Algorithmus zur Bestimmung der Zetafunktion von Kurven vom Geschlecht 5

Diplomarbeit

HUMBOLDT-UNIVERSITÄT ZU BERLIN
Mathematisch-Naturwissenschaftliche Fakultät II
Institut für Mathematik

eingereicht von: Sebastian Mitterle
geboren am: 27.04.1982, Offenbach am Main
Betreuer: Prof. Dr. Remke Kloosterman

Berlin, den

Inhaltsverzeichnis

Einleitung

In dieser Arbeit beschäftigen wir uns mit der Berechnung der Zetafunktion von Kurven über endlichen Körpern mittels p-adischer Kohomologie. Von ihr lässt sich die Anzahl ihrer $\mathbb{F}_{p^s}$-rationalen Punkte, die Ordnung ihrer Jakobi-Varietät oder auch die Güte des von ihr abgeleiteten Goppa-Codes ablesen.[1]

Insbesondere betrachten wir den Fall, dass es sich dabei um eine Kurve C vom Geschlecht $g(C) = 5$ handelt. Dieser Aspekt stellt uns vor das Problem, dass für diese Kurven kein glattes Modell als Hyperfläche existiert. Unter anderem deshalb lässt sich die Zetafunktion nicht mit bekannten Algorithmen wie die von Abbot-Kedlaya-Roe [26], Lauder [14] oder Gerkmann [6] berechnen. Möchten wir alternativ auf Kedlayas direkte Methode [10] zurückgreifen, dann steht uns im Allgemein die dafür notwendige Bestimmung einer Basis der entsprechenden Kohomologiegruppen im Wege.

Kloosterman [12] zeigt aber, dass sich der Algorithmus von Abbot, Kedlaya und Roe [26], so modifizieren lässt, dass der Output die Zetafunktion der singulären Hyperfläche $V(F) \subset \mathbb{P}^3_{\overline{\mathbb{F}}_q}$, $F = X_0^2 + X_1^2 + X_2^3 \in \mathbb{F}_q[X_0, X_1, X_2, X_3]$, korrekt berechnet.
Daher wählen wir für eine Kurve vom Geschlecht $g(C) = 5$ ein Modell mit höchstens gewöhnlichen Doppelpunkten als Singularitäten, und versuchen, ihre Zetafunktion zu berechnen, indem wir Kloostermans Ansatz auf diesen Fall übertragen.

[1] Näheres zu Goppa-Codes findet man beispielsweise in [8, Kapitel 13] ihrer Dekodierungsgüte in [23]. Zur Verwendung der Jakobi-Varietät in der *public-key*-Kryptographie siehe u.a. [18].

Im ersten Kapitel werden wir die notwendigen Grundlagen aus der algebraischen Geometrie zusammentragen, die wir benötigen, um die Zetafunktion von Kurven über endlichen Körpern vom Geschlecht 5 zu definieren.

Im zweiten Kapitel entwickeln wir den Algorithmus von Abbot, Kedlaya und Roe für glatte Kurven. Zu diesem Zweck definieren wir die dazu notwendigen Kohomologien und tragen die für uns wichtigen Eigenschaften von p-adischen Kohomologie-Gruppen zusammen.

Im dritten Kapitel übertragen wir den Algorithmus auf den singulären Fall. Wir entwickeln einen Algorithmus ihn für Kurven mit einem gewöhnlichen Doppelpunkt, unabhängig vom Geschlecht, der sich leicht verallgemeinern lässt. Abschließend besprechen wir Präzisionsfragen und präsentieren unsere Resultate.

1 Zetafunktion und Geschlecht von Kurven über endlichen Körpern

In diesem Kapitel behandeln wir die mathematischen Grundlagen, die zur Betrachtung unserer Objekte notwendig sind. Dabei ziehen wir die Definition und Eigenschaften von q-adischen Zahlen vor. Ihr Zusammenhang mit den endlichen Körpern ermöglicht später die Definition einer geeigneten Kohomologie für die Berechnung der Zetafunktion, die wir in Kapitel 2 behandeln. Hier und in allen folgenden Kapiteln sei p eine Primzahl, $q = p^m$, $m \in \mathbb{N}$ eine Primzahlpotenz. Wir werden $\mathbb{N}$ verstehen als $\mathbb{N}_0 - \{0\}$.

1.1 q-adische Zahlen und endliche Körper

In diesem Abschnitt tragen wir die nötigen Kenntnisse über endliche Körper und q-adische Zahlen kurz zusammen und geben die Resultate ohne Beweise an. Für eine ausführlichere Behandlung s. [13, V.5, XII.2 bis XII.6] und [19, II].

Aus der Eindeutigkeit der Primfaktorzerlegung einer ganzen Zahl $z \neq 0$ folgt, dass sie sich eindeutig als $z = p^r \cdot z'$ schreiben lässt, wobei $z' \notin p\mathbb{Z}$. Wir definieren $v_p(z) := r$. Für eine rationale Zahl $z = \frac{z_1}{z_2} \neq 0$ können wir dann $v_p(z) := v_p(z_1) - v_p(z_2)$ definieren. Für $z = 0$, setzen wir $v_p(0) := \infty$. Damit haben wir eine sogenannte *diskrete Bewertung* auf $\mathbb{Q}$ definiert. Durch sie wird wiederum eine Funktion $|\cdot|_p : \mathbb{Q} \to \mathbb{R}$ induziert, indem wir setzen $|z|_p := \frac{1}{p^{v(z)}}$, wobei $\frac{1}{p^\infty} := 0$. Dies ist die sogenannte *p-adische Norm* der rationalen Zahlen. Mittels der p-adischen Norm, wird $\mathbb{Q}$ ein metrischer Raum, den wir vervollständigen können.

Wir erhalten damit den Körper der *p-adischen Zahlen*, geschrieben $\mathbb{Q}_p$. Für sie gilt:

Satz 1.1. *(Eigenschaften der p-adischen Zahlen)*

(i) *Jedes Element $z \in \mathbb{Q}_p$ lässt sich eindeutig darstellen als unendliche Reihe $z = \sum_{i=l}^{\infty} a_i p^i$, $l \in \mathbb{Z}$. Wir schreiben $z \equiv \sum_{i=l}^{N-1} a_i p^i \mod p^N$.*

(ii) *$\upsilon_p(z) := \min\{i \mid a_i \neq 0\}$ ist eine diskrete Bewertung auf $\mathbb{Q}_p$.*

(iii) *Der Bewertungsring $\mathbb{Z}_p := \{z \in \mathbb{Q}_p \mid \upsilon_p(z) \geq 0\}$ ist ein lokaler Ring mit Maximalideal $\mathfrak{p} = \{z \in \mathbb{Q}_p \mid \upsilon_p(z) > 0\}$.*

(iv) *$\mathbb{Z}_p/\mathfrak{p} \cong \mathbb{Z}/p\mathbb{Z}$.*

(v) *$\mathbb{Z} \subset \mathbb{Z}_p$ und $\mathbb{Q} \subset \mathbb{Q}_p$.*

Wir wissen, dass $\mathbb{Z}/p\mathbb{Z}$ ein endlicher Körper mit p Elementen ist. Die endlichen Körper sind vollständig charakterisiert:

Satz 1.2. *(Endliche Körper)*
Sei $\bar{\mathbb{F}}_p$ der algebraische Abschluss von $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, und für $q = p^m$, $m \in \mathbb{N}$, sei $\mathbb{F}_q := \{x \in \bar{\mathbb{F}}_p \mid x^q = x\}$. Dann gilt:

(i) *$\mathbb{F}_q$ ist ein Körper mit q Elementen.*

(ii) *Sei k ein Körper, p seine Charakteristik. Dann existiert ein Körpermonomorphismus $k \hookrightarrow \bar{\mathbb{F}}_p$.*

(iii) *$\mathbb{F}_{p^{m_1}} \subset \mathbb{F}_{p^{m_2}} \Leftrightarrow m_2 \in m_1\mathbb{N}$.*

Endliche Körper der Charakteristik p sind also isomorph zu $\mathbb{F}_{p^m}$ für ein $m \in \mathbb{N}$. Endliche Körpererweiterungen von $\mathbb{F}_p$ stehen in engem Zusammenhang zu endlichen Körpererweiterungen von $\mathbb{Q}_p$:

Satz 1.3. *Seien $u = \sum_{i=0}^{d} a_i X^i \in (\mathbb{Z}_p/\mathfrak{p})[X]$, $a_d \neq \bar{0}$. ein irreduzibles Polynom, $\hat{a}_i \in a_i$ Repräsentanten und $U := \sum_{i=0}^{d} \hat{a}_i X^i \in \mathbb{Z}_p[X]$. Dann gilt:*

(i) *$\mathbb{F}_p[X]/(u) \cong \mathbb{F}_{p^d}$.*

(ii) *Die Norm $|\cdot|_p$ auf $\mathbb{Q}_p$ lässt sich eindeutig auf den Erweiterungskörper $K := \mathbb{Q}_p[X]/(U) \supset \mathbb{Q}_p$ fortsetzen, und K ist bezüglich dieser Norm, die wir ebenfalls mit $|\cdot|_p$ bezeichnen, ein vollständiger Körper.*

(iii) *Die Bewertung υ_p lässt sich eindeutig auf K fortsetzen. Der Bewertungsring R ist lokaler Ring mit Maximalideal $\mathfrak{q} = \mathfrak{p}R$.*

(iv) $R/\mathfrak{q} \cong \mathbb{F}_q$.

Es kann gezeigt werden, dass für eine andere Wahl von U und u mit den Eigenschaften wie in Satz 1.3 die Erweiterungskörper K, K' isomorph sind.

Definition 1.4. (q-adische Zahlen) K aus Satz 1.3 heißt Körper der *q-adischen Zahlen*. Wir schreiben $\mathbb{Q}_q$. Weiterhin nennen wir $\mathbb{Z}_q := R$ *die ganzen q-adischen Zahlen*, und $R/\mathfrak{q}$ heißt *Restklassenkörper* der Bewertung v_p auf $\mathbb{Q}_q$.

Wir sehen, dass nach Konstruktion $\mathbb{Q} \subset \mathbb{Q}_q$, und die Charakteristik des Körpers q-adischer Zahlen also 0 ist. Nach Satz 1.3 können wir eine q-adische Zahl schreiben als $\sum_{i=l}^{\infty} \alpha_i p^i$, $l \in \mathbb{Z}$, wobei $\alpha_i = \sum_{j=0}^{d} \alpha_{i,j} \xi^j$, $\alpha_{i,j} \in \mathbb{Q}_p$ und ξ ist Nullstelle von U. Normalerweise rechnen wir aber mit Computern mit einer endlichen Approximation, d.h. wir kennen eine q-adische Zahl nur bis zu einer bestimmten *Genauigkeit* N. Wir kennen eine q-adische Zahl $z = \sum_{i=l}^{\infty} \alpha_i p^i$ bis zur Genauigkeit N, indem wir $z_N = \sum_{i=l}^{N} \alpha_i p^i$ berechnen. Wir schreiben auch $z \equiv z_N \mod p^N$.

1.2 Algebraische Varietäten

In diesem Abschnitt definieren wir (affine und projektive) algebraische Varietäten und fassen die für unsere Zwecke dienlichen Ergebnisse über sie zusammen. Für eine ausführlichere Darstellung siehe [7, I.1 bis I.6]. In diesem Abschnitt sei k ein beliebiger Körper (z.B. $\mathbb{F}_q$ oder $\mathbb{Q}_q$) und $\bar{k}$ sein algebraischer Abschluss.

In einer ersten Annäherung sind algebraische Varietäten Punktmengen. Aus der linearen Algebra kennen wir beispielsweise die Punktmenge $k^n = \{a = (a_1, ..., a_n) \mid a_i \in k\}$. In der projektiven Geometrie betrachtet man herkömmlich die Menge L aller Geraden in k^{n+1}. Jeder Punkt in L ist eine Gerade in k^{n+1}. Diese Idee lässt sich präzisieren. Wir betrachten zwei Punkte $a, b \in k^{n+1}$ als äquivalent, falls $O := (0, ..., 0) \in \overline{ab}$, der Geraden, die a und b verbindet, i.e. $a = \lambda b$, $\lambda \in k$. O stört uns, da der Ursprung äquivalent zu jedem beliebigem Punkt ($\lambda = 0$) wäre. Betrachten wir also die Punktmenge $L := (k^{n+1} - \{O\})/\{a - \lambda a,\ \lambda \in k^*,\ a \in k^{n+1}\}$. Wir schreiben für Punkte $a \in L$, $a = (a_0 : ... : a_n) = (\lambda a_0 : ... : \lambda a_n)$ und

nennen das Tupel $(a_0 : ... : a_n)$ *homogene Koordinaten* von a.

Nun können wir mit den Punktmengen alleine nicht viel anfangen. Wir versehen sie mindestens mit einer Topologie:

Definition 1.5. Sei X eine Menge und $\mathfrak{T} \subset \mathfrak{P}(X)$ eine Teilmenge der Potenzmenge von X. Dann heißt $\mathfrak{T}$ eine *Topologie* und das Paar $(X, \mathfrak{T})$ *topologischer Raum*, falls folgende Bedingungen erfüllt sind:

- $U, V \in \mathfrak{T} \Rightarrow U \cap V \in \mathfrak{T}$
- $\{U_i,\, i \in I\} \subset \mathfrak{T} \Rightarrow \bigcup_{i \in I} U_i \in \mathfrak{T}$
- $X, \varnothing \in \mathfrak{T}$

Die Mengen $U \in \mathfrak{T}$ heißen *offen* und ihre Komplemente *abgeschlossen*.

Varietäten sind, grob gesprochen, Nullstellenmengen von Polynomen und topologische Räume. Definieren wir zuerst eine passende Topologie auf L, die von Polynomen induziert wird. Dafür ist aber notwendig, dass die Definition nicht von dem Repräsentanten $(a_0, ..., a_n) \in (a_0 : ... : a_n)$ abhängt. Indem wir nur *homogene* Polynome $\sum_{(i_0,...,i_n) \in I} a_{(i_0,...,i_n)} X_0^{i_0} \cdots X_n^{i_n}$, $\exists d \in \mathbb{N}_0$, $\forall (i_0, ..., i_n) \in I : \sum_{j=0}^{n} i_j = d$, betrachten, i.e. bei denen alle Summanden denselben Grad haben, erreichen wir dies, denn dann ist $F(\lambda a) = \sum_{(i_0,...,i_n) \in I} c_{(i_0,...,i_n)} (\lambda a_0)^{i_0} \cdots (\lambda a_n)^{i_n} = \lambda^{i_0+...+i_n} F(a) = \lambda^d F(a)$. Da wir $\lambda \neq 0$ vorausgesetzt haben, ist die Eigenschaft $F(a) \neq 0 \in L$ wohldefiniert.

Satz 1.6. *Für eine Teilmenge homogener Polynome $T \subset k[X_0, ..., X_n]$ sei $D(T) := \{a \in L \mid (\forall F \in T)(F(a) \neq 0)\}$. Dann ist $\mathfrak{T} := \{D(T) \mid T \subset k[X_0, ..., X_n]\}$ eine Topologie auf L.*

Für ein Polynome $F_1, ..., F_t$ schreiben wir kürzer $D(F_1, ..., F_t) := D(\{F_1, ..., F_t\})$.

Definition 1.7. $\mathfrak{T}$ aus obigem Satz heißt *Zariski-Topologie* L. Wir nennen $\mathbb{P}_k^n := (L, \mathfrak{T})$ den *n-dimensionalen projektiven Raum über k*

Wir schreiben die abgeschlossenen Teilmengen als $V(T) := \mathbb{P}_k^n - D(T)$, bzw. $V(F_1, ..., F_t) := V(\{F_1, ..., F_t\})$.

Es ist bekannt, dass jede Teilmenge Y eines topologischen Raums selbst ein topologischer Raum ist, wenn man die *induzierte Topologie* verwendet, $\mathfrak{T}_Y := \{D(T) \cap Y | D(T) \in \mathfrak{T}\}$. Da $a \in \mathbb{P}^n$ nicht vom Repräsentanten abhängt und gelten muss, dass mindestens eine Koordinate $a_i \neq 0$ ist, ist $a = (\frac{a_0}{a_i} : ... : 1 = \frac{a_i}{a_i} : ... : \frac{a_n}{a_i})$. Dadurch sind aber die Koordinaten $\frac{a_{i'}}{a_i}$ mit $i \neq i'$ fixiert. Daraus folgt, dass wir für jedes i eine bijektive (Mengen-)Abbildung haben, o.B.d.A $i = 0$, $\alpha : D(X_0) \to k^n$, $(1 : b_1 : ... : b_n) \mapsto (b_1, ..., b_n)$. Dann können wir die induzierte Topologie von $\mathfrak{T}_{D(X_0)}$ auf k^n übertragen:

Satz 1.8. *Sei $\mathfrak{T}_\alpha := \{\alpha(U) \mid U \in \mathfrak{T}_{D(X_0)}\}$. Dann ist $(k^n, \mathfrak{T}_\alpha)$ ein topologischer Raum.*

Definition 1.9. Wir nennen $\mathbb{A}_k^n := (k^n, \mathfrak{T}_\alpha)$ den *n-dimensionalen affinen Raum über k.*

Bemerkung 1.10. Wir sehen insbesondere, dass sich $\mathbb{P}_k^n$ von den $D(X_i)$, $i \in \{0, ..., n\}$, überdecken lässt.

Weiterhin werden wir von algebraischen Varietäten verlangen, dass sie irreduzibel sind.

Definition 1.11. Ein topologischer Raum X heißt *reduzibel*, falls zwei nichtleere abgeschlossene echte Teilmengen $Y_1, Y_2 \subsetneq X$ existieren, $Y_1 \neq Y_2$, sodass $X = Y_1 \cup Y_2$. Ein topologischer Raum, der keine solche Darstellung zulässt, heißt *irreduzibel*.

Irreduzible Räume haben folgende Eigenschaften:

Satz 1.12. *Sei X ein irreduzibler topologischer Raum, U eine offene Teilmenge von X.*

(i) Sei $\overline{U} := \bigcap_{X \supset C \supset U} C$, wobei die C abgeschlossen in X sind, der Abschluss von U in X. Dann ist $\overline{U} = X$, d.h. offene Teilmengen irreduzibler Räume liegen dicht.

(ii) U mit der induzierten Topologie $\mathfrak{T}_U$ ist ein irreduzibler topologischer Raum.

Definition 1.13. Wir definieren *projektive algebraische Varietäten* V als irreduzible abgeschlossene Teilmengen von $\mathbb{P}_k^n$ für ein $n \in \mathbb{N}$.

Bespiel 1.14. $\mathbb{P}_k^n = V(0)$ ist eine projektive Varietät.

Satz 1.15. *Für eine projektive Varietät $V \subset \mathbb{P}_k^n$, sei $T(V)$ die Menge aller $f \in k[X_0, ..., X_n]$, die homogen sind und die für alle Punkte $P \in V$ verschwinden, $f(P) = 0$. Dann gilt für das Ideal $I(V) := k[X_0, ..., X_n]T(V)$, dass $V = V(I(V))$. Da $k[X_0, ..., X_n]$ noethersch ist, existieren außerdem endlich viele homogene $f_1, ..., f_s$, sodass $I(V) = (f_1, ..., f_s)$, i.e. $V = V(f_1, ..., f_s)$.*

Definition 1.16. Für eine projektive Varietät $V \subset \mathbb{P}_k^n$ definieren wir den *Koordinatenring* $A(V) := k[X_0, ..., X_n]/I(V)$.

Definition 1.17. Wir definieren *affine algebraische Varietäten* W als den Durchschnitt einer projektiven Varietät $V \subset \mathbb{P}_k^n$ mit einer der offenen Mengen $D(X_i)$, $i = 0, ..., n$, mit der induzierten Topologie $\mathfrak{T}_{V \cap D(X_i)}$.

