0

□

6.2 Einzelbeispiele

Wir haben für $\mathbb{F}_q = \mathbb{F}_3$ alle Paare aus Drinfeld-Moduln $\phi = (\mathbb{F}_3, \mathbb{F}_3(u), u, u + g(u)\tau + \Delta(u)\tau^2)$ und Führern $\mathfrak{l}(T) \in \mathbb{P}_{\mathbb{F}_q[T]}$ mit $g, \Delta \in \mathbb{F}_q[u]$, $0 \leqslant \deg_u(g) < 4$, $0 \leqslant \deg_u(\Delta) < 4$, $0 \leqslant \deg_T(\mathfrak{l}) < 5$ untersucht. Dabei wurden nur Drinfeld-Moduln ohne komplexe Multiplikation betrachtet. Die Verteilung der Ergebnisse ist in Beispiel 6.1.6 zu finden.
In jedem Beispiel $(\phi, \mathfrak{l})$ haben wir die ersten bis zu 60 Stellen betrachtet, wobei die lexikographische Ordnung auf den Polynomen verwendet wurde. In den Fällen, in denen die Surjektivität nicht gezeigt werden konnte, haben wir zwei Beispiele als gleich betrachtet, wenn die Belegung der Schaltfunktion bei beiden nach Beendigung des Algorithmus gleich war. Aus jeder solchen Äquivalenzklasse werden wir nun einen Vertreter genauer untersuchen.
Für diese Vertreter haben wir den Algorithmus erneut gestartet, wobei deutlich mehr Stellen betrachtet wurden (meist etwa 2000). Dabei fielen unter Umständen einige Stellen fort, falls der Drinfeld-Modul an diesen schlechte Reduktion hatte. Ebenso wurde die Stelle $\mathfrak{p}(u) = \mathfrak{l}(u)$ nicht betrachtet.
Für festes ϕ und $\mathfrak{l}$ führen wir folgende Notation ein, dabei werden wir das Minimalpolynom einer Matrix M immer mit $\operatorname{minpol}(M)$ bezeichnen. Die Menge aller Minimalpolynome bezeichnen wir mit

$$\begin{aligned} \mathcal{MP} &:= \{\operatorname{minpol}(A) \mid A \in \mathrm{GL}(2, \mathbb{F}_\mathfrak{l})\} \\ &= \{x^2 + ax + b \mid a, b \in \mathbb{F}_\mathfrak{l},\ b \neq 0\} \cup \{x - b \mid b \in \mathbb{F}_\mathfrak{l},\ b \neq 0\} \quad . \end{aligned}$$

Es sei daran erinnert, daß der $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$-Konjugationstyp einer Matrix M durch ihr Minimalpolynom eindeutig bestimmt ist. Für $n \in \mathbb{N}$, $m(x) \in \mathcal{MP}$ sei

$$\mathbb{M}(n, m(x)) := \left\{ \mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]} \mid \begin{array}{l} \phi \text{ hat gute Reduktion an } \mathfrak{p},\ \mathfrak{p}(u) \neq \mathfrak{l}(u), \\ \operatorname{minpol}(\mathrm{Frob}_\mathfrak{p}) = m(x),\ \mathrm{Nrred}(\mathfrak{p}) < n \end{array} \right\} .$$

Für eine Untergruppe G von $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ und $m(x) \in \mathcal{MP}$ sei

$$\operatorname{Conj}(m(x), G) := \{A \in G \mid \operatorname{minpol}(A) = m(x)\} .$$

Zwei Elemente aus G, die in G nicht zueinander konjugiert sind, können durchaus in der gleichen Menge $\operatorname{Conj}(m(x), G)$ liegen.
Weiter sei

$$\begin{aligned} \tilde{n} &:= \sum_{m \in \mathcal{MP}} \#\mathbb{M}(n, m(x)) \\ &= \# \left\{ \mathfrak{p} \in \mathbb{P}_{\mathbb{F}_q[u]} \mid \begin{array}{l} \phi \text{ hat gute Reduktion an } \mathfrak{p},\ \mathfrak{p}(u) \neq \mathfrak{l}(u), \\ \mathrm{Nrred}(\mathfrak{p}) < n \end{array} \right\} \\ &= n + \mathrm{O}(1) . \end{aligned}$$

Ist nun $G = \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u))$, so sollte nach dem Satz von Chebotarev für hinreichend großes n für alle $m(x) \in \mathcal{MP}$

$$\frac{\#\mathbb{M}(n, m(x))}{\tilde{n}} \approx \frac{\#\mathrm{Conj}(m(x), G)}{\#G}$$

gelten. Mit $m(x) = x - 1$ ergibt sich insbesondere

$$\#\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{l}}\phi], \mathbb{F}_q(u)) \approx \frac{\tilde{n}}{\#\mathbb{M}(n, x-1)} \quad .$$

Es ist klar, daß es sich hierbei um heuristische Argumente und nicht um mathematisch exakt begründete Aussagen handelt. Dennoch geben uns diese Zahlen Hinweise auf die vorliegende Galoisgruppe.
Wir werden nun die einzelnen Beispiele diskutieren, wobei wir auch immer die Ausgabe des Programms mit angeben. Daher werden wir die Form der Ausgabe kurz erklären. In Simath wird ein Polynom $\sum_{i=0}^{n} a_i T^i \in K[T]$ als Liste

$$(n \quad a_n \quad n-1 \quad a_{n-1} \quad \ldots \quad 0 \quad a_0)$$

repräsentiert, wobei aber nur die a_i auftreten, die ungleich Null sind.
Endliche Primkörper $\mathbb{F}_p$ werden durch $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$ repräsentiert. Zum Beispiel repräsentiert die Liste $(2 \quad 3 \quad 0 \quad 6)$ ein Polynom $3y^2 + 6 \in \mathbb{F}_p[y]$ für $p \geqslant 7$. Beliebige endliche Körper werden als $\mathbb{F}_p[y]/h(y)$ mit irreduziblem $h(y) \in \mathbb{F}_p[y]$ repräsentiert. Daher bezeichnet $(2 \quad (0 \quad 1))$ das Element $1 \cdot T^2 \in \mathbb{F}_q[T] = (\mathbb{F}_p[y]/h(y))[T]$. Die Liste $(2 \quad (4 \quad 1 \quad 0 \quad 2))$ repräsentiert das Element $(y^4 + 2)T^2 \in \mathbb{F}_q[T]$, sofern $[\mathbb{F}_q : \mathbb{F}_p] \geqslant 5$ ist.
Zu einem Rang-2 Drinfeld-Modul ϕ wird das Polynom

$$\phi_T(\tau) = \frac{z_2}{n_2}\tau^2 + \frac{z_1}{n_1}\tau + \frac{z_0}{n_0}$$

durch

$$\mathtt{DM} = \begin{cases} (2\ z_2\ n_2\ 1\ z_1\ n_1\ 0\ z_0\ n_0) & ; \quad z_1 \neq 0 \\ (2\ z_2\ n_2\ 0\ z_0\ n_0) & ; \quad z_1 = 0 \end{cases}$$

repräsentiert. `TorsStelle` bezeichnet den Führer $\mathfrak{l}(T)$ und `Fl` den endlichen Körper $\mathbb{F}_q[T]/\mathfrak{l}$. Die Ausgabe der einzelnen Knoten des Schaltgraphen ist selbsterklärend.

Beispiel 6.2.1. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + 2u\tau + \tau^2)$$

und den

$$\text{Führer:} \qquad T + 2 \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 1  ( 0  2 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 )  0  ( 0  2 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 59
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
1 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
1 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
1 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
1 : [6]PG keine Ugr. von D_{2(l-1)}
0 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
1 : [11]ex. M in G mit <det(M)>=Fl^{ast}
1 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
1 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
1 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
0 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
0 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
1 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
0 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Dieses Ergebnis erklärt sich wie folgt: Es ist

$$\phi_{T+2}(\tau) = (\tau + 2u + 1)(\tau - 1)$$

und damit

$$\begin{aligned} \phi_{T+2}(x) &= x^9 + 2ux^3 + x(u+2) = (x^3 - x)^3 + (2u+1)(x^3 - x) \\ &= x(x+1)(x-1)(x^6 + x^4 + x^2 + (2u+1)) \in \mathbb{F}_q(u)[x], \end{aligned}$$

und dies ist bereits die vollständige Faktorisierung. An der Faktorisierung in $\mathbb{F}_q(u)\{\tau\}$ sehen wir bereits, daß der Drinfeld-Modul eine rationale $(T+2)$-Isogenie besitzt. Daher muß die Galoisgruppe eine Untergruppe der Borelgruppe sein, was auch die Belegung der Knoten 3 bis 10 nahelegt. Die Belegung von Knoten 62 ist ein Hinweis auf die Existenz von rationalen $(T+2)$-Torsionspunkten. Aus der Faktorisierung in $\mathbb{F}_q(u)[x]$ können wir direkt ablesen, daß $\mathbb{F}_3$ die Menge der rationalen $(T+2)$-Torsionspunkte ist. Die Galoisgruppe ist also Untergruppe von

$$\begin{pmatrix} 1 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix} .$$

Da in der Faktorisierung von $\phi_{T+2}(x)$ ein irreduzibler Faktor vom Grad 6 auftritt, hat die Erweiterung mindestens Grad 6 über $\mathbb{F}_3(u)$, und damit erhalten wir

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{T+2}\phi], \mathbb{F}_q(u)) = \begin{pmatrix} 1 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix} .$$

Dieses Beispiel haben wir an den ersten 2000 Stellen betrachtet. Wir fanden folgende Minimalpolynome von Frobeniuselementen.

$n = 2000, \quad \tilde{n} = 1999$			
$m(x)$	$x-1$	$(x-1)^2$	$(x-1)(x-2)$
$\#\mathbb{M}(n, m(x))$	320	668	1011
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.16	0.33	0.51

Die tatsächlichen Häufigkeiten lauten:

$G = \begin{pmatrix} 1 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix}, \quad \#G = 6$			
$m(x)$	$x-1$	$(x-1)^2$	$(x-1)(x-2)$
$\#\mathrm{Conj}(m(x), G)$	1	2	3
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.17	0.33	0.50

Wie man sieht, stimmen die geschätzten Häufigkeiten mit den tatsächlichen sehr gut überein.

