Die Siegeldivisorklassengruppe der Drinfeld'schen Modulkurve $X(\mathfrak{p})$ als Galois-Modul

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

von
Bodo Wack

Saarbrücken
2001

Tag des Kolloquiums:	
Dekan:	Prof. Dr. R. Schulze-Pillot
Berichterstatter:	Prof. Dr. E.-U. Gekeler
	Prof. Dr. R. Schulze-Pillot

Inhaltsverzeichnis

Einleitung

Klassengruppen gehören zu den grundlegenden Objekten zahlentheoretischer Untersuchungen. In expliziter Form traten sie als Idealklassengruppen unmittelbar zusammen mit der Einführung der "idealen Zahlen" durch Kummer auf. Tatsächlich ist das Auftreten nichttrivialer Idealklassengruppen bei der Untersuchung der Arithmetik von Kreisteilungskörpern überhaupt erst der Anlaß für Kummer gewesen, Zahlen durch Ideale zu ersetzen. Bis heute haben Idealklassengruppen ihre Bedeutung in der algebraischen Zahlentheorie erhalten; sie haben sogar über die ursprüngliche direkte arithmetische Anwendung, beispielsweise bei der Untersuchung der Fermat-Gleichung, hinweg Eingang gefunden in weiter reichende Strukturtheorien wie etwa der Klassenkörpertheorie. Dabei fand im Laufe der Zeit eine Weiterentwicklung von Idealen und deren Klassengruppen hin zu Divisoren und Divisorklassengruppen statt. Dies begründet sich unter anderem in der Erkenntnis, daß viele bei Zahlkörpern angewendete Methoden sich auf den Fall beliebiger globaler Körper verallgemeinern lassen, d.h. auch für Funktionenkörper über endlichen Körpern gelten. Von geometrischer Sicht aus ist das Interesse an Divisoren, also dem Zählen von Null- und Polstellen, unmittelbar klar. Dies trifft insbesondere bei der Untersuchung von Kurven zu, wo die (Grad 0-)Divisorklassengruppe die Struktur einer algebraischen Varietät besitzt und auch als Jacobische der Kurve bezeichnet wird.

Ein interessanter Berührpunkt zwischen Divisorklassengruppen von Zahlkörpern und Kurven ergibt sich nun bei der Betrachtung von Modulkurven. Diese lassen sich sowohl klassisch in Charakteristik 0 als auch in positiver Charakteristik definieren und weisen in beiden Fällen viele Ähnlichkeiten auf. So setzen sie sich beispielsweise immer in natürlicher Weise zusammen aus einem affinen Teil und einer endlichen Menge von sogenannten Spitzen, welche die Kurven projektiv abschließen. Die Punkte des affinen Teils parametrisieren Isomorphieklassen von zahlentheoretisch interessanten Objekten, nämlich elliptischen Kurven im Fall von Charakteristik 0 sowie Rang 2-Drinfeld-Moduln im Fall positiver Charakteristik. Obwohl die Spitzen selbst bei dieser Parametrisierung nicht auftreten, sind auch sie von zahlentheoretischem Interesse. Betrachtet man nämlich neben dem geometrischen Aspekt auch Rationalitätsfragen, so stellt sich heraus, daß die Spitzen in gewisser Weise triviale Punkte der Modulkurve sind, so ähnlich wie die

Punkte $(0,1)$ und $(1,0)$ der Fermat-Kurve $X^n+Y^n=1$. Im klassischen Fall, d.h. in Charakteristik 0, läßt die Erkenntnis, daß diese trivialen Punkte manchmal schon alle rationalen Punkte über einem Zahlkörper sind, wieder Rückschlüsse auf das Parametrisierungsproblem bei elliptischen Kurven zu [**Maz**]. Im Hinblick auf Klassengruppen zeichnen sich die Spitzen dadurch aus, daß die von ihnen in der Jacobischen der Modulkurve erzeugte Untergruppe formale Ähnlichkeiten mit Idealklassengruppen von Zahlkörpern besitzt. Betrachtet man wieder den Zahlkörperfall, so lassen sich durch die Untersuchung solcher Spitzendivisorklassengruppen wesentliche Aussagen über die Struktur von Idealklassengruppen von Kreisteilungskörpern folgern [**Ri**],[**MazWi**]. Das Ziel dieser Arbeit ist es, Informationen über die Spitzendivisorklassengruppe im Funktionenkörperfall zu gewinnen.

Natürlich spielt in all ihren Anwendungen die Struktur der oben beschriebenen Klassengruppen eine wesentliche Rolle. Obwohl sie, wie der Name schon sagt, eine Gruppenstruktur besitzen, ist sogar schon ihre Elementanzahl eine bedeutende Information, insbesondere die Frage, ob sie nur ein Element besitzen oder mehrere. Im Falle der Idealklassengruppen von Zahlkörpern kann man daran zum Beispiel ablesen, ob es in dem entsprechenden Ganzheitsring eine eindeutige Primfaktorzerlegung gibt oder nicht. Aber auch wenn man sich nur für ihre Elementanzahl interessiert, ist die Gruppenstruktur der Klassen schon nützlich, sie erlaubt beispielsweise eine Zerlegung in primäre Komponenten, welche getrennt voneinander untersucht werden können. Gehört zu dem betrachteten Zahl- oder Funktionenkörper sogar eine Galois-Gruppe, so tragen die Klassengruppen eine noch wesentlich reichere Struktur. Aufgrund der Operation der Galois-Gruppe auf dem Körper ergibt sich nämlich auch eine solche Operation auf einer ganzen Reihe von dem Körper in natürlicher Weise zugeordneten Objekten, wie eben auch der Ideal- oder Divisorklassengruppe. Solche Galois-Moduln sind ein wichtiges Beispiel für zahlentheoretische Anwendungen der Darstellungstheorie. In dem von uns betrachteten Fall von Modulkurven sind die vorkommenden Galois-Gruppen vom Typ GL(2) über endlichen Körpern. Wie bei allen klassischen Matrixgruppen sind alle darstellungstheoretischen Eigenschaften dieser Gruppen interessant, und zwar nicht nur aus zahlentheoretischer Sicht. Wir werden uns speziell mit den modularen Darstellungen der auftretenden Galois-Gruppen beschäftigen, d.h. mit Darstellungen in positiver Charakteristik. In den zahlentheoretischen Anwendungen von Klassengruppen ist nämlich oft eine Primzahl p ausgezeichnet, im klassischen Fall beispielsweise bei der Untersuchung des p-ten Kreisteilungskörpers, im Funktionenkörperfall durch die vorliegende Charakteristik. In solchen Fällen spielt die p-primären Komponente der Klassengruppe eine besondere Rolle. In ihr bildet die Untergruppe der von p annullierten Elemente einen

$\mathbb{F}_p$-Vektorraum und liefert so eine modulare Darstellung der Galois-Gruppe. Im Vergleich zu Darstellungen in Charakteristik 0 besitzen modulare Darstellungen im allgemeinen eine kompliziertere Struktur, da sie nicht halbeinfach sein müssen. Dieser Umstand wird in einer Arbeit von B. Gross im Fall klassischer Modulkurven ausgenutzt, um Aussagen über den p-Anteil der Spitzendivisorklassengruppe der klassischen Modulkurve $X(p)$ zu machen [**Gr**]. Dieser Ansatz läßt sich auch im Funktionenkörperfall bei der Drinfeld'schen Modulkurve $X(\mathfrak{p})$ verfolgen. Dabei treten allerdings im Gegensatz zur klassischen Situation als Koeffizientenbereich der Matrixgruppen nicht nur Primkörper auf, sondern beliebige endliche Körper, wodurch die Darstellungstheorie der betrachteten Gruppen wesentlich komplizierter wird.

Die vorliegende Arbeit gliedert sich in vier Teile. Im ersten Kapitel befassen wir uns mit Grundlagen von Modulkurven. Zur Motivation und Veranschaulichung betrachten wir zuerst klassische Modulkurven und geben verschiedene Methoden zu ihrer Beschreibung an. Danach wenden wir uns dem Funktionenkörperfall zu. Wir beschreiben Drinfeld-Moduln und gehen insbesondere auf solche von Rang 1 und 2 ein. Im Anschluß beschreiben wir Drinfeld'sche Modulkurven, welche Parameterräume für Rang 2-Drinfeld-Moduln darstellen, so wie klassische Modulkurven für elliptische Kurven. Nach einer kurzen Diskussion der Bedeutung von Ideal- und Divisorklassengruppen im allgemeinen wenden wir uns dann Spitzendivisorklassengruppen der klassischen Modulkurven $X(p)$ zu und skizzieren die Idee aus [**Gr**], diese mittels modularer Darstellungen zu untersuchen.

Im zweiten Kapitel beschäftigen wir uns dann speziell mit der Drinfeld'schen Modulkurve $X(\mathfrak{p})$ zu einer Hauptkongruenzuntergruppe $\Gamma(\mathfrak{p})$. Wir beschreiben den Funktionenkörper und die zugehörige Galois-Gruppe und untersuchen die darstellungstheoretische Struktur von modularen Einheiten, Divisoren und Divisorklassengruppen. Neben der Gruppe D_S^0 der Spitzendivisoren vom Grad 0 werden insbesondere die sogenannten Siegel-Funktionen, die von ihren Divisoren erzeugte Gruppe $\mathcal{S}$ sowie der von der Divisorabbildung induzierter Homomorphismus $\mathcal{S}/p\mathcal{S} \to D_S^0/pD_S^0$ von Interesse sein. Der Kern dieses Homomorphismus ist gerade die p-Torsion der Siegeldivisorklassengruppe, für die wir uns interessieren. Nach Identifikation der darstellungstheoretischen Struktur von $\mathcal{S}/p\mathcal{S}$ und D_S^0/pD_S^0 können diese Galois-Moduln dann losgelöst von ihrer geometrischen Herkunft mit abstrakten Methoden der modularen Darstellungstheorie untersucht werden.

In Kapitel 3 beschäftigen wir uns daher mit den Besonderheiten modularer Darstellungen. Der wesentliche Unterschied zur Darstellungstheorie in Charakteristik 0 besteht darin, daß modulare Darstellungen im allgemeinen nicht die direkte Summe ihrer einfachen Faktoren sein müssen. Wir entwickeln eine Methode, dies zur Untersuchung von Homomorphismen zwischen modularen Darstellungen auszunutzen, bei der man den vorliegenden Homomorphismus nicht kennen muß, sondern nur Information über die beteiligten Darstellungen verwendet. Dies wird uns später Informationen über den Kern von $\mathcal{S}/p\mathcal{S} \to D_S^0/pD_S^0$ liefern. Danach spezialisieren wir uns auf die Gruppe $\mathrm{GL}(2, \mathbb{F}_q)$, da die bei der Modulkurve $X(\mathfrak{p})$ auftretende Galois-Gruppe von diesem Typ ist. Neben den einfachen Darstellungen von $\mathrm{GL}(2, \mathbb{F}_q)$ untersuchen wir die spezielle Klasse der Hauptreihendarstellungen, aus denen sich die in Kapitel 2 gefundenen Galois-Moduln $\mathcal{S}/p\mathcal{S}$ und D_S^0/pD_S^0 zusammensetzen lassen. Als Matrix-Gruppe besitzt $\mathrm{GL}(2, \mathbb{F}_q)$ eine natürliche zweidimensionale Darstellung, und es stellt sich heraus, daß symmetrische Potenzen dieser natürlichen Darstellung sowohl bei den einfachen Darstellungen als auch bei den Hauptreihendarstellungen eine zentrale Rolle spielen. Insbesondere gelingt es uns, eine Methode zur Berechnung der Sockelreihe der symmetrischen Potenzen innerhalb des in unserer Situation auftretenden Parameterbereichs zu finden. Deren Kenntnis erlaubt Rückschlüsse auf die Hauptreihendarstellungen und damit auf die bei $X(\mathfrak{p})$ auftretenden Galois-Moduln.

Das vierte Kapitel enthält Anwendungen der Resultate des vorigen Kapitels. Wir geben einige Beispiele für die Berechnung von Sockelreihen symmetrischer Potenzen der natürlichen Darstellung von $\mathrm{GL}(2, \mathbb{F}_q)$ an und sind auch in der Lage, ein paar allgemeine strukturelle Aussagen zu zeigen. Auch in Bezug auf die Modulkurve geben wir in einigen Beispielen an, wie unsere darstellungstheoretischen Resultate zu Aussagen über Spitzendivisorklassengruppen führen, insbesondere über deren p-Anteil. Auch hier sind wir neben der konkreten Behandlung beliebiger Beispiele in der Lage, einige allgemeine Strukturaussagen anzugeben. Insbesondere wird sich herausstellen, daß die beiden Galois-Moduln $\mathcal{S}/p\mathcal{S}$ und D_S^0/pD_S^0 genau die gleichen einfachen Faktoren haben, wodurch die von uns getroffene Wahl der Untersuchungsmethoden gewissermaßen nachträglich als notwendig bestätigt wird.

An dieser Stelle möchte ich mich ganz besonders bei Herrn Prof. Dr. Ernst-Ulrich Gekeler bedanken, dessen Rat und Anleitung in mathematischen Dingen mich seit Beginn meines Studiums bis hin zur Fertigstellung der vorliegenden Arbeit begleitet haben. Auch bei allen weiteren Mitgliedern der Arbeitsgruppe bedanke ich mich für die gute Zusammenarbeit in den letzten Jahren.

KAPITEL 1

Grundlagen zu Modulkurven

In diesem Kapitel beschreiben wir einige Aspekte der Theorie klassischer und Drinfeld'scher Modulkurven. Obwohl der Gegenstand unserer Untersuchungen später Drinfeld'sche Modulkurven sein werden, beginnen wir im ersten Abschnitt mit einer kurzen Skizzierung der klassischen Theorie. Aufgrund der weitreichenden Analogien kann sie einerseits zur Motivation und andererseits als Orientierungshilfe für die Drinfeld'sche Theorie dienen. Zu diesem Zweck begnügen wir uns mit einer übersichtsartigen Darstellung ausgewählter Aspekte. Darüber hinaus gehende Informationen bzw. Beweise der geschilderten Sachverhalte findet man für den klassischen Fall in vielen Büchern über Modulformen, wie z.B. [**La2**],[**Mi**],[**Sh**], für den Fall von Drinfeld'schen Modulkurven in [**Ge4**],[**GeRe**]. Im zweiten Abschnitt gehen wir dann zu Drinfeld'schen Modulkurven über und beschreiben im wesentlichen dieselben Aspekte wie im vorigen Abschnitt. Da unser besonderes Interesse den Spitzendivisorklassengruppen von Modulkurven gilt, gehen wir im dritten Abschnitt etwas auf deren Bedeutung und Anwendungen ein. Im letzten Abschnitt dieses Kapitels erläutern wir eine Methode aus [**Gr**] zur Untersuchung der Galois-Modulstruktur von Spitzendivisorklassengruppen einer klassischen Modulkurve. Diese ist in den folgenden Kapiteln die Grundidee für unser Vorgehen bei Drinfeld'schen Modulkurven.

1.1. Klassische Modulkurven

Obwohl sie erstmals im Zusammenhang mit elliptischen Integralen und damit im Rahmen analytischer Untersuchungen auftraten, stellen elliptische Kurven heute einen wichtigen Bereich der Zahlentheorie dar. Über den komplexen Zahlen ist jede elliptische Kurve gegeben durch eine kurze Weierstraß-Gleichung

$$E : y^2 = x^3 + Ax + B$$

mit $4A^3 + 27B^2 \neq 0$. Definiert man die j-Invariante

$$j(E) := 1728 \cdot \frac{4A^3}{4A^3 + 27B^2},$$

so sind zwei elliptische Kurven genau dann isomorph, wenn sie die gleiche j-Invariante haben. Außerdem tritt jede komplexe Zahl als

j-Invariante einer elliptischen Kurve auf und somit hat man eine Bijektion

$$\{\text{Isomorphieklassen von elliptischen Kurven über } \mathbb{C}\} \xrightarrow[\cong]{j} \mathbb{C}\,.$$

Es gibt also eine projektive Kurve, nämlich die projektive Gerade $\mathbb{P}^1(\mathbb{C})$, deren affine Punkte $\mathbb{A}^1(\mathbb{C})$ in Bijektion stehen zu Isomorphieklassen elliptischer Kurven. Dies ist das einfachste Beispiel einer Modulkurve. Etwas allgemeiner sucht man projektive Kurven, deren affine Punkte Isomorphieklassen von elliptischen Kurven mit einer Zusatzstruktur parametrisieren. In dem für uns wesentlichen Fall ist diese Zusatzstruktur wie folgt gegeben. Für ein fest gewähltes $n \in \mathbb{N}$ und eine fest gewählte n-te Einheitswurzel betrachtet man elliptische Kurven E zusammen mit zwei Erzeugern a, b der n-Torsion, deren Weil-Paarung die fixierte Einheitswurzel ist. Zwei solche Tripel (E, a, b), (E', a', b') heißen isomorph, wenn es einen Isomorphismus zwischen E und E' gibt, der a auf a' und b auf b' abbildet.

Weitere Beispiele für mögliche Zusatzstrukturen bestehen bei fixiertem n in der Angabe einer zyklischen Untergruppe der Ordnung n oder der zusätzlichen Angabe eines Punktes der Ordnung n.

Eine Lösung für die eben beschriebenen Parametrisierungsaufgaben stellen nun gerade die Modulkurven dar. Sie lassen sich auf drei verschiedene Arten beschreiben.

Die erste Möglichkeit ist die Beschreibung als kompakte Riemannsche Fläche. Die Gruppe $\mathrm{GL}(2, \mathbb{Z})$ operiert auf $\mathbb{P}^1(\mathbb{C})$ durch

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot [z : w] = [az + cw : bz + dw]\,.$$

Schränkt man sich auf die Untergruppe $\mathrm{SL}(2, \mathbb{Z})$ ein, so ist die komplexe obere Halbebene $\mathbb{H} = \{z \in \mathbb{C} \mid \mathrm{Re}(z) > 0\}$ abgeschlossen unter der Operation, welche dort gegeben ist durch gebrochen-rationale Transformationen, d.h. durch

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot z = \frac{az + c}{bz + d}\,.$$

Sei nun wieder $n \in \mathbb{N}$ fest und Γ eine der folgenden Untergruppen:

$$\Gamma(n) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \,\middle|\, a \equiv d \equiv 1 \bmod n,\ b \equiv c \equiv 0 \bmod n \right\}\,,$$

$$\Gamma_1(n) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \,\middle|\, a \equiv d \equiv 1 \bmod n,\ b \equiv 0 \bmod n \right\}\,,$$

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}) \,\middle|\, b \equiv 0 \bmod n \right\}\,.$$

Der Quotient $\Gamma\backslash\mathbb{H}$ besitzt eine natürliche Struktur als offene Riemannsche Fläche, so daß bis auf endlich viele Ausnahmen für einen Punkt

$z \in \mathbb{H}$ eine lokale Koordinate von $p(z) := z \bmod \Gamma$ gegeben ist durch $p^{-1} : p(U) \xrightarrow{\cong} U$ für eine genügend kleine Umgebung U von z. Durch Hinzufügen endlich vieler Punkte, der sogenannten Spitzen, erhält man dann eine kompakte Riemannsche Fläche X_Γ, die komplexe Modulkurve zu Γ. Die Spitzen lassen sich wie folgt beschreiben. Die Bahn von ∞ unter der Operation von $\mathrm{SL}(2,\mathbb{Z})$ auf $\mathbb{P}^1(\mathbb{C})$ ist gerade $\mathbb{P}^1(\mathbb{Q})$, und die Menge der Spitzen läßt sich identifizieren mit $\Gamma\backslash\mathbb{P}^1(\mathbb{Q})$.

Da jede kompakte Riemannsche Fläche einer nichtsingulären projektiven algebraischen Kurve über $\mathbb{C}$ entspricht, gilt dies auch für die eben beschriebenen Riemannschen Flächen X_Γ. Dabei entspricht der offene Anteil $\Gamma\backslash\mathbb{H}$ einer affinen Kurve und die Spitzen den Punkten des projektiven Abschlußes. Eine Besonderheit dieser Modulkurven ist nun, daß sie schon über algebraischen Zahlkörpern definiert sind, im Falle von $\Gamma(n)$ über einem Kreisteilungskörper, in den Fällen $\Gamma_1(n)$ und $\Gamma_0(n)$ sogar schon über $\mathbb{Q}$. Bei der Untersuchung von Modulkurven spielen also auch arithmetische Eigenschaften eine Rolle, die aus der rein analytischen Beschreibung nicht direkt hervorgehen.

Neben der analytischen und der geometrischen Beschreibung gibt es auch noch eine algebraische Beschreibung, nämlich die mittels des Funktionenkörpers. Sowohl der Riemannschen Fläche als auch der algebraischen Kurve sind in natürlicher Weise Funktionenkörper zugeordnet. Im Fall der Riemannschen Fläche handelt es sich um den Körper der meromorphen Funktionen auf X_Γ. Zu X_Γ als algebraischer Kurve gehört der Körper der rationalen Funktionen auf X_Γ, den man z.B. als Quotientenkörper des affinen Koordinatenrings erhält. Dieser hängt natürlich davon ab, über welchem Grundkörper man die Kurve betrachtet. Wählt man als Grundkörper die komplexen Zahlen, so ist der Funktionenkörper von X_Γ als algebraische Kurve isomorph zum Körper der meromorphen Funktionen der Riemannschen Fläche X_Γ. Um arithmetische Eigenschaften zu untersuchen, wählt man als Grundkörper meist den kleinsten Körper, über dem die Kurve definiert ist.

Man kann natürlich auch noch andere als die angegebenen Gruppen $\Gamma(n)$, $\Gamma_1(n)$, $\Gamma_0(n)$ verwenden, solange sie gewisse Voraussetzungen erfüllen, die es erlauben, den Quotienten $\Gamma\backslash\mathbb{H}$ mit einer Struktur als Riemannsche Fläche zu versehen. Die angegebenen Beispiele sind aber die wichtigsten, sie liefern z.B. die Lösungen für die bereits erwähnten Parametrisierungsprobleme. Für $\Gamma_0(n)$ erhält man die Parametrisierung elliptischer Kurven mit einer zyklischen Torsionsuntergruppe der Ordnung n, für $\Gamma_1(n)$ ist die Zusatzstruktur die der Angabe eines Punktes der Ordnung n und für $\Gamma(n)$ die Angabe zweier Erzeuger der n-Torsion, deren Weil-Paarung eine fixierte n-te Einheitswurzel ist.

Klassische Modulkurven haben in der Zahlentheorie vielfältige Anwendungen, von denen wir im folgenden kurz einige erwähnen. Aufgrund des bereits geschilderten Zusammenhangs mit der Parametrisierung elliptischer Kurven ist es klar, daß Modulkurven in der Theorie der elliptischen Kurven eine wichtige Rolle spielen. Die Bestimmung aller Möglichkeiten für die Struktur von Torsionsgruppen elliptischer Kurven über $\mathbb{Q}$ durch Mazur [**Maz**] wurde durch die im wesentlichen dazu äquivalente Bestimmung der $\mathbb{Q}$-rationalen Punkte gewisser Modulkurven erreicht. Ein weiterer Zusammenhang mit elliptischen Kurven besteht in der Möglichkeit, die Modularitätseigenschaft einer elliptischen Kurve dadurch zu formulieren, daß ein nichtkonstanter Morphismus von einer bestimmten Modulkurve auf die betrachtete elliptische Kurve existiert. Man kann die Modularität aber auch dadurch definieren, daß die L-Reihe der betrachteten elliptischen Kurve die Mellin-Transformierte einer bestimmten Modulform ist. Auch die gesamte Theorie der Modulfunktionen und Modulformen hängt eng mit den Modulkurven zusammen, denn die Modulfunktionen sind gerade die Elemente des Funktionenkörpers der Modulkurve, während Modulformen mit Differentialformen auf der Modulkurve zusammenhängen.

Neben dem naheliegenden Zusammenhang mit elliptischen Kurven spielen Modulkurven aber auch eine wichtige Rolle in der Theorie der Kreisteilungskörper und insbesondere ihrer Idealklassengruppen. Dies wird im dritten Abschnitt genauer beschrieben. Aufgrund des Zusammenhangs mit Kreisteilungskörpern ist es auch nicht überraschend, daß es eine Verbindung zwischen Modulkurven und der Fermat-Gleichung gibt. Schon vor dem Beweis der Mordell-Vermutung durch Faltings war bekannt, daß die Fermat-Kurve $x^n + y^n = 1$ genau dann nur endlich viele rationale Punkte über jedem Zahlkörper hat, wenn dies auch für die Modulkurve $X_{\Gamma(2n)}$ zutrifft [**KuLa**, S. 196].

1.2. Drinfeld'sche Modulkurven

Nach der Betrachtung der klassischen Situation wenden wir uns nun dem Fall positiver Charakteristik zu. Während der Rahmen der Theorie in Charakteristik 0 gebildet wird durch den Ring $\mathbb{Z}$, seinen Quotientenkörper $\mathbb{Q}$, dessen Vervollständigung $\mathbb{R}$ sowie den algebraischen Abschluß $\mathbb{C}$ davon, so sind die grundlegenden Objekte nun wie folgt gegeben: wir starten mit dem Ring $A = \mathbb{F}_r[T]$ der Polynome in einer Unbestimmten über einem endlichen Körper $\mathbb{F}_r$ der Charakteristik p mit r Elementen. Der Quotientenkörper $K = \mathbb{F}_r(T)$ von A besitzt eine diskrete, nichtarchimedische Bewertung v_∞ mit Parameter $\frac{1}{T}$, und als Vervollständigung von K bezüglich dieser Bewertung erhält man den Körper $K_\infty = \mathbb{F}_r((\frac{1}{T}))$ der formalen Laurentreihen in dem Parameter. Schließt man diesen Körper algebraisch ab, so geht die Vollständigkeit zwar verloren, aber die algebraische Abgeschlossenheit bleibt bei erneutem Vervollständigen erhalten und man erhält einen vollständigen und algebraisch abgeschlossenen Oberkörper $C = \widehat{\overline{K}}_\infty$ von K, auf den sich die Bewertung v_∞ eindeutig fortsetzt.

Während im Fall von Charakteristik 0 der Körpergrad $[\mathbb{C} : \mathbb{R}] = 2$ vorliegt, ist C eine unendliche Erweiterung von K_∞. Eine Konsequenz daraus ist die Tatsache, daß es in C diskrete endlich erzeugte A-Moduln beliebigen Rangs gibt, während $\mathbb{Z}$-Gitter in $\mathbb{C}$ höchstens den Rang 2 haben können. Solche $\mathbb{Z}$-Gitter in $\mathbb{C}$ und die mit ihrer Hilfe gebildeten Quotienten haben große zahlentheoretische Bedeutung. Die komplexe Exponentialabbildung mit dem Periodengitter $2\pi i\mathbb{Z}$ beispielsweise liefert einen $\mathbb{Z}$-Modul-Isomorphismus

$$\mathbb{C}/2\pi i\mathbb{Z} \xrightarrow{\exp} \mathbb{C}^*$$

zwischen dem Quotienten $\mathbb{C}/2\pi i\mathbb{Z}$ und der multiplikativen Gruppe von $\mathbb{C}$, unter dem ein n-Torsionspunkt von $\mathbb{C}/2\pi i\mathbb{Z}$ auf eine n-te Einheitswurzel abgebildet wird. Ein Gitter Λ vom Rang 2 in $\mathbb{C}$ ist das Periodengitter einer Weierstraß'schen $\wp$-Funktion, welche einen Isomorphismus zwischen dem Torus $\mathbb{C}/\Lambda$ und einer elliptischen Kurve liefert.

Ist nun Λ ein A-Gitter in C, d.h. ein diskreter endlich erzeugter A-Untermodul, so definiert

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

eine ganze, surjektive $\mathbb{F}_r$-lineare Funktion auf C, die nur einfache Nullstellen hat, und zwar genau in den Punkten von Λ. Diese Funktion ist ein Analogon der klassischen Exponentialfunktion bzw. der Weierstraß'schen $\wp$-Funktion. Sie induziert einen $\mathbb{Z}$-Modul-Isomorphismus $C/\Lambda \to C$, durch den C eine neue, von dem Quotienten C/Λ kommende A-Modulstruktur erhält, deren Skalarmultiplikation wir mit $*_\Lambda$ bezeichnen.

Neben der analytischen Beschreibung mittels der Funktion e_Λ besitzt diese neue A-Modulstruktur auf C auch eine algebraische Beschreibung, welche man als Analogon der Multiplikation komplexer Zahlen in $\mathbb{C}^*$ bzw. der Gruppenstruktur auf einer elliptischen Kurve deuten kann. Eine A-Modulstruktur auf C entspricht einem Ring-Homomorphismus von A in den Endomorphismenring der additiven Gruppe $(C, +)$ von C. Da wir an einer algebraischen Beschreibung interessiert sind, betrachten wir nur solche Endomorphismen von $(C, +)$, die durch Polynome gegeben sind, und wir verlangen außerdem noch Verträglichkeit mit den Konstanten von A, d.h. wir lassen nur $\mathbb{F}_r$-lineare Polynome zu. Solche Polynome lassen sich durch den getwisteten Polynomring $C\{\tau\}$ beschreiben. Dieser hat als C-Vektorraum die Basis $\{\tau^k \mid k \in \mathbb{N}_0\}$ und die mit $\circ$ bezeichnete Multiplikation ist definiert durch

$$\sum_i a_i \tau^i \circ \sum_j b_j \tau^j = \sum_{i,j} a_i b_j^{r^i} \tau^{i+j} \,,$$

d.h. die Unbestimmte τ vertauscht nicht mit den Konstanten aus C, sondern es gilt die Regel $\tau \circ a = a^r \circ \tau$. Ersetzt man τ durch X^r und die Multiplikation durch die Hintereinanderausführung, so wird $C\{\tau\}$ gerade zum Unterring der $\mathbb{F}_r$-linearen Polynome, aufgefaßt als Unterring des Endomorphismenrings von $(C,+)$. Die algebraische Beschreibung der durch

$$C/\Lambda \xrightarrow{e_\Lambda} C$$

auf C induzierten A-Modulstruktur ergibt sich wie folgt: zu jedem $a \in A$ existiert ein Element $\varphi_a^\Lambda \in C\{\tau\}$ mit $e_\Lambda(a \cdot w) = \varphi_a^\Lambda(e_\Lambda(w))$, d.h. für ein $w \in e_\Lambda^{-1}(z)$ ist

$$a *_\Lambda z = e_\Lambda(a \cdot w) = \varphi_a^\Lambda(e_\Lambda(w)) = \varphi_a^\Lambda(z)\,.$$

Eine genauere Untersuchung der Eigenschaften der so definierten Abbildung $a \mapsto \varphi_a^\Lambda$ führt zum Begriff des Drinfeld-Moduls.

Definition 1.2.1. Ein Drinfeld-Modul vom Rang n über C ist ein $\mathbb{F}_r$-Algebren-Homomorphismus

$$\varphi : A \longrightarrow C\{\tau\};\ a \mapsto \varphi_a\,,$$

wobei $\varphi_T = \sum_{i=0}^n \alpha_i \tau^i$ ist mit $\alpha_0 = T$ und $\alpha_n \neq 0$. Sind φ und ψ zwei Drinfeld-Moduln, so ist ein Homomorphismus von φ nach ψ ein Element $u \in C\{\tau\}$ mit $u \circ \varphi_a = \psi_a \circ u$ für alle $a \in A$. Homomorphismen von Drinfeld-Moduln werden verknüpft, indem man sie in $C\{\tau\}$ mittels $\circ$ multipliziert.

Offensichtlich bilden Drinfeld-Moduln mit ihren Homomorphismen eine Kategorie. Die beiden Bedingungen an den speziellen Wert eines Drinfeld-Moduls φ an der Stelle T bewirken, daß für jedes $a \in A$ die Ableitung des φ_a entsprechenden additiven Polynoms mit a übereinstimmt und daß der τ-Grad von φ_a gerade das n-fache des T-Grades von a ist.

Man kann zeigen, daß die oben beschriebene, von einem Gitter Λ kommende Abbildung φ^Λ ein Drinfeld-Modul ist, dessen Rang mit dem Rang des Gitters übereinstimmt. Darüber hinaus ist jeder Drinfeld-Modul vom Rang n von der Form φ^Λ für ein geeignetes Gitter Λ vom Rang n in C, d.h. die durch $a *_\varphi z := \varphi_a(z)$ definierte A-Modul-Struktur auf C kommt von einem Quotienten C/Λ. Die Definition eines Homomorphismus $u : \varphi \longrightarrow \psi$ von Drinfeld-Moduln ist gerade so gewählt, daß das Einsetzen in das zu u gehörende additive Polynom einen Homomorphismus von C nach C bezüglich den von φ und ψ induzierten A-Modulstrukturen liefert. Definiert man Homomorphismen zwischen zwei A-Gittern Λ_1,Λ_2 durch $\mathrm{Hom}(\Lambda_1, \Lambda_2) = \{c \in C \,\big|\, c\Lambda_1 \subseteq \Lambda_2\}$ und die Verknüpfung solcher Homomorphismen durch Multiplikation in C, so erhält man ebenfalls eine Kategorie, und ein Homomorphismus zwischen Λ_1, Λ_2 induziert einen Homomorphismus zwischen den Quotienten C/Λ_1 und C/Λ_2. Insgesamt ergibt sich, daß die Kategorie der Drinfeld-Moduln über C zur Kategorie der A-Gitter in C äquivalent ist.

Es gibt viele Gründe, weshalb Drinfeld-Moduln, welche wir übrigens nur im technisch einfachsten Fall beschrieben haben, in der Arithmetik von Funktionenkörpern eine wichtige Rolle spielen. Eingeführt wurden sie von V. G. Drinfeld in [**Dr2**] auf dem Weg zu einem Beweis der globalen Langlands-Korrespondenz für GL(2) in positiver Charakteristik. Erste Beispiele von Rang 1-Drinfeld-Moduln traten aber schon lange vorher auf. In Analogie zur Beschreibung von Einheitswurzeln mittels der klassischen Exponentialfunktion lassen sich mit Hilfe von Rang 1-Drinfeld-Moduln Erweiterungen des rationalen Funktionenkörpers K konstruieren, deren zahlentheoretische Eigenschaften denen von klassischen Kreisteilungskörpern entsprechen. Diese Methode läßt sich bis zu einer expliziten Klassenkörpertheorie für globale Funktionenkörper ausbauen [**Ha1**],[**Ha2**]. Für uns spielen diese Körper eine Rolle, da sie im Zusammenhang mit Konstantenkörpern von Drinfeld'schen Modulkurven auftreten, genauso wie der n-te Kreisteilungskörper bei der komplexen Modulkurve $X(n)$. Deshalb gehen wir noch etwas ausführlicher auf den Rang 1-Fall ein

Betrachten wir einen beliebigen Rang 1-Drinfeld-Modul φ, bestimmt durch den Wert $T\tau^0 + \alpha\tau$ mit $\alpha \in C^*$, den er an T annimmt. Da C algebraisch abgeschlossen ist, erhält man unmittelbar, daß φ isomorph ist zu dem sogenannten Carlitz-Modul ρ mit

$$\rho_T = T\tau^0 + \tau\,.$$

Sei nun $\mathfrak{n} = (f)$ ein Ideal in A. Die Nullstellen des additiven Polynoms ρ_f in C bilden gerade die $\mathfrak{n}$-Torsion der auf C durch den Carlitz-Modul vermittelten A-Modulstruktur. Sei $K(\mathfrak{n})$ die Körpererweiterung von K, die durch Adjunktion dieser $\mathfrak{n}$-Torsion entsteht. Die so erhaltenen Körper $K(\mathfrak{n})$ sind die Kreisteilungskörper für den rationalen Funktionenkörper K. Von den vielen Analogien mit klassischen Kreisteilungskörpern, welche diese Bezeichnung rechtfertigen, wie z.B. dem Aussehen des Ganzheitsrings oder dem Verzweigungsverhalten von Primstellen, wollen wir nur eine der einfachsten genauer erwähnen. Die Erweiterung $K(\mathfrak{n})|K$ ist galoissch, ihre Galois-Gruppe ist isomorph zu $(A/\mathfrak{n})^*$, und ein Element $\overline{a} \in (A/\mathfrak{n})^*$ operiert auf einem $\mathfrak{n}$-Torsionspunkt $t \in C$ durch Einsetzen von t in das additive Polynom ρ_a. Ist z.B. $\mathfrak{n}$ teilerfremd zu T, so operiert $\overline{T}$ durch $t \mapsto Tt + t^r$.

Noch genauer werden wir im folgenden den Rang 2-Fall betrachten, der besondere Parallelen zur Theorie elliptischer Kurven aufweist. Insbesondere werden wir im folgenden Drinfeld'sche Modulkurven beschreiben und einige ihrer Anwendungen erwähnen.

In der von uns betrachteten Situation ist ein Drinfeld-Modul φ schon vollständig beschrieben durch seinen Wert an der Unbestimmten T, welcher im Fall von Rang 2 von der Form

$$\varphi_T = T\tau^0 + g\tau^1 + \Delta\tau^2$$

mit $g \in C$ und $\Delta \in C^*$ ist. Bildet man nun

$$j(\varphi) = \frac{g^{r+1}}{\Delta}\,,$$

so erhält man eine Invariante der Isomorphieklasse von φ, welche diese auch eindeutig bestimmt. Da $j(\varphi)$ offensichtlich jeden Wert aus C annehmen kann, erhält man eine Bijektion

$$\{\text{Isomorphieklassen von Rang 2-Drinfeld-Moduln über } C\} \xrightarrow[\cong]{j} C\,.$$

Ähnlich wie bei elliptischen Kurven parametrisieren also die Punkte der Kurve $\mathbb{A}^1(C)$ Isomorphieklassen von Rang 2-Drinfeld-Moduln und die projektive Gerade $\mathbb{P}^1(C)$ ist das erste Beispiel einer Drinfeld'schen Modulkurve. Genau wie die klassischen Modulkurven werden wir im folgenden Drinfeld'sche Modulkurven auf verschiedene Arten beschreiben.

Die Gruppe $\mathrm{GL}(2, A)$ operiert auf $\mathbb{P}^1(C)$ wieder durch

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix} \cdot [z : w] = [az + cw : bz + dw]$$

und die Bahn von ∞ unter dieser Gruppe ist $\mathbb{P}^1(K)$. Da es im Gegensatz zur Situation über den komplexen Zahlen aber keine natürliche Auswahl einer "oberen Halbebene" gibt, findet auch kein Übergang zur speziellen linearen Gruppe statt. Als Ersatz für die komplexe obere Halbebene dient uns die unter der Gruppenoperation stabile Menge $\mathcal{H} = C - K_\infty$. Obwohl sie also eigentlich der Vereinigung der beiden komplexen Halbebenen $\mathbb{H} \cup -\mathbb{H} = \mathbb{C} - \mathbb{R}$ entspricht, trägt $\mathcal{H}$ den Namen Drinfeld'sche obere Halbebene.

Sei nun $\mathfrak{n}$ ein von Null verschiedenes Ideal in A und Γ eine der Gruppen

$$\Gamma(\mathfrak{n}) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, A) \,\middle|\, a \equiv d \equiv 1 \bmod \mathfrak{n},\ b \equiv c \equiv 0 \bmod \mathfrak{n} \right\},$$

$$\Gamma_1(\mathfrak{n}) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, A) \,\middle|\, a \equiv d \equiv 1 \bmod \mathfrak{n},\ b \equiv 0 \bmod \mathfrak{n} \right\},$$

$$\Gamma_0(\mathfrak{n}) = \left\{ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \in \mathrm{GL}(2, A) \,\middle|\, b \equiv 0 \bmod \mathfrak{p} \right\}.$$

Der Quotient $\Gamma \backslash \mathcal{H}$ läßt sich mit einer analytischen Struktur versehen, welche in ihren Eigenschaften einer Riemannschen Fläche ähnlich ist. Die Theorie solcher rigid-analytischer Räume ist z.B. in [**FrPu**] beschrieben. Schon ihre Definition ist komplizierter als im Falle komplexer Analysis. Der von der nichtarchimedischen Bewertung v_∞ induzierte Absolutbetrag $|\ |_\infty$ führen zu einer metrischen Topologie auf C, die im Vergleich zu den komplexen Zahlen einige Besonderheiten aufweist, so sind z.B. Kreisscheiben entweder disjunkt oder ineinander enthalten. Dies zeigt, daß eine Definition von Holomorphie durch lokal in Potenzreihen entwickelbare Funktionen nicht sinnvoll ist, da z.B. keine Identitäts- oder Fortsetzbarkeitssätze gelten würden. In der tatsächlich verwendeten Struktur als rigid-analytischer Raum werden deshalb Mengen mit besseren Überlappungseigenschaften verwendet. Für $n \in \mathbb{N}$ sei

$$D_n = \{z \in C \bigm| |z - x|_\infty \geqslant |1/T^n|_\infty \text{ für alle } x \in K_\infty\}.$$

Dann ist $D_n \subseteq \mathcal{H}$ und $\mathcal{H} = \cup_{n \in \mathbb{N}} D_n$. Eine Funktion von $\mathcal{H}$ nach C heißt holomorph, wenn sie auf jedem D_n gleichmäßiger Grenzwert einer Folge rationaler Funktionen ist, deren Pole außerhalb von D_n liegen. Von diesem Holomorphiebegriff auf $\mathcal{H}$ ausgehend, wird auch der Quotient $\Gamma\backslash\mathcal{H}$ zu einem rigid-analytischen Raum, und durch Hinzunahme von endlich vielen neuen, wieder als Spitzen bezeichneten Punkte erhält man einen kompakten Raum. Die Spitzen stehen in Bijektion zu der Menge $\Gamma\backslash\mathbb{P}^1(K)$. Der durch die Kompaktifizierung erhaltene rigid-analytische Raum wird der Wahl von Γ entsprechend mit $X(\mathfrak{n})$, $X_0(\mathfrak{n})$ oder $X_1(\mathfrak{n})$ bezeichnet und heißt Drinfeld'sche Modulkurve. Ist $\mathfrak{n} = (1)$, so erhält man einen zu $\mathbb{P}^1(C)$ isomorphen Raum.

Wie bei kompakten Riemannschen Flächen entsprechen den Drinfeld'schen Modulkurven auch glatten projektiven algebraischen Kurven über C, welche wir mit demselben Symbol bezeichnen. Darüber hinaus lassen diese Kurven sich sogar über endlichen Erweiterungen von K bzw. über K selbst definieren.

Auch zu den Drinfeld'schen Modulkurven gehören natürlich Funktionenkörper, die zur Untersuchung der Kurven verwendet werden können. Insbesondere werden wir in Kapitel 2 die Tatsache benutzen, daß der Funktionenkörper von $X(\mathfrak{n})$ eine galoissche Erweiterung über dem Funktionenkörper von $X((1))$, d.h. dem rationalen Funktionenkörper ist. Dies liefert eine zusätzliche Struktur als Galois-Modul für eine Reihe von Objekten, die der Modulkurve in natürlicher Weise zugeordnet sind, insbesondere auch der Spitzendivisorklassengruppe, welche im Mittelpunkt der Untersuchungen des folgenden Kapitels steht.

Aus ihrer Konstruktion geht bereits hervor, daß Drinfeld'sche Modulkurven für Rang 2-Drinfeld-Moduln dieselbe Rolle spielen wie klassische Modulkurven für elliptische Kurven. Die Beschreibung der Kurven $X(\mathfrak{n})$, $X_0(\mathfrak{n})$, $X_1(\mathfrak{n})$ als Parameterräume von Isomorphieklassen von Rang 2-Drinfeld-Moduln ist fast wörtlich dieselbe wie die bei klassischen Modulkurven und elliptischen Kurven. Das selbe gilt für den Zusammenhang mit Drinfeld'schen Modulformen. Neben diesen naheliegenden Anwendungen in der Theorie der Drinfeld-Moduln gibt es aber auch Zusammenhänge mit elliptischen Kurven, so ist z.B. jede elliptische Kurve über dem rationalen Funktionenkörper K mit zerfallend multiplikativer Reduktion an ∞ der Quotient einer geeigneten Drinfeld'schen Modulkurve, d.h. es gilt eine der Vermutung von Shimura, Taniyama und Weil entsprechende Aussage [**GeRe**].

Unabhängig von ihrer Bedeutung für andere zahlentheoretisch interessante Objekte haben Drinfeld'sche Modulkurven aber auch für sich betrachtet bemerkenswerte Eigenschaften. Durch Reduktion an geeigneten Stellen des Grundkörpers erhält man aus ihnen Kurven über endlichen Körpern, unter denen sich Serien finden lassen, bei denen das Verhältnis zwischen der Anzahl der rationalen Punkte und dem Geschlecht asymptotisch optimal ist [**Ge10**],[**Ge11**].

1.3. Klassengruppen

Das zentrale Objekt unserer Untersuchungen im folgenden Kapitel wird die Spitzendivisorklassengruppe Drinfeld'scher Modulkurven sein. Eine Möglichkeit, dies zu motivieren, besteht im Vergleich mit Idealklassengruppen algebraischer Zahlkörper.

Eine grundlegende Eigenschaft der Arithmetik ganzer Zahlen besteht in der Existenz der eindeutigen Primfaktorzerlegung. Nun ist es bei der Untersuchung von ganzzahligen Gleichungen oft nützlich, zum Ganzheitsring eines algebraischen Zahlkörpers überzugehen. Bei der Untersuchung der Fermat-Gleichung $x^p + y^p = z^p$ für eine ungerade Primzahl p liegt es beispielsweise nahe, eine primitive p-te Einheitswurzel ξ zu wählen und über dem Ring $\mathbb{Z}[\xi]$ der ganzen Zahlen des p-ten Kreisteilungskörpers die Faktorisierung $\prod_{k=1}^{p}(x + \xi^k y) = z^p$ vorzunehmen.

Allerdings ist der Ganzheitsring O_L eines Zahlkörpers L im allgemeinen nur ein Dedekindring und kein Hauptidealring. Damit hat man auch keine eindeutige Primfaktorzerlegung mehr, sondern nur noch eine eindeutige Zerlegung von Idealen in Primideale. Es stellt sich unmittelbar die Frage, wie sehr die Gruppe der gebrochenen Ideale I_L des Ganzheitsrings von der Untergruppe H_L der Hauptideale abweicht. Dies begründet das Interesse an der Idealklassengruppe $Cl_L = I_L/H_L$ eines Zahlkörpers. Die Idealgruppe beschreibt allerdings nur einen Teil der Arithmetik von L. Zu jedem Primideal von O_L gehört eine diskrete nichtarchimedische Bewertung von L, bzw. die als Stelle bezeichnete Äquivalenzklasse dieser Bewertung. Die Menge $M_{L,\,\text{endl.}}$ dieser endlichen Stellen enthält aber noch nicht alle Stellen von L, sondern nur die nichtarchimedischen. Neben diesen gibt es auch noch archimedische Bewertungen, die zur Menge $M_{L,\infty}$ der sogenannten unendlichen Stellen von L führt. Nur die Betrachtung aller Stellen $M_L = M_{L,\,\text{endl.}} \cup M_{L,\infty}$ führt zu einem vollständigen Bild, wie man z.B. an der Produktformel [**Ne**, S. 195] sehen kann. Die Hinzunahme der unendlichen Stellen und ein gleichzeitiger Übergang von der multiplikativen Schreibweise der Idealgruppe zu einer additiven Schreibweise liefert die Divisorengruppe

$$D_L = \{ \sum_{v \in M_L} a_v \cdot v \,\Big|\, a_v \in \mathbb{R},\ a_v \in \mathbb{Z} \text{ für } v \in M_{L,\,\text{endl.}},\ \text{fast alle } a_v = 0\}\,.$$

Diese Gruppe hat die beiden Untergruppen $D_{L,\,\text{endl.}}$ und $D_{L,\infty}$ derjenigen Divisoren, in denen nur endliche bzw. unendliche Stellen vorkommen. Es ergibt sich auf natürliche Weise eine kurze exakte Folge

$$0 \to D_{L,\infty} \xrightarrow{i} D_L \xrightarrow{\pi} D_{L,\,\text{endl.}} \to 0$$

und $D_{L,\,\text{endl.}}$ ist isomorph zur Idealgruppe von L. Einem Element $x \in L^*$ ordnen wir den Divisor $\operatorname{div}(x)$ zu, dessen v-Koeffizient sich durch Auswertung eines geeignet normierten Vertreters aus der Klasse v an x ergibt. Solche Divisoren $\operatorname{div}(x)$ heißen Hauptdivisoren und bilden eine Untergruppe P_L. Mit ihrer Hilfe erhalten wir wieder eine Klassengruppe. Aufgrund der Produktformel ist es jedoch klar, daß nur ein Teil der Divisoren überhaupt eine Chance hat, ein Hauptdivisor zu sein. Mit Hilfe einer geeignet definierten Gradabbildung $\deg : D_L \to \mathbb{R}$ übersetzt sich die multiplikativ geschriebene Produktformel in $\deg(\operatorname{div}(x)) = 0$. Wir bezeichnen den Kern des Homomorphismus deg mit D_L^0 und definieren die Divisorklassengruppe

$$Pic_L = D_L^0 / P_L \,.$$

Der Zusammenhang der Divisorklassengruppe mit der Idealklassengruppe ergibt sich mittels der Projektion π durch

$$Pic_L = D_L^0/P_L \twoheadrightarrow \pi(D_L^0)/\pi(P_L) = D_{L,\,\text{endl.}}/\pi(P_L) \cong I_L/H_L = Cl_L \,.$$

Dabei mißt der Kern des Homomorphismus $Pic_L \twoheadrightarrow Cl_L$ auf der Ebene der Klassen den unendlichen Anteil, so wie die Gruppe $D_{L,\infty}$ den Unterschied zwischen Divisorgruppe und Idealgruppe vor dem Übergang zu den Klassen gemessen hat. Beschreiben läßt sich der Kern von $Pic_L \twoheadrightarrow Cl_L$ als Quotient der Kerne der Abbildungen $D_L^0 \xrightarrow{\pi} D_{L,\,\text{endl.}}$ und $P_L \xrightarrow{\pi} H_L$. Der Kern der ersten dieser beiden Abbildungen ist die Spur-Null-Hyperebene

$$H = \{ \sum_{v \in M_{L,\infty}} a_v \cdot v \,\big|\, \sum_v a_v = 0 \} = D_{L,\infty} \cap D_L^0 \,,$$

der Kern der zweiten ist das von den Einheiten von O_L darin aufgespannte Gitter $\operatorname{div}(O_L^*)$. Somit ergibt sich die exakte Folge

$$0 \to H/\operatorname{div}(O_L^*) \to Pic_L \to Cl_L \to 0 \,.$$

Wir werden nun den Zahlkörper durch eine algebraische Kurve ersetzen und uns später auf Modulkurven spezialisieren. Dabei werden wir all den oben beschriebenen Objekten wieder begegnen.

Über einem algebraisch abgeschlossenen Körper, z.B. über C, betrachten wir nun also eine glatte projektive algebraische Kurve X. Zu jedem Punkt x von X gehört eine Bewertung v_x des Funktionenkörpers $C(X)$ von X, welche die Null- bzw. Polstellenordnung in diesem Punkt zählt. Die so entstehenden Bewertungen sind nichtarchimedisch und im Gegensatz zum Fall des Zahlkörpers sind dies auch schon alle Bewertungen, die man betrachten muß. So hat beispielsweise eine

Funktion auf X mit Vielfachheiten gezählt genau so viele Nullstellen wie Polstellen, und diese Aussage entspricht gerade der Produktformel von oben. Wir bilden also direkt die Gruppe D_X der Divisoren von X als die freie abelsche Gruppe, die von den Punkten von X erzeugt wird. Für einen Divisor

$$A = \sum_{x \in X} a_x \cdot x$$

definieren wir den Grad

$$\deg A = \sum_{x \in X} a_x$$

und für ein von Null verschiedenes Element f des Funktionenkörpers von X sei

$$\operatorname{div}(f) = \sum_{x \in X} v_x(f) \cdot x\,.$$

Damit kann man nun die Gruppe D_X^0 der Divisoren vom Grad 0 sowie die Gruppe

$$P_X = \operatorname{div}(C(X)^*)$$

der Hauptdivisoren bilden. Schließlich ergibt sich die Divisorklassengruppe

$$Pic_X = D_X^0 / P_X$$

von X. Die beim Ganzheitsring eines Zahlkörpers auftretende Frage, ob ein Ideal ein Hauptideal ist, wird für die Kurve X zu der Frage, ob ein Divisor ein Hauptdivisor ist, d.h. ob es eine Funktion auf X mit gewissen vorgegebenen Null- und Polstellen gibt.

