Untersuchungen konstruktiver Probleme in globalen Funktionenkörpern

vorgelegt von
Diplom-Mathematiker

Martin Schörnig

aus Düsseldorf

Vom Fachbereich 3 Mathematik
der Technischen Universität Berlin
zur Erlangung des akademischen Grades eines
Doktors der Naturwissenschaften
genehmigte Dissertation.

Berlin 1996
D83

Promotionsausschuß

Vorsitzender:	Professor Dr. R. D. Grigorieff
Berichter:	Professor Dr. M. E. Pohst
Berichter:	Professor Dr. F. Grunewald

Tag der wissenschaftlichen Aussprache: 12. Juni 1996

Inhaltsverzeichnis

Einleitung

Die Theorie globaler Funktionenkörper F, d.h. endlicher Erweiterungen von rationalen Funktionenkörpern einer Variablen mit endlichem Konstantenkörper K, hat sich historisch gesehen aus verschiedenen Teilgebieten der Mathematik entwickelt.

Zum ersten bildet sie einen Teil der Theorie algebraischer Funktionenkörper, welche Ende des 19. Jahrhundert (für $K = \mathbb{C}$) von R. Dedekind und H. Weber [DW] begründet wurde und das Buch von K. Hensel und G. Landsberg [HL] inspirierte. Gegenstand ihrer Untersuchungen waren algebraische Funktionen ρ einer komplexen Variablen x, welche polynomiellen Gleichungen der Form $f(x, \rho) = 0$ genügen. Im Verlauf des 20. Jahrhunderts wurde die Theorie der algebraischen Funktionen (-körper) schließlich für eine größere Klasse von Konstantenkörpern von E. Artin, H. Hasse, F. K. Schmidt, A. Weil, M. Deuring, M. Eichler und C. Chevalley weitergeführt.

Ein weiterer Zugang zur Theorie der Funktionenkörper ergibt sich aus der algebraischen Geometrie: Für ein irreduzibles Polynom $f \in K[x, y]$ betrachten wir die algebraische Kurve $C := \{(\alpha, \beta) \in K \times K \mid f(\alpha, \beta) = 0\}$ und können Eigenschaften von C an Hand des Körpers der rationalen Funktionen auf C studieren. Wurden „klassischerweise“ Kurven über algebraisch abgeschlossenem K untersucht, so führte spätestens die Konstruktion fehlerkorrigierender Codes durch V. D. Goppa mit Hilfe algebraischer Kurven über endlichem K zu einer intensiveren Untersuchung globaler Funktionenkörper.

Eine dritte Sichtweise globaler Funktionenkörper begründet sich aus der Theorie globaler Körper, welche auf E. Artin zurückgeht. Diese bewertungstheoretische Charakterisierung stellt die Korrespondenzen algebraischer Zahlkörper und globaler Funktionenkörper in den Vordergrund und bildet die Grundlage der vorliegenden Arbeit.

In den letzten Jahren sind Invarianten von Zahlkörpern $\mathcal{F}$, wie z.B. die Maximalordnung $o_{\mathcal{F}}$ und ihre Einheitengruppe $U_{\mathcal{F}}$, ausgiebig algorithmisch untersucht worden. Für die Effizienz der dabei verwendeten Verfahren ist es wesentlich, eine Ganzheitsbasis zu wählen, die bzgl. einer bestimmten Längenfunktion ($T_2 : \mathcal{F} \to \mathbb{R}^{\geq 0}$) besonders „gute“ Eigenschaften besitzt. Dazu betten wir $\mathcal{F}$ vermöge der Minkowskiabbildung („isometrisch“) in den $\mathbb{R}^n$ ein, identifizieren die Maximalordnung mit einem Gitter im $(\mathbb{R}^n, \| \cdot \|_2)$ und verwenden den Lenstra-Lenstra-Lovász-Algorithmus (LLL-Algorithmus, siehe [LLL]) zur Basisreduktion.

In der vorliegenden Arbeit betrachten wir für ein irreduzibles Polynom $f \in \mathbb{F}_q[x, y]$ mit $\deg_y(f) = n$, welches bzgl. y normiert und separabel ist, den globalen Funktionenkörper

$$F = \mathbb{F}_q(x, \rho) \text{ mit } f(x, \rho) = 0,$$

wobei $\mathbb{F}_q$ den endlichen Körper mit q Elementen bezeichnet und x transzendent über $\mathbb{F}_q$ ist.

Analog zum Zahlkörper $\mathcal{F}/\mathbb{Q}$ untersuchen wir die endliche, separable Erweiterung $F/\mathbb{F}_q(x)$. Dabei übernimmt $\mathbb{F}_q[x]$ in $\mathbb{F}_q(x)$ die Rolle von $\mathbb{Z}$ in $\mathbb{Q}$, und der ganze Abschluß o_F von $\mathbb{F}_q[x]$ in F ist das Analogon zu $o_{\mathcal{F}}$. Wiederum analog ist o_F ein Dedekindring und freier $\mathbb{F}_q[x]$-Modul vom Rang n, und auch im Funktionenkörperfall ist die Wahl einer „geeigneten“ Ganzheitsbasis entscheidend für die Effizienz algorithmischer Untersuchungen. Da der LLL-Algorithmus im Zahlkörperfall das Skalarprodukt des $\mathbb{R}^n$ extensiv nutzt, läßt sich dieser nicht ohne weiteres auf den Funktionenkörperfall übertragen.

In dieser Arbeit entwickeln wir aufbauend auf einem Analogon zur Längenfunktion T_2 einen Reduktionsbegriff für Ganzheitsbasen in globalen Funktionenkörpern. Für den Fall, daß die „unendliche“ Stelle P_∞ in F zahm verzweigt ist, geben wir einen effizienten, deterministischen Reduktionsalgorithmus an, der eine beliebige Ganzheitsbasis in eine reduzierte überführt. Schließlich verwenden wir reduzierte Ganzheitsbasen und einen auf dem Reduktionsalgorithmus basierenden Wurzeltest bei der Berechnung der Einheitengruppe $U_F := o_F^*$. Damit ist es erstmals möglich, Einheitengruppen in Funktionenkörpern vom Grad $n \geq 3$ zu berechnen.

Die Arbeit gliedert sich wie folgt:

Im ersten Kapitel fassen wir Grundlagen über algebraische und speziell globale Funktionenkörper zusammen. Nach allgemeinen Definitionen und bewertungstheoretischen Aussagen untersuchen wir die Struktur der ganzen Abschlüsse von $\mathbb{F}_q[x]$ bzw. dem zu P_∞ gehörenden Bewertungsring $\mathcal{O}_\infty$ in F.

In Kapitel II geben wir eine verallgemeinerte Einführung in die Minkowskische Geometrie der Zahlen. Hierauf aufbauend erweitern wir den Gitterbegriff, den Begriff der Längenfunktion und die Definition sukzessiver Minima. Bezeichnen $P_1, \ldots, P_s$ die paarweise verschiedenen Stellen, welche in F über P_∞ liegen, und

$v_i, e_i, 1 \leq i \leq s$, die zugehörigen (exponentiellen) Bewertungen bzw. Verzweigungsindizes, so definieren wir die Längenfunktion (mit $q^{-\infty} := 0$)

$$B : F \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto q^{-\min_{i=1}^{s} v_i(\alpha)/e_i}.$$

Diese wird bei algorithmischen Betrachtungen die Rolle der von Zahlkörpern her bekannten T_2-Länge übernehmen. Nachdem wir bewiesen haben, daß immer eine Ganzheitsbasis $\omega_1, \ldots, \omega_n \in o_F$ existiert, welche die (verallgemeinerten) sukzessiven Minima $M_i, 1 \leq i \leq n$, von o_F bzgl. B realisiert (d.h. $M_i = B(\omega_i), 1 \leq i \leq n$), gehen wir genauer auf die Struktur der sukzessiven Minima ein.

Im dritten Kapitel stellen wir einen effizienten Algorithmus zur Berechnung einer $\mathbb{F}_q$-Basis des Riemann-Rochschen Raums

$$\mathcal{L}(D, t) := \{\alpha \in o_F \mid v_i(\alpha) \geq -c_i - te_i \quad 1 \leq i \leq s\}$$

für einen Divisor $D = \sum_{i=1}^{s} c_i P_i, \quad c_i \in \mathbb{Z}, 1 \leq i \leq s$, und $t \in \mathbb{R}$ vor. Hierbei erhalten wir die $\mathbb{F}_q$-Basis von $\mathcal{L}(D, t)$ aus einer Ganzheitsbasis von o_F, welche einer speziellen Reduktionsbedingung („D-Reduziertheit“) genügt. Da der Algorithmus die Existenz aller Puiseuxentwicklungen an $P_1, \ldots, P_s$ der Nullstellen von f voraussetzt, beginnen wir mit Existenzuntersuchungen und erhalten als hinreichendes Kriterium die Zahmverzweigtheit von P_∞ in F. Ist P_∞ zahm verzweigt, so berechnen wir speziell eine 0-reduzierte Ganzheitsbasis $\omega_1, \ldots, \omega_n \in o_F$, d.h. eine D-reduzierte Ganzheitsbasis für $D = 0$. Wir zeigen, daß diese die sukzessiven Minima von o_F bzgl. B realisiert. Weiter können wir mit dieser Ganzheitsbasis die Gruppe der Torsionseinheiten bestimmen und Elemente beschränkter Norm konstruieren, was im nachfolgenden Kapitel zur Einheitenberechnung wichtig wird. Darüber hinaus geben wir ein Verfahren zur Berechnung von $\mathcal{L}(D, t)$ im wild verzweigten Fall an.

In Kapitel IV berechnen wir die Einheitengruppe U_F. Nachdem wir im vorangegangenen Kapitel bereits die Gruppe der Torsionseinheiten bestimmt haben, berechnen wir nun Grundeinheiten, in dem wir die von Zahlkörpern her bekannte Relationenmethode auf den Funktionenkörperfall übertragen. Wir erzeugen Relationen mittels normbeschränkter Elemente, die wir im zahm verzweigten Fall aus der Berechnung von $\mathcal{L}(0, t)$ gewinnen. Im wild verzweigten Fall konstruieren wir solche Elemente, in dem wir eine Parallelotopmethode mit Hilfe von Gittertheorie aus dem Zahlkörperfall übertragen. Schließlich benutzen wir die Algorithmen zur Berechnung von $\mathcal{L}(D, t)$ bei einem Verfahren für Wurzeltests in U_F, um von unabhängigen Einheiten zu Grundeinheiten zu gelangen.

Schließlich geben wir im fünften Kapitel Beispiele zur 0-Reduktion von Ganzheitsbasen und zur Berechnung von Grundeinheiten in Funktionenörpern vom Grad ≥ 3, in denen P_∞ zahm verzweigt ist.

Abschließend weisen wir auf das Symbol- und Literaturverzeichnis am Ende der Arbeit hin, wobei letzteres neben zitierter auch weiterführende Literatur enthält.

An dieser Stelle möchte ich Herrn Professor Dr. M. E. Pohst herzlich für die Anregung dieses Themas, seine Unterstützung während der Anfertigung der Arbeit und die sehr gute Zusammenarbeit danken.

Ferner danke ich Herrn Professor Dr. F. Grunewald für die Übernahme des Koreferats, allen Mitgliedern der KANT-Gruppe und besonders Claus Fieker und Klaus Wildanger für die Durchsicht einer vorläufigen Fassung dieser Arbeit. Darüber hinaus möchte ich der Studienstiftung des deutschen Volkes für die Förderung während der letzten Jahre danken.

Mein besonderer Dank gilt schließlich meinen Eltern, meiner Schwester und meinen Freunden, die mich immer unterstützt haben. Ihnen ist diese Arbeit gewidmet.

KAPITEL I

Grundlagen

In diesem Kapitel werden die für die Arbeit relevanten theoretischen Grundlagen über algebraische Funktionenkörper bereitgestellt und Notationen vereinbart. Für allgemeine Einführungen in die Theorie algebraischer Funktionenkörper (einer Variablen) bzw. globaler Körper verweisen wir auf [Ar2], [Ch], [Coh2], [D], [E], [Ha], [St] und [We].

1. Algebraische Funktionenkörper

Wir beginnen mit zentralen Definitionen und Aussagen für Funktionenkörper. Da wir an einigen Stellen der Arbeit nicht nur Funktionenkörper über endlichen Körpern betrachten, treffen wir die folgenden Definitionen direkt im allgemeineren Rahmen der algebraischen Funktionenkörper über vollkommenen Körpern. Hierbei folgen wir der Darstellung in [St] und gehen auf Analogien zu Zahlkörpern ein.

Definition I.1. *Sei K ein vollkommener Körper. Dann heißt ein Körper $F \supset K$ algebraischer Funktionenkörper (über K), falls ein über K transzendentes $x \in F$ mit $[F : K(x)] < \infty$ existiert.*

F heißt globaler Funktionenkörper, falls K ein endlicher Körper ist.

Wir nennen K den Konstantenkörper von F und bezeichnen mit

$$\widetilde{K} := \{\alpha \in F \mid \alpha \textit{ ist algebraisch über } K\}$$

den sog. exakten Konstantenkörper (von F).

Im folgenden verwenden wir den Begriff „Funktionenkörper“ immer für einen algebraischen Funktionenkörper.

Eine erste Aussage über die Struktur von Funktionenkörpern gibt der folgende

Satz I.2. *Seien x transzendent über K, $f \in K[x,y]$ ein irreduzibles Polynom mit $\deg_y(f) = n$, welches bzgl. y normiert und separabel ist, und $\rho \in \overline{K(x)}$ mit $f(x,\rho) = 0$. Dann gelten*

(1) *$F := K(x,\rho)$ ist ein Funktionenkörper mit $n = [F : K(x)]$, und jeder Funktionenkörper F kann auf diese Weise durch eine geeignete Wahl von $x \in F$ separabel über $K(x)$ erzeugt werden. Ein solches x heißt separierendes Element von F/K.*
(2) *Es gilt $K \subset \widetilde{K} \subset F$, d.h., F kann immer als Funktionenkörper über $\widetilde{K}$ betrachtet werden. Für $l := [\widetilde{K} : K]$ folgt insbesondere $l \mid n$.*
(3) *Innerhalb der Körpererweiterung F/K ist der rationale Zwischenkörper $K(x)$ keine Invariante, da er von der Wahl des transzendenten Elements $x \in F$ abhängt.*

Bemerkung I.3. *Nach* [Ha, S. 319f] *gelten für einen vollkommenen Körper K mit positiver Charakteristik $p \in \mathbb{P}$ und ein über K transzendentes Element $x \in F$:*

Genau dann ist x separierendes Element von F/K, wenn x keine p-te Potenz in F ist. Weiter sind für ein irreduzibles Polynom $f \in K[x,y]$, welches bzgl. y normiert ist, äquivalent:

$$f \text{ ist separabel in } y \Longleftrightarrow f \in K[x,y] \setminus K[x,y^p].$$

Die folgenden Definitionen und Aussagen geben eine Einführung in die bewertungstheoretische Charakterisierung von Funktionenkörpern (siehe hierzu [Ch], [St]).

Definition und Satz I.4. *Sei $K \subsetneq \mathcal{O} \subsetneq F$ ein Ring mit $\alpha \in \mathcal{O}$ oder $\alpha^{-1} \in \mathcal{O}$ für alle $\alpha \in F^\times$. Dann heißt $\mathcal{O}$ (diskreter) Bewertungsring (von F), und es gelten*

(1) *$\mathcal{O}$ ist lokaler Euklidischer Ring mit maximalem Ideal $P := \mathcal{O} \setminus \mathcal{O}^*$.*
(2) *Ein Element $\pi \in P$ mit $P = \pi\mathcal{O}$ heißt Primelement (für P), und für jedes $\alpha \in F^\times$ existieren eindeutig $k \in \mathbb{Z}, u \in \mathcal{O}^*$ mit $\alpha = \pi^k u$. Hierbei hängt k nur von α ab.*

Wir setzen

$$\mathbb{P}(F) := \{Q \mid Q \text{ ist maximales Ideal eines Bewertungsrings von } F\}$$

und nennen $Q \in \mathbb{P}(F)$ eine Stelle von F.

Damit erhalten wir die folgende Bijektion zwischen Stellen und Bewertungsringen:

$$\begin{aligned} \mathbb{P}(F) \to \{\mathcal{O} \mid \mathcal{O} \text{ ist Bewertungsring von } F\} &: P \mapsto \mathcal{O}_P := \{\alpha \in F \mid \alpha^{-1} \notin P\}, \\ \{\mathcal{O} \mid \mathcal{O} \text{ ist Bewertungsring von } F\} \to \mathbb{P}(F) &: \mathcal{O} \mapsto P := \mathcal{O} \setminus \mathcal{O}^*. \end{aligned}$$

DEFINITION UND SATZ I.5. *Eine (diskrete, nichttriviale) Bewertung von F ist eine surjektive Abbildung $v : F \longrightarrow \mathbb{Z} \cup \{\infty\}$, so daß für alle $\alpha, \beta \in F$ gelten*

(1) $v(\alpha) = \infty \Leftrightarrow \alpha = 0$,
(2) $v(\alpha\beta) = v(\alpha) + v(\beta)$,
(3) $v(\alpha \pm \beta) \geq \min\{v(\alpha), v(\beta)\}$.

Ein Betrag von F ist eine Abbildung $|\cdot| : F \longrightarrow \mathbb{R}^{\geq 0}$ mit $|\cdot| = c^{-v(\cdot)}$ für fixiertes $c > 1$ und eine Bewertung v von F, wobei $c^{-\infty} := 0$. Im Fall globaler Funktionenkörper sei $c := \#K$.

Zu einer Stelle $P \in \mathbb{P}(F)$ mit Primelement $\pi \in P$ definieren wir eine Bewertung v_P und für fixiertes $c > 1$ einen Betrag $|\cdot|_P := c^{-v_P(\cdot)}$, mittels

$$v_P : F \longrightarrow \mathbb{Z} \cup \{\infty\} : \alpha \longmapsto \begin{cases} \infty & \alpha = 0, \\ k, \text{ wenn } \alpha = \pi^k u \text{ mit } u \in O_P^* & \text{sonst.} \end{cases}$$

Wir erhalten die folgende Bijektion zwischen Stellen und Bewertungen:

$$\begin{aligned} \mathbb{P}(F) \to \{v \mid v \text{ ist Bewertung von } F\} &\ :\ P \mapsto v_P, \\ \{v \mid v \text{ ist Bewertung von } F\} \to \mathbb{P}(F) &\ :\ v \mapsto \{\alpha \in F \mid v(\alpha) > 0\}. \end{aligned}$$

DEFINITION UND SATZ I.6. *Die Bewertungsringe des rationalen Funktionenkörpers $K(x)$ sind gegeben durch*

$$\begin{aligned} \mathcal{O}_\pi &:= \{g/h \mid g, h \in K[x], h \neq 0, \pi \nmid h\} \text{ für ein Primpolynom } \pi \in K[x] \text{ und} \\ \mathcal{O}_\infty &:= \{g/h \mid g, h \in K[x], h \neq 0, \deg(g) \leq \deg(h)\}. \end{aligned}$$

Die zu $\mathcal{O}_\infty$ korrespondierende Stelle bzw. Bewertung bezeichnen wir mit P_∞ bzw. v_∞. Dann gelten

$$\begin{aligned} P_\infty &= x^{-1}\mathcal{O}_\infty = \{g/h \mid g, h \in K[x], h \neq 0, \deg(g) < \deg(h)\} \text{ und} \\ v_\infty &: K(x) \longrightarrow \mathbb{Z} \cup \{\infty\} : \alpha = g/h \longmapsto \begin{cases} \infty & \alpha = 0, \\ \deg(h) - \deg(g) & \text{sonst.} \end{cases} \end{aligned}$$

Ferner bezeichnen wir den durch v_∞ definierten Betrag mit $|\cdot|_\infty$.

Wir formulieren nun Aussagen der Verzweigungstheorie.

DEFINITION UND SATZ I.7. *Sei F' ein Funktionenkörper über einem Konstantenkörper K', so daß $F' \supset F$ eine algebraische Erweiterung ist und $K' \supset K$. Dann heißt F'/K' algebraische Erweiterung von F/K. Ist $K' \supset K$ eine algebraische Erweiterung, so heißt $K'F/K'$ Konstantenkörpererweiterung (von F/K).*

Seien ferner $P \in \mathbb{P}(F)$ und $Q \in \mathbb{P}(F')$ mit $P \subset Q$. Dann „liegt Q über P“ (Schreibweise: $Q|P$), und es existiert $e(Q|P) \in \mathbb{N}$ mit $v_Q|_F = e(Q|P)v_P$. Die Zahl

$e(Q|P)$ heißt Verzweigungsindex von Q über P, und ferner gelten $P = Q \cap F$ sowie $\mathcal{O}_P = \mathcal{O}_Q \cap F$.

Die Quotienten $\mathcal{O}_Q/Q$ und $\mathcal{O}_P/P$ sind isomorph zu endlichen Erweiterungen von K' bzw. K. Wir setzen $\deg(Q) := [\mathcal{O}_Q/Q : K'] \in \mathbb{N}$, definieren den Trägheitsgrad $f(Q|P) := [\mathcal{O}_Q/Q : \mathcal{O}_P/P] \in \mathbb{N} \cup \{\infty\}$, und es gilt $f(Q|P) < \infty \Leftrightarrow [F' : F] < \infty$.

Weiter existieren $j \in \mathbb{N}, j \leq [F' : F]$ und $Q_1, \ldots, Q_j \in \mathbb{P}(F')$ mit $\{Q \in \mathbb{P}(F') \mid Q|P\} = \{Q_1, \ldots, Q_j\}$ sowie

$$\sum_{i=1}^{j} e(Q_i|P) f(Q_i|P) = [F' : F].$$

Schließlich heißt P zahm verzweigt (in F), falls $p \nmid e(Q_i|P), 1 \leq i \leq j$, gilt; ansonsten heißt P wild verzweigt.

Wir beschäftigen uns nun mit der freien, abelschen Gruppe

$$\operatorname{Div}(F) := \left\{ \sum_{P \in \mathbb{P}(F)} c_P P \mid c_P \in \mathbb{Z}, c_P = 0 \text{ für fast alle } P \in \mathbb{P}(F) \right\},$$

der Divisorengruppe von F. Dazu beginnen wir mit der folgenden

Definition I.8. *Ein Element $D = \sum_{P \in \mathbb{P}(F)} c_P P \in \operatorname{Div}(F)$ heißt Divisor und*

$$\deg(D) := \sum_{P \in \mathbb{P}(F)} c_P \deg(P) \in \mathbb{Z}$$

der Grad von D. Zu $\alpha \in F^\times$ definieren wir den sog. Hauptdivisor

$$(\alpha) := \sum_{P \in \mathbb{P}(F)} v_P(\alpha) P \in \operatorname{Div}(F).$$

Setzen wir ferner

$$\mathbb{P}_\infty(F) := \{Q \in \mathbb{P}(F) \mid Q|P_\infty\} \textit{ sowie } \mathbb{P}_0(F) := \mathbb{P}(F) \setminus \mathbb{P}_\infty(F),$$

so gilt offensichtlich

$$\begin{aligned}
\operatorname{Div}(F) &= \operatorname{Div}_0(F) \oplus \operatorname{Div}_\infty(F) \textit{ mit den Untergruppen} \\
\operatorname{Div}_0(F) &:= \left\{ \sum_{P \in \mathbb{P}_0(F)} c_P P \mid c_P \in \mathbb{Z}, c_P = 0 \textit{ für fast alle } P \in \mathbb{P}_0(F) \right\} \textit{ und} \\
\operatorname{Div}_\infty(F) &:= \left\{ \sum_{P \in \mathbb{P}_\infty(F)} c_P P \mid c_P \in \mathbb{Z} \right\}.
\end{aligned}$$

Bemerkung I.9. *Das Analogon zum Zahlkörperfall ist wie folgt: In der Maximalordnung $\mathfrak{o}_{\mathcal{F}}$ eines algebraischen Zahlkörpers $\mathcal{F}$ bilden die gebrochenen Ideale eine multiplikative Gruppe $\mathcal{I}_{\mathcal{F}}$, und jedes gebrochene Ideal $\mathcal{I}$ besitzt eine (bis auf Reihenfolge) eindeutige Darstellung als Potenzprodukt von Primidealen mit ganzzahligen Exponenten.*

Im Funktionenkörperfall benutzen wir die additive Schreibweise. Dann entspricht $\mathcal{I}_{\mathcal{F}}$ der Gruppe $\mathrm{Div}_0(F)$, $\mathcal{I}$ einem Divisor $D = \sum_{P\in\mathbb{P}_0(F)} c_P P \in \mathrm{Div}_0(F)$, wobei die Rolle der Primideale von Stellen $P \in \mathbb{P}_0(F)$ übernommen wird und die c_P den Exponenten entsprechen.

Wie schon bereits in Satz I.2.(3) erwähnt, ist der Zwischenkörper $\mathbb{F}_q(x)$ keine Invariante der Erweiterung $F/\mathbb{F}_q$, da er von der Wahl des transzendenten Elements $x \in F$ abhängt. Damit sind auch die Analoga der aus Zahlkörpern bekannten Invarianten, wie Signatur, Maximalordnung und Einheitengruppe, bei Funktionenkörpern abhängig von x.

Aus diesem Grund fixieren wir für den Rest der Arbeit einen globalen Funktionenkörper F. Dazu sei $\mathbb{F}_q$ der endliche Körper mit q Elementen und Charakteristik $p \in \mathbb{P}$ und F eine endliche, separable Körpererweiterung von $\mathbb{F}_q(x)$ wie in Satz I.2.(1), d.h., wir fixieren ein separierendes Element $x \in F$ von $F/\mathbb{F}_q$ und

$$F := \mathbb{F}_q(x,\rho) \text{ mit } f(x,\rho) = 0 \tag{1}$$

für ein irreduzibles Polynom $f \in \mathbb{F}_q[x,y]$ mit $\deg_y(f) = n$, welches bzgl. y normiert und separabel ist. Die n verschiedenen Nullstellen von f in $\overline{\mathbb{F}_q(x)}$ bezeichnen wir mit $\rho := \rho_1, \rho_2, \ldots, \rho_n$.

Von nun an betrachten wir $F/\mathbb{F}_q(x)$. Analog $\mathbb{Z}$ in $\mathbb{Q}$ übernimmt jetzt $\mathbb{F}_q[x]$ die Rolle der ganzen Zahlen in $\mathbb{F}_q(x)$. Mit dieser Festlegung können wir z.B. nun auch von *der* Maximalordnung, d.h. dem ganzen Abschluß von $\mathbb{F}_q[x]$ in F, sprechen. Im folgenden werden wir auf die Abhängigkeit von x nicht mehr gesondert hinweisen.

Wir beachten zunächst die fundamentale Charakterisierung durch die Produktformel für globale Körper (vgl. [AW]).

Satz I.10. *Für alle $\alpha \in F^\times$ gilt*

$$\prod_{P\in\mathbb{P}(F)} |\alpha|_P^{f(P|P\cap\mathbb{F}_q(x))} = 1 \text{ bzw. } \sum_{P\in\mathbb{P}(F)} f(P|P\cap\mathbb{F}_q(x))v_P(\alpha) = 0.$$

In Analogie zu Zahlkörpern definieren wir die Signatur von $F/\mathbb{F}_q(x)$.

DEFINITION I.11. *Es existiert* $s \in \{1, \dots, n\}$ *mit* $\{P_1, \dots, P_s\} := \mathbb{P}_\infty(F)$, *und wir setzen*

$$\begin{aligned} e_i &:= e(P_i|P_\infty), \quad f_i := \deg(P_i), \quad n_i := e_i f_i, \\ v_i &:= v_{P_i} \text{ und } |\cdot|_i := q^{-v_i(\cdot)}, \quad 1 \le i \le s. \end{aligned}$$

Indem wir $P_1, \dots, P_s$ *ggf. umnumerieren, gelte für alle* $1 \le i < j \le s$*:*

$$e_i \le e_j \text{ und falls } e_i = e_j : f_i \le f_j.$$

Wir bezeichnen das eindeutige $2s$*-Tupel* $(e_1, f_1; \dots; e_s, f_s) \in \mathbb{N}^{2s}$ *als Signatur von* $F/\mathbb{F}_q(x)$ *und setzen* $e := \mathrm{kgV}(e_1, \dots, e_s) \in \mathbb{N}$.

BEMERKUNG I.12. *Auf die Berechnung der Signatur werden wir am Ende des nächsten Abschnitts im Rahmen der Zerlegung von Hauptdivisoren eingehen.*

Um die Vervollständigung von F an einer Stelle P_i betrachten zu können und im Hinblick auf Anwendungen in der Gittertheorie, treffen wir im allgemeineren Rahmen die

DEFINITION I.13. *Für eine algebraische Körpererweiterung* $E/\mathbb{F}_q$ *und* $k \in \mathbb{N}$ *bezeichne*

$$E\langle x^{-1/k}\rangle := \left\{ \sum_{i=m}^{\infty} a_i x^{-i/k} \mid m \in \mathbb{Z}, a_i \in E \right\}$$

den Körper der Puiseuxreihen in $x^{-1/k}$ *mit Koeffizienten aus* E *und*

$$V_k : E\langle x^{-1/k}\rangle \longrightarrow \mathbb{Z} \cup \{\infty\} : \alpha = \sum_{i=m}^{\infty} a_i x^{-i/k} \longmapsto \begin{cases} \infty & \alpha = 0, \\ \min\{i \in \mathbb{Z} \mid a_i \ne 0\} & \textit{sonst}, \end{cases}$$

eine surjektive Bewertung auf $E\langle x^{-1/k}\rangle$.

Wir beachten, daß $\mathbb{F}_q\langle x^{-1}\rangle$ die Vervollständigung von $\mathbb{F}_q(x)$ an P_∞ ist, und erhalten

DEFINITION UND SATZ I.14. *Bezeichne* $\widehat{F}_i$ *die Vervollständigung von* F *an* P_i, $1 \le i \le s$. *Dann gilt (vgl.* [Coh2, Ch. 2, Proposition 3.1]*)*

$$\mathbb{F}_q\langle x^{-1}\rangle \otimes_{\mathbb{F}_q(x)} F \cong \prod_{i=1}^{s} \widehat{F}_i \text{ und } n_i = [\widehat{F}_i : \mathbb{F}_q\langle x^{-1}\rangle].$$

Wir fassen weitere Analogien zu Zahlkörpern zusammen.

BEMERKUNG I.15. *Die Analogien zum Zahlkörperfall sind wie folgt: Sei $\mathcal{F} = \mathbb{Q}(\tau)$ mit $g(\tau) = 0$, wo $\tau \in \overline{\mathbb{Q}}$ und $g \in \mathbb{Z}[t]$ ein normiertes, irreduzibles Polynom vom Grad n ist. Die Nullstellen $\tau_1, \dots, \tau_n$ von g seien angeordnet gemäß $\tau_i \in \mathbb{R}$, $1 \leq i \leq r_1$, $\overline{\tau}_i = \tau_{i+r_2} \in \mathbb{C} \setminus \mathbb{R}$, $r_1 + 1 \leq i \leq r_1 + r_2$ für geeignete $r_1, r_2 \in \mathbb{N}_0$. Bezeichnet $\cdot^{(i)}$ die Abbildung auf die i-te Konjugierte, so erhalten wir die folgenden Entsprechungen (vgl.* [We, Proposition 5-1-2.], [Coh2, S. 57]*):*

$$\begin{array}{lll} \mathbb{F}_q[x] \simeq \mathbb{Z}, & \mathbb{F}_q(x) \simeq \mathbb{Q}, & \mathbb{F}_q\langle x^{-1}\rangle \simeq \mathbb{R}, \\ s \simeq r_1 + r_2, & (e_1, f_1; \dots ; e_s, f_s) \simeq (r_1, r_2), & f_i \simeq 1, \quad 1 \leq i \leq r_1 + r_2, \end{array}$$

$$\begin{array}{llll} e_i & \simeq \begin{cases} 1 & 1 \leq i \leq r_1, \\ 2 & r_1 + 1 \leq i \leq r_1 + r_2, \end{cases} & n_i & \simeq \begin{cases} 1 & 1 \leq i \leq r_1, \\ 2 & r_1 + 1 \leq i \leq r_1 + r_2, \end{cases} \\ |\cdot|_i & \simeq \begin{cases} |\cdot^{(i)}| & 1 \leq i \leq r_1, \\ |\cdot^{(i)}|^2 & r_1 + 1 \leq i \leq r_1 + r_2, \end{cases} & \widehat{F}_i & \simeq \begin{cases} \mathbb{R} & 1 \leq i \leq r_1, \\ \mathbb{C} & r_1 + 1 \leq i \leq r_1 + r_2. \end{cases} \end{array}$$

Nachdem wir Grundlagen über (globale) Funktionenkörper zusammengestellt haben, betrachten wir nun ganze Abschlüsse in F.

2. Ganze Abschlüsse von $\mathbb{F}_q[x]$ und $\mathcal{O}_\infty$ in F

In diesem Abschnitt betrachten wir die ganzen Abschlüsse von $\mathbb{F}_q[x]$ bzw. $\mathcal{O}_\infty$ in F. Wir werden sehen, daß ihre Berechnung und die Zerlegung von Hauptdivisoren analog zum Zahlkörperfall erfolgen kann.