□

Beispiel 6.2.2. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + (u+1)\tau + (2u^3+1)\tau^2)$$

und den

$$\text{Führer:} \qquad T \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 3  ( 0  2 )  0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 1  ( 0  1 )  0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 58
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
1 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
1 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
0 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
0 : [6]PG keine Ugr. von D_{2(l-1)}
1 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
1 : [11]ex. M in G mit <det(M)>=Fl^{ast}
1 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
0 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
0 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
1 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
0 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
0 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
1 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Dieses Ergebnis erklärt sich wie folgt: Es ist

$$\begin{aligned}\phi_T(x) &= (2u^3+1)x^9+(u+1)x^3+ux\\ &= 2x\ \left((u^2+u+1)x^4+(2u+1)x^2+u\right)\ \left((u+2)x^4+x^2+2\right) \in \mathbb{F}_q(u)[x],\end{aligned}$$

und dies ist die vollständige Faktorisierung.
Wir werden nun zeigen, daß

$$\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,, \mathbb{F}_q(u)) = \mathrm{Gal}((u+2)x^4+x^2+2) \cong \mathrm{D}_8$$

ist.
Sei

$$f(x) := (u+2)x^4+x^2+2, \quad g(x) := (u^2+u+1)x^4+(2u+1)x^2+u\ .$$

Dann ist

$$\tilde{f}(x) := (u{+}2)^3\ f(\frac{x}{u+2}) = x^4{+}(u{+}2)x^2{+}2(u{+}2)^3 = \big(x^2-(u+2)\big)^2{-}u(u{+}2)^2$$

und

$$\tilde{g}(x) := (u{+}2)^2\ g(\frac{x}{u+2}) = x^4{+}2(u{+}2)x^2{+}u(u{+}2)^2 = \big(x^2+(u+2)\big)^2{+}(u{+}2)^3\ .$$

Die jeweiligen Diskriminanten ergeben sich zu

$$\mathrm{Disc}(\tilde{f}) = 2u^2\ (u+2)^7 \qquad \text{und} \qquad \mathrm{Disc}(\tilde{g}) = u\ (u+2)^8 \quad .$$

Es sei $\mathrm{Gal}(f)$ die Galoisgruppe des Zerfällungskörpers von f. Dann ist $\mathrm{Gal}(f) = \mathrm{Gal}(\tilde{f})$ eine transitive Untergruppe der S_4, und da alle Automorphismen die Nullstellen des Polynoms $y^2-u(u+2)^2$ entweder vertauschen oder festlassen, muß $\mathrm{Gal}(f) \leqslant \mathrm{D}_8$ sein. Die transitiven echten Untergruppen der D_8 sind die zyklische Gruppe C_4 und die Kleinsche Vierergruppe V_4. Da die Diskriminante von $\tilde{f}$ kein Quadrat ist, liegt die Galoisgruppe nicht in der A_4, und damit scheidet die V_4 aus. Da

$$\tilde{f}(x) \equiv (x^2+u+1)(x+2u)(x+u) \bmod (u^2+1)$$

ist, enthält die Galoisgruppe eine Transposition. Dies schließt die C_4 aus, und es folgt

$$\mathrm{Gal}(f) = \mathrm{Gal}(\tilde{f}) = D_8 \quad .$$

Mit analoger Argumentation erhält man unter Verwendung von

$$\tilde{g}(x) \equiv (x^2+2u)(x+u+2)(x+2u+1) \bmod (u^2+u+2) \quad ,$$

daß

$$\mathrm{Gal}(g) = \mathrm{Gal}(\tilde{g}) = D_8$$

gilt. Es ist also noch zu zeigen, daß die beiden Zerfällungskörper gleich sind. Wir bezeichnen die Nullstellen von $\tilde{f}(x)$ mit

$$\begin{aligned}
\mu_1 =& (\sqrt{u+2}) \cdot \left(\sqrt{1+\sqrt{u}}\right) \\
\mu_2 =& (\sqrt{u+2}) \cdot \left(\sqrt{1-\sqrt{u}}\right) \\
\mu_3 =& -(\sqrt{u+2}) \cdot \left(\sqrt{1+\sqrt{u}}\right) \\
\mu_4 =& -(\sqrt{u+2}) \cdot \left(\sqrt{1-\sqrt{u}}\right)
\end{aligned}$$

und die Nullstellen von $\tilde{g}(x)$ mit

$$\begin{aligned}
\eta_1 =& (\sqrt{2u+1}) \cdot \left(\sqrt{1-\sqrt{2u+1}}\right) \\
\eta_2 =& (\sqrt{2u+1}) \cdot \left(\sqrt{1+\sqrt{2u+1}}\right) \\
\eta_3 =& -(\sqrt{2u+1}) \cdot \left(\sqrt{1-\sqrt{2u+1}}\right) \\
\eta_4 =& -(\sqrt{2u+1}) \cdot \left(\sqrt{1+\sqrt{2u+1}}\right) \quad .
\end{aligned}$$

Die Numerierung der μ_i ist so gewählt, daß sich die Galoisgruppe $\mathrm{Gal}(\tilde{f})$ durch die Operation auf den Indizes als $\langle (1\ 2\ 3\ 4),\ (1\ 3) \rangle$ in die S_4 einbettet.
Auch die η_i sind so numeriert, daß $\mathrm{Gal}(\tilde{g})$ in der S_4 als $\langle (1\ 2\ 3\ 4),\ (1\ 3) \rangle$ dargestellt wird. Betrachten wir nun in beiden Zerfällungskörpern den Teilkörper, der von der Untergruppe $\{(1),\ (1\ 3)\ (2\ 4)\}$ elementweise fixiert wird. Es ist

$$\mu_1\mu_2 = \mu_3\mu_4 = (u+2)\sqrt{1+2u} \quad \text{und} \quad \frac{\mu_1}{\mu_2} = \frac{\mu_3}{\mu_4} = \frac{\sqrt{1+2u}}{1+2\sqrt{u}} \quad .$$

Ebenso ergibt sich

$$\eta_1\eta_2 = \eta_3\eta_4 = (2u+1)\sqrt{u} \quad \text{und} \quad \frac{\eta_2}{\eta_1} = \frac{\eta_4}{\eta_3} = \frac{\sqrt{u}}{1+2\sqrt{1+2u}} \quad .$$

Damit ist

$$\mathbb{F}_3(u)\left[\mu_1\mu_2, \frac{\mu_1}{\mu_2}\right] = \mathbb{F}_3(\sqrt{u}, \sqrt{1+2u}) = \mathbb{F}_3(u)\left[\eta_2\eta_1, \frac{\eta_2}{\eta_1}\right] \quad .$$

Da $[\mathbb{F}_3(\sqrt{u},\sqrt{1+2u}):\mathbb{F}_3(u)]=4$ ist, ist $\mathbb{F}_3(\sqrt{u},\sqrt{1+2u})$ bereits der Fixkörper zu obiger Untergruppe. Wir haben also einen gemeinsamen Teilkörper vom Grad 4 in den Zerfällungskörpern von $\tilde{f}$ und $\tilde{g}$ gefunden. Über diesem Teilkörper zerfallen $\tilde{f}(x)$ und $\tilde{g}(x)$ als

$$\tilde{f}(x)=\big((x-\mu_1)(x-\mu_3)\big)\cdot\big((x-\mu_2)(x-\mu_4)\big)$$

und

$$\tilde{g}(x)=\big((x-\eta_1)(x-\eta_3)\big)\cdot\big((x-\eta_2)(x-\eta_4)\big)$$

in quadratische Polynome. Sei

$$f_1(x)=(x-\mu_1)(x-\mu_3)\in\mathbb{F}_3(\sqrt{u},\sqrt{1+2u})[x]$$

und

$$g_1(x)=(x-\eta_1)(x-\eta_3)\in\mathbb{F}_3(\sqrt{u},\sqrt{1+2u})[x] \quad .$$

Dann haben f und g genau dann den gleichen Zerfällungskörper über $\mathbb{F}_3(u)$, wenn f_1 und g_1 denselben Zerfällungskörper über $\mathbb{F}_3(\sqrt{u},\sqrt{1+2u})$ haben. Daher betrachten wir

$$\begin{aligned}\frac{\mathrm{Disc}(f_1)}{\mathrm{Disc}(g_1)} &= \frac{(\mu_1-\mu_3)^2}{(\eta_1-\eta_3)^2}\\ &= \frac{(u+2)(1+\sqrt{u})}{(2u+1)(1-\sqrt{2u+1})}\\ &= \frac{2+2\sqrt{u}+2\sqrt{1+2u}+2\sqrt{u}\sqrt{1+2u}}{u}\\ &= \frac{(1+\sqrt{u}+\sqrt{1+2u})^2}{(\sqrt{u})^2} \quad .\end{aligned}$$

Da sich die Diskriminanten nur um ein Quadrat aus $\mathbb{F}_3(\sqrt{u},\sqrt{1+2u})$ unterscheiden, haben f_1 und g_1 (und damit auch f und g) denselben Zerfällungskörper. Insgesamt erhalten wir

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_T\phi],\mathbb{F}_q(u))=\mathrm{Gal}(f)=\mathrm{Gal}(\tilde{f})\cong \mathrm{D}_8 \quad .$$

Um die Gruppe als Untergruppe der $\mathrm{GL}(2,\mathbb{F}_3)$ zu identifizieren, haben wir zu den ersten 2000 Stellen aus $\mathbb{P}_{\mathbb{F}_q[T]}$ die Minimalpoynome berechnet.

$n=2000,\quad \tilde{n}=1998$				
$m(x)$	$x-1$	$x-2$	$(x-1)(x-2)$	x^2+1
$\#\mathbb{M}(n,m(x))$	242	250	1002	504
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.12	0.13	0.50	0.25

Da die Galoisgruppe die volle Diagonalgruppe und ein Element mit Minimalpolynom x^2+1 enthält, muß sie zur Gruppe

$$\langle\begin{pmatrix}1&0\\0&-1\end{pmatrix},\quad\begin{pmatrix}0&-1\\1&0\end{pmatrix}\rangle$$

konjugiert sein. Die tatsächliche Verteilung der Minimalpolynome in der obigen Gruppe lautet

$G = \langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle, \quad \#G = 8$				
$m(x)$	$x-1$	$x-2$	$(x-1)(x-2)$	x^2+1
$\#\mathrm{Conj}(m(x),G)$	1	1	4	2
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.125	0.125	0.50	0.25

.

$\square$

Beispiel 6.2.3. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + (2u^3 + 2u + 1)\tau + u^3\tau^2)$$

und den

$$\text{Führer:} \quad T + 2 \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 3  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 3  ( 0  2 )  1  ( 0  2 )  0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 )  0  ( 0  2 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 58
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
1 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
1 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
0 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
0 : [6]PG keine Ugr. von D_{2(l-1)}
0 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
1 : [11]ex. M in G mit <det(M)>=Fl^{ast}
1 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
0 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
0 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
0 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
0 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
0 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
0 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Es ist

$$\phi_{T+2}(\tau) = (u^3\tau - (u+2))(\tau - 1)$$

und damit

$$\phi_{T+2}(x) = x(x+1)(x+2)(ux^2+2u+1)(ux^2+ux+1)(ux^2+2ux+1) \quad .$$

Mit $f(x) := ux^2 + 2u + 1$ ist

$$f(x+1) = ux^2 + 2ux + 1$$

und

$$f(x+2) = ux^2 + ux + 1 \quad .$$

Daher hat der $(T+2)$-Torsionskörper Grad 2 über $\mathbb{F}_3(u)$. Da rationale Torsionspunkte existieren, wird die Galoisgruppe von einem Element der Ordnung 2 aus $\mathrm{GL}(2, \mathbb{F}_3)$ erzeugt, dessen einer Eigenwert 1 ist. Damit ist

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_T\phi], \mathbb{F}_q(u)) = \langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \rangle \leqslant \mathrm{GL}(2, \mathbb{F}_3) \quad .$$

Die ersten 2000 Stellen liefern

$n = 2000, \quad \tilde{n} = 1998$		
$m(x)$	$x-1$	$(x-1)(x-2)$
$\#\mathbb{M}(n, m(x))$	985	1013
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.49	0.51

.

