Extremaleigenschaften von Kreisteilungserweiterungen rationaler Funktionenkörper

Diplomarbeit

Alice Keller

Saarbrücken, Mai 1999
Fachbereich 9, Mathematik

Ich erkläre hiermit an Eides statt, diese Arbeit selbständig geschrieben und keine Hilfsmittel außer den angegebenen verwendet zu haben.

Inhaltsverzeichnis

Einleitung **7**

1 Grundlagen **11**

1.1 Divisoren 12
1.2 Erweiterung und Vervollständigung 13
1.2.1 Differente 15
1.2.2 Galoiserweiterungen 16
1.2.3 Lokal-Global-Prinzip 17
1.2.4 Komposita von Körpern 18
1.2.5 Unendliche Galoiserweiterungen 18
1.3 Der Körper $\mathbb{F}_q(T)$ 19
1.3.1 Vervollständigung an der ∞-Stelle 21
1.3.2 Erweiterungen von $\mathbb{F}_q(T)$ 21

2 Höhere Verzweigungsgruppen **23**

2.1 Globalisierung 25
2.2 Eigenschaften der Verzweigungsgruppen 25
2.3 Die Herbrand'sche φ-Funktion 26
2.4 Beispiel: Kreisteilungskörper über $\mathbb{Q}_p$ 28

3 Algebraische Funktionenkörper **29**

3.1 Das Geschlecht 29
3.2 Konstantenerweiterung 32

4 Algebraische Kurven **35**

4.1 Punkte und Ideale 35
4.2 Vollständige nichtsinguläre Kurven 36
4.3 Projektive ebene Kurven 37
4.4 Rationale Punkte 40
4.5 Projektive Transformationen 41

5 Der Carlitz–Modul **45**

5.1 Der Ring $k\{\tau\}$ 45

5.2 Drinfeld–Moduln 47
5.3 Der Carlitz–Modul 51

6 Kreisteilungserweiterungen **59**
6.1 Bezeichnungen 59
6.2 Das Geschlecht von $K(p^r)$ 62
6.2.1 Höhere Verzweigungsgruppen von $K(p^r)$ 62
6.2.2 Geschlechtsberechnung 65
6.3 Das Geschlecht von $K(n)$ 67
6.4 Der Fixkörper von $\mathbb{F}_q^*$ 68

7 Zwischenerweiterungen **71**
7.1 Zerlegungsgruppen 72
7.2 Galoisgruppen 74
7.3 Projektionsabbildungen 75
7.3.1 Einbettungen 75
7.3.2 Projektionen 76
7.3.3 Mächtigkeiten der Verzweigungsgruppen 77
7.3.4 Elementare Berechnung von $|H(n_\nu)^\alpha \cap \langle T \rangle_{G(n)}|$ 78
7.4 Geschlechtsberechnungen 78
7.5 Rationale Punkte 81
7.6 Beispiele 82
7.7 Weitere Aussichten 84

A Numerische Berechnung der $e_*(n)$ **89**

B Ausgewählte Beispiele **93**

Symbolverzeichnis **101**

Literaturverzeichnis **105**

Einleitung

In den letzten Jahren sind algebraische Funktionenkörper über endlichen Körpern mit gewissen "guten" Eigenschaften intensiv untersucht worden. Einerseits sind diese Körper beachtenswert in theoretischen Betrachtungen, die sich mit dem Zusammenhang von algebraischen Kurven und algebraischen Funktionenkörpern beschäftigen. Andererseits lieferte die Codierungstheorie Impulse zu diesem Studium. Denn 1975 gelang es V. D. Goppa zu zeigen, daß algebraische Funktionenkörper über einem endlichen Körper zur Konstruktion einer großen Klasse fehlerkorrigierender Codes, wie sie bei der Datenübertragung benötigt werden, genutzt werden können. Dabei stehen Eigenschaften dieser Codes in direktem Zusammenhang mit den Eigenschaften der Funktionenkörper. Von besonderem Interesse ist hier das Verhältnis des Geschlechts des Körpers zu der Zahl der rationalen Stellen.

Die vielen Arbeiten zugrunde liegende Idee ist es dann auch, solche Funktionenkörper zu finden, die möglichst viele rationale Stellen haben.
Für deren Zahl, die vom Geschlecht und der Elementanzahl des Grundkörpers abhängt, existieren obere Schranken. Eine erste solche ist die *Hasse–Weil–Schranke*, die J–P. Serre verbessern konnte. Verschiedene Methoden zur expliziten Berechnung lassen weitere Verbesserungen zu (vergleiche [NX99] und [Sei98]). Unklar bleibt, wie gut diese Schranken sind.

Auch dies mag Motivation sein, Beispiele für untere Schranken zu finden, zu verbessern und zu versuchen, dabei eine obere Schranke zu erreichen.

Als Klasse von Beispielen gerade die *Kreisteilungserweiterungen rationaler Funktionenkörper* zu wählen, ist in Bezug auf die Güte der Ergebnisse willkürlich. Sie erscheint vor allem deshalb geeignet, weil sie zahlentheoretisch gut zu erschließen ist.

In der klassischen Zahlentheorie bezeichnet man als Kreisteilungskörper jene Erweiterungen der rationalen Zahlen $\mathbb{Q}$, die durch Adjunktion einer primitiven n-ten Einheitswurzel ζ_n entstehen. Diese Galoiserweiterungen sind abelsch, und nach dem Satz von Kronecker und Weber ist jede abelsche Galoiserweiterung von $\mathbb{Q}$ ist in einem Kreisteilungskörper enthalten.

Carlitz konstruierte das Analogon zu den Kreisteilungspolynomen für den rationalen Funktionenkörper $K = \mathbb{F}_q(T)$ über einem endlichen Körper $\mathbb{F}_q$. Er ließ $A = \mathbb{F}_q[T]$ als Ring von Endomorphismen auf der additiven Gruppe von $\overline{K}$, dem algebraischen Abschluß von K, operieren. Für ein Element $f \in A$ ist die Operation gegeben durch ein separables Polynom mit Koeffizienten in A, dessen Nullstellenmenge eine Kreisteilungserweiterung von K erzeugt. Ad hoc konstruierte er nun ein Pendant zur klassischen e-Funktion. Als Funktionalgleichung erhielt er $e_\rho(az) = \rho_a(e_\rho(z))$ für $a \in A$, wobei ρ_a ein additives Polynom ist. Die Abbildung $a \mapsto \rho_a$ heißt *Carlitz–Modul*. Es gelang ihm, eine rein algebraische Beschreibung von ρ_a und somit von der Operation von A zu geben.

Sein Schüler D. Hayes beschrieb in [Hay74] schließlich die vollständige Analogie zur klassischen Theorie der Kreisteilungserweiterungen rationaler Zahlen.
Zur gleichen Zeit begann V. G. Drinfeld, die Idee von Carlitz zu verallgemeinern. Während $e_\rho(z)$ Rang 1 hat, konstruierte Drinfeld allgemeine Exponentialfunktionen beliebigen Ranges über einem beliebigen Funktionenkörper. Der Carlitz–Modul ist heute das einfachste Beispiel eines Drinfeld–Moduls.

Meine Arbeit beschäftigt sich mit jenen algebraischen Funktionenkörpern $K(n)$ mit $n \in A$, die man durch Adjunktion der n-Torsionselemente des Carlitz–Moduls aus dem rationalen Funktionenkörper $K = \mathbb{F}_q(T)$ erhält.

Nachdem in den ersten vier Kapiteln die theoretischen Grundlagen zur Verfügung gestellt wurden sowie der Zusammenhang mit algebraischen Kurven beschrieben wurde, wird in Kapitel 5 der für meine Arbeit zentrale Satz bewiesen, der die algebraische und zahlentheoretische Struktur der Kreisteilungserweiterungen beschreibt.

Davon ausgehend kann nun in Kapitel 6 das Geschlecht von $K(n)$ berechnet werden. Das allein führt jedoch nicht zu dem Ziel, Körper mit möglichst vielen rationalen Stellen zu finden. Wir werden in Kapitel 7 gewisse Zwischenerweiterungen L mit $K \subset L \subset K(n)$ betrachten. Denn zu einer rationalen Stelle von K läßt sich ein Zwischenkörper ermitteln, in dem die Stelle voll zerlegt ist. Dieser wird Zerlegungskörper genannt. Im Schnitt mehrerer Zerlegungskörper sind dann diese Stellen ebenfalls voll zerlegt und somit rational. Auf diese Weise läßt sich nun eine Mindestzahl rationaler Stellen von L ermitteln.

Zur Berechnung des Geschlechtes wird jeweils die *Riemann–Hurwitz–Formel* genutzt, deren Gestalt für den Spezialfall einer abelschen Erweiterung in Satz 3.9 beschrieben ist. Ein wesentliches Element sind hier die Mächtigkeiten der höheren Verzweigungsgruppen. Diese Gruppen zu ermitteln, ist im allgemeinen schwierig. Hier nun ist die Wahl der Kreisteilungserweiterungen als Klasse von Beispielen von besonderer Bedeutung. Dadurch, daß wir die Galoisgruppen genau kennen, können die Verzweigungsgruppen, wenn auch mit einigem theoretischen und rechnerischen Aufwand, bestimmt werden.

Die entwickelten Formeln sind so explizit, daß sie Herrn Dipl.–Math. B. Wack die Erstellung eines Computerprogrammes ermöglichten. Es berechnet über dem Körper mit zwei Elementen für Polynome $n \in \mathbb{F}_2[T]$ vom Grad ≤ 15 das Geschlecht des Körpers $K(n)$ sowie dreier Zwischenkörper. Die Beispiele sowohl in Abschnitt 7.6 als auch in Anhang B sind Ergebnisse dieses Programmes.

Eine Rücksprache mit Herrn Prof. Dr. H. Niederreiter, der so freundlich war, unsere Ergebnisse mit den ihm zur Verfügung stehenden Daten zu vergleichen, ergab, daß drei der ermittelten Beispiele eine Verbesserung bisher bekannter unterer Schranken darstellen. Dabei handelt es sich um Körper des Geschlechtes 38, 66 und 81. In Beispiel 7.22, 7.23 und 7.24 wird dies näher ausgeführt.

Insgesamt zeigt das Material, daß mit der angewendeten Methode gute Beispiele gefunden werden können, und zugleich, daß dies praktisch nur rechnergestützt möglich ist.

Eine weitere Verfeinerung der Methode, bei der Teilkörper der ermittelten Zwischenkörper betrachtet werden, kann – systematisch angewendet – weitere gute Beispiele zu Tage fördern. Im Abschnitt 7.7 führe ich drei Beispiele aus, die mögliche Vorgehensweisen und somit eine Fortführung der vorliegenden Arbeit beschreiben.

Mein Dank gilt Herrn Prof. Dr. E.–U. Gekeler für das interessante Thema und die intensive Betreuung. Herrn Dipl.–Math. B. Wack und Herrn Dipl.–Math. M. Gebhardt danke ich für ihre umfangreiche Programmierarbeit und die viele Zeit, die sie in inhaltliche Diskussionen und schließlich das Korrekturlesen meiner Arbeit investiert haben. Zudem danke ich Herrn Dr. O. Scheja für seine tatkräftige Unterstützung, einige Beweise im Zusammenhang zu verstehen. Schließlich danke ich meiner Freundin Frau G. Gindorf, die mich ermutigt hat, den Weg des Mathematik–Studiums einzuschlagen, und die mich immer wieder moralisch unterstützte.

Kapitel 1

Grundlagen

Die fundamentalen Begriffe und Zusammenhänge aus der algebraischen Zahlentheorie, die ich in meiner Arbeit verwende, erkläre ich im folgenden an der konkreten, der Arbeit zugrunde liegenden Situation. Eine Einführung in die Begrifflichkeit der algebraischen Zahlentheorie findet sich beispielsweise in dem Buch von Koch, [Koc97], oder Lang, [Lan70].

