Über Korrespondenzen zwischen algebraischen Funktionenkörpern

vorgelegt von
Diplom-Mathematiker
Markus Wagner
aus Hannover

Von der Fakultät II - Mathematik und Naturwissenschaften
der Technischen Universität Berlin
zur Erlangung des akademischen Grades
Doktor der Naturwissenschaften
Dr. rer. nat
genehmigte Dissertation

Promotionsausschuss:

Vorsitzender: Prof. Dr. Fredi Tröltzsch
Berichter: Prof. Dr. Florian Heß
Berichter: Prof. Dr. Pierrick Gaudry

Tag der wissenschaftlichen Aussprache: 21.11.2008

Berlin 2009

D83

Inhaltsverzeichnis

Symbolverzeichnis

Einleitung

Im Jahr 1937 legte M. Deuring mit seiner Arbeit „Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper", [Deu37], gefolgt von einem zweiten Teil [Deu40] um 1940, den Grundstein für seine arithmetische Theorie der Korrespondenzen. Mit Hilfe der Korrespondenzen lassn sich sämtliche Homomorphismen zwischen den Jacobischen zweier nichtsingulärer projektiver Kurven beschreiben. Korrespondenzen von Funktionenkörpern positiver Charakteristik haben in den letzten Jahren an Interesse gewonnen, weil es mehrere Anwendungen in der Kryptographie gibt: Zum Einen können wir mittels geeigneter Korrespondenzen die ganzzahlige Multiplikation auf den Jacobischen von Kurven beschleunigen. Zum Anderen zeigen sie Wege auf, wie man das Diskrete Logarithmusproblem, im Folgenden mit DLP abgekürzt, von hyperelliptischen Kurven vom Geschlecht drei auf nicht-hyperelliptische Kurven vom selben Geschlecht übertragen kann. Dies ist deshalb von Interesse, weil in der Arbeit [Die05] gezeigt wird, dass es möglich ist, das DLP in den Jacobischen letzterer Kurven effizienter zu lösen als in den Jacobischen hyperelliptischer Kurven vom Geschlecht drei. Und schließlich interessieren wir uns dafür, den Endomorphismenring der Jacobischen einer Kurve berechnen zu können, da er zu den wichtigsten Invarianten gehört.

Erst die algorithmische Betrachtung von Korrespondenzen zwischen Funktionenkörpern macht es möglich, nicht-triviale Beispiele von Endomorphismen berechnen zu können. Dabei fallen eine Reihe von aufwendigen Berechnungen an, wie zum Beispiel die Berechnung der Klassengruppe vom Grad null eines Funktionenkörpers $F/\mathbb{F}_q$, die Berechnung der Ordnung von Punkten in der Klassengruppe vom Grad null von $F/\mathbb{F}_q$ sowie die Faktorisierung von univariaten Polynomen, deren Koeffizienten in $F/\mathbb{F}_q$ liegen. Methoden zur Lösung dieser Probleme beherrscht man erst in jüngerer Zeit algorithmisch. Dies ist ein Grund, warum bislang kein algorithmischer Fortschritt bei der Berechnung von Korrespondenzen stattfand.

In dieser Arbeit konstruieren wir neue Algorithmen zur Berechnung des Endomorphismenrings einer beliebigen Kurve über einem endlichen Körper. Wir führen im ersten Kapitel zunächst in die Theorie der transzendenten

Konstantenkörpererweiterungen, abelsche Varietäten sowie zentral einfache Algebren ein. Viele Aussagen für die transzendenten Konstantenkörpererweiterungen bleiben dieselben wie im klassischen Fall. Allerdings müssen wir vom gewohnten Differentenbegriff abrücken und diesen neu definieren, da nun auch solche Primdivisoren Differententeiler sein können, die nicht verzweigen, deren Relativerweiterung aber inseparabel ist. Außerdem leiten wir wichtige Aussagen über das Verhalten der Dimension des Riemann-Roch-Raums, des Geschlechts und der Differente bei einer transzendenten Konstantenerweiterung her. Im Abschnitt über die abelschen Varietäten führen wir kurz in die Theorie der abelschen Varietäten über einem endlichen Körper $\mathbb{F}_q$ sowie deren dazugehörigen Endomorphismenringe ein. Schließlich skizzieren wir, wie eine Endomorphismenalgebra einer einfachen abelschen Varietät durch ihr Zentrum $F/\mathbb{Q}$ schon bis auf Isomorphie eindeutig bestimmt ist. Es zeigt sich, dass alle zentral-einfachen Algebren über einem Zahlkörper zyklisch sind. Diese Eigenschaft werden wir ausnutzen, um den vollen Endomorphismenring zu berechnen.

Im zweiten Kapitel beschäftigen wir uns mit den verschiedenen Sichtweisen auf die Korrespondenzen: Die algebraische Sicht und die geometrische Sicht. Im ersten Teil behandeln wir die Theorie der Korrespondenzen von M. Deuring, stützen uns aber auch auf M. Eichler. Im Fall, dass die regulären und algebraisch unabhängigen Funktionenkörper F_i/K $(i = 1, 2)$ isomorph sind, induzieren die Korrespondenzen Endomorphismen zwischen den Klassengruppen vom Grad null von F_1/K und F_2/K . Auf den Korrespondenzen lässt sich dann zusätzlich zur Addition noch eine Multiplikation einführen, womit diese dann einen nullteilerfreien Ring mit Einselement bilden. Im letzten Abschnitt des ersten Teils leiten wir den zentralen Satz von Deurings Theorie der Korrespondenzen her, nämlich den Restidealsatz. Im zweiten Teil dieses Kapitels stellen wir die Theorie der Korrespondenzen aus geometrischer Sicht dar. Daran anschließend führen wir eine Korrespondenzpaarung ein, die eine symmetrische positiv definite Bilinearform auf den Korrespondenzen induziert. Betrachten wir Endomorphismen, so ist es mit Hilfe der Korrespondenzpaarung möglich, das Minimalpolynom des einer Korrespondenz entsprechenden algebraischen Elements aus der Endomorphismenalgebra zu berechnen. Um die Anzahl der Schnittpunkte zweier Primkorrespondenzen mit Vielfachheit zu zählen, verwenden wir sogenannte Wechselsummen.

In seiner Arbeit [Deu40] zeigt Deuring, dass es möglich ist, Korrespondenzen zwischen den Funktionenkörpern F_2/K und F_1/K durch geeignete Matrizen darzustellen. Diese Matrizen mit Einträgen aus $\mathbb{F}_q$ beschreiben eine lineare Abbildung zwischen den Differentialen erster Gattung, s. [Kux04] und [Smi05]. Mit Hilfe solcher Matrizen können wir dann das charakteristische Polynom des der Korrespondenz entsprechenden Elements in der Endomorphismenalgebra berechnen. Damit dies funktioniert, müssen wir diese

Matrizen noch p-adisch liften, siehe dazu [Ver03]. Da wir in dieser Arbeit ausschließlich mit der Korrespondenzpaarung arbeiten, werden die Differentiale erster Gattung vernachlässigt.

Im dritten Kapitel werden verschiedene wichtige neue Algorithmen für die Korrespondenzen vorgestellt, hauptsächlich für den Fall, dass die Funktionenkörper isomorph sind, die Korrespondenzen also Endomorphismen induzieren. Zuerst konstruieren wir Algorithmen für die grundlegende Arithmetik, d.h. die Multiplikation der Korrespondenzen (s. Algorithmus 1). Dann stellen wir neue Algorithmen vor, die eine Korrespondenz als Homomorphismus oder Endomorphismus auf der Klassengruppe vom Grad null wirken lassen, siehe dazu Algorithmus 2 und 3. Anschließend zeigen wir, wie wir mit einem neuen Verfahren den Schnitt zweier Korrespondenzen mit Vielfachheit berechnen können (s. Algorithmus 4) und machen einige Bemerkungen zu den Laufzeiten der hier entwickelten Algorithmen.

Mit X_i/K bezeichnen wir die zu F_i/K gehörigen nicht-singulären projektiven, irreduziblen und reduzierten Kurven vom Geschlecht g_{X_i} $(i = 1, 2)$. Die Funktionenkörper sollen hier die definierenden Polynome $f_i(x_i, y_i) \in K(x_i)[y_i]$ besitzen, welche durch Vertauschen der Variablen auseinander hervorgehen. Die nicht-trivialen Korrespondenzen entsprechen dann unter gewissen Voraussetzungen an die Funktionenkörper F_i bestimmten nicht-trivialen Idealklassen der endlichen Maximalordnung von F_1F_2/F_2. Im vierten Kapitel stellen wir ein neues Verfahren vor, wie mit Hilfe der bereits entwickelten Algorithmen der volle Endomorphismenring der Jacobischen J_{X_2} berechnet werden kann, und zwar sowohl im kommutativen mittels Algorithmus 7 als auch im nicht-kommutativen Fall mit Algorithmus 8. Allerdings muss dazu die Jacobische J_{X_2} der Kurve $\mathbb{F}_q$-isogen zur Potenz einer einfachen abelschen Varietät A sein, d.h. $J_{X_2} \sim_K A^r$. Anderenfalls wenden wir Algorithmus 6 an, mit dessen Hilfe wir sogenannte orthogonale Korrespondenzen berechnen können. Mit Hilfe dieser orthogonalen Korrespondenzen können wir dann die Berechnung des Endomorphismenrings tensoriert mit $\mathbb{Z}[1/n]$ und einem bestimmten $n \in \mathbb{N}$. Die Endomorphismenalgebra $E_K := \mathrm{End}^0_K(J_{X_2})$ ist dann eine zentral-einfache Algebra über einem Zahlkörper und der gesuchte Endomorphismenring $R \subseteq E_K$ eine Ordnung darin. Sowohl im kommutativen Fall als auch im nicht-kommutativen Fall gilt, dass die Ordnung R in einer Maximalordnung $\mathcal{O}$ von E_K enthalten ist.

Als Erstes berechnen wir eine Ordnung $D \subseteq R$. Da in jedem Fall $\mathrm{disc}(D) = a\,\mathrm{disc}(\mathcal{O}) \in \mathbb{Z}$ gilt, steckt also im quadratischen Anteil von $a \in \mathbb{Z}$ die Information zu einem möglichen Aufstieg von D zur Ordnung R. Wir müssen also testen, ob Elemente von der Form α/m mit $m^2|a$ und $\alpha \in R \otimes \mathbb{Q}$ Endomorphismen sind. Um dies zu tun, beweisen wir in Satz 4.3, dass unter gewissen Annahmen an die Funktionenkörper F_i in jeder Korrespondenzklasse $[A]_C$ eine eindeutige und reduzierte Korrespondenz $C(A)$ vom Grad kleiner gleich

g_{X_2} mit bestimmten Eigenschaften existiert. Die in der Norm der gesuchten Korrespondenz $C(A)$ auftretenden Grade von Polynomen in der Variable x_2 lassen sich durch den positiven Ausdruck $\mathrm{Tr}_{E_K/\mathbb{Q}}(\alpha\alpha^\star)$ nach oben beschränken, was wir aus Lemma 4.7 und Lemma 4.9 folgern können. Hierbei soll $\alpha \in E_K$ das der Korrespondenz $C(A)$ entsprechende Element sein und $\alpha^\star$ sein Rosati. Wenn wir genügend geeignete Stellen $p \in \mathcal{D}_{F_2/K}$ vom Grad eins gefunden haben, interpolieren wir die Norm der dazugehörigen Korrespondenz mittels Algorithmus 5. Da dieser Algorithmus den Restidealsatz 2.16 benutzt, müssen wir an eine solche Stelle $p \in \mathcal{D}_{F_2/K}$ vom Grad eins noch die Anforderung stellen, dass für $C(A) = \sum e_i P_i$ mit $P_i \in \mathbb{P}_{F_2/K}$ jeweils p-reguläre Basen von $P_{i,0}$ existieren, so dass $C(A)(p) = \sum e_i \overline{P_i}^p$ gilt. Dieses Problem lösen wir mit Hilfe von Satz 4.6.

Wenn es einen Endomorphismus gibt, welcher einem ganzalgebraischen Element $\alpha \in E_K$ entspricht, so können wir die Norm und die Hochhebung der Norm der dazugehörigen Korrespondenz berechnen. Anderenfalls erhalten wir keine Lösung. Anschließend können wir im erfolgreichen Fall mit Hilfe der Korrespondenzpaarung ermitteln, welche der durch die Hochhebung erhaltenen Korrespondenzen unserer gesuchten Korrespondenz entspricht. Am Ende dieses Kapitels machen wir dann noch einige Bemerkungen zu den Laufzeiten der hier vorgestellten Algorithmen und stellen Vergleiche zu bereits bestehenden Verfahren zur Berechnung des Endomorphismenringes einer Kurve an. Hierbei wird sich herausstellen, dass das in dieser Arbeit vorgstellte Verfahren im Gegensatz zu den bereits bestehenden Verfahren ohne Schwierigkeiten zur Berechnung des Endomorphismenrings beliebiger Kurven von beliebigem Geschlecht herangezogen werden kann.

Im letzten Kapitel wollen wir anhand einiger Beispiele die gesamte Theorie der Korrespondenzen noch einmal Revue passieren lassen. Um die grundlegenden Eigenschaften der Korrespondenzen an Beispielen aufzuzeigen, eignen sich die Korrespondenzen von elliptischen Funktionenkörpern am besten. Anschließend geben wir kommutative Beispiele für Geschlecht zwei und drei, wobei wir im Fall von Geschlecht drei sowohl ein hyperelliptisches als auch nicht-hyperelliptisches Beispiel zeigen. Im Fall $g_{X_2} = 1$ und $g_{X_2} = 2$ zeigen wir, wie wir auch im nicht-kommutativen Fall den Endomorphismenring berechnen können. Abschließend folgt eine Tabelle mit Beispielen der Berechnungen des Endomorphismenrings der Klassengruppe vom Grad null über $\overline{K}$ für kommutative sowie nicht-kommutative Fälle.

Ich möchte mich an dieser Stelle bei Herrn Prof. Dr. F. Heß ganz herzlich für seine Hinweise, Unterstützung, Zusammenarbeit und anscheinend unendliche Geduld während der Anfertigung dieser Arbeit bedanken.

Ferner danke ich Herrn Dr. P. Gaudry für die Übernahme der Begutachtung dieser Arbeit und allen Mitgliedern der Kant-Gruppe. Besonders danke ich T. Lagemann, M. Minzlaff, O. Uzunkol und Dr. F. Nicolae für viele Anregungen und Tipps. Bei A.-K. Schlegel und Dr. J. Meyer bedanke ich mich für die Durchsicht einer vorläufigen Fassung.

Kapitel 1

Grundlagen

In diesem Kapitel werden die Grundlagen für die folgenden Kapitel geschaffen. Sämtliche Aussagen sind aus [Hes99], [Sti93], [Deu73], [Art67], [Sal06] oder [Eic63] entnommen und sollen hier, wenn sie nicht bewiesen werden, in knapper Form dargestellt werden.

Sei K ein Körper. Unter einem algebraischen Funktionenkörper F über K, kurz **Funktionenkörper**, wollen wir immer eine endlich erzeugte Erweiterung über K vom Transzendenzgrad eins verstehen. Sei F/K ein Funktionenkörper. Aus der Definition folgt, dass es ein über K transzendentes $x \in F$ gibt, so dass F eine endliche algebraische Erweiterung von $K(x)$ ist. Der Körper K eines Funktionenkörpers F/K wird **Konstantenkörper** genannt. Stimmt K mit seinem algebraischen Abschluss $\overline{K} \cap F$ in F überein, so nennen wir K den **genauen** Konstantenkörper des Funktionenkörpers F/K. Ein Funktionenkörper F/K heißt **regulär**, wenn K der genaue Konstantenkörper von F und F/K separabel ist.

Über die gesamte Arbeit wollen wir bei der Angabe eines Funktionenkörpers F/K stets voraussetzen, dass K, sofern nichts anderes deklariert wird, der genaue Konstantenkörper von F ist. Ist F/K durch $F = K(x, y)$ gegeben, so soll in der gesamten Arbeit y stets separabel über $K(x)$ sein.

1.1 Bewertungen, Stellen und Divisoren

Ein **Bewertungsring** eines Funktionenkörpers F/K ist ein Teilring $\mathcal{O} \subseteq F$ mit den Eigenschaften $K \subsetneq \mathcal{O} \subsetneq F$ und $z \in \mathcal{O}$ oder $z^{-1} \in \mathcal{O}$ für alle $z \in F$. Solch ein Ring ist lokal mit dem maximalen Ideal $P = t\mathcal{O}$, wobei $t \in P$ geeignet gewählt ist. Die Einheiten von $\mathcal{O}$ werden mit $\mathcal{O}^\times$ bezeichnet. Wir wollen dann P **Stelle** von F/K und t **Primelement zu P** nennen. Mit $\mathbb{P}_{F/K}$ bezeichnen wir die Gesamtheit aller Stellen von F/K. Den zu einer Stelle P zugehörigen Bewertungsring bezeichnen wir mit $\mathcal{O}_P$. Unter einer **diskreten**

Bewertung oder **Exponenten-Bewertung** von F/K verstehen wir eine Abbildung $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ mit den folgenden Eigenschaften:

(i) $v(x) = \infty \Leftrightarrow x = 0 \quad (x \in F)$,

(ii) $v(xy) = v(x) + v(y)$ für alle $x, y \in F$,

(iii) $v(x + y) \geq \min\{v(x), v(y)\}$ für alle $x, y \in F$,

(iv) es existiert ein Element $z \in F$ mit $v(z) = 1$ und

(v) $v(a) = 0$ für alle Konstanten aus $K^\times$.

Aus (ii) und (iv) folgt, dass v surjektiv ist. Wir ordnen nun jeder Stelle $P \in \mathbb{P}_{F/K}$ durch $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$, $z = t^n u \longmapsto n$ $(z \in F^\times)$ und $v_P(0) := \infty$ eine diskrete Bewertung zu, wobei $u \in \mathcal{O}_P^\times$, t ein Primelement zu P und $n \in \mathbb{Z}$ ist. Die Darstellung $z = t^n u$ ist eindeutig bis auf Einheiten und die Definition von v_P hängt nur von P ab. Für solch eine diskrete Bewertung gilt $\mathcal{O}_P = \{z \in F \mid v_P(z) \geq 0\}$, $\mathcal{O}_P^\times = \{z \in F \mid v_P(z) = 0\}$ und $P = \{z \in F \mid v_P(z) > 0\}$. Ist umgekehrt eine diskrete Bewertung v gegeben, so ist durch $P := \{z \in F \mid v(z) > 0\}$ eine Stelle von F/K und durch $\mathcal{O}_P := \{z \in F \mid v(z) \geq 0\}$ der zugehörige Bewertungsring bestimmt. Eine diskrete Bewertung v von F/K mit $v(x) = 0$ für alle $x \in F \backslash K$ heißt **trivial**. Stellen und Bewertungen entsprechen sich gegenseitig in eindeutiger Weise, und ein Funktionenkörper besitzt unendlich viele Stellen. Für eine Stelle $P \in \mathbb{P}_{F/K}$ bezeichne F_P den Restklassenkörper $\mathcal{O}_P/P$. Die Restklassenabbildung $x \longmapsto F_P$, welche K in F_P kanonisch einbettet, wird durch $x \longmapsto F_P \cup \{\infty\}$ auf ganz F fortgesetzt. Wir nennen $\deg P := [F_P : K]$ den **Grad** von P. Der Grad einer Stelle eines Funktionenkörpers ist stets endlich. Sei $x \in F$ ein über K transzendentes Element mit $F = K(x)$. Der Funktionenkörper F/K wird dann **rationaler Funktionenkörper** genannt. Sämtliche Stellen $P \in \mathbb{P}_{F/K}$ eines rationalen Funktionenkörpers F/K haben entweder ein Primpolynom oder $1/x$ als Primelement. Die zum Primelement $1/x$ gehörige Bewertung ist die durch $v_\infty(f(x)/g(x)) := \deg g - \deg f$ definierte Gradbewertung, wenn $f, g \in K[x]$ sind. Die Stellen $P \in \mathbb{P}_{F/K}$ vom Grad eins eines rationalen Funktionenkörpers F/K entsprechen in eindeutiger Weise den Elementen aus $K \cup \{\infty\}$.

Divisoren und Klassengruppen

Die von den Stellen $P \in \mathbb{P}_{F/K}$ erzeugte freie abelsche Gruppe heißt **Divisorengruppe** und deren Elemente **Divisoren**. Sie wird mit $\mathcal{D}_F$ bezeichnet und für ihre Gruppenoperation verwenden wir die additive Notation. Ein Divisor der Form $D = P$ heißt **Primdivisor**, und jedes Element $D \in \mathcal{D}_F$ besitzt

die eindeutige Darstellung $D = \sum_{P \in \mathbb{P}_{F/K}} n_P P$, wobei die n_P ganze Zahlen sind, welche fast immer $n_P = 0$ erfüllen. Die Bewertung einer Primstelle P kann mittels $v_P(D) := n_P$ auf die Divisorengruppe übertragen werden. Die Addition in $\mathcal{D}_F$ wird koeffizientenweise durchgeführt, und das neutrale Element ist $0 := \sum_{P \in \mathbb{P}_{F/K}} n_P P$, wobei $n_P = 0$ für alle n_P gilt. Für zwei Divisoren D_1 und D_2 können wir durch $D_1 \leq D_2 :\Leftrightarrow v_P(D_1) \leq v_P(D_2)$ für alle $P \in \mathbb{P}_{F/K}$ eine partielle Ordnung definieren. Ein Divisor $D \in \mathcal{D}_F$ mit $D \geq 0$ heißt **effektiv** oder **positiv**. Der **Grad eines Divisors** $D \in \mathbb{P}_{F/K}$ ergibt sich durch $\deg_{F/K} D := \sum_{P \in \mathbb{P}_{F/K}} v_P(D) \cdot \deg P$. Ist aus dem Zusammenhang klar, in welchem Funktionenkörper der Grad eines Divisors gebildet wird, so schreiben wir kurz $\deg D$. Für einen Divisor $D \in \mathcal{D}_F$ mit $D = \sum_{P \in \mathbb{P}_{F/K}} n_P P$ bezeichnet $\operatorname{supp} D := \{P \in \mathbb{P}_{F/K} \mid n_P \neq 0\}$ den **Träger** von D. Allgemein können wir für einen Divisor $D \in \mathcal{D}_F$ immer eine Darstellung $D = D_0 - D_\infty$ mit effektiven Divisoren $D_0, D_\infty \in \mathcal{D}_F$ finden, wobei D_0 **Nullstellendivisor** und D_∞ **Polstellendivisor** genannt wird. Ein **Hauptdivisor** $(x) = (x)_0 - (x)_\infty$ hat nur endliche viele Pol- und Nullstellen, und ist $x \in F \backslash K$, so gilt stets $\deg (x)_0 = \deg (x)_\infty = [F : K(x)]$. Für einen Hauptdivisor (x) mit $x \in F^\times$ ist $\deg (x) = 0$ und es gilt $x \in K^\times \Leftrightarrow (x) = 0$. Die Menge der **Divisoren vom Grad n** bezeichnen wir mit $\mathcal{D}_F^n$. Die **Divisoren vom Grad null** bilden eine Untergruppe von $\mathcal{D}_F$, und diese wird mit $\mathcal{D}_F^0$ bezeichnet.

Zwei Divisoren $D_1, D_2 \in \mathcal{D}_F$ nennen wir **äquivalent**, wenn $D_1 - D_2 = (x)$ ist mit $x \in F^\times$ und schreiben dafür $D_1 \sim D_2$. Mit $\mathcal{P}_F := \{(x) \mid x \in F^\times\}$ wollen wir die Untergruppe der Hauptdivisoren von F/K und mit der Faktorgruppe $\mathcal{C}_F := \mathcal{D}_F / \mathcal{P}_F$ die **Divisorenklassengruppe** bezeichnen, deren Elemente wir **Divisorenklassen** nennen wollen. Die Elemente der Faktorgruppe schreiben wir in der Form $[D]$, wobei D ein Vertreter der jeweiligen Restklasse sein soll. Die Gradfunktion auf einer Divisorenklasse $[D]$ ist wohldefiniert durch $\deg [D] := \deg D$. Mit $\mathcal{C}_F^n \subset \mathcal{C}_F$ sind dann die Divisorenklassen vom Grad n gemeint. Speziell ist $\mathcal{C}_F^0 = \mathcal{D}_F^0 / \mathcal{P}_F$ die **Divisorenklassengruppe vom Grad Null** von F/K, und die eventuell unendliche Zahl $h := |\mathcal{C}_F^0|$ nennen wir die **Klassenzahl** von F/K. Einen Zusammenhang zwischen Divisorenklassengruppe und Divisorenklassengruppe vom Grad null sowie eine Aussage über die Klassenzahl gibt die folgende Proposition [Hes99, Proposition 1.1, S. 3].

Proposition 1.1. *(i) Für die Divisorenklassengruppe eines Funktionenkörpers F/K gilt $\mathcal{C}_F \cong \mathcal{C}_F^0 \oplus \mathbb{Z}$.*

(ii) Die Klassenzahl eines Funktionenkörpers F/K über einem endlichen Körper K ist endlich.

Der Satz von Riemann-Roch

Sei F/K ein Funktionenkörper. Für einen Divisor $D \in \mathcal{D}_F$ bezeichne $\mathcal{L}(D) := \{x \in F^\times \mid (x) + D \geq 0\} \cup \{0\}$ den **Riemann-Roch-Raum** zu D. Dieser ist ein K-Vektorraum von endlicher Dimension $\dim D$. Äquivalente Divisoren $D, D' \in \mathcal{D}_{F/K}$ mit $D = D' + (f)$ besitzen isomorphe Riemann-Roch-Räume, d.h. insbesondere ist $\dim D = \dim D'$. Sind D, D' Divisoren mit $D' \leq D$, so gilt $\mathcal{L}(D') \subseteq \mathcal{L}(D)$ und $\dim \mathcal{L}(D)/\mathcal{L}(D') \leq \deg(D) - \deg(D')$. Das **Geschlecht** eines Funktionenkörpers F/K kann durch $g_{F/K} := \max\{ \deg D - \dim D + 1 \mid D \in \mathcal{D}_F \}$ definiert werden und ist stets eine nicht negative Zahl. Der Satz von Riemann-Roch trifft eine genaue Aussage über die Dimension eines Divisors. Wir fassen kurz alle wichtigen Aussagen im folgenden Satz zusammen [Sti93, p. 28-29].

Satz 1.2. *Sei F/K Funktionenkörper vom Geschlecht g. Dann gibt es eine eindeutige Divisorklasse $[W] \in \mathcal{C}_F$, so dass für beliebiges $D \in \mathcal{D}_F$ und jedes $W \in [W]$:*

$$\dim D = \deg D + 1 - g_{F/K} + \dim(W - D)$$

*ist. Die Elemente aus $[W]$ nennen wir **kanonische Divisoren**. Für einen kanonischen Divisor W von F/K gilt stets*

$$\deg W = 2g_{F/K} - 2 \quad \textit{und} \quad \dim W = g.$$

Ist $D \in \mathcal{D}_F$ mit $\deg_{F/K} D \geq 2g - 1$, so gilt

$$\dim D = \deg_{F/K} D + 1 - g.$$

1.2 Erweiterungen von Funktionenkörpern

Sämtliche Aussagen in diesem Abschnitt sind aus [Deu73] entnommen. Unter einer **Erweiterung** von F/K versteht man einen Funktionenkörper F'/K' mit $F \subseteq F'$ und $K' \cap F = K$. Ist $P' \in \mathbb{P}_{F'/K'}$ eine Stelle von F' mit $v_{P'}(z) = 0$ für alle $z \in F^\times$, so heißt $v_{P'}$ **trivial auf** F. Die Restriktion von $v_{P'}$ auf F definiert eine Bewertung v_P mit $P \in \mathbb{P}_{F/K}$ auf F, da $v_{P'}$ trivial auf K' und somit auf $K = K' \cap F$ ist. Ist $v_{P'}$ nicht trivial auf F, so wollen wir eine solche Stelle **konstant** nennen . Wir sagen dann P' **liegt über** P, kurz $P'|P$, und definieren die positive ganze Zahl $e(P'|P)$ durch die geltende Beziehung $v_{P'}(z) = e(P'|P)v_P(z)$ für alle $z \in F$. Die Zahl $e(P'|P)$ wollen wir **Verzweigungsindex** von P' über F nennen. Den Restklassenkörper F_P können wir kanonisch in den Restklassenkörper $F'_{P'}$ einbetten. Ist F'/K' Erweiterung von F/K und liegt die Stelle $P' \in \mathbb{P}_{F'/K'}$ über $P \in \mathbb{P}_{F/K}$, so wollen wir die endliche Zahl $f(P'|P) := [F'_{P'} : F_P]$ den **Relativgrad** von P'

über P nennen. Es gilt dann die Beziehung

$$f(P'|P) = \frac{[F'_{P'} : K'] \cdot [K' : K]}{[F_P : K]} = \frac{\deg_{F'/K'} P'}{\deg_{F/K} P} \cdot [K' : K].$$

Algebraische Erweiterungen

Eine Erweiterung F'/K' von F/K heißt **algebraisch**, wenn F'/F algebraisch ist, und **endlich**, wenn F'/F endlich ist. Ist F'/K' eine algebraische Erweiterung von F/K, so ist für eine Stelle $P' \in \mathbb{P}_{F'/K'}$ die korrespondierende auf F eingeschränkte Bewertung niemals trivial. Die Aussage P' liegt über P ist gleichbedeutend damit, dass $\mathcal{O}_P$ in $\mathcal{O}_{P'}$ enthalten ist. Endliche und algebraische Erweiterungen lassen sich wie folgt charakterisieren [Deu73, Chapter IV, p. 93].

Lemma 1.3. *Ist F'/K' eine Erweiterung von F/K, so sind folgende Aussagen äquivalent:*

(i) K'/K ist algebraisch (endlich).

(ii) F'/F ist algebraisch (endlich).

(iii) Liegt $P' \in \mathbb{P}_{F'/K'}$ über $P \in \mathbb{P}_{F/K}$, so ist $F'_{P'}/F_P$ algebraisch (endlich).

Ist F'/K' algebraische Erweiterung von F/K, so liegt jede Stelle $P' \in \mathbb{P}_{F'/K'}$ über genau einer Stelle $P = P' \cap F \in \mathbb{P}_{F/K}$, und über jeder Stelle $P \in \mathbb{P}_{F/K}$ liegt immer mindestens eine, höchstens aber endlich viele Stellen. Genaueres besagt folgender Satz [Deu73, Chapter IV, p. 97].

Satz 1.4. *Ist F'/K' eine algebraische Erweiterung von F/K und die Menge $\{P'_1, ..., P'_m\} \subseteq \mathbb{P}_{F'/K'}$ die Gesamtheit aller über der Stelle $P \in \mathbb{P}_{F/K}$ liegenden Stellen von $\mathbb{P}_{F'/K'}$, so gilt*

$$\sum_{i=1}^{m} e_i f_i = [F' : F],$$

wobei e_i und f_i die jeweiligen Verzweigungsindizes beziehungsweise Relativgrade der P'_i $(i = 1, ..., m)$ bezeichnen.

Norm und Conorm

Für eine Erweiterung F'/K' von F/K und einer Stelle $P \in \mathbb{P}_{F/K}$ bezeichnet $\mathrm{Con}_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P'$ die **Conorm** von P, wobei über alle $P' \in \mathbb{P}_{F'/K'}$ summiert wird, die über P liegen.

Die Conorm lässt sich zu einem additiven Homomorphismus von $\mathcal{D}_F$ nach $\mathcal{D}_{F'}$ fortsetzen durch $\mathrm{Con}_{F'/F}\left(\sum n_P \cdot P\right) := \sum n_P \cdot \mathrm{Con}_{F'/F}(P)$, und für den Funktionenkörperturm $F \subset F' \subset F''$, welcher aus sämtlich endlichen Erweiterungen besteht, gilt $\mathrm{Con}_{F''/F}(A) = \mathrm{Con}_{F''/F'}\left(\mathrm{Con}_{F'/F}(A)\right)$ mit $A \in \mathcal{D}_F$. Außerdem bildet die Conorm Hauptdivisoren auf Hauptdivisoren ab und lässt sich daher zu einem Homomorphismus $\mathcal{C}_F \longrightarrow \mathcal{C}_{F'}$ fortsetzen. Eine wichtige Aussage über das Verhalten des Grades eines Divisors beim Übergang in eine Erweiterung gibt uns folgender Satz und eine Folgerung aus [Deu73, Chapter IV, p. 106].

Satz 1.5. *Ist F'/K' eine Erweiterung von F/K, so existiert eine positive rationale Zahl $\lambda_{F'/F}$ so, dass für beliebiges $D \in \mathcal{D}_F$*

$$\deg_{F'/K'} \mathrm{Con}_{F'/F}(D) = \frac{\deg_{F/K} D}{\lambda_{F'/F}}$$

gilt. Ist F'/F endlich, so ist

$$\lambda_{F'/F} = \frac{[K' : K]}{[F' : F]}.$$

Sei F'/K' eine endliche Erweiterung von F/K und E/F die kleinste normale Erweiterung von F, welche F' enthält. Sei $G := G(E/F)$ die Galoisgruppe von E über F und $H \leq G$ die Untergruppe, die aus allen Automorphismen von E besteht die F' fix lassen. Für einen Divisor $D \in \mathcal{D}_{F'}$ ist dann die **Norm** über F durch

$$N_{F'/F}(D) = [F' : F]_i \cdot \sum_{\sigma \in G/H} \sigma(D)$$

definiert, wobei $[F' : F]_i$ den Inseparabilitätsgrad von F'/F bezeichnet. Die Norm ist ein additiver Homomorphismus zwischen den Klassengruppen $\mathcal{D}_{F'}$ und $\mathcal{D}_F$. Die wichtigsten Eigenschaften werden im folgendem Satz aufgezählt [Deu73, Chapter IV, p. 108/109].

Satz 1.6. *Sei F'/K' eine endliche Erweiterung von F/K. Dann gelten folgende Aussagen:*

(i) Liegt $P' \in \mathbb{P}_{F'/K'}$ über $P \in \mathbb{P}_{F/K}$, so gilt $N_{F'/F}(P') = f(P'|P)P$.

(ii) Ist $z \in F'$, so ist $N_{F'/F}((z)) = (N_{F'/F}(z))$, wobei auf der rechten Seite der Gleichung ein Hauptdivisor aus $\mathcal{D}_F$ steht.

(iii) Für $D \in \mathcal{D}_F$ gilt $N_{F'/F}(D) := N_{F'/F}(\mathrm{Con}_{F'/F}(D)) = [F' : F]D$.

(iv) Ist $F \subseteq F' \subseteq E$ ein Körperturm von Erweiterungen algebraischer Funktionenkörper, so gilt $N_{E/F}(D) = N_{F'/F}\left(N_{E/F'}(D)\right)$ für $D \in \mathcal{D}_E$.

(v) Für $D \in \mathcal{D}_{F'}$ ist $\deg_{F/K}\left(N_{F'/F}(D)\right) = [K' : K] \deg_{F'/K'}(D)$.

Konstantenkörpererweiterungen

Eine Erweiterung F'/K' von F/K heißt **Konstantenkörpererweiterung**, wenn F' das Kompositum von F und K' ist. Wir stellen uns folgende Frage: Wenn wir einen Funktionenkörper F/K und eine Erweiterung E von K gegeben haben, gibt es dann eine Konstantenkörpererweiterung F'/K' von F/K, so dass E und K' isomorph über K sind?

Dies ist nicht immer der Fall. Es gilt jedoch folgender Satz [Deu73, Chapter IV, p. 114].

Satz 1.7. *Sei F/K ein algebraischer Funktionenkörper und E eine Erweiterung von K. Dann existiert eine Erweiterung $\tilde{F}/\tilde{K}$ von F/K mit folgenden Eigenschaften:*

(i) Es existiert ein Teilkörper $\tilde{E}$ von $\tilde{K}$ mit $K \subseteq \tilde{E}$ und ein K-Isomorphismus $\lambda : \tilde{E} \longrightarrow E$.

(ii) Es gilt $\tilde{F} = F\tilde{E}$.

(iii) $\tilde{K}$ ist eine rein inseparable Erweiterung von $\tilde{E}$.

Ist F^*/K^* eine andere Erweiterung von F/K mit einem Teilkörper $\tilde{E}^* \subseteq K^*$ und einem K-Isomorphismus $\lambda^* : \tilde{E}^* \longrightarrow E$, und erfüllt diese die Bedingungen (i) und (ii), so gibt es einen K-Isomorphismus $\rho : F^* \longrightarrow F'$ so, dass

$$\rho_{|_{\tilde{E}^*}} = \lambda^{-1} \circ \lambda^*$$

gilt.

Seien nun F/K und E/K Funktionenkörper. Aus Satz 1.7 folgt, dass es bis auf Isomorphie eine Erweiterung F'/K' von F/K gibt, so dass $F' = FE$ mit K'/E algebraisch gilt, woraus $F' = FE = FK'$ folgt. Somit ist F'/K' eine Konstantenkörpererweiterung von F/K. Es stellt sich die Frage, wann der Fall $E = K'$ eintritt. Nach dem folgenden Satz aus [Deu73, Chapter IV, p. 124] ist dies der Fall, wenn F und K' linear disjunkt sind:

Satz 1.8. *Sei F/K Funktionenkörper und F'/K' eine Konstantenkörpererweiterung von F, d.h. $F' = FK'$. Ferner sei E/K eine Erweiterung von K mit $F' = FE$. Dann sind folgende Bedingungen äquivalent:*

(i) F und K' sind linear disjunkt über K.

(ii) Jeder über K endlich erzeugte Teilkörper $\tilde{E} \subseteq E$ ist bereits der volle Konstantenkörper von $F\tilde{E}$.

Sind obige Bedingungen erfüllt, so gilt (ii) für jeden (nicht notwendigerweise endlich erzeugten) Teilkörper $\tilde{E}$ von E, insbesondere für E selbst, d.h. also $K' = E$.

Für den Nachweis von $E = K'$ gibt es aber auch ein einfacheres Kriterium, um dieses festzustellen [Deu73, Chapter IV, p. 126].

Korollar 1.9. *Ist entweder F oder E separabel erzeugt über K, so gilt $K' = E$.*

Die in Satz 1.5 eingeführte Konstante $\lambda_{F'/F}$ für eine Erweiterung F'/K' von F/K hat nun folgende Bedeutung [Deu73, Chapter IV, p. 126].

Satz 1.10. *Sei F/K Funktionenkörper und F'/K' eine Konstantenkörpererweiterung von F sowie E ein Körper mit $E \subseteq K'$ und $F' = FE$. Ferner sei $\lambda_{F'/F}$ die positive rationale Konstante mit*

$$\lambda_{F'/F} \deg_{F'/K'}(\mathrm{Con}_{F'/F}(D)) = \deg_{F/K}(D)$$

für einen beliebigen Divisor $D \in \mathcal{D}_F$. Dann ist $\lambda_{F'/F}$ eine Potenz der Charakteristik von K mit nicht-negativem Exponenten im Falle $\mathrm{char}(K) > 0$. Ansonsten gilt $\lambda_{F'/F} = 1$. Es ist $\lambda_{F'/F} = 1$ genau dann, wenn F und K' linear disjunkt über K sind.

Der verallgemeinerte Differentensatz

Sämtliche Aussagen in diesem Abschnitt sind aus [Deu73] und [Sal06] entnommen. Da in dieser Arbeit oftmals Funktionenkörper betrachtet werden, welche einen nicht-vollkommenen Konstantenkörper besitzen, benötigen wir eine Verallgemeinerung des Differenten- und Diskriminantenbegriffs wie wir ihn zum Beispiel aus [Sti93] kennen. Folgender Satz aus [Sal06, Theorem 5.6.1, p. 148] liefert eine Grundlage für diese Definition.

Satz 1.11. *Sei F'/K' eine endliche separable Erweiterung eines Funktionenkörpers F/K, $P' \in \mathbb{P}_{F'/K'}$ und $P \in \mathbb{P}_{F/K}$ mit $P'|P$. Dann existiert eine ganze Zahl $m \geq 0$ so, dass wenn $x \in F_{P'}$ der Bedingung $v_{P'}(x) \geq -m$ genügt, dann $v_P\left(\mathrm{Tr}_{F_{P'}/F_P}(x)\right) \geq 0$ gilt. Genauso existiert ein $x_0 \in F_{P'}$ mit $v_{P'}(x_0) < -m$ und $v_P\left(\mathrm{Tr}_{F_{P'}/F_P}(x_0)\right) < 0$.*

Sei F'/K' eine endlich separable Erweiterung eines Funktionenkörpers F/K, $P' \in \mathbb{P}_{F'/K'}$ und $P \in \mathbb{P}_{F/K}$ mit $P'|P$. Die maximale positive ganze Zahl, die den Bedingungen von Satz 1.11 genügt, bezeichnen wir mit $m(P)$ und nennen sie den **Differentialexponenten** von P' bezüglich F. Nun können wir die Verallgemeinerung des Dedekindschen Differentensatzes formulieren [Sal06, Theorem 5.6.3, p. 148]:

Satz 1.12. *Sei F'/K' eine endlich separable Erweiterung des Funktionenkörpers F/K, $P' \in \mathbb{P}_{F'/K'}$ und $P \in \mathbb{P}_{F/K}$ mit $P'|P$. Dann gilt stets*

$$m(P') \geq e(P'|P) - 1. \tag{1.1}$$

Außerdem ist

$$m(P') > e(P'|P) - 1 \tag{1.2}$$

genau dann, wenn mindestens eine der beiden Bedingungen erfüllt ist:

(i) $e(P'|P)$ *ist durch* $\mathrm{char}(K)$ *teilbar*

(ii) $F_{P'}$ *ist inseparabel über* F_P*.*

Für fast alle Stellen $P' \in \mathbb{P}_{F'/K'}$ ist $m(P') = 0$. Die Summe aller Stellen P' mit Exponenten $m(P')$ liefert daher einen Divisor, die sogenannte Differente:

Definition 1.13. *Sei F'/K' eine endlich separable Erweiterung eines Funktionenkörpers F/K. Den Divisor*

$$\mathrm{Diff}(F'/F) := \sum_{P' \in \mathbb{P}_{F'/K'}} m(P')P'$$

wollen wir ***Differente*** *von F'/F und dessen Norm*

$$\mathrm{disc}(F'/F) := N_{F'/F}\left(\mathrm{Diff}(F'/F)\right)$$

die ***Diskriminante*** *von F'/F nennen. Seien $P' \in \mathbb{P}_{F'/K'}$ und $P \in \mathbb{P}_{F/K}$ Stellen mit $P'|P$. Die Stelle P' heißt* ***unverzweigt****, wenn $e(P'|P) = 1$ ist, andernfalls heißt P'* ***verzweigt****. Die Stelle P' heißt* ***total verzweigt*** *in F'/F, wenn $e(P'|P) = [F' : F]$ gilt. Die Stelle P' heißt* ***relativ inseparabel****, wenn ${F'}_{P'}/F_P$ inseparabel ist.*

In Körpertürmen erfüllt die Differente folgende Eigenschaft [Sal06, Theorem 5.7.15, p.157].

Korollar 1.14. *Für einen Körperturm $F \subseteq F' \subseteq F''$ von endlichen und separablen Funktionenkörpererweiterungen gilt*

$$\mathrm{Diff}(F''/F) = \mathrm{Con}_{F''/F'}(\mathrm{Diff}(F'/F)) + \mathrm{Diff}(F''/F').$$

Einen wichtigen Zusammenhang zwischen Geschlecht und Differente gibt folgender Satz, die sogenannte **Riemann-Hurwitzsche Geschlechtsformel** [Sal06, Korollar 9.4.3, p. 309]. Sie gilt auch für Körper mit nichtvollkommenem Konstantenkörper.

Satz 1.15. *Sei F'/K' eine endliche separable Erweiterung des Funktionenkörpers F/K. Dann gilt*

$$g_{F'/K'} = 1 + \frac{[F' : F]}{[K' : K]}(g_{F/K} - 1) + \frac{1}{2}\deg_{F'/K'} \mathrm{Diff}(F'/F).$$

Verhalten von Geschlecht, Dimension und Differente

Sei F'/K' eine Konstantenkörpererweiterung des Funktionenkörpers F/K. Wir wollen Aussagen über das Verhalten des Geschlechts von F'/K', seiner Differente und der Dimensionen des Riemann-Roch-Raumes $\mathcal{L}(D)$ eines Divisors $D \in \mathcal{D}_F$ machen. Dazu zitieren wir folgenden Satz aus [Deu73, Chapter IV, p. 132].

Satz 1.16. *Sei F'/K' eine Konstantenkörpererweiterung des Funktionenkörpers F/K mit $\lambda_{F'/F} = 1$, was nach Satz 1.10 gleichbedeutend damit ist, dass K' und F linear disjunkt über K sind. Dann gelten folgende Aussagen:*

(i) Für die Geschlechter besteht die Ungleichung $g_{F'/K'} \leq g_{F/K}$.

(ii) Ist $D \in \mathcal{D}_F$ ein beliebiger Divisor, so lässt sich die K-Basis von $\mathcal{L}(D)$ zu einer K'-Basis von $\mathcal{L}(\mathrm{Con}_{F'/F}(D))$ ergänzen, und somit gilt

$$\dim D \leq \dim \mathrm{Con}_{F'/F}(D).$$

Ist K' separabel erzeugt über K, so ist jede K-Basis des Riemann-Roch-Raumes $\mathcal{L}(D)$ eine K'-Basis des Riemann-Roch-Raumes $\mathcal{L}(\mathrm{Con}_{F'/F}(D))$ und die Geschlechter von F'/K' und F/K sind identisch. Insbesondere ist dann

$$\dim D = \dim \mathrm{Con}_{F'/F}(D).$$

Es gilt aber auch die Umkehrung [Deu73, Chapter IV, p.144].

Satz 1.17. *Seien F'/K' eine Konstantenkörpererweiterung des Funktionenkörpers F/K und $D \in \mathcal{D}_F$ beliebig. Ist $g_{F'/K'} = g_{F/K}$ und $\lambda_{F'/F} = 1$, so ist jede K-Basis des Riemann-Roch-Raumes $\mathcal{L}(D)$ eine K'-Basis des Riemann-Roch-Raumes $\mathcal{L}(\mathrm{Con}_{F'/F}(D))$. Insbesondere gilt*

$$\dim D = \dim \mathrm{Con}_{F'/F}(D).$$

Wir wollen jetzt Überlegungen anstellen, welche Gestalt die Differente von Konstantenkörpererweiterungen hat. Dazu betrachten wir zwei separabel und endlich erzeugte Funktionenkörper F_1/K und F_2/K, welche **algebraisch unabhängig** über K sind. Das Kompositum F_1F_2 über F_2 in einem geeigneten gemeinsamen Oberkörper bezeichnen wir mit L. Wir wollen nun zeigen, dass dann F_2 der genaue Konstantenkörper von L ist, was insbesondere bedeutet, dass wir L dann als Konstantenkörpererweiterung von F_1/K auffassen können.

Lemma 1.18. *Seien F_1/K und F_2/K jeweils zwei endlich erzeugte, separable und algebraisch unabhängige Funktionenkörper. Ferner sei $L := F_1F_2$ das Kompositum von F_1 und F_2 in einem geeignetem Oberkörper und es gelte $F_2 \subseteq K'$, wobei K' den genauen Konstantenkörper von L bezeichne. Dann gelten:*

(i) F_2 *ist genauer Konstantenkörper von* L*, d.h. es gilt* $K' = F_2$*.*

(ii) Die Geschlechter g_{L/F_2} *und* $g_{F_1/K}$ *stimmen überein.*

(iii) Die Körpergrade $[L : F_2(x_1)]$ *und* $[F_1 : K(x_1)]$ *stimmen überein. Ist außerdem* $F_1 = K(x_1, y_1)$*, so gilt* $L = F_2(x_1, y_1)$*.*

(iv) Für die Differente gilt $\mathrm{Diff}(L/F_2) = \mathrm{Con}_{L/F_1}(\mathrm{Diff}(F_1/K))$*.*

(v) Für $P' \in \mathbb{P}_{L/F_2}$ *und* $P \in \mathbb{P}_{F_1/K}$ *mit* $P'|P$ *gilt* $F_{P'} = F_P F_2$*, d.h.* $F_{P'}$ *ist das Kompositum von* F_P *und* F_2*.*

Beweis. Die Aussage (i) folgt aus Korollar 1.9, da nach Voraussetzung F_2/K separabel erzeugt ist. Andererseits gilt die lineare Disjunktheit von F_1 und F_2 über K wegen der algebraischen Unabhängigkeit und Regularität von F_1 und F_2. Damit folgt $\lambda_{L/F_1} = 1$ aus Satz 1.10 und Aussage (ii) mit Satz 1.16 auf Grund der Separabilität von F_1 und F_2. Aus der linearen Disjunktheit von F_1 und $F_2(x_1)$ über $K(x_1)$ und der Endlichkeit von $F_1/K(x_1)$ folgt, dass $[L : F_2(x_1)] = [F_1 : K(x_1)]$ ist. Daraus erhalten wir $L = F_2(x_1, y_1)$, weil das Minimalpolynom von y_1 über $K(x_1)$ auf Grund der algebraischen Unabhängigkeit von F_1 und F_2 über $F_2(x_1)$ irreduzibel bleibt. Für den Beweis der Aussage (iv) bemerken wir, dass eine Stelle $P \in \mathbb{P}_{F_1/K}$, die in F_1/K verzweigt ist, auch in L/F_2 verzweigt ist, d.h. wir haben

$$\mathrm{Con}_{L/F_1}(\mathrm{Diff}(F_1/K)) \leq \mathrm{Diff}(L/F_2). \tag{1.3}$$

Betrachten wir die Erweiterungen $L/F_2(x_1)$ vom Grad $[L : F_2(x_1)] = n$ und setzen in der Situation von Satz 1.15 $F' = L,\ F = F_2(x_1)$ und $K = F_2 = K'$, so erhalten wir einmal

$$g_{L/F_2} = 1 + \frac{[L : F_2(x_1)]}{[F_2 : F_2]}(g_{F_2(x_1)/F_2} - 1) + \frac{1}{2}\deg_{L/F_2(x_1)} \mathrm{Diff}(L/F_2). \tag{1.4}$$

Mit $F' = F_1$, $F = K(x_1)$ und $K' = K$ erhalten wir ebenso

$$g_{F_1/K} = 1 + \frac{[F_1 : K(x_1)]}{[K : K]}(g_{K(x_1)/K} - 1) + \frac{1}{2}\deg_{F_1/K(x_1)} \mathrm{Diff}(F_1/K). \tag{1.5}$$

Mit den Gleichungen (1.4) und (1.5) sowie

$$g_{L/F_2} = g_{F_1/K}, \quad [L : F_2(x_1)] = [F_1 : K(x_1)] \text{ und } \lambda_{L/F_1} = 1$$

folgt dann mit Satz 1.5

$$\deg_{L/F_2} \mathrm{Diff}(L/F_2)) = \deg_{L/F_2}(\mathrm{Con}_{L/F_1}(\mathrm{Diff}(F_1/K))\,.$$

Da die Differente ein effektiver Divisor ist, folgt aus (1.3) die Gleichheit

$$\mathrm{Diff}(L/F_2(x_1)) = \mathrm{Con}_{L/F_1}(\mathrm{Diff}(F_1/K(x_1)))\,.$$

Die Aussage (v) folgt aus [Deu73, Chapter IV, p.128]. □

1.3 Ringe und Algebren

Sämtliche Aussagen in diesem Abschnitt stützen sich auf [Mil05], [Poh89] oder [Hes06], wenn diese nicht bewiesen werden. Die in diesem Kapitel behandelten Ringe sind, wenn nichts Anderes gesagt wird, Integritätsringe. Sei F/K ein separabler Funktionenkörper. Wie fixieren eine Erzeugung $F = K(x, y)$ und definieren die zwei Ringe

$$\mathcal{O}_F := \mathrm{Cl}(K[x], F) = \bigcap_{v_P(x)\geq 0} \mathcal{O}_P$$

und

$$\mathcal{O}_{F,\infty} := \mathrm{Cl}(K[x^{-1}], F) = \bigcap_{v_P(x)\leq 0} \mathcal{O}_P$$

mit $P \in \mathbb{P}_{F/K}$. Hier soll $\mathrm{Cl}(K[x], F)$ bzw. $\mathrm{Cl}(K[x^{-1}], F)$ den ganzalgebraischen Abschluss von $K[x]$ bzw. $K[x^{-1}]$ in F bezeichnen. Unsere Definition von $\mathcal{O}_F$ und $\mathcal{O}_{F,\infty}$ sind also abhängig von der gewählten Erzeugung von F/K. Um die Notation so einfach wie möglich zu halten, haben wir eine fixierte Erzeugung von F/K vorausgesetzt. Die Ringe $\mathcal{O}_F$ und $\mathcal{O}_{F,\infty}$ sind Dedekindringe, welche als endlich erzeugte $K[x]$- bzw. $K[x^{-1}]$-Moduln eine Ganzheitsbasis besitzen. Wir wollen $\mathcal{O}_F$ die **endliche Maximalordnung** und $\mathcal{O}_{F,\infty}$ die **unendliche Maximalordnung** nennen. Die Differente von $\mathcal{O}_F$ ist dann durch

$$\mathrm{Diff}(\mathcal{O}_F) := \sum_{\nu_P(x)\geq 0} \nu_P(\mathrm{Diff}(F/K(x)))P$$

und die Diskriminante durch

$$\mathrm{disc}(\mathcal{O}_F) := N_{F/K}(\mathrm{Diff}(\mathcal{O}_F))$$

definiert. Analog machen wir diese Definition für die unendliche Maximalordnung. Für eine Stelle $P \in \mathbb{P}_{F/K}$ mit $v_P(x) \geq 0$ betrachten wir die Einbettung

$$\iota_P : \mathcal{O}_F \longrightarrow \mathcal{O}_P \tag{1.6}$$

und für eine Stelle $P \in \mathbb{P}_{F/K}$ mit $v_P(x) \leq 0$ die Einbettung

$$\iota_{P,\infty} : \mathcal{O}_{F,\infty} \longrightarrow \mathcal{O}_P. \tag{1.7}$$

Bei Stellen P mit $v_P(x) = 0$ können wir sowohl $\mathcal{O}_F$ als auch $\mathcal{O}_{F,\infty}$ in die Stellenringe $\mathcal{O}_P$ einbetten. Die Anzahl der Stellen mit $v_P(x) > 0$ bzw. $v_P(x) < 0$ ist endlich. Durch die Urbilder der Inklusionen werden die maximalen Ideale der Bewertungsringe $\mathcal{O}_P$ auf Primideale der jeweiligen Dedekindringe abgebildet. Jedes gebrochene Ideal von $\mathcal{O}_F$ oder $\mathcal{O}_{F,\infty}$ lässt sich bis auf Reihenfolge eindeutig als Produkt von Primidealen darstellen. Die jeweiligen Idealgruppen wollen wir mit $\mathfrak{I}_{\mathcal{O}_F}$ und $\mathfrak{I}_{\mathcal{O}_{F,\infty}}$ bezeichnen.

Einem Divisor $D = \sum_{i=1}^{n} n_i P_i \in \mathcal{D}_{F/K}$ können wir einen **endlichen** Teil

$$D_0 := \prod_{v_{P_i}(x) \geq 0} \iota_{P_i}^{-1}(P_i)^{n_i} \in \mathfrak{I}_{\mathcal{O}_F} \tag{1.8}$$

und einen **unendlichen** Teil

$$D_\infty := \prod_{v_{P_i}(x) \leq 0} \iota_{P_i,\infty}^{-1}(P_i)^{n_i} \in \mathfrak{I}_{\mathcal{O}_{F,\infty}} \tag{1.9}$$

zuordnen. Jeder Divisor besitzt dann eine Darstellung mit Idealen aus dem endlichen und unendlichen Teil. Definieren wir den unendlichen Teil von D wie folgt zu

$$D^\infty := \prod_{v_{P_i}(x_1) < 0} \iota_{P_i,\infty}^{-1}(P_i)^{n_i} \in \mathfrak{I}_{\mathcal{O}_{F,\infty}} \ , \tag{1.10}$$

so lässt sich dann jeder Divisor D durch D_0 und D^∞ eindeutig darstellen. Den Restklassenkörper $\mathcal{O}_F/P_0$ eines Primideales $P_0 = \iota_P^{-1}(P) \in \mathcal{O}_F$ wollen wir mit F_P bezeichnen. Der Körper K lässt sich in F_P einbetten und der **Grad eines Primideals** $P_0 = \iota_P^{-1}(P) \in \mathcal{O}_F$ ist durch

$$\deg_{F/K} P_0 = [F_P : K]$$

gegeben. Analoges erhalten wir für $\mathcal{O}_{F,\infty}$. Ein beliebiges Ideal eines Dedekindringes lässt sich dann in Primidealpotenzen faktorisieren, und der Grad eines Ideals wird ähnlich wie bei Divisoren als Summe der Grade aller beteiligten Primideale mit Vielfachheit definiert. Der Conorm für Divisoren entspricht die Hochhebung des entsprechenden endlichen und unendlichen Teils in den jeweiligen Dedekindringen.

Als Nächstes wollen wir den Fall betrachten, dass F_1/K und F_2/K zwei separable und algebraisch unabhängige Funktionenkörper mit Kompositum $L := F_1F_2$ über dem genauen Konstantenkörper F_2 sind. Wir wollen uns mit der Frage beschäftigen, wie jeweils die endliche und unendliche Maximalordnung von L/F_2 beschaffen ist.

Lemma 1.19. *Seien $F_1 = K(x_1, y_1)$ und $F_2 = K(x_2, y_2)$ zwei separable und algebraisch unabhängige Funktionenkörper. Ferner sei $L = F_2(x_1, y_1)$ ein Funktionenkörper mit genauem Konstantenkörper F_2.*

(i) Sei $\mathcal{O}_{F_1}$ aufgefasst als $K[x_1]$-Modul $\langle b_1, ..., b_n \rangle_{K[x_1]}$. Für die endliche Maximalordung $\mathcal{O}_{L/F_2}$ gilt dann

$$\mathcal{O}_{L/F_2} = \langle b_1, ..., b_n \rangle_{F_2[x_1]}.$$

(ii) Die Abbildung

$$\Phi : \mathcal{O}_{F_1} \otimes_K F_2 \longrightarrow \mathcal{O}_{L/F_2}, \quad a \otimes b \longmapsto ab$$

ist ein K-Algebrenisomorphismus.

(iii) Sei $U := K[x_1]^\times$. *Der Ring*

$$\mathcal{O}_{L/F_2}\big[U^{-1}\big]$$

ist wieder ein Dedekindring und die Abbildung

$$\hat{\Phi} : F_1 \otimes_K F_2 \longrightarrow \mathcal{O}_{L/F_2}\big[U^{-1}\big], \quad a \otimes b \longmapsto ab \tag{1.11}$$

ein K*-Algebrenisomorphismus.*

(iv) Sei Φ *wie in (ii) und* $U := \Phi^{-1}(K[x_1])$. *Dann lässt sich* $\mathcal{O}_{F_1} \otimes_K F_2$ *mittels der Abbildung*

$$\iota_U : \mathcal{O}_{F_1} \otimes_K F_2 \longrightarrow F_1 \otimes_K F_2, \quad \alpha \longmapsto \frac{\alpha}{1}$$

in $F_1 \otimes_K F_2$ *einbetten. Ist* P *Primideal in* $F_1 \otimes_K F_2$, *so ist das Urbild bezüglich dieser Einbettung ebenfalls ein Primideal.*

(v) Es gilt $\big(F_1 \otimes_K F_2\big)/P \cong \big(\mathcal{O}_{F_1} \otimes_K F_2\big)/P^*$, *wobei* P *ein Primideal von* $F_1 \otimes_K F_2$ *und* P^* *das Urbild von* P *bezüglich der Einbettung ist.*

(vi) Sei P *Primideal von* $F_1 \otimes_K F_2$. *Dann lassen sich* F_1 *und* F_2 *in die* K*-Algebra* $F_1 \otimes F_2$ *und in den Restklassenring* $\big(F_1 \otimes_K F_2\big)/P$ *einbetten.*

(vii) Sämtliche Aussagen dieses Lemmas gelten auch, wenn man $\mathcal{O}_{F_1}$ *durch* $\mathcal{O}_{F_{1,\infty}}$ *und* $\mathcal{O}_{L/F_2}$ *durch* $\mathcal{O}_{L/F_{2,\infty}}$ *ersetzt. Analog gelten sämtliche Aussagen, wenn wir* L *als eine Konstantenkörpererweiterung von* F_2 *betrachten.*

Beweis. (i) Sei $b_1, ..., b_n \in F_1$ eine Basis des $K[x_1]$-Moduls $\mathcal{O}_{F_1}$ und $R := \langle b_1, ..., b_n \rangle_{F_2[x_1]}$ der von $b_1, ..., b_n$ erzeugte $F_2[x_1]$-Modul. Da F_1/K und F_2/K algebraisch unabhängig und jeweils regulär sind, bilden die Elemente $b_1, ..., b_n$ eine $F_2[x_1]$-Basis von R und es ist $\operatorname{disc}(\mathcal{O}_{F_1}) = \operatorname{disc}(R)$. Aus Lemma 1.18 folgt

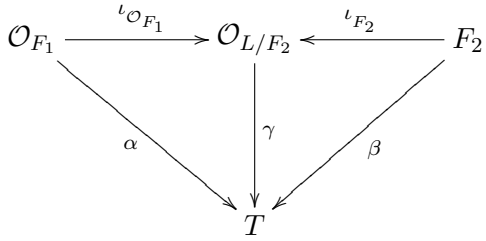
$$\operatorname{Diff}(L/F_2) = \operatorname{Con}_{L/F_1}(\operatorname{Diff}(F_1/K))$$

und damit die Gleichheit

$$\operatorname{disc}(L/F_2) = \operatorname{disc}(F_1/K)$$

von Divisoren von $F_2(x_1)$. Das Polynom $f := \operatorname{disc}(\mathcal{O}_{F_1})$ teilt dann das Polynom $F := \operatorname{disc}(\mathcal{O}_{L/F_2})$ in $F_2[x_1]$. Da $\deg(f) = \deg(F)$ gilt, haben wir $F = uf$ mit $u \in F_2$ geeignet. Somit unterscheidet sich die Übergangsmatrix vom $F_2[x_1]$-Modul $\mathcal{O}_{L/F_2}$ zu R nur um eine Einheit in $\mathcal{O}_{L/F_2}$, und die Basis von R ist auch eine Basis von $\mathcal{O}_{L/F_2}$. Daraus folgt dann $\mathcal{O}_{L/F_2} = R$ als $F_2[x_1]$-Moduln.