DEFINITION UND SATZ I.16. *Für einen unitären Teilring R von F definieren wir den ganzen Abschluß von R in F mittels*

$$\mathrm{Cl}(R, F) := \{\alpha \in F \mid \text{ es existiert ein normiertes } g \in R[z] \text{ mit } g(\alpha) = 0\}.$$

Setzen wir weiter

$$o_F := \mathrm{Cl}(\mathbb{F}_q[x], F) \text{ und } o_{F,\infty} := \mathrm{Cl}(\mathcal{O}_\infty, F),$$

so gelten:

(1) *o_F ist Dedekindring mit*

$$o_F = \bigcap_{P \in \mathbb{P}_0(F)} \mathcal{O}_P = \{\alpha \in F \mid v_P(\alpha) \geq 0 \text{ für alle } P \in \mathbb{P}_0(F)\}$$

und besitzt eine Ganzheitsbasis, d.h., es existieren Elemente $\omega_1, \dots, \omega_n \in o_F$ mit $o_F = \bigoplus_{i=1}^n \mathbb{F}_q[x]\omega_i$.

(2) *$o_{F,\infty}$ ist Hauptidealring mit*

$$o_{F,\infty} = \bigcap_{i=1}^{s} \mathcal{O}_{P_i} = \{\alpha \in F \mid v_i(\alpha) \geq 0, 1 \leq i \leq s\}$$

und besitzt eine Ganzheitsbasis, d.h., es existieren Elemente $\omega_1, \dots, \omega_n \in o_{F,\infty}$ mit $o_{F,\infty} = \bigoplus_{i=1}^{n} \mathcal{O}_\infty \omega_i$.

Bemerkung I.17. *1) Analog zum Zahlkörperfall ist o_F ein unitärer, freier Modul von vollem Rang.*

2) Nach Satz I.2.*(2) können wir F als Körpererweiterung von $\widetilde{\mathbb{F}}_q(x)$ auffassen. Dann gilt $o_F = \mathrm{Cl}(\widetilde{\mathbb{F}}_q[x], F)$, und o_F besitzt eine Ganzheitsbasis bzgl. $\widetilde{\mathbb{F}}_q[x]$, d.h., es existieren Elemente $\omega_1, \dots, \omega_{n/l} \in o_F$ mit $o_F = \bigoplus_{i=1}^{n/l} \widetilde{\mathbb{F}}_q[x]\omega_i$.*

3) Die beiden obigen Bemerkungen gelten analog für $o_{F,\infty}$.

Zur Berechnung von Ganzheitsbasen beachten wir die folgenden Aussagen (siehe [St, III.2, III.3.]):

Satz I.18. *Sei $P \in \mathbb{P}(\mathbb{F}_q(x))$. Dann besitzt $\mathrm{Cl}(\mathcal{O}_P, F)$ eine Ganzheitsbasis, d.h., es existieren $\omega_1, \dots, \omega_n \in \mathrm{Cl}(\mathcal{O}_P, F)$ mit*

$$\mathrm{Cl}(\mathcal{O}_P, F) = \bigcap_{Q|P} \mathcal{O}_Q = \bigoplus_{i=1}^{n} \mathcal{O}_P \omega_i.$$

Ist ferner $b_1, \dots, b_n \in F$ eine $\mathbb{F}_q(x)$-Basis von F, so gilt für alle, bis auf endlich viele $P \in \mathbb{P}(\mathbb{F}_q(x))$

$$\mathrm{Cl}(\mathcal{O}_P, F) = \bigoplus_{i=1}^{n} \mathcal{O}_P b_i.$$

Seien $\emptyset \neq S \subsetneq \mathbb{P}(\mathbb{F}_q(x))$ und

$$R_S := \{\alpha \in \mathbb{F}_q(x) \mid v_P(\alpha) \geq 0 \text{ für alle } P \in S\}.$$

Dann ist $\mathbb{F}_q(x)$ der Quotientenkörper von R_S, $\mathrm{Cl}(R_S, \mathbb{F}_q(x)) = R_S$, und es gilt

$$\mathrm{Cl}(R_S, F) = \bigcap_{P \in S} \mathrm{Cl}(\mathcal{O}_P, F) = \bigcap_{P \in S} \bigcap_{Q|P} \mathcal{O}_Q.$$

Für $S = \mathbb{P}_0(\mathbb{F}_q(x))$ bzw. $S = \{P_\infty\}$ erhalten wir Analogien zum Zahlkörperfall.

Definition und Satz I.19. *Für $P \in \mathbb{P}_0(\mathbb{F}_q(x))$ mit Primelement $\pi \in \mathbb{F}_q[x]$ gilt*

$$\pi^2 \nmid d(f) := \prod_{i \neq j} (\rho_i - \rho_j) \in \mathbb{F}_q[x] \Longrightarrow \mathrm{Cl}(\mathcal{O}_P, F) = \mathbb{F}_q[x, \rho].$$

Sei $f_\infty \in \mathcal{O}_\infty[y]$ irreduzibel, bzgl. y normiert und separabel mit Nullstellen $\rho_\infty := \rho_{1,\infty}, \rho_{2,\infty}, \ldots, \rho_{n,\infty} \in \overline{\mathbb{F}_q(x)}$ und gelte $F = \mathbb{F}_q(x, \rho_\infty)$. Dann folgt

$$x^{-2} \nmid d(f_\infty) := \prod_{i \neq j} (\rho_{i,\infty} - \rho_{j,\infty}) \in \mathcal{O}_\infty \Longrightarrow \mathrm{Cl}(\mathcal{O}_\infty, F) = \mathcal{O}_\infty[\rho_\infty].$$

BEMERKUNG I.20. *1) Aufgrund der Struktur des Rings $\mathcal{O}_\infty$ sind äquivalent*

$$x^{-2} \nmid d(f_\infty) \Longleftrightarrow v_\infty(d(f_\infty)) \in \{0, 1\}.$$

2) Zur Berechnung von f_∞ aus Definition und Satz I.19 *beachten wir $\mathbb{F}_q(x, x^k \rho) = F$ für alle $k \in \mathbb{Z}$. Ist nun*

$$f(x,y) = y^n + \sum_{i=0}^{n-1} a_i(x) y^i \text{ mit } a_i \in \mathbb{F}_q[x], 0 \leq i \leq n-1,$$

so wählen wir $k \in \mathbb{Z}$ maximal mit $v_\infty(a_i(x) x^{k(n-i)}) \geq 0$, also

$$k := \min\{\lfloor \deg(a_i)/(i-n) \rfloor \mid i \in \{0, \ldots, n-1\} \text{ und } a_i \neq 0\}.$$

Damit gilt für $f_\infty(x,y) := y^n + \sum_{i=0}^{n-1} a_i(x) x^{k(n-i)} y^i \in \mathcal{O}_\infty[y]$ und für $\rho_\infty := x^k \rho$

$$f_\infty(x, \rho_\infty) = (x^k \rho)^n + \sum_{i=0}^{n-1} a_i(x) x^{k(n-i)} (x^k \rho)^i = x^{kn} f(x, \rho) = 0.$$

Ferner bleiben Separabilität und Irreduzibilität bei Transformationen $\rho \mapsto \alpha\rho + \beta$ für $\alpha \in \mathbb{F}_q(x)^\times$ und $\beta \in \mathbb{F}_q(x)$ unverändert.

Zur Berechnung der ganzen Abschlüsse können wir wie im Zahlkörperfall vorgehen (siehe z.B. [P, Ch. V], [PZ, Ch. 4], [Coh1, 4.4] und [Fo]). Dabei beachten wir, daß $\mathbb{F}_q[x]$ und $\mathcal{O}_\infty$ Euklidische Ringe sind, womit uns die Hermite-Normalform für Matrizen zur Verfügung steht.

Um eine Ganzheitsbasis für o_F zu bestimmen, berechnen wir $d(f)$ und eine Liste von Primpolynomen $\{\pi_1, \ldots, \pi_j\}$, die $d(f)$ quadratisch teilen. Für diese π_i bestimmen wir jeweils Ganzheitsbasen von $\mathrm{Cl}(\mathcal{O}_{\pi_i}, F), 1 \leq i \leq j$, und setzen diese schließlich mittels Chinesischem Restsatz (Hermite-Normalform) zusammen.

Bei der Berechnung von $o_{F,\infty}$ gehen wir analog vor, wobei wir zunächst f_∞ berechnen. Weiter beachten wir, daß modulo Einheiten nur x^{-1} Primelement in $\mathcal{O}_\infty$ ist.

BEMERKUNG I.21. *Für die Berechnung eines ganzen Abschlusses mittels eines Algorithmus analog der Round-Two Methode für Zahlkörper (siehe* [P, Ch. V.2]*) weisen wir auf einen Unterschied hin. Bei der Berechnung der π_i-Radikale ist $\kappa \in \mathbb{N}$ minimal mit $p^\kappa \geq n$ zu wählen, d.h., κ ist von der Charakteristik des Grundkörpers abhängig.*

Wir kommen nun zur Zerlegung von Hauptdivisoren, d.h., zu gegebenem $\alpha \in \mathbb{F}^\times$ bestimmen wir

$$(\alpha) = \sum_{P \in \mathbb{P}(F)} v_P(\alpha) P.$$

Die Berechnung spalten wir auf in die Bestimmung von $D_0 \in \mathrm{Div}_0(F)$ und $D_\infty \in \mathrm{Div}_\infty(F)$ mit $(\alpha) = D_0 + D_\infty$.

Um D_0 zu berechnen, beginnen wir mit der Faktorisierung der Norm von α in das Produkt von Potenzen paarweise verschiedener Primpolynome

$$\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha) = \prod_{i=1}^{j} \pi_j^{\kappa_j} \text{ mit } \pi_i \in \mathbb{F}_q[x], \kappa_j \in \mathbb{Z}^\times, 1 \leq i \leq j,$$

und setzen $S := \{Q | \pi_i \mathcal{O}_{\pi_i} \mid 1 \leq i \leq j\} \subset \mathbb{P}_0(F)$.

Dann gilt $v_P(\alpha) = 0$ für alle $P \in \mathbb{P}_0(F) \setminus S$. Somit müssen wir in einem ersten Schritt S bestimmen und anschließend für jedes $Q \in S$ die Bewertung $v_Q(\alpha)$ berechnen.

Den ersten Schritt führen wir zurück auf die folgende Aufgabe: Zu einem gegebenen Primpolyom $\pi \in \mathbb{F}_q[x]$ bestimmen wir alle paarweise verschiedenen Stellen $Q_1, \ldots, Q_k \in \mathbb{P}_0(F)$ mit $Q | P := \pi \mathcal{O}_\pi$, d.h., wir berechnen die Zerlegung

$$\sum_{i=1}^{k} v_{Q_i}(\pi) Q_i = \sum_{i=1}^{k} e(Q_i | P) Q_i \in \mathrm{Div}_0(F).$$

Auch hier gilt die Theorie algebraischer Zahlkörper analog (siehe [St, III.3.7.] und [PZ, Ch. 6, (2.27)]):

Satz I.22. *Seien $R := \mathcal{O}_\pi / \pi \mathcal{O}_\pi$, $\overline{f}$ das Bild von f in $R[y]$ und*

$$\overline{f} = \prod_{i=1}^{r} \overline{g}_i^{\nu_i}, \quad \overline{g}_i \in R[y], \nu_i \in \mathbb{N}, 1 \leq i \leq r,$$

eine Faktorisierung in paarweise verschiedene, irreduzible Polynome. Sind $g_i \in \mathbb{F}_q[x,y]$ Urbilder von $\overline{g}_i, 1 \leq i \leq r$, und gilt $\mathrm{Cl}(\mathcal{O}_\pi, F) = \mathcal{O}_\pi[\rho]$, so folgen $r = k$ sowie

$$Q_i := \pi o_F + g_i(\rho) o_F, \quad e(Q_i|P) = \nu_i, \quad f(Q_i|P) = \deg(f_i), \quad 1 \leq i \leq k.$$

Bemerkung I.23. *Ist $\mathcal{O}_\pi[\rho] \subsetneq \mathrm{Cl}(\mathcal{O}_\pi, F)$, so können wir das aus dem Zahlkörperfall bekannte Verfahren zur Faktorisierung von Indexteilern (*[BL], *vgl.* [Coh1, 6.2]*) geeignet modifizieren, in dem wir die separable $\mathbb{F}_q$-Algebra beim Splitten als $\mathbb{F}_p$-Algebra auffassen (vgl.* [Coh1, 6.2.4.]*).*

Nachdem wir nun $Q_1, \dots, Q_k$ bestimmt haben, können wir z.B. mit dem in [Coh1, 4.8.3.] beschriebenen Verfahren die Bewertungen $v_{Q_i}(\alpha)$ berechnen. Damit kennen wir D_0.

Bei der Berechnung von D_∞ gehen wir analog vor, wobei wir zur Bestimmung von $P_1, \dots, P_s | P_\infty$ das Polynom f_∞ mit Nullstelle ρ_∞ und $\pi := x^{-1}$ verwenden (vgl. Bemerkung I.20.(2)).

BEMERKUNG I.24. *1) Mit der Bestimmung von D_∞ für (x^{-1}) berechnen wir die Signatur.*

2) Für die Bewertungsberechnung $v_i(\alpha), 1 \leq i \leq s, \alpha \in F^\times$, gibt es eine elegantere Möglichkeit als das in [Coh1, 4.8.3.] *beschriebene Verfahren, falls P_∞ zahm verzweigt ist, d.h. $p \nmid e$.*

In Kapitel III.1 werden wir sehen, daß in diesem Fall die Nullstellen $\rho_1, \dots, \rho_n$ über P_∞ in Puiseuxreihen entwickelbar sind. Damit sind alle $\alpha \in F$ an $P_1, \dots, P_s$ in Puiseuxreihen entwickelbar, und wir können die Bewertung $v_i(\alpha)$ direkt an der Ordnung der Puiseuxreihe an P_i ablesen (siehe Kapitel III).

Wir beschließen das Kapitel über Grundlagen mit einem Beispiel, welches wir im Verlauf der Arbeit noch häufiger aufgreifen werden.

BEISPIEL I.25. *Wir betrachten den kubischen Funktionenkörper $F = \mathbb{F}_5(x, \rho)$, welcher durch*

$$f(x, \rho) = \rho^3 + (4x^3 + 4x^2 + 2x + 2)\rho^2 + (3x + 3)\rho + 2 = 0$$

gegeben ist. Damit ist $p = q = 5$ und $n = 3$. In F zerlegt sich P_∞ in $P_1, P_2 \in \mathbb{P}(F)$ mit $e_1 = f_1 = n_1 = 1$ und $e_2 = 2, f_2 = 1, n_2 = 2$. Es gelten also $s = 2, e = 2$, und die Signatur ist $(1, 1; 2, 1)$.

KAPITEL II

Geometrie der Zahlen

In diesem Kapitel werden wir Grundlagen der Gittertheorie und Analoga zur Minkowskischen Geometrie der Zahlen basierend auf K. Mahler [Ma] (siehe auch [Arm]) sowie Längenfunktionen einführen. Hierauf aufbauend werden wir eine spezielle Längenfunktion B untersuchen und Aussagen über sukzessive Minima herleiten.

1. Gitter und Längenfunktionen

In diesem Abschnitt entwickeln wir die Minkowskische Geometrie der Zahlen für Funktionenkörper. Wir beginnen mit einigen Definitionen.

Definition II.1. *Für den Rest des Abschnitts fixieren wir $k, d \in \mathbb{N}$, setzen $L := E\langle x^{-1/k}\rangle := \mathbb{F}_{q^d}\langle x^{-1/k}\rangle$, $v := V_k$ und definieren:*

$$\begin{aligned} |\cdot| \quad &: \quad L \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto q^{-dv(\alpha)}, \\ V \quad &: \quad L^n \longrightarrow \mathbb{Z} \cup \{\infty\} : \alpha = (\alpha_1, \ldots, \alpha_n) \longmapsto \min_{i=1}^{n} v(\alpha_i) \text{ und} \\ \|\cdot\| \quad &: \quad L^n \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto q^{-dV(\alpha)}. \end{aligned}$$

Bemerkung II.2. *Die Abbildung $L^n \times L^n \longrightarrow \mathbb{R}^{\geq 0} : (\alpha, \beta) \longmapsto \|\alpha - \beta\|$ macht L^n zu einem (ultra-) metrischen Raum.*

Definition II.3. *Eine Abbildung $G : L^n \to \mathbb{R}^{\geq 0}$ ($G : F \to \mathbb{R}^{\geq 0}$) mit*

(1) $G(\alpha) = 0 \Leftrightarrow \alpha = 0$,
(2) $G(\lambda\alpha) = |\lambda| G(\alpha)$ ($G(\lambda\alpha) = |\lambda|_\infty G(\alpha)$) *und*
(3) $G(\alpha \pm \beta) \leq \max\{G(\alpha), G(\beta)\}$

für alle $\lambda \in L, \alpha, \beta \in L^n$ ($\lambda \in \mathbb{F}_q(x), \alpha, \beta \in F$) heißt Längenfunktion auf L^n (F).

BEMERKUNG II.4. *1) Die Abbildung* $\|\cdot\|$ *ist eine Längenfunktion auf* L^n.

2) Ist G *eine Längenfunktion auf* L^n *und* $M \in \mathrm{GL}(n, L)$, *so ist offensichtlich auch* $G \circ M$ *eine Längenfunktion auf* L^n.

Nach diesen grundlegenden Definitionen wenden wir uns zunächst der Gestalt konvexer Mengen in L^n zu.

DEFINITION II.5. *Eine Menge* $C \subset L^n$ *heißt konvexer Körper, wenn eine Längenfunktion* G *auf* L^n *existiert mit*

$$C = C(G) := \{\alpha \in L^n \mid G(\alpha) \leq 1\}.$$

Weiter heißt eine Menge $C \subset L^n$ *Parallelotop, wenn* $M \in \mathrm{GL}(n, L)$ *existiert mit*

$$C = C(M) := \{\alpha \in L^n \mid \|M\alpha\| \leq 1\}.$$

Nach [Ma] gilt dann der folgende

SATZ II.6. *Eine Menge* $C \subset L^n$ *ist genau dann ein konvexer Körper, wenn sie ein Parallelotop ist.*

BEMERKUNG II.7. *Die obige Äquivalenz legt die Vermutung nahe, daß jede Längenfunktion* G *von der Gestalt* $\|M \cdot \|$ *für ein geeignetes* $M \in \mathrm{GL}(n, L)$ *sei. Dies ist genau dann richtig, falls* $\{G(\alpha) \mid \alpha \in L^n\} = \{|\alpha| \mid \alpha \in L\}$.

Im Hinblick auf das Mahlersche Analogon zum Minkowskischen Gitterpunktsatz führen wir einen Volumenbegriff ein.

DEFINITION II.8. *Für* $M \in \mathrm{GL}(n, L)$ *sei* $C := C(M)$ *ein konvexer Körper. Dann heißt* $\mathrm{Vol}(C) := |\det M|^{-1}$ *das Volumen von* C.

BEMERKUNG II.9. *1) Es gilt:* $\mathrm{Vol}(C(\mathrm{Id}_n)) = \mathrm{Vol}(\{\alpha \in L^n \mid \|\alpha\| \leq 1\}) = 1$.

2) Für einen konvexen Körper C *ist das Volumen ein „Maß" für* $\#(C \cap (E[x^{1/k}])^n)$, *d.h. für die Anzahl der „ganzen" Punkte in* C.

Wir kommen zum zentralen Begriff des R-Gitters.

DEFINITION II.10. *Seien* R *ein Teilring von* $E[x^{1/k}]$ *und* $M \in \mathrm{GL}(n, L)$. *Dann heißt* $\Lambda = \Lambda(M, R) := \{M\alpha \mid \alpha \in R^n\}$ *R-Gitter in* L^n. $\Delta = \Delta(\Lambda) := |\det M|^{-1}$ *heißt Gitterdeterminante von* Λ.

BEMERKUNG II.11. *Für einen unitären Teilring* R *von* $E[x^{1/k}]$ *gilt* $\Delta(R^n) = 1$.

Wir bemerken die Analogie zu Zahlkörpern:

Bemerkung II.12. *Wegen der Diskretheit von R in L mit der von $|\cdot|$ induzierten Topologie und der Invertierbarkeit von M ist ein R-Gitter $\Lambda \subset L^n$ eine diskrete, additive Untergruppe von L^n. Wie bei Zahlkörpern läßt sich für $R \in \{E[x^{1/k}], \mathbb{F}_q[x]\}$ und $j \in \mathbb{N}$ zeigen: $a_1, \ldots, a_j \in \Lambda$ sind genau dann $E[x^{1/k}]$- bzw. $\mathbb{F}_q[x]$-linear unabhängig, wenn sie L- bzw. $\mathbb{F}_q\langle x^{-1}\rangle$-linear unabhängig sind.*

Schließlich treffen wir eine verallgemeinerte Definition von sukzessiven Minima, wobei wir beachten, daß o_F auch als freier $\widetilde{\mathbb{F}}_q[x]$-Modul vom Rang n/l aufgefaßt werden kann (vgl. Bemerkung I.17.(2)):

Definition II.13. *Seien R ein Teilring von $E[x^{1/k}]$, $\Lambda \subset L^n$ ein R-Gitter und G eine Längenfunktion auf L^n. Für $i \in \{1, \ldots, n\}$ heißt*

$$\begin{aligned} M_i(\Lambda, R, G) := \min\{ \ & \lambda \in \mathbb{R} \mid \textit{ es existieren } R\textit{-linear unabhängige} \\ & a_1, \ldots, a_i \in \Lambda \textit{ mit } G(a_j) \le \lambda, \quad 1 \le j \le i\} \end{aligned}$$

das i-te sukzessive Minimum von Λ (bzgl. R und G).

Spezialisieren wir in obiger Definition $R \in \{\mathbb{F}_q[x], \widetilde{\mathbb{F}}_q[x]\}$ und ersetzen G durch eine Längenfunktion auf F und Λ durch o_F, so definieren wir analog das i-te sukzessive Minimum $M_i(o_F, R, G)$ von o_F (bzgl. R und G).

Damit können wir abschließend das Mahlersche Analogon zum Minkowskischen Gitterpunktsatz und zum Minkowskischen Satz über sukzessive Minima zitieren (siehe [Ma]):

Satz II.14. *Seien G eine Längenfunktion auf L^n, $M \in \mathrm{GL}(n, L)$, $R := E[x^{1/k}]$, $\Lambda := \Lambda(M, R)$, $\Delta := \Delta(\Lambda)$, $V := \mathrm{Vol}(C(G))$ und bezeichne $M_i := M_i(\Lambda, R, G), 1 \le i \le n$. Dann existiert $T \in \mathrm{GL}(n, R)$ mit $|\det T| = 1$, und es gilt*

$$G(b_i) = M_i, \quad 1 \le i \le n, \textit{ wobei } (b_1, \ldots, b_n) := MT.$$

Ferner gelten

$$\prod_{i=1}^n M_i = \Delta/V \textit{ und } M_1 \le (\Delta/V)^{1/n},$$

d.h., es existiert ein Gitterpunkt

$$\alpha \in \Lambda^\times \textit{ mit } 0 < G(\alpha) \le (\Delta/V)^{1/n}.$$

2. Die Längenfunktion B

In diesem Abschnitt betrachten wir in Analogie zur T_2-Länge bei Zahlkörpern (siehe [P, Ch. IV.1]) eine spezielle Längenfunktion B, welche für konstruktive Untersuchungen von F eine zentrale Rolle einnehmen wird.

Definition und Satz II.15. *Die Funktion*

$$B : F \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto \max_{i=1}^{s} |\alpha|_i^{1/e_i}$$

ist eine Längenfunktion auf F mit $B(\cdot) = q^{B^*(\cdot)}$, wo

$$B^* : F \longrightarrow \{a/e \mid a \in \mathbb{Z}\} \cup \{-\infty\} : \alpha \longmapsto -\min_{i=1}^{s} v_i(\alpha)/e_i.$$

Weiter gilt $B^*|_{o_F^\times} \geq 0$.

Beweis: Wir prüfen zunächst die Bedingungen aus Definition II.3. Offensichtlich gilt $B(\alpha) = 0 \Leftrightarrow \alpha = 0$ für $\alpha \in F$. Seien nun $\alpha, \beta \in F$ und $\lambda \in \mathbb{F}_q(x)$ beliebig. Dann impliziert $v_i(\lambda) = e_i v_\infty(\lambda)$ für $i \in \{1, \ldots, s\}$ die zweite Bedingung. Wir beachten nun für $i \in \{1, \ldots, s\}$ und $\delta > 0$ die Abschätzung

$$|\alpha \pm \beta|_i^\delta \leq \max\{|\alpha|_i, |\beta|_i\}^\delta = \max\{|\alpha|_i^\delta, |\beta|_i^\delta\},$$

aus der

$$\begin{aligned} B(\alpha \pm \beta) &= \max_{i=1}^{s} |\alpha \pm \beta|_i^{1/e_i} \leq \max_{i=1}^{s} \max\{|\alpha|_i^{1/e_i}, |\beta|_i^{1/e_i}\} \\ &= \max\{\max_{i=1}^{s} |\alpha|_i^{1/e_i}, \max_{i=1}^{s} |\beta|_i^{1/e_i}\} = \max\{B(\alpha), B(\beta)\} \end{aligned}$$

folgt.

Wegen $|\cdot|_i = q^{-v_i(\cdot)}, 1 \leq i \leq s$, und $q > 1$ gilt $B(\cdot) = q^{B^*(\cdot)}$.

Für die letzte Aussage fixieren wir ein $\alpha \in o_F^\times$ und nehmen $B^*(\alpha) < 0$ an. Dies impliziert $v_i(\alpha) > 0$ für alle $1 \leq i \leq s$, womit $\sum_{i=1}^{s} f_i v_i(\alpha) > 0$ folgt. Damit ergibt sich der gewünschte Widerspruch aus der Produktformel und $v_P(\alpha) \geq 0$ für alle $P \in \mathbb{P}(F)$. □

Beispiel II.16. *Für* Beispiel I.25 *gilt also:*

$$B : F \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto \max\{|\alpha|_1, |\alpha|_2^{1/2}\}.$$

Bemerkung II.17. *Mit der Notation aus* Bemerkung I.15 *besitzt das Analogon zu B im Zahlkörperfall die Gestalt (vgl.* [N, Ch. 2, §1, 3.]*):*

$$\lceil\cdot\rceil : \mathcal{F} \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto \max_{i=1}^{r_1+r_2} |\alpha^{(i)}|.$$

Bei der algorithmischen Untersuchung von Zahlkörpern spielt die sog. T_2-Länge

$$T_2 : \mathcal{F} \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto \sum_{i=1}^{n} |\alpha^{(i)}|^2$$

eine zentrale Rolle (vgl. [P, Ch. IV.1]), und es gilt $\lceil\cdot\rceil^2 \leq T_2(\cdot) \leq n\lceil\cdot\rceil^2$.

Im Funktionenkörperfall werden wir unsere Untersuchungen auf die Längenfunktion B stützen und beweisen die erste Hauptaussage.

Theorem II.18. *Es existiert eine Ganzheitsbasis $\omega_1, \ldots, \omega_n \in o_F$ mit $B(\omega_i) = M_i(o_F, \mathbb{F}_q[x], B)$ für $1 \leq i \leq n$.*

Beweis: Seien $R := \mathbb{F}_q[x]$ und $\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n \in o_F$ eine fixierte Ganzheitsbasis. Wir zeigen, daß ein $T \in \mathrm{GL}(n, R)$ mit $B(\omega_i) = M_i(o_F, R, B)$ existiert, wobei $(\omega_1, \ldots, \omega_n) := (\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n)T$.

Wir setzen $L := \mathbb{F}_q\langle x^{-1}\rangle$ und fixieren für $i \in \{1, \ldots, s\}$ eine L-Basis $b_{i,1}, \ldots, b_{i,n_i}$ von $\widehat{F}_i/L$.

Für $i \in \{1, \ldots, s\}$ bezeichne ferner ι_i die Inklusion $F \hookrightarrow \widehat{F}_i$ und

$$\phi_i : L^{n_i} \longrightarrow \widehat{F}_i : \alpha = (\alpha_1, \ldots, \alpha_{n_i})^t \longmapsto \sum_{j=1}^{n_i} \alpha_j b_{i,j}.$$

Wir setzen

$$M := \begin{pmatrix} \phi_1^{-1}\iota_1(\widetilde{\omega}_1) & \cdots & \phi_1^{-1}\iota_1(\widetilde{\omega}_n) \\ \vdots & & \vdots \\ \phi_s^{-1}\iota_s(\widetilde{\omega}_1) & \cdots & \phi_s^{-1}\iota_s(\widetilde{\omega}_n) \end{pmatrix} \in L^{n\times n}$$

und zeigen $M \in \mathrm{GL}(n, L)$.

Angenommen es existieren $a_1, \ldots, a_n \in L$, nicht alle Null, mit

$$\sum_{i=1}^{n} a_i \begin{pmatrix} \phi_1^{-1}\iota_1(\widetilde{\omega}_i) \\ \vdots \\ \phi_s^{-1}\iota_s(\widetilde{\omega}_i) \end{pmatrix} = 0.$$

Dann implizieren zeilenweise Betrachtung und die Linearität von ϕ_i die Existenz von $\widetilde{a}_1, \ldots, \widetilde{a}_n \in L$, nicht alle Null, mit

$$\sum_{i=1}^{n} \widetilde{a}_i \begin{pmatrix} \iota_1(\rho^{i-1}) \\ \vdots \\ \iota_s(\rho^{i-1}) \end{pmatrix} = 0.$$

Damit folgt aber für $g(y) := \sum_{i=1}^{n} \widetilde{a}_i y^{i-1} \in L[y]$: $g(\rho_i) = 0, \quad 1 \leq i \leq n$, und wir erhalten den gewünschten Widerspruch mit $\deg(g) \in \{1, \ldots, n-1\}$.

Nun betrachten wir die Abbildung

$$\widetilde{B} : L^n = \prod_{i=1}^{s} L^{n_i} \longrightarrow \mathbb{R}^{\geq 0} : \beta = (\beta_1, \dots, \beta_s)^t \longmapsto \max_{i=1}^{s} |\phi_i(\beta_i)|_i^{1/e_i},$$

wobei $|\cdot|_i$ auf $\widehat{F}_i$ fortgesetzt zu verstehen ist.

Dann ist $\widetilde{B}$ eine Längenfunktion auf L^n (Beweis analog Definition und Satz II.15).

Wir setzen $\widetilde{\omega} := (\widetilde{\omega}_1, \dots, \widetilde{\omega}_n)$ und fixieren $k \in \{1, \dots, n\}$. Aus der R-linearen Unabhängigkeit von $\widetilde{\omega}_1, \dots, \widetilde{\omega}_n$ folgt nun für $\lambda_1, \dots, \lambda_k \in R^n$:

$$\begin{aligned} & \widetilde{\omega}\lambda_1, \dots, \widetilde{\omega}\lambda_k \in o_F \text{ sind } R\text{-linear unabhängig} \\ \Longleftrightarrow\ & \lambda_1, \dots, \lambda_k \in R^n \text{ sind } R\text{-linear unabhängig.} \end{aligned} \tag{2}$$

Schließlich beachten wir noch für $\nu = (\nu_1, \dots, \nu_n)^t \in R^n$ und $\alpha = \widetilde{\omega}\nu \in o_F$:

$$\begin{aligned} B(\alpha) &= \max_{i=1}^{s} |\alpha|_i^{1/e_i} = \max_{i=1}^{s} |\iota_i(\alpha)|_i^{1/e_i} \\ &= \widetilde{B}((\phi_1^{-1}\iota_1(\alpha), \dots, \phi_s^{-1}\iota_s(\alpha))^t) = \widetilde{B}(M\nu). \end{aligned} \tag{3}$$

Nach Satz II.14 existiert nun zu $\Lambda := \Lambda(M, R) \subset L^n$ ein $T \in \mathrm{GL}(n, R)$ mit

$$\widetilde{B}(b_i) = M_i(\Lambda, R, \widetilde{B}), \quad 1 \leq i \leq n, \text{ wobei } (b_1, \dots, b_n) := MT.$$

Daher folgt die Behauptung aus (2) und (3). □

Bemerkung II.19. *Für Gitter $\Lambda \subset \mathbb{R}^n$, $n \geq 4$, ist es i.allg. nicht immer möglich, Basen so zu wählen, daß sie die sukzessiven Minima bzgl. $\|\cdot\|_2$ realisieren (vgl.* [PZ, Ch. 3, (3.31), (3.32)]*).*

Abschließend gibt der nächste Satz Auskunft über die Struktur der sukzessiven Minima $M_i(o_F, \mathbb{F}_q[x], B)$:

Satz II.20. *Seien $n = \tilde{n}l$ und $\widetilde{\omega}_1, \dots, \widetilde{\omega}_{\tilde{n}} \in o_F$ mit $o_F = \bigoplus_{i=1}^{\tilde{n}} \widetilde{\mathbb{F}}_q[x]\widetilde{\omega}_i$, wobei $B(\widetilde{\omega}_i) = \widetilde{M}_i := M_i(o_F, \widetilde{\mathbb{F}}_q[x], B), 1 \leq i \leq \tilde{n}$. Dann gelten mit $\widetilde{\mathbb{F}}_q = \mathbb{F}_q(\zeta)$ ($\zeta \in \widetilde{\mathbb{F}}_q$ geeignet):*

1. *$\omega_{(i-1)l+j} := \zeta^{j-1}\widetilde{\omega}_i \in o_F, 1 \leq i \leq \tilde{n}, 1 \leq j \leq l$, ist eine Ganzheitsbasis von o_F.*
2. *$B(\omega_{(i-1)l+j}) = M_{(i-1)l+j} := M_{(i-1)l+j}(o_F, \mathbb{F}_q[x], B) = \widetilde{M}_i = B(\widetilde{\omega}_i), 1 \leq i \leq \tilde{n}, 1 \leq j \leq l$.*
3. *Es gelten $M_1 = 1$ und $M_l < M_{l+1}$.*

Beweis: Wegen

$$o_F = \bigoplus_{i=1}^{\tilde{n}} \widetilde{\mathbb{F}}_q[x]\widetilde{\omega}_i = \bigoplus_{i=1}^{\tilde{n}} \bigoplus_{j=1}^{l} \mathbb{F}_q[x]\zeta^{j-1}\widetilde{\omega}_i = \bigoplus_{i=1}^{n} \mathbb{F}_q[x]\omega_i$$

ist $\omega_1, \dots, \omega_n$ eine Ganzheitsbasis von o_F.

