Zahme Türme algebraischer Funktionenkörper

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

vorgelegt beim
Fachbereich Mathematik und Informatik
der Universität Essen

von Diplom-Mathematiker
Jörg Wulftange
aus Hannover

2002

Vorsitzender:	Prof. Dr. Karl Josef Witsch
Gutachter:	Prof. Dr. Dr. h.c. Gerhard Frey
	Prof. Dr. Henning Stichtenoth

Tag der mündlichen Prüfung: 07.02.2003

Danksagung

Zunächst und vor allem möchte ich Henning Stichtenoth danken, der mich während der Erstellung der Dissertation betreut hat. Während der gesamten Zeit meiner Promotion stand er mir mit hilfreichen Vorschlägen und interessanten Anregungen zur Seite. Seine kritischen Anmerkungen haben wesentlich zum Gelingen der Arbeit beigetragen.

Weiter möchte ich mich bei Hiren Maharaj für die Zusammenarbeit bei der Suche nach neuen asymptotisch guten Türmen bedanken. Die gemeinsame Arbeit, vor allen Dingen während des gemeinsamen Forschungsaufenthalts in Brasilien, war immer begeisternd und äußerst fruchtbar.

Schließlich gilt mein Dank Arnaldo Garcia für seine Unterstützung während meines Forschungsaufenthalts am IMPA. Insbesondere die Diskussionen über relativ unverzweigte Türme waren anregend und hilfreich.

Einleitung

Das Lösen von algebraischen Gleichungen in zwei Unbestimmten über endlichen Körpern gehört zu den grundlegenden Fragestellungen der klassischen Zahlentheorie. E. Artin vermutete eine obere Schranke für die Anzahl der Lösungen über einem gegebenen Körper $\mathbb{F}_q$, indem er eine Analogie für die Riemannsche Vermutung formulierte. Der Beweis dieser Vermutung (in der allgemeinen Form) gelang A. Weil (vgl. [17]).

Die Lösungen einer irreduziblen Gleichung $f(x,y)=0$ entsprechen in der Sprache algebraischer Funktionenkörper im wesentlichen den $\mathbb{F}_q$-rationalen Stellen des durch die Gleichung definierten Körpers F. Nun kann Weils Resultat in der Form

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

formuliert werden, wobei $N(F)$ die Anzahl $\mathbb{F}_q$-rationaler Stellen von F bezeichnet und $g(F)$ das Geschlecht von F angibt. Gleichheit kann dabei nur auftreten, wenn q ein Quadrat ist und das Geschlecht von F relativ klein ist. Genauer hat Y. Ihara bewiesen, daß Gleichheit höchstens für $g(F) \leq \sqrt{q}(\sqrt{q}-1)/2$ gilt (vgl. [11]).

Betrachtet man die maximale Anzahl $\mathbb{F}_q$-rationaler Stellen für sehr großes Geschlecht, so erhält man eine deutlich bessere Abschätzung. Dazu sei

$$N_q(g) = \max\{N(F) | F \text{ ist ein Funktionenkörper über } \mathbb{F}_q \text{ mit } g(F) = g\}$$

und

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

Dann gilt die Drinfeld-Vladut-Schranke (vgl. [2])

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

Folgen $(F_k)_{k\geq 0}$ algebraischer Funktionenkörper mit $F_k \subseteq F_{k+1}$ und gleichem Konstantenkörper $\mathbb{F}_q$ kann man als konstruktives Gegenstück zu der theoretischen Schranke ansehen. Fordert man zusätzlich, daß $g(F_k) > 1$ für ein $k \geq 0$ und daß F_{k+1}/F_k separabel ist für alle $k \geq 0$, so erhält man einen *Turm algebraischer Funktionenkörper* $\mathcal{T} := \cup_{k\geq 0} F_k$ als das interessierende algebraische Objekt (vgl. Definition 1.1.1).

Zu einem erheblichen Interesse in der Forschung führte die Beobachtung von M.A. Tsfasman, S.G. Vladut und T. Zink, daß Folgen $(F_k)_{k\geq 0}$ von Funktionenkörpern mit im Sinne der Drinfeld-Vladut-Schranke maximal vielen $\mathbb{F}_{q^2}$-rationalen Stellen verwendet werden können, um algebraisch-geometrische Codes oberhalb der Gilbert-Varshamov-Schranke zu konstruieren (vgl. [16]). Um diese Codes angeben zu können, benötigt man eine unendliche Folge algebraischer Funktionenkörper, die durch Relationen explizit gegeben sind, wie es bei rekursiv definierten Türmen der Fall ist. Die ersten Beispiele rekursiv definierter *asymptotisch optimaler Türme* wurden von A. Garcia und H. Stichtenoth gefunden (vgl. [7]).

In Kapitel 1 werden wir die für die Arbeit grundlegenden Konzepte bereitstellen. Wir beschränken uns dabei auf die Untersuchung *rekursiv definierter Türme*. Im wesentlichen heißt ein Turm $\mathcal{T} := \cup_{k\geq 0} F_k$ rekursiv definiert durch eine Gleichung $f(x,y) = 0$, falls $F_0 := \mathbb{F}_q(x_0)$ ein rationaler Funktionenkörper ist und die Erweiterungen F_{k+1}/F_k jeweils durch Adjunktion einer Nullstelle x_{k+1} des Polynoms $f(x_k, y)$ entsteht (dabei sind die Koeffizienten von $f(x,y)$ unabhängig von k, vgl. Definition 1.2.1).

Ist eine irreduzible Gleichung $f(x,y) = 0$ gegeben, so ist zunächst nicht klar, ob sie rekursiv einen Turm definiert. In Kapitel 2 werden wir hinreichende Kriterien diskutieren, die sicherstellen, daß eine Gleichung rekursiv einen Turm definiert. Diese Kriterien wurden verwendet, um computergestützt neue *asymptotisch gute* Türme zu finden. Die neu gefundenen Türme werden ebenfalls in Kapitel 2 diskutiert.

Sind für einen Turm $\mathcal{T} := \cup_{k\geq 0} F_k$ fast alle Erweiterungen F_{k+1}/F_k zahm, so ist er asymptotisch gut, falls die Anzahl über F_0 in F_k verzweigender Stellen für $k \geq 0$ (unabhängig von k) beschränkt werden kann und mindestens eine $\mathbb{F}_q$-rationale Stelle von F_{k_0} komplett zerfällt in jedem F_k (für ein $k_0 \geq 0$). Diese beiden Eigenschaften werden in Kapitel 3 genauer beleuchtet mit dem Ziel, den exakten Grenzwert für eine Klasse von Türmen anzugeben (rekursiv definierte total verzweigte zahme Türme).

Fermat Gleichungen

$$y^m = a(x+b)^m + c \text{ mit } a, b, c \in \mathbb{F}_q^*$$

definieren bekanntermaßen in einigen Fällen asymptotisch gute Türme. Durch eine solche Gleichung definierte Türme sind Gegenstand des 4. Kapitels. Dabei werden wir den exakten Grenzwert einer Klasse von Fermat Türmen bestimmen sowie notwendige Bedingungen an den Grad der Fermat Gleichung im Fall total verzweigter Fermat Türme formulieren, um einen endlichen Verzweigungsort zu erhalten.

In Kapitel 5 werden wir eine Klasse neuer asymptotisch guter Türme diskutieren. Diese haben die besondere Eigenschaft, daß sie nach endlich vielen Schritten unverzweigt sind. D.h. es existiert ein $k_0 \geq 1$, so daß F_k/F_{k_0} unverzweigt ist für alle $k \geq k_0$.

Inhaltsverzeichnis

Bezeichnungen

$\mathbb{N}$	Natürliche Zahlen
$\mathbb{Z}$	Ganze Zahlen
$\gcd(a, b)$	Größter gemeinsamer Teiler von a und b
$\deg f(x)$	Grad des Polynoms $f(x)$
$\mathbb{F}_q$	Endlicher Körper mit q Elementen
$\mathbb{F}_q^*$	Multiplikative Gruppe von $\mathbb{F}_q$
$\bar{\mathbb{F}}_q$	Algebraischer Abschluß von $\mathbb{F}_q$
F/K	Algebraischer Funktionenkörper F mit Konstantenkörper K
$\mathbb{P}_F$	Menge der Stellen von F/K
$P, Q, R, \ldots$	Stellen von F/K
$P'\|P$	Stelle P' über P in F'/F für einen Funktionenkörper F'
$e(P'\|P)$	Verzweigungsindex von $P'\|P$
$d(P'\|P)$	Differentenexponent von $P'\|P$
$\mathcal{O}_P$	Bewertungsring einer Stelle P
$\mathcal{O}_P^*$	Einheitengruppe von $\mathcal{O}_P$
$g(F)$	Geschlecht von F
$N(F)$	Anzahl K-rationaler Stellen von F
$\mathcal{F}, \mathcal{T}, \ldots$	Turm, 1.1.1
$F < \mathcal{F}$	Funktionenkörper F mit $K \subseteq F \subseteq \mathcal{T}$ und $\mathcal{F}/F$ separabel
	Asymptotisch guter (optimaler) Turm, 1.1.5
	Zahmer Turm, 1.1.7
	Komplett zerfallender Turm, 1.1.10
	Relativ unverzweigter (unendlich verzweigter) Turm, 1.1.15
	Rekursiv definierter Turm (Körper), 1.2.1
	Dualer Turm, 1.2.2
	Gerader (schiefer) Turm, 1.2.5
	Total verzweigter Turm, 3.1.3
$\lambda(\mathcal{T})$	Grenzwert von $\mathcal{T}$, 1.1.3
$\nu_{F_0}(\mathcal{T})$	F_0-Zerfällungsrate von $\mathcal{T}/F_0$, 1.1.6
$\gamma_{F_0}(\mathcal{T})$	F_0-Geschlecht von $\mathcal{T}/F_0$, 1.1.6
$V_{F_0}(\mathcal{T})$	F_0-Verzweigungsort von $\mathcal{T}$, 1.1.8
$\mathcal{E} \prec \mathcal{F}$	Turm $\mathcal{E}$, der Teilkörper vom Turm $\mathcal{F}$ ist

Kapitel 1

Türme und Pyramiden

1.1 Funktionenkörpertürme

Im ersten Abschnitt werden für diese Arbeit zentrale Begriffsbildungen eingeführt und grundsätzliche Eigenschaften von Türmen algebraischer Funktionenkörper diskutiert.

Es sei K ein beliebiger Körper. Ein Funktionenkörper F/K ist ein Erweiterungskörper $F \supseteq K$, so daß F eine endliche algebraische Erweiterung von $K(x)$ ist für ein über K transzendentes Element $x \in F$.

Definition 1.1.1 *Ein Turm über K ist ein Erweiterungskörper $\mathcal{T} \supseteq K$ mit den folgenden Eigenschaften:*

1. *Der Transzendenzgrad von $\mathcal{T}/K$ ist gleich eins.*
2. *K ist algebraisch abgeschlossen in $\mathcal{T}$.*
3. *Der Körper $\mathcal{T}$ ist nicht endlich erzeugt über K.*
4. *Es existiert ein Funktionenkörper $F \subseteq \mathcal{T}$ über K mit Geschlecht $g(F) > 1$ und $\mathcal{T}/F$ separabel.*

Im folgenden bezeichne $F < \mathcal{T}$ stets Funktionenkörper F mit $K \subseteq F \subseteq \mathcal{T}$ und $\mathcal{T}/F$ separabel. Jeder Turm $\mathcal{T}$ über K kann wie folgt beschrieben werden: Wir wählen einen Funktionenkörper $F < \mathcal{T}$. Dann existiert eine (unendliche) Folge algebraischer Funktionenkörper $F_i < \mathcal{T}$, so daß

$$F = F_0 \subseteq F_1 \subseteq F_2 \subseteq \ldots \text{ und } \mathcal{T} = \cup_{i=0}^{\infty} F_i.$$

Wir sagen: $(F_i)_{i \geq 0}$ ist eine Darstellung von $\mathcal{T}$.

Bemerkung 1.1.2 *Aufgrund der Bedingungen 3. und 4. in Definition 1.1.1 folgt aus der Hurwitzschen Geschlechtsformel für das Geschlecht der Körper F_i, daß $g(F_i) \to \infty$ für $i \to \infty$.*

Für eine Folge algebraischer Funktionenkörper $(F_i)_{i\geq 0}$ mit exaktem Konstantenkörper $\mathbb{F}_q$ (und $F_i \subseteq F_{i+1}$ für alle $i \geq 0$) ist sowohl aus zahlentheoretischer Sicht als auch aus codierungstheoretischer Sicht das asymptotische Verhältnis zwischen der Anzahl $\mathbb{F}_q$-rationaler Stellen und dem Geschlecht von F_i für $i \to \infty$ von ganz grundlegendem Interesse. Tatsächlich ist dieses Verhältnis eine Invariante des durch $(F_i)_{i\geq 0}$ definierten Turms.

Alle im Abschnitt 1.1 diskutierten Begriffsbildungen sind wohldefiniert; die Begriffe und Ergebnisse dieses Abschnitts entstammen größtenteils dem Artikel [10].

Definition 1.1.3 *Für einen Turm $\mathcal{T}$ über $\mathbb{F}_q$ heiße die reelle Zahl*

$$\lambda(\mathcal{T}) := \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}$$

der Grenzwert von $\mathcal{T}$ (dabei ist $(F_i)_{i\geq 0}$ eine beliebige Darstellung von $\mathcal{T}$, $N(F_i)$ ist gleich der Anzahl der $\mathbb{F}_q$-rationalen Stellen, und $g(F_i)$ bezeichnet das Geschlecht von F_i).

Theorem 1.1.4 *Für einen Turm $\mathcal{T}$ über $\mathbb{F}_q$ gilt stets*

$$0 \leq \lambda(\mathcal{T}) \leq \sqrt{q} - 1.$$

Beweis: Die untere Abschätzung ist trivial. Die obere Abschätzung ist gerade die Drinfeld-Vladut-Schranke. □

Diese Einsicht motiviert die folgende Definition.

Definition 1.1.5 *Ein Turm $\mathcal{T}$ über $\mathbb{F}_q$ heißt asymptotisch gut (resp. asymptotisch schlecht, resp. asymptotisch optimal), falls $\lambda(\mathcal{T}) > 0$ (resp. $\lambda(\mathcal{T}) = 0$, resp. $\lambda(\mathcal{T}) = \sqrt{q} - 1$) gilt.*

Die anschließenden Begriffsbildungen erlauben es, die Frage nach dem Grenzwert eines Turms in zwei voneinander unabhängige Teilfragen zu zerlegen.

Definition 1.1.6 *Sei $\mathcal{T}$ ein Turm über $\mathbb{F}_q$ mit Darstellung $(F_i)_{i\geq 0}$.*

1. *Es heißt*

$$\nu_{F_0}(\mathcal{T}) := \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}$$

die F_0-Zerfällungsrate von $\mathcal{T}$.

2. *Es heißt*

$$\gamma_{F_0}(\mathcal{T}) := \lim_{i\to\infty} \frac{g(F_i)}{[F_i : F_0]}$$

das F_0-Geschlecht von $\mathcal{T}$.

Dabei bezeichnen wieder $N(F_i)$ die Anzahl der $\mathbb{F}_q$-rationalen Stellen und $g(F_i)$ das Geschlecht von F_i.

Es ist $0 \leq \nu_{F_0}(\mathcal{T}) < \infty$ und $0 < \gamma_{F_0}(\mathcal{T}) \leq \infty$. Nun kann der Grenzwert in der Form

$$\lambda(\mathcal{T}) = \frac{\nu_{F_0}(\mathcal{T})}{\gamma_{F_0}(\mathcal{T})}$$

ausgedrückt werden. Offensichtlich ist $\mathcal{T}$ genau dann asymptotisch gut, wenn $\nu_{F_0}(\mathcal{T}) > 0$ und $\gamma_{F_0}(\mathcal{T}) < \infty$ gilt.

Die Untersuchung des F_0-Geschlechts eines Turms $\mathcal{T} := \cup_{k\geq 0} F_k$ hängt wesentlich davon ab, ob er unendlich viele wilde Erweiterungen F_{k+1}/F_k enthält. Dazu definieren wir:

Definition 1.1.7 *Sei $\mathcal{T}$ ein Turm über $\mathbb{F}_q$. Der Turm $\mathcal{T}$ heißt zahm, falls ein algebraischer Funktionenkörper $F < \mathcal{T}$ existiert, so daß E/F zahm ist für alle Funktionenkörper $E < \mathcal{T}$ mit $F \subseteq E$. Wir sagen in diesem Fall, daß $\mathcal{T}/F$ zahm ist.*

Das F-Geschlecht zahmer Türme läßt sich häufig durch die Anzahl der verzweigenden Stellen von F in einer beliebigen Erweiterung E mit $F \subseteq E < \mathcal{T}$ nach oben abschätzen.

Definition 1.1.8 *Sei $\mathcal{T}$ ein Turm über $\mathbb{F}_q$ und $F < \mathcal{T}$. Wir definieren den F-Verzweigungsort von $\mathcal{T}$ als die Menge*

$$\begin{aligned} V_F(\mathcal{T}) \quad = \quad & \{P \in \mathbb{P}_F | \textit{ Es gibt einen Funktionenkörper } E \textit{ mit } F \subseteq E < \mathcal{T}, \\ & \quad \textit{so daß } P \textit{ in } E/F \textit{ verzweigt}\} \end{aligned}$$

(wobei $\mathbb{P}_F$ die Menge der Stellen von F bezeichnet).

Ist $E < \mathcal{T}$ ein weiterer algebraischer Funktionenkörper in $\mathcal{T}$, so ist

$$V_F(\mathcal{T}) < \infty \Leftrightarrow V_E(\mathcal{T}) < \infty.$$

Wir sagen in diesem Fall auch: $\mathcal{T}$ ist von endlichem Verzweigungstyp.

Aus der Hurwitzschen Geschlechtsformel folgt:

Satz 1.1.9 *Ist $\mathcal{T}$ ein zahmer Turm über $\mathbb{F}_q$ von endlichem Verzweigungstyp und $F < \mathcal{T}$, so ist $\gamma_F(\mathcal{T}) < \infty$. Genauer gilt: Ist $\mathcal{T}/F$ zahm, dann ist*

$$\gamma_F(\mathcal{T}) \leq g(F) + \frac{s-2}{2},$$

mit $s = \sum_{P \in V_F(\mathcal{T})} \deg P$.

Definition 1.1.10 *Es sei $\mathcal{T}/\mathbb{F}_q$ ein Turm und $F < \mathcal{T}$. Wir sagen, daß eine $\mathbb{F}_q$-rationale Stelle $P \in \mathbb{P}_F$ in $\mathcal{T}/F$ komplett zerfällt, falls die Stelle P in allen Funktionenkörpern E mit $F \subseteq E < \mathcal{T}$ komplett zerfällt. Der Turm $\mathcal{T}$ heißt komplett zerfallend, falls ein Funktionenkörper $F < \mathcal{T}$ existiert, so daß mindestens eine $\mathbb{F}_q$-rationale Stelle von F komplett in $\mathcal{T}/F$ zerfällt.*

Nun können wir für die Zerfällungsrate festhalten:

Satz 1.1.11 *Ist der Turm $\mathcal{T}$ über $\mathbb{F}_q$ komplett zerfallend, dann ist $\nu_F(\mathcal{T}) > 0$. Genauer gilt:*

$$\nu_F(\mathcal{T}) \geq t,$$

wobei t gleich der Anzahl über F komplett zerfallender Stellen ist.

Damit erhalten wir:

Theorem 1.1.12 *Sei $\mathcal{T}/F$ ein zahmer Turm über $\mathbb{F}_q$ und $F < \mathcal{T}$. Es sei $s = \sum_{P \in V_F(\mathcal{T})} \deg P < \infty$, und $t > 0$ sei die Anzahl über F komplett zerfallender Stellen. Dann ist*

$$\lambda(\mathcal{T}) \geq \frac{2t}{2g(F) + s - 2}.$$

Insbesondere ist $\mathcal{T}$ asymptotisch gut.

Falls $\mathcal{T}/F$ galoissch ist für einen Funktionenkörper $F < \mathcal{T}$, so können wir notwendige Bedingungen dafür angeben, daß $\mathcal{T}$ asymptotisch gut ist.

Theorem 1.1.13 *Sei $\mathcal{T}$ ein asymptotisch guter Turm über $\mathbb{F}_q$, der galoissch ist über F für ein $F < \mathcal{T}$. Dann ist der Verzweigungsort $V_F(\mathcal{T})$ endlich, und $\mathcal{T}$ zerfällt komplett.*

Bemerkung 1.1.14 *Falls $\mathcal{T}/F$ galoissch und abelsch ist, so ist $\mathcal{T}$ asymptotisch schlecht (vgl. [6]).*

Es ist nicht bekannt, ob die Bedingungen aus Theorem 1.1.12 auch in anderen Fällen notwendige Bedingungen darstellen, um asymptotisch gute Türme zu erhalten. Für rekursiv definierte zahme Türme werden wir diese Frage später noch einmal aufgreifen (vgl. Kapitel 3).

Definition 1.1.15 *Es sei $\mathcal{T}$ ein Turm über $\mathbb{F}_q$. Dann heiße $\mathcal{T}$ relativ unverzweigt, falls ein $F < \mathcal{T}$ existiert, so daß E/F unverzweigt ist für alle $E < \mathcal{T}$ mit $F \subseteq E$. Wir sagen in diesem Fall auch, daß $\mathcal{T}$ unverzweigt ist über F. Falls $\mathcal{T}$ nicht relativ unverzweigt ist, so heiße $\mathcal{T}$ unendlich verzweigt.*

Der Grenzwert relativ unverzweigter Türme läßt sich in mancher Hinsicht leichter bestimmen als der Grenzwert unendlich verzweigter Türme. Wir diskutieren diesen Fall ausführlicher in Kapitel 5.