(ii) Sei T eine K-Algebra. Wir betrachten folgendes Diagramm, in dem nur K-Algebrenhomomorphismen auftauchen:



(1.12)

Hierbei sind $\iota_{\mathcal{O}_{F_1}}$ und ι_{F_2} jeweils Einbettungen. Es ist nicht schwer nachzuweisen, dass γ durch α und β eindeutig festgelegt ist, wobei $\gamma \circ \iota_{\mathcal{O}_{F_1}} = \alpha$ und $\gamma \circ \iota_{F_2} = \beta$ ist. Auf Grund der universellen Eigenschaft des Tensorproduktes gibt es einen K-Algebrenisomorphismus

$$\Phi : \mathcal{O}_{F_1} \otimes_K F_2 \longrightarrow \mathcal{O}_{L/F_2}$$

mit den gewünschten Eigenschaften.

(iii) Dass $\mathcal{O}_{L/K_2}[U^{-1}]$ wieder ein Dedekindring ist, folgt aus der Tatsache, dass die Lokalisierung eines Dedekindringes wieder ein Dedekindring ist. Die Lokalisierung einer K-Algebra ist ebenfalls wieder eine K-Algebra. Ersetzen wir im Diagramm (1.12) den Ring $\mathcal{O}_{F_1}$ durch F_1 und den Ring $\mathcal{O}_{L/F_2}$ durch $\mathcal{O}_{L/F_2}[U^{-1}]$, so folgt wie in (ii) aus der universellen Eigenschaft des Tensorproduktes, dass die Abbildung

$$\hat{\Phi} : F_1 \otimes_K F_2 \longrightarrow \mathcal{O}_{L/F_2}[U^{-1}], \quad a \otimes b \longmapsto ab$$

ein K-Algebrenisomorphismus ist.

(iv) Mit

$$\iota_U : \mathcal{O}_{F_1} \otimes_K F_2 \longrightarrow F_1 \otimes_K F_2, \quad \alpha \longmapsto \frac{\alpha}{1}$$

erhalten wir die gesuchte Einbettung. Dass $\iota_U^{-1}(P)$ ein Primideal in $\mathcal{O}_{F_1} \otimes_K F_2$ ist, ist klar.

(v) Sei $U := K[x_1]^\times \otimes_K 1$ und bezeichne

$$\pi_{P^*} : \mathcal{O}_{F_1} \otimes_K F_2 \longrightarrow (\mathcal{O}_{F_1} \otimes_K F_2)/P^*$$

die kanonische Restklassenabbildung. Wir erhalten

$$\pi_{P^*}(U) \subseteq ((\mathcal{O}_{F_1} \otimes_K F_2)/P^*)\,[\pi_{P^*}(U)^{-1}]^\times\,,$$

und da wir die Reihenfolge von Lokalisierung und Faktorisierung vertauschen dürfen, folgt mit (iii):

$$((\mathcal{O}_{F_1} \otimes_K F_2)/P^*)\,[\pi_{P^*}(U)^{-1}] \cong (F_1 \otimes_K F_2)/P.$$

Da $P^* = \iota_U^{-1}(P)$ und $P \cap \iota_U(U) = 0$ gilt, erhalten wir sogar

$$\pi_{P^*}(U) \subseteq ((\mathcal{O}_{F_1} \otimes_K F_2)/P^*)^\times \ ,$$

woraus mit der universellen Eigenschaft für Lokalisierungen die Isomorphie

$$(F_1 \otimes_K F_2)/P \cong (\mathcal{O}_{F_1} \otimes_K F_2)/P^*$$

folgt.

(vi) Mit $\iota_{F_1} : F_1 \longrightarrow F_1 \otimes_K F_2, \quad \alpha \longmapsto \alpha \otimes_K 1$ erhalten wir eine Einbettung für F_1 und analog für F_2 eine Einbettung ι_{F_2}. Da die eingebetteten Elemente aus F_1 und F_2 in $F_1 \otimes_K F_2$ Einheiten sind, gilt mit der Restklassenabbildung $\pi : F_1 \otimes_K F_2 \longrightarrow \big(F_1 \otimes_K F_2\big)/P$, dass $\pi \circ \iota_{F_i}$ eingeschränkt auf F_i eine Injektion ist $(i = 1, 2)$.

(vii) Diese Aussage ergibt sich aus der Tatsache, dass sämtliche Argumentationsketten der vorangegangenen Beweise sich ohne weiteres auf diese Fälle übertragen lassen.

□

Den Funktionenkörper L/F_2 können wir einmal als algebraische Erweiterung des rationalen Funktionenkörpers $F_2(x_1)$ oder als Konstantenerweiterung von F_1/K zu L/F_2 betrachten. Im ersten Fall gibt es nur konstante Stellen, und im zweiten sind genau die Stellen $P' \in \mathbb{P}_{L/F_2}$ konstant, für die ein $P \in \mathbb{P}_{F_1/K}$ mit $P'|P$ existiert. **Wenn wir im Folgenden von konstanten Stellen von L/F_2 sprechen, so meinen wir immer konstant in Bezug auf die Konstantenkörpererweiterung L/F_2 von F_1/K.** Konstante Divisoren sind dann solche, deren Träger nur aus konstanten Primdivisoren bestehen. Die Gesamtheit aller konstanten Divisoren von $\mathcal{D}_{L/F_2}$ bildet eine Untergruppe $C_{L/F_2} \leq \mathcal{D}_{L/F_2}$.

Mit $\mathscr{P}_R$ wollen wir die Menge aller Primideale eines Ringes R bezeichnen. Sei ι_P die Einbettung von (1.6). Ein Primideal $P_0 \in \mathscr{P}_{\mathcal{O}_{L/F_2}}$ heißt **konstant**, wenn es ein $P \in \mathbb{P}_{L/F_2}$ gibt, so dass für das Urbild $\iota_P(P)^{-1} = P_0$ gilt und P konstant ist. Ein gebrochenes Ideal $I \in \mathfrak{I}_{\mathcal{O}_{L/F_2}}$, das aus lauter konstanten Primidealen besteht, wollen wir **konstantes Ideal** nennen und deren Gesamtheit mit $\mathscr{C}_{\mathcal{O}_{L/F_2}}$ bezeichnen. Für ein nicht-konstantes Primideal P_0 aus $\mathcal{O}_{L/F_2}$ werden wir eine besondere Darstellung benutzen, die sogenannte **Zwei-Element-Darstellung**. Das ist diejenige Gestalt eines Primideales, die man gewinnt, wenn man den Kummerschen Zerlegungssatz anwenden kann, um die Hochhebung eines nicht-konstanten Primpolynomes aus $F_2[x_1]$ nach $\mathcal{O}_{L/F_2}$ zu berechnen. Da die nicht-konstanten Primdivisoren $P \in \mathcal{D}_{L/F_2}$ keine Differententeiler sind, können wir nicht-konstante Ideale stets in der Zwei-Element-Darstellung angeben.

Seien nun $S := \mathcal{O}_{L/F_2}\left[K[x_1]^{-1}\right]$ und $\iota : \mathcal{O}_{L/F_2} \longrightarrow S$ die Einbettung von $\mathcal{O}_{L/F_2}$ in S. Wir betrachten die Abbildung

$$\Psi : \mathscr{P}_{\mathcal{O}_{L/F_2}} \longrightarrow \mathscr{P}_S, \quad P_0 \longmapsto \iota(P_0).$$

Bezeichnet $P_0 := \iota^{-1}(\hat{P}_0)$ das Urbildideal von $\hat{P}_0 \in \mathscr{P}_S$, so definieren wir

$$A := \{P \in \mathbb{P}_{L/F_2} \mid \exists \hat{P}_0 \in S \text{ mit } P_0 = \iota^{-1}(\hat{P}_0)\}$$

und bezeichnen mit H_{L/F_2} die von den Primdivisoren von A erzeugte freie abelsche Untergruppe von $\mathcal{D}_{L/F_2}$. Wir können nun die Divisoren von $\mathcal{D}_{L/F_2}$ eindeutig durch einen konstanten und nicht-konstanten Divisor beschreiben:

Lemma 1.20. *Jeder Divisor $D \in \mathcal{D}_{L/F_2}$ lässt sich eindeutig schreiben als $D = D_H + D_C$ mit einem konstanten Divisor $D_C \in C_{L/F_2}$ und einem Divisor $D_H \in H_{L/F_2}$ ohne konstanten Träger, d.h. es gilt $\mathcal{D}_{L/F_2} = C_{L/F_2} \oplus H_{L/F_2}$.*

Beweis. Wir betrachten die Abbildungen $\beta : \mathcal{D}_{L/F_2} \longrightarrow H_{L/F_2}, \quad D \longmapsto D_H$ mit $D_{H_0} = \iota^{-1}(\iota(D_0))$ und $\alpha : C_{L/F_2} \longrightarrow \mathcal{D}_{L/F_2}, \quad D \longmapsto D$ sowie die kurze exakte Sequenz

$$0 \longrightarrow C_{L/F_2} \xrightarrow{\alpha} \mathcal{D}_{L/F_2} \xrightarrow{\beta} H_{L/F_2} \longrightarrow 0\,. \tag{1.13}$$

Mit $\tau : H_{L/F_2} \longrightarrow \mathcal{D}_{L/F_2}$, $D \longmapsto D$ erhalten wir $\beta\tau = \mathrm{id}_{H_{L/F_2}}$, woraus die Behauptung folgt. □

Wir betrachten nun den K-Isomorphismus $\tau : F_1 \longrightarrow F_3$ von separablen Funktionenkörpern $F_i = K(x_i, y_i)$ mit genauem Konstantenkörper K $(i = 1, 2, 3)$. Ferner seien die Funktionenkörper F_1, F_2 und F_3 paarweise algebraisch unabhängig und $U_i := K[x_i]^{\times}$. Mit $\hat{\Phi}_{12}$ und $\hat{\Phi}_{23}$ bezeichnen wir die jeweiligen Algebrenisomorphismen

$$\hat{\Phi}_{12} : F_1 \otimes_K F_2 \longrightarrow \mathcal{O}_{F_1F_2/F_2}[U_1^{-1}]$$

und

$$\hat{\Phi}_{23} : F_3 \otimes_K F_2 \longrightarrow \mathcal{O}_{F_3F_2/F_2}[U_3^{-1}]$$

wie in Lemma 1.19. Außerdem benötigen wir noch den Algebrenisomorphismus

$$\alpha : F_1 \otimes_K F_2 \longrightarrow F_3 \otimes_K F_2, \quad a \otimes b \longmapsto \tau(a) \otimes b.$$

Ist nun $P \in \mathbb{P}_{L/F_2}$, so definieren wir

$$Q_0 := \hat{\Phi}_{23}\left(\alpha\left(\hat{\Phi}_{12}^{-1}(\iota_P^{-1}(P))\right)\right)$$

und

$$\tau(P) := \iota_Q(Q_0), \tag{1.14}$$

wobei Q_0 ein Primideal in $\mathcal{O}_{F_2F_3/F_2}[U_3^{-1}]$ ist. Mit Q bezeichnen wir dann denjenigen Primdivisor in $\mathbb{P}_{F_2F_3/F_2}$ mit $Q_0 = \iota_Q^{-1}(Q)$, wobei hier

$$\iota_Q : \mathcal{O}_{F_2F_3/F_2}[U_3^{-1}] \longrightarrow \mathcal{O}_Q$$

die Einbettung von $\mathcal{O}_{F_2F_3/F_2}[U_3^{-1}]$ in den Bewertungsring $\mathcal{O}_Q$ von F_2F_3/F_2 ist. Diese Vorschrift setzen wir dann auf $\mathcal{D}_{L/F_2}$ fort und erhalten einen Isomorphismus von $\mathcal{D}_{L/F_2}$ nach $\mathcal{D}_{F_2F_3/F_2}$, d.h. also insbesondere $\tau(A) \in \mathcal{D}_{F_2F_3/F_2}$ für $A \in \mathcal{D}_{L/F_2}$. Im Falle eines Isomorphismus $\tau : F_2 \longrightarrow F_3$ gehen wir völlig analog vor, wobei hier dann $\tau(A) \in \mathcal{D}_{F_3F_1/F_3}$ für $A \in \mathcal{D}_{L/F_2}$ ist.

1.4 Abelsche Varietäten über endlichen Körpern

In diesem Abschnitt wollen wir eine Übersicht über die Theorie der abelschen Varietäten geben. Dazu halten wir uns an [Mil98], [Mil86], [Har77], [Eic63], [Mum70] und [Oor07]. Da für uns die abelschen Varietäten über endlichen Körpern oder deren algebraischer Abschluss von Hauptinteresse sind, wollen wir mit k immer einen endlichen Körper und mit $\overline{k}$ seinen algebraischen Abschluss bezeichnen.

Als **Gruppen-Varietät** über k bezeichnen wir eine Varietät über k, deren Punkte eine Gruppe bilden und deren Gruppenoperationen k-Morphismen sind. Eine **Abelsche Varietät** ist eine projektive Gruppen-Varietät. Da die Gruppenstruktur einer abelschen Varietät abelsch ist, werden wir diese immer additiv schreiben. Ein Homomorphismus zwischen abelschen Varietäten über k ist ein Morphismus, der ein Homomorphismus von abelschen Gruppen ist. Ist $\alpha : A \longrightarrow B$ ein Homomorphismus von abelschen Varietäten über k, so ist das Bild $\alpha(A)$ eine abelsche Teilvarietät von B, und der Kern von α ist ein Untergruppenschema von A. Für abelsche Varietäten A und B über k ist die Menge aller Homomorphismen von A nach B ein freier $\mathbb{Z}$-Modul von endlichem Rang, der durch

$$\mathrm{Rg}\left(\mathrm{Hom}(A,B)\right) \leq 4 \dim A \dim B$$

nach oben beschränkt ist, siehe [Mum70, Corollary 1, p. 178]. Eine **Isogenie** von abelschen Varietäten über k ist ein endlicher und dominanter Homomorphismus abelscher Varietäten. Existiert zwischen zwei abelschen Varietäten A und B über k eine Isogenie, so nennen wir A und B **isogen** über k, kurz $A \sim_k B$, und sagen A und B sind k-isogen. Damit zwei abelsche Varietäten A und B isogen sind, muss notwendiger Weise $\dim A = \dim B$ gelten. Für eine gegebene Isogenie $\alpha : A \longrightarrow B$ ist der Kern $A[\alpha]$ ein endliches Untergruppenschema der Ordnung $\deg \alpha$. Mit dem Hauptsatz für endlich erzeugte abelsche Gruppen folgt dann $A[\alpha] \cong \mathbb{Z}/n_1\mathbb{Z} \times ... \times \mathbb{Z}/n_r\mathbb{Z}$ mit $n_{i+1}|n_i$ für

$1 \leq i \leq r-1$. Ist α eine separable Isogenie, so nennen wir α auch $(n_1, ..., n_r)$-Isogenie. Ein **Endomorphismus** einer abelschen Varietät A über k ist ein k-rationaler Homomorphismus $\alpha : A \longrightarrow A$. Die k-rationalen Endomorphismen von A über k bilden einen Ring, den wir mit $\mathrm{End}_k(A)$ bezeichnen. Mit $\mathrm{End}_k^0(A)$ meinen wir das Tensorprodukt $\mathrm{End}_k(A) \otimes \mathbb{Q}$. Jede abelsche Varietät A besitzt Multiplikationen mit $n \in \mathbb{N}$, die durch die Endomorphismen

$$[n]_A : A \longrightarrow A, \quad P \longmapsto \underbrace{P + ... + P}_{n\ mal}$$

gegeben sind. Dadurch besitzt jede nicht-triviale abelsche Varietät einen zu $\mathbb{Z}$ isomorphen Teilring in $\mathrm{End}(A)$. Die Multiplikation mit n ist eine Isogenie. Betrachten wir eine abelsche Varietät A über einem endlichen Körper k und eine algebraische Erweiterung K von k, so ist die unter dieser Erweiterung erhaltene abelsche Varietät A' über K dann k-isogen zu $A \otimes_k K$, d.h. $A' \sim_k A \otimes_k K$. Eine abelsche Varietät über k wollen wir k-**einfach** nennen, wenn sie keine nicht-trivialen abelschen Untervarietäten enthält. Weiter nennen wir eine über k definierte abelsche Varietät A dann k-**elementar**, wenn sie k-isogen zur Potenz einer einfachen abelschen Varietät B über k ist, d.h. $A \sim_k B^m$. Jede nicht-triviale abelsche Varietät über k ist zu einem Produkt

$$\prod_{i=1}^{t} A_i^{r_i} \tag{1.15}$$

abelscher Varietäten k-isogen, wobei die A_i einfach und verschiedene A_i und A_j paarweise nicht k-isogen sind, siehe [Gee07, Corollary 12.4, Chapter XII]. Für abelsche Varietäten A ist $\mathrm{End}_k^0(A)$ eine endlich-dimensionale $\mathbb{Q}$-Algebra und wenn A einfach ist sogar ein endlich-dimensionaler Schiefkörper über $\mathbb{Q}$. Für eine beliebige abelsche Varietät A über k mit $A \sim_k \prod_i^n A_i^{r_i}$ besitzt die Endomorphismenalgebra $\mathrm{End}_k^0(A)$ die folgende Zerlegung in ein direktes Produkt ([Gee07, Corollary 12.6, Chapter XII]):

$$\mathrm{End}_k^0(A) \cong \prod_{i=1}^{t} M_{r_i}\left(\mathrm{End}_k^0(A_i)\right), \tag{1.16}$$

wobei $M_{r_i}\left(\mathrm{End}_k^0(A_i)\right)$ der Ring der $r_i \times r_i$-Matrizen über $\mathrm{End}_k^0(A_i)$ ist. Die Endomorphismenringe von einfachen abelschen Varietäten lassen sich wie folgt charakterisieren ([Mum70, Theorem 2, p. 201 and remark], [Ung05, p. 7-8]):

Satz 1.21. *Sei A eine einfache abelsche Varietät über k der Dimension g und $D = \mathrm{End}_k^0(A)$. Auf D sei eine Involution $'$ gegeben, so dass $\mathrm{Tr}_{D/\mathbb{Q}}(xx') > 0$ ist für alle $x \in D^\times$. Bezeichne F das Zentrum von D mit $[D : F] = m^2$ und $[F : \mathbb{Q}] = e$. Ferner sei F_0 der Teilkörper von F mit $e_0 := [F_0 : \mathbb{Q}]$, bestehend aus allen Elementen von F, die von der Involution gefixt werden. Dann ist D einer der folgenden Typen:*

(i) *$D = F = F_0$ ist ein total reeller algebraischer Zahlkörper und die Involution ist die Identität. Es gilt $e|g$.*

(ii) *$F = F_0$ ist ein total reeller Zahlkörper, und D ist eine Quaternionenalgebra über F, so dass die $\mathbb{R}$-Algebrenisomorphie*

$$\mathbb{R} \otimes_{\sigma(F)} D \cong M_2(\mathbb{R})$$

gilt, wobei $M_2(\mathbb{R})$ die Menge aller 2×2-Matrizen mit Einträgen aus $\mathbb{R}$ bezeichnet und $\sigma : F \longrightarrow \mathbb{R}$ eine Einbettung von F ist. Die Involution ist durch

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \longmapsto \begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$$

gegeben mit $\alpha, \beta, \gamma, \delta \in F$. Ferner gilt $2e|g$.

(iii) *$F = F_0$ ist ein total reeller algebraischer Zahlkörper und D ist eine Quaternionenalgebra über F, so dass die $\mathbb{R}$-Algebrenisomorphie*

$$\mathbb{R} \otimes_{\sigma(F)} D \cong \mathbb{H}$$

gilt, wobei $\mathbb{H}$ die gewöhnliche Quaternionenalgebra ist und $\sigma : F \longrightarrow \mathbb{R}$ eine Einbettung von F ist. Die Involution ist durch

$$\alpha + \beta i + \gamma j + \delta k \longmapsto \alpha - \beta i - \gamma j - \delta k \quad (\alpha, \beta, \gamma, \delta \in F)$$

gegeben. Ferner gilt $e|g$.

(iv) *F_0 ist ein total reeller algebraischer Zahlkörper, F ist eine imaginärquadratische Erweiterung von F_0, und D ist ein Schiefkörper mit endlicher Dimension m^2 über F. Es gilt die $\mathbb{C}$-Algebrenisomorphie*

$$\mathbb{R} \otimes_{\sigma(F)} D \cong M_m(\mathbb{C}),$$

wobei $M_m(\mathbb{C})$ die Menge aller $m \times m$-Matrizen mit Einträgen aus $\mathbb{C}$ und $\sigma : F \longrightarrow \mathbb{C}$ eine Einbettung von F ist. Die Involution ist durch

$$(a_{ij}) \longmapsto (\overline{a_{ji}})$$

gegeben. Es gilt $e_0 m|g$.

Sei p eine Primzahl und $q = p^n$, sowie A eine abelsche Varietät der Dimension g über $k = \mathbb{F}_q$. Eine q-**Weil-Zahl** ist eine ganzalgebraische Zahl ω, so dass für jede Einbettung $\psi : \mathbb{Q}(\omega) \longrightarrow \mathbb{C}$ dann $|\psi(\omega)| = \sqrt{q}$ gilt. Für den Frobeniusendomorphismus π_k bezüglich k von A ist das charakteristische Polynom f_{π_k} in $\mathbb{Z}[t]$, da $\mathrm{End}_k(A)$ ein endlich erzeugter freier $\mathbb{Z}$-Modul ist und somit das charakteristische Polynom f_α für $\alpha \in \mathrm{End}_k(A)$ ein normiertes Polynom mit Koeffizienten in $\mathbb{Z}$ ist. Ist f_{π_k} das charakteristische Polynom

des Frobeniusendomorphismus von A_k bezüglich k, so ist jede Nullstelle von f_{π_k} eine q-Weil-Zahl. Sei A eine abelsche Varietät der Dimension g. Ist A dann k-einfach, so hat f_{π_k} den Grad $2g$, und $f_{\pi_k} = g_{\pi_k}^m$ ist eine Potenz des Minimalpolynoms $g_{\pi_k} \in \mathbb{Z}[t]$ von π_k (s.[Tat69, Théorème 1 et Remarques, p. 96]). Ist A ferner k-isogen zum Produkt von Varietäten $\prod_i A_i^{r_i}$ über k wie in (1.15), so ist f_{π_k} das Produkt $\prod_i f_i^{r_i}$ charakteristischer Polynome über $\mathbb{Z}$ von Frobeniusendomorphismen der jeweiligen abelschen Varietäten $A_i^{r_i}$ mit $\deg f = 2g$, was aus [Tat66, Theorem 1, p. 139] folgt.

Eine weitere Charakterisierung von Endomorphismenringen abelscher Varietäten über endlichen Körpern k erfolgt in [Tat66]: Bezeichnet π_k den Frobeniusendomorphismus von A bezüglich k mit charakteristischem Polynom $f_{\pi_k} = \prod g_i^{e_i} \in \mathbb{Z}[t]$, dann definieren wir $r(f_{\pi_k}, f_{\pi_k}) := \sum e_i^2 \deg g_i$. Nun ist $\mathbb{Q}[\pi_k]$ eine endliche $\mathbb{Q}$-Algebra, und für die endlich-dimensionale $\mathbb{Q}$-Algebra $E_k := \mathrm{End}_k^0(A)$ einer abelschen Varietät A der Dimension g gilt

$$\begin{aligned} &2g \le [E_k : \mathbb{Q}] = r(f_{\pi_k}, f_{\pi_k}) \le (2g)^2, \\ &F = \mathrm{Z}(E_k) = \mathbb{Q}[\pi_k], \\ &2g = [E_k : \mathbb{Q}[\pi_k]]^{\frac{1}{2}} \cdot [\mathbb{Q}[\pi_k] : \mathbb{Q}] \text{ und} \\ &f_{\pi_k} = g_{\pi_k}^m \text{ mit } m = [E_k : \mathbb{Q}[\pi_k]]^{\frac{1}{2}}, \end{aligned} \tag{1.17}$$

wobei $\mathrm{Z}(E_k)$ das Zentrum von E_k bezeichnet und die letzten beiden Aussagen nur gelten, wenn A einfach ist. Betrachten wir nun wieder Satz 1.21 unter der Beachtung von (1.17), so erhalten wir folgendes Lemma:

Lemma 1.22. *Sei A eine einfache abelsche Varietät über k. Dann gilt: Gibt es eine Einbettung ψ von $\mathbb{Q}(\pi_k)$, so dass $\psi(\pi_k) \in \mathbb{R}$ ist, so muss* $\dim A = 1$ *oder* $\dim A = 2$ *sein.*

Beweis. Ist $\psi(\pi_k) \in \mathbb{R}$, so gilt $|\psi(\pi_k)| = \sqrt{q} = p^{n/2}$. Ist n gerade, so ist $\psi(\pi_k) = \pm p^{n/2} \in \mathbb{Q}$, was $F \cong \mathbb{Q}$ bedeutet. Ansonsten haben wir $F \cong \mathbb{Q}(\sqrt{p})$, aber in jedem Fall haben wir $[\mathbb{Q}[\pi_k] : \mathbb{Q}] \le 2$ und E kann nicht vom letzten Typ in Satz 1.21 sein, d.h. also $[E_k : F] \le 4$. Daraus folgt aber mit (1.17) dann

$$2g = [E_k : \mathbb{Q}[\pi_k]]^{\frac{1}{2}} \cdot [\mathbb{Q}[\pi_k] : \mathbb{Q}] \le 4,$$

d.h. also $g = 1$ oder $g = 2$. □

Damit erhalten wir folgendes Lemma:

Lemma 1.23. *Seien $k = \mathbb{F}_{p^n}$, A eine abelsche Varietät der Dimension g über k und f_{π_k} das charakteristische Polynom des Frobeniusendomorphismus von A. Ferner sei $\pi_k \in \mathbb{C}$ mit $f_{\pi_k}(\pi_k) = 0$ und $E_k := \mathrm{End}_k(A) \otimes \mathbb{Q}$. Dann gilt:*

(i) Ist $n = 1$ sowie A einfach und besitzt $\mathbb{Q}(\pi_k)$ keine reellen Einbettungen, so ist $E_k = F$, und F ist eine imaginär-quadratische Erweiterung eines total-reellen Zahlkörpers über $\mathbb{Q}$ vom Grad g.

(ii) Ist A einfach und $g \geq 3$, so besitzt $\mathbb{Q}(\pi_k)$ keine reelle Einbettung und somit kann nur der letzte Typ der $\mathbb{Q}$-Algebren von Theorem 1.21 für E_k vorliegen.

(iii) Ist $n = 1$ und $g \geq 3$, so gilt: A ist einfach $\Leftrightarrow$ f_{π_k} ist irreduzibel.

Beweis. Aus [Wat69, Theorem 6.1, p. 550] folgt, dass wenn $n = 1$ ist und $\mathbb{Q}(\pi_k)$ keine reelle Einbettung besitzt, der Endomorphismenring E_k kommutativ ist, was $m = 1$ nach sich zieht. Damit ist f_{π_k} irreduzibel, und mit Satz 1.21 ist E_k eine imaginär-quadratische Erweiterung eines total-reellen Zahlkörpers über $\mathbb{Q}$ vom Grad g. Die zweite Aussage folgt aus Lemma 1.22.

Sei $n = 1$ und $g \geq 3$. Ist f_{π_k} irreduzibel, so gilt mit [Tat66, Theorem 2, p. 140], dass $E_k = \mathbb{Q}(\pi_k)$ ein Körper ist. Wäre A nicht einfach, so hätte E_k entweder Nullteiler oder E_k wäre nicht kommutativ, was beides auf einen Widerspruch führt. Ist A einfach, so folgt aus den ersten beiden Aussagen dieses Lemmas, dass E_k ein Körper ist, und damit muss $m = 1$ sein, d.h. f_{π_k} ist irreduzibel. □

Wir erhalten nun folgende Aussagen über Endomorphismen-Algebren von einfachen abelschen Varietäten über endlichen Körpern:

Lemma 1.24. *Sei $k = \mathbb{F}_{p^n}$ und A eine einfache abelsche Varietät der Dimension g über k sowie $E_k := \mathrm{End}_k(A) \otimes \mathbb{Q}$. Dann treten folgende Typen von Endomorphismenalgebren auf:*

(i) $g = 1$: Quaternionenalgebra über $\mathbb{Q}$ oder imaginär-quadratischer Zahlkörper.

(ii) $g = 2$: Schiefkörper der Dimension 16 über $\mathbb{Q}$, eine Quaternionenalgebra über einem reell-quadratischen Zahlkörper oder eine imaginär-quadratische Erweiterung eines total-reellen quadratischen Zahlkörpers.

(iii) $g \geq 3$: Hier kann nur noch der letzte Typ aus Satz 1.21 auftreten.

Beweis. Im Falle $g = 1$ zeigt ein Blick auf Satz 1.21, dass nur die letzten beiden Typen in Frage kommen, und das ist eben eine Quaternionenalgebra oder ein imaginär-quadratischer Zahlkörper. Im Falle $g = 2$ kommen alle Typen bis auf den ersten Typ in Frage, was zu den besagten Möglichkeiten führt. Ist $g \geq 3$, so folgt die letzte Aussage mit Lemma 1.23. □

1.5 Zentral einfache Algebren

Die meisten Aussagen in diesem Abschnitt wurden aus [Pie82] entnommen, wenn nichts anderes gesagt wird. Da wir an der Berechnung von Endomorphismenringen interessiert sind, benötigen wir zusätzliche Informationen über die Darstellung von Schiefkörpern und Matrixalgebren über einem Zahlkörper F. Eine F-Algebra wollen wir **einfach** nennen, wenn sie nur triviale Ideale besitzt. Ist das Zentrum $Z(A)$ einer F-Algebra A gleich F, so nennen wir A **zentrale** Algebra. Ist A sowohl einfach als auch zentral, dann sagen wir kurz, dass A **zentral einfach** ist. Die Menge aller über F endlich-dimensionalen und zentral einfachen F-Algebren bezeichnen wir mit $\mathfrak{S}(F)$. Für $A \in \mathfrak{S}(F)$ ist die Vektorraumdimension $[A : F] = m^2$ und mit $\mathrm{Deg}(A) := [A : F]^{\frac{1}{2}} = m$ bezeichnen wir den **Grad** von A. Ein Teilkörper von $A \in \mathfrak{S}(F)$ ist eine Teilalgebra E von A, so dass E ein Körper ist. Die Dimension $[E : F]$ ist ein Teiler von m. Gibt es keinen Teilkörper K von $A \in \mathfrak{S}(F)$, so dass $E \subsetneq K$ gilt, so nennen wir E einen **maximalen Teilkörper** von A und ist $[E : F] = \mathrm{Deg}(A)$, so wollen wir E einen **strikt** maximalen Teilkörper von A nennen. Ist A ein Schiefkörper, so ist jeder maximale Teilkörper von A auch strikt maximal.

Mit dem Struktursatz von Wedderburn für halb-einfache Algebren folgt unter Anderem, dass für jedes $A \in \mathfrak{S}(F)$ die Isomorphie $A \cong M_n(D)$ mit einem Schiefkörper D besteht, wobei $M_n(D)$ die Menge aller Matrizen aus $D^{n\times n}$ bezeichnet. Für den Grad von A erhalten wir dann $\mathrm{Deg}(A) = n\mathrm{Deg}(D)$. Den Grad $\mathrm{Ind}(A) := \mathrm{Deg}(D)$ nennen wir den **Index** von A, und offensichtlich ist ein $A \in \mathfrak{S}(F)$ genau dann ein Schiefkörper, wenn $\mathrm{Ind}(A) = \mathrm{Deg}(A)$ gilt. Für ein $A \in \mathfrak{S}(F)$ ist $\mathrm{Ind}(A)$ ein Teiler von $\mathrm{Deg}(A)$. In unserem Fall ist der Index also, wie der Grad, stets endlich.

Seien $A, B, D \in \mathfrak{S}(F)$ und D ein Schiefkörper. Wir sagen, dass A und B äquivalent sind, kurz $A \sim B$, wenn es $m, n \in \mathbb{Z}^{\geq 1}$ so gibt, dass $A \cong M_n(D)$ und $B \cong M_m(D)$ gilt. Die Äquivalenzklassen bezeichnen wir mit $[A]$. Damit können wir die sogenannte **Brauer-Gruppe** definieren:

$$\mathbf{B}(F) := \{[A] \mid A \in \mathfrak{S}(F)\},$$

wobei $[A] \cdot [B] := [A \otimes B]$ für $[A], [B] \in \mathbf{B}(F)$ gilt, $[F]$ das Einselement von $\mathbf{B}(F)$ ist und $[A]^{-1} = [A^\star]$ ist. Dabei bezeichnet für $A \in \mathfrak{S}(F)$ die Algebra $A^\star \in \mathfrak{S}(F)$ eine solche, welche als F-Vektorraum mit A übereinstimmt. Die Multiplikation für $x, y \in A^\star$ ist dann durch $x \circ y := y \cdot x$ definiert, wenn $y \cdot x$ das Produkt in A ist. Zwei Algebren $A, B \in \mathfrak{S}(F)$ sind genau dann isomorph, wenn $[A] = [B]$ und $\mathrm{Deg}(A) = \mathrm{Deg}(B)$ gilt. Mit $\mathrm{Exp}(A)$ bezeichnen wir die **Ordnung** oder den **Exponenten** von $[A]$ in $\mathbf{B}(F)$. Für $A \in \mathfrak{S}(F)$ ist $\mathrm{Ind}(A)$ stets ein Exponent von A, d.h. $\mathrm{Exp}(A)$ teilt $\mathrm{Ind}(A)$. In unserem Falle hat also jedes $A \in \mathfrak{S}(F)$ stets den endlichen Exponenten $\mathrm{Exp}(A)$.

Sei E/F eine algebraische Erweiterung von F und $\iota : F \longrightarrow E$ eine Einbettung. Durch diese Einbettung wird eine Abbildung

$$\iota_* : \mathbf{B}(F) \longrightarrow \mathbf{B}(E), \quad [A] \longmapsto [A \otimes E]$$

mit $A \otimes E$ in $\mathfrak{S}(E)$ induziert. Der Kern von ι_* wird mit $\mathbf{B}(E/K)$ bezeichnet, und es ist $\mathbf{B}(E/F) := \{[A] \in \mathbf{B}(F) \mid [A \otimes E] \sim [E]\}$. Wir sagen, A **zerfällt über** E oder E ist ein Zerfällungskörper für A, wenn $A \otimes E \cong M_r(E)$ ist. Damit ist klar, dass $\mathbf{B}(E/F)$ genau aus denjenigen $[A] \in \mathbf{B}(F)$ besteht, für die A über E zerfällt. Ferner gilt

$$\mathbf{B}(F) = \bigcup_{E/F \text{ galoissch}} \mathbf{B}(E/F) \, .$$

Ist E/F endlich mit $[E : F] = n$, so ist n Exponent für alle $[A] \in \mathbf{B}(E/F)$, d.h. insbesondere ist dann $\mathbf{B}(E/F)$ eine Torsionsgruppe. Ist die Erweiterung E/F zusätzlich noch zyklisch, d.h. also E/F ist galoissch mit zyklischer Galoisgruppe $G(E/F)$, so gilt sogar die Isomorphie

$$\mathbf{B}(E/F) \cong F^\times / N_{E/F}(E^\times).$$

Wir wollen nun zeigen, dass ein $A \in \mathfrak{S}(F)$ durch F bereits vollständig beschrieben wird. Die Theorie, die wir dafür heranziehen, beruht unter anderem auf Klassenkörpertheorie. Wir wollen aber nicht zu sehr in die Tiefe dieser Theorie gehen, da wir hier nur spezielle Algebren betrachten und auch nur solche, deren Zentrum ein algebraischer Zahlkörper ist. Bezeichnet v eine Stelle von F, so soll F_v die Vervollständigung von F bezüglich v sein. Der Index $\mathrm{Ind}(A \otimes F_v)$ ist die Ordnung eines bestimmten Elements in $\mathbb{Q}/\mathbb{Z}$, welches wir mit $\mathrm{inv}_v(A \otimes F_v)$ bezeichnen wollen. Auf die Bedeutung von $\mathrm{Ind}(A \otimes F_v)$ gehen wir später genauer ein. Wir betrachten nun die exakte Sequenz von Gruppenhomomorphismen

$$1 \longrightarrow \mathbf{B}(F) \longrightarrow \mathbf{I}(F) \longrightarrow \mathbb{Q}/\mathbb{Z} \longrightarrow 1,$$

wobei $\mathbf{I}(F) := \bigoplus_{v \in S(F)} I_v(F)$ ist. Hierbei soll $S(F)$ die Menge aller Stellen von F bezeichnen und $I_v(F) = (\frac{1}{2})\mathbb{Z}/\mathbb{Z}$ sein, wenn v reell ist, $I_v(F) = 0$, wenn v komplex ist, und ansonsten ist $I_v(F) = \mathbb{Q}/\mathbb{Z}$. Die dort auftretenden nicht-trivialen Homomorphismen sind durch

$$\mathbf{B}(F) \longrightarrow \mathbf{I}(F), \quad [A] \longrightarrow (\mathrm{inv}_v(A \otimes F_v))_{v \in S(F)}$$

und

$$\mathbf{I}(F) \longrightarrow \mathbb{Q}/\mathbb{Z}, \quad (..., t_v, ...) \longmapsto \sum_{v \in S(F)} t_v$$

gegeben. Für die Wohldefiniertheit des zweiten Homomorphismus bemerken wir, dass $\mathrm{inv}_v(A \otimes F_v) = 0$ für fast alle $v \in S(F)$ ist. Es gilt sogar

$\sum_{v\in S(F)} \mathrm{inv}_v(A\otimes F_v) = 0$. Andererseits kann man zeigen, dass für ein Element $\xi = (...,t_v,...) \in \mathbf{I}(F)$ mit $\sum_v t_v = 0$ ein $A \in \mathfrak{S}(F)$ existiert mit $(...,\mathrm{inv}_v(A\otimes F_v),...) = \xi$.

Die Frage ist nun, wie wir entscheiden können, wann eine Erweiterung E/F ein Zerfällungskörper einer gegebenen Algebra $A \in \mathfrak{S}(F)$ ist. Dazu stellen wir zuerst fest, dass für ein $w \in S(E)$ und $v \in S(F)$ mit $w|v$ die Tatsache $\mathrm{inv}_w(A\otimes E_w) = [E_w : F_v]\mathrm{inv}_v(A\otimes F_v)$ gilt. Dann benutzen wir das lokal-global-Prinzip: E/F ist genau dann Zerfällungskörper von $A \in \mathfrak{S}(F)$, wenn für alle $v \in S(F)$ und alle $w \in S(E)$ mit $w|v$ gilt, dass

$$\mathrm{inv}_w(A\otimes E_w) = [E_w : F_v]\mathrm{inv}_v(A\otimes F_v) = 0$$

ist. Können wir also zu vorgegebenen $A \in \mathfrak{S}(F)$ und endlich vielen Werten $\mathrm{inv}_v(A\otimes F_v)$ eine endliche Erweiterung E/F so konstruieren, dass für die lokalen Grade $[E_w : F_v]$:

$$[E_w : F_v]\mathrm{inv}_v(A\otimes F_v) \in \mathbb{Z}$$

gilt, so ist E ein Zerfällungskörper von A.

Wir wollen hier einen Einschub machen und interessieren uns nun für spezielle zentral einfache F-Algebren A. Eine Algebra $A \in \mathfrak{S}(F)$ heißt **zyklisch**, wenn es einen strikt maximalen Teilkörper E von A gibt, so dass E/F zyklisch ist. Nun gilt folgender Satz:

Satz 1.25. *Sei F ein algebraischer Zahlkörper und $A \in \mathfrak{S}(F)$. Dann ist A zyklisch und es gilt* $\mathrm{Ind}(A) = \mathrm{Exp}(A)$.

Des Weiteren erhalten wir, dass, wenn A ein Schiefkörper ist mit $\mathrm{Deg}(A) = m$, dann A einen zu $F(a^{\frac{1}{m}})$ isomorphen maximalen Teilkörper enthält mit $a \in F$. Die gesamte Situation lässt sich nun durch folgendes Lemma beschreiben.

Lemma 1.26. *Sei E/F eine zyklische Erweiterung mit $G = G(E/F)$ und $G = \langle\sigma\rangle$ mit $|G| = m$. Ist $A \in \mathfrak{S}(F)$ und E ein strikt maximaler Teilkörper von A, so existiert ein $u \in A^\times$ mit*

(i) $A = \bigoplus_{0\le j<m} u^j E$,

(ii) $u^{-1}du = \sigma(d)$ *für alle* $d \in E$ *und*

(iii) $u^m = a \in F^\times$.

Die Darstellung von A in Lemma 1.26 können wir als Verallgemeinerung der Quaternionenalgebra über F auffassen. Ist $A \in \mathfrak{S}(F)$ zyklisch, so schreiben wir für A auch (E,σ,a). Wir werden später bei der Berechnung von Endomorphismenringen sehen, dass dieses Lemma sehr hilfreich ist. Um festzustellen, ob die zyklische und zentral einfache F-Algebra A ein Schiefkörper ist, ist folgendes Lemma von Nutzen (s. [Has32, Theorem 5', S. 180].

Lemma 1.27. *Sei $F/\mathbb{Q}$ endliche Erweiterung von $\mathbb{Q}$ und $A = (E, \sigma, a) \in \mathfrak{S}(F)$ vom Grad $\mathrm{Deg}(A) = n$. Dann ist der Index $\mathrm{Ind}(A)$ die Ordnung von a in $F^\times/N_{E/F}(E^\times)$, wobei wir hier $F^\times$ und $N_{E/F}(E^\times)$ als multiplikative Untergruppen von F auffassen. Insbesondere ist A genau dann ein Schiefkörper, wenn die Ordnung von a in $F^\times/N_{E/F}(E^\times)$ gleich n ist.*

Kennen wir $\mathrm{Ind}(A)$ für ein $A \in \mathfrak{S}(F)$, so können wir ein $a \in F^\times$ bestimmen, für das $a \in F^\times/N_{E/F}(E^\times)$ die Ordnung $\mathrm{Ind}(A)$ hat. Da wir die Endomorphismenringe bis auf Isomorphie bestimmen wollen, spielt es nach dem folgendem Lemma keine Rolle, welches Element wir in $[a] \in F^\times/N_{E/F}(E^\times)$ wählen:

Lemma 1.28. *Sei E/F zyklische Erweiterung vom Grad n mit $G(E/F) = \langle\sigma\rangle$ und $a, b \in F^\times$. Dann gilt $(E, \sigma, a) \cong (E, \sigma, b)$ genau dann, wenn $b/a \in N_{E/F}(E^\times)$ ist.*

Wir kommen nun wieder auf die Charakterisierung einer zentral einfachen Algebra durch sein Zentrum zurück. Das folgende Korollar macht deutlich, warum wir an einem Zerfällungskörper von $A \in \mathfrak{S}(F)$ interessiert sind:

Korollar 1.29. *Sei $A \in \mathfrak{S}(F)$ und E/F eine endliche Erweiterung mit $[E : F] = \mathrm{Deg}(A)$. Dann ist E genau dann ein Zerfällungskörper von A, wenn E als eine F-Algebra isomorph zu einem strikt maximalen Teilkörper von A ist.*

Haben wir eine abelsche Varietät der Form $C \sim_k B^r$ mit B einfach über k gegeben, so gilt für die Endomorphismenalgebra von C dann $\mathrm{End}_k^0(C) \cong M_r(D)$, wenn D die Endomorphismenalgebra von B bezeichnet, welche ein Schiefkörper sein muss. Die Bestimmung von $\mathrm{End}_k^0(B)$ läuft also darauf hinaus, den Schiefkörper D bis auf Isomorphie zu bestimmen. Für die Berechnung von $\mathrm{Ind}(D) = m$ benutzen wir unter anderem den folgenden Satz ([Mil91, Theorem 16.9, p. 62]).

Satz 1.30. *Sei B eine einfache abelsche Varietät über $k = \mathbb{F}_q$, $D = \mathrm{End}_k^0(B)$ und $\pi_{_k} \in D$ der Frobeniusendomorphismus von B. Dann gilt:*

(i) Das Zentrum F von D ist $F := \mathbb{Q}(\pi_{_k})$ und D ist ein Schiefkörper mit $D \in \mathfrak{S}(F)$.

(ii) Für $v \in S(F)$ bezeichne $i_v := \mathrm{inv}_{_v}(D \otimes F_v)$. Dann gilt $\|\pi_{_k}\|_{_v} = q^{-i_v}$, oder äquivalent dazu ist:

$$\mathrm{inv}_{_v}(D \otimes F_v) = \frac{\mathrm{ord}_v(\pi_{_k})}{\mathrm{ord}_v(q)}[F_v : \mathbb{Q}_p] \quad \textit{für} \quad v|p\,,$$

$\mathrm{inv}_{_v}(D \otimes F_v) = \frac{1}{2}$, wenn v eine reelle Stelle ist und ansonsten ist $\mathrm{inv}_{_v}(D \otimes F_v) = 0$.

Aus dem letzten Satz folgt, dass für alle Stellen v außer den archimedischen und denjenigen, die über p liegen, $i_v = 0$ ist. Außerdem ist D in $\mathfrak{S}(F)$, d.h. D ist zyklisch und somit von der Form $D = (E, \sigma, a)$, woraus wir zusätzlich $\mathrm{Exp}(D) = \mathrm{Ind}(D) = \mathrm{Deg}(D) = m$ erhalten. Schreiben wir die $\mathrm{inv}_{v_j}(D \otimes F_{v_j})$ in der Form

$$\mathrm{inv}_{v_j}(D \otimes F_{v_j}) = \frac{a_{v_j}}{m_{v_j}} + \mathbb{Z} \quad (\mathrm{ggT}(a_{v_j}, m_{v_j}) = 1),$$

so ist nach [Mil91, Theorem 16.8., p. 62] dann $m = \mathrm{Ind}(D) = \mathrm{kgV}(m_{v_j})$. Die zyklische Erweiterung E lässt sich mittels Klassenkörpertheorie bestimmen, indem wir ein Korollar des Grundwald-Wang-Theorems auf unsere Situation anwenden: (s. [Mil08, Corrollary 2.5, p. 226])

Korollar 1.31. *Sei $S = \{v_1, ..., v_l\}$ eine endliche Menge von Stellen von $F = Z(D)$ und $m_{v_j} \in \mathbb{Z}^{>0}$ $(j = 1, ..., l)$, wobei $m_{v_j} \in \{1, 2\}$ geeignet ist, wenn v_j archimedisch ist. Dann existiert eine zyklische Erweiterung E/F vom Grad $[E : F] = m = \mathrm{kgV}(m_{v_j})$ $(j = 1, ..., l)$, so dass für den lokalen Grad jeweils $[E_{w_j} : F_{v_j}] = m_{v_j}$ für alle $w_j \in S(E)$ mit $w_j | v_j$ gilt.*

Haben wir also einen Schiefkörper $D \in \mathfrak{S}(F)$ wie in Satz 1.30 mit den endlich vielen Werten $m_{v_j} > 1$ vorgegeben, so existiert nach dem letzten Korollar eine zyklische Erweiterung E/F mit den jeweils lokalen Graden $[E_{w_j} : F_{v_j}] = m_{v_j}$ für $w_j \in S(E)$ und $v_j \in S(F)$ mit $w_j | v_j$, was also

$$\mathrm{inv}_{w_j}(D \otimes E_{w_j}) = [E_{w_j} : F_{v_j}]\mathrm{inv}_{v_j}(D \otimes F_{v_j}) = 0$$

bedeutet und dies wiederum heißt, dass E ein Zerfällungskörper für D ist. Außerdem ist dann E/F, als F-Algebra aufgefasst, isomorph zu einem strikt maximalen Teilkörper von $D = \mathrm{End}_k^0(B)$. Um schließlich eine zyklische Erweiterung $\tilde{E}/F$ für die Endomorphismenalgebra $\mathrm{End}_k^0(C)$ zu erhalten, können wir mit Korollar 1.31 eine beliebige zyklische Erweiterung $\tilde{E}/F$ mit $E \subseteq \tilde{E}$ und $[\tilde{E} : F] = \mathrm{Deg}(\mathrm{End}_k^0(C))$ berechnen, welche dann ebenfalls Zerfällungskörper für $\mathrm{End}_k^0(C)$ ist.

Für Aussagen oder Definitionen in diesem Abschnitt verweisen wir auf [Eic37], [Eic55], [Deu35] und [Kir05]. Als letztes benötigen wir noch Aussagen über die Klassenzahl einer zentral einfachen Algebra A über F. Dazu benötigen wir eine Definition:

Definition 1.32. *Sei $F/\mathbb{Q}$ endliche Erweiterung und $A \in \mathfrak{S}(F)$. Wir sagen dann, dass A die **Eichlerbedingungen** bezüglich F erfüllt, wenn gilt:* $\mathrm{Deg}(A) > 2$ *oder nicht alle unendlichen Stellen von F in A verzweigen.*

Der folgende Satz von Eichler (s. [Eic37, Satz 2, S. 192]) erklärt, woraus sich obige Definition ergibt.

Satz 1.33. *Sei $F/\mathbb{Q}$ endliche Erweiterung von $\mathbb{Q}$ und $A \in \mathfrak{S}(F)$ mit $\mathrm{Deg}(A) = n$. Erfüllt A die Eichlerbedingungen bezüglich F und bezeichnet $\mathfrak{u}$ das Produkt aller unendlichen Stellen von F, welche in A verzweigen, so ist die Idealklassenzahl von A gleich der Strahlklassenzahl modulo $\mathfrak{u}$ in F.*

Es sei noch bemerkt, dass Eichler den Begriff "normale und einfache" Algebra benutzt, welcher gleichbedeutend mit "zentral einfach" ist. Satz 1.33 lässt sich genau dann nicht anwenden, wenn $A \in \mathfrak{S}(F)$ eine Quaternionenalgebra über einem total reellen Zahlkörper F ist. Diese Algebren entsprechen genau den in Satz 1.21 unter (ii) und (iii) auftretenden Algebren. Mit der Aufgabe der Berechnung der Klassenzahl solcher Algebren beschäftigte sich M. Eichler in [Eic55]. Allgemein gilt aber folgender Satz ([Deu35, Satz 1, S. 90]):

Satz 1.34. *Die Klassenzahl einer Algebra A über $\mathbb{Q}$ ist endlich.*

Des Weiteren betrachten wir ein $A \in \mathfrak{S}(F)$ und eine Maximalordnung M von A. Ist $\alpha \in A^\times$, so ist $\alpha^{-1} M \alpha =: \tilde{M}$ wieder eine Maximalordnung von A. Wir sagen dann, dass M und $\tilde{M}$ vom **gleichen Typ** sind. Die Anzahl der auf diese Weise zueinander nicht-konjugierten Klassen von Maximalordnungen ist ein Teiler der Klassenzahl von A (s. [Deu35, Abschnitt 2, S. 89]). Mit Satz 1.34 wissen wir dann, dass die Anzahl der Typen stets endlich ist.

Kapitel 2

Korrespondenzen

2.1 Algebraische Sicht der Korrespondenzen

2.1.1 Grundlagen

Ziel dieses Kapitels ist es, einen Überblick über Deurings Theorie der Korrespondenzen zwischen algebraischen Funktionenkörpern zu geben. Sämtliche Aussagen sind, wenn diese nicht bewiesen werden, aus [Deu37], [Deu40] oder [Eic63] entnommen.

Korrespondenzen induzieren Homomorphismen zwischen Divisorenklassengruppen. Ein wichtiger Spezialfall ist der Folgende: Es seien zwei isomorphe, separable und algebraisch unabhängige Funktionenkörper F_1 und F_2 über einem gemeinsamen Konstantenkörper K vorgegeben. Erweitern wir den Konstantenkörper K von F_1 zu F_2, so erhalten wir einen neuen Körper F_1F_2/F_2. Deuring zeigt in [Deu37, S. 188, unten] nun, dass es im Fall $K = \mathbb{C}$ mittels der von ihm eingeführten Theorie der Korrespondenzen möglich ist, den gesamten Endomorphismenring der Jacobischen von F_2/K zu beschreiben. Dies gilt aber auch für $K = \overline{\mathbb{F}_p}$, wie wir später sehen werden. Hierbei soll $\overline{\mathbb{F}_p}$ den algebraischen Abschluss von $\mathbb{F}_p$ bezeichnen. Die Korrespondenzen entsprechen Divisoren von F_1F_2/F_2, und sämtliche Endomorphismen von $\mathcal{C}^0_{F_2}$ lassen sich mit Hilfe der Korrespondenzen von F_1F_2/F_2 darstellen.

Im Folgenden betrachten wir zwei Funktionenkörper F_1/K und F_2/K mit dem gemeinsamen Konstantenkörper K, wobei Folgendes gelten soll:

$$\begin{array}{l} K \text{ ist algebraisch abgeschlossen,} \\ F_1/K \text{ und } F_2/K \text{ sind algebraisch unabhängig und} \\ F_1/K \text{ und } F_2/K \text{ sind regulär.} \end{array} \tag{2.1}$$

Wir erweitern nun den Konstantenkörper K von F_1 zu F_2. Bezeichnet F_1F_2 das Kompositum von F_1 und F_2, so erhalten wir einen Körper $L = F_1F_2$ mit

Konstantenkörper F_2. Es handelt sich um eine transzendente Erweiterung des Konstantenkörpers K von F_1. Wir wollen einige Feststellungen im folgenden Lemma festhalten:

Lemma 2.1. *Seien $F_1 = K(x_1, y_1)$ und $F_2 = K(x_2, y_2)$ zwei Funktionenkörper, welche die Bedingungen (2.1) erfüllen. Ferner sei $L = F_1F_2$ das Kompositum von F_1 und F_2. Dann gilt:*

(i) $[L : F_2(x_1)] = [F_1 : K(x_1)]$,

(ii) L/F_2 *hat den genauen Konstantenkörper* F_2,

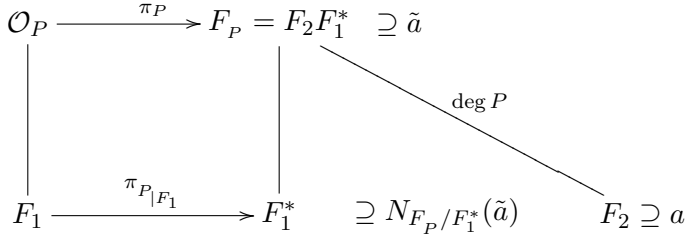
(iii) $g_{F_1/K} = g_{L/F_2}$,

(iv) besitzt F_1 *die Erzeugung* $F_1 = K(x_1, y_1)$ *mit* $x_1, y_1 \in F_1$, *so ist* $L/F_2 = F_2(x_1, y_1)$ *und*

(v) sämtliche Primdivisoren $P \in \mathbb{P}_{L/F_2}$, *die über* $F_2(x_1)/F_2$ *verzweigen, sind konstant.*

Beweis. Die Aussagen folgen aus Lemma 1.18. □

Die obigen Aussagen gelten auch mit vertauschten Rollen von F_1 und F_2, d.h. man betrachtet L/F_1 statt L/F_2. Wir wollen nun zeigen, wie man mit Hilfe der Divisoren von L/F_2 Homomorphismen zwischen den Divisorklassengruppen von F_2 und F_1 konstruieren kann. Dazu betrachten wir folgendes Diagramm, in dem $P \in \mathbb{P}_{L/F_2}$ ein nicht-konstanter Primdivisor sein soll. Für die bessere Lesbarkeit schreiben wir $F_P := F_{2_P}$.



(2.2)

Ein Divisor $a \in \mathcal{D}_{F_2/K}$ wird mittels der Conorm in die algebraische Erweiterung F_P zu $\tilde{a} = \mathrm{Con}_{F_P/F_2}(a)$ hochgehoben. Anschließend wird die Norm von $\tilde{a}$ über F_P/F_1^* gebildet. Da P nach Voraussetzung nicht konstant ist, folgt, dass π_P eingeschränkt auf F_1 ein Isomorphismus ist. Der Körper F_1^* soll der zu F_1 bezüglich der Restriktion von π_P auf F_1 isomorphe Teilkörper von F_P sein. Schließlich wenden wir auf $N_{F_P/F_1^*}(\tilde{a})$ das Inverse der eingeschränkten Restklassenabbildung von π_P an und erhalten einen Divisor von F_1. Diesen wollen wir mit

$$P(a) := {\pi_{P\,|F_1}}^{-1}\left(N_{F_P/F_1^*}(\mathrm{Con}_{F_P/F_2}(a))\right)$$

bezeichnen. Für konstante Divisoren $P \in \mathbb{P}_{L/F_2}$ definieren wir $P(a) := \deg a \cdot p$ für $a \in \mathbb{P}_{F_2/K}$ und $p := P \cap F_1$.

Diese Vorschrift lässt sich auf die Divisoren von $\mathcal{D}_{L/F_2}$ fortsetzen. Für einen Divisor $D = \sum_P n_P P \in \mathcal{D}_{L/F_2}$ und $a \in \mathcal{D}_{F_2/K}$ bedeutet das

$$D(a) := \sum_P n_P P(a) \in \mathcal{D}_{F_1/K}. \tag{2.3}$$

Damit erhalten wir folgende Definition:

Definition 2.2. *Seien $D \in \mathcal{D}_{L/F_2}$ und $a \in \mathcal{D}_{F_2/K}$. Ist D ein Primdivisor, so heißt die oben definierte Abbildung $a \longmapsto D(a)$ **Primkorrespondenz** von F_2 nach F_1, und für einen beliebigen Divisor D nennen wir die Abbildung $a \longmapsto D(a)$ eine **Korrespondenz** von F_2 nach F_1. Die durch einen Divisor D gegebene Korrespondenz wollen wir ebenfalls mit D bezeichnen.*

Es gilt die Gradformel

$$\deg_{F_1/K} D(a) = \left(\deg_{L/F_2} D\right) \cdot \left(\deg_{F_2/K} a\right), \tag{2.4}$$

und, wenn keine Missverständnisse zu erwarten sind, schreiben wir kurz

$$\deg D(a) = \deg D \cdot \deg a. \tag{2.5}$$

Der Begriff Divisor für ein Element $D \in \mathcal{D}_{L/F_2}$ ist also doppeldeutig. Zum Einem beschreibt D ein Element der freien abelschen Gruppe $\mathcal{D}_{L/F_2}$, zum Anderen eine Korrespondenz von F_2 nach F_1 oder einfach nur kurz eine Korrespondenz von L/F_2. Wir wollen aber auf diesen Unterschied nicht jedes Mal eingehen, wenn aus dem Zusammenhang hervorgeht, was gemeint ist.

Da sowohl die Conorm als auch die Norm additiv sind, d.h. die Reihenfolge von Addition und Abbildung unerheblich ist, sind die Korrespondenzen von L/F_2 Homomorphismen. Zuerst folgt nämlich aus eben Gesagtem und aus der Definition der Korrespondenzen $D(a+b) = D(a) + D(b)$ für $a, b \in \mathcal{D}_{F_2/K}$. Die wichtigsten weiteren Eigenschaften der Korrespondenzen enthält der folgende Satz [Deu37, S. 173, Satz 4 bis Satz 8].

Satz 2.3. *Sei $D \in \mathcal{D}_{L/F_2}$ eine Korrespondenz. Dann gilt:*

i) Ist $a \in \mathcal{P}_{F_2/K}$, so gilt $D(a) \in \mathcal{P}_{F_1/K}$.

ii) Es ist $D = 0$ genau dann, wenn $D(a) = 0$ für fast alle $a \in \mathcal{D}_{F_2/K}$ gilt.

iii) D ist genau dann konstant, wenn $D(a) = 0$ für fast alle $a \in \mathcal{D}^0_{F_2/K}$ gilt.

iv) Es ist $D \in \mathcal{P}_{L/F_2}$ genau dann, wenn $D(a) \in \mathcal{P}_{F_1/K}$ für fast alle $a \in \mathcal{D}_{F_2/K}$ gilt.

v) D ist genau dann zu einem konstanten Divisor äquivalent, wenn $D(a) \in \mathcal{P}_{F_1/K}$ für fast alle $a \in \mathcal{D}^0_{F_2/K}$ gilt.

Die Aussage i) von Satz 2.3 nennt man auch den **Homomorphiesatz** und Aussage iv) das **Additionstheorem** für Korrespondenzen. Nun treffen wir noch eine Verabredung.

Definition 2.4. *Mit $G \leq \mathcal{D}_{L/F_2}$ wollen wir die Untergruppe von $\mathcal{D}_{L/F_2}$ bezeichnen, welche von den Klassen der Gruppen C_{L/F_2} und $\mathcal{P}_{L/F_2}$ erzeugt wird. Für eine Korrespondenz $D \in \mathcal{D}_{L/F_2}$ bezeichne $[D]_C$ die Nebenklasse von D in $\mathcal{D}_{L/F_2}/G$ und wir nennen $[D]_C$ die **Korrespondenzklasse** von D.*

Aus dem Homomorphiesatz für Korrespondenzen und der Gradformel (2.4) folgt nun

Korollar und Definition 2.5. *Die Korrespondenzen von L/F_2 liefern Homomorphismen zwischen den Klassengruppen $\mathcal{C}^0_{F_2}$ und $\mathcal{C}^0_{F_1}$. Auf den Korrespondenzklassen der Korrespondenzen ist in natürlicher Weise eine Addition mittels Divisoraddition definiert, d.h. die Korrespondenzklassen bilden eine abelsche Gruppe. Diese wollen wir mit*

$$\mathrm{Cor}\,(F_2, F_1) := \left\{ [D]_C \mid D \in \mathcal{D}_{L/F_2} \right\}$$

bezeichnen.

