Berechnung von Zetafunktionen algebraischer Kurven über endlichen Körpern

Diplomarbeit
von Markus Böttle

Angefertigt am Institut für Mathematik der
Technischen Universität Berlin

Juni 2008

Inhaltsverzeichnis

Einleitung

Die vorliegende Arbeit beschäftigt sich mit der Berechnung von Zetafunktionen algebraischer Kurven über endlichen Körpern.

Die Zetafunktion einer Kurve beinhaltet wichtige Informationen. So lassen sich das Geschlecht sowie die Anzahl der rationalen Punkte auf der Kurve selbst und auf der zu ihr assoziierten jacobischen Varietät ablesen. Die Ursache des Interesses an diesen Informationen stammt aus der Kryptographie, denn die rationalen Punkte der jacobischen Varietät, die im elliptischen Fall isomorph zur Kurve selbst ist, bilden eine (additive) abelsche Gruppe endlicher Ordnung und es bietet sich an, diese für kryptographische Zwecke zu nutzen. Dazu wird eine sogenannte Einwegfunktion auf der jacobischen Varietät benötigt, also eine Abbildung, deren Umkehrabbildung schwierig zu berechnen ist. In additiven Gruppen liefert die Multiplikation mit einer ganzen Zahl unter gewissen Bedingungen eine Einwegfunktion und wir bezeichnen die Urbildberechnung eines Elements unter dieser Multiplikation als diskretes Logarithmusproblem (DLP). Um zu gewährleisten, dass dieses DLP tatsächlich schwierig zu lösen ist, muss insbesondere die Ordnung der Gruppe einen großen Primteiler besitzen. Das DLP wird dann auf dieser zyklischen Untergruppe beschrieben.

Die Bestimmung der Ordnung von Punktgruppen jacobischer Varietäten spielt daher eine zentrale Rolle bei der Konstruktion kryptographisch geeigneter Kurven und es existieren eine Reihe von Algorithmen zur Bestimmung der Zetafunktion.

Für elliptische Kurven liefert der SEA-Algorithmus [Sch95] von René Schoof, Noam Elkies und A.O.L. Atkin einen l-adischen Algorithmus zur Bestimmung der Punktezahl. Dieser Ansatz wird als l-adisch bezeichnet, da er den Zähler der Zetafunktion modulo verschiedener Primzahlen l berechnet und anschließend den gesuchten Zähler mittels chinesischem Restsatz konstruiert. Eine Verallgemeinerung für beliebige abelsche Varietäten lieferte Jonathan Pila [Pil90], die jedoch nur von theoretischer Natur ist, denn sie benötigt eine konkrete Beschreibung der jacobischen Varietät, die man im Allgemeinen nicht hat.

Neben diesem l-adischen Ansatz existiert ein p-adischer Ansatz, den Takakazu Satoh [Sat00] als Erster für elliptische Kurven beschrieb. Dabei wird die Kurve auf eine p-adische Struktur geliftet und der Zähler der Zetafunktion modulo einer geeigneten p-Potenz berechnet.

Einen weiteren p-adischen Ansatz lieferte Kiran Kedlaya [Ked01], der die Anzahl der Punkte auf hyperelliptischen Kurven mit Hilfe einer p-adischen Kohomologie, der Monsky-Washnitzer-Kohomologie, berechnete.

Zum Abschluss sei noch Alan Lauders Ansatz [Lau04a][Lau04b] erwähnt, der mittels Deformation die Punkte einer Kurve zählt. Dabei startet man mit einer Kurve, deren Zetafunktion einfach zu bestimmen ist und deformiert diese Kurve durch Hinzunahme einer weiteren Variablen in die ursprünglichen Kurve. Anschließend wird berechnet, wie sich die Zetafunktion dabei verändert hat.

Damit sind die wichtigsten Techniken zur Bestimmung der Zetafunktion genannt, wobei zu allen Ansätzen eine Reihe von Verallgemeinerungen und Verbesserungen existieren.

Wir werden uns in dieser Arbeit zunächst mit Kedlayas Algorithmus beschäftigen und anschließend einen eigenen Algorithmus vorstellen, der die Eigenschaften des Cartier-Operators auf den holomorphen Differentialen einer Kurve ausnutzt.

Die Arbeit gliedert sich wie folgt:

Im ersten Kapitel werden wir alle benötigten Grundlagen behandeln. Nachdem wir die unverzweigten Erweiterungen der p-adischen Zahlen kennen gelernt haben, führen wir affine und projektive Varietäten ein und definieren damit den Begriff der Kurve. Anschließend beschreiben wir deren Verbindung zu Funktionenkörpern und definieren mit Hilfe von Differentialen die de Rham-Kohomologie. Zum Abschluss werfen wir noch einen Blick auf abelsche Varietäten und deren Eigenschaften.

Im zweiten Kapitel definieren wir die Zetafunktion einer algebraischen Kurve und beschreiben ihre wichtigsten Eigenschaften. Außerdem werden wir die grundlegende Idee zur Berechnung der Zetafunktion mit Hilfe der Frobenius-Abbildung kennenlernen.

Das dritte Kapitel dient der Charakterisierung der Monsky-Washnitzer-Kohomologie, wobei wir uns auf den Fall von Kurven beschränken werden.

Im vierten Kapitel stellen wir Kedlayas Algorithmus zur Berechnung der Zetafunktion hyperelliptischer Kurven vor. Nachdem wir die Monsky-Washnitzer-Kohomologie konstruiert haben, werden wir die induzierte Frobenius-Abbildung auf dieser Kohomologie betrachten und zeigen, wie sich damit die Zetafunktion berechnen lässt. Abschließend werden wir den implementierten Algorithmus beschreiben und einige berechnete Beispiele angeben.

Das fünfte Kapitel wird einen anderen Ansatz zur Berechnung der Zetafunktion verfolgen. Dieser basiert zunächst auf dem Cartier-Operator, der auf den holomorphen Differentialen einer Kurve operiert und mit dessen Darstellungsmatrix es möglich ist, den Zähler der Zetafunktion modulo p zu bestimmen. Darauf aufbauend stellen wir einen Algorithmus vor, der daraus die Zetafunktion vollständig bestimmt. Auch dieses Kapitel schließen wir mit einigen Berechnungsbeispielen ab und geben im sechsten Kapitel eine kurze Zusammenfassung mit Ausblick.

Kapitel 1

Mathematische Grundlagen

In diesem ersten Kapitel werden wir die mathematischen Grundlagen für den Rest der Arbeit vorstellen. Auf Beweise werden wir dabei im Allgemeinen verzichten.

1.1 Bewertungstheorie

Die Beweise zu den Aussagen dieses Abschnitts sind, falls nicht anders erwähnt, in [Lor90], [Lan02] und [Neu99] zu finden.

1.1.1 Bewertungen

Definition 1.1 (Diskrete Bewertung)**.** *Es sei R ein Integritätsring. Eine Abbildung $v : R \to \mathbb{Z} \cup \{\infty\}$ heißt* (nichtarchimedische) diskrete Bewertung*, falls sie folgende Eigenschaften besitzt:*

(i) $v(a) = \infty \Leftrightarrow a = 0$,

(ii) $v(a \cdot b) = v(a) + v(b)$ für alle $a, b \neq 0$,

(iii) $v(a + b) \geq \min\{v(a), v(b)\}$ für alle $a, b \in R$.

Die dritte Bedingung nennen wir *ultrametrische Ungleichung* und für den Fall, dass $v(a) \neq v(b)$ gilt, folgt sogar die Gleichheit $v(a + b) = \min\{v(a), v(b)\}$.

Beispielsweise definiert jede Primzahl $p \in \mathbb{Z}$ durch $v_p(a) := \max\{i \mid a \in p^i\mathbb{Z}\}$ und $v_p(0) := \infty$ eine diskrete Bewertung auf $\mathbb{Z}$, die sich durch $v_p(\frac{1}{a}) = -v_p(a)$ auf ganz $\mathbb{Q}$ fortsetzen lässt.

Jede Bewertung v eines Rings R lässt sich auf den Polynomring $R[x]$ durch $v(f) := \min\{v(a_i)\}$ für $f = \sum_i a_i x^i$ fortsetzen.

Ausgehend von einer diskreten Bewertung v auf R können wir durch

$$|a| := \begin{cases} p^{-v(a)} & \text{, falls } a \neq 0 \\ 0 & \text{, falls } a = 0 \end{cases} \text{, wobei } p \in \mathbb{R},\ p > 1$$

eine (nichtarchimedische) Betragsfunktion auf R definieren. Das heißt, eine Abbildung mit den Eigenschaften

(i) $|a| = 0 \Leftrightarrow a = 0$,

(ii) $|a \cdot b| = |a| \cdot |b|$,

(iii) $|a + b| \leq \max\{|a|, |b|\}$.

Definition 1.2 (Bewertungsring, Restklassenkörper)**.** *Es sei K ein Körper mit einem nichtarchimedischen Betrag $|\cdot|$ (beziehungsweise einer Bewertung v). Dann heißt*

$$\mathcal{R} := \{a \in K \mid |a| \leq 1\} = \{a \in K \mid v(a) \geq 0\}$$

der Bewertungsring von K. *Der Ring $\mathcal{R}$ ist lokal und besitzt das maximale Ideal*

$$\mathcal{M} := \{a \in K \mid |a| < 1\} = \{a \in K \mid v(a) \geq 0\}.$$

Der Körper $\mathcal{K} := \mathcal{R}/\mathcal{M}$ heißt Restklassenkörper von K.

Die Projektion $\pi : \mathcal{R} \to \mathcal{K}$, die jedem Element $a \in \mathcal{R}$ seine Restklasse $a + \mathcal{M} \in \mathcal{K}$ zuordnet nennen wir *Restklassenabbildung*.

1.1.2 p-adische Zahlen

Wie im vorherigen Abschnitt gesehen, liefert jede Primzahl p eine Bewertung v_p und damit einen Betrag $|\cdot|_p$ auf $\mathbb{Q}$. Jede Betragsfunktion wiederum induziert eine Metrik d_p und wir können den Körper $\mathbb{Q}$ bezüglich dieser Metrik vervollständigen.

Definition 1.3 (p-adische Zahlen)**.** *Die Vervollständigung des metrischen Raumes ($\mathbb{Q}$,d_p) wird mit $\mathbb{Q}_p$ bezeichnet. Seine Elemente heißen* p-adische Zahlen. *Der Bewertungsring von $\mathbb{Q}_p$ wird mit $\mathbb{Z}_p$ bezeichnet und heißt* Ring der ganzen p-adischen Zahlen.

Die Vervollständigung lässt sich konstruieren, indem wir Äquivalenzklassen von Cauchy-Folgen bilden. Dabei heißen zwei Cauchy-Folgen äquivalent, wenn die Folge ihrer punktweisen p-adischen Abstände eine Nullfolge ist. Auf diese Weise erhalten wir einen vollständigen metrischen Raum, der (durch die wohldefinierten komponentenweisen Verknüpfungen der Cauchy-Folgen-Äquivalenzklassen) außerdem ein Körper ist.

Neben der obigen analytischen Konstruktion lassen sich die ganzen p-adischen Zahlen $\mathbb{Z}_p$ auch algebraisch definieren als der projektive Limes $\varprojlim \mathbb{Z}/p^i\mathbb{Z}$ mit den Restklassenabbildungen modulo p^i. Der Körper $\mathbb{Q}_p$ ist dann der Quotientenkörper von $\mathbb{Z}_p$.

Für die ganzen p-adischen Zahlen gilt folgende Aussage:

Satz 1.4. *Ein Element $a \in \mathbb{Z}_p$ ist genau dann invertierbar, wenn es nicht in dem maximalen Ideal $\mathcal{M} = \{a \in \mathbb{Z}_p \mid v_p(a) > 0\}$ enthalten ist. Für den Restklassenkörper gilt $\mathbb{Z}_p/\mathcal{M} \cong \mathbb{F}_p$.*

Die oben erwähnte Restklassenabbildung auf Bewertungsringen induziert auch eine Restklassenabbildung auf dem Koordinatenring $\mathbb{Z}_p[x]$ und wir definieren ihre „Umkehrung“ folgendermaßen.

Definition 1.5 (Lift)**.** *Ein Polynom $F \in \mathbb{Z}_p[x]$ heißt* Lift von $f \in \mathbb{F}_p[x]$*, falls F den gleichen Grad wie f besitzt und $F \equiv f \mod p$ gilt. Das heißt, F wird unter der Restklassenabbildung auf f abgebildet.*

Aus der Definition ist klar, dass der Lift eines Polynoms nicht eindeutig ist.

1.1.3 Erweiterungen der p-adische Zahlen

Wir wollen nun eine Verbindung zwischen endlichen Erweiterungen endlicher Primkörper und den p-adischen Zahlen herstellen. Dazu bezeichne $\mathbb{K}$ eine endliche Körpererweiterung von $\mathbb{Q}_p$, welche durch die Nullstelle eines irreduziblen Polynoms $U \in \mathbb{Q}_q[v]$ über $\mathbb{Q}_p$ erzeugt wird. Für die Beträge von $\mathbb{K}$ gilt der folgende Satz:

Satz 1.6. *Der p-adische Betrag $|\cdot|_p$ auf $\mathbb{Q}_p$ lässt sich eindeutig auf jede endliche Körpererweiterung $\mathbb{K}/\mathbb{Q}_p$ fortsetzen.*

Für unsere Zwecke benötigen wir lediglich unverzweigte Erweiterungen, welche folgendermaßen charakterisiert werden können.

Definition 1.7 (Unverzweigte Erweiterung)**.** *Eine Körpererweiterung $\mathbb{K}/\mathbb{Q}_p$ vom Grad d heißt* unverzweigt*, falls der Grad des Restklassenkörpers von $\mathbb{K}$ über $\mathbb{F}_p$ gleich d ist. Eine solche Erweiterung bezeichnen wir mit $\mathbb{Q}_q$ und ihren Bewertungsring mit $\mathbb{Z}_q$ (wobei $q = p^d$ gilt). Ihre Elemente nennen wir* (ganze) q-adische Zahlen*.*

Der Restklassenkörper einer unverzweigten Erweiterung $\mathbb{K}/\mathbb{Q}_p$ vom Grad d ist also isomorph zu $\mathbb{F}_{p^d}$. Wir werden später ausschließlich solche unverzweigten Erweiterungen benötigen. Aufschluss darüber, wie wir eine solche unverzweigte Erweiterung konstruieren können, gibt der nächste Satz.

Satz 1.8. *Es sei $\mathbb{K}/\mathbb{Q}_p$ eine endliche Körpererweiterung, die durch eine Nullstelle des irreduziblen Polynoms $U \in \mathbb{Z}_p[v]$ erzeugt wird und $u \in \mathbb{F}_p[v]$ die Restklassenprojektion von U (das heißt $U \equiv u \mod p$). Die Erweiterung $\mathbb{K}/\mathbb{Q}_p$ ist genau dann unverzweigt, wenn $\deg U = \deg u$ gilt. Zwei unverzweigte Erweiterungen von $\mathbb{Q}_p$ sind genau dann isomorph, wenn ihre definierenden Polynome gleichen Grad haben.*

Bei gegebenem, endlichen Körper $\mathbb{F}_q$ (mit $q = p^d$) können wir also einen bewerteten Körper $\mathbb{Q}_q$ der Charakteristik 0 konstruieren, dessen Restklassenkörper isomorph zu $\mathbb{F}_q$

ist. Wir wählen dazu einen beliebigen Lift $U \in \mathbb{Z}_p[v]$ des Polynoms $u \in \mathbb{F}_p[v]$, welches $\mathbb{F}_q$ erzeugt und vom Grad d ist. Dieses U liefert uns nach Satz 1.8 eine unverzweigte Erweiterung von $\mathbb{Q}_q$, die bis auf Isomorphie eindeutig ist.

Die Elemente in $\mathbb{Q}_q$ können wir folgendermaßen darstellen:
Es sei R ein Repräsentantensystem von $\mathbb{F}_q$ in $\mathbb{Z}_q$. Dann lässt sich jedes Element $a \in \mathbb{Q}_q$ eindeutig schreiben als

$$a = \sum_{i=n}^{\infty} a_i p^i, \text{ wobei } a_i \in R, n \in \mathbb{Z}.$$

Für die Automorphismengruppe von $\mathbb{Q}_q/\mathbb{Q}_p$ haben wir folgende Aussage.

Satz 1.9. *Unverzweigte Erweiterungen von $\mathbb{Q}_p$ sind Galois-Erweiterungen. Die Galoisgruppe ist zyklisch und wird durch eine Abbildung Σ_p erzeugt, die reduziert in den Restklassenkörper gleich dem Frobenius-Automorphismus ist. Die Abbildung $\Sigma_p$wird auch* Frobenius-Substitution *auf $\mathbb{Q}_q$ genannt.*

Wir wollen noch auf die Verbindung von Polynomen über Bewertungsringen und deren Reduktionen eingehen.

Satz 1.10 (Hensels Lemma)**.** *Es sei R der Bewertungsring eines p-adisch vollständigen Körpers und $F \in R[t]$. Außerdem existiere eine Zerlegung von F im Restklassenring R/pR in zwei teilerfremde Polynome g und h, das heißt $F \equiv g \cdot h \mod p$. Dann gibt es Polynome G und H in $R[t]$ mit*

$$F = G \cdot H,$$

wobei $G \equiv g \mod p$, $H \equiv h \mod p$ und $\deg G = \deg g$ gilt.

Die Wichtigkeit dieses Lemmas zeigt die folgende Interpretation. Angenommen, wir haben ein Polynom $F \in R[t]$ und ein Element $a_0 \in R$ gegeben, so dass a_0 eine einfache Nullstelle des reduzierten Polynoms von F ist. Es gelte also

$$F(a_0) \equiv 0 \mod p \quad \text{und} \quad F'(a_0) \not\equiv 0 \mod p.$$

Dann besagt Hensels Lemma, dass es ein $a \in R$ gibt, so dass

$$F(a) = 0 \quad \text{und} \quad a \equiv a_0 \mod p.$$

gilt. Wie wir zu einem gegebenen a_0 eine beliebig genaue Approximation von a erhalten zeigt der nächste Satz.

Satz 1.11 (Newton-Iteration)**.** *Es sei R ein p-adisch vollständiger Ring, $F \in R[t]$ und $a_0 \in R$, so dass $F(a_0) \equiv 0 \mod p$ und $F'(a_0) \not\equiv 0 \mod p$ gilt ($F'(a_0)$ ist also eine Einheit in R). Für die rekursiv definierte Folge*

$$a_{n+1} := a_n - \frac{F(a_n)}{F'(a_n)}$$

gilt dann $a_{n+1} \equiv a_n \mod p^n$ und $F(a_{n+1}) \equiv 0 \mod p^{2^n}$. Das heißt, die p-adische Präzision der Approximation verdoppelt sich mit jedem Iterationsschritt.

Beweis. Zunächst stellen wir fest, dass aus $F'(a_0) \not\equiv 0 \mod p$ und $a_{n+1} \equiv a_n \mod p^n$ folgt, dass $F'(a_n)$ in R invertierbar ist und die Rekursionsvorschrift somit wohldefiniert ist. Wegen $F(a_n) \equiv 0 \mod p^n$ folgt unmittelbar $a_{n+1} \equiv a_n \mod p^n$ und damit der erste Teil der Aussage. Für den zweiten Teil entwickeln wir $F(x)$ als Taylor-Reihe erster Ordnung im Punkt a_n. Wir haben also eine Darstellung der Form

$$F(x) = F(a_n) + F'(a_n)(x - a_n) + (x - a_n)^2 r(x)$$

mit dem Restglied $(x - a_n)^2 r(x) \in R[x]$. Es folgt

$$\begin{aligned} F(a_{n+1}) &= F(a_n) + F'(a_n)(a_{n+1} - a_n) + (a_{n+1} - a_n)^2 r(a_{n+1}) \\ &= F(a_n) + F'(a_n)\left(a_n - \frac{F(a_n)}{F'(a_n)} - a_n\right) \\ &\quad + \left(a_n - \frac{F(a_n)}{F'(a_n)} - a_n\right)^2 (a_{n+1}) \\ &= F(a_n) - F(a_n) + \underbrace{\left(\frac{F(a_n)}{F'(a_n)}\right)^2 r(a_{n+1})}_{\equiv 0 \mod p^{2^n \cdot 2}} \\ &\equiv 0 \mod p^{2^{n+1}}, \end{aligned}$$

und damit die Behauptung. □

Mit Hilfe dieses Satzes sind wir in der Lage, die Frobenius-Substitution aus Satz 1.9 zu approximieren. Dabei fassen wir $\mathbb{Q}_q$ als Vektorraum über $\mathbb{Q}_p$ mit der Basis $1, v, \ldots, v^{d-1}$ auf, wobei v die Nullstelle des Polynoms $U \in \mathbb{Z}_p[v]$ ist, welches $\mathbb{Q}_q$ erzeugt. Wir suchen eine Abbildung $\Sigma_p : \mathbb{Z}_q \to \mathbb{Z}_q$, welche reduziert auf $\mathbb{F}_q$ dem Frobenius-Automorphismus $a \mapsto a^p$ entspricht und deren Fortsetzung auf den Quotientenkörper $\mathbb{Q}_q$ die Galoisgruppe $\mathrm{Gal}(\mathbb{Q}_q/\mathbb{Q}_p)$ erzeugt. Da Σ_p alle Elemente aus $\mathbb{Z}_p$ fixieren muss, sind wir lediglich an der Wirkung von Σ_p auf v interessiert. Das gesuchte Σ_p muss außerdem Nullstellen von U wieder auf Nullstellen abbilden, das heißt, wir fordern $U(\Sigma_p(v)) = 0$. Wenn wir $a_0 := v^p$ wählen, gilt $U(a_0) \equiv 0 \mod p$ und aufgrund der Vollkommenheit endlicher Körper $U'(a_0) \not\equiv 0 \mod p$. Die oben definierte Folge konvergiert also quadratisch gegen den gesuchten Wert $\Sigma_p(v)$ und wir können Σ_p auf ganz $\mathbb{Q}_q$ fortsetzen.

1.2 Algebraische Geometrie

In diesem Abschnitt bezeichnen wir mit $\mathbb{K}$ einen endlichen Körper der Charakteristik $p \neq 2$ und mit $\overline{\mathbb{K}}$ einen fixierten algebraischen Abschluss davon. Auch in diesem Abschnitt werden wir die meisten Aussagen unbewiesen lassen und verweisen auf [Har77], [Sil86] und [Sti93].

1.2.1 Affine Varietäten

Wir wollen zunächst den Begriff der Varietät definieren. Dazu bezeichne $\mathbb{A}^n(\overline{\mathbb{K}})$ den *n-dimensionalen affinen Raum* über dem algebraisch abgeschlossenen Körper $\overline{\mathbb{K}}$, also die Menge aller n-Tupel über $\overline{\mathbb{K}}$. Für den Rest des Kapitels und immer dann, wenn klar ist, von welchem Körper die Rede ist, schreiben wir vereinfacht $\mathbb{A}^n$. Ein Element $P \in \mathbb{A}^n$ heißt *Punkt* und wird als $\mathbb{K}$-*rational* bezeichnet, falls seine Koordinateneinträge aus $\mathbb{K}$ sind (was gleichbedeutend damit ist, dass seine Koordinateneinträge durch alle Elemente der Galoisgruppe $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ fixiert werden). Es sei I ein Ideal von $\overline{\mathbb{K}}[x_1, \ldots, x_n]$, dann heißt

$$V_I := \{P \in \mathbb{A}^n \mid f(P) = 0 \text{ für alle } f \in I\}$$

die *Nullstellenmenge von I*. Eine Teilmenge $V \subseteq \mathbb{A}^n$ heißt *algebraisch*, falls wir ihr ein Ideal $I(V) \subseteq \overline{\mathbb{K}}[x_1, \ldots, x_n]$ zuordnen können, so dass $V_{I(V)} = V$ gilt.

Mit Hilfe der algebraischen Mengen können wir eine Topologie auf dem affinen Raum $\mathbb{A}^n$ definieren, indem wir die Komplemente von algebraischen Mengen als offen definieren. Diese Topologie wird *Zariski-Topologie* genannt.

Definition 1.12 (Affine Varietät)**.** *Eine algebraische Menge V heißt* affine Varietät*, falls $I(V)$ ein Primideal in $\overline{\mathbb{K}}[x_1, \ldots, x_n]$ ist. Wird $I(V)$ durch Polynome aus $\mathbb{K}[x_1, \ldots, x_n]$ erzeugt, heißt V* (definiert) über $\mathbb{K}$ *und wir schreiben $V/\mathbb{K}$. Die Menge der $\mathbb{K}$-rationalen Punkte von V bezeichnen wir mit $V(\mathbb{K})$. Eine offene Teilmenge einer affinen Varietät heißt* quasiaffine Varietät.

Definition 1.13 (Koordinatenring, Funktionenkörper)**.** *Es sei V eine über $\mathbb{K}$ definierte affine Varietät. Dann heißt*

$$\mathbb{K}[V] := \mathbb{K}[x_1, \ldots, x_n]/I(V)$$

der Koordinatenring von $V/\mathbb{K}$*. Der Quotientenkörper von $\mathbb{K}[V]$ wird mit $\mathbb{K}(V)$ bezeichnet und heißt* Funktionenkörper von $V/\mathbb{K}$*. Der Körper $\mathbb{K}$ heißt Konstantenkörper von $\mathbb{K}(V)$ und wir nennen ihn* exakt*, falls er algebraisch abgeschlossen in $\mathbb{K}(V)$ ist.*

Da es sich bei $I(V)$ um ein Primideal handelt, ist $\mathbb{K}[V]$ ein Integritätsring und die obige Konstruktion des Funktionenkörpers wohldefiniert. Natürlich können wir eine Varietät $V/\mathbb{K}$ auch als Varietät über einem beliebigen Erweiterungskörper $\mathbb{L}$ von $\mathbb{K}$ auffassen. Wir schreiben dann $\mathbb{L}[V] := \mathbb{L} \cdot \mathbb{K}[V]$.

Eine wichtige Eigenschaft von Varietäten ist die Glattheit.

Definition 1.14 (Singularität)**.** *Es sei $V \subseteq \mathbb{A}^n$ eine affine Varietät über $\mathbb{K}$, $P \in V$ und $f_1, \ldots, f_m \in \mathbb{K}[x_1, \ldots, x_n]$ Erzeuger von $I(V)$. Dann heißt V* nichtsingulär (oder glatt) in $P \in \mathbb{A}^n$*, falls die $m \times n$ Matrix*

$$\left(\frac{\partial f_i}{\partial x_j}(P)\right)_{1 \le i \le m, 1 \le j \le n}$$

den Rang $n - \dim V$ hat. Falls V nichtsingulär in jedem Punkt ist, nennen wir V nichtsingulär (oder glatt).

1.2.2 Projektive Varietäten

Um projektive Varietäten zu definieren, benötigen wir zunächst den Begriff des projektiven Raumes über $\overline{\mathbb{K}}$. Dazu definieren wir auf $\mathbb{A}^n(\overline{\mathbb{K}})$ eine Äquivalenzrelation, indem wir zwei Punkte als äquivalent bezeichnen, falls sie sich durch die (koordinatenweise) Multiplikation mit einem von Null verschiedenen Element unterscheiden. Der *n-dimensionale projektive Raum (über $\overline{\mathbb{K}}$)* ist dann definiert als $\mathbb{A}^{n+1}(\overline{\mathbb{K}})\setminus\{0\}$ modulo dieser Äquivalenzrelation und wird mit $\mathbb{P}^n(\overline{\mathbb{K}})$ (oder, wie im affinen Fall, vereinfacht mit $\mathbb{P}^n$) bezeichnet. Ein projektiver Punkt P ist also eine Äquivalenzklasse $\{(\lambda x_0,\ldots,\lambda x_n) \mid \lambda \in \overline{\mathbb{K}}^\times\}$ und wir schreiben $P=[x_0,\ldots,x_n]$. Ein Punkt heißt $\mathbb{K}$-*rational*, falls seine Äquivalenzklasse einen Vertreter $[x_0,\ldots,x_n]$ besitzt, dessen Einträge aus $\mathbb{K}$ sind. Für jedes $0\le i\le n$ können wir $\mathbb{P}^n$ in einen *affinen Teil* $\mathbb{A}^n_i$ und einen *projektiven Teil* $\mathbb{P}^{n-1}_i$ zerlegen, wobei wir $\mathbb{A}^n_i$ und $\mathbb{P}^{n-1}_i$ erhalten, indem wir die i-te Koordinate 1 beziehungsweise 0 setzen.

Wir interessieren uns für projektive Nullstellenmengen von Polynomen. Wenn wir bedenken, dass die Darstellung projektiver Punkte aufgrund der Äquivalenzrelation nur bis auf Multiplikation eindeutig ist, ist es nur sinnvoll, homogene Polynome zu betrachten (wir nennen ein Polynom *homogen vom Grad d*, falls $f(\lambda x_1,\ldots,\lambda x_n)=\lambda^d f(x_1,\ldots,x_n)$ für alle Konstanten λ gilt). Für ein Ideal $I\subseteq\overline{\mathbb{K}}[x_0,\ldots,x_n]$, welches durch homogene Polynome erzeugt wird, definieren wir die algebraische Menge V_I wie im affinen Fall. Ebenso analog definieren wir eine *projektive Varietät* V als eine projektive algebraische Menge, deren zugehöriges Ideal $I(V)$ ein Primideal in $\overline{\mathbb{K}}[x_0,\ldots,x_n]$ ist und nennen diese *(definiert) über* $\mathbb{K}$, falls $I(V)$ Erzeuger aus $\mathbb{K}[x_0,\ldots,x_n]$ hat. Die Menge der $\mathbb{K}$-rationalen Punkte einer Varietät bezeichnen wir, wie im affinen Fall, mit $V(\mathbb{K})$.

Wie in obiger Bemerkung über die Zerlegung des projektiven Raumes, können wir auch jede projektive Varietät $V\subseteq\mathbb{P}^n$ für jedes i folgendermaßen zerlegen

$$V=(V\cap\mathbb{A}^n_i)\cup(V\cap\mathbb{P}^{n-1}_i).$$

Der Teil $V\cap\mathbb{A}^n_i$ ist eine affine Varietät und wird *affiner Teil von* V genannt. Wenn klar ist, von welchem i die Rede ist, nennen wir die Punkte $V\cap\mathbb{P}^{n-1}_i$ *Punkte im Unendlichen*. Offensichtlich wird jede projektive Varietät vollständig durch ihre affinen Teile überdeckt.

Den Funktionenkörper einer projektiven Varietät V definieren wir als den Funktionenkörper eines nichtleeren affinen Teils von V. Diese Definition ist sinnvoll, denn es lässt sich zeigen, dass alle Funktionenkörper nichtleerer, affiner Teile isomorph sind. Auch die Glattheit einer projektiven Varietät definieren wir über einen affinen Teil. V heißt *nichtsingulär (oder glatt) in* $P\in V$, falls $V\cap\mathbb{A}^n_i$ nichtsingulär in P ist für einen affinen Teil $\mathbb{A}^n_i$, der P enthält.

Andersherum können wir bei gegebener affiner Varietät $V\subseteq\mathbb{A}^n$ die $n+1$ Einbettungen

$$\phi_i : V\to\mathbb{P}^n,\quad (x_1,\ldots,x_n)\mapsto[x_1,\ldots,x_i,1,x_{i+1},\ldots,x_n] \tag{1.1}$$

betrachten. Der *projektive Abschluss* $\overline{V}$ *von* V ist dann definiert als die kleinste, projektive algebraische Menge, deren zugehöriges homogenes Ideal $I(\overline{V})\subseteq\overline{\mathbb{K}}[x_0,\ldots,x_n]$ auf

$\phi_i(V)$ verschwindet. Diese Konstruktion ist offensichtlich für jedes i isomorph, weshalb wir bei der Definition von $\overline{V}$ die Wahl von i nicht berücksichtigen.

Damit haben wir folgenden Zusammenhang zwischen affinen und projektiven Varietäten.

Satz 1.15. *(i) Es sei $V \subseteq \mathbb{A}^n$ eine affine Varietät. Dann ist $\overline{V}$ eine projektive Varietät und es gilt*

$$V = \overline{V} \cap \mathbb{A}_i^n, \text{ wobei } \overline{V} = \phi_i(V).$$

(ii) Es sei $V \subseteq \mathbb{P}^n$ eine projektive Varietät. Dann ist $V \cap \mathbb{A}_i^n$ eine affine Varietät und es gilt

$$V \cap \mathbb{A}_i^n = \emptyset \text{ oder } V = \overline{V \cap \mathbb{A}_i^n}.$$

Aufgrund der Definitionen ist klar, dass der projektive Abschluss (affine Teil) einer über $\mathbb{K}$ definierten affinen (projektiven) Varietät ebenfalls über $\mathbb{K}$ definiert ist.

1.2.3 Morphismen von Varietäten

Wir wollen nun geeignete Abbildungen zwischen Varietäten definieren.

Definition 1.16 (Reguläre Abbildung)**.** *Es sei $V \subseteq \mathbb{A}^n$ eine (quasi-) affine Varietät über $\mathbb{K}$. Eine Abbildung $f : V \to \overline{\mathbb{K}}$ heißt* regulär im Punkt $P \in V$*, falls eine offene Teilmenge $U \subseteq V$ mit $P \in U$ und Polynome $g, h \in \mathbb{K}[x_1, \ldots, x_n]$ existieren, so dass h nirgends auf U verschwindet und f auf U mit g/h übereinstimmt. Wir nennen f* regulär auf V*, falls f regulär in jedem Punkt $P \in V$ ist.*

Reguläre Funktionen auf projektiven Varietäten definieren wir ganz analog, indem wir die Polynome g und h als homogen und vom gleichen Grad voraussetzen.

Wenn wir $\overline{\mathbb{K}}$ mit $\mathbb{A}^1$ identifizieren, lässt sich zeigen, dass reguläre Funktionen stetig bezüglich der Zariski-Topologie sind.

Definition 1.17 (Morphismus)**.** *Es seien U, V (quasi-) affine oder projektive Varietäten. Eine stetige Abbildung $\varphi : U \to V$ heißt* Morphismus*, falls für jede offene Teilmenge $W \subseteq V$ und jede reguläre Funktion $f : W \to \overline{\mathbb{K}}$ die Verknüpfung $f \circ \varphi : \varphi^{-1}(V) \to \overline{\mathbb{K}}$ regulär ist.*
Ein Morphismus $\varphi : U \to V$ heißt Isomorphismus*, falls ein Morphismus $\psi : V \to U$ existiert, so dass die Kompositionen $\varphi \circ \psi$ und $\psi \circ \varphi$ die Identitäten auf U beziehungsweise V sind.*

Ein nicht konstanter Morphismus $\varphi : U \to V$ induziert einen Körperhomomorphismus $\varphi^* : \mathbb{K}(V) \to \mathbb{K}(U)$ zwischen den entsprechenden Funktionenkörpern durch

$$\varphi^*(f) := f \circ \varphi. \tag{1.2}$$

Das Bild von φ^* ist ein Teilkörper von $\mathbb{K}(U)$ und $\mathbb{K}(U)/\varphi^*\mathbb{K}(V)$ ist eine endliche Körpererweiterung.

Definition 1.18 (Grad eines Morphismus)**.** *Es seien U und V über $\mathbb{K}$ definierte Varietäten und $\varphi : U \to V$ ein nicht konstanter Morphismus. Dann ist der* Grad von φ *definiert als*

$$\deg \varphi := [\mathbb{K}(V) : \varphi^*\mathbb{K}(U)].$$

Analog definieren wir den Separabilitätsgrad $\deg_s \varphi$ *und nennen φ separabel, falls* $\deg_s \varphi = \deg \varphi$ *gilt.*

Ein Beispiel für einen Morphismus ist die Frobenius-Abbildung.

Beispiel und Definition 1.19 (q-Frobenius)**.** *Es sei V eine projektive Varietät über dem endlichen Körper $\mathbb{F}_q$. Die Abbildung*

$$\Phi : V \longrightarrow V, \quad [x_0, \ldots, x_n] \mapsto [x_0^q, \ldots, x_n^q]$$

ist ein Morphismus vom Grad q und wird q-Frobenius *genannt. Der q-Frobenius kommutiert mit allen Morphismen von Varietäten über $\mathbb{F}_q$ und lässt sich analog auch für affine Varietäten definieren.*

Ein Beispiel für einen Isomorphismus, auf den wir später zurückgreifen werden, liefert das folgende Lemma.

Lemma 1.20. *Es seien eine affine Varietät V und eine Hyperebene H über $\mathbb{K}$ durch $f(x_1, \ldots, x_n) = 0$ beziehungsweise $k(x_1, \ldots, x_n) = 0$ gegeben. Dann ist die offene Menge $V \setminus H$ isomorph zur affinen Varietät $V' \subseteq \mathbb{A}^{n+1}$, die durch $f(x_1, \ldots, x_n) = 0$ und $x_{n+1}k(x_1, \ldots, x_n) = 1$ definiert ist. Für den Koordinatenring gilt also*

$$\mathbb{K}[V'] = \mathbb{K}[x_1, \ldots, x_n, x_{n+1}]/(f(x_1, \ldots, x_n), x_{n+1}k(x_1, \ldots, x_n) - 1).$$

Beweis. Wir definieren zwei Abbildungen durch

$$\begin{aligned} \varphi : V' \to V \setminus H, &\quad (a_1, \ldots, a_{n+1}) \mapsto (a_1, \ldots, a_n) \text{ bzw.} \\ \varphi^{-1} : V \setminus H \to V', &\quad (a_1, \ldots, a_n) \mapsto (a_1, \ldots, a_n, \frac{1}{k(a_1, \ldots, a_n)}). \end{aligned}$$

Die Wohldefiniertheit und die Tatsache, dass es sich bei den gegebenen Abbildungen um Morphismen handelt, folgt durch einfaches nachrechnen. Bleibt noch zu zeigen, dass sowohl $\varphi \circ \varphi^{-1}$, als auch $\varphi^{-1} \circ \varphi$ Identitäten sind. Bei $\varphi \circ \varphi^{-1}$ ist das offensichtlich. Für $\varphi^{-1} \circ \varphi$ beachten wir, dass alle $(a_1, \ldots, a_{n+1})$ in V' die Gleichung $a_{n+1}k(a_1, \ldots, a_n) = 1$ erfüllen und damit

$$\begin{aligned} (\varphi^{-1} \circ \varphi)(a_1, \ldots, a_{n+1}) &= \varphi^{-1}(a_1, \ldots, a_n) \\ &= (a_1, \ldots, a_n, \frac{1}{k(a_1, \ldots, a_n)}) \\ &= (a_1, \ldots, a_{n+1}) \end{aligned}$$

gilt. □

Beispiel 1.21. *Es seien eine affine Varietät C über $\mathbb{K}$ durch $y^2 - h(x) = 0$ und die Hyperebene H durch $y = 0$ gegeben. Dann gilt für den Koordinatenring von $C' := C \setminus H = \{(x, y) \in C \mid y \neq 0\}$ nach Lemma 1.20*

$$\mathbb{K}[C'] = \mathbb{K}[x, y, z]/(y^2 - h(x), zy - 1) = \mathbb{K}[x, y, y^{-1}]/(y^2 - h(x)).$$

Für die gerade beschriebene Varietät C wollen wir noch einen weiteren Morphismus angeben.

Beispiel und Definition 1.22 (Hyperelliptische Involution)**.** *Es sei die affine Varietät C durch $y^2 - h(x) = 0$ gegeben. Dann heißt der Morphismus*

$$\iota : C \longrightarrow C, \quad (x, y) \mapsto (x, -y)$$

hyperelliptische Involution *und es gilt $\iota \circ \iota = id_C$. Die Fixpunkte dieser Abbildung sind gerade die Punkte, die in Bsp 1.21 aus der Varietät C herausgenommen wurden und heißen* Weierstraßpunkte von C.

Wie wir später sehen werden, handelt es sich bei der Varietät C aus den Beispielen 1.21 und 1.22 um den affinen Teil einer *hyperelliptischen Kurve* (siehe Definition 1.35).

1.2.4 Algebraische Kurven

Mit den Begriffen der vorherigen Abschnitte sind wir nun in der Lage, die Objekte unseres eigentlichen Interesses zu definieren. Zuvor benötigen wir lediglich noch den Begriff der Dimension.

Definition 1.23 (Dimension)**.** *Es sei $V \subseteq \mathbb{A}^n$ eine affine Varietät über $\mathbb{K}$. Die* Dimension von V *ist definiert als der Transzendenzgrad des zugehörgien Funktionenkörpers $\mathbb{K}(V)$ über $\mathbb{K}$. Die Dimension einer projektiven Varietät $\emptyset \neq V \subseteq \mathbb{P}^n$ definieren wir als den Transzendenzgrad eines nichtleeren affinen Teils $V \cap \mathbb{A}_i^n$ von V.*

Definition 1.24 (Kurve)**.** *Eine projektive Varietät der Dimension* 1 *heißt* Kurve.

Definition 1.25 (lokaler Ring)**.** *Der* lokale Ring *einer affinen Varietät $V/\mathbb{K}$ an einem Punkt $P \in V$ ist definiert als*

$$\mathcal{O}_P := \{h \in \mathbb{K}(V) \mid h = \frac{f}{g} \text{ mit } f, g \in \mathbb{K}[V] \text{ und } g(P) \neq 0\}.$$

Für eine projektive Varietät $V \subseteq \mathbb{P}^n$ ist der lokale Ring an einem Punkt P definiert als der lokale Ring von $V \cap \mathbb{A}_i^n$ mit $P \in \mathbb{A}_i^n$ und wird ebenfalls mit $\mathcal{O}_P$ bezeichnet.

Die Ringe $\mathcal{O}_P$ entsprechen den Lokalisierungen der Koordinatenringe $\mathbb{K}[V]$ an den maximalen Idealen $\mathcal{M}_P := \{f \in \mathbb{K}[V] \mid f(P) = 0\}$.