Der offensichtliche Unterschied zum Fall des Zahlkörpers besteht darin, daß sich die Divisoren- bzw. die Divisorklassengruppe nicht in einen Anteil zu endlichen Stellen und einen zu unendlichen Stellen aufteilt. Diese Aufteilung im Zahlkörperfall resultiert aus der ausgezeichneten Rolle des Ganzheitsrings. Um etwas ähnliches im Fall einer Kurve X tun zu können, muß man eine im allgemeinen willkürliche Auswahl vornehmen. Wir beschreiben nun, wie man dann eine zum Fall des Zahlkörpers ganz analoge Situation erhält.

Interpretiert man die Kurve X als eine Überlagerung der projektiven Geraden $\mathbb{P}^1$, so entspricht dies dem Umstand, daß der Funktionenkörper $C(X)$ eine endliche Erweiterung eines rationalen Funktionenkörpers ist. Wählt man einen beliebigen, aber festen und mit ∞ bezeichneten Punkt der projektiven Geraden, so läßt sich der rationale Funktionenkörper der projektiven Geraden darstellen als $C(T)$ mit einer Funktion T, die in ∞ einen einfachen Pol hat. Die Körpererweiterung $C(X)|C(T)$ spielt nun die Rolle von $L|\mathbb{Q}$, und der ausgezeichnete Ring $\mathbb{Z}$ wird ersetzt durch den von der Wahl von ∞ abhängenden Polynomring $C[T]$. Bezeichnet S die Menge der Punkte von X über ∞, so ist der ganze Abschluß von $C[T]$ in $C(X)$ gerade der Ring $O_{X,\infty}$ der außerhalb von S regulären Funktionen auf X. Dieser Ring ist ein Dedekindring und seine Primideale stehen in Bijektion zu der Menge $X-S$. Damit erhält man eine Zerlegung der Divisorengruppe von X in zwei Untergruppen, nämlich die von den Punkten aus S erzeugte Gruppe $D_{X,S}$ sowie die von den Punkten aus $X-S$ erzeugte Gruppe, welche isomorph ist zur Idealgruppe I_∞ von $O_{X,\infty}$. Mittels der Projektion von D_X^0 auf I_∞ erhält man wieder einen surjektiven Homomorphismus

$$Pic_X \twoheadrightarrow Cl_\infty$$

von der Divisorklassengruppe auf die Idealklassengruppe von $O_{X,\infty}$.

Der Kern $\mathcal{C}$ dieser Abbildung läßt sich folgendermaßen beschreiben. Offensichtlich besteht $\mathcal{C}$ genau aus den Divisorklassen in Pic_X, die einen Vertreter aus $D_{X,S}$ haben. Setzen wir

$$D_{X,S}^0 = D_X^0 \cap D_{X,S}\,,$$

so ist $\mathcal{C}$ gleich dem Bild von $D_{X,S}^0$ in Pic_L, d.h.

$$\mathcal{C} = D_{X,S}^0/(D_{X,S}^0 \cap P_X)\,.$$

Nun besteht $P_X \cap D_{X,S}^0$ genau aus den Hauptdivisoren von Funktionen, die außerhalb von S weder Nullstellen noch Pole haben, und das sind genau die Elemente von $O_{X,\infty}^*$. Also ergibt sich

$$\mathcal{C} = D_{X,S}^0/\mathrm{div}\,(O_{X,\infty}^*)\,.$$

Ein Vergleich mit der Zahlkörpersituation zeigt, daß die Gruppe $\mathcal{C}$ als Kern von $Pic_X \twoheadrightarrow Cl_\infty$ das genaue Analogon des Kernes $H/\mathrm{div}\,(O_L^*)$ der Abbildung $Pic_L \twoheadrightarrow Cl_L$ ist.

Wir betrachten nun den Fall, daß die Kurve X eine klassische oder Drinfeld'sche Modulkurve ist. Dann besitzt X eine ausgezeichnete endliche Menge von Punkten, nämlich die Spitzen. Diese sind gerade die Punkte des projektiven Abschlußes der zu X gehörenden affinen Kurve und gleichzeitig genau die über der einzigen Spitze von $X((1)) = \mathbb{P}^1$ liegenden Punkte. Somit ist es naheliegend, als Menge S gerade die Spitzen zu wählen. Dann nennt man die Elemente von $O_{X,\infty}^*$ auch modulare Einheiten, die Divisoren von modularen Einheiten bilden die Gruppe $N = \mathrm{div}\,(O_{X,\infty}^*)$ der Hauptspitzendivisoren und die Gruppe $\mathcal{C} = D_{X,S}^0/\mathrm{div}\,(O_{X,\infty}^*)$ mit ihrer definierenden Folge

$$0 \to N \to D_S^0 \to \mathcal{C} \to 0 \tag{1.3.1}$$

ist die Spitzendivisorklassengruppe von X. Die Spitzendivisorklassengruppe einer Drinfeld'schen Modulkurve $X(\mathfrak{p})$ zu einem Primideal $\mathfrak{p}$ ist genau die Gruppe, die wir in den folgenden Kapiteln untersuchen wollen.

Vergleicht man die Zerlegung

$$0 \to \mathcal{C} \to Pic_X \to Cl_\infty \to 0$$

von Pic_X in die beiden Teile $\mathcal{C}$ und Cl_∞ mit der Situation des Zahlkörpers, so könnte man annehmen, daß die Gruppe Cl_∞ das interessantere Objekt ist, da es der Idealklassengruppe des Zahlkörpers entspricht. Trotzdem weist auch $\mathcal{C}$ Analogien zu Idealklassengruppen auf, wie etwa die folgende.

Ist p eine Primzahl und L der p-te Kreisteilungskörper über $\mathbb{Q}$ mit Galois-Gruppe G_L, so ist die Idealklassengruppe Cl_L ein Modul über dem Gruppenring $R = \mathbb{Z}[G_L]$. Mit Hilfe des ersten Bernoulli-Polynoms

$$B_1(X) = X - \frac{1}{2}$$

sowie des üblichen, hier mit σ bezeichneten Isomorphismus zwischen $(\mathbb{Z}/p\mathbb{Z})^*$ und G_L definiert man das Stickelbergerelement

$$\theta = \sum_{a=1}^{p-1} B_1\left(\frac{a}{p}\right)\sigma_a^{-1} \in \mathbb{Q}[G_L]$$

sowie das Stickelbergerideal

$$St = R\theta \cap R\,.$$

Es besteht nun ein enger Zusammenhang zwischen R/St und der Klassengruppe Cl_L, z.B. hat das Stickelbergerideal die besondere Eigenschaft, die Gruppe Cl_L zu annullieren. Eine Folgerung dieser Aussage ist das Herbrandt-Kriterium, welches besagt, daß man aus dem Nichtverschwinden von isotypischen Komponenten des p-Anteils von Cl_L auf die p-Teilbarkeit von bestimmten Bernoulli-Zahlen schließen kann.

Vergleichen wir dies nun mit der Spitzendivisorklassengruppe der klassischen Modulkurve $X(p)$. Es gibt eine Cartan-Untergruppe $Ca \subseteq \mathrm{GL}(2, \mathbb{F}_p)$, so daß die Menge der Spitzen in Bijektion steht zu $G = Ca/\{\pm 1\}$. Deshalb kann der Gruppenring $R = \mathbb{Z}[G]$ mit der Gruppe $D_{X,S}$ der Spitzendivisoren identifiziert werden. Mit Hilfe des zweiten Bernoulli-Polynoms

$$B_2(X) = X^2 - X + \frac{1}{6}$$

definiert man das Stickelbergerelement

$$\theta = p \cdot \sum_{\beta \in G} \frac{1}{2} B_2\left(\frac{T\beta}{p}\right)\beta^{-1}\,.$$

Dabei ordnet T einer Matrix aus G den kleinsten nichtnegativen Vertreter des Koeffizienten oben links zu. Das Stickelbergerideal in dieser Situation ist wieder $St = R\theta \cap \theta$ und es gilt nun sogar

$$R/St \cong \mathcal{S}\,.$$

Aufgrund dieser Analogien ist es nicht überraschend, daß Modulkurven und insbesondere deren Spitzendivisorklassengruppe Anwendungen in der Theorie der Kreisteilungserweiterungen besitzen. Ein

Beispiel dafür ist die von Ribet in [**Ri**] bewiesene Umkehrung des Herbrandt-Kriteriums, welche besagt, daß man aus der p-Teilbarkeit von Bernoulli-Zahlen auf das Nichtverschwinden von isotypischen Komponenten des p-Anteils der Idealklassengruppe p-ter Kreisteilungskörper schließen kann. Der Beweis von Ribet beruht auf der Konstruktion von unverzweigten zyklischen Erweiterungen vom Grad p des p-ten Kreisteilungskörpers, die aufgrund der Klassenkörpertheorie Aussagen über die Idealklassengruppe implizieren. Dazu wird eine geeignete Untergruppe g eines Quotienten der Jacobischen einer Modulkurve konstruiert. Die besagten Körpererweiterungen gewinnt man dann durch Adjunktion der Koordinaten von g an den Kreisteilungskörper.

Eine noch wesentlich detailliertere Aussage über die Struktur des p-Anteils von Idealklassengruppen sogar in dem Turm der p^n-ten Kreisteilungskörper stellt die in [**MazWi**] bewiesene Hauptvermutung der Iwasawa-Theorie dar. Insbesondere gelang Mazur und Wiles dabei die genaue Bestimmung der Ordnung der isotypischen Komponenten des p-Anteils der Idealklassengruppe des p-ten Kreisteilungskörpers durch eine Weiterentwicklung der Ideen Ribets. Auch hier wurden wieder Körpererweiterungen gewonnen durch die Adjunktion von Koordinaten einer Untergruppe der Jacobischen einer Modulkurve. Diese Untergruppe ist die Torsion eines sogenannten Eisensteinideals in der Heckealgebra der Modulkurve, welche auch auf der Jacobischen operiert. Der Zusammenhang mit der Spitzendivisorklassengruppe besteht darin, daß das Eisensteinideal gerade der Annullator einer Untergruppe der Spitzendivisorklassengruppe ist.

Damit wollen wir nun unsere Anmerkungen zur Bedeutung von Spitzendivisorklassen abschließen.

1.4. Klassische Spitzendivisorklassengruppen

Wie wir im letzten Abschnitt gesehen haben, ist die Spitzendivisorklassengruppe $\mathcal{C}$ einer Modulkurve X durch die exakte Folge

$$0 \to N \to D_S^0 \to \mathcal{C} \to 0$$

definiert als Quotient der Gruppe D_S^0 der Spitzendivisoren vom Grad 0 nach der Untergruppe $N = D_S^0 \cap P_X$ der darin enthaltenen Hauptdivisoren.

Im Falle klassischer Modulkurven besteht die erste wesentliche strukturelle Aussage bei den von uns beschriebenen Modulkurven $X(n)$, $X_0(n)$, $X_1(n)$ in der Endlichkeit der Spitzendivisorklassengruppe [**Man**], [**Dr1**]. Daraus folgt, daß N und D_S^0 denselben $\mathbb{Z}$-Rang haben. Für eine

Primzahl p betrachten wir das aus der Multiplikation mit p resultierende kommutative Diagramm

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & 0 & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N[p] & & D_S^0[p] & & \mathcal{C}[p] & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
0 \to & & N & \to & D_S^0 & \to & \mathcal{C} & \to 0 & \\
 & & \downarrow \cdot p & & \downarrow \cdot p & & \downarrow \cdot p & & \\
0 \to & & N & \to & D_S^0 & \to & \mathcal{C} & \to 0 & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & N/pN & & D_S^0/pD_S^0 & & \mathcal{C}/p\mathcal{C} & & \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

mit exakten Zeilen und Spalten, wobei die p-Torsion einer Gruppe durch Anhängen von $[p]$ bezeichnet wird. Da D_S^0 eine Untergruppe der freien abelschen Gruppe D_S ist, gilt $D_S^0[p] = 0$, und das Schlangenlemma liefert die exakte Folge

$$0 \to \mathcal{C}[p] \to N/pN \to D_S^0/pD_S^0 \to \mathcal{C}/p\mathcal{C} \to 0 \tag{1.4.1}$$

von $\mathbb{F}_p$-Vektorräumen. So wie beim p-ten Kreisteilungskörper der p-Anteil der Idealklassengruppe von besonderem Interesse ist, spielt bei klassischen Modulkurven der p-Anteil der Spitzendivisorklassengruppe von $X(p)$ eine besondere Rolle. In diesem Fall sind daher in der exakten Folge oben die Randterme von spezieller Bedeutung. Die Gruppe links enthält ja gerade die Elemente von $\mathcal{C}$ der Ordnung p, während die $\mathbb{F}_p$-Dimension von $\mathcal{C}/p\mathcal{C}$ die Anzahl der zyklischen Komponenten des p-Anteils von $\mathcal{C}$ ist. Da D_S^0 und N freie $\mathbb{Z}$-Moduln vom gleichen Rang sind, haben die beiden mittleren Terme N/pN und D_S^0/pD_S^0 dieselbe Dimension als $\mathbb{F}_p$-Vektorräume. Betrachtet man die Folge oben also nur als exakte Folge von $\mathbb{F}_p$-Vektorräumen, so kann man an ihr lediglich die triviale Aussage ablesen, daß die beiden Gruppen $\mathcal{C}[p]$ und $\mathcal{C}/p\mathcal{C}$ dieselbe Ordnung haben. Zusätzlich zur $\mathbb{Z}$-Modulstruktur operiert aber auf allen vorkommenden Gruppen noch die Galois-Gruppe des Funktionenkörpers von $X(p)$. Durch Ausnutzen der wesentlich reicheren Struktur solcher Galois-Moduln kann man weitere Informationen über die Gruppen $\mathcal{C}[p]$ und $\mathcal{C}/p\mathcal{C}$ gewinnen. Wir skizzieren im folgenden die Vorgehensweise in [**Gr**], welche die Grundidee für die spätere Untersuchung bei Drinfeld'schen Modulkurven beinhaltet.

Sei also p eine Primzahl, von der wir zudem $p \geqslant 5$ fordern. Wir wählen eine elliptische Kurve E über einem rationalen Funktionenkörper $k = \mathbb{Q}(j)$ mit der Invarianten $j(E) = j$. Ist $\overline{k}$ ein algebraischer Abschluß von k, so betrachten wir in der Menge der $\overline{k}$-rationalen Punkte $E(\overline{k})$ die Untergruppe $E[p]$ der p-Teilungspunkte. Durch Adjunktion der Koordinaten der Punkte der Ordnung p gewinnen wir eine normale Erweiterung $\mathcal{L}$. Die Galois-Gruppe von $\mathcal{L}|k$ operiert $\mathbb{Z}/p\mathbb{Z}$-linear auf

$E[p]$ und es ergibt sich sogar ein Isomorphismus

$$\mathrm{Gal}(\mathcal{L}|k) \cong \mathrm{Aut}(E[p])$$

sowie nach Wahl einer $\mathbb{F}_p$-Basis von $E[p]$ auch

$$\mathrm{Gal}(\mathcal{L}|k) \cong \mathrm{GL}(2, \mathbb{F}_p)\,.$$

Der Fixkörper $\mathcal{K}$ der Untergruppe $\{\pm 1\} \subseteq \mathrm{GL}(2, \mathbb{F}_p)$ wird über k erzeugt von den x-Koordinaten der Punkte der Ordnung p. Dieser Körper ist auch normal über k und hat die besondere Eigenschaft, unabhängig davon zu sein, welche elliptische Kurve mit Invariante j man wählt. Bezeichnet μ_p die Menge der p-ten Einheitswurzeln in $\overline{k}$, so ergibt sich folgender Körperturm mit den angegebenen Galois-Gruppen:

$$\left.\begin{array}{rc} & \mathcal{L}\\ \langle\pm1\rangle & |\\ \mathrm{GL}(2,\mathbb{F}_p)/\langle\pm1\rangle & \left\{\begin{array}{c}\mathcal{K}\\ | \\ k(\mu_p)\\ |\\ k\end{array}\right. \end{array}\right\}\mathrm{GL}(2,\mathbb{F}_p)$$

Der Körper $\mathcal{K}$ ist dann gerade der Funktionenkörper der Modulkurve $X(p)$ über dem Körper der Konstanten $\mathbb{Q}(\mu_p)$. Die Kurve $X(p)$ hat $(p^2 - 1)/2$ Spitzen, welche den Stellen von $\mathcal{K}$ entsprechen, die über $j = \infty$ liegen. Die Galois-Gruppe $G = \mathrm{GL}(2, \mathbb{F}_p)/\{\pm 1\}$ operiert also auf der Menge S der Spitzen und somit auch auf der Gruppe D_S der Spitzendivisoren sowie den beiden Untergruppen der Grad 0-Spitzendivisoren D_S^0 und der Hauptspitzendivisoren N. Die oben schon betrachtete Folge

$$0 \to N \to D_S^0 \to \mathcal{C} \to 0$$

ist also eine exakte Folge von Moduln über dem Gruppenring $\mathbb{Z}[G]$. Damit ist die Folge

$$0 \to \mathcal{C}[p] \to N/pN \to D_S^0/pD_S^0 \to \mathcal{C}/p\mathcal{C} \to 0$$

eine exakte Folge von $\mathbb{F}_p[G]$-Moduln, und als solche wird sie im folgenden auch untersucht. Dabei treten schon einige darstellungstheoretische Begriffe und Aussagen auf, welche im dritten Kapitel ausführlicher behandelt werden.

Zuerst nehmen wir eine Zerlegung in die isotypischen Komponenten des Zentrums $Z \cong {\mathbb{F}_p}^*/\{\pm 1\}$ von G vor. Ist W ein beliebiger $\mathbb{F}_p[G]$-Modul und ψ ein $\mathbb{F}_p$-wertiger Charakter des Zentrums, so sei

$$W(\psi) := \{w \in W \,\big|\, z \cdot w = \psi(z) \cdot w \text{ für alle } z \in Z\}\,.$$

Da die Charakteristik p die Ordnung des Zentrums von G nicht teilt, ergibt sich, wie z.B. in der komplexen Darstellungstheorie, eine Zerlegung von W in eine direkte Summe von isotypischen Komponenten

$W(\psi)$, wobei ψ die Charaktere von Z durchläuft. Das Bilden von zentralen isotypischen Komponenten wird somit zu einem exakten Funktor innerhalb der Kategorie der $\mathbb{F}_p[G]$-Moduln endlicher $\mathbb{F}_p$-Dimension.

Sei $\chi : {\mathbb{F}_p}^* \hookrightarrow \mathbb{F}_p$ die natürliche Einbettung. Dann sind die Charaktere von Z gegeben durch die Abbildungen χ^{2n} mit $0 \leqslant 2n < p-1$. Anstelle der obigen Folge betrachten wir also die χ^{2n}-Anteile

$$0 \to \mathcal{C}[p](\chi^{2n}) \to N/pN(\chi^{2n}) \to D_S^0/pD_S^0(\chi^{2n}) \to \mathcal{C}/p\mathcal{C}(\chi^{2n}) \to 0$$

getrennt. Um nun Informationen über die beiden äußeren Moduln zu erhalten, muß man die $\mathbb{F}_p[G]$-Modulstruktur der beiden mittleren Moduln untersuchen, wozu natürlich genauere Informationen über die Operation der Galois-Gruppe G auf Spitzen und modularen Einheiten notwendig sind. Es stellt sich schließlich heraus, daß die auftretenden Darstellungen von einem ganz bestimmten Typ sind.

Sei B das Bild der Standard-Borelgruppe $\{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}(2, \mathbb{F}_p)\}$ in G. Für zwei Charaktere φ, ψ von ${\mathbb{F}_p}^*/\{\pm 1\}$ sei (φ, ψ) der durch

$$\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \mapsto \varphi(a) \cdot \psi(d)$$

definierte Charakter von B. Dann gelten folgende Aussagen.

Satz 1.4.2. **[Gr]** Für $2 < 2n < p-1$ *gibt es folgende Isomorphismen von $\mathbb{F}_p[G]$-Moduln:*

1. $N/pN(\chi^{2n}) \cong \mathrm{ind}_B^G(\chi^{2n}, 1)$,
2. $D_S^0/pD_S^0(\chi^{2n}) \cong \mathrm{ind}_B^G(1, \chi^{2n})$.

Es stellt sich nun die Frage, welche Homomorphismen es zwischen den beiden induzierten Darstellungen geben kann. Würden wir Darstellungen in Charakteristik 0 betrachten, so wären die Moduln isomorph zur direkten Summe ihrer mit Vielfachheiten gezählten einfachen Faktoren. Der Vektorraum der Homomorphismen zwischen den beiden Moduln würde dann nur von den vorkommenden einfachen Faktoren und deren Vielfachheiten abhängen. Da Darstellungen in positiver Charakteristik aber im allgemeinen nicht halbeinfach sind, gilt eine entsprechende Aussage hier nicht. Die induzierten Darstellungen aus dem vorigen Satz sind gewissermaßen einfachstmögliche Beispiele für dieses Phänomen.

Satz 1.4.3. **[Gr]** *Sei $2 < 2k < p-1$ und $2j = p-1-2k$. Es gibt zwei nichtisomorphe einfache $\mathbb{F}_p[G]$-Moduln S_1 und S_2 der Dimensionen $2k+1$ und $2j+1$, so daß*

$$0 \to S_1 \to \mathrm{ind}_B^G(\chi^{2k}, 1) \to S_2 \to 0$$

und

$$0 \to S_2 \to \mathrm{ind}_B^G(1, \chi^{2k}) \to S_1 \to 0$$

nichtzerfallende exakte Folgen von $\mathbb{F}_p[G]$-Moduln sind.

Die beiden letzten Sätze zusammen implizieren, daß die zwei Galoismoduln $N/pN(\chi^{2n})$ und $D_S^0/pD_S^0(\chi^{2n})$ nicht isomorph sein können und daß außerdem jeder Homomorphismus von $N/pN(\chi^{2n})$ nach $D_S^0/pD_S^0(\chi^{2n})$ mindestens einen Faktor S_1 im Kern und einen Faktor S_2 im Kokern haben muß. Addiert man diese Ergebnisse über die zentralen isotypischen Komponenten auf, erhält man eine Größenabschätzung für die Randterme der Folge (1.4.1).

SATZ 1.4.4. **[Gr]** *Sei $p \geqslant 5$ eine Primzahl und $\mathcal{C}$ die Spitzendivisorklassengruppe der klassischen Modulkurve $X(p)$. Dann gilt*

$$\dim_{\mathbb{F}_p} \mathcal{C}/p\mathcal{C} \geqslant \frac{(p-5)(p-1)}{4}.$$

Natürlich stellt der Satz eine wesentliche Abschwächung der Information über die Galois-Modulstruktur von $\mathcal{C}$ dar, indem er nur eine Aussage über die Gruppenstruktur von $\mathcal{C}$ macht. Es bleibt zum Beispiel unberücksichtigt, daß $\mathcal{C}/p\mathcal{C}$ und $\mathcal{C}[p]$ als Galois-Moduln nicht isomorph sein müssen, obwohl sie es als elementarabelsche p-Gruppen derselben Ordnung natürlich sind. Aber selbst diese Abschwächung stellt ein nichttriviales Resultat über $\mathcal{C}$ dar, welches man bei alleiniger Betrachtung der Gruppenstruktur von $\mathcal{C}$ wohl nicht erzielen kann.

KAPITEL 2

Galois-Moduln von Drinfeld'schen Modulkurven

Von nun an werden wir uns nur noch mit einer bestimmten Modulkurve beschäftigen, nämlich mit der Drinfeld'schen Modulkurve $X(\mathfrak{p})$, die zum Kern $\Gamma(\mathfrak{p})$ der Reduktion $\mathrm{GL}(2, \mathbb{F}_r[T]) \to \mathrm{GL}(2, \mathbb{F}_r[T]/\mathfrak{p})$ an einem Primideal $\mathfrak{p} \subseteq \mathbb{F}_r[T]$ gehört. Da wir ja beabsichtigen, Informationen über die Spitzendivisorklassengruppe von $X(\mathfrak{p})$ mit Hilfe ihrer Struktur als Galois-Modul zu gewinnen, werden wir zuerst den Funktionenkörper der Modulkurve beschreiben und die zugehörige Galois-Gruppe angeben. Dann können wir die exakte Folge (1.3.1) als Folge von Galois-Moduln auffassen.

Der zu den Spitzendivisoren gehörende Modul läßt sich bestimmen, da eine genaue Beschreibung der Spitzen sowie der Operation der Galois-Gruppe auf ihnen möglich ist. Dies ist bei den modularen Einheiten nicht der Fall. Hier werden wir eine Approximation mittels einer bestimmten Klasse von modularen Einheiten, den Siegelfunktionen, vornehmen. Dies führt zu einer neuen, gegenüber (1.4.1) leicht modifizierten Folge von Galois-Moduln, deren mittlere Terme sich dann genau beschreiben lassen.

Da wir von nun an keine Zahlkörper mehr betrachten, sondern nur noch Funktionenkörper, werden wir die schon im letzten Kapitel eingeführten Bezeichnungen $A = \mathbb{F}_r[T]$, $K = \mathbb{F}_r(T)$, $K_\infty = \mathbb{F}_r((1/T))$, $C = \widehat{\overline{K}}_\infty$ und $\mathcal{H} = C - K_\infty$ weiter verwenden.

2.1. Der Funktionenkörper von $X(\mathfrak{p})$

Betrachtet man die Modulkurve $X(\mathfrak{p})$ als rigid-analytischen Raum, so besteht ihr Funktionenkörper gerade aus den rigid-analytisch meromorphen C-wertigen Funktionen auf $X(\mathfrak{p})$. Da die analytische Struktur von $X(\mathfrak{p})$ sich aus der von $\mathcal{H}$ durch Übergang zu dem Quotienten $\Gamma(\mathfrak{p})\backslash\mathcal{H}$ und Hinzufügen der Spitzen ergibt, kann man die meromorphen Funktionen auf $X(\mathfrak{p})$ als Modulformen vom Gewicht 0 auf $\mathcal{H}$ beschreiben, genauso wie im Fall komplexer Modulkurven.

Definition 2.1.1. Eine Modulform vom Gewicht $k \in \mathbb{Z}$ für $\Gamma(\mathfrak{p})$ ist eine Funktion $f : \mathcal{H} \to C$ mit den folgenden Eigenschaften:

1. $f(\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \cdot z) = (bz+d)^k f(z)$ für alle $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \Gamma(\mathfrak{p})$, $z \in \mathcal{H}$,
2. f ist rigid-analytisch meromorph auf $\mathcal{H}$,
3. f ist meromorph in den Spitzen von $X(\mathfrak{p})$.

Eine Modulform vom Gewicht 0 heißt Modulfunktion.

Dabei bedeutet Meromorphie von f in einer Spitze, daß sich f bezüglich eines geeignet lokalen Parameters in eine Laurentreihe mit nur endlich vielen negativen Exponenten entwickeln läßt (vgl. [**Ge4**], [**GeRe**]).

Mit dieser Definition sind Modulfunktionen für $\Gamma(\mathfrak{p})$ nichts anderes als meromorphe Funktionen auf $X(\mathfrak{p})$. Eine Möglichkeit zur Konstruktion von Modulfunktionen besteht darin, Quotienten von Modulformen gleichen Gewichts zu bilden.

Das erste Beispiel für Modulformen erhalten wir durch die Koeffizienten von Rang 2-Drinfeldmoduln. Für $z \in \mathcal{H}$ ist der von 1 und z in C erzeugte A-Modul $\Lambda_z = \langle 1, z\rangle_A$ ein Rang 2-Gitter. Ist ϕ^{Λ_z} der zu Λ_z gehörende Rang 2-Drinfeldmodul, so liefert die Auswertung

$$\phi_T^{\Lambda_z} = T\tau^0 + g(z)\tau^1 + \Delta(z)\tau^2$$

an T zwei von z abhängende Koeffizienten $g(z)$ und $\Delta(z)$. Ähnlich wie bei der Weierstraß-Parametrisierung von elliptischen Kurven mit Gittern in $\mathbb{C}$ stellt sich heraus, daß die Koeffizienten g und Δ Modulformen für $\Gamma(1)$ sind, und zwar vom Gewicht $r-1$ bzw. r^2-1. Somit wird die schon in Kapitel 1 definierte j-Invariante

$$j(z) = \frac{g(z)^{r+1}}{\Delta(z)}$$

zu einer Modulfunktion für $\Gamma(1)$ und natürlich auch für die Untergruppe $\Gamma(\mathfrak{p})$.

Das nächste Beispiel benutzt die bei der analytischen Beschreibung von Drinfeld-Moduln schon verwendete Funktion

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

Wir wählen wieder das Gitter Λ_z sowie ein von Null verschiedenes Element $u = (u_1, u_2) \in (K/A)^2$ mit $\mathfrak{p}\cdot u = 0$. Die Funktion

$$e_u(z) := e_{\Lambda_z}(u_1 z + u_2)$$

ist holomorph auf $\mathcal{H}$ und besitzt dort keine Nullstellen. Sie transformiert sich unter $\gamma = \binom{a\,c}{b\,d} \in \Gamma(1)$ mittels

$$e_u(\gamma\cdot z) = (bz+d)^{-1} e_{u\gamma}(z)\,.$$

Da die betrachteten Vektoren u invariant sind unter Multiplikation mit Matrizen aus $\Gamma(\mathfrak{p})$, liefert das Inverse e_u^{-1} eine Modulform vom Gewicht 1 für $\Gamma(\mathfrak{p})$. Damit ist die Funktion

$$h_u = g\cdot e_u^{r-1}$$

eine Modulfunktion für $\Gamma(\mathfrak{p})$. Aus dem Transformationsverhalten von e_u ergibt sich außerdem, daß für ein $\alpha \in \mathbb{F}_r^*$ die beiden Funktionen e_u und $e_{\alpha u}$ sich nur um einen Faktor α unterscheiden. Somit hängen e_u^{r-1} und h_u nur von der Klasse von u modulo $\mathbb{F}_r^*$ ab.

Wir setzen $U := ((\frac{1}{\mathfrak{p}}A/A)^2 - 0)/\mathbb{F}_r^*$. Die oben beschriebenen Modulfunktionen reichen aus, um den Funktionenkörper von $X(\mathfrak{p})$ zu erzeugen.

SATZ 2.1.2. **[Ge1]** *Der Körper der meromorphen Funktionen von $X(\mathfrak{p})$ wird über C erzeugt von j und den Funktionen h_u mit $u \in U$.*

Da $\Gamma(\mathfrak{p})$ normal ist in $\Gamma(1)$, operiert die Gruppe $\Gamma(1)$ von links auf den beiden Quotienten $\Gamma(\mathfrak{p})\backslash\mathcal{H}$ und $\Gamma(\mathfrak{p})\backslash\mathbb{P}^1(K)$ durch Operation auf den Vertretern der $\Gamma(\mathfrak{p})$-Klasse. Damit erhält man auch eine Operation auf dem rigid-analytischen Raum $X(\mathfrak{p})$. Folglich ergibt sich auf den Funktionen $f : X(\mathfrak{p}) \to C$ eine rechte Operation von $\Gamma(1)$ durch $f^\gamma(z) = f(\gamma z)$. Da die Funktionen aus $C(j, h_u \mid u \in U)$ als Modulfunktionen für $\Gamma(\mathfrak{p})$ invariant sind unter der Operation von $\Gamma(\mathfrak{p})$, erhält man eine Operation der Quotientengruppe $\Gamma(1)/\Gamma(\mathfrak{p})$. Darüber hinaus liest man an der Definition der Operation von $\Gamma(1)$ auf $\mathbb{P}^1(C)$ direkt ab, daß Skalarmatrizen trivial operieren. Betten wir $\mathbb{F}_r^*$ diagonal in $\Gamma(1)$ ein, so ergibt sich eine Operation von $\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^*$ auf dem Funktionenkörper von $X(\mathfrak{p})$. Da die Funktion j sogar eine Modulfunktion für die ganze Gruppe $\Gamma(1)$ ist, läßt die Operation von $\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^*$ auf $C(j, h_u \mid u \in U)$ den Unterkörper $C(j)$ elementweise fest. Es gilt sogar folgende Aussage.

SATZ 2.1.3. **[Ge1]** *Die Körpererweiterung $C(j, h_u \mid u \in U)|C(j)$ ist galoissch mit Galois-Gruppe*

$$\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^* \cong \{\gamma \in \mathrm{GL}(2, A/\mathfrak{p}) \mid \det\gamma \in \mathbb{F}_r^*\}/\mathbb{F}_r^* .$$

Die Gruppe $\{\gamma \in \mathrm{GL}(2, A/\mathfrak{p}) \mid \det\gamma \in \mathbb{F}_r^*\}/\mathbb{F}_r^*$, in die wir $\mathbb{F}_r^*$ wieder diagonal eingebettet haben, ist aber noch nicht die Galois-Gruppe, die wir verwenden wollen. Die folgenden Rationalitätsbetrachtungen liefern uns eine etwas größere und besser handhabbare Gruppe. Sei dazu $K(\mathfrak{p})$ der Körper, der durch Adjunktion der $\mathfrak{p}$-Torsion des Carlitz-Moduls an K entsteht. Wie im ersten Kapitel erwähnt, haben solche Körper viele Eigenschaften, die denen von Kreisteilungskörpern über den rationalen Zahlen ähnlich sind. Insbesondere ist die Erweiterung $K(\mathfrak{p})|K$ galoissch mit Galois-Gruppe $(A/\mathfrak{p})^*$. Wir bezeichnen den Fixkörper der Untergruppe $\mathbb{F}_r^* \hookrightarrow (A/\mathfrak{p})^*$ mit $K_+(\mathfrak{p})$. Er spielt im Funktionenkörperfall dieselbe Rolle wie die maximale reelle Teilerweiterung eines Kreisteilungskörpers über $\mathbb{Q}$. Bezüglich der Rationalität von $X(\mathfrak{p})$ erhalten wir eine ähnliche Aussage wie bei der klassischen Modulkurve $X(p)$.

SATZ 2.1.4. **[Ge2]** *Die Modulkurve $X(\mathfrak{p})$ ist als algebraische Kurve schon über dem Körper $K_+(\mathfrak{p})$ definiert und besitzt den Funktionenkörper $K(j, h_u \mid u \in U)$. Die Erweiterung $K(j, h_u \mid u \in U)|K(j)$ ist galoissch mit Galois-Gruppe $\mathrm{GL}(2, A/\mathfrak{p})/\mathbb{F}_r^*$. Für ein γ aus der Galois-Gruppe ist $h_u^\gamma = h_{u\gamma}$.*

Dabei verwenden wir die natürliche rechte Operation der Gruppe $\mathrm{GL}(2, A/\mathfrak{p})/\mathbb{F}_r^*$ auf U, d.h. wir wählen einen Vertreter $v \in K^2$ für u mit $\mathfrak{p}v \in A^2$ und multiplizieren diesen von rechts mittels üblicher Matrixmultiplikation mit einen Vertreter für γ mit Koeffizienten aus A und erhalten so einen Vertreter für $u\gamma$. Die durch $h_u^\gamma = h_{u\gamma}$ gegebene Operation von $\mathrm{GL}(2, A/\mathfrak{p})/\mathbb{F}_r^*$ ist mit der Operation der Untergruppe $\Gamma(1)/\Gamma(\mathfrak{p})$ verträglich, die wir bei der Erweiterung $C(j, h_u \bigm| u \in U)|C(j)$ verwendet haben. Die Funktion e_u transformiert sich unter $\gamma = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \Gamma(1)$ ja durch

$$e_u(\gamma z) = (bz + d)^{-1} e_{u\gamma}(z)$$

und die Modulform g durch

$$g(\gamma z) = (bz + d)^{r-1} g(z)\,,$$

woraus sich

$$\begin{aligned} h_{u\gamma}(z) &= g(z) e_{u\gamma}(z)^{r-1} = g(z)(bz + d)^{r-1} e_u(\gamma z) = g(\gamma z) e_u(\gamma z) \\ &= h_u(\gamma z) \end{aligned}$$

ergibt. Außerdem betrachten wir im folgenden immer die durch $\gamma \cdot h_u = h_u^{\gamma^{-1}}$ gegebene Linksoperation der Galois-Gruppe.

Damit haben wir alle grundlegenden Informationen gesammelt, die wir im folgenden benötigen. Wir werden deshalb jetzt in einer Definition all die Objekte zusammenfassen, die auch schon in den Erläuterungen im ersten Kapitel vorgekommen sind, allerdings nun in der Formulierung mittels Funktionenkörpern anstatt Kurven.

Definition 2.1.5. Sei $\mathfrak{p}$ ein Primideal von A und $q = \#A/\mathfrak{p}$. Manchmal schreiben wir auch $\mathfrak{p}$ für das normierte irreduzible Polynom, welches das Primideal erzeugt. Weiter sei $\Gamma(\mathfrak{p})$ der Kern der Reduktionsabbildung $\mathrm{GL}(2, A) \to \mathrm{GL}(2, A/\mathfrak{p})$ sowie $X(\mathfrak{p})$ die Drinfeld'sche Modulkurve zu $\Gamma(\mathfrak{p})$.

1. Es sei $\mathcal{K}(\mathfrak{p}) = K(j, h_u \bigm| u \in U)$ der Funktionenkörper von $X(\mathfrak{p})$ und $G(\mathfrak{p}) = \mathrm{GL}(2, A/\mathfrak{p})/\mathbb{F}_r^*$ die Galois-Gruppe von $\mathcal{K}(\mathfrak{p})|K(j)$.
2. Es sei ∞ die Stelle des rationalen Funktionenkörpers $K(j)$ zum Parameter $1/j$.
3. Die Menge S der Spitzen sei die Menge der Stellen von $\mathcal{K}(\mathfrak{p})$, die über ∞ liegen.
4. Es sei D die Divisorengruppe des Funktionenkörpers $\mathcal{K}(\mathfrak{p})|K(j)$, d.h. die von den Stellen von $\mathcal{K}(\mathfrak{p})|K(j)$ erzeugte freie abelsche Gruppe. Darin sei D^0 die Untergruppe der Divisoren vom Grad 0. Die Menge D_S sei die von S in D erzeugte Untergruppe und weiter sei $D_S^0 = D_S \cap D^0$.
5. Die Menge M der modulare Einheiten besteht aus den Elementen von $\mathcal{K}(\mathfrak{p})^*$, bei denen der Träger des Divisors in den Spitzen liegt.
6. Es sei N die Untergruppe der Divisorgruppe, welche von Hauptdivisoren mit Träger in S erzeugt wird.

7. Es sei $\mathcal{C}$ die Spitzendivisorklassengruppe D_S^0/N.

Die Endlichkeit der Spitzendivisorklassengruppe $\mathcal{C}$ für Drinfeld'sche Modulkurven vom Typ $X(\mathfrak{n})$ wurde zuerst in **[Ge2]** bewiesen. Weiterführende Ergebnisse finden sich in **[Ge9]**,**[Ge5]**,**[Ge6]**.

Aufgrund der Definition haben wir eine exakte Folge

$$0 \to N \to D_S^0 \to \mathcal{C} \to 0$$

von abelschen Gruppen. Da die Menge S der Spitzen gerade aus den Stellen von $\mathcal{K}(\mathfrak{p})$ besteht, die über der Stelle ∞ von $K(j)$ liegen, operiert die Galois-Gruppe von $\mathcal{K}(\mathfrak{p})|K(j)$ auf S und somit auch auf D_S und D_S^0. Die obige Folge wird somit zu einer Folge von $\mathbb{Z}[G(\mathfrak{p})]$-Moduln. Auch M ist ein $\mathbb{Z}[G(\mathfrak{p})]$-Modul und die Abbildung $M \xrightarrow{\text{div}} N \subseteq D_S^0$ ist natürlich ein $\mathbb{Z}[G(\mathfrak{p})]$-Homomorphismus. Da $K_+(\mathfrak{p})$ der algebraische Abschluß von K in $\mathcal{K}(\mathfrak{p})$ ist, erhält man als Kern gerade den Untermodul $K_+(\mathfrak{p})^*$. Weil wir mit der etwas größeren Galois-Gruppe von $\mathcal{K}(\mathfrak{p})|K(j)$ an Stelle der von $\mathcal{K}(\mathfrak{p})|K_+(\mathfrak{p})(j)$ arbeiten, ist dieser Kern zwar nicht elementweise fest unter der Galois-Gruppe, aber trotzdem ein $\mathbb{Z}[G(\mathfrak{p})]$-Untermodul und es gilt $N \cong M/K_+(\mathfrak{p})^*$. Die vorher schon verwendete Interpretation von N als modulare Einheiten modulo Konstanten ist also mit der exakten Folge oben verträglich. Aus dem Diagramm

$$\begin{array}{ccccccc}
 & 0 & & 0 & & 0 & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & N[p] & & D_S^0[p] & & \mathcal{C}[p] & \\
 & \downarrow & & \downarrow & & \downarrow & \\
0 \to & N & \to & D_S^0 & \to & \mathcal{C} & \to 0 \\
 & \downarrow \cdot p & & \downarrow \cdot p & & \downarrow \cdot p & \\
0 \to & N & \to & D_S^0 & \to & \mathcal{C} & \to 0 \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & N/pN & & D_S^0/pD_S^0 & & \mathcal{C}/p\mathcal{C} & \\
 & \downarrow & & \downarrow & & \downarrow & \\
 & 0 & & 0 & & 0 &
\end{array}$$

ergibt sich durch Anwenden des Schlangenlemmas die exakte Folge

$$0 \to \mathcal{C}[p] \to N/pN \to D_S^0/pD_S^0 \to \mathcal{C}/p\mathcal{C} \to 0$$

von $\mathbb{F}_p[G(\mathfrak{p})]$-Moduln. In den beiden folgenden Abschnitten wird die Galois-Modulstruktur der mittleren Terme untersucht. Dazu werden weitere Eigenschaften der Menge der Spitzen sowie der Galois-Operation darauf verwendet. Außerdem werden wir mit Hilfe von modularen Einheiten gewisse Hauptspitzendivisoren konstruieren, auf denen sich die Operation der Galois-Gruppe bestimmen läßt.

Um allerdings die im dritten Kapitel entwickelten darstellungstheoretischen Methoden anwenden zu können, ist es notwendig, über einem algebraisch abgeschlossenen Körper zu arbeiten. Wir fixieren deshalb einen algebraischen Abschluß $\mathbb{F}$ von $\mathbb{F}_p$, der $\mathbb{F}_r$ und $A/\mathfrak{p}$ enthält. Bei der Untersuchung darstellungstheoretischer Fragen betrachten wir die sich aus der obigen ergebende Folge

(2.1.6)
$$0 \to \mathcal{C}[p] \otimes_{\mathbb{F}_p} \mathbb{F} \to N/pN \otimes_{\mathbb{F}_p} \mathbb{F} \to D_S^0/pD_S^0 \otimes_{\mathbb{F}_p} \mathbb{F} \to \mathcal{C}/p\mathcal{C} \otimes_{\mathbb{F}_p} \mathbb{F} \to 0$$

von $\mathbb{F}[G(\mathfrak{p})]$-Moduln. Da das Tensorieren mit $\mathbb{F}$ ein exakter Funktor von $\mathbb{F}_p$-Vektorräumen ist und für einen beliebigen $\mathbb{F}_p$-Vektorraum V auch $\dim_{\mathbb{F}_p} V = \dim_{\mathbb{F}} V \otimes_{\mathbb{F}_p} \mathbb{F}$ gilt, ergeben sich aus Dimensionsaussagen der tensorierten Folge direkt entsprechende Aussagen für die ursprüngliche Folge.

2.2. Spitzen und Spitzendivisoren

Bei der Untersuchung der Galois-Modulstruktur von D_S^0/pD_S^0 gehen wir von der Gruppe der Spitzendivisoren aus. Trotz unserer neuen Definition der Spitzen als den Stellen von $\mathcal{K}(\mathfrak{p})$ über der Stelle ∞ von $K(j)$ können wir S immer noch mit der Menge $\Gamma(\mathfrak{p})\backslash\mathbb{P}^1(K)$ identifizieren. Diese Identifikation ist auch mit der Operation der Galois-Gruppe verträglich, d.h. die natürliche Operation von $\Gamma(1)$ auf $\Gamma(\mathfrak{p})\backslash\mathbb{P}^1(K)$ durch

$$\gamma \cdot \Gamma(\mathfrak{p})[x:y] = \Gamma(\mathfrak{p})\gamma[x:y] = \Gamma(\mathfrak{p})[ax+cy : bx+dy]$$

für $\gamma = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^*$ macht die Divisorabbildung div zu einem Homomorphismus von Galois-Moduln. In der Menge $\Gamma(\mathfrak{p})\backslash\mathbb{P}^1(K)$ zeichnen wir die Klasse von $[1:0]$ aus und bezeichnen sie ebenfalls mit ∞. Das folgende Lemma gibt zwei einfache, aber grundlegende Eigenschaften der Operation der Galois-Gruppe auf den Spitzen an.

LEMMA 2.2.1. *Die Gruppe $G(\mathfrak{p})$ operiert transitiv auf der Menge S der Spitzen. Die Fixgruppe der Spitze ∞ ist die Gruppe $\{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in G(\mathfrak{p}) \bigm| a \in \mathbb{F}_r^*\}$.*

BEWEIS. Es ist ein allgemeiner Sachverhalt, daß die Galois-Gruppe einer Erweiterung globaler Körper transitiv operiert auf der Menge der Stellen der größeren Körpers, die über einer festen Stelle des kleineren Körpers liegen. In unserem speziellen Fall sieht man das aber auch direkt. Da $\Gamma(1)$ transitiv auf $\mathbb{P}^1(K)$ operiert, gilt dies auch für die Operation der Galois-Gruppe $\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^*$ der Erweiterung $\mathcal{K}(\mathfrak{p})|K_+(\mathfrak{p})(j)$ auf $\Gamma(\mathfrak{p})\backslash\mathbb{P}^1(K)$ und somit erst recht für die größere Galois-Gruppe der Erweiterung $\mathcal{K}(\mathfrak{p})|K(j)$.

Die Fixgruppe von ∞ in $\Gamma(1)$ ist offensichtlich $\{\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \Gamma(1) \bigm| a \equiv 1 \bmod \mathfrak{p},\, b \equiv 0 \bmod \mathfrak{p}\}$. Das Bild $\{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \bigm| c \in A/\mathfrak{p},\, a, d \in \mathbb{F}_r^*\}/\mathbb{F}_r^*$ dieser Gruppe in der Galois-Gruppe von $\mathcal{K}(\mathfrak{p})|K_+(\mathfrak{p})(j)$ ist die Fixgruppe in dieser kleineren Galois-Gruppe. Wir benötigen nun noch die über den geometrischen Rahmen hinausgehende Aussage, daß die Untergruppe $V = \{\left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right) \bigm| d \in (A/\mathfrak{p})^*,\, a \in \mathbb{F}_r^*\}$ von $G(\mathfrak{p})$ auch die Stelle ∞ fixiert

[Ge2]. Da beide Galois-Gruppen transitiv auf der Menge der Spitzen operieren, gilt

$$\#S = \#G(\mathfrak{p}) \cdot \infty = \#\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^* \cdot \infty$$

und für die Fixgruppen $G(\mathfrak{p})_\infty$ und $(\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^*)_\infty$ ergibt sich

$$\#G(\mathfrak{p})_\infty = \frac{\#G(\mathfrak{p})_\infty}{\#\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^*} \cdot \#(\Gamma(1)/\Gamma(\mathfrak{p})\mathbb{F}_r^*)_\infty \,.$$

Mit $\#A/\mathfrak{p} = q$ ist der Index der Galois-Gruppen gerade $\#(A/\mathfrak{p})^*/\mathbb{F}_r^* = (q-1)/(r-1)$ und die Ordnung der kleineren Fixgruppe ergibt sich aus obigem zu $q \cdot (r-1)$. Die Ordnung der Fixgruppe von ∞ in $G(\mathfrak{p})$ ist also gleich $q \cdot (q-1)$. Da aber das Erzeugnis von V und $\{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \bigm| c \in A/\mathfrak{p},\, a, d \in \mathbb{F}_r^*\}/\mathbb{F}_r^*$ in $G(\mathfrak{p})$ gerade die im Lemma angegebene Gruppe $\{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in G(\mathfrak{p}) \bigm| a \in \mathbb{F}_r^*\}$ ist und diese die Ordnung $q \cdot (q-1)$ hat, ist dies die Fixgruppe von ∞ in $G(\mathfrak{p})$. $\square$

Wir halten das Ergebnis über die Fixgruppe in einer Definition fest.

DEFINITION 2.2.2. Es sei $F := \{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}(2, A/\mathfrak{p} \bigm| a \in \mathbb{F}_r^*\}$, so daß $F/\mathbb{F}_r^*$ die Fixgruppe der Spitze ∞ in $G(\mathfrak{p})$ ist.

Mittels der Bahngleichung kann man nun direkt die Anzahl der Spitzen bestimmen.

KOROLLAR 2.2.3. *Die Anzahl der Spitzen von $X(\mathfrak{p})$ ist gleich $\frac{q^2-1}{r-1}$. Insbesondere ist sie teilerfremd zur Charakteristik p von K.*

Als nächstes betrachten wir die Galois-Modulstruktur der Spitzendivisorengruppe. Da der in der folgenden Aussage vorkommende Begriff der induzierten Darstellung erst im dritten Kapitel zusammen mit einigen Eigenschaften eingeführt wird, erklären wir die Bedeutung des hier vorkommenden Spezialfalls innerhalb des Beweises.

LEMMA 2.2.4. *Sei $\overline{F}$ die Fixgruppe in $G(\mathfrak{p})$ einer beliebigen Spitze, z.B. $\overline{F} = F/\mathbb{F}_r^*$. Dann gibt es einen $\mathbb{Z}[G(\mathfrak{p})]$-Modul-Isomorphismus*

$$D_S \cong \mathrm{ind}_{\overline{F}}^{G(\mathfrak{p})} \mathbb{Z} \,,$$

wobei $\mathbb{Z}$ der triviale $\mathbb{Z}[\overline{F}]$-Modul ist. Weiter ist

$$D_S/pD_S \cong \mathrm{ind}_{\overline{F}}^{G(\mathfrak{p})} \mathbb{F}_p \,,$$

wobei $\mathbb{F}_p$ der triviale $\mathbb{F}_p[\overline{F}]$-Modul ist.

BEWEIS. Wir schreiben abkürzend G für die Galois-Gruppe $G(\mathfrak{p})$. Es sei $\overline{F}$ die Fixgruppe in G von $s \in S$. Da G transitiv auf S operiert, gibt es eine Bijektion $\overline{F}\backslash G \xrightarrow{\cong} S;\, \overline{F}g \mapsto g^{-1} \cdot s$. Da G von links auf S operiert, induziert diese Bijektion eine Linksoperation von G auf $\overline{F}\backslash G$, die gegeben ist durch $g' \cdot \overline{F}g = \overline{F}g{g'}^{-1}$. Damit besitzen die beiden freien abelschen Gruppen, die jeweils von S bzw. von $\overline{F}\backslash G$ erzeugt werden, eine Struktur als $\mathbb{Z}[G]$ -Moduln und sind als solche isomorph. Die von $\overline{F}\backslash G$ erzeugte freie abelsche Gruppe ist als $\mathbb{Z}[G]$-Modul isomorph zur abelschen Gruppe der Abbildungen von $\overline{F}\backslash G$ nach $\mathbb{Z}$, auf der man die G-Operation durch $(g'f)(\overline{F}g) = f(\overline{F}gg')$ definiert. Dabei ist das Bild der Summe $\sum a_{Fg} \cdot \overline{F}g$ unter dem Isomorphismus die Abbildung $\overline{F}g \mapsto a_{\overline{F}g}$. Der $\mathbb{Z}[G]$-Modul der Abbildungen von $\overline{F}\backslash G$ nach $\mathbb{Z}$ ist offensichtlich isomorph zum $\mathbb{Z}[G]$-Modul der Abbildungen $\{f : G \to \mathbb{Z} \,\big|\, f(hg) = f(g) \text{ für alle } h \in \overline{F}, g \in G\}$, bei dem G wieder durch $(g'f)(g) = f(gg')$ operiert. Ein Vergleich mit der Definition der induzierten Darstellung in 3.5.1 zeigt, daß dies der Spezialfall des von $\overline{F}$ nach G induzierten trivialen $\overline{F}$-Moduls $\mathbb{Z}$ ist. Die Aussage über D_S/pD_S folgt nun direkt aus $D_S/pD_S = D_S \otimes_{\mathbb{Z}} \mathbb{F}_p$. □

Nun untersuchen wir, was beim Übergang von der vollen Spitzendivisorgruppe D_S zur Gruppe D_S^0 der Spitzendivisoren vom Grad 0 geschieht. Die Untergruppe D_S^0 ist frei vom Rang $\#S - 1$, eine $\mathbb{Z}$-Basis ist beispielsweise die Menge $\{s - \infty \,\big|\, \infty \neq s \in S\}$. Natürlich ist D_S^0 als $\mathbb{Z}$-Untermodul von D_S komplementierbar, es ist z.B. $D_S = D_S^0 \oplus \mathbb{Z}\infty$. Dies gilt aber nicht mehr als $\mathbb{Z}[G(\mathfrak{p})]$-Modul.