Definition 1.18. Für eine affine Varietät $W = V \cap D(X_i) \subset \mathbb{P}_k^n$ definieren wir den *Koordinatenring* $A(W) := A(V)_{(X_i)} := \left\{ \frac{f}{X_i^r} \in A(V)_{X_i} \mid \deg(f) = r,\, r \in \mathbb{N}_0 \right\}$.

Definition 1.19. Sei V eine (affine oder projektive) Varietät mit Zariski-Topologie $\mathfrak{T}$. Eine *Untervarietät* von V ist eine Zariski-abgeschlossene, irreduzible Teilmenge $W \subset V$ mit der induzierten Topologie $\mathbb{T}_W$. W ist wieder eine (affine oder projektive) Varietät.

Bemerkung 1.20. Es ist leicht zu sehen, dass sich ein Element

$$X_0^{-r} \sum_{i \in I} a_i X_0^{i_0} \cdots X_n^{i_n} \in A(V)_{(X_0)}$$

schreiben lässt als

$$\sum_{i \in I} a_i (X_0/X_0)^{i_0} \cdots (X_n/X_0)^{i_n} \in k[X_0/X_0, ..., X_n/X_0] \cong k[Y_1, ..., Y_n].$$

Geometrisch bedeutet dies Folgendes:
Für gegebenes n und $i = 0, ..., n$ seien $\phi_i : \{f \in k[X_0, ..., X_n],\, f \text{ homogen } \} \to$

$k[Y_1, ..., Y_n]$ definiert durch die Zuordnung, $X_0 \mapsto Y_1, ..., X_i \mapsto 1, ..., X_n \mapsto Y_n$. Dann kann $V(f_1, ..., f_s) \cap D(X_i) = \{(a_0 : ... : 1 : ... : a_n) \mid f_j(a_0, ..., a_n) = 0, j = 1, ..., s\}$ auf die Nullstellenmenge $\{(b_1, ..., b_n) \in \mathbb{A}_k^n | \phi_i(f_j)(b_1, ..., b_n) = 0, j = 1, ..., s\}$ (mengentheoretisch) bijektiv abgebildet werden.
Die ϕ_i lassen sich umkehren mittels

$$\varphi_i(f)(Y_1, ..., Y_n) := X_i^{\deg(f)} f(X_0/X_i, ..., \hat{X}_i, ..., X_n/X_i),$$

wobei $\hat{X}_i$ meint, dass die Variable nicht in der Aufzählung vorkommt. Daher lässt sich jede Nullstellenmenge von beliebigen (nicht notwendig homogenen) Polynomen $W = V(g_1, ..., g_t) \subset \mathbb{A}_k^n$ bijektiv abbilden auf $V(\varphi_i(g_1), ..., \varphi_i(g_t)) \cap D(X_i)$ und wir können wie in 1.15 der affinen Varietät das Ideal $I(W) = \{f \in k[Y_1, ..., Y_t] | f(b) = 0, b \in W\}$ zuordnen. Insbesondere sehen wir, dass $A(W) \cong k[Y_1, ..., Y_n]/I(W)$.

Die obige Bemerkung motiviert die Frage, wann wir Varietäten als gleich ansehen wollen. Es gibt dazu in der algebraischen Geometrie zwei Konzepte, die wir im Folgenden definieren.

Definition 1.21. Sei V eine Varietät. Eine Funktion $f : V \to k$ heißt *regulär im Punkt* $P \in V$, falls eine offene Umgebung $U \subset V$ von P, und $g, h \in k[X_0, ..., X_n]$, homogene Polynome desselben Grades, existieren, sodass für alle benachbarten Punkte $Q \in U$ gilt, dass $h(Q) \neq 0$, $f(Q) = \frac{g(Q)}{h(Q)}$. Falls f regulär in allen Punkten von V ist, dann heißt f *regulär auf* V. Für jede Teilmenge $U \subset V$ definieren wir $\mathcal{O}(U)$ als die Menge der Funkionen $f : U \to k$, die regulär in allen Punkten $P \in U$ sind. Insbesondere ist also $\mathcal{O}(V)$ die Menge aller auf V regulären Funktionen.

Definition 1.22. Ein *Morphismus von Varietäten* ist eine Zariski-stetige Abbildung $\phi : V \to W$, sodass für alle $f \in \mathcal{O}(W)$ gilt, dass $f \circ \phi \in \mathcal{O}(\phi^{-1}(U))$. Sei k' ein Unterkörper von k, dann ist ϕ ein *k'-rationaler Morphismus*, falls $\phi(V \cap \mathbb{P}_{k'}^n) \subset \mathbb{P}_{k'}^n$. ϕ ist ein *Isomorphismus von Varietäten*, falls eine Umkehrabbildung φ existiert, die ebenfalls Morphismus ist, und $\phi \circ \varphi = \mathrm{id}_W$, $\varphi \circ \phi = \mathrm{id}_V$. Sind sowohl ϕ als auch φ k'-rational, dann heißt ϕ *k'-rationaler Isomorphismus*.

Bemerkung 1.23. Man kann zeigen, dass die ϕ_i und φ_i aus 1.20 tatsächlich Isomorphismen induzieren. Im Falle von $k = \bar{\mathbb{F}}_p$ handelt es sich sogar um $\mathbb{F}_p$-rationale

Isomorphismen. Wir können also Eigenschaften einer projektiven Varietät an einem Punkt $P = (x_0, ..., x_n)$ untersuchen, indem wir ihn in einer affinen Umgebung (bspw. $D(X_i) \cap V$, falls $x_i \neq 0$) mit der affinen Varietät in $\mathbb{A}_k^n$ identifizieren.

Bemerkung 1.24. Von jetzt an werden wir unter affiner Varietät auch ihre Einbettung in $\mathbb{A}_k^n$ für ein n verstehen.

Bemerkung 1.25. Es kann gezeigt werden, dass zwei affine Varietäten W_1, W_2 genau dann isomorph sind, wenn ihre Koordinatenringe isomorphe k-Algebren sind und dass $\mathcal{O}(W_1) \cong A(W_1)$ (s. [7, I Korollar 3.7 und I Theorem 3.2]).

Wir erinnern uns, dass Varietäten irreduzible Räume sind, und somit jede offene Teilmenge dicht liegt (Satz 1.12). Das heißt, wenn wir eine Abbildung auf einer offenen Menge kennen, dann fast auf dem ganzen Raum. Auf dieser Überlegung fußt die Definition des zweiten Gleichheitsbegriffs, der birationalen Äquivalenz:

Definition 1.26. Seien V und W Varietäten. Eine *rationale* Abbildung $\phi : V \to W$ ist eine Äquivalenzklasse von Morphismen $\phi_U : U \to W$, die auf offenen Teilmengen U von V definiert sind. Dabei sind ϕ_{U_1} und ϕ_{U_2} äquivalent, falls sie identisch auf $U_1 \cap U_2$ sind. Die Abbildung heißt birational, falls rationale Abbildungen $\varphi : W \to V$, $\phi : V \to W$, und offene Teilmengen $U \subset V$, $U' \subset W$ existieren mit $\phi(U) = U'$, $(\varphi \circ \phi)_U = \mathrm{id}_U$ und $(\phi \circ \varphi)_{U'} = \mathrm{id}_{U'}$. Falls eine solche birationale Abbildung existiert, sagen wir V und W sind *birational äquivalent*.

Bespiel 1.27. *Beispiele für Morphismen und birationale Abbildungen.*

(i) *Projektive Transformation.* Seien $F_j \in k[X_0, ..., X_n]$, $j = 0, ..., n$, homogene Polynome desselben Grades. Dann ist $(x_0 : ... : x_n) \mapsto (F_0(x_0, ..., x_n) : ... : F_n(x_0, ..., x_n))$ ein Morphismus. Insbesondere induziert ein linearer Isomorphismus $L : k^{n+1} \to k^{n+1}$ einen Isomorphismus $\bar{L} : \mathbb{P}_k^n \to \mathbb{P}_k^n$, der einem einfachen Koordinatenwechsel entspricht. Damit ist auch deutlich, dass $D(l)$ für ein homogenes, lineares Polynom $l = \sum_{i=0}^n a_i X_i$, mit $a_{i_0} \neq 0$, ebenfalls affin ist, denn die Abbildung $X_i \mapsto X_i$ für $i \neq i_0$ und $X_{i_0} \mapsto l$ ist ein linearer Isomorphismus in k^{n+1}.

(ii) *Projektion von einem Punkt.* Sei $V \subset \mathbb{P}_k^n$ eine Varietät. Seien weiter $\{P\}$, $V(X_i) \subset \mathbb{P}_k^n$ so gewählt, dass $V \cap V(X_i) \subsetneq V(X_i)$, $P \notin V$. Dann definie-

ren wir die Abbildung $\pi_P : V \to \mathbb{P}_k^{n-1} \cong V(X_i)$ als $\pi_P(Q) := Q'$, $\{Q'\} = \overline{PQ} \cap V(X_i)$. Im Falle von $P = (0 : ... : 0 : 1)$ und $i = n$, ist dies einfach die Projektion auf die ersten Koordinaten, $(a_0 : ... : a_n) \mapsto (a_0 : ... : a_{n-1})$. Die Projektion ist eine finite Abbildung, d.h. dass jedes $Q \in \pi_P(V)$ nur endlich viele Urbilder hat. Insbesondere ist $\pi_P(V)$ k'-isomorph zu einer offenen Teilmenge von V, für jeden Unterkörper $k' \subset k$.

(iii) *Blow Up*. Indem wir Variablen $Z_{i,j} := X_i Y_j$ definieren und sie nach (i, j) lexikographisch ordnen, können wir das kartesische Produkt $\mathbb{P}_k^n \times \mathbb{P}_k^{n-1}$ mengentheoretisch mittels der sogenannten *Segre-Einbettung* mit der Varietät $V(Z_{i,j} - Z_{j,i} \mid 0 \leq i \leq n, 0 \leq j \leq n-1) \subset \mathbb{P}_k^{n^2+n-1}$ identifizieren. Die entsprechende Abbildungsvorschrift ist $\phi(a_0 : ... : a_n; b_0 : ... : b_{n-1}) \mapsto (a_0 b_0 : ... : a_i b_j : ... : a_n b_{n-1})$. Sei $\pi : \mathbb{P}_k^{n^2+n-1} \to \mathbb{P}_k^n$ die (surjektive) Projektion definiert durch $\pi(z_{0,0} : ... : z_{n,n-1}) = \pi'(\phi(a_0 : ... : a_n; b_0 : ... : b_{n-1})) := (a_0 : ... : a_n)$. Sei $V \subset \mathbb{P}_k^n$ eine projektive Varietät, sodass $P = (0 : ... : 0 : 1) \in V$ (dies können wir durch Isomorphismen erreichen). Dann ist P in der affinen Varietät $V \cap D(X_n)$. Wir definieren den Blow Up von $V \cap D(X_n)$ in P als den algebraischen Abschluss von $\pi^{-1}(V \cap D(X_n))$ in $\mathbb{A}_k^n \times \mathbb{P}_k^{n-1} \subset \mathbb{P}_k^n \times \mathbb{P}_k^{n-1}$. Für $k' := \mathbb{F}_p$, $k := \overline{k'}$ gilt dann, dass $V \cap D(X_n)$ und $\pi^{-1}(V \cap D(X_n))$ k'-isomorph sind.

(iv) *Veronese-Einbettung, d-uple Einbettung.* Sei

$$F = \sum_{i \in I} a_i X_0^{i_0} \cdots X_n^{i_n} \in \bar{k}[X_0, ..., X_n]$$

ein homogenes, irreduzibles Polynom, $d = \deg(F)$. Wir können $\mathbb{P}_{\bar{k}}^n$ in $\mathbb{P}_{\bar{k}}^N$, $N := \binom{n+d}{d} - 1$, einbetten, indem wir die Koordinaten von $Q = (z_0 : ... : z_N) \in \mathbb{P}_{\bar{k}}^N = V(0)$, $0 \in k[Z_0, ..., Z_N]$, als Monome in den Koordinaten in $\mathbb{P}_{\bar{k}}^n$ interpretieren, i.e. $\nu(x_0 : x_1 : x_2) := (x_0^d : x_0^{d-1} x_1 : ... : x_1^d : x_1^{d-1} x_2 : ... : x_2^d)$. Sei V das Bild von $\mathbb{P}_{\bar{k}}^n$ unter dieser Abbildung. Für jedes Tupel $i = (i_0, ..., i_n) \in \mathbb{N}_0$, $\sum i_j = d$, sei $j(i) \in \{0, ..., N\}$ der Index, der der lexikographischen Ordnung der Tupel i entspricht. Dann ist $V(F) \mapsto_\nu V \cap V(F^\nu)$ ein Isomorphismus, wobei $F^\nu(Z_0, ..., Z_N) = \sum_{i \in I} a_i Z_{j(i)}$, d.h. $V(F)$ wird auf V mit einem *linearen* Polynom definiert.

Die Projektion von einem Punkt kann insbesondere verwendet werden, um die Dimension von Varietäten zu berechnen (s. [24, I.6]). Wir tun dies hier nicht, sondern begnügen uns mit ihrer Definition und einigen Eigeschaften, die wir im weiteren Verlauf brauchen werden.

Definition 1.28. Sei $(X, \mathfrak{T})$ ein nicht-leerer topologischer Raum, und $P \in X$ ein Punkt. Dann ist die *Dimension* von X definiert als die maximale Länge n von Inklusionen $P \subsetneq Z_1 \subsetneq ... \subsetneq Z_n = X$, wobei Z_i irreduzible, abgeschlossene Teilräume von X sind.

Satz 1.29. *(Dimension)*

(i) $\dim(\mathbb{P}_k^n) = n$.

(ii) $\dim(U) = \dim(\overline{U})$.

(iii) *Für eine projektive Varietät* $V \subset \mathbb{P}_k^n$ *ist* $\dim(V) = n - 1$ *genau dann, wenn* $V = V(F)$ *sich als Nullstellenmenge eines homogenen, irreduziblen Polynoms* $F \in k[X_0, ..., X_n]$ *darstellen lässt.*

(iv) *Für* $F \in k[X_0, ..., X_n]$ *gilt:* $\dim(D(F)) = n$.

1.3 Kurven und Singuläre Punkte

Wir beginnen diesen Abschnitt mit der Definition von Kurven. In diesem und allen weiteren Abschnitten sei stets $k = \mathbb{F}_q$ und $\bar{k}$ der algebraische Abschluss.

Definition 1.30. Wir definieren *Kurven* als eindimensionale algebraische Varietäten $C \subset \mathbb{P}_{\bar{k}}^n$, d.h. $\dim(C) = 1$. Eine Kurve $C = V(F)$, $F \in \bar{k}[X_0, X_1, X_2]$, in der Ebene $\mathbb{P}_{\bar{k}}^2$ heißt *definiert über* k, falls ein $c \in \bar{k}$ existiert, sodass $cF \in k[X_0, X_1, X_2]$. Eine beliebige Kurve $C' \subset \mathbb{P}_{\bar{k}}^n$ heißt definiert über k, falls eine offene Menge $U' \subset C'$, und eine Kurve in der Ebene C mit offener Teilmenge U existieren, sodass U und U' k-isomorph sind und C über k definiert ist.

Bemerkung 1.31. C ist definiert über $\mathbb{F}_q$ genau dann, wenn ein Punkt $P \in C$ existiert, dessen Koordinaten alle in $\mathbb{F}_q$ liegen. Ein solcher Punkt heißt $\mathbb{F}_q$*-rational*.

Hartshorne zeigt mithilfe von Blow Ups an Punkten in [7, V.3], dass jede Kurve über $\bar{k}$ birational äquivalent zu einer *glatten* Kurve über $\bar{k}$ ist. Was das bedeutet, sehen wir im Folgenden.

Satz 1.32. *Sei $P \in V$ Punkt einer affinen Varietät über $\bar{k}$, $A(V)$ ihr Koordinatenring und $\mathfrak{p} := \{f \in A(V) \mid f(P) = 0\}$. Dann gilt:*

(i) $\mathfrak{p}$ *ist ein Maximalideal in* $A(V)$.

(ii) Für den Lokalisierungsring $A(V)_\mathfrak{p}$ *mit Maximalideal* $\mathfrak{m}_P = \mathfrak{p}A(V)_\mathfrak{p}$ *ist*

$$A(V)_\mathfrak{p}/\mathfrak{m}_P \cong \bar{k}.$$

Definition 1.33. Für einen Punkt P einer affinen Varietät V heißt $\mathcal{O}_P := A(V)_\mathfrak{p}$ *lokaler Ring von P in V.*

Da isomorphe affine Varietäten isomorphe Koordinatenringe haben, ist auch der lokale Ring eines Punktes invariant unter Isomorphismen.

Definition 1.34. Für einen Punkt P einer projektiven Varietät V definieren wir den *lokalen Ring von P in V* als den lokalen Ring von P in einer affinen Umgebung $U \subset V$ von P.

Definition 1.35. Die *Dimension eines Ringes R*, $\dim(R)$ wird definiert als die maximale Länge von echten Inklusionen von Primidealen $\mathfrak{p}_0 \subsetneq ... \subsetneq \mathfrak{p}_n$.

Definition 1.36. Sei P ein Punkt in einer Varietät $V \subset \mathbb{P}^n_{\bar{k}}$ und $\mathcal{O}_P$ sein lokaler Ring, und $\mathfrak{m}_P$ das Maximalideal. Dann heißt V *regulär in P*, falls $\mathcal{O}_P$ ein regulärer Ring ist, d.h. $\dim_{\bar{k}}(\mathfrak{m}_P/\mathfrak{m}_P^2) = \dim(\mathcal{O}_P)$

Bemerkung 1.37. Wenn wir für $F \in k[X_0, ..., X_n]$, $\frac{\partial F}{\partial X_i}$ als die bekannte partielle Ableitung des Polynoms nach der i-ten Variable verstehen, dann ist $V = V(F)$ singulär in $P \in V$ genau dann, wenn für alle $i \in \{0, ..., n\}$, $\frac{\partial F}{\partial X_i}(P) = 0$ (s. [24, 1.4]).

Beispielsweise sind $\mathbb{A}^n_K$ und $\mathbb{P}^n_K$ glatte Varietäten für einen beliebigen Körper K und $n \in \mathbb{N}_0$. Ebenso ist aber auch jede offene Menge $D(F)$ eine affine, glatte Varietät:

Satz 1.38. *Sei $F \in \bar{k}[X_0, ..., X_n]$. Dann gilt:*

(i) $D(F) \subset \mathbb{P}^n_{\bar{k}}$ *ist eine affine Varietät.*

(ii) $D(F)$ *ist regulär in jedem Punkt* $P \in D(F)$.

