Modulformen über endlichen Körpern

Staatsexamensarbeit

Oda Wagner

Studiengang Mathematik und Biologie
Lehramt an Gymnasien
Prüfer: Prof. Dr. E.-U. Gekeler

Saarbrücken, November 1998
Fachbereich 9, Mathematik

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

Inhaltsverzeichnis

Kapitel 0

Einleitung

Die vorliegende Arbeit beschäftigt sich mit der Theorie der Modulformen über endlichen Körpern, die sich einerseits als eine Spezialisierung von einem weit allgemeineren Fall (vgl. [Gek88] und [Gek]) begreift. Andererseits stellt die im Rahmen dieser Arbeit diskutierte Situation eine Analogie zu dem klassischen Fall der Modulformen (vgl. [Ser73]) dar.

In dem klassischen Fall sind Modulformen zunächst einmal Funktionen über der komplexen oberen Halbebene $H = \{z \in \mathbb{C} \mid Im\, z > 0\}$, die bestimmten Bedingungen gehorchen. Um diese zu formulieren, benötigen wir die Tatsache, daß die spezielle lineare Gruppe über den ganzen Zahlen $Sl(2, \mathbb{Z})$ vermöge

$$gz = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

für alle $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2, \mathbb{Z})$ und alle $z \in H$ auf H operiert. Eine Funktion $f \in H(z)$ heißt dann eine Modulform vom Gewicht $2k$, wenn sie auf H holomorph ist, eine Fourierentwicklung der Form

$$f(z) = \tilde{f}(q(z)) = \sum_{n=0}^{\infty} a_n q(z)^n$$

mit $q(z) = e^{2\pi i z}$ besitzt und unter $Sl(2, \mathbb{Z})$ das Transformationsverhalten

$$f(gz) = (cz+d)^{2k} f(z)$$

für $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2, \mathbb{Z})$ aufweist.

Diese klassische Situation wird nun auf den Fall des endlichen Körpers $\mathbb{F}_q$ übertragen. Entsprechend der komplexen oberen Halbebene H wird als Definitionsbereich einer Modulform f über $\mathbb{F}_q$ die Menge $\Omega = \overline{\mathbb{F}}_q - \mathbb{F}_q$ gewählt. Es operiert $\Gamma = Gl(2, \mathbb{F}_q)$, sprich die lineare Gruppe über $\mathbb{F}_q$, durch

$$\gamma z = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

für alle $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ und alle $z \in \Omega$ auf Ω. Korrespondierend zu der Holomorphiebedingung des klassischen Falls besitzt die rationale Funktion f Pole höchstens auf $\mathbb{F}_q$. Die Transformationsbedingung lautet analog

$$f(\gamma z) = \frac{(cz+d)^k}{(det\gamma)^m} f(z)$$

für $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma = Gl(2, \mathbb{F}_q)$, wobei $k \in \mathbb{N}_0$ als das Gewicht und $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ als der Typ der Modulform f bezeichnet wird.

Ein typisches Beispiel für Modulformen sind die Eisenstein-Reihen

$$E_k(z) = {\sum_{a,b \in \mathbb{F}_q}}' \frac{1}{(az+b)^k} \in \mathbb{F}_q(z),$$

die nur für $k \equiv 0 \mod (q-1)$ nicht verschwinden. Das Symbol $\sum'_{a,b\in\mathbb{F}_q}$ bedeutet, daß über die Menge $\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \mid (a,b) \neq (0,0)\}$ summiert wird. Unser Interesse besteht nun darin, die Nullstellen der Eisenstein-Reihen zu bestimmen. Dies geschieht im Rahmen der Arbeit für Gewichte von der Form $k = q^j - 1$.
Bevor im folgenden die Vorgehensweise erläutert wird, sei bemerkt, daß die in dieser Arbeit gewonnenen Ergebnisse denen des allgemeineren und des klassischen Falls entsprechen, jedoch mit elementaren Methoden bewiesen werden können.

In Kapitel 1 sind die gruppentheoretischen Grundlagen der linearen Gruppe $\Gamma = Gl(2, \mathbb{F}_q)$ über dem endlichen Körper $\mathbb{F}_q$ zusammengestellt. Neben der Bruhat-Zerlegung dieser Gruppe studieren wir im wesentlichen Operationen von Γ auf verschiedenen Mengen. Die Operation von Γ auf Ω ist die entscheidende, da wir im weiteren Verlauf der Arbeit die disjunkte Zerlegung von Ω, die durch die Operation von Γ auf Ω gegeben ist, benötigen.

Kapitel 2 behandelt ausführlicher als im Rahmen der Einleitung bereits geschehen die Theorie der Modulformen über der komplexen oberen Halbebene H. Sowohl die gruppentheoretischen Überlegungen aus Kapitel 1 als auch die in den nachfolgenden Kapiteln gewonnenen Erkenntnisse bezüglich der Modulformen über endlichen Körpern stellen Analogien zu dieser Theorie dar.

Die Grundlagen der Modulformen über endlichen Körpern erörtern wir anschließend in Kapitel 3. Neben der Definition werden wir einige Eigenschaften von Modulformen kennenlernen und unter anderem sehen, daß die rationale Funktion

$$t(z) = \frac{1}{z - z^q} \in \mathbb{F}_q(z)$$

eine Modulform ist. Sie spielt eine wichtige Rolle, da jede Modulform f als ein Polynom in $t = t(z)$ dargestellt werden kann:

$$f(z) = \tilde{f}\,(t(z)) = \tilde{f}(t) = \sum_{n=i}^{d} a_n t^n \ \in \overline{\mathbb{F}}_q[t].$$

Dieses Polynom vom Grad d heißt die t-Entwicklung einer Modulform und ist ein Analogon zur Fourierentwicklung.

Die Modulformen f eines Gewichts k und eines Typs m bilden den $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,m}(\Gamma)$, mit dem wir uns in Kapitel 4 beschäftigen. Mit Hilfe von Divisoren können wir zunächst den zentralen Satz über den Zusammenhang der Nullstellenordnungen mit dem Gewicht k und dem Grad d der t-Entwicklung formulieren und beweisen:

(i) $\sum_{a\in R} \nu_a(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q-1} = \frac{k}{q^2-1}$ und

(ii) $\sum_{a\in R} \nu_a(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q^2-1} = \frac{d}{q^2-1}$,

wobei R ein Repräsentantensystem von $\Gamma\backslash(\overline{\mathbb{F}}_q - \mathbb{F}_{q^2})$, $\nu_a(f)$ die Nullstellenordnung in $a \in R$, $\nu_e(f)$ die Nullstellenordnung in $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ und $\nu_\infty(f)$ die Nullstellenordnung in $t(z) = 0$ sind.
Die Verwendung dieses Satzes ermöglicht uns die Angabe einer Basis von $M_{k,m}(\Gamma)$ und der zugehörigen Dimension.

Nach diesen Vorarbeiten wenden wir uns in Kapitel 5 der Bestimmung der Nullstellen der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ zu. Ein wichtiges Hilfsmittel dazu stellen die Goss-Polynome $G_k(X) \in \mathbb{F}_q[X]$ dar, die es uns ermöglichen, die t-Entwicklung der Eisenstein-Reihen

$$E_k(z) = -(1 + G_k(t)) \in \mathbb{F}_q[t]$$

anzugeben. Mit deren Hilfe können wir dann die Nullstellen bestimmen, was uns leider nur unter der Voraussetzung gelingt, daß die Gewichte von der Form $k = q^j - 1$ sind. In diesem Fall liegen die Nullstellen in $\mathbb{F}_{q^{j+1}} - \mathbb{F}_q$ und sind einfach.

Um die Nullstellen für allgemeine Gewichte k angeben zu können, wurde ein Programm implementiert, dessen Ergebnisse in Kapitel 6 erörtert werden. Letztendlich können wir aber trotzdem nicht für allgemeine k eine geschlossene Form der Nullstellen angeben. Somit bleibt weiter offen, wie solch eine geschlossene Form aussehen könnte.

In erster Linie möchte ich Herrn Prof. Dr. E.-U. Gekeler für das interessante Thema und die sehr gute Betreuung danken. Er brachte viel Zeit und Geduld auf, meine zahlreichen Fragen zu beantworten und Ideen aufzuzeigen.
Mein ganz besonders herzlicher Dank gilt Herrn Dipl.-Math. M. Gebhardt, der mir bei der Einarbeitung in das Computeralgebrasystem SIMATH und der Programmierung zur Seite stand. Weiter war er mir durch intensives Korrekturlesen eine große Hilfe. Ferner danke ich Herrn Dipl.-Math. B. Wack und Herrn Dipl.-Inf. O. Scheja für das Beantworten meiner Fragen.
Ein lieber Dank geht an alle, die mich während der Anfertigung dieser Arbeit in irgendeiner Form unterstützt und so zu einem Gelingen beigetragen haben.

Kapitel 1

Grundlagen

In diesem Kapitel sind die zum Verständnis der Arbeit notwendigen Grundlagen beschrieben. Zum einen handelt es sich dabei um Notationen, zum anderen sind einige Eigenschaften der linearen Gruppe über einem beliebigen Körper K bzw. über dem endlichen Körper $\mathbb{F}_q$ zusammengestellt. Darüber hinaus werden die p-Sylow-Gruppen und die Konjugationsklassen der linearen Gruppe über $\mathbb{F}_q$ angegeben.

1.1 Notationen

Die folgenden Bezeichnungen werden durchgängig in dieser Arbeit verwendet.

$$
\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \dots\} \\
\mathbb{N}_0 &= \{0, 1, 2, \dots\} \\
\mathbb{Z} &= \text{die Menge der ganzen Zahlen} \\
\mathbb{R} &= \text{die Menge der reellen Zahlen} \\
\mathbb{C} &= \text{die Menge der komplexen Zahlen} \\
p &= \text{eine Primzahl} \\
q &= p^s \text{ mit } s \in \mathbb{N}, \text{ eine Primzahlpotenz} \\
\mathbb{F}_q &= \text{der endliche Körper der Charakteristik } p \text{ mit } q \text{ Elementen} \\
\mathbb{F}_q^* &= \text{die multiplikative Gruppe von } \mathbb{F}_q \\
\overline{\mathbb{F}}_q &= \text{der algebraische Abschluß von } \mathbb{F}_q \\
\Omega &= \overline{\mathbb{F}}_q - \mathbb{F}_q \\
\mathbb{F}_{q^n} &= \text{die Körpererweiterung von } \mathbb{F}_q \text{ in } \overline{\mathbb{F}}_q \text{ vom Grad } n \text{ mit } n \in \mathbb{N} \\
K &= \text{ein beliebiger Körper} \\
K[z] &= \text{der Ring der Polynome über } K \\
K(z) &= \text{der Körper der rationalen Funktionen über } K
\end{aligned}
$$

$$
\begin{aligned}
Gl(2,K) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in K^{2\times 2} \;\middle|\; ad-bc \neq 0 \right\}, \\
& \quad \text{die lineare Gruppe über } K \\
\Gamma &= Gl(2,\mathbb{F}_q), \text{ die lineare Gruppe über } \mathbb{F}_q \\
\#\cdot &= \text{die Kardinalität einer Menge.}
\end{aligned}
$$

Die Menge $\Omega = \overline{\mathbb{F}}_q - \mathbb{F}_q$ heißt die obere Halbebene über $\mathbb{F}_q$. Dieser Name erklärt sich aus der Analogie dieser Situation zu den reellen bzw. komplexen Zahlen: die Menge $H = \{z \in \mathbb{C} \mid Im\, z > 0\}$ wird als die komplexe obere Halbebene über den reellen Zahlen bezeichnet.

1.2 Einige Eigenschaften der linearen Gruppe $\Gamma = Gl(2,\mathbb{F}_q)$

Die Gruppe $\Gamma = Gl(2,\mathbb{F}_q)$ spielt in dieser Arbeit eine zentrale Rolle, so daß es Sinn macht, auf einige Eigenschaften dieser Gruppe ausführlich einzugehen. Teilweise werden diese für den allgemeineren Fall der Gruppe $Gl(2,K)$ diskutiert.
Zuerst wird die Kardinalität von Γ berechnet und für $Gl(2,K)$ und damit auch für $\Gamma = Gl(2,\mathbb{F}_q)$ eine Zerlegung angegeben. Weiter behandeln wir die Operation von $Gl(2,K)$ auf der projektiven Geraden $\mathbb{P}^1(K)$ bzw. von Γ auf der projektiven Geraden $\mathbb{P}^1(\overline{\mathbb{F}}_q)$. Als letztes werden für Γ die Stabilisatoren und die Bahnen bestimmt.
Wir beginnen mit der Betrachtung der Kardinalität.

Proposition 1.1. *Für die Kardinalität der Gruppe* $\Gamma = Gl(2,\mathbb{F}_q)$ *gilt:*

$$\#\Gamma = (q-1)^2\, q\, (q+1).$$

Beweis. Da jedes Element der Gruppe Γ eindeutig bestimmt ist durch seine Wirkung auf die Basisvektoren von $\mathbb{F}_q^2$, ist die Mächtigkeit der Gruppe Γ gleich der Anzahl der geordneten Basen von $\mathbb{F}_q^2$. Dementsprechend ist die Anzahl der verschiedenen geordneten Basen von $\mathbb{F}_q^2$ zu bestimmen.
Es gibt genau $q^2 - 1$ Möglichkeiten, den ersten Basisvektor zu wählen. Da der zweite Basisvektor nicht in dem Spann des ersten liegen darf, kann er auf $q^2 - q$ verschiedene Möglichkeiten gewählt werden. Das Produkt ergibt die Mächtigkeit der Gruppe Γ. $\square$

Im weiteren Verlauf der Arbeit wird eine Zerlegung der Gruppe Γ benötigt. Wir betrachten an dieser Stelle den allgemeineren Fall der Gruppe $Gl(2,K)$, wobei K ein beliebiger Körper ist.
Bevor wir uns der Zerlegung zuwenden, schauen wir uns die Definition der Borelgruppe von $Gl(2,K)$ an. Nachzulesen ist dies bei [Lan93, XIII, §8].

Definition 1.2. *Es sei K ein beliebiger Körper und K^* die multiplikative Gruppe von K. Die Untergruppe*

$$B := \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in K^{2\times 2} \;\mid\; a, d \in K^*,\, b \in K \right\}$$

von $Gl(2,K)$ heißt die Standard-Borelgruppe von $Gl(2,K)$.

Satz 1.3. *Es sei B die Standard-Borelgruppe der Gruppe $Gl(2,K)$,*

$$\begin{aligned} U &:= \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in K^{2\times 2} \;\mid\; u \in K \right\} \quad \textit{und} \\ \omega &:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in Gl(2,K). \end{aligned}$$

Dann besitzt die Gruppe $Gl(2,K)$ die folgende disjunkte Zerlegung

$$Gl(2,K) = B \,\dot\cup\, U\,\omega\,B = B \,\dot\cup\, B\,\omega\,U.$$

Diese Zerlegung heißt Bruhat-Zerlegung.

Beweis. Es kann nachgerechnet werden, daß ein Element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl(2,K)$ mit $c \neq 0$ wie folgt dargestellt werden kann:

$$\gamma = \begin{pmatrix} b - \frac{ad}{c} & a \\ 0 & c \end{pmatrix} \omega \begin{pmatrix} 1 & \frac{d}{c} \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & \frac{a}{c} \\ 0 & 1 \end{pmatrix} \omega \begin{pmatrix} c & d \\ 0 & b - \frac{ad}{c} \end{pmatrix}.$$

□

Es ist klar, daß es sich bei der Standard-Borelgruppe B und bei der Gruppe U um Untergruppen von $Gl(2,K)$ handelt.

Wenden wir uns jetzt der Operation der Gruppe $Gl(2,K)$ auf der projektiven Geraden $\mathbb{P}^1(K)$ zu. Dazu ist es notwendig, zuerst den Begriff der projektiven Geraden über einem beliebigen Körper K zu definieren und näher zu erläutern (vgl. [Lan93, S. 386]).
Zunächst stellen wir fest, daß auf dem Vektorraum K^2 über dem Körper K die folgende Äquivalenzrelation definiert werden kann. Seien (s,t) und (u,v) zwei Tupel mit $s,t,u,v \in K$. Diese sind äquivalent genau dann, wenn ein $\lambda \in K^*$ existiert mit $(\lambda s, \lambda t) = (u,v)$. Die Äquivalenzklassen werden mit

$$(u : v) := \{(\lambda u, \lambda v) \mid \lambda \in K^*\} \tag{1.1}$$

bezeichnet. Diese Erkenntnisse führen zu der folgenden Definition:

Definition 1.4. *Sei K ein beliebiger Körper. Dann heißt*

$$\mathbb{P}^1(K) := K \cup \{\infty\} = \{(u : v) \mid u, v \in K \textit{ und } (u,v) \neq (0,0)\}$$

die projektive Gerade über K, wobei die Elemente $x \in K$ und ∞ folgendermaßen identifiziert werden:

$$\begin{array}{rcl} K \cup \{\infty\} & \longrightarrow & \{(u:v) \mid u, v \in K \text{ und } (u,v) \neq (0,0)\} \\ x & \longmapsto & (x:1) \quad \text{für alle} \quad x \in K \\ \infty & \longmapsto & (1:0). \end{array}$$

Es stellt sich nun die Frage, wie sich die projektive Gerade eines Körpers zu der eines Teilkörpers verhält. Die folgende Proposition erläutert dies.

Proposition 1.5. *Seien K und L zwei beliebige Körper mit $K \subset L$. Dann gilt für die projektiven Geraden über K bzw. über L:*

$$\mathbb{P}^1(K) \subset \mathbb{P}^1(L).$$

Beweis. Es ist zu zeigen, daß zwei unter dem Körper K disjunkte Äquivalenzklassen auch unter dem Körper L disjunkt sind.
Dazu seien $u, v, \tilde{u}, \tilde{v} \in K$ mit $(u:v) \neq (\tilde{u}:\tilde{v})$ und $\lambda \in L - K$. Aus der Annahme $(\lambda u : \lambda v) = (\tilde{u}, \tilde{v})$ erhalten wir $\lambda u = \tilde{u}$ und $\lambda v = \tilde{v}$. Da $u \neq 0$ oder $v \neq 0$ folgt $\lambda \in K$, was ein Widerspruch zur Voraussetzung ist. $\square$

Jetzt betrachten wir die Operation der Gruppe $Gl(2, K)$ auf der projektiven Geraden $\mathbb{P}^1(K)$. Als weiterführende Literatur sei auf [Mey80] verwiesen.

Proposition 1.6. *Die Gruppe $Gl(2, K)$ operiert von links auf der projektiven Geraden $\mathbb{P}^1(K)$ vermöge*

$$\gamma\,(u:v) = (au + bv : cu + dv)\,,$$

wobei $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl(2, K)$ und $(u:v) \in \mathbb{P}^1(K)$.

Beweis. Ein Element $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl(2, K)$ operiert auf $\mathbb{P}^1(K)$ mittels der Abbildung

$$\begin{array}{rcl} Gl(2,K) \times \mathbb{P}^1(K) & \longrightarrow & \mathbb{P}^1(K) \\ (\gamma, (u:v)) & \longmapsto & (au + bv : cu + dv), \end{array}$$

wobei zu untersuchen ist,

(i) ob die Abbildung wohldefiniert ist. Da für zwei verschiedene Elemente $(s:t)$ und $(u:v)$ einer Äquivalenzklasse der projektiven Geraden $\mathbb{P}^1(K)$ ein $\lambda \in K^*$ existiert mit $(s:t) = (\lambda u : \lambda v)$, gilt

$$\begin{array}{rcl} \gamma\,(s:t) & = & (as + bt : cs + dt) \\ & = & (a\lambda u + b\lambda v : c\lambda u + d\lambda v) \\ & = & (\lambda\,(au + bv) : \lambda\,(cu + dv)) \\ & \overset{Gl.\,(1.1)}{=} & (au + bv : cu + dv) \\ & = & \gamma\,(u:v). \end{array}$$

(ii) ob $\mathbb{P}^1(K)$ unter der Gruppenoperation abgeschlossen ist. Dazu sei

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl(2,K) \quad \text{und} \quad (u:v) \in \mathbb{P}^1(K).$$

Es ist zu zeigen, daß

$$\gamma\,(u:v) = \begin{pmatrix} a & b \\ c & d \end{pmatrix}(u:v) = (au+bv : cu+dv) \neq (0:0) \tag{1.2}$$

gilt. Aufgrund der Bruhat-Zerlegung

$$Gl(2,K) = B \,\dot\cup\, U\,\omega\,B = B \,\dot\cup\, B\,\omega\,U$$

genügt es, die Ungleichung (1.2) für die beiden Matrizen $\omega = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ und $\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B$ zu zeigen.

(a) Für die Matrix $\omega = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ folgt mit

$$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}(u:v) = (v:u)$$

die Ungleichung (1.2) offensichtlich.

(b) Für die Matrix $\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$ gilt

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}(u:v) = (au+bv : dv).$$

Für $v \neq 0$ folgt $dv \neq 0$ und somit Ungleichung (1.2).
Sei $v = 0$. Nach Voraussetzung ist dann $u \neq 0$. Da für $a \in K^*$ ebenfalls $a \neq 0$ gilt, folgt $au \neq 0$ und daher

$$\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}(u:0) = (au:0) \neq (0,0).$$

Somit ist die Abgeschlossenheit der Gruppenoperation bewiesen.

(iii) ob das neutrale Element der Gruppe $Gl(2,K)$ jedes Element der projektiven Geraden $\mathbb{P}^1(K)$ auf sich selbst abbildet. Das neutrale Element der Gruppenoperation ist $\epsilon = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Es gilt für alle $(u:v) \in \mathbb{P}^1(K)$:

$$\epsilon(u:v) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}(u:v) = (u:v).$$

(iv) ob die Gruppenoperation assoziativ ist. Um die Assoziativität zu beweisen, betrachten wir die beiden Elemente

$$\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \text{ und } \gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in Gl(2, K).$$

Es ist zu zeigen, daß $(\gamma\gamma')(u : v) = \gamma(\gamma'(u : v))$ gilt. Mit der Gleichungskette

$$\begin{aligned} (\gamma\gamma')(u:v) &= \begin{pmatrix} aa'+bc' & ab'+bd' \\ ca'+dc' & cb'+dd' \end{pmatrix}(u:v) \\ &= ((aa'+bc')u + (ab'+bd')v : (ca'+dc')u + (cb'+dd')v) \\ &= (a(a'u+b'v) + b(c'u+d'v) : c(a'u+b'v) + d(c'u+d'v)) \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}(a'u+b'v : c'u+d'v) \\ &= \gamma(\gamma'(u:v)) \end{aligned}$$

folgt die Behauptung.

□

Im folgenden wird nur noch der Spezialfall der Gruppe $\Gamma = Gl(2, \mathbb{F}_q)$ behandelt. Zunächst ist aufgrund der Propositionen 1.5 und 1.6 klar, daß die obere Halbebene $\Omega = \overline{\mathbb{F}}_q - \mathbb{F}_q = \mathbb{P}^1(\overline{\mathbb{F}}_q) - \mathbb{P}^1(\mathbb{F}_q)$ stabil ist unter der Operation von $\Gamma = Gl(2, \mathbb{F}_q)$. Wir erhalten damit unmittelbar das folgende

Korollar 1.7. *Die Gruppe Γ operiert von links auf der oberen Halbebene Ω über $\mathbb{F}_q$ vermöge*

$$\gamma z = \frac{az+b}{cz+d},$$

wobei $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ *und* $z \in \Omega$.

Sei $\varphi : \Omega \longrightarrow \overline{\mathbb{F}}_q,\ x \longmapsto (x : 1)$ aus Definition 1.4 die Einbettung von Ω in $\overline{\mathbb{F}}_q$. Dann gilt für die Operation von Γ auf Ω bzw. $\overline{\mathbb{F}}_q$ für alle $z \in \Omega$, $\gamma \in \Gamma$

$$\varphi(\gamma z) = \gamma \cdot \varphi(z).$$

An anderer Stelle der Arbeit wird eine Zerlegung der projektiven Geraden $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ bzw. der oberen Halbebene Ω in disjunkte Mengen benötigt. Vermöge einer Operation einer Gruppe G auf einer Menge N wird auf dieser eine Äquivalenzrelation

$$m \sim n \quad :\Leftrightarrow \quad \exists g \in G \text{ mit } gm = n \quad (m, n \in N)$$

induziert, d.h. durch die Operation der Gruppe Γ auf der projektiven Geraden $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ bzw. auf Ω werden diese Mengen in Äquivalenzklassen, die Bahnen, zerlegt. Um die Länge einer Bahn zu berechnen, wird der Begriff des Stabilisators, der auch Fixgruppe genannt wird, verwendet. Der Stabilisator von $z \in \Omega$ in Γ ist definiert als

$$\Gamma_z := \{\gamma \in \Gamma \mid \gamma z = z\}. \tag{1.3}$$

Jetzt kann die Länge der Bahn $\Gamma \cdot z$ von z mit Hilfe des Stabilisators über die Bahnengleichung

$$\#\Gamma \cdot z = \#(\Gamma : \Gamma_z)$$

berechnet werden.
Zunächst einmal betrachten wir die Bahn der Elemente $(u : v) \in \mathbb{P}^1(\mathbb{F}_q)$, über die das folgende Korollar Auskunft gibt.

Korollar 1.8. *Die Gruppe Γ operiert transitiv auf $\mathbb{P}^1(\mathbb{F}_q)$, d.h. die Elemente $(u : v)$ der projektiven Geraden $\mathbb{P}^1(\mathbb{F}_q)$ liegen alle in der Bahn*

$$\Gamma \cdot (u : v) = \mathbb{P}^1(\mathbb{F}_q).$$

Beweis. Die Aussage folgt direkt aus Proposition 1.6 und der Tatsache, daß Γ transitiv auf $\mathbb{F}_q^2 - \{0\}$ operiert. □

Wir behandeln jetzt die Operation der Gruppe Γ auf der oberen Halbebene Ω und bestimmen die Bahnen und die Stabilisatoren.

Proposition 1.9. *Für den Stabilisator Γ_z von $z \in \Omega$ gilt:*

$$\begin{aligned} \Gamma_z &= \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^* \right\} \quad \textit{für den Fall } z \notin \mathbb{F}_{q^2} \textit{ und} \\ \Gamma_z &\cong \mathbb{F}_{q^2}^* \quad \textit{für den Fall } z \in \mathbb{F}_{q^2} - \mathbb{F}_q. \end{aligned}$$

Dabei ist $\mathbb{F}_{q^2}$ die wohlbestimmte quadratische Erweiterung von $\mathbb{F}_q$ in $\overline{\mathbb{F}}_q$. Für die Bahnen $\Gamma \cdot z$ von Γ in Ω gilt:

$$\begin{aligned} \#\Gamma \cdot z &= (q-1)\, q\, (q+1) \quad \textit{für den Fall } z \notin \mathbb{F}_{q^2} \textit{ und} \\ \Gamma \cdot z &= \mathbb{F}_{q^2} - \mathbb{F}_q \quad \textit{für den Fall } z \in \mathbb{F}_{q^2} - \mathbb{F}_q. \end{aligned}$$

Beweis. Wir beginnen den Beweis mit der Bestimmung der Stabilisatoren. Dabei werden wir auf die Unterscheidung der beiden Fälle $z \in \Omega - \mathbb{F}_{q^2}$ und $z \in \mathbb{F}_{q^2} - \mathbb{F}_q$ stoßen. Für den ersten Fall lassen sich die Stabilisatoren und die Bahnen einfach berechnen. Der Beweis des zweiten Falls hingegen ist etwas langwieriger und vor allem sehr technisch.

Sofort ist klar, daß die Skalarmatrizen $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \Gamma$ mit $a \in \mathbb{F}_q^*$ trivial auf der oberen Halbebene Ω operieren. Demzufolge gilt für den Stabilisator die Inklusion

$$\Gamma_z \supseteq \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^* \right\}$$

in jedem Fall. Um festzustellen, ob es irgendwelche Elemente $z \in \Omega$ gibt, die einen größeren Stabilisator besitzen, verwenden wir die Definition des Stabilisators (1.3) und erhalten mit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ und $z \in \Omega$ die folgenden Äquivalenzumformungen

$$\begin{array}{rrcl} & \gamma z & = & z \\ \Leftrightarrow & \frac{az+b}{cz+d} & = & z \\ \Leftrightarrow & 0 & = & cz^2 + (d-a)z - b. \end{array} \tag{1.4}$$

Zu beachten ist, daß der Nenner $cz + d$ wegen $z \notin \mathbb{F}_q$ niemals verschwinden kann. Die Gleichung (1.4) besitzt genau dann Lösungen, wenn ihre Koeffizienten identisch gleich 0 sind oder wenn $z \in \Omega$ echt in der quadratischen Erweiterung $\mathbb{F}_{q^2}$ von $\mathbb{F}_q$ liegt. Folglich sind die beiden Fälle $z \in \Omega - \mathbb{F}_{q^2}$ und $z \in \mathbb{F}_{q^2} - \mathbb{F}_q$ zu unterscheiden.

Für $z \notin \mathbb{F}_{q^2}$ müssen alle Koeffizienten identisch gleich 0 sein. Der Stabilisator enthält daher nur die Skalarmatrizen, d.h.

$$\Gamma_z = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^* \right\},$$

und besitzt somit die Kardinalität $\#\Gamma_z = q - 1$.
Mit Hilfe der Bahnengleichung $\#\Gamma \cdot z = \#(\Gamma : \Gamma_z)$ berechnen wir die Länge der einzelnen Bahnen:

$$\#\Gamma \cdot z = \frac{(q-1)^2\, q\, (q+1)}{q-1} = (q-1)\, q\, (q+1).$$

Mit anderen Worten: $\overline{\mathbb{F}}_q - \mathbb{F}_{q^2}$ zerfällt in Bahnen der Länge $(q-1)\, q\, (q+1)$.

Wenden wir uns jetzt dem Fall $z \in \mathbb{F}_{q^2} - \mathbb{F}_q$ zu und betrachten Gleichung (1.4). Durch einfaches Abzählen der Anzahl der möglichen Lösungen für die Koeffizienten erhalten wir die Kardinalität des Stabilisators.
Wird c auf 1 skaliert, so betrachten wir das Minimalpolynom von $z \in \mathbb{F}_{q^2} - \mathbb{F}_q$. Es sind b und $d - a$ eindeutig bestimmt, d.h. es gibt genau q verschiedene Möglichkeiten a und somit d zu wählen. Für c existieren insgesamt q Alternativen. Zu beachten ist, daß für $c = 0$ gerade $b = 0$ und daher $a, d \neq 0$ gilt. Es ergibt sich für die Mächtigkeit des Stabilisators

$$\#\Gamma_z = q^2 - 1 = \#\mathbb{F}_{q^2}^*.$$

Aufgrund der Stabilität von $\mathbb{F}_{q^2} - \mathbb{F}_q$ unter Γ (vgl. Propositionen 1.5 und 1.6) folgt

$$\Gamma \cdot z = \mathbb{F}_{q^2} - \mathbb{F}_q.$$

Um als letztes noch die Isomorphie des Stabilisators Γ_z zu $\mathbb{F}_{q^2}^*$ zu zeigen, fassen wir $\mathbb{F}_{q^2}$ als einen $\mathbb{F}_q$-Vektorraum auf. Dieser besitzt die Dimension 2 und eine Basis $\mathcal{B} = \{1, z\}$. Weiter sei $z^2 + uz + v = 0$ für $z \in \mathbb{F}_{q^2} - \mathbb{F}_q$ die eindeutig bestimmte Minimalgleichung mit den Koeffizienten $u \in \mathbb{F}_q$ und $v \in \mathbb{F}_q^*$. Wir betrachten die Multiplikation mit z und stellen diese durch die Abbildung ψ_z und eine Abbildungsmatrix A bezüglich der Basis $\mathcal{B} = \{1, z\}$ dar:

$$\begin{aligned} \psi_z : \mathbb{F}_{q^2} &\longrightarrow \mathbb{F}_{q^2} \\ w &\longrightarrow w \cdot z. \end{aligned}$$

Da $\psi_z(1) = z$ und $\psi_z(z) = -uz - v$ ist, ergibt sich für die Abbildungsmatrix

$$A = \begin{pmatrix} -u & -v \\ 1 & 0 \end{pmatrix}.$$

Durch einfaches Nachrechnen läßt sich zeigen, daß die Abbildung

$$\begin{aligned} \varphi : \quad \mathbb{F}_{q^2}^* &\longrightarrow \Gamma_z \\ r + sz &\longrightarrow \begin{pmatrix} r - su & -sv \\ s & r \end{pmatrix} = \begin{pmatrix} r & 0 \\ 0 & r \end{pmatrix} + s \cdot \begin{pmatrix} -u & -v \\ 1 & 0 \end{pmatrix} \end{aligned}$$

mit $r, s \in \mathbb{F}_q$ und $(r, s) \neq (0, 0)$ ein Isomorphismus ist. $\square$

Wir haben gesehen, daß die projektive Gerade $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ durch die Operation der Gruppe Γ in disjunkte Bahnen zerlegt wird. Es gibt drei verschiedene Typen von Bahnen, die in der folgenden Tabelle übersichtlich zusammengestellt sind:

Typ der Bahn	Länge der Bahn	Anzahl der Bahnen
$z \in \mathbb{P}^1(\mathbb{F}_q)$	$q + 1$	1
$z \in \mathbb{F}_{q^2} - \mathbb{F}_q$	$(q - 1)q$	1
$z \in \Omega - \mathbb{F}_{q^2}$	$(q - 1)q(q + 1)$	∞

Mit diesen Erkenntnissen gelangen wir zu der folgenden Definition.