1.2 Rekursiv definierte Türme und Pyramiden

Im folgenden sei K ein Körper und $f(x,y)$ sei ein absolut irreduzibles, in beiden Variablen separables Polynom über K mit $\deg_x f(x,y) > 1$ und $\deg_y f(x,y) > 1$. Die meisten explizit bekannten asymptotisch guten Türme sind wesentlich auf Konstruktionen von der folgenden Gestalt zurückzuführen:

Definition 1.2.1 1. *Ein Turm $\mathcal{T}$ über K heißt rekursiv definiert durch die Gleichung*

$$f(x,y) = 0,$$

falls

$$\mathcal{T} = K(x_0, x_1, x_2, \ldots) \text{ mit } f(x_i, x_{i+1}) = 0 \text{ für alle } i \geq 0$$

und die Polynome $f(x_i, y)$ absolut irreduzibel sind über $K(x_0, x_1, \ldots, x_i)$ für alle $i \geq 0$.

2. *Ein Körper F_k über K heißt rekursiv definiert durch die Gleichung*

$$f(x,y) = 0,$$

falls

$$F_k = K(x_0, x_1, x_2, \ldots, x_k) \text{ mit } f(x_i, x_{i+1}) = 0 \text{ für alle } 0 \leq i \leq k-1$$

und die Polynome $f(x_i, y)$ absolut irreduzibel sind über $K(x_0, x_1, \ldots, x_i)$ für alle i mit $0 \leq i \leq k-1$.

Setzt man (mit den Bezeichnungen wie in der obigen Definition) $F_i = K(x_0, x_1, \ldots, x_i)$, so ist die Folge $(F_i)_{i \geq 0}$ eine Darstellung von $\mathcal{T}$. Falls nicht ausdrücklich anders angegeben, wählen wir diese Darstellung stets als kanonische Darstellung zu dem durch die Gleichung $f(x,y) = 0$ rekursiv definierten Turm.

Es sei $\mathcal{T}$ ein rekursiv durch die Gleichung $f(x,y) = 0$ definierter Turm über K. Dann erhalten wir eine Pyramide von Teilerweiterungen (vgl. Abb. 1.1). Setzen wir $F_{i,j} := K(x_i, x_{i+1}, \ldots, x_j)$, so sind die Körper $F_k, F_{1,k+1}, F_{2,k+2}, \ldots$ paarweise isomorph. Diese Struktur der Teilkörperpyramide werden wir häufig in der folgenden Weise verwenden: Da die isomorphen Körper $F_{k,k+1}/F_{k,k}$ (bzw. $F_{k,k+1}/F_{k+1,k+1}$) explizit durch eine Gleichung definierte Erweiterungen von rationalen Funktionenkörpern sind, können wir ihre Eigenschaften leicht beschreiben. Nun erzielen wir Ergebnisse für die Körpererweiterungen F_{k+1}/F_k, indem wir die für die Erweiterungen $F_{k,k+1}/F_{k,k}$ gewonnenen Eigenschaften "liften".

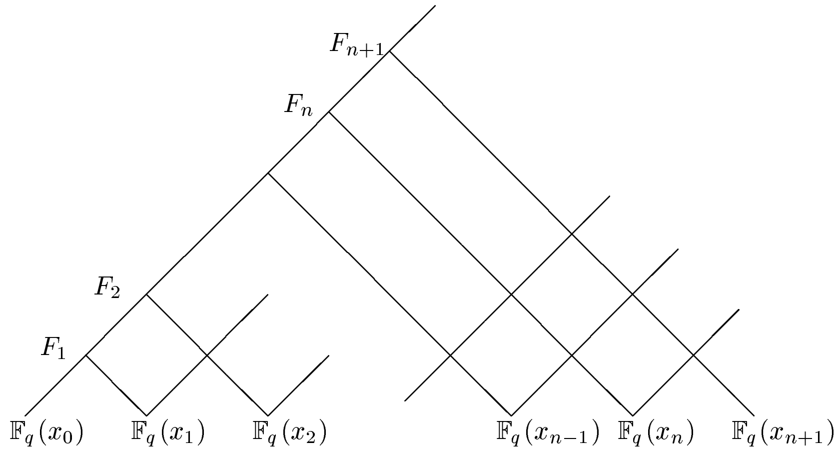

Abbildung 1.1: Pyramide algebraischer Funktionenkörper

Da für alle $k \geq 0$ das Polynom $f(x_k, y)$ absolut irreduzibel über F_k ist, erhalten wir für den Grad der Körpererweiterungen

$$[F_{k+1} : F_k] = [F_{1,k+1} : F_{1,k}].$$

Also ist

$$[F_{k+1} : F_{1,k+1}] = [F_k : F_{1,k}],$$

und die Gleichung $f(y_{k+1}, y_k) = 0$ definiert eine Folge $(E_k)_{k\geq 0}$, $E_k := K(y_0, y_1, y_2, \ldots, y_k)$, algebraischer Funktionenkörper, so daß die Polynome $f(x, y_k)$ absolut irreduzibel über E_k sind für alle $k \geq 0$. Da sich auch die Bedingungen (1),(2),(4) aus Definition 1.1.1 vom Turm $\mathcal{T}$ übertragen, erhalten wir einen Turm $\mathcal{S} := \cup_{k\geq 0} E_k$.

Definition 1.2.2 *Sei*

$$\mathcal{T} := \cup_{k\geq 0} F_k \text{ mit } F_{k+1} = F_k(x_{k+1}), \text{ wobei } f(x_k, x_{k+1}) = 0,$$

ein rekursiv definierter Turm. Dann heißt

$$\mathcal{S} := \cup_{k\geq 0} E_k \text{ mit } E_{k+1} = E_k(y_{k+1}), \text{ wobei } f(y_{k+1}, y_k) = 0,$$

der (unter $f(x,y)$) zu $\mathcal{T}$ duale Turm.

Bemerkung 1.2.3 *Seien* $(F_i)_{i\geq 0}$ *und* $(E_i)_{i\geq 0}$ *Darstellungen von zueinander dualen Türmen* $\mathcal{T}$ *und* $\mathcal{S}$. *Da* $F_i \cong E_i$, *erhalten wir*

$$\lambda(\mathcal{T}) = \lambda(\mathcal{S}).$$

Nur wenige Polynome $f(x,y)$ scheinen asymptotisch gute Türme zu definieren. Ein notwendiges Kriterium, um einen asymptotisch guten rekursiven Turm zu erhalten, können wir wie folgt angeben:

Theorem 1.2.4 *Es sei* $\mathcal{T}$ *ein rekursiv durch die Gleichung* $f(x,y) = 0$ *definierter Turm. Dann gilt notwendig*

$$\deg_x f(x,y) = \deg_y f(x,y).$$

Beweis: Vgl. [9]. □

Dieses Theorem motiviert die folgende Definition.

Definition 1.2.5 *Es sei* $\mathcal{T}$ *ein rekursiv durch die Gleichung* $f(x,y) = 0$ *definierter Turm.* $\mathcal{T}$ *heißt gerade, falls* $\deg_x f(x,y) = \deg_y f(x,y)$. *Der Turm heißt schief, falls er nicht gerade ist.*

Zur Erläuterung der hier eingeführten Begriffe wollen wir einen aus der Literatur bekannten asymptotisch optimalen Turm im Detail diskutieren.

Beispiel 1.2.6 *(Vgl. [8, Bsp. 2.4]). Die Gleichung*

$$y^2 = -(x+1)^2 + 1 \tag{1.1}$$

definiert rekursiv einen asymptotisch optimalen Turm $\mathcal{F} = \cup_{k\geq 0} F_k$ *über* $\mathbb{F}_9$, *d.h.* $\lambda(\mathcal{F}) = 2$.

Beweis: Zunächst beweisen wir, daß Gleichung 1.1 rekursiv einen Turm definiert. Wir zeigen dazu, daß in jedem Schritt k mindestens eine Stelle $P \in \mathbb{P}_{F_k}$ in F_{k+1} vom Index 2 verzweigt ist. Nach der Gradformel (vgl. [15, III.1.11]) ist dann $[F_{k+1} : F_k] = 2$ und $\mathbb{F}_9$ der exakte Konstantenkörper von F_{k+1} für alle $k \geq 0$ (da Konstantenkörpererweiterungen unverzweigt sind). Also ist $\mathcal{F}$ nicht endlich erzeugt und hat exakten Konstantenkörper $\mathbb{F}_9$. Die Gleichung 1.1 hat bei $x = 0$ eine einfache Nullstelle der rechten Seite. Nach der Theorie der Kummerschen Erweiterungen verzweigt die Nullstelle $P_0 \in \mathbb{P}_{F_0}$ von x_0 in F_1/F_0 vom Index 2. Die einzige Stelle $P_0' \in \mathbb{P}_{F_1}$ über P_0 ist eine einfache Nullstelle von x_1. Da die Gleichung (1.1) den Körper $\mathcal{F}$ rekursiv definiert, ist die Stelle P_0 in F_k für alle $k > 0$ vom Index 2^k verzweigt.

Als nächstes zeigen wir, daß zumindest eine $\mathbb{F}_9$-rationale Stelle von F_0 in $\mathcal{F}$ komplett zerfällt. Wir betrachten eine Polstelle Q von x_0 in F_i. Dann ist

Q auch eine Polstelle von x_i, und aus der definierenden Gleichung erhalten wir

$$\left(\frac{x_{i+1}}{x_i}\right)^2 = -\left(1+\frac{1}{x_i}\right)^2 + \frac{1}{x_i^2}.$$

Nach Reduktion modulo Q erhalten wir also die Kongruenz

$$\left(\frac{x_{i+1}}{x_i}\right)^2 \equiv -1 \pmod{Q},$$

die in $\mathbb{F}_9$ zwei Lösungen hat. Nach dem Theorem von Kummer (vgl. [15, III.5.10]) zerfällt die Stelle Q komplett in F_{i+1}/F_i. Induktiv erhalten wir, daß die Polstelle $P_\infty \in \mathbb{P}_{F_0}$ von x_0 in $\mathcal{F}$ komplett zerfällt.

Schließlich beweisen wir die Endlichkeit des Verzweigungsorts. Dazu sei $P \in \mathbb{P}_{F_0}$ irgendeine Stelle, die in $\mathcal{F}$ verzweigt. Dann existiert ein Index n und eine Stelle $Q \in \mathbb{P}_{F_n}$ über P, so daß Q in F_{n+1} verzweigt. Aus der Verzweigungstheorie Kummerscher Erweiterungen folgt nun

$$-(x_n(Q)+1)^2+1=0,$$

d.h. $x_n(Q) \in \mathbb{F}_3$ (beachte dazu, daß jede Polstelle von x_n unverzweigt ist). Durch Reduktion der definierenden Gleichung erhalten wir $x_{n-1}(Q) \in \mathbb{F}_3$ und induktiv $x_0(Q) \in \mathbb{F}_3$. Also ist die Stelle P Nullstelle von x_0, x_0-1 oder x_0+1 und der Verzweigungsort $V_{F_0}(\mathcal{F}) \subseteq \{P_0, P_1, P_{-1}\}$, wobei P_α die Nullstelle von $x_0-\alpha$ bezeichnet. Wir können nun den Grenzwert abschätzen:

$$2 \leq \lambda(\mathcal{F}) \leq 2,$$

wobei die erste Ungleichung aus Theorem 1.1.12 folgt und die zweite Ungleichung gerade die Drinfeld-Vladut-Schranke ist. □

Die definierende Gleichung einer Darstellung eines Turms ist nicht eindeutig bestimmt. Durch eineindeutige Variablentransformationen kann man unterschiedliche Gleichungen für die gleiche Darstellung angeben. Insbesondere ist die Frage, ob zwei Gleichungen denselben Turm definieren, durchaus nicht-trivial (vgl. dazu Kapitel 2.2 sowie die Diskussion in [10, rem. 5.9, 5.10] und [13]).

Beispiel 1.2.7 *Die Gleichung*

$$y^2 = \frac{x^2}{x-1}$$

definiert den gleichen Turm $\mathcal{F}$ über $\mathbb{F}_9$ wie die Gleichung aus Beispiel 1.2.6.

Beweis: Die Funktionen x_i aus Beispiel 1.2.6 genügen definitionsgemäß den Relationen

$$x_{i+1}^2 = -x_i^2 + x_i.$$

D.h. die Funktionen $\tilde{x}_i := 1/x_i$ genügen den Relationen

$$1/\tilde{x}_{i+1}^2 = -1/\tilde{x}_i^2 + 1/\tilde{x}_i,$$

also

$$\tilde{x}_{i+1}^2 = \frac{\tilde{x}_i^2}{\tilde{x}_i - 1}.$$

Da die Funktionen $x_0, x_1, \ldots, x_i$ und $\tilde{x}_0, \tilde{x}_1, \ldots, \tilde{x}_i$ dieselbe Funktionenkörpererweiterung über $\mathbb{F}_9(x_0)$ erzeugen, folgt die Behauptung. $\square$

Für die Untersuchung der Verbandsstruktur von Türmen über einem fest gewählten Konstantenkörper K erweist sich die folgende Diskussion der durch gebrochen rationale lineare Transformationen induzierten Turmautomorphismen als überaus hilfreich.

Es sei $\mathcal{F}/K$ ein durch eine Gleichung $f(x,y) = 0$ rekursiv definierter Turm mit Darstellung $(F_k)_{k\geq 0}$. Weiter sei $\epsilon \in PGL(2,K)$ eine gebrochen rationale lineare Transformation, so daß

$$f(\epsilon(x), \epsilon(y)) = \mu f(x,y) \text{ für ein } \mu \in K^*. \tag{1.2}$$

Dann induziert ϵ einen Körperautomorphismus σ_0 von F_0 mit $\sigma_0(x_0) = \epsilon(x_0)$, der gemäß Gleichung 1.2 fortgesetzt werden kann zu einem Automorphismus σ_k von F_k mit $\sigma_k(x_j) = \epsilon(x_j)$ für $0 \leq j \leq k$. Wir bezeichnen den Fixkörper von F_k unter $< \sigma_k >$ mit E_k und setzen $\mathcal{E} := \cup_{k\geq 0} E_k$. Es ist $\mathcal{F}/\mathcal{E}$ galoissch mit $[\mathcal{F} : \mathcal{E}] = ord(\epsilon)$. In Analogie zu [13] nennen wir diesen Turm den Quotienten von $\mathcal{F}$ (unter ϵ).

Ähnliches gilt, falls eine gebrochen rationale lineare Transformation $\epsilon \in PGL(2,K)$ existiert, so daß

$$f(\epsilon(x), y) = \mu f(x,y) \text{ für ein } \mu \in K^*. \tag{1.3}$$

Wir betrachten wieder den durch ϵ induzierten Körperautomorphismus $\sigma_0 \in Aut(F_0/K)$, der in diesem Fall zu einem Körperautomorphismus σ_k von F_k fortgesetzt werden kann mit $\sigma_k(x_j) = x_j$ für $1 \leq j \leq k$. Wir erhalten einen Teilturm $\mathcal{E} = K(y_0, x_1, x_2, \ldots)$, wobei y_0 erzeugendes Element von E_0 ist. Es ist wieder $\mathcal{F}/\mathcal{E}$ galoissch mit $[\mathcal{F} : \mathcal{E}] = ord(\epsilon)$. In diesem Fall gilt für den Quotienten und die isomorphen Türme $\mathcal{F} := K(x_0, x_1, x_2, \ldots)$ und $\tilde{\mathcal{F}} := K(x_1, x_2, x_3, \ldots)$, daß $\tilde{\mathcal{F}} \subseteq \mathcal{E} \subseteq \mathcal{F}$. Insbesondere ist also $\lambda(\mathcal{E}) = \lambda(\mathcal{F})$.

Unter den folgenden Voraussetzungen können wir den Quotienten $\mathcal{E}$, definiert durch ϵ wie in 1.2 oder in 1.3, explizit als rekursiv definierten Turm angeben: Es gebe eine rationale Funktion $r(t) \in K(t)$, so daß $E_1 = K(r(x_0), r(x_1))$ gilt. Weiter bezeichne $F(X,Y)$ ein vom Grad minimales Polynom, so daß

$$F(r(x_0), r(x_1)) = 0.$$

Falls die Gleichung $F(X,Y)=0$ rekursiv einen Turm $\mathcal{S}$ definiert, so gilt $\mathcal{S}=\mathcal{E}$. Der Quotient von $\mathcal{F}$ unter ϵ ist in diesem Fall also rekursiv durch die Gleichung $F(X,Y)=0$ definiert; denn wegen

$$r(x_k)^\sigma = r(x_k^\sigma) = r(x_k^\epsilon) = r(x_k) \text{ für alle } k \geq 0$$

im Fall 1.2 und

$$r(x_0)^\sigma = r(x_0) \text{ und } r(x_k)^\sigma = r(x_k^\sigma) = r(x_k^{id}) \text{ für alle } k \geq 1$$

im Fall 1.3 ist $\mathcal{S}$ fix unter σ. Also ist $\mathcal{S} \subseteq \mathcal{E}$. Da $E_1 = K(r(x_0), r(x_1))$, ist $\deg_Y F(X,Y) = [E_1 : E_0] = [F_1 : F_0]$. Da weiter $F(X,Y)$ rekursiv einen Turm definiert, ist $F(y_k, Y)$ absolut irreduzibel über dem durch $F(X,Y)$ rekursiv definierten Körper $K(y_0, y_1, \ldots, y_k)$. Wegen $E_k \supseteq K(y_0, y_1, \ldots, y_k)$, ist also sogar $E_k = K(y_0, y_1, \ldots, y_k)$ und damit $\mathcal{E} = \mathcal{S}$.

Falls $\mathcal{E}$ ein Teilturm von $\mathcal{F}$ ist, schreiben wir auch $\mathcal{E} \prec \mathcal{F}$.

Beispiel 1.2.8 *Als Beispiel betrachten wir den in [10] diskutierten asymptotisch optimalen Turm $\mathcal{M}/\mathbb{F}_{q^2}$, der durch*

$$x_{i+1}^2 = \frac{x_i^2+1}{2x_i} \text{ für } i \geq 0, \tag{1.4}$$

rekursiv definiert ist. Die rechte Seite von Gleichung 1.4 ist fix unter der Involution $\epsilon : x_i \mapsto 1/x_i$. Wir definieren den Quotienten, indem wir definierende Funktionen $y_i = x_i + 1/x_i$ einführen. Dann folgt aus Gleichung 1.4, $x_{i+1}^2 = \frac{1}{2} y_i$, $1/x_{i+1}^2 = 2/y_i$ und, indem wir beide Gleichungen addieren,

$$y_{i+1}^2 = \frac{(y_i+2)^2}{2y_i}. \tag{1.5}$$

Gleichung 1.5 definiert rekursiv denselben Unterturm $\mathcal{N}$ wie die in [10] angegebene Gleichung

$$y_{i+1}^2 = \frac{(y_i+1)^2}{4y_i}. \tag{1.6}$$

Dieselbe Involution wie oben kann nun auf Gleichung 1.6 angewandt werden, was zu dem (optimalen) Unterturm $\mathcal{L}$ führt, der rekursiv durch

$$z_{i+1}^2 = \frac{(z_i+3)^2}{8(z_i+1)}$$

definiert ist (vgl. [10]).

Kapitel 2

Konstruktion rekursiv definierter Türme

In diesem Kapitel wollen wir hinreichende Bedingungen diskutieren, damit ein Polynom $f(x,y)$ rekursiv einen Turm definiert, und neue Beispiele asymptotisch guter Türme angeben.

Es sei in diesem Kapitel stets $f(x,y) \in \mathbb{F}_q[x,y]$ ein in x und in y separables, absolut irreduzibles Polynom mit $\deg_x f(x,y) > 1$ und $\deg_y f(x,y) > 1$. Um zu prüfen, ob das Polynom $f(x,y)$ rekursiv einen nicht endlich erzeugten Körper $\mathcal{T}$ definiert, in dem $\mathbb{F}_q$ algebraisch abgeschlossen ist, betrachten wir die folgende rekursive Konstruktion:
Rekursionsbeginn: $F_0 := \mathbb{F}_q(x_0)$.
Rekursionsschritt: Falls $f(x_{k-1}, T)$ absolut irreduzibel ist über F_{k-1}, definiere $F_k := F_{k-1}(x_k)$ mit $f(x_{k-1}, x_k) = 0$.

Wenn die obige Konstruktion in einem Schritt abbricht, definiert das Polynom $f(x,y)$ rekursiv keinen Turm. Andernfalls ist der Körper $\mathcal{T} := \cup_{k\geq 0} F_k$ nicht endlich erzeugt, und $\mathbb{F}_q$ ist algebraisch abgeschlossen in $\mathcal{T}$. In diesem Fall genügt der Körper $\mathcal{T}$ den Bedingungen 1., 2. und 3. aus Definition 1.1.1.

Da wir uns nur für asymptotisch gute Türme $\mathcal{T}$ interessieren, können wir die Bedingung 4. aus Definition 1.1.1 ($\mathcal{T}$ enthält einen Funktionenkörper $F < \mathcal{T}$ mit $g(F) > 1$) wie folgt nachweisen: Falls die oben beschriebene Rekursion nicht abbricht, so erhalten wir höchstens dann einen asymptotisch guten Turm $\mathcal{T} := \cup_{k\geq 0} F_k$, wenn ($\mathcal{T}$ ein Turm ist und) die Zerfällungsrate $\nu_{F_0}(\mathcal{T})$ größer als Null ist. Das impliziert, daß die Anzahl $\mathbb{F}_q$-rationaler Stellen von F_k für wachsendes k ansteigen muß. Nach der Hasse-Weil-Schranke muß dann aber auch das Geschlecht der rekursiv definierten Körper F_k anwachsen. Entsprechend werden wir im folgenden stets von einem *nicht endlich erzeugten Körper* $\mathcal{T}$ sprechen, wenn die obige Rekursion nicht abbricht. Falls wir sicherstellen können, daß ein Körper $F < \mathcal{T}$ existiert mit $g(F) > 1$, so ist $\mathcal{T}$ ein Turm.