Sei l eine Primzahl, v eine natürliche Zahl und $q = l^v$.
Mit $\mathbb{F}_q$ wird stets der Körper mit q Elementen bezeichnet. Er hat die Charakteristik l und ist vollkommen.
Sei K eine rein transzendente Erweiterung von $\mathbb{F}_q$ vom Transzendenzgrad 1. Dann heißt K *rationaler Funktionenkörper über* $\mathbb{F}_q$.
Eine endliche Erweiterung L von K heißt *algebraischer Funktionenkörper über* $\mathbb{F}_q$. Im folgenden wird die Erweiterung stets als separabel vorausgesetzt.

Die nicht–trivialen diskreten Bewertungen von K bzw. L, die auf $\mathbb{F}_q$ trivial sind, bilden Äquivalenzklassen, die durch die normierten diskreten Bewertungen repräsentiert werden können. Eine Klasse von Bewertungen heißt eine *Stelle von* K *bzw. von* L. Die Menge aller Stellen von K bzw. L wird im folgenden mit $S(K)$ bzw. $S(L)$ bezeichnet.
Ein Element aus $S(K)$ bzw. $S(L)$ wird mit $\mathfrak{p}$ bzw. $\mathfrak{P}$ bezeichnet und die zugehörige normierte, diskrete Bewertung mit $v_\mathfrak{p}$ bzw. $v_\mathfrak{P}$.
Jeder Bewertung $v_\mathfrak{p}$ von K und $v_\mathfrak{P}$ von L lassen sich in eindeutiger Weise Bewertungsringe zuordnen, die als $\mathcal{O}_{(\mathfrak{p})} \subset K$ und $\mathcal{O}_{(\mathfrak{P})} \subset L$ geschrieben werden.
Der Ring $\mathcal{O}_{(\mathfrak{p})}$ enthält das maximale Ideal

$$\mathfrak{p} := \{x \in K \mid v_\mathfrak{p}(x) > 0\}$$

und $\mathcal{O}_{(\mathfrak{P})}$ das maximale Ideal

$$\mathfrak{P} := \{x \in L \mid v_\mathfrak{P}(x) > 0\}.$$

Das Symbol “$\mathfrak{P}$ “ werde ich im folgenden zur Bezeichnung sowohl der maximalen Ideale als auch der Stellen des Körpers und der Primdivisoren, die im nächsten Abschnitt definiert werden, gebrauchen, da sie sich eineindeutig entsprechen.

Der Körper $\mathcal{O}_{(\mathfrak{p})}/\mathfrak{p}$ ist der Restkörper von K bezüglich der Bewertung $v_{\mathfrak{p}}$ und $\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P}$ der von L bezüglich der Bewertung $v_{\mathfrak{P}}$.

1.1 Divisoren

Im Gegensatz zur klassischen Situation, bei der ein algebraischer Zahlkörper einen ausgezeichneten Teilring, nämlich den der ganzen Zahlen, besitzt, ist hier die Auswahl eines in K enthaltenen Hauptidealringes, mit dessen Hilfe sich die sogenannten endlichen Bewertungen definieren lassen, stets abhängig von der Wahl der Unbestimmten und der damit verbundenen willkürlichen Festlegung einer ∞ genannten Stelle. Daher wird der Begriff des Ideals durch den invarianten Begriff des *Divisors* ersetzt.

Definition 1.1. *Die* Divisorgruppe *eines algebraischen Funktionenkörpers L über $\mathbb{F}_q$ ist definiert durch*

$$Div\,(L) := \{ \sum_{\mathfrak{P}\in S(L)} n_{\mathfrak{P}}\,\mathfrak{P} \mid n_{\mathfrak{P}} \in \mathbb{Z} \textit{ und } n_{\mathfrak{P}} = 0 \textit{ für fast alle } \mathfrak{P}\},$$

Die Elemente der Gruppe werden Divisoren *genannt. Ein Divisor $\mathfrak{D}$ heißt* Primdivisor *genau dann, wenn er von der Form*

$$\mathfrak{D} = \mathfrak{P} \quad \textit{für ein} \quad \mathfrak{P} \in S(L)$$

ist. Für einen Divisor

$$\mathfrak{D} = \sum_{\mathfrak{P}\in S(L)} n_{\mathfrak{P}}\,\mathfrak{P} \quad \textit{ist} \quad v_{\mathfrak{P}}(\mathfrak{D}) := n_{\mathfrak{P}} \quad \textit{für alle } \mathfrak{P} \in S(L).$$

Einem Element $\alpha \in L^*$ wird der Divisor

$$(\alpha) := \sum_{\mathfrak{P}\in S(L)} v_{\mathfrak{P}}(\alpha)\,\mathfrak{P}$$

zugeordnet, dieser wird Hauptdivisor *genannt. Man sagt, ein Divisor $\mathfrak{A} \in S(L)$* teilt *einen anderen $\mathfrak{B} \in S(L)$, in Zeichen: $\mathfrak{A}|\mathfrak{B}$ genau dann, wenn mit*

$$\mathfrak{A} = \sum_{\mathfrak{P}\in S(L)} a_{\mathfrak{P}} \cdot \mathfrak{P} \quad \textit{und} \quad \mathfrak{B} = \sum_{\mathfrak{P}\in S(L)} b_{\mathfrak{P}} \cdot \mathfrak{P}$$

für alle $\mathfrak{P} \in S(L)$ gilt: $a_{\mathfrak{P}} \leq b_{\mathfrak{P}}$.

Definition 1.2. *Ist $\mathfrak{P} \in S(L)$ ein Primdivisor mit der Eigenschaft, daß $\mathcal{o}_{(\mathfrak{p})} \subset \mathcal{O}_{(\mathfrak{P})}$ ist, dann sagt man, „ $\mathfrak{P}$ liegt über $\mathfrak{p}$“ oder auch “$\mathfrak{P}$ teilt $\mathfrak{p}$“, in Zeichen:* $\mathfrak{P}|\mathfrak{p}$.
Die Bewertung $v_\mathfrak{P}$ von L heißt (eine) Fortsetzung der Bewertung $v_\mathfrak{p}$.
Die Zahl $e_\mathfrak{P}(L/K)$, für die

$$e_\mathfrak{P}(L/K)(v_\mathfrak{p}(x)) = v_\mathfrak{P}(x), \quad \textit{für alle} \quad x \in K$$

gilt, heißt Verzweigungsindex von $\mathfrak{P}$ in L/K. *Der (relative)* Rest(klassen-)grad von $\mathfrak{P}$ in L/K *oder auch der* Trägheitsindex von $\mathfrak{P}$ in L/K *ist*

$$f_\mathfrak{P}(L/K) = [\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P} : \mathcal{o}_{(\mathfrak{p})}/\mathfrak{p}].$$

(i) *Sind $e_\mathfrak{P}(L/K) = f_\mathfrak{P}(L/K) = 1$ für alle $\mathfrak{P}|\mathfrak{p}$ so heißt die Erweiterung* voll zerlegt *in* $\mathfrak{p}$.

(ii) *Ist $f_\mathfrak{P}(L/K) > 1$, so heißt die Erweiterung* träge *in* $\mathfrak{P}$.

(iii) *Ist $e_\mathfrak{P}(L/K) = 1$, so heißt L/K* unverzweigt *in* $\mathfrak{P}$.

(iv) *Ist $f_\mathfrak{P}(L/K) = 1$, so heißt L/K* rein verzweigt *in* $\mathfrak{P}$.

(v) *Die Erweiterung heißt* voll verzweigt in $\mathfrak{P}$, *falls $e_\mathfrak{P}(L/K) = [L : K]$ ist.*

(vi) *Wenn $l \nmid e_\mathfrak{P}(L/K)$ ist, so heißt die Erweiterung* zahm *in $\mathfrak{P}$, und sonst* wild verzweigt.

Satz 1.3. *Es gilt:*

$$[L : K] = \sum_{\mathfrak{P}|\mathfrak{p}} e_\mathfrak{P}(L/K) f_\mathfrak{P}(L/K).$$

Beweis: siehe [Neu92, S. 173].

1.2 Erweiterung und Vervollständigung

Für jede Stelle $\mathfrak{p} \in S(K)$ läßt sich der Körper K bezüglich der Bewertung $v_\mathfrak{p}$ vervollständigen. Indem mittels der gewählten Bewertung eine Metrik eingeführt wird und K als topologischer Raum betrachtet wird, läßt sich der Begriff der Cauchyfolge einführen. Nun wird der Ring der Cauchyfolgen gebildet und nach dem maximalen Ideal aller Nullfolgen faktorisiert. Der auf diese Weise entstandene Körper ist vollständig. Hier hinein wird der Körper K eingebettet, dabei wird jedes $a \in K$ als Klasse einer konstanten Cauchyfolge, deren Vetreter beispielsweise $(a, a, \dots)$ ist, aufgefaßt. Die Bewertung $v_\mathfrak{p}$ setzt sich auf die Vervollständigung eindeutig fort.

Eine ausführliche Beschreibung zur $\mathfrak{p}$-adischen Vervollständigung findet sich in [Sti93, S.140ff].

Die Vervollständigung von K an einer Stelle $\mathfrak{p}$ wird dann mit $K_\mathfrak{p}$ bezeichnet, der diskrete Bewertungsring von $K_\mathfrak{p}$ mit $\mathcal{O}_\mathfrak{p}$. Ist π eine Uniformisierende von $\mathcal{O}_{(\mathfrak{p})}$, so läßt sich $\mathcal{O}_\mathfrak{p}$ als projektiver Limes beschreiben:

$$\mathcal{O}_\mathfrak{p} = \varprojlim \mathcal{O}_{(\mathfrak{p})}/\pi^n\mathcal{O}_{(\mathfrak{p})}.$$

Die Elemente von $K_\mathfrak{p}$ sind von der Form

$$K_\mathfrak{p} \ni x = \sum_{i=n}^{\infty} a_i\pi^i, \qquad a_i \in \mathbb{F}_{q^m}\,,\ m = [\mathcal{O}_{(\mathfrak{p})}/\mathfrak{p} : \mathbb{F}_q],\ n \in \mathbb{Z},$$

somit ist $K_\mathfrak{p} = \mathbb{F}_{q^m}((\pi))$.

Der Körper L läßt sich bezüglich der Bewertung $v_\mathfrak{P}$ auf die gleiche Weise vervollständigen wie der Körper K. Die Vervollständigung von L bezüglich $v_\mathfrak{P}$ wird mit $L_\mathfrak{P}$ und mit $\mathcal{O}_\mathfrak{P}$ der Bewertungsring von $v_\mathfrak{P}$ in $L_\mathfrak{P}$ bezeichnet.

Sei nun L/K eine separable Körpererweiterung vom Grad n und $r_\mathfrak{p}(L/K)$ die Zahl der über $\mathfrak{p} \in S(K)$ liegenden Stellen; diese seien mit $\mathfrak{P}_i$, $i = 1, \ldots, r_\mathfrak{p}(L/K)$, und mit

$$e_i = e_{\mathfrak{P}_i}(L/K) \quad \text{bzw.} \quad f_i = f_{\mathfrak{P}_i}(L/K)$$

die Verzweigungs- bzw. die Trägheitsindizes bezeichnet. Weiter sei $L_{\mathfrak{P}_i}$ die Vervollständigung von L bezüglich $\mathfrak{P}_i$. Dann gilt:

(i) $L_{\mathfrak{P}_i}$ ist eine Erweiterung von $K_\mathfrak{p}$ vom Grad $n_i = e_if_i$.

(ii) Die Bewertung $v_{\mathfrak{P}_i}$ ist die einzige Fortsetzung von $v_\mathfrak{p}$ in $L_{\mathfrak{P}_i}$, und es ist

$$e_i = e_{\mathfrak{P}_i}(L_{\mathfrak{P}_i}/K_\mathfrak{p}) \quad \text{und} \quad f_i = f_{\mathfrak{P}_i}(L_{\mathfrak{P}_i}/K_\mathfrak{p}).$$

(iii) Der kanonische Homomorphismus

$$\phi : L \otimes_K K_\mathfrak{p} \longrightarrow \prod_{i=1}^{r_\mathfrak{p}(L/K)} L_{\mathfrak{P}_i}$$

ist ein Isomorphismus.