Definition 1.10. *Sei $\mathbb{F}_q$ der Körper mit q Elementen und $\mathbb{F}_{q^2}$ seine quadratische Erweiterung. $\overline{\mathbb{F}}_q$ sei der algebraische Abschluß von $\mathbb{F}_q$. Dann heißen alle Punkte $z \in \overline{\mathbb{F}}_q$, für die*

$$z \in \mathbb{F}_{q^2} - \mathbb{F}_q$$

gilt, elliptische Punkte. Sie werden mit $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ bezeichnet.

1.3 Die p-Sylow-Gruppen von $\Gamma = Gl(2, \mathbb{F}_q)$

Im folgenden schauen wir uns die p-Sylow-Gruppen (vgl. [Mey80]) der Gruppe Γ an, bei deren Berechnung ebenfalls die Operation der Gruppe Γ auf einer Menge, in diesem Fall auf der Menge aller Untergruppen der Gruppe Γ, eine Rolle spielen wird. Zuerst betrachten wir die Definition für p-Sylow-Gruppen.

Definition 1.11. *Es sei G eine endliche Gruppe und $U_1 \leq G$ eine Untergruppe von G. Die Gruppe U_1 heißt eine p-Sylow-Gruppe von G, wenn gilt:*

(i) U_1 ist eine p-Untergruppe von G und

(ii) ist U_2 eine p-Untergruppe von G mit $U_1 \subseteq U_2$, dann ist $U_1 = U_2$.

Mit dieser Definition ist klar, daß p-Sylow-Gruppen maximale p-Untergruppen einer Gruppe sind. Nach den Sätzen von Sylow [Mey80] sind alle p-Sylow-Gruppen einer endlichen Gruppe G zueinander konjugiert und haben die Ordnung p^n, falls $p^n \mid \#G$ und $p^{n+1} \nmid \#G$ gilt. Der folgende Satz gibt an, wie die p-Sylow-Gruppen der Gruppe Γ aussehen und wie viele es gibt.

Satz 1.12. *Es ist*

$$P := \{V \leq \Gamma \mid \exists\, \gamma \in \Gamma \textit{ mit } \gamma\, U\, \gamma^{-1} = V\}$$

die Menge aller p-Sylow-Gruppen der Gruppe Γ, wobei U die p-Sylow-Gruppe

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \;\mid\; u \in \mathbb{F}_q \right\}$$

ist. Insgesamt gibt es $q+1$ verschiedene p-Sylow-Gruppen der Gruppe Γ.

Bei der Gruppe U handelt es sich um die uns bekannte Gruppe U der Bruhat-Zerlegung (vgl. Satz 1.3) für den Spezialfall der Gruppe $\Gamma = Gl(2, \mathbb{F}_q)$.

Beweis. Der Beweis verläuft in zwei Schritten:
Im ersten Schritt wird gezeigt, daß U eine p-Sylow-Gruppe ist und daß alle p-Sylow-Gruppen in der Menge P zusammengefaßt werden können. Im zweiten Schritt wird die Anzahl der verschiedenen p-Sylow-Gruppen der Gruppe Γ bestimmt.

Die Gruppe $U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \;\mid\; u \in \mathbb{F}_q \right\}$ hat die Ordnung $q = p^s$. Da q der maximale p-Teiler von $\#\,\Gamma = (q-1)^2 q(q+1)$ ist, ist U eine p-Sylow-Gruppe von Γ.
Nach den Sylowschen Sätzen sind alle p-Sylow-Gruppen zueinander konjugiert, insbesondere sind sie alle zu der schon bekannten p-Sylow-Gruppe U konjugiert. Folglich können diese in der Menge

$$P = \{V \leq \Gamma \mid \exists\, \gamma \in \Gamma \text{ mit } \gamma\, U\, \gamma^{-1} = V\}$$

zusammengefaßt werden.

Die Anzahl der p-Sylow-Gruppen entspricht der Mächtigkeit der Menge P. Diese wird mit Hilfe der folgenden Überlegungen bestimmt.
Es sei $M := \{V < \Gamma\}$ die Menge aller Untergruppen V der Gruppe Γ. Vermöge der Konjugation

$$\begin{array}{rcl} \Gamma \times M & \longrightarrow & M \\ (\gamma, V) & \longmapsto & \gamma\, V\, \gamma^{-1} \end{array}$$

operiert die Gruppe Γ von links auf der Menge M. Die Menge M wird durch diese Konjugation in disjunkte Bahnen zerlegt. Da alle p-Sylow-Gruppen zueinander konjugiert sind und somit in einer Bahn liegen, gilt für die Bahn der p-Sylow-Gruppen von Γ

$$\Gamma \cdot U = \{\gamma\, U\, \gamma^{-1} \mid \gamma \in \Gamma\} = P.$$

Um mit Hilfe der Bahnengleichung

$$\#\Gamma \cdot U = \#(\Gamma : \Gamma_U)$$

die Mächtigkeit der Menge P bestimmen zu können, berechnen wir die Kardinalität des Stabilisators der p-Sylow-Gruppe U. Für den Stabilisator gilt:

$$\Gamma_U = \{\gamma \in \Gamma \mid \gamma\, U\, \gamma^{-1} = U\}. \tag{1.5}$$

Mit $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ und $\alpha = \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in U$ ergibt sich

$$\begin{aligned} \gamma\, \alpha\, \gamma^{-1} &= (ad-bc)^{-1} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix} \\ &= (ad-bc)^{-1} \cdot \begin{pmatrix} ad-bc-acu & a^2u \\ -c^2u & ad-bc+acu \end{pmatrix}. \end{aligned}$$

Folglich gilt $\gamma\, \alpha\, \gamma^{-1} \in U$ für alle $\alpha \in U$ genau dann, wenn $c = 0$ ist. Dementsprechend erhalten wir für den Stabilisator

$$\Gamma_U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, d \in \mathbb{F}_q^*, b \in \mathbb{F}_q \right\}.$$

Der Stabilisator Γ_U ist mit der Standard-Borelgruppe B (vgl. Definition 1.2) für den hier betrachteten Spezialfall von $\Gamma = Gl(2, \mathbb{F}_q)$ identisch.
Für die Kardinalität des Stabilisators gilt $\#\Gamma_U = (q-1)^2 q$. Somit läßt sich die Mächtigkeit der Menge P berechnen:

$$\#P = \frac{\#\Gamma}{\#\Gamma_U} = \frac{(q-1)^2 q(q+1)}{(q-1)^2 q} = q + 1.$$

Es gibt also $q+1$ verschiedene p-Sylow-Gruppen der Ordnung $p^s = q$, die alle zu der p-Sylow-Gruppe $U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \mid u \in \mathbb{F}_q \right\}$ konjugiert sind. $\square$

1.4 Die Konjugationsklassen von $\Gamma = Gl(2, \mathbb{F}_q)$

Als letzte Eigenschaft der Gruppe Γ beschäftigen wir uns mit den Konjugationsklassen, d.h. wir betrachten die Operation der Gruppe Γ von links auf sich selbst durch

$$\begin{array}{rcl} \Gamma \times \Gamma & \longrightarrow & \Gamma \\ (\delta, \gamma) & \longmapsto & \delta \, \gamma \, \delta^{-1} \end{array} \tag{1.6}$$

und berechnen die Bahnen von Elementen aus Γ. Diese Operation wird als Konjugation bezeichnet und die Bahnen heißen Konjugationsklassen. Bevor wir uns dem Satz [PS83] zuwenden, der uns Auskunft über die verschiedenen Konjugationsklassen gibt, benötigen wir folgende Definitionen [Lan93].

Definition 1.13. *Es sei $\mathbb{F}_q$ ein endlicher Körper und $\mathbb{F}_{q^n}$ eine Körpererweiterung vom Grad n. Dann wird mit*

$$Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) := \sum_{i=0}^{n-1} x^{q^i}$$

die Spur von $x \in \mathbb{F}_{q^n}$ und mit

$$N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) := \prod_{i=0}^{n-1} x^{q^i}$$

die Norm von $x \in \mathbb{F}_{q^n}$ bezeichnet.

Weiter werden die folgenden Bezeichnungen verwendet. Das Element

$$\bar{x} := x^q \ \in \mathbb{F}_{q^2} - \mathbb{F}_q$$

heißt zu $x \in \mathbb{F}_{q^2} - \mathbb{F}_q$ konjugiert. Sei $\epsilon = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ das neutrale Element der Gruppe Γ. Dann lautet das charakteristische Polynom für $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$

$$f_\gamma(z) := \det(\gamma - \epsilon z) = z^2 - (a+d)z + ad - bc \in \mathbb{F}_q[z]$$

und das Minimalpolynom von $\gamma \in \Gamma$ wird mit $m_\gamma(z) \in \mathbb{F}_q[z]$ bezeichnet.

Satz 1.14. *Es gibt vier verschiedene Typen von Konjugationsklassen der Gruppe Γ. Diese lauten folgendermaßen:*

(i)

$$c_1(x) := \Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix},$$

falls $x \in \mathbb{F}_q$ eine doppelte Nullstelle von $f_\gamma(z)$ ist und $f_\gamma(z) \neq m_\gamma(z)$ gilt.

(ii)
$$c_2(x) := \Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix},$$
falls $f_\gamma(z)$ in $x \in \mathbb{F}_q$ eine doppelte Nullstelle besitzt und $f_\gamma(z) = m_\gamma(z)$ ist.

(iii)
$$c_3(x, y) = c_3(y, x) := \Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix},$$
falls $f_\gamma(z)$ die zwei verschiedenen Nullstellen $x, y \in \mathbb{F}_q$ besitzt.

(iv)
$$c_4(x) = c_4(\bar{x}) := \Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} 0 & -N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \\ 1 & Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \end{pmatrix},$$
falls $x, \bar{x} \in \mathbb{F}_{q^2} - \mathbb{F}_q$ die zueinander konjugierten Nullstellen von $f_\gamma(z)$ sind.

Beweis. Wir betrachten die Konjugation der Gruppe Γ, wie sie in Gleichung (1.6) angegeben ist, wobei die Bahnen der durch diese Gruppenoperation induzierten Äquivalenzrelation die Konjugationsklassen sind.

Die in einer Konjugationsklasse liegenden Matrizen sind zueinander ähnlich. Da ähnliche Matrizen dasselbe charakteristische Polynom und dieselben Eigenwerte besitzen, sind alle in einer Konjugationsklasse liegenden Matrizen zu einer Matrix in Jordanscher Normalform ähnlich. Diese Zusammenhänge gelten über einem algebraisch abgeschlossenen Körper, d.h. in unserem Fall über $\overline{\mathbb{F}}_q$. Nach [Lan93, XIV, §2 Cor. 2.3.] sind zwei unter $Gl(2, \overline{\mathbb{F}}_q)$ zueinander konjugierte Matrizen aus $\Gamma = Gl(2, \mathbb{F}_q)$ auch unter Γ zueinander konjugiert. Da die Konjugationsklassen unter $Gl(2, \overline{\mathbb{F}}_q)$ eindeutig durch die Jordansche Normalform und diese im Fall von 2×2-Matrizen eindeutig durch $f_\gamma(z)$ und $m_\gamma(z)$ bestimmt sind, ist die Konjugationsklasse einer Matrix unter Γ eindeutig durch ihr charakteristisches Polynom und ihr Minimalpolynom beschrieben.

Das charakteristische Polynom zerfällt in Abhängigkeit von den Koeffizienten über $\mathbb{F}_q$ in Linearfaktoren oder es ist über $\mathbb{F}_q$ irreduzibel und zerfällt dann über der quadratischen Erweiterung $\mathbb{F}_{q^2}$ des Körpers $\mathbb{F}_q$ in Linearfaktoren. Wir unterscheiden bezüglich der Nullstellen mehrere Fälle.

(i) Sei $x \in \mathbb{F}_q$ eine doppelte Nullstelle von $f_\gamma(z)$ und $f_\gamma(z) \neq m_\gamma(z)$. Folglich sind alle in dieser Konjugationsklasse liegenden Matrizen der Matrix in Jordanscher Normalform $\delta_1 = \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ ähnlich und für die Konjugationsklasse gilt
$$\Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix} =: c_1(x).$$

(ii) Wiederum sei $x \in \mathbb{F}_q$ eine doppelte Nullstelle von $f_\gamma(z)$, wobei in diesem Fall $f_\gamma(z) = m_\gamma(z)$ gelte. Daher sind alle in dieser Konjugationsklasse liegenden Matrizen der Matrix in Jordanscher Normalform $\delta_2 = \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$ ähnlich und wir erhalten

$$\Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix} =: c_2(x).$$

(iii) Es seien $x, y \in \mathbb{F}_q$ die verschiedenen Nullstellen von $f_\gamma(z)$. Dies ist gleichbedeutend damit, daß alle in dieser Konjugationsklasse liegenden Matrizen ähnlich der Matrix in Jordanscher Normalform $\delta_3 = \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$ sind. Somit ist

$$\Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix} =: c_3(x, y),$$

wobei $c_3(x, y) = c_3(y, x)$ gilt.

(iv) Es seien $x, y \in \mathbb{F}_{q^2} - \mathbb{F}_q$ die Nullstellen von $f_\gamma(z)$, d.h. es gilt

$$f_\gamma(z) = m_\gamma(z).$$

Da $\mathbb{F}_q$ als endlicher Körper vollkommen ist, sind die Nullstellen einfach und es gilt $y = \bar{x} = x^q$. Somit besitzt $f_\gamma(z)$ die Form

$$\begin{aligned} f_\gamma(z) &= (z - x) \cdot (z - x^q) \\ &= z^2 - z \cdot (x + x^q) + x \cdot x^q \\ &= z^2 - Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \cdot z + N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x). \end{aligned}$$

Es stimmen γ und δ_4 im Minimalpolynom und im charakteristischen Polynom überein.

Dementsprechend ist γ konjugiert zu $\delta_4 = \begin{pmatrix} 0 & -N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \\ 1 & Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \end{pmatrix}$ und es ergibt sich

$$\Gamma \cdot \gamma = \Gamma \cdot \begin{pmatrix} 0 & -N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \\ 1 & Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \end{pmatrix} =: c_4(x),$$

wobei $c_4(x) = c_4(\bar{x})$ gilt.

$\square$

Nachdem wir jetzt wissen, wie die verschiedenen Typen der Konjugationsklassen aussehen, stellt sich die Frage nach der Anzahl der einzelnen Konjugationsklassen pro Typ und nach der jeweiligen Mächtigkeit. Die Anzahl dieser Klassen läßt sich direkt aus der Darstellung der Konjugationsklassen ablesen. Die Mächtigkeit der einzelnen Klassen, sprich die Länge der einzelnen Bahnen, wird wie üblich über die Bahnengleichung

$$\#c_i(x) = \frac{\#\Gamma}{\#\Gamma_{\delta_i}} \quad \text{für } i = 1, 2, 4$$

bzw.

$$\#c_3(x, y) = \frac{\#\Gamma}{\#\Gamma_{\delta_3}}$$

berechnet. Die einzelnen $\#c_i(x)$ mit $i = 1, 2, 4$ bzw. $\#c_3(x, y)$ besitzen für verschiedene x dieselbe Kardinalität. Im folgenden wird mit $\#c_i$ die Länge der $\#c_i(x)$ bzw. $\#c_3(x, y)$ bezeichnet.
Die Bestimmung der verschiedenen Stabilisatoren ist recht einfach, es sei denn die Nullstellen des charakteristischen Polynoms liegen in $\mathbb{F}_{q^2} - \mathbb{F}_q$. In diesem Fall berechnen wir die Kardinalität der Konjugationsklasse $c_4(x)$ über die Mächtigkeit und die Anzahl der übrigen Konjugationsklassen. Sei dazu a_i die Anzahl der Konjugationsklassen von dem Typ i, so gilt

$$\begin{array}{rcl} \#\Gamma & = & \sum_{i=1}^{4}(a_i \cdot \#c_i) \\ \text{und deshalb } \#c_4(x) & = & \frac{1}{a_4}\left(\#\Gamma - \sum_{i=1}^{3}(a_i \cdot \#c_i)\right). \end{array}$$

Auf einen detaillierten Beweis wird an dieser Stelle verzichtet und statt dessen auf [Lan93, XVIII, § 12] verwiesen. Die Ergebnisse sind in der folgenden Tabelle zusammengefaßt:

Klassentyp	Anzahl der Klassen	Elemente in der Klasse
$c_1(x),\ x \in \mathbb{F}_q^*$	$q-1$	1
$c_2(x),\ x \in \mathbb{F}_q^*$	$q-1$	q^2-1
$c_3(x,y),\ x, y \in \mathbb{F}_q^*,\ x \neq y$	$\frac{(q-1)(q-2)}{2}$	q^2+q
$c_4(x),\ x \in \mathbb{F}_{q^2} - \mathbb{F}_q$	$\frac{q^2-q}{2}$	q^2-q

Wir haben uns in diesem Kapitel der Arbeit mit der linearen Gruppe über dem endlichen Körper $\mathbb{F}_q$ vertraut gemacht. Insbesondere der Themenkomplex der Operation der Gruppe $\Gamma = Gl(2, \mathbb{F}_q)$ auf verschiedenen Mengen wurde sehr ausführlich erörtert. Dieses Wissen wird uns im Laufe der vorliegenden Arbeit von sehr großem Nutzen sein. Ein weiteres sehr wichtiges Ergebnis ist die Bruhat-Zerlegung der Gruppe Γ, die ebenfalls weitreichende Anwendung finden wird.

Kapitel 2

Die Modulformen über der komplexen oberen Halbebene

Bevor die Modulformen über endlichen Körpern definiert werden, soll aufgezeigt werden, wie die Arbeit durch den sogenannten klassischen Fall der Modulformen motiviert ist. In aller Kürze werden im folgenden die wichtigsten Ergebnisse dieser Theorie vorgestellt. Als weiterführende Literatur sei auf [Ser73] verwiesen.

Wir betrachten die komplexe obere Halbebene $H = \{z \in \mathbb{C} \mid Im(z) > 0\}$. Auf dieser operiert die spezielle lineare Gruppe

$$Sl(2,\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbb{Z}^{2\times 2} \mid ad - bc = 1 \right\}$$

vermöge

$$gz = \begin{pmatrix} a & b \\ c & d \end{pmatrix} z = \frac{az+b}{cz+d}$$

für alle $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2,\mathbb{Z})$ und alle $z \in H$.
An dieser Stelle sei auf einen Unterschied zu der Gruppe $\Gamma = Gl(2,\mathbb{F}_q)$ hinsichtlich der Determinanten hingewiesen. Die Matrizen der Gruppe $Sl(2,\mathbb{Z})$ besitzen Determinanten 1, wodurch sichergestellt ist, daß die komplexe obere Halbebene durch die Operation auf sich selbst abgebildet wird.
Auch die Gruppe $Gl(2,\mathbb{R})$ operiert durch dieselbe Formel auf $\mathbb{C} - \mathbb{R} = H \cup H^-$, wobei H^- die untere Halbebene bezeichnet.
Es werden H bzw. H^- jeweils auf sich selbst abgebildet, falls die Determinante der Matrix $g \in Gl(2,\mathbb{R})$ positiv ist. Im Falle einer negativen Determinante hingegen werden H und H^- vertauscht.

Wir erinnern uns daran, daß die projektive Gerade $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ durch die Operation der Gruppe $\Gamma = Gl(2,\mathbb{F}_q)$ in disjunkte Bahnen zerlegt wird. In dem Fall der Gruppenoperation von $Sl(2,\mathbb{Z})$ auf der komplexen oberen Halbebene H

wird diese ebenfalls in disjunkte Bahnen zerlegt. Hier gibt es drei verschiedene Typen von Bahnen, die in der folgenden Tabelle zusammengestellt sind. Dabei bezeichnet $\rho \in H$ die dritte und $i \in H$ die vierte primitive Einheitswurzel.

Elemente der Bahn	Mächtigkeit der Fixgruppe	Anzahl der Bahnen
$z \in Sl(2,\mathbb{Z}) \cdot i$	4	1
$z \in Sl(2,\mathbb{Z}) \cdot \rho$	6	1
sonst	2	∞

Betrachten wir als nächstes den Begriff des Fundamentalbereichs.

Definition 2.1. *Die Menge $R \subset H$ ist definiert als*

$$\begin{aligned} R \;&:=\; \left\{ z \in H \mid 0 \leq Re(z) < \frac{1}{2},\ |z| > 1 \right\} \\ &\cup \left\{ z \in H \mid -\frac{1}{2} \leq Re(z) \leq 0,\ |z| \geq 1 \right\}. \end{aligned}$$

Satz 2.2. *R ist ein Fundamentalbereich von H unter der Operation von $Sl(2,\mathbb{Z})$, d.h. R enthält aus jeder Bahn $Sl(2,\mathbb{Z}) \cdot z$ genau ein Element.*

Bevor wir zu der Definition einer Modulform kommen, ist es sinnvoll, schwache Modulformen kennenzulernen.

Definition 2.3. *Es sei $k \in \mathbb{N}_0$ eine natürliche Zahl. Die Funktion $f(z)$ heißt schwache Modulform vom Gewicht $2k$, wenn $f(z)$ eine auf H holomorphe Funktion ist und die Gleichung*

$$f(gz) = (cz+d)^{2k} f(z)$$

für alle $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2,\mathbb{Z})$ gilt.

Bei diesen schwachen Modulformen handelt es sich um unter der Gruppe $Sl(2,\mathbb{Z})$ nahezu invariante Funktionen. Diese sind sogar periodisch, denn es gilt

$$f(z+1) = f(z)$$

für alle $z \in H$.

Satz 2.4. *Jede schwache Modulform $f(z)$ vom Gewicht $2k$ kann als eine konvergente Fourier-Reihe in $q(z) = e^{2\pi i z}$ ausgedrückt werden:*

$$f(z) = \tilde{f}(q(z)) = \sum_{n \in \mathbb{Z}} a_n q(z)^n.$$

Mit Hilfe dieser Erkenntnisse kann nun eine Modulform definiert werden.

Definition 2.5. *Eine schwache Modulform $f(z)$ vom Gewicht $2k \in \mathbb{N}_0$ heißt Modulform, wenn für die Fourierentwicklung mit $q(z) = e^{2\pi i z}$*

$$f(z) = \tilde{f}(q(z)) = \sum_{n=0}^{\infty} a_n q(z)^n$$

gilt.

Die Modulformen, die an der Stelle ∞ verschwinden, heißen Spitzenformen oder im Englischen cusp forms. Mit anderen Worten: eine Modulform $f(z) = \tilde{f}(q(z)) = \sum_{n=0}^{\infty} a_n q(z)^n$ vom Gewicht $2k$ ist genau dann eine Spitzenform, wenn $a_0 = 0$ gilt.
Als nächstes behandeln wir ein Beispiel einer Modulform.

Beispiel 2.6. Die Eisenstein-Reihen

$$G_k(z) = \sum_{m,n \in \mathbb{Z}}{}' \frac{1}{(mz+n)^{2k}}$$

sind für $k \geq 2$ ein typisches Beispiel für eine Modulform. Mit $\sum'_{m,n\in\mathbb{Z}}$ ist die Summe über alle Tupel $(m,n) \in \mathbb{Z} \times \mathbb{Z}$ mit $(m,n) \neq (0,0)$ gemeint. Die Eisenstein-Reihen sind lokal gleichmäßig und normal konvergent und folglich holomorph.
Es ist noch zu bestimmen, wie sie sich unter der Gruppe $Sl(2,\mathbb{Z})$ verhalten. Dazu wählen wir $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Sl(2,\mathbb{Z})$ und werten die Eisenstein-Reihen an der Stelle gz für $z \in H$ aus:

$$\begin{aligned}
G_k(gz) &= G_k\left(\frac{az+b}{cz+d}\right) \\
&= \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{\left(m \cdot \frac{az+b}{cz+d} + n\right)^{2k}} \\
&= \sum_{m,n\in\mathbb{Z}}{}' \frac{(cz+d)^{2k}}{(amz+bm+cnz+dn)^{2k}} \\
&= (cz+d)^{2k} \sum_{m,n\in\mathbb{Z}}{}' \frac{1}{\left((am+cn)z+bm+dn\right)^{2k}} \\
&= (cz+d)^{2k} \sum_{s,t\in\mathbb{Z}}{}' \frac{1}{(sz+t)^{2k}} \\
&= (cz+d)^{2k}\, G_k(z).
\end{aligned}$$

Die bei der vorletzten Gleichung vorgenommene Umordnung ist wegen der normalen Konvergenz zulässig. Die Eisenstein-Reihen sind also schwache Modulformen vom Gewicht $2k$. Tatsächlich handelt es sich sogar um Modulformen vom Gewicht $2k$, da gezeigt werden kann, daß die Fourierentwicklung die Form $G_k(z) = \sum_{n=0}^{\infty} a_n q(z)^n$ hat.

Alle Modulformen $f(z)$ vom Gewicht $2k$ bilden einen $\mathbb{C}$-Vektorraum, der mit M_k bezeichnet wird. Um die Dimension von M_k bestimmen zu können, wird der Begriff der Ordnung an einer Stelle $w \in H$ einer Modulform $f(z)$ benötigt. Die Ordnung $\nu_w(f) \in \mathbb{Z}$ von f in w ist die Zahl $\nu \in \mathbb{Z}$, für die $f(z)/(z-w)^\nu$ holomorph ist und nicht in $w \in H$ verschwindet. Sofort ist klar, daß $\nu_w(f) = \nu_{g\cdot w}(f)$ gilt. Mit $\nu_\infty(f)$ wird die Ordnung von $\tilde{f}(q(z))$ in $q(z) = 0$ bezeichnet.
Der folgende Satz stellt einen Zusammenhang der Ordnungen einer Modulform $f(z)$ für verschiedene $z \in H$ und dem Gewicht $2k$ her.

Satz 2.7. *Seien $0 \neq f$ eine Modulform vom Gewicht $2k \in \mathbb{N}_0$ und R ein Fundamentalbereich von $Sl(2,\mathbb{Z})/H$. Dann gilt:*

$$\nu_\infty(f) + 2 \cdot \sum_{z\in R} \frac{1}{e_z}\, \nu_z(f) = \frac{k}{6},$$

wobei e_z die Ordnung des Stabilisators in dem Punkt $z \in H$ ist.

Da in dem Fall $z = i$ die Ordnung des Stabilisators 4, in dem Fall $z = \rho$ die Ordnung des Stabilisators 6 und ansonsten die Ordnung des Stabilisators 2 ist, kann die Gleichung auch folgendermaßen geschrieben werden:

$$\nu_\infty(f) + \frac{1}{2} \cdot \nu_i(f) + \frac{1}{3} \cdot \nu_\rho(f) + \sum_{z\in R}{}^{*}\, \nu_z(f) = \frac{k}{6}.$$

Die Summe $\sum^*_{z\in R}$ bedeutet, daß über alle $z \in R$ mit $z \notin Sl(2,\mathbb{Z}) \cdot i$ und $z \notin Sl(2,\mathbb{Z}) \cdot \rho$ summiert wird.
Als Folgerung aus diesem Satz erhalten wir ein Korollar, das Auskunft über die Dimension des $\mathbb{C}$-Vektorraums M_k gibt.

Korollar 2.8. *Für die Dimension des $\mathbb{C}$-Vektorraum M_k gilt:*

$$\dim_{\mathbb{C}} M_k = \begin{cases} [k/6]\,, & k \equiv 1 \bmod 6,\ k \geq 0 \\ [k/6]+1\,, & k \not\equiv 1 \bmod 6,\ k \geq 0 \end{cases}.$$

Dabei bezeichnet $[a]$ die größte ganze Zahl kleiner oder gleich $a \in \mathbb{R}$.

Als letztes liefert uns ein weiteres Korollar eine Basis dieses $\mathbb{C}-$Vektorraums.

Korollar 2.9. *Der $\mathbb{C}$-Vektorraums M_k besitzt als Basis die Familie der Monome $G_2^\alpha G_3^\beta$ mit $\alpha, \beta \in \mathbb{N}_0$ und $2\alpha + 3\beta = k$.*

Die Theorie der Modulformen über der komplexen obere Halbebene H motiviert im wesentlichen die vorliegende Arbeit. Wir werden in den nächsten Kapiteln die Theorie der Modulformen über endlichen Körpern kennenlernen und dabei feststellen, daß nahezu sämtliche Ergebnisse jener Theorie Analoga der soeben erörterten klassischen Theorie der Modulformen darstellen.

Kapitel 3

Der Vektorraum der Modulformen über endlichen Körpern

Nachdem wir uns im letzten Kapitel Modulformen über der komplexen oberen Halbebene angesehen haben, werden wir in diesem Kapitel Modulformen über endlichen Körpern kennenlernen.

3.1 Grundlegende Eigenschaften von Modulformen

Zuerst werden Modulformen über endlichen Körpern definiert. Wir werden sehen, daß diese einen Vektorraum über $\overline{\mathbb{F}}_q$ bilden und es wird die Frage nach der Dimension dieses Vektorraumes aufgeworfen. Um mit den Modulformen ein wenig vertrauter zu werden, werden wir uns mit den Eisenstein-Reihen, einem der wichtigsten Beispiele für Modulformen, ausführlich beschäftigen. Daneben behandeln wir noch weitere Beispiele für Modulformen. Im Verlauf dieses Kapitels wird auf einige Eigenschaften der Gruppe $\Gamma = Gl(2, \mathbb{F}_q)$, welche im ersten Kapitel zusammengestellt sind, zurückgegriffen.
Wenden wir uns der Definition einer Modulform zu.

Definition 3.1. *Eine Funktion $f : \Omega \longrightarrow \overline{\mathbb{F}}_q$ heißt eine Modulform vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ unter der Gruppe Γ, wenn gilt:*

(i) f ist eine rationale Funktion, d.h. $f(z) = \frac{g(z)}{h(z)}$, wobei $g(z)$ und $h(z)$ Polynome über $\overline{\mathbb{F}}_q$ sind,

(ii) $f(\gamma z) = \frac{(cz+d)^k}{(\det \gamma)^m} f(z)$ für alle $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ und

(iii) $f(\infty) \neq \infty$.

