Einbettungen globaler Funktionenkörper

Diplomarbeit von Gerriet Möhlmann

April 2008

Betreuer:
Prof. Dr. Florian Heß
Technische Universität Berlin
Institut für Mathematik

Die selbstständige und eigenhändige Anfertigung versichere ich an Eides statt.

Unterschrift

Berlin, den 12. September 2008

Inhaltsverzeichnis

Einleitung

Die Frage, ob zwei Objekte isomorph sind, gehört zu den grundlegenden Problemstellungen der Mathematik. Ihr Schwierigkeitsgrad variiert von sehr leicht für Vektorräume bekannter endlicher Dimension bis unentscheidbar für Gruppen. In [Hes04] wird ein im Geschlecht und der Anzahl der arithmetrischen Operationen im Grundkörper polynomieller Algorithmus angegeben, der für zwei gegebene Funktionenkörper vom Geschlecht größer gleich zwei entscheidet, ob sie isomorph sind und falls ja alle Isomorphismen berechnet. Den Algorithmus von [Hes04] verallgemeinernd beschäftigt sich diese Arbeit mit dem Problem, alle Homomorphismen zwischen zwei globalen Funktionenkörpern vom Geschlecht größer gleich zwei zu konstruieren. Da Körperhomomorphismen immer injektiv sind, werden also alle Isomorphismen des einen Funktionenkörpers auf einen Unterkörper des anderen berechnet. Wir beschränken uns auf Funktionenkörper vom Geschlecht größer als eins, um die Existenz einer Schranke für den Grad des Bildes des einen Funktionenkörpers als Unterkörper des anderen sicher zu stellen. Ein Beispiel dafür, dass diese Schranke bei niedrigerem Geschlecht nicht existieren muss, stellen die Einbettungen $\phi_n : k(x) \longrightarrow k(x)$ mit $x \mapsto x^n$ eines rationalen Funktionenkörpers in sich selbst dar.

Die Arbeit gliedert sich wie folgt:
Das erste Kapitel liefert eine kurze Einführung zu Funktionenkörpern. Es wird ein notwendiges Kriterium für die Existenz von Einbettungen angegeben. Dafür werden einige Aussagen über das Verhalten von Stellen bei endlichen Erweiterungen gemacht. Außerdem wird bewiesen, dass es nur endlich viele separable Einbettungen geben kann.
Im zweiten Kapitel skizzieren wir den Isomorphiealgorithmus. Wir zeigen, wie man ihn auf das Berechnen der Einbettungen verallgemeinern kann und präsentieren die Idee und den Aufbau des Einbettungsalgorithmus.
Die fehlenden Details zum Einbettungsalgorithmus werden im dritten Kapitel gegeben. Wir zeigen, wie man holomorphe Ringe durch P-adische Vervollständigung mit Gittern identifizieren kann, um dann mit einem Reduktionsalgorithmus aus einer Einbettung gewisser Riemann-Roch-Räume eine Einbettung der Funktionenkörper zu berechnen. Wir geben weitere notwendige Kriterien für die Existenz von Einbettungen an und zeigen, dass diese insgesamt sogar hinreichend sind. Außerdem beweisen wir die Korrektheit der verwendeten Unteralgorithmen und vergleichen den Isomorphie- und den Einbettungsalgorithmus.
Im vierten Kapitel analysieren wir die Laufzeit des Algorithmus. Dazu untersuchen wir die Anzahl der zum Ermitteln der Einbettungen benötigten Rechnungen im Grundkörper in Abhängigkeit von charakteristischen Größen des Funktionenkörpers.

Im fünften Kapitel werden die Ergebnisse einiger Beispielberechnungen angegeben. Das sechste Kapitel präsentiert die Zusammenhänge zwischen über Funktionenkörpern definierten Kurven und Einbettungen von Funktionenkörpern. Daran anknüpfend wird eine alternative Möglichkeit angegeben, um Funktionenkörperhomomorphismen zu berechnen. Weiterhin zeigen wir, wie man Einbettungen, deren Bilder galoissche Unterkörper sind, konstruieren kann und geben einen kurzen Ausblick.

Kapitel 1

Grundlagen zu Funktionenkörpern

In diesem Abschnitt werden die für die Arbeit notwendigen theoretischen Grundlagen von Funktionenkörpern und Einbettungen bereitgestellt und einige Notationen vereinbart.

Definition 1.0.1. *Sei k ein Körper. Eine Körpererweiterung F von k wird als* algebraischer Funktionenkörper in einer Variablen *bezeichnet, wenn F eine endliche Erweiterung von $k(x)$ und x ein über k transzendentes Element ist. In diesem Zusammenhang nennt man k den* Konstantenkörper. *Der algebraische Abschluss k_0 von k in F wird als der* exakte Konstantenkörper *bezeichnet. Handelt es sich bei k um einen endlichen Körper, so nennt man F einen* globalen Funktionenkörper. *Ist die Erweiterung $F/k(x)$ separabel, bezeichnet man x auch als* separierendes Element.

Bemerkung 1.0.2. *Im weiteren Verlauf der Arbeit ist mit einem Funktionenkörper immer ein algebraischer Funktionenkörper in einer Variablen gemeint. Je nach dem ob man die Bedeutung des Konstantenkörpers hervorheben will, schreibt man F oder F/k für einen Funktionenkörper. Für die folgenden Definitionen und Aussagen sei also F immer ein Funktionenkörper über dem exakten Konstantenkörper k.*

Definition 1.0.3. *Seien F_1/k und F_2/k zwei über dem selben Konstantenkörper definierte Funktionenkörper. Eine Abbildung $\phi : F_1 \longrightarrow F_2$ wird als* Funktionenkörperhomomorphismus *bezeichnet, wenn ϕ ein Körperhomomorphismus ist, der sich zur Identität auf dem Konstantenkörper einschränken lässt.*

Definition 1.0.4. *Das maximale Ideal P eines Bewertungsrings in F wird als* Stelle *bezeichnet. Für den Bewertungsring schreibt man $\mathcal{O}_P$ und für die dazugehörige Bewertung $v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$. Mit $\mathbb{P}_F$ bezeichnet man die Menge der Stellen von F und der Körper $F_p = \mathcal{O}_P/P$ wird* Restklassenkörper von P *genannt. Als den* Grad deg P *der Stelle P bezeichnet man den Grad der Körpererweiterung F_p über k.*

Das folgende Lemma rechtfertigt die Definition des Grades.

Lemma 1.0.5. *Für alle Stellen P von F/k gilt $k \subseteq F_P$ und $[F_P : k] < \infty$.*

Beweis. Ein Beweis findet sich in [Sti93, S.6]. □

Definition 1.0.6. *Sei $\emptyset \neq S \subsetneqq \mathbb{P}_F$. Dann bezeichnet*

$$\mathcal{O}_S := \{z \in F | v_P(z) \geq 0 \text{ für alle } P \in S\}$$

den Schnitt über alle Bewertungsringe $\mathcal{O}_P$ mit $P \in S$. Ringe dieser Art bezeichnet man als holomorphe Ringe.
Abkürzend schreibt man $\mathcal{O}^S := \mathcal{O}_{\mathbb{P}_F \setminus S}$.

Definition 1.0.7. *Die freie, von $\mathbb{P}_F$ erzeugte abelsche Gruppe $\mathcal{D}_F$ nennt man die* Divisorengruppe. *Ihre Elemente werden* Divisoren *genannt. Die Verknüpfung in der Gruppe wird additiv aufgefasst. Ein Element D aus $\mathcal{D}_F$ ist also eine formale Summe der Form $D = \sum_{P \in \mathbb{P}_F} n_P P$ mit $n_P \in \mathbb{Z}$, $n_P = 0$ für fast alle $P \in \mathbb{P}_F$. Die Abbildung $v_P : \mathcal{D}_F \longrightarrow \mathbb{Z}$, $D \mapsto n_P$ misst wie oft die Stelle P in der formalen Summe auftaucht. Die Menge $Supp(D)$ der Stellen Q mit $v_Q(D) \neq 0$ bezeichnet man als den* Träger *von D. Die Abbildung*

$$\deg : \mathcal{D}_F \longrightarrow \mathbb{Z},\ D \mapsto \sum_{P \in \mathbb{P}_F} v_P(D) \cdot \deg(P)$$

nennt man die Gradabbildung. *Bei ihr handelt es sich um einen Gruppenhomomorphismus. Weiterhin definiert man durch*

$$D_1 \leq D_2 :\Longleftrightarrow v_Q(D_1) \leq v_Q(D_2) \text{ für alle } Q \in \mathbb{P}_F$$

eine Partialordnung auf der Divisorengruppe. Einen Divisor D mit $0 \leq D$ nennt man auch effektiv. *Jeder Divisor D lässt sich schreiben als $D = D_0 - D_\infty$, wobei D_0 und D_∞ beide effektiv sind. Man nennt sie in diesem Zusammenhang* Nullstellen- *beziehungsweise* Poldivisor *von D. Die Abbildungen*

$$\iota : \mathbb{P}_F \longrightarrow \mathcal{D}_F,\ P \mapsto 1 \cdot P$$

und

$$(.) : F^\times \longrightarrow D_F,\ x \mapsto \sum_{P \in \mathbb{P}_F} v_P(x)\, P$$

liefern Inklusionen der Stellen und der multiplikativen Gruppe des Funktionenkörpers in die Divisorgruppe. Ihre Bilder werden als die Prim- *beziehungsweise* Hauptdivisoren *bezeichnet.*

Definition 1.0.8. *Sei D ein Divisor von F. Die durch*

$$\mathcal{L}(D) := \{x \in F^\times | -D \leq (x)\} \cup \{0\}$$

definierte Menge wird der Riemann-Roch-Raum von D *genannt.*

Lemma 1.0.9. *Bei $\mathcal{L}(D)$ handelt es sich um einen endlichdimensionalen Vektorraum über dem Konstantenkörper k. Mit* $\dim(D)$ *wird die k-Dimension von $\mathcal{L}(D)$ bezeichnet.*

Beweis. Ein Beweis findet sich in [Sti93, S.18]. □

Die Differenz zwischen dem Grad und der Dimension der Divisoren liefert eine wichtige Invariante eines Funktionenkörpers.

Definition 1.0.10. *Das* Geschlecht *g von F ist definiert als*

$$g := \max\{\deg A - \dim A + 1 | A \in \mathcal{D}_F\}.$$

Bemerkung 1.0.11. *Nach [Sti93, S.20] ist das Geschlecht eine wohldefinierte natürliche Zahl.*

Lemma 1.0.12. *Sei $\phi : F_1 \longrightarrow F_2$ ein Isomorphismus von Funktionenkörpern. Dann gilt:*

1. *ϕ bildet Stellen vom Grad d von F_1 auf Stellen vom Grad d von F_2 ab, induziert als eine graderhaltende Bijektion $\hat{\phi} : \mathbb{P}_{F_1} \longrightarrow \mathbb{P}_{F_2}$.*
2. *$\hat{\phi}$ lässt sich fortsetzen zu einem Gruppenisomorphismus $\hat{\phi} : \mathcal{D}_{F_1} \to \mathcal{D}_{F_2}$ auf den Divisorgruppen.*
3. *Sei D ein Divisor von F_1 und $n \in \mathbb{N}$. Dann induziert ϕ einen Vektorraumisomorphismus $\tilde{\phi} : \mathcal{L}(nD) \longrightarrow \mathcal{L}(n\hat{\phi}(D))$.*
4. *F_1 und F_2 haben dasselbe Geschlecht.*

Beweis. Dieser Satz folgt direkt aus den Isomorphieeigenschaften und Eigenschaften von Funktionenkörpern. In [Sti93] findet sich alles Nötige für einen vollständigen Beweis. □

Diesen Satz kann man als Auflistung notwendiger Bedingungen für die Existenz eines Funktionenkörperisomorphismus ansehen. Er lässt sich auf den Einbettungsfall verallgemeinern. Dafür werden aber einige Aussagen und Definitionen im Zusammenhang mit Erweiterungen von Funktionenkörpern benötigt. Darum sei im Folgenden F' eine endliche Erweiterung des algebraischen Funktionenkörpers F und k' der exakte Konstantenkörper von F'.

Definition 1.0.13. *Seien P' und P Stellen von F' beziehungsweise von F. Dann sagt man P'* liegt über *P oder P* liegt unter *P' und schreibt dafür $P'|P$ wenn gilt $P \subseteq P'$. Die ganze Zahl $e(P'|P)$ mit $v_{P'}(z) = e(P'|P)\, v_P(z)$ für alle $z \in F$ nennt man den* Verzweigungsindex *von P' über P und den Grad der Körpererweiterung $F_{P'}/F_P$ nennt man den* Trägheitsgrad *und bezeichnet ihn mit $f(P'|P)$.*

Lemma 1.0.14. *Unter jeder Stelle P' von F' liegt genau eine Stelle P von F und über jeder Stelle P von F liegen nur endlich viele Stellen von F'. Da wir $[F' : F]$ als endlich vorausgesetzt haben, sind der Verzweigungsindex und der Trägheitsgrad wohldefinierte natürliche Zahlen.*

Beweis. Diese Aussagen sind in [Sti93, S.60-63] bewiesen. □

Definition 1.0.15. *Sei P' eine Stelle von F'. Dann definiert man die* Norm von *P' als*

$$N_{F'/F}(P') := f(P'|P) \cdot P$$

wobei P die Stelle von F, die unter P' liegt bezeichnet. Diese Abbildung lässt sich $\mathbb{Z}$-linear zu einem Homomorphismus der Divisorgruppen fortsetzen.

Lemma 1.0.16. *Für eine Stelle P' von F' gilt* $\deg N_{F'/F}(P') = [k' : k] \deg P'$.

Beweis. Für einen Beweis siehe [Sal06, S.132]. □

Definition 1.0.17. *Die* Konorm *einer Stelle P von F ist definiert als:*

$$Con_{F'/F}(P) = \sum_{P'|P} e(P'|P) \cdot P'.$$

Auch hier liefert die $\mathbb{Z}$-lineare Fortsetzung einen Gruppenhomomorphismus zwischen den Divisorgruppen.

Theorem 1.0.18. *Sei P eine Stelle von F und $P_1, \ldots, P_s$ alle Stellen von F', die über P liegen. Dann gilt:*

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

Beweis. Einen Beweis findet man bei [Sti93, S.65]. □

Korollar 1.0.19. *Für einen Divisor $D \in \mathcal{D}_F$ gilt:*

$$\deg Con_{F'/F}(D) = \frac{[F' : F]}{[k' : k]} \cdot \deg D.$$

Beweis. Ein Beweis lässt sich bei [Sti93, S.65] finden. □

Lemma 1.0.20. *Sei $F \subseteq F' \subseteq F''$ ein Funktionenkörperturm. Dann verhält sich die Konorm transitiv, das heißt für alle $D \in \mathcal{D}_F$ gilt*

$$Con_{F''/F}(D) = Con_{F''/F'}(Con_{F'/F}(D)).$$

Beweis. In [Sti93, S.62] ist ein Beweis gegeben. □

Definition 1.0.21. *Für eine Stelle $P \in \mathbb{P}_F$ sei $\mathcal{O}'_P$ der ganze Abschluss von $\mathcal{O}_P$ in F'. Dann bezeichnet man die Menge*

$$\mathcal{C}_P := \{z \in F' \mid Tr_{F'/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

als den Komplementärmodul *von $\mathcal{O}_P$ bezüglich der Spur.*

Lemma 1.0.22. *In der Situation von Definition 1.0.21 gilt:*

1. *Es existiert ein $t \in F'$ mit $\mathcal{C}_P = t\mathcal{O}'_P$.*
2. *$v_{P'}(t) \leq 0$ für alle $P'|P$.*
3. *Für ein $t' \in F'$ gilt $\mathcal{C}_P = t'\mathcal{O}'_P$ genau dann wenn $v_{P'}(t) = v_{P'}(t')$ für alle $P'|P$.*
4. *$\mathcal{C}_P = \mathcal{O}'_P$ für fast alle $P \in \mathbb{P}_F$.*

Beweis. Für einen Beweis siehe [Sti93, S.81]. □

Definition 1.0.23. *Für $P'|P$ definiert man den* Differentenexponent *durch*

$$d(P'|P) := -v_{P'}$$

für ein $t \in F'$ mit $\mathcal{C}_P = t\mathcal{O}'_P$ und die Differente der Körpererweiterung durch:

$$Diff(F'/F) := \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot P'.$$

Nach Lemma 1.0.21 ist die Differente wohldefiniert und stellt einen effektiven Divisor von F' dar. Ihr Grad ist daher größer gleich null.

Theorem 1.0.24 (Hurwitz-Geschlechtsformel)**.** *Sei F'/F separabel und g' und g die Geschlechter von F' und F. Dann gilt*

$$2g' - 2 = \frac{[F' : F]}{[k' : k]}(2g - 2) + \deg \mathit{Diff}(F'/F).$$

Beweis. Ein Beweis ist in [Sti93, S.88] gegeben. □

Lemma 1.0.25. *Sei $\phi : F_1 \longrightarrow F_2$ eine Inklusion von Funktionenkörpern. Dann gilt:*

1. *$\phi(F_1) \subseteq F_2$ ist ein Unterkörper von F_2 mit $n := [F_2 : \phi(F_1)] < \infty$.*
2. *ϕ induziert einen Isomorphismus auf sein Bild.*
3. *Die Hurwitz-Geschlechtsformel stellt einen Zusammenhang zwischen den Geschlechtern g_1 von F_1 , g_2 von F_2 und dem Erweiterungsgrad n her. Es gilt nämlich:*
$$(2g_2 - 2) \geq n(2g_1 - 2).$$
Das liefert eine obere Schranke für den Erweiterungsgrad n unter der Annahme, dass die Erweiterung F_2 über $\phi(F_1)$ separabel ist.
4. *Über die Konorm induziert ϕ einen Monomorphismus $\hat{\phi} : \mathcal{D}_{F_1} \longrightarrow \mathcal{D}_{F_2}$, $D \mapsto Con_{F/F}(D)$ der Divisorgruppen.*
5. *Für $n \in \mathbb{N}$ und $D \in \mathcal{D}_{F_1}$ induziert ϕ einen Vektorraummonomorphismus $\tilde{\phi} : \mathcal{L}(nD) \longrightarrow \mathcal{L}(n\hat{\phi}(D))$.*
6. *Für $D \in \mathcal{D}_{F_1}$ lässt sich ϕ zu einer Abbildung $\phi : \mathcal{O}^{Supp(D)} \longrightarrow \mathcal{O}^{Supp(\hat{\phi}(D))}$ einschränken.*

Beweis. Dieser Satz wird ganz analog zu 1.0.12 bewiesen. Für (4) verwendet man einfach die grobe Abschätzung $\deg \mathit{Diff}(F_2/\phi(F_1)) \geq 0$. □

Bemerkung 1.0.26. *Den Satz kann man als notwendige Bedingungen für die Existenz einer Einbettung auffassen. In den folgenden Kapiteln wird gezeigt, wie man diese benutzen kann, um die Einbettungen zu berechnen.*

Definition 1.0.27. *Sei $\phi : F_1 \longrightarrow F_2$ eine Einbettung von Funktionenkörpern. Den* Grad von ϕ *definiert man als* $\deg \phi := [F_2 : \phi(F_1)]$. *Man nennt ϕ* separabel, *wenn F_2 eine separable Erweiterung von $\phi(F_1)$ ist.*

Für globale Funktionenkörper gilt noch etwas mehr.

Lemma 1.0.28. *Sei F ein über einem endlichen Konstantenkörper definierter Funktionenkörper und sei $d \in \mathbb{N}$. Dann besitzt F nur endlich viele Stellen vom Grad kleiner gleich d.*

Beweis. Die Aussage ist in [Sti93, S.158] bewiesen. □

Lemma 1.0.29. *Sei F'/k eine Erweiterung des globale Funktionenkörpers F/k mit $[F' : F] = n$ und seien m' und m die Anzahl der Stellen vom Grad eins von F' beziehungsweise F. Dann gilt:*

$$m' \leq nm.$$

Beweis. Unter einer Stelle vom Grad eins von F' kann nur eine Stelle vom Grad eins von F liegen. Umgekehrt liegen über jeder Stelle vom Grad eins von F maximal n Stellen vom Grad eins von F'. Geht man also vom total zerlegten Fall aus, gilt $m' = nm$. In den anderen Fällen gibt es mindestens eine Stelle vom Grad eins von F über der maximal $n-1$ Stellen liegen, also gilt $m' \leq nm$ □

Für die algorithmische Berechnung der Einbettungen wird die Abschätzung, die die Hurwitz-Geschlechtsformel liefert, wichtig. Diese gilt nur für separable Erweiterungen. Die nächsten Sätze sagen, was bei inseparablen Erweiterungen passiert:

Theorem 1.0.30. *Sei F ein Funktionenkörper über einem vollkommenen Konstantenkörper k der Charakteristik p und sei F' eine rein inseparable Erweiterung von F vom Grad m. Dann gilt:*

1. *Es gibt ein $d \in \mathbb{N}$ mit $m = p^d$.*
2. *$F = (F')^{p^d}$.*
3. *Der Frobeniusendomorphismus $\Phi_d : F' \longrightarrow F'$ $z \mapsto z^{p^d}$ definiert einen Isomorphismus von F' und F.*
4. *Die Geschlechter von F' und F sind gleich.*
5. *Über jeder Stelle P von F liegt genau eine Stelle $P' \in \mathbb{P}_{F'}$ mit $e(P'|P) = p^d$ und $f(P'|P) = 1$.*
6. *Sei umgekehrt F ein beliebiger Funktionenkörper über einem vollkommenen Konstantenkörper der Charakteristik p, dann ist für alle $d \in \mathbb{N}$ F^{p^d} ein Teilkörper von F und die Erweiterung F/F^{p^d} ist rein inseparabel vom Grad p^d.*

Beweis. Ein Beweis ist in [Sti93, S.128] gegeben. □

Korollar 1.0.31. *Seien F_1, F_2 zwei Funktionenkörper über dem Konstantenkörper $\mathbb{F}_q$ der Charakteristik p und sei $\phi : F_1 \longrightarrow F_2$ eine Einbettung. Dann definiert $\phi_p : F_1 \longrightarrow F_2$, $z \mapsto \phi(z)^p$ auch eine Einbettung.*

Beweis. Wir wissen, wenn ϕ eine Einbettung ist, dann ist $\phi(F_1)$ ein Unterkörper von F_2. Nach 1.0.30 ist $\phi(F_1)^p$ ein Unterkörper von $\phi(F_1)$. Die Erweiterung $\phi(F_1)/\phi(F_1)^p$ ist rein inseparabel und der Frobenius liefert einen Isomorphismus Φ von $\phi(F_1)$ und $\phi(F_1)^p$. Hintereinander Ausführen von ϕ und Φ liefert genau die Abbildung ϕ_p, also ist diese eine Einbettung. □

Theorem 1.0.32. *Sei F' eine algebraische Erweiterung des Funktionenkörpers F. Dann kann man diese Erweiterung aufspalten in einen separablen Teil F_s/F und einen rein inseparablen Teil F'/F_s. Man spricht in diesem Zusammenhang von dem separablen Abschluss von F in F'.*

Beweis. Diese Aussage wird in [Lor92, S.84] bewiesen. □

Korollar 1.0.33. *Sei F' eine endliche Erweiterung des Funktionenkörpers F und sei der Konstantenkörper von F vollkommen. Dann gibt es einen Zwischenkörper L, so dass L/F rein inseparabel und F'/L separabel ist. Diesen Zwischenkörper nennen wir den rein inseparablen Abschluss von F in F'.*

Beweis. Nach dem vorherigen Satz gibt es einen Zwischenkörper E, den separablen Abschluss von F in F', so dass E/F separabel und F'/E rein inseparabel ist. Da der Konstantenkörper vollkommen ist, sind F' und E nach 1.0.30 isomorph. Sei also $\Psi : E \longrightarrow F'$ ein Isomorphismus. Definiere $L := \Psi(F)$. Dann ist L offensichtlich ein zu F isomorpher Zwischenkörper von F'/F. Sei nun a ein beliebiges Element von F' und g das Minimalpolynom von a über L. Dann ist $\Psi^{-1}(g)$ das Minimalpolynom von $\Psi^{-1}(a) \in E$ über F. Dieses ist nach Konstruktion von E separabel, also ist F'/L auch separabel und es gilt $[F' : L] = [E : F]$. □

Seien F_1 und F_2 zwei Funktionenkörper über dem endlichen Körper k und $\phi : F_1 \longrightarrow F_2$ eine Einbettung. Dann wissen wir, dass $F_2/\phi(F_1)$ eine endliche Körpererweiterung ist. Man kann den rein inseparablen Abschluss L von $\phi(F_1)$ in F_2 betrachten und das liefert eine Zerlegung der Erweiterung in den rein inseparablen Teil $L/\phi(F_1)$ und den separablen Teil F_2/L. Da wir wissen, dass E und $\phi(F_1)$ isomorph sind, gibt es auch eine Einbettung $\phi' : F_1 \longrightarrow F_2$ mit $\phi'(F_1) = E$ und diese ist separabel. Will man also alle Einbettungen bestimmen, so genügt es, die zu berechnen, bei denen das Bild ein separabler Zwischenkörper ist. Dann bekommt man alle Einbettungen, indem man die separablen Einbettungen mit den Isomorphismen ihrer Bilder auf deren rein inseparablen Unterkörper verknüpft.

Theorem 1.0.34. *Sei F ein Funktionenkörper über einem beliebigen Konstantenkörper k und bezeichne $\overline{k}$ den algebraischen Abschluss von k. Sei das Geschlecht g des Kompositums $F\overline{k}$ größer gleich zwei. Dann ist die Automorphismengruppe $Aut_k(F)$ eine endliche Gruppe.*

Bemerkung 1.0.35. *Wenn man voraussetzt, dass der Konstantenkörper k vollkommen ist, dann ändert eine algebraische Konstantenkörpererweiterung das Geschlecht nicht. Bei endlichen Konstentenkörpern ist das immer der Fall. Die Automorphismengruppe von globalen Funktionenkörpern mit Geschlecht größer gleich zwei ist also endlich.*

Beweis. Diese Aussage ist in [Sal06, S.581] bewiesen. □

Korollar 1.0.36. *Seien F_1/k und F_2/k zwei Funktionenkörper über einem vollkommenen Konstantenkörper vom Geschlecht größer gleich zwei. Dann ist die Anzahl der Isomorphismen von F_1 nach F_2 endlich.*

Beweis. Sei $\phi : F_1 \longrightarrow F_2$ ein Isomorphismus der Funktionenkörper. Dann induzieren verschiedene Isomorphismen $\phi_i : F_1 \longrightarrow F_2$ $i \in \{1, \ldots, n\}$ durch $\phi_i^{-1} \circ \phi$ auch verschiedene Automorphismen von F_1. Aus der Endlichkeit der Automorphismengruppe von F_1 folgt somit auch die Endlichkeit der Isomorphismen. □

Theorem 1.0.37. *Sei F ein Funktionenkörper über dem vollkommenen Konstantenkörper k. Dann haben fast alle Teilkörper L mit $[F : L] = n$ das Geschlecht null.*

Beweis. Ein Beweis dafür findet sich in [Tam72]. □

Korollar 1.0.38. *Ein Funktionenkörper F vom Geschlecht $g \geq 2$ über einem vollkommenen Konstantenkörper besitzt nur endlich viele separierende Zwischenkörper vom Geschlecht größer gleich zwei.*

Beweis. Das Geschlecht aller separierenden Zwischenkörper ist durch g beschränkt, also kommen nur endlich viele Werte als Geschlecht für diese Zwischenkörper in Frage. Für die separierenden Zwischenkörper L vom Geschlecht größer gleich zwei kann man die Hurwitz-Geschlechtsformel anwenden. Daher ist auch der Grad $[F : L]$ beschränkt. Für diese endlich vielen verschiedenen Grade gibt es nach dem Theorem 1.0.37 nur endlich viele Zwischenkörper. Daraus folgt die Behauptung. □

Korollar 1.0.39. *Seien F_1, F_2 zwei Funktionenkörper vom Geschlecht $g_1, g_2 \geq 2$ über dem vollkommenen Konstantenkörper k. Dann gilt:*

1. *Es gibt nur endlich viele separable Einbettungen.*
2. *Sei $P \in \mathbb{P}_{F_1}$ vom Grad eins und $D \in \mathcal{D}_{F_2}$. Dann gibt es nur endlich viele Einbettungen ϕ mit $\hat{\phi}(P) = D$.*

Beweis. Jede separable Einbettung $\phi : F_1 \longrightarrow F_2$ induziert einen Isomorphismus auf ihr Bild, welches nach Voraussetzung ein Zwischenkörper $\phi(F_1)$ von F_2 vom Geschlecht g_1 ist, so dass $F_2/\phi(F_1)$ separabel ist. Nach 1.0.38 gibt es nur endlich viele solche Zwischenkörper und nach 1.0.36 gibt es jeweils nur endlich viele Isomorphismen auf diese Zwischenkörper. Daraus folgt die Endlichkeit der Anzahl der separablen Einbettungen. Sei nun ϕ eine, nicht notwendigerweise separable, Einbettung mit $\hat{\phi}(P) = D$. Dann gilt $[F_2 : \phi(F_1)] = \deg D$. Nach 1.0.37 gibt es nur endlich viele solche Zwischenkörper und somit folgt aus der Endlichkeit der Isomorphismen der zweite Teil der Behauptung. □

Da jeder endliche Körper vollkommen ist, rechtfertigt dieser Satz den Versuch für globale Funktionenkörper vom Geschlecht größer gleich zwei alle separablen Einbettungen zu berechnen. In diesem Fall lässt sich die Endlichkeit der Anzahl solcher Abbildungen aber auch elementar aus der Endlichkeit des Konstantenkörpers beweisen.

Kapitel 2

Der Einbettungsalgorithmus im Überblick

In diesem Abschnitt wird erst der Isomorphiealgorithmus aus [Hes04] skizziert und dann der Algorithmus zum Berechnen der Einbettungen vorgestellt. Einzelne Punkte bleiben noch offen und werden zusammen mit den benötigten mathematischen Konzepten im nächsten Abschnitt erklärt.

Der Einbettungsalgorithmus und der Isomorphiealgorithmus setzen voraus, dass es Methoden gibt, um verschiedene Rechnungen mit Funktionenkörpern durchzuführen. Beispielsweise werden folgende Methoden als gegeben vorausgesetzt: Man kann Funktionenkörper mittels einer definierenden Gleichung erzeugen und in ihnen rechnen. Zu Elementen des Funktionenkörpers können die Hauptdivisoren berechnet werden und man kann diese in Pol- und Nullstellendivisor zerlegen. Es können die Stellen von festem Grad konstruiert werden und man kann mit Riemann-Roch-Räumen rechnen sowie deren Dimension und Basen bestimmen. Weiterhin kann man mit endlichen Körpern, Polynomen und Laurentreihen arbeiten und einfache Gleichungssysteme lösen. Die Computeralgebrasysteme KASH [Kan04] und Magma [BCP97] stellen alle diese Methoden zur Verfügung. Sowohl der Isomorphiealgorithmus wie auch der Einbettungsalgorithmus sind in Magma implementiert.