1.2.1 Differente

Sei L/K eine endliche, separable Erweiterung, und seien $\mathfrak{p}$ bzw. $\mathfrak{P}$ eine Stelle von K bzw. L mit $\mathfrak{P}|\mathfrak{p}$ und $K_\mathfrak{p}$ bzw. $L_\mathfrak{P}$ die entsprechenden Vervollständigungen. Betrachtet man $L_\mathfrak{P}$ als $K_\mathfrak{p}$-Vektorraum, so läßt sich die *Spurform*

$$T(x, y) = Tr_{K_\mathfrak{p}}^{L_\mathfrak{P}}(xy)$$

definieren. Sie ist eine nicht-ausgeartete Bilinearform. Durch sie kann jedem (gebrochenen) Ideal $\mathfrak{a}$ von $L_\mathfrak{P}$ das duale (gebrochene) Ideal

$$\hat{\mathfrak{a}} = \{x \in L_\mathfrak{P} \mid Tr_{K_\mathfrak{p}}^{L_\mathfrak{P}}(x\mathfrak{a}) \subset \mathcal{O}_\mathfrak{p}\}$$

zugeordnet werden. Das Inverse des (gebrochenen) dualen Ideals

$$\hat{\mathcal{O}}_\mathfrak{P} = \{x \in L_\mathfrak{P} \mid Tr_{K_\mathfrak{p}}^{L_\mathfrak{P}}(x\mathcal{O}_\mathfrak{P}) \subset \mathcal{O}_\mathfrak{p}\}$$

ist die *Differente* von $L_\mathfrak{P}/K_\mathfrak{p}$, in Zeichen: $\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$.

Definition 1.4. *Das Ideal* $\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}}$ *heißt die* lokale Differente von L/K bezüglich $\mathfrak{P}$. *Die* Differente $\mathcal{D}_{L/K}$ *von* L/K *ist die Summe der lokalen Differenten:*

$$\mathcal{D}_{L/K} := \sum_{\mathfrak{P} \in S(L)} v_\mathfrak{P}(\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}})\,\mathfrak{P}.$$

Eigenschaften der Differente

(i) Ein Primivisor $\mathfrak{P}$ von L ist genau dann verzweigt über K, wenn $v_\mathfrak{P}(\mathcal{D}_{L/K}) \geq 1$ ist.
Da nur endlich viele Stellen in der Erweiterung L/K verzweigen, ist die Differente der Erweiterung L/K eine endliche Summe der lokalen Differenten.

(ii) Ist π eine Uniformisierende der lokalen Erweiterung $L_\mathfrak{P}/K_\mathfrak{p}$, so genügt π einem Eisensteinpolynom:

$$f_\pi(\pi) = \pi^e + \alpha_1\pi^{e-1} + \ldots + \alpha_e = 0 \quad \text{mit } e := e_\mathfrak{P}(L_\mathfrak{P}/K_\mathfrak{p})$$

und für die lokale Differente gilt:

$$\mathcal{D}_{L_\mathfrak{P}/K_\mathfrak{p}} = ({f_\pi}'(\pi)).$$

(iii) Dedekind'scher Differentensatz:
Für einen Divisor $\mathfrak{P}$ mit Verzweigungsindex e gilt

$$\begin{aligned} v_\mathfrak{P}(\mathcal{D}_{L/K}) &= e - 1, && \text{wenn } \mathfrak{P} \text{ zahm ist, also } l \nmid e \text{ und} \\ v_\mathfrak{P}(\mathcal{D}_{L/K}) &> e - 1, && \text{wenn } \mathfrak{P} \text{ wild verzweigt ist, also } l|e. \end{aligned}$$

(Beweis in [Sti93, S.89])

1.2.2 Galoiserweiterungen

Ist die Erweiterung L/K galoissch, so operiert die Galoisgruppe $G(L/K)$ transitiv auf der Menge der Stellen, die über einer Stelle $\mathfrak{p}$ von K liegen, Verzweigungsindizes und Restgrade hängen nur noch von $\mathfrak{p}$ ab und werden mit $e_{\mathfrak{p}}(L/K)$ bzw. $f_{\mathfrak{p}}(L/K)$ bezeichnet.
Ist $r_{\mathfrak{p}}(L/K)$ die Zahl der $\mathfrak{p}$ teilenden Stellen von L, so gilt die Beziehung:

$$[L:K] = r_{\mathfrak{p}}(L/K) \cdot e_{\mathfrak{p}}(L/K) \cdot f_{\mathfrak{p}}(L/K).$$

Für ein $\mathfrak{P} \in S(L)$ mit $\mathfrak{P}|\mathfrak{p}$ ist die Menge

$$Z_{\mathfrak{P}}(L/K) = \{\sigma \in G(L/K) \mid \sigma(\mathfrak{P}) = \mathfrak{P}\}$$

eine Untergruppe der Galoisgruppe, die *Zerlegungsgruppe* von $\mathfrak{P}$ in L/K. Mit $T_{\mathfrak{P}}(L/K)$ wird die *Trägheitsgruppe* bezeichnet, sie ist der Kern der Abbildung

$$\begin{array}{ccc} Z_{\mathfrak{P}}(L/K) & \longrightarrow & G(\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P} \,/\, \mathcal{o}_{(\mathfrak{p})}/\mathfrak{p}) \\ \sigma & \mapsto & \overline{\sigma} \end{array} \quad \text{mit} \quad \overline{\sigma}(x+\mathfrak{P}) = \sigma(x) + \mathfrak{P}.$$

Für den folgenden Abschnitt führe ich nun aus Gründen der Übersichtlichkeit die nachstehenden Abkürzungen ein:

$$Z(L/K) := Z_{\mathfrak{P}}(L/K), \qquad T(L/K) := T_{\mathfrak{P}}(L/K),$$

$$e := e_{\mathfrak{p}}(L/K), \quad f := f_{\mathfrak{p}}(L/K), \quad r := r_{\mathfrak{p}}(L/K).$$

Es gilt:

(i) Ist L^Z der Fixkörper von $Z(L/K)$ in L/K, dann ist

$$[L^Z : K] = r, \qquad [L : L^Z] = ef, \qquad G(L/L^Z) = Z.$$

(ii) Die Restkörpererweiterung $\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P} \,/\, \mathcal{o}_{(\mathfrak{p})}/\mathfrak{p}$ ist separabel, also gilt für den Fixkörper L^T der Trägheitsgruppe $T(L/K)$

$$[L : L^T] = e \quad \text{und} \quad [L^T : L^Z] = f.$$

(iii) Darüber hinaus ist bei separabler Restkörpererweiterung die Stelle $\mathfrak{p}$ in der Erweiterung L^Z/K voll zerlegt und in L^T/K unverzweigt, und alle über $\mathfrak{p}$ in L^T liegenden Stellen sind in der Erweiterung L/L^T voll verzweigt.

(iv) Für eine Zwischenerweiterung $K \subset E \subset L$ gilt:

$$\begin{aligned} Z(L/E) &= Z(L/K) \cap G(L/E) \\ T(L/E) &= T(L/K) \cap G(L/E) \end{aligned}$$

und das Diagramm

$$\begin{array}{ccccccccc} & & 1 & & 1 & & 1 & & \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & T(L/E) & \to & T(L/K) & \to & T(E/K) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & Z(L/E) & \to & Z(L/K) & \to & Z(E/K) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \to & G(\lambda/\gamma) & \to & G(\lambda/\kappa) & \to & G(\gamma/\kappa) & \to & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ & & 1 & & 1 & & 1 & & \end{array},$$

in dem κ, λ bzw. γ die Restkörper in K, L bzw. E bezeichnen, ist kommutativ mit exakten Zeilen und Spalten.

Bemerkung 1.5. Ist die Galoiserweiterung L/K zudem noch abelsch, so gilt für zwei Stellen $\mathfrak{P}$ und $\mathfrak{P}'$ von L, die eine Stelle $\mathfrak{p} \in S(K)$ teilen

$$Z_{\mathfrak{P}}(L/K) = Z_{\mathfrak{P}'}(L/K) \quad \text{und} \quad T_{\mathfrak{P}}(L/K) = T_{\mathfrak{P}'}(L/K),$$

da sowohl die Zerlegungs–, als auch die Trägheitsgruppen der verschiedenen $\mathfrak{p}$-teilenden Stellen zueinander konjugiert, im Falle einer abelschen Erweiterung also gleich sind. Dies erlaubt dann die Bezeichnung

$$Z_{\mathfrak{p}}(L/K) := Z_{\mathfrak{P}}(L/K) \quad \text{und} \quad T_{\mathfrak{p}}(L/K) := T_{\mathfrak{P}}(L/K).$$

1.2.3 Lokal-Global-Prinzip

Betrachten wir nun eine Körpererweiterung L/K, eine Bewertung $v_{\mathfrak{p}}$ und eine Fortsetzung $v_{\mathfrak{P}}$ mit $\mathfrak{P}|\mathfrak{p}$, so zeigt das Diagramm

$$\begin{tikzcd} & L_{\mathfrak{P}} \arrow[d, dash] \\ L \arrow[ur, dash] \arrow[d, dash] & K_{\mathfrak{p}} \\ K \arrow[ur, dash] & \end{tikzcd}$$

den Übergang von der "globalen Erweiterung" L/K zur "lokalen Erweiterung" $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. In dieser gilt, daß die kanonische Fortsetzung der Bewertung $v_{\mathfrak{P}}$ von L auf $L_{\mathfrak{P}}$ die eindeutige Fortsetzung der Bewertung $v_{\mathfrak{p}}$ auf $K_{\mathfrak{p}}$ in der Erweiterung $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ ist. Insbesondere ist $L_{\mathfrak{P}} = LK_{\mathfrak{p}}$.
Ist L/K eine Galoiserweiterung, so ist $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ ebenfalls galoissch mit Galoisgruppe

$$G(L_{\mathfrak{P}}/K_{\mathfrak{p}}) = Z_{\mathfrak{P}}(L/K)$$

(siehe dazu auch: [Ser79, S.31]).

1.2.4 Komposita von Körpern

Seien K', K_1 und K_2 Zwischenerweiterungen der separablen Körpererweiterung L/K mit der Eigenschaft, daß K' sowohl in K_1 als auch in K_2 liegt. Sei $\mathfrak{Q}$ ein Stelle von K_1K_2 und $\mathfrak{Q}'$, $\mathfrak{Q}_1$ bzw. $\mathfrak{Q}_2$ die zugehörigen Stellen in K', K_1 bzw. K_2, dann gilt:

$$(K_1K_2)_{\mathfrak{Q}} = K_{1,\mathfrak{Q}_1}K_{2,\mathfrak{Q}_2}.$$

Daraus folgt insbesondere:

(i) Ist $\mathfrak{Q}'$ in K_1 und K_2 voll zerlegt, dann ist es auch in K_1K_2 voll zerlegt.

(ii) Eine Stelle von K', die in K_1 und K_2 unverzweigt ist, ist auch in K_1K_2 unverzweigt.

(iii) Sind K_1 und K_2 linear disjunkt über K', und ist $\mathfrak{Q}_1$ in K_1 voll zerlegt sowie $\mathfrak{Q}_2$ in der Erweiterung K_2/K' voll verzweigt, so ist jede in K_1 über $\mathfrak{Q}_1$ liegende Stelle in K_1K_2 voll verzweigt.

1.2.5 Unendliche Galoiserweiterungen

Der Übergang von $\mathbb{F}_q$ zu $\overline{\mathbb{F}}_q$, dem algebraischen Abschluß von $\mathbb{F}_q$, kann zur Vereinfachung einiger der Berechnungen, die zur Geschlechtsbestimmung der betrachteten Körper notwendig sind, genutzt werden. Diese Erweiterung ist eine unendliche Galoiserweiterung.