Die Modulformen $f(z)$ vom Gewicht k und vom Typ m sind Funktionen, die unter der Gruppe Γ nahezu, d.h. bis auf den Automorphiefaktor $\alpha(\gamma, z) := \frac{(cz+d)^k}{(\det\gamma)^m}$, invariant sind. Es handelt sich um eine zu dem Fall der Modulformen über der komplexen oberen Halbebene H analoge Definition, wobei die Eigenschaften (i) und (iii) der Definition der Holomorphieeigenschaft entsprechen.
Aufgrund des Definitionsbereiches Ω ist klar, daß Modulformen Pole nur auf $\mathbb{F}_q$ besitzen. Offensichtlich bilden die Modulformen für festes k und m einen $\overline{\mathbb{F}}_q$-Vektorraum, der mit $M_{k,m}(\Gamma)$ bezeichnet wird. Es drängt sich nun die Frage nach der Dimension dieses $\overline{\mathbb{F}}_q$-Vektorraums auf. An dieser Stelle ist es nicht möglich, diese vollständig zu beantworten, da uns noch zu wenig über Modulformen und den $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,m}(\Gamma)$ bekannt ist. Trotzdem können wir schon eine einfache, sehr nützliche Aussage über die Dimension des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$ für einige bestimmte Gewichte $k \in \mathbb{N}_0$ und einige bestimmte Typen $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ treffen.

Proposition 3.2. *Sei $M_{k,m}(\Gamma)$ der $\overline{\mathbb{F}}_q$-Vektorraum der Modulformen vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Für alle k und m mit $k \not\equiv 2m \mod (q-1)$ gilt dann*

$$M_{k,m}(\Gamma) = 0.$$

Beweis. Es sei $f \in M_{k,m}(\Gamma)$ eine beliebige Modulform vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ mit $k \not\equiv 2m \mod (q-1)$ und es gelte

$$f(\gamma z) = \frac{(cz+d)^k}{(\det\gamma)^m} f(z)$$

für $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Für das Element $\gamma = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \in \Gamma$ mit $< a >= \mathbb{F}_q^*$ ergibt sich einerseits durch Verwenden des Automorphiefaktors

$$f(\gamma z) = a^{k-2m} f(z) \tag{3.1}$$

und andererseits durch Auswerten der Modulform an der Stelle γz

$$f(\gamma z) = f\left(\frac{az}{a}\right) = f(z). \tag{3.2}$$

Die Gleichungen (3.1) und (3.2) implizieren

$$\begin{aligned} f(z) &= a^{k-2m} f(z), \quad \text{d.h.} \\ 0 &= (a^{k-2m} - 1)\, f(z). \end{aligned}$$

Da nach Voraussetzung $k \not\equiv 2m \mod (q-1)$ gilt und das Element $a \in \mathbb{F}_q^*$ die multiplikative Gruppe $\mathbb{F}_q^*$ erzeugt, folgt $a^{k-2m} - 1 \neq 0$ und somit $f(z) \equiv 0$. Daher ist $M_{k,m}(\Gamma) = 0$, falls $k \not\equiv 2m \mod (q-1)$. $\square$

Die Frage der Dimension des $\overline{\mathbb{F}}_q$-Vektorraums für allgemeine Gewichte $k \in \mathbb{N}_0$ und Typen $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ wird zu einem späteren Zeitpunkt der Arbeit nach einer eingehenden Beschäftigung mit den Modulformen erörtert. Jetzt befassen wir uns mit einem konkreten Beispiel für Modulformen.

Beispiel 3.3. Die Eisenstein-Reihen

$$E_k(z) = {\sum_{a,b\in\mathbb{F}_q}}' \frac{1}{(az+b)^k}$$

sind wie auch schon in dem Fall der Modulformen über der komplexen oberen Halbebene H typische Beispiele für Modulformen. Die Summe ${\sum}'_{a,b\in\mathbb{F}_q}$ bedeutet, daß über die Indexmenge $\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \mid (a,b) \neq (0,0)\}$ summiert wird. Wir behandeln nur den Fall $k \equiv 0 \mod (q-1)$, werden aber später feststellen, daß wir dies tun dürfen.
Betrachten wir die einzelnen Bedingungen einer Modulform nach Definition 3.1. Da es sich bei den Eisenstein-Reihen um endliche Summen handelt, sind diese rationale Funktionen (vgl. Definition 3.1(i)).
Als nächstes prüfen wir die Bedingung (iii) der Definition, d.h. wir werten die Eisenstein-Reihen an der Stelle ∞ aus. Dazu formen wir die Eisenstein-Reihen wie folgt um:

$$\begin{aligned} E_k(z) &= {\sum_{a,b\in\mathbb{F}_q}}' \frac{1}{(az+b)^k} \\ &= \sum_{a=0,\, b\in\mathbb{F}_q^*} \frac{1}{(az+b)^k} + \sum_{a\in\mathbb{F}_q^*,\, b\in\mathbb{F}_q} \frac{1}{(az+b)^k} \\ &= \sum_{b\in\mathbb{F}_q^*} \frac{1}{b^k} + \sum_{a\in\mathbb{F}_q^*,\, b\in\mathbb{F}_q} \frac{1}{(az+b)^k} \\ &= -1 + \sum_{a\in\mathbb{F}_q^*,\, b\in\mathbb{F}_q} \frac{1}{(az+b)^k}. \end{aligned}$$

Für die letzte Umformung verwenden wir, daß $k \equiv 0 \mod (q-1)$ direkt $b^k = 1$ impliziert und somit $\sum_{b\in\mathbb{F}_q^*} \frac{1}{b^k} = -1$ folgt. Für $z := \frac{1}{w}$ mit $w \in \Omega$, eingesetzt in die Eisenstein-Reihen, ergibt sich

$$\begin{aligned} E_k\left(\frac{1}{w}\right) &= -1 + \sum_{a\in\mathbb{F}_q^*, b\in\mathbb{F}_q} \frac{1}{(\frac{a}{w}+b)^k} \\ &= -1 + \sum_{a\in\mathbb{F}_q^*, b\in\mathbb{F}_q} \frac{w^k}{(a+bw)^k}. \end{aligned}$$

Mit $w = 0$ erhalten wir

$$E_k\left(\frac{1}{w}\right) = -1 + \sum_{a\in\mathbb{F}_q^*, b\in\mathbb{F}_q} \frac{0}{(a+0)^k} = -1,$$

d.h. es gilt $E_k(\infty) = -1$.

Zum Schluß schauen wir uns noch an, wie sich die Eisenstein-Reihen unter der Gruppe Γ verhalten (vgl. Bedingung (i)). Dazu wählen wir $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$ und werten die Eisenstein-Reihen an der Stelle γz für $z \in \Omega$ aus. Mit den Umformungen

$$\begin{aligned}
E_k(\gamma z) &= E_k\left(\frac{az+b}{cz+d}\right) \\
&= \sum_{s,t\in\mathbb{F}_q}{}' \frac{1}{\left(s\frac{az+b}{cz+d}+t\right)^k} \\
&= \sum_{s,t\in\mathbb{F}_q}{}' \frac{(cz+d)^k}{(asz+bs+ctz+dt)^k} \\
&= (cz+d)^k \sum_{s,t\in\mathbb{F}_q}{}' \frac{1}{\left((as+ct)z+bs+dt\right)^k} \\
&\overset{\gamma\in\Gamma}{=} (cz+d)^k \sum_{u,v\in\mathbb{F}_q}{}' \frac{1}{(uz+v)^k} \\
&= (cz+d)^k\, E_k(z)
\end{aligned}$$

zeigt sich, daß die Eisenstein-Reihen Modulformen vom Gewicht k und vom Typ 0 sind, d.h. es gilt $E_k(z) \in M_{k,0}(\Gamma)$.

Bemerkung 3.4. *Die Eisenstein-Reihen E_k sind für jedes $k \geq 0$ eine Modulform in $M_{k,0}(\Gamma)$, verschwinden aber nach Proposition 3.2 identisch für $k \not\equiv 0 \mod (q-1)$. Deshalb war unsere Annahme $k \equiv 0 \mod (q-1)$ keine Einschränkung.*

Der $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,0}(\Gamma)$ der Modulformen vom Gewicht k und vom Typ 0 wird oft der Einfachheit halber mit $M_k(\Gamma)$ bezeichnet.

Um das Verhalten von Modulformen unter der Gruppe Γ in Zukunft möglichst einfach und schnell bestimmen zu können, schauen wir uns jetzt zwei Sätze an, die uns die notwendigen Hilfsmittel zur Verfügung stellen werden. An dieser Stelle sei an die Bruhat-Zerlegung (Satz 1.3) der Gruppe $Gl(2,K)$ erinnert. Im folgenden verwenden wir diese für den Spezialfall der Gruppe $\Gamma = Gl(2,\mathbb{F}_q)$. Mit den folgenden Definitionen

$$\begin{aligned}
B &:= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \;\middle|\; a,d \in \mathbb{F}_q^*,\, b \in \mathbb{F}_q \right\}, \\
U &:= \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \;\middle|\; u \in \mathbb{F}_q \right\} \quad \text{und} \\
\omega &:= \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}
\end{aligned}$$

läßt sich $\Gamma = Gl(2, \mathbb{F}_q)$ als disjunkte Vereinigung

$$\Gamma = B \,\dot{\cup}\, U \,\omega\, B = B \,\dot{\cup}\, B \,\omega\, U$$

darstellen. Es genügt, um das Verhalten einer Modulform unter der Gruppe Γ anzugeben, das Verhalten unter den beiden Matrizen

$$\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B \quad \text{und} \quad \omega = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \Gamma$$

zu untersuchen. Um zu gewährleisten, daß wir dies wirklich tun dürfen, muß die Verträglichkeit der Operation der Gruppe Γ auf der oberen Halbebene Ω mit der Automorphiebedingung Definition 3.1(ii) garantiert sein. Der folgende Satz leistet dieses.

Satz 3.5. *Es sei f eine Funktion auf Ω und $\alpha(\gamma, z) = \frac{(cz+d)^k}{(\det\gamma)^m}$ der Automorphiefaktor für eine Matrix $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma$. Gilt für alle $z \in \Omega$*

$$\begin{aligned} f(\gamma z) &= \alpha(\gamma, z)\, f(z) \quad \textit{und} \\ f(\gamma' z) &= \alpha(\gamma', z)\, f(z), \end{aligned}$$

so folgt

$$f(\gamma\gamma' z) = \alpha(\gamma\gamma', z)\, f(z) \tag{3.3}$$

für alle $z \in \Omega$.

Beweis. Es seien $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und $\gamma' = \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} \in \Gamma$ und weiter $\alpha(\gamma, z) = \frac{(cz+d)^k}{(\det\gamma)^m}$ und $\alpha(\gamma', z) = \frac{(c'z+d')^k}{(\det\gamma')^m}$ die entsprechenden Automorphiefaktoren.
Ist $f(z) = 0$, so ist nichts zu zeigen. Für $f(z) \neq 0$ ist (3.3) äquivalent zur Gültigkeit von

$$\alpha(\gamma\gamma', z) = \alpha(\gamma, \gamma' z) \cdot \alpha(\gamma', z)$$

für alle $z \in \Omega$. Diese Gleichung erhalten wir mit den Umformungen

$$\begin{aligned} \alpha(\gamma\gamma', z) &= \frac{((ca' + dc')z + cb' + dd')^k}{(\det\gamma\gamma')^m} \\ &= \frac{(c\,(a'z + b') + d\,(c'z + d'))^k}{(\det\gamma\, \det\gamma')^m} \\ &= \frac{(c'z + d')^k \cdot (c\,\frac{a'z+b'}{c'z+d'} + d)^k}{(\det\gamma)^m \cdot (\det\gamma')^m} \\ &= \frac{(c'z + d')^k}{(\det\gamma')^m} \cdot \frac{(c\gamma' z + d)^k}{(\det\gamma)^m} \\ &= \alpha(\gamma', z) \cdot \alpha(\gamma, \gamma' z). \end{aligned}$$

□

Für eine weitere Vereinfachung bei der Berechnung des Gewichts $k \in \mathbb{N}_0$ und des Typs $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ einer Modulform $f(z)$ sorgen die beiden in dem folgenden Satz zusammengefaßten Rechenregeln.

Satz 3.6. *(i) Es sei $f(z) \in M_{k,m}(\Gamma)$ eine beliebige Modulform vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Die Funktion $f(z)^i$ mit $i \in \mathbb{N}$ ist dann eine Modulform vom Gewicht $i \cdot k \in \mathbb{N}_0$ und vom Typ $i \cdot m \in \mathbb{Z}/(q-1)\mathbb{Z}$, d.h. $f(z)^i \in M_{i\cdot k, i\cdot m}(\Gamma)$.*

(ii) Es seien $f_1(z) \in M_{k_1,m_1}(\Gamma)$ und $f_2(z) \in M_{k_2,m_2}(\Gamma)$ zwei beliebige Modulformen vom Gewicht $k_1 \in \mathbb{N}_0$ bzw. $k_2 \in \mathbb{N}_0$ und vom Typ $m_1 \in \mathbb{Z}/(q-1)\mathbb{Z}$ bzw. $m_2 \in \mathbb{Z}/(q-1)\mathbb{Z}$. Das Produkt $(f_1f_2)(z)$ besitzt dann das Gewicht $k_1+k_2 \in \mathbb{N}_0$ und den Typ $m_1+m_2 \in \mathbb{Z}/(q-1)\mathbb{Z}$, d.h. $(f_1f_2)(z) \in M_{k_1+k_2,m_1+m_2}(\Gamma)$.

Beweis. (i) Für eine Modulform $f(z) \in M_{k,m}(\Gamma)$ vom Gewicht k und vom Typ m gilt

$$f(\gamma z) = \frac{(cz+d)^k}{(\det\gamma)^m}\, f(z) \quad \text{für alle } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma.$$

Dann ist für $f(z)^i$ mit $i \in \mathbb{N}$ für alle $\gamma \in \Gamma$

$$f(\gamma z)^i = \left(\frac{(cz+d)^k}{(\det\gamma)^m}\, f(z)\right)^i = \frac{(cz+d)^{i\cdot k}}{(\det\gamma)^{i\cdot m}}\, f(z)^i,$$

so daß die Behauptung $f(z)^i \in M_{i\cdot k,i\cdot m}(\Gamma)$ folgt.

(ii) Für die Modulformen $f_1(z) \in M_{k_1,m_1}(\Gamma)$ und $f_2(z) \in M_{k_2,m_2}(\Gamma)$ vom Gewicht k_1 bzw. k_2 und vom Typ m_1 bzw. m_2 gelten

$$\begin{aligned} f_1(\gamma z) &= \frac{(cz+d)^{k_1}}{(\det\gamma)^{m_1}} f_1(z) \quad \text{und} \\ f_2(\gamma z) &= \frac{(cz+d)^{k_2}}{(\det\gamma)^{m_2}} f_2(z) \quad \text{für alle } \gamma \in \Gamma. \end{aligned}$$

Analog zu dem Beweis von Aussage (i) folgt für das Produkt dieser beiden Modulformen

$$f_1(\gamma z)f_2(\gamma z) = \frac{(cz+d)^{k_1+k_2}}{(\det\gamma)^{m_1+m_2}} f_1(z)f_2(z) \quad \text{für alle } \gamma \in \Gamma$$

und somit die Behauptung $(f_1f_2)(z) \in M_{k_1+k_2,m_1+m_2}(\Gamma)$.

□

Bemerkung 3.7. *Trivialerweise gilt eine zu Satz 3.6(ii) analoge Aussage für das Produkt von mehr als zwei Modulformen. Die Aussage (i) ist also ein Spezialfall von (ii).*

Diese beiden Sätze versetzen uns in die angenehme Lage, ohne großen Aufwand das Gewicht $k \in \mathbb{N}_0$ und den Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ einer Modulform $f(z)$ zu bestimmen. Schauen wir uns dazu zwei Beispiele an.

Beispiel 3.8. (i) Es ist

$$t(z) := \frac{1}{z - z^q} \in \mathbb{F}_q(z)$$

eine rationale Funktion.
Der Funktionswert von $t(z)$ an der Stelle ∞ wird bestimmt, indem $t(z)$ in $\frac{1}{w}$ für $w = 0$ ausgewertet wird. Mit

$$t\left(\frac{1}{w}\right) = \frac{1}{\frac{1}{w} - \left(\frac{1}{w}\right)^q} = \frac{w^q}{w^{q-1} - 1}$$

und $w = 0$ folgt $t\left(\frac{1}{w}\right) = 0$ und somit $t(\infty) \neq \infty$. Um zu berechnen, wie sich $t(z)$ unter der Gruppe $\Gamma = Gl(2, \mathbb{F}_q)$ verhält, genügt es nach Satz 3.5, das Verhalten unter den Matrizen $\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B$ und $\omega = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \Gamma$ zu untersuchen. Aus

$$\begin{aligned} t(\beta z) &= t\left(\frac{az+b}{d}\right) = \frac{1}{\frac{az+b}{d} - \left(\frac{az+b}{d}\right)^q} = \frac{d}{a} \cdot t(z) = \frac{d^{q+1}}{\det \beta} \cdot t(z) \quad \text{und} \\ t(\omega z) &= t\left(\frac{1}{z}\right) = \frac{1}{\frac{1}{z} - \left(\frac{1}{z}\right)^q} = -z^{q+1} \cdot t(z) = \frac{z^{q+1}}{\det \omega} \cdot t(z) \end{aligned}$$

folgt $t(z) \in M_{q+1,1}(\Gamma)$.

(ii) Es ist $\Delta(z) := (z - z^q)^{1-q} = (t(z))^{q-1} \in \mathbb{F}_q(z)$.
Mit Aussage (i) dieses Beispiels gilt nach Satz 3.6 $\Delta(z) \in M_{q^2-1,0}(\Gamma)$.

3.2 Die t-Entwicklung einer Modulform

Die Modulform $t(z) = \frac{1}{z-z^q} \in M_{q+1,1}(\Gamma)$ ist eine ausgezeichnete Modulform, die im folgenden eine sehr wichtige Rolle spielt.
Alle Modulformen sind periodisch, denn mit $\alpha = \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \in \Gamma$ gilt

$$f(\alpha z) = f(z + b) = f(z)$$

für alle $b \in \mathbb{F}_q$. Insbesondere ist auch die Modulform $t(z) \in M_{q+1,1}(\Gamma)$ periodisch. Im klassischen Fall der Modulformen können diese aufgrund ihrer Periodizität in Fourierreihen entwickelt werden. In dem hier betrachteten Fall der Modulformen über endlichen Körpern gilt der folgende analoge Satz.

Satz 3.9. *Jede Modulform $f \in M_{k,m}(\Gamma)$ besitzt eine Darstellung*

$$f(z) = \tilde{f}(t(z)) = \sum_{n=i}^{d} a_n t(z)^n$$

mit $i, d \in \mathbb{N}_0$ $(i \leq d)$ und den Koeffizienten $a_n \in \overline{\mathbb{F}}_q$ für alle $i \leq n \leq d$.

Beweis. Mit der Definition

$$K := \overline{\mathbb{F}}_q(z),$$

wobei z die Unbestimmte ist, gilt $f(z) = \frac{g(z)}{h(z)} \in K = \overline{\mathbb{F}}_q(z)$.
Zunächst wird gezeigt, daß die Gruppe Γ als Automorphismen auf dem Körper K operieren. Anschließend wird der Körper der unter

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \mid u \in \mathbb{F}_q \right\}$$

invarianten Elemente K^U bestimmt und es wird bewiesen, daß $K^U = \overline{\mathbb{F}}_q(t)$ ist. Nach diesen Überlegungen ist klar, daß $f(z) = \tilde{f}(t) \in \overline{\mathbb{F}}_q(t)$ eine rationale Funktion in t ist. Als letztes muß noch gezeigt werden, daß es sich bei $\tilde{f}(t)$ wirklich um ein Polynom handelt.

Betrachten wir zunächst die Operation der Gruppe Γ auf dem Körper K. Wir wissen bereits, daß die Gruppe Γ von links auf $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ operiert. Auf $K = \overline{\mathbb{F}}_q(z)$ hingegen operiert sie von rechts vermöge

$$f_\gamma(z) := f(\gamma z)$$

für $\gamma \in \Gamma$ und $f \in K$. An dieser Stelle soll kein detaillierter Beweis der Operation gegeben werden, sondern nur kurz auf die Assoziativität eingegangen werden. Mit γ, $\gamma' \in \Gamma$ gilt

$$f_{\gamma\gamma'} = f_{\gamma\gamma'}(z) = f(\gamma\gamma' z) = f(\gamma(\gamma' z)) = f_\gamma(\gamma' z) = (f_\gamma)_{\gamma'}.$$

Als nächstes bestimmen wir den Körper K^U der unter

$$U = \left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in \mathbb{F}_q^{2\times 2} \ \mid \ u \in \mathbb{F}_q \right\}$$

invarianten Elemente. Nach der Definition

$$K^U = \overline{\mathbb{F}}_q(z)^U = \{f(z) \in \overline{\mathbb{F}}_q(z) \mid f_\alpha = f \ \ \forall\, \alpha \in U\}$$

ergibt sich für diesen

$$K^U = \{f(z) \in \overline{\mathbb{F}}_q(z) \mid f(z+b) = f(z) \ \forall\, b \in \mathbb{F}_q\}.$$

Aufgrund der Periodizität von $t(z)$ gilt $t(z) \in K^U = \overline{\mathbb{F}}_q(z)^U$ und somit $\overline{\mathbb{F}}_q(t) \subseteq K^U$.

Mit Hilfe des Hauptsatzes der Galoistheorie läßt sich sogar die Gleichheit dieser beiden Körper zeigen.
Es ist $\overline{\mathbb{F}}_q(t) \subseteq K^U \subseteq K$. Da die Mächtigkeit der Gruppe U gerade q beträgt, erhalten wir für den Grad der Körpererweiterung

$$[K : K^U] = \#U = q. \tag{3.4}$$

Betrachten wir jetzt den Grad der Körpererweiterung $[K : \overline{\mathbb{F}}_q(t)]$. Das Minimalpolynom $f(X) = X^q - X + \frac{1}{t}$ von z über $\overline{\mathbb{F}}_q(t)$ ist vom Grad q, so daß sich

$$[K : \overline{\mathbb{F}}_q(t)] \leq q \tag{3.5}$$

ergibt. Die Gleichungen (3.4) und (3.5) implizieren $[K^U : \overline{\mathbb{F}}_q(t)] = 1$, was gleichbedeutend mit $K^U = \overline{\mathbb{F}}_q(t)$ ist.
Mit diesem ersten Teil des Beweises wurde gezeigt, daß alle Modulformen $f(z) \in M_{k,m}(\Gamma)$ aufgrund ihrer Periodizität in dem Körper $\overline{\mathbb{F}}_q(t)$ liegen und deshalb $f(z) = \tilde{f}(t)$ gilt, wobei $\tilde{f}(t)$ eine rationale Funktion in t ist.

Es bleibt zu zeigen, daß $\tilde{f}(t) \in \overline{\mathbb{F}}_q(t)$ sogar ein Polynom ist.
Dazu nehmen wir an, die Modulform $f(z) = \tilde{f}(t) = \frac{\tilde{g}(t)}{\tilde{h}(t)} \in \overline{\mathbb{F}}_q(t)$ sei kein Polynom, sondern eine rationale Funktion mit dem nichtkonstanten Nenner $\tilde{h}(t)$.
Wir betrachten zunächst die Modulform $t(z) = \frac{1}{z-z^q}$ etwas genauer. Zum einen besitzt $t(z)$ laut der Definition für Modulformen Pole nur auf $\mathbb{F}_q$, zum anderen gilt nach Beispiel 3.8(i) gerade $t(\infty) = 0$. Weiter handelt es sich bei der Modulform $t(z)$ um eine surjektive Abbildung von $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ nach $\mathbb{P}^1(\overline{\mathbb{F}}_q)$.
Es ist zu zeigen, daß $\tilde{f}$ als rationale Funktion in t Pole höchstens in $t = \infty$ besitzt. Da $f(z) = \tilde{f}(t)$, $t(z) = \infty$ äquivalent zu $z \in \mathbb{F}_q$ und $f(z) \neq \infty$ für $z \notin \mathbb{F}_q$ ist, gilt tatsächlich, daß $\tilde{f}(t)$ keine endlichen Pole besitzt. Somit ist $\tilde{f}(t) \in \overline{\mathbb{F}}_q[t]$ ein Polynom. □

In der folgenden Definition erhält das Polynom $\tilde{f}(t) \in \overline{\mathbb{F}}_q[t]$ einen Namen.

Definition 3.10. *Sei $f(z) \in M_{k,m}(\Gamma)$ eine Modulform. Mit $t(z) = \frac{1}{z-z^q} \in M_{q+1,1}(\Gamma)$ heißt die Darstellung*

$$f(z) = \tilde{f}(t(z)) = \sum_{n=i}^{d} a_n t(z)^n \in \overline{\mathbb{F}}_q[t]$$

mit $i, d \in \mathbb{N}_0$ und $i \leq d$ die t-Entwicklung vom Grad d der Modulform $f(z)$.

Bemerkung 3.11. *Analog zum klassischen Fall der Modulformen unterscheiden wir auch in dem Fall der Modulformen über endlichen Körpern Spitzenformen (oder im Englischen cusp forms), d.h. Modulformen, die an der Stelle ∞ verschwinden, von den übrigen Modulformen.*

Schauen wir uns dazu zwei Beispiele an:

Beispiel 3.12. (i) Wir erinnern uns an die Eisenstein-Reihen

$$E_k(z) = \sum_{a,b \in \mathbb{F}_q}{}' \frac{1}{(az+b)^k} \in M_k(\Gamma).$$

Für $k \equiv 0 \mod (q-1)$ gilt nach Beispiel 3.3 $E_k(\infty) = -1$, was bedeutet, daß die Eisenstein-Reihen keine Spitzenformen sind.

(ii) Die Modulform $t(z) = \frac{1}{z-z^q} \in M_{q+1,1}(\Gamma)$ verschwindet nach Beispiel 3.8(i) an der Stelle ∞ und ist folglich eine Spitzenform.

In diesem Kapitel haben wir uns mit den Grundlagen der Theorie der Modulformen über endlichen Körpern vertraut gemacht. Wir verfügen jetzt über das nötige Wissen, um tiefergehende Fragen beantworten zu können. Mit Hilfe der t-Entwicklung einer Modulform $f(z) \in M_{k,m}(\Gamma)$ und den Eisenstein-Reihen $E_k(z) \in M_k(\Gamma)$ werden wir als nächstes die Dimension von $M_{k,m}(\Gamma)$, dem $\overline{\mathbb{F}}_q$-Vektorraum, bestimmen. Ferner benötigen wir die t-Entwicklung der Eisenstein-Reihen bei der Berechnung ihrer Nullstellen in Kapitel 5.

Kapitel 4

Die Dimension des Vektorraumes $M_{k,m}(\Gamma)$

Nachdem in Kapitel 3 einige grundlegende Eigenschaften einer Modulform $f(z) \in M_{k,m}(\Gamma)$ vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ über einem endlichen Körper $\mathbb{F}_q$ erörtert wurden, beschäftigt sich dieses Kapitel mit dem $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,m}(\Gamma)$ selbst.
Die Frage nach der Dimension dieses Vektorraumes wurde bereits aufgeworfen und wird im Verlauf dieses Kapitels beantwortet werden. Ein wichtiges Werkzeug dazu sind Divisoren, die im nächsten Abschnitt für den Fall des rationalen Funktionenkörpers $K(X)$ diskutiert werden. In dem darauf folgenden Abschnitt wird ein sehr zentraler Satz bewiesen, der einen Zusammenhang der Nullstellenordnungen einer Modulform $f(z) \in M_{k,m}(\Gamma)$ für verschiedene $z \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ herstellt. Mit Hilfe dieser Ergebnisse kann am Ende dieses Kapitels die Frage nach der Dimension des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$ beantwortet werden.

4.1 Divisoren

Im folgenden ist exkursartig die für diese Arbeit notwendige Theorie über Divisoren zusammengestellt. Dabei beschränken wir uns, wie schon angedeutet, auf den Fall des rationalen Funktionenkörpers $K(X)$. Für eine weitergehende Lektüre sei auf [Sti93] verwiesen.

Es sei $K = \overline{K}$ ein algebraisch abgeschlossener Körper. Weiter sei X transzendent über K und $K(X)$ der rationale Funktionenkörper. Ein Divisor von $K(X)/K$ ist eine formale Linearkombination der Form

$$D := \sum_{x \in \mathbb{P}^1(K)} a_x x,$$

wobei $a_x \in \mathbb{Z}$ für alle $x \in \mathbb{P}^1(K)$ und fast alle $a_x = 0$ sind. Ein Divisor der Form $P = x$ heißt Primdivisor.

Die Divisoren von $K(X)/K$ bilden eine additive Gruppe, die Divisorgruppe $\mathcal{D}_{K(X)}$. Zwei Divisoren $D = \sum_{x\in\mathbb{P}^1(K)} a_x x$ und $D' = \sum_{x\in\mathbb{P}^1(K)} a'_x x \in \mathcal{D}_{K(X)}$ werden koeffizientenweise addiert

$$D + D' = \sum_{x\in\mathbb{P}^1(K)} (a_x + a'_x)x$$

und das neutrale Element der Divisorgruppe ist der Divisor

$$0 := \sum_{x\in\mathbb{P}^1(K)} a_x x$$

mit $a_x = 0$ für alle $x \in \mathbb{P}^1(K)$.
Des weiteren definieren wir für $z \in \mathbb{P}^1(K)$ und $D = \sum_{x\in\mathbb{P}^1(K)} a_x x$

$$\mu_z(D) := a_z.$$

Auf der Divisorgruppe $\mathcal{D}_{K(X)}$ wird für $D, D' \in \mathcal{D}_{K(X)}$ durch

$$D \leq D' \quad :\Leftrightarrow \quad \mu_z(D) \leq \mu_z(D') \quad \text{für alle}\, z \in \mathbb{P}^1(K)$$

eine partielle Ordnung definiert.
Der Grad eines Divisors ist gegeben durch

$$degD := \sum_{x\in\mathbb{P}^1(K)} \mu_x(D).$$

Weiter werden die Begriffe des Nulldivisors, des Poldivisors und des Hauptdivisors benötigt. Dazu betrachten wir zunächst die folgende Definition.

Definition 4.1. *Es sei $0 \neq f(X) \in K(X)$ eine Funktion über dem Körper $K = \overline{K}$, für die*

$$f(X) = X^n \cdot \frac{g(X)}{h(X)}$$

mit $X \not| \, g(X) \cdot h(X)$, $g(X), h(X) \in K[X]$ und $n \in \mathbb{Z}$ gelte. Dann ist

$$\begin{aligned} \mu_0(f) &:= n \\ \mu_a(f) &:= \mu_0(f(X-a)) \quad \textit{für} \quad a \in K = \overline{K} \\ \mu_\infty(f) &:= \mu_0(f(\frac{1}{X})) = deg(Nenner f(X)) - deg(Zähler f(X)), \end{aligned}$$

wobei $\mu_a(f)$ die Bewertung von f in $a \in K$ und $\mu_\infty(f)$ die Bewertung von f in ∞ heißt.
Es sei $b \in \mathbb{P}^1(K)$. Dann ist b ein Nullstelle von $f(X)$, falls $\mu_b(f) > 0$, und ein Pol, falls $\mu_b(f) < 0$.

Trivialerweise gelten für zwei Funktionen $f(X), g(X) \in K(X)$ über einem beliebigen algebraisch abgeschlossenen Körper $K = \overline{K}$ und für $n \in \mathbb{N}$ die folgenden Rechenregeln für die Bewertungen in $z \in \mathbb{P}^1(K)$:

(i) $\mu_z(f \cdot g) = \mu_z(f) + \mu_z(g)$,

(ii) $\mu_z\left(\frac{f}{g}\right) = \mu_z(f) - \mu_z(g)$,

(iii) $\mu_z(f^n) = n \cdot \mu_z(f)$ und

(iv) $\mu_z(f+g) \geq \min\{\mu_z(f),\ \mu_z(g)\}$.