Dies paßt zur Verteilung der Minimalpolynome in der Gruppe.

$G = \langle \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \rangle, \quad \#G = 2$		
$m(x)$	$x-1$	$(x-1)(x-2)$
$\#\mathrm{Conj}(m(x), G)$	1	1
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.5	0.5

□

Beispiel 6.2.4. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + u\tau + 2u\tau^2)$$

und den

$$\text{Führer:} \qquad T \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 1  ( 0  2 ) )  ( 0  ( 0  1 ) )
      1  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 59
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
1 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
1 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
0 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
1 : [6]PG keine Ugr. von D_{2(l-1)}
1 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
1 : [11]ex. M in G mit <det(M)>=Fl^{ast}
1 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
0 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
0 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
1 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
1 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
1 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
0 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
1 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Die vollständige Faktorisierung von $\phi_T(x)$ ist

$$\phi_T(x) \quad = 2ux(x^8 + 2x^2 + 2) \in \mathbb{F}_q(u)[x] \quad .$$

Der T-Torsionskörper ist also $\mathbb{F}_{3^8}(u)$, und die Galoisgruppe ist zyklisch von der Ordnung 8. Da in der $\mathrm{GL}(2, \mathbb{F}_r)$ eine zyklische Untergruppe der Ordnung $r^2 - 1$ immer eine nichtzerfallende Cartanuntergruppe ist, ist (bis auf Konjugation)

$$\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,, \mathbb{F}_q(u)) = \langle \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \rangle \quad .$$

Die Untersuchung der ersten 2000 Primstellen liefert

$n = 2000, \quad \tilde{n} = 1999$					
$m(x)$	$x-1$	$x-2$	x^2+2x+2	x^2+1	x^2+x+2
$\#\mathbb{M}(n, m(x))$	810	18	360	119	692
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.41	0.01	0.18	0.06	0.35

.

Demgegenüber verteilen sich die Minimalpolynome in der Galoisgruppe

$G = \langle \begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \rangle, \quad \#G = 8$					
$m(x)$	$x-1$	$x-2$	x^2+2x+2	x^2+1	x^2+x+2
$\#\mathrm{Conj}(m(x), G)$	1	1	2	2	2
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.125	0.125	0.25	0.25	0.25

.

Es fällt auf, daß die geschätzten Werte stark von den tatsächlichen Werten abweichen. Dies erklärt sich wie folgt. Das Vorliegen einer nichttrivialen Konstantenerweiterung in $\mathbb{F}_q(u)[_\iota\phi]|\mathbb{F}_q(u)$ stört die Gleichverteilung der Frobeniuselemente. Da $\mathbb{F}_q(u)[_\iota\phi]|\mathbb{F}_q(u)$ eine reine Konstantenerweiterung ist, tritt dieser Effekt im vorliegenden Fall besonders stark auf. (In den Beispielen 6.2.7 und 6.2.8 ist der Effekt schwächer.) Wählen wir $\sigma : z \mapsto z^3$ als Erzeuger der Galoisgruppe von $\mathbb{F}_{3^8}|\mathbb{F}_3$, so ist $\mathrm{Frob}_\mathfrak{p} = \sigma^{\deg_u(\mathfrak{p})}$ für alle Stellen $\mathfrak{p}(u)$. Der Frobenius zu einer Stelle $\mathfrak{p}(u)$ hängt also nicht von der Stelle selbst, sondern nur von ihrem Grad ab. Indem wir eine passende $\mathbb{F}_3$-Basis von $_T\phi$ wählen, können wir das Element σ mit der Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_3)$ identifizieren. Damit korrespondieren die σ^i zu folgenden Matrizen und Minimalpolynomen:

σ^1	$\begin{pmatrix} 0 & 1 \\ 1 & 2 \end{pmatrix}$	x^2+x+2	σ^5	$\begin{pmatrix} 0 & 2 \\ 2 & 1 \end{pmatrix}$	x^2+2x+2
σ^2	$\begin{pmatrix} 1 & 2 \\ 2 & 2 \end{pmatrix}$	x^2+1	σ^6	$\begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$	x^2+1
σ^3	$\begin{pmatrix} 2 & 2 \\ 2 & 0 \end{pmatrix}$	x^2+x+2	σ^7	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$	x^2+2x+2
σ^4	$\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$	$x-2$	σ^8	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	$x-1$

Daraus erhält man

$$\operatorname{minpol}(\operatorname{Frob}_{\mathfrak{p}}) = \begin{cases} x^2+x+2 & ; \ \deg \mathfrak{p} \equiv 1,3 \bmod 8 \\ x^2+1 & ; \ \deg \mathfrak{p} \equiv 2,6 \bmod 8 \\ x-2 & ; \ \deg \mathfrak{p} \equiv 4 \bmod 8 \\ x^2+2x+2 & ; \ \deg \mathfrak{p} \equiv 5,7 \bmod 8 \\ x-1 & ; \ \deg \mathfrak{p} \equiv 0 \bmod 8 \end{cases} .$$

Berechnet man die Anzahl der irreduziblen Polynome zu vorgegebenem Grad, so erhält man die folgende Tabelle, wobei auch die Nrred der kleinsten und größten irreduziblen Polynome vom entsprechenden Grad angegeben sind.

d	$\#\{\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_3[u]} \mid \deg(\mathfrak{p}) = d\}$	Nrred
1	3	$1-3$
2	3	$4-6$
3	8	$7-14$
4	18	$15-32$
5	48	$33-80$
6	116	$81-196$
7	312	$197-508$
8	810	$509-1318$
9	2184	$1319-3502$
10	5880	$3503-9382$

Wir haben das Beispiel an allen $\mathfrak{p}$ mit $\operatorname{Nrred}(\mathfrak{p}) < 2000$ betrachtet. Wie man aus der Tabelle sieht, haben in diesem Bereich etwa 40 Prozent der auftretenden irreduziblen Polynome den Grad 8. Also werden die Frobeniuselemente, die zu Stellen vom Grad 8 gehören, in unserem Suchbereich stark überrepräsentiert. Nach unseren Überlegungen von oben ist das gerade die $1_{\mathrm{GL}(2,\mathbb{F}_3)}$. Da Elemente mit Minimalpolynom $x-2$ im von uns betrachteten Bereich nur von Stellen vom Grad 4 kommen, wurden sehr wenig von ihnen gefunden. Auch die Häufigkeiten der anderen Minimalpolynome erklären sich nun direkt. $\square$

Beispiel 6.2.5. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + u\tau + u\tau^2)$$

und den

$$\text{Führer:} \qquad T \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 59
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
0 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
0 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
1 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
1 : [6]PG keine Ugr. von D_{2(l-1)}
0 : [7]PG keine Ugr. von PBorel
0 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
0 : [11]ex. M in G mit <det(M)>=Fl^{ast}
0 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
1 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
1 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
0 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
0 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
1 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
0 : [61]ex. M in G mit det(M)!=1
0 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Dieses Ergebnis erklärt sich wie folgt: Es ist

$$\phi_T(\tau) = u(\tau-1)(\tau-1)$$

und damit

$$\begin{aligned}\phi_T(x) &= ux^9 + ux^3 + ux = u((x^3-x)^3 - (x^3-x)) \\ &= ux(x+1)(x+2)(x^3+2x+2)(x^3+3x+1) \in \mathbb{F}_q(u)[x].\end{aligned}$$

Es ist also $\mathbb{F}_3(u)({}_T\phi) = \mathbb{F}_{27}(u)$. Die Galoisgruppe ist zyklisch von der Ordnung 3. Da $\mathrm{GL}(2,\mathbb{F}_3)$ bis auf Konjugation nur ein Element der Ordnung 3 besitzt, ist

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_T\phi], \mathbb{F}_q(u)) = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle \leqslant \mathrm{GL}(2,\mathbb{F}_3) \quad .$$

An den ersten 2000 Stellen erhalten wir folgende Minimalpolynome:

$n = 2000, \quad \tilde{n} = 1999$		
$m(x)$	$x-1$	$(x-1)^2$
$\#\mathbb{M}(n,m(x))$	806	1193
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.40	0.60

.

Die Häufigkeiten in der Untergruppe sind

$G = \langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle, \quad \#G = 3$		
$m(x)$	$x-1$	$(x-1)^2$
$\#\mathrm{Conj}(m(x),G)$	1	2
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.33	0.67

.

Die Differenz der Werte von $\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$ und $\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$ rührt daher, daß $\mathbb{F}_q(u)[{}_T\phi]|\mathbb{F}_q(u)$ eine Konstantenerweiterung ist. Mit der Argumentation aus Beispiel 6.2.4 ergibt sich

$$\mathrm{minpol}(\mathrm{Frob}_{\mathfrak{p}}) = (x-1) \iff \mathrm{ord}_{\mathrm{GL}}(\mathrm{Frob}_{\mathfrak{p}}) = 1 \iff \deg_u(\mathfrak{p}) \equiv 0 \bmod 3$$

und

$$\begin{aligned}\mathrm{minpol}(\mathrm{Frob}_{\mathfrak{p}}) = (x-1)^2 &\iff \mathrm{ord}_{\mathrm{GL}}(\mathrm{Frob}_{\mathfrak{p}}) = 3 \\ &\iff \deg_u(\mathfrak{p}) \equiv 1,2 \bmod 3 \ .\end{aligned}$$

Unter Verwendung der Tabelle von Seite 130 erhält man

$$\begin{aligned} \#\mathbb{M}(2000, x-1) &= 8 + 116 + (2000 - 1318) = 806 \\ \#\mathbb{M}(2000, (x-1)^2) &= 2 + 3 + 18 + 48 + 312 + 810 = 1193 \quad . \end{aligned}$$

$\square$

Beispiel 6.2.6. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + 2u\tau + u\tau^2)$$

und den

$$\text{Führer:} \qquad T \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 1  ( 0  2 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 59
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
0 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
0 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
1 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
1 : [6]PG keine Ugr. von D_{2(l-1)}
0 : [7]PG keine Ugr. von PBorel
0 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
0 : [11]ex. M in G mit <det(M)>=Fl^{ast}
0 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
1 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
1 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
0 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
0 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
1 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
0 : [61]ex. M in G mit det(M)!=1
1 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Es ist

$$\phi_T(\tau) = u(\tau+1)(\tau+1)$$

und

$$\phi_T(x) \quad = ux(x^2+1)(x^6+2x^4+x^2+1) \in \mathbb{F}_q(u)[x].$$

Daher ist der T-Torsionskörper gleich $\mathbb{F}_{3^6}(u)$. Die Galoisgruppe ist eine zyklische Gruppe der Ordnung 6 und liegt in einer Borelgruppe. Betrachtet man die Elemente der Ordnung 6 in $\mathrm{GL}(2,\mathbb{F}_3)$, so erhält man direkt

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_T\phi]\,, \mathbb{F}_q(u)) = \langle \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \rangle \leqslant \mathrm{GL}(2,\mathbb{F}_3) \quad .$$

Die Galoisgruppe ist also eine Untergruppe der $\mathrm{SL}(2,\mathbb{F}_3)$. Dies ist auch aus Drinfeld-theoretischen Gründen klar, da die T-Torsionserweiterung des assoziierten Rang-1 Moduls $\psi = (\mathbb{F}_3, \mathbb{F}_3(u), u, u - u\tau)$ wegen

$$\psi_T(x) = u(x^3 - x) = ux(x-1)(x-2)$$

trivial ist.
Eine Betrachtung der ersten 2000 Stellen liefert

$n = 2000, \quad \tilde{n} = 1999$				
$m(x)$	$x-1$	$x-2$	$(x-1)^2$	$(x-2)^2$
$\#\mathbb{M}(n, m(x))$	116	690	831	362
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.06	0.35	0.42	0.18

.