Bemerkung 2.6. *Haben wir einen Funktionenkörper F/K gegeben, so können wir mit dem Satz von Riemann-Roch eine nicht-konstante Funktion $x \in F \backslash K$ so finden, dass die Stelle im Unendlichen in $F/K(x)$ genau eine Fortsetzung besitzt. Ist nämlich $P \in \mathbb{P}_{F/K}$ Primdivisor und $n \in \mathbb{N}$ genügend groß, so gibt es ein $x \in F$ und einen effektiven Divisor $B \in \mathcal{D}_{F/K}$ mit $(x) = B - nP$. Als Folge ergibt sich, dass in $F/K(x)$ ein Divisor genau dann Hauptdivisor ist, wenn sein endlicher Anteil ein gebrochenes Hauptideal in $\mathcal{O}_F$ ist. Besitzt die unendliche Stelle in L/F_2 genau eine Fortsetzung, so lassen sich die Aussagen von Satz 2.3 von Divisoren auf gebrochene Ideale der endlichen Maximalordnung übertragen.*

Bemerkung 2.7. *Die Repräsentanten der Divisorklassen von L/F_2 stellen die sämtlichen Homomorphismen zwischen den Jacobischen von F_2/K und F_1/K dar, wie wir später sehen werden. Für Deurings Theorie der Korrespondenzen spielen die konstanten Divisoren keine Rolle. Als Homomorphismen zwischen den Divisorenklassen vom Grad Null sind sie nach Aussage iii) in Satz 2.3 trivial. Sie werden hier nur deshalb eingeführt, weil wir sie später im algorithmischen Teil dieser Arbeit benötigen. Diejenigen Primdivisoren von L/F_2, welche sich in $\mathcal{O}_{L/F_2}$ nicht als Ideale darstellen lassen, sind konstant. Ist $0 \neq D \in \mathrm{Cor}\,(F_2, F_1)$, so können wir uns also statt der Divisoren*

auf die gebrochenen Ideale der endlichen Maximalordnung beschränken. Im Diagramm (2.2) zur Definition der Korrespondenzen muss dann $\mathcal{O}_P$ durch $\mathcal{O}_{L/F_2}[K[x_1]^{-1}]$ ersetzt werden.

2.1.2 Multiplikation der Korrespondenzen

Seien $F_i = K(x_i, y_i)$ $(i = 1, 2, 3)$ drei paarweise algebraisch unabhängige separable Funktionenkörper über K und $P \in \mathbb{P}_{F_3F_2/F_3}$ eine nicht-konstante Primkorrespondenz. Wir wollen nun eine weitere Verknüpfung, eine Multiplikation, für Korrespondenzen einführen. Dazu halten wir uns an [Eic63, Kapitel V]. Wir gehen in mehreren Schritten vor.

1.) Für Primdivisoren $P \in \mathbb{P}_{F_3F_2/F_3}$ vom Grad eins betrachten wir den Isomorphismus

$$\tau := \pi_{P|F_2} : F_2 \longrightarrow F_3.$$

Ist nun $Q \in \mathbb{P}_{F_2F_1/F_2}$, so definieren wir das Produkt $Q \cdot P := \tau(Q)$ wie in (1.14), welches ein Divisor in $\mathcal{D}_{F_3F_1/F_3}$ ist. Besteht der Divisor $D = \sum_{i=1}^{n} n_i Q_i \in \mathcal{D}_{F_2F_1/F_2}$ nur aus nicht-konstanten Primkorrespondenzen, so definieren wir

$$D \cdot P := \left(\sum_{i=1}^{n} n_i Q_i \right) \cdot P := \sum_{i=1}^{n} n_i \left(Q_i \cdot P \right) \quad \in \mathcal{D}_{F_3F_1/F_3}.$$

2.) Sei P eine rein inseparable Primkorrespondenz, d.h. F_P/F_3 ist eine rein inseparable Erweiterung. Dann ist $\deg_{F_2F_3/F_3}(P) = p^n$ mit $n \geq 0$. Erweitern wir F_3 durch eine rein inseparable Erweiterung vom Grad p^n zu ${F_3}'$, so gibt es genau ein $P' \in \mathcal{D}_{F_3'F_2/F_3'}$ mit $\deg_{F_3'F_2/F_3'}(P') = 1$ und $P = p^n P'$. Wir setzen dann

$$D \cdot P := p^n \left(D \cdot P' \right) \in \mathcal{D}_{F_3F_1/F_3}.$$

3.) Sei P eine separable Primkorrespondenz, d.h. F_P/F_3 ist eine endlich separable Erweiterung der Charakteristik p. Wir können eine endliche Erweiterung E/F_3 so finden, dass $\mathrm{Con}_{E/F_3}(P)$ komplett zerfällt in $\sum_{i=1}^{n} {Q'}_i$ mit lauter Primkorrespondenzen ${Q'}_i \in \mathcal{D}_{EF_2/E}$ vom Grad $\deg_{EF_2/{F'}_3}({Q'}_i) = 1$. Wir dürfen sogar o.B.d.A. annehmen, dass E/F_3 galoissch ist. In diesem Fall setzen wir

$$D \cdot P := \sum_{i=1}^{n} (D \cdot {Q'}_i) \quad \in \mathcal{D}_{F_3F_1/F_3}.$$

4.) Ist P eine beliebige nicht-konstante Primkorrespondenz aus $\mathbb{P}_{F_3F_2/F_3}$, so bilden wir zuerst den separablen Abschluss E von F_3 in F_P und betrachten die ganze Situation zuerst in der Konstantenkörpererweiterung EF_2/E von

F_3F_2/F_3. Dann zerfällt wie in 3.)

$$\mathrm{Con}_{EF_2/F_3F_2}(P) = \sum_{i=1}^{n} {Q'}_i \quad ({Q'}_i \in \mathcal{D}_{EF_2/E})$$

in lauter rein inseparable Korrespondenzen ${Q'}_i = p^n {P_i}'$, wobei ${P_i}' \in \mathcal{D}_{F_{P_i}F_2/F_{P_i}}$ vom Grad $\deg_{F_{P_i}F_2/F_{P_i}}({P_i}') = 1$ ist. Wir berechnen dann

$$D \cdot \mathrm{Con}_{EF_2/F_3F_2}(P) = \sum_{i=1}^{n} p^n (D \cdot {P_i}') = \sum_{i=1}^{n} D_i, \tag{2.6}$$

wobei jeder Summand D_i aus $\mathcal{D}_{EF_2/E}$ kommt. Schließlich setzen wir

$$C := \sum_{i=1}^{n} (D \cdot D_i) \quad \left(C \in \mathcal{D}_{F_3F_1/F_3}\right)$$

wie in 3.) und $D \cdot P := C$.

5.) Ist $C \in \mathcal{D}_{F_2F_1/F_2}$ oder $D \in \mathcal{D}_{F_3F_2/F_3}$ konstant, so definieren wir $D \cdot C = 0$. Für $C = \sum_{i=1}^{m} m_i C_i \in \mathcal{D}_{F_3F_2/F_3}$ und $D = \sum_{i=1}^{n} n_i Q_i \in \mathcal{D}_{F_2F_1/F_2}$ beliebig definieren wir schließlich

$$D \cdot C := \sum_{i=1}^{m} m_i (D \cdot C_i)$$

mit 1.) bis 4.) und der Definition für konstante Divisoren. Das Produkt zweier Korrespondenzen $C \in H_{F_2F_1/F_2}$ und $D \in H_{F_3F_2/F_3}$ hat den Grad

$$\deg_{F_3F_1/F_3} C \cdot D = \deg_{F_2F_1/F_2} C \cdot \deg_{F_3F_2/F_3} D.$$

Die Verknüpfungen $+$ und $\cdot$ von Korrespondenzen sind **assoziativ** und **distributiv**. Definieren wir die Verknüpfung $\cdot$ zwischen den Korrespondenzklassen von $\mathrm{Cor}\,(F_2, F_1)$, so ist diese unabhängig vom Repräsentanten. Deshalb können wir die Multiplikation, genauso wie die Addition, auf den Korrespondenzklassen definieren.

Sind die Funktionenkörper F_i/K $(i = 1, 2, 3)$ nun zusätzlich alle K-isomorph zueinander mittels $\tau_i : F_i \longrightarrow F_3$ $(i = 1, 2)$ und $\tau : F_1 \longrightarrow F_2$, so definieren wir für $D, C \in \mathcal{D}_{L/F_2}$ eine innere Verknüpfung durch

$$D \cdot C := \tau_2(D) \cdot \tau_1(C) \in \mathcal{D}_{L/F_2},$$

wobei $\tau_2(D)$ und $\tau_1(C)$ wie in (1.14) definiert sind. Damit bilden die Korrespondenzen einen Ring. Für eine Korrespondenz $D \in \mathcal{D}_{L/F_2}$ definieren wir nun

$$D : \mathcal{D}_{F_2/K} \longrightarrow \mathcal{D}_{F_2/K}, \quad a \longmapsto \tau(D(a)) \tag{2.7}$$

als Vorschrift für die Divisoren von $\mathcal{D}_{F_2/K}$.

Definition und Satz 2.8. *Seien F_1/K und F_2/K wie in (2.1) und K-isomorph. Ferner sei*

$$\mathrm{Cor}\,(F_2) := \left\{ [D]_C \mid D \in \mathcal{D}_{L/F_2} \right\}.$$

Dann wird durch die inneren Verknüpfungen

$$+ \,:\mathrm{Cor}\,(F_2) \times \mathrm{Cor}\,(F_2) \longrightarrow \mathrm{Cor}\,(F_2), \quad ([A]_C, [B]_C) \longmapsto [A+B]_C$$

und

$$\cdot \,:\mathrm{Cor}\,(F_2) \times \mathrm{Cor}\,(F_2) \longrightarrow \mathrm{Cor}\,(F_2), \quad ([A]_C, [B]_C) \longmapsto [A \cdot B]_C$$

die Menge $\mathrm{Cor}\,(F_2)$ *zu einem Ring* $(\mathrm{Cor}\,(F_2), +, \cdot)$*, dem* ***Ring der Korrespondenzen*** *von F_2. Wir wollen für* $(\mathrm{Cor}\,(F_2), +, \cdot)$ *einfach nur* $\mathrm{Cor}\,(F_2)$ *schreiben. Für Korrespondenzklassen* $[A]_C, [B]_C \in \mathrm{Cor}\,(F_2)$ *gilt dann mit (2.7)*

$$([A]_C \cdot [B]_C)(a) = [A]_C([B]_C(a)) \quad \textit{für alle} \quad a \in \mathcal{D}_{F_2/K}.$$

Der Rosati

Durch das Vertauschen des Konstantenkörpers von L/F_2 mit F_1 erhalten wir zusätzlich einen Homomorphismus

$$^\star : L/F_2 \longrightarrow L/F_1, \quad \alpha \mapsto \alpha^\star.$$

Wenden wir diesen auf die Korrespondenzklassen an, so erhalten wir einen involutorischen Isomorphismus zwischen den Korrespondenzklassen von L/F_2 und L/F_1. Das Bild für ein $[A]_C$ mit $A \in \mathcal{D}_{L/F_2}$ bezeichnen wir dann mit $[A^\star]_{C^\star}$, wobei $C^\star_{L/F_1} \leq \mathcal{D}_{L/F_1}$ die Untergruppe ist, welche von den Hauptdivisoren und konstanten Divisoren von L/F_1 erzeugt wird. Für $A, B \in \mathcal{D}_{L/F_2}$ definieren wir dann $A^\star \cdot B := \tau_2(A^\star) \cdot B$ und $A \cdot B^\star := \tau_1(A) \cdot B^\star$. Für den Grad von $A \in H_{L/F_2}$ und $A^\star \in H_{L/F_1}$ gelten

$$\deg_{L/F_2}(A^\star) = \deg_{L/F_1}(A) \quad \text{und} \quad \deg_{L/F_1}(A^\star) = \deg_{L/F_2}(A).$$

Wir setzen nun F_1 und F_2 als K-isomorph mittels $\tau : F_1 \longrightarrow F_2$ voraus. Ferner sei

$$\phi : F_1 \otimes_K F_2 \longrightarrow F_1 \otimes_K F_2, \quad a \otimes_K b \longmapsto \tau^{-1}(b) \otimes_K \tau(a).$$

Für ein nicht-konstantes $P \in \mathbb{P}_{L/F_2}$ ist $Q_0 := \hat{\Phi}(\phi(\hat{\Phi}^{-1}(P_0)))$ ein Primideal aus $\mathcal{O}_{L/F_2}[K[x_1]^{-1}]$. Hierbei ist $\hat{\Phi}$ der Algebrenisomorphismus aus Lemma 1.19. Diese Abbildung setzen wir dann auf $\mathcal{D}_{L/F_2}$ fort, und deren Bilder bezeichnen wir wieder mit $A^\star \in \mathcal{D}_{L/F_2}$ für $A \in \mathcal{D}_{L/F_2}$. Sind A und B Divisoren aus $\mathcal{D}_{L/F_2}$, so gelten $A \cdot B^\star := \tau_2(A) \cdot \tau_1(B^\star)$, $A^\star \cdot B := \tau_2(A^\star) \cdot \tau_1(B)$ und

$A^\star \cdot B^\star := \tau_2(A^\star) \cdot \tau_1(B^\star)$. Damit wird aus der Abbildung * ein involutorischer Antiautomorphismus auf den Korrespondenzklassen von L/F_2, der sogenannte Antiautomorphismus von **Rosati**, mit den Eigenschaften

$$(A \cdot B)^\star = B^\star \cdot A^\star \text{ und } (A+B)^\star = A^\star + B^\star$$

für $A, B \in \mathcal{D}_{L/F_2}$.

Die Einheits- und Frobeniuskorrespondenz

Sind F_1 und F_2 mittels $\tau : F_1 \longrightarrow F_2, \quad (x_1, y_1) \longmapsto (x_2, y_2)$ dann K-isomorph, so gilt für den Divisor $D \in \mathcal{D}_{L/F_2}$ mit dem endlichen Primideal $D_0 = \langle x_1 - x_2, y_1 - y_2 \rangle$ in Zwei-Element-Darstellung $D(a) = a$ für alle $a \in \mathcal{D}_{F_2/K}$. Denn aus

$$F_1^* = K(\pi_{_D}(x_1), \pi_{_D}(y_1)),$$

mit F_1^* wie in (2.2), $\pi_{_D}(x_1) = x_2$ und $\pi_{_D}(y_1) = y_2$ folgt $F_1^* = F_2$. Damit erhalten wir folgendes Korollar.

Korollar 2.9. *Der Ring* $\mathrm{Cor}\,(F_2)$ *besitzt das eindeutige Einselement* $[D]_C$.

Die Korrespondenz D wollen wir **Einheitskorrespondenz** nennen. Sei nun $K = \overline{\mathbb{F}_p}$. Wir kommen nun zu der sogenannten **Frobeniuskorrespondenz** F. Wir nehmen an, dass die definierenden Gleichungen $f(x_i, y_i)$ für die Funktionenkörper F_i/K durch Vertauschen von x_1 mit x_2 und y_1 mit y_2 auseinander hervorgehen und y_i ganz über x_i ist. Somit sind F_1 und F_2 dann K-isomorph. Ist n minimal mit $f_i \in \mathbb{F}_{p^n}(x_i, y_i)$ $(i = 1, 2)$, so ist mit $q := p^n$ der endliche Teil von $F \in \mathcal{D}_{L/F_2}$ durch $F_0 = \langle x_1 - x_2^q, y_1 - y_2^q \rangle$ in Zwei-Element-Darstellung gegeben. Für den endlichen Teil des Rosati $F^\star \in \mathcal{D}_{L/F_2}$ von F gilt ${F_0}^\star = \langle x_1^q - x_2, y_1^q - y_1 \rangle$. Zudem gilt nach [Eic63, Kapitel V, Abschnitt 7, S. 262]

$$F^n \cdot (F^\star)^n = (F^\star)^n \cdot F^n = q^n D. \tag{2.8}$$

Inseparable Primkorrespondenzen können wir wie folgt schreiben [Eic63, Kapitel V, Abschnitt 7, S. 262].

Lemma 2.10. *Ist* $0 \neq P \in \mathcal{D}_{L/F_2}$ *eine inseparable Primkorrespondenz, so lässt sich* P *als* $P = (F^\star)^n \cdot A$ *mit einer Primkorrespondenz* $0 \neq A \in \mathcal{D}_{L/F_2}$ *und* $n \in \mathbb{N}$ *geeignet schreiben. Für* L/F_1 *und* $0 \neq P \in \mathcal{D}_{L/F_1}$ *gilt dann analog* $P = B \cdot F^n$ *mit einer Primkorrespondenz* $0 \neq B \in \mathcal{D}_{L/F_1}$ *und* $n \in \mathbb{N}$ *geeignet.*

Bemerkung 2.11. *Aus Lemma 2.10 folgt, dass alle inseparablen Korrespondenzen* $A \in \mathcal{D}_{L/F_2}$ *in dem von* $F^\star$ *erzeugten Rechtsideal und analog im Falle für ein inseparables* $B \in \mathcal{D}_{L/F_1}$ *in dem von* F *erzeugten Linksideal liegen.*

2.1.3 Der Restidealsatz

Der Restidealsatz ist ein wichtiger Bestandteil im Beweis von Aussage (iv) in Satz 2.3. Er ist aber auch hilfreich für eine vereinfachte Berechnung der Bilder einer Korrespondenz $A \in \mathcal{D}_{L/F_2}$. In dieser Berechnung müssen bei einer fest gewählten Idealbasis des Ideales A_0 endlich viele Primdivisoren aus $\mathcal{D}_{F_2/K}$ ausgeschlossen werden. Da wir aber unsere Korrespondenzen als Homomorphismen von $\mathcal{C}^0_{F_2}$ nach $\mathcal{C}^0_{F_1}$ betrachten, können wir für die Repräsentanten der Elemente von $\mathcal{C}^0_{F_2}$ immer Zähler- und Nennerdivisoren so finden, dass in ihren Darstellungen keiner der endlich vielen Ausnahmedivisoren von $\mathcal{D}_{F_2}$ vorkommt.

Wie im letzten Abschnitt erwähnt (Bem. 2.7), können wir uns auf die gebrochenen Ideale der endlichen Maximalordnungen beschränken. Wir fixieren nun jeweils eine Erzeugung $F_i = K(x_i, y_i)$ von F_i/K $(i = 1, 2)$ sowie von $L/F_2 = F_2(x_1, y_1)$ und eine Ganzheitsbasis $\Omega := \{\omega_1, ..., \omega_n\} \subseteq \mathcal{O}_{F_1/K}$ von $\mathcal{O}_{L/F_2}$. Sei $b_1, ..., b_n$ eine $K[x_1]$-Basis von $\mathcal{O}_{F_1/K}$ mit $[F_1 : K] = n$. Wir wissen bereits nach Lemma 1.19, dass dann $\{b_1, ..., b_n\}$ ebenfalls eine $F_2[x_1]$-Basis von $\mathcal{O}_{L/F_2}$ ist. Ferner sei $A \in \mathcal{D}_{L/F_2}$ und A_0 der endliche Teil von A, d.h. A_0 ist ein gebrochenes Ideal von L/F_2. Als $F_2[x_1]$-Modul betrachtet, besitzt A_0 eine Basis der Form

$$B_i := \sum_{j=1}^{n} \frac{G_{ij}}{G}\omega_j \quad (i = 1, ..., n)$$

mit $G_{ij}, G \in F_2[x_1]$ und $G \neq 0$. Das gebrochene Ideal A_0 lässt sich dann als B_0/G schreiben mit einem ganzen Ideal B_0, so dass $G \cdot A_0 = B_0$ ist. Seien $p \in \mathbb{P}_{F_2/K}$, $\mathcal{O}_p \subseteq F_2$ der zugehörige Bewertungsring und

$$\Phi : \mathcal{O}_{F_1} \otimes_K F_2 \to \mathcal{O}_{L/F_2}, \quad a \otimes b \longmapsto ab$$

der K-Algebrenisomorphismus von Lemma 1.19. Ein Element $\alpha \in \mathcal{O}_{L/F_2}$ heißt **p-ganz** oder **ganz bezüglich p**, wenn $\Phi^{-1}(\alpha) \in \mathcal{O}_{F_1} \otimes_K \mathcal{O}_p$ gilt. Wir wollen eine Basis $\mathcal{B} := \{B_i \mid i = 1, ..., n\}$ von A_0 ganz bezüglich p nennen, wenn sowohl G als auch jedes Element von $G \cdot \mathcal{B}$ ganz bezüglich p sind. Ferner wollen wir $\mathcal{B}$ dann **p-regulär** oder **regulär bezüglich p** nennen, wenn $\mathcal{B}$ bezüglich p ganz ist und sowohl G als auch die Determinante F^p_Ω der Übergangsmatrix von Ω zur Basis $G \cdot \mathcal{B}$ von B_0 normierte Polynome in $\mathcal{O}_p[x_1]$ sind. Wir bezeichnen dann die Basis mit $\mathcal{B}^p_\Omega$. Besitzt das Ideal D_0 eines Divisors $D \in \mathcal{D}_{L/F_2}$ eine p-reguläre Basis bezüglich Ω, so sagen wir auch, dass D regulär bezüglich p und Ω ist. Ist aus dem Zusammenhang klar, was Ω ist, so sagen wir einfach, dass D regulär bezüglich p ist.

Definition 2.12. *Seien $B \in \mathcal{D}_{L/F_2}$ mit endlichem Anteil $B_0 \subseteq \mathcal{O}_{L/F_2}$, $p \in \mathbb{P}_{F_2/K}$ sowie $\mathcal{B}^p_\Omega = \{B_i \mid i = 1, ..., n\}$ eine p-reguläre Basis von B_0. Dann*

wollen wir das Ideal

$$B_{0,\mathcal{B}_\Omega^p} := \langle \Phi^{-1}(B_i) \mid i = 1, ..., n \rangle_{\mathcal{O}_{F_1} \otimes_K \mathcal{O}_p}$$

das p-reguläre Ideal von B_0 in $\mathcal{O}_{F_1} \otimes_K \mathcal{O}_p$ bezüglich $\mathcal{B}_\Omega^p$ nennen.

Wir definieren mittels $p \in \mathbb{P}_{F_2/K}$ und der dazugehörigen Restklassenabbildung $\pi : \mathcal{O}_p \longrightarrow K$ einen Ringhomomorphismus

$$\Pi : \mathcal{O}_{F_1} \otimes_K \mathcal{O}_p \longrightarrow \mathcal{O}_{F_1} \otimes_K K, \quad a \otimes b \longmapsto a \otimes \pi(b). \tag{2.9}$$

Ist $A \in \mathcal{D}_{L/F_2}$ und besitzt der endliche Anteil $A_0 = B_0/G$ eine p-reguläre Basis $\mathcal{B}_\Omega^p$, so setzen wir

$$I := \frac{\Pi(B_{0,\mathcal{B}_\Omega^p})}{\Pi(\Phi^{-1}(G))}.$$

Da B_0 ein Ideal und Π surjektiv ist, ist I isomorph zu einem gebrochenen Ideal in $\mathcal{O}_{F_1}$, welches wir wieder mit I bezeichnen wollen. Der endliche Anteil A_0 besitzt den Grad $\deg_{L/F_2} A_0 = \deg_{F_2(x_1)/F_2} N_{L/F_2}(A_0)$, welcher auf Grund der p-Regularität von $\mathcal{B}_\Omega^p$ identisch mit $\deg_{F_1/K} I = \deg_{L/F_2} A_0$ ist. Denn es werden alle p-ganzen Elemente von A_0 durch p-ganze Linearkombinationen der Basiselemente irgendeiner p-regulären Basis $\mathcal{B}_\Omega^p$ von A_0 erzeugt (s. [Deu37, S. 170, Mitte]). Weil F_Ω^p ein normiertes Polynom aus $\mathcal{O}_p[x_1]$ ist, lässt sich F_Ω^p als p-ganze Linearkombination jeder beliebigen p-regulären Basis $\mathcal{B}_\Omega^p$ von A_0 darstellen. Somit ist $\Phi^{-1}(F_\Omega^p)$ in $B_{0,\mathcal{B}_\Omega^p}$ enthalten, und die Leitkoeffizienten von F_Ω^p und G können modulo p nicht verschwinden. Es ist klar, dass es zu einem gegebenen Ideal A_0 nur endlich viele $p \in \mathbb{P}_{F_2/K}$ gibt, für die A_0 keine p-reguläre Basis besitzt. Hat I die Faktorisierung $\prod_{i=1}^n Q_{i,0}^{e_i}$ mit $\iota_{P_i}^{-1}(P_i) = Q_{i,0}$ $(P_i \in \mathbb{P}_{F_1/K},\ i = 1, ..., n)$, so wollen wir

$$\overline{A}^p := \sum_{i=1}^n e_i P_i \in \mathcal{D}_{F_1/K}$$

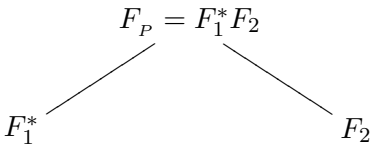
schreiben. Sind F_1 und F_2 mittels $\tau : F_1 \longrightarrow F_2$ isomorph über K, so setzen wir noch

$$\overline{A}^p := \tau \left(\sum_{i=1}^n e_i P_i \right) \in \mathcal{D}_{F_2/K} .$$

Mit Satz 2.16 zeigen wir, dass $\overline{A}^p$ von der gewählten p-regulären Basis unabhängig ist. Für Korrespondenzen $D, C, D + C \in \mathcal{D}_{L/F_2}$, deren endlicher Anteil jeweils eine p-reguläre Basis besitzt, gilt dann

$$\overline{D + C}^p = \overline{D}^p + \overline{C}^p. \tag{2.10}$$

Denn allgemein ist stets $\overline{D+C}^p \leq \overline{D}^p + \overline{C}^p$ erfüllt. Auf Grund der p-Regularität von $C+D$ folgt die Gleichheit. Ist $0 \neq P \in \mathcal{D}_{L/F_2}$ eine Primkorrespondenz, so betrachten wir folgendes Diagramm, in dem wiederum $F_{_P} := F_{2_{_P}}$ ist:



(2.11)

Wir können o.B.d.A. voraussetzen, dass bei den Funktionenkörpern $F_i = K(x_i, y_i)$ $(i = 1, 2)$ jeweils y_i ganz über $K[x_i]$ ist. Bezeichnet $\pi_{_P}$ die Restklassenabbildung von P und ist $x_1^* = \pi_{_P}(x_1)$ und $y_1^* = \pi_{_P}(y_1)$, so gilt für den Restklassenkörper $F_{_P} = F_2\,(x_1^*, y_1^*)$. Da $F_1^* = K(x_1^*, y_1^*)$ gilt, folgt hieraus $F_{_P} = F_1^*(x_2, y_2)$. Ferner sehen wir, dass die Körpererweiterung F_P/F_1^* endlich ist.

Wir benötigen für die anstehende Definition noch zwei Lemmata:

Lemma 2.13. *Seien K_1/K und K_2/K Zwischenkörper des Funktionenkörpers $E = K_1K_2$. Dann kann E nicht über K_1 und K_2 inseparabel sein.*

Beweis. Wäre E sowohl über K_1 als auch über K_2 inseparabel, so erhalten wir $K_i \subseteq KE^p \subsetneq E$. Dies ergäbe eine widersprüchliche Inklusionskette $K_1K_2 \subseteq KE^p \subsetneq E = K_1K_2$. □

Nun müssen wir noch einige Primdivisoren aus F_2 herausnehmen, um den Restidealsatz anwenden zu können. Diese werden im folgenden Lemma charakterisiert:

Lemma 2.14. *Seien die algebraischen Funktionenkörper K_1/K und K_2/K Zwischenkörper des Funktionenkörpers $E = K_1K_2$ und o.B.d.A. sei E separabel über K_1. Ferner sei $\Delta \subseteq K_2$ eine Basis von E/K_1. Dann gibt es in Abhängigkeit von Δ eine endliche Ausnahmemenge S_2 von Stellen in K_2 und eine endliche Ausnahmemenge S_1 von Stellen in K_1, so dass für alle $p \notin S_2$ und alle $q \notin S_1$ gilt:*

(i) Sei $I_2 := \mathrm{Con}_{E/K_2}(p)$ und $i_2 := N_{E/K_1}(I_2)$. Ist $\alpha \in K_1$ mit $\nu_{P_i}(\alpha) \geq \nu_{P_i}(I_2)$ für $P_i \in \mathrm{supp}(I_2)$, so gilt $\nu_{p_i}(N_{E/K_1}(\alpha)) \geq \nu_{p_i}(i_2)$ für $p_i \in \mathrm{supp}\, i_2$ und

(ii) ist $I_1 := \mathrm{Con}_{E/K_1}(q)$ und $i_1 := N_{E/K_2}(I_1)$. Ist $\alpha \in K_2$ mit $\nu_{Q_i}(\alpha) \geq \nu_{Q_i}(I_1)$ für $Q_i \in \mathrm{supp}(I_1)$, so gilt $\nu_{q_i}(N_{E/K_2}(\alpha)) \geq \nu_{q_i}(i_1)$ für $q_i \in \mathrm{supp}\, i_1$.

Beweis. S. Kapitel 5, Lemma 3.3. □

Idealtheoretisch bedeutet zum Beispiel der 1. Fall in Lemma 2.14 Folgendes: Wenn ein Element $\alpha \in K_1$, aufgefasst als ein Element in E, etwa im Ideal I_2 der endlichen Maximalordnung von E/K_1 liegt, so soll neben α^n mit $n = [E : K_1]$ auch α selbst in der Norm i_2 von I_2 liegen. Zwar liegt α stets in $I_2 \cap K_1$, aber im Allgemeinen ist $i_2 \neq (I_2 \cap K_1)$.

Das letzte Lemma motiviert folgende Definition:

Definition 2.15. *Sei $P \in \mathcal{D}_{L/F_2}$ eine nicht-konstante Primkorrespondenz und F_1^*, F_2 und F_P wie in (2.11) gegeben.*

(i) Ist F_P/F_2 separabel, so bezeichne $\Delta \subseteq F_1^*$ eine Basis von F_P/F_2. Mit $\mathcal{A}_{P,\Delta} \subseteq \mathbb{P}_{F_2/K}$ sei die endliche Ausnahmemenge von Divisoren aus Lemma 2.14 im Fall (ii), angewandt auf $E = F_P, K_2 = F_1^*$ und $K_1 = F_2$, bezeichnet.

(ii) Anderenfalls bezeichne $\Delta \subseteq F_2$ eine Basis von F_P/F_1^*. Mit $\mathcal{A}_{P,\Delta} \subseteq \mathbb{P}_{F_2/K}$ sei dann die endliche Ausnahmemenge von Divisoren aus Lemma 2.14 im Fall (i), angewandt auf $E = F_P, K_2 = F_2$ und $K_1 = F_1^*$, bezeichnet.

Der Restidealsatz von Deuring lautet nun in Divisorenschreibweise:

Satz 2.16. *Sei $0 \neq A \in \mathcal{D}_{L/F_2}$ eine Korrespondenz der Gestalt $A = \sum_{i=1}^n n_i Q_i$ mit nicht-konstanten Primdivisoren $Q_i \in \mathbb{P}_{L/F_2}$. Dann gilt*

$$A(p) = \overline{A}^p = \sum_{i=1}^n n_i \overline{Q_i}^p = \sum_{i=1}^n n_i Q_i(p)$$

für alle $p \in \mathbb{P}_{F_2/K}$, für welche die Ideale Q_{i0} und A_0 jeweils eine p-reguläre Basis $\mathcal{B}_{i\Omega}^p$ bzw. $\mathcal{A}_\Omega^p$ besitzen und $p \notin S := \bigcup \mathcal{A}_{Q_i,\Delta}$ gilt. Ferner ist $\overline{P}^p$ für ein p-reguläres $P \in \mathbb{P}_{L/F_2}$ nicht abhängig von der gewählten p-regulären Basis von P_0.

Beweis. Wir werden die Aussage zuerst für eine nicht-konstante Primkorrespondenz $P \in \mathcal{D}_{L/F_2}$ zeigen. Dazu benutzen wir folgende abkürzende Notation: Für einen Funktionenkörper F/K, einen Divisor $D \in \mathcal{D}_{F/K}$ und ein Element $\alpha \in F$ soll $\alpha \in D$ bedeuten, dass $\nu_q(\alpha) \geq \nu_q(D)$ für alle $q \in \operatorname{supp} D$ gilt.

Sei $p \in \mathbb{P}_{F_2/K} \backslash \mathcal{A}_{P,\Delta}$, und bezeichne $B_i := B_i(x_1, y_1)$ die Elemente einer p-regulären Basis $\mathcal{B}_\Omega^p$ von P_0 $(i = 1, ..., n)$. Wir benutzen wieder die Bezeichnungen aus (2.11). Ferner sei F_Ω^p die Determinante der Übergangsmatrix der Ganzheitsbasis Ω von $\mathcal{O}_{L/F_2}$ zur Basis $\mathcal{B}_\Omega^p$. Dann sind alle Koeffizienten von $F_\Omega^p \in F_2[x_1]$ nach Voraussetzung p-ganz, und der Leitkoeffizient von F_Ω^p ist in $\mathcal{O}_p^*$. Das Element x_1^* genügt in F_P also einer normierten Gleichung, was

bedeutet, dass x_1^* p-ganz ist. Da y_1 ganz über x_1 ist, ist auch y_1^* ganz bezüglich p. Anders ausgedrückt heißt dies, dass sowohl x_1^* als auch y_1^* an allen $Q \in \mathbb{P}_{F_P/F_2}$ mit $Q|p$ nicht-negative Ordnung $\nu_Q(x_1^*) \geq 0$ und $\nu_Q(y_1^*) \geq 0$ besitzen.

Sei $m := [F_P : K_1^*]$. Mit [Deu37, S. 170, Mitte] wissen wir, dass die p-ganzen Elemente von P_0 alle Elemente $\alpha \in P_0$ sind, welche sich als p-ganze Linearkombination der Basiselemente B_i darstellen lassen. Ist $\alpha = \sum_{i=1}^n f_i(x_1)B_i(x_1, y_1)$ mit $f_i(x_1) \in \mathcal{O}_p[x_1]$ $(i = 1, ..., n)$ ein beliebiges p-ganzes Element von P_0, so gilt

$$\beta := \pi_P(\alpha) = \sum_{i=1}^{n} f_i(x_1^*)B_i(x_1^*, y_1^*) = 0 \ \in F_P.$$

Da sämtliche Koeffizienten von den $B_i(x_1, y_1)$ und f_i nach Voraussetzung p-ganz sind, können wir zu den Restklassen bezüglich p übergehen, was die Koeffizienten der f_i und B_i angeht. Wir erhalten ein Element $\overline{\beta}^p \in F_P$ mit

$$\overline{\beta}^p = \sum_{i=1}^{n} \overline{f}_i^p(x_1^*)\overline{B}_i^p(x_1^*, y_1^*)$$

sowie

$$\beta = \underbrace{\left(\beta - \overline{\beta}^p\right)}_{=:\gamma} + \overline{\beta}^p = 0,$$

woraus $\gamma = -\overline{\beta}^p$ in F_P folgt. Es gilt dafür $\nu_{P_i}(\gamma) \geq e_i$, wenn die Conorm von p die Gestalt $\mathrm{Con}_{F_P/F_2}(p) = \sum e_i P_i$ hat, da für die P_i, wie oben bereits ausgeführt wurde, $\nu_{P_i}(x_1^*), \nu_{P_i}(y_1^*) \geq 0$ gilt. Daraus folgt also

$$\nu_{P_i}(\overline{\beta}^p) \geq e_i. \tag{2.12}$$

Da K algebraisch abgeschlossen ist, ist $\overline{\beta}^p$ sogar ein Element aus $F_1^* = K(x_1^*, y_1^*)$. Wenden wir nun auf $\overline{\beta}^p$ den Isomorphismus $\pi^{-1}_{P_{|F_1}}$ an, so erhalten wir

$$\overline{\alpha}^p := \pi^{-1}_{P_{|F_1}}(\overline{\beta}^p) = \sum_{i=1}^{n} \overline{f}_i^p(x_1)\overline{B}_i^p(x_1, y_1) = \Pi \circ \Phi^{-1}(\alpha) \in \overline{P}^p.$$

Daraus ersehen wir aber andererseits für ein Element $\alpha \in F_1$ mit $\alpha \in \overline{P}^p$, dass

$$\pi_{P_{|F_1}}(\alpha) \in \mathrm{Con}_{F_P/F_2}(p)$$

gilt. Setzen wir $I := \pi_{P_{|F_1}}(\overline{P}^p)$ und $J := \pi_{P_{|F_1}}(P(p))$, so erhalten wir als Erstes

$$\mathrm{Con}_{F_P/F_2}(p) \leq \mathrm{Con}_{F_P/F_1^*}(I). \tag{2.13}$$

Wenden wir hierauf die Norm von F_P/F_1^* an, so wird aus (2.13) schließlich

$$J = N_{F_P/F_1^*}\left(\mathrm{Con}_{F_P/F_2}(p)\right) \ \leq \ N_{F_P/F_1^*}\left(\mathrm{Con}_{F_P/F_1^*}(I)\right) = mI.$$

Lässt sich der Divisor J als $J = \sum q_i$ mit paarweise verschiedenen Primdivisoren $q_i \in \mathbb{P}_{F_1^*/K}$ schreiben, so erhalten wir $I \geq J$. Aus der p-Regularität folgt, wie wir später nochmal zeigen werden, nun aber

$$\deg_{F_1^*/K}(I) = \deg_{F_1^*/K}(J),$$

d.h. es gilt also $I = J$ und damit auch $P(p) = \overline{P}^p$. Diese Situation entspricht dem 1. Fall in Definition 2.15, d.h. wenn F_P/F_2 separabel ist. Ist F_P/F_2 inseparabel, so muss F_P/F_1^* nach Lemma 2.13 separabel sein. Dies entspricht dann dem 2. Fall in Definition 2.15. Ein anderer Extremfall ist, dass F_P/F_2 rein inseparabel ist: Dann ist J von der Form $J = lq$ mit $l \in \mathbb{N}$ geeignet. Ist dann $mI = jq$ mit $j \in \mathbb{N}$ geeignet, so gilt wiederum $J = I$. In den verbleibenden Fällen können wir nicht hoffen, dass J die Gestalt $\sum q_i$ mit paarweise verschiedenen Primdivisoren q_i hat.

Wir behandeln im Folgendem zwei Fälle gleichzeitig, nämlich F_P/F_2 ist inseparabel oder F_P/F_1^* ist inseparabel. Aus der Voraussetzung $p \in \mathbb{P}_{F_2/K} \backslash \mathcal{A}_{P,\Delta}$ folgt dann mit (2.12) und Lemma 2.14

$$\overline{\beta}^p \in N_{F_P/F_1^*}\left(\mathrm{Con}_{F_P/F_2}(p)\right).$$

Schließlich wenden wir $\pi^{-1}_{P|F_1}$ auf $\overline{\beta}^p$ an und erhalten

$$\overline{\alpha}^p = \pi^{-1}_{P|F_1}\left(\overline{\beta}^p\right) = \sum_{i=1}^{n} \overline{f}_i^p(x_1)\overline{B}_i^p(x_1, y_1) \in P(p).$$

Da α ein beliebiges p-ganzes Element von P_0 ist, folgt hieraus $P(p) \leq \overline{P}^p$. Mit dem Gradsatz (2.4), der algebraischen Abgeschlossenheit von K und der p-Regularität von P erhalten wir

$$\deg_{F_1/K} P(p) = \deg_{L/F_2} P = \deg_{L/F_2} P_0 = \deg_{F_1/K} \overline{P}^p.$$

Aus $0 \leq P(p) \leq \overline{P}^p$ und aus eben gesagten Gradgründen erhalten wir dann $\overline{P}^p = P(p)$. Weil wir im Beweis eine beliebige p-reguläre Basis benutzt haben, ist $\overline{P}^p$ somit unabhängig von der gewählten p-regulären Basis.

Für eine Korrespondenz $A = \sum_{i=1}^{n} n_i Q_i$ wenden wir für $p \notin S$ obige Vorgehensweise auf jeden Primdivisor Q_i an und erhalten mit Hilfe von (2.10) die gewünschte Gleichheit $A(p) = \overline{A}^p = \sum_{i=1}^{n} n_i \overline{Q_i}^p$. □

Im folgenden Spezialfall können wir wesentlich einfacher bestimmen, in welchem Fall $\overline{A}^p = A(p)$ gilt:

Korollar 2.17. *Sind $P \in \mathbb{P}_{L/F_2}$ und $p \in \mathbb{P}_{F_2/K}$ jeweils Primdivisoren vom Grad eins, so gilt $\overline{P}^p = P(p)$, falls P regulär bezüglich p ist.*

Beweis. Ist P regulär bezüglich p, so können wir $\overline{P}^p$ berechnen, und es ist $\deg_{F_1/K} P(p) = 1 = \deg_{F_1/K}(\overline{P}^p)$, d.h. $P(p)$ und $\overline{P}^p$ sind Primdivisoren. Auf Grund von $I \geq J$ erhalten wir hieraus $P(p) = \overline{P}^p$. □

Bemerkung 2.18. *Die Fixierung einer festen Ganzheitsbasis aus $\mathcal{O}_{F_1/K}$ ist notwendig, da ansonsten der Begriff der p-Regularität nicht wohldefiniert ist. Da wir später den Restidealsatz benutzen werden, um Bilder von Elementen $[a] = [a_0 - a_\infty] \in \mathcal{C}^0_{F_2}$ zu berechnen und wir, wie bereits erwähnt, die Repräsentanten immer so abändern können, dass keine der Ausnahmedivisoren in a_0 oder a_∞ vorkommen, spielt diese Abhängigkeit von den gewählten Basen Ω und Δ keine Rolle. Denn eine Korrespondenz bildet Hauptdivisoren auf Hauptdivisoren ab, und somit ist das Bild in $\mathcal{C}^0_{F_1}$ unabhängig vom gewählten Repräsentanten in $[a] \in \mathcal{C}^0_{F_2}$.*

2.2 Geometrische Sicht der Korrespondenzen

In diesem Abschnitt wollen wir eine kurze Einführung in die geometrische Sichtweise der Korrespondenzen geben und die wichtigsten Entsprechungen sowohl in der algebraischen als auch in der geometrischen Sichtweise aufzeigen. Sämtliche Aussagen sind, wenn sie nicht bewiesen werden, aus [Har77], [Mil05], [Hin91], [Coh06], [Tat66] oder [Smi05] entnommen.

2.2.1 Grundlagen

Wenn nichts anderes gesagt wird, so bezeichnen X_1, X_2 und X_3 immer reduzierte, irreduzible und nicht-singuläre projektive Kurven über einem gemeinsamen algebraisch abgeschlossenen Grundkörper K. Zu den Kurven X_1 und X_2 betrachten wir das Produkt $X := X_1 \times X_2$, welches eine nicht-singuläre projektive **Fläche** über K ist. Die Weil-Divisorengruppe von X, welche eine freie abelsche Gruppe ist die von den Primdivisoren erzeugt wird, bezeichnen wir mit $\mathrm{Div}(X)$. Mit π_1 und π_2 bezeichnen wir die jeweiligen Projektionen $\pi_i : X \longrightarrow X_i$. Einem Morphismus $\phi : X_1 \longrightarrow X_2$ können wir eine **Fortsetzung** (engl.: Pushforward) $\phi_* : \mathrm{Div}(X_1) \longrightarrow \mathrm{Div}(X_2)$ mittels

$$\phi_* \left(\sum n_i P_i \right) := \sum n_i \phi(P_i)$$

und eine **Zurückziehung** (engl.: Pullback) mittels $\phi^* : \mathrm{Div}(X_2) \longrightarrow \mathrm{Div}(X_1)$ durch

$$\phi^* \left(\sum n_i Q_i \right) := \sum n_i \sum_{P \in \phi^{-1}(Q_i)} \mathrm{ord}_P(t_{Q_i}) P$$

zuordnen. Hierbei soll t_{Q_i} eine lokale Uniformisierende bezüglich P sein. Für einen Morphismus $\phi : X_1 \longrightarrow X_2$ ist $\deg \phi := [K(X_1) : K(X_2)]$, wobei $K(X_i)$ den Funktionenkörper von X_i bezeichnet.

Eine **Korrespondenz der Kurven** X_1 und X_2 ist ein Divisor D von X und heißt **prim**, wenn D ein Primdivisor ist, d.h. eine reduzierte und irreduzible Kurve in X. Ist $P \in \mathrm{Div}(X)$ eine Primkorrespondenz, so definieren die Projektionen π_i eingeschränkt auf P jeweils Morphismen

$$\pi_{i_{|P}} : P \to X_i \quad (i = 1, 2) \; .$$

Ist $p_i \in X_i$, so ist $\pi_i^{-1}(p_i)$ eine Primkorrespondenz von X. Korrespondenzen, die Urbilder von Punkten sind, heißen **fibral** und ihre Gesamtheit wird mit $\mathrm{Fib}(X)$ bezeichnet. Die fibralen Divisoren bilden eine Untergruppe von $\mathrm{Div}(X)$, und es gilt die Isomorphie $\mathrm{Fib}(X) \cong \mathrm{Div}(X_1) \times \mathrm{Div}(X_2)$. Bezeichnet $\mathrm{Div}(X)^{nonFib}$ die von den nicht-fibralen Divisoren und dem Nulldivisor erzeugte Untergruppe von $\mathrm{Div}(X)$, so gilt

$$\mathrm{Div}(X) = \mathrm{Div}(X)^{nonFib} \bigoplus \mathrm{Fib}(X) \; .$$

Jede Korrespondenz D lässt sich dann eindeutig als Summe $D = C + C'$ von Divisoren schreiben mit $C \in \mathrm{Div}(X)^{nonFib}$ und $C' \in \mathrm{Fib}(X)$.

Für eine Primkorrespondenz $P \in \mathrm{Div}(X)$ gibt es zwei Grade

$$d_i(P) := \begin{cases} 0 & \text{falls } P \text{ fibral ist,} \\ \deg \pi_{i_{|P}} & \text{sonst,} \end{cases}$$

welche sich jeweils dann $\mathbb{Z}$-linear auf $\mathrm{Div}(X)$ fortsetzen lassen. Die Flächen $X_1 \times X_2$ und $X_2 \times X_1$ sind in natürlicher Weise isomorph zueinander. Das Bild einer Korrespondenz $C \in X_1 \times X_2$ unter diesem Isomorphismus wollen wir mit C^t bezeichnen und **Transponierte** von C nennen. Ist $X_1 = X_2$, so heißt eine Korrespondenz $C \in X_1 \times X_2$ **symmetrisch**, wenn $C = C^t$ gilt.

Jedem Morphismus $\phi : X_1 \longrightarrow X_2$ können wir eine Korrespondenz

$$\Gamma_\phi := (Id_{X_1} \times \phi)(X_1) \subseteq X$$

zuordnen, wobei $Id_{X_1} : X_1 \longrightarrow X_1$ der Identitätsmorphismus ist. Die Korrespondenz

$$\Delta_{X_1} := \Gamma_{Id_{X_1}} := (Id_{X_1} \times Id_{X_1})(X_1) \subseteq X_1 \times X_1$$

heißt **Diagonalkorrespondenz**. Ist $\mathbb{F}_q$ mit $q = p^n$ der kleinste Körper, über dem X_1 definiert ist, so erhalten wir für $r \geq 1$ den **Frobeniusmorphismus** $\mathcal{F}^{(r)} : X_1 \longrightarrow X_1$, $[x_1 : ... : x_l] \longmapsto [x_1^{q^r} : ... : x_l^{q^r}]$ und die **Frobeniuskorrespondenz** $\mathfrak{F}^r_{X_1} = \Gamma_{\mathcal{F}^{(r)}} := (Id_{X_1} \times \mathcal{F}^{(r)})(X_1)$.

Sei $P \in \mathrm{Div}(X)$ eine Primkorrespondenz und $\tau_i := \pi_{i|_P}$ die auf P eingeschränkten Projektionen. Wir erhalten dann einen Homomorphismus

$$\phi_P : \mathrm{Div}(X_1) \longrightarrow \mathrm{Div}(X_2), \tag{2.14}$$

$$d \longmapsto \begin{cases} (\tau_{2*} \circ {\tau_1}^*)(d) & \text{falls } P \in \mathrm{Div}(X)^{nonFib}, \\ (\deg d)\tau_2(P) & \text{sonst} \end{cases} \tag{2.15}$$

und durch $\mathbb{Z}$-lineare Fortsetzung einen Homomorphismus

$$\Psi : \mathrm{Div}(X) \longrightarrow \mathrm{Hom}(\mathrm{Div}(X_1), \mathrm{Div}(X_2)) \ .$$

Diesem können wir einen Homomorphismus

$$\Phi : \mathrm{Div}(X) \longrightarrow \mathrm{Hom}(J_{X_1}, J_{X_2}) \tag{2.16}$$

zuordnen, wobei J_{X_1} und J_{X_2} jeweils die Jacobischen von X_1 und X_2 sind. Bezeichnet $G_{X_1X_2}$ die von $\mathrm{Fib}(X)$ und den Hauptdivisoren $\mathrm{Prin}(X)$ von X erzeugte Untergruppe von $\mathrm{Div}(X)$, d.h. ist

$$G_{X_1X_2} := \langle \mathrm{Fib}(X), \mathrm{Prin}(X) \rangle, \tag{2.17}$$

so gilt die Isomorphie

$$\mathrm{Div}(X)/G_{X_1X_2} \cong \mathrm{Hom}(J_{X_1}, J_{X_2}).$$

Gilt für zwei Korrespondenzen $\Phi(D_1) = \Phi(D_2)$, so nennen wir diese **homomorph äquivalent**. Ist $\Phi(D) = 0$ für eine Korrespondenz $D \in \mathrm{Div}(X)$, so heißt D **homomorph trivial**. Zwei Korrespondenzen D_1 und D_2 sind genau dann homomorph äquivalent, wenn sie sich um einen Divisor unterscheiden, der die Summe von Hauptdivisoren und fibralen Divisoren ist.

Haben wir zwei Korrespondenzen $D_1 \in \mathrm{Div}(X_1 \times X_2)$ und $D_2 \in \mathrm{Div}(X_2 \times X_3)$, so können wir mittels der Homomorphismen $\Phi(D_1)$ und $\Phi(D_2)$ einen Homomorphismus $\phi : J_{X_1} \longrightarrow J_{X_3}$ konstruieren. Dem Homomorphismus ϕ entspricht eindeutig eine Korrespondenzklasse $[D] \in \mathrm{Div}(X_1 \times X_3)/G_{X_1X_3}$. Betrachten wir nun den Spezialfall $X = X_1 \times X_1$, so lässt sich auf $\mathrm{Div}(X)/G_{X_1X_1}$ eine Multiplikation mittels $[D_1] \cdot [D_2] := [D]$ einführen. Lassen sich D_1, D_2 und D durch Divisoren $D_1 = C_1 + C_1', D_2 = C_2 + C_2'$ und $D = C_3 + C_3'$ zerlegen, wobei keiner der Primdivisoren der $C_i = \sum_j {n_j}^{(i)} {P_j}^{(i)}$ in G liegt und die C_i' in G sind, so definieren wir $D_1 \cdot D_2 := C_1 \cdot C_2 := C_3$. Somit wird $(\mathrm{Div}(X), +, \cdot)$ zu einem Ring mit Einselement Δ_{X_1}, dem **Ring der Korrespondenzen**. Für eine Korrespondenz $D \in \mathrm{Div}(X)$ ist dann $\Phi(D)$ ein Endomorphismus von J_{X_1}.

2.2.2 Die Schnitt- und Korrespondenzpaarung

Auf den Korrespondenzen lässt sich nun eine eindeutige und bilineare Paarung definieren. Sind $C, D \in \mathrm{Div}(X)$ Korrespondenzen und ist $P \in C \cap D$ Schnittpunkt von C und D, so sagen wir C und D schneiden sich transversal an P, wenn die lokalen Gleichungen f von D und g von C an P das maximale Ideal $\mathfrak{m}_P$ von $\mathcal{O}_{X,P}$ erzeugen. Damit können wir die Schnittpaarung definieren:

Satz 2.19. *Es gibt eine eindeutige bilineare Paarung*

$$\mathrm{Div}(X)^2 \longrightarrow \mathbb{Z}, \quad (C, D) \longmapsto C.D \ ,$$

so dass gilt:

(i) *Sind C und D nicht-singuläre Kurven und transversal zueinander, so ist $C.D = \#(C \cap D)$,*

(ii) $C.D = D.C$,

(iii) $(C_1 + C_2) \cdot D = C_1.D + C_2.D$ *und*

(iv) *sind C_1 und C_2 linear äquivalent, d.h. ist $C_1 \sim C_2$, so gilt $C_1.D = C_2.D$.*

Sind $C, C' \in \mathrm{Div}(X)$, so dass $C.D = C'.D$ für alle $D \in \mathrm{Div}(X)$ gilt, so nennen wir C und C' **numerisch äquivalent**. Sei C eine irreduzible nichtsinguläre Kurve von X und sei D eine Kurve von X, welche C transversal schneidet. Dann ist [Har77, Lemma 1.3, p. 358]

$$\#(C \cap D) = \deg_C(\mathcal{L}(D) \otimes \mathcal{O}_C),$$

wobei $\mathcal{L}(D)$ die zu D zugehörige invertierbare Garbe von X ist und $\deg_C$ den Grad von $\mathcal{L}(D) \otimes \mathcal{O}_C$ bezeichnet, aufgefasst als Divisor von C. Jedoch können wir auf die Eigenschaft von D, die Kurve C transversal zu schneiden, verzichten: Haben die Korrespondenzen C und D keine gemeinsame irreduzible Komponente, so können wir den Schnitt $C.D$ mittels

$$C.D = \sum_{P \in C \cap D} (C.D)_P \tag{2.18}$$

definieren. Hierbei bezeichnet $(C.D)_P = \dim_k \mathcal{O}_{X,P}/(f, g)$ die **Schnittmultiplizität** von C und D an P, wobei f und g lokale Gleichungen für C und D an P sein sollen. Wir können für eine Korrespondenz C immer eine linear äquivalente Korrespondenz C' so finden, dass C und C' keine gemeinsame Komponente haben, wie in [Sha72, Lemma 1, p. 194] gezeigt wird. Für eine Korrespondenz C definieren wir dann den **Selbstschnitt** durch $C.C := C.C'$.

Bis zum Ende dieses Abschnitts soll, wenn nichts Anderes gesagt wird, $i \in \{1, 2\}$ gelten. Im Folgendem fassen wir X_1 und X_2 als abstrakte Varietäten der Dimension eins auf (s. [Har77, Definition , p. 105]), d.h. wir identifizieren insbesondere die Punkte der Kurven X_i mit Bewertungsringen, und die zu den Kurven zugehörigen regulären und algebraisch unabhängigen

Funktionenkörper seien von der Gestalt $F_i = K(x_i, y_i)$ mit $[F_i : K(x_i)] = n_i$. Damit erhalten wir jeweils als offene Überdeckungen

$$X_i = \underbrace{\mathrm{Spec}_{max}\Big(\mathrm{Cl}(K[x_i], F_i)\Big)}_{=:U_{1i}} \cup \underbrace{\mathrm{Spec}_{max}\Big(\mathrm{Cl}(K[x_i^{-1}], F_i)\Big)}_{=:U_{2i}} .$$

Bezeichnen $\mathcal{O}_{X_i}$ die jeweiligen Garben der Varietät X_i, so gilt $\mathcal{O}_{X_i}(U_{1i}) = \mathrm{Cl}(K[x_i], F_i) = \mathcal{O}_{F_i} =: A_{1i}$ und $\mathcal{O}_{X_i}(U_{2i}) = \mathrm{Cl}(K[x_i^{-1}], F_i) = \mathcal{O}_{F_i,\infty} =: A_{2i}$. Ist $X = X_1 \times X_2$, so können wir nach [Har77, Theorem 3.3, p. 87],

$$\bigcup_{1\leq j,k\leq 2} \mathrm{Spec}(A_{j1} \otimes_K A_{k2}) \tag{2.19}$$

als offene Überdeckung von $X = X_1 \times X_2$ wählen.

Sei $\Omega_0^i := \{\omega_{i1}, ..., \omega_{in_i}\}$ eine Basis der endlichen Maximalordnung $\mathcal{O}_{F_i}$ von F_i/K und $\Omega_\infty^i := \{\mu_{i1}, ..., \mu_{in_i}\}$ eine Basis der unendlichen Maximalordnung $\mathcal{O}_{F_i,\infty}$ von F_i/K. Dann lassen sich genau die Polstellen von (x_i) nicht als Ideale in $\mathcal{O}_{F_i}$ darstellen, und umgekehrt sind es genau die Nullstellen von (x_i), welche sich nicht als Ideale in $\mathcal{O}_{F_i,\infty}$ darstellen lassen. Jeder Divisor von F_i besitzt dann eine Darstellung mit gebrochenen Idealen aus $\mathcal{O}_{F_i}$ und $\mathcal{O}_{F_i,\infty}$. Mit [Hes02, Corollary 4.3 and Corollary 4.4, p. 6] wissen wir, dass wir spezielle Basen Ω_0^i und Ω_∞^i so wählen können, dass die Übergangsmatrizen $M_i \in K(x_i)^{n_i \times n_i}$ zwischen diesen beiden Basen jeweils Diagonalmatrizen und die Diagonalelemente von der Form $x_i^{m_{ij}}$ mit $m_{ij} \in \mathbb{Z}$ sind. Zwar wird hier als unendliche Maximalordnung ein semi-lokaler Ring betrachtet, da aber solch eine Übergangsmatrix in Diagonalform die Ganzheit der Basiselemente nur für die Null- und Polstellen des Hauptdivisors (x_i) abändert, könnnen wir die Aussagen leicht modifiziert auf unseren Fall anwenden.

Insgesamt erhalten wir vier Ringe $S_1 := \mathcal{O}_{F_1} \otimes_K \mathcal{O}_{F_2}$, $S_2 := \mathcal{O}_{F_1} \otimes_K \mathcal{O}_{F_2,\infty}$, $S_3 := \mathcal{O}_{F_1,\infty} \otimes_K \mathcal{O}_{F_2}$ und $S_4 := \mathcal{O}_{F_1,\infty} \otimes_K \mathcal{O}_{F_2,\infty}$. Um diese Ringe als affine Varietäten zu erzeugen, konstruieren wir uns spezielle Ideale $I_{\Omega_0^i}$ und $I_{\Omega_\infty^i}$. Für die Basis von $\mathcal{O}_{F_i}$ erzeugen wir das Ideal

$$I_{\Omega_0^i} := \langle \omega_{ij}\omega_{ik} - \sum_{l=1}^{n_i} \lambda_{\omega_{il}}^{jk} \omega_{il} \mid k, j = 1, ..., n_i \rangle, \tag{2.20}$$

mit dem die Isomorphie $\mathcal{O}_{F_i} \cong K[x_i, \omega_{i1}, ..., \omega_{in_i}]/I_{\Omega_0^i}$ folgt, wobei hier mit $R_{i,0} := K[x_i, \omega_{11}, ..., \omega_{1n_1}]$ ein Polynomring in $x_i, \omega_{i1}, ..., \omega_{in_i}$ gemeint ist. Analog erhalten wir

$$I_{\Omega_\infty^i} := \langle \mu_{ij}\mu_{ik} - \sum_{l=1}^{n_i} \nu_{\mu_{il}}^{jk} \mu_{il} \mid k, j = 1, ..., n_i \rangle \tag{2.21}$$

und die Isomorphie $\mathcal{O}_{F_i,\infty} \cong K[\frac{1}{x_i}, \mu_{i1}, ..., \mu_{in_i}]/I_{\Omega^i_\infty}$ sowie $R_{i,\infty}$. Für den Ring S_1 betrachten wir nun die Isomorphie

$$S_1 \cong K[x_1, \omega_{11}, ..., \omega_{1n_1}, x_2, \omega_{21}, ..., \omega_{2n_2}]/\langle I_{\Omega^1_0}, I_{\Omega^2_0}\rangle \ , \tag{2.22}$$

und Analoges gilt für die verbleibenden Ringe S_2, S_3 und S_4.

Wir fassen nun die $I_{\Omega^i_0}$ als Ideale der Polynomringe $R_{i,0}$ und die $I_{\Omega^i_\infty}$ als Ideale der Polynomringe $R_{i,\infty}$ auf $(i = 1, 2)$. Die affinen Kurven

$$\tilde{C}_{i,0} := V(I_{\Omega^i_0}) \text{ und } \tilde{C}_{i,\infty} := V(I_{\Omega^i_\infty})$$

sind jeweils nicht-singulär, da per Konstruktion die lokalen affinen Koordinatenringe jeweils diskrete Bewertungsringe sind. Mittels [Har77, Theorem 6.9, p. 44] können wir zeigen, dass es jeweils eine nicht-singuläre projektive Kurve $\tilde{X}_i$ gibt, welche $\tilde{C}_{i,0}$ und $\tilde{C}_{i,\infty}$ als offene Überdeckung besitzt. Mit [Har77, Corollary 4.5, p. 26] erhalten wir, dass die projektiven Kurven X_i und $\tilde{X}_i$ birational äquivalent sind, woraus folgt, dass die projektiven Flächen $X_1 \times X_2$ und $\tilde{X}_1 \times \tilde{X}_2$ birational äquivalent sind.

Sei nun $C \in \mathrm{Div}(X_1 \times X_2)$ eine Korrespondenz. Wir nutzen die Überdeckung (2.19) von $X_1 \times X_2$, mit deren Hilfe folgt, dass wir eine Korrespondenz C in allen vier Ringen S_j $(j = 1, 2, 3, 4)$ als Verschwindungsmenge $C_{S_j} := V(I_{C_j})$ jeweils geeigneter Ideale $I_{C_j} \subseteq S_j$ darstellen können. Um die Ideale I_{C_j} mit $j = 1, 2, 3, 4$ zu bestimmen, genügt es z.B. eine Darstellung I_{C_1} von C im Ring S_1 zu kennen. Wollen wir dann I_{C_2} berechnen, so betrachten wir den Oberring $S_{1,2} := S_1[U_2^{-1}]$ von S_1 und S_2, wenn $U_2 := \{x_2^j \mid j \in \mathbb{Z}^{\geq 0}\}$ die von x_2 erzeugte multiplikative Halbgruppe ist. In diesem Ring ist auf Grund unserer speziellen Wahl der jeweiligen Ganzheitsbasen sowohl das Ideal I_{C_1} als auch das Ideal I_{C_2} enthalten. Wir berechnen dann I_{C_2}, indem wir I_{C_1} als Ideal in $S_1[U_2^{-1}]$ auffassen und dann mit S_2 schneiden. Völlig analog können wir Oberringe $S_j[U_1^{-1}]$ mit $U_1 := \{x_1^j \mid j \in \mathbb{Z}^{\geq 0}\}$ oder $S_j[U_{1,2}^{-1}]$ mit $U_{1,2} := \{x_1^j x_2^l \mid j, l \in \mathbb{Z}^{\geq 0}\}$ betrachten. Ist z.B. j gleich eins, so ist $S_1[U_1^{-1}]$ ein gemeinsamer Oberring von S_1 und S_3 und $S_1[U_{1,2}^{-1}]$ ein Oberring von S_1, S_2, S_3 und S_4. Ist $J \subseteq \{1, 2, 3, 4\}$, so bezeichnen wir mit S_J einen gemeinsamen Oberring der Ringe S_j mit $j \in J$. Um den Schnitt zweier Korrespondenzen zu berechnen, benötigen wir noch ein Korollar aus [Cox05, Corollary 2.5, p. 150].