Um (2) zu zeigen, nehmen wir die Existenz von $k \in \{1, \dots, n\}$ und $\mathbb{F}_q[x]$-linear unabhängigen $b_1, \dots, b_k \in o_F$ mit

$$\max_{i=1}^{k} B(b_i) < B(\omega_k)$$

an.

Sei nun $k = (i_0 - 1)l + j_0$ für geeignete $i_0, j_0 \in \mathbb{N}$. Dann existieren $\kappa \geq i_0, 1 \leq i_1 < \ldots < i_\kappa \leq k$, so daß $b_{i_1}, \dots, b_{i_\kappa}$ $\widetilde{\mathbb{F}}_q[x]$-linear unabhängig sind.

Denn aus der gegenteiligen Annahme folgt

$$\mathrm{Rg}_{\widetilde{\mathbb{F}}_q[x]}[b_{i_1}, \dots, b_{i_\kappa}]_{\widetilde{\mathbb{F}}_q[x]} < \kappa \text{ für alle } \kappa \geq i_0 \text{ und } 1 \leq i_1 < \ldots < i_\kappa \leq k.$$

Dies impliziert

$$\mathrm{Rg}_{\widetilde{\mathbb{F}}_q[x]}[b_1, \dots, b_k]_{\widetilde{\mathbb{F}}_q[x]} < i_0,$$

womit der Widerspruch aus

$$\mathrm{Rg}_{\mathbb{F}_q[x]}[b_1, \dots, b_k]_{\mathbb{F}_q[x]} < (i_0 - 1)l < (i_0 - 1)l + j_0 = k$$

folgt.

Seien also o.B.d.A. $b_1, \dots, b_{i_0}$ $\widetilde{\mathbb{F}}_q[x]$-linear unabhängig.

Damit folgt (2) aus dem Widerspruch

$$\max_{i=1}^{i_0} B(b_i) \leq \max_{i=1}^{k} B(b_i) < B(\omega_k) = B(\zeta^{j_0-1}\widetilde{\omega}_{i_0}) = B(\widetilde{\omega}_{i_0}) = \widetilde{M}_{i_0}.$$

Schließlich gilt mit Definition und Satz II.15 sofort $M_1 = 1$. Beachten wir

$$U := \{\alpha \in o_F \mid v_i(\alpha) = 0, 1 \leq i \leq s\} = \widetilde{\mathbb{F}}_q^\times,$$

so bildet $U \cup \{0\}$ einen l-dimensionalen $\mathbb{F}_q$-Vektorraum.

Ferner gilt mit der Produktformel für $\xi \in o_F$

$$\xi \in U \iff B(\xi) = 1.$$

Nehmen wir nun $M_l = M_{l+1}$ an, so impliziert das bereits gezeigte $1 = M_1 = \ldots = M_{2l}$. Damit folgt $\omega_i \in U, 1 \leq i \leq 2l$, und wir erhalten einen Widerspruch zur $\mathbb{F}_q$-Dimension von $U \cup \{0\}$. $\square$

FOLGERUNG II.21. *Bezeichnet* $M_i := M_i(o_F, \mathbb{F}_q[x], B), 1 \leq i \leq n$, *so zeigt der vorhergehende Satz*

$$1 = M_1 = \ldots = M_l < M_{l+1} = \ldots = M_{2l} \leq \ldots \leq M_{n-l+1} = \ldots = M_n.$$

Für den Fall, daß P_∞ zahm verzweigt ist, werden wir im nächsten Kapitel einen effizienten Algorithmus zur Berechnung einer Ganzheitsbasis mit der Eigenschaft aus Theorem II.18 angeben.

KAPITEL III

Reduktion von Ganzheitsbasen

Im weiteren Verlauf der Arbeit wird sich zeigen, wie mit Hilfe von Elementen $\alpha \in F$ mit vorgegebenen unteren Abschätzungen für ihre Bewertungen über ∞ Ganzheitsbasen reduziert und Grundeinheiten berechnet bzw. Wurzeltests durchgeführt werden können.

Im Zahlkörperfall korrespondiert dies zur Berechnung von Elementen mit oberen Schranken für ihre Konjugiertenbeträge. Gewöhnlich geschieht dies mittels Auszählen einer gewichteten positiv definiten quadratischen Form (vgl. [PZ, Ch. 5, (3.11)]).

Im Fall, daß P_∞ zahm verzweigt ist, werden wir einen effizienten Algorithmus angeben, der es gestattet, Elemente $\alpha \in o_F$ mit $v_i(\alpha) \geq c_i$ für $c_i \in \mathbb{Z}, \quad 1 \leq i \leq s$, zu berechnen.

Allgemeiner werden wir für einen Divisor $D \in \mathrm{Div}_\infty(F)$ den Begriff einer D-reduzierten Ganzheitsbasis einführen, aus der wir leicht eine $\mathbb{F}_q$-Basis des folgenden Riemann-Rochschen Raums berechnen können, dessen Definition auf W. M. Schmidt [Sch2] zurückgeht:

Definition III.1. *Für $D = \sum_{i=1}^{s} c_i P_i \in \mathrm{Div}_\infty(F)$ und $t \in \mathbb{R}$ definieren wir den $\widetilde{\mathbb{F}}_q$-Vektorraum*

$$\mathcal{L}(D,t) := \{\alpha \in o_F \mid v_i(\alpha) \geq -c_i - te_i, \quad 1 \leq i \leq s\}.$$

Bemerkung III.2. *1) $\mathcal{L}(D,t)$ ist endlichdimensional (siehe z.B.* [St, I.4.9.]*), und die Produktformel impliziert $\mathcal{L}(D,t) = \{0\}$, wenn $\sum_{i=1}^{s} f_i(-c_i - te_i) > 0$.*

2) Wie schon oben erwähnt, ist das Analogon zur Berechnung von $\mathcal{L}(D,t)$ im Zahlkörperfall das Auszählen einer gewichteten positiv definiten quadratischen Form. Denn für $\alpha \in o_F$ sind äquivalent

$$\alpha \in \mathcal{L}(D,t) \Longleftrightarrow |\alpha|_i \leq q^{c_i + te}, \quad 1 \leq i \leq s.$$

Um im Zahlkörperfall (mit der Notation aus Bemerkung I.15*)* $\alpha \in o_{\mathcal{F}}$ *mit* $|\alpha^{(i)}| \leq \lambda_i$ *für* $\lambda_i \in \mathbb{R}^{>0}, 1 \leq i \leq r_1 + r_2$*, zu berechnen, betrachten wir*

$$T_{2,\lambda} : o_{\mathcal{F}} \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto \sum_{i=1}^{r_1} \frac{|\alpha^{(i)}|^2}{\lambda_i^2} + 2 \sum_{i=r_1+1}^{r_1+r_2} \frac{|\alpha^{(i)}|^2}{\lambda_i^2},$$

auf $o_{\mathcal{F}}$ *(vgl.* [P, Ch. VI.2]*). Wir bestimmen nun (mittels Auszählens, vgl.* [PZ, Ch. 3, (3.15)]*)* $\alpha \in o_{\mathcal{F}}$ *mit* $T_{2,\lambda}(\alpha) \leq n$ *und testen schließlich* $|\alpha^{(i)}| \leq \lambda_i, 1 \leq i \leq r_1+r_2$.

3) Wir beachten, daß $\mathcal{L}(D,t)$ *im Gegensatz zu* $\{\alpha \in o_{\mathcal{F}} \mid |\alpha^{(i)}| \leq \lambda_i, 1 \leq i \leq r_1+r_2\}$ *ein* $\widetilde{\mathbb{F}}_q$*- bzw.* $\mathbb{F}_q$*-Vektorraum ist. Kennen wir also eine Basis von* $\mathcal{L}(D,t)$*, so können wir die Elemente dieses Raums leicht angeben.*

In diesem Kapitel werden wir für den Fall, daß P_∞ *zahm verzweigt ist, einen effizienten Algorithmus zur Berechnung einer* $\mathbb{F}_q$*-Basis von* $\mathcal{L}(D,t)$ *angeben. Ist* P_∞ *wild verzweigt, so geben wir in Kapitel IV.1 einen allgemeinen Algorithmus zur Berechnung von* $\mathcal{L}(D,t)$*.*

Für Funktionenkörper über $\mathbb{C}$ existiert ein deterministischer Algorithmus zur Berechnung einer $\mathbb{C}$-Basis von $\mathcal{L}(D,t)$ (vgl. [Sch2]), welcher auf [Coa] basiert. Dieser Algorithmus benutzt Puiseuxentwicklungen aller Nullstellen von f über P_∞, was ohne weiteres möglich ist, da $\mathbb{C}$ Charakteristik 0 besitzt und algebraisch abgeschlossen ist.

Bevor wir eine geeignete Modifikation dieses Algorithmus geben können, betrachten wir zunächst Puiseuxentwicklungen der Nullstellen von f über P_∞.

Es wird sich hierbei zeigen, daß die Bedingung $p \nmid e$ (d.h., P_∞ ist zahm verzweigt) hinreichend für die Existenz von Puiseuxentwicklungen aller Nullstellen ist.

1. Puiseuxentwicklungen über P_∞

In diesem Abschnitt untersuchen wir die Gestalt von Puiseuxentwicklungen der Nullstellen $\rho_1, \ldots, \rho_n$ über P_∞. Dazu zeigen wir zunächst, in welcher k-ten Wurzel aus x^{-1} sich die Nullstellen entwickeln lassen, sofern P_∞ zahm verzweigt ist.

Satz III.3. *Gelte* $p \nmid e$ *und sei* $\tau \in \overline{\mathbb{F}_q(x)}$ *mit* $f(x,\tau) = 0$*. Dann folgt* $\tau \in \overline{\mathbb{F}}_q\langle x^{-1/e}\rangle$*.*

Beweis: Wir betrachten hierzu das Zerlegungsverhalten von (x^{-1}) bei Konstantenkörpererweiterungen.

Zunächst gelten über $\mathbb{F}_q$:

$$(x^{-1}) \;=\; D_0 + \sum_{i=1}^{s} e_i P_i \text{ mit } D_0 \in \mathrm{Div}_0(F),$$

$$\begin{aligned} f &= \prod_{i=1}^{s} g_i \in \mathbb{F}_q\langle x^{-1}\rangle[y] \text{ und} \\ \prod_{i=1}^{s} \widehat{F}_i &\cong \mathbb{F}_q\langle x^{-1}\rangle \otimes_{\mathbb{F}_q(x)} F, \end{aligned}$$

mit $\deg(P_i) = f_i$, irreduziblen, bzgl. y normierten und separablen $g_i \in \mathbb{F}_q\langle x^{-1}\rangle[y]$, $\deg_y(g_i) = e_i f_i = n_i = [\widehat{F}_i : \mathbb{F}_q\langle x^{-1}\rangle]$ und $\widehat{F}_i \cong \mathbb{F}_q\langle x^{-1}\rangle[y]/g_i\mathbb{F}_q\langle x^{-1}\rangle[y], 1 \le i \le s$.

Beim Übergang von $\mathbb{F}_q$ zum exakten Konstantenkörper $\widetilde{\mathbb{F}}_q \cong \mathbb{F}_{q^l}$ für ein passendes $l \in \mathbb{N}$ beachten wir (vgl. [Ha, S. 350ff, 398ff]):

$$f = \prod_{i=1}^{l} \tilde{f}^{(i)} \in \mathbb{F}_{q^l}(x)[y],$$

wobei die $\tilde{f}^{(i)}$ konjugiert sind bezüglich $\mathbb{F}_{q^l}/\mathbb{F}_q$ und $\deg(\tilde{f}^{(i)}) = \frac{n}{l} =: \tilde{n}$, $(1 \le i \le l)$. Ferner bemerken wir, daß $\tilde{f}^{(i)}$ absolut-irreduzibel ist $(1 \le i \le l)$, d.h. irreduzibel in $\overline{\mathbb{F}}_q(x)[y]$.

Es folgt $F \cong \mathbb{F}_{q^l}(x)[y]/\tilde{f}^{(i)}\mathbb{F}_{q^l}(x)[y]$ für $1 \le i \le l$, und o.B.d.A. sei $\tilde{f}^{(1)}(x,\tau) = 0$.

Wir beachten nun $F = \mathbb{F}_{q^l}F$. Setzen wir $P_i =: \tilde{P}_i \in \mathbb{P}_\infty(\mathbb{F}_{q^l}F)$ und fassen $F, \widehat{F}_i$ und $o_{F,\infty}$ über $\mathbb{F}_{q^l}$ auf, so erhalten wir:

$$\begin{aligned} (x^{-1}) &= \tilde{D}_0 + \sum_{i=1}^{s} e_i \tilde{P}_i \text{ mit } \tilde{D}_0 \in \mathrm{Div}_0(\mathbb{F}_{q^l}F), \\ \tilde{f}^{(1)} &= \prod_{i=1}^{s} \tilde{g}_i \in \mathbb{F}_{q^l}\langle x^{-1}\rangle[y] \text{ und} \\ \prod_{i=1}^{s} \widehat{F}_i &\cong \mathbb{F}_{q^l}\langle x^{-1}\rangle \otimes_{\mathbb{F}_{q^l}(x)} F, \end{aligned}$$

mit $\deg(\tilde{P}_i) = \frac{f_i}{l} =: \tilde{f}_i$, irreduziblen, bzgl. y normierten und separablen $\tilde{g}_i \in \mathbb{F}_{q^l}\langle x^{-1}\rangle[y]$, $\deg(\tilde{g}_i) = e_i\tilde{f}_i =: \tilde{n}_i = [\widehat{F}_i : \mathbb{F}_{q^l}\langle x^{-1}\rangle]$ und $\mathbb{F}_{q^l}\langle x^{-1}\rangle[y]/\tilde{g}_i\mathbb{F}_{q^l}\langle x^{-1}\rangle[y] \cong \widehat{F}_i, 1 \le i \le s$.

Da $\tilde{f}^{(1)}$ absolut-irreduzibel ist, ergibt sich schließlich beim Übergang von $\mathbb{F}_{q^l}$ nach $\overline{\mathbb{F}}_q$:

$$\begin{aligned} \overline{(x^{-1})} &= \overline{D}_0 + \sum_{i=1}^{s}\sum_{j=1}^{\tilde{f}_i} e_i \overline{P}_{i,j} \text{ mit } \overline{D}_0 \in \mathrm{Div}_0(\overline{\mathbb{F}}_q F), \\ \tilde{f}^{(1)} &= \prod_{i=1}^{s}\prod_{j=1}^{\tilde{f}_i} \overline{g}_{i,j} \in \overline{\mathbb{F}}_q\langle x^{-1}\rangle[y] \text{ und} \end{aligned}$$

$$\prod_{i=1}^{s}\prod_{j=1}^{\tilde{f}_i}\widehat{F}_{i,j} \quad\cong\quad \overline{\mathbb{F}}_q\langle x^{-1}\rangle \otimes_{\overline{\mathbb{F}}_q(x)} \overline{\mathbb{F}}_q F,$$

wobei $\overline{P}_{i,j} \in \mathbb{P}_\infty(\overline{\mathbb{F}}_q F)$, $1 \le i \le s, 1 \le j \le \tilde{f}_i$, und $\overline{(x^{-1})}$ den zu x^{-1} gehörenden Hauptdivisor in $\mathrm{Div}(\overline{\mathbb{F}}_q F)$ bezeichnet. Ferner gelten $\deg(\overline{P}_{i,j}) = 1$, $\overline{g}_{i,j} \in \overline{\mathbb{F}}_q\langle x^{-1}\rangle[y]$ sind irreduzibel und bzgl. y normiert und separabel, $\deg(\overline{g}_{i,j}) = e_i = [\widehat{F}_{i,j} : \overline{\mathbb{F}}_q\langle x^{-1}\rangle]$, wobei $\widehat{F}_{i,j} \cong \overline{\mathbb{F}}_q\langle x^{-1}\rangle[y]/\overline{g}_{i,j}\overline{\mathbb{F}}_q\langle x^{-1}\rangle[y]$ die Vervollständigung von $\overline{\mathbb{F}}_q F$ an $\overline{P}_{i,j}$ bezeichnet $(1 \le i \le s, 1 \le j \le \tilde{f}_i)$.

O.B.d.A. gelten nun $\overline{g}_{1,1}(x,\tau) = 0$ und $\tau \in \widehat{F}_{1,1}$. Da $p \nmid e_1$, existiert nach [Ch, Ch. IV, §6] ein $\pi \in \widehat{F}_{1,1}$ mit $\pi^{e_1} = x^{-1}$, und es gilt

$$v_{\overline{P}_{1,1}}(x^{-1/e_1}) = 1 \text{ und damit } \widehat{F}_{1,1} = \overline{\mathbb{F}}_q\langle x^{-1/e_1}\rangle,$$

wo x^{-1/e_1} eine beliebige der e_1-ten Wurzeln von x^{-1} in $\widehat{F}_{1,1}$ bezeichnet.
Dies impliziert $\tau \in \overline{\mathbb{F}}_q\langle x^{-1/e_1}\rangle \subset \overline{\mathbb{F}}_q\langle x^{-1/e}\rangle$. □

Im nachfolgenden Satz werden wir nun den Erweiterungsgrad des Konstantenkörpers für die Puiseuxentwicklungen klären.

Satz III.4. *Gelte $p \nmid e$ und sei $\tau \in \overline{\mathbb{F}_q(x)}$ mit $f(x,\tau) = 0$. Dann existiert $d = d(\tau) \in \{1,\dots,n\}$ mit $\tau \in \mathbb{F}_{q^d}\langle x^{-1/e}\rangle$.*

Beweis: Nach Satz III.3 gilt $\tau \in \overline{\mathbb{F}}_q\langle x^{-1/e}\rangle$, und da $f \in \mathbb{F}_q[x,y]$ irreduzibel ist, folgt $\tau \ne 0$. Somit existieren $m \in \mathbb{Z}, a_i \in \overline{\mathbb{F}}_q$ mit $\tau = \sum_{i=m}^{\infty} a_i x^{-i/e}$.
Wir betrachten dazu den algebraischen Körperturm

$$E_1 := \mathbb{F}_q(a_m), \quad E_i := E_{i-1}(a_{m+i-1}), i \ge 2 \quad \text{und} \quad E_\infty := \mathbb{F}_q(a_m, a_{m+1}, \dots) \subset \overline{\mathbb{F}}_q.$$

Angenommen, es gilt $d := [E_\infty : \mathbb{F}_q] > n$. Dann existieren $i_o \in \mathbb{N}$ mit $[E_{i_0} : \mathbb{F}_q] =: n_0 > n$ und n_0 paarweise verschiedene Einbettungen $\sigma_j : E_{i_0} \hookrightarrow \overline{\mathbb{F}}_q$ mit $\sigma_j |_{\mathbb{F}_q} \equiv \mathrm{Id}, 1 \le j \le n_0$.

Wir setzen σ_j zu $\tilde{\sigma}_j : E_\infty \hookrightarrow \overline{\mathbb{F}}_q$ fort und definieren $\tau_j = \sum_{i=m}^{\infty} \tilde{\sigma}_j(a_i)x^{-i/e} \in \overline{\mathbb{F}}_q\langle x^{-1/e}\rangle$ für $1 \le j \le n_0$. Diese sind paarweise verschieden, und wegen $\tilde{\sigma}_j |_{\mathbb{F}_q} \equiv \mathrm{Id}$ und $f \in \mathbb{F}_q[x,y]$ gilt $f(x,\tau_j) = 0, 1 \le j \le n_0$. Wegen $\deg(f) = n < n_0$ erhalten wir den gewünschten Widerspruch. Somit ist $[E_\infty : \mathbb{F}_q] = d \le n$ und damit $\tau \in \mathbb{F}_{q^d}\langle x^{-1/e}\rangle$ gezeigt. □

Mit diesen beiden Sätzen und anhand ihrer Beweise können wir die zweite Hauptaussage formulieren:

THEOREM III.5. *Gelte $p \nmid e$. Dann existieren ein*

$$d \in \{1, \ldots, \mathrm{kgV}(d(\rho_1), \ldots, d(\rho_n))\}$$

und eine Numerierung der Nullstellen $\rho_1, \ldots, \rho_n$ mit

$$(\rho_1, \ldots, \rho_n) = (\rho_{1,1}, \ldots, \rho_{1,n_1}, \rho_{2,1}, \ldots, \rho_{2,n_2}, \ldots, \rho_{s,1}, \ldots, \rho_{s,n_s}),$$

so daß $\rho_{i,j} \in \mathbb{F}_{q^d}\langle x^{-1/e_i}\rangle \subset \mathbb{F}_{q^d}\langle x^{-1/e}\rangle, 1 \leq j \leq n_i$, die Entwicklungen an $P_i, 1 \leq i \leq s$, sind. Weiterhin enthält $\mathbb{F}_{q^d}$ alle e_i-ten Einheitswurzeln, $1 \leq i \leq s$.

Beweis: Die Existenz von d und der Numerierung folgt direkt aus den beiden vorangegangenen Sätzen nebst ihrer Beweise.

Für die Aussage über die Einheitswurzeln betrachten wir nochmal $\tau \in \mathbb{F}_{q^d}\langle x^{-1/e}\rangle$ mit $f(x, \tau) = 0$ und gehen zurück zum Beweis von Satz III.3. Dort galt o.B.d.A. $\tau \in \overline{\mathbb{F}}_q\langle x^{-1/e_1}\rangle$, und es existierte $\overline{g}_{1,1} \in \overline{\mathbb{F}}_q\langle x^{-1}\rangle[y]$ mit $\deg(\overline{g}_{1,1}) = e_1$ und $\overline{g}_{1,1}(x, \tau) = 0$. Mit dem oben gezeigten gilt

$$\tau = \sum_{i=\tilde{m}}^{\infty} \tilde{a}_i (x^{-1/e_1})^i \in \mathbb{F}_{q^d}\langle x^{-1/e_1}\rangle,$$

wobei x^{-1/e_1} eine der e_1-ten Wurzeln von x^{-1} in $\widehat{F}_{1,1}$ ist.

Wegen $p \nmid e_1$ existieren in $\overline{\mathbb{F}}_q$ genau e_1 verschiedene e_1-te Einheitswurzeln, welche wir mit $\zeta_1 := 1, \zeta_2, \ldots, \zeta_{e_1}$ bezeichnen. Betrachten wir

$$0 = \overline{g}_{1,1}(x, \tau) = \overline{g}_{1,1}\left((x^{-1/e_1})^{-e_1}, \sum_{i=\tilde{m}}^{\infty} \tilde{a}_i (x^{-1/e_1})^i\right)$$

als Potenzreihen-Identität in x^{-1/e_1}, so gilt auch

$$0 = \overline{g}_{1,1}\left((\zeta_j x^{-1/e_1})^{-e_1}, \sum_{i=\tilde{m}}^{\infty} \tilde{a}_i (\zeta_j x^{-1/e_1})^i\right), \quad 1 \leq j \leq e_1.$$

Da die Nullstellen von $\overline{g}_{1,1}$ auch Nullstellen von f sind (vgl. Satz III.3), impliziert dies mit dem oben gezeigten $\sum_{i=\tilde{m}}^{\infty} \tilde{a}_i (\zeta_j x^{-1/e_1})^i \in \mathbb{F}_{q^d}\langle x^{-1/e_1}\rangle$. Wegen $0 \neq \tilde{a}_{\tilde{m}} = \tilde{a}_{\tilde{m}}\zeta_1 \in \mathbb{F}_{q^d}$ folgt auch $\zeta_j = \tilde{a}_{\tilde{m}}^{-1}(\tilde{a}_{\tilde{m}}\zeta_j) \in \mathbb{F}_{q^d}, 1 \leq j \leq e_1$. Wenden wir dieses Argument auf alle Nullstellen von f an, so folgt die Behauptung. $\square$

BEMERKUNG III.6. *1) Insbesondere ist P_∞ zahm verzweigt, falls $p > n$ oder $p > \max_{i=1}^{s} e_i$ gilt. Somit besitzt die Strukturaussage über die Nullstellen von f ihre Gültigkeit in den meisten Fällen.*

2) Die Puiseuxentwicklungen können mittels des Newton-Puiseux Verfahrens gewonnen werden. Die Methode ist für algebraisch abgeschlossene Konstantenkörper

K z.B. in [Wa, Ch. IV] *dargestellt. Für ein $h \in K[z,y]$ lassen sich damit alle $\tau = \sum_{i=m}^{\infty} a_i z^i, \quad a_i \in K$, mit $h(z,\tau) = 0$ berechnen.*

Mit der Information aus Satz III.4 *läßt sich der Algorithmus geeignet modifizieren, indem sukzessive Körpertürme über $\mathbb{F}_q$ betrachtet werden.*

Um nun alle Nullstellen von f in $z := x^{-1/e}$ zu entwickeln, transformieren wir das Ausgangspolynom $f \in \mathbb{F}_q[x,y] = \mathbb{F}_q[z^{-e}, y]$.

Dazu definieren wir $g \in \mathbb{F}_q[z^{-1}, y]$ mit $f \equiv g$, ferner $h \in \mathbb{F}_q[z,y]$ durch

$$h(z,y) := z^m g(z^{-1}, y) \text{ mit } m = \deg_{z^{-1}}(g)$$

und wenden hierauf das Newton-Puiseux Verfahren an.

3) Das Newton-Puiseux Verfahren liefert die Entwicklungen der Nullstellen $\rho_1, \dots, \rho_n$ an $P_1, \dots, P_s$. Um die Nullstellen richtig zu numerieren, d.h. eine Reihenentwicklung einer Stelle zuzuordnen, beachten wir folgendes:

Ist τ die Reihenentwicklung einer der Nullstellen, so können wir sofort den Verzweigungsindex $e(\tau)$ der Stelle $Q \in \{P_1, \dots, P_s\}$ ablesen, an der τ entwickelt wurde. Existiert genau eine Stelle $Q \in \{P_1, \dots, P_s\}$ mit diesem Verzweigungsindex, so ordnen wir τ der Stelle Q zu.

Existieren nun $k \in \{2, \dots, s\}, 1 \le i_1 < \dots < i_k \le s$ und Stellen $P_{i_1}, \dots, P_{i_k}$ mit $e_{i_j} = e(\tau), 1 \le j \le k$, so lesen wir an der Reihenentwicklung von τ die Bewertung $v(\tau)$ ab, welche τ an der Stelle besitzt, an welcher es entwickelt wurde. Wir berechnen $v_{i_j}(\rho), 1 \le j \le k$, und existiert genau ein j mit $v_{i_j}(\rho) = v(\tau)$, so ordnen wir τ der Stelle P_{i_j} zu.

Andernfalls existieren also $k' \in \{2, \dots, s\}, 1 \le i'_1 < \dots < i'_{k'} \le s$ mit

$$v_{i'_j}(\rho) = v(\tau) \text{ und } e_{i'_j} = e(\tau), \quad 1 \le j \le k'.$$

Nach dem (schwachen) Approximationssatz (siehe z.B. [St, I.3.1.]*) existiert nun $\alpha = \sum_{i=1}^{n} \lambda_i \rho^{i-1} \in F$, so daß $v_{i_j}(\alpha)$ paarweise verschieden sind für $1 \le j \le k'$. Wir bestimmen ein solches α (randomisiert), berechnen $e(\sum_{i=1}^{n} \lambda_i \tau^{i-1})$ und ordnen τ der eindeutigen Stelle P_j zu, für die $v_{i_j}(\alpha) = e(\sum_{i=1}^{n} \lambda_i \tau^{i-1})$ gilt.*

4) Wie auch bei Nullstellenberechnungen in $\mathbb{C}$ können Präzisionsprobleme auftreten. Als guter Kompromiß hat sich beim Newton-Puiseux Verfahren eine Iterationstiefe von 25 Schritten und eine globale Präzision von 50 Stellen für alle Reihenoperationen bewährt.

5) Im Fall $p \mid e$ besitzen die Nullstellen von f auch Reihenentwicklungen, welche mit dem Newton-Puiseux Verfahren erhalten werden können.

Diese Entwicklungen sind aber nicht mehr vom Puiseux-Typ, sondern allgemeiner *vom Hamburger-Noether-Typ. D.h., besitzt ρ die Darstellung*

$$\rho = \sum_{i=m}^{\infty} a_i x^{-n_i/d_i}, \quad m \in \mathbb{Z}, n_i \in \mathbb{Z}, d_i \in \mathbb{N}, \ \text{mit } \mathrm{ggT}(n_i, d_i) = 1,$$

so sind die d_i's unbeschränkt; damit existiert kein $k \in \mathbb{N}$, so daß $\rho \in \overline{\mathbb{F}}_q\langle x^{-1/k}\rangle$, und ρ ist nicht in eine Puiseuxreihe entwickelbar.

Die Erklärung dieses Phänomens und eine allgemeine Einführung in Hamburger-Noether-Entwicklungen können in [Ca, Ch. II] *nachgelesen werden. Eine detailierte (algorithmische) Betrachtungsweise gibt* [R], *und auch in* [Gr] *wird das obige Phänomen beobachtet. Ein einfaches Beispiel, daß Nullstellen nicht Puiseux-entwickelbar sind, gibt* [Ch, Ch. IV, §6].

6) Sind wir nicht am Erweiterungstypus $F/\mathbb{F}_q(x)$, sondern an $F/\mathbb{F}_q$ interessiert, so können wir mittels einer geeigneten rationalen Transformation $x \mapsto \widetilde{x}$ die Stelle P_∞ mit einer Stelle $P \in \mathbb{P}(\mathbb{F}_q(x))$ vom Grad 1 vertauschen.

Existiert also eine Stelle $P \in \mathbb{P}(\mathbb{F}_q(x))$ mit $\deg(P) = 1$, welche zahm verzweigt ist, so können wir P und P_∞ vertauschen. Betrachten wir nun $F/\mathbb{F}_q(\widetilde{x})$ anstelle von $F/\mathbb{F}_q(x)$, so ist besitzt jetzt $P_\infty \in \mathbb{P}(\mathbb{F}_q(\widetilde{x}))$ das Verzweigungsverhalten von P, d.h., es ist zahm verzweigt.

Korrespondiert das Polynom $x - a \in \mathbb{F}_q[x]$ zu P, so führt $x \mapsto \widetilde{x} := 1/(x-a)$ zu folgender Transformation des definierenden Polynoms $f \mapsto \widetilde{f}$:

$$\widetilde{f}(\widetilde{x}, y) := \widetilde{x}^m f(1/\widetilde{x} + a, y) \in \mathbb{F}_q[\widetilde{x}, y] \ \text{mit } m = \deg_x f,$$

wobei wir den Faktor $\widetilde{x}^m$ zum Annullieren von Nennern dazunehmen. Damit erhalten wir für $\widetilde{\rho} \in \overline{\mathbb{F}_q(\widetilde{x})}$ mit $\widetilde{f}(\widetilde{x}, \widetilde{\rho}) = 0$:

$$F \cong \widetilde{F} := \mathbb{F}_q(\widetilde{x}, \widetilde{\rho}),$$

und der Körperisomorphismus ist $\mathbb{F}_q$-linear.

Nach diesen Bemerkungen greifen wir erneut unser Beispiel auf.