Lemma 2.2.5. *Als $\mathbb{Z}[G(\mathfrak{p})]$-Modul ist D_S^0 kein direkter Summand von D_S.*

Beweis. Betrachten wir $\mathbb{Z}$ als trivialen $\mathbb{Z}[G(\mathfrak{p})]$-Modul, so ist

$$0 \to D_S^0 \to D_S \xrightarrow{\deg} \mathbb{Z} \to 0$$

eine exakte Folge von $\mathbb{Z}[G(\mathfrak{p})]$-Moduln. Wäre D_S^0 ein direkter Summand von D_S, so müßte das Komplement ein über $\mathbb{Z}$ von einem $G(\mathfrak{p})$-invarianten Spitzendivisor A erzeugter Modul sein, der zudem den Grad ± 1 hat. Da $G(\mathfrak{p})$ transitiv auf den Spitzen operiert, müßte der Träger von A aus allen Spitzen bestehen und wegen der $G(\mathfrak{p})$-Invarianz von A müßten alle Koeffizienten gleich sein. Dies ist für einen Divisor vom Grad ± 1 nur möglich, wenn es nur eine Spitze gäbe. □

Wir sind nun aber nicht an der Untergruppe D_S^0 von D_S interessiert, sondern vielmehr an der Untergruppe D_S^0/pD_S^0 von D_S/pD_S, die wir beide als $\mathbb{F}_p[G(\mathfrak{p})]$-Moduln betrachten.

Lemma 2.2.6. *Der $\mathbb{F}_p[G(\mathfrak{p})]$-Untermodul D_S^0/pD_S^0 ist ein direkter Summand von D_S/pD_S. Das Komplement ist isomorph zum trivialen $\mathbb{F}_p[G(\mathfrak{p})]$-Modul $\mathbb{F}_p$.*

Beweis. Wir fassen $D_S/pD_S = \mathbb{F}_p \otimes_{\mathbb{Z}} D_S$ als $\mathbb{F}_p$-Vektorraum mit Basis S auf und $D_S^0/pD_S^0 = \mathbb{F}_p \otimes_{\mathbb{Z}} D_S^0$ als den Unterraum der Elemente, bei denen die Summe der S-Koordinaten gleich 0 ist. Sei $V = \{a \sum_{s \in S} s \,\big|\, a \in \mathbb{F}_p\}$ der von $\sum_{s \in S} s$ in D_S/pD_S erzeugte $\mathbb{F}_p$-Untervektorraum. Da $G(\mathfrak{p})$ die Menge S permutiert, ist das sogar ein $\mathbb{F}_p[G(\mathfrak{p})]$-Untermodul, der isomorph ist zum trivialen $\mathbb{F}_p[G(\mathfrak{p})]$-Modul $\mathbb{F}_p$. Wir zeigen nun, daß V ein Komplement von D_S^0/pD_S^0 ist.

Sei $x = \sum_{s\in S} a_s \cdot s$ ein Element aus $D_S^0/pD_S^0 \cap V$. Wegen $x \in V$ existiert ein $a \in \mathbb{F}_p$ mit $x = a\sum_{s\in S} s$ und damit ist $\sum_{s\in S}(a_s - a)\cdot s = 0$, d.h. $a_s = a$ für alle $s \in S$. Da das Element x aber auch in D_S^0/pD_S^0 liegt, gilt $0 = \sum_{s\in S} a_s = \#S \cdot a$ und weil $\#S$ nicht durch p teilbar ist, folgt $a = 0$ und $x = 0$.

Außerdem erzeugen V und D_S^0/pD_S^0 zusammen ganz D_S/pD_S. Da die Anzahl der Spitzen nicht durch p teilbar ist, ist $\#S$ in $\mathbb{F}_p$ invertierbar und für ein beliebiges Element $\sum_{s\in S} a_s \cdot s \in D_S/pD_S$ kann man $a = \frac{1}{\#S} \cdot \sum_{s\in S} a_s$ bilden. Dann ist

$$\sum_{s\in S} a_s \cdot s = \sum_{s\in S}(a_s - a)\cdot s + \sum_{s\in S} a\cdot s = \sum_{s\in S}(a_s - a)\cdot s + a\sum_{s\in S} s\,,$$

wobei der zweite Summand in V liegt und der erste in D_S^0/pD_S^0 wegen $\sum_{s\in s}(a_s - a) = \sum_{s\in S} a_s - \#S\cdot a = 0$. $\square$

Wir haben die Galois-Modulstruktur von D_S/pD_S identifiziert als eine induzierte Darstellung. Da der für uns interessante Untermodul D_S^0/pD_S^0 darin ein direkter Summand ist mit dem trivialen eindimensionalen Modul als Komplement, lassen sich die zentralen Komponenten von D_S^0/pD_S^0 leicht bestimmen. Das Zentrum von $G(\mathfrak{p})$ ist isomorph zu $(A/\mathfrak{p})^*/\mathbb{F}_r^*$, also eine zyklische Gruppe der Ordnung $(q-1)/(r-1)$. Die Charaktere dieser Gruppe sind nicht alle über $\mathbb{F}_p$ definiert, weshalb wir bei der folgenden Aussage zu einem algebraischen Abschluß von $\mathbb{F}_p$ übergehen.

PROPOSITION 2.2.7. *Sei $\mathbb{F}$ ein algebraischer Abschluß von $\mathbb{F}_p$ und $F/\mathbb{F}_r^* = \left\{\left(\begin{smallmatrix} a & c \\ 0 & d\end{smallmatrix}\right) \in G(\mathfrak{p}) \,\middle|\, a \in \mathbb{F}_r^*\right\}$. Es gibt einen $\mathbb{F}[G(\mathfrak{p})]$-Modul-Isomorphismus*

$$\mathrm{ind}_{F/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F} \cong \mathbb{F} \oplus (D_S^0/pD_S^0 \otimes_{\mathbb{F}_p} \mathbb{F})\,.$$

Für einen nichttrivialen Charakter $1 \neq \psi : (A/\mathfrak{p})^*/\mathbb{F}_r^* \to \mathbb{F}^*$ des Zentrums von $G(\mathfrak{p})$ erhält man einen $\mathbb{F}[G(\mathfrak{p})]$-Modul-Isomorphismus

$$(\mathrm{ind}_{F/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F})(\psi) \cong (D_S^0/pD_S^0 \otimes_{\mathbb{F}_p} \mathbb{F})(\psi)\,.$$

BEWEIS. Aus Lemma 2.2.4 ergibt sich $D_S/pD_S = D_S \otimes_{\mathbb{Z}} \mathbb{F}_p = \mathrm{ind}_{F/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F}_p$ und somit auch $D_S/pD_S \otimes_{\mathbb{F}_p} \mathbb{F} = \mathrm{ind}_F^{G(\mathfrak{p})} \mathbb{F}$, wobei $\mathbb{F}_p$ und $\mathbb{F}$ als triviale $G(\mathfrak{p})$-Moduln aufgefaßt werden. Aus Lemma 2.2.6 folgt $D_S/pD_S \otimes_{\mathbb{F}_p} \mathbb{F} = \mathbb{F} \oplus D_S^0/pD_S^0 \otimes_{\mathbb{F}_p} \mathbb{F}$. Zusammen ergibt dies die erste Behauptung. Die zweite folgt daraus direkt, da für einen nichttrivialen Charakter ψ und den trivialen Modul $\mathbb{F}$ natürlich $\mathbb{F}(\psi) = 0$ ist. $\square$

2.3. Modulare Einheiten und Siegel-Divisoren

Bei der Untersuchung der Gruppe N der Hauptspitzendivisoren sowie des Quotienten N/pN werden wir Ergebnisse aus **[Ge2]** über modulare Einheiten verwenden, deren Divisoren ja Elemente aus N sind.

Die Konstruktion von modularen Einheiten wird sogenannte Siegel-Funktionen verwenden, welche wir nun beschreiben.

Ähnlich wie die Funktionen h_u aus Abschnitt 2.1, die ja zusammen mit j den Funktionenkörper $\mathcal{K}(\mathfrak{p})$ der Modulkurve erzeugen, werden die Siegel-Funktionen aus den Funktionen e_u und einem weiteren Faktor zusammengesetzt. Diesen werden wir aus der oben schon beschriebenen Modulform Δ gewinnen. Dabei verwenden wir eine Produktentwicklung, die das Analogon der Jacobi-Formel für die klassische Diskriminantenfunktion ist. Zuerst müssen wir uns einen Parameter verschaffen, der die Rolle von $e^{2\pi i z}$ in der klassischen Theorie spielt. Zu A als Rang 1-Gitter in C gehört die Funktion

$$e_A(z) = z \prod_{0 \neq a \in A} (1 - z/a) \,.$$

In der klassischen Theorie hat die Funktion $z \mapsto e^{2\pi i z}$ zwar ein einfacheres Periodengitter als die Funktion $z \mapsto e^z$, dafür aber auch transzendente Koeffizienten an Stelle von rationalen. Genauso hat die Wahl des besonders einfachen Gitters A den Nachteil, daß die Koeffizienten von e_A transzendent über K sind. Deshalb nehmen wir noch eine Umnormierung vor, durch die sich die Produktformel dann leichter angeben läßt.

Der Carlitz-Modul ist ein Drinfeld-Modul vom Rang 1 und gehört somit zu einem eindimensionalen Gitter $A\overline{\pi}$ mit einem von Null verschiedenen Element $\overline{\pi} \in C$, welches bis auf Einheiten von A wohlbestimmt ist. Mit Hilfe dieses Elements $\overline{\pi}$ definieren wir

$$t(z) := \overline{\pi}^{-1} e_A^{-1}(z)$$

und erhalten einen Parameter

$$s(z) := t(z)^{r-1}$$

der Modulkurve $X(1)$ an der Spitze ∞ **[Ge1]**. Zur Beschreibung der Faktoren der Produktentwicklung von Δ benötigen wir noch einige Polynome, die mit Hilfe des Carlitz-Moduls definiert werden. Wir fassen dabei die Bilder des Carlitz-Moduls als $\mathbb{F}_r$-lineare Polynome auf, d.h. wir definieren den Carlitz-Modul durch $\rho_T = TX + X^r$. Für ein Polynom $a \in A$ vom Grad d erhalten wir mit $f_a(X) = \rho_a(X^{-1})X^{r^d}$ ein Polynom vom Grad r^d in X mit Koeffizienten in A. Nun können wir die Aussage über die Produktentwicklung von Δ formulieren.

SATZ 2.3.1. **[Ge3]** *Die Drinfeldsche Diskriminantenfunktion Δ besitzt eine Produktentwicklung*

$$\Delta(z) = -\overline{\pi}^{r^2-1} t(z)^{r-1} \prod_{\substack{a \in A \\ unit\ddot{a}r}} f_a^{(r^2-1)(r-1)}(t(z))$$

für hinreichend kleines $|t(z)|$.

Da die Polynome f_a tatsächlich sogar Polynome in X^{r-1} sind, ist die angegebene Entwicklung auch wirklich eine Produktentwicklung von Δ in dem Parameter $s(z) = t^{r-1}(z)$.

Als nächstes definieren wir als Analogon der klassischen Dedekindschen η-Funktion eine formale Potenzreihe in $t^{\frac{1}{r+1}}$ durch

$$\eta = \overline{\pi} t^{\frac{1}{r+1}} \prod_{\substack{a \in A \\ \text{unitär}}} f_a^{r-1}(t) \,,$$

so daß $\eta^{r^2-1} = -\Delta$ gilt.

Die Koeffizienten der Reihenentwicklungen von Δ, η und verwandter Funktionen sind in **[Ge7]**,**[Ge8]**,**[LoWa]** untersucht worden. So hängen beispielsweise die Koeffizienten von η^{-1} mit bestimmten Summenzerlegungen natürlicher Zahlen zusammen, ähnlich wie die Koeffizienten der Inversen der klassischen η-Funktion mit Partitionszahlen **[Ge8]**.

Obwohl wir η nur als formale Potenzreihe in einer $r+1$-ten Wurzel von t definiert haben, kann man nachrechnen, daß η^{r+1} eine Modulform für $\Gamma(\mathfrak{p})$ vom Gewicht $r+1$ ist. Um die Siegel-Funktionen definieren zu können, benötigen wir aber erst einmal die Potenzreihe η.

Definition 2.3.2. Für $0 \neq u \in (K/A)^2$ mit $\mathfrak{p} \cdot u = 0$ ist die Siegel-Funktion g_u die durch $g_u = e_u \cdot \eta$ definierte formale Potenzreihe in $t^{\frac{1}{r+1}}$.

Aus der Definition ergibt sich, daß die Siegel-Funktionen selbst keine Elemente des Funktionenkörpers von $X(\mathfrak{p})$ sind. Da aber η^{r+1} eine auf $\mathcal{H}$ wohldefinierte Funktion liefert, ist auch ein endliches Produkt $\prod g_u^{m(u)}$ mit $m(u) \in \mathbb{N}_0$ eine wohldefinierte Funktion auf $\mathcal{H}$, falls $\sum m(u) \equiv 0 \bmod r+1$ ist. Weiter ist η^{r+1} eine Modulform für $\Gamma(\mathfrak{p})$ vom Gewicht $r+1$ und e_u eine solche vom Gewicht -1, also wird die Funktion $\prod g_u^{m(u)}$ dann sogar zu einer Modulform für $\Gamma(\mathfrak{p})$ vom Gewicht 0, also zu einem Element des Funktionenkörpers der Modulkurve $X(\mathfrak{p})$, allerdings vorerst über C betrachtet. Nun erhält man aber bei der Entwicklung von $\overline{\pi}^{-1}\eta$ und $\overline{\pi}e_u$ um die Spitze ∞ Koeffizienten, die schon in K liegen. Folglich haben die Siegel-Funktionen $g_u = \eta \cdot e_u$ auch Entwicklungskoeffizienten in K und die Produkte $\prod g_u^{m(u)}$ mit $\sum m(u) \equiv 0 \bmod r+1$ sind Elemente von $\mathcal{K}(\mathfrak{p})$.

Da die Divisoren der e_u und η^{r+1} nur Spitzen enthalten, besitzt auch eine Funktion $\prod g_u^{m(u)}$ mit $\sum m(u) \equiv 0 \bmod r+1$ einen Divisor, dessen Träger in der Menge der Spitzen von $X(\mathfrak{p})$ liegt. Darüber hinaus kann man für eine Siegel-Funktion g_u formal einen Divisor mit Träger in den Spitzen definieren, bei dem aber die Koeffizienten keine ganzen Zahlen sein müssen, sondern nur in $\mathbb{Q}$, genauer gesagt in $\frac{1}{r+1}\mathbb{Z}$ liegen. Für die Siegel-Funktion g_u ist nämlich g_u^{r+1} ein Element des Funktionenkörpers von $X(\mathfrak{p})$, für die Funktion g_u^{r+1} kann man also den Divisor $\operatorname{div} g_u^{r+1}$

bilden, dessen Träger in den Spitzen liegt. Für g_u selbst setzt man dann $\operatorname{div} g_u = \frac{1}{r+1}\operatorname{div} g_u^{r+1}$.

Schließlich bemerken wir noch, daß für ein $0 \neq u \in (K/A)^2$ mit $\mathfrak{p}u = 0$ die Siegelfunktion g_u nur bis auf einen konstanten Faktor von der Klasse von u in $U = ((\frac{1}{\mathfrak{p}}A/A)^2 - 0)/\mathbb{F}_r^*$ abhängt, d.h. beim Betrachten der Divisoren genügt es, die Siegelfunktionen mittels der Menge U zu indizieren.

Definition 2.3.3. Sei $\mathcal{S}' := \langle \operatorname{div} g_u \bigm| u \in U \rangle$ die von den Divisoren der Siegelfunktionen in $\frac{1}{r+1}D_S \subseteq D_S \otimes_{\mathbb{Z}} \mathbb{Q}$ erzeugte Untergruppe. Weiter sei die Gruppe der Siegel-Divisoren definiert durch $\mathcal{S} := \mathcal{S}' \cap D_S$.

Da $\mathcal{S}'$ eine Untergruppe von $\frac{1}{r+1}D_S$ ist, erhält man auf $\mathcal{S}'$ eine $\mathbb{Z}[G(\mathfrak{p})]$-Modul-Struktur. Aus dem obigen ergibt sich, daß $(r+1)\cdot \mathcal{S}' \subseteq \mathcal{S}$ gilt, insbesondere hat die Gruppe $\mathcal{S}'/\mathcal{S}$ eine zu p teilerfremde Ordnung und folglich gilt $\mathcal{S}'/p\mathcal{S}' \cong \mathcal{S}/p\mathcal{S}$ als abelsche Gruppe und natürlich auch als $\mathbb{Z}[G(\mathfrak{p})]$-Modul.

Wir werden nun die Struktur von $\mathcal{S}'$ genauer untersuchen. Dazu führen wir eine neue Parametrisierung der Spitzen ein.

Lemma 2.3.4. *Die Menge U steht in Bijektion zur Menge der Spitzen durch die Abbildung, welche ein Element $\Gamma(\mathfrak{p})[a:b] \in S$ mit teilerfremden $a, b \in A$ auf das Element $\frac{1}{\mathfrak{p}}(a,b) \bmod \mathbb{F}_r^*$ in U abbildet.*

Beweis. Die Anzahl der Spitzen haben wir bereits in Korollar 2.2.3 bestimmt, es ist $\#S = \frac{q^2-1}{r-1}$. Die Menge $(\frac{1}{\mathfrak{p}}A/A)^2$ hat q^2 Elemente, sie steht z.B. in Bijektion zu $(A/\mathfrak{p}A)^2$. Folglich hat die Menge der von 0 verschiedenen $\mathbb{F}_r^*$-Klassen auch gerade $\frac{q^2-1}{r-1}$ Elemente. Damit stehen S und U in Bijektion zueinander. Wir zeigen nun noch, daß die angegebene Abbildung eine solche Bijektion ist.

Zuerst behandeln wir die Wohldefiniertheit der Abbildung. Daß sich jede Spitze in der angegebenen Weise, d.h. als $\Gamma(\mathfrak{p})[a:b]$ mit teilerfremden $a, b \in A$, schreiben läßt, ist klar. Aufgrund der Teilerfremdheit von a, b ist (a,b) auch $\mathfrak{p}$-primitiv, d.h. $\frac{1}{\mathfrak{p}}(a,b) \notin A^2$. Die Bedingung der Ganzheit und Teilerfremdheit von a, b bewirkt auch, daß die Vertreter a, b der Klasse $[a:b]$ bis auf einen Faktor aus ${\mathbb{F}_r}^*$ bestimmt sind, der beim Übergang zu U verschwindet. Außerdem ist für teilerfremde $a, b \in A$ und beliebiges $\gamma \in \Gamma(\mathfrak{p})$ das Paar $(a', b') = \gamma(a,b)$ wieder ganz, teilerfremd und erfüllt $a' \equiv a \bmod \mathfrak{p}$ sowie $b' \equiv b \bmod \mathfrak{p}$, also ist $\frac{1}{\mathfrak{p}}(a,b) = \frac{1}{\mathfrak{p}}(a',b')$ in U. Folglich ist das Bild der Spitze von der Wahl von Repräsentanten unabhängig und die Abbildung wohldefiniert.

Für ein Element $\frac{1}{\mathfrak{p}}(a,b)$ aus U sei g der größte gemeinsame Teiler von a und b sowie x das Produkt der Primteiler, die in a/g vorkommen und nicht in g. Dann sind a und $b + \mathfrak{p}x$ teilerfremd und $\Gamma(\mathfrak{p})[a : b + \mathfrak{p}x]$ ist ein Urbild von $\frac{1}{\mathfrak{p}}(a,b)$. Die angegebene Abbildung ist also surjektiv und damit auch bijektiv. $\square$

Durch die Indizierung der Siegelfunktionen mittels der zu den Spitzen in Bijektion stehenden Menge U läßt sich die gruppentheoretische Struktur von $\mathcal{S}'$ leicht beschreiben. Die Gruppe $\mathcal{S}'$ wird nämlich von den $\operatorname{div} g_u$ mit $u \in U$ erzeugt, und zwar fast frei.

PROPOSITION 2.3.5. **[Ge2]** *Als abelsche Gruppe ist $\mathcal{S}'$ isomorph zu dem Quotienten*

$$(\oplus_{u \in U} \mathbb{Z} \cdot u)/\mathbb{Z} \cdot \sum_{u \in U} u$$

der von U erzeugten freien abelschen Gruppe.

Auf U haben wir schon die natürliche rechte Operation von $G(\mathfrak{p})$ betrachtet, die sich aus der üblichen Matrixmultiplikation ableitet. Wir benutzen nun die durch $\gamma \cdot u := u \cdot \gamma^{-1}$ definierte linke Operation. Durch sie wird $\sum_{u \in U} \mathbb{Z}u$ zu einem $\mathbb{Z}[G(\mathfrak{p})]$-Modul und offensichtlich ist die Untergruppe $\mathbb{Z} \cdot \sum_{u \in U} u$ auch ein Untermodul. Wir bestimmen nun die $\mathbb{Z}[G(\mathfrak{p})]$-Modulstruktur der Siegeldivisoren.

LEMMA 2.3.6. *Sei $u \in U$ und $\gamma \in G(\mathfrak{p})$. Dann ist $\gamma \cdot \operatorname{div} g_u = \operatorname{div} g_{\gamma \cdot u}$ und somit ist die Abbildung*

$$\sum_{u \in U} \mathbb{Z}u/\mathbb{Z} \cdot \sum_{u \in U} u \xrightarrow{\cong} \mathcal{S}';\ u \mapsto \operatorname{div} g_u$$

ein Isomorphismus von $\mathbb{Z}[G(\mathfrak{p})]$-Moduln.

BEWEIS. Aufgrund von Proposition 2.3.5 ist nur $\gamma \cdot \operatorname{div} g_u = \operatorname{div} g_{\gamma \cdot u}$ zu zeigen. Wegen der Definition des Divisors von g_u ist dies äquivalent zu $\gamma \cdot \operatorname{div} g_u^{r^2-1} = \operatorname{div} g_{\gamma \cdot u}^{r^2-1}$. Da die Divisorabbildung div ein $\mathbb{Z}[G(\mathfrak{p})]$-Homomorphismus ist, bleibt $\gamma \cdot g_u^{r^2-1} = g_{\gamma \cdot u}^{r^2-1}$ zu zeigen. Wir drücken nun die Funktion $g_u^{r^2-1}$ mittels der Funktionen h_u und j aus, auf denen die Operation von $G(\mathfrak{p})$ bekannt ist.

Aus den drei Formeln

$$j = \frac{g^{r+1}}{\Delta}, \quad \eta^{r^2-1} = -\Delta \quad \text{und} \quad h_u = g \cdot e_u^{r-1}$$

ergibt sich

$$\begin{aligned} g_u^{r^2-1} &= \eta^{r^2-1} \cdot e_u^{r^2-1} = -\Delta e_u^{r^2-1} = -\frac{g^{r+1}}{j} e_u^{r^2-1} \\ &= -\frac{(g \cdot e_u^{r-1})^{r+1}}{j} = -\frac{h_u}{j}. \end{aligned}$$

Da j unter der Galois-Gruppe $G(\mathfrak{p})$ invariant ist, folgt die Behauptung $\gamma \cdot g_u^{r^2-1} = g_{\gamma \cdot u}^{r^2-1}$ direkt aus der Operation der Galois-Gruppe $G(\mathfrak{p})$ auf h_u durch $\gamma \cdot h_u = h_u^{\gamma^{-1}} = h_{u\gamma^{-1}} = h_{\gamma \cdot u}$. $\square$

Wir untersuchen nun die Operation von $G(\mathfrak{p})$ auf U. Dabei erhalten wir ein zu Lemma 2.2.1 analoges Ergebnis.

LEMMA 2.3.7. *Die Gruppe $G(\mathfrak{p})$ operiert transitiv auf U. Die Fixgruppe von $\frac{1}{\mathfrak{p}}(1,0) \in U$ ist die Untergruppe $\{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in G(\mathfrak{p}) \bigm| d \in \mathbb{F}_r^*\}$.*

BEWEIS. Wir bestimmen zuerst die Fixgruppe von $\frac{1}{\mathfrak{p}}(1,0)$. Sei dazu $\left(\begin{smallmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{smallmatrix}\right)$ ein $\bmod \mathbb{F}_r^*$-Vertreter eines Elements γ aus $G(\mathfrak{p})$ mit $a, b, c, d \in A$. Sei weiter $x \in A$ ein Vertreter von $\det \left(\begin{smallmatrix} \overline{a} & \overline{c} \\ \overline{b} & \overline{d} \end{smallmatrix}\right)^{-1}$. Dann ist $\left(\begin{smallmatrix} \overline{xa} & \overline{xc} \\ \overline{xb} & \overline{xd} \end{smallmatrix}\right)$ ein Vertreter von γ^{-1} und in U gilt

$$\gamma \cdot \frac{1}{\mathfrak{p}}(1,0) = \frac{1}{\mathfrak{p}}(1,0) \begin{pmatrix} xa & xc \\ xb & xd \end{pmatrix} = \frac{1}{\mathfrak{p}}(xa, xc)\,.$$

Also fixiert γ das Element $\frac{1}{\mathfrak{p}}(1,0) \in U$ genau dann, wenn $xa \equiv 1 \bmod \mathfrak{p}$ und $xc \equiv 0 \bmod \mathfrak{p}$ gilt. Nun ist aber x teilerfremd zu $\mathfrak{p}$ und modulo $\mathfrak{p}$ gleich dem Inversen von $ad - bc$. Die beiden Bedingungen sind also äquivalent zu $\overline{c} = 0$ und $\overline{d} = 1$. Die Fixgruppe von $\frac{1}{\mathfrak{p}}(1,0)$ in $G(\mathfrak{p})$ ist also die behauptete. Da die beiden Mengen S und U gleichviele Elemente haben und die Fixgruppen in $G(\mathfrak{p})$ von $\infty \in S$ und $\frac{1}{\mathfrak{p}}(1,0) \in U$ offensichtlich auch, ergibt sich die Transitivität der Operation auf U aus der schon gezeigten Transitivität der Operation auf S. □

DEFINITION 2.3.8. Es sei $E := \{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in \mathrm{GL}(2, A/\mathfrak{p}) \bigm| d \in \mathbb{F}_r^*\}$, so daß $E/\mathbb{F}_r^*$ die Fixgruppe von $\frac{1}{\mathfrak{p}}(1,0) \in U$ in $G(\mathfrak{p})$ ist.

Wir können jetzt eine zur Proposition 2.2.7 analoge Aussage machen.

PROPOSITION 2.3.9. *Sei $\mathbb{F}$ ein algebraischer Abschluß von $\mathbb{F}_p$ und $\psi : (A/\mathfrak{p})^*/\mathbb{F}_r^* \to \mathbb{F}$ ein nichttrivialer Charakter des Zentrums von $G(\mathfrak{p})$. Es gibt $\mathbb{F}[G(\mathfrak{p})]$-Modul-Isomorphismen*

$$\mathrm{ind}_{E/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F} \cong \mathbb{F} \oplus (\mathcal{S}/p\mathcal{S} \otimes_{\mathbb{F}_p} \mathbb{F})$$

und

$$(\mathrm{ind}_{E/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F})(\psi) \cong (\mathcal{S}/p\mathcal{S} \otimes_{\mathbb{F}_p} \mathbb{F})(\psi)\,.$$

BEWEIS. Wir haben bereits die $\mathbb{Z}[G(\mathfrak{p})]$-Isomorphismen $\mathcal{S}/p\mathcal{S} \cong \mathcal{S}'/p\mathcal{S}'$ und $\mathcal{S}' \cong \bigoplus_{u \in U} \mathbb{Z}u/\mathbb{Z} \cdot \sum_{u \in U} u$ gefunden. Aus Lemma 2.3.7 folgt wie im Beweis von Lemma 2.2.4 ein Isomorphismus $\bigoplus_{u \in U} \mathbb{Z}u \cong \mathrm{ind}_E^{G(\mathfrak{p})} \mathbb{Z}$. Unter diesem Isomorphismus sei M das Bild des Untermoduls $\mathbb{Z} \sum_{u \in U} u$ von $\bigoplus_{u \in U} \mathbb{Z}u$. Offensichtlich operiert $G(\mathfrak{p})$ auf $\sum_{u \in U} u$ und damit auf M trivial. Genauso wie in Lemma 2.2.6 ergibt sich, daß man nach Tensorieren über $\mathbb{Z}$ mit $\mathbb{F}_p$ einen direkten Summanden $M \otimes_{\mathbb{Z}} \mathbb{F}_p$ erhält, der isomorph zum trivialen Modul ist. Nach weiterem Tensorieren mit $\mathbb{F}$ erhält man $\mathbb{F} \oplus \mathcal{S}/p\mathcal{S} \otimes_{\mathbb{F}_p} \mathbb{F} \cong \mathrm{ind}_E^{G(\mathfrak{p})} \mathbb{F}$. □

Wir sehen nun, daß die beiden mittleren $G(\mathfrak{p})$-Moduln in der Folge (2.1.6) formal ziemlich ähnlich aussehen. Der Unterschied besteht in der Untergruppe von $G(\mathfrak{p})$, von der aus der triviale Modul hochinduziert wird. In Kapitel 3 werden wir sehen, daß die Moduln $(\mathrm{ind}_{E/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F})(\psi)$

bzw. $(\mathrm{ind}_{F/\mathbb{F}_r^*}^{G(\mathfrak{p})}\mathbb{F})(\psi)$ beide zu einer besonderen Serie von Darstellungen gehören, allerdings in gewisser Weise zu komplementären Parametern.

2.4. Die Siegeldivisorklassengruppe

Im ersten Abschnitt dieses Kapitels haben wir die kurze exakte Folge

$$0 \to N \to D_S^0 \to \mathcal{C} \to 0$$

von $\mathbb{Z}[G(\mathfrak{p})]$-Moduln betrachtet, durch welche die Spitzendivisorklasse $\mathcal{C}$ als Quotient der Spitzendivisoren vom Grad 0 und der Hauptspitzendivisoren definiert ist. Mit Hilfe der Multiplikation mit p auf den drei Gruppen und einer Anwendung des Schlangenlemmas ergab sich nach Tensorieren mit dem algebraischen Abschluß $\mathbb{F}$ von $\mathbb{F}_p$ und Auswahl des isotypischen Anteils zu einem zentralen Charakter ψ von $G(\mathfrak{p})$ die exakte Folge

$$0 \to (\mathcal{C}[p] \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to (N/pN \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to (D_S^0/pD_S^0 \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to (\mathcal{C}/p\mathcal{C} \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to 0$$

von $\mathbb{F}[G(\mathfrak{p})]$-Moduln. Während die relativ einfache Struktur der Gruppe D_S^0 es erlaubte, die Struktur von $(D_S^0/pD_S^0 \otimes_{\mathbb{F}_p} \mathbb{F})(\psi)$ in Proposition 2.2.7 zu bestimmen, haben wir im vorigen Abschnitt die Gruppe N der Hauptspitzendivisoren durch die Untergruppe $\mathcal{S}$ der Siegeldivisoren ersetzt.

Definition 2.4.1. Die Gruppe $\mathcal{C}_{\text{Siegel}} := D_S^0/\mathcal{S}$ heißt Siegeldivisorklassengruppe.

Aus der definierenden Folge

$$0 \to \mathcal{S} \to D_S^0 \to \mathcal{C}_{\text{Siegel}} \to 0$$

der Siegeldivisorklassengruppe ergibt sich wie oben eine exakte Folge

$$0 \to (\mathcal{C}_{\text{Siegel}}[p] \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to (\mathcal{S}/p\mathcal{S} \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to (D_S^0/pD_S^0 \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to (\mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}} \otimes_{\mathbb{F}_p} \mathbb{F})(\psi) \to 0$$

von $\mathbb{F}[G(\mathfrak{p})]$-Moduln, bei der nun aber auch die Struktur des linken der beiden mittleren Terme in Proposition 2.3.9 beschrieben ist.

Die für die Drinfeld'sche Modulkurve verwendeten Siegelfunktionen bzw. Siegeldivisoren haben Vorbilder in der klassischen Theorie. Dort weiß man, daß die Siegeldivisoren schon alle Hauptspitzendivisoren liefern. Ob dies auch in unserer Situation gilt, ist nicht bekannt. Der Zusammenhang zwischen der Spitzendivisorklassengruppe $\mathcal{C}$ und der Siegeldivisorklassengruppe $\mathcal{C}_{\text{Siegel}}$ wird durch die exakte Folge

$$0 \to N/\mathcal{S} \to D_S^0/\mathcal{S} \to D_S^0/N \to 0$$

beschrieben, d.h. $\mathcal{C}$ ist der Quotient von $\mathcal{C}_{\text{Siegel}}$ nach der Untergruppe $N/\mathcal{S}$.

Eine obere Abschätzung für die Gruppe $N/\mathcal{S}$ ergibt sich daraus, daß der Index der Siegeldivisoren in D_S^0 bekannt ist. Für den p-Anteil von $[D_S^0 : \mathcal{S}]$ ergibt sich insbesondere folgendes.

PROPOSITION 2.4.2. *Sei $r = p^n$ und $q = r^d = p^{n \cdot d}$. Dann ist die p-adische Bewertung des Index der Siegeldivisoren in den Spitzendivisoren vom Grad 0 gegeben durch*

$$v_p([D_S^0 : \mathcal{S}]) = n \cdot \frac{d}{2}(\frac{r^{2d}-1}{r-1} - r^d - 1)\,.$$

BEWEIS. Die Behauptung ergibt sich direkt aus [**Ge2**, Korollar 6.15]. □

Damit erhalten wir eine Aussage über den Zusammenhang von $\mathcal{C}$ und $\mathcal{C}_{\text{Siegel}}$.

KOROLLAR 2.4.3. *Sei $r = p^n$ und $q = r^d$. Für die Anzahl zyklischer p-Komponenten der Spitzendivisorklassengruppe bzw. der Siegeldivisorklassengruppe, d.h. für $\dim_{\mathbb{F}_p} \mathcal{C}/p\mathcal{C}$ bzw. $\dim_{\mathbb{F}_p} \mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}}$ gelten die Abschätzungen*

$$\dim_{\mathbb{F}_p} \mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}} - n \cdot \frac{d}{2}(\frac{r^{2d}-1}{r-1} - r^d - 1) \leqslant \dim_{\mathbb{F}_p} \mathcal{C}/p\mathcal{C} \leqslant \dim_{\mathbb{F}_p} \mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}}\,.$$

BEWEIS. Da $\mathcal{C}$ der Quotient von $\mathcal{C}_{\text{Siegel}}$ nach der Untergruppe $N/\mathcal{S}$ ist, kann die Anzahl der zyklischen p-Komponenten von $\mathcal{C}$ höchstens so groß sein wie die von $\mathcal{C}_{\text{Siegel}}$ und sie ist mindestens so groß wie die Differenz der Anzahl der zyklischen p-Komponenten von $\mathcal{C}_{\text{Siegel}}$ und $N/\mathcal{S}$. Die Anzahl der zyklischen p-Komponenten von $N/\mathcal{S}$ ist höchstens so groß wie die p-adische Bewertung der Gruppenordnung von $N/\mathcal{S}$. Da $N/\mathcal{S}$ eine Untergruppe von $D_S^0/\mathcal{S}$ ist, ergibt sich die untere Abschätzung von $\dim_{\mathbb{F}_p} \mathcal{C}/p\mathcal{C}$ aus der vorigen Proposition. □

Aus der Proposition bzw. dem Korollar ergibt sich außerdem, daß im Falle eines linearen Polynoms $\mathfrak{p}$ die Siegeldivisorklassengruppe und die Spitzendivisorklassengruppe den gleichen p-Anteil haben. Tatsächlich sind in diesem Fall sogar schon die beiden Gruppen gleich [**Ge2**].

KAPITEL 3

Modulare Darstellungen von $\mathrm{GL}(2, \mathbb{F}_q)$

Wie wir im vorigen Kapitel gesehen haben, müssen wir zur weiteren Untersuchung der Spitzen- bzw. Siegeldivisorklassengruppe modulare Darstellungen, d.h. Darstellungen in positiver Charakteristik, der Gruppe $G(\mathfrak{p})$ untersuchen. Wir werden uns im folgenden zuerst mit einigen Aspekten der Darstellungstheorie beschäftigen, die von der vorliegenden Gruppe unabhängig sind. Danach spezialisieren wir uns auf die Gruppe $\mathrm{GL}(2, \mathbb{F}_q)$. Am Ende des Kapitels beschreiben wir den Zusammenhang zwischen den Darstellungen von $G(\mathfrak{p}) = \mathrm{GL}(2, A/\mathfrak{p})/\mathbb{F}_r^*$ und von $\mathrm{GL}(2, \mathbb{F}_q)$ mit $q = \#A/\mathfrak{p}$. Die Untersuchung der Darstellungen von $\mathrm{GL}(2, \mathbb{F}_q)$ sind nun von der geometrischen Herkunft der uns interessierenden Fälle unabhängig und rein darstellungstheoretischer Natur. Darüber hinaus sind sie aufgrund der großen allgemeinen Bedeutung der betrachteten Gruppen von eigenem Interesse.

Wie bereits im ersten Kapitel angedeutet, sind die im Vergleich zu Darstellungen über den komplexen Zahlen auftretenden Besonderheiten im modularen Fall für uns von besonderer Bedeutung. Im ersten Abschnitt dieses Kapitels stellen wir deshalb einige grundlegende Eigenschafte modularer Darstellungen für beliebige endliche Gruppen zusammen. Der Umstand, daß Darstellungen in positiver Charakteristik i.a. nicht halbeinfach sind, führt zu den Begriffen des Sockels und der Sockelreihe, welche später die wesentlichen Hilfsmittel der Strukturanalyse der betrachteten Darstellungen sind. Die Methode für die Nutzung der Sockelreihe wird in Abschnitt 2 und 3 beschrieben. Im vierten Abschnitt gehen wir genauer auf die modulare Darstellungstheorie linearer Gruppen vom Typ GL(2) und SL(2) über endlichen Körpern ein und beschreiben insbesondere deren einfache Darstellungen. Die Klassifikation der einfachen Darstellungen zeigt, daß für die betrachteten 2×2-Matrixgruppen symmetrische Potenzen der natürlichen zweidimensionalen Darstellung von grundlegender Bedeutung sind. Im fünften Abschnitt werden Eigenschaften von Hauptreihendarstellungen untersucht. Dies sind gewisse induzierte Darstellungen, zu denen auch die am Ende von Kapitel 2 aufgetretenen Darstellungen gehören. Dabei spielen auch wieder symmetrische Potenzen der natürlichen Darstellung eine Rolle. Deren Sockelreihe sowie die einfachen Faktoren der zugehörigen Quotienten werden im sechsten Abschnitt bestimmt. Die dabei gewonnenen Informationen können dann im folgenden Kapitel dazu benutzt werden, Darstellungen der Hauptreihe miteinander zu vergleichen. Wie die darstellungstheoretischen Ergebnisse mit der Modulkurve $X(\mathfrak{p})$ zusammenhängen, wird schließlich im letzten Abschnitt des Kapitels erläutert.

3.1. Besonderheiten modularer Darstellungen

Ganz allgemein ist eine Darstellung einer gegebenen Gruppe ein Homomorphismus dieser Gruppe in die Automorphismengruppe eines algebraischen Objekts, was einer strukturerhaltenden Operation der Gruppe auf der dem algebraischen Objekt zugrundeliegenden Menge entspricht.

Das wichtigste Beispiel hierfür ist die lineare Operation einer Gruppe auf einem Vektorraum. Der Homomorphismus zwischen der Ausgangsgruppe und der Automorphismengruppe des Vektorraums stellt einen Vergleich der beiden Gruppen dar, der den Einsatz von Methoden der linearen Algebra ermöglicht, um Informationen über die Gruppe zu gewinnen. Ein Beispiel für die Nützlichkeit linearer Darstellungen ist etwa der Beweis von Burnsides pq-Satz. Neben solchen allgemeinen gruppentheoretischen Resultaten findet die Darstellungstheorie natürlich auch überall dort Anwendung, wo spezielle Gruppen auf natürliche Weise mit einer Operation auf einem Vektorraum ausgestattet sind. Dies tritt z.B. häufig auf bei Galois-Gruppen von Zahlkörpern oder in unserem Fall von Funktionenkörpern. Es ist dabei nützlich, für lineare Darstellungen einer Gruppe auch die gleichwertige Sprechweise von Moduln über dem zugehörigen Gruppenring zu verwenden. Alle in diesem Zusammenhang verwendeten Begriffe (Gruppenring, einfach/halbeinfach, unzerlegbar, projektiv usw.) finden sich z.B. in [**La1**],[**CuRe**].

Im folgenden schränken wir den Fall einer beliebigen linearen Darstellung einer Gruppe noch weiter ein. Es sei G eine endliche Gruppe und alle betrachteten Darstellungen seien endlichdimensional über einem algebraisch abgeschlossenen Körper k. Die in diesem Kontext lebende Darstellungstheorie zerfällt aufgrund des folgenden Satzes in zwei wesentlich verschiedene Zweige.

SATZ 3.1.1. **(Maschke)** *Die Algebra $k[G]$ ist genau dann halbeinfach, wenn die Charakteristik von k die Ordnung von G nicht teilt. Insbesondere ist $k[G]$ in Charakteristik 0 immer halbeinfach.*

Das wichtigste Beispiel für den halbeinfachen Fall sind Darstellungen über den komplexen Zahlen. Hier sind alle Darstellungen direkte Summen einfacher Darstellungen. Die einfachen Darstellungen fallen mit den unzerlegbaren Darstellungen zusammen, sie sind sowohl die einfachen Faktoren als auch die unzerlegbaren Summanden des Gruppenrings selbst. Folglich gibt es nur endlich viele Isomorphieklassen einfacher/unzerlegbarer Darstellungen und alle Darstellungen sind projektiv. Darüber hinaus sind über den komplexen Zahlen alle Darstellungen bis auf Isomorphie durch ihre Charaktere festgelegt. Tatsächlich hat sich in Arbeiten von Frobenius die Theorie komplexer Darstellungen erst aus der Theorie komplexwertiger Charaktere entwickelt.

Ein weiteres Beispiel für die halbeinfache Situation stellt die im vorigen Kapitel schon angesprochene Zerlegung in zentrale isotypische Komponenten dar. Sei G eine endliche Gruppe, deren Zentrum Z eine zur Charakteristik von k teilerfremde Ordnung hat, z.B. $k = \mathbb{F}$, $G = G(\mathfrak{p})$ und $Z = (A/\mathfrak{p})^*/\mathbb{F}_r^*$. Ein $k[G]$-Modul M wird durch Einschränken auf die Untergruppe Z zu einem $k[Z]$-Modul. Obwohl er als $k[G]$-Modul nicht unbedingt halbeinfach sein muß, ist er es aber als $k[Z]$-Modul und zerlegt sich folglich in eine direkte Summe einfacher $k[Z]$-Moduln. Da Z eine abelsche Gruppe ist, sind alle einfachen Darstellungen von Z eindimensional, d.h. gegeben durch einen Gruppenhomomorphismus $\psi : Z \to \mathrm{GL}(1,k) = k^*$. Dies liegt daran, daß im halbeinfachen Fall der Gruppenring das Produkt von Matrizenringen über k ist, welche die Endomorphismenringe der einfachen Moduln sind. Da $k[Z]$ kommutativ ist, können nur 1×1-Matrizen auftauchen und damit auch nur einfache Moduln der Dimension 1. Die zu dem Charakter ψ gehörende isotypische Komponente

$$M(\psi) = \{m \in M \bigm| z \cdot m = \psi(z)m \text{ für alle } z \in Z\}$$

von M ist gerade die Summe aller einfachen $k[Z]$-Untermoduln von M, die als Darstellung isomorph sind zur Darstellung ψ. Die zentralen isotypischen Komponenten sind a priori zwar nur $k[Z]$-Moduln, aber man rechnet direkt nach, daß sie auch unter $k[G]$ abgeschlossen sind. Für $g \in G$, $z \in Z$ und $m \in M(\psi)$ ist nämlich

$$z \cdot g \cdot m = g \cdot z \cdot m = g \cdot \psi(z)m = \psi(z)g \cdot m\,,$$

also $g{\cdot}m \in M(\psi)$. Ist weiter $M \xrightarrow{f} N$ ein $k[G]$-Modul-Homomorphismus, so bildet f die ψ-Komponente von M in die ψ-Komponente von N ab, d.h. es ergibt sich ein $k[G]$-Homomorphismus $M(\psi) \xrightarrow{f(\psi)} N(\psi)$, wobei $f(\psi)$ für die Einschränkung $f_{|M(\psi)}$ steht.

Im Fall einer die Gruppenordnung teilenden Charakteristik treffen die aus der Theorie der halbeinfachen Ringe resultierenden Aussagen nicht mehr zu. Erstmals untersucht wurden solche Phänomene zu Beginn des 20.Jahrhunderts von Dickson. Die Grundlagen für die modulare Darstellungstheorie, welche sich gerade mit dieser Problematik beschäftigt, wurde in **[BrNe1]**,**[BrNe2]** gelegt. Während bei Brauer aber modulare Darstellungen und die zugehörigen modularen oder Brauer-Charaktere eine wesentliche Rolle dabei spielen, Aussagen über komplexwertige Charaktere zu gewinnen und diese für allgemeine gruppentheoretische Untersuchungen zu verwenden, werden wir im folgenden nur die modularen Darstellungen selbst benutzen und sie auch nicht in Verbindung setzen mit komplexen Darstellungen der gleichen Gruppe. Moderne Quellen für Beweise der im folgenden erläuterten grundlegenden Tatsachen der modularen Theorie finden sich z.B. in [**Al**],[**CuRe**],[**PuDi**].

Wir beginnen mit einer kurzen Anmerkung zum Beweis des Satzes von Maschke, welche schon einige der Schwierigkeiten der modularen Theorie veranschaulicht. Eine Möglichkeit, die Halbeinfachheit des Gruppenrings zu beschreiben, besteht darin, daß alle Untermoduln seiner Moduln komplementierbar, d.h. direkte Summanden sein müssen. Als Vektorraum ist ein Untermodul N des $k[G]$-Moduls M natürlich komplementierbar. Sei π eine Vektorraumprojektion von M auf N, so daß

$$M = \pi(M) \oplus \operatorname{Ker}\pi = N \oplus \operatorname{Ker}\pi$$

ist. Um nun π von einem k-Homomorphismus zu einem $k[G]$-Homomorphismus zu modifizieren und dadurch neben N auch $\operatorname{Ker}\pi$ zu einem $k[G]$-Modul zu machen, liegt folgende Definition nahe, welche einer Durchschnittsbildung bzw. einem Glättungsprozeß entspricht:

$$\pi' := \frac{1}{\#G} \sum_{g\in G} g\pi g^{-1} .$$

Diese Definition setzt natürlich voraus, daß die Gruppenordnung in k invertierbar ist, d.h. daß die Charakteristik die Gruppenordnung nicht teilt. Gerade das Verschwinden von gewissen ganzen Zahlen in Körpern positiver Charakteristik und die sich daraus ergebenden Konsequenzen regieren die gesamte modulare Darstellungstheorie.

Wie in der obigen Formulierung der Halbeinfachheit schon zu sehen, spielt im modularen Fall genauso wie im komplexen die Struktur des Gruppenrings für die Darstellungen von G die entscheidende Rolle. Es gibt zwei grundlegende Arten von Bausteinen: zum einen die einfachen Darstellungen, welche gerade die einfachen Faktoren von $k[G]$ als Modul über sich selbst sind; zum anderen die projektiven unzerlegbaren Darstellungen, welche die Summanden in der direkten Summenzerlegung von $k[G]$ als Modul über sich selbst sind. Aufgrund des Zusammenhangs mit dem Gruppenring ist klar, daß es jeweils nur endlich viele Isomorphieklassen von Darstellungen diesen Typs gibt, was z.B. für die Klasse der unzerlegbaren Darstellungen i.a. nicht mehr gilt [**Al**, S. 26]. Obwohl die einfachen und projektiven unzerlegbaren Darstellungen nicht zusammenfallen, so hängen sie doch noch sehr eng miteinander zusammen. Um dies zu formulieren, benötigen wir noch den Begriff des Radikals, welcher zusammen mit dem Begriff des Sockels in Abwesenheit der Halbeinfachheitseigenschaft für die Strukturanalyse von modularen Darstellungen von wesentlicher Bedeutung ist.

Definition 3.1.2.

1. Das Radikal $\operatorname{rad} M$ eines $k[G]$-Moduls M ist der Schnitt aller maximalen Untermoduln von M.
2. Der Sockel $\operatorname{soc} M$ ist die Summe der einfachen Untermoduln von M.

Radikal und Sockel sind in gewisser Hinsicht zueinander duale Begriffe, was man z.B. an folgender alternativer Charakterisierung sieht: der Sockel von M ist der größte halbeinfache Untermodul von M, während das Radikal der kleinste Untermodul ist, so daß der Quotient nach diesem Untermodul halbeinfach ist. Man kann auch sagen, daß $\operatorname{soc} M$ die $\operatorname{rad} k[G]$-Torsion von M ist und $\operatorname{rad} M = (\operatorname{rad} k[G]) \cdot M$. Es gilt nun folgender Satz, der den Zusammenhang zwischen einfachen und projektiven unzerlegbaren Darstellungen sowie der betrachteten Gruppe herstellt.

Satz 3.1.3. *Die Abbildung $P \mapsto P/\operatorname{rad} P$ liefert eine Bijektion zwischen der Menge der Isomorphieklassen projektiver unzerlegbarer $k[G]$-Moduln und der Menge der Isomorphieklassen einfacher $k[G]$-Moduln. Die gemeinsame Kardinalität der beiden genannten Mengen ist die Anzahl der Konjugationsklassen von Elementen von G, deren Ordnung zur Charakteristik von k teilerfremd ist.*

Die Charakterisierung ihrer Anzahl ist ein wesentliches Hilfsmittel bei der Bestimmung aller einfachen $k[G]$-Moduln für eine gegebene Gruppe. Ist dies geschehen, so liefert der Begriff des Sockels bzw. des Radikals eine naheliegende Vorgehensweise bei der Strukturanalyse beliebiger $k[G]$-Moduln.

Definition 3.1.4. Sei M ein $k[G]$-Modul.

1. Für $n \in \mathbb{N}_0$ sei $\operatorname{rad}^n M := (\operatorname{rad} k[G])^n M$.
2. Für $n \in \mathbb{N}_0$ sei $\operatorname{soc}^n M := \{m \in M \,\big|\, (\operatorname{rad} k[G])^n \cdot m = 0\}$.
3. Für $n \in \mathbb{N}$ sei $\operatorname{raq}^n M = \operatorname{rad}^{n-1} M/\operatorname{rad}^n M$.
4. Für $n \in \mathbb{N}$ sei $\operatorname{soq}^n M = \operatorname{soc}^n M/\operatorname{soc}^{n-1} M$.

Diese sogenannten Radikal- bzw. Sockelreihen stellen Filtrierungen endlicher Länge des Moduls dar, welche die besondere Eigenschaft haben, daß der Quotient zweier aufeinander folgender Glieder der Reihe halbeinfach ist. Dabei ist die Radikalreihe eine absteigende und die Sockelreihe eine aufsteigende Filtrierung. Beide Filtrierungen haben die gleiche Länge, d.h. die gleiche Anzahl nicht verschwindender Quotienten $\operatorname{raq}^n M$ bzw. $\operatorname{soq}^n M$. Eine alternative rekursive Beschreibung der Sockelreihe, welche sich für ihre Bestimmung eignet, ist die folgende: $\operatorname{soc}^n M$ ist das Urbild des Sockels von $M/\operatorname{soc}^{n-1} M$ in M. Man bestimmt also schrittweise den Sockel von M, von $M/\operatorname{soc} M$, von $M/\operatorname{soc}^2 M$ und so weiter. Der Sockel von $M/\operatorname{soc}^n M$ ist der n-te Quotient in der Sockelreihe von M und sein Urbild unter der Restklassenabbildung in M ist das $n+1$-te Glied in der Sockelreihe von M. Da ein

$k[G]$-Modul i.a. nicht halbeinfach ist, stellt die Kenntnis der Quotienten der Sockelreihe eine wesentlich exaktere Information über seine Struktur dar als nur die Kenntnis seiner einfachen Faktoren, auch wenn seine Isomorphieklasse dadurch natürlich noch nicht festgelegt ist.

Bevor wir im nächsten Abschnitt beschreiben, wie die Sockelreihe zur Untersuchung von Homomorphismen zwischen $k[G]$-Moduln benutzt werden kann, wollen wir aber zur Veranschaulichung der bisher eingeführten Begriffe das kleinste nichttriviale Beispiel durchrechnen.