Betrachten wir eine beliebige Galoiserweiterung F''/F mit Galoisgruppe $G(F''/F)$, dann erhalten wir für jede beliebige, endliche Galoiserweiterung F'/F die entsprechenden Galoisgruppen $G(F'/F)$.
Unter Nutzung der universellen Eigenschaft des projektiven Limes führt dies auf den Isomorphismus

$$G(F''/F) \longrightarrow \varprojlim_{H\in\mathcal{F}} H,$$

wobei $\mathcal{F}$ eine Familie von Galoisgruppen $G(F'/F)$ ist.

Beweis: [Neu92, S. 286]

Bemerkung 1.6. Für den Körper $\mathbb{F}_l$ mit l Elementen enthält die Galoisgruppe $G(\overline{\mathbb{F}}_l/\mathbb{F}_l)$ den Frobeniusautomorphismus φ, der durch

$$\varphi(x) = x^l \qquad \text{für alle} \qquad x \in \overline{\mathbb{F}}_l$$

definiert ist.
Die Untergruppe $(\varphi) = \{\varphi^n \mid n \in \mathbb{Z}\}$ hat denselben Fixkörper wie $G(\overline{\mathbb{F}}_l/\mathbb{F}_l)$, aber es gilt hier nicht, daß $(\varphi) = G(\overline{F}_l/\mathbb{F}_l)$ ist. Vielmehr ist wegen

$$G(\mathbb{F}_{l^v}/\mathbb{F}_l) \cong \mathbb{Z}/v\mathbb{Z}$$

die Galoisgruppe

$$G(\overline{\mathbb{F}}_l/\mathbb{F}_l) = \varprojlim_{v\in\mathbb{N}} \mathbb{Z}/v\mathbb{Z} = \hat{\mathbb{Z}},$$

wobei die Ordnungsrelation, die dem Limes zu Grunde liegt, die Teilbarkeit ist, und die Gruppe (φ) wird auf die dichte, allerdings nicht abgeschlossene Untergruppe $\mathbb{Z}$ von $\hat{\mathbb{Z}}$ abgebildet.

1.3 Der Körper $\mathbb{F}_q(T)$

Fixieren wir nun ein transzendentes Element des rationalen Funktionenkörpers K, z.B. T, so daß $K = \mathbb{F}_q(T)$ ist, so erhalten wir als Menge der Primdivisoren von $\mathbb{F}_q(T)$ die Primideale des Ringes $A = \mathbb{F}_q[T]$ und einen weiteren, der der Gradbewertung der Polynome entspricht.
Der Quotientenkörper des Polynomringes A wird mit $\mathbb{F}_q(T)$ bezeichnet. Dieser Körper ist eine Darstellung des rationalen Funktionenkörpers über $\mathbb{F}_q$ und isomorph zu jeder anderen Darstellung des rationalen Funktionenkörpers.
Als normierte, diskrete Bewertungen ergeben sich hier:

(i) Ist $p \in A$ ein irreduzibles (normiertes) Polynom, so wird die zum maximalen Ideal $\mathfrak{p} := (p)$ gehörige Bewertung definiert durch

$$\begin{aligned} v_\mathfrak{p} : \mathbb{F}_q(T)^* &\longrightarrow \mathbb{Z} \\ x = \frac{p^n a}{p^m b} &\longmapsto n - m, \end{aligned}$$

wobei $n, m \in \mathbb{N} \cup \{0\}$, $a, b \in A - \{0\}$, $\mathrm{ggT}(a,p) = \mathrm{ggT}(b,p) = 1$ ist und

$$v_\mathfrak{p}(0) := \infty$$

gesetzt wird. Offensichtlich gilt hier nun

$$v_{\mathfrak{p}}(xy) = v_{\mathfrak{p}}(x) + v_{\mathfrak{p}}(y)$$

sowie

$$v_{\mathfrak{p}}(x+y) \geq \min\{v_{\mathfrak{p}}(x), v_{\mathfrak{p}}(y)\}.$$

Bekannt ist, daß A ein Hauptidealring ist. Da jeder Hauptidealring ein Dedekindring ist, ist A auch ein Dedekindring.
Die Primideale werden von den Primelementen, also den irreduziblen Polynomen, erzeugt.
Die Lokalisierung von A nach $\mathfrak{p}$,

$$A_{(\mathfrak{p})} := \{\frac{a}{b} \in \mathbb{F}_q(T) \mid a, b \in A, b \notin \mathfrak{p}\},$$

ist ein Hauptidealring mit genau einem maximalem Ideal, nämlich $\mathfrak{p}A_{(\mathfrak{p})}$.
Der Ring der bezüglich $v_{\mathfrak{p}}$ ganzen Elemente von $\mathbb{F}_q(T)$,

$$\begin{aligned}\{x \in \mathbb{F}_q(T) \mid v_{\mathfrak{p}}(x) \geq 0\} &= \{\frac{a}{b} \mid a, b \in A, b \neq 0 \text{ und } v_{\mathfrak{p}}(a) \geq v_{\mathfrak{p}}(b)\} \\ &= \{\frac{a}{b} \mid a, b \in A, b \notin \mathfrak{p}\} = A_{(\mathfrak{p})}\end{aligned}$$

ist demnach ein diskreter Bewertungsring. Der Körper

$$A_{(\mathfrak{p})}/\mathfrak{p}A_{(\mathfrak{p})} \cong A/\mathfrak{p} = \mathbb{F}_{q^{deg(p)}}$$

wird als Restkörper von $\mathfrak{p}$ bezeichnet.

(ii) Des weiteren stellt die Funktion

$$v_\infty : \mathbb{F}_q(T)^* \longrightarrow \mathbb{Z},\ v_\infty(\frac{a}{b}) := deg(b) - deg(a)$$

wobei $a, b \in A - \{0\}$, mit $\mathrm{ggT}(a, b) = 1$ sind, und $v_\infty(0) := \infty$ ist, eine normierte, diskrete Bewertung dar mit Bewertungsring

$$A_\infty := \{\frac{a}{b} \in \mathbb{F}_q(T) \mid deg(a) \leq deg(b)\}$$

und maximalem Ideal

$$\mathfrak{m}_\infty = \{\frac{a}{b} \in \mathbb{F}_q(T) \mid deg(a) < deg(b)\}.$$

Hier ist der Restkörper

$$A_\infty/\mathfrak{m}_\infty \cong \mathbb{F}_q.$$

Die Menge aller normierten Bewertungen des Körpers $\mathbb{F}_q(T)$ findet eine eindeutige Zuordnung zur Menge

$$\{\mathfrak{p} \mid \mathfrak{p} \neq 0 \text{ ist Primideal}, \mathfrak{p} \subset A\} \cup \{\infty\}$$

und diese auch zur Menge aller Stellen $S(\mathbb{F}_q(T))$, wobei „$\mathfrak{p}$“, mit dem die diskreten Bewertungen zugeordneten Primideale bezeichnet wurden, als Symbol übernommen wird.

Weiter ist

$$A = \bigcap_{\substack{\mathfrak{p} \in S(\mathbb{F}_q(T)) \\ \mathfrak{p} \neq \infty}} A_{(\mathfrak{p})}.$$

1.3.1 Vervollständigung an der ∞-Stelle

Bezüglich der negativen Gradbewertung erhalten wir unter Vervollständigung den Körper

$$\mathbb{F}_q(T)_\infty = \mathbb{F}_q((\frac{1}{T})) = \{f(T) = \sum_{i=-\infty}^{n} a_i T^i \mid n \in \mathbb{Z} \text{ und } a_i \in \mathbb{F}_q\}.$$

Die Vervollständigung des algebraischen Abschlusses von $\mathbb{F}_q(T)_\infty$ wird mit C bezeichnet.

Bemerkung 1.7.

(i) C ist algebraisch abgeschlossen.
(Zum Beweis siehe [Gos96, S.37])

(ii) $\mathbb{F}_q(T)_\infty$ ist lokaler Körper, d.h., er ist vollständig diskret bewertet mit endlichem Restkörper.

1.3.2 Erweiterungen von $\mathbb{F}_q(T)$

Sei $L/\mathbb{F}_q(T)$ eine endliche, separable Erweiterung.
Der ganze Abschluß des Ringes A in L, den ich mit $\mathcal{O}$ bezeichne, ist ein Dedekindring. Insbesondere erhalten wir alle endlichen Stellen von L, indem man die maximalen Ideale von $\mathcal{O}$ betrachtet. Eine endliche Stelle $\mathfrak{P} \in S(L)$ teilt eine Stelle $\mathfrak{p} \in S(\mathbb{F}_q(T))$ genau dann, wenn $\mathfrak{p}\mathcal{O} \subset \mathfrak{P}$ ist.

Definition 1.8. *Für ein Ideal $\mathfrak{A} \subset \mathcal{O}$ der Form*

$$\mathfrak{A} = \prod_{i=1}^{s} \mathfrak{P}_i,$$

wobei $s \in \mathbb{N}$ *ist und die* $\mathfrak{P}_i$ *maximale Ideale in* $\mathcal{O}$ *sind, ist die* Norm *von* $\mathfrak{A}$ *gegeben durch*

$$N^L_{\mathbb{F}_q(T)}(\mathfrak{A}) = \prod_{i=1}^{s} \mathfrak{p}_i^{f_{\mathfrak{P}_i}(L/\mathbb{F}_q(T))},$$

wobei $\mathfrak{P}_i \cap A = \mathfrak{p}_i$ *ist.*
Die Diskriminante $D_{\mathcal{O}/A}$ *ist definiert als die Norm des Produktes der lokalen Differenten* $\mathcal{D}_{L_{\mathfrak{P}}/\mathbb{F}_q(T)_{\mathfrak{p}}}$*, wobei* $\mathfrak{p} \in S(\mathbb{F}_q(T))$ *eine endliche Stelle ist,*

$$D_{\mathcal{O}/A} := N^L_{\mathbb{F}_q(T)}\big(\prod_{\substack{\mathfrak{P} \subset \mathcal{O} \\ \mathfrak{P}\,\mathrm{max.\,Ideal}}} \mathcal{D}_{L_{\mathfrak{P}}/\mathbb{F}_q(T)_{\mathfrak{p}}} \big).$$

Es wird sich für die Untersuchung der ausgewählten Erweiterungen des rationalen Funktionenkörpers als sinnvoll erweisen, ab dem Kapitel 5 teilweise mittels der Fixierung der Unbestimmten und der ∞-Stelle zur idealtheoretischen Situation zurückzukehren.

Kapitel 2

Höhere Verzweigungsgruppen

Mittels der höheren Verzweigungsgruppen läßt sich unter anderem die Bewertung der Differente in einer separablen Erweiterung ermitteln, die im folgenden benötigt wird.

Neben der Definition werden hier nun sowohl einige Eigenschaften der höheren Verzweigungsgruppen genannt, die für diese Arbeit relevant sind, als auch darüber hinaus gehend solche, die den Kontext vermitteln sollen.

Dabei folge ich im wesentlichen den Aussagen von Serre, die er im Kapitel IV des Buches [Ser79] getroffen hat.

Voraussetzungen und Bezeichnungen

Sei k ein Körper mit diskreter Bewertung v_k, bezüglich der k vollständig ist. Der zugehörige Bewertungsring sei mit $\mathcal{O}_k$, das maximale Ideal von $\mathcal{O}_k$ mit $\mathfrak{p}_k$ und der Restkörper mit $\kappa = \mathcal{O}_k/\mathfrak{p}_k$ bezeichnet.
Weiter sei eine endliche galoissche Erweiterung L/k des Körpers k mit Galoisgruppe G gegeben, $\mathcal{O}_L$ bezeichne den ganzen Abschluß von $\mathcal{O}_k$ in L. Dann ist $\mathcal{O}_L$ wiederum ein diskreter Bewertungsring und analog werden v_L, $\mathfrak{p}_L$ und λ definiert.
Im folgenden setzen wir stets λ/κ als separable Erweiterung voraus.