2.1 Der Isomorphiealgorithmus

Der Isomorphiealgorithmus greift die Idee des Lemmas 1.0.12 auf. Dieses besagt, dass ein Isomorphismus $\phi : F_1 \longrightarrow F_2$ zweier Funktionenkörper auch eine graderhaltene Bijektion $\hat{\phi}$ der Stellen und für jede Stelle P einen Vektorraumisomorphismus $\tilde{\phi} : \mathcal{L}(nP) \longrightarrow \mathcal{L}(n\hat{\phi}(P))$ induziert. Zum Berechnen der Isomorphismen wählt man eine Stelle P_1 von F_1 vom Grad eins und testet, für welche Grad eins Stellen P_2 von F_2 die Vektorräume $\mathcal{L}(nP_1)$ und $\mathcal{L}(nP_2)$ isomorph sind. Wann immer das der Fall ist, wählt man Elemente $x_1, \ldots, x_r \in \mathcal{L}(nP_1)$ und $y_1, \ldots, y_r \in \mathcal{L}(nP_2)$ mit $F_1 = k(x_1, \ldots, x_r)$ und $F_2 = k(y_1, \ldots, y_r)$. Anhand dieser Elemente überprüft man, ob der Isomorphismus der Riemann-Roch-Räume mit der Multiplikation verträglich ist, also einen Isomorphismus von F_1 nach F_2 liefert. Diese Frage reduziert man durch spezielle Eigenschaften der x_i und y_i im wesentlichen auf ein Gleichungssystem in

zwei Unbekannten.

2.2 Idee des Einbettungsalgorithmus

Nach den Überlegungen zu rein inseparablen Körpererweiterungen wissen wir, dass man sich bei der Berechnung der Einbettungen auf die separablen einschränken kann.

Damit liefert Lemma 1.0.12 eine Idee, wie man den Isomorphiealgorithmus auf die Berechnung von Einbettungen verallgemeinern kann. Nehmen wir also an, dass wir eine separable Einbettung $\phi : F_1 \longrightarrow F_2$ besäßen. Dann wäre ihr Bild ein Unterkörper von F_2 von beschränktem Grad und ϕ induzierte die beschriebenen Abbildungen $\tilde{\phi}$ und $\hat{\phi}$ der Divisorgruppen und passender Riemann-Roch-Räume. Es gilt nun zu überprüfen, unter welchen Bedingungen diese induzierten Abbildungen existieren. Dafür versuchen wir für eine Stelle P von F_1 zu bestimmen, auf welche Divisoren D von F_2 sie abgebildet werden kann, indem wir testen, welche Riemann-Roch-Räume sich in welche einbetten lassen. Ausgehend von den Einbettungen der Riemann-Roch-Räume konstruieren wir nun die Einbettungen der Funktionenkörper, indem wir testen, welche Vektoraummonomorphismen mit der Multiplikation verträglich sind.

2.3 Aufbau des Einbettungsalgorithmus

Der Einbettungsalgorithmus

Algorithmus 1 Einbettungen

Input: Globale Funktionenkörper F_1 und F_2.
Output: Eine Liste aller separabler Inklusionen $\phi : F_1 \to F_2$.

1: Berechne die Geschlechter der Funktionenkörper und damit eine obere Schranke $n_{max} \geq [F_2 : \phi(F_1)]$.
2: Berechne aus der Anzahl der Stellen vom Grad eins von F_1 und F_2 eine untere Schranke $n_{min} \leq [F_2 : \phi(F_1)]$.
3: **for** $n \in \{n_{min}, \ldots, n_{max}\}$ **do**
4: Wähle eine Stelle P vom Grad eins von F_1.
5: Konstruiere Menge M aller effektiven Divisoren D der Divisorgruppe von F_2 mit $\deg(D) = n$.
6: **for** $D \in M$ **do**
7: Überprüfe ob $Con_{F_2/\phi(F_1)}(\phi(P)) = D$ möglich ist durch Überprüfung ob $\mathcal{L}(kP)$ in $\mathcal{L}(kD)$ für $k \in \mathbb{N}$ einbettbar.
8: **if** ist möglich **then**
9: Konstruiere die dazugehörigen Einbettungen falls sie existieren.
10: **end if**
11: **end for**
12: **end for**
13: Gebe die berechneten Einbettungen zurück.

Dabei werden einzelne Schritte von Unteralgorithmen ausgeführt:

1. Unteralgorithmus: Berechnen der oberen Schranke für $[F_2 : \phi(F_1)]$.
2. Unteralgorithmus: Berechnen der unteren Schranke für $[F_2 : \phi(F_1)]$.
3. Unteralgorithmus: Konstruktion der effektiven Divisoren von festem Grad.
4. Unteralgorithmus: Überprüfen welche Stelle auf welchen Divisor abgebildet werden kann.
5. Unteralgorithmus: Überprüfen ob die Abbildung der Divisoren von einem Funktionenkörperhomomorphismus kommt.
6. Unteralgorithmus: Konstruktion der Abbildungen zwischen den Funktionenkörpern.

Unteralgorithmus 1

Als Input bekommt dieser Unteralgorithmus zwei Funktionenkörper F_1 und F_2. Unter Verwendung der Hurwitz-Geschlechtsformel liefert er durch Berechnung der Geschlechter g_1 und g_2 der Funktionenkörper eine obere Schranke $n_{max} = \frac{2g_2-2}{2g_1-2}$ und gibt diese zurück. Hier wird verwendet, dass die Funktionenkörper ein Geschlecht größer als eins und den selben Konstantenkörper haben.

Unteralgorithmus 2

In diesem Unteralgorithmus wird für zwei Funktionenkörper F_1 und F_2 die Anzahl m_1 und m_2 ihrer Stellen vom Grad eins berechnet. Auf Grund von Lemma (1.0.29) bekommt man die Abschätzung $n_{min} = \max\{\lceil \frac{m_2}{m_1} \rceil, 2\}$.

Unteralgorithmus 3

Dieser Algorithmus bekommt als Input eine natürliche Zahl n und einen globalen Funktionenkörper F und liefert als Output die endliche Menge M aller effektiven Divisoren vom Grad n. Dabei handelt es sich eigentlich nur um ein kombinatorisches Problem. Da man alle Stellen vom Grad i für $i \in \{1, \ldots, n\}$ konstruieren kann, muss man nur alle Möglichkeiten finden, diese zu Divisoren vom Grad n zu kombinieren. Dazu müssen alle Möglichkeiten bestimmt werden, n als Summe von natürlichen Zahlen $n = k_1 + \ldots + k_s$ darzustellen. Anschließend müssen für jedes k_i alle Möglichkeiten, dieses als Produkt zweier natürlicher Zahlen $k_i = e_i \cdot f_i$ darzustellen, berechnet werden. Die Intuition ist nun, dass jedes der k_i eine Stelle des Divisors und dann e_i den Verzweigungsindex und f_i den Grad der Stelle beschreiben. Diese Aufgabe lässt sich durch eine einfache Rekursion lösen. Hat man nun alle verschiedenen Kombinationen $((e_1, f_1), \ldots, (e_k, f_k))$ gefunden, so kann man daraus alle effektiven Divisoren vom Grad n konstruieren, indem man zu einem Tupel $((e_1, f_1), \ldots, (e_k, f_k))$ alle Divisoren $D = e_1P_1 + \ldots + e_kP_k$ mit P_i beliebige Stelle vom Grad f_i aufbaut. Wenn man sich dabei geschickt anstellt, vermeidet man es auch, Divisoren doppelt zu konstruieren. Es ist offensichtlich, dass alle so konstruieren Divisoren Grad n haben und dass man jeden vom Grad n auf diese Weise bekommt.
Dieser Unteralgorithmus ist einer der wenigen, in dem verwendet wird, dass es sich bei den zu untersuchenden Funktionenkörpern um globale Funktionenkörper handelt, da

man die Endlichkeit der Anzahl von Stellen von beschränktem Grad benötigt, damit die Menge der Divisoren vom Grad n auch eine endliche Menge wird.

Unteralgorithmus 4

Der Input dieses Unteralgorithmus sind zwei Funktionenkörper F_1/k und F_2/k, eine Stelle P von F_1 und ein Divisor D von F_2. Zurückgegeben wird ein boolscher Wert, wobei FALSE ausdrückt, dass es nicht nicht möglich ist, dass ein Funktionenkörperhomomorphismus $\phi : F_1 \longrightarrow F_2$ existiert mit $\hat{\phi}(P) = D$ und TRUE bedeutet, dass es so eine Abbildung möglicherweise gibt.
Dazu sucht man sich zunächst das kleinste $m \in \mathbb{N}$ mit $\dim(\mathcal{L}(mP)) = 2$ und wählt eine Basis $\{1, x_1\}$ dieses Riemann-Roch-Raumes. Nun betrachtet man $\mathcal{L}(mD)$ und wählt auch hier eine Basis $\mathcal{B} = \{b_1, \ldots, b_k\}$. Wir wissen: für jedes $\phi : F_1 \longrightarrow F_2$ mit $\hat{\phi}(P) = D$ gilt $\phi(x_1) \in \mathcal{L}(mD)$ und $(\phi(x_1))_\infty = mD$, also gilt es zu überprüfen, ob es eine k-Linearkombination in $\mathcal{B}$ gibt, welche das entsprechende Polverhalten hat. Dies geschieht, indem man die Poldivisoren von $b_1, \ldots, b_k$ berechnet und testet, ob man mit ihnen unter Beachtung der ultrametrischen Dreiecksungleichung den Divisor mD konstruieren kann, das heißt, ob für jedes $Q \in \mathit{supp}(D)$ ein $b_i \in \mathcal{B}$ existiert mit $v_Q(b_i) = -m$.

Unteralgorithmus 5

Der Input ist derselbe wie in dem vorherigen Unteralgorithmus. Ganz analog wird ein $x_1 \in F_1$ gewählt und eine Basis $\mathcal{B} = \{b_1, \ldots, b_k\}$ von $\mathcal{L}(mD)$ bestimmt. Es muss also gelten: $\phi(x_1) = \lambda_1 b_1 + \ldots + \lambda_k b_k$ mit $\lambda_i \in k$. Dann wählt man spezielle Elemente $x_1, \ldots, x_r \in F_1$ mit $F_1 = k(x_1, \ldots, x_r)$. Wie man das macht und was weitere Eigenschaften dieser x_i sind, wird im nächsten Abschnitt beschrieben. Jeder Funktionenkörperhomomorphismus $\phi : F_1 \longrightarrow F_2$ ist also vollständig durch seine Bilder auf den x_i bestimmt. Ausgehend von $\phi(x_1) = \lambda_1 b_1 + \ldots + \lambda_k b_k$ muss man nun also alle möglichen Bilder $\phi(x_i)$ in Abhängigkeit von den λ_i bestimmen, die mit den algebraischen Relationen zwischen den x_i verträglich sind. Das geschieht durch einen speziellen Reduktionsalgorithmus, der im nächsten Abschnitt vorgestellt wird. Als Output liefert der Algorithmus nun alle Werte für die λ_i, die eine Abbildung von F_1 nach F_2 definieren und jeweils die dazugehörigen Bilder der x_i.

Unteralgorithmus 6

Dieser Unteralgorithmus konstruiert nun aus dem Output des 5. Unteralgorithmus die Einbettungen. Dazu wird $k(x_1, \ldots, x_r)$ wieder in die anfängliche Darstellung $F_1 = k(x, y)$ umgerechnet und aus den Bildern für die x_i die Bilder von x und y bestimmt. Das geschieht, indem man durch das Lösen von Gleichungssystemen die Darstellung von x und y in den x_i ermittelt. Es wird kein spezieller Algorithmus benötigt, da sich dieses durch die Eigenschaften der x_i auf einige einfache lineare Gleichungssystem reduzieren lässt.

Kapitel 3

Untersuchung des Einbettungsalgorithmus

In diesem Abschnitt werden zu einigen Teilschritten des Algorithmus nähere Informationen angegeben. Diese Teilschritte sind:

1. Ausschließen von bestimmten Funktionenkörpern im Voraus.
2. Entscheiden, welche Divisoren über welcher Stelle liegen können.
3. Berechnung einer Basis für bestimmte freie Moduln.
4. Auflisten der Eigenschaften spezieller Funktionenkörperelemente x_i.
5. Berechnen der Parameter, die wirklich eine Abbildung definieren.
6. Berechnen der Abbildungen.
7. Arbeit mit Stellen höheren Grades.
8. Wahl der Stelle P von F_1.
9. Probleme bei speziellen Funktionenkörpern.

3.1 Ausschluss bestimmter Funktionenkörper

In diesem Abschnitt wird ein weiteres notwendiges Kriterium vorgestellt, das anhand der Klassengruppen entscheidet, ob es möglich ist, einen bestimmten Funktionenkörper in den anderen einzubetten.

3.1.1 Mathematischer Aspekt

Definition 3.1.1. *Für einen Funktionenkörper F bezeichnet man die Gruppe der Hauptdivisoren $\mathcal{P}_F$ mit*

$$\mathcal{P}_F := \{(x) \,|\, 0 \neq x \in F\}.$$

Die Faktorgruppe

$$\mathcal{C}_F := \mathcal{D}_F/\mathcal{P}_F$$

wird Divisorklassengruppe *genannt. Mit* $\mathcal{C}_F^0$ *bezeichnet man die Untergruppe von* $\mathcal{C}_F$ *der Divisorklassen vom Grad null. Da Hauptdivisoren den Grad null haben und der Grad ein Gruppenhomomorphismus ist, ist* $\mathcal{C}_F^0$ *wohldefiniert. Wenn die Gruppe* $\mathcal{C}_F^0$ *endlich ist, bezeichnet man ihre Kardinalität* $h_F = \#\mathcal{C}_F^0$ *als* Klassenzahl *von* F.

Lemma 3.1.2. *Die Norm und die Konorm bilden Hauptdivisoren auf Hauptdivisoren ab und induzieren somit auch Homomorphismen der Divisorklassengruppen*

$$Con_{F'/F} : \mathcal{C}_F \longrightarrow \mathcal{C}_{F'}$$

$$N_{F'/F} : \mathcal{C}_{F'} \longrightarrow \mathcal{C}_F.$$

Außerdem werden durch Norm und Konorm Divisoren vom Grad null auf Divisoren vom Grad null abgebildet, daher kann man die Homomorphismen der Divisorklassengruppen auch auf die Divisorklassen von Grad null einschränken.

$$Con_{F'/F} : \mathcal{C}_F^0 \longrightarrow \mathcal{C}_{F'}^0$$

$$N_{F'/F} : \mathcal{C}_{F'}^0 \longrightarrow \mathcal{C}_F^0.$$

Beweis. Diese Aussagen sind in [Sal06, S.132] und [Sti93, S.63] bewiesen. □

Korollar 3.1.3. *Sei* F' *eine Erweiterung des Funktionenkörpers* F *vom Grad* n. *Seien* F *und* F' *über dem selben Konstantenkörper definiert. Dann liefert das Hintereinanderausführen von Norm und Konorm einen Endomorphismus* $\varrho : \mathcal{C}_F \longrightarrow \mathcal{C}_F$ *der Klassengruppe von* F. *Es gilt* $\varrho([D]) = n[D]$ *für alle* $[D] \in \mathcal{C}_F$. *Diese Abbildung lässt sich auch auf die Klassengruppe vom Grad null einschränken.*

Beweis. Sei $P \in \mathcal{D}_F$ ein beliebiger Primdivisor und sei D die Konorm von P mit $D := e_1P_1 + \ldots + e_sP_s$ und $f_i := deg(P_i)/deg(P)$, dann gilt

$$\deg(D) = n \deg(P) = \sum_{i=1}^{s} e_i \deg(P_i) = \left(\sum_{i=1}^{s} e_i f_i\right) \deg(P).$$

Also gilt

$$N_{F'/F}(Con_{F'/F}(P)) = N_{F'/F}(D) = \sum_{i=1}^{s} e_i N_{F'/F}(P_i) = \left(\sum_{i=1}^{s} (e_i f_i)\right) P = nP.$$

Auf Grund der $\mathbb{Z}$-Linearität von Norm und Konorm folgt die Behauptung für einen beliebigen Divisor der Divisorgruppe von F_1. Also gilt die Behauptung auch für die induzierte Abbildung auf den Divisorklassen und nach den obigen Aussagen auch lässt sich die Abbildung auf $\mathcal{C}_F^0$ einschränken. □

Theorem 3.1.4. *Bei Funktionenkörpern über einem endlichen Konstantenkörper ist die Klassenzahl endlich.*

Beweis. Für einen Beweis siehe [Sti93, S.159]. □

Lemma 3.1.5. *Seien $(G,+)$ und $(H,+)$ abelsche Gruppen und $\varrho_1 : G \longrightarrow H$, $\varrho_2 : H \longrightarrow G$ Gruppenhomomorphismen. Sei $\varrho := \varrho_2 \circ \varrho_1 : G \longrightarrow G$ und gelte $\varrho(a) = na$ für alle $a \in G$. Sei nun U_1 eine Untergruppe von G mit $ggT(\#U_1, n) = 1$, dann gibt es eine Untergruppe U_2 von H mit $U_1 \cong U_2$.*

Beweis. Man betrachte die Abbildung $\varrho|_{U_1} : U_1 \longrightarrow G$. Da die Ordnung von U_1 und n teilerfremd sind, gilt auch $ggT(ord(a), n) = 1$ für alle $a \in U_1$. Also ist $\varrho|_{U_1} : U_1 \longrightarrow G$ injektiv und induziert daher einen Isomorphismus auf sein Bild. Das liefert die Sequenz

$$U_1 \overset{\varrho_1|_{U_1}}{\longrightarrow} H \overset{\varrho_2}{\longrightarrow} \varrho(U_1)$$

von Gruppen und Gruppenhomomorphismen, bei denen $\varrho|_{U_1} = \varrho_2 \circ \varrho_1|_{U_1}$ ein Isomorphismus ist. Folglich ist $\varrho_1|_{U_1}$ injektiv und somit ist $U_2 := \varrho_1(U_1)$ eine zu U_1 isomorphe Untergruppe von H. □

Korollar 3.1.6. *Sei F'/F eine Erweiterung von Funktionenkörpern über endlichem Konstantenkörper k vom Grad n und p eine Primzahl, die n nicht teilt. Sei $d \in \mathbb{N}$. Gilt $p^d | h_F$, so teilt p^d auch $h_{F'}$.*

Beweis. Die Klassengruppen $\mathcal{C}_F^0$ und $\mathcal{C}_{F'}^0$ sind endliche abelsche Gruppen. Für jede Primzahlpotenz, die ihre Gruppenordnung teilt, gibt es auch eine Untergruppe dieser Ordnung und die Ordnung jeder Untergruppe teilt die Gruppenordnung. Also folgt die Behauptung daraus, dass man nach Lemma 3.1.5 für jede Untergruppe von $\mathcal{C}_F^0$, deren Ordnung teilerfremd zu n ist, auch eine isomorphe Untergruppe von $\mathcal{C}_{F'}^0$ bekommt. □

Bemerkung 3.1.7. *Diese Überlegungen beweisen die Korrektheit des im Folgenden vorgestellten Algorithmus formal.*

3.1.2 Algorithmischer Aspekt

Idee des Algorithmus

Sei nun $\phi : F_1 \longrightarrow F_2$ eine Einbettung von Funktionenkörpern. Wir wissen, dass man dann F_2 als einen Erweiterungskörper von $\phi(F_1)$ auffassen kann. Für $n = [F_2 : \phi(F_1)]$ liefern Norm und Konorm Abbildungen der Divisorklassengruppen vom Grad null, die hintereinander ausgeführt die Multiplikation mit n auf $\mathcal{C}_{F_1}^0$ beschreiben. Nach Lemma 3.1.5 bekommt man so einen Zusammenhang zwischen den Untergruppen von $\mathcal{C}_{F_1}^0$ und $\mathcal{C}_{F_2}^0$. Startet man nun umgekehrt mit Funktionenkörpern F_1 und F_2 und will bestimmen, ob es eine Einbettung $\phi : F_1 \longrightarrow F_2$ gibt, so dass $[F_2 : \phi(F_1)] = n$ gilt, dann kann man als Erstes die Klassengruppen von F_1 und F_2 bestimmen und untersuchen, ob sich deren Untergruppen so verhalten, wie in dem Lemma formuliert.

Pseudocode

Algorithmus 2 Klassengruppenkriterium

Input: Funktionenkörper F_1, F_2, obere Schranke n_{max} und untere Schranke n_{min} für den Grad von F_2 über dem Bild von F_1 unter einer Einbettung.

Output: Liste der $n \in \{n_{min}, \ldots, n_{max}\}$, die aufgrund der Klassengruppe als Grade für eine Einbettung in Frage kommen.

1: Berechne h_{F_1} und h_{F_2} die Klassenzahlen von F_1 und F_2.
2: Berechne die Faktorisierungen $h_{F_1} = p_1^{\epsilon_1} \cdot \ldots \cdot p_{m_1}^{\epsilon_{m_1}}$ und $h_{F_2} = q_1^{\nu_1} \cdot \ldots \cdot q_{m_2}^{\nu_{m_2}}$ der Klassenzahlen.
3: test:=TRUE.
4: zulässige_Grade := [ ].
5: **for** $n = n_{min}, \ldots, n_{max}$ **do**
6: **for** $p = p_1^{\epsilon_1}, \ldots, p_{m_1}^{\epsilon_{m_1}}$ **do**
7: **if** $ggT(n, p) = 1$ **then**
8: **if** $p \nmid h_{F_2}$ **then**
9: test := FALSE.
10: **end if**
11: **end if**
12: **end for**
13: **if** test **then**
14: Füge n in zulässige_Grade ein.
15: **end if**
16: **end for**
17: Gebe zulässige_Grade zurück.

Technische Probleme

In diesem Unteralgorithmus muss man die Klassenzahl der beiden Funktionenkörper berechnen. In der Praxis ist das algorithmisch möglich, dauert aber bei größeren Beispielen recht lange. Für kleine Beispiele lohnt es sich aber auf jeden Fall diesen Schritt durchzuführen, da man - besonders wenn die Funktionenkörper nicht einbettbar sind - die Anzahl der möglichen Grade oft sehr stark einschränken kann. Genauere Überlegungen dazu finden sich in dem Kapitel über die Laufzeiten.

3.2 Reduktion der Divisoren

Im vorherigen Abschnitt wurde beschrieben, wie man durch Untersuchung von gewissen Riemann-Roch-Räumen entscheiden kann, ob es möglich ist, dass ein bestimmter Divisor D über einer bestimmten Stelle P liegt. Dazu hat man ein Element $x_1 \in \mathcal{O}^P$ gewählt, welches die niedrigste Polzahl n_1 realisiert und untersucht, ob es ein $z \in F_2$ gibt mit $(z)_\infty = n_1 D$. Im folgenden Abschnitt wird ein Kriterium vorgestellt, mit dem man für eine Stelle P manche Divisoren D als Kandidaten für $\hat{\phi}(P) = D$ ausschließen kann, ohne die Riemann-Roch-Räume zu betrachten. Dazu benutzt man die

Hurwitz-Geschlechtsformel und schätzt die Differente etwas genauer ab.

3.2.1 Mathematischer Aspekt

Theorem 3.2.1 (Dedekinds Differententheorem)**.** *Sei F'/F eine endliche separable Erweiterung des globalen Funktionenkörpers F. Dann gilt:*

$$d(P'|P) \geq e(P'|P) - 1.$$

Beweis. Ein Beweis steht in [Sti93, S.89]. □

Korollar 3.2.2. *Sei $\phi : F_1 \longrightarrow F_2$ eine Einbettung und gelte $\hat{\phi}(Q) = e_1P_1 + \ldots + e_sP_s$ mit Q Stelle von F_1 und $P_1, \ldots, P_s$ Stellen von F_2. Dann gilt:*

$$\deg \mathit{Diff}(F_2/\phi(F_1)) \geq \sum_{i=1}^{s}(e_i - 1)\deg(P_i).$$

Beweis. Für die Differente gilt: $\mathit{Diff}(F_2/\phi(F_1)) = \sum_{P \in \mathbb{P}_{\phi(F_1)}} \sum_{P'|P} d(P'|P) \cdot P'$. Nach dem Differententheorem gilt $d(P'|P) \geq e(P'|P) - 1$. Somit

$$\begin{aligned}
\deg(\sum_{P \in \mathbb{P}_{\phi(F_1)}} \sum_{P'|P} d(P'|P) \cdot P') = \deg(&\sum_{P \in \mathbb{P}_{\phi(F_1)} \setminus \{Q\}} \sum_{P'|P} d(P'|P) \cdot P' \\
&+ d(P_1|Q) \cdot P_1 + \ldots + d(P_s|Q) \cdot P_s) \\
\geq \deg(&\sum_{P \in \mathbb{P}_{\phi(F_1)} \setminus \{Q\}} \sum_{P'|P} d(P'|P) \cdot P') \\
&+ (e_1 - 1)\deg(P_1) + \ldots + (e_s - 1)\deg(P_s) \\
\geq (e_1 - 1)&\deg(P_1) + \ldots + (e_s - 1)\deg(P_s).
\end{aligned}$$

□

In der Situation des Algorithmus ergibt sich daraus ein genauerer Zusammenhang zwischen den Geschlechtern der Funktionenkörper, dem Erweiterungsgrad $[F_2 : \phi(F_1)]$ und der Verzweigung einzelner Stellen:

Korollar 3.2.3. *Sei $\phi : F_1 \longrightarrow F_2$ eine Einbettung von Funktionenkörpern über dem Konstantenkörper k. Seien g_1 und g_2 die Geschlechter von F_1 beziehungsweise F_2 und gelte $\hat{\phi}(P) = e_1P_1 + \ldots e_sP_s$. Dann gilt:*

$$2g' - 2 \geq \deg(\hat{\phi}(P)) \cdot (2g - 2) + \sum_{i=1}^{s}(e_i - 1) \cdot \deg(P_i).$$

3.2.2 Algorithmischer Aspekt

Die Formel aus 3.2.3 liefert also durch das Berechnen der Geschlechter ein einfach zu überprüfendes Kriterium, mit dem man alle Divisoren D als Kandidaten für $\hat{\phi}(P)$ ausschließen kann, die diese Ungleichung nicht erfüllen.

3.3 Berechnung einer Basis von $\mathcal{O}^S$

Ziel dieses Abschnittes ist es, einen Algorithmus zur Berechnung einer $k[z]$-Basis des freien Moduls $\mathcal{O}^S$ vorzustellen, wobei z ein separierendes Element des Funktionenkörpers F/k ist und $S = Supp((z)_\infty)$ gilt. Der Algorithmus basiert auf einem Zusammenhang zwischen speziellen $k[z]$-Basen von $\mathcal{O}^S$ und Basen von gewissen Riemann-Roch-Räumen. Weiterhin wird die Entwicklung von Elementen in Reihen in einer lokalen Uniformisierenden, sowie einige Aspekte zur Reduktion von Gitterbasen verwendet. In diesem Abschnitt werden erst die benötigten mathematischen Methoden vorgestellt, anschließend der Algorithmus erläutert und dann noch einige Überlegungen zu dessen Korrektheit angestellt. Als Vorlage dienten [Hes99], [Hes02] und [Sch96]. In dem gesamten Abschnitt werden z und S so wie gerade beschrieben verwendet.

3.3.1 Mathematischer Aspekt

Gitter und Gitterreduktion

Dieser Abschnitt befasst sich mit den im Folgenden benötigten Grundlagen über Gitter. Weitere Details und Verallgemeinerungen von einigen Aussagen und Definitionen finden sich in [Sch96] und [Hes02].

Definition 3.3.1. *Sei $k = \mathbb{F}_q$ ein endlicher Körper, dann definiert man durch*

$$k((t^{-1})) := \left\{ \sum_{i=m}^{\infty} a_i t^{-i} \ | m \in \mathbb{Z},\, a_i \in k \right\}$$

den Körper der formalen Laurentreihen *in t^{-1} mit Koeffizienten aus k. Wir schreiben auch abkürzend $L := k((t^{-1}))$.*

$$V : k((t^{-1})) \to \mathbb{Z} \cup \{\infty\},\ \alpha = \sum_{i=m}^{\infty} a_i t^{-i} \mapsto \begin{cases} \infty & \alpha = 0, \\ min\{i \in \mathbb{Z} |\, a_i \neq 0\} & sonst \end{cases}$$

definiert eine surjektive Bewertung darauf.

Als den Grad eines Elementes *aus L bezeichnet man den Exponenten der höchsten auftauchenden t-Potenz. Es gilt $\deg(a) = -V(a)$ für alle $a \in L$. Analog zum Betrag definiert man*

$$|\,.\,| : L \to \mathbb{R}^{\geq 0},\ a \mapsto q^{\deg(a)}.$$

Definition 3.3.2. *Auf dem n-dimensionalen $k((t^{-1}))$ Vektorraum L^n definiert man für $v = (v_1, \ldots, v_n) \in L^n$ den* Spaltengrad *als*

$$\deg(v) = - \min_{i \in \{1,\ldots,n\}} V(v_i)$$

und

$$\|\,.\,\| : k((t^{-1}))^n \to \mathbb{R}^{\geq 0},\ v \mapsto q^{\deg(v)}.$$

Weiterhin definiert man

$$hc : L^n \to k^n,\ v = (\sum_{j=m_1}^{\infty} a_{1,j} t^{-j}, \ldots, \sum_{j=m_n}^{\infty} a_{n,j} t^{-j}) \mapsto (a_{1,-\deg(v)}, \ldots, a_{n,-\deg(v)}).$$

Diese Abbildung ordnet also einem Vektor aus L^n den Vektor der Koeffizienten der $\deg(v)$-ten t-Potenz zu oder null, wenn die Reihe ein niedrigeren Grad hat.

Bemerkung 3.3.3. *Die Abbildung* $\| \, . \, \|$ *definiert eine* Längenfunktion *auf* L^n. *Das bedeutet, sie erfüllt die Eigenschaften:*

- $\| \alpha \| = 0 \Leftrightarrow \alpha = 0$,
- $\| \lambda\alpha \| = |\lambda| \, \| \alpha \|$,
- $\| \alpha + \beta \| \leq max\{\| \alpha \|, \| \beta \|\}$.

Definition 3.3.4. *Sei* $z \in L$ *ein über* k *transzendentes Element mit* $\deg(z) > 0$. *Sei* $\Lambda \subseteq L^n$ *ein freier* $k[z]$*-Modul vom Rang* m *mit Basis* $\{v_1, \ldots, v_m\}$ *und seien die* v_i *sogar* L*-linear unabhängig. Dann bezeichnet man* Λ *als* $k[z]$-Gitter. *Das Maximum der Grade der* m*-Minoren von der durch die* v_i *induzierten Matrix bezeichnet man als die* Gitterdeterminante *von* Λ *in* L^n. *Als einen* Reduktionsschritt *bezeichnet man die Addition einer* $k[z]$*-Linearkombination der* v_j *zu einem* v_i , $i \neq j$, *so dass sich der Spaltengrad von* v_i *verringert.*

Bemerkung 3.3.5. *Da es aufgrund der Endlichkeit des Grundkörpers immer nur endlich viele Polynome von beschränktem Grad gibt, ist* $k[z] \subset L$ *eine diskrete Menge bezüglich der von der Gradbewertung induzierten Topologie. Damit ist die* L*-lineare Unabhängigkeit der Basis von* Λ *gleichbedeutend dazu, dass* Λ *diskret in* L^n *bezüglich* deg *ist.*

Definition 3.3.6. *Sei* $k[z]$ *ein Teilring von* L , $\Lambda \subset L^n$ *ein* $k[z]$*-Gitter. Dann bezeichnet man mit*

$$M_i(\Lambda, k[z], \deg) := min\{\lambda \in \mathbb{R} | \text{ Es existieren } k[z]\text{-linear unabhängige } a_1, \ldots, a_i \in \Lambda \text{ mit } \deg(a_j) \leq \lambda, \, 1 \leq j \leq i\}$$

das i-te sukzessive Minimum *von* Λ, *für* $i \in \{1. \ldots, n\}$.