Bemerkung 4.2. *Es ist klar, daß es sich bei μ_z um eine diskrete Bewertung handelt. Im einzelnen soll auf Bewertungen nicht weiter eingegangen werden, sondern es sei auf* [Sti93] *verwiesen. Kurz erwähnt werden soll nur die starke Dreiecksungleichung, da diese an anderer Stelle verwendet wird.*
Für zwei Funktionen $f, g \in K(X)$ mit $\mu_z(f) \neq \mu_z(g)$ gilt

$$\mu_z(f+g) = \min\{\mu_z(f), \mu_z(g)\}. \tag{4.1}$$

Für $0 \neq f \in K(X)$ sei Z die Menge der Nullstellen und N die Menge der Pole in $\mathbb{P}^1(K)$. Dann heißt

$$\begin{aligned} div(f)_0 &:= \sum_{z\in Z} \mu_z(f) \cdot z \quad \text{der Nullstellendivisor,} \\ div(f)_\infty &:= \sum_{z\in N} (-\mu_z(f)) \cdot z \quad \text{der Poldivisor und} \\ div(f) &:= div(f)_0 - div(f)_\infty \quad \text{der Hauptdivisor von } f. \end{aligned}$$

Für eine Teilmenge S von $\mathbb{P}^1(K)$ und einen Divisor D sei

$$D_S = \sum_{z\in S} \mu_z(D) \cdot z$$

die „Projektion" von D auf S. In dem folgenden Lemma wird der Grad eines Hauptdivisors betrachtet.

Lemma 4.3. *Seien $0 \neq f \in K(X)$ eine Funktion über K und $div(f)$ der Hauptdivisor von f. Dann gilt für den Grad des Hauptdivisors*

$$deg\ div(f) = 0.$$

Beweis. Es sei

$$f(X) = \frac{g(X)}{h(X)} = \frac{(X-a_1)^{n_1} \cdot \ldots \cdot (X-a_r)^{n_r}}{(X-b_1)^{m_1} \cdot \ldots \cdot (X-b_s)^{m_s}} \in K(X)$$

wobei $a_1, \ldots, a_r, b_1, \ldots, b_s \in K$ und $n_1, \ldots, n_r, m_1, \ldots, m_s \in \mathbb{N}$. Mit

$$\begin{aligned} deg\ div(f) &= \sum_{z\in K} \mu_z(f) + \mu_\infty(f) \\ &\overset{Def. 4.1}{=} \sum_{j=1}^{r} n_j - \sum_{i=1}^{s} m_i + \mu_\infty(g) - \mu_\infty(h) \\ &= \sum_{j=1}^{r} n_j - \sum_{i=1}^{s} m_i - \sum_{j=1}^{r} n_j + \sum_{i=1}^{s} m_i = 0 \end{aligned}$$

folgt die Behauptung. □

Offensichtlich ist die Gruppe der Hauptdivisoren

$$\mathcal{P}_{K(X)} := \{div(f) \mid 0 \neq f \in K(X)\}$$

eine Untergruppe der Divisorgruppe $\mathcal{D}_{K(X)}$. Durch

$$\mathcal{C}_{K(X)} := \mathcal{D}_{K(X)}/\mathcal{P}_{K(X)}$$

wird die Faktorgruppe, die Divisorklassengruppe, definiert. Das zu dem Divisor $D \in \mathcal{D}_{K(X)}$ korrespondierende Element der Faktorgruppe $\mathcal{C}_{K(X)}$ wird mit $[D]$ bezeichnet. Zwei Divisoren $D, D' \in \mathcal{D}_{K(X)}$ sind äquivalent genau dann, wenn

$$[D] = [D']$$

gilt. Dieses ist gleichbedeutend damit, daß ein $f \in K(X) - \{0\}$ existiert mit $D = D' + div(f)$.
Betrachten wir als nächstes den sogenannten $\mathcal{L}$-Raum.

Definition 4.4. *Mit obigen Definitionen heißt für einen Divisor $D \in \mathcal{D}_{K(X)}$*

$$\mathcal{L}(D) := \{f \in K(X) \mid div\,(f) \geq -D\} \cup \{0\}$$

der $\mathcal{L}$-Raum.

Überlegen wir uns zunächst, was diese Definition des Raums $\mathcal{L}(D)$ genau bedeutet. Sei $D \in \mathcal{D}_{K(X)}$ der folgendermaßen definierte Divisor:

$$D = \sum_{i=1}^{r} n_i x_i - \sum_{j=1}^{s} m_j z_j$$

mit $n_i > 0,\ m_j > 0$. In $\mathcal{L}(D)$ liegen somit alle Funktionen $f \in K(X)$ mit mindestens m_j-fachen Nullstellen an den Stellen z_j für $j = 1, \ldots, s$ und mit Polen höchstens an den Stellen $x_1, \ldots, x_r$, wobei die Ordnung des jeweiligen Pols an der Stelle x_i maximal n_i für $i = 1, \ldots, r$ beträgt.
Es ist offensichtlich, daß es sich bei dem Raum $\mathcal{L}(D)$ um einen K-Vektorraum handelt. Um die Dimension des $\mathcal{L}$-Raums zu bestimmen, betrachten wir nun das folgende Lemma.

Lemma 4.5. *Es seien $D \in \mathcal{D}_{K(X)}$ ein Divisor vom Grad $deg\,D \geq 0$ und $P \in \mathcal{D}_{K(X)}$ ein Primdivisor. Dann ist $\mathcal{L}(D)$ in $\mathcal{L}(D+P)$ enthalten und für die Kodimension gilt*

$$\dim_K \mathcal{L}(D+P)/\mathcal{L}(D) = 1.$$

Beweis. Da $D \leq D + P$ ist, gilt offensichtlich $\mathcal{L}(D) \subseteq \mathcal{L}(D+P)$.
Weiter ist zu zeigen, daß die Kodimension $\dim_K \mathcal{L}(D+P)/\mathcal{L}(D) \leq 1$ ist. Dazu nehmen wir an, es gelte $\dim_K \mathcal{L}(D+P)/\mathcal{L}(D) > 1$. Folglich existieren zwei modulo $\mathcal{L}(D)$ linear unabhängige Funktionen $f, g \in \mathcal{L}(D+P)$. Da jetzt

aber $\mathcal{L}(D+P)/\mathcal{L}(D)$ ein K-Vektorraum ist und $\mu_P(f) = \mu_P(g)$ gilt, gibt es zwei Elemente $m, n \in K$ mit $mf + ng \in \mathcal{L}(D)$. Die beiden Funktionen f und g sind also linear abhängig in $\mathcal{L}(D+P)/\mathcal{L}(D)$, was ein Widerspruch zur Annahme ist. Folglich gilt die Behauptung $\dim_K \mathcal{L}(D+P)/\mathcal{L}(D) \leq 1$.

Um zu zeigen, daß $\dim_K \mathcal{L}(D+P)/\mathcal{L}(D) = 1$ gilt, konstruieren wir eine Funktion, die in $\mathcal{L}(D+P)$, nicht aber in $\mathcal{L}(D)$ liegt. Dazu sei

$$D = \sum_{a \in \mathbb{P}^1(K)} n_a \cdot a \in \mathcal{D}_{K(X)}$$

ein Divisor. Für $P \neq \infty$ läßt sich leicht zeigen, daß die Funktion

$$g(X) = \prod_{a \in K} (X-a)^{-n_a} \cdot (X-P)^{-1} \in K(X)$$

in $\mathcal{L}(D+P)$, nicht aber in $\mathcal{L}(D)$ liegt. Im Fall $P = \infty$ gilt für

$$g(X) = \prod_{a \in K} (X-a)^{-n_a} \cdot X^{deg(D+\infty)} \in K(X)$$

analog $g(X) \in \mathcal{L}(D+P) - \mathcal{L}(D)$. □

Der folgende Satz liefert die Dimension des $\mathcal{L}$-Raumes.

Satz 4.6. *Sei $\mathcal{L}(D) = \{f \in K(X) \mid div(f) \geq -D\} \cup \{0\}$ der $\mathcal{L}$-Raum. Dann gilt für die Dimension*

$$\dim_K \mathcal{L}(D) = \begin{cases} \deg D + 1\,, & \deg D \geq 0 \\ 0\,, & \deg D < 0 \end{cases}.$$

Beweis. Für den Beweis werden die Fälle $\deg D < 0$ und $\deg D \geq 0$ unterschieden.
Um den einfacheren Fall $\deg D < 0$ zu zeigen, nehmen wir an, es gelte $\dim_K \mathcal{L}(D) > 0$. Dies impliziert, daß eine Funktion $0 \neq f \in \mathcal{L}(D)$ mit dem Divisor $div(f) \geq -D$ existiert, so daß für den Grad dieses Divisors $deg(div(f)) \geq deg(-D)$ folgt. Da ein Hauptdivisor den Grad 0 besitzt, ergibt sich $0 \geq deg(-D)$, was gleichbedeutend mit $0 \leq deg(D)$ ist. Somit existiert nur dann eine Funktion $f \in \mathcal{L}(D)$, wenn $deg(D) \geq 0$ gilt und es folgt $dim_K \mathcal{L}(D) = 0$, falls $deg(D) < 0$.

In dem Fall $\deg D \geq 0$ wird der Beweis mit Hilfe von vollständiger Induktion geführt. Für den Induktionsanfang sei $\deg D = 0$. Da eine Funktion $f \in K(X)$ genau dann den Divisor $div f = 0$ besitzt, wenn sie konstant ist, folgt direkt $\dim_K \mathcal{L}(D) = 1$.
Für den Induktionsschritt nehmen wir an, die Aussage sei gezeigt für alle Divisoren D vom Grad $deg(D) \leq d \in \mathbb{N}_0$. Sei der Divisor D' vom Grad $deg(D') = d+1$, dann gilt $D' = D + P$ mit $degD = d$. Da für den Divisor D die Aussage bereits gezeigt ist, folgt mit dem Induktionslemma 4.5 die Aussage für den Divisor D'. □

4.2 Die Nullstellenordnungen einer Modulform

Im folgenden betrachten wir eine Modulform $f(z) \in M_{k,m}(\Gamma)$ vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Nach Satz 3.9 besitzt diese eine t-Entwicklung der Form $f(z) = \tilde{f}(t) = a_i t^i + \ldots + a_d t^d \in \overline{\mathbb{F}}_q[t]$, wobei $d \in \mathbb{N}_0$ der Grad der t-Entwicklung ist. In dem zentralen Satz wird ein Zusammenhang zwischen den Nullstellenordnungen von verschiedenen Punkten $z \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$, dem Gewicht k und dem Grad d der Modulform hergestellt.
Wir erinnern uns daran, daß es auch in dem Fall der Modulformen über der komplexen oberen Halbebene H einen derartigen Zusammenhang gibt (vgl. Satz 2.7).
Wie auch in dem klassischen Fall der Modulformen können mit Hilfe des Satzes zum einen die Nullstellen von Modulformen $f(z) \in M_{k,m}(\Gamma)$ und zum anderen die Dimension des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$ bestimmt werden.

Zunächst wird der grundlegende Begriff der Nullstellenordnung einer Funktion in einem beliebigen Punkt erläutert.

Definition 4.7. *Es sei $f \in M_{k,m}(\Gamma)$ eine beliebige Modulform über dem Körper $\overline{\mathbb{F}}_q$. Dann sei*

$$\begin{aligned} \nu_a(f) &:= \mu_a(f) \quad \text{für alle } a \in \overline{\mathbb{F}}_q \text{ und} \\ \nu_\infty(f) &:= \frac{\mu_\infty(f)}{q}, \end{aligned}$$

wobei $\nu_a(f)$ die Nullstellenordnung der Modulform f in a für alle $a \in \overline{\mathbb{F}}_q$ und $\nu_\infty(f)$ entsprechend die Nullstellenordnung der Modulform f in ∞ heißt.

Bemerkung 4.8. *Entscheidend in obiger Definition ist, daß für die Nullstellenordnung von $t(z) = \frac{1}{z-z^q} \in M_{q+1,1}(\Gamma)$ in ∞ gerade $\nu_\infty(t) = 1$ gilt. Für eine beliebige Modulform $f(z) \in M_{k,m}(\Gamma)$ mit der t-Entwicklung*

$$f(z) = \tilde{f}(t) = a_i t^i + \ldots + a_d t^d \in \overline{\mathbb{F}}_q[t],$$

mit $i, d \in \mathbb{N}_0$, $i \leq d$ und $a_i \neq 0$ gilt dann nach der starken Dreiecksungleichung $\nu_\infty(f) = i$.

Weiter benötigen wir das folgende

Lemma 4.9. *Es sei $f \in M_{k,m}(\Gamma)$ eine Modulform. Die Nullstellenordnungen $\nu_a(f)$ von f in den Punkten $a \in \Omega$ sind unter der Gruppe Γ invariant.*

Beweis. Es sei $f \in M_{k,m}(\Gamma)$ eine Modulform, $a \in \Omega$ und $\gamma \in \Gamma$.

Mit $\gamma^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ und

$$\begin{array}{rcl} \nu_a\left(f(z)\right) & = & \nu_{\gamma a}\left(f(\gamma^{-1}z)\right) \\ & = & \nu_{\gamma a}\left((det\gamma)^{-m}\cdot(cz+d)^k\cdot f(z)\right) \\ & = & \nu_{\gamma a}\left((det\gamma)^{-m}\right)+\nu_{\gamma a}\left((cz+d)^k\right)+\nu_{\gamma a}\left(f(z)\right) \\ & \overset{\gamma a\notin\mathbb{F}_q}{=} & \nu_{\gamma a}\left(f(z)\right) \end{array}$$

folgt die Behauptung. □

Bevor wir uns nun den Zusammenhang von Nullstellenordnungen für verschiedene Punkte $z \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ anschauen, erinnern wir uns daran, daß, wie in Proposition 1.9 und in der Tabelle S. 14 dargestellt, die projektive Gerade $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ durch die Operation der Gruppe Γ in disjunkte Bahnen zerfällt. Es gibt drei verschiedene Typen von Bahnen.

(i) Von dem ersten Typ Bahn gibt es genau eine, in der alle Elemente aus $\mathbb{P}^1(\mathbb{F}_q)$ liegen. Sie ist von der Länge $q+1$.

(ii) Von dem zweiten Typ gibt es ebenfalls genau eine Bahn, wobei in dieser sämtliche elliptischen Punkte liegen, d.h. sie besitzt die Mächtigkeit q^2-q.

(iii) Von dem dritten Typ gibt es unendlich viele Bahnen, die alle die Länge $(q-1)q(q+1)$ haben. Diese Bahnen stellen eine disjunkte Zerlegung von $\Omega - \mathbb{F}_{q^2}$ dar.

Diese Erkenntnisse werden in dem folgenden Satz benötigt.

Satz 4.10. *Seien $0 \neq f(z) \in M_{k,m}(\Gamma)$ eine Modulform vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ und $\tilde{f}(t) = \sum_{n=i}^{d} a_n t^n$ die t-Entwicklung von $f(z)$ über $\overline{\mathbb{F}}_q$ mit dem Grad $\deg \tilde{f}(t) = d$ $(0 \leq i \leq d \in \mathbb{N}_0)$ und $a_i, a_d \neq 0$. Weiter seien $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ ein elliptischer Punkt und R ein Repräsentantensystem von $\Gamma\backslash(\overline{\mathbb{F}}_q - \mathbb{F}_{q^2})$. Dann gelten*

(i) $\sum_{a\in R} \nu_a(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q-1} = \frac{k}{q^2-1}$ *und*

(ii) $\sum_{a\in R} \nu_a(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q^2-1} = \frac{d}{q^2-1}$.

Bevor der Satz bewiesen wird, machen wir uns die Bedeutung der beiden Aussagen klar: die einzelnen Summanden spiegeln die Nullstellenordnungen der Modulform $f(z) \in M_{k,m}(\Gamma)$ in je einer Sorte von Punkten $a \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ wider. Eine Sorte von Punkten meint in diesem Zusammenhang Punkte, die einem Typ Bahn zugeordnet werden können.
So werden in dem ersten Summanden $\sum_{a\in R}\nu_a(f)$ die Nullstellenordnungen der Modulform $f(z)$ in den Punkten $a \in \overline{\mathbb{F}}_q - \mathbb{F}_{q^2}$ addiert. Nach Lemma 4.9 ist es ausreichend, über ein Repräsentantensystem R zu summieren.

Kurz bemerkt werden soll, daß der Begriff des Repräsentantensystems dem im klassischen Fall verwendeten Begriff des Fundamentalbereichs (vgl. S. 22) entspricht.
In dem zweiten Summanden $\frac{\nu_e(f)}{q+1}$ werden die Nullstellenordnungen der elliptischen Punkte berücksichtigt. Da alle elliptischen Punkte in einer Bahn liegen, ist es ausreichend, die Nullstellenordnung eines beliebigen, aber fest gewählten elliptischen Punktes $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ herauszugreifen.
In dem dritten Summanden werden die Nullstellenordnungen der Modulform $f(z)$ in den Punkten $a \in \mathbb{P}^1(\mathbb{F}_q)$ betrachtet, wobei dieses mit Hilfe der t-Entwicklung $\tilde{f}(t)$ geschieht: es sei $\tilde{f}(t) = a_i t^i + \ldots + a_d t^d$ die t-Entwicklung von $f(z) \in M_{k,m}(\Gamma)$. Dann ist $\nu_\infty(f)$ die Nullstellenordnung von $f(z)$ in $t(z) = 0$, d.h. $\nu_\infty(f) = i$.
Mit Hilfe dieses Satzes ergibt sich ein linearer Zusammenhang zwischen den Nullstellenordnungen für die $a \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ und dem Gewicht $k \in \mathbb{N}_0$ bzw. dem Grad $d \in \mathbb{N}_0$. Es gilt

$$k = q \cdot \nu_\infty(f) + d. \tag{4.2}$$

Kommen wir nun zu dem recht aufwendigen Beweis des Satzes.

Beweis. Wir beginnen mit der leichter zu beweisenden Aussage (*ii*). Dazu sei $0 \neq f(z) \in M_{k,m}(\Gamma)$ eine Modulform. Nach Satz 3.9 lautet die t-Entwicklung

$$f(z) = \tilde{f}(t) = a_i t^i + \ldots + a_d t^d \in \overline{\mathbb{F}}_q[t],$$

wobei $0 \leq i \leq d \in \mathbb{N}_0$, d der Grad der t-Entwicklung und $a_i, a_d \neq 0$ sind.
Durch die Bestimmung des Grads des Divisors der Modulform $f(z)$ auf der projektiven Geraden $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ ergibt sich die Behauptung.
Für den Divisor von $f(z)$ auf $\mathbb{P}^1(\overline{\mathbb{F}}_q)$ gilt

$$\begin{aligned} div(f)_{\mathbb{P}^1(\overline{\mathbb{F}}_q)} &= div(f)_\Omega + div(f)_{\mathbb{P}^1(\mathbb{F}_q)} \\ &= \sum_{a \in \Omega} \nu_a(f) \cdot a + div(f)_{\mathbb{P}^1(\mathbb{F}_q)} \\ &= \sum_{a \in \Omega - \mathbb{F}_{q^2}} \nu_a(f) \cdot a + \sum_{a \in \mathbb{F}_{q^2} - \mathbb{F}_q} \nu_a(f) \cdot a \\ &\quad + \sum_{a \in \mathbb{F}_q} \mu_a(f) \cdot a + \mu_\infty(f) \cdot \infty, \end{aligned} \tag{4.3}$$

wobei $\mu_a(f)$ die Bewertung von $f(z)$ als rationale Funktion in $a \in \mathbb{F}_q$ und $\mu_\infty(f)$ die Bewertung von $f(z)$ als rationale Funktion in ∞ ist. Diese beiden Bewertungen werden jetzt berechnet und anschließend in Gleichung (4.3) eingesetzt.
Da dieses mit Hilfe der t-Entwicklung geschieht, werden zuerst die Bewertungen $\mu_a(t)$ und $\mu_\infty(t)$ der Modulform $t(z) \in M_{q+1,1}(\Gamma)$ als rationale Funktion in $a \in \mathbb{F}_q$ bzw. in $z = \infty$ bestimmt. Weil $t(z)$ für alle $a \in \mathbb{F}_q$ einfache Pole besitzt, folgt

$$\mu_a(t) = -1 \quad \text{für alle } a \in \mathbb{F}_q.$$

Um die Bewertung in $z = \infty$ zu berechnen, setzen wir $z = \frac{1}{w}$ in $t(z)$ ein:

$$t\left(\frac{1}{w}\right) = \frac{1}{\frac{1}{w} - \frac{1}{w^q}} = \frac{w^q}{w^{q-1} - 1}.$$

Die Funktion $t\left(\frac{1}{w}\right)$ besitzt in $w = 0$ eine q-fache Nullstelle, d.h. es gilt

$$\mu_\infty(t) = q.$$

Mit Hilfe dieser beiden Ergebnisse und der t-Entwicklung

$$f(z) = \tilde{f}(t) = a_i t^i + \ldots + a_d t^d \ \in \overline{\mathbb{F}}_q[t]$$

ergibt sich nach der starken Dreiecksungleichung (4.1)

$$\begin{aligned} \mu_a(f) &= d \cdot \mu_a(t) = -d \quad \text{für alle } a \in \mathbb{F}_q \text{ und} \\ \mu_\infty(f) &= i \cdot \mu_\infty(t) = i \cdot q. \end{aligned}$$

Eingesetzt in Gleichung (4.3) erhalten wir für den Divisor von $f(z)$ auf $\mathbb{P}^1(\overline{\mathbb{F}}_q)$

$$\begin{aligned} div(f)_{\mathbb{P}^1(\overline{\mathbb{F}}_q)} &= \sum_{a \in \Omega - \mathbb{F}_{q^2}} \nu_a(f) \cdot a + \sum_{a \in \mathbb{F}_{q^2} - \mathbb{F}_q} \nu_a(f) \cdot a \\ &\quad + \sum_{a \in \mathbb{F}_q} (-d) \cdot a + iq \cdot \infty. \end{aligned}$$

Für den Grad des Divisors von $f(z)$ gilt

$$\deg\left(div(f)_{\mathbb{P}^1(\overline{\mathbb{F}}_q)}\right) = 0,$$

so daß wir mit $i = \nu_\infty(f)$ die folgende Gleichung erhalten

$$\deg(div(f)_{\mathbb{P}^1(\overline{\mathbb{F}}_q)}) = \sum_{a \in \Omega - \mathbb{F}_{q^2}} \nu_a(f) + \sum_{a \in \mathbb{F}_{q^2} - \mathbb{F}_q} \nu_a(f) - dq + q\nu_\infty(f) = 0. \quad (4.4)$$

Da die Nullstellenordnungen unter der Gruppe Γ invariant sind, gelten die beiden folgenden Zusammenhänge:

$$\begin{aligned} \textstyle\sum_{a \in \Omega - \mathbb{F}_{q^2}} \nu_a(f) &= (q-1)q(q+1) \cdot \textstyle\sum_{a \in R} \nu_a(f) \quad \text{und} \\ \textstyle\sum_{a \in \mathbb{F}_{q^2} - \mathbb{F}_q} \nu_a(f) &= q(q-1) \cdot \nu_e(f). \end{aligned}$$

Unter Verwendung dieser Erkenntnisse in Gleichung (4.4) und nach einer Division durch $(q-1)q(q+1)$ ergibt sich mit

$$\sum_{a \in R} \nu_a(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q^2 - 1} = \frac{d}{q^2 - 1}$$

die Aussage (ii).

Um die Aussage (i) zu zeigen, konstruieren wir mit Hilfe der Modulformen $0 \neq f(z) \in M_{k,m}(\Gamma)$ und $t(z) \in M_{q+1,1}(\Gamma)$ eine unter der Gruppe Γ invariante Funktion $F(z) \in \overline{\mathbb{F}}_q(z)$. Durch einen Vergleich der Divisoren ergibt sich die zu beweisende Aussage.

Sei $0 \neq f(z) \in M_{k,m}(\Gamma)$ eine beliebige Modulform. Da für $f(z)$

$$\nu_a(f^n) = n \cdot \nu_a(f)$$

für alle $a \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ gilt, kann eine Reduktion der Modulform $f(z)$ durchgeführt werden: Anstatt direkt die Nullstellenordnungen von $f(z)$ in verschiedenen $a \in \mathbb{P}^1(\overline{\mathbb{F}}_q)$ miteinander zu vergleichen, setzen wir die Nullstellenordnungen von $f(z)^n$ zueinander in Beziehung. Eine Division des Ergebnisses durch n liefert dann das gewünschte Resultat.
Nach Satz 3.6 gilt $f(z)^n \in M_{k\cdot n, m\cdot n}(\Gamma)$, so daß für den weiteren Beweis o.B.d.A. für das Gewicht $k \in \mathbb{N}_0$ und für den Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ gerade $k \equiv 0 \mod (q^2-1)(q-1)$ bzw. $m = 0$ angenommen werden kann. Mit anderen Worten: es gelte $f(z) \in M_{k,0}(\Gamma)$.
Als nächstes wird die unter der Gruppe Γ invariante Funktion $F(z) \in \overline{\mathbb{F}}_q(z)$ konstruiert, indem

$$F(z) := f(z) \cdot t(z)^{-\frac{k}{q+1}}$$

gesetzt wird. Einfaches Nachrechnen zeigt, daß die Funktion $F(z)$ unter den Matrizen

$$\beta = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in B \quad \text{und} \quad \omega = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in \Gamma$$

und somit nach Satz 3.5 unter der Gruppe Γ invariant ist. Dies bedeutet insbesondere, daß für alle $a, b \in \mathbb{F}_q$

$$F(a) = F(a+b) = F\left(\frac{1}{a}\right) \quad \text{und noch spezieller} \quad F(0) = F(\infty)$$

gilt.
Die Funktion $F(z)$ ist nicht zwingend eine Modulform, da nicht auszuschließen ist, daß $F(\infty) = \infty$ ist. Für den weiteren Beweis ist diese Tatsache aber nicht entscheidend.

Betrachten wir jetzt den Divisor von $F(z)$ auf $\mathbb{P}^1(\overline{\mathbb{F}}_q)$. Für den Grad des Hauptdivisors gilt

$$0 = deg\left(div_{\mathbb{P}^1(\overline{\mathbb{F}}_q)} F(z)\right) = deg\left(div_{\Omega} F(z)\right) + deg\left(div_{\mathbb{P}^1(\mathbb{F}_q)} F(z)\right). \tag{4.5}$$

Da sich die Funktion $F(z) = f(z) \cdot t(z)^{-\frac{k}{q+1}} \in \overline{\mathbb{F}}_q(z)$ und die Modulform $f(z) \in M_{k,0}(\Gamma)$ nur durch den Faktor $t(z)^{-\frac{k}{q+1}}$, der Nullstellen und Pole nur auf $\mathbb{P}^1(\mathbb{F}_q)$ besitzt, unterscheiden, gilt

$$\begin{aligned}
deg\,(div_\Omega F(z)) &= deg\,(div_\Omega f(z)) \\
&= \sum_{a\in\Omega} \nu_a(f) \\
&= \sum_{a\in\Omega-\mathbb{F}_{q^2}} \nu_a(f) + \sum_{a\in\mathbb{F}_{q^2}-\mathbb{F}_q} \nu_a(f) \\
&\overset{Le.4.9}{=} \sum_{a\in\Omega-\mathbb{F}_{q^2}} \nu_a(f) + (q^2-q)\cdot\nu_e(f) \\
&= (q-1)q(q+1)\cdot\sum_{a\in R}\nu_a(f) + (q^2-q)\cdot\nu_e(f).
\end{aligned} \tag{4.6}$$

Die Funktion $F(z)$ ist unter der Gruppe Γ invariant. Daher gilt für $a \in \mathbb{P}^1(\mathbb{F}_q)$ und $\gamma \in \Gamma$

$$\nu_a\left(F(z)\right) = \nu_{\gamma a}\left(F(\gamma^{-1}z)\right) = \nu_{\gamma a}\left(F(z)\right).$$

Aufgrund dessen folgt

$$deg\left(div_{\mathbb{P}^1(\mathbb{F}_q)}F(z)\right) = (q+1)\cdot\mu_\infty(F(z)). \tag{4.7}$$

Um die Bewertung von $F(z)$ an der Stelle ∞, sprich $\mu_\infty(F(z))$, berechnen zu können, betrachten wir die t-Entwicklung von $F(z)$. Die t-Entwicklung von $f(z)$ lautet nach Satz 3.9

$$f(z) = \tilde{f}(t) = a_i t^i + \ldots + a_d t^d \in \overline{\mathbb{F}}_q[t],$$

so daß für die t-Entwicklung von $F(z)$

$$\begin{aligned}
F(z) = \tilde{F}(t(z)) &= \left(\sum_{i\le l\le d} a_l t(z)^l\right)\cdot t(z)^{-\frac{k}{q+1}} \\
&= \sum_{i\le l\le d} a_l \cdot t(z)^{l-\frac{k}{q+1}} \\
&= t(z)^{i-\frac{k}{q+1}}\cdot\left(\sum_{i\le l\le d} a_l t(z)^{l-i}\right)
\end{aligned}$$

folgt. Daher gilt $\mu_\infty(F(z)) = q\left(i - \frac{k}{q+1}\right)$ und mit Gleichung (4.7) ergibt sich für den Grad des Divisors von $F(z)$ auf $\mathbb{P}^1(\mathbb{F}_q)$

$$deg\left(div_{\mathbb{P}^1(\mathbb{F}_q)}F(z)\right) = (q+1)\cdot q\left(i - \frac{k}{q+1}\right). \tag{4.8}$$

Werden die Ergebnisse der Gleichungen (4.6) und (4.8) in Gleichung (4.5) eingesetzt, so ergibt sich

$$0 = \sum_{a\in\Omega-\mathbb{F}_{q^2}} \nu_a(f) + (q-1)q\cdot\nu_e(f) + (q+1)\cdot q\left(i-\frac{k}{q+1}\right).$$

Mit $i = \nu_\infty(f)$ und einer Division durch $(q-1)q(q+1)$ folgt die Behauptung

$$\sum_{a \in R} \nu_a(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q-1} = \frac{k}{q^2-1}.$$

$\square$

4.3 Eine Basis des Vektorraumes $M_{k,m}(\Gamma)$

In diesem Abschnitt wird der gesamte $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,m}(\Gamma)$ der Modulformen $f(z)$ vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ betrachtet. Wir erinnern uns an die in Kapitel 3 aufgeworfene Frage nach der Dimension dieses Raums. In Proposition 3.2 konnte lediglich gezeigt werden, daß $M_{k,m}(\Gamma) = 0$, falls $k \not\equiv 2m \mod (q-1)$ gilt. Mit Hilfe der folgenden Überlegungen kann diese Fragestellung für alle Gewichte $k \in \mathbb{N}_0$ und alle Typen $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ beantwortet werden.