Betrachtung der Untergruppe selbst ergibt

$G = \langle \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \rangle, \quad \#G = 6$				
$m(x)$	$x-1$	$x-2$	$(x-1)^2$	$(x-2)^2$
$\#\mathrm{Conj}(m(x), G)$	1	1	2	2
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.17	0.17	0.33	0.33

.

Da es sich bei der Torsionserweiterung wieder um eine reine Konstantenerweiterung handelt, erklären sich die Abweichungen zwischen den beiden Tabellen analog zu den Abweichungen in Beispiel 6.2.4. $\square$

Beispiel 6.2.7. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + (u^3 + u + 1)\tau + (u^3 + 1)\tau^2)$$

und den

$$\text{Führer:} \qquad T \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 3  ( 0  1 )  0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 3  ( 0  1 )  1  ( 0  1 )  0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 58
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
1 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
1 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
0 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
0 : [6]PG keine Ugr. von D_{2(l-1)}
0 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
1 : [11]ex. M in G mit <det(M)>=Fl^{ast}
1 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
0 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
0 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
0 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
0 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
0 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
1 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Dieses Ergebnis erklärt sich wie folgt: Es ist

$$\phi_T(\tau) = ((u^3+1)\tau + u)(\tau + 1)$$

und damit

$$\begin{aligned}\phi_T(x) &= (u^3+1)x^9 + (u^3+u+1)x^3 + ux = (u^3+1)(x^3+x)^3 + u(x^3+x) \\ &= x(x^2+1)((u+1)x^2+u)((u^2+2u+1)x^4 + (u^2+2)x^2+1) \in \mathbb{F}_q(u)[x],\end{aligned}$$

und dies ist die vollständige Faktorisierung. An der Faktorisierung in $\mathbb{F}_q(u)\{\tau\}$ sehen wir bereits, daß der Drinfeld-Modul eine rationale T-Isogenie besitzt und daß die Galoisgruppe eine Untergruppe der Borelgruppe ist. Allerdings gibt es wegen Knoten 62 keinen rationalen T-Torsionspunkt.
Wir berechnen nun die Galoisgruppe von $\phi_T(x)$ ohne Verwendung der Theorie der Drinfeld-Moduln. Sei

$$\begin{aligned} f(x) &:= (u^2+2u+1)x^4 + (u^2+2)x^2 + 1 \quad , \\ g(x) &:= (u+1)x^2 + u \quad , \\ h(x) &:= x^2+1 \quad . \end{aligned}$$

Wir werden zeigen, daß für die Zerfällungskörper

$$\mathrm{ZerfKp}(g) \cdot \mathrm{ZerfKp}(h) = \mathrm{ZerfKp}(f)$$

gilt. Dazu betrachten wir

$$\begin{aligned} \tilde{f}(x) &:= (u+1)^2 \; f\left(\frac{x}{u+1}\right) = (x^2 - (u^2+2))^2 - u(u+1)^3 \\ \tilde{g}(x) &:= (u+1) \cdot g\left(\frac{x}{u+1}\right) = x^2 + u(u+1) \quad . \end{aligned}$$

Sei $\mathrm{Gal}(\tilde{f})$ die Galoisgruppe des Zerfällungskörpers von $\tilde{f}$ über $\mathbb{F}_3(u)$. Da ein Element aus $\mathrm{Gal}(\tilde{f})$ die Nullstellen von $y^2 - u(u+1)^3$ fixieren oder vertauschen muß, ist

$$\mathrm{Gal}(\tilde{f}) \leqslant \mathrm{D}_8 < S_4 \quad .$$

Da $\tilde{f}$ irreduzibel ist, muß $\mathrm{Gal}(\tilde{f})$ eine transitive Untergruppe von D_8 sein, also D_8, die zyklische Gruppe C_4 oder die Kleinsche Vierergruppe V_4. Die Diskriminante $\mathrm{Disc}(\tilde{f}) = (u+1)^8 \; u^2$ ist ein Quadrat, daher muß die Galoisgruppe in der A_4 enthalten sein. Dies schließt D_8 und C_4 aus, und es folgt

$$\mathrm{Gal}(\tilde{f}) = V_4 \quad .$$

Wir müssen nun in $\mathrm{ZerfKp}(\tilde{f})$ die Zerfällungskörper von $g(x)$ und $h(x)$ finden. Dazu betrachten wir die Nullstellen

$$\alpha_1 := (\sqrt{u+1}) \cdot \left(\sqrt{u-1+\sqrt{u^2+u}}\right)$$

$$\alpha_2 := -(\sqrt{u+1}) \cdot \left(\sqrt{u-1+\sqrt{u^2+u}}\right)$$

$$\alpha_3 := (\sqrt{u+1}) \cdot \left(\sqrt{u-1-\sqrt{u^2+u}}\right)$$

$$\alpha_4 := -(\sqrt{u+1}) \cdot \left(\sqrt{u-1-\sqrt{u^2+u}}\right)$$

auf denen V_4 durch die Permutationen

$$\{(1),\ (\alpha_1\alpha_2)(\alpha_3\alpha_4),\ (\alpha_1\alpha_3)(\alpha_2\alpha_4),\ (\alpha_1\alpha_4)(\alpha_2\alpha_3)\}$$

operiert. Wir betrachten die Elemente α_1^2 und $\alpha_1 + \alpha_3$. Die V_4 operiert auf ihnen wie folgt:

	α_1^2	$\alpha_1 + \alpha_3$
(1)	α_1^2	$\alpha_1 + \alpha_3$
$(\alpha_1\alpha_2)(\alpha_3\alpha_4)$	$\alpha_2^2 = (-\alpha_1)^2 = \alpha_1^2$	$\alpha_2 + \alpha_4 = -(\alpha_1 + \alpha_3) \neq \alpha_1 + \alpha_3$
$(\alpha_1\alpha_3)(\alpha_2\alpha_4)$	$\alpha_3^2 \neq \alpha_1^2$	$\alpha_3 + \alpha_1$
$(\alpha_1\alpha_4)(\alpha_2\alpha_3)$	$\alpha_4^2 \neq \alpha_1^2$	$\alpha_4 + \alpha_2 \neq \alpha_1 + \alpha_3$

Die Körper $\mathbb{F}_3(u, \alpha_1^2)$ und $\mathbb{F}_3(u, \alpha_1 + \alpha_3)$ sind also quadratische Zwischenerweiterungen von $\mathrm{ZerfKp}(\tilde{f})|\mathbb{F}_3(u)$. Es ist

$$\alpha_1^2 = (u+1)(u-1+\sqrt{u^2+u}),$$

also $\mathbb{F}_3(u, \alpha_1^2) = \mathbb{F}_3(u, \sqrt{u^2+u})$,

$$(\alpha_1 + \alpha_3)^2 = 2u(u+1)$$

bzw.

$$\alpha_1 + \alpha_3 = \pm\sqrt{2u(u+1)} \quad .$$

Damit erhalten wir als dritten Zwischenkörper vom Grad 2 den Körper

$$\mathbb{F}_3\left(u, \frac{\sqrt{2u(u+1)}}{\sqrt{u^2+u}}\right) = \mathbb{F}_9(u) \quad .$$

Es liegen also

$$\mathrm{ZerfKp}(g) = \mathrm{ZerfKp}(\tilde{g}) = \mathbb{F}_3(u, \sqrt{2u(u+1)})$$

und

$$\mathrm{ZerfKp}(h) = \mathbb{F}_9(u)$$

im Zerfällungskörper von f bzw. $\tilde{f}$. Da der Zerfällungskörper Grad 4 hat, wird er bereits von den beiden anderen Zerfällungskörpern erzeugt.
Wir haben also gezeigt, daß

$$\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,,\mathbb{F}_q(u)) = \mathrm{Gal}(\tilde{f}) \cong V_4$$

gilt. Da die Galoisgruppe (als Untergruppe der $\mathrm{GL}(2,\mathbb{F}_3)$) in einer Borelgruppe liegt und isomorph zu V_4 ist, erhalten wir

$$\mathrm{Gal}(\mathbb{F}_q(u)[_T\phi]\,,\mathbb{F}_q(u)) = \begin{pmatrix} \mathbb{F}_3^* & 0 \\ 0 & \mathbb{F}_3^* \end{pmatrix} \quad .$$

Die Nullstellenmengen der Polynome $x((u+1)x^2+u) = (u+1)x^3+ux$ und $x(x^2+1) = x^3+x$ bilden die beiden ϕ-invarianten $\mathbb{F}_3$-Vektorräume. Damit ist

$${}_T\phi = \langle\ \sqrt{2}, \sqrt{\frac{2u}{u+1}}\ \rangle_{\mathbb{F}_3} \quad ,$$

da für $\alpha \in \mathbb{F}_3$, $\eta \in {}_T\phi$

$$\alpha *_\phi \eta = \alpha \cdot \eta$$

gilt.
Eine Untersuchung der ersten 2000 Stellen liefert folgende Minimalpolynome:

$n = 2000, \quad \tilde{n} = 1998$			
$m(x)$	$x-1$	$x-2$	$(x-1)(x-2)$
$\#\mathbb{M}(n,m(x))$	465	523	1010
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.23	0.26	0.51

Die tatsächlichen Werte lauten:

$G = \begin{pmatrix} \mathbb{F}_3^* & 0 \\ 0 & \mathbb{F}_3^* \end{pmatrix}, \quad \#G = 4$			
$m(x)$	$x-1$	$x-2$	$(x-1)(x-2)$
$\#\mathrm{Conj}(m(x),G)$	1	1	2
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.25	0.25	0.50