Korollar 2.20. *Sei K ein algebraisch abgeschlossener Körper und I ein nulldimensionales Ideal von $R := K[x_1, ..., x_n]$. Sind $P_1, ..., P_m \in V(I)$ paarweise verschieden und bezeichnen die $\mathcal{O}_i$ die Lokalisierungen von R nach den maximalen Idealen $I(P_i)$, so gilt*

$$\dim K[x_1, ..., x_n]/I = \sum_{i=1}^{m} \dim \mathcal{O}_i/I\mathcal{O}_i.$$

Seien nun $C, D \in \mathrm{Div}(X_1 \times X_2)$ ohne gemeinsamen Träger und $j \in J$. Wir wollen dann die K-Dimension von $C \cap D$ im Ring S_J, als affine Varietät des Rings S_J aufgefasst, mit

$$s_J := \dim_{S_J}(C \cap D) := \dim_K S_J / \left(I_{C_j} + I_{D_j} \right) \quad (j \in J)$$

bezeichnen. Nun können wir den Schnitt zweier Korrespondenzen wie im folgendem Lemma berechnen:

Lemma 2.21. *Sei $X := X_1 \times X_2$ eine nicht-singuläre projektive Fläche und $C, D \in \mathrm{Div}(X)$ zwei Korrespondenzen ohne gemeinsamen Träger. Dann gilt*

$$C.D = \sum_{i=1}^{4} s_{\{i\}} - \left(s_{\{1,2\}} + s_{\{2,3\}} + s_{\{3,4\}} + s_{\{4,1\}} \right) + s_{\{1,2,3,4\}}. \tag{2.23}$$

Beweis. Wir machen zuerst die Annahme, dass C und D Primdivisoren sind. Da C und D keine gemeinsame Komponente besitzen, sind alle Dimensionen s_I ($I \subseteq \{1,2,3,4\}$) endlich. Berechnen wir $s_{\{1\}} + s_{\{2\}}$, so zählen wir die Schnittmultiplizität der Punkte in $s_{\{1,2\}}$ doppelt. Wir müssen also $s_{\{1\}} + s_{\{2\}} - s_{\{1,2\}}$ berechnen, um die Schnittmultiplizität von C und D in $V(S_1) \cup V(S_2)$ zu erhalten. Als Nächstes addieren wir $s_{\{3\}}$ hinzu. Um nicht wieder doppelt zu zählen, müssen wir $s_{\{2,3\}} + s_{\{1,3\}}$ subtrahieren und $s_{\{1,2,3\}}$ wieder addieren und erhalten die Schnittmultiplizität in $\bigcup_{j=1}^{3} V(S_j)$. Schließlich addieren wir $s_{\{4\}}$, ziehen $s_{\{3,4\}} + s_{\{4,1\}}$ ab und addieren wieder $s_{\{1,3,4\}}$. Damit erhalten wir unter der Beachtung, dass $s_{\{1,2,3\}} + s_{\{1,3,4\}} - s_{\{1,3\}} = s_{\{1,2,3,4\}}$ ist, die Schnittmultiplizität von C und D auf $\bigcup_{j=1}^{4} V(S)_j$ wie in (2.23). Sind nun C und D beliebige Divisoren ohne gemeinsame Komponenten, so berechnen wir $C.D$ durch $\mathbb{Z}$-lineare Fortsetzung in beiden Eingängen der Paarung. □

Ist mindestens einer der beiden Korrespondenzen C und D in G, so wenden wir folgendes Lemma aus ([Smi05, Proposition 4.1.7]) an:

Lemma 2.22. *Seien $C, D \in Div(X)$ Korrespondenzen. Ist $C \in G$, wobei G wie in 2.17 definiert ist, so gilt*

$$C.D = d_1(C)d_2(D) + d_2(C)d_1(D). \tag{2.24}$$

Mit Hilfe der Schnittpaarung können wir eine weitere Paarung einführen, die **Korrespondenzpaarung**, mittels

$$\mathrm{Div}(X_1 \times X_2)^2 \longrightarrow \mathbb{Z}, \tag{2.25}$$

$$(C, D) \longmapsto \langle C, D \rangle := (\, d_1(C)d_2(D) + d_2(C)d_1(D) \,) - C.D \, ,$$

für die Folgendes gilt ([Smi05, Theorem 5.1.2]):

Satz 2.23. *Die Korrespondenzpaarung in (2.25) ist symmetrisch, bilinear und invariant auf den homomorphen Äquivalenzklassen. Ferner wird durch die Paarung auf der Menge der numerisch äquivalenten Korrespondenzklassen eine positiv-definite Paarung definiert.*

Für die Einheitskorrespondenz Δ_{X_1} und die Frobeniuskorrespondenz $\mathfrak{F}_X^r$ auf der Fläche $X = X_1 \times X_1$ hat der Selbstschnitt und die Korrespondenzpaarung nun folgende Werte (s. [Smi05, p. 54 and p. 59-60]):

Lemma 2.24. *Für die Korrespondenzen Δ_{X_1} und $\mathfrak{F}_{X_1}^r$ mit $r \in \mathbb{Z}^{\geq 0}$ erhalten wir folgende Werte für die Schnitt- und Korrespondenzpaarung, wobei $g = g_{X_1}$ das Geschlecht von X_1 bezeichnet:*

(i) $\Delta_{X_1}.\Delta_{X_1} = 2 - 2g,$

(ii) $\langle \Delta_{X_1}, \Delta_{X_1} \rangle = 2g,$

(iii) $\mathfrak{F}_{X_1}^r.\Delta_{X_1} = \#X_1(\mathbb{F}_{q^r}),$

(iv) $\langle \mathfrak{F}_{X_1}^r, \mathfrak{F}_{X_1}^r \rangle = 2gq^r,$

(v) $\langle \mathfrak{F}_{X_1}^s, \mathfrak{F}_{X_1}^r \rangle = q^r + q^s - q^r \#X(F_{q^{s-r}})$, *wobei $s > r$ gilt und*

(vi) $\langle \mathfrak{F}_{X_1}^r, \Delta_{X_1} \rangle = 1 + q^r - \#X(F_{q^r}),$

wobei $\#X_1(\mathbb{F}_{q^r})$ die Anzahl der $\mathbb{F}_{q^r}$-rationalen Punkte von $X_1/\mathbb{F}_q$ bezeichnet.

Als Nächstes wollen wir zeigen, wie wir nun eine Schnittpaarung auf $\mathcal{D}_{L/F_2}$ einführen können. Sei $P \in \mathbb{P}_{L/F_2}$ und $U_i := 1 \otimes K[x_i]^\times$. Dann erhalten wir mittels der Einbettung

$$\iota : S_1 \longrightarrow \mathcal{O}_{F_1} \otimes F_2$$

die Isomorphie $S_1[U_2^{-1}] \cong \mathcal{O}_{F_1} \otimes F_2$ von K-Algebren. Analog erhalten wir mittels der Einbettung

$$\iota_\infty : S_3 \longrightarrow \mathcal{O}_{F_{1,\infty}} \otimes F_2$$

die Isomorphie $S_3[U_2^{-1}] \cong \mathcal{O}_{F_{1,\infty}} \otimes F_2$. Seien die K-Algebrenisomorphismen $\Phi : \mathcal{O}_{F_1} \otimes_K F_2 \longrightarrow \mathcal{O}_{L/F_2}$ und $\tilde{\Phi} : \mathcal{O}_{F_{1,\infty}} \otimes_K F_2 \longrightarrow \mathcal{O}_{L/F_{2,\infty}}$ wie in Lemma 1.19 gegeben. Ist $P_0 \in \mathcal{O}_{L/F_2}$ ein nicht-triviales Ideal, so definieren wir

$$I_{P_1} := \iota^{-1}(\Phi^{-1}(P_0)) \in S_1, \tag{2.26}$$

wobei mit ι^{-1} das Urbild von ι gemeint ist. Ansonsten sei $P_0 \in \mathcal{O}_{L/F_{2,\infty}}$ ein nicht-triviales Ideal, und wir definieren

$$I_{P_3} := \iota_\infty^{-1}(\tilde{\Phi}^{-1}(P_0)) \in S_3.$$

Damit können wir, wie bereits erläutert wurde, die jeweils restlichen Ideale I_{P_j} mit $j = 1, 2, 3, 4$ berechnen. Bei beliebigen effektiven Divisoren von $\mathcal{D}_{L/F_2}$ wenden wir die Vorschrift auf jeden Primdivisor an. Sind nun $A, B \in \mathcal{D}_{L/F_2}$ effektive Divisoren, so berechnen wir jeweils die Ideale I_{A_j} und I_{B_j}. Damit können wir auf $\mathcal{D}_{L/F_2}$ eine bilineare Paarung durch

$$A.B := \sum_{i=1}^{4} s_{\{i\}} - \left(s_{\{1,2\}} + s_{\{2,3\}} + s_{\{3,4\}} + s_{\{4,1\}}\right) + s_{\{1,2,3,4\}}$$

wie in Lemma 2.21 definieren, wenn wir zusätzlich noch $A.(-B) := -(A.B)$ und $(-B).A := -(A.B)$ setzen.

Damit allerdings Hauptdivisoren (F) von L/F_2 auf Hauptdivisoren von $X_1 \times X_2$ abgebildet werden müssen wir noch einiges tun. Als erstes brauchen wir noch einige weitere Einbettungen wie

$$\kappa : S_1 \longrightarrow F_1 \otimes \mathcal{O}_{F_2}$$

und

$$\kappa_\infty : S_2 \longrightarrow F_1 \otimes \mathcal{O}_{F_{2,\infty}},$$

welche die Isomorphien $S_1[U_1^{-1}] \cong F_1 \otimes \mathcal{O}_{F_2}$ und $S_2[U_1^{-1}] \cong F_1 \otimes \mathcal{O}_{F_{2,\infty}}$ von K-Algebren nach sich ziehen. Ausserdem benötigen wir noch die K-Algebrenisomorphismen

$$\Gamma : F_1 \otimes_K \mathcal{O}_{F_2} \longrightarrow \mathcal{O}_{L/F_1} \quad \text{und } \tilde{\Gamma} : F_1 \otimes_K \mathcal{O}_{F_{2,\infty}} \longrightarrow \mathcal{O}_{L/F_{1,\infty}} .$$

Sei $F \in L/F_2$ von der Form $F = \frac{f}{s}$ mit $f \in \mathcal{O}_{L/F_2}$ und $s \in F_2[x_1]$ geeignet. Wir betrachten nun den allgemeinen Fall, dass F_1 und F_2 nicht isomorph sind. Im Falle, dass F_1 und F_2 isomorph sind, verläuft die Argumentation ähnlich. Auf Grund der Isomorphie zwischen den Divisorengruppen

$$\mathrm{Div}(X)^{nonFib} \oplus \mathrm{Div}(X^t)^{nonFib} \oplus \mathrm{Div}(X_1) \oplus \mathrm{Div}(X_2)$$

und

$$H_{L/F_1} \oplus H_{L/F_2} \oplus C_{L/F_2} \oplus C_{L/F_1}$$

ist sind die Divisoren $A \in \mathcal{D}_{L/F_2}$ und $A^\star$ genau dann Hautdivisoren von L/F_2 und L/F_1, wenn der zu auf der Fläche X zugehörige Divisor ein Hauptdivisor ist. Besitzt also der Hauptdivisor (F) in L/F_2 bzw. in L/F_1 die Darstellung

$$(F) = \sum e_i P_i - \sum f_i Q_i \quad \text{bzw. } (F^\star) = \sum e_i P_i^\star - \sum f_i Q_i^\star$$

mit lauter effektiven Primdivisoren, so erhalten wir also auf der Fläche X die Darstellung

$$(F) = \left(\sum e_i P_i - \sum f_i Q_i\right) + (F^\star)' .$$

Wir haben hier der Einfachheit wegen die Bezeichnungen für die Divisoren der Fläche X beibehalten. Hierbei soll $(F^\star)'$ nur den fibralen Anteil des Divisors $(F^\star)$ von X^t bezeichnen, welcher in $\mathrm{Div}(X_2)$ liegt. Für ein gegebenes $F \in L/F_2$ betrachten wir also jeweils $(F)_0$ und $(F)^\infty$ bzw. in L/F_1 dann $(F)_0^\star$ und $(F)^{\infty\star}$ und machen $(F)_0$ und F^∞ wie oben gezeigt zu Idealen in S_1 und S_3. Analog benutzen wir die oben definierten Einbettungen κ und κ_∞ um aus $(F)_0^\star$ und $(F)^{\infty\star}$ dann Ideale in S_1 und S_2 zu erhalten. Damit können wir dann (F) als Hauptdivisor auf X darstellen. Jedem Hauptdivisor (F) von L/F_2 wird so ein Hauptdivisor auf X zugeordnet, welcher bis auf Isomorphie aus den selben Primdivisoren besteht. Insgesamt folgt nun mit Lemma 2.22, dass die so definierte bilineare Abbildung auf $\mathcal{D}_{L/F_2}$ eine bilineare Abbildung der Divisorenklassen $[A]$ und $[B]$ ist (aber nicht der Korrespondenzklassen $[A]_C$ und $[B]_C$).

Wir wollen nun zeigen, wie wir für eine Korrespondenz $A \in \mathcal{D}_{L/F_2}$ den **Selbstschnitt** $A.A$ berechnen können. Wir nehmen o.B.d.A. dazu an, dass A effektiv ist. Mittels des schwachen Approximationssatzes für den Funktionenkörper L/F_2 können wir ein Element $F \in L/F_2$ so finden, dass $\nu_P(F) = -\nu_P(A)$ ist für $P \in \operatorname{supp} A$. Damit ist dann $\operatorname{supp}(A + (F)) \cap \operatorname{supp} A = \emptyset$, und wir können $A.A$ mittels $(A + (F)).A$ berechnen. Vorher müssen wir uns aber noch überlegen, warum der Schnitt zweier verschiedener Primkorrespondenzen nur endlich viele Punkte enthält. Sind P und Q zwei verschiedene nicht-konstante Primkorrespondenzen aus $\mathbb{P}_{L/F_2}$, so sind die Ideale I_{P_j} und I_{Q_j} ebenfalls prim zueinander. Wir können nun $V(I_{P_j})$ und $V(I_{Q_j})$ als affine Kurven in $V(S_j)$ auffassen. Als Varietäten sind dann $V(I_{P_j})$ und $V(I_{Q_j})$ jeweils irreduzibel. Sei $U := V(I_{P_j}) \cap V(I_{Q_j})$. Die Schnittmenge U muss echt in $V(I_{P_j})$ und $V(I_{Q_j})$ enthalten sein, ansonsten erhalten wir einen Widerspruch. Damit ist aber U eine echte algebraische Teilmenge von jeweils $V(I_{P_j})$ und $V(I_{Q_j})$, was bedeutet, dass $1 = \dim V(I_{P_j}) > \dim U = 0$ ist ([Mil05, Proposition 2.26, p. 41]). Damit kann U nur endlich viele Punkte besitzen.

Mit Hilfe des letzten Satzes und den vorangegangenen Aussagen können wir nun eine Korrespondenzpaarung auf den Korrespondenzklassen $\mathcal{D}_{L/F_2}$ definieren:

Korollar 2.25. *Auf der Menge der Korrespondenzklassen von $\mathcal{D}_{L/F_2}$ lässt sich eine positiv definite bilineare Korrespondenzpaarung einführen.*

Beweis. Ist $P \in \mathbb{P}_{L/F_2}$ nicht konstant, so berechnen wir das Ideal $I_{P_1} \subseteq S_1$ und bezeichnen mit $C_P \in \mathrm{Div}(X_1 \times X_2)$ den projektiven Abschluss von $V(I_{P_1})$ in X. Für die Grade d_1 und d_2 auf der Fläche $X_1 \times X_2$ gilt dann

$$d_2(C_P) = \deg_{L/F_2} P \quad \text{ und } d_1(C_P) = \deg_{L/F_1} P^\star.$$

Für eine beliebige Korrespondenz $A \in \mathcal{D}_{L/F_2}$ mit Primdivisorzerlegung $A = \sum_{j=1}^k n_j P_j$ ist dann $d_2(C_A) = \deg_{L/F_2} A$ und $d_1(C_A) = \deg_{L/F_1} A^\star$. Damit

ist für $A, B \in \mathcal{D}_{L/F_2}$ durch

$$\langle A, B\rangle := \deg A^\star \deg B + \deg A + \deg B^\star - A.B$$

auf Grund von Lemma 2.22 und Satz 2.23 eine bilineare positiv definite Paarung auf den Korrespondenzklassen $[A]_C$ und $[B]_C$ gegeben. □

2.3 Vergleich der Korrespondenzen

Jede Primkorrespondenz $C \in \mathrm{Div}(X)\backslash\mathrm{Fib}(X)$ lässt sich in S_1 mit einem Ideal $I_{C_1} \subseteq S_1$ als irreduzible und reduzierte Varietät $V(I_{C_1})$ beschreiben. Wenden wir darauf $\Phi \circ \iota$ an, so erhalten wir ein nicht-konstantes Primideal $P_0 := \Phi \circ \iota(I_{C_1}) \subseteq \mathcal{O}_{L/F_2}$ mit $P \in \mathbb{P}_{L/F_2}$. Ist andererseits $P \in \mathbb{P}_{L/F_2}$ eine nicht-konstante Primkorrespondenz, so können wir das Ideal I_{P_1} bilden. Das Ideal I_{P_1} ist dann ein Primideal in S_1 und der Abschluss $C \in \mathrm{Div}(X)$ von $V(I_{P_1})$ ist dann eine nicht-fibrale Primkorrespondenz. Damit haben wir folgende einfache Aussage, welche wir ohne Beweis im folgendem Lemma festhalten wollen.

Lemma 2.26. *Die nicht-konstanten und nicht-fibralen Primkorrespondenzen entsprechen einander, d.h. ist $P \in \mathbb{P}_{L/F_2}$ nicht konstant, so ist der projektive Abschluss C von $V(I_{P_1})$ eine nicht-fibrale Primkorrespondenz. Ist andererseits C eine nicht-fibrale Primkorrespondenz und $V(I_{C_1}) \subseteq S_1$ eine affine Darstellung von C in S_1, so ist $\Phi(\iota(I_{C_1})) \in \mathcal{D}_{L/F_2}$ eine nicht-konstante Primkorrespondenz.*

Ist $P \in \mathbb{P}_{L/F_2}$ eine nicht-konstante Primkorrespondenz, so betrachten wir wieder das Diagramm

$$\begin{array}{ccc} & F_{_P} = F_1^* F_2 & \\ \swarrow & & \searrow \\ F_1^* & & F_2 \end{array} \tag{2.27}$$

in dem $F_{_P} := F_{2_{_P}}$ ist. Sei τ_{p_i} die Restklassenabbildung des Primdivisors $p_i \in \mathbb{P}_{F_i/K}$. Der Einfachheit wegen nehmen wir an, dass y_i jeweils ganz ist über x_i und die X_i ebene nicht-singuläre Kurven sind, d.h. es ist $X_i \subseteq \mathbb{P}^2$ mit affinem Teil $\mathcal{C}_i : f_i(x_i, y_i) = 0$, wobei $f_i \in K[x_i, y_i]$ irreduzibel ist. Im Allgemeinen darf die Kurve X_i aber durchaus singulär sein. Der singuläre Fall würde aber nur ein Mehraufwand an Notation bedeuten. Ist $p_i \in \mathbb{P}_{F_i/K}$ mit $\nu_{p_i}(x_i) \geq 0$ und endlichem Primideal $p_{i,0} = \langle x_i - \alpha_i, y_i - \beta_i\rangle$ in Zwei-Element Darstellung, so können wir p_i durch $p_i \longmapsto (x_i(p_i), y_i(p_i))) = (\alpha_i, \beta_i) \in K^2$ in eindeutiger Weise einen Punkt aus K^2 mit $f_i(\alpha_i, \beta_i) = 0$ zuordnen. Die endlich vielen Polstellen von x_i lassen wir hier jeweils außer Acht. Ist $C \in \mathrm{Div}(X)$ eine

nicht-fibrale Primkorrespondenz, so betrachten wir die dazugehörige nichtkonstante Primkorrespondenz $P \in \mathbb{P}_{L/F_2}$ mit $P_0 = \Phi \circ \iota(I_{C_1})$. Nun gilt für ein $p_2 \in \mathbb{P}_{F_2/K}$ mit $\nu_{p_2}(x) \geq 0$

$$\sum_{i=1}^{n}(\alpha_{1i}, \beta_{1i}) := \pi_{1|C_*} \circ {\pi_{2|C}}^* (x_2(p_2), y_2(p_2))$$

und weiter mit

$$\sum_{i=1}^{n} p_{1i} := P(p_2) = {\pi_{P|F_1}}^{-1} \left(N_{F_P/F_1^*}(\mathrm{Con}_{F_P/F_2}(p_2)) \right) \quad \left(p_{1i} \in \mathbb{P}_{F_1/K}\right)$$

schließlich

$$\sum_{i=1}^{n}(x_1(p_{1i}), y_1(p_{1i})) = \sum_{i=1}^{n}(\alpha_{1i}, \beta_{1i}).$$

Die Zurückziehung ${\pi_{2|C}}^*$ entspricht hier der Hochhebung Con_{F_P/F_2}, und die Fortsetzung $\pi_{1|C_*}$ ist nichts anderes als die Norm ${\pi_{P|F_1}}^{-1} \circ N_{F_P/F_1^*}$. Dass jeweils für die Bilder $\nu_{p_{1i}}(x_i) \geq 0$ gilt, können wir erreichen, indem wir den Restidealsatz anwenden. Dabei müssen wir wieder endlich viele Primdivisoren aus jeweils $\mathbb{P}_{F_i/K}$ ausschließen. Per Definition sind dann die Bilder Summen von Vielfachen von Primdivisoren aus F_1, die sämtlich keine Poldivisoren von x_1 sind. Wir können nun folgendes einfaches Lemma ohne Beweis formulieren:

Lemma 2.27. *Eine nicht-konstante Primkorrespondenz von L/F_2 induziert denselben Homomorphismus zwischen J_{X_2} und J_{X_1} wie die dazugehörige nicht-fibrale Primkorrespondenz auf X.*

Dabei spielt es keine Rolle, dass wir jeweils endlich viele Primdivisoren außer Acht gelassen haben, denn wir können einen Repräsentanten von $\mathcal{C}^0_{F_i/K}$ immer so abändern, dass keiner der endlich vielen Ausnahmedivisoren vorkommt. Jede Korrespondenz $C \in \mathrm{Div}(X_1 \times X_2)$ induziert also einen Homomorphismus $J_{X_2} \longrightarrow J_{X_1}$ von Jacobischen. Das Umgekehrte ist ebenfalls der Fall ([Smi05, Lemma 3.3.11, p. 40]):

Lemma 2.28. *Sei $\phi \in \mathrm{Hom}(J_{X_2}, J_{X_1})$, dann existiert eine Korrespondenz Γ_ϕ aus $\mathrm{Div}(X_1 \times X_2)$, so dass $\pi_{1|\Gamma_\phi *} \circ {\pi_{2|\Gamma_\phi}}^* = \phi$ ist.*

Damit wissen wir auch, dass jeder Homomorphismus von J_{X_2} nach J_{X_1} durch eine Korrespondenz $[A]_C \in \mathrm{Cor}\,(F_2, F_1)$ induziert wird. Wir können damit also sämtliche Homomorphismen von J_{X_2} nach J_{X_1} mittels Korrespondenzklassen $\mathrm{Cor}\,(F_2, F_1)$ beschreiben, wobei anzumerken ist, dass sich die fibralen und die konstanten Divisoren entsprechen. Wir halten diese einfache Feststellung im folgendem Lemma ohne Beweis fest.

Lemma 2.29. *Jeder Homomorphismus $\phi \in \mathrm{Hom}(J_{X_2}, J_{X_1})$ wird durch eine Korrespondenzklasse $[A]_C$ aus $\mathrm{Cor}\,(F_2, F_1)$ induziert, d.h. es gilt $\phi(p) = A(p)$ für alle $p \in J_{X_2}$.*

Sei $k := \mathbb{F}_q$ ein endlicher Körper. Mit $X_i(k)$ bezeichnen wir die k-rationalen Punkte der Kurven X_i und mit $J_{X_i}(k)$ die k-rationalen Punkte von J_{X_i}. Sei $X_1 = X_2$, X_2/k Kurve über k, F_2/k der Funktionenkörper von X_2/k und K/k eine endliche Erweiterung. Mit

$$\mathrm{End}_K(J_{X_2}) := \mathrm{Cor}\,(F_2K/K)$$

bezeichnen wir die K-Endomorphismen der Jacobischen J_{X_2}.

Prinzipale Polarisierung

Mit K sei wieder der algebraishe Abschluss eines endlichen Körpers bezeichnet.Im Folgenden wollen wir kurz auf den Begriff der prinzipalen Polarisierung eingehen. Seien A und B abelsche Varietäten. Für $a \in A$ definieren wir die Abbildung $\iota_a : B \longrightarrow A \times B,\ b \longmapsto (a, b)$ und analog definieren wir für $b \in B$ eine Abbildung $\iota_b : A \longrightarrow A \times B,\ a \longmapsto (a, b)$. Wir nennen A und B **dual** zueinander, wenn es eine Divisorenklasse $\mathcal{P} \in \mathrm{Pic}(A \times B)$ gibt, so dass die Abbildungen $A \longrightarrow \mathrm{Pic}(B),\ a \longmapsto \iota_a^*(\mathcal{P})$ und $B \longrightarrow \mathrm{Pic}^0(A),\ b \longmapsto \iota_b^*(\mathcal{P})$ Bijektionen sind. Für die Existenz solcher dualen Varietäten und Divisorenklassen $\mathcal{P}$ siehe [Hin91]. Die zu A duale abelsche Varietät bezeichnen wir mit $\hat{A}$. Bezeichnen wir mit $t_a : A \longrightarrow A,\ x \longmapsto x + a$ die Translation um a, so definiert die Abbildung $\Phi_c : A \longrightarrow \mathrm{Pic}^0(A),\ a \longmapsto t_a^*(c) - c$ mit $c \in \mathrm{Pic}(A)$ einen Gruppenhomomorphismus. Wenn der Kern $K(c)$ von Φ_c endlich ist, so induziert dies sogar eine Isogenie $\Phi_c : A \longrightarrow \hat{A}$. Solch eine Isogenie wollen wir **Polarisierung** nennen. Gilt $K(c) = 0$, so sprechen wir von einer **prinzipalen Polarisierung**. Somit ist durch $c \in \mathrm{Pic}(A)$ mit $\Phi_c : A \longrightarrow \hat{A}$ eine prinzipale Polarisierung gegeben, wenn Φ_c ein Isomorphismus ist ([Hin91, p. 130]).

Die Jacobische J_X einer Kurve X ist ein Beispiel für eine prinzipal polarisierte abelsche Varietät. Eine Kurve X vom Geschlecht ≥ 1 kann immer in ihre Jacobische J_X eingebettet werden, wenn es eine Stelle vom Grad eins gibt, und zusätzlich gilt die Isomorphie $J_X \cong \mathrm{Pic}^0(X)$. Die Jacobische J_X einer Kurve X hat die Dimension $\dim_{J_X} = g_X$, d.h. das Geschlecht der Kurve ist die Dimension der zugehörigen Jacobischen.

Für einen gegebenen Homomorphismus $\phi : A \longrightarrow B$ gibt es einen **dualen Homomorphismus** $\hat{\phi} : \hat{B} \longrightarrow \hat{A}$. Sind $\lambda_i : J_{X_i} \longrightarrow \hat{J}_{X_i}$ die prinzipalen Polarisierungen der Jacobischen J_{X_i} und $\phi \in \mathrm{Hom}(J_{X_1}, J_{X_2})$, so wollen wir $\lambda_{X_1}^{-1} \circ \hat{\phi} \circ \lambda_{X_2} : J_{X_2} \longrightarrow J_{X_1}$ den **Rosati** von ϕ nennen. Die Abbildung

$$\dagger : \mathrm{Hom}(J_{X_1}, J_{X_2}) \longrightarrow \mathrm{Hom}(J_{X_2}, J_{X_1}),\ \phi \longmapsto \lambda_{X_1}^{-1} \circ \hat{\phi} \circ \lambda_{X_2}$$

nennen wir **Rosati-Involution**. Durch die Transponierte C^t einer Korrespondenz $C \in \mathrm{Div}(X_1 \times X_2)$ können wir eine Involution

$$^t : \mathrm{Hom}(J_{X_1}, J_{X_2}) \longrightarrow \mathrm{Hom}(J_{X_2}, J_{X_1})$$

definieren, und es lässt sich zeigen, dass $\phi^t = \dagger(\phi)$ ist für $\phi \in \mathrm{Hom}(J_{X_1}, J_{X_2})$ (s. [Smi05, Proposition 3.3.17., p.42]).

Seien $C, D \in \mathrm{Div}(X_1 \times X_1)$ und $A, B \in \mathcal{D}_{L/F_2}$ die C bzw. B entsprechenden algebraischen Korrespondenzen. Es ist nun möglich, die Werte der Korrespondenzpaarung direkt zu berechnen durch

$$\langle C, \Delta_{X_1} \rangle = \mathrm{Tr}_{\mathrm{End}(J_{X_1}) \otimes \mathbb{Q}/\mathbb{Q}} \left(\Phi(C) \right),$$

der sogenannten **Spurformel** von C, wobei hier Φ wie in (2.16) ist. Für die Korrespondenzen C und D lässt sich der Wert $\langle C, D \rangle$ mit Hilfe der Spurformel durch

$$\langle C, D \rangle = \mathrm{Tr}_{\mathrm{End}(J_{X_1}) \otimes \mathbb{Q}/\mathbb{Q}} \left(\Phi(C) \circ \Phi(D)^t \right), \tag{2.28}$$

berechnen, wie z.B. in [Smi05, Theorem 5.4.4., p. 60] zu finden ist. Damit erhalten wir dann

$$\langle A, B \rangle = \mathrm{Tr}_{\mathrm{End}(J_X) \otimes \mathbb{Q}/\mathbb{Q}} \left(\alpha \circ \beta^\star \right),$$

wobei wir die den Korrespondenzen A und B entsprechenden Endomorphismen mit α und β bezeichnet haben und $\beta^\star$ der Endomorphismus ist, welcher der Korresponenz $B^\star$ entspricht.

Kapitel 3

Algorithmen für Korrespondenzen

In diesem Kapitel werden die gesamten Aussagen, Bezeichnungen und Notationen der vorangegangenen Kapitel benutzt. Für die meisten Aussagen die algebraische Geometrie und abelschen Varietäten betreffend stützen wir uns auf [Har77], [Mum70] ,[Gee07], [Mil98], [Mil05], [Mil86], [Coh06] und [Oor07]. Für die Algebrentheorie verweisen wir auf [Pie82] und [Deu35]. Für die Idealtheorie in beliebigen Algebren verweisen wir auf [Irv03] und [Deu35]. Eine gute Einführung in die Theorie der Quaternionenalgebren gibt [Kir05]. In dieser Arbeit benötigen wir aber insbesondere die Idealtheorie in zentral einfachen F-Algebren A, wobei $F/\mathbb{Q}$ eine endliche Erweiterung von $\mathbb{Q}$ ist.

In diesem Kapitel sind $\mathcal{C}_1$ und $\mathcal{C}_2$ die zu den regulären und algebraisch unabhängigen Funktionenkörpern F_1/K und F_2/K dazugehörigen affinen Kurven, die durchaus singulär sein können und $K = \mathbb{F}_q$ mit $q = p^n$. Wir halten noch einmal die wichtigsten Eigenschaften der hier vorkommenden Funktionenkörper fest und treffen, solange nichts Anderes festgelegt wird, folgende Verabredung:

1. K bezeichne immer einen endlichen Körper $\mathbb{F}_{p^n}$, K'/K eine endliche Erweiterung von K, und mit $\overline{K}$ bezeichnen wir den algebraischen Abschluss von K.

2. Die definierenden Gleichungen $f_1(x_1, y_1)$ und $f_2(x_2, y_2)$ der Funktionenkörper F_1 und F_2 sollen durch Vertauschen von x_1 mit x_2 und y_1 mit y_2 auseinander hervorgehen. Insbesondere sind F_1 und F_2 damit K-isomorph mittels $\tau : F_1 \longrightarrow F_2,\ (x_1, y_1) \longmapsto (x_2, y_2)$.

3. Es sei immer y_1 ganz über x_1 und y_2 ganz über x_2.

4. Wir fixieren immer Erzeugungen $F_i = K(x_i, y_i)$ $(i = 1, 2)$ sowie $L/F_2 = F_2(x_1, y_1)$ und eine Ganzheitsbasis $\Omega := \{\omega_1, ..., \omega_n\} \subseteq \mathcal{O}_{F_1/K}$ von

$\mathcal{O}_{L/F_2}$. Wir definieren dann ausserdem $N_{L/F_2} := N_{L/F_2(x_1)}$ und genauso $N_{L/F_1} := N_{L/F_1(x_2)}$.

5. Für die Geschlechter gilt $g_{L/F_2} = g_{F_1/K} = g_{F_2/K}$.

6. Für einen Divisor a aus $\mathcal{D}_{F_1/K}$ gilt immer

$$\deg_{L/F_2} \mathrm{Con}_{L/F_1}(a) = \deg_{F_1/K} a$$

7. Die unendlichen Stellen $p_{\infty,i} \in F_i/K$ und $\mathrm{Con}_{L/F_j}(p_{\infty,i}) = P_{\infty,i} \in L/F_j$ sollen jeweils total verzweigt sein. Daraus folgt dann für die Grade $\deg_{F_i/K} p_{\infty,i} = 1 = \deg_{L/F_j} P_{\infty,i}$ $(i, j \in \{1, 2\}, i \neq j)$.

8. Insbesondere folgt aus 7: Ist $A \in \mathcal{D}^0_{L/F_2}$, so gilt: A ist genau dann Hauptdivisor, wenn der endliche Teil A_0 ein gebrochenes Hauptideal in $\mathcal{O}_{L/F_2}$ ist.

9. Sämtiche Ideale werden, wenn nichts anderes festgelegt wird, in Zwei-Element-Darstellung angegeben.

3.1 Multiplikation der Korrespondenzen

In diesem Abschnitt widmen wir uns der Arithmetik der Korrespondenzen. Für Korrespondenzen $A, B \in \mathcal{D}_{L/F_2}$ ist die Addition nichts weiter als die Addition von Divisoren. Nehmen wir an, dass F_1/K und F_2/K nun mittels τ wie oben isomorph sind, so erhalten wir die definierende Gleichung für F_2 durch Austauschen von x_1 mit x_2 und y_1 mit y_2 in der definierenden Gleichung für F_1. In diesem Falle ist der Rosati, angewandt auf ein Element aus L/F_2, nichts weiter als das Vertauschen von x_1 mit x_2 und y_1 mit y_2. Der Rosati, angewandt auf eine Korrespondenz A, ist dann nichts weiter als der zugehörige Divisor des gebrochenen Ideales $(A^\star)_0$ von $\mathcal{O}_{L/F_2}$, das wir erhalten, wenn wir den Rosati auf die Erzeuger von A_0 anwenden. Allerdings müssen wir hier erst A_0 als ein gebrochenes Ideal in $\mathcal{O}_{L/F_2}[K[x_1]^{\times -1}]$ auffassen, dann die Vertauschung der Variablen bei den Basiselementen von A_0 vornehmen und schließlich Urbilder berechnen, so dass wir wieder ein gebrochenes Ideal in $\mathcal{O}_{L/F_2}$ haben. Das Produkt von $A \cdot B$ berechnen wir wie folgt:

Sei (F) ein Hauptdivisor von L/F_2. Aus Satz 2.3 wissen wir, dass für die Korrespondenzen $A \in \mathcal{D}_{L/F_2}$ nun $[A \cdot (F)]_C = [0]_C$ und $[(F) \cdot A]_C = [0]_C$ gilt. Ist nun $P \in \mathcal{D}_{L/F_2}$ eine nicht-konstante separable Primkorrespondenz, d.h. also F_P/F_2 ist separabel, so betrachten wir den Zerfällungskörper E von F_P/F_2 und bezeichnen mit L' den Körper F_1E/E. Nun zerfällt $\mathrm{Con}_{L'/L}(P) = \sum_i Q_i$ in lauter Primkorrespondenzen vom Grad 1 in L'. Sei nun $Q := Q_i$ eine der in $\mathrm{Con}_{L'/L}(P)$ auftretenden Primkorrespondenzen. Wir wenden nun

$\tau_{Q_{|F_1}} \circ \tau^{-1}$ auf die Koeffizienten der Erzeuger des Ideales A_0 an und erhalten ein Ideal A_i von $\mathcal{O}_{L'/L}$. Hierbeit ist τ_Q wie in (1.14). Schließlich bilden wir das Produkt von Idealen $I := \prod A_i$ und erhalten ein Ideal $I \subseteq \mathcal{O}_{L/F_2}$.

Ist $P \in \mathcal{D}_{L/F_2}$ eine nicht-konstante inseparable Primkorrespondenz, so ist nach Lemma 2.10 $P = F^{\star n} \cdot B$ mit einer Primkorrespondenz B und einem geeigneten $n \in \mathbb{N}$. Hierbei ist $F^\star$ der Rosati der Frobeniuskorrespondenz. Da aber $\deg_{L/F_2}(F^{\star n} \cdot B) = q^n \deg_{L/F_2}(B)$ ist und P und B effektiv sind, gibt es ein maximales $m \in \mathbb{N}$ so, dass dann $P = F^{\star m} \cdot \tilde{B}$ ist mit $\tilde{B} \in \mathcal{D}_{L/F_2}$ effektiv und separabel. Da sämtliche nicht-konstante Primkorrespondenzen nach Lemma 1.18 keine Differententeiler sein können, ist für eine nicht-konstante inseparable Primkorrespondenz P der Restklassenkörper $F_P := \mathcal{O}_P/P$ nicht inseparabel über $F_2[x_1]/(G)$, wenn $G^f := N_{L/F_2}(P_0)$ ist und f der Trägheitsgrad von P ist. Sei $z_2 := \sqrt[q^m]{x_2}$. Zerlegt sich G in $F_2(z_2)[x_1]$ in das Produkt $G = H^{q^m}$ mit einem separablen Primpolynom $H \in F_2(z_2)[x_1]$, so berechnen wir den Zerfällungskörper $E/F_2(z_2)$ von H. In $L' := F_1E/E$ zerlegt sich dann P in $\mathrm{Con}_{L'/L}(P) = q^m \sum_{i=1}^{l} Q_i$ mit Grad $\deg_{L'/E}(Q_i) = 1$, wenn l der Separabilitätsgrad von E/F_2 und $L = F_1F_2$ ist. Wir erhalten dann $A \cdot B$ durch die Berechnung von $q^m(\sum_i A \cdot Q_i)$, wobei die Berechnung von $A \cdot Q_i$ der separable Fall ist.

Sind nun $B = \sum_{i=1}^{n} e_i P_i$ mit P_i und A gegeben, so berechnen wir dann $A \cdot B = \sum e_i (A \cdot P_i)$. Hierbei reicht es, sich auf effektive Korrespondenzen A und B zu beschränken, da z.B. in der Klasse $[A]_C$ ein effektiver Repräsentant $\tilde{A}$ so gefunden werden kann, das $A = \tilde{A} + lP_{\infty,1} + (F)$ mit einem geeigneten $l \in \mathbb{Z}$ und Hauptdivisor (F) von L/F_2. Wir können nun unseren Algorithmus formulieren:

Algorithmus 1: Produkt von Korrespondenzen

Input: Effektive Korrespondenzen $A, B \in \mathcal{D}_{L/F_2}$ ohne konstante Komponenten

Output: $D \in [A \cdot B]_C$ mit $D \geq 0$

1.) (Initialisierung)

   (i) Es sei $A_0 = \langle G_i \mid i = 1, ..., [L : F_2] \rangle$, wobei $G_i = \sum g_{ij} x_1^i y_1^j$ eine $F_2[x_1]$-Basis von A_0 aus $K(x_2, y_2)[x_1, y_1]$ ist.

   (ii) Mit F bezeichnen wir die Frobeniuskorrespondenz von L/F_2, mit J_0 das Einsideal von $\mathcal{O}_{L/F_2}$ und mit p die Charakteristik von $K = \mathbb{F}_q$ mit $q = p^n$.

2.) Berechne Zerlegung $B = \sum e_i P_i$ in L/F_2.

3.) (Schleife über i): Berechne Primpolynom $H_i \in F_2(z_2^{(i)})[x_1]$ und die Norm $N_{L/F_2}(P_{i,0}) = (H_i{}^{q^{m_i}})^{f_i} \in F_2(z_2^{(i)})[x_1]$ mit m_i maximal. Ist $m_i = 0$, so gehe zu 4.), ansonsten gehe zu 5.).

4.) (Separabler Teil): Berechne Zerfällungskörper E/F_2 von H und Zerlegung $P_i = \sum Q_j^{(i)}$ in $L' := F_1 E/E$. Bestimme für jedes j Restklassenabbildung $\tau_{Q_j^{(i)}}$ und Ideal

$$I_{j,0}^{(i)} := \left\langle \left(\tau_{Q_j^{(i)}} \circ \tau^{-1}(g_{ij}) \right) x_1^i y_1^j \mid i \in \{1, ..., [L : F_2]\} \right\rangle$$

   in $\mathcal{O}_{L'/E}$ und dann die Produkte von Idealen $I_0^{(i)} := \prod_j I_{j,0}^{(i)} \subseteq \mathcal{O}_{L/F_2}$ und setze $J_0 \longleftarrow J_0 \cdot {I_0^{(i)}}^{e_i}$. Gehe dann wieder zu 3.).

5.) (Inseparabler Teil) Berechne Zerfällungskörper $E/F_2(z_2^{(i)})$ von H. Bestimme die Zerlegung $\mathrm{Con}_{L'/L}(P_i) = q^{m_i} \sum_j Q_j^{(i)}$ und berechne dann für alle j jeweils $I_{j,0}^{(i)} := A \cdot Q_j$ wie in 4.) und setze $J_0 \longleftarrow J_0 (\prod_j I_{j,0}^{(i)})^{q^{m_i} e_i}$.

6.) (Ende Schleife über i)

7.) Gib das Ideal J_0 als Divisor von L/F_2 zurück und terminiere.

3.2 Korrespondenzen als Homomorphismen

Wie zum Anfang des Kapitels erwähnt, fixieren wir jeweils Erzeugungen der Funktionenkörper F_1,F_2 und L/F_2 und eine Ganzheitsbasis Ω von $\mathcal{O}_{L/F_2}$. Für einen Repräsentanten a von $[a] \in \mathcal{C}^0_{F_2}$ schreiben wir $a = a_0 - a_\infty$ mit effektiven Divisoren a_0, a_∞. In diesem Abschnitt wollen wir zeigen, wie eine Korrespondenz als Homomorphismus zwischen den Klassengruppen $\mathcal{C}^0_{F_2}$ und $\mathcal{C}^0_{F_1}$ operiert. Dazu verwenden wir den Restidealsatz 2.16. Haben wir eine Korrespondenz A gegeben, welche nur aus nicht-konstanten Primdivisoren besteht, so betrachten wir den endlichen Teil $A_0 = \frac{D_0}{G}$ mit einem ganzen Ideal $D_0 \subseteq \mathcal{O}_{L/F_2}$ und $G \in F_2[x_1]$ geeignet. Als Divisor in L/F_2 geschrieben bedeutet das $A = D + \deg_{L/F_2}(G)_0 P_{\infty,1} - (G)$ mit $D \geq 0$ und einem Hauptdivisor (G) und daher $[A]_C = [D]_C$. Mit Satz 2.3 wissen wir, dass sich A und D als Homomorphismen von $\mathcal{C}^0_{F_2}$ nach $\mathcal{C}^0_{F_1}$ nicht unterscheiden. Wir können uns also immer auf effektive Korrespondenzen ohne konstante Komponenten beschränken. Konstante Korrespondenzen sind nämlich per Definition trivial auf den Klassengruppen vom Grad null, und eine Korrespondenz, welche ein Hauptdivisor ist, bildet jeden Divisor auf einen Hauptdivisor ab und ist somit trivial auf $\mathcal{C}^0_{F_2}$.

Sei nun $P \in \mathbb{P}_{L/F_2}$ ein nicht-konstanter Primdivisor. Nun betrachten wir den endlichen Teil P_0 von P, welcher ein ganzes nicht-konstantes Primideal von $\mathcal{O}_{L/F_2}$ ist. Sei $n := [L : F_2]$. Wir wählen eine Basis von P_0 so, dass die Übergangsmatrix $M \in F_2[x_1]^{n\times n}$ von Ω zur Basis von P_0 Hermite-Normalform hat. Zusätzlich setzen wir noch voraus, dass die Diagonalelemente von M normierte Polynome in $F_2[x_1]$ sind. Die so erhaltene Basis von P_0 wollen wir mit $\mathcal{B} := \{B_k \mid k = 1, ..., n\}$ bezeichnen, wobei $B_k = \sum G^k_{ij} x_1^i y_1^j$ mit $G^k_{ij} \in F_2$ ist. Die Elemente G^k_{ij} können wir dann als $G^k_{ij} = H^k_{ij}/h^k_{ij}$ schreiben mit $h^k_{ij} \in K[x_2]$ und $H^k_{ij} \in \mathcal{O}_{F_2}$. Ist die Basis $\mathcal{B}$ dann p-ganz für einen Primdivisor aus $\mathcal{D}_{F_2/K}$, so ist $\det(M)$ ein normiertes Polynom aus $\mathcal{O}_p[x_1]$ und $\mathcal{B}$ ist damit p-regulär.

In einer geeigneten endlichen Erweiterung K'/K zerfallen dann die sämtlichen Elemente h^k_{ij} von jedem Basiselement B_k in $K'[x_2]$ in Primfaktoren vom Grad 1. Der Divisor $\tilde{c} \in \mathcal{D}_{F_2K'/K'}$ soll nun die Summe aller Primdivisoren von F_2K'/K' sein, die über einem solchen Primfaktor liegen. Schließlich definieren wir dann $\tilde{C} := \tilde{c} + \mathrm{Con}_{F_2K'/F_2}(p_{\infty,2})$. Bei den Elementen der Gestalt $a = a_0 - a_\infty \in \mathcal{C}^0_{F_2}$ können wir uns auf effektive Divisoren $a_0, a_\infty \in \mathcal{D}_{F_2/K}$ beschränken mit

$$\deg_{F_2/K} a_0, \deg_{F_2/K} a_\infty \leq g_{F_2/K}.$$

Nun machen wir noch gegebenenfalls eine $(\deg a_0)!$-Erweiterung K'' von K'. Dann zerfallen a_0 und a_∞ in F_2K''/K'' in lauter Primdivisoren vom Grad

eins und wir definieren

$$C := \{\mathrm{Con}_{F_2K''/F_2K'}(p) \mid p \in \mathrm{supp}(\tilde{C})\} \; . \tag{3.1}$$

Die problematischen Elemente $a = a_0 - a_\infty \in \mathcal{C}^0_{F_2}$ sind dann diejenigen, bei deren Zerlegungen $\mathrm{Con}_{F_2K''/F_2}(a_0) = \sum p_i$ und $\mathrm{Con}_{F_2K''/F_2}(a_\infty) = \sum q_i$ in Stellen vom Grad eins ein Primdivisor aus C auftaucht. Wir können aber dann immer einen Repräsentanten $b_0 - b_\infty \in [a_0 - a_\infty]$ so finden, dass weder in b_0 noch in b_∞ ein Primdivisor von c auftaucht:

Lemma 3.1. *Sei $K = \mathbb{F}_{p^n}$ und F/K ein Funktionenkörper vom Geschlecht $g \geq 1$ mit $F = K(x, y)$. Sei C eine endliche Menge von Stellen in F/K. Ferner sei $[a_0 - a_\infty] \in \mathcal{C}^0_F$ und $a := a_0 - a_\infty$. Dann existiert ein $b_0 - b_\infty \in [a]$ so, dass $(\mathrm{supp}(b_0) \cup \mathrm{supp}(b_\infty)) \cap C = \emptyset$ ist.*

Beweis. Taucht weder in a_0 noch in a_∞ ein Primdivisor von C auf, so ist nichts zu zeigen. Andernfalls sei $S := (\mathrm{supp}(a_0) \cup \mathrm{supp}(a_\infty))$. Nun können wir mit Hilfe des schwachen Approximationssatzes ein Element $f \in F$ so berechnen, dass $\nu_{p_i}(f) = 0$ ist für $p_i \in C \backslash S$ und $\nu_{p_i}(f) = -n_i$, wenn $\nu_{p_i}(a) = n_i$ ist für $p_i \in S$. Damit ist $a + (f) = b_0 - b_\infty$ mit effektiven Divisoren b_0 und b_∞ aus F/K so, dass $(\mathrm{supp}(b_0) \cup \mathrm{supp}(b_\infty)) \cap C = \emptyset$ ist. □

Ist $A = \sum_j e_j P_j \in \mathcal{D}_{L/F_2}$ ein effektiver Divisor ohne konstante Komponente, so wenden wir eben Gesagtes auf jeden Primdivisor P_j von A einzeln an. Zu der berechneten endlichen Menge C von Ausnahmedivisoren aus K'/K kommen nun noch diejenigen aus Lemma 2.14 hinzu. Dazu müssen wir das folgende Lemma beweisen, damit wir wissen, wie wir diese Ausnahmedivisoren berechnen können. **Wir setzen vorerst voraus, dass der Konstantenkörper K der Charakteristik $p > 0$ algebraisch abgeschlossen ist**. Wir betrachten nun wieder einen algebraischen Funktionenkörper E/K und Zwischenkörper K_1/K und K_2/K mit $E = K_1K_2$ und E/K_1 separabel. Ferner sei $\Delta := \{\delta_i \mid i = 1, ..., m\} \subseteq K_2$ eine Basis von E/K_1 mit $m := [E : K_1]$ und D bezeichne die Diskriminante $D := \det \mathrm{Tr}_{E/K_1}(\delta_i\delta_j)$ von Δ. Dann gilt:

Lemma 3.2. *Sei $P \in \mathbb{P}_{E/K}$, $p_1 \in \mathbb{P}_{K_1/K}$ und $p_2 \in \mathbb{P}_{K_2/K}$ mit $P|p_1$ und $P|p_2$. Ferner $C := \bigcup_i \mathrm{supp}(\delta_i)_\infty \cup \mathrm{supp}\,(D)$ und*

$$I_1 := \mathrm{Con}_{E/K_1}(p_1) = \sum e_iQ_i \text{ und } I_2 := \mathrm{Con}_{E/K_2}(p_2) = \sum f_iR_i.$$

Wir definieren $S := \mathrm{supp}\, I_2 \cap \mathrm{supp}\, I_1$ mit $S := \{P_1, ..., P_r\}$, wobei $P_1 := P$ sein soll, und einen Divisor

$$(p_1, p_2) := \sum_{P_i \in S} \min(\nu_{P_i}(I_1), \nu_{P_i}(I_2))P_i$$

in E. Sind dann $p_1, p_2 \notin C$, so gilt $(p_1, p_2) = P$.

Beweis. Seien $p_1, p_2 \notin C$. Als erstes erhalten wir, dass die Hochhebung $I_1 := \mathrm{Con}_{E/K_1}(p_1) = \sum Q_i$ mit paarweise verschiedenen Q_i, da p_1 in E/K_1 nicht verzweigt. Damit ist (p_1, p_2) von der Form $(p_1, p_2) = \sum_{P_i \in S} P_i$. Wir wollen nun zeigen, dass für ein P-ganzes Element $z = \sum a_j \delta_j \in E$ mit $a_j \in K_1$ folgt, dass die a_j stets p_1-ganz sind. Daraus erhalten wir nämlich, dass für ein $z \in E$ dann $\nu_{P_i}(z) \geq 0$ für $\forall P_i \in S$ gilt, sobald $\nu_P(z) \geq 0$ ist und umgekehrt. Dies wiederum bedeutet

$$\mathcal{O}_P = \bigcap \mathcal{O}_{P_i} \ ,$$

woraus dann $P_i = P$ für $i = 1, ..., r$ folgt, also $(p_1, p_2) = P$.

Wir zeigen nun, dass aus $\nu_P(z) \geq 0$ dann $\nu_{p_1}(a_j) \geq 0$ folgt. Da die δ_i nach Voraussetzung p_2-ganz und damit P-ganz sind, ist $z\delta_i$ und $\delta_i\delta_j$ stets P-ganz. Damit sind $\mathrm{Tr}_{E/K_1}(z\delta_1)$ und $\mathrm{Tr}_{E/K_1}(\delta_i\delta_j)$ ebenfalls p_1-ganz. Mittels der Matrix $M := (\mathrm{Tr}_{E/K_1}(\delta_i\delta_j)$ und den Vektoren

$$b := (\mathrm{Tr}_{E/K_1}(z\delta_1), ..., \mathrm{Tr}_{E/K_1}(z\delta_m))^t \text{ und } a = (a_1, ..., a_m)^t$$

erhalten wir ein Gleichungssystem $b = Ma$ mit $\det M = D \neq 0$. Ist $M^{-1} = \frac{M^\sharp}{D}$ mit einer geeigneten $m \times m$-Matrix $M^\sharp$ und p_1-ganzen Einträgen, so erhalten wir, dass die Ausdrücke Da_i $(i = 1, ..., m)$ p_1-ganz sind. Da p_1 nicht in (D) aufgehen kann nach Voraussetzung, sind auch die a_i stets p_1-ganz. □

Lemma 3.2 dient als technisches Hilfsmittel für das folgende Lemma 3.3. Angenommen, wir haben $P_1, P_2 \in \mathbb{P}_{E/K}$ mit $P_1 \neq P_2$, und es gilt sowohl $P_1|p_1, P_1|p_2, P_2|p_1$ und $P_2|\tilde{p}_2$ mit $p_1 \in \mathbb{P}_{K_1/K}\backslash C$ und $p_2, \tilde{p}_2 \in \mathbb{P}_{K_2/K}\backslash C$, wobei C wie in Lemma 3.2 ist. Dann folgt mit Lemma 3.2, dass $p_2 \neq \tilde{p}_2$ gelten muss.

Nun können wir unser eigentliches Lemma formulieren und beweisen:

Lemma 3.3. *Seien die algebraischen Funktionenkörper K_1/K und K_2/K Zwischenkörper des Funktionenkörpers $E = K_1K_2$ und o.B.d.A. sei E separabel über K_1. Ferner sei $\Delta \subseteq K_2$ eine Basis von E/K_1, $[E : K_1] = n$ und $[E : K_2] = m$. Dann gibt es in Abhängigkeit von Δ eine endliche Ausnahmemenge S_2 von Stellen in K_2 und eine endliche Ausnahmemenge S_1 von Stellen in K_1, so dass für alle $p \notin S_2$ und alle $q \notin S_1$ gilt:*

(i) Sei $I_2 := \mathrm{Con}_{E/K_2}(p)$ und $i_2 := N_{E/K_1}(I_2)$. Ist $\alpha \in K_1$ mit $\nu_{P_i}(\alpha) \geq \nu_{P_i}(I_2)$ für $P_i \in \mathrm{supp}(I_2)$, so gilt $\nu_{p_i}(\alpha) \geq \nu_{p_i}(i_2)$ für $p_i \in \mathrm{supp}\ i_2$ und

(ii) ist $I_1 := \mathrm{Con}_{E/K_1}(q)$ und $i_1 := N_{E/K_2}(I_1)$. Ist $\alpha \in K_2$ mit $\nu_{Q_i}(\alpha) \geq \nu_{Q_i}(I_1)$ für $Q_i \in \mathrm{supp}(I_1)$, so gilt $\nu_{q_i}(\alpha) \geq \nu_{q_i}(i_1)$ für $q_i \in \mathrm{supp}\ i_1$.

Beweis. Zum Beweis der ersten Aussage definieren wir

$$S_2 := N_{E/K_2}(\mathrm{Con}_{E/K_1}(\mathrm{supp}(D))) \cup \bigcup_i \mathrm{supp}(\delta_i)_\infty$$

und betrachten dann ein $p \in \mathbb{P}_{K_2/K} \backslash S_2$. Für $I_2 = \mathrm{Con}_{E/K_2}(p) = \sum_{i=1}^{l} e_i Q_i$ mit paarweise verschiedenen Q_i und ein $p_{1i} \in \mathbb{P}_{K_1/K}$ mit $Q_i | p_{1i}$ liegt die Situation von Lemma 3.2 vor, da $p_{1i} \in \mathrm{supp}\, i_2$ gilt und $\mathrm{supp}\, i_2 \cap \mathrm{supp}(D) = \emptyset$ ist. Damit ist p_{1i} unverzweigt in E/K_1 und wir erhalten $(p_{1i}, p) = Q_i$ mit paarweise verschieden p_{1i}. Außerdem erhalten wir $i_2 = \sum_{i=1}^{l} e_i p_{1i}$. Für ein $\alpha \in K_1$ mit obigen Eigenschaften erhalten wir zuerst $\nu_{p_i}(\alpha^n) \geq \nu_{p_i}(i_2)$ für $p_i \in \mathrm{supp}\, i_2 = \{p_{1i} : i = 1, ..., l\}$. Wir wollen jetzt zeigen, dass unter den gemachten Voraussetzungen auch $\nu_{p_i}(\alpha) \geq \nu_{p_i}(i_2)$ gilt. Es reicht, die Aussage für ein Q_i und p_{1i} mit $Q_i | p_{i1}$ zu zeigen. Wir betrachten die unverzweigte Zerlegung $\mathrm{Con}_{E/K_1}(p_{1i}) = \sum_{j=1}^{l} R_j$ mit $R_1 := Q_i$. Nach Voraussetzung ist $\alpha \in e_i R_1$. Betrachten wir die Galoissche Hülle H von E/K_1, so gilt ebenfalls $\alpha \in \sigma(e_i R_1) = e_i R_j$ mit $\sigma \in G(H/K_1)$ und $j \in \{1, ..., l\}$ geeignet. Da in der rechten Seite der letzten Gleichung alle R_j ($j \in \{1, ..., l\}$) vorkommen müssen, folgt also

$$\alpha \in e_i \left(\sum_{j=1}^{l} R_j \right) = e_i \mathrm{Con}_{E/K_1}(p_{1i})$$

und $\nu_{R_j}(\alpha) \geq e_i$. Damit folgt dann $\nu_{p_{1i}}(\alpha) \geq e_i = \nu_{p_{1i}}(i_2)$ und somit die Behauptung. Nun sei

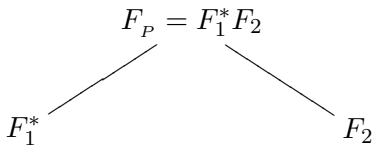
$$S_1 := \mathrm{supp}(D) \cup \bigcup_i \mathrm{supp}\, N_{E/K_1}(\mathrm{Con}_{E/K_2}\, (\delta_i)_\infty)$$

und $q \in \mathbb{P}_{F_1/K} \backslash S_1$. Nach Voraussetzung ist dann $I_1 := \mathrm{Con}_{E/K_1}(q) = \sum Q_i$ unverzweigt, und mit Lemma 3.2 folgt dann, dass $(q, p_{2i}) = Q_i$ ist mit $p_{2i} \in \mathbb{P}_{F_2/K}$ und $Q_i | p_{2i}$. Somit sind also die p_{2i} paarweise verschieden und es gilt $i_1 = \sum p_{2i}$. Daraus ergibt sich die Behauptung. □

Idealtheoretisch gesprochen soll z.B. der erste Fall in Lemma 3.3 einfach nur Folgendes bedeuten: Wenn ein Element $\alpha \in K_1$, aufgefasst als ein Element in E, z.B. im Ideal I_2 der endlichen Maximalordnung $\mathcal{O}_{E/K_1}$ liegt, so soll neben α^n, wobei $n = [E : K_1]$ ist, auch α selbst in der Norm i_2 von I_2 liegen. Zwar wissen wir, dass $\alpha \in I_2 \cap K_1$ ist. Aber im Allgemeinen ist $i_2 \neq (I_2 \cap K_1)$. Wenn aber $i_2 = \prod_{i=1}^{t} q_i$ mit paarweise verschiedenen Idealen q_i aus $\mathcal{O}_{K_1/K}$ ist, so gilt $\alpha \in q_i$ ($i = 1, ..., t$) und damit $\alpha \in i_2$. Um solch eine Zerlegung in paarweise verschiedene Ideale von K_1 zu erhalten, benutzen wir Lemma 3.2.

Jetzt sei K wieder $\mathbf{K} = \mathbb{F}_{\mathbf{p^n}}$. Die Aussagen von Lemma 3.3 lassen sich auch im nicht algebraisch abgeschlossenen Fall anwenden, da wir die ganze Situation stets in $\overline{K}$ einbetten können. Dies bedeutet aber, dass wir bei

unseren Berechnungen für die Ausnahmedivisoren geeignete endliche Erweiterungen K' von K machen müssen, damit diese in Grad 1 Primdivisoren zerfallen. Haben wir eine Primkorrespondenz $P \in \mathcal{D}_{L/F_2}$ vorliegen, so betrachten wir wieder die folgende Situation wie in 2.11



(3.2)

Ferner sei $\tau_P(x_1) =: x_1^*$ und $\tau_P(y_1) =: y_1^*$. Dann ist $F_P = F_2\,(x_1^*, y_1^*) = F_1^*(x_2, y_2)$ und $F_1^* = K(x_1^*, y_1^*)$. Somit haben wir als Erzeugendensystem von F_P/F_2 eine Menge von eventuell gemischten Potenzen von x_1^* und y_1^*, aus der wir eine Basis $\Delta \subseteq F_1^*$ für F_P/F_2 erhalten können. Ist F_P/F_2 nicht separabel, so betrachten wir als Erzeugermenge die eventuell gemischten Potenzen von x_2 und y_2 und erhalten daraus eine Basis $\Delta \subseteq F_2$ für F_P/F_1^*. Nun könnnen wir unseren Algorithmus formulieren:

Algorithmus 2: Korrespondenz als Homomorphismus

Input: 1) Ein $A \in \mathcal{D}_{L/F_2} \geq 0$ frei von konstanten Komponenten
2) $a = a_0 - a_\infty \in \mathcal{C}^0_{F_2}$
3) Eine Basis Ω von $\mathcal{O}_{L/F_2}$

Output: Ein Repräsentant in $[A(a_0 - a_\infty)] \in \mathcal{C}^0_{F_1}$

1.) (Initialisierung) Setze $C := \emptyset$.