Zunächst setzen wir uns mit der Struktur des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$ auseinander. Dazu wird Satz 4.10(i) verwendet, wobei zur Vereinfachung

$$\nu^*(f) := \sum_{z \in R} \nu_z(f)$$

gesetzt wird. Es sei darauf hingewiesen, daß eine Modulform $f(z) \in M_{k,m}(\Gamma)$ aufgrund des Definitionsbereichs Ω Pole höchstens auf $\mathbb{F}_q$ besitzt. Somit gilt

$$\nu_a(f) \geq 0 \quad \text{für alle } a \in \Omega \quad \text{und} \quad \nu_\infty(f) \geq 0.$$

Des weiteren spielen die uns schon bekannte Modulform

$$t(z) = \frac{1}{z - z^q} \in M_{q+1,1}(\Gamma)$$

sowie die spezielle Eisenstein-Reihe

$$E_{q-1}(z) = {\sum_{a,b \in \mathbb{F}_q}}' \frac{1}{(az+b)^{q-1}} \in M_{q-1,0}(\Gamma)$$

eine zentrale Rolle. Zur Vereinfachung werden die Bezeichnungen

$$\begin{aligned} g &:= E_{q-1}(z) \in M_{q-1,0}(\Gamma) \quad \text{und} \\ h &:= -t(z) \in M_{q+1,1}(\Gamma) \end{aligned}$$

eingeführt.
Betrachten wir nun die Nullstellenordnungen dieser beiden Modulformen. Nach Satz 4.10(i) gilt für die Nullstellenordnungen von $g = E_{q-1}(z)$

$$\nu^*(g) + \frac{\nu_e(g)}{q+1} + \frac{\nu_\infty(g)}{q-1} = \frac{q-1}{q^2-1} = \frac{1}{q+1}.$$

Da alle Nullstellenordnungen von g nichtnegativ sind, folgt

$$\nu^*(g) = \nu_\infty(g) = 0 \quad \text{und} \quad \nu_e(g) = 1.$$

Analog erhalten wir für die Nullstellenordnungen von $h = -t(z)$ mit

$$\nu^*(h) + \frac{\nu_e(h)}{q+1} + \frac{\nu_\infty(h)}{q-1} = \frac{q+1}{q^2-1} = \frac{1}{q-1}$$

gerade $\nu^*(h) = \nu_e(h) = 0$ und $\nu_\infty(h) = 1$.

Liegt $g^i h^j$ in $M_{k,m}(\Gamma)$, so gilt mit den obigen Ergebnissen und Satz 4.10(i)

$$\begin{aligned} \tfrac{i\cdot\nu_e(g)}{q+1} + \tfrac{j\cdot\nu_\infty(h)}{q-1} &= \tfrac{k}{q^2-1}, \\ \text{d.h.}\quad i\cdot(q-1) + j\cdot(q+1) &= k. \end{aligned}$$

Wir werden sehen, daß Monome von dem Typ $g^i h^j$, die einer weiteren Bedingung gehorchen, den Vektorraum $M_{k,m}(\Gamma)$ erzeugen.
Das folgende Lemma erhellt die Struktur des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$.

Lemma 4.11. *Sei $M_{k,m}(\Gamma)$ der $\overline{\mathbb{F}}_q$-Vektorraum der Modulformen vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Für den Vektorraum $M_{k,m}(\Gamma)$ gelten:*

(i) Sei

$$M^r_{k,m} := \{f \in M_{k,m}(\Gamma) \mid \nu_\infty(f) \geq r\}$$

der $\overline{\mathbb{F}}_q$-Vektorraum der Modulformen $f(z) \in M_{k,m}(\Gamma)$, die in $t(z) = 0$ eine mindestens r-fache Nullstelle besitzen. Diese $\overline{\mathbb{F}}_q$-Vektorräume mit $0 \leq r \leq r_{max}$ bilden eine Vektorraumkette wie folgt

$$0 = M^{r_{max}}_{k,m} \subseteq \ldots \subseteq M^r_{k,m} \subseteq \ldots \subseteq M^2_{k,m} \subseteq M^1_{k,m} \subseteq M^0_{k,m} = M_{k,m}(\Gamma),$$

wobei die Kodimension $\dim M^r_{k,m}/M^{r+1}_{k,m} \leq 1$ *für alle $0 \leq r \leq r_{max} - 1$ ist.*

(ii) Aus der obigen Vektorraumkette kann eine Teilfolge herausgegriffen werden

$$0 = {}^0M_{k,m} \subset {}^1M_{k,m} \subset {}^2M_{k,m} \subset \ldots \subset {}^{dim_{\overline{\mathbb{F}}_q} M_{k,m}}M_{k,m} = M_{k,m}(\Gamma).$$

Dabei ist ${}^sM_{k,m}$ der wohlbestimmte Vektorraum der Dimension s in der Kette in (i).

Beweis. (i) Es seien $f_1, f_2 \in M^r_{k,m}$. Liegen beide Modulformen nicht in $M^{r+1}_{k,m}$, so besitzen sie nichtverschwindende Koeffizienten in t^r. Eine geeignete Linearkombination $af_1 + bf_2$ hat den t^r-Koeffizienten Null, liegt also in $M^{r+1}_{k,m}$. Damit sind die Klassen von f_1 und f_2 modulo $M^{r+1}_{k,m}$ linear abhängig und es folgt die Behauptung.

(ii) Diese Aussage folgt offensichtlich aus (i).

□

Bevor wir schlußendlich den Satz formulieren, der uns zu einer Basis von $M_{k,m}(\Gamma)$ verhilft, wenden wir uns zwei weiteren Lemmata zu. Diese werden für den Beweis des Satzes benötigt.

Lemma 4.12. *Sei $f \in M_{0,m}(\Gamma)$ eine Modulform vom Gewicht 0 und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Dann ist f konstant und es gilt $f \in M_{0,0}(\Gamma)$.*

Beweis. Es sei $f \in M_{0,m}(\Gamma)$ eine Modulform mit

$$\sum_{a \in R} \nu_a(f) + \frac{\nu_e(f)}{q+1} + \frac{\nu_\infty(f)}{q-1} = \frac{k}{q^2-1} = 0.$$

Aufgrund von $\nu_b(f) \geq 0$ für alle $b \in \Omega \cup \{\infty\}$ folgt direkt $\nu_b(f) = 0$ für alle $b \in \Omega \cup \{\infty\}$. Folglich ist f konstant und es gilt $f \in M_{0,0}(\Gamma)$. □

Lemma 4.13. *Sei $f \in M_{k,m}(\Gamma)$ eine Modulform vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Weiter sei $k \equiv 2m \mod (q-1)$. Dann gilt für alle in der t-Entwicklung*

$$f(z) = \tilde{f}(t(z)) = a_i t(z)^i + \ldots + a_d t(z)^d \in \overline{\mathbb{F}}_q[t]$$

auftretenden Exponenten $l \in \mathbb{N}_0$ (d.h. $a_l \neq 0$) mit $i \leq l \leq d$

$$l \equiv m \mod (q-1).$$

Beweis. Es ist $t(z) = \frac{1}{z-z^q} \in M_{q+1,1}(\Gamma)$ und $f(z) \in M_{k,m}(\Gamma)$ eine beliebige Modulform vom Gewicht k und vom Typ m mit der t-Entwicklung

$$f(z) = \tilde{f}(t(z)) = a_i t(z)^i + \ldots + a_l t(z)^l + \ldots + a_d t(z)^d \in \overline{\mathbb{F}}_q[t].$$

Sei $b \in \mathbb{F}_q^*$ mit $< b >= \mathbb{F}_q^*$. Mit $\beta = \begin{pmatrix} b & 0 \\ 0 & 1 \end{pmatrix} \in \Gamma$ und $f \in M_{k,m}(\Gamma)$ folgt einerseits

$$\begin{aligned} f(\beta z) &= f(b \cdot z) = b^{-m} \cdot f(z) \\ &= b^{-m}\left(a_i t(z)^i + \ldots + a_l t(z)^l + \ldots + a_d t(z)^d\right) \\ &= b^{-m} a_i t(z)^i + \ldots + b^{-m} a_l t(z)^l + \ldots + b^{-m} a_d t(z)^d \qquad (4.9) \end{aligned}$$

und andererseits

$$\begin{aligned} f(\beta z) &= a_i t(\beta z)^i + \ldots + a_l t(\beta z)^l + \ldots + a_d t(\beta z)^d \\ &= a_i t(bz)^i + \ldots + a_l t(bz)^l + \ldots + a_d t(bz)^d \\ &= b^{-i} a_i t(z)^i + \ldots + b^{-l} a_l t(z)^l + \ldots + b^{-d} a_d t(z)^d. \qquad (4.10) \end{aligned}$$

Die Gleichungen 4.9 und 4.10 implizieren

$$b^{-m} = b^{-l}$$

für alle $l \in \mathbb{N}_0$ mit $i \leq l \leq d$ und $a_l \neq 0$. Wegen $< b >= \mathbb{F}_q^*$ folgt für solche l nun $l \equiv m \mod (q-1)$. □

Bemerkung 4.14. *In dem Spezialfall $\nu_\infty(f) = 0$ (d.h. $a_0 \neq 0$) gilt für eine Modulform $f \in M_{k,m}(\Gamma)$ vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ mit $k \equiv 2m \mod (q-1)$ gerade $m = 0$, d.h. $f \in M_{k,0}(\Gamma)$.*

Nach diesen umfangreichen Vorbereitungen sind wir nun in der Lage, uns Gedanken über die Basis des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$ zu machen.

Satz 4.15. *Sei $M_{k,m}(\Gamma)$ der $\overline{\mathbb{F}}_q$-Vektorraum der Modulformen $f(z) \in \overline{\mathbb{F}}_q(z)$ vom Gewicht $k \in \mathbb{N}$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$. Er besitzt als Basis die Monome $g^i h^j$ mit $0 \leq i, j$, für die*

$$i \cdot (q-1) + j \cdot (q+1) = k \quad \textit{und} \quad m \equiv j \, mod(q-1) \tag{4.11}$$

gilt.

Beweis. Es ist zu zeigen, daß für

$$i \cdot (q-1) + j \cdot (q+1) = k \quad \text{und} \quad m \equiv j \, mod(q-1)$$

mit $0 \leq i, j$

(i) die Monome $g^i h^j$ Elemente von $M_{k,m}(\Gamma)$ sind. Da

$$g = E_{q-1}(z) \in M_{q-1,0}(\Gamma) \quad \text{und} \quad h = -t(z) \in M_{q+1,1}(\Gamma)$$

folgt mit Satz 3.6 (i) und (ii), daß $g^i h^j \in M_{i\cdot(q-1)+j\cdot(q+1),j}(\Gamma)$ gilt. Somit liegen alle Monome $g^i h^j$, die Gleichung (4.11) erfüllen, in $M_{k,m}(\Gamma)$.

(ii) die Monome $g^i h^j$ linear unabhängig sind.
Die Monome $g^i h^j$ sind durch Gleichung (4.11) eindeutig bestimmt. Da sie paarweise verschiedene $\nu_\infty(g^i h^j) = j$ besitzen, sind sie linear unabhängig.

(iii) die Monome $g^i h^j$ den $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,m}(\Gamma)$ erzeugen.
Zuerst überlegen wir uns, ob die $i, j \in \mathbb{N}_0$ mit $i \cdot (q-1) + j \cdot (q+1) = k$ und $j \equiv m \mod (q-1)$ wirklich für $k \not\equiv 2m \mod (q-1)$ einen $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,m}(\Gamma)$ der Dimension $dim_{\overline{\mathbb{F}}_q} M_{k,m}(\Gamma) = 0$ erzeugen. Dazu betrachten wir die Folgerungen:

$$\begin{array}{lllll} & i \cdot (q-1) + j \cdot (q+1) = k & \text{und} & j \equiv m & \mod (q-1) \\ \Rightarrow & j \cdot (q+1) \equiv k \mod (q-1) & \text{und} & j \equiv m & \mod (q-1) \\ \Rightarrow & 2j \equiv k \mod (q-1) & \text{und} & j \equiv m & \mod (q-1) \\ \Rightarrow & 2m \equiv k \mod (q-1). & & & \end{array}$$

Somit gilt für $k \not\equiv 2m \mod (q-1)$ gerade $M_{k,m}(\Gamma) = 0$. Im weiteren sei $k \equiv 2m \mod (q-1)$.

Die Aussage wird mit Hilfe von vollständiger Induktion über k bewiesen.
Für den Induktionsanfang sei $k = 0$ und es gilt nach Lemma 4.12

$$M_{0,m}(\Gamma) =< g^i h^j \mid i = 0, j = 0, 0 \equiv m \mod (q-1) > .$$

Weiter setzen wir als Induktionsannahme voraus, die Aussage

$$M_{l,m}(\Gamma) = \left\langle \begin{array}{l} g^i h^j \mid i, j \in \mathbb{N}_0,\ i \cdot (q-1) + j \cdot (q+1) = l, \\ j \equiv m \mod (q-1) \end{array} \right\rangle$$

sei für alle $l \in \mathbb{N}_0$ mit $l < k$ und $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ bereits gezeigt. Im Induktionsschritt schließen wir von $k-1$ auf k. Dazu sei $f(z) \in M_{k,m}(\Gamma)$ eine Modulform mit der t-Entwicklung

$$f(z) = \tilde{f}(t) = a_i t^i + \ldots + a_d t^d \in \overline{\mathbb{F}}_q[t]$$

und $i = \nu_\infty(f)$. Die $\nu_\infty(f)$ sind nichtnegativ, da f eine Modulform und deswegen insbesondere $f(\infty) \neq \infty$ ist. Wir unterscheiden die Fälle $\nu_\infty(f) > 0$ und $\nu_\infty(f) = 0$.
1. Fall: $\nu_\infty(f) > 0$
Es folgt $f(\infty) = 0$. Für die t-Entwicklung von $f \in M_{k,m}(\Gamma)$ gilt

$$f(z) = \tilde{f}(t) = a_i t^i + \ldots + a_d t^d$$

mit $i > 0$ bzw.

$$f(z) = -t \cdot (-a_i t^{i-1} - \ldots - a_d t^{d-1}),$$

wobei $-t(z) = h$ ist. Setze $F(z) := -a_i t^{i-1} \ldots - a_d t^{d-1}$. Es folgt nach Satz 3.6(ii) mit $f(z) \in M_{k,m}(\Gamma)$ und $t(z) \in M_{q+1,1}(\Gamma)$ gerade $F(z) \in M_{k-(q+1),m-1}(\Gamma)$ und nach Induktionsannahme existiert eine Darstellung

$$F(z) = \sum b_{xy} g^x h^y$$

mit $x, y \in \mathbb{N}_0$, $x \cdot (q-1) + y \cdot (q+1) = k - (q+1)$, $m - 1 \equiv y \mod (q-1)$ und $b_{xy} \in \overline{\mathbb{F}}_q$, so daß

$$f(z) = h \cdot F(z) = \sum b_{xy} g^x h^{y+1}$$

mit $x, y+1 \in \mathbb{N}_0$, $x \cdot (q-1) + (y+1) \cdot (q+1) = k$, $y+1 \equiv (m-1)+1 \equiv m \mod (q-1)$ und $b_{xy} \in \overline{\mathbb{F}}_q$ folgt. Somit ist der Fall $\nu_\infty(f) > 0$ bewiesen.

2. Fall: $\nu_\infty(f) = 0$
Folglich gilt $i = 0$ und daher nach Bemerkung 4.14 auch $m = 0$. Also ist

$$M_{k,0}(\Gamma) = \left\langle \begin{array}{l} g^i h^j \mid i, j \in \mathbb{N}_0,\ i \cdot (q-1) + j \cdot (q+1) = k, \\ j \equiv 0 \mod (q-1) \end{array} \right\rangle$$

zu zeigen.
Wir konstruieren nun eine Modulform, die in $M_{k,0}(\Gamma)$ liegt.
Aus $w := \frac{k}{q-1} \in \mathbb{N}_0$ ergibt sich $g^w \in M_{k,0}(\Gamma)$ und aus $\nu_\infty(g) = 0$ folgt $0 \neq g(\infty) \in \overline{\mathbb{F}}_q$. Da $\frac{f(\infty)}{g(\infty)^w} \in \overline{\mathbb{F}}_q$ gilt $\nu_\infty\left(f - \frac{f(\infty)}{g(\infty)^w} \cdot g^w\right) > 0$. Aufgrund dieser Überlegungen erhalten wir die Modulform

$$f - \frac{f(\infty)}{g(\infty)^w} \cdot g^w \in M_{k,0}(\Gamma).$$

Betrachten wir die t-Entwicklung dieser Modulform

$$\begin{aligned} f - \frac{f(\infty)}{g(\infty)^w} \cdot g^w &= c_u t^u + \ldots + c_v t^v \\ &= -t \cdot (-c_u t^{u-1} - \ldots - c_v t^{v-1}) \end{aligned}$$

mit $c_u \neq 0,\ u \geq 1$. Mit dem gleichen Argument wie im ersten Fall folgt, daß $b_{xy} \in \overline{\mathbb{F}}_q$ existieren, so daß

$$f - \frac{f(\infty)}{g(\infty)^w} \cdot g^w = \sum b_{xy} g^x h^{y+1}$$

mit $x, y+1 \in \mathbb{N}_0$, $x \cdot (q-1) + (y+1) \cdot (q+1) = k$ und $y + 1 \equiv m \equiv 0 \mod (q-1)$ gilt. Es folgt

$$\begin{aligned} f &= \frac{f(\infty)}{g(\infty)^w} \cdot g^w + \sum b_{xy} g^x h^{y+1} \\ &\in \left\langle \begin{array}{l} g^i h^j \mid i,j \in \mathbb{N}_0,\ i \cdot (q-1) + j \cdot (q+1) = k, \\ j \equiv 0 \mod (q-1) \end{array} \right\rangle . \end{aligned}$$

Mit dem 1. und 2. Fall ist der Induktionsschritt komplett und es folgt: $f(z) \in M_{k,m}(\Gamma)$ liegt in dem Erzeugnis von

$$\{g^i h^j \mid i,j \in \mathbb{N}_0,\ i \cdot (q-1) + j \cdot (q+1) = l,\ j \equiv 0 \mod (q-1)\}.$$

□

Nachdem wir uns eingehend mit dem $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,m}(\Gamma)$ der Modulformen vom Gewicht $k \in \mathbb{N}_0$ und vom Typ $m \in \mathbb{Z}/(q-1)\mathbb{Z}$ beschäftigt haben, können wir jetzt seine Dimension bestimmen.

Lemma 4.16. *Für die Dimension des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$ gilt*

$$\dim_{\overline{\mathbb{F}}_q} M_{k,m}(\Gamma) = \begin{cases} [\frac{k}{q^2-1} - \frac{m}{q-1}] + 1\ , & k \equiv 2m \bmod q-1 \\ 0\ , & \textit{sonst} \end{cases} .$$

Dabei bezeichnet $[a]$ die größte ganze Zahl kleiner oder gleich $a \in \mathbb{R}$ und m in $\{0, 1, \ldots, q-2\}$ den eindeutig bestimmten Vertreter der Äquivalenzklasse $\overline{m}$.

Beweis. Die Aussage $\dim_{\overline{\mathbb{F}}_q} M_{k,m}(\Gamma) = 0$ für den Fall $k \not\equiv 2m \mod (q-1)$ entspricht Proposition 3.2.
Für $k \equiv 2m \mod (q-1)$ ist nach Satz 4.15 klar, daß für die Dimension des $\overline{\mathbb{F}}_q$-Vektorraums $M_{k,m}(\Gamma)$ gilt

$$\dim_{\overline{\mathbb{F}}_q} M_{k,m}(\Gamma) = \# \left\{ \begin{array}{l} (i,j) \mid i,j \in \mathbb{N}_0,\ i(q-1)+j(q+1)=k, \\ j \equiv m \mod (q-1) \end{array} \right\}.$$

Durch Abzählen der Elemente dieser Menge ergibt sich die Behauptung. Wir beginnen mit den folgenden Überlegungen

$$\begin{aligned}
\dim_{\overline{\mathbb{F}}_q} M_{k,m}(\Gamma) &= \# \left\{ \begin{array}{l} (i,j) \mid i,j \in \mathbb{N}_0,\ j \equiv m \mod (q-1), \\ i \cdot (q-1) + j \cdot (q+1) = k \end{array} \right\} \\
&= \# \left\{ \begin{array}{l} \alpha \in \mathbb{Z} \mid j = m + \alpha \cdot (q-1) \in \mathbb{N}_0, \\ i = \frac{1}{q-1} \cdot (k - j \cdot (q+1)) \in \mathbb{N}_0 \end{array} \right\} \\
&= \# \left\{ \begin{array}{l} \alpha \in \mathbb{Z} \mid m + \alpha \cdot (q-1) \in \mathbb{N}_0, \\ \frac{1}{q-1} \cdot (k - (m + \alpha \cdot (q-1)) \cdot (q+1)) \in \mathbb{N}_0 \end{array} \right\} \\
&= \# \left\{ \begin{array}{l} \alpha \in \mathbb{Z} \mid \alpha \geq -\frac{m}{q-1}, \\ \frac{1}{q-1} \cdot (k - m \cdot (q+1) - \alpha \cdot (q-1) \cdot (q+1)) \in \mathbb{N}_0 \end{array} \right\} \\
&= \# \left\{ \begin{array}{l} \alpha \in \mathbb{Z} \mid \alpha \geq -\frac{m}{q-1}, \\ \frac{1}{q-1} \cdot (k - m \cdot (q+1) - \alpha \cdot (q-1) \cdot (q+1)) \in \mathbb{Z}, \\ \frac{1}{q-1} \cdot (k - m \cdot (q+1) - \alpha \cdot (q-1) \cdot (q+1)) \geq 0 \end{array} \right\}.
\end{aligned}$$

Um die Struktur der Menge weiter zu vereinfachen, machen wir uns klar, daß der Term $k - m \cdot (q+1) + \alpha \cdot (q-1)(q+1)$ durch $q-1$ teilbar ist:

$$\begin{aligned}
& k - m \cdot (q+1) + \alpha \cdot (q-1)(q+1) \mod (q-1) \\
= \;& k - m \cdot (q+1) \mod (q-1) \\
\overset{k \equiv 2m \mod (q-1)}{=} \;& 2m - mq - m \mod (q-1) \\
= \;& m - mq \mod (q-1) \\
= \;& -m \cdot (q-1) \mod (q-1) \\
= \;& 0.
\end{aligned}$$

Beachten wir dies in der Betrachtung der Dimension, so ergibt sich

$$\begin{aligned}
\dim_{\overline{\mathbb{F}}_q} M_{k,m}(\Gamma) &= \# \left\{ \begin{array}{l} \alpha \in \mathbb{Z} \mid \alpha \geq -\frac{m}{q-1}, \\ k - m \cdot (q+1) - \alpha \cdot (q-1)(q+1) \geq 0 \end{array} \right\} \\
&= \# \left\{ \begin{array}{l} \alpha \in \mathbb{Z} \mid \alpha \geq -\frac{m}{q-1}, \\ k - m \cdot (q+1) \geq \alpha \cdot (q-1)(q+1) \end{array} \right\} \\
&= \# \{\alpha \in \mathbb{Z} \mid \alpha \geq -\frac{m}{q-1}, \quad \frac{k}{(q-1)(q+1)} - \frac{m}{q-1} \geq \alpha\} \\
&= \# \{\alpha \in \mathbb{Z} \mid -\frac{m}{q-1} \leq \alpha \leq \frac{k}{q^2-1} - \frac{m}{q-1}\} \\
&= [\frac{k}{q^2-1} - \frac{m}{q-1}] + 1.
\end{aligned}$$

$\square$

In diesem Kapitel haben wir uns die Struktur des $\overline{\mathbb{F}}_q$-Vektorraumes $M_{k,m}(\Gamma)$ verdeutlicht. Im Grunde verlaufen die Überlegungen analog zu denen im Fall der Modulformen über der komplexen oberen Halbebene H.

Kapitel 5

Die Nullstellen der Eisenstein-Reihen

Bereits in den letzten beiden Kapiteln wurde deutlich, daß die Eisenstein-Reihen in der Theorie der Modulformen über endlichen Körpern eine bedeutende Rolle spielen. Nachdem sie bisher hauptsächlich als Hilfsmittel für beispielsweise die Bestimmung der Dimension des $\overline{\mathbb{F}}_q$-Vektorraumes $M_{k,m}(\Gamma)$ verwandt wurden, werden in diesem Kapitel die Nullstellen der Eisenstein-Reihen bestimmt.
Das wichtigste hierzu benötigte Hilfsmittel sind die Goss-Polynome. Um einige Eigenschaften von diesen beweisen zu können, sind im ersten Abschnitt dieses Kapitels verschiedene Hilfsmittel zusammengestellt.

5.1 Die Newton-Formeln

Zentral in diesem Abschnitt sind die Newton-Formeln [CLO92, 7.1, Beweis zu Th. 8], die im weiteren Verlauf des Kapitels eine wichtige Rolle spielen. Außerdem wird noch ein Lemma bewiesen, das ebenfalls im nächsten Abschnitt benötigt wird.

Satz 5.1. *Es sei K ein beliebiger Körper,*

$$f(X) = X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n$$

ein Polynom über K und

$$S_k = \sum_{i=1}^{n} \alpha_i^k$$

die Summe der k-ten Potenzen der Nullstellen α_i von $f(X)$ mit $k \in \mathbb{N}_0$, gezählt mit Vielfachheiten. Dann gelten die beiden folgenden Relationen für $k \in \mathbb{N}_0$:

$$\begin{aligned} S_k + a_1S_{k-1} + \ldots + a_{k-1}S_1 + ka_k &= 0 \quad (k \leq n) && (5.1)\\ S_k + a_1S_{k-1} + \ldots + a_{n-1}S_{k-n+1} + a_nS_{k-n} &= 0 \quad (k \geq n). && (5.2) \end{aligned}$$

Diese Relationen heißen Newton-Formeln.

Bevor wir mit dem Beweis beginnen, überlegen wir uns, daß die beiden Relationen für den Fall $k = n$ übereinstimmen. Offensichtlich ist dies genau dann der Fall, wenn $n = S_0$ gilt. Dies folgt aber aus $S_0 = \sum_{i=1}^n \alpha_i^0 = n$.

Wir verwenden die Notationen

$$\begin{aligned} S_k^n(X_1, \ldots, X_n) &:= X_1^k + \ldots + X_n^k \in K[X_1, \ldots, X_n] \quad \text{und} \\ \sigma_k^n(X_1, \ldots, X_n) &:= \sum_{\substack{S \subseteq \{1, \ldots, n\} \\ \#S = k}} \prod_{i \in S} X_i \in K[X_1, \ldots, X_n] \end{aligned}$$

für die Summe der k-ten Potenzen in n Variablen und das k-te elementarsymmetrische Polynom in n Variablen in den abkürzenden Schreibweisen

$$\begin{aligned} S_k^n &:= S_k^n(X_1, \ldots, X_n) \quad \text{und} \\ \sigma_k^n &:= \sigma_k^n(X_1, \ldots, X_n). \end{aligned}$$

Ferner benötigen wir für den Beweis ein Lemma [CLO92, 7.1, Ex. 3, 14].

Lemma 5.2. *Seien σ_k^n das k-te elementarsymmetrische Polynom in n Variablen und S_k^n die Summe der k-ten Potenzen in n Variablen. Dann gilt mit $\sigma_0^n = 1$ und $\sigma_k^n = 0$ für $k < 0$ oder $k > n$*

$$\begin{aligned} \sigma_k^n &= \sigma_k^{n-1} + X_n \cdot \sigma_{k-1}^{n-1} \quad \textit{und} \\ S_k^n &= S_k^{n-1} + X_n^k \end{aligned}$$

für $n \geq 2$ und $k \in \mathbb{Z}$.

Beweis. Der Beweis der ersten Aussage wird mit Hilfe von vollständiger Induktion über n geführt.
Für den Induktionsanfang sei $n = 2$ und die Behauptung gilt offensichtlich. Weiter nehmen wir an, $\sigma_k^n = \sigma_k^{n-1} + X_n \cdot \sigma_{k-1}^{n-1}$ sei für n bewiesen. Mit dem Induktionsschritt von n auf $n+1$ folgt die Behauptung:

$$\begin{aligned} \sigma_k^{n+1} &= \sum_{\substack{S \subseteq \{1, \ldots, n+1\} \\ \#S = k}} \prod_{j \in S} X_j \\ &\overset{Ind.Ann.}{=} \sum_{\substack{S \subseteq \{1, \ldots, n\} \\ \#S = k}} \prod_{j \in S} X_j + \sum_{\substack{S \subseteq \{1, \ldots, n\} \\ \#S = k-1}} X_{n+1} \cdot \prod_{j \in S} X_j \\ &= \sigma_k^n + X_{n+1} \cdot \sigma_{k-1}^n. \end{aligned}$$

Die zweite Aussage gilt trivialerweise nach der Definition der S_k^n. □

Beweis des Satzes 5.1. Wir beweisen, daß die Newton-Formeln eine Identität als Polynome sind [CLO92, 7.1, Ex. 14]. Mit obigen Notationen sind die Relationen (5.1) und (5.2) identisch mit

$$\begin{aligned} S_k - \sigma_1 S_{k-1} + \ldots + (-1)^{k-1}\sigma_{k-1}S_1 + (-1)^k k\sigma_k &= 0 \quad (k \leq n) \\ S_k - \sigma_1 S_{k-1} + \ldots + (-1)^{n-1}\sigma_{n-1}S_{k-n+1} + (-1)^n \sigma_n S_{k-n} &= 0 \quad (k \geq n). \end{aligned}$$

Diese wiederum sind für $\sigma_0 = 1$ und $\sigma_i = 0$, falls $i < 0$ oder $i > n$ ist, trivialerweise äquivalent zu

$$S_k - \sigma_1 S_{k-1} + \ldots + (-1)^{k-1}\sigma_{k-1}S_1 + (-1)^k k\sigma_k = 0 \quad \text{für} \quad k \geq 1.$$

Diese Gleichung wird mittels Induktion über n bewiesen, d.h. die Anzahl der Variablen wird variiert. Dazu schreiben wir die Gleichung wie folgt:

$$\begin{aligned} 0 &= S_k^n - \sigma_1^n \cdot S_{k-1}^n + \ldots + (-1)^{k-1} \cdot \sigma_{k-1}^n \cdot S_1^n + (-1)^k \cdot k \cdot \sigma_k^n \\ &= \sum_{i=0}^{k-1} (-1)^i \cdot \sigma_i^n \cdot S_{k-i}^n + (-1)^k \cdot k \cdot \sigma_k^n \\ &=: F_k(X_1, \ldots, X_n) \\ &=: F_k^n \end{aligned}$$

für $k \geq 1$. Für den Induktionsanfang ist für $n = 1$ und $k \geq 1$

$$F_k^1 = \sum_{i=0}^{k-1} (-1)^i \cdot \sigma_i^1 \cdot S_{k-i}^1 + (-1)^k \cdot k \cdot \sigma_k^1 = 0$$

zu zeigen. Dies gilt trivialerweise.
Für die Induktionsannahme sei

$$F_k^l = \sum_{i=0}^{k-1} (-1)^i \cdot \sigma_i^l \cdot S_{k-i}^l + (-1)^k \cdot k \cdot \sigma_k^l = 0$$

für $l \leq n$ und $k \geq 1$ bewiesen. Im Induktionsschritt wird nun von n auf $n+1$ geschlossen:

$$\begin{aligned} F_k^{n+1} &= \sum_{i=0}^{k-1} (-1)^i \cdot \sigma_i^{n+1} \cdot S_{k-i}^{n+1} + (-1)^k \cdot k \cdot \sigma_k^{n+1} \\ &\overset{Le. 5.2}{=} \sum_{i=0}^{k-1} (-1)^i \cdot \Big(\sigma_i^n \cdot S_{k-i}^n + X_{n+1} \cdot \sigma_{i-1}^n \cdot S_{k-i}^n + X_{n+1}^{k-i} \cdot \sigma_i^n \\ &\quad + X_{n+1}^{k-i} \cdot X_{n+1} \cdot \sigma_{i-1}^n \Big) + (-1)^k \cdot k \cdot \sigma_k^n + (-1)^k \cdot k \cdot X_{n+1} \cdot \sigma_{k-1}^n \\ &\overset{Ind.Ann.}{=} \sum_{i=0}^{k-1} (-1)^i \cdot \Big(X_{n+1} \cdot \sigma_{i-1}^n \cdot S_{k-i}^n + X_{n+1}^{k-i} \cdot \sigma_i^n + X_{n+1}^{k-i+1} \cdot \sigma_{i-1}^n \Big) \\ &\quad + (-1)^k \cdot k \cdot X_{n+1} \cdot \sigma_{k-1}^n. \end{aligned}$$

Wir klammern den Faktor X_{n+1} aus und ziehen die Terme für $i=0$ aus der Summe heraus. Damit erhalten wir

$$\begin{aligned}
F_k^{n+1} &= X_{n+1}\cdot\Bigg(X_{n+1}^{k-1}+\sum_{i=1}^{k-1}(-1)^i\cdot\sigma_{i-1}^n\cdot S_{k-i}^n+\sum_{i=1}^{k-1}(-1)^i\cdot X_{n+1}^{k-i-1}\cdot\sigma_i^n \\
&\quad+\sum_{i=1}^{k-1}(-1)^i\cdot X_{n+1}^{k-i}\cdot\sigma_{i-1}^n+(-1)^k\cdot k\cdot\sigma_{k-1}^n\Bigg) \\
&\overset{j-1=i}{=} X_{n+1}\cdot\Bigg(X_{n+1}^{k-1}+\sum_{i=1}^{k-1}(-1)^i\cdot\sigma_{i-1}^n\cdot S_{k-i}^n+\sum_{j=2}^{k}(-1)^{j-1}\cdot X_{n+1}^{k-j}\cdot\sigma_{j-1}^n \\
&\quad+\sum_{i=1}^{k-1}(-1)^i\cdot X_{n+1}^{k-i}\cdot\sigma_{i-1}^n+(-1)^k\cdot k\cdot\sigma_{k-1}^n\Bigg) \\
&\overset{j-1=i}{=} X_{n+1}\cdot\Bigg(X_{n+1}^{k-1}+\sum_{i=1}^{k-1}(-1)^i\cdot\sigma_{i-1}^n\cdot S_{k-i}^n+(-1)^{k-1}\cdot\sigma_{k-1}^n-X_{n+1}^{k-1} \\
&\quad+(-1)^k\cdot k\cdot\sigma_{k-1}^n\Bigg) \\
&= X_{n+1}\cdot\left(\sum_{i=1}^{k-1}(-1)^i\cdot\sigma_{i-1}^n\cdot S_{k-i}^n-(-1)^{k-1}\cdot(k-1)\cdot\sigma_{k-1}^n\right).
\end{aligned}$$

Für den Fall $k=1$ ergibt sich direkt die Behauptung, für den Fall $k>1$ folgt mit der Induktionsannahme

$$\begin{aligned}
F_k^{n+1} &\overset{Ind.Ann.}{=} X_{n+1}\cdot\left(\sum_{i=1}^{k-1}(-1)^i\cdot\sigma_{i-1}^n\cdot S_{k-i}^n+\sum_{i=0}^{k-2}(-1)^i\cdot\sigma_i^n\cdot S_{k-i-1}^n\right) \\
&\overset{j=i-1}{=} X_{n+1}\cdot\left(\sum_{i=0}^{k-2}(-1)^{i+1}\cdot\sigma_i^n\cdot S_{k-i-1}^n+\sum_{i=0}^{k-2}(-1)^i\cdot\sigma_i^n\cdot S_{k-i-1}^n\right) \\
&= 0.
\end{aligned}$$

□

Neben den Newton-Formeln benötigen wir im weiteren Verlauf dieses Kapitels ein Lemma.