Somit hat $\mathcal{O}_L$ eine Basis über $\mathcal{O}_k$, die von den Potenzen eines einzelnen Elementes x gebildet wird (vergleiche [Ser79, S.57]).
Wird der Verzweigungsindex mit $e_{L/k}$ und der Trägheitsgrad mit $f_{L/k}$ bezeichnet, so gilt die Beziehung:

$$e_{L/k} f_{L/k} = [L : k].$$

Wir fixieren nun ein $x \in \mathcal{O}_L$, das $\mathcal{O}_L$ als $\mathcal{O}_k$-Algebra erzeugt.
Sei $\sigma \in G$ und $-1 \leq i \in \mathbb{Z}$. Dann sind die folgenden drei Bedingungen äquivalent:

(i) σ operiert trivial auf dem Quotientenring $\mathcal{O}_L/\mathfrak{p}_L^{i+1}$.

(ii) Für alle $a \in \mathcal{O}_L$ ist $v_L(\sigma(a) - a) \geq i + 1$.

(iii) Es ist $v_L(\sigma(x) - x) \geq i + 1$.

Definition 2.1. *Für alle ganzen Zahlen $i \geq -1$ bezeichne G_i die Menge der $\sigma \in G$, die eine der drei oben genannten Bedingungen erfüllen. G_i heißt die i-te* Verzweigungsgruppe *von L/k.*

Proposition 2.2. *Die Verzweigungsgruppen G_i bilden eine Filtration der Galoisgruppe G. Weiter gilt:*

(i) G_{-1} ist die Galoisgruppe von L/k,

(ii) G_0 ist gleich der Trägheitsgruppe von L/k,

(iii) $G/G_0 \cong G(\lambda/\kappa)$ und

(iv) für ausreichend große i ist $G_i = \{1\}$.

Proposition 2.3. *Sei $H \leq G$ eine Untergruppe der Galoisgruppe, $k \subset k' \subset L$ die zugehörige Zwischenerweiterung, es ist also $H = G(L/k')$. Dann gilt:*

$$H_i = G_i \cap H.$$

Korollar 2.4. *Sei k_{nr} die maximale unverzweigte Teilerweiterung von k, die in L enthalten ist, und sei H die zugehörige Untergruppe. Dann ist $H = G_0$ und die Verzweigungsgruppen von G mit einem Index, der größer oder gleich 0 ist, entsprechen denen von H. Die Erweiterung L/k_{nr} ihrerseits ist voll verzweigt.*

Proposition 2.5. *Ist $H = G_j$ für ein $j \neq 0$, so ist*

$$(G/H)_i = \begin{cases} G_i/H, & \text{für } i \leq j \quad \text{und} \\ \{1\} & \text{für } i \geq j \end{cases} .$$

Proposition 2.6. *Für die Differente $\mathcal{D}_{L/k}$ der Erweiterung L/k gilt:*

$$v_L(\mathcal{D}_{L/k}) = \sum_{i=0}^{\infty} (|G_i| - 1),$$

wobei $|M|$ die Zahl der Elemente einer endlichen Menge M bezeichnet.

2.1 Globalisierung

Das Lokal-Global-Prinzip bietet die Möglichkeit, die hier in der lokalen Situation getroffenen Aussagen auf globale Körpererweiterungen zu übertragen. Sei K'/K eine endliche Galoiserweiterung des rationalen Funktionenkörpers K mit Galoisgruppe G. Dann sind sowohl K' als auch K globale Körper. Weiter sei $\mathfrak{p}$ eine Stelle von K und $K_\mathfrak{p}$ die Vervollständigung von K bezüglich $\mathfrak{p}$ sowie $K'_\mathfrak{P}$ jene von K' bezüglich $\mathfrak{P}$, wobei $\mathfrak{P}|\mathfrak{p}$ gelten soll, so ist die i-te Verzweigungsgruppe $G_i(\mathfrak{P})$ von G relativ zu $\mathfrak{P}$ die i-te Verzweigungsgruppe von $\mathfrak{P}$ in der Erweiterung $K'_\mathfrak{P}/K_\mathfrak{p}$:

$$G_i(\mathfrak{P}) := \left(G(K'_\mathfrak{P}/K_\mathfrak{p})\right)_i .$$

Für ein beliebiges $\sigma \in G$ gilt die Äquivalenz:

$$\sigma \in G_i(\mathfrak{P}) \quad \text{genau dann, wenn} \quad \sigma(a) \equiv a \bmod \mathfrak{P}^{i+1} \text{ für alle } a \in \mathcal{O}_{(\mathfrak{P})} \text{ ist.}$$

Sind nun $\mathfrak{P}$ und $\mathfrak{Q}$ zwei $\mathfrak{p}$ teilende Stelle von K', so gilt die Beziehung:

$$|G_i(\mathfrak{P})| = |G_i(\mathfrak{Q})| \qquad \text{für alle } i \in \mathbb{Z},\ i \geq -1.$$

Da nämlich die Galoisgruppe transitiv auf der Menge der $\mathfrak{p}$ teilenden Primideale operiert, folgt sofort für ein $\tau \in G$ mit $\tau(\mathfrak{P}) = \mathfrak{Q}$:

$$\text{für alle } \sigma \in G_i(\mathfrak{P}) \text{ ist } \tau \circ \sigma \circ \tau^{-1} \in G_i(\mathfrak{Q}).$$

Bezeichnung 2.7. Im Falle einer globalen Galoiserweiterung werde ich die Mächtigkeit der höheren Verzweigungsgruppen einer $\mathfrak{p}$ teilenden Stelle $\mathfrak{P}$ mit

$$g_i(\mathfrak{p}) := |G_i(\mathfrak{P})|$$

bezeichnen.

Auch die Schnittbildung läßt sich auf die globale Situation übertragen. Für einen Normalteiler $H \leq G$ der Galoisgruppe G ist $H_i(\mathfrak{P}) = H \cap G_i(\mathfrak{P})$.

2.2 Eigenschaften der Verzweigungsgruppen

(i) Die Gruppe G_0/G_1 ist zyklisch. Ihre Ordnung ist relativ prim zur Charakteristik des Restklassenkörpers λ.

(ii) Die Gruppe G_0 ist auflösbar. Wenn der Restkörper κ endlich ist, so ist auch die Gruppe G auflösbar.

(iii) Sei G abelsch und $e_0 = |G_0/G_1|$.
Gilt für ein $i \in \mathbb{Z}$, daß e_0 kein Teiler von i ist, so ist $G_i = G_{i+1}$.

Sei im folgenden $char(\lambda) = l \neq 0$.

(iv) Für alle $i \geq 1$ sind die Quotienten G_i/G_{i+1} abelsche Gruppen und direkte Produkte zyklischer Gruppen der Ordnung l. Insbesondere ist die Gruppe G_1 eine l-Gruppe.

(v) Die Trägheitsgruppe ist das semidirekte Produkt einer zyklischen Gruppe mit Ordnung prim zu l und eines Normalteilers mit l-Potenz–Ordnung.

(vi) Die ganzen Zahlen $i \geq 1$, für die $G_i \neq G_{i+1}$ gilt, sind modulo l kongruent zueinander.

2.3 Die Herbrand'sche φ-Funktion

Sei $u \geq -1$ eine reelle Zahl. Mit G_u wird die Verzweigungsgruppe G_i bezeichnet, deren Index i die kleinste ganze Zahl ist, die größer oder gleich u ist.
Demnach ist für alle $u \in \mathbb{R},\ u \geq -1$,

$$\sigma \in G_u \qquad \text{genau dann, wenn} \qquad v_L(\sigma(x) - x) \geq u + 1$$

ist.

Bezeichne $|G : H|$ den Index der Untergruppe H der Gruppe G.
Unter der *Herbrand'schen φ-Funktion* versteht man die Funktion

$$\varphi_{L/k} : [-1, \infty) \longrightarrow \mathbb{R}, \qquad \varphi_{L/k}(u) = \int_0^u \frac{dt}{|G_0 : G_t|},$$

wobei

$$\begin{array}{lll} \text{für} \quad t = -1 & |G_0 : G_t| = |G_{-1} : G_0|^{-1} & \text{und} \\ \text{für} \quad -1 < t \leq 0 & |G_0 : G_t| = |G_0 : G_0| = 1 & \end{array}$$

gesetzt wird.
Die Funktion $\varphi_{L/k}$ läßt sich auch als konkrete Summe schreiben. Für eine reelle Zahl u und eine natürliche Zahl m mit $m < u \leq m + 1$ ist

$$\varphi_{L/k}(u) = \frac{1}{g_0}\left(g_1 + \ldots + g_m + (u - m) g_{m+1}\right) \quad \text{mit } g_i = |G_i|.$$

Insbesondere ist

$$\varphi_{L/k}(m) + 1 = \frac{1}{g_0} \sum_{i=0}^{m} g_i.$$

Die zu $\varphi_{L/k}$ inverse Funktion wird mit $\psi_{L/k}$ bezeichnet.

Es gilt:

(i) Die Funktion $\varphi_{L/k}$ ist stetig, stückweise linear, wachsend und konkav.

(ii) Es ist $\varphi_{L/k}(0) = 0$.

(iii) Die Funktion $\psi_{L/k}$ ist stetig, stückweise linear und konvex.

(iv) Auch ist $\psi_{L/k}(0) = 0$.

(v) Ist $v = \varphi_{L/k}(u)$ eine ganze Zahl, so ist $u = \psi_{L/k}(v)$.

(vi) In einem Körperturm galoisscher Erweiterungen $k \subset k' \subset L$ gelten die Beziehungen

$$\varphi_{L/k} = \varphi_{k'/k} \circ \varphi_{L/k'} \quad \text{und} \quad \psi_{L/k} = \psi_{L/k'} \circ \psi_{k'/k}.$$

Definition 2.8. *Nun läßt sich für die Verzweigungsgruppen eine obere Numerierung einführen. Es wird*

$$G^v = G_{\psi_{L/k}(v)}$$

gesetzt oder - dazu äquivalent -

$$G^{\varphi_{L/k}(u)} = G_u$$

Es ist also $G^{-1} = G$, $G^0 = G_0$ und für ausreichend große v ist $G^v = \{1\}$.

Proposition 2.9. *Ist H ein Normalteiler der Galoisgruppe $G = G(L/k)$, so ist für alle v*

$$(G/H)^v = G^v H/H.$$

Lemma 2.10. *Sei $k \subset k' \subset L$ der Fixkörper der Gruppe $H \leq G$ und $v = \varphi_{L/k'}(u)$ für ein $u \neq -1$. Dann gilt*

$$G_u H/H = (G/H)_v.$$

Satz 2.11 (Hasse – Arf). *Ist G eine abelsche Gruppe, und ist $v \in \mathbb{R}$ eine Sprungstelle der Filtration (G^v), dann ist v eine ganze Zahl.*

Oder in der unteren Numerierung ausgedrückt: wenn $G_i \neq G_{i+1}$ ist, dann ist $\varphi_{L/k}(i)$ eine ganze Zahl.

2.4 Beispiel: Kreisteilungskörper über $\mathbb{Q}_p$

Den Namen "Kreisteilungskörper" erhielten die Erweiterungen von $\mathbb{Q}$, die durch Adjunktion einer Einheitswurzel entstehen, weil diese bei Teilung der Kreislinie in gleichlange Abschnitte auftreten. In der Theorie der algebraischen Zahlkörper spielen sie eine ausgezeichnete Rolle. Nach dem Satz von Kronecker und Weber ist jede abelsche Erweiterung $L/\mathbb{Q}$ enthalten in einer geeigneten Kreisteilungserweiterung $\mathbb{Q}(\zeta_n)$, wobei ζ_n eine n-te, primitive Einheitswurzel ist [Lan70, S. 210].

