Ganzheitsbasen in einem Turm algebraischer Funktionenkörper: ein Beitrag zur Konstruktion asymptotisch guter algebraisch-geometrischer Codes.

Dissertation
zur Erlangung des Grades
Doktor der Naturwissenschaften
- Dr. rer. nat. -

vorgelegt beim
Fachbereich Mathematik und Informatik
der Universität GH Essen

von
Ilia Aleschnikov
aus Kaliningrad

2000

Vorsitzender:	Prof. Dr. W. Heinrichs
Erster Gutachter:	Prof. Dr. Tom Hoholdt, TU of Denmark
Zweiter Gutachter:	Prof. Dr. Hans-Georg Rück
Tag der mündlichen Prüfung:	2.10.2000

1 Einleitung

Sei q eine Primzahlpotenz und $\mathbb{F}_q$ der endliche Körper mit q Elementen. Ist $F/\mathbb{F}_q$ ein algebraischer Funktionenkörper über $\mathbb{F}_q$ mit genauem Konstantenkörper $\mathbb{F}_q$, so bezeichnen wir $g = g(F)$ als das Geschlecht von $F/\mathbb{F}_q$ und $N = N(F)$ als die Anzahl der rationalen Stellen von $F/\mathbb{F}_q$. Nach dem Satz von Hasse-Weil gilt

$$N(F) \leq q + 1 + 2g\sqrt{q}.$$

Wie Ihara bemerkte, kann diese Schranke wesentlich verbessert werden, falls g groß ist im Verhältnis zu q. Sei dazu

$$N_q(g) := \max\{N(F) \mid F/\mathbb{F}_q \text{ ist vom Geschlecht } g\}$$

und sei

$$A(q) := \limsup_{g\to\infty} \frac{N_q(g)}{g}.$$

Dann gilt die sogenannte Drinfeld-Vladut Schranke

$$A(q) \leq \sqrt{q} - 1.$$

Ist q ein Quadrat, so gilt sogar

$$A(q) = \sqrt{q} - 1 \tag{1}$$

[Iha] und [Tsf-Vla-Zin].

Dieses Ergebnis hat nun große Bedeutung für die Codierungstheorie im Bezug auf die Existenz guter langer Codes. Wir erinnern dazu an die folgenden Begriffe. Ist $C \subseteq \mathbb{F}_q^n$ ein $[n, k, d]$-Code, so bezeichnet man mit $R = R(C) := k/n$ die Rate von C und mit $\delta = \delta(C) := d/n$ den relativen Minimalabstand von C. Sei ferner

$$V_q := \{(\delta(C), R(C)) \in [0,1]^2 \mid C \text{ ist ein Code über } \mathbb{F}_q\}$$

und $U_q \subseteq [0,1]^2$ die Menge der Häufungspunkte von V_q. Nach Manin gibt es eine stetige Funktion $\alpha_q : [0,1] \to [0,1]$, so daß gilt

$$U_q = \{(\delta, R) \mid 0 \leq \delta \leq 1 \text{ und } 0 \leq R \leq \alpha_q(\delta)\}.$$

Weiter ist $\alpha_q(0) = 1$, $\alpha_q(\delta) = 0$ für $1 - 1/q \leq \delta \leq 1$, und α_q ist monoton fallend auf dem Intervall $0 \leq \delta \leq 1 - 1/q$. Mit Hilfe von Goppas Konstruktion algebraisch-geometrischer Codes erhalten wir nun die folgende untere Schranke für α_q. Sei $A(q) > 1$, dann ist

$$\alpha_q(\delta) \geq \left(1 - A(q)^{-1}\right) - \delta \tag{2}$$

für $0 \leq \delta \leq 1 - A(q)^{-1}$ [Sti1]. In dem Fall, daß q ein Quadrat ist, liefert (2) zusammen mit (1)

$$\alpha_q(\delta) \geq \left(1 - \frac{1}{\sqrt{q}-1}\right) - \delta$$

für $0 \leq \delta \leq 1-(\sqrt{q}-1)^{-1}$. Das ist die sogenannte Tsfasman-Vladut-Zink Schranke. Leider beweist dieses Resultat nur die Existenz und gibt keine explizite Konstruktion dieser Codes.

1996 haben Garcia und Stichtenoth zwei Funktionenkörpertürme gefunden [Gar-Sti1], [Gar-Sti2], die die Drinfeld-Vladut Schranke auch erreichen. Diese Türme haben eine explizite und einfache Beschreibung. Für die Konstruktion der auf diesen Funktionenkörpertürmen basierenden Codes braucht man jedoch die Bestimmung einer Basis des Vektorraums $\mathcal{L}(rP)$, der die sämtliche Funktionen mit Polen nur an der Stelle P und Polordnung $\leq r$ enthält.

Im Hauptteil dieser Arbeit beschreiben wir einen neuen Ansatz zur Aufstellung eines Algorithmus, um explizit Basen der Räume $\mathcal{L}(rP)$ in einem der Garcia-Stichtenoth-Türme zu bestimmen.

Wir untersuchen auch die Automorphismen dieser Funktionenkörper und geben einen neuen Beweis dafür, daß der erste von Garcia-Stichtenoth angegebene Funktionenkörperturm die Drinfeld-Vladut-Schranke erreicht.

An dieser Stelle möchte ich mich bei Henning Stichtenoth bedanken. Ohne seine Geduld und Hilfe hätte diese Arbeit nicht entstehen können.

Ich bedanke mich auch bei meinem Vater für alles, was er mich gelehrt und für meine Ausbildung getan hat.

2 Vorbereitungen

Mit einem Funktionenkörper meinen wir im folgenden immer eine Körpererweiterung F/K vom Transzendenzgrad 1, so daß $[F : K(x)]$ endlich ist, für x transzendent über K. Für die grundlegenden Begriffe der Theorie der Funktionenkörper verweisen wir auf [Sti1].

In diesem Abschnitt führen wir die Bezeichnungen ein und erinnern an manche grundlegende Ergebnisse, die wir später brauchen werden. Im folgenden werden wir folgende Bezeichnungen benutzen:

$K = \mathbb{F}_{q^2}$	- der endliche Körper der Kardinalität q^2.
F, E, F_0, F_1, F_2, ...	- algebraische Funktionenkörper einer Variablen über K.
$\mathbb{P}(F)$	- die Menge aller Stellen von F/K.
v_P	- die zu $P \in \mathbb{P}(F)$ zugehörige diskrete Bewertung.
$g(F)$	- das Geschlecht von F/K.
$\mathcal{O}_P$	- der Bewertungsring der Stelle $P \in \mathbb{P}(F)$.
$ic_E(A)$	- der ganze Abschluß eines Unterrings $A \subset E$ in E.
Ω	- $\Omega := \{\gamma \in K \mid \gamma^q + \gamma = 0\}$.
Ω^*	- $\Omega^* := \Omega \setminus \{0\}$.

Sei E/F eine endliche separable Funktionenkörpererweiterung (über K), $P \in \mathbb{P}(F)$ und $P' \in \mathbb{P}(E)$ eine Stelle von E, die über P liegt. Dann bezeichnen wir:

$e(P' \mid P)$	- der Verzweigungsindex von P' über P.
$f(P' \mid P)$	- der relative Grad von P' über P.
$d(P' \mid P)$	- der Differentenexponent von P' über P.
$\mathrm{Diff}(E/F)$	- die Differente von E/F.

Wir schreiben für $x, y \in F$ und $P \in \mathbb{P}(F)$

$$x = y + \mathcal{O}(1) \ \text{ an der Stelle } \ P,$$

wenn $v_P(x - y) \geq 0$.

Wir erinnern an einige Fakten über den zweiten Funktionenkörperturm $\mathcal{F} = (F_0, F_1, F_2, \dots)$ von Garcia und Stichtenoth [Gar-Sti2]. Dieser Turm ist wie folgt definiert:

$$F_0 = \mathbb{F}_{q^2}(x_0) \ \text{ und, für } \ n \geq 1, \quad F_n = F_{n-1}(x_n),$$

wobei x_n die folgende Gleichung erfüllt.

$$x_n^q + x_n = \frac{x_{n-1}^q}{x_{n-1}^{q-1} + 1}$$

Der nächste Satz beschreibt das Verhalten von Stellen in den Erweiterungen F_n/F_{n-1}, siehe [Gar-Sti2, 3.3].

Satz 2.1

i) Sei $P \in \mathbb{P}(F_n)$ ein Pol von x_0 oder eine Nullstelle von $x_0 - \alpha$, für $\alpha \in \Omega^*$. Dann ist P vollverzweigt in der Erweiterung F_n/F_0. Der Differentenexponent $d(P)$ von P bzgl. F_n/F_{n-1} ist gegeben als $d(P) = 2(q-1)$.

ii) Sei $R \in \mathbb{P}(F_n)$ eine Stelle, die weder ein Pol von x_0, noch eine Nullstelle von $x_0 - \gamma$ für alle $\gamma \in \Omega = \Omega^* \cup \{0\}$ ist. Dann ist R unverzweigt in F_n/F_0.

iii) Es gibt genau eine gemeinsame Nullstelle $P_0^{(n)}$ von $x_0, \ldots, x_n$. Sie ist unverzweigt in der Erweiterung F_n/F_0.

Definition 2.2 Für $n \geq 0$ definieren wir

$$S^{(n)} := \{P \in \mathbb{P}(F_n) \mid x_0(P) = 0\},$$

und, für $1 \leq t \leq n$,

$$S_t^{(n)} := \{P \in S^{(n)} \mid x_t(P) = \alpha \in \Omega^*\}.$$

Es gilt insbesondere:

$$S^{(n)} = \bigcup_{1 \leq t \leq n} S_t^{(n)} \cup \{P_0^{(n)}\}.$$

Satz 2.3 *Sei $P \in S_t^{(n-1)}$. Dann gilt*

i) für $1 \leq t < n/2$ ist die Stelle P voll verzweigt in F_n/F_{n-1} und unverzweigt in $F_n/K(x_n)$. Der Differentenexponent $d(P)$ von P in F_n/F_{n-1} ist gegeben als $d(P) = 2(q-1)$;

ii) für $n/2 \leq t < n$ ist P unverzweigt in F_n/F_{n-1}.

Wir werden auch einige Tatsachen über Ganzheitsbasen benötigen (siehe [Chev, IV, §8]):

Lemma 2.4 *Sei E/F eine endliche Funktionenkörpererweiterung vom Grad n. Sei $T \subsetneq \mathbb{P}(F)$ eine Untermenge von $\mathbb{P}(F)$. Dann ist $(\gamma_1, \ldots, \gamma_n)$ eine Ganzheitsbasis von $ic_E(\bigcap_{P \in T} \mathcal{O}_P)$ über $\bigcap_{P \in T} \mathcal{O}_P$ genau dann, wenn sie eine Ganzheitsbasis für $ic_E(\mathcal{O}_P)$ über $\mathcal{O}_P$ für alle $P \in T$ ist.*

Lemma 2.5 *Sei E/F eine endliche separable Funktionenkörpererweiterung vom Grad $n := [E : F]$. Für $P \in \mathbb{P}(F)$, sei $\mathcal{O}_{E,P}$ der ganze Abschluß von $\mathcal{O}_P$ in E. Sei weiter $(\alpha_1, \ldots, \alpha_n)$ eine Ganzheitsbasis für P und $\beta_1, \ldots, \beta_n \in \mathcal{O}_{E,P}$. Dann ist $(\beta_1, \ldots, \beta_n)$ eine Ganzheitsbasis für die Stelle P genau dann, wenn*

$$v_P(\Delta(\alpha_1, \ldots, \alpha_n)) = v_P(\Delta(\beta_1, \ldots, \beta_n)).$$

Dabei bezeichnet $\Delta(\alpha_1, \ldots, \alpha_n)$ die Diskriminante von $(\alpha_1, \ldots, \alpha_n)$.

Lemma 2.6 *Sei E/F eine endliche separable Funktionenkörpererweiterung vom Grad $n := [E : F]$, $P \in \mathbb{P}(F)$ eine Stelle von F. Sei ferner $(\alpha_1, \ldots, \alpha_n)$ eine Ganzheitsbasis für P, dann gilt*

$$v_P(\Delta(\alpha_1, \ldots, \alpha_n)) = \sum_{\substack{Q \in \mathbb{P}(E) \\ Q \mid P}} d(Q \mid P) f(Q \mid P).$$

Nach Satz 2.1 besitzt das Element x_0 im Funktionenkörper F_n genau einen Pol, den wir mit $P_\infty^{(n)}$ bezeichnen. Wir beschreiben nun unser Vorgehen für die Konstruktion einer Basis des Vektorraums $\mathcal{L}(rP_\infty^{(n)})$.

Definition 2.7 Sei P_0 bzw. P_∞ die Nullstelle bzw. der Pol von x_0 in F_0. Wir definieren

$$\mathcal{O}_0 := \{z \in F_0 \mid v_P(z) \geq 0 \text{ für alle } P \in \mathbb{P}(F_0) \setminus \{P_0, P_\infty\}\} = K[x_0, x_0^{-1}]$$

und, für $n \geq 1$, sei

$$\mathcal{O}_n := ic_{F_n}(\mathcal{O}_0).$$

Für $n \geq 0$ definieren wir

$$R_n := ic_{F_n}(\mathcal{O}_{P_0}).$$

Die Idee unserer Konstruktion ist es, Ganzheitsbasen für $\mathcal{O}_n$ über $\mathcal{O}_0$ bzw. für R_n über R_0 zu finden, siehe §§ 3 und 4. Daraus kann man dann wegen

$$\mathcal{O}_n \cap R_n = \bigcup_{r \geq 0} \mathcal{L}(rP_\infty^{(n)})$$

Basen der Räume $\mathcal{L}(rP_\infty^{(n)})$ erhalten, für alle $r \geq 0$ und $n \geq 0$.

3 Ganzheitsbasis über P_0

In diesem Abschnitt konstruieren wir eine Ganzheitsbasis von R_n über R_0.

Lemma 3.1 *Sei E/F eine galoissche Erweiterung vom Grad $n := [E : F]$ und $(u_1, \ldots, u_n)$ eine Ganzheitsbasis für $P \in \mathbb{P}(F)$. Seien $w, z_1, \ldots, z_n \in E$ Elemente mit den Eigenschaften*

$$v_{P'}(w) = 0, \; v_{P'}(z_i) > \frac{1}{2} v_{P'}(\Delta(u_1, \ldots, u_n)),$$

für alle Fortsetzungen $P' \in \mathbb{P}(F_n)$ von P und $1 \leq i \leq n$. Dann ist

$$(wu_1 + z_1, \ldots, wu_n + z_n)$$

eine Ganzheitsbasis an der Stelle P.

Beweis.
Seien $\sigma_1, \ldots, \sigma_n$ die verschiedenen Automorphismen von E/F. Sei $Q \in \mathbb{P}(E)$ eine Fortsetzung von P in E. Wir setzen $m := v_Q(\Delta(u_1, \ldots, u_n))$; dann gilt

$$\begin{aligned} \Delta(wu_1 + z_1, \ldots, wu_n + z_n) &= det\,(\sigma_i(wu_j) + \sigma_i(z_j))^2 \equiv \\ \equiv det(\sigma_i(wu_j))^2 &= N_{E/F}(w)^2 \cdot det(u_1, \ldots, u_n)^2 \mod Q^{m+1}, \end{aligned}$$

da $\sigma_i(z_j) \in Q^{[\frac{m}{2}]+1}$ und $2([\frac{m}{2}] + 1) \geq m + 1$. Nach der Dreiecksungleichung bekommt man

$$v_Q\left(\Delta(wu_1 + z_1, \ldots, wu_n + z_n)\right) = v_Q\left(\Delta(u_1, \ldots, u_n)\right).$$

Die Behauptung des Lemmas ergibt sich nach Lemma 2.5.

□

Insbesondere, wenn die Basis aus Potenzen eines Elementes besteht, gilt folgendes:

Lemma 3.2 *Sei $(1, u, \ldots, u^{n-1})$ eine Ganzheitsbasis für $P \in \mathbb{P}(F)$, $z \in E$ ein Element mit*

$$v_{P'}(z) > \frac{1}{2} v_{P'}(\Delta(1, u, \ldots, u^{n-1})),$$

für alle Stellen $P'|P$ in E. Dann ist

$$(1, u + z, \ldots, (u + z)^{n-1})$$

eine Ganzheitsbasis an der Stelle P.