Lemma 5.3. *Es ist $\mathbb{F}_q$ ein endlicher Körper. Dann gilt für alle $j\in\mathbb{N}$*

(i) $\sum_{a\in\mathbb{F}_q}\prod_{b\in\mathbb{F}_q,b\neq a}(X-b)=(-1)^{q^j}$ *über $\mathbb{F}_q[X]$ und*

(ii) $\sum_{a\in\mathbb{F}_q^*}a\prod_{b\in\mathbb{F}_q^*,b\neq a}(X-b)=(-1)^{q^j}$ *über $\mathbb{F}_q[X]$.*

Beweis. Die Beweise für die beiden Aussagen dieses Lemmas verlaufen analog, so daß nur der Beweis für die Aussage (i) detailliert ausgeführt. In beiden Aussagen sei p die Charakteristik von $\mathbb{F}_q$.

(i) Es sei $f(X) = \sum_{a \in \mathbb{F}_q} \prod_{b \in \mathbb{F}_q, b \neq a} (X - b) - (-1)^{q^j}$ ein Polynom in $\mathbb{F}_q[X]$ mit dem Grad $\deg f(X) \leq q - 1$. Für $c \in \mathbb{F}_q$ gilt dann

$$
\begin{aligned}
f(c) &= \sum_{a \in \mathbb{F}_q} \prod_{b \in \mathbb{F}_q, b \neq a} (c - b) - (-1)^{q^j} \\
&= \prod_{b \in \mathbb{F}_q, b \neq c} (c - b) - (-1)^{q^j} \\
&= \prod_{d \in \mathbb{F}_q^*} d - (-1)^{q^j} \\
&= -1 - (-1)^{q^j} \\
&\stackrel{char \mathbb{F}_q = p}{=} -1 - \begin{cases} 1 & , \text{ für } p = 2 \\ -1 & , \text{ für } p \neq 2 \end{cases} \\
&= 0.
\end{aligned}
$$

Es ist $\prod_{d \in \mathbb{F}_q^*} d = -1$, da jedes Element der multiplikativen Gruppe $\mathbb{F}_q^*$ mit Ausnahme von -1 und 1 ein von sich selbst verschiedenes inverses Element besitzt. Die Elemente -1 und 1 sind jeweils zu sich selbst invers.
Da $c \in \mathbb{F}_q$ beliebig gewählt werden kann, hat $f(X)$ mindestens q verschiedene Nullstellen. Wegen $\deg f(X) \leq q - 1$ folgt $f \equiv 0$ und somit die Behauptung.

(ii) Es sei $f(X) = \sum_{a \in \mathbb{F}_q^*} a \prod_{b \in \mathbb{F}_q^*, b \neq a} (X - b) - (-1)^{q^j}$ ein Polynom vom Grad $\deg f(X) \leq q - 2$. Für $c \in \mathbb{F}_q^*$ gilt analog zu dem Beweis der Aussage (i)

$$f(c) = \sum_{a \in \mathbb{F}_q^*} \prod_{b \in \mathbb{F}_q^*, b \neq a} (c - b) - (-1)^{q^j} = 0,$$

so daß $f(X)$ mindestens $q - 1$ verschiedene Nullstellen besitzt. Wegen $\deg f(X) \leq q - 2$ folgt $f \equiv 0$ und somit die Behauptung.

$\square$

Im folgenden benötigen wir das logarithmische Differenzieren.

Bemerkung 5.4. *Die logarithmische Ableitung einer Funktion* $0 \neq f \in K(X)$ *nach der Unbestimmten* X *ist definiert durch*

$$dlog f(X) := \frac{f'(X)}{f(X)}.$$

Für zwei Funktionen $f, g \in K(X)$ *gilt mittels der Produktregel*

$$dlog(f \cdot g) = dlog\, f + dlog\, g.$$

5.2 Die Goss-Polynome

In diesem Abschnitt wird zu Beginn eine Definition der Goss-Polynome gegeben. Anschließend werden die wichtigsten Eigenschaften ausführlich dargestellt und erörtert, wobei für die Beweise auf die Ergebnisse des vorangegangenen Abschnitts zurückgegriffen wird.
Beginnen wir mit der

Definition 5.5. *Die Polynome $G_k(X)$ aus $\mathbb{F}_q[X]$, die durch die folgende Rekursion definiert werden,*

(i) $G_k(X) = 0$ *für alle* $k \leq 0$,

(ii) $G_1(X) = X$ *und*

(iii) $G_k(X) = X\left(G_{k-1}(X) - G_{k-q}(X)\right)$ *für alle* $k \geq 1$

heißen Goss-Polynome. G_k *heißt das* k*-te Goss-Polynom über* $\mathbb{F}_q$.

Mit dieser rekursiven Definition gelten die im folgenden Satz zusammengefaßten Eigenschaften für die Goss-Polynome.

Satz 5.6. *Für die in Definition 5.5 definierten Goss-Polynome gelten die folgenden Eigenschaften:*

(i) $deg\, G_k(X) = k$ *für* $k \geq 0$,

(ii) $\sum_{a\in\mathbb{F}_q} \frac{1}{(z-a)^k} = G_k(t(z))$ *mit* $t(z) = \frac{1}{z-z^q} \in M_{q+1,1}(\Gamma)$ *für* $k \geq 1$,

(iii) $G_k(X) = X^k$ *für alle* $1 \leq k \leq q$,

(iv) $G_{pk}(X) = (G_k(X))^p$, *wobei* p *die Charakteristik von* $\mathbb{F}_q$ *ist,*

(v) $X^2 \cdot G'_k(X) = k \cdot G_{k+1}(X)$ *für alle* $k \geq 0$,

(vi) $\sum_{k\geq 0} G_k(X)u^k = \frac{uX}{1-X(u-u^q)} \in \mathbb{F}_q(X,u)$, *wobei* u *eine Unbestimmte ist (Erzeugende Funktion),*

(vii) $G_k(X) = \sum_{0\leq i<j} X^{q^j-q^i}$ *falls* $k = q^j - 1$.

Beweis. Die einzelnen Eigenschaften der Goss-Polynome werden nun nacheinander bewiesen. Im Großen und Ganzen sind die Beweise recht einfach zu führen, nur die der Aussagen (*ii*) und (*vii*) gestalten sich schwieriger.

(i) Diese Aussage folgt trivial aus der rekursiven Definition der Goss-Polynome.

(ii) Um diese Eigenschaft zu beweisen, benötigen wir die Newton-Formeln. Wir setzen

$$\begin{aligned} e(z) &= z \prod_{b \in \mathbb{F}_q^*} \left(\frac{z}{b} - 1\right) \\ &= -(\prod_{b \in \mathbb{F}_q^*} b)^{-1} \prod_{b \in \mathbb{F}_q} (b - z) \\ &= z - z^q \\ &= t(z)^{-1}. \end{aligned}$$

Durch logarithmisches Differenzieren der Funktion $e(z)$ nach der Unbestimmten z und $e'(z) = 1$ ergibt sich

$$t(z) = \frac{1}{e(z)} = \frac{e'(z)}{e(z)} = dlog\,(e(z)) = dlog\left(\prod_{b \in \mathbb{F}_q} (b - z)\right) = \sum_{b \in \mathbb{F}_q} \frac{1}{z - b}. \tag{5.3}$$

Jetzt betrachten wir das Polynom

$$e(X - z) = (X - z) - (X - z)^q \in \overline{\mathbb{F}}_q(z)[X]$$

und bestimmen dessen Nullstellen. Da

$$e(X) - e(z) = (X - z) - (X - z)^q = e(X - z) = \prod_{b \in \mathbb{F}_q} (b - (X - z))$$

gilt, bilden alle Nullstellen dieser Funktion die Menge $\{z + b \mid b \in \mathbb{F}_q\}$. Die Nullstellen des „inversen Polynoms"

$$e(X^{-1} - z) \cdot X^q = \prod_{b \in \mathbb{F}_q} (b - (X^{-1} - z)) \cdot X^q = \prod_{b \in \mathbb{F}_q} ((b + z) \cdot X - 1)$$

in $\overline{\mathbb{F}}_q(z)[X]$ werden dann zu der Menge $\{\frac{1}{z+b} \mid b \in \mathbb{F}_q\}$ zusammengefaßt. Wie folgt konstruieren wir nun das Polynom $f(X) \in \mathbb{F}_q(z)[X]$, auf das die Newton-Formeln angewendet werden:

$$\begin{aligned} f(X) &:= -e(z)^{-1} \cdot e(X^{-1} - z) \cdot X^q \\ &= -t(z) \cdot e(X^{-1} - z) \cdot X^q \\ &= -t(z) \cdot (e(X^{-1}) - e(z)) \cdot X^q \\ &= -t(z) \cdot (X^{-1} - X^{-q}) \cdot X^q + t(z) \cdot e(z) \cdot X^q \\ &= X^q - t(z) X^{q-1} + t(z). \end{aligned}$$

Um die Newton-Formeln benutzen zu können, erinnern wir uns an die zu verwendenden Bezeichnungen. Es ist

$$n = q,\ a_1 = -t,\ a_2 = \ldots = a_{q-1} = 0,\ a_q = t,$$

$$\alpha_{i+1} = \frac{1}{z - i} \quad \text{mit } 0 \leq i \leq q - 1 \text{ und}$$

$$S_k = \sum_{i=1}^{q} \alpha_i^k = \sum_{a \in \mathbb{F}_q} \frac{1}{(z - a)^k}.$$

Die Behauptung folgt aufgrund von vollständiger Induktion.
Für den Induktionsanfang sei $k = 1$ und wir erhalten mit der Newton-Formel (5.1) direkt

$$S_1 = \sum_{a \in \mathbb{F}_q} \frac{1}{z-a} \overset{Gl. 5.3}{=} t(z) \overset{Def. 5.5(ii)}{=} G_1(t).$$

Im Induktionsschritt werden die Fälle $k \leq q$ und $k > q$ unterschieden. Betrachten wir zuerst den Fall $k \leq q$ und nehmen an, die Behauptung $S_l = \sum_{a \in \mathbb{F}_q} \frac{1}{(z-a)^l} = t(z)^l = G_l(t)$ sei für alle $l \in \mathbb{N}$ mit $l < k$ bereits gezeigt. Im Induktionsschritt von $k-1$ auf k gilt

$$\begin{array}{rclcl} S_k & = & \sum_{a \in \mathbb{F}_q} \frac{1}{(z-a)^k} & \overset{Gl. 5.1}{=} & t(z) \cdot S_{k-1} \\ & \overset{Ind. Ann.}{=} & t(z) \cdot G_{k-1}(t) & \overset{Def. 5.5(iii), k \leq q}{=} & G_k(t). \end{array}$$

Im Fall $k > q$ sei die Aussage

$$S_l = \sum_{a \in \mathbb{F}_q} \frac{1}{(z-a)^l} = t \cdot S_{l-1} - t \cdot S_{l-q} = t \cdot (G_{l-1}(t) - G_{l-q}(t)) = G_l(t)$$

für alle $l \in \mathbb{N}$ mit $l < k$ bewiesen. Für k gilt nun

$$\begin{array}{rclcl} S_k & = & \sum_{a \in \mathbb{F}_q} \frac{1}{(z-a)^k} & \overset{Gl. 5.2}{=} & t \cdot S_{k-1} - t \cdot S_{k-q} \\ & = & t \cdot (G_{k-1}(t) - G_{k-q}(t)) & \overset{Def. 5.5(iii)}{=} & G_k(t). \end{array}$$

Somit ist diese Aussage bewiesen.

(iii) Diese Behauptung folgt wie (i) unmittelbar aus der rekursiven Definition.

(iv) Die Charakteristik des Körpers $\mathbb{F}_q$ ist p und es gilt für die auf Ω surjektive Modulform $t(z) \in M_{q+1,1}(\Gamma)$

$$\begin{array}{rclcl} G_{pk}(t(z)) & = & \sum_{a \in \mathbb{F}_q} \frac{1}{(z-a)^{pk}} & = & \sum_{a \in \mathbb{F}_q} \left(\frac{1}{(z-a)^k}\right)^p \\ & = & \left(\sum_{a \in \mathbb{F}_q} \frac{1}{(z-a)^k}\right)^p & = & (G_k(t(z)))^p. \end{array}$$

Aufgrund der obigen Überlegungen stimmen die beiden Goss-Polynome vom Grad pk in unendlich vielen Punkten, nämlich dem Bildbereich von t, überein. Damit folgt die Aussage.

(v) Auch diese Aussage wird mittels vollständiger Induktion bewiesen. Für den Induktionsanfang sei $k = 0$ und es gilt $X^2 \cdot G'_k = k \cdot G_{k+1}$ offensichtlich.
Für die Induktionsannahme sei

$$X^2 \cdot G'_l = l \cdot G_{l+1}$$

für alle $l \in \mathbb{N}_0$ mit $l < k$ bewiesen und es wird gezeigt, daß diese dann auch für $l = k$ gilt. Dies ergibt sich mit

$$\begin{aligned}
X^2 \cdot G'_k &= X^2 \cdot \frac{d}{dX}(X \cdot (G_{k-1} - G_{k-q})) \\
&= X^2 \cdot (G_{k-1} - G_{k-q}) + X^3 \cdot (G'_{k-1} - G'_{k-q}) \\
&= X \cdot X(G_{k-1} - G_{k-q}) + X(X^2 G'_{k-1} - X^2 G'_{k-q}) \\
&\overset{Def. 5.5(iii)}{=} X \cdot G_k + X \cdot (X^2 G'_{k-1} - X^2 G'_{k-q}) \\
&\overset{Ind.Ann.}{=} X \cdot (G_k + (k-1) \cdot G_k - (k-q) \cdot G_{k+1-q}) \\
&= k \cdot X \cdot (G_k - G_{k+1-q}) \\
&= k \cdot G_{k+1}.
\end{aligned}$$

(vi) Um zu beweisen, daß für die erzeugende Funktion

$$\sum_{k \geq 0} G_k(X) u^k = \frac{uX}{1 - X(u - u^q)}$$

gilt, wird $G(X, u) := \sum_{k \geq 0} G_k(X) u^k$ gesetzt. Aufgrund von

$$\begin{aligned}
G(X, u) - uX &= \sum_{k \geq 0} G_k(X) u^k - uX \\
&= \sum_{k \geq 2} u^k \cdot (X(G_{k-1}(X) - G_{k-q}(X))) \\
&= X \cdot \left(u \sum_{k \geq 2} u^{k-1} G_{k-1}(X) - u^q \sum_{k \geq 2} u^{k-q} G_{k-q}(X) \right) \\
&= X \cdot \left(u \sum_{k \geq 0} u^k G_k(X) - u^q \sum_{k \geq 0} u^k G_k(X) \right) \\
&= X \cdot (u - u^q) \cdot G(X, u)
\end{aligned}$$

ergibt sich durch Auflösen der Gleichung

$$G(X, u) - uX = X \cdot (u - u^q) \cdot G(X, u)$$

nach $G(X, u)$ die Behauptung.

(vii) Die letzte Eigenschaft der Goss-Polynome zu zeigen, ist nicht ganz einfach und erfordert ein wenig Aufwand. Zu Beginn wird

$$\begin{aligned}
P(X) &:= G_k(X^{-1}) X^{k+1} \quad \text{und} \\
Q(X) &:= \sum_{0 \leq i < j} X^{q^i}
\end{aligned}$$

gesetzt. Aufgrund der folgenden Überlegungen

$$\begin{array}{rrcl} & P(X) & = & Q(X) \\ \Leftrightarrow & G_{q^j-1}(X^{-1}) \cdot X^{q^j} & = & \sum_{0\le i<j} X^{q^i} \\ \Leftrightarrow & G_{q^j-1}(X^{-1}) & = & X^{-q^j} \sum_{0\le i<j} X^{q^i} \\ \Leftrightarrow & G_k(X^{-1}) & = & \sum_{0\le i<j} X^{q^i-q^j} \\ \Leftrightarrow & G_k(X) & = & \sum_{0\le i<j} X^{q^j-q^i} \end{array}$$

ist es ausreichend, die Gleichheit von $P(X)$ und $Q(X)$ zu zeigen. Betrachten wir zunächst das Polynom $Q(X) = \sum_{0\le i<j} X^{q^i}$.
Die Funktion $e(z) = z - z^q$ eingesetzt in $Q(X)$ ergibt

$$Q(e(z)) = \sum_{0\le i<j} (z - z^q)^{q^i} = z - z^{q^j}. \tag{5.4}$$

Als nächstes wenden wir uns der Funktion $P(X) = G_k(X^{-1}) \cdot X^{k+1}$ zu und werten diese für $e(z) = z - z^q$ aus. Mit $e^{-1}(z) = t(z)$ ergibt sich

$$\begin{aligned} P(e(z)) &= G_{q^j-1}(e^{-1}(z)) \cdot e^{q^j}(z) \\ &= G_{q^j-1}(t(z)) \cdot e^{q^j}(z) \\ &= \sum_{a\in\mathbb{F}_q} \frac{1}{(z-a)^{q^j-1}} \cdot (z-z^q)^{q^j} \\ &= \sum_{a\in\mathbb{F}_q} \frac{1}{(z-a)^{q^j-1}} \cdot (-1)^{q^j} \prod_{b\in\mathbb{F}_q} (z-b)^{q^j}. \end{aligned}$$

Formen wir diese Gleichung weiter um, so erhalten wir

$$\begin{aligned} P(e(z)) &= \sum_{a\in\mathbb{F}_q} (z-a)^{1-q^j} \cdot (-1)^{q^j} \prod_{b\in\mathbb{F}_q} (z-b)^{q^j} \\ &= (-1)^{q^j} \sum_{a\in\mathbb{F}_q} (z-a)(z-a)^{-q^j} \cdot \prod_{b\in\mathbb{F}_q} (z-b)^{q^j} \\ &= (-1)^{q^j} \sum_{a\in\mathbb{F}_q} (z-a) \prod_{b\in\mathbb{F}_q, b\neq a} (z-b)^{q^j} \\ &= (-1)^{q^j} \sum_{a\in\mathbb{F}_q} (z-a) \prod_{b\in\mathbb{F}_q, b\neq a} (z^{q^j}-b). \end{aligned}$$

Nun wird die Summe aufgespalten und es folgt

$$\begin{aligned} P(e(z)) &= (-1)^{q^j} \sum_{a\in\mathbb{F}_q} z \prod_{b\in\mathbb{F}_q, b\neq a} (z^{q^j} - b) \\ &\quad -(-1)^{q^j} \sum_{a\in\mathbb{F}_q} a \prod_{b\in\mathbb{F}_q, b\neq a} (z^{q^j} - b) \\ &= (-1)^{q^j} z \sum_{a\in\mathbb{F}_q} \prod_{b\in\mathbb{F}_q, b\neq a} (z^{q^j} - b) \\ &\quad -(-1)^{q^j} \sum_{a\in\mathbb{F}_q^*} a \prod_{b\in\mathbb{F}_q, b\neq a} (z^{q^j} - b) \\ &= (-1)^{q^j} z \sum_{a\in\mathbb{F}_q} \prod_{b\in\mathbb{F}_q, b\neq a} (z^{q^j} - b) \\ &\quad -(-1)^{q^j} z^{q^j} \sum_{a\in\mathbb{F}_q^*} a \prod_{b\in\mathbb{F}_q^*, b\neq a} (z^{q^j} - b). \end{aligned} \tag{5.5}$$

Betrachten wir die Gleichungen (5.4) und (5.5), so ist offensichtlich, daß $P(X) = Q(X)$ dann gilt, wenn

$$\sum_{a\in\mathbb{F}_q} \prod_{b\in\mathbb{F}_q, b\neq a} (z^{q^j} - b) = (-1)^{q^j} \text{ und } \sum_{a\in\mathbb{F}_q^*} a \prod_{b\in\mathbb{F}_q^*, b\neq a} (z^{q^j} - b) = (-1)^{q^j}$$

ist. Mit den beiden Aussagen des Lemmas (5.3) folgt die Behauptung.

□

Neben der Möglichkeit, Goss-Polynome über die rekursive Definition zu bestimmen, können diese auch mit Hilfe des folgenden Satzes dargestellt werden.

Satz 5.7. *Es sei $G_{k+1}(X) \in \mathbb{F}_q[X]$ das $(k+1)$-te Goss-Polynom vom Grad $k+1$. Dann gilt*

$$G_{k+1}(X) = \sum_{0\leq i\leq \frac{k}{q}} \binom{k - i(q-1)}{i} (-1)^i \cdot X^{k-i(q-1)+1}.$$

Beweis. Um diesen Satz zu beweisen, wird die erzeugende Funktion aus Satz 5.6(*vi*)

$$G(X,u) = \sum_{k\geq 0} G_k(X) u^k = \frac{uX}{1 - X(u - u^q)} \in \mathbb{F}_q(X,u)$$

verwendet, wobei diese durch die geometrische Reihe dargestellt wird. Es ergibt sich

$$
\begin{aligned}
G(X,u) &= \frac{uX}{1-X(u-u^q)} \\
&= uX\cdot\sum_{j\geq 0}(X\cdot(u-u^q))^j \\
&= uX\cdot\sum_{j\geq 0}X^j\cdot\sum_{i=0}^{j}\binom{j}{i}u^{j-i}\cdot(-u^q)^i \\
&= uX\cdot\sum_{j\geq 0}\sum_{i\geq 0}(-1)^i\binom{j}{i}X^j\cdot u^{j-i+qi} \\
&\overset{k:=j-i+qi}{=} uX\cdot\sum_{i=0}^{\infty}\sum_{k=qi-i}^{\infty}(-1)^i\binom{k-i(q-1)}{i}X^{k-i(q-1)}\cdot u^k \\
&= uX\cdot\sum_{k\geq 0}\sum_{i\geq 0}(-1)^i\binom{k-i(q-1)}{i}X^{k-i(q-1)}\cdot u^k.
\end{aligned}
$$

Der Binomialkoeffizient für $0\leq k<qi-i$ ist identisch gleich 0. Folglich leisten die entsprechenden Summanden keinen Beitrag und die letzte Umformung ist gerechtfertigt. Da der Binomialkoeffizient $\binom{k-i(q-1)}{i}$ nur für $0\leq i\leq\frac{k}{q}$ nicht verschwindet, folgt

$$
\begin{aligned}
G(X,u) &= uX\cdot\sum_{k\geq 0}\sum_{i=0}^{\frac{k}{q}}(-1)^i\binom{k-i(q-1)}{i}X^{k-i(q-1)}\cdot u^k \\
&= \sum_{k\geq 0}\sum_{i=0}^{\frac{k}{q}}(-1)^i\binom{k-i(q-1)}{i}X^{k-i(q-1)+1}\cdot u^{k+1}.
\end{aligned}
$$

Durch Koeffizientenvergleich erhalten wir

$$
G_{k+1}(X)=\sum_{i=0}^{\frac{k}{q}}(-1)^i\binom{k-i(q-1)}{i}X^{k-i(q-1)+1}.
$$

□

5.3 Die Nullstellen von $E_k(z)$

Nach diesen Vorbereitungen wenden wir uns jetzt der Bestimmung der Nullstellen der Eisenstein-Reihen $E_k(z)=\sum'_{a,b\in\mathbb{F}_q}\frac{1}{(az+b)^k}\in M_k(\Gamma)$ zu. Dazu benötigen wir die t-Entwicklung der Eisenstein-Reihen und wie bereits angedeutet die in Kapitel 5.2 eingeführten Goss-Polynome. Das folgende Korollar liefert uns die t-Entwicklung.

Korollar 5.8. *Für die t-Entwicklung der Eisenstein-Reihen $E_k(z) \in M_k(\Gamma)$ vom Gewicht $k \equiv 0 \mod (q-1)$ gilt:*

$$E_k(z) = -(1 + G_k(t)) \in \mathbb{F}_q[t].$$

Beweis. Zuerst erinnern wir uns daran, daß nach Satz 3.9 jede Modulform eine t-Entwicklung besitzt. Weiter gilt nach Proposition 3.2 für das Gewicht der Eisenstein-Reihen $E_k(z) \in M_k(\Gamma)$ gerade $k \equiv 0 \mod (q-1)$. Aus den Umformungen

$$\begin{aligned}
E_k(z) &= \sum_{a,b \in \mathbb{F}_q}{}' \frac{1}{(az+b)^k} \\
&= \sum_{a=0, b \in \mathbb{F}_q^*} \frac{1}{(az+b)^k} + \sum_{a \in \mathbb{F}_q^*, b \in \mathbb{F}_q} \frac{1}{(az+b)^k} \\
&= \sum_{b \in \mathbb{F}_q^*} \frac{1}{b^k} + \sum_{a \in \mathbb{F}_q^*, b \in \mathbb{F}_q} \frac{1}{a^k(z+\frac{b}{a})^k} \\
&\overset{k \equiv 0 \mod (q-1)}{=} \sum_{b \in \mathbb{F}_q^*} \frac{1}{1} + \sum_{a \in \mathbb{F}_q^*} \frac{1}{a^k} \cdot \sum_{b \in \mathbb{F}_q} \frac{1}{(z+\frac{b}{a})^k} \\
&= \sum_{b \in \mathbb{F}_q^*} 1 + \sum_{a \in \mathbb{F}_q^*} \frac{1}{a^k} \cdot \sum_{b \in \mathbb{F}_q} \frac{1}{(z+b)^k} \\
&\overset{5.6(ii)}{=} (q-1) + \sum_{a \in \mathbb{F}_q^*} \frac{1}{a^k} \cdot G_k(t) \\
&= -1 + G_k(t) \sum_{a \in \mathbb{F}_q^*} \frac{1}{a^k} \\
&\overset{k \equiv 0 \mod (q-1)}{=} -1 - G_k(t)
\end{aligned}$$

folgt die Behauptung. □

Mit Hilfe der t-Entwicklung der Eisenstein-Reihen können nun die Nullstellen für einige Gewichte $k \in \mathbb{N}_0$ bestimmt werden.

Korollar 5.9. *Die Nullstellen der Eisenstein-Reihen $E_k(z) \in M_k(\Gamma)$ sind genau die Elemente von $\mathbb{F}_{q^{j+1}} - \mathbb{F}_q$, falls $k = q^j - 1$ gilt.*

Beweis. Sei $a \in \Omega$ mit $E_k(a) = 0$. Nach Korollar 5.8 lautet die t-Entwicklung der Eisenstein-Reihen

$$E_k(z) = -(1 + G_k(t)) \in \mathbb{F}_q[t].$$

Wir lösen nun die Gleichung $0 = E_k(a) = 1 + G_k(t(a))$ nach a auf und erhalten durch die folgenden Schritte

$$\begin{array}{rrcl}
 & 0 & = & 1 + G_k\left(t(a)\right) \\
\overset{k=q^j-1,\, Satz 5.6(vii)}{\Leftrightarrow} & 0 & = & \sum_{0\leq i\leq j}\left(t(a)\right)^{q^j-q^i} \\
\Leftrightarrow & 0 & = & (t(a))^{q^j}\sum_{0\leq i\leq j}(a-a^q)^{q^i} \\
\Leftrightarrow & 0 & = & \sum_{0\leq i\leq j}(a-a^q)^{q^i} \\
\Leftrightarrow & 0 & = & \sum_{0\leq i\leq j}(a^{q^i}-a^{q^{i+1}}) \\
\Leftrightarrow & 0 & = & a-a^{q^{j+1}} \\
\overset{a\in\Omega}{\Leftrightarrow} & a & \in & \mathbb{F}_{q^{j+1}}-\mathbb{F}_q
\end{array}$$

die Aussage. □

Wir kennen nun für einige bestimmte Gewichte $k \in \mathbb{N}_0$ die Nullstellen der Eisenstein-Reihen. Mit Hilfe des folgenden Korollars können wir über die Nullstellen eine weitere Aussage treffen.