Sei p eine beliebige Primzahl, n eine natürliche Zahl und ζ_n eine primitive n-te Einheitswurzel. Die Körper $\mathbb{Q}$ und $\mathbb{Q}(\zeta_n)$ sind bezüglich der p-adischen Bewertung nicht vollständig. Allerdings läßt sich die globale Situation wie oben beschrieben auf die lokale Situation $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ zurückführen. Die Verzweigung des Primideals (p) ist abhängig von der Wahl von n. Gilt nämlich $\mathrm{ggT}(n,p) = 1$, dann ist (p) unverzweigt in $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$.

Wir betrachten nun den Fall, daß $n = p^m$ ist. Die Erweiterung $\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p$ hat dann den Grad $\varphi(n) = p^{m-1}(p-1)$, die Galoisgruppe G ist gleich der Gruppe der invertierbaren Elemente von $\mathbb{Z}/n\mathbb{Z}$, bezeichnet mit $G(n)$, und (p) ist total verzweigt. Das Element $1 - \zeta_n$ ist eine Uniformisierende von $\mathbb{Q}_p(\zeta_n)$.
Die höheren Verzweigungsgruppen sind hier:

$$\begin{array}{rcll} G_0 & = & G, & \\ G_u & = & G(n)^1 & \text{falls } 1 \leq u \leq p-1, \\ G_u & = & G(n)^2 & \text{falls } p \leq u \leq p^2-1, \\ \vdots & & & \quad\vdots \\ G_u & = & G(n)^m \;\; = \{1\} & \text{falls } p^{m-1} \leq u, \end{array}$$

wobei $G(n)^i := \{x \in G(n) \mid x \equiv 1 \bmod p^i\}$ ist.

Die Sprünge der Filtration (G^v) sind ganze Zahlen, und darüber hinaus gilt:

$$\begin{array}{rl} G^v = G(n)^v & \text{für } 0 \leq v \leq m, \\ G^v = \{1\} & \text{für } v \geq m, \end{array}$$

denn die Sprünge in der Filtration (G_u) geschehen an den Stellen $u = p^k - 1$, mit $0 \leq k \leq m-1$ (mit Ausnahme von $p = 2$, da 0 keine Sprungstelle ist), und $\varphi_{\mathbb{Q}_p(\zeta_n)/\mathbb{Q}_p}(p^k - 1) = k$ für alle $k = 0, 1, \ldots, m-1$.

Kapitel 3

Algebraische Funktionenkörper

In diesem Kapitel widmen wir uns dem Begriff des Geschlechtes eines algebraischen Funktionenkörpers sowie der Geschlechtsberechnung mittels der Riemann–Hurwitz–Formel.

Sei K der rationale Funktionenkörper über dem endlichen Körper $\mathbb{F}_q$ und L/K eine endliche und separable Körpererweiterung von K.

Definition 3.1. *Seien* $\mathfrak{p}$ *bzw.* $\mathfrak{P}$ *Stellen des Körpers* K *bzw.* L*. Der* Grad von $\mathfrak{p}$ *bzw.* $\mathfrak{P}$ *ist definiert durch*

$$deg\ \mathfrak{p} = [\mathcal{O}_{(\mathfrak{p})}/\mathfrak{p} : \mathbb{F}_q] \qquad bzw. \qquad deg\ \mathfrak{P} = [\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P} : \mathbb{F}_q],$$

und der Grad eines Divisors $\mathfrak{a}$ *bzw.* $\mathfrak{A}$ *von* K *bzw.* L *ergibt sich zu*

$$deg\ \mathfrak{a} = \sum_{\mathfrak{p} \in S(K)} v_{\mathfrak{p}}(\mathfrak{a}) \cdot deg\ \mathfrak{p} \qquad bzw. \qquad deg\ \mathfrak{A} = \sum_{\mathfrak{P} \in S(L)} v_{\mathfrak{P}}(\mathfrak{A}) \cdot deg\ \mathfrak{P}$$

Unter der Conorm eines Divisors

$$\mathfrak{A} = \sum_{\mathfrak{P} \in S(L)} v_{\mathfrak{P}}(\mathfrak{A}) \cdot \mathfrak{P}$$

in einer endlichen Erweiterung L'/L *versteht man den Ausdruck*

$$Con_{L'/L}(\mathfrak{A}) = \sum_{\mathfrak{P} \in S(L)} \sum_{\substack{\mathfrak{P}' | \mathfrak{P} \\ \mathfrak{P}' \in S(L')}} e_{\mathfrak{P}'}(L'/L) \cdot v_{\mathfrak{P}}(\mathfrak{A}) \cdot \mathfrak{P}'.$$

3.1 Das Geschlecht

Allgemein kann das Geschlecht eines Funktionenkörpers als eine Invariante betrachtet werden, die die Komplexität des Körpers mißt. Um den Begriff inhaltlich zu füllen, ist es notwendig, die Klasse der kanonischen Divisoren zu erklären.

In der Divisorengruppe $Div(L)$ ist die Gruppe der Hauptdivisoren $div(L)$ enthalten. Die Faktorgruppe $Div(L)/div(L) = C(L)$ ist die *Divisorklassengruppe* oder kurz die *Klassengruppe* von L. Die kanonische Klasse ist ein spezielles Element dieser Faktorgruppe.

Erinnerung: Eine *Derivation* auf einem kommutativen Ring R mit 1 ist eine Abbildung $D : R \longrightarrow R$ mit den Eigenschaften:

(i) $D(x+y) = D(x) + D(y)$,

(ii) $D(xy) = (Dx) \cdot y + x \cdot Dy$.

Ist R eine k-Algebra über einem Körper k und gilt $D|_k = 0$, so heißt D *k-Derivation* oder *Derivation über k*.

Im Funktionenkörperfall $L/\mathbb{F}_q$ ist eine $\mathbb{F}_q$-Derivation durch die Wirkung auf ein separierendes Element vollständig bestimmt.

Es gilt:

(i) Jede Derivation auf dem Körper K läßt sich eindeutig auf der Erweiterung L/K fortsetzen.

(ii) Auf $\mathbb{F}_q(T)$ hat man die Derivation $D = \frac{d}{dT}$ mit $DT = \frac{dT}{dT} = 1$.

(iii) Die Derivationen des Körpers L bilden unter punktweiser Addition und skalarer Multiplikation einen Vektorraum, den ich mit $V(L/\mathbb{F}_q)$ bezeichne.

Definition 3.2. *Ein* Differential *d eines algebraischen Funktionenköpers L über $\mathbb{F}_q$ ist ein Element des Dualraumes*

$$\hat{V}(L/\mathbb{F}_q) = Hom_L(V(L/\mathbb{F}_q), L).$$

Einem Element $u \in L$ wird das Differential

$$du : V(L/\mathbb{F}_q) \longrightarrow L, D \mapsto Du$$

zugeordnet.

Die Differentiale bilden einen eindimensionalen L-Vektorraum mit Basis dx, wobei x ein separierendes Element von $L/\mathbb{F}_q$ ist.
Ist $\pi_{\mathfrak{P}} \in L$ ein Primelement zu $\mathfrak{P} \in S(L)$, so ist $\pi_{\mathfrak{P}}$ separierend für $L/\mathbb{F}_q$; und für alle $\mathfrak{P} \in S(L)$ ist $\frac{dx}{d\pi_{\mathfrak{P}}} \neq 0$.

Definition 3.3. *Der Divisor des Differentials*

$$(dx) = \sum_{\mathfrak{P} \in S(L)} v_{\mathfrak{P}} \left(\frac{dx}{d\pi_{\mathfrak{P}}} \right) \mathfrak{P}$$

heißt der kanonische Divisor $W := (dx)$. *Die Divisorklasse von* W *wird analog die* kanonische Klasse *oder die* Differentialklasse *genannt.*
Der Grad des Divisors ist

$$\begin{aligned} deg\, W &= \sum_{\mathfrak{P} \in S(L)} v_{\mathfrak{P}}(W) \cdot deg\, \mathfrak{P} = \sum_{\mathfrak{P} \in S(L)} f_{\mathfrak{P}} \cdot (e_{\mathfrak{P}} - 1) - 2 \cdot [L : K] \\ &= 2g - 2. \end{aligned}$$

Die Zahl $g = g(L)$ *heißt das* Geschlecht *des Körpers* L*.*

Bemerkung 3.4. Der kanonische Divisor, wie er oben angeführt wird, ist wohldefiniert.
Denn sind x und y zwei separierende Elemente, so ist $dy = \frac{dy}{dx}dx$. Sind π und π' zwei Uniformisierende zu $\mathfrak{P}$, dann ist $v_{\mathfrak{P}}(\frac{d\pi}{d\pi'}) = 0$ und daher ist $v_{\mathfrak{P}}(\frac{dx}{d\pi_{\mathfrak{P}}})$ unabhängig von der Wahl der Uniformisierenden. Darüber hinaus ergibt sich daraus, daß die Summe endlich ist (vergleiche [Coh91, S. 138ff]).

Beispiele 3.5. (i) Sei $L = K$. Dann ist $(dx) = -2 \cdot \mathfrak{m}_\infty$, und daher ist $g = 0$, denn

$$v_{\mathfrak{p}}(dx) = v_{\mathfrak{p}}(\frac{dx}{d\pi_{\mathfrak{p}}}) = \begin{cases} 0\ , & \text{falls } \mathfrak{p} \text{ endlich ist,} \\ -2\ , & \text{falls } \mathfrak{p} = \mathfrak{m}_\infty \text{ ist.} \end{cases}$$

Sei nun die Charakteristik des Körpers $char\,(\mathbb{F}_q) \neq 2, 3$.

(ii) (Elliptischer Funktionenkörper) Betrachte $y^2 = f(T)$, wobei $f \in A$ ein quadratfreies Polynom vom Grad drei ist. Dann hat der Körper $\mathbb{F}_q(y, T)$ das Geschlecht eins.

(iii) Ist $f \in A$ ein quadratfreies Polynom vom Grad fünf und $y^2 = f(T)$, dann hat der Körper $\mathbb{F}_q(y, T)$ das Geschlecht zwei.

(iv) (Hyperelliptische Funktionenkörper) Allgemein gilt: sei g eine beliebige, natürliche Zahl. Dann hat der Körper $\mathbb{F}_q(y, T)$ mit $y^2 = f(T)$, wobei $f \in A$ ein quadratfreies Polynom vom Grad $\deg f = 2g + 1$ ist, das Geschlecht g. Ist $g \geq 2$, so heißt der Körper $\mathbb{F}_q(y, T)$ hyperelliptischer Funktionenkörper.

Bemerkung 3.6. Ein vollständig anderer Zugang zu dem Begriff des Geschlechtes wird in [Bea86] beschrieben.

Die Geschlechter der einzelnen Körper eines Körperturms stehen zueinander in Beziehung. Hurwitz gelang es, diese Beziehung ausgehend von dem Satz von Riemann und Roch explizit zu beschreiben. Um diese Beziehung darstellen zu können, benötigen wir zunächst einen weiteren Begriff.

Unter dem *Konstantenkörper* eines algebraischen Funktionenkörpers L versteht man den Körper

$$\tilde{F} := \{x \in L \mid x \text{ ist algebraisch über } \mathbb{F}_q\}.$$

Der Körper $\tilde{F}$ heißt *algebraisch abgeschlossen* in L oder auch der *volle Konstantenkörper.*

Satz 3.7 (Riemann-Hurwitz-Formel). *Sei L'/L eine endliche und separable Erweiterung des algebraischen Funktionenkörpers L. Seien F bzw. F' die vollen Konstantenkörper von L bzw. L'. Dann gilt für das Geschlecht von L':*

$$2g(L') - 2 = \frac{[L' : L]}{[F' : F]}\,(2g(L) - 2) + deg\,\mathcal{D}_{L'/L}.$$

3.2 Konstantenerweiterung

Im allgemeinen ist der Körper $\mathbb{F}_q$ in L nicht algebraisch abgeschlossen.
Sei nun L ein algebraischer Funktionenkörper über $\mathbb{F}_q$ mit vollem Konstantenkörper F. Weiter sei F' eine algebraische Erweiterung von F, die im algebraischen Abschluß von L enthalten ist. Das Kompositum $L' = LF'$ ist ein algebraischer Funktionenkörper über F'. Nun gilt der folgende Satz:

Satz 3.8. *(i) F' ist der volle Konstantenkörper von L'.*

(ii) Jede über F linear unabhängige Teilmenge von L ist dies auch über F'.