2.) Faktorisiere A_0 zu $A_0 = \prod_i P_{i,0}^{e_i}$.

3.) (Schleife über i) Berechne für $P_{i,0}$ eine Basis $\mathcal{B}_i \subseteq \mathcal{O}_{L/F_2}$ bzgl. Ω , so dass die Übergangsmatrix von Ω zu $\mathcal{B}_i$ eine untere Dreiecksmatrix ist und normiere ggf. die Diagonalelemente.

4.) Berechne für $\mathcal{B}_i$ wie in (3.1) eine geeignete endliche Erweiterung K_i/K und Menge C_i, so dass C_i aus Primdivisoren vom Grad 1 aus F_2K_i besteht.

5.) Berechne gemeinsamen endlichen Oberkörper K'/K mit $K_i \subseteq K'$ für alle K_i und $\tilde{C} \longleftarrow C \cup \bigcup\{\mathrm{Con}_{F_2K'/F_2K_i}(p_i) \mid p_i \in C_i\}$.

6.) Sei P_i mit P bezeichnet. Ist F_P/F_2 separabel, so bestimme Basis

$$\Delta := \{1, x_1^*, ..., x_1^{*m}, ..., y_1^{*l}, ..., x_1^{*m} y_1^{*l}\} \subseteq F_1^*$$

von F_P/F_2 mit $m, l \in \mathbb{N}^{\geq 0}$ geeignet. Berechne Diskriminante $D \in F_2$ von Δ und $(x_1^*)_\infty$ und $(y_1^*)_\infty$. Bestimme

$$S_2 := \text{supp}\ (D)\ \cup\ \text{supp}\, N_{F_P/F_2}\left(\text{Con}_{F_P/F_1^*}((x_1^*)_\infty + (y_1^*)_\infty)\right).$$

Berechne gegebenenfalls endliche Erweiterung K'' von K', so dass alle Divisoren von S_2 in Primdivisoren vom Grad eins zerfallen. Mache Divisoren in S_2 und $\tilde{C}$ zu Divisoren $\tilde{S_2}$ und $\tilde{\tilde{C}}$ von F_2K''/K'' und bilde Vereinigung $C \longleftarrow C \cup \tilde{S} \cup \tilde{\tilde{C}}$.

7.) Anderenfalls sei F_P/F_2 nicht separabel. Bestimme Basis

$$\Delta := \{1, x_2, ..., x_2^m, ..., y_2^l, ..., x_2^m y_2^l\} \subseteq F_2 \text{ von } F_P/F_1^*$$

mit $m, l \in \mathbb{N}^{\geq 0}$ geeignet. Berechne Diskriminante $D \in F_1^*$ von Δ. Bestimme

$$S_2 := \text{supp}\ \ N_{F_P/F_2}(\text{Con}_{F_P/F_1^*}((D)))\ \cup\ \text{supp}\,((x_2)_\infty + (y_2)_\infty).$$

Berechne gegebenenfalls endliche Erweiterung K'' von K', so dass alle Divisoren von S_2 in Primdivisoren vom Grad eins zerfallen. Mache Divisoren in S_2 und $\tilde{C}$ zu Divisoren $\tilde{S_2}$ und $\tilde{\tilde{C}}$ von F_2K''/K'' und bilde Vereinigung $C \longleftarrow C \cup \tilde{S} \cup \tilde{\tilde{C}}$.

8.) (Ende Schleife über i)

9.) Berechne wie in Lemma 3.1 mit Hilfe des schwachen Approximationssatzes ein $\tilde{b} := \tilde{b}_0 - \tilde{b}_\infty \in [a]$ mit effektiven Divisoren $\tilde{b}_0, \tilde{b}_\infty$ aus F_2K''/K'', so dass $\text{supp}(\tilde{b}_0) \cup \text{supp}(\tilde{b}_\infty) \cap C = \emptyset$ gilt. Setze anschliessend $b_0 := N_{F_2K''/F_2}(\tilde{b}_0)$ und $b_\infty := N_{F_2K''/F_2}(\tilde{b}_\infty)$.

10.) (Schleife über i) Berechne endliche Erweiterung K'''/K, so dass sich $\text{Con}_{F_2K'''/F_2}(b_0) = \sum p_i$ und $\text{Con}_{F_2K'''/F_2}(b_\infty) = \sum q_i$ in F_2K''' in Primdivisoren vom Grad eins zerlegen.

11.) Bette Basis $\mathcal{B}_i$ in F_1F_2'/F_2' ein mit $F_2' := F_2K'''$ und berechne $D_i := \sum_j \overline{P_i}^{p_j} - \overline{P_i}^{q_j}$ wie beim Abschnitt über den Restidealsatz.

12.) (Ende Schleife über i)

13.) Gib $\sum e_i D_i \in \mathcal{D}_{F_1/K}$ zurück und terminiere.

Die Berechnung der Ausnahmemenge S_2 im obigen Algorithmus wird mit größer werdendem Grad einer Primkorrespondenz P komplizierter. Im

Fall, dass F_1 und F_2 isomorph über K sind, können wir eine algorithmisch einfachere Variante der Operation der Korrespondenzen als Endomorphismen auf der Jacobischen angeben. Wir betrachten dazu eine nicht-konstante Primkorrespondenz $P \in \mathcal{D}_{L/F_2}$. Ist P_0 regulär bezüglich einem $p \in \mathbb{P}_{F_2/K}$ mit $\deg_{F_2/K} p = 1$ und zudem P separabel, so können wir $\overline{P}^p$ berechnen. Sei nun $\overline{P}^p = \sum_{i=1}^r q_i \geq 0$ mit paarweise verschiedenen $q_i \in \mathbb{P}_{F_1/K}$ und $p \notin \text{supp } \text{disc}(F_{_P}/F_2)$. Da $p \notin \text{supp } \text{disc}(F_{_P}/F_2)$ gilt und P_0 bezüglich p regulär ist, können wir im Restidealsatz Satz 2.16 folgern, dass $\overline{P}^p \geq P(p) \geq 0$ gilt, da dann in der Zerlegung von $P(p)$ jeder Primdivisor nur einfach vorkommt. Auf Grund der p-Regularität von P_0 gilt dann $\deg_{F_1/K} \overline{P}^p = \deg_{F_1/K} P(p)$, und somit wissen wir bereits, dass $P(p) = \overline{P}^p$ gelten muss. Wir können dann in der Klasse $[a]$ einen geeigneten Repräsentanten $b_0 - b_\infty \in [a]$ so suchen, dass in $\overline{P_i}^{p_j}$ und $\overline{P_i}^{q_j}$ wie in 10) von Algorithmus 2 jeweils sämtliche Primdivisoren nur einmal vorkommen und die p_j und q_j nicht im Träger von $\text{disc}(F_{_P}/F_2)$ sind.

Ist schließlich P inseparabel, so folgt durch mehrmalige Anwendung von Lemma 2.10, dass P die Gestalt $P = (F^\star)^m B$ mit einer separablen Primkorrespondenz $B \in \mathbb{P}_{L/F_2}$ besitzt. Sei $a \in \mathbb{P}_{F_2/K}$ vom Grad eins und P regulär bezüglich a. Wir berechnen dann zuerst $b := B(a)$. Für $P(a) = (F^\star)^m(b)$ erhalten wir dann die Darstellung $(F^\star)^m(b) = (p^{nm})c$ mit einem geeigneten Divisor $c \in \mathcal{D}_{F_2}$, wobei p die Charakteristik von $K = \mathbb{F}_{p^n}$ ist. Besteht für c eine Darstellung der Gestalt $c = \sum_{i=1}^r q_i$ mit paarweise verschiedenen Primdivisoren q_i und ist $a \notin \text{supp } \text{disc}(F_{_B}/F_2)$, so gilt wieder $P(a) = \overline{P}^a$.

Algorithmus 3: Korrespondenz als Endomorphismus

Input: 1) Ein $A \in \mathcal{D}_{L/F_2} \geq 0$ frei von konstanten Komponenten
2) $a = a_0 - a_\infty \in \mathcal{C}^0_{F_2}$
3) Eine Basis Ω von $\mathcal{O}_{L/F_2}$

Output: Ein Repräsentant in $[A(a_0 - a_\infty)] \in \mathcal{C}^0_{F_1}$

1.) Sei $I := 0$ der Nulldivisor von F_2/K. Berechne ähnlich wie in Algorithmus 2 Faktorisierung von $A_0 = \prod P_{i,0}^{e_i}$ und die Menge C der Ausnahmedivisoren für das Ideal A_0 wie in (3.1).

2.) (Schleife über i) Berechne $(G_i)^{q^{m_i} f} = N_{L/F_2}(P_{i,0})$ mit $m_i \geq 0$ maximal mit dieser Eigenschaft, f bezeichne den Trägheitsgrad von P_i und $q = p^n$ mit $p = \text{char}\, K$. Setze $C_i \longleftarrow C \cup \text{supp } \text{disc}\, F_{_{B_i}}/F_2$, wobei $P_i = (F^\star)^{m_i} B_i$ ist.

3.) Berechne einen zufälligen Repräsentanten b von $[a] \in \mathcal{C}^0_{F_2}$, so dass $\text{supp}\, b \cap C_i = \emptyset$ ist. Mache gegebenenfalls eine geeignete endliche Er-

weiterung K' von K, so dass b_0, b_∞ und sämtliche Divisoren von C_i in Divisoren vom Grad eins zerfallen.

4.) Sei $b_0 = \sum_i e_i p_i$ und $b_\infty = \sum_i r_i q_i$ mit jeweils $\deg p_i = 1 = \deg q_i$. Sind sämtiche Exponenten in der von jedem Summanden von $\sum_i \overline{P_i}^{p_i}$ und $\sum_i \overline{P_i}^{q_i}$ vorkommenden Zerlegung in Primdivisoren identisch mit p^{nm_i}, so setze

$$I \longleftarrow I + e_i \left(\sum_i \overline{P_i}^{p_i} - \sum_i \overline{P_i}^{q_i} \right).$$

Ansonsten gehe zu 3.).

5.) (Ende Schleife über i)

6.) Gib I zurück und terminiere.

Bemerkung 3.4. *Die Anzahl der Primdivisoren p von F_2, für die $P(p)$ nicht von der Gestalt $P(p) = \sum q_i$ mit paarweise verschiedenen Primdivisoren q_i ist, ist endlich. Ist P_0 regulär bezüglich p, so reicht es sogar aus sich darauf zu beschränken, dass p nicht im Träger der Diskriminante von F_P vorkommt. Da wir immer geeignete Erweiterungen K'/K so machen können, gibt es beliebig viele Stellen p vom Grad eins, die geeignet sind, bis auf die endlich vielen Stellen, die im Träger der Diskriminante F_P/F_2 vorkommen. Die Wahrscheinlichkeit, dass wir eine Stelle vom Grad eins zufällig wählen und diese im Träger der Diskriminante F_P/F_2 ist, ist verschwindend gering.*

3.3 Die Schnitt- und Korrespondenzpaarung

Die Funktionenkörper F_1 und F_2 müssen in diesem Abschnitt nicht isomorph sein. Wir wollen nun zeigen, wie wir den Schnitt zweier Korrespondenzen berechnen können. Dazu gehen wir in zwei Schritten vor. Im ersten Schritt zeigen wir, wie man den Schnitt zweier Korrespondenzen ohne gemeinsamen Träger berechnen kann. Im zweiten Schritt werden wir dann zeigen, wie wir die Korrespondenzklasse so geschickt abändern können, dass wir den Selbstschnitt berechnen können. Im letzten Teil dieses Abschnitts widmen wir uns dann der Schnittpaarung. Für den Index i gilt, wenn nichts anderes festgelegt wird, im gesamten Abschnitt $i \in \{1, 2\}$.

Wir stützen uns hier u.A. auf die Bezeichnungen wie sie im zweiten Kapitel gemacht wurden. Insgesamt benötigen wir vier Ringe, wie im Lemma 2.21 bereits erwähnt wurde. Die beiden Funktionenkörper $F_i = K(x_i, y_i)$ seien jeweils durch Gleichungen $f_i(x_i, y_i) = 0$ mit $f_i \in K(x_1)[T]$ erzeugt. Mit

$\mathcal{C}_i \subseteq K^2$ bezeichnen wir dann die durch f_i gegebene affine Kurve und mit X_i jeweils den projektiven Abschluss der $\mathcal{C}_i$.

Nun betrachten wir jeweils eine Basis $\Omega_0^i := \{\omega_{i1}, ..., \omega_{in_i}\}$ der endlichen Maximalordnung $\mathcal{O}_{F_i}$ von F_i/K und eine Basis der $\Omega_\infty^i := \{\mu_{i1}, ..., \mu_{in_i}\}$ der unendlichen Maximalordnung $\mathcal{O}_{F_i,\infty}$ von F_i/K. Dann lassen sich genau die Polstellen von x_i nicht als Ideale in $\mathcal{O}_{F_i}$ darstellen, und umgekehrt sind es genau die Nullstellen von x_i, welche sich nicht als Ideale in $\mathcal{O}_{F_i}$ darstellen lassen. Jeder Divisor von F_i besitzt dann eine Darstellung mit Idealen aus $\mathcal{O}_{F_i}$ und $\mathcal{O}_{F_i,\infty}$. Dies ist auch der Grund, warum wir die Wechselsumme aus Lemma 2.21 berechnen müssen. Mit [Hes02, Corollary 4.4 und Corollary 4.4] wissen wir, dass wir die Basen Ω_0^i und Ω_∞^i so wählen können, dass die Übergangsmatrizen $M_i \in K(x_i)^{n_i \times n_i}$ zwischen diesen beiden Basen jeweils Diagonalmatrizen und die Diagonalelemente von der Form $x_i^{m_{ij}}$ mit $m_{ij} \in \mathbb{Z}$ sind.

Insgesamt erhalten wir vier Ringe, mit deren Hilfe wir, wie in Lemma 2.21 ausgeführt, den Schnitt berechnen können: $S_1 := \mathcal{O}_{F_1} \otimes_K \mathcal{O}_{F_2}$, $S_2 := \mathcal{O}_{F_1} \otimes_K \mathcal{O}_{F_2,\infty}$, $S_3 := \mathcal{O}_{F_1,\infty} \otimes_K \mathcal{O}_{F_2}$ und $S_4 := \mathcal{O}_{F_1,\infty} \otimes_K \mathcal{O}_{F_2,\infty}$. Um diese Ringe als affine Varietäten zu erzeugen, konstruieren wir uns spezielle Ideale $I_{\Omega_0^i}$ und $I_{\Omega_\infty^i}$. Für die Basen Ω_0^i und Ω_∞^i von $\mathcal{O}_{F_i}$ bzw. $\mathcal{O}_{F_i,\infty}$ betrachten wir die $I_{\Omega_0^i}$ bzw. $I_{\Omega_\infty^i}$ wieder als Ideale der Ringe $R_{i,0}$ bzw. $R_{i,\infty}$ wie in (2.20) und (2.21).

Wir betrachten nun zwei nicht-konstante Primkorrespondenzen $A, B \in \mathbb{P}_{L/F_2}$ ohne gemeinsamen Träger. Die dazugehörigen Ideale A_0 und B_0 besitzen jeweils $F_2[x_1]$-Basen

$$\mathcal{A} := \{a_1, ..., a_n\} \text{ und } \mathcal{B} := \{b_1, ..., b_n\}$$

in $\mathcal{O}_{L/F_2}$. Für die a_k und b_k schreiben wir

$$a_k = \frac{a_{k0}}{r_k} \quad \text{und} \quad b_k = \frac{b_{k0}}{s_k} \tag{3.3}$$

mit jeweils $r_k, s_k \in K[x_2]$ für $k = 1, ..., n_2$. Nun nutzen wir die Isomorphie

$$S_1 \cong K[x_1, \omega_{11}, ..., \omega_{1n_1}, x_2, \omega_{21}, ..., \omega_{2n_2}]/\langle I_{\Omega_1^0}, I_{\Omega_2^0}\rangle \tag{3.4}$$

aus und schreiben wieder S_1 für den rechten Ring in (3.4). Für ein Element a_{k0} schreiben wir nun

$$a_{k0} = \sum_{j=1}^{n_1} G_{kj}\omega_{1j} \quad \text{und} \quad b_{k0} = \sum_{j=1}^{n_1} H_{kj}\omega_{1j}$$

mit $G_{kj}, H_{kj} \in F_2[x_1]$. Die G_{kj} und H_{kj} lassen sich wiederum als

$$G_{kj} = \sum_{l=1}^{n_2} g_l^{(kj)}\omega_{2l} \text{ und } H_{kj} = \sum_{l=1}^{n_2} h_l^{(kj)}\omega_{2l}$$

mit $g_l^{(kj)}, h_l^{(kj)} \in K[x_2]$ schreiben. Sei $U := K[x_2]^\times$. Wir betrachten nun die K-Algebrenisomorphie $\Psi : \mathcal{O}_{F_1} \otimes F_2 \longrightarrow S_1[U^{-1}]$ und die Einbettung

$$\iota_{1,0} : S_1 \longrightarrow S_1[U^{-1}], \quad \alpha \longmapsto \frac{\alpha}{1}.$$

Sei dann Φ wie in Lemma 1.19. Behalten wir für die eingebetteten Basiselemente $\Psi \circ \Phi^{-1}(a_k)$ und $\Psi \circ \Phi^{-1}(b_k)$ die Bezeichnungen bei, so berechnen wir für die Ideale $\langle a_k \mid k = 1, ..., n_1 \rangle \subset S_1[U^{-1}]$ und $\langle b_k \mid k = 1, ..., n_1 \rangle \subseteq S_1[U^{-1}]$ dann jeweils die Urbilder

$$\mathcal{I}_{A_1} := \iota_{1,0}^{-1} \left(\langle a_k \mid k = 1, ..., n_1 \rangle \right) \subseteq S_1$$

und

$$\mathcal{I}_{B_1} := \iota_{1,0}^{-1} \left(\langle b_k \mid k = 1, ..., n_1 \rangle \right) \subseteq S_1.$$

Dazu machen wir einen Zwischenschritt: Erst betrachten wir die Einbettung von $S_1[V^{-1}]$ in $S_1[U^{-1}]$ mit einer geeigneten multiplikativen Untergruppe $V \subseteq K[x_2]$ und dann von S_1 in $S_1[V^{-1}]$. Dazu definieren wir V als die von den Elementen $\{a_k, b_j \mid j \in \{1, ..., n\}\}$ in 3.3 erzeugte multiplikative Halbgruppe von $K[x_1]$, machen die Ideale $\mathcal{A}$ und $\mathcal{B}$ zu Idealen von $S_1[V^{-1}]$ und bezeichnen diese mit I_{A_1} bzw. I_{B_1}. Schließlich berechnen wir Ideale

$$I_{A_1} \cap K[x_1, \omega_{11}, ..., \omega_{1n_1}, x_2, \omega_{21}, ..., \omega_{2n_2}] = \mathcal{I}_{A_1}$$

und

$$I_{B_1} \cap K[x_1, \omega_{11}, ..., \omega_{1n_1}, x_2, \omega_{21}, ..., \omega_{2n_2}] = \mathcal{I}_{B_1}$$

mittels Eliminationsidealen und definieren dann

$$\dim_{S_1}(A, B) := \dim_{S_1}(\mathcal{I}_{A_1} + \mathcal{I}_{B_1}) = \dim_K S_1/(\mathcal{I}_{A_1} + \mathcal{I}_{B_1}).$$

Um die affine Darstellung von $\mathcal{I}_{A_1}$ und $\mathcal{I}_{B_1}$ in den restlichen Ringen S_2, S_3 und S_4 zu erhalten, benutzen wir die Übergangsmatrizen $M_i \in k(x_i)^{n_i \times n_i}$ in Diagonalform. Diese seien so gewählt, dass $(\omega_{i1}, ..., \omega_{in_i})M_i = (\mu_{i1}, ..., \mu_{in_i})$ gilt, d.h. also $\omega_{ij} x_i^{r_{ij}} = \mu_{ij}$ mit $r_{ij} \in \mathbb{Z}^{\leq 0}$ geeignet. Wir zeigen nun, wie wir die Darstellung von A und B in S_4 berechnen können. Für die Ringe S_2 und S_3 verläuft der Vorgang dann ähnlich. Besitzen die Ideale $\mathcal{I}_{A_1}$ und $\mathcal{I}_{B_1}$ jeweils Erzeuger $\{\alpha_i \mid i \in \{1, ..., t_1\}\} \subseteq S_1$ und $\{\beta_i \mid i \in \{1, ..., t_2\}\} \subseteq S_1$, so betrachten wir die Lokalisierung

$$\iota_2 : S_1 \longrightarrow S_1[U_{12}^{-1}] = S_{\{1,4\}},$$

wobei U_{12} die von der Menge $\{x_1, x_2\}$ erzeugte multiplikative Halbgruppe in $K[x_1, x_2]$ sein soll. Ferner bezeichnen wir mit U_i die von der Menge $\{x_i\}$ erzeugte multiplikative Halbgruppe in $K[x_1, x_2]$. Da die Erzeuger α_i und β_i in S_1 liegen, können wir sie in $S_1[U_{12}^{-1}]$ wieder als $K[x_1, x_2]$-Linearkombinationen der Basen Ω_0^i darstellen. Der Ring $S_1[U_{12}^{-1}]$ enthält nun

sowohl eine Darstellung von A bzw. B in S_1 als auch in S_4, da beide Basen in ihm enthalten sind. Deshalb können wir bei den Erzeugern der Ideale $\iota_2(\mathcal{I}_{A_1})$ und $\iota_2(\mathcal{I}_{B_1})$ jeweils die Basiselemente ω_{ij} durch $\mu_{ij}x_i^{-r_{ij}}$ ersetzen, da sich in $S_1[U_{12}^{-1}]$ die Basiselemente ω_{ij} und μ_{ij} nur um eine Einheit unterscheiden. Schließlich berechnen wir die Schnittideale

$$\iota_2(\mathcal{I}_{A_1}) \cap S_4 =: \mathcal{I}_{A_4} \quad \text{und} \quad \iota_2(\mathcal{I}_{B_1}) \cap S_4 =: \mathcal{I}_{B_4}$$

der so modifizierten Ideale und erhalten so Darstellungen von A und B in S_4. Dazu benutzen wir wieder die Eliminationsideale, die wir mit Hilfe von Gröbnerbasen berechnen können. Die restlichen Oberringe sind dann $S_{\{1,2\}} = S_1[U_2^{-1}]$, $S_{\{1,3\}} = S_1[U_1^{-1}]$ und $S_{\{1,2,3,4\}} = S_{\{2,3\}} = S_{\{1,4\}}$ sowie $S_{\{3,4\}} = S_{\{1,2\}}$.

Nun berechnen wir wie in Lemma 2.21 die Schnittmultiplizität von A und B, wobei wir bei der jeweiligen Bestimmung der Dimensionen noch geeignete endliche Erweiterungen K' von K so machen müssen, dass Komponenten der endlichen vielen Punkte eines jeweiligen Schnittes in K' liegen.

Für den Selbstschnitt einer Primkorrespondenz $P \in \mathbb{P}_{L/F_2}$ wenden wir, wie bereits im zweiten Kapitel erläutert, den schwachen Approximationssatz an. Sind nun $A, B \in \mathcal{D}_{L/F_2}$ Korrespondenzen mit $A = \sum_{j=1}^{m} e_j P_j$ und $B = \sum_{k=1}^{n} f_k Q_k$, wobei die Primdivisoren $P_j, Q_k \in \mathbb{P}_{L/F_2}$ jeweils nicht-konstant sein sollen, so berechnen wir die Schnittpaarung durch

$$(A.B) = \sum_j \sum_k (P_j, Q_k) \; .$$

Auf Grund der Eigenschaften $A.(-B) = -(A.B)$ und $\langle A, -B\rangle = -\langle A, B\rangle$ der Schnitt- und Korrespondenzpaarung für effektive Divisoren $A, B \in \mathcal{D}_{L/F_2}$ reicht es aus, den Algorithmus nur für effektive Korrespondenzen zu formulieren:

Algorithmus 4: Schnitt- und Korrespondenzpaarung

Input: Zwei effektive Korrespondenzen $A, B \in \mathcal{D}_{L/F_2}$

Output: Der Schnitt $A.B \in \mathbb{Z}$ und die Korrespondenzpaarung $\langle A, B\rangle \in \mathbb{Z}$

1.) Berechne Darstellungen $A = A_H + A_C$ und $B = B_H + B_C$. Dann ist

$$A.B = A_H.B_H + A_H.B_C + A_C.B_H + A_C.B_C$$

und mit Lemma 2.22 erhalten wir dann

$$A_C.B_C = 0, \quad A_C.B_H = \deg_{L/F_2} A_C \cdot \deg_{L/F_1} B_H^{\star} =: s_1$$

und

$$A_H.B_C = \deg_{L/F_2} B_C \cdot \deg_{L/F_1} A_H^\star =: s_2.$$

Bezeichne mit $\mathcal{S} := s_1 + s_2$ und setze $A := A_H$ und $B := B_H$.

2.) Bestimme Ganzheitsbasen Ω_0^i und Ω_∞^i mit jeweils Übergangsmatrix $M_i = (m_{kj}^{(i)}) \in k(x_i)^{n_i \times n_i}$ von Ω_0^i nach Ω_∞^i in Diagonalform, so dass $m_{jj}^{(i)} = x_i^{m_{ij}}$ ist mit $m_{ij} \in \mathbb{Z}^{\leq 0}$.

3.) Bestimme

$$f_{A,B} := \mathrm{Res}(N_{L/F_2(x_1)}(A_0), N_{L/F_2(x_1)}(B_0)).$$

Ist $f_{A,B} \neq 0$, so gehe zu 5), ansonsten zu 8).

4.) Berechne Basen $A_0 = \langle a_k \mid k = 1, ..., n_1\}\rangle$ und $B_0 = \langle b_k \mid k = 1, ..., n_1\rangle$ und Ideale

$$\mathcal{I}_{A_1} := \iota_{1,0}^{-1}\left(\langle \Psi \circ \Phi^{-1}(a_k) \mid k = 1, ..., n_1\rangle\right)$$

und

$$\mathcal{I}_{B_1} := \iota_{1,0}^{-1}\left(\langle \Psi \circ \Phi^{-1}(b_k) \mid k = 1, ..., n_1\}\rangle\right)$$

mittels Eliminationsidealen und $V_1 := V(\mathcal{I}_{A_1}, \mathcal{I}_{B_1})$.

5.) Konstruiere Oberringe $S_{\{1,2\}} = S_1[U_2^{-1}], S_{\{1,3\}} = S_1[U_1^{-1}]$ und $S_{\{1,4\}} = S_1[U_{12}^{-1}]$.

6.) (Schleife über j) Mache $\mathcal{I}_{A_1}$ und $\mathcal{I}_{B_1}$ zu Idealen von $S_{1,j}$. Berechne mittels Eliminationsidealen $\mathcal{I}_{A_j}$ und $\mathcal{I}_{B_j}$ und schließlich $V_j := V(\mathcal{I}_{A_j}, \mathcal{I}_{B_j})$, wobei $j = 2, 3, 4$ ist.

7.) Berechne gemeinsamen Oberkörper K'/K, so dass alle Komponenten der Punkte der Varietäten V_1, V_2, V_3, V_4 in K' liegen. Schließlich berechne

$$\dim_{K'} S_J / \left(\mathcal{I}_{A_i} + \mathcal{I}_{B_i}\right) \quad (i \in J)$$

mit $J \in \{\{1\}, \{2\}, \{3\}, \{4\}, \{1,2\}, \{2,3\}, \{3,4\}, \{4,1\}, \{1,2,3,4\}\}$ und dann Wechselsumme Σ wie in Lemma 2.23. Gib Wechselsumme $\Sigma + S$ und

$$\deg_{L/F_2} A \deg_{L/F_1} B^\star + \deg_{L/F_2} B \deg_{L/F_1} A^\star - (\Sigma + \mathcal{S})$$

zurück und terminiere.

8.) (Selbstschnitt) Bestimme $A = \sum e_i P_i$ und $B = \sum f_i Q_i$ und dann mittels schwachen Approximationssatz ein $F \in L/F_2$ mit $\nu_{P_i}(F) = -e_i$ und $\nu_{Q_i}(F) = 0$. Berechne $\tilde{A} := A + (F)$ und setze $A := \tilde{A}$. Schreibe $A = A_1 - A_2$ mit effektiven Divisoren $A_1, A_2 \in \mathcal{D}_{L/F_2}$, führe Berechnungen für $A_1.B$ und $A_2.B$ wie in den Schritten 4.) - 7.) aus und terminiere.

Wenn gewisse Voraussetzungen erfüllt sind, können wir die Schnittzahl wesentlich effizienter berechnen. Die Hauptdivisoren (x_i) von F_i/K schreiben wir in der Form $(x_i) = x_{i,0} - x_{i,\infty}$. Ist $p \in \mathbb{P}_{F_2/K} \setminus \operatorname{supp} x_{2,\infty}$ vom Grad 1 und $P \in \mathbb{P}_{L/F_2}$ effektiv, so sei

$$P(p) = \sum e_j q_j + \sum f_k r_k \geq 0$$

mit $q_j \in \mathbb{P}_{F_1/K} \setminus \operatorname{supp} x_{1,\infty}$ und $r_i \in \operatorname{supp} x_{1,\infty}$. Für die endlichen und unendlichen Anteile der Primdivisoren können wir

$$p_0 = \langle x_2 - \beta_0, \omega_{21} - \beta_1, ..., \omega_{2n_2} - \beta_{n_2} \rangle,$$

$$q_{j,0} = \langle x_1 - \delta_{j0}, \omega_{11} - \delta_{j1}, ..., \omega_{1n_1} - \delta_{jn_1} \rangle$$

und

$$r_{k,\infty} = \langle z_1 - \eta_{k0}, \mu_{11} - \eta_{k1}, ..., \mu_{1n_1} - \eta_{kn_1} \rangle$$

mit $\beta_i, \eta_{kj}, \delta_{jl}$ aus $\overline{K}$ und $\frac{1}{x_1} = z_1$ schreiben. Bildet die Korrespondenz P den Primdivisor p auf $P(p)$ ab, so können wir dies auch mit geeigneten Elementen aus den Varietäten $V(\mathcal{I}_{A_1})$ bzw. $V(\mathcal{I}_{A_3})$ ausdrücken. Sei $p \in \mathbb{P}_{F_2/K}$ und $q \in \mathbb{P}_{F_1/K}$ mit $\deg_{F_1/K} p = 1$. Ist $p \notin \mathcal{A}_{P,\Delta}$ und P regulär bezüglich p, so gilt

$$q_j \in \operatorname{supp} P(p) = \overline{P}^p \quad \Longleftrightarrow \quad (\delta_{j0}, \delta_{j1}, ..., \delta_{jn_1}, \beta_0, ..., \beta_{n_2}) \in V(\mathcal{I}_{A_1})$$

und

$$r_k \in \operatorname{supp} P(p) = \overline{P}^p \quad \Longleftrightarrow \quad (\eta_{k0}, \eta_{k1}, ..., \eta_{kn_1}, \beta_0, ..., \beta_{n_2}) \in V(\mathcal{I}_{A_3}).$$

Ist $\Omega := \{1, ..., \omega_n\} \subseteq F_1$ eine Ganzheitsbasis von $\mathcal{O}_{F_2/K}$ und $\Omega_\infty := \{1, ..., \gamma_n\}$ mit $r_j \in \mathbb{Z}^{\geq 0}$ und $\gamma_j z_i^{-r_j} = \omega_j$ eine Ganzheitsbasis von $\mathcal{O}_{L/F_{2,\infty}}$, so betrachten wir den Isomorphismus

$$\mu : L/F_2 \longrightarrow L/F_2, \quad (1, ..., \omega_n) \longmapsto (1, ..., \gamma_n z_i^{-r_n})$$

und dann die Ideale $\mu(P)_0$. Analog könnnen wir dann obigen Sachverhalt auch für einen Primdivisor p mit $\nu_p(x_2) < 0$ ausdrücken. Nun gilt folgendes Lemma:

Lemma 3.5. *Sei A eine effektive und nicht-konstante Korrespondenz von $\mathcal{D}_{L/F_2}$. Gilt*

$$\overline{A}^p = A(p) \text{ und } \operatorname{supp} A(p) \cap \operatorname{supp} x_{1,\infty} = \emptyset \quad \forall p \in \operatorname{supp} x_{2,0}$$

als auch

$$\overline{\mu(A)}^p = A(p) \text{ und } \operatorname{supp} A(p) \cap \operatorname{supp} x_{1,0} = \emptyset \quad \forall p \in \operatorname{supp} x_{2,\infty},$$

d.h. insbesondere, dass A bzw. $\mu(A)$ jeweils regulär bezüglich p ist, so ist $A.B = s_1 + s_4 - s_{14}$ für alle effektiven $B \in \mathcal{D}_{L/F_2}$. Anders ausgedrückt: Bildet A Polstellen nicht auf Nullstellen und Nullstellen nicht auf Polstellen ab, so reicht es, die Schnittmultiplizität nur in $S_1 \cup S_4$ zu berechnen.

Beweis. Die Bedingungen sagen nichts Anderes, als dass die zu den Primdivisoren q_j des Bildes $A(p) = \sum e_j q_j$ gehörigen Punkte alle schon in $V(\mathcal{I}_{A_1}) \cup V(\mathcal{I}_{A_4})$ liegen. Damit liegen aber erst recht die Punkte von $V(\mathcal{I}_{A_j} + \mathcal{I}_{B_j})$ mit $j = 1, 2, 3, 4$ in $V(\mathcal{I}_{A_1}) \cup V(\mathcal{I}_{A_4})$. Deshalb genügt es, die Schnittmultiplizität in $S_1 \cup S_4$ zu berechnen, und dies bedeutet dann $A.B = s_1 + s_4 - s_{14}$. □

3.4 Bemerkungen zu den Laufzeiten

Wir wollen noch einige Bemerkungen zu den Laufzeiten der Algorithmen dieses Kapitels machen und beginnen mit einigen Aussagen zur Arithmetik der Korrespondenzen. Bezeichne $\mathcal{B} = \{B_1, ..., B_n\}$ eine $F_2[x_1]$-Basis einer Korrespondenz $B \in \mathcal{D}_{L/F_2}$, wobei $[L : F_2] = n$ ist. Mit größer werdender Charakteristik werden in der Regel die Grade der Polynome in x_2 der Koeffizienten der Erzeuger B_i größer, wodurch die Idealarithmetik schwerfälliger wird. Allerdings können wir wie in (4.8) mit Hilfe der Spurformel versuchen, Elemente in der Endomorphismenalgebra zu finden, für die der Wert in (4.8) minimal wird. Dadurch können wir die auftretenden Grade der Koeffizienten überblicken. In Algorithmus 1 zur Berechnung des Produktes zweier Korrespondenzen müssen wir den Zerfällungskörper eines Polynoms $F \in F_2[x_1]$ berechnen. Bevor wir das Produkt $A \cdot B$ zweier effektiver Korrespondenzen A und B aus $\mathcal{D}_{L/F_2}$ berechnen, empfiehlt es sich, die Korrespondenz B bezüglich dem Primdivisor $P_{\infty,1}$ zu einem effektiven Divisor $\tilde{B}$ zu reduzieren, um ein Ideal $\tilde{B}_0$ mit $\deg \tilde{B}_0 \leq g_{F/K}$ zu erhalten. Um ein Polynom $F \in F_2[x_1]$ zu faktorisieren, reicht es aus, die Polynomnorm $f := N(F) \in K(x_2)[x_2]$ in $\mathbb{F}_q(x_2)[x_1]$ faktorisieren zu können. Aus [Bel07] entnehmen wir zum bivariaten Faktorisieren in $\mathbb{F}_q[x_2][x_1]$ die Laufzeitabschätzung $(q \min(n,p) n^{\omega+1}) \log(q \min(n,p) n^{\omega+1})^{O(1)}$, wobei n der Totalgrad von f ist, für die Resultante bezüglich x_2 dann $\operatorname{Res}(f, f')_{x_2}(0) \neq 0$ gilt und $2 \leq \omega \leq 3$ ist. Sei $K = \mathbb{F}_q$ und K'/K eine endliche Erweiterung von K. In Algorithmus 2 und 3, welche die Operation einer Korrespondenz auf der Klassengruppe vom Grad null von F_2/K als Homomorphismus bzw. Endomorphismus berechnen, ist der aufwendigste Teil die Bestimmung der Hochhebung von Divisoren von F_2/K nach F_2/K', was auf das Faktorisieren von Polynomen in $K[x_1]$ zurückgeht. Der Aufwand hierfür wird in [Gat99]

mit $O(nM(n)\log(qn))$ angegeben, wobei hier $M(n)$ die Multiplikationszeit für Polynome in $K[x_1]$ und n der Grad des zu faktorisierenden Polynoms ist. In Algorithmus 4 zur Berechnung der Werte der Korresponenzpaarung sind vor allem die Berechnung der Eliminationsideale und die Berechnung der Dimensionen von Varietäten am aufwendigsten, da dies mittels Gröbnerbasen geschieht. Die Berechnung von Gröbnerbasen hat im schlimmsten Fall exponentielle Laufzeit, siehe dazu auch [Gat99].

Kapitel 4

Berechnung von Endomorphismenringen

In diesem Kapitel gelten wieder, wenn nichts anderes festgelegt wird, sämtliche Bezeichnungen und Aussagen aus den vorherigen Kapiteln. Wir wollen in diesem Abschnitt eine kleine Änderung der Notation einführen: mit k bezeichnen wir einen Körper $k = \mathbb{F}_q$ und K/k soll eine endliche Erweiterung sein. Die Funktionenkörper F_i und die dazugehörigen affinen Kurven $\mathcal{C}_i$ sollen dann über k definiert sein.

4.1 Einführung

In diesem Abschnitt wollen wir uns dem Hauptanliegen dieser Arbeit widmen: Der Berechnung des Endomorphismenringes $\mathrm{End}_K(J_{X_2})$ der Jacobischen J_{X_2}. Ist J_{X_2} nun K-isogen zu dem Produkt $\prod A_i^{r_i}$ von Potenzen einfacher abelscher Varietäten über K, so wissen wir bereits aus Kapitel 1, dass für $E_{_K} := \mathrm{End}^0_K(J_{X_2})$ die Isomorphie

$$E_{_K} \cong \prod_{i=1}^{t} \mathrm{End}^0_K(A_i^{r_i})$$

gilt. Wir wollen nun annehmen, dass $J_{X_2} \sim_K A^r$ mit einer einfachen abelschen Varietät A über K gilt. Das bedeutet, dass J_{X_2} elementar und $E_{_K}$ eine zentral einfache F-Algebra ist, wenn $F = Z(E_{_K})$ das Zentrum von $E_{_K}$ bezeichnet. Haben wir umgekehrt das charakteristische Polynom $f := f_{\pi_K}$ des Frobeniusendomorphismuses einer abelschen Varietät A gegeben und ist $f := g^n$ mit $g \in \mathbb{Z}[t]$ irreduzibel, so können wir mit Hilfe von [Tat66, Theorem 2, p. 140] schließen, dass $A \sim_K B^r$ mit einer einfachen abelschen Varietät B über K ist ($r \in \mathbb{Z}^{>0}$). Zudem wissen wir dann auch, dass $\mathrm{End}^0_K(A)$ eine zentral einfache F-Algebra mit $F = \mathbb{Q}(\pi_{_K})$ ist. Aus der Einfachheit von B

folgt, dass $D := \mathrm{End}_K^0(B)$ ein Schiefkörper ist. Letztlich ist $\mathrm{End}_K^0(A) \cong M_r(D)$ eine Matrixalgebra vom Grad $\mathrm{Deg}(\mathrm{End}_K(A)) = r \cdot \mathrm{Deg}(D)$ mit $\mathrm{Deg}(\mathrm{End}_K^0(A)) \cdot [F : \mathbb{Q}] = \deg f_{\pi_K} = 2g$, wenn g die Dimension von A ist. Im Falle $r = 1$ ist $\mathrm{End}_K^0(A)$ also ein Schiefkörper. Aus Satz 1.25 wissen wir, dass $\mathrm{End}_K^0(A)$ eine zyklische Algebra (E, σ, a) ist, und mit Lemma 1.27 folgt $r = 1$ genau dann, wenn ein $a \in F^\times / N_{E/F}(E^\times)$ mit der Ordnung $\mathrm{Deg}(\mathrm{End}_K^0(A))$ existiert.

Bezeichnet $\mathrm{End}_k(A)$ den Endomorphismenring einer abelschen Varietät A über k, so können wir den Endomorphismenring $\mathrm{End}_K(A)$ betrachten, wobei K/k eine endliche Erweiterung ist. Die Endomorphismen entsprechen dann wieder den Korrespondenzklassen in L/F_2K, und wir können $\mathrm{End}_k(A)$ in $\mathrm{End}_K(A)$ einbetten. Jetzt kann aber durchaus der Fall eintreten, dass $\mathrm{End}_k(A) \subsetneq \mathrm{End}_K(A)$ ist, wie wir später an einem Beispiel sehen werden. Es gilt nämlich das folgende Lemma (s. [Oor07, Proposition 5.11], proposition 5.11):

Lemma 4.1. *Sei K/k eine endliche Erweiterung von k mit $[K : k] = n$ und A eine abelsche Varietät über k. Bezeichnet π_K den Frobeniusendomorphismus von $A \otimes K$, so gilt $\pi_K = \pi_k^n$ und die Äquivalenz* $\mathrm{End}_k(A) \subsetneq \mathrm{End}_k(A \otimes K) \Leftrightarrow \mathbb{Q}(\pi_k^n) \subsetneq \mathbb{Q}(\pi_k)$.

Mit Lemma aus [Oor07, Lemma 5.10] können wir sogar den Endomorphismenring über dem algebraischen Abschluss $\overline{K}$ bestimmen:

Lemma 4.2. *Sei $F = \mathbb{Q}(\pi)$ endliche Erweiterung und $F' = \mathbb{Q}'(\pi)$ die galoissche Hülle von F. Bezeichnen $\{\pi^{(i)} \mid i = 1, ..., e\}$ die verschiedenen Konjugierten von π in F' mit $\pi^{(1)} := \pi$, so gilt (mit $1 \neq z \in \mathbb{Q}'(\pi)$):*

$$\mathbb{Q}(\pi^n) \subsetneq \mathbb{Q}(\pi) \Leftrightarrow \exists z, i, j : \ 1 \leq i < j \leq e, \ z^n = 1, \ \pi^{(j)}/\pi^{(i)} = z.$$

Indem wir also F' wie im Lemma und die Torsionseinheiten von F' berechnen, können wir leicht feststellen, ob wir bereits den vollen Endomorphismenring über $\overline{K}$ berechnet haben.

4.2 Der Divisor $C(A)$ der Korrespondenzklasse $[A]_C$

Als Nächstes benötigen wir einige Aussagen über die Korrespondenzen. Wir schreiben für den Divisor $p_{\infty,2}$ kurz p_∞ und wollen nun zeigen, dass es in jeder Korrespondenzklasse $[A]_C$ mit $A \in \mathcal{D}_{L/F_2}$ eine Korrespondenz $A' \in [A]_C$ so gibt, dass $A'(p_\infty) = lp_\infty + (f)$ ist mit $1 \leq l \leq g_{L/F_2}$, einem geeignetem Hauptdivisor $(f) \in \mathcal{P}_{F_2/K}$ und außerdem $A' \geq 0$ ist mit $\deg_{L/F_2} A' = l$. Mit g bezeichnen wir das Geschlecht $g_{L/F_2} = g_{F_1/K}$ von L/F_2.

Satz 4.3. *Sei $A \in \mathcal{D}_{L/F_2}$. Dann gibt es in $[A]_C$ eine eindeutige effektive Korrespondenz A' vom Grad l mit $1 \leq l \leq g$ so, dass $A'(p_\infty) = lp_\infty + (f)$ ist mit $(f) \in \mathcal{P}_{F_2/K}$.*

Beweis. Ist $A \in \mathcal{D}_{L/F_2}$ eine Korrespondenz, so sei $A(p_\infty) = b \in \mathcal{D}_{F_2/K}$. Sei $B := \mathrm{Con}_{L/F_1}(\tau^{-1}(b))$. Dann ist B ein konstanter Divisor von L/F_2 mit $B \cap F_1 = \tau^{-1}(b)$, und wir definieren $\tilde{A} := A - B$ mit effektiven Divisoren A und B. Da nach der Gradformel 2.4 nun $\deg_{F_2/K} p_\infty = 1$ und damit $\deg_{F_2/K} b = \deg_{L/F_2} A$ gilt, erhalten wir mit Satz 1.10

$$\deg_{L/F_2} B = \deg_{F_1/K} \tau^{-1}(b) = \deg_{F_2/K} b = \deg_{L/F_2} A \, .$$

Denn nach Voraussetzung sind F_1 und F_2 algebraisch unabhängig über K, und K ist der genaue Konstantenkörper von F_1/K. Da zudem F_1/K als separabel vorausgesetzt ist, folgt dann, dass F_1 und F_2 auch linear disjunkt über K sind. Nun gilt $\tilde{A}(p_\infty) = b - \deg_{F_2/K} p_\infty \cdot \tau(B \cap F_1) = b - B(b) = b - b = 0$. Als Nächstes können wir den Divisor $\tilde{A}$ maximal entlang $P_{\infty,1}$ reduzieren und erhalten einen effektiven Divisor $A' \in \mathcal{D}_{L/F_2}$ mit

$$\tilde{A} = A' - lP_{\infty,1} + (F), \tag{4.1}$$

wobei $1 \leq l \leq g$ und (F) ein geeigneter Hauptdivisor von L/F_2 ist. Dadurch erhalten wir mit [Hes02, Proposition 8.2, S.14] dann $[A' - lP_{\infty,1}] = [\tilde{A}]$ mit einem eindeutigen und effektiven Divisor $A' \in \mathcal{D}_{L/F_2}$ vom Grad $1 \leq l \leq g$. Schließlich gilt $A'(p_\infty) = lp_\infty + (f)$ mit $(f) \in \mathcal{P}_{F_2/K}$ geeignet.

Wir müssen nun noch zeigen, dass A' in seiner Korrespondenzklasse $[A']_C$ eindeutig ist. Ist $B \in [A']_C$ mit $\tilde{B} = B' - rP_{\infty,1} + (G)$ wie in (4.1), so erhalten wir als Erstes $\tilde{B} = \tilde{A} + C + (H)$ mit einer konstanten Korrespondenz C vom Grad null. Wir reduzieren C entlang $P_{\infty,1}$ maximal und erhalten dann $\tilde{B} = \tilde{A} + \tilde{C} - sP_{\infty,1} + (\tilde{H})$ mit einer effektiven Korrespondenz $\tilde{C}$ und $1 \leq s \leq g$. Bilden wir p_∞ bezügliche $\tilde{B}$ ab, so erhalten wir schließlich $\tilde{C}(p_\infty) - sp_\infty + (h) = 0$, d.h. also $\tilde{C}(p_\infty) = sp_\infty$ und somit $\tilde{C} = sP_{\infty,1}$. Ingesamt erhalten wir nun $\tilde{B} = \tilde{A} + (\tilde{H})$ und können mit [Hes02, Proposition 8.2, S.14] dann auf $A' = B'$ schließen. □

Ist $A \in \mathcal{D}_{L/F_2}$ und A' wie in Lemma 4.3 mit mindestens einem inseparablen $P \in \mathrm{supp}(A')$, so folgt mit Hilfe von Lemma 2.10, dass $A' = F^{\star m} \cdot B$ mit $m \in \mathbb{N}$ maximal und einer separablen effektiven Korrespondenz $B \in \mathcal{D}_{L/F_2}$ ist. Für ein inseparables A' ersetzen wir dann A' durch B.

Definition 4.4. *Sei $A \in \mathcal{D}_{L/F_2}$. Dann wollen wir den wie in Lemma 4.3 bezeichneten effektiven Divisor A' mit $C(A) := A'$ bezeichnen, wenn A' separabel ist. Ansonsten setzen wir $A' = B$ und und $C(A) := B$.*

Betrachten wir Elemente $[a_0 - a_\infty] \in \mathcal{C}^0_{F_2/K}$, so können wir uns immer auf effektive Divisoren $a_0, a_\infty \in \mathcal{D}_{F_2/K}$ mit

$$\deg_{F_2/K} a_0,\ \deg_{F_2/K} a_\infty \leq g$$

beschränken. Wenn nichts Anderes festgelegt wird, so wollen wir dann für ein $[a] \in \mathcal{C}^0_{F_2/K}$ immer solch einen Repräsentanten in der Form $a = a_0 - a_\infty$ wählen. Das folgende Lemma ist später für die Interpolation der Norm einer Korrespondenz wichtig.

Lemma 4.5. *Sei $A \in \mathcal{D}_{L/F_2}$ und $p \in \mathcal{P}_{F_2}$ mit $p \neq p_\infty$ vom Grad eins und $C(A)(p - p_\infty) = C(A)(p) - lp_\infty + (f)$, wobei $g_{F_2/K} \geq l = \deg C(A)$ und $(f) \in \mathcal{P}_{F_2}$ ist. Ferner sei für den entlang p_∞ maximal reduzierten Divisor $C(A)(p)$ dann $C(A)(p) - lp_\infty = b_0 - \tilde{l}p_\infty + (f)$ mit $g_{F_2/K} \geq \tilde{l}$ und $(f) \in \mathcal{P}_{F_2/K}$. Ist $l = \tilde{l}$, so gilt $C(A)(p) = b_0$.*

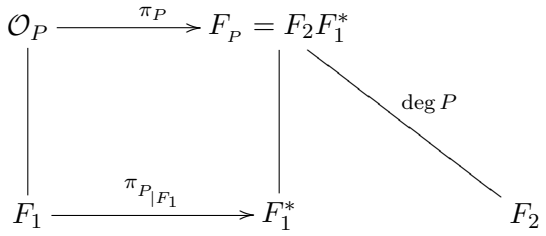
Beweis. Als Erstes sehen wir, dass $[p - p_\infty] \in \mathcal{C}^0_{F_2/K}$ ist. Daraus folgt zuerst $[C(A)(p - p_\infty)] = [C(A)(p) - lp_\infty] \in \mathcal{C}^0_{F_2/K}$ mit $l = \deg_{L/F_2} C(A)$. In dieser Klasse können wir nach [Hes02, Proposition 8.2, S.14] und Bemerkung kurz vorher, einen eindeutigen effektiven Divisor $b_0 \in \mathcal{D}_{F_2/K}$ so finden, dass

$$C(A)(p) - lp_\infty = b_0 - \tilde{l}p_\infty + (f)$$

mit $\deg_{F_2/K} b_0 = \tilde{l} \leq l \leq g$ und $\dim_K \mathcal{L}(b_0) \leq 1$ ist. Gilt nun $\tilde{l} = l$, so ist $C(A)(p) = b_0 + (f)$, und da b_0 effektiv ist und $\dim_K \mathcal{L}(b_0) \leq 1$ gilt, erhalten wir $C(A)(p) = b_0$. □

4.3 Nachweis der Existenz einer geeigneten p-regulären Basis

Sei $C(A) = \sum_i e_i P_i$ mit $P_i \in \mathbb{P}_{L/F_2}$. Wir wollen nun die Frage klären, welche Anforderungen wir an $p \in \mathbb{P}_{F_2/K}$ stellen müssen, so dass wir jeweils eine p-reguläre Basis von $P_{i,0}$ finden können. Dazu sei $P \in \mathbb{P}_{L/F_2}$ eine separable Primkorrespondenz. Dann erhalten wir folgendes Diagramm:



(4.2)

Bezeichnet π_P wieder die Restklassenabbildung von P, so soll $F_1^* := \pi_P(F_1)$, $x_1^* := \pi_P(x_1)$ und $y_1^* := \pi_P(y_1)$ bezeichnen. Damit ist F_1^* dann K-isomorph zu F_1 und die definierenden Gleichungen für F_1 und F_1^* gehen durch Vertauschen von x_1 mit x_1^* und y_1 mit y_1^* auseinander hervor. Auf Grund unserer Annahmen für F_1/K ist dann $(x_1^*) = r - np_\infty^*$ mit einem geeigneten effektiven Divisor $r \in \mathcal{D}_{F_1^*/K}$ und $n := [F_1^* : K(x_1^*)] = [F_1 : K(x_1)]$, d.h. die unendliche Stelle p_∞^* ist in F_1^* wieder total verzweigt. Seien $(x_1^*) = x_{1,0}^* - x_{1,\infty}^*$ und $(y_1^*) = y_{1,0}^* - y_{1,\infty}^*$. Sei

$$C_1 := \operatorname{supp} N_{F_P/F_2}(\operatorname{Con}_{F_P/F_1^*}(x_{1,\infty}^*)) \cup N_{F_P/F_2}(\operatorname{Con}_{F_P/F_1^*}(y_{1,\infty}^*))$$

und $C_2 := \operatorname{supp} \operatorname{disc}(F_P/F_2)$. Wir definieren nun $C := C_1 \cup C_2 \subseteq D_{F_2/K}$ und zeigen nun, dass die p-Regularität von P für ein $p \in \mathbb{P}_{F_2/K}$ vom Grad eins bereits aus $p \notin C$ folgt:

Satz 4.6. *Sei $P \in \mathbb{P}_{L/F_2}$ separabel und nicht-konstant sowie $p \in \mathbb{P}_{F_2/K}$ vom Grad eins. Dann sind folgende Aussagen äquivalent:*

(i) Es gilt $p_\infty \notin \operatorname{supp} P(p)$ und $P(p) = \sum_{i=1}^r q_i$ mit paarweise verschiedenen $q_i \in \mathbb{P}_{F_2/K}$ $(i = 1, .., r)$.

(ii) Es gilt $p \notin C$, P ist p-regulär und $\overline{P}^p = P(p)$.

Beweis. Gelte $p_\infty \notin \operatorname{supp} P(p)$ und $P(p) = \sum_{i=1}^r q_i$ mit paarweise verschiedenen $q_i \in \mathbb{P}_{F_2/K}$ $(i = 1, .., r)$. Wäre $p \in C$, so folgte entweder, dass p Diskriminantenteiler von F_P/F_2 ist oder es gilt

$$\operatorname{supp} \operatorname{Con}_{F_P/F_2}(p) \cap \operatorname{supp}(x_{1,\infty}^* + y_{1,\infty}^*) \neq \emptyset.$$

Im ersteren Falle könnten dann aber die q_i nicht paarweise verschieden sein, und im zweiten Falle würde dann im Widerspruch zur Voraussetzung $p_\infty \in \operatorname{supp} P(p)$ gelten. Das zeigt $p \notin C$. Nun ist x_1^* ganz bezüglich p genau dann, wenn

$$\nu_Q\left(\operatorname{Con}_{F_P/F_1^*}((x_1^*)\right) \geq 0 \quad \forall Q \in \mathbb{P}_{F_P/F_2} \text{ mit } Q|p$$

gilt, was wiederum genau dann der Fall ist, wenn $p_\infty \notin P(p)$ ist. Dies bedeutet also, dass x_1^* ganz bezüglich p ist. Ist $N_{L/F_2}(P_0) = f^r$ mit $f \in F_2[x_1]$ Primpolynom, so haben wir mit f das Minimalpolynom von x_1^* in F_P gefunden, wenn wir f noch normieren. Bezeichnen wir das eventuell normierte Primpolynom wieder mit f, so muss $f \in \mathcal{O}_p[x_1]$ gelten, da wir ansonsten einen Widerspruch zur Ganzheit von x_1^* bezüglich p erhalten.

Sei nun $\mathcal{B} = \{B_1, ..., B_n\} \subseteq P_0$ eine Basis von P_0 mit $\Omega M = \mathcal{B}$ und $\Omega := \{\omega_1, ..., \omega_n\} \subseteq F_1$ Ganzheitsbasis mit $n = [F_2 : K(x_2)]$. Ferner sei $\tilde{r} = [F_P : F_2(x_1^*)] \leq n$. Wir schreiben $\pi_P(y_1^j) = y_1^{*j}$ und $\pi_P(\omega_j) = \omega_j^*$ und

erhalten dann

$$F_P = \bigoplus_{i=0}^{\tilde{r}-1} \bigoplus_{j=0}^{\deg f-1} y_1^{*i} x_1^{*j} F_2 = \bigoplus_{i=0}^{\tilde{r}-1} \bigoplus_{j=0}^{\deg f-1} \omega_i^* x_1^{*j} F_2. \tag{4.3}$$

Auf Grund von (4.3) ist es nicht schwer einzusehen, dass $\tilde{r} = r$ mit $N_{L/F_2}(P_0) = f^r$ gilt. Ferner sei $M \in F_2[x_1]^{n\times n}$ obere Dreiecksmatrix in zeilenreduzierter Hermitenormalform und Ω o.B.d.A., so dass mit $J \subseteq \{1, ..., n\}$ dann $\{\pi_P(\omega_j) \mid j \in J\}$ genau dann unabhängig über $F_2(x_1^*)$ ist, wenn es $\{y_1^{*j} \mid j \in J\}$ ist. Gegebenenfalls normieren wir die Diagonalelemente von M und bezeichnen die so erhaltene Matrix wieder mit M und die Basis wieder mit $\mathcal{B}$.

Unsere Matrix M hat nun die Eigenschaft, dass die Einträge von M von der Form $m_{ii} = f$ und $m_{ji} = 0$ sind, wenn $i = 1, ..., r$ und $j = 1, ..., i-1$ für $i > 1$ ist. Dies bedeutet also für unsere Basis B_0, dass die Elemente B_i mit $i = 1, ..., r$ von der Form $f\omega_i$ sind. Die restlichen Elemente sind dann von der Gestalt $B_i = \omega_i + \sum_{j=1}^{i-1} m_{ji}\omega_j$ für $i = (r+1), ..., n$, wobei $m_{ji} = 0$ für $j > r$ ist, ansonsten ist $m_{ji} \in F_2[x_1]$ mit $\deg m_{ij} < \deg f$. Das bedeutet also, dass die Elemente B_i mit $i \geq r$ von der Form $B_i = \omega_i + \sum_{j=1}^{r} m_{ji}\omega_j$ sind, wobei $\deg m_{ji} < \deg f$ ist. Wenden wir nun auf diejenigen B_i mit $i \geq r$ die Restklassenabbildung π_P an, so erhalten wir mit $m_{ji}^* = \pi_P(m_{ji})$ und $\pi_P(B_i) = 0$ schließlich

$$-\omega_i^* = \sum_{j=1}^{r} m_{ji}^*\omega_j^* = \sum_{j=1}^{r} \sum_{k=1}^{\deg f-1} \lambda_{ji,k} x_1^{*k} \omega_j^* \,. \quad (\lambda_{ji,k} \in F_2)$$

Jetzt argumentieren wir wie folgt: Zuerst ist $-\omega_i^*$ ganz bezüglich p wegen $p_\infty \notin P(p)$, und die Elemente $x_1^{*k}\omega_j^*$ bilden eine Basis von F_P. Nun ist aber nach Voraussetzung $p \notin C$, was die Tatsache nach sich zieht, dass p kein Diskriminantenteiler von $\mathrm{disc}(F_P/F_2)$ ist. Damit können wir wie in Lemma 3.2 argumentieren, dass die Koeffizienten $\lambda_{ji,k}$ ganz bezüglich p sind, d.h. wir haben $\lambda_{ji,k} \in \mathcal{O}_p$. Aus $\pi_P(\lambda_{ji,k}) = \lambda_{ji,k}$ erhalten wir schließlich, dass auch die $m_{ji} \in \mathcal{O}_p[x_1]$ sind. Damit ist $\mathcal{B}$ dann p-regulär, und es ist $p \notin \mathcal{A}_{P,\Delta}$, wenn $\Delta := \{y_1^{*i} x_1^{*j} \mid j = 0, ..., \deg f - 1, i = 0, .., r-1\}$ ist, woraus aus Satz 2.16 schließlich $\overline{P}^p = P(p)$ folgt.

Ist umgekehrt $p \notin C$ und P regulär bezüglich p, so ist per Definition $p_\infty \notin \mathrm{supp}\, P(p)$ wegen $\overline{P}^p = P(p)$ und $\overline{P}_0^p \in \mathcal{O}_{F_2/K}$. Außerdem sind die auftretenden Primdivisoren $q_i \in \mathbb{P}_{F_2/K}$ in $P(p) = \sum_{i=1}^{r} q_i$ paarweise verschiedenen, da $p \notin \mathcal{A}_{P,\Delta}$ mit $\Delta \subseteq \{x_1^{*j} y_1^{*i} \mid i, j \in \{0, ..., [F_P : F_2^*] - 1\}\}$ ist. □

Sei $A \in \mathcal{D}_{L/F_2}$, $p \in \mathbb{P}_{F_2/K}$ vom Grad eins und $C(A) = \sum e_i P_i$ mit separablen $P_i \in \mathbb{P}_{L/F_2}$. Gilt $C(A)(p) = \sum e_i P_i(p)$, wobei $P_i(p) = \sum_j q_{ij}$

sein soll mit paarweise verschiedenen Primdivisoren q_{ij} aus F_2, und $p_\infty \notin \operatorname{supp} C(A)(p)$, so folgt aus Satz 4.6 die Gleichheit $C(A)(p) = \sum e_i \overline{P}_i^p$. Außerdem ist $N_{L/F_2}(C(A)_0) = \prod_i N_{L/F_2}(P_{i,0})^{e_i} \in \mathcal{O}_p[x_1]$ normiert, wenn wir für die Primideale $P_{i,0}$ jeweils die Basen aus Satz 4.6 nehmen. Daraus erhalten wir dann aber

$$N_{F_2/K}((C(A)(p))_0) = \prod_i N_{F_2/K}(\overline{P}_{i,0}^p)^{e_i} = \tau(\overline{N_{L/F_2}(C(A)_0)}^p), \qquad (4.4)$$

wobei wir mit $\overline{N_{L/F_2}(C(A)_0)}^p$ dasjenige normierte Polynom in $K[x_1]$ meinen, dass wir erhalten, wenn wir auf die Koeffizienten des normierten Polynoms $N_{L/F_2}(C(A)_0) \in \mathcal{O}_p[x_1]$ die Restklassenabbildung $\pi : \mathcal{O}_p \longrightarrow K$ anwenden. Außerdem können wir o.B.d.A. annehmen, dass $N_{F_2/K}(C(A)(p)_0) \in K[x_2]$ normiert ist. Haben wir also genügend geeignete Stellen $p \in \mathcal{D}_{F_2/K'}$ vom Grad eins in einer geeigneten endlichen Erweiterung K'/K, so können wir die Korrespondenz $C(A)$ rekonstruieren, indem wir seine Norm durch eine Interpolation rekonstruieren und dann die Hochhebung nach $\mathcal{O}_{L/F_2}$ berechnen.