Man sieht leicht, daß die obige, rekursive Konstruktion genau dann abbricht, wenn sie über einem algebraischen Abschluß $\bar{\mathbb{F}}_q$ anstelle von $\mathbb{F}_q$ abbricht. Wir können also die Konstruktion stets über einem algebraisch abgeschlossenen Konstantenkörper ausführen.

2.1 Unendlich verzweigte Türme

Im allgemeinen kann man von der Irreduzibilität des Polynoms $f(x,y)$ über $\bar{\mathbb{F}}_q$ nicht darauf schließen, daß $f(x,y)$ rekursiv einen Turm definiert. So konnte bislang für eine Familie von Fermat-Gleichungen nur unter der Annahme, daß sie rekursiv einen Turm definieren, gezeigt werden, daß dieser dann asymptotisch gut ist (vgl. [10, ch. 3], dazu Kap. 4, Theorem 4.1.1).

Beispiel 2.1.1 *Die Gleichung*

$$y^m = ax^m + c \textit{ mit } a, c \in \mathbb{F}_q^* \textit{ und } (m,q) = 1 \tag{2.1}$$

definiert rekursiv keinen Turm $\mathcal{F}$.

Beweis: Angenommen die Gleichung 2.1 definierte rekursiv einen Turm $\mathcal{F}/\bar{\mathbb{F}}_q$ mit $\mathcal{F} = \cup_{k\geq 0} F_k$. Dann wäre $\mathcal{F}$ nicht endlich erzeugt und insbesondere $[F_k : F_{k-1}] > 1$ für alle $k \geq 1$, vgl. Kapitel 1.2. Nun ist aber $F_k = F_{k-1}(x_k)$, und

$$x_k^m = a^k x_0^m + (1 + a + a^2 + \ldots + a^{k-1})c.$$

D.h. $[F_k : F_{k-1}] = 1$ für $k = char\mathbb{F}_q$, falls $a = 1$, bzw. $k = ord(a)$ sonst. □

Wie in Abschnitt 2.2 ausgeführt wird, wurde computergestützt nach Polynomen $f(x,y)$ mit $\deg_x f(x,y) = \deg_y f(x,y) = 2$ über kleinen Körpern mit kleiner Charakteristik gesucht, die rekursiv asymptotisch gute Türme liefern. Für einige Gleichungen ist es nicht gelungen nachzuweisen, daß sie rekursiv nicht endlich erzeugte Körper definieren. Unter der Annahme jedoch, daß sie nicht endlich erzeugte Körper definieren, definieren sie sogar asymptotisch gute Türme. Im folgenden sind einige Beispiele aufgeführt, von denen man zeigen kann, daß sie rekursiv endlich erzeugte Körper definieren. Für eine genauere Beschreibung der computergestützten Suche verweisen wir auf Abschnitt 2.2.

Beispiel 2.1.2 *Als ein Beispiel betrachten wir das Polynom*

$$f(x,y) = xy^2 + (2x^2 + x + 1)y + 2x \tag{2.2}$$

über $\mathbb{F}_3$. Die Gleichung $f(x,y) = 0$ definiert rekursiv keinen Turm $\mathcal{T}$.

Beweis: Da die Nullstelle von $x_0^4 + x_0^3 + 2x_0 + 1$ in F_0 verzweigt ist in F_1, ist das Polynom $f(x_0, x_1)$ absolut irreduzibel über F_0. Wir nehmen an, daß die Gleichung $f(x,y) = 0$ rekursiv eine Turm $\mathcal{T}$ definiert. Es sei $\epsilon(x) := 2/x$. Dann ist

$$\begin{array}{rcr} f(\epsilon(x), \epsilon(y)) & = 2x^{-1}y^{-2} + x^{-2}y^{-1} + x^{-1}y^{-1} + 2y^{-1} + x^{-1} & = 0 \\ \Leftrightarrow & 2x + y + xy + 2x^2y + xy^2 = f(x,y) & = 0. \end{array}$$

Gemäß der Diskussion am Ende von Abschnitt 1.2 induziert ϵ einen Automorphismus σ auf $\mathcal{T}$. Wir betrachten die durch die Funktionen $X_i = x_i + \epsilon(x_i)$ definierten Teilkörper $E_i := \mathbb{F}_3(X_0, X_1, \ldots, X_i)$ vom Fixkörper von F_i unter σ. Nun ist

$$\begin{array}{rcr} f(x_i, x_{i+1}) & = 2(x_i^2 x_{i+1} + 2x_{i+1} + 2x_{i+1}^2 x_i + x_i + 2x_i x_{i+1}) & = 0 \\ \Leftrightarrow & x_i + 2x_i^{-1} + 2x_{i+1} + x_{i+1}^{-1} + 2 = X_i + 2X_{i+1} + 2 & = 0. \end{array}$$

Daher ist $X_i = X_{i+3}$. Da das Minimalpolynom von x_i über $\mathbb{F}_3(X_i)$ gleich $m_{x_i}(T) = T^2 + 2X_i + 2 = (T - x_i)(T + x_i^{-1})$ ist, folgt nun, daß $x_{i+3} \in F_i$. Also definiert, im Widerspruch zu der Annahme, $f(x,y)$ keinen unendlich erzeugten Körper und insbesondere keinen Turm. $\Box$

In ähnlicher Weise können wir für die folgenden Polynome argumentieren, daß sie keine Türme definieren:

$(x^2+1)y^2 + (x^2+x)y + 1 + 2x$	über $\mathbb{F}_3$
$(x^2+1)y^2 + (x^2+2x+2)y + 2 + x$	über $\mathbb{F}_3$
$x^2y^2 + (x^2+2x+2)y + x^2 + 2x + 2$	über $\mathbb{F}_3$
$xy^2 + (4x^2+x+4)y + x$	über $\mathbb{F}_5$
$xy^2 + (4x^2+x+2)y + 3x$	über $\mathbb{F}_5$
$xy^2 + (4x^2+x+1)y + 4x$	über $\mathbb{F}_5$
$xy^2 + (2x^2+x+4)y + 2x$	über $\mathbb{F}_5$
$xy^2 + (2x^2+x+3)y + 4x$	über $\mathbb{F}_5$

Als nächstes wollen wir ein allgemeines Kriterium für das definierende Polynom $f(x,y)$ angeben, welches sicherstellt, daß es über jedem der rekursiv definierten Körper F_k absolut irreduzibel ist. Wir benötigen dazu das folgende Lemma, welches im Zusammenhang mit rekursiv definierten Türmen weite Anwendung findet.

Lemma 2.1.3 *Es seien F_1 und F_2 über $F := F_1 \cap F_2$ linear disjunkte algebraische Funktionenkörper über einem perfekten Konstantenkörper. Es sei $F' := F_1F_2$ das Kompositum von F_1 und F_2. Weiter sei P eine Stelle von F, und P_1 resp. P_2 seien Stellen über P in F_1 resp. F_2. Dann existiert mindestens eine Stelle P' in F', die über P_1 und P_2 liegt.*

Beweis: Es seien zunächst F_1/F und F_2/F separabel. Mit $\tilde{F}$ bezeichnen wir die normale Hülle von F' über F. Weiter seien $Q_1 = P_1, Q_2, \ldots, Q_n$ die Stellen von F_1 über P. Wir wählen ein Element $t \in F_1$ mit $v_{Q_1}(t) > 0$ und $v_{Q_i}(t) < 0$ für $i = 2, \ldots, n$ (eine solche Wahl ist nach dem schwachen Approximationssatz möglich).

Wir betrachten eine Stelle $\tilde{P}$ von $\tilde{F}$ über P_2. Es sei $\tilde{Q}_1 \in \mathbb{P}_{\tilde{F}}$ eine Stelle über Q_1. Da die Galoisgruppe von $\tilde{F}/F$ transitiv auf den Stellen über P wirkt, existiert ein $\sigma \in Gal(\tilde{F}/F)$ mit $\tilde{Q}_1^{\sigma} = \tilde{P}$. Dann ist insbesondere $t^{\sigma} \in \tilde{P}$.

Es sei f das Minimalpolynom von t über F. Da F_1 und F_2 über F linear disjunkt sind, ist f irreduzibel über F_2. Die Galoisgruppe von $\tilde{F}/F_2$ wirkt transitiv auf den Nullstellen von f. Da t und t^{σ} Nullstellen von f sind, existiert ein $\tau \in Gal(\tilde{F}/F_2)$ mit $t^{\sigma\tau} = t$.

Wir setzen $P' := \tilde{P}^{\tau} \cap F'$. Da $\tilde{P}|P_2$ nach der Wahl von $\tilde{P}$ und τ den Körper F_2 elementweise fest läßt, gilt $P'|P_2$. Da $t \in P'$ gilt, folgt aus $P' \cap F_1 = Q_j$ für ein $j \in \{1, \ldots, n\}$, daß $P'|P_1$ gilt.

Sei nun $F \subseteq E_i \subseteq F_i, E_i/F$ separabel und F_i/E_i rein inseparabel. Wir setzen $E' := E_1E_2$ und $Q_i := P_i \cap E_i$. Nach dem ersten Teil des Beweises existiert eine Stelle Q' mit $Q'|Q_i$. Da die Erweiterung F'/E' rein inseparabel ist und in rein inseparable Erweiterungen alle Stellen nur total verzweigte Erweiterungen besitzen, folgt nun das Lemma auch im inseparablen Fall. $\square$

Korollar 2.1.4 *Es sei $F_n = K(x_0, x_1, \ldots, x_n)$ ein rekursiv durch die Gleichung $f(x, y)$ definierter Körper über einem perfekten Konstantenkörper K für ein $n \geq 1$. Wir setzen $F_{i,j} = K(x_i, x_{i+1}, \ldots, x_j)$ für $0 \leq i \leq j \leq n$. Für $0 \leq i \leq j \leq k \leq l \leq n$ seien P, P_1 resp. P_2 Stellen in $F_{j,k}, F_{i,k}$ resp. $F_{j,l}$ mit $P_1|P$ und $P_2|P$. Dann existiert eine Stelle P' in $F_{i,l}$, die über P_1 und P_2 liegt.*

Beweis: Da das Polynom $f(x_k, Y)$ absolut irreduzibel über F_k ist für $k = 0, \ldots, n-1$, ist
$$[F_{j,l} : F_{j,k}] = [F_{i,l} : F_{i,k}].$$
Also ist $[F_{i,l} : F_{j,l}] = [F_{i,k} : F_{j,k}]$, und die Körper $F_{i,k}$ und $F_{j,l}$ sind über $F_{j,k}$ linear disjunkt. Damit folgt die Behauptung aus Lemma 2.1.3. $\square$

Es bezeichne $\bar{\mathbb{F}}_q$ einen algebraischen Abschluß von $\mathbb{F}_q$, und $F = \bar{\mathbb{F}}_q(x, y)$ sei ein algebraischer Funktionenkörper mit definierender Gleichung
$$f(x, y) = 0. \tag{2.3}$$
Für Elemente $\nu, \mu \in \mathbb{P}^1 = \bar{\mathbb{F}}_q \cup \{\infty\}$ schreiben wir $\nu \leftarrow \mu$, falls eine Stelle Q in F existiert, so daß $x(Q) = \nu$ und $y(Q) = \mu$ ist. Weiter definieren wir die

Mengen

$$
\begin{aligned}
M \quad := \quad & \Big\{\alpha \in \mathbb{P}^1 | P \in \mathbb{P}_{\bar{\mathbb{F}}_q(x)} \text{ mit } x(P) = \alpha \text{ verzweigt in} \\
& F/\bar{\mathbb{F}}_q(x) \text{ vom Index } e = \deg_y f \Big\}
\end{aligned}
\tag{2.4}
$$

und

$$
\begin{aligned}
N \quad := \quad & \Big\{\alpha \in \mathbb{P}^1 | Q \in \mathbb{P}_{\bar{\mathbb{F}}_q(y)} \text{ mit } y(Q) = \alpha \text{ hat mindestens eine} \\
& \text{Fortsetzung in } F\text{, die vom Index } e \text{ verzweigt ist} \\
& \text{mit } \gcd(e, \deg_y f) > 1 \Big\}\,.
\end{aligned}
\tag{2.5}
$$

Lemma 2.1.5 *Es existiere für ein $\mu_0 \in M \setminus N$ eine Folge $(\mu_i)_{i\geq 0}$ in $\mathbb{P}^1 \setminus N$, so daß $\mu_{i+1} \leftarrow \mu_i$ für alle $i \geq 0$. Dann gilt für die durch Gleichung 2.3 über $\mathbb{F}_q$ rekursiv definierten Körper $F_{k+1} = F_k(x_{k+1})$, daß $[F_{k+1} : F_k] = deg_y f$ und daß $\mathbb{F}_q$ der exakte Konstantenkörper von F_{k+1} ist. Insbesondere ist der Körper $\mathcal{F} = \cup_{k\geq 0} F_k$ nicht endlich erzeugt.*

Beweis: Wir zeigen induktiv, daß in jedem Körper F_k mindestens eine Stelle existiert, die in F_{k+1} vom Index $m = [F_1 : F_0]$ verzweigt ist. Die Behauptung ist dann eine direkte Folgerung aus der Gradformel und der Tatsache, daß Konstantenkörpererweiterungen unverzweigt sind.

Für den Körper F_0 ist dieses richtig, da die Stelle $P \in \mathbb{P}_{F_0}$ mit $x_0(P) = \mu_0$ in F_1 total verzweigt. Sei nun die Behauptung richtig für $0 \leq i < k$. Gemäß der Definition der Folge $(\mu_i)_{i\geq 0}$ existieren Stellen Q_i in $\bar{\mathbb{F}}_q(x_i, x_{i+1})$, so daß $x_i(Q_i) = \mu_{k-i}$ und $x_{i+1}(Q_i) = \mu_{k-i-1}$ für $0 \leq i < k$. Nach Induktionsvoraussetzung sind die Polynome $f(x_i, Y)$ für $0 \leq i < k$ absolut irreduzibel. Durch wiederholte Anwendung von Korollar 2.1.4 erhalten wir eine Stelle Q in F_k, die über allen Stellen Q_i mit $0 \leq i < k$ liegt. Da die Stelle Q über $Q \cap \bar{\mathbb{F}}_q(x_k)$ den Verzweigungsindex r mit $\gcd(r, m) = 1$ hat und die Stelle $Q \cap \bar{\mathbb{F}}_q(x_k)$ in $\bar{\mathbb{F}}_q(x_k, x_{k+1})$ total verzweigt, verzweigt die Stelle Q nach Abhyankars Lemma in F_{k+1} vom Index m. $\square$

Wir betrachten den Körper $F := \mathbb{F}_q(x, y)$ mit $f(x, y) = 0$. Das Minimalpolynom $m_y(Y)$ von y, dem erzeugenden Element von $F/\mathbb{F}_q(x)$, erhalten wir, indem wir das Polynom

$$f(x, Y) = f_0(x) + f_1(x)Y + \ldots + f_m(x)Y^m$$

durch den Leitkoeffizienten $f_m(x)$ teilen. Ist andererseits $m_y(Y) \in \mathbb{F}_q(x)[Y]$ das Minimalpolynom eines erzeugenden Elements von $F/\mathbb{F}_q(x)$, so erhalten wir eine definierende Gleichung in $\mathbb{F}_q[x, y]$, indem wir $m_y(Y)$ mit einem geeigneten Polynom in x multiplizieren und Y durch y ersetzen. Man sieht daher, daß wir rekursiv definierte Türme mit Hilfe des Minimalpolynoms eines $F/\mathbb{F}_q(x)$ erzeugenden Elements anstelle der Gleichung $f(x, y) = 0$ definieren können.

Falls $m_y(Y) \in \mathbb{F}_q(x)[Y]$ ganz ist über einer der Stellen P_μ mit $\mu \in M \setminus N$, können wir häufig mithilfe des Theorems von Kummer die Existenz von Folgen $(\mu_k)_{k\geq 0}$, wie in Lemma 2.1.5 verlangt, sicherstellen.

Wir definieren das zu $m_y(Y)$ reziproke Polynom

$$\bar{m}_y(Y) := \frac{1}{a_0} Y^m m_y(Y^{-1}),$$

wobei m der Grad von $m_y(Y)$ ist und a_0 den konstanten Term von $m_y(Y)$ bezeichnet.

Weiter sei $P_\mu \in \mathbb{P}_{\bar{\mathbb{F}}_q(x)}$ die Stelle mit $x(P_\mu) = \mu$.

Satz 2.1.6 *Es existiere eine Folge $(\mu_k)_{k\geq 0}$ in $\mathbb{P}^1 \setminus N$, so daß*

1. *$\mu_0 \in M \setminus N$ und*
2. *für jedes $k \geq 0$ das Polynom $m_y(Y)$ ganz über der Stelle P_{μ_k} sei und $m_y(\mu_{k+1}, \mu_k) = 0$ oder das Polynom $\bar{m}_y(Y)$ ganz über der Stelle P_{μ_k} sei und $\bar{m}_y(\mu_{k+1}, \mu_k) = 0$.*

Dann definiert $m_y(Y)$ über $\mathbb{F}_q$ rekursiv einen unendlich erzeugten Körper $\mathcal{T}/\mathbb{F}_q$.

Beweis: Nach dem Theorem von Kummer gilt für alle $k \geq 0$, daß $\mu_{k+1} \leftarrow \mu_k$. Damit folgt die Behauptung aus 2.1.5. □

2.2 Beispiele unendlich erzeugter Körper

Viele *Kummersche Gleichungen* definieren rekursiv unendlich erzeugte Körper. Dabei nennen wir eine Gleichung Kummersch, wenn sie vom Typ

$$y^m = g(x)$$

ist, wobei $g(x) \in \mathbb{F}_q(x)$ mit $\gcd(m, q) = 1$ und $g \neq \omega^d$ für alle $d|m, d > 1$, und alle $\omega \in \mathbb{F}_q(x)$. Für $g(x) = g_1(x)/g_2(x)$ mit $g_1(x), g_2(x) \in \mathbb{F}_q[x]$ und $\gcd(g_1(x), g_2(x)) = 1$ vereinbaren wir, wie üblich,

$$\deg g(x) = \max\{\deg g_1(x), \deg g_2(x)\}.$$

Lemma 2.2.1 *Es sei*

$$m_y(Y) = Y^m - \frac{g_1(x)}{g_2(x)} \tag{2.6}$$

(für teilerfremde Polynome $g_1(x)$ und $g_2(x)$). Weiter sei

1. *$g_1(x) = x^r \tilde{g}_1(x)$ mit $\tilde{g}_1(0) \neq 0$ und $\gcd(r, m) = 1$ oder*

2. $\deg g_1(x) - \deg g_2(x) = r > 0$ *mit* $\gcd(r,m) = 1$.

Dann definiert Gleichung 2.6 über $\mathbb{F}_q$ *rekursiv einen unendlich erzeugten Körper* $\mathcal{T}/\mathbb{F}_q$.

Beweis: Wir setzen zunächst 1. voraus. Es sei P_0 die Nullstelle von x_0 in F_0. Wir zeigen induktiv, daß $[F_{k+1} : F_k] = m$ und daß genau eine total verzweigte Stelle P_{k+1} in F_{k+1} über P_k liegt, die Nullstelle der Funktionen x_j ist für $0 \leq j \leq k+1$ und Verzweigungsindex $e(P_{k+1}|P_{k+1} \cap \bar{\mathbb{F}}_q(x_{k+1})) = r^{k+1}$ hat.

Da $\gcd(r,m) = 1$, folgt für $k = 0$ aus dem Eisensteinkriterium (vgl. [15, III.1.14]), daß $[F_1 : F_0] = m$ und daß genau eine total verzweigte Stelle P_1 über der Stelle P_0 liegt. Gemäß der definierenden Gleichung ist die Stelle P_1 gemeinsame Nullstelle von x_0 und x_1. Wir setzen $Q := P_1 \cap \bar{\mathbb{F}}_q(x_1)$. Dann folgt wieder aus der definierenden Gleichung

$$m \cdot e(P_1|Q) = r \cdot e(P_1|P),$$

also $e(P_1|Q) = r$.

Seien nun die Induktionsbehauptungen richtig für alle j mit $0 \leq j < k$. Dann existiert nach Induktionsvoraussetzung eine Stelle P_k, die Nullstelle von x_k ist, mit $e(P_k|P_k \cap \bar{\mathbb{F}}_q(x_k)) = r^k$. Wegen $\gcd(r^k, m) = 1$ folgt aus Abhyankars Lemma und aus der Gradformel, daß $[F_{k+1} : F_k] = m$ und daß über der Stelle P_k genau eine total verzweigte Stelle P_{k+1} liegt. Gemäß der definierenden Gleichung ist die Stelle P_{k+1} gemeinsame Nullstelle der Funktionen x_j für $0 \leq j \leq k+1$. Da die Körper F_j, $0 \leq j \leq k+1$, rekursiv definiert sind, folgt aus Abhyankars Lemma, daß

$$e(P_{k+1}|P_{k+1} \cap K(x_{k+1})) = r^{k+1}.$$

Gilt nun 2., so folgt die Behauptung mit derselben Argumentation nach der Variablentransformation $\tilde{x} = 1/x$ und $\tilde{y} = 1/y$. □

Theorem 2.2.2 *Es sei* $F = \bar{\mathbb{F}}_q(x,y)$ *mit*

$$y^m = g(x). \tag{2.7}$$

Für kein $\alpha \in \bar{\mathbb{F}}_q^*$ *sei die Menge der* m*-ten Wurzeln von* α *in der Menge der Null- und Polstellen von* $g(x)$ *enthalten. Weiter existiere eine Stelle* P *in* $\mathbb{F}_q(y)$ *mit* $g(y) \in \mathcal{O}_P^*$*, die in* F *vom Index* $\deg g(x)$ *verzweigt ist.*
Dann definiert die Gleichung 2.7 über $\mathbb{F}_q$ *rekursiv einen nicht endlich erzeugten Körper* $\mathcal{F}$ *mit exaktem Konstantenkörper* $\mathbb{F}_q$.

