Modulkurven und Codes

Überarbeitete und erweiterte Version meiner Diplomarbeit

angefertigt von Markus Klein
nach einem Thema von
Prof. Dr. R. Schulze-Pillot
am Fachbereich Mathematik der
Universität des Saarlandes

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Codierungstheorie

Die Codierungstheorie beschäftigt sich mit dem Problem der Übermittlung von Nachrichten durch einen Rauschkanal, also einen Kanal, bei dem durch Übertragung von Nachrichten Fehler auftreten können. Die Erkennung und Korrektur solcher Fehler ist eines der Hauptprobleme der Theorie. Ihr Ursprung liegt in einem Satz von Shannon, der die Existenz von Codes garantiert, die Informationen durch einen Informationskanal mit einer Rate übertragen können, die nahe an der Übertragungskapazität des Kanals liegt. Das heißt zu gegebenem Kanal gibt es Codes, so dass die Fehlerwahrscheinlichkeit bei der Übertragung einer Nachricht beliebig klein ist.

Eine Nachricht besteht im Allgemeinen aus einer endlichen Folge von Symbolen über einem endlichen Alphabet, von dem wir annehmen, dass es ein endlicher Körper $\mathbb{F}_q$ ist. Da in einem Übertragungskanal Störungen auftreten, die übermittelte Nachricht also mit Fehlern behaftet sein kann und Fehler bei der Interpretation der Nachricht gemacht werden können, ist eines der Ziele der Theorie, diese Fehler möglichst unwahrscheinlich zu machen. Die Idee besteht darin, im Allgemeinen überflüssige Informationen zusammen mit der Nachricht zu übermitteln, das heißt, die Folge der Nachrichtensymbole systematisch zu vergrößern.
Eine Teilmenge C des Vektorraums $\mathbb{F}_q^n$ nennen wir einen Code der Länge n. Ist H eine $(n-k) \times n$-Matrix über $\mathbb{F}_q$ mit Rang $n-k$, dann heißt der Unterraum C aller Vektoren $c \in \mathbb{F}_q^n$ mit $Hc^T = 0$ linearer Code über $\mathbb{F}_q$. Eine $k \times n$ Matrix G mit Rang k, die Gleichung $GH^t = 0$ erfüllt, nennen wir Erzeugermatrix von C. Die lineare Hülle der Zeilen von G erzeugt den Code C. Für die beiden Vektoren x, y aus $\mathbb{F}_q^n$ nennen wir die Anzahl der in x und y unterschiedlichen Koordinaten den Abstand $d(x, y)$ von x und y und die Anzahl der von null verschiedenen Koordinaten in x bezeichnen wir mit dem Gewicht $w(x)$ von x. Die Zahl $d = \min\limits_{u,v \in C, u \neq v} d(u, v)$ nennen wir den minimalen Abstand des Codes C. Ist C ein linearer Code, so ist $d = \min\limits_{0 \neq c \in C} w(c)$. Im linearen Fall bezeichnen wir $k = log_q(\#C)$ als die Dimension von C. Wir sagen auch C ist ein linearer $[n, k, d]$-Code. Ist C nicht notwendig linear, so nennt man C auch einen (n, M, d)-Code. M bezeichnet hierbei die Anzahl der Elemente von C.

1.1.1 Schranken von Codes

Satz 1.1 (Singleton Schranke)
Für einen (n, M, d)-Code C über $\mathbb{F}_q$ gilt: $M \leq q^{n-d+1}$. Ist C insbesondere linear, so gilt: $n \geq k + d - 1$.

Beweis:
Sei C ein Code, der für gegebene Länge n und Abstand d die maximal mögliche Anzahl von Elementen M hat. Durch $d-1$-maliges punktieren, also streichen des letzten Symbols jedes Codewortes erhält man einen $(n-d+1, M, 1)$-Code. Dies ist ein Code, in dem jedes Codewort verschieden ist. Insbesondere muss gelten $M \leq q^{n-d+1}$, woraus im linearen Fall $n \geq k+d-1$ wird.

□

Satz 1.2 (Hamming Schranke)
Sei C ein (n, M, d)-Code über $\mathbb{F}_q$ und t der ganzzahlige Anteil von $\frac{d+1}{2}$. Dann ist

$$M\left(1+\binom{n}{1}(q-1)+\cdots+\binom{n}{t}(q-1)^t\right) \leq q^n.$$

Beweis:
Es gibt $\binom{n}{m}(q-1)^m$ Vektoren mit n Koordinaten über $\mathbb{F}_q$, die das Gewicht m haben. Die Kugeln mit Radius e und mit Mittelpunkt in einem Codewort sind alle paarweise disjunkt. Jede der M Kugeln enthält

$$1+\binom{n}{1}(q-1)+\cdots+\binom{n}{t}(q-1)^t$$

aller q^n Vektoren in $\mathbb{F}_q^n$. Daraus folgt die Behauptung.

□

Satz 1.3 (Plotkin Schranke)
Für einen $[n, k, d]$-Code C über $\mathbb{F}_q$ gilt:

$$d \leq \tfrac{nq^{k-1}(q-1)}{q^k-1}.$$

Beweis:
Sei $1 \leq i \leq n$, so dass C ein Codewort enthält, dessen i-te Komponente nicht null ist. Sei D_i der Unterraum, der aus allen Codewörtern besteht, deren i-te Stelle gleich null ist. In C/D_i gibt es q Elemente, die den q möglichen Werten der i-ten Komponente eines Codewortes entsprechen. Die Gleichung $|C|/|D_i| = |C/D_i|$ liefert uns $|D_i| = q^{k-1}$. Addiert man nun die Gewichte aller Codewörter von C durch Summation über alle Komponenten, von denen es maximal n Stück gibt, so erhält man einen Wert, der kleiner gleich $nq^{k-1}(q-1)$ ist (Zu jedem D_i gibt es, ohne D_i selbst gezählt, $q-1$ Nebenklassen. In C gibt es also $(q-1)q^{k-1}$ Vektoren deren i-te Komponente ungleich null ist.). Der minimale Abstand d des Codes ist das minimale Gewicht, das nicht gleich null ist, und da die Anzahl der Codewörter, die nicht gleich null sind, q^k-1 ist, erhält man für d die obige Ungleichung, da das Minimum der Gewichte über alle Codewörter kleiner gleich dem Mittel der Gewichte über alle Codewörter sein muss.

□

Lemma 1.1
Ein linearer Code C hat genau dann minimalen Abstand $d \geq s+1$, falls je s Spaltenvektoren in der Matrix H linear unabhängig sind.

Beweis:
Seien s Spalten von H linear abhängig, dann gibt es ein Codewort $c \in C, c \neq 0$, für das $Hc^T = 0$ und $w(c) \leq s$ gilt. Also ist $d = \min\limits_{0 \neq c \in C} w(c) < s+1$. Umgekehrt, falls je s Spalten von H linear unabhängig sind, kann es kein $c \in C, c \neq 0$ geben, das ein Gewicht $w(c) \leq s$ hat und deshalb ist $d \geq s+1$.

□

Satz 1.4 (Gilbert-Varshamov Schranke)
Es gibt einen $[n, k, d']$-Code über $\mathbb{F}_q$ mit minimalem Abstand d' größer gleich d, falls

$$q^{n-k} > \sum_{i=0}^{d-2} \binom{n-1}{i} (q-1)^i.$$

Beweis:
Wir konstruieren eine Paritätsprüfungsmatrix H für einen Code mit obiger Eigenschaft. Die Konstruktion wird so ausgeführt, dass H den Rang $n-k$ hat und je $d-1$ Spalten von H linear unabhängig sind. Mit Lemma 1.1 folgt, dass der konstruierte Code minimalen Abstand größer gleich d hat.

Zur Konstruktion wählen wir zunächst die erste Spalte von H als einen beliebigen Vektor $v_1 \neq 0$ der Länge $n-k$ über $\mathbb{F}_q$. Als zweite Spalte wählen wir einen beliebigen Vektor $v_2 \neq 0$ der Länge $n-k$ über $\mathbb{F}_q$, der kein skalares Vielfaches von v_1 ist. Allgemein nehmen wir nun an, wir haben bereits $j-1$ Vektoren ausgesucht ($j < n$), so dass je $d-1$ linear unabhängig sind. Dann können höchstens

$$\sum_{i=0}^{d-2} \binom{j-1}{i} (q-1)^i$$

Vektoren durch lineare Kombinationen von $d-2$ oder weniger dieser $j-1$ Spaltenvektoren gebildet werden. Solange $j < n$ gilt, können wir einen weiteren Spaltenvektor von H so auswählen (hier eine j-te Spalte), dass er keine durch Linearkombination von $d-2$ oder weniger der $j-1$ schon ausgewählten Spaltenvektoren ist. Insbesondere sind dann je $d-1$ Spaltenvektoren linear unabhängig. Die Konstruktion kann so ausgeführt werden, dass H den Rang $n-k$ hat (Wähle zum Beispiel die ersten n-k Vektoren linear unabhängig.).

$\square$

1.1.2 Asymptotische Schranken

Im Satz von Shannon wird deutlich, dass gute Codes, also solche, bei denen das Auftreten von Fehlern bei der Übertragung unwahrscheinlich ist, auch lange Codes sind. Deshalb ist das asymptotische Verhalten von Codes von besonderem Interesse.
Sei nun q, die Anzahl der Elemente des Alphabets, fest vorgegeben. Jedem Code über dem Alphabet ordnen wir ein Paar $\left(\delta(C) = \frac{d}{n},\ R(C) = \frac{k}{n}\right)$ aus $[0,1]^2$ zu. Betrachtet man nun Folgen $\{C_i\}_{i \in I}$ von Codes, deren Länge für $i \to \infty$ gegen Unendlich strebt, so definieren wir, falls die Grenzwerte existieren,

$$(\delta, R) := \lim_{i \to \infty} (\delta(C), R(C)) \subset [0,1]^2$$

und nennen die Familie von Codes gut, falls δ und R größer als null sind. Bezeichnen wir mit U_q die Menge aller Punkte P aus $[0,1]^2$, für die es eine Folge von Codes gibt, so dass für diese Folge (δ, R) gleich P ist, dann ergibt sich folgenden Satz:

Satz 1.5
Es gibt eine stetige Funktion

$$\alpha_q : [0,1] \to [0,1] \ mit$$
$$U_q = \{(\delta, R) \in [0,1]^2 | R \leq \alpha_q(\delta)\}.$$

Weiter gilt:

- $\alpha_q(0) = 1$

- $\alpha_q(\delta) = 0$ *für* $\frac{q-1}{q} \leq \delta \leq 1$
- α_q *ist streng monoton fallend im Intervall* $[0, \frac{q-1}{q}]$

Beweis:
Siehe [TV, Part I, Chapter 3, Paragraph 1, Theorem 1.3.1, p. 68 ff].

□

Bemerkung 1.1

Obige Konstruktionen können für lineare, sowie für nicht notwendig lineare Codes durchgeführt werden. Man weiß nicht, ob beide Konstruktionen dieselbe stetige Funktion liefern.

□

Die oben angegebenen Schranken für Codes liefern uns nun folgende Abschätzungen für α_q:
Als obere Schranken:

- asymptotische Singleton Schranke:

$$\alpha_q(\delta) \leq 1 - \delta$$

- asymptotische Plotkin Schranke:

$$\alpha_q(\delta) \leq 1 - \tfrac{q-1}{q}\delta$$

- asymptotische Kugelpackungsschranke:

$$\alpha_q(\delta) \leq 1 - H_q(\tfrac{\delta}{2})$$

Als untere Schranke:

- asymptotische Gilbet-Varschamov Schranke:

$$\alpha_q(\delta) \geq 1 - H_q(\delta)$$

Mit H_q bezeichnen wir hier die Entropiefunktion, die gegeben ist durch:

$$H_q(x) = xlog_q(q-1) - xlog_q(x) - (1-x)log_q(1-x)$$

Bemerkung 1.2

Es gibt bessere obere Schranken. Siehe hierzu zum Beispiel [TV, Part I, Chapter 3]. In Paragraph 4.2 wird noch ein Satz angegeben, der die asymptotische Gilbert-Varschamov Schranke für $q \geq 49$ verbessert.

□

1.2 Algebraische Geometrie

1.2.1 Affine und projektive Räume

Sei im Weiteren k ein algebraisch abgeschlossener Körper. Mit $\mathbb{A}^n(k)$ oder einfach $\mathbb{A}^n$ bezeichnen wir den n-dimensionalen affinen Raum über k. Die Elemente $P \in \mathbb{A}^n(k)$ nennen wir Punkte. Sie sind n-Tupel $(x_1, \ldots, x_n)$, deren i-ten Eintrag wir i-te Koordinate nennen. Der affine Raum ist mit einer Topologie ausgestattet, der sogenannten Zariski-Topologie, deren abgeschlossene Mengen aus den Nullstellenmengen $V(I)$ von Idealen I aus $k[x_1, \ldots, x_n]$ bestehen,

$$V(I) = \{(x_1, \ldots, x_n) \in \mathbb{A}^n | f(x_1, \ldots, x_n) = 0 \text{ für alle } f \in I\}.$$

Diese nennen wir algebraische Mengen. Hat man umgekehrt eine algebraische Menge $V \subset \mathbb{A}^n$, so ist die Menge

$$I(V) = \{f \in k[x_1, \ldots, x_n] | f(P) = 0 \text{ für alle } P \in V\}$$

ein Ideal in $k[x_0, \ldots, x_n]$, das wir das Ideal von V nennen. Dieses Ideal ist endlich erzeugt, da $k[x_0, \ldots, x_n]$ ein noetherscher Ring ist. Das Radikal $\sqrt{I}$ eines Ideals I ist definiert als

$$\sqrt{I} = \{f \in k[x_1, \ldots, x_n] | f^r \in I \text{ für ein } r \in \mathbb{N} - \{0\}\}.$$

Diejenigen Ideale, die mit ihrem eigenen Radikal übereinstimmen, heißen Radikalideale.

Satz 1.6 (Korrespondenz von Idealen und algebraischen Mengen)
Die beiden oben beschriebenen Abbildung I und V zwischen der Menge der algebraischen Mengen von $\mathbb{A}^n$ und der Menge der Radikalideale von $k[x_1, \ldots, x_n]$ sind bijektiv und invers zueinander.

Beweis:
Siehe [CLS, Chapter 4, Paragraph 2, Theorem 7, p. 175] oder [Ha, Chapter 1, Paragraph 1, Corollary 1.4, p. 4]

□

Eine algebraische Menge V nennen wir reduzibel, wenn wir sie als Vereinigung zweier unterschiedlicher algebraischer Mengen $V = V_1 \cup V_2$ schreiben können, die beide nicht gleich V sind. Sonst nennen wir sie irreduzibel und bezeichnen sie auch als Varietät. Auf der algebraischen Seite entsprechen Varietäten Primidealen. Man hat folgenden Satz:

Satz 1.7
Die Abbildungen I und V aus Satz 1.6 induzieren eine bijektive Abbildung zwischen der Menge der Primideale von $k[x_1, \ldots, x_n]$ und der Menge der irreduziblen algebraischen Mengen von $\mathbb{A}^n$.

Beweis:
Siehe [CLS, Chapter 4, Paragraph 5, Corollary 4, p. 196]

□

Desweiteren gilt:

Satz 1.8
Die Abbildungen I und V aus Satz 1.6 induzieren eine bijektive Abbildung zwischen der Menge der maximalen Ideale von $k[x_1, \ldots, x_n]$ und der Menge der Punkte von $\mathbb{A}^n$.

Beweis:
Siehe [CLS, Chapter 4, Paragraph 5, Corollary 12, p. 199]

□

Für ein Ideal I aus $k[x_1, \ldots, x_n]$ korrespondieren also die Punkte von $V(I)$ mit denjenigen maximalen Idealen, die I enthalten. Da $k[x_1, \ldots, x_n]$ noethersch ist existiert zu jeder algebraischen Menge V eine bis auf die Reihenfolge eindeutige Zerlegung $V_1 \cup \ldots \cup V_s$ von V in Varietäten, so dass V_i nicht in V_j enthalten ist, falls i $\neq$ j. Die V_i nennen wir die irreduziblen Komponenten von V. Siehe hierzu zum Beispiel [Ha, Chapter 1, Paragraph 1, Proposition 1.5 und Corollary 1.6, p. 5] oder [CLS, Chapter 4, Paragraph 6, Theorem 4, p. 203 und Theorem 5, p. 204]. Ist V eine Varietät, dann ist der Ring $k[x_1, \ldots, x_n]/I(V)$ ein Integritätsring, den wir als Koordinatenring $A[V]$ von V bezeichnen. Dessen Quotientenkörper $k(V) = Quot(A[V])$ nennen wir Funktionenkörper von V.

Mit $\mathbb{P}^n(k)$ oder kurz $\mathbb{P}^n$ bezeichnen wir den n-dimensionalen projektiven Raum. Seine Punkte sind Äquivalenzklassen von $(n+1)$-Tupeln $(a_0, \ldots, a_n)$, die mindestens einen Eintrag a_i haben, der ungleich 0 ist. Dabei gilt: $(x_0, \ldots, x_n) \sim (y_0, \ldots, y_n)$ falls es eine Zahl $\lambda \in k - \{0\}$ mit $(x_0, \ldots, x_n) = (\lambda y_0, \ldots, \lambda y_n)$ gibt. Beachte dabei, dass es wohldefiniert ist, ob ein Eintrag gleich oder ungleich 0 ist. Die einzelnen Einträge des (n+1)-Tupels nennen wir homogene Koordinaten. Um nun auf dem projektiven Raum $\mathbb{P}^n$ eine Topologie zu definieren, müssen wir homogene Ideale betrachten, das heißt Ideale, deren Erzeuger homogene Polynome sind, denn die Nullstellenmengen dieser Ideale sind auf den Äquivalenzklassen wohldefiniert. Für die Topologie nehmen wir als abgeschlossene Mengen die Nullstellenmengen von homogenen Idealen und nennen diese wieder algebraische Mengen. Die irreduziblen Mengen werden wiederum als Varietäten bezeichnet. Insbesondere nennen wir den Schnitt einer projektiven Varietät mit einer offenen Menge eine quasi-projektive Varietät. Wie im affinen Fall erhalten wir wieder eine bijektive Abbildung I zwischen der Menge der algebraischen Mengen von $\mathbb{P}^n$ und der Menge der homogenen Radikalideale von $k[x_0, \ldots, x_n]$, jedoch ohne das Ideal $(x_0, \ldots, x_n)$. Die Umkehrabbildung von I bezeichnen wir wie im Affinen mit V. Dabei werden abermals irreduzible algebraische Mengen auf homogene Primideale (ohne das Ideal $(x_0, \ldots, x_n)$) abgebildet und umgekehrt. Siehe hierzu [CLS, Chapter 8, Paragraph 3, Theorem 10].
Betrachten wir nun die offenen Mengen $U_i := \mathbb{P}^n - V((x_i))$ mit $i \in \{0, \ldots, n\}$. Sei $P = (a_0, \ldots, a_n)$ ein Punkt aus $\mathbb{P}^n$. Da mindestens eine Koordinate von P, zum Beispiel a_i, ungleich 0 sein muss, ist P für diesen Index i aus U_i. Die $U_i, i \in \{1, \ldots, n\}$ bilden also eine endliche Überdeckung von $\mathbb{P}^n$. Durch die Abbildungen

$$\phi_i : U_i \to \mathbb{A}^n,\ \phi_i((a_0, \ldots, a_n)) := (\tfrac{a_0}{a_i}, \ldots, \tfrac{a_{i-1}}{a_i}, \tfrac{a_{i+1}}{a_i}, \ldots, \tfrac{a_n}{a_i})$$

wird ein Homöomorphismus von U_i auf $\mathbb{A}^n$ definiert. Die Umkehrabbildung wird durch $(x_1, \ldots, x_n) \mapsto (x_1, \ldots, x_i, 1, x_{i+1}, \ldots, x_n)$ gegeben. Jeder projektive Raum kann also durch endlich viele affine Räume überdeckt werden. Insbesondere können wir jede projektive Varietät V durch affine Varietäten $V_i = U_i \cap V$ überdecken. Die Ideale $I(V_i)$ erhält man, indem man im homogenen Ideal $I(V) = (f_j(x_0, \ldots, x_n), j \in \{1, \ldots, s\})$ die i-te Koordinate x_i durch 1 ersetzt. Demzufolge ist $I(V_i)$ gleich $(f_j(x_0, \ldots, x_{i-1}, 1, x_{i+1}, \ldots, x_n) | f_j \in V j \in \{1, \ldots, s\})$. Umgekehrt erhält man aus dem zu einer affinen Varietät V gehörenden Ideal I den projektiven Abschluss $\overline{V}$, die kleinste algebraische Menge, die V enthält, indem man $< \{x_0^{deg(f)} f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) | f \in I\} >$, das Erzeugnis der homogenisierten Elemente von I, bildet. Dieses homogene Ideal kann man berechnen, indem man eine Gröbner Basis eines Erzeugendensystems von I bezüglich einer graduierten Ordnung berechnet und dessen Erzeuger homogenisiert. Eine graduierte Ordnung ist dabei eine Ordnung, bei der die Monome zuerst nach dem Totalgrad geordnet werden. Man hat folgende Proposition.

Proposition 1.1
Sei V eine n-dimensionale affine Varietät und $\overline{V}$ ihr projektiver Abschluss in $\mathbb{P}^n$, dann gilt:

i) $\overline{V} \cap U_0 = V$.

ii) Ist V irreduzibel, so auch $\overline{V}$.

Beweis:
Siehe [CLS, Chapter 8,Paragraph 4, Proposition 7, p. 381].

□

Die oben beschriebene kleinste algebraische Menge $\overline{V}$, die V enthält, ist also eine projektive Varietät.

1.2.2 Morphismen

Seien $X \subset \mathbb{A}^n$ und $Y \subset \mathbb{A}^m$ affine Varietäten. Wir nennen die Abbildung $\phi : X \to Y$ einen Morphismus von X nach Y, falls es Polynome $f_1, \ldots, f_s$ aus $k[x_1, \ldots, x_n]$ gibt, so dass $\phi(P) = (f_1(P), \ldots, f_s(P))$ für alle $P \in X$. Morphismen sind stetig in der Zariski-Topologie. Sie induzieren k-Algebrahomomorphismen von A[Y] nach A[X]. So erhält man zum Beispiel von obigem Morphismus ϕ den Homomorphismus $\phi^* : A[Y] \to A[X]$, der das Polynom $g(y_1, \ldots, y_m)$ in die Nebenklasse von $g(f_1, \ldots, f_m)$ abbildet. Umgekehrt liefert jeder k-Algebrahomomorphismus $\lambda : A[Y] \to A[X]$ einen Morphismus $\phi : X \to Y$. Sind $y_1, \ldots, y_m$ die Erzeuger von $A[Y]$, und $f_1, \ldots, f_m)$ deren Bilder im Koordinatenring von X. Seine $f_1^{'}, \ldots, f_m^{'}$ Repräsentanten der $f_1, \ldots, f_m$ und ist P ein Punkt von X. Dann liegen $f_1'(P), \ldots, f_m'(P)$ in Y und $\phi = (f_1', \ldots f_m')$ liefert einen Morphismus von X nach Y. Es gilt dabei $\phi^* = \lambda$. Einen Morphismus $\phi : X \to Y$ nennen wir einen Isomorphismus, falls ein Morphismus $\psi : Y \to X$ existiert, so dass $\phi \circ \psi$ die Identität auf Y und $\psi \circ \phi$ die Identität auf X ist. Es gilt dann offenbar:

Satz 1.9
Die Varietäten X und Y sind genau dann isomorph, wenn $A[X]$ und $A[Y]$ isomorphe k-Algebren sind.

Beweis:
Siehe [LG, Part II, Chapter I, Proposition 1.1, p. 37] oder [Ha, Chapter I, Paragraph 3, Corrollary 3.7 oder 3.8].

□

Sei nun P ein Punkt einer affinen (beziehungsweise projektiven) Varietät X. Wir nennen eine stetige Funktion $\phi : X \to \mathbb{A}^1$ regulär bei P, wenn es eine offene Umgebung U von P und Polynome f und g aus $k[x_1, \ldots, x_n]$ (beziehungsweise homogene Polynome f und g aus $k[x_0, \ldots, x_n]$ vom gleichen Grad) gibt, so dass $g(P) \neq 0$ in U und $\phi = \frac{f}{g}$ in U ist. Die Abbildung ϕ heißt regulär auf $V \subset X$, wenn sie regulär in jedem Punkt von U ist. Die regulären Funktionen auf U bilden einen Ring, den wir mit $O_X(U)$ oder einfach $O(U)$ bezeichnen. Seien U eine offene Umgebung von P und f eine reguläre Funktion auf U, Die Äquivalenzklassen von Paaren (U, f), unter der Äquivalenzrelation

$$(U, f) \sim (V, g) \Leftrightarrow f \text{ und } g \text{ stimmen auf } U \cap V \text{ überein,}$$

bilden einen Ring O_p, den wir den lokalen Ring von P nennen. Dies ist ein lokaler Ring im algebraischen Sinn. Er enthält also genau ein maximales Ideal $\mathfrak{m}_p$. Den

Restklassenkörper $k(P) = O_P/\mathfrak{m}_P$ nennen wir den Restklassenkörper von P. Der lokale Ring O_P ist isomorph zu $A[X]_{\mathfrak{m}_p}$, die Lokalisierung von $A[X]$ bei $\mathfrak{m}_p$.

Betrachten wir nun für eine quasi-projektive Varietät X die Paare (U, f) nichtleerer, offener Teilmengen von X und regulärer Funktionen auf U. Die Äquivalenzklassen solcher Paare unter der Äquivalenzrelation

$$(U, f) \sim (V, g) \Leftrightarrow f \text{ und } g \text{ stimmen auf } U \cap V \text{ überein}$$

bilden einen Körper, den Funktionenkörper $k(X)$ von X. Die Äquivalenzklassen nennen wir rationale Funktionen. Ist X affin, so stimmt $k(X)$ mit dem Quotientenkörper von A[X] überein. Seien nun X und Y (quasi-)projektive Varietäten. Eine stetige Abbildung $\phi : X \to Y$ heißt Morphismus, falls für alle offenen Teilmengen U von Y und reguläre Funktionen $g \in O(U)$ die Hintereinanderausführung $\phi \circ g : \phi^{-1}(U) \to \mathbb{A}^1$ regulär ist. Dieser Begriff stimmt im affinen Fall mit dem oben definierten überein. Wir betrachten wieder Paare (U, f), wobei U eine nichtleere offene Menge von X und $f : U \to Y$ ein Morphismus ist. Eine Äquivalenzklasse der Äquivalenzrelation

$$(U, f) \sim (V, g) \Leftrightarrow f \text{ und } g \text{ stimmen auf } U \cap V \text{ überein}$$

heißt rationale Abbildung von X nach Y. Wir nennen eine rationale Abbildung ϕ dominant, wenn das Bild $\phi(X)$ von X unter ϕ dicht in Y ist. Dabei ist $\phi(X)$ die Menge der Punkte $P \in Y$ so dass es ein Paar (U, f) einer nichtleerern offenen Menge $U \subset X$ und eines Morphismus $f : U \to Y$ gibt, so dass P das Bild eines Punktes P' aus U unter f ist. In diesem Fall induziert die rationale Abbildung ϕ einen k-Algebrahomomorphismus $\phi^* : k(X) \to k(Y)$ zwischen den Funktionenkörpern von $k(X)$ und $k(Y)$. Umgekehrt kann aus jedem k-Algebrahomomorphismus $\phi : k(Y) \to k(X)$ eine dominante rationale Abbildung von X nach Y konstruiert werden. Man wählt dazu eine offene Umgebung U von Y . Die Bilder der Erzeuger von $A[U]$ sind dann regulär für eine offene Menge V von X. Damit erhält man einen k-Algebrahomomorphismus von $A[U]$ nach $A[X]$, also einen Morphismus von X nach Y. Zwei Varietäten heißen birational äquivalent, wenn es rationale Abbildungen $\phi : X \to Y$ und $\psi : Y \to X$ gibt, so dass $\phi \circ \psi$ die Identität auf einer offenen Menge von Y und $\psi \circ \phi$ die Identität auf einer offenen Menge von X ist. Es gilt also:

Satz 1.10
Zwei Varietäten X und Y sind genau dann birational äquivalent, wenn ihre Funktionenkörper $k(X)$ und $k(Y)$ als k-Algebren isomorph sind.

□

1.2.3 Die Dimension von Varietäten

Sei X eine affine Varietät. Dann wird die natürliche Zahl $n = dim(X)$ die Dimension von X genannt, wenn die drei folgenden äquivalenten Bedingungen erfüllt sind.

i) (topologisch) n ist das Supremum der Länge von Ketten $X_0 \subsetneq \ldots \subsetneq X_n \subsetneq X$ irreduzibler abgeschlossener Mengen von X.

ii) (algebraisch) n ist das Supremum der Länge von Ketten $\mathfrak{p}_0 \subsetneq \ldots \subsetneq \mathfrak{p}_n = I(X)$ von Primidealen in A[X].

iii) n ist der Transzendenzgrad des Funktionenkörpers K(X) von X über K. (Siehe hierzu [Ha, p. 5f]).

Die Dimension des projektiven Abschlusses von X stimmt mit der von X überein. Sie ist eine birationale Invariante. Insbesondere sind die Dimensionen von $\mathbb{A}^n$ und $\mathbb{P}^n$

gleich n. Varietäten der Dimension 1 nennen wir Kurven. Die Funktionenkörper von Kurven haben also Transzendenzgrad 1. Umgekehrt gehört zu jedem algebraischen Funktionenkörper vom Transzendenzgrad 1 eine Kurve. Hierzu mehr im nächsten Abschnitt.

1.2.4 Kurven

Sei P ein Punkt auf einer Kurve X und U eine offene affine Teilmenge von X, die P enthält. Seien ferner $f_1, \dots, f_m \in k[x_1, \dots, x_n]$ die Erzeuger von $I(U)$. Wir nennen dann P nicht singulär oder regulär, wenn die nachstehenden drei äquivalenten Bedingungen erfüllt sind.

i) Die Matrix $(\frac{\partial f_i}{\partial x_j})_{i \in \{1,\dots,m\}; j \in \{1,\dots,n\}}$ hat den Rang $n-1$.

ii) Der lokale Ring O_P ist ein diskreter Bewertungsring.

iii) Der $k(P)$-Modul $\mathfrak{m}_P/\mathfrak{m}_P^2$ hat Dimension 1.

Sonst nennen wir P einen singulären Punkt. Sind alle Punkte von X nicht-singulär, so nennen wir X nicht-singulär. Hat X einen singulären Punkt, so nennen wir X singulär. Da die Menge der singulären Punkte einer Varietät eine echte, abgeschlossene Teilmenge dieser Varietät ist, kann es auf jeder Kurve nur endlich viele singuläre Punkte geben (Siehe [Ha, Chapter I, Paragraph 5, Theorem 5.3].). Falls P ein nicht singulärer Punkt ist, so können wir, da O_P ein Bewertungsring ist, alle Elemente f von O_P in der Form $f = t^n m_p$ darstellen. Dabei ist t ein geeignetes Element aus O_P, n eine natürliche Zahl und m_P ein Erzeuger des maximalen Ideals $\mathfrak{m}_P$ in O_P. Die Zahl n ist unabhängig von der Wahl des Erzeugers und ist eindeutig bestimmt. Sie wird auch mit $\nu_P(f)$ bezeichnet (ν_P ist dann die Bewertung des Bewertungsrings O_P). Wir nennen t einen lokalen Parameter bei P. Betrachten wir den Fall einer ebenen Kurve X, die durch ein Polynom f aus $k[X,Y]$ gegeben ist. Sei P ein Punkt von X und $T = aX + bY + c$ eine Gerade durch den Punkt P. Dann ist für jede solche Gerade, die keine Tangente von X im Punkt P ist, $t = aX + bY + c \in k[X,Y]/(f)$ ein lokaler Parameter bei P. Vergleiche hierzu auch [Fu, Chapter 3.2, Theorem 1, p 70f]. Zwischen den Punkten einer nicht-singulären projektiven Kurve und den lokalen Ringen des zugehörigen algebraischen Funktionenkörpers vom Transzendenzgrad eins gibt es also eine bijektive Abbildung.

Sei nun P ein nicht-singulärer Punkt und t_P ein lokaler Parameter bei P. Es gibt eine eindeutig bestimmte Einbettung ξ_P von O_P in den Ring der Potenzreihen $k[[T_p]]$ über k, so dass für eine im Punkt P reguläre Funktion f und eine natürliche Zahl n die Differenz $f - \sum_{i=1}^{n} \alpha_i t_p^i$ in $\mathfrak{m}_P^{n+1}$ liegt, wobei $\xi_P(f)$ gleich $\sum_{i=1}^{n} \alpha_i T_p^i$ ist ([Sha, Chapter II, 2, p.84ff]). Jede rationale Funktion kann also in jedem nicht-singulären Punkt eindeutig in einer Laurent-Reihe entwickelt werden.

Im Hinblick darauf und auf Satz 1.10 wollen wir einen algebraischen Funktionenkörper vom Transzendenzgrad eins auch als abstrakte Kurve oder einfach als Kurve bezeichnen. Durch die algebraischen Funktionenkörper vom Transzendenzgrad eins werden die birationalen Äquivalenzklassen von Kurven klassifiziert. Einen Repräsentanten dieser Klasse, sei er nun durch eine Varietät oder sein erzeugendes Ideal gegeben, nennen wir Modell der Kurve. Insbesondere gibt es zu jeder abstrakten Kurve ein nicht-singuläres projektives Modell, (Siehe hierzu auch [Ha] I,6, Corollary 6.11.). Das dieses Modell definierende Ideal ist nicht eideutig bestimmt ist und hängt von der Einbettung in den projektiven Raum ab.

Bemerkung 1.3

Genauer gilt: Die Kategorie der Funktionenkörper vom Transzendenzgrad eins über einem algebraisch abgeschlossenen Körper k mit k-Homomorphismen ist äquivalent zur Kategorie der nicht-singulären projektiven Kurven mit nicht konstanten Morphismen.

□

1.2.5 Kurven über nicht algebraisch abgeschlossenen Körpern

Sei k ein nicht algebraisch abgeschlossener, perfekter Körper. Wir interessieren uns hier für den Fall eines endlichen Körpers $\mathbb{F}_q$, wobei q die Potenz einer Primzahl p sei. Sei ferner $\overline{k}$ der algebraische Abschluss von k und $G = Gal(\overline{k}/k)$ die Galois-Gruppe von $\overline{k}$ über k. Diese operiert auf $\mathbb{A}^n(\overline{k})$ vermöge der Abbildung

$$\mathbb{A}^n(\overline{k}) \ni P = (x_1, \dots, x_n) \mapsto \sigma P = (\sigma x_1, \dots, \sigma x_n) \text{ mit } \sigma \in Gal(\overline{k}/k) \text{ und } x_i \in \overline{k}.$$

Da die Galoisgruppe trivial auf k operiert gilt: $\sigma P = P$ für alle $P \in \mathbb{A}^n(k)$ und $\sigma \in G$. Für Polynome aus $k[x_1, \dots, x_n]$ und $P \in \mathbb{A}^n(\overline{k})$ gilt $f(\sigma P) = \sigma f(P)$, da σ auf den Koeffizienten von f trivial operiert.