Satz 1.26. *Es sei $C/\mathbb{K}$ eine Kurve und $P \in C$ ein nichtsingulärer Punkt. Dann ist $\mathcal{O}_P$ ein diskreter Bewertungsring.*

Die (nichtarchimedische) Bewertung auf $\mathcal{O}_P$ ist gegeben durch

$$\begin{aligned} &\mathrm{ord}_P : \mathcal{O}_P \to \mathbb{Z} \cup \{\infty\} \\ &\mathrm{ord}_P(f) := \max\{n \in \mathbb{Z} \cup \{\infty\} \mid f \in \mathcal{M}_P^n\} \end{aligned}$$

und kann auf den ganzen Quotientenkörper $\mathbb{K}(C)$ von $\mathcal{O}_P$ durch

$$\mathrm{ord}_P(f/g) := \mathrm{ord}_P(f) - \mathrm{ord}_P(g)$$

fortgesetzt werden.

Wir sagen, eine Funktion $f \in \mathbb{K}(C)$ hat einen *Pol in P*, falls $\mathrm{ord}_P(f) < 0$ gilt und f hat eine *Nullstelle in P*, falls $\mathrm{ord}_P(f) > 0$. Wenn $\mathrm{ord}_P(f) \geq 0$ gilt, ist f regulär in P und wir können $f(P)$ auswerten. Der lokale Ring $\mathcal{O}_P$ besteht also gerade aus allen Elementen des Funktionenkörpers, die in P keinen Pol besitzen. Eine Funktion $t \in \mathbb{K}(C)$ mit $\mathrm{ord}_P(t) = 1$ heißt *Uniformisierende in P* und erzeugt das maximale Ideal $\mathcal{M}_P$.

Satz 1.26 liefert zu jedem nichtsingulären Punkt einer Kurve einen diskreten Bewertungsring. Das eindeutige, maximale Ideal eines solchen Bewertungsringes heißt *Stelle von $\mathbb{K}(C)$* und wir bezeichnen die Menge aller Stellen mit $\mathcal{P}l(\mathbb{K}(C))$. Weiterhin bezeichnen wir den zu einer Stelle $\mathcal{M}_P$ gehörigen Bewertungsring mit $\mathcal{O}_P$ und den Restklassenkörper $\mathcal{O}_P/\mathcal{M}_P$ mit $\mathcal{K}_P$. Im Folgenden werden wir einen Punkt P mit der assoziierten Stelle $\mathcal{M}_P$ identifizieren.

Zwei Punkte $P_1, P_2 \in C$ liefern genau dann den gleichen Bewertungsring in $\mathbb{K}(C)$ (und damit das gleiche maximale Ideal), falls ein $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ mit $\sigma(P_1) = P_2$ existiert. Die Galoisgruppe wirkt hierbei auf den Koordinateneinträgen der Punkte. Die Stellen von $\mathbb{K}(C)$ stehen also in Bijektion zu den Orbits der Galoisgruppe $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ auf den Punkten von C. Die Stellen von $\overline{\mathbb{K}}(C)$ sind demnach bijektiv zu den Punkten von C. Der Grad einer Stelle $P \in \mathcal{P}l(\mathbb{K}(C))$ ist definiert als

$$\deg P := \#\{Q \in C \mid \mathcal{M}_Q = P\} = [\mathbb{K}(C)_P : \mathbb{K}].$$

Zu einer (möglicherweise singulären) Kurve C existiert immer eine nichtsinguläre Kurve $\widetilde{C}$, so dass die beiden Funktionenkörper $\overline{\mathbb{K}}(C)$ und $\overline{\mathbb{K}}(\widetilde{C})$ isomorph sind (siehe [Har77, I.6]). Wir nennen $\widetilde{C}$ ein *nichtsinguläres Modell von C* und können die Punkte von $\widetilde{C}$ mit den Stellen von $\overline{\mathbb{K}}(C)$ identifizieren. Auf die Konstruktion solcher Modelle wollen wir nicht weiter eingehen und verweisen auf [Har77, I.6] und [Lue03].

In diesem Zusammenhang wollen wir noch einmal die hyperelliptische Kurve aus den Beispielen 1.21 und 1.22 aufgreifen, die durch $f(x, y) = y^2 - h(x) = 0$ mit $h \in \mathbb{K}[x]$ vom Grad n gegeben ist. Der projektive Abschluss $\overline{C}$ wird dann durch die homogene Gleichung $f^{hom}(x, y, z) = y^2 z^{n-2} - z^n h(\frac{x}{z})$ beschrieben und enthält genau einen Punkt

im Unendlichen, nämlich $[0,1,0]$. Der einzige affine Teil, der diesen Punkt enthält ist $\overline{C} \cap \mathbb{A}^3_y$ und ist durch $f_y(x,z) := z^{n-2} - z^n h(\frac{x}{z}) = 0$ definiert. Für $n > 3$ gilt allerdings

$$\frac{\partial f_y}{\partial x}(0,0) = 0 \text{ und } \frac{\partial f_y}{\partial z}(0,0) = 0,$$

das heißt, die Kurve $\overline{C}$ ist nach Definition 1.14 singulär in $[0,1,0]$. Wie erwähnt können wir aber zu einer geeigneten, glatten Kurve übergehen, die einen isomorphen Funktionenkörper erzeugt. Da wir hauptsächlich in Koordinatenringen rechnen werden, sind wir nicht daran interessiert, wie dieses nichtsinguläre Modell aussieht, sondern beschränken uns auf die Aussage, dass ein solches existiert. Wir wollen lediglich erwähnen, dass das nichtsinguläre Modell einer ebenen Kurve im Allgemeinen nicht eben ist.

Wenn wir im Folgenden eine Kurve durch einen nichtsingulären Teil definieren, meinen wir immer ein nichtsinguläre Modell des projektiven Abschlusses.

1.2.5 Stellen und Divisoren

Wir wollen nun mit Hilfe von Kurven eine algebraische Struktur definieren. Dazu benötigen wir Divisoren, die wir aus den Stellen beziehungsweise den Punkten einer Kurve konstruieren.

Definition 1.27 (Divisorengruppe)**.** *Die freie abelsche Gruppe, die durch die Punkte einer glatten Kurve C erzeugt wird, heißt* Divisorengruppe von C *und wird mit $\mathcal{D}(C)$ bezeichnet. Ein Divisor $D \in \mathcal{D}(C)$ ist also eine formale Summe $\sum_{P \in C} n_P P$ mit $n_P \in \mathbb{Z}$ und $n_P \neq 0$ für nur endlich viele $P \in C$.*

Der *Grad* eines Divisors $D = \sum_{P \in C} n_P P$ ist definiert als $\deg(D) := \sum_{P \in C} n_P$ und der *Träger* als $\operatorname{supp}(D) := \{P \mid n_P \neq 0\}$. Ein Divisor heißt *effektiv*, falls $n_P \geq 0$ für alle P. Somit können wir eine Halbordnung auf $\mathcal{D}(C)$ definieren durch

$$D \leq D' :\Longleftrightarrow D' - D \text{ ist effektiv.}$$

Die Divisoren vom Grad Null bilden eine Untergruppe, welche wir mit $\mathcal{D}^0(C)$ bezeichnen. Analog schreiben wir $\mathcal{D}^n(C)$ für die Menge der Divisoren vom Grad n.

Wenn C über dem Körper $\mathbb{K}$ definiert ist, operiert die Galoisgruppe $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ auf den Punkten von C und damit auch auf den Divisoren durch $D^\sigma = \sum_{P \in C} n_P P^\sigma$ (σ bezeichnet dabei ein Element der Galoisgruppe und P^σ die koordinatenweise Anwendung von σ auf P). Wir nennen einen Divisor $\mathbb{K}$-*rational*, falls $D^\sigma = D$ für alle $\sigma \in \mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$ gilt. Für einen $\mathbb{K}$-rationalen Divisor $D = \sum_{P \in C} n_P P$ gilt also $n_{P_i} = n_{P_j}$ für alle P_i, P_j aus demselben $\mathrm{Gal}(\overline{\mathbb{K}}/\mathbb{K})$-Orbit. Aufgrund der Bijektion zwischen den Galois-Orbits und den Stellen von $\mathbb{K}(C)$, können wir jeden $\mathbb{K}$-rationalen Divisor als Summe von Stellen von $\mathbb{K}(C)$ schreiben. Wir sprechen deshalb auch von den Divisoren des Funktionenkörpers $\mathbb{K}(C)$ und bezeichnen diese als $\mathcal{D}(\mathbb{K}(C))$.

Ein $\mathbb{K}$-rationaler Divisor D heißt *Primdivisor*, falls er effektiv ist und für jeden $\mathbb{K}$-rationalen, effektiven Divisor D' mit $D' \leq D$ entweder $D' = 0$ oder $D' = D$ gilt. Ein Primdivisor $D \in \mathcal{D}(\mathbb{K}(C))$ entspricht also einer Stelle $P \in \mathcal{P}l(\mathbb{K}(C))$.

Der nächste Satz stellt eine Verbindung zwischen Elementen eines Funktionenkörpers und Divisoren her.

Satz 1.28. *Es sei $f \in \mathbb{K}(C) \setminus \{0\}$. Dann gibt es nur endlich viele Punkte $P \in C$ mit $\mathrm{ord}_P(f) \neq 0$ und der Divisor*

$$(f) := \sum_{P \in C} \mathrm{ord}_P(f) P \in \mathcal{D}(\mathbb{K}(C))$$

ist vom Grad Null.

Divisoren der Form (f) heißen *Hauptdivisoren* und werden häufig als Differenz der beiden effektiven Divisoren $(f)_0$ und $(f)_\infty$ geschrieben. Wir nennen $(f)_0$ und $(f)_\infty$ den *Nulldivisor* beziehungsweise den *Poldivisor von f*.

Beispiel 1.29. *Es sei ein affiner Teil einer Kurve über einem Körper $\mathbb{K}$ der Charakteristik Null oder $p \neq 2$ durch $y^2 = h(x)$ definiert, wobei h im algebraischen Abschluss von $\mathbb{K}$ nur einfache Nullstellen $\alpha_1, \ldots, \alpha_n$ besitze. Eine solche Kurve besitzt genau einen Punkt im Unendlichen, den wir mit P_∞ bezeichnen.*

Wir wollen den Divisor eines Polynoms $f \in \mathbb{K}[x]$ vom Grad m mit den (nicht unbedingt paarweise verschiedenen) Nullstellen $\beta_1, \ldots, \beta_m \in \overline{\mathbb{K}}$ bestimmen. Im Nulldivisor $(f)_0$ können nur Punkte der Kurve auftreten, in denen f verschwindet, also Punkte, deren erste Koordinate eine Nullstelle von f ist. Für die zweite Koordinate bleiben dann genau die zwei Möglichkeiten $+\sqrt{h(\beta_i)}$ und $-\sqrt{h(\beta_i)}$ $(1 \leq i \leq m)$. Es lässt sich zeigen, dass die Ordnung von f in diesen Punkten gleich der algebraischen Vielfachheit der Nullstelle ist und es folgt $(f)_0 = \sum_{i=1}^{m} \left(\left(\beta_i, +\sqrt{h(\beta_i)} \right) + \left(\beta_i, -\sqrt{h(\beta_i)} \right) \right)$. Aufgrund der Gradaussage für Hauptdivisoren aus Satz 1.28 muss auch der Poldivisor von f den Grad $2m$ besitzen. Der einzige in Frage kommende Punkt für eine Polstelle ist P_∞ und es folgt

$$(f) = \sum_{i=1}^{m} \left(\left(\beta_i, +\sqrt{h(\beta_i)} \right) + \left(\beta_i, -\sqrt{h(\beta_i)} \right) \right) - 2mP_\infty.$$

Für den Divisor von $x - a$ mit $a \in \mathbb{K}$ folgt daraus unmittelbar

$$(x - a) = \left(a, +\sqrt{h(a)} \right) + \left(a, -\sqrt{h(a)} \right) - 2P_\infty.$$

Das heißt, $(x - a)$ hat für $a = \alpha_i$ eine Nullstelle der Ordnung zwei in $(a, 0)$ und überall sonst nur einfache Nullstellen. Mit der gleichen Argumentation erhalten wir

$$(y) = (\alpha_1, 0) + \ldots + (\alpha_n, 0) - nP_\infty.$$

Die Menge der Hauptdivisoren von $\mathbb{K}(C)$ wird mit $\mathcal{P}(\mathbb{K}(C))$ bezeichnet und bildet eine Untergruppe von $\mathcal{D}(\mathbb{K}(C))$, denn es gilt $(f) + (g) = (f \cdot g)$.

Definition 1.30 (Klassengruppe)**.** *Die Faktorgruppe*

$$\mathcal{C}l(\mathbb{K}(C)) := \mathcal{D}(\mathbb{K}(C))/\mathcal{P}(\mathbb{K}(C))$$

heißt (Divisoren-)klassengruppe *von* $\mathbb{K}(C)$*. Die Divisorenklassen vom Grad Null bilden eine Untergruppe und werden mit*

$$\mathcal{C}l^0(\mathbb{K}(C)) := \mathcal{D}^0(\mathbb{K}(C))/\mathcal{P}(\mathbb{K}(C))$$

bezeichnet. Für die Menge der Divisorklassen vom Grad $d \in \mathbb{N}$ *schreiben wir* $\mathcal{C}l^d(\mathbb{K}(C))$*.*

Satz 1.31. *Die Gruppe* $\mathcal{C}l^0(\mathbb{K}(C))$ *ist endlich. Ihre Ordnung heißt* Klassenzahl von $\mathbb{K}(C)$ *und wird mit* $h(\mathbb{K}(C))$ *bezeichnet. Für die Struktur der Klassengruppe gilt*

$$\mathcal{C}l(\mathbb{K}(C)) \cong \mathbb{Z} \oplus \mathcal{C}l^0(\mathbb{K}(C)).$$

1.2.6 Klassifizierung von Kurven

Die wichtigste Invariante einer Kurve ist ihr Geschlecht. Um das zu definieren, benötigen wir noch einen weiteren Begriff.

Definition 1.32 (Riemann-Roch-Raum)**.** *Für einen Divisor* $D \in \mathcal{D}(\mathbb{K}(C))$ *heißt die Menge*

$$\mathcal{L}(D) := \{x \in \mathbb{K}(C) \mid (x) \geq -D\} \cup \{0\}$$

Riemann-Roch-Raum von D*.*

Die Riemann-Roch-Räume sind endlichdimensionale Vektorräume über $\mathbb{K}$ und wir nennen die Dimension $\dim D := \dim \mathcal{L}(D)$ die *Dimension von* D*.*

Definition 1.33 (Geschlecht)**.** *Das* Geschlecht einer Kurve $C/\mathbb{K}$ *ist definiert als die ganze, nichtnegative Zahl*

$$g := \max\{\deg D - \dim D + 1 \mid D \in \mathcal{D}(\mathbb{K}(C))\}.$$

Wir haben Kurven in der Regel durch einen affinen Teil gegeben. Deshalb werden wir die nachfolgenden Klassen von Kurven auch über einen solchen definieren. Ein anderer affiner Teil derselben Kurve kann dabei eine vollkommen andere Form besitzen. Wie bereits erwähnt, meinen wir mit der Kurve C, die wir einem nichtsingulären, affinen Teil zuordnen, ein nichtsinguläres Modell des projektiven Abschlusses.

Definition 1.34 (Superelliptische Kurve)**.** *Es sei der affine Teil einer Kurve C über einem vollkommenen Körper $\mathbb{K}$ der Charakteristik $p > 2$ durch*

$$y^a = h(x)$$

gegeben, wobei $h \in \mathbb{K}[x]$ normiert und quadratfrei ist (das heißt, h ist teilerfremd zu seiner Ableitung h') und außerdem $gcd(a, b) = gcd(a, p) = 1$ mit $b := \deg h$ gilt. Dann heißt C superelliptische Kurve.

Mit dieser Definition ist C nichtsingulär und besitzt genau einen Punkt im Unendlichen. Das Geschlecht einer solchen Kurve lässt sich durch $g = \frac{(a-1)(b-1)}{2}$ angeben.

Definition 1.35 (Hyperelliptische Kurve)**.** *Eine superelliptische Kurve wie in Definition 1.34 heißt* hyperelliptisch*, falls $a = 2$ gilt.*

Das Geschlecht einer hyperelliptischen Kurve lässt sich aus der Gleichung $2g + 1 = \deg h$ ablesen. Für eine allgemeinere Definition von hyperelliptischen Kurven (die auch den Fall $\operatorname{char}\mathbb{K} = 2$ beinhaltet) verweisen wir auf [Sti93, VI.2.]. Eine hyperelliptische Kurve vom Geschlecht 1 heißt *elliptische Kurve*.

1.2.7 Differentiale

Für die späteren Berechnungen benötigen wir den Begriff des Differentials.

Definition 1.36 (Differentialmodul)**.** *Es sei R ein kommutativer Ring mit Eins und A eine R-Algebra. Der* universelle Differentialmodul $\Omega_{A/R}$ *ist definiert als der A-Modul, der durch die Symbole df mit $f \in A$ erzeugt wird und den folgenden Relationen genügt:*

(i) $d(f + g) = df + dg$ *für alle* $f, g \in A$,

(ii) $d(fg) = fdg + gdf$ *für alle* $f, g \in A$,

(iii) $da = 0$ *für alle* $a \in R$.

Der universelle Differentialmodul existiert und ist bis auf Isomorphie eindeutig. Wir können ihn konstruieren, indem wir aus dem freien A-Modul, der durch die Symbole df mit $f \in A$ erzeugt wird, den durch

$$\{d(f + g) - df - dg, d(fg) - fdg - gdf, dr \mid f, g \in A, r \in R\}$$

erzeugten Untermodul herausfaktorisieren.

Jeder R-Algebra-Endomorphismus φ von A induziert eine R-lineare Abbildung φ^* auf dem Differentialmodul $\Omega_{A/R}$ durch

$$fdg \mapsto \varphi(f)d(\varphi(g)). \tag{1.3}$$

Von dieser induzierten Abbildung werden wir später noch Gebrauch machen.

Im Fall einer Kurve $C/\mathbb{K}$ schreiben wir für den (universellen) Differentialmodul $\Omega_{\mathbb{K}(C)/\mathbb{K}}$ auch $\Omega(\mathbb{K}(C))$. Seine Elemente bilden einen eindimensionalen Vektorraum über $\mathbb{K}(C)$. Für jede Uniformisierende $t \in \mathbb{K}(C)$ einer Stelle P von $\mathbb{K}(C)$ und jedes $\omega \in \Omega(\mathbb{K}(C))$ existiert ein eindeutiges $f \in \mathbb{K}(C)$ mit $\omega = f\,dt$. Jede Uniformisierende t liefert also eine Basis dt von $\Omega(\mathbb{K}(C))$. Wir schreiben auch $f = \omega/dt$. Die Zahl $\operatorname{ord}_P(\omega) := \operatorname{ord}(\omega/dt)$ ist unabhängig von der Wahl der Uniformisierenden t und heißt *Ordnung von ω in P*.

Weiterhin gilt $\operatorname{ord}_P(\omega) = 0$ für fast alle $P \in C$, wir können also jedem Differential $\omega \in \Omega(\mathbb{K}(C))$ einen Divisor $(\omega) := \sum_{P \in C} \operatorname{ord}_P(\omega) P \in \mathcal{D}(\mathbb{K}(C))$ zuordnen. Differentiale der Form (ω) heißen *exakt*. Ein Differential ω heißt *holomorph*, wenn der Divisor (ω) effektiv ist. Die Menge aller holomorphen Differentiale wird mit $\Omega^0(\mathbb{K}(C))$ bezeichnet und bildet einen g-dimensionalen Vektorraum über $\mathbb{K}$ (wobei g das Geschlecht der Kurve ist).

Um Divisoren von Differentialen zu untersuchen ist der nachstehende Satz sehr hilfreich.

Satz 1.37. *Es sei $C/\mathbb{K}$ eine glatte Kurve, P eine fixierte Stelle von $\mathbb{K}(C)$ und $f, g \in \mathbb{K}(C)$.*

(i) Hat f in P keinen Pol, so gilt $\operatorname{ord}_P(df) \geq 0$.

(ii) Es gelte $\operatorname{ord}_P(g) \geq 1$. *Für* $\operatorname{char} \mathbb{K} = 0$ *oder* $\operatorname{char} \mathbb{K} \nmid \operatorname{ord}_P(g)$ *gilt*

$$\operatorname{ord}_P(f\,dg) = \operatorname{ord}_P(f) + \operatorname{ord}_P(g) - 1.$$

Beweis. Siehe [Sil86, Proposition 4.3. (b) und (d)]. □

Außerdem werden wir später die folgende Aussage benötigen.

Satz 1.38. *Es sei C eine glatte Kurve über einem Körper $\mathbb{K}$ der Charakteristik Null. Dann kann ein exaktes Differential $df \in \Omega(\mathbb{K}(C))$ keine einfache Polstelle besitzen.*

Beweis. Wir wählen eine beliebige Stelle P mit Uniformisierender t. Dann gilt $f = \widetilde{f} t^n$ mit $\operatorname{ord}_P(\widetilde{f}) = 0$ und $n := \operatorname{ord}_P(f)$. Wegen $\operatorname{ord}_P(\widetilde{f}) = 0$ gilt auch $\operatorname{ord}_P(d\widetilde{f}) \geq 0$ und wir können $d\widetilde{f}$ schreiben als $u\,dt = \widetilde{u} t^m dt$ mit $m := \operatorname{ord}_P(u) \geq 0$ und $\operatorname{ord}_P(\widetilde{u}) = 0$. Daraus

ergibt sich mit Satz 1.37

$$\begin{aligned}
\mathrm{ord}_P(df) &= \mathrm{ord}_P\left(d(\widetilde{f}t^n)\right) \\
&= \mathrm{ord}_P\left(\widetilde{f}nt^{n-1}dt + t^n d\widetilde{f}\right) \\
&= \mathrm{ord}_P\left((\widetilde{f}nt^{n-1} + t^n u)dt\right) \\
&= \mathrm{ord}_P\left((\widetilde{f}nt^{n-1} + \widetilde{u}t^{n+m})dt\right) \\
&= \mathrm{ord}_P\left(\widetilde{f}nt^{n-1} + \widetilde{u}t^{n+m}\right) + \mathrm{ord}_P(t) - 1 \\
&= \begin{cases} n-1, \text{ falls } n \neq 0 \\ n+m, \text{ falls } n = 0 \end{cases}
\end{aligned}$$

Diese Werte sind für alle $n \in \mathbb{Z}$ ungleich -1 und es folgt die Behauptung. □

Beispiel 1.39. *Wir betrachten die gleiche Situation wie in Beispiel 1.29 und wollen den Divisor (dx) bestimmen. Da die einzigen Polstelle von x bei P_∞ sind, kann auch dx nach Satz 1.37(i) nur dort einen Pol besitzen. Mit der Identität $dx = -x^2 d(x^{-1})$ und Satz 1.37(ii) folgt*

$$\begin{aligned}
\mathrm{ord}_\infty(dx) &= \mathrm{ord}_\infty(-x^2 d(x^{-1})) \\
&= \mathrm{ord}_\infty(-x^2) + \mathrm{ord}_\infty(x^{-1}) - 1 \\
&= 2\mathrm{ord}_\infty(x) - \mathrm{ord}_\infty(x) - 1 \\
&= -3.
\end{aligned}$$

Kommen wir nun zu den Nullstellen von dx. Es gilt $dx = d(x-a)$ für alle $a \in \mathbb{K}$ und damit mit den Ergebnissen aus Beispiel 1.29 und Satz 1.37(ii)

$$\begin{aligned}
\mathrm{ord}_{\left(a,\pm\sqrt{h(a)}\right)}(dx) &= \mathrm{ord}_{\left(a,\pm\sqrt{h(a)}\right)}(d(x-a)) \\
&= \mathrm{ord}_{\left(a,\pm\sqrt{h(a)}\right)}(x-a) - 1 \\
&= \begin{cases} 0, \textit{ falls } h(a) \neq 0, \\ 1, \textit{ falls } h(a) = 0. \end{cases}
\end{aligned}$$

Zusammenfassend erhalten wir

$$(dx) = (\alpha_1, 0) + \ldots + (\alpha_{2g+1}, 0) - 3P_\infty.$$

Wir wollen noch auf eine weitere, wichtige Konstruktion eingehen.

Dazu sei R ein Ring mit Eins, M ein R-Modul und $T^n(M)$ das n-fache Tensorprodukt von M mit der multilinearen Abbildung

$$\tau_n : M^n \to T^n(M), \quad \tau_n(x_1, \ldots, x_n) := x_1 \otimes \ldots \otimes x_n.$$

Außerdem sei I_n das Ideal von T^n, welches durch

$$\{x_1 \otimes \ldots \otimes x_n \in T^n(M) \mid \text{es existieren } 1 \leq i < j \leq n \text{ mit } x_i = x_j\}$$

erzeugt wird. Dann ist das *n-fache äußere Produkt von M* definiert als

$$\bigwedge^n M := T^n(M)/I_n.$$

Die Bilder von $(x_1, \ldots, x_n) \in M^n$ unter τ_n in $\bigwedge^n M$ bilden ein Erzeugendensystem und werden mit $x_1 \wedge \ldots \wedge x_n$ bezeichnet. Für den oben beschriebenen Differentialmodul und $i \geq 0$ können wir also

$$\Omega^i_{A/R} := \bigwedge^i \Omega_{A/R}$$

definieren, wobei $\Omega^0_{A/R} := A$ gelten soll. Außerdem liefern die Abbildungen

$$d_i : \Omega^i_{A/R} \to \Omega^{i+1}_{A/R},$$

$$xdx_1 \wedge dx_2 \wedge \ldots \wedge dx_i \mapsto dx \wedge dx_1 \wedge \ldots \wedge dx_i$$

eine Folge von Homomorphismen mit der Eigenschaft $d_i \circ d_{i-1} = 0$ für alle $i \geq 1$. Denn es gilt

$$\begin{aligned} d_i(d_{i-1}(xdx_1 \wedge dx_2 \wedge \ldots \wedge dx_{i-1})) &= d_i(1dx \wedge dx_1 \wedge \ldots \wedge dx_{i-1}) \\ &= d1 \wedge dx \wedge dx_1 \wedge \ldots \wedge dx_{i-1} \\ &= 0. \end{aligned}$$

Diese Eigenschaften liefern einen Kettenkomplex.

Definition 1.40 (de Rham-Komplex)**.** *Mit den obigen Definitionen heißt die Sequenz*

$$0 \xrightarrow{d_{-1}} A \xrightarrow{d_0} \Omega^1_{A/R} \xrightarrow{d_1} \Omega^2_{A/R} \xrightarrow{d_2} \ldots$$

der de Rham-Komplex von A/R.

Der de Rham-Komplex einer R-Algebra A existiert und ist eindeutig bestimmt (siehe [MW68, S. 196]). Wir nennen ein Element $\omega \in \Omega^i_{A/R}$ *geschlossen*, falls $d_i\omega = 0$ gilt und *exakt*, falls ein $\theta \in \Omega^{i-1}_{A/R}$ mit $d_{i-1}\theta = \omega$ existiert. Aufgrund der Eigenschaft $d_i \circ d_{i-1} = 0$ sind alle exakten Elemente geschlossen und bilden eine Untergruppe in der Gruppe der geschlossenen Differentiale.

Definition 1.41 (de Rham-Kohomologie)**.** *Die i-te Homologiegruppe des de Rham-Komplexes*

$$H^i_{dR}(A/R) := \ker d_i / d_{i-1}(\Omega^{i-1}_{A/R})$$

heißt i-te de Rham-Kohomologiegruppe von A/R.

1.2.8 Abelsche Varietäten

In diesem Abschnitt wollen wir uns mit Varietäten beschäftigen, die eine zusätzliche Struktur besitzen. Die meisten der folgenden Aussagen sind in [Mum70] oder [CF06] zu finden.

Eine *Gruppenvarietät* ist eine Varietät, versehen mit einer Gruppenstruktur, die verträglich mit der Struktur der Varietät ist. Das heißt, die Gruppengesetze können durch Morphismen beschrieben werden.

Definition 1.42 (Abelsche Varietät)**.** *Eine* abelsche Varietät *ist eine nichtsinguläre, projektive, kommutative Gruppenvarietät.*

Aus der Definition eines Morphismus geht hervor, dass die $\mathbb{L}$-rationalen Punkte $\mathcal{A}(\mathbb{L})$ einer abelschen Varietät $\mathcal{A}/\mathbb{K}$ Untergruppen von $\mathcal{A}$ für alle Zwischenkörper $\mathbb{K} \subseteq \mathbb{L} \subseteq \overline{\mathbb{K}}$ bilden.

Elliptische Kurven sind beispielsweise abelsche Varietäten. Für Kurven im Allgemeinen gilt dies nicht. Allerdings können wir jeder glatten Kurve $C/\mathbb{K}$ vom Geschlecht g mit einem $\mathbb{K}$-rationalen Punkt eine abelsche Varietät Jac_C der Dimension g zuordnen, so dass für jeden Zwischenkörper $\mathbb{K} \subseteq \mathbb{L} \subseteq \overline{\mathbb{K}}$ die Isomorphie

$$\mathrm{Jac}_C(\mathbb{L}) \cong \mathcal{C}l^0(\mathbb{L}(C)) \tag{1.4}$$

gilt (für eine Beweisskizze siehe [Sil94, III. Proposition 2.6.]). Wir nennen Jac_C die *jacobische Varietät* (oder kurz *Jacobische*) von C. Die Kurve C lässt sich dabei in ihre jacobische Varietät einbetten.

Im folgenden bezeichnen $\mathcal{A}$ und $\mathcal{B}$ abelsche Varietäten, die über einem endlichen Körper $\mathbb{K}$ der Charakteristik p definiert sind und g die Dimension von $\mathcal{A}$.

Definition 1.43 (Isogenie)**.** *Ein Morphismus von abelschen Varietäten $\varphi : \mathcal{A} \to \mathcal{B}$, der gleichzeitig ein Gruppenhomomorphismus ist, heißt* Isogenie*, falls er surjektiv ist und einen endlichen Kern besitzt.*

Beispielsweise ist die Multiplikation mit einer ganzen Zahl $n \neq 0$ eine Isogenie auf jeder abelschen Varietät $\mathcal{A}$ und wird mit $[n]$ bezeichnet. Der Kern einer solchen Isogenie heißt *n-Torsionsgruppe* und wird mit $\mathcal{A}[n]$ bezeichnet. Für die Struktur dieser Gruppen gilt:

- $\mathcal{A}[l^k] \cong (\mathbb{Z}/l^k\mathbb{Z})^{2g}$
- $\mathcal{A}[p^k] \cong (\mathbb{Z}/p^k\mathbb{Z})^r$ mit $0 \leq r \leq g$

wobei $l \neq p$ eine Primzahl und $k \in \mathbb{N}$ ist. Mit Hilfe der Abbildungen $[l] : \mathcal{A}[l^k] \to \mathcal{A}[l^{k-1}]$ ($k \in \mathbb{N}$) können wir den projektiven Limes dieser Gruppen definieren.

Definition 1.44 (Tate-Modul)**.** *Für eine Primzahl $l \neq p$ ist der* (l-adische) Tate-Modul *definiert als*

$$T_l(\mathcal{A}) := \varprojlim \mathcal{A}[l^k].$$

Die Elemente von $T_l(\mathcal{A})$ sind also Folgen $(a_1, a_2, a_3, \ldots)$ mit $a_k \in \mathcal{A}[l^k]$ und $la_k = a_{k-1}$ für alle $k \in \mathbb{N}$. Aufgrund der Strukturaussagen über die Torsionsgruppen folgt

$$T_l(\mathcal{A}) \cong \mathbb{Z}_l^{2g}.$$

Ein weiteres Beispiel für eine Isogenie einer abelschen Varietät $\mathcal{A}$ über $\mathbb{F}_q$ ist der q-Frobenius, den wir in Beispiel 1.19 beschrieben haben. Die Fixpunkte dieser Abbildung sind gerade die $\mathbb{F}_q$-rationalen Punkte von $\mathcal{A}$.

Da es sich bei Isogenien um Gruppenhomomorphismen handelt, kommutieren diese mit der Multiplikation mit l und induzieren somit $\mathbb{Z}_l$-lineare Abbildungen auf $T_l(\mathcal{A})$. Eine noch stärkere Aussage liefert der Satz von John Tate.

Satz 1.45 (Tate)**.** *Für eine abelsche Varietät $\mathcal{A}/\mathbb{K}$ ist die natürliche Abbildung*

$$\mathrm{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Z}_l \to \mathrm{End}(T_l(\mathcal{A}))$$

ein Isomorphismus. Das Bild eines $\varphi \in \mathrm{End}(\mathcal{A})$ unter dieser Abbildung bezeichnen wir mit φ_l.

Beweis. Siehe [Tat66, S. 134 (1)]. □

Für eine fixierte $\mathbb{Z}_l$-Basis von $T_l(\mathcal{A})$ können wir jedem Endomorphismus φ_l eine Matrix $M_{\varphi_l} \in \mathbb{Z}_l^{2g \times 2g}$ zuordnen, die offensichtlich sowohl von der Wahl von l als auch von der Wahl der Basis abhängt. Es lässt sich allerdings zeigen, dass das charakteristische Polynom einer solchen Matrix bereits in $\mathbb{Z}[t]$ liegt und unabhängig von l ist. Folgende Definition ist also sinnvoll.

Definition 1.46 (Charakteristisches Polynom)**.** *Das* charakteristische Polynom *einer Isogenie $\varphi : \mathcal{A} \to \mathcal{A}$ ist definiert als*

$$\chi_\varphi(t) := \det(t - M_{\varphi_l}).$$

Aufgrund der Kommutativität von Isogenien mit $[l]$ liefert jeder Endomorphismus φ eine Einschränkung $\overline{\varphi} : \mathcal{A}[l] \to \mathcal{A}[l]$ und für das charakteristische Polynom $\chi_{\overline{\varphi}}$ von $\overline{\varphi}$ gilt

$$\chi_{\overline{\varphi}} \equiv \chi_\varphi \mod l. \tag{1.5}$$

Den Bezug zum Punktezählen stellen die beiden folgenden Aussagen her.

Satz 1.47. *Für eine Isogenie $\varphi : \mathcal{A} \to \mathcal{A}$ gilt*

$$deg\varphi = detM_{\varphi_l} = \chi_\varphi(0)$$

und damit

$$deg([n] - \varphi) = \chi_\varphi(n).$$

Satz 1.48. *Für den Kern einer Isogenie $\varphi : \mathcal{A} \to \mathcal{A}$ gilt*

$$\#\ker(\varphi) = deg_s(\varphi).$$

Wir können die Fixpunkte einer Abbildung $\varphi : \mathcal{A} \to \mathcal{A}$, für die $[1] - \varphi$ separabel ist, also bestimmen, indem wir das charakteristische Polynom χ_φ berechnen und dieses an der Stelle 1 auswerten.

Kapitel 2

Die Zetafunktion algebraischer Kurven

Im ersten Kapiteln haben wir alle nötigen Grundlagen über Varietäten behandelt. In diesem Kapitel führen wir nun die Zetafunktion einer algebraischen Kurve ein und beschreiben den Zusammenhang zum Punktezählen. Außerdem werden wir Methoden zur Berechnung der Zetafunktion vorstellen.

Viele der gemachten Definitionen und Aussagen lassen sich deutlich allgemeiner fassen, wir werden uns aber auf den Fall von glatten Kurven beschränken.

2.1 Definition und Weil-Vermutungen

In diesem Abschnitt bezeichne C eine glatte Kurve vom Geschlecht g, die über dem endlichen Körper $\mathbb{F}_q$ ($q = p^n$, p prim) definiert ist. Außerdem werden wir die Bezeichnung $N_k := \#C(\mathbb{F}_{q^k})$ verwenden. Zunächst wollen wir die Zetafunktion definieren und ihre wichtigsten Eigenschaften formulieren.

Definition 2.1 (Zetafunktion)**.** *Die* Zetafunktion *einer Kurve $C/\mathbb{F}_q$ ist definiert als*

$$\zeta(C;t) := \exp\left(\sum_{k=1}^{\infty} \frac{N_k}{k} t^k\right).$$

Diese Definition lässt sich ganz analog auch für höherdimensionale Varietäten definieren und ist als formale Potenzreihe in $\mathbb{Q}[[t]]$ zu interpretieren. André Weil formulierte 1949 in [Wei49] die folgenden Vermutungen über die Zetafunktion, welche mittlerweile alle bewiesen sind.

Satz 2.2 (Weil-Vermutungen für Kurven)**.** *Es sei C eine glatte Kurve über $\mathbb{F}_q$ vom Geschlecht g. Dann gilt für ihre Zetafunktion:*

(i) Rationalität*: ζ ist eine rationale Funktion und lässt sich schreiben als $\frac{L(t)}{(1-t)(1-qt)}$ mit einem Polynom $L \in \mathbb{Z}[t]$ vom Grad $2g$. Das Polynom L heißt* L-Polynom von C über $\mathbb{F}_q$.

(ii) Funktionalgleichung*: $L(t) = q^g t^{2g} L(\frac{1}{qt})$*

(iii) Riemannsche Vermutung für Funktionenkörper*: Die Inversen der Nullstellen von ζ haben den Absolutbetrag $\sqrt{q}$. Das heißt, L zerfällt (über $\mathbb{C}$) in $\prod_{i=1}^{2g}(1-\alpha_i t)$ mit $|\alpha_i| = \sqrt{q}$ $(i = 1, \ldots, 2g)$.*

Beweis. Siehe [Sti93, V.1.12. und V.1.15]. □

Die letzte Aussage ist das Analogon zur Vermutung von Bernhard Riemann über die klassische Zetafunktion. Diese besagt, dass alle nicht reellen Nullstellen der meromorphen Fortsetzung von $\zeta(s) = \sum_{k=1}^{\infty} k^{-s}$ ($\mathrm{Re}s > 1$) auf ganz $\mathbb{C}$ auf der „kritischen Geraden“ $\mathrm{Re}s = \frac{1}{2}$ liegen.

Der Zusammenhang zu der oben gemachten Aussage ist folgendermaßen zu sehen: Wir können die Zetafunktion einer Kurve schreiben als $\zeta(C;t) = \sum_{k=0}^{\infty} A_k t^k$ (siehe [Sti93, V.1.5.]), wobei A_k die Anzahl der effektiven Divisoren vom Grad k bezeichnet. Wenn wir nun die Norm eines Divisors $A \in \mathcal{D}(\mathbb{F}_q(C))$ durch $\mathcal{N}(A) := q^{\deg A}$ definieren, erhalten wir für $s \in \mathbb{C}$ mit $\mathrm{Re}s > 1$ die Darstellung

$$\zeta(C; q^{-s}) = \sum_{k=0}^{\infty} A_k q^{-sk} = \sum_{A \in \mathcal{D}(\mathbb{F}_q(C)), A \geq 0} \mathcal{N}(A)^{-s},$$

welche das Analogon zur klassischen Zetafunktion ist. Aussage *(iii)* liefert nun für die Nullstellen $|q^{-s}| = q^{-\mathrm{Re}s} = \frac{1}{q^{1/2}}$ und damit $\mathrm{Re}s = \frac{1}{2}$.

Korollar 2.3. *Es sei $L(t) = a_0 + a_1 t + \ldots + a_{2g} t^{2g}$ das L-Polynom einer Kurve $C/\mathbb{F}_q$. Dann gilt:*

(i) $L(1) = h(\mathbb{F}_q(C))$.

(ii) $a_{2g-i} = q^{g-i} a_i$ *für* $i = 0, \ldots, g$. *Das heißt, L ist bereits durch die Koeffizienten $a_0, \ldots, a_g$ eindeutig bestimmt.*

(iii) $|a_i| \leq \binom{2g}{i} q^{i/2}$ *für* $i = 0, \ldots, 2g$.

(iv) $N_k = q^k + 1 + a_1$. *Insbesondere gilt* $|N_1 - q - 1| \leq 2g\sqrt{q}$.

(v) Für das L-Polynom der Kurve $C/\mathbb{F}_{q^k}$ gilt

$$L_k(t) = \prod_{i=1}^{2g} (1 - \alpha_i^k t)$$

mit $\alpha_i \in \mathbb{C}$ und $\alpha_i \alpha_{g+i} = q$ für $i = 1, \ldots, g$.

(vi) Mit der Bezeichnung $S_k := N_k - q^k - 1$ *gilt für* $i = 1, \ldots, g$*:*

$$a_0 = 1 \text{ und } \; ia_i = S_i a_0 + S_{i-1} a_1 + \ldots + S_1 a_{i-1}.$$

Das heißt, L ist bereits durch $N_1, \ldots, N_g$ *eindeutig bestimmt.*

Beweis. (i) Siehe [Sti93, V.1.15].

(ii) Siehe [Sti93, V.1.15].

(iii) Mit Satz 2.2(iii) gilt

$$|a_i| = \left| \sum_{j_1 < \ldots < j_i} \alpha_{j_1} \cdot \ldots \cdot \alpha_{j_i} \right| \leq \sum_{j_1 < \ldots < j_i} q^{i/2} \leq \binom{2g}{i} q^{i/2}$$

(iv) Durch logarithmieren der Definition von ζ und mit der Identität $\ln(1-x) = -\sum_{k=1}^{\infty} \frac{x^k}{k}$ erhalten wir

$$\begin{aligned} \sum_{k=1}^{\infty} N_k \frac{t^k}{k} &= \ln \zeta(C;t) \\ &\overset{Satz\ 2.2}{=} -\ln(1-qt) - \ln(1-t) + \sum_{i=1}^{2g} \ln(1-\alpha_i t) \\ &= \sum_{k=1}^{\infty} \left(q^k + 1 - \sum_{i=1}^{2g} \alpha_i \right) \frac{t^k}{k}. \end{aligned}$$

Ein Vergleich der Koeffizienten liefert dann $N_k = q^k + 1 - \sum_{i=1}^{2g} \alpha_i = q^k + 1 + a_1$. Die zweite Behauptung folgt damit aus *(iii)*.

(v) Siehe [Sti93, V.1.15].

(vi) Siehe [Sti93, V.1.17.].