(iii) Für jedes $x \in L - F'$ ist $[L' : F'(x)] = [L : F(x)]$.

(iv) L'/L ist unverzweigt in jeder Stelle $\mathfrak{P}' \in S(L')$.

(v) L' hat das gleiche Geschlecht wie L.

(vi) Für jeden Divisor $\mathfrak{A} \in Div(L)$ ist

$$deg\,\mathfrak{A} = deg\,Con_{L'/L}(\mathfrak{A}).$$

(vii) Ist W ein kanonischer Divisor von L, dann ist $Con_{L'/L}(W)$ ein kanonischer Divisor von L'.

(viii) Die Conormabbildung $Con_{L'/L} : C(L) \to C(L')$ von der Divsorklassengruppe von L in die von L' ist injektiv.

(ix) Der Restklassenkörper einer Stelle $\mathfrak{P}'$ von L' ist das Kompositum des Körpers F' mit dem Restklassenkörper der Stelle $\mathfrak{P}$, für die $\mathfrak{P}'|\mathfrak{P}$ gilt.

Beweis: siehe [Sti93, S.102ff].

Der Satz zeigt, daß für einen algebraischen Funktionenkörper L, in dem $\mathbb{F}_q$ der volle Konstantenkörper ist, bei der Berechnung des Verzweigungsindexes und Geschlechtes zum algebraischen Abschluß $\overline{\mathbb{F}}_q$ von $\mathbb{F}_q$ übergegangen werden kann, da diese unter der Konstantenerweiterung invariant sind.
In Korollar 5.22 werden wir sehen, daß $\mathbb{F}_q$ in einer Kreisteilungserweiterung des rationalen Funktionenkörpers algebraisch abgeschlossen ist.

$$\begin{tikzcd}
 & L \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q \arrow[d, dash] \\
L \arrow[ur, dash] \arrow[d, dash] & K \otimes_{\mathbb{F}_q} \overline{\mathbb{F}}_q \\
K \arrow[ur, dash] &
\end{tikzcd}$$

Dieser Übergang erleichtert zahlreiche Berechnungen. Dabei ist vor allem von Bedeutung, daß in $\overline{\mathbb{F}}_q[T]$ alle Polynome in lineare Polynome zerfallen. Es existieren demnach nur Primpolynome vom Grad eins, ebenso sind alle relativen Restgrade gleich eins.
Für den Konstantenkörper gilt nämlich, daß er im Restkörper $\mathcal{O}_{(\mathfrak{P})}/\mathfrak{P}$ einer Stelle $\mathfrak{P}$ enthalten ist. Zugleich ist der Restkörper eine algebraische Erweiterung des Konstantenkörpers. Da aber $\overline{\mathbb{F}}_q$ algebraisch abgeschlossen ist, folgt Gleichheit.

Darüberhinaus vereinfacht sich die Riemann-Hurwitz-Formel in diesem Fall. Ist mit den Bezeichnungen von Satz 3.7 $\;F = \overline{\mathbb{F}}_q$ der algebraische Abschluß von $\mathbb{F}_q$, so ist $F' = F$ und es gilt

$$2g(L') - 2 = [L' : L]\,(2g(L) - 2) + deg\; \mathcal{D}_{L'/L}.$$

Zudem ergibt sich für den Grad der Differente die Vereinfachung:

$$deg\; \mathcal{D}_{L'/L} = \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{L'/L}) \cdot deg\; \mathfrak{P}' \;=\; \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{L'/L}).$$

Dies führt nun schließlich zu der Form der Riemann-Hurwitz-Formel, die wir im folgenden verwenden werden.

Satz 3.9 (Riemann-Hurwitz-Formel). *Sei L ein algebraischer Funktionenkörper mit algebraisch abgeschlossenem Konstantenkörper, sei L'/L eine endliche, separable Erweiterung von L. Dann gilt für das Geschlecht des Körpers L':*

$$2g(L') - 2 = [L' : L]\,(2g(L) - 2) + \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{L'/L}).$$

Ist die Erweiterung L'/L galoissch vom Grad m, so ist

$$2g(L') - 2 = m(2g(L) - 2) + \sum_{\mathfrak{P} \in S(L)} \frac{m}{e_{\mathfrak{P}}(L'/L)} \sum_{i=o}^{\infty} \left(g_i(\mathfrak{P}) - 1\right).$$

Beweis: Die Differente einer globalen Erweiterung ist die Summe der lokalen Differenten, also

$$\mathcal{D}_{L'/L} = \sum_{\mathfrak{P}' \in S(L')} v_{\mathfrak{P}'}(\mathcal{D}_{{L'}_{\mathfrak{P}'}/L_{\mathfrak{P}}})\mathfrak{P}',$$

so daß sich für die Bewertung der Differente an einer Stelle $\mathfrak{P}'$ ergibt:

$$v_{\mathfrak{P}'}(\mathcal{D}_{L'/L}) = v_{\mathfrak{P}'}(\mathcal{D}_{{L'}_{\mathfrak{P}'}/L_{\mathfrak{P}}}) = \sum_{i=0}^{\infty} \left(|G_i(\mathfrak{P}')| - 1\right).$$

Speziell in einer galoisschen Erweiterung gilt, daß die Mächtigkeiten der höheren Verzweigungsgruppen zu den verschiedenen über $\mathfrak{P}$ liegenden Stellen $\mathfrak{P}'$ einander entsprechen, so daß hier nur die Zahl der über $\mathfrak{P}$ in L' liegenden Stellen Einfluß nimmt. Da der Trägheitsindex jeder Stelle gerade eins ist, ist der Grad der Zerlegung $\frac{m}{e_{\mathfrak{P}}(L'/L)}$. □

Kapitel 4

Algebraische Kurven

Dem algebraischen Objekt des Funktionenkörpers entspricht in der Geometrie das der algebraischen Kurve. In diesem Kapitel werde ich einige der Beziehungen zwischen diesen beiden Objekten darstellen. Die Beweise der einzelnen Aussagen finden sich in dem Buch [Lor97].

Sei k ein beliebiger vollkommener Körper, $\overline{k}$ ein (fixierter) algebraischer Abschluß und F ein Zwischenkörper. Die Menge $\mathbb{A}^n(F) := F^n$ ist die Menge der Punkte des affinen n-Raumes mit Koordinaten in F. Die Mengen $\mathbb{A}^1(F)$ bzw. $\mathbb{A}^2(F)$ werden *affine Gerade* bzw. *affine Ebene* genannt.

Sei $f(x, y) \in k[x, y]$ ein Polynom in zwei Variablen vom Totalgrad [1] $deg\, f = d$. Die Menge der Nullstellen von f mit Koordinaten in F wird mit

$$Z_f(F) := \{(a, b) \in F \times F \mid f(a, b) = 0\}$$

bezeichnet. Sie heißt die *Menge der Punkte mit Koordinaten in F* der affinen ebenen Kurve $Z_f(\overline{k})$ vom Grad d.

Sei nun im folgenden f ein irreduzibles Polynom.

4.1 Punkte und Ideale

Der Ring $C_f := \overline{k}[x, y]/(f)$ ist ein Integritätsbereich. Wir setzen $K_f := \mathrm{Quot}\,(C_f)$. Dieser Körper wird *Körper der rationalen Funktionen* genannt, die Elemente von K_f heißen *rationale Funktionen auf $Z_f(\overline{k})$*.
Mit $Max(C_f)$ sei die Menge der maximalen Ideale in C_f bezeichnet.

[1] das Maximum der Summen der Exponenten von x und y eines Monoms von $f(x, y)$ mit einem Koeffizienten ungleich Null

Die Abbildung

$$\begin{array}{rcl} I_f : Z_f(\overline{k}) & \longrightarrow & Max(C_f) \\ (a,b) & \mapsto & (x-a, y-b) \end{array}$$

ist eine Bijektion zwischen den Punkten der Kurve $Z_f(\overline{k})$ und den maximalen Idealen von C_f. Diese bestehen aus allen Funktionen, die in (a,b) "verschwinden", d.h. der Funktionswert eines solchen Polynoms an der Stelle (a,b) ist gleich 0. Eine affine Kurve über k kann also als das Paar $(Max(R), R)$ betrachtet werden, wobei R eine endlich erzeugte k-Algebra der Dimension eins ist. Ist R ein Integritätsbereich, so wird die Kurve $(Max(R), R)$ *irreduzibel und reduziert* genannt. Die Kurve $(Max(\mathbb{F}_q[T]), \mathbb{F}_q[T])$ ist die affine Gerade.

Singuläre Punkte

Ein Punkt (a,b) in $Z_f(\overline{k})$ heißt *singulär*, falls

$$\frac{\partial f}{\partial x}(a,b) = \frac{\partial f}{\partial y}(a,b) = 0.$$

Sonst heißt der Punkt *nichtsingulär*. Wenn (a,b) ein singulärer Punkt ist, so sagt man, die Kurve $Z_f(\overline{k})$ hat in (a,b) eine Singularität oder ist in (a,b) singulär. Die Kurve heißt *nichtsingulär*, wenn sie in keinem Punkt singulär ist.

Satz 4.1. *Sei dem Punkt $(a,b) \in Z_f(\overline{k})$ das maximale Ideal $\mathfrak{m} \subset C_f$ zugeordnet. Der Punkt (a,b) ist ein nichtsingulärer Punkt von $Z_f(\overline{k})$ genau dann, wenn das maximale Ideal der Lokalisierung $(C_f)_{(\mathfrak{m})}$ von einem Element erzeugt wird.*

Beweis: [Lor97, S.67]

Naheliegend ist es nun, eine nichtsingulären Kurve über einem Körper k als eine irreduzible affine Kurve $(Max(R), R)$ über k, so daß R ein Dedekindring ist, aufzufassen.

4.2 Vollständige nichtsinguläre Kurven

Sei L/k eine endlich erzeugte Körpererweiterung vom Transzendenzgrad eins. Die Menge aller diskreten Bewertungen von L, die auf k trivial sind, $\mathcal{V}(L/k)$, ist "größer" als die Menge der maximalen Ideale eines Dedekindringes $\mathcal{O}$, dessen Quotientenkörper L ist. Um eine Analogie zum "Funktionenkörperfall" zu erhalten, wird es sinnvoll sein, all jene Bewertungsringe von L zu betrachten, die den Körper k beinhalten, und nicht nur jene, die den Dedekindring beinhalten. Dies führt zu der Definition:

Definition 4.2. *Sei k ein beliebiger Körper. Eine* vollständige nichtsinguläre Kurve X/k über k *ist ein Paar $(X, k(X))$, das aus einem Körper $k(X)/k$ vom Transzendenzgrad eins über k und einer Menge X besteht, die der Menge $\mathcal{V}(k(X)/k)$ bijektiv zugeordnet werden kann. Ein Element P von X wird* Punkt *genannt. Der Körper $k(X)$ heißt der* Körper der rationalen Funktionen von X. *Jedem Punkt P entspricht eine Bewertung v_P von $\mathcal{V}(k(X)/k)$ und ein lokaler diskreter Bewertungsring $\mathcal{O}_P$ mit maximalem Ideal $\mathfrak{m}_P$. Der Ring $\mathcal{O}_P$ heißt der* Ring der in P definierten, rationalen Funktionen. *Eine Funktion $\alpha \in \mathcal{O}_P$* verschwindet *in P oder hat eine Null in P, falls $\alpha \in \mathfrak{m}_P$. Die Zahl $v_P(\alpha)$ heißt dann* Nullstellenordnung von α. *Ist $\alpha \in k(X) - \mathcal{O}_P$, so hat α einen* Pol *in P von der Ordnung $|v_P(\alpha)|$.*

Jeder Körpererweiterung L/k vom Transzendenzgrad eins entspricht eine vollständige nichtsinguläre Kurve, nämlich $(\mathcal{V}(L/k), L/k)$. Wird nun ein transzendentes Element, z.B. T, von L fixiert, und damit eine ∞-Stelle ausgezeichnet, so ist nun sinnvoll, den Punkt, der der " ∞ - Bewertung" zugeordnet wird, mit ∞ zu bezeichnen.