Beispiel III.7. *Für* Beispiel I.25 *gilt $e = 2 \nmid p = 5$, und wir können die Nullstellen $(\rho_1, \rho_2, \rho_3) = (\rho_{1,1}, \rho_{2,1}, \rho_{2,2})$ an P_1 und P_2 in Puiseuxreihen entwickeln. Es folgt $\rho_1, \rho_2, \rho_3 \in \mathbb{F}_{5^2}\langle z\rangle$ mit $z := x^{-1/2}$, und wir erhalten*

$$\begin{aligned}
\rho_1 &= z^{-6} + z^{-4} + 3z^{-2} + 3 + 2z^4 + 4z^8 + z^{12} + z^{16} + \dots, \\
\rho_2 &= w^{15}z^3 + 4z^4 + w^{15}z^5 + w^{15}z^7 + 3z^8 + w^{15}z^9 + \dots, \\
\rho_3 &= w^3z^3 + 4z^4 + w^3z^5 + w^3z^7 + 3z^8 + w^3z^9 + \dots,
\end{aligned}$$

wobei $\langle w\rangle = \mathbb{F}_{5^2}^*$ ein primitives Element mit Minimalpolynom $w^2 + 4w + 2 = 0$ ist.

2. Der Reduktionsalgorithmus

Ausgehend von Theorem III.5 werden wir nun den Algorithmus von W. M. Schmidt geeignet modifizieren. Da wir hierzu die Puiseuxentwicklungen aller Nullstellen benötigen, gelte bis zum Ende dieses Kapitels:

$p \nmid e$, d.h., P_∞ sei zahm verzweigt, und die Nullstellen

$$(\rho_1, \dots, \rho_n)^t = (\rho_{1,1}, \dots, \rho_{s,n_s})^t \in (\mathbb{F}_{q^d}\langle x^{-1/e}\rangle)^n =: (E\langle x^{-1/e}\rangle)^n =: L^n$$

seien gemäß Theorem III.5 angeordnet. Ferner bezeichne $D = \sum_{i=1}^{s} c_i P_i \in \mathrm{Div}_\infty(F)$ einen beliebigen Divisor.

Um den Begriff einer D-reduzierten Ganzheitsbasis einzuführen, beginnen wir mit der Definition dreier Abbildungen, die den Zusammenhang zur Gittertheorie aus Kapitel II herstellen:

Definition III.8. *Wir definieren eine Einbettung, eine Transformation und eine Projektion:*

$$\overline{\cdot} : F \to L^n : \alpha = \sum_{j=1}^{n} \lambda_j \rho^{j-1} \mapsto \overline{\alpha} := \big(\sum_{j=1}^{n} \lambda_j \rho_i^{j-1}\big)_{1 \le i \le n},$$

$$\cdot^D : L^n \to L^n : \beta = \big(\sum_{j=m_i}^{\infty} a_{i,j} x^{-j/e}\big)_{1\le i\le n} \mapsto \beta^D := \begin{pmatrix} \big(\sum_{j=m_i+c_1 e/e_1}^{\infty} a_{i,j} x^{-j/e}\big)_{1\le i\le n_1} \\ \vdots \\ \big(\sum_{j=m_i+c_s e/e_s}^{\infty} a_{i,j} x^{-j/e}\big)_{n-n_s+1\le i\le n} \end{pmatrix},$$

$$\theta_k : L^n \to E^n : \beta = \big(\sum_{j=m_i}^{\infty} a_{i,j} x^{-j/e}\big)_{1\le i\le n} \mapsto (a_{i,k})_{1\le i\le n}, \text{ for } k \in \mathbb{Z}.$$

Wir erinnern an die Abbildungen $v, |\cdot|, V$ und $\|\cdot\|$ aus Definition II.1 (mit $k := e$) und schließen zunächst eine Bemerkung an.

Bemerkung III.9. *1) Die Abbildung $\cdot^D$ läßt sich durch*

$$T := \mathrm{Diag}(t_1, \dots, t_n) \in L^{n\times n} \textit{ mit}$$
$$t_1 := x^{-c_1/e_1}, \dots, t_{n_1} := x^{-c_1/e_1}, \dots, t_{n-n_s+1} := x^{-c_s/e_s}, \dots, t_n := x^{-c_s/e_s}$$

darstellen und entspricht einer Gittertransformation mit

$$v(\det(\cdot^D)) = \sum_{i=1}^{s} n_i c_i e/e_i = e\sum_{i=1}^{s} f_i c_i.$$

Für alle $\alpha \in F, \beta \in L^n, \lambda \in L$ gelten $(\lambda\overline{\alpha})^D = \lambda\overline{\alpha}^D$ und $(\lambda\beta)^D = \lambda\beta^D$.

2) Für $\beta = (\beta_1, \dots, \beta_n)^t \in L^n$ gilt:

$$V(\beta) = \min_{i=1}^{n} v(\beta_i) = \min\{k \in \mathbb{Z} \mid \theta_k(\beta) \neq 0\}.$$

Um o_F mit einem geeigneten $\mathbb{F}_q[x]$-Gitter identifizieren zu können, benötigen wir noch den folgenden

SATZ III.10. *Für*

$$M := (\overline{1}, \overline{\rho}, \dots, \overline{\rho}^{n-1}) = \begin{pmatrix} 1 & \rho_1 & \cdots & \rho_1^{n-1} \\ \vdots & \vdots & & \vdots \\ 1 & \rho_n & \cdots & \rho_n^{n-1} \end{pmatrix}$$

gilt $M \in \mathrm{GL}(n, L)$.

Beweis: Nach Theorem III.5 gilt $M \in L^{n\times n}$. Die Aussage $M \in \mathrm{GL}(n, L)$ beweist man analog der entsprechenden Aussage in Theorem II.18. □

Aus diesem Satz erhalten wir sofort

THEOREM III.11. *Sei P_∞ zahm verzweigt, $R := \mathbb{F}_q[x]$ und $\omega_1, \dots, \omega_n \in o_F$ eine Ganzheitsbasis. Dann gilt*

$$M' := (\overline{\omega}_1, \dots, \overline{\omega}_n) \in \mathrm{GL}(n, L),$$

und o_F läßt sich mittels $\bar{\cdot}$ mit dem R-Gitter $\Lambda := \Lambda(M', R)$ identifizieren, d.h.

$$\overline{o_F} = \bigoplus_{i=1}^{n} R\overline{\omega}_i = \Lambda \subset L^n.$$

Beweis: Bezeichnet $M \in \mathrm{GL}(n, L)$ die Matrix aus Satz III.10, so gilt

$$M' = d_0^{-1} M T_0 \text{ mit } d_0 \in \mathbb{F}_q[x]^\times \text{ und } T_0 \in \mathrm{GL}(n, \mathbb{F}_q[x]).$$

Dies impliziert $M' \in \mathrm{GL}(n, L)$. □

BEMERKUNG III.12. *Somit haben wir im Fall, daß P_∞ zahm verzweigt ist, ein Analogon zur Minkowskiabbildung (siehe* [PZ, S. 383]*) gefunden. Betrachten wir noch einmal den Beweis von* Theorem II.18, *so entspricht dies einer speziellen Basiswahl $b_{i,1}, \dots, b_{i,n_i}$, $1 \le i \le s$.*

Mit diesen Vorarbeiten können wir nun den Begriff einer D-reduzierten Ganzheitsbasis einführen:

Definition III.13. *Eine Ganzheitsbasis $\omega_1, \dots, \omega_n \in o_F$ heißt D-reduziert, falls für alle $j \in \{0, \dots, e-1\}$ die folgende Menge $\mathbb{F}_q$-linear unabhängig ist (definitionsgemäß sei $\emptyset$ linear unabhängig):*

$$\{\theta_{V(\overline{\omega}_i^D)}(\overline{\omega}_i^D) \in E^n \mid i \in \{1, \dots, n\} \text{ mit } V(\overline{\omega}_i^D) \equiv j \mod e\}.$$

Bevor wir die Existenz einer D-reduzierten Ganzheitsbasis beweisen, bestimmen wir mit ihrer Hilfe eine $\mathbb{F}_q$-Basis von $\mathcal{L}(D, t)$. Dazu beweisen wir zwei Sätze (vgl. [Sch2]), von denen der erste auch die Motivation für obige Definition erklärt:

Satz III.14. *Sei $\omega_1, \dots, \omega_n \in o_F$ eine D-reduzierte Ganzheitsbasis. Dann gilt für $\alpha = \sum_{i=1}^n \lambda_i \omega_i \in o_F$, $\lambda_i \in \mathbb{F}_q[x], 1 \le i \le n$:*

$$V(\overline{\alpha}^D) = \min_{i=1}^n \{V(\lambda_i \overline{\omega}_i^D)\} = \min_{i=1}^n \{v(\lambda_i) + V(\overline{\omega}_i^D)\} = \min_{i=1}^n \{ev_\infty(\lambda_i) + V(\overline{\omega}_i^D)\}$$

Beweis: Die beiden rechten Identitäten sowie die Aussage für $\alpha = 0$ sind klar.

Sei also $\alpha \neq 0$ und setze

$$m := \min_{i=1}^n \{V(\lambda_i \overline{\omega}_i^D)\} \neq \infty \text{ sowie } I := \{i \in \{1, \dots, n\} \mid m = V(\lambda_i \overline{\omega}_i^D)\} \neq \emptyset.$$

Bezeichnet $\gamma_i \in \mathbb{F}_q$ den Leitkoeffizienten von $\lambda_i, i \in I$, so gelten

$$\begin{aligned}
\overline{\alpha}^D &= \theta_m(\overline{\alpha}^D) x^{-m/e} + \theta_{m+1}(\overline{\alpha}^D) x^{-(m+1)/e} + \dots \text{ und} \\
\theta_m(\overline{\alpha}^D) &= \theta_m \left(\overline{\sum_{i=1}^n \lambda_i \omega_i}^D \right) = \theta_m \left(\sum_{i=1}^n \lambda_i \overline{\omega}_i^D \right) \\
&= \sum_{i \in I} \gamma_i \theta_{V(\overline{\omega}_i^D)}(\overline{\omega}_i^D)) =: \gamma \in E^n,
\end{aligned}$$

wobei „…“ für Summanden in höheren $x^{-1/e}$-Potenzen steht.

Um $\gamma \neq 0$ zu zeigen, beachten wir, daß wegen $v(\lambda_i) = ev_\infty(\lambda_i) \equiv 0 \mod e$ die Elemente $\overline{\omega}_i^D$ für $i \in I$ der gleichen Restklasse modulo e angehören. Da nun $\omega_1, \dots, \omega_n$ eine D-reduzierte Ganzheitsbasis ist, ist $\{\theta_{V(\overline{\omega}_i^D)}(\overline{\omega}_i^D) \in E^n | i \in I\}$ $\mathbb{F}_q$-linear unabhängig. Damit folgen $\gamma \neq 0$ und die Behauptung. □

Um eine $\mathbb{F}_q$-Basis von $\mathcal{L}(D, t)$ angeben zu können, benötigen wir noch den folgenden

Satz III.15. *Seien $\alpha \in F$ und $\overline{\alpha} = (\overline{\alpha}_1, \dots, \overline{\alpha}_n)^t = (\overline{\alpha}_{1,1}, \dots, \overline{\alpha}_{s,n_s})^t \in L^n$. Dann gilt*

$$V(\overline{\alpha}) = \min_{i=1}^n v(\overline{\alpha}_i) = \min_{i=1}^s \min_{j=1}^{n_i} v(\overline{\alpha}_{i,j}) = e \min_{i=1}^s v_i(\alpha)/e_i = -eB^*(\alpha),$$

und es folgt (mit $d = [E : \mathbb{F}_q]$)

$$B(\cdot) = q^{B^*(\cdot)} = q^{-V(\bar{\cdot})/e} = \|\bar{\cdot}\|^{1/de}.$$

Beweis: Wir beachten die Anordnung der ρ_i's und erhalten

$$\widehat{F}_i \cong \widehat{F}_{i,j} := \mathbb{F}_q\langle x^{-1}\rangle(\rho_{i,j}), \quad 1 \le i \le s, 1 \le j \le n_i.$$

Bezeichnen wir mit ι_i ($\iota_{i,j}$) die Einbettungen von $F \hookrightarrow \widehat{F}_i$ ($F \hookrightarrow \widehat{F}_{i,j}$), so gilt für $\alpha \in F$

$$v_i(\alpha) = v_i(\iota_i\alpha) = v_i(\iota_{i,j}\alpha) = v_i(\overline{\alpha}_{i,j}), \quad 1 \le i \le s, 1 \le j \le n_i,$$

wobei v_i auf $\widehat{F}_i$ bzw. $\widehat{F}_{i,j}$ fortgesetzt zu verstehen ist. Zusammen mit $1 = v(x^{-1/e}) = v_i(x^{-1/e})e_i/e$ folgt die dritte Identität, was mit der Definition von B^* (vgl. Definition und Satz II.15) die erste Gleichungskette impliziert.

Die Aussage über $\|\bar{\cdot}\|$ folgt direkt aus Definition II.1. $\square$

Bemerkung III.16. *Beachten wir* Bemerkung II.7 *und die zweite Gleichungskette in* Satz III.15*, so läßt sich B auf L^n im zahm verzweigten Fall genau dann durch eine Matrix realisieren (d.h., es existiert ein $M \in \mathrm{GL}(n, L)$ mit $B(\cdot) = \|M \cdot\|$), wenn $1 = [E : \mathbb{F}_q] = e_1 = \ldots = e_s$ gilt.*

Damit erhalten wir

Satz III.17. *Sei $\omega_1, \ldots, \omega_n \in o_F$ ein D-reduzierte Ganzheitsbasis mit $V(\overline{\omega}_i^D)/e =: t_i \in \mathbb{Q}, 1 \le i \le n$. Dann gilt (mit $\deg(0) = -\infty$)*

$$\mathcal{L}(D, t) = \left\{ \sum_{i=1}^{n} \lambda_i\omega_i \mid \lambda_i \in \mathbb{F}_q[x] \ \textit{mit} \ \deg(\lambda_i) \le t_i + t, \quad 1 \le i \le n \right\}$$

für alle $t \in \mathbb{R}$.

Beweis: Wir fixieren $t \in \mathbb{R}$ und beachten für alle $\alpha = \sum_{i=1}^n \lambda_i\omega_i \in o_F, \lambda_i \in \mathbb{F}_q[x], 1 \le i \le n$ den vorhergehenden Satz, die Definition von $\cdot^D$ und die folgenden Äquivalenzen:

$$\begin{aligned}
\alpha \in \mathcal{L}(D, t) &\iff v_i(\alpha) \ge -c_i - te_i, \quad 1 \le i \le s \\
&\iff ev_i(\alpha)/e_i \ge -c_ie/e_i - te, \quad 1 \le i \le s \\
&\iff V(\overline{\alpha}^D) \ge -te \\
&\iff \min_{i=1}^{n}\{V(\lambda_i\overline{\omega}_i^D)\} = \min_{i=1}^{n}\{ev_\infty(\lambda_i) + V(\overline{\omega}_i^D)\} \ge -te \\
&\iff \min_{i=1}^{n}\{-e\deg(\lambda_i) + et_i\} \ge -te \\
&\iff \min_{i=1}^{n}\{-\deg(\lambda_i) + t_i\} \ge -t
\end{aligned}$$

$$\iff \quad \deg(\lambda_i) \leq t_i + t, \quad 1 \leq i \leq n.$$

Da $t \in \mathbb{R}$ beliebig war, folgt die Behauptung. $\square$

Als Dimensionsaussage notieren wir:

FOLGERUNG III.18. *Seien $t \in \mathbb{R}$ und $t_i, 1 \leq i \leq n$ wie im Satz zuvor. Dann gilt mit $l = [\widetilde{\mathbb{F}}_q : \mathbb{F}_q]$:*

$$\dim_{\mathbb{F}_q} \mathcal{L}(D,t) = \sum_{i=1}^{n} \max\{0, 1 + \lfloor t_i + t \rfloor\},$$

und trivialerweise $l \dim_{\widetilde{\mathbb{F}}_q} \mathcal{L}(D,t) = \dim_{\mathbb{F}_q} \mathcal{L}(D,t)$.

Als Vorbereitung auf den Beweis der Existenz D-reduzierter Ganzheitsbasen benötigen wir noch die folgende Aussage:

DEFINITION UND SATZ III.19. *Wir setzen*

$$\Omega := \{(\omega_1, \ldots, \omega_n)^t \in o_F^n \mid \omega_1, \ldots, \omega_n \textit{ ist eine Ganzheitsbasis } \}$$

und definieren die Abbildung

$$\Psi : \Omega \longrightarrow \mathbb{Z} : (\omega_1, \ldots, \omega_n)^t \longmapsto v(\det((\overline{\omega}_1^D, \ldots, \overline{\omega}_n^D))) - \sum_{i=1}^{n} V(\overline{\omega}_i^D).$$

Dann gilt $\Psi(\Omega) \subset \mathbb{N}_0$, und $\Psi(\omega) = 0$ für ein $\omega := (\omega_1, \ldots, \omega_n)^t \in \Omega$ impliziert die D-Reduziertheit von $\omega_1, \ldots, \omega_n$.

Beweis: Zunächst implizieren Theorem III.11 und Bemerkung III.9.(1) die Existenz von $k \in \mathbb{Z}$ mit $v(\det(\overline{\omega}_1^D, \ldots, \overline{\omega}_n^D)) = k$ für alle $(\omega_1, \ldots, \omega_n)^t \in \Omega$, d.h., der erste Summand von Ψ ist unabhängig vom Argument.

Wir fixieren nun $\omega = (\omega_1, \ldots, \omega_n)^t \in \Omega$ und setzen $(\phi_{i,j}) := (\phi_1, \ldots, \phi_n) := (\overline{\omega}_1^D, \ldots, \overline{\omega}_n^D) \in \mathrm{GL}(n, L)$. Wegen

$$\begin{aligned} v(\det((\phi_1, \ldots, \phi_n))) &= v\left(\sum_{\sigma \in S_n} \mathrm{sign}(\sigma)\phi_{1,\sigma(1)} \cdot \ldots \cdot \phi_{n,\sigma(n)}\right) \\ &\geq \min_{\sigma \in S_n} v(\phi_{1,\sigma(1)} \cdot \ldots \cdot \phi_{n,\sigma(n)}) \\ &= \min_{\sigma \in S_n} \sum_{i=1}^{n} v(\phi_{i,\sigma(i)}) \\ &\geq \sum_{i=1}^{n} \min_{j=1}^{n} v(\phi_{i,j}) = \sum_{i=1}^{n} V(\phi_i), \end{aligned}$$

folgt schließlich $\Psi(\Omega) \subset \mathbb{N}_0$.

Gelte nun $\Psi(\omega) = 0$. Wir beachten

(4) $\det((\phi_1, \ldots, \phi_n)) = \det\Big((\theta_{V(\phi_1)}(\phi_1), \ldots, \theta_{V(\phi_n)}(\phi_n))\Big)\, x^{-\sum_{i=1}^n V(\phi_i)/e} + \ldots,$

wobei „...“ wieder für Summanden in höheren $x^{-1/e}$-Potenzen steht. Wegen $\Psi(\omega) = 0$ folgt

$$v\left(\det((\phi_1, \ldots, \phi_n))\right) = \sum_{i=1}^{n} V(\phi_i),$$

was mit (4) $\det\Big((\theta_{V(\phi_1)}(\phi_1), \ldots, \theta_{V(\phi_n)}(\phi_n))\Big) \neq 0$ impliziert. Dann ist $\{\theta_{V(\phi_i)}(\phi_i) \in E^n \mid 1 \leq i \leq n\}$ E-linear unabhängig und somit $\mathbb{F}_q$-linear unabhängig, womit die letzte Aussage folgt. □

Kommen wir nun zur Existenzaussage, wobei der nachfolgende Beweis auch direkt einen Algorithmus liefert (vgl. [Sch2]):

Satz III.20. *Sei $\omega_1, \ldots, \omega_n \in o_F$ eine Ganzheitsbasis von o_F. Dann läßt sich aus ihr eine D-reduzierte Ganzheitsbasis durch maximal $\Psi((\omega_1, \ldots, \omega_n)^t)$ Reduktionsschritte bestimmen.*

Beweis: Wir setzen $\omega = (\omega_1, \ldots, \omega_n)^t \in \Omega$ und $(\phi_{i,j}) := (\phi_1, \ldots, \phi_n) := (\overline{\omega}_1^D, \ldots, \overline{\omega}_n^D) \in \mathrm{GL}(n, L)$.

Wegen Definition und Satz III.19 genügt es zu zeigen: Ist $\Psi(\omega) > 0$, so ist entweder $\omega_1, \ldots, \omega_n$ bereits D-reduziert, oder es existiert ein $T \in \mathrm{GL}(n, \mathbb{F}_q[x])$, und für $\widetilde{\omega} := (\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n)^t := ((\omega_1, \ldots, \omega_n)T)^t$ gilt $\Psi(\widetilde{\omega}) < \Psi(\omega)$.

Sei dazu $\omega_1, \ldots, \omega_n$ nicht D-reduziert, also $\Psi(\omega) > 0$. Dann existiert $\kappa \in \{1, \ldots, e-1\}$, so daß

$$\Big\{\theta_{V(\phi_i)}(\phi_i) \in E^n \mid i \in \{1, \ldots, n\} \text{ mit } V(\phi_i) \equiv \kappa \mod e\Big\}$$

$\mathbb{F}_q$-linear abhängig ist. O.B.d.A. gelte nun $V(\phi_i) \equiv \kappa \bmod e$ genau für $i \in \{1, \ldots, k\}$ für ein geeignetes $k \in \{2, \ldots, n\}$ und ferner $V(\phi_1) \leq \ldots \leq V(\phi_k)$. Dann existieren $j \in \{1, \ldots, k-1\}$ und $\alpha_{j+1}, \ldots, \alpha_k \in \mathbb{F}_q$ mit

$$\theta_{V(\phi_j)}(\phi_j) + \sum_{i=j+1}^{k} \alpha_i \theta_{V(\phi_i)}(\phi_i) = 0.$$

Wir beachten $(V(\phi_i) - V(\phi_j))/e \in \mathbb{N}_0$ für $i \in \{j+1, \ldots, k\}$ und setzen

$$\begin{aligned} \widetilde{\omega}_j &:= \omega_j + \sum_{i=j+1}^{k} \alpha_i x^{(V(\phi_i)-V(\phi_j))/e} \omega_i \text{ und} \\ \widetilde{\omega}_i &:= \omega_i \text{ für } i \neq j. \end{aligned}$$

Wir definieren $T \in \mathbb{F}_q[x]^{n\times n}$ durch $(\widetilde{\omega}_1, \dots, \widetilde{\omega}_n) =: (\omega_1, \dots, \omega_n)T$ und bemerken, daß T eine untere Dreiecksmatrix mit Einsen auf der Diagonalen ist. Damit ist $T \in \mathrm{GL}(n, \mathbb{F}_q[x])$. Wegen $V(\overline{\widetilde{\omega}_j}^D) > V(\overline{\omega}_j^D)$ folgt mit dem Beweis zu Definition und Satz III.19 schließlich $\Psi((\widetilde{\omega}_1, \dots, \widetilde{\omega}_n)^t) < \Psi((\omega_1, \dots, \omega_n)^t)$.

Aufgrund der obigen Konstruktion ist die Aussage über die Anzahl der Reduktionsschritte offensichtlich. □

Wie wir dem Beweis des vorhergehenden Satzes entnehmen, terminiert der folgende Algorithmus:

Algorithmus III.21. (D-Reduktion einer Ganzheitsbasis)
Eingabe: $(\phi_1, \dots, \phi_n) := (\overline{\omega}_1^D, \dots, \overline{\omega}_n^D) \in \mathrm{GL}(n, L)$, *wobei* $(\omega_1, \dots, \omega_n)^t \in \Omega$.
Ausgabe: $T \in \mathrm{GL}(n, \mathbb{F}_q[x])$, *so daß* $(\omega_1, \dots, \omega_n)T$ *eine* D*-reduzierte Ganzheitsbasis ist.*

1: *Initialisiere* $T \leftarrow \mathrm{Id}_n(\mathbb{F}_q[x])$.
2: **Repeat**
  3: *Berechne* $T_0 \in \mathrm{GL}(n, \mathbb{F}_q[x])$ *mit* $V(\widetilde{\phi}_1) \leq \dots \leq V(\widetilde{\phi}_n)$, *wobei* $(\widetilde{\phi}_1, \dots, \widetilde{\phi}_n) := (\phi_1, \dots, \phi_n)T_0$. *Setze* $(\phi_1, \dots, \phi_n) \leftarrow (\phi_1, \dots, \phi_n)T_0, T \leftarrow TT_0$ *und* $b \leftarrow 0$.
  4: **For** $\kappa = 0, \dots, e-1$
    5: *Berechne* $k = \#\{i \in \{1, \dots, n\} \mid V(\phi_i) \equiv \kappa \mod e\}$ *und* $i_1 < \dots < i_k$ *mit* $V(\phi_{i_m}) \equiv \kappa \mod e, 1 \leq m \leq k$.
    6: **If** *(*$(k > 1)$ *und* $(\{\theta_{V(\phi_{i_m})}(\phi_{i_m}) \in E^n \mid 1 \leq m \leq k\}$ *ist* $\mathbb{F}_q$*-linear abhängig))*
      7: *(Reduktionsschritt) Es existiert* $j \in \{1, \dots, k-1\}$ *und* $(0, \dots, 0, \alpha_j, \dots, \alpha_k)^t \in \mathbb{F}_q^k, \alpha_j = 1$ *mit* $\sum_{m=j}^k \alpha_m \theta_{V(\phi_{i_m})}(\phi_{i_m}) = 0$.
      Setze $\xi \leftarrow \phi_{i_j} + \sum_{m=j+1}^k \alpha_m x^{(V(\phi_{i_m}) - V(\phi_{i_j}))/e} \phi_{i_m}$ *und berechne* $T_1 \in \mathrm{GL}(n, \mathbb{F}_q[x])$ *mit* $(\phi_1, \dots, \phi_{i_j - 1}, \xi, \phi_{i_j+1}, \dots, \phi_n) = (\phi_1, \dots, \phi_n)T_1$.
      Setze $\phi_{i_j} \leftarrow \xi, T \leftarrow TT_1$ *und* $b \leftarrow 1$.
    8: **end-If**
  9: **end-For**
10: **until** *(*$b = 0$*)*
11: *Gebe* T *aus und terminiere.*

Bemerkung III.22. *Zur Betrachtung der algebraischen Komplexität des obigen Algorithmus definieren wir (zweckmäßigerweise) eine arithmetische Operation in* $\mathbb{Z}, \mathbb{F}_q, \mathbb{F}_q[x], E$ *und* L *bzw. das Berechnen von* $v(\alpha)$ *für* $\alpha \in L$ *als eine (algebraische) Operation. (Ansonsten müssen wir noch implementations-spezifische Details, z.B. von endlichen Körpern oder Reihen, berücksichtigen.)*

Wir beachten, daß für ein $\beta = (\beta_1, \dots, \beta_n)^t \in L^n$ *der Wert* $V(\beta) = \min_{i=1}^n v(\beta_i)$ *mit* n *Operationen berechnet werden kann. Damit ist die Anzahl der Operationen* *bei einem Durchlauf der Repeat-Schleife (Schritte 3–9) offensichtlich polynomiell in n.*

Weiter haben wir gezeigt, daß die Anzahl der Durchläufe der Repeat-Schleife durch $\Psi((\omega_1, \dots, \omega_n)^t) \in \mathbb{N}_0$ beschränkt ist.

Bezeichnet $T \in \mathrm{GL}(n, L)$ die zu $\cdot^D$ gehörige Matrix (vgl. Satz III.10*), so gilt mit* Bemerkung III.9.*(1)*

$$\begin{aligned}\Psi((\omega_1, \dots, \omega_n)^t) &= v(\det(T(\overline{\omega}_1, \dots, \overline{\omega}_n))) - \sum_{i=1}^{n} V(\overline{\omega}_i^D) \\ &= e\sum_{i=1}^{s} f_i c_i + v(\det(\overline{\omega}_1, \dots, \overline{\omega}_n)) - e\sum_{i=1}^{n} \min_{j=1}^{s}(v_j(\omega_i) + c_j)/e_j.\end{aligned}$$

Wir beachten, daß $v(\det(\overline{\omega}_1, \dots, \overline{\omega}_n))$ unabhängig von der Wahl der Ganzheitsbasis ist ($\det(\overline{\omega}_1, \dots, \overline{\omega}_n)^2$ entspricht der Körperdiskriminante im Zahlkörperfall).

Damit hängt $\Psi((\omega_1, \dots, \omega_n)^t)$ von Invarianten der Körpererweiterung $F/\mathbb{F}_q(x)$ (genauer: von $v(\det(\overline{\omega}_1, \dots, \overline{\omega}_n))$ und dem Zerlegungsverhalten von P_∞) sowie von c_i und $v_i(\omega_j), 1 \le i \le s, 1 \le j \le n$, ab.

Wir kommen zurück auf unser Beispiel.

Beispiel III.23. *Es gelten $o_F = \mathbb{F}_5[x, \rho]$ und*

$$B^*(1) = 0, \quad B^*(\rho) = 3, \quad B^*(\rho^2) = 6.$$

Für eine 0-reduzierte Ganzheitsbasis ($D := 0 \in \mathrm{Div}(F)$)

$$\widetilde{\omega}_1 = 1, \quad \widetilde{\omega}_2 := (2x^3 + 2x^2 + x + 1)\rho + 3\rho^2, \quad \widetilde{\omega}_3 := (4x^3 + 4x^2 + 2x)\rho + \rho^2$$

erhalten wir dagegen

$$B^*(\widetilde{\omega}_1) = 0, \quad B^*(\widetilde{\omega}_2) = 3/2, \quad B^*(\widetilde{\omega}_3) = 3.$$

Damit ist die Basis erheblich „kürzer“ geworden (bzgl. B).

3. 0-reduzierte Ganzheitsbasen

In diesem Abschnitt werden wir Aussagen für D-reduzierte Ganzheitsbasen beweisen, wenn $D = 0 \in \mathrm{Div}_\infty(F)$. Diese werden u.a. bei der Einheitenberechnung noch wichtig werden.

In Theorem II.18 hatten wir die Existenz einer Ganzheitsbasis gezeigt, welche die sukzessiven Minima von o_F bzgl. der Längenfunktion B realisiert. Ist P_∞ zahm verzweigt, so läßt sich eine solche Ganzheitsbasis leicht berechnen, wie wir nun zeigen.

THEOREM III.24. *Sei $\omega_1, \ldots, \omega_n \in o_F$ eine 0-reduzierte Ganzheitsbasis mit $B(\omega_1) \leq \ldots \leq B(\omega_n)$. Dann realisiert diese die sukzessiven Minima von o_F bzgl. der Längenfunktion B.*

Beweis: Angenommen, es existieren $k \in \{1, \ldots, n\}$ und $\mathbb{F}_q[x]$-linear unabhängige $b_1, \ldots, b_k \in o_F$ mit

$$B(b_i) \leq B(b_k) =: q^t < B(\omega_k), \quad 1 \leq i < k.$$

Wir beachten nun für $i \in \{1, \ldots, k\}$:

$$B^*(b_i) \leq t \Leftrightarrow -\min_{j=1}^{s} v_j(b_i)/e_i \leq t \Leftrightarrow v_j(b_i) \geq -te_j, \quad 1 \leq j \leq s.$$

Dies impliziert $b_1, \ldots, b_k \in \mathcal{L}(0, t)$.
Da nach Satz III.15 aber $V(\bar{\cdot})/e = -B^*(\cdot)$ gilt, folgt mit Satz III.17: $\mathcal{L}(0,t) \subset [\omega_1, \ldots, \omega_{k-1}]_{\mathbb{F}_q[x]}$. Damit können aber

$$b_1, \ldots, b_k \in \mathcal{L}(0,t) \subset [\omega_1, \ldots, \omega_{k-1}]_{\mathbb{F}_q[x]}$$

nicht $\mathbb{F}_q[x]$-linear unabhängig sein, und wir erhalten den gewünschten Widerspruch. □

BEMERKUNG III.25. *Im Fall, daß P_∞ zahm verzweigt ist, können wir also eine Ganzheitsbasis effizient berechnen, welche die sukzessiven Minima von o_F bzgl. B realisiert. In diesem Sinne ist der o.g. Reduktionsalgorithmus der LLL-Reduktion (angewendet auf eine in den $\mathbb{R}^n$ eingebettete Basis einer Ordnung eines Zahlkörpers) überlegen.*

Der nächste Satz liefert ein Hilfsmittel, um Elemente beschränkter Norm zu konstruieren. Dies wird im nachfolgenden noch von Bedeutung sein.