□

Zusammenfassend stellen wir fest, dass die Zetafunktion (beziehungsweise das L-Polynom) viele interessante Informationen enthält. Wir können daraus für beliebiges $k \in \mathbb{N}$ die Zahlen $\#C(\mathbb{F}_{q^k})$ sowie $\#\mathcal{C}l^0(\mathbb{F}_{q^k}(C))$ einfach berechnen. Die Anzahl der $\mathbb{F}_{q^k}$-rationalen Punkte der Kurve und ihrer jacobischen Varietät sind also eng miteinander verknüpft.

2.2 Punktezählen

Wie wir gesehen haben, liefert die Zetafunktion einer Kurve die Anzahl der rationalen Punkte auf der Kurve sowie auf der jacobischen Varietät. Wenn wir von „Punktezählen“ sprechen, ist deshalb in der Regel das Bestimmen der Zetafunktion gemeint und wir stellen uns die Frage, wie wir diese (effizient) berechnen können.

Es sei nun ein affiner Teil $C/\mathbb{F}_q$ einer glatten Kurve $\overline{C}$ durch $f(x,y) = 0$ gegeben. Rein algebraisch betrachtet, sind wir an der Anzahl der Lösungen $(x,y) \in \mathbb{F}_{q^k}^2$ dieser Gleichung für $k = 1, \ldots, g$ interessiert, denn wir wissen bereits, dass wir, nach Hinzunahme der Punkte im Unendlichen, ζ daraus eindeutig bestimmen können (Satz 2.3(vi)). Natürlich können wir diese Zahlen durch ausprobieren bestimmen. In einigen Fällen (siehe [Cas06, S. 7]) können wir die Gleichung auch so umformen, dass sich die Anzahl der Lösungen nicht ändert, und erhalten eine Gleichung, aus der die Lösungen einfach ersichtlich sind. Im Allgemeinen erhalten wir aber erst durch eine geometrischere Betrachtung des Problems effiziente Lösungsansätze. Dabei fassen wir die $\mathbb{F}_{q^k}$-rationalen Punkte als Fixpunkte der (iterierten) q-Frobenius Abbildung

$$(x,y) \mapsto (x^q, y^q)$$

auf. Letztendlich haben wir es also mit einem Fixpunktproblem zu tun, für das uns die algebraische Topologie den Fixpunktsatz von Lefschetz zur Verfügung stellt. André Weils Idee war es, diesen Satz auf den Fall von Varietäten über endlichen Körpern zu übertragen um damit seine Vermutungen zu beweisen. Er hoffte also, eine geeignete Kohomologie definieren zu können um damit die Zetafunktion auszudrücken. Dazu werden Vektorräume $H^i(C)$ benötigt, die den folgenden Bedingungen genügen:

- Der q-Frobenius auf der Kurve induziert eine lineare Abbildungen Φ^* auf den $H^i(C)$.
- Mit den Abbildungen Φ^* auf $H^i(C)$ gilt der Fixpunktsatz von Lefschetz, also eine Aussage der Form

$$\#\overline{C}(\mathbb{F}_{q^k}) = \sum_{i=0}^{2} (-1)^i \mathrm{Tr}\left(\Phi^{*k} | H^i(C)\right).$$

Insbesondere muss die Spur von Φ^* auf den Vektorräumen $H^i(C)$ wohldefiniert sein, weshalb wir fordern, dass die Vektorräume endlichdimensional sind (obwohl dies kein notwendiges Kriterium für die Existenz der Spur ist).

Für weitere Überlegungen benötigen wir das folgendes Lemma.

Lemma 2.4. *Es sei V ein endlichdimensionaler $\mathbb{K}$-Vektorraum und $\phi : V \to V$ ein Endomorphismus. Dann gilt die folgende Gleichheit von formalen Potenzreihen*

$$\exp\left(\sum_{k=1}^{\infty} \mathrm{Tr}(\phi^k)\frac{t^k}{k}\right) = \frac{1}{\det(1-\phi t)}.$$

Beweis. Für den Fall, dass V eindimensional ist, entspricht ϕ einer Multiplikation mit einem Skalar $\lambda \in \mathbb{K}$ und es ist die Identität

$$\sum_{k=1}^{\infty} \lambda^k \frac{t^k}{k} = \ln\left(\frac{1}{1-\lambda t}\right) \tag{2.1}$$

zu zeigen. Diese folgt unmittelbar, wenn wir die rechte Seite als formale Taylor-Reihe im Punkt $t = 0$ entwickeln.

Kommen wir zum höherdimensionalen Fall mit $\dim(V) =: n > 1$. Dazu betrachten wir einen algebraischen Abschluss $\overline{\mathbb{K}}$ von $\mathbb{K}$ und die $\overline{\mathbb{K}}$-lineare Fortsetzung von ϕ

$$\overline{\phi} : V \otimes_{\mathbb{K}} \overline{\mathbb{K}} \to V \otimes_{\mathbb{K}} \overline{\mathbb{K}}.$$

$V \otimes_{\mathbb{K}} \overline{\mathbb{K}}$ ist dann ein $\overline{\mathbb{K}}$-Vektorraum und da $\overline{\mathbb{K}}$ algebraisch abgeschlossen ist, können wir annehmen, dass die Darstellungsmatrix von $\overline{\phi}$ bezüglich einer geeigneten Basis in Jordan-Normalform gegeben ist. Das charakteristische Polynom der Abbildung ändert sich sowohl durch das tensorieren, als auch durch die Basistransformation nicht und es gilt insbesondere $\mathrm{Tr}(\phi^k) = \mathrm{Tr}(\overline{\phi}^k)$. Bezeichnen wir die Diagonaleinträge der Jordan-Normalform mit $\lambda_1, \ldots, \lambda_n \in \overline{\mathbb{K}}$, dann folgt für die Spur $\mathrm{Tr}(\phi) = \mathrm{Tr}(\overline{\phi}) = \sum_{i=1}^{n} \lambda_i$ und aufgrund der Multiplikativität der Determinante $\mathrm{Tr}(\phi^k) = \sum_{i=1}^{n} \lambda_i^k$. Insgesamt ergibt sich also

$$\begin{aligned}
\sum_{k=1}^{\infty} \mathrm{Tr}(\phi^k)\frac{t^k}{k} &= \sum_{k=1}^{\infty} (\sum_{i=1}^{n} \lambda_i^k)\frac{t^k}{k} \\
&= \sum_{i=1}^{n}\sum_{k=1}^{\infty} \lambda_i^k \frac{t^k}{k} \\
&\overset{(2.1)}{=} \sum_{i=1}^{n} \ln\left(\frac{1}{1-\lambda_i t}\right) \\
&= \ln\left(\prod_{i=1}^{n} \frac{1}{1-\lambda_i t}\right) \\
&= \ln\left(\frac{1}{\det(1-\phi t)}\right)
\end{aligned}$$

und damit die Behauptung. □

Angenommen, es existieren solche Vektorräume $H^i(C)$. Dann gilt für die Anzahl der $\mathbb{F}_{q^k}$-rationalen Punkte

$$N_k = \#\overline{C}(\mathbb{F}_{q^k}) = \mathrm{Tr}\left(\Phi^{*k} | H^0(C)\right) - \mathrm{Tr}\left(\Phi^{*k} | H^1(C)\right) + \mathrm{Tr}\left(\Phi^{*k} | H^2(C)\right)$$

und für die Zetafunktion folgt

$$\begin{aligned}
\zeta(\overline{C};t) &= \exp\left(\sum_{k=1}^{\infty}\frac{N_k}{k}t^k\right)\\
&= \exp\left(\sum_{k=1}^{\infty}\frac{\operatorname{Tr}\left(\Phi^{*k}|H^0(C)\right)-\operatorname{Tr}\left(\Phi^{*k}|H^1(C)\right)+\operatorname{Tr}\left(\Phi^{*k}|H^2(C)\right)}{k}t^k\right)\\
&= \exp\left(\sum_{k=1}^{\infty}\frac{\operatorname{Tr}\left(\Phi^{*k}|H^0(C)\right)}{k}t^k\right)\cdot\exp\left(-\sum_{k=1}^{\infty}\frac{\operatorname{Tr}\left(\Phi^{*k}|H^1(C)\right)}{k}t^k\right)\\
&\quad\cdot\exp\left(\sum_{k=1}^{\infty}\frac{\operatorname{Tr}\left(\Phi^{*k}|H^2(C)\right)}{k}t^k\right)\\
&= \frac{\det\left(1-\left(\Phi^*|H^1(C)\right)t\right)}{\det\left(1-\left(\Phi^*|H^0(C)\right)t\right)\det\left(1-\left(\Phi^*|H^2(C)\right)t\right)}.
\end{aligned}$$

Die Rationalität der Zetafunktion würde damit unmittelbar folgen. Gleichzeitig liefert diese Darstellung die Möglichkeit, ζ zu bestimmen, indem wir die charakteristischen Polynome von Φ^* auf den $H^i(C)$ berechnen.

In den 1960ern wurde eine geeignete l-adische Kohomologietheorie entwickelt. Das heißt, man definierte Kohomologiegruppen $H^i(C;\mathbb{Q}_l)$, die Vektorräume über den l-adischen Zahlen $\mathbb{Q}_l$ darstellen und die oben beschriebenen Bedingungen erfüllen (l bezeichnet hierbei wieder eine von p verschiedene Primzahl). Auf die Definition dieser Vektorräume wollen wir nicht weiter eingehen (eine ausführliche Darstellung ist beispielsweise in [Mil98] zu finden), weisen aber auf die Isomorphie

$$H^1(C;\mathbb{Q}_l)\cong T_l(\mathrm{Jac}_{\overline{C}})\otimes_{\mathbb{Z}_l}\mathbb{Q}_l$$

hin, mit der es möglich ist, das L-Polynom durch das charakteristische Polynom χ_Φ des q-Frobenius Φ auf der jacobischen Varietät von $\overline{C}$ auszudrücken. Es gilt

$$L(t)=t^{2g}\chi_\Phi(\frac{1}{t}) \tag{2.2}$$

(Siehe auch [CF06, Proposition 8.4]). Aus der Theorie über abelsche Varietäten folgt damit unmittelbar die Aussage (i) aus Satz 2.3, denn $[1]-\Phi$ ist separabel und es gilt

$$L(1)=\chi_\Phi(1)=\deg([1]-\Phi)=\deg_s([1]-\Phi)=\#\ker(\Phi)=h(\mathbb{F}_q(\overline{C})).$$

Es stellt sich also die Frage nach der effizienten Berechnung des charakteristischen Polynoms χ_Φ.

Die Idee l-adischer Verfahren ist es, χ_Φ modulo l für alle Primzahlen l unter einer gewissen Schranke zu berechnen, indem man die Einschränkung von Φ auf die jeweilige

l-Torsionsgruppe betrachtet (siehe (1.5)). Dank Korollar 2.3 haben wir Schranken für die Absolutbeträge der Koeffizienten von L (beziehungsweise χ) und können somit mittels chinesischem Restsatz das L-Polynom eindeutig bestimmen.

Eine andere Herangehensweise ist die p-adische. Bereits 1960 konnte mittels p-adischer Kohomologie (also mit Kohomologiegruppen, die $\mathbb{Q}_q$-Vektorräume sind) die Rationalität der Zetafunktion bewiesen werden. Daraus entwickelten Paul Monsky und Gerard Washnitzer Ende der 1960er Jahre eine Kohomologie [MW68, Mon68, Mon71], die wir in Kapitel 3 beschreiben werden und in Kapitel 4 zur Berechnung von Zetafunktionen hyperelliptischer Kurven mit Kedlayas Algorithmus [Ked01] benutzen werden. Für diese Kohomologiegruppen $H^i_{MW}(C)$ lieferte Paul Monsky folgende Version des Lefschetzschen Fixpunktsatzes:

Satz 2.5. *Es sei C ein glatter, affiner Teil einer Kurve über $\mathbb{F}_q$. Dann gilt für die Anzahl der $\mathbb{F}_{q^k}$-rationalen Punkte ($k \geq 1$)*

$$\#C(\mathbb{F}_{q^k}) = \mathrm{Tr}\left(q^k \Phi^{*-k} | H^0_{MW}(C)\right) - \mathrm{Tr}\left(q^k \Phi^{*-k} | H^1_{MW}(C)\right).$$

Beweis. Siehe [Mon71, S.335]. □

Hierbei bezeichnet Φ^* wieder die vom q-Frobenius induzierte Abbildung auf den Vektorräumen $H^i_{MW}(C)$. Paul Monsky formulierte und bewies diesen Satz deutlich allgemeiner für höherdimensionale Varietäten. Dies gelang ihm ohne die Aussage, dass die Vektorräume $H^i_{MW}(C)$ endlichdimensional sind, indem er zeigte, dass die induzierte Abbildung Φ^* ein sogenannter nuklearer Operator ist. Dies hat zur Folge, dass die Spur von Φ^* eine konvergente Reihe bildet und damit wohldefiniert ist.

Wir weisen darauf hin, dass hier lediglich die Spuren auf der nullten und ersten Kohomologiegruppe addiert werden. Dies folgt aus der Tatsache, dass $H^i_{MW}(C) = 0$ für $i > 1$ gilt (siehe Satz 3.5).

Wir werden später sehen, dass $H^0_{MW}(C)$ ein eindimensionaler $\mathbb{Q}_q$-Vektorraum ist und Φ^* darauf als Identität operiert (siehe Satz 3.5). Es gilt also $\mathrm{Tr}(q^k \Phi^{*-k} | H^0_{MW}(C)) = q^k$. Weiterhin ist $H^1_{MW}(C)$ ein $\mathbb{Q}_q$-Vektorraum der Dimension $2g + m - 1$, wobei m die Anzahl der Punkte im Unendlichen ist.

Für die Anzahl der rationalen Punkte auf der projektiven Kurve gilt demnach

$$N_k = \#\overline{C}(\mathbb{F}_{q^k}) = m + q^k - \mathrm{Tr}\left(q^k \Phi^{*-k} | H^1_{MW}(C)\right)$$

und es folgt analog den obigen Berechnungen

$$\zeta(\overline{C}; t) = \frac{\det\left(1 - \left(q\Phi^{*-1} | H^1_{MW}(C)\right) t\right)}{(1-t)^m (1-qt)}. \tag{2.3}$$

Für den Fall, dass $\overline{C}$ genau einen unendlichen Punkt besitzt, gilt also $L(t) = \det\left(1 - \left(q\Phi^{*-1}|H^1_{MW}(C)\right)t\right)$ und wir erhalten mit Hilfe des nachfolgenden Lemmas 2.6 die Darstellung

$$\zeta(\overline{C};t) = \frac{\det\left(1 - \left(\Phi^*|H^1_{MW}(C)\right)t\right)}{(1-t)(1-qt)}. \tag{2.4}$$

Wir haben also einen Ausdruck der Zetafunktion, in dem lediglich das charakteristische Polynom der induzierten q-Frobeniusabbildung auf der ersten Monsky-Washnitzer-Kohomologiegruppe zu berechnen ist.

Lemma 2.6. *Es sei $\phi : V \to V$ ein Automorphismus des n-dimensionalen Vektorraumes V. Ferner sei $\det(1 - q\phi^{-1}t) \in \mathbb{Z}[t]$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$ und der Faktorisierung $\prod_{i=1}^{n}(1-\alpha_i t)$ über $\mathbb{C}$ mit $|\alpha_i| = \sqrt{q} \in \mathbb{R}$ für $i = 1, \ldots, n$. Dann gilt*

$$\det(1 - q\phi^{-1}t) = \det(1 - \phi t).$$

Beweis. Durch Umformen der gegebenen Determinante erhalten wir

$$\det(1 - q\phi^{-1}t) = t^n \det(\frac{1}{t} - q\phi^{-1}) = t^n \chi_{q\phi^{-1}}(\frac{1}{t}) = t^n \prod_{i=1}^{n}(\frac{1}{t} - \alpha_i).$$

Das auftretende charakteristische Polynom von $q\phi^{-1}$ hat also die Nullstellen $\alpha_1, \ldots, \alpha_n$ und die Eigenwerte von ϕ sind demnach $\frac{q}{\alpha_1}, \ldots, \frac{q}{\alpha_n}$. Da die $\frac{1}{\alpha_i}$ alle Nullstellen des gegebenen Polynoms sind, welches Koeffizienten in $\mathbb{Z}$ hat, werden die α_i durch komplexe Konjugation lediglich permutiert. Wenn wir außerdem bedenken, dass die α_i alle Absolutbetrag $\sqrt{q}$ haben, gilt für die Konjugierten $\overline{\alpha_i} = \frac{q}{\alpha_i}$ und wir können die Eigenwerte von ϕ schreiben als $\alpha_1, \ldots, \alpha_n$. Für das charakteristische Polynom von ϕ folgt dann

$$\chi_\phi(t) = \prod_{i=1}^{n}(t - \alpha_i)$$

und damit

$$\det(1 - \phi t) = t^n \chi_\phi(\frac{1}{t}) = t^n \prod_{i=1}^{n}(\frac{1}{t} - \alpha_i) = t^n \chi_{q\phi^{-1}}(\frac{1}{t}) = \det(1 - q\phi^{-1}t).$$

□

Kapitel 3

Monsky-Washnitzer-Kohomologie für Kurven

In diesem Kapitel wollen wir uns mit der Kohomologie von Monsky und Washnitzer [MW68] beschäftigen. Grob gesprochen handelt es sich dabei um die de Rham-Kohomologie (siehe Definition 1.41) einer Algebra, die aus dem Koordinatenring einer glatten Kurve konstruiert wird. Dass diese Kohomologie einer Version des Fixpunktsatzes von Lefschetz genügt, haben wir bereits in Satz 2.5 gesehen. Nun wollen wir sie konstruieren und dabei aufzeigen, warum einige andere Ansätze, eine geeignete Kohomologie zu definieren, nicht funktionieren (können).

Im Folgenden bezeichne C einen affinen Teil einer glatten Kurve über $\mathbb{F}_q$ mit dem Koordinatenring

$$\overline{A} := \mathbb{F}_q[x_1, \ldots, x_n]/(f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n)).$$

Ein erster Ansatz wäre, die de Rham-Kohomologiegruppen von $\overline{A}$ zu wählen. Auf $\overline{A}$ induziert der q-Frobenius auf natürliche Weise eine Abbildung (siehe (1.2)), die sich auch auf die Kohomologiegruppen fortsetzen lässt. Allerdings wären wir damit von vornherein nur in der Lage, Ergebnisse modulo p zu erhalten. Außerdem wäre die erste Kohomologiegruppe „zu groß“ wie wir am Beispiel der affinen Geraden über $\mathbb{F}_q$ zeigen wollen.

Für den Koordinatenring $\mathbb{F}_q[x]$ der affinen Geraden sind alle Differentiale der Form $x^{np-1}dx$ ($n \in \mathbb{N}$) nicht exakt. Da auch keine endliche, nichttriviale $\mathbb{F}_q$-Linearkombination dieser Elemente exakt ist, sind die Elemente $x^{np-1}dx$ ($n \in \mathbb{N}$) linear unabhängig in $H^1_{dR}(\mathbb{F}_q[x]/\mathbb{F}_q)$ und die erste Kohomologiegruppe somit ein unendlichdimensionaler $\mathbb{F}_q$-Vektorraum . Aufgrund der Darstellung (2.4) erwarten wir allerdings, dass die Dimension Null beträgt, denn die affine Gerade hat Geschlecht Null. Die Ursache für diese Problematik liegt in der positiven Charakteristik des Körpers $\mathbb{F}_q$.

Um zu einer Struktur mit Charakteristik Null zu gelangen, wählen wir beliebige Lifts (siehe Definition 1.5) $F_1, \ldots, F_m$ der definierenden Polynome f_i nach $\mathbb{Z}_q[x_1, \ldots, x_n]$ und

betrachten den Lift des Koordinatenringes $\overline{A}$

$$A_+ := \mathbb{Z}_q[x_1, \ldots, x_n]/(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)).$$

Es gilt $A_+/pA_+ = \overline{A}$ und für den Koordinatenring der gelifteten Kurve über $\mathbb{Q}_q$ erhalten wir

$$A := A_+ \otimes_{\mathbb{Z}_q} \mathbb{Q}_q = \mathbb{Q}_q[x_1, \ldots, x_n]/(F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)).$$

Allerdings treten dann neue Schwierigkeiten auf, denn sicherlich ist der Koordinatenring A abhängig von der Wahl der Lifts F_i. Hinzu kommt, dass der Frobenius im Allgemeinen keinen Endomorphismus $\Phi : A \to A$ induziert. Lediglich für den Fall von elliptischen Kurven lässt sich solch ein ausgezeichneter Lift (der *kanonische Lift*) konstruieren. Dann gilt $\mathrm{End}(A) = \mathrm{End}(\overline{A})$ und wir haben eine eindeutige, induzierte Frobenius-Abbildung mit Hilfe derer wir das L-Polynom berechnen können (siehe dazu [Sat00]).

Um die Unabhängigkeit von der Wahl des Lifts zu erreichen, müssen wir zu analytischeren Objekten übergehen. Dazu definieren wir A_+^∞ als den p-adischen Abschluss von A_+, also

$$A_+^\infty := \left\{ \sum_{\alpha \in (\mathbb{N}_0)^n} a_\alpha x^\alpha \,\middle|\, a_\alpha \in \mathbb{Z}_q \text{ und } |a_\alpha|_p \to 0 \text{ für } |\alpha| \to \infty \right\} \Big/ (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)).$$

Dabei bezeichnet $\alpha := (\alpha_1, \ldots, \alpha_n)$ einen Multiindex mit $|\alpha| := \sum_{i=1}^n \alpha_i$ und $x^\alpha := x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$. Die $\mathbb{Q}_q$-Algebra $A^\infty := A_+^\infty \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ist dann unabhängig von der Wahl der Lifts F_i und es lässt sich mit Hensels Lemma eine Fortsetzung der Frobenius-Abbildung auf A_+^∞ und damit auf A^∞ konstruieren. Allerdings stellt sich auch hier heraus, dass die de Rham-Kohomologie ungeeignet ist. Wir wollen dies wieder am Beispiel der affinen Geraden über $\mathbb{F}_q$ veranschaulichen. In diesem Fall ist

$$A^\infty = \left\{ \sum_{i \geq 0} a_i x^i \,\middle|\, a_i \in \mathbb{Q}_q \text{ mit } |a_i|_p \to 0 \text{ für } i \to \infty \right\}$$

und jedes der Elemente $p^{kn} x^{p^{kn}-1} dx = d(x^{p^{kn}}) \in \Omega_{A^\infty/\mathbb{Q}_q}$ $(k, n \in \mathbb{N})$ ist exakt. Wenn wir nun für $k \in \mathbb{N}$ die Reihen

$$s_k := \sum_{n=0}^{\infty} p^{kn} x^{p^{kn}-1} dx$$

bilden, erhalten wir für jedes k ein Element aus $\Omega_{A^\infty/\mathbb{Q}_q}$. Dieses ist jedoch für kein $k \in \mathbb{N}$ exakt, denn $d\left(\sum_{n=0}^\infty x^{p^{kn}}\right)$ ist nicht in $\Omega_{A^\infty/\mathbb{Q}_q}$ enthalten. Da auch keine endliche, nichttriviale $\mathbb{Q}_q$-Linearkombination der s_k exakt ist, ist die erste de Rham-Kohomologiegruppe von A^∞ unendlichdimensional (als $\mathbb{Q}_q$-Vektorraum).

Der Grund für die gerade beschriebene Problematik liegt darin, dass die Reihen s_k nicht schnell genug konvergieren. Wir gehen deshalb zu den sogenannten überkonvergenten Reihen über.

Definition 3.1 (Schwache Vervollständigung)**.** *Die* schwache p-adische Vervollständigung *einer $\mathbb{Z}_q$-Algebra A_+ ist definiert als die Menge aller Elemente der Form*

$$\sum_{k=0}^{\infty} h_k(a_1, \ldots, a_m),$$

wobei $m \in \mathbb{N}$, $a_1, \ldots, a_m \in A_+$, $h_k \in p^k \mathbb{Z}_q[X_1, \ldots, X_m]$ und ein $c \in \mathbb{R}$ existiert, so dass $\deg h_k \leq c(k+1)$ *für alle $k \geq 0$ gilt (*deg *bezeichnet dabei den Totalgrad). Die schwache Vervollständigung von A_+ wird mit $A_+^\dagger$ bezeichnet.*

Die schwache Vervollständigung $A_+^\dagger$ ist wieder eine $\mathbb{Z}_q$-Algebra und eine Unteralgebra des p-adischen Abschlusses A_+^∞ von A_+.

Für den Ring $\mathbb{Z}_q[x_1, \ldots, x_n]$ können wir die schwache Vervollständigung schreiben als

$$\mathbb{Z}_q[x_1, \ldots, x_n]^\dagger = \left\{ \sum_{\alpha \in (\mathbb{N}_0)^n} a_\alpha x^\alpha \,\middle|\, a_\alpha \in \mathbb{Z}_q, \liminf_{|\alpha| \to \infty} \frac{v_p(a_\alpha)}{|\alpha|} > 0 \right\},$$

wobei wir mit x^α wieder das Monom $x_1^{\alpha_1} \cdot \ldots \cdot x_n^{\alpha_n}$ bezeichnen und $|\alpha| = \sum_{i=1}^n \alpha_i$ gilt (ein Beweis dieser Aussage ist in [MW68, Theorem 2.3.] zu finden).

Definition 3.2 (w.c.f.g. Algebra)**.** *Eine $\mathbb{Z}_q$-Algebra heißt* „weakly complete finitely generated“ *(kurz* w.c.f.g.*), falls sie ein homomorphes Bild von $\mathbb{Z}_q[x_1, \ldots, x_n]^\dagger$ für ein beliebiges $n \in \mathbb{N}_0$ ist.*

Die schwache Vervollständigung des gelifteten Koordinatenringes A_+ ist demnach eine w.c.f.g. Algebra über $\mathbb{Z}_q$ und es gilt

$$A_+^\dagger = \left\{ \sum_{\alpha \in (\mathbb{N}_0)^n} a_\alpha x^\alpha \,\middle|\, a_\alpha \in \mathbb{Z}_q, \liminf_{|\alpha| \to \infty} \frac{v_p(a_\alpha)}{|\alpha|} > 0 \right\} \Big/ (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)).$$

Diese Algebra ist flach über $\mathbb{Z}_q$ (denn sie ist frei) und es gilt $A_+^\dagger / pA_+^\dagger = \overline{A}$. Damit erfüllt $A_+^\dagger$ alle Bedingungen für den folgenden Satz.

Satz 3.3. *Mit den obigen Bezeichnungen gilt:*

(i) Die Algebra $A_+^\dagger$ ist unabhängig von der Wahl der Lifts $F_1, \ldots, F_m$.

(ii) Für jeden $\mathbb{F}_q$-Algebra-Endomorphismus $\varphi : \overline{A} \to \overline{A}$ existiert ein $\mathbb{Z}_q$-Algebra-Endomorphismus $\widetilde{\varphi} : A_+^\dagger \to A_+^\dagger$, so dass das Diagramm

$$\begin{array}{ccc} A_+^\dagger & \xrightarrow{\widetilde{\varphi}} & A_+^\dagger \\ {\scriptstyle \text{mod } p}\downarrow & & \downarrow{\scriptstyle \text{mod } p} \\ \overline{A} & \xrightarrow[\varphi]{} & \overline{A} \end{array}$$

kommutiert.

Beweis. Siehe [Put86, Theorem 2.4.4. (i) und (ii)]. □

Damit haben wir sichergestellt, dass eine Fortsetzung des q-Frobenius von $\overline{A}$ auf $A_+^\dagger$ existiert.

Wenn wir $A_+^\dagger$ mit $\mathbb{Q}_q$ tensorieren, erhalten wir eine $\mathbb{Q}_q$-Algebra $A^\dagger$ und es gilt mit den Bezeichnungen von oben

$$\begin{aligned} A^\dagger \quad := \quad & \left\{ \sum_{\alpha \in (\mathbb{N}_0)^n} a_\alpha x^\alpha \,\middle|\, a_\alpha \in \mathbb{Q}_q, \liminf_{|\alpha| \to \infty} \frac{v_p(a_\alpha)}{|\alpha|} > 0 \right\} \\ & \Big/ (F_1(x_1, \ldots, x_n), \ldots, F_m(x_1, \ldots, x_n)). \end{aligned} \tag{3.1}$$

Die de Rham-Kohomologie dieser Algebra wird uns die gewünschte Kohomologie liefern. Bevor wir dazu kommen, wollen wir den universellen Differentialmodul dieser Algebra betrachten, der per Definition von den Elementen da mit $a \in A^\dagger$ als $A^\dagger$-Modul erzeugt wird. Aufgrund der Stetigkeit der Derivation d, können wir die Grenzwertbildung und die Derivation vertauschen und es gilt

$$d\left(\sum_{i_1, \ldots, i_n \in \mathbb{N}_0} a_{i_1, \ldots, i_n} x_1^{i_1} \cdot \ldots \cdot x_n^{i_n} \right) = \sum_{i_1, \ldots, i_n \in \mathbb{N}_0} a_{i_1, \ldots, i_n} d\left(x_1^{i_1} \cdot \ldots \cdot x_n^{i_n} \right).$$

Die Elemente $d\big(x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}\big)$ lassen sich als $A^\dagger$-Linearkombination der dx_i schreiben und wir sehen, dass der Differentialmodul bereits durch $dx_1, \ldots, dx_n$ erzeugt wird. Es gilt also

$$\Omega_{A^\dagger/\mathbb{Q}_q} = A^\dagger dx_1 + \ldots + A^\dagger dx_n.$$

Nun kommen wir zur Definition der Objekte unseres eigentlichen Interesses.

Definition 3.4 (Monsky-Washnitzer-Kohomologie)**.** *Es sei $C/\mathbb{F}_q$ ein affiner Teil einer glatten Kurve mit dem Koordinatenring $\overline{A}$. Außerdem bezeichnet $A_+^\dagger$ die schwache Vervollständigung eines Lifts A_+ von $\overline{A}$ und $A^\dagger := A_+^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$. Die* i-te Monsky-Washnitzer-Kohomologiegruppe *von C ist definiert als die i-te de Rham-Kohomologiegruppe der $\mathbb{Q}_q$-Algebra $A^\dagger$ und wird mit $H^i_{MW}(C)$ bezeichnet.*

Über die Struktur der Kohomologiegruppen können wir folgende Aussage machen.

Satz 3.5. *Für den affinen Teil C einer glatten Kurve sei $A^\dagger$ definiert wie in (3.1). Dann gilt für die Monsky-Washnitzer-Kohomologiegruppen*

$$\begin{aligned} H^0_{MW}(C) &= \mathbb{Q}_q, \\ H^1_{MW}(C) &= \Omega_{A^\dagger/\mathbb{Q}_q}/d(A^\dagger), \\ H^i_{MW}(C) &= 0 \quad \textit{für alle } i > 1. \end{aligned}$$

Beweis. Per Definition gilt $H^0_{MW}(C) = \ker d/0 = \mathbb{Q}_q$. Nach [Har77, Theorem 8.15] ist $\Omega_{A^\dagger/\mathbb{Q}_q}$ lokal frei vom Rang eins, das heißt jede Lokalisierung von $\Omega^2_{A^\dagger/\mathbb{Q}_q}$ ist trivial und es folgt mit [Eis95, Lemma 2.8], dass auch $\Omega^2_{A^\dagger/\mathbb{Q}_q}$ verschwindet. Die Definition von H^1_{MW} liefert dann die Aussage $H^1_{MW}(C) = \Omega_{A^\dagger/\mathbb{Q}_q}/d(A^\dagger)$. □

Die nach Satz 3.3 existierende Fortsetzung der Frobenius-Abbildung auf $A^\dagger_+$ liefert zunächst einen $\mathbb{Q}_q$-Algebra-Endomorphismus auf $A^\dagger$ und damit auf natürliche Weise eine Abbildung auf den Kohomologiegruppen $H^i_{MW}(C)$ (siehe (1.3)).

Wie bereits in Satz 2.5 gesehen, erfüllen diese Gruppen eine Version des Fixpunktsatzes von Lefschetz und wir können damit prinzipiell für beliebige, glatte Kurven die Zetafunktion berechnen. Dazu müssen wir zunächst eine Basis des Vektorraums H^1_{MW} bestimmen, die Wirkung des gelifteten q-Frobenius Φ auf diese Basiselemente berechnen und dafür die Darstellung in den Basiselementen finden. Dies liefert uns eine Darstellungsmatrix von Φ und wir können die Zetafunktion mittels (2.3) oder (2.4) bestimmen.

Im nächsten Kapitel werden wir dieses Vorgehen im Fall von hyperelliptischen Kurven über einem Körper der Charakteristik $p > 2$ ausführlich beschreiben. Allgemeinere Fälle werden beispielsweise in [DV06b] (hyperelliptische Kurven in Charakteristik zwei), [GG01] (superelliptische Kurven) oder [DV06a] (C_{ab}-Kurven) beschrieben.

Kapitel 4

Kedlayas Algorithmus

In diesem Kapitel werden wir detailliert zeigen, wie wir die Zetafunktion einer hyperelliptischen Kurve mit der im vorherigen Kapitel definierten Kohomologie berechnen können.

Im gesamten Kapitel bezeichnen wir mit C den affinen Teil einer hyperelliptischen Kurve $\overline{C}/\mathbb{F}_q$, der durch $f(x,y) := y^2 - h(x) = 0$ mit einem $h \in \mathbb{F}_q[x]$ vom Grad $d := 2g+1$ definiert ist. Wir beschränken uns dabei auf den Fall, dass $q = p^n$ für eine Primzahl $p > 2$ gilt.

Bevor wir uns mit der Konstruktion der Kohomologiegruppen befassen, wenden wir uns dem Differentialmodul des Koordinatenringes $\mathbb{F}_q[C] = \mathbb{F}_q[x,y]/(f(x,y))$ zu. Dieser wird als $\mathbb{F}_q[C]$-Modul durch dx und dy erzeugt und mit der Identität $y^2 = h(x,y)$ gilt der Zusammenhang

$$2ydy = h'(x)dx.$$

Könnten wir y invertieren, wäre der Modul also bereits durch dx erzeugt und wir erhielten eine sehr einfache Darstellung. Wie wir in Beispiel 1.21 gesehen haben, erhalten wir durch Herausnehmen der Weierstraßpunkte (also aller affinen Punkte mit $y = 0$) aus C eine quasiaffine Varietät, die isomorph zu einer Varietät C' mit dem Koordinatenring $\mathbb{F}_q[C'] = \mathbb{F}_q[x,y,y^{-1}]/(f(x,y))$ ist. In diesem Ring können wir y invertieren und es gilt

$$\Omega_{\mathbb{F}_q[C']/\mathbb{F}_q} = \mathbb{F}_q[C']dx.$$

Im Folgenden werden wir deshalb anstelle des affinen Teils C nur noch den „gelochten“ Teil C' der Kurve betrachten. Wir werden sehen, dass wir damit dennoch die Zetafunktion der Kurve $\overline{C}$ erhalten.

Wir starten unsere Konstruktion also mit dem Koordinatenring

$$\overline{A} := \mathbb{F}_q[C'] = \mathbb{F}_q[x,y,y^{-1}]/(f(x,y)).$$

Nun wählen wir einen beliebigen Lift $H \in \mathbb{Z}_q[x]$ von h und erhalten durch $F(x,y) := y^2 - H(x)$ einen Lift von $f(x,y)$ (wir könnten auch einen beliebigen anderen Lift von

$f(x,y)$ wählen) und erhalten

$$A := \mathbb{Q}_q[x,y,y^{-1}]/(y^2 - H(x)),$$

wobei wir im Folgenden die Darstellung

$$A = \sum_{\substack{0 \le i < d \\ j \in \mathbb{Z}}} \mathbb{Q}_q x^i y^j$$

benutzen werden. Der Index j durchläuft hier und in späteren Beschreibungen von A nur endlich viele Werte aus $\mathbb{Z}$. Die de Rham-Kohomologie der schwachen Vervollständigung dieses Rings liefert uns später die Monsky-Washnitzer-Kohomologie.

4.1 Die erste de Rham-Kohomologiegruppe von A

Bevor wir die de Rham-Kohomologie von $A^\dagger$ betrachten, wollen wir zunächst die de Rham-Kohomologie der $\mathbb{Q}_q$-Algebra $A = \mathbb{Q}_q[x,y,y^{-1}]/(y^2 - H(x))$ untersuchen und das Ergebnis später auf die schwache Vervollständigung $A^\dagger$ von A übertragen.

Zunächst stellen wir fest, dass aufgrund der Identität $y^2 = H(x)$ der Zusammenhang $dy = \frac{H'(x)}{2y}dx$ besteht und wir den Differentialmodul von A deshalb schreiben können als

$$\Omega_{A/\mathbb{Q}_q} = A \cdot dx. \tag{4.1}$$

Dieser Modul ist torsionsfrei und damit frei.

Wir erinnern an dieser Stelle an die hyperelliptische Involution aus Beispiel 1.22, die auf natürliche Weise eine $\mathbb{Q}_q$-lineare Abbildung auf A durch

$$\iota : A \to A, \quad \sum_{\substack{0 \le i < d \\ j \in \mathbb{Z}}} a_{i,j} x^i y^j \mapsto \sum_{\substack{0 \le i < d \\ j \in \mathbb{Z}}} a_{i,j} x^i (-y)^j$$

induziert. Diese Abbildung spaltet den $\mathbb{Q}_q$-Vektorraum A in eine direkte Summe der beiden Eigenräume A^+ und A^-, wobei wir

$$\begin{aligned} A^+ &:= \sum_{\substack{0 \le i < d \\ j \in 2\mathbb{Z}}} \mathbb{Q}_q x^i y^j = \sum_{\substack{0 \le i < d \\ j \in \mathbb{Z}}} \mathbb{Q}_q x^i H^j(x) \quad \text{und} \\ A^- &:= \sum_{\substack{0 \le i < d \\ j \in 2\mathbb{Z}+1}} \mathbb{Q}_q x^i y^j \end{aligned} \tag{4.2}$$

definieren. Wir erinnern noch einmal daran, dass der Index j hier nur endlich viele Werte annimmt, da in A nur endliche Summen erlaubt sind. Damit können wir den Differentialmodul als direkte Summe der beiden freien Moduln A^+dx und A^-dx schreiben.

Nun faktorisieren wir aus dem $\mathbb{Q}_q$-Vektorraum $\Omega_{A/\mathbb{Q}_q}$ den Unterraum $d(A)$ heraus und erhalten

$$H^1_{dR}(A/\mathbb{Q}_q) = H^1_{dR}(A/\mathbb{Q}_q)^+ \oplus H^1_{dR}(A/\mathbb{Q}_q)^- \tag{4.3}$$

mit

$$\begin{aligned} H^1_{dR}(A/\mathbb{Q}_q)^+ &:= A^+dx/(A^+dx \cap d(A)) = A^+dx/(d(A^+)) \quad \text{und} \\ H^1_{dR}(A/\mathbb{Q}_q)^- &:= A^-dx/(A^-dx \cap d(A)) = A^-dx/(d(A^-)). \end{aligned}$$

Diese beiden Unterräume sind gerade die beiden Eigenräume der induzierten Involution ι auf $H^1_{dR}(A/\mathbb{Q}_q)$ mit den Eigenwerten $+1$ und -1. Wir nennen sie deshalb auch positiven beziehungsweise negativen Eigenraum.

Satz 4.1. *Es sei A wie oben definiert. Die erste de Rham-Kohomologiegruppe $H^1_{dR}(A/\mathbb{Q}_q)$ der $\mathbb{Q}_q$-Algebra A ist ein $\mathbb{Q}_q$-Vektorraum der Dimension $4g+1$ mit der Basis*

$$B := B^+ \cup B^-,$$

wobei $B^+ := \left\{ x^i \frac{dx}{y^2} \,\middle|\, 0 \le i \le 2g \right\}$ und $B^- := \left\{ x^i \frac{dx}{y} \,\middle|\, 0 \le i < 2g \right\}$ Basen von $H^1_{dR}(A/\mathbb{Q}_q)^+$ beziehungsweise $H^1_{dR}(A/\mathbb{Q}_q)^-$ sind.

Beweis. Der Beweis gliedert sich in zwei Teile. Zuerst zeigen wir, dass die Menge B ein Erzeugendensystem von $H^1_{dR}(A/\mathbb{Q}_q)$ ist und anschließend beweisen wir die lineare Unabhängigkeit dieser Erzeuger. Aufgrund der Aufspaltung (4.3) können wir uns auf die beiden Eigenräume $H^1_{dR}(A/\mathbb{Q}_q)^+$ und $H^1_{dR}(A/\mathbb{Q}_q)^-$ beschränken.

Es sei zunächst ein beliebiges Element $adx \in A^+dx$ gegeben. Wir wollen zeigen, dass adx durch B^+ dargestellt werden kann.

Wir können a schreiben als $a(x,y) = \sum_{j\in\mathbb{Z}} a_j(x)y^{2j}$ mit $a_j \in \mathbb{Q}_q[x]$ vom Grad $\le 2g$ und $a_j \neq 0$ für nur endlich viele $j \in \mathbb{Z}$. Das nachfolgende Lemma 4.3 liefert für jedes j ein $\bar{a}_j \in \mathbb{Q}_q[x]$, so dass

$$a_j(x)y^{2j}dx \equiv \bar{a}_j(x)\frac{dx}{y^2}$$

gilt und damit $a(x,y)dx \equiv \bar{a}(x)\frac{dx}{y^2}$ mit einem $\bar{a} \in \mathbb{Q}_q[x]$ (Das „$\equiv$“ bedeutet hier Gleichheit in dem Faktorraum $H^1_{dR}(A/\mathbb{Q}_q)$). Wir haben also die y-Potenz auf die benötigte Form gebracht und müssen nun eventuell selbiges für die x-Potenzen tun, denn wir haben keine Gradabschätzung für $\bar{a}$. Um die x-Potenzen auf unter $2g+1$ zu reduzieren, stellen wir fest, dass $\mathbb{Q}_q[x]$ ein euklidischer Ring ist und wir $\bar{a}$ deshalb schreiben können als $\bar{a}(x) = q(x)H(x) + \hat{a}(x)$ mit $q, \hat{a} \in \mathbb{Q}_q[x]$ und $\deg \hat{a} < \deg H = 2g+1$. Das Polynom $q(x) = \sum_i q_i x^i$ besitzt die Stammfunktion $Q(x) = \sum_i \frac{q_i}{i+1}x^{i+1} \in A^+$ und es gilt $q(x)dx = d(Q(x)) \equiv 0$. Zusammenfassend ergibt sich

$$a(x,y)dx \equiv \bar{a}(x)\frac{dx}{y^2} = (q(x)H(x) + \hat{a}(x))\frac{dx}{y^2} \overset{y^2=H(x)}{=} q(x)dx + \hat{a}(x)\frac{dx}{y^2} \equiv \hat{a}(x)\frac{dx}{y^2}$$

mit einem $\hat{a} \in \mathbb{Q}_q[x]$ vom Grad $\leq 2g$ und wir erhalten eine Darstellung von adx als $\mathbb{Q}_q$-Linearkombination der Menge B^+. Die Menge B^+ ist also ein Erzeugendensystem des Unterraums $H^1_{dR}(A/\mathbb{Q}_q)^+$.