Beweis.
Sei $Q|P$ eine Fortsetzung von P, dann gilt für jedes $1 \leq i \leq n-1$

$$v_Q((z+u)^i - u^i) \geq v_Q(z) > \frac{1}{2} v_Q(\Delta(u_1, \dots, u_n)).$$

Nach Lemma 3.1 ist dann $(1, u+z, \dots, (u+z)^{n-1})$ eine Ganzheitsbasis in P.
□

Sei $n \geq 0$. Wir bemerken, daß

$$R_n = \bigcap_{Q \in S^{(n)}} \mathcal{O}_Q$$

ist (siehe [Sti1, III.2.6]). Deswegen sind wir, als nächstes, interessiert an Ganzheitsbasen in F_n/F_{n-1} für Stellen $Q \in S^{(n-1)}$. Bevor wir aber die allgemeine Situation beschreiben, wollen wir ein paar Lemmata vorausschicken, die wir später für die Konstruktion der Ganzheitsbasis benutzen werden.

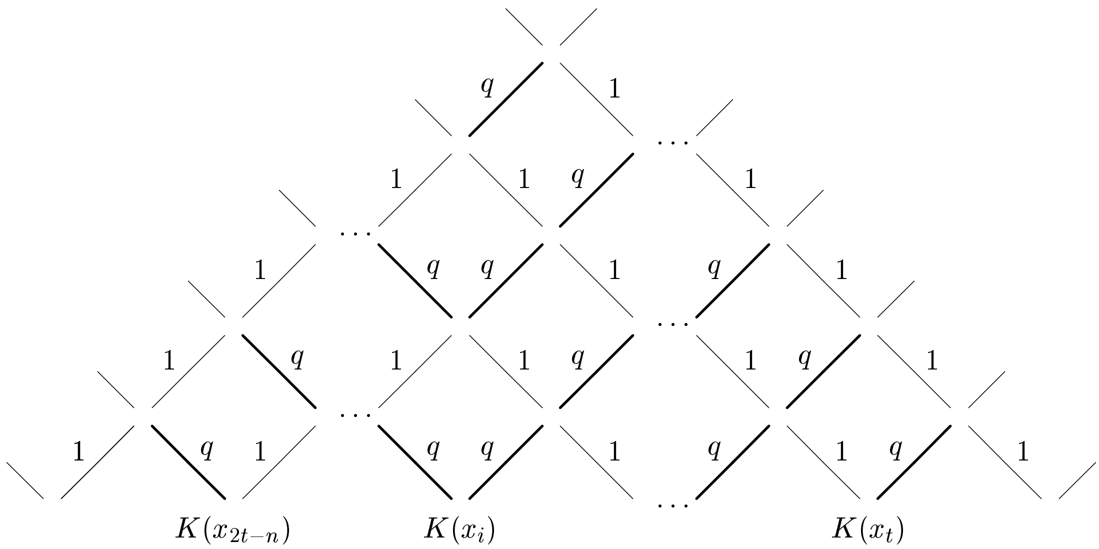

Abbildung 1:

Lemma 3.3 *Sei $Q \in S_i^{(n)}$ mit $1 \leq i < n/2$ und $x_i(Q) = \alpha \in \Omega^*$, dann gilt:*

$$\begin{aligned} v_Q(x_t) &= q^{n-2i+t}, \text{ für alle } 0 \leq t < i, \\ v_Q(x_i) &= 0, \\ v_Q(x_i - \alpha) &= q^{n-i}, \\ v_Q(x_t) &= -q^{n-t}, \text{ für alle } i < t \leq n. \end{aligned}$$

Beweis.
Die Verzweigungsindizes der Einschränkung von Q in den Erweiterungen $K(x_i, x_{i+1})$ über $K(x_i)$, bzw. $K(x_{i+1})$ sind in Abbildung 1 gegeben. Daraus kann man leicht die Behauptung des Satzes ablesen. □

Lemma 3.4 *Sei $Q \in S_j^{(n)}$ mit $n/2 \le j \le n$ und $x_j(Q) = \alpha \in \Omega^*$. Dann gilt:*

$$\begin{aligned} v_Q(x_t) &= q^t, \quad \text{für alle } \ 0 \le t < j, \\ v_Q(x_j) &= 0, \\ v_Q(x_j - \alpha) &= q^j, \\ v_Q(x_t) &= -q^{2j-t}, \quad \text{für alle } \ j < t \le n. \end{aligned}$$

Beweis.
Die Verzweigungsindizes der Einschränkung von Q sind gegeben wie in folgender Abbildung:

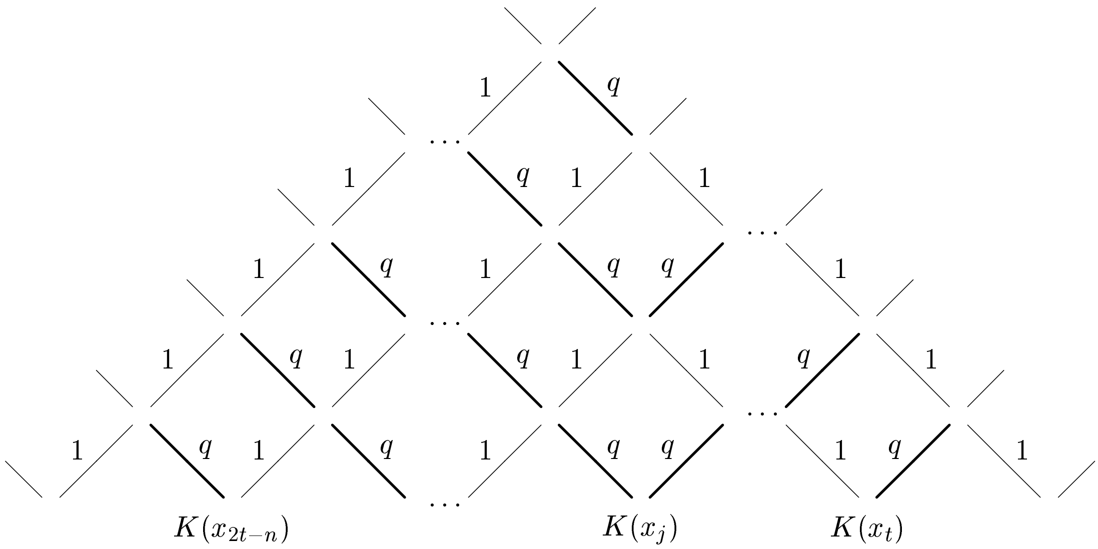

Abbildung 2:

Die Behauptung des Satzes folgt dann aus Abbildung 2.

□

Nun beschreiben wir Ganzheitsbasen von Stellen $P \in S^{(n-1)}$ in der Erweiterung F_n/F_{n-1}.

Lemma 3.5 *Sei $P \in S^{(n-1)}$. Dann gilt:*

i) $\left(1, \frac{1}{x_n}, \dots, \frac{1}{x_n^{q-1}}\right)$ *ist eine Ganzheitsbasis in F_n/F_{n-1} für alle* $P \in \bigcup_{1 \le t < n/2} S_t^{(n-1)}$.

ii) Für $P \in S_t^{(n-1)}$ mit $n/2 \leq t < n$ ist

$$\Big(1, x_n + \frac{x_t^2}{x_{2t-n}}, \ldots , \big(x_n + \frac{x_t^2}{x_{2t-n}}\big)^{q-1}\Big)$$

eine Ganzheitsbasis in F_n/F_{n-1}.

iii) $(1, x_n, \ldots , x_n^{q-1})$ ist eine Ganzheitsbasis in der Erweiterung F_n/F_{n-1} an der Stelle $P_0^{(n-1)}$.

Beweis.
i) Sei $P \in \cup_{1\leq t<n/2} S_t^{(n-1)}$, dann ist P voll verzweigt in F_n/F_{n-1} und $\frac{1}{x_n}$ ist ein lokaler Parameter in P. Es folgt nach [Sti1, III.5.12], daß $\big(1, \frac{1}{x_n}, \ldots , \frac{1}{x_n^{q-1}}\big)$ eine Ganzheitsbasis für P in F_n/F_{n-1} ist.

ii) Sei nun $P \in S_t^{(n-1)}$ mit $x_t(P) = \alpha \in \Omega^*$. Wir haben nach [Gar-Sti2, 3.4]

$$v_Q\Big(x_n + \frac{\alpha^2}{x_{2t-n}}\Big) \geq 0$$

für jede Fortsetzung $Q \in \mathbb{P}(F_n)$ von P. Dann gilt

$$\begin{aligned} v_Q\big(x_n + \frac{x_t^2}{x_{2t-n}}\big) &= v_Q\Big(\big(x_n + \frac{\alpha^2}{x_{2t-n}}\big) + \frac{(x_t-\alpha)(x_t+\alpha)}{x_{2t-n}}\Big) \geq \\ &\geq \min\{0, v_Q(x_t-\alpha) - v_Q(x_{2t-n})\} = \\ &= \min\{0, q^t - q^{2t-n}\} = 0\,. \end{aligned}$$

Das bedeutet, daß das Minimalpolynom

$$\psi(T) = T^q + T - \left(\frac{x_{n-1}^q}{x_{n-1}^{q-1}+1} + \frac{x_t^2}{x_{2t-n}} + \frac{x_t^{2q}}{x_{2t-n}^q}\right)$$

des Elementes $x_n + \dfrac{x_t^2}{x_{2t-n}}$ über F_{n-1} die Koeffizienten in $\mathcal{O}_P$ hat. Wir bemerken, daß die Stelle P unverzweigt in F_n/F_{n-1} ist. Daher gilt

$$v_P\Big(\psi'\big(x_n + \frac{x_t^2}{x_{2t-n}}\big)\Big) = 0 = d(Q\,|\,P)$$

für alle $Q\,|\,P$, und die Behauptung folgt nach [Sti1, III.5.10].

iii) Man kann leicht sehen, daß

$$v_{P_0^{(n-1)}}\left(\frac{x_{n-1}^q}{x_{n-1}^{q-1}+1}\right) > 0.$$

Dann liegen alle Koeffizienten des minimalen Polynoms

$$\phi(T) = T^q + T - \frac{x_{n-1}^q}{x_{n-1}^{q-1} + 1}$$

von x_n über F_{n-1} in $\mathcal{O}_{P_0^{(n-1)}}$. Ähnlich wie in *ii*), da die Stelle $P_0^{(n-1)}$ unverzweigt in F_n/F_{n-1} ist, gilt

$$v_P\big(\phi'(x_n)\big) = 0 = d(Q \mid P_0^{(n-1)})$$

für alle $Q \mid P$. Nach [Sti1, III.5.10] ist $(1, x_n, \ldots, x_n^{q-1})$ eine Ganzheitsbasis an der Stelle $P_0^{(n-1)}$. □

Definition 3.6 Wir bezeichnen

$$y_n := \sum_{n/2 \le j < n} \frac{x_j^2}{x_{2j-n}}.$$

Im nächsten Theorem beschreiben wir Bedingungen, die uns eine gemeinsame Ganzheitsbasis für alle Stellen $Q \in S^{(n-1)}$ zu konstruieren ermöglichen.

Theorem 3.7 *Sei $w \in F_n$ mit folgenden Eigenschaften:*

i) $v_Q(w + x_n + y_n) > q(q-1)$, für alle $Q \in S_t^{(n)}$ mit $1 \le t < n/2$;

ii) $v_Q\Big(w + \dfrac{1}{x_n} + y_n - \dfrac{x_t^2}{x_{2t-n}}\Big) > 0$, für alle $Q \in S_t^{(n)}$ mit $n/2 \le t < n$;

iii) $v_Q\big(w + \dfrac{1}{x_n} + y_n\big) > 0$, für alle $Q \in S_n^{(n)} \cup \{P_0^{(n)}\}$.

Dann ist

$$\Big(1,\ \big(w + x_n + \frac{1}{x_n} + y_n\big), \ldots, \big(w + x_n + \frac{1}{x_n} + y_n\big)^{q-1}\Big)$$

eine Ganzheitsbasis in der Erweiterung F_n/F_{n-1} für jedes $Q \in S^{(n-1)}$.

Beweis.
Es folgt sofort aus Lemma 3.2, Lemma 2.6 und Lemma 3.5.

□

Nun wollen wir ein Element w, das den Bedingungen aus Theorem 3.7 genügt, explizit beschreiben. Zuerst müssen wir aber ein paar Zwischenresultate beweisen.

Definition 3.8 Für $1 \le j \le n$ definieren wir

$$\pi_j := \prod_{i=1}^{j} (x_i^{q-1} + 1),$$

und für $l := [\frac{n-1}{2}]$, $n/2 \leq t < n$, setzen wir

$$u := \frac{\pi_l^2}{\pi_n}, \quad u_t := \frac{(x_t^{q-1}+1)^2}{\pi_{n-1}x_n}.$$

Lemma 3.9 *Es gilt:*

i) $v_Q(u) > 0$, *für alle* $Q \in \bigcup_{1\leq i<n/2} S_i^{(n)}$,
$v_Q(u) < 0$, *für alle* $Q \in \bigcup_{n/2\leq j\leq n} S_j^{(n)}$,
$v_{P_0^{(n)}}(u+1) = 0$, *falls* $char(K) \neq 2$.

ii) *Für* $\frac{n}{2} \leq t < n$
$v_Q(u_t) > 0$, *für alle* $Q \in S_t^{(n)}$,
$v_Q(u_t) < 0$, *für alle* $Q \in S^{(n)} \setminus \big(S_t^{(n)} \bigcup S_n^{(n)}\big)$,
$v_Q(u_t+1) = 0$, *für alle* $Q \in S_n^{(n)}$, *falls* $char(K) \neq 2$.

Beweis.
i) • Sei $x_i(Q) = \alpha \in \Omega^*$ mit $1 \leq i < n/2$. Wir schreiben u als

$$u = \frac{(x_1^{q-1}+1)\cdot\ldots\cdot(x_l^{q-1}+1)}{(x_{l+1}^{q-1}+1)\cdot\ldots\cdot(x_n^{q-1}+1)}.$$

und wenden das Lemma 3.3 an:

$$\begin{aligned} v_Q(u) &= \sum_{j=1}^{l} v_Q(x_j^{q-1}+1) - \sum_{j=l+1}^{n} v_Q(x_j^{q-1}+1) = \\ &= q^{n-i} - (q-1)\big(q^{n-i-1}+\ldots+q^{n-l}\big) + (q-1)\big(q^{n-l-1}+\ldots+1\big) = \\ &= 2q^{n-l}-1 > 0. \end{aligned}$$

• Für $Q \in S^{(n)}$ mit $x_j(Q) = \alpha \in \Omega^*$ $(n/2 \leq j \leq n)$ gilt nach dem Lemma 3.4:

$$v_Q(\pi_l) = 0$$

und folglich

$$\begin{aligned} v_Q(\pi_n) &= q^j - (q-1)\big(q^{2j-(j+1)}+\ldots+q^{2j-n}\big) = \\ &= q^j - (q-1)\big(q^{j-1}+\ldots+q^{j-(n-j)}\big) = \\ &= q^j - q^j + q^{j-(n-j)} = q^{2j-n}. \end{aligned}$$

Das impliziert $v_Q(u) = -v_Q(\pi_n) = -q^{2j-n} < 0$.
• Für $P_0^{(n)}$ gilt

$$\begin{aligned} v_{P_0^{(n)}}(u+1) &= v_{P_0^{(n)}}\big((x_1^{q-1}+1)\cdot\ldots\cdot(x_l^{q-1}+1) + \\ &\quad +(x_{l+1}^{q-1}+1)\cdot\ldots\cdot(x_n^{q-1}+1)\big) = \\ &= v_{P_0^{(n)}}\big(2+\sum_{i=1}^{n} x_i^{q-1} + \text{ höhere Potenzen}\big) = 0, \end{aligned}$$

falls $char(K) \neq 2$.

ii) • Sei $x_t(Q) = \alpha \in \Omega^*$ mit $n/2 \leq t < n$, dann gilt nach Lemma 3.4

$$\begin{aligned} v_Q(u_t) &= v_Q(x_t - \alpha) - (q-1)\sum_{i=t+1}^{n-1} v_Q(x_i - \alpha) - v_Q(x_n) = \\ &= q^t + (q-1)\big(q^{t-1} + \ldots + q^{2t-n+1}\big) + q^{2t-n} > 0. \end{aligned}$$

• Ferner sei $Q \in S^{(n)}$ mit $x_i(Q) = \alpha \in \Omega^*$, $1 \leq i < t$. Wir betrachten zuerst den Fall $1 \leq i < n/2 \leq t$. Es gilt

$$\begin{aligned} v_Q(\pi_{n-1}) &= q^{n-i} - (q-1)\big(q^{n-(i+1)} + \ldots + q\big) = \\ &= q^{n-i} - q^{n-i} + q = q, \end{aligned}$$

und folglich ist

$$v_Q(u_t) = 2v_Q(x_t^{q-1} + 1) - v_Q(\pi_{n-1}) - v_Q(x_n) = -2(q-1)q^{n-t} - q - 1 < 0.$$

Im Fall $1 < n/2 \leq i < t$ gilt

$$\begin{aligned} v_Q(\pi_{n-1}) &= q^i - (q-1)\big(q^{2i-(i+1)} + \ldots + q^{2i-(n-1)}\big) = \\ &= q^i - q^i + q^{2i-n+1} = q^{2i-n+1}. \end{aligned}$$

Dann ist

$$\begin{aligned} v_Q(u_t) &= 2v_Q(x_t^{q-1} + 1) - v_Q(\pi_{n-1}) - v_Q(x_n) = \\ &= -2(q-1)q^{2i-t} - q^{2i-n+1} + q^{2i-n} < 0. \end{aligned}$$

Sei nun $Q \in S^{(n)}$ mit $x_j(Q) = \alpha \in \Omega^*$, $t < j < n$, dann hat man

$$\begin{aligned} v_Q(u_t) &= -\sum_{i=j}^{n-1} v_Q(x_i^{q-1} + 1) - v_Q(x_n) = \\ &= -\Big(q^j - (q-1)\big(q^{j-1} + \ldots + q^{2j-n+1}\big) - q^{2j-n}\Big) = \\ &= -\big(q^j - q^j + q^{2j-n+1} - q^{2j-n}\big) = q^{2j-n} - q^{2j-n+1} < 0. \end{aligned}$$

Für $P_0^{(n)}$ ist es leicht zu sehen, daß $v_{P_0^{(n)}}(u_t) = -q^n < 0$.