SATZ III.26. *Sei $t \in \mathbb{R}$. Dann gilt*

$$\deg(\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha)) \leq tn \textit{ für alle } \alpha \in \mathcal{L}(0,t).$$

Beweis: Zunächst gilt für alle $\alpha \in \mathcal{L}(0,t)$:

$$-v_i(\alpha) \leq te_i, \quad 1 \leq i \leq s.$$

Bezeichnet $L := \mathbb{F}_q\langle x^{-1}\rangle$, so folgt die Behauptung aus

$$\begin{aligned}\deg(\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha)) &= -v_\infty(\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha)) = -v_\infty\Big(\prod_{i=1}^{s} \mathrm{N}_{\widehat{F}_i/L}(\alpha)\Big) \\ &= -\sum_{i=1}^{s} v_\infty(\mathrm{N}_{\widehat{F}_i/L}(\alpha)) = -\sum_{i=1}^{s} f_i v_i(\alpha)\end{aligned}$$

$$\leq \sum_{i=1}^{s} f_i t e_i = tn.$$

□

Schließlich bestimmen wir den exakten Konstantenkörper, d.h. $l \in \mathbb{N}$ mit $l = [\widetilde{\mathbb{F}}_q : \mathbb{F}_q]$, wobei der nachfolgende Satz auch ein weiterer Beweis für Satz II.20.(3) ist:

Satz III.27. *Sei $\omega_1, \ldots, \omega_n \in o_F$ eine 0-reduzierte Ganzheitsbasis mit $B(\omega_1) \leq \ldots \leq B(\omega_n)$. Dann gilt*

$$\begin{aligned} l &= \dim_{\mathbb{F}_q} \mathcal{L}(0,0) \text{ und } 1 = B(\omega_1) = \ldots = B(\omega_l) < B(\omega_{l+1}), \text{ d.h.} \\ l &= \max\{i \in \{1, \ldots, n\} \mid B(\omega_i) = 1\}. \end{aligned}$$

Beweis: Wir beachten die sich aus der Produktformel ergebenden Äquivalenzen

$$\begin{aligned} \alpha \in \widetilde{\mathbb{F}}_q^\times &\Leftrightarrow v_P(\alpha) = 0 \text{ für alle } P \in \mathbb{P}(F) \\ &\Leftrightarrow \alpha \in o_F \text{ und } v_i(\alpha) = 0, \quad 1 \leq i \leq s \\ &\Leftrightarrow \alpha \in \{\beta \in o_F^\times \mid v_i(\beta) \geq 0, 1 \leq i \leq s\} \\ &\Leftrightarrow \alpha \in \mathcal{L}(0,0)^\times. \end{aligned}$$

Wegen Satz III.17 und Satz III.15 gilt nun

$$\mathcal{L}(0,0) = \left\{ \sum_{i=1}^{n} \lambda_i \omega_i \mid \lambda_i \in \mathbb{F}_q[x], \deg(\lambda_i) \leq -B^*(\omega_i), 1 \leq i \leq n \right\}.$$

Aus Satz II.20.(3) erhalten wir $0 = B^*(\omega_1) \leq \ldots \leq B^*(\omega_n)$, was

$$\begin{aligned} \mathcal{L}(0,0) &= \left\{ \sum_{i=1}^{l} \lambda_i \omega_i \mid \lambda_i \in \mathbb{F}_q, 1 \leq i \leq l \right\} \text{ mit} \\ l &:= \max\{i \in \{1, \ldots, n\} \mid B(\omega_i) = q^{B^*(\omega_i)} = 1\}. \end{aligned}$$

impliziert. □

Beispiel III.28. *Kommen wir zurück zu* Beispiel III.23. *Mit dem oben gezeigten sind $1, \sqrt{125}, 125$ die sukzessiven Minima von o_F bzgl. B. Außerdem gilt $l = 1$, d.h. $\widetilde{\mathbb{F}}_5 \cong \mathbb{F}_5$.*

Damit beschließen wir das Kapitel über Ganzheitsbasenreduktion und wenden uns der Einheitenberechnung zu.

KAPITEL IV

Einheitenberechnung

Ziel dieses Kapitels ist die Berechnung der Einheitengruppe $U_F := o_F^*$, wobei die Ergebnisse des letzten Kapitels wesentlich zum Tragen kommen werden. Die Struktur dieser Gruppe wird durch den Dirichletschen Einheitensatz (siehe z.B. [We, 5-3-10]) vollständig beschrieben:

Definition und Satz IV.1. *Die Einheitengruppe U_F ist das direkte Produkt aus $r := s - 1$ unendlichen zyklischen Gruppen und der endlichen zyklischen Gruppe TU_F aller in F enthaltenen Einheitswurzeln, d.h., es existieren $\zeta, \varepsilon_1, \ldots, \varepsilon_r \in o_F, TU_F = \langle\zeta\rangle$ mit*

$$U_F = TU_F \times \langle\varepsilon_1\rangle \times \ldots \times \langle\varepsilon_r\rangle.$$

Die Gruppe TU_F heißt Gruppe der Torsionseinheiten, r Einheitenrang, und die Elemente $\varepsilon_1, \ldots, \varepsilon_r$ Grundeinheiten.

Als bewertungstheoretische Charakterisierung erhalten wir aus der Produktformel sofort:

Satz IV.2. *Für $\alpha \in o_F$ gelten*

$$\begin{aligned} \alpha \in U_F \quad &\Leftrightarrow \quad v_P(\alpha) = 0 \text{ für alle } P \in \mathbb{P}_0(F) \\ &\Leftrightarrow \quad \sum_{i=1}^{s} f_i v_i(\alpha) = 0 \text{ und } v_P(\alpha) \geq 0 \text{ für alle } P \in \mathbb{P}_0(F) \\ &\Leftrightarrow \quad \sum_{i=1}^{s} f_i v_i(\alpha) = 0, \end{aligned}$$

sowie

$$\begin{aligned} \alpha \in TU_F \quad &\Leftrightarrow \quad v_P(\alpha) = 0 \text{ für alle } P \in \mathbb{P}(F) \\ &\Leftrightarrow \quad v_P(\alpha) \geq 0 \text{ für alle } P \in \mathbb{P}(F) \end{aligned}$$

$$\begin{aligned} &\Leftrightarrow \quad \alpha \in U_F \textit{ und } v_i(\alpha) = 0, 1 \le i \le s \\ &\Leftrightarrow \quad \alpha \in (o_F \cap o_{F,\infty})^\times = (\cap_{P \in \mathbb{P}(F)} \mathcal{O}_P)^\times \\ &\Leftrightarrow \quad \alpha \in \widetilde{\mathbb{F}}_q^\times \cong \mathbb{F}_{q^l}^\times . \end{aligned}$$

Insgesamt gilt also: $U_F \cong \mathbb{F}_{q^l}^\times \times \mathbb{Z}^r$.

Wie auch im Zahlkörperfall erleichert die Betrachtung der Einheitengruppe als Gitter im Logarithmenraum ihre Berechnung. Daher definieren wir:

Definition IV.3. *Wir bezeichnen mit*

$$L^\infty : F^\times \longrightarrow \mathbb{Z}^r : \alpha \longmapsto (v_1(\alpha), \dots, v_r(\alpha))^t$$

die Logarithmenabbildung.

Für eine Teilmenge $M \subset U_F$ ist $L^\infty(\langle M \rangle)$ ein Gitter in $\mathbb{Z}^r$, und offensichtlich gilt

$$L^\infty(TU_F) = \{0\}.$$

Wir führen nun den Begriff des Regulators ein.

Definition IV.4. *Für* $k \in \mathbb{N}$ *heißen* $\eta_1, \dots, \eta_k \in U_F$ *unabhängig, falls die Vektoren* $L^\infty(\eta_1), \dots, L^\infty(\eta_k) \in \mathbb{Z}^r$ $\mathbb{Z}$*-linear unabhängig sind. Andernfalls heißen* $\eta_1, \dots, \eta_k$ *abhängig.*

Für eine Untergruppe $U := \langle \eta_1, \dots, \eta_r \rangle < U_F$ *definieren wir den Regulator*

$$\begin{aligned} \mathrm{Reg}(U) &:= \left| \det \begin{pmatrix} f_1 v_1(\eta_1) & \cdots & f_1 v_1(\eta_r) \\ \vdots & & \vdots \\ f_r v_r(\eta_1) & \cdots & f_r v_r(\eta_r) \end{pmatrix} \right| \\ &= \left| \det(L^\infty(\eta_1), \dots, L^\infty(\eta_r)) \right| \prod_{i=1}^r f_i \in \mathbb{N}_0 . \end{aligned}$$

Damit gilt offensichtlich der

Satz IV.5. *Für eine Untergruppe* $U := \langle \eta_1, \dots, \eta_r \rangle < U_F$ *sind äquivalent*

$$\eta_1, \dots, \eta_r \in U_F \textit{ sind unabhängig } \Leftrightarrow [U_F : U] < \infty \Leftrightarrow \mathrm{Reg}(U) \neq 0.$$

Bemerkung IV.6. *Die Definition von Logarithmenabbildung und Regulator über die Bewertungen* $v_1, \dots, v_r$ *ist insofern willkürlich, als daß hier nicht notwendig* v_s*, sondern irgendeine der Bewertungen* $v_1, \dots, v_s$ *ausgelassen werden kann und ferner die Reihenfolge der Bewertungen keine Rolle spielt.*

Dazu beachten wir, daß wegen $\sum_{i=1}^s f_i v_i(\alpha) = 0$ *für alle* $\alpha \in U_F$ *die Menge*

$$H := \{(v_1(\alpha), \dots, v_s(\alpha))^t \in \mathbb{Z}^s \mid \alpha \in U_F\}$$

eine Hyperebene in $\mathbb{Z}^s$ ist. Um also die multiplikative Struktur von U_F auf eine additive (Gitter-) Struktur zurückführen zu können, betrachten wir $H \cap \mathbb{Z}^r$. Wie wir leicht nachprüfen, sind der Begriff der Unabhängigkeit von Einheiten und des Regulators unabhängig davon, welche der Bewertungen $v_1, \dots, v_s$ wir auslassen.

Nach diesen Vorbereitungen beginnen wir mit der Berechnung von TU_F.

1. Torsionseinheiten

In diesem Abschnitt berechnen wir $l = [\widetilde{\mathbb{F}}_q : \mathbb{F}_q]$. Darüber hinaus skizzieren wir ein allgemeines Verfahren, um die Elemente von $\mathcal{L}(D,t)$ zu bestimmen. Wir beginnen mit grundlegender Theorie (vgl. [Ha, S. 350ff]).

Satz IV.7. *Für $l = [\widetilde{\mathbb{F}}_q : \mathbb{F}_q]$ gelten*

$$l \mid n, \quad l \mid \deg(P) \text{ für alle } P \in \mathbb{P}(F),$$
$$l = \min\{\deg(P) \mid P \in \mathbb{P}(F)\} \text{ und } l = \operatorname{ggT}\{\deg(P) \mid P \in \mathbb{P}(F)\}.$$

Damit folgt sofort: Existiert ein $P \in \mathbb{P}(F)$ mit $\deg(P) = 1$, so gilt $l = 1$.

Wir erinnern an unsere Resultate aus den vorhergehenden Kapiteln (Satz II.20, Theorem III.24 und Satz III.27):

Seien $M_i := M_i(o_F, \mathbb{F}_q[x], B), 1 \le i \le n$. Dann gelten

$$\widetilde{\mathbb{F}}_q^\times = TU_F = \mathcal{L}(0,0)^\times \text{ und}$$
$$l = \dim_{\mathbb{F}_q} \mathcal{L}(0,0) = \max\{i \in \{1, \dots, n\} \mid M_i = 1\}.$$

Ist P_∞ zahm verzweigt, so läßt sich l mittels einer 0-reduzierten Ganzheitsbasis berechnen.

Die Bedingung der Zahmverzweigtheit an P_∞ kann für die Berechnung von l abgeschwächt werden. Dazu beachten wir das folgende triviale

Lemma IV.8. *Seien $\tilde{x}$ transzendent über $\mathbb{F}_q, \tilde{\rho} \in \overline{\mathbb{F}_q(\tilde{x})}$ und*

$$\phi : F \longrightarrow \widetilde{F} := \mathbb{F}_q(\tilde{x}, \tilde{\rho})$$

ein $\mathbb{F}_q$-linearer Körperisomorphismus. Dann gilt

$$\widetilde{\mathbb{F}}_q \cong \{\alpha \in \widetilde{F} \mid \alpha \text{ ist algebraisch über } \mathbb{F}_q\}.$$

Erinnern wir uns nun an Bemerkung III.6.(6), so können wir l dann explizit berechnen, wenn eine zahm verzweigte Stelle $P \in \mathbb{P}(\mathbb{F}_q(x))$ mit $\deg(P) = 1$ existiert. Dazu transformieren wir $x \mapsto \tilde{x}$, und wir berechnen l mittels einer 0-reduzierten Ganzheitsbasis von $o_{\widetilde{F}}$, wo $\widetilde{F} := \mathbb{F}_q(\tilde{x}, \tilde{\rho})$ (vgl. Bemerkung III.6.(6)).

Ist keine Stelle zahm verzweigt, so können wir l aus der Elementzahl von $\mathcal{L}(0,0) \cong \mathbb{F}_{q^l}$ bestimmen. Wie schon zu Beginn des letzten Kapitels angekündigt, skizzieren wir nun einen allgemeinen Algorithmus, um $\mathcal{L}(D,t)$ für $D = \sum_{i=1}^s c_i P_i \in \mathrm{Div}_\infty(F)$, und $t \in \mathbb{R}$ zu bestimmen.

Dazu betrachten wir zunächst

$$\begin{aligned}
\mathcal{L}(D,t) &= \{\alpha \in o_F \mid v_i(\alpha) \geq -c_i - te_i, 1 \leq i \leq s\} \\
&= \{\alpha \in o_F \mid v_i(\alpha) \geq -\lceil c_i + te_i \rceil =: -\widetilde{c}_i, 1 \leq i \leq s\} \\
&= \{\alpha \in o_F \mid \alpha \in \prod_{i=1}^s P_i^{-\widetilde{c}_i}\}.
\end{aligned}$$

Fixieren wir nun Ganzheitsbasen $\omega_1, \ldots, \omega_n \in o_F$ und $\widetilde{\omega}_1, \ldots, \widetilde{\omega}_n \in o_{F,\infty}$, so erhalten wir reguläre Matrizen $M_0 \in \mathbb{F}_q[x]^{n\times n}, M_1 \in \mathcal{O}_\infty^{n\times n}$ und $d_0 \in \mathbb{F}_q[x], d_1 \in \mathcal{O}_\infty$ mit

$$\begin{aligned}
o_F &= \left\{(1,\rho,\ldots,\rho^{n-1})\frac{1}{d_0}M_0\lambda \mid \lambda \in \mathbb{F}_q[x]^n\right\} \text{ und} \\
\prod_{i=1}^s P^{-\widetilde{c}_i} &= \left\{(1,\rho_\infty,\ldots,\rho_\infty^{n-1})\frac{1}{d_1}M_1\nu \mid \nu \in \mathcal{O}_\infty^n\right\}.
\end{aligned}$$

Damit existiert eine invertierbare Diagonalmatrix $D_1 \in \mathbb{F}_q(x)^{n\times n}$, so daß

$$\begin{aligned}
\mathcal{L}(D,t) &= \left\{(1,\rho,\ldots,\rho^{n-1})\frac{1}{d_0}M_0\lambda \mid \lambda \in \mathbb{F}_q[x]^n\right\} \\
&\quad \cap \left\{(1,\rho,\ldots,\rho^{n-1})\frac{1}{d_1}D_1M_1\nu \mid \nu \in \mathcal{O}_\infty^n\right\}.
\end{aligned}$$

Mittels der Hermite-Normalformen $H_0 := M_0U_0 := \mathrm{HNF}(M_0)$ und $H_1 := M_1U_1 := \mathrm{HNF}(M_1)$ mit $U_0 \in \mathrm{GL}(n,\mathbb{F}_q[x]), U_1 \in \mathrm{GL}(n,\mathcal{O}_\infty)$ lassen sich somit alle Elemente von $\mathcal{L}(D,t)$ aus den Lösungen des Gleichungssystems

$$\frac{1}{d_0}H_0\lambda = \frac{1}{d_1}D_1H_1\nu \text{ mit } \lambda \in \mathbb{F}_q[x]^n, \nu \in \mathcal{O}_\infty^n,$$

gewinnen, wobei die Lösungen mit U_0^{-1} bzw. U_1^{-1} zurücktransformiert werden müssen.

Setzen wir noch $D_2 := \frac{d_0}{d_1}D_1$, so erhalten wir schließlich alle Lösungen aus dem Gleichungssystem

$$H_0\lambda = D_2H_1\nu \text{ mit } \lambda \in \mathbb{F}_q[x]^n, \nu \in \mathcal{O}_\infty^n,$$

welches wir rekursiv lösen können.

Bemerkung IV.9. *1) Mit dem oben beschriebenen Verfahren sind wir in der Lage, $\mathcal{L}(D,t)$ zu bestimmen. Da der rekursive Lösungsansatz allerdings das Testen von potentiellen Lösungen λ, ν verlangt, ist dieses Verfahren nicht besonders effizient.*

2) Da häufig nicht nur l, sondern die Gruppe U_F vollständig berechnet werden soll, bietet sich folgende Strategie an: Um unabhängige Einheiten zu berechnen, wird im dritten Abschnitt die sog. Relationenmethode beschrieben, bei der eine große Anzahl von $P \in \mathbb{P}(F)$ berechnet werden. Somit ist es ratsam, die Berechnung dieser Stellen abzuwarten, da die Existenz einer Stelle vom Grad 1 hinreichend für $l = 1$ ist (siehe Satz IV.7*).*

Nachdem wir nun TU_F berechnet haben, bereiten wir die Konstruktion unabhängiger Einheiten vor. Hierbei kommt Elementen beschränkter Norm eine zentrale Bedeutung zu.

2. Elemente beschränkter Norm

In diesem Abschnitt werden wir untersuchen, wie wir Elemente beschränkter Norm konstruieren können, d.h.

$$\alpha \in o_F \text{ mit } \deg(\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha)) \le \delta$$

für ein beliebiges $\delta \ge 0$. Solche Elemente werden wir für die Konstruktion unabhängiger Einheiten im nächsten Abschnitt benötigen.

Ist P_∞ zahm verzweigt, so hatten wir bereits in Satz III.26 gezeigt, wie solche Elemente zu erhalten sind:

Für $t \in \mathbb{R}$ gilt

$$\deg(\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha)) \le tn \text{ für alle } \alpha \in \mathcal{L}(0,t).$$

Im Fall, daß P_∞ wild verzweigt ist, beschreiben wir ein Verfahren, das auf der für Zahlkörper bekannten Parallelotopmethode ([PZ, S. 351]) beruht.

Dazu erinnern wir zunächst an die Geometrie der Zahlen für $d = k = 1$ (vgl. Kapitel II), d.h., wir setzen $L := \mathbb{F}_q\langle x^{-1}\rangle, R := \mathbb{F}_q[x]$ und betrachten in L^n das Fundamental-Parallelotop

$$C_1 := C(\mathrm{Id}_n) = \{\beta = (\beta_1, \dots, \beta_n)^t \in L^n \mid \|\beta\| = \max_{i=1}^{n} |\beta_i|_\infty \le 1\}$$

sowie das R-Gitter $\Lambda := R^n$.

Wir fixieren nun eine Ganzheitsbasis $\omega_1, \dots, \omega_n \in o_F$ und setzen

$$\Theta : \mathbb{F}_q(x)^n \longrightarrow F : (\alpha_1, \dots, \alpha_n) \longmapsto \sum_{i=1}^{n} \alpha_i \omega_i.$$

Dann ist Θ ein $\mathbb{F}_q(x)$-Vektorraumisomorphismus mit $\Theta(\Lambda) = o_F$.

Im folgenden werden wir für $\alpha \in o_F^\times$ das Parallelotop C_1 zu Parallelotopen $C_\alpha^\pm$ transformieren und die Elemente $\Theta(C_\alpha^\pm \cap \Lambda) \subset o_F$ betrachten.

Informationen über die Normen der Elemente in $\Theta(C_\alpha^\pm \cap \Lambda)$ gibt der nachfolgende

Satz IV.10. *Seien* $\alpha \in o_F^\times$, M_α *die Darstellungsmatrix von* α *bzgl.* $\omega_1, \dots, \omega_n$ *und* $\deg(\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha)) = kn + m$ *mit* $k \in \mathbb{N}_0, 0 \le m < n$. *Setzen wir* $c_\alpha^+ := x^{-k}, c_\alpha^- := x^{-k-1}$ *und*

$$\begin{aligned}
M_\alpha^\pm &:= c_\alpha^\pm M_\alpha \in \mathbb{F}_q(x)^{n\times n},\\
C_\alpha^\pm &:= M_\alpha^\pm C_1 := \{M_\alpha^\pm \beta \mid \beta \in C_1\} = C((M_\alpha^\pm)^{-1}) \subset L^n,\\
\Gamma_\alpha^\pm &:= \Theta(C_\alpha^\pm \cap \Lambda) \subset o_F\\
c_1 &:= \sup_{\beta \in C_1 \cap \mathbb{F}_q(x)^n} |\mathrm{N}_{F/\mathbb{F}_q(x)}(\Theta(\beta))|_\infty,
\end{aligned}$$

so gelten

(1) $\sup_{\gamma\in\Gamma_\alpha^\pm} |\mathrm{N}_{F/\mathbb{F}_q(x)}(\gamma)|_\infty \le c_1 |\det(M_\alpha^\pm)|_\infty$,
(2) $|\det(M_\alpha^+)|_\infty = q^m \ge 1$ *und* $|\det(M_\alpha^-)|_\infty = q^{m-n} < 1$,
(3) $1 \le \#(\Gamma_\alpha^+ \setminus \{0\}) < \infty, 0 \le \#(\Gamma_\alpha^- \setminus \{0\}) < \infty$ *und*
(4) $c_1 \le \max_{i=1}^n B(\omega_i)^{sn}$.

Beweis: Um (1) zu zeigen, beachten wir $M_\alpha^\pm \in \mathbb{F}_q(x)^{n\times n}$ und

$$\begin{aligned}
\sup_{\gamma\in\Gamma_\alpha^\pm} |\mathrm{N}_{F/\mathbb{F}_q(x)}(\gamma)|_\infty &= \sup_{\gamma\in\Theta(M_\alpha^\pm C_1 \cap R^n)} |\mathrm{N}_{F/\mathbb{F}_q(x)}(\gamma)|_\infty\\
&\le \sup_{\gamma\in\Theta(M_\alpha^\pm C_1 \cap \mathbb{F}_q(x)^n)} |\mathrm{N}_{F/\mathbb{F}_q(x)}(\gamma)|_\infty\\
&= \sup_{\gamma\in c_\alpha^\pm \alpha\Theta(C_1 \cap \mathbb{F}_q(x)^n)} |\mathrm{N}_{F/\mathbb{F}_q(x)}(\gamma)|_\infty\\
&= c_1 |\mathrm{N}_{F/\mathbb{F}_q(x)}(c_\alpha^\pm \alpha)|_\infty\\
&= c_1 |\det(M_\alpha^\pm)|_\infty.
\end{aligned}$$

Die zweite Aussage folgt sofort aus der Definition von $|\cdot|_\infty$.

Für (3) beachten wir $\#(\Gamma_\alpha^\pm \setminus \{0\}) = \#(M_\alpha^\pm C_1 \cap \Lambda^\times)$ und $M_\alpha^\pm C_1 = C((M_\alpha^\pm)^{-1})$. Um den Minkowskischen Gitterpunktsatz anzuwenden, definieren wir eine Längenfunktion $G(\cdot) := \|(M_\alpha^+)^{-1} \cdot \|$ auf L^n, und es gilt $M_\alpha^+ C_1 = C(G)$. Nach Satz II.14 folgt nun

$$(M_1(\Lambda, R, G))^n \le \prod_{i=1}^n M_i(\Lambda, R, G) = \mathrm{Vol}(C(G))^{-1} = |\det((M_\alpha^+)^{-1})|_\infty.$$

Dies impliziert die Existenz von $\gamma \in \Lambda^\times$ mit

$$G(\gamma) \le |\det((M_\alpha^+)^{-1})|_\infty \le 1$$

und somit

$$\gamma \in (C(G) \cap \Lambda)^\times = (M_\alpha^+ C_1 \cap \Lambda)^\times.$$

Die Endlichkeitsaussage für $\#\Gamma_\alpha^\pm$ folgt aus der Beschränktheit dieser Mengen in L^n mit der von $\|\cdot\|$ induzierten Topologie und der Diskretheit von R^n.

Für die letzte Aussage beachten wir $\max_{i=1}^s |\alpha|_i \geq 1$ für alle $\alpha \in o_F^\times$ (vgl. Definition und Satz II.15) und setzen $\Gamma := C_1 \cap \mathbb{F}_q(x)^n$. Dann folgt die Behauptung aus

$$\begin{aligned}
c_1 &= \sup_{\beta\in\Gamma} |\mathrm{N}_{F/\mathbb{F}_q(x)}(\Theta(\beta))|_\infty = \sup_{\beta\in\Gamma} \prod_{i=1}^s |\mathrm{N}_{\widehat{F}_i/L}(\Theta(\beta))|_\infty \\
&= \sup_{\beta\in\Gamma} \prod_{i=1}^s |\Theta(\beta)|_i^{f_i} = \sup_{\beta\in\Gamma} \prod_{i=1}^s |\sum_{j=1}^n \beta_j\omega_j|_i^{f_i} \\
&\leq \sup_{\beta\in\Gamma} \prod_{i=1}^s (\max_{j=1}^n \ |\beta_j\omega_j|_i)^{f_i} = \sup_{\beta\in\Gamma} \prod_{i=1}^s (\max_{j=1}^n |\beta_j|_\infty^{e_i} |\omega_j|_i)^{f_i} \\
&\leq \prod_{i=1}^s (\max_{j=1}^n |\omega_j|_i)^{f_i} \leq \max_{i=1}^s (\max_{j=1}^n |\omega_j|_i^{f_i})^s \\
&= \max_{i=1}^s \max_{j=1}^n |\omega_j|_i^{sn_i/e_i} \leq \max_{i=1}^s \max_{j=1}^n |\omega_j|_i^{sn/e_i} \\
&= \max_{j=1}^n B(\omega_j)^{sn}.
\end{aligned}$$

□

Bemerkung IV.11. *1) Die Bestimmung der Elemente von* $\Gamma_\alpha^\pm$ *kann analog zum Zahlkörperfall erfolgen (vgl.* [PZ, S. 351f]*).*

2) Der Minkowskische Gitterpunktsatz garantiert nur für Γ_α^+ *die Existenz eines nichttrivialen Elements. In vielen Fällen enthält aber auch schon* Γ_α^- *hinreichend viele Elemente, so daß wir bei Berechnungen zunächst mit* Γ_α^- *starten.*

3) Offensichtlich sollte c_1 *so klein wie möglich sein. Wegen* Satz IV.10.*(4) wäre daher eine Ganzheitsbasis optimal, welche die sukzessiven Minima von* o_F *bzgl.* B *realisiert. Ist* P_∞ *wild verzweigt, so bieten sich zur Reduktion einer Ganzheitsbasis bzgl.* B *z.B. Methoden aus der kombinatorischen Optimierung an, welche hier aber nicht diskutiert werden.*

Nachdem wir nunmehr in der Lage sind, Elemente beschränkter Norm zu berechnen, wenden wir uns jetzt der Konstruktion unabhängiger Einheiten zu.

3. Berechnung unabhängiger Einheiten

In diesem Abschnitt werden wir für $r' \in \{1, \dots, r\}$ unabhängige Einheiten $\eta_1, \dots, \eta_{r'} \in U_F$ konstruieren, indem wir ein Teilgitter

$$\Lambda' \subset \Lambda := L^\infty(U_F) \subset \mathbb{Z}^r$$

vom Rang r' bestimmen (vgl. Satz IV.5). Dies erfolgt mit dem aus Zahlkörpern bekannten Relationenverfahren (siehe [PZ, 6.5], welches wir im folgenden kurz erläutern.

Wir fixieren zunächst eine Faktorbasis, d.h. für $m \in \mathbb{N}$ paarweise verschiedene Stellen $Q_1, \dots, Q_m \in \mathbb{P}_0(\mathbb{F}_q(x))$ mit normierten Primelementen $\pi_1, \dots, \pi_m \in \mathbb{F}_q[x]$ und berechnen mittels Hauptdivisorzerlegung jeweils alle $s_i \in \mathbb{N}$ paarweise verschiedenen Stellen

$$Q'_{i,j} \mid Q_i, 1 \leq i \leq m, 1 \leq j \leq s_i.$$

Weiter beachten wir für $\alpha \in o_F^\times$ und $Q \in \mathbb{P}_0(\mathbb{F}_q(x))$ mit Primelement $\pi_Q \in \mathbb{F}_q[x]$

$$\pi_Q \nmid \mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha) \Longrightarrow v_{Q'}(\alpha) = 0 \text{ für alle } Q' \mid Q.$$

Wir sagen, daß $\alpha \in o_F^\times$ über der Faktorbasis zerfällt, wenn für jedes normierte Primpolynom $\pi \in \mathbb{F}_q[x]$ gilt

$$\pi \mid \mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha) \Longrightarrow \pi \in \{\pi_1, \dots, \pi_m\}.$$

Schließlich definieren wir für $\kappa = \sum_{i=1}^m s_i \in \mathbb{N}$

$$L^0 : F^\times \longrightarrow \mathbb{Z}^\kappa : \alpha \longmapsto (v_{Q'_{1,1}}(\alpha), \dots, v_{Q'_{1,s_1}}(\alpha), v_{Q'_{2,1}}(\alpha), \dots, v_{Q'_{m,s_m}}(\alpha))^t.$$

Mit diesen Vorbereitungen können wir das Relationenverfahren formulieren:

Induktiv bilden wir für über der Faktorbasis zerfallende $\alpha_i \in o_F^\times, i = 1, 2, \dots$ die Relationenmatrizen

$$R_i := (L^\infty(\alpha_1), \dots, L^\infty(\alpha_i)) \in \mathbb{Z}^{r \times i} \text{ und } R'_i := (L^0(\alpha_1), \dots, L^0(\alpha_i)) \in \mathbb{Z}^{\kappa \times i}.$$

Nun gilt

$$\prod_{j=1}^{i} \alpha_j^{\nu_j} \in U_F \Longleftrightarrow \nu = (\nu_1, \dots, \nu_i)^t \in \mathrm{Ker}(R'_i),$$

und wir bestimmen eine Basis

$$\nu_{i,1}, \dots, \nu_{i,k_i} \in \mathbb{Z}^i \text{ von } \mathrm{Ker}(R'_i) \text{ für geeignetes } k_i \in \mathbb{N}.$$

Wir wählen solange über der Faktorbasis zerfallende Elemente $\alpha_i \in o_F^\times$, bis

$$\mathrm{Rg}(R_{i'}(\nu_{i',1}, \dots, \nu_{i',k_{i'}})) = r' \text{ für ein } i' \in \mathbb{N}.$$

Dies impliziert

$$
\begin{aligned}
U &:= \left\{ \prod_{j=1}^{i} \alpha_j^{\nu_j} \in U_F \mid \nu = (\nu_1, \dots, \nu_i) \in \operatorname{Ker}(R_i') \right\} \\
&= \{\alpha \in U_F \mid L^\infty(\alpha) \in \Lambda'\}, \text{ wobei} \\
\Lambda' &:= \{H\nu := \operatorname{HNF}(R_i(\nu_{i,1}, \dots, \nu_{i,k_i}))\nu \mid \nu \in \mathbb{Z}^r\}. \qquad (5)
\end{aligned}
$$

Mit $L^\infty(TU_F) = \{0\}$ gilt daher

$$L^\infty(U) = \Lambda' = \{H\nu \mid \nu \in \mathbb{Z}^r\} \cong U/(TU_F \cap U).$$

Offensichtlich sind bei diesem Verfahren die beiden folgenden Parameter von entscheidender Bedeutung, um i' so klein wie möglich zu halten:

(1) Der Aufbau der Faktorbasis, d.h. die Wahl von m und den $Q_1, \dots, Q_m$,
(2) Die Auswahl der über der Faktorbasis zerfallenden Elemente $\alpha_1, \dots, \alpha_{i'}$.

Der restliche Abschnitt dient der Diskussion verschiedener Strategien für (1) und (2). Dazu benötigen wir noch die folgende

Definition IV.12. *Wir setzen für $m \in \mathbb{N}$*

$$
\begin{aligned}
W_m &:= \{\alpha \in o_F \mid \deg(\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha)) \le m\}, \\
A_m &:= \#\{g \in \mathbb{F}_q[x] \mid g \textit{ normiert, irreduzibel mit } \deg(g) = m\}
\end{aligned}
$$

und definieren die Möbiussche μ-Funktion

$$\mu : \mathbb{N} \to \{-1, 0, 1\} : k \mapsto \begin{cases} 1 & k = 1, \\ 0 & k \textit{ ist nicht quadratfrei}, \\ (-1)^i & k \textit{ ist das Produkt } i \textit{ verschiedener Primzahlen.} \end{cases}$$

Von wesentlicher Bedeutung sind die beiden folgenden Aussagen (siehe [PZ, Ch. 5, (2.3) und Ch. 2, (5.15)]):

Lemma IV.13. *Für alle $m \in \mathbb{N}$ enthält die Menge W_m nur endlich viele nicht-assoziierte Elemente.*

Theorem IV.14. *Für $m \in \mathbb{N}$ gelten*

$$q^m = \sum_{d|m} dA_d, \quad A_m = \frac{1}{m} \sum_{d|m} \mu(d) q^{m/d}, \quad A_m \ge 1 \textit{ und } A_m \sim q^m/m \textit{ für } q \to \infty.$$

Somit wächst die Anzahl der Primpolynome vom Grad m aus $\mathbb{F}_q[x]$ exponentiell in m. Dies legt es nahe, bei Elementen möglichst kleiner Norm zu testen, ob sie über einer Faktorbasis mit kleinen $\deg(\pi_1), \dots, \deg(\pi_m)$ zerfallen.