Für den Fall eines $b(x,y)dx \in A^-dx$ können wir zunächst vollkommen analog vorgehen und erhalten die Darstellung

$$b(x,y)dx \equiv \bar{b}(x)\frac{dx}{y},$$

mit einem Polynom $\bar{b} \in \mathbb{Q}_q[x]$. Die Reduktion des x-Grades, wie wir sie für $H^1_{dR}(A/\mathbb{Q}_q)^+$ durchgeführt haben, lässt sich hier nicht anwenden. Falls $m := \deg \bar{b} \geq 2g$ gilt, betrachten wir stattdessen das exakte Differential

$$\begin{aligned} d(2x^{m-2g}y) &= 2x^{m-2g}dy + 2(m-2g)x^{m-2g-1}ydx \\ &= \left(x^{m-2g}H'(x)\right)\frac{dx}{y} + \left(2(m-2g)x^{m-2g-1}H(x)\right)\frac{dx}{y} \\ &= \left((2m-2g+1)x^m + p(x)\right)\frac{dx}{y} \in d(A^-), \end{aligned}$$

wobei p ein Polynom in $\mathbb{Q}_q[x]$ vom Grad $< m$ bezeichnet. Durch sukzessives subtrahieren geeigneter Vielfacher solcher Differentiale von $\bar{b}(x)\frac{dx}{y}$ erhalten wir also ein Darstellung

$$b(x,y)dx \equiv \hat{b}(x)\frac{dx}{y},$$

mit $\deg(\hat{b}) < 2g$ und damit eine $\mathbb{Q}_q$-Linearkombination der Menge B^-. Damit haben wir gezeigt, dass B ein Erzeugendensystem von $H^1_{dR}(A/\mathbb{Q}_q)$ ist.

Kommen wir nun zur linearen Unabhängigkeit. Auch hier können wir uns auf die beiden Eigenräume beschränken und zeigen die lineare Unabhängigkeit der beiden Mengen B^+ und B^-. Die Ideen der Beweise stammen dabei aus [Mad02] beziehungsweise [Edi03]. Wir beginnen wieder mit dem positiven Teil.

Wir wollen zeigen, dass $x^i\frac{dx}{y^2}$ (mit $i = 0, \ldots, 2g$) linear unabhängig in $A^+dx/(d(A^+))$ sind. Angenommen, die Elemente wären linear abhängig. Dann existieren $\lambda_i \in \mathbb{Q}_q$, so dass

$$0 \neq \underbrace{\sum_{k=0}^{2g} \lambda_k x^k}_{=:f(x)} \frac{dx}{y^2} \in A^+dx$$

exakt ist. Die Beispiele 1.29 und 1.39 liefern den Divisor dieser Linearkombination:

$$\begin{aligned} \left(f\frac{dx}{y^2}\right) &= (f) + (dx) - 2(y) \\ &= \sum_{i=1}^{\deg f}\left(\beta_i, +\sqrt{H(\beta_i)}\right) + \left(\beta_i, -\sqrt{H(\beta_i)}\right) - ((\alpha_1,0) + \ldots + (\alpha_{2g+1},0)) \\ &\quad +(4g-1-2\deg f)P_\infty, \end{aligned}$$

wobei α_i und β_i die Nullstellen von G beziehungsweise von f im algebraischen Abschluss von $\mathbb{Q}_q$ bezeichnen. Die auftretenden negativen Summanden $(\alpha_i, 0)$ können sich hierbei aufgrund der Gradabschätzung für f nicht alle gleichzeitig wegheben und $f\frac{dx}{y^2}$ hat damit mindestens eine einfache Polstelle. Dies liefert zusammen mit Satz 1.38 einen Widerspruch zur Exaktheit.

Kommen wir nun zur linearen Unabhängigkeit der Menge B^-. Hier werden wir einen anderen Weg einschlagen. Zunächst stellen wir fest, dass die exakten Differentiale $d(A^-)$ als $\mathbb{Q}_q$-Vektorraum von den Elementen $d(x^i y^j)$ mit $0 \leq i < d$ und $j \in 2\mathbb{Z}+1$ erzeugt werden. Wir wollen diese Erzeuger etwas genauer unter die Lupe nehmen.

Da $\mathbb{Q}_q[x]$ ein euklidischer Ring ist und das Polynom $H(x)$ teilerfremd zu seiner Ableitung $H'(x)$ ist, können wir $x^i H'(x)$ in $\mathbb{Q}_q[x]$ für $0 \leq i < d$ eindeutig schreiben als

$$x^i H'(x) = a_i(x)H(x) + b_i(x) \quad \text{mit } \deg(b_i) < d.$$

Für $i = 0$ gilt offensichtlich $a_0 = 0$ und $b_0 = H'$. Außerdem sehen wir, dass der führende Koeffizient von a_i für $i \neq 0$ gleich d ist und $\deg a_i = i - 1$ gilt. Damit können wir die $d(x^i y^j)$ schreiben als

$$\begin{aligned} d(x^i y^j) &= \left(i x^{i-1} y^{j+1} + \frac{1}{2} j x^i H'(x) y^{j-1} \right) \frac{dx}{y} \\ &= \left(\underbrace{\left(i x^{i-1} + \frac{1}{2} j a_i(x) \right)}_{:=\widetilde{a}_i(x)} y^{j+1} + \underbrace{\frac{1}{2} j b_i(x)}_{=:\widetilde{b}_i(x)} y^{j-1} \right) \frac{dx}{y} \\ &=: f_{i,j}(x,y)\frac{dx}{y}. \end{aligned}$$

In den Polynomen $f_{i,j}$ mit $i \neq 0$ treten also genau die y-Potenzen $j-1$ und $j+1$ auf, während in den $f_{i,0}$ ausschließlich die y-Potenz $j-1$ auftritt. Der Grad von $\widetilde{a}_i = i x^{i-1} + \frac{1}{2} j a_i$ ist wegen $i + \frac{1}{2} j d \neq 0$ gleich $i - 1$ und es gilt $\deg(\widetilde{a}_i) \leq d - 2$.

Nun kommen wir zum eigentlichen Beweis der linearen Unabhängigkeit. Wir nehmen an, dass die Menge B^- linear abhängig ist und wollen dies zu einem Widerspruch führen. Es existieren also $\lambda_k, \mu_{i,j} \in \mathbb{Q}_q$ mit $\mu_{i,j} \neq 0$ für nur endlich viele $0 \leq i \leq d-1$ und $j \in 2\mathbb{Z}+1$, so dass

$$0 \neq \sum_{0 \leq k \leq d-2} \lambda_k x^k \frac{dx}{y} = \sum_{\substack{0 \leq i \leq d-1 \\ j \in 2\mathbb{Z}+1}} \mu_{i,j} f_{i,j}(x,y) \frac{dx}{y}. \tag{4.4}$$

Da $A^- dx$ frei ist, ist dies äquivalent zu

$$\sum_{0 \leq k \leq d-2} \lambda_k x^k = \sum_{\substack{0 \leq d-1 \\ j \in 2\mathbb{Z}+1}} \mu_{i,j} f_{i,j}(x,y). \tag{4.5}$$

Wir fassen nun die auftretenden Polynome als Elemente des Funktionenkörpers der Kurve auf und betrachten deren Bewertung ord_∞ an der unendlichen Stelle P_∞. In Beispiel 1.29 haben wir gesehen, dass $\mathrm{ord}_\infty(x) = -2$ und $\mathrm{ord}_\infty(y) = -d$ gilt. Mit Hilfe der obigen Überlegungen zu den $f_{i,j}$ und der ultrametrischen Ungleichung (siehe Definition 1.1) schließen wir

$$\begin{aligned}\mathrm{ord}_\infty(f_{i,j}) &= \min\left\{\mathrm{ord}_\infty(\widetilde{a}_i) + \mathrm{ord}_\infty\left(y^{j+1}\right), \mathrm{ord}_\infty(\widetilde{a}_i) + \mathrm{ord}_\infty\left(y^{j-1}\right)\right\} \\ &= -2(i-1) - (j+1)d\end{aligned}$$

und sehen, dass die Ordnung zweier unterschiedlicher $f_{i,j}$ verschieden ist. Die Ordnung einer $\mathbb{Q}_q$-Linearkombination mehrerer $f_{i,j}$ können wir damit mit Hilfe der Ultrametrik als das Minimum aller Ordnungen der $f_{i,j}$ angeben.

Die Ordnung der linken Seite von (4.5) lässt sich nach unten durch $-2d+4$ abschätzen und wir können schlussfolgern, dass auf der rechten Seite keine $f_{i,j}$ mit $j \geq 1$ auftreten. Es gilt also $\mu_{i,j} = 0$ für alle $0 \leq i \leq d-1$ und $j \geq 1$. Durch Umsortieren nach y-Potenzen folgt damit aus (4.5)

$$\sum_{k=0}^{d-2} \lambda_k x^k = \sum_{i=1}^{d-1} \mu_{i,-1}\widetilde{a}_i(x)y^0 + \sum_{\substack{j\in 2\mathbb{Z}+1 \\ j\leq -3}} \left(\sum_{i=1}^{d-1} \mu_{i,j}\widetilde{a}_i(x) + \underbrace{\sum_{i=0}^{d-1} \mu_{i,j+2}\widetilde{b}_i(x)}_{=:\circledast} \right) y^{j+1}.$$

Nun können wir Koeffizienten vergleichen. Da die linke Seite nach Annahme ungleich Null ist, ist mindestens ein $\mu_{i,-1}$ ungleich Null. Dieselben $\mu_{i,-1}$ treten in der Gleichung noch einmal in $\circledast$ für $j = -3$ auf. Da die Polynome $\widetilde{b}_i$ nach Lemma 4.2 linear unabhängig sind, gilt für $j = -3$ auch $\circledast \neq 0$. Dies impliziert wiederum, dass mindestens ein $\mu_{i,-3}$ ungleich Null existiert. Wir können das Argument induktiv fortführen und erhalten damit unendlich viele von Null verschiedene $\mu_{i,j} \in \mathbb{Q}_q$, was ein Widerspruch zur Annahme (4.4) ist. □

Im letzten Schritt des Beweises haben wir das folgende Lemma benutzt.

Lemma 4.2. *Es sei H ein Polynom vom Grad d über $\mathbb{Q}_q$ gegeben, so dass die (formale) Ableitung H' teilerfremd zu H ist. Außerdem bezeichne $\mathbb{Q}_q[x]_{<d}$ den $\mathbb{Q}_q$-Vektorraum der Polynome vom Grad $< d$ und wir definieren die Elemente $b_i \in \mathbb{Q}_q[x]$ eindeutig durch*

$$x^i H' = a_i H + b_i, \text{ mit } a_i \in \mathbb{Q}_q[x] \text{ und } \deg b_i < d.$$

Dann liefern die Polynome $b_0, \ldots, b_{d-1}$ eine Basis von $\mathbb{Q}_q[x]_{<d}$.

Beweis. Wir betrachten die Isomorphie (von Vektorräumen) $\phi : \mathbb{Q}_q[x]_{<d} \to \mathbb{Q}_q[x]/(H)$ mit $\phi(f) := f + H$. Die Umkehrabbildung ϕ^{-1} bildet jedem Element $f + H \in \mathbb{Q}_q[x]/(H)$ den eindeutigen Vertreter der Klasse vom Grad $< d$ zu. Da H' teilerfremd zu H ist, liefert die Multiplikation mit H' einen Isomorphismus auf $\mathbb{Q}_q[x]/(H)$ und wir erhalten aus der kanonischen Basis $1, x, \ldots, x^{d-1}$ von $\mathbb{Q}_q[x]_{<d}$ die Basis $\phi^{-1}(H' \cdot \phi(x^i)) = b_i$ $(i = 0, \ldots, d-1)$. □

Auch das folgende Lemma haben wir aus dem Beweis des Satzes herausgenommen. Es liefert einen Reduktionsalgorithmus, der auch für die Monsky-Washnitzer-Kohomologie gültig sein wird.

Lemma 4.3 (Reduktion der y-Potenz)**.** *Es gelten die Bezeichnungen wie oben. Für jedes $a \in \mathbb{Q}_q[x]$ und $n \in \mathbb{Z}$ existieren Elemente $b, c, B, C \in \mathbb{Q}_q[x]$, so dass*

$$\begin{aligned} a(x)y^n dx &= b(x)y^{n+2}dx + d(B(x)y^{n+2}) \text{ und} \\ a(x)y^n dx &= c(x)y^{n-2}dx + d(C(x)y^n) \end{aligned}$$

gilt. Das heißt, in $H^1_{dR}(A/\mathbb{Q}_q)$ gilt die Gleichheit

$$a(x)y^n dx \equiv b(x)y^{n+2}dx \equiv c(x)y^{n-2}dx.$$

Beweis. Wir werden die Polynome b, B, c und C explizit angeben. Dazu bezeichnen wir mit $A \in \mathbb{Q}_q[x]$ eine Stammfunktion von a und definieren

$$\begin{aligned} c(x) &:= -\frac{n}{2}A(x)H'(x) \text{ und} \\ C(x) &:= A(x). \end{aligned}$$

Es gilt

$$\begin{aligned} d(C(x)y^n) &= A(x)ny^{n-1}dy + a(x)y^n dx \\ &= A(x)ny^{n-1}\frac{H'(x)}{2y}dx + a(x)y^n dx \\ &= \frac{n}{2}A(x)H'(x)y^{n-2}dx + a(x)y^n dx \\ &= -c(x)y^{n-2}dx + a(x)y^n dx \end{aligned}$$

und damit die erste Behauptung.

Das Polynom $h \in \mathbb{F}_q[x]$ ist nach Voraussetzung teilerfremd zu seiner Ableitung h', es existieren also Polynom $s, t \in \mathbb{F}_q[x]$ mit $sh + th' = 1$. Solch eine Darstellung existiert auch für das geliftete Polynom $H \in \mathbb{Z}_q[x]$ und wir können zwei Polynome $S, T \in \mathbb{Z}_q[x]$ konstruieren, so dass $SH + TH' = 1$ gilt (siehe Algorithmus 4). Da $\mathbb{Q}_q[x]$ euklidisch ist, erhalten wir eine eindeutige Darstellung $aT = qH + r$ mit $q, r \in \mathbb{Q}_q[x]$ und $\deg r < \deg H$. Nun definieren wir

$$\begin{aligned} b(x) &:= a(x)S(x) + q(x)H'(x) - \frac{2}{n+2}r'(x) \text{ und} \\ B(x) &:= \frac{2}{n+2}r(x). \end{aligned}$$

Es gilt

$$\begin{aligned} d(B(x)y^{n+2}) &= d\left(\frac{2}{n+2}r(x)y^{n+2}\right) \\ &= \frac{2}{n+2}r(x)(n+2)y^{n+1}\frac{H'(x)}{2y}dx + \frac{2}{n+2}r'(x)y^{n+2}dx \\ &= r(x)H'(x)y^n dx + \frac{2}{n+2}r'(x)y^{n+2}dx \\ &\overset{r=aT-qH}{=} (a(x)T(x) - q(x)H(x))H'(x)y^n dx + \frac{2}{n+2}r'(x)y^{n+2}dx \end{aligned}$$

und damit

$$\begin{aligned} b(x)y^{n+2}dx + d(B(x)y^{n+2}) &= \left(a(x)S(x) + q(x)H'(x) - \frac{2}{n+2}r'(x)\right)y^{n+2}dx \\ &\quad +(a(x)T(x) - q(x)H(x))H'(x)y^n dx \\ &\quad +\frac{2}{n+2}r'(x)y^{n+2}dx \\ &\overset{y^2=H}{=} (a(x)S(x)H(x) + q(x)H'(x)H(x))y^n dx \\ &\quad +(a(x)T(x)H'(x) - q(x)H'(x)H(x))y^n dx \\ &= a(x)(S(x)H(x) + T(x)H'(x))y^n dx \\ &\overset{SH+TH=1}{=} a(x)y^n dx. \end{aligned}$$

Damit haben wir das Lemma vollständig bewiesen. □

Wir wollen diese Ergebnisse im nächsten Abschnitt auf die de Rham-Kohomologie der schwachen Vervollständigung von A übertragen. Dazu müssen wir uns mit dem Verhalten der p-Bewertungen bei der Reduktion beschäftigen, wobei wir uns auf $H^1_{dR}(A/\mathbb{Q}_q)^-$ beschränken.

Lemma 4.4. *Es sei $\omega = a(x)y^{2m}\frac{dx}{y}$ mit $m \in \mathbb{Z}$, $a \in \mathbb{Z}_q[x]$ und $\deg a < d$ gegeben. Dann existieren eindeutige $b \in \mathbb{Q}_q[x]$ und $f \in A^-$ mit $\deg b < d-1$, so dass*

$$\omega = a(x)y^{2m}\frac{dx}{y} = b(x)\frac{dx}{y} + d(f(x,y))$$

und es gilt

(i) für $m < 0$:

$$\begin{aligned} &f(x,y) = \sum_{j=2m+1}^{-1} f_j(x)y^j \in A^- \text{ und } f_j \in \mathbb{Q}_q[x],\ \deg f_j < d \text{ mit} \\ &p^{\lfloor \log_p(-2m-1)\rfloor}b \in \mathbb{Z}_q[x] \text{ und} \\ &p^{\lfloor \log_p(-2m-1)\rfloor}f_j \in \mathbb{Z}_q[x] \text{ für alle } j. \end{aligned}$$

(ii) für $m > 0$:

$$f(x,y) = \sum_{j=1}^{2m-1} f_j(x)y^j \in A^- \text{ und } f_j \in \mathbb{Q}_q[x],\ \deg f_j < d \text{ mit}$$
$$p^{\lfloor \log_p(2dm+d-2)\rfloor} b \in \mathbb{Z}_q[x] \text{ und}$$
$$p^{\lfloor \log_p(2dm+d-2)\rfloor} f_j \in \mathbb{Z}_q[x] \text{ für alle } j.$$

Beweis. Die Existenz und Eindeutigkeit von b und f folgt unmittelbar aus der eindeutigen Darstellung bezüglich der Basis B^-.

Für die anderen Aussagen beginnen wir mit dem Fall $m < 0$.
Die Tatsache, dass in f nur die y-Potenzen $2m+1$ bis -1 auftreten und dass die x-Potenzen maximal $d-1$ betragen, folgt direkt aus dem Reduktionsalgorithmus. Kommen wir nun zu den Ganzheitsaussagen (die Beweisidee stammt aus [Mad02, S.14]). Zunächst wählen wir eine geeignete Erweiterung $\mathbb{Z}_{q^r}$ ($r \in \mathbb{N}$) von $\mathbb{Z}_q$, so dass $H(x)$ eine Nullstelle $\alpha \in \mathbb{Z}_{q^r}$ besitzt und bezeichnen mit P die Stelle des affinen Punktes $(\alpha, 0)$ in dem Funktionenkörper $\mathbb{Q}_{q^r}(C')$ der gelifteten Kurve. Wir haben in Beispiel 1.29 gesehen, dass y dort eine einfache Nullstelle besitzt, also eine Uniformisierende von P ist (wir merken an, dass sich der Funktionenkörper durch das Herausnehmen der Weierstraßpunkte nicht ändert). Nun betrachten wir die Vervollständigung dieses Körpers bezüglich P (für Informationen zur Vervollständigung bezüglich eines Punktes verweisen wir auf [Sti93, IV.2.]). In diesem Abschluss lässt sich jedes Element eindeutig als Potenzreihe in $\mathbb{Q}_{q^r}[y^{-1}][[y]]$ schreiben. Insbesondere erhalten wir die Darstellungen

$$d(f(x,y)) = \sum_{j=2m}^{\infty} c_j y^j dy \quad \text{und damit} \quad f(x,y) = \sum_{j=2m}^{\infty} \frac{c_j}{j+1} y^{j+1},$$

mit $c_j \in \mathbb{Q}_{q^r}$ und $c_j = 0$ für alle ungeraden j. Wir können noch mehr über die Koeffizienten aussagen: Mit den Beispielen 1.29 und 1.39 folgt, dass $b(x)\frac{dx}{y}$ keinen Pol in P hat, die Reihenentwicklung davon besitzt also keine negativen Koeffizienten. Da außerdem $a(x)$ nach Voraussetzung in $\mathbb{Z}_q[x]$ liegt, können wir mittels Koeffizientenvergleich schließen, dass die Koeffizienten c_j für $j < 0$ ganz sind, also in $\mathbb{Z}_{q^r}$ liegen (denn die Reihenentwicklung von $a(x)$ besitzt Koeffizienten aus $\mathbb{Z}_{q^r}$). Mit der Bezeichnung $n := \lfloor \log_p(-2m-1)\rfloor$ gilt damit $p^n \frac{c_j}{j+1} \in \mathbb{Z}_{q^r}$ für alle $j < 0$.

Wir kommen nun zur Darstellung $f(x,y) = \sum_{j=2m+1}^{-1} f_j(x)y^j$ zurück. Wenn wir f_{2m+1} in dem Punkt P auswerten, gilt nach den obigen Überlegungen $f_{2m+1}(P) = \frac{c_{2m+1}}{2m+2}$ und damit $p^n f_{2m+1}(P) \in \mathbb{Z}_{q^r}$. Die gleiche Argumentation können wir für alle anderen Punkte $P_i := (\alpha_i, 0)$ mit $H(\alpha_i) = 0$ $(i = 1, \ldots, 2g+1)$ durchführen und erhalten $p^n f_{2m+1}(P_i) = p^n f_{2m+1}(\alpha_i) \in \overline{\mathbb{Z}}_q$ für alle i. Wir schreiben $p^n f_{2m+1}$ als $\sum_{k=0}^{2g} F_k x^k$ und

erhalten die Darstellung

$$\begin{pmatrix} 1 & \alpha_1 & \alpha_1^2 & \cdots & \alpha_1^{2g} \\ 1 & \alpha_2 & \alpha_2^2 & \cdots & \alpha_2^{2g} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha_{2g+1} & \alpha_{2g+1}^2 & \cdots & \alpha_{2g+1}^{2g} \end{pmatrix} \begin{pmatrix} F_0 \\ F_1 \\ \vdots \\ F_{2g} \end{pmatrix} = \begin{pmatrix} p^n f_{2m+1}(\alpha_1) \\ p^n f_{2m+1}(\alpha_2) \\ \vdots \\ p^n f_{2m+1}(\alpha_{2g+1}) \end{pmatrix} \in \overline{\mathbb{Z}}_q^{2g+1}.$$

Die Matrix auf der linken Seite ist eine Vandermonde-Matrix und wir können ihre Determinante angeben als $\prod_{1\le i<j\le 2g}(\alpha_i - \alpha_j)$. Da H reduziert modulo p nur einfache Nullstellen besitzt, ist die Determinante modulo p von Null verschieden und damit eine Einheit in $\overline{\mathbb{Z}}_q$. Wir können die Matrix also invertieren und erhalten eine Darstellung der F_i durch ganze Elemente. Damit gilt $F_i \in \overline{\mathbb{Z}}_q \cap \mathbb{Q}_q = \mathbb{Z}_q$ für $0 \le i \le 2g$ und somit $p^n f_{2m+1} \in \mathbb{Z}_q[x]$. Nun betrachten wir die Reihenentwicklung von

$$p^n \sum_{j=2m+2}^{-1} f_j(x) y^j \quad = \quad p^n f(x,y) - p^n f_{2m+1}(x) y^{2m+1}$$

und können mit der gleichen Argumentation wie oben zeigen, dass $p^n f_{2m+2} \in \mathbb{Z}_q[x]$ gilt. Sukzessives Vorgehen liefert letztendlich $p^n f_j(x) \in \mathbb{Z}_q[x]$ für alle $i = 2m+1, \ldots, -1$. Die Ganzheitsaussage für $p^n b(x)$ folgt damit unmittelbar aus der Identität $b(x)\frac{dx}{y} = a(x)y^{2m}\frac{dx}{y} - d(f(x,y))$.

Kommen wir nun zu dem Fall $m > 0$:
Wir wollen analog zum ersten Fall vorgehen. Allerdings betrachten wir nun die unendliche Stelle P_∞. Die Beispiele 1.29 und 1.39 liefern uns zusammen mit Satz 1.37 folgende Ordnungen:

$$\mathrm{ord}_\infty(x) = -2,\ \mathrm{ord}_\infty(y) = -d,\ \mathrm{ord}_\infty(f) \ge -2md - d + 2,$$

$$\mathrm{ord}_\infty(dx) = -3,\ \mathrm{ord}_\infty(\frac{dx}{y}) = d - 3,\ \mathrm{ord}_\infty(b(x)\frac{dx}{y}) \ge -d + 1.$$

Das Element $t := \frac{x^g}{y}$ liefert demnach eine Uniformisierende der Stelle P_∞, denn es gilt $\mathrm{ord}_\infty(\frac{x^g}{y}) = g \cdot \mathrm{ord}_\infty(x) - \mathrm{ord}_\infty(y) = -2g + d = 1$. Wie oben können wir zum Abschluss bezüglich P_∞ übergehen und f in der Uniformisierenden entwickeln. Es gilt

$$d(f(x,y)) = \sum_{j \ge -2md-d+2}^{\infty} c_j t^j dt \quad \text{und damit} \quad f(x,y) = \sum_{j \ge -2md-d+2}^{\infty} \frac{c_j}{j+1} t^{j+1},$$

wobei $c_j \in \mathbb{Q}_q$ und $c_j = 0$ für alle ungeraden j. Da die Entwicklung $a(x)\frac{dx}{y}$ Koeffizienten aus $\mathbb{Z}_q$ hat und $\mathrm{ord}_\infty(b(x)\frac{dx}{y}) \ge -d + 1$ gilt, können wir schließen, dass $c_j \in \mathbb{Z}_q$ für $j \le -d$ gilt. Mit der Bezeichnung $n := \lfloor \log_p(2dm + d - 2) \rfloor$ gilt damit $p^n \frac{c_j}{j+1} \in \mathbb{Z}_{q^r}$ für alle $j \le -d$.
Für die Bewertungen der Monome $x^i y^j$ (mit $0 \le i \le d-1$ und $j \ge 1$) von $f(x,y)$ gilt

$$\mathrm{ord}_\infty(x^i y^j) = -2i - jd \le -d \ \text{ und } \ \mathrm{ord}_\infty(x^i y^j) \ne \mathrm{ord}_\infty(x^k y^l) \text{ für } (i,j) \ne (k,l).$$

Iterativ erhalten wir mit obiger Argumentation daraus die Behauptung $p^n f_j \in \mathbb{Z}_q[x]$ für $j = 1, \ldots, 2m-1$ und damit auch $p^n b \in \mathbb{Z}_q[x]$. □

Die Aussage dieses Lemmas wird im nächsten Abschnitt von Bedeutung sein, wenn wir eine Basis der Monsky-Washnitzer-Kohomologie bestimmen. Außerdem kommt es später im Algorithmus zur Anwendung, denn wir können damit die minimale p-adische Präzision der Darstellung von a bestimmen, die wir benötigen, um eine gewisse Präzision der Reduktion b zu erhalten. Wenn wir b modulo p^k korrekt benötigen, muss die Eingabe von a also modulo p^{k+n} exakt sein.

Wir merken an, dass für die Reduktion von Elementen aus A^+dx eine ähnliche Abschätzung gilt. Da wir diese nicht explizit benötigen werden, verzichten wir aber auf eine entsprechende Formulierung.

4.2 Monsky-Washnitzer-Kohomologie für hyperelliptische Kurven

Nachdem wir nun die de Rham-Kohomologie der Algebra A kennen, wollen wir diese Ergebnisse auf die Kohomologie der schwachen Vervollständigung $A^\dagger$ von A übertragen. Dabei interessiert uns lediglich die erste Kohomologiegruppe. Die Struktur der restlichen Gruppen kennen wir bereits aus Satz 3.5. Wir erinnern daran, dass wir weiterhin ausschließlich mit der Kurve C' (also der Kurve ohne ihre Weierstraßpunkte) anstelle von C arbeiten. Dieses Vorgehen werden wir in Abschnitt 4.3 rechtfertigen, wo wir eine Verbindung der Kohomologie von C' zur Zetafunktion von $\overline{C}$ herstellen werden. Wir haben bereits gesehen, dass sich die Rechnungen dadurch stark vereinfachen.

Zunächst stellen wir fest, dass die Involution ι auch $A^\dagger$ in zwei Eigenräume teilt. Es lässt sich zeigen, dass die Involution mit der Vervollständigung kommutiert und die beiden Eigenräume deshalb den schwachen Vervollständigungen der Eigenräume A^+ und A^- entsprechen. Außerdem wird auch der Differentialmodul von $A^\dagger$ durch dx erzeugt und wir können diesen schreiben als

$$\Omega_{A^\dagger/\mathbb{Q}_q} = A^\dagger \cdot dx = (A^+)^\dagger dx \oplus (A^-)^\dagger dx.$$

Für die erste de Rham-Kohomologiegruppe von $A^\dagger$ gilt demnach

$$H^1_{MW}(C') = H^1_{MW}(C')^+ \oplus H^1_{MW}(C')^-,$$

und die beiden Eigenräume lassen sich schreiben als

$$\begin{aligned} H^1_{MW}(C')^+ &= (A^+)^\dagger dx/d((A^+)^\dagger) = H_{dR}((A^+)^\dagger/\mathbb{Q}_q) \quad \text{und} \\ H^1_{MW}(C')^- &= (A^-)^\dagger dx/d((A^-)^\dagger) = H_{dR}((A^-)^\dagger/\mathbb{Q}_q). \end{aligned} \tag{4.6}$$

Wir können uns bei der Bestimmung einer Basis also wieder auf die beiden Eigenräume beschränken und die Reduktionsschritte aus dem Beweis zu Satz 4.1 verwenden. Die

zu reduzierenden Elemente sind nun allerdings keine endlichen Summen mehr, sondern Reihen mit gewissen Konvergenzbedingungen (siehe (3.1)). Es ist also noch nicht klar, ob wir nach einer formalen Reduktion überhaupt wieder Elemente aus $\Omega_{A^\dagger/\mathbb{Q}_q}$ erhalten.

Satz 4.5 (Basis der Monsky-Washnitzer-Kohomologie)**.** *Der Unterraum $H^1_{MW}(C')^-$ der ersten Monsky-Washnitzer-Kohomologiegruppe $H^1_{MW}(C')$ der affinen Varietät C' ist ein $\mathbb{Q}_q$-Vektorraum der Dimension $2g$ mit der Basis*

$$\left\{ x^i \frac{dx}{y} \middle|\ 0 \leq i < 2g \right\}.$$

Beweis. Wir wollen zeigen, dass die Elemente $x^i \frac{dx}{y}$ $(i = 0, \ldots, 2g-1)$ Erzeuger von $H^1_{MW}(C')^-$ sind. Es sei also ein beliebiges Element $a(x,y)dx = \sum_{j\in\mathbb{Z}} a_j(x) y^{2j} \frac{dx}{y}$ aus $\Omega_{A^\dagger/\mathbb{Q}_q}$ mit $\deg a_j \leq 2g$ und den nötigen Konvergenzbedingungen für die Koeffizienten der a_j gegeben. Jeder Summand dieser Reihe ist bereits in $\Omega_{A/\mathbb{Q}_q} \subset \Omega_{A^\dagger/\mathbb{Q}_q}$ enthalten und es existieren nach Lemma 4.4 eindeutige $b_j \in \mathbb{Q}_q[x]$ vom Grad kleiner als $d-1$ und $f_j \in A \subset A^\dagger$, so dass

$$a_j(x) y^{2j} \frac{dx}{y} = b_j(x) \frac{dx}{y} + d(f_j(x,y))$$

für alle $j \in \mathbb{Z}$ gilt. Formal folgt daraus

$$\sum_{j\in\mathbb{Z}} a_j(x) y^{2j} \frac{dx}{y} = \underbrace{\sum_{j\in\mathbb{Z}} b_j(x)}_{=:b(x)} \frac{dx}{y} + d\Bigg(\underbrace{\sum_{j\in\mathbb{Z}} f_j(x,y)}_{=:f(x,y)} \Bigg)$$

und wir müssen lediglich noch zeigen, dass die Elemente b und f Sinn ergeben, dass also $b \in \mathbb{Q}_q[x]$ und $f \in A^\dagger$ gilt.

Da der Grad von b nach oben durch $d-1$ beschränkt beschränkt ist, müssen wir nur noch zeigen, dass jeder der Koeffizienten von b in $\mathbb{Q}_q$ liegt. Mit der Abschätzung

$$v_p(a_j(x)) \leq \begin{cases} \lfloor \log_p(-2j-1) \rfloor + v_p(b_j(x)), \text{ falls } j < 0 \\ \lfloor \log_p(2dj + d - 2) \rfloor + v_p(b_j(x)), \text{ falls } j > 0 \end{cases},$$

die wir aus Lemma 4.4 erhalten und der Überkonvergenz von a folgt $v_p(b_j(x)) \to \infty$ für $j \to \infty$ und damit $b \in \mathbb{Q}_q[x]$.

Betrachten wir nun f: Mit der Schreibweise $f_j(x,y) = \sum_{k\in\mathbb{Z}} f_{j,k}(x) y^k$ und $f_{j,k} \in \mathbb{Q}_q[x]$ mit maximalem Grad $2g$ erhalten wir mittels Lemma 4.4 die Abschätzung

$$v_p(a_j(x)) \leq \begin{cases} \lfloor \log_p(-2j-1) \rfloor + v_p(f_{j,k}(x)), \text{ falls } j < 0 \\ \lfloor \log_p(2dj + d - 2) \rfloor + v_p(f_{j,k}(x)), \text{ falls } j > 0 \end{cases} \quad \text{für alle } k$$

und aufgrund der Überkonvergenz von a die Überkonvergenz von f. Es gilt also $f \in A^\dagger$.

Es bleibt noch die lineare Unabhängigkeit zu zeigen. Angenommen, es existiert eine nichttriviale Linearkombination der Null. Dann können wir die ganze Gleichung mit einer geeigneten p-Potenz multiplizieren, so dass alle auftretenden Koeffizienten in $\mathbb{Z}_q$ liegen. Wenn wir nun modulo einer beliebigen p-Potenz reduzieren, erhalten wir eine Relation in $\Omega_{A/\mathbb{Q}_q}$ die aufgrund der linearen Unabhängigkeit der Elemente in $\Omega_{A/\mathbb{Q}_q}$ nicht Null sein kann. Dieser Widerspruch beendet den Beweis. □

Wir haben uns hier auf den negativen Eigenraum von $H^1_{MW}(C')$ beschränkt. Dies hat den Grund, dass wir zur Berechnung der Zetafunktion nur diesen Teil benötigen, denn wir werden in Abschnitt 4.3 sehen, dass sich das Herausnehmen der Weierstraßpunkte und das Einschränken auf den negativen Eigenraum gegenseitig „aufheben".

Wir wollen aber nicht unerwähnt lassen, dass sich auch die Basis des positiven Eigenraums von $H^1_{dR}(A/\mathbb{Q}_q)$ auf $H^1_{MW}(C')$ überträgt. Der Beweis dazu verläuft genauso wie im negativen Fall, mit Hilfe entsprechender Ganzheitsaussagen analog zu Lemma 4.4.

4.3 Formel für die Zetafunktion

Im vorherigen Abschnitt haben wir gesehen, wie eine Basis des negativen Eigenraums von $H^1_{MW}(C')$ aussieht. Dabei blieb zum einen noch ungeklärt, warum wir uns auf den negativen Eigenraum beschränken können und zum anderen, warum wir die Monsky-Washnitzer-Kohomologie des affinen Teils C' anstelle von C betrachtet haben. Dies soll in diesem Abschnitt geklärt werden. Wir benutzen dabei die Aussage aus Kapitel 3, dass auf der Monsky-Washnitzer-Kohomologie eine induzierte Frobeniusabbildung existiert, für die der Fixpunktsatz von Lefschetz gilt.

Lemma 4.6. *Es sei ein affiner Teil C einer hyperelliptischen Kurve über $\mathbb{F}_q$ durch $y^2 = h(x)$ mit $\deg h = d$ gegeben. Außerdem bezeichne C' den affinen Teil C ohne seine Weierstraßpunkte und L die affine Gerade über $\mathbb{F}_q$ ohne die Nullstellen von $h(x)$, also $L := \mathbb{A}^1 \setminus \{a \in \overline{\mathbb{F}_q} \mid h(a) = 0\}$. Dann gilt*

$$H^0_{MW}(C') = H^0_{MW}(L) \quad \textit{und} \quad H^1_{MW}(C')^+ = H^1_{MW}(L).$$

Beweis. Für den Koordinatenring von L gilt $\mathbb{F}_q[L] = \mathbb{F}_q[x, h^{-1}(x)]$. Um die Monsky-Washnitzer-Kohomologie dieser Varietät zu konstruieren, wählen wir einen Lift $H \in \mathbb{Z}_q[x]$ von h. Da diese Wahl beliebig ist, können wir den gleichen Lift wählen, der auch für die Konstruktion von $H^1_{MW}(C')$ benutzt wurde. Als Koordinatenring des Lifts von L erhalten wir

$$B := \mathbb{Q}_q[x, H^{-1}(x)] = \sum_{i,j \in \mathbb{N}_0} \mathbb{Q}_q x^i H^{-j}(x) = \sum_{\substack{0 \le i < d \\ j \in \mathbb{Z}}} \mathbb{Q}_q x^i H^j(x)$$

mit nur endlich vielen, von Null verschiedenen Summanden. Dieser Ring entspricht nach (4.2) gerade dem positiven Eigenraum A^+ des gelifteten Koordinatenringes

$A = \mathbb{Q}_q[C'] = \mathbb{Q}_q[x, y, y^{-1}]/(y^2 - H(x))$ von C'. Aufgrund der Identität $B = A^+$ folgt mittels (4.6)

$$\begin{aligned} H^1_{MW}(C')^+ &= H_{dR}((A^+)^\dagger/\mathbb{Q}_q) \\ &= H_{dR}(B^\dagger/\mathbb{Q}_q) \\ &= H^1_{MW}(L). \end{aligned}$$

Die erste Aussage folgt unmittelbar aus der Tatsache, dass der Kern von d sowohl auf $(A^+)^\dagger$ als auch auf $B^\dagger$ gleich $\mathbb{Q}_q$ ist. □

Nun können wir die zentrale Aussage, die wir zur Berechnung der Zetafunktion benutzen, formulieren und beweisen.

Satz 4.7. *Sei $\overline{C}/\mathbb{F}_q$ eine glatte, hyperelliptische Kurve vom Geschlecht g mit einem affinen Teil C, der durch $y^2 = h(x) \in \mathbb{F}_q[x, y]$ definiert wird. Weiterhin bezeichnet C' die zu $C \setminus \{(x, y) \in C \mid y = 0\}$ isomorphe, affine Varietät und $\chi\left(\Phi^* |\ H^1_{MW}(C')^-; t\right)$ das charakteristische Polynom der induzierten q-Frobeniusabbildung Φ^* auf dem negativen Eigenraum der ersten Monsky-Washnitzer-Kohomologiegruppe von C'. Dann ist die Zetafunktion von $\overline{C}$ gegeben durch*

$$\zeta(\overline{C}; t) = \frac{t^{2g}\chi\left(\Phi^* |\ H^1_{MW}(C')^-; \frac{1}{t}\right)}{(1-t)(1-qt)}.$$

Beweis. Es sei L definiert wie in Lemma 4.6 und η_k bezeichne die Anzahl der $\mathbb{F}_{q^k}$-rationalen Weierstraßpunkte von C. Es gilt also $\#C(\mathbb{F}_{q^k}) = \#C'(\mathbb{F}_{q^k}) + \eta_k$ und $\#L(\mathbb{F}_{q^k}) = q^k - \eta_k$. Auf die beiden affinen Varietäten C' und L können wir den Fixpunktsatz von Lefschetz anwenden und erhalten

$$\begin{aligned} \#C'(\mathbb{F}_{q^k}) &= \operatorname{Tr}\left(q^k\Phi^{*-k} | H^0_{MW}(C')\right) - \operatorname{Tr}\left(q^k\Phi^{*-k} | H^1_{MW}(C')\right) \text{ und} \\ \#L(\mathbb{F}_{q^k}) &= \operatorname{Tr}\left(q^k\Phi^{*-k} | H^0_{MW}(L)\right) - \operatorname{Tr}\left(q^k\Phi^{*-k} | H^1_{MW}(L)\right). \end{aligned}$$

Da der projektive Abschluss $\overline{C}$ des affinen Teils C genau einen Punkt im Unendlichen besitzt folgt

$$\begin{aligned} \#\overline{C}(\mathbb{F}_{q^k}) &= \eta_k + 1 + \#C'(\mathbb{F}_{q^k}) \\ &= \eta_k + 1 + \operatorname{Tr}\left(q^k\Phi^{*-k} | H^0_{MW}(C')\right) - \operatorname{Tr}\left(q^k\Phi^{*-k} | H^1_{MW}(C')\right). \end{aligned}$$

Wir wissen bereits, dass die Involution ι den Vektorraum $H^1_{MW}(C')$ in die beiden Eigenräume $H^1_{MW}(C')^+$ und $H^1_{MW}(C')^-$ teilt. Wie wir später in Satz 4.9 sehen werden, sind diese beiden Eigenräume invariant unter Φ^* und damit unter $q^k\Phi^{*-k}$. Die Spuren

auf $H^1_{MW}(C')$ lassen sich also aufspalten und es folgt

$$\begin{aligned}
\#\overline{C}(\mathbb{F}_{q^k}) &= \eta_k + 1 + \mathrm{Tr}\left(q^k\Phi^{*-k}|H^0_{MW}(C')\right) \\
&\quad -\mathrm{Tr}\left(q^k\Phi^{*-k}|H^1_{MW}(C')^+\right) - \mathrm{Tr}\left(q^k\Phi^{*-k}|H^1_{MW}(C')^-\right) \\
&\overset{Lemma\ 4.6}{=} \eta_k + 1 + \underbrace{\mathrm{Tr}\left(q^k\Phi^{*-k}|H^0_{MW}(L)\right) - \mathrm{Tr}\left(q^k\Phi^{*-k}|H^1_{MW}(L)\right)}_{=\#L(\mathbb{F}_{q^k})=q^k-\eta_k} \\
&\quad -\mathrm{Tr}\left(q^k\Phi^{*-k}|H^1_{MW}(C')^-\right) \\
&= q^k + 1 - \mathrm{Tr}\left(q^k\Phi^{*-k}|H^1_{MW}(C')^-\right)
\end{aligned}$$

Die Behauptung folgt nun analog den Rechnungen in Abschnitt 2.2. □

4.4 Der Frobenius auf der Monsky-Washnitzer-Kohomologie

Im vorherigen Abschnitt haben wir gesehen, dass wir die Zetafunktion einer hyperelliptischen Kurve mit Hilfe einer induzierten Frobenius-Abbildung auf ihrer Monsky-Washnitzer-Kohomologie ausdrücken können. Wir haben uns dabei auf die Existenzaussage einer solchen Abbildung auf der Kohomologiegruppe nach Satz 3.3 gestützt. Nun wollen wir diese Abbildung explizit beschreiben. Im Folgenden benutzen wir die Bezeichnung $z := y^{-1}$.