Beweis. Zu (i): Nach Beispiel 1.27 (iv) ist $D(F) \cap \mathbb{P}^n_{\bar{k}} = D(F) \cong \nu(\mathbb{P}^n_{\bar{k}}) \cap D(F^\nu) \subset \mathbb{P}^N_{\bar{k}}$. Sei $\phi : \mathbb{P}^N_{\bar{k}} \to \mathbb{P}^N_{\bar{k}}$ die projektive Transformation, die F^ν auf ein Z_j abbildet. Dann ist $D(F) \cong \phi(\nu(\mathbb{P}^n_{\bar{k}})) \cap D(Z_j)$.
Zu (ii): Mit ϕ wie in Bemerkung 1.20 und ν wie in Beispiel 1.27 (iv) gilt für den Koordinatenring von $D(F)$: $A(D(F)) = A(\phi(\nu(\mathbb{P}^n_{\bar{k}})) \cap D(Z_j)) = A(\phi(\nu(\mathbb{P}^n_{\bar{k}})))_{(Z_j)} \cong A(\nu(\mathbb{P}^n_{\bar{k}}))_{(F^\nu)} \cong A(\mathbb{P}^n_{\bar{k}})_{(F)} \cong A(\mathbb{A}^n_{\bar{k}})_{\phi_i(F)}$. Dann ist für einen Punkt $P \in D(F)$, $\mathcal{O}_P \cong A(\mathbb{A}^n_{\bar{k}})_{\phi_i(F),\mathfrak{m}_P} \cong A(\mathbb{A}^n_{\bar{k}})_{\mathfrak{m}_P,\phi_i(F)}$. Da $\mathbb{A}^n_{\bar{k}}$ glatt ist, ist $A(\mathbb{A}^n_{\bar{k}})_{\mathfrak{m}_P}$ ein regulärer Ring und nach [7, II, Korollar 8.16] ist die Lokalisierung eines regulären Rings wieder ein regulärer Ring. □

Und schließlich gilt für die Anzahl singulärer Punkte einer Kurve folgender Satz:

Satz 1.39. *Die Menge $\Sigma(C)$ der singulären Punkte einer Kurve ist leer oder endlich.*

Beweis. Falls C glatt ist, ist $\Sigma(C) = \varnothing$. Nehmen wir an $\Sigma(C) \neq \varnothing$. Dann ist nach [7, I.5.3], $\Sigma(C)$ eine echte, (Zariski-)abgeschlossene Teilmenge von C. □

Weiterhin zeigt Hartshorne in [7, IV.3], dass jede nicht-singuläre Kurve – per Projektion von einem geschickt gewählten Punkt aus – sich in $\mathbb{P}^3_{\bar{\mathbb{F}}_q}$ einbetten lässt und von dort auf eine Kurve *mit höchstens gewöhnlichen Doppelpunkten als Singularitäten* projiziert werden kann, i.e. zu dieser ebenfalls birational äquivalent ist. Dies ist die Klasse von Kurven, auf die wir uns im Weiteren beschränken wollen. Zwar gilt nicht notwendig, dass jede über $\mathbb{F}_q$ definierte Kurve C zu einer anderen C' birational äquivalent ist, die ebenfalls über $\mathbb{F}_q$ definiert ist und höchstens gewöhnliche Doppelpunkte als Singularitäten hat; dennoch zeigt die Konstruktion der birationalen Äquivalenz von C und C', wie sie Hartshorne in endlich vielen Schritten vornimmt, dass eine Körpererweiterung $\mathbb{F}_{q^s} \supset \mathbb{F}_q$ existiert, sodass C und C' über $\mathbb{F}_{q^s}$ definiert sind.

Gewöhnliche Doppelpunkte sind, grob gesprochen, Punkte, an denen sich eine Kurve selbst überschneidet. Insbesondere sind sie singuläre Punkte. Betrachten wir eine Kurve $C = V(F) \subset \mathbb{P}^2_{\bar{k}}$ an einem Punkt $P = (x_0 : x_1 : x_2)$, $x_i \neq 0$

in einer affinen Umgebung $D(X_i)$. Sei ohne Beschränkung der Allgemeinheit $i = 0$. Dann ist die definierende Gleichung in dieser Umgebung durch das Polynom $G = \phi_0(F) = F(1, Y_1, Y_2) \in k[Y_1, Y_2]$ gegeben. Wir können durch eine lineare Transformation, $(y_1, y_2) \mapsto (y_1 - x_1/x_0, y_2 - x_2/x_0)$, P auf den Ursprung $O = (0, 0)$ abbilden; dem entspricht die folgende Abbildung auf den Koordinatenringen: $f(Y_1, Y_2) \mapsto g(Y_1, Y_2) = f(Y_1 + x_1/x_0, Y_2 + x_2/x_0)$. Dann ist $g(0, 0) = 0$, $g(Y_1, Y_2) = (a_{1,0}Y_1 + a_{0,1}Y_2) + (a_{2,0}Y_1^2 + a_{1,1}Y_1Y_2 + a_{0,2}Y_2^2) + g_3(Y_1, Y_2) = g_1(Y_1, Y_2) + g_2(Y_1, Y_2) + g_3(Y_1, Y_2)$.

Definition 1.40. Sei $g(Y_1, Y_2) = g_1(Y_1, Y_2) + g_2(Y_1, Y_2) + g_3(Y_1, Y_2)$ das Polynom einer Kurve C in einer Umgebung von O. Dann heißt O *Doppelpunkt von* C, falls $g_1 \equiv 0$, $g_2 \not\equiv 0$. O heißt *gewöhnlich*, falls lineare Polynome $l_1, l_2 \in k[Y_1, Y_2]$ existieren, sodass $g_2 = l_1 l_2$ und $l_1 \neq cl_2$, für alle $c \in \bar{k}$. l_1, l_2 heißen *Tangenten* von C in O.

Bespiel 1.41. Sei $F = X_1^5 + X_0^5 - 5X_0^4X_2 + 10X_0^3X_2^2 - 9X_0^2X_2^3 + 3X_0X_2^4 \in \bar{\mathbb{F}}_7[X_0, X_1, X_2]$. Dann verschwinden die partiellen Ableitungen $\partial F/\partial X_0(P) = \partial F/\partial X_1(P) = \partial F/\partial X_2(P) = F(P) = 0$ simultan genau dann, wenn $P = (1 : 0 : 1)$. Wir betrachten P in der Umgebung $C \cap D(X_2)$ und erhalten $f = Y_2^5 + Y_1^5 - 5Y_1^4 + 10Y_1^3 - 9Y_1^2 + 3Y_1$ und können P mit $(1, 0)$ identifizieren. Wir bewegen P nach $O = (0, 0)$ und erhalten $\tilde{f} = Y_2^5 + Y_1^5 + Y_2^2 + Y_1^2$. P ist also Doppelpunkt. Und da jeder algebraisch abgeschlossene Körper, in unserem Falle $\bar{\mathbb{F}}_7$, $i := \sqrt{-1}$ enthält, ist $g_2 = (Y_1 - iY_2)(Y_1 + iY_2)$, P also ein gewöhnlicher Doppelpunkt.

1.4 Geschlecht und Zetafunktion

Eine Möglichkeit der Klassifizierung von Kurven, bzw. ebenso aller glatter Kurven, aus denen sie hervorgehen, ist ihr *Geschlecht*:

Definition 1.42. Sei $C = V(F) \subset \mathbb{P}^2_{\bar{k}}$ eine Kurve mit r gewöhnlichen Doppelpunkten als einzige Singularitäten, $d := \deg(F)$. Dann heißt die Zahl

$$g(C) := \frac{1}{2}(d-1)(d-2) - r$$

das *Geschlecht* von C. Für eine beliebige Kurve $C_1 \subset \mathbb{P}^n_{\bar{k}}$, gibt es eine Kurve C_2 in der Ebene, mit höchstens gewöhnlichen Doppelpunkten als Singularitäten, die zu ihr birational äquivalent ist. Wir definieren $g(C_1) := g(C_2)$.

Bemerkung 1.43. Da die Anzahl der Singularitäten endlich ist, ist das Geschlecht wohldefiniert (s. Satz 1.39).

Satz 1.44. *Seien $C, C' \subset \mathbb{P}^2_{\bar{k}}$ Kurven über k. Dann gilt:*

(i) Existieren k-isomorphe offene Mengen $U \subset C$, $U' \subset C'$, dann ist $g(C) = g(C')$.

(ii) $g(C) \geq 0$.

Beweis. Zu (i): Die Normalisierung der Kurve $\tilde{C} \to C$ ist birational zu ihr äquivalent (wähle $Z = Y$ in [7, II, Übung 3.17]). Somit ist nach [7, IV, Bemerkung 3.11.1], $g(\tilde{C}) = g(C)$, und nach [7, II, Theorem 8.19], folgt $g(\tilde{C'}) = g(\tilde{C})$, also $g(C) = g(C')$.
Zu (ii): Das Geschlecht stimmt mit dem *geometrischen Geschlecht (geometric genus)* aus [7] überein, das als Dimension eines linearen Vektorraums definiert wird. Diese haben nicht-negative Dimension. □

Wir haben uns die Aufgabe gestellt, die Zetafunktion von Kurven vom Geschlecht 5 über endlichen Körpern zu berechnen. Da wir jetzt wissen, was Kurven vom Geschlecht 5 über endlichen Körpern sind, bleibt uns nun noch, die Zetafunktion für sie zu definieren.

Definition 1.45. Sei $k_r = \mathbb{F}_{q^r}$, $r \in \mathbb{N}$, $V \subset \mathbb{P}^n_{\bar{k}}$ eine Varietät, definiert über k, und $N_r := \sharp V \cap \mathbb{P}^n_{k_r}$ die Anzahl der k_r-rationalen Punkte von V. Dann heißt die Funktion

$$Z(V,T) := \exp\left(\sum_{r\in\mathbb{N}} N_r \frac{T^r}{r}\right)$$

aus $\mathbb{Q}[[T]]$ *Zetafunktion von V*.

Die Zetafunktion hat folgende Eigenschaften:

Satz 1.46. *Sei $k = \mathbb{F}_q$. Und sei $Z_p(V,T)$ die Zetafunktion von V über $\mathbb{F}_p$.*

(i) $Z(V,T^n) = \prod_{\zeta^n=1} Z_p(V,\zeta T)$, *d.h. wir nehmen das Produkt über die* n*-ten Einheitswurzeln* ζ.

(ii) $Z(\mathbb{P}^2_{\bar{k}},T) = \frac{1}{(1-T)(1-qT)(1-q^2T)}$

(iii) Für eine Varietät V *und eine abgeschlossene Teilmenge* $W \subset V$ *gilt:* $Z(V,T) = Z(W,T)Z(V-W,T)$

(iv) Für $C = V(F) \subset \mathbb{P}^2_{\bar{k}}$ *und* $U := D(F)$ *ist* $Z(C,T) = \frac{1}{Z(U,T)(1-T)(1-qT)(1-q^2T)}$

(v) Für eine glatte Kurve C *mit Geschlecht* $g = g(C)$ *gilt:*

(a) $Z(C,T) = \frac{L(T)}{(1-T)(1-qT)}$

(b) Weil-Vermutungen[1]*. Es gilt, dass* $L(T) = \sum_{i=1}^{2g} a_i T^i \in \mathbb{Z}[T]$ *und für die* a_i *gilt:*

i. $a_0 = 1$, $a_{2g} = q^g$

ii. $a_{2g-i} = q^{g-i}a_i$, *für* $0 \leq i \leq g$

iii. $L(T) = \prod_{i=1}^{2g}(1-\alpha_i T) \in \mathbb{C}[T]$.

Dabei sind α_i *ganz über* $\mathbb{Z}$ *und* $|\alpha_i|_{\mathbb{C}} = \sqrt{q}$.

iv. $|a_i|_{\mathbb{C}} \leq \binom{2g}{i} q^{\frac{i}{2}}$ *für* $i = 0,...,2g$.

Beweis. Zu (i): s. [25, Satz 5.1.10].

Zu (ii): Mit k_r wie oben, $\mathbb{P}^n_{k_r} = D(X_0) \sqcup V(X_0) \cong \mathbb{A}^n_{k_r} \times \mathbb{P}^{n-1}_{k_r}$. Also ist $\mathbb{P}^2_{k_r} \cong \mathbb{A}^2_{k_r} \times \mathbb{A}^1_{k_r} \times \mathbb{P}^0_{k_r}$ und somit $N_r = q^{2r} + q^r + 1$. Schließlich

$$\begin{aligned}
Z(\mathbb{P}^2_{\bar{k}},T) &= \exp\left(\sum_{r\in\mathbb{N}}(q^{2r}+q^r+1)\frac{T^r}{r}\right) \\
&= \exp\left(\sum_{r\in\mathbb{N}}\frac{(q^2T)^r}{r} + \sum_{r\in\mathbb{N}}\frac{(qT)^r}{r} + \sum_{r\in\mathbb{N}}\frac{T^r}{r}\right) \\
&= \exp\left(-\sum_{r\in\mathbb{N}}(-1)^{r-1}\frac{(-q^2T)^r}{r} - \sum_{r\in\mathbb{N}}(-1)^{r-1}\frac{(-qT)^r}{r} - \sum_{r\in\mathbb{N}}(-1)^{r-1}\frac{(-T)^r}{r}\right) \\
&= \exp\left(-\log\left(1-q^2T\right) - \log\left(1-qT\right) - \log\left(1-T\right)\right) \\
&= (1-q^2T)^{-1}(1-qT)^{-1}(1-T)^{-1}
\end{aligned}$$

Zu (iii): [7, Appendix C, Übung 5.1]

[1] Dies ist nur ein Teil der Weil-Vermutungen, die bspw. in [7, Anhang C] genauer besprochen werden.

Zu (iv): Folgt unmittelbar aus (ii) und (iii)

Zu (v): [25, Theorem 5.1.15]

Zu (v)((b))iv: Nach [25, Theorem 5.1.15] ist $L(T) = \prod_{i=1}^{2g}(1-\alpha_i T) = T^{2g}\prod_{i=1}^{2g}(T^{-1}-\alpha_i)$ und $|\alpha_i|_{\mathbb{C}} = \sqrt{q}$ für alle i. Also ist $T^{-2g}L(T) = T^{-2g}\sum_{i=0}^{2g} a_i T^i = \sum_{i=0} a_{2g-i}(T^{-1})^i$ und die a_{2g-i} sind elementarsymmentrische Polynome in $\{-\alpha_i\}$. Daraus folgt:

$$\begin{aligned} |a_{2g-i}|_{\mathbb{C}} &= \left| \sum_{1\le i_1<\ldots<i_{2g-i}\le 2g} \prod_{j=1}^{2g-i} (-\alpha_{i_j}) \right|_{\mathbb{C}} \\ &\le \sum_{1\le i_1<\ldots<i_{2g-i}\le 2g} \prod_{j=1}^{2g-i} |\alpha_{i_j}|_{\mathbb{C}} \\ &= \binom{2g}{2g-i} \sqrt{q}^{2g-i} \end{aligned}$$

bzw. $|a_i|_{\mathbb{C}} \le \binom{2g}{i} q^{\frac{i}{2}}$. □

2 Berechnung der Zetafunktion glatter Kurven

Aus der algebraischen Topologie ist bekannt, dass sich die Anzahl der Fixpunkte einer Selbstabbildung σ eines Raums X mittels der sogenannten *Homologie-* bzw. *Kohomologie-Gruppen* berechnen lassen. In unserem Falle beschränken wir uns auf die Kohomologie, die wir uns vorerst als eine Menge von $\mathbb{Q}_q$-Vektorräumen $\{H^i(X) \mid i \in \mathbb{N}_0\}$ vorstellen können. Die Selbstabbildung σ wird dann eine $\mathbb{Q}_q$-lineare Abbildung σ^* auf allen $H^i(X)$ induzieren, mithilfe derer man die Anzahl der Fixpunkte von σ auf X mit der sogenannten *Lefschetz-Fixpunkt-Formel*, s. [27, 4, Satz 4.2], bestimmen kann. Wir erinnern uns, dass wir in Satz 1.2 $\mathbb{F}_q$ als die Menge der $x \in \bar{\mathbb{F}}_p$ definiert hatten, für die $x^q = x$. Die Abbildung $\mathrm{Frob}_q(x) = x^q$ heißt *(absoluter q-)Frobenius-Morphismus*. Offensichtlich ist dann die Fixpunktmenge von Frob_q^r gerade der Körper $\mathbb{F}_{q^r}$. Wir können den Frobenius-Morphismus auf unsere Kurven C übertragen, indem wir $\mathrm{Frob}_q(x_0 : x_1 : x_2) := (x_0^q : x_1^q : x_2^q)$ setzen. Dann gibt uns die Fixpunktmenge von Frob_q^r die Anzahl der Punkte mit Koordinaten in $\mathbb{F}_{q^r}$ an. Die grundlegende Idee bei der Berechnung der Zetafunktion einer Kurve (oder von Varietäten im Allgemeinen) ist also, eine geeignete Kohomologie zu finden, mit derer sich die Anzahl der Fixpunkte der Kurve unter dem Frobenius-Morphismus bestimmen lässt. Für glatte, affine Varietäten haben dies P. Monsky und G. Washnitzer erreicht (s. [20], [21] und [22], bzw. [27]), wo sie die *Monsky-Washnitzer-Kohomologie* konstruieren und wichtige Eigenschaften von ihr beweisen. Wie man letztlich algorithmisch mit dieser Kohomologie umgeht zeigt K. Kedlaya in [10]. Die Strategie in [10] ist, eine projektive Kurve C als disjunkte Vereinigung einer affinen Kurve und einer projektiven Varietät zu zerlegen, $C = C' \sqcup V$, sodass C' eine glatte, affine Varietät ist und V niedrigere Dimen-

sion hat und sich insbesondere einfacher berechnen lässt. Die Herausforderung besteht dann insbesondere darin, eine Basis, d.h. eine Darstellung, für $H^1(C')$ zu finden. Im Falle hyperelliptischer Kurven hat K. Kedlaya dies in [10] getan. Im allgemeineren Fall ist es aber nicht so einfach. Stattdessen werden wir uns der Methode von T. Abbot, K. Kedlaya und G. Roe aus [26] bedienen. Dabei richten wir unsere Aufmerksamkeit weg von C und berechnen stattdessen die Zetafunktion des Komplements $U = \mathbb{P}^2_{\bar{\mathbb{F}}_q} - C$, das, wie wir in Satz 1.38 gesehen haben, eine affine, glatte Varietät ist, und erhalten die Zetafunktion von C mittels Satz 1.46 (iv). Wir werden sehen, dass die zu berechnenden Kohomologien eine kanonische Darstellung (im Falle glatter Kurven) haben, mit der wir rechnen können. Dazu werden wir uns einer weiteren, nämlich der *algebraischen De-Rham-Kohomologie* eines sogenannten *Lifts* der Varietät bedienen, die unter bestimmten Bedingungen isomorph zur Monsky-Washnitzer-Kohomologie ist. Doch definieren wir nun zuerst die beiden erwähnten Kohomologien.

2.1 Lift einer Varietät und Kohomologien

In diesem Abschnitt definieren wir die notwendigen Kohomologie-Gruppen. [1]

Definition 2.1. Sei K ein Körper und A eine endlich erzeugte K-Algebra. Sei $M = \langle da \mid a \in A \rangle_A$ das von den Symbolen da über A erzeugte freie Modul, und N das Untermodul $\langle dr \mid r \in K;\ d(aa')-a'da-ada',\ d(a+a')-da-da' \mid a, a' \in A \rangle_A$ von M. Dann heißen die Elemente in dem A-Modul $\Omega_{A/K} := M/N$ *Kähler-Differentiale von A über K*.

Bespiel 2.2. Für $A = K[t]$ folgt aus der Definition, dass $da = 0$ für $a \in K$, $dt^2 = tdt + tdt = 2tdt$, also insbesondere $df(t) = f'dt$ die gewöhnliche Ableitung aller $f \in A$ nach t ist. Falls die Charakteristik von K nun 0 ist, ist also $\Omega_{K[t]/K} = K[t]dt$, denn wir können dann ja für jedes $g \in K[t]$ ein $h \in K[t]$ finden, sodass

[1] Unsere Darstellung der Kähler-Differentiale folgt [7, II, 8] bzw. [7, II, Übung 5.16]. Für die algebraische De-Rham-Kohomologie und die Monsky-Washnitzer-Kohomologie nehmen wir [11, 2.1 bzw. 2.2] und [27, 2]. Wir identifizieren aber von vorneherein $\Omega_{(\mathbb{Z}_q[\overline{X}]/(f_i|i\in I))^\dagger/\mathbb{Z}_q} \otimes_{\mathbb{Z}_q} \mathbb{Q}_q$ mit $\Omega_{(\mathbb{Q}_q[\overline{X}]/(f_i|i\in I))^\dagger/\mathbb{Q}_q}$ wie in [12, Definition 10].