Beweis: Genau dann ist $\mathcal{F}$ nicht endlich erzeugt, wenn der durch $g(y) = x^m$ rekursiv definierte Körper $\mathcal{T}$ nicht endlich erzeugt ist (vgl. Diskussion zu

Definition 1.2.2). Wir verwenden Lemma 2.1.5 angewandt auf den Körper $\mathcal{T}$ über $\bar{\mathbb{F}}_q$. Dazu seien M und N die durch die Gleichungen 2.4 und 2.5 definierten Mengen bezogen auf das Polynom $g(y) = x^m$.

Wir setzen $\mu_0 := y(P) \in \mathbb{P}^1$. Nach Voraussetzung ist $\mu_0 \in M \setminus N$, da $g(y) \in \mathcal{O}_P^*$ (beachte, daß $F/\bar{\mathbb{F}}_q(x)$ eine Kummererweiterung ist, also nur Polstellen und Nullstellen von $g(x)$ in $F/\bar{\mathbb{F}}_q(x)$ verzweigen).

Da für kein $\alpha \in \bar{\mathbb{F}}_q^*$ die Menge der m-ten Wurzeln von α in der Menge der Null- und Polstellen von $g(x)$ enthalten ist, können wir rekursiv Elemente $\mu_k \in \bar{\mathbb{F}}_q^*$ wählen, so daß $g(\mu_k) \in \bar{\mathbb{F}}_q^*$ und

$$\begin{aligned} \mu_1^m &= g(\mu_0), \\ \mu_2^m &= g(\mu_1), \\ \mu_3^m &= g(\mu_2), \\ &\vdots \qquad\qquad . \end{aligned}$$

$m_y(Y) = Y^m - g(x)$ ist das Minimalpolynom von y über $\bar{\mathbb{F}}_q(x)$. Da $g(\mu_i) \neq \infty$ für alle $i \geq 0$, ist $m_y(Y)$ ganz über den Nullstellen P_{μ_i} von $x - \mu_i$. Gemäß dem Theorem von Kummer gilt nun $\mu_{k+1} \leftarrow \mu_k$.

Da $g(\mu_k) \notin \{0, \infty\}$ nach Konstruktion der Elemente μ_k, gilt $\mu_k \notin N$.

Die Folge $(\mu_k)_{k\geq 0}$ erfüllt also die Voraussetzung aus Lemma 2.1.5, was die Behauptung beweist. □

Bemerkung 2.2.3 *Falls die Menge der Null- und Polstellen von g für ein $\alpha \in \bar{\mathbb{F}}_q$ die Menge der m-ten Wurzeln von α enthält, also die Voraussetzungen von Theorem 2.2.2 verletzt sind, kann die Gleichung trotzdem einen Turm definieren (vgl. Korollar 2.2.1 und Beispiel 2.3.3).*

Die folgenden Ergebnisse sind in Zusammenarbeit mit H. Maharaj entstanden. Um Gleichungen zu finden, die rekursiv gute Türme definieren, wurde ein Algorithmus in KASH implementiert, der die Bedingungen aus Lemma 2.1.5 überprüft sowie nach Beispielen mit endlichem Verzweigungsort und über $\mathbb{F}_q(x_0)$ komplett zerfallenden Stellen sucht. Es wurden dabei systematisch alle Polynome $f(x,y) \in \mathbb{F}_p[x,y]$ mit $\deg_x f(x,y) = \deg_y f(x,y) = 2$ mit $p = 3, 5, 7$ getestet (nach Theorem 1.2.4 genügt es, Polynome zu betrachten, die den selben Grad in x und y haben).

Um die Anzahl der Gleichungen zu reduzieren sowie Gleichungen, die den selben Turm definieren, miteinander zu identifizieren, wurde die folgende Vereinbarung getroffen: Es sei ϵ eine gebrochenrationale lineare Transformation. Dann definieren $f(x,y)$ und $f(\epsilon(x), \epsilon(y))$ den gleichen Turm $\mathcal{T}$. Wir definieren die folgende Äquivalenzrelation $\sim$ auf der Menge der Polynome: $f \sim g$ genau dann, wenn $f(x,y) = (cx+d)^m(cy+d)^m g(\epsilon(x), \epsilon(y))$ oder $f(x,y) = (cx+d)^m(cy+d)^m g(\epsilon(y), \epsilon(x))$ für eine gebrochenrationale lineare Transformation $\epsilon(x) = (ax+b)/(cx+d)$ und $\deg_x f(x,y) = \deg_y f(x,y) = m$

(vgl. dazu die Diskussion in 1.2). Es ist klar, daß $\sim$ eine Äquivalenzrelation definiert. Betrachtet werden nur noch kleinste Repräsentanten der Äquivalenzklassen bezüglich einer fest gewählten lexikographischen Anordnung der untersuchten Polynome.

Im folgenden wollen wir die gefundenen asymptotisch guten Türme für $q = 9, 25, 49$ und 7^4 auflisten und ein klares Bild ihrer Verbandsstruktur geben. Der Parameter q gibt dabei, wie oben erläutert, den Konstantenkörper $\mathbb{F}_q$ an, über dem der Turm definiert ist.

<u>$\mathbf{q = 9}$:</u>

Das Polynom

$$f(x, y) = (x^2 + 1)y^2 + 2xy + 2x^2 + 1 \tag{2.8}$$

definiert rekursiv einen Turm $\mathcal{T}$ über $\mathbb{F}_9$ mit Verzweigungsort

$$R_{\mathcal{T}} = \{\text{Nullstellen von } x_0^4 + x_0^2 + 2 \text{ und } x_0^4 + 2x_0^2 + 2\}.$$

Die Nullstellen von $x_0^4 + x_0^2 + 2$ sind im Turm total verzweigt. Es sei w ein primitives Element von $\mathbb{F}_9$, das der Gleichung $w^2 + 2w + 2 = 0$ genügt. Dann zerfallen die 6 Nullstellen der Elemente von

$$S = \{1/x_0, x_0, x_0 - w^j \text{ für } j = 2, 4, 6, 8\}$$

komplett in $\mathcal{T}$ über F_0. Gemäß Theorem 1.1.12 können wir den Grenzwert durch $\lambda(\mathcal{T}) \geq 2 \cdot 6/(-2 + 8) = 2$ abschätzen. Nach der Drinfeld-Vladut-Schranke ist der Turm $\mathcal{T} = \mathcal{T}_9$ optimal über $\mathbb{F}_9$.

In der gleichen Weise wie in [13] kann gezeigt werden, daß $\mathcal{T}$ kein Teilturm eines bekannten Turms ist, außer unter Umständen von $\mathcal{T}_1$. Der Vergleich von $\mathcal{T}$ und $\mathcal{T}_1$ scheint schwierig zu sein. Allerdings kann gezeigt werden, daß f_9 und f_1 nicht unter $\sim$ konjugiert sind.

Die folgenden Polynome $f_i(x, y)$ für $1 \leq i \leq 11$ definieren asymptotisch gute Türme $\mathcal{T}_i$ über $\mathbb{F}_9[x, y]$. Die Abschätzung des Grenzwerts $\lambda(\mathcal{T}_i)$ ist in der letzten Spalte angegeben (der Grenzwert wurde außer in den Fällen $i = 10, 11$ gemäß Theorem 1.1.12 abgeschätzt).

Ref:		$f_i(x,y)$:	$\lambda(\mathcal{T}_i) \geq$
[8]	$\mathcal{T}_1$:	$f_1(x,y) = y^2 + x^2 + x$	2
	$\mathcal{T}_2$:	$f_2(x,y) = y^2 + xy + 2x^2 + 1$	2/3
	$\mathcal{T}_3$:	$f_3(x,y) = y^2 + xy + 2x^2 + 2$	2/3
[3]	$\mathcal{T}_4$:	$f_4(x,y) = y^2 + x^2y + 1$	2
[10]	$\mathcal{T}_5$:	$f_5(x,y) = y^2 + (x^2+1)y + 1$	2
	$\mathcal{T}_6$:	$f_6(x,y) = y^2 + (x^2+1)y + 2x^2$	2/3
[13]	$\mathcal{T}_7$:	$f_7(x,y) = xy^2 + (2x^2+x+2)y + x^2 + 2x + 2$	2
	$\mathcal{T}_8$:	$f_8(x,y) = x^2y^2 + (2x+1)y + x^2 + 2x + 1$	2/3
	$\mathcal{T}_9$:	$f_9(x,y) = (x^2+1)y^2 + 2xy + 2x^2 + 1$	2
[13]	$\mathcal{T}_{10}$:	$f_{10}(x,y) = xy^2 + 2x^2y + x^2 + 2x + 1$	2
[13]	$\mathcal{T}_{11}$:	$f_{11}(x,y) = y^2 + (x^2+1)y + x^2 + x + 1$	2

Die Türme $\mathcal{T}_1$, $\mathcal{T}_4$ und $\mathcal{T}_5$ sind die Repräsentanten der Türme $\mathcal{L}$, $\mathcal{M}$ und $\mathcal{N}$ in [10] (vgl. Beispiel 1.2.7). Mittels der in Abschnitt 1.2 erklärten Technik können wir die folgenden Verbandsrelationen bestimmen:

-$\mathcal{T}_1 \prec \mathcal{T}_2, \mathcal{T}_3$

-$\mathcal{T}_5 \prec \mathcal{T}_6, \mathcal{T}_8$

-$\mathcal{T}_{11} \prec \mathcal{T}_{10} \prec \mathcal{T}_7, \mathcal{T}_9$

Nach Beispiel 1.2.7 haben wir weiterhin $\mathcal{T}_1 \prec \mathcal{T}_5 \prec \mathcal{T}_4$. Da die Türme $\mathcal{T}_{10}$ und $\mathcal{T}_{11}$ Teiltürme optimaler Türme sind, sind auch sie optimal. Das Polynom f_9 ist nicht $\sim$ konjugiert zu einem der anderen Polynome.

$\mathbf{q = 25}$:

Die folgenden Polynome $f_i(x,y)$ für $1 \leq i \leq 27$ definieren asymptotisch gute Türme $\mathcal{T}_i$ über $\mathbb{F}_{25}[x,y]$. Die Abschätzung des Grenzwerts $\lambda(\mathcal{T}_i)$ ist in der letzten Spalte angegeben (der Grenzwert wurde außer in den Fällen $i = 2, 19, 27$ gemäß Theorem 1.1.12 abgeschätzt).

Ref:		$f_i(x,y)$:	$\lambda(\mathcal{T}_i) \geq$
[10]	$\mathcal{T}_1$:	$f_1(x,y) = y^2 + x^2y + 4$	4
[4]	$\mathcal{T}_2$:	$f_2(x,y) = y^2 + x^2y + x$	4
[4]	$\mathcal{T}_3$:	$f_3(x,y) = y^2 + x^2y + 3x$	4
[10]	$\mathcal{T}_4$:	$f_4(x,y) = y^2 + (x^2+2)y + 1$	4
[3]	$\mathcal{T}_5$:	$f_5(x,y) = y^2 + (x^2+2)y + x^2$	4
[3]	$\mathcal{T}_6$:	$f_6(x,y) = y^2 + (x^2+2)y + 2x^2 + 1$	4
[4]	$\mathcal{T}_7$:	$f_7(x,y) = y^2 + (x^2+2)y + 3x^2 + 4x + 4$	4
	$\mathcal{T}_8$:	$f_8(x,y) = y^2 + (x^2+3)y + 4x^2$	1
[13]	$\mathcal{T}_9$:	$f_9(x,y) = xy^2 + (4x^2+x+1)y + x^2 + 2x + 3$	4
	$\mathcal{T}_{10}$:	$f_{10}(x,y) = xy^2 + (4x^2+x+2)y + 3x^2 + x + 4$	4
	$\mathcal{T}_{11}$:	$f_{11}(x,y) = x^2y^2 + (x^2+3)y + 4$	4
	$\mathcal{T}_{12}$:	$f_{12}(x,y) = x^2y^2 + (x^2+3x+3)y + 4$	3
	$\mathcal{T}_{13}$:	$f_{13}(x,y) = x^2y^2 + (x^2+4x+2)y + 4$	4
	$\mathcal{T}_{14}$:	$f_{14}(x,y) = x^2y^2 + (x^2+4x+2)y + 4x^2 + 2$	3
	$\mathcal{T}_{15}$:	$f_{15}(x,y) = x^2y^2 + (x^2+4x+4)y + 4x^2 + 3x + 2$	3
	$\mathcal{T}_{16}$:	$f_{16}(x,y) = (x^2+1)y^2 + (x+1)y + 2x^2 + 4x + 1$	1
	$\mathcal{T}_{17}$:	$f_{17}(x,y) = (x^2+1)y^2 + (x^2+3x+3)y + x^2 + 4$	4
	$\mathcal{T}_{18}$:	$f_{18}(x,y) = (x^2+1)y^2 + (2x^2+2x+4)y + 3x^2 + 3$	4
[5]	$\mathcal{T}_{19}$:	$f_{19}(x,y) = y^2 + x^2y + 3x^2 + 3$	4
	$\mathcal{T}_{20}$:	$f_{20}(x,y) = y^2 + 2xy + 4x^2 + 1$	1
	$\mathcal{T}_{21}$:	$f_{21}(x,y) = y^2 + 2xy + 4x^2 + 2$	1
[4]	$\mathcal{T}_{22}$:	$f_{22}(x,y) = y^2 + 4xy + x^2 + x$	2
[4]	$\mathcal{T}_{23}$:	$f_{23}(x,y) = y^2 + x^2y + 2x^2 + 2x$	4
	$\mathcal{T}_{24}$:	$f_{24}(x,y) = xy^2 + (4x^2+x+2)y + 2x^2 + 2x + 3$	4
	$\mathcal{T}_{25}$:	$f_{25}(x,y) = x^2y^2 + xy + 4x^2 + 1$	4
	$\mathcal{T}_{26}$:	$f_{26}(x,y) = x^2y^2 + 2xy + 2x^2 + 4$	4
[4]	$\mathcal{T}_{27}$:	$f_{27}(x,y) = y^2 + (x^2+1)y + x^2 + 4x + 4$	4

Hier sind die Türme $\mathcal{T}_1$, $\mathcal{T}_4$ und $\mathcal{T}_6$ Repräsentanten von $\mathcal{M}$, $\mathcal{N}$ and $\mathcal{L}$ in [10]. Alle Türme außer unter Umständen $\mathcal{T}_i$, $i = 8, 16, 12, 14, 15, 20, 21, 22$ sind optimal.

Jeder der oben angegebenen Türme ist ein Ober-Turm von einem der Türme $\mathcal{T}_i$, $i = 2, 6, 22, 27, 19$. Genauer gilt:
-$\mathcal{T}_2 \prec \mathcal{T}_i$ für $i = 7, 12, 14, 15$ und $\mathcal{T}_7 \prec \mathcal{T}_i$ für $i = 3, 13$
-$\mathcal{T}_6 \prec \mathcal{T}_i$ für $i = 8, 16$
-$\mathcal{T}_{19} \prec \mathcal{T}_i$ für $i = 5, 10, 11, 18$ und $\mathcal{T}_{10} \prec \mathcal{T}_i$ für $i = 9, 17$
-$\mathcal{T}_{27} \prec \mathcal{T}_i$ für $i = 23, 24, 25, 26$
-$\mathcal{T}_{22} \prec \mathcal{T}_i$ für $i = 20, 21$
Wiederum nach Beispiel 1.2.7 gilt $\mathcal{T}_6 \prec \mathcal{T}_4 \prec \mathcal{T}_1$.

Die Türme $\mathcal{T}_i$, $i = 2, 19, 27$, sind optimal, da sie Teiltürme optimaler Türme sind. Die Einbettungen $\mathcal{T}_{19} \prec \mathcal{T}_{10} \prec \mathcal{T}_9$ wurden von Elkies in [13] gezeigt. Nun folgt, daß $\mathcal{T}_2$ und $\mathcal{T}_{19}$ optimal sind, da sie Teiltürme optimaler Türme sind.

Wir können nun leicht das F_0-Geschlecht $\gamma_{F_0}(\mathcal{T}_i)$ in jedem der optimalen Türme $\mathcal{T}_i$ für $i = 1, 3, 4, 5, 6, 7, 9, 10, 11, 13, 17, 18, 23, 24, 25, 26$ als eine ganze Potenz von 2 ausrechnen.

Satz 2.2.4 *Die Türme $\mathcal{T}_2$, $\mathcal{T}_{19}$ und $\mathcal{T}_{27}$ sind nicht isomorph zu einem der optimalen Türme $\mathcal{T}_i$ für $i = 1, 3, 4, 5, 6, 7, 9, 10, 11, 13, 17, 18, 23, 24, 25, 26$.*

Beweis: Wir zeigen, daß $\mathcal{T}_2$ nicht isomorph zu einem der Türme $\mathcal{T}_i$ für $i = 1, 3, 4, 5, 6, 7, 9, 10, 11, 13, 17, 18, 23, 24, 25, 26$ ist am Beispiel von $i = 1$ (der Beweis ist analog in den anderen Fällen).

Es seien $(F_i)_{i \geq 0}$ und $(E_i)_{i \geq 0}$ Darstellungen von $\mathcal{T}_2$ und $\mathcal{T}_1$. Angenommen $\iota : \mathcal{T}_1 \cong \mathcal{T}_2$ ist ein Isomorphismus. Wir bezeichnen das Bild von E_i unter ι wieder als E_i, so daß $\cup_{i=0}^{\infty} E_i = \cup_{i=0}^{\infty} F_i$. Wir wählen nun ein j, so daß F_j den Körper E_0 enthält, und ein i, so daß E_i den Körper F_j enthält. Dann teilt $[F_j : E_0]$ den Körpergrad $[E_i : E_0] = 2^i$. Nun folgt aus Lemma 2.6 in [10], daß
$$[F_j : E_0] \cdot \gamma_{E_0}(\mathcal{T}_1) = [F_j : F_0] \cdot \gamma_{F_0}(\mathcal{T}_2). \tag{2.9}$$
Es ist $\gamma_{E_0}(\mathcal{T}_1) = 2$ und $\gamma_{F_0}(\mathcal{T}_2) = 3/2$ (man beachte, daß auch $\gamma_{\mathbb{F}_{25}(x_0)}(\mathcal{T}_j) = 3/2$ für $j = 19, 27$). Aus Gleichung (2.9) folgt nun, daß $[F_j : E_0] = 3 \cdot 2^{j-2}$, ein Widerspruch. $\square$

Während es unbekannt ist, ob zwei der Türme $\mathcal{T}_2$, $\mathcal{T}_{19}$, $\mathcal{T}_{27}$ isomorph sind, kann gezeigt werden, daß keine zwei Polynome f_2, f_{19} und f_{27} unter $\sim$ zueinander konjugiert sind.

$\mathbf{q = 49}$:

Mit den Bezeichnungen wie in den vorhergehenden Fällen erhalten wir:

Ref:		$f_i(x,y)$:	$\lambda(\mathcal{T}_i) \geq$
[10]	$\mathcal{T}_1$:	$f_1(x,y) = y^2 + x^2y + 4$	6
[4]	$\mathcal{T}_2$:	$f_2(x,y) = y^2 + x^2y + 5x$	6
[5]	$\mathcal{T}_3$:	$f_3(x,y) = y^2 + x^2y + 5x^2 + 5$	4
	$\mathcal{T}_4$:	$f_4(x,y) = y^2 + x^2y + 6x^2 + 3x$	6
[10]	$\mathcal{T}_5$:	$f_5(x,y) = y^2 + (x^2+1)y + 6x^2 + 2$	6
[5]	$\mathcal{T}_6$:	$f_6(x,y) = y^2 + (x^2+4)y + x^2$	6
[10]	$\mathcal{T}_7$:	$f_7(x,y) = y^2 + (x^2+6)y + 2$	6
	$\mathcal{T}_8$:	$f_8(x,y) = y^2 + (x^2+6)y + x^2$	6
[4]	$\mathcal{T}_9$:	$f_9(x,y) = y^2 + (x^2+6)y + 4x^2 + 6x + 4$	6
	$\mathcal{T}_{10}$:	$f_{10}(x,y) = xy^2 + (6x^2+1)y + x^2 + 5x + 2$	6
	$\mathcal{T}_{11}$:	$f_{11}(x,y) = xy^2 + (6x^2+x+2)y + 4x^2 + 6x + 6$	6
	$\mathcal{T}_{12}$:	$f_{12}(x,y) = xy^2 + (6x^2+x+5)y + x^2 + 4$	6
	$\mathcal{T}_{13}$:	$f_{13}(x,y) = x^2y^2 + xy + 2x^2 + 1$	6
	$\mathcal{T}_{14}$:	$f_{14}(x,y) = x^2y^2 + xy + 3x^2 + 4$	6
	$\mathcal{T}_{15}$:	$f_{15}(x,y) = x^2y^2 + xy + 4x^2 + 4$	6
	$\mathcal{T}_{16}$:	$f_{16}(x,y) = x^2y^2 + xy + 5x^2 + 1$	6
	$\mathcal{T}_{17}$:	$f_{17}(x,y) = x^2y^2 + 3xy + 6x^2 + 2$	6
	$\mathcal{T}_{18}$:	$f_{18}(x,y) = x^2y^2 + (x^2+2)y + 4$	6
	$\mathcal{T}_{19}$:	$f_{19}(x,y) = x^2y^2 + (x^2+6)y + 1$	6
	$\mathcal{T}_{20}$:	$f_{20}(x,y) = x^2y^2 + (x^2+3x+6)y + x^2 + 2x + 1$	6
[13]	$\mathcal{T}_{21}$:	$f_{21}(x,y) = (x^2+1)y^2 + xy + 6x^2 + 4$	6
	$\mathcal{T}_{22}$:	$f_{22}(x,y) = (x^2+1)y^2 + 6xy + 6x^2 + 4$	6
	$\mathcal{T}_{23}$:	$f_{23}(x,y) = (x^2+1)y^2 + (x^2+x+6)y + 3x^2 + 6x + 5$	6
	$\mathcal{T}_{24}$:	$f_{24}(x,y) = (x^2+1)y^2 + (x^2+2x+2)y + 5x^2 + 5$	6
	$\mathcal{T}_{25}$:	$f_{25}(x,y) = (x^2+1)y^2 + (2x^2+6x+1)y + 6x^2 + 1$	6
	$\mathcal{T}_{26}$:	$f_{26}(x,y) = (x^2+1)y^2 + (3x^2+2x+6)y + 5x^2 + 5$	6
	$\mathcal{T}_{27}$:	$f_{27}(x,y) = y^2 + (x^2+4)y + 3x^2 + 4x + 5$	6
[5]	$\mathcal{T}_{28}$:	$f_{28}(x,y) = y^2 + x^2y + 5x^2 + 5$	6
[4]	$\mathcal{T}_{29}$:	$f_{29}(x,y) = y^2 + (x^2+4)y + 6x^2 + x + 1$	6
	$\mathcal{T}_{30}$:	$f_{30}(x,y) = xy^2 + (6x^2+x+4)y + 2x^2 + 4x + 3$	6
[4]	$\mathcal{T}_{31}$:	$f_{31}(x,y) = y^2 + x^2y + 2x$	6
[13]	$\mathcal{T}_{32}$:	$f_{32}(x,y) = y^2 + (x^2+x+6)y + 2x^2 + 5x + 6$	6
[4]	$\mathcal{T}_{33}$:	$f_{33}(x,y) = y^2 + (x^2+6)y + 4x^2 + 2x + 2$	6
	$\mathcal{T}_{34}$:	$f_{34}(x,y) = y^2 + (x^2+4)y + 3x^2 + 4x + 1$	6

Die Türme $\mathcal{T}_1$, $\mathcal{T}_5$ und $\mathcal{T}_7$ sind Repräsentanten von $\mathcal{M}$, $\mathcal{L}$ und $\mathcal{N}$ in [10].