Die leichten Abweichungen erklären sich wie folgt. Wir haben die Galoisgruppe bzgl. der geordneten Basis $\sqrt{2}, \sqrt{\frac{2u}{u+1}}$ als $\begin{pmatrix} \mathbb{F}_3^* & 0 \\ 0 & \mathbb{F}_3^* \end{pmatrix}$ repräsentiert. Betrachten wir den Körperturm

$$\begin{array}{c} \mathbb{F}_3(u)[_T\phi] \\ | \\ \mathbb{F}_{3^2}(u) \\ | \\ \mathbb{F}_3(u) \end{array} \quad ,$$

dann gilt für $\mathfrak{p}(u) \neq u, u+1$

$$\mathrm{Frob}_{\mathfrak{p}} \in \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \right\} \iff \mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(\mathbb{F}_3(u)[{}_T\phi], \mathbb{F}_{3^2}(u))$$
$$\iff \mathfrak{p} \text{ zerfällt in } \mathbb{F}_{3^2}(u)|\mathbb{F}_3(u)$$
$$\iff \deg_u(\mathfrak{p}) \equiv 0 \bmod 2 \quad .$$

Ebenso erhält man

$$\mathrm{Frob}_{\mathfrak{p}} \in \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix} \right\} \iff \deg_u(\mathfrak{p}) \equiv 1 \bmod 2 \quad .$$

Nach der Tabelle in Beispiel 6.2.4 ist

$$\#\{\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_3[u]} \mid \mathrm{Nrred}(\mathfrak{p}) < 2000,\ \deg_u(\mathfrak{p}) \equiv 0 \bmod 2\} = 947 \quad ,$$
$$\#\{\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_3[u]} \mid \mathrm{Nrred}(\mathfrak{p}) < 2000,\ \deg_u(\mathfrak{p}) \equiv 1 \bmod 2,\ \mathfrak{p} \neq u, u+1\} = 1051 \quad .$$

Nach Chebotarev sollten dann die Minimalpoynome $x-1$, $x-2$, $(x-1)(x-2)$ etwa $\frac{947}{2}$, $\frac{1051}{2}$ bzw. $\frac{947+1051}{2}$ mal vorkommen. Dies korrespondiert sehr gut zu den gefundenen Werten. □

Beispiel 6.2.8. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + (u+1)\tau + \tau^2)$$

und den

$$\text{Führer:} \qquad T \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 1  ( 0  1 )  0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 1  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 59
surjektiv=0
Fl=GF(3)
0 : [0]G=GL(2,Fl)
1 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
1 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
1 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
1 : [6]PG keine Ugr. von D_{2(l-1)}
0 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
1 : [11]ex. M in G mit <det(M)>=Fl^{ast}
1 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
1 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
1 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
0 : [17]ex. M in G mit cpol(M) irreduzibel
0 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
0 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
1 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
0 : [41]ex. M in G mit ord_{PGL}([M])>3
0 : [42]ex. M in G mit ord_{PGL}([M])>4
0 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
0 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
1 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
1 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Dieses Ergebnis erklärt sich wie folgt: Es ist

$$\phi_T(\tau) = (\tau + u)(\tau + 1)$$

und damit

$$\begin{aligned} \phi_T(x) &= x^9 + (u+1)x^3 + ux = (x^3+x)^3 + u(x^3+x) \\ &= x(x^2+1)(x^6+2x^4+x^2+u) \in \mathbb{F}_q(u)[x], \end{aligned}$$

und dies ist bereits die vollständige Faktorisierung. An der Faktorisierung in $\mathbb{F}_q(u)\{\tau\}$ sehen wir bereits, daß der Drinfeld-Modul eine rationale T-Isogenie besitzt. Daher muß die Galoisgruppe eine Untergruppe der Borelgruppe sein, was auch die Belegung der Knoten 3 bis 10 nahelegt. Allerdings besagt die Belegung von Knoten 62, daß es keinen rationalen T-Torsionspunkt gibt, in Übereinstimmung mit der Faktorisierung von $\phi_T(x)$.
Wir haben dieses Beispiel an den ersten 2000 Stellen genauer untersucht und folgende Minimalpolynome von Frobeniuselementen gefunden:

$n = 2000, \quad \tilde{n} = 1999$					
$m(x)$	$x-1$	$x-2$	$(x-1)^2$	$(x-2)^2$	$(x-1)(x-2)$
$\#\mathbb{M}(n, m(x))$	149	176	316	353	1005
$\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$	0.07	0.09	0.16	0.18	0.50

Wir wissen bereits, daß die Galoisgruppe Untergruppe einer Borelgruppe ist. Wegen der gefundenen verschiedenen Konjugationstypen muß sogar (bis auf Konjugation)

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_T\phi], \mathbb{F}_q(u)) = \begin{pmatrix} \mathbb{F}_3^* & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix}$$

gelten.
Betrachten wir nun, wie sich die Elemente einer Borelgruppe auf die Minimalpolynome verteilen, so erhalten wir

$G = \begin{pmatrix} \mathbb{F}_3^* & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix}, \quad \#G = 12$					
$m(x)$	$x-1$	$x-2$	$(x-1)^2$	$(x-2)^2$	$(x-1)(x-2)$
$\#\mathrm{Conj}(m(x), G)$	1	1	2	2	6
$\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$	0.08	0.08	0.17	0.17	0.50

Wir sehen, daß die geschätzten Häufigkeiten $\frac{\#\mathbb{M}(n,m(x))}{\tilde{n}}$ mit den tatsächlichen Häufigkeiten $\frac{\#\mathrm{Conj}(m(x),G)}{\#G}$ gut übereinstimmen.

In diesem Beispiel können wir mit dem Körperturm

$$\begin{array}{c} \mathbb{F}_3(u)[{}_T\phi] \\ | \\ \mathbb{F}_{3^2}(u) \\ | \\ \mathbb{F}_3(u) \end{array}$$

analog argumentieren wie in Beispiel 6.2.7. Wir erhalten für $\mathfrak{p}(u) \neq u$

$$\begin{aligned} \mathrm{Frob}_{\mathfrak{p}} \in \begin{pmatrix} 1 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix} &\iff \mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(\mathbb{F}_3(u)[{}_T\phi], \mathbb{F}_{3^2}(u)) \\ &\iff \deg_u(\mathfrak{p}) \equiv 0 \bmod 2 \end{aligned}$$

und

$$\mathrm{Frob}_{\mathfrak{p}} \in \begin{pmatrix} 2 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix} \iff \deg_u(\mathfrak{p}) \equiv 1 \bmod 2 \quad .$$

Aus der Tabelle in Beispiel 6.2.4 folgt

$$\#\{\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_3[u]} \mid \mathrm{Nrred}(\mathfrak{p}) < 2000,\ \deg_u(\mathfrak{p}) \equiv 0 \bmod 2\} = 947 \quad ,$$
$$\#\{\mathfrak{p} \in \mathbb{P}_{\mathbb{F}_3[u]} \mid \mathrm{Nrred}(\mathfrak{p}) < 2000,\ \deg_u(\mathfrak{p}) \equiv 1 \bmod 2,\ \mathfrak{p} \neq u\} = 1052 \quad .$$

Nimmt man an, daß zwei Matrizen aus $\begin{pmatrix} 1 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix}$ (bzw. aus $\begin{pmatrix} 2 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix}$) jeweils mit der gleichen Wahrscheinlichkeit auftreten, und untersucht, wie sich die Minimalpolynome auf die beiden Mengen verteilen, so erhält man folgende Vermutung über das Auftreten und die Häufigkeiten dieser Polynome:

$x-1$	$x-2$	$(x-1)^2$	$(x-2)^2$	$(x-1)(x-2)$
$\frac{947}{6}$	$\frac{1052}{6}$	$2 \cdot \frac{947}{6}$	$2 \cdot \frac{1052}{6}$	$3 \cdot \frac{947}{6} + 3 \cdot \frac{1052}{6}$
0.08	0.09	0.16	0.18	0.50

Die mit dem Computer ermittelten Häufigkeiten werden hierdurch sehr genau approximiert. □

Beispiel 6.2.9. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + \tau + u\tau^2)$$

und den

$$\text{Führer:} \qquad T^2 + 1 \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 2  ( 0  1 )  0  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 58
surjektiv=0
Fl=GF(9)
0 : [0]G=GL(2,Fl)
1 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
1 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
1 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
0 : [6]PG keine Ugr. von D_{2(l-1)}
0 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
1 : [11]ex. M in G mit <det(M)>=Fl^{ast}
1 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
1 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
0 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
0 : [17]ex. M in G mit cpol(M) irreduzibel
1 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
0 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
1 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
0 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
1 : [41]ex. M in G mit ord_{PGL}([M])>3
1 : [42]ex. M in G mit ord_{PGL}([M])>4
1 : [43]ex. M in G mit ord_{PGL}([M])>6
0 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
1 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
0 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
1 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Dieses Ergebnis erklärt sich wie folgt: Es ist

$$\phi_{T^2+1}(\tau) = (u^{10}\tau^2 + (u+u^3)\tau + u^2 + 1)(\tau^2 + 1) \quad ,$$

und die vollständige Faktorisierung lautet

$$\begin{aligned}\phi_{T^2+1}(x) = x\ (x^4 + 2x^2 + 2)\ (x^4 + x^2 + 2)& \\ \Big(u^{10}x^{72} + 2u^{10}x^{64} + u^{10}x^{56} + 2u^{10}x^{48} + u^{10}x^{40}& \\ + 2u^{10}x^{32} + u^{10}x^{24} + (u+u^3)x^{18} + 2u^{10}x^{16}& \\ + (2u^3 + 2u)x^{10} + u^{10}x^8 + (u+u^3)x^2 + 1 + u^2\Big)& \quad .\end{aligned}$$

An der Faktorisierung in $\mathbb{F}_q(u)\{\tau\}$ sehen wir bereits, daß der Drinfeld-Modul eine rationale (T^2+1)-Isogenie besitzt. Daher muß die Galoisgruppe eine Untergruppe der Borelgruppe sein, was auch die Belegung der Knoten 3 bis 10 nahelegt. Allerdings besagt die Belegung von Knoten 62, daß es keinen rationalen (T^2+1)-Torsionspunkt gibt, in Übereinstimmung mit der Faktorisierung von $\phi_{T^2+1}(x)$. Um die Erweiterung genauer zu untersuchen, numerieren wir die Torsionspunkte wie folgt durch:

$$\begin{aligned}\eta_1 = 0 \quad &, \quad \prod_{i=2}^{5}(x-\eta_i) = x^4 + 2x^2 + 2, \\ \prod_{i=6}^{9}(x-\eta_i) = x^4 + x^2 + 2 \quad &, \quad \prod_{i=10}^{81}(x-\eta_i) = \frac{\phi_{T^2+1}(x)}{x^9 + x} \quad ,\end{aligned}$$

und betrachten den Körperturm

$$\begin{array}{cl} \mathbb{F}_3(u)[{}_{T^2+1}\phi] & \\ | & \\ \mathbb{F}_3(u)[\eta_1, \ldots, \eta_9] & = \mathbb{F}_{3^4}(u) \quad . \\ | & \\ \mathbb{F}_3(u) & \end{array}$$