$dh(t) = g(t)dt$.

Sei jetzt $V = V(F)$, $F \in K[t]$ eine Varietät mit Koordinatenring $A(V) = K[t]/(F)$ und K wieder von Charakteristik 0. Jedes $G \in A(V)$ lässt sich schreiben als $G = \hat{G} + HF$, $H \in K[t]$. Also ist $dG = [d(\hat{G} + HF)] = [\hat{G}'dt + HF'dt + H'Fdt]$ und es folgt, dass $\Omega_{A(V)/K} = K[t]/(F, F')$. Das heißt, $\Omega_{A(V)/K} = (0)$ genau dann, wenn $(F, F') = (1)$, d.h. F hat keine wiederholten Nullstellen.

Definition 2.3. Sei K ein Körper und M eine K-Algebra. Sei für $n \in \mathbb{N}$, $T^n(M) := M^{\otimes n}$ und $S^n(M)$ der Untervektorraum $\langle x_1 \otimes ... \otimes x_n \in T^n(M) \mid \exists i_1, i_2 \in \{1, ..., n\}, x_{i_1} = x_{i_2} \rangle_K$. Dann heißt $\bigwedge^n(M) := T^n(M)/S^n(M)$ die *äußere Algebra von M über K*. Wir schreiben ein Element aus $\bigwedge^n(M)$ mit Repräsentant $x_1 \otimes ... \otimes x_n$ als $x_1 \wedge ... \wedge x_n$. Zusätzlich setzen wir $\bigwedge^0(M) := K$.

Wir setzen $\Omega^n_{A/K} := \bigwedge^n \Omega_{A/K}$ und nennen seine Elemente *n-Formen von A über K*. Wir haben natürliche Abbildungen $d^n : \Omega^n_{A/K} \to \Omega^{n+1}_{A/K}$, $d^n(adx_1 \wedge ... \wedge dx_n) = da \wedge dx_1 \wedge ... \wedge dx_n$. Insbesondere gilt $d^{n+1} \circ d^n = 0$ und wir können definieren:

Definition 2.4. $D^\bullet := \{(d^n, \Omega^n_{A/K})\}$ heißt *De-Rham-Komplex von A über K*. Wir definieren die *De-Rham-Kohomologie von $D^\bullet$* als Folge von Gruppen

$$H^n(A/K) := \begin{cases} \ker(d^n)/\operatorname{im}(d^{n-1}),\ n \in \mathbb{Z},\ n \geq 0 \\ (0),\ n < 0 \end{cases},$$

wobei $d^{-1} : 0 \to A$ die Nullabbildung sei.

Entscheidend für die Definition einer geeigneten Kohomologie ist nun die Wahl eines Körpers K und einer K-Algebra A. Der Ansatz der p-adischen Kohomologie-Theorien ist der, die über endlichen Körpern $\mathbb{F}_q$ definierten algebraischen Varietäten *nach Charakteristik 0 zu liften*.

Definition 2.5. Sei $\overline{U}$ eine affine Varietät über $\mathbb{F}_q$ mit Koordinatenring $A(\overline{U}) = \overline{\mathbb{F}}_q[Y_1, ..., Y_n]/(\overline{f_1}, ..., \overline{f_t})$, $\overline{f_i} \in \mathbb{F}_q[Y_1, ..., Y_n]$. Nach Satz 1.3 können wir $\mathbb{F}_q$ mit dem Restklassenkörper $\mathbb{Z}_q/\mathfrak{q}$ identifizieren und finden $f_1, ..., f_t \in \mathbb{Z}_q[Y_1, ..., Y_n]$, sodass $f_i \equiv \overline{f_i} \mod \mathfrak{q}$. Wir nennen die algebraische Varietät $U := V(f_1, ..., f_t) \subset \mathbb{A}^n_{\mathbb{Q}_q}$, mit Koordinatenring $A(U) := \mathbb{Q}_q[Y_1, ..., Y_n]/(f_1, ..., f_t)$, einen *Lift von $\overline{U}$ nach*

Charakteristik 0. Ein Morphismus $\phi : U_1 \to U_2$ heißt *Lift von* $\bar{\phi} : \overline{U}_1 \to \overline{U}_2$ *nach Charakteristik* 0, falls $\phi(y_1, ..., y_n) \equiv \bar{\phi}(\overline{y_1}, ..., \overline{y_n}) \mod \mathfrak{q}$, für alle $(y_1, ..., y_n) \in \mathbb{A}^n_{\mathbb{Q}_q} \cap \mathbb{Z}^n_q$.

Bespiel 2.6. Sei $\overline{U}$ die affine Varietät $D(X_0) \subset \mathbb{P}^2_{\overline{\mathbb{F}}_7}$ über $\mathbb{F}_7$. Wir interpretieren X_0 als Polynom aus $\mathbb{Z}_7[X_0, X_1, X_2]$ und erhalten den Lift $U = D(X_0) \subset \mathbb{P}^2_{\mathbb{Q}_7}$.

Wir können jetzt die erste Kohomologie-Theorie definieren:

Definition 2.7. *(Algebraische De-Rham-Kohomologie)*
Sei $\overline{U}$ eine affine glatte Varietät über $\mathbb{F}_q$ und $A(\overline{U})$ ihr Koordinatenring. Sei U ein Lift von $\overline{U}$ nach $\mathbb{Q}_q$. Wir definieren die *algebraische De-Rham-Kohomologie von* U durch

$$H^i_{dR}(U/\mathbb{Q}_q) := H^i(A(U)/\mathbb{Q}_q).$$

Bespiel 2.8. Sei $X = \{P_1\} \subset \mathbb{P}^n_{\overline{\mathbb{F}}_p}$ ein Punkt im projektiven Raum. Wir können annehmen, dass $P_1 = (1 : \overline{t_1})$, d.h. $X = V(\bar{f})$, $\bar{f} = \bar{a}(t - \overline{t_1})$, $\bar{a} \in \mathbb{F}_q$. Es ist dann $(\bar{f}, \bar{f}') = (1)$, also folgt für den glatten Lift $V(f)$, $f = a(t - t_1)$, dass $(f, f') = \mathbb{Q}_q[t]$. Dann gilt für den De-Rham-Komplex (s. Beispiel 2.2):

$$0 \to \mathbb{Q}_q[t]/(f) \to \Omega^1_{(\mathbb{Q}_q[t]/(f))/\mathbb{Q}_q)} = \mathbb{Q}_q[t]/(f, f') = (0).$$

Das heißt also:

$$H^i_{dR}(X/\mathbb{Q}_q) = \begin{cases} \mathbb{Q}_q, \text{ falls } i = 0 \\ (0), \text{ sonst.} \end{cases}$$

Wir hatten erwähnt, dass der Frobenius-Morphismus eine Abbildung auf den Kohomologie-Gruppen induzieren wird. Dies ist im Allgemeinen für die eben definierte Kohomologie-Theorie nicht möglich. Dieses Problem wird gelöst, indem man bei der Definition der Monsky-Washnitzer-Kohomologie nicht den Lift des Koordinatenrings $A(U)$, sondern die sogenannte *schwache Vervollständigung von* $A(U)$ verwendet.

Definition 2.9. Mit $\overline{U}$, U und $A(U)$ wie in Definition 2.5. Seien weiter $B \subset \mathbb{Q}_q[[Y_1, ..., Y_n]]$ die Menge aller formalen Potenzreihen $h = \sum_{\substack{i=(i_1,...,i_n) \\ i \in \mathbb{N}_0^n}} a_i Y_1^{i_1} \cdots Y_n^{i_n}$ mit Konvergenzradius $\rho > 1$ bezüglich der induzierten p-adischen Norm $|\cdot|_p$ auf $\mathbb{Q}_q^n$ und $I := (f_1, ..., f_t)B$. Dann heißt

$$A(U)^\dagger := B/I$$

die *schwache Vervollständigung von* $A(U)$.

Definition 2.10. *(Monsky-Washnitzer-Kohomologie)*
Sei $\overline{U}$ eine affine glatte Varietät über $\mathbb{F}_q$ und $A(\overline{U})$ ihr Koordinatenring. Sei U ein Lift von $\overline{U}$ nach $\mathbb{Q}_q$ und $A(U)^\dagger$ die schwache Vervollständigung eines Lifts. Wir definieren die *Monsky-Washnitzer-Kohomologie von* $\overline{U}$ durch

$$H^i_{MW}(\overline{U}/\mathbb{Q}_q) := H^i(A(U)^\dagger/\mathbb{Q}_q).$$

Van der Put zeigt, dass die Definition von $H^i_{MW}(\overline{U}/\mathbb{Q}_q)$ nicht von der Wahl des Lifts U abhängt und dass diese Kohomologie-Gruppen endlich-dimensionale K-Vektorräume sind (s. [27]).

Wie erwähnt, lässt sich der Frobenius-Morphismus auf die Monsky-Washnitzer-Kohomologie übertragen. Er induziert die folgende Abbildung auf den Koordinatenringen $A(\overline{U})$ einer affinen Varietät $\overline{U}$:

Definition 2.11. Der *Frobenius-Homomorphismus*

$$\mathrm{Frob}_q : A(\overline{U}) = \overline{\mathbb{F}}_q[X_0, ..., X_n]/(\overline{f_1}, ..., \overline{f_s}) \to A(\overline{U})$$

ist die lineare Fortsetzung von

$$\mathrm{Frob}_q\left(\bar{a}\prod X_j^{j_i} + (\overline{f_1}, ..., \overline{f_s})\right) := \bar{a}^q \prod X_j^{qj_i} + (\overline{f_1}, ..., \overline{f_s}),\ \bar{a} \in \overline{\mathbb{F}}_q.$$

Wir übertragen diesen Homomorphismus auf die Kohomologien, indem wir auch ihn nach Charakteristik 0 liften:

Definition 2.12. Ein *Lift des Frobenius nach Charakterstik* 0, $\mathrm{F} : A(U) \to A(U)$, ist eine Abbildung, für die

$$\mathrm{F}\left(a\prod X_j^{j_i}\right) \equiv \mathrm{Frob}\left(\bar{a}\prod X_j^{j_i}\right) \mod \mathfrak{q},\ \forall a \in \mathbb{Z}_q.$$

Die Lifts des Frobenius sind nicht eindeutig, aber offensichtlich induziert jede Abbildung F auf $A(U)$ eine Abbildung $\mathrm{F}^\dagger$ auf $A(U)^\dagger$ und damit auch F_i auf $\Omega^i_{A(U)^\dagger/\mathbb{Q}_q}$ und $\mathrm{F}^* = \mathrm{F}_i^*$ auf $H^i_{MW}(\overline{U}/\mathbb{Q}_q)$. Van der Put zeigt nun in [27, Satz 3.2]:

Satz 2.13. *Seien* F *und* F′ *zwei Lifts des Frobenius nach Charakterstik* 0. *Dann gilt* $\mathrm{F}^* = (\mathrm{F}')^*$ *und* $\mathrm{Frob}^* := \mathrm{F}^*$ *ist ein* $\mathbb{Q}_q$*-linearer Automorphismus.*

2.2 Wichtige Eigenschaften der Kohomologien

Außer den eben definierten gibt es auch noch andere Kohomologie-Theorien. Die ursprüngliche Motivation für ihre Definition war, die *Weil-Vermutungen* zu beweisen, von denen wir einige in Satz 1.46 (v)(b) kennengelernt haben. Eine genauere Besprechung der Weil-Vermutungen findet man bspw. in [16, 1.2.1] .

Die Klasse der Kohomologie-Theorien, mit denen sich die Weil-Vermutungen für projektive Varietäten beweisen lässt, ist die der *Weil-Kohomologie-Theorien* (s. [16, 1.2.2]). Beispielsweise erfüllt die sogenannte *l-adische Kohomologie-Theorie* die Axiome einer Weil-Kohomologie-Theorie (s. [7, Anhang C] und ausführlicher [17]). Die *rigide Kohomologie*, geschrieben $H^i_{rig}(X)$, ist ebenfalls eine Weil-Kohomologie und eine Verallgemeinerung der Monsky-Washnitzer-Kohomologie. Die rigide Kohomologie wird nicht nur für Varietäten in dem von uns definierten Sinne, sondern allgemeiner für Schemata, die lokal von endlichem Typ sind, definiert, s. beispielsweise das Buch von Le Stum [15] bzw. den ursprünglichen Artikel von Berthelot [3].

Bemerkung 2.14. Die von uns definierten algebraischen Varietäten sind alle solche Schemata, die lokal von endlichem Typ sind. Schemata, lokal von endlichem Typ, sind allerdings nicht notwendig irreduzible topologische Räume. Deshalb verstehen wir in diesem Abschnitt unter algebraischer Varietät jede Menge, die sich als Nullstellenmenge $V(T)$ bzw. $V(T) \cap D(X_i)$ schreiben lässt, wobei $T \subset \mathbb{F}_q[X_0, ..., X_n]$ eine Menge homogener Polynome ist.

Weiterhin existiert eine Verallgemeinerung der De-Rham-Kohomologie für diese Varietäten und, da sie für affine, irreduzible Varietäten mit der von uns definierten De-Rham-Kohomologie übereinstimmt, schreiben wir ebenfalls $H^i_{dR}(X)$ (s. [9]).

Sowohl $H^i_{rig}(\overline{X})$ als auch $H^i_{dR}(X/\mathbb{Q}_q)$ sind $\mathbb{Q}_q$-Vektorräume. Wir werden sie hier nicht konstruieren. Stattdessen setzen wir ihre Existenz voraus und zählen einige ihrer Eigenschaften auf, die für uns im weiteren Verlauf bei der Berechnung der Kohomologie-Gruppen auf affinen Varietäten behilflich sein werden. Beispielsweise sind die $\mathbb{Q}_q$-Vektorräume $H^i_{rig}(\overline{X})$ einer glatten Varietät X immer endlichdimensional.

Analog zum Fall von Kurven, sagen wir, dass eine Varietät $V \subset \mathbb{P}^n_{\bar{\mathbb{F}}_q}$ über $\mathbb{F}_q$ definiert ist, wenn ein Punkt $P \in V$ mit Koordinaten in $\mathbb{F}_q$ existiert; hinreichend dazu ist, dass sich die Varietät mittels homogener Polynome $f_j \in \mathbb{F}_q[X_0, ..., X_n]$ definieren lässt. Ebenso definiert man analog den Begriff eines Lifts nach Charakteristik 0.

Unser erster Satz setzt dann die De-Rham-Kohomologie und die rigide Kohomologie zueinander in Beziehung:

Satz 2.15. *(Baldassari-Chiarellotto)*
Seien $\overline{X}$ und $\overline{Z} \subset \overline{X}$ glatte, irreduzible, projektive Varietäten ($\overline{Z} = \varnothing$ lassen wir ebenfalls zu) definiert über $\mathbb{F}_q$. Seien X, Z Lifts nach Charakteristik 0 und $U = X - Z$. Dann existieren für alle $i \in \mathbb{Z}$ kanonische Isomorphismen $H^i_{dR}(U/\mathbb{Q}_q) \to H^i_{rig}(\overline{U})$.

Außerdem gilt nach Berthelot [4, Satz 1.10]:

Satz 2.16. *Sei X eine glatte, irreduzible, affine Varietät über $\mathbb{F}_q$, dann existieren für alle $i \in \mathbb{Z}$ kanonische Isomorphismen von $\mathbb{Q}_q$-Vektorräumen $H^i_{rig}(\overline{U}) \to H^i_{MW}(\overline{U}/\mathbb{Q}_q)$.*

Damit haben wir folgenden Satz, den wir bei der Berechnung der Zetafunktion in späteren Abschnitten benutzen werden:

Satz 2.17. *Seien $\overline{V} = V(F)$, $F \in \mathbb{F}_q[X_0, ..., X_n]$, eine glatte, irreduzible Varietät in $\mathbb{P}^n_{\bar{\mathbb{F}}_q}$, $\overline{U}$ ihr Komplement, und U ein glatter Lift von $\overline{U}$ nach Charakteristik 0. Dann existiert ein $\mathbb{Q}_q$-linearer Isomorphismus*

$$\phi : H^n_{dR}(U/\mathbb{Q}_q) \to H^n_{MW}(\overline{U}/\mathbb{Q}_q).$$

Beweis. Aus Satz 2.15 folgt mit $\overline{Z} = \overline{V}$ und $\overline{X} = \mathbb{P}^n_{\overline{\mathbb{F}}_q}$, dass $H^n_{dR}(U/\mathbb{Q}_q) \cong H^n_{rig}(\overline{U})$. Analog wie in Satz 1.38 kann man zeigen, dass $\overline{U}$ affin ist. Also können wir Satz 2.16 anwenden. □

Wie alle Weil-Kohomologie-Theorien hat die rigide Kohomologie folgende Eigenschaften (s. [16, 1.2.2]):

Satz 2.18. *Seien $\overline{X}$ eine glatte, irreduzible, projektive Varietät über $\mathbb{F}_q$ von Dimension n und X ein Lift nach Charakteristik 0. Dann gilt:*

(i) $H^i_{rig}(X) = 0$ *für* $i \notin \{0, ..., 2n\}$.

(ii) Es existiert ein $\mathbb{Q}_q$-linearer Isomorphismus $H^{2n}_{rig}(\overline{X}) \to \mathbb{Q}_q$.

(iii) Sei $M^i(X) := \{Z \subset X \mid \dim(X) - \dim(Z) = i\}$ die Menge aller Untervarietäten der Kodimension $\operatorname{codim}(Z) = \dim(X) - \dim(Z) = i$. Sei $C^i(X) := \langle M_i \rangle_{\mathbb{Z}}$ die von ihr erzeugte freie abelsche Gruppe. Das heißt, alle Elemente $E \in C^i(X)$ sind formale endliche Summen $E = \sum_{i=1}^m n_i Z_i$, $Z_i \in M^i(X)$, $n_i \in \mathbb{Z}$, $m \in \mathbb{N}_0$. Dann existiert für alle $i \in \mathbb{N}_0$ eine funktorielle, nichttriviale Abbildung von $\mathbb{Z}$-Modulen $\gamma_X : C^i(X) \to H^{2i}_{rig}(X)$. $C^i(X)$ heißt die Zyklengruppe von Kodimension i in X.

Schließlich existiert noch eine weitere Kohomologie-Theorie, die wir für unsere Berechnungen verwenden werden (s. [3, Kapitel 3] und [5, Satz 1.10]). Ihre Wichtigkeit liegt insbesondere in der Existenz einer sogenannten *Ausschneide-Sequenz* (*excision sequence*). Wir erinnern kurz die Definition von exakten Sequenzen im Falle von Vektorräumen:

Definition 2.19. Seien $\{V_i,\ i \in \mathbb{Z}\}$ eine Familie von Vektorräumen und $\tau = (\tau_{i+1} : V_i \to V_{i+1})$ lineare Homomorphismen. Dann heißt

$$... \xrightarrow{\tau} V_{i-1} \xrightarrow{\tau} V_i \xrightarrow{\tau} V_{i+1} \xrightarrow{\tau} ...$$

eine *exakte Sequenz*, falls $\ker(\tau_i) = \operatorname{im}(\tau_{i-1})$ für alle $i \in \mathbb{Z}$.