Wir sagen die Kurve $X \subset \mathbb{A}^n(\overline{k})$ (beziehungsweise $X \subset \mathbb{P}^n(\overline{k})$) sei über k definiert, wenn das Ideal $I(X)$ durch Polynome $f_1, \dots, f_m$ aus $k[x_1, \dots, x_n]$ (beziehungsweise durch homogene Polynome $f_1, \dots, f_m$ aus $k[x_0, \dots, x_n]$) erzeugt werden kann. In diesem Fall nennen wir $X(k) = X \cap \mathbb{A}^n(k) = \{P \in X |$ die Koordinaten von P sind aus $k\}$ (beziehungsweise $X(k) = X \cap \mathbb{P}^n(k) = \{P \in X|$ Es gibt homogenen Koordinaten von P, die aus k sind $\}$) die Menge der k-rationalen Punkte von X.

Sei nun $X \subseteq \mathbb{A}^n$ über k definiert. Dann definieren wir $I(X/k) = I(X) \cap k[x_1, \dots, x_n]$, $k[X] = k[x_1, \dots, x_n]/I(X/k)$ und $k(X) = Quot(k[X]) \subseteq \overline{k}(X)$. Analog gehen wir im projektiven Fall vor. Der Ring $k[X]$ (beziehungsweise $k(X)$) ist der unter der Operation von G invariante Unterring von $\overline{k}[X]$ (beziehungsweise $\overline{k}(X)$).

Sei X nun eine nicht-singuläre Kurve. Dies können wir annehmen, da wir uns ein nicht-singuläres Modell von $\overline{k}(X)$ wählen können. Dann ist für einen Punkt P aus X (P hat also nicht notwendig Koordinaten in k) $O_P(k) = \{f \in k(X)|$ f ist regulär in P $\} = O_P(\overline{k}) \cap k(X)$ ein diskreter Bewertungsring mit maximalem Ideal $M_P(k) = \{f \in O_P(k) | f(P) = 0\} = M_P(\overline{k}) \cap k(X)$. Der Restklassenkörper $k(P) = O_P(k)/M_P(k)$ ist eine endliche algebraische Erweiterung von k. Sei der Grad dieser Erweiterung d und seien $P = \sigma_1(P), \sigma_2(P), \dots, \sigma_d(P)$ die Konjugierten von P unter $Gal(k(P)/k)$ in $\overline{k}$. Dies sind dann d Punkte vom Grad Eins über k'. Die Gesamtheit P' dieser Punkte über k' nennen wir einen abgeschlossenen Punkt vom Grad d. Da wir X auch als algebraischen Funktionenkörper vom Transzendenzgrad eins auffassen können, für den die Bewertungsringe in Bijektion mit den abgeschlossenen Punkten der Kurve X stehen, können wir $O_{P'}(k)$ oder die zugehörige Bewertung auch als abgeschlossenen Punkt bezeichnen. Für einen algebraisch abgeschlossenen Körper k haben alle abgeschlossenen Punkte einer Kurve über k den Grad Eins. Im anderen Fall entspricht der abgeschlossene Punkt P aus $\overline{k}$ den Konjugierten unter $Gal(\overline{k}/k)$. Dies sind $deg(P)$ Punkte (Diese haben in $X(\overline{k})$ Grad eins).

1.2.6 Divisoren, Differenziale und Satz von Riemann-Roch

Sei X eine glatte projektive Kurve über k. Die Elemente der freien abelschen Gruppe $Div_k(X)$, formale endliche Summen von Punkten von X, die die Form $D = \sum\limits_{P \in X(k)} n_P P$ mit $n_P \in \mathbb{Z}$ haben, nennen wir Divisoren von X. Die Menge $Supp(D) = \{P \in X | n_P \neq 0\}$ ist endlich und heißt Träger von D. Ist $k' \subset k$ und X

über k' definiert, so nennen wir einen Divisor k'-rational, wenn er das Bild eines Divisors von $Div_{k'}(X)$ unter der natürlichen Einbettung $Div_{k'}(X) \rightarrow Div_k(X)$ ist. Wir nennen einen Divisor effektiv, falls alle seine Koeffizienten n_P größer gleich null sind. Der Grad eines Divisors ist definiert durch $deg(D) = \sum_{p \in X} n_P deg(P)$. Sei f eine rationale Funktion auf X, dann definiert $(f) = \sum_{P \in X} \nu_P(f) P$ einen Divisor, den wir den Divisor von f nennen. Es gilt $deg((f)) = 0$. Die Menge $\{(f) | f \in k(X)^*\}$ bildet eine Untergruppe von $Div(X)$, deren Quotientengruppe $Pic(X) = Div(X)/\{(f)|f \in k(X)^*\}$ wir mit Picardgruppe oder Divisorenklassengruppe bezeichnen. Ihre Elemente sind Klassen von Divisoren unter der Äquivalenzrelation

$$D \sim D' \Leftrightarrow D - D' = (f) \text{ für ein } f \in k(X)^*.$$

Man nennt diese Äquivalenzrelation lineare Äquivalenz. Jedem Divisor D ordnen wir einen endlichdimensionalen k-Vektorraum zu, $L(D) = \{f \in k(X)^* | (f) + D$ ist effektiv $\} \cup \{0\}$. Die Dimension $l(D)$ des Vektorraumes $L(D)$ können wir mit Hilfe des Satzes von Riemann-Roch berechnen, auf den wir später noch zurückkommen werden.

Betrachten wir nun wieder eine Varietät. Jeder affinen Varietät V läßt sich in eindeutiger Weise ein $k[V]$-Modul $\Omega[V]$ und eine Abbildung $d : k[V] \rightarrow \Omega[V]$ zuordnen, so dass gilt:

i) $\Omega(V)$ wird von allen $d(f)$ erzeugt, $f \in k[V]$

ii) $d(f + g) = d(f) + d(g)$ für $f, g \in k[V]$

iii) $d(fg) = fd(g) + gd(f)$

iv) $d(a) = 0$ für alle $a \in k$

Die Elemente von $\Omega[V]$ nennen wir reguläre Differenzialformen und schreiben anstatt $d(f)$ auch kürzer df. Eine regulaere Differentialform ω kann auch als Abbildung $\omega : X \rightarrow \bigcup_{P \in X} \mathfrak{m}_P/\mathfrak{m}_P^2$ aufgefasst werden, die in einer geeigneten Umgebung von P durch $Q \mapsto (f - f(Q)) \bmod \mathfrak{m}_Q^2$ für ein in der Umgebung regunläres $f \in k[X]$ gegeben ist. Siehe hierzu auch [Sha, Paragraph 4, p. 156ff]. Für projektive Varietäten V betrachten wir eine offene, affine Überdeckung $\{U_i\}$ von V und nennen die Äquivalenzklassen von Paaren (U_i, ω_i) ,ω_i sei eine reguläre Differenzialform auf U_i, unter der Äquivalenzrelation

$$(U_i, \omega_i) \sim (U_j, \omega_j) \Leftrightarrow \text{auf } U_i \cap U_j \text{ gilt: } \omega_i = \omega_j.$$

eine reguläre Differenzialform und schreiben für die Menge der Äquivalenzklassen ebenfalls $\Omega[X]$. Ist nun V wieder eine Kurve, so können wir analog zur Definition der rationalen Funktionen die rationalen Differenzialformen definieren. Dies sind die Äquivalenzklassen von Paaren (U, ω) einer nichtleeren, offenen, affinen Teilmengen von X, und einer regulären Differenzialform ω auf U unter der Äquivalenzrelation

$$(U, \omega) \sim (V, \eta) \Leftrightarrow \omega \text{ und } \eta \text{ sind auf } U \cap V \text{ gleich.}$$

Für affine Varietäten ist der $k(X)$-Modul der rationalen Differenzialformen gleich $k(X)\Omega[X]$. Er wird erzeugt durch die Elemente $d(\frac{g}{h})$ mit $\frac{g}{h} \in k(X)$ und es gilt $d(\frac{g}{h}) = \frac{hdg - gdh}{h^2}$. Sei nun ω eine geeignete Differenzialform auf X. Auf einer geeigneten Umgebung von P ist $\Omega[U]$ ein freier $A[U]$-Modul mit Erzeuger dt, wobei t ein lokaler Parameter von O_P ist. Wir können ω in einer geeigneten Umgebung des Punktes P als $\omega = f_P dt_P$ interpretieren, wobei f_P eine rationale Funktion und t_P ein lokaler Parameter bei P ist. Wir definieren nun den Divisor von ω als

$(\omega) = \sum_{P \in X} \nu_P(f_P)P$. Die Divisoren der rationalen Differenzialformen von X liegen alle in einer linearen Äquivalenzklasse. Diese nennen wir die kanonische Divisorenklasse. Ihre Elemente nennen wir kanonische Divisoren und bezeichnen sie meist mit κ. Die Dimension des k-Vektorraumes $L(\kappa)$ ist unabhängig von der Wahl von κ und wird als Geschlecht $g = dim_k(L(\kappa))$ von X bezeichnet. Es ist eine birationale Invariante. Falls k'/k eine separable Körpererweiterung ist, wie dies für die endlichen Körper der Fall ist, so ist das Geschlecht X über k' gleich dem Geschlecht von X über k. Der Satz von Riemann-Roch besagt nun:

Satz 1.11
Für eine nicht singuläre, projektive Kurve X vom Geschlecht g gilt: $l(D) = deg(D) + 1 - g + l(\kappa - D)$. Dabei ist κ ein kanonischer Divisor von X.

Beweis:
Siehe [St, Chapter I, Paragraph 5, Theorem I.5.15 , p. 28] oder [Ha, Chapter IV, Papagraph 1, Theorem 1.3].

□

Dabei gilt insbesondere:

Lemma 1.2
Ist der Grad des Divisors D größer als $2g - 2$, so hat der Raum $L(\kappa - D)$ die Dimension null. Also gilt $l(D) = deg(D) + 1 - g$.

□

1.3 Riemannsche Flächen

Eine Riemannsche Fläche ist eine eindimensionale, zusammenhängende, komplexe Manigfaltigkeit, genauer: ein zusammenhängender Hausdorff Raum X, auf dem eine komplexe Struktur S definiert ist, die die folgenden Eigenschaften hat:

(i) S ist eine Familie von Paaren (U_α, ϕ_α), wobei $\{U_\alpha\}_{\alpha \in A}$ eine offene Überdeckung von X mit der Indexmenge A ist, und für alle α ist das Bild der Homöomorphismen ϕ_α eine offene Teilmenge von $\mathbb{C}$.

(ii) Falls für α und β aus A die beiden Mengen U_α und U_β nicht leeren Schnitt haben, dann ist die Abbildung

$$\phi_\alpha \circ \phi_\beta^{-1} : \phi_\alpha(U_\alpha \cap U_\beta) \to \phi_\beta(U_\alpha \cap U_\beta)$$

biholomorph.

Dabei heißen zwei komplexe Strukturen äquivalent, wenn ihre Vereinigung ebenfalls eine komplexe Struktur ist. Abbildung 1.1 verdeutlicht die Situation.

Wir wollen nun zeigen, dass der Begriff der glatten Kurve über den komplexen Zahlen und der Begriff der Riemannschen Fläche im Wesentlichen äquivalent sind. Wir folgen hier dem Kapitel 2.1.5 aus [Ts]. Sei dazu X eine quasi-projektive Kurve über den komlexen Zahlen. Wir wollen nun eine komplexe Topologie auf X definieren. Dazu nehmen wir an, dass X in $\mathbb{P}^n(\mathbb{C})$ eingebettet sei. Der affine Raum $\mathbb{A}^n(\mathbb{C}) \cong \mathbb{C}^n$ ist homöomorph zum $\mathbb{R}^{2n}$, welcher mit einer Topologie ausgestattet ist. Die Topologie des $\mathbb{P}^n(\mathbb{C})$ definieren wir nun als Quotiententopologie unter der kanonischen Abbildung $\pi : \mathbb{A}^{n+1}(\mathbb{C}) - \{0\} \to \mathbb{P}^n(\mathbb{C})$, das heißt eine Menge U in $\mathbb{P}^n(\mathbb{C})$ ist genau dann offen, wenn ihre Urbildmenge $\pi^{-1}(U)$ offen ist. Da die Einschränkung

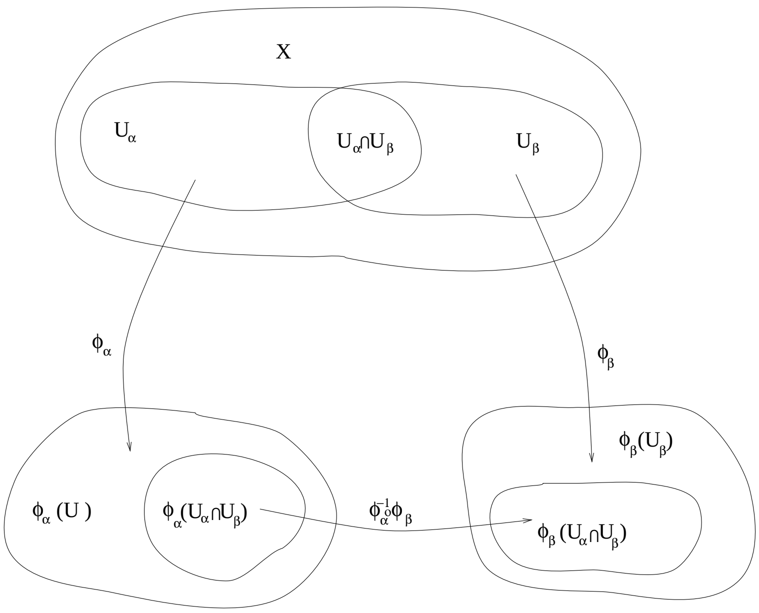

Abbildung 1.1: Komplexe Struktur einer Riemannschen Fläche

von π auf die Einheitskugel $S^{2n+1} = \{(z_0, \ldots, z_n) \in \mathbb{A}^{n+1}(\mathbb{C}) - \{0\} | \sum_{i=1}^{n} z_i^2 = 1\}$ surjektiv ist, ist mit S^{2n+1} auch $\mathbb{C}^n$ kompakt. Die komplexe Topologie auf X sei nun als die Einschränkung der oben beschriebenen Topologie definiert. Falls X projekiv ist, so ist es eine abgeschlossene Teilmenge von $\mathbb{P}^n(\mathbb{C})$. Da die Kurve X als Schnitt von Nullstellenmengen stetiger Funktionen auf $\mathbb{P}^n(\mathbb{C})$ definiert ist, ist sie kompakt in der komplexen Topologie. Sei nun P ein Punkt von X. Dieser ist nicht singulär, da X als glatt angenommen wurde. Sei weiter $U \subset \mathbb{A}^n(\mathbb{C})$ eine offene affine Umgebung von P und t_P ein lokaler Parameter von X bei P. Da t_P eine rationale,insbesondere reguläre Funktion ist, gibt es ein $\epsilon > 0$, so dass $U_\epsilon := \{Q \ inX | t_P(Q) < \epsilon\}$ stetig auf $\mathbb{C}$ abgebildet wird. Seien nun $t_1, \ldots, t_n$ die Einschränkungen der Koordinatenfunktionen von $\mathbb{A}^n$ auf X und $\Phi_i(t)$ die Potenzreihenentwicklung von t_i bei P. Man kann nun zeigen, dass $\Phi_i(t)$ auf einer Kugel vom Radius ϵ_i konvergiert. Wir definieren die Abbildung $u : \mathbb{C} \supset D_\epsilon \to \mathbb{A}^n(\mathbb{C})$ durch $u(t) \mapsto (\Phi_1(t), \ldots, \Phi_n(t))$, wobei D_ϵ eine Kugel vom Radius $\epsilon = \min_i \epsilon_i$ um null in $\mathbb{C}$ ist. Weiter kann nun gezeigt werden, dass $t_P \circ u$ in einer Umgebung $V_P \subset \mathbb{C}$ der Null und $u \circ t_P$ in einer Umgebung U_P von P gleich der Identität sind. t_P ist also ein Homöomorphismus von U_P nach V_P. Die Situation wird in Abbildung 1.2 verdeutlicht. Da insbesondere t_P und die Einbettung von X in $\mathbb{P}^n(\mathbb{C})$ beliebig gewählt waren, hängt die komplexe Topologie der Kurve weder von der Wahl des lokalen Parameters noch von der Einbettung der Kurve X in den projektiven Raum ab. Die Familie der Paare $(U_P, u_P), p \in X$ ist eine komplexe Struktur auf X. Um zu zeigen, dass X zusammen mit der komplexen Topologie eine Riemannsche Fläche ist, muss noch gezeigt werden, dass X zusammenhängend ist. Einen Beweis hierfür findet sich zum Beispiel in [Ts, Theorem 2.1.84, p. 137]. Wir nennen die so konstruierte Riemannsche Fläche die zu X assoziierte Riemannsche Fläche. Diese Konstruktion kann im kompakten Fall umgekehrt werden.

Satz 1.12
Sei Y eine kompakte Riemannsche Fläche, dann gibt es eine, bis auf Isomorphie eindeutig bestimmte, (glatte,) projektive Kurve X, so dass Y zu der zu X assoziierten Riemannschen Fläche homöomorph ist.

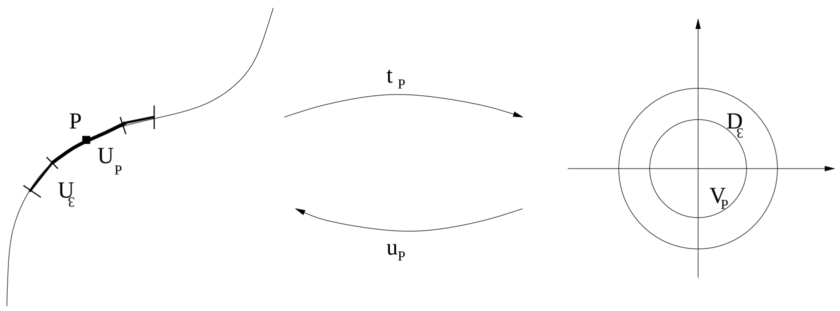

Abbildung 1.2: Homöomorphismus der komplexen Struktur auf einer Kurve X in die komplexe Ebene

Siehe hierzu auch [Gu, Chapter X, p. 239ff].

□

Bemerkung 1.4

In der Sprache der Kategorien heißt dies, dass die Kategorie der Riemannschen Flächen zusammen mit komplex analytischen Abbildungen und die Kategorie der glatten projektiven Kurven über den komplexen Zahlen zusammen mit regulären Abbildungen äquivalent sind.

□

1.3.1 Weierstraß-Punkte

Sei X eine glatte projektive Kurve. Ein Divisor D aus $Pic(X)$ nennen wir speziell, falls $l(\kappa - D) > 0$ ist. Ansonsten nennen wir ihn nicht speziell.

Lemma 1.3
Jeder Divisor D vom Grad größer oder gleich $2g-1$ ist nicht speziell, und jeder Divisor vom Grad kleiner als $g-2$ ist speziell.

□

Sei nun weiter $P \in X$ ein Punkt von X und $a \geq 1$ eine natürliche Zahl. Wir nennen a eine Lücke von P, wenn $l(aP) = l((a-1)P)$ gilt. Sonst nennen wir a eine Nichtlücke von P. Die Zahl a ist also eine Nichtlücke von P, wenn es ein $f \in k(X)$ gibt, mit $\nu_P(f) = a$. Gibt es dies nicht, so ist a eine Lücke von P.

Lemma 1.4

i) Es gibt g Lücken von P.

ii) Eins ist eine Lücke von P.

iii) Jedes $a \geq 2g$ ist eine Nichtlücke von P.

iv) Sind a und b Nichtlücken von P, so ist auch $a+b$ eine Nichtlücke von P.

□

Die Folge $\{a_1, \ldots, a_g\}$ der Lücken von P nennen wir Lückenfolge von P. Der Punkt P heißt Weierstraß-Punkt, wenn die Lückenfolge von P nicht mit $\{1, \ldots, g\}$ übereinstimmt. P ist genau dann ein Weierstraß-Punkt, wenn gP ein spezieller Divisor ist, beziehungsweise genau dann, wenn aP für ein $a \geq g$ speziell ist. Die Anzahl $w(X)$ der Weierstraß-Punkte von X ist endlich. Ist X hyperelliptisch und $char(k) \neq 2$, so ist $w(X) = 2g+2$ und die Lückenfolge der Weierstraß-Punkte ist $\{2, 4, \ldots, 2g-2\}$.

1.4 Algebraisch-geometrische Codes

Im Weiteren sollen die Parameter n, d und k eines Codes auch mit len, dim und dis bezeichnt werden. In diesem Abschnitt beschreiben wir die Konstruktion und grundlegende Eigenschaften von algebraisch-geometrischen Codes. Dabei folgen wir im Wesentlichen [TV], Chapter 3.1. Es gibt mehrere Arten lineare Codes aus algebraischen Kurven zu konstruieren. Diese sind im Wesentlichen äquivalent. Wir werden uns hier nur mit der L-Konstruktion beschäftigen.

Sei X eine projektive, glatte und absolut irreduzible Kurve über einem endlichen Körper $\mathbb{F}_q$. Ferner sei $X(\mathbb{F}_{q^i})$ die Menge der $\mathbb{F}_{q^i}$-rationalen Punkte von X und $D_i = \{P_1, \ldots, P_{n_i}\}$ eine Teilmenge von $X(\mathbb{F}_{q^i})$. $G \in Div(X)$ ein Divisor von X mit Grad $a \in \{0, \ldots, n_i - 1\}$, so dass der Schnitt des Trägers $Supp(G)$ von G mit D_i leer ist. Dann erhalten wir mittels der linearen Abbildung:

$$\begin{aligned} Ev_D : L(D) &\to \mathbb{F}_q^n \\ f &\mapsto (f(P_1), \ldots, f(P_n)) \end{aligned}$$

einen linearen Code, den wir mit $C_L(X, D_i, G)$ bezeichnen wollen.

Bemerkung 1.5

i) Ein zu G linear äquivalenter Divisor G', für den $Supp(G')$ ebenfalls einen leeren Schnitt mit D hat, liefert einen äquivalenten Code.

ii) Die Voraussetzung, dass $Supp(G)$ und D leeren Schnitt haben, kann umgangen werden (siehe zum Beispiel [TV, Chapter3.1, p. 271ff] oder [LG, Part II, III, Remark, p 55]).

□

Über die Parameter dieser Codes macht der folgende Satz eine Aussage.

Satz 1.13
Sei X eine Kurve mit Geschlecht g. Mit den oben gemachten Bezeichnungen und Voraussetzungen gilt für die Parameter von $C_L(X, D_i, G)$:

$$\begin{array}{lcl} len & = & n_i, \\ dim & \geq & a - g + 1 \; mit \; Gleichheit \; falls \; 2g - 1 \leq a < len, \\ dis & \geq & len - a. \end{array}$$

Beweis:
Siehe [TV, Theorem 3.1.1 und Remark 3.1.3] oder [LG, Part II, III, p. 55].

□

Bemerkung 1.6

i) Diese Abschätzungen sind keine Gleichungen. Es gilt für dim genauer: $dim = a - g + 1 + dim(L(\kappa - D))$, falls κ ein kanonischen Divisor ist. Wir haben für $a \leq 2g - 1$ also die Abschätzung $0 \leq dim \leq g$.

ii) Der Parameter für dim kann also nur verbessert werden, wenn $dim(L(\kappa - D)) > 0$ ist. Wegen Lemma 1.3 ist dies nur dann der Fall, wenn der Grad des Divisors D kleiner als $2g - 1$ ist. Zur Konstruktion guter Codes (Klassen von Codes mit asymptotisch guten Parametern) sind also insbesondere Kurven von großem Geschlecht wünschenswert. Man sucht folglich Kurven, deren Verhältnis von Punkteanzahl zum Geschlecht 'günstig' ist. Der Divisor aP ist ein spezieller Divisor, wenn P ein geeignetes Vielfaches eines Weierstraß-Punktes ist. Um gute Codes zu erzeugen, interessieren wir uns also insbesondere für Weierstraß-Punkte.

□

1.4.1 Adjungierter Divisor, Basen von L(D) und Brill-Noether Algorithmus

Dieser Abschnitt basiert im Wesentlichen auf [BR],[CF] und [HB]. Wir beschränken uns nun auf ebene, projektive und absolut irreduzible Kurven, das heißt auf Kurven C, die durch eine Form $F \in k[X,Y,Z]$ definiert sind. Durch sukzessives Blowing-up (Siehe hierzu das Kapitel vier oder [HA, Chapter I, Paragraph 4, p. 28ff]) erhalten wir ein glattes Modell C' von C, und für jeden singulären Punkt P_s von C einen Desingularisierungsbaum $\mathfrak{T}_{P_s}$ über einer endlichen Erweiterung k' von k (Siehe hierzu auch [TV, p. 230]), dessen Blätter k'-rationalen Punkten von C' entsprechen. Die Knoten dieses Baumes entsprechen singulären Punkten $P_1, \ldots, P_{n_s}$ auf einer Kurve C_i ($C_1 = C$) der Ordnung $e_{i,s}$. Die Kanten entsprechen den Blowing-up's $\pi_i : C_j \to C_i$ für ein $j \in \{1, \ldots, n_s\}$ der Kurve C_i im Punkt P_i. Sei $E_{i,s}$ der Ausnahmedivisor von π_i, das heißt der Divisor der zur Ausnahmegeraden des Blowing-up's π_i gehört. Der Träger von $E_{i,s}$ besteht also aus den gemeinsamen Punkten der Ausnahmegeraden und der direkten Transformierten von C_i. Den adjungierten Divisor $\mathfrak{A}$ definieren wir als $\sum\limits_{P_s} \sum\limits_{i=1}^{n_s} (r_{i,s} - 1) E_{i,s}$. Er ist ein k-rationaler Divisor. Sei $G \in k[X,Y,Z]$ eine Form, die nicht von F geteilt wird. Die Kurve die durch die Gleichung $G = 0$ beschrieben wird, nennen wir Adjungierte von C, wenn $(G) \geq \mathfrak{A}$ ist. Für einen beliebigen Divisor D von C' gilt dann mit obigen Notationen:

Satz 1.14
Ist G_0 eine Form vom Grad d in $k[X,Y,Z]$, so dass $(G_0) \geq \mathfrak{A} + D$ gilt, dann ist

$$L(D) = \{\overline{G}/\overline{G_0} \mid G \text{ ist eine Form vom Grad } d \in k[X,Y,Z] \text{ mit } (G) \geq (G_0) - D\} \cup \{0\}.$$

Dabei bezeichnet $\overline{G}$ die Restklasse von G im Koordinatenring von C.

Beweis:
Siehe [HB, Theorem 4.3].

□

Mit dem folgenden Algorithmus lässt sich nun eine Basis von $L(D)$ berechnen (Brill-Noether-Algorithmus).

1) Berechne den adjungierten Divisor von C, das heißt insbesondere: Suche die singulären Punkte und desingularisiere.

2) Wähle eine Form G_0 von genügend großem Grad $b \in \mathbb{N}$ so, dass G_0 nicht von F geteilt wird, $G_0 = 0$ eine Adjungierte von C definiert und $(G_0) \geq 0$ ist.

3) Berechne eine k-rationale Basis von $\{G | G$ ist eine Form vom Grad b, $(G) \geq (G_0) - D$ und G wird nicht von F geteilt$\}$.

4) Falls $\{G_0, \ldots, G_n\}$ eine Basis aus 3) ist, dann ist die Menge $\{1, \frac{\overline{G_1}}{\overline{G_0}}, \ldots, \frac{\overline{G_n}}{\overline{G_0}}\}$ eine Basis von $L(D)$.

Einige Beispiele hierzu finden sich in Kapitel 4.

Kapitel 2

Modulkurven

2.1 Operation von Gruppen auf topologischen Räumen

Sei G eine Gruppe und X ein topologischer Raum. Wir sagen G operiert stetig (von links) auf X (kurz operiert auf X), wenn es eine Abbildung $G \times X \to X$ gibt, deren Bild von (g, x) wir auch mit gx bezeichnen und für die gilt:

i) Für jedes $g \in G$ ist $x \mapsto gx$ eine stetige Abbildung.

ii) $(gh)x = g(hx)$ für je zwei Elemente g und h aus G.

iii) Für die Einheit 1 aus G gilt $1x = x$ für alle x aus X.

G operiere im Folgenden auf X. Wir nennen die Menge $G_x = \{g \in G | gx = g\}$ den Stabilisator von x in X, und ein Element x aus X nennen wir Fixpunkt von g aus G, wenn gilt: $gx = x$. Das heißt, x ist genau dann Fixpunkt von g, wenn g aus G_x ist. Für jedes Element g aus G gilt $G_{gx} = gG_xg^{-1}$, denn $gG_xg^{-1} = \{gg'g^{-1} \in G | g'x = x\} = \{gg'g^{-1} \in G | gg'g^{-1}gx = gx\} = \{g'' \in G | g''gx = gx\} = G_{gx}$. Die Menge $Gx = \{gx | g \in G\}$ nennen wir die G-Bahn von x in X. Für zwei Elemente x, y aus X gilt entweder $Gx = Gy$ oder $Gx \cap Gy = \emptyset$. Deshalb können wir X als disjunkte Vereinigung von G-Bahnen schreiben. Ist dabei insbesondere $X = Gx$ für ein x aus X, so sagen wir: G operiert transitiv auf X. Äquivalent dazu ist: Für je zwei Elemente x, y aus X existiert ein g aus G , so dass $gx = y$ ist. Die Menge der G-Bahnen schreiben wir als $G\backslash X$.

Sei nun $\pi : X \to G\backslash X$ die natürliche Projektion, die jedem x aus X seine Bahn Gx aus $G\backslash X$ zuordnet. Wir nennen eine Teilmenge U aus $G\backslash X$ offen, wenn die Teilmenge $\pi^{-1}(U)$ offen in X ist. Dies definiert eine Topologie auf $G\backslash X$, die wir Quotiententopologie nennen. $G\backslash X$ mit der Quotiententopologie nennen wir den Quotientenraum von X und schreiben dafür ebenfalls $G\backslash X$.

2.2 Gebrochen-rationale Transformationen

Sei R ein kommutativer Ring mit Eins. Die 2×2-Matrizen über R, deren Determinante eine Einheit in R ist, bilden unter Multiplikation eine Gruppe $GL(2, R)$, die wir die allgemeine lineare Gruppe nennen. Die spezielle lineare Gruppe $SL(2, R)$ ist die Untergruppe von $GL(2, R)$, die aus allen Matrizen mit Determinante eins besteht. Hier interessieren wir uns hauptsächlich für $R = \mathbb{R}$ und $R = \mathbb{Z}$. Die allgemeine lineare Gruppe $GL(2, \mathbb{R})$ und ihre Untergruppen operieren auf natürliche Weise auf $\mathbb{C} \cup \{\infty\}$ vermöge der Abbildung:

$$\begin{array}{c} GL(2,\mathbb{R}) \times (\mathbb{C} \cup \{\infty\}) \to \mathbb{C} \cup \{\infty\}, \\ (\gamma, z) \mapsto \gamma z := \frac{az+b}{cz+d}. \end{array}$$

Für Elemente ν aus der oberen Halbebene $\mathbb{H} = \{z \in \mathbb{C} | Im(z) > 0\}$ und $\gamma \in GL(2,\mathbb{R})$ folgt aus $Im(\nu) > 0$ und $det(\gamma) > 0$, dass $Im(\gamma\nu) > 0$ gilt. Also operiert $GL^{+}(2,\mathbb{R}) = \{g \in Gl(2,\mathbb{R}) \mid det(g) > 0\}$ und deren Untergruppen auf $\mathbb{H}$ Wie wir leicht feststellen können, operieren die skalaren Vielfachen der Eins trivial. Speziell für $SL(2,\mathbb{Z})$ ist dies $\{1_2, -1_2\} = Z(SL(2,\mathbb{Z}))$ das Zentrum von $SL(2,\mathbb{Z})$. Die Elemente $\gamma, \gamma\text{‘} \in SL(2,\mathbb{Z})$ beschreiben genau dann dieselbe Operation auf $\mathbb{H}$, wenn $\gamma = \gamma\text{‘}$ oder $\gamma = -\gamma\text{‘}$. Die Elemente γ aus $SL(2,\mathbb{Z})/\{\pm I_2\}$ bezeichnet man als gebrochen-rationale Transformationen. Mit Hilfe der Jordan'schen Normalform unterscheiden wir folgende Fälle:

i) γ hat die Jordan'sche Normalform $\begin{pmatrix} \lambda & 1 \\ 0 & \lambda \end{pmatrix}$ und somit genau einen Fixpunkt. In diesem Fall nennen wir γ parabolisch.

ii) γ hat die Jordan'sche Normalform $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$ und zwei Fixpunkte. Sind diese zueinander konjugiert komplexe Punkte, so nennen wir γ elliptisch, sind sie aus $\mathbb{R} \cup \infty$, so nennen wir γ hyperbolisch.

Wir haben folgende Klassifikation:
Sei $\sigma \in SL(2,\mathbb{R})$, dann gilt:

$$\begin{array}{rcl} \sigma \quad ist \quad parabolisch & \Leftrightarrow & tr(\sigma) = \pm 2 \\ elliptisch & \Leftrightarrow & |tr(\sigma)| < 2 \\ hyperbolisch & \Leftrightarrow & |tr(\sigma)| > 2. \end{array}$$

Sei nun Γ eine diskrete Untergruppe von $SL(2,\mathbb{R})$. Wir nennen $\nu \in \mathbb{H}$ einen elliptischen Punkt von Γ, falls es ein elliptisches Element von $\gamma \in \Gamma$ gibt, so dass gilt: $\gamma\nu = \nu$. Ein Punkt s aus $\mathbb{R}\cup\infty$ nennen wir Spitze von Γ, wenn ein parabolisches Element $\gamma \in \Gamma$ existiert, so dass $\gamma s = s$. Die Menge der Spitzen von Γ bezeichnen wir mit $S(\Gamma)$. Ist ν eine Spitze (beziehungsweise ein elliptischer Punkt) von Γ, so ist auch für alle $\gamma \in \Gamma$ das Element $\gamma\nu$ eine Spitze (beziehungsweise ein elliptischer Punkt). Für einen elliptischen Punkt ν ist der Stabilisator $\Gamma_\nu = \{\gamma \in \Gamma | \gamma\nu = \nu\}$ eine endliche, zyklische Gruppe, und umgekehrt sind die Elemente endlicher Ordnung in Γ (außer $\pm I_2$) die elliptischen Elemente. Die Ordnung der Gruppe $\{\gamma \in \Gamma/(\Gamma \cap \{\pm I_2\}) | \gamma\nu = \nu\}$ nennen wir die Ordnung des elliptischen Punktes ν bezüglich Γ.

Bemerkung 2.1

Bei der Definition der Ordnung eines elliptischen Elementes werden Untergruppen der Gruppe der gebrochen-rationalen Transformationen verwendet, die im Allgemeinen nicht mit den Untergruppen der Matrixgruppen verwechselt werden dürfen. Um zwischen der Matrixgruppe und der Gruppe der gebrochen-rationalen Transformationen zu unterscheiden, bezeichnen wir $\Gamma/(\Gamma \cap \{\pm 1_2\})$ auch kurz mit $\overline{\Gamma}$.