Die Konstruktion beginnt mit der q-Frobenius-Abbildung $\Phi : C' \to C'$ aus Beispiel 1.19, die auf natürliche Weise einen $\mathbb{F}_q$-Algebra-Morphismus auf dem Koordinatenring $\overline{A} = \mathbb{F}_q[x,y,z]/(y^2-h(x), zy-1)$ durch $a \mapsto a^q$ für alle $a \in \overline{A}$ induziert. Unser Ziel ist es, diese Abbildung zu einem $\mathbb{Q}_q$-Algebra-Morphismus $\Phi : A^\dagger \to A^\dagger$ zu liften. Dabei werden wir einen Lift auf den p-adischen Abschluss A^∞_+ von $A_+ = \mathbb{Z}_q[x,y,z]/(y^2-H(x), zy-1)$ konstruieren und zeigen, dass dessen Einschränkung auf die Unteralgebra $A^\dagger_+$ einen Endomorphismus liefert. Diesen können wir dann auf $A^\dagger = A^\dagger_+ \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ fortsetzen und erhalten damit eine induzierte Abbildung auf der de Rham-Kohomologie $H^1_{MW}(C')$ wie in (1.3).

Wir werden im Folgenden alle Lifts und induzierten Abbildungen von Φ wieder mit Φ bezeichnen.

Wir erhalten den q-Frobenius-Automorphismus auf einem endlichen Körper durch n-fache Hintereinanderausführung des p-Frobenius (es gilt $q = p^n$). Selbiges ist auch mit der Abbildung auf $\overline{A}$ möglich. Wir erhalten $\Phi : \overline{A} \to \overline{A}$ durch n-faches Ausführen der Abbildung Φ_p, die jedes Element $a \in \overline{A}$ auf a^p abbildet. Dieses $\Phi_p : \overline{A} \to \overline{A}$ ist zwar nicht mehr $\mathbb{F}_q$-linear, aber zumindest $\mathbb{F}_p$-linear und es existiert ein $\mathbb{Z}_p$-linearer Lift auf $A^\dagger$. Wenn wir eine Darstellungsmatrix von Φ_p berechnet haben, erhalten wir durch Potenzieren eine Darstellungsmatrix von Φ.

Aus algorithmischer Sicht ist diese Faktorisierung von Φ der entscheidende Schritt des Algorithmus, denn die Berechnung des p-Frobenius Φ_p auf die Basis der Kohomologie ist bei weitem nicht so aufwendig wie die Berechnung von Φ. Das hat zur Folge, dass Kedlayas Algorithmus insbesondere für Kurven über Körpern kleiner Charakteristik geeignet ist.

Wir beginnen unsere Konstruktion mit einer Fortsetzung des p-Frobenius von $\mathbb{F}_q$ auf $\mathbb{Q}_q$. Diese haben wir bereits in Satz 1.9 erwähnt und gezeigt, dass wir sie mit einer Newton-Iteration berechnen können (siehe Algorithmus 1). Die Frobenius-Substitution Σ_p ist stetig (im p-adischen Sinne), denn es gilt $v_p(\Sigma_p(\lambda)) = v_p(\lambda)$ für alle $\lambda \in \mathbb{Z}_q$.

Nun wollen wir eine stetige Fortsetzung $\Phi_p : A_+ \to A_+^\infty$ der Frobenius-Substitution definieren und diese anschließend stetig auf ihren p-adischen Abschluss A_+^∞ fortsetzen. Da Φ_p ein $\mathbb{Z}_p$-Algebra-Morphismus werden soll, benötigen wir lediglich die Bilder der Erzeuger x, y und z. Dabei stellen wir folgende Bedingungen:

- Da wir einen Lift der Abbildung $\Phi_p : \overline{A} \to \overline{A}$ suchen, muss gelten:

$$\begin{aligned} \Phi_p(x) &\equiv x^p \mod p, \\ \Phi_p(y) &\equiv y^p \mod p, \\ \Phi_p(z) &\equiv z^p \mod p. \end{aligned}$$

- Die Abbildung muss mit der Faktorstruktur verträglich sein, das heißt, es müssen die Identitäten

$$\Phi_p(y)^2 = \Phi_p(y^2) = \Phi_p(H(x)), \quad \text{und} \tag{4.7}$$

$$\Phi_p(y) \cdot \Phi_p(z) = \Phi_p(yz) = \Phi_p(1) = 1. \tag{4.8}$$

  gelten.

Zunächst fixieren wir das Bild von x. Wir können dabei ein beliebiges Element wählen, welches modulo p gleich x^p ist. Um die Rechnungen einfach zu halten, definieren wir $\Phi_p(x) := x^p$ und betrachten das Bild von $H(x)$ unter Φ_p. Es muss

$$\Phi_p(H(x)) \equiv H^p(x) \mod p$$

gelten und es folgt, dass die Differenz von $\Phi_p(H(x))$ und $H^p(x)$ in $\mathbb{Z}_q[x]$ durch p teilbar ist. Wir definieren

$$E(x) := \frac{\Phi_p(H(x)) - H^p(x)}{p} \in \mathbb{Z}_q[x]$$

und erhalten mit den Bedingungen (4.7) und (4.8):

$$\Phi_p(y)^2 = \Phi_p(H(x)) = H^p(x) + pE(x) = y^{2p} + pE(x) = y^{2p}(1 + pE(x)z^{2p}) \in A_+^\infty,$$

$$\Phi_p(z)^2 = \left(\Phi_p(y)^2\right)^{-1} = \left(y^{2p}(1 + pE(x)z^{2p})\right)^{-1} = z^{2p}\left(1 + pE(x)z^{2p}\right)^{-1} \in A_+^\infty.$$

Um die Bilder von y und z zu bestimmen, müssen wir also die (inverse) Quadratwurzel aus $1 + pE(x)z^{2p}$ ziehen. Die Existenz dieser Wurzeln in A_+^∞ sichert Hensels Lemma, denn reduziert modulo p existieren diese Wurzeln. Wir können die Wurzeln in Taylor-Reihen entwickeln:

$$\left(1 + pE(x)z^{2p}\right)^{1/2} = \sum_{k=0}^{\infty} \binom{1/2}{k} p^k E^k(x) z^{2pk} \in A_+^\infty,$$
$$\left(1 + pE(x)z^{2p}\right)^{-1/2} = \sum_{k=0}^{\infty} \binom{-1/2}{k} p^k E^k(x) z^{2pk} \in A_+^\infty,$$

wobei der Ausdruck $\binom{t}{k}$ für $\frac{t(t-1)\cdot\ldots\cdot(t-k+1)}{k!}$ steht. Damit können wir den $\mathbb{Z}_p$-Algebra-Homomorphismus vollständig beschreiben:

$$\begin{aligned}
\Phi_p : A_+ &\to A_+^\infty, \\
\lambda &\mapsto \Sigma_p(\lambda), \text{ für } \lambda \in \mathbb{Z}_q, \\
x &\mapsto x^p, \\
y &\mapsto y^p \sum_{k=0}^{\infty} \binom{1/2}{k} p^k E^k(x) z^{2pk}, \\
z &\mapsto z^p \sum_{k=0}^{\infty} \binom{-1/2}{k} p^k E^k(x) z^{2pk}.
\end{aligned}$$

Um die Stetigkeit dieser Abbildung zu zeigen, müssen wir lediglich nachweisen, dass jedes Element $a \in pA_+$ auf ein Element in pA_+^∞ abgebildet wird. Mit der Darstellung

$$\begin{aligned}
\binom{-1/2}{k} &= \frac{-\frac{1}{2}(-\frac{1}{2}-1)(-\frac{1}{2}-2)\cdot\ldots\cdot(-\frac{1}{2}-k+1)}{k!} \\
&= \frac{(-1)^k}{2^k} \cdot \frac{1\cdot 3\cdot 5\cdot\ldots\cdot(2k-1)}{k!} \cdot \frac{2^k k!}{2^k k!} \\
&= \frac{(-1)^k}{2^{2k}} \cdot \frac{(2k)!}{k!k!} \\
&= \frac{(-1)^k}{2^{2k}} \cdot \binom{2k}{k}
\end{aligned}$$

sehen wir, dass $\binom{-1/2}{k} \in \mathbb{Z}_q$ und analog $\binom{1/2}{k} \in \mathbb{Z}_q$ für alle $k \in \mathbb{N}$ gilt. Da auch die Koeffizienten von E^k in $\mathbb{Z}_q$ liegen, lässt sich die Stetigkeit der Abbildung unmittelbar aus ihrer Definition erkennen.

Nun wollen wir diese Abbildung auf A_+^∞ fortsetzen. Da A_+ dicht in A_+^∞ liegt, können wir Φ_p stetig auf A_+^∞ fortsetzen, indem wir

$$\Phi_p\left(\sum_{\substack{0\le i\le 2g \\ j\in\mathbb{Z}}} a_{i,j}x^i y^j\right) := \sum_{\substack{0\le i\le 2g \\ j\in\mathbb{Z}}} \Phi_p\left(a_{i,j}x^i y^j\right) \quad \text{für alle } \sum_{\substack{0\le i\le 2g \\ j\in\mathbb{Z}}} a_{i,j}x^i y^j \in A_+^\infty$$

definieren. Der nächste Satz sagt uns, dass dieses Φ_p auch einen Endomorphismus auf der gewünschten Algebra $A^\dagger$ liefert.

Satz 4.8 (p-Frobenius auf $A^\dagger$)**.** *Es gelten die Definitionen wie oben. Dann ist der durch*

$$\begin{aligned}
\Phi_p : A^\dagger &\to A^\dagger, \\
\lambda &\mapsto \Sigma_p(\lambda), \text{ für } \lambda \in \mathbb{Z}_q, \\
x &\mapsto x^p, \\
y &\mapsto y^p \sum_{k=0}^{\infty} \binom{1/2}{k} p^k E^k(x) z^{2pk}, \\
z &\mapsto z^p \sum_{k=0}^{\infty} \binom{-1/2}{k} p^k E^k(x) z^{2pk}.
\end{aligned}$$

definierte $\mathbb{Z}_p$-Algebra-Endomorphismus ein Lift der Abbildung $\Phi_p : \overline{A} \to \overline{A}$, die jedes Element auf seine p-te Potenz abbildet.

Beweis. Dass die definierte Abbildung ein Lift von $\Phi_p : \overline{A} \to \overline{A}$ ist, folgt aus der Konstruktion. Außerdem haben wir bereits gesehen, dass die gegebenen Abbildungsvorschriften einen $\mathbb{Z}_p$-Algebra-Endomorphismus auf A_+^∞ definieren.

Es bleibt also zu zeigen, dass die Einschränkung auf die Unteralgebra $A_+^\dagger$ eine Selbstabbildung ist und sich damit als Endomorphismus auf $A^\dagger$ fortsetzen lässt. Wir betrachten zunächst die Bilder von $x, y, z \in A_+^\dagger$.

Offensichtlich gilt $\Phi_p(x) = x^p \in A_+^\dagger$. Kommen wir nun zu dem Bild von z. Aufgrund der Konstruktion ist klar, dass $\deg E < p(2g+1)$ gilt und wir können die auftretenden Polynome $E^k(x)$ schreiben als

$$E^k(x) = \sum_{i=0}^{kp(2g+1)} E_{k,i} x^i \quad \text{mit } E_{k,i} \in \mathbb{Z}_q.$$

Es folgt die Darstellung

$$\Phi_p(z) = \sum_{k=0}^{\infty} \sum_{i=0}^{kp(2g+1)} \binom{-1/2}{k} p^k E_{k,i} x^i z^{2pk+p}$$

und wir erhalten die Abschätzung

$$\liminf_{\substack{i+2pk\to\infty \\ i\le kp(2g+1)}} \frac{v_p\left(\binom{-1/2}{k} p^k E_{k,i}\right)}{i+2pk+p} \ge \liminf_{k\to\infty} \frac{k}{i+2pk+p} = \frac{1}{2p} > 0.$$

Diese Abschätzung zeigt gerade die Überkonvergenz der Reihe und damit $\Phi_p(z) \in A_+^\dagger$ nach (3.1). Ganz analog lässt sich zeigen, dass auch $\Phi_p(y) \in A_+^\dagger$ gilt und wir können

schließen, dass auch jedes Monom der Form $a_{i,j}x^iy^j$ ($i \in \mathbb{N}_0$, $j \in \mathbb{Z}$, $a_{i,j} \in \mathbb{Z}_q$) in $A_+^\dagger$ liegt.

Es bleibt zu zeigen, dass auch unendliche Summen aus $A_+^\dagger$ nach $A_+^\dagger$ abgebildet werden. Wenn wir die Identität $y^2 = H(x)$ nutzen, können wir mit der Abschätzung $\deg E^k < kp(2g+1)$ die Darstellungen

$$\Phi_p(y) = y^p \sum_{\substack{0\le k\le 2g\\ l\in\mathbb{N}_0}} p^l\lambda_{k,l}x^kz^{2l} \quad \text{und} \tag{4.9}$$

$$\Phi_p(z) = z^p \sum_{\substack{0\le k\le 2g\\ l\in\mathbb{N}_0}} p^l\mu_{k,l}x^kz^{2l}, \tag{4.10}$$

mit $\lambda_{i,j}, \mu_{i,j} \in \mathbb{Z}_q$ wählen.

Nun sei ein beliebiges $a \in A_+^\dagger$ gegeben, dann erhalten wir aufgrund der Stetigkeit von Φ_p eine Darstellung der Form

$$\begin{aligned}\Phi_p(a(x,y)) &= \sum_{\substack{0\le i\le 2g\\ j\in\mathbb{Z}}} a_{i,j}x^{ip}\Phi_p(y)^j \\ &= \sum_{\substack{0\le i\le 2g\\ j\in\mathbb{N}}} a_{i,-j}x^{ip}\Phi_p(z)^j + \sum_{0\le i\le 2g} a_{i,0}x^{ip} + \sum_{\substack{0\le i\le 2g\\ j\in\mathbb{N}}} a_{i,j}x^{ip}\Phi_p(y)^j. \end{aligned}\tag{4.11}$$

Wir betrachten die drei Summanden einzeln. Der Mittlere ist offensichtlich in $A^\dagger$. Mit (4.9) ist der dritte Summand gleich

$$\sum_{i=0}^{2g}\sum_{j=1}^{\infty} a_{i,j}x^{ip}y^{jp}\left(\sum_{l=0}^{\infty} p^l\lambda_{0,l}x^0z^{2l} + \ldots + \sum_{l=0}^{\infty} p^l\lambda_{2g,l}x^{2g}z^{2l}\right)^j$$

und wir erhalten mit dem Multinomialsatz (angewandt auf die j-te Potenz des geklammerten Ausdrucks)

$$\sum_{i=0}^{2g}\sum_{j=1}^{\infty} a_{i,j}x^{ip}y^{jp} \underbrace{\sum_{\alpha_0+\ldots+\alpha_{2g}=j} \binom{j}{\alpha_0,\ldots,\alpha_{2g}} \prod_{k=0}^{2g}\left(\sum_{l=0}^{\infty} p^l\lambda_{k,l}x^kz^{2l}\right)^{\alpha_k}}_{=:\circledast}. \tag{4.12}$$

Hierbei gilt die Bezeichnung $\binom{j}{\alpha_0,\ldots,\alpha_{2g}} := \frac{j!}{\alpha_0!\cdot\ldots\cdot\alpha_{2g}!}$, wobei die α_i aus $\mathbb{N}_0$ kommen. Wir stellen fest, dass diese Multinomialkoeffizienten ganzzahlige Werte annehmen und deshalb in $\mathbb{Z}_q$ liegen.

Im Folgenden werden wir die Schreibweise noch etwas verkürzen und definieren den Multiindex $\alpha := (\alpha_0,\ldots,\alpha_{2g}) \in \mathbb{N}_0^{2g+1}$ und $|\alpha| := \alpha_0 + \ldots + \alpha_{2g}$. Für den Teil $\circledast$ gilt dann

$$\circledast = \sum_{|\alpha|=j} \binom{j}{\alpha} \prod_{k=0}^{2g}\left(\sum_{l=0}^{\infty} p^l\lambda_{k,l}x^kz^{2l}\right)^{\alpha_k}$$

und mit der Schreibweise $\sigma_\alpha := \sum_{k=0}^{2g} k\alpha_k$ folgt

$$\begin{aligned}\sum_{|\alpha|=j}\binom{j}{\alpha}\prod_{k=0}^{2g}\left(\sum_{l=0}^{\infty}p^l\lambda_{k,l}x^kz^{2l}\right)^{\alpha_k} &= \sum_{|\alpha|=j}\binom{j}{\alpha}x^{\sigma_\alpha}\prod_{k=0}^{2g}\left(\sum_{l=0}^{\infty}p^l\lambda_{k,l}z^{2l}\right)^{\alpha_k}\\ &= \sum_{|\alpha|=j}\binom{j}{\alpha}x^{\sigma_\alpha}\prod_{k=0}^{2g}\left(\sum_{l=0}^{\infty}p^l\mu_{k,l,\alpha}z^{2l}\right),\end{aligned}$$

wobei die $\mu_{k,l,\alpha}$ geeignete Elemente aus $\mathbb{Z}_q$ sind, die wir aus den $\lambda_{k,l}$ berechnen können. Nun lösen wir das Produktzeichen auf und erhalten

$$\sum_{|\alpha|=j}\binom{j}{\alpha}x^{\sigma_\alpha}\prod_{k=0}^{2g}\left(\sum_{l=0}^{\infty}p^l\mu_{k,l,\alpha}z^{2l}\right) = \sum_{|\alpha|=j}\binom{j}{\alpha}x^{\sigma_\alpha}\left(\sum_{l=0}^{\infty}p^l\eta_{l,\alpha}z^{2l}\right),$$

mit geeigneten $\eta_{l,\alpha}$, die wir aus den $\mu_{k,l,\alpha}$ gewinnen und die wiederum in $\mathbb{Z}_q$ liegen. Dieses Ergebnis setzen wir nun in (4.12) ein:

$$\begin{aligned}(4.12) &= \sum_{i=0}^{2g}\sum_{j=1}^{\infty}a_{i,j}x^{ip}y^{jp}\sum_{|\alpha|=j}\binom{j}{\alpha}x^{\sigma_\alpha}\left(\sum_{l=0}^{\infty}p^l\eta_{l,\alpha}z^{2l}\right)\\ &= \sum_{i=0}^{2g}\sum_{j=1}^{\infty}\sum_{|\alpha|=j}\sum_{l=0}^{\infty}a_{i,j}x^{ip}y^{jp}\binom{j}{\alpha}x^{\sigma_\alpha}p^l\eta_{l,\alpha}z^{2l}\\ &= \sum_{i=0}^{2g}\sum_{j=1}^{\infty}\sum_{|\alpha|=j}\sum_{l=0}^{\infty}\binom{j}{\alpha}\eta_{l,\alpha}a_{i,j}p^lx^{ip+\sigma_\alpha}z^{2l-jp}. \qquad (4.13)\end{aligned}$$

Wir müssen nun zeigen, dass dieser Ausdruck eine überkonvergente Reihe beschreibt. Dazu müssen wir die Indizes j und l gegen Unendlich laufen lassen und die Bewertung der Koeffizienten der entsprechenden Monome betrachten.

Nach Voraussetzung gilt $a \in A_+^\dagger$, es existiert also ein $\varepsilon > 0$, so dass

$$\liminf_{i+|j|\to\infty}\frac{v_p(a_{i,j})}{i+|j|} = \varepsilon > 0.$$

Außerdem wissen wir, dass $\binom{j}{\alpha}\eta_{l,\alpha}$ in $\mathbb{Z}_q$ liegt und damit eine nichtnegative p-Bewertung besitzt. Wenn wir weiterhin bedenken, dass $\sigma_\alpha = \sum_{k=0}^{2g} k\alpha_k$ nach oben durch $K|\alpha| = Kj$ mit einer Konstanten $K \geq 2$ abgeschätzt werden kann, folgt für die Bewertungen

$$\liminf_{|ip+\sigma_\alpha|+|2l-jp|\to\infty}\frac{v_p\left(\binom{j}{\alpha}\eta_{l,\alpha}a_{i,j}p^l\right)}{|ip+\sigma_\alpha|+|2l-jp|} \geq \liminf_{ip+Kj+|2l-jp|\to\infty}\frac{v_p(a_{i,j})+l}{2gp+Kj+2l+jp}.$$

Der Index geht genau dann gegen Unendlich, wenn j oder l gegen Unendlich gehen. Wir fixieren zunächst $j \in \mathbb{N}$ und erhalten

$$\liminf_{l\to\infty}\frac{v_p(a_{i,j})+l}{2gp+Kj+2l+jp} = \frac{1}{2} > 0.$$

Für ein fixiertes $l \in \mathbb{N}_0$ gilt

$$\liminf_{j\to\infty} \frac{v_p(a_{i,j})+l}{2gp+Kj+2l+jp} = \frac{\varepsilon}{K+p} > 0.$$

Nun müssen wir noch den Fall betrachten, dass j und l gleichzeitig gegen Unendlich streben:

$$\begin{aligned}
\liminf_{j,l\to\infty} \frac{v_p(a_{i,j})+l}{2gp+Kj+2l+jp} &\geq \liminf_{j,l\to\infty} \frac{v_p(a_{i,j})+l}{2gp+(K+p)(j+l)} \\
&= \liminf_{j,l\to\infty} \frac{v_p(a_{i,j})/j+l/j}{2gp/j+(K+p)(1+l/j)} \\
&= \begin{cases} \frac{\varepsilon+C}{(K+p)(1+C)} > 0, \text{ falls } \lim \frac{l}{j} =: C \in \mathbb{R} \\ \frac{1}{K+p} > 0, \text{ sonst} \end{cases},
\end{aligned}$$

Für den ersten Summanden aus (4.11) können wir analog vorgehen und haben damit gezeigt, dass jedes Element $a(x,y) \in A_+^\dagger$ nach $A_+^\dagger$ abgebildet wird und Φ_p somit ein $\mathbb{Z}_p$-Algebra-Endomorphismus auf $A_+^\dagger$ ist. Dieser lässt sich natürlich auf $A^\dagger = A_+^\dagger \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ fortsetzen und der Satz ist vollständig bewiesen. □

Dieser Endomorphismus induziert wie in (1.3) eine Abbildung auf dem Differentialmodul und liefert damit den gewünschten Endomorphismus auf der ersten de Rham-Kohomologiegruppe $H^1_{MW}(C')$, den wir wieder mit Φ_p bezeichnen.

In Satz 4.7 haben wir gesehen, dass wir zur Berechnung der Zetafunktion das charakteristische Polynom von Φ auf dem Eigenraum $H^1_{MW}(C')^-$ benötigen. Eine Begründung dafür, dass Φ eine Selbstabbildung auf den beiden Eigenräumen von $H^1_{MW}(C')$ ist, sind wir dabei schuldig geblieben. Diese holen wir nun nach.

Lemma 4.9. *Die beiden Eigenräume $H^1_{MW}(C')^+$ und $H^1_{MW}(C')^-$ sind invariant unter Φ_p und Φ.*

Beweis. Wir wollen zunächst zeigen, dass die Abbildungen Φ_p und ι kommutieren. Sowohl Φ_p, als auch ι sind stetige $\mathbb{Q}_q$-Algebra-Endomorphismen auf $A^\dagger$ und es gilt für beliebige $\sum a_{i,j}x^iy^j dx \in H^1_{MW}(C')$:

$$\begin{aligned}
\Phi_p \circ \iota \left(\sum a_{i,j}x^iy^j dx\right) &= \Phi_p \left(\sum a_{i,j}x^i(-y)^j dx\right) \\
&= \sum \Sigma_p(a_{i,j})x^{ip}\big(\underbrace{-\Phi_p(y)}_{=\iota(\Phi_p(y))}\big)^j dx \\
&= \iota \left(\sum \Sigma_p(a_{i,j})x^{ip}(\Phi_p(y))^j dx\right) \\
&= \iota \circ \Phi_p \left(\sum a_{i,j}x^iy^j dx\right).
\end{aligned}$$

Damit folgt

$$\Phi_p(H^1_{MW}(C)^+) = \Phi_p(\iota(H^1_{MW}(C)^+)) = \iota(\Phi_p(H^1_{MW}(C)^+))$$
$$\Rightarrow \Phi_p(H^1_{MW}(C)^+) \subseteq H^1_{MW}(C)^+$$

und

$$\Phi_p(H^1_{MW}(C)^-) = \Phi_p(\iota(H^1_{MW}(C)^-)) = \iota(\Phi_p(H^1_{MW}(C)^-))$$
$$\Rightarrow \Phi_p(H^1_{MW}(C)^-) \subseteq H^1_{MW}(C)^-.$$

Da Φ der n-fachen Ausführung von Φ_p entspricht, folgt die Invarianz unter Φ. □

Mit diesen Ergebnissen sind wir in der Lage eine Darstellungsmatrix $M_p \in \mathbb{Q}_q^{2g\times 2g}$ von Φ_p auf $H^1_{MW}(C')^-$ zu bestimmen.

Um daraus eine Darstellungsmatrix M von $\Phi = \Phi_p^n$ zu erhalten, müssen wir bedenken, dass Φ_p lediglich $\mathbb{Z}_p$-linear ist und für ein beliebiges $\lambda \in \mathbb{Q}_q$

$$\Phi_p(\lambda x^i \frac{dx}{y}) = \Sigma_p(\lambda)\Phi_p(x^i \frac{dx}{y}) \tag{4.14}$$

gilt. Diese Eigenschaft nennen wir auch Σ_p-*Linearität*. Für die Darstellungsmatrix von Φ folgt damit

$$M = M_p M_p^{\Sigma_p} \cdot \ldots \cdot M_p^{\Sigma_p^{n-1}}, \tag{4.15}$$

wobei $M_p^{\Sigma_p^k}$ für die k-fache Anwendung des p-Frobenius auf die Koeffizienten von M_p steht.

4.5 Der Algorithmus

In diesem Abschnitt wollen wir beschreiben, wie wir mit den Ergebnissen der vorherigen Abschnitte die Zetafunktion einer hyperelliptischen Kurve berechnen. Der Algorithmus wurde in KASH3 implementiert und getestet.

4.5.1 p-adische Arithmetik

Fast alle Berechnungen des Algorithmus laufen in p-adischen Strukturen ab, genauer gesagt in Polynomringen über $\mathbb{Q}_q$ oder in $\mathbb{Q}_q$ selbst. Der Körper $\mathbb{Q}_q$ ist eine Erweiterung von $\mathbb{Q}_p$ und wird durch ein irreduzibles Polynom $U \in \mathbb{Q}_p[v]$ vom Grad n erzeugt, das heißt, es gilt die Isomorphie $\mathbb{Q}_q \cong \mathbb{Q}_p[v]/(U)$ und wir können jedes Element aus $\mathbb{Q}_q$ eindeutig darstellen als Polynom aus $\mathbb{Q}_p[v]$ mit einem Grad kleiner als n.

Da die Elemente von $\mathbb{Q}_p$ eine unendliche Darstellung besitzen, können wir nicht mit exakten Werten rechnen, sondern müssen uns mit einer gewissen p-adischen Präzision begnügen. Wir werden also zu Beginn eine geeignete Präzision wählen und im Anschluss

alle auftretenden Elemente $\sum_{k=\nu}^{\infty} a_k p^k \in \mathbb{Q}_p$ nur bis zu einem gewissen Index k speichern.

Die von KASH3 bereitgestellte Arithmetik in $\mathbb{Q}_p$ bereitete teilweise Probleme. So ist es beispielsweise nicht möglich, Determinanten von Matrizen über $\mathbb{Q}_q[x]$ zu berechnen. Außerdem wurde in vielen Fällen ein fehlerhafter Umgang mit den (relativen) p-adischen Präzisionen festgestellt. Wir haben uns deshalb für die Darstellung der Elemente in $\mathbb{Z}_q$ entschieden, wo KASH3 mit einer fixierten absoluten Präzision rechnet. Dabei treten jedoch neue Probleme auf, denn nicht alle auftretenden Elemente liegen tatsächlich in $\mathbb{Z}_q$. Wie wir später sehen werden, ist es allerdings möglich, ein $\mu \in \mathbb{N}$ zu bestimmen, so dass alle Rechnungen in $p^{-\mu}\mathbb{Z}_q$ stattfinden. Wir werden also alle auftretenden Elemente mit p^μ multiplizieren und können damit alle Berechnungen in $\mathbb{Z}_q$ durchführen. Ein Nachteil der $\mathbb{Z}_q$-Arithmetik in KASH3 ist, dass wir Divisionen durch p etwas umständlich durchführen müssen, denn p ist keine Einheit in $\mathbb{Z}_q$ und es bedarf jedes mal eines Teilbarkeitstests.

4.5.2 Darstellung der Differentiale

Wir müssen noch klären, wie wir die auftretenden Differentiale aus $\Omega^-_{A^\dagger/\mathbb{Q}_q}$ speichern. Jedes Differential aus $\Omega^-_{A^\dagger/\mathbb{Q}_q}$ lässt sich als $a(x,y,z)zdx$ mit $a \in \mathbb{Q}_q[x, y^2, z^2]$ darstellen und mit den Identitäten $yz = 1$, $y^2 = H(x)$ und $z^2H(x) = 1$ können wir jedes a schreiben als

$$a(x,z) = a_0(x) + \sum_{k\geq 1} a_k(x) z^{2k},$$

mit $\deg a_k \leq 2g$ für alle $k \geq 1$. In dieser Form werden wir die auftretenden Differentiale speichern. Alle Berechnungen, die wir mit Polynomen dieser Form durchführen, liefern wieder Polynome dieser Form, allerdings ohne die Gradbeschränkungen für a_k mit positivem Index k. Wir werden dann das gesamte Polynom modulo $Hz^2 - 1$ reduzieren, um wieder die gewünschte Darstellung zu erhalten.

Das Umrechnen in diese Form nimmt bei Polynomen mit hohen Potenzen zwar eine beträchtliche Zeit in Anspruch, wird aber durch die Vereinfachung der weiteren Rechnungen mehr als kompensiert.

4.5.3 Präzisionsfragen

In diesem Abschnitt wollen wir klären, mit welchen Präzisionen wir arbeiten müssen, um am Ende korrekte Ergebnisse zu erhalten. Konkret stellen wir uns folgende Fragen:

- Welche p-adische Präzision wählen wir für die Darstellung der Elemente aus $\mathbb{Z}_q$? Das heißt, wie groß müssen wir $N \in \mathbb{N}$ wählen, so dass wir in $\mathbb{Z}_q/p^N\mathbb{Z}_q$ rechnen können?

- Bei der Berechnung des p-Frobenius auf die Basiselemente tritt eine Reihendarstellung auf. Wieviele Summanden davon müssen wir berechnen?

Zunächst überlegen wir uns, welche Präzision wir für die korrekte Darstellung des gesuchten L-Polynoms benötigen. In der Schreibweise $L(t) = \sum_{i=0}^{2g} a_i t^i$ erhalten wir mit Korollar 2.3 die Abschätzung

$$|a_i| \leq \binom{2g}{i} q^{i/2} \leq 2^{2g} q^{i/2}.$$

Des Weiteren sagt uns Korollar 2.3, dass wir aus den Koeffizienten $a_0, \ldots, a_g$ mittels $a_{2g-i} = q^{g-i} a_i$ die restlichen Koeffizienten berechnen können. Wenn wir außerdem bedenken, dass wir aufgrund des Vorzeichens die Präzision verdoppeln müssen, benötigen wir das L-Polynom modulo p^{N_1} korrekt, wobei N_1 eine natürliche Zahl ist mit

$$p^{N_1} > 2 \cdot 2^{2g} q^{g/2}.$$

Es genügt allerdings nicht, mit dieser Präzision N_1 alle Rechnungen durchzuführen, da wir an mehreren Stellen im Algorithmus Präzision verlieren werden und das Ergebnis damit nicht mehr korrekt wäre.

Um ein geeignetes N zu bestimmen, sehen wir uns noch einmal die Wirkung des p-Frobenius auf die Basiselemente von $H^1_{MW}(C')^-$ an:

$$\Phi_p(x^i z dx) = \sum_{k=0}^{\infty} p^{k+1} \underbrace{\binom{-\frac{1}{2}}{k} x^{pi+p-1} E(x)^k}_{=:a_k^{(i)}(x)} z^{2pk+p-1} z dx.$$

Wie bereits gesehen, liegen die $a_k^{(i)}$ in dieser Darstellung in $\mathbb{Z}_q[x]$. Da der Grad von $E(x)$ maximal $p(2g+1)-1$ ist, haben wir für die Grade der $a_k^{(i)}$ folgende Abschätzung:

$$\begin{aligned} \deg(a_k^{(i)}) &= pi + p - 1 + \deg(E^k) \\ &\leq p(i+1) - 1 + k(p(2g+1)-1) \\ &\leq 2pg + 2kpg + kp - k - 1 \\ &< 2pg + 2kpg + kp + p \\ &= (k+1)(2g+1)p \end{aligned} \tag{4.16}$$

Wobei wir für die letzten beiden Ungleichungen $i + 1 \leq 2g$ und $-k - 1 < p$ benutzt haben.

Bevor der Reduktionsalgorithmus beginnt, senken wir die x-Grade, indem wir die Identität $H(x) = y^2 = z^{-2}$ benutzen. Das heißt, wir reduzieren modulo $H(x)z^2 - 1$ und

erhalten dank der Gradabschätzung (4.16) eine untere Schranke für die z-Potenzen und damit eine Darstellung der Form

$$\Phi_p(x^i z dx) = \sum_{k=0}^{\infty} p^{k+1} \sum_{\substack{l=-p+1 \\ l \text{ gerade}}}^{(2k+1)p-1} \bar{a}_{k,l}^{(i)}(x) z^l z dx, \tag{4.17}$$

wobei die $\bar{a}_{k,l}^{(i)}$ aus $\mathbb{Z}_q[x]$ mit maximalem Grad $2g$ sind. Nun reduzieren wir (4.17) auf

$$\sum_{k=0}^{\infty} p^{k+1} \hat{a}_k^{(i)}(x) z dx \tag{4.18}$$

mit $\deg \hat{a}_k^{(i)} \leq 2g-1$. In Lemma 4.4 haben wir gezeigt, dass für die Reduktion von $a(x)z^m z dx$ zu $b(x)z dx$ die Ganzheitsaussagen

$$p^{\lfloor \log_p(m-1) \rfloor} b \in \mathbb{Z}_q[x] \text{ für } m > 0 \text{ und}$$
$$p^{\lfloor \log_p((2g+1)|m|+2g-1) \rfloor} b \in \mathbb{Z}_q[x] \text{ für } m < 0$$

gelten. Wenn wir

$$m_k := \max\{\lfloor \log_p((2k+1)p-2) \rfloor, \lfloor \log_p((2g+1)p-2) \rfloor\}$$

wählen, gilt also $p^{m_k} \hat{a}_k^{(i)}(x) \in \mathbb{Z}_q[x]$. Selbst wenn wir den Faktor p^{k+1} mit in Betracht ziehen, stellen wir fest, dass nicht alle Koeffizienten der Darstellung (4.18) zwangsläufig in $\mathbb{Z}_q$ liegen, denn für die minimal auftretende Bewertung gilt

$$\begin{aligned} \min_{k \in \mathbb{N}_0}\{k+1-m_k\} &= 1 - \lfloor \log_p((2g+1)p-2) \rfloor \\ &= -\lfloor \log_p(2g+1-2/p) \rfloor \\ &=: -\mu \end{aligned}$$

und diese Zahl kann negative Werte annehmen. Wenn wir Φ_p auf die Basiselemente $p^\mu x^i z dx$ berechnen, können wir also gewährleisten, dass alle Rechnungen in $\mathbb{Z}_q$ ablaufen. Dadurch müssen wir μ zusätzliche Stellen speichern und setzen deshalb

$$N_2 := N_1 + \mu.$$

Die Tatsache, dass die Matrixeinträge des p-Frobenius im Allgemeinen nicht in $\mathbb{Z}_q$ sind, stellt uns allerdings noch vor ein anderes Problem, denn schließlich sind wir an der Darstellungsmatrix M des q-Frobenius $\Phi = \Phi_p^n$ interessiert und diese erhalten wir durch potenzieren der p-Frobenius-Matrix M_p. Die p-Potenz, mit der wir die Matrix M multiplizieren müssten, um Einträge aus $\mathbb{Z}_q$ zu erhalten, würde sich vervielfachen und wir müssten die Präzision um entsprechend viele Stellen erhöhen. Einen Ausweg liefert uns das folgende Lemma.

Lemma 4.10. *Es bezeichne A den $\mathbb{Z}_q$-Modul $\oplus_{0\le i\le 2g-1}\mathbb{Z}_q \cdot x^i z dx \subseteq H^1_{MW}(C')^-$ und es sei t eine Uniformisierende der Stelle P_∞, die von der hyperelliptischen Involution fixiert wird (zum Beispiel $t := x^g z$). Außerdem bezeichne L den $\mathbb{Z}_q$-Untermodul von A, dessen Elemente, aufgefasst als Elemente in $(t^{-2g}\mathbb{Z}_q[[t]]dt)/(t^{-1}\mathbb{Z}_q[[t]]dt)$, integrierbar sind. Das heißt, L ist der Schnitt des Bildes der Derivation*

$$d : \frac{t^{-2g+1}\mathbb{Z}_q[[t]]}{\mathbb{Z}_q[[t]]} \to \frac{t^{-2g}\mathbb{Z}_q[[t]]dt}{t^{-1}\mathbb{Z}_q[[t]]dt}$$

mit A. Dann ist der $\mathbb{Z}_q$-Modul L invariant unter $\Phi_p : H^1_{MW}(C')^- \to H^1_{MW}(C')^-$.

Beweisskizze. Siehe [Edi03, S. 18] □

Das Lemma besagt, dass die Darstellungsmatrix von Φ_p bezüglich einer Basis von L Koeffizienten aus $\mathbb{Z}_q$ besitzt. Das heißt, wir können durch eine geeignete Basistransformation eine p-Frobenius-Matrix erhalten, deren Koeffizienten in $\mathbb{Z}_q$ liegen. Wie wir eine solche Transformation erhalten, werden wir später detailliert sehen. Außerdem werden wir sehen, dass durch diese Transformation lediglich ein Präzisionsverlust von $\lfloor \log_p(2g-1) \rfloor$ Stellen anfällt.

Insgesamt benötigen wir für die Basisdarstellung der $\Phi_p\left(p^\mu x^i z dx\right)$ also

$$\begin{aligned} N_3 &:= N_2 + \lfloor \log_p(2g-1) \rfloor \\ &= \lceil \log_p(2^{2g+1} q^{g/2}) \rceil + \lfloor \log_p(2g+1-2/p) \rfloor + \lfloor \log_p(2g-1) \rfloor \end{aligned}$$

p-adische Stellen. Wir merken an, dass dies die benötigte Präzision nach dem Reduktionsalgorithmus ist. Wir müssen noch zusätzliche Stellen speichern, um den Präzisionsverlust, der bei der Reduktion anfällt, zu kompensieren. Zunächst wollen wir aber klären, bis zu welchem Index M wir die Reihendarstellung

$$\Phi_p(p^\mu x^i z dx) = \sum_{k=0}^{\infty} p^{\mu+k+1} a_k^{(i)}(x) z^{2pk+p-1} z dx = \sum_{k=0}^{\infty} p^{\mu+k+1} \sum_{\substack{l=-p+1 \\ l \text{ gerade}}}^{(2k+1)p-1} \bar{a}_{k,l}^{(i)}(x) z^l z dx$$

berechnen müssen.