Satz 2.20. *(Kohomologie mit kompaktem Träger)*
Seien $\overline{X}$ eine Varietät über $\mathbb{F}_q$, $\overline{U} \subset \overline{X}$ eine offene Teilmenge, $\overline{Z} = \overline{X} - \overline{U}$, und X,

Z, U die Lifts nach Charakteristik 0. Dann existiert eine Kohomologie-Theorie, genannt rigide Kohomologie mit kompaktem Träger, geschrieben $H^i_{rig,c}(\overline{X})$. Für sie gilt:

(i) $H^i_{rig,c}(\overline{X})$ *sind* $\mathbb{Q}_q$*-Vektorräume.*

(ii) Für alle $i \in \mathbb{Z}$ *existieren kanonische* $\mathbb{Q}_q$*-lineare Homomorphismen* $H^i_{rig,c}(\overline{X}) \to H^i_{rig}(\overline{X})$*, und falls X projektiv ist, dann sind sie Isomorphismen.*

(iii) Es existiert eine exakte Sequenz von Vektorräumen

$$... \to H^{i-1}_{rig,c}(\overline{U}) \to H^i_{rig,c}(\overline{Z}) \to H^i_{rig,c}(\overline{X}) \to H^i_{rig,c}(\overline{U}) \to H^{i+1}_{rig,c}(\overline{Z}) \to ...$$

(iv) Poincaré-Dualität. Falls $\overline{X}$ eine (affine oder projektive) glatte, irreduzible Varietät ist, dann gilt für $i = 0, ..., 2n$, $n = \dim(\overline{X})$:

$$H^i_{rig}(\overline{X}) \cong H^{2n-i}_{rig,c}(\overline{X})^*.$$

Insbesondere gilt also mit Satz 2.18 für eine projektive, glatte Varietät X:

$$H^i_{rig}(\overline{X}) \cong H^{2n-i}_{rig}(\overline{X})^*.$$

Mit den genannten Eigenschaften kann man das folgende Lemma beweisen, das wir im nächsten Abschnitt verwenden werden:

Lemma 2.21. *Sei $\overline{C} \subset \mathbb{P}^2_{\overline{\mathbb{F}}_q}$ eine projektive, irreduzible Kurve über $\mathbb{F}_q$ mit höchstens gewöhnlichen Doppelpunkten als Singularitäten und $\overline{U} = \mathbb{P}^2_{\overline{\mathbb{F}}_q} - \overline{C}$. Dann gilt:*

(i) $H^0_{MW}(\overline{U}/\mathbb{Q}_q) = \mathbb{Q}_q$,

(ii) $H^1_{MW}(\overline{U}/\mathbb{Q}_q) = (0)$.

Beweis. Zu (i): Nach Definition ist $H^0_{MW}(\overline{U}/\mathbb{Q}_q) = \ker\left(d : A(U)^\dagger \to \Omega_{A(U)^\dagger/\mathbb{Q}_q}\right)$. Nun ist der Körper der q-adischen Zahlen von Charakteristik 0.

Zu (ii): Wir haben in Satz 1.38 gesehen, dass $\overline{U}$ affin und glatt ist. Nach dem Satz von Berthelot, Satz 2.16, ist $H^1_{MW}(\overline{U}/\mathbb{Q}_q) \cong H^1_{rig}(\overline{U})$ und es reicht zu zeigen, dass $\dim(H^1_{rig}(\overline{U})) = 0$.

Mit der Poincaré-Dualität aus Satz 2.20 haben wir $H^1_{rig}(\overline{U}) \cong H^3_{rig,c}(\overline{U})^*$. Da dies endlich-dimensionale Vektorräume sind, folgt insbesondere $H^1_{rig}(\overline{U}) \cong H^3_{rig,c}(\overline{U})$. Es reicht also zu zeigen, dass $\dim(H^3_{rig,c}(\overline{U})) = 0$.

Für die rigide Kohomologie mit kompaktem Träger haben wir die lange, exakte Sequenz:

$$... \to H^2_{rig,c}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) \to H^2_{rig,c}(\overline{C}) \to H^3_{rig,c}(\overline{U}) \to H^3_{rig,c}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) \to ...$$

Da $\mathbb{P}^2_{\bar{\mathbb{F}}_q}$ glatt und projektiv ist, folgt mit den Sätzen 2.15 und 2.20:

$$H^2_{rig,c}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) \cong H^2_{rig}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) \cong H^2_{dR}(\mathbb{P}^2_{\mathbb{Q}_q}),$$

und man kann zeigen (s. [26, Korollar 3.1.4]), dass

$$H^i_{dR}(\mathbb{P}^n_{\mathbb{Q}_q}) \cong \begin{cases} \mathbb{Q}_q, \text{ falls } i \in \{0, 2, ..., 2n\} \\ (0), \text{ sonst.} \end{cases}$$

Dann verkürzt sich die exakte Sequenz auf der rechten Seite und wir erhalten:

$$... \to H^2_{rig,c}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) \to_h H^2_{rig,c}(\overline{C}) \to H^3_{rig,c}(\overline{U}) \to 0.$$

Also ist $H^3_{rig,c}(\overline{U}) \cong H^2_{rig,c}(\overline{C})/h(H^2_{rig,c}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}))$. Es reicht also zu zeigen, dass

$$\dim\left(H^2_{rig,c}(\overline{C})/h(H^2_{rig,c}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}))\right) = 0.$$

Hierfür hinreichend ist offensichtlich, dass

a.) $\dim(H^2_{rig,c}(\overline{C})) = 1$ und dass

b.) h nicht die Nullabbildung ist.

Zu a.): Nach [24, 5.3] ist die Normalisierung $\nu : C^\nu \to \overline{C}$ von $\overline{C}$ eine glatte Kurve, und es existieren offene Teilmengen $U_1 \subset C^\nu$, $U_2 \subset \overline{C}$, sodass $\nu_{U_1} : U_1 \to U_2$ ein Isomorphismus ist. Dann sind sowohl $E := C^\nu - U_1$ als auch $D := \overline{C} - U_2$ 0-dimensionale Zariski-abgeschlossene Teilmengen (D ist die Menge der gewöhnlichen Doppelpunkte, also endlich, und ν ist ein endlicher Morphismus). Wir haben dann wieder exakte Sequenzen:

$$... \to H^1_{rig,c}(D) \to H^2_{rig,c}(U_2) \to H^2_{rig,c}(\overline{C}) \to H^2_{rig,c}(D) \to ...$$
$$... \to H^1_{rig,c}(E) \to H^2_{rig,c}(U_1) \to H^2_{rig,c}(C^\nu) \to H^2_{rig,c}(E) \to ...$$

Für eine 0-dimensionale Varietät $X = \{P_1, ..., P_s\}$ ist außerdem

$$... \to H^{i-1}_{rig,c}(\{P_j\}) \to H^i_{rig,c}(X - \{P_j\}) \to H^i_{rig,c}(X) \to H^i_{rig,c}(\{P_j\}) \to ...,$$

$j \in \{1, ..., s\}$. Aus Satz 2.20 und Beispiel 2.8 wissen wir, dass

$$H^i_{rig,c}(\{P_j\}) \cong H^i_{rig}(\{P_j\}) \cong H^i_{MW}(\{P_j\}) \cong \begin{cases} \mathbb{Q}_q, \text{ falls } i = 0 \\ (0), \text{ sonst.} \end{cases}$$

Wir können also per Induktionsschritt $i \mapsto i-1$ schließen, dass $H^i_{rig,c}(X) \cong H^i_{dR}(P_j) = (0)$ für $i > 0$. Damit verkürzen sich die exakten Sequenzen zu

$$0 \to H^2_{rig,c}(U_2) \to H^2_{rig,c}(\overline{C}) \to 0$$

$$0 \to H^2_{rig,c}(U_1) \to H^2_{rig,c}(C^\nu) \to 0.$$

Und da $U_1 \cong U_2$ und $H^2_{rig,c}(C^\nu) = H^2_{rig}(C^\nu)$, ist dann also $H^2_{rig,c}(\overline{C}) = H^2_{rig}(C^\nu)$. Nun ist C^ν aber glatt, also folgt mit [26, Satz 3.2.2] $\dim(H^2_{rig}(C^\nu)) = 1$.
Zu b.): Aus der Poincaré-Dualität folgt, dass h die Poincaré-duale Abbildung zur von der Inklusion $i : \overline{C} \to \mathbb{P}^2_{\bar{\mathbb{F}}_q}$ induzierten Abbildung $i^* : H^2_{rig}(\overline{C}) \to H^2_{rig}(\mathbb{P}^2_{\bar{\mathbb{F}}_q})$ ist. Wir können $H^2_{rig}(C^\nu) = H^2_{rig,c}(\overline{C})$ schreiben (s.o.). Dann folgt die Aussage daraus, dass die Zyklengruppen-Abbildung γ funktorial und nicht trivial ist, d.h. wir haben das kommutierende Diagramm

$$\begin{array}{ccc} H^2_{rig,c}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) & \xrightarrow{h} & H^2_{rig,c}(\overline{C}) \\ \downarrow \| & & \downarrow \| \\ H^2_{rig}(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) & \xleftarrow{i^*} & H^2_{rig,c}(C^\nu) \cong H^2_{rig}(C^\nu) \\ \uparrow \gamma_{\mathbb{P}^2_{\bar{\mathbb{F}}_q}} & & \gamma_{C^\nu} \uparrow \\ C^1(\mathbb{P}^2_{\bar{\mathbb{F}}_q}) & \xleftarrow{\gamma(i^*)} & C^1(C^\nu) \end{array}$$

□

2.3 Berechnung der Zetafunktion mittels Kohomologie

Kommen wir nun zu der Frage, wie sich die Zetafunktion einer *glatten* Kurve $\overline{C} = V(\overline{F}) \subset \mathbb{P}^2_{\bar{\mathbb{F}}_q}$ mittels Monsky-Washnitzer-Kohomologie berechnen lässt.

Bemerkung 2.22. In diesem und allen folgenden Abschnitten setzen wir wieder voraus, dass Varietäten irreduzibel sind (s. Bemerkung 2.14).

Wir verwenden zur Berechnung der Zetafunktion den folgenden Satz von Van der Put [27, Satz 1.3].

Satz 2.23. *Sei $\overline{U}$ eine affine, glatte Varietät über $\mathbb{F}_q$, U ein Lift nach Charakteristik 0, $\mathrm{Frob}^* : H^i_{MW}(\overline{U}/\mathbb{Q}_q) \to H^i_{MW}(\overline{U}/\mathbb{Q}_q)$ der induzierte Frobenius-Automorphismus auf der Kohomologie. Für $n = \dim(U)$ gilt dann:*

$$Z(\overline{U}, T) = \prod_{i \in \{0,\ldots,2n\}} P_i(T)^{(-1)^{i+1}},$$

wobei $P_i(T) = \det(1 - q^n(\mathrm{Frob}^*)^{-1}T \mid H^i_{MW}(\overline{U}/\mathbb{Q}_q))$.

In unserem Falle, d.h. $\overline{C} \subset \mathbb{P}^2_{\overline{\mathbb{F}}_q}$ eine projektive Kurve über $\mathbb{F}_q$ und $\overline{U} = \mathbb{P}^2_{\overline{\mathbb{F}}_q} - \overline{C}$ heißt das, dass $Z(\overline{U}, T)$ gleicht dem folgenden Ausdruck ist:

$$\frac{\det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^1_{MW}(\overline{U}/\mathbb{Q}_q))}{\det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^0_{MW}(\overline{U}/\mathbb{Q}_q)) \det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q))}.$$

Mit Satz 1.46 folgt dann:

Satz 2.24. *Sei $\overline{C} \subset \mathbb{P}^2_{\overline{\mathbb{F}}_q}$ eine projektive Kurve über $\mathbb{F}_q$ mit höchstens gewöhnlichen Doppelpunkten als Singularitäten und $\overline{U} = \mathbb{P}^2_{\overline{\mathbb{F}}_q} - \overline{C}$. Dann ist*

$$Z(\overline{U}, T) = ((1 - q^2T) \det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q)))^{-1}$$

und insbesondere

$$Z(\overline{C}, T) = \frac{\det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q))}{(1 - T)(1 - qT)}.$$

Beweis. Wir verwenden Lemma 2.21 aus dem letzten Abschnitt:

$$H^0_{MW}(\overline{U}) = \mathbb{Q}_q,$$
$$H^1_{MW}(\overline{U}/\mathbb{Q}_q)) = (0).$$

Da $(\mathrm{Frob}^*)^{-1}$ ein $\mathbb{Q}_q$-linearer Homomorphismus von Vektorräumen ist, ist seine Wirkung auf $\mathbb{Q}_q$ die Identität $\mathrm{id}_{\mathbb{Q}_q}$, also $\det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^0_{MW}(\overline{U}/\mathbb{Q}_q)) = 1 - q^2T$. Und da $1 - q^2(\mathrm{Frob}^*)^{-1}$ nicht die Nullabbildung ist, ist

$$\det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^0_{MW}(\overline{U}/\mathbb{Q}_q)) = 1.$$

Es folgt dann mit Satz 1.46:

$$\begin{aligned} Z(\overline{C},T) &= \frac{1}{Z(\overline{U},T)(1-T)(1-qT)(1-q^2T)} \\ &= \frac{\det(1-q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q))(1-q^2T)}{(1-T)(1-qT)(1-q^2T)} \\ &= \frac{\det(1-q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q))}{(1-T)(1-qT)}. \end{aligned}$$

□

Korollar 2.25. *Für $\overline{C}$, $\overline{U}$ wie in Satz 2.24, aber $\overline{C}$ glatt, und $L(T)$ wie in Satz 1.46 ist*

$$L(T) = \det(1-q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q)).$$

Das heißt, die Berechnung der Zetafunktion einer glatten Kurve reduziert sich auf die Bestimmung der Determinante von $1-q^2(\mathrm{Frob}^*)^{-1}T$ auf $H^2_{MW}(\overline{U}/\mathbb{Q}_q)$. Wir brauchen hierfür zuerst eine Basis von $H^2_{MW}(\overline{U}/\mathbb{Q}_q)$. Dank Satz 2.17 können wir die Monsky-Washnitzer- mit der De-Rham-Kohomologie identifizieren. $H^n_{dR}(U/\mathbb{Q}_q)$ kann man mit [26, Definition 3.2.3] explizit aufschreiben. Wir formulieren das Resultat für Kurven:

Satz 2.26. *(Griffiths)*
Sei $\overline{C} = V(\overline{F}) \subset \mathbb{P}^2_{\bar{\mathbb{F}}_q}$, $\overline{U} := \mathbb{P}^2_{\bar{\mathbb{F}}_q} - \overline{C}$, $U = D(F)$ ein Lift nach Charakteristik 0. Definiere die 2-Form $\Omega \in \Omega^2_{A(U)/K}$ als

$$\Omega := X_0 dX_1 \wedge dX_2 - X_1 dX_0 \wedge dX_2 + X_2 dX_0 \wedge dX_1.$$

Seien weiter

$$\begin{aligned} M &= \left\{ \frac{G}{F^m}\Omega \mid \deg(G) = m\deg(F) - 3,\ G \in K[X_0,X_1,X_2] \text{ homogen} \right\}, \\ N &= \left\{ \frac{D_i(G)}{F^m}\Omega - m\frac{GD_i(F)}{F^{m+1}}\Omega \right\} \subset M, \end{aligned}$$

wobei $D_i(G) := \frac{\partial G}{\partial X_i}$ die partielle Ableitung nach der i-ten Variablen, $i = 0,1,2$. Dann ist

$$H^2_{dR}(U/\mathbb{Q}_q) \cong M/N.$$

Bemerkung 2.27. Wir werden gelegentlich M und N kürzer schreiben als:

$$M \cong \{G \in \mathbb{Q}_q[X_0, X_1, X_2] \mid G \text{ ist homogen, } \deg(G) = \deg(F)m - 3,\ m \in \mathbb{N}\}$$
$$N \cong \{GD_i(F) - m^{-1}D_i(G)\}.$$

Definition 2.28. Für ein $G \in M$ definieren wir die *Polordnung von* G als

$$m = m(G) = \deg(F)^{-1}(\deg(G) + 3).$$

Wenn F nicht singulär ist, dann ist $\mathbb{Q}_q[X_0, X_1, X_2]/(D_i(F), i = 0, 1, 2)$ ein endlich dimensionaler Vektorraum, dessen Basis wir leicht wie in [26, Bemerkung 3.2.5] bestimmen. Wir können endlich viele Monome $\omega_i \in \mathbb{Q}_q[X_0, X_1, X_2]$ mit minimalem Grad $\deg(\omega_i)$, $i \in I$ finden, sodass $\langle \omega_i \rangle_{\mathbb{Q}_q} = \mathbb{Q}_q[X_0, X_1, X_2]/(D_j(F), j = 0, 1, 2)$. Dann ist $\{\omega_i \mid \deg(\omega_i) = t\deg(F) - 3,\ t = 1, 2\}$ eine Basis von M/N, da ja dann $H \in M$ sich darstellen lässt als $H = \sum_{j=0}^{2} H_j D_j(F)$ und nach einem Reduktionsschritt erhält man dann $H \mapsto m^{-1}\left(\sum_{j=0}^{2} D_j(H_j)\right) \in M$.

Zur Berechnung definieren wir jetzt noch eine Inverse von Frob*. Wir wählen wie in [12] dazu die folgende Linksinverse des Frobenius:

Definition 2.29. Definiere ψ auf $A(U)$ als die $\mathbb{Q}_q$-lineare Fortsetzung von

$$\psi(X_0^{i_0}X_1^{i_1}X_2^{i_2}) := \begin{cases} X_0^{i_0/q}X_1^{i_1/q}X_2^{i_2/q} & \text{, falls } \forall j = 0, 1, 2,\ i_j \equiv 0 \mod q \\ 0 & \text{, sonst.} \end{cases}$$

Dann lässt sich ψ auf $A(U)^\dagger$ erweitern und induziert für $q > 2$ und Basiselemente $\omega_i = \frac{X_0^{i_0}X_1^{i_1}X_2^{i_2}}{F^t}\Omega \in H^2_{MW}(\overline{U}/K)$:

$$\psi^*(\omega_i) = \left[\frac{\sum_{j\geq 1}\psi(F^{q-t}X_0^{i_0}X_1^{i_1}X_2^{i_2}\Delta^j)}{F_{j+1}}\frac{\Omega}{p^2X_0X_1X_2}\right],$$

wobei $\Delta = F(X_0^q, X_1^q, X_2^q) - F(X_0, X_1, X_2)^q$, $t = (\sum_{j=0,1,2} i_{1,j} + 3)/\deg(F)$ und $[H]$ ist die Äquivalenzklasse von $H \in M \mod N$. ψ^* ist eine Linksinverse von Frob* auf $H^2_{MW}(\overline{U}/K)$. Wir schreiben für einen Repräsentanten von $\psi^*(\omega_i)$ gelegentlich auch $\widehat{\psi^*(\omega_i)} = (p^2X_0X_1X_2)^{-1}\sum_{j\geq 1}\psi\left(F^{q-t}X_0^{i_0}X_1^{i_1}X_2^{i_2}\Delta^j\right)$.

Wir wählen also eine Basis $\{\omega_i \mid i = 1, ..., m\}$ von $H^2_{MW}(\overline{U}/K)$.[2] Wir sind aber nicht in der Lage die unendliche Summe in Definition 2.29 zu berechnen.

[2] Die Berechnung von ψ^* teilt sich in die Berechnung von $\psi(\sum_i a_i X_0^{i_0}X_1^{i_1}X_2^{i_2})$ in $M = \{G \in$

Jede endliche Teilsumme $\psi_N^*(\omega_i)$ ist allerdings eine Klasse in $H^2_{dR}(U/\mathbb{Q}_q)$. Und für die Vektornorm $|\sum_i \alpha_i\omega_i|_p = p^{-\upsilon_p(\sum_i \alpha_i\omega_i)}$, $\upsilon_p(\sum_i \alpha_i\omega_i) = \min_i \upsilon_p(\alpha_i)$, gilt dann $\lim_{N\to\infty} |\psi_N^*(\omega_i) - \psi^*(\omega_i)|_p \to 0$. Wir nennen N die *Anfangspräzision*. Zur Bestimmung einer hinreichenden Anfangspräzision steht uns der folgende Satz zur Verfügung.