□

Beispiel 2.1

Die Gruppe $\Gamma = SL(2,\mathbb{Z})$ ist eine diskrete Untergruppe von $SL(2,\mathbb{R})$. Die Matrix $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma$ ist parabolisch und hat Fixpunkt ∞. Also ist ∞ eine Spitze von Γ.

Die Matrizen $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ und $\begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$ sind elliptisch und haben als Fixpunkte i und $p = e^{\frac{2\pi i}{3}}$, so dass i und p elliptische Punkte sind. Die Elemente des Stabilisators Γ_i von i können durch die beiden Matrizen I_2 und $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ repräsentiert werden, also hat i die Ordnung zwei. Der Punkt p hat Ordnung drei und darüber hinaus gilt: Zu jedem elliptischen Punkt p' der Ordnung zwei existiert ein γ aus Γ, so dass $\gamma p' = p$. Genauso existiert zu jedem elliptischen Punkt p' der Ordnung drei ein γ aus Γ, so dass $\gamma p' = p$. Siehe hierzu [Mi, Lemma 4.2.6 p.107].

□

2.3 Einige Untergruppen von $SL(2,\mathbb{Z})$

In diesem Abschnitt werden wir uns mit einigen wichtigen Untergruppen der speziellen linearen Gruppe $SL(2,\mathbb{Z})$ und deren Eigenschaften beschäftigen.

Definition 2.1
$\Gamma(1) := SL(2,\mathbb{Z})$ *oder eine ihrer Untergruppen von endlichem Index bezeichnen wir als Modulgruppen. Insbesondere für eine positive, ganze Zahl* N *aus* $\mathbb{N}$ *sei weiter*
$\Gamma(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) | a,d \equiv 1 (mod N); b,c \equiv 0 (mod N)\}$ *und*
$\Gamma_0(N) := \{\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(1) | c \equiv 0 (mod N)\}$.
Wir schreiben kurz $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} (mod \quad N)$, *falls* $a' \equiv a(mod \quad N), b' \equiv b(mod \quad N), c' \equiv c(mod \quad N), d' \equiv d(mod \quad N)$.
Wir nennen $\Gamma(N)$ *die Hauptkongruenzuntergruppe der Stufe* N.

Die Gruppen $\Gamma(N)$ und $\Gamma_0(N)$ sind Modulgruppen, da sie einen endlichen Index in $\Gamma(1)$ haben, den wir im Folgenden noch angeben werden (Vergleiche Proposition 2.1). Man sieht sofort, dass für N gleich eins gilt: $\Gamma(1)$ gleich $\Gamma_0(1)$ und für N größer als eins hat man eine echte Inklusion $\Gamma(N) \subset \Gamma_0(N)$, so dass die Gruppen $\Gamma_0(N)$ auch Modulgruppen sind. Da $SL(2,\mathbb{Z})$ auf der oberen Halbebene operiert, tut dies auch jede ihrer Untergruppen, insbesondere jede Modulgruppe.
Mit $\Gamma_0^+(N)$ bezeichnen wir das Erzeugnis von $\Gamma_0(N)$ und $\omega'_N = \begin{pmatrix} 0 & 1/\sqrt{N} \\ -\sqrt{N} & 0 \end{pmatrix}$.
Da die Determinante von ω'_N eins ist, liegt ω'_N in $SL_2(\mathbb{R})$. Es ist ein skalares Vielfaches von $\omega_N = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix}$. Die Matrix ω_N, beziehungsweise den dadurch beschriebenen Automorphismus $\omega_N : \mathbb{H} \to \mathbb{H}$, $\omega_N \nu = \frac{-1}{N\nu}$, bezeichnen wir als die Fricke-Involution ($\omega_N^2 = id$). Jedes Element γ^+ aus $\Gamma_0^+(N)$ hat eine Darstellung als $\gamma(\omega'_N)^j$ mit γ aus $\Gamma_0(N)$ und j aus $\{1,2\}$. Also ist der Index $[\Gamma_0^+(N) : \Gamma_0(N)]$ gleich zwei. $\Gamma_0^+(N)$ ist eine diskrete Untergruppe von $SL(2,\mathbb{R})$ und operiert ebenfalls auf der oberen Halbebene. Ist N kein vollkommenes Quadrat, dann stimmen die Spitzen von $\Gamma_0^+(N)$ mit denen von $\Gamma_0(N)$ überein.
Nun werden wir die Indices $[\overline{\Gamma}(1) : \overline{\Gamma}(N)]$ und $[\overline{\Gamma}(1) : \overline{\Gamma}_0(N)]$ angeben.

Lemma 2.1
Für alle positiven natürlichen Zahlen N *ist* $\Gamma(N)$ *eine normale Untergruppe von* $SL(2,\mathbb{Z})$, *und es gilt:*
$SL(2,\mathbb{Z})/\Gamma(N) \cong SL(2,\mathbb{Z}/N)$.

Beweis:
Der Kern der natürlichen Abbildung

$$\lambda_N : SL(2,\mathbb{Z}) \to SL(2,Z/N),$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \overline{a} & \overline{b} \\ \overline{c} & \overline{d} \end{pmatrix}$$

ist $\Gamma(N)$. Die Surjektivität wird in [Mi, Theorem 4.2.1, p.104] gezeigt.

□

Lemma 2.2
Sei N eine ganze Zahl, $\prod_{p_i \in \mathbb{P}} p_i^{e_i}$ ihre Primfaktorzerlegung, wobei die e_i natürliche Zahlen fast alle gleich null seien. P_N bezeichne die Menge der Primfaktoren von N. Dann ist die Abbildung:

$$\Xi : Sl(2,\mathbb{Z}/N) \to \bigoplus_{p_i \in P_N} SL(2,\mathbb{Z}/p_i)^{e_i},$$
$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \bigoplus_{p_i \in P_N} \begin{pmatrix} a_i & b_i \\ c_i & d_i \end{pmatrix} (mod \quad p_i^{e_i})$$

ein Isomorphismus.

Beweis:
Siehe [Mi, Lemma 4.2.3, p.105].

□

Proposition 2.1

a) $[\overline{\Gamma}(1) : \overline{\Gamma}(N)] = \begin{cases} \frac{N^3}{2} \prod_{p|N, p \in \mathbb{P}} (1-p^{-2}) & N > 2 \\ 6 & N = 2 \end{cases},$

b) $[\overline{\Gamma}(1) : \overline{\Gamma}_0(N)] = N \prod_{p|N, p \in \mathbb{P}} (1+p^{-1}).$

Beweis:
Siehe [Mi, Theorem 4.2.5, (1) und (2), p. 106].

□

2.4 Der topologische Raum $\Gamma\backslash\overline{\mathbb{H}}$

Sei Γ eine Modulgruppe oder eine der Gruppen $\Gamma^+(N)$. Dann bezeichnen wir die Vereinigung von $\mathbb{H}$ mit den Spitzen von Γ als $\overline{\mathbb{H}}$. Die Gruppe Γ operiert auf $\overline{\mathbb{H}}$ und wir können den Quotientenraum betrachten. Dabei heißen die Elemente ν_1 und ν_2 Γ-äquivalent, wenn sie in derselben Bahn unter Γ liegen. Da Spitzen auf Spitzen und elliptische Punkte auf elliptische Punkte abgebildet werden, nennen wir die Äquivalenzklassen von Γ (beziehungsweise die elliptischen Punkte von Γ) die Spitzen von $\Gamma\backslash\overline{\mathbb{H}}$ (beziehungsweise die elliptischen Punkte von $\Gamma\backslash\overline{\mathbb{H}}$) und bezeichnen sie mit $S(\Gamma\backslash\overline{\mathbb{H}})$ (beziehungsweise $E(\Gamma\backslash\overline{\mathbb{H}})$.

Beispiel 2.2

In Beispiel 2.1 haben wir gesehen, dass alle Spitzen von $\Gamma(1)$ zu ∞ $\Gamma(1)$-äquivalent sind. $\Gamma(1)\backslash\overline{\mathbb{H}}$ hat also genau eine Spitze. Wir sehen auch, dass $\Gamma(1)\backslash\overline{\mathbb{H}}$ genau einen elliptischen Punkt der Ordnung zwei und einen elliptischen Punkt der Ordnung drei hat.
Die Anzahl der elliptischen Punkte und Spitzen von $\Gamma_0(N)\backslash\overline{\mathbb{H}}$ kann man explizit

angeben. Siehe [Mi,Theorem 4.2.7, p.108ff] oder [Sh, Proposition 1.43, p.24ff]. Sei dazu μ_2 die Anzahl der elliptischen Punkte der Ordnung zwei, μ_3 die Anzahl der elliptischen Punkte der Ordnung zrei und μ_∞ die Anzahl der Spitzen. Dann ist:

$$\begin{aligned}
\mu_2 &= \begin{cases} 0 & 4|N \\ \prod_{p|N}(\frac{-1}{p}) & sonst \end{cases}, \\
\mu_3 &= \begin{cases} 0 & 9|N \\ \prod_{p|N}(\frac{-3}{p}) & sonst \end{cases}, \\
\mu_\infty &= \sum_{d|N, d>0} \phi((d, \frac{N}{d})).
\end{aligned}$$

Dabei bezeichnet ϕ die Euler-ϕ-Funktion und es gilt:

$$\begin{aligned}
(\frac{-1}{p}) &= \begin{cases} 0 & = & p = 2 \\ 1 & = & p \cong 1 mod(4) \\ -1 & = & p \cong 3 mod(4) \end{cases}, \\
(\frac{-3}{p}) &= \begin{cases} 0 & = & p = 3 \\ 1 & = & p \cong 1 mod(3) \\ -1 & = & p \cong 2 mod(3) \end{cases}.
\end{aligned}$$

Ist insbesondere N eine Primzahl, dann hat $\Gamma_0(N)\backslash\overline{\mathbb{H}}$ genau zwei Spitzen, die durch 0 und ∞ repräsentiert werden können. Da die Spitzen von $\Gamma_0^+(N)$ und $\Gamma_0(N)$ übereinstimmen, wenn N kein echtes Quadrat ist, und darüber hinaus ∞ von ω_0' auf 0 abgebildet wird, hat $\Gamma_0^+(N)\backslash\mathbb{H}$ genau eine Spitze, falls N eine Primzahl ist.

□

Um eine komplexe Struktur auf $\Gamma\backslash\overline{\mathbb{H}}$ einzuführen, konstruieren wir uns zuerst eine geeignete Topologie auf $\overline{\mathbb{H}}$. Dazu definieren wir ein Fundamentalsystem von offenen Umgebungen von ν aus $\overline{\mathbb{H}}$. Für alle ν aus $\mathbb{H}$ nehmen wir das übliche Fundamentalsystem von der Abstandstopologie in $\mathbb{C}$. Für eine Spitze ν aus $S(\Gamma)$ nehmen wir als Fundamentalsystem die Vereinigung von $\{\nu\}$ mit dem Inneren einer Kreisscheibe, welche die reelle Achse im Punkt ν berührt falls die Spitze nicht ∞ ist. Im Fall $\nu = \infty$ ist ein Fundamentalsystem von offenen Umgebungen von ∞ durch die Mengen $N_c := \{z \in \mathbb{H} \, | Im(z) > c\} \cup \{\infty\}$, $0 < c \in \mathbb{R}$ gegeben. Zur Verdeutlichung siehe Abbildung 2.1.
Als Topologie auf $\Gamma\backslash(\overline{\mathbb{H}})$ nehmen wir die Quotiententopologie bezüglich der natürlichen Projektion π von $\overline{\mathbb{H}}$ nach $\Gamma\backslash(\overline{\mathbb{H}})$, so dass eine Menge U von $\Gamma\backslash(\overline{\mathbb{H}})$ genau dann offen ist, wenn ihr Urbild $\pi^{-1}(U)$ offen ist.

Darüber hinaus haben wir folgende Proposition:

Proposition 2.2
Der topologische Raum $\Gamma\backslash\mathbb{H}$ *ist Hausdorff in seiner Quotiententopologie.*

Beweis:
Da $SL(2,\mathbb{Z})$ ist, folgt die Proposition aus [Mi, Corollary 1.5.3, p.17f] und [Mi, Lemma 1.7.2, p.24f].

□

2.5 Die Riemannsche Fläche $\Gamma\backslash\overline{\mathbb{H}}$.

Nun zur Definition der Riemannsche Struktur auf $\Gamma\backslash(\overline{\mathbb{H}})$. Sei dazu wie oben π die natürliche Projektion von $\overline{\mathbb{H}}$ nach $\Gamma\backslash(\overline{\mathbb{H}})$. Für alle ν aus $\overline{\mathbb{H}}$ sei $\Gamma_\nu = \{\gamma \in \Gamma | \gamma(\nu) = \nu\}$

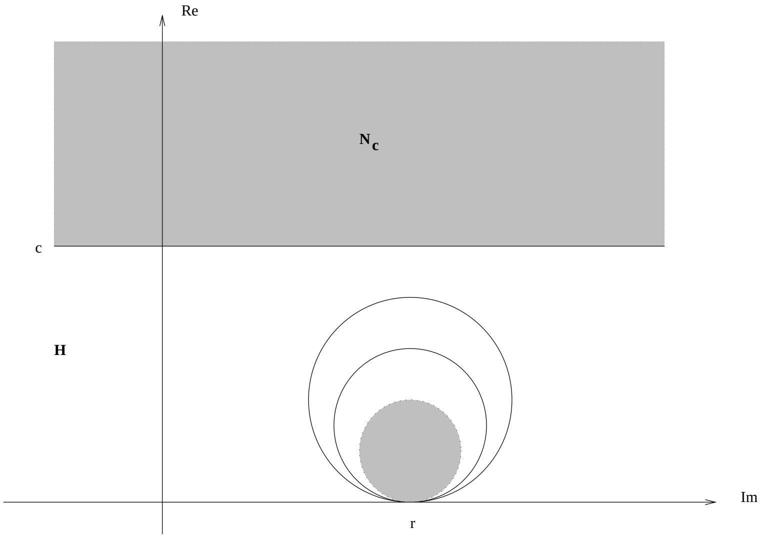

Abbildung 2.1: Offene Umgebungen von ∞ bzw $r \in \mathbb{Q}$

der Stabilisator von ν. Nach [Sh, Proposition 1.7 und Lemma 1.26] existiert für alle $\nu \in \mathbb{H}$ eine offene Umgebung $U \subset \mathbb{H}$, so dass $\Gamma_\nu = \{\gamma \in \Gamma | \gamma(U) \cap U \neq \emptyset\}$. Für ein solches ν gibt es eine natürliche Einbettung $\Gamma_\nu \backslash U \to \Gamma \backslash \overline{\mathbb{H}}$. Sei P ein Punkt aus $\Gamma \backslash \mathbb{H}$ und ν_P ein Punkt aus $\mathbb{H}$, so dass $\pi(\nu_P)$ gleich P ist. Sei weiterhin U_P eine offene Umgebung von ν_P, so dass $\Gamma_{\nu_P} = \{\gamma \in \Gamma | \gamma(U_P) \cap U_P \neq \emptyset\}$. Für jedes $\nu_P \in \mathbb{H}$ ist die Abbildung $\mu_{\nu_P} : \mathbb{H} \to B_1(0) \subset \mathbb{C}$ von der oberen Halbebene in die offene komplexe Kreisscheibe mit Radius eins um null, die ν seinem Bild $\frac{\nu - \nu_P}{\nu - \overline{\nu_P}}$ zuordnet, ein holomorpher Isomorphismus mit $\mu_{\nu_P}(\nu_P) = 0$.
Sei nun e_P die Ordnung von ν_P bezüglich Γ, falls P ein elliptischer Punkt ist, und sei e_P gleich eins, falls es kein elliptischer Punkt ist. Wir definieren:

$$\begin{gathered} \psi_P : \Gamma_{\nu_P} \backslash U \to \mathbb{C}, \\ \psi(\pi(\nu_P)) = (\mu_{\nu_P}(\nu))^{e_P} = \left(\frac{\nu - \nu_P}{\nu - \overline{\nu_P}} \right)^{e_P}, \text{ und} \\ S_1 := \{(\Gamma_{\nu_P} \backslash U_P, \nu_P)\}. \end{gathered}$$

Ist ν_P eine Spitze, dann sei $\sigma_P \in SL_2(\mathbb{R})$, so dass

$$\sigma_P \Gamma_{\nu_p} \sigma_{P^{-1}} \{\pm I_2\} = \left\{ \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m | m \in \mathbb{Z} \right\}$$

(Siehe hierzu [Sh, Proposition 1.17, p.8]). Wir definieren nun:

$$\begin{gathered} \psi_P : \Gamma_{\nu_P} \backslash U \to \mathbb{C}, \\ \psi(\pi(\nu_P)) = \begin{cases} exp(2\pi i \frac{\sigma_P(\nu)}{h}) & falls \quad \sigma_P(\nu) \neq \infty \\ 0 & falls \quad \sigma_P(\nu) = \infty \end{cases}, \text{ und} \\ S_2 := \{(\Gamma_{\nu_P} \backslash U_P, \nu_P)\}. \end{gathered}$$

Die Familie $S = S_1 \cup S_2$ definiert eine komplexe Struktur auf $\Gamma \backslash \overline{\mathbb{H}}$. Siehe hierzu auch [Mi, Paragraph 1.8, p.28ff]. Wir haben folgenden Satz:

Satz 2.1
Die Menge $\Gamma\backslash(\overline{\mathbb{H}})$ ist eine zusammenhängende, kompakte Riemannsche Fläche.

Beweis:
Die Behauptung folgt aus [Sh, Proposition 1.3.1, p.13] und dem Sachverhalt, dass $SL(2,\mathbb{Z})\backslash\overline{\mathbb{H}}$ isomorph zur Riemannschen Zahlenkugel ist ([Sh, Proposition 1.4 und Bemerkungen im ersten Abschnitt von Paragraph 1.6]).

□

In Paragraph 1.3 haben wir gesehen, dass der Begriff der kompakten Riemannschen Fläche und der glatten, projektiven Kurve äquivalent sind. Wir erhalten also zu jeder Modulgruppe eine assoziierte Kurve, die wir für $\Gamma(N)$ mit $X(N)$ und für $\Gamma_0(N)$ mit $X_0(N)$ bezeichnen. Für die Gruppe $\Gamma^+(N)$ ist der Quotientenraum $\Gamma_0^+(N)\backslash\overline{\mathbb{H}}$ ebenfalls eine kompakte Riemannsche Fläche. Die dazu assoziierte Kurve bezeichnen wir mit $X_0^+(N)$.

2.6 Modulformen für Modulgruppen

Sei $GL^+(2,\mathbb{R})$ die Untergruppe der Matritzengruppe $GL(2,\mathbb{R})$, die aus allen Matrizen mit positiver Determinante besteht. Sei weiter k eine gerade, ganze Zahl und $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in GL^+(2,\mathbb{R})$. Für eine meromorphe Funktion f auf der oberen Halbebene definieren wir den Operator $[\gamma]_k$ durch

$$f|[\gamma]_k\,(\nu) := (det\gamma)^{\frac{k}{2}}(c\nu+d)^{-k}f(\gamma\nu).$$

Skalare Vielfache der Einheitsmatrix operieren dabei trivial. Ist insbesondere γ aus $SL(2,\mathbb{R})$ dann gilt:

$$f|[\gamma]_k\,(\nu) = (c\nu+d)^{-k}f(\gamma\nu),$$

und für γ_1, γ_2 aus $Gl^+(2,\mathbb{R})$ ist

$$f|[\gamma_1\gamma_2]_k = (f|[\gamma_1]_k)|[\gamma_2]_k.$$

Die Operation von $[\gamma]_k$ ist verträglich mit Skalarmultiplikation und Addition von Funktionen, das heißt für die Funktionen f und g auf $\mathbb{H}$ und $\alpha\in\mathbb{C}$ gilt:

$$(\alpha f)|[\gamma]_k = (\alpha f)|[\gamma]_k \text{ und}$$
$$(f+g)|[\gamma]_k = f|[\gamma]_k + g|[\gamma]_k.$$

Sei nun Γ eine Modulgruppe und $s\in S(\Gamma)$ eine Spitze von Γ. Sei weiterhin $\gamma_0\in SL(2,\mathbb{R})$, so dass $\gamma_0 s=\infty$. Dann kann der Stabilisator $\Gamma_s = \{\gamma\in\Gamma|\gamma s = s\}$ für eine positive reelle Zahl h beschrieben werden als

$$\gamma_0\Gamma_s\gamma_0^{-1} = \left\{\pm\begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix}^m |m\in\mathbb{Z}\right\}.$$

Ist f invariant unter $[\gamma]_k$ für alle $\gamma\in\Gamma$, dann ist $f|[\gamma_0^{-1}]_k$ invariant unter $[\sigma]_k$ für alle σ aus $\gamma_0\Gamma_s\gamma_0^{-1}$, da für $\sigma = \gamma_0\gamma\gamma_0^{-1}$ mit $\gamma\in\Gamma_s\subset\Gamma$ gilt:

$$(f|[\gamma_0^{-1}]_k)|[\sigma]_k = f|[\gamma_0^{-1}\sigma]_k = f|[\gamma_0^{-1}\gamma_0\gamma\gamma_0^{-1}] = f|[\gamma\gamma_0^{-1}]_k = f|[\gamma_0^{-1}]_k.$$

Also ist $f|[\gamma_0^{-1}]_k\,(\nu)$ invariant unter $\nu\mapsto\nu+h$. Die Abbildung $\nu\mapsto q_h := e^{2\pi i\frac{\nu}{h}}$ bildet die obere Halbebene auf die punktierte Einheitskreisscheibe ab, und es existiert eine meromorphe Funktion $\phi(q_h)$ auf einer punktierten, offenen Kreisscheibe $0<|q_h|<r\in\mathbb{R}, r>0$, so dass $f|[\gamma_0^{-1}]\,(\nu) = \phi(q_h)$. Wir nennen $f(\nu)$ meromorph in der Spitze s, falls $\phi(q_h)$ meromorph in null ist. Diese Definition hängt nicht von γ_0 ab, und ist f in der Spitze s meromorph, so auch in jeder dazu Γ-äquivalenten anderen Spitze. Nun zur Definition einer automorphen Form.

Definition 2.2

Sei f eine Funktion auf $\mathbb{H}$ und k eine gerade, ganze Zahl. Wir nennen f eine automorphe Form vom Gewicht k für die Modulgruppe Γ, wenn die folgenden Bedingungen erfüllt sind:

i) $f(\nu)$ ist meromorph auf $\mathbb{H}$,

ii) $f|[\gamma]_k\,(\nu) = f(\nu)$ für alle $\gamma \in \Gamma$,

iii) $f(\nu)$ ist meromorph in jeder Spitze von Γ.

□

Da die oben beschriebene Funktion $\phi(q_h)$ meromorph in einem Ringgebiet ist, lässt sie sich in eine Potenzreihe um null entwickeln:

$$\phi(q_h) = \sum_{n\in\mathbb{Z}} a_n q_h^n = \sum_{n\in\mathbb{Z}} a_n e^{2\pi i \frac{\nu}{h}},$$

die wir die Fourier- oder q_h- Entwicklung von f für s nennen. Dabei ist $f(\nu)$ genau dann meromorph, wenn für ein $n < 0$ höchstens endlich viele a_n von null verschieden sind. Ist a_n für alle $n < 0$ gleich null, dann nennen wir f in s holomorph. Wir sagen $f(\nu)$ verschwindet in s, falls $\phi(q_h)$ in null verschwindet.

Definition 2.3

Sei f eine Funktion auf $\mathbb{H}$ und k eine gerade, ganze Zahl. $f(\nu)$ heißt Modulform (beziehungsweise Spitzenform) vom Gewicht k für die Modulgruppe Γ, wenn die folgenden Bedingungen erfüllt sind:

i) $f(\nu)$ ist holomorph auf $\mathbb{H}$,

ii) $f|[\gamma]_k\,(\nu) = f(\nu)$ für alle $\gamma \in \Gamma$,

iii) $f(\nu)$ ist holomorph (beziehungsweise verschwindet) in jeder Spitze von Γ.

□

Mit $M_k(\Gamma)$ (beziehungsweise $S_k(\Gamma)$) bezeichnen wir die Menge der Modulformen (beziehungsweise Spitzenformen) vom Gewicht k für Γ. Aufgrund der Verträglichkeit der Operation von $[\gamma]_k$ mit Skalarmultiplikation und Addition von Funktionen sind $M_k(\Gamma)$ und $S_k(\Gamma)$ $\mathbb{C}$-Vektorräume. Das Produkt zweier Modulformen (beziehungsweise zweier automorpher Formen oder Spitzenformen) vom Gewicht k_1 und k_2 ist eine Modulform (beziehungsweise automorphe Form oder Spitzenform) vom Gewicht $k_1 + k_2$. Der Quotient einer Modulform (beziehungsweise automorphen Form) vom Gewicht k_1 mit einer von null verschiedenen Modulform (beziehungsweise einer automorphen Form) vom Gewicht k_2 ist eine Modulform (beziehungsweise automorphe Form) vom Gewicht $k_1 - k_2$. Die Menge der automorphen Formen vom Gewicht null für Γ bildet also einen Körper, deren Elemente wir Modulfunktionen nennen.

Beispiel 2.3

Die Funktion

$$j = j(\tau) = \frac{\left(1+240\sum_{n=1}^{\infty}\sigma_3(n)q^n\right)^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}}, \text{ mit } \sigma_3(n) = \sum_{d|n, d\in\mathbb{N}} d^3$$

ist eine Modulfunktion für $\Gamma(1)$ und deren Untergruppen, und $j_N := j(N\tau)$ ist eine Modulfunktion für $\Gamma_0(N)$.

□

Da Modulfunktionen für Γ invariant unter allen Elementen γ aus Γ sind, können wir sie als Funktionen auf der Riemannschen Fläche $\Gamma\backslash\mathbb{H}$ auffassen. Ist speziell $\Gamma = \Gamma_0(N)$, so haben wir folgenden Satz:

Satz 2.2
Der Körper der meromorphen Funktionen von $\mathbb{C}(X_0(N))$ wird von j und j_N erzeugt.

Beweis:
Siehe [Sh, Proposition 2.10, p.34] oder [Kn, Chapter XI, Theorem 11.33, p.336].

□

Betrachten wir nun $\Gamma_0^+(N)$. Da $\Gamma_0^+(N)$ das Erzeugnis von $\Gamma_0(N)$ und ω'_N ist, sind die Modulfunktionen von $\Gamma_0^+(N)$ invariant unter $\Gamma_0(N)$ und ω'_N.

Da ω'_N ein skalares Vielfaches von ω'_N ist, beschreiben $[\omega_N]_k$ und $[\omega'_N]_k$ dieselbe Operation.

Definition 2.4

Eine meromorphe Funktion f auf $\mathbb{H}$ nennen wir ω_n- invariant oder einfach invariant, falls $\omega_n f := f|[\omega_N]_k = f$, und ω_n-anti-invariant oder einfach anti-invariant, falls $\omega_n f = -f$.

□

Ist f eine Modulfunktion oder Spitzenform von $\Gamma(1)$, so ist $f(\nu) + \omega_N f(\nu)$ invariant und $f(\nu) - \omega_N f(\nu)$ anti-invariant.

2.7 Das Geschlecht der Modulkurven

Satz 2.3
Sei Γ eine Untergruppe von $\Gamma(1)$ mit endlichem Index μ. Seien weiterhin ν_2 beziehungsweise ν_3 die Anzahl der Γ- inäquivalenten, elliptischen Punkte der Ordnung zwei beziehungsweise drei und ν_∞ die Anzahl der Γ-inäquivalenten Spitzen von Γ. Dann hat $\Gamma\backslash\overline{\mathbf{H}}$ das Geschlecht

$$g = 1 + \frac{\mu}{12} - \frac{\nu_2}{4} - \frac{\nu_3}{3} - \frac{\nu_\infty}{2}.$$

Beweis:
Siehe [Sh, Proposition 1.40, p.23].

□

Ist insbesondere $\Gamma = \Gamma_0(N)$, so haben wir in Beispiel 2.2 die Werte für ν_2, ν_3 und ν_∞ angegeben. Die Werte für ν sind Proposition 2.1 zu entnehmen.

2.8 Elliptische Kurven und Modulräume

Es gibt viele Methoden elliptische Kurven zu definieren. Beginnen wir hier mit einem Gitter $L = \mathbb{Z} + \tau\mathbb{Z}$ mit $\tau \in \mathbb{H}$. Der Quotient von $\mathbb{C}$ mit diesem Gitter ist ein eindimensionaler Torus, den wir mit $E(\tau) = \mathbb{C}/L$ bezeichnen und elliptische Kurve nennen. Durch die Weierstraß'sche p-Funktion

$$\begin{aligned} p(z,L) &:= \frac{1}{z^2} + \sum_{\omega \in L - \{0\}} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right), z \notin L \\ p(z) &:= \infty, z \in L \end{aligned}$$

und deren Ableitung

$$\begin{aligned} p'(z) &:= -2 \sum_{\omega \in L - \{0\}} \frac{1}{(z-\omega)^3}, z \notin L \\ p'(z) &= \infty, z \in L \end{aligned}$$

wird durch

$$\begin{aligned} \mathbb{C}/L &\to E \\ z &\mapsto (p(z), p'(z), 1),\ z \neq 0 \\ z &\mapsto (0,1,0),\ z = 0 \end{aligned}$$

ein Isomorphismus von Riemannschen Flächen (und ein Gruppenhomomorphismus) erklärt ([Si, Chapter VI, Proposition 3.6, p.158]). Dabei ist $E = E(g_1, g_2) \subset \mathbb{P}^2(\mathbb{C})$ eine ebene, projektive Kurve. Hat $\mathbb{P}^2(\mathbb{C})$ die homogenen Koordinaten $(x : y : z)$, so wird E im affinen Teilraum U_3 in den Koordinaten x und y durch die Gleichung $y^2 = 4x^3 - g_2 x - g_3$ beschrieben. Die Zahlen g_2 und g_3 sind bestimmt durch:

$$\begin{aligned} g_2 &= 60 \sum_{\omega \in L - \{0\}} \frac{1}{(\omega)^4}, \\ g_3 &= 140 \sum_{\omega \in L - \{0\}} \frac{1}{(\omega)^6}. \end{aligned}$$

Die obige Gleichung E nennen wir die Weierstraß-Form der elliptischen Kurve $E(\tau)$. Die Diskriminante der Kurve E ist $\Delta = g_2^3 - 27g_3^2$. E ist genau dann ungleich null, wenn Δ ungleich null ist. Siehe hierzu [Si, III, Proposition 1.4, p.50]. Die Zahl $j = j(E) := \frac{12g_2^3}{\Delta}$ heißt j-Invariante.

Satz 2.4
Über einem algebraisch abgeschlossenen Körper k sind zwei elliptisch Kurven E, E' genau dann isomorph, wenn ihre j-Invarianten j(E) und j(E') gleich sind.

Beweis:
Siehe [Si, Chapter III, Paragraph 1, Proposition 1.4(b)], falls die Charakteristik von k nicht zwei oder drei ist, und siehe [Si, Apendix A] für die Charakteristik zwei und drei.

□

Bemerkung 2.2

Sei k ein algebraisch abgeschlossener Körper. Für einen gegebenen Wert von j erhält man, falls $char(k) \neq 2, 3$, folgende elliptische Kurven in Weierstraß-Form:

i) Falls $j \neq 0, 1728$, dann ist E gegeben durch $y^2 = 4x^3 - \frac{27j}{j-1728}(x+1)$.

ii) Falls $j = 0$, dann ist E gegeben durch $y^2 = 4x^3 - 1$.

iii) Falls $j = 1728$, dann ist E gegeben durch $y^2 = 4x^3 - 3x$.

Für $j = \infty$ erhält man eine singuläre, 'elliptische' Kurve, die durch ein Modell der Form $y^2 = x^3$ beschrieben werden kann.
Man kann zeigen, dass die j-Invariante invariant unter der Modulgruppe $\Gamma(1)$ ist. Das heißt: $j(\tau) = j(\sigma(\tau)) \forall \sigma \in \Gamma(1)$. Die Modulgruppe ihrerseits klassifiziert wiederum die Isomorphieklassen von elliptischen Kurven. Wir können also $\Gamma(1)\backslash\mathbb{H}\cup\{\infty\} =$

$\Gamma_0(1)\backslash\overline{\mathbb{H}} = X_0(1)$ als Parameterraum für elliptische Kurven auffassen. Deshalb nennen wir $X_0(1)$ den Modulraum der elliptischen Kurven über k. Eine exakte Darstellung dessen findet sich in [Si2, Paragraph 4, p.34-38].

Beschreiben wir nun weitere Modulräume. Sei $N \in \mathbb{N}$ und $E = \mathbb{C}/L$ wieder eine elliptische Kurve zum Gitter $L = \mathbb{Z} + \tau\mathbb{Z}$ mit $\tau \in \mathbb{H}$. Sei weiterhin $C = C(L)$ eine zyklische Untergruppe der Ordnung N von E, die wir ohne Einschränkung der Allgemeinheit als die Vielfachen von $\frac{\tau}{N}$ wählen können (∞ sei dabei als das additiv Neutrale der elliptischen Gruppe gewählt). Unter einer gebrochen-rationalen Transformation σ mit Determinante eins geht L nach $\sigma(L)$ und $C(L)$ genau dann nach $C(\sigma(L))$, falls σ aus $\Gamma_0(N)$ist , so dass die Isomorphieklassen von Paaren (E, C) von elliptischen Kurven E mit zyklischer Untergruppe C der Ordnung N mit den Bahnen von $\Gamma_0(N)\backslash\mathbb{H}$ in Bijektion stehen. Kompaktifizieren wir nun $\Gamma_0(N)\backslash\mathbb{H}$, indem wir die Spitzen $S(\Gamma_0(N))$ zu $\Gamma_0(N)\backslash\mathbb{H}$ hinzufügen. Wollen wir $X_0(N)$ nun als Modulraum auffassen, so müssen wir den Spitzen noch 'verallgemeinerte, elliptische Kurven' zuordnen. Diese Kurven haben nur noch arithmetisches Geschlecht eins. Sie haben auch eine Gruppenstruktur mit einer Untergruppe der Ordnung N.
Ist der Grundkörper nicht algebraisch abgeschlossen, so gibt es zwischen der j-Invarianten und den Isomorphieklassen von Paaren elliptischer Kurven und Untergruppen der Ordnung N nicht notwendig eine bijektive Korrespondenz. Igusa zeigt nun in [Ig], dass es eine Kurve $X_0(N)$ gibt, die als Kurve über $\mathbb{C}$ die Isomorphieklassen elliptischer Kurven parametrisiert, und durch Gleichungen über $\mathbb{Z}[\frac{1}{N}]$ definiert ist. Dabei gilt für alle Primzahlen p, die N nicht teilen: Reduziert man die Gleichungen modulo p, so erhalten wir eine nichtsinguläre Kurve über $\overline{\mathbb{F}}_p$, deren Punkte die Isomorphieklassen von Paaren (E, C) parametrisieren.

Bemerkung 2.3

Um diese Aussage genau zu fassen, benötigt man die Theorie der Schemata. Einzelheiten finden sich in [Ig] oder in den Arbeiten:

- N.Katz B.Mazur, Arithmetic Moduli of Elliptic Curves, Ann. of Math. Studies, Princton Univ. Press, 1985.
- P.Deligne, M. Rappoport, Schemes des courbes elliptiques, Lecture Notes in Math. 349, 1973, p.143-316.