• Schließlich, für $Q \in S_n^{(n)}$ mit $x_n(Q) = \alpha \in \Omega^*$ gilt

$$\begin{aligned} v_Q(u_t + 1) &= v_Q\big((x_t^{q-1} + 1)^2 + \pi_{n-1}x_n\big) = \\ &= v_Q\big((x_t^{q-1} + 1)^2 + \alpha\pi_{n-1} + \pi_{n-1}(x_n - \alpha)\big) = \\ &= v_Q\big((1+\alpha) + (x_n - \alpha)\pi_{n-1} + R(x_1, \ldots, x_{n-1})\big) = 0, \end{aligned}$$

(falls $char(K) \neq 2$) wobei $R(x_1, \ldots, x_{n-1})$ ein Polynom in $K[x_1, \ldots, x_{n-1}]$ ist und $R(0, \ldots, 0) = 0$. Das beweist das Lemma. □

Lemma 3.10 *Für $Q \in S^{(n)}$, $n/2 \le t < n$ gilt*

$$v_Q(x_n) \ge -q^n,\ v_Q\left(\frac{1}{x_n}\right) \ge -q^n \ \text{ und } \ v_Q\left(\frac{x_t^2}{x_{2t-n}}\right) \ge -q^n.$$

Insbesondere hat man

$$v_{P_0^{(n)}}(x_n) = q^n$$

und, für $Q \in S_n^{(n)} \cup \{P_0^{(n)}\}$,

$$v_Q(y_n) = 2q^{\left[\frac{n+1}{2}\right]} - q^{2\left[\frac{n+1}{2}\right]-n}.$$

Beweis.
Es ist klar für x_n und $\dfrac{1}{x_n}$.

Die Bewertungen des Elementes $x_n + \dfrac{x_t^2}{x_{2t-n}}$ $(n/2 \le t < n)$ bei $Q \in S^{(n)}$ lassen sich mit Hilfe des Lemmas 3.3 und 3.4 berechnen:

$$v_Q\left(\frac{x_t^2}{x_{2t-n}}\right) \ge$$

$$\ge \begin{cases} -2q^{n-t} + q^{2n-2t}, \text{ falls } Q \in S_l^{(n)} \text{ und } 1 \le l < 2t-n < t < n; \\ -2q^{n-t}, \text{ falls } Q \in S_{2t-n}^{(n)}; \\ -2q^{n-t} - q^{2t-2l}, \text{ falls } Q \in S_l^{(n)} \text{ und } 1 < 2t-n < l < n/2 < t < n; \\ -2q^{2l-t} - q^{2t-n}, \text{ falls } Q \in S_l^{(n)} \text{ und } 1 < 2t-n \le n/2 \le l < t < n; \\ -q^{2t-n}, \text{ falls } Q \in S_t^{(n)}; \\ 2q^t - q^{2t-n}, \text{ falls } Q \in S_l^{(n)} \text{ und } 1 < 2t-n < t < l \le n; \\ -2q^{2l-t} - q^{2l-2t+n}, \text{ falls } Q \in S_l^{(n)} \text{ und } 1 < n/2 \le l < 2t-n < t < n; \\ 2q^t - q^{2t-n}, \text{ falls } Q = P_0^{(n)}. \end{cases}$$

In jedem Fall ist also $v_Q\left(\dfrac{x_t^2}{x_{2t-n}}\right) \ge -q^n$.

Schließlich, für $Q \in S_n^{(n)} \cup \{P_0^{(n)}\}$ ist die Folge

$$\left(v_Q\left(\frac{x_i^2}{x_{2i-n}}\right)\right)_{\left[\frac{n+1}{2}\right] \le i \le n-1} = \left(2q^i - q^{2i-n}\right)_{\left[\frac{n+1}{2}\right] \le i \le n-1}$$

monoton steigend. Das beweist, daß

$$v_Q(y_n) = 2q^{\left[\frac{n+1}{2}\right]} - q^{2\left[\frac{n+1}{2}\right]-n}.$$

$\square$

Definition 3.11 Wir definieren

$$\xi := \Big(\frac{1}{1+u}\Big)^{q^{n+1}}, \ \chi := \Big(\frac{1}{x_n^q + x_n + 1}\Big)^{q^{n+1}},$$

und, für $n/2 \leq t < n$,

$$\eta_t := \Big(\frac{1}{1+u_t}\Big)^{q^{n+1}}.$$

Lemma 3.12 *Sei T/K ein Funktionenkörper, und Γ_1, Γ_2 seien disjunkte Teilmengen von $\mathbb{P}(T)$. Sei weiter $z \in T$ mit*

$$\begin{aligned} v_P(z) > 0 \quad &, \quad \textit{für alle } \ P \in \Gamma_1, \\ v_P(z) < 0 \quad &, \quad \textit{für alle } \ P \in \Gamma_2. \end{aligned}$$

Wir bezeichnen $\bar{z} := \dfrac{1}{1+z}$. Dann gilt

$$\begin{aligned} v_P(\bar{z} - 1) > 0 \quad &, \quad \textit{für alle } \ P \in \Gamma_1, \\ v_P(\bar{z}) > 0 \quad &, \quad \textit{für alle } \ P \in \Gamma_2. \end{aligned}$$

Beweis.
Für $P \in \Gamma_1$ hat man

$$v_P(\bar{z} - 1) = v_P\Big(\frac{-z}{1+z}\Big) > 0.$$

Ähnlich ist für $P \in \Gamma_2$

$$v_P(\bar{z}) = -v_P(z) > 0.$$

□

Korollar 3.13 *Sei $char(K) \neq 2$. Man hat für die Elemente ξ, η_t $(n/2 \leq t < n)$ und χ:*

i)

$$\begin{aligned} v_Q(\xi - 1) \geq q^{n+1} \quad &, \quad \textit{für alle } \ Q \in \cup_{1 \leq i < n/2} S_i^{(n)}, \\ v_Q(\xi) \geq q^{n+1} \quad &, \quad \textit{für alle } \ Q \in \cup_{n/2 \leq j \leq n} S_j^{(n)}, \\ v_{P_0^{(n)}}(\xi) = 0; & \end{aligned}$$

ii) für $n/2 \leq t < n$

$$\begin{aligned} v_Q(\eta_t - 1) \geq q^{n+1} \quad &, \quad \textit{für alle } \ Q \in S_t^{(n)}, \\ v_Q(\eta_t) \geq q^{n+1} \quad &, \quad \textit{für alle } \ Q \in S^{(n)} \setminus \big(S_t^{(n)} \cup S_n^{(n)}\big), \\ v_Q(\eta_t) = 0 \quad &, \quad \textit{für alle } \ Q \in S_n^{(n)}; \end{aligned}$$

iii)

$$\begin{aligned} v_Q(\chi-1) \geq q^{n+1} \quad &, \quad \textit{für alle } \ Q \in S_n^{(n)} \cup \{P_0^{(n)}\}, \\ v_Q(\chi) \geq q^{n+1} \quad &, \quad \textit{für alle } \ Q \in \cup_{i=1}^{n-1} S_i^{(n)}. \end{aligned}$$

Beweis.
Wegen Lemma 3.9 und Lemma 3.13 genügt es, die Aussage nur für χ zu beweisen. Wir haben

$$v_Q(\chi-1) = q^{n+1} v_Q\Big(\frac{x_n^q + x_n}{x_n^q + x_n + 1}\Big) \geq q^{n+1}, \ \text{ für alle } \ Q \in S_n^{(n)} \cup \{P_0^{(n)}\},$$

und

$$v_Q(\chi) = -q^{n+1} v_Q(x_n^q + x_n + 1) \geq q^{n+1}, \ \text{ für alle } \ Q \in \cup_{i=1}^{n-1} S_i^{(n)}.$$

□

Lemma 3.14 *Sei $T/\mathbb{F}_r$ ein Funktionenkörper und Γ_i, $(1 \leq i \leq m)$ seien disjunkte Teilmengen von $\mathbb{P}(T)$. Sei $z_i \in T$ und $r_i \in \mathbb{Z}$, $(1 \leq i \leq m)$. Seien w_j $(1 \leq j \leq m)$ Elemente in T mit den Eigenschaften*

$$\begin{aligned} v_P(w_j - 1) > r_j - s \quad &, \quad \textit{für alle } P \in \Gamma_j, \\ v_P(w_j) > r_i - s \quad &, \quad \textit{für alle } P \in \Gamma_i, \ i \neq j, \end{aligned}$$

wobei $s = min_{i,j}\{v_P(z_i) \mid P \in \Gamma_j\}$. Wir bezeichnen $z = -\sum_{j=1}^{m} w_j z_j$. Dann ist

$$v_P(z + z_i) > r_i, \ \textit{ für alle } \ P \in \Gamma_i (1 \leq i \leq m).$$

Beweis.
Sei $P \in \Gamma_i$. Dann gilt

$$v_P(z + z_i) = v_P\big(-\sum_{j=1}^{m} w_j z_j + z_i\big) = v_P\Big((z_i - 1) - \sum_{j \neq i}^{m} w_j z_j\Big) > r_i.$$

□

Nun können wir das in Theorem 3.7 erwähnte Element explizit beschreiben.

Satz 3.15 *Das Element*

$$\begin{aligned} w : \ = & \ -x_n\Big(\xi + \sum_{n/2 \leq t < n} \eta_t\Big) - \frac{1}{x_n}\Big(\chi + \sum_{n/2 \leq t < n} \eta_t\Big) - \\ - & \ \ y_n\Big(\xi + \chi + \sum_{n/2 \leq t < n} \eta_t\Big) + \sum_{n/2 \leq t < n} \Big(x_n + \frac{x_t^2}{x_{2t-n}}\Big)\eta_t \end{aligned}$$

erfüllt die Bedingungen von Theorem 3.7.

Beweis.
Wir schreiben das Element w in der Form

$$w = -(x_n + y_n)\xi - (\frac{1}{x_n} + y_n)\chi - \sum_{n/2 \le t < n} \Big(x_n + \frac{1}{x_n} + y_n - \big(x_n + \frac{x_t^2}{x_{2t-n}}\big)\Big)\eta_t.$$

und prüfen die Bedingungen des Theorems 3.7.

Es folgt aus Lemma 3.10, 3.13 und 3.14

i)

$$v_Q(w + x_n + y_n) \ge q^{n+1} - q^n > q(q-1), \quad \text{für alle} \;\; Q \in \bigcup_{1 \le i < n/2} S_i^{(n)},$$

ii)

$$v_Q(w + \frac{1}{x_n} + x_n + y_n - \frac{x_t^2}{x_{2t-n}}) \ge q^{n+1} - q^n > 0, \quad \text{für alle} \;\; Q \in \bigcup_{n/2 \le j < n} S_j^{(n)}.$$

Für $Q \in S_n^{(n)} \cup \{P_0^{(n)}\}$ gilt

$$v_Q\big(w + \frac{1}{x_n} + y_n\big) =$$

$$= v_Q\Bigg(-(x_n + y_n)\xi - (\tfrac{1}{x_n} + y_n)(\chi - 1) - \sum_{n/2 \le t < n} \big(x_n + \frac{1}{x_n} + y_n - \frac{x_t^2}{x_{2t-n}}\big)\eta_t\Bigg) \ge$$

$$\ge \left\{ \begin{array}{l} \min\{2q^{\left[\frac{n+1}{2}\right]} - q^{2\left[\frac{n+1}{2}\right]-n}, \, -q^n + q^{n+1}\}, \;\; \text{falls } Q = P_0^{(n)} \\ \min\{v_Q(y_n) + q^{n+1}, \, -q^n + q^{n+1}, \, v_Q(y_n)\}, \;\; \text{falls } Q \in S_n^{(n)} \end{array} \right\} > 0,$$

d.h. das Element w erfüllt die Bedingungen des Theorems 3.7.

□

Nun betrachten wir den Fall *char* $K = 2$. Wie wir im Satz 3.15 gesehen haben, erfüllt das Element

$$\begin{aligned} w : \; &= \; -x_n\Big(\xi + \sum_{n/2 \le t < n} \eta_t\Big) - \frac{1}{x_n}\Big(\chi + \sum_{n/2 \le t < n} \eta_t\Big) - \\ &- \; y_n\Big(\xi + \chi + \sum_{n/2 \le t < n} \eta_t\Big) + \sum_{n/2 \le t < n} \Big(x_n + \frac{x_t^2}{x_{2t-n}}\Big)\eta_t \end{aligned}$$

die Bedingungen von Theorem 3.7, sobald wir die Elemente $\bar{\xi}$, $\bar{\eta}_t$ $(n/2 \le t < n)$ und $\bar{\chi}$ mit den Eigenschaften i)

$$\begin{aligned} &v_Q(\bar{\xi}-1) \geq q^{n+1}, \quad \text{für alle } \ Q \in \cup_{1\leq i<n/2} S_i^{(n)}, \\ &v_Q(\bar{\xi}) \geq q^{n+1}, \quad \text{für alle } \ Q \in \cup_{n/2\leq j\leq n} S_j^{(n)} \cup \{P_0^{(n)}\}, \end{aligned} \tag{3}$$

ii) für $n/2 \leq t < n$

$$\begin{aligned} &v_Q(\bar{\eta}_t - 1) \geq q^{n+1}, \quad \text{für alle } \ Q \in S_t^{(n)}, \\ &v_Q(\bar{\eta}_t) \geq q^{n+1}, \quad \text{für alle } \ Q \in S^{(n)} \setminus S_t^{(n)}, \end{aligned} \tag{4}$$

iii)

$$\begin{aligned} &v_Q(\bar{\chi}-1) \geq q^{n+1}, \quad \text{für alle } \ Q \in S_n^{(n)} \cup \{P_0^{(n)}\}, \\ &v_Q(\chi) \geq q^{n+1}, \quad \text{für alle } \ Q \in \cup_{i=1}^{n-1} S_i^{(n)} \end{aligned} \tag{5}$$

haben. Wir definieren sie wie folgt:

Definition 3.16 Für $1 \leq l < n$, $\alpha \in \Omega^*$ bezeichnen wir

$$v_{l,\alpha} := (x_l - \alpha)\left(\frac{1}{x_n^q + x_n} + x_n\right), \ w_{l,\alpha} := \frac{1}{1 + v_{l,\alpha}^{q^{n+1}}}$$

und

$$\bar{\xi} := \sum_{1\leq l<n/2} \sum_{\alpha\in\Omega^*} w_{l,\alpha}, \quad \bar{\eta}_t := \sum_{\alpha\in\Omega^*} w_{t,\alpha} \ \ (n/2 \leq t < n),$$

$$\bar{\chi} := \chi = \frac{1}{(x_n^q + x_n + 1)^{q^{n+1}}}.$$

Lemma 3.17 *Die Elemente $\bar{\xi}$, $\bar{\eta}_t$ $(n/2 \leq t < n)$ und $\bar{\chi}$ erfüllen die Bedingungen (3), (4), (5).*

Um das zu beweisen, brauchen wir folgendes Lemma:

Lemma 3.18

$$\frac{1}{x_n^q + x_n} = \sum_{\beta\in\Omega} \frac{1}{x_n - \beta}.$$

Beweis.
Wir haben

$$\sum_{\beta\in\Omega} \frac{1}{x_n - \beta} = \frac{f(x_n)}{x_n^q + x_n},$$

für ein $f(x_n) \in K[x_n]$ mit $deg\ f(x_n) < q$.