Weiter können wir zeigen, daß jeder der oben angegebenen Türme ein Ober-Turm von $\mathcal{T}_i$, $i = 3, 5, 27, 28, 31, 33$, ist. Genauer gilt:

-$\mathcal{T}_3 \prec \mathcal{T}_{18}$

-$\mathcal{T}_5 \prec \mathcal{T}_7 \prec \mathcal{T}_i$ für $i = 1, 4, 10, 14, 15$ und $\mathcal{T}_1 \prec \mathcal{T}_j$ für $j = 8, 11, 19, 26$

-$\mathcal{T}_{27} \prec \mathcal{T}_2$

-$\mathcal{T}_{28} \prec \mathcal{T}_i$ für $i = 6, 23, 24$

-$\mathcal{T}_{29} \prec \mathcal{T}_i$ für $i = 9, 13, 16, 17$
-$\mathcal{T}_{31} \prec \mathcal{T}_{30}, \mathcal{T}_{37}$, und $\mathcal{T}_{30} \prec \mathcal{T}_{20}, \mathcal{T}_{12}$, und $\mathcal{T}_{37} \prec \mathcal{T}_{25}$
-$\mathcal{T}_{33} \prec \mathcal{T}_{32} \prec \mathcal{T}_i$ für $i = 21, 22$
$\underline{\mathbf{q = 7^4}:}$

Indem wir den Konstantenkörper vergrößern, erhalten wir die folgenden weiteren Türme. Interessanterweise erhalten wir auch hier 6 als Abschätzung für den Grenzwert.

	$f_i(x,y)$:	$\lambda(\mathcal{F}_i) \geq$
$\mathcal{F}_1$:	$f_1(x,y) = y^2 + (x^2+3)y + 5x + 4$	6
$\mathcal{F}_2$:	$f_2(x,y) = y^2 + (x^2+5)y + 5x + 2$	6
$\mathcal{F}_3$:	$f_3(x,y) = x^2y^2 + (x^2+4x+5)y + 5x^2 + x + 6$	6
$\mathcal{F}_4$:	$f_4(x,y) = y^2 + (x^2+4)y + 6x^2 + 3x + 6$	6

Es gilt:
-$\mathcal{T}_{33} \prec \mathcal{F}_4 \prec \mathcal{F}_1$
-$\mathcal{T}_8 \prec \mathcal{F}_2$
-$\mathcal{T}_{18} \prec \mathcal{F}_3$,
wobei sich der jeweils linke Turm auf den Fall $q = 49$ bezieht.

2.3 Relativ unverzweigte Türme

Alle bisherigen Resultate für die Konstruktion von rekursiv definierten Türmen hängen wesentlich von der Existenz einer total verzweigten Stelle in jedem Schritt ab. Offensichtlich sind sie daher für relativ unverzweigte Türme nicht anwendbar. Als nächstes wollen wir ein Kriterium für die Konstruktion von unendlich erzeugten Körpern diskutieren, das nicht auf der Existenz total verzweigter Stellen in jedem Schritt beruht - und daher Anwendung für relativ unverzweigte Türme findet.

Satz 2.3.1 *Es sei $F = \mathbb{F}_q(x_0, x_1)/\mathbb{F}_q$ mit definierender Gleichung*

$$f(x_0, x_1) = 0 \text{ und } \deg_{x_1} f = m. \tag{2.10}$$

Es existiere eine $\mathbb{F}_q$-rationale Stelle $P \in \mathbb{P}_{\mathbb{F}_q(x_0)}$ mit den folgenden Eigenschaften:

(∗) *P zerfalle komplett in F, und es gebe eine Erweiterung $P'|P$ mit $x_1(P') = x_0(P)$.*

(∗∗) *Für ein $n \geq 1$ existiere eine endliche Folge $(\mu_i)_{0 \leq i \leq n}$ mit $\mu_n = x_0(P)$, so daß $\mu_{i+1} \leftarrow \mu_i$, die Stelle $P_{\mu_0} := Q$ nur eine total träge Erweiterung in F besitzt und die Stellen P_{μ_i} in F komplett zerfallen für $0 < i \leq n$.*

Dann definiert die Gleichung (2.10) rekursiv Körpererweiterungen $F_{k+1} = F_k(x_{k+1})$ mit:

1. $[F_{k+1} : F_k] = m$.

2. $\mathbb{F}_q$ *ist der exakte Konstantenkörper von* F_{k+1}.

3. F_{k+1} *enthält eine* $\mathbb{F}_q$*-rationale Stelle* Q_{k+1} *mit* $x_{k+1}(Q_{k+1}) = x_0(Q)$.

Insbesondere ist der Körper $\mathcal{F} = \cup_{k\geq 0} F_k$ *nicht endlich erzeugt.*

Beweis: Wir beweisen den Satz durch Induktion über k.

Für $k = 0$ folgen alle Behauptungen aus den Voraussetzungen.

Sei nun die Behauptung richtig für $k-1$. Nach Induktionsvoraussetzung existiert eine $\mathbb{F}_q$-rationale Stelle $Q_k \in \mathbb{P}_{F_k}$ mit $x_k(Q_k) = x_0(Q)$. Wir setzen $R := Q_k \cap \mathbb{F}_q(x_k)$. Dann folgt aus den Voraussetzungen, daß R nur eine Erweiterung R' in $\mathbb{F}_q(x_k, x_{k+1})$ besitzt, die total träge ist. Wir wählen eine Stelle $\tilde{Q}$ über Q_k in F_{k+1}. Diese Stelle liegt dann notwendig über R', da R' die einzige Erweiterung von R in $\mathbb{F}_q(x_k, x_{k+1})$ ist. Also ist $\deg \tilde{Q} \geq m$. Da Q_k $\mathbb{F}_q$-rational ist, folgt aus der Grad-Formel, daß $\deg \tilde{Q} = m$ und $[F_{k+1} : F_k] = m$ ist.

Da $\mu_n = x_0(P)$ und $x_0(P) \leftarrow x_0(P)$ kann die Folge $(\mu_i)_{0\leq i\leq n}$ in $\mathbb{F}_q$ stets um weitere Elemente $\mu_{n+1} = x_0(P), \mu_{n+2} = x_0(P), \ldots$ verlängert werden, und es gilt weiterhin $\mu_{i+1} \leftarrow \mu_i$. Wir wählen nun die ersten $k+2$ Elemente der eventuell verlängerten Folge. Da $[F_{j+1} : F_j] = m$ für alle $0 \leq j \leq k$, erhalten wir durch wiederholte Anwendung von Korollar 2.1.4 eine $\mathbb{F}_q$-rationale Stelle Q_{k+1} mit $x_i(Q_{k+1}) = \mu_{k+1-i}$ für $i = 0, \ldots, k+1$. Insbesondere ist $x_{k+1}(Q_{k+1}) = x_0(Q)$.

Die zweite Behauptung folgt aus der Tatsache, daß die $\mathbb{F}_q$-rationale Stelle P_k komplett zerfällt und $[F_{k+1} : F_k] = m$ gilt. □

Bemerkung 2.3.2 1. *Die Voraussetzungen von Satz 2.3.1 hängen wesentlich von der konkreten Arithmetik im Konstantenkörper ab, über dem der Körper F definiert ist. Es scheint daher schwer zu beweisen, daß die Reduktionen einer Gleichung in $\mathbb{Z}[X, Y]$ in jeder Charakteristik rekursiv einen nicht endlich erzeugten Körper definieren.*

2. *Ob eine Gleichung rekursiv einen nicht endlich erzeugten Körper $\mathcal{F}$ definiert, hängt nur von der Charakteristik des Konstantenkörpers ab. Um die Voraussetzungen von Satz 2.3.1 zu überprüfen, kann man stets über dem kleinsten Körper in der jeweiligen Charakteristik rechnen, über dem die rekursive Gleichung definiert ist. Anstelle der komplett zerfallenden Stellen P bzw. $P_{\mu_i}, 0 < i \leq n$, verlangt man die Existenz von Stellen P bzw. $P_{\mu_i}, 0 < i \leq n$, die keine verzweigten oder trägen Erweiterungen haben. Alle anderen Voraussetzungen übertragen sich von Satz 2.3.1.*

Beispiel 2.3.3 *Die Gleichung*

$$y^3 = 1 + \frac{x^3}{(x+1)^3} \tag{2.11}$$

definiert rekursiv einen nicht endlich erzeugten Körper $\mathcal{F}$ *über* $\mathbb{F}_4$.

Beweis:. Wir betrachten den durch Gleichung 2.11 definierten Körper F. Es sei α ein primitives Element von $\mathbb{F}_4$. Die Nullstelle P von $x^3 + x + 1$ in F_0 zerfällt komplett in der Erweiterung F_1/F_0. Eine der Erweiterungen $P_1|P$ ist Nullstelle von $y^3 + y + 1$, und eine Erweiterung $Q_1|P$ ist Nullstelle von $y^3 + \alpha y + 1$. Die Nullstelle von $x^3 + \alpha x + 1$ hat nur eine total träge Erweiterung in F_1. Damit können wir Satz 2.3.1 anwenden (alle diskutierten Stellen sind rational über dem Konstantenkörper $\mathbb{F}_{2^6}$). $\square$

Eine ausführlichere Diskussion der Konstruktion relativ unverzweigter Türme folgt in Kapitel 5.

Kapitel 3

Über das F-Geschlecht und die F-Zerfällungsrate

In Theorem 1.1.12 haben wir festgehalten, daß ein endlicher Verzweigungsort sowie die Existenz komplett zerfallender Stellen eine hinreichende Bedingung geben, damit ein zahmer Turm $\mathcal{T}$ asymptotisch gut ist. Weiter haben wir in Theorem 1.1.13 referiert, daß diese Bedingung im Fall galoisscher Türme auch notwendig ist.

Für rekursiv definierte zahme Türme wollen wir in diesem Kapitel die oben benannte Bedingung genauer untersuchen.

3.1 Die F-Zerfällungsrate rekursiv definierter zahmer Türme

Es sei $\mathcal{T}$ ein rekursiv definierter zahmer Turm über $\mathbb{F}_q$ mit Darstellung $(F_k)_{k\geq 0}$. Falls eine $\mathbb{F}_q$-rationale Stelle $Q \in \mathbb{P}_{F_k}, k \geq 0$, in $\mathcal{T}/F_k$ komplett zerfällt, so ist die Zerfällungsrate $\nu_{F_0}(\mathcal{T})$ echt größer als Null. Zerfällt keine $\mathbb{F}_q$-rationale Stelle in $\mathcal{T}$ komplett, so hat jede $\mathbb{F}_q$-rationale Stelle entweder eine träge Erweiterung oder eine verzweigte Erweiterung in $\mathcal{T}$.

Wir untersuchen zunächst $\mathbb{F}_q$-rationale Stellen mit trägen Erweiterungen. Für $\alpha \in \mathbb{P}^1 := \bar{\mathbb{F}}_q \cup \{\infty\}$ bezeichne für das ganze Kapitel 3 wieder P_α die Nullstelle von $x_0 - \alpha$ bzw. den Pol von x_0.

Lemma 3.1.1 *Es sei $\mathcal{T} := \cup_{k\geq 0} F_k$ ein rekursiv definierter zahmer Turm über $\mathbb{F}_q$. Weiter sei $P \in \mathbb{P}_{F_0}$ eine $\mathbb{F}_q$-rationale Stelle. Wir definieren*

$$\begin{aligned} M \quad := \quad & \{\alpha \in \mathbb{P}^1 | \textit{Für ein } k \geq 0 \textit{ existiert eine } \mathbb{F}_q\textit{-rationale} \\ & \textit{Stelle } Q \in \mathbb{P}_{F_k} \textit{ über } P \textit{ mit } x_k(Q) = \alpha\}. \end{aligned}$$

Falls für alle $\alpha \in M$ die ($\mathbb{F}_q$-rationalen) Stellen P_α eine träge Erweiterung *in $\mathcal{T}$ haben, so ist*

$$\mu(P) := \lim_{k\to\infty} \frac{|\{Q \in \mathbb{P}_{F_k} | Q|P \text{ und } Q \text{ ist } \mathbb{F}_q\text{-rational}\}|}{[F_k : F_0]} = 0.$$

Beweis: Es sei $\alpha \in M$. Da die Stelle P_α nach Voraussetzung eine träge Erweiterung besitzt, existiert eine kleinste Zahl k_α, so daß $f(Q|P_\alpha) > 1$ für eine Stelle $Q \in \mathbb{P}_{F_{k_\alpha}}$. Wir setzen

$$k := \max\{k_\alpha | \alpha \in M\}.$$

Über einer Stelle $P_\alpha, \alpha \in M$, sind dann höchstens $([F_k : F_0] - 1)$ $\mathbb{F}_q$-rationale Stellen in F_k.

Es sei nun $R|P$ eine $\mathbb{F}_q$-rationale Stelle in F_{rk} für ein $r \geq 1$. Wenn wir zeigen, daß R eine träge Erweiterung in $F_{(r+1)k}$ besitzt, folgt das Lemma induktiv:

$$\mu(P) \leq \lim_{r\to\infty} \frac{([F_k : F_0] - 1)^r}{[F_k : F_0]^r} = 0.$$

Wir setzen $Q := R \cap \mathbb{F}_q(x_{rk})$. Da die Stelle R über P liegt und der Turm $\mathcal{T}$ rekursiv definiert ist, hat Q eine träge Erweiterung, etwa Q', in $\mathbb{F}_q(x_{rk}, x_{rk+1}, \ldots, x_{(r+1)k})$ nach Definition von k. Gemäß Korollar 2.1.4 existiert eine Stelle $R' \in \mathbb{P}_{F_{(r+1)k}}$, die über Q' und R liegt. Da $\deg R' \geq \deg Q' > 1$, ist die Stelle R' träge über R. □

Korollar 3.1.2 *Es sei $\mathcal{T} := \cup_{k\geq 0} F_k$ ein rekursiv definierter zahmer Turm über $\mathbb{F}_q$. Haben alle $\mathbb{F}_q$-rationalen Stellen in $\mathcal{T}$ eine träge Erweiterung, so ist die F_0-Zerfällungsrate $\nu_{F_0}(\mathcal{T})$ gleich Null.*

Beweis: Die Behauptung folgt direkt aus Lemma 3.1.1, da

$$\nu_{F_0}(\mathcal{T}) = \sum_{\alpha\in\mathbb{P}^1} \mu(P_\alpha).$$

□

Wir diskutieren nun $\mathbb{F}_q$-rationale Stellen mit verzweigten oder trägen Erweiterungen in einer Klasse rekursiv definierter Türme.

Definition 3.1.3 *Es sei $\mathcal{T} := \cup_{k\geq 0} F_k$ ein Turm über $\mathbb{F}_q$. $\mathcal{T}$ heißt total verzweigt über F_0, falls für jede in F_1/F_0 verzweigende Stelle $P \in \mathbb{P}_{F_0}$ die Stelle P total verzweigt in F_k für alle $k \geq 1$. Wir sagen auch, P ist total verzweigt in $\mathcal{T}/F_0$.*

Bemerkung 3.1.4 *Man beachte, daß diese Definition von total verzweigten Türmen nicht mit der in [10] übereinstimmt.*

Beispiel 3.1.5 *Es sei $\mathcal{T}/\mathbb{F}_q$ rekursiv definiert durch*

$$y^m = g(x) \tag{3.1}$$

für ein Polynom $g(x)$ vom Grad $m, \gcd(m,q) = 1$, mit $g(0) = 0$ und mit nur einfachen Nullstellen. Dann sieht man leicht, daß $\mathcal{T}/F_0$ ein total verzweigter Turm ist; denn zunächst definiert die Gleichung 3.1 nach Lemma 2.2.1 einen nicht endlich erzeugten Körper $\mathcal{T}$ über dem Konstantenkörper $\mathbb{F}_q$. Es bezeichne $P_\alpha, \alpha \in \{0, \infty\}$, die Null- bzw. Polstelle von x_0 in $F_0 = \mathbb{F}_q(x_0)$. Nach einer geeigneten Konstantenkörpererweiterung zerfällt die Stelle $P_\infty \in \mathbb{P}_{F_0}$ komplett in $\mathcal{T}/F_0$. Aus der Hasse-Weil-Schranke folgt nun, daß ein $F < \mathcal{T}$ existiert mit $g(F) > 1$. Somit ist $\mathcal{T}$ ein Turm. Nach der Theorie der Kummererweiterungen sind alle in F_1/F_0 verzweigten Stellen total verzweigt. Da die Stelle P_0 total verzweigt ist in $\mathcal{T}/F_0$, ist $\mathcal{T}/F_0$ total verzweigt.

Es sei $\mathcal{T} = \cup_{k \geq 0} F_k$ ein rekursiv definierter über F_0 total verzweigter zahmer Turm über $\mathbb{F}_q$. Falls $Q \in \mathbb{P}_{F_k}$ eine in F_{k+1} verzweigende Stelle ist, so verzweigt nach Abhyankars Lemma auch die Stelle $P := \mathbb{F}_q(x_k) \cap Q$ in $\mathbb{F}_q(x_k, x_{k+1})$.

Es bezeichne

$$Z := \{\alpha \in \mathbb{F}_q \cup \{\infty\} | P_\alpha \in \mathbb{P}_{F_0} \text{ verzweigt total in } \mathcal{T}/F_0\}.$$

Lemma 3.1.6 *Es sei $\mathcal{T} := \cup_{k \geq 0} F_k$ ein rekursiv definierter über F_0 zahmer und total verzweigter Turm über $\mathbb{F}_q$. Für alle $k \geq 0$ gilt:*

$$\lim_{i \to \infty} \sum_{\substack{P \in \mathbb{P}_{F_k} \\ x_k(P) \in Z}} \sum_{\substack{Q \in \mathbb{P}_{F_i} \\ Q|P}} \frac{\deg Q}{[F_i : F_0]} = 0.$$

Beweis: Wir setzen $[F_1 : F_0] = m$. Sei $k \geq 0$ und $P \in \mathbb{P}_{F_k}$ mit $x_k(P) = \alpha \in Z$. Da die Stelle $P_\alpha \in \mathbb{P}_{F_0}$ in $\mathcal{T}/F_0$ total verzweigt, gilt für alle $Q \in \mathbb{P}_{F_j}, j \geq k$, mit $Q|P$, daß $x_j(Q) \in Z$. Wir schreiben $e(P|P \cap \mathbb{F}_q(x_k)) = e' \cdot e''$ mit e' maximal, so daß $\gcd(e', m) = 1$. Nun können wir ein $s \in \mathbb{Z}$ wählen, so daß $e''|m^s$. Es sei $Q \in \mathbb{P}_{F_{k+s}}$ eine Stelle über P. Wir setzen $e_1 := e(Q|Q \cap \mathbb{F}_q(x_k, x_{k+1}, \ldots, x_{k+s}))$ und $e_2 = e(Q \cap \mathbb{F}_q(x_k, x_{k+1}, \ldots, x_{k+s})|Q \cap \mathbb{F}_q(x_{k+s}))$. Nach Abhyankars Lemma ist nun $gcd(e_1, m) = 1$, da $e''|m^s$. Weiter ist $\gcd(e_2, m) = 1$, da $x_j(Q) \in Z$ für $j \geq k$. Damit ist $gcd(e(Q|Q \cap \mathbb{F}_q(x_{k+s})), m) = 1$, und die Stelle Q ist total verzweigt in $\mathcal{T}/F_{k+s}$, da $x_{k+s}(Q) \in Z$ gilt.