Beispiel 3.1.5. Sei p eine Primzahl und $\mathbb{F}_p$ der Körper mit p Elementen sowie k sein algebraischer Abschluß. Die betrachtete Gruppe G sei die zyklische Gruppe mit p Elementen, dargestellt durch die $\mathbb{F}_p$ zugrundeliegende additive Gruppe. Als p-Gruppe hat G nur eine Konjugationsklasse von Elementen p-freier Ordnug, also nur eine Isomorphieklasse einfacher Moduln. Dies muß also die für jede Gruppe existierende einfache Darstellung, die sogenannte triviale Darstellung sein. Diese ist eindimensional und jedes Gruppenelement operiert als Identität. Wir betrachten nun eine zweidimensionale Darstellung auf dem Vektorraum V der Spaltenvektoren der Länge 2, gegeben durch

$$G \to \mathrm{GL}(V);\ g \mapsto \begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}.$$

Diese Darstellung ist nicht halbeinfach, da sie sonst ja direkte Summe zweier Kopien der trivialen Darstellung sein müßte und jedes Gruppenelement trivial operieren würde. Das ist offensichtlich nicht der Fall. Aus Dimensionsgründen und da es nur eine einfache Darstellung gibt, muß der Sockel also isomorph zur trivialen Darstellung sein und $\operatorname{soc}^2 V$ ist schon ganz V. Die in der Sockelreihe auftretenden Quotienten $\operatorname{soc} V$ und $\operatorname{soc}^2 V/\operatorname{soc}^1 V = V/\operatorname{soc} V$ sind beide sogar einfach und isomorph zur trivialen Darstellung von G. Dieses aus allgemeinen Gründen gefundene Ergebnis läßt sich auch konkret nachrechnen. Da die triviale Darstellung die einzige einfache Darstellung ist, besteht jeder einfache Modul aus einem Untervektorraum, der von einem von Null verschiedenen, G-invarianten Vektor erzeugt wird. Der Vektor $\binom{1}{0}$ ist offensichtlich G-invariant, also ist der Sockel von V gleich $U := \left\{\binom{x}{0} \,\middle|\, x \in k\right\}$. Außerdem sieht man, daß V/U als Vektorraum von $\binom{0}{1} \bmod U$ erzeugt wird und dies ist ein G-invariantes Element von V/U wegen

$$\begin{pmatrix} 1 & g \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} \bmod U = \begin{pmatrix} g \\ 1 \end{pmatrix} \bmod U = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \bmod U\,.$$

Damit ist die Sockelreihe mitsamt ihrer Quotienten explizit bestimmt.

3.2. Filtrierte Moduln

In diesem Abschnitt beschreiben wir eine Methode zur Untersuchung von Kern und Kokern von Morphismen, welche nur Informationen über die beteiligten Moduln benutzt und nicht von dem Morphismus zwischen den Moduln abhängt. Wir beschränken uns dabei auf die im vorigen Abschnitt beschriebene Situation von endlichdimensionalen Moduln über einem Gruppenring $k[G]$ mit endlicher Gruppe G und algebraisch abgeschlossenem Körper k, obwohl alle Resultate bei geeigneter Formulierung auch in allgemeineren Situationen gelten.

Das einfachste und grundlegendste Beispiel für obige Idee ist das Lemma von Schur.

LEMMA 3.2.1. **(Schur)** *Seien M und N einfache $k[G]$-Moduln. Sind M und N isomorph, so gilt $\mathrm{Hom}_{k[G]}(M,N) \cong k$. Sind M und N nicht isomorph, so gilt $\mathrm{Hom}_{k[G]}(M,N) = 0$.*

Sind also M und N nichtisomorphe einfache $k[G]$-Moduln, so ist für jeden Homomorphismus von M nach N der Kern isomorph zu M und der Kokern isomorph zu N. Im Fall isomorpher einfacher Moduln kommt noch die Möglichkeit hinzu, daß Kern und Kokern gleich Null sind. Dieses einfache Beispiel zeigt, daß aus Struktureigenschaften von Moduln Aussagen über Kerne und Kokerne beliebiger Morphismen zwischem den betrachteten Moduln folgen können. Wir führen folgende nützliche Bezeichnungsweise ein.

DEFINITION 3.2.2. Sei S ein einfacher $k[G]$-Modul. Für einen beliebigen $k[G]$-Modul M sei $v_S(M)$ die Anzahl der zu S isomorphen einfachen Faktoren von M, d.h. die Anzahl der zu S isomorphen Quotienten in einer Jordan-Hölder-Reihe von M.

Die obige Schlußfolgerung aus dem Lemma von Schur läßt sich nun folgendermaßen verallgemeinern.

LEMMA 3.2.3. *Sei $f : M \to N$ ein Homomorphismus von $k[G]$-Moduln. Dann gilt $v_S(\mathrm{Ker}\, f) - v_S(M) + v_S(N) - v_S(\mathrm{Koker}\, f) = 0$ für jeden einfachen $k[G]$-Modul S.*

BEWEIS. Sei

$$0 \to A \to B \to C \to 0$$

eine kurze exakte Folge von $k[G]$-Moduln, d.h. $C \cong B/A$. Eine Jordan-Hölder-Reihe von A läßt sich zu einer Jordan-Hölder-Reihe von B fortsetzen, folglich ist

$$v_S(C) = v_S(B/A) = v_S(B) - v_S(A)\,.$$

Die Aussage über die exakte Folge

$$0 \to \mathrm{Ker}\, f \to M \to N \to \mathrm{Koker}\, f \to 0$$

erhält man daraus durch Zerlegen in die beiden kurzen exakten Folgen

$$0 \to \operatorname{Ker} f \to M \to f(M) \to 0$$

und

$$0 \to f(M) \to N \to \operatorname{Koker} f \to 0\,.$$

$\square$

Löst man die Gleichung des Lemmas nach $v_S(\operatorname{Ker} f)$ auf, so erhält man

$v_S(\operatorname{Ker} f) = v_S(M) - v_S(N) + v_S(\operatorname{Koker} f) \geqslant \max\{0, v_S(M) - v_S(N)\}\,,$

d.h. falls M mehr S-Faktoren besitzt als N, so müssen die überzähligen Faktoren im Kern auftauchen. Eine entsprechende Aussage erhält man für den Kokern. Besitzt N mehr Faktoren S als M, so müssen entsprechend viele Faktoren S im Kokern sein.

Befindet man sich nun in der Situation, daß M und N halbeinfach sind, so ist diese Abschätzung optimal, d.h. es gibt einen Homomorphismus $f : M \to N$ mit

$$v_S(\operatorname{Ker} f) = \max\{0, v_S(M) - v_S(N)\}$$

und mit

$$v_S(\operatorname{Koker} f) = \max\{0, v_S(N) - v_S(M)\}\,.$$

Sei z.B. $M = S^m \oplus M'$ und $N = S^n \oplus N'$, wobei M' und N' keine zu S isomorphe Faktoren besitzen. Ist $m \geqslant n$, so definiere die Abbildung

$$f : M = S^n \oplus S^{m-n} \oplus M' \to N = S^n \oplus N'$$

auf der S^n-Komponente von M als Identität in die S^n-Komponente von N und als 0 sonst. Dann ist der Kern gerade $S^{m-n} \oplus M'$ und enthält genau $m - n$ Faktoren S, während das Bild gleich S^n und der Kokern damit isomorph zu N' ist, also keine S-Faktoren enthält. Eine ähnliche Konstruktion im Fall $m \leqslant n$ liefert einen Kokern mit genau $n - m$ Faktoren vom Typ S und einen Kern ohne S-Faktoren.

Da die Struktur eines halbeinfachen Moduls sich schon aus seinen einfachen Faktoren ergibt, kann man also ohne Kenntnis des Homomorphismus keine weiteren Aussagen über Kern und Kokern machen als die, welche sich nur aus den Jordan-Hölder-Faktoren ergeben. Im Falle nicht halbeinfacher Moduln stimmt dies nicht mehr. Hier kann es vorkommen, daß zwischen zwei Moduln kein injektiver oder surjektiver Homomorphismus existiert, obwohl die Moduln genau dieselben einfachen Faktoren haben.

Beispiel 3.2.4. Wir setzen das Beispiel aus dem vorigen Abschnitt fort, d.h. G ist die additive Gruppe $\mathbb{F}_p$ und k der algebraische Abschluß von $\mathbb{F}_p$. Der $k[G]$-Modul V sei definiert als der Vektorraum der Spaltenvektoren der Länge 2 mit der Gruppenoperation

$$g \cdot \begin{pmatrix} x \\ y \end{pmatrix} := \begin{pmatrix} x + gy \\ y \end{pmatrix} \text{ für } g \in G.$$

Weiter betrachten wir k auch als den trivialen $k[G]$-Modul und k^2 als die direkte Summe zweier trivialer $k[G]$-Moduln. Da es nur einen einzigen einfachen $k[G]$-Modul gibt, nämlich den trivialen, haben zwei $k[G]$-Moduln genau dann dieselben Jordan-Hölder-Faktoren, wenn sie dieselbe Dimension haben. Insbesondere haben also k^2 und V dieselben einfachen Faktoren. Trotzdem gibt es keinen $k[G]$-Homomorphismus f von k^2 nach V, für den

$$v_k(\operatorname{Ker} f) = \max\{0, v_k(k^2) - v_k(V)\} = 0$$

oder

$$v_k(\operatorname{Koker} f) = \max\{0, v_k(V) - v_k(k^2)\} = 0$$

gilt, da ein solcher dann aus Dimensionsgründen ein Isomorphismus sein müßte. Wir haben aber schon gesehen, daß V im Gegensatz zu k^2 nicht halbeinfach ist, also ist V auch nicht isomorph zu k^2. Der Grund für dieses Phänomen liegt darin, daß die beiden Moduln unterschiedliche Sockel haben. Während k^2 halbeinfach und somit der Sockel mit dem Modul identisch ist, hat V einen einfachen Sockel. Da nun homomorphe Bilder einfacher Moduln verschwinden oder einfach sind, bildet ein Morphismus den Sockel des Ausgangsmoduls in den Sockel des Zielmoduls ab. Da in unserem Fall der Sockel des Ausgangsmoduls größer ist als der des Zielmoduls, muß es einen von Null verschiedenen Kern geben.

Wir werden nun die dem Beispiel zugrunde liegende Idee formalisieren.

Definition 3.2.5.

1. Ein (aufsteigend) filtrierter $k[G]$-Modul ist ein $k[G]$-Modul M mit einer Folge von Untermoduln $(M_i)_{i\in\mathbb{N}}$, so daß $M_i \subseteq M_{i+1}$ ist für alle $i \in \mathbb{N}$. Außerdem sei immer $M_0 = 0$ vereinbart.
2. Ein Morphismus filtrierter $k[G]$-Moduln $(M, (M_i)_{i\in\mathbb{N}}), (N, (N_i)_{i\in\mathbb{N}})$ ist ein $k[G]$-Homomorphismus $f : M \to N$ mit $f(M_i) \subseteq N_i$ für alle $i \in \mathbb{N}$.

In Abschnitt 3.2 haben wir bereits eine aufsteigende Filtrierung kennengelernt, die man für jeden Modul bilden kann, nämlich die Sockelreihe. Diese Filtrierung ist auch mit jedem $k[G]$-Homomorphismus verträglich.

Lemma 3.2.6. *Sei $f : M \to N$ ein Morphismus von $k[G]$-Moduln. Dann gilt $f(\operatorname{soc}^i M) \subseteq \operatorname{soc}^i N$ für alle $i \in \mathbb{N}$.*

Beweis. Die Elemente von $\operatorname{soc}^i M$ sind gerade die $\operatorname{rad}^i k[G]$-Torsion von M. Da unter einem $k[G]$-Homomorphismus eine Torsionseigenschaft erhalten bleibt, folgt die Aussage. □

Wir können also alle vorkommenden $k[G]$-Moduln und -Morphismen als filtrierte Moduln und Morphismen filtrierter Moduln bzgl. der fest gewählten Sockel-Filtrierung ansehen. Für filtrierte Moduln und ihre Morphismen gelten nun stärkere Aussagen also in der allgemeinen Situation. Für uns wesentlich ist die folgende.

PROPOSITION 3.2.7. *Sei $f : (M, (M_i)_{i\in\mathbb{N}}) \to (N, (N_i)_{i\in\mathbb{N}})$ Morphismus filtrierter $k[G]$-Moduln. Weiter sei $P_i = M_i/M_{i-1}$ und $Q_i = N_i/N_{i-1}$ für alle $i \in \mathbb{N}$. Für einen einfachen $k[G]$-Modul S gelten:*

1. $v_S(\operatorname{Ker} f) \geqslant \sum\limits_{i\in\mathbb{N}} \max\{0, v_S(P_i) - v_S(Q_i)\}$,
2. $v_S(\operatorname{Koker} f) \geqslant \sum\limits_{i\in\mathbb{N}} \max\{0, v_S(Q_i) - v_S(P_i)\}$.

BEWEIS. Wir betrachten das folgende Diagramm:

$$\begin{array}{ccccccc}
 & & & 0 & & & \\
 & & & \downarrow & & & \\
 & & & \operatorname{Ker} f_i\ (\vartheta_i) & & & \\
 & & & \downarrow & & & \\
0 \to & M_i/M_{i-1}\ (\alpha_i) & \to & M/M_{i-1}\ (\beta_i) & \to & M/M_i\ (\gamma_i) & \to 0 \\
 & & & \downarrow f_i & & & \\
0 \to & N_i/N_{i-1}\ (\delta_i) & \to & N/N_{i-1}\ (\varepsilon_i) & \to & N/N_i\ (\varphi_i) & \to 0 \\
 & & & \downarrow & & & \\
 & & & \operatorname{Koker} f_i\ (\sigma_i) & & & \\
 & & & \downarrow & & & \\
 & & & 0 & & &
\end{array}$$

Die dabei nicht angegebenen Abbildungen sind die kanonischen Einbettungen oder Projektionen und die Abbildung f_i ist die von f induzierte. Sie ist wohldefiniert, da $f(M_{i-1}) \subseteq N_{i-1}$ ist. Die beiden Zeilen des Diagramms sowie die Spalte sind exakt. Die in Klammern stehenden Zahlen $\alpha_i, \ldots, \sigma_i$ seien die Anzahlen der zu S isomorphen Jordan-Hölder-Faktoren der Moduln, neben denen sie stehen. Da die Filtrierungen aufsteigend sind, gilt $\vartheta_i \geqslant \vartheta_{i+1}$ und $\sigma_i \geqslant \sigma_{i+1}$. Direkt aus den Definitionen ergeben sich $\alpha_i = \beta_i - \beta_{i+1}$ und $\delta_i = \varepsilon_i - \varepsilon_{i+1}$. Aus Lemma 3.2.3 folgen $\vartheta_i - \beta_i = \sigma_i - \varepsilon_i$ und $\vartheta_{i+1} - \beta_{i+1} = \sigma_{i+1} - \varepsilon_{i+1}$. Setzt man dies zusammen, so ergibt sich zum einen

$$\vartheta_i - \beta_i + \varepsilon_i = \sigma_i \geqslant \sigma_{i+1} = \vartheta_{i+1} - \beta_{i+1} + \varepsilon_{i+1}$$

und daraus

$$\vartheta_i \geqslant \vartheta_{i+1} + \alpha_i - \delta_i$$

sowie zum anderen

$$\beta_i - \varepsilon_i + \sigma_i = \vartheta_i \geqslant \vartheta_{i+1} = \beta_{i+1} - \varepsilon_{i+1} + \sigma_{i+1}$$

und daraus

$$\sigma_i \geqslant \sigma_{i+1} + \delta_i - \alpha_i$$

Aus den Formeln

$$\vartheta_i \geqslant \max\{\vartheta_{i+1}, \vartheta_{i+1} + \alpha_i - \delta_i\}$$

und

$$\sigma_i \geqslant \max\{\sigma_{i+1}, \sigma_{i+1} + \delta_i - \alpha_i\}$$

folgen durch wiederholtes Einsetzen ineinander die Formeln

$$\vartheta_1 \geqslant \sum_{i \in \mathbb{N}} \max\{0, \alpha_i - \delta_i\}$$

und

$$\sigma_1 \geqslant \sum_{i \in \mathbb{N}} \max\{0, \delta_i - \alpha_i\}\,.$$

Dies sind genau die zu beweisenden Formeln. □

Die Proposition besagt also, daß nicht nur solche einfache Moduln im Kern vorkommen müssen, die in dem Ausgangsmodul häufiger vorkommen als im Zielmodul, sondern daß man diesen Vergleich unabhängig auf jeder Quotientenstufe der Filtrierung durchführen kann. Entsprechendes gilt auch für den Kokern.

Beispiel 3.2.8. Betrachten wir wieder unser Beispiel. Für V war der erste Quotient isomorph zu k und der zweite auch. Für k^2 war der erste Quotient isomorph zu k^2 und der zweite war Null. Nach unserer Proposition muß also der Kern jedes $k[G]$-Modul-Homomorphismus von k^2 nach V mindestens $\max\{0, 1-2\} + \max\{0, 1-0\} = 1$ einfache Faktoren vom Typ k haben und der Kokern muß mindestens $\max\{0, 2-1\} + \max\{0, 0-1\} = 1$ einfache Faktoren vom Typ k haben. Obwohl die Proposition eine feinere Analyse erlaubt als nur die Betrachtung der einfachen Faktoren selbst, ist sie natürlich auch nicht optimal. So ist z.B. die Isomorphieklasse eines $k[G]$-Moduls i.a. nicht durch die Quotienten seiner Sockelreihe festgelegt. Betrachten wir z.B. die additive Gruppe $G = \mathbb{F}_p \times \mathbb{F}_p$ und die beiden zweidimensionalen Darstellungen

$$G \to \mathrm{GL}(2, k);\ (a, b) \mapsto \begin{pmatrix} 1 & a+b \\ 0 & 1 \end{pmatrix}$$

und

$$G \to \mathrm{GL}(2, k);\ (a, b) \mapsto \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}.$$

Da G wieder eine p-Gruppe ist, hat sie nur eine einfache Darstellung, nämlich die eindimensionale triviale Darstellung. Der Sockel eines $k[G]$-Moduls läßt sich also wieder bestimmen, indem man nach Vektoren sucht, die unter der ganzen Gruppe fix sind. Bei beiden Darstellungen stellt man direkt fest, daß der Unterraum der von G fixierten Vektoren im Darstellungsraum k^2 gerade $U = \{\binom{x}{0}\}$ ist und die Dimension 1 hat. Damit hat die Sockelreihe in beiden Fällen die Länge 2 und die beiden Quotienten sind isomorph zu trivialen Darstellung. Trotzdem sind die beiden Darstellungen offensichtlich nicht isomorph, bei der ersten z.B. operieren alle Gruppenelemente der Form $(a,-a)$ trivial, bei der zweiten nicht. Jeder Homomorphismus zwischen diesen beiden Darstellungen hat also einen nichtverschwindenden Kern und Kokern, der sich aufgrund der Gleichheit der Quotienten der Sockelreihe mit unserer Proposition nicht vorhersagen läßt. Daß die Methode trotzdem effektiv zu sein verspricht, sieht man z.B. daran, daß das gerade angegebene Negativbeispiel nicht die zyklische Gruppe mit p Elementen verwendet. Für diese Gruppe werden die unzerlegbaren Darstellungen nämlich gerade gegeben durch Vektorräume der Dimension 1 bis p, auf denen der Erzeuger der Gruppe durch den Jordan-Block

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

operiert [**A1**, S. 24]. Die Sockelreihe einer solchen unzerlegbaren Darstellung hat nur einfache Quotienten und ihre Anzahl legt die Dimension und damit die Isomorphieklasse der unzerlegbaren Darstellung fest. Damit ist auch die Isomorphieklasse einer nicht notwendig unzerlegbaren Darstellung der Gruppe mit p Elementen durch die Quotienten ihrer Sockelreihe bereits festgelegt.

Wir spezialisieren nun auf den Fall, daß die Filtrierung der zu vergleichenden Moduln durch die Sockelreihe gegeben ist. Um Proposition 3.2.7 anzuwenden, muß man die Vielfachheit des einfachen Moduls S in den Quotienten $\mathrm{soq}^n M$ und $\mathrm{soq}^n N$ kennen oder zumindest nach oben bzw. nach unten abschätzen können. Wir beschreiben nun eine Möglichkeit, dies zu tun.

Wir nehmen an, daß uns eine kurze exakte Folge

$$0 \to M' \to M \to M'' \to 0$$

von $k[G]$-Moduln vorliegt und wir versuchen, aus Informationen über die Sockelreihen von M', M'' auf die Sockelreihe von M zurückzuschließen. Bei dem Untermodul ist das einfach.

LEMMA 3.2.9. *Ist M' ein Untermodul eines $k[G]$-Moduls M, so gibt es eine $k[G]$-Modul-Einbettung* $\mathrm{soq}^n M' \hookrightarrow \mathrm{soq}^n M$.

BEWEIS. Es gilt $\mathrm{soq}^n M = \mathrm{soc}^n M/\mathrm{soc}^{n-1} M$ und auch $\mathrm{soq}^n M' = \mathrm{soc}^n M'/\mathrm{soc}^{n-1} M'$. Da der n-te Untermodul in der Sockelreihe eines Moduls gerade die $(\mathrm{rad}\, k[G])^n$-Torsion ist, gilt $\mathrm{soc}^n M' = M' \cap \mathrm{soc}^n M \subseteq \mathrm{soc}^n M$. Dies liefert eine kanonische injektive Abbildung von $\mathrm{soq}^n M'$ nach $\mathrm{soq}^n M$. $\square$

Die Beziehung zwischen der Sockelreihe von M'' und M ist komplizierter. Da wir jeweils immer nur das Vorkommen eines einfachen Moduls S untersuchen, ist folgender Begriff nützlich.

Definition 3.2.10. Sei M ein $k[G]$-Modul und S ein einfacher $k[G]$-Modul. Ist S isomorph zu einem Faktor von $\operatorname{soq}^n M$, so nennen wir n (Sockel-)Höhe von S in M.

Natürlich kann ein einfacher Modul S auf verschiedenen Höhen von M vorkommen und auch auf einer Höhe mehrfach.

Lemma 3.2.11. *Sei M ein $k[G]$-Modul mit Untermodul M'. Kommt ein einfacher $k[G]$-Modul S in $M'' = M/M'$ auf Höhe n vor, so kommt S in M auf einer Höhe $m \geqslant n$ vor.*

Beweis. Wenn S in M' auf Höhe n vorkommt, so gibt es einen Untermodul U'' von M'' mit $\operatorname{soc}^{n-1} U'' \subseteq U'' \subseteq \operatorname{soc}^n M''$ und $U''/\operatorname{soc}^{n-1} U'' \cong S$. Sei $U'' = U/M'$ für einen Untermodul $U \subseteq M$. Dann ist $\operatorname{soc}^{n-1} U'' = V/M'$ für $V = \{x \in U \mid (\operatorname{rad} k[G])^{n-1} \cdot x \subseteq M'\}$. Es gilt also insbesondere $\operatorname{soc}^{n-1} U \subseteq V$ und man erhält eine Surjektion $S \cong U''/\operatorname{soc}^{n-1} U'' = U/V \twoheadleftarrow U/\operatorname{soc}^{n-1} U$. Dies bedeutet aber, daß in U und folglich auch in M der einfache Modul S auf einer Höhe vorkommt, die mindestens n beträgt. $\square$

Obwohl diese Aussage über den Zusammenhang zwischen der Höhe in einem Modul und der Höhe in einem Quotienten des Moduls weniger Information über die Sockelreihe des Moduls liefert, als sich mit Lemma 3.2.9 aus einem Untermodul ableiten läßt, ist sie dennoch sehr nützlich, wie in den Beispielen in Kapitel 4 zu sehen sein wird.

3.3. Dualisieren

Wie bei Vektorräumen über Körpern kann man auch bei $k[G]$-Moduln Duale bilden. Ist M ein $k[G]$-Modul, so ist das Dual M^* der Vektorraum $\operatorname{Hom}_k(M, k)$ versehen mit der G-Operation

$$(g \cdot f)(m) = f(g^{-1} m)$$

für $g \in G$, $f \in M^*$ und $m \in M$. Bezüglich Unter- und Quotientenstrukturen verhält sich das Dualisieren bei $k[G]$-Moduln so wie bei Vektorräumen. Ist N ein Untermodul von M, so besitzt M^* einen zu $(M/N)^*$ isomorphen Untermodul, nämlich gerade den Untermodul der Funktionen in M^*, die auf N verschwinden. Der Quotient $M^*/(M/N)^*$ ist isomorph zu N^*. Da wir $k[G]$-Moduln endlicher k-Dimension betrachten, gibt es auch einen kanonischen Isomorphismus $M \cong (M^*)^*$, während M^* im allgemeinen nicht isomorph zu M ist. Ist nun eine Filtrierung

$$0 \underset{M_1}{\subseteq} M_1 \underset{M_2/M_1}{\subseteq} M_2 \subseteq \ldots \subseteq M_{n-1} \underset{M_n/M_{n-1}}{\subseteq} M_n = M$$

von M mit den jeweiligen Quotienten gegeben, so liefert Dualisieren eine Filtrierung

$$0 \underset{(M_n/M_{n-1})^*}{\subseteq} (M/M_{n-1})^* \subseteq (M/M_{n-2})^* \subseteq \ldots \subseteq (M/M_2)^* \underset{(M_2/M_1)^*}{\subseteq} (M/M_1)^* \underset{M_1^*}{\subseteq} M^*$$

von M^*. Als Quotienten tauchen also die Duale der ursprünglichen Quotienten auf, und zwar in umgekehrter Reihenfolge. Wählt man als Filtrierung eine Jordan-Hölder-Reihe, so ergibt sich, daß die einfachen Faktoren von M^* gerade die Duale der einfachen Faktoren von M sind.

Wie wir schon im vorigen Abschnitt erwähnt haben, sind Sockel und Radikal dual zueinander, und dies setzt sich auf die gesamte Sockel- bzw. Radikalreihe fort. Dualisieren von

$$0 \underset{\mathrm{soq}^1 M}{\subseteq} \mathrm{soc}^1 M \underset{\mathrm{soq}^2 M}{\subseteq} \mathrm{soc}^2 M \subseteq \ldots \subseteq \mathrm{soc}^{n-1} M \underset{\mathrm{soq}^n M}{\subseteq} \mathrm{soc}^n M = M$$

liefert

$$0 \underset{\mathrm{raq}^n M^*}{\subseteq} \mathrm{rad}^{n-1} M^* \underset{\mathrm{raq}^{n-1} M^*}{\subseteq} \mathrm{rad}^{n-2} M^* \subseteq \ldots \subseteq \mathrm{rad}^1 M^* \underset{\mathrm{raq}^1 M^*}{\subseteq} M^* ,$$

d.h. es gilt

$$\mathrm{rad}^i(M^*) = (M/\mathrm{soc}^i M)^*$$

und

$$\mathrm{raq}^i M^* \cong (\mathrm{soq}^i M)^* .$$

Da wir später eigentlich mit der Sockelreihe arbeiten wollen, beim Dualisieren aber die Radikalreihe auftaucht, stellt sich die Frage nach dem Zusammenhang zwischen den beiden Reihen. Wir betrachten zunächst den einfachsten Fall.

Definition 3.3.1. Ein $k[G]$-Modul heißt uniseriell, wenn er genau eine Jordan-Hölder-Reihe besitzt.

Es ist unmittelbar klar, daß ein $k[G]$-Modul M genau dann uniseriell ist, wenn die Quotienten seiner Sockelreihe alle einfach sind, da dann $\mathrm{soc}^i M$ der einzige minimale echte Obermodul von $\mathrm{soc}^{i-1} M$ ist. In diesem Fall stimmen die Sockel- und Radikalreihe überein, d.h. es gilt $\mathrm{soc}^i M = \mathrm{rad}^{n-i+1} M$ und $\mathrm{raq}^i M = \mathrm{soq}^{n-i+1} M$, falls n die Länge von M ist.

Für einen uniseriellen Modul M der Länge n erhält man die Sockelreihe des Duals M^* also durch

$$\mathrm{soc}^i(M^*) \cong \mathrm{rad}^{n-i+1}(M^*) \cong (M/\mathrm{soc}^{n-i+1} M)^*$$

mit den Quotienten

$$\mathrm{soq}^i(M^*) \cong (\mathrm{soq}^{n-i+1} M)^* .$$

Aber auch bei nicht notwendig uniseriellen Moduln gibt es einen, wenn auch schwächeren Zusammenhang zwischen Sockel- und Radikalreihe.

Lemma 3.3.2. *Sei M ein $k[G]$-Modul, dessen Sockelreihe die Länge n besitzt. Dann gilt $\mathrm{rad}^i M \subseteq \mathrm{soc}^{n-i} M$ für alle $0 \leqslant i \leqslant n$.*

BEWEIS. Wir müssen $(\operatorname{rad} k[G])^{n-i} \cdot \operatorname{rad}^i M = 0$ zeigen. Nun ist $\operatorname{rad}^i M = (\operatorname{rad} k[G])^i \cdot M$, also $(\operatorname{rad} k[G])^{n-i} \cdot \operatorname{rad}^i M = (\operatorname{rad} k[G])^n \cdot M = \operatorname{rad}^n M$ und da die Sockel- bzw. Radikalreihe von M die Länge n hat, ist $\operatorname{rad}^n M = 0$. □

Damit ergibt sich eine Abschätzung der Höhe in der Sockelreihe des Duals eines Moduls.

LEMMA 3.3.3. *Sei M ein $k[G]$-Modul mit Sockelreihenlänge n und S ein einfacher $k[G]$-Modul, der in M auf Höhe i vorkommt. Dann kommt S^* in M^* auf einer Höhe $\leqslant n - i + 1$ vor.*

BEWEIS. Ist S ein einfacher Faktor von $\operatorname{soq}^i M$, so ist S^* ein einfacher Faktor von $(\operatorname{soq}^i M)^* = \operatorname{raq}^i M^* = \operatorname{rad}^{i-1} M^* / \operatorname{rad}^i M^*$. Also ist $v_S(\operatorname{rad}^{i-1} M^*) > 0$ und wegen des vorigen Lemmas auch $v_S(\operatorname{soc}^{n-i+1} M^*) > 0$. Dies bedeutet, daß S in der Sockelreihe von M^* auf einer Höhe $\leqslant n - i + 1$ vorkommt. □

3.4. Einfache Darstellungen von GL($2,\mathbb{F}_q$) und SL($2,\mathbb{F}_q$)

Die im vorigen Abschnitt verwendeten Beispiele waren sehr leicht zu berechnen, da nur p-Gruppen vorkamen, welche nur eine einfache Darstellung besitzen, nämlich die triviale. Im allgemeinen ist die Bestimmung aller einfachen Darstellungen einer Gruppe für sich allein betrachtet bereits ein schwieriges Problem, dessen Lösung aber eine notwendige Voraussetzung bei der Bestimmung der Sockelreihe einer Darstellung mitsamt ihrer Quotienten ist.

Durch die Einschränkung unserer Betrachtungen auf die Gruppen GL($2,\mathbb{F}_q$) und SL($2,\mathbb{F}_q$) treten eine Vielzahl zusätzlicher spezieller Aspekte gegenüber der bisher betrachteten allgemeinen Theorie auf. Viele davon gelten sogar in ähnlicher Weise für alle Gruppen vom Typ GL und SL, d.h. im Rahmen linearer algebraischer Gruppen, Lie-Gruppen oder eben für endliche Gruppen, es existieren sogar gewisse Analogien zwischen den modularen und komplexen Darstellungen dieser Gruppen. Ein wesentliches Motiv dabei ist der enge Zusammenhang den Gruppen vom Typ GL, SL mit den Lie-Algebren $\mathfrak{gl}$ und $\mathfrak{sl}$. Da die Theorie der Lie-Algebren als Orientierung dienen kann für die meist schwierigere Theorie der entsprechenden Gruppen, folgt nun eine kurze Skizze derjenigen Gesichtspunkte, die in unserem Zusammenhang eine Rolle spielen. Auf eine ausführliche Darstellung der Grundlagen von Lie-Algebren verzichten wir allerdings, da diese im weiteren nicht wesentlich benutzt wird und wir auch nur am einfachsten Fall, nämlich dem von SL(2) bzw. $\mathfrak{sl}(2)$ interessiert sind. Grundlagen zur Theorie der Lie-Algebren findet man z. B. in [**Hu**], die für uns relevanten Zusammenhänge zwischen den Algebren und den Gruppen werden ausführlicher in [**Bo**],[**Ca**] beschrieben.

Während man üblicherweise meist von der Lie-Gruppe zu der als Tangentialraum im Neutralelement definierten Lie-Algebra übergeht, starten wir mit einer komplexen einfachen Lie-Algebra L. Diese ist mit der adjungierten Darstellung versehen, d.h. L operiert auf sich selbst vermöge der Lie-Klammer. Für eine Wurzel α von L und ein Element x_α aus dem zugehörigen Wurzelraum ist $\exp(\mathrm{ad}(t \cdot x_\alpha))$ ein wohldefinierter Automorphismus von L für jedes $t \in \mathbb{C}$. Die von all diesen Elementen erzeugte Untergruppe der Automorphismengruppe von L ist die zu L gehörende Lie-Gruppe. Um nun einen Übergang zu anderen Koeffizientenbereichen zu ermöglichen, muß man erkennen, daß L schon über $\mathbb{Z}$ definiert ist. Dies geschieht, indem man eine sogenannte Chevalley-Basis von L angibt, welche die Eigenschaft hat, daß alle Strukturkoeffizienten der Lie-Klammer bzgl. dieser Basis ganzzahlig sind. Das von der Chevalley-Basis in L erzeugte Gitter $L_\mathbb{Z}$ hat dann die Struktur einer Lie-Algebra über $\mathbb{Z}$. Für einen beliebigen Körper K definiert man dann $L_K := L_\mathbb{Z} \otimes_\mathbb{Z} K$. Der K-Vektorraum L_K erbt nicht nur die Struktur als Lie-Algebra, sondern es läßt sich auch das Exponential eines Elements aus L_K als Operator auf L_K definieren. Das Erzeugnis der auf diese Weise erhaltenen Automorphismen von L_K ist von der Wahl der Chevalley-Basis unabhängig und wird als die Chevalley-Gruppe von L über K bezüglich der adjungierten Darstellung bezeichnet. Analog erhält man Chevalley-Gruppen für beliebige Darstellungen von L an Stelle der adjungierten Darstellung. Auf diese Weise erhält man dann also aus Darstellungen der komplexen Lie-Algebra L Darstellungen der Chevalley-Gruppe über beliebigen Körpern. Für die Lie-Algebra $\mathfrak{sl}(2, \mathbb{C})$ mit der adjungierten Darstellung und $K = \mathbb{F}_q$ erhält man z.B. als Chevalley-Gruppe $\mathrm{PSL}(2, \mathbb{F}_q)$, für die natürliche Darstellung $\mathfrak{sl}(2, \mathbb{C}) \hookrightarrow \mathfrak{gl}(2, \mathbb{C})$ und $K = \mathbb{F}_q$ erhält man die Gruppe $\mathrm{SL}(2, \mathbb{F}_q)$.

Eine Anwendung dieser Konstruktion ist der Tensorprodukt-Satz von Steinberg, der irreduzible Darstellungen von Chevalley-Gruppen mittels Darstellungen von Lie-Algebren klassifiziert **[St1]**,**[St2]**. Ein Spezialfall dieses Satzes liefert beispielsweise die einfachen Darstellungen der Gruppe $\mathrm{SL}(2, \mathbb{F}_q)$ in definierender Charakteristik. Zuerst bestimmt wurden die einfachen modularen Darstellungen von $\mathrm{SL}(2, \mathbb{F}_q)$ und $\mathrm{GL}(2, \mathbb{F}_q)$ allerdings schon in dem Artikel **[BrNe2]**, dem wir auch bei unserer Beschreibung folgen.

Die spezielle und die allgemeine lineare Gruppe über einem beliebigen Körper sind als Matrixgruppen mit einer natürlichen Darstellung versehen, nämlich der Operation auf Spaltenvektoren der entsprechenden Dimension durch die übliche Matrixmultiplikation. Im Fall der von uns betrachteten Gruppen $\mathrm{SL}(2, \mathbb{F}_q)$ und $\mathrm{GL}(2, \mathbb{F}_q)$ werden alle einfachen Darstellungen aus diesem Grundbaustein konstruiert.

Definition 3.4.1. Sei $\mathbb{F}$ der algebraische Abschluß von $\mathbb{F}_q$ und $F : \mathbb{F} \to \mathbb{F}$; $x \mapsto x^p$ der absolute Frobenius-Automorphismus. Der

Gruppen-Homomorphismus

$$\mathrm{GL}(2,\mathbb{F}_q) \to \mathrm{GL}(2,\mathbb{F}_q);\ \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \begin{pmatrix} F(a) & F(c) \\ F(b) & F(d) \end{pmatrix}$$

sei ebenfalls mit F bezeichnet.

1. Der Vektorraum $V = \mathbb{F}^2$ der Spaltenvektoren der Länge 2 über $\mathbb{F}$, auf dem $\mathrm{SL}(2,\mathbb{F}_q)$ und $\mathrm{GL}(2,\mathbb{F}_q)$ durch Multiplikation von links operieren, heißt natürliche Darstellung von $\mathrm{SL}(2,\mathbb{F}_q)$ bzw. $\mathrm{GL}(2,\mathbb{F}_q)$. Wir bezeichnen die Standardbasis von V mit $X := \binom{1}{0}$ und $Y := \binom{0}{1}$.
2. Für $k \in \mathbb{N}_0$ sei Sym_k das k-fache symmetrische Produkt von V, so daß Sym_k als Vektorraum isomorph ist zum Vektorraum der homogenen Polynome in X und Y vom Gesamtgrad k.
3. Ist M ein $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul, der zur Darstellung ρ gehört und φ ein Gruppen-Endomorphismus von $\mathrm{GL}(2,\mathbb{F}_q)$, so sei M^φ der $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul, der zur Darstellung $\rho \circ \varphi$ gehört.
4. Die Darstellung, welche zu dem Gruppen-Homomorphismus

$$\mathrm{GL}(2,\mathbb{F}_q) \to \mathrm{GL}(1,\mathbb{F}) = \mathbb{F}^*;\ g \longmapsto \det g^m$$

gehört, wird mit Δ^m bezeichnet.

Auf dem Modul Sym_k läßt sich die Operation der Gruppen bezüglich der Basis $\{X^{k-i}Y^i \mid i = 0, \dots, k\}$ leicht beschreiben. Insbesondere für die ausgezeichneten Elemente $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$ und $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ erhält man kompakte Formeln.

Lemma 3.4.2. *Für die Operation von* $\mathrm{GL}(2,\mathbb{F}_q)$ *auf* Sym_k *gelten folgende Formeln:*

1. $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \cdot X^iY^{k-i} = (aX+bY)^i(cX+dY)^{k-i}$,
2. $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) \cdot X^iY^{k-i} = \sum\limits_{j=0}^{k-i} \binom{k-i}{j} t^j X^{i+j}Y^{k-i-j}$,
3. $\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right) \cdot X^iY^{k-i} = \sum\limits_{j=0}^{i} \binom{i}{j} t^j X^{i-j}Y^{k-i+j}$,
4. $\left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right) \cdot X^iY^{k-i} = t^iX^iY^{k-i}$,
5. $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot X^iY^{k-i} = (-1)^{k-i}X^{k-i}Y^i$.

Beweis. In unserer Notation gelten für die natürliche Darstellung gerade $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \cdot X = aX + bY$ und $\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \cdot Y = cX + dY$. Daraus folgt direkt Formel 1. Die anderen Formeln sind Spezialisierungen. □

Wir setzen die oben definierten Bausteine nun zu neuen Darstellungen zusammen, welche sich als die einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$- und $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln erweisen werden. Gleichzeitig führen wir eine Multiindexnotation ein, welche die Rechnungen in diesen Darstellungen stark vereinfachen wird. Man beachte, daß dabei der Körpergrad $e = [\mathbb{F}_q : \mathbb{F}_p]$ von $\mathbb{F}_q$ über seinem Primkörper eine Rolle spielt.

DEFINITION 3.4.3. Es sei $e := [\mathbb{F}_q : \mathbb{F}_p]$ und $I := \{0,\dots,p-1\}^e$. Für $\underline{r} = (r_0,\dots,r_{e-1})$, $\underline{i} = (i_0,\dots,i_{e-1})$, $\underline{j} = (j_0,\dots,j_{e-1}) \in I$ definieren wir:

1. $\underline{i} \preccurlyeq \underline{j} :\Longleftrightarrow i_\nu \leqslant j_\nu$ für alle $\nu = 0,\dots,e-1$,
2. $S_{\underline{r}} := \bigotimes_{\nu=0}^{e-1} \mathrm{Sym}_{r_\nu}^{F^\nu}$,
3. $\underline{X}^{\underline{r}-\underline{i}}\underline{Y}^{\underline{i}} := X^{r_0-i_0}Y^{i_0} \otimes \ldots \otimes X^{r_{e-1}-i_{e-1}}Y^{i_{e-1}} \in S_{\underline{r}}$, so daß die Menge $\{\underline{X}^{\underline{r}-\underline{i}}\underline{Y}^{\underline{i}} \,\big|\, \underline{i} \in I,\, \underline{i} \preccurlyeq \underline{r}\}$ eine Basis von $S_{\underline{r}}$ ist,
4. $t^{\underline{i}} := t^{v(\underline{i})}$ mit $v(\underline{i}) := \sum_{\nu=0}^{e-1} i_\nu p^\nu$ für $t \in \mathbb{F}$,
5. $\binom{\underline{i}}{\underline{j}} := \binom{i_0}{j_0} \cdot \ldots \cdot \binom{i_{e-1}}{j_{e-1}}$ mit der Konvention, daß $\binom{i}{j} = 0$ für $j > i$.

Die gerade definierten Moduln $S_{\underline{r}}$ werden sich als die einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduln erweisen. Um effektiv in ihnen rechnen zu können, werden wir noch einige zusätzliche Bezeichnungen benötigen. Durch die Notation mittels Multiindizes für die Basis von $S_{\underline{r}}$ erhält man für die Gruppenoperation Formeln, die formal denen aus Lemma 3.4.2 ähnlich sind.

LEMMA 3.4.4. *Seien $\underline{r}, \underline{i} \in I$ mit $\underline{i} \preccurlyeq \underline{r}$ und $t \in \mathbb{F}_q$. Dann gelten:*
1. $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \cdot \underline{X}^{\underline{i}}\underline{Y}^{\underline{r}-\underline{i}} = \sum\limits_{I \ni \underline{j} \preccurlyeq \underline{r}-\underline{i}} \binom{\underline{r}-\underline{i}}{\underline{j}} t^{\underline{j}} \underline{X}^{\underline{i}+\underline{j}}\underline{Y}^{\underline{r}-\underline{i}-\underline{j}}$,
2. $\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \cdot \underline{X}^{\underline{i}}\underline{Y}^{\underline{r}-\underline{i}} = \sum\limits_{I \ni \underline{j} \preccurlyeq \underline{i}} \binom{\underline{i}}{\underline{j}} t^{\underline{j}} \underline{X}^{\underline{i}-\underline{j}}\underline{Y}^{\underline{r}-\underline{i}+\underline{j}}$.

BEWEIS. Da ein Gruppenelement auf einem reinen Tensor durch Operation auf allen Tensorfaktoren operiert, ergeben sich die Formeln unter Verwendung der Multiindexschreibweise unmittelbar aus denen von Lemma 3.4.2. □

Man beachte, daß man bei diesen Formeln den Index $\underline{j}$ in der Summe auch durch die ganze Menge I laufen lassen könnte, da die Binomialkoeffizienten der Multiindizes der dann zusätzlich vorkommenden Summanden verschwinden. Betrachtet man die Formeln in Abhängigkeit von t, so erkennt man eine besondere Struktur. Läßt man z.B. in der ersten Formel die Variable t durch ganz $\mathbb{F}_q$ laufen, so erhält man ein Gleichungssystem der Form $A \cdot x = y$, wobei die Einträge des Vektors y aus den $\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \cdot \underline{X}^{\underline{i}}\underline{Y}^{\underline{r}-\underline{i}}$, $t \in \mathbb{F}_q$ besteht, die Einträge des Vektors x aus den $\binom{\underline{r}-\underline{i}}{\underline{j}}\underline{X}^{\underline{i}+\underline{j}}\underline{Y}^{\underline{r}-\underline{i}-\underline{j}}$, $\underline{j} \preccurlyeq \underline{r}-\underline{i}$, und die Matrix A aus Potenzen der $t \in \mathbb{F}_q$. Solche Gleichungssysteme bzw. Matrizen spielen im folgenden noch eine wesentliche Rolle.

DEFINITION 3.4.5. Seien $a_0,\dots,a_{m-1}$ paarweise verschiedene Elemente eines beliebigen Körpers. Die Matrix

$$\begin{pmatrix} a_0^0 & a_0^1 & \ldots & a_0^{m-1} \\ a_1^0 & a_1^1 & \ldots & a_1^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ a_{m-1}^0 & a_{m-1}^1 & \ldots & a_{m-1}^{m-1} \end{pmatrix}$$

heißt Van der Monde-Matrix. Wir verwenden diese Bezeichnung auch für nicht notwendig quadratische Matrizen, falls diese durch Hinzufügen von Spalten auf der rechten Seite zu quadratischen Van der Monde-Matrizen gemacht werden können.

LEMMA 3.4.6. *Sei $A \cdot x = y$ ein lineares Gleichungssystem mit einer Van der Monde-Matrix A. Dann liegen die Einträge des Vektors x im linearen Spann der Einträge von y.*

BEWEIS. Für eine quadratische Van der Monde-Matrix wie in der Definition ist das klar, da deren Determinante gleich $\prod_{i<j}(a_j - a_i)$, also von Null verschieden ist und man die Gleichung durch Linksmultiplikation mit der Inversen von A nach x auflösen kann. Sonst kann man das Gleichungssystem zu einem größeren System

$$A' \cdot \begin{pmatrix} x \\ 0 \\ \vdots \\ 0 \end{pmatrix} = y$$

ergänzen, wobei A' eine quadratische Van der Monde-Matrix ist. Auch nun liefert Multiplikation mit ${A'}^{-1}$ das gewünschte Ergebnis. □

Eine erste Anwendungsmöglichkeit der Van der Monde-Matrix ergibt sich im Beweis des folgenden Satzes.

SATZ 3.4.7. *Die $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduln $S_{\underline{r}}$, $\underline{r} \in I$, sind ein Repräsentantensystem aller Isomorphieklassen einfacher $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduln. Die $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln $S_{\underline{r}} \otimes_{\mathbb{F}} \Delta^m$, $\underline{r} \in I$, $m \in \{0,\dots,q-2\}$, sind ein Repräsentantensystem aller Isomorphieklassen einfacher $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln. Jeder einfache $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul ist auch als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul einfach.*

Ein direkter Beweis für die Gruppen $\mathrm{GL}(2,\mathbb{F}_q)$ und $\mathrm{SL}(2,\mathbb{F}_q)$ findet sich schon in [**BrNe2**]. Eine Verallgemeinerung der Aussage für beliebige Chevalley-Gruppen findet sich in [**St1**],[**St2**].

Wir skizzieren im folgenden kurz, wie man die Einfachheit der angegebenen Darstellungen nachweisen kann, da wir später einige ähnliche Argumente verwenden werden. Da die Anzahl der angegebenen Darstellungen gerade q bzw. $q(q-1)$ beträgt, muß man dann nach Satz 3.1.3 noch zeigen, daß die Darstellungen paarweise nichtisomorph sind, um einen vollständigen Beweis des obigen Satzes zu erhalten.

Bei der Skizzierung des Nachweises der Einfachheit beschränken wir uns auf die Gruppe $\mathrm{SL}(2,\mathbb{F}_q)$. Sei U ein von 0 verschiedener Untermodul von $S_{\underline{r}}$ mit $0 \neq f \in S_{\underline{r}}$. Wir nehmen erst einmal an, daß $f = \underline{Y}^{\underline{r}}$ ist. Mit $\underline{Y}^{\underline{r}}$ enthält U auch alle Elemente $f_t := \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) \cdot \underline{Y}^{\underline{r}} = \sum\limits_{\underline{j} \preccurlyeq \underline{r}} t^{\underline{j}} \binom{\underline{r}}{\underline{j}} \underline{X}^{\underline{j}} \underline{Y}^{\underline{r}-\underline{j}}$. Durchläuft t alle Elemente $t_0,\dots,t_{q-1}$ des Körpers $\mathbb{F}_q$, so liefert dies ein Gleichungssystem $A \cdot x = y$, wobei x die Einträge $\binom{\underline{r}}{\underline{j}} \underline{X}^{\underline{j}} \underline{Y}^{\underline{r}-\underline{j}}$ mit

$\underline{j} \in I$ hat und y die Einträge f_t, $t \in \mathbb{F}_q$. Wegen Lemma 3.4.6 folgt, daß die Vektoren $\underline{X}^{\underline{j}}\underline{Y}^{\underline{r}-\underline{j}}$, $\underline{j} \in I$, Linearkombinationen der in U liegenden f_t sind und folglich auch in U liegen. Dies bedeutet aber $U = S_{\underline{r}}$.

Im Falle eines beliebigen $f \neq 0$ zeigt man auf ähnliche Weise unter Verwendung von $\left(\begin{smallmatrix}1 & 0\\ t & 1\end{smallmatrix}\right) \cdot f$, daß U mit f auch $\underline{Y}^{\underline{r}}$ enthält.

Daß ein einfacher $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul auch als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul einfach ist, sieht man daran, daß Δ^k als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul der triviale eindimensionale Modul ist.

Neben den schon angegebenen Quellen findet man einen vollständigen Beweis für die Klassifizierung der einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$- bzw. $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln auch in **[Wa]**, wo außerdem die projektiven unzerlegbaren Moduln dieser Gruppen und deren Zuordnung zu den einfachen Moduln gemäß Satz 3.1.3 bestimmt werden.

Bei der Berechnung von Sockelreihen von $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduln werden wir später neben der reinen Kenntnis der Struktur der einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduln auch eine Methode zu deren Identifizierung brauchen. Dies läßt sich mit Hilfe von sogenannten Höchstgewichtsvektoren erreichen. Diese erlauben es, die Bestimmung der einfachen Summanden eines Sockels durch die Suche nach einzelnen Vektoren zu ersetzen.

Wir werden im folgenden nur die Definition und einige Eigenschaften von Höchstgewichtsvektoren für die Gruppe $\mathrm{SL}(2,\mathbb{F}_q)$ angeben, weisen aber darauf hin, daß dies nur ein Spezialfall (sogar der einfachste) einer für alle Chevalley-Gruppen gültigen Theorie ist, die z.B. in **[St2]** beschrieben wird.

Definition 3.4.8. Sei $U = \{\left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right) \mid t \in \mathbb{F}_q\} \subseteq \mathrm{SL}(2,\mathbb{F}_q)$, $U^{\mathrm{t}} := \{\left(\begin{smallmatrix}1 & 0\\ t & 1\end{smallmatrix}\right) \mid t \in \mathbb{F}_q\}$, $w = \left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right) \in \mathrm{SL}(2,\mathbb{F}_q)$ und $\overline{U} := \sum_{t\in\mathbb{F}_q} \left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right) \in \mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$. Ein von Null verschiedenes Element m eines $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduls M heißt Höchstgewichtsvektor, wenn folgende Bedingungen erfüllt sind:

1. Das Element m ist U-invariant,
2. $\overline{U}w \cdot m = \alpha m$ für ein $\alpha \in \mathbb{F}$,
3. $\left(\begin{smallmatrix}t & 0\\ 0 & t^{-1}\end{smallmatrix}\right) \cdot m = \psi(t) \cdot m$ für einen Charakter ψ von $\mathbb{F}_q^*$.

In diesem Fall heißt das Paar (α, ψ) das Gewicht von m.

Wir geben nun die wichtigsten Eigenschaften von Höchstgewichtsvektoren an, insbesondere den Zusammenhang mit einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduln.