Korollar 5.10. *Die Nullstellen der Eisenstein-Reihen $E_k(z) \in M_k(\Gamma)$ sind für den Fall $k = q^j - 1$ alle einfach.*

Beweis. Um zu zeigen, daß es sich bei den Nullstellen der Eisenstein-Reihen ausschließlich um einfache Nullstellen handelt, wird wieder die t-Entwicklung $E_k(z) = -(1 + G_k(t)) \in \mathbb{F}_q[t]$ nach Korollar 5.8 verwendet. Betrachten wir die erste Ableitung der Modulform $t(z) = \frac{1}{z-z^q} \in M_{q+1,1}(\Gamma)$:

$$t'(z) = -\frac{1}{(z-z^q)^2} = -(t(z))^2.$$

Differenzieren wir nun die Eisenstein-Reihen, so ergibt sich

$$\begin{array}{rcl}
E_k'(z) & = & -G_k'(t)\cdot t'(z) \\
 & \overset{Satz 5.6(v)}{=} & -k\cdot\left((G_{k+1}(t)\cdot(t(z))^{-2})\right)\cdot\left((-1)(t(z))^2\right) \\
 & = & k\cdot G_{k+1}(t) \\
 & \overset{k=q^j-1}{=} & (q^j-1)\cdot G_{q^j}(t) \\
 & = & -G_{q^j}(t) \\
 & \overset{Satz 5.6(iv)}{=} & -(G_1(t))^{q^j} \\
 & \overset{Def. 5.5(ii)}{=} & -(t(z))^{q^j}.
\end{array}$$

Da $t(z) \neq 0$ für alle $z \in \mathbb{F}_{q^{j+1}} - \mathbb{F}_q$, gilt ebenfalls $t(z)^{q^j} \neq 0$. Folglich handelt es sich bei den Nullstellen ausschließlich um einfache Nullstellen. □

In diesem Kapitel haben wir die Nullstellen der Eisenstein-Reihen für Gewichte von der Form $k = q^j - 1$ bestimmt. Interessant wäre es nun, die Nullstellen für allgemeine Gewichte zu berechnen. Dieses Problem ist leider nach wie vor ungelöst. Naheliegend ist es nun, zunächst mit Hilfe des Computers die Nullstellen für kleine k zu ermitteln.

Kapitel 6

Programm zur Bestimmung der Nullstellen von G_k und E_k

Mit Hilfe der Theorie der Modulformen über endlichen Körpern, die in den ersten Kapiteln dieser Arbeit diskutiert wurde, konnten wir schließlich in Kapitel 5 die Nullstellen der Eisenstein-Reihen

$$E_k(z) = \sum_{a,b\in\mathbb{F}_q}{}' \frac{1}{(az+b)^k} \in M_k(\Gamma)$$

für einige Gewichte $k \in \mathbb{N}_0$ bestimmen. In dem Fall $k = q^j - 1$ sind dies genau die Elemente von $\mathbb{F}_{q^{j+1}} - \mathbb{F}_q$.
Für allgemeine $k \in \mathbb{N}_0$ ist dieses Problem nach wie vor ungelöst. Um eine Idee über das Verhalten der Nullstellen für diese k zu bekommen, ist es sinnvoll, mit Hilfe des Computers für einige Gewichte die Nullstellen in $\overline{\mathbb{F}}_q$ zu berechnen. Im Rahmen dieser Arbeit wurden dazu zwei Programme implementiert: das eine berechnet die Nullstellen der Goss-Polynome $G_k(X) \in \mathbb{F}_q[X]$, das andere die der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$.
Zunächst stellen wir einige Vorüberlegungen an, die den Programmieraufwand verringern. Im Anschluß daran werden kurz die Algorithmen erläutert und einige Ergebnisse vorgestellt. Als letztes werden einige der Vermutungen über die Lage der Nullstellen der Goss-Polynome und der Eisenstein-Reihen bewiesen.

6.1 Vorüberlegungen

Im folgenden sind die wichtigsten Vereinfachungen zusammengestellt, die zur Implementierung der Algorithmen zur Bestimmung der Nullstellen der Goss-Polynome $G_k(X) \in \mathbb{F}_q[X]$ bzw. der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ benutzt werden.
Um die Nullstellen der Eisenstein-Reihen zu bestimmen, verwenden wir analog dem Korollar 5.9 die t-Entwicklung. Nach Korollar 5.8 lautet diese

$$E_k(z) = -\left(1 + G_k(t)\right) \in \mathbb{F}_q[t].$$

Es ist also notwendig, die Goss-Polynome zu erzeugen. Wir erinnern uns an die rekursive Definition 5.5 der Goss-Polynome $G_k(X) \in \mathbb{F}_q[X]$, wobei p die Charakteristik von $\mathbb{F}_q$ist:

$$\begin{aligned} G_1(X) &= X, \\ G_k(X) &= X^k \quad \text{für} \quad 1 \leq k \leq q \quad \text{und} \\ G_k(X) &= X \cdot (G_{k-1}(X) - G_{k-q}(X)) \quad \text{für} \quad k > q. \end{aligned}$$

Damit folgt direkt $G_k(X) \in \mathbb{F}_p[X]$ für alle $k \geq 1$, d.h. wir betrachten die $G_k(X)$ über dem Primkörper $\mathbb{F}_p$ und benötigen nicht den Erweiterungskörper $\mathbb{F}_q$.

Werden die Goss-Polynome $G_k(X) \in \mathbb{F}_p[X]$ über die rekursive Definition 5.5 ermittelt, müssen viele $G_k(X)$ berechnet werden und es wird zu viel Speicherplatz benötigt. Deswegen werden die $G_k(X)$ mit Hilfe von Satz 5.7 bestimmt:

$$G_{k+1}(X) = \sum_{0 \leq i \leq \frac{k}{q}} \binom{k - i(q-1)}{i} (-1)^i \cdot X^{k-i(q-1)+1}.$$

Wie wir in der Beschreibung der Algorithmen sehen werden, zerlegt das Programm die Polynome $G_k(X) \in \mathbb{F}_p[X]$ und $E_k(t) \in \mathbb{F}_p[t]$ in irreduzible Faktoren. Das folgende Lemma macht klar, daß zwei verschiedene irreduzible Faktoren eines Polynoms keine gemeinsame Nullstellen besitzen.

Lemma 6.1. *Es sei K ein beliebiger Körper. Dann besitzen zwei irreduzible Faktoren eines Polynoms $f \in K[X]$ keine gemeinsamen Nullstellen in $\overline{K}$.*

Beweis. Es sei $f \in K[X]$ ein Polynom mit der Zerlegung

$$f(X) = \prod_{n=1}^{l} f_n(X) \in K[X]$$

in irreduzible Faktoren $f_n \in K[X]$ mit $1 \leq n \leq l$. Weiter sei L eine Körpererweiterung von K und es gelte $z \in L - K$ mit $f_i(z) = f_j(z) = 0$ für $1 \leq i, j \leq l$ und $i \neq j$. Folglich existieren zwei Minimalpolynome von $z \in L$ über K. Da ein Minimalpolynom eindeutig bestimmt ist, ist dies ein Widerspruch zu der Annahme $f_i(z) = f_j(z) = 0$. $\square$

6.2 Der Algorithmus

Wie schon angedeutet, wurden zwei Programme mit Hilfe des Computeralgebrasystems SIMATH implementiert: das eine berechnet die Nullstellen der Goss-Polynome $G_k(X) \in \mathbb{F}_p[X]$ und das zweite die Nullstellen der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$. Es werden die Nullstellen nicht explizit bestimmt, sondern es wird jeweils die Anzahl der Nullstellen, die in einen Erweiterungskörper $\mathbb{F}_{q^n}$ $(n \in \mathbb{N})$ von $\mathbb{F}_q$ liegen, ermittelt. Im folgenden sind in aller

Kürze die Vorgehensweisen der beiden Algorithmen beschrieben.

Die Bestimmung der Nullstellen der Goss-Polynome:
Die Goss-Polynome $G_k(X) \in \mathbb{F}_p[X]$ werden erzeugt und durch eine SIMATH-Funktion in irreduzible Faktoren zerlegt:

$$G_k(X) = f_1(X)^{e_1} \cdot f_2(X)^{e_2} \cdot \ldots \cdot f_j(X)^{e_j} \in \mathbb{F}_p[X],$$

wobei $f_i(X) \in \mathbb{F}_p[X]$ irreduzible Polynome vom Grad d_i für $1 \leq i \leq j$ sind, die mit den Exponenten e_i auftreten. Es werden nicht explizit die einzelnen Nullstellen ermittelt, sondern es wird die Anzahl (n) der irreduziblen Faktoren vom Grad (d), die mit dem Exponenten (e) auftreten, bestimmt.
Es ist offensichtlich, daß die Goss-Polynome neben einer meist mehrfachen Nullstelle in $X = 0$ weitere Nullstellen in dem Primkörper $\mathbb{F}_p$ besitzen können.

Die Bestimmung der Nullstellen der Eisenstein-Reihen:
Um die t-Entwicklung der Eisenstein-Reihen

$$E_k(z) = -\left(1 + G_k(t)\right) \in \mathbb{F}_p[t]$$

zu ermitteln, werden zunächst die Goss-Polynome $G_k(t) \in \mathbb{F}_p[t]$ berechnet. Anschließend werden die Eisenstein-Reihen als Polynome in t faktorisiert. Diese irreduziblen Faktoren in $t(z) = \frac{1}{z-z^q}$ werden als nächstes in Faktoren in der Unbestimmten z umgerechnet. Wiederum wird die Anzahl (n) der irreduziblen Faktoren vom Grad (d), die mit dem Exponenten (e) auftreten, angegeben.
Die Eisenstein-Reihen besitzen keine Nullstellen in $\mathbb{F}_q$, sondern nur in verschiedenen Erweiterungskörpern von $\mathbb{F}_q$.

Die Nullstellen sollen in Abhängigkeit des Grads k der Goss-Polynome bzw. des Gewichts k der Eisenstein-Reihen berechnet werden. Daher werden p und $q = p^s$ fest gewählt und mit Hilfe einer Schleife über k wird die jeweilige Anzahl der Nullstellen in den verschiedenen Erweiterungskörpern berechnet. Um ein mögliches Muster in dem Verhalten der Nullstellen leichter in einen Zusammenhang mit k bringen zu können, wird k in der p-adischen Entwicklung

$$k = \sum_{i=0}^{n} a_i \cdot p^i =: (a_0, a_1, \ldots, a_n)$$

mit $n, a_i \in \mathbb{N}_0$, $a_n \neq 0$ und $0 \leq a_i < p$ für $0 \leq i \leq n$ ausgegeben.

6.3 Ergebnisse

In diesem Abschnitt sind exemplarisch einige Ergebnisse zusammengestellt. Sowohl die Nullstellen der Goss-Polynome $G_k(X) \in \mathbb{F}_p[X]$ als auch die Nullstellen der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ sind für $p = q$ und den Parameter

k mit $1 \leq k \leq 100$ berechnet worden. In den Tabellen wird k in der p-adischen Darstellung ausgegeben. Die Nullstellen, die in den Erweiterungskörpern liegen, werden wie bereits beschrieben jeweils in Form von Tupeln mit drei Elementen (n, d, e) angegeben, wobei n die Anzahl der irreduziblen Faktoren vom Grad d ist, die mit dem Exponenten e auftreten. In dem Fall der Nullstellenbestimmung der Goss-Polynome wird ferner die Vielfachheit der Nullstelle in $X = 0$ ausgegeben.
In den ersten beiden Tabellen sind die Nullstellen der Goss-Polynome für $p = q = 2$ bzw. für $p = q = 3$ dargestellt. In der dritten bzw. in der vierten Tabelle sind die Nullstellen der Eisenstein-Reihen für $p = q = 2$ bzw. für $p = q = 3$ zu finden.
Im nächsten Abschnitt sind Beobachtungen bezüglich der Nullstellen der Goss-Polynome und der Eisenstein-Reihen zusammengestellt. Einige von ihnen wurden bereits in Kapitel 5 gezeigt, die übrigen werden wir im Anschluß beweisen.

6.3.1 Beobachtungen

Im folgenden sind die Vermutungen über die Nullstellen der Goss-Polynome $G_k(X) \in \mathbb{F}_p[X]$ und der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ übersichtlich aufgelistet. Die meisten Vermutungen sind direkt für $q = p^s$ formuliert. Auffällig ist, daß sowohl die Goss-Polynome als auch die Eisenstein-Reihen sehr stark faktorisieren.
Aus den ersten beiden Tabellen kann für die Nullstellen der Goss-Polynome $G_k(X) \in \mathbb{F}_p[X]$ entnommen werden:

(i) Die Goss-Polynome besitzen in $X = 0$ eine mindestens $[\frac{k}{q}]$-fache Nullstelle.

(ii) Falls der Grad k der Goss-Polynome von der Form $k = a \cdot p^n$ mit $0 < a \leq q$ ist, liegt in $X = 0$ eine k-fache Nullstelle vor.

(iii) Für die Goss-Polynome $G_k(X) \in \mathbb{F}_q[X]$ gilt

$$G_{pk}(X) = (G_k(X))^p \, .$$

Die Beobachtung (ii) ist eine unmittelbare Folge aus Satz 5.6(iii) und 5.6(iv) und (iii) ist die Aussage von 5.6(iv). Lediglich die Vermutung (i) werden wir im nächsten Abschnitt beweisen.

Wenden wir uns nun den Tabellen zu, in denen die Nullstellen der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ dargestellt sind. Anhand dieser Tabellen läßt sich folgendes feststellen:

(i) Die Nullstellen der Eisenstein-Reihe $E_{q^j-1}(z)$ liegen in $\mathbb{F}_{q^{j+1}} - \mathbb{F}_q$ und sind einfach.

(ii) Die Nullstellen der Eisenstein-Reihe vom Gewicht $q-1$ sind die elliptischen Punkte und sie sind einfach.

(iii) Die Eisenstein-Reihe $E_k(z) \in \mathbb{F}_q(z)$ vom Gewicht k besitzt genau $q \cdot k$ Nullstellen $z \in \Omega$ gezählt mit Vielfachheiten.

(iv) Ist ein elliptischer Punkt $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ eine Nullstelle der Eisenstein-Reihen E_k, so sind alle elliptischen Punkte Nullstellen von E_k.

(v) Sei $k \in \mathbb{N}_0$ beliebig. Ist ein Element aus $\mathbb{F}_{q^3} - \mathbb{F}_q$ Nullstelle von E_k, so sind alle Elemente aus $\mathbb{F}_{q^3} - \mathbb{F}_q$ Nullstellen.

(vi) Für alle $k \in \mathbb{N}_0$ gilt

$$E_{pk}(z) = (E_k(z))^p .$$

(vii) Wenn j ungerade ist, besitzt die Eisenstein-Reihe $E_{q^j-1}(z) \in \mathbb{F}_q(z)$ in den elliptischen Punkten Nullstellen.

(viii) Die Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ vom Gewicht $k \equiv 0 \mod (q^2-1)$ besitzen in den elliptischen Punkten keine Nullstellen.

(ix) Sei $1 \leq a \leq q$. Dann gilt für die Nullstellenordnung der Eisenstein-Reihe vom Gewicht $a \cdot (q-1)$ in $x \in \Omega$:

$$\nu_x(E_{a\cdot(q-1)}) = a \cdot \nu_x(E_{q-1}).$$

Die Aussagen (i) und (ii) wurden schon in Korollar 5.9 und Korollar 5.10 bewiesen, (iv) folgt sofort aus der Invarianz von $\nu_z(f)$ unter Γ und (vi) aus der in Charakteristik p geltenden Gleichung $(X+Y)^p = X^p + Y^p$.
Die übrigen Vermutungen werden im nächsten Abschnitt bewiesen.

6.3.2 Aussagen

Die im Verlauf des vorangegangenen Abschnitts aufgestellten Vermutungen, die nicht schon bewiesen sind, werden wir nun zeigen. Dabei wird im wesentlichen auf die Sätze und Definitionen aus Kapitel 5.2 zurückgegriffen. Beginnen wir mit der Aussage (i), die die Nullstellen der Goss-Polynome $G_k(X) \in \mathbb{F}_q[X]$ betrifft.

Proposition 6.2. *Sei $G_k(X) \in \mathbb{F}_p[X]$ das k-te Goss-Polynom. Dann gilt für die Nullstellenordnung in $X = 0$*

$$\mu_0\left(G_k(X)\right) \geq \left[\frac{k}{q}\right].$$

Beweis. Wir betrachten für $G_k(X) \in \mathbb{F}_p[X]$ die beiden Fälle $1 \leq k \leq q$ und $k \geq q$.
Für den Fall $1 \leq k \leq q$ folgt für die Nullstellenordnung

$$\mu_0\left(G_k(X)\right) \overset{Satz\,5.6(iii)}{=} \mu_0(X^k) = k \geq \left[\frac{k}{q}\right].$$

Den Fall $k \geq q$ beweisen wir durch vollständige Induktion. Der Induktionsanfang ist $k = q$ und mit dem ersten Fall gezeigt. Für die Induktionsannahme sei die Behauptung $\mu_0\left(G_l(X)\right) \geq \left[\frac{l}{q}\right]$ für alle $l < k$ bereits bewiesen. Im Induktionsschluß folgt

$$\begin{aligned}
\mu_0\left(G_k(X)\right) &\overset{Def.\,5.5}{=} \mu_0(X) + \mu_0\left(G_{k-1}(X) - G_{k-q}(X)\right) \\
&\geq 1 + min\{\mu_0\left(G_{k-1}(X)\right), \mu_0\left(G_{k-q}(X)\right)\} \\
&\overset{Ind.Ann}{\geq} 1 + \left[\frac{k-q}{q}\right] \\
&= \left[\frac{k}{q}\right].
\end{aligned}$$

Für die Abschätzung der Nullstellenordnung benutzten wir die Rechenregeln für Bewertungen (vgl. Seite 36). □

Als nächstes wenden wir uns den Nullstellen der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ zu.

Proposition 6.3. *Die Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ vom Grad k besitzen genau $q \cdot k$ Nullstellen gezählt mit Vielfachheiten.*

Beweis. Es seien $E_k(z) \in \mathbb{F}_q(z)$ die Eisenstein-Reihe vom Gewicht k und $G_k(X) = \sum_{i=j}^{k} a_i X^i$ das k-te Goss-Polynom mit $a_j \neq 0$. Aus der Definition der Goss-Polynome folgt direkt, daß $a_k \neq 0$ und $j \geq 1$ ist. Dann gilt:

$$\begin{aligned}
E_k(z) &\overset{Kor.\,5.8}{=} -\left(1 + G_k(t)\right) \\
&= -\left(1 + \sum_{i=j}^{k} a_i \frac{1}{(z - z^q)^i}\right) \\
&= -\frac{1}{(z-z^q)^k} \cdot \left((z-z^q)^k + \sum_{i=j}^{k} a_i (z-z^q)^{k-i}\right) \\
&= -\frac{1}{(z-z^q)^k} \cdot \left((z-z^q)^k + \sum_{i=j}^{k-1} a_i (z-z^q)^{k-i} + a_k\right).
\end{aligned}$$

Die Nullstellen des Nenners sind die Elemente aus $\mathbb{F}_q$. Da $j \geq 1$ und $a_k \neq 0$ ist, liegen die Nullstellen des Zählers in $\Omega = \overline{\mathbb{F}}_q - \mathbb{F}_q$. Folglich sind Zähler und Nenner der Eisenstein-Reihen teilerfremd. Also ist die Anzahl der Nullstellen von $E_k(z)$ gezählt mit Vielfachheiten gleich dem Grad des Zählers gleich $q \cdot k$. □

Proposition 6.4. *Sei $E_k(z) \in \mathbb{F}_q(z)$ die Eisenstein-Reihe vom Gewicht k.*

(i) Ist ein elliptischer Punkt Nullstelle der Eisenstein-Reihe, so sind alle elliptischen Punkte Nullstellen der Eisenstein-Reihe.

(ii) Wenn ein Punkt $x \in \mathbb{F}_{q^3} - \mathbb{F}_q$ eine Nullstelle der Eisenstein-Reihe ist, dann sind alle $x \in \mathbb{F}_{q^3} - \mathbb{F}_q$ Nullstellen.

Beweis. (i) Diese Behauptung wurde bereits bewiesen.

(ii) Sei $x \in \mathbb{F}_{q^3} - \mathbb{F}_q$ und $E_k(x) = 0$. Für den Stabilisator von $x \in \mathbb{F}_{q^3} - \mathbb{F}_q$ gilt

$$\Gamma_x = \left\{ \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix} \mid a \in \mathbb{F}_q^* \right\},$$

so daß wir mit Hilfe der Bahnengleichung

$$\#\Gamma \cdot x = \frac{\#\Gamma}{\#\Gamma_x} = \frac{(q-1)^2 q(q+1)}{q-1} = q^3 - q = \#(\mathbb{F}_{q^3} - \mathbb{F}_q)$$

gerade $\Gamma \cdot x = \mathbb{F}_{q^3} - \mathbb{F}_q$ erhalten. Für ein beliebiges $y = \gamma \cdot x$ aus $\mathbb{F}_{q^3} - \mathbb{F}_q$ gilt also

$$E_k(y) = E_k(\gamma \cdot x) = (cx + d)^k \cdot E_k(x) = 0.$$

□

Proposition 6.5. *Es sei $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ eine Nullstelle der Eisenstein-Reihe $E_{q^j-1}(z) \in \mathbb{F}_q(z)$. Wenn j ungerade ist, besitzt $E_{q^j-1}(z)$ in allen elliptischen Punkten Nullstellen.*

Beweis. Für die Eisenstein-Reihe $E_{q^j-1}(z) \in \mathbb{F}_q(z)$ mit $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ und $E_{q^j-1}(e) = 0$ ergibt sich mit den folgenden Äquivalenzumformungen die Behauptung:

$$\begin{aligned} & E_{q^j-1}(e) = 0 \\ \overset{Kor.5.9}{\Leftrightarrow} \quad & e \in \mathbb{F}_{q^{j+1}} - \mathbb{F}_q \\ \Leftrightarrow \quad & j \equiv 1 \mod 2. \end{aligned}$$

□

Proposition 6.6. *Genau die Eisenstein-Reihe $E_k(z)$ vom Gewicht $k \equiv 0 \mod (q^2-1)$ besitzt in den elliptischen Punkten keine Nullstellen.*

Beweis. Sei $E_k(z) \in \mathbb{F}_q(z)$ die Eisenstein-Reihe vom Gewicht k. Weiter sei $e \in \mathbb{F}_{q^2} - \mathbb{F}_q$ ein elliptischer Punkt und $E_k(e) \neq 0$.
Wegen Proposition 6.4 sei o.B.d.A. $< e >= \mathbb{F}_{q^2}^*$. Es habe e über $\mathbb{F}_q$ das Minimalpolynom $x^2 + ux + v$. Wir wählen nun $\gamma := \begin{pmatrix} -u & -v \\ 1 & 0 \end{pmatrix} \in \Gamma$. Folglich gilt $\gamma \in \Gamma_e$ und

$$E_k(e) = E_k(\gamma e) = e^k \cdot E_k(e).$$

Aus $E_k(e) \neq 0$ folgt $1 = e^k$, d.h. mit $< e >= \mathbb{F}_{q^2}^*$ gilt $k \equiv 0 \mod (q^2-1)$. Sei nun $e \in \mathbb{F}_{q^2} - F_q$ ein elliptischer Punkt und $k \equiv 0 \mod (q^2-1)$. Dann existiert eine natürliche Zahl $n \in \mathbb{N}_0$ mit $k = n \cdot (q^2-1)$. Es ergibt sich

$$\begin{aligned}
E_k(e) &= \sum_{a,b\in\mathbb{F}_q}{}' \frac{1}{(ae+b)^k} \\
&= \sum_{a,b\in\mathbb{F}_q}{}' \frac{1}{((ae+b)^{q^2-1})^n} \\
&\overset{e\in\mathbb{F}_{q^2}-F_q}{=} \sum_{a,b\in\mathbb{F}_q}{}' \frac{1}{1^n} \\
&= q^2-1 \\
&= -1.
\end{aligned}$$

□

Proposition 6.7. *Sei $E_{q-1}(z) \in \mathbb{F}_q(z)$ eine Eisenstein-Reihen und $1 \leq a \leq q$. Dann gilt für die Nullstellenordnung der Eisenstein-Reihen vom Gewicht $a \cdot (q-1)$ in $x \in \Omega$*

$$\nu_x(E_{a\cdot(q-1)}) = a \cdot \nu_x(E_{q-1}).$$

Beweis. Sei $1 \leq a \leq q$. Damit lautet die Dimension des $\overline{\mathbb{F}}_q$-Vektorraums $M_{a\cdot(q-1)}(\Gamma)$

$$dim_{\overline{\mathbb{F}}_q} M_{a\cdot(q-1)} = [\frac{a\cdot(q-1)}{q^2-1} - \frac{0}{q-1}] + 1 = 1.$$

Da die beiden Eisenstein-Reihen $E_{a\cdot(q-1)}$ und $(E_{q-1})^a$ in $M_{a\cdot(q-1)}(\Gamma)$ liegen, existiert ein $c \in \overline{\mathbb{F}}_q$ mit

$$E_{a\cdot(q-1)} = c \cdot (E_{q-1})^a.$$

Somit ergibt sich für die Nullstellenordnung von $x \in \Omega$

$$\begin{aligned}
\nu_x\left(E_{a\cdot(q-1)}\right) &= \nu_x\left(c\cdot(E_{q-1})^a\right) \\
&= \nu_x\left((E_{q-1})^a\right) \\
&= a\cdot\nu_x(E_{q-1}).
\end{aligned}$$

□

Leider konnte für allgemeine Gewichte k keine Regelmäßigkeit in dem Verhalten der Nullstellen festgestellt werden: Es war anhand der Daten nicht möglich, einen Zusammenhang zwischen der p-adischen Entwicklung des Gewichts k und den Erweiterungskörpern $\mathbb{F}_{q^n}$, in denen die Nullstellen liegen, herzustellen. Das Problem der Bestimmung der Nullstellen der Eisenstein-Reihen $E_k(z) \in \mathbb{F}_q(z)$ bleibt weiterhin ungelöst.

Die Nullstellen der Goss-Polynome für $p = q = 2$ und $1 \leq k \leq 100$

k	p-adische Entw.	(n,d,e)	X=0
1	(1)		1
2	(0,1)		2
3	(1,1)	(1,1,1)	2
4	(0,0,1)		4
5	(1,0,1)	(1,2,1)	3
6	(0,1,1)	(1,1,2)	4
7	(1,1,1)	(1,3,1)	4
8	(0,0,0,1)		8
9	(1,0,0,1)	(1,1,1),(1,3,1)	5
10	(0,1,0,1)	(1,2,2)	6
11	(1,1,0,1)	(1,5,1)	6
12	(0,0,1,1)	(1,1,4)	8
13	(1,0,1,1)	(1,6,1)	7
14	(0,1,1,1)	(1,3,2)	8
15	(1,1,1,1)	(1,1,1),(1,2,1),(1,4,1)	8
16	(0,0,0,0,1)		16
17	(1,0,0,0,1)	(2,4,1)	9
18	(0,1,0,0,1)	(1,1,2),(1,3,2)	10
19	(1,1,0,0,1)	(1,9,1)	10
20	(0,0,1,0,1)	(1,2,4)	12
21	(1,0,1,0,1)	(1,1,1),(1,3,1),(1,6,1)	11
22	(0,1,1,0,1)	(1,5,2)	12
23	(1,1,1,0,1)	(1,11,1)	12
24	(0,0,0,1,1)	(1,1,8)	16
25	(1,0,0,1,1)	(1,2,1),(1,10,1)	13
26	(0,1,0,1,1)	(1,6,2)	14
27	(1,1,0,1,1)	(1,1,1),(1,3,1),(1,9,1)	14
28	(0,0,1,1,1)	(1,3,4)	16
29	(1,0,1,1,1)	(1,14,1)	15
30	(0,1,1,1,1)	(1,1,2),(1,2,2),(1,4,2)	16
31	(1,1,1,1,1)	(3,5,1)	16
32	(0,0,0,0,0,1)		32
33	(1,0,0,0,0,1)	(1,1,1),(3,5,1)	17
34	(0,1,0,0,0,1)	(2,4,2)	18
35	(1,1,0,0,0,1)	(1,2,1),(1,3,1),(1,12,1)	18

k	p-adische Entw.	(n,d,e)	X=0
36	(0,0,1,0,0,1)	(1,1,4),(1,3,4)	20
37	(1,0,1,0,0,1)	(1,18,1)	19
38	(0,1,1,0,0,1)	(1,9,2)	20
39	(1,1,1,0,0,1)	(1,1,1),(1,6,1),(1,12,1)	20
40	(0,0,0,1,0,1)	(1,2,8)	24
41	(1,0,0,1,0,1)	(2,10,1)	21
42	(0,1,0,1,0,1)	(1,1,2),(1,3,2),(1,6,2)	22
43	(1,1,0,1,0,1)	(3,7,1)	22
44	(0,0,1,1,0,1)	(1,5,4)	24
45	(1,0,1,1,0,1)	(1,1,1),(1,2,1),(1,3,1),(1,4,1),(1,12,1)	23
46	(0,1,1,1,0,1)	(1,11,2)	24
47	(1,1,1,1,0,1)	(1,23,1)	24
48	(0,0,0,0,1,1)	(1,1,16)	32
49	(1,0,0,0,1,1)	(1,3,1),(1,21,1)	25
50	(0,1,0,0,1,1)	(1,2,2),(1,10,2)	26
51	(1,1,0,0,1,1)	(1,1,1),(2,4,1),(2,8,1)	26
52	(0,0,1,0,1,1)	(1,6,4)	28
53	(1,0,1,0,1,1)	(1,26,1)	27
54	(0,1,1,0,1,1)	(1,1,2),(1,3,2),(1,9,2)	28
55	(1,1,1,0,1,1)	(1,2,1),(1,5,1),(1,20,1)	28
56	(0,0,0,1,1,1)	(1,3,8)	32
57	(1,0,0,1,1,1)	(1,1,1),(3,9,1)	29
58	(0,1,0,1,1,1)	(1,14,2)	30
59	(1,1,0,1,1,1)	(1,29,1)	30
60	(0,0,1,1,1,1)	(1,1,4),(1,2,4),(1,4,4)	32
61	(1,0,1,1,1,1)	(1,30,1)	31
62	(0,1,1,1,1,1)	(3,5,2)	32
63	(1,1,1,1,1,1)	(1,1,1),(2,3,1),(4,6,1)	32
64	(0,0,0,0,0,0,1)		64
65	(1,0,0,0,0,0,1)	(1,2,1),(5,6,1)	33
66	(0,1,0,0,0,0,1)	(1,1,2),(3,5,2)	34
67	(1,1,0,0,0,0,1)	(1,33,1)	34
68	(0,0,1,0,0,0,1)	(2,4,4)	36
69	(1,0,1,0,0,0,1)	(1,1,1),(1,11,1),(1,22,1)	35
70	(0,1,1,0,0,0,1)	(1,2,2),(1,3,2),(1,12,2)	36

k	p-adische Entw.	(n,d,e)	X=0
71	(1,1,1,0,0,0,1)	(1,35,1)	36
72	(0,0,0,1,0,0,1)	(1,1,8),(1,3,8)	40
73	(1,0,0,1,0,0,1)	(4,9,1)	37
74	(0,1,0,1,0,0,1)	(1,18,2)	38
75	(1,1,0,1,0,0,1)	(1,1,1),(1,2,1),(1,4,1),(1,10,1),(1,20,1)	38
76	(0,0,1,1,0,0,1)	(1,9,4)	40
77	(1,0,1,1,0,0,1)	(1,3,1),(1,5,1),(1,30,1)	39
78	(0,1,1,1,0,0,1)	(1,1,2),(1,6,2),(1,12,2)	40
79	(1,1,1,1,0,0,1)	(1,39,1)	40
80	(0,0,0,0,1,0,1)	(1,2,16)	48
81	(1,0,0,0,1,0,1)	(1,1,1),(1,3,1),(1,9,1),(1,27,1)	41
82	(0,1,0,0,1,0,1)	(2,10,2)	42
83	(1,1,0,0,1,0,1)	(1,41,1)	42
84	(0,0,1,0,1,0,1)	(1,1,4),(1,3,4),(1,6,4)	44
85	(1,0,1,0,1,0,1)	(1,2,1),(2,4,1),(4,8,1)	43
86	(0,1,1,0,1,0,1)	(3,7,2)	44
87	(1,1,1,0,1,0,1)	(1,1,1),(1,14,1),(1,28,1)	44
88	(0,0,0,1,1,0,1)	(1,5,8)	48
89	(1,0,0,1,1,0,1)	(4,11,1)	45
90	(0,1,0,1,1,0,1)	(1,1,2),(1,2,2),(1,3,2),(1,4,2),(1,12,2)	46
91	(1,1,0,1,1,0,1)	(1,3,1),(1,6,1),(3,12,1)	46
92	(0,0,1,1,1,0,1)	(1,11,4)	48
93	(1,0,1,1,1,0,1)	(1,1,1),(3,5,1),(3,10,1)	47
94	(0,1,1,1,1,0,1)	(1,23,2)	48
95	(1,1,1,1,1,0,1)	(1,2,1),(1,9,1),(1,36,1)	48
96	(0,0,0,0,0,1,1)	(1,1,32)	64
97	(1,0,0,0,0,1,1)	(2,24,1)	49
98	(0,1,0,0,0,1,1)	(1,3,2),(1,21,2)	50
99	(1,1,0,0,0,1,1)	(1,1,1),(1,3,1),(3,5,1),(2,15,1)	50
100	(0,0,1,0,0,1,1)	(1,2,4),(1,10,4)	52