Es existieren Untergruppen H_1 und H_2 von $\mathbb{F}_9^*$ und eine Teilmenge M von $\mathbb{F}_9$, so daß nach passender Konjugation

$$\mathrm{Gal}(\mathbb{F}_3(u)[{}_{T^2+1}\phi], \mathbb{F}_3(u)) = \left\{ \begin{pmatrix} \alpha & \beta \\ 0 & \delta \end{pmatrix} \mid \alpha \in H_1, \delta \in H_2, \beta \in M \right\}$$

gilt. Dann ist die Galoisgruppe der Erweiterung $\mathbb{F}_3(u)[{}_{T^2+1}\phi]|\mathbb{F}_{3^4}(u)$ gerade

$$\left\{ \begin{pmatrix} 1 & \beta \\ 0 & \delta \end{pmatrix} \mid \delta \in H_2, \beta \in M \right\} \quad ,$$

und die Galoisgruppe der Konstantenerweiterung $\mathbb{F}_{3^4}(u)|\mathbb{F}_3(u)$ ist isomorph zu H_1. Da diese Erweiterung Grad 4 hat, muß $H_1 = \{\alpha^2 \mid \alpha \in \mathbb{F}_9^*\}$ sein. Wir werden nun zeigen, daß die Galoisgruppe $\mathrm{Gal}(\mathbb{F}_3(u)[{}_{T^2+1}\phi], \mathbb{F}_3(u))$ die ganze Gruppe

$$G := \left\{ \begin{pmatrix} \alpha^2 & \beta \\ 0 & \delta \end{pmatrix} \mid \alpha, \delta \in \mathbb{F}_9^*, \beta \in \mathbb{F}_9 \right\}$$

ist. Dazu haben wir zu den ersten 3000 endlichen Stellen $\mathfrak{p}(u)$ die Frobeniuselemente betrachtet. Es traten 30 verschiedene Minimalpolynome auf, unter anderem alle Minimalpolynome der Form $(x - \alpha^2)$ mit $\alpha \in \mathbb{F}_9^*$. Weiter auch ein Minimalpolynom der Form $(x-1)(x-\xi)$ mit $\langle \xi \rangle = \mathbb{F}_9^*$ und das Minimalpolynom $(x-1)^2$. Daher liegen für passende $\beta_\xi \in \mathbb{F}_9$, $b \in \mathbb{F}_9^*$ (die wir nicht genauer bestimmen können) die beiden Matrizen

$$\begin{pmatrix} 1 & \beta_\xi \\ 0 & \xi \end{pmatrix}, \quad \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

in der Galoisgruppe. Auch alle Matrizen

$$\begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^2 \end{pmatrix}$$

mit $\alpha \in \mathbb{F}_9^*$ kommen vor. Weiter ist

$$\langle \begin{pmatrix} 1 & \beta_\xi \\ 0 & \xi \end{pmatrix} \rangle = \left\{ \begin{pmatrix} 1 & f(\delta) \\ 0 & \delta \end{pmatrix} \mid \delta \in \mathbb{F}_9^* \right\}$$

für eine passende Funktion $f : \mathbb{F}_9^* \to \mathbb{F}_9$, und alle diese Matrizen liegen in der Galoisgruppe. Damit liegt für jedes $v \in \mathbb{F}_9^*$ auch

$$\begin{pmatrix} 1 & f(\frac{v}{b}) \\ 0 & \frac{v}{b} \end{pmatrix}^{-1} \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & f(\frac{v}{b}) \\ 0 & \frac{v}{b} \end{pmatrix} = \begin{pmatrix} 1 & v \\ 0 & 1 \end{pmatrix}$$

in der Galoisgruppe. Mit der Zerlegung

$$\begin{pmatrix} \alpha^2 & \beta \\ 0 & \delta \end{pmatrix} = \begin{pmatrix} \alpha^2 & 0 \\ 0 & \alpha^2 \end{pmatrix} \begin{pmatrix} 1 & f(\frac{\alpha^2}{\delta}) \\ 0 & \frac{\alpha^2}{\delta} \end{pmatrix}^{-1} \begin{pmatrix} 1 & \frac{\beta}{\alpha^2} + f(\frac{\alpha^2}{\delta})\frac{\delta}{\alpha^2} \\ 0 & 1 \end{pmatrix}$$

folgt dann

$$\mathrm{Gal}(\mathbb{F}_3(u)[{}_{T^2+1}\phi], \mathbb{F}_3(u)) = \left\{ \begin{pmatrix} \alpha^2 & \beta \\ 0 & \delta \end{pmatrix} \mid \alpha, \delta \in \mathbb{F}_9^*, \beta \in \mathbb{F}_9 \right\} \quad .$$

Betrachten wir diese Gruppe genauer. Es ist

$$\begin{aligned}
\mathcal{MP} \cap \{\mathrm{minpol}(A) \mid A \in G\} \\
&= \{(x-\alpha^2) \mid \alpha \in \mathbb{F}_9^*\} \\
&\quad \cup \{(x-\alpha^2)^2 \mid \alpha \in \mathbb{F}_9^*\} \\
&\quad \cup \{(x-\alpha^2)(x-\delta) \mid \alpha \in \mathbb{F}_9^*, \delta \in \mathbb{F}_9^* - (\mathbb{F}_9^*)^2\} \\
&\quad \cup \{(x-\alpha^2)(x-\delta^2) \mid \alpha, \delta \in \mathbb{F}_9^*, \alpha^2 \neq \delta^2\} \quad .
\end{aligned}$$

Die Mächtigkeiten dieser Mengen sind $4, 4, 16$ und 6. In den jeweiligen Mengen $\mathrm{Conj}(m(x), G)$ liegen $1, 8, 9$ bzw. 18 Elemente. Wir sehen, daß in G genau $4 + 4 + 16 + 6 = 30$ verschiedene Minimalpolynome auftreten können und daß unter den ersten 3000 Stellen alle diese Polynome gefunden wurden. □

Beispiel 6.2.10. Wir betrachten den

$$\text{Drinfeld-Modul:} \qquad (\mathbb{F}_3, \mathbb{F}_3(u), u, u + \tau + (u^3 + 2u + 1)\tau^2)$$

und den

$$\text{Führer:} \qquad T^3 + 2T + 1 \quad .$$

Das Programm liefert die folgende Ausgabe:

```
>>>>>
Drinfeldmodul=(GF(3), {GF(3)}(u) , u , DM)
DM= ( 2  ( 3  ( 0  1 )  1  ( 0  2 )  0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      1  ( 0  ( 0  1 ) )  ( 0  ( 0  1 ) )
      0  ( 1  ( 0  1 ) )  ( 0  ( 0  1 ) ) )
TorsStelle= ( 3  ( 0  1 )  1  ( 0  2 )  0  ( 0  1 ) )
Anzahl betrachtete Frob. (nur unverzweigte Stellen)= 59
surjektiv=0
Fl=GF(27)
0 : [0]G=GL(2,Fl)
0 : [1]det(G)=Fl^{ast}
0 : [2]PG=PGL(2,Fl)
0 : [3]PG keine Ugr. von PSL(2,Fl) oder PSL(2,Fl) keine echte Ugr.
1 : [4]PG keine Ugr. von PGL(2,Fn) mit Fn echter Teilkoerper von Fl
1 : [5]PG keine Ugr. von D_{2(l+1)}
       oder D_{2(l+1)} keine echte Ugr. von PGL(2,Fl)
1 : [6]PG keine Ugr. von D_{2(l-1)}
1 : [7]PG keine Ugr. von PBorel
1 : [8]PG keine Ugr. von A_{4} oder A_{4} keine echte Ugr. von PGL(2,Fl)
1 : [9]PG keine Ugr. von S_{4} oder S_{4} keine echte Ugr. von PGL(2,Fl)
1 : [10]PG keine Ugr. von A_{5} oder A_{5} keine echte Ugr. von PGL(2,Fl)
0 : [11]ex. M in G mit <det(M)>=Fl^{ast}
0 : [13]ex. M in G mit det(M) kein Quadrat
1 : [14]ex. M in G mit Tr(M)^2/det(M) nicht in Fn
        fuer alle echten TlKp Fn von Fl
1 : [15]ex. M in G mit 2(l+1) != 0 mod ord_{PGL}([M])
1 : [16]ex. M in G mit 2(l-1)  != 0 mod ord_{PGL}([M])
1 : [17]ex. M in G mit cpol(M) irreduzibel
1 : [18]ex. M in G mit 12 != 0 mod ord_{PGL}([M])
1 : [19]ex. M in G mit 24 != 0 mod ord_{PGL}([M])
1 : [20]ex. M in G mit 60 != 0 mod ord_{PGL}([M])
0 : [21]char(Fl)=2
0 : [22]#Fl=2
0 : [23]#Fl=3
0 : [24]#Fl=4
0 : [25]#Fl=5
1 : [30]char(Fl)!=2
0 : [31]char(Fl)!=3
1 : [32]char(Fl)!=5
1 : [41]ex. M in G mit ord_{PGL}([M])>3
1 : [42]ex. M in G mit ord_{PGL}([M])>4
1 : [43]ex. M in G mit ord_{PGL}([M])>6
1 : [44]ex. M in G mit cpol_{M} irreduzibel und Tr(M)!=0
```

```
1 : [45]ex. M in G mit cpol_{M}=(x-a)(x-b), a!=b und Tr(M)!=0
0 : [46]ex. M in G mit v_{p}(ordPGL(M))>0
1 : [61]ex. M in G mit det(M)!=1
1 : [62]ex. M in G mit cpol_{M}(1)!=0
<<<<<
```

Dieses Ergebnis erklärt sich wie folgt: Wir betrachten den assoziierten Rang-1 Modul

$$\psi = (\mathbb{F}_3, \mathbb{F}_3(u), u, u - (u^3 + 2u + 1)\tau) .$$

Dann ist

$$\psi_{T^3+2T+1}(x) = -(u^3 + 2u + 1)\ x\ p(x)\ p(-x)$$

mit

$$\begin{aligned} p(x) = {} & (u^{18} + u^{12} + 2u^9 + u^6 + u^3 + 1)\ x^{13} \\ & + (u^{15} + u^{13} + 2u^{12} + u^{11} + u^{10} + 2u^7 + 2u^6 + 2u^5 + u^3 + u^2 + u + 1)\ x^{10} \\ & + (2u^{12} + u^{10} + 2u^9 + u^6 + 2u^4 + u + 2)\ x^7 + (2u^9 + u^3 + 2)\ x^6 \\ & + (2u^9 + u^6 + u^4 + u^2 + u)\ x^4 + (2u^6 + 2u^4 + u^3 + 2u^2 + 2u + 2)\ x^3 \\ & + (u^3 + 2u + 1)\ x^2 + (u^3 + 2u + 1)\ x + 1 \quad . \end{aligned}$$

Daher ist

$$[\mathbb{F}_q(u)[{}_{\mathfrak{f}}\psi] : \mathbb{F}_q(u)] = 13$$

und

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{f}}\psi]\,, \mathbb{F}_q(u)) = \{\alpha^2 \mid \alpha \in \mathbb{F}_{\mathfrak{f}}{}^* = \mathbb{F}_{27}^*\} .$$