Proposition 3.4.9. *Für die Höchstgewichtsvektoren von* $\mathrm{SL}(2,\mathbb{F}_q)$ *gelten die folgenden Aussagen:*

1. *Jeder einfache* $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$*-Modul besitzt bis auf skalare Vielfache genau einen Höchstgewichtsvektor. Das Gewicht der Höchstgewichtsvektors eines einfachen* $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$*-Moduls legt dessen Isomorphieklasse eindeutig fest.*

2. *Es gibt die Gewichte* $(0,\chi^0),\dots,(0,\chi^{q-2})$ *und* $(-1,\chi^0)$. *Zu dem einfachen Modul* $S_{\underline{r}}$ *gehört* $(0,\chi^{v(\underline{r})})$, *falls* $\underline{r}\neq(p-1,\dots,p-1)$ *und* $(-1,\chi^0)$, *falls* $\underline{r}=(p-1,\dots,p-1)$.
3. *Besitzt ein* $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$*-Modul einen Höchstgewichtsvektor zu einem bestimmten Gewicht, so besitzt er auch einen Jordan-Hölder-Faktor zu diesem Gewicht.*
4. *Das* $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$*-Modulerzeugnis eines Höchstgewichtsvektors ist mit dem* $\mathbb{F}[U^t]$*-Modulerzeugnis identisch.*

Beweis. Wir schreiben im folgenden $\underline{i}\precneqq\underline{j}$, falls $\underline{i},\underline{j}\in I$ mit $\underline{i}\preccurlyeq\underline{j}$, $\underline{i}\neq\underline{j}$. Zuerst zeigen wir, daß die einzigen U-invarianten Elemente in einem einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul $S_{\underline{r}}$ die skalaren Vielfachen von $\underline{X}^{\underline{r}}$ sind. Sei $v=\sum_{\underline{i}\preccurlyeq\underline{r}}\alpha_{\underline{i}}\underline{X}^{\underline{i}}\underline{Y}^{\underline{r}-\underline{i}}\in S_{\underline{r}}$ invariant unter U. Es ist

$$\begin{aligned}\begin{pmatrix}1&t\\0&1\end{pmatrix}\cdot v &= \sum_{\underline{i}\preccurlyeq\underline{r}}\alpha_{\underline{i}}\sum_{\underline{j}\preccurlyeq\underline{r}-\underline{i}}\binom{\underline{r}-\underline{i}}{\underline{j}}t^{\underline{j}}\underline{X}^{\underline{i}+\underline{j}}\underline{Y}^{\underline{r}-\underline{i}-\underline{j}}\\ &= \sum_{\underline{i}\preccurlyeq\underline{r}}\alpha_{\underline{i}}\underline{X}^{\underline{i}}\underline{Y}^{\underline{r}-\underline{i}}\qquad\text{für alle } t\in\mathbb{F}_q.\end{aligned}$$

Aus der U-Invarianz folgt $\alpha_{\underline{k}}-\sum_{\underline{i}+\underline{j}=\underline{k}}\alpha_{\underline{i}}\binom{\underline{r}-\underline{i}}{\underline{j}}t^{\underline{j}}=0$ für alle $\underline{k}\preccurlyeq\underline{r}$ und alle $t\in\mathbb{F}_q$. Die linke Seite hat, aufgefaßt als Polynom in t, höchstens den Grad $v(\underline{k})\leqslant v(\underline{r})\leqslant q-1$ und q Nullstellen. Also muß jeder der Koeffizienten gleich Null sein, insbesondere ist $\binom{\underline{r}-\underline{i}}{\underline{j}}\alpha_{\underline{i}}=0$ für alle $\underline{i}\precneqq\underline{k}$. Da der vorkommende Binomialkoeffizient nicht verschwindet und diese Gleichung für alle $\underline{k}$ mit $\underline{k}\preccurlyeq\underline{r}$ gilt, muß $\alpha_{\underline{i}}=0$ sein für alle $\underline{i}\precneqq\underline{r}$. Folglich ist v ein skalares Vielfaches des U-invarianten Elements $\underline{X}^{\underline{r}}$.

Auf $\underline{X}^{\underline{r}}$ operiert $\left(\begin{smallmatrix}t&0\\0&t^{-1}\end{smallmatrix}\right)$ offensichtlich als Multiplikation mit $t^{\underline{r}}$. Als nächstes untersuchen wir die Operation von $\overline{U}w$. Es gilt

$$\begin{aligned}\overline{U}w\cdot\underline{X}^{\underline{r}} &= \sum_{t\in\mathbb{F}_q}\begin{pmatrix}1&t\\0&1\end{pmatrix}\left(\begin{smallmatrix}0&-1\\1&0\end{smallmatrix}\right)\underline{X}^{\underline{r}}=\sum_{t\in\mathbb{F}_q}\begin{pmatrix}1&t\\0&1\end{pmatrix}\underline{Y}^{\underline{r}}\\ &= \sum_{t\in\mathbb{F}_q}\sum_{\underline{j}\preccurlyeq\underline{r}}\binom{\underline{r}}{\underline{j}}t^{\underline{j}}\underline{X}^{\underline{j}}\underline{Y}^{\underline{r}-\underline{j}}\\ &= \sum_{\underline{j}\preccurlyeq\underline{r}}\binom{\underline{r}}{\underline{j}}\sum_{t\in\mathbb{F}_q}t^{\underline{j}}\underline{X}^{\underline{j}}\underline{Y}^{\underline{r}-\underline{j}}.\end{aligned}$$

Für $\underline{j}\precneqq\underline{r}\preccurlyeq(p-1,\dots,p-1)$ ist $v(\underline{j})<q-1$ und folglich $\sum\limits_{t\in\mathbb{F}_q}t^{\underline{j}}=\sum\limits_{t\in\mathbb{F}_q}t^{v(\underline{j})}=0$, d.h. der entsprechende $\underline{X}^{\underline{j}}\underline{Y}^{\underline{r}-\underline{j}}$-Koeffizient von $\overline{U}w\underline{X}^{\underline{r}}$ ist gleich 0. Für $\underline{j}=\underline{r}$ erhält man den Koeffizienten

$$\binom{\underline{r}}{\underline{r}}\sum_{t\in\mathbb{F}_q}t^{\underline{r}}=\begin{cases}0 & \text{falls}\quad \underline{r}\neq(p-1,\dots,p-1)\,,\\ -1 & \text{falls}\quad \underline{r}=(p-1,\dots,p-1)\,.\end{cases}$$

Also ist $\overline{U}w \cdot \underline{X}^{\underline{r}} = \alpha \underline{X}^{\underline{r}}$ mit $\alpha = 0$, falls $\underline{r} \neq (p-1,\dots,p-1)$ und mit $\alpha = -1$, falls $\underline{r} = (p-1,\dots,p-1)$.

Insgesamt erhält man, daß der einfache $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$ -Modul $S_{\underline{r}}$ bis auf skalare Vielfache genau den Höchstgewichtsvektor $\underline{X}^{\underline{r}}$ hat mit Gewicht $(0,\chi^{v(\underline{r})})$, falls $\underline{r} \neq (p-1,\dots,p-1)$ und mit Gewicht $(-1,\chi^0)$ für $\underline{r} = (p-1,\dots,p-1)$. Insbesondere sind die Gewichte der einfachen $\mathrm{SL}(2,\mathbb{F}_q)$ -Moduln $S_{\underline{r}}$ paarweise verschieden.

Sei nun m Höchstgewichtsvektor eines beliebigen $\mathrm{SL}(2,\mathbb{F}_q)$-Moduls M. Wir wählen einen maximalen Untermodul N in dem von m erzeugten $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)] \cdot m$. Dann ist $m \bmod N$ ein Höchstgewichtsvektor des einfachen Moduls $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)] \cdot m/N$ zum selben Gewicht. Insbesondere hat M als einen Jordan-Hölder-Faktor den zu diesem Gewicht gehörenden einfachen Modul. Außerdem zeigt dies, daß es keine weiteren Gewichte als die schon gefundenen gibt.

Wir zeigen nun noch, daß das $\mathrm{SL}(2,\mathbb{F}_q)$-Erzeugnis eines Höchstgewichtsvektors m zum Gewicht (α,ψ) schon mit dem U^{t}-Erzeugnis übereinstimmt. Dafür reicht es schon, $w \cdot m \in \mathbb{F}[U^{\mathrm{t}}] \cdot m$ zu zeigen, da $\mathrm{SL}(2,\mathbb{F}_q)$ ja von w und U^{t} erzeugt wird. Aus $\overline{U}w \cdot m = \alpha m$ folgt $w \cdot m = \alpha m - \sum_{t \in \mathbb{F}_q{}^*} \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) w \cdot m$. Also reicht es, zu zeigen, daß $\sum_{t \in \mathbb{F}_q{}^*} \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) \cdot m$ in $\mathbb{F}[U^{\mathrm{t}}] \cdot m$ liegt. Nun gilt

$$
\begin{aligned}
\sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} w \cdot m &= \sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot m = \sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \cdot m \\
&= \sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & t^{-1} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -t^{-1} \\ 0 & 1 \end{pmatrix} \cdot m \\
&\overset{\text{(i)}}{=} \sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} t & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & t^{-1} \\ 0 & 1 \end{pmatrix} \cdot m = \sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} t & 0 \\ 1 & t^{-1} \end{pmatrix} \cdot m \\
&= \sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} 1 & 0 \\ t^{-1} & 1 \end{pmatrix} \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \cdot m \\
&\overset{\text{(ii)}}{=} \sum_{t \in \mathbb{F}_q^*} \begin{pmatrix} 1 & 0 \\ t^{-1} & 1 \end{pmatrix} \psi(t) m \,.
\end{aligned}
$$

Dabei haben wir bei (i) die U-Invarianz von m benutzt und bei (ii) die Operation von Diagonalmatrizen auf m durch ψ. Wir erhalten am Ende der Rechnung einen Ausdruck, der offensichtlich in $\mathbb{F}[U^{\mathrm{t}}] \cdot m$ liegt.

Damit sind alle Aussagen der Proposition bewiesen. □

Als Korollar erhalten wir eine nützliche Abschätzung für die Anzahl der Jordan-Hölder-Faktoren des Sockels eines beliebigen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduls.

KOROLLAR 3.4.10. *Sei M ein beliebiger $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul. Die Anzahl der Jordan-Hölder-Faktoren des Sockels von M ist höchstens so groß wie die Dimension des Untervektorraums der U-Invarianten von M.*

BEWEIS. Nach Proposition 3.4.9 hat jeder einfache Modul in einer direkten Zerlegung des Sockels den Höchstgewichtsvektor als U-invariantes Element. □

Wie in Abschnitt 3.2 bereits angedeutet, werden im folgenden auch duale Darstellungen eine Rolle spielen, deren einfache Faktoren ja die Duale der Faktoren der Ausgangsdarstellung sind. Deshalb wird es notwendig sein, Duale von einfachen Darstellungen zu berechnen. Dazu muß man im wesentlichen das Dual der Darstellungen Sym_k für $0 \leqslant k \leqslant p-1$ kennen. Der Formulierung der entsprechenden Aussage und ihrem Beweis stellen wir noch einige Ausführungen voran, die auf gewisse Besonderheiten aufmerksam machen sollen, welche aus der positiven Charakteristik resultieren.

Eine leicht zu beweisende Aussage im Zusammenhang mit Dualität und symmetrischen Potenzen der natürlichen Darstellung ist die folgende. Wir schreiben dabei wieder ausführlich $\mathrm{Sym}_k V$ für Sym_k, um deutlich zwischen $(\mathrm{Sym}_k V)^*$ und $\mathrm{Sym}_k(V^*)$ unterscheiden zu können. Wenn später wieder nur noch die Moduln $\mathrm{Sym}_k V$ und $(\mathrm{Sym}_k V)^*$ vorkommen, lassen wir das V der Einfachheit halber wieder weg.

LEMMA 3.4.11. *Sei $k \in \mathbb{N}_0$. Es gibt einen $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul-Isomorphismus*

$$\mathrm{Sym}_k(V) \cong \mathrm{Sym}_k(V^*) \otimes \Delta^k.$$

BEWEIS. Sei X^*, Y^* die duale Basis zur Basis X, Y von V, so daß die $(X^*)^{k-j}(Y^*)^j$, $j = 0, \ldots, k$, eine Basis von $\mathrm{Sym}_k(V^*)$ bilden. Die Abbildung

$$\mathrm{Sym}_k(V) \to \mathrm{Sym}_k(V^*) \otimes \Delta^k;\ X^{k-j}Y^j \mapsto (-1)^j (X^*)^j (Y^*)^{k-j} \otimes 1$$

definiert offensichtlich einen Vektorraum-Isomorphismus. Sei nun $g = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_q)$. Das Element $g \cdot X^{k-j}Y^j = (aX+bY)^{k-j}(cX+dY)^j$ wird auf $(aY^* - bX^*)^{k-j}(cY^* - dX^*)^j \otimes 1$ abgebildet.

Aus

$$\begin{aligned}(g \cdot X^*)(X) &= X^*\Big(\frac{1}{\det g}\begin{pmatrix} d & -c \\ -b & a \end{pmatrix} X\Big) \\ &= X^*\Big(\frac{1}{\det g}(dX - bY)\Big) = \frac{1}{\det g} d,\end{aligned}$$

$$(g \cdot X^*)(Y) = \frac{1}{\det g} \cdot (-c),$$

$$(g \cdot Y^*)(X) = \frac{1}{\det g} \cdot (-b)$$

und

$$(g \cdot Y^*)(Y) = \frac{1}{\det g} a$$

folgt

$$g \cdot X^* = \frac{1}{\det g}(dX^* - cY^*),$$

$$g \cdot Y^* = \frac{1}{\det g}(-bX^* + aY^*)$$

und daraus

$$\begin{aligned} g \cdot ((-1)^j (X^*)^j (Y^*)^{k-j} \otimes 1) \;=\; & \frac{1}{\det g^j}(cY^* - dX^*)^j \\ & \cdot \frac{1}{\det g^{k-j}}(-bX^* + aY^*)^{k-j} \otimes \det g^k . \end{aligned}$$

Ein Vergleich mit dem Bild von $g \cdot X^{k-j} Y^j$ zeigt, daß die Abbildung ein $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$-Homomorphismus ist. □

Wir sind aber nicht an $\mathrm{Sym}_k(V^*)$, sondern an $(\mathrm{Sym}_k V)^*$ interessiert. In Analogie zur Aussage des letzten Lemmas könnte man vermuten, daß es auch einen $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$-Isomorphismus gibt zwischen $\mathrm{Sym}_k V$ und $(\mathrm{Sym}_k V)^* \otimes \Delta^m$ für ein $m \in \mathbb{N}_0$. Dies ist im allgemeinen aber nicht der Fall.

Beispiel 3.4.12. Es sei $q = 4$ und $k = 2$. Wir berechnen die Dimension des Vektorraums der unter der Untergruppe $\{\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{SL}(2, \mathbb{F}_q)\}$ fixen Vektoren von $\mathrm{Sym}_k V$ und von $(\mathrm{Sym}_k V)^*$. Für $\mathrm{Sym}_k V$ wählen wir die Basis $B = \{X^2, XY, Y^2\}$. Es ist

$$\begin{aligned} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}(aX^2 + bXY + cY^2) &= aX^2 + bX(tX + Y) + c(tX + Y)^2 \\ &= (a + bt + ct^2)X^2 + bXY + cY^2 , \end{aligned}$$

also sind genau die skalaren Vielfachen von X^2 fest unter der Operation aller $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$ und die Dimension des Fixraums ist 1.

Für $(\mathrm{Sym}_k V)^*$ benutzen wir die zu B duale Basis $B^* = \{(X^2)^*, (XY)^*, (Y^2)^*\}$. Für $v \in B$ ist der v^*-Koeffizient von $f \in (\mathrm{Sym}_k V)^*$ gerade $f(v)$. Da die Matrizen $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$ die Ordnung zwei haben, ist $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) f(v) = f(\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)^{-1} v) = f(\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) v)$. Für $f = a(X^2)^* + b(XY)^* + c(Y^2)^*$ ergibt sich

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \cdot f(X^2) = f(\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} X^2) = f(X^2) = a ,$$

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \cdot f(XY) = f(tX^2 + XY) = at + b ,$$

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \cdot f(Y^2) = f(t^2 X^2 + Y^2) = at^2 + c ,$$

also ist f genau dann fest unter allen $\binom{1\,t}{0\,1}$, wenn $f = b(XY)^* + c(Y^2)^*$ ist. Bei der Darstellung $(\mathrm{Sym}_k V)^*$ hat der Vektorraum der unter den $\binom{1\,t}{0\,1}$ fixen Elemente also die Dimension zwei. Damit können $\mathrm{Sym}_2 V$ und $(\mathrm{Sym}_2 V)^*$ als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_4)]$-Moduln nicht isomorph sein und folglich gibt es auch keinen $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_4)]$-Isomorphismus zwischen $\mathrm{Sym}_k V$ und einem $(\mathrm{Sym}_k V)^* \otimes \Delta^m$.

Der folgende Satz besagt nun, daß die Vermutung aber richtig ist, solange man nur den Fall $k < p$ betrachtet. Dieser Umstand ist ein Beispiel für ein typisches Phänomen in der Theorie der modularen Darstellungen von $\mathrm{GL}(2,\mathbb{F}_q)$. Aufgrund der positiven Charakteristik spielt manchmal die Größe von auftretenden ganzzahligen Parametern eine Rolle, indem sie bestimmt, ob gewisse Binomialkoeffizienten verschwinden oder nicht. Dies kann man auch schon im Beweis der Einfachheit der Darstellungen Sym_k für $k < p$ beobachten, welcher aus dem eben erwähnten Grund für $k = p$ scheitert. Das Verhalten von Binomialkoeffizienten in positiver Charakteristik wird in diesem Kapitel noch öfter eine entscheidende Rolle spielen. Die Tatsache, daß die folgende Aussage im Gegensatz zu der von Lemma 3.4.11 nicht für alle k gilt, weist außerdem darauf hin, daß man keinen ähnlich elementaren Beweis erwarten darf. Wir werden deshalb auch keinen expliziten Isomorphismus angeben, sondern mit Höchstgewichtsvektoren arbeiten.

Satz 3.4.13. *Sei $0 \leqslant k < p$. Dann gibt es einen $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul-Isomorphismus*

$$\mathrm{Sym}_k \cong \mathrm{Sym}_k^* \otimes \Delta^k.$$

Beweis. Wir zeigen zunächst, daß es einen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul-Isomorphismus zwischen Sym_k und Sym_k^* gibt. Dazu zeigen wir, daß die Höchstgewichtsvektoren dieser beiden einfachen Moduln das gleiche Gewicht besitzen. In unserer Notation ist $\mathrm{Sym}_k = S_{(k,0,\ldots,0)}$ und der Höchstgewichtsvektor von Sym_k ist somit X^k mit dem Gewicht $(0,\chi^k)$ für $k \leqslant p-1 < q-1$ und $(-1,\chi^k)$ für $k = p-1 = q-1$. Im Fall von $p = q$ ergibt sich die $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul-Isomorphie $\mathrm{Sym}_k \cong \mathrm{Sym}_k^*$ bereits aus Dimensionsgründen, da dann jeder einfache $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul schon durch seine Dimension charakterisiert ist. Sei also $p < q$, so daß das Gewicht gleich $(0,\chi^k)$ ist. Zur Bestimmung des Höchstgewichtsvektors von Sym_k^* berechnen wir den Untervektorraum der U-Invarianten. Dazu betrachten wir die zur Basis $X^{k-i}Y^i$, $0 \leqslant i \leqslant k$, von Sym_k duale Basis $(X^{k-i}Y^i)^*$, $0 \leqslant i \leqslant k$, von Sym_k^*. Ein Vektor $v^* = \sum_{i=0}^{k} \alpha_i (X^{k-i}Y^i)^* \in \mathrm{Sym}_k^*$ ist genau dann U-invariant, wenn $\binom{1\,t}{0\,1} v^*(X^{k-j}Y^j) = v^*(X^{k-j}Y^j) = \alpha_j$ gilt für alle $t \in \mathbb{F}_q$, $0 \leqslant j \leqslant k$.

Nun ist

$$\begin{aligned}\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} v^*(X^{k-j}Y^j) &= v^*(\begin{pmatrix}1 & -t\\ 0 & 1\end{pmatrix} X^{k-j}Y^j)\\ &= \sum_{i=0}^{k} \alpha_i (X^{k-i}Y^i)^* (\sum_{\nu=0}^{j} \binom{j}{\nu} (-t)^\nu X^{k-j+\nu} Y^{j-\nu})\\ &= \sum_{i=0}^{j} \alpha_i \binom{j}{j-i} (-t)^{j-i}\end{aligned}$$

und somit gilt $\left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right) v^*(X^{k-j}Y^j) = \alpha_j$ für alle $t \in \mathbb{F}_q$, $0 \leqslant j \leqslant k$ genau dann, wenn $\alpha_0 = \ldots = \alpha_{k-1} = 0$ ist.

Die U-Invarianten von Sym_k^* bestehen also aus dem von $(Y^k)^*$ aufgespannten Untervektorraum und folglich ist $(Y^k)^*$ der Höchstgewichtsvektor von Sym_k^*. Wegen $\left(\begin{smallmatrix}t & 0\\ 0 & t^{-1}\end{smallmatrix}\right)(Y^k)^* = t^k (Y^k)^*$ ist das dazu gehörende Gewicht wieder $(0, \chi^k)$. Daraus folgt die Existenz eines $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Isomorphismus zwischen Sym_k und Sym_k^*.

Ist nun $\mathrm{Sym}_k^* \cong S_{\underline{r}} \otimes \Delta^m$ ein $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Isomorphismus, so muß aufgrund des gerade bestimmten $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Isomorphismus der Index $\underline{r}$ gleich $(k, 0, \ldots, 0)$ sein. Um den Wert von m bei dem $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Isomorphismus $\mathrm{Sym}_k \cong \mathrm{Sym}_k^* \otimes \Delta^{-m}$ zu bestimmen, betrachten wir die Operation von $\left(\begin{smallmatrix}t & 0\\ 0 & 1\end{smallmatrix}\right)$ auf den U-Invarianten. Zum einen ist $\left(\begin{smallmatrix}t & 0\\ 0 & 1\end{smallmatrix}\right) X^k = t^k X^k$ in Sym_k und zum anderen $\left(\begin{smallmatrix}t & 0\\ 0 & 1\end{smallmatrix}\right)(Y^k)^* \otimes 1 = t^{-m}(Y^k)^* \otimes 1$ in $\mathrm{Sym}_k^* \otimes \Delta^{-m}$. Daraus ergibt sich $-m = k$ und $\mathrm{Sym}_k \cong \mathrm{Sym}_k^* \otimes \Delta^k$. □

Wir machen noch auf einen weiteren allgemeinen Aspekt der Darstellungstheorie von $\mathrm{SL}(2,\mathbb{F}_q)$ bzw. $\mathrm{GL}(2,\mathbb{F}_q)$ aufmerksam, nämlich daß im Fall $q = p$ viele Betrachtungen wesentlich einfacher werden. Wie in dem Beweis eben bereits erwähnt, ist im Fall $q = p$ die Isomorphieklasse eines einfachen Moduls bereits durch seine Dimension festgelegt, da die einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_p)]$-Moduln durch die Sym_k mit $k = 0, \ldots, p-1$ mit der jeweiligen Dimension $k+1$ gegeben sind. Im Fall von $q = p$ muß man zum Beweis der obigen Aussage also nicht auf die Verwendung von Höchstgewichtsvektoren zurückgreifen. Für beliebiges q funktioniert dieses Argument nicht, da es dann nichtisomorphe einfache Moduln gleicher Dimension gibt, selbst unter der Nebenbedingung, daß die Dimension kleiner als p ist.

Wir wenden Satz 3.4.13 nun an zur Bestimmung der Duale einfacher Moduln.

Korollar 3.4.14. *Seien $k \in \mathbb{N}_0$ und $\underline{r} \in I$. Es gibt die folgenden Isomorphien von $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln:*

1. $(\Delta^k)^* \cong \Delta^{-k}$,
2. $(\Delta^k)^F \cong \Delta^{k\cdot p}$,
3. $(M^F)^* \cong (M^*)^F$,
4. $(S_{\underline{r}} \otimes \Delta^k)^* \cong S_{\underline{r}} \otimes \Delta^{-k-v(\underline{r})}$.

BEWEIS. Zu 1: Der offensichtliche Vektorraum-Isomorphismus ist auch ein G-Homomorphismus. Sei nämlich $f : \mathbb{F} \to \mathbb{F}$ ein Element aus $(\Delta^k)^*$, das auf $f(1) \in \Delta^{-k}$ abgebildet wird. Dann wird $g \cdot f$ auf $(g \cdot f)(1) = f(g^{-1} \cdot 1) = f((\det g^{-1})^k \cdot 1) = (\det g)^{-k} f(1) = g \cdot f(1)$ abgebildet.

Zu 2: Auf beiden Moduln operiert $g \in G$ als Multiplikation mit $\det g^{k \cdot p}$.

Zu 3: Beiden Moduln liegt der Vektorraum M^* zugrunde. Wir schreiben im folgenden zur Verdeutlichung bei jeder G-Operation hinzu, in welchem Modul sie ausgeführt wird. Sei $m \in M$ und $f \in M^*$. Dann ist

$$(g \cdot_{(M^F)^*} f)(m) = f(g^{-1} \cdot_{M^F} m) = f(F(g^{-1}) \cdot_M m)$$

und

$$(g \cdot_{(M^*)^F} f)(m) = (F(g) \cdot_{M^*} f)(m) = f(F(g)^{-1} \cdot_M m)\,.$$

Zu 4: Aufgrund von Satz 3.4.13 gilt

$$\begin{aligned} (S_{\underline{r}} \otimes \Delta^k)^* &= (\bigotimes_{\nu=0}^{e-1} \mathrm{Sym}_{r_\nu}^{F^\nu} \otimes \Delta^k)^* \cong \bigotimes_{\nu=0}^{e-1} (\mathrm{Sym}_{r_\nu}^{F^\nu})^* \otimes (\Delta^k)^* \\ &\cong \bigotimes_{\nu=0}^{e-1} (\mathrm{Sym}_{r_\nu} \otimes \Delta^{-r_\nu})^{F^\nu} \otimes \Delta^{-k} \cong S_{\underline{r}} \otimes \Delta^{-k-v(\underline{r})}\,. \end{aligned}$$

□

3.5. Hauptreihendarstellungen

Hauptreihendarstellungen spielen eine wichtige Rolle in der Darstellungstheorie von GL(2), unabhängig vom Koeffizientenbereich für die Matrizengruppe und unabhängig vom Koeffizientenbereich der betrachteten Darstellungen. Dies sieht man beispielsweise daran, daß die Darstellungen der Hauptreihe über den komplexen Zahlen der Gruppe $\mathrm{GL}(2, \mathbb{F}_q)$ fast alle einfach sind und man auch fast alle einfachen Darstellungen auf diese Weise erhält. Wir werden in Abschnitt 3.7 zeigen, wie die am Ende von Kapitel 2 auftretenden Darstellungen von $G(\mathfrak{p})$ mit Darstellungen von $\mathrm{GL}(2, \mathbb{F}_q)$ und insbesondere mit Hauptreihendarstellungen zusammenhängen. Auch in der im ersten Kapitel skizzierten Situation von klassischen komplexen Modulkurven sind Darstellungen dieses Typs aufgetaucht.

Im folgenden werden wir einige grundlegende Eigenschaften unserer Hauptreihdarstellungen in positiver Charakteristik beweisen. Dabei werden auch wieder symmetrische Potenzen der natürlichen Darstellung auftreten, für die auch noch einige ergänzende Eigenschaften gezeigt werden.

Da die im Anschluß definierten Hauptreihendarstellungen von Borel-Untergruppen induziert sind und zum Nachweis vieler Eigenschaften explizite Rechnungen notwendig werden, erinnern wir kurz an eine für unsere Zwecke besonders gut geeignete Definition induzierter Darstellungen und geben einige grundlegende Eigenschaften an.

DEFINITION 3.5.1. Sei k ein beliebiger Körper sowie H Untergruppe einer endlichen Gruppe G und M ein $k[H]$-Modul. Dann ist die induzierte Darstellung $\operatorname{ind}_H^G M$ definiert als der k-Vektorraum aller Funktionen $f : G \to M$ mit $f(hx) = h \cdot f(x)$ für alle $h \in H$, $x \in G$, versehen mit der G-Operation $(g \cdot f)(x) := f(xg)$. Außerdem bezeichnen wir für einen $k[G]$-Modul N den durch Einschränkung gewonnenen $k[H]$-Modul mit N_H.

Man kann diese Definition auch benutzen, wenn k nur ein kommutativer Ring ist, so wie wir es im vorigen Kapitel schon getan haben. Im folgenden verwenden wir aber nur noch den Fall eines Körpers k.

Die große Bedeutung induzierter Darstellungen ist durch eine universelle Eigenschaft gegeben, welche im ersten Punkt des folgenden Lemmas beschrieben wird. Die weiteren Eigenschaften ergeben sich daraus ziemlich leicht (vgl. [**La1**],[**CuRe**]). Insbesondere sind die auftretenden Isomorphismen kanonisch und funktoriell in den auftretenden Moduln.

LEMMA 3.5.2. *Sei G endliche Gruppe und $H \subseteq U$ Untergruppen von G. Weiter seien M, M' zwei $k[H]$-Moduln und N ein $k[G]$-Modul. Dann gelten:*

1. *Jeder $k[H]$-Modul-Homomorphismus von M nach N faktorisiert eindeutig über $\operatorname{ind}_H^G M$.*
2. $\operatorname{ind}_H^G M \cong k[G] \otimes_{k[H]} M$.
3. $\dim_k \operatorname{ind}_H^G M = [G : H] \cdot \dim_k M$.
4. $\operatorname{ind}_U^G(\operatorname{ind}_H^U M) \cong \operatorname{ind}_H^G M$.
5. $\operatorname{ind}_H^G(M \oplus M') \cong \operatorname{ind}_H^G M \oplus \operatorname{ind}_H^G M'$.
6. $\operatorname{ind}_H^G M^* \cong (\operatorname{ind}_H^G M)^*$.
7. $\operatorname{ind}_H^G M \otimes N \cong \operatorname{ind}_H^G(M \otimes N_H)$.

Wir kommen nun zur Definition der Hauptreihendarstellungen und der mit ihnen verbundenen Begriffe. Zur Vereinfachung der Notation werden wir im Rest dieses Abschnitts die Gruppe $\mathrm{GL}(2, \mathbb{F}_q)$ mit G bezeichnen.

DEFINITION 3.5.3. Sei $G := \mathrm{GL}(2, \mathbb{F}_q)$ und $B := \{\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \mid a, d \in \mathbb{F}_q^*,\ c \in \mathbb{F}_q\}$ die Standard-Borel-Untergruppe von G.

1. Ein Charakter von $\mathbb{F}_q^*$ ist ein Homomorphismus $\psi : \mathbb{F}_q^* \to \mathbb{F}^*$.
2. Für einen Charakter ψ von $\mathbb{F}_q^*$ sei Δ^ψ die eindimensionale Darstellung von $\mathrm{GL}(2, \mathbb{F}_q)$, welche zu dem Homomorphismus $\psi \circ \det$ gehört.
3. Für zwei Charaktere ψ_1, ψ_2 von $\mathbb{F}_q^*$ sei (ψ_1, ψ_2) die eindimensionale Darstellung $B \to \mathrm{GL}(1, \mathbb{F})$; $\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \mapsto \psi_1(a) \cdot \psi_2(d)$ von B.

4. Eine Hauptreihendarstellung ist eine Darstellung von G der Form $\operatorname{ind}_B^G(\psi_1, \psi_2)$.

Zuerst beweisen wir einige einfache Eigenschaften, welche die Abhängigkeit der Hauptreihendarstellungen von den vorkommenden Charakteren beschreibt.

Vorher erinnern wir aber noch kurz an einige grundlegende Eigenschaften von Charakteren von $\mathbb{F}_q^*$. Die $\mathbb{F}$-wertigen Charaktere von $\mathbb{F}_q^*$ bilden in offensichtlicher Weise, wie wir oben bereits benutzt haben, eine Gruppe. Da $\mathbb{F}_q^*$ eine zyklische Gruppe mit $q-1$ Elementen ist und $\mathbb{F}$ die $(q-1)$-ten Einheitswurzeln enthält, ist die Charaktergruppe ebenfalls zyklisch und zum Beispiel erzeugt von der Einbettung von $\mathbb{F}_q^*$ in $\mathbb{F}$, aufgefaßt als Charakter von $\mathbb{F}_q^*$.

Definition 3.5.4. Der Charakter $\mathbb{F}_q^* \hookrightarrow \mathbb{F}$, der die Charaktergruppe von $\mathbb{F}_q^*$ erzeugt, wird mit χ bezeichnet. Das Neutralelement der Charaktergruppe von $\mathbb{F}_q^*$ wird mit 1 bezeichnet.

Lemma 3.5.5. *Seien φ, ψ, ω Charaktere von $\mathbb{F}_q^*$. Es gelten:*

1. $\operatorname{ind}_B^G(\varphi, \psi) \otimes \Delta^\omega \cong \operatorname{ind}_B^G(\varphi\omega, \psi\omega)$,
2. $\operatorname{ind}_B^G(1, \psi)^* \cong \operatorname{ind}_B^G(1, \psi^{-1})$.

Beweis. Für 1. reicht es wegen Teil 7 von Lemma 3.5.2 zu zeigen, daß die $\mathbb{F}[B]$-Moduln $(\varphi, \psi) \otimes (\Delta^\omega)_B$ und $(\varphi\omega, \psi\omega)$ isomorph sind. Das ist aber offensichtlich, da beide eindimensional sind und $\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right)$ durch Multiplikation mit $\varphi(a)\psi(d)\omega(\det \left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right)) = \varphi(a)\omega(a)\psi(d)\omega(d)$ operiert.

Wegen Lemma 3.5.2, Teil 6 genügt es für 2. zu zeigen, daß der $\mathbb{F}[B]$-Modul $(1, \psi)^*$ isomorph ist zu $(1, \psi^{-1})$. Nun operiert ein Gruppenelement g auf dem Dual einer Darstellung M durch $g \cdot f(m) = f(g^{-1}m)$ für $f \in M^*$, $m \in M$. Daraus ergibt sich, daß $\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in B$ bzgl. $(1, \psi)^*$ als Multiplikation mit $\psi(d^{-1})$ operiert, also genauso wie bzgl. $(1, \psi^{-1})$. □

Die erste Aussage des Lemmas erlaubt es uns insbesondere, von nun an nur noch Hauptreihendarstellungen der Form $\operatorname{ind}_B^G(1, \psi)$ zu betrachten, da das Tensorieren mit einem Twist der Determinante leicht zu kontrollieren ist. Wir werden nun solche Hauptreihendarstellungen jeweils in einen Untermodul und einen Quotienten zerlegen, welche sich in ihrer Struktur sehr ähnlich sind und sich mittels symmetrischer Potenzen der natürlichen Darstellung beschreiben lassen. Der erste Schritt dabei ist ziemlich leicht.

Lemma 3.5.6. *Sei $0 \leqslant k \leqslant q$. Dann ist* Sym_k *isomorph als* $\mathbb{F}[G]$*-Modul zu einem Untermodul von* $\operatorname{ind}_B^G(1, \chi^k)$.

Beweis. Wir zeigen, daß es eine $\mathbb{F}[G]$-Einbettung

$$\mathrm{Sym}_k \hookrightarrow \operatorname{ind}_B^G(1, \chi^k);\; F(X, Y) \mapsto f_F : G \to \mathbb{F} \text{ mit } f_F(\begin{pmatrix} x & z \\ y & w \end{pmatrix}) = F(y, w)$$

gibt.

1. Die Abbildung ist wohldefiniert, d.h. f_F liegt tatsächlich in $\mathrm{ind}_B^G(1, \chi^k)$: Sei $b = \left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in B$ und $g = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right) \in G$. Zu zeigen ist $f_F(bg) = bf_F(g)$. Nun ist
$$f_F(bg) = f_F(\begin{pmatrix} ax + cy & az + cw \\ dy & dw \end{pmatrix}) = F(dy, dw) = d^k F(y, w)\,,$$
da F homogen vom Grad k ist. Außerdem gilt
$$bf_F(g) = bF(y, w) = \chi^k(d) F(y, w) = d^k F(y, w)\,.$$
2. Die Abbildung ist ein $\mathbb{F}[G]$-Homomorphismus: Seien dazu $g = \left(\begin{smallmatrix} x & z \\ y & w \end{smallmatrix}\right)$ und $g' = \left(\begin{smallmatrix} x' & z' \\ y' & w' \end{smallmatrix}\right)$ aus G. Es ist
$$g' \cdot F(X, Y) = F(x'X + y'Y, z'X + w'Y)$$
und somit
$$f_{g' \cdot F}(g) = F(x'y + y'w, z'y + w'w)\,.$$
Dach Definition der induzierten Darstellung ist
$$\begin{aligned} g' \cdot f_F(g) = f_F(gg') &= f_F\left(\begin{pmatrix} xx' + zy' & xz' + zw' \\ yx' + wy' & yz' + ww' \end{pmatrix}\right) \\ &= F(x'y + y'w, z'y + w'w)\,, \end{aligned}$$
also gilt die Gleichheit $f_{g' \cdot F} = g' \cdot f_F$.
3. Die Abbildung ist injektiv: Seien $F(X, Y)$ und $G(X, Y)$ aus Sym_k. Aus $f_F = f_G$ folgt insbesondere $F(x, 1) = G(x, 1)$ für alle $x \in \mathbb{F}_q$. Ist $k \leqslant q-1$, so sind $F(X, 1)$ und $G(X, 1)$ Polynome vom Grad $\leqslant q-1$ und stimmen an q Stellen überein, also ist $F(X, 1) = G(X, 1)$ und somit auch $F(X, Y) = G(X, Y)$. Ist $k = q$, so betrachtet man das Polynom $H(X, Y) = F(X, Y) - G(X, Y)$. Die Polynome $H(X, 1)$ und $H(1, Y)$ sind vom Grad $k = q$ und haben beide q Nullstellen aus $\mathbb{F}_q$. Somit ist $H(X, 1) = c(X^q - X)$ und $H(1, Y) = c'(Y^q - Y)$ mit $c, c' \in \mathbb{F}$. Da $H(X, Y)$ homogen ist, muß $H(X, Y) = c(X^q - XY^{q-1}) = c'(Y^q - YX^{q-1})$ sein. Dies ist nur für $c = c' = 0$, d.h. im Fall $H(X, Y) = 0$ möglich.

□

Aus Dimensionsgründen liefert das Lemma insbesondere
$$\mathrm{Sym}_q \cong \mathrm{ind}_B^G(1, \chi^q) \cong \mathrm{ind}_B^G(1, \chi^1)$$
und somit hat Sym_q den Untermodul Sym_1. Für die Anwendung bei Modulkurven werden wir nur die Fälle $0 \leqslant k \leqslant q-1$ benutzen. Im Falle $k = q-1$ erhält man wegen $\chi^{q-1} = 1$ zwei Untermoduln von $\mathrm{ind}_B^G(1, 1)$, nämlich den mit der trivialen G-Operation versehenen einfachen Modul $\mathrm{Sym}_0 = \mathbb{F}$ sowie den q-dimensionalen Modul Sym_{q-1}. Wir werden später zeigen, daß auch Sym_{q-1} ein einfacher $\mathbb{F}[G]$-Modul ist und somit $\mathrm{ind}_B^G(1, 1)$ die direkte Summe dieser beiden Untermoduln ist.

Den zu dem im vorigen Lemma gefundenen Untermodul gehörenden Quotienten der Hauptreihendarstellung zu bestimmen, ist wesentlich schwieriger, aber wie der folgende Satz zeigt, hängt er auch wieder eng mit einer symmetrischen Potenz der natürlichen Darstellung zusammen.

SATZ 3.5.7. *Sei* $0 \leqslant k \leqslant q-1$ *und* $k+j=q-1$. *Dann gibt es einen* $\mathbb{F}[G]$*-Modul-Isomorphismus*

$$(\mathrm{Sym}_j)^* \cong \mathrm{ind}_B^G(1,\chi^k)/\mathrm{Sym}_k.$$

BEWEIS. Wir beweisen die äquivalente Isomorphie

$$\mathrm{Sym}_j \cong (\mathrm{ind}_B^G(1,\chi^k)/\mathrm{Sym}_k)^*\,.$$

Zuerst zeigen wir, daß beide Seiten die gleiche Dimension haben. Es ist $\dim \mathrm{Sym}_j = j+1$. Weiter ist $\dim_{\mathbb{F}} \mathrm{ind}_B^G(1,\chi^k) = [G:B] = q+1$ und $\dim_{\mathbb{F}} \mathrm{Sym}_k = k+1$. Wegen $q+1 = q-1+2 = k+j+2$ folgt die Aussage über die Dimensionen.

Zum Nachweis der Isomorphie gehen wir wie folgt vor. Für einen beliebigen $\mathbb{F}[G]$-Modul M mit Untermodul N identifiziert sich das Dual $(M/N)^*$ mit dem Untermodul von M^*, der aus allen Funktionen besteht, die auf N verschwinden. Um also eine Isomorphie $L=(M/N)^*$ zu zeigen, kann man eine Einbettung $L \hookrightarrow M^*$ angeben, so daß L als Untermodul von M^* aufgefaßt auf N verschwindet. Bei Dimensionsgleichheit von L und $(M/N)^*$ folgt dann $L \cong (M/N)^*$. In unserem Fall ist $M = \mathrm{ind}_B^G(1,\chi^k)$ und $N = \mathrm{Sym}_k$ sowie $L = \mathrm{Sym}_j$. Wir haben schon gesehen, daß $M^* \cong (\mathrm{ind}_B^G(1,\chi^k))^* \cong \mathrm{ind}_B^G(1,\chi^{-k}) = \mathrm{ind}_B^G(1,\chi^j)$ ist und daß sich $L = \mathrm{Sym}_j$ in $M^* = \mathrm{ind}_B^G(1,\chi^j)$ einbettet. Wir werden diese Einbettung explizit ausrechnen und dann prüfen, ob $L = \mathrm{Sym}_j$ auch tatsächlich auf $N = \mathrm{Sym}_k$ verschwindet.

Ein Element aus $M^* = \mathrm{ind}_B^G(1,\chi^k)^*$ ist eine Abbildung von $\mathrm{ind}_B^G(1,\chi^k)$ nach $\mathbb{F}$, wobei $\mathrm{ind}_B^G(1,\chi^k)$ selbst aus Abbildungen von G nach $\mathbb{F}$ besteht. Nun wird $\mathrm{ind}_B^G(1,\chi^k)$ als $\mathbb{F}[G]$-Modul von $(1,\chi^k)$ erzeugt, d.h. man muß von einem Element aus M^* nur wissen, wie es sich auf Elementen $g\cdot m$ mit $g \in G$, $m \in (1,\chi^k)$ auswertet. Dabei bettet sich $(1,\chi^k)$ als $\mathbb{F}[B]$-Untermodul in $\mathrm{ind}_B^G(1,\chi^k)$ ein durch $(1,\chi^k) = \mathbb{F} \ni x \mapsto \overline{x}$ mit

$$\overline{x}(g) = \begin{cases} 0 & \text{für} \quad g \notin B\,, \\ d^k \cdot x & \text{für} \quad g = \left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in B\,. \end{cases}$$

Sei nun $F(X,Y)$ ein Element von Sym_j, d.h. ein homogenes Polynom vom Grad j. Das Bild von F unter $\mathrm{Sym}_j \hookrightarrow \mathrm{ind}_B^G(1,\chi^j)$ ist die im Beweis von Lemma 3.5.6 definierte Abbildung f_F. Diese bildet unter dem Isomorphismus $\mathrm{ind}_B^G(1,\chi^j) \cong \mathrm{ind}_B^G(1,\chi^k)^*$ ab auf f_F' mit

$$f_F'(g)(x) = \overline{(f_F(g))}(x) = f_F(g)\cdot x$$

für $x \in \mathbb{F}$. Unter dem Isomorphismus $(\mathrm{ind}_B^G(1,\chi^k))^* \cong \mathrm{ind}_B^G(1,\chi^k)^*$ bildet f'_F ab auf f''_F mit

$$\begin{aligned} f''_F(g\overline{x}) &= f'_F(g^{-1})(x) = \overline{f_F(g^{-1})}(x) = f_F(g^{-1}) \cdot x \\ &= F(\frac{-b}{\det g}, \frac{a}{\det g}) \cdot x \\ &= \det g^{-j} F(-c, a) \cdot x \end{aligned}$$

für $g = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in G$.

Als nächstes müssen wir die Elemente von Sym_k als Linearkombinationen von Elementen der Form $g\overline{x}$ schreiben, um f''_F darauf auswerten zu können. Wir zeigen zunächst, daß

$$R = \{\begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix} \,\Big|\, a \in \mathbb{F}_q\} \cup \{\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\}$$

ein Repräsentantensystem von $B\backslash G$ ist. Offensichtlich ist $\#R = q+1 = [G : B]$, und jedes Element $g = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in G$ liegt in einem Br, $r \in R$: Ist $d = 0$, so sind $b, c \neq 0$ und $\left(\begin{smallmatrix} \frac{1}{c} & -\frac{a}{bc} \\ 0 & \frac{1}{b} \end{smallmatrix}\right)\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Ist $d \neq 0$, so ist $\left(\begin{smallmatrix} \frac{d}{ad-bc} & -\frac{c}{ad-bc} \\ 0 & \frac{1}{d} \end{smallmatrix}\right)\left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & 0 \\ \frac{b}{d} & 1 \end{smallmatrix}\right)$. Außerdem ist das Repräsentantensystem sogar abgeschlossen unter Inversenbildung.

Da $\{\overline{1}\}$ mit

$$\overline{1} : G \to \mathbb{F};\ g \mapsto \begin{cases} 0 & \text{für } \ g \notin B\,, \\ g \cdot 1 = d^k & \text{für } \ g = \left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in B\,, \end{cases}$$

eine Basis des eindimensionalen Vektorraums $(1, \chi^k)$ ist, bildet die Menge $\{r\overline{1} \,|\, r \in R\}$ eine Basis von $\mathrm{ind}_B^G(1,\chi^k)$. Für $r \in R$ definieren wir $f_r := r^{-1} \cdot \overline{1}$. Dann gilt

$$f_r(g) = \begin{cases} 0 & \text{für } \ g \notin Br\,, \\ gr^{-1} \cdot 1 = b \cdot 1 & \text{für } \ g = br \in Br\,. \end{cases}$$

Wir berechnen nun die Koeffizienten eines beliebigen Elementes von $\mathrm{ind}_B^G(1,\chi^k)$ bezüglich der Basis $\{f_r \,|\, r \in R\}$. Sei also $f \in \mathrm{ind}_B^G(1,\chi^k)$. Dann gilt $f = \sum\limits_{r \in R} f(r) \cdot f_r$, denn für $r_1, r_2 \in R$ ist offensichtlich

$$f_{r_1}(r_2) = \begin{cases} 0 & \text{für } \ r_1 \neq r_2\,, \\ 1 & \text{für } \ r_1 = r_2\,. \end{cases}$$

Daraus folgt die behauptete Gleichheit für $f = f_r$ mit $r \in R$ und diese liefert die Gleichheit für beliebiges f.

Wir können nun f''_F auf Elementen von Sym_k auswerten.

$$\begin{aligned}
f''_{X^{j-\nu}Y^{\nu}}(X^{k-\mu}Y^{\mu}) &= f''_{X^{j-\nu}Y^{\nu}}(\sum_{r\in R} X^{k-\mu}Y^{\mu}(r^{-1})f_{r^{-1}}) \\
&= \sum_{r\in R} X^{k-\mu}Y^{\mu}(r^{-1})\cdot f''_{X^{j-\nu}Y^{\nu}}(r\cdot\overline{1}) \\
&= \sum_{a\in\mathbb{F}_q} X^{k-\mu}Y^{\mu}(\begin{pmatrix}1 & 0\\ -a & 1\end{pmatrix})\cdot f''_{X^{j-\nu}Y^{\nu}}(\begin{pmatrix}1\ 0\\ a\ 1\end{pmatrix}\overline{1}) \\
&\quad + X^{k-\mu}Y^{\mu}(\begin{pmatrix}0\ 1\\ 1\ 0\end{pmatrix}) f''_{X^{j-\nu}Y^{\nu}}(\begin{pmatrix}0\ 1\\ 1\ 0\end{pmatrix}\overline{1}) \\
&= \sum_{a\in\mathbb{F}_q} (-a)^{k-\mu}\cdot\frac{1}{1^j}\cdot(-a)^{j-\nu}1^{\nu} + 1^{k-\mu}0^{\mu}\cdot\frac{1}{(-1)^j}(-1)^{j-\nu}0^{\nu} \\
&= \sum_{a\in\mathbb{F}_q} a^{q-1-\mu-\nu} + (-1)^{\nu}\cdot 0^{\nu}\cdot 0^{\mu}\,.
\end{aligned}$$

Wir unterscheiden zwei Fälle: Ist $\mu=\nu=0$, so erhält man

$$f''_{X^{j-\nu}Y^{\nu}}(X^{k-\mu}Y^{\mu}) = \sum_{a\in\mathbb{F}_q} a^{q-1} + 1 = 0\,.$$

Ist $\mu+\nu>0$, so erhält man

$$f''_{X^{j-\nu}Y^{\nu}}(X^{k-\mu}Y^{\mu}) = \sum_{a\in\mathbb{F}_q} a^{q-1-\nu-\mu} = 0$$

wegen $0\leqslant q-1-\nu-\mu<q-1$.

Also verschwindet f''_F auf einer Basis von Sym_k, wenn F eine Basis von Sym_j durchläuft. Damit verschwindet ganz Sym_j, aufgefaßt als Untermodul von $\mathrm{ind}_B^G(1,\chi^k)^*$, auf dem Untermodul Sym_k von $\mathrm{ind}_B^G(1,\chi^k)$. Wegen der Dimensionsgleichheit ist also $(\mathrm{ind}_B^G(1,\chi^k)/\mathrm{Sym}_k)^*$ isomorph zu Sym_j und somit $\mathrm{ind}_B^G(1,\chi^k)/\mathrm{Sym}_k \cong (\mathrm{Sym}_j)^*$. $\square$

Wir fassen Lemma 3.5.6 und Satz 3.5.7 zusammen.

KOROLLAR 3.5.8. *Sei $0\leqslant k\leqslant q-1$ und $j+k=q-1$. Es gibt eine kurze exakte Folge von $\mathbb{F}[G]$-Moduln*

$$0\to\mathrm{Sym}_k\to\mathrm{ind}_B^G(1,\chi^k)\to(\mathrm{Sym}_j)^*\to 0\,.$$

Die Aussage des Korollars erlaubt es, gewisse Fragen zur Struktur von Hauptreihendarstellungen auf symmetrische Potenzen der natürlichen Darstellung und des Duals davon zurückzuführen.

3.6. Bestimmung der Sockelreihe von Sym_k

Obwohl wir uns für die Darstellungen Sym_k interessieren, da sie die Bausteine der auftretenden Hauptreihendarstellungen sind, und wir deshalb auch im wesentlichen nur Parameter $k\leqslant q-1$ betrachten, sind strukturelle Aussagen über Sym_k für alle $k \in \mathbb{N}$ von allgemeinem Interesse, wie beispielsweise die Bestimmung der Vielfachheit der Steinbergdarstellung $S_{(p-1,\dots,p-1)}$ in Sym_k [**KuMi**],[**Ge12**]. In diesem Abschnitt beschreiben wir eine Methode, die Sockelreihe der Darstellungen Sym_k mit $k \leqslant q-1$ zu bestimmen. Dabei wird zum einen die Untermodul-Struktur der Darstellungen Sym_k eine wesentliche Rolle spielen, insbesondere die Verwendung der aus den Monomen bestehenden Standardbasis $X^{k-j}Y^j$, $j = 0,\dots,k$. Zum anderen werden wir Höchstgewichtsvektoren verwenden, um einfache Darstellungen zu erkennen.

Wie wir bereits gesehen haben, verhalten sich die Darstellungen der Form Sym_k im Fall $k \geqslant p$ deutlich komplizierter als für $k < p$. Der Grund hierfür liegt in dem besonderen Verhalten modulo p der auftretenden Binomialkoeffizienten. Die folgende Definition dient dazu, dies besser zu kontrollieren.

Definition 3.6.1. Seien $j, k \in \mathbb{N}_0$ mit den p-adischen Darstellungen $\sum\limits_{\nu\geqslant 0} j_\nu \cdot p^\nu$ und $k = \sum\limits_{\nu\geqslant 0} k_\nu \cdot p^\nu$. Auf $\mathbb{N}_0$ sei die partielle Ordnungsrelation $\preccurlyeq$ definiert durch $j \preccurlyeq k :\Leftrightarrow j_\nu \leqslant k_\nu$ für alle ν.

Es ist klar, daß dies eine Ordnungsrelation definiert, die aber nur partiell ist. Außerdem impliziert $j \preccurlyeq k$ offensichtlich $j \leqslant k$. Das Zusammenspiel zwischen der Ordnungsrelation $\preccurlyeq$ auf der Menge $\mathbb{N}_0$ bzw. auf der für uns wesentlichen Teilmenge $\{0,\dots,q-1\}$ und der in Definition 3.4.3 eingeführten Ordnungsrelation $\preccurlyeq$ auf der Menge I ist der wesentliche Punkt bei den folgenden Untersuchungen. Genauer gesagt ergibt sich die Bedeutung der neuen $\preccurlyeq$-Relation im Zusammenhang mit unseren Darstellungen Sym_k aus der sogenannten Lucas-Kongruenz.