Da nur endlich viele Stellen $P \in \mathbb{P}_{F_k}$ mit $x_k(P) \in Z$ existieren, gibt es eine Zahl r, so daß für alle Stellen $P \in \mathbb{P}_{F_k}$ mit $x_k(P) \in Z$ alle Stellen $Q \in \mathbb{P}_{F_{k+r}}$ über P total verzweigen in $\mathcal{T}/F_{k+r}$. Somit erhalten wir mit $t = |\{P \in \mathbb{P}_{F_k} | x_k(P) \in Z\}|$

$$\lim_{i\to\infty} \sum_{\substack{P\in\mathbb{P}_{F_k}\\ x_k(P)\in Z}} \sum_{\substack{Q\in\mathbb{P}_{F_i}\\ Q|P}} \frac{\deg Q}{m^i} \leq \lim_{i\to\infty} \frac{tm^r}{m^i} = 0.$$

□

Wir sind nun in der Lage, das folgende allgemeine Resultat zu beweisen:

Theorem 3.1.7 *Es sei $\mathcal{T} := \cup_{k\geq 0} F_k$ ein rekursiv definierter über F_0 zahmer und total verzweigter Turm. Dann gilt*

$$\nu_{F_0}(\mathcal{T}) > 0 \Longleftrightarrow \mathcal{T} \textit{ zerfällt komplett.}$$

Beweis: Die Richtung $\Longleftarrow$ ist gerade Satz 1.1.11. Um die andere Richtung zu beweisen, nehmen wir an, daß $\mathcal{T}$ nicht komplett zerfällt. Wir setzen

$$r := \max_{P\in R(F_0)} \{i | P \text{ zerfällt in } F_{i-1} \text{ komplett}\}.$$

Zunächst zeigen wir die folgende Behauptung:

(†) Sei R eine $\mathbb{F}_q$-rationale Stelle in F_{nr} mit $n \geq 1$. Dann hat R in $F_{(n+1)r}$ eine träge Erweiterung, oder es existiert eine Stelle $R' \in \mathbb{P}_{F_{(n+1)r}}$ über R mit $x_{(n+1)r}(R') \in Z$.

Wir betrachten die $\mathbb{F}_q$-rationale Stelle $Q := R \cap \mathbb{F}_q(x_{nr})$. Da $\mathcal{T}$ rekursiv definiert ist, existiert nach Definition von r mindestens eine Stelle $Q' \in \mathbb{P}_{\mathbb{F}_q(x_{nr}, x_{nr+1}, \ldots, x_{(n+1)r})}$, die träge ist oder verzweigt ist. Nach Korollar 2.1.4 ist damit aber mindestens eine Stelle $R' \in \mathbb{P}_{F_{(n+1)r}}$ über R träge, oder es existiert ein j mit $r \leq j \leq (n+1)r$, so daß $x_j(R') \in Z$. Da jede verzweigte Stelle P_α mit $\alpha \in Z$ in $\mathcal{T}/F_0$ aber total verzweigt ist, ist dann auch $x_{(n+1)r}(R') \in Z$.

Sei nun $\varepsilon > 0$. Wir wählen ein $k \in \mathbb{N}$, so daß für ein $s \in \mathbb{N}$ gilt

$$k = rs \text{ und } \frac{(m^r - 1)^s}{m^{rs}} < \varepsilon.$$

Es sei $R(F_i)$ die Menge der $\mathbb{F}_q$-rationalen Stellen in F_i. Dann gilt

$$\nu_{F_0}(\mathcal{T}) = \lim_{i\to\infty} \frac{N(F_i)}{[F_i : F_0]}$$

$$
\begin{aligned}
&\leq \lim_{i\to\infty} \sum_{P\in R(F_k)} \sum_{\substack{Q\in\mathbb{P}_{F_i}\\ Q|P}} \frac{1}{m^i} \\
&= \lim_{i\to\infty} \sum_{\substack{P\in R(F_k)\\ x_k(P)\in Z}} \sum_{\substack{Q\in\mathbb{P}_{F_i}\\ Q|P}} \frac{1}{m^i} + \lim_{i\to\infty} \sum_{\substack{P\in R(F_k)\\ x_k(P)\notin Z}} \sum_{\substack{Q\in\mathbb{P}_{F_i}\\ Q|P}} \frac{1}{m^i}.
\end{aligned}
$$

Nach Lemma 3.1.6 ist

$$
\lim_{i\to\infty} \sum_{\substack{P\in R(F_k)\\ x_k(P)\in Z}} \sum_{\substack{Q\in\mathbb{P}_{F_i}\\ Q|P}} \frac{1}{m^i} = 0.
$$

Daher ist

$$
\begin{aligned}
\nu_{F_0}(\mathcal{T}) &\leq \lim_{i\to\infty} \sum_{\substack{P\in R(F_k)\\ x_k(P)\notin Z}} \sum_{\substack{Q\in\mathbb{P}_{F_i}\\ Q|P}} \frac{1}{m^i} \\
&\leq \lim_{i\to\infty} \sum_{\substack{P\in R(F_k)\\ x_k(P)\notin Z}} \frac{m^{i-k}}{m^i} \\
&\overset{(\dagger)}{\leq} \lim_{i\to\infty} \frac{(m^r-1)^s m^{(i-rs)}}{m^i} \leq \frac{(m^r-1)^s}{m^{rs}} < \varepsilon.
\end{aligned}
$$

□

3.2 Das F-Geschlecht rekursiv definierter zahmer Türme

Im folgenden sei $\bar{\mathbb{F}}_q$ ein fest gewählter algebraischer Abschluß von $\mathbb{F}_q$.

Ein rekursiv definierter zahmer und gerader Turm $\mathcal{T}$ ist höchstens dann asymptotisch gut, wenn sein F-Geschlecht endlich ist. Wir zeigen nun, daß dieses nur dann der Fall sein kann, wenn der Verzweigungsort von $\mathcal{T}$ mit dem Verzweigungsort des dualen Turms (definiert über F) übereinstimmt.

Satz 3.2.1 *Sei $\mathcal{T} := \cup_{k\geq 0} F_k$ ein rekursiv definierter zahmer und gerader Turm über $\mathbb{F}_q$ und $\mathcal{S} := \cup_{k\geq 0} E_k$ der zu $\mathcal{T}$ duale Turm mit $F_0 = E_0$. Falls $\gamma_{F_0}(\mathcal{T}) < \infty$, so gilt $V_{F_0}(\mathcal{T}) = V_{E_0}(\mathcal{S})$.*

Beweis: Wir betrachten den Turm $\mathcal{T}$ über dem algebraisch abgeschlossenen Körper $\bar{\mathbb{F}}_q$. Wir zeigen zunächst $V_{F_0}(\mathcal{T}) \subseteq V_{E_0}(\mathcal{S})$. Angenommen $V_{F_0}(\mathcal{T}) \not\subseteq V_{E_0}(\mathcal{S})$, etwa $P_\alpha \in V_{F_0}(\mathcal{T}) \setminus V_{E_0}(\mathcal{S})$. Dann existiert (für ein geeignetes $k \in \mathbb{N}$) eine Stelle $Q \in \mathbb{P}_{F_k}$ über P_α, die über F_{k-1} verzweigt ist. Da nach Voraussetzung $P_\alpha \notin V_{E_0}(\mathcal{S})$, existieren dann nach Korollar 2.1.4 $m := [E_1 : E_0]$ in F_{k+1}/F_k verzweigte Stellen, an denen die Funktion x_1 den Wert α annimmt. Induktiv erhalten wir so m^s in F_{k+s} über F_{k+s-1} verzweigte Stellen von F_{k+s}, an denen die Funktion x_s den Wert α annimmt.

Somit können wir den Grad der Differente abschätzen (indem wir die Transitivität der Differente ausnutzen, vgl. [15, III.4.11]):

$$\begin{aligned}\deg Diff(F_{k+s}/F_0) &= \sum_{j=0}^{k+s-1} m^j \deg Diff(F_{k+s-j}/F_{k+s-j-1}) \\ &\geq \sum_{j=0}^{s-1} m^j \deg Diff(F_{k+s-j}/F_{k+s-j-1}) \\ &\geq sm^{s-1}.\end{aligned}$$

Also ist

$$\lim_{s\to\infty} \frac{\deg Diff(F_{k+s}/F_0)}{[F_{k+s} : F_0]} = \lim_{s\to\infty} \frac{\deg Diff(F_{k+s}/F_0)}{[E_{k+s} : E_0]} = \infty.$$

Der Widerspruch folgt nun aus der Hurwitzschen Geschlechtsformel. Damit ist $V_{F_0}(\mathcal{T}) \subseteq V_{E_0}(\mathcal{S})$.

Da der Turm $\mathcal{T}$ nach Voraussetzung gerade ist, gilt

$$[F_{k+1} : F_k] = [E_{k+1} : E_k]$$

für alle $k \geq 0$. Daher ist $\gamma_{F_0}(\mathcal{T}) = \gamma_{E_0}(\mathcal{S})$. Nun folgt die Behauptung aus $V_{F_0}(\mathcal{T}) \subseteq V_{E_0}(\mathcal{S})$ angewandt auf den dualen Turm $\mathcal{S}$. $\square$

Alle bekannten asymptotisch guten zahmen Türme haben einen endlichen Verzweigungsort $V_F(\mathcal{T})$. Daher scheint es sinnvoll, Türme mit endlichem Verzweigungsort zu konstruieren, um neue Kandidaten für asymptotisch gute Türme zu erhalten. Spezieller gilt nach [8] für zahme Türme, die durch eine Kummer-Gleichung definiert sind:

Theorem 3.2.2 *Sei $m > 1$ eine ganze Zahl mit $q \equiv 1 \pmod m$, und sei $S_0 \subseteq \bar{\mathbb{F}}_q$ eine endliche Teilmenge von $\bar{\mathbb{F}}_q$ mit $0 \in S_0$. Weiter sei $f(t) \in \mathbb{F}_q[t]$ ein Polynom, dessen Leitkoeffizient eine m-te Potenz in $\mathbb{F}_q$ ist und das den folgenden Bedingungen genügt:*

1. *$f(t) = t^d f_1(t)$ mit $f_1(t) \in \mathbb{F}_q[t], f_1(0) \neq 0$ und $\gcd(d, m) = 1$.*

2. *$\deg f(t) = m$.*

3. *Für jedes $\alpha \in S_0$ gehören alle Wurzeln der Gleichung $f(t) = \alpha^m$ zu S_0.*

Dann definiert die Gleichung

$$y^m = f(x)$$

rekursiv einen asymptotisch guten Turm.

H.W. Lenstra hat gezeigt, daß das obige Theorem nicht verwendet werden kann, um asymptotisch gute Türme über Primkörpern $\mathbb{F}_p$ zu konstruieren (vgl. [12]). Der Beweis von Lenstra beruht ganz wesentlich auf einer Schlüsselidentität.

Eine ganz ähnliche Identität erweist sich auch in einem anderen Zusammenhang als hilfreich, nämlich wenn man den exakten Verzweigungsort für durch eine Kummer-Gleichung rekursiv definierte Türme berechnet.

Lemma 3.2.3 *Sei $\mathcal{T}$ ein rekursiv definierter Turm über $\bar{\mathbb{F}}_q$ mit definierender Gleichung*

$$y^m = g(x) \in \mathbb{F}_q[x] \ \textit{mit} \ \deg g(x) = m \ \textit{und} \ \gcd(m,q) = 1.$$

Weiter sei $g(x) = x^d g_1(x)$ mit $g_1(0) \neq 0$ und $\gcd(d,m) = 1$. Der Turm $\mathcal{T}$ habe einen endlichen Verzweigungsort $V_{F_0}(\mathcal{T})$. Wir setzen $T := \{\alpha^m | P_\alpha \in V_{F_0}(\mathcal{T})\}$ und $t := |T|$.
Dann ist

$$mx^{m-1} \prod_{\alpha \in T} (g(x) - \alpha) = a^{t-1} g'(x) \prod_{\alpha \in T} (x^m - \alpha), \tag{3.2}$$

wobei a den Leitkoeffizienten von $g(x)$ bezeichnet und $g'(x)$ die formale Ableitung von $g(x)$ ist.

Beweis: Wir zeigen zunächst, daß $V_{F_0}(\mathcal{T}) = \cup_{k \geq 0} V_k$, wobei $V_0 := \{P_0\}$ und $V_{k+1} := \{P_\alpha \in \mathbb{P}_{\bar{\mathbb{F}}_q(x_0)} |$Es existiert ein $P_\beta \in V_k$ mit $f(\alpha) = \beta^m\}$. Offensichtlich ist $V_{F_0}(\mathcal{T}) \subseteq \cup_{k \geq 0} V_k$. Um die andere Inklusion zu zeigen, zeigen wir induktiv $\cup_{k \leq n} V_k \subseteq V_{F_0}(\mathcal{T})$. Die Behauptung gilt für $n = 0$, da $\gcd(d,m) = 1$. Sei nun die Behauptung richtig für n. Wir müssen zeigen, daß $V_{n+1} \subseteq V_{F_0}(\mathcal{T})$. Sei also $P_\alpha \in V_{n+1}$. Dann existiert ein $\beta \in \bar{\mathbb{F}}_q$, so daß $\beta^m = f(\alpha)$ und $P_\beta \in V_n$. Nach Induktionsvoraussetzung existiert für ein $k \in \mathbb{N}$ eine Stelle $Q \in \mathbb{P}_{F_k}$ mit $e(Q|P_\beta) > 1$. Da $\mathcal{T}$ rekursiv definiert ist, existiert eine Stelle $\tilde{Q} \in \mathbb{P}_{\bar{\mathbb{F}}_q(x_1,x_2,\ldots,x_{k+1})}$ über der Nullstelle $\tilde{P}$ von $x_1 - \beta$ in $\bar{\mathbb{F}}_q(x_1)$ mit $e(\tilde{Q}|\tilde{P}) > 1$. Es sei R eine Stelle über P_α und $\tilde{P}$ in F_1. Da $\gcd(d,m) = 1$ gilt, ist für alle $s > k$ die Stelle $\tilde{Q}$ total verzweigt über $\bar{\mathbb{F}}_q(x_1,x_2,\ldots,x_{k+1})$ in der Erweiterung $\bar{\mathbb{F}}_q(x_1,x_2,\ldots,x_s)$. Insbesondere gibt es ein $s \in \mathbb{N}$, so daß für die Stelle $\tilde{Q}_s | \tilde{Q}$ in $\mathbb{F}_q(x_1,x_2,\ldots,x_s)$ gilt, daß $e(\tilde{Q}_s|\tilde{P}) \nmid e(R|\tilde{P})$. Nach Korollar 2.1.4 existiert nun eine Stelle $S \in \mathbb{P}_{F_s}$ mit $S|R$ und $S|\tilde{Q}_s$. Nach Abhyankars Lemma ist $e(S|R) > 1$. Damit ist aber auch $e(S|P_\beta) > 1$.

Als nächstes zeigen wir, daß die linke Seite der Gleichung 3.2 die rechte Seite teilt. Es sei $\beta \in \bar{\mathbb{F}}_q$ eine Nullstelle der linken Seite. Ist $\beta = 0$, so ist β eine mindestens m-fache Nullstelle der rechten Seite, da $P_0 \in V_{F_0}(\mathcal{T})$. Ist $\beta \neq 0$, so existiert ein $P_\gamma \in V_{F_0}(\mathcal{T})$ mit $\gamma^m = g(\beta)$. Folglich ist $P_\beta \in V_{F_0}(\mathcal{T})$ gemäß dem ersten Teil des Beweises, und β ist Nullstelle der rechten Seite. Die Vielfachheit von β in $g(x) - \alpha$ ist höchstens um eins größer als die Vielfachheit von β in $g'(x)$.

Vergleich der Grade und der Leitkoeffizienten in 3.2 liefert nun die Behauptung. □

Bemerkung 3.2.4 *Aus dem ersten Teil des Beweises von Lemma 3.2.3 folgt insbesondere, daß (unter den Voraussetzungen von 3.2.3) für jedes* $0 \neq \alpha \in T$ *m paarweise verschiedene Stellen* $P_{\alpha_1}, P_{\alpha_2}, \ldots, P_{\alpha_m}$ *im Verzweigungsort* $V_{F_0}(\mathcal{T})$ *liegen, die Nullstellen von* $x_0 - \alpha_i$ *sind für Elemente* α_i *mit* $\alpha_i^m = \alpha$*.*

Wir werden das obige Lemma in Kapitel 4 verschiedentlich verwenden.

In rekursiv definierten über F zahmen und total verzweigten Türmen mit endlichem Verzweigungsort ist es möglich, das exakte F-Geschlecht und die exakte F-Zerfällungsrate zu berechnen, falls man den Verzweigungsort und die Anzahl komplett zerfallender Stellen kennt.

Für den Rest von Kapitel 3 sei $\mathcal{T} := \cup_{k \geq 0} F_k$ ein rekursiv definierter über F_0 zahmer und total verzweigter Turm mit endlichem Verzweigungsort. Weiter definieren wir

$$V_{F_0}(F_k) := \{P \in \mathbb{P}_{F_0} | P \text{ verzweigt in } F_k/F_0\}.$$

In über F_0 zahmen Türmen können wir den Grad der Differente von F_k/F_0 wie folgt berechnen:

$$\begin{aligned}
\deg Diff(F_k/F_0) &= \sum_{P \in V_{F_0}(F_k)} \sum_{Q|P} d(Q|P) \deg Q \\
&= \sum_{P \in V_{F_0}(F_k)} \sum_{Q|P} (e(Q|P) - 1) \deg Q \\
&= \sum_{P \in V_{F_0}(F_k)} (\sum_{Q|P} e(Q|P) f(Q|P)) \deg P - \sum_{P \in V_{F_0}(F_k)} \sum_{Q|P} \deg Q \\
&= \sum_{P \in V_{F_0}(F_k)} [F_k : F_0] \deg P - \sum_{P \in V_{F_0}(F_k)} \sum_{Q|P} \deg Q,
\end{aligned}$$

wobei sich die Summen über alle Stellen $Q \in \mathbb{P}_{F_k}$ mit $Q|P$ erstrecken.

Sei

$$a_k := \sum_{P \in V_{F_0}(F_k)} \sum_{Q|P} \deg Q \tag{3.3}$$

der "Korrekturterm" aus der obigen Differenz (die zweite Summe erstreckt sich dabei wieder über alle $Q \in \mathbb{P}_{F_k}$).

Lemma 3.2.5 *Es sei $\mathcal{F} := \cup_{k\geq 0} F_k$ ein rekursiv definierter über F_0 zahmer und total verzweigter Turm mit endlichem Verzweigungsort. Dann ist*

$$\lim_{k\to\infty} \frac{a_k}{[F_k : F_0]} = 0.$$

Beweis: Da der Verzweigungsort endlich ist, können wir nach geeigneter Konstantenkörpererweiterung davon ausgehen, daß nur Stellen vom Grad eins im Verzweigungsort liegen. Nun folgt die Behauptung direkt aus Lemma 3.1.6. □

Mit $P_\alpha, \alpha \in \bar{\mathbb{F}}_q \cup \{\infty\}$, bezeichnen wir weiterhin die Nullstelle von $x_0 - \alpha$ bzw. den Pol von x_0 in F_0.

Beispiel 3.2.6 *Wir betrachten den Turm $\mathcal{T}_2$ aus der in Kapitel 2.2 für den Fall $q = 9$ angegebenen Tabelle. Es sei w ein primitives Element von $\mathbb{F}_9$, das der Gleichung $w^2 + 2w + 2 = 0$ genügt. Die Differente von F_1/F_0 ist durch*

$$Diff(F_1/F_0) = P_{w^2} + P_{w^6}$$

gegeben (dabei bezeichnet P_α die Nullstelle von $x_0 - \alpha$). Da $\deg_x f_2 = \deg_y f_2 = 2$ und $w^2 \leftarrow w^2$ und $w^6 \leftarrow w^6$, ist $\mathcal{T}_2$ total verzweigt über F_0. Der Verzweigungsort von $\mathcal{T}_2/F_0$ ist gleich $V_{F_0}(\mathcal{T}_2) = \{P_0, P_1, P_2, P_{w^2}, P_{w^6}\}$. Nun erhalten wir für das F_0-Geschlecht (nach der Hurwitzschen Geschlechtsformel und Lemma 3.2.5)

$$\gamma_{F_0}(\mathcal{T}_2) = \lim_{i\to\infty} \frac{-2\cdot 2^i + \sum_{P\in V_{F_0}(\mathcal{T}_2)} 2^i - a_i + 2}{2\cdot 2^i} = \frac{5-2}{2} = \frac{3}{2}.$$

Die Stellen P_{w^j} für $j = 1, 3, 5, 7$ sind träge in F_1, und die Stelle P_∞ zerfällt komplett in $\mathcal{T}_2$. Also erhalten wir für die F_0-Zerfällungsrate (nach Lemma 3.2.5 und Lemma 3.1.1)

$$\nu_{F_0}(\mathcal{T}_2) = \lim_{i\to\infty} \frac{2^i + a_i}{2^i} = 1,$$

und somit ist die in der Tabelle angegebene Abschätzung scharf:

$$\lambda(\mathcal{T}_2) = \frac{2}{3}.$$

Ähnlich können wir zeigen, daß auch die Abschätzungen für die Türme $\mathcal{T}_3$ und $\mathcal{T}_6$ aus derselben Tabelle scharf sind.

Kapitel 4

Fermat Türme

In diesem Kapitel diskutieren wir zahme Türme, die durch eine Gleichung vom Typ

$$y^m = a(x+b)^m + c \text{ mit } a, b, c \in \mathbb{F}_q^* \text{ und } gcd(m, q) = 1 \tag{4.1}$$

rekursiv definiert sind. Diese Gleichungen sind von Interesse, da sie bekanntermaßen eine Reihe asymptotisch guter Türme definieren.

4.1 Konstruktion von Fermat Türmen

Es sei im folgenden stets $\bar{\mathbb{F}}_q$ ein fest gewählter algebraischer Abschluß von $\mathbb{F}_q$. Zunächst wollen wir sicherstellen, daß durch Gleichung 4.1 tatsächlich rekursiv Türme definiert werden. Damit können wir angeben, unter welchen Bedingungen [10, Hypothesis (A)] erfüllt ist.

Theorem 4.1.1 *Die Gleichung*

$$y^m = a(x+b)^m + c \textit{ mit } a, b, c \in \mathbb{F}_q \textit{ und } (q, m) = 1 \tag{4.2}$$

definiert genau dann rekursiv einen Turm $\mathcal{F}$, wenn $a, b, c \in \mathbb{F}_q^*$.