4.4 Die obere Schranke für die Anzahl der Stellen vom Grad eins

Als Nächstes brauchen wir eine Aussage über eine obere Schranke $s \in \mathbb{N}$ für die benötigte Anzahl der Stellen vom Grad 1 in F_2/K'. Dazu dient das folgende Lemma:

Lemma 4.7. *Sei $A \in \mathcal{D}_{L/F_2}$ ohne konstanten Träger und effektiv und weiter*

$$N_{L/F_2}(A_0) = x_1^r + \sum_{i=0}^{r-1} x_1^i \frac{f_i}{g_i} \quad (r \in \mathbb{N})$$

mit $g_i \in K[x_2]$ und $f_i \in K[x_2, y_2]$. Dann gilt:

$$|\nu_{p_\infty}(g_i)|, |\nu_{p_\infty}(f_i)| \leq n^2 \deg_{L/F_2} A^\star \quad (f_i \neq 0)$$

wobei $n = [F_1 : K(x_1)]$ ist.

Beweis. Wir zeigen die Behauptung zuerst für einen nicht-konstanten Primdivisor $P \in \mathbb{P}_{L/F_2}$. Seien $\tilde{f} := P_0 \cap F_2[x_1]$ und $\tilde{g} := P_0^\star \cap F_2[x_1]$. Dann sind $\tilde{f}$ und $\tilde{g}$ irreduzibel in $F_2[x_1]$. Seien nun $h_1, h_2 \in K[x_2]$ so, dass $\tilde{f}h_1, \tilde{g}h_2 \in K[x_1, x_2, y_2]$ gilt. Wir setzen dann $f := h_1\tilde{f}$ und $g := h_2\tilde{g}$. Auf Grund unserer Voraussetzung an die Funktionenkörper F_1/K und F_2/K ist der Rosati, angewandt auf f und g, nichts weiter als das Vertauschen von x_1 mit x_2 und y_1 mit y_2.

Sei E_i die normale Hülle von $F_i/K(x_i)$. Für $f = \sum_{l=0}^{m} f_l x_j^l \in F_i[x_j]$ definieren wir dann $\sigma(f) := \sum_{l=0}^{m} \sigma(f_l) x_j^l$ für ein $\sigma \in G_K(E_i/K(x_i))$. Wir bezeichnen dann mit n_i jeweils die Polynomnorm

$$n_i : F_i[x_j] \longrightarrow K(x_i)[x_j], \quad f \longmapsto \prod_{\sigma \in G_K(E_i/K(x_i))} \sigma(f) \ ,$$

wobei $i, j \in \{1, 2\}$ mit $i \neq j$ ist. Für ein $\alpha \in L/F_2$ setzen wir noch

$$\deg \alpha := -\nu_{P_{\infty,1}}(\alpha) \tag{4.5}$$

und den Grad in $F_2[x_1]$ bezeichnen wir mit $\deg_{F_2[x_1]}$. Nach Voraussetzung sind f und g irreduzibel in $F_2[x_1]$. Wir unterscheiden nun zwei Fälle: Sind f und g beide in $K[x_1, x_2] \subseteq F_2[x_1]$, so erhalten wir aus $f^\star \in P_0^\star$ als erstes $f^\star = gs$ mit einem geeigneten $s \in K[x_1, x_2]$. Da f irreduzibel ist, muss s in K liegen, woraus dann $\deg f^\star = \deg g$ folgt.

Im anderen Fall, wo mindestens f oder g nicht in $K[x_1, x_2]$ aber in $F_2[x_1]$ liegt, betrachten wir die Polynomnorm $n_2(f) = f \cdot f^{(2)} \cdot \ldots \cdot f^{(n)} = h_1 \cdot r$ und $n_2(g) = g \cdot g^{(2)} \cdot \ldots \cdot g^{(n)} = h_2 \cdot t$, wobei $h_1, h_2, r, t \in K[x_1, x_2]$ und h_1, h_2 irreduzibel mit $f | h_1$ und $g | h_2$ sind und wir noch $f^{(1)} := f$ und $g^{(1)} := g$ gesetzt haben.

Aus $h_1^\star \in P_0^\star$ erhalten wir dann $g | h_1^\star$ und daraus folgt $n_2(g) \cdot s = h_1^{\star n}$ mit $s \in K[x_1, x_2]$ geeignet. Schließlich erhalten wir $h_1^\star | h_2$ und dann $h_1^\star = h_2$. Wollen wir nun den Grad von $f^\star$ bestimmen, so benötigen wir die in (4.5) definierte Gradfunktion, da durchaus $f^\star \notin F_2[x_1]$ gelten kann. Damit erhalten wir wegen $f | h_1$ und $h_1^\star = h_2$ die folgende Abschätzung

$$\deg f^\star \leq \deg h_1^\star = \deg h_2 \leq \deg n_2(g) = n \cdot \deg g \ .$$

Insgesamt erhalten wir nun $\deg f^\star \leq n \cdot \deg g$, woraus dann

$$\deg \left(h_1^{\star l} \cdot N_{L/F_2}(P_0)^\star \right) = \deg f^{\star l} \leq n^2 \cdot \deg_{L/F_2} P^\star \tag{4.6}$$

mit $l \leq n$ folgt, wobei l der Relativgrad von L_P ist. Ist nun

$$\tilde{f} = x_1^r + \sum_{i=0}^{r-1} x_1^i \frac{\tilde{f}_i}{g_i},$$

so wählen wir als $h_1 := \mathrm{kgV}(\{g_1, \ldots, g_r\})$ und erhalten dann ein $f = h_1 x_1^r + \sum_{i=1}^{r-1} x_1^i f_i \in K[x_1, y_2, x_2]$, d.h. es ist $f_i \in K[x_2, y_2]$. Aus (4.6) folgt nun, dass $\max\{\deg h_1^\star, \deg f_1^\star, \ldots, \deg f_{r-1}^\star\} \leq n^2 \deg_{L/F_2} P^\star$ ist, woraus wir dann wiederum $|\nu_{p_\infty}(\tilde{f}_i)|, |\nu_{p_\infty}(g_i)| \leq n^2 \deg_{L/F_2} P^\star$ erhalten ($f_i \neq 0$). Für ein effektives $A \in \mathcal{D}_{L/F_2}$ mit $A = \sum e_i P_i$ wenden wir die Aussage dann auf jedes P_i an und erhalten somit die Behauptung. $\square$

Bemerkung 4.8. *Ist* $[F_i : K(x_i)] = 2$*, so vereinfacht sich (4.6) zu*

$$\deg\left(h_1^{\star l} \cdot N_{L/F_2}(P_0)^\star\right) \leq n \cdot \deg_{L/F_2} P^\star \ ,$$

da im Falle, dass der Trägheitsgrad gleich 2 *ist, der Primdivisor* P *ein Hauptdivisor ist und somit eine triviale Korrespondenz darstellt. Damit werden in diesem Falle die Grade* $\deg_{F_2[x_1]} g_i$ *und* $\deg_{F_2[x_1]} f_i$ *nur durch* $\deg_{L/F_2} A^\star$ *bestimmt.*

Um den Grad des Rosati $C(A)^\star$ abschätzen zu können, bedienen wir uns folgendem Lemma:

Lemma 4.9. *Sei* $g \geq 1$*,* $A \in \mathcal{D}_{L/F_2K}$ *effektiv, ohne konstanten Träger und vom Grad* $\deg_{L/F_2K} A = g$*. Ferner sei* $\alpha \in \mathrm{End}_K(J_{X_2})$ *der zur Korrespondenzklasse* $[A]_C$ *entsprechende Endomorphismus und* $E_{_K} := \mathrm{End}^0_K(J_{X_2})$*. Dann gilt*

$$\deg_{L/F_2K} A^\star \leq \frac{\mathrm{Tr}_{E_{_K}/\mathbb{Q}}(\alpha\alpha^\star)}{2},$$

wobei $\mathrm{Tr}_{E_{_K}/\mathbb{Q}}$ *die Spur von* $E_{_K}$ *bezeichnet und* * *der Rosati von* $E_{_K}$ *ist.*

Beweis. Mit der Spurformel (2.28) wissen wir, dass

$$\mathrm{Tr}_{E_{_K}/\mathbb{Q}}(\alpha\alpha^\star) = \langle A, A\rangle = 2\deg_{L/F_2} A \deg_{L/F_2} A^\star - A.A > 0$$

gilt. Aus [Eic63, Kapitel 5, S. 310 ff.] folgt $\langle A, A\rangle \geq 2\deg_{L/F_2} A^\star$, wenn A den Voraussetzungen des Lemmas genügt und $g \geq 1$ ist. Daraus erhalten wir dann die gewünschte Abschätzung. □

4.5 Algorithmus zum Interpolieren der Norm einer Korrespondenz

In diesem Abschnitt soll D die Einheitskorrepondenz und F die Frobeniuskorrespondenz in $\mathcal{D}_{L/F_2}$ bezeichnen. Sei nun $J_{X_2} \sim_K B^r$ mit einer über K einfachen abelschen Varietät. Wir betrachten die zentral einfache Algebra $E_{_K} := \mathrm{End}^0_K(J_{X_2})$ mit Zentrum $F := Z(E_{_K})$, wobei $F = \mathbb{Q}(\pi_{_K})$ mit $[F : \mathbb{Q}] = l$, $d := \mathrm{Deg}(E_{_K})$ und $e := d^2 l$ ist. Sei $\mathcal{O} \subseteq E_{_K}$ eine Ordnung, $\beta_1, ..., \beta_e \subseteq E_{_K}$ eine $\mathbb{Z}$-Basis von $\mathcal{O}$ und $\alpha = \sum_{i=1}^e \lambda_i\beta_i \in \mathcal{O}$ mit $\lambda_i \in \mathbb{Z}$ so, dass die den Elementen β_i entsprechenden Korrespondenzen $B_i \in \mathcal{D}_{L/F_2K}$ bereits berechnet wurden. Mit $\Gamma = \sum_{i=1}^e \lambda_i B_i$ bezeichnen wir dann die dem Element α entsprechende Korrespondenz. Wir nehmen nun an, wir haben ein $m \in \mathbb{N}$ so, dass $\frac{\alpha}{m}$ ganz über $\mathbb{Z}$ ist. Wir wollen nun testen, ob $\frac{\alpha}{m} \in \mathrm{End}_K(J_{X_2})$ liegt.

Ist $\frac{\alpha}{m} \in \mathrm{End}_K(J_{X_2})$ und bezeichnet $[A]_C$ die zu $\frac{\alpha}{m}$ gehörige Korrespondenzklasse, so ist $C(A)$ effektiv und vom Grad $\leq g$. Sei $A' \in [A]_C$ wie in Lemma 4.3 mit $A' = \sum e_i P_i$ und $P_i \in \mathbb{P}_{L/F_2K}$. Ist P_i inseparabel, so erhalten wir aus Lemma 2.10, dass es ein maximales $s_i \in \mathbb{N}$ so gibt, dass $P_i = (F^\star)^{s_i} A_i$ mit einer separablen Primkorrespondenz A_i ist. Insgesamt erhalten wir dann ein maximales $s \in \mathbb{N}$, so dass $A' = F^{\star s} \cdot B$ vom Grad $q^s t$ mit effektivem und separablem $B \in \mathcal{D}_{L/F_2K}$ vom Grad t ist ($q \nmid t$). Wir haben dann in Definition 4.4 $C(A) = B$ gesetzt. Für das der Korrespondenz A' entsprechende Element $\frac{\alpha}{m}$ gilt dann $\frac{\alpha}{m} = \pi^{\star s}\beta$ mit einem geeigneten $\beta \in \mathrm{End}_K(J_{X_2})$, wenn $\pi \in \mathrm{End}_K(J_{X_2})$ das der Frobeniuskorrespondenz $F \in \mathcal{D}_{L/F_2}$ entsprechende Element ist. Aus (2.8) folgt aber, dass $F^s \cdot F^{\star s} = q^s$ mit $q = p^n$ ist, was gleichbedeutend ist mit $\pi^s \cdot \pi^{\star s} = q^s$ in $\mathrm{End}_K(J_{X_2})$. Der Korrespondenz $C(A)$ entspricht also das Element $\beta = (\pi^s\alpha)/(mq^s)$ und ist $g = q^r t$ mit $p \nmid t$, so haben wir $s \leq r$.

Im inseparablen Fall testen wir dann also, ob $(\pi^s\alpha)/(mq^s) \in \mathrm{End}_K(J_{X_2})$ ist, und wir setzen dazu $\Gamma' := F^s \cdot \Gamma$ und $m' := mq^s$ mit $s \leq r$. Der Test, ob $\beta \in \mathrm{End}_K(J_{X_2})$ liegt, verläuft dann genauso wie im separablen Fall. Der Einfachheit halber wollen wir deshalb annehmen, dass A' separabel ist.

Um die Notation zu vereinfachen, setzen wir o.B.d.A. voraus, dass die Korrespondenz $C(A)$ den Grad g besitzt und bezeichnen mit $\phi \in E_K$ den von Γ induzierten Endomorphismus. Ferner sei $n := [F_2 : K(x_2)]$. Zudem soll $C(A)$ noch eine Primkorrespondenz sein. Später werden wir sehen, wie wir den allgemeinen Fall behandeln. Bezeichne

$$f = x_1^g + \sum_{i=0}^{g-1} x_1^i \frac{f_i}{g_i}$$

die Norm von $C(A)_0$ mit $f_i \in K[x_2, y_2]$ und $g_i \in K[x_2]$.

Auffinden von geeigneten Stellen

Mit $\mathbb{P}_K^1$ bezeichnen wir die Stellen $p \in \mathbb{P}_{F_2/K}$ vom Grad 1. Ist $p \in \mathbb{P}_K^1$, so betten wir mittels

$$\Phi : \mathbb{P}_K^1 \longrightarrow \mathcal{C}_{F_2}^0, \quad p \longmapsto p - p_\infty$$

die Stellen von $\mathbb{P}_K^1$ in $\mathcal{C}_{F_2}^0$ ein. Sei nun $p_i \in \mathbb{P}_K^1$ und $P := \Phi(p_i)$ mit $\mathrm{ggT}(\mathrm{ord}(P), m) = 1$. Als erstes erhalten wir

$$m \cdot C(A)(P) = \phi(P) \text{ und } \mathrm{ggT}(\mathrm{ord}(C(A)(P)), m) = 1, \tag{4.7}$$

da die Ordnung des Bildes $C(A)(P)$ des von der Korrespondenz $C(A)$ induzierten Endomorphismuses auf $\mathcal{C}_{F_2/K}^0$ ein Teiler von $\mathrm{ord}(P)$ ist. Nun berechnen wir ein $t \in \mathbb{N}$ mit $t \cdot m \equiv 1 \mod \mathrm{ord}(P)$. Daraus folgt dann

$t \cdot m \equiv 1 \mod \mathrm{ord}(\phi(P))$, da ϕ ein Endomorphismus von $\mathcal{C}^0_{F_2/K}$ ist und somit $\mathrm{ord}(\phi(P))|\mathrm{ord}(P)$ gilt, und schließlich erhalten wir $C(A)(P) = t \cdot \phi(P) =: Q$ mit eindeutigem Q auf Grund von $\mathrm{ggT}(\mathrm{ord}(P), m) = 1$. Dann reduzieren wir Q bezüglich p_∞ zu einem $\tilde{Q} \in \mathcal{C}^0_{F_2/K}$, wobei $\tilde{Q} = a - rp_\infty$ mit $0 \leq r \leq g$ und $a \in \mathcal{D}_{F_2/K}$ effektiv ist. Ist $r = g$ und $a = \sum q_i$ mit paarweise verschiedenen $q_i \in \mathbb{P}_{F_2/K}$, so bedeutet das $C(A)(p) = a$ wegen Lemma 4.5 und $p_\infty \notin \mathrm{supp}\, a$. Also können wir auf die P_i von $C(A) = \sum e_i P_i$ Satz 4.6 anwenden.

Bezeichnen wir für solch ein p mit π_p die Restklassenabbildung $\mathcal{O}_p \longrightarrow K$ und mit $\alpha := \pi_p(x_2),\ \beta := \pi_p(y_2)$, so erhalten wir mit

$$N_{F_2/K}((C(A)(p))_0) = x_2^g + \sum_{j=0}^{g-1} c_{ji} x_2^j = \tau\left(\overline{N_{L/F_2}(C(A)_0)}^p\right) \in K[x_2]$$

wie in (4.4) schließlich

$$x_2^g + \sum_{j=0}^{g-1} c_{ji} x_2^j = x_2^g + \sum_{j=0}^{g-1} \frac{f_j(\alpha,\beta)}{g_j(\alpha)} x_2^j.$$

Dabei ist zu beachten, dass $g_j(\alpha) \neq 0$ gilt, da $C(A)_0$ nach Voraussetzung p-regulär ist.

Abschätzung der Grade der Polynome in x_2

Mit Lemma 4.7 und Lemma 4.9 erhalten wir die Abschätzung

$$|\nu_{p_\infty}(f_i)|, |\nu_{p_\infty}(g_i)| \leq n^2 \frac{\mathrm{Tr}_{E_K/\mathbb{Q}}(\alpha\alpha^\star)}{2m^2} =: s\ , \quad (f_i \neq 0) \tag{4.8}$$

wobei hier $n = [F_2 : K(x_2)]$ ist. Nach [Hes02] existieren Ganzheitsbasen $\Omega := \{\omega_1, ..., \omega_n\}$ und $\Omega_\infty := \{\omega_{\infty 1}, ..., \omega_{\infty n}\}$ von $\mathcal{O}_{F_2/K}$ und $\mathcal{O}_{F_2/K,\infty}$, so dass $\omega_j = x_2^{-d_j}\omega_{\infty j}$ mit ganzen Zahlen $d_1 \geq ... \geq d_n$ gilt und die Basis Ω_∞ bezüglich p_∞ reduziert ist. Dies bedeutet, dass für $f_i \in K[x_2, y_2] \subseteq \mathcal{O}_{F_2/K}$ eine Darstellung

$$f_i = \sum \mu_{ji}\omega_j = \sum (\mu_{ji} x_2^{-d_j}) x_2^{d_j} \omega_j = \sum (\mu_{ji} x_2^{-d_j}) \omega_{\infty j}$$

mit $\mu_{ji} \in K[x_2]$ existiert und unter der Voraussetzung $d_j \leq 0$ erhalten wir

$$|\nu_{p_\infty}(f_i)| = \max_j |\nu_{p_\infty}(\mu_{ji} x_2^{-d_j} \omega_{\infty j})| \quad (f_i \neq 0). \tag{4.9}$$

Anderenfalls müssen wir beide Seiten in (4.9) mit einer geeigneten Potenz x_2^r so multiplizieren, dass jeweils die Ausdrücke $\mu_{ji} x_2^{-d_j} x_2^r$ in $K[x_2]$ liegen. Daraus erhalten wir aber in jedem Fall eine obere Schranke für die Grade der

Polynome μ_{ji} und damit eine obere Schranke $\mathcal{T} \in \mathbb{Z}^{>0}$ für die auftretenden Polynome in der folgenden Darstellung von f_i durch

$$f_i = \sum_{j=0}^{n-1} y_2^j h_j^{(i)} \text{ mit } h_j^{(i)} = \sum_{l=0}^{\mathcal{T}} \lambda_{lj}^{(i)} x_2^l \,, \tag{4.10}$$

wobei $\lambda_{lj} \in K$. Die Nenner $g_i \in K[x_2]$ besitzen die Gestalt

$$g_i = \sum_{l=0}^{s/n} \mu_{li} x_2^l \,. \tag{4.11}$$

Aufstellen des Gleichungssystemes

Auf Grund unserer Voraussetzungen ist $|\nu_{p_\infty}(x_2)| = n$ und $|\nu_{p_\infty}(y_2)| := \gamma > 0$. Für jedes f_j benötigen wir also höchstens $\mathcal{S}_1$ und für jedes g_j maximal $\mathcal{S}_2$ Koeffizienten, insgesamt also $\mathcal{S} := \mathcal{S}_1 + \mathcal{S}_2$, wobei

$$\mathcal{S}_1 := \sum_{j=0}^{n-1} |\lfloor (\mathcal{T} - j\gamma)/n \rfloor + 1| = \sum_{j=0}^{n-1} s_j, \quad \text{und} \quad \mathcal{S}_2 := (\tilde{s}+1) \tag{4.12}$$

ist mit $\tilde{s} := s/n$ ist. Um f_j und g_j zu berechnen, müssen wir schließlich das Gleichungssystem $\mathcal{M}_j v_j = 0$ mit $\mathcal{M}_j :=$

$$\begin{pmatrix} 1 & \alpha_1 & \dots & \alpha_1^{s_0} & \dots & \beta_1^{n-1} & \dots & \beta_1^{n-1}\alpha_1^{s_{n-1}} & -c_{ji} & -c_{ji}\alpha_1 & \dots & -c_{ji}\alpha_1^{\tilde{s}+1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & \alpha_r & \dots & \alpha_r^{s_0} & \dots & \beta_r^{n-1} & \dots & \beta_r^{n-1}\alpha_r^{s_{n-1}} & -c_{ji} & -c_{ji}\alpha_r & \dots & -c_{ji}\alpha_r^{\tilde{s}+1} \end{pmatrix} \tag{4.13}$$

und

$$v_j := \begin{pmatrix} \lambda_{00}^{(j)} & \cdots & \lambda_{s_{00}}^{(j)} & \cdots & \lambda_{0\,n-1}^{(j)} & \cdots & \lambda_{s_{n-1}\,n-1}^{(j)} & \mu_{0i} & \cdots & \mu_{\tilde{s}j} \end{pmatrix}^t \tag{4.14}$$

lösen, wobei $0 \le j \le g-1$ und die Einträge $\lambda_{ij}^{(j)}, \mu_{kl}$ wie in (4.10) und (4.11) sind. Da getestet werden soll, ob $\frac{\alpha}{m}$ ein Endomorphismus aus $\mathrm{End}_K(J_{X_2})$ ist, können wir uns auf Lösungen aus $K^{\mathcal{S}}$ beschränken.

Um aber genügend Elemente $P \in \mathcal{C}_{F_2}^0$ mit der Eigenschaften wie in (4.7) zu erhalten, müssen wir eventuell eine endliche Erweiterung von K vornehmen. Da die zugehörigen Ideale zu den Korrespondenzen allesamt durch Terme aus $K(x_2, y_2, x_1, y_1)$ beschrieben sind, können wir diese auch als Korrespondenzen von F_1F_2'/F_2' auffassen, wenn $F_2' = F_2K'$ mit einer endlichen Erweiterung K'/K ist.

Auffinden geeigneter Erweiterungsgrade von K'/K

Sei $C(A) = \sum_{i=1}^{t} e_i P_i$, $M_1 := \bigcup \mathcal{A}_{P_i}$ und

$$M_2 := \left\{ p \in \mathbb{P}_{F_2/K} \mid P_i \text{ ist nicht } p\text{-ganz für ein } i \in \{1, ..., t\} \right\}.$$

Dann ist $M := M_1 \cup M_2$ endlich. Da die Untergruppe der mq^s-Torsionspunkte in $\mathcal{C}^0_{F_2\overline{K}/\overline{K}}$ endlich ist, können wir genügend Punkte $p - p_\infty \in \mathcal{C}^0_{F_2\overline{K}/\overline{K}}$ mit $p \in \mathbb{P}^1_{\overline{K}}$ finden, so dass sowohl

$$p \notin M \text{ als auch } \mathrm{ggT}(\mathrm{ord}(p - p_\infty), mq) = 1 \tag{4.15}$$

gilt. Daraus folgt, dass wir stets eine geeignete endliche Körpererweiterung K'/K bestimmen können, so dass wir genügend viele geeignete Elemente $P \in \mathcal{C}^0_{F_2'/K'}$ mit der Eigenschaft (4.15) vorliegen haben. Um eine Aussage über das Verhalten der Ordnung von Elementen in $\mathcal{C}^0_{F_2'}$ im Vergleich zu $\mathcal{C}^0_{F_2}$ zu machen, benötigen wir eine Definition:

Definition 4.10. *Sei l eine Primzahl und $l \neq p = \mathrm{char}(K)$. Dann ist $d(l) := kgV(l-1, ..., l^{2g}-1)$. Ist $l = p$, so definieren wir $l(p) := kgV(l-1, ..., l^g-1)$.*

Mit $h(K')$ wollen wir die Klassenzahl von $\mathcal{C}^0_{F_2K'/K'}$ bezeichnen. Ist $L_K(t)$ das L-Polynom von F_2/K, so erhalten wir $h(K') = L_{K'}(1) = f_{\pi_{K'}}(1)$, wenn $f_{\pi_{K'}}$ das charakteristische Polynom des Frobeniusendomorphismus von $\mathrm{End}_{K'}(J_{X_2})$ bezeichnet. Wir wollen bei Bedarf endliche Konstantenkörpererweiterungen F_2K'/K' von F_2/K bilden, so dass in der Klassenzahl $h_{K'}$ möglichst wenig Primteiler von mq^s vorkommen. Dafür sind folgende Aussagen von Nutzen ([Ros73, Corollary 1, Proposition 3 und Proposition 4, p. 289]):

Satz 4.11.
1. *Sei l eine Primzahl. Gilt $l|h(K)$ und $l|n$ mit $n = [K' : K]$, so folgt $l|\,(h(K')/h(K))$.*
2. *Angenommen l ist eine Primzahl mit $l \nmid h(K)$ und $ggT(d(l), n) = 1$. Dann gilt $l \nmid h(K')$, wobei $[K' : K] = n$ ist.*
3. *Sei l eine Primzahl. Ferner sei n minimal mit $l|h(K')$ und $[K' : K] = n$. Dann gilt $n|d(l)$.*

Um möglichst zu vermeiden, dass Teiler von $mq^s = \prod p_i^{e_i}$ in $h_{K'}$ auftreten, wählen wir dann $n \in \mathbb{N}$ minimal mit $\mathrm{ggT}(n, mq) = 1 = \mathrm{ggT}(n, \prod l(pi))$. Wir wissen aber, dass nur endlich viele solcher Erweiterungen nötig sind.

Eindeutigkeit der Lösung

Da die Norm f von $C(A)_0$ bezüglich unserer Ganzheitsbasis Ω als normiertes Polynom eindeutig ist, müssen je zwei Lösungen aus $K^{\mathcal{S}}$ denselben rationalen Ausdruck f_i/g_i ergeben, wenn $\frac{\alpha}{m} \in \mathrm{End}_K(J_{X_2})$ ist. Sind etwa $v, w \in \ker \mathcal{M}_i$, dann ergibt sich $f_{i,v} = f_i \cdot h_v$ und $g_{i,v} = g_i \cdot h_v$ bzw. $f_{i,w} = f_i \cdot h_w$ und $g_{i,w} = g_i \cdot h_w$ also jeweilige Lösungen für f_i und g_i durch die Koeffizienten von v bzw. w, wobei hier noch $h_v, h_w \in K'[x_2, y_2]$ sind und K' eine endliche

Erweiterung von K ist. Damit erhalten wir $f_{i,v+w} = f_i(h_v+h_w)$ und $g_{i,v+w} = g_i(h_v + h_w)$, d.h. also $f_{i,v}/g_{i,v} = f_{i,w}/g_{i,w} = f_{i,w+v}/g_{i,w+v}$. Es reicht also ein nicht-triviales Element aus $\ker \mathcal{M}_i$ zu bestimmen.

Haben wir nun das Polynom $f = x_1^g + \sum_{j=0}^{g-1}(f_i/g_i)x_1^j$ bestimmt, so berechnen wir die Hochhebung $f\mathcal{O}_{L/F_2} = \prod_{i=1}^{n} P_{i,0}^{e_i}$ mit $P_i \in \mathbb{P}_{L/F_2}$ und $e_i \geq 0$. Ist $f\mathcal{O}_{L/F_2}$ kein Hauptideal, so können wir mit Hilfe der Korrespondenzpaarung eine effektive Korrespondenz B berechnen, welche dem Element $\frac{\pi^s\alpha}{mq^s}$ entspricht: Ist etwa $P_i = \sum_{k=1}^{n} q_{ki}B_k$ mit $q_{ki} \in \mathbb{Q}$, so erhalten wir $\langle P_i, B_j\rangle = \mu_{ij} = \sum_{k=1}^{n} q_{ki}\langle B_k, B_i\rangle$ und lösen dann das Gleichungssystem $Nq_i = m_i$ mit $N := (\langle B_i, B_j\rangle)_{1\leq i,j\leq n}$, $q_i := (q_{i1}, \ldots, q_{ni})^t$ und $m_i := (\mu_{1i}, \ldots, \mu_{ni})$ für $i = 1, ..., n$. Damit können wir den Korrespondenzen P_i Elemente aus $\mathrm{End}_K(J_{X_2})$ zuordnen und eine Darstellung $B := \prod_{i=1}^{n} P_{i,0}^{e_i'}$ mit $e_i' \in \mathbb{Z}^{\geq 0}$ geeignet und $e_i \geq e_i' > 0$ bezüglich $\frac{\pi^s\alpha}{mq^s}$ berechnen.

Der Grad von $C(A)$

Im Allgemeinen wissen wir nur, dass $1 \leq \deg C(A) \leq g_{F_2/K}$ gilt. Deshalb beginnen wir mit der Annahme, dass $1 \leq \deg C(A) = l \leq g_{F_2/K}$ ist. Sei die Stelle p eine geeignete Stelle vom Grad eins. Wir reduzieren dann $C(A)(p)$ maximal entlang p_∞ zum effektiven Divisor b_0. Gilt nun $C(A)(p - lp_\infty) = C(A) - lp_\infty = b_0 - \tilde{l}p_\infty + (f)$ und ist $\tilde{l} > l$, so haben wir einen Widerspruch erhalten und wissen, dass die Korrespondenz $C(A)$, sofern sie überhaupt existiert, mindestens den Grad $\tilde{l}$ haben muss. Im weiteren Verlauf des Algorithmus können wir uns dann auf $\deg C(A) \geq \tilde{l}$ beschränken. Anderenfalls versuchen wir, genügend viele geeignete Stellen vom Grad eins zu finden. War die Berechnung erfolglos, so gehen wir zum nächsthöheren möglichen Grad über.

Das Zerlegungsverhalten von $C(A)(p)$

Zudem kommt noch, dass wir keine genaue Aussage über das Zerlegungsverhalten von $C(A)$ machen können. Ist $C(A) = \sum e_iP_i$, so können wir aber o.B.d.A. $p \in \mathbb{P}_K^1$ so wählen, dass $\mathrm{supp}\, P_i(p) \cap \mathrm{supp}\, P_j(p) = \emptyset (i \neq j)$ und $p_\infty \notin \mathrm{supp}\, P_j(p)$ gilt sowie dass die Primdivisoren q_{ij} in der Darstellung $P_i(p) = \sum_j q_{ij}$ paarweise verschieden sind. Wenn mindestens für einen der Exponenten $e_i > 1$ gilt, so müssen wir dies im Bild $C(A)(p)$ berücksichtigen, da wir in diesem Fall niemals erreichen können, dass $C(A)(p)$ von der Form $C(A)(p) = \sum_i q_i$ ist mit paarweise verschieden q_i. Unter den gemachten Voraussetzungen gehen wir nun folgendermaßen vor: Wir machen eine Fallunterscheidung für die endlich vielen Möglichkeiten der Zerlegung von $C(A)$ in Primdivisoren. Auf Grund unserer speziellen Wahl von p läßt sich das Zerlegungsverhalten im Bild $C(A)(p)$ wiederfinden, d.h. also aus

$C(A) = \sum e_i P_i$ folgt $C(A)(p) = \sum e_i P_i(p)$, wobei $\sum P_i(p) = \sum q_i$ aus paarweise verschiedenen Primdivisoren besteht. Wir müssen hier aber noch darauf achten, dass eventuell auch Diskriminantenteiler der F_{P_i} auftreten können. Insgesamt müssen also die endlich vielen Möglichkeiten einer Zerlegung von $C(A)$ in Primdivisoren durchtesten. Wir können nun unseren Algorithmus formulieren:

Algorithmus 5: Approximation

Input: 1.) $\mathcal{O}_{L/F_2}$ und g,
2.) $d := \mathrm{Deg}(E_K)$ und $l := [F : \mathbb{Q}]$
3.) eine $\mathbb{Z}$-Basis $\{\beta_1, ..., \beta_{d^2 l}\} \subseteq E_K$ einer Ordnung $\mathcal{O} \subseteq E_K$,
4.) $\alpha = \sum_{i=1}^{n} \lambda_i \beta_i \in \mathcal{O}$ mit $\lambda_i \in \mathbb{Z}$,
5.) Korrespondenzen $B_1, ..., B_n \subseteq \mathcal{D}_{L/F_2}$, die jeweils $\beta_1, ..., \beta_{d^2 l}$ entsprechen,
6.) ein $m \in \mathbb{N}$ so, dass $\frac{\alpha}{m}$ ganz über $\mathbb{Z}$ ist

Output: Das Tupel $\langle B, \frac{\pi^k \alpha}{mq^k} \rangle$, wobei B eine effektive Korrespondenz $B \in \mathcal{D}_{L/F_2}$ ohne Konstanten Träger ist, welche $\frac{\pi^k \alpha}{mq^k}$ entspricht, falls $\frac{\pi^k \alpha}{mq^k} \in \mathrm{End}_K(J_{X_2})$ ist, anderenfalls **false**

1.) (Initialisierung) Setze $l := g - 1, i := 0, j := 1, k := 0$ und ϕ sei der durch $\Gamma := \sum_{i=1}^{n} \lambda_i B_i$ induzierte Endomorphismus auf J_{X_2}. Setze $K^{(0)} := K$, $S := \emptyset$ und $T := \emptyset$. Setze

$$f := N_{L/F_2}(C(A)_0) = x_1^{g-l} + \sum_{i=0}^{g-l-1} x_1^i \frac{f_i}{g_i} \quad (f_i \in K[x_2, y_2], g_i \in K[x_2]),$$

berechne $r \in \mathbb{Z}^{\geq 0}$ mit $g = q^r t$ und $p \nmid t$ und $d(mq^s) := \prod d(p_i)$ mit $mq^s = \prod p_i^{e_i}$ und $d(p_i)$ wie in Definition 4.10. Berechne $z \in \mathbb{Z}^{\geq 2}$ minimal mit $\mathrm{ggT}(z, d(mq^s)) = 1 = \mathrm{ggT}(z, mq^s)$.

2.) (Schleife über k) Setze $m' := mq^k$, $\Gamma' := F^k \Gamma$ und $\phi' = \pi^k \phi \in \mathrm{End}_K(J_{X_2})$ bezeichne den durch Γ' induzierten Endomorphismus.

3.) (Schleife über l) Berechne

$$s := n^2 \frac{\mathrm{Tr}_{E_K/\mathbb{Q}}(\phi' + l) \circ (\phi' + l)^\star}{2m'^2}$$

und $\mathcal{S}$ wie in (4.12)

4.) Bezeichne $\mathcal{Z}$ Menge aller unterschiedlicen Möglichkeiten der Zerlegungen von $C(A)$ in Primdivisoren, wobei hier $\deg C(A) = g - l$ ist.

5.) (Schleife über $\delta \in \mathcal{Z}$)

6.) (Schleife über j) Für $p_j \in \mathbb{P}^1_{K^{(i)}}$ berechne $o_j := \mathrm{ord}(\Phi^{(i)}(p_j))$ und teste p_j auf folgende Eigenschaft:

(i) Prüfe, ob $\mathrm{ggT}(o_j, m') = 1$ ist. Wenn ja, berechne $\phi(\Phi^{(i)}(p_j)) = a_j - rp_\infty + (f)$ mit $1 \leq r \leq g$ und $a_j \in \mathcal{D}_{F_2/K^{(i)}}$ effektiv vom Grad r,

(ii) berechne $t_j \in \mathbb{N}$ mit $t_j \cdot n \equiv 1 \mod o_j$ sowie $t_j(a_j - rp_\infty) = b_j - (g-l)p_\infty + (f)$ und teste dann, ob die Zerlgegung von b_j in Primdivisoren der Zerlegung δ entspricht und ob $p_\infty \notin \mathrm{supp}(b_j)$ gilt. Überprüfe, ob $\langle p_j, b_j \rangle \notin S$ und $\deg b_j = g - l$ gilt.

War der Test erfolgreich, so setze $S \longleftarrow S \cup \{\langle p_j, b_j \rangle\}$. Ist $|S| = \mathcal{S}$, so gehe zu 8.). Ist $j < |\mathbb{P}^1_{K^{(i)}}|$, so setze $j \longleftarrow j + 1$ und gehe zu 6.).

7.) Ist $\deg b_j > g - l$, so gehe zu 14.). Entspricht Zerlegung von Primdivisoren von b_j nicht der Zerlegung δ, so gehe zu 12.). Anderenfalls setze $i \longleftarrow i + 1$ und berechne $K^{(i)}/K^{(i-1)}$ mit $[K^{(i)} : K^{(i-1)}] = z$. Bette Divisoren von S in $K^{(i)}$ ein und gehe zu 6.).

8.) (Ende Schleife über j)

9.) Sei $S = \{\langle p_j, b_j \rangle \mid j \in \{1, ..., |S|\}\}$. Berechne für alle $j \in \{1, ..., |S|\}$ dann

$$N_{F_2/K}(b_{j_0}) = x_2^{g-l} + \sum_{i=0}^{g-l-1} c_{ij} x_2^i \in K[x_2]$$

und $\alpha_j := \pi_{p_j}(x_2)$ und $\beta_j := \pi_{p_j}(y_2)$. Setze

$$T := \{\langle \langle c_{g-1-l,i}, ..., c_{0i} \rangle, \langle \alpha_i, \beta_i \rangle \rangle \mid i = 1, ..., |S|\}.$$

10.) Berechne für jedes $j \in \{0, ..., g-l-1\}$ Matrix M_j wie in (4.13) mit Hilfe von T und jeweils eine nicht-triviale Lösung $w_j \in K^{\mathcal{S}}$ von $M_j v_j = 0$, wobei v_j wie in (4.14) ist. Berechne für w_j jeweils f_j und g_j. Ist $g_j \neq 0$, so gehe zu 11.). Anderenfalls gehe zu 14.)

11.) Setze $f := x_1^{g-l} + \sum_{j=0}^{g-l-1} f_j/g_j$. Ist $f\mathcal{O}_{L/F_2}$ Hauptideal, so gehe zu 9.). Anderenfalls berechne $f\mathcal{O}_{L/F_2} = \prod_{i=1}^n P_{i,0}^{e_i}$ mit $P_i \in \mathbb{P}_{L/F_2}$. Berechne mit Hilfe der Korrespondenzpaarung und Basiselementen $\{\beta_1, ..., \beta_{d^2 l}\}$ Elemente $\alpha_i \in \mathrm{End}_K(J_{X_2})$, die jeweils den Korrespondenzen P_i entsprechen. Entspricht $\frac{\pi^k \alpha}{m'}$ der Korrespondenz $B_0 := \prod_{i=1}^n P_{i,0}^{e_i'}$ mit $e_i' \in \mathbb{Z}^{\geq 0}$ geeignet und $e_i \geq e_i' > 0$, so gib $\langle B, \frac{\pi^k \alpha}{m'} \rangle$ zurück und terminiere.

12.) Ist $\mathcal{Z} \neq \emptyset$, so setze $\mathcal{Z} \leftarrow \mathcal{Z} \backslash \delta$ und $\delta \in \mathcal{Z}$ beliebig und gehe zu 5.).

13.) (Ende Schleife über δ)

14.) Ist $l \geq 0$, so setze $l \longleftarrow l - 1$ und gehe zu 3.).

15.) (Ende Schleife über l)

16.) Ist $k < r$ so, $k \longleftarrow k + 1$ und gehe zu 1.)

17.) Gib **false** zurück und terminiere.

Bemerkung 4.12. *Es hat sich in der Praxis gezeigt, dass bei Geschlecht $g \leq 4$ die $C(A)(p)$ fast immer von der Gestalt $C(A)(p) = \sum_i q_i$ mit paarweise verschiedenen Primdivisoren q_i sind. Dies bedeutet, dass in der Zerlegung $C(A) = \sum_{i=1}^{n} e_i P_i$ die Primdivisoren P_i alle nur einfach vorkommen, d.h. also es gilt $e_i = 1$. Meistens waren die Divisoren $C(A)$ sogar Primkorrespondenzen. Das Auffinden geeigneter Stellen vom Grad eins hat sich in der Praxis als unproblematisch erwiesen, wenn die Klassenzahl teilerfremd zu m' war. Allerdings war es oft unmöglich, die Hochhebung der Norm zu brechnen. Der Algorithmus zur Berechnung der Hochhebung hat nicht terminiert, wenn die in der Norm auftretenden Grade der Polynome in x_2 oder der Körpergrad $[F_2 : K(x_2)]$ zu groß wurden.*

4.6 Berechnung von Orthogonalen Korrespondenzen

Für die Jacobische J_{X_2} betrachten wir eine isogene Zerlegung in paarweise nicht-isogene und einfache abelsche Varietäten A_i über K mit

$$J_{X_2} \sim_K \prod_{i=1}^{t} A_i^{r_i} \quad (r_i \geq 1),$$

woraus dann, wie wir bereits wissen, die Isomorphie

$$\mathrm{End}_K^0(J_{X_2}) \cong \prod_{i=1}^{t} \mathrm{End}_K^0(A_i^{r_i})$$

folgt (s. (1.15) und (1.16)). Da wir nun die Korrespondenzen aus $\mathcal{D}_{L/F_2}$ als K-Endomorphismen von $\mathcal{C}^0_{F_2\overline{K}/\overline{K}}$ auffassen, schreiben wir für Korrespondenzklasse $[D]_C$ einfach nur D mit $D \in \mathcal{D}_{L/F_2}$. Die Matrixalgebren $M_{r_i}(\mathrm{End}_K^0(A_i))$ sind jeweils einfach, da die Algebren $\mathrm{End}_K^0(A_i)$ Schiefkörper sind (s. [Pie82, Section 1.4, Lemma, p. 9]).

Nach [Zar05, Remark 1.4, p. 192] können wir in $\mathrm{End}_K^0(J_{X_2})$ eine orthogonale idempotente Zerlegung der Eins bestimmen, d.h. es gibt Elemente $D_i \in \mathrm{End}_K^0(J_{X_2})$, so dass $D = \sum_{i=1}^{t} D_i$ mit $D_i^2 = 1$ und $D_i D_j = \delta_{ij}$ gilt, wobei mit δ_{ij} das Kroneckersymbol gemeint ist. Mit $F_i \in \mathrm{End}_K^0(A_i^{r_i})$ bezeichnen wir dann das Element $D_i F \in \mathrm{End}_K^0(A_i^{r_i})$. Damit ordnen wir jeder abelschen Varietät $A_i^{r_i}$ ein Endomorphismenpaar (D_i, F_i) aus $\mathrm{End}_K^0(A_i^{r_i})$ zu.

Im Allgemeinen entsprechen die Elemente D_i und F_i keinen Korrespondenzen, jedoch ist leicht zu sehen, dass es jeweils ein $n_i \in \mathbb{N}$ geeignet gibt, so dass $n_i D_i$ und $n_i F_i$ sogar Endomorphismen sind und somit durch Korrespondenzen dargestellt werden können. Allerdings können wir dann nicht den vollen Endomorphismenring von $\mathrm{End}_K(J_{X_2})$ berechnen, sondern diesen nur von $R := \mathrm{End}_J(J_{X_2}) \otimes \mathbb{Z}[1/\prod n_i]$. Die Berechnung von R erfolgt dann durch die einzelnen Berechnungen der Endomorphismenringe $\mathrm{End}_K(A_i^{r_i}) \otimes \mathbb{Z}[1/n_i]$ mit dem jeweiligen Frobeniusendomorphismus $n_i F_i$ und Einselement $n_i D_i$.

Algorithmus 6: Orthogonale Korrespondenzen

Input: 1.) Das charakteristische Polynom $f = \prod_{i=1}^{r} g_i^{e_i} \in \mathbb{Z}[t]$ des Frobeniusendomorphismus
2.) Die Frobeniuskorrespondenz F

Output: Ein Tupel $(D_1, , ..., D_r)$ von orthogonalen Korrespondenzen

1.) (Initialisierung): Setze $i := 1$

2.) (Schleife über i) Berechne mittels chinesischen Restsatzes Elemente $d_i \in \mathbb{Q}[t]$ mit $d_i \equiv 0 \mod g_j^{e_j}$ für $j \neq i$ und $d_i \equiv 1 \mod g_j^{e_j}$ für $j = i$ und $j = 1, ..., r$.

3.) Berechne $n_i \in \mathbb{Z}$, so dass $n_i d_i$ in $\mathbb{Z}[t]$ normiert ist

4.) Berechne $(n_i d_i)(F) =: n_i D_i$ mit Hilfe von Algorithmus 1

5.) (Ende Schleife über i)

6.) Gib $(n_i D_1, ..., n_r D_r)$ zurück und terminiere.

4.7 Die Berechnung des kommutativen Teils eines Endomorphismenringes

Im Folgendem wollen wir den Endomorphismenring $\mathrm{End}_K^0(J_{X_2})$ der elementaren Jacobischen $J_{X_2} \sim_K A^r$ berechnen, wobei A eine einfache abelsche Varietät über K ist ($r \geq 0$). Um $\mathrm{End}_K(A^r)$ zu berechnen, bestimmen wir zuerst das Zentrum der $\mathbb{Q}$-Algebra $E_{_K} = \mathrm{End}_K^0(A^r)$, d.h. also $Z(E_{_K}) = \mathbb{Q}[\pi_{_K}]$, wenn $\pi_{_K}$ den Frobenius von A^r bezeichnet. Ist $f_{\pi_{_K}} = g_{\pi_{_K}}^{rm}$, so gilt $F := Z(E_{_K}) = \mathbb{Q}(\pi_{_K})$, wobei $g_{\pi_{_K}}$ das Minimalpolynom von $\pi_{_K}$ ist.

Für eine abelsche Varietät A^r mit zugehöriger Endomorphismenalgebra $E_{_K} = \mathrm{End}_K^0(A^r)$ gehen wir nun in zwei Schritten vor, um $\mathrm{End}_K(A^r)$ zu berechnen: Zuerst müssen wir eine Ordnung $\mathcal{O}$ in der Maximalordnung $\mathcal{O}_F$ so berechnen, dass $\mathrm{End}_K(A^r) \cap F = \mathcal{O}$ gilt und $\mathcal{O}$ maximal mit dieser Eigenschaft ist. Aus [Deu35, Satz 7, S. 71], folgt nämlich, dass $\mathcal{O}_F$ und damit auch $\mathcal{O}$ in jeder Maximalordnung von $E_{_K}$ enthalten ist.

Wir wollen nun zuerst den Algorithmus zu Berechnung von $\mathcal{O}$ formulieren. Dazu fassen wir die für uns wichtigsten Gegebenheiten und Definitionen zusammen, wobei $\pi := \pi_{_K}$ sein soll:

(1) Vorgegeben ist ein Zahlkörper $F = \mathbb{Q}(\pi)$ vom Grad $[F : \mathbb{Q}] = l$, die Gleichungsordnung $\mathbb{Z}[\pi] \subseteq \mathcal{O}$ und die Maximalordung $\mathcal{O}_F$ von F. Es gilt also $\mathbb{Z}[\pi] \subseteq \mathcal{O} \subseteq \mathcal{O}_F$.

(2) Sei $\mathcal{O}^{(i)} \subseteq \mathcal{O}_F$ ($i \geq 0$) eine Teilordnung von $\mathcal{O}_F$ mit $\mathcal{O}^{(i)} \subseteq \mathcal{O}$. Dann gibt es Basen $\Delta^{(i)} := \{\delta_1^{(i)}, ..., \delta_n^{(i)}\}$ von $\mathcal{O}^{(i)}$ und Basen $\Omega^{(i)} := \{\omega_1^{(i)}, ..., \omega_n^{(i)}\}$ von $\mathcal{O}_F$, so dass $\delta_j^{(i)} = m_{jj}^{(i)}\omega_j^{(i)}$ mit $m_{jj}^{(i)} \in \mathbb{Z}^{>0}$ und

$$m_{11}^{(i)} | m_{22}^{(i)} | ... | m_{nn}^{(i)}$$

gilt ($j = 1, ..., n$). Die Existenz einer solchen Basis folgt aus Lemma 1.6, [Poh93, Lemma 1.1, p 34].

(3) Sei $\Lambda^{(i)} := \prod_{j=1}^{n}[-(m_{jj}^{(i)} - 1)...(m_{jj}^{(i)} - 1)]$. Ein Element von $\Lambda^{(i)}$ bezeichnen wir mit $\underline{\lambda}^{(i)}$, und mit $\underline{0}$ bezeichnen wir das Element $(0, ..., 0) \in \Lambda^{(i)}$.

Wir gehen nun folgendermaßen vor, um den vollen Endomorphismenring zu berechnen: Wir gehen davon aus, dass wir einen Algorithmus A haben, welcher bei Eingabe eines Elementes $h(\pi)$ mit $h \in \mathbb{Z}[t]$ vom Grad $\leq l$ und $m \in \mathbb{Z}^{\geq 2}$ bestimmen kann, ob $h(\pi)/m$ ein Endomorphismus ist und gegebenenfalls die zugehörige Korrespondenz berechnet. Ist $\alpha \in \mathcal{O}$, so besitzt α eine Darstellung

$$\alpha = \sum_{j=1}^{l} \lambda_j \omega_j^{(i)} = \sum_{j=1}^{n} \frac{\lambda_j}{m_{jj}^{(i)}} \delta_j^{(i)} = \frac{\sum_{j=1}^{n} \lambda_j' \delta_j^{(i)}}{m_{nn}^{(i)}}$$

mit $\lambda_j, \lambda'_j \in \mathbb{Z}$. Aus $\delta_j^{(i)} \in \mathcal{O}^{(i)}$ folgt, dass $\mathrm{ord}([\alpha])|m_{nn}^{(i)}$ in $\mathcal{O}/\mathcal{O}^{(i)}$ gilt, wenn $[\alpha]$ die Nebenklasse von α in $\mathcal{O}/\mathcal{O}^{(i)}$ bezeichnet. Nun durchläuft $\underline{\lambda}^{(i)}$ nacheinander alle Elemente aus $\Lambda^{(i)}\backslash\{\underline{0}\}$ und für jedes solche $\underline{\lambda}^{(i)} = (\lambda_1^{(i)}, ..., \lambda_n^{(i)})$ bilden wir das Element $\alpha := \sum \lambda_j^{(i)} \omega_j^{(i)} \in \mathcal{O}_F$ und testen mit dem gegebenen Algorithmus A, ob $\alpha \in \mathcal{O}$ gilt. Ist dies der Fall, so gibt der Algorithmus A eine Korrespondenz $B \in \mathcal{D}_{L/F_2}$ zurück, für welche $[B]_C$ dem Element α entspricht. Dann berechnen wir $\mathcal{O}^{(i+1)} := \mathcal{O}^{(i)}[\alpha]$, Basen $\Omega^{(i)}$ und $\Delta^{(i)}$ wie in (2) und $\Lambda^{(i+1)}$. Schließlich speichern wir das Tupel $\langle \alpha, B \rangle$ in einer Liste L und verfahren dann weiter wie oben. Am Ende gibt der Algorithmus die Liste L aus, welche zusammen mit der Menge $\{D, F, ..., F^{n-1}\}$ ein Erzeugendensystem von $\mathcal{O}$ ist. Nun können wir unseren Algorithmus formulieren:

Algorithmus 7: Kommutativer Endomorphismenring

Input: 1.) Einen Zahlkörper $F : \mathbb{Q}$ mit $[F : \mathbb{Q}] = l$ und $F = \mathbb{Q}(\pi)$, die Maximalordnung $\mathcal{O}_F$
2.) $\mathcal{O}_{L/F_2}$ und das Geschlecht g von L/F_2
3.) Die Frobeniuskorrespondenz F und Einheitskorrespondenz D von L/F_2

Output: Den vollen Endomorphismenring $\mathrm{End}_K(J_{X_2}) = \mathcal{O} \subseteq \mathcal{O}_F$ und die Liste L

1.) (Initialisierung): Setze $\mathcal{O}^{(0)} := \mathbb{Z}[\pi]$, berechne Basen $\Omega^{(0)}$ und $\Delta^{(0)}$ sowie $m_{jj}^{(0)}$ wie in (2). Setze $i := 0$ und $L := \emptyset$.

2.) Berechne $\Lambda^{(i)}$ wie in (3)

3.) (Schleife über $\Lambda^{(i)}$) Für $\underline{0} \neq \underline{\lambda}^{(i)} \in \Lambda^{(i)}$ berechne

$$\alpha = \sum_{j=1}^{l} \lambda_j^{(i)} \omega_j^{(i)} = \sum_{j=1}^{l} \frac{\lambda_j^{(i)}}{m_{jj}^{(i)}} \delta_j^{(i)} = \frac{\sum_{j=0}^{l-1} \mu_j^{(i)} \pi^j}{m} \quad (\mu_j^{(i)} \in \mathbb{Z})$$

4.) Rufe Algorithmus **Approximation** mit Parametern

(i) $\mathcal{O}_{L/F_2}$ und g,

(ii) $d = 1$ und l,

(iii) $\{1, \pi, ..., \pi^{l-1}\}$,

(iv) $\sum_{j=0}^{l-1} \mu_j^{(i)} \pi^j$,

(v) $\{D, F, ..., F^{l-1}\}$,

(vi) m

auf. Gibt der Algorithmus ein Tupel $\langle B, \alpha \rangle$ mit $B \in \mathcal{D}_{L/F_2}$ zurück, so setze $L \longleftarrow L \cup \{\langle B, \alpha \rangle\}$, $\mathcal{O}^{(i+1)} := \mathcal{O}^{(i)}[\alpha]$ und $i \longleftarrow i+1$.

5.) Teste dann, ob $[\mathcal{O}_F : \mathcal{O}^{(i)}] = 1$ ist. Wenn ja, gib L und $\mathcal{O}_F$ zurück und terminiere. Andernfalls berechne $\Omega^{(i)}, \Delta^{(i)}$ und $m_{jj}^{(i)}$ wie in (2), $\Lambda^{(i)}$ wie in (3) und gehe zu 3.)

6.) (Ende Schleife über $\Lambda^{(i)}$)

7.) Gib L und $\mathcal{O}^{(i)}$ zurück und terminiere.

4.8 Berechnung eines nicht-kommutativen Endomorphismenringes

Sei nun $\mathrm{End}_K^0(J_{X_2}) \cong \mathrm{End}_K^0(A^r) = E_{\mathfrak{K}}$. Da das charakteristische Polynom von $f_{\pi_{\mathfrak{K}}}$ von der Form $f_{\pi_{\mathfrak{K}}} = g_{\pi_{\mathfrak{K}}}^{rm}$ ist, wissen wir nach [Tat66, Theorem 2, p. 140], dass $E_{\mathfrak{K}} \cong M_r(D)$ eine zentral einfache $F = \mathbb{Q}(\pi_{\mathfrak{K}})$-Algebra ist mit $n = \mathrm{Deg}(E_{\mathfrak{K}}) = rm$, wobei $D = \mathrm{End}_K(A)$ ein Schiefkörper und $m = \mathrm{Deg}(D) = \mathrm{Ind}(E_{\mathfrak{K}})$ ist. Da D ebenfalls in $\mathfrak{S}(F)$ liegt, erhalten wir das Zentrum von $M_r(D)$, in dem wir $F = Z(D)$ mittels Diagonalmatrizen isomorph in $\mathrm{End}_K^0(A^r)$ einbetten. Mit Satz 1.25 und Lemma 1.26 folgt nun, dass $E_{\mathfrak{K}}$ einen strikt maximalen und zyklischen Teilkörper E/F vom Grad $n = [E : F] = \mathrm{Deg}(E_{\mathfrak{K}})$ enthält. Damit bekommen wir eine Darstellung von $E_{\mathfrak{K}}$ in der Form

(i) $E_{\mathfrak{K}} = \bigoplus_{0 \le j < n} u^j E$,

(ii) $u^{-1} d u = \sigma(d)$ für alle $d \in E$ und

(iii) $u^n = a \in F^\times$,

wobei $G(E/F) = \langle \sigma \rangle$ und $a \in F^\times / N_{E/F}(E^\times)$ mit $\mathrm{ord}(a) = m$ ist (s. Lemma 1.27). Wir müssen also sowohl E als auch a finden, um eine Darstellung von $E_{\mathfrak{K}}$ zu bekommen. Den Index $m = \mathrm{kgV}(m_{v_j}) = \mathrm{Ind}(E_{\mathfrak{K}})$ bestimmen wir mit Hilfe von Satz 1.30. Schließlich berechnen wir mit Hilfe eines geeigneten Strahlklassenkörpers ein Körpererweiterung E/F, so dass E/F galoissch und zyklisch ist und zuletzt ein Element $a \in F^\times$ mit $\mathrm{ord}(aF^\times / N_{E/F}(E^\times)) = m$.

Sei $E = F(\beta)$ mit $E = \sum_{i=0}^{n-1} F\beta^i$. Wir können o.B.d.A. voraussetzen, dass β und a ganz über $\mathbb{Z}$ sind mit $\sigma(\beta) \in \mathcal{O}_F[\beta]$. Somit erhalten wir einen $\mathcal{O}_F$-Modul $\mathfrak{O}$ vom Rang m^2, erzeugt durch die Elemente

$$B := \{u^j\beta^i \mid i, j = 0, ..., m-1\}. \tag{4.16}$$

Mittels Induktion erhalten wir $u^i\beta u^j = u^{i+j}\sigma^j(\beta)$ für $i, j \in \{0, ..., m-1\}$. Daraus und aus $\sigma(\beta) \in \mathcal{O}_F[\beta]$ folgt dann für zwei Elemente $\beta, \alpha \in \mathfrak{O}$ mit $\beta = \sum_i u^i\lambda_i$ und $\alpha = \sum_j u^j\mu_j$ $(\lambda_i, \mu_j \in \mathcal{O}_F[\beta])$ dann $\beta\cdot\alpha, \alpha\cdot\beta \in \mathfrak{O}$. Somit ist $\mathfrak{O}$ eine $\mathcal{O}_F$-Ordnung von E_K. Insbesondere können wir aber auch $\mathfrak{O}$ als eine Ordnung vom vollen Rang $[F : \mathbb{Q}]m^2$ über $\mathbb{Z}$ auffassen. Damit ist die $\mathbb{Z}$-Basis von $\mathfrak{O}$ auch eine $\mathbb{Q}$-Basis von $\mathrm{End}_K^0(A^r)$. Dies bedeutet insbesondere, dass für jedes $\alpha \in \mathrm{End}_K^0(A^r)$ ein minimales $n \in \mathbb{N}$ existiert, so dass $n\alpha \in \mathrm{End}_K(A^r)$ gilt, denn $\mathrm{End}_K(A^r)$ ist ebenfalls eine Ordnung in $\mathrm{End}_K^0(A^r)$.

Als Erstes berechnen wir mit Algorithmus 7 den kommutativen Teil $\mathcal{O} = \mathrm{End}_K(A^r) \cap F$ des Endomorphismenrings. Gegebenenfalls ändern wir a mit einem geeigneten Element n aus $\mathbb{Z} \cap N_{E/F}(E^\times)$ so ab, dass $na \in \mathcal{O}$ liegt, bezeichnen aber na wieder mit a. Sei nun $f_\beta = \sum_i b_i t^i \in \mathbb{Z}[t]$ irreduzibel mit $f_\beta(\beta) = 0$. Ziel ist es, Korrespondenzen $B, U \in \mathcal{D}_{L/F_2}$ so zu bestimmen, dass $[f_\beta(B)]_C = [0]_C$ und $[U^n - A]_C = [0]_C$ gilt, wobei A eine Korrespondenz ist, die dem Element a entspricht. Dazu berechnen wir zuerst die Klassengruppe $G := \mathcal{C}^0_{F_2/K}$ vom Grad Null. Ist etwa

$$G_{_K} \cong \prod_{i=1}^{t} \mathbb{Z}/p_i^{e_i}\mathbb{Z}$$

und $B \in \mathcal{D}_{F_2/K}$, so induziert B einen Endomorphismus $B : G_{_K} \longrightarrow G_{_K}$, da per Definition $B(G_{_K}) \subseteq G_{_K}$ gilt. Wir können nun B auf $G_{_K}$ durch eine geeignete Matrix $M \in \mathbb{Z}^{t\times t}$ darstellen, wobei die Einträge der Spalten zwischen 0 und $p_i^{e_i}$ sind und $f_\beta(M) = 0$ ist. Von solchen Matrizen, die wir als Endomorphismen von $G_{_K}$ auffassen, gibt es nur endlich viele und diese wollen wir mit

$$\mathcal{M}(B) := \{M = (m_{ij}) \in \mathbb{Z}^{t\times t},\ M \neq 0 \mid 0 \leq m_{ij} < p_i^{e_j} \text{ und } f_\beta(M) = 0\}, \tag{4.17}$$

bezeichnen. Nun berechnen wir für β den Wert

$$s = n^2\mathrm{Tr}_{E_{_K}/\mathbb{Q}}(\beta\beta^\star)$$

wie in (4.8) und $\mathcal{S}$ wie in (4.12). Bezeichnet $\Phi : \mathbb{P}^1_K \longrightarrow G_{_K}$ wieder die Einbettung der Stellen vom Grad eins von F_2/K in $G_{_K}$, so bestimmen wir den Wert

$$T_{_K} := \min_i \left\{\ |\{\Phi(\mathbb{P}^1_K)\} \setminus \ker M_i\}|\ \right\}. \tag{4.18}$$

Ist $T_{K} < \mathcal{S}$, so nehmen wir eine endliche geeignete Erweiterung K'/K so vor, dass dann $\mathcal{S} \leq T_{K'}$ ist, bezeichnen diese aber wieder mit K. Insbesondere müssen wir eventuell noch durch geeignete Erweiterungen K'/K sicherstellen, dass die Multiplikation mit b_0, wobei $b_0 \in \mathbb{Z}$ der konstante Koeffizient von f_β ist, und A nicht auf $G_{K'}$ verschwinden. Wir setzen also voraus, dass wir genügend Stellen vom Grad eins in $\mathbb{P}^1_K$ haben um die Norm der den Matrizen eventuell entsprechenden Korrespondenzen zu interpolieren. Mit Hilfe der Matrizen $M_i \in \mathcal{M}(B)$ können wir nun alle in Frage kommenden Endomorphismen $\phi \in \mathrm{End}_K(A^r)$, d.h. diejenigen mit $f_\beta(\phi) = 0$, eindeutig beschreiben. Denn wir wissen, dass ϕ eine Korrespondenz in $\mathcal{D}_{F_2/K}$ ist und somit einem Ideal A_0 in $\mathcal{O}_{L/F_2}$ entspricht, welches als Korrespondenz aufgefasst ϕ induziert. Auf Grund unserer Voraussetzungen haben wir aber genügend Stellen in $\mathbb{P}^1_K$, so dass die Norm $N_{L/F_2}(C(A)_0)$ dann eindeutig bestimmt ist. Gibt es also einen solchen nicht-trivialen Endomorphismus ϕ in $\mathrm{End}_K(A^r)$, so muss er sich eingeschränkt auf G_K durch eine der Matrizen $M_i \in \mathcal{B}(M)$ beschreiben lassen. Gibt es keinen, so wissen wir, dass ein $m \in \mathbb{N}$ mit $m\phi \in \mathrm{End}_K(A^r)$ existieren muss, d.h. also, dass wir im erfolglosen Fall ein minimales $m \in \mathbb{N}$ so bestimmen müssen, das $m\phi$ ein Endomorphismus ist. Analog gehen wir vor, um ein U mit $U^n = A \in \mathcal{O}$ zu bestimmen.