Lemma 3.6.2. [**Lu**] *Seien $j, k \in \mathbb{N}_0$ mit den p-adischen Darstellungen $\sum_{\nu\geqslant 0} j_\nu \cdot p^\nu$ und $k = \sum_{\nu\geqslant 0} k_\nu \cdot p^\nu$. Dann gilt*

$$\binom{k}{j} \equiv \prod_{\nu\geqslant 0} \binom{k_\nu}{j_\nu} \bmod p\,.$$

Insbesondere gilt also

$$\binom{k}{j} \not\equiv 0 \bmod p \;\Leftrightarrow\; j \preccurlyeq k\,.$$

Die Formeln für die Operation von $\left(\begin{smallmatrix}1 & t\\ 0 & 1\end{smallmatrix}\right)$ und $\left(\begin{smallmatrix}1 & 0\\ t & 1\end{smallmatrix}\right)$ auf den Monomen $X^{k-j}Y^j$ lassen sich damit auch wie folgt schreiben.

Lemma 3.6.3. *In Sym_k gelten folgende Formeln:*

1.

$$\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix} \cdot X^iY^{k-i} = \sum_{j\preccurlyeq k-i} \binom{k-i}{j} t^j X^{i+j} Y^{k-i-j}\,,$$

2.
$$\begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix} \cdot X^i Y^{k-i} = \sum_{j \preccurlyeq i} \binom{i}{j} t^j X^{i-j} Y^{k-i+j} .$$

Beweis. Die beiden Formeln ergeben sich aus den Formeln von Lemma 3.4.2 einfach durch Weglassen der Summanden, bei denen der Binomialkoeffizient verschwindet. □

Wir untersuchen nun, wie der von einem Monom erzeugte Untermodul in einem Modul Sym_k aussieht.

Proposition 3.6.4. *Seien $0 \leqslant k \leqslant q-1$ und $0 \leqslant j \leqslant k$ sowie M der von $X^{k-j}Y^j$ erzeugte $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Untermodul von Sym_k. Sei I_1 die kleinste Teilmenge von $\{0,\ldots,k\}$, welche das Element j enthält und mit jedem $i \in I_1$ auch alle $i' \in \{0,\ldots,k\}$ mit $i' \preccurlyeq i$ oder $k-i' \preccurlyeq k-i$. Weiter sei I_2 die kleinste Teilmenge von $\{0,\ldots,k\}$, welche das Element j enthält und mit jedem $i \in I_2$ auch $k-i$ sowie alle $i' \in \{0,\ldots,k\}$ mit $i' \preccurlyeq i$. Dann ist $I_1 = I_2$ und die Menge $\{X^{k-i}Y^i \,\big|\, i \in I_1 = I_2\}$ ist eine Vektorraumbasis von M. Der von $X^{k-j}Y^j$ erzeugte $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Untermodul ist mit dem von diesem Element erzeugten $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul identisch.*

Beweis. Sei $\mathbb{F}_q = \{t_1,\ldots,t_q\}$ und für $t \in \mathbb{F}_q$ sei $F_t := \left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) X^{k-j}Y^j = \sum_{i=0}^{j} \binom{j}{i} t^i X^{k-j+i} Y^{j-i}$. Sei weiter $H_i := \binom{j}{i} X^{k-j+i}Y^{j-i}$ für $i = 0,\ldots,j$, so daß $F_t = \sum_{i=0}^{j} t^i H_i$ ist. Läuft t nun durch ganz $\mathbb{F}_q$, so ergibt sich ein Gleichungssystem
$$\begin{pmatrix} t_1^0 & \ldots & t_1^j \\ \vdots & \ddots & \vdots \\ t_q^0 & \ldots & t_q^j \end{pmatrix} \begin{pmatrix} H_0 \\ \vdots \\ H_j \end{pmatrix} = \begin{pmatrix} F_{t_1} \\ \vdots \\ F_{t_q} \end{pmatrix}$$
mit einer Van der Monde-Matrix. Nach Lemma 3.4.6 liegen die H_i also in dem von den F_t aufgespannten Vektorraum, also insbesondere in dem von $X^{k-j}Y^j$ erzeugten $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul M. Da $\binom{j}{i} \not\equiv 0 \bmod p$ genau dann gilt, wenn $i \preccurlyeq j$ ist, enthält M alle $X^{k-j+i}Y^{j-i}$ mit $i \preccurlyeq j$. Wegen $i \preccurlyeq j \Leftrightarrow j-i \preccurlyeq j$ enthält M also alle $X^{k-i}Y^i$ mit $i \preccurlyeq j$.

Genau das gleiche Argument mit $E_t := \left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right) X^{k-j}Y^j$ an der Stelle der F_t zeigt, daß M auch alle $X^{k-i}Y^i$ mit $k-i \preccurlyeq k-j$ enthält. Da die Matrizen $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 1 & 0 \\ t & 1 \end{smallmatrix}\right)$ die Gruppe $\mathrm{SL}(2,\mathbb{F}_q)$ erzeugen, folgt, daß M als Vektorraum von den $X^{k-i}Y^i$, $i \in I_1$, aufgespannt wird.

Außerdem wird $\mathrm{SL}(2,\mathbb{F}_q)$ von den Matrizen $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ erzeugt. Wegen $\left(\begin{smallmatrix} 0 & -1 \\ 0 & 1 \end{smallmatrix}\right) \cdot X^{k-j}Y^j = \pm X^jY^{k-j}$ folgt, daß M als Vektorraum auch auch von den $X^{k-i}Y^i$, $i \in I_2$, aufgespannt wird.

Da die angegebenen Mengen M nicht nur als Vektorraum erzeugen, sondern sogar Teilmengen der Standardbasis $\{X^{k-i}Y^i \mid i = 0,\ldots,k\}$

von Sym_k sind, müssen sie gleich sein. Da außerdem $\mathrm{GL}(2,\mathbb{F}_q)$ von $\mathrm{SL}(2,\mathbb{F}_q)$ und den Elementen der Form $\left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$ erzeugt wird, und $\left(\begin{smallmatrix} t & 0 \\ 0 & 1 \end{smallmatrix}\right)$ auf den Monomen $X^{k-i}Y^i$ als Multiplikation mit dem Skalar t^{k-i} operiert, ist klar, daß $\mathrm{GL}(2,\mathbb{F}_q)$ denselben Modul erzeugt wie $\mathrm{SL}(2,\mathbb{F}_q)$. □

Diese Proposition werden wir insbesondere auf Höchstgewichtsvektoren anwenden, da wir ja mit deren Hilfe die Sockel der auftretenden $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduln erzeugen wollen. Man beachte jedoch, daß die Existenz eine Höchstgewichtsvektors zwar die Existenz eines zum entsprechenden einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul isomorphen Jordan-Hölder-Faktors erzwingt, daß das $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Erzeugnis des Höchstgewichtsvektors selbst aber nicht unbedingt einfach sein muß. Umgekehrt besitzt zwar jeder Modul mindestens einen Höchstgewichtsvektor, z.B. den eines einfachen Untermoduls, aber es muß nicht zu jedem einfachen Jordan-Hölder-Faktor einen Höchstgewichtsvektor geben.

Beispiel 3.6.5. Wie in Beispiel 3.4.12 betrachten wir zuerst Sym_2 als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_4)]$-Modul. Da X^2 bis auf skalare Vielfachen der einzige U-invariante Vektor war, muß er ein Höchstgewichtsvektor sein, und zwar der einzige. Das Gewicht von X^2 ist $(0,\chi^2)$, also ist der entsprechende einfache Modul $S_{(0,1)}$. Dieser hat nur die Dimension 2, während Sym_2 die Dimension 3 hat. Also ist Sym_2 als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_4)]$-Modul nicht einfach, obwohl nur ein Höchstgewichtsvektor in Sym_2 vorkommt. Aus Dimensionsgründen gibt es noch genau einen weiteren Jordan-Hölder-Faktor, der isomorph zum trivialen Modul ist und dessen Höchstgewichtsvektor erst in einem Quotienten von Sym_2 sichtbar wird.

Im nächsten Beispiel taucht ein Höchstgewichtsvektor auf, dessen Erzeugnis nicht einfach ist. Dazu wählen wir die Gruppe $\mathrm{SL}(2,\mathbb{F}_2)$. Sie besitzt nur die beiden Gewichte $(0,\chi^1)$ und $(1,\chi^0)$. Der Vektor X ist der Höchstgewichtsvektor der einfachen Darstellung Sym_1. Er ist unter U invariant und auch unter $\overline{U}w$, sein Gewicht ist also $(1,\chi^0)$. Wir betrachten die 4-dimensionale Darstellung $\mathrm{Sym}_1 \otimes \mathrm{Sym}_1$ und darin das Element $X \otimes X$. Da X invariant ist unter U und $\overline{U}w$, gilt dies auch für $X \otimes X$. Also ist $X \otimes X$ auch Höchstgewichtsvektor zum selben Gewicht wie X. In dem von $X\otimes X$ erzeugten Modul liegen aber $X\otimes X$, $Y \otimes Y = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \cdot X \otimes X$ und $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right) \cdot X \otimes X = (X+Y)\otimes(X+Y) = X\otimes X + Y\otimes Y + X\otimes Y + Y\otimes X$. Der von $X \otimes X$ erzeugte Modul hat also mindestens die Dimension 3. Wäre er einfach, müßte er aber isomorph zu Sym_1 sein, d.h. Dimension 2 haben.

Definition 3.6.6. Ein Höchstgewichtsvektor, dessen Erzeugnis ein einfacher $\mathrm{SL}(2,\mathbb{F}_q)$-Modul ist, heißt *zulässig*.

Wir kommen nun gleich zum ersten Schritt bei der Bestimmung der Sockelreihe der Darstellungen Sym_k mit $k \leqslant q-2$, nämlich der Bestimmung des Sockels. Diese ist zwar in der später beschriebenen Methode zur Berechnung der Sockelreihe enthalten, aber wir werden diesen ersten Schritt trotzdem explizit ausführen, da er typisch für die gesamte Berechnung der Sockelreihe ist und somit zu deren Verständnis beiträgt. Vorher bemerken wir noch, daß im folgenden trivialerweise nur die Gewichte der Form $(0, \chi^k)$ eine Rolle spielen.

LEMMA 3.6.7. *Sei $0 \leqslant k \leqslant q-2$. Dann operiert $\overline{U}w$ auf ganz Sym_k als Multiplikation mit 0. Insbesondere ist kein Jordan-Hölder-Faktor des $\mathbb{F}[\mathrm{SL}(2, \mathbb{F}_q)]$-Moduls Sym_k isomorph zu $S_{(p-1,\ldots,p-1)}$.*

BEWEIS. Die zweite Aussage folgt aus der ersten, ist aber auch direkt aus Dimensionsgründen klar, da die Dimension des Moduls $S_{(p-1,\ldots,p-1)}$ gleich q ist, die von Sym_k aber höchstens $q-1$. Die erste Aussage rechnen wir auf den Basisvektoren $X^i Y^{k-i}$ nach. Es ist $wX^iY^{k-i} = \pm X^{k-i}Y^i$ und

$$\begin{aligned}\overline{U} \cdot X^{k-i}Y^i &= \sum_{t\in\mathbb{F}_q} \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} X^{k-i}Y^i = \sum_{t\in\mathbb{F}_q} \sum_{j=0}^{i} \binom{i}{j} t^j X^{k-i+j} Y^{i-j} \\ &= \sum_{j=0}^{i} \binom{i}{j} \sum_{t\in\mathbb{F}_q} t^j X^{k-i+j} Y^{i-j} = 0\end{aligned}$$

wegen $\sum_{t\in\mathbb{F}_q} t^j = 0$ für $0 \leqslant j \leqslant q-2$. □

PROPOSITION 3.6.8. *Sei $k \leqslant q-1$ mit der p-adischen Darstellung $k = \sum_{\nu=0}^{e-1} k_\nu \cdot p^\nu$. Dann definiert*

$$\begin{aligned} S_{(k_0,\ldots,k_{e-1})} = \bigotimes_{\nu=0}^{e-1} (\mathrm{Sym}_{k_\nu})^{F^\nu} \quad &\hookrightarrow \quad \mathrm{Sym}_k\,; \\ \bigotimes_{\nu} f_\nu(X,Y) \quad &\mapsto \quad \prod_{\nu} f_\nu(X^{p^\nu}, Y^{p^\nu}) \end{aligned}$$

eine Einbettung von $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$-Moduln, deren Bild der Sockel des $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$-Moduls Sym_k ist. Der Sockel des $\mathbb{F}[\mathrm{SL}(2, \mathbb{F}_q)]$-Moduls Sym_k ist mit dem $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$-Sockel identisch und wird von dem Höchstgewichtsvektor X^k erzeugt.

BEWEIS. Wir zeigen zuerst, daß der $\mathbb{F}[\mathrm{SL}(2, \mathbb{F}_q)]$-Sockel von Sym_k einfach ist und isomorph zu $S_{(k_0,\ldots,k_{e-1})}$. Dazu bestimmen wir die Dimension der U-Invarianten von Sym_k. Sei $0 \neq v = \sum_{i=0}^{k} \alpha_i X^{k-i} Y^i \in \mathrm{Sym}_k$ ein U-invariantes Element. Dann gilt

$$v = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} v = \sum_{i=0}^{k} \alpha_i \sum_{j=0}^{i} \binom{i}{j} t^i X^{k-i+j} Y^{i-j}$$

für alle $t \in \mathbb{F}_q$. Ein Vergleich der $X^{k-n}Y^n$-Koeffizienten liefert $\alpha_n = \sum_{i=n}^{k} \alpha_i \binom{i}{n} t^{i-n}$ für alle $t \in \mathbb{F}_q$. Da die rechte Seite davon ein Polynom in t vom Grad $\leqslant k \leqslant q-1$ ist, muß $\alpha_i\binom{i}{n} = 0$ sein für alle $i > n$. Für $n = 0$ liefert das $\alpha_i = 0$ für alle $i > 0$. Bis auf skalare Vielfache gibt es also nur den U-invarianten Vektor X^k. Dieser muß dann schon der bis auf Skalare einzige Höchstgewichtsvektor sein und den somit notwendigerweise einfachen Sockel erzeugen. Das Gewicht von X^k ist $(0, \chi^k)$ und gehört zum einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul $S_{(k_0,\dots,k_{e-1})}$. Wir haben schon gesehen, daß der von X^k erzeugte $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul auch ein $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul ist und als solcher ist er auch einfach. Da jeder weitere einfache $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Untermodul einen einfachen $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul enthalten würde, muß der von X^k erzeugte Modul auch schon der Sockel von Sym_k als $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul sein.

Daß auf die in der Proposition angegebene Weise eine Vektorraum-Einbettung definiert wird, ist klar. Wir zeigen noch, daß diese Einbettung auch ein $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Homomorphismus ist. Sei $g = \left(\begin{smallmatrix} a & c \\ b & d \end{smallmatrix}\right) \in \mathrm{GL}(2,\mathbb{F}_q)$. Dann ist

$$g \cdot \bigotimes_{\nu=0}^{e-1} f_\nu(X,Y) = \bigotimes_{\nu=0}^{e-1} f_\nu(a^{p^\nu}X + c^{p^\nu}Y, b^{p^\nu}X + d^{p^\nu}Y)\,.$$

Dies wird abgebildet auf

$$\prod_{\nu=0}^{e-1} f_\nu(a^{p^\nu}X^{p^\nu} + c^{p^\nu}Y, b^{p^\nu}X^{p^\nu} + d^{p^\nu}Y^{p^\nu})\,.$$

Da auch

$$\begin{aligned} g \cdot \prod_{\nu=0}^{e-1} f_\nu(X^{p^\nu}, Y^{p^\nu}) &= \prod_{\nu=0}^{e-1} f_\nu((aX+cY)^{p^\nu}, (bX+dY)^{p^\nu}) \\ &= \prod_{\nu=0}^{e-1} f_\nu(a^{p^\nu}X^{p^\nu} + c^{p^\nu}Y^{p^\nu}, b^{p^\nu}Y^{p^\nu} + d^{p^\nu}Y^{p^\nu}) \end{aligned}$$

ist, erhält man einen $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Homomorphismus. □

Proposition 3.6.4 und Proposition 3.4.9 zusammen zeigen, daß der von dem Höchstgewichtsvektor X^k in Sym_k erzeugte Untermodul die Vektorraumbasis $\{X^{k-i}Y^i \,\big|\, 0 \leqslant i \leqslant k,\ i \preccurlyeq k\}$ hat. Da diese Basis eine Teilmenge der für alle Rechnungen in Sym_k verwendeten Standardbasis der Monome ist, lassen sich insbesondere Rechnungen in dem Quotienten $\mathrm{Sym}_k/S_{(k_0,\dots,k_{e-1})} = \mathrm{Sym}_k/\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]\cdot X^k = \mathrm{Sym}_k/\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]\cdot X^k$ leicht ausführen, indem man einfach in Sym_k rechnet und alle dabei auftretenden Terme mit Monomen $X^{k-i}Y^i$ und $i \preccurlyeq k$ ignoriert. Insbesondere ist es nicht allzu schwierig, die U-Invarianten bzw. die Höchstgewichtsvektoren von $\mathrm{Sym}_k/S_{(k_0,\dots,k_{e-1})}$ zu bestimmen, was wieder der erste Schritt bei der Berechnung des Sockels von $\mathrm{Sym}_k/S_{(k_0,\dots,k_{e-1})} = \mathrm{Sym}_k/\mathrm{soc}(\mathrm{Sym}_k)$ ist. Verträglichkeit mit der Standardbasis $\{X^{k-i}Y^i \mid 0 \leqslant i \leqslant k\}$ von Sym_k wird dabei im folgenden eine wichtige Rolle spielen.

Definition 3.6.9. Ein Untervektorraum von Sym_k heißt monomial, wenn er eine Basis besitzt, die aus Monomen besteht. Ist M ein monomialer Untervektorraum von Sym_k, so heißt ein Element $\overline{m} \in \mathrm{Sym}_k/M$ monomial, wenn es die Restklasse eines Monoms $m \in \mathrm{Sym}_k$ ist.

Aus Proposition 3.6.4 folgt, daß das $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Erzeugnis von monomialen Vektoren mit ihrem $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Erzeugnis übereinstimmt und daß ein monomialer Untervektorraum genau dann ein $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul ist, wenn er ein $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul ist. Der wesentliche Vorteil der Monomialität besteht aber darin, daß sie bei wiederholter Quotientenbildung modulo $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$- oder $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Untermoduln erhalten bleibt: Ist M monomialer Untermodul von Sym_k und $\overline{m} \in \mathrm{Sym}_k/M$ monomial, so zeigt Proposition 3.6.4, daß $(\mathrm{Sym}_k/M)/\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]\cdot\overline{m} \cong \mathrm{Sym}_k/M'$ ist mit monomialem M'.

Im folgenden werden wir zeigen, daß die Moduln der Sockelreihe von Sym_k monomial sind. Dies wäre natürlich unmittelbar klar, wenn man zeigen könnte, daß alle Höchstgewichtsvektoren der Quotienten $\mathrm{Sym}_k/\mathrm{soc}^n(\mathrm{Sym}_k)$ monomial wären. Leider können wir dies weder beweisen noch widerlegen. Einfach zu zeigen ist aber folgende Abschwächung, welche für die späteren Zwecke ausreichend ist.

Proposition 3.6.10. *Sei $0 \leqslant k \leqslant q-2$ und M ein monomialer $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$- bzw. $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Untermodul von Sym_k. Sei $m = \sum_{i=0}^{k} \alpha_i X^{k-i}Y^i \in \mathrm{Sym}_k$ ein Vektor, für den $m \bmod M$ ein Höchstgewichtsvektor von Sym_k/M ist. Dann ist $m \bmod M$ Linearkombination zweier monomialer Elemente von Sym_k/M.*

Beweis. Sei $(0, \chi^j)$ mit $0 \leqslant j \leqslant q-2$ das Gewicht von $m \bmod M$. Dann ist

$$\begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} \cdot m = \sum_i t^{k-2i}\alpha_i X^{k-i}Y^i \equiv t^j \cdot \sum_i \alpha_i X^{k-i}Y^i \bmod M\,.$$

Alle i zwischen 0 und k, für die $X^{k-i}Y^i \notin M$ und $\alpha_i \neq 0$ ist, müssen somit $2i \equiv k-j \bmod q-1$ erfüllen. Da $m \bmod M$ gleich der Summe der $\alpha_i X^{k-i}Y^i \bmod M$ mit diesen i ist und es wegen $0 \leqslant i \leqslant k \leqslant q-2$ höchstens zwei solcher Zahlen geben kann, folgt die behauptete Aussage. □

Interessanterweise ist hier der Fall der Charakteristik $p = 2$ sogar einfacher als der Fall ungerader Charakteristik, da dann nämlich $q-1$ ungerade ist und aus $2i \equiv k-j \bmod q-1$ schon $i \equiv \frac{1}{2}(k-j) \bmod q-1$ folgt und somit nur eine Möglichkeit für $0 \leqslant i \leqslant q-2$ existiert. Im Fall ungerader Charakteristik erhält man, daß $m \bmod M$ bis auf einen Skalar von der Form $X^{k-i_0}Y^{i_0} + \alpha X^{k-i_1}Y^{i_1} \bmod M$ ist mit $i_1 = i_0 + \frac{q-1}{2}$.

Wir nutzen nun weitere Eigenschaften von Höchstgewichtsvektoren aus.

PROPOSITION 3.6.11. *Es sei* $0 \leqslant k \leqslant q-2$ *sowie* M *ein monomialer* $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$*-Untermodul von* Sym_k. *Sei weiter* $m = X^{k-i_0}Y^{i_0} + \alpha X^{k-i_1}Y^{i_1} \in \mathrm{Sym}_k$ *mit* $i_0 < i_1$ *und* $X^{k-i_0}Y^{i_0}, X^{k-i_1}Y^{i_1} \notin M$. *Ist* $m \bmod M$ *Höchstgewichtsvektor von* Sym_k/M *zum Gewicht* $(0,\psi)$, *dann sind auch* $X^{k-i_0}Y^{i_0} \bmod M$ *und* $X^{k-i_1}Y^{i_1} \bmod M$ *Höchstgewichtsvektoren von* Sym_k/M *zu diesem Gewicht.*

BEWEIS. Wie wir bereits in Lemma 3.6.7 gesehen haben, ist die Bedingung 2 aus Definition 3.4.8 im vorliegenden Fall leer. Daß $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right)$ auf $X^{k-i_0}Y^{i_0} \bmod M$ und $X^{k-i_1}Y^{i_1} \bmod M$ als Multiplikation mit $\psi(t)$ operiert, ist auch unmittelbar klar: es ist

$$\begin{aligned} t^{k-2i_0}X^{k-i_0}Y^{i_0} + t^{k-2i_1}X^{k-i_1}Y^{i_1} \bmod M &= \begin{pmatrix} t & 0 \\ 0 & t^{-1} \end{pmatrix} m \bmod M \\ &= \psi(t)X^{k-i_0}Y^{i_0} + \psi(t)X^{k-i_1}Y^{i_1} \bmod M \end{aligned}$$

und da sich $X^{k-i_0}Y^{i_0} \bmod M$ und $X^{k-i_1}Y^{i_1} \bmod M$ zu einer Basis von Sym_k/M ergänzen lassen, operiert $\left(\begin{smallmatrix} t & 0 \\ 0 & t^{-1} \end{smallmatrix}\right)$ als Multiplikation mit $\psi(t) = t^{k-2i_0} = t^{k-2i_1}$ auf $X^{k-i_0}Y^{i_0} \bmod M$ und $X^{k-i_1}Y^{i_1} \bmod M$.

Da $m \bmod M$ als Höchstgewichtsvektor U-invariant ist und dies eine lineare Bedingung ist, müssen entweder sowohl $X^{k-i_0}Y^{i_0} \bmod M$ als auch $X^{k-i_1}Y^{i_1} \bmod M$ invariant unter U und damit Höchstgewichtsvektoren zu $(0,\psi)$ sein, oder $X^{k-i_0}Y^{i_0} \bmod M$ und $X^{k-i_1}Y^{i_1} \bmod M$ sind beide nicht U-invariant. Wir nehmen an, sie wären beide nicht U-invariant. Wegen

$$\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} X^{k-i_{0/1}}Y^{i_{0/1}} = \sum_{j=0}^{i_{0/1}} \binom{i_{0/1}}{j} t^j X^{k-i_{0/1}+j}Y^{i_{0/1}-j}$$

existieren $0 < j_{0/1} \leqslant i_{0/1}$ mit $\binom{i_{0/1}}{j_{0/1}} t^{j_{0/1}} X^{k-i_{0/1}+j_{0/1}}Y^{i_{0/1}-j_{0/1}} \notin M$. Der Koeffizient von $X^{k-i_0+j_0}Y^{i_0-j_0}$ in $\left(\begin{smallmatrix} 1 & t \\ 0 & 1 \end{smallmatrix}\right) m$ ergibt sich als $\binom{i_0}{j_0} t^{j_0} + \alpha \binom{i_1}{i_1-i_0+j_0} t^{i_1-i_0+j_0}$. Da $\binom{i_0}{j_0} \not\equiv 0 \bmod p$ und $j_0 \not\equiv i_1 - i_0 + j_0 \bmod q-1$ ist, bleibt dieser Koeffizient nicht konstant, wenn t den Körper $\mathbb{F}_q$ durchläuft. Da aber die in Sym_k/M nicht verschwindenden Monome eine Basis bilden und $X^{k-i_0+j_0}Y^{i_0-j_0} \notin M$ ist, kann $m \bmod M$ nicht U-invariant sein. Die Annahme, daß $X^{k-i_0}Y^{i_0} \bmod M$ und $X^{k-i_1}Y^{i_1} \bmod M$ beide nicht U-invariant sind, liefert also einen Widerspruch. $\square$

Die Proposition zeigt, daß in einem Quotienten Sym_k/M mit monomialem M der von allen Höchstgewichtsvektoren erzeugte $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Untermodul gleich dem von allen monomialen Höchstgewichtsvektoren erzeugte Untermodul ist. Da für die Sockelreihe aber nur zulässige Höchstgewichtsvektoren eine Rolle spielen, d.h. solche, deren Erzeugnis einfach ist, müssen wir diese Eigenschaft noch genauer untersuchen.

PROPOSITION 3.6.12. *Sei* $0 \leqslant k \leqslant q-2$ *und* M *ein monomialer* $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$*-Untermodul von* Sym_k. *Sei weiter* $m = X^{k-i_0}Y^{i_0} +$

$\alpha X^{k-i_1}Y^{i_1} \in \mathrm{Sym}_k$ mit $i_0 < i_1$ und $X^{k-i_0}Y^{i_0}, X^{k-i_1}Y^{i_1} \notin M$. Sind $m \bmod M$, $X^{k-i_0}Y^{i_0} \bmod M$ und $X^{k-i_1}Y^{i_1} \bmod M$ Höchstgewichtsvektoren von Sym_k/M und $m \bmod M$ sogar zulässig, so sind auch $X^{k-i_0}Y^{i_0} \bmod M$ und $X^{k-i_1}Y^{i_1} \bmod M$ zulässig.

Beweis. Sei $m_{0/1} = X^{k-i_{0/1}}Y^{i_{0/1}}$, so daß $m = m_0 + \alpha m_1$ ist. Setze $v(i, 0/1) := \binom{k-i_{0/1}}{i} X^{k-i_{0/1}-i}Y^{i+i_{0/1}}$. Dann ist

$$\begin{aligned}\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix} m_{0/1} = (X+tY)^{k-i_{0/1}}Y^{i_{0/1}} &= \sum_{i=0}^{k-i_{0/1}} t^i \binom{k-i_{0/1}}{i} X^{k-i_{0/1}-i}Y^{i+i_{0/1}}\\ &= \sum_{i=0}^{k-i_{0/1}} t^i v(i, 0/1)\end{aligned}$$

Aus Proposition 3.4.9 und Lemma 3.4.6 folgt, daß der von $m_{0/1}$ erzeugte $\mathbb{F}[\mathrm{SL}(2, \mathbb{F}_q)]$-Modul als Vektorraum von $\{v(i, 0/1) \mid i = 0, \ldots, k - i_{0/1}\}$ erzeugt wird.

Da $m \bmod M$ nicht monomial ist, muß, wie bereits erwähnt, p ungerade und $i_1 = i_0 + \frac{q-1}{2}$ sein. Für $0 \leqslant i \leqslant k - i_1 = k - i_0 - \frac{q-1}{2}$ setzen wir $w(i) := v(i, 0) + \alpha v(i, 1)$ und für $i > k - i_1$ setzen wir $w(i) := v(i, 0)$. Damit gilt dann

$$\begin{aligned}\begin{pmatrix}1 & 0\\ t & 1\end{pmatrix} m = \begin{pmatrix}1 & 0\\ t & 1\end{pmatrix}(m_0 + \alpha m_1) &= \sum_{i=0}^{k-i_0} t^i v(i, 0) + \alpha \sum_{i=0}^{k-i_0-\frac{q-1}{2}} t^i v(i, 1)\\ &= \sum_{i=0}^{k-i_0} t^i w(i)\end{aligned}$$

und wegen Proposition 3.4.9 und Lemma 3.4.6 wird der von m erzeugte $\mathbb{F}[\mathrm{SL}(2, \mathbb{F}_q)]$-Untermodul als Vektorraum von $\{w(i) \mid 0 \leqslant i \leqslant k - i_0\}$ erzeugt.

Wir vergleichen nun die Dimensionen der jeweils von $m \bmod M$, $m_0 \bmod M$ und $m_1 \bmod M$ erzeugten Moduln. Sei dazu noch $z(i) := X^{k-i}Y^i$ für $i = 0, \ldots, k$. Die von 0 verschiedenen $z_i \bmod M$ bilden eine Vektorraumbasis von Sym_k/M. Wir stellen nun die $v(i, j)$ und die $w(j)$ bezüglich der Basis $z_0, \ldots, z_k$ dar. Es ist $v(i, 0) = \alpha_i z(i_0 + i)$ und $v(i, 1) = \beta_i w(i_1 + i) = \beta_i w(i_0 + \frac{q-1}{2} + i)$ für gewisse $\alpha_i, \beta_i \in \mathbb{F}_p$. Somit ergibt sich

$$w(i) = \begin{cases} v(i, 0) + \alpha v(i, 1) & = \alpha_i z(i_0 + i) + \alpha\beta_i z(i_1 + i) \quad \text{für} \quad i \leqslant k - i_1\,,\\ v(i, 0) & = \alpha_i z(i_0 + i) \quad \text{für} \quad i > k - i_1\,.\end{cases}$$

Für die Darstellung der $w(i)$ in $z(j)$-Koordinaten ergibt sich insgesamt

$w(i) \backslash z(j)$	0	$\dots$	$i_0 - 1$	i_0	$i_0 + 1$	$i_0 + 2$	$\dots$	$i_1 - 1$	i_1	$i_1 + 1$	$i_1 + 2$	$\dots$	k
$w(0)$				α_0					$\alpha\beta_0$				
$w(1)$					α_1					$\alpha\beta_1$			
$w(2)$						α_2					$\alpha\beta_2$		
$\vdots$							$\ddots$					$\ddots$	
$w(k - i_1)$								$\ddots$					$\alpha\beta_{k-i_1}$
$w(k - i_1 + 1)$									$\ddots$				
$\vdots$										$\ddots$			
$\vdots$											$\ddots$		
$\vdots$												$\ddots$	
$w(k - i_0)$													α_{k-i_0}

Aus dieser Dreiecksgestalt und der Tatsache, daß die von 0 verschiedenen $z(i) \bmod M$ eine Basis von Sym_k/M bilden, folgt, daß die von 0 verschiedenen $w(i) \bmod M$ linear unabhängig sind. Da offensichtlich $w(i) \bmod M$ von 0 verschieden ist, falls $v(i,0) \bmod M$ von 0 verschieden ist oder $v(i,1) \bmod M$ von 0 verschieden ist, ist die Dimension des von den $w(i) \bmod M$ aufgespannten Vektorraums mindestens so groß wie die Dimension des von den $v(i,0) \bmod M$ aufgespannten Vektorraums und auch mindestens so groß wie die des Vektorraums, der von den $v(i,1) \bmod M$ aufgespannt wird. Dies bedeutet aber, daß die Dimension des von $m \bmod M$ erzeugten $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Moduls mindestens so groß ist wie die Dimension des von $m_1 \bmod M$ erzeugten Moduls und auch mindestens so groß wie die Dimension des von $m_2 \bmod M$ erzeugten Moduls. Folglich kann es nicht sein, daß einer der Höchstgewichtsvektoren $m_1 \bmod M$, $m_2 \bmod M$ nicht zulässig ist, wenn $m \bmod M$ zulässig ist. $\square$

Aus den bisherigen Resultaten folgt bereits eine starke strukturelle Aussage über die Sockelreihe der uns interessierenden Darstellungen.

Satz 3.6.13. *Sei $0 \leqslant k \leqslant q-2$. Die Moduln der $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Sockelreihe von Sym_k sind alle monomial. Jeder einfache Summand des $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Sockels von $\mathrm{Sym}_k/\mathrm{soc}^n(\mathrm{Sym}_k)$ wird von einem monomialen Höchstgewichtsvektor erzeugt. Die $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Sockelreihe ist auch die $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Sockelreihe.*

Beweis. Wir beweisen die Aussagen induktiv. Der Induktionsanfang ist durch Proposition 3.6.8 gesichert, die ja besagt, daß der Sockel von Sym_k einfach ist, von dem Monom X^k erzeugt wird und die Basis $\{X^{k-i}Y^i \mid 0 \leqslant i \leqslant k,\ i \preccurlyeq k\}$ hat.

Ist nun $\mathrm{soc}^n(\mathrm{Sym}_k)$ monomial, so sind nach den Propositionen 3.6.11 und 3.6.12 die zulässigen Höchstgewichtsvektoren zu einem festen Gewicht in $\mathrm{Sym}_k/\mathrm{soc}^n(\mathrm{Sym}_k)$ entweder monomial oder Linearkombination von zwei monomialen zulässigen Höchstgewichtsvektoren zum selben

Gewicht. Auf jeden Fall wird also der zu diesem Gewicht gehörende Anteil des Sockels von monomialen Höchstgewichtsvektoren erzeugt. Da $\mathrm{soc}^{n+1}(\mathrm{Sym}_k)$ vom Urbild dieser monomialen Höchstgewichtsvektoren zu allen Gewichten zusammen mit dem Urbild des monomialen Untermoduls $\mathrm{soc}^n(\mathrm{Sym}_k)$ erzeugt wird, ist auch $\mathrm{soc}^{n+1}(\mathrm{Sym}_k)$ monomial.

Daß die $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Sockelreihe mit der $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Sockelreihe übereinstimmt, liegt daran, daß alle auftretenden Moduln monomial und somit sowohl $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$- als auch $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln sind. $\square$

Neben dieser theoretischen Aussage sind wir nun auch in der Lage, einen leicht berechenbaren Algorithmus zur Bestimmung der Sockelreihe anzugeben. Zum einen müssen wir nur unter den monomialen Vektoren eines Quotienten $\mathrm{Sym}_k/\mathrm{soc}^n(\mathrm{Sym}_k)$ nach zulässigen Höchstgewichtsvektoren suchen, um $\mathrm{soc}^n(\mathrm{Sym}_k)$ zu $\mathrm{soc}^{n+1}(\mathrm{Sym}_k)$ zu erweitern. Hat man einen solchen zulässigen Höchstgewichtsvektor gefunden, so ist es aufgrund der Monomialität leicht, sein Erzeugnis bzw. das Erzeugnis seines Urbilds in Sym_k auszurechnen. Aufgrund der Monomialität von $\mathrm{soc}^n(\mathrm{Sym}_k)$ selbst und der daraus resultierenden einfachen Vektorraumstruktur von $\mathrm{Sym}_k/\mathrm{soc}^n(\mathrm{Sym}_k)$ wiederum ist es einfach, einen monomialen Vektor dieses Quotienten darauf zu testen, Höchstgewichtsvektor zu sein und auch der Test auf Zulässigkeit ist einfach. Wir fassen dies vor der Beschreibung des Algorithmus zur Bestimmung der Sockelreihe von Sym_k noch einmal zusammen.

PROPOSITION 3.6.14. *Sei $0 \leqslant k \leqslant q-2$ und M ein monomialer $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Untermodul von Sym_k mit Basis $\{X^{k-i}Y^i \mid i \in I_M\}$. Ein von 0 verschiedenes Element $X^{k-j}Y^j \bmod M$ aus Sym_k/M ist genau dann Höchstgewichtsvektor, wenn alle j' mit $j' \precneqq j$ in I_M liegen. In diesem Fall ist das Gewicht gerade $(0, \chi^{k-2j \bmod q-1})$, und der von $X^{k-j}Y^j \bmod M$ erzeugte $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul hat die Vektorraumbasis $\{X^{k-i}Y^i \bmod M \mid k-i \preccurlyeq k-j \text{ und } i \notin I_M\}$. Ist außerdem $\#\{i \mid 0 \leqslant i \leqslant k,\ k-i \preccurlyeq k-j,\ i \notin I_M\} = \prod_\nu (r_\nu+1)$, wobei $\sum_\nu r_\nu p^\nu$ die p-adische Darstellung des kleinsten nichtnegativen Repräsentanten von $k-2j \bmod q-1$ ist, so ist der Höchstgewichtsvektor auch zulässig. Als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul ist der zugehörige einfache Modul dann isomorph zu $S_{\underline{r}} = S_{(r_0,\dots,r_{e-1})}$, als $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul ist er isomorph zu $S_{\underline{r}} \otimes \Delta^j$.*

BEWEIS. Die Bedingung für die U-Invarianz von $X^{k-j}Y^j \bmod M$ folgt aus der Formel für die Operation von $\left(\begin{smallmatrix}1&t\\0&1\end{smallmatrix}\right)$ auf Monomen in Lemma 3.6.3. Da die Matrix $\left(\begin{smallmatrix}t&0\\0&t^{-1}\end{smallmatrix}\right)$ auf $X^{k-j}Y^j$ durch Multiplikation mit t^{k-2j} operiert und $\overline{U}w$ auf ganz Sym_k als Multiplikation mit 0 operiert, ist die U-Invarianz die einzige Bedingung, die ein monomiales Element erfüllen muß, um Höchstgewichtsvektor zu sein und in diesem Fall ist das Gewicht dann das behauptete. Daß der von einem solchen Höchstgewichtsvektor erzeugte $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul die angegebene Basis hat, folgt wie in Proposition3.6.4 aus der Tatsache, daß das $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Erzeugnis eines Höchstgewichtsvektors gleich dem U^{t}-Erzeugnis ist. Ist die Dimension des erzeugten Moduls gleich der Dimension des zu dem Gewicht gehörenden einfachen Moduls, so ist das Erzeugnis natürlich auch einfach und der Höchstgewichtsvektor zulässig.

Ein einfacher $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul, der als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul zum Gewicht $(0,\chi^{k-2j})$ gehört, d.h. als $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul isomorph zu $S_{(r_0,\dots,r_{e-1})}$ ist, muß als $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul isomorph zu $S_{(r_0,\dots,r_{e-1})}\otimes\Delta^m$ sein für ein m. Diese Zahl m ist dadurch festgelegt, daß $\left(\begin{smallmatrix} t & 0\\ 0 & 1\end{smallmatrix}\right)$ auf den U-Invarianten als Multiplikation mit $t^{v(\underline{r})+m}$ operiert. Im vorliegenden Fall liefert dies $k-j=v(\underline{r})+m$. Wegen $v(\underline{r})=k-2j \bmod q-1$ ist also $m=j \bmod q-1$. □

Aus der Proposition ergibt sich direkt der folgende Algorithmus zur Bestimmung der Sockelreihe von Sym_k für $k\leqslant q-2$.

Algorithmus 3.6.15. `Berechnung der Sockelreihe von` Sym_k `für` $0\leqslant k\leqslant q-2$:

1. $B:=\emptyset$, $n:=1$
2. `suche alle` j `mit` $0\leqslant j\leqslant k$ `und`
   (a) $j\notin B$
   (b) $\{i \mid 0\leqslant i\leqslant k,\ i\precneqq j\}\subseteq B$
   (c) $\#\{i \mid 0\leqslant i\leqslant k,\ k-i\preccurlyeq k-j\}=\prod_\nu(r_\nu+1)$, `wobei` $\sum_\nu r_\nu p^\nu$ `die` p`-adische Darstellung von` $k-2j \bmod q-1$ `ist.`
3. `Sei` J `die Menge der in 2. gefundenen` j`'s. Wurden in 2. keine solchen` j `gefunden, so ist der Algorithmus beendet.`
4. `Für jedes` $j\in J$ `sei` $B:=B\cup\{i \mid 0\leqslant i\leqslant k,\ k-i\preccurlyeq k-j\}$
5. $\mathrm{soc}^n(\mathrm{Sym}_k)$ `hat die Basis` $X^{k-i}Y^i$, $i\in B$. `Die einfachen` $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$`-Summanden des Quotienten` $\mathrm{soc}^n(\mathrm{Sym}_k)/\mathrm{soc}^{n-1}(\mathrm{Sym}_k)$ `sind gegeben durch die Gewichte` $(0,\chi^{k-2j})$, $j\in J$. `Der Exponent von` Δ `im zugehörigen einfachen` $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$`-Modul ist` j.
6. $n:=n+1$; `gehe zu 1.`

Zum Ende dieses Kapitels kehren wir noch einmal zu den Hauptreihendarstellungen zurück. Deren Sockelreihe haben wir mittels der nun berechenbaren Sockelreihe von symmetrischen Potenzen der natürlichen Darstellung zumindest abgeschätzt. Eine kleine Verbesserung dieser Abschätzung ergibt sich dadurch, daß man bei den konkreten Berechnungen weniger zugänglichen Hauptreihendarstellungen wenigstens den Sockel bestimmen kann.

Proposition 3.6.16. *Für $0<k\leqslant q-2$ ist der Sockel von $\mathrm{ind}_B^G(1,\chi^k)$ mit dem in Proposition 3.6.8 bestimmten Sockel des Untermoduls $\mathrm{Sym}_k\hookrightarrow\mathrm{ind}_B^G(1,\chi^k)$ identisch. Für $k=0$ ist $\mathrm{ind}_B^G(1,\chi^0)=\mathrm{ind}_B^G(1,1)\cong\mathbb{F}\oplus\mathrm{Sym}_{q-1}\cong\mathbb{F}\oplus S_{(p-1,\dots,p-1)}$ halbeinfach.*

BEWEIS. Wir betrachten zuerst den Fall $k = 0$. Aus Lemma 3.5.6 folgt die Existenz zweier $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$-Einbettungen $\mathrm{Sym}_0 \hookrightarrow \mathrm{ind}_B^G(1, \chi^0)$ und $\mathrm{Sym}_{q-1} \hookrightarrow \mathrm{ind}_B^G(1, \chi^{q-1})$. Da aber $\chi^0 = \chi^{q-1} = 1$ ist, hat $\mathrm{ind}_B^G(1, \chi^0)$ die beiden Untermoduln Sym_0 und Sym_{q-1}. Der erste ist der triviale eindimensionale $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$-Modul $\mathbb{F}$, also insbesondere einfach, der zweite hat nach Prop 3.6.8 den Untermodul $S_{(p-1,\dots,p-1)}$ und ist aus Dimensionsgründen schon gleich $S_{(p-1,\dots,p-1)}$, also auch einfach. Damit ist $\mathrm{ind}_B^G(1, 1)$ halbeinfach und isomorph zu $\mathbb{F} \oplus S_{(p-1,\dots,p-1)}$.

Sei nun also $k > 0$. Wir bestimmen zuerst wieder den Untervektorraum der U-Invarianten von $\mathrm{ind}_B^G(1, \chi^k)$. Dieser hat die Dimension 2 und wird von den beiden Funktionen

$$f_1 : \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto b^k$$

und

$$f_2 : \begin{pmatrix} a & c \\ b & d \end{pmatrix} \mapsto \begin{cases} d^k & \text{für } b = 0\,, \\ 0 & \text{für } b \neq 0\,, \end{cases}$$

erzeugt. Der Träger von f_1 ist offensichtlich $G - B$, der von f_2 ist B.

Daß diese Funktionen Elemente der induzierten Darstellung sind, rechnet man ebenso leicht nach wie die U-Invarianz. Daß sie den Vektorraum der U-Invarianten erzeugen, folgt daraus, daß sich jede U-invariante Funktion f aus $\mathrm{ind}_B^G(1, \chi^k)$ schreiben läßt als

$$f = f(w) \cdot f_1 + f(1_G) \cdot f_2\,.$$

Diese Gleichheit rechnen wir nun nach, zuerst auf B und dann auf $G - B = BwU$. Es ist

$$\begin{aligned} f(\begin{pmatrix} a & c \\ 0 & d \end{pmatrix}) &= f(\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \cdot 1_G) \\ &= (1, \chi^k)(\begin{pmatrix} a & c \\ 0 & 1 \end{pmatrix}) \cdot f(1_G) \\ &= d^k \cdot f(1_G) = f(1_G) \cdot f_2(\begin{pmatrix} a & c \\ 0 & d \end{pmatrix}) \\ &= f(w) f_1(\begin{pmatrix} a & c \\ 0 & d \end{pmatrix}) + f(1_G) f_2(\begin{pmatrix} a & c \\ 0 & d \end{pmatrix}) \end{aligned}$$

wie behauptet.

Weiter gilt

$$\begin{aligned} f(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} w \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}) &= (\begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} f)(\begin{pmatrix} a & c \\ 0 & b \end{pmatrix} w) \\ &= f(\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} w) \\ &= d^k f(w) \end{aligned}$$

und

$$\begin{aligned}(f(w)f_1+f(1_G)f_2)(\begin{pmatrix}a & c\\ 0 & d\end{pmatrix}w\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}) &= f(w)f_1(\begin{pmatrix}c & ct-a\\ d & dt\end{pmatrix})+f(1_G)f_2(\begin{pmatrix}c & ct-a\\ d & dt\end{pmatrix})\\ &= f(w)\cdot d^k+0=d^kf(w)\,.\end{aligned}$$

Daß die beiden Elemente f_1 und f_2 linear unabhängig sind, ist offensichtlich, also bilden sie eine Basis der U-Invarianten von $\mathrm{ind}_B^G(1,\chi^k)$.

Sei nun $\alpha f_1+\beta f_2$ ein beliebiges U-invariantes Element. Wenn es in einem einfachen $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Untermodul $S_{\underline{r}}\otimes\Delta^m$ von $\mathrm{ind}_B^G(1,\chi^k)$ liegen sollte, so müßte $\left(\begin{smallmatrix}a & 0\\ 0 & d\end{smallmatrix}\right)$ darauf als Multiplikation mit $a^{v(\underline{r})+m}d^m$ operieren. Nun operiert $\left(\begin{smallmatrix}a & 0\\ 0 & d\end{smallmatrix}\right)$ auf f_1 als Multiplikation mit a^k und auf f_2 als Multiplikation mit d^k. Aus den Gleichungen $\alpha a^{v(\underline{r})+m}d^m=\alpha a^k$ und $\beta a^{v(\underline{r})+m}d^m=\beta d^k$ folgt, daß nicht beide Koeffizienten α, β von 0 verschieden sein können.

Wir untersuchen jetzt also noch den von f_1 und den von f_2 erzeugten Modul. Nun ist das Bild von X^k unter der Einbettung $\mathrm{Sym}_k\hookrightarrow\mathrm{ind}_B^G(1,\chi^k)$ gerade die Funktion f_1, also ist der von f_1 erzeugte Modul isomorph zu dem von X^k erzeugten einfachen Sockel von Sym_k. Die Funktion f_2 hingegen erzeugt den $\mathbb{F}[B]$-Untermodul $(1,\chi^k)$ in $\mathrm{ind}_B^G(1,\chi^k)$ und somit ist der von f_2 erzeugte $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul die gesamte induzierte Darstellung. Der Sockel von $\mathrm{ind}_B^G(1,\chi^k)$ ist in diesem Fall also einfach und stimmt mit dem Sockel des Untermoduls Sym_k überein. $\square$

3.7. Der Zusammenhang mit $X(\mathfrak{p})$

Obwohl die in den letzten Abschnitten gewonnenen Resultate über Hauptreihendarstellungen von $\mathrm{GL}(2,\mathbb{F}_q)$ sowie von symmetrischen Potenzen der natürlichen Darstellung von eigenem Interesse sind, war unser ursprüngliches Ziel ja, Informationen über die Folge

$$0\to\mathcal{C}_{\mathrm{Siegel}}[p]\otimes\mathbb{F}\to\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}\to D_S^0/pD_S^0\otimes\mathbb{F}\to\mathcal{C}_{\mathrm{Siegel}}/p\mathcal{C}_{\mathrm{Siegel}}\otimes\mathbb{F}\to 0$$

von $\mathbb{F}[G(\mathfrak{p})]$-Moduln zu gewinnen. Zuerst beschreiben wir den Übergang der Quotientengruppe $G(\mathfrak{p})=\mathrm{GL}(2,A/\mathfrak{p})/\mathbb{F}_r^*$ zur Gruppe $\mathrm{GL}(2,\mathbb{F}_q)$ mit $q=\#A/\mathfrak{p}$. Dabei sieht man insbesondere, welche Rolle es spielt, wie sich die Größe des Restkörpers $\mathbb{F}_q=A/\mathfrak{p}$ aus dem Grad von $\mathfrak{p}$ und der Größe des Konstantenkörpers $\mathbb{F}_r$ zusammensetzt.

Wir betrachten dazu eine beliebige Gruppe G und eine normale Untergruppe H sowie einen algebraisch abgeschlossenen Körper k. Aus der Beschreibung einer Darstellung als Homomorphismus der Gruppe in die Automorphismengruppe eines Vektorraums ergibt sich direkt, daß Darstellungen von G/H dasselbe sind wie Darstellungen von G, bei denen H trivial operiert. Ist weiter $M\xrightarrow{f}N$ ein Homomorphismus von $k[G/H]$-Moduln, so ist f auch ein Morphismus zwischen M,N als $k[G]$-Moduln. Wir können die obige Folge also auch als Folge von $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln interpretieren. Die Zerlegung in zentrale isotypische Komponenten verhält sich dabei wie folgt.

Ist $\psi : Z(G/H) \to k^*$ ein k-wertiger Charakter des Zentrums von G/H, so liefert dieser durch Komposition mit der Restklassenabbildung von G nach G/H einen Charakter $Z(G) \to Z(G/H) \xrightarrow{\psi} k^*$ des Zentrums von G, der auf $H \cap Z(G)$ verschwindet. Im allgemeinen hat G natürlich mehr zentrale Charaktere als die, welche auf $Z(G) \cap H$ verschwinden. Bei der Zerlegung in zentrale isotypische Komponenten eines von einem $k[G/H]$-Modul M kommenden $k[G]$-Moduls spielen aber nur Charaktere von $Z(G)$ eine Rolle, die auf $Z(G) \cap H$ verschwinden. Ist nämlich ψ ein Charakter von $Z(G)$ und $M(\psi) \neq 0$, so ergibt sich für $M \ni m \neq 0$ und $z \in Z(G) \cap H$ gerade $m = zH \cdot m = z \cdot M = \psi(z) \cdot m$ und damit $\psi(z) = 1$. Die Zerlegung eines $k[G/H]$-Moduls M in zentrale isotypische Komponenten stimmt also mit der des entsprechenden Zerlegung von M als $k[G]$-Modul überein.

In dem von uns in Kapitel 2 betrachteten Fall ist $G = \mathrm{GL}(2, \mathbb{F}_q)$ und $H = \mathbb{F}_r^*$, d.h. es gilt schon $H \subseteq Z(G)$ und damit spielen nur Charaktere von $\mathrm{GL}(2, \mathbb{F}_q)$ eine Rolle, die auf $\mathbb{F}_r^*$ verschwinden.

Wir untersuchen nun noch, wie sich der Übergang zu Quotientengruppen bei Induktion verhält.