Sei $\alpha \in \Omega$, dann gilt

$$1 + \sum_{\substack{\beta \in \Omega \\ \beta \neq \alpha}} \frac{x_n - \alpha}{x_n - \beta} = \frac{f(x_n)}{\prod_{\substack{\beta \in \Omega \\ \beta \neq \alpha}} (x_n - \beta)}$$

und folglich

$$f(\alpha) = \prod_{\substack{\beta \in \Omega \\ \beta \neq \alpha}} (\alpha - \beta).$$

Andererseits gilt

$$\sum_{\gamma \in \Omega} \prod_{\substack{\beta \in \Omega \\ \beta \neq \gamma}} (x_n - \beta) = \left(\prod_{\beta \in \Omega} (x_n - \beta) \right)' = \left(x_n^q + x_n \right)' = 1.$$

Dies impliziert

$$\prod_{\substack{\beta \in \Omega \\ \beta \neq \alpha}} (\alpha - \beta) = f(\alpha) = 1,$$

für alle $\alpha \in \Omega$. Da *deg* $f(x_n) < q$ und $|\Omega| = q$, bekommen wir $f(x_n) = 1$.

□

Beweis des Lemmas 3.17.
Wir schreiben das Element $v_{t,\alpha}$ in der Form

$$v_{t,\alpha} = (x_t - \alpha) \left(\sum_{\beta \in \Omega} \frac{1}{x_n - \beta} + x_n \right).$$

Jetzt sieht man, daß

$$\begin{aligned} v_Q(v_{t,\alpha}) > 0, \quad &\text{für} \quad Q \in S_t^{(n)} \quad \text{mit} \quad x_t(Q) = \alpha, \\ v_Q(v_{t,\alpha}) < 0, \quad &\text{für} \quad Q \in S^{(n)} \quad \text{mit} \quad x_t(Q) \neq \alpha. \end{aligned}$$

Dann gilt für $w_{t,\alpha}$ nach Lemma 3.12

$$\begin{aligned} v_Q(w_{t,\alpha} - 1) \geq q^{n+1}, \quad &\text{für} \quad Q \in S_t^{(n)} \quad \text{mit} \quad x_t(Q) = \alpha, \\ v_Q(w_{t,\alpha}) \geq q^{n+1}, \quad &\text{für} \quad Q \in S^{(n)} \quad \text{mit} \quad x_t(Q) \neq \alpha. \end{aligned}$$

Für $\bar{\chi}$ gilt die Aussage nach Korollar 3.13.

□

Nachdem wir eine Ganzheitsbasis für R_n über R_{n-1} berechnet haben, kann man leicht eine Ganzheitsbasis für R_n über R_0 erhalten, indem man Produkte von Basiselementen bildet. Dazu benötigen wir das folgende Lemma, dessen Beweis trivial ist.

Lemma 3.19 *Für $1 \leq i \leq n$ sei $(w_1^{(i)}, \dots, w_q^{(i)})$ eine Ganzheitsbasis von R_i/R_{i-1}. Dann bilden die Elemente*

$$\prod_{i=1}^{n} w_{j_i}^{(i)}, \quad 1 \leq j_i \leq q$$

eine Ganzheitsbasis von R_n/R_0.

4 Ganzheitsbasis außerhalb P_0 und P_∞

In diesem Abschnitt konstruieren wir eine Ganzheitsbasis für $\mathcal{O}_n$ über $\mathcal{O}_0$. In anderen Worten, wir finden eine Ganzheitsbasis in F_n/F_0 für alle Stellen Q, die weder ein Pol noch eine Nullstelle von x_0 sind.

Unsere Konstruktion basiert auf folgendem Satz ([Sti1, III.3.4]):

Lemma 4.1 *Sei F/K ein Funktionenkörper, E/F sei eine endliche separable Funktionenkörpererweiterung vom Grad n. Sei R ein ganzabgeschlossener Unterring von F mit Quotientenkörper F. Ist $(z_1, \dots, z_n)$ eine Basis von E/F mit $z_i \in ic_E(R)$ und $(z_1^*, \dots, z_n^*)$ seine duale Basis, dann gilt:*

$$\sum_{i=1}^{n} Rz_i \subset ic_E(R) \subset \sum_{i=1}^{n} Rz_i^*.$$

Lemma 4.2 *Sei K ein Körper der Charakteristik $p > 0$, und $L = K(\alpha)$ mit*

$$\alpha^q + \alpha \in K \;\; \textit{und} \;\; [L : K] = q = p^r.$$

Dann ist $(1, \alpha, \dots, \alpha^{q-1})$ die duale Basis zur Basis $(1 + \alpha^{q-1}, \alpha^{q-2}, \dots, \alpha, 1)$.

Beweis.
Das Minimalpolynom von α über K ist

$$\varphi(T) = T^q + T - \gamma \in K[T].$$

Da $\varphi(\alpha) = 0$, gilt

$$\varphi(T) = (T - \alpha)(T^{q-1} + \alpha T^{q-2} + \ldots + \alpha^{q-2}T + (1 + \alpha^{q-1})),$$

und nach [Sti1, III.5.10] ist $(1 + \alpha^{q-1}, \alpha^{q-2}, \dots, \alpha, 1)$ die duale Basis zu Basis $(1, \alpha, \dots, \alpha^{q-1})$. □

Lemma 4.3 *Seien M/L und L/K separable Körpererweiterungen von endlichem Grad. Seien $(\alpha_1, \dots, \alpha_s)$ bzw. $(\beta_1, \dots, \beta_t)$ Basen von M/L bzw. L/K. Wir bezeichnen $(\alpha_1^*, \dots, \alpha_s^*)$ bzw. $(\beta_1^*, \dots, \beta_t^*)$ ihre duale Basen. Dann ist*

$$\{\alpha_i^* \, \beta_j^* \,|\, 1 \le i \le s,\, 1 \le j \le t\}$$

die duale Basis von

$$\{\alpha_i \, \beta_j \,|\, 1 \le i \le s,\, 1 \le j \le t\}$$

in der Erweiterung M/K.

Beweis.
Wir bezeichnen mit $\mathrm{Tr}_{M/L}$, $\mathrm{Tr}_{L/K}$ und $\mathrm{Tr}_{M/K}$ die Spurabbildungen bzgl. M/L, L/K und M/K; dann haben wir für $1 \leq i,k \leq s$ und $1 \leq j,l \leq t$

$$\begin{aligned} \mathrm{Tr}_{M/K}\big((\alpha_i\beta_j)(\alpha_k^*\beta_l^*)\big) &= \mathrm{Tr}_{L/K}\big((\beta_j\beta_l^*)\mathrm{Tr}_{M/L}(\alpha_i\alpha_k^*)\big) = \\ \mathrm{Tr}_{L/K}\big((\beta_j\beta_l^*)\delta_{ik}\big) &= \delta_{ik}\delta_{jl}, \end{aligned}$$

wobei δ_{ik} das Kronecker Symbol bezeichnet.

□

Wir kommen nun zurück zu dem Funktionenkörperturm $\mathcal{F} = (F_0, F_1, F_2, \dots)$ aus §2.

Definition 4.4 Wir definieren

$$\begin{aligned} u_{1,0} &:= (x_0^{q-1}+1)(x_1^{q-1}+1) \\ u_{1,1} &:= (x_0^{q-1}+1)x_1^{q-2} \\ &\vdots \\ u_{1,q-2} &:= (x_0^{q-1}+1)x_1 \\ u_{1,q-1} &:= (x_0^{q-1}+1), \end{aligned}$$

und, für $2 \leq i \leq n$,

$$\begin{aligned} u_{i,0} &:= x_i^{q-1}+1 \\ u_{i,1} &:= x_i^{q-2} \\ &\vdots \\ u_{1,q-1} &:= 1. \end{aligned}$$

Sei

$$\mathcal{E}_n := \{\underline{\nu} = (\nu_1, \dots, \nu_n) \,|\, 0 \leq \nu_i \leq q-1\}.$$

Für $\underline{\nu} = (\nu_1, \dots, \nu_n) \in \mathcal{E}_n$ setzen wir

$$u_{\underline{\nu}} := \prod_{i=1}^{n} u_{i,\nu_i}.$$

Lemma 4.5 *Die Familie $(u_{\underline{\nu}} \,|\, \underline{\nu} \in \mathcal{E}_n)$ ist eine Basis von F_n/F_0. Ihre duale Basis $(u_{\underline{\nu}}^* \,|\, \underline{\nu} \in \mathcal{E}_n)$ ist gegeben durch*

$$u_{\underline{\nu}}^* = \frac{1}{x_0^{q-1}+1}\prod_{i=1}^{n} x_i^{\nu_i}.$$

Beweis.
Dies folgt offensichtlich aus Lemma 4.2 und 4.3. □

Lemma 4.6 *$u_{\underline{\nu}} \in \mathcal{O}_n$ für alle $\underline{\nu} \in \mathcal{E}_n$.*

Beweis.
Die Elemente $u_{\underline{\nu}}$ lassen sich in der Form $u_{\underline{\nu}} = (x_0^{q-1}+1)\, f(x_1, \ldots, x_n)$ beschreiben, mit Polynomen $f(x_1, \ldots, x_n) \in K[x_1, \ldots, x_n]$.

Sei $Q \in \mathbb{P}(F_n)$ mit $Q \cap F_0 \neq P_0$, P_∞. Dann gilt:
i) Ist $Q \cap F_0$ keine Nullstelle von $x_0^{q-1}+1$, dann ist Q kein Pol von $x_1, \ldots, x_n$ (ein Pol von x_j muß entweder ein Pol von x_0 oder eine Nullstelle von $x_0^q + x_0$ sein). Daraus folgt, daß $f(x_1, \ldots, x_n) \in \mathcal{O}_Q$ und daher $u_{\underline{\nu}} \in \mathcal{O}_Q$.
ii) Ist $Q \cap F_0$ eine Nullstelle von $x_0 - \alpha$ mit $\alpha \in \Omega^*$, dann ist $v_Q(x_0^{q-1}+1) = q^n$ und $v_Q(x_j) = -q^{n-j}$ für $1 \leq j \leq n$. Es folgt

$$\begin{aligned} v_Q(u_{\underline{\nu}}) = q^n - (q-1-\nu_1)q^{n-1} - (q-1-\nu_2)q^{n-2} - \ldots - (q-1-\nu_n) \geq \\ \geq q^n - (q-1)(q^{n-1} + q^{n-2} + \ldots + 1) = 1, \end{aligned}$$

d.h. $u_{\underline{\nu}} \in \mathcal{O}_Q$.

Wir bemerken, daß

$$\mathcal{O}_n = \bigcap_{\substack{Q \in \mathbb{P}(F_n) \\ Q \cap F_0 \neq P_0, P_\infty}} \mathcal{O}_Q$$

(siehe [Sti1, III.2.6]). Das beweist das Lemma. □

Lemma 4.7

$$\mathcal{O}_n \subset \sum_{\underline{\nu} \in \mathcal{E}_n} \mathcal{O}_0 u_{\underline{\nu}}^* = \frac{1}{x_0^{q-1}+1} \sum_{\underline{\nu} \in \mathcal{E}_n} K[x_0, x_0^{-1}] \prod_{i=1}^{n} x_i^{\nu_i}.$$

Beweis. Nach Lemma 4.6 ist

$$\sum_{\underline{\nu} \in \mathcal{E}_n} \mathcal{O}_0 u_{\underline{\nu}} \subset \mathcal{O}_n.$$

Dann folgt die Behauptung des Lemmas aus Lemma 4.1.

□

Im nächsten Theorem werden wir eine Ganzheitsbasis von $\mathcal{O}_n$ über $\mathcal{O}_0 = K[x_0, x_0^{-1}]$ ausrechnen.

Theorem 4.8

$$\mathcal{O}_n = \mathcal{O}_0 + (x_0^{q-1}+1) \sum_{\underline{0} \neq \underline{\nu} \in \mathcal{E}_n} \mathcal{O}_0 \prod_{i=1}^{n} x_i^{\nu_i}.$$

Beweis. Sei $z \in \mathcal{O}_n$. Nach Lemma 4.7 gilt

$$z = x_0^{-N} \sum_{\underline{\nu} \in \mathcal{E}_n} \frac{f_{\underline{\nu}}(x_0)}{x_0^{q-1}+1} \prod_{i=1}^{n} x_i^{\nu_i},$$

mit einem $N \in \mathbb{Z}$ und Polynomen $f_{\underline{\nu}}(x_0) \in K[x_0]$.

Sei $Q \in \mathbb{P}(F_n)$ mit $v_Q(x_0^{q-1}+1) > 0$. Dann gilt $v_Q(x_0^{q-1}+1) = q^n$ und

$$v_Q(\prod_{i=1}^{n} x_i^{\nu_i}) = -\sum_{i=1}^{n} \nu_i q^{n-i}.$$

Diese Werte sind paarweise inkongruent modulo q^n.

Wegen $v_Q(z) \geq 0$ und $v_Q(x_0^{-N}) = 0$, folgt

$$v_Q\left(\frac{f_{\underline{0}}(x_0)}{x_0^{q-1}+1}\right) \geq 0$$

und

$$v_Q\left(\frac{f_{\underline{\nu}}(x_0)}{x_0^{q-1}+1}\right) > 0$$

für alle $\underline{\nu} \neq \underline{0}$. Das impliziert $(x_0^{q-1}+1) \mid f_{\underline{0}}(x_0)$ und $(x_0^{q-1}+1)^2 \mid f_{\underline{\nu}}(x_0)$ für $\underline{\nu} \neq \underline{0}$. Daraus folgt, daß

$$\mathcal{O}_n \subset \mathcal{O}_0 + (x_0^{q-1}+1) \sum_{\underline{0} \neq \underline{\nu} \in \mathcal{E}_n} \mathcal{O}_0 \prod_{i=1}^{n} x_i^{\nu_i}.$$

Die inverse Inklusion liefert uns das Lemma 4.6. □

Korollar 4.9 *Für alle $P \neq P_0,\, P_\infty$ bilden die Elemente*

$$w_{\underline{\nu}} := \begin{cases} 1, & \text{für } \underline{\nu} = \underline{0} \\ (x_0^{q-1}+1)\prod_{i=1}^{n} x_i^{\nu_i}, & \text{für } \underline{\nu} = (\nu_1, \ldots, \nu_n) \neq \underline{0} \end{cases}$$

eine Ganzheitsbasis an der Stelle P. Ihre duale Basis $(w_{\underline{\nu}}^* \mid \underline{\nu} \in \mathcal{E}_n)$ ist gegeben als

$$w_{\underline{\nu}}^* := \begin{cases} (x_0^{q-1}+1)^{-1} u_{\underline{0}}, & \text{für } \underline{\nu} = \underline{0} \\ (x_0^{q-1}+1)^{-2} u_{\underline{\nu}}, & \text{für } \underline{\nu} \neq \underline{0}. \end{cases}$$

Bemerkung 4.10 Für den Ring

$$\mathcal{Q}_n := \bigcup_{r \geq 1} \mathcal{L}(rP_\infty^{(n)})$$

gilt $\mathcal{Q}_n \subset \mathcal{O}_n$ (siehe Abschnitt 2), d.h. jedes $z \in \mathcal{Q}_n$ kann geschrieben werden, als

$$z = \sum_{\underline{\nu} \in \mathcal{E}_n} g_{\underline{\nu}}(x_0) w_{\underline{\nu}}$$

mit $g_{\underline{\nu}}(x_0) \in K[x_0,\, x_0^{-1}]$. In anderen Worten,

$$g_{\underline{\nu}}(x_0) x_0^a \in K[x_0] \text{ für ein } a \in \mathbb{N}.$$

Wir wollen den Exponenten a abschätzen.

Lemma 4.11 *Sei $Q \in \mathbb{P}(F_n)$ eine Fortsetzung von P_0. Dann gilt*

$$v_Q(u_{\underline{\nu}}) \geq -(q^{n-1}-1) \text{ für alle } \underline{\nu} \in \mathcal{E}_n.$$

Beweis.
Zuerst betrachten wir den Fall $v_Q(x_n) \geq 0$. Dann $v_Q(x_i) > 0$, für alle $0 \leq i \leq n-1$, und folglich $v_Q(u_{\underline{\nu}}) \geq 0$.

Sei nun $Q \in \mathbb{P}(F_n)$ mit $v_Q(x_n) < 0$. Da $v_Q(x_0) > 0$, existiert genau ein j $(1 \leq j \leq n-1)$, sodaß Q eine Nullstelle von $x_j - \alpha$ mit $\alpha^{q-1}+1 = 0$ ist. Dann ist $v_Q(x_i) > 0$ für $0 \leq i < j$, und $v_Q(x_{j+i}) \geq -q^{n-i-1}$ für $1 \leq i \leq n-j$. Das liefert uns

$$v_Q(u_{\underline{\nu}}) \geq -(q-1)(q^{n-2}+q^{n-3}+\ldots+1) = -(q^{n-1}-1).$$

□

Lemma 4.12 *Jedes $z \in \mathcal{Q}_n$ kann in der Form*

$$z = x_0^{-(q^{n-1}-1)}\left(h_{\underline{0}}(x_0) + (x_0^{q-1}+1)\sum_{\underline{0}\neq\underline{\nu}\in\mathcal{E}_n} h_{\underline{\nu}}(x_0)\prod_{i=1}^{n} x_i^{\nu_i}\right)$$

dargestellt werden, mit Polynomen $h_{\underline{\nu}}(x_0) \in K[x_0]$.