□

2.9 Das Modulpolynom

Wir betrachten nun ein weiteres Modell für die Modulkurve. Die Riemannsche Fläche $\mathbb{H}/\Gamma_0(N)$ hat einen Funktionenkörper vom Transzendenzgrad eins, der von den Funktionen $j(\tau)$ und $j_N(\tau) := j(\begin{pmatrix} N & 0 \\ 0 & 1 \end{pmatrix}\tau)$ erzeugt wird. Die Funktion j_N , deren Minimalpolynom wir mit Φ_N bezeichnen, und das Modulpolynom zur Stufe N nennen, ist algebraisch über $\mathbb{C}(j)$. Es ist absolut irreduzibel und hat Koeffizienten in $\mathbb{Z}$. Siehe hierzu [Kn, Chapter XI, Theorem 11.32 und 11.33]. Desweiteren gilt:

i) $\Phi_N(x, j) = \prod_{\alpha \in A} (x - (\alpha(j)))$ mit
$$A = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} | a, b, d \in \mathbb{Z}; a > 0; d > 0; 0 \leq b < d; (a, b, d) = 1, ad = n \right\},$$

ii) $\Phi_N(x, j) = x^{\psi(N)} + y^{\psi(N)} + \sum_{a,b<\psi(N)} c_{ab} x^a j^b$ mit $\psi(N) = [\Gamma(1) : \Gamma_0(N)]$,

iii) $\Phi_N(x, j) = \Phi_N(j, x)$, also $c_{ab} = c_{ba}$.

Das Modulpolynom liefert uns ein affines Modell für $X_0(N)$. Dieses Modell ist singulär und hat die Eigenschaft, dass die Koeffizienten der Polynome sehr rasch mit N wachsen, so dass sie praktisch nicht zu handhaben sind.

Reduzieren wir nun die Koeffizienten von Φ_N modulo einer Primzahl p. Ist $N = p^e N'$ mit $p \not| N'$ dann zerfällt Φ_N modulo p wie folgt:

$$\Phi_N(x,y) \equiv \Phi_{N'}(x^{p^e}, y)\Phi_{N'}(x, y^{p^e}) \prod_{i=1}^{e-1} \Phi_{N'}(x^{p^{e-i-1}}, y^{p^{i-1}}) \bmod p.$$

Dabei ist $\Phi_{N'}$ das Modulpolynom zur Stufe N'. Es ist modulo p absolut irreduzibel. Ist insbesondere $N = p$, so zerfällt Φ_p modulo p in $(x^p - y)(x - y^p)$. Siehe hierzu [Ig, 3 A digression] und [IG2,Theorem 7].

Kapitel 3

Die Modelle von M. Pfeifer

In diesem Kapitel wollen wir uns mit den von M. Pfeifer in [Pf] angegebenen Modellen von $X_0(l)$ für Primzahlen l beschäftigen. Andere Modelle für Modulkurven finden sich in Arbeiten von M. Shimura [ShM] und S. G. Rovira [Ro], der Modelle für hyperelliptische Modulkurven angibt. Dabei stimmen die von Roviera angegebenen Modelle mit denen des M. Pfeifer überein, insofern in beiden Artikeln ein Modell zur selben Stufe angegeben wurde. Eine andere Quelle für einige Modelle mit kleinem Geschlecht ist [Bi].

3.1 Konstruktion der Modelle

Um die von M.Pfeifer angegebenen Modelle zu konstruieren, wurden mittels Relationen geeigneter Funktionen auf $X_0(l)$ Gleichungen in einem affinen Raum angegeben, die eine eindimensionale algebraische Menge Y_l definieren. Es kann gezeigt werden, dass Modelle für $Y_0(l)$ in Y_l enthalten sind. Es sind Relationen für alle Primzahlen zwischen 2 und 179, sowie für 191 und 239 angegeben worden. Dazu wurden Fourierentwicklungen der Elemente von Erzeugendensystemen der Spitzenräume $S_2(\Gamma_0(l))$ vom Gewicht zwei für $\Gamma_0(l)$ bestimmt. Mit deren Hilfe wurden dann wiederum die Fourierentwicklungen der Erzeuger für den Raum $S_k(\Gamma_0(l))$ der Spitzenformen vom Gewicht k für $\Gamma_0(l)$ berechnet (k gerade, größer gleich zwei). Insbesondere ist es möglich für $k = 12$ eine Basis von $S_{12}(\Gamma_0(l))$ zu bestimmen. Da man die Operation der Fricke-Involution kennt, kann man den Raum in einen unter dieser Operation invarianten Teilraum $S_{12}^+(\Gamma_0(l))$ und einen anti-invarianten Teilraum $S_{12}^-(\Gamma_0(l))$ aufspalten. Mit Hilfe dieser Basen gelingt es dann Modulfunktionen ohne endliche Pole auf $\Gamma_0(l)$ zu berechnen. Genauer gesagt: man berechnet Funktionen $1, x_1, \ldots, x_{g_0^+ +1}$ auf $X_0^+(l)$. Mit Hilfe des Satzes von Riemann-Roch kann die Dimension $g^+ + 2$ von $L((2g^+ + 1)\infty)$ bestimmt werden. Dies sind Funktionen auf $X_0^+(l)$ ohne endliche Pole, deren Polstellenordnung kleiner gleich $2g^+ + 1$ ist. Desweiteren berechnet man eine geeignete anti-invariante Modulfunktion s. Man kann dann zeigen, dass die Funktionen $1, x_1, \ldots, x_{g_0^+ +1}, s$ die $\mathbb{C}$-Algebra $O(X_0(l))$ der Modulfunktionen ohne endliche Pole auf $X_0(l)$ erzeugen. Dabei werden nicht alle diese Funktionen benötigt, wenn $X_0^+(l)$ im Unendlichen einen Weierstraß-Punkt hat. Alle diese Konstruktionen lassen sich in einer Art und Weise durchführen, dass die Fourierkoeffizienten der auftretenden Entwicklungen ganz sind.
Es werden nun in Abhängigkeit einiger zufällig gewählter, natürlicher Zahlen Linearkombinationen von Potenzen der Erzeuger von $O(X_0(l))$ gewählt. Eine Relation zwischen diesen erhält man, wenn das durch Koeffizientenvergleich gegebene, lineare Gleichungssystem nichttrivial lösbar ist ([Pf, p.84f]). Diese Relationen haben auch ganzzahlige Koeffizienten. Beschreiben wir die Konstruktion nun etwas genauer.

3.1.1 Quaternionenalgebren

Eine Quaternionenalgebra $\mathfrak{A}$ über k ist eine vierdimensionale Algebra über k, deren Zentrum k ist und die keine echten, zweiseitigen Ideale besitzt. $\mathfrak{A}$ hat eine Basis $\{1, i, j, l\}$ für die die Relationen

$$i^2 = a,\ j^2 = b \text{ und } ij = l = -ji \text{ mit } a, b \in k$$

gelten. Umgekehrt gibt es zu $a, b \in k^*$ eine Quaternionenalgebra, die durch obige Relationen definiert wird. Über einem algebraisch abgeschlossenen Körper k gibt es bis auf Isomorphie genau eine solche Algebra. Ist k ein lokaler Körper der Charakteristik null, so gibt es bis auf Isomorphie genau zwei Quaternionenalgebren. Eine davon ist die 2×2-Matrizenalgbra, die andere ist eine eindeutig bestimmte Quaternionendivisonsalgebra [Lam, Theorem 2.10, p.154ff]. Ist $\mathfrak{A}$ eine Quaternionenalgebra über $\mathbb{Q}$, so ist $\mathbb{Q}_p = \mathfrak{A}\otimes_{\mathbb{Q}}\mathbb{Q}_p$ eine Quaternionenalgebra über $\mathbb{Q}_p$ (p Primzahl). Analog dazu ist $\mathfrak{A}_\infty = \mathfrak{A} \otimes_{\mathbb{Q}} \mathbb{R}$. Wir sagen: p ist zerlegt in $\mathfrak{A}$, wenn $\mathfrak{A}_p$ die Matrizenalgebra ist, und p ist verzweigt, wenn $\mathfrak{A}_p$ die Divisonsalgebra ist ($p \in \mathbb{P}\cup\infty$). Auf einer Quaternionenalgebra gibt es eine Konjugation $\mathfrak{A} \ni a = w+xi+yj+zl \mapsto \overline{a} = w-xi-yj-zl$ mit $\overline{\overline{a}} = a$, $\overline{a_1 a_2} = \overline{a_1}\ \overline{a_2}$ und $\overline{a} = a \Leftrightarrow a \in k$. Man erhält hiermit eine Spur $tr(a) = a+\overline{a}$, und eine Norm $N(a) = a\overline{a}$ und für jedes $a \in \mathfrak{A}$ gilt: $a^2-(tr(a))+N(a) = 0$. Die Norm kann auch als quadratische Form über dem vierdimensionalen Vektorraum über k aufgefasst werden $N(w + xi + yj + zl) = w^2 - ax^2 - by^2 + abz^2$ (hier: $i^2 = a, j^2 = b$ und $ij = l = -ji$). Ein Kriterium für die Isomorphie von $\mathfrak{A}_p$ und einer Matrixalgebra -also ein Kriterium für die Zerlegtheit von p in $\mathfrak{A}$- ist, dass Spur und Norm gleichzeitig in $\mathfrak{A}$ verschwinden. Die Spur verschwindet auf einem dreidimensionalen Unterraum von $\mathfrak{A}$. Die Norm beschreibt auf diesem eine Quadrik, die an allen außer endlich vielen Primstellen nicht triviale Lösungen hat. Die Quaternionenalgebra $\mathfrak{A}$ ist also nur an endlich vielen Primstellen verzweigt [Lam, 5.5, p.181ff]. Umgekehrt bestimmt die Menge der Primstellen schon die Quaternionenalgebra bis auf Isomorphie [OMe,Theorem 71:19, p.203]. Sei nun $\mathfrak{A}$ eine Quaternionenalgebra über $\mathbb{Q}$ beziehungsweise über $\mathbb{Q}_p$. Ein Gitter in $\mathfrak{A}$ ist ein freier $\mathbb{Z}$-Modul beziehungsweise ein freier $\mathbb{Z}_p$ Modul vom Rang vier in $\mathfrak{A}$. Eine Ordnung $\mathfrak{O}$ in $\mathfrak{A}$ ist ein Gitter in $\mathfrak{A}$, das ein Unterring ist und die Eins enthält. Sei $\{v_1, v_2, v_3, v_4\}$ eine $\mathbb{Z}$-Basis eines Ideals I in $\mathfrak{O}$ und $a = n_1v_1 + n_2v_2 + n_3v_3 + n_4v_4 \in I$ gegeben. Die zu I gehörige Normform Q ist dann durch $N(a) = a\overline{a} = Q(n_1, n_2, n_3, n_4)$ definiert und ist eine positiv definite quadratische Form.

3.1.2 Konstruktion von Basen von $S_k(\Gamma_0(l))$

Zunächst wird mit Hilfe des folgenden Satzes ein Erzeugendensystem für $S_2(\Gamma_0(l))$ berechnet.

Satz 3.1
Sei $\mathfrak{A}$ eine Quaternionenalgebra, die genau in l und ∞ verzweigt ist, $\mathfrak{O}$ eine Ordnung der Stufe l in $\mathfrak{A}$ und $\{I_1, \ldots, I_H\}$ ein vollständiges Vertretersystem der Links-$\mathfrak{O}$-Idealklassen. Sei außerdem $Q'_{ij}(n_1, n_2, n_3, n_4)$ die Normform des Ideals $I_j^{-1}I_i$, wobei $I_j^{-1} = \{a \in \mathfrak{A} \mid I_j a I_j \subset I_j\}$, sowie $Q_{ij} = \frac{Q'_{ij}}{N(I_j^{-1}I_i)}$ und

$$\Theta_{ij}(\tau) = \sum_{n\in\mathbb{Z}} a_{Q_{ij}}(n)q^n = \sum_{n\in\mathbb{Z}^4} e^{2\pi i Q_{ij}(n)\tau}$$

die zu Q_{ij} gehörige Thetareihe, wobei $a_{Q_{ij}}(n)$ die Anzahl der Darstellungen von n durch die quadratische Form Q_{ij} ist. Dann ist

$$S_2(\Gamma_0(l)) = \sum_{i,j=2}^{H} < \theta_{ij}(\tau) - \theta_{1j}(\tau) > .$$

Beweis:
Siehe [Ei, Chapter IV, p.138ff].

□

Bemerkung 3.1

$H = H(l)$ bezeichnet hier die Klassenzahl der Links-$\mathfrak{A}$-Ideale der Quaternionenalgebra $\mathfrak{A}$, die genau in l und ∞ verzweigt ist.

$$
\begin{aligned}
H(l) &= \frac{l}{12}\left(1-\frac{1}{l}\right)+\frac{1}{4}\left(1-\left(\frac{-1}{l}\right)\right)+\frac{1}{3}\left(1-\left(\frac{-3}{l}\right)\right) \\
&= dim(S_2(\Gamma_0(l))+1 \\
&\overset{(l\geq 3)}{=} \begin{cases} n & falls \quad l=12n+1 \\ n+1 & falls \quad l=12n+5 \\ n+1 & falls \quad l=12n+7 \\ n+2 & falls \quad l=12n+11 \end{cases}
\end{aligned}
$$

Siehe [Ei, Theorem 6, p.113]

□

Mit Hilfe von verallgemeinerten Thetareihen lässt sich nun eine Basis der Räume $S_k(\Gamma_0(l))$ bestimmen. Hierzu werden zu einer quadratischen Form $Q(x) = \frac{1}{2}x^t Ax = \frac{1}{2}(Sx)^t Sx$ sphärische Polynome definiert. Ein homogenes Polynom P vom Grad d in vier Unbekannten heißt sphärisch vom Grad d bezüglich Q, falls für $P(x) = H(y)$ mit $y = Sx$ gilt:

$$\Delta(H(y)) = \sum_{n\in\mathbb{Z}^4} \frac{\partial^2 P}{\partial y_i^2} = 0.$$

Sei P ein sphärisches Polynom P bezüglich Q. Eine verallgemeinerte Thetareihe zur quadratischen Form Q und ein sphärisches Polynom P bezüglich Q ist definiert durch

$$\Theta(\tau; Q, P) = \sum_{n\in\mathbb{Z}^{2r}} P(n) e^{2\pi i Q(n)\tau}.$$

Da nun für $(a^*_{ij})_{i,j\in\{1,\dots,4\}} = A^{-1}$ ein homogenes Polynom P genau dann ein sphärisches Polynom ist, wenn gilt

$$\sum_{i,j=1}^{4} a^*_{i,j} \frac{\partial^2 P}{\partial x_i \partial x_j} = 0$$

(Siehe hierzu [Sch]) kann man durch Lösen eines linearen Gleichungssystems eine Basis des $(d+1)^2$-dimensionalen Raumes der sphärischen Polynome vom Grad d in vier Unbekannten bestimmen ([Pf], Bemerkung 3.31 und Korollar 3.30). Mit dem folgenden Satz erhält man dann eine Basis von $S_k(\Gamma_0(l))$.

Satz 3.2
Sei l eine Primzahl und $\mathbb{N} \ni k \geq 4$. Sei außerdem $\mathfrak{A}$ eine Quaternionenalgebra, die genau in l und ∞ verzweigt ist. $\mathfrak{O}$ sei eine Ordnung der Stufe l in $\mathfrak{A}$ und $\{I_1, \dots, I_H\}$ ein vollständiges Vertretersystem der Links-$\mathfrak{O}$-Idealklassen. Sei desweiteren $Q'_{ij}(n_1, n_2, n_3, n_4)$ die Normform des Ideals $I_j^{-1} I_i$, $Q_{ij} = \frac{Q'_{ij}}{N(I_j^{-1} I_i)}$ und $\{P_1^{i,y}, \dots, P_{(k-1)^2}^{i,y}\}$ eine Basis des Raumes der sphärischen Polynome bezüglich der quadratischen Form $Q_{ij}(x)$. Dann ist

$$S_k(\Gamma_0(l)) = \sum_{l=1}^{(k-1)^2} \sum_{i,j=1}^{H} < \sum_{n\in\mathbb{Z}^4} P_l^{(i,j)(n) e^{2\pi i Q_{ij}(n)\tau}} > \bigoplus S_k(SL_2(\mathbb{Z})) \bigoplus S_k(SL_2(\mathbb{Z}))^l.$$

(Die ersten beiden Summenzeichen stehen hier fuer eine nicht direkte Summe von Räumen.)

Beweis:
Siehe [Ei, Chapter IV].

□

3.1.3 Konstruktion von Modulfunktionen ohne endliche Nullstellen

Folgendes Lemma gibt uns Auskunft über die Operation der Fricke-Operation auf verallgemeinerten Thetareihen.

Lemma 3.1
Sei Q eine quadratische Form in vier Veränderlichen der Stufe l mit Diskriminante l^2 (l Primzahl), P ein sphärisches Polynom vom Grad d bezüglich Q. Q^* die zu Q adjungierte, quadratische Form und P^* die zu P adjungierte, sphärische Funktion, also $P^*(x) = P(A^{-1}x)$, wobei A die Darstellungsmatrix der quadratischen Form Q ist. Dann ist

$$\Theta(\tau; Q, P)|[\omega_l]_{(2+l)} = -l^{\frac{d}{2}}\Theta(\tau; Q^*, P^*).$$

Beweis:
Siehe [Pf, Korollar 3.33, p.41].

□

Durch obiges Lemma können die Räume $S_k(\Gamma_0(l))$ explizit in einen invarianten

$$S_k^+(\Gamma_0(l)) = \{f \in S_k(\Gamma_0(l)) | \omega_l f = f\}$$

und einen anti-invarianten Teilraum

$$S_k^-(\Gamma_0(l)) = \{f \in S_k(\Gamma_0(l)) | \omega_l f = -f\}$$

aufgespalten werden.

Betrachten wir im Weiteren den Fall $k = 12$. Die Funktion $\phi(\tau) := (\eta(\tau)\eta(l\tau))^{12}$ mit $\eta(\tau) = e^{\frac{2\pi i\tau}{24}} \prod_{n=1}^{\infty}(1 - e^{2\pi i n\tau}) = q^{\frac{1}{24}} \prod_{n=1}^{\infty}(1 - q^n)$ ist für $l > 3$ eine invariante Modulform für $\Gamma_0(l)$ vom Gewicht 12 ohne endliche Nullstellen. Sie hat unter allen invarianten Modulformen vom Gewicht 12 maximale Nullstellenordnung $\frac{l+1}{2}$ in 0 und ∞. Jede andere invariante Modulform vom Gewicht 12 für $\Gamma_0(l)$ ohne endliche Nullstellen ist ein skalares Vielfaches von ϕ. Ist nun $\{f_0(\tau), \ldots, f_r(\tau)\}$ eine Basis von $S_{12}^+(\Gamma_0(l))$ (beziehungsweise von $S_{12}^-(\Gamma_0(l))$), so sind die Funktionen $\frac{f_0(\tau)}{\phi(\tau)}, \ldots, \frac{f_r(\tau)}{\phi(\tau)}$ invariante (beziehungsweise anti-invariante) Modulfunktionen ohne endliche Pole für $\Gamma_0(l)$. War die Basis dabei entsprechend ihrer Polstellenordnung in ∞ angeordnet, so gilt dies auch für $\frac{f_i(\tau)}{\phi(\tau)}, i \in \{1, \ldots, r\}$. Desweiteren ist auch $ord_\infty\left(\frac{f_i(\tau)}{\phi(\tau)}\right)$ gleich $ord_0\left(\frac{f_i(\tau)}{\phi(\tau)}\right)$.

3.1.4 Darstellung von Modulfunktionen ohne endliche Pole

Die Fricke-Involution ω_l identifiziert die beiden Spitzen von $X_0(l)$, so dass $X_0^+(l)$ genau eine Spitze ∞^+ hat. Sei g^+ das Geschlecht von $X_0^+(l)$, was einfach berechnet werden. Siehe hierzu [Fr, p.366] und [He]. Der Raum $L((2g^+ + 1)\infty^+)$ hat nach Lemma 1.2 die Dimension $g^+ + 2$. Ist $\{f_0(\tau) = \phi(\tau), f_1(\tau), \ldots, f_r(\tau)\}$ eine Basis von $S_{12}(\Gamma_0(l))$, die ihrer Polstellenordnung entsprechend geordnet ist, so sind die Funktionen $1, x_1(\tau) = \frac{f_1(\tau)}{\phi(\tau)}, \ldots, x_{g^+ +1}(\tau) = \frac{f_{g^+ +1}(\tau)}{\phi(\tau)}$ eine Basis von $L((2g^+ + 1)\infty^+)$. Insbesondere ist $r \geq g^+ + 2$. Siehe hierzu [Pf, Proposition 4.16 und 4.17, p.73f]. Diese Modulfunktionen haben rationale Fourierkoeffizienten. Analog zu oben beschriebenem Verfahren kann man mit Hilfe von $S_{12}^-(\Gamma_0(l))$ eine anti-invariante Modulfunktion $s(\tau)$ berechnen. Es wird in [Pf, Proposition 4.22] gezeigt, dass sich jede invariante Modulfunktion f von $\Gamma_0(l)$ ohne endliche Pole als Polynom $P_f \in \mathbb{Q}[x_1(\tau), \ldots, x_{g^+ +1}(\tau)]$ darstellen lässt. Sei nun $f(\tau)$ eine beliebige Modulfunktion ohne endliche Pole für $\Gamma_0(l)$, die auch anti-invariant sein kann, so ist $\frac{1}{2}(f(\tau) + \omega_l f(\tau))$ eine invariante und $\frac{1}{2}(f(\tau) - \omega_l f(\tau))$ eine anti-invariante Modulfunktion für $\Gamma_0(l)$ ohne endliche Pole. Da $s(\tau)$ auch anti-invariant ist, muss das Produkt $\frac{1}{2}s(\tau)(f(\tau) - \omega_l f(\tau))$ invariant sein. Man erhält also für $\frac{1}{2}(f(\tau) + \omega_l(\tau))$ (beziehungsweise $\frac{1}{2}(f(\tau) - \omega_l f(\tau)))$ eine Darstellung als Polynom P (beziehungsweise Q) in $x_1(\tau), \ldots, x_{g^+ +1}(\tau)$ mit rationalen Koeffizienten. Dies gilt insbesondere für die Funktion $j(\tau)$ und $\omega_l j(\tau) = j(l\tau)$. Nach Satz 2.2 wird der Funktionenkörper von $\Gamma_0(l)$ von $j(\tau)$ und $j(l\tau)$ erzeugt, also auch von $x_1(\tau), \ldots, x_{g^+ +1}(\tau), s(\tau)$.

Bemerkung 3.2

i) Wir heben hier insbesondere hervor, dass bei der Konstruktion dieser Polynome ein Faktor 2 auftritt.

ii) Hat $X_0^+(l)$ in ∞^+ einen Weierstraß-Punkt, so werden im Allgemeinen nicht alle der Funktionen $x_1(\tau), \ldots, x_{g^+ +1}(\tau)$ zur Darstellung der invarianten Modulfunktionen ohne endliche Pole benötigt.

iii) Hat $X_0^+(l)$ in ∞ keinen Weierstraß-Punkt, so benötigt man im Allgemeinen alle Funktionen zur Darstellung der invarianten Modulfunktionen.

□

3.1.5 Relationen zwischen Modulfunktionen

Auf der Menge $Y_0(l) = X_0(l) - S(X_0(l)) = X_0(l) - \{0, \infty\}$ sind die Funktionen $j(\tau)$ und $j(l(\tau))$ definiert, und für $Y_0'(l) = Y_0(l) - \{\tau \in \mathbb{H} | s(\tau) = 0\}$ ist die Abbildung

$$\begin{aligned} \phi_l : Y_0'(l) &\to C_M(l) \subset \mathbb{A}^2 \\ \tau &\mapsto (j(\tau, j(l\tau)) \end{aligned}$$

eine Bijektion auf eine offene Teilmenge $C_M'(l)$ der glatte Kurve $C_M(l)$, die durch die Nullstellenmenge des Modulpolynoms beschrieben wird. Bezeichnen wir mit $C_p(l)$ die Varietät aus $\mathbb{A}^{n+1}$, die durch die Relationen zwischen $x_1, \ldots, x_n, s$ beschrieben werden, dann bildet auch die Abbildung

$$\begin{aligned} \psi_l : Y_0'(l) &\to C_P(l) \subset \mathbb{A}^{n+1} \\ \tau &\mapsto (x_1(\tau), \ldots, x_n(\tau), s(\tau)) \end{aligned}$$

bijektiv auf eine offene Teilmenge $C_P'(l)$ von $C_P(l)$ ab. Denn durch

$$\begin{gathered} p_l : C_P'(l) \to C_M(l) \\ (x_1(\tau), \ldots, x_n(\tau), s(\tau)) \mapsto (R_1(x_1(\tau), \ldots, x_n(\tau), s(\tau)), R_2(x_1(\tau), \ldots, x_n(\tau), s(\tau))) \end{gathered}$$

erhält man mit ϕ_l ein kommutatives Diagramm. Siehe hierzu auch Abbildung 3.1. Dabei sind R_1 und R_2 die Darstellungen von $j(\tau)$ und $j(l\tau)$ rationale Funktionen in $x_1(\tau), \ldots, x_n(\tau), s(\tau)$. Um die Varietät $C_P(l)$ zu beschreiben, können nun Relationen zwischen den Funktionen $x_1, \ldots, x_n, s$ gesucht werden. Da der Funktionenkörper von $\mathbb{Q}[x_1, \ldots, x_n, s]$ Transzendenzgrad eins hat, gibt es zu je zwei (oder mehr) Funktionen x_i, x_j ein Polynom P aus $\mathbb{Z}[X_i, X_j]$, so dass $P(x_i(\tau), x_j(\tau)) = 0$ gilt. Um eine solche Relation P zwischen m Funktionen zu bestimmen, setzt man formal

$$\begin{tikzcd}
& Y'(l) \arrow[dl, "\phi_l"'] \arrow[dr, "\psi_l"] \arrow[d, phantom, "\#"] & \\
\mathrm{Im}\,\phi_l = C'_M(l) \subseteq \mathbb{A}^2(\mathbb{C}) & & C'_P(l) \subseteq \mathbb{A}^{n+1}(\mathbb{C}) \arrow[ll, "p_l"]
\end{tikzcd}$$

Abbildung 3.1: Kommutatives Diagramm

$$P = \sum_{(e_1,\ldots,e_m)\in N_1\times\ldots\times N_m} \prod_{i=1}^{m} X_i^{e_i},$$

wobei $N_i = \{0, \ldots, a_i\}$ für eine zufällig gewählte, natürliche Zahl a_i ist. Nach Einsetzen der Fourierentwicklungen von x_i in X_i erhält man durch Koeffizientenvergleich ein lineares Gleichungssystem, das uns, falls es nichttrivial lösbar ist, eine Relation liefert. Gibt es keine nichttriviale Lösung, so erhöhe man eine der Zahlen a_i und stelle ein neues Gleichungssystem auf. Auf diese Art hat M. Pfeifer Relationen der Form $P_1(x_1, x_2), \ldots, P_{g^+}(x_1, \ldots, x_{g^++1})$ bestimmt (Falls $X_0^+(l)$ in ∞^+ einen Weierstraß-Punkt hat, reichen nach Bemerkung 3.2 weniger Relationen aus.). Die Funktion s^2 kann als invariante Funktion -wie oben gesehen- auch als ganzes Polynom in $x_1, \ldots, x_n$ dargestellt werden. Die so gewonnenen Relationen können also als Polynome über $\mathbb{Q}$ aufgefasst werden und sind nicht eindeutig bestimmt, da sie von der Wahl einiger, natürlicher Zahlen abhängen. Die von M. Pfeifer angegebenen Relationen wurden so gewählt, dass sie in einer rechnerisch günstigen Dreiecksform vorliegen. Diese Relationen wurden als Standard-Relationen bezeichnet. Von der durch das Ideal $(P_1(x_1, x_2), \ldots, P_{g^+}(x_1, \ldots, x_{g^++1}))$ definierten algebraischen Menge wissen wir nur dass sie eindimensional ist und eine ihrer Komponenten mit der gesuchten Kurve übereinstimmt. Das Modell, das zu dieser Komponente gehört, wollen wir Standardmodell nennen. Die durch obiges Ideal beschriebene algebraische Menge wollen wir mit C_P bezeichnen, die gesuchte Varietät mit C''_P.

Um eine Einteilung der Modelle vorzunehmen machen wir folgende Definition:

Definition 3.1
Wir teilen die Kurven $\Gamma_0(l)$ in Klassen ein. Wir sagen die Kurve $\Gamma_0(l)$ gehört zur Klasse N, falls die Kurve $\Gamma_0^+(l)$ das Geschlecht $g_0^+(l) = N$ hat.

□

Bemerkung 3.3

- Wir werden die Menge der Standard-Relationen gelegentlich auch als Standardmodelle bezeichnen. Dabei wird aus dem Kontext klar, ob wir die Varietät oder die algebraische Menge betrachten.

- Betrachten wir die oben beschriebene Konstruktion etwas genauer, so werden die Räume $L((2g^+ + 2)\infty^+)$ von $X_0^+(l)$ von $g_0^+ + 2$ Modulfunktionen erzeugt. Desweiteren braucht man noch eine unter der Fricke-Involution invariante Modulfunktion ohne endliche Pole, um den vollen Raum $O(X_0(l))$ zu erzeugen.

Damit hat $O(X_0(l))$ also $g^+ + 3$ Erzeuger. Ein Standardmodell der Klasse l liefert folglich eine algebraische Menge im $\mathbb{A}^{l+2}$, die durch höchstens $l+1$ Polynome gegeben ist. Hat $X_0^+(l)$ im Unendlichen keinen Weierstraß-Punkt, so werden diese im Allgemeinen benötigt, sonst weniger. Im Fall eines Weierstraß-Punktes hat man ein Standard-Modell in einem Raum $\mathbb{A}^{l'}$ mit $l' < l+2$, das durch $l'-1$ Polynome dargestellt wird.

□

3.2 Reduzibilität der Modelle

3.2.1 Reduktion einer Kurve

In diesem Abschnitt beschreiben wir den Begriff der Reduktion und folgen dabei [TV, Part 2, 2.6.1, p.234f]. Die hier eingeführte 'ad hoc' Definition werden wir übernehmen. Eine exakte Definition hingegen findet man zum Beispiel in

- G. Shimura, Abelian Varieties with Complex Multiplication and Modular Functions, Princeton University Press, 1998, Chapter III.

Sei P eine Primzahl, X eine affine Kurve über $\mathbb{Q}$ und $F_1, \ldots, F_n \in \mathbb{Z}[x_1, \ldots, x_m]$ eine Basis des Ideals $I = I(X)$. Mit $\overline{F_i}$, $i \in \{1, \ldots, n\}$ bezeichnen wir die Polynome aus $\mathbb{F}_p[x_1, \ldots, x_m]$, die man erhält, wenn man die Koeffizienten von F_i modulo p reduziert. Wir können ohne Einschränkung annehmen, dass jedes Polynom F_i mindestens einen Koeffizienten hat, der nicht durch p teilbar ist, so dass die Polynome $\overline{F_i}$ nicht verschwinden. Darüberhinaus kann eine Basis des Ideals I auch so gewählt werden, dass das System $0 = \overline{F_1} = \ldots = \overline{F_n}$ eine eindimensionale Varietät in $\mathbb{A}^m(\overline{\mathbb{F}_p})$ definiert. Bezeichnen wir diese mit $\overline{X}$ und nennen sie eine Reduktion von X modulo p. Der so definierte Begriff der Reduktion ist nicht eindeutig, er hängt von der Wahl einer Basis des Ideals I ab. Bei der Wahl einer anderen Basis für I erhalten wir eine andere Reduktion $\overline{X'}$ von X modulo p. Beide Reduktionen müssen nicht isomorph sein, im Gegenteil ist es sogar möglich dass $\overline{X}$ irreduzibel und $\overline{X'}$ reduzibel ist. Siehe hierzu auch Abschnitt 3.4. Gibt es eine irreduzible, glatte Reduktion von X, so sagen wir: X hat gute Reduktion modulo p. Es ist möglich, dass X zwei nicht isomorphe, gute Reduktionen hat. Ist X jedoch eine glatte, projektive Kurve, so ist die gute Reduktion von X modulo p bis auf Isomorphie eindeutig bestimmt.

Bemerkung 3.4

Der hier angegebene Begriff der guten Reduktion gibt keine Auskunft darüber, wie man eine Basis eines Ideals $I(X)$ einer Kurve X mit guter Reduktion finden kann, so dass diese bei Reduktion eine irreduzible Kurve $\overline{X}$ definiert. Es ist auch nicht klar welche der möglichen, guten Reduktionen einer affinen Kurve diejenige ist, an der man interessiert ist. Eine Möglichkeit den Begriff der guten Reduktion genauer zu fassen, liefert die Theorie der Schemata.

□

Nun wollen wir die von M. Pfeifer in [Pf] angegebenen Kurven bezüglich Reduktion untersuchen, das heißt wir werden die Koeffizienten der Kurven reduzieren und die Kurven, die wir erhalten auf Reduzibilität untersuchen. ersuchen, das heißt wir werden die Koeffizienten der Kurven reduzieren und die Kurven, die wir erhalten auf Reduzibilität untersuchen.

Proposition 3.1
Für einen algebraisch abgeschlossenen Körper ist eine algebraische Menge V genau dann irreduzibel, wenn das zugehörige Ideal I(V) ein Primideal ist.

Beweis:
Siehe [Ha,Chapter I, Paragraph 1, Corollary 1.4, p.4]
oder [CLS,Chapter 4, Paragraph 5, Corollary 4, p.196].

□

3.3 Primärzerlegung

Sei R ein kommutativer Ring mit Eins.

Definition 3.2
Ein Ideal Q aus R ($Q \neq R$) heißt Primärideal, falls für alle $a, b \in R$ gilt:

$$ab \in Q, a \notin Q \Rightarrow b^n \in Q \text{ für ein } n \in \mathbb{N}.$$

□

Ist Q ein Primärideal, so ist sein Radikal $\sqrt{Q}$ ein Primideal ([Hu, Theorem 2.9, p.380]), das wir das zu Q assoziierte Primideal nennen. Ist der Ring R darüberhinaus noethersch, dann lässt sich jedes Ideal I aus R als Schnitt endlich vieler Primärideale $I = \bigcap_{i=1}^{m} Q_i$ darstellen ([Hu, Theorem3.6, p.385]). Diese Darstellung nennen wir eine Primärzerlegung von I. Sei P_i das zu Q_i assoziierte Primideal. Enthält in einer Primärzerlegung keines der Q_i das Ideal $Q_1 \cap \ldots \cap Q_{i-1} \cap Q_{i+1} \ldots \cap Q_m$ und gilt für jedes P_i: $P_i \not\subset P_j$ für alle $j \neq i$, so nennen wir die Primärzerlegung reduziert. Die P_i nennen wir in diesem Fall isolierte Primideale. Zu jeder Primärzerlegung existiert eine reduzierte Primärzerlegung $I = \bigcap_{i=1}^{n} Q_i$ und die Menge der assoziierten $\{P_1, \ldots, P_n\}$ ist eindeutig bestimmt ([Hu, Theorem 3.4, Theorem 3.5]). In Satz 1.6 haben wir gesehen, wenn k ein algebraisch abgeschlossener Körper ist, gibt es eine bijektive Korrespondenz zwischen algebraischen Mengen im $\mathbb{A}^n(k)$ und Radikalidealen aus $k[x_1, \ldots, x_n]$. Ebenfalls haben wir gesehen, dass es eine bijektive Korrespondenz zwischen algebraischen Mengen in $\mathbb{P}^n$ und homogenen Radikalidealen in $k[x_0, \ldots, x_n]$ außer $(x_0, \ldots, x_n)$ gibt. Sei I ein Ideal in $k[x_1, \ldots, x_n]$ und $I = \bigcap_{i=1}^{m} Q_i$ eine reduzierte Primärzerlegung von I, dann ist $V(I) = V(P_1) \cup \ldots \cup V(P_m)$ eine Zerlegung von $V(I)$ in irreduzible Varietäten. Dabei ist jedes Primideal P_i das assoziierte Ideal von Q_i. Ist umgekehrt $V = V_1 \cup \ldots \cup V_m$ eine Zerlegung einer algebraischen Menge in Varietäten und für alle V_i gilt: $V_i \not\subset V_j$ falls $j \neq i$, dann ist $\sqrt{I(V)} = I(V_1) \cap \ldots I(V_m)$.