Darauf aufbauend hat sich bei Berechnungen folgendes Vorgehen als günstig erwiesen:

Wir geben uns $m, b, b' \in \mathbb{N}$ vor und starten mit einer leeren Faktorbasis. Für $\alpha \in W_b$ berechnen wir

$$\mathrm{N}_{F/\mathbb{F}_q(x)}(\alpha) = \prod_{j=1}^{k} \widetilde{\pi}_i^{\kappa_j} \text{ mit Primpolynomen } \widetilde{\pi}_j, \kappa_j \in \mathbb{N}, 1 \leq j \leq k.$$

Gilt $\deg(\widetilde{\pi}_j) \leq b', 1 \leq j \leq k$, so ist α ein neues α_i, wir nehmen die Stellen $\widetilde{\pi}_1 \mathcal{O}_{\widetilde{\pi}_1}, \dots, \widetilde{\pi}_k \mathcal{O}_{\widetilde{\pi}_k}$ in die Faktorbasis auf und berechnen alle $Q|\widetilde{\pi}_i \mathcal{O}_{\widetilde{\pi}_i}, 1 \leq i \leq k$. Andernfalls wählen wir ein nächstes $\alpha \in W_b$. Wir beenden den Aufbau der Faktorbasis, wenn die Anzahl der Primstellen erstmals mindestens m beträgt. Ist dies nach Elementen $\alpha_1, \dots, \alpha_{k'}$ der Fall, so berechnen wir jetzt die Relationenmatrizen $R_{k'}$ und $R'_{k'}$.

Anschließend wählen wir $\alpha \in W_b$ und testen, ob diese über der Faktorbasis zerfallen. Immer, wenn α über der Faktorbasis zerfällt, tragen wir $L^\infty(\alpha)$ und $L^0(\alpha)$ in die entsprechenden Relationenmatrizen ein (d.h., wir hängen Spalten an). Haben wir i' erreicht, so erhalten wir die Matrix H aus (5) als Ergebnis und terminieren.

In der nachfolgenden Bemerkung erläutern wir noch einige Strategien.

Bemerkung IV.15. *1) Um sich zu überlegen, daß das Verfahren bei hinreichend großer Wahl der Schranken terminiert, beachten wir*

$$|v_i(\varepsilon_j)| \leq t := \mathrm{Reg}(U_F) / \prod_{k=1}^{s} f_i, \quad 1 \leq i, j \leq r.$$

Dies impliziert $\varepsilon_1, \dots, \varepsilon_r \in \mathcal{L}(0, t)$. Diese Menge können wir berechnen.

Allerdings ist die Wahl zufälliger Elemente und kleiner Schranken m, b, b' wesentlich für die Effizienz des Verfahrens, und die Auswahl der $\alpha \in W_b$ hängt davon ab, ob P_∞ zahm verzweigt ist oder nicht:

Ist P_∞ wild verzweigt, so berechnen wir $\alpha \in \Gamma_\beta^\pm \subset W_b$ iterativ mit dem Parallelotopverfahrens (vgl. Satz IV.10*) für zufällige, normbeschränkte $\beta \in o_F$. Im zahm verzweigten Fall wählen wir zufällig $\alpha \in \mathcal{L}(0, b/n)$ als Linearkombination einer* 0*-reduzierten Ganzheitsbasis mit zufälligen, im Grad beschränkten Polynomen (vgl.* Satz III.26*).*

2) Der oben beschriebene Aufbau der Faktorbasis stellt sicher, daß die zuerst gewählten α über der Faktorbasis zerfallen. Diese Methode ist einer willkürlichen

Wahl der Faktorbasis vorzuziehen. Wie im Zahlkörperfall lehnen wir auch solche α ab, deren Norm Indexteiler enthält (vgl. Bemerkung I.23*).*

3) Als Ergebnis des obigen Verfahrens erhalten wir nicht unabhängige Einheiten, sondern die Matrix $H = (h_1, \dots, h_{r'}) = (h_{i,j}) \in \mathbb{Z}^{r \times r'}$. Um aus H unabhängige Einheiten $\eta_1, \dots, \eta_{r'}$ mit $L^\infty(\langle \eta_1, \dots, \eta_{r'} \rangle) = \{H\nu \mid \nu \in \mathbb{Z}^{r'}\}$ zu berechnen, bestimmen wir zunächst

$$H' := (h'_1, \dots, h'_{r'}) := \begin{pmatrix} h_1 & \cdots & h_{r'} \\ -\sum_{i=1}^r f_i h_{i,1}/f_s & \cdots & -\sum_{i=1}^r f_i h_{i,r'}/f_s \end{pmatrix} \in \mathbb{Z}^{s \times r'}.$$

Danach berechnen wir mit dem im nächsten Abschnitt beschriebenen Verfahren zur Berechnung von Einheiten mit vorgegebenen Bewertungen

$$\eta_1, \dots, \eta_{r'} \in o_F \ mit\ (v_1(\eta_j), \dots, v_s(\eta))^t = h'_j, \quad 1 \le j \le r',$$

die das gewünschte leisten.

Das bei Zahlkörpern übliche Verfahren, unabhängige Einheiten direkt über das Potenzprodukt aus den Relationen auszurechnen, hat sich bei Funktionenkörpern aufgrund der Komplexität der Polynomarithmetik nicht bewährt.

4) Ist P_∞ zahm verzweigt, so bietet es sich an, sog. Dirichletelemente zu faktorisieren. In Anlehnung an die Definition von Dirichleteinheiten im Zahlkörperfall heißt $\alpha \in o_F$ Dirichletelement zur Richtung $i \in \{1, \dots, s\}$, falls

$$v_i(\alpha) < 0 \ und\ v_j(\alpha) \ge 0, j \in \{1, \dots, s\} \setminus \{i\}.$$

Dazu fixieren wir $i \in \{1, \dots, s\}$ und $m \in \mathbb{N}$. Dann impliziert die Produktformel für $j \in \{1, \dots, s\} \setminus \{i\}$

$$\begin{aligned} \alpha \in \mathcal{L}(mP_i, 0)^\times &\implies -m \le v_i(\alpha) \le 0 \ und\ v_j(\alpha) \ge 0, \ sowie \\ \alpha \in \mathcal{L}(mP_i, 0)^\times \setminus TU_F &\implies -m \le v_i(\alpha) < 0 \ und\ v_j(\alpha) \ge 0. \end{aligned}$$

Bei Berechnungen hat es sich als günstig erwiesen, zuerst Dirichletelemente zu faktorisieren (und damit die Faktorbasis aufzubauen), da hierbei häufig schon Einheiten gefunden werden.

Wir kommen nun zum letzten Schritt bei der Berechnung der Einheitengruppe.

4. Ein Wurzeltest und die Konstruktion von Grundeinheiten

In diesem Abschnitt werden wir von einer Untergruppe von endlichem Index

$$U := \langle \eta_1, \dots, \eta_r \rangle < U_F := TU_F \times \langle \varepsilon_1, \dots, \varepsilon_r \rangle$$

zu U_F aufsteigen, indem wir Grundeinheiten $\varepsilon_1, \dots, \varepsilon_r$ explizit berechnen.

Wie schon im letzten Abschnitt werden wir die Einheitengruppe hauptsächlich im Logarithmengitter betrachten. Dabei ist die Untergruppe U durch eine reguläre Matrix

$$H := (h_1, \dots, h_r) := (L^\infty(\eta_1), \dots, L^\infty(\eta_r)) \in \mathbb{Z}^{r\times r}$$

gegeben (vgl. Bemerkung IV.15.(3)). Es gilt demnach

$$L^\infty(U) = \{H\nu \mid \nu \in \mathbb{Z}^r\} \cong U/(TU_F \cap U),$$

wobei wir $L^\infty(TU_F) = \{0\}$ beachten.

Bei der Berechnung von Grundeinheiten werden neben den Besonderheiten von Gittern in $\mathbb{Z}^r$ das bereits in Bemerkung IV.15.(3) angekündigte Verfahren zur Berechnung von Einheiten mit vorgegebenen Bewertungen Verwendung finden. Das Verfahren entscheidet, ob zu $c_1, \dots, c_s \in \mathbb{Z}$ mit $\sum_{i=1}^s f_i c_i = 0$ eine Einheit $\varepsilon \in U_F$ mit

$$v_i(\varepsilon) = c_i, 1 \le i \le s,$$

existiert und berechnet diese gegebenenfalls.

Grundlage hierfür bildet der folgende

Satz IV.16. *Sei* $D = \sum_{i=1}^s c_i P_i \in \mathrm{Div}_\infty(F)$ *und* $\deg(D) = 0$. *Dann gelten*

$$\alpha \in U_F \text{ und } v_i(\alpha) = -c_i, 1 \le i \le s \Longleftrightarrow \alpha \in \mathcal{L}(D,0)^\times$$

und $\dim_{\widetilde{\mathbb{F}}_q} \mathcal{L}(D,0) \in \{0,1\}$.

Beweis: „$\Rightarrow$“: Dies gilt offensichtlich.

„$\Leftarrow$“: Sei $\alpha \in \mathcal{L}(D,0)^\times$, also

$$v_P(\alpha) \ge 0 \text{ für alle } P \in \mathbb{P}_0(F) \text{ und } v_i(\alpha) \ge -c_i, 1 \le i \le s.$$

Dann implizieren $\deg(D) = 0$ und die Produktformel sofort

$$0 \ge \sum_{i=1}^s f_i v_i(\alpha) \ge -\sum_{i=1}^s f_i c_i = 0 \text{ und damit } v_P(\alpha) = 0 \text{ für alle } P \in \mathbb{P}_0(F).$$

Für $\mathcal{L}(D,0) = \{0\}$ ist die Dimensionsaussage richtig. Im Fall $\mathcal{L}(D,0) \ne \{0\}$ fixieren wir $\alpha \in \mathcal{L}(D,0)^\times$ und zeigen

$$\mathcal{L}(D,0)^\times = \{\xi\alpha \mid \xi \in TU_F\}.$$

Sei dazu $\beta \in \mathcal{L}(D,0)^\times$. Mit dem bereits gezeigten folgen

$$\xi := \beta/\alpha \in U_F \text{ und } v_i(\xi) = 0, 1 \le i \le s.$$

Dies impliziert $\xi \in TU_F$, und wegen $TU_F = \widetilde{\mathbb{F}}_q^\times$ folgt die Behauptung. $\square$

Mit diesen Vorarbeiten ist der nachfolgende Algorithmus kanonisch.

Algorithmus IV.17. (Bestimmung einer Einheit mit vorgegebenen Bewertungen)
Eingabe: $c_1, \dots, c_s \in \mathbb{Z}$ *mit* $\sum_{i=1}^{s} f_i c_i = 0$.
Ausgabe: $\varepsilon \in U_F$ *mit* $v_i(\varepsilon) = c_i, 1 \le i \le s$, *falls diese existiert;* 0 *sonst.*

Berechne $\mathcal{L}(D, 0)$ *für* $D := -\sum_{i=1}^{s} c_i P_i$.
If *(*$\mathcal{L}(D, 0) = \{0\}$*)*
  Gebe 0 *aus und terminiere.*
else
  Gebe beliebiges $\varepsilon \in \mathcal{L}(D, 0)^\times$ *aus und terminiere.*
end-If-else

Aufbauend auf diesem Verfahren können wir nun einen Wurzeltest formulieren. Dieser entscheidet, ob zu gegebenen $\eta \in U_F, k \in \mathbb{Z}$ Einheiten $\varepsilon \in U_F, \xi \in TU_F$ mit

$$\xi \varepsilon^k = \eta$$

existieren und berechnet diese gegebenenfalls.

Algorithmus IV.18. (Wurzeltest)
Eingabe: $\eta \in U_F, k \in \mathbb{Z}$.
Ausgabe: $\varepsilon \in U_F, \xi \in TU_F$ *mit* $\xi \varepsilon^k = \eta$, *falls diese existieren;* 0 *sonst.*

Initialisiere $c_i \leftarrow v_i(\eta)/k, 1 \le i \le s$.
If *(*$(c_1, \dots, c_s) \notin \mathbb{Z}^s$*)*
  Gebe 0 *aus und terminiere.*
else
  If *(Es existiert* $\varepsilon \in U_F$ *mit* $v_i(\varepsilon) = c_i, 1 \le i \le s$*)*
    Setze $\xi \leftarrow \eta/\varepsilon^k$, *gebe* ε, ξ *aus und terminiere.*
  else
    Gebe 0 *aus und terminiere.*
  end-If-else
end-If-else

Bemerkung IV.19. *Wie schon in* Bemerkung III.2.*(2) angemerkt, korrespondiert die Berechnung von* $\mathcal{L}(D, t)$ *zum Auszählen einer gewichteten positiv definiten quadratischen Form* $T_{2,\lambda}$. *Mit der Notation aus* Bemerkung I.15 *stellt sich das Analogon des obigen Wurzeltests bei Zahlkörpern wie folgt dar (vgl.* [Wi, Lemma

4.7]*): Falls* $\varepsilon \in o_{\mathcal{F}}$ *mit* $\varepsilon^k = \eta$ *existiert, so gilt* $T_{2,\lambda}(\varepsilon) = n$*, wo*

$$T_{2,\lambda} : o_{\mathcal{F}} \to \mathbb{R}^{\geq 0} : \alpha \mapsto \sum_{i=1}^{n} \frac{1}{\lambda_i^2} |\alpha^{(i)}|^2 \text{ und } \lambda_i := |\eta^{(i)}|^{1/k}, 1 \leq i \leq n.$$

Bevor wir das Problem der Grundeinheitenberechnung allgemein angehen, beschäftigen wir uns noch mit dem Spezialfall $r = 1$.

Bemerkung IV.20. *1) Im Fall* $r = 1$ *gilt*

$$f_1 v_1(\eta) = -f_2 v_2(\eta) \text{ für alle } \eta \in U_F = TU_F \times \langle \varepsilon_1 \rangle$$

mit einer Grundeinheit ε_1 *und*

$$\mathrm{Reg}(U_F) = f_1 |v_1(\varepsilon_1)| = f_2 |v_2(\varepsilon_1)|.$$

In vielen Fällen läßt sich ε_1 *direkt bestimmen, indem wir sukzessive*

$$\mathcal{L}(mP_1 - (f_1 m/f_2)P_2, 0) \text{ für } m = 1, 2, \ldots$$

berechnen. Offensichtlich gilt $\mathcal{L}(mP_1 - (f_1 m/f_2)P_2, 0) \neq \{0\}$ *zum ersten Mal nach* $\mathrm{Reg}(U_F)/f_1$ *Schritten.*

2) Im reell-quadratischen Fall, d.h. $e_1 = e_2 = f_1 = f_2 = 1$*, läßt sich* ε_1 *auch mit dem bekannten Kettenbruchverfahren bestimmen (vgl.* [Ar1],[WZ]*).*

Kommen wir nun zum allgemeinen Fall. Analog zum Zahlkörperfall werden wir für bestimmte $\widetilde{p} \in \mathbb{P}$ induktiv die sog. $\widetilde{p}$-maximalen Obergruppen von $U/(TU_F \cap U)$ bestimmen und schließlich Grundeinheiten $\varepsilon_1, \ldots, \varepsilon_r$ konstruieren. Wir folgen der Darstellung in [Wi, Kapitel 4] und beginnen mit einer

Definition IV.21. *Seien* M *eine abelsche Gruppe und* $N < M$ *eine Untergruppe von endlichem Index. Für jedes* $\widetilde{p} \in \mathbb{P}$ *ist*

$$N_{\widetilde{p}} := \{\alpha \in M \mid \text{ es existiert } k \in \mathbb{N} \text{ mit } \alpha^{\widetilde{p}^k} \in N\}$$

eine Untergruppe von M *mit* $N < N_{\widetilde{p}} < M$*, die wir die* $\widetilde{p}$*-maximale Obergruppe von* N *in* M *nennen;* N *heißt* $\widetilde{p}$*-maximal, falls* $N = N_{\widetilde{p}}$ *gilt.*

Wir beachten nun

Lemma IV.22. *Seien* M *eine abelsche Gruppe und* $N < M$ *eine Untergruppe mit*

$$[M : N] = \prod_{i=1}^{j} p_i^{l_i}, \quad p_i \in \mathbb{P}, l_i \in \mathbb{N}, 1 \leq i \leq j \in \mathbb{N}_0.$$

Dann gilt

$$N < N_{p_1} < (N_{p_1})_{p_2} < \ldots < (\ldots(N_{p_1})_{p_2} \ldots)_{p_j} = M. \tag{6}$$

Um dieses Lemma nun auf $M := U_F/TU_F$ und $N := U/(TU_F \cap U)$ anwenden zu können, benötigen wir eine Aussage über $[U_F/TU_F : U/(TU_F \cap U)]$. Dazu beachten wir das folgende

LEMMA IV.23. *Es gelten*

$$\mathrm{Reg}(U_F) \mid \mathrm{Reg}(U) = \det(H) \prod_{i=1}^{r} f_i \text{ und } [U_F/TU_F : U/(TU_F \cap U)] \mid |\det(H)|.$$

Beweis: Wir betrachten U_F/TU_F und $U/(TU_F \cap U)$ im Logarithmenraum und setzen $H' := (L^\infty(\varepsilon_1), \ldots, L^\infty(\varepsilon_r)) \in \mathbb{Z}^{r\times r}$. Dann existiert eine reguläre Matrix $T \in \mathbb{Z}^{r\times r}$ mit $H = H'T$ und

$$\mathrm{Reg}(U) = |\det(H)| \prod_{i=1}^{r} f_i = |\det(H')||\det(T)| \prod_{i=1}^{r} f_i = \mathrm{Reg}(U_F)|\det(T)|.$$

Wegen

$$U_F/TU_F \cong \{H'\nu \mid \nu \in \mathbb{Z}^r\} \text{ und } U/(TU_F \cap U) \cong \{H\nu \mid \nu \in \mathbb{Z}^r\}$$

folgt $[U_F/TU_F : U/(TU_F \cap U)] = |\det(T)| \mid |\det(H)|$. □

Nach Lemma IV.22 und Lemma IV.23 können wir also U_F/TU_F bestimmen, wenn wir induktiv die p_i-maximalen Obergruppen von $U/(TU_F \cap U)$ für

$$\{p_1, \ldots, p_j\} = \{\widetilde{p} \in \mathbb{P} \mid \quad \widetilde{p} \mid |\det(H)|\}$$

berechnen.

BEMERKUNG IV.24. *Bei Zahlkörpern verwenden wir eine untere Regulatorabschätzung, um die Menge $\{p_1, \ldots, p_j\}$ zu bestimmen. Da wir hier Gitter in $\mathbb{Z}^r$ betrachten, erhalten wir sofort ein ganzzahliges (natürliches) Vielfaches des Regulators. Daher müssen wir nicht alle Primzahlen bis zu einer Schranke testen, sondern günstigerweise nur Primteiler.*

Im folgenden beschreiben wir exemplarisch die Berechnung von $(U/(TU_F \cap U))_{\widetilde{p}}$ für ein fixiertes $\widetilde{p} \in \{p_1, \ldots, p_j\}$; die induktive Berechnung der p_i-maximalen Obergruppen gemäß (6) ist dann kanonisch.

Bevor wir das unten beschriebene Verfahren verwenden, prüfen wir zunächst, ob einer der Erzeuger von U eine $\widetilde{p}$-te Potenz ist. Dazu beachten wir Bemerkung IV.15.(3) und testen für $i \in \{1, \ldots, r\}$ mit Algorithmus IV.17, ob $\varepsilon \in U_F$ mit

$$\widetilde{p}L^\infty(\varepsilon) = h_i$$

existiert und ersetzen gegebenenfalls H durch $\mathrm{HNF}(H, L^\infty(\varepsilon))$.

Das Verfahren wird durch das folgende Lemma gegeben (vgl. [PZ, Ch. 5, (7.1)]):

Lemma IV.25. *Die Gruppe $U/(TU_F \cap U)$ ist genau dann $\widetilde{p}$-maximal in U_F/TU_F, falls für alle $\nu = (\nu_1, \dots, \nu_r)^t \in \{0, \dots, \widetilde{p}-1\}^r$ mit $\nu_1 + \dots + \nu_r > 0$ kein $\varepsilon \in U_F$ existiert, so daß*

$$\widetilde{p}L^\infty(\varepsilon) = H\nu.$$

Beachten wir $U/(TU_F \cap U) \cong \{H\nu \mid \nu \in \mathbb{Z}^r\}$, so können wir direkt einen Algorithmus formulieren.

Algorithmus IV.26. (Bestimmung der $\widetilde{p}$-maximalen Obergruppe)
Eingabe: *Eine reguläre Matrix $H \in \mathbb{Z}^{r\times r}$ mit $U/(TU_F \cap U) \cong \{H\nu \mid \nu \in \mathbb{Z}^r\}, \widetilde{p} \in \mathbb{P}, \kappa \in \mathbb{N}$ mit $\widetilde{p}^\kappa \mid |\det(H)|$.*
Ausgabe: *Eine reguläre Matrix $\widetilde{H} \in \mathbb{Z}^{r\times r}$ mit $(U/(TU_F \cap U))_{\widetilde{p}} \cong \{\widetilde{H}\nu \mid \nu \in \mathbb{Z}^r\}$*

1: *Initialisiere $\widetilde{H} = (\widetilde{h}_1, \dots, \widetilde{h}_r) = (\widetilde{h}_{i,j}) \leftarrow H$.*
2: **Repeat**
 3: *Setze*

$$H' \leftarrow \begin{pmatrix} \widetilde{h}_1 & \cdots & \widetilde{h}_r \\ -\sum_{i=1}^r f_i \widetilde{h}_{i,1}/f_s & \cdots & -\sum_{i=1}^r f_i \widetilde{h}_{i,r}/f_s \end{pmatrix} \in \mathbb{Z}^{s\times r}.$$

 4: **For** $\nu = (\nu_1, \dots, \nu_r)^t \in \{0, \dots, \widetilde{p}-1\}^r$
  5: *Setze $(\widetilde{c}_1, \dots, \widetilde{c}_s)^t \leftarrow H'\nu$ und $c_i \leftarrow \widetilde{c}_i/\widetilde{p}, 1 \le i \le s$.*
  6: **If** *((($c_1, \dots, c_s)^t \in \mathbb{Z}^s$) und (es existiert $\varepsilon \in \mathcal{L}(-\sum_{i=1}^s c_i P_i, 0)^\times$))*
   7: *Gehe nach 11.*
  8: **end-If**
 9: **end-For**
 10: *Gebe $\widetilde{H}$ aus und terminiere.*
 11: *Setze $\widetilde{H} \leftarrow \mathrm{HNF}(\widetilde{H}, L^\infty(\varepsilon))$ und $\kappa \leftarrow \kappa - 1$.*
12: **until** *($\kappa = 0$)*
13: *Gebe $\widetilde{H}$ aus und terminiere.*

Bemerkung IV.27. *Die zweite Bedingung in Schritt 6 wird mit* Algorithmus IV.17 *getestet.*

Führen wir induktiv obiges Verfahren für $p_1, \dots, p_j$ durch, so erhalten wir eine reguläre Matrix $\widetilde{H} \in \mathbb{Z}^{r\times r}$ mit

$$U_F/TU_F \cong \{\widetilde{H}\nu \mid \nu \in \mathbb{Z}^r\}.$$

Erinnern wir uns nun an Bemerkung IV.15.(3), so sind wir in der Lage, Grundeinheiten $\varepsilon_1, \dots, \varepsilon_r$ zu berechnen.

Wir beschließen das Kapitel mit einer letzten

Bemerkung IV.28. *Bei obigem Verfahren müssen in der For-Schleife im Extremfall* $\widetilde{p}^r$ *Riemann-Rochsche Räume* $\mathcal{L}(D,0)$ *bestimmt werden.*

An dieser Stelle existiert für Zahlkörper ein effizienteres Verfahren, welches auf dem Čebotarevschen Dichtigkeitssatz basiert (vgl. [Wi, Kapitel 4] *und* [FJ, Ch. 5]*).*

Grundlage dieses Verfahrens bilden u.a. die drei folgenden Aussagen (siehe [Wi, 4.11, 4.15 und 4.16]*):*

(1) *Seien* Σ *ein Körper und* $a \in \Sigma^\times$. *Dann gilt*

$$a \text{ ist keine } \widetilde{p}\text{-te Potenz in } \Sigma \Leftrightarrow t^{\widetilde{p}} - a \in \Sigma[t] \text{ ist irreduzibel.}$$

(2) *Seien* $\mathcal{F}$ *ein Zahlkörper mit Maximalordnung* $o_{\mathcal{F}}$ *und* $a \in o_{\mathcal{F}}^\times$, *welches keine* $\widetilde{p}$*-te Potenz ist. Dann besitzt die Menge*

$$\mathbb{P}(\mathcal{F},\widetilde{p},a) := \{\mathcal{P} \text{ Primideal in } o_{\mathcal{F}} \mid t^{\widetilde{p}} - a \text{ ist irreduzibel in } o_{\mathcal{F}}/\mathcal{P}[t]\}$$

unendlich viele Elemente.

(3) *Seien* $\mathcal{F}$ *und* a *wie in (2). Dann gilt*

$$\mathcal{P} \in \mathbb{P}(\mathcal{F},\widetilde{p},a) \Rightarrow \widetilde{p} \mid b^{f_{\mathcal{P}}} - 1,$$

wo $b := \min\{\mathcal{P} \cap \mathbb{N}\} \in \mathbb{P}$ *und* $f_{\mathcal{P}}$ *den Trägheitsgrad von* $\mathcal{P}$ *über* $b\mathbb{Z}$ *bezeichnet.*

Betrachten wir nun analog für $a \in o_F^\times$, *welches keine* $\widetilde{p}$*-te Potenz ist, die Menge*

$$\mathbb{P}_0(F,\widetilde{p},a) := \{P \in \mathbb{P}_0(F) \mid t^{\widetilde{p}} - a \text{ ist irreduzibel in } o_F/P[t]\},$$

und wählen $Q \in \mathbb{P}_0(F,\widetilde{p},a), \pi \in \mathbb{F}_q[x]$ *mit* $Q \cap \mathbb{F}_q[x] =: \pi\mathbb{F}_q[x] =: P \in \mathbb{P}_0(\mathbb{F}_q(x))$, *so gilt*

$$\widetilde{p} \mid q^{f(Q|P)\deg(\pi)} - 1. \tag{7}$$

Dies impliziert sofort $\mathbb{P}_0(F,p,a) = \emptyset$, *da* $\mathrm{ggT}(p,p^k-1) = 1$ *für alle* $k \in \mathbb{N}$.

Um für $\widetilde{p} \neq p$ *ein* $Q \in \mathbb{P}(F,\widetilde{p},a)$ *explizit zu berechnen, werden für Primpolynome* $\pi \in \mathbb{F}_q[x]$ *Hauptdivisoren* (π) *zerlegt und die beteiligten Stellen getestet. Wegen* (7) *und* $f(Q|P) \leq n$ *müssen hier häufig Polynome* π *von sehr großem Grad gewählt werden. Aus diesem Grund ist das Verfahren — im Gegensatz zum Zahlkörperfall — nicht effizient.*

Das obige Phänomen erklärt sich aus der Charakteristik der Restklassenkörper $o_{\mathcal{F}}/\mathcal{P}$ *bzw.* o_F/P. *Im Zahlkörperfall können wir jede beliebige Charakteristik erzeugen, wohingegen bei Funktionenkörpern nur die Charakteristik des Konstantenkörpers möglich ist.*

Beispiel IV.29. *Kommen wir zurück auf* Beispiel III.23. *Wie in* Bemerkung IV.20.*(1) beschrieben, berechnen wir eine Grundeinheit*

$$\varepsilon_1 = (x+1)\widetilde{\omega}_1 + 4\widetilde{\omega}_2 \textit{ mit } L^\infty(\varepsilon_1) = (3).$$

Damit erhalten wir auch $\mathrm{Reg}(U_F) = 3$.

Nachdem wir nun in der Lage sind, Ganzheitsbasen zu reduzieren und Grundeinheiten zu berechnen, geben wir im abschließenden Kapitel V einige Beispiele.

KAPITEL V

Beispiele

Aufbauend auf den bisherigen theoretischen Ergebnissen, geben wir in diesem Kapitel Beispiele zur 0-Reduktion von Ganzheitsbasen und zur Berechnung von Grundeinheiten für Körper vom Grad ≥ 3, in denen P_∞ zahm verzweigt ist.

In den nachfolgenden Tabellen werden u.a. Elemente der endlichen Körper $\mathbb{F}_q$ und E dargestellt.

Dazu beachten wir: Ist $q = p$, so werden die Elemente von $\mathbb{F}_q$ durch $0, \dots, p-1$ repräsentiert. Ist $q = p^k$ mit $k > 1$, so werden die Elemente des Primkörpers $\mathbb{F}_p$ durch $0, \dots, p-1$ dargestellt; die Darstellung von $\mathbb{F}_q \setminus \mathbb{F}_p$ erfolgt als Potenz eines primitiven Elements $\langle w \rangle = \mathbb{F}_q^*$. Für w geben wir auch das Minimalpolynom über $\mathbb{F}_p$ an. Die Puiseuxentwicklungen der Nullstellen $\rho_1, \dots, \rho_n$ werden immer als Potenzen von $z := x^{-1/e}$ dargestellt, d.h. $\rho_i \in E\langle z \rangle, 1 \leq i \leq n$. Zur Darstellung der Elemente von E verwenden wir entweder ein primitives Element $\langle u \rangle = E^*$, für welches wir das Minimalpolynom über $\mathbb{F}_p$ angeben, oder die Vektorraum-Darstellung $E = \mathbb{F}_q(\xi)$ mit geeigntem $\xi \in E$.

In den Tabellen gibt T die Laufzeit in Sekunden an. Alle Beispiele wurden mit einer modifizierten KASH-Software (siehe [K]) auf IBM RS6000 Workstations mit 64 MB RAM unter AIX 3.2 gerechnet.

1. Ganzheitsbasenreduktion

In diesem Abschnitt geben wir einige Beispiele zur 0-Reduktion von Ganzheitsbasen. Genauer gesagt berechnen wir für Körpererweiterungen $F/\mathbb{F}_q(x)$, in denen P_∞ zahm verzweigt ist, eine Ganzheitsbasis $\omega_1, \dots, \omega_n \in o_F$ mit der Round-Two Methode. Diese reduzieren wir bzgl. $D = 0$ zu einer Ganzheitsbasis $\widetilde{\omega}_1, \dots, \widetilde{\omega}_n \in o_F$.

Für beide Ganzheitsbasen geben wir die B^*-Werte an, womit wir wegen $B(\cdot) = q^{B^*(\cdot)}$ und Theorem III.24 auch die sukzessiven Minima von o_F bzgl. B kennen.

Ferner bezeichnen in den folgenden Tabellen

$$\Sigma := \sum_{i=1}^{n} B^*(\omega_i), \quad \widetilde{\Sigma} := \sum_{i=1}^{n} B^*(\widetilde{\omega}_i), \quad \Delta\Sigma := \Sigma - \widetilde{\Sigma},$$
$$M := \max_{i=1}^{n} B^*(\omega_i), \quad \widetilde{M} := \max_{i=1}^{n} B^*(\widetilde{\omega}_i), \quad \Delta M := M - \widetilde{M}.$$

Der Wert $\Delta\Sigma$ gibt hierbei an, um wieviel „kürzer" die Ganzheitsbasis bzgl. B geworden ist. Beachten wir die Abschätzungen für c_1 aus Satz IV.10, so ist die Bedeutung von ΔM für die Konstruktion von Elementen beschränkter Norm offensichtlich.

Es folgen 15 Beispiele, welche nach Erweiterungsgrad n und Charakteristik des Konstantenkörpers p angeordnet sind. Sie sind so gewählt, daß an ihnen entweder eine effektive Reduktion (vgl. $\Delta\Sigma$ mit Σ und ΔM mit M) sichtbar wird oder $\widetilde{\mathbb{F}}_q \neq \mathbb{F}_q$ gilt. Die drei letzten Beispiele demonstrieren die Algorithmen an großen Erweiterungsgraden. Wir schließen mit der Untersuchung aller bzgl. y normierten kubischen Polynome $f \in \mathbb{F}_3[x,y]$, deren Koeffizienten im Grad durch 1 beschränkt sind.