Beweis: Seien zunächst $a, b, c \in \mathbb{F}_q^*$. Wir setzen $g(x) = a(x+b)^m + c$. Das Polynom $\frac{1}{a}g(x) = (x+b)^m + \frac{c}{a}$ ist normiert und separabel (da $\frac{c}{a} \neq 0$). Wegen

$$(x+b)^m + \frac{c}{a} = x^m + mbx^{m-1} + \ldots \tag{4.3}$$

und $b \neq 0$ ist $g(x) \neq x^m - \alpha$ für alle $\alpha \in \bar{\mathbb{F}}_q^*$. Daher ist für kein $\alpha \in \bar{\mathbb{F}}_q^*$ die Menge der m-ten Wurzeln von α in der Menge der Nullstellen von g enthalten.

Sei $\bar{\mathbb{F}}_q(x, y)$ durch Gleichung 4.2 definiert. $\bar{\mathbb{F}}_q(x, y)/\bar{\mathbb{F}}_q(y)$ ist eine Kummererweiterung. Über $\bar{\mathbb{F}}_q(y)$ verzweigen genau die Nullstellen von $y - \alpha$ mit

$\alpha^m = c$, und zwar jeweils vom Index m. Es folgt somit aus Gleichung 4.3, daß eine Stelle P von $\bar{\mathbb{F}}_q(y)$ existiert, die in $\bar{\mathbb{F}}_q(x,y)$ total verzweigt und nicht Nullstelle von $a(y+b)^m + c$ ist.

Aus Theorem 2.2.2 folgt nun, daß $\mathcal{F}$ nicht endlich erzeugt ist und $\mathbb{F}_q$ der exakte Konstantenkörper von $\mathcal{F}$ ist.

Analog zu Beispiel 1.2.6 sehen wir, daß der Pol von x_0 in F_0 nach einer geeigneten Konstantenkörpererweiterung komplett in $\mathcal{F}$ zerfällt. Daher ist die Anzahl rationaler Stellen von F_k für wachsendes k nicht beschränkt, und nach der Hasse-Weil-Schranke ist das Geschlecht von F_k für wachsendes k nicht beschränkt. Also ist $\mathcal{F}$ ein Turm über $\mathbb{F}_q$.

Ist $a = 0$ oder $c = 0$, so ist $\mathcal{F}$ ganz offensichtlich endlich erzeugt. Der Fall $b = 0$ wurde in Beispiel 2.1.1 diskutiert. □

Das obige Theorem nehmen wir zum Anlaß für die folgende Definition:

Definition 4.1.2 *Es sei $\mathcal{F} = \cup_{k\geq 0} F_k$ rekursiv definiert über $\mathbb{F}_q$ durch die Gleichung*

$$y^m = a(x+b)^m + c \text{ mit } a,b,c \in \mathbb{F}_q^* \text{ und } (m,q) = 1.$$

Dann heißt $\mathcal{F}$ ein Fermat-Turm.

Bemerkung 4.1.3 *Der zu einem Fermat Turm $\mathcal{F}$ duale Turm $\mathcal{E}$ ist wieder ein Fermat Turm mit definierender Gleichung $y^m = a^{-1}(x-b)^m - \frac{c}{a}$.*

Die bislang bekannten asymptotisch guten Fermat Türme lassen sich in zwei Klassen unterteilen (vgl. u.a. [10]).

Theorem 4.1.4 (Norm Fermat Turm) *Es sei l eine Potenz der Charakteristik von $\mathbb{F}_q$, und sei $q = l^r$ mit $r \geq 2$. Dann definiert die Gleichung*

$$y^{(q-1)/(l-1)} = a(x+b)^{(q-1)/(l-1)} + c \text{ mit } a,c \in \mathbb{F}_l^* \text{ und } b \in \mathbb{F}_q^* \tag{4.4}$$

einen asymptotisch guten Fermat Turm $\mathcal{F}$ über $\mathbb{F}_q$. Der Grenzwert von $\mathcal{F}$ genügt der Abschätzung

$$\lambda(\mathcal{F}) \geq \frac{2}{q-2}.$$

Beweis: Der Exponent $m := (q-1)/(l-1)$ von Gleichung 4.4 definiert gerade die Normabbildung von $\mathbb{F}_q/\mathbb{F}_l$. Damit zeigt man analog zu Beispiel 1.2.6, daß $V_{F_0}(\mathcal{F}) \subseteq \{P_\alpha | \alpha \in \mathbb{F}_q\}$. Da $a \in \mathbb{F}_l$ eine m-te Wurzel in $\mathbb{F}_q$ ist, zeigt man wiederum wie in Beispiel 1.2.6, daß der Pol von x_0 in $\mathcal{F}$ komplett zerfällt. Die angegebene Abschätzung für $\lambda(\mathcal{F})$ folgt nun aus Theorem 1.1.12. □

Bemerkung 4.1.5 *Für $q = 4$ (und $l = 2$) ist der oben definierte Norm Fermat Turm optimal über $\mathbb{F}_4$.*

Theorem 4.1.6 *Es sei l eine Potenz der Charakteristik von $\mathbb{F}_q$, und sei $q = l^r$ mit $r \geq 1$ und $l > 2$. Weiter sei*

$$r \equiv 0 \pmod 2 \text{ oder } l \equiv 0 \pmod 2.$$

Dann definiert die Gleichung

$$y^{l-1} = -(x+b)^{l-1} + 1 \text{ mit } b \in \mathbb{F}_l^*$$

einen asymptotisch guten Fermat Turm $\mathcal{F}$ über $\mathbb{F}_q$. Der Grenzwert von $\mathcal{F}$ kann abgeschätzt werden durch

$$\lambda(\mathcal{F}) \geq \frac{2}{l-2}.$$

Beweis: Die Kongruenz $r \equiv 0 \pmod 2$ (bzw. $l \equiv 0 \pmod 2$) stellt sicher, daß $a = -1$ eine $(l-1)$-te Potenz in $\mathbb{F}_q$ ist. Damit folgt das Resultat ganz analog zu Beispiel 1.2.6. □

4.2 Der Grenzwert über F_0 total verzweigter Norm Fermat Türme

Als nächstes wollen wir den exakten Grenzwert von über F_0 total verzweigten Norm Fermat Türmen $\mathcal{F}$ bestimmen. Wir gehen dabei in zwei Schritten vor. Zunächst bestimmen wir den Verzweigungsort von $\mathcal{F}$ über F_0, und anschließend bestimmen wir den exakten Grenzwert von $\mathcal{F}$.

Ein Fermat Turm $\mathcal{F}$ verzweigt genau dann total über F_0, wenn die Nullstelle P_0 von x_0 total verzweigt ist in $\mathcal{F}/F_0$. Dieses ist genau dann der Fall, wenn $ab^m + c = 0$ gilt.

Für den Rest des Abschnitts 4.2 sei l eine Primzahlpotenz, $q = l^r$ für ein $r \geq 2$, $m := (q-1)/(l-1)$ und $\mathcal{F}$ ein rekursiv durch die Gleichung

$$y^m = a(x+b)^m + c \text{ mit } a, c \in \mathbb{F}_l, b \in \mathbb{F}_q \text{ und } ab^m + c = 0 \tag{4.5}$$

definierter Fermat Turm.

Lemma 4.2.1 *Es sei l eine Potenz der Primzahl p und $m = l^{s-1} + l^{s-2} + \ldots + l + 1$ für ein $s \geq 1$. Dann gilt für die Binomialkoeffizienten*

1. $$\binom{m-1}{k} \equiv \begin{cases} 1 \pmod p, \text{ falls } k = \sum_{i=1}^{t} l^{s_i} \text{ für} \\ 1 \leq s_1 < s_2 < \ldots < s_t \leq s-1 \text{ oder } k = 0. \\ 0, \text{ sonst.} \end{cases}$$

2. $\left(\begin{array}{c} m \\ k \end{array}\right) \equiv \left\{ \begin{array}{c} 1 \pmod p,\ \textit{falls } k = \sum_{i=1}^{t} l^{s_i} \textit{ für} \\ 0 \leq s_1 < s_2 < \ldots < s_t \leq s-1 \textit{ oder } k = 0. \\ 0,\ \textit{sonst.} \end{array}\right.$

Beweis: Wir beweisen die erste Behauptung durch Induktion über s (man beachte: $(x+1)^{m-1} = \sum_{k=0}^{m-1} \left(\begin{array}{c} m-1 \\ k \end{array}\right) x^k$).
Für $s = 1$ gilt $(x+1)^{m-1} = 1$.
Sei nun die Behauptung richtig für s. Wir setzen $m := l^s + l^{s-1} + l^{s-2} + \ldots + l + 1$. Dann ist

$$\begin{aligned} (x+1)^{m-1} &= (x+1)^{l^s}(1 + x^l + x^{l^2} + x^{l^2+l} + x^{l^3} + \ldots \\ &\qquad + x^{l^{s-1}+l^{s-2}+\ldots+l}) \\ &= \quad (1 + x^l + x^{l^2} + \ldots + x^{l^{s-1}+l^{s-2}+\ldots+l} \\ &\qquad + x^{l^s} + x^{l^s+l} + \ldots + x^{l^s+l^{s-1}+\ldots+l}). \end{aligned}$$

Die zweite Behauptung erhalten wir nun durch Multiplikation von $(x+1)^{m-1}$ mit $(x+1)$. □

Wir können für die Fermat Gleichung o.B.d.A. $b = 1$ annehmen, indem wir in Gleichung 4.1 die Variablentransformation $\tilde{x}_i = b^{-1}x_i$ vornehmen (es ist $\mathbb{F}_q(x_0, \ldots, x_n) = \mathbb{F}_q(\tilde{x}_0, \ldots, \tilde{x}_n)$).

Für den Rest des Abschnitts 4.2 bezeichne wieder P_α die Nullstelle von $x_0 - \alpha$ in F_0.

Lemma 4.2.2 *Es sei $\mathcal{F}$ ein rekursiv durch Gleichung 4.5 definierter Fermat Turm. Dann ist der Verzweigungsort $V_{F_0}(\mathcal{F}) = \{P_\alpha \in \mathbb{P}_{F_0} | \alpha \in \mathbb{F}_q\}$.*

Beweis: Nach Theorem 4.1.4 gilt $V_{F_0}(\mathcal{F}) \subseteq \{P_\alpha \in \mathbb{P}_{F_0} | \alpha \in \mathbb{F}_q\}$. Also ist insbesondere $|V_{F_0}(\mathcal{F})| < \infty$. Wir definieren $T := \{\alpha^m | P_\alpha \in V_{F_0}(\mathcal{F})\}$ und $t := |T|$. Mithilfe von Lemma 3.2.3 erhalten wir die Identität

$$f(x) = a^t(x+1)^{m-1} \prod_{\alpha \in T}(x^m - \alpha) = x^{m-1} \prod_{\alpha \in T}(a(x+1)^m + c - \alpha).$$

Nach Lemma 4.2.1 ist

$$f(x) = a^t(x^{m-1} + x^{m-1-l} + x^{m-1-l^2} + \ldots + x^l + 1) \prod_{\alpha \in T}(x^m - \alpha) =$$

$$= x^{m-1} \prod_{\alpha \in T}(a(x^m + x^{m-1} + x^{m-l} + x^{m-l-1} + \ldots + x + 1) + c - \alpha).$$

Es sei $f(x) = \sum_{i=0}^{tm+m-1} f_i x^i$. Dann folgt aus der linken Seite von obiger Gleichung:

$$\begin{aligned} f_{tm+m-2} &= 0 \\ f_{tm+m-3} &= 0 \\ &\vdots \\ f_{tm+m-l} &= 0. \end{aligned}$$

Die rechte Seite ergibt:

$$\begin{aligned}
f_{tm+m-2} &= a^t \cdot t \\
f_{tm+m-3} &= a^t \cdot \binom{t}{2} \\
f_{tm+m-4} &= a^t \cdot \binom{t}{3} \\
&\vdots \\
f_{tm+m-l} &= a^t \cdot \binom{t}{l-1}.
\end{aligned}$$

Also erhalten wir $t \equiv 0 \pmod p$ und $t > l-1$. Für alle $0 \neq \alpha \in T$ existieren m paarweise verschiedene Stellen $P_{\alpha_1}, P_{\alpha_2}, \ldots, P_{\alpha_m} \in V_{F_0}(\mathcal{F})$ mit $\alpha_i^m = \alpha$ (vgl. Bemerkung 3.2.4). D.h. der Verzweigungsort $V_{F_0}(\mathcal{F})$ hat mindestens die Mächtigkeit $1 + (t-1)m \geq 1 + (l-1)m = q$. □

Wir erhalten nun für den Grenzwert von über F_0 total verzweigten Norm Fermat Türmen das folgende Resultat.

Theorem 4.2.3 *Der exakte Grenzwert eines durch Gleichung 4.5 definierten Fermat Turms $\mathcal{F}$ ist*

$$\lambda(\mathcal{F}) = \frac{2}{q-2}.$$

Beweis: Es bezeichne a_i den durch Gleichung 3.3 eingeführten Korrekturterm. Wir haben $\lambda(\mathcal{F}) = \frac{\nu_{F_0}(\mathcal{F})}{\gamma_{F_0}(\mathcal{F})}$ mit

$$\nu_{F_0}(\mathcal{F}) := \lim_{i\to\infty} \frac{N(F_i)}{m^i} = \lim_{i\to\infty} \frac{m^i + a_i}{m^i} = 1,$$

nach Lemma 3.2.5, und

$$\begin{aligned}
\gamma_{F_0}(\mathcal{F}) &:= \lim_{i\to\infty} \frac{g(F_i)}{m^i} \\
&= \lim_{i\to\infty} \frac{-2m^i + \sum_{P \in V_{F_0}(\mathcal{F})} m^i - a_i + 2}{2m^i} = \frac{q-2}{2},
\end{aligned}$$

nach der Hurwitzschen Geschlechtsformel, Lemma 4.2.2 und Lemma 3.2.5. □

Bemerkung 4.2.4 *Für den Fall $q = l^2$ haben Özbudak und Thomas dieses Ergebnis mit anderen Mitteln bewiesen (vgl. [14]).*

4.3 Fermat Türme mit unendlichem Verzweigungsort

Man konnte bislang nur von den in Abschnitt 4.1 angeführten Fermat Türmen zeigen, daß sie asymptotisch gut sind. Zugleich scheint es ebenfalls schwierig zu zeigen, daß für andere Fermat Gleichungen die resultierenden Türme asymptotisch schlecht sind (über geeigneten Konstantenkörpererweiterungen).

Im folgenden wollen wir einen Fermat Turm mit unendlichem Verzweigungsort diskutieren. Weiter werden wir im Fall über F_0 total verzweigter Fermat Türme ein allgemeines Kriterium für den Grad der Fermat Gleichung angeben, damit der resultierende Turm einen endlichen Verzweigungsort hat. Wir übernehmen dabei die in Lemma 3.2.3 eingeführte Notation.

Satz 4.3.1 *Sei char $\mathbb{F}_q \neq 2$. Dann hat der durch die Gleichung*

$$y^2 = (x+1)^2 - 1 \tag{4.6}$$

rekursiv definierte Turm $\mathcal{F}/\mathbb{F}_q$ einen unendlichen Verzweigungsort.

Beweis: Der Turm $\mathcal{F}$ ist total verzweigt über F_0. Angenommen $|T| = t < \infty$. Dann ist nach Lemma 3.2.3

$$f(x) := (x+1)\prod_{\alpha\in T}(x^2-\alpha) = x\prod_{\alpha\in T}(x^2+2x-\alpha).$$

Wir setzen $f(x) = a_{2t+1}x^{2t+1} + a_{2t}x^{2t} + \ldots + a_1 t + a_0$. Dann folgt aus der linken Seite der obigen Identität $a_{2t} = 1$. Aus der rechten Seite folgt $a_{2t} = 2t$, also ist $2t \equiv 1 \pmod p$. Insbesondere gilt $t \not\equiv 0 \pmod p$ und $t-1 \not\equiv 0 \pmod p$. Für den Koeffizienten a_{2t-1} folgt (aus der linken Seite)

$$a_{2t-1} = \sum_{\alpha\in T} -\alpha.$$

Die rechte Seite erzwingt hingegen

$$a_{2t-1} = \sum_{\alpha\in T} -\alpha + \frac{t(t-1)}{2}2^2,$$

im Widerspruch zu der Annahme. □

Bemerkung 4.3.2 *Die oben diskutierte Gleichung 4.6 unterscheidet sich nur durch Multiplikation der rechten Seite mit -1 von der in Beispiel 1.2.6 diskutierten Gleichung, die rekursiv einen asymptotisch guten Turm definiert.*

Falls der Grad der Fermat Gleichung echt größer als zwei ist und der resultierende Turm total verzweigt ist über F_0, ergibt sich aus der Forderung eines endlichen Verzweigungsorts eine allgemeine Bedingung für den Grad der Fermat Gleichung.

Theorem 4.3.3 *Es sei $\mathcal{F}$ ein Fermat Turm rekursiv definiert durch*

$$y^m = a(x+b)^m + c \text{ mit } m > 2 \text{ und } ab^m + c = 0.$$

Ist der Verzweigungsort $V_{F_0}(\mathcal{F})$ von $\mathcal{F}$ endlich, so ist $m \equiv \pm 1 \pmod p$.

Beweis: Wegen $ab^m + c = 0$ ist $\mathcal{F}$ total verzweigt über F_0. Sei $|T| = t$. Nach Lemma 3.2.3 gilt

$$x^{m-1} \prod_{\alpha \in T} (a(x+b)^m + c - \alpha) = a^t (x+b)^{m-1} \prod_{\alpha \in T} (x^m - \alpha).$$

O.B.d.A. können wir $b = 1$ annehmen, indem wir die Koordinatentransformation $\tilde{x}_i = b^{-1} x_i$ vornehmen (dann ist $\mathbb{F}_q(x_0, \ldots, x_n) = \mathbb{F}_q(\tilde{x}_0, \ldots, \tilde{x}_n)$). Daher erhalten wir

$$\begin{aligned}
& (x+1) \textstyle\prod_{c \neq \alpha \in T} ((x+1)^m + \frac{c-\alpha}{a}) = x \prod_{0 \neq \alpha \in T} (x^m - \alpha) \\
\Leftrightarrow \quad & x \textstyle\prod_{c \neq \alpha \in T} (x^m + m x^{m-1} + \begin{pmatrix} m \\ 2 \end{pmatrix} x^{m-2} + \ldots + mx + 1 + \frac{c-\alpha}{a}) + \\
& \textstyle\prod_{c \neq \alpha \in T} (x^m + m x^{m-1} + \begin{pmatrix} m \\ 2 \end{pmatrix} x^{m-2} + \ldots + mx + 1 + \frac{c-\alpha}{a}) \\
= \quad & x^{(t-1)m+1} + \left(\textstyle\sum_{0 \neq \alpha \in T} -\alpha \right) x^{(t-2)m+1} + \ldots + (-1)^{t-1} \prod_{0 \neq \alpha \in T} \alpha x.
\end{aligned}$$

Koeffizientenvergleich (beim Exponenten $(t-1)m$) ergibt:

$$(t-1)m \equiv -1 \pmod p$$

(man beachte, daß $(t-2)m+1 < (t-1)m$). Im Fall $p = 2$ ist die Behauptung trivial. Im Fall $p \neq 2$ ergibt ein Vergleich der Koeffizienten beim Exponenten $(t-1)m - 1$ (man beachte $m > 2$)

$$\begin{aligned}
& (t-1) \begin{pmatrix} m \\ 2 \end{pmatrix} + \begin{pmatrix} t-1 \\ 2 \end{pmatrix} m \equiv -m(t-1) \pmod p \\
\Leftrightarrow \quad & -\tfrac{m-1}{2} - \tfrac{t-2}{2} \equiv 1 \pmod p \\
\Leftrightarrow \quad & m - 1 + t \equiv 0 \pmod p \\
\Leftrightarrow \quad & m - \tfrac{1}{m} \equiv 0 \pmod p \\
\Leftrightarrow \quad & m \equiv \pm 1 \pmod p.
\end{aligned}$$

□

Bemerkung 4.3.4 *Obwohl wir in Satz 4.3.1 und Theorem 4.3.3 zeigen konnten, daß viele Gleichungen zu Fermat Türmen mit unendlichem Verzweigungsort führen, ist es nicht gelungen zu entscheiden, ob das F_0-Geschlecht $\gamma_{F_0}(\mathcal{F})$ in einem der Fälle unendlich ist.*

Kapitel 5

Relativ unverzweigte Türme

5.1 Der Grenzwert relativ unverzweigter Türme

Für relativ unverzweigte Türme kann das F-Geschlecht verhältnismäßig leicht bestimmt werden.

Theorem 5.1.1 *Sei $\mathcal{T}$ ein relativ unverzweigter Turm über $\mathbb{F}_q$. Dann hat $\mathcal{T}$ endliches F-Geschlecht. Genauer gilt: Ist $\mathcal{T}$ unverzweigt über F, so ist*

$$\gamma_F(\mathcal{T}) = g(F) - 1.$$

Beweis: Die Behauptung folgt direkt aus der Hurwitzschen Geschlechtsformel; denn es sei $(F_k)_{k\geq 0}$ eine Darstellung von $\mathcal{T}$ mit $F_0 = F$. Dann ist

$$\gamma_F(\mathcal{T}) = \lim_{k\to\infty} \frac{g(F_k)}{[F_k : F_0]} = \lim_{k\to\infty} \frac{[F_k : F_0](g(F) - 1) + 1}{[F_k : F_0]} = g(F) - 1.$$

□

Theorem 5.1.2 *Sei $\mathcal{T}$ ein relativ unverzweigter rekursiv definierter Turm über $\mathbb{F}_q$. Dann sind äquivalent:*

i) $\lambda(\mathcal{T}) > 0$.

ii) $\nu_{F_0}(\mathcal{T}) > 0$.

iii) Es existiert mindestens eine $\mathbb{F}_q$-rationale Stelle in $\mathcal{T}$, die komplett zerfällt.