Ein Verfahren zur Berechnung der Primärzerlegung und der assoziierten Primideale lässt sich insbesondere dazu benutzen, um zu testen, ob ein gegebenes Ideal I ein Primideal ist. Algorithmen zur Berechnung wurden in [GTZ] und [SY] angegeben und sind im Computeralgebrasystem Singular [Si] implementiert. Weitere Algorithmen findet man in [DGP]. Für die Rechnungen über endlichen Körpern wurde der in [SY] beschriebene Algorithmus benutzt. Insbesondere wurden Rechnungen in den Polynomringen $K[X_1, \ldots, X_n]$ durchgeführt, wobei K hier einer der endlichen Körper $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{31}$, $\mathbb{F}_{1021}$ und n eine natürliche Zahl bezeichnet. In Charakteristik null wurde der Algorithmus aus [GTZ] verwendet.

Bemerkung 3.5

Es ist nicht notwendig, eine komplette Primärzerlegung zu berechnen. Es würde beispielsweise schon ausreichen die assoziierten Primideale zu berechnen. Gibt es nur ein assoziiertes Ideal, so muss dieses bereits das gesuchte Primideal sein.

□

Beispiel 3.1

Wir betrachten die Kurve $\Gamma_0(73)$ mit Geschlecht $g = 5$. Die Kurve $\Gamma_0^+(73)$ hat Geschlecht $g^+ = 2$, also handelt es sich hier um ein Modell der Klasse 2. Die algebraische Menge $C_P(73)$ hat in $\mathbb{Q}[X, Y, Z, S]$ drei definierende Gleichungen:

$$\begin{aligned} f_0 &= -Y^3 - 4XY^2 - 43Y^2 - 5X^2Y - 111XY - 606Y + \\ &\quad X^4 + 15X^3 + 39X^2 - 467X - 2508, \\ f_1 &= -YZ - 3XZ - 23Z - 6XY - 28Y + X^3 - 2X^2 - 133X - 474, \\ f_2 &= -S^2 - 8Y + X^2 - 12X - 144. \end{aligned}$$

Wenn wir diese nun über dem Körper mit drei Elementen betrachten, das heißt die Koeffizienten modulo drei reduzieren und die Primärzerlegung des von Ihnen aufgespannten Ideals (f_0, f_1, f_2) berechnen, erhalten wir eine Zerlegung des Ideals I in drei primäre Ideale Q_1, Q_2, Q_3. Dabei ist

$$\begin{aligned} Q_1 &= (Y^2 + Y + 1, X - YZ - Y + Z, S^2 + X - Y + 1), \\ Q_2 &= (Y^5 - Y^3Z - Y^3 - Y^2Z + YZ^2 - YZ + Y - Z^4 - Z, \\ &\quad XZ^2 + XZ - Y^3 - Y^2Z - Y + Z^2 + Z, \\ &\quad XY^2 - XYZ + XZ^2 - XZ + X - Y^2Z - YZ, \\ &\quad X^2 - XY + XZ - Y^2 + Y - Z, \\ &\quad S^2 - XY + XZ - Y^2 - Z), \\ Q_3 &= (Y - 1, X^2 - X + 1, S^2 - X). \end{aligned}$$

Die beiden Ideale Q_2 und Q_3 sind dabei schon Primideale, hingegen ist Q_1 ein primäres Ideal und hat als Radikal $Rad(Q_1) = (Y-1, X+1, S^2+1)$. Die algebraische Menge $C_p(73)$ ist also über dem Körper mit drei Elementen reduzibel. Siehe hierzu ~/data/primacp/k067-191c3.

□

Die Ergebnisse einiger solcher Rechnungen sind in Tabelle 3.3 zusammengefasst. Dabei bedeutet:

- I: Das Modell ist im angegebenen Fall irreduzibel,
- R: Das Modell ist im angegebenen Fall reduzibel,
- ?: Eine Rechnung ist nicht durchgeführt worden,
- H: Eine Rechnung wurde wegen Mangel an Speicher, Error, etc. abgebrochen.
- (W): Bei so gekennzeichneten Kurven der Stufe l hat die Kurve $X_0^+(l)$ im Unendlichen einen Weierstraß-Punkt.

Betrachten wir die Tabelle, so fällt sofort auf, dass die untersuchten, algebraischen Mengen $C_p(l)$ der Klasse N für N größer oder gleich zwei in allen untersuchten Fällen reduzibel sind. Desweiteren sieht man, dass viele Standardmodelle über dem Körper mit zwei Elementen ebenfalls zerfallen. Dies werden wir nun in den nächsten beiden Paragraphen genauer untersuchen.

3.3.1 Die Modelle über dem Körper $\mathbb{F}_2$

Die Standardmodelle der Klasse 0 haben die Form $S^2 = f(X)$. An den Diskriminanten der Polynome $f(X)$ sieht man direkt (Siehe Tabelle 3.3.1), dass die Modelle in Charakteristik zwei reduzibel sind. Für Modelle höherer Klassen kann man dies

Klasse	Stufe	Geschlecht	Primzahl 2	3	5	7	31	1021
0	11	1	R	I	I	I	I	I
	17	1	R	I	I	I	I	I
	19	1	R	I	I	I	I	I
	23	2	R	I	I	I	I	I
	29	2	R	I	I	I	I	I
	31	2	R	I	I	I	R	I
	41	3	R	I	I	I	I	I
	47	3	R	I	I	I	I	I
	59	5	R	I	I	I	I	I
	71	6	R	I	I	I	I	I
1	37	2	R	I	I	I	I	I
	43	3	R	I	I	I	I	I
	53	4	?	I	I	I	I	I
	61	4	?	I	I	I	I	I
	79	6	?	I	I	I	I	I
	83	7	?	I	I	I	I	I
	89	7	?	I	I	I	I	I
	101	8	?	I	I	I	I	I
	131	11	?	I	I	I	I	I
2	67	5	R	R	R	R	R	R
	73	5	R	R	R	R	R	R
	103	8	R	R	R	R	R	R
	107	9	R	R	R	R	R	R
	167	14	?	R	H	R	H	H
	191	16	H	R	R	R	R	R
3	97	7	H	H	R	R	R	R
	113	9	?	R	R	R	R	R
	127	10	?	R	R	R	R	R
	139	11	?	R	R	R	R	R
	149	12	?	R	R	R	R	R
	239	20	?	R	R	R	R	R
	109(W)	8	?	R	R	R	R	R
	151(W)	12	R	R	R	R	R	R
	179(W)	15	R	R	R	R	R	R
4	137	11	?	R	?	?	R	R
	173	14	?	R	?	?	R	R
5	157	12	?	H	?	?	?	?
6	163	13	?	?	?	?	?	?

Tabelle 3.1: Tabelle zur Beschreibung der Reduzibilität der Reduktion der Standardmodelle über den endlichen Körpern $\mathbb{F}_2$, $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{31}$ und $\mathbb{F}_{1021}$

Stufe	11	17	19	23	29
Diskriminante	$-2^8 \times 11^5$	$-2^8 \times 17^4$	$-2^8 \times 19^3$	$2^{12} \times 23^6$	$2^{12} \times 29^5$
Stufe	31	41	47	59	71
Diskriminante	$2^{12} \times 31^4$	$-2^{16} \times 41^6$	$2^{20} \times 47^8$	$2^{24} \times 59^9$	$2^{28} \times 71^{10}$

Tabelle 3.2: Diskriminanten der Polynome f(X) der Standardmodelle der Klasse null

noch einfach nachrechnen. So haben wir zum Beispiel für die Stufe 61 nach der Reduktion des Modells modulo zwei eine Varietät in $\mathbb{A}^3(\overline{\mathbb{F}_2})$, die in $\mathbb{F}_2[X,Y,S]$ durch das Ideal $(Y^3+X^2+XY+X, S^2+Y^4+Y^3+Y^2+Y+XY) = (Y^3+x^2+XY+X, S^2+Y^4+Y^2+X^2)$ beschrieben wird. Das Ideal auf der rechten Seite obiger Gleichung erhält man durch Addition des ersten Erzeugers zum Zweiten. Da wir nun in Charakteristik zwei rechnen, sehen wir, dass $S^2+Y^4+Y^2+X^2 = (S+Y^2+Y+X)^2$ ein Quadrat ist. Die linke Seite der Gleichung ist eine Gröbner Basis des Ideals bezüglich der lexikographischen Ordnung $S > X > Y$. Da die beiden Erzeuger als höchste Koeffizienten S^2 und X^2 haben, kann das Polynom $S+Y^2+X+Y$ nicht in obigem Ideal enthalten sein. Damit sind das angegebene Ideal, sowie das betrachtete Modell reduzibel. Ähnlich kann man auch für fast alle anderen angegebenen Modelle zeigen, dass sie über $\mathbb{F}_2$ reduzibel sind. Nicht nachgeprüft wurde dies für die Standardmodelle der Stufen $103, 107, 113, 127, 139, 149, 167, 173, 179, 191$ und 239. Deshalb und aufgrund von Problemen beim Einsatz von Singular für die Primzahl zwei (Siehe ˜/dip/primac2/) werden diese Modelle nicht in Charakteristik zwei behandelt.

Bemerkung 3.6

Betrachten wir die in [ShM] angegebenen Modelle, so sieht man, dass für alle dort angegebenen hyperelliptischen Kurven (diese Modelle haben Geschlecht größer als eins und haben nicht notwendig eine Primzahlstufe), die durch eine Gleichung der Form $y^2 = f(x)$ gegeben sind, die Diskriminante von $f(x)$ durch zwei teilbar ist. Genau wie bei [Pf] tritt bis auf die Teiler der Stufe kein weiterer Faktor in der Diskriminante auf.

□

Bemerkung 3.7

Bei der Konstruktion des Standardmodelles tritt, wie in Bemerkung 3.2 schon hervorgehoben wurde, die Zahl zwei als Faktor auf. Genauer gesagt: Betrachtet man die Abbildung 3.1, dann beschreibt p_l einen Morphismus von $C_p''(l)$ nach $C_M(l)$, den man, wie aus der Konstruktion der Modelle hervorgeht, durch $(\frac{sP+Q}{2s}, \frac{sP-Q}{2s})$ mit Polynomen P und Q aus $\mathbb{Z}[x_1,\ldots,x_n]$ angeben kann. Die Zahl zwei im Nenner der beiden rationalen Abbildungen wird wohl für die Reduzibilität modulo zwei verantwortlich sein. Die beiden Polynome P und Q sind, wie in [Pf, p 79] angegeben groß, können wohl aber noch für die vorliegenden Modelle berechnet werden.

□

3.3.2 Die Modelle der Klassen größer oder gleich zwei über $\mathbb{Q}$

Die Modelle der Klassen größer gleich zwei sind in allen untersuchten Fällen reduzibel. Der Gedanke, dass die Modelle auch schon in Charakteristik null reduzibel sind, liegt nahe. Berechnet man nun (hier mit Hilfe des Computeralgebrasystems Singular [Si]) eine Primärzerlegung in Charakteristik null, so sieht man, dass die angegebenen Relationen in der Tat eine reduzibele algebraische Menge definieren.

Beispiel 3.2

Das Standardmodell für $Y_0(67)$ in $\mathbb{Q}[X,Y,Z,S]$ ist gegeben durch die Relationen f_1, f_2, f_3, wobei:

$$\begin{aligned}
f_1 &= -Y^3 - 4XY^2 - 47Y^2 - 5X^2Y - 121XY - 724Y + X^4 + 15X^3 \\
&\quad +34X^2 - 602X - 3348, \\
f_2 &= -YZ - 3XZ - 22Z - 6XY - 27Y + X^3 - X^2 - 131X - 474, \\
f_3 &= -S^2 - 4Z + Y^2 + 2XY + 20Y - 7X^2 - 76X - 204.
\end{aligned}$$

Berechnen wir eine Primärzerlegung für das Ideal $I = (f_1, f_2, f_3)$, so erhalten wir eine Zerlegung $I = \bigcap_{i=1}^{4} Q_i$, wobei die Q_i primäre Ideale sind, die gegeben sind durch:

$$\begin{aligned}
Q_1 &= (Y^2 + 20Y + 100, \quad 3XZ + 15X + YZ + 3Y + 22Z + 90, \\
&\quad XY + 10X + 4Y + 40, X^2 + 8X + 16, \quad S^2 + 40X + 8Y + 4Z + 272) \\
Q_2 &= (Y - 8, \quad X + 10, \quad S^2 + 4Z + 80), \\
Q_3 &= (Y + 13, \quad X + 3, \quad S^2 + 4Z + 52), \\
Q_4 &= (Y^5 + 12Y^4 - 15Y^3Z - 482Y^3 - 15Y^2Z^2 - 767Y^2Z - 12264Y^2 \\
&\quad -242YZ^2 - 10317YZ - 101615Y - Z^4 - 25Z^3 - 1149Z^2 \\
&\quad -42385Z - 293100, \\
&\quad XZ^4 + 159XZ^3 + 8754XZ^2 + 157428XZ + 669960X + 3Y4Z + 126Y^4 \\
&\quad -Y^3Z^2 - 93Y^3Z - 318Y^3 - Y^2Z^3 - 141Y^2Z^2 - 6261Y^2Z - 77382Y^2 \\
&\quad -30YZ^3 - 2477YZ^2 - 69459YZ - 772314Y + 15Z^4 + 1766Z^3 \\
&\quad +59229Z^2 + 719286Z + 1784520, \\
&\quad 1368XY + XZ^3 + 117XZ^2 + 4296XZ + 35820X + 3Y^4 - Y^3Z - 51Y^3 \\
&\quad -Y^2Z^2 - 99Y^2Z - 2559Y^2 - 30YZ^2 - 1217YZ - 11505Y + 15Z^3 \\
&\quad +1136Z^2 + 22461Z + 170820, \\
&\quad 5472X^2 + XZ^3 + 117XZ^2 + 5664XZ + 72756X + 3Y^4 - Y^3Z - 51Y^3 \\
&\quad -Y^2Z^2 - 99Y^2Z - 3927Y^2 - 30YZ^2 - 1217YZ - 45705Y + 15Z^3 \\
&\quad +1136Z^2 + 27933Z + 80532, \\
&\quad 5472S^2 + XZ^3 + 117XZ^2 - 5280XZ + 193140X + 3Y^4 \\
&\quad -Y^3Z - 51Y^3 - Y^2Z^2 - 99Y^2Z + 1545Y^2 - 30YZ^2 - 1217YZ \\
&\quad +118455Y + 15Z^3 + 1136Z^2 + 6045Z + 1919124).
\end{aligned}$$

Dabei sind Q_2, Q_3 und Q_4 Primideale, und das zu Q_1 assoziierte Primideal kann durch $P_1 = (Y + 10, X + 4, S2 + 4Z + 32)$ angegeben werden (Die Ergebnisse der Berechnungen der Primärzerlegung befinden sich in ~/data/primac0/k067c0). Reduzieren wir nun die gegebenen Primideale modulo der Primzahl 67 und berechnen für jedes dieser Ideale wiederum eine Primärzerlegung, dann sehen wir, dass nur das Primideal Q_4 modulo 67 reduzibel ist. Der Funktionenkörper $\mathbb{Q}(j, j_l)$ der Modulkurve $C_M(l)$ ist, wie wir bereits in Abschnitt 3.1.4 gesehen haben, in $\mathbb{Q}(x_1, \ldots, x_, s)$ enthalten und die Kurve $C''_P(67)$ ist birational zu $C_M(67)$. In Abschnitt 2.9 haben wir gesehen, dass $C_M(67)$ modulo 67 reduzibel ist. In [Ig] wird gezeigt, dass die Reduktion modulo 67 von $C_P(67)$ entweder reduzibel oder eine Kurve von kleinerem Geschlecht ist.

Eine Möglichkeit nachzuweisen, welche der Primideale die Kurve $C''_p(67)$ definiert, besteht darin, die in [Pf] bei der Konstruktion des obigen Modells angegebenen Fourierentwicklungen der Basen der Spitzenformen zu betrachten. Diese sind im Fall der Stufe 67:

$$\begin{aligned}
X &= q^{-3}+q^{-2}+3q^{-1}+9q+13q^2+23q^3+33q^4+52q^5+75q^6+111q^7\\
&\quad +156q^8+225q^9+308q^{10}+430q^{11}+583q^{12}+796q^{13}+1061q^{14}\\
&\quad +1424q^{15}+1873q^{16}+O(q^{17}),\\
Y &= q^{-4}+3q^{-2}+3q^{-1}+14q+30q^2+45q^3+84q^4+129q^5+214q^6\\
&\quad +326q^7+512q^8+758q^9+1149q^{10}+1669q^{11}+2445q^{12}\\
&\quad +3488q^{13}+4989q^{14}+6993q^{15}+O(q^{16}),\\
Z &= q^{-5}+3q^{-1}+13q+28q^2+64q^3+120q^4+237q^5+414q^6+739q^7\\
&\quad +1234q^8+2052q^9+3290q^{10}+5239q^{11}+8106q^{12}+12456q^{13}\\
&\quad +18772q^{14}+O(q^{15}),\\
S &= q^{-4}+q^{-3}-4-11q-21q^2-42q^3-77q^4-127q^5-213q^6-341q^7\\
&\quad -536q^8-817q^9-1233q^{10}-1817q^{11}-2662q^{12}-3828q^{13}\\
&\quad -5462q^{14}-7693q^{15}+O(q^{16}).
\end{aligned}$$

Setzen wir diese in die Erzeuger der Ideale Q_1, Q_2, Q_3 ein, dann sehen wir sofort, dass diese Erzeuger keine Relationen zwischen Funktionen auf $X_0(67)$ erfüllen. Deshalb kann nur Q_4 ein Modell für $Y_0(67)$sein.

□

Im Laufe der Ausführungen werden noch weitere Kurven angegeben die mit Hilfe dieses Verfahrens bestimmt wurden. Siehe hierzu auch das Verzeichnis '~/data/verbmod'. Bei dieser Darstellung des Modells können wir nun aber weder davon ausgehen, dass es in einer Dreiecksgestalt vorliegt, noch, dass ein Modell der Klasse N durch $N+1$ Polynome gegeben ist. Die so gewonnenen Darstellungen der Modelle haben allerdings im Vergleich zu den Modulpoynomen in den berechneten Fällen aufgrund ihrer kleinen Koeffizienten ein 'kleines' Modell, das oft in wenigen Zeilen hingeschrieben werden kann. Bei der Berechnung dieser Darstellung der Modelle wird aber eine Primärzerlegung berechnet, was sehr aufwendig ist. Man kann sich damit begnügen die assoziierten Primideale zu berechnen, was keine direkte Verbesserung darstellt. Mit Hilfe der beiden Singular-Funktionen 'minAssGTZ();' und 'minAssChar();', mit denen man die assoziierten Primideale eines Ideals berechnen kann, konnten keine weiteren Kurven bestimmt werden. Eine Verbesserung wäre es wohl Eine Methode anzugeben, mit deren Hilfe man direkt aus den angegebenen Fourierentwicklungen Relationen berechnen kann die die gesuchte Modulkurve darstellen .

Allgemein haben wir also folgendes Problem zu lösen:
Gegeben seien die Fourierentwicklungen der Koordinatenfunktionen $x_1, \ldots, x_n$ eines algebraischen Funktionenkörpers vom Transzendenzgrad eins. Gebe nun ein Verfahren an, die die zu diesem Funktionenkörper gehörende Kurve in möglichst günstiger Zeit bestimmt. Anders ausgedrückt: Bestimme eine Menge von Relationen $R := \{r_1, \ldots, r_m\}$ zwischen $x_1, \ldots, x_n$, die aufgefasst als Polynome in $k[x_1, \ldots, x_n]$ ein Primideal definieren.

Bemerkung 3.8

Mit oben angegebenem Verfahren kann man das Problem zwar lösen, aus Zeitgründen wäre es aber wünschenswert die Berechnung einer Primärzerlegung zu vermeiden. Zum Testen ob R ein Ideal Primideal ist,könnte man versuchen einen Algorithmus(Ein Beispiel eines solchen Algorithmus findet sich in [AL]) so zu modifizieren, dass man zu einem Ideal R, das aus schon bestimmten Relationen besteht, aber noch kein Primideal ist, Bedingungen findet, die an die noch zu suchenden Relationen gestellt werden, um zu garantieren, dass diese zusammen mit den schon gefundenen Relationen ein Primideal erzeugen. Gut wäre es, eine obere Schranke für den (Total-)Grad der Polynome von R anzugeben, so dass alle Relationen mit kleinerem Grad das gesuchte Ideal erzeugen. Dies wird im Allgemeinen wohl nicht möglich sein. Hier kann man sich aber auf den Spezialfall der Modelle für Modulkurven zurückziehen. Weitere Möglichkeiten zur Beschleunigung der Berechnungen von Primärzerlegungen (beziehungsweise zur Berechnung der Menge der Assoziierten zu einem Ideal) sind in [DGP] beschrieben. Dort finden sich unter Anderem auch Laufzeitvergleiche der angegebenen Algorithmen.

□

Wendet man obiges Verfahren (Einsetzen von Erzeugern in eine Primärzerlegung) auf die anderen Standardmodelle an, dann erhalten wir die unten nach ihrer Stufe aufgelisteten Modelle. Die Reduzibilität der einzelnen Komponenten modulo Stufe des Modells wurde in den meisten Fällen auch untersucht. Es fällt auf, dass in allen Fällen das Modell für $C'_P(l)$ modulo l reduzibel ist. Die Ergebnisse sind vor jedem Modell kurz zusammengefasst. Rechnungen hierzu finden sich in dem Verzeichnis '~/data/komtest'.

Stufe 67: Das Ideal zerfällt in vier Primärideale. wovon drei Primideale sind. Eines ist modulo 67 reduzibel. Die anderen und das Radikal des Primärideals sind nicht reduzibel. Als Modell erhalten wir:

$$\begin{aligned}
f_1 &= Y^5+12Y^4-15Y^3Z-482Y^3-15Y^2Z^2-767Y^2Z-12264Y^2\\
&\quad -242YZ^2-10317YZ-101615Y-Z^4-25Z^3-1149Z^2\\
&\quad -42385Z-293100,\\
f_2 &= XZ^4+159XZ^3+8754XZ^2+157428XZ+669960X+3Y^4Z\\
&\quad +126Y^4-Y^3Z^2-93Y^3Z-318Y^3-Y^2Z^3-141Y^2Z^2-6261Y^2Z\\
&\quad -77382Y^2-30YZ^3-2477YZ^2-69459YZ-772314Y+15Z^4\\
&\quad +1766Z^3+59229Z^2+719286Z+1784520,\\
f_3 &= 214113888XY+156516XZ^3+18312372XZ^2+672392736XZ\\
&\quad +1159Y^5Z+5606403120X+75126Y^5+13908Y^4Z+1371060Y^4\\
&\quad -17385Y^3Z^2-1842044Y^3Z-44193048Y^3-17385Y^2Z^3\\
&\quad -2172359Y^2Z^2-87330702Y^2Z-1321869708Y^2-280478YZ^3\\
&\quad -34833375YZ^2-1083326699YZ-9434645070Y-1159Z^5\\
&\quad -104101Z^4-862101Z^3+42358187Z^2-8412534Z\\
&\quad +4716632520,\\
f_4 &= 5472X^2+XZ^3+117XZ^2+5664XZ+72756X+3Y^4-Y^3Z\\
&\quad -51Y^3-Y^2Z^2-99Y^2Z-3927Y^2-30YZ^2-1217YZ\\
&\quad -45705Y+15Z^3+1136Z^2+27933Z+80532,\\
f_5 &= 5472S^2+XZ^3+117XZ^2-5280XZ+193140X+3Y^4-Y^3Z\\
&\quad -51Y^3-Y^2Z^2-99Y^2Z+1545Y^2-30YZ^2-1217YZ\\
&\quad +118455Y+15Z^3+1136Z^2+6045Z+1919124.
\end{aligned}$$

Stufe 73: Das Ideal zerfällt in drei Primärideale. Zwei davon sind Primideale und modulo 73 reduzibel, das Radikal des Dritten ist modulo 73 nicht reduzibel. Als Modell erhalten wir:

$$f_1 = Y^5-19Y^3Z-667Y^3-15Y^2Z^2-679Y^2Z-10194Y^2-164YZ^2$$

$$
\begin{aligned}
& -7429YZ - 55226Y - Z^4 - 9Z^3 - 282Z^2 - 25732Z - 98520, \\
f_2 &= XZ^4 + 173XZ^3 + 9193XZ^2 + 112143XZ - 553518X + 3Y^4Z \\
& +171Y^4 - Y^3Z^2 - 115Y^3Z - 906Y^3 - Y^2Z^3 - 154Y^2Z^2 \\
& -6966Y^2Z - 96309Y^2 - 24YZ^3 - 2239YZ^2 - 74245YZ \\
& -1126086Y + 16Z^4 + 1949Z^3 + 54262Z^2 + 179319Z - 6416514, \\
f_3 &= 4900145019890491511800920 0XY + 2722302788828050839889 4XZ^3 \\
& +12448847172826100Y^5Z^3 + 3157871235040538974271704XZ^2 \\
& +28131806504283233 50Y^5Z^2 + 8659645171262029721688181 4XZ \\
& +2851168295444746049 75Y^5Z - 4736806852560808461407556X \\
& +995536029088568134147 5Y^5 + 8166908366484152519668 2Y^4 \\
& -236528096283695900Y^3Z^4 - 6175381342241315235 0Y^3Z^3 \\
& -729361125518070916897 5Y^3Z^2 - 4065477987212730154052 44Y^3Z \\
& -821916093154101894189967 7Y^3 - 186732707592391500Y^2Z^5 \\
& -5065047698677377215 0Y^2Z^4 - 6313805652887739892675Y^2Z^3 \\
& -39882532306273031352894 4Y^2Z^2 \\
& -12306804303050961068669393Y^2Z \\
& -15693825061371603120354322 8Y^2 - 2041610936343480400YZ^5 \\
& -55384411231717012630 0YZ^4 - 6834577913129234358165 0YZ^3 \\
& -4559525398310440367261731YZ^2 - 12448847172826100Z^7 \\
& -113415490920105204035603799YZ - 2925220274983758250Z^6 \\
& -82741516582913726241621936 2Y - 31394603030106647532 5Z^5 \\
& -1363506243565790117615 0Z^4 + 1919520327426867198918 79Z^3 \\
& +1780908750259850611969842 8Z^2 - 786563890207998858700091 8Z \\
& -25271245259681667638360939 88, \\
f_4 &= 7200X^2 + XZ^3 + 116XZ^2 + 4981XZ + 53826X + 3Y^4 - Y^3Z \\
& -58Y^3 - Y^2Z^2 - 97Y^2Z - 3837Y^2 - 24YZ^2 - 871YZ - 46198Y \\
& +16Z^3 + 1037Z^2 + 19153Z - 67602, \\
f_5 &= 7200S^2 + XZ^3 + 116XZ^2 + 4981XZ + 140226X + 3Y^4 - Y^3Z \\
& -58Y^3 - Y^2Z^2 - 97Y^2Z - 3837Y^2 - 24YZ^2 - 871YZ + 11402Y \\
& +16Z^3 + 1037Z^2 + 19153Z + 969198.
\end{aligned}
$$

Stufe 103: Das Ideal zerfällt in drei Primärideale. Zwei davon sind Primideale. Als Modell erhalten wir:

$$
\begin{aligned}
f_1 &= 85X^2 - 12XY + Y^2 - XZ - 382X + 67Y - 5Z - 33, \\
f_2 &= 179XYZ - 22Y^2Z + 22XZ^2 + 85S^2 - 5176077XY + 22596Y^2 + \\
& 1024083XZ - 9464YZ - 2525Z^2 + 142639853X - 22858798Y \\
& +1600496Z + 10463112, \\
f_3 &= 85Y^3 - 1303XYZ + 144Y^2Z - 144XZ^2 - 510S^2 + 38393913XY \\
& -774889Y^2 - 7434509XZ + 204043YZ + 10075Z^2 - 998992477X \\
& +161564527Y - 11391802Z - 74261163, \\
f_4 &= 12XY^2 - Y^3 + XYZ - 30627XY - 4715Y^2 + 7283XZ + 1025YZ \\
& -85Z^2 + 1311691X - 198163Y + 13210Z + 87339, \\
f_5 &= 15215S^2X + 2258025Y^2Z - 10291545XZ^2 + 517310YZ^2 \\
& -15215Z^3 - 25985605S^2 + 1225129597792XY - 53748105631Y^2
\end{aligned}
$$

$$
\begin{aligned}
& -230234654024XZ + 13041496875YZ - 102584545Z^2 \\
& -29066989623658X + 4777718694693Y - 341135335275Z \\
& -2220689177472, \\
f_6 \quad = \quad & 15215Y^2Z^2 - 15215XZ^3 - 2723485S^2Y - 182580S^2Z \\
& -6376140445Y^2Z + 10809928380XZ^2 + 197931935YZ^2 \\
& -21650945Z^3 + 16364134550S^2 - 1708316087450576XY \\
& +168750039783508Y^2 + 295964541172387XZ \\
& -38839394336275YZ + 1478229965365Z^2 \\
& +31389277347371224X - 5423661800653649Y \\
& +401223855748555Z + 2576466232608771, \\
f_7 \quad = \quad & 3043S^2Y^2 - 106505XZ^3 + 66946YZ^3 - 3043Z^4 - 175130736S^2Y \\
& -12969266S^2Z - 388124942354Y^2Z + 838055552208XZ^2 \\
& -5093279067YZ^2 - 601585885Z^3 + 1459078424064S^2 \\
& -122462915456684912XY + 10389996706780315Y^2 \\
& +21671705727322449XZ - 2408169078865176YZ \\
& +81654479578513Z^2 + 2416440188815859960X \\
& -411309577297000511Y + 30114017281121251Z \\
& +194102912912355606, \\
f_8 \quad = \quad & 852040XZ^4 - 15215YZ^4 + 15215S^4 - 158099065S^2YZ \\
& -13678285S^2Z^2 + 571728045075XZ^3 - 9419530425YZ^3 \\
& -600201320Z^4 - 82505268466080S^2Y \\
& -3561137467775S^2Z - 1977324692039286 35Y^2Z \\
& +370631835023804360XZ^2 + 3033018332153025YZ^2 \\
& -554734850847265Z^3 + 566629396424567850S^2 \\
& -5573525355093425076 1456XY + 5087777186995411255533Y^2 \\
& +976802457401549206 1417XZ - 1175166042719465532095YZ \\
& +422784497932783858 60Z^2 + 10647446711716065425 74924X \\
& -182446182254336923753039Y + 134196250774683296213 90Z \\
& +863326414341954494 00286, \\
f_9 \quad = \quad & 852040YZ^5 - 47714240S^4Y - 852040S^4Z + 1505554680S^2YZ^2 \\
& -1333442600S^2Z^3 - 2982386072195YZ^4 + 92299789120Z^5 \\
& -2005266082885S^4 + 8307083375589235S^2YZ \\
& +1493926577923415S^2Z^2 - 4673193282073978954 5XZ^3 \\
& +126492903211436607 5YZ^3 + 1587892877858 0720Z^4 \\
& +599062100176893242 5560S^2Y + 236984840578788741925S^2Z \\
& +14325233361092667759210985Y^2Z \\
& -27134368364789262183840880XZ^2 \\
& -19615932919071141374775 5YZ^2 + 393865571588947105465 95Z^3 \\
& -4177253755184701649357 8270S^2 \\
& +40586900991104766248325856 45392XY \\
& -36708087255692242301996088 2191Y^2 \\
& -71223276803324570743402940 6059XZ \\
& +84824938428136334521019729605YZ
\end{aligned}
$$

$$
\begin{aligned}
& -3030149920606321959741401140Z^2 \\
& -77868206426598823278598180990468X \\
& +13330899720524067753581342257533Y \\
& -979931261180969334113043648050Z \\
& -6305589150182651964665838245202, \\
f_{10} \quad = \quad & 170408S^2YZ^4 - 9542848Z^7 - 170408S^6 + 14901668376S^4YZ \\
& +477653624S^4Z^2 - 990258780840S^2YZ^3 + 293494380032S^2Z^4 \\
& -33402647665800Z^6 + 54794317074335104S^4Y \\
& +1564253165260856S^4Z - 4330197374334734112S^2YZ^2 \\
& +1076452007989552880S^2Z^3 + 3317054476232293263899YZ^4 \\
& -112098076215459516840Z^5 + 2051735968694283465029S^4 \\
& -8774772945725394170364283S^2YZ \\
& -1564087761090159438484175S^2Z^2 \\
& +48169512160009668027902214961XZ^3 \\
& -1236686361696205210919567035YZ^3 \\
& -20445131288808033061308592Z^4 \\
& -6307071427173289550965115161568S^2Y \\
& -253431926078278352990138507789S^2Z \\
& -15075617560766525597086279678354881Y^2Z \\
& +28548991643418429724804235164418320XZ^2 \\
& +206436000302373312940399610651051YZ^2 \\
& -41415531859352070765111375107683Z^3 \\
& +43954449624182165993414714862407278S^2 \\
& -4272236419820700273728331756757791236560XY \\
& +386638647595856156890905417315710255927Y^2 \\
& +749640347353460111017437973449284849667XZ \\
& -89341565486070503434723896635052817053YZ \\
& +3193047035547461832609436938004010628Z^2 \\
& +81941484094319730116382141458743361997124X \\
& -14029092585713499805228742989760353236885Y \\
& +1031297718510230438694607765134844393242Z \\
& +6636030308732194372387483414363464736818, \\
f_{11} \quad = \quad & 106505Z^8 - 106505S^6Y - 162952650S^4YZ^2 - 8307390S^4Z^3 \\
& -3069580605S^2Z^5 + 618910885985Z^7 - 81156810S^6 \\
& -977320502637115S^4YZ - 26442383708685S^4Z^2 \\
& +76690727792168420S^2YZ^3 - 19547854789872150S^2Z^4 \\
& +2008248536618741235Z^6 - 3329418458973250214410S^4Y \\
& -96186583518183406640S^4Z + 262610130898511183081490S^2YZ^2 \\
& -65020531862530212757145S^2Z^3 \\
& -201328855919750617593640975YZ^4 \\
& +6805890408283280756192100Z^5 \\
& -124497223078915375892482200S^4 \\
& +532408720904386195950247733105S^2YZ
\end{aligned}
$$

$$
\begin{aligned}
&+949157961025049226700626217 20S^2Z^2\\
&-2922682372725941490974004321890545XZ^3\\
&+750112536385724404501187074215 35YZ^3\\
&+1241943256906706807023463719485Z^4\\
&+38273385347126887373068655934101 5845S^2Y\\
&+153806955558187847487570038466708 35S^2Z\\
&+914834589622012965377432296253517694785Y^2Z\\
&-1732444879589498196669934759810592470320XZ^2\\
&-1252648434406645985968076653122072 3475YZ^2\\
&+251318026488236440322991336538301 8605Z^3\\
&-266730986781769080976055735706063 9069255S^2\\
&+2592534787710500107973647786065481673716 25424XY\\
&-234625439968747168362297595134528590256632 87Y^2\\
&-454906551732653869546472689091845316562 92163XZ\\
&+542154873966118711482861117576426125061 8250YZ\\
&-193765086047147380202858133019855918098415Z^2\\
&-4972478358930832488692357294233766444623454756X\\
&+8513315114361695197654708871268518532299941 91Y\\
&-625825449673895855890770101561511264866129 55Z\\
&-402696188096432715457285537047932163635592024.
\end{aligned}
$$