Der k-te Summand ist hier offensichtlich durch $p^{\mu+k+1}$ und, nach der Reduktion gemäß unseren Abschätzungen, noch durch $p^{\mu+k+1-m_k}$ teilbar (in $\mathbb{Z}_q[x]$). Wir wissen bereits, dass wir nur die Summanden benötigen, deren Reduktion Informationen über die ersten N_3 Stellen liefert, also alle Summanden, deren Index k der Ungleichung

$$\mu + k + 1 - m_k < N_3$$

genügt. Es reicht also, die Reihe bis zum Index M zu berechnen, wobei wir

$$M := \max\{k \in \mathbb{N} \mid \mu + k + 1 - m_k < N_3\} \tag{4.19}$$

setzen. Daraus können wir unmittelbar folgern, dass wir insgesamt die Präzision

$$N := N_3 + \max\{m_k \mid k = 0, \ldots, M\} \tag{4.20}$$

benötigen. Das heißt, wir erhalten das korrekte L-Polynom, wenn alle Berechnungen in $\mathbb{Z}_q$ modulo p^N stattfinden.

4.5.4 Die Schritte des Algorithmus

In diesem Abschnitt wollen wir auf die einzelnen Schritte des Algorithmus eingehen. Dem Algorithmus wird beim Start ein Polynom $h \in \mathbb{F}_q[x]$ vom Grad $2g+1$ mit einfachen Nullstellen übergeben, welches die hyperelliptische Kurve C durch $y^2 = h(x)$ erzeugt.

Initialisierung

Im ersten Schritt des Algorithmus berechnen wir die benötigten Präzisionen, das heißt wir bestimmen $M, N \in \mathbb{N}$ wie in (4.19) beziehungsweise (4.20). Dann erzeugen wir den Ring $\mathbb{Z}_q$ mit der absoluten Präzision N als Erweiterung von $\mathbb{Z}_p$ vom Grad n, indem wir das definierende Polynom u von $\mathbb{F}_q$ nach $U \in \mathbb{Z}_p[v]$ liften und $\mathbb{Z}_q := \mathbb{Z}_p[v]/(U)$ definieren. Zur Bestimmung des Lifts wählen wir für die Koeffizienten von u die Vertreter $0, \ldots, p-1$ und betten diese in $\mathbb{Z}_p$ ein. Auf dieselbe Weise liften wir das Polynom $h \in \mathbb{F}_q[x]$ nach $H \in \mathbb{Z}_q[x]$.

Frobeniusberechnung

Um den p-Frobenius auf die Basiselemente $x^i z dx$ $(i = 0, \ldots, 2g-1)$ zu berechnen, benötigen wir zunächst die Frobenius-Substitution aus Satz 1.9, die wir mit einer Newton-Iteration gemäß Satz 1.11 bestimmen können.

Algorithmus 1 : Frobenius-Substitution

Eingabe : $U \in \mathbb{Z}_p[v]$, so dass $\mathbb{Q}_q \cong \mathbb{Q}_p[v]/(U)$ und die gewünschte Präzision N.
Ausgabe : Approximation von $\Sigma_p(v)$ mit der Präzision N.

begin
  $a \leftarrow v^p$
  $n \leftarrow 1$
  while $n < N$ **do**
    $n \leftarrow 2n$
    $a \leftarrow a - \frac{U(a)}{U'(a)} \mod p^n$
  end
  return $a \mod p^N$
end

Da wir $\Phi_p(x) = x^p$ gewählt haben, können wir $pE(x) = \Phi_p(H(x)) - H^p(x)$ bestimmen und daraus $\Phi_p(z)$ gemäß Satz 4.8 in eine Taylor-Reihe zu entwickeln, wobei wir die Reihe nur bis zum Index $k = M$ bestimmen müssen.

Eine schnellere Möglichkeit erhalten wir jedoch, wenn wir an die Darstellung

$$\Phi_p(z) = z^p \left(1 + pE(x)z^{2p}\right)^{-1/2}$$

erinnern, denn die inverse Quadratwurzel lässt sich mittels Newton-Iteration mit quadratischer Konvergenz bestimmen. Die Korrektheit des folgenden Algorithmus lässt sich analog dem Beweis zu Satz 1.11 zeigen.

Algorithmus 2 : Inverse Quadratwurzel

Eingabe : $s := 1 + pE(x)z^{2p} \in \mathbb{Z}_q[x][z^2]$ mit $E(x) \in \mathbb{Z}_q[x]$ und gewünschte p-adische Präzision $N \in \mathbb{N}$.
Ausgabe : $r \in \mathbb{Z}_q[x][z^2]$, so dass $r^2 s \equiv 1 \mod p^N$.

begin
  $r \leftarrow 1$
  $n \leftarrow 1$
  while $n < N$ **do**
    $n \leftarrow 2n$
    $r \leftarrow \frac{3}{2}r - \frac{1}{2}r^3 s \mod p^n$
    $r \leftarrow r \mod (Hz^2 - 1)$
  end
  return $r \mod p^N$
end

Um die Potenzen der auftretenden Polynome in den Berechnungen klein zu halten, führen wir nach jedem Schritt eine Reduktion mit der Identität $H(x)z^2 = 1$ durch.

Da wir unsere Berechnungen in $\mathbb{Z}_q$ durchführen wollen, berechnen wir die Bilder der modifizierten Basis $p^\mu x^i z dx$ $(i = 0, \ldots, 2g-1)$, wobei μ wie in (4.19) definiert ist. Es gilt

$$\Phi_p(p^\mu x^i z dx) = p^\mu \Phi_p(x^i)\Phi_p(z)d(\Phi_p(x)) = p^{\mu+1} x^{ip+p-1}\Phi_p(z)dx. \tag{4.21}$$

Im folgenden Algorithmus werden wir nur die Polynome vor dem Ausdruck zdx speichern.

Algorithmus 3 : Berechnung des p-Frobenius auf die Basiselemente

Eingabe : Benötigte p-adische Präzision N.
Ausgabe : $B_0, \ldots, B_{2g-1} \in \mathbb{Z}_q[x]$, so dass $B_i z dx$ das Bild des Basiselementes $p^\mu x^i z dx$ unter Φ_p ist $(i = 0, \ldots, 2g-1)$.

begin
  $\mu \leftarrow \lfloor \log_p(2g + 1 - 2/p) \rfloor$
  $R \leftarrow$ die inverse Quadratwurzel von $1 + pE(x)z^{2p}$ mit Algorithmus 2 bis zur Präzision N
  for $i = 0$ **to** $2g - 1$ **do**
    $B_i \leftarrow p^{\mu+1} x^{ip+p-1} z^{p-1} R \mod (Hz^2 - 1)$
  end
  return $B_0, \ldots, B_{2g-1}$
end

Reduktion

Die mit Gleichung (4.21) erhaltenen Darstellungen werden im nächsten Schritt auf die Basisdarstellung reduziert. Dazu benötigen wir zunächst Polynome $S, T \in \mathbb{Z}_q[x]$, so dass

$$SH + TH' = 1 \tag{4.22}$$

gilt. Diese Polynome existieren, denn der größte gemeinsame Teiler von h und h' ist Eins und damit auch der größte gemeinsame Teiler von H und H'. KASH3 stellt eine Methode zur Berechnung von Polynomen $s, t \in \mathbb{F}_q[x]$ mit $sH + tH' \equiv 1 \mod p$ bereit. Diese Polynome wollen wir nun so nach $\mathbb{Z}_q[x]$ liften, dass (4.22) gilt. Dabei verwenden wir wieder eine Newton-Iteration, indem wir zur Faktorstruktur $\mathbb{Z}_q[x]/(H)$ übergehen und T zu einer Nullstelle von $f(X) := X^{-1} - H'$ liften. Als Startwert für diese Iteration können wir t wählen, denn es gilt $t^{-1} - H' \equiv 0 \mod H$ und erhalten wie in Satz 1.11 eine quadratische Konvergenz.

Das Polynom S können wir anschließend durch auflösen als $\frac{1-TH'}{H}$ bestimmen.

Algorithmus 4 : Berechnung von S und T

Eingabe : Polynom $H \in \mathbb{Z}_q[x]$ mit einfachen Nullstellen und gewünschte p-adische Präzision N.

Ausgabe : Polynome $S, T \in \mathbb{Z}_q[x]$, so dass $SH + TH' \equiv 1 \mod p^N$.

begin
- $S, T \leftarrow$ Polynome aus $\mathbb{F}_q[x]$, so dass $SH + TH' \equiv 1 \mod p$
- $n \leftarrow 1$
- **while** $n < N$ **do**
  - $n \leftarrow 2n$
  - $T \leftarrow 2T - H'S^2 \mod H$
- **end**
- $S \leftarrow \frac{1-TH'}{H}$
- **return** S, T

end

Die Polynome S und T werden nun für die eigentliche Reduktion benötigt.

Algorithmus 3 liefert Polynome der Form

$$B_i(x,z) = \sum_{k \geq 0} a_k(x) z^{2k} \in \mathbb{Z}_q[x,z],$$

wobei aufgrund der Reduktion modulo $Hz^2 - 1$ die Grade der a_k für alle $k > 0$ maximal $2g$ betragen. Da in den B_i keine negativen z-Potenzen auftreten, benötigen wir im ersten Reduktionsschritt lediglich eine der „Reduktionsrichtungen“ aus Lemma 4.3. Im folgenden Algorithmus bezeichnen wir mit $\deg_z(a)$ die höchste auftretende z-Potenz in einem Polynom $a \in \mathbb{Z}_q[x,z]$.

Algorithmus 5 : Reduktion der z-Potenzen

Eingabe : Ein Polynom $a(x,z) = \sum_{k\geq 0} a_k(x) z^{2g} \in \mathbb{Z}_q[x,z]$.
Ausgabe : Ein Polynom $b \in \mathbb{Z}_q[x]$, so dass $b(x)zdx \equiv a(x,z)zdx$ in $H^1_{MW}(C')^-$.

begin
  $S, T \leftarrow$ Die Polynome S und T aus Algorithmus 4
  $L \leftarrow \deg_z(a)$
  while $L > 0$ **do**
    $A \leftarrow a_L \cdot T$
    $R \leftarrow A \mod H$
    $R' \leftarrow$ Ableitung von R nach x
    $Q \leftarrow \frac{A-R}{H}$
    $a_{L-2} \leftarrow a_{L-2} + a_L S + QH' + \frac{2}{L-2} R'$
    $a_L \leftarrow 0$
    $L \leftarrow \deg_z(a)$
  end
  $b \leftarrow a_0$
  return b
end

Im nächsten Schritt werden wir den Grad der Rückgabe b (die wir als $b(x)zdx$ interpretieren) auf unter $2g$ reduzieren, um eine Basisdarstellung zu erhalten.

Algorithmus 6 : Reduktion der x-Potenzen

Eingabe : Ein Polynom $b \in \mathbb{Z}_q[x]$.
Ausgabe : Ein Polynom $\bar{b} \in \mathbb{Z}_q[x]$ vom Grad $< 2g$, so dass $\bar{b}(x)zdx \equiv b(x)zdx$ in $H^1_{MW}(C')^-$.

begin
  $L \leftarrow \deg(b)$
  while $L \geq 2g$ **do**
    $K \leftarrow x^{L-2g}$
    $K' \leftarrow$ Ableitung von K nach x
    $I \leftarrow KH' + 2K'H$
    $n \leftarrow$ Führender Koeffizient von b
    $b \leftarrow b - \frac{n}{2m-2g+1} I$
    $L \leftarrow \deg(b)$
  end
  $\bar{b} \leftarrow b$
  return $\bar{b}$
end

Damit können wir die Bilder der Basiselemente $p^\mu x^i zdx$ $(i = 0, \ldots, 2g-1)$ unter Φ_p in der Basis $x^i zdx$ mit Koeffizienten aus $\mathbb{Z}_q$ darstellen. Die Darstellung bezüglich $p^\mu x^i zdx$

hat im Allgemeinen jedoch Koeffizienten, die nicht in $\mathbb{Z}_q$ liegen.

Berechnung einer geeigneten Transformationsmatrix

Wir wollen nun eine Transformationsmatrix T von der Basis $x^i z dx$ $(i = 0, \ldots, 2g-1)$ zu einer Basis des in Lemma 4.10 definierten $\mathbb{Z}_q$-Moduls L berechnen. Der Modul L ist invariant unter Φ_p und damit ist die Darstellungsmatrix von Φ_p bezüglich einer Basis von L über $\mathbb{Z}_q$ definiert. Da wir nicht gewährleisten können, dass die Koeffizienten von T in $\mathbb{Z}_q$ liegen, finden die folgenden Berechnungen in $\mathbb{Q}_q$ statt.

Wir suchen eine Basis des $\mathbb{Z}_q$-Moduls L. Die Elemente aus L sind diejenigen Elemente aus $A = \oplus_{0 \le i \le 2g-1} \mathbb{Z}_q \cdot x^i z dx$, die in $B := \frac{t^{-2g}\mathbb{Z}_q[[t]]dt}{t^{-1}\mathbb{Z}_q[[t]]dt}$ mit $t = x^g z$ integrierbar sind.

Überlegen wir zunächst, wie die Basiselemente $x^i z dx$ in $\frac{t^{-2g}\mathbb{Z}_q[[t]]dt}{t^{-1}\mathbb{Z}_q[[t]]dt}$ aussehen. Es gilt

$$dt = d(x^g z) = \left(g x^{g-1} - \frac{1}{2} x^g z^2 H'(x) \right) z dx$$

und damit

$$x^i z dx = \frac{x^i}{g x^{g-1} - \frac{1}{2} x^g z^2 H'(x)} dt = \underbrace{\frac{H(x) x^i}{H(x) g x^{g-1} - \frac{1}{2} x^g H'(x)}}_{=:h_i(x)} dt.$$

Die $h_i(x)$ können wir im Abschluss bezüglich der Stelle P_∞ des Funktionenkörpers $\mathrm{Quot}\left(\mathbb{Q}_q[x,y,z]/(y^2 - H(x), zy - 1)\right)$ in der Uniformisierenden t entwickeln und erhalten für jedes i eine Darstellung

$$h_i(x) = \sum_{j=n_i}^{\infty} \lambda_{i,j} t^j, \tag{4.23}$$

mit $n_i = \mathrm{ord}_\infty(h_i(x))$ und $\lambda_{i,j} \in \mathbb{Z}_q$.

Da die Elemente $x^i z dx$ im negativen Eigenraum der hyperelliptischen Involution ι liegen und $\iota(t) = -t$ gilt, können in der Reihenentwicklung (4.23) nur gerade Potenzen von t auftreten.

Wie wir in Beispiel 1.29 gesehen haben, gilt $\mathrm{ord}_\infty(x) = -2$ und damit

$$\mathrm{ord}_\infty(h_i(x)) = \mathrm{ord}_\infty\left(H(x)x^i\right) - \mathrm{ord}_\infty\left(H(x) g x^{g-1} - \frac{1}{2} x^g H'(x)\right) = 2g - 2i - 2.$$

Des weiteren kann man leicht nachrechnen, dass der Koeffizient mit Index $(2g - 2i - 2)$

für jedes i gleich -2 ist. Schließlich erhalten wir in B die Darstellungen

$$\begin{aligned} x^i z dx &= \sum_{\substack{j=2g-2i-2 \\ j \text{ gerade}}}^{-2} \lambda_{i,j} t^j dt + t^{-1}\mathbb{Z}_q[[t]]dt \\ &= -2t^{2g-2i-2} + \sum_{\substack{j=2g-2i \\ j \text{ gerade}}}^{-2} \lambda_{i,j} t^j dt + t^{-1}\mathbb{Z}_q[[t]]dt \end{aligned}$$

und sehen, dass die $x^i z dx$ für $i = 0, \ldots, g-1$ gleich $0 \in B$ und damit integrierbar sind. Alle weiteren $x^i z dx$ sind genau dann integrierbar, wenn alle $\lambda_{i,j}$ durch $j+1$ teilbar sind. Eine mögliche Basis von L wäre also beispielsweise

$$x^0 z dx, x^1 z dx, \ldots, x^{g-1} z dx, -2p^{v_p(-1)} t^{-2} dt, \ldots, -2p^{v_p(-2g+1)} t^{-2g} dt, \tag{4.24}$$

welche wir problemlos als $\mathbb{Z}_q$-Linearkombinationen der $x^i z dx$ erhalten. Offensichtlich ist $\lfloor \log_p(2g-1) \rfloor$ die maximale p-Potenz, mit der dabei multipliziert wird und wir müssen aufgrund der Basistransformation die p-adische Präzision in unseren Berechnungen um diesen Wert erhöhen.

Algorithmus 7 : P_∞-adische Entwicklung

Eingabe : Ein Element h des Funktionenkörpers
Quot $\left(\mathbb{Q}_q[x,y,z]/(y^2 - H(x), zy - 1)\right)$.

Ausgabe : P_∞-adische Entwicklung von h in der Variablen $t = x^g z$ bis zum Index -1.

```
begin
    n ← ord_∞(h)
    if n ≥ −1 then
        return 0
    end
    for i = n to −2 do
        b_{−i} ← t^i h(P_∞)
        h ← h − b_{−i} t^i
    end
    return b
end
```

Algorithmus 8 : Berechnung einer Transformationsmatrix

Eingabe : Geliftetes Polynom $H \in \mathbb{Z}_q[x]$ von $h \in \mathbb{F}_q[x]$, das die hyperelliptische Kurve durch $y^2 = h(x)$ definiert.

Ausgabe : Transformationsmatrix der Basis $\{x^i z dx | 0 \leq i \leq 2g-1\}$ zur Basis (4.24).

begin
  for $i = g$ **to** $2g-1$ **do**
    $\sum b_{-n}^{(i)} t^n \leftarrow$ Entwicklung von $x^i z dx$ in der Variablen t bis zum Index -1 mittels Algorithmus 7
  end
  for $i = g$ **to** $2g-1$ **do**
    $T^{(i)} \leftarrow 1 \in \mathbb{Q}_q^{2g \times 2g}$
    for $j = i+1$ **to** $2g-1$ **do**
      $T_{i+1,j+1}^{(i)} \leftarrow -\frac{1}{-2} b_{2i-2g+2}^{(j)}$
    end
  end
  $T \leftarrow T^{(g)} \cdot \ldots \cdot T^{(2g-1)}$
  # T IST NUN TRANSFORMATIONSMATRIX ZU $-2t^{2g-2i-2}dt + t^{-1}\mathbb{Z}_q[[t]]dt$
  for $i = g$ **to** $2g-1$ **do**
    for $j = g$ **to** $2g-1$ **do**
      $T_{i+1,j+1} \leftarrow p^{v_p(2g-2i-1)} T_{i+1,j+1}$
    end
  end
  return T
end

Berechnung des L-Polynoms

Aus den reduzierten Bildern $\Phi_p(p^\mu x^i z dx) = \sum_{k=0}^{2g-1} B_{i,k} x^k z dx$ $(i = 0, \ldots, 2g-1)$ und der Transformationsmatrix T aus Algorithmus 8 wollen wir nun eine Darstellungsmatrix $M \in \mathbb{Z}_q^{2g \times 2g}$ von Φ berechnen, um daraus das charakteristische Polynom χ_Φ von Φ bestimmen.

Die $B_{i,k} \in \mathbb{Z}_q$ liefern eine Darstellungsmatrix von Φ_p bezüglich $x^i z dx$ durch

$$M_p := p^{-\mu} \begin{pmatrix} B_{0,0} & \cdots & B_{0,2g-1} \\ \vdots & \ddots & \vdots \\ B_{2g-1,0} & \cdots & B_{2g-1,2g-1} \end{pmatrix} \in \mathbb{Q}_q^{2g \times 2g}.$$

Aufgrund der Σ_p-Linearität (4.14) berechnet sich die Darstellungsmatrix bezüglich der

transformierten Basis als

$$\widetilde{M_p} := T^{-1} M_p T^{\Sigma_p} = p^{-\mu} T^{-1} \begin{pmatrix} B_{0,0} & \cdots & B_{0,2g-1} \\ \vdots & \ddots & \vdots \\ B_{2g-1,0} & \cdots & B_{2g-1,2g-1} \end{pmatrix} T^{\Sigma_p},$$

wobei T^{Σ_p} durch koeffizientenweises Anwenden von Σ_p auf T entsteht. Die Koeffizienten dieser Matrix sind aus $\mathbb{Z}_q$ und wir berechnen die Matrix M von Φ gemäß (4.15):

$$M := \widetilde{M_p} \cdot \widetilde{M_p}^{\Sigma_p} \cdot \ldots \cdot \widetilde{M_p}^{\Sigma_p^{n-1}} \in \mathbb{Z}_q^{2g \times 2g}.$$

Damit haben wir alle nötigen Ergebnisse, um das L-Polynom zu bestimmen. Aufgrund des Zusammenhangs $L(t) = t^{2g}\chi_\Phi(\frac{1}{t})$ und den Vermutungen von Weil können wir χ_Φ schreiben als

$$\chi_\Phi(t) = t^{2g} + a_1 t^{2g-1} + \ldots + a_g t^g + \ldots + q^{g-1} a_1 t + q^g$$

mit den Abschätzungen $|a_i| \leq \binom{2g}{i} q^{i/2}$. Wir haben die p-adische Präzision gerade so gewählt, dass wir die Koeffizienten $a_1, \ldots, a_g$ eindeutig bestimmen können. Alle weiteren werden wir also mit der Beziehung $a_{2g-i} = q^{g-i} a_i$ bestimmen.

Algorithmus 9 : Berechnung des charakteristischen Polynoms χ_Φ aus der Darstellungsmatrix.

Eingabe : Darstellungsmatrix $M \in (\mathbb{Z}_q/p^N\mathbb{Z}_q)^{2g\times 2g}$ von Φ.
Ausgabe : Das charakteristische Polynom von Φ.

begin
  $a_0t^{2g} + a_1t^{2g-1} + \ldots + a_{2g} \leftarrow \det(t - M)$
  $\chi_\Phi \leftarrow t^{2g} + q^g$
  for $i = 1$ **to** $g - 1$ **do**
    $k \leftarrow \lceil \log_p \left(2\binom{2g}{i} + \frac{ni}{2}\right) \rceil$
    if $a_i \leq \left\lceil \frac{p^k}{2} \right\rceil$ **then**
      $\chi_\Phi \leftarrow \chi_\Phi + a_it^{2g-i} + q^{g-i}a_it^i$
    end
    else
      $\chi_\Phi \leftarrow \chi_\Phi + (a_i - p^k)t^{2g-i} + q^{g-i}(a_i - p^k)t^i$
    end
  end
  # Bestimmung des mittleren Koeffizienten
  $k \leftarrow \left\lceil \log_p \left(2\binom{2g}{g} + \frac{ng}{2}\right) \right\rceil$
  if $a_g \leq \left\lceil \frac{p^k}{2} \right\rceil$ **then**
    $\chi_\Phi \leftarrow \chi_\Phi + a_gt^g$
  end
  else
    $\chi_\Phi \leftarrow \chi_\Phi + (a_g - p^k)t^g$
  end
  return χ_Φ
end

4.5.5 Rechenaufwand und Beispiele

Bevor wir einige Berechnungsbeispiele betrachten, wollen wir kurz auf die asymptotische Laufzeit des beschriebenen Algorithmus eingehen. Wir verwenden dabei die „Soft-Oh“ Schreibweise $\widetilde{O}$, wobei $\widetilde{O}(N)$ definiert ist als $O(N(\log N)^k)$ für ein beliebiges $k \in \mathbb{R}$.

Die Eingabegrößen sind die Charakteristik p, die Größe des endlichen Körpers $q = p^n$ und das Geschlecht g der Kurve.

Satz 4.11. *Der Gesamtkomplexität des beschriebenen Algorithmus zur Berechnung des L-Polynoms ist* $\widetilde{O}(pn^3g^4)$.

Wir verzichten auf einen Beweis dieses Satzes und verweisen auf die ausführliche Berechnung dieses Ergebnisses in [GG03, S. 398].

Für festes p haben wir die asymptotische Laufzeit relativ gut im Griff, für wachsendes p besteht allerdings eine sehr ungünstige Abhängigkeit. Der Grund für die lineare Abhängigkeit von p ist, dass wir die Bilder der Basiselemente unter Φ_p in eine Reihe mit $O(p)$ Summanden entwickeln und anschließend $O(p)$ Reduktionsschritte benötigen, um eine Basisdarstellung zu erhalten.

David Harvey liefert in [Har06] eine Verbesserung des Algorithmus für große p, indem er eine Reihendarstellung von $\Phi_p(x^i z dx)$ wählt, deren benötigte Länge unabhängig von p ist und anschließend einen Baby-Step-Giant-Step-Algorithmus zur Reduktion der Elemente verwendet. Damit ist es immerhin möglich, eine lineare Abhängigkeit von $\sqrt{p}$ zu erreichen. Allerdings führt diese Modifikation zu einer Verlangsamung bei kleinem p.

Die folgenden Rechnungen wurden in KASH3 auf einem 64bit UNIX-System mit Intel Core2Duo-Prozessor (3 GHz) durchgeführt. Die Eingabe erfordert dabei ein Polynom $h \in \mathbb{F}_q[x]$, das teilerfremd zu seiner Ableitung ist und von ungeradem Grad ist. Als Rückgabe erhalten wir das L-Polynom der hyperelliptischen Kurve, die durch $y^2 = h(x)$ definiert wird.

Wir betrachten die Polynome

$$
\begin{aligned}
h_1 &:= x^3 + vx^2 + v^{41}x + v^{37}x + v^{62} \\
h_2 &:= x^5 + v^{32}x^4 + v^{41}x^3 + v^{21}x^2 + v^2x + v^{21}x + v^{43} \\
h_3 &:= x^9 + v^{30}x^8 + v^{11}x^7 + v^{58}x^6 + v^{12}x^5 + v^{53}x^4 + v^{19}x^3 + v^{54}x^3 + v^{38}x^2 + \\
&\quad v^{10}x + v^{25} \\
h_4 &:= x^{15} + v^{23}x^{14} + v^{23}x^{13} + v^{32}x^{12} + vx^{11} + v^2x^{10} + vx^9 + v^{23}x^8 + v^{54}x^7 + \\
&\quad v^{12}x^6 + vx^5 + v^{10}x^4 + v^{33}x^3 + v^{23}x^2 + v^{22}x + v^{22} \\
h_5 &:= x^{19} + v^{32}x^{17} + v^{13}x^{16} + v^{43}x^{15} + v^{12}x^{10} + v^{33}x^9 + v^{60}x^8 + v^{18}x^7 + v^{51}x^6 + \\
&\quad v^9x^5 + v^{68}x^4 + v^{50}x^3 + v^{78}x^3 + v^{19}x^2 + v^{44}x + v^{43} \\
h_6 &:= x^{21} + v^{77}x^{20} + v^{49}x^{19} + v^{10}x^{17} + v^{30}x^{15} + v^{23}x^{13} + v^{32}x^{12} + vx^{11} + v^{30}x^8 + \\
&\quad v^{11}x^7 + v^{51}x^6 + v^9x^5 + v^{41}x^3 + v^{21}x^2 + v^9x + v^{41} \\
h_7 &:= x^25 + v^{27}x^{24} + v^{70}x^{22} + v^{23}x^{20} + v^{12}x^{21} + v^{10}x^{17} + v^{70}x^{15} + v^{33}x^{13} + \\
&\quad v^{12}x^{12} + vx^{11} + v^{30}x^8 + v^{21}x^7 + v^{11}x^6 + v^{12}x^5 + v^{41}x^3 + v^21x^2 + v^{18}x + v
\end{aligned}
$$

über dem Körper $\mathbb{F}_{3^4} := \mathbb{F}_3[v]/(v^4 + 2v^3 + 2)$ und erhalten für die zugehörigen L-Polynome $L(t) = 1 + a_1t + \ldots + a_gt^g + \ldots + q^{g-1}a_1t^{2g-1} + q^gt^{2g}$ die folgenden Ergebnisse:

	g	Zeit	Koeffizienten von L	$\#C$
h_1	1	$1s$	$a_1 = 13$	95
h_2	2	$5s$	$a_1 = 4$ $a_2 = -54$	6836
h_3	4	$37s$	$a_1 = 9$ $a_2 = 107$ $a_3 = 1475$ $a_4 = 8667$	43761186
h_4	7	$390s$	$a_1 = 9$ $a_2 = 47$ $a_3 = -68$ $a_4 = -3235$ $a_5 = -29051$ $a_6 = 225391$ $a_7 = 3231028$	25577721838656
h_5	9	$1162s$	$a_1 = 13$ $a_2 = 175$ $a_3 = 2041$ $a_4 = 21033$ $a_5 = 193645$ $a_6 = 2083597$ $a_7 = 21714117$ $a_8 = 230133202,$ $a_9 = 2001080800$	178846719105456128
h_6	10	$1508s$	$a_1 = -5$ $a_2 = 56$ $a_3 = -768$ $a_4 = 1273$ $a_5 = -62166$ $a_6 = 718421$ $a_7 = -3896088$ $a_8 = 54998036$ $a_9 = -327249373$ $a_{10} = 1791356026$	11493564000881319120
h_7	12	$4001s$	$a_1 = -12$ $a_2 = 167$ $a_3 = -1554$ $a_4 = 17466$ $a_5 = -136872$ $a_6 = 1104810$ $a_7 = -5129880$ $a_8 = 35206150$ $a_9 = -36791155$ $a_{10} = 974679126$ $a_{11} = 11540899377$ $a_{12} = 70513437248$	69775804624922067159056

Nun wollen wir die Charakteristik und das Geschlecht fixieren und den Grundkörper variieren. Dazu betrachten wir die Körper

$$
\begin{aligned}
\mathbb{F}_{5^2} &:= \mathbb{F}_5[v]/(v^2+4v+2),\\
\mathbb{F}_{5^5} &:= F_5[v]/(v^5+4v+3),\\
\mathbb{F}_{5^{10}} &:= \mathbb{F}_5[v]/(v^{10}+3v^5+3v^4+2v^3+4v^2+v+2),\\
\mathbb{F}_{5^{15}} &:= \mathbb{F}_5[v]/(v^{15}+2v^5+3v^3+3v^2+4v+3),\\
\mathbb{F}_{5^{30}} &:= \mathbb{F}_5[v]/(v^{30}+4v^{21}+3v^{19}+4v^{17}+4v^{16}+4v^{14}+4v^{13}+3v^{12}+2v^{11}+2v^9+\\
&\quad 2v^8+4v^7+3v^6+4v^5+v^4+v^2+v+2),\\
\mathbb{F}_{5^{50}} &:= \mathbb{F}_5[v]/(v^{50}+2v^{49}+2v^{48}+2v^{47}+4v^{46}+v^{44}+4v^{42}+3v^{40}+4v^{38}+v^{37}+\\
&\quad v^{36}+2v^{34}+4v^{33}+4v^{32}+2v^{30}+2v^{29}+v^{28}+4v^{27}+4v^{26}+v^{25}+4v^{24}+\\
&\quad 2v^{23}+3v^{22}+4v^{21}+2v^{20}+3v^{18}+3v^{17}+v^{16}+2v^{15}+2v^{14}+2v^{12}+2v^{11}+\\
&\quad 2v^{10}+4v^9+v^8+2v^7+4v^5+v^4+2v^3+3v^2+v+3),\\
\mathbb{F}_{5^{70}} &:= \mathbb{F}_5[v]/v^{70}+4v^{69}+2v^{68}+v^{67}+v^{66}+v^{65}+v^{64}+v^{63}+3v^{62}+3v^{61}+3v^{60}+\\
&\quad 2v^{59}+v^{58}+4v^{57}+2v^{56}+4v^{55}+3v^{54}+v^{53}+v^{51}+2v^{48}+v^{47}+3v^{46}+\\
&\quad v^{45}+2v^{44}+2v^{43}+v^{41}+v^{40}+4v^{39}+v^{38}+4v^{36}+4v^{35}+v^{33}+3v^{32}+v^{31}+\\
&\quad 3v^{30}+2v^{29}+3v^{28}+2v^{27}+v^{26}+4v^{25}+2v^{24}+3v^{23}+3v^{21}+2v^{20}+2v^{18}+\\
&\quad v^{14}+3v^{13}+2v^{12}+3v^{11}+v^{10}+2v^9+v^7+3v^6+4v^4+3v^3+v^2+v+2.
\end{aligned}
$$

Wenn wir das Polynom $h(x) := x^5+v^{98324}x^4+v^{102}x^3+v^2x+v^{922110}$ als Polynom aus dem jeweiligen Körper auffassen, erhalten wir die folgenden Ergebnisse.

	Zeit	Koeffizienten von L	$\#C$
$\mathbb{F}_{5^2}$	$3s$	$a_1 = 2$ $a_2 = -6$	672
$\mathbb{F}_{5^5}$	$5s$	$a_1 = 35$ $a_2 = 3619$	9878655
$\mathbb{F}_{5^{10}}$	$15s$	$a_1 = 2881$ $a_2 = 15950184$	95395582359316
$\mathbb{F}_{5^{15}}$	$58s$	$a_1 = 9172$ $a_2 = -10180949954$	931322854512524137344
$\mathbb{F}_{5^{30}}$	$541s$	$a_1 = -3404768028$ $a_2 = 536988805196647559956$	867361737985232609880693803857225713495054
$\mathbb{F}_{5^{50}}$	$3056s$	$a_1 = -67539453505309035$ $a_2 = 160963972200214640883290912496907016$	7888609052210118048118577144652316218679751807160460145337810 6940816732
$\mathbb{F}_{5^{70}}$	$13176s$	$a_1 = -706924427144789466508927$ $a_2 = 24745604757620964600522213725443354664010317198422$	7174648137343063403129489478561560487065550908324936505387547466242871764281534789551012199984574 6

Abschließend wollen wir noch die Charakteristik p variieren. Dazu betrachten wir das Polynom $h(x) = x^5 + 24351x^4 + 91x^3 + 110x^2 + 81x + 234$ und fassen es als Polynom über $\mathbb{F}_p$ mit einer wechselnden Primzahl p auf. Die dadurch definierten Kurven sind für alle angegebenen p glatt. Wir erhalten die folgenden Ergebnisse:

p	Zeit	Koeffizienten von L	$\#C$
11	$4s$	$a_1 = 3$ $a_2 = 12$	170
53	$11s$	$a_1 = 1$ $a_2 = 20$	2884
101	$22s$	$a_1 = -20$ $a_2 = 278$	8440
211	$63s$	$a_1 = -4$ $a_2 = 18$	43692
503	$281s$	$a_1 = 12$ $a_2 = 330$	259388
1103	$1187s$	$a_1 = -4$ $a_2 = -1048$	1211146
2003	$6730s$	$a_1 = -45$ $a_2 = 1866$	3923696

Kapitel 5

Berechnung der Zetafunktion mittels Cartier-Operator

In diesem Kapitel wollen wir uns dem Berechnen von Zetafunktionen von Kurven über Körpern mit großer Charakteristik zuwenden. Wir haben gesehen, dass die Komplexität von Kedlayas Algorithmus für hyperelliptische Kurven ungefähr linear in der Charakteristik p ist. Unser Ziel ist es, diese Abhängigkeit für eine möglichst große Klasse von Kurven zu verbessern.

Wir stellen eine Möglichkeit vor, die lineare Abhängigkeit von der Charakteristik p auf $\sqrt{p}$ zu reduzieren. Für diesen Ansatz beschränken wir uns von vornherein auf Kurven vom Geschlecht drei über einem Primkörper $\mathbb{F}_p$, merken aber an, dass die Methode vollkommen analog auch für den Fall $g = 1$ und $g = 2$ anwendbar ist. Dabei gehen wir in zwei Schritten vor. Zunächst werden wir das L-Polynom modulo p berechnen (siehe Abschnitt 5.1) und daraus anschließend das gesuchte Polynom konstruieren (siehe Abschnitt 5.2). Die Komplexität in Abhängigkeit von p sollte daher in beiden Schritten $\sqrt{p}$ nicht überschreiten.

Um den zweiten Schritt zu realisieren, werden wir in Abschnitt 5.3 beschreiben, wie wir für ein gegebenes Polynom testen können, ob es das charakteristische Polynom des Frobenius ist.

Im gesamten Kapitel bezeichnet C eine glatte Kurve in der Ebene über einem Primkörper $\mathbb{F}_p$ mit $p > 2$ und Φ den p-Frobenius.

5.1 Der Cartier-Operator

In diesem Abschnitt wollen wir den Cartier-Operator definieren und aufzeigen, wie wir damit das L-Polynom modulo p bestimmen können. Der Cartier-Operator lässt sich deutlich allgemeiner definieren, als wir dies tun werden. Für eine ausführliche und

allgemeine Darstellung verweisen wir auf [SV87] oder [Lan73, S. 311].

5.1.1 Definition und Eigenschaften

Es sei also C eine glatte, ebene Kurve vom Geschlecht g über $\mathbb{F}_p$ mit dem Funktionenkörper $F = \mathbb{F}_p(C)$ und F^p der Teilkörper aller p-ten Potenzen von F. Wenn wir ein festes Element $x \in F$ wählen, so dass $F/\mathbb{F}_p(x)$ separabel ist, können wir jedes Element ω des F-Vektorraums $\Omega(F) := \Omega_{F/\mathbb{F}_p}$ (siehe Abschnitt 1.2.7) eindeutig schreiben als

$$\omega = d\lambda + \alpha^p x^{p-1} dx, \text{ mit } \lambda, \alpha \in F. \tag{5.1}$$

Definition 5.1 (Cartier-Operator)**.** *Mit der Darstellung (5.1) ist der* Cartier-Operator $\mathfrak{C} : \Omega(F) \to \Omega(F)$ *definiert als*

$$\mathfrak{C}(\omega) := \alpha dx.$$

Die Unabhängigkeit dieser Definition von der Wahl des separierenden Elementes x und damit die Wohldefiniertheit von $\mathfrak{C}$ lässt sich aus den Eigenschaften der Tate-Spur (siehe [Tat52, Theorem 1]) folgern.

Satz 5.2. *Der Cartier-Operator besitzt folgende Eigenschaften:*

(i) Für alle $\omega \in \Omega(F)$ und $z \in F$ gilt $\mathfrak{C}(z^p\omega) = z\mathfrak{C}(\omega)$. Das heißt, $\mathfrak{C}$ ist $(1/p)$-linear und insbesondere $\mathbb{F}_p$-linear.

(ii) Der $\mathbb{F}_p$-Vektorraum $\Omega^0(F)$ der holomorphen Differentiale ist invariant unter $\mathfrak{C}$.

Beweis. Siehe [Hes99, Satz 3.25] □

Der Cartier-Operator ist also eine lineare Abbildung auf dem Vektorraum $\Omega^0(F)$ und wir können ihm für eine fixierte Basis eine Darstellungsmatrix $M \in \mathbb{F}_p^{g\times g}$ zuordnen. Diese Matrix nennen wir *Hasse-Witt Matrix von C*. Wir interessieren uns für diese Matrix aufgrund der folgenden Eigenschaft.

Satz 5.3. *Es bezeichne χ_M das charakteristische Polynom der Hasse-Witt-Matrix. Dann gilt für das charakteristische Polynom χ des Frobenius*

$$\chi(t) \equiv t^g \chi_M(t) \mod p.$$

Beweis. Siehe [Man65, Theorem 1]. □

Dieser Satz liefert die Möglichkeit, das L-Polynom modulo p mit Hilfe der Hasse-Witt-Matrix zu bestimmen. Im Folgenden werden wir uns deshalb mit der Berechnung der Hasse-Witt-Matrix beschäftigen.

5.1.2 Berechnung der Hasse-Witt-Matrix

Es sei ein affiner Teil von C durch $f(x,y)=0$ gegeben, wobei f ein Polynom in $\mathbb{F}_p[x,y]$ und x ein separierendes Element des Funktionenkörpers F ist (das heißt $F/\mathbb{F}_p(x)$ ist eine separable Erweiterung). Des Weiteren bezeichne f_y die formale, partielle Ableitung von f nach y. Mit dem Differentialoperator

$$\nabla := \frac{\partial^{2p-2}}{\partial x^{p-1}\partial y^{p-1}}$$

liefern Karl-Otto Stöhr und José Felipe Voloch folgende Darstellung des Cartier Operators.

Satz 5.4. *Mit den obigen Bezeichnungen gilt für jedes $u \in F$*

$$\mathfrak{C}\left(u\frac{dx}{f_y}\right) = \left(\nabla(f^{p-1}u)\right)^{\frac{1}{p}}\frac{dx}{f_y}$$

Beweis. Siehe [SV87, Theorem 1.1.]. □

Mit dieser Darstellung können wir den Cartier-Operator explizit berechnen. Der folgende Satz liefert eine nützliche Information über die Basen von $\Omega^0(F)$.

Satz 5.5. *Es gelten die Definitionen wie oben. Jede $\mathbb{F}_p$-Basis von $\Omega^0(F)$ ist von der Form*

$$\left\{u_i\frac{dx}{f_y} \mid i=1,\ldots,g\right\}$$

mit Polynomen $u_i \in \mathbb{F}_p[x,y]$.

Beweis. Nach [Che51, Chapter VI. Theorem 8] lässt sich jedes holomorphe Differential als $u\frac{dx}{f_y}$ mit einem Polynom $u \in \mathbb{F}_p[x,y]$ schreiben. Damit folgt die Behauptung unmittelbar. □

Um die Hasse-Witt-Matrix zu bestimmen, müssen wir also $\left(\nabla(f^{p-1}u_i)\right)^{\frac{1}{p}}$ für gewisse Polynome $u_1,\ldots,u_g \in \mathbb{F}_p[x,y]$ berechnen und daraus die Basisdarstellung ermitteln.

Da wir an großen p interessiert sind, besteht die Schwierigkeit darin, das Polynom f^{p-1} zu bestimmen. Die Komplexität der Berechnung einer solchen Potenz ist linear in p, wir sind also nicht in der Lage, in der vorgegebenen Zeit das Polynom f^{p-1} vollständig zu berechnen.

Einen Ausweg liefert die folgende Darstellung von ∇, angewendet auf ein Polynom $\sum_{i,j\geq 0} c_{i,j}x^iy^j$:

$$\begin{aligned}\nabla\left(\sum_{i,j\geq 0} c_{i,j}x^iy^j\right) &= \sum_{i,j\geq 0}\underbrace{\left(1\cdot 2\cdot\ldots\cdot(p-1)\right)^2}_{\equiv 1 \mod p} c_{(i+1)p-1,(j+1)p-1}x^{ip}y^{jp} \\ &= \sum_{i,j\geq 0} c_{(i+1)p-1,(j+1)p-1}x^{ip}y^{jp}. \qquad (5.2)\end{aligned}$$

Aufgrund der Charakteristik p können wir daraus einfach die p-te Wurzel ziehen und erhalten $\sum_{i,j} c_{(i+1)p-1,(j+1)p-1} x^i y^j$.