$n=3, \quad q=3, \quad E=\mathbb{F}_{3^2}, \quad u^2+2u+2=0$	$T=3s$
$f(x,y) = y^3+(2x^2+x+1)y^2+(2x+1)y+2$	
$d(f) = x^5+2x^4+2x^3+x^2+2$	
ω_i	$1, \quad \rho, \quad \rho^2$
$B^*(\omega_i)$	$0, \quad 2, \quad 4$ $\qquad \Sigma=6, \quad M=4$
$s=2, \quad e=2,$ Signatur: $(1,1;2,1)$	
$\rho_1=\rho_{1,1}=z^{-4}+2z^{-2}+2+z^2+z^6+z^8+z^{12}+z^{14}+z^{16}+2z^{20}+z^{22}+2z^{24}+\dots$ $\rho_2=\rho_{2,1}=z^2+u^6z^3+z^6+z^8+u^6z^9+u^2z^{11}+z^{12}+u^2z^{13}+z^{14}+u^2z^{15}+\dots$ $\rho_3=\rho_{2,2}=z^2+u^2z^3+z^6+z^8+u^2z^9+u^6z^{11}+z^{12}+u^6z^{13}+z^{14}+u^6z^{15}+\dots$	
$\widetilde{\omega}_i$	$1, \quad (2x^2+x+1)\rho+\rho^2, \quad 2x^2+(x^3+x^2)\rho+(2x+1)\rho^2$
$B^*(\widetilde{\omega}_i)$	$0, \quad 1, \quad 3/2$ $\qquad \widetilde{\Sigma}=5/2, \quad \widetilde{M}=3/2$
$l=1$	$\Delta\Sigma=9/2, \quad \Delta M=5/2$

$n=3, \quad q=3, \quad E=\mathbb{F}_{3^3}, \quad u^3+2u+1=0$	$T=0s$
$f(x,y) = y^3+y^2+y+2$	
$d(f) = 2$	
ω_i	$1, \quad \rho, \quad \rho^2$
$B^*(\omega_i)$	$0, \quad 0, \quad 0$ $\qquad \Sigma=0, \quad M=0$
$s=1, \quad e=1,$ Signatur: $(1,3)$	
$\rho_1=\rho_{1,1}=u^{18}$ $\qquad \rho_2=\rho_{1,2}=u^2$ $\rho_3=\rho_{1,3}=u^6$	
$\widetilde{\omega}_i$	$1, \quad \rho, \quad \rho^2$
$B^*(\widetilde{\omega}_i)$	$0, \quad 0, \quad 0$ $\qquad \widetilde{\Sigma}=0, \quad \widetilde{M}=0$
$l=3$	$\Delta\Sigma=0, \quad \Delta M=0$

$n=3,\quad q=7^2,\quad w^2+6w+3=0,\quad E=\mathbb{F}_{7^2}$		$T=91s$
$f(x,y)=y^3+(3x^2+2x+6)y^2+(2x+3)y+1$		
$d(f)=2(x+w)(x+w^7)(x^2+w^{34}x+w^{15})(x^2+w^{46}x+w^9)$		
ω_i	$1,\quad \rho,\quad \rho^2$	
$B^*(\omega_i)$	$0,\quad 2,\quad 4$	$\Sigma=6,\quad M=4$
$s=3,\quad e=1,\quad$ Signatur: $(1,1;1,1;1,1)$		
$\rho_1=\rho_{1,1}=w^{29}z+w^{45}z^2+w^{35}z^3+w^{30}z^4+w^{44}z^5+w^4z^6+3z^7+w^{38}z^8+6z^9+\dots$ $\rho_2=\rho_{2,1}=w^{11}z+w^{27}z^2+w^5z^3+w^{18}z^4+w^{20}z^5+w^{28}z^6+3z^7+w^{26}z^8+6z^9+\dots$ $\rho_3=\rho_{3,1}=4z^{-2}+5z^{-1}+1+3z+6z^2+4z^3+3z^4+z^7+2z^8+2z^9+z^{11}+2z^{12}+\dots$		
$\widetilde{\omega}_i$	$1,\quad (4x^2+5x+1)\rho+6\rho^2,\quad (3x^2+2x)\rho+\rho^2$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 1,\quad 2$	$\widetilde{\Sigma}=3,\quad \widetilde{M}=2$
$l=1$		$\Delta\Sigma=3,\quad \Delta M=2$

$n=3,\quad q=13^2,\quad w^2+12w+2=0,\quad E=\mathbb{F}_{13^2}$		$T=11s$
$f(x,y)=y^3+(11x^2+3x+4)y^2+(2x+3)y+2x$		
$d(f)=(x+11)(x^3+wx^2+w^{82}x+w^{117})(x^3+w^{13}x^2+w^{58}x+w^9)$		
ω_i	$1,\quad \rho,\quad \rho^2$	
$B^*(\omega_i)$	$0,\quad 2,\quad 4$	$\Sigma=6,\quad M=4$
$s=2,\quad e=2,\quad$ Signatur: $(1,1;2,1)$		
$\rho_1=\rho_{1,1}=2z^{-4}+10z^{-2}+9+12z^2+10z^4+6z^6+5z^8+3z^{10}+7z^{12}+6z^{14}+2z^{16}+\dots$ $\rho_2=\rho_{2,1}=12z+7z^2+4z^3+8z^4+10z^5+10z^6+7z^7+4z^8+8z^9+5z^{10}+3z^{11}+\dots$ $\rho_3=\rho_{2,2}=z+7z^2+9z^3+8z^4+3z^5+10z^6+6z^7+4z^8+5z^9+5z^{10}+10z^{11}+\dots$		
$\widetilde{\omega}_i$	$1,\quad (6x^2+4x+1)\rho+10\rho^2,\quad (11x^2+3x)\rho+\rho^2$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 3/2,\ 2$	$\widetilde{\Sigma}=7/2,\quad \widetilde{M}=2$
$l=1$		$\Delta\Sigma=5/2,\quad \Delta M=2$

$n=4,\quad q=5,\quad E=\mathbb{F}_5$		$T=9s$
$f(x,y)=y^4+4x^2$		
$d(f)=4x^6$		
ω_i	$1,\quad \rho,\quad \rho^2/x,\quad \rho^3/x$	
$B^*(\omega_i)$	$0,\quad 1/2,\quad 0,\quad 1/2$	$\Sigma=1,\quad M=1/2$
$s=2,\quad e=2,\quad$ Signatur: $(2,1;2,1)$		
$\rho_1=\rho_{1,1}=3z^{-1}$ $\rho_3=\rho_{2,1}=4z^{-1}$	$\rho_2=\rho_{1,2}=2z^{-1}$ $\rho_4=\rho_{2,2}=z^{-1}$	
$\widetilde{\omega}_i$	$1,\quad \rho^2/x,\quad \rho,\quad \rho^3/x$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 0,\quad 1/2,\quad 1/2$	$\widetilde{\Sigma}=1,\quad \widetilde{M}=1/2$
$l=2$		$\Delta\Sigma=0,\quad \Delta M=0$

$n=4,\quad q=5,\quad E=\mathbb{F}_5,$		$T=48s$
$f(x,y)=y^4+(2x+3)y^3+(2x^2+3x+1)y^2+(3x^2+2x+4)y+3$		
$d(f)=x^{10}+x^9+4x^8+4x^6+x^5+x^4+3x+4$		
ω_i	$1,\quad \rho,\quad \rho^2,\quad \rho^3$	
$B^*(\omega_i)$	$0,\quad 1,\quad 2,\quad 3$	$\Sigma=6,\quad M=3$
$s=4,\quad e=1,\quad$ Signatur: $(1,1;1,1;1,1;1,1)$		
$\rho_1=\rho_{1,1}=1+4z+3z^4+z^5+3z^6+z^7+z^8+2z^{10}+3z^{11}+3z^{12}+4z^{13}+\dots$ $\rho_2=\rho_{2,1}=4z^2+4z^3+3z^4+2z^5+4z^6+3z^7+z^8+2z^9+2z^{10}+3z^{11}+2z^{12}+\dots$ $\rho_3=\rho_{3,1}=2z^{-1}+2+2z+2z^3+2z^4+2z^5+3z^6+2z^8+4z^9+z^{11}+z^{12}+\dots$ $\rho_4=\rho_{4,1}=z^{-1}+4+4z+z^2+4z^3+2z^4+z^7+z^8+4z^9+z^{10}+3z^{11}+4z^{12}+\dots$		
$\widetilde{\omega}_i$	$1,\quad \rho,\quad \rho^2,\quad 2x^2\rho+2x\rho^2+\rho^3$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 1,\quad 2,\quad 2$	$\widetilde{\Sigma}=5, \widetilde{M}=2$
$l=1$		$\Delta\Sigma=1,\quad \Delta M=1$

$n=4,\quad q=7,\quad E=\mathbb{F}_{7^4},\quad u^4+5u^2+4u+3=0$		$T=1s$
$f(x,y)=y^4+(x+2)y^3+(x^2+2x+3)y^2+(x^3+2x^2+3x+4)y$ $+x^4+2x^3+3x^2+4x+5$		
$d(f)=6(x+6)^{12}$		
ω_i	$1,\quad (6+\rho)/(x+6),\quad (1+5\rho+\rho^2)/(x^2+5x+1),$ $(6+3\rho+4\rho^2+\rho^3)/(x^3+4x^2+3x+6)$	
$B^*(\omega_i)$	$0,\quad 0,\quad 0,\quad 0$	$\Sigma=0.\quad M=0$
$s=1,\quad e=1,\quad$ Signatur: $(1,4)$		
$\rho_1=\rho_{1,1}=u^{1440}z^{-1}+u^{95}$ $\qquad \rho_2=\rho_{1,2}=u^{1920}z^{-1}+u^{1385}$ $\rho_3=\rho_{1,3}=u^{480}z^{-1}+u^{665}$ $\qquad \rho_4=\rho_{1,4}=u^{960}z^{-1}+u^{2255}$		
$\widetilde{\omega}_i$	$1,\quad (6+\rho)/(x+6),\quad (1+5\rho+\rho^2)/(x^2+5x+1),$ $(6+3\rho+4\rho^2+\rho^3)/(x^3+4x^2+3x+6)$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 0,\quad 0,\quad 0$	$\widetilde{\Sigma}=0,\quad \widetilde{M}=0$
$l=4$		$\Delta\Sigma=0,\quad \Delta M=0$

$n=4,\quad q=13^2,\quad w^2+12w+2=0,\quad E=\mathbb{F}_{13^6}=\mathbb{F}_{13^2}(\xi),$		$T=25s$
$f(x,y)=y^4+(2x+3)y^3+2y^2+y+4x+5$		
$d(f)=4(x^3+w^{89}x^2+w^{76}x+w^{121})(x^3+w^{149}x^2+w^{148}x+w^{61})$		
ω_i	$1,\quad \rho,\quad \rho^2,\quad \rho^3$	
$B^*(\omega_i)$	$0,\quad 1,\quad 2,\quad 3$	$\Sigma=6,\quad M=3$
$s=2,\quad e=1,\quad$ Signatur: $(1,1;1,3)$		
$\rho_1=\rho_{1,1}=11z^{-1}+10+z+2z^2+10z^3+7z^4+5z^5+7z^6+7z^7+z^8+z^9+\dots$ $\rho_2=\rho_{2,1}=w^{157}\xi^2+w^{113}\xi+w^{156}+(w^{80}\xi^2+w^{166}\xi+w^{150})z+\dots$ $\rho_3=\rho_{2,2}=w^{45}\xi^2+w\xi+w^{44}+(w^{51}\xi^2+w^{13}\xi+w^{139})z+\dots$ $\rho_4=\rho_{2,3}=w^{101}\xi^2+w^{57}\xi+w^{100}+(w^{34}\xi^2+w^{17}\xi+w^{94})z+\dots$		
$\widetilde{\omega}_i$	$1,\quad \rho,\quad 2x\rho+\rho^2,\quad 7x\rho+2x\rho^2+\rho^3$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 1,\quad 1,\quad 1$	$\widetilde{\Sigma}=3,\quad \widetilde{M}=1$
$l=1$		$\Delta\Sigma=3,\quad \Delta M=2$

$n=5,\quad q=5,\quad E=\mathbb{F}_{5^2},\quad u^2+4u+2=0$		$T=4s$
$f(x,y)=y^5+3y^4+(4x+2)y^2+(4x+3)y+1$		
$d(f)=3(x+3)(x^2+x+2)(x^3+4x+3)$		
ω_i	$1,\quad \rho,\quad \rho^2,\quad \rho^3,\quad \rho^4$	
$B^*(\omega_i)$	$0,\quad 1/3,\quad 2/3,\quad 1,\quad 4/3$	$\Sigma=10/3,\quad M=4/3$
$s=3,\quad e=3,\quad$ Signatur: $(1,1;1,1;3,1)$		
$\rho_1=\rho_{1,1}=z^3+2z^6+4z^9+3z^{12}+4z^{15}+2z^{21}+z^{24}+3z^{33}+2z^{36}+3z^{39}+\dots$ $\rho_2=\rho_{2,1}=4+3z^3+3z^6+2z^9+z^{12}+2z^{21}+2z^{24}+z^{27}+4z^{30}+z^{33}+z^{36}+\dots$ $\rho_3=\rho_{3,1}=u^{16}z^{-1}+1+2z^3+u^{20}z^4+u^4z^5+u^{20}z^7+u^4z^8+3z^9+u^2z^{10}+\dots$ $\rho_4=\rho_{3,2}=z^{-1}+1+2z^3+4z^4+4z^5+4z^7+4z^8+3z^9+3z^{10}+z^{11}+2z^{12}+\dots$ $\rho_5=\rho_{3,3}=u^8z^{-1}+1+2z^3+u^4z^4+u^{20}z^5+u^4z^7+u^{20}z^8+3z^9+u^{10}z^{10}+\dots$		
$\widetilde{\omega}_i$	$1,\quad \rho,\quad \rho^2,\quad \rho^3,\quad \rho^4$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 1/3,\quad 2/3,\quad 1,\quad 4/3$	$\widetilde{\Sigma}=10/3,\quad M=4/3$
$l=1$		$\Delta\Sigma=0,\quad \Delta M=0$

$n=5,\quad q=5^2,\quad E=\mathbb{F}_{5^6},\quad u^6+u^4+4u^3+u^2+2=0$		$T=86s$
$f(x,y)=y^5+2y^4+y^3+2y+1$		
$d(f)=2$		
ω_i	$1,\quad \rho,\quad \rho^2,\quad \rho^3,\quad \rho^4$	
$B^*(\omega_i)$	$0,\quad 0,\quad 0,\quad 0,\quad 0$	$\Sigma=0,\quad M=0$
$s=3,\quad e=1,\quad$ Signatur: $(1,1;1,1;1,3)$		
$\rho_1=\rho_{1,1}=u^{6510}$ $\rho_3=\rho_{3,1}=u^{9576}$ $\rho_5=\rho_{3,3}=u^{5040}$	$\rho_2=\rho_{2,1}=u^{1302}$ $\rho_4=\rho_{3,2}=u^{1008}$	
$\widetilde{\omega}_i$	$1,\quad \rho,\quad \rho^2,\quad \rho^3,\quad \rho^4$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 0,\quad 0,\quad 0,\quad 0$	$\widetilde{\Sigma}=0,\quad \widetilde{M}=0$
$l=5$		$\Delta\Sigma=0,\quad \Delta M=0$

$n=5,\quad q=7^2,\quad w^2+6w+3=0,\quad E=\mathbb{F}_{7^2},\quad u=w$		$T=245s$
$f(x,y)=y^5+(2x+3)y^4+1$		
$d(f)=2(x+1)(x^2+w^5x+w^{30})(x^2+w^{35}x+w^{18})$		
ω_i	$1,\quad \rho,\quad \rho^2,\quad \rho^3,\quad \rho^4$	
$B^*(\omega_i)$	$0,\quad 1,\quad 2,\quad 3,\quad 4$	$\Sigma=10,\quad M=4$
$s=2,\quad e=4,\quad$ Signatur: $(1,1;4,1)$		
$\rho_1=\rho_{1,1}=5z^{-4}+4+3z^{16}+3z^{20}+z^{24}+4z^{28}+4z^{36}+2z^{40}+5z^{44}+z^{48}+\dots$ $\rho_2=\rho_{2,1}=u^{26}z+u^{10}z^5+u^{28}z^6+u^{18}z^9+u^{36}z^{10}+u^{10}z^{13}+u^{12}z^{14}+z^{16}+\dots$ $\rho_3=\rho_{2,2}=u^{38}z+u^{22}z^5+u^4z^6+u^{30}z^9+u^{12}z^{10}+u^{22}z^{13}+u^{36}z^{14}+z^{16}+\dots$ $\rho_4=\rho_{2,3}=u^2z+u^{34}z^5+u^{28}z^6+u^{42}z^9+u^{36}z^{10}+u^{34}z^{13}+u^{12}z^{14}+z^{16}+\dots$ $\rho_5=\rho_{2,4}=u^{14}z+u^{46}z^5+u^4z^6+u^6z^9+u^{12}z^{10}+u^{46}z^{13}+u^{36}z^{14}+z^{16}+\dots$		
$\widetilde{\omega}_i$	$1,\quad \rho,\quad \rho^2,\quad \rho^3,\quad \rho^4$	
$B^*(\widetilde{\omega}_i)$	$0,\quad 3/4,\quad 1,\quad 11/4,\quad 15/4$	$\widetilde{\Sigma}=33/4,\quad \widetilde{M}=15/4$
$l=1$		$\Delta\Sigma=7/4,\quad \Delta M=1/4$

$n=5, \quad q=11, \quad E=\mathbb{F}_{11^2}, \quad u^2+7u+2=0$	$T=37s$
$f(x,y)=y^5+(3x+2)y^4+(4x+2)y^3+(3x+2)y^2+3y+1$	
$d(f)=3(x+2)(x+3)^3(x^3+6x^2+2x+5)$	
ω_i	$1, \quad \rho, \quad \rho^2, \quad \rho^3, \quad \rho^4$
$B^*(\omega_i)$	$0, \quad 1, \quad 2, \quad 3, \quad 4 \qquad \Sigma=10, \quad M=4$
$s=3, \quad e=2, \quad$ Signatur: $(1,1;1,2;2,1)$	
$\rho_1=\rho_{1,1}=8z^{-2}+3+9z^2+10z^4+7z^6+8z^8+9z^{10}+9z^{12}+6z^{14}+7z^{16}+\dots$ $\rho_2=\rho_{2,1}=u^{110}+u^{87}z^2+u^{118}z^4+u^{85}z^6+u^{39}z^8+u^{70}z^{10}+u^{116}z^{12}+u^{21}z^{14}+\dots$ $\rho_3=\rho_{2,2}=u^{10}+u^{117}z^2+u^{98}z^4+u^{95}z^6+u^{69}z^8+u^{50}z^{10}+u^{76}z^{12}+u^{111}z^{14}+\dots$ $\rho_4=\rho_{3,1}=u^{102}z+4z^2+u^{54}z^3+10z^4+10z^6+u^{54}z^7+z^8+4z^{10}+u^{78}z^{11}+\dots$ $\rho_5=\rho_{3,2}=u^{42}z+4z^2+u^{114}z^3+10z^4+10z^6+u^{114}z^7+z^8+4z^{10}+u^{18}z^{11}+\dots$	
$\widetilde{\omega}_i$	$1, \quad (7x+1)\rho+(2x+1)\rho^2+(7x+1)\rho^3+6\rho^4, \quad 3x\rho+\rho^2, \quad 9x\rho+3x\rho^2+\rho^3,$ $x\rho+9x\rho^2+3x\rho^3+\rho^4$
$B^*(\widetilde{\omega}_i)$	$0, \quad 1/2, \quad 1, \quad 1, \quad 1 \qquad \widetilde{\Sigma}=7/2, \quad \widetilde{M}=1$
$l=1$	$\Delta\Sigma=13/2, \quad \Delta M=3$

$n=11, \quad q=7, \quad E=\mathbb{F}_{7^{10}}=\mathbb{F}_7(\xi)$	$T=443s$
$f(x,y)=y^{11}+x$	
$d(f)=2x^{10}$	
ω_i	$1, \quad \rho, \quad \rho^2, \quad \rho^3, \quad \rho^4, \quad \rho^5, \quad \rho^6, \quad \rho^7, \quad \rho^8, \quad \rho^9, \quad \rho^{10}$
$B^*(\omega_i)$	$0, 1/11, 2/11, 3/11, 4/11, 5/11, 6/11, 7/11, 8/11, 9/11, 10/11 \quad \Sigma=5, \quad M=10/11$
$s=1, \quad e=11, \quad$ Signatur: $(11,1)$	
$\rho_1=\rho_{1,1}=6z^{-1}$ $\rho_2=\rho_{1,2}=(4\xi^9+\xi^8+4\xi^7+3\xi^6+6\xi^5+6\xi^3+6\xi^2+6\xi+4)z^{-1}$ $\rho_3=\rho_{1,3}=(6\xi^9+2\xi^8+3\xi^7+5\xi^5+6\xi^4+\xi^2)z^{-1}$ $\rho_4=\rho_{1,4}=(2\xi^9+3\xi^8+6\xi^7+3\xi^6+\xi^5+2\xi^4+6\xi^3+\xi^2+6)z^{-1}$ $\rho_5=\rho_{1,5}=(5\xi^9+\xi^8+2\xi^6+6\xi^5+6\xi^4+\xi+3)z^{-1}$ $\rho_6=\rho_{1,6}=(2\xi^9+4\xi^8+\xi^7+6\xi^6+3\xi^5+4\xi^4+5\xi^2+6\xi+5)z^{-1}$ $\rho_7=\rho_{1,7}=(\xi^9+\xi^8+\xi^7+2\xi^6+3\xi^5+\xi^4+6\xi^3+3\xi^2+6\xi)z^{-1}$ $\rho_8=\rho_{1,8}=(4\xi^9+6\xi^8+\xi^7+2\xi^3+4\xi^2+4\xi+4)z^{-1}$ $\rho_9=\rho_{1,9}=(5\xi^9+3\xi^8+6\xi^7+2\xi^5+\xi^4+5\xi^3+3\xi^2+5\xi+5)z^{-1}$ $\rho_{10}=\rho_{1,10}=(6\xi^9+2\xi^7+\xi^6+\xi^5+2\xi^4+\xi^3+5\xi^2+6\xi+2)z^{-1}$ $\rho_{11}=\rho_{1,11}=(4\xi^7+4\xi^6+\xi^5+6\xi^4+2\xi^3+\xi)z^{-1}$	
$\widetilde{\omega}_i$	$1, \quad \rho, \quad \rho^2, \quad \rho^3, \quad \rho^4, \quad \rho^5, \quad \rho^6, \quad \rho^7, \quad \rho^8, \quad \rho^9, \quad \rho^{10}$
$B^*(\widetilde{\omega}_i)$	$0, 1/11, 2/11, 3/11, 4/11, 5/11, 6/11, 7/11, 8/11, 9/11, 10/11 \quad \widetilde{\Sigma}=5, \quad \widetilde{M}=10/11$
$l=1$	$\Delta\Sigma=0, \quad \Delta M=0$

$n=12,\quad q=5,\quad E=\mathbb{F}_{5^2},\quad u^2+4u+2=0$	$T=636s$
$f(x,y)=y^{12}+x$	
$d(f)=x^{11}$	
ω_i	$1,\ \rho,\ \rho^2,\ \rho^3,\ \rho^4,\ \rho^5,\ \rho^6,\ \rho^7,\ \rho^8,\ \rho^9,\ \rho^{10},\ \rho^{11}$
$B^*(\omega_i)$	$0,\ 1/12,\ 1/6,\ 1/4,\ 1/3,\ 5/12,\ 1/2,\ 7/12,\ 2/3,\ 3/4,\ 5/6,\ 11/12$ $\quad \Sigma=11/2,\quad M=11/12$
$s=1,\quad e=12,\quad$ Signatur: $(12,1)$	
$\rho_1=\rho_{1,1}=u^{13}z^{-1}$	$\rho_2=\rho_{1,2}=u^{15}z^{-1}$
$\rho_3=\rho_{1,3}=u^{17}z^{-1}$	$\rho_4=\rho_{1,4}=u^{19}z^{-1}$
$\rho_5=\rho_{1,5}=u^{21}z^{-1}$	$\rho_6=\rho_{1,6}=u^{23}z^{-1}$
$\rho_7=\rho_{1,7}=uz^{-1}$	$\rho_8=\rho_{1,8}=u^{3}z^{-1}$
$\rho_9=\rho_{1,9}=u^{5}z^{-1}$	$\rho_{10}=\rho_{1,10}=u^{7}z^{-1}$
$\rho_{11}=\rho_{1,11}=u^{9}z^{-1}$	$\rho_{12}=\rho_{1,12}=u^{11}z^{-1}$
$\widetilde{\omega}_i$	$1,\ \rho,\ \rho^2,\ \rho^3,\ \rho^4,\ \rho^5,\ \rho^6,\ \rho^7,\ \rho^8,\ \rho^9,\ \rho^{10},\ \rho^{11}$
$B^*(\widetilde{\omega}_i)$	$0,\ 1/12,\ 1/6,\ 1/4,\ 1/3,\ 5/12,\ 1/2,\ 7/12,\ 2/3,\ 3/4,\ 5/6,\ 11/12$ $\quad \widetilde{\Sigma}=11/2,\quad \widetilde{M}=11/12$
$l=1$	$\Delta\Sigma=0,\quad \Delta M=0$

$n=13,\quad q=5,\quad E=\mathbb{F}_{5^4},\quad u^4+4u^2+2=0$	$T=1037s$
$f(x,y)=y^{13}+x^3$	
$d(f)=3x^{36}$	
ω_i	$1,\ \rho,\ \rho^2,\ \rho^3,\ \rho^4,\ \rho^5/x,\ \rho^6/x,\ \rho^7/x,\ \rho^8/x,\ \rho^9/x^2,\ \rho^{10}/x^2,\ \rho^{11}/x^2,\ \rho^{12}/x^2$
$B^*(\omega_i)$	$0,\ 3/13,\ 6/13,\ 9/13,\ 12/13,\ 2/13,\ 5/13,\ 8/13,\ 11/13,\ 1/13,\ 4/13,\ 7/13,\ 10/13$ $\quad \Sigma=78/13,\quad M=12/13$
$s=1,\quad e=13,\quad$ Signatur: $(13,1)$	
$\rho_1=\rho_{1,1}=4z^{-3}$	$\rho_2=\rho_{1,2}=u^{360}z^{-3}$
$\rho_3=\rho_{1,3}=u^{408}z^{-3}$	$\rho_4=\rho_{1,4}=u^{456}z^{-3}$
$\rho_5=\rho_{1,5}=u^{504}z^{-3}$	$\rho_6=\rho_{1,6}=u^{552}z^{-3}$
$\rho_7=\rho_{1,7}=u^{600}z^{-3}$	$\rho_8=\rho_{1,8}=u^{24}z^{-3}$
$\rho_9=\rho_{1,9}=u^{72}z^{-3}$	$\rho_{10}=\rho_{1,10}=u^{120}z^{-3}$
$\rho_{11}=\rho_{1,11}=u^{168}z^{-3}$	$\rho_{12}=\rho_{1,12}=u^{216}z^{-3}$
$\rho_{13}=\rho_{1,13}=u^{264}z^{-3}$	
$\widetilde{\omega}_i$	$1,\ \rho^9/x^2,\ \rho^5/x,\ \rho,\ \rho^{10}/x^2,\ \rho^6/x,\ \rho^2,\ \rho^{11}/x^2,\ \rho^7/x,\ \rho^3,\ \rho^{12}/x^2,\ \rho^8/x,\ \rho^4$
$B^*(\widetilde{\omega}_i)$	$0,\ 1/13,\ 2/13,\ 3/13,\ 4/13,\ 5/13,\ 6/13,\ 7/13,\ 8/13,\ 9/13,\ 10/13,\ 11/13,\ 12/13$ $\quad \widetilde{\Sigma}=78/13,\quad \widetilde{M}=12/13$
$l=1$	$\Delta\Sigma=0,\quad \Delta M=0$

Wir beschließen die Beispiele zur Ganzheitsbasenreduktion mit der Untersuchung aller kubischen Polynome der Form $f(x,y)=y^3+a_2(x)y^2+a_1(x)y+a_0(x)\in\mathbb{F}_3[x,y]$ mit $\deg(a_i)\in\{-\infty,0,1\}, 0\le i\le 2$.

Von den $3^6=729$ Polynomen erzeugen 428 separable Körpererweiterungen $F/\mathbb{F}_q(x)$ vom Grad 3, in denen P_∞ zahm verzweigt ist.

In der folgenden Tabelle sind die Werte in Abhängigkeit von der Signatur aufgeführt. In der letzten Spalte gibt $\overline{T}$ die durchschnittliche Laufzeit in Sekunden an; Werte in runden Klammern bedeuten absolute Anzahlen.

Signatur	$[E:\mathbb{F}_3]$	Σ	M	$\widetilde{\Sigma}$	$\widetilde{M}$	$\Delta\Sigma$	ΔM	$\overline{T}$
$(1,3)$ (8)	3	0	0	0	0	0	0	0,017
$(1,1;1,2)$ (144)	2	3	2	2	1	1	1	3,028
$(1,1;2,1)$ (204)	1 (102) 2 (102)	3/2 (96) 3 (108)	1 (96) 2 (108)	3/2	1	0 (96) 3/2 (108)	0 (96) 1 (108)	7,672
$(1,1;1,1;1,1)$ (72)	1	3	2	2	1	1	1	5,736

2. Einheitenberechnung

In diesem Abschnitt geben wir einige Beispiele zur Berechnung der Einheitengruppe im zahm verzweigten Fall. In den folgenden Tabellen bezeichnet $\widetilde{\omega}_1, \dots, \widetilde{\omega}_n \in o_F$ immer eine 0-reduzierte Ganzheitsbasis und $\varepsilon_1, \dots, \varepsilon_r$ Grundeinheiten.