Stufe 107: Das Ideal zerfällt in drei Primärideale. wovon zwei Primideale sind. Beide und das Radikal des dritten Primärideals sind modulo 107 reduzibel. Als Modell erhalten wir:

$$
\begin{aligned}
f_1 &= Y^5+8Y^4-Y^3Z+9Y^3-5Y^2Z^2-53Y^2Z-160Y^2-29YZ^2\\
&\quad -285YZ-739Y-Z^4-17Z^3-142Z^2-646Z-1144,\\
f_2 &= XZ^4+24XZ^3+205XZ^2+722XZ+860X+2Y^4-Y^3Z^2\\
&\quad -11Y^3Z-12Y^3-Y^2Z^3-22Y^2Z^2-143Y^2Z-244Y^2-4YZ^3\\
&\quad -77YZ^2-441YZ-774Y+4Z^4+86Z^3+646Z^2+2004Z+2048,\\
f_3 &= 1178089575981462XY+5478119302100Y^5Z^3\\
&\quad +589044787990731XZ^2+174699255379280Y^5Z^2\\
&\quad +6479492667898041XZ+1494087090858139Y^5Z\\
&\quad +16493254063740468X+4162331631979121Y^5\\
&\quad +43824954416800Y^4Z^3+1397594043034240Y^4Z^2\\
&\quad +11952696726865112Y^4Z+33298653055832968Y^4\\
&\quad -5478119302100Y^3Z^4-125396181660380Y^3Z^3\\
&\quad +78206207555381Y^3Z^2+9284452185744130Y^3Z\\
&\quad +36871939899821358Y^3-27390596510500Y^2Z^5\\
&\quad -1163836599907700Y^2Z^4-1760599507772853 5Y^2Z^3\\
&\quad -127950154836061772Y^2Z^2-460246555820186384Y^2Z\\
&\quad -671274464208575939Y^2-158865459760900YZ^5\\
&\quad -6627542407097620YZ^4-97166143582232731YZ^3\\
&\quad -675625187947252044YZ^2-5478119302100Z^7
\end{aligned}
$$

$$\begin{aligned}
& -2292751054410177130YZ - 2678272835149 80Z^6 \\
& -3085976837428412846Y - 5241867373204099Z^5 \\
& -57907971509581844Z^4 - 402042692102118075Z^3 \\
& -1753731121437326372Z^2 - 4378074343408538328Z \\
& -4719296162248781792, \\
f_4 &= 2X^2 + XZ^2 + 13XZ + 36X - Y^3 - Y^2Z - 11Y^2 - 4YZ - 35Y \\
& +4Z^2 + 38Z + 56, \\
f_5 &= 2S^2 + XZ^3 - 180XZ^2 - 2139XZ - 4246X - Y^3Z + 185Y^3 \\
& -Y^2Z^2 + 178Y^2Z + 1917Y^2 - 6YZ^2 + 767YZ + 5779Y + 4Z^3 \\
& -710Z^2 - 6226Z - 7738.
\end{aligned}$$

Stufe 167 Das Ideal zerfällt in vier Primärideale. Drei davon sind Primideale. Eines der Primideale ist modulo 167 reduzibel. Die anderen Beiden und das Radikal des vierten Primärideals sind modulo 167 nicht reduzibel. Als Modell erhalten wir:

$$\begin{aligned}
f_1 &= 2X^2 - XY - Y^2 + XZ + 3X - 6Y - 5, \\
f_2 &= 2Y^3 - XYZ + Y^2Z - XZ^2 - 8XY + 8Y^2 - 11XZ - 2YZ \\
& -6Z^2 - 24X - 2Y - 29Z - 32, \\
f_3 &= XY^2 + Y^3 - XYZ - 4XY + 3Y^2 - 5XZ - 4YZ - 2Z^2 - 17X \\
& -13Y - 18Z - 39, \\
f_4 &= 9XYZ^3 + 5Y^2Z^3 - XZ^4 + 2YZ^4 - 119XYZ^2 - 71Y^2Z^2 \\
& +66XZ^3 + 36YZ^3 + 4Z^4 - 2328XYZ - 1332Y^2Z - 243XZ^2 \\
& -970YZ^2 - 91Z^3 - 2S^2 - 6724XY - 3868Y^2 - 6416XZ \\
& -11220YZ - 3529Z^2 - 16700X - 27184Y - 23940Z - 45258, \\
f_5 &= 12YZ^5 - 6Z^6 - 62Y^2Z^3 - 230XZ^4 + 58YZ^4 - 108Z^5 \\
& +3S^2XY + 3S^2Y^2 - 3S^2XZ + 3764XYZ^2 + 1478Y^2Z^2 \\
& -666XZ^3 + 1092YZ^3 - 646Z^4 - 9S^2X + 18S^2Y - 36S^2Z \\
& +4260XYZ + 1008Y^2Z + 11154XZ^2 + 16378YZ^2 + 2764Z^3 \\
& -199S^2 - 44975XY - 26879Y^2 + 8075XZ + 1848YZ + 31018Z^2 \\
& -110155X - 185234Y - 24240Z - 302949, \\
f_6 &= 54XZ^5 + 36YZ^5 - 4Y^2Z^3 - 334XZ^4 + 200YZ^4 - 90Z^5 \\
& -12449XYZ^2 - 8603Y^2Z^2 + 4017XZ^3 + 1566YZ^3 \\
& -1652Z^4 + 54S^2X + 18S^2Y - 36S^2Z - 292974XYZ \\
& -170586Y^2Z - 20547XZ^2 - 109366YZ^2 - 19072Z^3 \\
& -686S^2 - 966592XY - 558592Y^2 - 814634XZ - 1449168YZ \\
& -423595Z^2 - 2396822X - 3915922Y - 3150378Z - 6505170.
\end{aligned}$$

Stufe 191 Das Ideal zerfällt in fünf Primärideale. Vier davon sind Primideale. Als Modell erhalten wir:

$$\begin{aligned}
f_1 &= X^2 - Y^2 + XZ + 4X - 3Y + Z + 1, \\
f_2 &= Y^3 - XYZ - 3XY + 3Y^2 - 3XZ - YZ - Z^2 - 6X - Y - 5Z - 6, \\
f_3 &= XY^2 - Y^2Z + XZ^2 + XY - 2Y^2 + 5XZ - 4YZ + Z^2 + 6X \\
& -8Y + 2Z, \\
f_4 &= 4XYZ^4 + 11Y^2Z^4 - 10XZ^5 + 7XYZ^3 - 61Y^2Z^3 + 83XZ^4
\end{aligned}$$

$$
\begin{aligned}
& +53YZ^4+6Z^5-1913XYZ^2-3017Y^2Z^2+1940XZ^3\\
& -627YZ^3-81Z^4-11068XYZ-14034Y^2Z+6584XZ^2\\
& -14385YZ^2-1705Z^3-S^2-15310XY-17246Y^2+4185XZ\\
& -58482YZ-12789Z^2-4358X-67055Y-38615Z-38864,\\
f_5 \;=\; & 4Z^7+1831Y^2Z^4-2114XZ^5-248YZ^5+24Z^6+12619XYZ^3\\
& +6515Y^2Z^3+5011XZ^4+11513YZ^4+2458Z^5-4S^2XY\\
& +16S^2Y^2-16S^2XZ-377601XYZ^2-628637Y^2Z^2\\
& +425388XZ^3-48327YZ^3-9045Z^4+44S^2X-16S^2Y\\
& -24S^2Z-2713476XYZ-3474546Y^2Z+1673120XZ^2\\
& -3093629YZ^2-329581Z^3-413S^2-4086862XY\\
& -4604534Y^2+1180733XZ-14556614YZ-2914021Z^2\\
& -1163734X-17903467Y-9703895Z-10378808,\\
f_6 \;=\; & 2YZ^6-981Y^2Z^4+1228XZ^5+168YZ^5+48Z^6-9097XYZ^3\\
& -8255Y^2Z^3+1763XZ^4-6319YZ^4-928Z^5-2S^2Y^2+2S^2XZ\\
& +143123XYZ^2+246693Y^2Z^2-171636XZ^3-4975YZ^3+1527Z^4\\
& -2S^2X-12S^2Y+10S^2Z+1139810XYZ+1463246Y^2Z\\
& -712382XZ^2+1231295YZ^2+119689Z^3+165S^2+1750438XY\\
& +1971944Y^2-513457XZ+6137652YZ+1185973Z^2+498234X\\
& +7667509Y+4098627Z+4444600,\\
f_7 \;=\; & 4XZ^6+153Y^2Z^4-214XZ^5-36YZ^5-28Z^6+1209XYZ^3\\
& +1013Y^2Z^3-491XZ^4+859YZ^4-86Z^5-13355XYZ^2\\
& -23287Y^2Z^2+15912XZ^3+1415YZ^3-435Z^4-20S^2X\\
& +16S^2Y-4S^2Z-100796XYZ-128586Y^2Z+62564XZ^2\\
& -114367YZ^2-10575Z^3-7S^2-144574XY-162730Y^2\\
& +41587XZ-536750YZ-106491Z^2-40970X-632785Y\\
& -354597Z-366472,\\
f_8 \;=\; & 20Y^2Z^5-24XZ^6-1363Y^2Z^4+1734XZ^5+316YZ^5+88Z^6\\
& -13999XYZ^3-13403Y^2Z^3+3681XZ^4-9069YZ^4-1194Z^5\\
& +187725XYZ^2+326837Y^2Z^2-229732XZ^3-17005YZ^3+1065Z^4\\
& -16S^2Y+4S^2Z+1536116XYZ+1972466Y^2Z-963004XZ^2\\
& +1637117YZ^2+153585Z^3+197S^2+2363494XY+2662470Y^2\\
& -694757XZ+8274310YZ+1584741Z^2+672670X+10352395Y\\
& +5525587Z+6000592.
\end{aligned}
$$

Für folgende Modelle der Klasse drei haben die Kurven $X_0^+(l)$ einen Weierstraß-Punkt in ∞^+. Deshalb ist das Standardmodell von einer 'einfachereren' Gestalt, was die Berechnung dieser Modelle ermöglicht.

Stufe 109 Das Ideal zerfällt in vier Primärideale. Drei davon sind Primideale und modulo 109 reduzibel. Das Radikal des vierten Primärideals ist modulo 109 irreduzibel. Als Modell erhalten wir:

$$
\begin{aligned}
f_1 \;=\; & 3S^2-8WX+29X^2-3WY+5XY-Y^2-42W+227X\\
& +16Y+462,\\
f_2 \;=\; & WXY+38X^2Y+8XY^2-Y^3+3W^2-124WX-620X^2
\end{aligned}
$$

$$
\begin{aligned}
& -27WY - 282XY - 94Y^2 - 597W - 6374X - 2347Y - 16302, \\
f_3 &= 288X^3 - WXY - 38X^2Y - 8XY^2 + Y^3 - 3W^2 + 220WX \\
& +1388X^2 + 27WY - 390XY - 2Y^2 + 885W - 2362X - 1013Y \\
& -13650, \\
f_4 &= 6WX^2 - 96X^3 + WXY + 32X^2Y + 2XY^2 - Y^3 + 3W^2 \\
& -70WX - 374X^2 - 9WY + 174XY - 22Y^2 - 381W + 1204X \\
& +137Y + 4758, \\
f_5 &= 9X^2Y^2 + 3W^2X + 1461X^2Y - 3WY^2 + 264XY^2 - 48Y^3 \\
& +162W^2 - 5309WX - 27826X^2 - 1176WY - 13852XY \\
& -4240Y^2 - 25170W - 282874X - 103676Y - 715884, \\
f_6 &= 27XY^4 + 9W^3X - 9W^2Y^2 - 225WY^3 - 927XY^3 + 441Y^4 \\
& +513W^3 - 10362W^2X - 5688W^2Y + 4544754X^2Y - 19419WY^2 \\
& +765195XY^2 - 123720Y^3 + 390123W^2 - 16008889WX \\
& -77298596X^2 - 3561438WY - 37552091XY - 11996141Y^2 \\
& -75653112W - 794909216X - 295677412Y - 2028873288, \\
f_7 &= 3Y^6 + W^4X - W^3Y^2 - 34W^2Y^3 - 134WY^4 + 239Y^5 \\
& +33W^4 - 1048W^3X + 118W^3Y - 3830W^2Y^2 - 25516WY^3 \\
& +145072XY^3 + 12702Y^4 + 29409W^3 - 1295921W^2X \\
& -403083W^2Y + 313341012X^2Y - 2190551WY^2 + 51206194XY^2 \\
& -10800474Y^3 + 22353237W^2 - 1117356014WX - 5212031608X^2 \\
& -267819726WY - 2623350952XY - 885079175Y^2 - 5318890773W \\
& -53995399234X - 20716173641Y - 138716150118.
\end{aligned}
$$

Stufe 151: Das Ideal zerfällt in vier Primärideale. Drei davon sind Primideale. Alle drei und das Radikal des vierten Primärideals sind modulo 151 reduzibel. Als Modell erhalten wir:

$$
\begin{aligned}
f_1 &= WXY + 6X^2Y + XY^2 - Y^3 + W^2 + 7WX + 22X^2 - WY + 8XY \\
& -18Y^2 + 3W + 17X - 110Y - 210, \\
f_2 &= X^3 + WX + 5X^2 - 3XY - Y^2 + 2W - 3X - 13Y - 30, \\
f_3 &= WX^2 + 5X^3 + WXY + 6X^2Y - Y^3 + W^2 + 11WX + 44X^2 \\
& -19Y^2 + 11W + 33X - 118Y - 210, \\
f_4 &= 5Y^4 + W^3 - S^2X + 49W^2X - 7W^2Y + 483X^2Y - 53WY^2 \\
& +76XY^2 - 121Y^3 + 3S^2 + 254W^2 + 1330WX + 2234X^2 \\
& -1090WY - 3864XY - 4140Y^2 - 673W - 13760X - 34316Y \\
& -76149, \\
f_5 &= XY^3 - W^2X - 93X^2Y + WY^2 - 31XY^2 + 4Y^3 - S^2 - 14W^2 \\
& -12WX - 318X^2 + 36WY - 437XY + 36Y^2 + 92W - 1085X \\
& +87Y + 63, \\
f_6 &= X^2Y^2 + W^2X + 17X^2Y - WY^2 + 6XY^2 - 4Y^3 + 6W^2 + 30WX \\
& +60X^2 - 23WY - 58XY - 93Y^2 - 12W - 259X - 743Y - 1650, \\
f_7 &= W^3Y - S^2XY - 2W^2Y^2 - 4WY^3 + 5S^2W + 8W^3 + 13S^2X \\
& -11W^2X + 3S^2Y - 17W^2Y + 1668X^2Y - 58WY^2 + 602XY^2 \\
& +13Y^3 + 62S^2 + 76W^2 - 838WX + 5098X^2 - 294WY \\
& +11797XY + 1810Y^2 - 2051W + 32562X + 21234Y + 52644,
\end{aligned}
$$

$$
\begin{aligned}
f_8 &= S^2X^2 - W^2Y^2 + 2WY^3 - W^3 + S^2X - 16W^2X - 4S^2Y - 7W^2Y \\
&\quad -864X^2Y + 50WY^2 - 292XY^2 + 69Y^3 - 31S^2 - 172W^2 \\
&\quad -228WX - 2955X^2 + 605WY - 3172XY + 1071Y^2 + 1169W \\
&\quad -7235X + 5889Y + 10863, \\
f_9 &= 5W^3X - 5W^2Y^2 - 25WY^3 + 27W^3 - 2S^2X + 58W^2X + 5S^2Y \\
&\quad -84W^2Y + 12996X^2Y - 521WY^2 + 4867XY^2 - 192Y^3 + 151S^2 \\
&\quad +1088W^2 - 2815WX + 42498X^2 - 4720WY + 78317XY \\
&\quad +4970Y^2 - 16631W + 208840X + 81808Y + 215817, \\
f_{10} &= 5W^4 - 30S^2WX - 35S^2XY + 25S^2Y^2 - 190W^2Y^2 + 130WY^3 \\
&\quad +90S^2W + 46W^3 + 159S^2X - 2331W^2X - 190S^2Y - 1517W^2Y \\
&\quad -33907X^2Y + 3967WY^2 - 10064XY^2 + 8669Y^3 - 1562S^2 \\
&\quad -17581W^2 - 61480WX - 139456X^2 + 60280WY + 107856XY \\
&\quad +200505Y^2 + 53382W + 483010X + 1566069Y + 3444096.
\end{aligned}
$$

Stufe 179: Das Ideal zerfällt in vier Primärideale. Drei davon sind Primideale. Zwei der Primideale sind modulo 179 reduzibel. Das Dritte und das Radikal des vierten Primärideals sind modulo 179 nicht reduzibel. Als Modell erhalten wir:

$$
\begin{aligned}
f_1 &= WXY + 4X^2Y + XY^2 - Y^3 + W^2 + WX - 3X^2 - WY + 5XY \\
&\quad -9Y^2 - 3W - 26X - 31Y - 55, \\
f_2 &= X^3 + WX + 3X^2 - 3XY - Y^2 + 2W - 4X - 9Y - 14, \\
f_3 &= WX^2 + 3X^3 + WXY + 4X^2Y - Y^3 + W^2 + 5WX + 13X^2 \\
&\quad +2XY - 10Y^2 + 3W - X - 34Y - 43, \\
f_4 &= WY^3 - 4XY^3 + 2Y^4 - W^3 + 19W^2X - 2W^2Y - 27X^2Y \\
&\quad -3WY^2 - 30XY^2 - 30Y^3 - S^2 + 68W^2 + 174WX - 888X^2 \\
&\quad -153WY - 1289XY - 650Y^2 + 105W - 4957X - 4014Y - 7340, \\
f_5 &= X^2Y^2 + W^2X + 10X^2Y - WY^2 + 4XY^2 - 4Y^3 + 6W^2 + 5WX \\
&\quad -42X^2 - 15WY - 37XY - 47Y^2 - 12W - 260X - 235Y - 426, \\
f_6 &= W^4 - 4W^3X - S^2X^2 + 2W^2Y^2 + 26XY^3 + 9Y^4 + 2W^3 \\
&\quad +37W^2X + 4S^2Y - 4W^2Y - 1393X^2Y - 79WY^2 - 652XY^2 \\
&\quad -124Y^3 + 6S^2 + 65W^2 + 1269WX - 5549X^2 - 490WY \\
&\quad -11715XY - 3812Y^2 + 1906W - 28883X - 23974Y - 39363, \\
f_7 &= Y^5 - 2W^3X - 21XY^3 - 23Y^4 - 8W^3 - S^2X - 74W^2X \\
&\quad +52W^2Y - 880X^2Y + 34WY^2 - 548XY^2 - 127Y^3 + 4S^2 \\
&\quad -293W^2 - 106WX + 1569X^2 + 827WY - 745XY + 705Y^2 \\
&\quad +1023W + 10269X + 7365Y + 17735, \\
f_8 &= XY^4 + Y^5 - W^3X - W^2Y^2 - 40XY^3 - 12Y^4 - 7W^3 - S^2X \\
&\quad +45W^2X + 24W^2Y - 686X^2Y - 54WY^2 - 726XY^2 - 420Y^3 \\
&\quad -S^2 + 199W^2 + 691WX - 3525X^2 - 457WY - 7683XY \\
&\quad -4005Y^2 + 744W - 19202X - 18087Y - 27541, \\
f_9 &= W^3Y^2 + S^2WX + 16W^3X + 4S^2X^2 + 12W^3Y - S^2Y^2 \\
&\quad -3W^2Y^2 - 196XY^3 - 24Y^4 + 6S^2W + 42W^3 + 24S^2X \\
&\quad +392W^2X - 13S^2Y + 9W^2Y + 2435X^2Y - 136WY^2 \\
&\quad +101XY^2 - 1045Y^3 - 16S^2 + 1524W^2 + 636WX - 7132X^2 \\
&\quad -3029WY - 4059XY - 9022Y^2 - 3274W - 45264X
\end{aligned}
$$

$$-40389Y - 75936.$$

3.3.3 Einige Modelle von $X_0^+(N)$

Wendet man das im letzten Paragraphen beschriebene Verfahren auf die Relationen der Standardmodelle an, bei denen man die Relation $s^2 = f(x)$ wegläßt, dann erhält man Modelle für Kurven, die im allgemeinen mit $X_0^+(N)$ bezeichnet werden. Wir halten hier folgende Modelle fest:
Für $X_0^+(67)$:

$$\begin{aligned}
f_1 &= 4X^2 - XY - Y^2 + XZ + 27X - 25Y + 4Z - 66 \\
f_2 &= 4Y^3 - 3XYZ + Y^2Z - XZ^2 - 126XY + 66Y^2 - 129XZ - 15YZ - 24Z^2 \\
&\quad -1830X - 634Y - 866Z - 11820 \\
f_3 &= 6XY^2 + 2Y^3 - 3XYZ - Y^2Z + XZ^2 - 90XY + 6Y^2 - 33XZ - 57YZ \\
&\quad -1560X - 1496Y - 526Z - 13920
\end{aligned}$$

Für $X_0^+(103)$:

$$\begin{aligned}
f_1 &= 85X^2 - 12XY + Y^2 - XZ - 382X + 67Y - 5Z - 33 \\
f_2 &= 85Y^3 - 229XYZ + 12Y^2Z - 12XZ^2 + 7337451XY - 639313Y^2 \\
&\quad -1290011XZ + 147259YZ - 5075Z^2 - 143153359X + 24411739Y \\
&\quad -1788826Z - 11482491 \\
f_3 &= 85XY^2 - 12XYZ + Y^2Z - XZ^2 + 394513XY - 86674Y^2 - 55913XZ \\
&\quad +19532YZ - 1025Z^2 - 2638302X + 630657Y - 55498Z - 338223
\end{aligned}$$

Für $X_0^+(109)$:

$$\begin{aligned}
f_1 &= 90XY^2 + 3Y^3 - 114X^2W - 3XYW - 7678X^2 - 3562XY \\
&\quad -478Y^2 - 1262XW - 261YW - 9W^2 - 69532X - 18875Y - 4137W \\
&\quad -161538 \\
f_2 &= 56X^2Y + 26XY^2 - Y^3 - 18X^2W + XYW - 2126X^2 - 978XY - 214Y^2 \\
&\quad -382XW - 81YW + 3W^2 - 20372X - 6439Y - 1533W - 49530 \\
f_3 &= 3X^3 + 8X^2 - 7XY - Y^2 + XW - 91X - 35Y + 3W - 312 \\
f_4 &= 90Y^4 - 21Y^3W + 78X^2W^2 + 21XYW^2 + 1164Y^3 - 24986X^2W \\
&\quad -13970XYW - 2084Y^2W - 586XW^2 - 603YW^2 + 63W^3 - 2514484X^2 \\
&\quad -1499956XY - 228754Y^2 - 454852XW - 102133YW + 4407W^2 \\
&\quad -23366716X - 7229900Y - 1604250W - 54842424
\end{aligned}$$

Für $X_0^+(167)$:

$$\begin{aligned}
f_1 &= 2X^2 - XY - Y^2 + XZ + 3X - 6Y - 5 \\
f_2 &= 2Y^3 - XYZ + Y^2Z - XZ^2 - 8XY + 8Y^2 - 11XZ - 2YZ - 6Z^2 \\
&\quad -24X - 2Y - 29Z - 32 \\
f_3 &= 7XY^2 + 3Y^3 - 5XYZ - 2Y^2Z + 2XZ^2 - 12XY + 5Y^2 - 13XZ \\
&\quad -24YZ - 2Z^2 - 71X - 87Y - 68Z - 209
\end{aligned}$$

Für $X_0^+(151)$:

$$\begin{aligned}
f_1 &= = XY^2 - X^2W + 3X^2 - 7XY - 4Y^2 + XW - YW - 31X - 57Y \\
&\quad +2W - 150
\end{aligned}$$

$$\begin{aligned}
f_2 &= 6X^2Y + 3XY^2 - Y^3 - 2X^2W + XYW + 28X^2 - 6XY - 26Y^2 + 9XW \\
&\quad -3YW + W^2 - 45X - 224Y + 7W - 510 \\
f_3 &= X^3 + 5X^2 - 3XY - Y^2 + XW - 3X - 13Y + 2W - 30 \\
f_4 &= 6Y^4 - Y^3W - 5X^2W^2 + XYW^2 + 23Y^3 + 80X^2W - 146XYW - 74Y^2W \\
&\quad +48XW^2 - 12YW^2 + W^3 + 205X^2 - 2739XY - 1364Y^2 + 318XW \\
&\quad -1103YW + 146W^2 - 9402X - 14807Y - 1727W - 35520
\end{aligned}$$

Für $X_0^+(179)$:

$$\begin{aligned}
f_1 &= = XY^2 - X^2W - 7X^2 - 6XY - 2Y^2 - XW - YW - 37X - 24Y - 54 \\
f_2 &= 4X^2Y + 3XY^2 - Y^3 - 2X^2W + XYW - 17X^2 - 7XY - 13Y^2 - XW \\
&\quad -3YW + W2 - 100X - 79Y - 3W - 163 \\
f_3 &= X^3 + 3X^2 - 3XY - Y^2 + XW - 4X - 9Y + 2W - 14 \\
f_4 &= 4Y^4 - Y^3W - 3X^2W^2 + XYW^2 - 40X^2W - 57XYW - 31Y^2W \\
&\quad +14XW^2 - 8YW^2 + W^3 - 676X^2 - 912XY - 432Y^2 - 109XW \\
&\quad -311YW + 57W^2 - 3816X - 3024Y - 301W - 5700
\end{aligned}$$

Für $X_0^+(191)$:

$$\begin{aligned}
f_1 &= X^2 - Y^2 + XZ + 4X - 3Y + Z + 1 \\
f_2 &= Y^3 - XYZ - 3XY + 3Y^2 - 3XZ - YZ - Z^2 - 6X - Y - 5Z - 6 \\
f_3 &= 7XY^2 - 6Y^3 + 6XYZ - 7Y^2Z + 7XZ^2 + 25XY - 32Y^2 + 53XZ \\
&\quad -22YZ + 13Z^2 + 78X - 50Y + 44Z + 36
\end{aligned}$$

3.4 Reduzibilität der neu gewonnen Modelle über Körpern mit Primzahlcharakteristik

Reduzieren wir die oben angegebenen Modelle für $X_0(N)$ nun modulo einer Primzahl p, und berechnen wiederum eine Primärzerlegung, so erhalten wir die in Tabelle 3.4 zusammengefassten Aussagen über die Reduzibilität dieser Modelle.
Dabei bedeutet:

I: Das Modell im angegebenen Fall ist irreduzibel,

R: Das Modell im angegebenen Fall ist reduzibel,

?: Eine Rechnung ist nicht durchgeführt worden,

(W): Bei so gekennzeichneten Kurven von Stufe N hat die Kurve $X_0^+(l)$ im Unendlichen einen Weierstraß-Punkt.

Die Kurve der Stufe 67 ist hier zweimal aufgelistet. Die erste Zeile von Tabelle 3.4 enthält dabei die Information über das Modell, das man durch Reduktion des Ideals Q_4 aus Beispiel 3.2 bestimmt. In der zweiten Zeile befinden sich Aussagen, bei denen die folgende Darstellung des Modells verwendet wurde:

$$\begin{aligned}
f_1 &= 4X^2 - XY - Y^2 + XZ + 27X - 25Y + 4Z - 66, \\
f_2 &= 4S^2 - XY + 3Y^2 - 7XZ + 115X + 95Y - 12Z + 1278, \\
f_3 &= 4Y^3 - 3XYZ + Y^2Z - XZ^2 - 126XY + 66Y^2 - 129XZ \\
&\quad -15YZ - 24Z^2 - 1830X - 634Y - 866Z - 11820, \\
f_4 &= XY^2 + Y^3 - XYZ - 36XY + 12Y^2 - 27XZ - 12YZ - 4Z^2 \\
&\quad -565X - 355Y - 232Z - 4290.
\end{aligned}$$

Klasse	Stufe	Geschlecht	Primzahl				
			3	5	7	31	1021
2	67	5	R	I	I	I	I
	67(2)	5	I	I	I	I	I
	73	5	R	R	I	I	I
	103	8	R	?	?	?	?
	107	9	?	?	?	?	?
	167	14	I	I	I	I	I
	191	16	?	?	?	?	?
3	109(W)	8	R	I	I	I	I
	151(W)	12	I	I	I	I	I
	179(W)	15	I	I	I	I	I

Tabelle 3.3: Reduzibilität der neu gewonnenen Modelle über den endlichen Körpern $\mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{31}$, und $\mathbb{F}_{1021}$

Es fällt auf, dass die Ideale, die man durch Reduktion gewinnt, je nach Darstellung des Ausgangsmodells reduzibel beziehungsweise irreduzibel über $\mathbb{F}_3$ sind. Die Erklärung hierfür findet sich in Abschnitt 3.2.1. Die abstrakten Modulkurven haben gute Reduktion. Hier haben wir aber nur affine, singuläre Modelle dieser Kurve. Von den Kurven, die man durch Reduktion der Modelle erhält, die hier vorliegen, wissen wir also nicht, ob sie isomorph zu Reduktionen der abstrakten Modulkurven sind. Um ein dazu isomorphes Modell zu erhalten, müsste man den projektiven Abschluss der Modelle konstruieren und diesen dann desingularisieren. Wie wir schon an der Reduktion der Modelle modulo zwei gesehen haben sind die in Abschnitt 3.1.5 beschriebenen Morphismen p_l für die Reduzibilität der Modelle modulo zwei verantwortlich. Wir können nicht davon ausgehen, dass diese nicht für weitere Primzahlen eine 'schlechte' Reduktion der Modelle verursachen, so dass wir zusätzlich zu den projektiven, glatten Modellen auch noch die Morphismen p_l konstruieren und untersuchen müssen, um sicher zu stellen, dass die konstruierten Kurven Modelle von Reduktionen der Modulkurven sind.

3.5 Absolute Irreduzibilität

Bisher wurde nur die Irreduzibilität der Modelle über Körpern mit p Elementen untersucht (p Primzahl). Um die absolute Irreduzibilität der Modelle zu zeigen, müssen wir noch die Irreduzibilität der Modelle über dem algebraischen Abschluss der uns interessierenden Körper untersuchen. Von den Modulpolynomen wissen wir, dass sie modulo aller Primzahlen, bis auf diejenigen die die Stufe teilen, gute Reduktion haben, das heißt, sie liefern bei Reduktion der Koeffizienten modulo Primzahl eine absolut irreduzible Kurve über $\overline{\mathbb{F}_p}$. Von den Standardmodellen wissen wir dies nicht. Für die Kurven der Klasse null können wir noch einige Aussagen machen.

3.5.1 Hyperelliptischer Fall

Wir haben folgende Charakterisierung von absolut irreduziblen Kurven über endlichen Körpern der Form $S^d - f(X)$ in $k[S, X]$.

Proposition 3.2
Für ein Polynom der Form $S^d - f(X)$ mit Koeffizienten im endlichen Körper k sind äquivalent:

(i) $S^d - f(X)$ ist absolut irreduzibel

	Primzahl				
Stufe	3	5	7	31	1021
11	1,1	1,1	1,1,1	1,1	1,1,1,1
17	1	1,1	1	1	1,1
19	1,1,1	1,1	1,1	1,1,1	1,1,1
23	1,1	1,1,1,1	1,1,1,1	1,1	1,1
29	1	1,1	1,1,1,1	1	1,1
31	1,1,1,1	1,1	1,1	2,2,2	1,1,1,1
41	1	1,1	1	1,1,1,1,1	1,1
47	1,1	1,1,1,1,1,1	1,1	1,1,1,1,1,1	1,1
59	1,1	1,1	1,1	1,1,1,1,1,1,1	1,1,1,1,1,1,1
71	1,1	1,1	1,1,1,1,1,1,1,1	1,1,1,1,1,1,1,1	1,1

Tabelle 3.4: Folgen von Exponenten irreduzibler Faktoren der Polynome $f(X)$ von hyperelliptischen Standardmodellen über einigen endlichen Körpern

(ii) Wenn $f(X) = a(X - x_1)^{d_1} \dots (X - x_r)^{d_r}$ eine Zerlegung von f über $\overline{k}$ mit $x_i \neq x_j$ falls $i \neq j$, dann ist der größte gemeinsame Teiler von $\{d, d_1 \dots, d_r\}$ gleich eins.

Beweis:
siehe [Sc, Paragraph 2, Lemma 2C].

□

Betrachten wir nun die Standardmodelle der Klasse null. Dies sind genau die Modelle für hyperelliptische Kurven im $\mathbb{A}^2$, die durch ein Polynom der Form $S^2 - f(X)$ in k[S,X] gegeben sind. Wir interessieren uns hier für die Fälle $k = \mathbb{F}_3$, $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{31}$ und $\mathbb{F}_{1021}$. Wie die Polynome $f(X)$ in $\mathbb{F}_p[X]$ zerfallen, ist in der Tabelle 3.4 beschrieben. Als Einträge hat man eine Folge von Exponenten der verschiedenen Faktoren von f(X) in $\mathbb{F}_p[X]$. Falls also $f(X)$ in das Produkt $g_1(X)^{e_1} \dots g_r(x)^{e_r}$ unterschiedlicher Faktoren zerfällt, so erhält man an entsprechender Stelle einen Eintrag $e_1, \dots, e_r$. Man sieht sofort, dass alle Polynome in verschiedene irreduzible Faktoren zerfallen, mit Ausnahme des Polynoms des Standardmodells der Stufe 31 über dem Körper $\mathbb{F}_{31}$. Da die betrachteten Körper separabel sind, zerfallen die Polynome $f(X)$ mit obiger Ausnahme alle über $\overline{\mathbb{F}_p}$ für $p \in \{3, 5, 7, 31, 1021\}$ in unterschiedliche Linearfaktoren. Nach obiger Proposition sind die Modelle also in diesen Fällen absolut irreduzibel.