Lemma 3.3.7. *Sei* $v_1, \ldots, v_m$ *die Basis eines* $k[z]$*-Gitters, dann sind die folgenden Bedingungen äquivalent:*

1. $\{hc(v_i) \,|\, 1 \leq i \leq m \wedge \deg(v_i) \equiv j \mod \deg(z)\}$ *ist eine* k*-linear unabhängige Menge im* k^n *für alle* $0 \leq j < \deg(z)$,
2. $\deg(\sum_{i=1}^{m} \lambda_i v_i) = \max_{i=1,\ldots,m} \deg(\lambda_i v_i)$ *für alle* $\lambda_i \in k[z]$, $1 \leq i \leq m$,
3. *Die Elemente* $v_1, \ldots, v_m$ *realisieren die sukzessiven Minima des Gitters.*

Beweis. Eine Beweisskizze findet sich in [Hes02]. □

Eine Basis, die diese Bedingungen erfüllt, bezeichnet man als reduzierte Basis. An Bedingung (2) sieht man, dass bei einer solchen kein Reduktionsschritt mehr durchgeführt werden kann. Sind umgekehrt diese Bedingungen nicht erfüllt, so lässt sich immer ein Reduktionsschritt durchführen. Im Folgenden werde ich einen Algorithmus vorstellen, der aus einer Gitterbasis eine reduzierte Gitterbasis berechnet. Vorher muss aber noch gezeigt werde, wie Gitterbasen mit den Basen bestimmter holomorpher Ringe in Verbindung gebracht werden können.

Bewertete Körper, Reihenentwicklungen und lokale Uniformisierende

Definition 3.3.8. *Sei P eine Stelle von F, $\mathcal{O}_P$ der Bewertungsring und v_P die dazugehörige Bewertung. Dann bezeichnet man ein Element $\pi \in F$ als* lokale Uniformisierende *von P wenn gilt: $P = \pi\mathcal{O}_P$. Ein Element $\pi \in F$ ist genau dann lokale Uniformisierende von P, wenn es $v_p(\pi) = 1$ erfüllt.*

Definition 3.3.9. *Sei T ein Körper und $v : T \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung darauf. Eine Folge $(x_n) \in T^{\mathbb{N}}$ heißt* konvergent, *wenn es ein $x \in T$ gibt, so dass für alle $c \in \mathbb{R}$ ein $n_0 \in \mathbb{N}$ existiert, mit $v(x - x_n) \geq c$ für alle $n \geq n_0$. Man bezeichnet (x_n) als* Cauchyfolge, *wenn gilt : für alle $c \in \mathbb{R}$ existiert ein $n_0 \in \mathbb{N}$ mit $v(x_n - x_m) \geq c$ für alle $n, m \geq n_0$.*

Definition 3.3.10. *Ein Körper T zusammen mit einer diskreten Bewertung v heißt* vollständig, *wenn jede Cauchyfolge bezüglich v in T konvergiert. Für einen beliebigen bewerteten Körper (T, v) definiert man die* Vervollständigung *bezüglich v als bewerteten Körper $(\hat{T}, \hat{v})$, für den gilt:*

1. *$T \subseteq \hat{T}$ und v ist die Einschränkung von $\hat{v}$ auf T,*
2. *$\hat{T}$ ist vollständig bezüglich $\hat{v}$,*
3. *T liegt dicht in $\hat{T}$.*

Theorem 3.3.11. *Die Vervollständigung eines bewerteten Körpers existiert und ist eindeutig bis auf isometrische Isomorphie.*

Beweis. In [Lor90, S.62] ist diese Aussage bewiesen. □

Definition 3.3.12. *Sei F ein Funktionenkörper und P eine Stelle. Die Vervollständigung von F bezüglich v_P nennt man die P-*adischen Vervollständigung von *F. Diese bezeichnet man mit $\hat{F}_P$ und die Bewertung wieder mit v_P.*

Theorem 3.3.13. *Sei $P \in \mathbb{P}_F$ eine Stelle vom Grad eins mit lokaler Uniformisierender π. Dann hat jedes Element $z \in \hat{F}_P$ eine eindeutige Darstellung der Form*

$$z = \sum_{i=n}^{\infty} a_i \pi^i \text{ mit } n \in \mathbb{Z}, \quad a_i \in k.$$

Beweis. Ein Beweis findet sich in [Sti93, S.143]. □

Man kann also Elemente des Funktionenkörpers mit Laurentreihen identifizieren.

Definition 3.3.14. *Sei P eine Stelle vom Grad eins von F und π eine lokale Uniformisierende von P. Dann definiere*

$$\iota_{\pi,P} : F \to \hat{F}_P$$

als die Abbildung, die jedem Funktionenkörperelement seine Reihenentwicklung in der entsprechenden lokalen Uniformisierenden zuordnet.

Theorem 3.3.15. *Sei (K, v) ein bewerteter Körper und F/K eine separable, endliche Körpererweiterung vom Grad n mit definierendem Polynom $g \in K[T]$. Dann gilt:*

1. *Es gibt eine Fortsetzung von v zu einer Bewertung auf F.*

2. *Es gibt höchstens n verschiedene Fortsetzungen von v zu Bewertungen auf F.*

3. *Die Faktorisierung von g über der Vervollständigung $\hat{K}$ von K bezüglich v korrespondiert zu den verschiedenen Fortsetzungen von v auf F. Das heißt, falls $g = g_1 \dots g_s$ die Faktorisierung von g über $\hat{K}$ in irreduzible Polynome vom Grad $\deg(g_i) = n_i$ ist, kann man v zu s verschiedenen Bewertungen $v_1, \dots, v_s$ auf F fortsetzen und es gilt $n_i = e_i f_i$ wobei e_i der Verzweigungsindex und f_i der Trägheitsgrad der Bewertungsfortsetzung v_i ist.*

4. *Seien $v_1, \dots, v_s$ alle verschiedenen Fortsetzungen von v auf F und sei $\hat{F}_i$ die Vervollständigung von F bezüglich v_i für $i \in \{1, \dots, s\}$. Dann gilt $\hat{F}_i \cong \hat{K}[T]/g_i$. Weiterhin bekommt man einen Isomorphismus*

$$\Psi : F \otimes_K \hat{K} \to \prod_{i=1}^{s} \hat{F}_i.$$

Beweis. Für einen Beweis siehe [Lor90, S.77]. □

Korollar 3.3.16. *Sei F ein Funktionenkörper, P eine Stelle und $z \in F$ ein separierendes Element mit $v_P(z) = -n$. Dann ist $\hat{F}_P$ ein $n \cdot \deg(P)$-dimensionaler $k((z^{-1}))$-Vektorraum.*

Beweis. Die Behauptung folgt direkt aus Theorem 3.3.15, wenn man F als endliche Erweiterung von $k(z)$ betrachtet. Dann ist P eine Fortsetzung der ∞-Bewertung auf $k(z)$. Der Abschluss von $k(z)$ bezüglich der ∞-Bewertung ist $k((z^{-1}))$ also $\hat{F}_{P_i} \cong k((z^{-1}))[T]/g$ für ein geeignetes $g \in k((z^{-1}))[T]$. □

Holomorphe Ringe und Ganzheitsbasen

Definition 3.3.17. *Ein* Teilring *des Funktionenkörpers F/k ist ein Ring R mit $k \subseteq R \subseteq F$, der kein Körper ist.*

Theorem 3.3.18. *Sei $\mathcal{O}_S$ ein holomorpher Ring von F/k. Dann gilt:*

1. *$\mathcal{O}_S$ ist ein Teilring von F/k,*

2. *F ist der Quotientenkörper von $\mathcal{O}_S$,*

3. *$\mathcal{O}_S$ ist ganz abgeschlossen.*

Beweis. Dieser Satz ist in [Sti93, S.68] bewiesen. □

Theorem 3.3.19. *Sei R ein ganz abgeschlossener Teilring von F/k, dessen Quotientenkörper F ist. Sei F'/F eine endliche separable Erweiterung vom Grad n. Sei $R' = Cl(R, F')$ der ganze Abschluss von R in F'. Dann gilt:*

1. *Für jede Basis $\{x_1, \ldots, x_n\}$ von F'/F gibt es Elemente $a_i \in R\backslash\{0\}$, sodass gilt $a_1x_1, \ldots, a_nx_n \in R'$.*
2. *Ist $\{z_1, \ldots, z_n\} \subseteq R'$ eine Basis von F'/F und $\{z_1^*, \ldots, z_n^*\}$ die bezüglich der Spur duale Basis, so gilt:*
$$\sum_{i=1}^{n} Rz_i \subseteq R' \subseteq \sum_{i=1}^{n} Rz_i^*.$$
3. *Ist R sogar ein Hauptidealring, dann gibt es eine Basis $\{u_1, \ldots, u_n\}$ von F'/F mit*
$$R' = \sum_{i=1}^{n} Ru_i.$$

Beweis. Für einen Beweis siehe [Sti93, S.73]. □

Korollar 3.3.20. *Sei $z \in F\backslash k$, $S := \text{Supp}\ ((z)_\infty)$. Dann ist $\mathcal{O}^S$ ein freier $k[z]$-Modul vom Rang $\deg(z)_\infty$.*

Beweis. Es genügt zu zeigen, dass die Voraussetzungen von 3.3.19 erfüllt sind. Dazu betrachtet man F als Erweiterung von $k(z)$. Dann gilt: $[F : k(z)] = \deg(z)_\infty$ und $k[z]$ ist per Definition ein Teilring von $k(z)$, dessen Quotientenkörper $k(z)$ ist. Als holomorpher Ring der Form $\mathcal{O}_Q$ mit $Q = \mathbb{P}_{k(z)}\backslash\{\infty\}$ ist $k[z]$ ganz abgeschlossen. Weiterhin ist $k[z]$ als Polynomring in einer Variablen über einem Körper ein Hauptidealring. S entspricht dann genau der Menge aller Stellen von F, die über der ∞-Stelle von $k(z)$ liegen, also gilt $\mathcal{O}^S = Cl(k[z], F)$ □

Zusammenhang zwischen holomorphen Ringen und geeigneten Gittern

In diesem Abschnitt identifizieren wir $\mathcal{O}^S$ mit einem geeigneten $k[z]$-Gitter.

Theorem 3.3.21. *Sei F ein Funktionenkörper, $S \subseteq \mathbb{P}_F$ und $\mathcal{O}^S$ ein holomorpher Teilring. Dann kann man $\mathcal{O}^S$ mit einem Gitter in einem geeigneten Vektorraum identifizieren.*

Beweis. Nach den Vorüberlegungen wissen wir, dass $\mathcal{O}^S$ für ein geeignetes $z \in F$ ein freier $k[z]$-Modul ist. Sei also $\omega_1, \ldots, \omega_n$ eine Basis und gelte $(z)_\infty = e_1P_1 + \ldots + e_sP_s$. Nun betrachten wir F als eine Erweiterung von $k(z)$ mit definierendem separablen Polynom g vom Grad n. Offensichtlich gilt $n = [F : k(z)] = \sum_{i=1}^{s} e_i \deg(P_i)$. Sei weiterhin $g = g_1 \ldots g_s$ die Faktorisierung von g über $k((z^{-1}))$. Nach Korollar 3.3.16 wissen wir, dass $\hat{F}_{P_i}$ für $i \in \{1, \ldots, s\}$ ein n_i-dimensionaler $k((z^{-1}))$-Vektorraum ist, mit $n_i = \deg(g_i)$. Fixiert man Basen $b_{i,1}, \ldots, b_{i,n_i}$, so bekommt man Vektorraumisomorphismen

$$\Psi_i : k((z^{-1}))^{n_i} \longrightarrow \hat{F}_{P_i} \quad (\alpha_1, \ldots, \alpha_{n_i}) \mapsto \sum_{j=1}^{n_i} \alpha_j b_{i,j}.$$

Weiterhin haben wir die Inklusionen $\iota_{P_i} : F \to \hat{F}_{P_i}$. Zusammen ergibt das eine Abbildung

$$\Gamma : F \to k((z^{-1}))^n \quad \alpha \mapsto (\Psi_1^{-1}(\iota_{P_1}(\alpha)), \ldots, \Psi_s^{-1}(\iota_{P_s}(\alpha))^t.$$

Als Nächstes ist zu zeigen, dass die Bilder der ω_i unter Γ $k((z^{-1}))$-linear unabhängig sind. Sei also $a_1, \ldots, a_n \in k((z^{-1}))$ mit

$$\sum_{i=1}^{n} a_i \begin{pmatrix} \Psi_1^{-1}(\iota_{P_1}(\omega_i)) \\ \vdots \\ \Psi_s^{-1}(\iota_{P_s}(\omega_i)) \end{pmatrix} = 0.$$

Da $k(z) \subset k((z^{-1}))$ kann man $\{1, \rho, \ldots, \rho^{n-1}\}$ durch eine $k((z^{-1}))$-unimodulare Transformation der ω_i darstellen, wobei ρ eine Nullstelle von g ist. Unter Verwendung der $k((z^{-1}))$-Linearität von den Ψ_i liefert dieses $\tilde{a}_1, \ldots, \tilde{a}_n \in k((z^{-1}))$, so dass

$$\sum_{i=1}^{n} \tilde{a}_i \begin{pmatrix} \iota_{P_1}(\rho^{i-1}) \\ \vdots \\ \iota_{P_s}(\rho^{i-1}) \end{pmatrix} = 0.$$

Betrachtet man nun das Polynom $\sum_{i=1}^{n} \tilde{a}_i T^{i-1} \in k((z^{-1}))[T]$, so sieht man, dass es einen Grad kleiner n hat. Alle n verschiedenen Nullstellen ρ_i von g liefern jedoch auch Nullstellen dieses Polynoms. Es handelt sich also um das Nullpolynom und somit gilt $\tilde{a}_1 = \ldots = \tilde{a}_n = 0$ und folglich $a_1 = \ldots = a_n = 0$.
Unter Verwendung von Γ kann man eine skalare Multiplikation von den $\Gamma(\omega_i)$ mit Elementen aus $k[z]$ definieren. Dadurch wird $\Lambda := \bigoplus_{i=1}^{n} k[z] \cdot \Gamma(\omega_i)$ ein $k[z]$-Gitter in $k((z^{-1}))^n$. Sei $e = kgV(e_1, \ldots, e_s)$, dann induzieren die zu P_i gehörigen Bewertungen v_i auf F durch

$$\deg(.) := -\min_{i=1}^{s} e \cdot v_i(\Gamma^{-1}(.))/e_i$$

eine Gradfunktion auf Λ. □

Für die algorithmische Durchführung kann man sogar noch etwas mehr zeigen:

Lemma 3.3.22. *Sei die Situation wie in Theorem 3.3.21, sei ρ eine Nullstelle von g in $\overline{k(z)}$ und seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen Einbettungen von F in den algebraischen Abschluss $\overline{k((z^{-1}))}$ von $k((z^{-1}))$. Dann gilt:*

1. *$\sigma : F \longrightarrow \overline{k((z^{-1}))}^n$, $\alpha \mapsto (\sigma_1(\alpha), \ldots, \sigma_n(\alpha))$ liefert eine Abbildung, mit der man $\mathcal{O}^S$ mit einem $k[z]$-Gitter in $k((z^{-1}))^n$ eingebettet in $\overline{k((z^{-1}))}^n$, identifizieren kann. Diese Identifikation entspricht der in 3.3.21 durch Γ beschriebenen durch eine spezielle Basenwahl.*

2. *Es gibt eine Partition der Menge $\{\sigma_i(F) \mid i \in \{1, \ldots, n\}\}$ in s Teilmengen $\{F_{1,1}, \ldots, F_{1,n_1}\}, \ldots, \{F_{s,1}, \ldots, F_{s,n_s}\}$, so dass $F_{j,k}$ und $F_{j,l}$ für alle $1 \leq j \leq s$ $1 \leq k, l \leq n_j$ isometrisch isomorph sind. Diese Teilmengen stehen kanonisch in Bijektion zu $\{P_1, \ldots, P_s\}$.*

3. *Sei nun $\mathcal{O}^S$ wie beschrieben mit einem Gitter identifiziert. Ein Reduktionsschritt, der den Grad der l-ten Komponente eines Gittervektors reduziert, reduziert auch automatisch den aller Komponenten, die zu derselben Stelle P_j gehören.*

Beweis. Die σ_i sind jeweils durch ihr Bild auf ρ festgelegt. Dieses ist eine Nullstelle ρ_i von g in $\overline{k((z^{-1}))}$. Ganz analog zum Beweis von Theorem 3.3.21 zeigt man, dass man so wirklich ein Gitter bekommt. Unter Verwendung des Zusammenhanges zwischen der Faktorisierung von g über $k((z^{-1}))$ und den Stellen von F, die über der ∞-Stelle von $k(z)$ liegen, bekommt man die in (2) beschriebene Partition, indem man einfach definiert, dass $\sigma_i(F)$ und $\sigma_j(F)$ genau dann in derselben Teilmenge sind, wenn ρ_i und ρ_j Nullstellen desselben irreduziblen Faktors von g sind. Aufgrund der Eindeutigkeit der Vervollständigung eines bewerteten Körpers ergibt sich die isometrische Isomorphie. Aus dieser folgt auch (3). Sei nämlich $\sum_{j=1}^{n} \lambda_j \sigma(\omega_j)$ mit $\lambda_i \in k[z]$ ein Reduktionsschritt, welcher den Grad von $\sigma(\omega_1)$ an der l-ten Komponente reduziert und gehöre die k-te Komponente zu derselben Stelle. Sei weiterhin $\tau : \sigma_l(F) \longrightarrow \sigma_k(F)$ ein isometrischer Isomorphismus. Dann liefert zeilenweises Betrachten der l-ten und der k-ten Komponente jeweils eine $k[z]$-Linearkombination von Reihen in den entsprechenden lokalen Uniformisierenden. Da τ $k((z^{-1}))$-linear ist, also auch $k[z]$ fix lässt und die eine lokale Uniformisierende auf die andere abbildet, kann man auch sagen, dass die k-te Komponente das Bild der l-ten unter τ ist. Folglich haben sie auch denselben Grad. □

Wenn man also nur eine reduzierte Gitterbasis berechnen möchte, braucht man sich gar nicht alle Zeilen anzusehen. Wegen 3.3.22 reicht es, für jede Stelle P_i eine Zeile zu betrachten. Weiterhin sei hier angenommen, dass alle Stellen in S den Grad eins haben. Das ist zwar eine starke Einschränkung, die nach den Vorüberlegungen nicht notwendig ist. Im 6. Abschnitt dieses Kapitels wird aber gezeigt, wie man diese Einschränkung algorithmisch gut umgehen kann. Das führt zu folgenden Abbildungen, welche letztlich auch in dem Algorithmus verwendet werden:

Definition 3.3.23. *Sei für $i \in \{1, \ldots, s\}$ π_i eine lokale Uniformisierende von P_i Definiere wie folgt:*

1. $\bar{\cdot} : F \to \overline{k((z^{-1}))}^s$, $\alpha \mapsto (\iota_{\pi_1,P_1}(\alpha), \ldots, \iota_{\pi_s,P_s}(\alpha))$
2. *$hc : \bar{F} \to \mathbb{F}_q^s$ die Abbildung die einen Gittervektor v auf den Vektor seiner $\deg(v)$-ten Koeffizienten abbildet.*

Bemerkung 3.3.24. *Aufgrund der Annahme, dass alle Stellen in S den Grad eins haben, bildet die Abbildung hc in einen s-dimensionalen Vektorraum über dem Konstantenkörper ab.*

Damit kann man den Begriff reduziert auch auf Ganzheitsbasen holomorpher Ringe in Funktionenkörpern übertragen:

Definition 3.3.25. *Sei $\mathcal{O}^S$ ein holomorpher Ring mit $k[z]$-Basis $\mathcal{B} = \{\omega_1, \ldots, \omega_n\}$. Dann bezeichnet man $\mathcal{B}$ als* reduziert*, wenn $\mathcal{B}$ über die oben beschriebenen Abbildungen zu einer reduzierten Gitterbasis korrespondiert.*

Theorem 3.3.26. *Sei D ein Divisor des Funktionenkörpers F/k, z ein separierendes Element mit $S = Supp((z)_\infty)$ und $n = [F : k(z)]$. Dann existieren ganze Zahlen*

$d_1 \geq \ldots \geq d_n$ und $v_1, \ldots, v_n \in F$, so dass die Menge

$$\{z^j v_i \,|\, 1 \leq i \leq n\,, 0 \leq j \leq d_i + r\}$$

eine k Basis von $\mathcal{L}(D+r(z)_\infty)$ für alle $r \in \mathbb{Z}$ darstellt. Der für uns interessante Spezialfall ergibt sich für $D = 0$. Eine Basis dieser Art bezeichnet man als $\mathbb{Z}$-parametrisierte Basis von D

Beweis. Ein Beweis befindet sich in [Hes02]. □

Einen Zusammenhang zwischen einer $\mathbb{Z}$-parametrisierten Basis und reduzierten Gitterbasen stellt der folgende Satz dar:

Theorem 3.3.27. *Die Elemente $v_1, \ldots, v_n \in F$ bilden eine $\mathbb{Z}$-parametrisierte Basis des Nulldivisors, wenn sie eine reduzierte Basis des entsprechenden Gitters bilden.*

Beweis. Diese Aussage ist in [Hes02] bewiesen. □

3.3.2 Algorithmischer Aspekt

Idee des Algorithmus

Wir wissen nun nach den Vorüberlegungen, dass es zu dem Riemann-Roch-Raum $\mathcal{L}(m(z)_\infty)$ Elemente $v_1, \ldots, v_n \in F$ und $d_1, \ldots, d_n \in \mathbb{Z}$ gibt, für die die Menge

$$\{z^j v_i \mid 1 \leq i \leq n,\ 0 \leq j \leq d_i + m\}$$

eine Basis von $\mathcal{L}(m(z)_\infty)$ bildet. Umgekehrt bedeutet das, startet man mit einer ausreichend großen beliebigen Basis von $\mathcal{L}(m(z)_\infty)$ und identifiziert diese via $\bar{\cdot}$ mit dem Erzeugendensystem eines Gitters in L^n, so kann man darauf einen Algorithmus zur Berechnung einer reduzierten Gitterbasis anwenden, um die v_i zu bestimmen. Ausreichend groß bedeutet in diesem Zusammenhang, dass $v_i \in \mathcal{L}(m(z)_\infty)$ für alle $i \in \{1, \ldots, n\}$, was eine Grundvoraussetzung dafür ist, dass man durch Reduktion wirklich alle v_i aus einer Basis von $\mathcal{L}(m(z)_\infty)$ berechnen kann.

Lemma 3.3.28. *Sei $n = \deg(z)_\infty$ und $m \in \mathbb{N}$. Gilt $\dim m(z)_\infty - \dim (m-1)(z)_\infty = n$, so sind alle v_i in $\mathcal{L}(m(z)_\infty)$ enthalten. Weiterhin gilt: Es gibt ein $m \in \mathbb{N}$, so dass diese Bedingung erfüllt ist.*

Beweis. Es gilt $\mathcal{L}((m-1)(z)_\infty) \subseteq \mathcal{L}(m(z)_\infty)$. Wenn sich die Dimensionen um n unterscheiden, dann gibt es n linear unabhängige Vektoren in $\mathcal{L}(m(z)_\infty)$, die nicht in $\mathcal{L}((m-1)(z)_\infty)$ liegen. Folglich ist die Menge $\{z^{d_1+m}v_1, \ldots, z^{d_n+m}v_n\}$ n-elementig und somit gilt $d_i + m \geq 0$ für alle $i \in \{1, \ldots, n\}$, also liegen auch alle v_i in $\mathcal{L}(m(z)_\infty)$. Um so ein m zu bekommen, reicht es, dieses so zu wählen, dass $\deg(m-1)(z)_\infty \geq 2g-2$ erfüllt ist, wobei g das Geschlecht von F bezeichnet. Dann gilt nämlich $\dim m(z)_\infty - \dim (m-1)(z)_\infty = \deg(z)_\infty = n$. □

Die Bedingung des Lemmas lässt sich algorithmisch durch das Berechnen der Dimensionen einiger Riemann-Roch-Räume relativ leicht überprüfen.

Pseudocode

Algorithmus 3 Basis von $\mathcal{O}^S$

Input: Funktionenkörper F, $z \in F$ mit $Supp((z)_\infty) = S$.
Output: Eine $k[z]$-Basis $\omega_1, \ldots, \omega_n$ von $\mathcal{O}^S$.

1: Berechne $(z)_\infty = e_1 P_1 + \ldots + e_s P_s$.
2: $e := kgV(e_i)$, $S := \{P_1, \ldots, P_s\}$.
3: Berechne $m \in \mathbb{N}$ so dass die Bedingung von Lemma 3.3.28 erfüllt ist.
4: Berechne Basis $\mathcal{B} = \{b_1, \ldots, b_l\}$ von $\mathcal{L}(m(z)_\infty)$.
5: Berechne $A := \{\psi_1, \ldots, \psi_l\} := \{\bar{b_1}, \ldots, \bar{b_l}\}$.
6: $T := Id_n(k[z])$.
7: **repeat**
8: fertig= $TRUE$.
9: **for** $\kappa = 0, \ldots, e-1$ **do**
10: Sortiere A aufsteigend gemäß dem Spaltengrad und bezeichen die dafür notwendige Permutationsmatrix mit T_0.
11: $T := TT_0$.
12: Berechne $\tilde{A} = \{\psi_i \,|\, i \in \{1, \ldots, n\} \text{ und } \deg(\psi_i) \equiv \kappa \mod e\}$ die Menge der Elemente deren Spaltengrad mod e gleich ist mit Indexmenge $\{i_1, \ldots, i_r\}$.
13: **if** $r := \#\tilde{A} \geq 2 \wedge (hc(\psi_i) \,|\, \psi_i \in \tilde{A}\}$ ist linear abhängig) **then**
14: Berechne $j \in \{1, \ldots, r\}$ und $(0, \ldots, 0, \alpha_j, \ldots, \alpha_r) \in k^n$ mit $\sum_{m=j}^{r} \alpha_m hc(\psi_{i_m}) = 0$.
15: $\xi := \psi_{i_j} + \sum_{m=j+1}^{r} \alpha_m z^{(\deg(\psi_{i_m}) - \deg(\psi_{i_j}))/e} \psi_{i_m}$ und berechne als T_1 die Matrix die diese Transformation beschreibt.
16: $\psi_{i_j} := \xi$, $T := TT_1$, fertig $= FALSE$.
17: **end if**
18: **end for**
19: **until** fertig= $TRUE$
20: Berechne $(\omega_1, \ldots, \omega_n, 0, \ldots, 0) = (b_1, \ldots, b_l)T$.
21: Gebe $\omega_1, \ldots, \omega_n$ zurück.

Technische Probleme

Dieser Algorithmus basiert darauf, mit den Reihenentwicklungen der zu reduzierenden Basis des Riemann-Roch-Raums zu rechnen. Daher muss man sich überlegen, welche Präzision bei den Reihen benötigt wird. Da alle auftretenden Elemente nur Pole an den Stellen aus S haben, ist es notwendig für jede Reihe zumindest den gesamten Hauptteil zu kennen, um entscheiden zu können, ob ein durch einen Reihenvektor beschriebenes Element null ist. Das ist nämlich der Fall, wenn es an keiner der Stellen aus S einen Pol hat, aber mindestens eine Nullstelle. Entwickelt man die Elemente mit einer Präzision, die größer ist als das Negative der minimalen Bewertung an den Stellen aus S, so kann man sicher stellen, dass alle Hauptteile bekannt sind. Problematisch ist nur, dass z eine negative Bewertung an allen Stellen von S hat.

Daher verliert man Präzision, wann immer man mit z multipliziert, was im Verlauf des Algorithmus häufiger passieren kann. Wenn man verlangt, dass bei den in den Vektoren auftauchenden Reihen die Hauptteile vollständig bekannt sind, so hat man zwei Möglichkeiten:

1. Man kann bei dem Berechnen der Reihenentwicklungen mit einer so hohen Präzision arbeiten, dass man selbst nach der maximalen Anzahl von Multiplikationen mit z noch auf den Hauptteilen exakt ist.

2. Man berechnet die Reihenentwicklungen nur so weit wie nötig. Im Verlauf des Algorithmus prüft man regelmäßig, ob durch eine weitere Multiplikation mit z zu viel Präzision verloren ginge. Sollte dies der Fall sein, so berechnet man die neue Basis, die man durch das Ausführen der bisherigen Reduktionsschritte bekommt. Anschließend ruft man den Algorithmus mit der neuen Basis als Input auf und in diesem werden wieder die Reihenentwicklungen mit ausreichender Präzision neu bestimmt.

Beide Methoden haben Vor- und Nachteile. Bei der Implementation habe ich mich für die zweite entschieden. Zwar muss man hier möglicherweise häufiger die Reihenentwicklungen berechnen, dafür gehen alle Rechenschritte deutlich schneller, da man mit kürzeren Reihen rechnen kann.

Überlegungen zur Korrektheit

Theorem 3.3.29. *Sei $\omega_1, \ldots, \omega_n \in \mathcal{O}^S$ eine Ganzheitsbasis. Dann lässt sich aus dieser durch endlich viele Schritte eine reduzierte Ganzheitsbasis berechnen.*

Beweis. Ein detaillierter Beweis findet sich bei [Sch96, S.33]. Die Idee ist, erst die Existenz einer reduzierten Basis des Gitters zu zeigen. Anschließend zeigt man, dass jeder Schritt des Algorithmus den Grad eines Gittervektors verringert. Die Gitterdeterminante aber, welche eine von der Basis unabhängige Invariante des Gitters ist, liefert eine untere Schranke für die Grade. Folglich ist man nach endlich vielen Schritten bei einer reduzierten Gitterbasis angekommen. □

Dieser Satz beweist, dass der beschriebene Algorithmus bei korrektem Input nach endlich vielen Schritten terminiert und eine reduzierte Ganzheitsbasis liefert.

Berechnung der Darstellung von Elementen in der Basis

Nun haben wir gezeigt, wie man zu einem holomorphen Teilring $\mathcal{O}^S$ und einem geeigneten Element $z \in \mathcal{O}^S$ eine Basis $y_1, \ldots, y_l$ berechnen kann, so dass $\mathcal{O}^S$ zu einem freien $k[z]$-Modul wird. Es verbleibt die Frage, wie man für Elemente a des Funktionenkörpers $F = k(x, y)$, die in diesem Teilring liegen, eine Darstellung in der Basis berechnen kann. Wir nehmen an, wir sind für beliebige Elemente $a_1, \ldots, a_n \in F$ in der Lage effizient zu ermitteln, ob diese k-linear abhängig sind und wie die Koeffizienten einer nicht trivialen k-Linearkombination $\mu_1 a_1 + \ldots + \mu_n a_n = 0$ aussehen. Für diese Berechnungen wird nur das Lösen linearer Gleichungssysteme benötigt. Sei nun $a \in \mathcal{O}^S$ gegeben. Dann untersuchen wir die Mengen $U_i := \{a, z^j y_1, \ldots, z^j y_l \,|\, 0 \leq j \leq i\}$ für größer werdendes i auf lineare Abhängigkeit. Da $a \in \mathcal{O}^S$ ist, gibt es Polynome $p_1, \ldots, p_l \in k[T]$ mit $a = p_1(z)y_1 + \ldots + p_l(z)y_s$. Sei $i_{max} = \max_{j=1}^{l} \deg(p_j)$. Dann ist $U_{i_{max}}$ linear abhängig. Löst man $0 = \mu a + \sum_{i=1}^{l} \sum_{j=0}^{i_{max}} \mu_{i,j} z^j y_i$ nach a auf und fasst die Koeffizienden gleicher y_i zusammen, erhält man die gewünschte Darstellung.