Beweis.
Wir schreiben $z \in \mathcal{Q}_n$ als

$$z = \sum_{\underline{\nu}\in\mathcal{E}_n} g_{\underline{\nu}}(x_0) w_{\underline{\nu}},$$

mit $g_{\underline{\nu}}(x_0) \in K[x_0, x_0^{-1}]$.

Sei $Q \in \mathbb{P}(F_n)$ eine Fortsetzung der Stelle P_0, $\underline{\mu} \in \mathcal{E}_n$. Dann gilt

$$v_Q(w^*_{\underline{\mu}}) = v_Q(u_{\underline{\mu}}), \quad \text{wegen Korollar 4.9.}$$

Weiter ist

$$v_Q(zw^*_{\underline{\mu}}) = v_Q(zu_{\underline{\mu}}) \geq v_Q(u_{\underline{\mu}}) \geq -(q^{n-1}-1),$$

und folglich gilt

$$v_Q(zx_0^{q^{n-1}-1}w^*_{\underline{\mu}}) \geq 0.$$

Das liefert uns

$$v_{P_0}\big(\mathrm{Tr}_{F_n/F_0}(zx_0^{q^{n-1}-1}w^*_{\underline{\mu}})\big) = v_{P_0}\big(x_0^{q^{n-1}-1}\mathrm{Tr}_{F_n/F_0}(zw^*_{\underline{\mu}})\big) = v_{P_0}(x_0^{q^{n-1}-1}g_{\underline{\mu}}(x_0)) \geq 0.$$

Da $g_{\underline{\nu}}(x_0) \in K[x_0, x_0^{-1}]$, bekommen wir

$$x_0^{q^{n-1}-1}g_{\underline{\mu}}(x_0) \in K[x_0].$$

□

Bemerkung 4.13 Wir bezeichnen als c den Führer der Weierstraß-Halbgruppe von $P_\infty^{(n)}$ und setzen $s := c + q^n$. Ist eine Basis von $\mathcal{L}(sP_\infty^{(n)})$ mit paarweise verschiedenen Polordnungen gegeben, dann ist es leicht zu sehen, wie man eine Basis des Vektorraums $\mathcal{L}(rP_\infty^{(n)})$ für ein beliebiges $r \geq 0$ konstruieren kann. Man multipliziert mit entsprechender Potenz von x_0.

Der Führer ist bekannt (siehe [Pel-Sti-Tor, 2.1]), er ist $< q^{n+1}$. Also wird es ausreichen, den K-Vektorraum $\mathcal{L}((q^{n+1} + q^n - 1)P_\infty^{(n)})$ zu konstruieren, um alle Vektorräume $\mathcal{L}(rP_\infty^{(n)})$ explizit beschreiben zu können.

Theorem 4.14 *Jedes $z \in \mathcal{L}((q^{n+1} + q^n - 1)P_\infty^{(n)})$ kann in der Form*

$$z = x_0^{-(q^{n-1}-1)} \left(h_{\underline{0}}(x_0) + (x_0^{q-1} + 1) \sum_{\underline{0} \neq \underline{\nu} \in \mathcal{E}_n} h_{\underline{\nu}}(x_0) \prod_{i=1}^{n} x_i^{\nu_i} \right)$$

geschrieben werden, wobei $h_{\underline{\nu}}(x_0) \in K[x_0]$ Polynome vom Grad

$$deg\, h_{\underline{\nu}}(x_0) \leq \begin{cases} q^{n-1} + q - 1, & \textit{für } \underline{\nu} = \underline{0} \\ q^{n-1}, & \textit{für } \underline{\nu} \neq \underline{0} \end{cases}$$

sind.

Beweis.
Sei $z \in \mathcal{L}((q^{n+1} + q^n - 1)P_\infty^{(n)}) \subset \mathcal{Q}_n$. Nach Lemma 4.12 existieren Polynome $h_{\underline{\nu}}(x_0) \in K[x_0]$, sodaß

$$z = x_0^{-(q^{n-1}-1)} \left(h_{\underline{0}}(x_0) + (x_0^{q-1} + 1) \sum_{\underline{0} \neq \underline{\nu} \in \mathcal{E}_n} h_{\underline{\nu}}(x_0) \prod_{i=1}^{n} x_i^{\nu_i} \right).$$

Für $0 \leq i \leq n$ gilt $v_{P_\infty^{(n)}}(x_i) = -q^{n-i}$. Daher sind die Werte

$$v_{P_\infty^{(n)}}(\prod_{i=1}^{n} x_i^{\nu_i}) = -\sum_{i=1}^{n} \nu_i q^{n-i}.$$

paarweise inkongruent modulo q^n. Dann folgt wegen

$$v_{P_\infty^{(n)}}(z) \geq -(q^{n+1} + q^n - 1),$$

daß

$$\begin{aligned} & v_{P_\infty^{(n)}}(x_0^{-(q^{n-1}-1)} h_{\underline{0}}(x_0)) \geq -q^{n+1} - q^n + 1 \\ \Rightarrow\ & (q^{n-1} - 1)q^n - q^n\, deg\, h_{\underline{0}}(x_0) \geq -q^{n+1} - q^n + 1 \\ \Rightarrow\ & q^{n-1} - 1 - deg\, h_{\underline{0}}(x_0) \geq -q \\ \Rightarrow\ & deg\, h_{\underline{0}}(x_0) \leq q^{n-1} + q - 1. \end{aligned}$$

Ähnlich erhalten wir für $\underline{\nu} \neq \underline{0}$:

$$v_{P_\infty^{(n)}}\left(x_0^{-(q^{n-1}-1)}(x_0^{q-1}+1) \sum_{\underline{0}\neq\underline{\nu}\in\mathcal{E}_n} h_{\underline{\nu}}(x_0) \prod_{i=1}^{n} x_i^{\nu_i} \right) \geq -(q^{n+1}+q^n-1)$$

$$\Rightarrow \quad (q^{n-1}-1)q^n - (q-1)q^n - q^n \, deg\, h_{\underline{\nu}}(x_0) - \sum_{i=1}^{n} \nu_i q^{n-i} \geq -(q^{n+1}+q^n-1)$$

$$\Rightarrow \quad q^{n-1} - q - \; deg\, h_{\underline{\nu}}(x_0) \geq -(q+1) + q^{-n}\big(1 + \sum_{i=1}^{n} \nu_i q^{n-i}\big)$$

$$\Rightarrow \quad q^{n-1} + 1 \geq deg\, h_{\underline{\nu}}(x_0) + 1$$

$$\Rightarrow \quad deg\, h_{\underline{\nu}}(x_0) \leq q^{n-1}.$$

□

Bemerkung 4.15 Als nächstes für die Bestimmung einer Basis des Vektorraums $\mathcal{L}(rP_\infty^{(n)})$ braucht man eine Basis des Durchschnitts

$$\mathcal{O}_n \cap R_n = \bigcup_{r\geq 0} \mathcal{L}(rP_\infty^{(n)})$$

über $\mathcal{O}_0 \cap R_0 = K[x_0]$. Danach kann man die Elemente einer solchen Basis nach steigender Polordnung bei $P_\infty^{(n)}$ sortieren und dadurch eine Basis von $\mathcal{L}(rP_\infty^{(n)})$ erhalten.

5 Ein anderer Funktionenkörperturm

In [Gar-Sti1] wurde ein anderer als der in §§ 2–4 betrachtete Funktionenkörperturm über $\mathbb{F}_{q^2}$ untersucht, und es wurde gezeigt, daß auch dieser die Drinfeld-Vladut-Schranke erreicht. In diesem Abschnitt präsentieren wir einen neuen Beweis für diese Tatsache.

Der in [Gar-Sti1] untersuchte Turm $\mathcal{E}$ ist gegeben durch $\mathcal{F} = (F_1, F_2, F_3, \dots)$ mit

$$F_1 := K(x_1)$$

und für $n > 1$ ist

$$F_{n+1} := F_n(z_{n+1}),$$

wobei z_{n+1} die Gleichung

$$z_{n+1}^q + z_{n+1} = x_n^{q+1}, \quad \text{mit } \ x_n := \frac{z_n}{x_{n-1}} \tag{6}$$

erfüllt. Wir setzen $z_{n+1} = x_{n+1}x_n$ in (6) und sehen, daß

$$x_{n+1}^q + x_{n+1}\frac{1}{x_n^{q-1}} = x_n.$$

Wir definieren den Turm $\mathcal{T} = (T_1, T_2, T_3, \dots)$ durch

$$T_n := K(x_1, \dots, x_n)$$

mit der Gleichung

$$x_{i+1}^q + x_{i+1}\frac{1}{x_i^{q-1}} = x_i, \quad \text{für } \ 1 \le i \le n-1;$$

dann gilt also $T_i = F_i$.

Das Hauptresultat dieses Abschnitts ist:

Theorem 5.1 *Der Funktionenkörperturm $\mathcal{T}$ erreicht die Drinfeld-Vladut-Schranke über $\mathbb{F}_{q^2}$, d.h.*

$$\lambda(\mathcal{T}) := \lim_{i\to\infty} \frac{N(T_i)}{g(T_i)} = q - 1.$$

Zur Vorbereitung des Beweises wollen wir folgenden Satz vorausschicken, den wir später noch mehrfach benutzen werden.

Satz 5.2 *Sei der Funktionenkörper $F = K(y, z)$ durch die Gleichung*

$$z^q + z\frac{1}{y^{q-1}} = y \tag{7}$$

definiert. Dann gilt:

i) *Die Erweiterung $F/K(y)$ ist galoissch und*

$$[F : K(y)] = [F : K(z)] = q.$$

ii) *Die Funktion y hat einen einzigen Pol P_∞ in F; die Stelle P_∞ ist vollverzweigt in $F/K(y)$.*

iii) *Die Funktion z hat eine einzige Nullstelle Q_0 in F. Diese Stelle Q_0 ist vollverzweigt in $F/K(z)$.*

iv) *Die Stelle $Q_0 \cap K(y)$ ist voll zerlegt in $F/K(y)$. Sind $Q_0, R_1, \ldots, R_{q-1}$ die sämtliche Erweiterungen von $Q_0 \cap K(y)$ in F, dann sehen die Hauptdivisoren der Funktionen y und z in F wie folgt aus:*

$$\begin{aligned} (y) &= Q_0 + R_1 + \ldots + R_{q-1} - qP_\infty, \\ (z) &= qQ_0 - R_1 - \ldots - R_{q-1} - P_\infty. \end{aligned} \tag{8}$$

v) *Die Stelle P_∞ ist die einzige Stelle in F, die über $K(y)$ verzweigt ist. Ihr Differentenexponent in der Erweiterung $F/K(y)$ ist*

$$d(P_\infty) = q^2 + q - 2.$$

vi) *Die Stelle Q_0 ist die einzige Stelle in F, die über $K(z)$ verzweigt ist. Ihr Differentenexponent in $F/K(z)$ ist gleich*

$$d(Q_0) = q^2 + q - 2.$$

Beweis.
Das Polynom

$$\varphi(T) = T^q + T\frac{1}{y^{q-1}} - y \in K(y)[T]$$

ist irreduzibel über $K(y)$; daher ist $\varphi(T)$ das Minimalpolynom von z in der Erweiterung $F/K(y)$, und der Pol von y ist vollverzweigt in $F/K(y)$, siehe [Sti1, III.1.14]. Insbesondere ist $[F : K(y)] = q$.

Die Nullstellen des Polynoms

$$\varphi(T) = \frac{1}{y^q}\big((yT)^q + (yT) - y^{q+1}\big)$$

sind von der Form $(z + \frac{\alpha}{y})$, wobei $\alpha \in \Omega$. Sie sind alle verschieden und liegen im Körper F. Das bedeutet, daß die Erweiterung $F/K(y)$ galoissch ist.

Das Element y hat folgendes Minimalpolynom in $F/K(z)$:

$$\psi(T) = T^q - T^{q-1}z^q - z.$$

Wir wenden den Satz [Sti1, III.1.14] wieder an und finden, daß z eine einzige Nullstelle Q_0 in F besitzt. Diese ist in $F/K(z)$ vollverzweigt. Damit sind die Aussagen *i*), *ii*) und *iii*) bewiesen.

Nun beweisen wir die Aussage *iv*). Wir setzen $u := zy$. Die Gleichung (7) ist dann äquivalent zu

$$u^q + u = y^{q+1}, \tag{9}$$

und es gilt

$$qv_{P_\infty}(u) = v_{P_\infty}(u^q + u) = (q+1)v_{P_\infty}(y).$$

Daraus folgt

$$v_{P_\infty}(y) = -q, \quad v_{P_\infty}(u) = -(q+1)$$

und schließlich $v_{P_\infty}(z) = -1$.

Ähnlicherweise bekommen wir aus (7) mit Hilfe der Dreiecksungleichung

$$v_{Q_0}(y) = v_{Q_0}(z^q - y) = v_{Q_0}\left(z\frac{1}{y^{q-1}}\right) = v_{Q_0}(z) - (q-1)v_{Q_0}(y),$$

denn $v_{Q_0}(z) = q$ und $v_{Q_0}(y) \leq q$. Also ist $v_{Q_0}(z) = qv_{Q_0}(y)$ und folglich $v_{Q_0}(y) = 1$. Das bedeutet, daß die Stelle Q_0 unverzweigt in $F/K(y)$ ist.

Da Q_0 vollverzweigt in $F/K(z)$ ist, gilt $deg\,(Q_0) = 1$. Wir benutzen die Tatsache, daß die Erweiterung $F/K(y)$ galoissch ist. In diesem Fall gilt

$$q = [F : K(y)] = e(Q_0)f(Q_0)r = r$$

(siehe [Sti1, III.7.2]), wobei r die Anzahl der Erweiterungen von $Q_0 \cap K(y)$ in F ist. Also ist die Stelle $Q_0 \cap K(y)$ voll zerlegt in $F/K(y)$ und der Hauptdivisor des Elements y ist gleich

$$(y) = Q_0 + R_1 + \ldots + R_{q-1} - qP_\infty.$$

Zu *iv*) bleibt es nur noch zu zeigen, daß $v_{R_i}(z) = -1$, für $1 \leq i \leq n-1$. Da Q_0 die einzige Nullstelle von z in F ist, gilt $v_{R_i}(z) \leq 0$ und

$$v_{R_i}(z^q - y) = q\,v_{R_i}(z).$$

Schließlich bekommt man aus (7)

$$q\,v_{R_i}(z) = v_{R_i}(z^q - y) = v_{R_i}(z) - (q-1)v_{R_i}(y)$$

und

$$v_{R_i}(z) = -v_{R_i}(y) = -1.$$

Zu *v*). Sei $P \in \mathbb{P}(F)\backslash\{P_\infty, Q_0, R_1, \ldots, R_{q-1}\}$. Wir zeigen, daß die Stelle P unverzweigt in $F/K(y)$ ist. In der Tat:

das Minimalpolynom $\varphi(T)$ von z über $K(y)$ hat Koeffizienten in $\mathcal{O}_P$, dann folgt nach [Sti1, III.5.10]

$$0 \leq d(P) \leq v_P(\varphi'(z)) = v_P\left(\frac{1}{y^{q-1}}\right) = 0.$$

Nach dem Dedekind'schen Differentensatz (siehe [Sti1, III.5.1]) ist P unverzweigt in der Erweiterung $F/K(y)$.

Nun berechnen wir den Differentenexponenten der Stelle P_∞ in $F/K(y)$. Das Element $t := 1/z$ ist ein lokaler Parameter von P_∞. Sein Minimalpolynom ist gleich

$$\phi(T) = T^q - T^{q-1}\frac{1}{y^q} - \frac{1}{y}.$$

Wir wenden den Satz [Sti1, III.5.12] an und erhalten

$$d(P_\infty) = v_{P_\infty}\left(\phi'(\tfrac{1}{z})\right) = v_{P_\infty}\left(\frac{1}{z^{q-2}} \cdot \frac{1}{y^q}\right) = q^2 + q - 2.$$

Der Beweis von $vi)$ geht ähnlich. Das Element y ist ein lokaler Parameter von Q_0 und sein Minimalpolynom über $K(z)$ ist $\psi(T)$. Dann gilt wieder nach dem Satz [Sti1, III.5.12]

$$d(Q_0) = v_{Q_0}(\psi'(y)) = v_{Q_0}(z^q y^{q-2}) = q^2 + q - 2.$$

□

Der Turm $\mathcal{T} = (T_1, \ldots, T_n)$ hat folgende Eigenschaften:

Satz 5.3

i) $[T_n : K(x_i)] = q^{n-1}$, *für alle* $1 \leq i \leq n$.

ii) Sei $P \in \mathbb{P}(T_n)$ *ein Pol von* x_1 *in* T_n. *Dann ist* P *auch ein Pol der Funktionen* $x_2, x_3, \ldots, x_n$. *Die Stelle* P *ist vollverzweigt in* T_n/T_1 *und unverzweigt in* $T_n/K(x_n)$. *Der Differentenexponent* $d(P)$ *von* P *bezüglich der Erweiterung* T_n/T_{n-1} *ist gegeben durch*

$$d(P) = q^2 + q - 2.$$

iii) Ist $R \in \mathbb{P}(T_n)$ *eine Stelle, die weder ein Pol noch eine Nullstelle von* x_1 *ist, dann ist* R *unverzweigt in* T_n/T_1.