Damit muß

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{f}}\phi]\,, \mathbb{F}_q(u)) \leqslant \{M \in \mathrm{GL}(2, \mathbb{F}_{27}) \mid \det(M) \in (\mathbb{F}_{27}^*)^2\}$$

sein. Da für $\mathfrak{p}(u) = u^3 + 2u + 1$

$$\mathrm{v}_{\mathfrak{p}}(j(\phi)) = -1 < 0 \quad \text{und} \quad \mathrm{ggT}(3^{\deg_T(\mathfrak{f})}, \mathrm{v}_{\mathfrak{p}}(j(\phi))) = 1$$

ist, folgt aus Korollar 4.7.6, daß $\begin{pmatrix} 1 & \mathbb{F}_{27} \\ 0 & 1 \end{pmatrix}$ in der Galoisgruppe liegt. Die Belegung von Knoten [44] im Schaltgraph zeigt, daß es ein Element mit irreduziblem charakteristischen Polynom gibt. Nach Satz 3.2.5 liegt dann bereits ganz $\mathrm{SL}(2, \mathbb{F}_{27})$ in der Galoisgruppe. Da $\{\det(A) \mid A \in \mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{f}}\phi]\,, \mathbb{F}_q(u))\} = (\mathbb{F}_{27}^*)^2$ ist, ist

$$[\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{f}}\phi]\,, \mathbb{F}_q(u)) : \mathrm{SL}(2, \mathbb{F}_{27})] = 13$$

und damit

$$\mathrm{Gal}(\mathbb{F}_q(u)[{}_{\mathfrak{f}}\phi]\,, \mathbb{F}_q(u)) = \{A \in \mathrm{GL}(2, \mathbb{F}_{27}) \mid \det(A) \in (\mathbb{F}_{27}^*)^2\} \quad .$$

Da der Führer in diesem Beispiel Grad 3 hat, wurden alle Berechnungen deutlich aufwendiger. Insbesondere dauerte es viel länger, die GL-Ordnung (bzw. PGL-Ordnung) des Frobenius zu ermitteln, falls dessen charakteristisches Polynom eine doppelte Nullstelle hatte. Daher haben wir für den vorliegenden Drinfeld-Modul nur die ersten 1000 Stellen getestet. Da andererseits in der obigen Gruppe 377 Minimalpolynome auftreten können, ist die Datenbasis zu gering, um Vergleiche durchzuführen. Es sei nur erwähnt, daß unter den ersten 1000 Stellen bereits 325 verschiedene Minimalpolynome gefunden wurden. $\square$

Zur besseren Übersicht fassen wir die betrachteten Beispiele in einer Tabelle zusammen.

$\mathrm{DM} = (\mathbb{F}_3, \mathbb{F}_3(u), u, \phi_T)$			
Beispiel	ϕ_T	$\mathfrak{l}(T)$	$\mathrm{Gal}(\mathbb{F}_q(u)[\mathfrak{l}\phi], \mathbb{F}_q(u))$
6.2.1	$u + 2u\tau + \tau^2$	$T+2$	$\begin{pmatrix} 1 & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix}$
6.2.2	$u + (u+1)\tau + (2u^3+1)\tau^2$	T	$\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \rangle$
6.2.3	$u + (2u^3+2u+1)\tau + u^3\tau^2$	$T+2$	$\langle \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \rangle$
6.2.4	$u + u\tau + 2u\tau^2$	T	nichtzerfallende Cartangruppe
6.2.5	$u + u\tau + u\tau^2$	T	$\langle \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \rangle$
6.2.6	$u + 2u\tau + u\tau^2$	T	$\langle \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix} \rangle$
6.2.7	$u + (u^3+u+1)\tau + (u^3+1)\tau^2$	T	$\begin{pmatrix} \mathbb{F}_3^* & 0 \\ 0 & \mathbb{F}_3^* \end{pmatrix}$
6.2.8	$u + (u+1)\tau + \tau^2$	T	$\begin{pmatrix} \mathbb{F}_3^* & \mathbb{F}_3 \\ 0 & \mathbb{F}_3^* \end{pmatrix}$
6.2.9	$u + \tau + u\tau^2$	T^2+1	$\left\{ \begin{pmatrix} \alpha^2 & \beta \\ 0 & \delta \end{pmatrix} \mid \begin{array}{c} \alpha, \delta \in \mathbb{F}_9^* \\ \beta \in \mathbb{F}_9 \end{array} \right\}$
6.2.10	$u + \tau + (u^3+2u+1)\tau^2$	T^3+2T+1	$\left\{ \begin{array}{c} M \in \mathrm{GL}(2, \mathbb{F}_{27}), \\ \det(M) \in (\mathbb{F}_{27}^*)^2 \end{array} \right\}$

6.3 Ausblick

Zum Abschluß wollen wir noch kurz einige Verallgemeinerungen des in dieser Arbeit behandelten Problems ansprechen.

Betrachtet man statt der $\mathfrak{l}$-Torsion die $\mathfrak{l}^i$-Torsion, so ändert sich nichts am Drinfeld-theoretischen Teil des Problems. Allerdings ist in diesem Fall die Galoisgruppe eine Untergruppe von $\mathrm{GL}(2, \mathbb{F}_q[T]/\mathfrak{l}^i)$. Im Fall $i > 1$ ist $\mathbb{F}_q[T]/\mathfrak{l}^i$ nurnoch ein endlicher lokaler Ring und kein Körper mehr. Lineare Gruppen über solchen Ringen sind nicht vollständig verstanden. Zum Beispiel scheint eine Klassifikation der Konjugationsklassen solcher Gruppen noch nicht vorzuliegen. Charakteristisches Polynom und Ordnung reichen i.a. nicht, um für ein Element aus $\mathrm{GL}(2, \mathbb{F}_q[T]/\mathfrak{l}^i)$ die Konjugationsklasse festzulegen.

Demgegenüber sollte der Übergang von $\mathfrak{l}$ zu einem Produkt paarweise verschiedener irreduzibler Polynome $\prod_{i=1}^n \mathfrak{l}_i$ auf weniger Probleme stoßen. Es ist lediglich zu klären, unter welchen Bedingungen die Erweiterungen $\mathbb{F}_q(u)[\mathfrak{l}_i\phi]$ und $\mathbb{F}_q(u)[\mathfrak{l}_j\phi]$ linear disjunkt sind. Dies sollte im allgemeinen der Fall sein, obwohl zum Bei-

spiel im Fall $\phi = (\mathbb{F}_q, \mathbb{F}_q(u), u, u-\tau^2)$ die Körper $\mathbb{F}_q(u)[{}_T\phi]$ und $\mathbb{F}_q(u)[{}_{T+1}\phi]$ den gemeinsamen Teilkörper $\mathbb{F}_{q^2}(u)$ enthalten.
Eine andere Möglichkeit wäre es, die $\mathfrak{l}$-Torsion eines Rang-r Moduls für $r > 2$ zu betrachten. Dies würde zur Gruppe $\mathrm{GL}(r, \mathbb{F}_\mathfrak{l})$ führen. Deren Untergruppenstruktur ist zwar komplizierter als die der $\mathrm{GL}(2, \mathbb{F}_\mathfrak{l})$ aber immer noch gut untersucht (siehe [KL90]). Allerdings reicht bereits in der $\mathrm{GL}(3, \mathbb{F}_\mathfrak{l})$ die Kenntnis von Ordnung und charakteristischem Polynom nicht mehr aus, um die Konjugationstypen festzulegen, wie die Matrizen

$$\begin{pmatrix} a & 1 & 0 \\ 0 & a & 0 \\ 0 & 0 & a \end{pmatrix} \qquad \text{und} \qquad \begin{pmatrix} a & 1 & 0 \\ 0 & a & 1 \\ 0 & 0 & a \end{pmatrix}$$

zeigen. Außerdem müßten dann die charakteristischen Polynome von endlichen Rang-r Drinfeld-Moduln berechnet werden. Für solche Drinfeld-Moduln gibt es noch keine befriedigende Definition einer Hasse-Invarianten, es steht insbesondere keine Deligne-Kongruenz zur Verfügung. Dadurch wird die Berechnung des charakteristischen Polynoms aufwendiger. Sie wäre aber immer noch wie folgt möglich:
Sei $\phi = (\mathbb{F}_q, L, b, b + \sum_{i=1}^r b_i\tau^i)$ ein endlicher Drinfeld-Modul. Weiter sei $n := [L : \mathbb{F}_q]$, $\mathfrak{p}(T) = \mathrm{char}(\phi)$ und $\sum_{i=0}^r \alpha_i(T)\ x^i \in (\mathbb{F}_q[T])[x]$ das charakteristische Polynom. Dann gilt

$$\begin{aligned} \alpha_r(T) &= 1 \\ \alpha_0(T) &= \epsilon_\phi \cdot \mathfrak{p}(T) \\ \deg_T(\alpha_i) &\leqslant \frac{r-1}{r} \cdot n \end{aligned}$$

mit einem $\epsilon_\phi \in \mathbb{F}_q{}^*$. Da der Frobenius $\tau^n : x \mapsto x^{q^n} = x^{(\#L)}$ das charakteristische Polynom annulieren muß, erhält man die Bedingung

$$\sum_{i=0}^r \phi_{\alpha_i}(\tau) \cdot \tau^{i\cdot n} = 0 \quad .$$

Setzt man für $1 \leqslant i \leqslant (r-1)$ die $\alpha_i(T) = \sum_{j=0}^{\lfloor\frac{(r-1)n}{r}\rfloor} c_{ij} \cdot T^j \in \mathbb{F}_q[T]$ allgemein an, so erhält man

$$\sum_{i=1}^{r-1} \lfloor \frac{1}{r}(r-i)n \rfloor \leqslant \sum_{i=1}^{r-1} \frac{r-i}{r} n = \frac{1}{2}(r-1)n$$

Unbestimmte c_{ij}. Koeffizientenvergleich nach τ-Potenzen liefert $rn+1$ lineare Gleichungen. Um die c_{ij} (und damit die $\alpha_i(T)$) und das ϵ_ϕ zu bestimmen, muß man also ein überbestimmtes lineares Gleichungssystem über L lösen, das aus theoretischen Gründen bereits Lösungen über $\mathbb{F}_q$ haben muß.