3.4 Eigenschaften der x_i

3.4.1 Mathematischer Aspekt

Definition 3.4.1. *Sei F ein Funktionenkörper und $P \in \mathbb{P}_F$ eine Stelle vom Grad eins. Ein $n \in \mathbb{Z}$, $n \geq 0$ wird* Polzahl *von P genannt, wenn es ein $x \in F$ gibt, mit $(x)_\infty = nP$. Sollte es kein solches Element geben, so bezeichnet man n als* Fehlzahl *von P.*

Offensichtlich bilden die Polzahlen eine additive Unterhalbgruppe von $\mathbb{N}$. Diese Unterhalbgruppe bezeichnet man auch als die Polfolge von P.

Lemma 3.4.2. *Sei U eine Unterhalbgruppe von $\mathbb{N}$, dann ist U endlich erzeugt.*

Beweis. Sei n_1 das betraglich kleinste Element von U, dann gibt es modulo n_1 genau n_1 verschiedene Reste $0, 1, \ldots, n_1 - 1$. Seien nun $n_2, \ldots, n_r$ die betraglich kleinsten Elemente von U, die diese Reste realisieren, falls sie existieren. Diese Elemente $\{n_1, \ldots, n_r\}$ bilden nun ein Erzeugendensystem von U, denn für ein beliebiges Element $a \in U$ existiert ein n_i mit $a \equiv n_i \mod n_1$. Folglich ist a als Summe von n_i und einem Vielfachen von n_1 darstellbar. Nach Konstruktion erfüllt dieses Erzeugendensystem die Bedingung $n_i \not\equiv n_j \mod n_1$ für $1 \leq i < j$, $1 \leq j \leq r$. □

Theorem 3.4.3 (Fehlzahlsatz)**.** *Sei F ein Funktionenkörper vom Geschlecht g und P eine Stelle vom Grad eins. Dann besitzt P genau g Fehlzahlen $i_1 < \ldots < i_g$ und es gilt $g_1 = 1$ und $i_g \leq 2g - 1$.*

Beweis. Ein Beweis lässt sich in [Sti93, S.32] finden. □

Lemma 3.4.4. *Sei F ein Funktionenkörper und P eine Stelle von F vom Grad eins. Sei U die Polfolge von P und $\{n_1, \ldots, n_r\}$ ein Erzeugendensystem wie aus dem vorherigen Lemma. Seien $\{x_1, \ldots, x_r\} \subset F$ Elemente mit $(x_i)_\infty = n_i P$ für alle $i \in \{1, \ldots, r\}$. Dann ist $\{1, x_2, \ldots, x_r\}$ eine Basis des freien $k[x_1]$-Moduls $\mathcal{O}^P$. Weiterhin gilt $r = n_1$.*

Beweis. Nach Korollar 3.3.20 wissen wir, dass es sich bei $\mathcal{O}^S$ um einen freien x_1-Modul vom Rang n_1 handelt. Wir betrachten $\{x_1, \ldots, x_r\}$ und identifizieren diese mit einer Gitterbasis. Aufgrund der mod n_1 verschiedenen Bewertungen der x_i an P ist Bedingung (1) von 3.3.7 erfüllt. Also hat man schon eine reduzierte Gitterbasis und daher bilden $\{x_1, \ldots, x_r\}$ auch eine $k[x_1]$-Basis von $\mathcal{O}^S$. □

Korollar 3.4.5. *Seien Elemente $x_1, \ldots, x_r$ wie im vorherigen Lemma gewählt. Dann gilt:*

$$F = k(x_1, \ldots, x_r).$$

Beweis. Dieses Korollar folgt direkt aus der Tatsache, dass $\{1, x_2, \ldots, x_r\}$ eine $k[x_1]$-Basis von $\mathcal{O}^P$ ist und $F = Quot(\mathcal{O}^P)$ gilt. Es gilt sogar: jedes Element $a \in F$ besitzt eine Darstellung $a = f/g$ mit $f, g \in \bigoplus_{b \in \{1, x_2, \ldots, x_r\}} k[x_1]b$. □

Definition 3.4.6. *Seien $x_1, \ldots, x_r \in F$. Als* algebraische Relation *der x_i bezeichnet man eine nichttriviale algebraische Kombination der Null, das heißt ein $p \in k[t_1, \ldots, t_r]$ mit $p(x_1, \ldots, x_r) = 0$ und $p \neq 0$.*

Lemma 3.4.7. *Die Menge der algebraischen Relationen zwischen den Elementen $x_1, \ldots, x_r$ eines Funktionenkörpers bildet ein Ideal I in dem Polynomring $k[t_1, \ldots, t_r]$. Für dieses Ideal kann man einfach ein Erzeugendensystem E der Form*

$$E = \{t_i t_j - p_{1,i,j}(t_1) - \sum_{k=2}^{r} p_{k,i,j}(t_1) t_k \mid i,j \in \{1,\ldots,r\},\ p_{k,i,j} \in k[t_1] \text{ geeignet } \}$$

berechnen.

Beweis. Als Kern des Einsetzhomomorphismus $\Psi : k[t_1, \ldots, t_r] \to k(x_1, \ldots, x_r)$ ist die Menge I ein Ideal. Der zweite Teil folgt aus den folgenden beiden Beobachtungen:

1. Wegen der mod n_1 unterschiedlichen Bewertungen der x_i, sind Ausdrücke der Form $p_1(x_1)+p_2(x_1)x_2+\ldots+p_r(x_1)x_r$ genau dann null, wenn alle p_i gleich null sind. Denn für $p_i \neq 0$ unterscheiden sich die Bewertungen aller Summanden und somit ist deren Summe wegen der ultrametrischen Dreiecksungleichung ungleich null.

2. Wir wissen, dass $\mathcal{O}^S$ ein freier $k[x_1]$-Modul ist. Da $x_i x_j$ in $\mathcal{O}^S$ liegt, gibt es eine eindeutige Basisdarstellung mit Koeffizienten aus $k[x_1]$:

$$x_i x_j = p_{1,i,j}(x_1) + \sum_{k=2}^{r} p_{k,i,j}(x_1) x_k,\ i,j \in \{1,\ldots,r\}.$$

Wählt man die $p_{i,j,k}$ so wie in (2) beschrieben, so liegen alle Elemente aus E offensichtlich in I. Sei nun $a \in I$ beliebig. Mit Hilfe der Ausdrücke aus E kann man in a alle Produkte von t_i und t_j durch Summen ersetzen, in denen solche nicht mehr auftauchen. Dadurch hat man sie auf eine Form wie in (1) gebracht, woraus die Behauptung folgt. □

3.4.2 Algorithmischer Aspekt

Das Berechnen von Elementen $x_1, \ldots, x_j$ mit den oben beschriebenen Eigenschaften ist algorithmisch recht einfach. Dazu berechnet man iterativ die Dimension größer werdender Riemann-Roch-Räume der Form $\mathcal{L}(kP)$ und deren Basis und bekommt so die n_i und die x_i.

3.5 Berechnen der Parameter

Bisher wurde gezeigt, wie man zu einer Stelle P von F_1 alle möglichen Kandidaten $D \in \mathcal{D}_{F_2}$ bestimmt, so dass $\deg D$ mit dem vermuteten Grad für $[F_2 : \phi(F_1)]$ übereinstimmt und es für die erste Polzahl n_1 von P und das Element x_1 mit $(x_1)_\infty = n_1 P$ ein Element $z \in \mathcal{L}(n_1 D)$ mit $(z)_\infty = n_1 D$ gibt. Weiterhin wurde gesagt, dass wenn man nun z zu einer Basis $\{z, b_2, \ldots, b_m\}$ von $\mathcal{L}(n_1 D)$ ergänzt, für jede Einbettung $\phi : F_1 \longrightarrow F_2$ mit $\hat{\phi}(P) = D$ gelten muss: $\phi(x_1) = \lambda_1 z + \sum_{i=2}^{m} \lambda_i b_i$ mit $\lambda_i \in k$.
Ziel des Abschnittes ist es zu zeigen, wann diese notwendigen Bedingungen für die Existenz einer Einbettung sogar hinreichend sind und wie das algorithmisch überprüft

werden kann. Dafür wird ein hinreichendes Kriterium angegeben und untersucht für welche Werte der λ_i sich der Vektorraummonomorphismus

$$\psi : \mathcal{L}(n_1 P) \longrightarrow \mathcal{L}(n_1 D)),\ 1 \mapsto 1,\ x_1 \mapsto \lambda_1 z + \sum_{i=2}^{m} \lambda_i b_i$$

zu einem Homomorphismus der Funktionenkörper fortsetzen lässt.

3.5.1 Mathematischer Aspekt

Lemma 3.5.1. *Seien $P \in \mathbb{P}_{F_1}$, $D \in \mathcal{D}_{F_2}$ und $n \in \mathbb{N}$ eine ausreichend große natürliche Zahl. Sei $\psi : \mathcal{L}(nP) \longrightarrow \mathcal{L}(nD)$ ein Vektorraummonomorphismus. Dann gibt es maximal einen Funktionenkörperhomomorphismus $\phi : F_1 \longrightarrow F_2$ mit $\tilde{\phi} = \psi$.*

Dieses Lemma liefert folgende interessante Konsequenz: Wenn man versucht Einbettungen $\phi : F_1 \longrightarrow F_2$ zu finden, indem man nach möglichen induzierten Einbettungen der Divisorgruppen sucht, dann wird ein Funktionenkörperhomomorphismus schon vollständig dadurch beschrieben, wie er auf einem ausreichend großen Riemann-Roch-Raum wirkt. Diese Aussage rechtfertigt die im vorherigen Kapitel beschriebene Idee des Einbettungsalgorithmus.

Beweis. Nach Lemma 3.4.4 gibt es $x_1, \ldots, x_r \in F_1$ mit $F_1 = k(x_1, \ldots, x_r)$ und man kann diese x_i alle in $\mathcal{L}(nP)$ für ein ausreichend großes $n \in \mathbb{N}$ wählen. Jeder Funktionenkörperhomomorphismus ist durch seine Bilder auf den x_i eindeutig festgelegt, also kann es zu vorgegebenen Bildern der x_i maximal eine Einbettung geben. □

Dieses Lemma liefert ein hinreichendes Kriterium für die Existenz einer Einbettung:

Lemma 3.5.2. *Sei $F_1 = Quot(k[x_1, \ldots, x_r])$ und $F_2 = Quot(k[y_1, \ldots, y_s])$ und seien I_1 und I_2 die Kerne des Einsetzhomomorphismus, der den passenden multivariaten Polynomring in den Funktionenkörper abbildet. Jeder Funktionenkörperhomomorphismus $\phi : F_1 \longrightarrow F_2$ mit $\phi(k[x_1, \ldots, x_r]) \subseteq k[y_1, \ldots, y_s]$ definiert dann auch einen Homomorphismus auf den Polynomringen $\varphi : k[T_1, \ldots, T_r] \longrightarrow k[T_1, \ldots, T_s]$ mit $\varphi(I_1) \subseteq I_2$. Umgekehrt definiert auch jeder Homomorphismus der Polynomringe $\varphi : k[T_1, \ldots, T_r] \longrightarrow k[T_1, \ldots, T_s]$ mit $\varphi(I_1) \subseteq I_2$ einen Funktionenkörperhomomorphismus $\phi : F_1 \longrightarrow F_2$ mit $\phi(k[x_1, \ldots, x_r]) \subseteq k[y_1, \ldots, y_s]$.*

Beweis. Sei also $\phi : F_1 \longrightarrow F_2$ eine Funktionenkörpereinbettung, die sich zu einer Abbildung $\phi : k[x_1, \ldots, x_r] \longrightarrow k[y_1, \ldots, y_s]$ einschränken lässt. Dann sind die Bilder der x_i Polynome in den y_j. Also liefert das auch eine Abbildung φ der Polynomringe. Als Homomorphismus bildet ϕ nichttriviale Darstellungen der Null in den x_i auch wieder auf null ab und somit gilt $\varphi(I_1) \subseteq I_2$. Sei nun $\varphi : k[T_1, \ldots, T_r] \longrightarrow k[T_1, \ldots, T_s]$, seien I_1, I_2 die Kerne des Einsetzhomomorphismus und gelte $\varphi(I_1) \subseteq I_2$. Dann definieren I_1 und I_2 affine Kurven deren Koordinatenringe $k[T_1, \ldots, T_r]/I_1$ beziehungsweise $k[T_1, \ldots, T_s]/I_2$ sind. Wegen $\varphi(I_1) \subseteq I_2$ bekommt man also eine Abbildung der Koordinatenringe und somit auch eine Abbildung der Funktionenkörper. □

Bemerkung 3.5.3. *Die für das Berechnen der Einbettungen interessante Anwendung dieses Lemmas ergibt sich, wenn man zu $P \in \mathbb{P}_{F_1}$ und $D \in \mathcal{D}_{F_2}$ die Ringe $\mathcal{O}^P$ und $\mathcal{O}^S$ mit $S = Supp(D)$ betrachtet. Nach den Vorüberlegungen wissen wir, dass es Elemente $x_1, \ldots, x_r \in F_1$ und $y_1, \ldots, y_s \in F_2$ gibt, mit $\mathcal{O}^P = k[x_1, \ldots, x_r]$ und $\mathcal{O}^S = k[y_1, \ldots, y_s]$ und dass jeder Homomorphismus $\phi : F_1 \longrightarrow F_2$ mit $\hat{\phi}(P) = D$ sich zu einer Abbildung von $\mathcal{O}^P$ nach $\mathcal{O}^S$ einschränken lässt. Umgekehrt lassen sich nun auch alle Funktionenkörperhomomorphismen, die P auf D abbilden, finden. Diese Einbettungen zu finden reduziert sich auf das Problem die Abbildungen $\psi : k[T_1, \ldots, T_r] \longrightarrow k[T_1, \ldots, T_s]$ der multivariaten Polynomringe zu konstruieren, die I_1 in I_2 einbetten. Hierbei bezeichnen I_1 und I_2 jeweils das Ideal der algebraischen Relationen der x_i beziehungsweise y_i. Wie dieses zu bewerkstelligen ist, wird im Folgenden gezeigt.*

Lemma 3.5.4. *Seien F ein Funktionenkörper über dem endlichen Konstantenkörper $k = \mathbb{F}_q$ und $z \in F$ mit $(z)_\infty = n_1P_1 + \ldots + n_sP_s$, $n_i \in \mathbb{N}$, $P_i \in \mathbb{P}_F$ und seien die Grade der P_i gleich eins. Sei $i \in \{1, \ldots, s\}$ und gelte $char(k) \nmid n_i$. Dann gibt es ein Element π_i in $\hat{F}_{P_i}$ mit $\pi_i^{-n_i} = uz$ für ein geeignetes $u \in k^\times$. Weiterhin sind $\hat{F}_{P_i}$ und $k((\pi_i))$ isometrisch isomorph, daher bekommt man über diesen Isomorphismus auch eine Einbettung ι_i von F in $k((\pi_i))$.*

Beweis. Gelte also $char(k) \nmid n_i$. Wählen wir nun eine lokale Uniformisierende t von P_i, so gilt nach Theorem 3.3.13 $\hat{F}_{P_i} \cong k((t))$, also kann man z^{-1} in eine Laurentreihe entwickeln: $z^{-1} = \sum_{j=n_i}^{\infty} a_j t^j$ mit $a_j \in k$. Für $u := a_{n_i}$ gilt dann $u^{-1}z^{-1} = t^{n_i} + \tilde{a}_{n_i+1}t^{n_i+1} + \ldots$. Wir wollen nun zeigen, dass man dieses Element beliebig gut durch eine Reihe aus $k((t))$ approximieren kann. Dazu betrachten wir $b_1 := t$. Dann gilt $v(uz^{-1} - b_1^{n_i}) = n_i + 1$ also wird π_i von b_1 bis zur Ordnung $n_i + 1$ approximiert, wobei v die diskrete Bewertung auf $k((t^{-1}))$ ist. Angenommen b_k approximiert π_i bis zur Ordnung $n_i + k$, dann können wir ohne Beschränkung der Allgemeinheit annehmen, dass $b_k = t + \mu_2 t^2 + \ldots + \mu_k t^k$ gilt, da $b_k^{n_i} - uz^{-1} \in O(t^{n_i+k+1})$ gilt. Somit können höhere t-Potenzen vernachlässigt werden. Sei nun also $b_k^{n_i} - uz^{-1} = ct^{n_i+k+1} + O(t^{n_i+k+2})$ und setze $b_{k+1} := b_k - cn_i^{-1}t^{k+1}$. Dann gilt: $b_{k+1}^{n_i} = b_k^{n_i} - ct^{n_i+k+1} + O(t^{n_i+k+2})$, also wird π_i von b_{k+1} bis zur Ordnung $k + 1$ approximiert. Die Elemente $(b_j)_{j\in\mathbb{N}}$ bilden eine Cauchyfolge, folglich liegt auch ihr Grenzwert in $\hat{F}_{P_i}$. Sei π_i der Grenzwert, dann gilt $\pi^{-n_i} = uz$. Nach Konstruktion ist $v(\pi_i) = 1$ daher auch $\hat{F}_{P_i} \cong k((\pi_i))$. □

Bemerkung 3.5.5. *Nach Theorem 3.3.21 kann man holomorphe Ringe mit Gittern in einem geeigneten Vektorraum identifizieren. Wie in dem Beweis beschrieben, ist diese Identifikation abhängig von der Wahl gewisser Basen. Mit Lemma 3.5.4 bekommt man nun eine spezielle Identifikation, indem man nämlich diese Elemente π_i als lokale Uniformisierende ansieht. Im weiteren werden die π_i immer als die speziellen lokalen Uniformisierenden bezeichnet.*

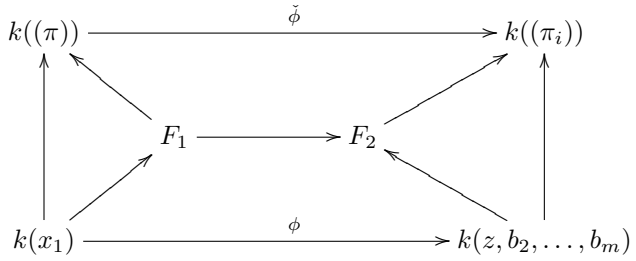
Lemma 3.5.6. *Sei $\phi : F_1 \longrightarrow F_2$ eine Einbettung mit $\hat{\phi}(P) = D = e_1P_1 + \ldots + e_sP_s$ und seien $x_1 \in F_1$ mit $(x_1)_\infty = n_1P$ und $z, b_2, \ldots, b_m$ eine Basis von $\mathcal{L}(n_1D)$ mit $v_{P_i}(z) = -e_in_1$ und $v_{P_r}(b_j) > -e_rn_1$ für ein $r \in \{1, \ldots, s\}$ und alle $j \in \{2, \ldots, m\}$. Seien P und P_i für ein $i \in \{1, \ldots, s\}$ beide vom Grad eins. Dann gilt:*

1.

$$\phi(x_1) = \lambda_1 z + \sum_{j=2}^{m} \lambda_j b_j \tag{3.5.1}$$

mit $\lambda_i \in k$ und $\lambda_1 \neq 0$. Die Abbildung ϕ lässt sich also zu einer Abbildung $\phi : k(x_1) \longrightarrow k(z, b_2, \ldots, b_m)$ einschränken.

2. Wird $e_i n_1$ nicht von der Charakteristik von k geteilt, dann lässt sich jeder Homomorphismus $\phi : k(x_1) \longrightarrow k(z, b_2, \ldots, b_m)$, $x_1 \mapsto \lambda_1 z + \sum_{j=2}^{m} \lambda_j b_j$ zu einer Abbildung $\check{\phi} : \hat{F}_{1P} \longrightarrow \hat{F}_{2P_i}$ fortsetzen.



Beweis. Der erste Punkt wurde bereits bewiesen, deswegen wenden wir uns gleich (2) zu. Dazu wählen wir $\pi \in \hat{F}_{1P}$ und $\pi_i \in \hat{F}_{2P_i}$ mit $\pi^{-n_1} = ux_1$ und $\pi_i^{-e_i n_1} = u'z$ gemäß Lemma 3.5.4. Dann gilt $\hat{F}_{1P} \cong k((\pi))$ sowie $\hat{F}_{2P_2} \cong k((\pi_i))$ und über diese Isomorphismen kann man auch $k(x_1)$ und $k(z, b_2, \ldots, b_m)$ als Teilkörper von $k((\pi))$ und $k((\pi_i))$ auffassen und alle b_i können als Reihen in π_i entwickelt werden, welche wir mit $\beta_2, \ldots, \beta_m$ bezeichnen. Weiterhin wissen wir, dass aus $v_{P_i}(\phi(x)) = -e_i n_1$ folgt $\phi(\pi) = \sum_{j=0}^{\infty} c_j \pi_i^{e_i+j}$ mit $c_j \in k$. Mit Hilfe von 3.5.1 bekommen wir einen Zusammenhang zwischen π und π_i. Es gilt:

$$u^{-1}\phi(\pi)^{-n_1} = \lambda_1 u'^{-1} \pi_i^{-e_i n_1} + \sum_{j=2}^{m} \lambda_j \beta_j.$$

Einsetzen und Umstellen der Gleichung liefert:

$$u'\pi_i^{e_i n_i} = \lambda_1 u \left(\sum_{j=0}^{\infty} c_j \pi_i^{e_i+j} \right)^{n_1} + uu'\pi_i^{e_i n_1} \left(\sum_{j=0}^{\infty} c_j \pi_i^{e_i+j} \right)^{n_1} \sum_{j=2}^{m} \lambda_j \beta_j. \tag{3.5.2}$$

Durch den Vergleich der Koeffizienten bekommt man eine Darstellung der c_j als Ausdruck in den λ_i, also das Bild von π unter ϕ in Abhängigkeit von den λ_i und somit eine Fortsetzung der Abbildung auf die Vervollständigungen der Funktionenkörper.

□

3.5.2 Algorithmischer Aspekt

Idee des Algorithmus

In diesem Abschnitt wird ein Algorithmus angegeben, der ermittelt, wie viele Einbettungen ϕ mit $\hat{\phi}(P) = D$ existieren. Seien Elemente $x_1, \ldots, x_r \in F_1$ gemäß Lemma 3.4.4 gewählt und sei $\{z, b_2, \ldots, b_m\}$ eine Basis von $\mathcal{L}(n_1 D)$ mit $(z)_\infty = n_1 D$. Nach den Vorüberlegungen wissen wir, dass $\phi(x_1) = \lambda_1 z + \sum_{i=2}^{m} \lambda_i b_i$ mit $\lambda_i \in k$ für jede Einbettung ϕ gelten muss. Weiterhin wissen wir, dass $F_1 = k(x_1, \ldots, x_r)$ und $\phi(\mathcal{O}^P) \subseteq \mathcal{O}^S$ gelten muss. Wir können eine $k[z]$-Basis $\{y_1, \ldots, y_l\}$ von $\mathcal{O}^S$ wählen und dann gilt $F_2 = k(y_1, \ldots, y_l)$. Durch Anwendung des hinreichenden Kriteriums reduziert sich die Frage darauf, für welche Werte für die λ_i diese Abbildung auf die anderen x_i fortgesetzt werden kann, so dass das Ideal der Relationen der x_i in das der y_i abgebildet wird. Im Folgenden werden die λ_i immer als die Parameter bezeichnet. Die Idee ist nun umgekehrt wie in Lemma 3.5.6 vorzugehen. Wir starten mit einer Abbildung $k(x_1) \longrightarrow k(z, b_2, \ldots, b_m)$ und berechnen, wann sich diese Abbildung auf $x_2, \ldots, x_r$ fortsetzen lässt. Dazu wählen wir für alle $i \in \{1, \ldots, s\}$ spezielle lokale Uniformisierende so wie beschrieben und setzen die Abbildung zu einer Abbildung $k((\pi)) \longrightarrow k((\pi_i))$ der Laurentreihenkörper fort. Da man F_1 und F_2 nach Konstruktion als Teilkörper von $k((\pi))$ und $k((\pi_i))$ auffassen kann, reduziert sich die Frage der Fortsetzbarkeit zu einer Abbildung der Funktionenkörper darauf, zu bestimmen, ob die Abbildung der Laurentreihenkörper sich zu einer Abbildung $\phi : F_1 \longrightarrow F_2$ einschränken lässt. Dazu stellen wir anhand von einigen Kriterien Gleichungen für die Parameter auf, so dass die Tupel aus dem k^m, die alle Gleichungen erfüllen, zu einer Einbettung der Funktionenkörper korrespondieren.

Interpretation der Parameter als Varietät

In den nächsten Abschnitten wird erklärt, wie man Gleichungen aufstellen kann, die die Parameter $\lambda_1, \ldots, \lambda_m \in k$ erfüllen müssen, damit die durch sie festgelegte Abbildung wirklich einen Homomorphismus von Funktionenkörpern beschreibt. Bei diesen Gleichungen handelt es sich um Polynome. Somit kann man die Menge aller Parametertupel, die sämtliche Gleichungen erfüllen als die k-rationalen Punkte der affinen Varietät im $\overline{k}^m$ auffassen, die durch das Ideal der Gleichungen $I \subset k[t_1, \ldots, t_m]$ bestimmt wird. Definitionen und Erklärungen zu Varietäten und Idealen finden sich in [Har77].

Fortsetzung der Abbildung auf die Laurentreihenkörper

Die Idee, wie man einen Funktionenkörperhomomorphismus auf geeignete Laurentreihenkörper fortsetzen kann, liefert der Beweis von Lemma 3.5.6. Erst werden die speziellen lokalen Uniformisierenden π und π_i bestimmt. Lemma 3.5.4 liefert ein konstruktives Verfahren, mit dem man diese zu beliebiger Präzision berechnen kann. Die Fortsetzung der Abbildung $\phi : k(x_1) \longrightarrow k(z, b_2, \ldots, b_m),\ x_1 \mapsto \lambda_1 z + \sum_{j=2}^{m} \lambda_j b_j$ auf die Laurentreihenkörper bekommt man, indem man durch Koeffizientenvergleich die Unbekannten c_i in $\phi(\pi)$ in Abhängigkeit von den λ_j aus der Gleichung

$$u'\pi_i^{e_i n_i} = \lambda_1 u \left(\sum_{j=0}^{\infty} c_j \pi_i^{e_i+j} \right)^{n_1} + uu'\pi_i^{e_i n_1} \left(\sum_{j=0}^{\infty} c_j \pi_i^{e_i+j} \right)^{n_1} \sum_{j=2}^{m} \lambda_j \beta_j$$

errechnet. Da man $\phi(\pi)$ nur bis zu einer gewissen Präzision berechnen will, genügt es diese Gleichung bis zu einem festen Grad aus zu multiplizieren und dann das Gleichungssystem der Koeffizienten zu lösen. Nun kann man für $x_2, \ldots, x_r \in F_1$ die Darstellung als Reihe in π errechnen und bekommt damit auch die Bilder $\phi(x_2), \ldots, \phi(x_r)$ in Abhängigkeit von den λ_i als Reihen in π_i und somit die gesuchte Fortsetzung der Abbildung.

Gleichungen für die Parameter durch das Polverhalten

Sei $\{y_1, \ldots, y_l\}$ eine $k[z]$-Basis von $\mathcal{O}^S$. Dann werden die x_i durch eine Einbettung auf eine Linearkombination der Basiselemente abgebildet. Ziel ist es zu überprüfen, für welche Parameter das der Fall ist. Dazu berechnet man für jedes y_j eine Darstellung als Reihe in den speziellen lokalen Uniformisierenden $\pi_1, \ldots, \pi_s$ und fasst Darstellungen desselben Elementes bezüglich unterschiedlicher lokaler Uniformisierender zu einem Vektor $\Psi(y_j)$ zusammen. Damit bekommt man ganz analog zu Lemma 3.3.22 eine Identifikation der y_j mit einer Gitterbasis im $k((z^{-1}))^n$. Für jedes x_i konstruiert man nun einen Vektor $\Psi(x_i)$, indem man zuerst x_i in eine Reihe in π entwickelt. Anschließend konstruiert man daraus einen Vektor, indem man als j-te Komponenten die Reihe wählt, die man bekommt, wenn man in der Reihenentwicklung von x_i das π durch $\phi(\pi)$ als Reihe in π_j ersetzt. Die anfängliche Frage ist somit darauf reduziert, zu bestimmen für welche Parameter die Vektoren $\Psi(x_i)$ Gittervektoren sind. Problematisch ist nur, dass die Koordinaten der Vektoren unendliche Laurentreihen sind, wir algorithmisch aber nur bis zu einer vorgegebenen Präzision rechnen können. Daher ist es algorithmisch nur möglich zu bestimmen, ob sich die Vektoren $\Psi(x_i)$ bis zu einer bestimmten Präzision durch Gittervektoren approximieren lassen. Dazu wird ein Algorithmus verwendet, der sehr ähnlich zu dem Reduktionsalgorithmus zur Bestimmung einer reduzierten Gitterbasis arbeitet. Als Input bekommt dieser Algorithmus einmal die Vektoren $\Psi(y_1), \ldots, \Psi(y_l)$ und $\Psi(z)$ der Reihenentwicklungen, sowie den Vektor $\Psi(x_i)$ für $i \in \{1, \ldots, r\}$, wobei die Koordinaten des letzten Vektors Reihen sind, deren Koeffizienten noch von den Parametern $\lambda_1, \ldots, \lambda_m$ abhängen. Damit berechnet der Algorithmus eine Menge von Gleichungen, die $\lambda_1, \ldots, \lambda_l$ erfüllen müssen, damit man $\Psi(x_i)$ durch einen Vektor aus $span_{k[z]}(\Psi(y_1), \ldots, \Psi(y_l))$ approximieren kann. Außerdem wird die Darstellung dieser Approximation in Abhängigkeit von den Parametern berechnet. Dazu addiert man iterativ $k[z]$-Linearkombinationen der Vektoren $\Psi(y_1), \ldots, \Psi(y_l)$ zu $\Psi(x_i)$, so dass der Spaltengrad von $\Psi(x_i)$ sinkt. Diesen Vorgang wiederholt man so lange, bis der Spaltengrad von $\Psi(x_i)$ kleiner als eine gewisse Grenze ist. Dabei stellt man in den einzelnen Schritten Gleichungen für die λ_i auf, die diese erfüllen müssen, damit man weitere Reduktionsschritte durchführen kann.

Pseudocode

Algorithmus 4 Parameterberechnung 1

Input: $z, y_1, \ldots, y_l$ eine reduzierte $k[z]$-Basis von $\mathcal{O}^S$, x Element dessen Bild approximiert werden soll, *bound* die Genauigkeit der Approximation.

Output: *gl* Menge von Gleichungen für die Parameter, T Transformationsmatrix zur Beschreibung der Approximation von x durch eine $k[z]$-Linearkombination der y_i.