Da die Elemente u_i Polynome sind, können wir diese Rechnung auch für unsere Basiselemente verwenden und benötigen zur Bestimmung von $\mathfrak{C}\left(u_i \frac{dx}{f_y}\right)$ somit nur gewisse Koeffizienten der Polynome $f^{p-1}u_i$.

Die Anzahl der benötigten Koeffizienten ist dabei unabhängig von p. Wenn wir also in der Lage sind, jeden beliebigen Koeffizienten der Polynome $f^{p-1}u_i$ in $\widetilde{O}(\sqrt{p})$ zu bestimmen, können wir die gesamte Hasse-Witt-Matrix in $\widetilde{O}(\sqrt{p})$ berechnen (der Ausdruck $\widetilde{O}$ ist dabei definiert wie in Abschnitt 4.5.5).

Lineare Rekurrenzen

Bevor wir näher auf die Berechnung der Hasse-Witt-Matrix eingehen, beschreiben wir eine Technik, um bestimmte Folgenglieder einer linearen Rekurrenz zu berechnen.

Eine *lineare Rekurrenzrelation der Ordnung d* ist eine Relation der Form

$$c_k := a_1(k)c_{k-d} + a_2(k)c_{k-d+1} + \cdots + a_d(k)c_{k-1}, \tag{5.3}$$

wobei die a_i polynomielle Ausdrücke in k sind. Solch einer Rekurrenz können wir eine Begleitmatrix

$$A(k) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ a_1(k) & a_2(k) & \cdots & \cdots & a_d(k) \end{pmatrix}$$

zuordnen. Für den Startvektor $U_0 := (0, \ldots, 0, c_0)^t$ und $U_{k+1} := A(k+1)U_k$ gilt dann $U_k = (c_{k-d+1}, \ldots, c_k)^t$. Der folgende Satz liefert für die Berechnung des Vektors U_k eine Laufzeit von $\widetilde{O}(\sqrt{k})$, falls die Polynome a_i vom Grad Eins sind.

Satz 5.6. *Es sei A eine $d \times d$ Matrix mit Einträgen aus $RX + R$, wobei R einen kommutativen Ring mit Eins und X eine Variable bezeichnet. Außerdem sei eine rekursive Folge U_k mit einem Startvektor $U_0 \in R^d$ durch*

$$U_k := A(k)U_{k-1} \in R^d$$

definiert. Falls die Elemente $1, \ldots, 2\lceil\sqrt{k}\rceil + 1$ invertierbar in R sind, lässt sich der Vektor U_k in der Laufzeit $\widetilde{O}(\sqrt{k})$ berechnen.

Beweis. Siehe [BGS03, Theorem 1] □

Der Algorithmus zu diesem Satz ist eine Verbesserung von Gregory und David Chudnovskys Algorithmus, der ebenfalls eine Laufzeit von $\widetilde{O}(\sqrt{k})$ besitzt. Die Verbesserungen in [BGS03] haben also lediglich Auswirkungen auf den logarithmischen Faktor in $\widetilde{O}(\sqrt{k})$.

Chudnovskys Algorithmus basiert im wesentlichen auf einem Baby-Step-Giant-Step Verfahren, das wir an dieser Stelle erläutern wollen.

Zur Vereinfachung gehen wir davon aus, dass k eine Quadratzahl in $\mathbb{N}$ ist. Wir beginnen mit dem Baby-Step und berechnen die Matrix

$$C(X) := \prod_{i=1}^{\sqrt{k}} A(X+i),$$

wobei $A \in R[X]^{d\times d}$ die oben beschriebene Begleitmatrix ist (die Einträge von $C(X)$ sind dann maximal vom Grad $\sqrt{k}$). Im Giant-Step berechnen wir anschließend das Produkt $\prod_{j=0}^{\sqrt{k}-1} C(j\sqrt{k})$, welches offensichtlich gleich $\prod_{i=1}^{k} A(k)$ ist und erhalten

$$U_k = \left(\prod_{j=0}^{\sqrt{k}-1} C(j\sqrt{k})\right) U_0.$$

In diesem Schritt werden die polynomiellen Ausdrücke in der Matrix $C(X)$ an den Stellen $0, \sqrt{k}, 2\sqrt{k}, \ldots, (\sqrt{k}-1)\sqrt{k}$ ausgewertet. Dazu werden in [BGS03] Techniken zur schnellen Auswertung von Polynomen in Stellen mit arithmetischer Progression verwendet, wobei wir auch mit eine naiven Auswertung die Laufzeit $\widetilde{O}(\sqrt{p})$ erhalten.

Berechnung der Hasse-Witt-Matrix mittels linearer Rekurrenzen

Wir wollen nun beschreiben, wie wir die obige Aussage über lineare Rekurrenzen nutzen können, um die Hasse-Witt-Matrix superelliptischer Kurven (siehe Definition 1.34) zu berechnen. Wir verallgemeinern dabei die Vorgehensweise für den hyperelliptischen Fall in [BGS03].

Es sei ein affiner Teil einer superelliptischen Kurve $C/\mathbb{F}_p$ durch $f(x,y) = y^a - h(x)$ mit $b := \deg h$ und den Eigenschaften aus Definition 1.34 gegeben. Mit Hilfe der Polynome u_i sehen wir aus Gleichung (5.2), welche Koeffizienten wir von $F := f^{p-1}$ zur Bestimmung der Hasse-Witt Matrix benötigen. Im Folgenden bezeichnet $F_{k,l}$ den Koeffizienten von $x^k y^l$ eines Polynoms $F \in \mathbb{F}_p[x,y]$ und h_i den Koeffizienten von x^i eines Polynoms $h \in \mathbb{F}_p[x]$. Es gilt

$$f^{p-1} = \sum_{j=0}^{p-1} \binom{p-1}{j} (-h)^j y^{(p-1-j)a}$$

und wir sehen, dass der Koeffizient $F_{k,l}$ für alle Vielfachen l von a gleich dem Koeffizienten von x^k in $\binom{p-1}{l/a}(-h)^{p-1-l/a}$ ist. Andernfalls gilt $F_{k,l} = 0$. Diese Gleichung können

wir noch etwas vereinfachen, denn es gilt (in $\mathbb{F}_p$)

$$\binom{p-1}{j} = \frac{(p-1)(p-2)\cdot\ldots\cdot(p-j)}{1\cdot 2\cdot\ldots\cdot j} = (-1)^j$$

und wir erhalten

$$f^{p-1} = \sum_{j=0}^{p-1} h^j y^{(p-1-j)a}. \tag{5.4}$$

Wir haben das Problem damit auf die Berechnung von Koeffizienten eines univariaten Polynoms $H := h^N \in \mathbb{F}_p[x]$ mit $N := p-1-l/a$ zurückgeführt.

Im Folgenden gehen wir davon aus, dass $h_0 \neq 0$ gilt (andernfalls führen wir die Rechnungen mit $\widetilde{h} := \frac{h}{x}$ fort). Das Polynom H erfüllt die Differentialgleichung

$$hH' = Nh'H \in \mathbb{F}_p[x]$$

und ein Vergleich des Koeffizienten von x^{k-1} liefert

$$\sum_{i=0}^{b} (k-i)h_i H_{k-i} = N \sum_{i=1}^{b} i h_i H_{k-i}$$

und damit

$$H_k = \frac{1}{kh_0} \sum_{i=1}^{b} (Ni - k + i)h_i H_{k-i} \text{ für } p \nmid k.$$

Damit diese Gleichung auch für alle $k \in \mathbb{N}$ mit $p \mid k$ sinnvoll ist, müssen wir die Berechnungen in $\mathbb{Z}_p$ weiter führen und erhalten einen rekursiven Zusammenhang mit der Begleitmatrix

$$A(k) = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & & \ddots & \ddots & 0 \\ 0 & \cdots & \cdots & 0 & 1 \\ \frac{h_b(Nb-k+b)}{kh_0} & \frac{h_{b-1}(N(b-1)-k+b-1)}{kh_0} & \cdots & \cdots & \frac{h_1(N-k+1)}{kh_0} \end{pmatrix} \in \mathbb{Z}_q(k)^{b\times b}, \tag{5.5}$$

der aufgrund des k im Nenner einiger Einträge jedoch nicht von der Form (5.3) ist. Dies lässt sich einfach beheben, indem wir stattdessen die rekursive Folge $\widetilde{H}_k := k!H_k$ betrachten (für die Begleitmatrix $\widetilde{A}(k)$ von $\widetilde{H}_k$ gilt dann $\widetilde{A}(k) = kA(k)$). Wir erhalten also eine lineare Rekurrenz der Ordnung b und können $\widetilde{H}_k$ nach Satz 5.6 in $\widetilde{O}(\sqrt{k})$ berechnen. Den gesuchten Wert H_k erhalten wir dann durch $H_k = \frac{1}{k!}\widetilde{H}_k$.

Da wir lediglich an Potenzen kleiner als p interessiert sind, können wir jeden Koeffizienten in der Laufzeit $\widetilde{O}(\sqrt{p})$ berechnen. Wir erinnern daran, dass bei der Bestimmung des Koeffizienten H_k gleichzeitig die Koeffizienten $H_{k-1}, \ldots, H_{k-b}$ berechnet werden, wir ersparen uns also im Allgemeinen die Berechnung jedes Einzelnen. Zusammenfassend erhalten wir die folgende Aussage.

Satz 5.7. *Die Hasse-Witt-Matrix einer superelliptischen Kurve über $\mathbb{F}_p$ lässt sich in $\widetilde{O}(\sqrt{p})$ Rechenschritten berechnen.*

Wir merken an, dass sich das beschriebene Verfahren problemlos auf den Fall von Kurven über $\mathbb{F}_q$ verallgemeinern lässt.

Es stellt sich natürlich die Frage, inwiefern wir dieses Vorgehen auf eine größere Klasse von Kurven verallgemeinern können. Angenommen, die Variable y tritt in einem weiteren Monom von $f(x,y)$ auf, das heißt, f ist von der der Form

$$f(x,y) = y^a + x^n y^b - h(x),$$

mit $n \in \mathbb{N}_0$, $b \in \mathbb{N}$ und $h \in \mathbb{F}_p[x]$, dann folgt analog der Darstellung (5.4)

$$f^{p-1} = \sum_{\substack{\alpha_1,\alpha_2,\alpha_3 \in \mathbb{N} \\ \alpha_1+\alpha_2+\alpha_3=p-1}} \frac{(p-1)!}{\alpha_1!\alpha_2!\alpha_3!} y^{\alpha_1 a+\alpha_2 b} x^{\alpha_2 n} (-h)^{\alpha_3}.$$

Dabei treten für gewisse $l \in \mathbb{N}$ bereits $O(p)$ Summanden mit der y-Potenz l auf und wir müssten zur Berechnung des Koeffizienten $F_{k,l}$ von $F := f^{p-1}$ ungefähr p verschiedene Potenzen von h bestimmen. Der beschriebene Ansatz, das Problem auf das Berechnen von Koeffizienten univariater Polynome zu reduzieren, ist daher im Allgemeinen nicht möglich.

5.2 Bestimmung des L-Polynoms aus L modulo p

Wir nehmen an, dass wir das L-Polynom (beziehungsweise das charakteristische Polynom χ des p-Frobenius Φ) modulo p kennen und wollen daraus das korrekte L-Polynom bestimmen.

Da wir uns von vornherein auf den Fall einer Kurve vom Geschlecht drei über einem Primkörper $\mathbb{F}_p$ beschränkt haben, liefern die Weil-Vermutungen die Darstellung

$$\chi(t) = t^6 + a_1 t^5 + a_2 t^4 + a_3 t^3 + p a_2 t^2 + p^2 a_1 t + p^3 \in \mathbb{Z}[t],$$

mit $|a_i| \leq \binom{6}{i} p^{i/2}$. Unter diesen Bedingungen können wir die möglichen Werte der Koeffizienten a_i folgendermaßen einschränken:

- $|a_1| \leq 6p^{1/2} \Rightarrow a_1$ ist eindeutig festgelegt (falls $p > 144$).
- $|a_2| \leq 15p \Rightarrow$ für a_2 bleiben noch maximal 31 mögliche Werte.
- $|a_3| \leq 20p^{3/2} \Rightarrow$ für a_3 bleiben noch maximal $2\lfloor 20\sqrt{p} \rfloor + 1$ mögliche Werte.

Vorausgesetzt wir kennen χ modulo p, dann kommen für χ also nur noch $O(\sqrt{p})$ potenzielle Polynome in Frage. Wenn wir für ein gegebenes Polynom $P \in \mathbb{Z}[t]$ prüfen können,

ob $P = \chi$ gilt, können wir sukzessive jedes der verbleibenden Polynome testen und finden nach durchschnittlich $O(\sqrt{p})$ Tests das gesuchte Polynom.

Wir wollen nun darauf eingehen, wie wir diese Gleichheit prüfen können. Dazu stellen wir an P zusätzlich die beiden folgenden notwendigen Bedingungen:

1. Nach den Weil-Vermutungen müssen alle Nullstellen von P den Absolutbetrag $\sqrt{p}$ besitzen.
2. Nach dem Satz von Cayley und Hamilton muss $P(\Phi)$ die Nullabbildung auf dem Tate-Modul $T_l(\mathrm{Jac})$ der jacobischen Varietät liefern.

Die erste Eigenschaft lässt sich einfach überprüfen, indem wir die Nullstellen des gegebenen Polynoms über $\mathbb{C}$ approximieren. Die zweite Eigenschaft ist dank der Isomorphie $\mathrm{End}(\mathcal{A}) \otimes_{\mathbb{Z}} \mathbb{Z}_l \cong \mathrm{End}(T_l(\mathcal{A}))$ aus Satz 1.45 gleichbedeutend damit, dass $\chi(\Phi)$ die Nullabbildung auf der jacobischen Varietät Jac ist. Wie wir diese Eigenschaft testen können werden wir im nächsten Abschnitt behandeln.

Diese Bedingungen sind jedoch nicht hinreichend für die Gleichheit $P = \chi$, wir können allerdings schließen, dass alle Linearfaktoren von χ auch in P auftreten. Damit wissen wir, dass χ von der Form

$$\chi(t) = \prod_{i=1} (t - \alpha_i)^{e_i} \tag{5.6}$$

ist, wobei α_i die Nullstellen von P bezeichnen und $e_i \geq 0$ gilt. Da wir eine Menge von potenziellen Polynomen gegeben haben, von der wir wissen, dass das korrekte Polynom enthalten ist, erhalten wir letztendlich eine nichtleere Menge von Polynomen P mit $P(\Phi) = 0$. Davon können wir diejenigen Polynome ausschließen, deren Anzahl paarweise verschiedener Nullstellen größer ist als bei anderen. Die Nullstellenmenge der verbleibenden Polynome ist dann gleich der Nullstellenmenge von χ und die Polynome unterscheiden sich nur noch durch die Vielfachheiten ihrer Nullstellen. Im Fall $g = 3$ besagt das folgende Lemma, dass genau ein Polynom übrig bleibt.

Lemma 5.8. *Es existiert genau ein Polynom mit den oben beschriebenen Eigenschaften.*

Beweis. Angenommen P_1 und P_2 seien zwei solche Polynome mit der gleichen Anzahl paarweise verschiedener Nullstellen. Da kein Polynom mit den beschriebenen Eigenschaften existiert, das weniger Nullstellen besitzt, haben die Polynome P_1, P_2 und χ die gleiche Nullstellenmenge $\{\alpha_1, \ldots, \alpha_{2r} \mid \alpha_i \in \mathbb{C}\}$. Die Anzahl der paarweise verschiedenen Nullstellen ist gerade, denn nach Korollar 2.3 ist mit jeder Nullstelle auch ihre komplex Konjugierte eine Nullstelle (das heißt insbesondere, dass alle reellen Nullstellen doppelt auftreten). Außerdem tritt mit jeder reellen Nullstelle $\sqrt{p}$ auch $-\sqrt{p}$ als Nullstelle auf, da p keine Quadratzahl in $\mathbb{Z}$ ist.

Für den Fall, dass die Anzahl der paarweise verschiedenen Nullstellen zwei ist, folgt unmittelbar $P_1(t) = (t - \alpha)^3(t - \overline{\alpha})^3 = P_2(t)$ für ein $\alpha \in \mathbb{C}$. Ebenso folgt die Identität $P_1 = P_2$, wenn P_1 und P_2 jeweils sechs verschiedene Nullstellen besitzen.

Es bleibt also noch der Fall

$$\begin{aligned} P_1(t) &= (t-\alpha_1)^2(t-\overline{\alpha}_1)^2(t-\alpha_2)(t-\overline{\alpha}_2) \text{ und} \\ P_2(t) &= (t-\alpha_1)(t-\overline{\alpha}_1)(t-\alpha_2)^2(t-\overline{\alpha}_2)^2 \end{aligned}$$

mit $\alpha_1, \alpha_2 \in \mathbb{C}$ und $\alpha_1 \neq \alpha_2 \neq \overline{\alpha}_1$. Angenommen, einer dieser Nullstellen sei reell. Dann ist auch die andere Nullstelle reell und die Vielfachheiten müssen übereinstimmen. Dies liefert einen Widerspruch zu obiger Darstellung.

Es gelte also $\alpha_1, \alpha_2 \notin \mathbb{R}$. Die Polynome P_1 und P_2 sind modulo p gleich, das heißt insbesondere, dass (für $p > 144$) die Summen der Nullstellen übereinstimmen. Es folgt $\alpha_1 + \overline{\alpha}_1 = \alpha_2 + \overline{\alpha}_2$ und damit im Widerspruch zur Annahme die Gleichheit $\alpha_1 = \alpha_2$ oder $\alpha_1 = \overline{\alpha}_2$. □

Den Fall $p < 144$ schließen wir an dieser Stelle aus. Da wir an großen p interessiert sind, fällt diese Einschränkung jedoch nicht ins Gewicht.

Wir haben gezeigt, dass wir unter allen Polynomen P_i mit $P_i \equiv \chi \mod p$ und $P_i(\Phi) = 0$ das charakteristische Polynom bestimmen können als das eindeutige Polynom mit der minimalen Anzahl an paarweise verschiedenen Nullstellen.

5.3 Test auf Nullabbildung

In diesem Abschnitt betrachten wir ein Kurve über $\mathbb{F}_q$ vom Geschlecht g und bezeichnen mit Φ den q-Frobenius. Wir wollen beschreiben, wie wir für ein Polynom $P = \sum_{i=0}^{2g} a_i t^{2g-i}$, dessen ganzzahlige Koeffizienten der Abschätzung $|a_i| \leq \binom{2g}{i} q^{i/2}$ genügen, testen können, ob die Abbildung $P(\Phi)$ die Nullabbildung auf der jacobischen Varietät Jac ist. Obwohl wir diese Methode später nur für den Fall $g = 3$ und eine Primzahl q benötigen, wollen wir die Überlegungen allgemein durchführen, denn wir können das Verfahren beispielsweise auch in folgender Situation nutzen:

Es sei eine beliebige Kurve und ein Polynom $P \in \mathbb{Z}[t]$ gegeben und wir wollen überprüfen, ob P das charakteristische Polynom des Frobenius ist. Dann können wir zunächst die notwendigen Bedingungen aus den Weil-Vermutungen (Satz 2.2) überprüfen und anschließend mit dem nachfolgenden Test, die Identität $P(\Phi) = 0$ prüfen. Sollte P jede dieser Eigenschaften besitzen, wissen wir, dass alle Nullstellen des charakteristischen Polynoms χ auch Nullstellen von P sind und wir erhalten eine Menge von Polynomen P_i der Form (5.6) unter denen χ zu finden ist. Durch weitere Tests $P_i(\Phi) = 0$ können wir damit in den meisten Fällen durch Ausschlussverfahren das korrekte Polynom bestimmen. Lediglich in dem Fall, dass χ mehrfache Nullstellen besitzt, kann es passieren, dass wir keine Aussage treffen können. Für diesen Fall wollen wir ein Beispiel anführen:

Es sei $\chi(t) = (t - i\sqrt{p})(t + i\sqrt{p})(t - \sqrt{p})^4(t + \sqrt{p})^4$ das charakteristische Polynom einer Kurve vom Geschlecht fünf über einem Primkörper $\mathbb{F}_p$. Dann gilt auch für das Polynom $P(t) = (t - i\sqrt{p})^3(t + i\sqrt{p})^3(t - \sqrt{p})^2(t + \sqrt{p})^2$ die Identität $P(\Phi) = 0$ und wir

können mit unseren Testmethoden nicht zwischen den beiden Polynomen unterscheiden. In diesem Beispiel sind die beiden Polynome sogar modulo p gleich, das heißt wir können im höhergeschlechtlichen Fall selbst mit der Kenntnis von χ modulo p nicht immer eine Aussage über die Gleichheit $P = \chi$ treffen.

5.3.1 Idee

Wir wollen untersuchen, ob ein Endomorphismus der jacobischen Varietät die Nullabbildung ist. Dabei stellt sich zunächst die Frage nach der Jacobischen selbst, denn diese kennen wir gar nicht. Wir wissen lediglich dass sie existiert und dass ihre $\mathbb{L}$-rationale Punktgruppe für jede algebraische Erweiterung $\mathbb{L}/\mathbb{F}_q$ isomorph zu $\mathcal{C}l^0(\mathbb{L}(C))$ ist. Wir werden die Abbildung $P(\Phi)$ deshalb als Gruppenendomorphismus auf den Klassengruppen $\mathcal{C}l^0(\mathbb{L}(C))$ auffassen ($\mathbb{F}_q \subseteq \mathbb{L} \subseteq \overline{\mathbb{F}}_q$). Die Wirkung von $P(\Phi)$ auf eine Divisorklasse können wir dabei explizit berechnen, denn wir wissen, wie Φ auf den Punkten der Kurve und damit auf den Divisoren operiert.

Die Bedingung $P(\Phi) = 0 \in \mathrm{End}(\mathrm{Jac})$ besagt also, dass jede Divisorklasse $D \in \mathcal{C}l^0(\mathbb{L}(C))$ für ein beliebiges $\mathbb{L} = \mathbb{F}_{q^r}$ ($r \in \mathbb{N}$) auf einen Hauptdivisor abgebildet wird. Wir gehen deshalb folgendermaßen vor:

Wir wählen (für ein noch zu bestimmendes $r \in \mathbb{N}$) einen zufälligen $\mathbb{F}_{q^r}$-rationalen Divisor vom Grad Null und überprüfen, ob dieser auf einen Hauptdivisor abgebildet wird. Ist das nicht der Fall, kann $P(\Phi)$ nicht die Nullabbildung sein und wir sind fertig. Andernfalls ist es natürlich möglich, dass die gewählte Divisorklasse im Kern von $P(\Phi)$ liegt, ohne dass dies die Nullabbildung ist. Wir benötigen also eine Aussage über die Wahrscheinlichkeit, bei der zufälligen Wahl einer $\mathbb{F}_{q^r}$-rationalen Divisorklasse ein Element des Kerns von $P(\Phi)$ zu erhalten.

Wir werden im folgenden die Gruppenisomorphie $\mathrm{Jac}(\mathbb{F}_{q^r}) \cong \mathcal{C}l^0(\mathbb{F}_{q^r}(C))$ stillschweigend verwenden.

Satz 5.9. *Für die Anzahl der $\mathbb{F}_{q^r}$-rationalen Punkte der jacobischen Varietät* Jac *der Kurve $C/\mathbb{F}_q$ vom Geschlecht g gilt*

$$(\sqrt{q^r} - 1)^{2g} \leq \#\mathrm{Jac}(\mathbb{F}_{q^r}) \leq (\sqrt{q^r} + 1)^{2g}.$$

Beweis. Die Aussage folgt unmittelbar mit Satz 2.2 und Korollar 2.3 aus der Identität $\#\mathrm{Jac}(\mathbb{F}_{q^r}) = h(\mathbb{F}_{q^r}(C)) = \prod_{i=1}^{2g}(1 - \alpha_i^r)$ und $|\alpha_i| = \sqrt{q}$. □

Wir wissen, dass sowohl die Multiplikation mit einer von Null verschiedenen, ganzen Zahl als auch die Frobenius-Abbildung Φ eine Isogenie auf der jacobischen Varietät ist und diese Morphismen somit einen endlichen Kern besitzen (siehe Definition 1.43). Damit ist auch die Verknüpfung dieser Morphismen und insbesondere $P(\Phi)$ entweder die Nullabbildung oder eine Isogenie. Falls $P(\Phi) \neq 0$ gilt, können wir also die Kardinalität des Kerns betrachten.

Satz 5.10. *Es gelten die Definitionen wie oben. Dann ist $P(\Phi)$ entweder die Nullabbildung oder es gilt*

$$\#\ker P(\Phi_q) \leq (4q)^{2g^2}.$$

Beweis. Wir nehmen an, dass $P(\Phi)$ nicht die Nullabbildung ist und benutzen die Abschätzung (siehe Abschnitt 1.2.8)

$$\#\ker(P(\Phi)) = \deg_s P(\Phi) \leq \deg P(\Phi) = \det M_{P(\Phi)}.$$

Damit können wir uns vollständig auf lineare Algebra zurückziehen. Die Darstellungsmatrix M_Φ von Φ hat bezüglich einer geeigneten Basis (in einer geeigneten Körpererweiterung von $\mathbb{F}_q$) Jordan-Normalform und ist damit eine obere Dreiecksmatrix mit den Eigenwerten π_j auf der Diagonalen (Aufgrund von Gleichung (2.2) und Satz 2.2 gilt dabei $|\pi_j| = \sqrt{q}$). Die Potenzen von Φ liefern also ebenfalls obere Dreiecksmatrizen und haben als Diagonaleinträge die entsprechenden Potenzen der Eigenwerte. Sowohl die Multiplikation mit einer Konstanten a_i als auch die Addition zweier solcher Matrizen ändert nichts an der oberen Dreiecksform und wir erhalten für $P(\Phi)$ schließlich eine obere Dreiecksmatrix mit den Diagonaleinträgen $a_0\pi_j^{2g} + a_1\pi_j^{2g-1} + \cdots + a_{2g}$ $(j = 1, \ldots, 2g)$. Für den Kern gilt damit

$$\begin{aligned}
\#\ker P(\Phi) &\leq \det M_{P(\Phi)} \\
&= \prod_{j=1}^{2g} a_0\pi_j^{2g} + a_1\pi_j^{2g-1} + \cdots + a_{2g} \\
&\leq \prod_{j=1}^{2g} \sum_{i=0}^{2g} \underbrace{|a_i\pi_j^{2g-i}|}_{\leq \binom{2g}{i} q^g} \\
&\leq \Bigg(\underbrace{\sum_{i=0}^{2g} \binom{2g}{i}}_{=2^{2g}} q^g \Bigg)^{2g} \\
&= (4q)^{2g^2}.
\end{aligned}$$

□

Wenden wir nun diese Aussagen auf unsere Situation an. Angenommen, $P(\Phi)$ ist nicht die Nullabbildung. Setzen wir $r \in \mathbb{N}$ so, dass $\#\mathrm{Jac}(\mathbb{F}_{q^r}) > \#\ker P(\Phi)$ gilt, hat der Kern der Abbildung $P(\Phi)$, eingeschränkt auf $\mathrm{Jac}(\mathbb{F}_{q^r})$, als Untergruppe mindestens den Index $\left\lceil \frac{\#\mathrm{Jac}(\mathbb{F}_{q^r})}{\#\ker P(\Phi)} \right\rceil \geq 2$. Wenn wir also eine zufällige $\mathbb{F}_{q^r}$-rationale Divisorklasse wählen, ist die Wahrscheinlichkeit, dass diese Klasse nicht im Kern liegt $\geq 0,5$. Mit Hilfe der Abschätzungen der Sätze 5.9 und 5.10 sehen wir, dass wir dazu r in der Größenordnung $2g$ wählen müssen (für großes q).

Setzen wir r groß genug, erhalten wir sogar eine beliebig hohe Wahrscheinlichkeit, dass eine zufällige Divisorklasse nicht im Kern liegt. Alternativ können wir für ein „kleines“ r mehrere Divisoren wählen und abschätzen, mit welcher Wahrscheinlichkeit mindestens eines dieser Elemente nicht im Kern liegt.

Damit erhalten wir einen Monte-Carlo-Algorithmus, der für ein gegebenes Polynom P entweder die Aussage $P(\Phi) = 0$ mit einer beliebig kleinen Fehlerwahrscheinlichkeit trifft, oder das Ergebnis $P(\Phi) \neq 0$ (ohne Fehler) liefert.

5.3.2 Wahl einer zufälligen Divisorklasse

Für den oben beschriebenen Test, werden „zufällige“ Divisorklassen benötigt. Wir wollen nun darauf eingehen, wie wir solche Divisorklassen vom Grad Null eines Funktionenkörpers $F := \mathbb{F}_q(C)$ bestimmen können. Mit „zufällig“ meinen wir im Folgenden, dass wir pseudozufällig ein Element aus einer Menge mit möglichst gleichverteilter Wahrscheinlichkeit wählen.

Wir stellen zunächst fest, dass die Divisorklassen vom Grad Null in Bijektion mit den Divisorklassen eines beliebigen Grades $d \in \mathbb{N}$ stehen. Beispielsweise liefert jeder Divisor A vom Grad Eins eine solche Bijektion durch

$$[\cdot]_A : \mathcal{C}l^d(F) \to \mathcal{C}l^0(F),\ D \mapsto [D]_A := D - dA. \tag{5.7}$$

Wir können uns also darauf beschränken, eine zufällige Divisorklasse eines beliebigen Grades zu bestimmen und erhalten dann mittels $[\cdot]_A$ eine zufällige Divisorklasse vom Grad Null.

Um eine Klasse vom Grad d zu wählen, werden wir einen zufälligen Primdivisor vom Grad d wählen und dessen Klasse betrachten. Dazu müssen wir allerdings wissen, dass sich die Primdivisoren eines bestimmten Grades gleichmäßig auf die Klassen verteilen. Das wollen wir nun untersuchen.

Zunächst eine Aussage über die Anzahl der Primdivisoren.

Lemma 5.11. *Es bezeichne B_d die Anzahl der Primdivisoren vom Grad d des Funktionenkörpers F einer Kurve $C/\mathbb{F}_q$ vom Geschlecht g. Es gilt*

$$\left| B_d - \frac{q^d}{d} \right| < (2 + 7g)\frac{q^{d/2}}{d}.$$

Beweis. Siehe [Sti93, V.2.10.]. □

Nun wollen wir klären, wie sich diese Primdivisoren auf die Divisorklassen $\mathcal{C}l^d(F)$ verteilen.

Lemma 5.12. *Es sei $D \in \mathcal{C}l^d(F)$ beliebig und $B_{d,D}$ bezeichne die Anzahl der Primdivisoren in der Klasse D. Dann gilt*

$$\left| B_{d,D} - \frac{1}{h} B_d \right| \leq (2g-2) q^{d/2}.$$

Beweis. Wir bezeichnen mit $(\mathcal{C}l^0)^*$ und $\mathcal{C}l^*$ die Charaktergruppen von $\mathcal{C}l^0(F)$ beziehungsweise von $\mathcal{C}l(F)$ und nennen einen Charakter $\widetilde{\chi} \in \mathcal{C}l^*$ *von endlicher Ordnung*, falls dessen Kern endlichen Index in $\mathcal{C}l(F)$ besitzt. Charaktere endlicher Ordnung bilden jedes Element auf den Einheitskreis in $\mathbb{C}$ ab. Außerdem bezeichnen wir mit $\widetilde{\chi} \in \mathcal{C}l^*$ eine beliebige Fortsetzung endlicher Ordnung eines $\chi \in (\mathcal{C}l^0)^*$ auf $\mathcal{C}l(F)$.

Es seien $d \in \mathbb{N}$, $D \in \mathcal{C}l^0(F)$ beliebig und $A \in \mathcal{D}(F)$ ein beliebiger, fixierter Divisor vom Grad Eins. Es gilt mit Hilfe der Orthogonalitätsrelation für die endliche Gruppe $\mathcal{C}l^0$ ([SP07, Satz 7.14]) und der Isomorphie $\mathcal{C}l^0 \cong (\mathcal{C}l^0)^*$:

$$\begin{aligned}
B_{d,D} &= \sum_{P \in \mathcal{P}l^d} \frac{1}{h} \sum_{\chi \in (\mathcal{C}l^0)^*} \chi\left([P]_A - D\right) \\
&= \frac{1}{h} \sum_{\chi \in (\mathcal{C}l^0)^*} \frac{1}{\chi(D)} \sum_{P \in \mathcal{P}l^d} \chi\left(P - dA\right) \\
&= \frac{1}{h} \sum_{\chi \in (\mathcal{C}l^0)^*} \frac{1}{\widetilde{\chi}(D+dA)} \sum_{P \in \mathcal{P}l^d} \widetilde{\chi}(P) \\
&= \frac{1}{h} B_d + \frac{1}{h} \sum_{\substack{\chi \in (\mathcal{C}l^0)^* \\ \chi \neq 1}} \frac{1}{\widetilde{\chi}(D+dA)} \sum_{P \in \mathcal{P}l^d} \widetilde{\chi}(P).
\end{aligned}$$

Da $\widetilde{\chi}$ ein Charakter endlicher Ordnung ist, gilt $|\widetilde{\chi}(D+dA)| = 1$ für alle $D \in \mathcal{C}l^0(F)$ und damit

$$\begin{aligned}
\left| B_{d,D} - \frac{1}{h} B_d \right| &= \left| \frac{1}{h} \sum_{\substack{\chi \in (\mathcal{C}l^0)^* \\ \chi \neq 1}} \frac{1}{\widetilde{\chi}(D+dA)} \sum_{P \in \mathcal{P}l^d} \widetilde{\chi}(P) \right| \\
&\leq \frac{1}{h} \sum_{\substack{\chi \in (\mathcal{C}l^0)^* \\ \chi \neq 1}} 1 \cdot \left| \sum_{P \in \mathcal{P}l^d} \widetilde{\chi}(P) \right| \\
&\leq \left| \sum_{P \in \mathcal{P}l^d} \widetilde{\chi}(P) \right|. \qquad (5.8)
\end{aligned}$$

Für die weitere Abschätzung benötigen wir die beiden folgenden Aussagen:

(1) Für eine arithmetische Funktion $f : \mathbb{N} \to \mathbb{C}$ und ihre summatorische Funktion $h(n) := \sum_{r|n} f(r)$ gilt die Möbius-Umkehrformel $f(n) = \sum_{r|n} \mu(\frac{n}{r})h(r)$, wobei μ die Möbiusfunktion bezeichnet (siehe [SP07, Satz 3.15]).

(2) Mit einem Charakter $\widetilde{\chi} \in \mathcal{C}l^*$ endlicher Ordnung, der eingeschränkt auf $\mathcal{C}l^0(F)$ nicht der Hauptcharakter ist, gilt für jedes $d \in \mathbb{N}$

$$k(r) := \sum_{\substack{P \in \mathcal{P}l^s \\ s|r}} s \cdot \widetilde{\chi}(P)^{d/s} = -\sum_{i=1}^{2g-2} \omega_i(\widetilde{\chi}^{d/r})^r,$$

mit $|\omega_i(\widetilde{\chi}^{d/r})| = \sqrt{q}$ für $i = 1, \ldots, 2g-2$ (siehe [Hes99, Satz 3.2. und 3.10.]). Der Ausdruck $\widetilde{\chi}^{d/r}$ bezeichnet hier den durch $\widetilde{\chi}^{d/r}(P) := (\widetilde{\chi}(P))^{d/r}$ definierten Charakter.

Wir definieren für ein festes $d \in \mathbb{N}$ die arithmetische Funktion

$$f_d(n) := \sum_{P \in \mathcal{P}l^n} n \cdot \widetilde{\chi}(P)^{d/n}$$

und sehen, dass für den Term aus (5.8) gilt:

$$\sum_{P \in \mathcal{P}l^d} \widetilde{\chi}(P) = \frac{1}{d} f_d(d). \tag{5.9}$$

Nun sei h die summatorische Funktion von f_d, also $h(n) = \sum_{r|n} f_d(r)$, dann liefert (1) die Identität

$$f_d(n) = \sum_{r|n} \mu(\frac{n}{r})h(r)$$

und aus (5.9) folgt weiter

$$\begin{aligned}
\frac{1}{d} f_d(d) &= \frac{1}{d} \sum_{r|d} \mu(\frac{d}{r})h(r) \\
&= \frac{1}{d} \sum_{r|d} \mu(\frac{d}{r}) \sum_{s|r} f_d(s) \\
&= \frac{1}{d} \sum_{r|d} \mu(\frac{d}{r}) \sum_{s|r} \sum_{P \in \mathcal{P}l^s} s \cdot \widetilde{\chi}(P)^{d/s} \\
&= \frac{1}{d} \sum_{r|d} \mu(\frac{d}{r}) \sum_{\substack{P \in \mathcal{P}l^s \\ s|r}} s \cdot \widetilde{\chi}(P)^{d/s} \\
&\overset{(2)}{=} \frac{1}{d} \sum_{r|d} \mu(\frac{d}{r}) \left(-\sum_{i=1}^{2g-2} \omega_i(\widetilde{\chi}^{d/r})^r \right).
\end{aligned}$$

Zusammenfassend ergibt sich

$$\begin{aligned}\left|B_{d,D} - \frac{1}{h}B_d\right| &\leq \left|\frac{1}{d}f_d(d)\right| \\ &\leq \frac{1}{d}\sum_{r|d}\underbrace{\left|\mu(\frac{d}{r})\right|}_{\leq 1}\cdot\sum_{i=1}^{2g-2}\underbrace{|\omega_i(\widetilde{\chi})^r|}_{=q^{r/2}\leq q^{d/2}} \\ &\leq (2g-2)q^{d/2}\end{aligned}$$

und damit die Behauptung. □

Nun sind wir in der Lage zu bestimmen, wie groß wir d wählen müssen, so dass sich die Primdivisoren vom Grad d gleichmäßig auf die Divisorklassen verteilen. Die Wahrscheinlichkeit $P(D)$, dass ein zufällig gewählter Primdivisor vom Grad d in einer bestimmten Divisorklasse D liegt, sollte also möglichst nahe an $\frac{1}{h}$ liegen. Lemma 5.12 liefert die Abschätzung

$$\frac{\frac{1}{h}B_d - (2g-2)q^{d/2}}{B_d} \leq P(D) \leq \frac{\frac{1}{h}B_d + (2g-2)q^{d/2}}{B_d}$$

und damit

$$\left|P(D) - \frac{1}{h}\right| \leq \frac{(2g-2)q^{d/2}}{B_d} =: e$$

für jede beliebige Klasse $D \in \mathcal{C}l^d(F)$. Um zu gewährleisten, dass wir jede Klasse mit einer positiven Wahrscheinlichkeit wählen, sollte offensichtlich $e < \frac{1}{h}$ gelten. Da B_d (für wachsendes d) exponentiell in q wächst und $d \in \mathbb{N}$ geeignet gewählt wurde, sind wir in der Lage den Wert e beliebig klein werden zu lassen. Damit können wir eine Wahrscheinlichkeitsverteilung erhalten, die beliebig nahe an einer Gleichverteilung ist.

Für die Anzahl der Primdivisoren in einer beliebigen Klasse $D \in \mathcal{C}l^d(F)$ gilt

$$\begin{aligned}B_{d,D} &\geq \frac{1}{h}B_d - (2g-2)q^{d/2} \\ &\geq \frac{1}{(\sqrt{q}+1)^{2g}}\left(\frac{q^d}{d} - (2+7g)\frac{q^{d/2}}{d}\right) - (2g-2)q^{d/2} \\ &= \frac{q^d - (2+7g)q^{d/2}}{d(\sqrt{q}+1)^{2g}} - (2g-2)q^{d/2}. \qquad (5.10)\end{aligned}$$

Diese Anzahl ist genau dann positiv, wenn $e < \frac{1}{h}$ und wir sehen, dass wir d in der Größenordnung $2g$ wählen müssen, um das zu erreichen.

Die bisherigen Überlegungen setzen voraus, dass wir in der Lage sind, einen Primdivisor beliebigen Grades d zufällig zu wählen. Darauf wollen wir nun genauer eingehen.

Ein Primdivisor vom Grad d des Funktionenkörpers $F = \mathbb{F}_q(C)$ entspricht einem $\mathbb{F}_{q^d}$-rationalen Punkt der Kurve, der für kein $s < d$ bereits $\mathbb{F}_{q^s}$-rational ist. Um einen solchen

Punkt zu bestimmen, wählen wir zunächst ein zufälliges Element $a \in \mathbb{F}_{q^d}$ (wir setzen voraus, dass wir dazu in der Lage sind) und testen, ob das Polynom $f(a, y)$ mindestens eine Nullstelle in $\mathbb{F}_{q^d}$ besitzt. Falls ja, wählen wir zufällig eine dieser Nullstellen $b \in \mathbb{F}_{q^d}$ und prüfen für alle echten Teiler s von d, ob das Tupel (a, b) in $\mathbb{F}_{q^s}^2$ liegt. Ist das nicht der Fall, haben wir einen Punkt (a, b), welcher einen Primdivisor P vom Grad d in F liefert. Mit der Bezeichnung $n := [F : \mathbb{F}_q(x)]$ hat die beschriebene Methode folgende Eigenschaften:

- Es ist ausgeschlossen, einen Punkt im Unendlichen des gewählten affinen Teils zu erhalten (davon existieren maximal n Stück).
- Die Wahrscheinlichkeit, einen Punkt zu wählen kann bis zum Faktor n variieren. Das folgt aus der Tatsache, dass für ein gewähltes $a \in \mathbb{F}_{q^d}$ bis zu n verschiedene $b_1, \ldots, b_n \in \mathbb{F}_{q^d}$ existieren können, so dass $f(a, b_i) = 0$ $(i = 1, \ldots, n)$ gilt.