Die zu den so berechneten Korrespondenzen B und U dazugehörigen Elemente von E_K bezeichnen wir mit β bzw. mit u. Wir erhalten somit eine Ordnung

$$\mathfrak{D} := \bigoplus_{i=1}^{n-1} \mathcal{O}[\beta]u^i = \langle b_1, ..., b_n \rangle ,$$

wobei $b_1, ..., b_n \subseteq \mathrm{End}_K(A^r)$ eine $\mathbb{Z}$-Basis von $\mathfrak{D}$, aufgefasst als $\mathbb{Z}$-Ordnung, ist. Nun berechnen wir die Diskriminante $d := \mathrm{disc}(\mathfrak{D}) = \prod_i p_i^{e_i} \in \mathbb{Z}$. Aus [Mum70, Corollary 1, p. 178] wissen wir, dass $\mathrm{End}_K(A^r)$ eine endlich erzeugte $\mathbb{Z}$-Ordnung ist. Deshalb kommen für einen eventuellen Aufstieg nur die quadratischen Diskriminantenteiler von $\mathrm{disc}(\mathfrak{D})$ in Frage. Wir berechnen zuerst die endlich vielen Konjugationsklassen von Maximalordnungen und dann die Diskriminante $\tilde{d} := \mathrm{disc}\,\mathcal{O}_1$. Dabei merken wir an, dass sämtliche Maximalordnungen von E_K die selbe Diskriminante besitzen. Ist dann $\mathfrak{D}$ eine Maximalordnung, so muss $d = \tilde{d}$ gelten. Nun gilt mit [Deu35, Satz 6, S.70], dass $\mathfrak{D} \subseteq \gamma\mathcal{O}_i\gamma^{-1}$ mit $\gamma \in E_K^\times$ und $i \in \{1, ..., t\}$ geeignet ist. Daraus folgt, dass $\mathfrak{D}$ genau dann maximal ist, wenn $d = \tilde{d}$ gilt. In diesem Fall haben wir bereits den vollen Endomorphismenring berechnet. Um zu testen, ob $d = \tilde{d}$ ist, benötigen wir außerdem nur eine Maximalordnung. Nun müssen wir alle Möglichkeiten eines eventuellen Aufstiegs, ähnlich wie im kommutativen Fall, durchprobieren.

Algorithmus 8: Nicht-kommutativer Endomorphismenring

Input: 1.) Das Zentrum $F = \mathbb{Q}(\pi_K) = Z(\mathrm{End}_K^0(A^r))$ mit $[F : \mathbb{Q}] = l$, $\mathcal{O}_F$ und f_{π_K}
2.) $\mathcal{O}_{L/F_2}$ und das Geschlecht g von L/F_2
3.) Die Frobeniuskorrespondenz F und Einheitskorrespondenz D von L/F_2

Output: Der Endomorphismenring $\mathrm{End}_K(A^r)$

1.) Bestimme mittels Algorithmus 7 den kommutativen Teilring $\mathcal{O} := F \cap \mathrm{End}_K(A_K^r)$, d.h. Liste $L = \{\langle A_i, \alpha_i\rangle \mid i = 1, ..., l\}$ mit $A_i \in \mathcal{D}_{L/F_2}$ und $\alpha_i \in F$.

2.) Berechne $f_{\pi_K} = g_{\pi_K}^s$ mit $2g = rm \deg g_{\pi_K}$, $s = rm$ und g_{π_K} irreduzibel.

3.) Bestimme die endlich vielen Invarianten

$$\mathrm{inv}_{v_j}(F_{v_j} \otimes D) = \frac{a_{v_j}}{m_{v_j}} \quad \big(\mathrm{ggT}(a_{v_j}, m_{v_j}) = 1\big)$$

von $\mathrm{End}_K(A^r) \cong M_r(D)$ wie in Satz 1.30 und setze $m := \mathrm{kgV}(m_{v_j})$ sowie $r := s/m$.

4.) Berechne zyklische Galoiserweiterung E/F mit $[E : F] = m$, $E = F(\beta)$ und β ganz, so dass $e(\mathfrak{p}_j)f(\mathfrak{p}_j) = m_{v_j}$ ist, wenn $\mathfrak{p}_j \subseteq \mathcal{O}_E$ Primideal zu v_j ist mit $\mathfrak{p}_j | p$ und $[E_{v_j} : F_{v_j}] = 2$, wenn v_j eine reelle Stelle von F ist. (s. dazu Abschnitt 1.5)

5.) Berechne $a \in \mathcal{O}^\times$ mit $\mathrm{ord}(aN_{E/F}(E^\times)) = m$ in $F^\times/N_{E/F}(E^\times)$ so, dass u mit $u^n = a$ die Bedingungen in Lemma 1.26 erfüllt. Bezeichne mit $A \in \mathcal{D}_{L/F_2}$ eine a entsprechende Korrespondenz.

6.) Bezeichne $f_\beta = \sum_i b_i t^i \in \mathbb{Z}[t]$ das Minimalpolynom von β in E. Berechne K'/K und $G := \mathcal{C}^0_{F_2/K'}$, so dass die Multiplikation mit b_0 und A auf G nicht verschwinden. Berechne dann $\mathcal{M}(B)$ wie in (4.17) und T_K wie in (4.18) und mache eventuell wieder eine geeignete Erweiterung K'' von K' und setze $K := K''$.

7.) Berechne B und U durch jeweils Interpolation der Norm und Hochhebung, und seien β bzw. u die B und U in E_K entsprechenden Elemente. Definiere

$$\mathfrak{D} := \bigoplus_{i=1}^{s^2 l} \mathcal{O}[\beta]u^i$$

mit $\mathbb{Z}$-Basis $\langle b_1, ..., b_{s^2 l}\rangle$ und berechne $d := \mathrm{disc}\,\mathfrak{D}$.

8.) Berechne eine Maximalordnung $\mathcal{O}_1$ von E_K, $\tilde{d} := \operatorname{disc} \mathcal{O}_1$ und $m := d/\tilde{d} = a^2 b$ mit $a, b \in \mathbb{Z}$ und b quadratfrei.

9.) Ist $m = 1$, so gib $\{\langle B_i, b_i \rangle \mid i = 1, ..., s^2 l\}$ zurück, wobei $B_i \in \mathcal{D}_{L/F_2}$ die dem Element $b_i \in \mathrm{End}_K(A^r)$ entsprechende Korrespondenz ist.

10.) Anderenfalls berechne mit Algorithmus 5 den maximalen Aufstieg $R \subseteq \mathrm{End}_K(A^r)$ von $\mathfrak{D}$ in $\mathrm{End}_K(A^r)$ für alle Teiler von a, d.h. also eine Ordnung $R := \langle c_1, ..., c_{s^2 l} \rangle$, und gib $\{\langle C_i, c_i \rangle \mid i = 1, ..., s^2 l\}$ zurück, wobei $C_i \in \mathcal{D}_{L/F_2}$ die dem Element $c_i \in \mathrm{End}_K(A^r)$ entsprechende Korrespondenz ist.

4.9 Bemerkungen zu den Laufzeiten

Wir wollen in diesem Abschnitt noch einige Bemerkungen zu den Laufzeiten der in diesem Kapitel vorgestellten Algorithmen machen. Dazu zählen wir zunächst die wichtigsten Berechnungen auf.

(i) Die Berechnung der Klassengruppe vom Grad null von F_2/K,

(ii) die Reduktion von Divisoren entlang eines Divisors vom Grad eins,

(iii) die Berechnung des L-Polynoms von F_2/K,

(iv) die Bestimmung der Ordnung eines Elements aus $\mathcal{C}^0_{F_2}$,

(v) die Berechnung der Stellen vom Grad eins von F_2/K,

(vi) die Berechnung des Kerns von Matrizen mit Einträgen aus $\mathbb{F}_q$,

(vii) die Berechnung der Operation der Korrespondenzen auf $\mathcal{C}^0_{F_2}$ mittels Algorithmus 3,

(viii) die Berechnung einer Maximalordnung eines Zahlkörpers oder einer Algebra

(ix) die Berechnung der Endomorphismenalgebra im nicht-kommutativen Fall und

(x) die Berechnung einer $\mathbb{Q}$-Basis der Endomorphismenalgebra im nicht-kommutativen Fall.

Sei $L_n[u,v] = \exp(v(\log n)^u(\log\log n)^{1-u})$ und $g = g_{F_2/K}$ mit $K = \mathbb{F}_q$ mit $q = p^n$. Der Aufwand für die Arithmetik in der Klassengruppe vom Grad null eines Funktionenkörpers F_2/K ist bei geeigneter Darstellung von F_2/K polynomiell in $g \log q$. Die Laufzeit zur Berechnung der Klassengruppe $\mathcal{C}_{F_2}$ sowie zur Reduktion verhält sich für festes q und $g \to \infty$ nach [Hes99] unter bestimmten Annahmen wie $L_{q^g}\left(\frac{1}{2}, c\right)$ mit einer Konstanten $c \in \mathbb{R}^{\geq 0}$. Für festes g und $q \to \infty$ hat nach [Coh93] das Berechnen der Klassengruppe den Aufwand $O(q^{\frac{g}{2}})$. Die Berechnung des L-Polynoms von F_2/K ist nach [Lau02] polynomiell in $p^2d^4n^2$, wobei d den Totalgrad des definierenden Polynoms von F_2/K bezeichnet. Der Aufwand zur Bestimmung der Ordnung eines Elementes von $\mathcal{C}^0_{F_2}$ ist im Wesentlichen durch die Arithmetik in $\mathcal{C}_{F_2/K}$ bestimmt. Der Aufwand für die Berechnung von Stellen vom Grad eins lässt sich auf den Aufwand zum Faktorisieren von univariaten Polynomen über endlichen Körpern zurückführen, siehe dazu Abschnitt 3.4. Dasselbe gilt für den Aufwand zur Berechnung der Operation der Korrespondenzen auf $\mathcal{C}^0_{F_2}$ mittels Algorithmus 3. Der Aufwand für die Berechnung des Kerns einer Matrix $M \in \mathbb{F}_q^{n\times m}$ ist $O(nm^2)$, wie wir aus [Coh93] entnehmen können. Die Komplexität für die Berechnung von Maximalordnungen in Zahlkörpern oder Algebren wird im Wesentlichen von der Faktorisierung der Diskriminante beeinflusst, siehe dazu [Fri00] und [Poh93].

Für die Berechnung der zyklischen Erweiterung in Korollar 1.31 gibt es in der Literatur keine Aufwandsabschätzung. Im wesentlichen müssen wir die Maximalordung des Zentrums $F = Z(E_K)$ der vorgegebenen Algebra E_K berechnen, dann Strahlklassengruppen, deren Strahlklassenkörper und von diesen den Führer berechnen. Der Grad von $F/\mathbb{Q}$ ist nach oben durch das Geschlecht g beschränkt. Zudem kommt nocht die Berechnung der Normgruppe $F^\times/N_{E/F}(E^\times)$, welche isomorph zu $G(E/F)$ ist nach dem Artinschen Reziprozitätsgesetz (s. [Pie82, Chapter 18, Section 7, p. 362]).

Die Berechnung einer $\mathbb{Q}$-Basis der Endomorphismenalgebra im nichtkommutativen Fall hätte im schlimmsten Fall exponentiellen Aufwand, da dann alle in Frage kommenden Matrizen, welche einen Endomorphismus von $\mathcal{C}^0_{F_2}$ darstellen könnten, getestet werden müssten.

4.10 Vergleich mit anderen Verfahren

Wir wollen das in dieser Arbeit entwickelte Verfahren zur Brechnung des Endomorphismenringes $\mathrm{End}_{\mathbb{F}_q}(J_{X_2})$ vergleichen mit denen, die in [Fre07] und [Koh96] angegeben werden. In [Fre07] geht es um die Bestimmung des vollen Endomorphismenringes von Kurven $X_2/\mathbb{F}_p$ vom Geschlecht zwei mit probabilistischen Methoden. Dabei wird noch vorausgesetzt, dass die Jacobische J_{X_2} der Kurve über $\mathbb{F}_p$ einfach ist. In diesem Fall wissen wir, dass der Endomorphismenring in einem CM-Körper $F/\mathbb{Q}$ mit $[F : \mathbb{Q}] = 4$ enthal-

ten ist. Bezeichnet $\mathbb{Z}[\pi]$ die vom Frobenius von $\mathrm{End}_{\mathbb{F}_p}(J_{X_2})$ erzeugte Gleichungsordnung, so sind es die Primteiler l des Index $[\mathcal{O}_F : Z[\pi]]$, die als Nenner in einem Endomorphismus von der Form $\alpha = f(\pi)/l^d \notin \mathbb{Z}[\pi]$ mit $f \in \mathbb{Z}[x]$ vom Grad $\deg f \leq 3$ vorkommen können, wobei hier $l \neq p$ sein muss. In [Fre07] wird gezeigt, dass solch ein Endomorphismus genau dann existiert, wenn $f(\pi)$ auf der l^d-Torsionsuntergruppe $J_{X_2}[l^d]$ der Jacobischen J_{X_2} verschwindet. Das bedeutet, dass wir in einer geeigneten Erweiterung $k' := \mathbb{F}_{p^n}$ von $k := \mathbb{F}_p$ so, dass $J_{X_2}[l^d] \subseteq J_{X_2}(k')$ ist, testen, ob $\phi(p) = 0$ für alle $p \in J_{X_2}[l^d]$ gilt. Der Aufwand für solch einen Test wird dort mit $O(n^3 \log n(\log^3 p)l^{s-4d}(-\log \epsilon))$ angegeben, wobei $\epsilon \in (0,1)$ und $s \in \mathbb{Z}^{\geq 0}$ der maximale Exponent mit $l^s m = \#J_{X_2}(k')$ ist. Der Test ist dann mit der Wahrscheinlichkeit $1-\epsilon$ erfolgreich. Die Schwierigkeit hier ist also vor allem die Berechnung eines minimalen n, so dass $J_{X_2}[l^d] \subseteq J_{X_2}(\mathbb{F}_{p^n})$ gilt, was bei grossen Indexteilern l erwartungsgemäß sehr aufwendig ist.

In dem in dieser Arbeit vorgestellten Verfahren zur Berechnung des Endomorphismenrings im kommutativen Fall ist ein großes l mit $\alpha = f(\pi)/l$ von Vorteil, weil dadurch der Ausdruck $\mathrm{Tr}_{F/\mathbb{Q}}(\alpha\alpha^\star)/l^2$ wie in (4.8) minimiert wird. Bezeichne $C(A) \in \mathcal{D}_{L/F_2}$ die eindeutige Korrespondenz zur dem Element α entsprechenden Korrespondenzklasse, wobei hier der Funktionenkörper $K(X_2) = F_2$ von der Form $F_2 = \mathbb{F}_p(x_2, y_2)$ ist. Mit der positiven ganzen Zahl $s := \mathrm{Tr}_{F/\mathbb{Q}}(\alpha\alpha^\star)/l^2$ können wir die in der Norm der Korrespondenz $C(A)$ vorkommenden Grade der Polyome in x_2 nach oben beschränken. Ist s klein, so benötigen wir wenig Stellen zur Interpolation der Norm von $C(A)$. Allerdings müssen die Punkte der Klassengruppe vom Grad null von der Form $p - p_\infty \in \mathcal{C}^0_{F_2}$ mit $\deg p = 1$ eine zu l teilerfremde Ordnung besitzen, wodurch eventuell eine geeignete Erweiterung $\mathbb{F}_{p^n}$ betrachtet werden muss, so dass in der Jacobischen $J_{X_2}(\mathbb{F}_{p^n})$ genügend Punkte vorkommen.

Bezeichne $\mathcal{S}$ die benötigte Anzahl der Stellen vom Grad eins. Im Fall, dass $l \nmid h_{F_2k'/k}$ und für die Anzahl N der Stellen vom Grad eins nach der Hasse-Weil Schranke ([Sti93, Theorem V.2.3., p. 170]) noch $N \geq -2g\sqrt{q}+q-1 \geq \mathcal{S}$ mit $q = p^n$ gilt, ist der Aufwand im Wesentlichen nur durch die Reduktion bestimmt. Im kommutativen Fall hat der Algorithmus dann, abgesehen von der Berechnung der Maximalordnung und des L-Polynoms, einen Aufwand von $O(q^{g/2} + \mathcal{S}^{g+1}) + \mathrm{poly}(p^2 d^4 n^2) + \mathrm{poly}(g \log q)$, wobei $\mathrm{poly}(r)$ polynomiell in r im Aufwand bedeuten soll.

In [Koh96] wird ein Verfahren vorgestellt, um den Endomorphismenring einer elliptischen Kurve $X_2/\mathbb{F}_q$ zu berechnen. Vom Prinzip her ist die Vorgehensweise ähnli ch wie oben, da auch hier versucht wird mittels Indexteiler von $[\mathcal{O}_F : \mathbb{Z}[\pi]]$ einen eventuellen Aufstieg der Gleichungsordnung $\mathbb{Z}[\pi]$ zu berechnen. Hier ist $F/\mathbb{Q}$ eine imaginär-quadratische Erweiterung. Im kommutativen Fall werden dabei geeignete Isogenien konstruiert, welche isogene elliptische Kurven als Bild und Urbild mit demselben Endomorphismenring und

Frobeniusendomorphismus besitzen. Die Isogenien werden nach bestimmten Vorschriften solange konstruiert, bis kein Aufstieg des Endomorphismenrings mehr möglich ist. Der wesentliche Aufwand ist hier das Faktorisieren von an einer Variable ausgewerteten Modulpolynomen, d.h. das Faktorisieren von Polynomen über endlichen Körpern. Insgesamt ist dieser unter gewissen Voraussetzungen in $O(q^{1/3+\epsilon})$ für beliebiges $\epsilon > 0$. Allerdings bereitet hier die Berechnung des l-ten Modulpolynomes bei großer Primzahl l Probleme, da die Koeffizienten sehr groß werden. Im Falle, dass das Geschlecht der Kurve X_2/F_q eins und F_2 wie oben ist, lassen sich alle Elemente $p - p_\infty \in \mathcal{C}^0_{F_2}$ mit einem Primdivisor $p \in \mathcal{D}_{F_2/\mathbb{F}_q}$ vom Grad $\deg p = 1$ darstellen. Damit stehen uns wesentlich mehr Punkte zur Interpolation der Norm der gesuchten Korrespondenz zur Verfügung. Ansonsten verhält sich der Aufwand wie im obigen Fall beschrieben.

Im nicht-kommutativen Fall wird in [Koh96] ein Algorithmus vorgestellt, mit dem es möglich ist, eine $\mathbb{Q}$-Basis der Endomorphismenalgebra, bestehend aus Endomorphismen, zu berechnen. Anschließend wird gezeigt, dass unter bestimmten Voraussetzungen die von der $\mathbb{Q}$-Basis erzeugte Ordnung in der Endomorphismenalgebra bereits der gesuchte Endomorphismenring ist. Der Aufwand zur Berechnung dieser $\mathbb{Q}$-Basis wird in [Koh96] mit $O(p^{2/3+\epsilon})$ angebeben, wobei $\epsilon > 0$ ist. Bei dem in dieser Arbeit vorgestellten Algorithmus zur Berechnung des Endomorphismenrings im nicht-kommutativen Fall ist der Aufwand zur Berechnung einer $\mathbb{Q}$-Basis im schlimmsten Fall exponentiell, wie bereits erwähnt. Haben wir aber eine $\mathbb{Q}$-Basis berechnet, so können wir mit unserem Algorithmus den vollen Endomorphismenring berechnen.

Das in [Koh96] vorgestellte Verfahren lässt sich nur mit großem Aufwand auf ein höheres Geschlecht übertragen, da hierfür die Verallgemeinerung der j-Invariante nötig ist. Der in dieser Arbeit vorgestellte Algorithmus ist auf beliebige Kurven mit beliebigem Geschlecht anwendbar.

Kapitel 5

Beispiele

In diesem Kapitel wollen wir Beispiele angeben, um zu zeigen, wie die im vorherigen Kapitel entwickelten Algorithmen angewendet werden. Es gelten die Voraussetzungen und Bezeichnungen der vorangegangenen Kapitel. Wir betrachten Funktionenkörper F/K über einem endlichen Konstantenkörper $K = \mathbb{F}_q$ sowie deren zugehörigen projektiven Abschluss X_i/K der affinen Kurven $C(F_i/K) = \mathcal{C}_i/K$. Ein Ideal in $\mathcal{O}_{L/F_2}$ bzw. $\mathcal{O}_{F_i/K}$ schreiben wir als $F_2[x_1]$- bzw. $K[x_j]$-Modul mit jeweils einer $F_2[x_1]$- bzw. $K[x_j]$-Basis ($j = 1, 2$). Punkte von affinen Kurven $\mathcal{C}/K$ mit definierendem Polynom $f(x, y) \in K(x)[y]$ schreiben wir in der Form $(\alpha, \beta) \in \overline{K}^2$ mit $f(\alpha, \beta) = 0$. Für eine Korrespondenz $A \in \mathcal{D}_{L/F_2}$ bezeichnen wir den auf $\mathcal{C}^0_{F_2\overline{K}}$ induzierten Endomorphismus wieder mit A. Mit $\mathbb{P}^1_K$ bezeichnen wir wieder die Stellen vom Grad eins in F_2/K. Alle hier vorkommenden Funktionenkörper sind separabel. Der Polstellendivisor des Hauptdivisors (x) des Funktionenkörpers F ist stets total verzweigt und damit vom Grad eins. Somit wissen wir zudem, dass die Funktionenkörper F/K regulär sind. Mit Hilfe von Lemma 4.2 können wir leicht zeigen, dass in den Fällen, in denen das Geschlecht eins ist, die vollen Endomorphismenringe berechnet wurden. Dies gilt auch in den Fällen, in denen das Geschlecht drei ist. Im Beispiel für das Geschlecht zwei läßt sich dann ebenfalls zeigen, dass der nicht-kommutative Endomorphismenring der Endomorphismenring über dem algebraischen Abschluss ist.

5.1 Geschlecht $g = 1$

5.1.1 Ein Analogon zu Vélu

In diesem Abschnitt wollen wir uns zusätzlich an [Sil86] halten, sofern die dortige Notation mit unserer verträglich ist. Wir beginnen bei Geschlecht $g_{F/K} = 1$. Die Darstellung von Endomorphismen der Jacobischen einer el-

liptischen Kurve als Isogenien war schon Vélu bekannt, siehe [Vél71]. Wir werden sehen, dass die entlang dem Divisor $P_{\infty,1}$ maximal reduzierten Primdivisoren $P \in \mathbb{P}_{L/F_2}$ der Darstellung von Vélu entsprechen. Die meisten der hier im elliptischen Fall gemachten Berechnungen sind schon bekannt mittels Isogenien. Allerdings eignet sich der elliptsiche Fall besonders gut, um die grundlegenden Eigenschaften der Korrespondenzen aufzuzeigen.

Mit Lemma 4.3 wissen wir, dass in jeder Korrespondenzklassse $[A]_C \neq [0]_C$ mit $A \in \mathcal{D}_{L/F_2}$ ein eindeutiger effektiver Divisor $C(A)$ vom Grad $g = 1$ liegt. Das heißt insbesondere, dass $C(A)$ eine Primkorrespondenz ist. Da die Endomorphismen von $\mathrm{End}_{K'}(J_{X_2})$ mit $[K' : K] \leq n$ eindeutig den Korrespondenzklassen von L/F_2K' entsprechen, können wir uns also im Falle nicht-trivialer Endomorphismen auf effektive Divisoren vom Grad eins beschränken, welche nicht konstant sind. Nun gilt folgendes Lemma:

Lemma 5.1. *Sei $A \in \mathcal{D}_{L/F_2}$ mit $[A]_C \neq [0]_C$, $C(A) = P \in \mathbb{P}_{L/F_2}$ und $\deg_{L/F_2}(P) = 1$. Ferner sei $p \in \mathbb{P}_K^1$. Dann sind folgende Aussagen äquivalent:*

(i) $P(p) = p_\infty$,

(ii) $P(p - p_\infty) = 0$, *d.h. also* $p - p_\infty \in \ker P$ *und*

(iii) P *ist nicht p-regulär.*

Beweis. Nach Voraussetzung gilt $P(p_\infty) = p_\infty$, d.h. also $P(p) = p_\infty \iff P(p - p_\infty) = 0$. Das zeigt (i) $\iff$ (ii). Die Äquivalenz (iii) $\Leftrightarrow$ (i) folgt aus Satz 4.6 und Korollar 2.17: Denn wenn P regulär bezüglich p ist, so folgt $P(p) = \overline{P}^p$ nach Korollar 2.17, und per Definition ist dann $P(p) \neq p_\infty$. Gilt andererseits $P(p) \neq p_\infty$, so wissen wir mit Satz 4.6, dass P regulär bezüglich p ist und $\overline{P}^p = P(p) \neq p_\infty$ gilt. □

Um festzustellen, ob P für ein $p \in \mathbb{P}_{F_2/K}$ nicht p-regulär ist, benutzen wir das folgende Lemma:

Lemma 5.2. *Sei $[L : F_2(x_1)] = 2$, $P \in \mathbb{P}_{L/F_2}$ nicht konstant vom Grad $\deg_{L/F_2} P = 1$ und $B_0 \subseteq P_0 \subseteq \mathcal{O}_{L/F_2}$ eine $F_2[x_1]-$Basis von P_0, so dass die Übergangsmatrix $M \in F_2[x_1]^{2\times 2}$ mit $\Omega M = B_0$ in zeilenreduzierter Hermite-Normalform mit normierten Diagonalelementen ist. Ferner sei $p \in \mathbb{P}_{F_2/K}$ vom Grad eins. Dann sind folgende Aussagen äquivalent:*

(i) P *ist p-regulär,*

(ii) B_0 *ist p-regulär,*

(iii) $\det M \in \mathcal{O}_p[x_1]$.

Beweis. Sei P regulär bezüglich p. Dann gibt es insbesondere eine p-ganze Basis $B_{0,\Omega}$ von P_0 und eine Übergangsmatrix $N \in F_2[x_1]^{n\times n}$ mit $N\Omega = B_{0,\Omega}$, so dass $f := \det N \in \mathcal{O}_p[x_1]$ normiert ist. Nach Voraussetzung ist auch $g := \det M$ ein normiertes Polynom in $\mathcal{O}_p[x_1]$, und somit gilt $f = g$. Sei nun $\Omega := \{1, \omega_1\}$ und $B_0 = \{f_0, f_1 + f_2\omega_1\}$ mit $f_i \in F_2[x_1]$ $(i = 0, 1, 2)$. Nach Voraussetzung sind f_0 und f_2 normierte Polynome in $\mathcal{O}_p[x_1]$, da M von der Form

$$M = \begin{pmatrix} f_0 & f_1 \\ 0 & f_2 \end{pmatrix}$$

ist. Aus $\deg_{L/F_2} P = 1$ folgt, dass f irreduzibel in $F_2[x_1]$ ist, und somit erhalten wir $f_0 = f$ und $f_2 = 1$ mit $\deg f_0 = 1$.

Ist nun $f_1 = 0$, so ist B_0 regulär bezüglich p, da die Elemente von $\Omega \subseteq F_1$ immer p-ganz sind. Ansonsten ist $f_1 \neq 0 \mod f_0$ mit $\deg f_1 < \deg f_0$, also $f_1 \in F_2$. Genauso können wir voraussetzen, dass $\omega_1 \notin P_0$ ist. Das bedeutet aber, dass $\pi_P(\omega_1)$ Nullstelle des normierten Polynomes $F(T) := T - \pi_P(f_1) \in F_2[T]$ ist. Da nach Voraussetzung ω_1 ganz bezüglich p ist, muss $\pi_P(f_1)$ in $\mathcal{O}_p$ liegen, d.h. also f_1 ist p-ganz. Damit ist B_0 ganz bezüglich p und somit p-regulär, d.h. wir haben (i) $\Rightarrow$ (ii) und (iii) $\Rightarrow$ (ii) gezeigt. Die Richtung (ii) $\Rightarrow$ (i) ist trivial, ebenso (ii) $\Rightarrow$ (iii). □

5.1.2 Der kommutative Fall

Die zu den Funktionenkörpern F_i vom Geschlecht eins dazugehörigen affinen Kurven E_i seien durch

$$E_i : y_i^2 + a_1x_iy_i + a_3y_i = x_i^3 + a_2x_i^2 + a_4x_i + a_6$$

$(a_i \in K,\ i = 1, 2)$ in Weierstraßnormalform gegeben. Wären die E_i singulär, so würden wir wie in Kapitel 4 die Normalisierungen der projektiven Abschlüsse der Kurven E_i betrachten. Der Einfachheit halber aber nehmen wir an, dass die E_i nicht-singulär sind. Ist der endliche Teil von $C(A)$ durch

$$C(A)_0 = \langle x_1 - f,\ y_2 - g\rangle \quad (f, g \in F_2)$$

gegeben, so definieren wir mittels

$$\phi : E_2 \longrightarrow E_2, \quad [\alpha : \beta : 1] \longmapsto [f(\alpha, \beta) : g(\alpha, \beta) : 1] \tag{5.1}$$

einen Morphismus auf E_2. Umgekehrt ist durch einen Morphismus ϕ, welcher durch (5.1) gegeben ist, eine Korrespondenz aus $\mathcal{D}_{L/F_2}$ definiert. Denn ist $C(A)$ regulär bezüglich p mit $p_0 = \langle x_2 - \alpha, y_2 - \beta\rangle$, so erhalten wir $C(A)(p) = \overline{C(A)}^p$ mit Korollar 2.17, was $[f(\alpha, \beta) : g(\alpha, \beta) : 1] = \phi(p)$ entspricht und ist P nicht p-regulär, so ist $C(A)(p) = p_\infty$, d.h $[0 : 1 : 0] = \phi(p)$.

Da wir hier $[F_i : K(x_i)] = 2$ haben, greift also Lemma 5.2. Insbesondere wissen wir, dass p_∞ genau dann auf p_∞ abgebildet wird, wenn $\det M$ mit M

wie in Lemma 5.1 nicht p_∞-ganz ist, was gleichbedeutend ist, dass $[0:1:0]$ auf $[0:1:0]$ abgebildet wird. Dies bedeutet wiederum, dass wir aus einer nicht-konstanten Primkorrespondenz $C(A)$ für $A \in \mathcal{D}_{L/F_2}$ dann eine Isogenie $\phi : E_2 \longrightarrow E_2$ erhalten, wenn $C(A)$ nicht p_∞-regulär ist, oder, was mit Lemma 5.1 gleichbedeutend ist, dass $C(A)(p_\infty) = p_\infty$ gilt. Letzteres gilt aber per Definition von $C(A)$.

Sei nun $q = 5$, d.h. also $K = \mathbb{F}_5$, und $f_1(x_1, y_1) = y_1^2 - (x_1^3 + x_1) \in K[x_1, y_1]$ und $f_2(x_2, y_2) = y_2^2 - (x_2^3 + x_2) \in K[x_2, y_2]$. Für die Ganzheitsbasis von $\mathcal{O}_{L/F_2}$ wählen wir $\Omega := \{1, y_1\}$. Mit $\mathcal{C}_2/K = E : y_2^2 = x_2^3 + x_2$ bezeichnen wir die zu F_2 dazugehörige affine Kurve. Mittels des L-Polynoms von F_2 berechnen wir das charakteristische Polynom $f_{\pi_K}(t) = t^2 - 2t + 5 = (t - (1 + 2i))(t - (1 - 2i)) \in \mathbb{Z}[i][t]$ des Frobenius π_K von $\mathrm{End}_K(J_{X_2})$ mit $i^2 = -1$. Für die bessere Lesbarkeit wollen wir $X := x_1, Y := y_1$ und $x := x_2$ und $y := y_2$ setzen. Die Frobenius-Korrespondenz von L/F_2 lässt sich dann in der endlichen Maximalordnung $\mathcal{O}_{L/F_2}$ als $F_2[x_1]$-Modul mit den beiden Basiselementen

$$F = \left\langle X - x^5, \quad Y - y^5 \right\rangle$$

beschreiben. Der Endomorphismenring $\mathrm{End}_K(J_{X_2})$ ist eine Ordnung in der Maximalordnung von $\mathbb{Q}(\pi_K)$, da $f_{\pi_K}(t)$ irreduzibel und J_{X_2} über K einfach ist. Für die Korrespondenz F ist dann $f_{\pi_K}(t)$ das charakteristische Polynom. Die Korrespondenzklasse $[A]_C$ mit $A := F - D$ entspricht dem Element $\pm 2i$. Dies können wir testen, indem wir das Produkt $B := A \cdot A$ mittels Algorithmus 1 berechnen und überprüfen, ob $[B]_C = [-4D]_C$ gilt. Dazu berechnen wir $C(A)_0 =$

$$\left\langle X - \tfrac{(x^4+3x^2+1)}{x^3+x}, Y - \tfrac{y(4x^6+1)}{x^6+2x^4+x^2} \right\rangle \tag{5.2}$$

und mit $h_1(x) := \frac{(x^4+3x^2+1)}{x^3+x} \in K(x)$ und $h_2(x, y) := \frac{y(4x^6+1)}{x^6+2x^4+x^2} \in K(x)[y]$ erhalten wir dann $C(B)_0 = \langle X - h_1(h_1(x)), Y - h_2(h_1(x), h_2(x, y)) \rangle =$

$$\Big\langle X - \tfrac{x^{16}+3x^{12}+3x^8+3x^4+1}{x^{15}+x^{13}+3x^9+3x^7+x^3+x}, \\ Y - y\tfrac{x^{24}+3x^{22}+x^{20}+4x^{18}+4x^{16}+3x^{14}+4x^{12}+3x^{10}+4x^8+4x^6+x^4+3x^2+1}{x^{24}+2x^{22}+x^{20}+2x^{18}+4x^{16}+2x^{14}+3x^{12}+x^{10}+3x^8+4x^6+3x^4+4x^2} \Big\rangle .$$

Für die Multiplikation mit 4, d.h. der Korrespondenz $4D$, berechnen wir $C(4D)_0 =$

$$\Big\langle X - \tfrac{x^{16}+3x^{12}+3x^8+3x^4+1}{x^{15}+x^{13}+3x^9+3x^7+x^3+x}, \\ Y + y\tfrac{x^{24}+3x^{22}+x^{20}+4x^{18}+4x^{16}+3x^{14}+4x^{12}+3x^{10}+4x^8+4x^6+x^4+3x^2+1}{x^{24}+2x^{22}+x^{20}+2x^{18}+4x^{16}+2x^{14}+3x^{12}+x^{10}+3x^8+4x^6+3x^4+4x^2} \Big\rangle ,$$

und aus

$$C(4D) + C(B) = \left(X - \tfrac{x^{16}+3x^{12}+3x^8+3x^4+1}{x^{15}+x^{13}+3x^9+3x^7+x^3+x}\right)$$

sehen wir, dass $C(4D) + C(B)$ ein Hauptdivisor ist. Daraus folgt mit Satz 2.3, dass $[4D]_C + [B]_C = [0]_C$ ist, wenn wir die ganze Situation in $L/F_2\overline{K}$ betrachten. Es sei hier noch nebenbei bemerkt, dass wir die Darstellung der Multiplikation mit n mittels Divisionspolynomen einfach dadurch erhalten, in dem wir den Divisor nD entlang $P_{\infty,1}$ maximal reduzieren. Dies gilt auch im Falle $g \geq 2$.

Wir können nun in (5.2) den Kern von $C(A)$ direkt ablesen: Für die Norm berechnen wir

$$f := N_{L/F_2}(C(A)_0) = X - \tfrac{(x^4+3x^2+1)}{x^3+x},$$

und da Y ganz über X ist, reicht es nach Lemma 5.2, diejenigen $p \in \mathbb{P}^1_{\overline{K}}$ zu bestimmen, für die f nicht p-ganz ist. Sind $p_{1_0} := \langle x, y\rangle, p_{2_0} := \langle x + 2, y\rangle$ und $p_{3_0} := \langle x + 3, y\rangle$ die zu den Punkten $(0,0), (3,0)$ und $(2,0) \in K^2$ dazugehörigen Primideale in $\mathcal{O}_{F_2/K}$, so bilden die dazugehörigen Punkte $\mathcal{P}_i := p_i - p_\infty \in \mathcal{C}^0_{F_2}$ $(i = 1, 2, 3)$ zusammen mit $0 \in \mathcal{C}^0_{F_2}$ die 2-Torsionsgruppe in $\mathcal{C}_{F_2/K}$, welche isomorph zu $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist. Aus $x^3 + x = x(x+2)(x+3)$ ersehen wir, dass $C(A)$ für genau die Primdivisoren p_1, p_2, p_3 und p_∞ nicht ganz ist. Es gilt also $\ker A = \{0, \mathcal{P}_1, \mathcal{P}_2, \mathcal{P}_3\}$. Der endliche Teil des Rosati $A^\star$ von A ist ein Primideal

$$A_0^\star = \Big\langle X^4 - xX^3 - 2X^2 - xX - 4, \tag{5.3}$$

$$Y - y\left(\tfrac{X^3}{x^3+x} + \tfrac{3X^2}{x^2+1} + \tfrac{4X}{x^3+1} + \tfrac{1}{x^2+1}\right)\Big\rangle \tag{5.4}$$

mit $\deg_{L/F_2} C(A)^\star = 4 = |\ker A|$. Wie bereits erwähnt, können wir die Primkorrespondenzen $P \in \mathbb{P}_{L/F_2}$ mit $P_0 = \langle X - f, Y - g\rangle$ und $f, g \in F_2$ auch als Isogenien

$$\phi : \mathcal{C}_2(\overline{K}) \longrightarrow \mathcal{C}_2(\overline{K}), \quad (x, y) \longmapsto (f(x, y), g(x, y))$$

mit $f, g \in F_2/K$ interpretieren und umgekehrt. Der Grad einer Isogenie $\phi : (x, y) \longmapsto (f(x, y), g(x, y))$ ist dann der Grad des Rosati $P^\star$, wenn $P_0 = \langle X - f, Y - g\rangle$ ist. Mit Blick auf (4.2) heißt das $\deg \phi = [F_P : F_1^*]$.

Offensichtlich haben $2D$ und A denselben Kern. Für $C(2D)$ erhalten wir

$$C(2D)_0 = \left\langle X - \tfrac{(4x^4+2x^2+4)}{x^3+x}, Y - \tfrac{y(2x^6+3)}{x^6+2x^4+x^2}\right\rangle , \tag{5.5}$$

und setzen wir $A := 1$ und $B := 0$, so erhalten wir für die Divisionspolynome (s. [Sil86, p. 105])

1. $\psi_0 = 0,\ \psi_1 = 1,\ \psi_2 = 2y,\ \psi_3 = 3x^4 + 6x^2 - 1, \psi_4 = 4y(x^6 + 5x^4 - 5x^2 - 1)$,
2. $\phi_2 = x(2y)^2 - \psi_3\psi_1 = x(2y)^2 - (3x^4 + 6x^2 - 1)$ und
3. $\omega_2 = \frac{\psi_4\psi_1^2 - \psi_0\psi_3^2}{4y} = x^6 + 4$.

Damit lässt sich die Multiplikation mit 2, als Isogenie geschrieben $[2] : \mathcal{C}_2/\overline{K} \longrightarrow \mathcal{C}_2/\overline{K}$, wie folgt darstellen:

$$[2]P = \left(\frac{\phi_2(P)}{\psi_2(P)^2}, \frac{\omega_2(P)}{\psi_2(P)^3}\right), \quad (P \in \overline{K}^2) \tag{5.6}$$

wobei hier

$$\frac{\phi_2}{{\psi_2}^2} = \frac{4x^4+2x^2+4}{x^3+x} \quad \text{und} \quad \frac{\omega_2}{{\psi_2}^3} = \frac{y(2x^6+3)}{x^6+2x^4+x^2}$$

ist, d.h. also aus (5.5) wird dann

$$C(2D)_0 = \left\langle X - \frac{\phi_2}{{\psi_2}^2}, Y - \frac{\omega_2}{{\psi_2}^3} \right\rangle.$$

Betrachten wir nun $C(2D)$ als Endomorphismus von $\mathcal{C}^0_{F_2'}$, und ist $Q \in \mathcal{C}^0_{F_2'}$ kein 2-Torsionspunkt, so können wir den Restidealsatz anwenden, um das Bild $C(2D)(Q)$ zu berechnen. Dazu betrachten wir K'/K mit $[K' : K] = 2$, $K' = K(\alpha)$ und Minimalpolynom $t^2 + 4t + 2 \in \mathbb{F}_5[t]$ von α sowie den Primdivisor $p \in \mathcal{D}_{F_2K'/K'}$ und das Ideal $p_0 := \langle x - \alpha, y - \alpha^{21}\rangle \subseteq \mathcal{O}_{F_2K'/K'}$. Das Element $\mathcal{P} := p - p'_\infty \in \mathcal{C}^0_{F_2K'/K'}$ mit $p'_\infty := \mathrm{Con}_{F_2K'/F_2}(p_\infty)$ besitzt Ordnung 8. Ferner lässt sich die Klassengruppe $\mathcal{C}^0_{F_2K'/K'}$ berechnen:

$$\mathcal{C}^0_{F_2K'/K'} \cong \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z}.$$

Da $\mathcal{P} \notin \ker C(2D)$ ist, ist $C(2D)$ mit Lemma 5.1 p-regulär. Das bedeutet $C(2D)(p) = \overline{C(2D)}^p =$

$$\left\langle X - \frac{(4\alpha^4+2\alpha^2+4)}{\alpha^3+\alpha}, Y - \frac{\alpha^{21}(2\alpha^6+3)}{\alpha^6+2\alpha^4+\alpha^2} \right\rangle = \langle x - 1, y - \alpha^{15}\rangle =: q_0,$$

d.h. also nach Voraussetzung an $C(2D)$ erhalten wir $C(2D)(Q) = q - p'_\infty$, ein Element der Ordnung vier. Insbesondere entspricht die Anwendung des Restidealsatzes auf eine Korrespondenz P vom Grad eins und einem Punkt $\mathcal{P}$ dann dem Bild von $\mathcal{P}$ unter der P entsprechenden Isogenie.

Wir betrachten nun noch den Fall der Multiplikation mit $p = \mathrm{char}\, K$. Der Isogenie $[p] = [5]$, also die Multiplikation mit 5, entspricht die Korrespondenz $C(5D)$ mit $C(5D)_0 =$

$$\left\langle X - \frac{(4x^{25}+x^{15}+x^5)}{x^{20}+x^{10}+4}, \right.$$
$$\left. Y - \frac{y(2x^{36}+4x^{34}+2x^{32}+2x^{26}+4x^{24}+2x^{22}+3x^{16}+x^{14}+3x^{12}+4x^6+3x^4+4x^2)}{x^{30}+4x^{20}+2x^{10}+2} \right\rangle$$

mit $x^{20} + x^{10} + 4 = (x^2 + 3)^{10}$. Daraus können wir wiederum ablesen, dass $|\ker[5]| = 5$ ist.

Mit Hilfe von Algorithmus 7 berechnen wir nun den vollen Endomorphismenring $\mathrm{End}_K(J_{X_2}) = \mathbb{Z}[i]$. Die dem Element i entsprechende Korrespondenzklasse ist die Klasse $[B]_C$ mit

$$C(B)_0 = \langle X - 4x, Y - 2y\rangle.$$

Wir wollen hier nicht auf die Details der Berechnungen eingehen, da wir das in den anderen Fällen, in denen $g \geq 2$ ist, bereits tun werden.

5.1.3 Das charakteristische Polynom

Im elliptischen Fall lässt sich das charakteristische Polynom eines Endomorphismus direkt berechnen: Ist P eine nicht-konstante Primkorrespondenz vom Grad eins, so gilt $P^\star P(p) = (\deg_{L/F_2} P^\star)p$ für alle $p \in \mathbb{P}^1_K$, wie man recht schnell mit Hilfe von (4.2) sehen kann. Denn $P^\star P(p)$ ist nichts Anderes als

$$\mathrm{Con}_{F_P/F_1^*}(N_{F_P/F_1^*}(p)) = [F_P : F_1^*]p = (\deg_{L/F_2} P^\star)p.$$

Aus

$$(P + D)(P + D)^\star = (P + D)(P^\star + D) = PP^\star + P + P^\star + D$$

erhalten wir

$$[P + P^\star]_C = [C(P + D)C(P + D)^\star - PP^\star - D]_C,$$

d.h. mit $a_0 := \deg_{L/F_2} P^\star$ und $a_1 := \deg_{L/F_2} C(P + D)^\star - \deg_{L/F_2} P^\star - 1$ erhalten wir als charakteristisches Polynom $f_P(t) := t^2 - a_1 t + a_0$ von P mit $[P^2 - a_1 P + a_0 D] = [0]_C$. Für die Korrespondenz A erhalten wir $C(A+D)_0^\star =$

$$\left\langle X^5 - x^5, Y - \tfrac{yX^4}{x^2+1} - \tfrac{yX^3}{x^3+x} - \tfrac{3yX^2}{x^2+1} + \tfrac{3y}{x^2+1} \right\rangle$$

und $\deg_{L/F_2} C(A + D)^\star = 5$. Daraus berechnen wir mit (5.3) nun $a_0 = 4$ und $a_1 = 5 - 4 - 1 = 0$. Für das charakteristische Polynom von A erhalten wir damit $f_A(t) = t^2 + 4$, $[A]_C$ entspricht also $\pm 2i$, was wir bereits festgestellt haben. Des Weiteren sehen wir, dass $[AA^\star]_C = [N_{\mathbb{Q}(\pi_K)/\mathbb{Q}}(\alpha)D]_C$ gilt, wenn $\alpha \in \mathcal{O}_{\mathbb{Q}(\pi_K)}$ das der Korresponenzklasse $[A]_C \in \mathcal{D}_{L/F_2}$ entsprechende algebraische Element ist.

Es gibt aber noch eine weitere Möglichkeit, das charakteristische Polynom zu bestimmen: Ist $A \in \mathcal{D}_{L/F_2}$ und $\alpha \in \mathcal{O}_F$ das der Korrespondenzklasse $[A]_C$ entsprechende algebraische Element, so gilt $\alpha = (z_0 + z_1\pi_K)/n$ mit $n \in \mathbb{N}$ geeignet und $z_0, z_1 \in \mathbb{Z}$. Nach [Sil86, Corollary 6.3, p. 88] ist durch

$$\langle\ ,\ \rangle : \mathrm{End}(E) \times \mathrm{End}(E) \longrightarrow \mathbb{Z},$$

$$\langle \phi, \psi \rangle \longmapsto \deg(\phi + \psi) - \deg\phi - \deg\psi$$

eine positiv definite Bilinearform auf dem Produkt $\mathrm{End}(E) \times \mathrm{End}(E)$ von Isogenien gegeben. Mit Korrespondenzen ausgedrückt bedeutet das:

$$\langle\ ,\ \rangle : \mathcal{D}_{L/F_2} \times \mathcal{D}_{L/F_2} \longrightarrow \mathbb{Z},$$

$$\langle B_1, B_2 \rangle \longmapsto \deg_{L/F_2} C(B_1 + B_2)^\star - \deg_{L/F_2} C(B_1)^\star - \deg_{L/F_2} C(B_2)^\star.$$

Nun berechnen wir für unsere anfangs gewählte Korrespondenz A die Werte $\langle A, D\rangle = \frac{z_0}{n}\langle D, D\rangle + \frac{z_1}{n}\langle F, D\rangle = 5 - 4 - 1 = 0$ und $\langle A, F\rangle = \frac{z_0}{n}\langle D, F\rangle + \frac{z_1}{n}\langle F, F\rangle = 17 - 4 - 5 = 8$ und weiter $\langle D, D\rangle = 4 - 1 - 1 = 2$, $\langle F, F\rangle = 20 - 5 - 5 = 10$ und $\langle D, F\rangle = 8 - 1 - 5 = 2$. Um nun $x_1 := z_1/n$ und $x_2 := z_0/n$ zu berechnen, lösen wir das Gleichungssystem

$$\begin{pmatrix} 2 & 2 \\ 2 & 10 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 0 \\ 8 \end{pmatrix}$$

und erhalten $x_1 = -1, x_2 = 1$. Dies bedeutet also $A = F - D$, was wir ja bereits schon festgestellt haben.

5.1.4 Verschiedene Darstellungen der Korrespondenzen

Die Tatsache, dass z.B. $\ker C(A) = \{0, Q_1, Q_2, Q_3\}$ ist, können wir auch mit Hilfe des Restidealsatzes direkt nachrechnen, wenn wir eine Darstellung von $C(A)_0$ in $\mathcal{O}_{L/F_2,\infty}$ benutzen. Wir setzen $Z := \frac{1}{X}$ und $V := \frac{Y}{X^2}$ und betrachten den F_2-Isomorphismus

$$\mu : L/F_2 \longrightarrow L/F_2, \quad (X, Y) \longmapsto (\tfrac{1}{Z}, \tfrac{V}{Z^2}),$$

welcher auf F_1 eingschränkt einen K-Isomorphismus $\hat{\mu} := \mu_{|F_1}$ von F_1 nach F_1 mit $V^2 - (Z^3 + Z) = 0$ induziert. Die Maximalordnung $\mathcal{O}_{L/F_2,\infty}$ besitzt als $K[\frac{1}{X}]$-Modul die Ganzheitsbasis $\Omega_i := \{1, \frac{Y}{X^2}\}$, und für $\mathcal{O}_{L/F_2}$ ist $\Omega = \{1, Y\}$ eine Ganzheitsbasis. Nun vermittelt μ einen Isomorphismus zwischen den nicht-konstanten Idealen von $\mathcal{O}_{L/F_2}$ und $\mathcal{O}_{L/F_2,\infty}$, da ein Primdivisor von L/F_2 genau dann in beiden Ringen eine Darstellung als Primideal besitzt, wenn dieser weder ein Pol- noch Nullstellendivisor von X ist. Die Pol- und Nullstellen von $X \in L/F_2$ sind aber allesamt konstante Divisoren.

Wir wollen nun $C(A)_0$ als Ideal in $\mathcal{O}_{L/F_2,\infty}$ darstellen. Wir setzen noch

(i) $f_1(x) := x^4 + 3x^2 + 1$,

(ii) $g_1(x) := x^3 + x$,

(iii) $f_2 := (4x^6 + 1)$ und

(iv) $g_2(x) := x^6 + 2x^4 + x^2$,

wobei die $f_1, g_1, f_2, g_2 \in \mathbb{F}_5[x]$ sind. Für $C(A)_0$ hatten wir $C(A)_0 =$

$$\left\langle X - \tfrac{f_1}{g_1},\ Y - \tfrac{yf_2}{g_2} \right\rangle = \left\langle X - \tfrac{(x^4+3x^2+1)}{x^3+x},\ \ Y - \tfrac{y(4x^6+1)}{x^6+2x^4+x^2} \right\rangle$$

berechnet. Wir behaupten nun, dass das Ideal $\mu(C(A))_0$ von der Gestalt $\mu(C(A))_0 =$

$$\left\langle Z - \tfrac{g_1}{f_1},\ V - \tfrac{yf_2}{g_2}\left(\tfrac{g_1}{f_1}\right)^2 \right\rangle \tag{5.7}$$

ist, d.h. also

$$\left\langle Z - \tfrac{x^3+x}{(x^4+3x^2+1)}, V - \tfrac{y(4x^4+4x^2+4)}{x^6+2x^4+3x^2+4} \right\rangle \subseteq \mathcal{O}_{L/F_{2,\infty}}$$

gilt. Zuerst bilden wir die Erzeuger von $C(A)_0$ ab und erhalten ein Ideal

$$\left\langle \tfrac{1}{Z} - \tfrac{f_1}{g_1}, \tfrac{V}{Z^2} - \tfrac{yf_2}{g_2} \right\rangle \quad \subseteq \ \mathcal{O}_{L/F_{2,\infty}} \left[K[Z]^{-1}\right]$$

per Definition von $\mu(C(A))$ (s. (1.14)). Dies lässt sich dann weiter umformen zu

$$\left\langle \tfrac{1-\frac{f_1}{g_1}Z}{Z}, \tfrac{V-\frac{yf_2}{g_2}Z^2}{Z^2} \right\rangle = \left\langle Z - \tfrac{g_1}{f_1}, V - \tfrac{yf_2}{g_2}Z^2 \right\rangle ,$$

und aus $Z^2 \equiv (g_1/f_1)^2$ erhalten wir dann eine Darstellung wie in (5.7), da wir nun dieses Ideal auch als Ideal in $\mathcal{O}_{L/F_{2,\infty}}$ auffassen können.

Das Ideal $\mu(C(A))_0$ ist regulär bezüglich p_i, wenn $Q_i = p_i - p_\infty$ ist $(i = 1, 2, 3)$ mit

$$p_{1_0} := \langle x, y\rangle, \quad p_{2_0} := \langle x+2, y\rangle \text{ und } p_{3_0} := \langle x+3, y\rangle,$$

denn es ist $x^6+2x^4+3x^2+4 = (x+1)^3(x+4)^3$, $x^4+3x^2+1 = (x+1)^2(x+4)^2$, und die Norm von $\mu(C(A))_0$ ist $Z-(x^3+x)/(x^4+3x^2+1)$. Daraus erhalten wir dann mit dem Restidealsatz und Korollar 2.17

$$\mu(C(A))(p_i)_0 = \overline{\mu(C(A))_0}^{p_i} = \langle Z, V\rangle \in \mathcal{O}_{F_{1,\infty}}.$$

Wenden wir darauf nun $\gamma := \tau \circ \hat{\mu}^{-1}$ an, so erhalten wir $\gamma(\mu(C(A))(p_i)_0) = \langle \frac{1}{x}, \frac{y}{x^2}\rangle$, was nichts Anderes als die Darstellung von p_∞ als Ideal in der unendlichen Maximalordnung von F_2 ist. Das Ideal $\mu(C(A))_0$ ist aber auch regulär bezüglich p_∞: Wir können $(x^3+x)/(x^4+3x^2+1)$ umformen zu

$$\tfrac{1}{x}\left(\tfrac{1+(\frac{1}{x})^3}{1+3\frac{1}{x}+(\frac{1}{x})^4}\right) \in \mathcal{O}_{p_\infty}$$

und analog $y(4x^4+4x^2+4)/(x^6+2x^4+3x^2+4)$ zu

$$\tfrac{y}{x^2}\left(\tfrac{4+4(\frac{1}{x})^2+4(\frac{1}{x})^4}{1+2(\frac{1}{x})^4+3(\frac{1}{x})^3+4(\frac{1}{x})^6}\right) \in \mathcal{O}_{p_\infty}.$$

Daraus können wir dann ersehen, dass ebenfalls $\gamma\left(\overline{\mu(C(A))_0}^{p_\infty}\right) = \langle \frac{1}{x}, \frac{y}{x^2}\rangle$ gilt, womit wir also mit Hilfe des Restidealsatzes direkt verifiziert haben, dass $\ker C(A) = \{0, Q_1, Q_2, Q_3\}$ ist.

5.1.5 Der nicht-kommutative Fall

Wir wollen nun noch ein Beispiel für den nicht-kommutativen Fall bringen. Sei dazu $q = 19$, d.h. also $K = \mathbb{F}_{19}$, und $f_1(x_1, y_1) = y_1^2 - (x_1^3 + x_1) \in K[x_1, y_1]$ sowie $f_2(x_2, y_2) = y_2^2 - (x_2^3 + x_2) \in K[x_2, y_2]$. Dann sind F_1 und F_2 wieder separable Erweiterungen mit genauem Konstantenkörper K und der Unendlichdivisor ist jeweils total verzweigt. Für die Ganzheitsbasis von $\mathcal{O}_{L/F_2}$ wählen wir $\Omega := \{1, y_1\}$.

Mit $\mathcal{C}_2/K = E : y_2^2 = x_2^3 + x_2$ bezeichnen wir die zu F_2 dazugehörige affine Kurve. Mittels des L-Polynomes von F_2 berechnen wir das charakteristische Polynom $f_{\pi_K}(t) = t^2 + 19 \in \mathbb{Z}[t]$ des Frobenius π_K von $\mathrm{End}_K(J_{X_2})$, d.h. also $Z(E_K) = \mathbb{Q}(\pi_K) =: F$. Für die bessere Lesbarkeit schreiben wir wieder $X := x_1, Y := y_1$ und $x := x_2$ und $y := y_2$.

Algorithmus 7 berechnet für $\mathrm{End}_K(J_{X_2}) = \mathbb{Z}[\pi_K]$. Setzen wir nun $K' := \mathbb{F}_{19^2}$ mit $K'^{\times} = \langle \alpha \rangle$ mit α Nullstelle des irreduziblen Polynoms $t^2 + 18t + 2 \in \mathbb{F}_{19}[t]$, so ist $f_{\pi_{K'}} = (x + 19)^2$. Damit ist mit $E_{K'} := \mathrm{End}^0_{K'}(J_{X_2})$ dann $E_{K'} \otimes \mathbb{R} \cong \mathbb{H}$. Für E können wir $E = F$ setzen. Denn für die Invarianten von Satz 1.30 sind $\mathrm{inv}_{v_j}(F_{v_j} \otimes D) = \frac{1}{2}$ für $v_1 = \nu_p$ und $v_2 = |\cdot|$. Da $[E_{v_1} : \mathbb{Q}_{v_1}] = 2$ und $E/\mathbb{Q}$ total-imaginär ist, zerfällt also $E_{K'}$ über E, und außerdem ist $E/\mathbb{Q}$ zyklische Galoiserweiterung von $Z(E_{K'}) = \mathbb{Q}$ mit $G(E/\mathbb{Q}) = \langle \sigma \rangle$. Damit ist insbesondere $\mathrm{Ind}(E_{K'}) = 2$. Als Element $u \in \mathbb{Q}^{\times}$ mit $\mathrm{ord}(u) = 2$ in $\mathbb{Q}^{\times}/N_{E/\mathbb{Q}}(E^{\times})$ können wir $u = -1$ wählen.

Algorithmus 8 berechnet dann die Korrespondenzen

$$B := \left\langle X - x^{19}, Y - y^{19} \right\rangle$$

und

$$U := \langle X + x, Y + \alpha^{90} y \rangle$$

mit $U^2 = -D$ und $B^2 = -19D$, wobei hier D die Einheitskorrespondenz $D = \langle X - x, Y - y \rangle$ bezeichnen soll. Damit haben wir bis auf Isomorphie $\mathrm{End}^0_{K'}(J_{X_2}) \cong (E, \sigma, -1)$, wobei $(E, \sigma, -1)$ eine Quaternionenalgebra über $\mathbb{Q}$ mit der $\mathbb{Q}$-Basis $(1, \pi, u, \pi u)$ ist und den Relationen $\pi^2 = -19, u^2 = -1$ und $\pi u = -u\pi$ oder $u^{-1}\pi u = -\pi = \sigma(\pi)$. In $E_{K'}$ können wir zwei Konjugationsklassen $\{[\mathcal{O}_1], [\mathcal{O}_2]\}$ von Maximalordnungen berechnen, welche als $\mathbb{Z}$-Moduln von der Form

$$\mathcal{O}_1 = \left\langle 1, u, \tfrac{u+\pi u}{2}, \tfrac{1+\pi}{2} \right\rangle \text{ und } \mathcal{O}_2 = \left\langle \tfrac{2+u+3\pi u}{4}, \tfrac{2\pi+u+7\pi u}{4}, \tfrac{u+3\pi u}{2}, 2\pi u \right\rangle$$

mit jeweils Diskriminante $\mathrm{disc}\, \mathcal{O}_i = 19$ $(i = 1, 2)$ sind. Für die Ordnung $\mathfrak{D} = \langle 1, \pi, u, \pi u \rangle \subseteq \mathrm{End}_{K'}(J_{X_2})$ berechnen wir $\mathrm{disc}\, \mathfrak{D} = 2^2 \cdot 19$. Algorithmus 8 berechnet nun die Korrespondenzen

$$A_1 := \left\langle X + \tfrac{4x^5 + \alpha^{30}x^4 + 13x^3 + \alpha^{150}x^2 + x + \alpha^{210}}{x^4 + \alpha^{350}x^3 + 9x^2 + \alpha^{50}x + 7}, \right.$$
$$\left. Y + \tfrac{y\left(\alpha^{150}x^6 + 2x^5 + \alpha^{190}x^4 + 4x^3 + \alpha^{70}x^2 + 12x + \alpha^{90}\right)}{x^6 + \alpha^{230}x^5 + 3x^4 + \alpha^{230}x^3 + 5x^2 + \alpha^{350}x + 18} \right\rangle$$

und

$$A_2 := \langle\, X + \frac{15x^5+\alpha^{210}x^4+6x^3+\alpha^{330}x^2+18x+\alpha^{30}}{x^4+\alpha^{350}x^3+9x^2+\alpha^{50}x+7},$$
$$Y + \frac{y\big(8x^6+\alpha^{290}x^5+13x^4+\alpha^{310}x^3+10x^2+\alpha^{210}x+1\big)}{x^6+\alpha^{230}x^5+3x^4+\alpha^{230}x^3+5x^2+\alpha^{350}x+18} \Big\rangle,$$

wobei A_1 dem Element $\frac{\pi+u}{2}$ und A_2 dem Element $\frac{1+\pi u}{2}$ entspricht. Die Ordnung $\mathcal{O}_3 := \langle 1, \pi, \frac{\pi+u}{2}, \frac{1+\pi u}{2}\rangle$ ist maximal und somit ist $\mathrm{End}_{K'}(J_{X_2}) \cong \mathcal{O}_3$.