1: Berechne $(z)_\infty = e_1P_1 + \ldots + e_sP_s$ und $e = kgV(e_i)$.
2: Berechne $\Psi_1, \ldots, \Psi_l$ die Gittervektoren zu den y_j.
3: Berechne Ψ_x den von den Parametern abhängigen Vektor, den man für das Bild von x bekommt.
4: $T := Id_l(k[z])$ und $gl := [\,]$.
5: **repeat**
6: Berechne Spaltengrad g von Ψ_x.
7: Berechne $A := \{\Psi_i \,|\, i \in \{1, \ldots, l\}, \deg(\Psi_i) \equiv g \mod e, \deg(\Psi_i) \leq g\}$ mit Indexmenge $\{i_1, \ldots, i_r\}$.
8: **if** $\#A = 0$ **then**
9: Berechne $hc(\Psi_x)$ und setze die Einträge dieses Vektors gleich null und nimm sie als Gleichungen in *gl* auf.
10: Aktualisiere den Vektor Ψ_x in dem man die Parameter mit den Gleichungen aus *gl* umformt.
11: **else**
12: Erstelle Matrix $M \in k(\lambda_1, \ldots, \lambda_m)^{s \times r+1}$ deren Spalten die Vektoren aus der Menge $\{hc(\Psi_x)\} \cup \{hc(z^{(g-\deg(\Psi_j)/e)}\Psi_j) | j \in \{i_1, \ldots, i_r\}\}$ sind.
13: **if** Spalten von M sind $k(\lambda_1, \ldots, \lambda_m)$-linear abhängig **then**
14: Berechne k-Linearkombination der ersten Spalte durch die anderen: $hc(\Psi_x) = \sum_{j=1}^{r} \alpha_j hc(z^{(g-\deg(\Psi_j)/e)}\Psi_j)$.
15: Setze $\Psi_x := \Psi_x - \sum_{j=1}^{r} \alpha_j z^{(g-\deg(\Psi_j)/e)}\Psi_{i_j}$.
16: Sei T_1 die Matrix die diese Transformation beschreibt.
17: $T := TT_1$
18: **else**
19: Berechne alle $(r+1) \times (r+1)$ Minoren von M.
20: Setze die Minoren gleich null und füge diese zu den Gleichungen *gl* hinzu.
21: Forme die Einträge von M gemäß der Gleichungen *gl* um, so dass die erste Spalte eine k-Linearkombination der anderen Spalten ist.
22: Berechne $hc(\Psi_x) = \sum_{j=1}^{r} \alpha_j hc(z^{(g-\deg(\Psi_j)/e)}\Psi_j)$ für die umgeformten Koeffizienten.
23: Setze $\Psi_x := \Psi_x - \sum_{j=1}^{r} \alpha_j z^{(g-\deg(\Psi_j)/e)}\Psi_{i_j}$.
24: Sei T_1 die Matrix die diese Transformation beschreibt.
25: $T := TT_1$.
26: **end if**
27: **end if**
28: **until** $g \leq bound$
29: Gebe die Matrix T und die Gleichungen *gl* zurück.

Technische Probleme

Wie auch der Gitterreduktionsalgorithmus basiert dieser Algorithmus darauf Linearkombinationen von Vektoren, deren Einträge Reihen sind, zu berechnen. Da man die Einträge aber nur bis zu einer gewissen Präzision kennt, ist die Frage wie hoch diese sein muss, damit die Ergebnisse trotzdem korrekt sind. Ziel ist es, den Vektor $\Psi(x)$ durch einen Gittervektor v mit der Genauigkeit α zu approximieren, das heißt man sucht eine $k[z]$-Linerkombination v der Gitterbasis, so dass $\deg(\Psi(x) - v) \leq \alpha$ gilt. Also muss man alle Einträge von $\Psi(x)$ mit einer Genauigkeit kennen, die mindestens so hoch ist, dass Fehler erst bei einem niedrigeren Spaltengrad auftreten. Für die Präzisionen der Reihen, die die Einträge von $\Psi(x)$ bilden, sind zwei Dinge verantwortlich: Zum einen die Präzision mit der man x als Element von F_1 als Reihe in π entwickelt und zum anderen die Genauigkeit, mit der man das Gleichungssystems der Koeffizienten der Darstellung von $\phi(\pi)$ als Reihe in π_i löst. Bei den Vektoren der Gitterbasis hängt die Präzision der Einträge nur davon ab, wie genau diese als Reihen in den speziellen lokalen Uniformisierenden entwickelt wurden. Analog zu dem Abschnitt über technische Probleme beim Berechnen von reduzierten Gitterbasen kann Präzision verloren gehen, wenn man Vektoren mit Potenzen von z multipliziert. Dort wurde auch beschrieben, wie sich das Problem umgehen lässt. In dieser speziellen Situation kann man aber auch anders vorgehen. Wenn man davon ausgeht, dass es für dieselbe Präzision länger dauert das Gleichungssystem der Koeffizienten der Darstellung von $\phi(\pi)$ zu lösen, als Elemente in Reihen zu dieser Genauigkeit zu entwickeln, dann kann man $\Psi(x)$ gerade so genau entwickeln, dass die Präzision ausreicht, um ohne Präzisionsverluste bis zur Genauigkeit α zu approximieren. Die Vektoren $\Psi_1, \ldots, \Psi_l$ der Gitterbasis hingegen berechnet man zu einer deutlich höheren Präzision. Da bei der Reduktion in jedem Schritt nur Vektoren Ψ_i mit z-Potenzen multipliziert werden, verlieren auch nur diese Präzision. Da diese aber trotzdem noch deutlich höher ist als die von $\Psi(x)$, kommt es bei der Addition zu keinem weiteren Präzisionsverlust.

Überlegungen zu Korrektheit

Lemma 3.5.7. *Bei jedem Schleifendurchlauf sinkt der Spaltengrad von Ψ_x und alle Parameter, für die Ψ_x einen Gittervektor beschreibt, erfüllen alle Gleichungen in gl. Sei weiterhin Ψ_x ein Gittervektor und sei v ein Gittervektor mit $\deg(\Psi_x - v) \leq bound < 0$, dann gilt schon $\Psi_x = v$.*

Beweis. Die Vektoren $\Psi_1, \ldots, \Psi_l$ bilden nach Voraussetzung eine reduzierte Gitterbasis, das heißt, man kann an ihnen keine Reduktionsschritte durchführen. Betrachtet man also die Vektoren Ψ_i und einen weiteren Vektor Ψ_x und es ist ein Reduktionsschritt möglich, dann kann man diesen Reduktionsschritt auf den Vektor Ψ_x anwenden. Weiterhin wissen wir, dass ein Vektor, dessen Spaltengrad niedriger ist als der aller Ψ_i, kein Gittervektor sein kann. Man betrachte die verschiedenen Fälle, die auftreten können:
1.Fall: $\#A = 0$
In diesem Fall gibt es keinen Gittervektor, der den gleichen Spaltengrad wie Ψ_x hat. Alle Gittervektoren sind $k[z]$-Linearkombinationen der Ψ_i und daher sind auf Grund der Reduziertheit für Gittervektoren als Spaltengrade nur Werte der Form $ke + \deg(\Psi_i)$ mit $k \in \mathbb{N}$ möglich. Sollte Ψ_x also ein Gittervektor sein, dann müssen die Leitkoeffizienten der Reihen, die den maximalen Grad haben, gleich null sein. Setzt man also diese Leitkoeffizienten auf null, so sinkt der Spaltengrad und alle Git-

tervektoren erfüllen die Gleichungen.
2.Fall: $\#A \geq 1$ und die Spalten der Matrix M sind linear abhängig.
Da die Spalten linear abhängig sind, kann man diese so linear kombinieren, dass der Spaltengrad sinkt. Nach der Vorüberlegung gilt sogar, dass man diesem Reduktionsschritt auf den Vektor Ψ_x anwenden kann und zwar unabhängig von den Parametern. Also sinkt der Spaltengrad von Ψ_x und da keine neuen Gleichungen hinzukommen ist die zweite Bedingung immer noch erfüllt.
3.Fall: $\#A \geq 1$ und die Spalten von M sind linear unabhängig.
Wenn Ψ_x ein Gittervektor ist, dann ist er darstellbar als $k[z]$-Linearkombination der Gitterbasis, also gibt es einen Reduktionsschritt, der den Spaltengrad von Ψ_x reduziert. Das ist nach 3.3.7 der Fall, wenn die Spalten von M linear abhängig sind. Sie sind linear abhängig, wenn alle $(r+1)\times(r+1)$ Minoren gleich null sind. Setzt man die Minoren gleich null und nimmt sie zu den Gleichungen hinzu, so werden die Vektoren linear abhängig, wenn man ihre Einträge mit den Gleichungen umformt. Man kann also den Spaltengrad von Ψ_x senken.

Wenn Ψ_x ein Gittervektor ist, dann kann man diesen Vektor nach Konstruktion mit einem Element a aus $\mathcal{O}^S$ identifizieren. Analog identifiziert man v mit $b \in \mathcal{O}^S$. Das zu $\Psi_x - v$ gehörige Element $a - b \in \mathcal{O}^S$ besitzt wegen $\deg(\Psi_x - v) < 0$ an allen Stellen aus S eine Bewertung größer null. Da diese Stellen die einzigen sind, an denen ein Element aus $\mathcal{O}^S$ Pole haben kann, muss $a - b = 0$ gelten. Daraus folgt der zweite Teil der Behauptung. □

Bemerkung 3.5.8. *Der Spaltengrad kann nur endlich oft sinken, bis er kleiner als eine bestimmte vorgegebene Schranke ist. Daher terminiert der Algorithmus nach endlich vielen Schritten. Der zweite Teil beweist, dass der Algorithmus für die Parameter, die eine Einbettung ϕ beschreiben, wirklich die exakte Darstellung von $\psi(x_i)$ berechnet, wenn man eine Schranke kleiner null vorgibt.*

Gleichungen für die Parameter über die Relationen

In diesem Abschnitt wird ein Unteralgorithmus vorgestellt, der zu gegebenen Elementen $x_1, \ldots, x_r \in F_1$ und $\phi(x_1), \ldots, \phi(x_r) \in F_2$, wobei die Letzteren von gewissen Parametern $\lambda_1, \ldots, \lambda_m$ abhängig sind, überprüft bei welchen Werten für die Parameter für jede nicht triviale algebraische Kombination $0 = p(x_1, \ldots, x_r)$, $p \in k[T_1, \ldots, T_r]$ auch $p(\phi(x_1), \ldots, \phi(x_r)) = 0$ gilt. Damit ist es möglich den zweiten Teil des hinreichenden Kriteriums 3.5.2 zu überprüfen. Die Elemente $x_1, \ldots, x_r$ werden gemäß 3.4.4 gewählt. Die parametrisierten Elemente $\phi(x_1), \ldots, \phi(x_r)$ sind genau die Approximationen der Bilder, die der zuvor beschriebene Algorithmus berechnet hat. In 3.4.7 wurde bewiesen, wie man die algebraischen Relationen der x_i als ein Ideal in einem multivariaten Polynomring auffassen kann und wie ein einfaches Erzeugendensystem dieses Ideals aussieht. Wie bereits gezeigt, gibt es ein Erzeugendensystem des Relationenideals der Form:

$$E = \{T_iT_j - p_{1,i,j}(T_1) - \sum_{k=2}^{r} p_{k,i,j}(T_1)T_k \mid i,j \in \{1,\ldots,r\},\ p_{k,i,j} \in k[T_1] \text{ geeignet } \}.$$

Es gilt also zu überprüfen, für welche Parameter die Gleichungen

$$\phi(x_i)\phi(x_j) - p_{1,i,j}(\phi(x_1)) - \sum_{k=2}^{r} p_{k,i,j}(\phi(x_1))\phi(x_k) = 0$$

für alle $i, j \in \{1, \ldots, r\}$ erfüllt sind. Dazu berechnet man für die Ausdrücke $\phi(x_i)\phi(x_j)$ und $p_{1,i,j}(\phi(x_1)) - \sum_{k=2}^{r} p_{k,i,j}(\phi(x_1))\phi(x_k)$ jeweils eine Darstellung in der $k[z]$-Basis von $\mathcal{O}^S$ und vergleicht die zueinander gehörigen Koeffizienten. Diese liefern dann weitere Bedingungen an die Parameter.

Pseudocode

Algorithmus 5 Parameterberechnung 2

Input: $x_1, \ldots, x_r \in F_1$, $\phi(x_1), \ldots, \phi(x_r) \in F_2$ abhängig von den Parametern $\lambda_1, \ldots, \lambda_m$.
Output: gl Menge an Gleichungen in den λ_i.

1: $gl := [\,]$.
2: **for** $i = 2, \ldots, r$ **do**
3: **for** $j = i, \ldots, r$ **do**
4: Berechne $a = x_i x_j \in F_1$.
5: Berechne eine Darstellung von a in der $k[x_1]$-Basis von $\mathcal{O}^S$: $x_i x_j = p_{1,i,j}(x_1) + \sum_{k=2}^{r} p_{k,i,j}(x_1)x_k$.
6: Ersetze in dieser Darstellung jedes x_i durch $\phi(x_i)$: $\phi(x_i x_j) = p_{1,i,j}(\phi(x_1)) + \sum_{k=2}^{r} p_{k,i,j}(\phi(x_1))\phi(x_k)$ um eine von den Parametern abhängige Darstellung von $\phi(x_i x_j)$ in F_2 zu bekommen.
7: Berechne für dieses Element eine parametrisierte Darstellung in der $k[z]$-Basis von $\mathcal{O}^S$: $\phi(x_i x_j) = \sum_{k=1}^{l} q_k(z) y_k$ mit $q_k \in k[T_1]$ abhängig von $\lambda_1, \ldots, \lambda_m$.
8: Berechne $\phi(x_i)\phi(x_j)$ als Element von F_2.
9: Berechne dafür eine $k[z]$-Darstellung: $\phi(x_i)\phi(x_j) = \sum_{k=1}^{l} \tilde{q}_k(z) y_k$.
10: **for** $d = 1, \ldots, l$ **do**
11: Berechne die Differenzen der Koeffizienten gleicher Monome von q_d und $\tilde{q}_d$.
12: Setze diese Differenzen gleich null und füge die entstehenden Gleichungen zu gl hinzu.
13: **end for**
14: **end for**
15: **end for**
16: Gebe gl zurück.

Technische Probleme

In diesem Unteralgorithmus muss man für Elemente aus F_2, die von den Unbekannten $\lambda_1, \ldots, \lambda_m$ abhängen, eine Darstellung in einer $k[z]$-Basis von $\mathcal{O}^S$ berechnen. Das kann man machen, indem man sich vorstellt, der Funktionenkörper F_2 ist über dem multivariaten rationalen Funktionenkörper $k(\lambda_1, \ldots, \lambda_m)$ als Konstantenkörper definiert. Das ist genau der Funktionenkörper, den man bekommt, wenn man eine rein transzendente Konstantenkörpererweiterung vom Transzendenzgrad m auf F_2 anwendet. Im Abschnitt 3.7.3 wird die mathematische Theorie dazu vorgestellt und gezeigt, dass dieses Vorgehen zulässig ist. In der Praxis ist es jedoch aufwendig eine Darstellungen in der Basis von $\mathcal{O}^S$ über dem erweiterten Konstantenkörper zu berechnen. Da

der auf der Gitterreduktion basierende Algorithmus vergleichsweise schnell arbeitet, hat es sich als nützlich erwiesen, diesen bis zu einer relativ niedrigen Schranke laufen zu lassen, so dass die Anzahl der Parametertupel, die diese Gleichungen erfüllen, schon sehr eingeschränkt ist. Für die verbleibenden Parametertupel kann man dann direkt nachprüfen, ob die durch sie definierte Abbildung die algebraischen Relationen respektiert. In vielen kleinen Beispielen hat sich dieses Vorgehen als schneller erwiesen.

Überlegungen zur Korrektheit

Lemma 3.5.9. *Die Parametertupel, die alle Gleichungen aus den Unteralgorithmen 4 und 5 erfüllen, definieren einen Funktionenkörperhomomorphismus $\phi : F_1 \longrightarrow F_2$.*

Beweis. Nach 3.5.2 kennen wir ein hinreichendes Kriterium, wann es sich bei einer Abbildung um eine Einbettung der Funktionenkörper handelt. Bei den Überlegungen zur Korrektheit von Algorithmus 4 wurde bereits der erste Teil des Kriteriums nachgewiesen. Es genügt zu zeigen, dass die durch die Parameter definierte Abbildung die Relationen der x_i erhält. Das gilt, da der Algorithmus diese Eigenschaft genau auf einem speziellen Erzeugendensystem nachprüft. □

Bemerkung 3.5.10. *Da der Unteralgorithmus 5 nur über endlich viele Elemente iteriert, terminiert er. Es wird also nach endlich vielen Schritten ein korrektes Ergebnis berechnet.*

3.6 Konstruktion der Abbildungen

Mit den Überlegungen des vorherigen Abschnitts sind wir nun in der Lage zu entscheiden, welche Parameter eine Einbettung $\phi : F_1 \longrightarrow F_2$ definieren. Zu diesem Zeitpunkt ist aber nur bekannt, wie die Abbildung auf speziellen Elementen $x_1, \ldots, x_r \in F_1$ operiert. Ziel ist es daraus die gesamte Abbildung zu berechnen. Geht man davon aus, dass die Funktionenkörper als endliche separable Erweiterungen eines rationalen Funktionenkörpers gespeichert sind, das heißt $F_1 = k(x, y)$ und $F_2 = k(\hat{x}, \hat{y})$, so kann man einen Homomorphismus von F_1 nach F_2 vollständig durch die Darstellung seiner Bilder auf x und y in der $\hat{y}$-Potenzbasis von F_2 beschreiben. In Magma [BCP97] und KASH [Kan04] werden Funktionenkörper und ihre Homomorphismen genau auf diese Weise gespeichert, daher ist diese Annahme sinnvoll.

3.6.1 Algorithmischer Aspekt

Wir wollen also die Bilder von x und y unter der Voraussetzung bestimmen, dass die Bilder von $x_1, \ldots, x_r$ bekannt sind. Da $F_1 = Quot(k[x_1, \ldots, x_r])$ gilt, gibt es für ein beliebiges Element $a \in F_1$ eine Darstellung als rationale Funktion in den x_i. Diese wollen wir als Erstes berechnen. Das Vorgehen dazu ist vergleichbar mit dem in 3.3.2. Wir machen den Ansatz $a = f/g$ mit $f, g \in \mathcal{O}^S$ und betrachten Mengen der Form $U_i := \{x_1^j, x_1^j x_2, \ldots, x_1^j x_r \,|\, 0 \leq j \leq i\} \cup \{a x_1^j, a x_1^j x_2, \ldots, a x_1^j x_r \,|\, 0 \leq j \leq i\}$ für größer werdende $i \in \mathbb{N}$. Da $f \in \mathcal{O}^S$ und $f = ag$ gilt, werden die U_i ab einem gewissen i_{max} k-linear abhängig. Sei also eine solche nichttriviale k-Linearkombination der Null mit $\mu_{i,j}, \nu_{i,j} \in k,\ 1 \leq i \leq r,\ 0 \leq j \leq i_{max}$ mindestens ein $\mu_{i,j}, \nu_{i,j} \neq 0$ berechnet. Dann

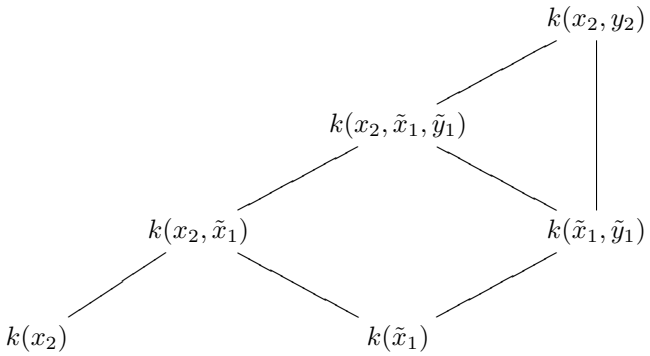
gilt:

$$\begin{aligned} 0 &= \sum_{j=0}^{i_{max}} \mu_{1,j} x_1^j + \sum_{i=2}^{r} \sum_{j=0}^{i_{max}} \mu_{i,j} x_1^j x_i + \sum_{j=0}^{i_{max}} \nu_{1,j} a x_1^j + \sum_{i=2}^{r} \sum_{j=0}^{i_{max}} \nu_{i,j} a x_1^j x_i \\ &= p_1(x_1) + \sum_{k=2}^{r} p_k(x_1) x_k + a \left(\tilde{p}_1(x_1) + \sum_{k=2}^{r} \tilde{p}_k(x_1) x_k \right) \end{aligned}$$

mit $p_i(x_1) = \sum_{j=1}^{i_{max}} \mu_{i,j} x^j$ und $\tilde{p}_i(x_1) = \sum_{j=1}^{i_{max}} \nu_{i,j} x^j$. Das Umstellen nach a liefert die gewünschte Darstellung als rationale Funktion in den x_i. Auf diese Weise berechnen wir nun eine Darstellung von x und y und bekommen die Bilder $\phi(x)$ und $\phi(y)$, in dem wir jeweils x_i durch $\phi(x_i)$ ersetzen. Das liefert die Einbettung in der gewünschten Form. Es ist damit nicht gesichert, dass alle so konstruierten Einbettungen separabel sind. Das folgende Lemma zeigt, wie man die separablen finden kann.

Lemma 3.6.1. *Sei $\phi : F_1 \longrightarrow F_2$ eine Einbettung von Funktionenkörpern und seien F_1 und F_2 gegeben als separable Erweiterung der rationalen Funktionenkörper $k(x_1)$ beziehungsweise $k(x_2)$. Es gilt: ϕ ist genau dann separabel, wenn das Minimalpolynom von x_2 separabel über $k(\phi(x_1))$ ist.*

Beweis. Wir definieren $\tilde{x}_1 := \phi(x_1)$ und $\tilde{y}_1 := \phi(y_1)$ und betrachten das folgende Diagramm von Körpererweiterungen:



Die Erweiterung $k(x_2, y_2)/k(x_2)$ ist nach Voraussetzung separabel und damit auch alle Teilschritte, insbesondere $k(x_2, y_2)/k(x_2, \tilde{x}_1, \tilde{y}_1)$. Weiterhin ist $k(x_1, y_1)/k(x_1)$ nach Voraussetzung separabel also auch $k(\tilde{x}_1, \tilde{y}_1)/k(\tilde{x}_1)$. Ist nun $k(x_2, \tilde{x}_1)/k(\tilde{x}_1)$ separabel, dann auch $k(x_2, \tilde{x}_1, \tilde{y}_1)/k(\tilde{x}_1, \tilde{y}_1)$. Die Erweiterung $k(x_2, y_2)/k(\tilde{x}_1, \tilde{y}_1)$ ist genau dann separabel, wenn die Teilschritte $k(x_2, y_2)/k(x_2, \tilde{x}_1, \tilde{y}_1)$ und $k(x_2, \tilde{x}_1, \tilde{y}_1)/k(\tilde{x}_1, \tilde{y}_1)$ separabel sind. Daraus folgt die Behauptung.

□

3.7 Stellen höheren Grades

In den Abschnitten zur Berechnung einer Basis des freien Moduls $\mathcal{O}^S$ und zur Berechnung der Parameter, die eine Einbettung definieren, wurde angenommen, dass der Divisor D nur Stellen vom Grad eins besitzt. In dem folgenden Abschnitt wird gezeigt, wie der Fall, dass D Stellen höheren Grades besitzt, auf den Grad Eins Fall reduziert werden kann. Dazu wird ein Theorem über Konstantenkörpererweiterungen benötigt.

3.7.1 Mathematischer Aspekt

Im Folgenden bezeichnet F einen Funktionenkörper mit Konstantenkörper k. Für den Algorithmus ist nur der Fall $k = \mathbb{F}_q$ von Interesse. Die nächsten Aussagen gelten aber auch für einen beliebigen vollkommenen Konstantenkörper. Weiterhin wird mit k' eine algebraische Erweiterung von k bezeichnet. Dann ist das Kompositum $F' = Fk'$ ein Funktionenkörper über k'.

Definition 3.7.1. *Sei k' eine Körpererweiterung von k. Dann bezeichnet man den Funktionenkörper $F' = Fk'$ als* Konstantenkörpererweiterung *von F.*

Lemma 3.7.2. *Sei $F' = Fk'$ eine algebraische Konstantenkörpererweiterung. Dann gilt:*

1. *k' ist der volle Konstantenkörper von F'.*
2. *$[F : k(x)] = [F' : k'(x)]$ für jedes $x \in F \setminus k$.*

Beweis. Ein Beweis findet sich bei [Sti93, S.101]. □

Das folgende Theorem fasst die Aussagen über Konstantenkörpererweiterungen zusammen, die für den Algorithmus benötigt werden.

Theorem 3.7.3. *Für eine algebraische Konstantenkörpererweiterung $F' = Fk'$ von F/k gilt:*

1. *F'/F ist unverzweigt, das heißt, $e(P'|P) = 1$ für alle $P \in \mathbb{P}_F$ und $P' \in \mathbb{P}_{F'}$ mit $P'|P$.*
2. *F' und F haben dasselbe Geschlecht.*
3. *Für jeden Divisor $D \in \mathcal{D}_F$ gilt:* $\deg Con_{F'/F}(D) = \deg D$.
4. *Jede k-Basis von $\mathcal{L}(D)$ ist auch eine k'-Basis von $\mathcal{L}(Con_{F'/F}(D))$ für jeden Divisor $D \in \mathcal{D}_F$. Also gilt auch* $\dim Con_{F'/F}(D) = \dim D$.
5. *Der Restklassenkörper $F'_{P'}$ einer Stelle $P' \in \mathbb{P}_{F'}$ ist das Kompositum $F_P k'$ vom k' und dem Restklassenkörper F_P mit $P = P' \cap F$.*
6. *Ist k'/k endlich, dann ist eine Basis von k'/k auch eine Ganzheitsbasis von F'/F für alle $P \in \mathbb{P}_F$.*

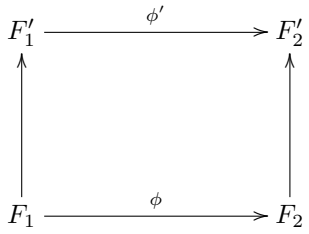
Beweis. Dieser Satz ist in [Sti93, S.103] bewiesen. □

Korollar 3.7.4. *Sei F' eine endliche Erweiterung von F mit $[F' : F] = n$ und $P \in \mathbb{P}_F$ eine Stelle vom Grad eins mit $Con_{F'/F}(P) = P_1 + \ldots + P_s$ wobei $P_i \in \mathbb{P}_{F'}$ und $\deg P_i = f_i$ für $i \in \{1, \ldots, s\}$ gilt. Seien F und F' über dem endlichen Konstantenkörper $k = \mathbb{F}_q$ definiert. Betrachtet man nun die Konstantenkörpererweiterungen $F\mathbb{F}_{q^d}$ und $F'\mathbb{F}_{q^d}$ mit $d = kgV(f_i)$, dann gilt: es liegt genau eine Stelle Q von $F\mathbb{F}_{q^d}$ über P und $Con_{F'\mathbb{F}_{q^d}/F\mathbb{F}_{q^d}}(Q) = Q_1 + \ldots + Q_n$.*

Beweis. Als Erstes betrachtet man die Körpererweiterung $F\mathbb{F}_{q^d}/F$. Diese ist eine Konstantenkörpererweiterung. Nach 3.7.3 gilt $1 = \deg P = \deg Con_{F\mathbb{F}_{q^d}/F}$. Daher kann nur eine Stelle Q vom Grad eins über P liegen. Dann betrachtet man die

Erweiterung $F'\mathbb{F}_{q^d}/F'$. Auch hierbei handelt es sich um eine Konstantenkörpererweiterung, die daher unverzweigt ist. Sei nun Q_i eine Stelle aus $F'\mathbb{F}_{q^d}$, die über $P_i \in \mathbb{P}_{F'}$ liegt. Der Restklassenkörper $(F'\mathbb{F}_{q^d})_{Q_i}$ ist das Kompositum von $\mathbb{F}_{q^d}$ und $\mathbb{F}_{q^{f_i}}$. Er ist isomorph zu $\mathbb{F}_{q^d}$, da d ein Vielfaches von f_i ist. Folglich haben alle Stellen von $F'\mathbb{F}_{q^d}$, die über einem P_i liegen, den Grad eins. Wegen der Transitivität der Konorm gilt $Con_{F'\mathbb{F}_{q^d}/F}(P) = Q_1 + \cdots + Q_n$ mit $\deg Q_i = 1$ und daher auch $Con_{F'\mathbb{F}_{q^d}/F\mathbb{F}_{q^d}}(Q) = Q_1 + \cdots + Q_n$. □

Lemma 3.7.5. *Sei $\phi : F_1 \longrightarrow F_2$ ein Funktionenkörperhomomorphismus. Sei k' eine beliebige Körpererweiterung des Konstantenköpers k von F_1 und F_2. Betrachtet man die Funktionenkörper $F_1' := F_1k'$ und $F_2' := F_2k'$, so lässt sich ϕ eindeutig zu einem Funktionenkörperhomomorphismus $\phi' : F_1' \longrightarrow F_2'$ fortsetzen, so dass das Diagramm kommutiert.*



Beweis. Es gilt $F_1 = k(x_1, y_1)$ und $F_2 = k(x_2, y_2)$ für geeignete Elemente x_1, y_1, x_2, y_2 aus den Funktionenkörpern. Dann gilt auch $F_1' = k'(x_1, y_1)$ und $F_2' = k'(x_2, y_2)$. Der Funktionenkörperhomomorphismus ϕ ist durch die Bilder von x_1 und y_1 festgelegt. Also sind auch die Bilder von x_1 und y_1 unter ϕ' bereits festgelegt. Wegen der k'-Linearität von ϕ' ist somit die gesamte Abbildung bestimmt. □

3.7.2 Algorithmischer Aspekt

Idee des Algorithmus

Wir wollen nun Theorem 3.7.3 und das dazugehörige Korollar verwenden um für eine Stelle P vom Grad eins von F_1 und einen beliebigen Divisor $D = e_1P_1 + \ldots + e_sP_s$ von F_2 von passendem Grad alle Einbettungen $\phi : F_1 \longrightarrow F_2$ mit $\hat{\phi}(P) = D$ zu berechnen. Da bereits bekannt ist, wie man dieses Problem lösen kann, wenn $\deg(P_1) = \ldots = \deg(P_s) = 1$ gilt, genügt es die anderen Fälle darauf zu reduzieren. Man berechnet zunächst die Grade aller Stellen im Träger von D, sowie deren kleinstes gemeinsames Vielfaches d. Nun wird bei den Funktionenkörpern F_1 und F_2 jeweils eine Konstantenkörpererweiterung vom Grad d durchgeführt. Wenn also F_1 und F_2 über $\mathbb{F}_q$ definiert sind, dann berechnet man $F_1' = F_1\mathbb{F}_{q^d}$ und $F_2' = F_2\mathbb{F}_{q^d}$ die Komposita von F_1 und F_2 mit $\mathbb{F}_{q^d}$, um zwei neue Funktionenkörper mit den gewünschten Konstantenkörpern zu erhalten. Nach 3.7.4 liegt in F_1' genau eine Stelle P' vom Grad eins unverzweigt über P und $D' = Con_{F_2'/F_2}(D)$ besteht nur aus Stellen vom Grad eins. Es sind alle Voraussetzungen erfüllt um die Einbettungen $\phi' : F_1' \longrightarrow F_2'$ mit $\hat{\phi}'(P') = D'$ zu berechnen. Hat man eine solche Abbildung gefunden, so muss noch geprüft werden, ob diese sich zu einer Abbildung $F_1 \longrightarrow F_2$ einschränken lässt.