Beweis.
Sei $P \in \mathbb{P}(T_n)$ ein Pol von x_1. Die Einschränkung von P auf T_1 ist vollverzweigt in T_2/T_1 und nach dem Satz 5.2 ein einfacher Pol von x_2. Das Element x_2 hat ein einzigen Pol in $K(x_2, x_3)$. Er ist vollverzweigt in $K(x_2, x_3)/K(x_2)$ und ist ein einfacher Pol von x_3. Per Induktion bekommt man dann heraus, daß P ein gemeinsamer Pol von $x_2, \ldots, x_n$ ist und die Verzweigungsindizes der Einschränkungen von P in den Erweiterungen $K(x_i, x_{i+1})/K(x_i)$ (bzw. $K(x_i, x_{i+1})/K(x_{i+1})$) wie in Abbildung 3 gegeben sind.

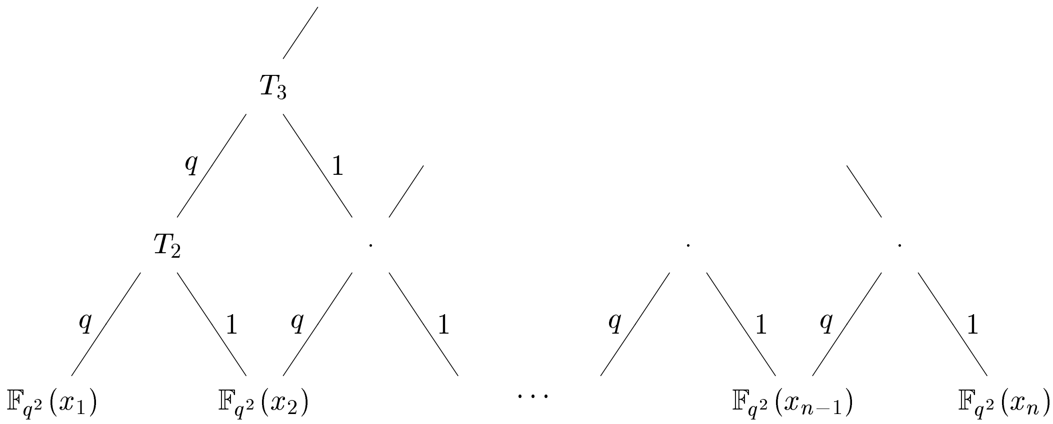

Abbildung 3:

Die folgenden Aussagen ergeben sich aus Satz 5.2 und der obigen Abbildung:

i) P ist vollverzweigt in T_n/T_1 mit dem Verzweigungsindex q^{n-1}.

ii) $[T_n : K(x_i)] = q^{n-1}$ für alle $1 \leq i \leq n$.

iii) P ist unverzweigt in $T_n/K(x_n)$.

iv) Der Differentenexponent von P in der Erweiterung T_n/T_{n-1} ist

$$d(P) = q^2 + q - 2.$$

Sei jetzt $R \in \mathbb{P}(T_n)$, und R sei weder ein Pol noch eine Nullstelle von x_1. Per Induktion kann man leicht mit Hilfe von Satz 5.2 sehen, daß R auch weder ein Pol noch eine Nullstelle von x_i für alle $1 \leq i \leq n-1$ ist. Nun zeigt der Satz 5.2,daß R unverzweigt in allen Einschränkungen $K(x_i, x_{i+1})/K(x_i)$ und $K(x_i, x_{i+1})/K(x_{i+1})$ ist. Folglich ist R unverzweigt in den Erweiterungen $T_n/K(x_i)$ für alle $1 \leq i \leq n-1$.

□

Nach obigem Satz bleibt noch das Verhalten der Nullstellen des Elementes x_1 in der Erweiterung T_n/T_{n-1} zu untersuchen, um den Grad der Differente $\mathrm{Diff}(T_n/T_1)$ bestimmen zu können.

Nach dem Satz 5.2 bekommen wir folgende Möglichkeiten für eine Nullstelle $Q \in \mathbb{P}(T_n)$ von x_1:

a) Q ist eine gemeinsame Nullstelle von $x_1, x_2, \dots, x_n$.

b) Es existiert ein t, $1 \leq t \leq n$ mit

   i) Q ist eine gemeinsame Nullstelle von $x_1, \dots, x_t$,

ii) Q ist gemeinsamer Pol von $x_{t+1}, \dots, x_n$.

(Wir bemerken, daß die Bedingung: *Q ist Nullstelle von x_t und Pol von x_{t+1}* beide *i)* und *ii)* impliziert.)

Im Fall a) hat die Einschränkung von Q in $K(x_i, x_{i+1})$ über $K(x_i)$ (bzw. $K(x_{i+1})$) die folgenden Verzweigungsindizes:

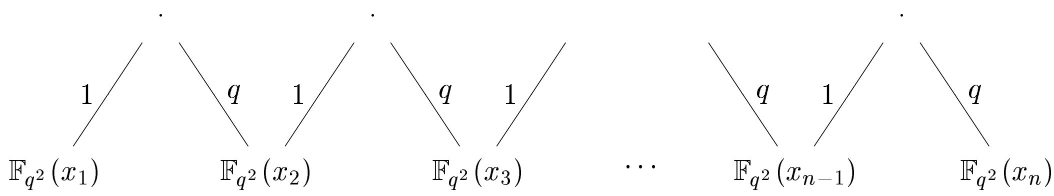

Abbildung 4:

Es folgt dann, daß Q unverzweigt in T_n/T_1 ist. Außerdem ist Q vollverzweigt in der Erweiterung $T_n/K(x_n)$, und Q ist die einzige gemeinsame Nullstelle von $x_1, \dots, x_n$.

Im Fall b) sehen die Verzweigungsindizes der Einschränkung von Q in den Körpern $K(x_i, x_{i+1}, x_{i+2})$ folgenderweise aus:

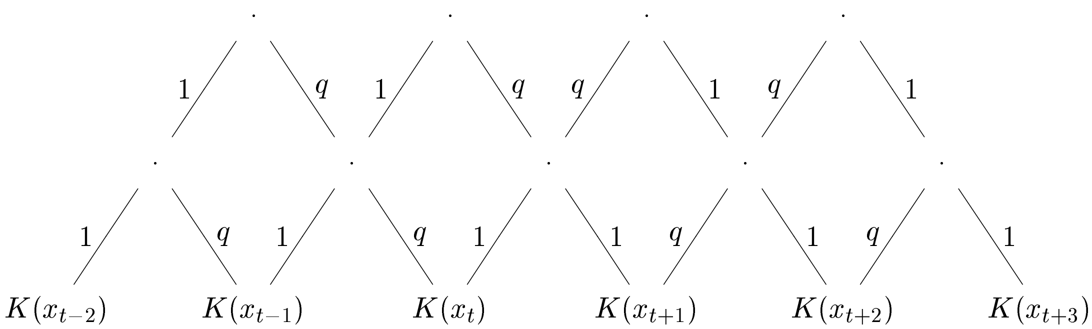

Abbildung 5:

Leider ist es unmöglich, die Verzweigungsindizes von Q in der Erweiterungen $T_n/K(x_i)$ aus diesem Bild für alle i zu bestimmen. Was ist insbesondere der Verzweigungsindex der Einschränkung von Q in

$$K(x_{t-1}, x_t, x_{t+1}, x_{t+2})/K(x_{t-1}, x_t, x_{t+1})?$$

Satz 5.4 *Für $1 \leq k \leq t-1$ definieren wir $E_k := K(x_{t-k}, \dots, x_{t+k})$ und $H_k := E_k(x_{t+k+1})$. Ist $Q \in \mathbb{P}(H_k)$ sowohl eine Nullstelle von x_t, als auch ein Pol von x_{t+1}, dann ist die Stelle Q unverzweigt in H_k/E_k.*

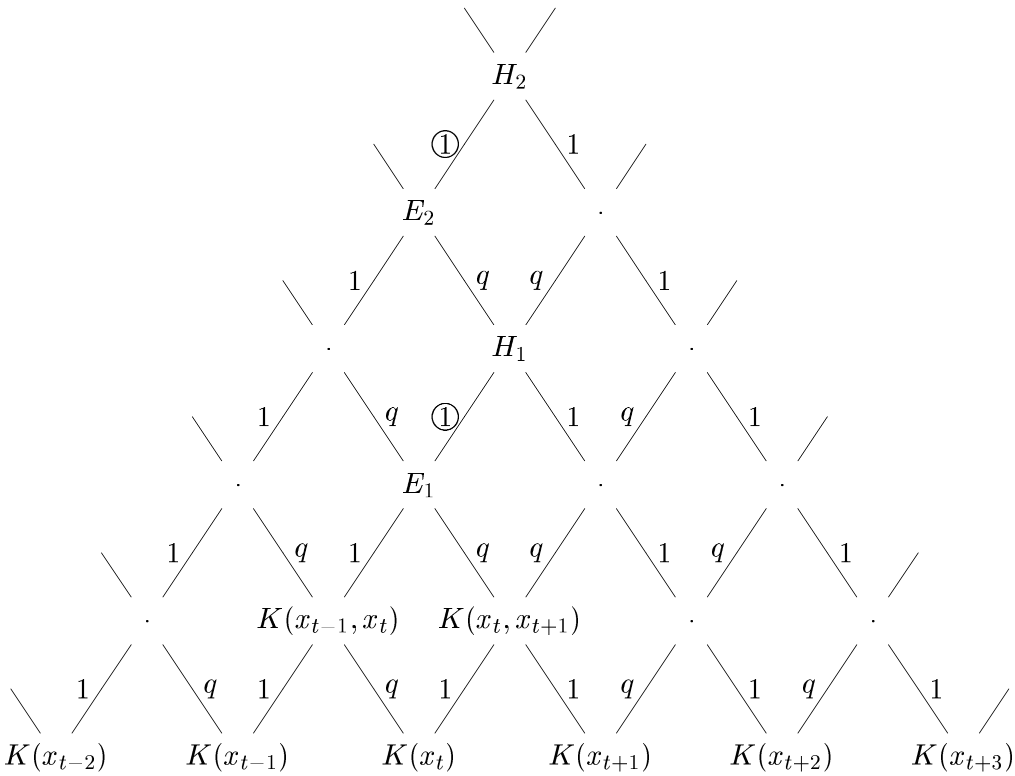

Abbildung 6:

Beweis.
Die eingekreiste ① in der Abbildung 6 ist das Ziel unseres Beweises. Die anderen Verzweigungsindizes von Q erhält man daraus unmittelbar.

Für $1 \leq t \leq n-1$, bezeichnen wir $u_{t+1} := x_{t+1}x_t$. Dann gilt für jedes $z \in E_k$

$$H_k = E_k(u_{t+k+1} - z).$$

Das Minimalpolynom des Elementes $u_{t+k+1} - z$ über E_k ist

$$\varphi(T) = T^q + T - (x_{t+k}^{q+1} - (z^q + z)).$$

Wegen $v_Q(\varphi'(u_{t+k+1} - z)) = v_Q(1) = 0$, bleibt es nur zu zeigen, daß ein $z \in E_k$ mit

$$v_Q((u_{t+k+1} - z)^q + (u_{t+k+1} - z)) = v_Q(x_{t+k}^{q+1} - (z^q + z)) \geq 0$$

existiert, siehe [Sti1, III.5.10].

Für x_t und u_{t+1} haben wir $v_Q(u_{t+1}) = 0$ und $v_Q(x_t) > 0$. Dann folgt aus der Gleichung

$$\prod_{\gamma \in \Omega} (u_{t+1} - \gamma) = u_{t+1}^q + u_{t+1} = x_t^{q+1},$$

daß ein $\alpha \in \Omega^*$ mit $v_Q(u_{t+1} - \alpha) > 0$ existiert.

Wir beweisen durch Induktion über k die folgende Aussage:

$$\left(u_{t+k+1} - \frac{\alpha^{q+1}}{u_{t+1-k}}\right)^q + \left(u_{t+k+1} - \frac{\alpha^{q+1}}{u_{t+1-k}}\right) = \mathcal{O}(1).$$

Daraus folgt dann insbesondere, daß $u_{t+k+1} - \frac{\alpha^{q+1}}{u_{t+1-k}} = \mathcal{O}(1)$.

Für $k = 1$ hat man $H_1 = E_1(u_{t+2})$, und es gilt an der Stelle Q:

$$\begin{aligned}(u_{t+1} - \alpha)^q + (u_{t+1} - \alpha) = u_{t+1}^q + u_{t+1} = x_t^{q+1} = \frac{u_t^{q+1}}{x_{t-1}^{q+1}} = \\ = \frac{u_t^q}{u_t^{q-1} + 1} = u_t^q(1 - u_t^{q-1} + \mathcal{O}(u_t^q)).\end{aligned}$$

Weiter ist

$$\begin{aligned}u_{t+1} - \alpha = u_t^q(1 - u_t^{q-1} + \mathcal{O}(u_t^q)) - (u_{t+1} - \alpha)^q = \\ = u_t^q(1 - u_t^{q-1} + \mathcal{O}(u_t^q)),\end{aligned}$$

und folglich

$$\frac{1}{u_{t+1} - \alpha} = u_t^{-q}(1 + u_t^{q-1} + \mathcal{O}(u_t^q)) = u_t^{-q} + u_t^{-1} + \mathcal{O}(1). \tag{10}$$

Andererseits gilt an der Stelle Q:

$$u_{t+2}^q + u_{t+2} = \frac{(u_{t+1} - \alpha)^q + \alpha^q}{u_{t+1}^{q-1} + 1} = \frac{\alpha^q}{u_{t+1}^{q-1} - 1} + \mathcal{O}(1). \tag{11}$$

Wir schreiben $u_{t+1}^{q-1} + 1 = (u_{t+1} - \alpha)h(u_{t+1})$, wobei $h(u_{t+1})$ ein Polynom vom Grad $q - 2$ ist. Differenzierung dieser Gleichung ergibt:

$$-u_{t+1}^{q-2} = h(u_{t+1}) + (u_{t+1} - \alpha)h'(u_{t+1}),$$

und folglich ist $h(\alpha) = -\alpha^{q-2}$. Da

$$1 - \alpha h(\alpha) = 1 - \alpha(-\alpha^{q-2}) = 1 + \alpha^{q-1} = 0,$$

bekommen wir:

$$\frac{\alpha^q}{u_{t+1}^{q-1} + 1} = \frac{\alpha^q(1 - \alpha h(u_{t+1}))}{u_{t+1}^{q-1} + 1} + \frac{\alpha^{q+1}}{u_{t+1} - \alpha} = \frac{\alpha^{q+1}}{u_{t+1} - \alpha} + \mathcal{O}(1). \tag{12}$$

Endlich liefern (10), (11) und (12) (da $(\alpha^{q+1})^q = \alpha^{q+1}$) das Ergebnis:

$$\begin{aligned} u_{t+2}^q + u_{t+2} &= \frac{\alpha^q}{u_{t+1}^{q-1}+1} + \mathcal{O}(1) = \frac{\alpha^{q+1}}{u_{t+1}-\alpha} + \mathcal{O}(1) = \\ &= \left(\frac{\alpha^{q+1}}{u_t}\right)^q + \frac{\alpha^{q+1}}{u_t} + \mathcal{O}(1). \end{aligned}$$

Sei nun $k \geq 2$, so haben wir an der Stelle Q:

$$\begin{aligned} u_{t+k+1}^q + u_{t+k+1} &= x_{t+k}^{q+1} = \frac{u_{t+k}^q}{u_{t+k}^{q-1}+1} = \frac{u_{t+k}}{1+(u_{t+k}^{-1})^{q-1}} = \\ &= u_{t+k}(1-(u_{t+k}^{-1})^{q-1} + \mathcal{O}(u_{t+k}^{-q})). \end{aligned}$$

Da $v_Q(u_{t+k}) = v_Q(x_{t+k}x_{t+k-1}) < 0$, ist Q eine Nullstelle des Elementes u_{t+k}^{-1}. Dann gilt:

$$u_{t+k+1}^q + u_{t+k+1} = u_{t+k} + \mathcal{O}(1). \tag{13}$$

Andererseits hat man an dieser Stelle:

$$u_{t+2-k}^q + u_{t+2-k} = \frac{u_{t+1-k}^q}{u_{t+1-k}^{q-1}+1} = u_{t+1-k}^q(1 - u_{t+1-k}^{q-1} + \mathcal{O}(u_{t+1-k}^q)).$$

Da $v_Q(u_{t+1-k}) > 0$ ist, gilt

$$u_{t+2-k} = u_{t+1-k}^q(1 - u_{t+1-k}^{q-1} + \mathcal{O}(u_{t+1-k}^q))$$

und

$$u_{t+2-k}^{-1} = u_{t+1-k}^{-q}(1 + u_{t+1-k}^{q-1} + \mathcal{O}(u_{t+1-k}^q)) = u_{t+1-k}^{-q} + u_{t+1-k}^{-1} + \mathcal{O}(1). \tag{14}$$

Nach Induktionsannahme ist

$$u_{t+k} = \frac{\alpha^{q+1}}{u_{t+2-k}} + \mathcal{O}(1), \tag{15}$$

dann liefern (13), (14) und (15)

$$\begin{aligned} u_{t+k+1}^q + u_{t+k+1} &= u_{t+k} + \mathcal{O}(1) = \frac{\alpha^{q+1}}{u_{t+2-k}} + \mathcal{O}(1) = \\ &= \left(\frac{\alpha^{q+1}}{u_{t+1-k}}\right)^q + \frac{\alpha^{q+1}}{u_{t+1-k}} + \mathcal{O}(1). \end{aligned}$$

Das beendet den Beweis des Satzes.