Satz 2.30. *Seien $\overline{C} = V(\overline{F}) \subset \mathbb{P}^2_{\overline{\mathbb{F}}_q}$ eine glatte, projektive Kurve über $\mathbb{F}_q$ von Geschlecht $g = (\overline{C})$ und $\overline{U}$ ihr Komplement in der projektiven Ebene, U ein Lift nach Charakteristik 0 und $L_N(T) := \det(1-q^2\psi_N^* T \mid H^2_{dR}(U/\mathbb{Q}_q)) = \sum_{i=0}^{2g} a_{i,N}T^i$. Definiere*

$$n := \left\lceil \log_q\left(2gq^{\frac{g}{2}}\right)\right\rceil$$
$$N := \min_m\{m - \upsilon_p(m!) \geq n+2\}.$$

Dann existiert für alle $i = 1, ..., g$ genau ein $b_i \in \left[-\binom{2g}{i}q^{\lfloor i/2\rfloor}, \binom{2g}{i}q^{\lfloor i/2\rfloor}\right] \cap \mathbb{Z}$ mit

$$|b_i - a_{i,N}|_p = \min\left\{|a - a_{i,N}|_p \ , \ a \in \left[-\binom{2g}{i}q^{\lfloor i/2\rfloor}, \binom{2g}{i}q^{\lfloor i/2\rfloor}\right] \cap \mathbb{Z}\right\}$$

und $b_i = a_i$ für $L(T) = \sum_{i=0}^{2g} a_i T^i$.

Beweis. Sei ω ein beliebiges Basiselement von $H^2_{dR}(U/\mathbb{Q}_q)$ und $\hat{\omega} = X_0^{i_{0,i}}X_1^{i_{1,i}}X_2^{i_{2,i}}$ der Repräsentant in M mit der niedrigsten Polordnung. Nach der Definition von $\psi_{N_0}^*$ ist

$$\begin{aligned}\nu_{N_0} &:= \widehat{\psi_{N_0}^*(\omega)} - \widehat{\psi_{N_0-1}^*(\omega)} \\ &= (p^2X_0X_1X_2)^{-1}\psi(F^{q-t}X_0^{i_{0,i}+1}X_1^{i_{1,i}+1}X_2^{i_{2,i}+1}\Delta^{N_0}) \in M\end{aligned}$$

von Polordnung $m := N_0 + 1$. Nach [26, Korollar 3.4.7] ist dann $\upsilon_p([\nu_{N_0}]) \geq \upsilon_p(\nu_{N_0}) - \upsilon_p(N_0!)$. Nun ist $\Delta \equiv 0 \mod p$, also $\Delta^i \equiv 0 \mod p^i$, für alle $i \geq 1$ und

$\mathbb{Q}_q[X_0, X_1, X_2] \mid G$ ist homogen, $\deg(G) = \deg(F)m - 3$, $m \in \mathbb{N}\}$ und die Reduktion $\rho : M \to H^2_{MW}(\overline{U}/K)$ durch die Relationen in $N = \{GD_i(F) - m^{-1}D_i(G)\}$. Für jeden Schritt $\hat{\rho}(H) : M \to M$ in der Reduktion schreiben wir $H \in M$, $\deg(H) = m\deg(F) - 3$, als $H = \sum_{i=0,1,2} H_iD_i(F)$ und setzen $\hat{\rho}(H) := m^{-1}\sum_{i=0,1,2} D_i(H_i)$. Die Darstellung von H mittels der partiellen Ableitungen ist nicht eindeutig, aber falls der Reduktionsschritt $\hat{\rho}'$ eine andere Darstellung verwendet, so gilt doch $\hat{\rho}^m(H) = \hat{\rho}'^m(H)$.

somit $v_p(\nu_{N_0}) = v_p(p^{N_0-2}(X_0X_1X_2)^{-1}\psi(F^{q-t}X_0^{i_{0,i}+1}X_1^{i_{1,i}+1}X_2^{i_{2,i}+1}p^{-N_0}\Delta^{N_0})) \geq N_0 - 2$. Daraus folgt, dass $v_p([\nu_{N_0}]) \geq N_0 - 2 - v_p(N_0!)$. Andererseits ist $a_i \in \left[-\binom{2g}{i}q^{\lfloor i/2 \rfloor}, \binom{2g}{i}q^{\lfloor i/2 \rfloor}\right] \cap \mathbb{Z}$ bzw. $|a_i|_{\mathbb{C}} \leq gq^{\lfloor i/2 \rfloor}$ für $i = 1, ..., g$. Und nach [11, 3.4] ist die endliche p-adische Entwicklung $a^{(n)} := \sum_{i=0}^{n} \alpha_i p^i$ aller

$$a \in \left[-gq^{\lfloor g/2 \rfloor}, gq^{\lfloor g/2 \rfloor}\right] \cap \mathbb{Z}$$

eindeutig. □

Definition 2.31. Wir nennen n aus obigem Satz die *Endpräzision*.

Für glatte Kurven sieht unser Algorithmus dann folgendermaßen aus:

Algorithmus 1. *Zetafunktion für glatte Kurven*

Input: Glatte Kurve $V(F)$ über k definiert durch $q = p^r$, $r \in \mathbb{N}$, $F \in \bar{k}[X_0, X_1, X_2]$.

Output: $Z(V(F), T)$.

(i) Wähle eine Basis $\{\omega_i \mid i = 1, ..., 2g\}$ von $H^2_{MW}(\overline{U}/K)$.

(ii) Setze n und N wie in Satz 2.30.

(iii) Für $i = 1, ..., 2g$ berechne

$$\psi^*_N(\omega_i) := \left[(p^2X_0X_1X_2)^{-1}\sum_{j\geq 1}^{N}\psi(F^{q-t}X_0^{i_{0,i}+1}X_1^{i_{1,i}+1}X_2^{i_{2,i}+1}\Delta^j)\right].$$

(iv) Berechne $\sum_{i=1}^{2g} a_{i,N}T^i = \det(1 - q^2\psi^*_N T)$.

(v) Für $i = 1, ..., g$ bestimme $a_i \in \left[-\binom{2g}{i}q^{\lfloor i/2 \rfloor}, \binom{2g}{i}q^{\lfloor i/2 \rfloor}\right] \cap \mathbb{Z}$.

(vi) Setze $a_0 := 1$, $a_{2g} := q^g$, $a_{2g-i} := q^{g-i}a_i$, für $0 < i < g$.

(vii) Setze $Z(V(F), T) := \frac{\sum_{i=0}^{2g} a_i T^i}{(1-T)(1-qT)}$.

3 Zetafunktion einer Kurve von Geschlecht 5

Wir haben im letzten Kapitel den Algorithmus von Abbott, Kedlaya und Roe [26] kennengelernt. Dabei haben wir die Identität $H^2_{dR}(U/\mathbb{Q}_q) \cong H^2_{MW}(\overline{U}/\mathbb{Q}_q)$, auf affinen $\overline{U}$, U mit glattem Komplement $C = \mathbb{P}^2_{\mathbb{Q}_q} - U$, genutzt, um eine Darstellung für die Kohomologie-Gruppe $H^2_{MW}(\overline{U}/\mathbb{Q}_q)$ zu erhalten, die uns in die Lage versetzt, die Wirkung der Inversen ψ^* des Frobenius auf dieser Gruppe zu berechnen. In diesem Kapitel versuchen wir, Kloostermans Ansatz [12] folgend, den Algorithmus so zu modifizieren, dass er uns ermöglicht, die Zetafunktion von Kurven mit gewöhnlichen Doppelpunkten zu berechnen.

3.1 Berechnung der Zetafunktion einer singulären Hyperfläche

In diesem Abschnitt fassen wir kurz die Berechnung einer singulären Hyperfläche, wie sie Kloosterman [12] beschreibt, zusammen. Die Grundideen werden wir im nächsten Abschnitt dann verallgemeinern, um einen Algorithmus für singuläre Kurven abzuleiten.

Zunächst bemerken wir, dass wir uns bei unseren Betrachtungen auf den Fall von Kurven mit höchstens gewöhnlichen Doppelpunkten als Singularitäten beschränkt haben. Die Betrachtungen aus [26] sind aber allgemeiner formuliert. Insbesondere gelten die wichtigen Sätze auch für das Beispiel Kloostermans, der Hyperfläche $V(\overline{F})$, $\overline{F} = X_1^2 + X_2^2 + X_3^2 \in \bar{\mathbb{F}}_p[X_0, X_1, X_2, X_3]$. Die Hyperfläche hat eine Singularität am Punkt $P = (1 : 0 : 0 : 0)$. Wenn wir einen Lift U von $\overline{U} = \mathbb{P}^3_{\bar{\mathbb{F}}_p} - V(\overline{F})$ wählen, dann können wir den Satz von Baldassari-Chiarellotto (Satz 2.17), d.h.

die Identifikation von De-Rham- und Monsky-Washnitzer-Kohomologie, nicht anwenden, da dort die Glattheit des Komplements vorausgesetzt wurde. Es gelingt Kloosterman aber, die Zetafunktion von $V(\overline{F})$ für $p > 2$ korrekt zu bestimmen, indem er Folgendes verwendet:

Satz 3.1. *Seien $\overline{V} = V(F)$, $F \in \mathbb{F}_q[X_0, ..., X_n]$, eine Varietät in $\mathbb{P}^n_{\overline{\mathbb{F}}_q}$, für die gilt, dass der Unterraum aller singulären Punkte Dimension 0 hat. Seien weiter $\overline{U}$ ihr Komplement, und U ein glatter Lift von $\overline{U}$ nach Charakteristik 0, mit glattem Komplement $V = \mathbb{P}^n_{\mathbb{Q}_q} - U$. Dann existiert ein $\mathbb{Q}_q$-linearer Epimorphismus*

$$\phi : H^n_{dR}(U/\mathbb{Q}_q) \to H^n_{MW}(\overline{U}/\mathbb{Q}_q),$$

für den das folgende Diagramm kommutiert:

$$\begin{array}{ccc} H^n_{dR}(U/\mathbb{Q}_q) & \xrightarrow{\phi} & H^n_{MW}(\overline{U}/\mathbb{Q}_q) \\ \downarrow{\scriptstyle \psi^*} & & \downarrow{\scriptstyle (\mathrm{Frob}^*)^{-1}} \\ H^n_{dR}(U/\mathbb{Q}_q) & \xrightarrow{\phi} & H^n_{MW}(\overline{U}/\mathbb{Q}_q) \end{array}$$

Beweis. Wir beweisen den Satz nur für den Fall, dass $\overline{V}$ eine Kurve mit höchstens r gewöhnlichen Doppelpunkten als Singularitäten in der projektiven Ebene ($n = 2$) ist: Wir wissen, dass $H^n_{dR}(U/\mathbb{Q}_q)$ und $H^n_{MW}(\overline{U}/\mathbb{Q}_q)$ endlich-dimensionale $\mathbb{Q}_q$-Vektorräume sind. Für die De-Rham-Kohomologie folgt dies aus der Darstellung nach Griffiths, s. Satz 2.26, für die Monsky-Washnitzer-Kohomologie (und glattem $\overline{U}$) zeigt dies Van der Put [27]. Somit ist die Aussage äquivalent dazu, dass $\dim\left(H^n_{dR}(U/\mathbb{Q}_q)\right) \geq \dim\left(H^n_{MW}(\overline{U}/\mathbb{Q}_q)\right)$. Es gilt aber, dass

$$\begin{aligned} \dim\left(H^n_{dR}(U/\mathbb{Q}_q)\right) &= 2 \cdot g(V) + 2r \\ \dim\left(H^n_{MW}(\overline{U}/\mathbb{Q}_q)\right) &= 2 \cdot g(\overline{V}) + r. \end{aligned}$$

Beide Gleichungen folgen aus den Eigenschaften der Zetafunktion, s. Satz 1.46, Satz 2.23 und [7, IV, Bemerkung 3.11.1]. Die Behauptung folgt dann aus der Gleichheit $g(\overline{V}) = g(V)$. Die Konvergenz von ψ^* und die Kompatibilität mit der Inversen des Frobenius folgt aus [12, Beispiel 12 und Bemerkung 14]. □

Es gilt dann auch:

Satz 3.2. *Seien ψ^* und ϕ wie in Satz 3.1 und $\lambda v = \psi^*(v)$, $v \neq \overrightarrow{0}$. Dann sind folgende Bedingungen äquivalent:*

(i) $\lambda = 0$

(ii) $v \in \ker(\phi)$.

Beweis. ϕ ist surjektiv; also können wir die Abbildung faktorisieren $\phi = \bar{\phi} \circ \pi$, wobei $\pi : H^n_{dR}(U/\mathbb{Q}_q) \to H^n_{dR}(U/\mathbb{Q}_q)/\ker(\phi)$ die Restklassenabbildung und $\bar{\phi}$ ein Isomorphismus sind. Das heißt, wir erhalten ein kommutatives Diagramm:

$$\begin{array}{ccccc} H^n_{dR}(U/\mathbb{Q}_q) & \xrightarrow{\pi} & H^n_{dR}(U/\mathbb{Q}_q)/\ker(\phi) & \xrightarrow{\bar{\phi}} & H^n_{MW}(\overline{U}/\mathbb{Q}_q) \\ \downarrow{\scriptstyle \psi^*} & & \downarrow{\scriptstyle \overline{\psi^*}} & & \downarrow{\scriptstyle (\mathrm{Frob}^*)^{-1}} \\ H^n_{dR}(U/\mathbb{Q}_q) & \xrightarrow{\pi} & H^n_{dR}(U/\mathbb{Q}_q)/\ker(\phi) & \xrightarrow{\bar{\phi}} & H^n_{MW}(\overline{U}/\mathbb{Q}_q) \end{array}$$

Da der Frobenius-Morphismus auf der Monsky-Washnitzer-Kohomologie ein Automorphismus ist, folgt dies auch für $\overline{\psi^*}$. Eine Basis aus Eigenvektoren e_i, $i = 1, ..., l$, von ψ^* mit Eigenwerten λ_i liefert dann eine Basis $\bar{\phi}(\overline{e_i})$ von $H^n_{MW}(\overline{U}/\mathbb{Q}_q)$ für alle i mit $\phi(e_i) \neq \overrightarrow{0}$. Außerdem gilt $\overline{\psi^*}(\overline{e_i}) = \overline{\psi^*(e_i)} = \overline{\lambda_i e_i} = \lambda_i \overline{e_i}$. Und schließlich

$$\begin{aligned} (\mathrm{Frob}^*)^{-1}(\bar{\phi}(\overline{e_i})) &= \bar{\phi}(\overline{\psi^*}(\overline{e_i})) \\ &= \bar{\phi}(\lambda_i \overline{e_i})) \\ &= \lambda_i \bar{\phi}(\overline{e_i}). \end{aligned}$$

□

Damit ist es Kloosterman [12] möglich, den Kern von ϕ zu bestimmen, indem er geschickt Lifts U_k wählt, ψ^* mit einer Arbeitspräzision von N berechnet und zeigt, dass die Eigenwerte hinreichend klein sind, d.h. hinreichend große p-adische Bewertung haben:

Satz 3.3. *Seien $\overline{F} = X_1^2 + X_2^2 + X_3^2 \in \bar{\mathbb{F}}_p[X_0, X_1, X_2, X_3]$, $\overline{U} = D(\overline{F_k}) \subset \mathbb{P}^2_{\bar{\mathbb{F}}_p}$, $F_k = F + p^k X_0^2$, $k \in \mathbb{N}$, $F = \overline{F}$ interpretiert als Polynom in $\mathbb{Q}_p[X_0, X_1, X_2, X_3]$. Dann existiert ein $k_0 \in \mathbb{N}$, sodass*

$$\ker(\phi) = H^3_{dR}(U_{k_0}/\mathbb{Q}_p).$$

Beweis. Beweisskizze, Details s. [12, 3.2]

(i) $H^3_{dR}(U_k/\mathbb{Q}_p) = \left\langle \frac{1}{F_k^2}\Omega \right\rangle_{\mathbb{Q}_p}$.

(ii)

$$\begin{aligned}
&\psi^*\left(\frac{1}{F_k^2}\Omega\right) \mod p^N \\
&\equiv \sum_{j=0}^{N-1}(-1)^j \sum_{i=j}^{N-1}\binom{i}{j}\frac{\psi\left(X_0X_1X_2X_3F_k^{(j+1)p-2}\right)}{F_k^{j+1}}\frac{\Omega}{p^3X_0X_1X_2X_3}.
\end{aligned}$$

(iii) Jedes Monom m in $\psi\left(X_0X_1X_2X_3F_k^{(j+1)p-2}\right)$ hat die Form

$$m = p^{k\left(\frac{p-1}{2}\right)+pt_0}bX_0^{1+2t_0}X_1^{1+2t_1}X_2^{1+2t_2}X_3^{1+2t_3}$$

mit Parametern $t_j \in \mathbb{N}_0$ und $b \in \mathbb{Z}_p$, sodass also jedes Monom m' im Zähler von $\psi^*\left(\frac{1}{F_k^2}\Omega\right) \mod p^N$ sich schreiben lässt als:

$$m' = p^{k\left(\frac{p-1}{2}\right)+pt_0}bX_0^{2t_0}X_1^{2t_1}X_2^{2t_2}X_3^{2t_3}.$$

(iv) Die Reduktion des Summands $\frac{m'}{F_k^s}\Omega$ hat die Form $\gamma bp^{k\left(\frac{p-1}{2}\right)+pt_0-kt_0}\frac{1}{F_k^2}\Omega$, $\gamma \in \mathbb{Z}_p$, $t_0 \in \mathbb{N}_0$, d.h. $\frac{m'}{F_k^2}\Omega$ hat nach Reduktion die Form $cp^{\frac{1+2t_0}{2}k(p-1)}\frac{1}{F_k^2}\Omega$, $c \in \mathbb{Z}_p$.

(v) Für die Reduktion $\omega_{k,N} := p^3\psi_N^*\left(\frac{1}{F_k^2}\Omega\right)$ ist dann $\omega_{k,N} \equiv 0 \mod p^{k\left(\frac{p-1}{2}\right)}$, wenn mindestens $N > 1$, da ja $\frac{1+2t_0}{2}k(p-1) \geq \frac{1}{2}k(p-1)$.

(vi) Aus Satz 3.1 folgt, dass für Eigenwerte λ von $\phi \circ \psi^*$ gilt: $|\lambda|_{\mathbb{C}} \leq p^3$.

(vii) Indem man nun einen Lift U_{k_0} wählt, sodass $k_0(p-1) \geq 8$, erhält man $\omega_{k_0,N} \equiv 0 \mod p^4$, also gilt insbesondere für den Eigenwert μ der 1×1-Matrix $[\psi^*_{N+1}]$, dass $|\mu|_{\mathbb{C}} > p^3$, d.h. μ kann kein Eigenwert von $[\phi \circ \psi^*_{N+1}]$ sein.

Da nun $\dim\left(H^3_{dR}\left(U_{k_0}/\mathbb{Q}_p\right)\right) = 1$, ist $H^3_{MW}\left(\overline{U}/\mathbb{Q}_q\right) = (0)$, und somit folgt die Behauptung. □

Wir sehen hier auch, dass der Eigenwert für wachsendes k schneller p-adisch gegen 0 konvergiert, entsprechend Satz 3.2.

3.2 Zetafunktion einer Kurve mit einem gewöhnlichen Doppelpunkt

In diesem Abschnitt leiten wir einen Algorithmus für die Berechnung der Zetafunktion einer Kurve mit einem gewöhnlichen Doppelpunkt ab. Genauer gesagt, entwickeln wir ihn für Kurven, die den folgenden zwei Bedingungen genügen:

Bedingung 1. *$\overline{C}$ sei eine Kurve in $\mathbb{P}^2_{\bar{\mathbb{F}}_p}$ mit einem gewöhnlichen Doppelpunkt P. Sie sei über $\mathbb{F}_p$ definiert, der Punkt P habe Koordinaten in $\mathbb{F}_p$ und es existiere eine glatte Kurve $\tilde{C}$ mit einer birationalen Abbildung $\pi : \tilde{C} \to \overline{C}$ gibt, sodass*

(i) $\pi^{-1}(P) = \{Q_1, Q_2\}$, *und die* Q_i, $i = 1, 2$, $Q_1 \neq Q_2$, *haben Koordinaten in* $\mathbb{F}_p$.