Einschränken der Abbildungen

Angenommen man hat eine Einbettung $\phi' : F_1' \longrightarrow F_2'$ der Funktionenkörper F_1', F_2', die über dem Konstantenkörper k' definiert sind. Wenn F_1' und F_2' durch Konstantenkörpererweiterung aus den Funktionenkörpern F_1 und F_2 hervorgehen, dann gilt es zu bestimmen, ob sich ϕ' zu einer Abbildung von F_1 nach F_2 einschränken lässt. Dazu wählt man $x_1, y_1 \in F_1,\ x_2, y_2 \in F_2$ mit $F_1 = k(x_1, y_1), F_2 = k(x_2, y_2)$. Dann gilt auch $F_1' = k'(x_1, y_1), F_2' = k'(x_2, y_2)$. Nun genügt es zu überprüfen, ob es sich bei der Darstellung von $\phi'(x_1)$ und $\phi'(y_1)$ als $k'(x_2)$-Linearkombination in der y_2-Potenzbasis bereits um eine $k(x_2)$-Linearkombination handelt. Dazu zerlegt man diese Darstellung in ihre Monome und überprüft, ob die Koeffizienten aller Monome aus k stammen. Genau wenn das der Fall ist, lässt sich die Abbildung zu einer Einbettung von F_1 in F_2 einschränken.

Pseudocode

Algorithmus 6 Gradreduktion

Input: Globale Funktionenkörper F_1, F_2, eine Stelle P von F_1 vom Grad eins, ein Divisor $D = e_1P_1 + \ldots + e_sP_s$ von F_2.

Output: Menge aller Einbettungen $\phi : F_1 \longrightarrow F_2$ mit $\hat{\phi}(P) = D$.

1: Berechne den Grad aller Stellen im Träger von D, $f_i := \deg P_i$.
2: Berechne das kleinste gemeinsame Vielfache der f_i : $d := kgV(f_i)$.
3: Berechne den Konstantenkörper $\mathbb{F}_q$ von F_1 und F_2 .
4: Berechne die Konstantenkörpererweiterungen $F_1' = F_1\mathbb{F}_{q^d}$ und $F_2' = F_2\mathbb{F}_{q^d}$.
5: Berechne $P' := Con_{F_1'/F_1}(P)$ und $D' := Con_{F_2'/F_2}(D)$.
6: Berechne M' die Menge aller Einbettungen von F_1' in F_2', die P' auf D' abbilden unter Verwendung der bisherigen Methoden.
7: **for** $\phi \in M'$ **do**
8: **if** ϕ lässt sich zu Abbildung $F_1 \longrightarrow F_2$ einschränken **then**
9: Berechne die Einschränkung und füge in diese in Menge M ein.
10: **end if**
11: **end for**
12: Gebe M zurück.

Überlegungen zur Korrektheit

Aus 3.7.5 folgt, dass sich, wenn man bei F_1 und F_2 die selbe Konstantenkörpererweiterung durchführt, jede Abbildung $\phi : F_1 \longrightarrow F_2$ zu einer Abbildung der erweiterten Funktionenkörper $\phi' : F_1' \longrightarrow F_2'$ fortsetzt. Das Berechnen aller Einbettungen von F_1' in F_2' liefert also erst recht alle Einbettungen von F_1 in F_2. Interessiert man sich nun für die Einbettungen $\phi : F_1 \longrightarrow F_2$, die eine bestimmte Stelle P auf einen bestimmten Divisor D abbilden, so bekommt man diese, indem man die Abbildungen $\phi' : F_1' \longrightarrow F_2'$ sucht, die P' auf D' abbilden, wobei $P' = Con_{F_1'/F_1}(P)$ und $D' = Con_{F_2'/F_2}(D)$ gilt. Der Grund dafür ist, dass Funktionenkörperhomomorphismen durch ihre Bilder auf ausreichend großen Riemann-Roch-Räumen vollständig bestimmt sind, bei einer Konstantenkörpererweiterung aber die Basis von einem

Riemann-Roch-Raum zu einem Divisor auch eine Basis des Riemann-Roch-Raums der Konorm liefert. Nach Korrolar 3.7.4 zerfallen bei einer Konstantenkörpererweiterung vom Grad d alle Stellen, deren Grad d teilt, zu Stellen vom Grad eins. Diese beiden Überlegungen begründen die Korrektheit der Reduktion von Stellen höheren Grades auf den Fall, dass alle Stellen des betrachteten Divisors den Grad eins haben. In dem Abschnitt zur Berechnung der Parameter wurde dargelegt, dass man eine von den unbekannten Parametern $\lambda_1, \ldots, \lambda_m$ abhängige Abbildung $F_1 \longrightarrow F_2$ für algorithmische Zwecke auch als eine Abbildung in den Funktionenkörper F_2', der aus F_2 durch eine transzendente Konstantenkörpererweiterung mit $k(\lambda_1, \ldots, \lambda_m)$ hervorgeht, auffassen kann. Dieses ist möglich, da wie in Theorem 3.7.3 gezeigt wurde, bei einer Konstantenkörpererweiterung die für den Algorithmus entscheidenen Größen wie das Geschlecht, der Grad von Divisoren und die Basen von den Riemann-Roch-Räumen erhalten bleiben.

3.8 Wahl der Stelle P von F_1

In den vorgestellten Schritten des Algorithmus wurden sehr wenig Voraussetzungen an die Wahl von P gestellt. Die einzige Forderung war, dass P eine Stelle vom Grad eins sein muss, deren erste Polzahl nicht von der Charakteristik des Funktionenkörpers geteilt wird. Damit stellt man sicher, dass eine spezielle lokale Uniformisierende, die die Form von 3.5.4 erfüllt, berechnet werden kann und dass die Koeffizienten einer Reihenentwicklungen von Elementen aus F_1 in einer beliebigen lokalen Uniformisierenden von P alle aus dem Konstantenkörper stammen. Bei vielen Beispielen gibt es verschiedene solche Stellen. Für die Frage, ob es möglich ist die Einbettungen zu berechnen, sind alle Stellen P, die diese Voraussetzungen erfüllen, gleichwertig. In der Praxis kann durch eine speziellere Wahl von P in einigen Schritten die Arbeit verringert werden. In dem Abschnitt über die Eigenschaften der Elemente $x_1, \ldots, x_r \in \mathcal{O}^P$ mit $F_1 = k(x_1, \ldots, x_r)$ wurde gezeigt, dass ihre Anzahl gleich der ersten Polzahl n_1 von P ist. Im nächsten Kapitel wird gezeigt, dass für wachsende Anzahl der x_i auch die Laufzeit einiger Teilalgorithmen wächst. Weiterhin werden für alle Divisoren $D \in \mathcal{D}_{F_2}$ von passendem Grad, für die dim $\mathcal{L}(n_1\, D) \geq 2$ erfüllt ist, Berechnungen durchgeführt. Bei niedrigerer erster Polzahl n_1 sinkt also auch die Anzahl an Divisoren, mit denen gearbeitet werden muss. Somit ist es das Ziel, P so aus der Menge der Stellen vom Grad eins zu wählen, dass die erste Polzahl minimal unter der Nebenbedingung ist, dass sie nicht von der Charakteristik geteilt wird.

3.9 Probleme bei speziellen Funktionenkörpern

Im vorherigen Abschnitt wurde dargelegt, dass der Algorithmus zum Berechnen der Einbettungen eine Stelle P vom Grad eins von F_1 benötigt, deren erste Polzahl nicht von der Charakteristik geteilt wird. Normalerweise existiert solch eine Stelle und dann kann der Algorithmus genau wie beschrieben anwendet werden. Es ist jedoch auch möglich globale Funktionenkörper zu konstruieren, die keine Stellen vom Grad eins besitzen oder bei denen alle ersten Polzahlen von Stellen vom Grad eins von der Charakteristik geteilt werden. In diesen Fällen lässt sich der Algorithmus leicht modifizieren, so dass er weiterhin anwendbar bleibt.

Keine Stellen vom Grad eins

Wenn man die Einbettungen eines Funktionenkörpers, der keine Stellen vom Grad eins besitzt, berechnen will, dann kann dies über Konstantenkörpererweiterungen erreicht werden. In dem Abschnitt über Stellen höheren Grades findet sich die mathematische Theorie, die hier verwendet wird. Dort wird bewiesen, dass wenn Q eine Stelle vom Grad d von F_1 ist, dann zerfällt diese bei einer Konstantenkörpererweiterung vom Grad d zu d Stellen vom Grad eins. Diese Aussage kann man verwenden, wenn man die Einbettungen von F_1 in F_2 berechnen will und F_1 keine Stellen vom Grad eins besitzt. In diesem Fall wählt man eine Stelle Q höheren Grades von F_1 und betrachtet die Funktionenkörper F_1' und F_2' die durch eine Konstantenkörpererweiterung vom Grad deg Q aus F_1 und F_2 hervorgehen. Dann besitzt F_1 nach Konstruktion mindestens d Stellen vom Grad eins, daher kann der Algorithmus angewendet werden, um die Einbettungen von F_1' in F_2' zu berechnen. Anschließend muss man noch prüfen, welche dieser Einbettungen der erweiterten Funktionenkörper sich zu Einbettungen von F_1 in F_2 einschränken lassen. In dem Abschnitt über Stellen höheren Grades wird beschrieben, wie dies algorithmisch geprüft werden kann. Insgesamt kann man also die Einbettungen auch ausgehend von einer Stelle höheren Grades berechnen. Das folgende Lemma gibt an, ab welcher natürlichen Zahl d es mindestens eine Stelle vom Grad d gibt.

Lemma 3.9.1. *Sei F ein Funktionenkörper vom Geschlecht g, der über dem endlichen Körper mit q Elementen definiert ist. Sei B_d die Anzahl der Stellen von F vom Grad d. Dann gilt für alle $d \geq 1$:*

$$|B_d - \frac{q^d}{d}| \leq \left(\frac{q}{q-1} + 2g \frac{q^{1/2}}{q^{1/2}-1} \right) \cdot \frac{q^{r/2}-1}{r}.$$

Beweis. Der Beweis ist bei [Sti93, S.179] nachzulesen. □

Bemerkung 3.9.2. *Nach dieser Formel existiert für d mit $2g+1 \leq q^{(d-1)/2}(q^{1/2}-1)$ mindestens eine Stelle vom Grad d.*

Die Charakteristik teilt die ersten Polzahlen

Bei dem Teilalgorithmus, in dem getestet wird, ob es eine Einbettung ϕ gibt, die die Stelle P auf den Divisor D abbildet, werden Elemente aus F_1 in Reihen in einer speziellen lokalen Uniformisierenden von P entwickelt. Diese lokale Uniformisierende π erhält man, indem zu P ein Element x_1 gewählt wird, welches die erste Polzahl n_1 realisiert, und dann $\pi = \sqrt[n_1]{1/x_1}$ berechnet wird. Dann ermittelt man eine Basis $\{b_1, \ldots, b_m\}$ von $\mathcal{L}(n_1 D)$. Da $\phi(x_1) = \sum_{i=1}^{m} \lambda_i b_i$ gelten muss, liefert diese Gleichung auch eine Darstellung für $\phi(\pi)$ als Reihe, die von den λ_i abhängt und die Berechnung kann mit $\phi(\pi)$ fortgesetzt werden. Damit π als eine n_1-te Wurzel berechnet werden kann, setzt man voraus, dass n_1 nicht von der Charakteristik des Funktionenkörpers geteilt wird. Sollte das jedoch der Fall sein, so kann man im Allgemeinen auf diese Weise keine speziellen lokalen Uniformisierenden berechnen. Es ist trotzdem möglich eine lokale Uniformisierende $\tilde{\pi}$ von P zu berechnen, die in einem Zusammenhang mit den Elementen $x_1, \ldots, x_r \in \mathcal{O}^P$ steht. Berechnet man die gesamte Polsequenz $\{n_1, n_2, \ldots\}$ von P, so fehlen in dieser nach 3.4.3 nur endlich viele natürliche Zahlen, also existiert eine minimale Polzahl n_k, die nicht von der Charakteristik geteilt wird und ein Element $x_k \in F_1$ mit $(x_k)_\infty = n_k P$. Nun kann man eine Basis von $\mathcal{L}(n_1 D)$ zu

einer Basis $\{b_1, \ldots, b_{\tilde{m}}\}$ von $\mathcal{L}(n_k\, D)$ ergänzen und es muss $\phi(x_k) = \sum_{i=1}^{\tilde{m}} \lambda_i b_i$ gelten. Indem man die n_k-te Wurzel aus $1/x_k$ zieht, bekommt man eine lokale Uniformisierende $\tilde{\pi}$ von P, deren Bild unter ϕ als Reihe, die von $\lambda_1, \ldots, \lambda_{\tilde{m}}$ abhängt, bekannt ist. Mit diesem parametrisierten $\phi(\tilde{\pi})$ können die folgenden Schritte des Algorithmus ganz analog durchgeführt werden. Wird also die erste Polzahl an P von der Charakteristik geteilt, so besteht der einzige Unterschied beim Berechnen der Einbettungen darin, dass man nicht mit der ersten sondern mit einer höheren Polzahl arbeitet und daher die Reihen von mehr Parametern abhängen. In der Theorie macht das keinen Unterschied, in der Praxis ist es jedoch ein sehr großer Unterschied, von wie vielen Parametern ein Gleichungssystem abhängt. In dem Abschnitt über die Laufzeit wird analysiert, dass gerade das Lösen dieses Gleichungssystems einen sehr hohen Einfluss auf die Gesamtlaufzeit haben kann. In manchen Fällen kann es daher von Vorteil sein, so vorzugehen, wie wenn es keine Stellen vom Grad eins gäbe. Man führt dann eine Konstantenkörpererweiterung durch und testet, ob unter den Stellen vom Grad eins des erweiterten Funktionenkörpers eine existiert, deren erste Polzahl nicht von der Charakteristik geteilt wird.

3.10 Vergleich des Isomorphie- und des Einbettungsalgorithmus

Wie wir schon im Kapitel 2 gesehen haben, handelt es sich bei dem Einbettungsalgorithmus um eine Verallgemeinerung des Isomorphiealgorithmus. Um die Einbettungen oder Isomorphismen $\phi : F_1 \longrightarrow F_2$ zu berechnen, verwenden beide Algorithmen dieselbe Idee. Man bestimmt mit der Hurwitz-Geschlechtsformel eine obere Schranke n_{max} für den Grad $[F_2 : \phi(F_1)]$. Dann versucht man die Isomorphismen oder Inklusionen zu bestimmen, indem man für eine Stelle P von F_1 vom Grad eins die endliche Menge aller effektiven Divisoren D von F_2 vom Grad kleiner gleich n_{max} daraufhin untersucht, ob es einen Isomorphismus beziehungsweise eine Einbettung der Riemann-Roch-Räume $\mathcal{L}(nP)$ und $\mathcal{L}(nD)$ gibt und ob sich diese Abbildung zu einem Funktionenkörperhomomorphismus fortsetzen lässt. Im Isomorphiefall ist die obere Schranke n_{max} immer gleich eins, also besteht der Divisor D nur aus einer Stelle vom Grad eins. Da n_{max} im Einbettungsfall größer als eins ist, ergibt sich die Notwendigkeit einige Schritte des Algorithmus zu verallgemeinern. So muss man zum Beispiel zwischen separablen und nicht separablen Einbettungen unterscheiden, ein Problem, das bei Isomorphismen nicht auftritt. Weitere Unterschiede resultieren daraus, dass für $n_{max} \geq 2$ deutlich mehr Divisoren als im Isomorphiefall zu überprüfen sind, aber man diese Menge durch ein paar zusätzliche Kriterien, so wie in 3.1 und 3.2 beschrieben, reduzieren kann. Bei beiden Algorithmen verwendet man reduzierte Ganzheitsbasen von $\mathcal{O}^P$ und $\mathcal{O}^S$ mit $S = supp(D)$ um zu testen ob sich ein Vektorraumhomomorphismus der Riemann-Roch-Räume $\mathcal{L}(nP) \longrightarrow \mathcal{L}(nD)$ zu einem Homomorphismus der Funktionenkörper fortsetzen lässt. Ein Unterschied zwischen den beiden Algorithmen liegt darin, wie man die reduzierten Basen bestimmt. Im Isomorphiefall bekommt man, wie in Lemma 3.4.4 beschrieben, eine reduzierte Basis von $\mathcal{O}^S$, indem man Elemente wählt, die spezielle Erzeuger der Polsequenz von D realisieren. Im Einbettungsfall ist der Aufwand um eine reduzierte Basis von $\mathcal{O}^S$ zu berechnen deutlich höher. Hier muss man den holomorphen Ring $\mathcal{O}^S$ mit einem Gitter identifizieren, um dann durch einen Gitterreduktionsalgorithmus eine reduzierte Basis zu bestimmen, so wie in Abschnitt 3.3 beschrieben. Dieser Unterschied tritt auch

auf, wenn man die Fortsetzung der Abbildung konstruiert. In beiden Fällen berechnet man spezielle lokale Uniformisierende der Stelle P und der Stellen aus S und setzt die Abbildung auf die Vervollständigungen der dazugehörigen Bewertungen fort. Im Unterschied zum Isomorphiefall kann S beim Einbettungsfall aus mehr als einer Stelle bestehen. Dann muss man für weitere Untersuchungen die Fortsetzungen auf alle Vervollständigungen gleichzeitig betrachten und dazu identifiziert man diese wieder mit einem Gitter (siehe auch 3.5). Weitere Unterschiede ergeben sich dadurch, dass der Träger von D nicht nur aus mehr als einer Stelle, sondern auch aus Stellen höheren Grades bestehen kann. Die damit verbundenen notwendigen Verallgemeinerungen werden in dem Abschnitt 3.7 beschrieben.

Kapitel 4

Laufzeitanalyse

In diesem Kapitel wird die Laufzeit des Einbettungsalgorithmus analysiert. Im gesamten Abschnitt werden die Funktionenkörper mit F, F_1 und F_2 und ihre Geschlechter mit g, g_1 und g_2 bezeichnet. Sie sind über dem endlichen Körper $\mathbb{F}_q$ definiert. Für einen globalen Funktionenkörper F wird die Anzahl der Stellen vom Grad n mit $B_n(F)$ bezeichnet, und $A_n(F)$ ist definiert als

$$A_n(F) := \#\{D \in \mathcal{D}_F | D \geq 0 \text{ und } \deg D = n\},$$

also als die Anzahl der effektiven Divisoren vom Grad n. Wenn eindeutig ist, welcher Funktionenkörper gemeint ist, schreiben wir nur A_n oder B_n.

Für das Berechnen der Einbettungen besteht die Arbeit des Algorithmus aus zwei Phasen. Als erstes werden einige Vorberechnungen durchgeführt, dann beginnt der Hauptteil.

Bei den Vorberechnungen wird ermittelt, welche Möglichkeiten es für den Grad der Körpererweiterung, die der zweite Funktionenkörper über dem Bild des ersten darstellt, gibt. Dazu werden die Geschlechter der Funktionenkörper sowie deren Klassenzahlen berechnet und es werden alle Stellen bis zu einem bestimmten Grad konstruiert. Diese Schritte können, wie zum Beispiel das Berechnen der Klassenzahlen, mitunter sehr aufwendig sein. Da sie aber nur einmal durchgeführt werden, vernachlässigen wir ihren Einfluss auf die Gesamtlaufzeit erst einmal und betrachten diese Berechnung separat.

Der Hauptteil besteht aus zwei ineinander geschachtelten Schleifen. Die äußere Schleife iteriert über alle möglichen Grade und die innere iteriert über alle effektiven Divisoren des entsprechenden Grades. Für jeden dieser Divisoren wird die Basis eines Riemann-Roch-Raumes und daraus eine reduzierte Ganzheitsbasis berechnet. Es werden spezielle lokale Uniformisierende errechnet und Elemente des Funktionenkörpers in Reihen entwickelt sowie Gleichungssysteme aufgestellt und gelöst. Für die Laufzeit ist daher die Anzahl der Iterationen der Schleifen sowie die Laufzeit der Berechnungen innerhalb der Schleifen relevant.

4.1 Anzahl der Iterationen

Die maximale Anzahl der Iterationen der äußeren Schleife hängt mit den Geschlechtern der beiden Funktionenkörper zusammen. Im schlechtesten Fall kann man durch

die Klassenzahlen keine Grade ausschließen. Dann durchläuft diese Schleife alle natürlichen Zahlen n von 2 bis $\lfloor \frac{g_2-1}{g_1-1} \rfloor$. Bei jedem Durchlauf wird die innere Schleife aufgerufen, wobei diese in der n-ten Iteration der äußeren über alle effektiven Divisoren vom Grad n von F_2 iteriert. Also gibt $A_n(F_2)$ die Anzahl der Iterationen der inneren Schleife in der n-ten Iteration der äußeren an. Somit werden die Berechnungen der inneren Schleife maximal $\sum_{n=2}^{\lfloor g_2-1/g_1-1 \rfloor} A_n(F_2)$-mal aufgerufen. Folglich wird die Anzahl der Iterationen durch das Verhältnis der Geschlechter und durch die Werte $A_n(F_2)$ bestimmt.

Abschätzen der A_n

Um A_n abzuschätzen wird etwas Kombinatorik benötigt.

Lemma 4.1.1. *Man kann mit n Elementen $\binom{n+k-1}{k}$ verschiedene k-elementige Multimengen bilden.*

Beweis. Das kann man einfach nachzählen. □

Definition 4.1.2. *Sei n eine natürliche Zahl. Als* Partition *von n bezeichnet man eine Darstellung von n als Summe natürlicher Zahlen $n = n_1 + \ldots + n_k$. Jede Partition von n lässt sich schreiben als $1^{\alpha_1} 2^{\alpha_2} \ldots n^{\alpha_n}$, wobei α_i die Anzahl der Terme i in der Summe ist. Die Anzahl der verschiedenen Partitionen der Zahl n wird durch die Funktion $p(n)$ gezählt.*

Da die Summe der Grade der Stellen eines Divisors vom Grad n genau n ergibt, liefert jeder effektive Divisor auch eine Partition von n. Für einen beliebigen Funktionenkörper kann man keine genauen Angaben über die Anzahl der Stellen von festem Grad machen, also gibt es nicht unbedingt zu jeder Partition von n auch einen Divisor, bei dem die Grade der Stellen im Träger dieser Partition entsprechen. Trotzdem besteht die Hoffnung, durch das Abschätzen von $p(n)$ Aussagen über A_n machen zu können. Die Funktion $p(n)$ ist für verschiedene kombinatorische Probleme relevant und daher schon sehr genau untersucht worden.

Lemma 4.1.3. *Es gilt:*

$$p(n) < \left\lfloor \frac{\varphi^{n+1}}{\sqrt{5}} + \frac{1}{2} \right\rfloor$$

mit $\varphi = \frac{1+\sqrt{5}}{2}$. Diese Abschätzung kann man noch verfeinern, es bleibt aber $p(n) \sim \frac{e^{\pi\sqrt{2n/3}}}{4n\sqrt{3}}$. Folglich wächst p subexponentiell in n.

Beweis. Ein Beweis findet sich bei [AE04, S.22]. □

Lemma 4.1.4. *Auf der Menge der effektiven Divisoren von Grad n von F definiert*

$$\begin{aligned} A \sim B \quad :\Leftrightarrow \quad & \text{es gibt Stellen } P_1, \ldots, P_k, Q_1, \ldots, Q_k \text{ von } F \text{ mit} \\ & A = P_1 + \ldots + P_k,\ B = Q_1 + \ldots + Q_k \\ & \text{und } \deg(P_i) = \deg(Q_i) \text{ für alle } i \in \{1, \ldots, k\} \end{aligned}$$

eine Äquivalenzrelation. Mit $D_n(F)$ sei die Menge der Äquivalenzklassen bezeichnet. Weiterhin induzieren zwei Repräsentanten derselben Äquivalenzklasse dieselbe Partition von n. Man erhält somit eine wohldefinierte Abbildung von $D_n(F)$ in die Partitionen von n.

Beweis. Die Eigenschaften einer Äquivalenzrelation sind offensichtlich erfüllt. Sind nun A und B Repräsentanten derselben Äquivalenzklasse, so kann man sie jeweils schreiben als $A = P_1 + \ldots + P_k$ und $B = Q_1 + \ldots + Q_k$, wobei gleich indizierte Stellen den gleichen Grad haben. Die von A induzierte Partition ergibt sich genau durch die Summe der Grade der Stelle, ist also gleich der von B induzierten. □

Korollar 4.1.5. *Für einen beliebigen Funktionenkörper F gilt $p(n) \geq \#D_n(F)$.*

Beweis. Wir wissen, dass jede Äquivalenzklasse eine Partition induziert, es aber nicht unbedingt zu jeder Partition eine Klasse gibt, die diese induziert. Gleichheit gilt, wenn der Funktionenkörper ausreichend viele Stellen von jedem Grad besitzt, wobei ausreichend viele bedeutet: $B_k(F) \geq \lfloor n/k \rfloor$. □

Um nun $A_n(F)$ abzuschätzen gilt es, eine Abschätzung für die Kardinalität der Äquivalenzklassen zu bestimmen.

Lemma 4.1.6. *Sei $[A]$ eine Äquivalenzklasse in $D_n(F)$ und $\lambda = 1^{\alpha_1} 2^{\alpha_2} \ldots n^{\alpha_n}$ die dazugehörige Partition von n. Dann gilt:*

$$\#[A] = \prod_{i=1}^{n} \binom{B_i + \alpha_i - 1}{\alpha_i}.$$

Beweis. Wenn man die Partition λ betrachtet, so folgt aus i^{α_i}, dass alle Divisoren der Klasse α_i viele Stellen vom Grad i besitzen. Die Anzahl der Stellen vom Grad i von F ist mit B_i bezeichnet. Nach 4.1.1 gibt es für diesen Anteil des Divisors $\binom{B_i+\alpha_i-1}{\alpha_i}$ verschiedene Möglichkeiten. Das Produkt aller dieser Binomialkoeffizienten gibt die Anzahl an verschiedenen Divisoren, die die Partition λ induzieren. □

Somit kann man die Anzahl der Iterationen in Abhängigkeit von der Anzahl der Stellen von bestimmtem Grad ausdrücken.

Lemma 4.1.7. *Für $r \in \mathbb{N}$ gilt*

$$|B_r - \frac{q^r}{r}| < (2 + 7g)\frac{q^{r/2}}{r}$$

Beweis. Ein Beweis findet sich bei [Sti93, S.178]. □

Fasst man nun diese Ergebnisse zusammen, so sieht man, dass die Anzahl der Iterationen zum Berechnen der Einbettungen hauptsächlich durch zwei Größen, nämlich das Verhältnis der Geschlechter und die Kardinalität des Konstantenkörpers, beeinflusst wird. Nach Lemma 4.1.3 wissen wir, dass die Anzahl der Möglichkeiten, Divisoren vom Grad $n \leq n_{max}$ zusammenzusetzen, subexponentiell in $n_{max} = \frac{g_2-1}{q_1-1}$ wächst. Weiterhin wächst nach Lemma 4.1.7 auch die Anzahl der Stellen vom Grad k exponentiell in k. Außerdem zeigt Lemma 4.1.7 den Einfluss der Kardinalität q des Konstantenkörpers, da sich die Anzahl der Stellen vom Grad k wie ein Polynom vom Grad k in q verhält.

4.2 Aufwand einer Iteration

Um den Aufwand einer Iteration zu berechnen, wird die Anzahl der Operationen gezählt, die bei der Überprüfung, ob die Stelle $P \in \mathbb{P}_{F_1}$ auf $D \in \mathcal{D}_{F_2}$ abgebildet werden kann, durchgeführt werden. Als Operationen bezeichnen wir das Entwickeln eines Elements in eine Reihe, das Berechnen einer Basis eines Riemann-Roch-Raumes, das Berechnen des Poldivisors eines Elements des Funktionenkörpers, Durchführen von elementaren Rechnungen in einem Funktionenkörper und das Lösen von linearen Gleichungssystemen über endlichen Körpern sowie das Rechnen in $\mathbb{Z}$ und $\mathbb{F}_q$. Wenn man die einzelnen Operationen vergleichen oder eine Gesamtlaufzeit angeben will, dann könnte man theoretisch jede von ihnen auf die Anzahl ihrer Rechnungen im Konstantenkörper reduzieren und dann mit diesen Zahlen arbeiten. Doch die genaue Anzahl der Rechnungen in $\mathbb{F}_q$ hängt davon ab, welcher Algorithmus nun im Detail verwendet wird. Ich beschränke mich also darauf anzugeben, von welchen Größen die Laufzeiten der einzelnen Operationen abhängen. Als Quellen für diesen Abschnitt dienten [Hes99] und [Hes02].

Rechnen in $\mathbb{F}_q$

Das Rechnen mit Elementen eines endlichen Körpers ist bei mir die kleinste Einheit, in der der Aufwand von Operationen gemessen wird. Dabei wird angenommen, dass alle Operationen $+$, $-$, $\cdot$, $/$ und das Testen auf Gleichheit unabhängig von den Elementen aus $\mathbb{F}_q$ denselben Aufwand verursachen. Da alle auftretenden ganzen Zahlen relativ klein sind, nehme ich der Einfachheit halber auch an, dass ihre Addition und Multiplikation dieselben Kosten wie das Rechnen in $\mathbb{F}_q$ verursacht. Damit ist dann die Anzahl der Rechnungen in $\mathbb{F}_q$, die das Addieren oder Multiplizieren zweier Polynome aus $\mathbb{F}_q[t]$ benötigen, linear beziehungsweise quadratisch in ihrem Grad. Daraus folgt direkt, dass auch das Addieren oder Multiplizieren zweier Reihen aus $\mathbb{F}_q((t))$ linear beziehungsweise quadratisch in ihrer absoluten Präzision ist.

Rechnen im Funktionenkörper

Ein Funktionenkörper F lässt sich algorithmisch als Quotientenkörper des Restklassenrings $k[x,y]/f(x,y)k[x,y]$ realisieren. Dabei ist das definierende Polynom $f = y^n + a_1 y^{n_1} + \cdots + a_n \in k[x][y]$ irreduzibel, normiert und separabel in y. Wir nehmen an, dass alle Rechnungen in F immer bezüglich dieser Darstellung durchgeführt werden. Der Rechenaufwand bezüglich dieser Darstellung lässt sich in der Größe $C_f := \max\{\lfloor \deg(a_i)/i \rfloor | 1 \leq i \leq n\}$ ausdrücken. Nähere Informationen zu dieser Darstellung finden sich in [Hes99, S.5]. Dort wird auch angegeben, dass die benötigte Zeit für das Addieren und Multiplizieren sowie Invertieren und Vergleichen von Elementen a und b aus F polynomiell in C_f, dem Grad der Körpererweiterung n und dem maximalen Grad der in der Darstellung von a und b auftauchenden Polynome aus $k[x]$ ist. Im Folgenden werden die definierenden Polynome der Funktionenkörper F_1 und F_2, bezüglich denen gerechnet wird, mit f_1 und f_2 oder mit f für einen nicht näher spezifizierten Funktionenkörper bezeichnet.

Rechnen mit Divisoren

Die Divisoren eines Funktionenkörpers kann man entweder als Ideale oder als abstrakte Elemente der von den Stellen erzeugten freien abelschen Gruppe betrachten.

In [Hes02] wird gezeigt, dass das Rechnen mit ihnen sowie das Berechnen von Hauptdivisoren in der einen oder der anderen Form jeweils polynomiell in C_f, $n := [F : k(x)]$ und der Höhe der Divisoren ist. Dabei definiert man die Höhe eines Divisors als $h(D) := \deg(D)_0 + \deg(D)_\infty$. Weiterhin wird dort bewiesen, dass für einen Divisor D auch die Laufzeit des Berechnens der Basis von $\mathcal{L}(D)$ polynomiell in C_f, n und $h(D)$ ist.