3.5.2 Projektiver Abschluss und Berechnung von rationalen Punkten

Haben wir eine affine, absolut irreduzible Varietät, dann ist auch deren projektiver Abschluss nach Proposition 1.1 absolut irreduzibel. Speziell im hyperelliptischen Fall der Standardmodelle erhalten wir also je ein irreduzibles, homogenes Polynom in k[A,S,X] für die im letzten Abschnitt angegebenen Fälle. Mit A wollen wir die Variable bezeichnen mit der wir homogenisieren. Um einen projektiven Abschluss der Modelle höherer Klassen zu erhalten, müssen wir eine Gröbner Basis der durch das Modell gegebenen Ideale berechnen. Falls wir ein affines Modell in Dreiecksform haben, können wir nicht mehr davon ausgehen, dass das projektive Modell auch in Dreiecksform vorliegt.

Ein Standardmodell der Stufe N hat, wie wir bereits in Abschnitt 4.1 gesehen haben, höchstens $N + 1$ Polynome. Ist das Modell durch weniger Polynome gegeben, so ersetze im Folgenden $N + 1$ durch die Anzahl der Polynome. Betrachten wir die im $\mathbb{A}^{N+2}$ gegebene Dreiecksform des Standardmodells. Das Finden der Punkte auf der algebraischen Menge durch Auswertung aller $p^{e(N+2)}$ Punkte des umgebenden Raumes $\mathbb{A}^{N+2} = (\mathbb{F}_{p^e})^{N+2}$ in allen $N+1$ Polynomen würde $(N+1)p^{e(N+2)}$ Auswertungen von Polynomen beanspruchen. Nutzt man nun die Dreiecksform zur Bestimmung der $\mathbb{F}_{p^e}$-rationalen Punkte, so sind zunächst p^{2e} Auswertungen des Polynoms P_2 in zwei Variablen nötig. Wertet man das Polynom P_3 in drei Variablen nur noch in den Nullstellen von P_2 aus, so sind hierzu höchstens $r_2(p^e+1) + \sum_{i=1}^{r_2} g_{2,i}[2\sqrt{p^e}]$ Auswertungen von P_3 nötig. Dabei ist r_2 die Anzahl von Faktoren, in die P_2 über $\overline{\mathbb{F}_p}$ zerfällt, und $g_{2,i}$ ist das Geschlecht der ebenen Kurven, die von diesen Faktoren definiert werden. Siehe hierzu auch die Ausführungen nach Bemerkung 4.2 (Hasse-Weil-Serre-Schranke). Das Polynom P_4 muss entsprechend in höchstens $r_3(p^e+1) + \sum_{i=1}^{r_3} g_{3,i}[2\sqrt{p^e}]$ Punkten ausgewertet werden. Nun ist r_3 die Anzahl der Assoziierten der Primärideale in einer reduzierten Primärzerlegung des Ideals (P_2, P_3) und $g_{3,i}$ das entsprechende Geschlecht der Kurven, die durch diese Ideale definiert werden. Fährt man so bis zum Polynom P_{N+1} fort, muss man insgesamt maximal $p^{2e} + c_1(p^e + 1 + c_2[2\sqrt{p^2}]$ Polynome auswerten, wobei $c_1 = \sum_{i=2}^{N} r_i$ und $c_2 = \sum_{j=2}^{N} \sum_{i=1}^{r_i} g_{j,i}$. Anschließend müssen die gefundenen Punkte noch einmal in die die Modulkurve definierenden Polynome eingesetzt werden, um sicher zu stellen, dass es auch wirklich Punkte der Kurve sind, die durch das Standardmodell definiert wird. Dies erhöht die Abschätzung der Anzahl der Auswertungen von Polynomen nocheinmal um den Faktor c. Hier ist c die Anzahl der Polynome der Gröbner Basis (man setze hierbei $A = 1$).

Bemerkung 3.9

Weder das Auswerten eines Polynoms kann als exakte Laufzeitangabe aufgefasst werden, noch können die Konstanten c_1 und c_2 in einfacher Weise bestimmt werden, so dass man obige Argumentation nicht als quantitative Abschätzung auffassen kann. In der Praxis liefert der oben beschriebene Algorithmus aber dennoch eine deutliche Laufzeitersparnis.

□

Um die Punkte im Unendlichen zu bestimmen, setzen wir in allen Erzeugern der Gröbner Basis A gleich null. Aus dem resultierenden Ideal können wir eine Teilmenge auswählen, die einer Dreiecksform möglichst nahe kommt. Haben wir eine gemeinsame Nullstelle dieser Polynome gefunden, so müssen wir anschließend noch nachprüfen, ob sie auch Nullstelle aller Polynome der Gröbner Basis ist.

Kapitel 4

Beispiele für Codes

Um zwischen affinen und projektiven Punkten einer Kurve zu unterscheiden bezeichne im Folgenden $(a_1, \ldots, a_n)$ einen Punkt auf einer affinen und $(a_0 : \ldots : a_n)$ einen Punkt auf einer projektiven Kurve.

Beispiel 4.1

Wir betrachten die elliptische Kurve $X_0(11)$ über $\overline{\mathbb{F}_3}$. Das Standardmodell $C_P(11)$ für den affinen Teil $Y_0(11)$ in $\mathbb{F}_3[S,X]$ ist durch das Polynom $f = -S^2 + X^4 + X^3 - X^2 + X$ gegeben. Wir wissen bereits, dass f eine absolut irreduzible, glatte, ebene Kurve in $\mathbb{A}(\overline{\mathbb{F}_3})$ darstellt. Die durch $f^h = -S^2A^2 + X^4 + X^3A - X^2A^2 + XA^3$ in $\mathbb{F}_3[A,S,X]$ definierte, homogene Kurve hat im Unendlichen aber einen singulären Punkt $P_\infty = (0:1:0)$ mit der Ordnung zwei. Es gibt keine weiteren singulären Punkte, wie man sich leicht an Hand der Jacobischen von f^h klar machen kann. Die anderen (regulären) Punkte über $\mathbb{F}_3$ sind $P_1 = (1:0:0)$, $P_2 = (1:1:-1)$ und $P_3 = (1:-1:-1)$. Wir wollen nun den singulären Punkt im Unendlichen genauer untersuchen. Deshalb beschaffen wir uns ein glattes Modell der Kurve im Unendlichen. Dazu betrachten wir den affinen Teil von $\mathbb{P}(\overline{\mathbb{F}_3})$ der durch $S = 1$ gegeben ist. Hier ist unser Modell nun durch das Polynom $-A^2 + X^4 + X^3A - X^2A^2 + XA^3$ in $\overline{\mathbb{F}_3}[A,X]$ gegeben. Der Punkt P_∞ liegt nun im Ursprung. Der Punkt P_1 ist ins Unendliche gerückt. Wir machen nun ein Blowing-up (im Ursprung) und folgen hierbei [Ha, Chapter I, 4, p.28ff]. Dazu betrachten wir das Produkt $\mathbb{A}^2 \times \mathbb{P}^1$. Seien A, X die affinen Koordinaten und R, T die projektiven Koordinaten. Dieser Raum kann durch zwei affine Räume überdeckt werden, wovon wir einen für $T = 1$, den anderen für $R = 1$ erhalten. Wir machen die Transformation $XR = TA$ und projizieren dabei X auf X und A auf RX. Als direkte Transformierte im affinen Teilraum für $T = 1$ erhalten wir $R^2 - X^2 - X^2R + X^2R^2 - X^2R^3$. Diese hat nun über $\mathbb{F}_3$ in den Koordinaten (R,X) die Punkte $P'_\infty = (0,0)$, $P'_2 = (-1,-1)$ und $P'_3 = (-1,1)$. Nur der Punkt P'_∞ liegt auf der Ausnahmegeraden (auch über $\overline{\mathbb{F}_3}$). Er ist der Schnittpunkt der direkten Transformierten mit der Ausnahmegeraden. Die Punkte P'_i werden auf die Punkte P_i projiziert, entsprechen also der Transformation der P_i. Führen wir dasselbe für $R = 1$ durch und betrachten den anderen affinen Teil von $\mathbb{A}^2 \times \mathbb{P}^1$, so erhalten wir ebenfalls zwei Punkte, die der Transformation der Punkte P_2 und P_3 entsprechen. Hier erhält man aber keinen Schnittpunkt der Ausnahmegeraden mit der direkten Transformierten. Betrachten wir nun die Transformation des Punktes P_∞, so sehen wir, dass dieser nur in einen Punkt P'_∞ transformiert wurde, der auch singulär ist. Dies liegt darin begründet, dass der Ausgangspunkt P_∞ eine doppelte Tangente hat. Bei P'_∞ sehen wir nun aber, dass zwei unterschiedliche Tangenten $X + R$ und $X - R$ vorliegen. Mit einer weiteren Transformation des gleichen Typs erhalten wir also ein glattes Modell. Betrachten wir nun wieder das Produkt $\mathbb{A}^2 \times \mathbb{P}^1$ mit affinen Koordinaten R, X und projektiven Koordinaten V, W (XW = RV). Im affinen Teil $W = 1$ haben wir als Modell $f'' = -1 + V^2 + RV^2 - R^2V^2 + R^3V^2$. Nun erhalten wir in den Koordinaten (R, V) zwei Schnittpunkte $P_{1,\infty} = (0, 1)$ und $P_{2,\infty} = (0, -1)$ der Ausnahmegeraden $R = 0$ mit der direkten Transformierten. Die beiden Punkte P'_2 und P'_3 wurden dabei in die Punkte $P''_2 = (-1, 1)$ und $P''_3 = (-1, -1)$ transformiert. Im affinen Teil $V = 1$ würden wir ein ähnliches Bild erhalten. Um die beiden Punkte genauer zu untersuchen ist es günstiger, wenn diese jeweils im Ursprung liegen. Durch je eine Translation können wir dies erreichen oder aber wir wenden die Substitutionen $R = R$, $X = R(X - 1)$ und $R = R$, $X = R(X + 1)$ auf den Punkt P'_∞ an, so dass sich in jedem der beiden Fälle die Ausnahmekurve mit der direkten Transformierten im Ursprung der (R, V)-Ebene schneidet. Beide Vorgehensweisen liefern offenbar dasselbe Ergebnis. Das Beispiel ist in Abbildung 4.1 als Desingularisierungsbaum zusammengefasst. Mit r wird hier jeweils die Vielfachheit des betrachteten Punktes bezeichnet.

□

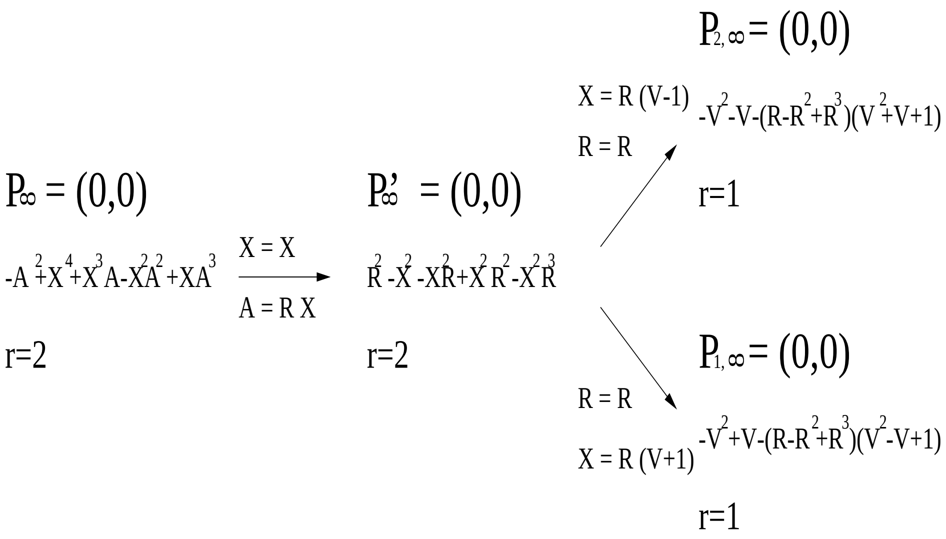

Abbildung 4.1: Desingularisierungsbaum der Kurve $C_P(11)/\mathbb{F}_3$ im Punkt P_∞.

4.1 Zeta-Funktionen und rationale Punkte auf Kurven über endlichen Körpern

In diesem Abschnitt folgen wir zunächst [LG, Part II, Chapter IV]. Für eine glatte, projektive Kurve X vom Geschlecht g über dem endlichen Körper $\mathbb{F}_q$ definieren wir ähnlich zur Riemannschen Zeta-Funktion für $s \in \mathbb{C}$ die Funktion

$$\zeta(X, s) := \prod_P (1 - q^{(-s)deg(P)})^{-1} = \sum_{D \geq 0} q^{deg(D)(-s)},$$

wobei das Produkt über alle abgeschlossenen Punkte und die Summe über alle nicht negativen Divisoren der Kurve X gebildet wird. Diese Funktion konvergiert für $Re(s) > 1$, und wir nennen sie die Zeta-Funktion von X über $\mathbb{F}_q$. Wir schreiben auch $Z(X, q^{-s})$ anstatt $\zeta(X, s)$. Wenn wir mit N_r die Anzahl der Punkte vom Grad eins über $\mathbb{F}_{q^r}$ bezeichnen, dann ist

$$log Z(X,t) = \sum_{r=1}^{\infty} N_r \frac{t^r}{r}.$$

Desweiteren erfüllt $Z(X,t)$ die Funktionalgleichung

$$Z(X,t) = q^{1-g} t^{2-2g} Z(X,t).$$

$Z(X,t)$ ist eine rationale Funktion in t und hat als Faktorisierung

$$Z(X,t) = \frac{P(t)}{(1-t)(1-qt)},$$

wobei $P(t)$ gleich $\prod_{i=1}^{g}(1-\alpha_i t)(1-\overline{\alpha_i} t)$ ist. Die α_i sind ganze algebraische Zahlen mit Absolutbetrag $|\alpha_i|$ gleich $\sqrt{q}$. Mit Hilfe dieser sehr starken Eigenschaften von $Z(X,t)$ erhalten wir für die Anzahl der Punkte $N_r(X) = N_r(X/\mathbb{F}_q)$ von X über $\mathbb{F}_q$ die Gleichung (Satz von Hasse und Weil):

$$N_r(X) = q^r + 1 - \sum_{i=1}^{g}(\alpha_i^r + \overline{\alpha_i}^r). \tag{4.1}$$

Stufe	Geschlecht	Punkteanzahlen in kleinen Körpern der Charakteristik:				
		3	5	7	31	1021
11	1	5	5	10	25	1000
17	1	4	5	6	42	1017
19	1	6	3	9	36	1062
23	2	4,12	8,34	6,66		
29	2	2,16	8,44	8,62		
31	2	6,10	4,44	12,60		
41	3	4,20,34	8,44,116	2,72,392		
47	4	4,20,40,84				
59	5	6,20,33,100,186				
71	6	4,20,40,100,264,764				

Tabelle 4.1: Anzahlen rationaler Punkte der hyperelliptischen Kurven $C_P(N)$ über einigen endlichen Körpern $\mathbb{F}_{p^r}$

Kennen wir also die Anzahl der Punkte in den Erweiterungen von $\mathbb{F}_q$ vom Grad kleiner oder gleich g, dann können wir die Anzahl der Punkte über allen Erweiterungen explizit angeben. Die Anzahl der Punkte über den Körpern $\mathbb{F}_{p^i}$, i klein, wurde für einige Kurven $C_P(N)$ berechnet. Die Ergebnisse für die hyperelliptischen Kurven sind in Tabelle 4.1 zusammengefasst. Sie sind der Reihe nach für $i = 1, \ldots, g$ aufgelistet und durch Kommata getrennt. Die dazu gehörenden Rechnungen finden sich in den Verzeichnissen '~/data/pun/' und '~/data/punhyp/'.

Bemerkung 4.1

In der Tabelle 4.2 sind einige weitere Anzahlen von Punkten für Kurven der Klasse eins aufgelistet. Hier wurden nur Anzahlen über den Körpern mit p Elementen berechnet; $p \in \{3,5,7,31\}$. Dabei stehen die Einträge 'Se' und 'Su', um anzugeben, ob die jeweilige Kurve im Affinen bzw im Unendlichen eine Singularität hat.

Stufe	Geschlecht	Punkteanzahlen in Körpern mit p Elementen											
		p=3			p=5			p=7			p=31		
37	2	5	Su		8	Su	Se	8	Su	Se	38	Su	Se
43	3	7		Se	5		Se	11		Se	40		Se
53	4	4	Su	Se	8	Su	Se	7	Su	Se	30	Su	Se
61	4	4	Su	Se	8	Su	Se	8	Su	Se	34	Su	Se
79	6	4	Su	Se	2	Su	Se	14	Su		38	Su	Se
83	7	3	Su		5	Su		7	Su		23	Su	
89	7	4	Su	Se	10	Su	Se	2	Su	Se	16	Su	Se
101	8	2	Su	Se	7	Su		8	Su		43	Su	
131	11	3	Su		3	Su		7	Su		27	Su	

Tabelle 4.2: Anzahlen rationaler Punkte der Kurven $C_P(N)$ der Klasse eins über einigen endlichen Körper $\mathbb{F}_p$

□

Beispiel 4.2

Die Kurve $C_P(11)$über dem Körper $\mathbb{F}_3$ hat Geschlecht eins. In Beispiel 4.1 haben wir gesehen, dass $C_P(11)$ über $\mathbb{F}_3$ fünf Punkte hat. Es ist also $N_1(C_P(11)) = 5 = 3+1-(\alpha_1+\overline{\alpha_1})$. Mit $\alpha_1\overline{\alpha_1} = 3$ erhalten wir $\alpha_1 = -\frac{1}{2} - \frac{\sqrt{-11}}{2}$ und $\overline{\alpha_1} = -\frac{1}{2} + \frac{\sqrt{-11}}{2}$. Für die Zeta-Funktion und die Anzahl der Punkte $N_r(C_P(11))$ gilt folglich:

$$Z(C_P(11)/\mathbb{F}_3, t) = \frac{1+t+3t^2}{(1-t)(1-3t)}$$
$$N_r(C_P(11)) = 3^r - 1 - \left(-\frac{1}{2} - \frac{\sqrt{-11}}{2}\right)^r - \left(-\frac{1}{2} + \frac{\sqrt{-11}}{2}\right)^r.$$

□

Die Zeta-Funktionen und die dazugehörigen algebraischen Zahlen $\alpha_i, \overline{\alpha_i}$ sind für einige hyperelliptische Kurven über den endlichen Körpern mit 3, 5, 7, 31 und 1021 in den Tabellen 4.3, 4.4, 4.5, 4.6 und 4.7 zusammengefasst. Die Rechnungen zur Bestimmung dieser finden sich in '~/dip/data/zeta/' . In Tabelle 4.1 sind die zur Berechnung notwendigen Anzahlen von Punkten aufgeführt.

Bemerkung 4.2

Eine andere Möglichkeit die Zeta-Funktionen für Modulkurven $X_0(N)$ über endlichen Körpern zu bestimmen besteht darin Fourierkoeffizienten von Spitzenformen vom Gewicht zwei zu berechnen die simultane Eigenformen bezüglich Hecke-Operatoren sind, das heißt man bestimmt die Eigenwerte von Hecke-Operatoren $e_1(p), \ldots, e_g(p)$ und nutzendann aus dass gilt:

$$P(t) = \prod_{i=1}^{g}(1 - e_i(p) + pt^2), \text{ falls } p \not| N.$$

Vergleiche hierzu zum Beispiel [LG, Part II, V, Theorem 5.4, p.79] oder [Mo, 5.6.6, p.198ff].

□

Als Folgerung des Satzes von Hasse und Weil erhält man für die maximale Anzahl $N_{q^r}(g)$ der Punkte einer projektiven glatten Kurve vom Geschlecht g über dem endlichen Körper $\mathbb{F}_{q^r}$ die Abschätzung:

Stufe	Zeta-Funktionen von Kurven C_P über $\mathbb{F}_3$ und deren Nullstellen in $\mathbb{C}$	
	$P(t)$	$\alpha_1, \overline{\alpha_1}, \ldots, \alpha_{2g}, \overline{\alpha_{2g}}$
11	$1 + t + 3t^2$	$\frac{1}{2}(-1 + \sqrt{-11}), \quad \frac{1}{2}(-1 - \sqrt{-11})$
17	$1 + 3t^2$	$\sqrt{-3}, \quad -\sqrt{-3}$
19	$1 + 2t + 3t^2$	$-1 + \sqrt{-2}, \quad -1 - \sqrt{-2}$
23	$1 + t^2 + 9t^4$	$1/2\sqrt{-2 + 2\sqrt{-35}}, \quad -1/2\sqrt{-2 + 2\sqrt{-35}},$ $1/2\sqrt{-2 - 2\sqrt{-35}}, \quad -1/2\sqrt{-2 - 2\sqrt{-35}}$
29	$1 - 2t + 5t^2 - 6t^3 + 9t^4$	$1/2(1 + \sqrt{2} + \sqrt{-9 + 2\sqrt{2}}),$ $1/2(1 + \sqrt{2} - \sqrt{-9 + 2\sqrt{2}}),$ $1/2(1 - \sqrt{2} + \sqrt{-9 - 2\sqrt{2}}),$ $1/2(1 - \sqrt{2} - \sqrt{-9 - 2\sqrt{2}})$
31	$1 + 2t + 2t^2 + 6t^3 + 9t^4$	$1/2(-1 + \sqrt{-1} + \sqrt{5} + \sqrt{-5}),$ $1/2(-1 - \sqrt{-1} + \sqrt{5} - \sqrt{-5}),$ $1/2(-1 + \sqrt{-1} - \sqrt{5} - \sqrt{-5}),$ $1/2(-1 - \sqrt{-1} - \sqrt{5} + \sqrt{-5})$

Stufe	$P(t)$
	Annäherungen für $\alpha_1, \ldots, \alpha_{2g}$
41	$1 + 5t^2 + 2t^3 + 15t^4 + 27t^6$
	$-1.107159872 - 1.331989872\sqrt{-1}, -1.107159872 + 1.331989872\sqrt{-1},$ $0.2695944364 - 1.710940922\sqrt{-1}, 0.2695944364 + 1.710940922\sqrt{-1},$ $0.8375654353 - 1.516075243\sqrt{-1}, 0.8375654353 + 1.516075243\sqrt{-1}$
47	$1 + 5t^2 + 4t^3 + 13t^4 + 12t^5 + 45t^6 + 81t^8$
	$-1.437881791 - 0.9656583018\sqrt{-1}, -1.437881791 + 0.9656583018\sqrt{-1},$ $-0.0941393303 - 1.729490615\sqrt{-1}, -0.0941393303 + 1.729490615\sqrt{-1},$ $0.4123939712 - 1.682239939\sqrt{-1}, 0.4123939712 + 1.682239939\sqrt{-1},$ $1.119627150 - 1.321527542\sqrt{-1}, 1.119627150 + 1.321527542\sqrt{-1}$
59	$1 + 2t + 7t^2 + 13t^3 + 31t^4 + 41t^5 + 93t^6$ $+117t^7 + 189t^8 + 162t^9 + 243t^{10}$
	$-1.453617273 - 0.9418050873\sqrt{-1}, -1.453617273 + 0.9418050873\sqrt{-1},$ $-1.153609275 - 1.291969675\sqrt{-1}, -1.153609275 + 1.291969675\sqrt{-1},$ $0.04155695785 - 1.731552199\sqrt{-1}, 0.04155695785 + 1.731552199\sqrt{-1},$ $0.3773752721 - 1.690440151\sqrt{-1}, 0.3773752721 + 1.690440151\sqrt{-1},$ $1.188294318 - 1.260141505\sqrt{-1}, 1.188294318 + 1.260141505\sqrt{-1}$
71	$(1 + t + t^2 + 3t^3 + 3t^4 + 9t^5 + 27^6)$ $(1 - t + 5t^2 - 3t^3 + 15t^4 - 9t^5 + 27^6)$
	$-1.602200775 - 0.6579913951\sqrt{-1}, -1.602200775 + 0.6579913951\sqrt{-1},$ $-0.1822240296 - 1.722438505\sqrt{-1}, -0.1822240296 + 1.722438505\sqrt{-1},$ $1.284424805 - 1.162003839\sqrt{-1}, 1.284424805 + 1.162003839\sqrt{-1},$ $-0.9561145892 - 1.444245440\sqrt{-1}, -0.9561145892 + 1.444245440\sqrt{-1},$ $0.3567689675 - 1.694908819\sqrt{-1}, 0.3567689675 + 1.694908819\sqrt{-1},$ $1.099345622 - 1.338446564\sqrt{-1}, 1.099345622 + 1.338446564\sqrt{-1}$

Tabelle 4.3: Nenner einiger Zeta-Funktionen von hyperelliptischen Kurven C_P über $\mathbb{F}_3$ und deren Nullstellen in $\mathbb{C}$.

Stufe	Zeta-Funktionen von Kurven C_P über $\mathbb{F}_5$ und deren Nullstellen in $\mathbb{C}$	
	$P(t)$	$\alpha_1, \overline{\alpha_1}, \ldots, \alpha_{2g}, \overline{\alpha_2 g}$
11	$1 - t + 5t^2$	$1/2(1+\sqrt{-19})$, $1/2(1-\sqrt{-19})$
17	$1 - t + 5t^2$	$1/2(1+\sqrt{-19})$, $1/2(1-\sqrt{-19})$
19	$1 - 3t + 5t^2$	$1/2(3+\sqrt{-11})$, $1/2(3-\sqrt{-11})$
23	$1 + 2t + 6t^2 + 25t^4 + 10t^3$	$1/2(-1+\sqrt{5}+\sqrt{-14-2\sqrt{5}})$, $1/2(-1+\sqrt{5}-\sqrt{-14-2\sqrt{5}})$, $1/2(-1+\sqrt{5}+\sqrt{-14+2\sqrt{5}})$, $1/2(-1+\sqrt{5}-\sqrt{-14+2\sqrt{5}})$
29	$(1 + t + 5t^2)^2$	$1/2(-1+\sqrt{-19})$,$1/2(-1-\sqrt{-19})$, $1/2(-1+\sqrt{-19})$,$1/2(-1-\sqrt{-19})$
31	$(1 - t + 5t^2)^2$	$1/2(1+\sqrt{-19})$,$1/2(1-\sqrt{-19})$, $1/2(1+\sqrt{-19})$,$1/2(1-\sqrt{-19})$

Stufe	$P(t)$
	Annäherungen für $\alpha_1, \ldots, \alpha_{2g}$
41	$1 + 2t + 11t^2 + 16t^3 + 55t^4 + 50t^5 + 125t^6$
	$-1.451605963 - 1.700835127\sqrt{-1}, -1.451605963 + 1.700835127\sqrt{-1}$, $-0.4030317168 - 2.199446620\sqrt{-1}, -0.4030317168 + 2.199446620\sqrt{-1}$, $0.8546376797 - 2.066299697\sqrt{-1}, 0.8546376797 + 2.066299697\sqrt{-1}$
47	$1 + 2t + 4t^2 + 14t^3 + 38t^4 + 70t^5 + 100t^6 + 250t^7 + 625t^8$,
	$-2.126757060 - 0.6905826593\sqrt{-1}, -2.126757060 + 0.6905826593\sqrt{-1}$, $-1.197126298 - 1.888620827\sqrt{-1}, -1.197126298 + 1.888620827\sqrt{-1}$, $0.7474684539 - 2.107437048\sqrt{-1}, 0.7474684539 + 2.107437048\sqrt{-1}$, $1.576414903 - 1.585848685\sqrt{-1}, 1.576414903 + 1.585848685\sqrt{-1}$

Tabelle 4.4: Nenner einiger Zeta-Funktionen von hyperelliptischen Kurven C_P über $\mathbb{F}_5$ und deren Nullstellen in $\mathbb{C}$.

Stufe	Zeta-Funktionen von Kurven C_P über $\mathbb{F}_5$ und deren Nullstellen in $\mathbb{C}$	
	$P(t)$	$\alpha_1, \ldots, \alpha_{2g}$
11	$1+2t+7t^2$	$-1+\sqrt{-6}$,$-1-\sqrt{-6}$
17	$1-2t+7t^2$	$1+\sqrt{-6}$,$1-\sqrt{-6}$
19	$1+t+7t^2$	$1/2(-1+3\sqrt{-3})$, $1/2(-1-3\sqrt{-3})$
23	$1-2t+10t^2-14t^3+49t^4$	$1/2(1+\sqrt{5}+\sqrt{-22+2\sqrt{5}})$, $1/2(1+\sqrt{5}-\sqrt{-22+2\sqrt{5}})$, $1/2(1-\sqrt{5}+\sqrt{-22-2\sqrt{5}})$, $1/2(1-\sqrt{5}-\sqrt{-22-2\sqrt{5}})$
29	$1+6t^2+49t^4$	$\sqrt{-3+2\sqrt{-10}}$, $-\sqrt{-3+2\sqrt{-10}}$, $\sqrt{-3-2\sqrt{-10}}$, $-\sqrt{-3-2\sqrt{-10}}$
31	$1+4t+13t^2+28t^3+49t^4$	$-1+1/2\sqrt{5}+1/2\sqrt{-19-4\sqrt{5}}$, $-1+1/2\sqrt{5}-1/2\sqrt{-19-4\sqrt{5}}$, $-1-1/2\sqrt{5}+1/2\sqrt{-19+4\sqrt{5}}$, $-1-1/2\sqrt{5}-1/2\sqrt{-19+4\sqrt{5}}$
Stufe	$P(t)$ Annäherungen für $\alpha_1, \ldots, \alpha_{2g}$	
41	$1-6t+29t^2-86t^3+203t^4-294t^5+343t^6$ $0.1624345647-2.640760309\sqrt{-1}, 0.1624345647+2.640760309\sqrt{-1}$, $0.7304055636-2.542932896\sqrt{-1}, 0.7304055636+2.542932896\sqrt{-1}$, $2.107159872-1.599961648\sqrt{-1}, 2.107159872+1.599961648\sqrt{-1}$	

Tabelle 4.5: Nenner einiger Zeta-Funktionen von hyperelliptischen Kurven C_P über $\mathbb{F}_7$ und deren Nullstellen in $\mathbb{C}$.

Stufe	Zeta-Funktionen von Kurven C_P über $\mathbb{F}_{31}$ und deren Nullstellen in $\mathbb{C}$	
	$P(t)$	$\alpha_1, \ldots, \alpha_{2g}$
11	$1-7t+31t^2$	$1/2(7+5\sqrt{-3})$, $1/2(7-5\sqrt{-3})$
17	$1+10t+31t^2$	$-5+\sqrt{-6}$, $-5-\sqrt{-6}$
19	$1+4t+31t^2$	$-2+3\sqrt{-3}$, $-2-3\sqrt{-3}$
23	$1+17t^2+961t^4$	$1/2\sqrt{-34+6\sqrt{-395}}$, $-1/2\sqrt{-34+6\sqrt{-395}}$, $1/2\sqrt{-34-6\sqrt{-395}}$, $-1/2\sqrt{-34-6\sqrt{-395}}$
29	$1-6t+21t^2-186t^3+961t^4$	$1/2(3+5\sqrt{2}+\sqrt{-65+30\sqrt{2}})$, $1/2(3+5\sqrt{2}-\sqrt{-65+30\sqrt{2}})$, $1/2(3-5\sqrt{2}+\sqrt{-65-30\sqrt{2}})$, $1/2(3-5\sqrt{2}-\sqrt{-65-30\sqrt{2}})$

Tabelle 4.6: Nenner einiger Zeta-Funktionen von hyperelliptischen Kurven C_P über $\mathbb{F}_{31}$ und deren Nullstellen in $\mathbb{C}$.

Stufe	Zeta-Funktionen von Kurven C_P über $\mathbb{F}_{1021}$ und deren Nullstellen in $\mathbb{C}$	
	$P(t)$	$\alpha_1, \ldots, \alpha_{2g}$
11	$1 - 22t + 1021t^2$	$11 + 30\sqrt{-1}$, $11 - 30\sqrt{-1}$
17	$1 - 5t + 1021t^2$	$1/2(5 - 3\sqrt{-451})$, $1/2(5 + 3\sqrt{-451})$
19	$1 + 40t + 1021t^2$	$-20 + 3\sqrt{-69}$, $-20 - 3\sqrt{-69}$

Tabelle 4.7: Nenner einiger Zeta-Funktionen von hyperelliptischen Kurven C_P über $\mathbb{F}_{1021}$ und deren Nullstellen in $\mathbb{C}$.

$$N_{q^r}(g) \leq q^r + 1 + [2g\sqrt{q^r}].$$

Serre hat dieses Ergebnis verbessert:

$$N_{q^r}(g) \leq q^r + 1 + g[2\sqrt{q^r}] \text{ (Hasse-Weil-Serre-Schranke).}$$

Siehe hierzu [LG, Part II, IV, p.70] und [St, Theorem V.2.3, Theorem V.3.1]. Für das Geschlecht $g = 1$ und $g = 2$ kann man Werte von $N_{q^r}(g)$ explizit angeben.

Satz 4.1
Sei p eine Primzahl.
Dann ist für $g = 1$:

$$N_{p^r}(1) = \begin{cases} q^r + [2\sqrt{q^r}] & falls \quad p|[2\sqrt{q^r}], \quad r \geq 3, \quad r \quad ungerade \\ q^r + 1 + [2\sqrt{q^r}] & sonst, \end{cases}$$

und für $g = 2$:

i) $N_4(2) = 10$, $N_9(2) = 20$

ii) falls für ungerades p gilt: $p|[2\sqrt{p^r}]$ oder $p^r = \begin{cases} m^2 + 1 \\ m^2 + m + 1 \\ m^2 + m + 2 \end{cases}, m \in \mathbb{Z}$ *, dann ist*

$$N_{p^r}(2) = \begin{cases} p^r + 2[\sqrt{p^r}] & , \textit{für } 2\sqrt{p^r} - [2\sqrt{p^r}] > \frac{\sqrt{5}-1}{2} \\ p^r + 2[\sqrt{p^r}] - 1 & , \textit{für } 2\sqrt{p^r} - [2\sqrt{p^r}] < \frac{\sqrt{5}-1}{2} \end{cases}$$

falls nicht, so ist $N_{p^r}(2) = p^r + 1 + 2[2\sqrt{p^r}]$.

Beweis:
Vergleiche [TV, Theorem 2.3.16 (und 2.3.17(Druckfehler)), p. 179] und [GF].

In Tabelle 4.8 sind einige für uns interessante Werte für maximal mögliche Anzahlen von Punkten aufgelistet. Diese wurden meist aus oben genannten Quellen übernommen. Die Eintragungen geben die maximale Anzahl von Punkten einer Kurve über $\mathbb{F}_{p^r}$ (p Primzahl) wieder, beziehungsweise Intervalle (Zahl-Zahl) oder obere Schranken (-Zahl) dieser Anzahlen. Sie sind im entsprechenden Kästchen der Reihe nach für $r = 1, 2, \ldots$ aufgelistet und durch Kommata getrennt.

Die folgende Definition und Proposition ist aus [La] übernommen.