Als weitere Verallgemeinerung könnte man Drinfeld-Moduln $\phi = (\mathbb{F}_q, K, u, u + g\tau + \Delta\tau^2)$ mit $\mathrm{char}(\phi) = \infty$ und $1 < [K : \mathbb{F}_q(u)]$ betrachten. In diesem Fall wäre die Galoisgruppe immer noch Untergruppe von $\mathrm{GL}(2, \mathbb{F}_{\mathfrak{l}})$. Die Berechnung von $\mathcal{P}_{\mathrm{Dred}(\phi,\mathfrak{p})}$ wird allerdings schwieriger. Sei $\mathfrak{P}$ eine Stelle von O_K, $L := O_K/\mathfrak{P}$ und ϕ habe gute Reduktion an $\mathfrak{P}$. Es sei

$$\overline{\phi} = (\mathbb{F}_q, L, \overline{u}, \overline{u} + \overline{g}\tau + \overline{\Delta}\tau^2)$$

der an $\mathfrak{P}$ reduzierte Drinfeld-Modul mit Charakteristik $\mathrm{char}(\overline{\phi}) = \mathfrak{p}(T)$. Dann ist

$$\mathcal{P}_{\bar{\phi}} = X^2 + A(T) \cdot X + \epsilon_\phi \mathfrak{p}^{[L:i_{\bar{\phi}}(\mathbb{F}_q[T])]} \in \mathbb{F}_q[T][X]$$

und

$$\deg_T(A) \leqslant \frac{\deg_T(\mathfrak{p})}{2} \cdot [L : i_{\bar{\phi}}(\mathbb{F}_q[T])] \ .$$

Da $[L : i_\phi(\mathbb{F}_q[T])] > 1$ ist, genügt in diesem Fall die Gleichung

$$i_\phi(A(T)) = -\epsilon_\phi \cdot \mathrm{Norm}^L_{\mathbb{F}_\mathfrak{p}}(\mathrm{H}(\phi))$$

nicht, um aus der Hasse-Invarianten das Polynom $A(T)$ zu bestimmen. Es ist natürlich möglich, $A(T)$ wie oben beschrieben durch das Lösen eines linearen Gleichungssystems zu ermitteln. Ist O_K kein Hauptidealring, so wird es auch schwieriger, ein Minimalmodell eines Drinfeld-Moduls zu erhalten. Weiter ist zu beachten, daß man in diesem Fall nicht mehr mit Polynomen rechnen kann, sondern zu Idealen übergehen muß. Dadurch werden alle Rechnungen aufwendiger.
Viele neue Probleme treten auf, wenn wir den Ring $\mathbb{F}_q[T]$ durch einen beliebigen Drinfeld-Ring A ersetzen. Wird dieser als $\mathbb{F}_q[T,Y]/f(T,Y)$ repräsentiert, so muß der Drinfeld-Modul durch zwei Frobenius-Polynome ϕ_T, ϕ_Y beschrieben werden. Für diese muß

$$\phi_T \cdot \phi_Y = \phi_{TY} = \phi_{YT} = \phi_Y \cdot \phi_T$$

und

$$0 = \phi_{f(T,Y)} = \phi_{\sum_{k=0}^d \sum_{i=0}^k c_{ki} T^i Y^{k-i}} = \sum_{k=0}^{d} \sum_{i=0}^{k} c_{ki} \phi_T^i \phi_Y^{k-i}$$

gelten. Dies liefert ein nichtlineares System von Bedingungen an die Koeffizienten von ϕ_T und ϕ_Y. Daher ist es in diesem Fall bereits ein nichttriviales Problem, einen Drinfeld-Modul explizit anzugeben.

Index

Literaturverzeichnis

[And86] Greg W. Anderson. t-motives. *Duke Math. J.*, 53(2):457–502, 1986.

[Bae95a] Sunghan Bae. Drinfeld modules with bad reduction over complete local rings. *Bull. Korean Math. Soc.*, 32(2):349–357, 1995.

[Bae95b] Sunghan Bae. Hecke characters of singular Drinfeld modules. *Pacific J. Math.*, 167(2):215–230, 1995.

[BK92] Sunghan Bae and Pyung-Lyun Kang. On Tate-Drinfeld modules. *Canad. Math. Bull.*, 35(2):145–151, 1992.

[BK93] Sunghan Bae and Pyung-Lyun Kang. Local isogeny theorem for Drinfeld modules with nonintegral invariants. *Proc. Amer. Math. Soc.*, 119(1):19–25, 1993.

[Che02] Imin Chen. Surjectivity of mod l representations attached to elliptic curves and congruence primes. *Canad. Math. Bull.*, 45(3):337–348, 2002.

[Cor99] Gunther Cornelissen. Deligne's congruence and supersingular reduction of Drinfeld modules. *Arch. Math. (Basel)*, 72(5):346–353, 1999.

[Dav01] Chantal David. Frobenius distributions of Drinfeld modules of any rank. *J. Number Theory*, 90(2):329–340, 2001.

[Dic01] Leonard Eugene Dickson. *Linear groups: With an exposition of the Galois field theory (Nachdruck New York: Dover Publ. 1958.* Teubner, Leipzig, 1901.

[Dri74] V. G. Drinfeld. Elliptic modules. *Mat. Sb. (N.S.)*, 94(136):594–627, 656, 1974.

[FJ86] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]*. Springer-Verlag, Berlin, 1986.

[FPS92] G. Frey, M. Perret, and H. Stichtenoth. On the different of abelian extensions of global fields. In *Coding theory and algebraic geometry (Luminy, 1991)*, volume 1518 of *Lecture Notes in Math.*, pages 26–32. Springer, Berlin, 1992.

[Gar01] Francis Gardeyn. *t-Motives and Galois Representations.* Dissertation, Gent, 2001.

[Geb02] Max Gebhardt. Constructing function fields with many rational places via the Carlitz module. *Manuscripta Math.*, 107(1):89–99, 2002.

[Gek88] Ernst-Ulrich Gekeler. On the coefficients of Drinfeld modular forms. *Invent. Math.*, 93(3):667–700, 1988.

[Gek91] Ernst-Ulrich Gekeler. On finite Drinfeld modules. *J. Algebra*, 141:187–203, 1991.

[GJ98] Wulf-Dieter Geyer and Moshe Jarden. Bounded realization of l-groups over global fields. The method of Scholz and Reichardt. *Nagoya Math. J.*, 150:13–62, 1998.

[Gos96] David Goss. *Basic Structures of Function Field Arithmetic.* Springer, Berlin, 1996.

[GS97] Ernst-Ulrich Gekeler and Brian A. Snyder. Drinfeld modules over finite fields. In E.-U. Gekeler et al, editor, *Drinfeld modules, modular schemes and applications (Alden-Biesen, 1996)*, pages 66–87. World Sci. Publishing, River Edge, NJ, 1997.

[Ham93] Yoshinori Hamahata. Tensor products of Drinfeld modules and v-adic representations. *Manuscripta Math.*, 79(3-4):307–327, 1993.

[Hay74] David R. Hayes. Explicit class field theory for rational function fields. *Trans. Amer. Math. Soc.*, (189):77–91, 1974.

[Hay79] David R. Hayes. Explicit class field theory in global function fields. In *Studies in algebra and number theory*, volume 6 of *Adv. in Math. Suppl. Stud.*, pages 173–217. Academic Press, New York, 1979.

[Hay92] David R. Hayes. A brief introduction to Drinfeld modules. In D. Goss et al, editor, *The Arithmetic of Function Fields*, pages 1–32. de Gruyter, 1992.

[Hup67] B. Huppert. *Endliche Gruppen*, volume 1. Springer-Verlag, 1967.

[HY00] Liang-Chung Hsia and Jing Yu. On characteristic polynomials of geometric Frobenius associated to Drinfeld modules. *Compositio Math.*, 122(3):261–280, 2000.

[Jun00] Florian Jung. Charakteristische Polynome von Drinfeld-Moduln. Diplomarbeit, Saarbrücken, 2000.

[Kel01] Alice Keller. Cyclotomic function fields with many rational places. In *Finite fields and applications (Augsburg, 1999)*, pages 293–302. Springer, Berlin, 2001.

[KL90] Peter Kleidman and Martin Liebeck. *The subgroup structure of the finite classical groups*, volume 129 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1990.

[Lan76] Serge Lang. *Introduction to modular forms*. Springer-Verlag, Berlin, 1976. Grundlehren der mathematischen Wissenschaften, No. 222.

[Lan93] Serge Lang. *Algebra*. Addison-Wesley, third edition, 1993.

[LN94] Rudolf Lidl and Harald Niederreiter. *Indroduction to finite fields and their applications*. Cambridge University Press, 1994.

[Lud95] Andrea Ludwig. Galoisdarstellungen auf den Torsionspunkten von elliptischen Kurven. Diplomarbeit, Saarbrücken, 1995.

[Maz78] B. Mazur. Rational isogenies of prime degree. *Invent. Math.*, 44(2):129–162, 1978.

[NX97] Harald Niederreiter and Chaoping Xing. Cyclotomic function fields, Hilbert class fields, and global function fields with many rational places. *Acta Arith.*, 79(1):59–76, 1997.

[Pin97] Richard Pink. The Mumford-Tate conjecture for Drinfeld-modules. *Publ. Res. Inst. Math. Sci.*, 33(3):393–425, 1997.

[Ros02] Michael Rosen. *Number Theory in Function Fields*. Springer, Berlin Heidelberg, 2002.

[Sch90] Fred Schultheis. Carlitz-Kummer function fields. *J. Number Theory*, 36(2):133–144, 1990.

[Sch96] Andreas Schweizer. *Zur Arithmetik der Drinfeld'schen Modulkurve* $X_0(\mathfrak{n})$. Dissertation, Saarbrücken, 1996.

[Ser68] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves.* McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968.

[Ser72] Jean-Pierre Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[Ser79] Jean-Pierre Serre. Points rationnels des courbes modulaires $X_0(N)$. In *Séminaire Bourbaki, 30e année (1977/78)*, volume 710 of *Lecture Notes in Math.*, pages Exp. No. 511, pp. 89–100. Springer, Berlin, 1979.

[Ser83] Jean-Pierre Serre. Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini. *C. R. Acad. Sci. Paris Sér. I Math.*, 296(9):397–402, 1983.

[Sil86] Joseph H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1986.

[Sil94] Joseph H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics.* Springer-Verlag, New York, 1994.

[Sim] Simath, homepage: http://tnt.math.metro-u.ac.jp/simath/.

[SSW96] R. Scheidler, A. Stein, and Hugh C. Williams. Key-exchange in real quadratic congruence function fields. *Des. Codes Cryptogr.*, 7(1-2):153–174, 1996. Special issue dedicated to Gustavus J. Simmons.

[Sti93] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer, Berlin Heidelberg, 1993.

[Tag92] Yuichiro Taguchi. Ramifications arising from Drinfeld modules. In *The arithmetic of function fields (Columbus, OH, 1991)*, volume 2 of *Ohio State Univ. Math. Res. Inst. Publ.*, pages 171–187. de Gruyter, Berlin, 1992.

[Tak82] Toyofumi Takahashi. Good reduction of elliptic modules. *J. Math. Soc. Japan*, 34(3):475–487, 1982.

[vdGvdV00] Gerard van der Geer and Marcel van der Vlugt. Tables of curves with many points. *Math. Comp.*, 69(230):797–810, 2000.

[vdGvdV03] Gerard van der Geer and Marcel van der Vlugt. Tables of curves with many points, updated version. available at http://www.wins.uva.nl/˜geer, 2003.

[VM80] Robert C. Valentini and Manohar L. Madan. A hauptsatz of L. E. Dickson and Artin-Schreier extensions. *J. Reine Angew. Math.*, 318:156–177, 1980.