Lösen von linearen Gleichungssystemen über $\mathbb{F}_q$

Das Lösen eines linearen Gleichungssystems mit n Gleichungen und n Unbekannten kann man sich als das Ausführen von Zeilenumformungen an einer Matrix aus $M(n \times n, \mathbb{F}_q)$ vorstellen. Offensichtlich ist die Anzahl der benötigten Rechnungen in $\mathbb{F}_q$ für die Überführung einer solchen Matrix in Zeilenstufenform, und somit das Lösen eines solchen Gleichungssystems, polynomiell in n.

Entwickeln von Elementen in Reihen

Für eine lokale Uniformisierende π einer Stelle P und ein Element $a \in F$ kann man die Reihenentwicklung von a bezüglich P berechnen, indem man die Bewertung von a an P ermittelt, dann a durch eine entsprechende π-Potenz teilt und anschließend die entstehende rationale Funktion an P auswertet. Wenn man danach das Vielfache einer geeigneten π-Potenz von a abzieht, kann man dieses Vorgehen wiederholen, um a bis zu einer beliebigen Präzision zu entwickeln. Man erkennt, dass die Anzahl der dafür benötigten Rechnungen in $\mathbb{F}_q$ polynomiell von dem Aufwand für Rechnungen in F abhängt und linear in der gewünschten Präzision wächst.

Ziel ist es nun, eine Abschätzung für die Anzahl der einzelnen Operationen innerhalb einer Iteration anzugeben. Es wird sich zeigen, dass diese Anzahl hauptsächlich von der ersten Polzahl r von P, von $n = \deg D = h(D)$ und von $t = \dim \mathcal{L}(rD)$ abhängig ist. Man möchte nun bestimmen, in welchem Maße diese Werte die Laufzeit beeinflussen und wie sie von Größen wie den Geschlechtern der Funktionenkörper und der Kardinalität des Konstantenkörpers abhängen. Nach 3.4.3 ist die erste Polzahl r einer beliebigen Stelle vom Grad eins immer durch $2g_1$ beschränkt. Diese Abschätzung macht man nicht, da man durch eine geschickte Wahl von P Einfluss auf die erste Polzahl nehmen kann, und es zu untersuchen gilt, was das für Auswirkungen auf die Laufzeit hat. Im Folgenden bezeichnet S den Träger von D, $x_1, \ldots, x_r$ die Erzeuger der Polsequenz von P und $y_1, \ldots, y_l$ eine reduzierte $k[z]$-Basis von $\mathcal{O}^S$. Da man in manchen Schritten mit der Basis eines Riemann-Roch-Raumes arbeitet, erweist sich die folgende Ungleichung als nützlich:

Lemma 4.2.1. *Sei A ein effektiver Divisor. Dann gilt:*

$$\dim \mathcal{L}(A) \leq \deg A + 1.$$

Beweis. Ein Beweis dieser Aussage findet sich in [Sti93, S.18]. □

Innerhalb einer Iteration werden die folgenden aufwendigeren Berechnungen durchgeführt:

1. Berechnen einer Basis eines freien Moduls mit Algorithmus 3.
2. Berechnen von Gleichungen für die Parameter mit Algorithmus 4.

3. Berechnen von Gleichungen für die Parameter mit Algorithmus 5.

4. Lösen des Gleichungssystems der Parameter.

Basis eines freien Moduls

In diesem Teilalgorithmus ist ein Element $z \in F_2$ mit $S = supp((z)_\infty)$ gegeben und man möchte eine $k[z]$-Basis von $\mathcal{O}^S$ berechnen, indem man einen Reduktionsalgorithmus auf die Basis $\mathcal{B}$ eines gewissen Riemann-Roch-Raumes anwendet. Die Anzahl der benötigten Operationen ist abhängig von s der Anzahl der Stellen in S und von der Kardinalität m von $\mathcal{B}$. Als erstes berechnet man den Poldivisor $(z)_\infty$. Es gilt $\deg(z)_\infty = rn$. Dann wird die zu reduzierende Riemann-Roch-Basis $\mathcal{B}$ berechnet. Der Grad des Divisors, zu dem die Basis $\mathcal{B}$ bestimmt wird, ist durch $2g_2 - 2 + \deg(z)_\infty$ beschränkt. Mit dieser Abschätzung kann man auch die minimale Bewertung eines Elementes durch $-(2g_2 - 2 + rn)$ nach unten und ihre Anzahl m mit Lemma 4.2.1 durch $m \leq 2g_2 - 1 + rn$ nach oben abschätzen.

Danach wird jeder Basisvektor an jeder Stelle aus S in eine Reihe entwickelt, was sm Reihenentwicklungen entspricht, wobei die benötigte Präzision in der Größenordnung $2g_2 + rn$ ist. Auf diese Reihenvektoren wird dann der Reduktionsalgorithmus angewandt. Da jeder Reduktionsschritt die Bewertung von mindestens einer Reihe erhöht, diese aber insgesamt nicht größer als null werden, kann man die Anzahl der Schritte des Reduktionsalgorithmus grob durch $s(2g_2 + rn)$ abschätzen. In jedem Schritt wird mit den Reihenvektoren gearbeitet. Dabei wird aber jede Reihe maximal ein Mal mit einer anderen multipliziert und dann addiert, also ist die Anzahl der Rechnungen mit Reihen der Präzision kleiner $2g_2 + rn$ polynomiell in m und s. Anschließend hat man eine Matrix T, die beschreibt, welche Operationen man auf die Basis $\mathcal{B}$ anwenden muss, um eine reduzierte Basis und somit eine Basis von $\mathcal{O}^S$ zu bekommen. Bei T handelt es sich um eine $m \times m$ Matrix mit Einträgen aus F_2. Um die reduzierte Basis zu bekommen, muss man also einen Vektor der Länge m, dessen Einträge die Elemente aus $\mathcal{B}$ sind, an T multiplizieren. Grob abgeschätzt werden dazu m^2 Multiplikationen und $(m-1)m$ Additionen, also $(2m-1)m$ Rechnungen in F_2, benötigt. Wenn man nun $\#S = \#supp((z)_\infty)$ durch den Grad des Divisors D nach oben abschätzt, sieht man, dass sich die Gesamtanzahl an Rechnungen im Konstantenkörper polynomiell in n, g_2, C_{f_2} und dem Grad von F_2 als eine durch f_2 definierte Erweiterung eines rationalen Funktionenkörpers verhält. Da die so erzeugte Basis von $\mathcal{O}^S$ durch Reduktion aus $\mathcal{B}$ hervorgeht, liefert $-(2g_2 - 2 + rn)$ auch eine Schranke für die minimale Bewertung eines Basiselements. Diese Abschätzung wird im Folgenden noch verwendet.

Parameterberechnung 1

Mit diesem Algorithmus wird geprüft, für welche Parameter sich Elemente $x_1, \ldots, x_r$ durch eine $k[z]$-Linearkombination von Elementen $y_1, \ldots, y_l$ darstellen lassen. Um dieses mit einem Gitteralgorithmus berechnen zu können, müssen, analog zu dem oberen Algorithmus, für die Elemente $y_1, \ldots, y_l$ Reihenvektoren berechnet werden. Dafür werden sl Funktionenkörperelemente in Reihen entwickelt. Hier ist man hauptsächlich an den Hauptteilen der Reihen interessiert, daher kann man die benötigte Präzision durch den maximalen Pol der y_i plus eine Konstante abschätzen. Dieser maximale Pol ist nach der Bemerkung des letzten Abschnitts durch $2g_2 - 2 + rn$ nach oben beschränkt. Weiterhin muss für alle $i \in \{1, \ldots, r\}$ die Darstellung von x_i als ein

Vektor, der von gewissen Parametern abhängig ist, berechnet werden. Dazu muss für jede Stelle P in S eine spezielle lokale Uniformisierende π_i bestimmt werden, indem man eine gewisse Wurzel eines Elements aus F_2 berechnet. Das geschieht, indem man das Element, dessen Wurzel berechnet werden soll, in eine Reihe entwickelt und dann die Wurzel iterativ approximiert. Im Beweis zu Lemma 3.5.4 kann man erkennen, dass die dafür benötigte Anzahl an Rechenoperationen im Grundkörper polynomiell in der gewünschten Präzision und der Bewertung des Elements ist. Anschließend entwickelt man x_i in eine Reihe in einer beliebigen lokalen Uniformisierenden π und rechnet diese in eine Reihe in der speziellen lokalen Uniformisierenden π_i um, indem man π durch eine auf p Stellen genaue Approximation von π in π_i ersetzt. Der Aufwand dafür hängt von der Präzision p von π_i und dem betraglich höchsten Exponenten e von π in der Reihenentwicklung von x_i ab. Er entspricht dem Aufwand der Auswertung eines Polynoms vom Grad e an einem Polynom vom Grad p. Verwendet man dafür zum Beispiel das Horner Schema, so lässt sich dieses auf die Multiplikation von e Polynomen vom Grad kleiner gleich ep reduzieren, ist also polynomiell in e und p. Diese Rechnungen werden für alle x_i und alle Stellen in S, also insgesamt rs mal, durchgeführt. Auf die daraus resultierenden Reihenvektoren wendet man einen Reduktionsalgorithmus an. Analog zur Berechnung einer Basis von $\mathcal{O}^S$ zeigt man, dass die dafür benötigte Anzahl an Rechnungen sich durch ein Polynom in g_2, r, und n abschätzen lässt. Nun lässt sich noch e als maximaler Pol eines der x_i durch $2g_1$ und die benötigte Genauigkeit p durch ein Polynom in g_2 abschätzen. Insgesamt verhält sich also die Laufzeit dieses Teilalgorithmus polynomiell in r, n, g_1, g_2 und C_{f_1}, C_{f_2} und den Graden von f_1 und f_2 als Polynome in y..

Parameterberechnung 2

Mit diesem Algorithmus berechnet man, für welche Parameter die Abbildung die algebraischen Relationen zwischen den Elementen erhält. Dazu wird für $x_1, \ldots, x_r$ und von Parametern abhängige $\phi(x_1), \ldots, \phi(x_r)$ getestet, wann für alle $i, j \in \{1, \ldots, r\}$ gilt: $\phi(x_i x_j) = \phi(x_i)\phi(x_j)$. Hierbei kann man sich, wegen der Kommutativität der Multiplikation in Funktionenkörpern, auf solche Paare i, j mit $i \geq j$ beschränken. Es gibt $r(r-1)/2$ solche Paare. Für jedes Paar i, j muss man $x_i x_j$ durch eine Multiplikation in F_1 berechnen und durch das Lösen eines linearen Gleichungssystems eine Darstellung $x_i x_j = p_{1,i,j}(x_1) + \sum_{k=2}^{r} p_{k,i,j}(x_1)x_k$ finden. Die Anzahl der Unbekannten in dem Gleichungssystem verhält sich linear in r und der maximalen Bewertung der x_i an P. Diese ist durch $g_1 + r$ beschränkt. Dann berechnet man $\phi(x_i)\phi(x_j) = p_{1,i,j}(\phi(x_1)) + \sum_{k=2}^{r} p_{k,i,j}(\phi(x_1))\phi(x_k)$, indem man die entsprechenden Additionen und Multiplikationen in F_2 durchführt. Dafür werden r Multiplikationen und $r-1$ Additionen also $2r-1$ Rechnungen in F_2 benötigt und durch das Lösen eines weiteren linearen Gleichungssystems derselben Größenordnung bekommt man die endgültige Darstellung von $\phi(x_i x_j)$ in der Basis von $\mathcal{O}^S$. Zur Berechnung von $\phi(x_i)\phi(x_j)$ ist nur eine Multiplikation in F_2 sowie das Lösen eines weiteren genauso großen linearen Gleichungssystems nötig. Das Vergleichen von $\phi(x_i x_j)$ und $\phi(x_i)\phi(x_j)$ basiert auf dem Vergleich der Koeffizienten. Deren Anzahl entspricht der Anzahl der Unbekannten in den zuvor gelösten Gleichungssystemen. Insgesamt verhält sich also die Anzahl der Rechnungen in $\mathbb{F}_q$, die in diesem Unteralgorithmus durchgeführt werden, polynomiell in r und g_1 sowie in C_{f_1}, C_{f_2} und den Graden der f_i.

Lösen des Gleichungssystems der Parameter

In diesem Unteralgorithmus muss das Gleichungssystem, das beschreibt, welche Parameter eine Einbettung definieren, gelöst werden. Schon im vorherigen Kapitel wurde gezeigt, dass man die Lösungen dieses Gleichungssystems als eine affine Varietät auffassen kann. Die k-rationalen Punkte dieser Varietät lassen sich bestimmen, indem man eine Gröbnerbasis des von den Gleichungen erzeugten Ideals berechnet. Der Aufwand für das Berechnen einer Gröbnerbasis hängt von der Anzahl der Variablen t, von dem höchsten Grad d der das Ideal definierenden Polynome und der Dimension der Varietät ab. Die Anzahl der Variablen wird durch die Dimension von $\mathcal{L}(rD)$ bestimmt. Nach Lemma 4.2.1 kann man sie durch $rn+1$ nach oben abschätzen. Der maximale Grad d ist abhängig von den Bewertungen der Elemente x_i und von der Präzision, mit der das parametrisierte Bild der speziellen lokalen Uniformisierenden berechnet wird. Im Abschnitt zum ersten Teil der Parameterberechnung wurde gezeigt, wie sich die parametrisierten Bilder der x_i berechnen. Dort kann man erkennen, dass der maximale Grad polynomiell in g_1 und g_2 beschränkt ist.

Theorem 4.2.2. *Sei I ein Ideal in einem Polynomring in n Unbekannten über einem Körper. Dann ist die benötigte Zeit für das Berechnen einer Gröbnerbasis in $\mathcal{EXPTIME} = \bigcup_{c>0} O(2^{n^c})$.*

Beweis. Ein Beweis findet sich in [vzGG98]. □

Bemerkung 4.2.3. *Das Berechnen einer Gröbnerbasis ist sogar $\mathcal{EXPTIME}$ vollständig, das bedeutet, man kann jedes in exponentieller Zeit lösbare Problem in exponentieller Zeit auf das Berechnen von Gröbnerbasen reduzieren.*

Erschwerend kommt noch hinzu, dass diese Berechnungen möglicherweise sehr viel Speicherplatz benötigen.

Theorem 4.2.4. *Das Berechnen von Gröbnerbasen ist $\mathcal{EXPSPACE}$ vollständig, das heißt, der benötigte Speicherplatz für das Berechnen einer Gröbnerbasis bei n Unbekannten ist in der Größenordnung 2^{n^c} für ein geeignetes $c \in \mathbb{N}$ und jedes Problem, das mit exponentiell viel Speicherplatz lösbar ist, lässt sich auf das Berechnen von Gröbnerbasen reduzieren.*

Beweis. Für einen Beweis siehe [vzGG98, S.606]. □

Somit besteht wenig Hoffnung, Gröbnerbasen im Allgemeinen effizient zu berechnen, und man kann auch leicht Beispiele konstruieren, bei denen der Algorithmus nicht mehr in der Lage ist, die Einbettungen zu ermitteln. Trotzdem kann man in einigen Fällen etwas bessere Schranken für die Komplexität angeben.

Theorem 4.2.5. *Sei I ein Ideal in einem Polynomring über einem Körper K in n Variablen und sei d der höchste Exponent in einem Erzeugendensystem. Sei die Dimension der Varietät zu I höchstens nulldimensional. Dann ist der benötigte Speicherplatz und die Anzahl der Rechnungen in K in $d^{O(n^2)}$.*

Beweis. Diese Aussage findet sich in [FGLM93]. □

Wie das folgende Lemma zeigt, sind die Voraussetzungen, um Gröbnerbasen in $d^{O(n^2)}$ zu berechnen, in unserem Fall erfüllt.

Lemma 4.2.6. *Die Dimension der durch die Gleichungen bestimmten affinen Varietät im $\overline{k}^m$ ist kleiner gleich null.*

Beweis. Seien die Funktionenkörper $F_1 = k(x_1, \ldots, x_r)$ und $F_2 = k(y_1, \ldots, y_l)$. Angenommen die Dimension der Varietät ist größer gleich eins. Jeder k-rationale Punkt auf der Varietät beschreibt eine Möglichkeit die x_i nach F_2 abzubilden, so dass die Relationen zwischen ihnen erfüllt sind und das Polverhalten korrekt ist. Da der algebraische Abschluss $\overline{k}$ von k unendlich viele Elemente besitzt, besitzt die Varietät auch unendlich viele Punkte, wenn ihre Dimension größer als null ist. Nun betrachtet man die Funktionenkörper $\overline{k}(x_1, \ldots, x_r)$ und $\overline{k}(y_1, \ldots, y_l)$. Sie gehen durch eine Konstantenkörpererweiterung aus F_1 und F_2 hervor. In dem Abschnitt 3.7 über Konstantenkörpererweiterungen wird gezeigt, dass sie jeweils das gleiche Geschlecht und die gleichen Basen für die Riemann-Roch-Räume haben. Daher definiert jeder Punkt der Varietät auch eine Einbettung $\overline{\phi} : \overline{k}(x_1, \ldots, x_r) \longrightarrow \overline{k}(y_1, \ldots, y_l)$, wobei unterschiedliche Punkte offensichtlich unterschiedliche Abbildungen liefern. Das stellt einen Widerspruch dazu dar, dass die Anzahl der Einbettungen ϕ mit $\hat{\phi}(P) = D$ nach Korrolar 1.0.39 endlich ist. □

Zusammenfassung

Wir haben gesehen, dass die Laufzeit in vielen Schritten des Algorithmus polynomiell in den Geschlechtern g_1 und g_2, der ersten Polzahl r, in dem maximalen Einbettungsgrad n_{max} und C_{f_1}, C_{f_2} und den Graden von f_2 und f_2 ist. Insgesamt ist sie aber exponentiell. Der Grund dafür ist die für steigendes n_{max} exponentiell wachsende Anzahl an zu überprüfenden Divisoren und die in der Anzahl der Parameter doppelt exponentielle Laufzeit für das Lösen der Gleichungssysteme der Parameter.

Berechnung der Klassenzahl

Das Berechnen aller Einbettungen eines Funktionenkörpers in einen anderen setzt nicht zwingend die Berechnung der Klassenzahlen voraus. Aber man kann sie als Kriterium zur Einschränkung der möglichen Einbettungsgrade verwenden. Da es mit unter sehr lange dauert, die Klassenzahl zu berechnen, man aber mit ihrer Hilfe möglicherweise die Anzahl der zu überprüfenden Divisoren sehr stark einschränken kann, ist es schwierig zu entscheiden, wann diese Berechnung sinnvoll ist und wann nicht. Wie man in dem Abschnitt 5 der Beispielrechnungen sehen kann, ist es leicht, Funktionenkörper zu konstruieren, bei denen das Berechnen der Einbettungen unter Zuhilfenahme der Klassenzahl wesentlich schneller geht, und andere, bei denen man die Einbettungen leicht, die Klassenzahl aber nur mit sehr viel Aufwand berechnen kann. Grund dafür ist die hohe Komplexität des Problems Klassenzahlen zu berechnen:

Theorem 4.2.7. *Es gibt einen deterministischen Algorithmus, der die Klassenzahl eines globalen Funktionenkörpers berechnet. Die Laufzeit dieses Algorithmus ist polynomiell in C_f und der Kardinalität des Konstantenkörpers aber exponentiell im Geschlecht.*

Beweis. Ein Beweis sowie eine Beschreibung dieses Algorithmus findet sich in [Hes99]. □

Betrachtet man also eine Folge von Tupeln von Funktionenkörpern, bei denen der Quotient der Geschlechter fix bleibt, die Geschlechter aber wachsen, so sieht man, dass

der Aufwand für das Berechnen der Klassenzahlen exponentiell in den Geschlechtern wächst. Der Aufwand für die Berechnungen des Hauptteils des Einbettungsalgorithmus wächst aber nur polynomiell in den Geschlechtern. Daher gibt es einen gewissen Punkt, ab dem es sich bei dieser Folge nicht mehr lohnt die Klassenzahlen zu berechnen, da dieses länger dauert als das gesamte Berechnen der Einbettungen. Weiterhin teilt die Klassenzahl des ersten Funktionenkörpers die des zweiten häufig, wenn eine Einbettung existiert. In diesem Fall gewinnt man durch das Berechnen der Klassenzahl keine hilfreichen Informationen. Hat man andererseits Funktionenkörper F_1 und F_2, zwischen denen keine Einbettungen existieren und deren Geschlecht nicht zu hoch ist, dann ist es recht wahrscheinlich, dass h_{F_1} einen Teiler hat, der h_{F_2} nicht teilt, und in diesem Fall kann man oft ohne weitere Berechnungen sagen, dass keine Einbettungen existieren können.

Kapitel 5

Beispiele

In diesem Kapitel betrachten wir einige Beispiele für die Berechnungen von Einbettungen. Alle Berechnungen wurden mit dem Computeralgebrasystem Magma [BCP97] auf einem Intel Core2Duo (64-Bit) System mit 2-GHz-Taktung durchgeführt. Die Ergebnisse sind in den folgenden Tabellen aufgelistet. Jedes Kästchen korrespondiert zu einer Berechnung der Einbettungen von F_1 nach F_2 und enthält die folgenden Werte: Die definierenden Gleichungen f_1 und f_2 der Funktionenkörper, ihre Geschlechter g_1 und g_2, den Konstantenkörper k, über dem F_1 und F_2 definiert sind, die Anzahl der gefundenen separablen Einbettungen $\#\mathrm{Hom}(F_1, F_2)$, die Dauer t der Berechnung in Sekunden und die Anzahl der zu überprüfenden Divisoren $\#D$.

Wachsende Konstantenkörper

In der ersten Testreihe wird der Einfluss der Kardinalität des Konstantenkörpers auf die Laufzeit untersucht. Dazu sind die Funktionenkörper F_1 und F_2 so konstruiert, dass Einbettungen existieren. Nun betrachten wir, wie sich die Laufzeit des Algorithmus bei Konstantenkörpererweiterungen verhält. Bei den Tests wurden die Klassenzahlen nicht mitberechnet. Die Dauer dafür ist bei großen Konstantenkörpern recht hoch. Bei beiden Testserien reicht der Speicherplatz ab dem Konstantenkörper $\mathbb{F}_{p^5}$ nicht mehr aus, um die Menge der zu überprüfenden Divisoren zu konstruieren.

$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + 1)y^2 + x^{14} + x^9 + x^4$				
$g_1 = 3$	$g_2 = 7$	$\#D = 110$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 20$
$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_{3^2}$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + 1)y^2 + x^{14} + x^9 + x^4$				
$g_1 = 3$	$g_2 = 7$	$\#D = 1256$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 40$

$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_{3^3}$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + 1)y^2 + x^{14} + x^9 + x^4$				
$g_1 = 3$	$g_2 = 7$	$\#D = 37136$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 430$
$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_{3^4}$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + 1)y^2 + x^{14} + x^9 + x^4$				
$g_1 = 3$	$g_2 = 7$	$\#D = 645500$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 7516$
$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + x + 1)y^2 + x^{14} + 3x^9 + 4x^8 + 3x^7 + x^4$				
$+x^3 + x^2 + x + 1$				
$g_1 = 3$	$g_2 = 6$	$\#D = 15$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 141$
$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_{5^2}$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + x + 1)y^2 + x^{14} + 3x^9 + 4x^8 + 3x^7 + x^4$				
$+x^3 + x^2 + x + 1$				
$g_1 = 3$	$g_2 = 6$	$\#D = 667$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 613$
$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_{5^3}$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + x + 1)y^2 + x^{14} + 3x^9 + 4x^8 + 3x^7 + x^4$				
$+x^3 + x^2 + x + 1$				
$g_1 = 3$	$g_2 = 6$	$\#D = 13989$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 16779$
$f_1(x,y) = y^2 + x^7 + 1$				$k = \mathbb{F}_{5^4}$
$f_2(x,y) = y^4 + (2x^7 + 2x^2 + x + 1)y^2 + x^{14} + 3x^9 + 4x^8 + 3x^7 + x^4$				
$+x^3 + x^2 + x + 1$				
$g_1 = 3$	$g_2 = 6$	$\#D = 412339$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 20620$

Wachsende Geschlechter

Bei dieser Testserie sind die Funktionenkörper so konstruiert, dass Einbettungen existieren und der maximale Einbettungsgrad jeweils zwei ist, sich aber die Geschlechter ändern. Bei den Berechnungen wurde die Klassengruppe nicht berechnet, da die Dauer dafür bei wachsendem Geschlecht stark ansteigt, also den Einfluss der Geschlechter auf die Dauer der anderen Berechnungen verzerrt.

$f_1(x,y) = y^2 + x^5 + x + 1$	$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^5 + 2x^2 + 4x + 4)y^2 + x^{10} + 3x^7 + x^4$	
$g_1 = 2 \quad g_2 = 3 \quad \#D = 70 \quad \#\mathrm{Hom}(F_1, F_2) = 8$	$t = 49$
$f_1(x,y) = y^2 + x^7 + x + 1$	$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^7 + 4x + 4)y^2 + x^{14}$	
$g_1 = 3 \quad g_2 = 6 \quad \#D = 86 \quad \#\mathrm{Hom}(F_1, F_2) = 2$	$t = 519$
$f_1(x,y) = y^2 + x^9 + x^2 + 1$	$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^9 + 4x^2 + 2x + 4)y^2 + x^{18} + 3x^{10} + x^2$	
$g_1 = 4 \quad g_2 = 9 \quad \#D = 71 \quad \#\mathrm{Hom}(F_1, F_2) = 2$	$t = 210$
$f_1(x,y) = y^2 + x^{11} + x + 1$	$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^{11} + 2x^2 + 2x)y^2 + x^{22} + 3x^{13} + 2x^{12} + 4x^{11}$	
$+x^4 + 3x^3 + 2x^2 + 4x + 4$	
$g_1 = 5 \quad g_2 = 11 \quad \#D = 41 \quad \#\mathrm{Hom}(F_1, F_2) = 2$	$t = 277$
$f_1(x,y) = y^2 + x^{13} + x + 1$	$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^{13} + 2x^2 + 2x)y^2 + x^{26} + 3x^{15} + 2x^{14} + 4x^{13}$	
$+x^4 + 3x^3 + 2x^2 + 4x + 4$	
$g_1 = 6 \quad g_2 = 13 \quad \#D = 52 \quad \#\mathrm{Hom}(F_1, F_2) = 2$	$t = 2233$
$f_1(x,y) = y^2 + x^5 + 2x^3 + x^2 + x + 1$	$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^5 + x^3 + 1)y^2 + x^{10} + x^8 + x^7 + 2x^6 + 2x^5 + 2x^3 + x^2$	
$g_1 = 2 \quad g_2 = 3 \quad \#D = 14 \quad \#\mathrm{Hom}(F_1, F_2) = 4$	$t = 7$
$f_1(x,y) = y^2 + x^7 + 2x^6 + x^5 + x^4 + 2$	$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^7 + x^6 + 2x^5 + 2x^4 + 2x^2 + 2)y^2 + x^{14} + x^{13}$	
$+2x^{10} + x^7 + x^6 + x^4$	
$g_1 = 3 \quad g_2 = 6 \quad \#D = 17 \quad \#\mathrm{Hom}(F_1, F_2) = 2$	$t = 10$
$f_1(x,y) = y^2 + x^9 + x^7 + x + 2$	$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^9 + 2x^7 + x^2)y^2 + x^{18} + 2x^{16} + x^{14} + 2x^{11} + x^{10}$	
$+x^9 + x^8 + 2x^7 + x^4 + x^3 + x + 1$	
$g_1 = 4 \quad g_2 = 7 \quad \#D = 25 \quad \#\mathrm{Hom}(F_1, F_2) = 2$	$t = 58$

$f_1(x,y) = y^2 + x^{11} + x^3 + 2x + 2$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^{11} + 2x^3 + x^2 + 2x)y^2 + x^{22} + 2x^{14} + 2x^{13}$				
$+2x^{11} + x^6 + 2x^5 + x^4 + 2x^3 + 2x^2 + 1$				
$g_1 = 5$	$g_2 = 9$	$\#D = 14$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 20$
$f_1(x,y) = y^2 + x^{13} + 2x^4 + x + 2$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^{13} + x^4 + x^2)y^2 + x^{26} + x^{17} + 2x^{15} + x^{14}$				
$+2x^{13} + x^8 + x^6 + 2x^5 + 2x^4 + x^3 + x + 1$				
$g_1 = 6$	$g_2 = 11$	$\#D = 14$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 58$

Einfluss der Klassenzahl

Die folgenden Beispiele sollen den Einfluss der Berechnung der Klassenzahl auf die Gesamtdauer illustrieren. Es wird jeweils angegeben, ob die Klassenzahl berechnet wurde und welche Einbettungsgrade möglich sind. Die Beispiele sind so konstruiert, dass sich die Dauer einmal kaum ändert, einmal stark wächst und einmal deutlich geringer ist. Trotzdem stellen sie keine Sonderfälle dar. Vielmehr soll man erkennen, dass bei Beispielen, bei denen sowohl der Konstantenkörper als auch die Geschlechter klein sind oder bei denen man vermutet, dass es keine Einbettungen gibt, die Berechnung der Klassenzahl fast immer sinnvoll ist, bei wachsendem Geschlecht aber schnell die Dauer der Klassengruppenberechnung die Gesamtdauer dominieren kann.