$n=3, \quad q=3, \quad$ Signatur: $(1,1;2,1)$	$T=35s$
$f(x,y)=y^3+(2x+1)y^2+(2x^3+x^2+x+1)y+x^2+2$	
$r=1, \quad \mathrm{Reg}(U_F)=19, \quad l=1$	
$\widetilde{\omega}_i$	$1, \quad \rho, \quad \rho^2$
$\varepsilon_1=(2x^7+2x^6+2x^5+x^4+2x^3+2x^2+2x+1)\widetilde{\omega}_1+(x^8+x^5+2x^3+x^2)\widetilde{\omega}_2+(2x^6+2x^5+x^2+x+1)\widetilde{\omega}_3$	$L^\infty(\varepsilon_1)=(19)$

$n=3, \quad q=3, \quad$ Signatur: $(1,1;1,1;1,1)$	$T=23s$
$f(x,y)=y^3+(x^2+2)y^2+(2x^2+2)y+2$	
$r=2, \quad \mathrm{Reg}(U_F)=4, \quad l=1$	
$\widetilde{\omega}_i$	$1, \quad \rho, \quad x^2\rho+\rho^2$
$\varepsilon_1=(2x^2+1)\widetilde{\omega}_1+2\widetilde{\omega}_2+\widetilde{\omega}_3$	$L^\infty(\varepsilon_1)=(2,0)^t$
$\varepsilon_2=(x^2+1)\widetilde{\omega}_1+\widetilde{\omega}_2+2\widetilde{\omega}_3$	$L^\infty(\varepsilon_2)=(0,2)^t$

$n=3, \quad q=5, \quad$ Signatur: $(1,1;1,2)$	$T=8s$
$f(x,y)=y^3+(x^2+2x+2)y^2+(x+2)y+2$	
$r=1, \quad \mathrm{Reg}(U_F)=2, \quad l=1$	
$\widetilde{\omega}_i$	$1, \quad (3x^2+x+1)\rho+3\rho^2, \quad (x^2+2x)\rho+\rho^2$
$\varepsilon_1=(3x+1)\widetilde{\omega}_1+\widetilde{\omega}_2$	$L^\infty(\varepsilon_1)=(2)$

$n=3, \quad q=5^2, \quad$ Signatur: $(1,1;2,1)$	$T=10s$
$f(x,y)=y^3+(3x+4)y^2+2y+1$	
$r=1, \quad \mathrm{Reg}(U_F)=1, \quad l=1$	
$\widetilde{\omega}_i$	$1, \quad (2x+1)\rho+4\rho^2, \quad 3x\rho+\rho^2$
$\varepsilon_1=\widetilde{\omega}_1+2\widetilde{\omega}_2$	$L^\infty(\varepsilon_1)=(1)$

$n = 3, \quad q = 7, \quad$ Signatur: $(1,1;2,1)$	$T = 9s$
$f(x,y) = y^3 + (2x+3)y^2 + 1$	
$r = 1, \quad \mathrm{Reg}(U_F) = 1, \quad l = 1$	
$\widetilde{\omega}_i$ | $1, \quad (3x+1)\rho + 5\rho^2, \quad 2x\rho + \rho^2$	
$\varepsilon_1 = \widetilde{\omega}_2$	$L^\infty(\varepsilon_1) = (1)$

$n = 3, \quad q = 7^2, \quad$ Signatur: $(1,1;3,1)$	$T = 22s$
$f(x,y) = y^4 + 2y^3 + (2x^2+3x+4)y + 1$	
$r = 1, \quad \mathrm{Reg}(U_F) = 2, \quad l = 1$	
$\widetilde{\omega}_i$ | $1, \quad \rho, \quad \rho^2, \quad \rho^3$	
$\varepsilon_1 = \widetilde{\omega}_2$	$L^\infty(\varepsilon_1) = (2)$

$n = 3, \quad q = 11, \quad$ Signatur: $(1,1;1,1;1,1)$	$T = 534s$
$f(x,y) = y^3 + (8x^2+x)y^2 + (6x^2+3x+3)y + 8$	
$r = 2, \quad \mathrm{Reg}(U_F) = 268, \quad l = 1$	
$\widetilde{\omega}_i$ | $1, \quad \rho, \quad (8x^2+x)\rho + \rho^2$	
$\varepsilon_1 = \widetilde{\omega}_2$	$L^\infty(\varepsilon_1) = (2,0)^t$
$\varepsilon_2 = (10x^{128}+2x^{127}+8x^{126}+6x^{125}+3x^{124}+6x^{123}+4x^{122}+2x^{121}+4x^{120}+x^{119}+7x^{118}+x^{117}+6x^{116}+3x^{115}+8x^{114}+9x^{113}+8x^{112}+8x^{111}+3x^{110}+5x^{109}+10x^{108}+3x^{107}+5x^{106}+2x^{105}+4x^{104}+10x^{103}+2x^{102}+4x^{101}+5x^{100}+10x^{99}+9x^{98}+10x^{96}+3x^{95}+3x^{94}+9x^{93}+3x^{92}+9x^{91}+8x^{90}+3x^{89}+5x^{88}+5x^{87}+8x^{86}+4x^{85}+9x^{84}+4x^{83}+x^{82}+4x^{81}+7x^{80}+9x^{79}+6x^{78}+5x^{77}+2x^{76}+9x^{75}+2x^{74}+8x^{73}+2x^{72}+4x^{71}+7x^{70}+9x^{69}+5x^{68}+3x^{66}+8x^{64}+7x^{63}+10x^{62}+x^{61}+8x^{60}+3x^{59}+2x^{58}+6x^{57}+10x^{56}+7x^{55}+4x^{54}+5x^{53}+5x^{52}+3x^{51}+3x^{50}+5x^{49}+9x^{48}+3x^{46}+5x^{45}+6x^{44}+5x^{43}+7x^{42}+10x^{41}+9x^{40}+6x^{39}+7x^{38}+6x^{37}+4x^{36}+4x^{35}+5x^{34}+x^{33}+4x^{32}+9x^{31}+3x^{30}+10x^{29}+6x^{28}+5x^{27}+10x^{26}+8x^{25}+6x^{24}+7x^{23}+4x^{22}+4x^{21}+9x^{20}+3x^{19}+2x^{18}+6x^{17}+9x^{16}+6x^{15}+5x^{13}+3x^{12}+8x^{11}+x^{10}+10x^9+x^8+3x^7+6x^6+2x^5+8x^3+6x^2+8x+1)\widetilde{\omega}_1+(8x^{132}+8x^{131}+9x^{130}+4x^{129}+5x^{127}+5x^{126}+10x^{125}+4x^{124}+4x^{123}+x^{122}+7x^{121}+9x^{119}+3x^{118}+10x^{117}+2x^{116}+10x^{115}+10x^{114}+9x^{113}+2x^{112}+8x^{111}+3x^{110}+8x^{109}+2x^{108}+9x^{107}+5x^{106}+9x^{105}+7x^{104}+3x^{103}+7x^{102}+10x^{100}+10x^{99}+10x^{98}+5x^{97}+2x^{96}+4x^{95}+4x^{94}+10x^{93}+10x^{92}+6x^{91}+3x^{90}+10x^{89}+8x^{88}+3x^{87}+2x^{86}+7x^{85}+8x^{84}+4x^{83}+4x^{82}+3x^{81}+4x^{80}+2x^{79}+10x^{77}+7x^{76}+6x^{75}+7x^{74}+x^{73}+2x^{72}+x^{71}+x^{68}+9x^{67}+10x^{66}+5x^{64}+9x^{63}+x^{62}+2x^{61}+8x^{60}+7x^{59}+6x^{57}+6x^{56}+4x^{55}+5x^{54}+2x^{53}+10x^{52}+2x^{50}+3x^{48}+8x^{46}+x^{45}+5x^{43}+5x^{42}+3x^{40}+5x^{39}+10x^{38}+5x^{37}+3x^{36}+7x^{35}+x^{34}+x^{33}+2x^{32}+8x^{31}+2x^{30}+10x^{29}+8x^{28}+4x^{27}+9x^{26}+8x^{24}+8x^{23}+10x^{22}+x^{21}+7x^{19}+x^{18}+6x^{17}+5x^{16}+4x^{15}+3x^{14}+4x^{13}+8x^{12}+6x^{11}+x^{10}+5x^9+5x^8+7x^7+7x^6+8x^5+6x^4+6x^3+3x^2+7x+4)\widetilde{\omega}_2+(10x^{130}+6x^{129}+8x^{128}+5x^{127}+9x^{125}+9x^{124}+5x^{123}+x^{122}+4x^{121}+6x^{120}+2x^{118}+3x^{116}+2x^{114}+6x^{113}+9x^{112}+2x^{111}+8x^{110}+10x^{109}+9x^{108}+x^{107}+7x^{106}+10x^{105}+3x^{104}+4x^{103}+9x^{102}+8x^{101}+4x^{100}+x^{99}+5x^{98}+6x^{97}+10x^{96}+9x^{95}+6x^{94}+3x^{93}+9x^{91}+10x^{90}+9x^{89}+10x^{88}+4x^{86}+8x^{85}+9x^{84}+9x^{83}+5x^{82}+8x^{81}+x^{80}+10x^{79}+4x^{78}+5x^{77}+7x^{76}+8x^{74}+5x^{73}+5x^{72}+5x^{70}+2x^{69}+7x^{68}+7x^{67}+10x^{66}+7x^{65}+6x^{64}+x^{63}+6x^{62}+9x^{61}+4x^{60}+x^{59}+x^{58}+8x^{56}+x^{55}+4x^{54}+x^{53}+9x^{52}+4x^{50}+5x^{49}+7x^{48}+10x^{47}+9x^{46}+x^{45}+4x^{44}+6x^{43}+3x^{42}+8x^{41}+3x^{40}+6x^{39}+7x^{37}+7x^{36}+7x^{35}+4x^{33}+2x^{32}+3x^{31}+10x^{30}+2x^{29}+10x^{28}+9x^{27}+2x^{26}+8x^{25}+5x^{23}+2x^{22}+2x^{21}+10x^{20}+x^{19}+2x^{18}+9x^{17}+10x^{16}+6x^{15}+8x^{14}+2x^{13}+3x^{12}+x^{11}+9x^{10}+x^9+9x^8+6x^7+9x^6+6x^5+5x^4+7x^3+6x^2+5x+9)\widetilde{\omega}_3$	$L^\infty(\varepsilon_2) = (0,134)^t$

$n = 3,\quad q = 13,\quad$ Signatur: $(1,1;1,1;1,1)$	$T = 23s$
$f(x,y) = y^3 + (10x^2 + 7x + 1)y^2 + (2x^2 + 8x + 5)y + 7$	
$r = 2,\quad \mathrm{Reg}(U_F) = 4,\quad l = 1$	
$\widetilde{\omega}_i$ | $1,\quad 9/x + (7x^2 + x + 9)\rho/x + 2\rho^2/x,\quad 11/x + (10x^2 + 11)\rho/x + 1\rho^2/x$	
$\varepsilon_1 = \widetilde{\omega}_2 + 11\widetilde{\omega}_3$	$L^\infty(\varepsilon_1) = (2,0)^t$
$\varepsilon_2 = 3x\widetilde{\omega}_2 + (7x+1)\widetilde{\omega}_3$	$L^\infty(\varepsilon_2) = (1,2)^t$

$n = 3,\quad q = 17,\quad$ Signatur: $(1,1;1,2)$	$T = 1301s$
$f(x,y) = y^3 + 2y^2 + (6x^2 + 14x + 6)y + 10x^2 + 10x + 1$	
$r = 1,\quad \mathrm{Reg}(U_F) = 32,\quad l = 1$	
$\widetilde{\omega}_i$ | $1,\quad \rho,\quad \rho^2$	
$\varepsilon_1 = (14x^{15} + 12x^{14} + 12x^{13} + 3x^{12} + 15x^{11} + 13x^{10} + 5x^9 + 4x^8 + 6x^7 + 16x^6 + 10x^5 + 4x^4 + 14x^3 + 8x^2 + 5x + 1)\widetilde{\omega}_1 + (5x^{15} + 7x^{14} + 11x^{13} + 14x^{12} + 12x^{11} + 14x^{10} + 2x^9 + 14x^8 + 2x^7 + x^6 + 16x^5 + 4x^4 + 3x^3 + 11x^2 + 10x)\widetilde{\omega}_2 + (2x^{14} + 9x^{13} + 7x^{12} + 3x^{11} + 15x^9 + 6x^8 + 14x^7 + 9x^6 + 4x^5 + x^4 + 5x^3 + 6x^2 + 5x + 10)\widetilde{\omega}_3$	$L^\infty(\varepsilon_1) = (32)$

$n = 4,\quad q = 3^2,\quad$ Signatur: $(2,1;2,1)$	$T = 47s$
$f(x,y) = y^4 + 2y^3 + (2x+1)y^2 + 2y + 1$	
$r = 1,\quad \mathrm{Reg}(U_F) = 1,\quad l = 1$	
$\widetilde{\omega}_i$ | $1,\quad \rho,\quad \rho^2,\quad \rho^3$	
$\varepsilon_1 = \widetilde{\omega}_2$	$L^\infty(\varepsilon_1) = (1)$

$n = 4,\quad q = 5,\quad$ Signatur: $(1,1;1,1;1,1;1,1)$	$T = 3803s$
$f(x,y) = y^4 + (2x+3)y^3 + y^2 + (3x+2)y + 1$	
$r = 3,\quad \mathrm{Reg}(U_F) = 1,\quad l = 1$	
$\widetilde{\omega}_i$ | $1,\quad \rho,\quad 2x\rho + \rho^2,\quad 4x\rho + 2x\rho^2 + \rho^3$	
$\varepsilon_1 = \widetilde{\omega}_1 + \widetilde{\omega}_3 + 4\widetilde{\omega}_4$	$L^\infty(\varepsilon_1) = (1,0,0)^t$
$\varepsilon_2 = \widetilde{\omega}_1 + 2\widetilde{\omega}_3 + 3\widetilde{\omega}_4$	$L^\infty(\varepsilon_2) = (0,1,0)^t$
$\varepsilon_3 = \widetilde{\omega}_1 + 3\widetilde{\omega}_3 + 2\widetilde{\omega}_4$	$L^\infty(\varepsilon_3) = (0,0,1)^t$

$n = 4,\quad q = 5^2,\quad$ Signatur: $(2,1;2,1)$	$T = 32s$
$f(x,y) = y^4 + 2y^3 + (3x+2)y^2 + y + 2$	
$r = 1,\quad \mathrm{Reg}(U_F) = 1,\quad l = 1$	
$\widetilde{\omega}_i$ | $1,\quad \rho,\quad \rho^2,\quad \rho^3$	
$\varepsilon_1 = \widetilde{\omega}_2$	$L^\infty(\varepsilon_1) = (1)$

$n = 4,\quad q = 5^2,\quad$ Signatur: $(1,1;3,1)$	$T = 44s$
$f(x,y) = y^4 + (2x+3)y^3 + y^2 + 1$	
$r = 1,\quad \mathrm{Reg}(U_F) = 2,\quad l = 1$	
$\widetilde{\omega}_i$ | $1,\quad (4x+1)\rho + 2\rho^2,\quad 2x\rho + \rho^2,\quad x^3\rho + 3x^2\rho^2 + \rho^3$	
$\varepsilon_1 = \widetilde{\omega}_1 + 3\widetilde{\omega}_2$	$L^\infty(\varepsilon_1) = (2)$

$n = 4,\quad q = 5^2,\quad$ Signatur: $(1,1;1,1;1,1;1,1)$	$T = 3433s$
$f(x,y) = y^4 + (2x+3)y^3 + (x+1)y^2 + (4x+3)y + 1$	
$r = 3,\quad \mathrm{Reg}(U_F) = 1,\quad l = 1$	
$\widetilde{\omega}_i$ | $1,\quad \rho,\quad 2x\rho + \rho^2,\quad 2x\rho^2 + \rho^3$	
$\varepsilon_1 = \widetilde{\omega}_1 + 2\widetilde{\omega}_2 + \widetilde{\omega}_3 + 3\widetilde{\omega}_4$	$L^\infty(\varepsilon_1) = (1,0,0)^t$
$\varepsilon_2 = \widetilde{\omega}_1 + \widetilde{\omega}_2 + 3\widetilde{\omega}_3 + 4\widetilde{\omega}_4$	$L^\infty(\varepsilon_2) = (0,1,0)^t$
$\varepsilon_3 = \widetilde{\omega}_1 + 4\widetilde{\omega}_2 + 2\widetilde{\omega}_3 + \widetilde{\omega}_4$	$L^\infty(\varepsilon_3) = (0,0,1)^t$

$n=4, \quad q=7^2, \quad w^2+6w+3=0,$ Signatur: $(1,1;1,1;1,1;1,1)$	$T=4371s$
$f(x,y)=y^4+(2x+3)y^3+(3x+2)y^2+(4x+5)y+1$	
$r=3, \quad \mathrm{Reg}(U_F)=1, \quad l=1$	
$\widetilde{\omega}_i$ | $1, \quad \rho, \quad 2x\rho+\rho^2, \quad 4x\rho+2x\rho^2+\rho^3$	
$\varepsilon_1=\widetilde{\omega}_1+w^{22}\widetilde{\omega}_2$	$L^\infty(\varepsilon_1)=(1,0,0)^t$
$\varepsilon_2=\widetilde{\omega}_2$	$L^\infty(\varepsilon_2)=(0,1,0)^t$
$\varepsilon_3=\widetilde{\omega}_1+w^{10}\widetilde{\omega}_2$	$L^\infty(\varepsilon_3)=(0,0,1)^t$

$n=5, \quad q=5,$ Signatur: $(2,1;3,1)$	$T=28s$
$f(x,y)=y^5+(2x+3)y^2+3y+1$	
$r=1, \quad \mathrm{Reg}(U_F)=1, \quad l=1$	
$\widetilde{\omega}_i$ | $1, \quad \rho, \quad \rho^2, \quad \rho^3, \quad \rho^4$	
$\varepsilon_1=\widetilde{\omega}_2$	$L^\infty(\varepsilon_1)=(1)$

Symbolverzeichnis

Im folgenden Symbolverzeichnis sind die in der Arbeit verwendeten Symbole aufgeführt. Die Zahlen in der rechten Spalte bezeichnen die Seite ihres erstmaligen Auftretens bzw. ihrer Definition.

$\mathbb{N}$, $\mathbb{N}_0$	die natürlichen Zahlen $\{1, 2, \dots\}$, $\mathbb{N} \cup \{0\}$
$\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$	die ganzen, rationalen, reellen und komplexen Zahlen
$\mathbb{P}$	die Menge der Primzahlen
$A \subset B$	$\alpha \in A \Rightarrow \alpha \in B$
$A < B$	für Gruppen: A ist Untergruppe von B
$A^\times$, R^*	$A \setminus \{0\}$, die invertierbaren Elemente eines Rings R
$[a_1, \dots, a_k]_R$	von $a_1, \dots, a_k$ erzeugter R-Modul
$\mathrm{Rg}_R M$, $\mathrm{Rg} A$	Rang des R-Moduls M, Rang einer Matrix A
$\mathrm{Ker}(M)$, $\deg_y(g)$	Kern einer Matrix M, Grad von $g \in R[y]$ bzgl. y
$\dim_k B$	Dimension des k-Vektorraums B
$\mathrm{N}_{K/k}$	Norm von K nach k (K Körpererweiterung von k)
$\overline{K}$	algebraischer Abschluß des Körpers K
S_n	symmetrische Gruppe mit $n!$ Elementen
$\mathrm{sign}(\sigma)$	Signum einer Permutation σ
$\mathrm{GL}(k, R)$	allg. lineare Gruppe in k Variablen über dem Ring R
Id, Id_n	Identität (Abbildung), Identität ($n \times n$-Matrix)
$\mathrm{Diag}(a_1, \dots, a_k)$	Diagonalmatrix mit Elementen $a_1, \dots, a_k$.
$\mathrm{HNF}(M)$	regulärer Teil der Spalten-Hermite-Normalform der Matrix M
K	(vollkommener) Konstantenkörper, 1
F	algebraischer Funktionenkörper, 1; ab 5: globaler —
x	transzendentes Element, 1; ab 5: separierendes —
$\widetilde{K}$	exakter Konstantenkörper von F/K, 1
l	$[\widetilde{K} : K]$, 2; ab 5: $[\widetilde{\mathbb{F}}_q : \mathbb{F}_q]$
$\mathcal{O}$, π	Bewertungsring von F, 2, Primelement, 2
$\mathbb{P}(F)$, P, Q	Menge aller Stellen von F, 2; Stellen, 2
$\mathcal{O}_P$	zur Stelle P gehörender Bewertungsring, 2

v	eine Bewertung, 3; ab 13: $v := V_k$
$\lvert\cdot\rvert$	ein Betrag, 3; ab 13: Betrag auf L
v_P	zur Stelle P gehörende Bewertung, 3
$\lvert\cdot\rvert_P$	zur Stelle P gehörender Betrag, 3
$\mathcal{O}_\pi$	zum Primelement π gehörender Bewertungsring, 3
$\mathcal{O}_\infty$	„unendlicher“ Bewertungsring, 3
P_∞, v_∞, $\lvert\cdot\rvert_\infty$	Stelle, Bewertung und Betrag zu $\mathcal{O}_\infty$, 3, 3, 3
$Q\vert P$	die Stelle Q „liegt über“ der Stelle P, 3
$e(Q\vert P)$	Verzweigungsindex von Q über P, 3
$f(Q\vert P)$	Trägheitsgrad von Q über P, 4
$\deg(Q)$, $\mathrm{Div}(F)$	Grad einer Stelle, 4, Divisorengruppe von F, 4
D	ein Divisor, 4; ab 28: $D \in \mathrm{Div}_\infty(F)$
$\deg(D)$	Grad eines Divisors, 4
(α)	Hauptdivisor zu $\alpha \in F^\times$, 4
$\mathbb{P}_\infty(F)$	Menge aller Stellen von F über P_∞, 4
$\mathbb{P}_0(F)$	$\mathbb{P}(F) \setminus \mathbb{P}_\infty(F)$, 4
$\mathrm{Div}_0(F)$, $\mathrm{Div}_\infty(F)$	$\mathrm{Div}(F) \cap \oplus_{P\in\mathbb{P}_0(F)}\mathbb{Z}P$, 4, $\oplus_{P\in\mathbb{P}_\infty(F)}\mathbb{Z}P$, 4
$\mathcal{F}$	ein algebraischer Zahlkörper, 5
(r_1, r_2)	die Signatur von $\mathcal{F}$, 7
$o_\mathcal{F}$, $\mathcal{I}_\mathcal{F}$	Maximalordnung von $\mathcal{F}$, 5, Idealgruppe von $o_\mathcal{F}$, 5
$\mathcal{I}$	Ideal in $\mathcal{I}_\mathcal{F}$, 5
p	(positive) Charakteristik des Konstantenkörpers, 5
q	eine p-Potenz, 5
$\mathbb{F}_q$	der endliche Körper mit q Elementen, 5
$\widetilde{\mathbb{F}}_q$	exakter Konstantenkörper von $F/\mathbb{F}_q$
f	definierendes Polynom für $F/\mathbb{F}_q(x)$ aus $\mathbb{F}_q[x,y]$, 5
n	$\deg_y(f)$, 5
$\rho := \rho_1$, ρ_i, $\rho_{i,j}$	die verschiedenen Nullstellen von f, 5, 25
s, $P_1, \ldots, P_s$	$\#\mathbb{P}_\infty(F)$, 6, $\{P_1, \ldots, P_s\} = \mathbb{P}_\infty(F)$, 6
e_i, f_i, n_i, v_i, $\lvert\cdot\rvert_i$	$e(P_i\vert P_\infty)$, 6, $f(P_i\vert P_\infty)$, 6, e_if_i, 6, v_{P_i}, 6, $q^{-v_i(\cdot)}$, 6
$(e_1, f_1; \ldots ; e_s, f_s)$	die Signatur von $F/\mathbb{F}_q(x)$, 6
e	$\mathrm{kgV}(e_1, \ldots, e_s)$, 6
E	algebraische Körpererweiterung von $\mathbb{F}_q$, 6
$E\langle x^{-1/k}\rangle$	Puiseuxreihen in $x^{-1/k}$ mit Koeffizienten aus E, 6
L	$E\langle x^{-1/k}\rangle$, 13
V_k	Bewertung auf $E\langle x^{-1/k}\rangle$, 6
$\widehat{F}_i$	Vervollständigung von F an P_i, 6
$\mathrm{Cl}(R, F)$	ganzer Abschluß des unitären Rings R in F, 7
o_F, $o_{F,\infty}$	ganzer Abschluß von $\mathbb{F}_q[x]$ bzw. $\mathcal{O}_\infty$ in F, 7
$\omega_1, \ldots, \omega_n$	eine Ganzheitsbasis, 7
f_∞	definierendes Polynom für $F/\mathbb{F}_q(x)$ aus $\mathcal{O}_\infty[y]$, 9
$\rho_\infty := \rho_{1,\infty}, \rho_{i,\infty}$	die verschiedenen Nullstellen von f_∞, 9
$d(f)$, $d(f_\infty)$	Polynomdiskriminante von f bzw. f_∞, 8, 9
V, $\lVert\cdot\rVert$	Ordnungsfunktion auf L^n, 13, „Betrag“ auf L^n, 13
G	eine Längenfunktion, 13
$C(G)$, $C(M)$	ein konvexer Körper, 14, ein Parallelotop in L^n, 14

Literaturverzeichnis

[Arm] Armitage, J. V.: *Algebraic functions and an analogue of the geometry of numbers: The Riemann-Roch theorem*; Arch. Math., Vol. 18; 1967; 383 - 393

[Ar1] Artin, E.: *Quadratische Körper im Gebiete der höheren Kongruenzen I. und II.*; Math. Z., Nr. 19; 1924; 153 - 206 und 207 - 246

[Ar2] Artin, E.: *Algebraic numbers and algebraic functions*; Gordon and Breach, Science Publishers, Inc.; New York - London - Paris; 1967

[AW] Artin, E.; Whaples, G.: *Axiomatic charcterization of fields by the product formula for valuations*; Bull. Amer. Math. Soc. 51; 1945; 469 - 492

[BL] Buchmann, J. A.; Lenstra H. W. Jr.: *Computing maximal orders and factoring over* $\mathbb{Z}_p$; Manuskript

[Ca] Campillo, A.: *Algebroid curves in positive characteristic*; Springer-Verlag; Berlin - Heidelberg - New York; 1980

[Ch] Chevalley, C.: *Introduction to the theory of algebraic functions of one variable*; AMS; New York; 1951

[Coa] Coates, J.: *Construction of rational functions on a curve*; Proc. Camb. Phil. Soc., No. 68; 1970; 105 - 123

[Coh1] Cohen, H.: *A course in computational algebraic number theory*; Springer-Verlag; Berlin - Heidelberg - New York; 1993

[Coh2] Cohn, P. M.: *Algebraic numbers and algebraic functions*; Chapman & Hall; London - New York - Tokyo; 1991

[DW] Dedekind, R.; Weber, H.: *Theorie der algebraischen Funktionen einer Veränderlichen*; J. Reine Angew. Mathematik, Nr. 92; 1879; 181 - 290

[D] Deuring, M.: *Lectures on the theory of algebraic functions of one variable*; Springer-Verlag; Berlin - Heidelberg - New York; 1973

[E] Eichler, M.: *Einführung in die Theorie der algebraischen Zahlen und Funktionen*; Birkhäuser Verlag; Basel - Stuttgart; 1963

[Fo] Ford, D. J.: *The construction of maximal orders over a Dedekind domain*; J. Symb. Comput., Vol. 4, No. 1; 1987; 69 - 75

[FJ] Fried, M. D.; Jarden, M.: *Field arithmetic*; Springer-Verlag; Berlin - Heidelberg - New York; 1986

[Fr] Freson, R.: *Die Kultur der französischen Küche*; DuMont Buchverlag; Köln; 1984

[Fu] Fulton, W.: *Algebraic curves*; W. A. Benjamin; New York - Amsterdam; 1969

[GHR] Goss, D.; Hayes, D. R.; Rosen, M. (Eds.): *The arithmetic of function fields*; Proc. of the workshop at the Ohio State Univ., June 17 - 26, 1991, Columbus, Ohio/U.S.A.; Walter de Gruyter; Berlin; 1992

[Gr] Griffiths, D.: *Series expansion of algebraic functions*; Bosma, W.; van der Poorten, A. (Eds.): *Computational algebra and number theory*; Kluwer Academic Publishers; Boston - Dordrecht - London; 1995

[Ha] Hasse, H.: *Zahlentheorie*; Akademie-Verlag; Berlin; 1963

[HL] Hensel, K.; Landsberg, G.: *Theorie der algebraischen Funktionen einer Variablen*; G. B. Teubner; Leipzig; 1902

[Ho] van Hoeij, M.: *An algorithm for computing an integral basis in an algebraic function field*; J. Symb. Comput., Vol. 18, No. 4; 1994; 353 - 363

[K] KANT group: *KANT V4*; erscheint im J. Symb. Comput.

[LLL] Lenstra, A. K.; Lenstra, H. W. Jr.; Lovász, L.: *Factoring polynomials with rational coefficients*; Math. Ann., Vol. 261; 1982; 515 - 534

[LN] Lidl, R.; Niederreiter, H.: *Finite fields*; Addison-Wesley Publishing Company; London - Amsterdam - Don Mills, Ontario; 1983

[Ma] Mahler, K.: *An analogue to Minkowski's geometry of numbers in a field of series*; Ann. Math., Vol. 42, No. 2; 1941; 488 - 522

[Mo] Moreno, C.: *Algebraic curves over finite fields*; Cambridge University Press; Cambridge - New York - Port Chester; 1991

[N] Narkiewicz, W.: *Elementary and analytic theory of algebraic numbers*; Springer-Verlag; PWN–Polish Scientific Publishers; Warszawa; 1990

[P] Pohst, M. E.: *Computational algebraic number theory*; Birkhäuser Verlag; Basel - Boston - Berlin; 1993

[PS] Pohst, M. E.; Schörnig, M.: *On integral basis reduction in global function fields*; erscheint in: Proc. of ANTS II, May 18 - 25, 1996, Université Bordeaux I, Talence/France

[PZ] Pohst, M. E.; Zassenhaus, H.: *Algorithmic algebraic number theory*; Cambridge University Press; Cambridge - New York - Melbourne; 1989

[R] Ribowicz, M.: *Calcul de paramétrisation de courbes algébriques: Les développements de Hamburger-Noether*; Rapport de recherche RR 798-M; TIM 3/IMAG Informatique et Mathématiques Appliquées de Grenoble; 1989

[Sch1] Schmidt, F. K.: *Analytische Zahlentheorie in Körpern der Charakteristik p*; Math. Z., Nr. 33; 1931; 1 - 32

[Sch2] Schmidt, W. M.: *Construction and estimation of bases in function fields*; J. Number Th., Vol. 39, No. 2; 1991; 181 - 224

[Sh] Shafarevich, I. R.: *Basic algebraic geometry*; Springer-Verlag; Berlin - Heidelberg - New York; 1974

[St] Stichtenoth, H.: *Algebraic function fields and codes*; Springer-Verlag; Berlin - Heidelberg - New York; 1993

[Wa] Walker, R. J.: *Algebraic curves*; Springer-Verlag; New York - Heidelberg - Berlin; 1978

[WZ] Weis, B.; Zimmer, H. G.: *Artins Theorie der quadratischen Kongruenzfunktionenkörper und ihre Anwendung auf die Berechnung der Einheiten- und Klassengruppen*; Festschrift der Math. Ges. in Hamburg zu ihrem 300 jährigen Bestehen 1990; Hamburg; 1991

[We] Weiss, E.: *Algebraic number theory*; Chelsea Publishing Company; New York; 1976

[Wi] Wildanger, K.: *Über Grundeinheitenberechnung in algebraischen Zahlkörpern*; Diplomarbeit; Düsseldorf; 1993

Zusammenfassung

Bezeichne $\mathbb{F}_q$ den endlichen Körper mit q Elementen und x ein über $\mathbb{F}_q$ transzendentes Element. Für ein irreduzibles Polynom $f \in \mathbb{F}_q[x,y]$ mit $\deg_y(f) = n$, welches bzgl. y normiert und separabel ist, betrachten wir den globalen Funktionenkörper

$$F = \mathbb{F}_q(x,\rho) \text{ mit } f(x,\rho) = 0.$$

Analog zu Zahlkörpern ist $F/\mathbb{F}_q(x)$ eine endliche, separable Erweiterung vom Grad n mit primitivem Element ρ. Der ganze Abschluß o_F von $\mathbb{F}_q[x]$ in F ist ein Dedekindring und freier $\mathbb{F}_q[x]$-Modul vom Rang n.

Wie auch bei algebraischen Zahlkörpern ist die Wahl einer geeigneten Ganzheitsbasis, d.h. von Elementen $\omega_1, \ldots, \omega_n \in o_F$ mit $o_F = \bigoplus_{i=1}^n \mathbb{F}_q[x]\omega_i$, entscheidend für die Effizienz algorithmischer Untersuchungen von o_F.

Um einen geeigneten Reduktionsbegriff für Ganzheitsbasen definieren zu können, untersuchen wir die Längenfunktion (mit $q^{-\infty} := 0$)

$$B : F \longrightarrow \mathbb{R}^{\geq 0} : \alpha \longmapsto q^{-\min_{i=1}^s v_i(\alpha)/e_i},$$

wobei $v_i, e_i, 1 \leq i \leq s$, die zu den paarweise verschiedenen Stellen $P_1, \ldots, P_s$, welche in F über der „unendlichen“ Stelle P_∞ liegen, gehörenden (exponentiellen) Bewertungen bzw. Verzweigungsindizes bezeichnen. Wir zeigen mit Mitteln der Gittertheorie, daß immer eine Ganzheitsbasis mit $B(\omega_i) = M_i, 1 \leq i \leq n$, existiert, wobei $M_i, 1 \leq i \leq n$, (verallgemeinerte) sukzessive Minima von o_F bzgl. B bezeichnen.

Im Fall, daß P_∞ in F zahm verzweigt ist, lassen sich alle Nullstellen von f über P_∞ in Puiseuxreihen entwickeln. Damit modifizieren wir einen Algorithmus von W. M. Schmidt, mit dem wir eine $\mathbb{F}_q$-Basis des Riemann-Rochschen Raums

$$\mathcal{L}(D,t) := \{\alpha \in o_F \mid v_i(\alpha) \geq -c_i - te_i \quad 1 \leq i \leq s\}$$

für einen Divisor $D = \sum_{i=1}^s c_i P_i, \quad c_i \in \mathbb{Z}, 1 \leq i \leq s$, und $t \in \mathbb{R}$ effizient berechnen können. Hierzu konstruieren wir im Algorithmus eine „D-reduzierte“ Ganzheitsbasis, aus der wir sofort die $\mathbb{F}_q$-Basis erhalten. Wir zeigen, daß eine 0-reduzierte Ganzheitsbasis die sukzessiven Minima M_i realisiert.

Schließlich berechnen wir die Einheitengruppe $U_F := o_F^*$ analog der aus Zahlkörpern bekannten Relationenmethode. Hierbei setzen wir im zahm verzweigten Fall den obigen Algorithmus zur Bestimmung der Torsionseinheiten, der Konstruktion von Elementen beschränkter Norm und für Wurzeltests ein. Für den wild verzweigten Fall geben wir Alternativen an.

Wir schließen mit illustrativen Beispielen zur 0-Reduktion von Ganzheitsbasen ($3 \leq n \leq 13$) und der Berechnung von U_F ($3 \leq n \leq 5$) im zahm verzweigten Fall.

Lebenslauf

Persönliche Daten

	Martin Schörnig geb. am 13.3.1969 in Düsseldorf ledig

Schulausbildung

8/74 – 7/75	Vorschule, Rather Kreuzweg, Düsseldorf.
8/75 – 7/79	Katholische Grundschule, Rather Kreuzweg, Düsseldorf.
8/79 – 6/88	Städt. Gymnasium Rückertstraße, Düsseldorf.
7.6.88	Abitur.

Studium

10/88 – 11/93	Studium der Mathematik mit Nebenfach Informatik an der Heinrich-Heine-Universität Düsseldorf.
16.10.90	Vordiplom in Mathematik.
12.11.93	Diplom in Mathematik.
11/93 – 4/96	Anfertigung der Dissertation an der Technischen Universität Berlin.
11/93 –	Wissenschaftlicher Mitarbeiter von Prof. Dr. M. E. Pohst am Fachbereich 3 Mathematik der Technischen Universität Berlin.
12.6.96	Tag der wissenschaftlichen Aussprache.
10/88 – 9/93, 4/94 – 6/96	Stipendiat der Studienstiftung des deutschen Volkes.