Wenn wir $d \in \mathbb{N}$ nun so wählen, dass für beliebiges D die Abschätzung $B_{d,D} > n$ gilt, folgt für die beschriebene Wahl einer Divisorklasse:

- Die Wahrscheinlichkeit, eine beliebige Divisorklasse zu wählen ist größer als Null.
- Die Wahrscheinlichkeiten, bestimmte Klassen zu wählen unterscheiden sich maximal durch einen von n abhängigen Faktor.

Diese Eigenschaften einer „zufälligen“ Wahl sind für unsere Zwecke vollkommen ausreichend.

Für eine so gewählte Divisorklasse $D \in \mathcal{C}l^d(F)$ erhalten wir mit Hilfe der Bijektion (5.7) durch $P - dA$ letztendlich eine Divisorklasse vom Grad Null (wobei A ein fixierter Divisor vom Grad Eins ist).

5.4 Der Algorithmus

Wir gehen nun auf die Implementierung des beschriebenen Verfahrens ein.

5.4.1 Berechnung von χ modulo p

Wir bezeichnen mit $f(x, y) = y^a - h(x)$ wieder das definierende Polynom der superelliptischen Kurve mit $b := \deg h$. Um so eine Kurve vom Geschlecht drei zu definieren, haben wir folgende Möglichkeiten:

(I) $a = 2$ und $b = 7$,

(II) $a = 3$ und $b = 4$,

(III) $a = 4$ und $b = 3$,

(IV) $a = 7$ und $b = 2$.

Bevor wir mit der Berechnung des Cartier-Operators beginnen, benötigen wir eine Basis der holomorphen Differentiale, also drei $\mathbb{F}_p$-linear unabhängige Polynome u_1, u_2, u_3, so dass $u_i \frac{dx}{f_y}$ holomorph ist (denn die holomorphen Differentiale bilden eine $\mathbb{F}_p$-Vektorraum der Dimension g). Diese liefert der folgende Satz:

Satz 5.13. *Für die oben genannten Fälle (I) bis (IV) liefern die folgenden Polynome $u_1, u_2, u_3 \in \mathbb{F}_p[x, y]$ eine Basis $u_i \frac{dx}{f_y}$ der holomorphen Differentiale des zugehörigen Funktionenkörpers:*

(I) $u_1 = 1,\ u_2 = x,\ u_3 = x^2$

(II) $u_1 = 1,\ u_2 = x,\ u_3 = y$

(III) $u_1 = 1,\ u_2 = x,\ u_3 = y$

(IV) $u_1 = 1,\ u_2 = y,\ u_3 = y^2$

Beweis. Dass die Elemente $\mathbb{F}_p$-linear unabhängig sind ist offensichtlich. Es bleibt also nur zu zeigen, dass alle Differentiale $u_i \frac{dx}{f_y}$ holomorph sind. Wir beschränken uns auf den Fall (I), die anderen Fälle lassen sich vollkommen analog beweisen.

Wir betrachten den Divisor $\left(u_i \frac{dx}{f_y}\right)$ und erhalten mit den Beispielen 1.29 und 1.39:

$$\begin{aligned}\left(u_i \frac{dx}{f_y}\right) &= (u_i) + (dx) - (2y) \\ &= (u_i) + (\alpha_1, 0) + \ldots + (\alpha_7, 0) - 3P_\infty - ((\alpha_1, 0) + \ldots + (\alpha_7, 0) - 7P_\infty) \\ &= (u_i) + 4P_\infty\end{aligned}$$

Das Differential $u_i \frac{dx}{f_y}$ ist also genau dann holomorph, wenn $(u_i) \geq -4P_\infty$ gilt. Aufgrund von $\mathrm{ord}_\infty(x) = -2$ und $\mathrm{ord}_\infty(y) = -7$ sehen wir, dass die Differentiale $x^i \frac{dx}{f_y}$ für $i = 0, 1, 2$ holomorph sind und die Behauptung gilt. □

Nun können wir aus der Darstellung (5.2) bestimmen, welche Koeffizienten des Polynoms $F = \sum_{k,l} F_{k,l} x^k y^l = f^{p-1}$ wir benötigen, um die relevanten Koeffizienten der Polynome $f^{p-1} u_i$ zu bestimmen. Für die Hasse-Witt-Matrix der genannten Fälle gilt

(I):

$$M = \begin{pmatrix} F_{p-1,p-1} & F_{2p-1,p-1} & F_{3p-1,p-1} \\ F_{p-2,p-1} & F_{2p-2,p-1} & F_{3p-2,p-1} \\ F_{p-3,p-1} & F_{2p-3,p-1} & F_{3p-3,p-1} \end{pmatrix}$$

(II) und (III):

$$M = \begin{pmatrix} F_{p-1,p-1} & F_{2p-1,p-1} & F_{p-1,2p-1} \\ F_{p-2,p-1} & F_{2p-2,p-1} & F_{p-2,2p-1} \\ F_{p-1,p-2} & F_{2p-1,p-2} & F_{p-1,2p-2} \end{pmatrix}$$

(IV):

$$M = \begin{pmatrix} F_{p-1,p-1} & F_{p-1,2p-1} & F_{p-1,3p-1} \\ F_{p-1,p-2} & F_{p-1,2p-2} & F_{p-1,3p-2} \\ F_{p-1,p-3} & F_{p-1,2p-3} & F_{p-1,3p-3} \end{pmatrix}$$

Wir erinnern an die Darstellung

$$F(x,y) := \sum_{j=0}^{p-1} h^j(x) y^{(p-1-j)a}$$

und daran, dass der Koeffizient $F_{k,l}$ genau dann ungleich Null ist, wenn l von a geteilt wird. Wir können die beschriebenen Matrizen also durch Koeffizienten der Polynome $\sum_i H_i^{(N)} x^i := h^N(x)$ ausdrücken und erhalten die folgenden Darstellungen:

(I):

$$M = \begin{pmatrix} H_{p-1}^{(\frac{p-1}{2})} & H_{2p-1}^{(\frac{p-1}{2})} & H_{3p-1}^{(\frac{p-1}{2})} \\ H_{p-2}^{(\frac{p-1}{2})} & H_{2p-2}^{(\frac{p-1}{2})} & H_{3p-2}^{(\frac{p-1}{2})} \\ H_{p-3}^{(\frac{p-1}{2})} & H_{2p-3}^{(\frac{p-1}{2})} & H_{3p-3}^{(\frac{p-1}{2})} \end{pmatrix}$$

(II):

- $p \equiv 1 \mod 3$:

$$M = \begin{pmatrix} H_{p-1}^{(\frac{2p-2}{3})} & H_{2p-1}^{(\frac{2p-2}{3})} & 0 \\ H_{p-2}^{(\frac{2p-2}{3})} & H_{2p-2}^{(\frac{2p-2}{3})} & 0 \\ 0 & 0 & H_{p-1}^{(\frac{p-1}{3})} \end{pmatrix}$$

- $p \equiv 2 \mod 3$:

$$M = \begin{pmatrix} 0 & 0 & H_{p-1}^{(\frac{2p-1}{3})} \\ 0 & 0 & H_{p-2}^{(\frac{2p-1}{3})} \\ H_{p-1}^{(\frac{p-2}{3})} & H_{2p-1}^{(\frac{p-2}{3})} & 0 \end{pmatrix}$$

(III):

- $p \equiv 1 \mod 4$:

$$M = \begin{pmatrix} H_{p-1}^{(\frac{3p-3}{4})} & H_{2p-1}^{(\frac{3p-3}{4})} & 0 \\ H_{p-2}^{(\frac{3p-3}{4})} & H_{2p-2}^{(\frac{3p-3}{4})} & 0 \\ 0 & 0 & H_{p-1}^{(\frac{2p-2}{4})} \end{pmatrix}$$

- $p \equiv 3 \mod 4$:

$$M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & H_{p-1}^{(\frac{2p-2}{4})} \end{pmatrix}$$

(IV):

- $p \equiv 1 \mod 7$:

$$M = \begin{pmatrix} H_{p-1}^{(\frac{6p-6}{7})} & 0 & 0 \\ 0 & H_{p-1}^{(\frac{5p-5}{7})} & 0 \\ 0 & 0 & H_{p-1}^{(\frac{4p-4}{7})} \end{pmatrix}$$

- $p \equiv 2 \mod 7$:

$$M = \begin{pmatrix} 0 & 0 & 0 \\ H_{p-1}^{(\frac{6p-5}{7})} & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

- $p \equiv 3 \mod 7$:

$$M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & H_{p-1}^{(\frac{4p-5}{7})} \\ H_{p-1}^{(\frac{6p-4}{7})} & 0 & 0 \end{pmatrix}$$

- $p \equiv 4 \mod 7$:

$$M = \begin{pmatrix} 0 & H_{p-1}^{(\frac{5p-6}{7})} & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

- $p \equiv 5 \mod 7$:

$$M = \begin{pmatrix} 0 & 0 & H_{p-1}^{(\frac{4p-6}{7})} \\ 0 & 0 & 0 \\ 0 & H_{p-1}^{(\frac{5p-4}{7})} & 0 \end{pmatrix}$$

- $p \equiv 6 \mod 7$ oder $p = 7$:

$$M = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$$

Damit haben wir die Hasse-Witt-Matrix einer beliebigen superelliptischen Kurve vom Geschlecht drei in den Koeffizienten von $h^N \in \mathbb{F}_p[x]$ (für geeignete $N \in \mathbb{N}$) ausgedrückt. Da wir eigentlich an den charakteristischen Polynomen dieser Matrizen interessiert sind, können wir im Fall (IV) mit $p \not\equiv 1 \mod 7$ das charakteristische Polynom χ_M direkt als t^3 angeben und ersparen uns jegliche Rechnungen.

In den anderen Fällen liefert der nachfolgende Algorithmus die gesuchten Koeffizienten. Da dieser zur Berechnung eines Koeffizienten H_k auch immer die Koeffizienten $H_{k-1}, \ldots, H_{k+1-b}$ liefert, müssen wir maximal drei solcher Vektoren $(H_{k+1-b}, \ldots, H_k)$ berechnen.

Algorithmus 10 : Berechnung einzelner Koeffizienten von Polynompotenzen

Eingabe : Ein Polynom $h(x) = \sum_i h_i x^i \in \mathbb{F}_p[x]$ mit $h_0 \neq 0$ vom Grad b und $N, k \in \mathbb{N}$.

Ausgabe : $(H_{k+1-b}, \ldots, H_{k-1}, H_k) \in \mathbb{F}_p^b$, so dass $h^N(x) = \sum_i H_i x^i$.

begin

$\widetilde{A} \in \mathbb{Z}_p[X]^{b \times b} \leftarrow$ modifizierte Begleitmatrix mittels (5.5)

$U_0 \in \mathbb{Z}_p^b \leftarrow$ Startvektor $(0, \ldots, 0, h_0)$

$C(X) \leftarrow \prod_{i=1}^{\lfloor \sqrt{k} \rfloor} \widetilde{A}(X+i)$

$U_k \leftarrow \prod_{j=k}^{\lfloor \sqrt{k} \rfloor^2+1} \widetilde{A}(j) \prod_{j=\lfloor \sqrt{k} \rfloor}^{0} C(j) U_0$

$U_k \leftarrow U_k / k!$

return U_k

end

Für den Fall, dass der konstante Term des Polynoms h Null ist, wenden wir den Algorithmus für $\frac{h}{x}$ an und berechnen davon den Koeffizienten mit Index $k-N$. Wie gesehen, finden die Berechnungen in $\mathbb{Z}_p$ statt. Dazu wählen wir für alle auftretenden Elemente aus $\mathbb{F}_p$ einen beliebigen Lift in $\mathbb{Z}_p$ und reduzieren das Endergebnis modulo p.

Es bleibt noch zu klären, welche Präzisionen wir für $\mathbb{Z}_p$ wählen. Um den Vektor U_k zu berechnen, müssen wir durch $k!$ teilen können. Da k maximal den Wert $3p-1$ annimmt und die p-Bewertung von $(3p-1)!$ genau zwei ist, genügt es in allen Fällen mit drei p-adischen Stellen, also in $\mathbb{Z}/p^3\mathbb{Z}$ zu rechnen.

Zum Abschluss erhalten wir mit Satz 5.3 das charakteristische Polynom des Frobenius modulo p als

$$\chi \equiv t^3 \chi_M \mod p.$$

5.4.2 Berechnung von χ

Wir kennen also χ modulo p. Damit sind wir in der Lage, Indexmengen $I, J, K \subset \mathbb{Z}$ zu bestimmen, so dass alle Polynome der Form

$$t^6 + (a_1 + ip)t^5 + (a_2 + jp)t^4 + (a_3 + kp)t^3 + (a_2 + jp)pt^2 + (a_1 + kp)p^2 t + p^3$$

mit $i \in I, j \in J, k \in K$ den Koeffizientenabschätzungen

$$|a_1 + ip| \leq 6p^{1/2}, \quad |a_2 + jp| \leq 15p, \quad |a_3 + kp| \leq 20p^{3/2}$$

genügen und modulo p gleich χ sind. In dieser Form können wir alle $O(\sqrt{p})$ potenziellen Polynome nacheinander konstruieren und testen, ob deren Nullstellen den Absolutbetrag $\sqrt{p}$ besitzen. Ist das der Fall, speichern wir das Polynom in einer Liste und verwerfen es andernfalls.

Wir benutzen dazu die von KASH3 bereitgestellte Methode, die Nullstellen eines Polynoms über $\mathbb{C}$ zu approximieren. Da der Grad des Polynoms fixiert ist, genügt eine recht grobe Approximation bis auf wenige Nachkommastellen.

Für die verbleibenden Polynome P_i soll nun getestet werden, ob $P_i(\Phi) = 0$ gilt. Dazu bestimmen wir zunächst ein minimales $r \in \mathbb{N}$, so dass die Anzahl der $\mathbb{F}_{p^r}$-rationalen Punkte der Jacobischen größer ist als der Kern der Abbildung $P_i(\Phi)$ (vorausgesetzt, sie ist nicht Null). Wir benutzen dabei die Abschätzungen aus Satz 5.9 und Satz 5.10 und erhalten die Bedingung $p^{r/2} - 1 > (4p)^3$. Damit ist gewährleistet, dass die Gruppe $\mathcal{C}l^0(\mathbb{F}_{p^r}(C))$ nicht komplett im Kern einer von Null verschiedenen Abbildung $P_i(\Phi)$ liegt.

Kommen wir nun zur Bestimmung einer zufälligen Divisorklasse des Funktionenkörpers $F := \mathbb{F}_q(C)$ mit $q := p^r$. Wie bereits beschrieben, werden wir dazu einen Primdivisor eines noch zu bestimmenden Grades d bestimmen, indem wir einen $\mathbb{F}_{q^d}$-rationalen Punkt der Kurve „erraten“, der für kein $s < d$ bereits $\mathbb{F}_{q^s}$-rational ist. Da die definierende Gleichung $f(x, y)$ nach Korollar 2.3 ungefähr q^d Lösungen in $\mathbb{F}_{q^d}^2$ besitzt und zu jedem $a \in \mathbb{F}_{q^d}$ maximal $n := [\mathbb{F}_{q^d}(C) : \mathbb{F}_{q^d}(x)]$ Elemente $b \in \mathbb{F}_{q^d}$ mit $f(a, b) = 0$ existieren, finden wir nach durchschnittlich n Versuchen zu einem zufällig gewählten $a \in \mathbb{F}_{q^d}$ ein $b \in \mathbb{F}_{q^d}$ mit $f(a, b) = 0$ und damit einen $\mathbb{F}_{q^d}$-rationalen Punkt der Kurve. Die Wahrscheinlichkeit, dass dessen Koordinaten bereits in einem echten Teilkörper von $\mathbb{F}_{q^d}$ liegen, ist aufgrund der Abschätzung $|\#C(\mathbb{F}_{q^r}) - q^r - 1| \leq 2g\sqrt{q}^r$ für $r \in \mathbb{N}$ verschwindend gering. Dieser Punkt liefert nun eine Stelle vom Grad d in F und wir erhalten durch Subtrahieren eines fixierten Divisors vom Grad d eine Divisorklasse vom Grad Null.

Um zu gewährleisten, dass jede Divisorklasse gewählt werden kann, wählen wir $d \in \mathbb{N}$ mit Hilfe von (5.10) so, dass $B_{d,D} > n$ für jede Divisorklasse D gilt.

Algorithmus 11 : Wahl einer zufälligen Divisorklasse

Eingabe : Funktionenkörper F mit definierender Gleichung $f(x, y)$ über dem endlichen, exakten Konstantenkörper $\mathbb{F}_q$; Divisor A vom Grad eins.

Ausgabe : Eine zufällige Divisorklasse von F.

begin
  $d \leftarrow$ kleinste natürliche Zahl, so dass $B_{d,D} > n$ gilt (mittels (5.10))
  repeat
    $a \leftarrow$ zufälliges Element von $\mathbb{F}_{q^d}$
    if $f(a, y)$ *hat Nullstelle in* $\mathbb{F}_{q^d}$ **then**
      $b \leftarrow$ zufällige Nullstelle von $f(a, y)$ in $\mathbb{F}_{q^d}$
    end
  until $(a, b) \notin \mathbb{F}_{q^s}^2$ *für alle echten Teiler* s *von* d
  $\mathrm{mipo}_a(x) \leftarrow$ Minimalpolynom (in der Variablen x) von a über $\mathbb{F}_q$
  $\mathrm{mipo}_b(y) \leftarrow$ Minimalpolynom (in der Variablen y) von b über $\mathbb{F}_q$
  $P \leftarrow$ Stelle von F, die durch $\mathrm{mipo}_a(x)$ und $\mathrm{mipo}_b(y)$ erzeugt wird
  return $[P - dA]$
end

Als Nächstes wollen wir für die verbleibenden Polynome P_i und die gewählte Divisorklasse $[D]$ testen, ob die Gleichheit $P_i(\Phi)([D]) = 0$ gilt. Dazu berechnen wir einmalig die Divisoren $\Phi(D), \Phi^2(D), \ldots, \Phi^6(D)$ und testen anschließend für alle i, ob $P_i(\Phi)(D)$ einen Hauptdivisor liefert. Die Polynome P_i mit $P_i(\Phi)([D]) \neq 0$ können wir verwerfen und damit die Anzahl der verbleibenden Polynome, aufgrund der Wahl von $r \in \mathbb{N}$, (in der Regel) mindestens halbieren (in allen berechneten Beispielen blieb noch genau ein Polynom übrig).

Diesen Vorgang wiederholen wir so lange, bis nur noch ein Polynom übrig bleibt, oder wir mit einer ausreichenden Wahrscheinlichkeit sagen können, dass $P_i(\Phi) = 0$ für alle verbleibenden Polynome gilt. Das Polynom mit den wenigsten paarweise verschiedenen Nullstellen liefert dann nach den Überlegungen in Abschnitt 5.2 das charakteristische Polynom χ.

5.5 Rechenaufwand und Beispiele

Eingangs haben wir das Ziel formuliert, einen Algorithmus zu beschreiben, dessen Komplexität in Abhängigkeit von p höchstens $\widetilde{O}(\sqrt{p})$ ist. Dazu darf die Komplexität der beiden anfallenden Schritte $\widetilde{O}(\sqrt{p})$ nicht überschreiten.

Der erste Schritt beginnt mit der Berechnung der Hasse-Witt-Matrix. Dazu müssen bis zu drei Folgenglieder einer linearen Rekurrenz bestimmt werden. Der Index der benötigten Folgenglieder ist dabei in der Größenordnung $O(p)$ und das Berechnen eines solchen Folgengliedes kann nach [BGS03, Proposition 2] in $\widetilde{O}(\sqrt{p})$ Rechenschritten realisiert

werden und wir erhalten nach insgesamt $\widetilde{O}(\sqrt{p})$ Rechenschritten die Hasse-Witt-Matrix.

Das charakteristische Polynom der Hasse-Witt-Matrix liefert eine Menge von $O(\sqrt{p})$ Polynomen, aus der wir das charakteristische Polynom des Frobenius bestimmen wollen. Dazu testen wir jedes einzelne Polynom und es bleibt zu zeigen, dass die Komplexität eines einzelnen Tests höchstens polynomiell von $\log p$ abhängt.

Im ersten Schritt werden die komplexen Nullstellen eines jeden Polynoms numerisch approximiert. Da der Grad des Polynoms und die benötigte Präzision konstant ist, erhalten wir lediglich eine logarithmische Abhänigkeit von p (siehe beispielsweise [Pan95]).

Anschließend wird eine zufällige Stelle vom Grad d gewählt. Dabei bestimmen wir die Nullstellen eines Polynoms $f(a, y)$ in $\mathbb{F}_{p^{rd}}$, was einem Aufwand von $\widetilde{O}(\log p^{rd})$ entspricht (siehe [GG99, Corollary 14.16.]). Nun bestimmen wir die Minimalpolynome von zwei Elementen $a, b \in \mathbb{F}_{p^{rd}}$, erzeugen daraus eine Stelle, subtrahieren einen beliebigen Divisor vom Grad d und erhalten damit einen Repräsentanten einer Divisorklasse vom Grad Null. Insgesamt bleibt dabei die Abhängigkeit der Komplexität von p logarithmisch.

Nun berechnen wir die Potenzen des p-Frobenius auf diesen Divisor, indem wir ihn in Stellen zerlegen und die Koeffizienten der Erzeuger potenzieren. Anschließend bilden wir aus den verbleibenden Polynomen P_i formale $\mathbb{Z}$-Linearkombinationen dieser Divisoren und erhalten die Divisoren $P_i(\Phi)(D)$. Auch in diesem Schritt bleibt die Komplexität für jedes Polynom logarithmisch in p.

Als Nächstes testen wir, ob die Divisoren $P_i(\Phi)(D)$ Hauptdivisoren sind. Dazu wird jeder der Divisoren nach [Hes02] in eine eindeutige, reduzierte Darstellung (bezüglich eines fixierten Divisors vom Grad Eins) gebracht, die genau dann der Nulldivisor ist, falls der ursprüngliche Divisor ein Hauptdivisor war. Die Größe des Konstantenkörpers geht dabei logarithmisch in die Komplexität der Reduktion ein, genauer gesagt logarithmisch in der Höhe der Divisoren $P_i(\Phi)(D)$ (siehe [Hes02, Remark 8.6.]), wobei wir die Höhe durch Kp^3 mit einer Konstanten $K \in \mathbb{R}$ abschätzen können.

Die letzten beiden Schritte müssen wir eventuell mehrmals durchführen, wobei durch die Wahl des Parameters $r \in \mathbb{N}$ die erwartete Anzahl an Wiederholungen (unabhängig von p) beschränkt ist.

Insgesamt erhalten wir damit für die vollständige Berechnung des L-Polynoms die Komplexität $\widetilde{O}(\sqrt{p})$.

Die nachfolgenden Berechnungen wurden in KASH3 durchgeführt. Als Eingabe erwartet der Algorithmus eine Zahl $a \in \mathbb{N}$ und ein Polynom $h \in \mathbb{F}_p[x]$, so dass durch $y^a = h(x)$ eine glatte, superelliptische Kurve vom Geschlecht drei definiert wird.

Wir beginnen mit einer hyperelliptischen Kurve C, die durch

$$y^2 = x^7 + 235x^5 + 19x^4 + 234x^3 + 12x + 1$$

über wechselndem Grundkörper $\mathbb{F}_p$ definiert ist (die Kurve ist für alle gewählten p glatt). In der nachfolgenden Tabelle bezeichnet N die Anzahl der Polynome, die modulo p gleich χ sind und a_i die Koeffizienten des L-Polynoms $L(t) = 1 + a_1 t + a_2 t^2 + a_3 t^3 + \ldots + p^3 t^6$.

p	N	Zeit	Koeffizienten von L	$\#C$
502	27390	$747s$	$a_1 = -15$ $a_2 = 490$ $a_3 = -15576$	137589336
1009	38130	$1045s$	$a_1 = 0$ $a_2 = 480$ $a_3 = 1724$	1027730254
2003	53730	$1538s$	$a_1 = 139$ $a_2 = 10790$ $a_3 = 558894$	8615905472
10007	120060	$4742s$	$a_1 = 95$ $a_2 = 18985$ $a_3 = 1434153$	1011806211127
21503	175980	$8343s$	$a_1 = 189$ $a_2 = 24350$ $a_3 = 1858472$	10030450944290
50503	269670	$18503s$	$a_1 = -228$ $a_2 = 55459$ $a_3 = -13239144$	128231840189440
99809	379110	$30448s$	$a_1 = 122$ $a_2 = 215363$ $a_3 = 26273720$	995517803037684
2120009	1747230	$163321s$	$a_1 = 565$ $a_2 = -770453$ $a_3 = -18621410$	9530787073488921120

Anhand der Tabelle können wir die theoretische berechnete lineare Abhängigkeit der Laufzeit von $\sqrt{p}$ bestätigen und sehen, dass im Vergleich zu den Ergebnissen auf Seite 76, die Abhängigkeit von p erheblich verringert wurde. Obwohl die Kurven, für die wir Kedlayas Algorithmus getestet haben, lediglich Geschlecht zwei hatten, sind wir hier in der Lage deutlich größere Beispiele zu berechnen.

Aus Gründen der Vollständigkeit wollen wir noch einige Beispiele für superelliptische Kurven angeben und erwarten, die Abhängigkeit von der Charakteristik p bestätigen zu können. Dazu betrachten wir wieder einen wechselnden Grundkörper $\mathbb{F}_p$ und die fixierte Gleichung

$$y^3 = x^4 + 1335x^3 + 19x^4 + 214x^2 + 402x + 11,$$

die einen affinen Teil einer glatte Kurve vom Geschlecht drei definiert. Die Spalten der folgenden Tabelle sind wie oben zu interpretieren.

p	N	Zeit	Koeffizienten von L	$\#C$
991	37770	$2445s$	$a_1 = 16$ $a_2 = -358$ $a_3 = -62759$	988537689
5003	84870	$8077s$	$a_1 = 0$ $a_2 = 11175$ $a_3 = 0$	125281054728
9719	118290	$11029s$	$a_1 = 0$ $a_2 = 7227$ $a_3 = 0$	918116888400
20011	169740	$18502s$	$a_1 = -74$ $a_2 = 620$ $a_3 = 2506159$	7983589605903
50021	268410	$43056s$	$a_1 = 0$ $a_2 = 3525$ $a_3 = 0$	125157742486812

Wir merken an, dass bei allen berechneten Beispielen die Wahl eines einzigen Divisors ausreichend war, um alle übrigen Polynome auszuschließen. Für jedes potenzielle Polynom war also genau ein Hauptdivisortest notwendig.

Kapitel 6

Zusammenfassung und Ausblick

Im ersten Teil der vorliegenden Arbeit wurden die theoretischen Grundlagen zur Berechnung von Zetafunktionen algebraischer Kurven über endlichen Körpern erarbeitet. Es wurden die wichtigsten Begriffe aus der algebraischen Geometrie eingeführt und anschließend die Zetafunktion einer Kurve mit ihren Eigenschaften beschrieben.

Nach Vorstellung der Monsky-Washnitzer-Kohomologie wurde der darauf basierende Algorithmus von Kedlaya für hyperelliptische Kurven ausführlich beschrieben und in KASH3 implementiert. Das Programm lief bei allen getesteten Beispielen problemlos und lieferte Ergebnisse, deren Korrektheit mit Hilfe der Ergebnisse des zweiten Teils der Arbeit bestätigt werden konnten.

Bei der Implementierung traten einige Komplikationen auf, welche zum Teil mit der $\mathbb{Z}_q$- beziehungsweise $\mathbb{Q}_q$-Arithmetik in KASH3 zusammenhingen (die gleiche Problematik wurde auch in Magma festgestellt). Neben dem bereits angesprochenen (teilweise) fehlerhaften Umgang mit Präzisionen, lieferte beispielsweise der erweiterte euklidische Algorithmus für Polynome über $\mathbb{Q}_q$ falsche Ergebnisse und es dauerte sehr lange, diese Problemstellen zu finden und zu beheben.

Der vorliegende Algorithmus soll in erster Linie als Umsetzung der theoretischen Ergebnisse dienen und ist sicherlich deutlich laufzeit- und speichereffizienter programmierbar. So blieben unter anderem die Verbesserung von David Harvey [Har06] unberücksichtigt. Trotz alledem ist der Algorithmus erheblich schneller als der von KASH3 bereitgestellte Algorithmus zur Berechnung des L-Polynoms.

Im zweiten Teil der Arbeit wurde zunächst eine effiziente Berechnung des Cartier-Operators für hyperelliptische Kurven mittels linearer Rekurrenzen nach [BGS03] auf den superelliptischen Fall verallgemeinert und implementiert. Mit diesem Algorithmus ist es uns möglich, das L-Polynom einer superelliptischen Kurve über einem Primkörper $\mathbb{F}_p$ modulo p in der Laufzeit $\widetilde{O}(\sqrt{p})$ zu berechnen.

Anschließend wurde eine Methode vorgestellt, mit der es möglich ist, das L-Polynom einer beliebigen Kurve über einem Primkörper vom Geschlecht drei in $\widetilde{O}(\sqrt{p})$ zu bestim-

men, falls das L-Polynom modulo p vorliegt. Dieses Verfahren liefert kombiniert mit der Cartier-Berechnung einen vollständigen Algorithmus zur Bestimmung der Zetafunktion superelliptischer Kurven vom Geschlecht drei über einem Primkörper $\mathbb{F}_p$ in $\widetilde{O}(\sqrt{p})$. Die Methode wurde ebenfalls in KASH3 implementiert und lieferte korrekte Ergebnisse.

Auch hier ist eine Optimierung der Laufzeit möglich. So dürfte beispielsweise der Test, ob alle Nullstellen eines Polynoms einen bestimmten Absolutbetrag besitzen, schneller zu realisieren sein, denn wir approximieren zunächst die Nullstellen in der komplexen Ebene und berechnen daraus ihren Absolutbetrag. Außerdem wurden die Verbesserungen bei der Berechnung des Cartier-Operator nach [BGS03] nicht berücksichtigt.

Da der zweite Schritt dieses Verfahrens für beliebige Kurven anwendbar ist, wäre eine weitere Verallgemeinerung der schnellen Berechnung des Cartier-Operators wünschenswert, um damit einen vollständigen Algorithmus zur Berechnung des L-Polynoms für eine größere Klasse von Kurven zu erhalten.

Symbolverzeichnis

$(f)_0, (f)_\infty$	Nullstellen- und Polstellendivisor eines Elements f	13
$[\cdot]_A$	Abbildung, die jedem Divisor eine Divisorklasse vom Grad Null zuordnet	88
$[n]$	Multiplikation mit n	19
$\mathbb{A}^n(\overline{\mathbb{K}})$,$\mathbb{A}^n$	n-dimensionaler affiner Raum	6
$\mathbb{A}^n_i$	Affiner Teil von $\mathbb{P}^n$	7
$A^\dagger$	Schwache p-adische Vervollstandigung von A	34
$A^\dagger_+$	Schwache p-adische Vervollstandigung von A_+	33
χ	Charakteristisches Polynom des Frobenius	83
χ_φ	Charakteristisches Polynom von φ	20
$\mathcal{C}l$	Divisorenklassengruppe	14
$\mathcal{C}l^d$	Divisorklassen vom Grad d	14
$\mathcal{D}$	Divisorengruppe	12
$\mathcal{D}^n$	Divisoren vom Grad n	12
ι	Hyperelliptische Involution	10
Jac	Jacobische Varietät	19
$\mathbb{K}(V)$	Funktionenkörper der Varietät $V/\mathbb{K}$	6
$\mathbb{K}[V]$	Koordinatenring der Varietät $V/\mathbb{K}$	6
$\mathfrak{C}$	Cartier-Operator	78
$\mathcal{A}[n]$	n-Torsionsgruppe von $\mathcal{A}$	19
$\mathcal{K}$	Restklassenkörper eines Bewertungsringes	2
$\mathcal{L}$	Riemann-Roch Raum	14
$\mathcal{M}$	Maximales Ideal eines Bewertungsringes	2
$\mathcal{R}$	Bewertungsring	2
$\mathcal{O}_P$	Lokaler Ring in P	10
$\overline{A}$	Koordinatenring einer Kurve uber dem endlichen Korper $\mathbb{F}_q$	31
$\Omega^0(F)$	Holomorphe Differentiale von F	16
$\Omega^i_{A/R}$	i-faches äußeres Produkt von $\Omega_{A/R}$	18
$\Omega_{F/K}, \Omega(F)$	Differentialmodul von F über K	16
$\widetilde{O}$	„Soft Oh“	72
$\mathbb{P}^n(\overline{K}), \mathbb{P}^n$	n-dimensionaler projektiver Raum	7
$\mathbb{P}^{n-1}_i$	Projektiver Teil von $\mathbb{P}^n$	7

Φ	q-Frobenius-Abbildung	9
Φ^*	Induzierte Frobenius-Abbildung auf der Kohomologie	26
Φ_p	p-Frobenius	51
$\mathcal{P}l$	Menge aller Stellen	11
$\mathcal{P}$	Menge der Hauptdivisoren	14
$\mathbb{Q}_p$	p-adische Zahlen	2
$\mathbb{Q}_q$	Unverzweigte Erweiterung von $\mathbb{Q}_p$	3
Σ_p	Frobenius-Substitution auf $\mathbb{Q}_q$	4
φ^*	Von φ induzierte Abbildung auf den Funktionenkörpern	8
$\mathbb{Z}_p$	Ganze p-adische Zahlen	2
$\mathbb{Z}_q$	Bewertungsring von $\mathbb{Q}_q$	3
ζ	Zetafunktion einer Kurve	23
A	Lift des Koordinatenringes $\overline{A}$ nach $\mathbb{Q}_q$	32
A^∞	p-adischer Abschluss von A	32
A_+	Lift des Koordinatenringes $\overline{A}$ nach $\mathbb{Z}_q$	32
A_+^∞	p-adischer Abschluss von A_+	32
f_y	Formale, partielle Ableitung des Polynoms f nach der Variablen y	79
g	Geschlecht einer Kurve	14
h	Klassenzahl	14
H^i_{dR}	i-te de Rham-Kohomologiegruppe	18
$H^1_{MW}(C')^+$	Positiver Eigenraum der ersten MW-Kohomologiegruppe	47
$H^1_{MW}(C')^-$	Negativer Eigenraum der ersten MW-Kohomologiegruppe	47
H^i_{MW}	i-te Monsky-Washnitzer-Kohomologiegruppe	34
$I(V)$	Verschwindungsideal der Varietät V	6
L	L-Polynom	24
l	Von p verschiedene Primzahl	19
M	Darstellungsmatrix des q-Frobenius Φ auf $H^1_{MW}(C')^-$	58
M	Hasse-Witt-Matrix	78
M_p	Darstellungsmatrix des p-Frobenius Φ_p auf $H^1_{MW}(C')^-$	58
N_k	Anzahl der $\mathbb{F}_{q^k}$-rationalen Punkte	23
O	Landau O	72
T_l	l-adischer Tate-Modul	20
V_I	Nullstellenmenge eines Ideals I	6

Literaturverzeichnis

[BGS03] Bostan, A. ; Gaudry, P. ; Schost, E.: Linear Recurrences with Polynomial Coefficients and Computation of the Cartier-Manin Operator on Hyperelliptic Curves. In: *International Conference on Finite Fields and Applications*, 2003, S. 40–58

[Cas06] Castryck, W.: *Point counting on nondegenerate curves*, Katholieke Universiteit Leuven, PhD Thesis, 2006

[CF06] Cohen, H. ; Frey, G.: *Handbook of Elliptic and Hyperelliptic Curve Cryptography.* London : Chapman & Hall, 2006

[Che51] Chevalley, C.: *Introduction to the Theory of Algebraic Functions of One Variable.* American Mathematical Society : Mathematical Surveys Number VI, 1951

[DV06a] Denef, J. ; Vercauteren, F.: Computing zeta functions of C_{ab} curves using Monsky-Washnitzer Cohomology. In: *Finite Fields and Their Applications* 12 (2006), S. 78–102

[DV06b] Denef, J. ; Vercauteren, F.: An extension of Kedlaya's algorithm to hyperelliptic curves in characteristic 2. In: *J. Cryptology* 19 (2006), S. 1–25

[Edi03] Edixhoven, B.: Point counting after Kedlaya. In: *EIDMA-Stieltjes Graduate course* (2003)

[Eis95] Eisenbud, D.: *Commutative Algebra with a View Toward Algebraic Geometry.* Berlin-Heidelberg-New York : Springer-Verlag, 1995

[GG99] von zur Gathen, J. ; Gerhard, J.: *Modern Computer Algebra.* Cambridge : Cambridge University Press, 1999

[GG01] Gaudry, P. ; Guerel, N.: An extension of Kedlaya's algorithm to superelliptic curves. In: *Advances in Cryptology – ASIACRYPT 2001* Bd. 2248, Springer-Verlag, 2001, S. 480–494

[GG03] Gaudry, P. ; Guerel, N.: Counting points in medium characteristic using Kedlaya's algorithm. In: *Experimental Mathematics* 12 (2003), S. 395–402

[Har77] HARTSHORNE, R.: *Algebraic Geometry.* Berlin-Heidelberg-New York : Springer-Verlag, 1977

[Har06] HARVEY, D. *Kedlaya's algorithm in larger characteristic.* 2006

[Hes99] HESS, F.: *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern*, Technische Universität Berlin, Dissertation, 1999

[Hes02] HESS, F.: Computing Riemann-Roch spaces in algebraic function fields and related topics. In: *J. Symbolic Comp.* 33 (2002), S. 425–445

[Ked01] KEDLAYA, K. S.: Counting Points on Hyperelliptic Curves using Monsky-Washnitzer Cohomology. In: *Journal of the Ramanujan Mathematical Society* 16 (2001), S. 323–338

[Lan73] LANG, S.: *Elliptic Functions.* Reading, Massachusetts : Addison-Wesley Publishing Company, 1973

[Lan02] LANG, S.: *Algebra.* Berlin-Heidelberg-New York : Springer-Verlag, 2002 (3rd edition, GTM 211)

[Lau04a] LAUDER, A.: Counting solutions to equations in many variable over finite fields. In: *Foundations of Computational Mathematics* 4 (2004), S. 221–267

[Lau04b] LAUDER, A.: Deformation theory and the computation of zeta functions. In: *Proceedings of the London Mathematical Society* 88 (2004), S. 565–602

[Lor90] LORENZ, F.: *Einführung in die Algebra Teil 2.* Mannheim/Wien/Zürich : B.I. Wissenschaftsverlag, 1990

[Lue03] LUETKEBOHMERT, W.: *Codierungstheorie.* Braunschweig : Vieweg Verlag, 2003

[Mad02] MADSEN, M. S.: Determining the group order of a Jacobian from a hyperelliptic curve defined over a finite field of odd characteristic using Monsky and Washnitzer cohomology. (2002). – http://home.imf.au.dk/marc/doc/phd/progress/main.ps

[Man65] MANIN, J. I.: The Hasse-Witt matrix of an algebraic curve. In: *Transactions of the American Mathematical Society* 45 (1965), S. 245–264

[Mil98] MILNE, J.: *Lectures on Etale Cohomology.* course notes. 1998. – http://www.jmilne.org

[Mon68] MONSKY, P.: Formal cohomology. II. The cohomology sequence of a pair. In: *Annals of Mathematics* 88 (1968), S. 218–238

[Mon71] MONSKY, P.: Formal cohomology. III. Fixed point theorems. In: *Annals of Mathematics* 93 (1971), S. 315–343

[Mum70] Mumford, D.: *Abelian Varieties.* London : Oxford University Press, 1970

[MW68] Monsky, P. ; Washnitzer, G.: Formal cohomology. I. In: *Annals of Mathematics* 88 (1968), S. 181–217

[Neu99] Neukirch, J.: *Algebraic Number Theory.* Berlin-Heidelberg-New York : Springer-Verlag, 1999

[Pan95] Pan, V. Y.: Optimal (up to Polylog Factors) Sequential and Parallel Algorithms for Approximating Complex Polynomial Zeros. In: *SIAM Journal on Computing* (1995), S. 741–750

[Pil90] Pila, J.: Frobenius maps of abelian varieties and finding roots of unity in finite fields. In: *Mathematics Of Computation* 55 (1990), S. 745–763

[Put86] van der Put, M.: The cohomology of Monsky and Washnitzer. In: *Mémoires de la Société Mathématique de France* 23 (1986), S. 33–59

[Sat00] Satoh, T.: The Canonical Lift of an Ordinary Elliptic Curve over a Finite Field and its Point Counting. In: *Journal of the Ramanujan Mathematical Society* 15 (2000), S. 247–270

[Sch95] Schoof, R.: Counting Points on Elliptic Curves Over Finite Fields. In: *Journal de Théorie des Nombres de Bordeaux* 7 (1995), S. 219–254

[Sil86] Silverman, J. H.: *The Arithmetic of Elliptic Curves.* Berlin-Heidelberg-New York : Springer-Verlag, 1986

[Sil94] Silverman, J. H.: *Advanced Topics in the Arithmetic of Elliptic Curves.* Berlin-Heidelberg-New York : Springer-Verlag, 1994

[SP07] Schulze-Pillot, R.: *Elementare Algebra und Zahlentheorie.* Berlin-Heidelberg-New York : Springer-Verlag, 2007

[Sti93] Stichtenoth, H.: *Algebraic Function Fields and Codes.* Berlin-Heidelberg-New York : Springer-Verlag, 1993

[SV87] Stoehr, K. ; Voloch, J. F.: A formula for the Cartier operator on plane algebraic curves. In: *Journal für die reine und angewandte Mathematik* 377 (1987), S. 49–64

[Tat52] Tate, J.: Genus change in inseparable extensions of function fields. In: *Proceedings of the American Mathematical Society* 3 (1952), S. 400–406

[Tat66] Tate, J.: Endomorphisms of Abelian Varieties over Finite Fields. In: *Inventiones Mathematicae* 2 (1966), S. 134–144

[Wei49] Weil, A.: Numbers of solutions of equations in finite fields. In: *Bulletin of the American Mathematical Society* 55 (1949), S. 497–508