Die Nullstellen der Goss-Polynome für $p = q = 3$ und $1 \leq k \leq 100$

k	p-adische Entw.	(n,d,e)	X=0
1	(1)		1
2	(2)		2
3	(0,1)		3
4	(1,1)	(2,1,1)	2
5	(2,1)	(1,2,1)	3
6	(0,2)		6
7	(1,2)	(1,2,2)	3
8	(2,2)	(1,2,1)	6
9	(0,0,1)		9
10	(1,0,1)	(2,1,1),(2,2,1)	4
11	(2,0,1)	(2,3,1)	5
12	(0,1,1)	(2,1,3)	6
13	(1,1,1)	(2,1,1),(1,2,1),(1,4,1)	5
14	(2,1,1)	(2,2,1),(1,4,1)	6
15	(0,2,1)	(1,2,3)	9
16	(1,2,1)	(1,2,1),(1,8,1)	6
17	(2,2,1)	(2,1,1),(2,3,1)	9
18	(0,0,2)		18
19	(1,0,2)	(2,6,1)	7
20	(2,0,2)	(2,6,1)	8
21	(0,1,2)	(1,2,6)	9
22	(1,1,2)	(2,7,1)	8
23	(2,1,2)	(2,1,1),(1,2,3),(2,3,1)	9
24	(0,2,2)	(1,2,3)	18
25	(1,2,2)	(2,1,2),(2,3,2)	9
26	(2,2,2)	(2,1,1),(2,3,1)	18
27	(0,0,0,1)		27
28	(1,0,0,1)	(6,3,1)	10
29	(2,0,0,1)	(1,2,1),(1,16,1)	11
30	(0,1,0,1)	(2,1,3),(2,2,3)	12
31	(1,1,0,1)	(1,2,2),(1,4,1),(1,12,1)	11
32	(2,1,0,1)	(1,2,1),(1,8,1),(1,10,1)	12
33	(0,2,0,1)	(2,3,3)	15
34	(1,2,0,1)	(2,4,1),(2,7,1)	12
35	(2,2,0,1)	(2,2,1),(2,3,1),(1,10,1)	15

k	p-adische Entw.	(n,d,e)	X=0
36	(0,0,1,1)	(2,1,9)	18
37	(1,0,1,1)	(1,2,1),(1,4,1),(2,9,1)	13
38	(2,0,1,1)	(2,1,3),(1,6,1),(1,12,1)	14
39	(0,1,1,1)	(2,1,3),(1,2,3),(1,4,3)	15
40	(1,1,1,1)	(1,2,1),(1,4,1),(4,5,1)	14
41	(2,1,1,1)	(2,6,1),(1,14,1)	15
42	(0,2,1,1)	(2,2,3),(1,4,3)	18
43	(1,2,1,1)	(2,1,1),(2,3,1),(2,10,1)	15
44	(2,2,1,1)	(2,4,1),(2,9,1)	18
45	(0,0,2,1)	(1,2,9)	27
46	(1,0,2,1)	(1,4,1),(1,26,1)	16
47	(2,0,2,1)	(1,2,3),(2,7,1),(1,10,1)	17
48	(0,1,2,1)	(1,2,3),(1,8,3)	18
49	(1,1,2,1)	(2,1,1),(2,3,1),(1,8,1),(1,16,1)	17
50	(2,1,2,1)	(1,32,1)	18
51	(0,2,2,1)	(2,1,3),(2,3,3)	27
52	(1,2,2,1)	(2,1,1),(2,3,1),(2,13,1)	18
53	(2,2,2,1)	(1,2,1),(6,4,1)	27
54	(0,0,0,2)		54
55	(1,0,0,2)	(1,2,2),(1,12,1),(1,20,1)	19
56	(2,0,0,2)	(2,1,1),(1,2,1),(1,8,1),(1,10,1),(1,14,1)	20
57	(0,1,0,2)	(2,6,3)	21
58	(1,1,0,2)	(1,4,1),(1,6,1),(2,14,1)	20
59	(2,1,0,2)	(2,9,1),(1,20,1)	21
60	(0,2,0,2)	(2,6,3)	24
61	(1,2,0,2)	(1,2,1),(2,12,1),(1,14,1)	21
62	(2,2,0,2)	(2,1,1),(1,36,1)	24
63	(0,0,1,2)	(1,2,18)	27
64	(1,0,1,2)	(2,1,2),(3,2,1),(2,8,1),(1,16,1)	22
65	(2,0,1,2)	(2,1,1),(2,20,1)	23
66	(0,1,1,2)	(2,7,3)	24
67	(1,1,1,2)	(1,8,1),(3,12,1)	23
68	(2,1,1,2)	(2,4,1),(1,8,1),(1,10,1),(1,18,1)	24
69	(0,2,1,2)	(2,1,3),(1,2,9),(2,3,3)	27
70	(1,2,1,2)	(2,23,1)	24

k	p-adische Entw.	(n,d,e)	X=0
71	(2,2,1,2)	(1,2,10),(6,4,1)	27
72	(0,0,2,2)	(1,2,9)	54
73	(1,0,2,2)	(1,20,1),(1,28,1)	25
74	(2,0,2,2)	(2,9,1),(2,15,1)	26
75	(0,1,2,2)	(2,1,6),(2,3,6)	27
76	(1,1,2,2)	(1,6,1),(2,11,1),(1,22,1)	26
77	(2,1,2,2)	(2,1,3),(1,2,1),(2,3,3),(6,4,1)	27
78	(0,2,2,2)	(2,1,3),(2,3,3)	54
79	(1,2,2,2)	(1,2,2),(6,4,2)	27
80	(2,2,2,2)	(1,2,1),(6,4,1)	54
81	(0,0,0,0,1)		81
82	(1,0,0,0,1)	(2,1,1),(2,2,1),(12,4,1)	28
83	(2,0,0,0,1)	(2,27,1)	29
84	(0,1,0,0,1)	(6,3,3)	30
85	(1,1,0,0,1)	(1,2,1),(2,14,1),(1,26,1)	29
86	(2,1,0,0,1)	(2,14,1),(1,28,1)	30
87	(0,2,0,0,1)	(1,2,3),(1,16,3)	33
88	(1,2,0,0,1)	(2,1,1),(3,2,1),(2,3,1),(1,10,1),(2,17,1)	30
89	(2,2,0,0,1)	(2,18,1),(1,20,1)	33
90	(0,0,1,0,1)	(2,1,9),(2,2,9)	36
91	(1,0,1,0,1)	(2,1,1),(2,2,1),(5,6,1),(3,8,1)	31
92	(2,0,1,0,1)	(1,10,1),(1,12,1),(1,16,1),(1,22,1)	32
93	(0,1,1,0,1)	(1,2,6),(1,4,3),(1,12,3)	33
94	(1,1,1,0,1)	(1,4,1),(4,5,1),(2,7,1),(1,24,1)	32
95	(2,1,1,0,1)	(2,1,1),(1,2,3),(2,3,1),(2,9,1),(2,15,1)	33
96	(0,2,1,0,1)	(1,2,3),(1,8,3),(1,10,3)	36
97	(1,2,1,0,1)	(2,3,1),(2,29,1)	33
98	(2,2,1,0,1)	(2,6,1),(1,22,1),(1,28,1)	36
99	(0,0,2,0,1)	(2,3,9)	45
100	(1,0,2,0,1)	(2,5,1),(2,12,1),(2,16,1)	34

Die Nullstellen der Eisenstein-Reihen für $p = q = 2$ und $1 \leq k \leq 100$

k	p-adische Entw.	(n,d,e)
1	(1)	(1,2,1)
2	(0,1)	(1,2,2)
3	(1,1)	(2,3,1)
4	(0,0,1)	(1,2,4)
5	(1,0,1)	(1,2,2),(2,3,1)
6	(0,1,1)	(2,3,2)
7	(1,1,1)	(1,2,1),(3,4,1)
8	(0,0,0,1)	(1,2,8)
9	(1,0,0,1)	(2,9,1)
10	(0,1,0,1)	(1,2,4),(2,3,2)
11	(1,1,0,1)	(1,2,5),(3,4,1)
12	(0,0,1,1)	(2,3,4)
13	(1,0,1,1)	(1,2,1),(2,3,2),(3,4,1)
14	(0,1,1,1)	(1,2,2),(3,4,2)
15	(1,1,1,1)	(6,5,1)
16	(0,0,0,0,1)	(1,2,16)
17	(1,0,0,0,1)	(1,2,2),(2,3,1),(2,12,1)
18	(0,1,0,0,1)	(2,9,2)
19	(1,1,0,0,1)	(1,2,1),(2,3,1),(3,10,1)
20	(0,0,1,0,1)	(1,2,8),(2,3,4)
21	(1,0,1,0,1)	(3,6,1),(3,8,1)
22	(0,1,1,0,1)	(1,2,10),(3,4,2)
23	(1,1,1,0,1)	(1,2,8),(6,5,1)
24	(0,0,0,1,1)	(2,3,8)
25	(1,0,0,1,1)	(1,2,1),(3,16,1)
26	(0,1,0,1,1)	(1,2,2),(2,3,4),(3,4,2)
27	(1,1,0,1,1)	(2,3,4),(6,5,1)
28	(0,0,1,1,1)	(1,2,4),(3,4,4)
29	(1,0,1,1,1)	(1,2,2),(3,4,2),(6,5,1)
30	(0,1,1,1,1)	(6,5,2)
31	(1,1,1,1,1)	(1,2,1),(2,3,1),(9,6,1)
32	(0,0,0,0,0,1)	(1,2,32)
33	(1,0,0,0,0,1)	(2,3,1),(4,15,1)
34	(0,1,0,0,0,1)	(1,2,4),(2,3,2),(2,12,2)
35	(1,1,0,0,0,1)	(1,2,5),(3,20,1)

k	p-adische Entw.	(n,d,e)
36	(0,0,1,0,0,1)	(2,9,4)
37	(1,0,1,0,0,1)	(1,2,1),(3,4,1),(2,30,1)
38	(0,1,1,0,0,1)	(1,2,2),(2,3,2),(3,10,2)
39	(1,1,1,0,0,1)	(3,8,1),(3,10,1),(2,12,1)
40	(0,0,0,1,0,1)	(1,2,16),(2,3,8)
41	(1,0,0,1,0,1)	(1,2,2),(2,3,2),(3,4,1),(2,9,1),(3,12,1)
42	(0,1,0,1,0,1)	(3,6,2),(3,8,2)
43	(1,1,0,1,0,1)	(1,2,1),(3,4,1),(2,36,1)
44	(0,0,1,1,0,1)	(1,2,20),(3,4,4)
45	(1,0,1,1,0,1)	(2,3,1),(2,42,1)
46	(0,1,1,1,0,1)	(1,2,16),(6,5,2)
47	(1,1,1,1,0,1)	(1,2,17),(2,3,1),(9,6,1)
48	(0,0,0,0,1,1)	(2,3,16)
49	(1,0,0,0,1,1)	(1,2,1),(3,14,1),(2,27,1)
50	(0,1,0,0,1,1)	(1,2,2),(3,16,2)
51	(1,1,0,0,1,1)	(2,21,1),(2,30,1)
52	(0,0,1,0,1,1)	(1,2,4),(2,3,8),(3,4,4)
53	(1,0,1,0,1,1)	(1,2,2),(3,8,1),(2,15,1),(3,16,1)
54	(0,1,1,0,1,1)	(2,3,8),(6,5,2)
55	(1,1,1,0,1,1)	(1,2,1),(2,3,9),(9,6,1)
56	(0,0,0,1,1,1)	(1,2,8),(3,4,8)
57	(1,0,0,1,1,1)	(3,8,1),(2,9,1),(3,24,1)
58	(0,1,0,1,1,1)	(1,2,4),(3,4,4),(6,5,2)
59	(1,1,0,1,1,1)	(1,2,5),(2,3,1),(3,4,4),(9,6,1)
60	(0,0,1,1,1,1)	(6,5,4)
61	(1,0,1,1,1,1)	(1,2,1),(2,3,1),(6,5,2),(9,6,1)
62	(0,1,1,1,1,1)	(1,2,2),(2,3,2),(9,6,2)
63	(1,1,1,1,1,1)	(18,7,1)
64	(0,0,0,0,0,0,1)	(1,2,64)
65	(1,0,0,0,0,0,1)	(1,2,2),(2,9,1),(6,18,1)
66	(0,1,0,0,0,0,1)	(2,3,2),(4,15,2)
67	(1,1,0,0,0,0,1)	(1,2,1),(3,4,1),(2,60,1)
68	(0,0,1,0,0,0,1)	(1,2,8),(2,3,4),(2,12,4)
69	(1,0,1,0,0,0,1)	(2,3,2),(3,8,1),(2,9,1),(3,28,1)
70	(0,1,1,0,0,0,1)	(1,2,10),(3,20,2)

k	p-adische Entw.	(n,d,e)
71	(1,1,1,0,0,0,1)	(1,2,8),(3,4,1),(2,9,1),(3,32,1)
72	(0,0,0,1,0,0,1)	(2,9,8)
73	(1,0,0,1,0,0,1)	(1,2,1),(2,3,1),(3,4,1),(6,9,1),(6,12,1)
74	(0,1,0,1,0,0,1)	(1,2,2),(3,4,2),(2,30,2)
75	(1,1,0,1,0,0,1)	(2,3,1),(3,14,1),(2,18,1),(3,22,1)
76	(0,0,1,1,0,0,1)	(1,2,4),(2,3,4),(3,10,4)
77	(1,0,1,1,0,0,1)	(1,2,2),(6,5,1),(3,8,1),(3,32,1)
78	(0,1,1,1,0,0,1)	(3,8,2),(3,10,2),(2,12,2)
79	(1,1,1,1,0,0,1)	(1,2,1),(3,52,1)
80	(0,0,0,0,1,0,1)	(1,2,32),(2,3,16)
81	(1,0,0,0,1,0,1)	(3,8,1),(3,46,1)
82	(0,1,0,0,1,0,1)	(1,2,4),(2,3,4),(3,4,2),(2,9,2),(3,12,2)
83	(1,1,0,0,1,0,1)	(1,2,5),(2,3,4),(3,8,1),(2,54,1)
84	(0,0,1,0,1,0,1)	(3,6,4),(3,8,4)
85	(1,0,1,0,1,0,1)	(1,2,1),(6,5,1),(6,8,1),(9,10,1)
86	(0,1,1,0,1,0,1)	(1,2,2),(3,4,2),(2,36,2)
87	(1,1,1,0,1,0,1)	(2,3,1),(3,16,1),(3,40,1)
88	(0,0,0,1,1,0,1)	(1,2,40),(3,4,8)
89	(1,0,0,1,1,0,1)	(1,2,2),(2,3,1),(3,4,2),(6,5,1),(6,19,1)
90	(0,1,0,1,1,0,1)	(2,3,2),(2,42,2)
91	(1,1,0,1,1,0,1)	(1,2,1),(6,5,1),(2,9,1),(2,12,1),(3,36,1)
92	(0,0,1,1,1,0,1)	(1,2,32),(6,5,4)
93	(1,0,1,1,1,0,1)	(3,28,1),(3,34,1)
94	(0,1,1,1,1,0,1)	(1,2,34),(2,3,2),(9,6,2)
95	(1,1,1,1,1,0,1)	(1,2,32),(18,7,1)
96	(0,0,0,0,0,1,1)	(2,3,32)
97	(1,0,0,0,0,1,1)	(1,2,1),(2,3,2),(3,4,1),(6,19,1),(2,27,1)
98	(0,1,0,0,0,1,1)	(1,2,2),(3,14,2),(2,27,2)
99	(1,1,0,0,0,1,1)	(2,42,1),(2,57,1)
100	(0,0,1,0,0,1,1)	(1,2,4),(3,16,4)

Die Nullstellen der Eisenstein-Reihen für $p = q = 3$ und $1 \leq k \leq 100$

k	p-adische Entw.	(n,d,e)
2	(2)	(3,2,1)
4	(1,1)	(3,2,2)
6	(0,2)	(3,2,3)
8	(2,2)	(8,3,1)
10	(1,0,1)	(3,2,1),(6,4,1)
12	(0,1,1)	(3,2,6)
14	(2,1,1)	(3,2,3),(8,3,1)
16	(1,2,1)	(8,3,2)
18	(0,0,2)	(3,2,9)
20	(2,0,2)	(3,2,6),(8,3,1)
22	(1,1,2)	(3,2,3),(8,3,2)
24	(0,2,2)	(8,3,3)
26	(2,2,2)	(3,2,1),(18,4,1)
28	(1,0,0,1)	(3,2,2),(12,6,1)
30	(0,1,0,1)	(3,2,3),(6,4,3)
32	(2,1,0,1)	(12,8,1)
34	(1,2,0,1)	(3,2,1),(8,3,1),(6,12,1)
36	(0,0,1,1)	(3,2,18)
38	(2,0,1,1)	(3,2,3),(12,8,1)
40	(1,1,1,1)	(8,3,1),(6,4,1),(12,6,1)
42	(0,2,1,1)	(3,2,9),(8,3,3)
44	(2,2,1,1)	(3,2,10),(18,4,1)
46	(1,0,2,1)	(3,2,3),(8,3,1),(8,6,1),(6,8,1)
48	(0,1,2,1)	(8,3,6)
50	(2,1,2,1)	(3,2,1),(8,3,3),(18,4,1)
52	(1,2,2,1)	(3,2,2),(18,4,2)
54	(0,0,0,2)	(3,2,27)
56	(2,0,0,2)	(8,6,1),(8,15,1)
58	(1,1,0,2)	(3,2,1),(8,9,1),(6,16,1)
60	(0,2,0,2)	(3,2,18),(8,3,3)
62	(2,2,0,2)	(3,2,19),(18,4,1)
64	(1,0,1,2)	(12,16,1)
66	(0,1,1,2)	(3,2,9),(8,3,6)
68	(2,1,1,2)	(3,2,10),(8,3,3),(18,4,1)
70	(1,2,1,2)	(3,2,11),(18,4,2)

k	p-adische Entw.	(n,d,e)
72	(0,0,2,2)	(8,3,9)
74	(2,0,2,2)	(3,2,1),(8,3,6),(18,4,1)
76	(1,1,2,2)	(3,2,2),(8,3,3),(18,4,2)
78	(0,2,2,2)	(3,2,3),(18,4,3)
80	(2,2,2,2)	(48,5,1)
82	(1,0,0,0,1)	(3,2,1),(30,8,1)
84	(0,1,0,0,1)	(3,2,6),(12,6,3)
86	(2,1,0,0,1)	(3,2,3),(8,3,1),(8,6,1),(12,8,1),(6,12,1)
88	(1,2,0,0,1)	(8,15,1),(8,18,1)
90	(0,0,1,0,1)	(3,2,9),(6,4,9)
92	(2,0,1,0,1)	(3,2,6),(8,3,1),(8,27,1)
94	(1,1,1,0,1)	(3,2,3),(8,3,2),(12,6,1),(12,12,1)
96	(0,2,1,0,1)	(12,8,3)
98	(2,2,1,0,1)	(3,2,1),(8,3,1),(12,10,1),(6,24,1)
100	(1,0,2,0,1)	(3,2,2),(8,3,2),(12,20,1)

Symbolverzeichnis

$\mathbb{N}$	die natürlichen Zahlen	6
$\mathbb{N}_0$	die natürlichen Zahlen mit Null	6
$\mathbb{Z}$	die Menge der ganzen Zahlen	6
$\mathbb{R}$	die Menge der reellen Zahlen	6
$\mathbb{C}$	die Menge der komplexen Zahlen	6
p	eine Primzahl	6
s	eine natürliche Zahl	6
q	p^s mit $s \in \mathbb{N}$, eine Primzahlpotenz	6
$\mathbb{F}_q$	der endliche Körper der Charakteristik p mit q Elementen	6
$\mathbb{F}_q^*$	die multiplikative Gruppe von $\mathbb{F}_q$	6
$\overline{\mathbb{F}}_q$	der algebraische Abschluß von $\mathbb{F}_q$	6
Ω	$\overline{\mathbb{F}}_q - \mathbb{F}_q$	6
$\mathbb{F}_{q^n}$	die Körpererweiterung von $\mathbb{F}_q$ in $\overline{\mathbb{F}}_q$ vom Grad n	6
K	ein beliebiger Körper	6
$K[z]$	der Ring der Polynome über K	6
$K(z)$	der Körper der rationalen Funktionen über K	6
$K^{2\times 2}$	die Menge der 2×2-Matrizen über K	6
$Gl(2,K)$	die lineare Gruppe über K	6
Γ	die lineare Gruppe über $\mathbb{F}_q$	7
$\#\cdot$	die Kardinalität einer Menge	7
H	die komplexe obere Halbebene	7
B	die Standard-Borelgruppe von $Gl(2,K)$	8
U	die Untergruppe $\left\{ \begin{pmatrix} 1 & u \\ 0 & 1 \end{pmatrix} \in K^{2\times 2} \;\middle|\; u \in K \right\}$ von $Gl(2,K)$	8
ω	das Element $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ aus $Gl(2,K)$	8
γ	das Element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ aus $Gl(2,K)$	8
K^*	die multiplikative Gruppe von K	8
(s,t)	ein Tupel mit den Elementen $s, t \in K$	8
$(u:v)$	eine Äquivalenzklasse in K^2	8
$\mathbb{P}^1(K)$	die projektive Gerade über K	8

$\gamma(u:v)$	das Element $(au+bv:cu+dv)$ aus $\mathbb{P}^1(K)$	9
ϵ	das Element $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ aus $Gl(2,K)$	10
$m \sim n$	die Elemente m und n sind äquivalent zueinander	11
Γ_z	der Stabilisator von $z \in \Omega$ in Γ	12
$\Gamma \cdot z$	die Bahn von $z \in \Omega$ unter der Operation von Γ	12
γz	das Element $\frac{az+b}{cz+d}$ aus Ω	11
e	ein elliptischer Punkt	14
P	die Menge aller p-Sylow-Gruppen der Gruppe Γ	15
V	eine p-Untergruppe von Γ	15
U	eine p-Sylow-Gruppe von Γ	15
M	die Menge aller Untergruppen von Γ	16
$Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x)$	die Spur von $x \in \mathbb{F}_{q^n}$, wobei $\mathbb{F}_{q^n}$ eine Körpererweiterung vom Grad n von $\mathbb{F}_q$ ist	17
$N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x)$	die Norm von $x \in \mathbb{F}_{q^n}$, wobei $\mathbb{F}_{q^n}$ eine Körpererweiterung vom Grad n von $\mathbb{F}_q$ ist	17
$\bar{x}$	das zu x konjugierte Element	17
$f_\gamma(z)$	das charakteristische Polynom von $\gamma \in \Gamma$ in z	17
$m_\gamma(z)$	das Minimalpolynom von $\gamma \in \Gamma$ in z	17
$c_1(x)$	die Konjugationsklasse von $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ in Γ	17
$c_2(x)$	die Konjugationsklasse von $\begin{pmatrix} x & 1 \\ 0 & x \end{pmatrix}$	18
$c_3(x,y)$	die Konjugationsklasse von $\begin{pmatrix} x & 0 \\ 0 & y \end{pmatrix}$	18
$c_4(x)$	die Konjugationsklasse von $\begin{pmatrix} 0 & -N_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \\ 1 & Tr_{\mathbb{F}_q}^{\mathbb{F}_{q^n}}(x) \end{pmatrix}$	18
$Sl(2,\mathbb{Z})$	die spezielle lineare Gruppe über $\mathbb{Z}$	21
$Gl(2,\mathbb{R})$	die lineare Gruppe über $\mathbb{R}$	21
ρ	die dritte primitive Einheitswurzel in H	22
i	die vierte primitive Einheitswurzel in H	22
R	ein Fundamentalbereich von $Sl(2,\mathbb{Z})\backslash H$ in Kapitel 2	22
$Sl(2,\mathbb{Z}) \cdot z$	die Bahn von $z \in H$	22
$f(z)$	eine (schwache) Modulform über H	(22,) 23
$2k$	das Gewicht einer Modulform über H	22

$q(z)$	$= e^{2\pi i z}$	22
$\tilde{f}(q(z))$	die Fourierentwicklung einer Modulform über H	22
$G_k(z)$	die Eisenstein-Reihen über H	23
$\sum'_{m,n\in\mathbb{Z}}$	die Summe über die Indexmenge $\{(m,n) \in \mathbb{Z} \times \mathbb{Z} \mid (m,n) \neq (0,0)\}$	23
M_k	der $\mathbb{C}$-Vektorraum der Modulformen über H	24
$\nu_w(f)$	die Ordnung von $f(z)$ in $w \in H$	24
$\nu_\infty(f)$	die Ordnung von $\tilde{f}(z)$ in $q(z) = 0$	24
e_z	die Ordnung des Stabilisators in dem Punkt $z \in H$	24
$\sum^*_{z\in R}$	die Summe über alle $z \in R$ mit $z \notin Sl(2,\mathbb{Z}) \cdot i$ und $z \notin Sl(2,\mathbb{Z}) \cdot \rho$	24
$[a]$	die größte ganze Zahl kleiner oder gleich $a \in \mathbb{R}$	24
$G_2^\alpha G_3^\beta$	ein Monom über $\mathbb{C}$	24
$f(z)$	eine Modulform über $\mathbb{F}_q$	25
k	das Gewicht einer Modulform über $\mathbb{F}_q$	25
$\mathbb{Z}/(q-1)\mathbb{Z}$	Menge der Restklassen $\mathbb{Z}$ modulo $q-1$	25
m	der Typ einer Modulform über $\mathbb{F}_q$	25
$\alpha(\gamma, z)$	der Automorphiefaktor $\frac{(cz+d)^k}{(\det\gamma)^m}$ einer Modulform	26
$M_{k,m}(\Gamma)$	der $\overline{\mathbb{F}}_q$-Vektorraum der Modulformen vom Gewicht k und vom Typ m	26
$E_k(z)$	die Eisenstein-Reihen $\sum'_{a,b\in\mathbb{F}_q} \frac{1}{(az+b)^k}$	27
$\sum'_{a,b\in\mathbb{F}_q}$	die Summe über die Indexmenge $\{(a,b) \in \mathbb{F}_q \times \mathbb{F}_q \mid (a,b) \neq (0,0)\}$	27
$M_k(\Gamma)$	der $\overline{\mathbb{F}}_q$-Vektorraum $M_{k,0}(\Gamma)$	28
$t(z)$	die Modulform $\frac{1}{z-z^q}$ aus $M_{q+1,1}(\Gamma)$	31
$\Delta(z)$	die Modulform $(t(z))^{q-1}$ aus $M_{q^2-1,1}(\Gamma)$	31
$\tilde{f}(t(z))$	die t-Entwicklung einer Modulform über $\mathbb{F}_q$	32
K	der Körper der rationalen Funktionen über $\overline{\mathbb{F}}_q$ in Kapitel 3.2	32
d	der Grad der t-Entwicklung einer Modulform	33
$\overline{K}$	der algebraische Abschluß von K	35
X	ein über K transzendentes Element	35
D	ein Divisor von $K(X)/K$ der Form $\sum_{x\in\mathbb{P}^1(K)} a_x x$	35
P	ein Primdivisor	35
$\mathcal{D}_{K(X)}$	die Divisorgruppe	36
$\mu_z(D)$	die Nullstellenordnung des Divisors D in z	36

$deg\ D$	der Grad des Divisors D	36
$\mu_a(f)$	die Bewertung von f in $a \in K$	36
$\mu_\infty(f)$	die Bewertung von f in ∞	36
$div(f)_0$	der Nullstellendivisor von f	37
$div(f)_\infty$	der Poldivisor von f	37
$div(f)$	der Hauptdivisor von f	37
D_S	die Projektion von D auf $S \subseteq \mathbb{P}^1(K)$	37
$\mathcal{P}_{K(X)}$	die Gruppe der Hauptdivisoren	38
$\mathcal{C}_{K(X)}$	die Divisorrestklassengruppe	38
$[D]$	ein Element der Faktorgruppe $\mathcal{C}_{K(X)}$	38
$\mathcal{L}(D)$	der $\mathcal{L}$-Raum	38
$\nu_a(f)$	die Nullstellenordnung einer Modulform $f \in M_{k,m}(\Gamma)$ in $a \in \overline{\mathbb{F}}_q$	40
R	ein Repräsentantensystem von $\Gamma\backslash(\overline{\mathbb{F}}_q - \mathbb{F}_{q^2})$ in Kapitel 4	41
$\nu^*(f)$	die Summe aller $\nu_a(f)$ mit $a \in R$	46
g	die Modulform $E_{q-1}(z)$	46
h	die Modulform $-t(z)$	46
$g^i h^j$	ein Monom aus $M_{k,m}(\Gamma)$	47
$M_{k,m}^r$	der $\overline{\mathbb{F}}_q$-Vektorraum der Modulformen, die in $t(z) = 0$ eine mindestens r-fache Nullstelle besitzen	47
S_k	die Summe der k-ten Potenzen	54
S_k^n	die Summe der k-ten Potenzen in n Variablen	55
σ_k^n	die k-te elementarsymmetrische Summe in n Variablen	55
$dlogf(z)$	die logarithmische Differentiation einer Funktion f nach der Unbestimmten z	58
$G_k(X)$	das k-te Goss-Polynom	59
$\mathbb{F}_q(X,u)$	der Körper der rationalen Funktionen in X und u	64
$\mathbb{F}_q(z)[X]$	der Polynomring über $\mathbb{F}_q(z)$	60
$G(X,u)$	die erzeugende Funktion der $G_k(X)$	62
$(a_0, a_1, \ldots, a_n)$	die p-adische Entwicklung von k	70
(n,d,e)	die Anzahl n der irreduziblen Faktoren vom Grad d, die mit dem Exponenten e auftreten	71

Literaturverzeichnis

[CLO92] D. Cox, J. Little, and D. O'Shea. *Ideals, Varieties, and Algorithms An Introduction to Computational Algebraic Geometry and Commutative Algebra.* Springer-Verlag, 1992.

[Gek] E.-U. Gekeler. Some new results on modular forms for $GL(2, \mathbb{F}_q[T])$. Eingereicht.

[Gek88] E.-U. Gekeler. On the coefficients of drinfeld modular forms. *Invent. Math. 93*, pages 667–700, 1988.

[Lan93] S. Lang. *Algebra.* Addison-Wesley, third edition, 1993.

[Mey80] K. Meyberg. *Algebra, Teil 1.* Carl Hanser Verlag München Wien, 2. edition, 1980.

[PS83] I. Piatetski-Shapiro. *Complex representations of $GL(2,K)$ for finite fields K.* AMS, number 16 in contempory mathematics edition, 1983.

[Ser73] J.-P. Serre. *A Course in Arithmetic.* Springer-Verlag, 1973.

[Sti93] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer-Verlag, 1993.