Definition 4.1
Eine glatte projektive Kurve vom Geschlecht g über $\mathbb{F}_q$ heißt maximal, wenn sie mit obigen Notationen eine der drei folgenden äquivalenten Bedingungen erfüllt.

i) $P(t) = (1 + [2\sqrt{q}]t + qt^2)^g$

ii) $\alpha_i + \overline{\alpha_i} = -[2\sqrt{q}]$ *für* $1 \leq i \leq g$

iii) $N_1(X) = q + 1 + g[2\sqrt{q}]$

g	1	2
$N_{3^r}(g)$	7,16,38,100,275,783,2281	8,20,48,118,306,838,2372
$N_{5^r}(g)$	10,36,148,676,3237	12,46,168,726,3347
$N_{7^r}(g)$	13,64,381,2500	18,68,418,2598
$N_{31^r}(g)$	43,1024	52,1086
$N_{1021^r}(g)$	1085	1148
g	3	4
$N_{3^r}(g)$	10,28,56,136,-337,-892,-2467	12,30,64-68,154,-368,-946,-2560
$N_{5^r}(g)$	16,56,-192,-776,-3459	-22,-66,-214,-826,-3570
$N_{7^r}(g)$	20,-92,-455,-2696	-28,-106,-492,-2794
$N_{31^r}(g)$	-65,-1148	-76,-1210
$N_{1021^r}(g)$	-1212	-1274
g	5	6
$N_{3^r}(g)$	12-13,32-36,68-78,156-172,-399,-1000	14-15,35-40,76-86,190,-430,-1054
$N_{5^r}(g)$	-26,-76,-236,-876,-3681	-30,-86,-256,-926,-3792
$N_{7^r}(g)$	-33,-120,-529,-2892	-38,-134,-566,-2990
$N_{31^r}(g)$	-87,-1272	-98,-1334
$N_{1021^r}(g)$	-1337	-1400

Tabelle 4.8: Maximale Anzahlen von Punkten einer glatten projektiven Kurve über einem endlichen Körper $\mathbb{F}_{p^r}$.

Bemerkung 4.3

Eine Kurve mit maximal möglicher Anzahl von Punkten ist nicht notwendig maximal, denn nicht für alle Geschlechter und Körper wird die Hasse-Weil-Serre Schranke angenommen, wie man mit Hilfe von Satz 4.1 erkennt.

□

Proposition 4.1
Für eine Kurve X über $\mathbb{F}_{q^2}$ sind äquivalent:

i) X *ist maximal*

ii) $P(t) = (1 + qt)^{2g}$

iii) $N_1(X) = q^2 + 1 + 2gq$

iv) $N_s(X) = q^{2s} + 1 + (-1)^{s-1} 2gq^s$

□

Bedingung *iv)*obiger Proposition besagt demnach, dass eine maximale Kurve X über einem endlichen Körper $\mathbb{F}_{q^2}$ auch maximale Kurve über dem Körper $\mathbb{F}_{q^{2+4i}}$, $i \in \mathbb{N}$ ist.

Beispiel 4.3

Betrachten wir wieder die Kurve $C_P(11)$. In Beispiel 4.2 haben wir für $r \in \mathbb{N}$ eine Formel zur Berechnung von $N_r(C_P(11)/\mathbb{F}_{3^r})$ angegeben. Berechnen wir nun einige Werte für kleines r so erhalten wir folgende Tabelle:

r	1	2	3	4	5	6	7	8	9	10
$N_r(X_0(11)/\mathbb{F}_{3^r})$	5	15	20	75	275	720	2105	6675	19820	58575

Wir sehen also, dass $C_P(11)$ eine maximale Kurve über $\mathbb{F}_{3^5}$ ist. Nutzen wir die in den Tabellen 4.3, 4.4, 4.5, 4.6 und 4.7 aufgeführten algebraischen Zahlen α_i, $\overline{\alpha_i}$ und die Gleichung 4.1, so sehen wir, dass $C_P(11)\ /\mathbb{F}_{5^7}$, $C_P(17)\ /\mathbb{F}_{3^2}$, $C_P(17)\ /\mathbb{F}_{5^7}$ und $C_P(31)\ /\mathbb{F}_{5^7}$ maximale Kurven sind. Die Rechnungen dazu finden sich im Verzeichnis '~/data/zet/' und deren Zusammenfassung in der Datei '~/data/zet/maxkur'. Aus Proposition 4.1 erhalten wir, dass $C_P(17)$ maximale Kurve über $\mathbb{F}_{3^{2+4i}}$ für $i \in \mathbb{N}$ ist.

□

4.2 Codes, die über der asymptotischen Gilbert-Varshamov-Schranke liegen

Satz 4.2 (Tsfasman,Vladut,Zink)
Sei $q = p^2$ und l eine Primzahl, die größer als p ist. Dann gilt

$$\lim_{l\to\infty} \frac{g(X_0(l))}{N_l(X_0(l))} = \frac{1}{\sqrt{q}-1}$$

Beweis:
Siehe [TVZ], [Mo 5.6.9].

□

Bemerkung 4.4

Dieser Satz gilt auch für $q = p^4$, was ebenfalls in [TVZ] bewiesen wird. Der allgemeine Fall $q = p^{2n}, n \in \mathbb{N}$ wurde unabhängig von Manin, Vladut beziehungsweise Ihara bewiesen. Dabei wurden nicht die klassischen Modulkurven sondern Drinfeldmodulen benutzt.

□

Vergleicht man für großes l die Parameter der daraus resultierenden Codes mit der asymptotischen Gilbert-Varshamov-Schranke, so erhält man folgende Proposition:

Proposition 4.2
Für $p \geq 7$ gibt es Folgen von Goppa-Codes, deren Grenzwerte im $\delta - R$ Diagramm über der Gilbert-Varshamov-Schranke liegen. Sie liegen auf der Geraden $R - \delta = \frac{1}{\sqrt{q}-1}$.

4.3 Konstruktion einiger Codes

Wir wollen nun zunächst am Beispiel $C_p(11)$ über $\mathbb{F}_{3^i}$ $(i \in \mathbb{N})$ einige Codes konstruieren.

Beispiel 4.4

In Beispiel 4.1 haben wir uns ein nicht singuläres Modell dieser Kurve konstruiert. Sei nun $\mathfrak{P}_i$ die Menge $\{P_1, \ldots, P_{n_i}\}$ der $\mathbb{F}_{3^i}$-rationalen, endlichen Punkte von $C_P(11)$ über dem Körper $\mathbb{F}_{3^i}$. Seien dabei $P_{1,\infty}$ und $P_{2,\infty}$ die beiden unendlichen Punkte. Wir wollen nun Codes der Form $C_L(X_0(11), \mathfrak{P}_i, G)$ untersuchen. Dabei sei $G := (P_{1,\infty} + P_{2,\infty})$. In [Wi, Kapitel 6] wird im Fall einer Kurve X mit einem Modell $s^m + f(x)$ in $K[s,x]$ ($m \in \mathbb{N}$, K ist endlicher Körper) und einem einfachen Punkt im Unendlichen P_∞ eine Basis des Raumes $L(nP_\infty)$ und resultierende Erzeugermatritzen der Codes $C_L(X, \mathfrak{P}_i, nP_\infty)$ für natürliche Zahlen $n \in \mathbb{N}$ angegeben.

Würden wir analog zur dort angegebenen Basis hier dieselbe wählen, dann würden wir folgende Basis erhalten:

$$B(L(lG)) \quad = \quad \{s^r x^t | mt + deg(f)r \leq deg(D), r \leq m\} \tag{4.2}$$

Für $C_P(11)$ wäre dann also

$$B(L(lG)) = \{s^r x^t | 2t + 4r \leq 2l, r \in \{0,1\}\}.$$

Als Erzeugermatrix hätte man:

$$\begin{pmatrix} 1 & \dots & 1 \\ x(P_1) & \dots & x(P_{n_i}) \\ x^2(P_1) & \dots & x^2(P_{n_i}) \\ \dots & \dots & \dots \\ x^l(P_1) & \dots & x^l(P_{n_i}) \\ sx(P_1) & \dots & sx(P_{n_i}) \\ sx^2(P_1) & \dots & sx^2(P_{n_i}) \\ \dots & \dots & \dots \\ sx^{l-2}(P_1) & \dots & sx^{l-2}(P_{n_i}) \end{pmatrix}$$

Eine Möglichkeit diese Codes zu konstruieren, liefert der Brill-Noether Algorithmus (Siehe Abschnitt 1.4.1). Wir werden bei dessen Beschreibung dabei im Wesentlichen [HB] folgen (Siehe auch [BR] und [CF]). In Beispiel 4.1 haben wir bereits den Desingularisierungsbaum $\mathfrak{T}_{P_\infty}$ von C_P im Punkt P_∞ berechnet. Wir sehen, dass der adjungierte Divisor $\mathfrak{A}$ von C_P gleich $2P_{1,\infty} + 2P_{2,\infty}$ ist. Bestimmen wir nun die Ordnungen der Transformierten von $a := \frac{A}{S}$ und $x := \frac{X}{S}$ im Punkt $P_{1,\infty}$ und $P_{2,\infty}$. Wie man aus $\mathfrak{T}_{P_\infty}$ abliest, wird a in $P_{1,\infty}$ in $R^2V - R^2$ und in $P_{2,\infty}$ in $R^2V + R^2$ transformiert. Da sowohl R als auch V lokale Parameter der Punkte $P_{1,\infty}$ und $P_{2,\infty}$ sind, sehen wir, dass die Ordnung der Transformierten von a in $P_{1,\infty}$ und $P_{2,\infty}$ jeweils zwei ist. Analog erhalten wir, da sich x in $P_{1,\infty}$ in $RV - R$ und in $P_{2,\infty}$ in $RV + R$ transformiert, dass die Ordnung der Transformierten von x in $P_{1,\infty}$ und $P_{2,\infty}$ jeweils eins ist. Mit Hilfe dieser Ordnungen erhalten wir:

$$\begin{aligned} (A) &= 2P_{1,\infty} + 2P_{2,\infty} \\ (S) &= Q_1 + R_1 + R_2 + R_3 \\ (X) &= P_{1,\infty} + P_{2,\infty} + 2Q_1 \end{aligned}$$

Dabei ist $Q_1 = (1,0,0)$ wie in Beispiel 4.1 und $R_1 := (1,0,e^7)$, $R_2 := (1,0,e^{11})$ und $R_3 := (1,0,e^{21})$ die drei Schnittpunkte von $C_P(11)$ mit der Geraden $S = 0$ über dem Körper $\mathbb{F}_3[e]/(e^3 - e + 1)$.
Wir wählen nun die Form $G_0 := A^d$ vom Grad $d \geq 1$. Da $(G_0) \geq \mathfrak{A}$ und $Supp(G_0) \subset Supp(\mathfrak{A})$ ist können wir wie in Algorithmus 1.4.1 beschrieben wurde, fortfahren. Sei $D_d := (G_0) - \mathfrak{A} = 2(d-1)(P_{1,\infty} + P_{2,\infty})$. Nach dem Satz von Riemann-Roch ist $l(D_d)$ gleich $deg(D_d) - g + 1 + l(\kappa - D_d)$. Das Geschlecht von $C_P(11)$ ist 1 und nach Lemma 1.2 ist folglich für alle effektiven Divisoren D_d die Dimension von $L(\kappa - D_d)$ gleich null. Ist also $d \geq 2$, dann ist $l(D_d) = deg(D_d) = 4(d-1)$. Im Fall $d = 1$ ist A die einzige Form vom Grad 1 für die $(A) \geq (G_0) - D_d = \mathfrak{A}$ und $Supp(A) \subset Supp(\mathfrak{A})$ gilt. Also ist $L(D_d) = L((0)) = \{1\}$ und somit $l(D_d) = 1$. Ist d größer oder gleich zwei, so hat jedes Monom G vom Grad d außer S^d und $S^{d-1}X$ einen Divisor, der größer als $(G_0) - D_d$ ist. Insgesamt gibt es also $\frac{(d+2)(d+1)}{2} - 2$ Monome vom Grad d, für die $G \geq (G_0) - D_d$ gilt. Unter diesen gibt es nun noch $\frac{(d-2)(d-3)}{2}$, die durch S^2A^2 geteilt werden. Es verbleiben also $\frac{(d+2)(d-1)}{2} - 2 - \frac{(d-2)(d-3)}{2} = 4(d-1)$ Monome. Diese sind als Elemente des Raumes der Formen vom Grad d, die nicht von f^h (siehe Beispiel 4.1) geteilt werden und für die $(G) \geq (G_0) - \mathfrak{A}$ gilt, linear

unabhängig. Teilen wir die Formen des oben beschriebenen Raumes noch durch die Form A^d, so erhalten wir eine Basis von $L(D_d)$. Für $d = 2, 3, 4$ ist dies zum Beispiel:

$$\begin{aligned}
B(L(D_2)) &= \left\{1, \frac{S}{A}, \frac{X}{A}, \frac{X^2}{A^2}\right\} \\
B(L(D_3)) &= \left\{1, \frac{S}{A}, \frac{X}{A}, \frac{X^2}{A^2}, \frac{SX}{A^2}, \frac{X^3}{A^3}, \frac{SX^2}{A^3}, \frac{S^2}{A^2}\right\} \\
B(L(D_4)) &= \left\{1, \frac{S}{A}, \frac{X}{A}, \frac{X^2}{A^2}, \frac{SX}{A^2}, \frac{X^3}{A^3}, \frac{SX^2}{A^3}, \frac{X^4}{A^4}\right. \\
&\quad \left.\frac{S^3}{A^3}, \frac{S^2X}{A^3}, \frac{SX^3}{A^4}, \frac{S^2X^2}{A^4}\right\}
\end{aligned}$$

Falls $d \geq 5$ gilt, dann erhalten wir folgende Basis:

$$\begin{aligned}
B(L(D_d)) = &\left\{1, \frac{X}{A}, \frac{X^2}{A}, \frac{X^3}{A^3}, \ldots, \frac{X^{d-1}}{A^{d-1}}, \frac{X^d}{A^d},\right. \\
&\frac{S}{A}, \frac{SX}{A^2}, \frac{SX^2}{A^3}, \ldots, \frac{SX^{d-2}}{A^{d-1}}, \frac{SX^{d-1}}{A^d}, \\
&\frac{S^2X^{d-3}}{A^{d-1}}, \frac{S^3X^{d-4}}{A^{d-1}}, \frac{S^4X^{d-5}}{A^{d-1}}, \ldots, \frac{S^{d-2}X}{A^{d-1}}, \frac{S^{d-1}}{A^{d-1}} \\
&\left.\frac{S^2X^{d-2}}{A^d}, \frac{S^3X^{d-3}}{A^d}, \frac{S^4X^{d-4}}{A^d} \ldots, \frac{S^{d-3}X^3}{A^d}, \frac{S^{d-2}X^2}{A^d}\right\}
\end{aligned}$$

Betrachten wir nun den affinen Teil $A = 1$ dieser Basen. Wird in den Monomen der Erzeugenden obiger Basen S^2 mit X^4 ersetzt, dann verlieren diese Mengen nicht die Eigenschaft, Basen von $L(D_d)$ zu sein, Daraus wird ersichtlich, dass gilt:

$$B(L(D_d)) = \{s^r x^t | t + 2r \leq 2d, r \in \{0, 1\}\}$$

Wir haben also die in (4.2) angegebenen Basen von [Wi] für gerade l konstruiert.

Beispiel 4.5

Gehen wir nun analog zu Beispiel 4.4 für die Kurven $C_P(17)$ und $C_P(19)$ in Charakteristik drei vor. Der einzige, singuläre Punkt jeder dieser Kurven ist der Punkt $P_\infty = (0 : 1 : 0)$. Wir können auch in beiden Fällen mit denselben Transformationen wie im Fall der Kurve $C_P(11)$ desingularisieren. In Abbildung 4.2 ist dies in einem gemeinsamen Desingularisierungsbaum dargestellt. Die oberen Polynome an jedem Knoten des Baumes gehören zur Kurve $C_P(11)/\overline{\mathbb{F}_3}$, die mittleren zur Kurve $C_P(17)/\overline{\mathbb{F}_3}$ und die unteren zu $C_P(19)/\overline{\mathbb{F}_3}$. Für die Kurven $C_P(17)$ und $C_P(19)$ erhalten wir dieselben Basen $B(L((D_d)))$ wie im Falle von $C_P(11)$.

Die Codes $C_L(C_P/\mathbb{F}_{3^i}, \mathfrak{P}_i, D_d)$ $(d \geq 2)$, die wir dann erhalten, haben für $4 \leq deg(D_d) = 4(d-1) < deg(\mathfrak{P}_i)$ nach Satz 1.13 die Parameter

$$\begin{aligned}
len &= n_i, \\
dim &= 4(d-1) - g(C_P) + 1 = 4(d-1), \\
dis &\geq n_i - 4(d-1).
\end{aligned}$$

Dabei ist $\mathfrak{P}_i$ die Summe der restlichen $\mathbb{F}_{3^i}$-rationalen Punkte der jeweiligen Kurve. Für die Dimension der Codes gilt dabei Gleichheit, da wir bereits gesehen haben, dass die Divisoren D_d für $d \geq 2$ nicht speziell sein können.

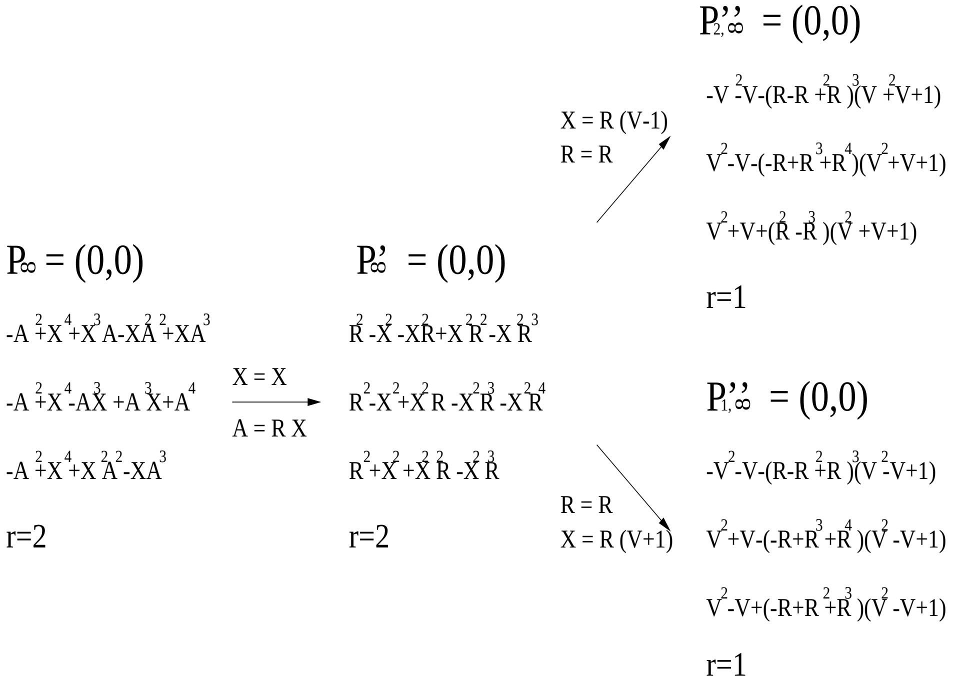

Abbildung 4.2: Desingularisierungsbaum der Kurve $C_P(11)/\overline{\mathbb{F}_3}$, $C_P(17)/\overline{\mathbb{F}_3}$ und $C_P(19)/\overline{\mathbb{F}_3}$ im Punkt P_∞ (S=1).

Ist d=1, so erhalten wir die trivialen Codes $[n_i, 1, n_i - 1]$, die nur aus den Codewörtern $(0, \ldots, 0), (1, \ldots, 1) und (-1, \ldots, -1)$ bestehen.

Über $\mathbb{F}_9 = \mathbb{F}_3[e]/(e^2 + e - 1)$ hat $C_P(11)$, außer den drei Punkten von $\mathbb{F}_3$, zehn weitere Punkte, nämlich

$$(-e+1, 1),\ (e-1, 1),\ (-e+1, -e+1),\ (e-1, -e+1),\ (-e-1, -e),$$
$$(e+1, -e),\ (-e+1, e-1),\ (e-1, e-1),\ (e, e+1) \text{ und } (-e, e+1).$$

Wir erhalten für $d \in \{2, 3, 4\}$ die Codes $C_L(X_0(11)/\overline{\mathbb{F}_3}, \mathfrak{P}_2, D_d)$, mit den Parameter $[13, 4(d-1), \geq 13 - 4(d-1)]$, falls $d \in \{2, 3, 4\}$ und $[13, 1, 12]$, falls d=1 ist. Der $[13, 12, 1]$ Code hat Erzeugermatrix:

$$\begin{pmatrix}
1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\
0 & 1 & -1 & -e+1 & e-1 & -e+1 & e-1 & -e-1 & e+1 & -e+1 & e-1 & e & -e \\
0 & -1 & -1 & 1 & 1 & -e+1 & -e+1 & -e & -e & e-1 & e-1 & e+1 & e+1 \\
0 & 1 & 1 & 1 & 1 & -1 & -1 & -e+1 & -e+1 & -1 & -1 & e-1 & e-1 \\
0 & -1 & 1 & -e+1 & e-1 & -1 & 1 & 1 & -1 & 1 & -1 & 1 & -1 \\
0 & -1 & -1 & 1 & 1 & e-1 & e-1 & e+1 & e+1 & -e+1 & -e+1 & -e & -e \\
0 & 1 & 1 & 1 & 1 & 1 & 1 & -e & -e & 1 & 1 & -e & -e \\
0 & 1 & -1 & -e+1 & e-1 & e-1 & -e+1 & -e & e & e-1 & -e+1 & e+1 & -e+1 \\
0 & 1 & -1 & e-1 & -e+1 & e-1 & -e+1 & 1 & -e & e-1 & -e+1 & -e-1 & e+1 \\
0 & -1 & -1 & 1 & 1 & 1 & 1 & -e-1 & -1 & 1 & 1 & -1 & -1 \\
0 & -1 & 1 & -e+1 & e-1 & 1 & -1 & -e+1 & e-1 & -1 & 1 & e-1 & -e+1 \\
0 & 1 & 1 & -1 & -1 & 1 & 1 & e+1 & 1 & 1 & 1 & 1 & 1
\end{pmatrix}$$

Die Erzeugermatrix für $d = i$, $i \in \{2, 3, 4\}$ erhalten wir aus derjenigen für $d = 4$, indem wir die letzten $4(4 - i)$ Zeilen obiger Matrix streichen.

In Beispiel 4.3 haben wir eine Tabelle mit der Anzahl der Punkte von $C_P(11)$ über einigen kleinen Erweiterungen von $\mathbb{F}_3$ angegeben. Mit deren Hilfe und der oben angegebenen Parameterabschätzungen erhalten wir für die Codes $C_L(C_P(11)/\overline{\mathbb{F}_{p^i}}$, $\mathfrak{P}_i$, $D_d)$ mit $4 \leq 4(d-1) < deg(\mathfrak{P}_i)$ folgende Parameter

$$\begin{array}{rll}
[13, & 4(d-1), & 13-4(d-1) \text{ oder } 14-4(d-1)],\\
[18, & 4(d-1), & 18-4(d-1) \text{ oder } 19-4(d-1)],\\
[73, & 4(d-1), & 73-4(d-1) \text{ oder } 74-4(d-1)],\\
[273, & 4(d-1), & 273-4(d-1) \text{ oder } 274-4(d-1)],\\
[718, & 4(d-1), & 718-4(d-1) \text{ oder } 719-4(d-1)],\\
[2103, & 4(d-1), & 2103-4(d-1) \text{ oder } 2104-4(d-1)],\\
[6673, & 4(d-1), & 6673-4(d-1) \text{ oder } 6674-4(d-1)],\\
[19818, & 4(d-1), & 19818-4(d-1) \text{ oder } 19819-4(d-1)],\\
[58573, & 4(d-1), & 58573-4(d-1) \text{ oder } 58574-4(d-1)].
\end{array}$$

Im Allgemeinen ($d > 1$) haben die Codes $C_L(C_P(11)/\overline{\mathbb{F}_{p^i}}, \mathfrak{P}_i, D_d)$ die Parameter

$$\begin{array}{rcl}
len & = & 3^i - 3 - \left(-\frac{1}{2} - \frac{\sqrt{-11}}{2}\right)^i - \left(-\frac{1}{2} + \frac{\sqrt{-11}}{2}\right)^i,\\
dim & = & 4(d-1),\\
dis \quad oder \quad dis - 1 & = & 3^i - 3 - \left(-\frac{1}{2} - \frac{\sqrt{-11}}{2}\right)^i - \left(-\frac{1}{2} + \frac{\sqrt{-11}}{2}\right)^i - 4(d-1).
\end{array}$$

Genauso erhalten wir nun die Codes $C_L(C_P(17)/\overline{\mathbb{F}_{p^i}}, \mathfrak{P}_i, D_d)$, $(4 \leq 4(d-1) < deg(\mathfrak{P}_i))$ mit den Parametern

$$\begin{array}{rll}
[14, & 4(d-1), & 14-4(d-1) \text{ oder } 15-4(d-1)],\\
[26, & 4(d-1), & 26-4(d-1) \text{ oder } 27-4(d-1)],\\
[62, & 4(d-1), & 62-4(d-1) \text{ oder } 63-4(d-1)],\\
[242, & 4(d-1), & 242-4(d-1) \text{ oder } 243-4(d-1)],\\
[782, & 4(d-1), & 782-4(d-1) \text{ oder } 783-4(d-1)],\\
[2186, & 4(d-1), & 2186-4(d-1) \text{ oder } 2187-4(d-1)].
\end{array}$$

Im Allgemeinen ($d > 1$):

$$\begin{array}{rcl}
len & = & 3^i - 3 - \left(\sqrt{-3}\right)^i - \left(-\sqrt{-3}\right)^i\\
dim & = & 4(d-1)\\
dis \quad oder \quad dis - 1 & = & 3^i - 3 - \left(\sqrt{-3}\right)^i - \left(-\sqrt{-3}\right)^i
\end{array}$$

und die Codes $C_L(C_P(19)/\overline{\mathbb{F}_{p^i}}, \mathfrak{P}_i, D_d)$, $(4 \leq 4(d-1) < deg(\mathfrak{P}_i))$ mit den Parametern:

$$\begin{array}{rll}
[10, & 4(d-1), & 10-4(d-1) \text{ oder } 11-4(d-1)],\\
[16, & 4(d-1), & 16-4(d-1) \text{ oder } 17-4(d-1)],\\
[94, & 4(d-1), & 94-4(d-1) \text{ oder } 95-4(d-1)],\\
[244, & 4(d-1), & 244-4(d-1) \text{ oder } 245-4(d-1)],\\
[682, & 4(d-1), & 682-4(d-1) \text{ oder } 683-4(d-1)],\\
[2274, & 4(d-1), & 2274-4(d-1) \text{ oder } 2275-4(d-1)].
\end{array}$$

Im Allgemeinen ($d > 1$):

$$\begin{array}{rcl}
len & = & 3^i - 3 - \left(-1 + \sqrt{-2}\right)^i - \left(-1 - \sqrt{-2}\right)^i\\
dim & = & 4(d-1)\\
dis \quad oder \quad dis - 1 & = & 3^i - 3 - \left(-1 + \sqrt{-2}\right)^i - \left(-1 - \sqrt{-2}\right)^i
\end{array}$$

Steigen wir nun von der Erweiterung $\mathbb{F}_{3^i}$ in den Grundkörper $\mathbb{F}_3$ ab, betrachten wir also den Isomorphismus der Vektorräume

$$ab : \mathbb{F}_{3^i} \to \mathbb{F}_3{}^i,\ ab\left(\sum_{j=1}^{i-1} a_j e^j\right) \mapsto (a_0, \ldots, a_{i-1}),$$

so wird ein Code C mit den Parametern $[n, k, \geq d]$ über $\mathbb{F}_{3^i}$ in einen Code $ab(C)$ über $\mathbb{F}_3$ mit den Parametern $[in, ik, d]$ abgebildet. Nehmen wir an, dass wir durch den Abstieg den Minimalabstand d erhalten, dann sind obige Codes asymptotisch betrachtet, also für $i \to \infty$ eine für jede Wahl von d 'schlechte' Familie von Codes, das heißt die resultierenden Abschätzungen liegen im Grenzwert unterhalb der asymptotischen Gilbert-Varshamov-Schranke. Sie liegen im (δ, R)-Diagramm sogar auf der Gerade $\delta = 0$.

$\square$

Literaturverzeichnis

[**AL**] W. W. Adams,P. Loustaunau, An Introduction to Groebner Bases, Graduate Studies in Mathematics, Vol. 3, 1994.

[**BR**] D. Le Brigand, J. J. Risler, Algorithme de Brill-Noether et Codes de Goppa, Bull. Soc. Math. France, 116, 1988, p.231-253.

[**Bi**] B. J. Birch, Some Calculations of Modular Relations in Modular Functions on One Variable I, Springer Lecture Notes 320, 1972, p.175-186.

[**CF**] A. Campillo, J. I. Farran, Construction of AG Codes from Symbolic Hamburger-Noether Expressions of Plane Curves, Universidad de Valladolid, Prepublicaciones del Departamento de Algebra, Geometria Y Topologia, $n°$ 71, 1998.

[**CLS**] D. Cox, J. Little, D. O'Shea, Ideals, Varieties and Algorithms An Introduction to Computational Algebraic Geometrie and Commutative Algebra, 2nd Ed., Springer, 1996.

[**DGP**] W. Decker, G. M. Greul, G. Pfister, Primary Decomposition: Algorithms and Comparisons, in Algorithmic Algebra and Number Theory, Springer, 1998, p.187-220 oder http://loge.math.uni-sb.de/ ~agdecker.

[**Ei**] M. Eichler, The Basis Problem for Modular Forms and the Traces of the Hecke Operators, in Modular Functions of One Variable, Lecture Notes in Mathematics, 320, Springer, 1972, p. 75-151.

[**El**] N. D. Elkies, Shimura Curve Computations, Lecture Notes in Computer science 1423, (proceedings of ANTS-3, 1998; J.P.Buhler, ed), p.1-47.

[**Fr**] R. Fricke, Die elliptischen Funktionen und ihre Anwendungen, Zweiter Teil, Teubner, 1922.

[**Fu**] W.Fulton, Algebraic Curves, The Benjamin/Cummings Publishing Company, Inc., 1969.

[**GF**] G. van der Geer, M. van der Flught, Tables of Curves with many Points, 1991, http://www.wins.uva.nl/ geer.

[**GTZ**] P. Gianni, B. Träger, G. Zacharias, Gröbner bases and primary decomposition of polynomial ideals, in Computational Aspects of commutative Algebra, edited by L.Robbiano, Academic Press, New York, 1988,p.15-33.

[**Gu**] R. C. Gunning Vorlesungen über Riemannsche Flächen (Deutsche Übersetzung), Bibliographisches Institut, 1972.

[**Ha**] R. Hartshorne, Algebraic Geometrie, Graduate Texts in Mathematics, Springer-Verlag, 1977.

[**HB**] G. Hache D. Le Brigand, Effective Construction of Algebraic Geometric Codes, IEEE Transactions on Information Theoriy, Vol 41, 1995, p. 1615-1628.

[**He**] E. Hecke, Die Klassenzahl imaginär-quadratischer Körper in der Theorie der elliptischen Modulfunktionen in Mathematische Werke, Vandenhoeck und Ruprecht, 1959.

[**Hu**] T. W. Hungerford, Algebra, Springer Verlag, Graduate Texts in Mathematics 73 (8th Printing), 1996.

[**Ig**] J. I. Igusa, Kronekerian Model of Fields of Elliptic Functions, American Journal of Mathematics, 81, 1959, p.561-577.

[**Ig2**] J. I. Igusa, Fibre Systems of Jacobian Varieties (III Fibre Systems of Elliptic Curves) American Journal of Mathematics, 81, 1959, p.453-476.

[**Kn**] A. W. Knapp, Elliptic Curves, Mathematical Notes, Princeton University Press, 1992.

[**Ko**] N. Koblitz, Introduction to elliptic curves and modular Forms Graduate texts in Mathematics,Springer-Verlag, 1984.

[**La**] G. Lachaud, Somme d'Eisenstein et nombre de points de certaines courbes algébraic sur les courps finis, C.R.Acad.Sci. Paris,t. 305, Série I, 1987, p. 729-732.

[**Lam**] T. Y. Lam, The Algebraic Theory of Quadratic Forms, Mathematics Lecture Note Series, The Benjamin/Cummings Publishing Company, 1973.

[**LG**] J. van Lint, G. van der Geer, DMV Seminar Band 8, Introduction to Coding Theory and Algebraic Geometry, Birkhäuser Verlag,Basel, 1988.

[**LN**] R. Lidl, H. Niederreiter, Introduction to finite fields and their applications, Cambridge University Press, 1986.

[**Mi**] T. Miake, Modular Forms, Springer Verlag, 1989.

[**Mo**] C. J. Moreno, Algebraic Curves over Finite Fields, Cambridge Tracts in Mathematics 97, Cambridge University Press, 1991.

[**OMe**] O. T. Meara, Introduction to Quadratic Forms, Springer 1973, Third Corrected Printing.

[**Pf**] M. Pfeifer, Relationen von Funktionen auf $X_0(l)$ und Zahlentheoretische Anwendungen, Dissertation im Fachbereich Mathematik der Universität des Saarlandes, 1998.

[**Ro**] J. G. Rovira, Equations of hyperelliptic modular curves, Ann. Inst. Fourier, Grenoble, 41(4), 1991, p. 779-795

[**Sc**] W. M. Schmidt, Equations over Finite Fields An Elementary Approach, Lecture Notes in Mathematics 536, Springer, 1976.

[**Sch**] B. Schoeneberg, Das Verhalten von mehrfachen Thetareihen bei Modulsubstitutionen, Mathematische Annalen, 116, 1939, p.511-523.

[**ScP**] R. Schulze-Pillot Vorlesungsmitschrift, Codierungstheorie WS 1998/99.

[**Sh**] G. Shimura, Introduction to the Arithmetic Theory of Automorphic Functions, Princeton University Press, 1971.

[**Sha**] I.R. Shafarevich, Basic Algebraic Geometry, Springer 1977.

[**Si**] J. H. Silverman, The arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 106, Springer, 1986.

[**Si2**] J.H.Silverman, Advanced Topics in the Arithmetic of Elliptic Curves, Graduate Texts in Mathematics, 151, Springer 1994.

[**Sing**] Singular, a Computer Algebra System for Polynomial Computations version 1.2.0, FB Mathematik der Universität Kaiserslautern, 1998.

[**St**] H. Stichtenoth, Algebraic Function Fields and Codes, Universitext, Springer, Berlin, 1993.

[**SY**] T. Shimoyama,K. Yokoyama,Journal of Symbolic Computations 22 Localization and Primary Decomposition of Polynomial Ideals, 1996 p.247-277.

[**TV**] M. A. Tsfasman, S. G. Vladut, Algebraic-geometric Codes, Mathematics and its Applications, Soviet Series 58, Kluwer Academic Publishers, 1991.

[**TVZ**]M. A. Tsfasman, S. G. Vladut, T. Zink, Modular Curves, Shimura Curves, and Goppa codes better than Varshamov-Gilbert bound, Math. Nachr.,109, 1982, p.21-28.

[**Wi**] M. Wirtz, Diplomarbeit, Verallgemeinerte Goppa-Codes, Westfälische Wilhelms-Universität Münster, Fachbereich Mathematik, 1986.