(ii) $\pi : \tilde{C} - \{Q_1, Q_2\} \to \overline{C} - \{P\}$ *ist ein* $\mathbb{F}_p$*-Isomorphismus.*

Bemerkung 3.4. Diese Konfiguration wird leicht erreicht, indem man den gewöhnlichen Doppelpunkt P nach O transformiert, dann die Kurve $\overline{C}$ in O aufbläst (s. Blow Up 1.27) und p so wählt, dass das definierende affine Polynom $\hat{F}$ in einer Umgebung von O einen Term von Grad 2 hat, der bereits über $\mathbb{F}_p$ in Linearfaktoren zerfällt.

Bedingung 2. *Für das Komplement $\overline{U}$ der Kurve $\overline{C} = V(\overline{F}) \subset \mathbb{P}^2_{\bar{\mathbb{F}}_q}$ existiert eine Familie von Lifts U_k wie in Satz 3.3, d.h. wir haben eine Familie von Lifts $U_k = D(F_k)$ mit $F_k = F + p^k X_2^{\deg(F)}$ und die F_k definieren glatte Kurven $V(F_k) \subset \mathbb{P}^2_{\mathbb{Q}_p}$.*

Bespiel 3.5. Wir betrachten die Kurve

$$V(X_1^5 + X_0^5 - 5X_0^4X_2 + 10X_0^3X_2^2 - 9X_0^2X_2^3 + 3X_0X_2^4) \subset \mathbb{P}^2_{\bar{\mathbb{F}}_{13}}.$$

Sie hat einen gewöhnlichen Doppelpunkt $P = (1 : 0 : 1)$ und ist $\bar{\mathbb{F}}_{13}$-isomorph zu der Kurve

$$\overline{C} = V(X_0^5 + X_1^5 + X_0^2X_2 + X_1^2X_2)$$

mit gewöhnlichem Doppelpunkt in $O = (0:0:1)$ (s. Beispiel 1.41). Da $5^2 = 25 \equiv -1 \mod 13$ sind dann für den Blow Up in O,

$$\begin{aligned}\tilde{C} =&\{(x_0 : x_1 : x_2; x_0 : x_1) \mid x_0 \neq 0 \neq x_1,\, x_0^5 + x_1^5 + x_2^3 x_0^2 + x_2^3 x_1^2 = 0\} \\ &\cup \{(0:0:1; z_0 : z_1) \mid z_0^2 + z_1^2 = (z_0 + iz_1)(z_0 - iz_1) = 0\},\end{aligned}$$

$Q_1 = (0:0:1;1:1)$, $Q_2 = (0:0:1;1:-1)$ und $\pi(Q_1) = \pi(Q_2) = P$, $\pi(x_0 : x_1 : x_2; x_1 : x_2) = (x_0 : x_1 : x_2)$ die Projektion von einem Punkt $R \in \overline{Q_1 Q_2}$ aus (s. Beispiel 1.27) und insbesondere $\pi_{|\tilde{C} - \{Q_1, Q_2\}}$ ein $\mathbb{F}_{13}$-Isomorphismus.
Eine Familie von Lifts $U_k = D(F_k)$, $F_k = F + p^k X_2^5$, steht dann analog wie im Beweis von Satz 3.3 zur Verfügung, mit $F = X_0^5 + X_1^5 + X_0^2 X_2 + X_1^2 X_2$ interpretiert in $\mathbb{Q}_{13}[X_0, X_1, X_2]$.

Der Algorithmus ließe sich leicht für eine beliebige Anzahl von gewöhnlichen Doppelpunkten als Singularitäten verallgemeinern. Wir werden aber noch sehen, dass wir mit dem Algorithmus nicht in der Lage sein werden, die Zetafunktion der Kurve aus Beispiel 3.5, eine Kurve von Geschlecht 5, zu bestimmen.

3.2.1 Der Algorithmus

Für eine Kurve, die den Bedingungen 1 und 2 genügt, gibt es nach Satz 3.1 für jedes $k \in \mathbb{N}$ eine surjektive Abbildung ϕ_k und ein kommutierendes Diagramm:

$$\begin{array}{ccc} H^n_{dR}(U_k/\mathbb{Q}_q) & \xrightarrow{\phi_k} & H^n_{MW}(\overline{U}/\mathbb{Q}_q) \\ \Big\downarrow{\scriptstyle \psi^* = \psi_k^*} & & \Big\downarrow{\scriptstyle (\mathrm{Frob}^*)^{-1}} \\ H^n_{dR}(U_k/\mathbb{Q}_q) & \xrightarrow{\phi_k} & H^n_{MW}(\overline{U}/\mathbb{Q}_q) \end{array}$$

Sei $\chi(p^2\psi^*, S, k) = \det(S - p^2\psi^* \mid H^2_{dR}(U_k/\mathbb{Q}_p))$ das charakteristische Polynom von $\psi^* = \psi_k^*$ in S. Dann ist mit Satz 3.2

$$\begin{aligned}\chi(p^2\psi^*, S, k) &= \det(S - p^2\psi^* \mid H^2_{dR}(U_k/\mathbb{Q}_p)) \\ &= \prod (S - \lambda)^{\mu_\lambda} \\ &= S^{\dim(\ker(\phi_k))} \det(S - p^2 \phi_k \circ \psi^* \mid H^2_{dR}(U_k/\mathbb{Q}_p)),\end{aligned}$$

wobei die μ_λ die Multiplizitäten der Nullstellen in λ sind. Da nun

$$\phi_k \circ \psi^* = (\mathrm{Frob}^*)^{-1} \circ \phi_k$$

folgt außerdem:

Satz 3.6. *Für eine Kurve $\overline{C}$, die die Bedingungen 1 und 2 erfüllt, gilt:*

$$\det\left(1 - p^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_p)\right) = T^d\chi(p^2\psi^*, T^{-1}, k)$$

Beweis.

$$\chi(p^2\psi^*, S, k) = S^{\dim(\ker(\phi_k))}\det(S - p^2\phi_k \circ \psi^* \mid H^2_{dR}(U_k/\mathbb{Q}_p)).$$

Es gilt außerdem mit $d := \dim\left(H^2_{dR}(U_k/\mathbb{Q}_q)\right)$:

$$S^{-d}\chi(p^2\psi^*, S, k) = \det(1 - p^2\psi^*S^{-1} \mid H^2_{dR}(U_k/\mathbb{Q}_p))$$

Also ist

$$S^{-\dim(\ker(\phi_k))}\chi(p^2\psi^*, S, k) = \det(S - p^2\phi_k \circ \psi^* \mid H^2_{dR}(U_k/\mathbb{Q}_p)),$$

woraus folgt, dass

$$\begin{aligned} S^{-d}\chi(p^2\psi^*, S, k) &= S^{\dim(\mathrm{im}(\phi_k))}(S^{-\dim(\ker(\phi_k))}\chi(p^2\psi^*, S, k)) \\ &= S^{\dim(\mathrm{im}(\phi_k))}\det(S - p^2\phi_k \circ \psi_N^* \mid H^2_{dR}(U_k/\mathbb{Q}_p)) \\ &= \det(1 - p^2\phi_k \circ \psi^*S^{-1} \mid H^2_{dR}(U_k/\mathbb{Q}_p)) \end{aligned}$$

Setze nun $T := S^{-1}$, dann folgt die Behauptung mit Satz 3.2. □

In Satz 2.24 haben wir gesehen, dass wir die Zetafunktion einer Kurve $\overline{C}$ mit höchstens gewöhnlichen Doppelpunkten als Singularitäten mittels ihres Komplements $\overline{U}$ ausdrücken können. Insbesondere gilt:

Satz 3.7. *Sei $\overline{C} = V(\overline{F}) \subset \mathbb{P}^2_{\overline{\mathbb{F}}_p}$ eine Kurve, die die Bedingung 1 erfüllt. Sei $Z(\tilde{C}, T) = \frac{\sum_{i=0}^{2g(\tilde{C})} a_iT^i}{(1-T)(1-pT)}$ die Zetafunktion der glatten Kurve $\tilde{C}$. Dann gilt für die Zetafunktion von $\overline{C}$:*

$$Z(\overline{C}, T) = \frac{\sum_{i=0}^{2g(\tilde{C})} a_iT^i}{(1-pT)}.$$

Beweis. Nach Voraussetzung existiert ein $\mathbb{F}_p$-Isomorphismus $\overline{C} - \{P\} \cong \tilde{C} - \{Q_1, Q_2\}$. Also ist $Z(\overline{C}, T) = Z(\tilde{C} - \{Q_1, Q_2\}, T)Z(\{P\}, T)$. Nun gilt für jeden Punkt Q, dessen Koordinaten alle in $\mathbb{F}_p$ liegen:

$$\begin{aligned} Z(Q,T) &= \exp\left(\sum_{r>0} N_r \frac{T^r}{r}\right) \\ &= \exp\left(\sum_{r>0} \frac{T^r}{r}\right) \\ &= \exp\left(-\sum_{r>0} (-1)^{r+1} \frac{(-T)^r}{r}\right) \\ &= \exp\left(-\log(1-T)\right) \\ &= \frac{1}{1-T}. \end{aligned}$$

Also folgt unter der Bedingung, dass Q_1, Q_2 ebenfalls $\mathbb{F}_p$-rational sind:

$$\begin{aligned} Z(\overline{C}, T) &= Z(\tilde{C} - \{Q_1, Q_2\}, T)Z(\{P\}, T) \\ &= \frac{Z(\tilde{C}, T)Z(\{P\}, T)}{Z(\{Q_1, Q_2\}, T)} \\ &= \frac{Z(\tilde{C}, T)Z(\{P\}, T)}{Z(\{Q_1\}, T)Z(\{Q_2\}, T)} \\ &= \frac{Z(\tilde{C}, T)}{Z(\{Q_1\}, T)} \\ &= Z(\tilde{C}, T)(1-T). \end{aligned}$$

□

Korollar 3.8. *Für $\overline{C}$ und $\tilde{C}$ wie in Satz 3.7, $g = g(\tilde{C})$, ist*

$$\det(1 - p^2\psi^* T \mid H^2_{dR}(U_k/\mathbb{Q}_p)) = (1-T)\sum_{i=0}^{2g} a_i T^i$$

Beweis. Aus den Sätzen 3.7 und 2.24 folgt, dass

$$\frac{\det(1 - p^2(\mathrm{Frob}^*)^{-1} T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_p))}{(1-T)(1-pT)} = \frac{\sum_{i=0}^{2g(\tilde{C})} a_i T^i}{(1-pT)}.$$

Und schließlich

$$\begin{aligned}
&\det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q)) \\
&= \prod_{i=1}^{2g}(1-\alpha_i T)(1-T) \\
&= (1-T)\sum_{i=0}^{2g} a_i T^i \\
&= \sum_{i=0}^{2g+1} b_i T^i,
\end{aligned}$$

wobei $b_0 = a_0$, $b_i = a_i - a_{i-1}$, $i = 1, ..., 2g$, $b_{2g+1} = -a_{2g}$. □

Wir wissen außerdem, dass für die b_i gelten muss: $|b_i|_{\mathbb{C}} \leq 2|a_i|_{\mathbb{C}} \leq 2\binom{2g}{i}p^{\frac{i}{2}}$. Außerdem kennen wir $a_0 = 1$ und können a_i, $i = 1, ..., g$, aus b_i, $i = 1, ..., g$, wiederherstellen, sodass es reicht, $p^2\psi_N^*$ bis zu einer Endpräzision von $\left\lceil \log_p\left(4gp^{\frac{g}{2}}\right)\right\rceil$ zu berechnen.

Wir haben in Satz 3.3 gesehen, dass die Wahl von k die Konvergenz der trivialen Eigenwerte beschleunigen kann. Die Frage eines guten k hängt also eng mit der Frage der Wahl der richtigen Arbeitspräzision N zusammen. Gehen wir fürs erste davon aus, wir würden hinreichende Werte für k und N kennen, dann sieht der Algorithmus folgendermaßen aus:

Algorithmus 2. *(Zetafunktion einer Kurve mit einem gewöhnlichen Doppelpunkt)*
Input: Kurve $V(\overline{F})$, die die Bedingungen 1 und 2 erfüllt, (n, k, N, p), F_k
Output: $Z(\overline{C}, T)$

(i) Berechne die Matrix $[p^2\psi_N^*]$ auf $H^2_{dR}(U_k/\mathbb{Q}_p)$.
(ii) Berechne $L_1(T) := \det(1 - p^2\psi_N^* T \mid H^2_{dR}(U_k/\mathbb{Q}_p)) = \sum_{i=0}^{2g(\overline{C})+1} b_{N,i}T^i$.
(iii) Setze $b_0 := 1$ und berechne $b_i \in \left[-\binom{2g}{i}p^{\lfloor g/i \rfloor}, \binom{2g}{i}p^{\lfloor g/i \rfloor}\right]$ für $i = 1, ..., g(\overline{C})$.
(iv) Setze $a_0 := 1$, für $i = 1, ..., g(\overline{C})$, $a_i := b_i - a_{i-1}$ und $a_{2g(\overline{C})-i} := q^{g(\overline{C})-i}a_i$.
(v) Setze $Z(\overline{C}, T) = \frac{\sum_i a_i T^i}{1-qT}$.

Bemerkung 3.9. Der Algorithmus lässt sich leicht für Kurven mit beliebiger Konfiguration von gewöhnlichen Doppelpunkten verallgemeinern. Wir tun dies nur beispielhaft: Falls Q_1, Q_2 nicht alle Koordinaten in $\mathbb{F}_p$ haben, dann lässt sich aus

den Eigenschaften des Blow Ups und der Definition von gewöhnlichen Doppelpunkten ableiten, dass ihre Koordinaten alle in $\mathbb{F}_{p^2}$ liegen müssen. Daraus folgt dann nach Satz 1.2, (iii), dass $N_r = 2$ falls $r \in 2\mathbb{N}$, sonst ist $N_r = 0$. Dann ist $Z(\{Q_1, Q_2\}, T) = (1-T^2)^{-1}$ und schließlich gilt analog wie in Satz 3.7:

$$Z(\overline{C}, T) = Z(\tilde{C}, T)(1+T) = \frac{\sum_{i=0}^{2g(\overline{C})} a_i T^i (1+T)}{(1-T)(1-qT)}$$

Und für die Determinante folgt dann

$$\begin{aligned}
&\det(1 - q^2(\mathrm{Frob}^*)^{-1}T \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q)) \\
&= \prod_{i=1}^{2g}(1-\alpha_i T)(1+T) \\
&= (1+T)\sum_{i=0}^{2g} a_i T^i \\
&= \sum_{i=0}^{2g+1} b_i T^i,
\end{aligned}$$

mit $b_0 = a_0, b_i = a_i + a_{i-1}, b_{2g+1} = a_{2g}$. Wenn wir im Algorithmus die Bestimmung der b_i, $i = 1, ..., g$, entsprechend anpassen, können wir also auch die Zetafunktion in diesem Fall berechnen.

3.3 Präzisionsfragen und Resultate

Wir haben im Algorithmus 2 die Kenntnis von N und k für die Endpräzision n vorausgesetzt. Auch haben wir im letzten Abschnitt gesehen, dass $n := \left\lceil \log_p \left(4gp^{\frac{g}{2}}\right) \right\rceil$ eine hinreichende Endpräzision ist. Wir können versuchen, wie im Falle von glatten Kurven, s. Satz 2.30, insbesondere aber wie im Beweis von Satz 3.3, $N = N(k)$ für festes k explizit zu bestimmen. Wie im Beweis von Satz 3.3 müssen wir dazu

(i) einen allgemeinen Ausdruck für alle monomialen Terme m in ψ_N^* finden, anhand dessen wir die p-adische Bewertung der m vor der Reduktion $m \mapsto \overline{m} \in M/N$ (s. Satz 2.26) ablesen können, und

(ii) den Präzisionsverlust, der durch die Reduktion auftritt, bestimmen.

Wir können (i) nicht allgemein lösen. Das sehen wir leicht, wenn wir die Definition von ψ^* (s. Definition 2.29) mit dem folgenden Ausdruck vergleichen:

$$\begin{aligned}
\Delta^i &= (\mathrm{Frob}_p(F_k) - F_k^p)^i \\
&= (\mathrm{Frob}_p(F) + p^k X_2^{\deg(F)p} - \sum_{j=0}^{p} \binom{p}{j} F^{p-j}(p^k X_2^{\deg(F)})^j)^i \\
&= (\mathrm{Frob}_p(F) + p^k X_2^{\deg(F)p} - (F^p + (p^k X_2^{\deg(F)})^p) - \sum_{j=1}^{p-1} \binom{p}{j} F^{p-j}(p^k X_2^{\deg(F)})^j)^i \\
&= (p^k(1-p^{(k-1)p})X_2^{\deg(F)p} + \sum_l b_l X_0^{l_0} X_1^{l_1} X_2^{l_2} - \sum_{j=1}^{p-1} \binom{p}{j} F^{p-j}(p^k X_2^{\deg(F)})^j)^i \\
&= \sum_{\substack{i_0+i_1+i_2=i \\ i_j \geq 0}} \binom{i}{i_0, i_1, i_2} \left(p^k(1-p^{(k-1)p})X_2^{\deg(F)p}\right)^{i_0} \\
&\cdot \left(\sum_l b_l X_0^{l_0} X_1^{l_1} X_2^{l_2}\right)^{i_1} \left(-\sum_{j=1}^{p-1} \binom{p}{j} F^{p-j}(p^k X_2^{\deg(F)})^j\right)^{i_2},
\end{aligned}$$

wobei die $b_l X_0^{l_0} X_1^{l_1} X_2^{l_2}$ die Monome aus F^p sind mit $\deg(b_l X_0^{l_0} X_1^{l_1} X_2^{l_2}) < p\deg(F)$. Wir haben allerdings folgende Aussage:

Satz 3.10. *Sei $[\psi^*_{k,N}] = (a_{i,j})$ die Matrix von ψ^* auf $H^2_{dR}(D(F_k)/\mathbb{Q}_q)$, berechnet mit Arbeitspräzision N und $\mu_{k,N} := \min_{i,j}\{v_p(a_{i,j})\}$. Dann sind für festes k_0 und N_0 aus $\mathbb{N}$ sowohl $\mu_{k_0,N}$ als auch μ_{k,N_0} monoton wachsende Folgen jeweils in k und N aus $\mathbb{N}$.*

Beweis. Nach Definition von Δ (Definition 2.29) und F_k (Bedingung 2) gilt:

$$\begin{aligned}
\Delta &\equiv 0 \mod p^k, \\
\Delta &\not\equiv 0 \mod p^{k+1}.
\end{aligned}$$

Hieraus folgt, dass

$$\begin{aligned}
\Delta^i &\equiv 0 \mod p^{ki}, \\
\Delta^i &\not\equiv 0 \mod p^{i(k+1)}.
\end{aligned}$$

Die Monotonie der $\mu_{k,N}$ folgt dann aus $p^{ki} < p^{(k+1)i}$ und $p^{ki} < p^{k(i+1)}$. □

Mit diesem Satz ist es uns möglich, die notwendige Präzision dynamisch zu bestimmen, und wir erhalten folgenden Algorithmus:

Algorithmus 3.

Input: Eine Kurve $\overline{C} = V(F_k \mod p)$*, die den Bedingungen 1 und 2 genügt.*

Output: Die Zetafunktion $Z(\overline{C}, T)$*.*

(i) *Berechne* $g = g(\overline{C})$ *und* $n = \left\lceil \log_p \left(4gp^{\frac{g}{2}}\right)\right\rceil$.