Beweis: i) $\Leftrightarrow$ *ii)*: Ist eine direkte Konsequenz aus $\lambda(\mathcal{T}) = \frac{\nu_F(\mathcal{T})}{\gamma_F(\mathcal{T})}$ und Theorem 5.1.1.
ii) $\Leftarrow$ *iii)*: Gilt nach Satz 1.1.11.

ii) $\Rightarrow$ *iii)*: Da der Turm relativ unverzweigt ist, zerfällt genau dann keine $\mathbb{F}_q$-rationale Stelle komplett in $\mathcal{T}$, wenn jede $\mathbb{F}_q$-rationale Stelle von F_0 eine träge Erweiterung in $\mathcal{T}$ besitzt (gemäß Korollar 2.1.4). Damit folgt das Theorem aus Korollar 3.1.2. $\square$

Weiter erhalten wir für den Grenzwert:

Theorem 5.1.3 *Es sei $\mathcal{T}$ ein relativ unverzweigter rekursiv definierter Turm über $\mathbb{F}_q$. $F < \mathcal{T}$ sei ein Funktionenkörper, so daß $\mathcal{T}/F$ unverzweigt ist. Dann gilt:*

$$\lambda(\mathcal{T}) \geq \frac{t}{g(F) - 1},$$

wobei t die Anzahl der über F komplett zerfallenden Stellen bezeichnet.

5.2 Asymptotisch gute relativ unverzweigte Türme

Es sei $q \neq 2, 3$ eine Primzahlpotenz und $m = q - 1$. Weiter sei

$$K = \begin{cases} \mathbb{F}_{q^m} & \text{falls } q \equiv 0 \pmod 4 \text{ oder } q \equiv 3 \pmod 4 \\ \mathbb{F}_{q^{2m}} & \text{falls } q \equiv 1 \pmod 4. \end{cases}$$

Wir betrachten rekursiv durch die Gleichung

$$y^m = 1 - \frac{x^m}{(x-1)^m} \tag{5.1}$$

definierte Körper.

Zunächst diskutieren wir ein Kriterium, das sicherstellt, daß die obenstehende Gleichung rekursiv einen nicht endlich erzeugten Körper definiert.

Lemma 5.2.1 *Die Gleichung (5.1) hat als Fixpunkte gerade die von 1 verschiedenen Nullstellen des Polynoms*

$$x^{2m+1} - 2x^m + 1.$$

Beweis: Ausmultiplizieren von Gleichung (5.1) und Multiplizieren der Gleichung mit $x - 1$ liefert das Ergebnis. $\square$

Lemma 5.2.2 *Falls für eine Nullstelle $\alpha \neq 1$ von $x^{2m+1} - 2x^m + 1$ und ein $\omega \in \mathbb{F}_q^* \setminus \{1\}$ die folgende Bedingung gilt:*

Für alle $r|m$ mit $r > 1$ ist $\frac{\alpha-1}{\omega\alpha-1} \notin \mathbb{F}_q(\alpha)^r$.

Dann ist $\mathcal{T}$ ein Turm.

Beweis: Gemäß dem Theorem von Kummer und Lemma 5.2.1 besitzt die Stelle P mit $x_0(P) = \alpha$ gerade die Erweiterungen $P' \in \mathbb{P}_{K(x_0,x_1)}$ mit $x_1(P') = \omega\alpha$ für $\omega \in \mathbb{F}_q^*$. Insbesondere existiert eine Erweiterung $P'|P$ mit $x_1(P') = \alpha$. Nach dem Trägheitskriterium (Satz 2.3.1) ist $\mathcal{T}$ nicht endlich erzeugt, falls eine Stelle $Q \in \mathbb{P}_{K(x_0)}$ mit $x_0(Q) = \omega\alpha, \omega \in \mathbb{F}_q^*$, total träge ist in $K(x_0, x_1)$. Eine solche Stelle existiert, falls das Polynom

$$f(x) = x^m - (1 - \frac{(\omega\alpha)^m}{(\omega\alpha - 1)^m})$$

irreduzibel ist über $\mathbb{F}_q(\alpha)$. Da $\mathbb{F}_q$ eine primitive m-te Einheitswurzel enthält, folgt aus der Theorie zyklischer Erweiterungen, daß $f(x)$ genau dann irreduzibel über $\mathbb{F}_q(\alpha)$ ist, wenn für das Element

$$\eta = (1 - \frac{(\omega\alpha)^m}{(\omega\alpha - 1)^m}) = \frac{(\omega\alpha)^m - 1}{(\omega\alpha - 1)^q}$$

gilt, daß $\eta \notin \mathbb{F}_q(\alpha)^r$ ist (für alle $r|m$ mit $r > 1$). Nun ist

$$\eta = \frac{\alpha^{2m+1} + (\omega\alpha)^m - 2\alpha^m}{(\omega\alpha - 1)^q} = \alpha^m \frac{(\alpha - 1)^q}{(\omega\alpha - 1)^q}.$$

Also ist nur dann $\eta \in \mathbb{F}_q(\alpha)^r$, wenn

$$\frac{\alpha - 1}{\omega\alpha - 1} \in \mathbb{F}_q(\alpha)^r \text{ bzw. } \frac{\alpha - 1}{\omega\alpha - 1} \in -4\mathbb{F}_q(\alpha)^4,$$

was die Behauptung beweist. □

Mithilfe von Satz 2.3.1 läßt sich rechnergestützt für kleine Primzahlpotenzen zeigen, daß Gleichung 5.1 rekursiv nicht endlich erzeugte Körper definiert. Zur Konstruktion der Stelle P aus der Bedingung $(*)$ in 2.3.1 wurden Stellen P_α gewählt mit $x_0 = \alpha \pmod{P}$ für einen Fixpunkt α wie in Lemma 5.2.1 beschrieben. Ausgehend von einem Fixpunkt α wurden dann gemäß der definierenden Gleichung Folgen $(\mu_k)_{k\geq 0}$ konstruiert. Es wurden dabei zunächst alle Folgen von der Länge 2, dann Folgen der Länge 3 getestet, bis eine Folge gefunden wurde, die der Bedingung $(**)$ aus Satz 2.3.1 genügt. Die Ergebnisse sind in den folgenden Tabellen aufgelistet. Dabei gibt die linke Spalte den Körper $\mathbb{F}_q$ an, über dem gerechnet wurde. Die Nullstellen des Polynoms in der mittleren Spalte sind total träge, und können als Stellen P_{μ_0} aus Bedingung $(**)$ in Satz 2.3.1 herangezogen werden (für eine geeignete Erweiterung des Konstantenkörpers, vgl. Bemerkung 2.3.2). Die dritte Spalte gibt die Länge einer kürzesten Folge zwischen einem Fixpunkt und einer der in der zweiten Spalte angegebenen Nullstellen an. In allen untersuchten Beispielen garantiert Satz 2.3.1, daß Gleichung 5.1 rekursiv nicht endlich erzeugte Körper definiert.

q	Träge Nullstelle	Länge der Folge (μ_k)
5	x^2+4x+2	2
7	$x^{12}+2x^{11}+6x^{10}+5x^8+x^7+2x^6$	
	$+2x^5+x^4+3x^3+2x^2+6$	3
11	x^2+5x+1	2
13	$x^{20}+2x^{19}+2x^{18}+4x^{17}+2x^{16}$	
	$+4x^{15}+4x^{14}+5x^{13}+10x^{12}+10x^{11}+$	
	$6x^{10}+7x^9+8x^8+9x^7+5x^6+2x^5+7x^4$	
	$+10x^3+8x^2+7x+11$	3

q	Träge Nullstelle	Länge der Folge (μ_k)
4	$x^6+x^4+x^2+x+1$	2
8	$x^6+x^4+x^2+x+1$	2
16	$x^{20}+x^{17}+x^{14}+x^{12}+x^{11}+x^{10}+x^9$	
	$+x^8+x^7+x^6+1$	2
32	$x^{10}+x^5+x^4+x^2+1$	2
64	$x^{42}+x^{36}+x^{30}+x^{29}+x^{21}+x^{18}+x^{17}$	
	$+x^{15}+x^{11}+x^{10}+x^9+x^8+x^6+x^4$	
	$+x^3+x+1$	2
128	$x^{14}+x^7+x^2+x+1$	2
256	$x^{24}+x^{19}+x^{18}+x^{16}+x^{14}+x^{13}+x^{11}$	
	$+x^6+x^4+x^2+1$	2

Lemma 5.2.3 *Es sei $F := K(x,y)$ durch Gleichung (5.1) definiert.*

1. *Über $K(x)$ verzweigen genau die Nullstellen von $x-\alpha, \alpha \in \mathbb{F}_q^* \setminus \{1\}$, und die Polstelle von x in F, jeweils vom Index m.*

2. *Über $K(y)$ verzweigen genau die Nullstellen von $y-\alpha, \alpha \in \mathbb{F}_q^*$, in F, jeweils vom Index m.*

Beweis: Es sind $F/K(x)$ und $F/K(y)$ Kummererweiterungen (im zweiten Fall substituieren wir $z = x/(x-1)$). Nun folgen die Behauptungen leicht mit Hilfe der Darstellung

$$y^m = \frac{x^{m-1}+x^{m-2}+x^{m-3}+\ldots+x+1}{(x-1)^m}.$$

□

Im folgenden setzen wir voraus, daß die Gleichung 5.1 rekursiv einen nicht endlich erzeugten Körper $\mathcal{T} = \cup_{k\geq 0} F_k$ definiert. Weiter bezeichne P_α resp. P_∞ die Nullstelle von $x_0 - \alpha$ resp. den Pol von x_0 in F_0.

Satz 5.2.4 *Sei $\mathcal{T}$ rekursiv definiert durch Gleichung (5.1).*

1. *$\mathcal{T}$ ist unverzweigt über F_2.*

2. *In F_2/F_1 verzweigen genau die Stellen über der Stelle P_1, jeweils vom Index m.*

Beweis: Wir zeigen zunächst 2. Sei $Q \in \mathbb{P}_{F_1}$ eine in F_2 verzweigende Stelle. Dann verzweigt $P := Q \cap K(x_1)$ nach Abhyankars Lemma in $K(x_1, x_2)$. Angenommen $x_1(P) = \alpha \in \mathbb{F}_q^* \setminus \{1\}$. Dann verzweigt P in F_1 vom Index m, und nach Abhyankars Lemma ist Q unverzweigt in F_2. Also ist P eine Polstelle von x_1. Wiederum nach Abhyankars Lemma verzweigt dann Q in F_2/F_1 vom Index m. Die Polstellen von x_1 sind gerade die Stellen über der Nullstelle von $x_0 - 1$.

Angenommen es gäbe ein $Q \in \mathbb{P}_{F_2}$, das in $\mathcal{T}$ verzweigt. Dann hat Q eine Erweiterung $R \in \mathbb{P}_{F_j}$ für ein $j \geq 2$, so daß R in F_{j+1} verzweigt. Analog zum ersten Teil des Beweises sieht man, daß R eine Polstelle von x_j sein muß. Dann ist aber $x_{j-1}(R) = 1$ und nach Abhyankars Lemma ist R unverzweigt in F_{j+1} (da $j \geq 2$), ein Widerspruch. □

Satz 5.2.5 *Das F_2-Geschlecht von $\mathcal{T}$ ist gleich*

$$\gamma_{F_2}(\mathcal{T}) = \frac{1}{2}m^3 - m^2 - \frac{1}{2}m.$$

Beweis: Nach der Hurwitzschen Geschlechtsformel ist

$$\begin{aligned} g(F_1) &= -[F_1 : F_0] + \frac{1}{2}\deg Diff(F_1/F_0) + 1 \\ &= \frac{1}{2}m^2 - \frac{3}{2}m + 1 \end{aligned}$$

und

$$\begin{aligned} g(F_2) &= m(\frac{1}{2}m^2 - \frac{3}{2}m) + \frac{1}{2}m(m-1) + 1 \\ &= \frac{1}{2}m^3 - m^2 - \frac{1}{2}m + 1. \end{aligned}$$

Damit folgt die Behauptung aus Theorem 5.1.1. □

Satz 5.2.6 *$\mathcal{T}$ zerfällt komplett über K. Genauer gilt: Sei Q eine Stelle in F_2 über einer $\mathbb{F}_q$-rationalen Stelle von F_0. Dann zerfällt Q in $\mathcal{T}/F_2$ komplett.*

Beweis: Wir konstruieren zunächst die Stellen über $P_\alpha \in \mathbb{P}_{F_0}$ in F_3 ($\alpha \in \mathbb{F}_q \cup \{\infty\}$). Dazu unterscheiden wir die möglichen Fälle. Zudem betrachten wir zunächst den Fall $2 \not| q$:

1. Sei $\alpha \in \mathbb{F}_q^* \setminus \{1\}$ oder $\alpha = \infty$. Dann liegt über P_α genau eine (total verzweigte) $\mathbb{F}_q$-rationale Stelle P' in F_1 mit $x_1(P') = 0$. Die Stelle P' zerfällt in F_2 in lauter $\mathbb{F}_q$-rationale Stellen Q in F_2 mit $x_2(Q) \in \mathbb{F}_q^*$ (nach dem Theorem von Kummer). Da F_3/F_2 galoissch ist, zerfällt jede der Stellen Q nun in F_3 in lauter $\mathbb{F}_{q^m}$-rationale Stellen (vgl. Satz 5.2.4 und Gradformel).

2. Sei $\alpha = 1$. Wir substituieren $z := x_1(x_0 - 1)$. Dann ist $F_1 = F_0(z)$ und

$$z^m \equiv x_0^{m-1} + x_0^{m-2} + x_0^{m-3} + \ldots + x_0 + 1 \equiv -1 \pmod{P'}.$$

Daraus folgt, daß P_α in lauter $\mathbb{F}_{q^2}$-rationale Stellen P' in F_1 zerfällt, die sämtlich x_1 als Pol haben. Über jeder Stelle P' liegt in F_2 genau eine total verzweigte Stelle Q (vgl. Satz 5.2.4). Jede dieser Stellen Q zerfällt nun in F_3 in lauter $\mathbb{F}_{q^2}$-rationale Stellen in F_3 (nach dem Theorem von Kummer).

3. Sei nun $\alpha = 0$. Dann zerfällt P_α in F_1 in lauter $\mathbb{F}_q$-rationale Stellen P' mit $x_1(P') = \beta \in \mathbb{F}_q^*$. Wir betrachten zunächst den Fall $\beta \neq 1$. Dann zerfällt die Stelle P' in F_2 in lauter $\mathbb{F}_{q^m}$-rationale Stellen (mit $x_2(Q) = 0$), die ihrerseits in F_3 in lauter $\mathbb{F}_{q^m}$-rationale Stellen zerfallen. Wir betrachten nun den Fall $\beta = 1$. Die Stelle P' zerfällt in F_2 in lauter $\mathbb{F}_{q^2}$-rationale Stellen. Da F_3/F_2 galoissch ist, zerfallen diese ihrerseits in lauter $\mathbb{F}_{q^{2m}}$-rationale Stellen Q' in F_3. Wir müssen zeigen, daß die Stellen Q' genau dann $\mathbb{F}_{q^m}$-rational sind, wenn $q \equiv 3 \pmod 4$ gilt. Sei also $Q' \in \mathbb{P}_{F_3}$ mit $x_0(Q') = 0, x_1(Q') = 1, x_2(Q') = \infty$ und $x_3(Q') = 0$. Wir schreiben $z = x + \mathcal{O}(nQ')$, falls $v_{Q'}(z - x) \geq n$ gilt. Sei $\alpha \in \mathbb{F}_{q^2} \leq \mathbb{F}_{q^m}$ mit $\alpha^m = -1$. Dann ist

$$x_1^m = 1 + t^m, \text{ wobei } t = \frac{\alpha x_0}{x_0 - 1},$$

also $x_1 = 1 - t^m + t^{2m} + \mathcal{O}(3mQ')$ und somit $(x_1 - 1)^{-1} = -t^{-m}(1 + t^m + \mathcal{O}(2mQ'))$. Da

$$((x_1 - 1)x_2)^m = (-t^m + t^{2m} + \mathcal{O}(3mQ'))^m - 1 - t^m,$$

ist außerdem

$$\frac{(x_1 - 1)x_2}{\alpha} = 1 - t^m + t^{2m} + \mathcal{O}(3mQ')$$

(man beachte $q \neq 3$), also

$$x_2 = \frac{\alpha - \alpha t^m + \alpha t^{2m} + \mathcal{O}(3mQ')}{(x_1 - 1)} = -\alpha t^{-m} + \mathcal{O}((-m + 1)Q'),$$

und damit $(x_2-1)^{-1} = -\alpha^{-1}t^m + \mathcal{O}((m+1)Q')$. Weiter ist

$$\begin{aligned} x_3^m &= \frac{(x_2-1+1)^{m-1}+(x_2-1+1)^{m-2}+\mathcal{O}(-m(m+3)Q')}{(x_2-1)^m} \\ &= \frac{1}{(x_2-1)} - \frac{1}{(x_2-1)^2} + \mathcal{O}(3mQ'). \end{aligned}$$

Damit erhalten wir

$$\left(\frac{x_3}{t}\right)^m = -\alpha^{-1} + \mathcal{O}(Q').$$

$-\alpha^{-1}$ ist eine m-te Potenz in $\mathbb{F}_{q^m}$ genau dann, wenn α eine m-te Potenz in $\mathbb{F}_{q^m}$ ist. Es ist $\alpha^q = -\alpha$ und $\alpha^{q^2} = \alpha$, also $\alpha^{q^i} = (-1)^i\alpha$. Nun ist α eine m-te Potenz in $\mathbb{F}_{q^m}$, wenn ein $\beta \in \mathbb{F}_{q^m}$ existiert mit $\beta^m = \alpha$. Wegen $(-1)(-1)^{\frac{m}{2}} = \alpha^{\frac{q^m-1}{q-1}} = \beta^{q^m-1}$ ist β genau dann in $\mathbb{F}_{q^m}$, wenn $q \equiv 3 \pmod 4$ ist.

Der Fall $2|q$ verläuft ganz analog; wegen $1 \equiv -1 \pmod 2$ zerfallen alle Stellen schon über $\mathbb{F}_{q^m}$.

Sei nun $k \geq 3$ und $Q'|P_\alpha$ eine K-rationale Stelle von F_k. Dann ist $x_{k-2}(Q') \in \mathbb{F}_q \cup \{\infty\}$, und die Stelle $Q' \cap K(x_{k-2}, x_{k-1}, x_k)$ zerfällt komplett (über K) in $K(x_{k-2}, x_{k-1}, x_k, x_{k+1})$, was aus der obigen Diskussion folgt. Nach Korollar 2.1.4 zerfällt damit auch die Stelle Q' komplett in F_{k+1}. □

Korollar 5.2.7 *In $\mathcal{T}/K$ zerfallen über F_2 mindestens $2m^2+m$ Stellen komplett.*

Theorem 5.2.8 *Der Turm $\mathcal{T}/K$ definiert durch Gleichung 5.1 hat Grenzwert*

$$\lambda(\mathcal{T}) \geq \frac{4m+2}{m^2-2m-1}.$$

Beweis: Die Behauptung folgt mit Theorem 5.1.3 aus Korollar 5.2.7 und Satz 5.2.5. □

Bemerkung 5.2.9

Der Fall $q = 4$ ist ein Spezialfall eines von N.D. Elkies gefundenen Shimura-Turms (vgl. [3]).

Literaturverzeichnis

[1] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, *KANT V4*, in J. Symbolic Comp. **24** (1997), 267-283.

[2] V. G. Drinfeld, S. G. Vladut: Number of rational points of an algebraic curve, Funct. Anal. 17 (1983), 53-54.

[3] N. D. Elkies: Explicit modular towers. In: Proceedings of the Thirty-Fifth Annual Allerton Conference on Communication, Control and Computing. T. Basar and A. Vardy (Eds.), 1997, 23-32.

[4] N. D. Elkies: `http://www.math.harvard.edu/~elkies/tower2_1.html`

[5] N. D. Elkies: `http://www.math.harvard.edu/~elkies/tower2_2.html`

[6] G. Frey, M. Perret, H. Stichtenoth: On the Different of Abelian Extensions of Global Fields. In: Coding Theory and Algebraic Geometry. Proceedings, Luminy, 1991. H. Stichtenoth and M.A. Tsfasman (Eds.). Lecture Notes in Math., 1518, 26-32. Springer-Verlag, New York, Berlin, 1992.

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

[8] A. Garcia, H. Stichtenoth, M. Thomas: On Towers and Composita of Towers of Function Fields over Finite Fields. In: Finite Fields And Their Applications 3, 257-274 (1997).

[9] A. Garcia, H. Stichtenoth: Skew Pyramids of Function Fields Are Asymptotically Bad. In: Coding Theory, Cryptography and Related Areas. Berlin, New York and Heidelberg (2000).

[10] A. Garcia, H. Stichtenoth: On Tame Towers of Function Fields. To appear in: J. Reine Angew. Math.

[11] Y. Ihara: Some remarks on the number of rational points of algebraic curves over finite fields. J. Fac. Sci. Univ. Tokyo Sect. IA Math 28 (1981), 721 - 724.

[12] H.W. Lenstra: On a problem of Garcia, Stichtenoth, and Thomas. In: Finite Fields Appl. 8 (2001), 166 - 170.

[13] W-C. W. Li, H. Maharaj and H. Stichtenoth with an appendix by N. D. Elkies, New Optimal towers over fields of small characteristic. In: Lecture Notes in Computer Science 2369 (proceedings of ANTS-5, 2002), 100-116.

[14] F. Özbudak, M. Thomas: A Note on Towers Of Function Fields Over Finite Fields. In: Communications in Algebra, 26,11 (1998).

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

[16] M. A. Tsfasman, S. G. Vladut and T. Zink: Modular Curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound. Math. Nachr. 109 (1982),21 - 28.

[17] A. Weil: Sur les courbes algébrique et les variétés qui s'en déduisent. Act. Sc. et Industrielles 1041. Hermann, Paris (1948).