$f_1(x,y) = y^2 + x^7 + 3x^4 + 1$				$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^7 + x^4 + 2x^2 + 3)y^2 + x^{14} + x^{11} + 3x^9 + 4x^8 + x^7$				
$+4x^6 + 4x^4 + 4x^2 + 4$				
$g_1 = 3$	$g_2 = 7$	$\#D = 136$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 40$
Klassenzahlen berechnet: $TRUE$				mögliche Grade:2, 3
$f_1(x,y) = y^2 + x^7 + 3x^4 + 1$				$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^7 + x^4 + 2x^2 + 3)y^2 + x^{14} + x^{11} + 3x^9 + 4x^8 + x^7$				
$+4x^6 + 4x^4 + 4x^2 + 4$				
$g_1 = 3$	$g_2 = 7$	$\#D = 136$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$t = 38$
Klassenzahlen berechnet: $FALSE$				mögliche Grade:2, 3
$f_1(x,y) = y^3 + x^7 + x^2 + 1$				$k = \mathbb{F}_5$
$f_2(x,y) = y^6 + (4x^2 + 2)y^4 + (2x^7 + 2x^2 + 2)y^3 + (2x^4 + 2x^2 + 3)y^2$				
$+(2x^9 + x^7 + 2x^4 + 3x^2 + 1)y + x^{14} + 2x^9 + 2x^7 + 2x^6 + 4x^4 + x^2$				
$g_1 = 6$	$g_2 = 14$	$\#D = 34$	$\#\mathrm{Hom}(F_1, F_2) = 1$	$t = 875$
Klassenzahlen berechnet: $TRUE$				mögliche Grade:2

$f_1(x,y) = y^3 + x^7 + x^2 + 1$				$k = \mathbb{F}_5$
$f_2(x,y) = y^6 + (4x^2+2)y^4 + (2x^7+2x^2+2)y^3 + (2x^4+2x^2+3)y^2$				
$+(2x^9 + x^7 + 2x^4 + 3x^2 + 1)y + x^{14} + 2x^9 + 2x^7 + 2x^6 + 4x^4 + x^2$				
$g_1 = 6$	$g_2 = 14$	$\#D = 34$	$\#\mathrm{Hom}(F_1, F_2) = 1$	$t = 36$
Klassenzahlen berechnet: $FALSE$				mögliche Grade:2

$f_1(x,y) = y^2 + x^5 + 3x^4 + 3$				$k = \mathbb{F}_7$
$f_2(x,y) = y^3 + x^6 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 350$	$\#\mathrm{Hom}(F_1, F_2) = 0$	$t =< 1$
Klassenzahlen berechnet: $TRUE$				mögliche Grade: keine

$f_1(x,y) = y^2 + x^5 + 3x^4 + 3$				$k = \mathbb{F}_7$
$f_2(x,y) = y^3 + x^6 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 350$	$\#\mathrm{Hom}(F_1, F_2) = 0$	$t = 38$
Klassenzahlen berechnet: $FALSE$				mögliche Grade:2, 3

Einfluss der Polynomgrade und der Koeffizienten

Bei dieser Testreihe wird der Einfluss von C_{f_1}, C_{f_2} und den Graden der definierenden Polynome f_1 und f_2 untersucht. Dazu werden die Funktionenkörper F_1 und F_2 durch unterschiedliche definierende Polynome erzeugt und jeweils die benötigte Zeit zur Berechnung der Einbettungen ermittelt. Die angegebene Zeit bezieht sich hierbei nur auf die Dauer der Berechnung der Einbettungen vom Grad zwei. Es wird jeweils darauf verzichtet die Klassenzahlen zu ermitteln. Bei wachsenden Graden der Polynome oder wachsendem C_f ist besonders der zweite Teil der Parameterberechnung für den Anstieg der Laufzeit verantwortlich. In diesem Schritt werden die parametrisierten Bilder $\phi(x_i)\phi(x_j)$ und $\phi(x_i x_j)$ berechnet. Das kann sehr aufwändig sein, da es sich bei den Elementen, mit denen gearbeitet wird, um sehr große multivariate rationale Funktionen handelt, sodass es mitunter schon lange dauert, diese einfach nur zu addieren. Für größer werdende Grade von F_1 und F_2 als Erweiterungen ihrer rationalen Funktionenkörper und wachsendes C_{f_1} und C_{f_2} werden auch die rationalen Funktionen, mit denen gerechnet wird, noch komplexer und die Berechnung von $\phi(x_i)\phi(x_j)$ und $\phi(x_i x_j)$ daher aufwändiger. Hierbei hat der Grad von F_2 und C_{f_2} einen weit stärkeren Einfluss auf die Laufzeit als der Grad von F_1 und C_{f_1}. Der Grund dafür ist, dass es sich bei $\phi(x_i)$ um ein von Parametern abhängiges Element von F_2 handelt und darum die meisten Rechungen dieses Unteralgorithmus in F_2 stattfinden.

$f_1(x,y) = y^2 + x^5 + x^2 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$				
$g_1 = 4$	$g_2 = 7$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 10$
$C_{f_1} = 3$	$C_{f_2} = 3$	$\deg(f_1) = 2$	$\deg(f_2) = 4$	
$f_1(x,y) = y^8 + y^6 + 2xy^4 + (2x^3 + x + 1)y^2 + x^5 + 2x^3 + x^2$				$k = \mathbb{F}_3$
$+2x + 1$				
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 11$
$C_{f_1} = 1$	$C_{f_2} = 3$	$\deg(f_1) = 8$	$\deg(f_2) = 4$	
$f_1(x,y) = y^{14} + y^{12} + xy^{10} + (2x + 2)y^8 + (2x^2 + x + 2)y^6$				$k = \mathbb{F}_3$
$+xy^4 + (x^3 + 2x + 1)y^2 + 2x^5 + x^3 + x + 1$				
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 13$
$C_{f_1} = 1$	$C_{f_2} = 3$	$\deg(f_1) = 14$	$\deg(f_2) = 4$	
$f_1(x,y) = y^{18} + y^{14} + y^{12} + 2y^{10} + (x^2 + 2x)y^8 + (x^2 + 2)y^6$				$k = \mathbb{F}_3$
$+(x^2 + x + 2)y^4 + (x^3 + x^2 + x + 2)y^2 + 2x^5 + x^3 + x + 2$				
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 58$
$C_{f_1} = 1$	$C_{f_2} = 3$	$\deg(f_1) = 18$	$\deg(f_2) = 4$	
$f_1(x,y) = y^{22} + 2y^{20} + (2x + 2)y^{16} + (2x^2 + 1)y^{12} + (2x^2 + 1)y^{10}$				$k = \mathbb{F}_3$
$+(2x^2 + x)y^8 + (x^2 + 2x + 2)y^6 + xy^4 + (2x^4 + x^3 + x + 2)y^2$				
$+2x^5 + 2x^4 + x^3 + x^2 + 2x + 1$				
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 69$
$C_{f_1} = 1$	$C_{f_2} = 3$	$\deg(f_1) = 22$	$\deg(f_2) = 4$	
$f_1(x,y) = y^2 + x^5 + x^2 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^{16} + (2x + 1)y^{12} + (2x^5 + 2x^3 + x^2 + x)y^8 + (x^5 + x^4)y^6$				
$+(x^8 + x^5)y^2 + x^{10} + 2x^5 + 1 + (2x^5 + 2x^3 + 2x + 1)y^4$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 1758$
$C_{f_1} = 3$	$C_{f_2} = 1$	$\deg(f_1) = 2$	$\deg(f_2) = 16$	

$f_1(x,y) = y^2 + x^5 + x^2 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^{32} + 2y^{28} + (2x+1)y^{24} + 2x^2y^{22} + (2x^3 + x^2 + 2x + 2)y^{20}$				
$+(2x^4 + x^3 + 2x^2)y^{18} + (2x^5 + x^4 + x^3 + x^2 + 1)y^{16} + (x^5 + x^4 + x^3)y^{14}$				
$+(x^5 + x^3 + 2x + 2)y^{12} + (x^4 + 2x^2)y^{10} + (x^6 + 2x^5 + 2x^4 + x^3 + x^2$				
$+2x + 1)y^8 + (x^7 + 2x^5 + x^4 + x^3 + 2x^2)y^6 + (x^8 + x^5 + x^4 + 2x^32)y^4$				
$+(x^9 + x^5 + 2x^4)y^2 + x^{10} + 2x^5 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t > 10^5$
$C_{f_1} = 3$	$C_{f_2} = 1$	$\deg(f_1) = 2$	$\deg(f_2) = 32$	
$f_1(x,y) = y^2 + x^4y + x^8 + x^5 + x^2 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 11$
$C_{f_1} = 4$	$C_{f_2} = 3$	$\deg(f_1) = 2$	$\deg(f_2) = 4$	
$f_1(x,y) = y^2 + x^{20}y + x^{40} + x^5 + x^2 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 11$
$C_{f_1} = 20$	$C_{f_2} = 3$	$\deg(f_1) = 2$	$\deg(f_2) = 4$	
$f_1(x,y) = y^2 + x^5 + x^2 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^{15} + x^6)y^2 + x^{30} + x^{15} + 1$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 32$
$C_{f_1} = 3$	$C_{f_2} = 8$	$\deg(f_1) = 2$	$\deg(f_2) = 4$	
$f_1(x,y) = y^2 + x^5 + x^2 + 1$				$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^{23} + x^{14})y^2 + x^{46} + x^{31} + x^{16}$				
$g_1 = 2$	$g_2 = 4$	$\#D = 9$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$t = 33$
$C_{f_1} = 3$	$C_{f_2} = 12$	$\deg(f_1) = 2$	$\deg(f_2) = 4$	

Kapitel 6

Weitere Berechnungsmöglichkeiten für Einbettungen

6.1 Kurven über Funktionenkörpern

In diesem Abschnitt werden einige Überlegungen zum Zusammenhang zwischen Einbettungen von Funktionenkörpern und den Punkten einer über einem Funktionenkörper definierten Kurve gemacht. Für ausführlichere Informationen über Kurven und Varietäten sei auf [Har77] verwiesen. In unserem Zusammenhang reicht die folgende etwas abgespeckte Definition.

Definition 6.1.1. *Sei K ein beliebiger Körper und p ein bivariates irreduzibles Polynom mit Koeffizienten aus K. Dann bezeichnen wir die Menge*

$$S_p := \{(a,b) \in \overline{K}^2 \,|\, p(a,b) = 0\}$$

als Kurve. *Für eine beliebige algebraische Körpererweiterung $\tilde{K}$ von K wird die Menge*

$$S_p(\tilde{K}) := \{(a,b) \in \tilde{K}^2 \,|\, p(a,b) = 0\}$$

*als die $\tilde{K}$-*rationalen Punkte *der Kurve bezeichnet.*

Zwei Funktionenkörper F_1 und F_2 über dem Konstantenkörper k kann man durch die Wahl separierender Elemente x_1 und x_2 schreiben als $F_1 = k(x_1, y_1)$ und $F_2 = k(x_2, y_2)$, wobei y_1 und y_2 algebraisch über $k(x_1)$ beziehungsweise $k(x_2)$ sind und die Gleichungen f_1 beziehungsweise f_2 erfüllen. Durch Ausmultiplizieren aller Nenner wird f_1 ein irreduzibles Polynom in zwei Variablen über k. Da aber k eine Teilmenge von F_2 ist, kann man f_1 auch als multivariates Polynom über F_2 auffassen.

Lemma 6.1.2. *Seien $F_1 = k(x_1, y_1)$ und $F_2 = k(x_2, y_2)$ zwei Funktionenkörper mit definierenden Gleichungen f_1 beziehungsweise f_2 und fasst man wie oben beschrieben f_1 als bivariates Polynom über F_2 auf, dann gilt: Jede Einbettung $\phi : F_1 \longrightarrow F_2$ liefert einen Punkt auf der durch f_1 definierten Kurve S_{f_1}. Dieser Punkt liegt in $(F_2 \setminus k)^2$. Umgekehrt korrespondiert jeder F_2-rationale Punkt der Kurve, der nicht in k_0^2 liegt, zu einer Einbettung von F_1 in F_2.*

Beweis. Für alle Elemente a, b von F_2 gilt $\phi(f_1(a,b)) = f_1(\phi(a), \phi(b))$, da ϕ die im Konstantenkörper k liegenden Koeffizienten des Polynoms f_1 fix lässt. Somit gilt $f_1(\phi(x_1), \phi(y_1)) = 0$ und $(\phi(x_1), \phi(y_1) \in F_2^2$ liegt auf der Kurve S_{f_1}. Da ϕ als Körperhomomorphismus injektiv ist und da x_1 und y_1 nicht in k liegen, liegen auch ihre Bilder nicht im Konstantenkörper. Sei nun $(a,b) \in F_2^2 \setminus k_0^2$ mit $f_1(a,b) = 0$. Sei ohne Beschränkung der Allgemeinheit $a \notin k_0$. Dann ist a transzendent über k. Also ist auch b transzendent über k, da sonst $f_1(a,b) = 0$ einen Widerspruch zur Transzendenz von a darstellen würde. Somit liegt (a,b) in $(F_2 \setminus k_0)^2$. Setzt man nun die Identität auf dem Konstantenkörper durch $x_1 \mapsto a$, $y_1 \mapsto b$ fort, so liefert das einen Ringhomomorphismus ϕ von $k[x_1, y_1]$ nach F_2. Da $\phi(f_1(a,b)) = 0$ gilt, ist ϕ auch eingeschränkt auf den Restklassenring $k[x_1, y_1]/(f(x_1, y_1))$ wohldefiniert und lässt sich auch auf dessen Quotientenkörper fortsetzen. Dieser Quotientenkörper ist isomorph zu F_1, also liefert uns das insgesamt einen Funktionenkörperhomomorphismus $\phi : F_1 \longrightarrow F_2$. □

Dieses Lemma liefert einen alternativen Ansatz zur Berechnung von Einbettungen durch das Finden von Nullstellen eines bivariaten Polynoms über einem Funktionenkörper.

Idee des Algorithmus

Seien wie zuvor $F_1 = k(x_1, y_1)$ und $F_2 = k(x_2, y_2)$ zwei durch f_1 beziehungsweise f_2 definierte Funktionenkörper. Ziel ist es nun, die Nullstellen von f_1 über F_2 zu finden, die nicht im exakten Konstantenkörper liegen. Dazu gibt man sich eine Schranke n vor und schreibt $\phi(x_1) = \frac{p_1(x_2,y_2)}{p_2(x_2,y_2)}$ und $\phi(y_1) = \frac{q_1(x_2,y_2)}{q_2(x_2,y_2)}$, wobei p_1, p_2, q_1, q_2 Polynome in zwei Variablen mit unbekannten Koeffizienten und durch n beschränkten Graden sind. Nun kann man f_1 an $(\frac{p_1(x_2,y_2)}{p_2(x_2,y_2)}, \frac{q_1(x_2,y_2)}{q_2(x_2,y_2)})$ auswerten und die resultierende rationale Funktion modulo f_2 reduzieren. Man bekommt ein Element a aus F_2, das noch von den unbekannten Koeffizienten der Polynome p_1, p_2, q_1 und q_2 abhängt. Gesucht sind die Werte für die Koeffizienten, für die $a = 0$ gilt. Diese lassen sich bestimmen, indem man das resultierende Gleichungssystem durch Gröbnerbasenberechnung löst. Für eine ausreichend hohe Schranke n sollten sich auf diese Weise alle Nullstellen von f_1 über F_2 und somit alle Einbettungen berechnen lassen.

Praktische Probleme

In der Praxis erweist sich diese Methode leider als nicht sehr praktikabel. Selbst bei relativ niedrigen Polynomgraden genügt der Speicher, der mir zur Verfügung stehenden Rechner nicht, um das Gleichungssystem zu lösen oder zu entscheiden, ob es Lösungen geben kann. Die Ursache dafür liegt in dem exponentiellen Wachstum des Speicherplatzes, den das Lösen von polynomiellen Gleichungssystemen mit steigender Anzahl der Variablen benötigt. Die Laufzeit des in den vorherigen Kapiteln vorgestellten Algorithmus ist zwar auch exponentiell und es müssen Gröbnerbasen berechnet werden, doch die Anzahl der Variablen in den Gleichungssystemen ist deutlich niedriger. Dieses Reduzieren der Anzahl der Variablen hat einen entscheidenden Einfluss auf die Laufzeit und rechtfertigt die wesentlich umfangreichere Theorie, die für den Algorithmus verwendet wird.

6.2 Einbettungen unter speziellen Voraussetzungen

Anhand der Beispiele in 5 erkennt man, dass das Berechnen aller Einbettungen mitunter sehr lange dauern kann. Wir beschäftigen uns mit der Frage, ob und wie sich die Dauer der Berechnung reduzieren lässt, wenn man zusätzliche Voraussetzungen schafft. Im Folgenden wird ein Algorithmus vorgestellt, der nur solche Einbettungen $\phi : F_1 \longrightarrow F_2$ berechnet, bei denen $F_2/\phi(F_1)$ galoissch ist. Solche Abbildungen werden wir galoissch nennen.

Idee des Algorithmus

Der Algorithmus zum Berechnen der galoisschen Einbettungen basiert darauf, dass man mit Hilfe des in [Hes04] vorgestellten Algorithmus deutlich schneller Isomorphismen von Funktionenkörpern als deren Einbettungen berechnen kann. Ist nun $F_2/\phi(F_1)$ galoissch, so ist $\phi(F_1)$ der Fixkörper einer $[F_2 : \phi(F_1)]$-elementigen Untergruppe der k-Automorphismengruppe von F_2. Wenn man mit der Hurwitz-Geschlechtsformel eine obere Schranke n_{max} für den Grad einer galoisschen Abbildung bestimmt, dann reduziert sich das Problem darauf, die zu F_1 isomorphen Fixkörper von Untergruppen der Ordnung kleiner gleich n_{max} der k-Automorphismengruppe von F_2 zu bestimmen. Falls die Automorphismengruppe von F_2 nur relativ wenig in Frage kommende Untergruppen besitzt und diese sich schnell berechnen lassen, besteht die Hoffnung, dass man die galoisschen Einbettungen im Vergleich zu allen Einbettungen deutlich schneller finden kann. Es verbleibt die Frage, wie man zu einer Untergruppe U der k-Automorphismengruppe von F_2 den Fixkörper F_2^U berechnen kann. Die folgende Aussage zeigt, dass dieser genau der gesuchte Unterkörper ist.

Lemma 6.2.1. *Sei F/k ein Funktionenkörper und G eine endliche Untergruppe der k-Automorphismengruppe von F. Bezeichne F^G den Fixkörper von G. Dann ist die Erweiterung F/F^G galoissch mit Galoisgruppe G.*

Beweis. Ein Beweis findet sich bei [Lor92, S.91]. □

Berechnung von Fixkörpern

Die im Folgenden vorgestellte Methode zum Berechnen von Fixkörpern basiert auf einem Lemma aus [LV93]. Dort finden sich auch ein Beweis sowie detailliertere Informationen zu dem Berechnen von Unterkörpern.

Lemma 6.2.2. *Sei K ein Körper, α algebraisch über K und L ein Zwischenkörper von $K(\alpha)$ und K mit $d = [K(\alpha) : L]$. Seien $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ die Konjugierten von α über L. Dann wird L über K durch die d elementarsymmetrischen Polynome in $\alpha_1, \ldots, \alpha_d$ erzeugt.*

Dieses Lemma bezieht sich auf die Konstruktion von Zwischenkörpern. Will man es für die Berechnung von Fixkörpern verwenden, dann erweist sich die folgende Aussage als nützlich.

Lemma 6.2.3. *Sei U eine Untergruppe der Automorphismengruppe eines globalen Funktionenkörpers F der Charakteristik p. Dann gibt es ein separierendes Element von F, das von den Automophismen aus U fix gelassen wird.*

Beweis. Als Untergruppe einer endlichen Gruppe ist U selbst endlich. Sei nun x ein beliebiges Element von F, das transzendent über dem Konstantenkörper ist. Für $x' = \prod_{\sigma \in U} \sigma(x)$ gilt dann

$$\tau(x') = \prod_{\sigma \in U} \tau(\sigma(x)) = \prod_{\sigma' \in U} \sigma'(x) = x' \text{ für alle } \tau \text{ in } U.$$

Das heißt x' wird von U fix gelassen. Weiterhin ist nach 6.2.1 die Erweiterung F/F^U galoissch vom Grad $\#U$. Somit gilt $x' = N_{F/F^U}(x)$, also ist x' ebenfalls transzendent. Wenn nun x' kein separierendes Element von F ist, dann gibt es nach [Sti93, S.128] ein Element $z \in F$ mit $z^p = x'$. Für $\sigma \in U$ gilt dann $\sigma(z)^p = z^p$ also $\sigma(z) = \omega z$ für eine p-te Einheitswurzel. Da aber F die Charakteristik p hat, muss gelten $\omega = 1$, also $\sigma(z) = z$. Sukzessives Wiederholen dieses Arguments liefert nach endlich vielen Schritten ein separierendes Element, das von U fix gelassen wird. □

Sei nun F/k ein globaler Funktionenkörper und U eine d-elementige Untergruppe von $Aut_k(F)$. Dann wählen wir ein separierendes Element x', das von den Automorphismen aus U fix gelassen wird. Nun gilt $k(x') \subseteq F^U \subseteq F$, die Voraussetzungen von 6.2.2 sind also erfüllt. Für ein primitives Element y von $F/k(x')$ enthält die Menge $M := \{\sigma(y) \mid \sigma \in U\}$ nach 6.2.1 genau die Konjugierten von y über F^U. Also bekommt man F^U durch Adjunktion der elementarsymmetrischen Funktionen in den Elementen von M an $k(x')$. Für praktische Anwendungen hat diese Methode aber den Nachteil, dass der Grad $[F : k(x')]$ sehr groß werden kann. Dadurch können die Rechnungen, die man in F durchführt, ziemlich aufwendig werden. Eine alternative Methode zum Berechnen der Fixkörper ist in Magma implementiert. Sie ist effizienter, verwendet aber Aussagen über Differentiale.

Vergleich der Laufzeiten

In diesem Abschnitt wird anhand einiger Beispiele die Dauer für das Berechnen aller Einbettungen und für das Berechnen der galoisschen Einbettungen verglichen. Die Berechnungen fanden unter denselben Bedingungen wie im Abschnitt 5 statt. Die Ergebnisse sind in der folgenden Tabelle aufgelistet. In jedem Kasten sind die definierenden Polynome f_1 und f_2 der Funktionenkörper F_1 beziehungsweise F_2 und der Konstantenkörper k angegeben. Weiterhin wird jeweils die Zeit t_1 und t_2 und die Anzahl der gefundenen Einbettungen $\#\mathrm{Hom}(F_1, F_2)$ und $\#\mathrm{Hom}_{galois}(F_1, F_2)$ mit dem allgemeinen beziehungsweise dem speziellen Algorithmus angegeben.

$f_1(x,y) = y^2 + x^5 + x^2 + 1$			$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^5 + x^2)y^2 + x^{10} + x^5 + 1$			
$t_1 = 109$	$t_2 = 2$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$\#\mathrm{Hom}(F_1, F_2)_{galois} = 4$
$f_1(x,y) = y^2 + x^9 + x^2 + 1$			$k = \mathbb{F}_5$
$f_2(x,y) = y^4 + (2x^9 + 4x^2 + 2x + 4)y^2 + x^{18} + 3x^{10} + x^2$			
$t_1 = 210$	$t_2 = 3$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$\#\mathrm{Hom}(F_1, F_2)_{galois} = 2$

$f_1(x,y) = y^2 + 4x^5 + 3x + 1$			$k = \mathbb{F}_5$
$f_2(x,y) = y^6 + (2x^5 + 4x + 3)y^4 + (4x^3 + 2x^2 + 1)y^3 + (3x^{10} + 2x^6 + 4x^5$			
$+2x^2 + 3x + 3)y^2 + (2x^8 + x^7 + 3x^5 + 4x^4 + 4x^2 + x + 2)y + 4x^{15} + 4x^{11}$			
$+3x^{10} + 3x^7 + x^6 + x^5 + x^4 + 4x^3 + 3x^2 + 4x$			
$t_1 = 284$	$t_2 = 1$	$\#\mathrm{Hom}(F_1, F_2) = 4$	$\#\mathrm{Hom}(F_1, F_2)_{galois} = 0$
$f_1(x,y) = y^2 + x^{11} + 1$			$k = \mathbb{F}_3$
$f_2(x,y) = y^4 + (2x^{11} + 2x^2 + 1)y^2 + x^{22} + x^{13} + x^4$			
$t_1 = 68$	$t_2 = 3$	$\#\mathrm{Hom}(F_1, F_2) = 2$	$\#\mathrm{Hom}(F_1, F_2)_{galois} = 2$
$f_1(x,y) = y^2 + x^5 + 1$			$k = \mathbb{F}_5$
$f_2(x,y) =$			
$y^4 + (2x^5 + 4x^3 + 2x^2 + 10)y^2 + x^{10} + 7x^8 + 9x^7 + 4x^6$			
$+9x^5 + x^4 + x^3 + 6x^2 + 9$			
$t_1 = 29$	$t_2 = 1$	$\#\mathrm{Hom}(F_1, F_2) = 10$	$\#\mathrm{Hom}(F_1, F_2)_{galois} = 10$
$f_1(x,y) = y^2 + xy + x^7 + 2$			$k = \mathbb{F}_5$
$f_2(x,y) = y^{10} + 3y^6 + (x^5 + 2x)y^5 + y^2 + (4x^5 + 3x)y + x^{35}$			
$+3x^{21} + 4x^{16} + 3x^{14} + 4x^{11} + x^9 + 2x^7 + 4x^6 + 3x^4 + 3x^2 + 3$			
$t_1 = --$	$t_2 = 457$	$\#\mathrm{Hom}(F_1, F_2) = --$	$\#\mathrm{Hom}(F_1, F_2)_{galois} = 2$
$f_1(x,y) = y^2 + x^6 + 1$			$k = \mathbb{F}_5$
$f_2(x,y) = y^{10} + 3y^6 + (2x + 2)y^5 + y^2 + (3x + 3)y + x^{30} + 3x^{18} + 4x^{12}$			
$+x^2 + 2x + 1$			
$t_1 = --$	$t_2 = 2553$	$\#\mathrm{Hom}(F_1, F_2) = --$	$\#\mathrm{Hom}(F_1, F_2)_{galois} = 8$

Bei diesen Beispielen ist der in diesem Kapitel vorgestellte Algorithmus zum Berechnen der galoisschen Einbettungen deutlich schneller als unser Algorithmus zum Berechnen aller Einbettungen. Dieses Ergebnis wird von vielen weiteren Beispielen bekräftigt und ist nicht verwunderlich, wenn man den Aufwand der beiden Algorithmen vergleicht. Wie im Kapitel 4 bewiesen wurde, ist der Aufwand für das Berechnen aller Einbettungen nicht mehr polynomiell. Die Berechnung der galoisschen Einbettungen hingegen basiert hauptsächlich auf dem Berechnen von Isomorphismen. Nach [Hes04] lassen sich Isomorphismen mit einem in dem Geschlecht polynomiellen Aufwand bestimmen. Da zudem die Automorphismengruppen in der Praxis oft relativ klein sind, liefert das eine Erklärung für die meist wesentlich niedrigere Laufzeit. Die letzten zwei Beispiele sollen demonstrieren, dass für Funktionenkörper mit hohem Geschlecht und für höhere Einbettungsgrade auch die Laufzeit des Algorithmus zum Berechnen der galoisschen Einbettungen stark wächst. In diesen Beispielen sind die gefundenen Einbettungen vom Grad fünf. Der allgemeine Einbettungsalgorithmus wurde nicht angewendet, da dieses zu lange dauern würde.

6.3 Ausblick

In diesem Abschnitt gehen wir abschließend kurz auf weitere Möglichkeiten ein, den Algorithmus zu beschleunigen oder zu verallgemeinern.

Beschleunigen

Eine einfache Möglichkeit, die Berechnung von Einbettungen zu beschleunigen, geht aus den Überlegungen zu galoisschen Einbettungen hervor. Da wir wissen, dass separable Körpererweiterungen vom Grad zwei immer galoissch sind, kann man alle Einbettungen vom Grad zwei mit dem Algorithmus für galoissche Einbettungen finden. Das geht in der Praxis oft deutlich schneller. Vom komplexitätstheoretischen Gesichtspunkt liefert dieser Trick aber keine Verbesserung. Der Aufwand wächst weiterhin exponentiell in dem maximalen Einbettungsgrad und das Problem der Gröbnerbasenberechnung bleibt bestehen, da sich für die Grade größer als zwei nichts in der Berechnung ändert.

Einen Ansatzpunkt um die Laufzeit zu verringern bietet die Menge M der Divisoren D, die daraufhin untersucht werden, ob es zu einer Stelle P eine Einbettung ϕ mit $\hat{\phi}(P) = D$ gibt. Diese Menge wächst mit steigendem Einbettungsgrad mindestens subexponentiell und hat starken Einfluß auf die Laufzeit. Wenn man in der Lage wäre ein einfach zu überprüfendes Kriterium zu formulieren, das die Kardinalität von M für eine spezielle Wahl der Stelle P reduziert, so könnte man damit die Laufzeit entscheidend verbessern.

Verallgemeinerungen

Der Einbettungsalgorithmus setzt voraus, dass der Konstantenkörper k der Funktionenkörper ein endlicher Körper ist. Es verbleibt die Frage, ob man den Algorithmus auch auf andere Konstantenkörper verallgemeinern kann. Die Voraussetzung der Endlichkeit des Konstantenkörpers wird an verschiedenen Stellen verwendet. Zum einen verwenden wir, dass es nur endlich viele Stellen von beschränktem Grad gibt und sich somit die Suche nach Einbettungen auf das Überprüfen von endlich vielen Divisoren reduzieren lässt und zum anderen verwenden wir, dass endliche Körper immer vollkommen sind. Viele der Aussagen, die für die Korrektheit des Algorithmus verwendet werden, wie zum Beispiel die Aussage über Konstantenkörpererweiterungen oder über die Endlichkeit der Anzahl der separablen Einbettungen, sind für nicht vollkommene Konstantenkörper falsch. Will man daher weiterhin voraussetzen, dass der Konstantenkörper vollkommen ist, so könnte man versuchen den Algorithmus auf Funktionenkörper über Körpern der Charakteristik null zu verallgemeinern. Diese Funktionenkörper können aber unendlich viele Stellen vom Grad eins besitzen, so dass man nicht mehr alle effektiven Divisoren beschränkten Grades überprüfen kann. Im Isomorphiefall kann man stattdessen mit der endlichen Menge der Weierstrass Stellen arbeiten. Offen ist, ob man Eigenschaften der Weierstrass Stellen oder anderer spezieller Stellen benutzen kann, um das Berechnen der Einbettungen auf das Untersuchen von endlich vielen Divisoren zu reduzieren.

Literaturverzeichnis

[AE04] Andrews, G. E. und K. Eriksson: *Integer Partitions.* Cambridge University Press, Cambridge, 2004.

[BCP97] Bosma, W., J. Cannon und C. Playoust: *The Magma algebra system I: The user language.* J. Symbolic Comp., 24, 3/4:235–265, 1997.

[FGLM93] Faugère, J. C., P. Gianni, D. Lazard und T. Mora: *Efficient computation of zero-dimensional Gröbner bases by change of ordering.* J. Symbolic Comp., 16(4):329–344, 1993.

[Har77] Hartshorne, R.: *Algebraic Geometry.* Springer-Verlag, Berlin-Heidelberg-New York, 1977.

[Hes99] Hess, F.: *Zur Divisorenklassengruppenberechnung in globalen Funktionenkörpern.* PhD Thesis, Technische Universität Berlin, 1999.

[Hes02] Hess, F.: *Computing Riemann-Roch spaces in algebraic function fields and related topics.* J. Symbolic Comp., 33(4):425–445, 2002.

[Hes04] Hess, F.: *An algorithm for computing isomorphisms of algebraic function fields.* In: Buell, D. (Herausgeber): *Proceedings of the Sixth Symposium on Algorithmic Number Theory, ANTS-VI*, LNCS 3076, Seiten 263–271, Burlington, Vermont USA, 2004. Springer-Verlag, Berlin-Heidelberg-New York.

[Kan04] Kant group: Kash. `http://www.math.tu-berlin.de/~kant`, 2004.

[Lor90] Lorenz, F.: *Einführung in die Algebra Teil 2.* B.I. Wissenschaftsverlag, Mannheim/Wien/Zürich, 1990.

[Lor92] Lorenz, F.: *Einführung in die Algebra Teil 1.* 2rd edition. B.I. Wissenschaftsverlag, Mannheim/Wien/Zürich, 1992.

[LV93] Lazard, D. und A. Valibouze: *Computing subfields: Reverse of the primitive element problem.* Computational Algebraic Geometry, 109:163–176, 1993.

[Sal06] Salvador, G. D. Villa: *Topics in the Theory of Algebraic Function Fields.* Birkhäuser Verlag, Basel, 2006.

[Sch96] Schörnig, M.: *Untersuchung konstruktiver Probleme in globalen Funktionenkörpern.* PhD Thesis, Technische Universität Berlin, 1996.

[Sti93] STICHTENOTH, H.: *Algebraic Function Fields and Codes.* Springer-Verlag, Berlin-Heidelberg-New York, 1993.

[Tam72] TAMME, G.: *Teilkörper algebraischer Funktionenkörper.* Arch. Math., 13:257–259, 1972.

[vzGG98] GATHEN, J. VON ZUR und J. GERHARD: *Modern Computer Algebra.* Cambridge University Press, Cambridge, 1998.