Proposition 3.7.1. *Seien G eine endliche Gruppe und seien $U \subseteq H$ Untergruppen, wobei U normal in G und H ist. Sei weiter M ein $k[H/U]$-Modul. Dann ist $\mathrm{ind}_{H/U}^{G/U} M$ auch ein $k[G]$-Modul und M auch ein $k[H]$-Modul und es gibt einen $k[G]$-Modul-Isomorphismus $\mathrm{ind}_{H/U}^{G/U} M \cong \mathrm{ind}_H^G M$.*

Beweis. Wir haben

$$\mathrm{ind}_H^G(M) = \{\tilde{f} : G \to M \mid \tilde{f}(hg) = h \cdot \tilde{f}(g) = hU \cdot \tilde{f}(g)\}$$

und

$$\mathrm{ind}_{H/U}^{G/U}(M) = \{f : G/U \to M \mid f(hU \cdot gU) = hU \cdot f(gU)\}\,.$$

Da der Index von H in G gleich dem Index von H/U in G/U ist, haben beide Moduln die gleiche k-Dimension. Ein $k[G]$-Modul-Isomorphismus ist gegeben durch

$$\mathrm{ind}_{H/U}^{G/U}(M) \ni f \mapsto \tilde{f} \in \mathrm{ind}_H^G(M) \text{ mit } \tilde{f}(g) = f(gU)\,.$$

Wir zeigen zuerst die Wohldefiniertheit der Abbildung. Für $h \in H$, $g \in G$ und $f \in \mathrm{ind}_{H/U}^{G/U}(M)$ ist

$$\tilde{f}(hg) = f(hgU) = f(hU \cdot gU) = hU \cdot f(gU) = h \cdot \tilde{f}(g)\,,$$

also liegt $\tilde{f}$ wirklich in $\mathrm{ind}_H^G(M)$.

Nun rechnen wir die Homomorphie-Eigenschaft nach. Seien $g, x \in G$ und $f \in \mathrm{ind}_{H/U}^{G/U}(M)$. Dann gilt

$$\widetilde{(g \cdot f)}(x) = (g \cdot f)(xU) = (gU \cdot f)(xU) = f(xU \cdot gU) = f(xgU)$$

und

$$(g\cdot\tilde{f})(x)=\tilde{f}(x\cdot g)=f(xgU)\,.$$

Die Injektivität ist wegen $f(gU)=\tilde{f}(g)$ offensichtlich und aus Dimensionsgründen ergibt sich ein $k[G]$-Modul-Isomorphismus. □

Wir benötigen außerdem noch die folgende Aussage über das Verhalten von Induktion bei direkten Produkten von Gruppen.

LEMMA 3.7.2. *Für zwei endliche Gruppen G und H sowie einen $k[H]$-Modul M gilt $\mathrm{ind}_H^{G\times H}M\cong M\otimes_k k[G]$, wobei die $G\times H$-Operation rechts gegeben ist durch $(g,h)\cdot m\otimes x=gm\otimes hx$.*

BEWEIS. Als Modul über sich selbst ist $k[G\times H]$ durch die Abbildung $(g,h)\mapsto g\otimes h$ isomorph zu $k[G]\otimes_k k[H]$ mit der Operation $(g,h)\cdot g'\otimes h'=gg'\otimes hh'$. Folglich ist $\mathrm{ind}_H^{G\times H}M=k[G\times H]\otimes_{k[H]}M\cong(k[G]\otimes_k k[H])\otimes_{k[H]}M\cong k[G]\otimes_k(k[H]\otimes_{k[H]}M)=k[G]\otimes_k M$. □

Nach diesen allgemeinen Bemerkungen kommen wir jetzt wieder auf die spezielle Situation von Kapitel 2 zurück. Zur Vereinfachung der Notation verwenden wir folgende Bezeichnungen. Es sei $G=\mathrm{GL}(2,\mathbb{F}_q)$ mit $\mathbb{F}_q=A/\mathfrak{p}$. Weiter sei $B=\{\left(\begin{smallmatrix}a&c\\0&d\end{smallmatrix}\right)\in G\}$ die Borel-Untergruppe sowie $E=\{\left(\begin{smallmatrix}a&c\\0&d\end{smallmatrix}\right)\in G\,\big|\,a\in\mathbb{F}_r^*\}$ und $F=\{\left(\begin{smallmatrix}a&c\\0&d\end{smallmatrix}\right)\in G\,\big|\,d\in\mathbb{F}_r^*\}$. Außerdem schreiben wir $Z=(A/\mathfrak{p})^*$ für das Zentrum von G und $W=\mathbb{F}_r^*\subseteq Z$. Dann ist $G(\mathfrak{p})=G/W$ mit Zentrum Z/W. Die in den Propositionen 2.2.7 und 2.3.9 aufgetretenen Darstellungen waren die $\mathbb{F}[G/W]$-Moduln $\mathrm{ind}_{E/W}^{G/W}\mathbb{F}(\chi)$ und $\mathrm{ind}_{F/W}^{G/W}\mathbb{F}(\psi)$ für einen Charakter ψ von Z/W. Die folgende Proposition besagt, daß diese Moduln als $\mathbb{F}[G]$-Moduln betrachtet zu den Hauptreihendarstellungen gehören.

PROPOSITION 3.7.3. *Unter Verwendung der oben eingeführten Notation gibt es $\mathbb{F}[G]$-Modul-Isomorphismen $\mathrm{ind}_{E/W}^{G/W}\mathbb{F}(\psi)=\mathrm{ind}_B^G(\psi,1)$ und $\mathrm{ind}_{F/W}^{G/W}\mathbb{F}(\psi)=\mathrm{ind}_B^G(1,\psi)$.*

BEWEIS. Aus der Transitivität der Induktion ergibt sich $\mathrm{ind}_{E/W}^{G/W}\mathbb{F}=\mathrm{ind}_{B/W}^{G/W}\mathrm{ind}_{E/W}^{B/W}\mathbb{F}$. Für die Gruppe B/W gibt es eine direkte Produktzerlegung $B/W\cong Z/W\times E/W$. Aus Lemma 3.7.2 erhält man einen $\mathbb{F}[B/W]$-Isomorphismus $\mathrm{ind}_{E/W}^{B/W}\mathbb{F}\cong\mathbb{F}[Z/W]\otimes_{\mathbb{F}}\mathbb{F}$, wobei ein bezüglich $B/W=Z/W\times E/W$ zerlegtes Element $B/W\ni b=z\cdot e$ auf $\mathbb{F}[Z/W]\otimes_{\mathbb{F}}\mathbb{F}$ durch $b\cdot\alpha\otimes\beta=z\cdot\alpha\otimes e\cdot\beta$ operiert. Da $\mathbb{F}$ aber der triviale $\mathbb{F}[E/W]$-Modul ist, ergibt sich, daß Elemente aus B/W auf $\mathbb{F}[Z/W]\otimes_{\mathbb{F}}\mathbb{F}$ nur durch ihre Z/W-Komponente operieren.

Da die Ordnung von Z/W ja p-frei ist, zerlegt sich der $\mathbb{F}[Z/W]$-Modul $\mathbb{F}[Z/W]$ in eine direkte Summe einfacher Moduln. Da Z/W abelsch ist, sind die einfachen $\mathbb{F}[Z/W]$-Moduln alle eindimensional und jeder kommt mit Vielfachheit eins in $\mathbb{F}[Z/W]$ vor. Identifizieren wir

Charaktere von Z/W mit den dazu gehörenden eindimensionalen Darstellungen, so gilt $\mathbb{F}[Z/W] = \bigoplus_{\substack{\varphi \text{ Charakter} \\ \text{von } Z/W}} \varphi$. Ist nun ψ ein fester zentraler Charakter von G/W, so ergibt sich

$$\mathrm{ind}_{E/W}^{G/W} \mathbb{F}(\psi) = \mathrm{ind}_{B/W}^{G/W}(\mathbb{F}[Z/W] \otimes_{\mathbb{F}} \mathbb{F})(\psi) = \mathrm{ind}_{B/W}^{G/W}\Big(\bigoplus_{\substack{\varphi \text{Charakter} \\ \text{von } Z/W}} \varphi \otimes_{\mathbb{F}} \mathbb{F})(\psi)\,.$$

Nun ist offensichtlich $(\bigoplus_{\substack{\varphi \text{Charakter} \\ \text{von } Z/W}} \varphi \otimes_{\mathbb{F}} \mathbb{F})(\psi) = \psi \otimes_{\mathbb{F}} \mathbb{F}$. Dies ist eine eindimensionale Darstellung von B/W, auf der $\left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \bmod W$ durch Multiplikation mit $\psi(a)$ operiert. Als $\mathbb{F}[B]$-Modul aufgefaßt ist diese Darstellung isomorph zu der eindimensionalen Darstellung $(\psi, 1)$ aus Definition 3.5.3. Mit Proposition 3.7.1 ergibt sich also, daß $\mathrm{ind}_{E/W}^{G/W} \mathbb{F}(\psi)$ als $\mathbb{F}[G]$-Modul aufgefaßt isomorph ist zu der Hauptreihendarstellung $\mathrm{ind}_B^G(\psi, 1)$.

Für die Gruppe F an Stelle von E argumentiert man entsprechend. $\square$

Wendet man obiges Ergebnis auf die Darstellungen aus den Propositionen 2.2.7 und 2.3.9 an, so ergibt sich für die zu der Modulkurve $X(\mathfrak{p})$ gehörenden Galois-Moduln nun direkt folgendes.

KOROLLAR 3.7.4. *Seien ψ ein nichttrivialer Charakter des Zentrums von $G(\mathfrak{p})$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$ sowie $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ als $\mathbb{F}[G] = \mathbb{F}[\mathrm{GL}(2, A/\mathfrak{p})]$-Moduln aufgefaßt. Dann gibt es $\mathbb{F}[G]$-Modul-Isomorphismen*

$$(D_S^0/pD_S^0 \otimes \mathbb{F})(\psi) \cong \mathrm{ind}_B^G(\psi, 1)$$

und

$$(\mathcal{S}/p\mathcal{S} \otimes \mathbb{F})(\psi) \cong \mathrm{ind}_B^G(1, \psi)\,.$$

KAPITEL 4

Ergebnisse

Aufgrund der Ergebnisse des vorigen Kapitels sind wir in der Lage, die Sockelreihe mitsamt den dazu gehörenden Quotienten für alle $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln Sym_k mit $0 \leqslant k \leqslant q$ zu berechnen. Da wir außerdem die zentralen isotypischen Komponenten der uns interessierenden Galois-Moduln $\mathcal{S}/p\mathcal{S}$ und D_S^0/pD_S^0 als Hauptreihendarstellungen identifiziert haben und diese mittels symmetrischer Potenzen der natürlichen Darstellung und deren Dualen zerlegen können, ergeben sich auch Informationen über die Sockelreihen von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$. Mittels dieser Informationen kann man dann auf die Struktur von $\mathcal{C}_{\mathrm{Siegel}}[p] \otimes \mathbb{F}$ und $\mathcal{C}_{\mathrm{Siegel}}/p\mathcal{C}_{\mathrm{Siegel}} \otimes \mathbb{F}$ schließen und insbesondere untere Abschätzungen für die Gruppenordnung von $\mathcal{C}_{\mathrm{Siegel}}[p]$ und $\mathcal{C}_{\mathrm{Siegel}}/p\mathcal{C}_{\mathrm{Siegel}}$ angeben. Sowohl bei der Untersuchung der Sockelreihe der Sym_k als auch bei der Betrachtung der Galois-Moduln der Modulkurve werden wir zum einen konkrete Beispiele berechnen, darüber hinaus aber auch in der Lage sein, Aussagen allgemeiner Art zu beweisen.

4.1. Beispiele für Sockelreihen

Wir rechnen im folgenden mit Hilfe von Algorithmus 3.6.15 zwei Beispiele vollständig von Hand durch. Um die Funktionsweise des Algorithmus bestmöglich zu verdeutlichen, werden wir dabei keine sich aus der Theorie ergebenden zusätzlichen Informationen benutzen, wie etwa die Tatsache, daß ein von Null verschiedener $\mathbb{F}[\mathrm{SL}(2,\mathbb{F}_q)]$-Modul immer mindestens einen Höchstgewichtsvektor haben muß.

Da die p-adische Darstellung von Zahlen für den Algorithmus ja eine wesentliche Rolle spielt, schreiben wir im folgenden für eine natürliche Zahl $i \leqslant q-1 = p^e - 1$ mit p-Entwicklung $i = i_0 + i_1 p + \ldots + i_{e-1}p^{e-1}$ auch $i = (i_0, \ldots, i_{e-1})$. Manchmal geben wir dabei auch die Nummer einer Stelle in eckigen Klammern an, wie z.B. bei $p^n = (0, \ldots, 0, 1\,[n], 0, \ldots, 0)$. Auch bei den Elementen $\underline{r} \in I$, die als Indizes von einfachen Moduln $S_{\underline{r}}$ vorkommen, tun wir dies gelegentlich. Für die Ordnungsrelation $\preccurlyeq$ spielt es dabei keine Rolle, ob Tupel $(i_0, \ldots, i_{e-1})$ als Elemente von I oder als p-adische Darstellung natürlicher Zahlen interpretiert werden. Weiter nennen wir die Zahl $\prod_\nu (i_\nu + 1)$ das p-adische Querprodukt von i.

Beispiel 4.1.1. Als erstes wählen wir $p = 3$, $q = 3^3 = 27$ und untersuchen den $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul Sym_9. Zu Beginn des Algorithmus ist $B = \emptyset$ die Basis des Null-Moduls $\mathrm{soc}^0(\mathrm{Sym}_9)$. Wir suchen Zahlen j zwischen 0 und $k = 9$, welche die drei Bedingungen a), b) und c) des Algorithmus erfüllen:

a) $j \notin B$

b) $\{i \,\big|\, 0 \leqslant i \leqslant k,\, i \precneqq j\} \subseteq B$

c) $\#\{i \,\big|\, 0 \leqslant i \leqslant k,\, k-i \preccurlyeq k-j\}$ gleich dem p-adischen Querprodukt von $k - 2j \bmod q - 1$.

Bedingung a) ist noch leer, da $B = \emptyset$ ist. Bedingung b) fordert, daß es keine $0 \leqslant i \leqslant k$ mit $i \precneqq j$ geben darf. Dies ist offensichtlich nur für $j = 0$ erfüllt. Die potentielle Dimension des zugehörigen einfachen Moduls ist das p-adische Querprodukt von $k - 2j = k = (0, 0, 1)$, also gleich 2. Die tatsächliche Dimension des Erzeugnisses des Hauptgewichtsvektors ist $\#\{i \,\big|\, 0 \leqslant i \leqslant k,\, i \notin B$ und $i' := k - i \preccurlyeq k - j\}$. Wegen $k - j = k = (0, 0, 1)$ gibt es genau zwei Zahlen i' mit $i' \preccurlyeq k - j$, nämlich $i' = 0 = (0, 0, 0)$ und $i' = 9 = (0, 0, 1)$, und wegen $B = \emptyset$ liegt das jeweilige $i = k - i'$ nicht in B. Somit ist $X^{k-j}Y^j = X^9Y^0$ zulässiger Höchstgewichtsvektor. Der Sockel von Sym_9 ist also einfach, isomorph zu $S_{(0,0,1)} \otimes \Delta^0$ und hat die Basis $\{X^9Y^0, X^0Y^9\}$, d.h. jetzt ist $B = \{0, 9\}$.

Im zweiten Durchlauf des Algorithmus sind jetzt für j noch die Werte $1 = (1, 0, 0)$, $2 = (2, 0, 0)$, $3 = (0, 1, 0)$, $4 = (1, 1, 0)$, $5 = (2, 1, 0)$, $6 = (0, 2, 0)$, $7 = (1, 2, 0)$ und $8 = (2, 2, 0)$ möglich. Davon bestehen nur 1 und 3 den Test in b) . Die einzige Möglichkeit für i mit $i \precneqq 1$ oder $i \precneqq 3$ ist nämlich $i = 0$ und 0 liegt schon in B. Die anderen Kandidatenerfüllen Bedingung b) nicht, bei 2 gibt es z.B. $1 = (1, 0, 0) \precneqq (2, 0, 0) = 2$ mit $1 \notin B$.

Wir testen nun die Bedingung c) bei den beiden Möglichkeiten für j. Im Falle $j = 1$ besteht die Menge der i' mit $i' = k - i \preccurlyeq k - j = 8 = (2, 2, 0)$ aus den Elementen $0, \ldots, 8$ und die Menge der zugehörigen $i = k - i'$ aus den Elementen $1, \ldots, 9$. Davon liegen 8 Stück nicht in B. Da die p-adische Querprodukt von $k - 2j = 7 = (1, 2, 0)$ aber nur 6 beträgt, ist der zu $j = 1$ gehörende Höchstgewichtsvektor $X^{9-1}Y^1 \bmod \mathrm{soc}^1(\mathrm{Sym}_9)$ nicht zulässig. Im Fall $j = 3$ besteht die Menge der i' mit $i' \preccurlyeq k - j = 6 = (0, 2, 0)$ aus den Elementen $0 = (0, 0, 0)$, $3 = (0, 1, 0)$ und $6 = (0, 2, 0)$. Von den $i = k - i'$ liegen 2 Stück noch nicht in B, nämlich $i = 3$ und $i = 6$. Da das p-adische Querprodukt von $k - 2j = 3 = (0, 1, 0)$ gleich 2 ist, ist der Vektor $X^6Y^3 \bmod \mathrm{soc}^1(\mathrm{Sym}_9)$ zulässiger Höchstgewichtsvektor von $\mathrm{Sym}_9/\mathrm{soc}^1(\mathrm{Sym}_9)$. Es ist $\mathrm{soq}^2(\mathrm{Sym}_9) \cong \mathrm{S}_{(0,1,0)} \otimes \Delta^3$ und $\mathrm{soc}^2(\mathrm{Sym}_9)$ hat die Basis $\{X^9Y^0, X^0Y^9, X^6Y^3, X^3Y^6\}$, d.h. es ist jetzt $B = \{0, 3, 6, 9\}$.

Im dritten Durchlauf bleiben für j noch die Werte $1 = (1, 0, 0)$, $2 = (2, 0, 0)$, $4 = (1, 1, 0)$, $5 = (2, 1, 0)$, $7 = (1, 2, 0)$ und $8 = (2, 2, 0)$. Von diesen besteht nur $j = 1$ den Test in b). Die Bedingung $i' \preccurlyeq k - j = 8 = (2, 2, 0)$ erfüllen die $i' = 0, \ldots, 8$. Von den entsprechenden Werten $1, \ldots, 9$ für $i = k - i'$ liegen 6 Stück noch nicht in B, nämlich

$1, 2, 4, 5, 7, 8$. Da das p-adische Querprodukt von $k - 2j = 7 = (1, 2, 0)$ gerade 6 beträgt, ist $X^8Y^1 \bmod \mathrm{soc}^2(\mathrm{Sym}_9)$ zulässiger Höchstgewichtsvektor von $\mathrm{Sym}_9/\mathrm{soc}^2(\mathrm{Sym}_9)$. Damit ist $\mathrm{soq}^3(\mathrm{Sym}_9) = S_{(1,2,0)} \otimes \Delta^1$ und $\mathrm{soc}^3(\mathrm{Sym}_9)$ hat die Basis $\{X^9Y^0, X^0Y^9, X^6Y^3, X^3Y^6, X^8Y^1, X^7Y^2, X^5Y^4, X^4Y^5, X^2Y^7, X^1Y^8\}$, d.h. $\mathrm{soc}^3(\mathrm{Sym}_9) = \mathrm{Sym}_9$ und im nächsten Durchlauf bricht der Algorithmus ab, da $B = \{0, \dots, 9\}$ ist.

Wir fassen das Ergebnis zusammen. Der $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_{27})]$-Modul Sym_9 ist uniseriell, hat die Länge 3 und die Faktoren $\mathrm{soq}^1(\mathrm{Sym}_9) \cong S_{(0,0,1)} \otimes \Delta^0$, $\mathrm{soq}^2(\mathrm{Sym}_9) \cong S_{(0,1,0)} \otimes \Delta^3$, $\mathrm{soq}^3(\mathrm{Sym}_9) \cong S_{(1,2,0)} \otimes \Delta^1$.

Beispiel 4.1.2. Als nächstes betrachten wir Sym_{12}, immer noch mit $q = 27$. Der erste Durchlauf beginnt so wie beim vorigen Beispiel, es kommt nur $j = 0$ in Frage. Wegen $k - 2j = 12 = (0, 1, 1)$ ist der Sockel $\mathrm{soc}^1(\mathrm{Sym}_{12})$ isomorph zu $S_{(0,1,1)} \otimes \Delta^0$. Die Menge der $i' \preccurlyeq k - j = (0, 1, 1)$ besteht aus den Elementen $12 = (0, 1, 1)$, $9 = (0, 0, 1)$, $3 = (0, 1, 0)$ und $0 = (0, 0, 0)$, also hat $\mathrm{soc}^1(\mathrm{Sym}_{12})$ die Basis $\{X^{12}Y^0, X^9Y^3, X^3Y^9, X^0Y^{12}\}$.

Zu Beginn des zweiten Durchlaufs ist $B = \{0, 3, 9, 12\}$. Für j kommen jetzt also noch $1 = (1, 0, 0)$, $2 = (2, 0, 0)$, $4 = (1, 1, 0)$, $5 = (2, 1, 0)$, $6 = (0, 2, 0)$, $7 = (1, 2, 0)$, $8 = (2, 2, 0)$, $10 = (1, 0, 1)$ und $11 = (2, 0, 1)$ in Frage. Davon bestehen 1 und 6 den Test in b).

Für $j = 1$ besteht die Menge der i' mit $i' \preccurlyeq k - j = 11 = (2, 0, 1)$ aus den 6 Elementen $0 = (0, 0, 0)$, $1 = (1, 0, 0)$, $2 = (2, 0, 0)$, $9 = (0, 0, 1)$, $10 = (1, 0, 1)$ und $11 = (2, 0, 1)$. Von den entsprechenden $i = k - i' = 1, 2, 3, 10, 11, 12$ liegen 4 Stück noch nicht in B. Da das p-adische Querprodukt von $k - 2j = 10 = (1, 0, 1)$ gerade 4 beträgt, ist der zu $j = 1$ gehörende Höchstgewichtsvektor $X^{11}Y^1 \bmod \mathrm{soc}^1(\mathrm{Sym}_{12})$ von $\mathrm{Sym}_{12}/\mathrm{soc}^1(\mathrm{Sym}_{12})$ zulässig. Der dazu gehörende einfache Modul ist $S_{(1,0,1)} \otimes \Delta^1$, in $\mathrm{Sym}_{12}/\mathrm{soc}^1(\mathrm{Sym}_{12})$ wird er erzeugt von den Klassen der Vektoren $X^{11}Y^1$, $X^{10}Y^2$, X^2Y^{10} und X^1Y^{11}.

Für $j = 6$ besteht die Menge der $i' \preccurlyeq k - j = 6 = (0, 2, 0)$ aus den Elementen $0, 3$ und 6 und die entsprechenden i sind $0, 6$ und 9. Davon liegt nur 6 noch nicht in B. Da das p-adische Querprodukt von $k - 2j = 0$ gleich 1 ist, ergibt sich ein weiterer einfacher Faktor von $\mathrm{soq}^2(\mathrm{Sym}_{12})$, der isomorph ist zu $S_{(0,0,0)} \otimes \Delta^6$ und von der Klasse von X^6Y^6 erzeugt wird.

Als Basis von $\mathrm{soc}^2(\mathrm{Sym}_{12})$ ergibt sich $\{X^{12}Y^0, X^9Y^3, X^3Y^9, X^0Y^{12}, X^{11}Y^1, X^{10}Y^2, X^2Y^{10}, X^1Y^{11}, X^6Y^6\}$ und somit ist $B = \{0, 1, 2, 3, 6, 9, 10, 11, 12\}$. Der zweite Quotient $\mathrm{soq}^2(\mathrm{Sym}_{12})$ ist nicht einfach und isomorph zu $(S_{(1,0,1)} \otimes \Delta^1) \oplus (S_{(0,0,0)} \otimes \Delta^6)$.

Im dritten Durchlauf bleiben für j noch die möglichen Werte $4 = (1, 1, 0)$, $5 = (2, 1, 0)$, $7 = (1, 2, 0)$ und $8 = (2, 2, 0)$. Die Bedingung b) des Algorithmus wird nur von $j = 4$ erfüllt. Die Menge der i' mit $i' \preccurlyeq k - j = 8 = (2, 2, 0)$ enthält $0, 1, 2, 3, 4, 5, 6, 7$ und 8. Davon liegen 4 Elemente noch nicht in B. Dies ist auch die richtige Anzahl, da das p-adische Querprodukt von $k-2j=4=(1,1,0)$ auch 4 ist. Es ergibt sich der dritte und letzte Quotient der Sockelreihe von Sym_{12} als $\mathrm{soq}^3(\mathrm{Sym}_{12}) \cong S_{(1,1,0)} \otimes \Delta^4$.

Die beiden Beispiele oben zeigen insbesondere, daß es unter den Sym_k sowohl uniserielle als auch nicht uniserielle Exemplare gibt. Obwohl es etwas umständlich ist, Beispiele von Hand auszurechnen, läßt sich der Algorithmus sehr leicht implementieren und arbeitet auch für größere Beispiele in akzeptabler Zeit. Für $p=5$ und $q=5^7=78125$ dauert die Berechnung der Sockelreihe von Sym_k für $k=21457=(1,2,3,4,3,2,1)$ beispielsweise ca. 100 Sekunden.

Als nächstes untersuchen wir den Ablauf des Algorithmus im allgemeinen Fall. Im Gegensatz zu einzelnen konkreten Beispielen, bei denen der Algorithmus leicht auszuführen ist, sind allgemeine Aussagen deutlich schwieriger. Dies liegt daran, daß für die im Algorithmus auftretende Zahlen i sowohl $\preccurlyeq$-Relationen mit i als auch mit $k-i$ vorkommen, und bei allgemeinem k aus den p-adischen Koeffizienten von i keine explizite Information über die p-adischen Koeffizienten von $k-i$ abgeleitet werden können, da man nicht weiß, welche Überträge auftreten.

Einige allgemeine Aussagen lassen sich aber doch machen. In den berechneten Beispielen sieht man beispielsweise, daß in den Sym_k kein einfacher Faktor mehrfach auftritt. Dies ist ein ganz unmittelbare Folge aus der Bestimmung der Sockelreihe von Sym_k mittels des Algorithmus.

SATZ 4.1.3. *Die einfachen Faktoren eines* $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$*-Moduls* Sym_k *mit* $0 \leqslant k \leqslant q$ *besitzen alle die Vielfachheit* 1.

BEWEIS. Bei $k=q-1$ und $k=q$ ist das trivial, da Sym_{q-1} selbst einfach ist und $\mathrm{Sym}_q \cong \mathbb{F} \otimes S_{(p-1,\dots,p-1)}$ gilt. Im Fall $k<q-1$ erhält man die einfachen Faktoren von Sym_k mittels des Algorithmus als Moduln $S_{\underline{r}} \otimes \Delta^j$ mit paarweise verschiedenen j aus $\{0,\dots,k\}$. Diese j sind also paarweise inkongruent modulo $q-1$ und folglich sind die $S_{\underline{r}} \otimes \Delta^j$ paarweise nichtisomorph. □

Auch die ersten beiden Durchläufe des Algorithmus sind noch ziemlich überschaubar.

SATZ 4.1.4. *Sei* $q=p^e$ *und* $0 \leqslant k=(k_0,\dots,k_{e-1}) \leqslant q-2$. *Der Sockel des* $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$*-Moduls* Sym_k *ist einfach und isomorph zu* $S_{(k_0,\dots,k_{e-1})} \otimes \Delta^0$. *Der zweite Quotient* $\mathrm{soq}^2(\mathrm{Sym}_k)$ *der Sockelreihe hat höchstens* $e-1$ *einfache Faktoren.*

BEWEIS. Die Aussage über den Sockel haben wir schon in Proposition 3.6.8 gezeigt. Beim ersten Durchlauf des Algorithmus ergibt sich dies wie folgt. Zu Beginn ist B leer und das einzige j, welches Bedingung b) erfüllt, ist $j=0$. Die Menge $\{i \mid 0 \leqslant i \leqslant k,\, i \notin B \text{ und } k-i \preccurlyeq k-j\} = \{i \mid 0 \leqslant i \leqslant k,\, i \preccurlyeq k\}$ hat genau soviele Elemente, wie die

p-adische Querprodukt von $k - j = k$ angibt. Es ergibt sich also als Sockel ein zu $S_{(k_0,\dots,k_{e-1})} \otimes \Delta^0$ isomorpher Modul, der eine aus den $X^{k-i}Y^i$ mit $i \preccurlyeq k$ bestehende Basis besitzt. Zu Beginn des zweiten Durchlaufs ist daher $B = \{i \,\big|\, i \preccurlyeq k\}$ und es werden Zahlen j zwischen 0 und k gesucht, die nicht in B liegen (Bedingung a)), d.h. die nicht $\preccurlyeq k$ sind, für die aber alle i mit $i \precnsim j$ schon in B liegen (Bedingung c)), d.h. $i \preccurlyeq k$ erfüllen. Nun bedeutet $j \not\preccurlyeq k$ gerade, daß mindestens eine Ziffer der p-adischen Darstellung von j die entsprechende Ziffer von k um mindestens 1 überschreitet. Daß für ein solches j jedes i mit $i \precnsim k$ schon $i \preccurlyeq k$ erfüllen soll, bedeutet, daß genau eine Ziffer von j exakt um 1 größer ist als die entsprechende Ziffer in k und daß alle anderen Ziffern von j gleich 0 sind. Da ja $j \leqslant k$ sein muß, kommt die höchste Ziffer dafür nicht in Frage und es gibt höchstens $e-1$ Möglichkeiten für ein solches j, nämlich die $j = (k_\nu + 1)p^\nu$ mit $0 \leqslant \nu \leqslant e-2$ und $k_\nu + 1 \leqslant p-1$. Diese j gehören zu Höchstgewichtsvektoren. Ob diese Höchstgewichtsvektoren zulässig sind, hängt davon ab, ob das entsprechende j auch Bedingung c) erfüllt. Jedenfalls ist die Zahl der zulässigen Höchstgewichtsvektoren von $\mathrm{Sym}_k/\mathrm{soc}^1(\mathrm{Sym}_k)$ und damit die Anzahl der einfachen Faktoren dieses Moduls nach oben abgeschätzt durch $e-1$. $\square$

Für den einfachsten nichttrivialen Fall $q = p^2$ ergibt sich sogar ein vollständiges Resultat.

Satz 4.1.5. *Sei $q = p^2$ und $0 \leqslant k \leqslant q-2$.*

1. *Ist $k \leqslant p-1$, so ist $\mathrm{Sym}_k \cong S_{(k,0)} \otimes \Delta^0$ einfach.*
2. *Ist $k = (p-1, k_1)$ mit $k_1 > 0$, so ist $\mathrm{Sym}_k \cong S_{(p-1,k_1)} \otimes \Delta^0$ einfach.*
3. *Ist $k = (k_0, k_1)$ mit $k_0 < p-1$ und $k_1 > 0$, so ist $\mathrm{soc}^1(\mathrm{Sym}_k) \cong S_{(k_0,k_1)} \otimes \Delta^0$ und $\mathrm{soc}^2(\mathrm{Sym}_k) = \mathrm{Sym}_k$ mit $\mathrm{soq}^2(\mathrm{Sym}_k) \cong S_{(p-k_0-2,k_1-1)} \otimes \Delta^{k_0+1}$.*

Insbesondere sind hier alle Sym_k uniseriell.

Beweis. Die erste Teil des Satzes ist klar, da Sym_k bei $k \leqslant p-1$ ja schon als $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_p)]$-Modul einfach ist. Wie im vorigen Satz ergibt sich im Teil 2 und 3 der Sockel als $S_{(k_0,k_1)} \otimes \Delta^0$. Die Dimension des Sockels ist $(k_0 + 1\ )\cdot(k_1 + 1)$. Ist $k_0 = p-1$, so hat der Sockel die Dimension $p \cdot (k_1 + 1)$ und der Modul Sym_k selbst hat die Dimension $k + 1 = k_0 + k_1 \cdot p + 1 = p + k_1 \cdot p = p \cdot (k_1 + 1)$ und stimmt deshalb schon mit seinem Sockel überein.

Ist $k_0 \leqslant p-2$, so ist die Dimension von Sym_k größer als die Dimension seines Sockels. Nach Satz 4.1.4 ist der zweite Quotient $\mathrm{soq}^2(\mathrm{Sym}_k)$ der Sockelreihe einfach. Im zweiten Durchlauf des Algorithmus wird also nur ein j die Bedingungen a), b) und c) erfüllen, und zwar $j = k_0 + 1$. Wegen $k - 2j = k_0 + k_1 p - 2k_0 - 2 = k_1 p - k_0 - 2 = (k_1 - 1)p + p - k_0 - 2 = (p - k_0 - 2, k_1 - 1)$ gehört zu diesem j der einfache

Modul $S_{(p-k_0-2,k_1-1)} \otimes \Delta^{k_0+1}$. Dieser hat die Dimension $(p-k_0-1)\cdot k_1$. Die Summe dieser Dimension und der Dimension des Sockels ergibt $(p-k_0-1)\cdot k_1+(k_0+1)\cdot(k_1+1) = k_1 p+k_0+1 = k+1$ und dies ist die Dimension von Sym_k. Also stimmt Sym_k mit $\mathrm{soc}^2(\mathrm{Sym}_k)$ überein. $\square$

An Beispiel 4.1.2 sieht man, daß die obere Abschätzung aus Satz 4.1.4 für die Länge von $\mathrm{soq}^2(\mathrm{Sym}_k)$ optimal ist. Umgekehrt sieht man an Satz 4.1.5 oder auch an Beispiel 4.1.1, daß es für die Längen aller $\mathrm{soq}^n(\mathrm{Sym}_k)$ nach unten nur die triviale Abschätzung gegen 1 gibt, da manche Sym_k uniseriell sind. Nach der oberen Abschätzung der Länge von $\mathrm{soq}^2(\mathrm{Sym}_k)$ kann man sich für die maximale Länge unter allen $\mathrm{soq}^n(\mathrm{Sym}_k)$ interessieren. Eine ähnlich naheliegende Frage ist die nach der Länge der Sockelreihe.

Die folgende Tabellen zeigt Ergebnisse entsprechender Computer-Berechnungen bei $p = 3$. Wie man in Tabelle 4.1.9 sehen kann, treten die maximalen Sockelreihenlängen bzw. die Quotienten maximaler Länge in der Sockelreihe bei festem q für mehrere Werte von k auf.

TABELLE 4.1.6.

$p = 3, q = p^e$ mit	$e = 1$	2	3	4	5	6	7	8	9
Maximale Sockelreihenlänge bei Sym_k, $k \leqslant q-2$	1	2	3	4	5	6	7	8	9
Maximale Länge eines $\mathrm{soq}^n(\mathrm{Sym}_k)$, $k \leqslant q-2$	1	1	2	3	6	10	20	35	70

Im Gegensatz zu dem zweiten Quotienten der Sockelreihe ist die Länge eines beliebigen $\mathrm{soq}^n(\mathrm{Sym}_k)$ also nicht durch $e-1$ beschränkt. Die maximale Sockelreihenlänge hingegen scheint gerade gleich e zu sein. Der folgende Satz zeigt, daß die maximale Sockelreihenlänge mindestens gleich e ist.

SATZ 4.1.7. *Sei $q = p^e$. Als $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul ist Sym_{q-2} uniseriell mit Länge e und es gilt*

$$\mathrm{soq}^n(\mathrm{Sym}_{q-2}) \cong S_{(0,\dots,0,p-2\,[n-1],p-1,\dots,p-1)} \otimes \Delta^{(p-1,\dots p-1\,[n-2],0,\dots,0)}.$$

BEWEIS. Wir untersuchen den Ablauf des Algorithmus bei $k = q-2 = (p-2, p-1, \dots, p-1)$ und beweisen induktiv die folgende Behauptung:

Im n-ten Durchlauf erfüllt genau ein j die Bedingungen a), b) und c), nämlich $j = (p-1, \dots, p-1\,[n-2], 0, \dots, 0)$, was im Fall von $n = 1$ als $j = 0$ zu lesen ist. Am Ende des n-ten Durchlaufs ist $B = \{0, \dots, k\} - \{(p-1, \dots, p-1\,[n-1], *, \dots, *)\}$ (Dabei steht $*$ für einen beliebigen Koeffizienten).

Aus dieser Behauptung folgt die Aussage des Satzes, denn für das angegebene j gilt

$$\begin{aligned} k-2j &= (p-2,p-1,\dots,p-1) - (p-1,\dots,p-1\,[n-2],0,\dots,0) \\ &\quad -(p-1,\dots,p-1\,[n-2],0,\dots,0) \\ &= (p-1,\dots,p-1\,[n-2],p-2,p-1,\dots,p-1) \\ &\quad -(p-1,\dots,p-1\,[n-2],0,\dots,0) \\ &= (0,\dots,0\,[n-2],p-2,p-1,\dots,p-1) \end{aligned}$$

und dazu gehört der im Satz beschriebene einfache $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul.

Nun zum Beweis der Behauptung. Der Induktionsanfang bei $n=1$ ist klar, da der Sockel eines Sym_k immer einfach und isomorph zu $S_{(k_0,\dots,k_{e-1})}\otimes\Delta^0 = S_{(p-2,p-1,\dots,p-1)}\otimes\Delta^0$ ist und sich aus $j=0$ ergibt. Zudem ist nach Ende des ersten Durchlaufs $B=\{i \,\big|\, i\preccurlyeq k\} = \{0,\dots,k\}-\{i\,\big|\, i\not\preccurlyeq k\} = \{0,\dots,k\}-\{(p-1,*,\dots,*)\}$.

Wir zeigen jetzt den Induktionsschritt von n nach $n+1$. Zu Beginn des $n+1$-ten Durchlaufs sei $B=\{0,\dots,k\}-\{(p-1,\dots,p-1\,[n-1],*,\dots,*)\}$. Damit j die Bedingung a) erfüllt, d.h. nicht in B liegt, muß es von der Form $j=(p-1,\dots,p-1\,[n-1],*,\dots,*)$ sein. Bedingung b) fordert, daß alle i mit $i\precnsim j$ in B liegen, d.h. nicht von der Form $(p-1,\dots,p-1\,[n-1],*,\dots,*)$ sind. Dies ist genau dann erfüllt, wenn $j=(p-1,\dots,p-1\,[n-1],0,\dots,0)$ ist.

Da auf dieser Stufe also nur ein Höchstgewichtsvektor existiert, muß er auch zulässig sein, d.h. das entsprechende j erfüllt auch Bedingung c). Es bleibt noch die Aussage über das Aussehen von B am Ende des $n+1$-ten Durchlaufs zu zeigen. Da das einzige gefundene $j=(p-1,\dots,p-1\,[n-1],0,\dots,0)$ ist, kommen zu B die Elemente i mit $k-i\preceq k-j$ hinzu, oder anders ausgedrückt, von den bisher nicht in B liegenden Elementen der Form $i=(p-1,\dots,p-1\,[n-1],*,\dots,*)$ kommen diejenigen nicht zu B hinzu, bei denen $k-i\not\preccurlyeq k-j$ gilt. Da

$$\begin{aligned} k-j &= (p-2,p-1,\dots,p-1)-(p-1,\dots,p-1\,[n-1],0,\dots,0) \\ &= (p-1,\dots,p-1,p-2\,[n],p-1,\dots,p-1) \end{aligned}$$

ist, sind dies genau die $i=(p-1,\dots,p-1\,[n-2],i_n,\dots,i_{e-1})$, bei denen der n-te Koeffizient von $k-i$ gleich $p-1$ ist. Ist nun $i_n\leqslant p-2$, so ergibt sich

$$\begin{aligned} k-i &= (p-2,p-1,\dots,p-1)-(p-1,\dots,p-1\,[n-1],i_n,\dots,i_{e-1}) \\ &= (p-1,\dots,p-1\,[n-1],p-2-i_n,p-1-i_{n+1},\dots,p-1-i_{e-1}) \end{aligned}$$

und somit ist der n-te Koeffizient von $k-i$ nicht gleich $p-1$. Ist aber $i_n=p-1$, d.h. i von der Form $(p-1,\dots,p-1\,[n],*,\dots,*)$, so erhält man

$$\begin{aligned} k-i &= (p-2,p-1,\dots,p-1)-(p-1,\dots,p-1\,[n],i_{n+1},\dots,i_{e-1}) \\ &= (p-1,\dots,p-1\,[n],p-1-i_{n+1},\dots,p-1-i_{e-1}) \end{aligned}$$

und nun ist der n-te Koeffizient von $k-i$ gleich $p-1$. Die Elemente, welche nicht zu B hinzukommen, sind also gerade diejenigen der Form $(p-1,\dots,p-1\,[n],*,\dots,*)$, und damit ist am Ende des $n+1$-ten Durchlaufs $B=\{0,\dots,k\}-\{(p-1,\dots,p-1\,[n],*,\dots,*)\}$. Die Behauptung ist damit vollständig bewiesen. $\square$

Der vorige Satz zeigt, daß für gewisse Werte von k, deren p-adische Darstellungen eine besondere Struktur haben, genauere Aussagen möglich sind. Ein weiteres einfaches Beispiel dieser Art ist das folgende.

Satz 4.1.8. *Sei $q=p^e$ und $k=q-1-p^n$ für ein $0\leqslant n\leqslant e-1$. Ist $n=e-1$, so ist Sym_k einfach. Ist $n<e-1$, so ist Sym_k nicht einfach, aber $\mathrm{soq}^1(\mathrm{Sym}_k)$ und $\mathrm{soq}^2(\mathrm{Sym}_k)$ sind einfach. Ist $n=e-2$, so ist Sym_k uniseriell mit Länge 2.*

Beweis. Die Dimension von Sym_k ist $q-p^n$, die Dimension des Sockels $S_{(k_0,\dots,k_{e-1})}\otimes\Delta^0$ ist gleich dem p-adischen Querprodukt von $k=(k_0,\dots,k_{e-1})=(p-1,\dots,p-1,p-2\,[n],p-1,\dots,p-1)$, also gleich $p^{e-1}\cdot(p-1)=q-p^{e-1}$. Im Falle von $n=e-1$ stimmt Sym_k folglich mit seinem einfachen Sockel überein.

Ist $n<e-1$, so ist dies nicht der Fall. Da $k=(p-1,\dots,p-1,p-2\,[n],p-1,\dots,p-1)$ ist, gibt es nur ein j, welches Bedingung a) und b) erfüllt, nämlich $j=(p-1)\cdot p^n$. Insbesondere ist also der zweite Quotient $\mathrm{soq}^2(\mathrm{Sym}_k)$ der Sockelreihe einfach. Wegen

$$\begin{aligned} k-2j &= (p-1,\dots,p-1,p-2\,[n],p-1,\dots,p-1)-2(0,\dots,0,p-1\,[n],0,\dots,0)\\ &= (p-1,\dots,p-1,0[n],p-2,p-1,\dots,p-1) \end{aligned}$$

ist seine Dimension gleich $p^{e-1}-p^{e-2}$. Die Summe der Dimensionen von $\mathrm{soq}^1(\mathrm{Sym}_k)$ und $\mathrm{soq}^2(\mathrm{Sym}_k)$ ist daher gleich $q-p^{e-1}+p^{e-1}-p^{e-2}=q-p^{e-2}$. Im Fall von $n=e-2$ ist dies gleich der Dimension von Sym_k. Damit ist alles gezeigt. $\square$

Es gibt sicher noch weitere Fälle besonders strukturierter Werte für k, in denen man bei Bedarf ähnliche Aussagen über die Struktur der Sockelreihe von Sym_k zeigen kann.

An den bisherigen Ergebnissen sieht man unter anderem, daß die Größe der Dimension $k+1$ von Sym_k kein Maß für die Komplexität der Untermodulstruktur ist, So ist Sym_k z.B. einfach für $k=0,1,\dots,p-1,q-1-\frac{q}{p},q-1$. Uniseriell und nicht einfach ist Sym_k für $k=q-1-q/p^2,q-2$. Manchmal ist Sym_k aber auch nicht uniseriell. Die folgende Liste enthält für $p=3$, $q=3^3$ die einfachen Faktoren aller Sockelreihenquotienten aller $k=0,\dots,q-2$. Dabei wird ein einfacher Modul $S_{(r_0,\dots,r_{e-1})}\otimes\Delta^j$ durch $(r_0,\dots,r_{e-1})^j$ abgekürzt.

TABELLE 4.1.9.

k	$\mathrm{soq}^1(\mathrm{Sym}_k)$	$\mathrm{soq}^2(\mathrm{Sym}_k)$	$\mathrm{soq}^3(\mathrm{Sym}_k)$
0	$(0,0,0)^0$		
1	$(1,0,0)^0$		
2	$(2,0,0)^0$		
3	$(0,1,0)^0$	$(1,0,0)^1$	
4	$(1,1,0)^0$	$(0,0,0)^2$	
5	$(2,1,0)^0$		
6	$(0,2,0)^0$	$(1,1,0)^0$	
7	$(1,2,0)^0$	$(0,1,0)^2$	
8	$(2,2,0)^0$		
9	$(0,0,1)^0$	$(0,1,0)^3$	$(1,2,0)^1$
10	$(1,0,1)^0$	$(1,1,0)^3$	$(0,2,0)^2$
11	$(2,0,1)^0$	$(2,1,0)^3$	
12	$(0,1,1)^0$	$(1,0,1)^1, (0,0,0)^6$	$(1,1,0)^4$
13	$(1,1,1)^0$	$(0,0,1)^2, (1,0,0)^6$	$(0,1,0)^5$
14	$(2,1,1)^0$	$(2,0,0)^6$	
15	$(0,2,1)^0$	$(1,1,1)^1$	$(1,0,0)^7$
16	$(1,2,1)^0$	$(0,1,1)^2$	$(0,0,0)^8$
17	$(2,2,1)^0$		
18	$(0,0,2)^0$	$(0,1,1)^3$	$(1,2,1)^1$
19	$(1,0,2)^0$	$(1,1,1)^3$	$(0,2,1)^2$
20	$(2,0,2)^0$	$(2,1,1)^3$	
21	$(0,1,2)^0$	$(1,0,2)^1, (0,0,1)^6$	$(1,1,1)^4$
22	$(1,1,2)^0$	$(0,0,2)^2, (1,0,1)^6$	$(0,1,1)^5$
23	$(2,1,2)^0$	$(2,0,1)^6$	
24	$(0,2,2)^0$	$(1,1,2)^1$	$(1,0,1)^7$
25	$(1,2,2)^0$	$(0,1,2)^2$	$(0,0,1)^8$

4.2. Anwendungen auf die Modulkurve

Wir kommen nun zurück zu Drinfeld'schen Modulkurven. Es sei $A = \mathbb{F}_r[T]$ mit $r = p^n$ sowie $\mathfrak{p} \subseteq A$ ein Primideal und $\mathbb{F}_q = A/\mathfrak{p}$ mit $q = p^e = p^{n \cdot d}$. In Kapitel 2 haben wir zu der Drinfeld'schen Modulkurve $X(\mathfrak{p})$ den Galois-Modul-Homomorphismus $\mathcal{S}/p\mathcal{S} \xrightarrow{\mathrm{div}} D_S^0/pD_S^0$ für die Gruppe $G(\mathfrak{p}) = \mathrm{GL}(2, \mathbb{F}_q)/\mathbb{F}_r^*$ betrachtet und uns für seinen Kern und Kokern interessiert. Nach Tensorieren mit $\mathbb{F}$ und Übergang zu einer zentralen isotypischen Komponente zu einem nichttrivialen Charakter $\psi : \mathbb{F}_q^*/\mathbb{F}_r^* \to \mathbb{F}^*$ ergaben sich in Korollar 3.7.4 die $\mathbb{F}[G]$-Modul-Isomorphismen

$$(\mathcal{S}/p\mathcal{S} \otimes \mathbb{F})(\psi) \cong \mathrm{ind}_B^G(1, \psi)$$

und

$$(D_S^0/pD_S^0 \otimes \mathbb{F})(\psi) \cong \mathrm{ind}_B^G(\psi, 1)\,,$$

wobei $G = \mathrm{GL}(2, \mathbb{F}_q)$ und $B = \{ \left(\begin{smallmatrix} a & c \\ 0 & d \end{smallmatrix}\right) \in G\}$ sind. Durch Verwendung der Sockelreihe ergab sich, daß für einen einfachen $\mathbb{F}[G]$-Modul S die Abschätzungen

$$v_S(\mathrm{Ker}\,\mathrm{div}\,(\psi)) \geqslant \sum_{i \geqslant 1} \max\{0, v_S(\mathrm{soq}^i(\mathrm{ind}_B^G(1,\psi))) - v_S(\mathrm{soq}^i(\mathrm{ind}_B^G(\psi,1)))\}$$

und

$$v_S(\mathrm{Koker}\,\mathrm{div}\,(\psi)) \geqslant \sum_{i \geqslant 1} \max\{0, v_S(\mathrm{soq}^i(\mathrm{ind}_B^G(\psi,1))) - v_S(\mathrm{soq}^i(\mathrm{ind}_B^G(1,\psi)))\}\,.$$

Ist $\psi = \chi^k$, so verwenden wir zur Abschätzung von $v_S(\mathrm{ind}_B^G(1,\chi^k))$ bzw. von $v_S(\mathrm{ind}_B^G(\chi^k,1)) = v_S(\mathrm{ind}_B^G(1,\chi^{q-1-k}) \otimes \Delta^k)$ die beiden exakten Folgen

$$0 \to \mathrm{Sym}_k \to \mathrm{ind}_B^G(1,\chi^k) \to \mathrm{Sym}^*_{q-1-k} \to 0 \tag{4.2.1}$$

und

$$0 \to \mathrm{Sym}_{q-1-k} \otimes \Delta^k \to \mathrm{ind}_B^G(1,\chi^{q-1-k}) \otimes \Delta^k \to \mathrm{Sym}^*_k \otimes \Delta^k \to 0 \tag{4.2.2}$$

sowie die Informationen, die wir über die Sockelreihen der Sym_k besitzen.

Zuerst betrachten wir aber den Sonderfall der zentralen isotypischen Komponente, die zum trivialen Charakter gehört.

Satz 4.2.3. *Als $\mathbb{F}[G(\mathfrak{p})]$- bzw. als $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Modul sind $(\mathcal{S}/p\mathcal{S} \otimes \mathbb{F})(1)$ und $(D_S^0/pD_S^0 \otimes \mathbb{F})(1)$ isomorph. Genauer gesagt sind beide isomorph zu dem einfachen $\mathbb{F}[G]$-Modul $S_{(p-1,\dots,p-1)} \otimes \Delta^0$.*

Beweis. Aus Proposition 2.2.7 und 2.3.9 ergeben sich die Isomorphismen

$$\mathbb{F} \oplus (\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}) \cong \mathrm{ind}_{F/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F}$$

und

$$\mathbb{F} \oplus (D_S^0/pD_S^0 \otimes \mathbb{F}) \cong \mathrm{ind}_{E/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F}.$$

Für die 1-Komponente folgt

$$\mathbb{F} \oplus (\mathcal{S}/p\mathcal{S} \otimes \mathbb{F})(1) \cong \mathrm{ind}_{F/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F}(1)$$

und

$$\mathbb{F} \oplus (D_S^0/pD_S^0 \otimes \mathbb{F})(1) \cong \mathrm{ind}_{E/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F}(1)\,.$$

Aus Proposition 3.7.3 ergibt sich

$$\mathrm{ind}_{F/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F}(1) = \mathrm{ind}_{F/\mathbb{F}_r^*}^{G/\mathbb{F}_r^*} \mathbb{F}(1) = \mathrm{ind}_B^G(1,1) = \mathrm{ind}_B^G \mathbb{F}$$

und auch

$$\mathrm{ind}_{E/\mathbb{F}_r^*}^{G(\mathfrak{p})} \mathbb{F}(1) = \mathrm{ind}_B^G \mathbb{F}.$$

Zusammen ergibt sich

$$\mathbb{F} \oplus (\mathcal{S}/p\mathcal{S} \otimes \mathbb{F})(1) \cong \mathrm{ind}_B^G \mathbb{F} \cong \mathbb{F} \oplus (D_S^0/pD_S^0 \otimes \mathbb{F})(1)$$

und somit die Isomorphie zwischen

$$(\mathcal{S}/p\mathcal{S} \otimes \mathbb{F})(1) \cong (D_S^0/pD_S^0 \otimes \mathbb{F})(1)\,.$$

Mit dem in Proposition 3.6.16 gefundenen Isomorphismus

$$\mathrm{ind}_B^G \mathbb{F} \cong \mathbb{F} \oplus S_{(p-1,\dots,p-1)}$$

ist der Satz vollständig bewiesen. □

Da also die 1-Komponente der beiden zu vergleichenden Moduln gleich ist, kann man über sie im allgemeinen nichts aussagen, da sowohl ein Isomorphismus oder die Null-Abbildung vorliegen kann. Ist aber der Grad von $\mathfrak{p}$ gleich 1, so ergibt sich folgende Aussage.