□

Der nächste Satz ist eine direkte Folgerung von Abbildung 6,Satz 5.3 und [Gar-Sti2, 1.2].

Satz 5.5 *Sei $1 \leq t < n$ und $Q \in \mathbb{P}(T_n)$ eine Stelle in T_n mit folgenden Eigenschaften:*

- *Q ist gemeinsame Nullstelle von $x_1, \ldots, x_t$;*
- *Q ist gemeinsamer Pol von $x_{t+1}, \ldots, x_n$.*

Dann gilt:

i) Ist $n \leq 2t$, dann ist Q unverzweigt in der Erweiterung T_n/T_{n-1}.

ii) Für $2t < n$ ist Q ist vollverzweigt in T_n/T_{2t}, und für $2t \leq s \leq n$ ist Q unverzweigt in $T_n/K(x_s)$.

iii) Ist $2t < n$, dann ist der Differentenexponent $d(Q)$ von Q in der Erweiterung T_n/T_{n-1} gleich

$$d(Q) = q^2 + q - 2.$$

Satz 5.6 *Für $1 \leq t < \frac{n}{2}$, definieren wir die Menge*

$X_t := \{Q \in \mathbb{P}(T_n) |\, Q \textit{ ist sowohl eine Nullstelle von } x_t \textit{ als auch ein Pol von } x_{t+1}\}$

und den Divisor

$$A_t := \sum_{Q \in X_t} Q,$$

dann gilt

$$deg\, A_t = (q-1)q^{t-1}.$$

Beweis.
Nach dem Satz 5.2 sind die Hauptdivisoren von x_t und x_{t+1} in $K(x_t, x_{t+1})$ als

$$(x_t) = Q_t + R_t^{(1)} + \ldots + R_t^{(q-1)} - qP_t,$$
$$(x_{t+1}) = qQ_t - R_t^{(1)} - \ldots - R_t^{(q-1)} - P_t$$

gegeben. Dann existiert für jede Stelle Q aus X_t ein $1 \leq i \leq q-1$ so, daß

$$Q \cap K(x_t, x_{t+1}) = R_t^{(i)}.$$

Aus Satz 5.4 und Abbildung 5 kann man sehen, daß der Verzweigungsindex der Einschränkung von Q in der Erweiterung $T_{2t}/K(x_t, x_{t+1})$ gleich q^{t-1} ist. Da die

Stelle Q vollverzweigt in T_n/T_{2t} ist (siehe Satz 5.5), ist $deg\, Q = deg\,(Q \cap T_{2t})$. Also gilt:

$$\begin{aligned} deg\, A_t &= \frac{\sum_{i=1}^{q-1} deg\ \mathrm{Con}_{T_{2t}/K(x_t,x_{t+1})}(R_t^{(i)})}{q^{t-1}} = \\ &= \frac{\sum_{i=1}^{q-1} [T_{2t} : K(x_t, x_{t+1})] deg\,(R_t^{(i)})}{q^{t-1}} = \\ &= \frac{(q-1)q^{2t-2}}{q^{t-1}} = (q-1)q^{t-1}. \end{aligned}$$

□

Lemma 5.7 *Für $n \geq 2$ ist der Grad der Differente* $\mathrm{Diff}(T_n/T_{n-1})$ *der Erweiterung T_n/T_{n-1} gleich*

$$deg\ \mathrm{Diff}(T_n/T_{n-1}) = (q^2 + q - 2)q^{[\frac{n-1}{2}]}.$$

Beweis.
Wir bekommen aus Satz 5.4 *i*), *ii*), Satz 5.5 und Satz 5.6:

$$\begin{aligned} deg\ \mathrm{Diff}(T_n/T_{n-1}) &= (q^2 + q - 2) + \sum_{t=1}^{[\frac{n-1}{2}]} (q-1)q^{t-1}(q^2 + q - 2) \\ &= (q^2 + q - 2)(1 + (q^{[\frac{n-1}{2}]} - 1)) = (q^2 + q - 2)q^{[\frac{n-1}{2}]}. \end{aligned}$$

□

Jetzt betrachten wir Stellen vom Grad 1 im Funktionenkörper T_n/K.

Lemma 5.8 *Für $\alpha \in K$ bezeichnen wir mit $R_\alpha \in \mathbb{P}(T_1)$ die Nullstelle von $x_1 - \alpha$ in T_1. Sei $S := \{R_\alpha \in \mathbb{P}(T_1) \mid \alpha \in K^*\}$. Dann ist jede Stelle $R \in S$ voll zerlegt in allen Erweiterungen T_n/T_1.*

Beweis.
Sei $R \in S$. Wir beweisen die folgende Aussagen durch Induktion über n.

i) R ist voll zerlegt in T_n/T_1.

ii) Für jede Stelle $R' \in \mathbb{P}(T_n)$, die über R liegt, gibt es ein $\alpha \in K^*$ so, daß R' eine Nullstelle von $x_n - \alpha$ ist.

Für $n = 1$ sind die Behauptungen trivial.

Wir nehmen an, daß sie für n gelten. Sei $R' \in \mathbb{P}(T_n)$ eine Stelle, die über $R \in S$ liegt, d.h. es existiert ein $\alpha \in K^*$ so, daß R' eine Nullstelle von $x_n - \alpha$ ist. Weiter gilt $T_{n+1} = T_n(x_{n+1})$, wobei x_{n+1} eine Nullstelle des irreduziblen separablen Polynoms

$$\varphi(T) = T^q + T \cdot \frac{1}{x_n^{q-1}} - x_n \in \mathcal{O}_{R'}[T]$$

ist. Das Restklassenpolynom von $\varphi(T)$ ist gleich

$$\begin{aligned}\bar{\varphi}(T) = T^q + T\,\frac{1}{\alpha^{q-1}} - \alpha &= \frac{1}{\alpha^q}\big((T\alpha)^q + (T\alpha) - \alpha^{q+1}\big) = \\ &= \frac{1}{\alpha^q} \cdot \prod_{\gamma \in Tr^{-1}_{K/\mathbb{F}_q}(\alpha^{q+1})} (T\alpha - \gamma).\end{aligned}$$

Dann behauptet das Kummer'sche Theorem (siehe [Sti1, III.3.7]), daß R' voll zerlegt in der Erweiterung T_n/T_{n-1} ist und es für jede Stelle $R'' \in \mathbb{P}(T_{n+1})$, die über R' liegt, ein $\beta \in K^*$ gibt so, daß R'' Nullstelle von $x_{n+1} - \beta$ ist.

□

Wir können nun den Beweis von 5.1 führen.

Beweis.
Wir betrachten den Unterturm $\mathcal{T}' = (T_1', T_2', T_3', \dots)$ von $\mathcal{T}$, wo $T_n' := T_{2n-1}$ für alle $n \geq 1$. Nach [Gar-Sti2, 2.4] gilt $\lambda(\mathcal{T}) = \lambda(\mathcal{T}')$. Wegen der Drinfeld-Vladut-Schranke ist $\lambda(\mathcal{T}') \leq q-1$, und es genügt zu zeigen, daß

$$\lambda(\mathcal{T}') \geq q-1.$$

Wir wenden den Satz [Gar-Sti2, 2.7] auf den Turm $\mathcal{T}'$ an. Dann gilt mit den Bezeichnungen $D_{n+1} := deg\,\mathrm{Diff}(T_{n+1}/T_n)$ und $D'_{n+1} := deg\,\mathrm{Diff}(T'_{n+1}/T'_n)$:

$$\begin{aligned}D'_{n+1} &= deg\,\mathrm{Diff}(T_{2n+1}/T_{2n-1}) = D_{2n+1} + [T_{2n+1} : T_{2n}]D_{2n} = \\ &= (q^2+q-2)q^n + q(q^2+q-2)q^{n-1} = 2(q^2+q-2)q^n = qD'_n.\end{aligned}$$

Also sind die Voraussetzungen des Satzes [Gar-Sti2, 2.7] mit $\varepsilon = q^{-1}$ erfüllt, und wir erhalten

$$\lambda(\mathcal{T}') \geq \frac{2(1-q^{-1})q^2(q^2-1)}{2(q^2+q-2)q + (1-q^{-1})q^2(-2)} = \frac{(q-1)(q^2-1)}{q^2+q-2-q+1} = q-1.$$

□

6 Automorphismen

Wie wir in §2 gesehen haben, ist der durch die Gleichung

$$y^q + y = \frac{x^q}{x^{q-1}+1} \tag{16}$$

definierte Funktionenkörper $F = K(x, y)$ (wobei q eine Potenz der Charakteristik von K ist) von besonderem Interesse. In diesem Abschnitt wollen wir die Automorphismengruppe von F/K bestimmen.

Sei $\bar{K}$ ein algebraischer Abschluß des Körpers K und $\bar{F}/\bar{K}$ die Konstantenkörpererweiterung von F/K mit $\bar{K}$. Wir setzen voraus, daß das Geschlecht $g \geq 2$ ist. Dann ist die Automorphismengruppe G von $\bar{F}/\bar{K}$ endlich. In unserem Fall bedeutet das, daß

$$g = (q-1)^2 \geq 2$$

ist, d.h. $q \geq 3$ (siehe [Gar-Sti2, 3.8]).

Zuerst bestimmen wir die Gruppe $G(P_\infty)$ aller Automorphismen von $\bar{F}/\bar{K}$, welche P_∞, den Pol von x in $\bar{F}$, fest lassen. Dazu brauchen wir folgendes Lemma:

Lemma 6.1 *Die Elemente* $1, x, \ldots, x^{q-1}, y(x^{q-1}+1)$ *bilden eine Basis des Vektorraums* $\mathcal{L}((q^2-q+1)P_\infty)$.

Beweis.
Es wurde in [Pel-Sti-Tor, 3.2] gezeigt, daß für alle $c \geq q^2 - q$ gilt:

$$dim(c\,P_\infty) = c + 1 - g.$$

Wir setzen $c = q^2 - q + 1$ ein und bekommen für die Dimension des Vektorraums $\mathcal{L}((q^2-q+1)P_\infty)$

$$dim((q^2-q+1)P_\infty) = q^2 - q + 1 + 1 - (q-1)^2 = q + 1.$$

Nach [Gar-Sti2, 3.2] haben die Hauptdivisoren in $\bar{F}$ der Elemente $x - \alpha$, $y - \gamma$ (α, $\gamma \in \Omega$) folgende Gestalt:

$$\begin{aligned}
(x) &= \sum_{\gamma\in\Omega} Q_\gamma - qP_\infty, \\
(x-\alpha) &= qP_\alpha - qP_\infty, \quad \text{für} \quad \alpha \in \Omega^* \\
(y-\gamma) &= qQ_\gamma - P_\infty - \sum_{\alpha\in\Omega^*} P_\alpha, \quad \text{für} \quad \gamma \in \Omega.
\end{aligned}$$

Wir zeigen, daß die Elemente $1, x, \ldots, x^{q-1}, y(x^{q-1}+1)$ linear unabhängig sind und alle in $\mathcal{L}((q^2-q+1)P_\infty)$ liegen. In der Tat:

$$\begin{aligned}(x^i) &= i\sum_{\gamma\in\Omega} Q_\gamma - iqP_\infty \geq -(q^2-q+1)P_\infty, \quad \text{für} \;\; 0\leq i\leq q-1,\\ \big(y(x^{q-1}+1)\big) &= qQ_0 - P_\infty - \sum_{\alpha\in\Omega^*} P_\alpha + q\sum_{\alpha\in\Omega^*} P_\alpha - (q^2-q)P_\infty = \\ &= qQ_0 + (q-1)\sum_{\alpha\in\Omega^*} P_\alpha - (q^2-q+1)P_\infty.\end{aligned}$$

Da diese Elemente verschiedene Polordnungen in P_∞ haben, sind sie linear unabhängig. □

Satz 6.2 *Die Kardinalität von $G(P_\infty)$ ist*

$$\mid G(P_\infty) \mid = q(q-1).$$

Außerdem hat jedes $\sigma \in G(P_\infty)$ die Gestalt:

$$\begin{aligned}\sigma(x) &= ax,\\ \sigma(y) &= ax+b, \;\; \textit{wobei}\; a\in\mathbb{F}_q^*, b\in\Omega.\end{aligned}$$

Beweis.
Sei $\sigma \in G(P_\infty)$. Da σ die Stelle P_∞ fest läßt, ist

$$\sigma(\mathcal{L}((q^2-q+1)P_\infty)) = \mathcal{L}((q^2-q+1)P_\infty).$$

Wir bemerken, daß jedes Element der Folge $1, x, \ldots, x^{q-1}, y(x^{q-1}+1)$ eine echt kleinere Polordnung als das folgende hat. Deshalb bekommt man:

$$\begin{aligned}\sigma(x) &= cx+d,\\ \sigma(y(x^{q-1}+1)) &= ay(x^{q-1}+1)+P(x),\end{aligned}$$

wobei $a, c, d \in \bar{K}, a\neq 0, c\neq 0$ und $P(x)\in\bar{K}[x]$ mit $deg\, P(x) \leq q-1$. Daraus folgt

$$\sigma(y) = \frac{ay(x^{q-1}+1)+P(x)}{(cx+d)^{q-1}+1}. \tag{17}$$

Nun setzen wir die Ausdrücke für $\sigma(x)$ und $\sigma(y)$ in die Gleichung (16) ein.

$$\frac{a^q y^q (x^{q-1}+1)^q + P(x)^q}{((cx+d)^{q-1}+1)^q} + \frac{ay(x^{q-1}+1)+P(x)}{(cx+d)^{q-1}+1} = \frac{(cx+d)^q}{(cx+d)^{q-1}+1} \quad \Leftrightarrow$$

$$\begin{aligned} y^q\frac{a^q(x^{q-1}+1)^q}{((cx+d)^{q-1}+1)^q} \quad &+ \quad y\frac{a(x^{q-1}+1)}{(cx+d)^{q-1}+1} = \frac{(cx+d)^q}{(cx+d)^{q-1}+1} - \\ &- \left(\frac{P(x)}{(cx+d)^{q-1}+1}\right)^q - \left(\frac{P(x)}{(cx+d)^{q-1}+1}\right) \quad \Leftrightarrow\end{aligned}$$

$$y^q \quad + \quad y\frac{\big((cx+d)^{q-1}+1\big)^{q-1}}{a^{q-1}(x^{q-1}+1)^{q-1}} = \frac{\big((cx+d)^{q-1}+1\big)^{q}}{a^{q}(x^{q-1}+1)^{q}} \times \tag{18}$$
$$\times \quad \left(\frac{(cx+d)^q}{(cx+d)^{q-1}+1} - \left(\frac{P(x)}{(cx+d)^{q-1}+1}\right)^q - \left(\frac{P(x)}{(cx+d)^{q-1}+1}\right)\right).$$

Jetzt liefert uns der Koeffizientenvergleich von (16) und (18):

$$\big((cx+d)^{q-1}+1\big)^{q-1} = a^{q-1}(x^{q-1}+1)^{q-1} \quad \Leftrightarrow \tag{19}$$

$$\Big((cx)^{q-1} + \tbinom{q-1}{q-2}(cx)^{q-2}d + \ldots + \tbinom{q-1}{1}(cx)d^{q-2} + d^{q-1} + 1\Big)^{q-1} =$$
$$= a^{q-1}(x^{q-1}+1)^{q-1}.$$

Wieder bekommen wir nach Koeffizientenvergleich bei x^0 und x^1:

$$\begin{array}{lcl} x^0 & : & (d^{q-1}+1)^{q-1} = a^{q-1}, \\ x^1 & : & \tbinom{q-1}{1}cd^{q-2}(d^{q-1}+1)^{q-2} = 0. \end{array}$$

Da $a \neq 0$, $c \neq 0$, ist $d = 0$ und (19) kann als

$$(c^{q-1}x^{q-1}+1)^{q-1} = a^{q-1}(x^{q-1}+1)^{q-1}$$

geschrieben werden. Daraus folgt $a^{q-1} = c^{q-1} = 1$, was insbesondere bedeutet, daß $a, c \in \mathbb{F}_q^*$, und die Gleichung (18) vereinfacht sich zu der Form:

$$y^q + y = \frac{c}{a} \cdot \frac{x^q}{x^{q-1}+1} - \frac{1}{a} \cdot \left(\left(\frac{P(x)}{x^{q-1}+1}\right)^q + \left(\frac{P(x)}{x^{q-1}+1}\right)\right).$$

Dann folgt durch Vergleich mit (16):

$$a = c \;\text{ und }\; P(x) = b(x^{q-1}+1), \;\text{ mit }\; b \in \Omega.$$

Zusammen mit (17) erhält man schließlich:

$$\begin{aligned} \sigma(x) &= ax, \\ \sigma(y) &= \frac{ay(x^{q-1}+1) + b(x^{q-1}+1)}{a^{q-1}x^{q-1}+1} = ax + b. \end{aligned}$$

$\square$

Nachdem wir die Gruppe $G(P_\infty)$ berechnet haben, können wir die ganze Automorphismengruppe von $\bar{F}/\bar{K}$ bestimmen. Wir gehen folgenderweise vor:

Zuerst zeigen wir, daß die Stelle P_∞ nur auf endlich viele Stellen von $\bar{F}$ mit Hilfe eines Automorphismus $\sigma \in G = Aut\,(\bar{F}/\bar{K})$ abgebildet werden kann. Das impliziert, daß der Index $(G : G(P_\infty))$ endlich ist. Schließlich werden wir für jede Restklasse einen Vertreter genau beschreiben.