(ii) *Seien* $\nu_{k,N} := \psi^*_{N+1} - \psi^*_N$ *auf* $H^2_{dR}(U_1/\mathbb{Q}_q)$, $\Psi_N(k) := \sum_{i=1}^{N} \nu_{k,i}$ *und* $\mu_{k,N}$ *wie in Satz 3.10, und außerdem* $\beta : \mathbb{N} \to (\mathbb{N}^2, <_{lex})$ *die lexikografische Ordnung der Paare natürlicher Zahlen.*

(iii) *Setze* $i := 1$.

(iv) *Berechne für* $(k_i, N_i) := \beta(i)$, ν_{k_i,N_i}, $\Psi_{N_i}(k_i)$ *und* μ_{k_i,N_i}.

(v) *Falls* $\mu_{k_i,N_i} \geq n$*, gehe zu (vi). Sonst erhöhe* $i \mapsto i+1$ *und gehe zu (iv).*

(vi) *Berechne* $L(T) := \det(1 - p^2 T \Psi_{N_i}(k_i)) = \sum_{j=0}^{2g+1} b_{N,j} T^j$.

(vii) *Setze* $b_0 := 1$ *und bestimme für* $j = 1, ..., g$ *das* $b_j \in [-2\binom{j}{2g} q^{j/2}, \binom{j}{2g} q^{j/2}] \cap \mathbb{Z}$*, für das* $\upsilon_p(b_j - b_{N,j})$ *maximal ist.*

(viii) *Berechne* $a_0 := 1$, $a_i := b_i - a_{i-1}$, $a_{2g-i} := q^{g-i} a_i$ *für* $i = 0, ..., g-1$.

(ix) *Setze* $b_{2g+1} := -a_{2g}$, $b_i := a_i - a_{i-1}$, $i = g+1, ..., 2g$.

(x) *Gebe zurück* $Z(\overline{C}, T) := \frac{\sum_{i=0}^{2g+1} b_i T^i}{1-pT}$.

3.3.1 Bemerkungen zur Implementation

Wir haben Algorithmus 2 in `SINGULAR`, implementiert (s. Anhang 1). Damit haben wir die Zetafunktion von Kurven mit einem gewöhnlichen Doppelpunkt von Geschlecht $g = 3, 4$ erfolgreich über $\mathbb{F}_p$, $p = 5, 7$, bestimmen können. Im Falle von $g = 5$ ist uns dies nicht gelungen. Einerseits haben wir einen höheren Rechenaufwand, da ja $\dim(H^2_{dR}(U_k/\mathbb{Q}_q) = 2g + 2r = 10 + 2 = 12$. Andererseits fordert die Definition von ψ^* (s. Definition 2.29), dass wir für alle monomialen Terme $aX_0^{e_0} X_1^{e_1} X_2^{e_2}$ in $HX_0X_1X_2F^{q-t}\Delta^i$ feststellen müssen, ob e_i, $i = 0, 1, 2$, simultan modulo q verschwinden. Dies erfordert die Implementation verschachtelter Schleifenaufrufe. Die Anzahl der Schleifen wächst in Abhängigkeit mit der Anzahl der monomialen Terme in F, was man an dem Ausdruck für Δ^i im letzten Abschnitt ablesen kann. Außerdem müssen wir $q > \deg(F)$ wählen, was den Rechenaufwand zusätzlich erhöht. Wir können den Rechenaufwand verringern, indem wir eine andere Implementation von ψ^* oder dem Algorithmus selbst wählen. Andererseits

werden sich die Schleifenaufrufe vermutlich kaum verringern lassen. Deshalb können wir alternativ eine andere Wahl für die Frobenius-Inverse auf $H^2_{dR}(U_k/\mathbb{Q}_q)$ in Erwägung ziehen. Unsere Resultate sind also:

$\mathbf{g = 0}$: $F_{3,k} = X_0^2X_2 + X_1^2X_2 + X_0^3 + p^kX_2^3$

- Über $\mathbb{F}_5$: $\frac{1-T}{1-5T}$
- Über $\mathbb{F}_7$: $\frac{1+T}{(1+T)(1-7T)} = \frac{1}{1-7T}$

$\mathbf{g = 2}$: $F_{4,k} = X_0^2X_2^2 + X_0^2X_1^2 + X_0^4 + X_1^4 + p^kX_2^4$

- Über $\mathbb{F}_5$: $\frac{-25T^5+5T^4+6T^3+10T^2+3T+1}{1-5T}$
- Über $\mathbb{F}_7$: $\frac{49T^5-7T^4-26T^3+22T^2-7T+1}{(1+T)(1-7T)}$

$\mathbf{g = 5}$: $F_{5,k} = X_0^2X_2^3 + X_1^2X_2^3 + X_0^5 + X_1^5 + p^kX_2^5$

- Die Implementation unseres Algorithmus 2 gibt für $k, N \in \{1, ..., 9\}$ und p, ein Polynom $L(T)$ zurück, aber es gibt mindestens eine Nullstelle $\alpha \notin \{1, -1\}$ und $|\alpha|_{\mathbb{C}} \neq q^{\frac{1}{2}}$. Also kann $L(T)$ nicht der Zähler der Zetafunktion der Kurve sein.
- Bereits für $N = 9$ dauert die Berechnung sehr lange. Außerdem bekommen wir in Version 3.1.5 von `SINGULAR` Speicherverletzungsfehler bei der Berechnung bereits ab $N > 9$. Das gibt Anlass zur Vermutung, dass die Koeffizienten des charakteristischen Polynoms so groß werden, dass sie von `SINGULAR` nicht korrekt gespeichert werden können.

Anhang

1 Bemerkungen zur Implementation in SINGULAR

Zur Implementation der Algorithmen haben wir das Computer-Algebra-System SINGULAR [1] verwendet. Der Quellcode kann auf Github [2] eingesehen bzw. von dort heruntergeladen werden. Im Ordner *example* können unsere Resultate nachvollzogen werden. Für eigene Berechnungen folgende Bemerkungen:
Wir können für einen Repräsentanten $\omega = X_0^{e_0} X_1^{e_1} X_2^{e_1} \in M$ eines Basiselements $\bar{\omega} \in M/N \cong H^2_{dR}(U_k/\mathbb{Q}_q)$ schreiben:

$$
\begin{aligned}
&\widehat{\psi^*_{N+1}(\omega)} \\
&= \sum_{i\geq 1}^{N} \frac{\psi\left(F_k^{q-t} X_0^{e_0+1} X_1^{e_1+1} X_2^{e_1+1} \Delta^i\right)}{F_k^{i+1}} \frac{\Omega}{p^2 X_0 X_1 X_2} \\
&= \sum_{i\geq 1}^{N} \frac{\psi\left(F_k^{q-t} X_0^{e_0+1} X_1^{e_1+1} X_2^{e_2+1} \left(F_k(\overline{X}^q) - F_k(\overline{X})^q\right)^i\right)}{F_k^{i+1}} \frac{\Omega}{p^2 X_0 X_1 X_2} \\
&= \sum_{i\geq 1}^{N} \frac{\psi\left(F_k^{q-t} X_0^{e_0+1} X_1^{e_1+1} X_2^{e_2+1} \sum_{i=0}^{j} \binom{j}{i} F_k(\overline{X}^q)^{i-j} (-1)^j F_k(\overline{X})^{qj}\right)}{F_k^{i+1}} \frac{\Omega}{p^2 X_0 X_1 X_2} \\
&= \sum_{i\geq 1}^{N} \sum_{j=0}^{i} \binom{i}{j} (-1)^j \frac{\psi\left(F_k^{q-t} X_0^{e_0+1} X_1^{e_1+1} X_2^{e_2+1} F_k(\overline{X}^q)^{i-j} F_k(\overline{X})^{qj}\right)}{F_k^{i+1}} \frac{\Omega}{p^2 X_0 X_1 X_2} \\
&= \sum_{i\geq 1}^{N} \sum_{j=0}^{i} \binom{i}{j} (-1)^j \frac{F_k(\overline{X})^{i-j} \psi\left(F_k^{q-t+qj} X_0^{e_0+1} X_1^{e_1+1} X_2^{e_2+1}\right)}{F_k^{i+1}} \frac{\Omega}{p^2 X_0 X_1 X_2} \\
&= \sum_{i\geq 1}^{N} \sum_{j=0}^{i} \binom{i}{j} (-1)^j \frac{\psi\left(F_k^{q-t+qj} X_0^{e_0+1} X_1^{e_1+1} X_2^{e_2+1}\right)}{F_k^{j+1}} \frac{\Omega}{p^2 X_0 X_1 X_2} \\
&= \sum_{i\geq 1}^{N} \sum_{j=0}^{i} \binom{i}{j} (-1)^j \frac{\sum_{\tilde{t}\in T_j} \binom{q-t+qj}{\tilde{t}} \phi(p,\tilde{t}) X_0^{e_0(\tilde{t})} X_1^{e_1(\tilde{t})} X_2^{e_2(\tilde{t})}}{F_k^{j+1}} \frac{\Omega}{p^2} \\
&= \sum_{j\geq 1}^{N} (-1)^j \sum_{i=j}^{N} \binom{i}{j} \frac{\sum_{\tilde{t}\in T_j} \binom{q-t+qj}{\tilde{t}} \phi(p,\tilde{t}) X_0^{e_0(\tilde{t})} X_1^{e_1(\tilde{t})} X_2^{e_2(\tilde{t})}}{F_k^{j+1}} \frac{\Omega}{p^2},
\end{aligned}
$$

wobei $(e_0(\tilde{t}), e_1(\tilde{t}), e_1(\tilde{t}))$ die Exponenten der Monome sind, die nicht auf 0 abgebildet werden, und die Parametermenge T_j durch die Gleichung bestimmt wird, die sich bei Ausmultiplizieren von $F^{q-t+qj} X_0^{e_0} X_1^{e_1} X_2^{e_2}$ ergibt (s. Definition 2.29

und Kloostermans Beispiel in [12]).
Hieraus folgt, dass wir schreiben können:

$$\widehat{\psi^*_{N+1}(\omega)} = \sum_{j=0}^{N} c_j \frac{\sigma_j}{F_k^{j+1}} \frac{\Omega}{p^2}$$

und

$$\widehat{\nu_{k,N+1}(\omega)} = \sum_{j=0}^{N} d_j \frac{\sigma_j}{F_k^{j+1}} \frac{\Omega}{p^2}$$

wenn wir c_j, d_j und σ_j wie folgt setzen:

$$\begin{aligned}
c_j &:= \sum_{j\geq 1}^{N} (-1)^j \sum_{i=j}^{N} \binom{i}{j}, \\
\sigma_j &:= \sum_{\bar{t}\in T_j} \binom{q-t+qj}{\bar{t}} \phi(p,\bar{t}) X_0^{e_0(\bar{t})} X_1^{e_1(\bar{t})} X_2^{e_2(\bar{t})}, \\
d_j &:= (-1)^j \binom{N}{j}.
\end{aligned}$$

Diese Funktionen entsprechen den Funktionen `C(...), Sigma(...)` und `D(...)`.
Wie man anhand der Beispiele in *examples* nachvollziehen kann, muss für jedes definierende Polynom F dann außerdem eine Funktion `IndicesExponentsPhis(...)` definiert werden, die $\left(\left\{\sum_{\bar{t}\in T_j}\binom{q-t+qj}{\bar{t}}\right\}, \left\{\phi(p,\bar{t})\right\}, \left\{(e_0(\bar{t}), e_1(\bar{t}), e_1(\bar{t}))\right\}\right)$ für j zurückgibt. Die Funktion `Psi(...)` liefert ψ^*_{N+1} und `ReduceAllForPoleOrder(...)` liefert die Matrix $\nu_{k,N+1} = \left(\psi^*_{N+1} - \psi^*_N\right)_{|H^2_{dR}(U_k/\mathbb{Q}_q)}$.
Wollen wir die Zetafunktion von $\overline{F_{3,k}}$ (s. Abschnitt 3.3.1) über $\mathbb{F}_5$ berechnen, würden wir also zuerst die Definition von `IndicesExponentsPsi(...)` in eine Datei

`examples/indices_exponents/x2z_y2z_x3.sing`

schreiben und folgendes Skript aufrufen, vorausgesetzt, wir wollen die Zetafunktion mit Präzision N auf $H^2_{dR}(U_k/\mathbb{Q}_q)$ berechnen:

```
ring Q = (0,T), (x,y,z), dp;

execute(read("../lib/setup.sing"));
execute(read("./indices_exponents/x2z_y2z_x3.sing"));

k = 3;
N = 3;
p = 5;
r = 1;
g = 0;
vorz = -1;//vorz = -1 if sqrt(-1)\in F_p, vorz = 1 else
poly fpk = x^2*z + y^2*z + x3+(number(p)^k)*z^3;
list vals = setup(fpk,  intvec(0,3) ); //d*1-3, d*2-3
d = vals[1];
jf = vals[2];
bf = vals[3];
DIM = vals[4];
matrix PsiN = calc(p,1,k,N);
string L1 = getL1(PsiN,p);
list b1 = approximateBs(L1, p, r, g);//b_1,...,b_g
string L=LWithOrdinaryDP(b1,vorz,p,r);
write(":w L.txt",string(L));
exit;
```

Literaturverzeichnis

[1] SINGULAR - Computer Algebra System v3.1.5, Oktober 2012. URL `http://www.singular.uni-kl.de/`.

[2] Quellcode, Oktober 2012. URL `http://github.com/mathume/scurve`.

[3] P. Berthelot. Géométrie rigide et cohomologie des variétés algébriques de charactéristique p. *Mémoires de la S. M. F. 2e série*, 23, 1986.

[4] P. Berthelot. Finitude et pureté cohomologique en cohomologie rigide. *Invent. Math.*, 128, 1997.

[5] P. Berthelot. Dualité de Poincaré et formule de Künneth en cohomologie rigide. *C. R. Acad. Sci.*, 325, 1997.

[6] R. Gerkmann. Relative rigid cohomology and deformation of hypersurfaces. *International Mathematics Research Papers*, 2007, 2007.

[7] R. Hartshorne. *Algebraic Geometry*. Springer Verlag, New York, 1977.

[8] F. Torres J.W.P. Hirschfeld, G. Korchmaros. *Algebraic Curves over a Finite Field*. Princeton University Press, Woodstock, Oxfordshire, 2008.

[9] K. Kedlaya. p-adic cohomology - from theory to practice, 2007. URL `http://math.arizona.edu/~swc/aws/2007/`.

[10] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. 2001.

[11] K. S. Kedlaya. Computing zeta functions via p-adic cohomology. 2004.

[12] R. Kloosterman. Point counting on singular hypersurfaces. 2008.

[13] S. Lang. *Algebra.* Springer Verlag, New York, 2002.

[14] A. Lauder. Counting solutions to equations in many variables over finite fields. *Foundations of Computational Mathematics*, 4, 2004.

[15] B. Le Stum. *Rigid cohomology.* Cambridge University Press, Cambridge, 2007.

[16] Walker G. MacInnes. Computing zeta functions of varieties via fibration, 2009. URL `http://www.maths.bris.ac.uk/~magmw/GMW_thesis.pdf`.

[17] James S. Milne. Lectures on etale cohomology (v2.20), 2012. Available at www.jmilne.org/math/.

[18] A. Menezes N. Koblitz. A survey of public-key cryptosystems. *SIAM Review*, 46, 2004.

[19] J. Neukirch. *Algebraic Number Theory.* Springer Verlag, New York, 1999.

[20] G. Washnitzer P. Monsky. Formal cohomology: I. *The Annals of Mathematics*, 88, 1968.

[21] G. Washnitzer P. Monsky. Formal cohomology: II. *The Annals of Mathematics*, 88, 1968.

[22] G. Washnitzer P. Monsky. Formal cohomology: III. *The Annals of Mathematics*, 93, 1971.

[23] R. Pellikaan. On a decoding algorithm for codes on maximal curves. *IEEE Trans. Info. Theory*, 35, 6, 1989.

[24] I. R. Shafarevich. *Basic Algebraic Geometry*, volume 2. Springer Verlag, New York, 1997.

[25] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer Verlag, New York, 2009.

[26] D. Roe T. G. Abbott, K. S. Kedlaya. Bounding Picard numbers of surfaces using p-adic cohomology. 2006.

[27] M. van der Put. The cohomology of Monsky-Washnitzer. *Memoires de la S. F. M. 2 serie*, 23, 1986.

Index

Thesen

(i) Kurven von Geschlecht 5, $\overline{C} = V(\overline{F})$, $F \in \mathbb{F}_q[X_0, X_1, X_2]$, $q = p^r$, $r \in \mathbb{N}$ Primzahl, haben ein projektives, singuläres Modell mit gewöhnlichen Doppelpunkten als Singularitäten.

(ii) Das Komplement $\overline{U} = \mathbb{P}^2_{\overline{\mathbb{F}}_q} - \overline{C}$ einer Kurve mit höchstens gewöhnlichen Doppelpunkten als Singularitäten ist eine glatte, affine Varietät. Die Zetafunktion der Kurve kann durch ihr Komplement mittels Monsky-Washnitzer-Kohomologie berechnet werden:

$$Z(\overline{C}, T) = \frac{\det(1 - q^2 T(\mathrm{Frob}^*)^{-1} \mid H^2_{MW}(\overline{U}/\mathbb{Q}_q))}{(1-T)(1-qT)}$$

(iii) Für $\overline{U}$ wie oben und einen Lift U davon nach Charakteristik 0, sodass $V = \mathbb{P}^2_{\mathbb{Q}_q} - U$ eine glatte Kurve ist, existiert ein Epimorphismus von $\mathbb{Q}_q$-Vektorräumen ϕ und eine Darstellung einer Frobenius-Inversen ψ^*, sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} H^2_{dR}(U/\mathbb{Q}_q) & \xrightarrow{\phi} & H^2_{MW}(\overline{U}/\mathbb{Q}_q) \\ {\scriptstyle \psi^*}\downarrow & & {\scriptstyle (\mathrm{Frob}^*)^{-1}}\downarrow \\ H^2_{dR}(U/\mathbb{Q}_q) & \xrightarrow{\phi} & H^2_{MW}(\overline{U}/\mathbb{Q}_q) \end{array}$$

Und es folgt, dass

$$\ker(\phi) = \ker(\psi^*).$$

(iv) Also lässt sich die Determinante von $(1 - q^2 T(\mathrm{Frob}^*)^{-1})$ genauso berechnen wie im Fall, dass $\overline{C}$ eine glatte Kurve ist, d.h. man kann ψ^*_N bis zu einer Genauigkeit von $n = n(N)$ auf der De-Rham-Kohomologie berechnen und erhält bei hinreichender Präzision die Determinante von $(1 - q^2 T(\mathrm{Frob}^*)^{-1})$ auf der Monsky-Washnitzer-Kohomologie.

(v) Indem man eine Familie von Lifts $U_k = D(F_k)$, $F_k = F + p^k X_i^{\deg(F)}$ für geeignetes i betrachtet, kann die notwendige Arbeitspräzision N heruntergesetzt werden.

(vi) Die Matrix-Norm $|\psi^*_{N,k}|_p := \sup_{i,j} |(\psi^*_{N,k})_{i,j}|_p$ von ψ^* auf $H^2_{dR}(U_k/\mathbb{Q}_q)$ konvergiert monoton wachsend sowohl in k als auch in N.

(vii) Es gibt einen Algorithmus, der die Zetafunktion der Kurve $\overline{C}$ mit einem gewöhnlichen Doppelpunkt korrekt zurückgibt.

(viii) Eine naive Implementation des Algorithmus ist ineffizient, da für die Berechnung von $\psi^*_{N,k}$ verschachtelte Schleifenaufrufe implementiert werden müssen.

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe.

Ort, Datum	Unterschrift