Bemerkung 5.3. *In [Deu41] zeigt Deuring, dass im nicht-kommutativen Fall der Endomorphismenring einer elliptischen Kurve über einem endlichen Körper der Charakteristik p isomorph zu einer Maximalordnung in der Algebra $\mathbb{Q}_{\infty,p}$ ist.*

5.2 Geschlecht $g = 2$

5.2.1 Der kommutative Fall

Wir betrachten nun ein Beispiel für Geschlecht $g = 2$. Sei $K = \mathbb{F}_3$ und $F_i/K = K(x_i, y_i)$ mit $y_i^2 - (x_i^5 + x_i^4 + x_i^3 + 2x_i^2 + x_i) = 0$ $(i = 1, 2)$ mit dazugehörigen affinen Kurven $\mathcal{C}_i$.

Wir schreiben wieder $X := x_1, Y := y_1, x := x_1$ und $y := y_1$. Wir setzen $\Omega := \{1, Y\}$, und für das charakteristische Polynom des Frobenius berechnen wir mittels des L-Polynoms von F_2 nun $f_{\pi_K} = t^4 - 2t^2 + 9 \in \mathbb{Z}[t]$, wobei f_{π_K} irreduziebel ist. Für das Zentrum erhalten wir also $F = \mathbb{Q}(\pi_K)$. Mit (1.17) wissen wir, dass mit $E_K := \mathrm{End}_K^0(J_{X_2})$ und $[E_K : \mathbb{Q}] = 4$ dann $E_K = F$ gilt, d.h. also E_K ist ein Körper. Wir wollen nun die einzelnen Schritte der Algorithmen 5 und 7 nachvollziehen und zeigen, wie wir den vollen Endomorphismenring in E_K berechnen können.

Wir bezeichnen mit π wieder π_K und setzen $\mathcal{O}^{(0)} := \mathbb{Z}[\pi]$. Mit den Bezeichnungen von Satz 1.21 erhalten wir $F = \mathbb{Q}(\pi)$, und F besitzt einen totalreellen Teilkörper $F_0 = \mathbb{Q}(\beta)$ von F, wobei $f_0(t) := t^2 - 8t + 8 \in \mathbb{Q}[t]$ das Minimalpolynom von β ist. Schließlich ist $F = F_0(\gamma)$ mit $g(t) := t^2 - (\beta+4)t + 3 \in F_0[t]$ als Minimalpolynom von γ eine imaginärquadratische Erweiterung von F_0. Damit liegt also der letze Typ von Endomorphismenring in Satz 1.21 vor, und Spur und Norm der Endomorphismenalgebra E_K sind die gewöhnliche Spur und Norm von F. Außerdem ist unsere Involution, der Rosati, nach Satz 1.21 die komplexe Konjugation. Wir berechnen nun Basen

$$\Omega^{(0)} = \Big\{1, \pi, \tfrac{1+\pi^2}{2}, \tfrac{9+7\pi+3\pi^2+\pi^3}{12}\Big\}$$

von $\mathcal{O}_F$ und

$$\Delta^{(0)} = \big\{1, \pi, 1 + \pi^2, 9 + 7\pi + 3\pi^2 + \pi^3\big\}$$

von $Z[\pi]$ mit $m_{11}^{(0)} = m_{22}^{(0)} = 1$, $m_{33}^{(0)} = 2$ und $m_{44}^{(0)} = 12$ und schließlich

$$\Lambda^{(0)} = \{0\} \times \{0\} \times \{-1, .., 1\} \times \{-11, .., 11\}.$$

Der Algorithmus 7 durchläuft nun alle $\underline{\lambda}^{(i)} \in \Lambda^{(i)}$ mit $\underline{\lambda}^{(i)} \neq \underline{0}$ und bildet jedesmal ein Element

$$\alpha = \sum_{j=1}^{l} \lambda_j^{(i)} \omega_j^{(i)} = \sum_{j=1}^{l} \frac{\lambda_j^{(i)}}{m_{jj}^{(i)}} \delta_j^{(i)} = \frac{\sum_{j=0}^{l-1} \mu_j^{(i)} \pi^j}{m} \quad (\mu_j^{(i)} \in \mathbb{Z}),$$

das nun mit Hilfe von Algorithmus 5 daraufhin getestet werden soll, ob es eine Korrespondenz $B \in \mathcal{D}_{L/F_2}$ so gibt, dass $[B]_C$ dem Element α als Endomorphismus entspricht. Ist nun $\underline{\lambda}^{(i)} = (0, 0, 1, 0)$, so erhalten wir $\alpha = \frac{1+\pi^2}{2}$. Da hier $g \neq \mathrm{char}(K)$ ist, kann der inseparable Fall nicht auftreten, d.h. also $k = 0$ mit den Bezeichnungen von Algorithmus 5, den wir nun mit den Parametern

1. $\mathcal{O}_{L/F_2}$ und $g = 2$,
2. $d = 1$ und $l = 4$,
3. der Basis $\{1, \pi, \pi^2, \pi^3\}$ von $\mathbb{Z}[\pi]$,
4. $1 + \pi^2$,
5. D, F, F^2, F^3 und
6. $m = 2$

aufrufen. Der Endomorphismus ϕ ist der durch die Korrespondenz $D + F^2$ induzierte K-Endomorphismus auf $\mathcal{C}_{F_2'}^0$, und $[D+F^2]_C$ entspricht $1+\pi^2 = \phi$. Für den Wert s erhalten wir mit $l = 0$, $m' = m$ und $2 = [F_2 : K(x_2)]$ dann

$$s = 2\frac{\mathrm{Tr}_{F/\mathbb{Q}}(\phi \circ \phi^\star)}{2 \cdot 4} = \frac{\mathrm{Tr}_{F/\mathbb{Q}}(\phi \circ \phi^\star)}{4} = 12.$$

Weiter ist mit $\tilde{s} = 6$ und $\gamma = 5$ dann $\mathcal{S}_1 = (6+1) + (3+1) = 11$ und $\mathcal{S}_2 = 7$ sowie $\mathcal{S} = \mathcal{S}_1 + \mathcal{S}_2 = 18$. Wir benötigen also 18 Stellen $p_1, ..., p_{18} \subseteq \mathbb{P}_{F_2/K^{(i)}}$ vom Grad eins von $F_2/K^{(i)}$ mit eventuell einer geeigneten Konstantenkörpererweiterung $K^{(i)}$ (wobei dieses i das von Algorithmus 5 ist) von K, die den folgenden Bedingungen genügen: (mit den Bezeichnungen von Algorithmus 5)

(i) $p_j \neq p_\infty$,

(ii) $\mathrm{ggT}(o_j, 2) = 1$,

(iii) $\phi(p_j - p_\infty) = a_j - r p_\infty + (f)$ mit $a_j \in \mathcal{D}_{F_2/K^{(i)}}$ effektiv vom Grad $1 \leq r \leq 2$,

(iv) $t_j(a_j - rp_\infty) = b_j - 2p_\infty + (f)$ mit $t_j m \equiv 1 \mod o_j$, wobei $b_j = \sum_t q_t$ ist mit $q_t \in \mathbb{P}_{F_2/K^{(i)}}$ paarweise verschieden und $p_\infty \notin \mathrm{supp}(b_j)$.

Die Klassengruppe $\mathcal{C}^0_{F_2/K} \cong \mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times Z/2\mathbb{Z}$ enthält nur 2-Torsionspunkte. Der Algorithmus findet aber in $\mathcal{C}^0_{F_2K'/K'} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times Z/14642\mathbb{Z}$ mit $[K' : K] = 5$ die gesuchten 18 Punkte. Für T erhalten wir mit $K' = K(\alpha)$ dann $T =$

$$\{\ \langle\langle\alpha^{26},\alpha^{202}\rangle,\langle\alpha^2,\alpha^{189}\rangle\rangle,\ \langle\langle\alpha^{26},\alpha^{202}\rangle,\langle\alpha^2,\alpha^{68}\rangle\rangle,\ \langle\langle\alpha^{78},\alpha^{122}\rangle,\langle\alpha^6,\alpha^{204}\rangle\rangle,$$
$$\langle\langle\alpha^{78},\alpha^{122}\rangle,\langle\alpha^6,\alpha^{83}\rangle\rangle,\ \langle\langle\alpha^{82},1\rangle,\langle\alpha^{14},2\rangle\rangle,\ \langle\langle\alpha^{82},1\rangle,\langle\alpha^{14},1\rangle\rangle,$$
$$\langle\langle\alpha^{234},\alpha^{124}\rangle,\langle\alpha^{18},\alpha^{128}\rangle\rangle,\ \langle\langle\alpha^{234},\alpha^{124}\rangle,\langle\alpha^{18},\alpha^{7}\rangle\rangle,\ \langle\langle\alpha^{4},1\rangle,\langle\alpha^{42},2\rangle\rangle,$$
$$\langle\langle\alpha^{4},1\rangle,\langle\alpha^{42},1\rangle\rangle,\ \langle\langle\alpha^{218},\alpha^{130}\rangle,\langle\alpha^{54},\alpha^{142}\rangle\rangle,\ \langle\langle\alpha^{218},\alpha^{130}\rangle,\langle\alpha^{54},\alpha^{21}\rangle\rangle,$$
$$\langle\langle\alpha^{38},\alpha^{132}\rangle,\langle\alpha^{122},\alpha^{209}\rangle\rangle,\ \langle\langle\alpha^{38},\alpha^{132}\rangle,\langle\alpha^{122},\alpha^{88}\rangle\rangle,\ \langle\langle\alpha^{114},\alpha^{154}\rangle,\langle\alpha^{124},\alpha^{143}\rangle\rangle,$$
$$\langle\langle\alpha^{114},\alpha^{154}\rangle,\langle\alpha^{124},\alpha^{22}\rangle\rangle\ \langle\langle\alpha^{12},1\rangle,\langle\alpha^{126},2\rangle\rangle\ \langle\langle\alpha^{12},1\rangle,\langle\alpha^{126},1\rangle\rangle\ \}$$

und erstellen dann die Matrizen $\mathcal{M}_0 \in {\mathbb{F}_{3^5}}^{18\times18}$ und $\mathcal{M}_1 \in {\mathbb{F}_{3^5}}^{18\times18}$. Der Kern $\ker\mathcal{M}_0 \cap \mathbb{F}_3$ wird durch die Zeilen der folgenden Matrix $\mathcal{N}_0 :=$

$$\begin{pmatrix} 2&2&1&1&2&2&0&0&0&0&0&1&0&0&2&0&0&0\\ 0&2&2&1&1&2&2&0&0&0&0&0&1&0&0&2&0&0 \end{pmatrix}$$

erzeugt, und $\ker\mathcal{M}_1 \cap \mathbb{F}_3$ wird von den Zeilen der Matrix $\mathcal{N}_1 :=$

$$\begin{pmatrix} 0&0&0&2&0&0&0&0&0&0&0&1&0&0&2&0&0&0\\ 0&0&0&0&2&0&0&0&0&0&0&0&1&0&0&2&0&0\\ 0&0&0&0&0&2&0&0&0&0&0&0&0&1&0&0&2&0\\ 0&0&0&2&0&0&2&0&0&0&0&1&0&0&0&0&0&2 \end{pmatrix}$$

erzeugt. Sei

$$f = N_{L/F_2}(C(B)_0) = X^2 + X\tfrac{f_1}{g_1} + \tfrac{f_0}{g_0}$$

mit $f_1, f_0 \in K[x, y]$ und $g_1, g_0 \in K[x]$ und

$$f_k = yh_1^{(k)} + h_0^{(k)} \text{ mit } h_1^{(k)} = \textstyle\sum_{l=0}^{4} \lambda_{l1}^{(k)} x^l \text{ und } h_0^{(k)} = \sum_{l=0}^{6} \lambda_{l0}^{(k)} x^l$$

sowie

$$g_k = \textstyle\sum_{l=0}^{6} \mu_{l0} x^l \quad (k = 0, 1).$$

Für die erste Zeile von $\mathcal{N}_0$ erhalten wir z.B.

$$h_0^{(0)} = 2 + 2x + x^2 + x^3 + 2x^4 + 2x^5 + 0x^6, \quad h_1^{(0)} = 0 \text{ und } g_0 = 1 + 2x^3.$$

Führen wir dasselbe mit der zweiten Zeile von $\mathcal{N}_0$ durch, so erhalten wir $h_0^{(0)} = x(2 + 2x + x^2 + x^3 2x^4 + 2x^5)$, $h_1^{(0)} = 0$ und $g_0 = x(1 + 2x^3)$. Daraus ersehen wir, dass der Quotient f_0/g_0 unabhängig von der Wahl des nicht-trivialen Elements aus dem Kern sind. Derselbe Sachverhalt lässt sich für

den Quotienten f_1/g_1 feststellen. Schließlich erhalten wir die eindeutigen Lösungen

$$\frac{f_0}{g_0} = \frac{x^5+x^4+2x^3+2x^2+x+1}{x^3+2} \quad \text{und} \quad \frac{f_1}{g_1} = \frac{x^3}{x^3+2},$$

d.h. also für die Norm erhalten wir

$$f := N_{L/F_2}(C(B)_0) = X^2 + \frac{x^3}{x^3+2}X + \frac{x^5+x^4+2x^3+2x^2+x+1}{x^3+2}.$$

Nun können wir die Hochhebung $f\mathcal{O}_{L/F_2}$ berechnen und erhalten die beiden Primideale $P_0 :=$

$$\left\langle X^2 + \frac{x^3}{x^3+2}X + \frac{x^5+x^4+2x^3+2x^2+x+1}{x^3+2}, \right.$$
$$\left. Y + \frac{y(2x^4+x^3+x+1)}{x^5+x^4+x^3+2x^2+2x+2}X + \frac{y(x^5+2x^4+2x^2+2x)}{x^5+x^4+x^3+2x^2+2x+2} \right\rangle$$

und $Q_0 :=$

$$\left\langle X^2 + \frac{x^3}{x^3+2}X + \frac{x^5+x^4+2x^3+2x^2+x+1}{x^3+2}, \right.$$
$$\left. Y + \frac{y(x^4+2x^3+2x+2)}{x^5+x^4+x^3+2x^2+2x+2}X + \frac{y(2x^5+x^4+x^2+x)}{x^5+x^4+x^3+2x^2+2x+2} \right\rangle$$

Da weder P_0 noch Q_0 Hauptideale sind, haben wir also nicht-triviale Korrespondenzen berechnet. Um schließlich zu bestimmen, welcher der Divisoren P und Q der gesuchten Korrespondenz $B \in \mathcal{D}_{L/F_2}$ entspricht, benutzen wir die Korrespondenzpaarung. Wir wissen zumindest, dass $Q = -P$ ist, da

$$Q + P = \left(X^2 + \frac{x^3}{x^3+2}X + \frac{x^5+x^4+2x^3+2x^2+x+1}{x^3+2}\right) \in \mathcal{P}_{L/F_2}$$

gilt, d.h. also $[Q+P]_C = [0]_C$. Somit entspricht eine der Korrespondenzen P und Q dem Element $(1+\pi^2)/2$, die andere dann $-(1+\pi^2)/2$.

Es sei an dieser Stelle bemerkt, dass die Kurve $\mathcal{C}_2/K$ an der unendlichen Stelle eine Singularität besitzt. Da wir aber die jeweiligen affinen Kurven mit Hilfe der endlichen bzw. unendlichen Maximalordnung darstellen, handelt es sich hier, wie in Kapitel 2 bereits ausgeführt, um normalisierte Kurven, d.h. bei der Korrespondenzpaarung betrachten wir nicht-singuläre Kurven, die birational äquivalent zu den Ausgangskurven sind.

Wir fassen die Korrespondenzklasse $[P]_C$ bzw. $[Q]_C$ als Element von $F/\mathbb{Q}$ auf und bezeichnen dieses mit ζ bzw. η. Beide Elemente lassen sich als $\mathbb{Q}$-Linearkombination $\zeta = \sum_{i=0}^{3} q_i\pi^i$ und $\eta = \sum_{i=0}^{3} r_i\pi^i$ darstellen. Mit Hilfe der Bilinearität der Korrespondenzpaarung (s. Korollar 2.25) können wir die Koeffizienten durch den Ansatz

$$\langle P, F^j\rangle = \sum_{i=0}^{3} q_i\langle F^i, F^j\rangle = s_j \quad (j = 0,1,2,3) \tag{5.8}$$

bestimmen, indem wir mit Hilfe von Lemma 2.24 eine symmetrische Matrix M der Gestalt $M =$

$$\begin{pmatrix} \langle D,D\rangle & \langle D,F\rangle & \langle D,F^2\rangle & \langle D,F^3\rangle \\ \langle F,D\rangle & \langle F,F\rangle & \langle F,F^2\rangle & \langle F,F^3\rangle \\ \langle F^2,D\rangle & \langle F^2,F\rangle & \langle F^2,F^2\rangle & \langle F^2,F^3\rangle \\ \langle F^3,D\rangle & \langle F^3,F\rangle & \langle F^3,F^2\rangle & \langle F^3,F^3\rangle \end{pmatrix} = \begin{pmatrix} 4 & 0 & 4 & 0 \\ 0 & 12 & 0 & 12 \\ 4 & 0 & 36 & 0 \\ 0 & 12 & 0 & 108 \end{pmatrix}$$

berechnen und dann das Gleichungssystem $M(q_0,q_1,q_2,q_3)^t = (s_0,s_1,s_2,s_3)^t$ lösen. Für $(s_0,s_1,s_2,s_3)^t$ berechnen wir nun $(s_0,s_1,s_2,s_3)^t = (-4,0,-20,0)$ und dann $(q_0,q_1,q_2,q_3)^t = (-\frac{1}{2},0,-\frac{1}{2},0)^t$, d.h. also die Korrespondenzklasse $[P]_C$ entspricht dem Element $-(1+\pi^2)/2$. Damit wissen wir bereits, dass Q die gesuchte Korrespondenz ist.

Nun berechnen wir die Ordnung $\mathcal{O}^{(1)} := Z[\pi][\frac{\pi^2+1}{2}]$ und Basen

$$\Delta^{(1)} = \left\{1, \pi, \tfrac{1+\pi^2}{2}, \tfrac{9+7\pi+3\pi^2+\pi^3}{2}\right\}$$

und

$$\Omega^{(1)} = \left\{1, \pi, \tfrac{1+\pi^2}{2}, \tfrac{9+7\pi+3\pi^2+\pi^3}{12}\right\}$$

mit $m_{11}^{(1)} = m_{22}^{(1)} = m_{33}^{(1)} = 1$ und $m_{44}^{(1)} = 6$. Als Letztes berechnen wir

$$\Lambda^{(1)} = \{0\} \times \{0\} \times \{0\} \times \{-5, ..., 5\}.$$

Für das Element $\underline{\lambda}^{(1)} = (0,0,0,1)^t$ erhalten wir $\alpha = \frac{9+7\pi+3\pi^2+\pi^3}{12}$, d.h. wir rufen den Algorithmus 5 mit den vorgenannten Parametern außer $m = 12$ auf. Der Algorithmus berechnet dann die Norm $f = N_{L/F_2}(C(B)_0) =$

$$X^2 + \tfrac{x^5+x^4+x^3+2x^2+2}{x^5}X + \tfrac{x^5+2x^4+2x^3+x^2+x+2}{x^5},$$

und damit gilt diesmal für die Hochhebung $f\mathcal{O}_{L/F_2} = R_0S_0$ mit $S_0 :=$

$$\Big\langle X^2 + \tfrac{x^5+x^4+x^3+2x^2+2}{x^5}X + \tfrac{x^5+2x^4+2x^3+x^2+x+2}{x^5}, \\ Y + \tfrac{y(2x^6+2x^4+x^2+2x+1)}{x^8}X + \tfrac{y(x^6+x^3+x+1)}{x^8}\Big\rangle$$

und $R_0 :=$

$$\Big\langle X^2 + \tfrac{x^5+x^4+x^3+2x^2+2}{x^5}X + \tfrac{x^5+2x^4+2x^3+x^2+x+2}{x^5}, \\ Y + \tfrac{y(x^6+x^4+2x^2+x+2)}{x^8}X + \tfrac{y(2x^6+2x^3+2x+2)}{x^8}\Big\rangle.$$

Wir berechnen dann für das der Klasse $[R]_C$ entsprechende Element $\zeta = \sum_{i=0}^{3} q_i\pi^i$ den Vektor $(q_0,q_1,q_2,q_3) = (\frac{3}{4}, \frac{7}{12}, \frac{1}{4}, \frac{1}{12})$, d.h. also R ist die gesuchte Korrespondenz gewesen. Schließlich gibt der Algorithmus die Liste

$$L = \left\langle \left\langle Q, \tfrac{1+\pi^2}{2}\right\rangle, \left\langle R, \tfrac{9+7\pi+3\pi^2+\pi^3}{12}\right\rangle\right\rangle$$

zurück. Damit haben wir den vollen Endomorphismenring $\mathrm{End}_K(J_{X_2}) = \mathcal{O}_F$ berechnet.

5.2.2 Der nicht-kommutative Fall

Jetzt betrachten wir $E_{K'} = \mathrm{End}^0_{K'}(J_{X_2}) \cong \mathrm{End}^0_{K'}(A^r)$ mit $r \leq 2$ und $K' = K(\alpha)$, wobei α Nullstelle des irreduziblen Polynoms $t^2 + 2t + 2 \in K[t]$ und A einfache abelsche Varietät über K' ist. Für das charakteristische Polynom des Frobenius $\pi_{K'}$ erhalten wir $f_{\pi_{K'}}(t) = (t^2 - 2t + 9)^2 \in \mathbb{Z}[t]$. Daraus ersehen wir, dass $E_{K'}$ nicht mehr kommutativ und $\mathrm{Deg}(E_{K'}) = 2$ ist. Das Zentrum $Z(E_{K'}) = F' = \mathbb{Q}(\pi_{K'})$ ist eine imaginär-quadratische Erweiterung von $\mathbb{Q}$. Indem wir den Index $d = \mathrm{Ind}(E_{K'}) = \mathrm{Deg}(D)$ berechnen, wobei hier D ein Schiefkörper $D \in \mathfrak{S}(F')$ mit $D = \mathrm{End}^0_{K'}(A_{K'})$ sein soll, können wir bestimmen, ob $E_{K'} \cong M_2(F')$ oder $E_{K'} = D$ gilt. Für den Index berechnen wir mit Satz 1.30 nun $\mathrm{inv}_{v_j}(F_{v_j} \otimes D) = 1$ für $v_i \in S(F)$ mit $v_i | p$. Da F total-imaginär ist, erhalten wir $d = 1$, d.h. also $E_{K'} \cong M_2(F')$, $r = 2$ und $\dim A_{K'} = 1$.

Nun bestimmen wir eine zyklische Galoiserweiterung E/F'. Das Zentrum $F = \mathbb{Q}(\pi_K) \subseteq E_{K'}$ enthält F' als Teilkörper mit $[F : F'] = \mathrm{Deg}(E_{K'}) = 2$. Wir erhalten $F = F'(\beta)$ mit β Nullstelle des irreduziblen Polynoms $f(t) = t^2 - \pi_{K'} \in F'[t]$. Damit haben wir ein geeignetes E mit $G(F/F') = \langle\sigma\rangle$ bestimmt und wir setzen $E := F$. Aus

$$N_{E/F'}\left(\tfrac{(\beta^2-5)\beta+3(3-\beta^2)}{12}\right) = -1$$

ersehen wir $\mathrm{ord}(-1) = 1 = \mathrm{Ind}(E_{K'})$ in ${F'}^{\times}/N_{E/F'}(E^{\times})$. Damit wissen wir, dass $E_{K'} \cong (E, \sigma, -1)$ gilt. Für die dem Element β entsprechende Korrespondenz B können wir $B = \langle X - x^p,\ Y - y^p\rangle$ wählen. Algorithmus 8 findet für $u \in (E, \sigma - 1)$ mit $u^2 = -1$ die Korrespondenz $U = \langle X + x + 1,\ Y + \alpha^6 y\rangle$. Zur Verifikation berechnen wir mit Algorithmus 1 dann $U^2 = \langle X + 2x,\ Y + y\rangle = -D$ und $UB = -BU$, wobei $D = \langle X + 2x, Y + 2y\rangle$ hier die Einheitskorrespondenz bezeichnen soll.

Die Algebra $(E, \sigma, -1)$ ist eine Quaternionenalgebra über F' mit der F'-Basis $(1, \pi, u, \pi u)$ und den Relationen $\pi^2 = \pi_{K'}$, $u^2 = -1$ und $u^{-1}\pi u = -\pi$. Wir erhalten nun folgende $\mathbb{Z}$-Ordnung $\mathfrak{D} \subseteq \mathrm{End}_{K'}(A^2_{K'})$ mit der $\mathbb{Z}$-Basis

$$\Big\langle 1, \pi, \tfrac{\beta^2+1}{2}, \tfrac{3(\beta^2+3)+(\beta^2+7)\pi}{12}, u, u\pi, \tfrac{(\beta^2+1)u}{2}, \tfrac{3(\beta^2+3)u-(\beta^2+7)\pi u}{12}\Big\rangle$$

sowie der Diskriminante $\mathrm{disc}\,\mathfrak{D} = 4$. Aus $h_{F'} = 1$ folgt, dass es in $(E, \sigma, -1)$ nur eine Konjugationsklasse gibt. Eine Maximalordnung $\mathcal{O}$ von $(E, \sigma, -1)$ ist durch die $\mathbb{Z}$-Basis

$$\Big\langle 1, \tfrac{\beta^2+1}{2}, 3+\pi, \tfrac{(3+\pi)(\beta^2+7)}{12}, 1+u, \tfrac{(\beta^2+3)(1+u)}{4}, \tfrac{3+\pi+3u+\pi u}{2}, \tfrac{(\beta^2+1)(3+\pi+3u+\pi u)}{12}\Big\rangle$$

mit $\operatorname{disc}\mathcal{O} = 1$ gegeben. Algorithmus 8 berechnet nun für das Element

$$\gamma := \tfrac{\beta^2+1+2\pi+(\beta^2+1)u-2\pi u}{4} \notin \mathfrak{D}$$

die Korrespondenz

$$\Big\langle X^2 + \tfrac{\alpha^2x^4+\alpha^2x^3+\alpha^6x^2+x+\alpha^5}{x+1}X + \tfrac{(2x^5+\alpha^6x^4+\alpha^6x^3+\alpha^2x^2+x+\alpha^7)}{(x+1)},$$
$$Y + \tfrac{y(\alpha x^4+\alpha^5x^2+\alpha^5x+\alpha)}{x^2+2x+1}X + \tfrac{y(\alpha^3x^5+2x^4+\alpha^7x^3+\alpha^6x^2+\alpha x+\alpha^5)}{x^2+2x+1}\Big\rangle.$$

Die Ordnung $\mathfrak{D}' := \mathfrak{D}[\gamma]$ ist maximal, es gilt sogar $\mathfrak{D}' = \mathcal{O}$, und somit ist $\mathfrak{D}'$ der volle Endomorphismenring von $A^2_{K'}$.

5.2.3 Beispiel zur Berechnung des Selbstschnittes

Wir wollen nun noch einen genaueren Blick auf die Berechnung der Schnittzahlen in (5.8) werfen. In den Eingängen der Korrespondenzpaarung ist hierbei der Divisor im rechten Eingang immer von der Form F^j mit $j = 0, 1, 2, 3$. Die Divisoren D und F^j genügen aber den Bedingungen von Lemma 3.5, denn zum Einen sind diese sämtlich vom Grad eins, daher können wir nach Lemma 2.17 den Restidealsatz anwenden, wenn die Divisoren F^j regulär bezüglich einem $p \in \mathbb{P}_{F_2/K}$ vom Grad eins sind. Andererseits besitzt der endliche Teil jeweils eine $F_2[x_1]$-Basis

$$F_0^j = \langle X - x^{p^j},\ Y - y^{p^j}\rangle, \quad (j = 0, 1, 2, 3)\ ,$$

weil $[L : F_2(x_1)] = 2$ ist. Daher sind die Divisoren F^j regulär für jedes $p \neq p_\infty$, also für alle Primdivisoren von F_2/K, welche keine Polstellen von x_2 sind, was gleichbedeutend damit ist, dass Nullstellen von x_2 auf Nullstellen von x_2 abgebildet werden. Außerdem erhalten wir mittels des F_2-Isomorphismuses $\mu : L/F_2 \longrightarrow L/F_2, \quad (X, Y) \longmapsto (Z, V)$ mit $Z = \frac{1}{X}$ und $V = \frac{Y}{X^3}$

$$\mu(F^j)_0 = \left\langle Z - \left(\tfrac{1}{x_2}\right)^{p^j},\ V - \left(\tfrac{y}{x^3}\right)^{p^j}\right\rangle.$$

Daraus ersehen wir aber, dass die $\mu(F^j)_0$ bezüglich p_∞ ganz sind, d.h. also Polstellen von x_2 werden wieder auf Polstellen abgebildet. Somit brauchen wir nur die Schnittmultiplizität auf $S_1 \cup S_4 = \mathcal{O}_{F_1} \otimes_K \mathcal{O}_{F_2} \cup \mathcal{O}_{F_{1,\infty}} \otimes_K \mathcal{O}_{F_{2,\infty}}$ mittels $s_1 + s_4 - s_{14}$ zu berechnen. Insgesamt erhalten wir für Q dann $Q.D = 9 + 11 - 9 = 11, \quad Q.F = 9 + 11 - 9 = 11$, $Q.F^2 = 41 + 43 - 41 = 43$, und $Q.F^3 = 57 + 59 - 57 = 59$. Für R erhalten wir $R.D = 3 + 3 - 3 = 3, \quad R.F = 3 + 3 - 3 = 3$, $R.F^2 = 11 + 11 - 11 = 11$ und $R.F^3 = 43 + 43 - 43 = 43$.

Wir wollen nun zuletzt noch zeigen, wie wir den Selbstschnitt anhand eines einfachen Beispiels berechnen können. Wir wissen bereits aus Lemma

2.24, dass $D.D = 2 - 2g = -2$ sein muss. Mit dem schwachen Approximationssatz berechnen wir ein $F \in L/F_2$ mit

$$F = \frac{1}{X+2x}\left(\frac{2yY}{(x^5+x^4+x^3+2x^2+x)} + \frac{X(x^5+2x^3+2x^2+2x+1)+(2x^5+2x^4+2x+1)}{(x^5+x^4+x^3+2x^2+x)+(x^4+x^3+x^2+2x+1)}\right)$$

und $\nu_D(F) = -1$. Der Hauptdivisor $(F) \in \mathcal{P}_{L/F_2}$ hat dann die Gestalt $(F) = A - (3P_{\infty,1} + D)$, wobei A effektiv mit $D \notin \mathrm{supp}(A)$ ist. Für die Grade von A erhalten wir Grad $\deg_{L/F_2}(A) = 4$ und $\deg_{L/F_2}(A^\star) = 10$. Die den auf der Fläche entsprechenden Divisoren bezeichnen wir wieder gleich, außer dass $D = \Delta_{X_1}$ ist. Auf der Fläche besitzt nun (F) die Gestalt $(F) = A - (3P_{\infty,1} + 9P_{\infty,2} + \Delta_{X_1})$, da ja (F) als Hauptdivisor der Fläche sowohl bezüglich d_1 als auch d_2 den Grad null haben muss. Aus $d_1(F) = 10 - (9 + 1) = 0$ und $d_2(F) = 4 - (3 + 1) = 0$ sehen wir, dass unser so definiertes (F) ein Hauptdivisor ist. Den Schnitt $\Delta_{X_1}.A$ können wir aber mit unserem Algorithmus 4 berechnen, da Δ_{X_1} und A keine gemeinsame Komponente haben und dieser nichts Anderes ist als $D.A$. Wir erhalten dann $\Delta_{X_1}.A = 10$. Schließlich haben wir $\Delta_{X_1} + (F) = A - (3P_{\infty,1} - 9P_{\infty,2})$, und mit Hilfe von Lemma 2.22 erhalten wir

$$\Delta_{X_1}.(\Delta_{X_1} + (F)) = \Delta_{X_1}.A - \Delta_{X_1}.3P_{\infty,1} - \Delta_{X_1}.9P_{\infty,2} = 10 - 3 - 9 = -2,$$

d.h. also $\Delta_{X_1}.\Delta_{X_1} = -2$, was ja auch, wie wir bereits wissen, das Ergebnis sein soll.

5.3 Geschlecht $g = 3$

5.3.1 Ein hyperelliptischer Fall

Wir betrachten die Funktionenkörper F_i/K mit $F_i = K(x_i, y_i)$ und $f_i(x_i, y_i) = y_i^2 - (x_i^7 + 5x^4 + x + 4)$ mit $K = \mathbb{F}_7$. Für das irreduzible charakteristische Polynom des Frobenius berechnen wir

$$f_{\pi_K}(t) = t^6 + 4t^5 + 17t^4 + 48t^3 + 119t^2 + 196t + 343 \in \mathbb{Z}[t]$$

und $F = \mathbb{Q}(\pi_K)$. Mit (1.17) wissen wir, dass mit $E_K := \mathrm{End}_K^0(J_{X_2})$ und $[E_K : \mathbb{Q}] = 6$ dann $E_K = F$ gilt, d.h. also E_K ist ein Körper. Wir wollen wieder $\pi_K = \pi$ und $X := x_1, Y := y_1, x := x_2$ und $y := y_2$ schreiben. Als Erstes berechnen wir $\Omega^{(0)} = \{\omega_i^{(0)} \mid i = 1, ..., 6\}$ mit (in der selben Reihenfolge)

$$\Omega^{(0)} = \left\{1, \pi, \frac{1+\pi^2}{2}, \frac{\pi+\pi^3}{2}, \frac{21+20\pi+10\pi^2+4\pi^3+\pi^4}{28}, \frac{21\pi+48\pi^2+66\pi^3+4\pi^4+\pi^5}{196}\right\}$$

und $\Delta^{(0)} := \{\delta_i^{(0)} \mid i = 1, .., 6\}$ mit $\Delta^{(0)} = \{1, \pi, 2\omega_3^{(0)}, 2\omega_4^{(0)}, 28\omega_5^{(0)}, 196\omega_6^{(0)}\}$ (wieder in der selben Reihenfolge) sowie $m_{11} = m_{22} = 1, m_{33} = m_{44} =$

$2, m_{55} = 28, m_{66} = 196$. Dann berechnen wir

$$\Lambda^{(0)} = \{0\}\times\{0\}\times\{-1,...,-1\}\times\{-1,...,-1\}\times\{-27,...,27\}\times\{-195,...,195\}.$$

Für das Element $\underline{\lambda} = (0,0,0,0,1,0)^t$ erhalten wir die Korrespondenz $A := D + B$ mit $B =$

$$\left\langle X^2 + X(5x+3) + (x^2+3x+4), \quad Y + 6y \right\rangle ,$$

und es gilt $\mathbb{Z}[\pi][\alpha] = \mathcal{O}_F$, d.h. der Endomorphismenring ist isomorph zur Maximalordnung von F.

5.3.2 Ein nicht-hyperelliptischer Fall

Wir betrachten nun noch ein nicht-hyperelliptisches Beispiel. Die Funktionenkörper F_i/K mit $F_i = K(x_i, y_i)$ und $f_i(x_i, y_i) = y_i^4 + (x_i+1)y_i + x_i^3 + 2$ mit $K = \mathbb{F}_3$ haben das Geschlecht $g_{K_i} = 3$, sind aber nicht hyperelliptisch. Für das irreduzible charakteristische Polynom des Frobenius berechnen wir

$$f_{\pi_K}(t) = t^6 - t^5 - 9t + 27 \in \mathbb{Z}[t]$$

und $F = \mathbb{Q}(\pi_K)$. Mit (1.17) wissen wir, dass mit $E_K := \mathrm{End}_K^0(J_{X_2})$ und $[E_K : \mathbb{Q}] = 6$ dann $E_K = F$ gilt, d.h. also E_K ist ein Körper. Wir wollen wieder $\pi_K = \pi$ und $X := x_1, Y := y_1, x := x_2$ und $y := y_2$ schreiben. Als Erstes berechnen wir

$$\Omega^{(0)} = \left\{1, \pi, \pi^2, \tfrac{2\pi^2+\pi^3}{3}, \tfrac{\pi^4+2\pi^2}{3}, \tfrac{6\pi^2+2\pi^4+\pi^5}{9}\right\}$$

und

$$\Delta^{(0)} = \left\{1, \pi,\ \pi^2,\ 2\pi^2+\pi^3,\ \pi^4+2\pi^2,\ 6\pi^2+2\pi^4+\pi^5\right\}$$

mit $m_{11} = m_{22} = m_{33} = 1, m_{44} = m_{55} = 3, m_{66} = 9$. Dann berechnen wir

$$\Delta^{(0)} = \{0\}\times\{0\}\times\{0\}\times\{-2,...,2\}\times\{-2,...,2\}\times\{-8,...,8\}.$$

Für das Element $\underline{\lambda} = (0,0,0,0,-1,1)^t$ berechnet Algorithmus 7 einen Aufstieg, d.h. also dass $\alpha := -\omega_5^{(0)} + \omega_6^{(0)} = \frac{\pi^5-\pi^4}{9}$ einer Korrespondenz entspricht. Aus Darstellungsgründen berechnen wir die dem Element $\beta := \alpha - 1$

entsprechende Korrespondenz $B \in \mathcal{D}_{L/F_2}$, nämlich $B_0 =$

$$\Big\langle X^3 + \tfrac{2y^2}{x^2+x+1}X^2 + \Big(\tfrac{y^3}{x^2+x+1} + \tfrac{y^2}{x^2+x+1} + \tfrac{y(2x+2)}{x^4+2x^3+2x+1} + \tfrac{2}{x+2}\Big)X + \\ + \tfrac{y^3}{x^2+x+1} + \tfrac{y^2(2x^2+x+1)}{x^4+2x^3+2x+1} + \tfrac{y(x^3+2x^2+x)}{x^4+2x^3+2x+1} + \tfrac{2x^2+x+2}{x+2},$$
$$Y + \Big(\tfrac{y^3}{x^6+x^3+2} + \tfrac{y^2(2x^2+2x+2)}{x^6+x^3+2} + \tfrac{y(x^4+2x^3+2x+1)}{x^6+x^3+2} + \tfrac{x+2}{x^6+x^3+2}\Big)X^2 + \\ \Big(\tfrac{2y^3}{x^4+2x^3+2x^2+x+1} + \tfrac{y^2(2x^4+x^3+2x^2+2)}{x^6+2x^4+2x^3+x^2+2x+1} + \\ + \tfrac{y(2x^2+2x)}{x^4+2x^3+2x^2+x+1} + \tfrac{2x+1}{x^4+2x^3+2x^2+x+1}\Big)X + \\ \Big(\tfrac{y^3(x^6+2x^4+2x^3+x^2+2x+2)}{x^8+x^7+x^6+x^5+x^4+x^3+2x^2+2x+2} + \tfrac{y^2(2x^6+2x^4+x+2)}{x^8+x^7+x^6+x^5+x^4+x^3+2x^2+2x+2} + \\ \tfrac{y(x^4+2x^3+2x+2)}{x^6+x^3+2} + \tfrac{2x^3+x}{x^6+x^3+2}\Big)\Big\rangle$$

in 2-Element-Darstellung. Dann berechnen wir

$$\Delta^{(1)} = \Big\{1, \pi, \pi^2, 2\pi^2+\pi^3, 2\pi^2+\pi^4, \tfrac{6\pi^3+2\pi^4+\pi^5}{3}\Big\}$$

$$\Omega^{(1)} = \Big\{1, \pi, \pi^2, \tfrac{2\pi^2+\pi^3}{3}, \tfrac{2\pi^2+\pi^4}{3}, \tfrac{6\pi^3+2\pi^4+\pi^5}{9}\Big\}.$$

Algorithmus 7 findet keinen weiteren Aufstieg, und damit ist $\mathrm{End}_K(J_{X_2}) \cong \mathcal{O} := \langle \Delta^{(1)} \rangle$, wobei $[\mathcal{O}_F : \mathcal{O}] = 3$ ist.

5.4 Tabelle mit Beispielen

In diesem Abschnitt wollen wir Berechnungen von Endomorphismenringen samt Laufzeit aufführen. Wir wollen für den Funktionenkörper F_2 einfach nur F schreiben, und der Konstantenkörper sei mit K bezeichnet. Dabei soll $\max \mathcal{S}$ die während der Berechnung des Endomorphismenringes maximal aufgetretene Anzahl der notwendigen Stellen vom Grad eins sein. Mit $\max s$ ist die größte obere Schranke für die Grade der in der Norm der berechneten Korrespondenzen auftretenden Polynome in x_2 bezeichnet. Analog dazu ist $\max x_2$ der maximale Grad der Polynome in x_2, welche bei den Normen der berechneten Korrespondenzen auftreten. Die benötigte Laufzeit T ist in Sekunden angegeben. Zusätzlich werden noch unter Anderem die berechneten Korrespondenzen als algebraische Elemente angegeben. Mit $\mathcal{O}$ haben wir den Endomorphismenring bezeichnet. Der Algorithmus für den kommutativen Fall wurde noch dahingehend optimiert, dass für die positiv definite Form

$$\phi : \mathrm{End}^0_{\mathbb{F}_q}(J_{X_2}) \times \mathrm{End}^0_{\mathbb{F}_q}(J_{X_2}) \longrightarrow \mathbb{Q}^{>0},$$

$$(\alpha, \alpha^\star) \longmapsto \mathrm{Tr}_{\mathrm{End}^0_{\mathbb{F}_q}(J_{X_2})/\mathbb{Q}}(\alpha\alpha^\star)$$

eine geeignete positive definiete Matrix M berechnet wurde mit der Eigenschaft

$$\phi(\alpha, \alpha^\star) = x^t M x,$$

wenn $\alpha = \sum_{i=1}^n x_i b_i$, $x = (x_1, ..., x_n) \in \mathbb{Q}^n$ und b_i eine fest gewählte $\mathbb{Q}$-Basis von $\mathrm{End}^0_{\mathbb{F}_q}(J_{X_2})$ ist. Mittels einer LLL-Reduktion suchen wir dann diejenigen ganzen Elemente α aus $\mathrm{End}_{\mathbb{F}_q}(J_{X_2})$ und geeignete Vielfache von diesen, für die $\phi(\alpha, \alpha^\star)$ minimal ist, und testen zuerst diese Elemente durch. Dann geht der Algorithmus den in dieser Arbeit beschriebenen Rechenweg durch. Die Berechnungen wurden mit dem Computeralgebrasystem Magma V2.14-14 auf einem Rechner mit einem Core-Duo-Prozessor mit 1998 MHz durchgeführt.

1.) $K = \mathbb{F}_{271}$ $F = y^2 - (x^3 + 70x + 137)$	$[\mathcal{O}_F : \mathcal{O}] = 3$ $g_{F/K} = 1$ $[K' : K] = 3$
$h_{F/K'} = 2^2 \cdot 3^4 \cdot 7 \cdot 8779$	$\pm\frac{\pi - 13}{2}$
$\max \mathcal{S} = 1652 \quad \max s = 90$	$\max \deg x_2 = 45 \quad T = 153.9$

2.) $K = \mathbb{F}_{53}$ $F = y^2 - (x^3 + x + 2)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 1$ $[K' : K] = 3$
$h_{F/K'} = 2^4 \cdot 3^2 \cdot 1039$	$\pm\frac{\pi-1}{4}$
$\max \mathcal{S} = 20 \quad \max s = 6$	$\max \deg x_2 = 3 \quad T = 0.13$

3.) $K = \mathbb{F}_{31}$ $F = y^2 - (x^3 + x + 2)$	$\mathcal{O} = \mathbb{Z}[\pi]$ $g_{F/K} = 1$ $[K' : K] = 3$
$h_{F/K'} = 2^3 \cdot 3^3 \cdot 139$	
$\max \mathcal{S} = 62$	$T = 0.54$

4.) $K = \mathbb{F}_{11}$ $F = y^2 - (x^3 + x + 2)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 1$ $[K' : K] = 3$
$h_{F/K'} = 2^4 \cdot 79$	$\pm\frac{\pi+1}{2}$
$\max \mathcal{S} = 14 \quad \max s = 4$	$\max \deg x_2 = 2 \quad T = 0.10$

5.) $K = \mathbb{F}_{31}$ $F = y^2 - (x^5 + 1)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 2$ $[K' : K] = 3$
$h_{F/K'} = 2^4 \cdot 71 \cdot 778201$	$\pm\frac{3\pi^3+43\pi^2-327\pi-279}{2728}$
$\max \mathcal{S} = 19 \quad \max s = 6$	$\max \deg x_2 = 1 \quad T = 0.48$

6.) $K = \mathbb{F}_{11}$ $F = y^2 + (x^5 + x^2 + x + 1)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 2$ $[K' : K] = 5$
$h_{F/K'} = 2^5 \cdot 3 \cdot 41 \cdot 6654971$	$\pm\frac{\pi^3+8\pi^2-12\pi+33}{22}, \pm\frac{-\pi^3+3\pi^2-10\pi+22}{11}$
$\max \mathcal{S} = 295 \quad \max s = 90$	$\max \deg x_2 = 44 \quad T = 21.49$

7.) $K = \mathbb{F}_{61}$ $F = y^2 - (x^5 + x^4 + x^3 + 2x^2 + x)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 2$ $[K' : K] = 3$
$h_{F/K'} = 2^4 \cdot 13^2 \cdot 19 \cdot 937 \cdot 1069$	$\pm\frac{\pi^3+2\pi^2+45\pi}{122}$, $\pm\frac{\pi^3-59\pi^2+45\pi-3111}{244}$
$\max \mathcal{S} = 751$ $\max s = 250$	$\max \deg x_2 = 122$ $T = 1121.81$

8.) $K = \mathbb{F}_{23}$ $F = y^2 - (x^5 + x^4 + x^3 + 2x^2 + x)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 2$ $[K' : K] = 3$
$h_{F/K'} = 2^3 \cdot 47 \cdot 691 \cdot 159544531$	$\pm\frac{-\pi^3+8\pi^2-45\pi+92}{46}$, $\pm\frac{3\pi^3-\pi^2+45\pi-207}{92}$
$\max \mathcal{S} = 121$ $\max s = 40$	$\max \deg x_2 = 19$ $T = 6.3$

9.) $K = \mathbb{F}_{11}$ $F = y^2 - (x^7 + 1)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 3$ $[K' : K] = 5$
$h_{F/K'} = 2^3 \cdot 7 \cdot 23 \cdot 71 \cdot 45678945211$	$\pm\frac{\pi^3-11}{22}$, $\pm\frac{-\pi^5+44\pi^2}{121}$
$\max \mathcal{S} = 198$ $\max s = 66$	$\max \deg x_2 = 23$ $T = 11.9$

10.) $K = \mathbb{F}_{29}$ $F = y^2 - (x^7 + 1)$	$\mathcal{O}_F = \mathcal{O}$ $g_{F/K} = 3$ $[K' : K] = 5$
$h_{F/K'} = 2^6 \cdot 7 \cdot 43 \cdot 17875327$	$\pm\frac{7\pi^5-129\pi^4-410\pi^3+2502\pi^2+1827\pi-91669}{53824}$
$\max \mathcal{S} = 102$ $\max s = 34$	$\max \deg x_2 = 1$ $T = 27.59$

11.) $K = \mathbb{F}_3$ $F = y^4 + (x+1)y + x^3 + 2$	$[\mathcal{O}_F : \mathcal{O}] = 3$ $g_{F/K} = 3$ $[K' : K] = 11$
$h_{F/K'} = 2 \cdot 3^2 \cdot 312304602522287$	$\pm\frac{\pi^5-\pi^4-9}{9}$
$\max \mathcal{S} = 460$ $\max s = 36$	$\max \deg x_2 = 4$ $T = 320.31$

Es folgen nun einige nicht-kommutative Beispiele für Geschlecht eins und zwei. Der Algorithmus geht hier davon aus, dass bereits eine $\mathbb{Q}$-Basis der

Endomorphismenalgebra berechnet wurde, welche aus Endomorphismen besteht. Die Kurven sind so gewählt, dass wir neben dem Frobenius π von $\mathrm{End}_{\mathbb{F}_p}(J_{X_2})$ noch mindestens einen nicht-trivialen Automorphismus des Funktionenkörpers $F/\mathbb{F}_{p^2}$ erhalten. Dieser induziert eine nicht-triviale Korrespondenz, die nicht mit π kommutiert. Bezeichnet u das zu dieser Korrespondenz dazugehörige Element in der Endomorphismenalgebra, so wird π so gewählt, dass $\pi u = -u\pi$ ist. Im Fall, dass das Geschlecht zwei ist, haben wir zuerst den Endomorphismenring über $\mathbb{F}_p$ berechnet. Die Basis des Endomorphismenrings haben wir benutzt, um eine $\mathbb{Z}$-Basis einer Ordnung des Endomorphismenrings mit möglichst kleiner Diskriminante zu erhalten. Von dieser Ordnung aus starten wir unsere Suche nach einem möglichen Aufstieg des bereits berechneten Endomorphismenrings.

12.) $K = \mathbb{F}_{3^2}$ $F = y^2 - (x^3 + x)$	$\mathbb{Q}_{3,\infty}$ $g_{F/K} = 1$ $[K' : K] = 3$
$h_{F/K'} = 2^4 \cdot 7^2$	$\mathcal{O} = \langle 1, \frac{1+\pi}{2}, u, \frac{u+\pi u}{2} \rangle$ $(\pi, u) = (-3, -1)$
$\max \mathcal{S} = 26 \quad \max s = 8$	$\max \deg x_2 = 2 \quad T = 6.63$

13.) $K = \mathbb{F}_{19^2}$ $F = y^2 - (x^3 + x)$	$\mathbb{Q}_{19,\infty}$ $g_{F/K} = 1$ $[K' : K] = 3$
$h_{F/K'} = 2^4 \cdot 5^2 \cdot 7^6$	$\mathcal{O} = \langle 1, u, -\frac{1+\pi}{2}, -\frac{u+\pi u}{2} \rangle$ $(\pi, u) = (-19, -1)$
$\max \mathcal{S} = 122 \quad \max s = 40$	$\max \deg x_2 = 10 \quad T = 62.67$

14.) $K = \mathbb{F}_{11^2}$ $F = y^2 + y - x^3$	$\mathbb{Q}_{11,\infty}$ $g_{F/K} = 1$ $[K' : K] = 3$
$h_{F/K'} = 2^4 \cdot 3^4 \cdot 37^2$	$\mathcal{O} = \langle 1, \frac{-u+\pi u}{6}, u, -\frac{1+\pi}{2} \rangle_{\mathbb{Z}}$ $(\pi, u) = (-11, -3)$
$\max \mathcal{S} = 290 \quad \max s = 96$	$\max \deg x_2 = 48 \quad T = 166.23$

15.) $K = \mathbb{F}_{3^2}$ $F = y^2 + 2x^5 + 2x^4 + 2x^3 + x^2 + 2x$	$\mathrm{End}^0_K(J_{X_2}) \cong M_2(\mathbb{Q}(\pi_K))$ $g_{F/K} = 2$ $[K' : K] = 5$
$h_{F/K'} = 2^6 \cdot 7321^2$	$\mathcal{O}$ ist eine Maximalordnung $-\frac{1+\pi+u-\pi u}{2}, -\frac{(\pi^2+3)+(pi^2+3)u}{4}$ $(\pi^2_{\mathbb{F}_3}, -1)$
$\max \mathcal{S} = 37 \quad \max s = 12$	$\max \deg x_2 = 3 \quad T = 29.54$

16.) $K = \mathbb{F}_{5^2}$ $F = y^2 + (x^5 + x^4 + x^3 + 4x + 2)$	$\mathrm{End}^0_K(J_{X_2}) \cong M_2(\mathbb{Q}(\pi_K))$ $g_{F/K} = 2$ $[K' : K] = 5$
$h_{F/K'} = 2^6 \cdot 3^2 \cdot 11^4 \cdot 3361^2$	$\mathcal{O}$ ist eine Maximalordnung $\frac{\pi^2+1+4\pi+2\pi u}{4}$ $(\pi^2_{\mathbb{F}_3}, 1)$
$\max \mathcal{S} = 163 \quad \max s = 32$	$\max \deg x_2 = 10 \quad T = ca.3600$

Zusammenfassung

Seien F_1/K und F_2/K zwei algebraisch unabhängige und reguläre Funktionenkörper über dem endlichen Körper K. Ferner bezeichne X_i/K jeweils die dazugehörige projektive, irreduzible und reduzierte Kurve vom Geschlecht g_{X_i}. Wir konstruieren wichtige Algorithmen für die Arithmetik von Korrespondenzen aus L/F_2 zwischen den Funktionenkörpern F_1/K und F_2/K, deren Wirkung auf den Jacobischen J_{X_i} der Kurven X_i/K sowie eine Schnitt- und Korrespondenzpaarung. Mit Hilfe dieser grundlegenden Algorithmen können wir die Korrespondenzen als Homomorphismen zwischen den Jacobischen J_{X_2} und J_{X_1} operieren lassen. Außerdem lässt sich im Fall, dass die Korrespondenzen Endomorphismen auf der Jacobischen J_{X_2} induzieren, das charakteristische Polynom des der Korrespondenz entsprechenden Endomorphismus mit der Korrespondenzpaarung bestimmen.

Im Falle, dass die Funktionenkörper F_1 und F_2 isomorph über K sind, induzieren die Korrespondenzen Endomorphismen von J_{X_2}. Das Hauptergebnis ist ein Verfahren, mit dem wir den Endomorphismenring einer beliebigen Kurve über einem endlichen Körper mit irreduzibler Jacobischen berechnen können. Wir beweisen, dass unter gewissen Annahmen in jeder Korrespondenzklasse $[A]_C$ eine effektive Korrespondenz $C(A)$ vom Grad $\leq g_{X_2}$ mit der Eigenschaft $C(A)(p_\infty) = lp_\infty + (f)$ existiert, welche innerhalb der Korrespondenzklasse mit diesen Eigenschaften eindeutig ist. Bezeichne $E_K := \mathrm{End}_K^0(J_{X_2})$ die Endomorphismenalgebra von J_{X_2} über K und $\alpha \in E_K$ das der Korrespondenz $C(A)$ entsprechende Element. Wir beweisen, dass sich die Grade der in der Norm von $C(A)_0$ auftretenden Polynome in x_2 durch die Spur mittels der Größe $\mathrm{Tr}_{E_K/\mathbb{Q}}(\alpha\alpha^\star)(n/2)$ beschränken lassen, wobei $\alpha^\star$ der Rosati von α und $n = [F_2 : K(x_2)]$ ist. Haben wir mit Hilfe dieser oberen Schranke genügend viele geeignete Stellen vom Grad eins bestimmt, so können wir die Norm von $C(A)_0$ interpolieren. Dazu beweisen wir ein Kriterium mit dem wir feststellen können, ob für eine Stelle $p \in \mathcal{D}_{F_2/K}$ vom Grad und eine Zerlegung $C(A) = \sum e_i P_i$ mit $P_i \in \mathbb{P}_{F_2/K}$ jeweils p-reguläre Basen von $P_{i,0}$ existieren, so dass $C(A)(p) = \sum e_i \overline{P_i}^p$ gilt. Ist das Element α kein Endomorphismus, so existiert keine Lösung beim Versuch, die Norm zu interpolieren. Damit sind wir in der Lage, den Endomorphismenring zu bestimmen.

Den Abschluss bilden einige Beispiele. Wir zeigen, wie wir mit Hilfe der in dieser Arbeit entwickelten Algorithmen sowohl im Fall eines kommutativen Endomorphismenrings wie auch im nicht-kommutativen Fall den Endomorphismenring berechnen können.

Index

Literaturverzeichnis

[Art67] Artin, E.: *Algebraic Numbers and Algebraic Functions.* Gordon and Breach, 1967.

[Bel07] Belabas, van Hoej et al.: *Factoring Polynomials Over Global Fields.* to appear in Journal de Théorie des Nombres de Bordeaux, 2007.

[Coh93] Cohen, H.: *A Course in Computational Algebraic Number Theory.* Springer-Verlag, 1993.

[Coh06] Cohen,H., Frey,G.: *Handbook of Elliptic And Hyperelliptic Curve Cryptography.* Chapman and Hall, 2006.

[Cox05] Cox, D. A., Little, J., O'Shea, D.: *Using Algebraic Geometry.* Springer, 2005.

[Deu35] Deuring, M.: *Algebren, Zweite Auflage.* Springer Verlag, 1935.

[Deu37] Deuring, M.: *Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper I.* Crelle Journal, 177:161–191, 1937.

[Deu40] Deuring, M.: *Arithmetische Theorie der Korrespondenzen algebraischer Funktionenkörper II.* Crelle Journal, 182:25–36, 1940.

[Deu41] Deuring, M.: *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper.* Abh. Math. Semin. Hansische Univ., 14:197–272, 1941.

[Deu73] Deuring, M.: *Lectures on the Theory of Algebraic Functions of One Variable.* Springer Verlag, 1973.

[Die05] Diem, C.: *Index Calculus in Class Groups of Plane Curves of Small Degree.* Preprint, 2005.

[Eic37] Eichler, M.: *Bestimmung der Idealklassen in gewissen normalen einfachen Algebren.* Journal f. die reine angewandte Mathematik, 176:192–202, 1937.

[Eic55] Eichler, M.: *Zur Theorie der Quaternionen-Algebren.* Journal f. die reine angewandte Mathematik, 195:127–151, 1955.

[Eic63] Eichler, M.: *Einführung in die Theorie der algebraischen Zahlen und Funktionen.* Birkhäuser Verlag Basel und Stuttgart, 1963.

[Fre07] Freeman, D., Lauter, K.: *Computing Endomorphism Rings of Jacobians of Genus 2 Curves Over Finite Fields.* Preprint, 2007.

[Fri00] Friedrichs, C.: *Berechnung von Maximalordnungen über Dedekind-ringen.* Doktorarbeit, TU Berlin, 2000.

[Gat99] Gathen, J. von zur, Gerhard, J.: *Modern Computer Algebra.* Cambridge University Press, 1999.

[Gee07] Geer, G. van der, Moonen, B.: *Abelian Varieties.* To appear, 2007.

[Har77] Hartshorne, R.: *Algebraic Geometry.* Springer Verlag, 1977.

[Has32] Hasse, H.: *Theory of Cyclic Algebras Over An Algebraic Number Field.* Transactions of the American Mathematical Society, No.1, 34:171–214, 1932.

[Hes99] Hess, F.: *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern.* Doktorarbeit, TU Berlin, 1999.

[Hes02] Hess, F.: *Computing Riemann-Roch spaces in algebraic function fields and related topics.* J. Symbolic Comp., 33:425–445, 2002.

[Hes06] Hess, F.: *Algebra I + II, Vorlesungsskript.* TU-Berlin, 2006.

[Hin91] Hindry, M., Silvermann, J.H: *Diophantine Geometry.* Springer, 1991.

[Irv03] Irving, R.: *Maximal Orders.* Oxford Science Publications, 2003.

[Kir05] Kirschmer, M.: *Konstruktive Idealtheorie in Quaternionenalgebren.* Diplomarbeit, Universität Ulm, 2005.

[Koh96] Kohel, D.: *Endomorphism rings of elliptic curves over finite fields.* Phd, University of California, Berkley, 1996.

[Kux04] Kux, G.: *Construction of algebraic correspondences between hyperelliptic function fields using Deuring's theory.* Doktorarbeit, Universität Kaiserslautern, 2004.

[Lau02] Lauder, A.G.B, Wan, D.: *Counting Points On Varieties Over Finite Fields Of Small Characteristic.* Preprint, 2002.

[Mil86] Milne, J.S.: *Jacobian Varieties.* Springer, 1986.

[Mil91] Milne, J.S.: *Abelian Varieties.* Univeristy of Michigan, 1991.

[Mil98] Milne, J.S.: *Abelian Varieties.* Lecture notes, 1998.

[Mil05] Milne, J.S.: *Algebraic Geometry.* Taiaroa Publishing, 2005.

[Mil08] Milne, J.S.: *Class Field Theory.* Univeristy of Michigan, 2008.

[Mum70] Mumford, D.: *Abelian Varieties.* Oxford Univeristy Press VIII, 1970.

[Oor07] Oort, F.: *Abelian Varieties over Finite Fields.* Summer school in Göttingen, 2007.

[Pie82] Pierce, R.S.: *Associative Algebras.* Springer Verlag, 1982.

[Poh89] Pohst, M.E., Zassenhaus, H.: *Algorithmic Algebraic Number Theory.* Encyclopaedia of mathematics and its applications. Cambridge University Press, 1989.

[Poh93] Pohst, M.E.: *Computational Algebraic Number Theory.* Birkauser, DMV Seminar, Band 21, 1993.

[Ros73] Rosen, M.: *The Asymptotic Behaviour of the Class Group of a Function Field over a Finite Field.* Archiv der Mathematik, 24:287–296, 1973.

[Sal06] Salvador, G.D.V.: *Topics in the theory of algebraic function fields.* Birkhäuser, 2006.

[Sha72] Shafarevich, I.R.: *Basic Alegbraic Geometry.* Springer, 1972.

[Sil86] Silverman, J.H.: *The Arithmetic of Elliptic Curves.* Springer Verlag, 1986.

[Smi05] Smith, B.: *Explicit Endomorphisms and Correspondences.* Phd, University of Sidney, 2005.

[Sti93] Stichtenoth, H.: *Algebraic Function Fields and Codes.* Springer Verlag, 1993.

[Tat66] Tate, J.: *Endomorphisms of Abelian Varieties over Finite Fields.* Inventiones math., 2:134–144, 1966.

[Tat69] Tate, J.: *Classes d' isogénie des variétés abéliennes sur un corps fini.* Séminaire N. Bourbaki, 352:95–110, 1968-1969.

[Ung05] Unger, A.: *Structure of Endomorphism Algebras of Abelian Varieties.* Number Theory Seminar 2005, 2005.

[Vél71] Vélu, J.: *Isogénies entre courbes elliptiques.* Comptes-Rendus de l' Académie des Sciences, Série I, 273:238–241, 1971.

[Ver03] Vercauteren, F.: *Computing zeta functions of curves over finite fields.* Phd, Katholieke Universiteit Leuven, 2003.

[Wat69] Waterhouse, W.C.: *Abelian Varieties over Finite Fields.* Annales Scientifiques de L' É.N.S., 4:521–560, 1969.

[Zar05] Zarhin, Y.G.: *Homomorphisms of abelian varieties.* Séminaires et Congrès, 11:189–215, 2005.