SATZ 4.2.4. *Sei $\mathfrak{p}$ von einem linearen Polynom erzeugt. Dann sind die $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD^0_{S\otimes\mathbb{F}}$ beide isomorph zu dem einfachen Modul $S_{(p-1,\dots,p-1)} \otimes \Delta^0$ und der $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Homomorphismus $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F} \xrightarrow{\mathrm{div}} D_S^0/pD_S^0 \otimes \mathbb{F}$ ist ein Isomorphismus. Die Ordnung der Siegeldivisorklassengruppe von $X(\mathfrak{p})$ ist p-frei.*

BEWEIS. Im Falle eines Primideals $\mathfrak{p}$ vom Grad 1 ist das Zentrum von $G(\mathfrak{p})$ trivial, d.h. es gibt nur den trivialen zentralen Charakter. Insbesondere stimmen $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$ schon mit ihrer 1-Komponente überein und sind nach Satz 4.2.3 isomorph zu $S_{(p-1,\dots,p-1)} \otimes \Delta^0$. Wäre nun div kein Isomorphismus, so wäre es die Null-Abbildung, woraus die Inklusion $\mathcal{S} \subseteq pD_S^0$ folgen würde. Wählt man aber einen Erzeuger f von $\mathfrak{p}$ und setzt $u = (1/f, 0)$ so ergibt sich für die Siegel-Funktion $g_u^{q+1} = e_u^{q+1}\eta^{q+1}$ der Divisor

$$\mathrm{div}\, g_u^{q+1} = (q+1)\mathrm{div}\, e_u + \mathrm{div}\,(\eta^{q+1}) \equiv \mathrm{div}\, e_u \bmod pD_S\,,$$

da η^{q+1} q-fache Nullstellen in den Spitzen hat [**Ge2**, S. 111]. Für e_u ergibt sich ein einfacher Pol an der Stelle ∞ [**Ge2**, Korollar 2.2] und damit liegt der Divisor der Siegel-Funktion g_u^{q+1} nicht in pD_S^0 und es kann auch nicht $\mathcal{S} \subseteq pD_S^0$ gelten. □

Eine wesentlich genauere Analyse der Ordnungen der beteiligten Gruppen zeigt, daß im Fall eines Primideals vom Grad 1 sogar schon die ganze Spitzendivisorklassengruppe von $X(\mathfrak{p})$ trivial ist [**Ge2**].

BEISPIEL 4.2.5. Wir kommen nun zum ersten Beispiel, das wir vollständig ausführen. Es sei $r = p = 3$ und $\mathfrak{p}$ ein Primideal in $\mathbb{F}_3[T]$ vom Grad 2, so daß sich $q = 3^2 = 9$ ergibt. Die nichttrivialen Charaktere des Zentrums $\mathbb{F}_9^*/\mathbb{F}_3^*$ von $G(\mathfrak{p})$ sind gegeben durch die χ^k, $k = 2, 4, 6$. Wir müssen also die Struktur der $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_9)]-$Moduln Sym_2, Sym_4, Sym_6 und ihrer Duale untersuchen. Indem man den Algorithmus durchführt oder Satz 4.1.5 verwendet, ergibt sich für die Sockelreihe der Sym_k folgendes.

TABELLE 4.2.6.

k	Sockelreihenlänge von Sym_k	einfache Faktoren von $\mathrm{soq}^1(\mathrm{Sym}_k)$	einfache Faktoren von $\mathrm{soq}^2(\mathrm{Sym}_k)$
2	1	$S_{(2,0)} \otimes \Delta^0$	
4	2	$S_{(1,1)} \otimes \Delta^0$	$S_{(0,0)} \otimes \Delta^2$
6	2	$S_{(0,2)} \otimes \Delta^0$	$S_{(1,1)} \otimes \Delta^1$

Insbesondere sind alle vorkommenden Sym_k und damit auch die $(\mathrm{Sym}_k)^*$ uniseriell. Daher kann man auch wie in Abschnitt 3.3 beschrieben die Sockelreihe der Duale bestimmen.

TABELLE 4.2.7.

k	Sockelreihenlänge von Sym_k^*	einfache Faktoren von $\mathrm{soq}^1(\mathrm{Sym}_k^*)$	Einfache Faktoren von $\mathrm{soq}^2(\mathrm{Sym}_k^*)$
2	1	$S_{(2,0)} \otimes \Delta^6$	
4	2	$S_{(0,0)} \otimes \Delta^6$	$S_{(1,1)} \otimes \Delta^4$
6	2	$S_{(1,1)} \otimes \Delta^3$	$S_{(0,2)} \otimes \Delta^2$

Da $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ die direkte Summe der 1-Komponente $S_{(2,2)} \otimes \Delta^0$ und der $\mathrm{ind}_B^G(1, \chi^k)$ mit $k = 2, 4, 6$ ist und sich diese mittels

$$0 \to \mathrm{Sym}_k \to \mathrm{ind}_B^G(1, \chi^k) \to \mathrm{Sym}_{8-k}^* \to 0$$

zerlegen, haben wir alle einfachen Faktoren von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ bestimmt, nämlich $S_{(2,2)} \otimes \Delta^0$ und alle einfachen Faktoren aus den beiden Tabellen oben. Addiert man die Dimensionen dieser Moduln auf, so ergibt sich 39, und tatsächlich ist die Anzahl der Spitzen von $X(\mathfrak{p})$ auch $\frac{q^2-1}{r-1} = \frac{80}{2} - 1 = 39$.

Da für einen nichttrivialen zentralen Charakter χ^k von $G(\mathfrak{p})$ die entsprechende Komponente von $D_S^0/pD_S^0 \otimes \mathbb{F}$ durch

$$\mathrm{ind}_B^G(\chi^k, 1) \cong \mathrm{ind}_B^G(1, \chi^{q-1-k}) \otimes \Delta^k$$

gegeben ist und sich dieser Modul mittels

$$0 \to \mathrm{Sym}_{q-1-k} \otimes \Delta^k \to \mathrm{ind}_B^G(1, \chi^{q-1-k}) \otimes \Delta^k \to \mathrm{Sym}_k^* \otimes \Delta^k \to 0$$

zerlegt, erhält man für $D_S^0/pD_S^0 \otimes \mathbb{F}$ die folgende Liste einfacher Faktoren: $S_{(2,2)} \otimes \Delta^0$ von der 1-Komponente, $S_{(0,2)} \otimes \Delta^0 \otimes \Delta^2 = S_{(1,1)} \otimes \Delta^2$, $S_{(1,1)} \otimes \Delta^1 \otimes \Delta^2 = S_{(1,1)} \otimes \Delta^3$ und $S_{(2,0)} \otimes \Delta^6 \otimes \Delta^2 = S_{(2,0)} \otimes \Delta^0$ für $k = 2$, $S_{(1,1)} \otimes \Delta^{0+4}$, $S_{(0,0)} \otimes \Delta^{2+4}$, $S_{(0,0)} \otimes \Delta^{6+4}$ und $S_{(1,1)} \otimes \Delta^{4+4}$ für $k = 4$ sowie $S_{(2,0)} \otimes \Delta^{0+6}$, $S_{(1,1)} \otimes \Delta^{3+6}$ und $S_{(0,2)} \otimes \Delta^{2+6}$ für $k = 6$. Ein Vergleich mit den einfachen Faktoren von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ zeigt, daß beide genau die gleichen einfachen Faktoren haben.

Da außerdem jeder einfache Faktor von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ bzw. $D_S^0/pD_S^0 \otimes \mathbb{F}$ nur mit einfacher Vielfachheit vorkommt, ist seine Höhe bezüglich der Sockelreihe eindeutig festgelegt. Wir betrachten nun nacheinander die isotypischen Komponenten von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ bzw. $D_S^0/pD_S^0 \otimes \mathbb{F}$ zu den nichttrivialen zentralen Charakteren χ^k und geben für die vorkommenden einfachen Faktoren die Höhe in der Sockelreihe oder zumindest eine Abschätzung davon an.

Zuerst untersuchen wir die χ^2-Komponente. Die einfachen Faktoren von $\mathrm{ind}_B^G(1,\chi^2)$ sind $S_{(2,0)}\otimes\Delta^0$, $S_{(1,1)}\otimes\Delta^3$ und $S_{(0,2)}\otimes\Delta^2$. Da $S_{(2,0)}\otimes\Delta^0$ im Sockel des Untermoduls Sym_2 von $\mathrm{ind}_B^G(1,\chi_0^2)$ vorkommt, hat dieser Faktor in $\mathrm{ind}_B^G(1,\chi^2)$ die Höhe 1. Der Faktor $S_{(1,1)}\otimes\Delta^3$ hat in dem Quotienten Sym_6^* von $\mathrm{ind}_B^G(1,\chi^2)$ die Höhe 1, also hat er in $\mathrm{ind}_B^G(1,\chi^2)$ selbst mindestens die Höhe 1. Da wir sogar wissen, daß der Sockel von $\mathrm{ind}_B^G(1,\chi^2)$ mit dem Sockel des Untermoduls Sym_2 übereinstimmt, hat $S_{(1,1)}\otimes\Delta^3$ in $\mathrm{ind}_B^G(1,\chi^2)$ sogar mindestens die Höhe 2. Der Faktor $S_{(0,2)}\otimes\Delta^2$ hat in Sym_6^* die Höhe 2 und damit in $\mathrm{ind}_B^G(1,\chi^2)$ mindestens die Höhe 2.

Die einfachen Faktoren von $\mathrm{ind}_B^G(\chi^2,1) = \mathrm{ind}_B^G(1,\chi^6)\otimes\Delta^2$ sind $S_{(0,2)}\otimes\Delta^2$, $S_{(1,1)}\otimes\Delta^3$ und $S_{(2,0)}\otimes\Delta^0$. Da $S_{(0,2)}\otimes\Delta^2$ die Höhe 1 in dem Untermodul $\mathrm{Sym}_6\otimes\Delta^2$ von $\mathrm{ind}_B^G(\chi^2,1)$ hat, ist die Höhe in $\mathrm{ind}_B^G(\chi^2,1)$ selbst auch gleich 1. Der Faktor $S_{(1,1)}\otimes\Delta^3$ hat die Höhe 2 in $\mathrm{Sym}_6\otimes\Delta^2$, also auch in $\mathrm{ind}_B^G(\chi^2,1)$. Der Faktor $S_{(2,0)}\otimes\Delta^0$ hat die Höhe 1 in dem Quotienten $\mathrm{Sym}_2^*\otimes\Delta^2$ von $\mathrm{ind}_B^G(\chi^2,1)$ und damit mindestens diese Höhe in $\mathrm{ind}_B^G(\chi^2,1)$ selbst. Auch hier muß die Höhe aber sogar mindestens 2 sein, da $S_{(2,0)}\otimes\Delta^0$ nicht in dem gemeinsamen Sockel von $\mathrm{Sym}_2^*\otimes\Delta^2$ und $\mathrm{ind}_B^G(\chi^2,1)$ vorkommt.

Wir fassen dies zusammen.

TABELLE 4.2.8.

Faktor	Höhe in $\mathrm{ind}_B^G(1,\chi^2)$	Höhe in $\mathrm{ind}_B^G(\chi^2,1)$
$S_{(2,0)}\otimes\Delta^0$	1	$\geqslant 2$
$S_{(1,1)}\otimes\Delta^3$	$\geqslant 2$	2
$S_{(0,2)}\otimes\Delta^2$	$\geqslant 2$	1

Ein Vergleich der Höhen der einfachen Faktoren läßt jetzt Rückschlüsse auf Kern und Kokern von $\mathrm{div}\,(\chi^2) : \mathrm{ind}_B^G(1,\chi^2)\to\mathrm{ind}_B^G(\chi^2,1)$ zu. Da $S_{(2,0)}\otimes\Delta^0$ im Ausgangsmodul auf Höhe 1 vorkommt, im Zielmodul aber erst auf Höhe $\geqslant 2$, muß $S_{(2,0)}\otimes\Delta^0$ im Kern vorkommen. Da $S_{(0,2)}\otimes\Delta^2$ im Ausgangsmodul auf Höhe $\geqslant 2$ vorkommt, im Zielmodul aber nur auf Höhe 1, muß auch dieser Faktor im Kern auftreten. Mit einer entsprechenden Argumentation ergibt sich umgekehrt, daß auch $S_{(0,2)}\otimes\Delta^2$ und $S_{(2,0)}\otimes\Delta^0$ im Kokern von $\mathrm{div}\,(\chi^2)$ vorkommen müssen. Über den Faktor $S_{(1,1)}\otimes\Delta^3$ kann man nichts sagen.

Für $k=4$ ergibt sich aus den berechneten Sockelreihen die folgende Tabelle.

TABELLE 4.2.9.

Faktor	Höhe in $\mathrm{ind}_B^G(1,\chi^4)$	Höhe in $\mathrm{ind}_B^G(\chi^4,1)$
$S_{(1,1)} \otimes \Delta^0$	1	$\geqslant 2$
$S_{(0,0)} \otimes \Delta^2$	2	$\geqslant 2$
$S_{(0,0)} \otimes \Delta^6$	$\geqslant 2$	2
$S_{(1,1)} \otimes \Delta^4$	$\geqslant 2$	1

Folglich muß der Kern von $\mathrm{div}\,(\chi^4)$ die Faktoren $S_{(1,1)} \otimes \Delta^0$ und $S_{(1,1)} \otimes \Delta^4$ enthalten, und der Kokern ebenso.

Nun noch zu $k = 6$.

TABELLE 4.2.10.

Faktor	Höhe in $\mathrm{ind}_B^G(1,\chi^6)$	Höhe in $\mathrm{ind}_B^G(\chi^6)$
$S_{(0,2)} \otimes \Delta^0$	1	$\geqslant 2$
$S_{(1,1)} \otimes \Delta^1$	2	$\geqslant 2$
$S_{(2,0)} \otimes \Delta^6$	$\geqslant 2$	1

Folglich enthalten sowohl Kern als auch Kokern die Faktoren $S_{(0,2)} \otimes \Delta^0$ und $S_{(2,0)} \otimes \Delta^6$.

Da der Kern von div direkte Summe der Kerne der $\mathrm{div}\,(\chi^k)$, $k = 0, 2, 4, 6$ ist, enthält er mindestens die einfachen Faktoren $S_{(2,0)} \otimes \Delta^0$, $S_{(0,2)} \otimes \Delta^2$, $S_{(1,1)} \otimes \Delta^0$, $S_{(1,1)} \otimes \Delta^4$, $S_{(0,2)} \otimes \Delta^0$ und $S_{(2,0)} \otimes \Delta^6$. Das selbe gilt für den Kokern. Insbesondere ist die Dimension von Kern und Kokern mindestens $3 \cdot 1 + 1 \cdot 3 + 2 \cdot 2 + 2 \cdot 2 + 1 \cdot 3 + 3 \cdot 1 = 20$. Für die Siegeldivisorklassengruppe $\mathcal{C}_{\mathrm{Siegel}}$ bedeuted dies

$$\#\mathcal{C}_{\mathrm{Siegel}}/p\mathcal{C}_{\mathrm{Siegel}} = \#\mathcal{C}_{\mathrm{Siegel}}[p] \geqslant 3^{20}\,.$$

Leider läßt dies keinen Schluß auf die Spitzendivisorklassengruppe zu, da sich aus Korollar 2.4.3 nur ergibt, daß sich die $\mathbb{F}_p$-Dimensionen von C/pC und $\mathcal{C}_{\mathrm{Siegel}}/p\mathcal{C}_{\mathrm{Siegel}}$ bei $r = p^n$ und $q = r^d$ möglicherweise um $n \cdot \frac{d}{2} \cdot (\frac{r^{2d}-1}{r-1} - r^d - 1)$ unterscheiden, was in unserer Situation eine mögliche Differenz der $\mathbb{F}_p$-Dimension um $1 \cdot \frac{1}{2}(\frac{3^4-1}{2} - 9 - 1) = 30$ ergibt. Die formale Ähnlichkeit zur klassischen Situation und die große Symmetrie zwischen den zentralen Komponenten von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$ (die beiden Folgen (4.2.1) und (4.2.2) sind fast dual zueinander) können aber als weiterer Hinweis gedeutet werden auf die schon in **[Ge2]** geäußerte Vermutung, daß bei primem $\mathfrak{p}$ die Siegeldivisorengruppen von $X(\mathfrak{p})$ schon alle Hauptspitzendivisoren liefert. In diesem Fall würden alle Aussagen über die Siegeldivisorklassengruppe $\mathcal{C}_{\mathrm{Siegel}}$ auch auf die Gruppe $\mathcal{C}$ der Spitzendivisorklassengruppe zutreffen.

Wir werden nun noch einige andere Beispiele betrachten, beschränken uns dabei aber immer auf einzelne zentrale isotypische Komponenten. Dies ist zum einen darin begründet, daß bei wachsendem Grad von $\mathfrak{p}$ die Anzahl der zentralen Charaktere sehr stark wächst und vollständige Beispiele zu viel Platz in Anspruch nehmen würden. Zum anderen ist es auch bei größeren Parametern oft so, daß das Verhalten der einzelnen zentralen Komponenten ziemlich ähnlich ist. Im folgenden wollen wir aber gezielt solche Beispiele betrachten, bei denen die Struktur der Sockelreihe unterschiedlich ist.

Beispiel 4.2.11. In Beispiel 4.2.5 hätten wir dieselben Resultate erhalten, wenn wir von $\mathrm{ind}_B^G(1,\chi^k)$ bzw. $\mathrm{ind}_B^G(\chi^k,1)$ nur den Sockel gekannt hätten. Im allgemeinen liefert die Kenntnis der Sockelreihen von Sym_k, Sym_{q-1-k} insbesondere bei größeren Sockelreihenlängen aber mehr Information. Die besten Ergebnisse erhält man, wenn Sym_k und Sym_{q-1-k} uniseriell sind, da man dann nicht nur die Sockelreihe der Untermoduln Sym_k und $\mathrm{Sym}_{q-1-k} \otimes \Delta^k$ kennt, sondern auch die der Quotienten Sym^*_{q-1-k} und $\mathrm{Sym}^*_k \otimes \Delta^k$. Wir betrachten den Fall $p = r = 3$, $q = 3^4 = 81$ und die zum Charakter χ^k mit $k = 28$ gehörende zentrale Komponente. Für Sym_{28} und den ebenfalls benötigten Modul $\mathrm{Sym}_{q-1-k} \otimes \Delta^k = \mathrm{Sym}_{52} \otimes \Delta^{28}$ ergibt sich folgende Tabelle.

Tabelle 4.2.12.

	Sym_{28}	Sym_{52}	$\mathrm{Sym}_{52} \otimes \Delta^{28}$
soq^1	$S_{(1,0,0,1)} \otimes \Delta^0$	$S_{(1,2,2,1)} \otimes \Delta^0$	$S_{(1,2,2,1)} \otimes \Delta^{28}$
soq^2	$S_{(1,0,1,0)} \otimes \Delta^9$	$S_{(0,1,2,1)} \otimes \Delta^2$	$S_{(0,1,2,1)} \otimes \Delta^{30}$
soq^3	$S_{(1,1,2,0)} \otimes \Delta^3$	$S_{(0,0,1,1)} \otimes \Delta^8$	$S_{(0,0,1,1)} \otimes \Delta^{36}$
soq^4	$S_{(0,2,2,0)} \otimes \Delta^2$	$S_{(0,0,0,0)} \otimes \Delta^{26}$	$S_{(0,0,0,0)} \otimes \Delta^{54}$

Insbesondere sind diese beiden Moduln uniseriell der Länge 4. Da sie uniseriell sind, lassen sich die Quotienten der Sockelreihe der benötigten Duale berechnen. Man erhält:

Tabelle 4.2.13.

	$\mathrm{Sym}^*_{28} \otimes \Delta^{28}$	Sym^*_{52}
soq^1	$S_{(0,2,2,0)} \otimes \Delta^2$	$S_{(0,0,0,0)} \otimes \Delta^{54}$
soq^2	$S_{(1,1,2,0)} \otimes \Delta^3$	$S_{(0,0,1,1)} \otimes \Delta^{36}$
soq^3	$S_{(1,0,1,0)} \otimes \Delta^3$	$S_{(0,1,2,1)} \otimes \Delta^{30}$
soq^4	$S_{(1,0,0,1)} \otimes \Delta^0$	$S_{(1,2,2,1)} \otimes \Delta^{28}$

Für die Höhe der einfachen Faktoren in der Sockelreihe der beiden Moduln $\mathrm{ind}_B^G(1,\chi^{28})$ und $\mathrm{ind}_B^G(\chi^{28},1)$ ergibt sich folgende Liste:

Tabelle 4.2.14.

Faktor	Höhe in $\mathrm{ind}_B^G(1,\chi^{28})$	Höhe in $\mathrm{ind}_B^G(\chi^{28},1)$
$S_{(1,0,0,1)} \otimes \Delta^0$	1	$\geqslant 4$
$S_{(1,0,1,0)} \otimes \Delta^9$	2	$\geqslant 3$
$S_{(1,1,2,0)} \otimes \Delta^3$	3	$\geqslant 2$
$S_{(0,2,2,0)} \otimes \Delta^2$	4	$\geqslant 2$
$\vdots$	$\vdots$	$\vdots$

Faktor	Höhe in $\mathrm{ind}_B^G(1,\chi^{28})$	Höhe in $\mathrm{ind}_B^G(\chi^{28},1)$
$S_{(0,0,0,0)} \otimes \Delta^{54}$	$\geqslant 2$	4
$S_{(0,0,1,1)} \otimes \Delta^{36}$	$\geqslant 2$	3
$S_{(0,1,2,1)} \otimes \Delta^{30}$	$\geqslant 3$	2
$S_{(1,2,2,1)} \otimes \Delta^{28}$	$\geqslant 4$	1

Damit enthalten sowohl Kern als auch Kokern jedes $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Homomorphismus von $\mathrm{ind}_B^G(1,\chi^{28})$ nach $\mathrm{ind}_B^G(\chi^{28},1)$ und insbesondere auch $\mathrm{div}\,(\chi^{28})$ mindestens die Faktoren $S_{(1,0,0,1)} \otimes \Delta^0$, $S_{(1,0,1,0)} \otimes \Delta^9$, $S_{(0,1,2,1)} \otimes \Delta^{30}$ und $S_{(1,2,2,1)} \otimes \Delta^{28}$. Bei alleiniger Kenntnis des Sockels von $\mathrm{ind}_B^G(1,\chi^{28})$ und $\mathrm{ind}_B^G(\chi^{28},1)$ hätte man nur auf die Faktoren $S_{(1,0,0,1)} \otimes \Delta^0$ und $S_{(1,2,2,1)} \otimes \Delta^{28}$ schließen können.

Beispiel 4.2.15. Als nächstes betrachten wir eine Situation, in der Sym_k nicht uniseriell ist. In diesem Fall kennt man die Sockelreihe der dualen Darstellungen Sym_k^* bzw. von $\mathrm{Sym}_k^* \otimes \Delta^k$ nicht vollständig, aber man kann sie zumindest abschätzen. Es sei wieder $p = r = 3$ und $q = 3^4$, jetzt aber $k = 30$.

Tabelle 4.2.16.

	Sym_{30}	Sym_{50}	$\mathrm{Sym}_{50} \otimes \Delta^{30}$
soq^1	$S_{(0,1,0,1)} \otimes \Delta^0$	$S_{(2,1,2,1)} \otimes \Delta^0$	$S_{(2,1,2,1)} \otimes \Delta^{30}$
soq^2	$S_{(1,0,0,1)} \otimes \Delta^1$, $S_{(0,1,1,0)} \otimes \Delta^9$	$S_{(2,0,1,1)} \otimes \Delta^6$	$S_{(2,0,1,1)} \otimes \Delta^{36}$
soq^3	$S_{(0,0,2,0)} \otimes \Delta^6$, $S_{(1,0,1,0)} \otimes \Delta^{10}$	$S_{(2,0,0,0)} \otimes \Delta^{24}$	$S_{(2,0,0,0)} \otimes \Delta^{54}$
soq^4	$S_{(1,1,2,0)} \otimes \Delta^4$		

Während also Sym_{30} nicht uniseriell ist und Sockelreihenlänge 4 besitzt, ist Sym_{50} uniseriell mit Länge 3. Damit ist bei dem Modul $\mathrm{ind}_B^G(1,\chi^{30})$ die Sockelreihe sowohl des Untermoduls Sym_{30} als auch des Quotienten Sym_{50}^* bekannt. Für die Höhen der einfachen Faktoren ergibt sich folgendes:

Tabelle 4.2.17.

Faktor	Höhe in $\mathrm{ind}_B^G(1,\chi^{30})$
$S_{(0,1,0,1)} \otimes \Delta^0$	1
$S_{(1,0,0,1)} \otimes \Delta^1$	2
$S_{(0,1,1,0)} \otimes \Delta^9$	2
$S_{(0,0,2,0)} \otimes \Delta^6$	3
$S_{(1,0,1,0)} \otimes \Delta^{10}$	3
$S_{(1,1,2,0)} \otimes \Delta^4$	4
$S_{(2,0,0,0)} \otimes \Delta^{54}$	$\geqslant 2$
$S_{(2,0,1,1)} \otimes \Delta^{36}$	$\geqslant 2$
$S_{(2,1,2,1)} \otimes \Delta^{30}$	$\geqslant 3$

Für den Modul $\operatorname{ind}_B^G(\chi^{30}, 1)$ kann man zunächst nur folgende Tabelle angeben:

TABELLE 4.2.18.

Faktor	Höhe in $\operatorname{ind}_B^G(\chi^{30}, 1)$
$S_{(2,1,2,1)} \otimes \Delta^{30}$	1
$S_{(2,0,1,1)} \otimes \Delta^{36}$	2
$S_{(2,0,0,0)} \otimes \Delta^{54}$	3

Diese Tabelle berücksichtigt nur die Faktoren des Untermoduls $\mathrm{Sym}_{50} \otimes \Delta^{30}$. Von den verbleibenden Faktoren, d.h. denen des Quotienten $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$, weiß man zuerst einmal nur, daß sie mindestens Höhe 2 in $\operatorname{ind}_B^G(\chi^{30}, 1)$ haben, da sie nicht zum Sockel gehören. Die Quotienten der Sockelreihe von $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$ ergeben sich zwar nicht aus der Sockelreihe von Sym_{30}, dafür aber diejenigen der Radikalreihe:

TABELLE 4.2.19.

	$\mathrm{Sym}_{30}^* \otimes \Delta^{30}$
raq^1	$S_{(0,1,0,1)} \otimes \Delta^0$
raq^2	$S_{(1,0,0,1)} \otimes \Delta^1$, $S_{(0,1,1,0)} \otimes \Delta^9$
raq^3	$S_{(0,0,2,0)} \otimes \Delta^6$, $S_{(1,0,1,0)} \otimes \Delta^{10}$
raq^4	$S_{(1,1,2,0)} \otimes \Delta^4$

Nun kommen die Faktoren von $\mathrm{raq}^n(\mathrm{Sym}_{30}^* \otimes \Delta^{30})$ in $\mathrm{rad}^{n-1}(\mathrm{Sym}_{30}^* \otimes \Delta^{30}) \subseteq \mathrm{soc}^{4-n+1}(\mathrm{Sym}_{30}^* \otimes \Delta^{30})$ vor, haben also in der Sockelreihe von $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$ die Höhe $\leqslant 4 - n + 1$. Wir erhalten damit folgende Information:

TABELLE 4.2.20.

Faktor	Höhe in $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$
$S_{(1,1,2,0)} \otimes \Delta^4$	$\leqslant 1$
$S_{(0,0,2,0)} \otimes \Delta^6$	$\leqslant 2$
$S_{(1,0,1,0)} \otimes \Delta^{10}$	$\leqslant 2$
$S_{(1,0,0,1)} \otimes \Delta^1$	$\leqslant 3$
$S_{(0,1,1,0)} \otimes \Delta^9$	$\leqslant 3$
$S_{(0,1,0,1)} \otimes \Delta^0$	$\leqslant 4$

Da die Höhe eines Faktors nicht kleiner als 1 sein kann, ist die Höhe von $S_{(1,1,2,0)} \otimes \Delta^4$ in $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$ genau 1. Außerdem hat $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$ die gleiche Sockellänge wie Sym_{30}, nämlich 4. Der einzig mögliche Kandidat für eine Höhe von 4 ist $S_{(0,1,0,1)} \otimes \Delta^0$, also hat dieser Faktor genau die Höhe 4. Genauso muß es mindestens einen Faktor der Höhe 3 in $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$ geben. Daher muß mindestens einer der beiden Faktoren $S_{(1,0,0,1)} \otimes \Delta^1$, $S_{(0,1,1,0)} \otimes \Delta^9$ die Höhe 3 haben. Da wir wissen, daß keiner der Faktoren des Quotienten $\mathrm{Sym}_{30}^* \otimes \Delta^{30}$ zum Sockel von $\operatorname{ind}_B^G(\chi^{30}, 1)$ gehört, ergeben sich für die Faktoren von $\operatorname{ind}_B^G(\chi^{30}, 1)$ folgende Höhen:

TABELLE 4.2.21.

Faktor	Höhe in $\mathrm{ind}_B^G(\chi^{30},1)$
$S_{(2,1,2,1)}\otimes\Delta^{30}$	1
$S_{(2,0,1,1)}\otimes\Delta^{36}$	2
$S_{(2,0,0,0)}\otimes\Delta^{54}$	3
$S_{(1,1,2,0)}\otimes\Delta^{4}$	$\geqslant 2$
$S_{(1,0,1,0)}\otimes\Delta^{10}$	$\geqslant 2$
$S_{(0,0,2,0)}\otimes\Delta^{6}$	$\geqslant 2$
$S_{(1,0,0,1)}\otimes\Delta^{1}$ $S_{(0,1,1,0)}\otimes\Delta^{9}$	$\geqslant 2$ mindestens einmal $\geqslant 3$
$S_{(0,1,0,1)}\otimes\Delta^{0}$	$\geqslant 4$

Im Vergleich mit der entsprechenden Tabelle für $\mathrm{ind}_B^G(1,\chi^{30})$ ergibt sich, daß Kern und Kokern eines beliebigen $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Homomorphismus von $\mathrm{ind}_B^G(1,\chi^{30})$ nach $\mathrm{ind}_B^G(\chi^{30},1)$ mindestens die Faktoren $S_{(2,1,2,1)}\otimes\Delta^{30}$, $S_{(0,1,0,1)}\otimes\Delta^{0}$ und einen der beiden Faktoren $S_{(1,0,0,1)}\otimes\Delta^{1}$, $S_{(0,1,1,0)}\otimes\Delta^{9}$ enthalten muß. Auch in dem Fall, daß die Moduln $\mathrm{ind}_B^G(1,\chi^k)$ bzw. $\mathrm{ind}_B^G(\chi^k,1)$ in nicht notwendig uniserielle Moduln zerfallen, läßt sich unsere Methode also anwenden, auch wenn sie etwas komplizierter ist und die Aussagen etwas schwächer als im uniseriellen Fall.

In den Beispielen fällt auf, daß die zentralen isotypischen Komponenten der beiden $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln $\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}$ und $D_S^0/pD_S^0\otimes\mathbb{F}$ bei gleichem Charakter immer dieselben einfachen Faktoren haben. Dies ist kein Zufall, sondern ein allgemein gültiger Sachverhalt.

SATZ 4.2.22. *Die $\mathbb{F}[\mathrm{GL}(2,\mathbb{F}_q)]$-Moduln $\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}$ und $D_S^0/pD_S^0\otimes\mathbb{F}$ haben dieselben einfachen Faktoren.*

BEWEIS. Wir zeigen dies jeweils für die zentralen isotypischen Komponenten $\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}(\psi)$ und $D_S^0/pD_S^0\otimes\mathbb{F}(\psi)$. Für $\psi=1$ gilt die Behauptung nach Satz 4.2.3. Für einen nichttrivialen zentralen Charakter $\psi=\chi^k$ zerlegen sich $\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}(\psi)=\mathrm{ind}_B^G(1,\psi)$ und $D_S^0/pD_S^0\otimes\mathbb{F}=\mathrm{ind}_B^G(\psi,1)=\mathrm{ind}_B^G(1,\chi^{q-1-k})\otimes\Delta^k$ mittels der exakten Folgen

$$0\to\mathrm{Sym}_k\to\mathrm{ind}_B^G(1,\chi^k)\to\mathrm{Sym}^*_{q-1-k}\to 0$$

und

$$0\to\mathrm{Sym}_{q-1-k}\otimes\Delta^k\to\mathrm{ind}_B^G(1,\chi^{q-1-k})\otimes\Delta^k\to 0\,.$$

Ist $S_{\underline{r}}\otimes\Delta^j$ ein einfacher Faktor von Sym_k, so gilt nach Proposition 3.6.14 die Kongruenz $v(\underline{r})\equiv k-2j \bmod q-1$. Für das Dual des einfachen Moduls bedeuted dies $(S_{\underline{r}}\otimes\Delta^j)^*\cong S_{\underline{r}}\otimes\Delta^{-j-v(\underline{r})}\cong S_{\underline{r}}\otimes\Delta^{j-k}$. Da die Duale der Faktoren von Sym_k gerade die Faktoren von Sym_k^* sind, haben Sym_k und $\mathrm{Sym}_k^*\otimes\Delta^k$ dieselben einfachen Faktoren. Entsprechend haben auch Sym_{q-1-k} und $\mathrm{Sym}^*_{q-1-k}\otimes\Delta^{q-1-k}$ dieselben einfachen Faktoren. Damit sind die einfachen Faktoren von $\mathrm{ind}_B^G(1, \chi^k)$ und $\mathrm{ind}_B^G(\chi^k, 1) \otimes \Delta^k$ dieselben. $\square$

Der Satz zeigt insbesondere, daß bei der Untersuchung eines Homomorphismus zwischen $\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}$ und $D_S^0/pD_S^0\otimes\mathbb{F}$ die Kenntnis der einfachen Faktoren allein noch keine Information über Kern und Kokern liefert. Auch eine Bestimmung der Brauer-Charaktere der Darstellungen würde somit nicht weiterhelfen, da $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$ wegen Satz 4.2.22 die gleichen Brauer-Charaktere haben.

Eine weitere Beobachtung bei den Beispielen besteht darin, daß in den Moduln $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$ kein einfacher Faktor mehrmals vorgekommen ist. Auch umfangreichere Computer-Berechnungen scheinen darauf hinzudeuten, daß dies immer der Fall ist. Beweisen können wir aber nur das folgende.

Satz 4.2.23. *Die einfachen Faktoren der* $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$*-Moduln* $\mathcal{S}/p\mathcal{S}\otimes \mathbb{F}$ *und* $D_S^0/pD_S^0 \otimes \mathbb{F}$ *haben alle höchstens die Vielfachheit* 2. *Ist* $r = p$ *und* $\mathfrak{p}$ *vom Grad* 2, *so haben die einfachen* $\mathbb{F}[\mathrm{GL}(2, \mathbb{F}_q)]$*-Faktoren von* $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ *und* $D_S^0/pD_S^0 \otimes \mathbb{F}$ *alle die Vielfachheit* 1.

Beweis. Aus Symmetriegründen reicht es, nur $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ zu betrachten. Zudem muß man die Behauptungen jeweils nur für die verschiedenen zentralen isotypischen Komponenten zeigen. Die Komponente zum trivialen zentralen Charakter ist selbst schon einfach. Sei also $\psi = \chi^k$ ein nichttrivialer zentraler Charakter. Die χ^k-Komponente von $\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}$ ist $\mathrm{ind}_B^G(1, \chi^k)$, ihre einfachen Faktoren sind die von Sym_k und Sym^*_{q-1-k}. Die Faktoren der Sym_k sind paarweise nichtisomorph, das gleiche gilt also auch für Sym^*_{q-1-k}. In $\mathrm{ind}_B^G(1, \chi^k)$ kann also höchstens Vielfachheit 2 auftreten.

Im Fall $q = p^2$ benutzen wir Satz 4.1.5, der explizit die Faktoren aller Sym_k angibt. Da wir nur an den Sym_k in den nichttrivialen zentralen Komponenten interessiert sind, genügt es, die k mit $k \equiv 0 \bmod p-1$ zu betrachten, d.h. die $k = x \cdot (p-1) = (x-1, p-x)$ für $x = 1, \ldots, p$, und zu zeigen, daß Sym_k und Sym^*_{q-1-k} keine einfachen Faktoren gemeinsam haben.

Ist $x = 1$, d.h. $k = p-1$, so hat Sym_k nur den Faktor $S_{(k,0)} \otimes \Delta^0$. Da dann $q-1-k = (0, p-1)$ ist, hat Sym_{q-1-k} die einfachen Faktoren $S_{(0,p-1)} \otimes \Delta^0$ und $S_{(p-2,p-2)} \otimes \Delta^1$. Die einfachen Faktoren von Sym^*_{q-1-k} sind daher $S_{(0,p-1)} \otimes \Delta^{-0-p\cdot(p-1)} = S_{(0,p-1)} \otimes \Delta^{p-1}$ und $S_{(p-2,p-2)} \otimes \Delta^{-1-[p-2+p\cdot(p-2)]} = S_{(p-2,p-2)} \otimes \Delta^p$ und folglich von dem Faktor von Sym_k verschieden.

Ist $x > 1$, so sind die Faktoren von Sym_k gerade $M_1 = S_{(p-x,x-1)} \otimes \Delta^0$ und $M_2 = S_{(x-2,x-2)} \otimes \Delta^{p-x+1}$. Die einfachen Faktoren von $q-1-k = (x-1, p-x)$ sind $S_{(x-1,p-x)}\otimes\Delta^0$ und $S_{(p-x-1,p-x-1)}\otimes\Delta^x$. Damit hat Sym^*_{q-1-k} die einfachen Faktoren $M_3 = S_{(x-1,p-x)} \otimes \Delta^{-0-[x-1+p\cdot(p-x)]} = S_{(x-1,p-x)} \otimes \Delta^{px-x}$ und $M_4 = S_{(p-x-1,p-x-1)} \otimes \Delta^{-x-[p-x-1+p\cdot(p-x-1)]} =$

$S_{(p-x-1,p-x-1)} \otimes \Delta^{px}$. Ein Vergleich der vorkommenden Indizes zeigt, daß M_1 verschieden von M_4 sowie M_2 verschieden von M_3 ist. Daß M_1 und M_3 verschieden sind, sieht man direkt durch Vergleich der Exponenten von Δ. Wäre schließlich $M_2 = M_4$, so ergäbe sich aus der Gleichheit der Indizes $x - 2 = p - x - 1$ und aus der Gleichheit der Δ-Exponenten $px \equiv p-x+1 = p-x-1+2 = x-2+2 = x \bmod q-1$, also $px - x \equiv 0 \bmod q - 1$ und auch das ist nicht möglich. □

Will man allgemeine Aussagen über die Siegeldivisorengruppe von $X(\mathfrak{p})$ machen, d.h. ohne in konkreten Beispielen den Algorithmus zu benutzen, so kann man nur die Information über die Sockel der zentralen isotypischen Komponenten von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$ verwenden.

Satz 4.2.24. *Sei $r = p^n$ und $\mathfrak{p}$ ein Primideal von $\mathbb{F}_r[T]$ vom Grad $d > 1$. Dann gilt für die Siegeldivisorklassengruppe $\mathcal{C}_{\text{Siegel}}$ der Drinfeld'schen Modulkurve $\#\mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}} = \#\mathcal{C}_{\text{Siegel}}[p] \geqslant p^r$, insbesondere ist $\#\mathcal{C}_{\text{Siegel}}$ durch p teilbar.*

Beweis. Wir müssen zeigen, daß die $\mathbb{F}$-Dimension des Kerns von $\operatorname{div} : \mathcal{S}/p\mathcal{S}\otimes\mathbb{F} \to D_S^0/pD_S^0\otimes\mathbb{F}$ mindestens r ist. Nun sind die zentralen isotypischen Komponenten zu einem nichttrivialen Charakter χ^k, $k \equiv 0 \bmod r-1$ von $\mathcal{S}/p\mathcal{S} \otimes \mathbb{F}$ und $D_S^0/pD_S^0 \otimes \mathbb{F}$ gegeben durch $\operatorname{ind}_B^G(1, \chi^k)$ und $\operatorname{ind}_B^G(1, \chi^{q-1-k}) \otimes \Delta^k$. Die Sockel dieser Moduln sind $S_{(k_0,\ldots,k_{e-1})} \otimes \Delta^0$ und $S_{(p-1-k_0,\ldots,p-1-k_{e-1})} \otimes \Delta^k$, wobei $e = d \cdot n$ und $k = (k_0, \ldots , k_{e-1})$ ist. Da diese Moduln nie isomorph sind, enthält der Kern von div mindestens die einfachen Faktoren $S_{(k_0,\ldots,k_{e-1})} \otimes \Delta^k$ für alle $0 < k < q-1$, $k \equiv 0 \bmod r-1$. Da die Dimension dieses Moduls das p-adische Querprodukt von k ist und dieses bei $k = r-1 = (p-1, \ldots , p-1\,[n-1], 0, \ldots , 0)$ gerade $p^n = r$ ergibt, folgt die Behauptung. □

Die in dem Beweis verwendete Abschätzung ist jedoch ziemlich schlecht. Zum einen betrachten wir nur der Sockel und nicht die gesamte Sockelreihe, zum anderen wird nur eine zentrale isotypische Komponente verwendet, da man für die p-adische Darstellung der $k \equiv 0 \bmod r - 1$ keine allgemeine Formel angeben kann, was zur Dimensionsberechnung aber nötig wäre. In der Situation von Beispiel 4.2.5 sagt Satz 4.2.24 nur $\#\mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}} \geqslant 3^3$ voraus, während unsere explizite Rechnung $\#\mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}} \geqslant 3^{20}$ ergab. Das Ergebnis von Satz 4.2.24 läßt sich allerdings noch deutlich verbessern, wenn man sich auf den einfachsten Fall, d.h. $r = p$, $q = p^2$ beschränkt.

Satz 4.2.25. *Sei $r = p$ und $\mathfrak{p}$ ein Primideal von $\mathbb{F}_r[T]$ vom Grad 2. Für die Siegeldivisorklassengruppe $\mathcal{C}_{\text{Siegel}}$ von $X(\mathfrak{p})$ gilt dann*

$$\#\mathcal{C}_{\text{Siegel}}/p\mathcal{C}_{\text{Siegel}} = \#\mathcal{C}_{\text{Siegel}}[p] \geqslant p^{(\frac{1}{6}p^3+\frac{1}{2}p^2+\frac{1}{3}p)}\,.$$

Beweis. Die nichttrivialen zentralen Charaktere von $G(\mathfrak{p})$ sind χ^k, $k = p-1, 2(p-1), \ldots , p(p-1)$. Die p-adische Darstellung eines $k = x \cdot (p-1)$ mit $1 \leqslant x \leqslant p$ ist $k = (p-x, x-1)$. Damit ist der Sockel von $(\mathcal{S}/p\mathcal{S}\otimes\mathbb{F})(\chi^k) = \mathrm{ind}_B^G(1,\chi^k)$ gerade $S_{(p-x,x-1)}\otimes\Delta^0$, während der Sockel von $D_S^0/pD_S^0\otimes\mathbb{F} = \mathrm{ind}_B^G(\chi^k,1)$ isomorph zu $S_{(x-1,p-x)}\otimes\Delta^k$ ist. Da die vorkommenden Exponenten von Δ nicht gleich bzw. kongruent modulo $q-1$ und die Sockel folglich nicht isomorph sind, enthält der Kern der Abbildung div mindestens die Faktoren $S_{(p-x,x-1)}\otimes\Delta^0$ für alle $x = 1,\ldots,p$. Die Dimension von $S_{(p-x,x-1)}\otimes\Delta^0$ ist gleich $x\cdot(p-x+1)$ und somit hat der Kern von div mindestens die Dimension $\sum_{x=1}^{p} x\cdot(p-x+1) = \frac{1}{6}p^3+\frac{1}{2}p^2+\frac{1}{3}p$. □

Im Fall von Beispiel 4.2.5 liefert dieser Satz nun immerhin $\mathcal{C}_{\mathrm{Siegel}}/p\mathcal{C}_{\mathrm{Siegel}} \geqslant 3^{10}$.

Um in der allgemeinen Situation noch bessere Ergebnisse zu erhalten, könnte man versuchen, nach weiteren Werten für den Parameter k zu suchen, die eine so speziell strukturierte p-adische Entwicklung besitzen, daß man das Ergebnis des Algorithmus in geschlossener Form vorhersagen kann. Je nach Resultat könnte dies in günstigen Fällen zu einer Verbesserung der Abschätzung der Ordnung von $\mathcal{C}_{\mathrm{Siegel}}/p\mathcal{C}_{\mathrm{Siegel}}$ führen. Im allgemeinen erhält man bestmögliche Ergebnisse aber nur, wenn man alle Informationen über die Sockelreihen von $\mathcal{S}/p\mathcal{S}\otimes\mathbb{F}$ und $D_S^0/pD_S^0\otimes\mathbb{F}$ ausnutzt, die sich mittels Algorithmus 3.6.15 für die vorkommenden symmetrischen Potenzen der natürlichen Darstellung ergeben. Neben den besseren Ergebnissen rechtfertigt sich diese Vorgehensweise außerdem auch dadurch, daß dabei als Parameter nur die Elementanzahl des Grundkörpers $\mathbb{F}_r$ und der Grad des Polynoms $\mathfrak{p}$ eingehen und die resultierende Abschätzung für die Anzahl der zyklischen p-Komponenten der Siegeldivisorklassengruppe von $X(\mathfrak{p})$ von der konkreten Wahl von $\mathfrak{p}$ unabhängig ist.

Literaturverzeichnis

[Al] Alperin, J. L.: Local representation theory. Cambridge Studies in Advanced Mathematics, 11. Cambridge University Press, Cambridge, 1986.

[Bo] Borel, A.: Properties and linear representations of Chevalley groups. 1970 Seminar on Algebraic Groups and Related Finite Groups (The Institute for Advanced Study, Princeton, N.J., 1968/69) pp. 1–55, Lecture Notes in Mathematics 131.

[BrNe1] Brauer, R.; Nesbitt, C.: On the modular representations of groups of finite order. Univ. of Toronto Studies, Math. Ser. 4. Toronto: Univ. of Toronto Press, 1937.

[BrNe2] Brauer, R.; Nesbitt, C.: On the modular characters of groups. Ann. of Math. (2) 42, (1941). 556-590.

[Ca] Carter, R. W.: Simple groups of Lie type. Pure and Applied Mathematics, Vol. 28. John Wiley & Sons, London-New York-Sydney, 1972.

[CuRe] Curtis, C. W.; Reiner, I.: Methods of representation theory. Vol. I. Pure and Applied Mathematics. A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1981.

[Dr1] Drinfeld, V. G.: Two theorems on modular curves. Functional Anal. Appl. 7 (1973), 155-156.

[Dr2] Drinfeld, V. G.: Elliptic modules. Math. USSR-Sb. 23 (1974), no. 4, 561-592.

[FrPu] Fresnel, J.; van der Put, M.: Géométrie analytique rigide et applications. Progress in Mathematics, 18. Birkhäuser, Boston, Mass., 1981.

[Ge1] Gekeler, E.-U.: Drinfeld-Moduln und modulare Formen über rationalen Funktionenkörpern. Bonner Mathematische Schriften 119. Universität Bonn, Mathematisches Institut, Bonn, 1980.

[Ge2] Gekeler, E.-U.: Modulare Einheiten für Funktionenkörper. J. Reine Angew. Math. 348 (1984), 94-115.

[Ge3] Gekeler, E.-U.: A product expansion for the discriminant function of Drinfeld modules of rank two. J. Number Theory 21 (1985), no. 2, 135-140.

[Ge4] Gekeler, E.-U.: Drinfeld modular curves. Lecture Notes in Mathematics 1231. Springer-Verlag, Berlin, 1986.

[Ge5] Gekeler, E.-U.: On the cuspidal divisor class group of a Drinfeld modular curve. Doc. Math. 2 (1997), 351-374.

[Ge6] Gekeler, E.-U.: Cuspidal divisor class groups of modular curves. Algebraic number theory and Diophantine analysis (Graz, 1998), 163-189, de Gruyter, Berlin, 2000.

[Ge7] Gekeler, E.-U.: On the Drinfeld discriminant function. Compositio Math. 106 (1997), no. 2, 181-202.

[Ge8] Gekeler, E.-U.: Growth order and congruences of coefficients of the Drinfeld discriminant function. J. Number Theory 77 (1999), no. 2, 314-325.

[Ge9] Gekeler, E.-U.: A note on the finiteness of certain cuspidal divisor class groups. Israel J. Math. 118 (2000), 357-368.

[Ge10] Gekeler, E.-U.: Asymptotically optimal towers of curves over finite fields AlgebraicGeometry Purdue 2000 (Abhyankar 70, to appear).

[Ge11] Gekeler, E.-U.: Invariants of some algebraic curves related to Drinfeld modular curves J. Number Theory (to appear).

[Ge12] Gekeler, E.-U.: Finite modular forms. Finite Fields Appl. (to appear).

[GeRe] Gekeler, E.-U.; Reversat, M.: Jacobians of Drinfeld modular curves. J. Reine Angew. Math. 476 (1996), 27-93.

[Gr] Gross, B. H.: Representation theory and the cuspidal group of $X(p)$. Duke Math. J. 54 (1987), no. 1, 67-75.

[Ha1] Hayes, D. R.: Explicit class field theory for rational function fields. Trans. Amer. Math. Soc. 189 (1974), 77-91.

[Ha2] Hayes, D. R.: Explicit class field theory in global function fields. Studies in algebra and number theory, pp. 173-217, Adv. in Math. Suppl. Stud., 6, Academic Press, New York-London, 1979.

[Hu] Humphreys, J. E.: Introduction to Lie algebras and representation theory. Graduate Texts in Mathematics, Vol. 9. Springer-Verlag, New York-Berlin, 1972.

[KuLa] Kubert, D. S.; Lang, S.: Modular units. Grundlehren der Mathematischen Wissenschaften 244. Springer-Verlag, New York-Berlin, 1981.

[KuMi] Kuhn, N. J.; Mitchell, S. A.: The multiplicity of the Steinberg representation of $\mathrm{GL}_n(\mathbb{F}_q)$ in the symmetric algebra. Proc. Amer. Math. Soc. 96 (1986), no. 1, 1-6.

[La1] Lang, S.: Algebra. Second edition. Addison-Wesley Publishing Company, Advanced Book Program, Reading, MA, 1984.

[La2] Lang, S.: Introduction to modular forms. Grundlehren der mathematischen Wissenschaften, No. 222. Springer-Verlag, Berlin-New York, 1976.

[Lu] Lucas, E.: Sur les congruences des nombres eulériens et des coefficients différentiels des fonctions trigonométriques, suivant un module premier. Bull. Soc. Math. France 6 (1878), 49-54.

[LoWa] López, B.; Wack, B.: On the expansion of a product formula related with the Drinfeld discriminant function. J. Number Theory 74 (1999), no. 2.

[Man] Manin, J. I. Parabolic points and zeta functions of modular curves. Math. USSR-Izv. 6 (1972), 19-64.

[Maz] Mazur, B.: Modular curves and the Eisenstein ideal. Inst. Hautes Études Sci. Publ. Math. No. 47 (1977), 33–186.

[MazWi] Mazur, B.; Wiles, A.: Class fields of abelian extensions of $\mathbb{Q}$. Invent. Math. 76 (1984), no. 2, 179–330.

[Mi] Miyake, T.: Modular forms. Springer-Verlag, Berlin, 1989.

[Ne] Neukirch, J.: Algebraische Zahlentheorie. Springer-Verlag, Berlin, 1992.

[PuDi] Puttaswamaiah, B. M.; Dixon, John D: Modular representations of finite groups. Pure and Applied Mathematics, No. 73. Academic Press, New York-London, 1977.

[Ri] Ribet, K. A.: A modular construction of unramified p-extensions of $\mathbb{Q}(\mu_p)$. Invent. Math. 34 (1976), no. 3, 151–162.

[Sh] Shimura, G.: Introduction to the arithmetic theory of automorphic functions. Publications of the Mathematical Society of Japan, No. 11. Iwanami Shoten, Publishers, Tokyo; Princeton University Press, Princeton, N.J., 1971.

[St1] Steinberg, R.: Representations of algebraic groups. Nagoya Math. J. 22 (1963), 33-56.

[St2] Steinberg, R.: Lectures on Chevalley groups. Notes prepared by John Faulkner and Robert Wilson. Yale University, New Haven, Conn., 1968.

[Wa] Wack, B.: Darstellungen von $\mathrm{SL}(2, \mathbb{F}_q)$ und $\mathrm{GL}(2, \mathbb{F}_q)$ in definierender Charakteristik. Diplomarbeit, Saarbrücken, 1996.

Symbolverzeichnis