Die Stellen von $\bar{F}/\bar{K}$, die von P_∞ und den Nullstellen von $x - \alpha$ ($\alpha \in \Omega$) in $\bar{F}$ verschieden sind, sind die Stellen $P_{a,b}$:

$$x \longrightarrow a,\ y \longrightarrow b.$$

Dabei durchläuft a alle Elemente von $\bar{K}\backslash\Omega$ und b durchläuft bei festem a alle Nullstellen von

$$b^q + b = \frac{a^q}{a^{q-1}+1}.$$

Das Element $x - a$ ist ein Primelement von $P_{a,b}$, und $y - b$ hat $P_{a,b}$ als Nullstelle.

Wir untersuchen nun die Polzahlverteilung der Stellen $P_{a,b}$. Wir betrachten folgenden kanonischen Divisor

$$W = (dx) = -2(x)_\infty + \mathrm{Diff}(\bar{F}/\bar{K}(x)).$$

Mit Hilfe von [Gar-Sti2, 3.2] bekommen wir

$$W = -2qP_\infty + 2(q-1)\sum_{\alpha\in\Omega^*} P_\alpha + 2(q-1)P_\infty = -2P_\infty + 2(q-1)\sum_{\alpha\in\Omega^*} P_\alpha.$$

Lemma 6.3 *Die Zahl k ist genau dann eine Fehlzahl von $P_{a,b}$, wenn es ein Element $z \in \mathcal{L}(W)$ gibt mit $v_{P_{a,b}}(z) = k - 1$.*

Beweis.
k ist eine Fehlzahl von $P_{a,b}$ genau dann, wenn

$$\mathcal{L}((k-1)P_{a,b}) = \mathcal{L}(k\,P_{a,b}).$$

Dies ist nach Riemann-Rochschen Satz gleichbedeutend mit

$$\mathcal{L}(W - (k-1)P_{a,b}) \subsetneqq \mathcal{L}(W - k\,P_{a,b}).$$

Weil $P_{a,b}$ nicht in W auftritt, ist das gerade die Behauptung des Lemmas. □

Lemma 6.4 *Sei $a \in \bar{K}\backslash\Omega$, $b \in \bar{K}$ eine Nullstelle des Polynoms $T^q + T - \frac{a^q}{a^{q-1}+1}$. Dann ist*

$$B_{a,b} := \left\{ \frac{x^{q-i-2}(x-a)^i(y-b)^j}{x^{q-1}+1} \;\Big|\; 0 \le i,\, j \le q-2 \right\}$$

eine Basis des Vektorraums $\mathcal{L}(W)$.

Beweis.
Zuerst bestimmen wir die Hauptdivisoren der Funktionen $x - a$ und $y - b$. Aus [Gar-Sti2, 3.2] sehen wir, daß

$$(x-a) = \sum_{c^q + c = \frac{a^q}{a^{q-1}+1}} P_{a,c} - qP_\infty$$

und

$$(y-b) = P_{a,b} + A_{a,b} - P_\infty - \sum_{\alpha \in \Omega^*} P_\alpha,$$

wobei $A_{a,b} \geq 0$ ein Divisor mit deg $A_{a,b} = q$ und $v_{P_\alpha}(A_{a,b}) = 0$.

Wir zeigen jetzt, daß $v_{P_{a,b}}(A_{a,b}) = 0$. Es gilt

$$(y-b)^q + (y-b) = \frac{x^q}{x^{q-1}+1} - \frac{a^q}{a^{q-1}+1} =$$
$$= \frac{1}{x^{q-1}+1}\left(x^q - \frac{a^q}{a^{q-1}+1}x^{q-1} - \frac{a^q}{a^{q-1}+1}\right) = \frac{x-a}{x^{q-1}+1}\, Q(x),$$

wobei $Q(x)$ ein Polynom in $K[x]$ ist. Da

$$\left.\left(x^q - \frac{a^q}{a^{q-1}+1}x^{q-1} - \frac{a^q}{a^{q-1}+1}\right)'\right|_{x=a} =$$
$$= qa^{q-1} - (q-1)\frac{a^q}{a^{q-1}+1}a^{q-2} = \frac{a^{2q-2}}{a^{q-1}+1} \neq 0,$$

ist $x = a$ keine Nullstelle des Polynoms $Q(x)$. Daraus folgt

$$v_{P_{a,b}}(y-b) = v_{P_{a,b}}(x-a) = 1.$$

Nun können wir den Hauptdivisor berechnen:

$$\begin{aligned}
\left(\frac{x^{q-i-2}(x-a)^i(y-b)^j}{x^{q-1}+1}\right) &= (q-i-2)\sum_{\gamma\in\Omega} Q_\gamma - (q-i-2)qP_\infty + \\
+i \sum_{c^q + c = \frac{a^q}{a^{q-1}+1}} P_{a,c} - iqP_\infty &+ jP_{a,b} + jA_{a,b} - jP_\infty - j\sum_{\alpha\in\Omega^*} P_\alpha - \\
-q\sum_{\alpha\in\Omega^*} P_\alpha + (q-1)qP_\infty &= i \sum_{c^q + c = \frac{a^q}{a^{q-1}+1}} P_{a,c} + (q-i-2)\sum_{\gamma\in\Omega} Q_\gamma + \\
+jP_{a,b} + jA_{a,b} &+ (q-j)P_\infty - (q+j)\sum_{\alpha\in\Omega^*} P_\alpha \geq \\
&\geq 2P_\infty - 2(q-1)\sum_{\alpha\in\Omega^*} P_\alpha.
\end{aligned}$$

Also liegen die Elemente

$$\frac{x^{q-i-2}(x-a)^i(y-b)^j}{x^{q-1}+1},$$

für $0 \leq i,\, j \leq q-2$, in $\mathcal{L}(W)$.

Man kann leicht sehen, daß sie linear unabhängig sind (sonst wäre y Nullstelle eines Polynoms über $K(x)$ vom Grad $< q$). Da $dim\, \mathcal{L}(W) = g(\bar{F}) = (q-1)^2$, folgt, daß $B_{a,b}$ eine Basis von $\mathcal{L}(W)$ ist. $\square$

Korollar 6.5 *Sei $a, b \in \bar{K}$, $a \notin \Omega$ und $b^q + b = \frac{a^q}{a^{q-1}+1}$. Dann ist die Zahl q eine Fehlzahl für die Stelle $P_{a,b}$.*

Beweis.
Nach Lemma 6.4 liegt das Element $\frac{x^{q-3}(x-a)(y-b)^{q-2}}{x^{q-1}+1}$ in $\mathcal{L}(W)$, und es ist

$$v_{P_{a,b}}(\frac{x^{q-3}(x-a)(y-b)^{q-2}}{x^{q-1}+1}) = q-1.$$

Dann folgt aus Lemma 6.3, daß q eine Fehlzahl von $P_{a,b}$ ist. Den Rest erhält man sofort aus Lemma 6.4.

$\square$

Nun können wir die volle Automorphismengruppe G von $\bar{F}/\bar{K}$ bestimmen.

Theorem 6.6 *Sei $F = K(x,y)$ durch $y^q + y = \frac{x^q}{x^{q-1}+1}$ definiert und nicht elliptisch. Dann operiert die Gruppe $Aut\,(F/K)$ transitiv auf den Stellen P_∞, P_α und Q_γ, mit $\alpha \in \Omega^*$, $\gamma \in \Omega$. Die Ordnung von $Aut\,(F/K)$ ist*

$$\mid G \mid = 2q \mid G(P_\infty) \mid = 2q^2(q-1).$$

Außerdem hat jedes $\sigma \in Aut\,(F/K)$ die Gestalt:

i)

$$\begin{aligned} \sigma(x) &= ax, \\ \sigma(y) &= ay + b, \quad \textit{wobei} \;\; a \in \mathbb{F}_q^*,\; b \in \Omega, \end{aligned}$$

ii)

$$\begin{aligned} \sigma(x) &= \frac{c}{y-\gamma}, \\ \sigma(y) &= \frac{c}{x} + d, \quad \textit{wobei} \;\; c \in \mathbb{F}_q^*,\; d, \gamma \in \Omega, \end{aligned}$$

iii)

$$\sigma(x) = \frac{ex}{1 - \frac{x}{\alpha}},$$
$$\sigma(y) = ey + f, \quad \textit{wobei} \;\; e \in \mathbb{F}_q^*, \; f \in \Omega, \; \alpha \in \Omega^*.$$

Beweis
Wir betrachten die Konstantenerweiterung $\bar{F}/\bar{K}$ von F/K. Nach [Gar-Sti2, 3.2] hat die Stelle P_∞ die Zahl q als Polzahl. Andererseits ist q nach Korollar 6.5 eine Fehlzahl von $P_{a,b}$ für alle $a \in \bar{K} \backslash \Omega$, d.h. es existiert kein $\sigma \in G$ mit $\sigma(P_\infty) = P_{a,b}$.

Nun geben wir einen Vertreter für jede Restklasse von G modulo $G(P_\infty)$ an.

Sei $\gamma \in \Omega$. Wir definieren

$$\sigma_\gamma(x) = \frac{1}{y - \gamma}, \quad \sigma(y) = \frac{1}{x}.$$

σ_γ ist ein Automorphismus von $\bar{F}/\bar{K}$, da

$$\sigma_\gamma^q(y) + \sigma_\gamma(y) = \frac{1}{x^q} + \frac{1}{x} = \frac{x^{q-1}+1}{x^q} = \frac{1}{y^q + y} =$$
$$= \frac{1}{(y-\gamma)^q + (y - \gamma)} = \frac{\frac{1}{(y-\gamma)^q}}{\frac{1}{(y-\gamma)^{q-1}} + 1} = \frac{\sigma_\gamma(x)^q}{\sigma_\gamma(x)^{q-1} + 1}.$$

Dabei bildet σ_γ die Stelle P_∞ auf Q_γ ab.

Schließlich bildet die Abbildung

$$\sigma_\alpha(x) = \frac{x}{1 - \frac{x}{\alpha}}, \quad \sigma(y) = y$$

die Stelle P_∞ auf die Stelle P_α für jedes $\alpha \in \Omega^*$ ab, und sie ist ein Automorphismus von $\bar{F}/\bar{K}$, denn

$$\frac{\sigma_\alpha(x)^q}{\sigma_\alpha(x)^{q-1} + 1} = \frac{\frac{\alpha^q x^q}{(\alpha - x)^q}}{\frac{\alpha^{q-1}x^{q-1}}{(\alpha-x)^{q-1}} + 1} = \frac{\alpha^q x^q}{\alpha^{q-1}x^{q-1}(\alpha - x) + \alpha^q - x^q} =$$
$$= \frac{\alpha^q x^q}{\alpha^q x^{q-1} + \alpha^q - x^q(\alpha^{q-1} + 1)} = \frac{x^q}{x^{q-1} + 1} = y^q + y = \sigma_\alpha(y)^q + \sigma_\alpha(y).$$

Man sieht, daß jedes $\sigma \in \mathit{Aut}\,(\bar{F}/\bar{K})$ auch ein Automorphismus von F/K ist, wegen $\Omega \subset K$. Das bedeutet $\mathit{Aut}\,(F/K) = \mathit{Aut}\,(\bar{F}/\bar{K})$, und der Satz ist bewiesen.

$\square$

Literatur

[Ale-Deo-Kum-Sti] Aleshnikov, I., Deolalikar, V., Kumar, P.V., Stichtenoth, H.: Towards a basis of the space of regular functions in a tower of function fields meeting the Drinfeld-Vladut bound. To appear in the proceedings of the *Fifth International Conference on Finite Fields and Applications*, August 2-6, 1999, University of Augsburg, Germany.

[Chev] Chevalley, C.: Introduction to the Theory of Algebraic Functions of One Variable. AMS Math. Surveys, New York, 1951.

[Gar-Sti1] Garcia, A., Stichtenoth, H.: A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound. Invent. Math. **121**, pp. 211-222, 1995

[Gar-Sti2] Garcia, A., Stichtenoth, H.: On the asymptotic behaviour of some towers of function fields over finite fields. J. of Number Th. **61**, 248-273, 1996

[Hac] Haché, G.: Construction effective des codes geométriques. Thèse. Université Pierre & Marie Curie Paris VI, 1996

[Iha] Ihara, Y.: Some Remarks on the Number of Rational Points of Algebraic Curves over Finite Fields. J. Fac. Sci. Tokyo, **28**, pp. 721-724, 1981

[Lin] van Lint, J. H.: Introduction to coding theory. Springer 1982.

[Mat-Miu] R. Matsumoto and S. Miura: Computing a Basis of L(D) on an Affine Algebraic Curve with One Rational Place at Infinity. In the Proceedings of 13-th AAECC Symposium on Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes, Lecture Note in Computer Science, **1719**, pp.271-281, Springer, 1999

[Nie-Xin] Niederreiter, H., Xing, C.P.: Curve sequences with asymptotically many rational points. Contemporary Mathematics **245** (1999), 3-14.

[Pel-Sti-Tor] Pellikaan R., Stichtenoth, H., Torres F.: Weierstrass Semigroups in an Asymptotically Good Towers of Function Fields. Finite Fields and Their Applications **4**, 381-392, 1998

[Ser] Serre, J.-P.: Sur le nombre des points d'une courbe algébrique sur un corps fini. C. R. Acad. Sci. Paris, **269**, Series I, pp. 397-402, 1983

[Sti1] Stichtenoth, H.: Algebraic Function Fields and Codes. Springer, Berlin-Heidelberg-New York, 1993

[Sti2] Stichtenoth, H.: Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. Teil 1: Eine Abschätzung der Ordnung der Automorphismengruppe. Arch. Math. **24** , 524-544, 1973

[Tsf-Vla] Tsfasman, M. A., Vladut, S. G.: Algebraic-Geometric Codes. Kluwer Acad. Publ., Dordrecht-Boston-London, 1991

[Tsf-Vla-Zin] Tsfasman, M. A., Vladut, S. G., Zink, T.: Modular Curves, Shimura Curves and Goppa Codes, better than the Varshamov-Gilbert Bound. Math. Nachr. **109**, pp. 21-28, 1982

[Voss-Hoe] Voss, C., Hoeholdt, T.: An explicit construction of a sequences of codes attaining the Tsfasman-Vladut-Zink bound: The first steps. IEEE Trans. Inf. Theory **43**, No.1, 128-135, 1997