Definition 4.3. *Eine* projektive Gerade über k *ist eine vollständige nichtsinguläre Kurve $\mathbb{P}^1/k$ mit der Eigenschaft, daß der Körper $k(\mathbb{P}^1)$ als k-Algebra isomorph zum rationalen Funktionenkörper in einer Variablen ist.*

Für die projektive Gerade $\mathbb{P}^1/k$, die zum Funktionenkörper $k(x)/k$, wobei x eine Unbestimmte ist, assoziiert ist, gilt:

$$\mathbb{P}^1 = \{v_{g(x)} \mid g(x) \in k[x] \text{ ist irreduzibel und normiert}\} \cup \{\infty\}.$$

Somit ist nun für den Körper $\mathbb{F}_q(T)$ eine geeignete Kurve gefunden.

4.3 Projektive ebene Kurven

Neben der projektiven Geraden sind in Zusammenhang mit Funktionenkörpern auch die projektiven ebenen Kurven von besonderer Bedeutung.
Dabei ist der *projektive n-dimensionale Raum* über einem Körper k definiert durch:

$$\mathbb{P}^n(k) := (k^{n+1} - \{(0, \ldots, 0)\})/(\text{Operation von } k^*).$$

Die Elemente des projektiven Raumes sind also Äquivalenzklassen. Haben die Punkte P und P' als Elemente des $(n+1)$-dimensionalen k-Vektorraumes die Koordinaten $(p_0, p_1, \ldots, p_n)$ bzw. $(p'_0, p'_1, \ldots, p'_n)$, so gilt:

$$P \sim P' \qquad \begin{cases} \text{genau dann, wenn ein } \lambda \in k^* \text{ existiert, so daß} \\ (p_0, p_1, \ldots, p_n) = \lambda(p'_0, p'_1, \ldots, p'_n) \text{ist.} \end{cases}$$

Diesem Umstand wird auch in der Notation Rechnung getragen, indem einem Punkt P des projektiven n-Raumes die Koordinaten $(p_0 : p_1 : \ldots : p_n)$ zugeordnet werden.

Eine etwas andere Definition einer projektiven Ebene $\mathbb{P}^2(k)$ kann wie folgt gegeben werden:
Sei $f(x, y)$ ein lineares Polynom. Dann ist $Z_f(k)$ die Menge der Punkte einer affinen Geraden, deren Koordinaten in k liegen. Ist $g \in k[x, y]$ ein anderes Polynom vom Grad eins, dann gilt:

(i) $Z_f(k) = Z_g(k)$ genau dann, wenn ein $\lambda \in k^*$ existiert mit $f(x, y) = \lambda \cdot g(x, y)$ für alle $(x, y) \in \mathbb{A}^2(k)$.

(ii) $Z_f(k) \cap Z_g(k) = \emptyset$ genau dann, wenn ein $\lambda \in k^*$ existiert mit

$$f(x, y) - \lambda \cdot g(x, y) \in k^* \text{ für alle } (x, y) \in \mathbb{A}^2(k).$$

(iii) Der Schnitt $Z_f(k) \cap Z_g(k)$ ist genau dann ein einziger Punkt, wenn kein $\lambda \in k^*$ existiert mit $f(x, y) - \lambda \cdot g(x, y) \in k$.

Nun wird die affine Ebene $\mathbb{A}^2(k)$ erweitert. Jede Ursprungsgerade L von $\mathbb{A}^2(k)$ wird durch Hinzunahme eines einzelnen Punktes, der ∞_L genannt wird, erweitert. Dann ist $\mathbb{P}^2(k)$, die Menge der Punkte der projektiven Ebene mit Koordinaten in k, gerade die Menge

$$\mathbb{P}^2(k) = \mathbb{A}^2(k) \cup \{\infty_L \mid L \text{ ist eine Ursprungsgerade von } \mathbb{A}^2(k)\}.$$

Definition 4.4. *Ein von Null verschiedenes Polynom $f \in k[x_0, x_1, \ldots, x_n]$ heißt* homogen vom Grad d, *wenn f von der Form*

$$f(x_0, x_1, \ldots, x_n) = \sum_{\substack{i_j \geq 0 \\ i_0 + i_1, \cdots + i_n = d}} c_{i_0, i_1, \ldots, i_n} x_0^{i_0}, x_1^{i_1}, \ldots, x_n^{i_n}$$

ist.
Für ein homogenes Polynom f wird die Menge $X_f(k)$ definiert als

$$X_f(k) := \{(a_0 : \ldots : a_n) \in \mathbb{P}^n(k) \mid f(a_0, \ldots, a_n) = 0\}.$$

Diese Menge ist wohldefiniert, denn, wenn $(a_0, \ldots, a_n)$ und $(a'_0, \ldots, a'_n)$ zwei verschiedene Repräsentanten derselben Klasse sind, es also ein $\lambda \in k^*$ gibt mit

$$(a_0, \ldots, a_n) = (\lambda a'_0, \ldots, \lambda a'_n),$$

so folgt daraus, daß

$$f(a_0, \ldots, a_n) = \lambda^d \cdot f(a'_0, \ldots, a'_n)$$

ist; insbesondere ist $(a_0, \ldots, a_n)$ genau dann eine Nullstelle von f, wenn $(a'_0, \ldots, a'_n)$ eine Nullstelle ist.

Definition 4.5. *Ist $f \in k[x_0, x_1, x_2]$ ein homogenes Polynom vom Grad d, dann heißt die Menge $X_f(\overline{k})$ eine* ebene projektive Kurve. *Die Menge $X_f(k)$ heißt die Menge der k*-rationalen Punkte *der projektiven Kurve, die durch f definiert ist. Das* Geschlecht der Kurve *ist das des Funktionenkörpers $\overline{k}(X_f)/\overline{k}$ (siehe* 4.10*).*

Definition 4.6. *Betrachten wir nun die Einbettung*

$$\begin{array}{rcl} \phi_2 : \mathbb{A}^2(\overline{k}) & \longrightarrow & \mathbb{P}^2(\overline{k}) \\ (a,b) & \mapsto & (a:b:1), \end{array}$$

so ist das Komplement des Bildes von $\mathbb{A}^2(\overline{k})$ in $\mathbb{P}^2(\overline{k})$ die Gerade $X_{x_2}(\overline{k})$. Sie wird die Gerade im Unendlichen *der Einbettung ϕ_2 genannt. Sei nun $\tilde{f} \in \overline{k}[x,y]$ ein irreduzibles Polynom vom Grad d. Dann ist das Bild der affinen Kurve $Z_{\tilde{f}}(\overline{k})$ unter der Abbildung ϕ_2 in der projektiven Kurve X_f enthalten, die durch das Polynom*

$$f(x_0, x_1, x_2) := x_2^d \cdot \tilde{f}(x_0/x_2, x_1/x_2)$$

definiert wird. Die Punkte von $\mathbb{P}^2(\overline{k})$ der Form $(c_0 : c_1 : 0)$ mit $f(c_0, c_1, 0) = 0$ heißen Punkte im Unendlichen der affinen Kurve $Z_{\tilde{f}}(\overline{k})$.

Im folgenden beschränken wir unsere Betrachtungen auf die projektive Ebene.

Definition 4.7. *Sei f ein homogenes Polynom vom Grad d. Jede partielle Ableitung $\frac{\partial f}{\partial x_i}(x_0, x_1, x_2)$ ist ein homogenes Polynom vom Grad $d-1$. Ein Punkt $(a : b : c)$ der projektiven Kurve $X_f(\overline{k})$ heißt* nichtsingulär, *wenn*

$$\mathit{grad}(f)(a,b,c) := \left(\frac{\partial f}{\partial x_0}(a,b,c), \frac{\partial f}{\partial x_1}(a,b,c), \frac{\partial f}{\partial x_2}(a,b,c) \right) \neq (0,0,0)$$

ist.

Bemerkung 4.8. Wir skizzieren kurz den Zusammenhang mit der Nichtsingularität aus Abschnitt 4.1.
Dazu betrachten wir zu f die Dehomogenisierung $f_i(x,y)$, die sich aus

$$x_i^d \, f_i(x_j/x_i, x_k/x_i) = f(x_0, x_1, x_2),$$

ergibt, wobei $i = 0, 1, 2$ und $j < k$ sowie $j, k \neq i$ sind. Wir definieren

$$U_i := X_f(\overline{k}) \cap (\mathbb{P}^2 - X_{x_i}(\overline{k})).$$

Dann gilt für einen Punkt $P = (c_0 : c_1 : c_2) \in U_i$ die folgende Äquivalenz: P ist ein nicht-singulärer Punkt von $X_f(\overline{k})$ genau dann, wenn der Punkt $(c_j/c_i, c_k/c_i)$ mit $j < k$ und $j, k \neq i$ ein nicht-singulärer Punkt der affinen Kurve $Z_{f_i}(\overline{k})$ ist.

Definition 4.9. *Sei f ein homogenes, irreduzibles Polynom. Der Körper L' sei der Quotientenkörper des Ringes $k[x_0, x_1, x_2]/(f)$. Des weiteren sei*

$$k(X_f) := \left\{ \frac{\textit{Klasse von } g}{\textit{Klasse von } h} \in L' \;\middle|\; \begin{array}{l} g(x_0,x_1,x_2) \textit{ und } h(x_0,x_1,x_2) \textit{ sind homogene} \\ \textit{Polynome gleichen Grades in } k[x_0,x_1,x_2] \end{array} \right\}.$$

Diese Menge ist ein Teilkörper von L'.

Definition 4.10. *Sei $f \in \overline{k}[x_0, x_1, x_2]$ ein irreduzibles Polynom, das die projektive Kurve $X_f(\overline{k})$ definiert. Der Körper $\overline{k}(X_f)$ ist der* Körper der rationalen Funktionen *von $X_f(\overline{k})$. Ein Element ψ von $\overline{k}(X_f)$ heißt rationale Funktion. ψ ist in $P = (p_0 : p_1 : p_2) \in X_f(\overline{k})$ definiert, falls $\psi = \frac{g}{h}$ sowie g und h vom gleichen Grad und zueinander teilerfremd sind und $h(p_0 : p_1 : p_2) \neq 0$ ist.*
Für einen Punkt $P = (p_0 : p_1 : p_2) \in X_f(\overline{k})$ sei

$$\mathcal{O}_P := \{\psi \in \overline{k}(X_f) \mid \psi \textit{ ist definiert in } P\}.$$

Die Menge $\mathcal{O}_P$ ist ein lokaler Ring, dessen maximales Ideal $\mathfrak{m}_P$ alle rationalen Funktionen enthält, die in P verschwinden. Ein Punkt $P \in X_f(\overline{k})$ ist genau dann nicht singulär, wenn der Ring $\mathcal{O}_P$ ein lokaler Hauptidealring ist, der kein Körper ist.
Darüber hinaus gilt der folgende Satz:

Satz 4.11. *Vorausgesetzt die ebene projektive Kurve $X_f(\overline{k})$ ist vollständig und nichtsingulär. Mit $\mathcal{P}(\overline{k}(X_f)/\overline{k})$ sei die Menge aller lokalen Hauptidealringe $\mathcal{O} \subset \overline{k}(X_f)$, die ein echtes Ideal enthalten, bezeichnet. Dann sind die beiden Abbildungen*

$$\begin{array}{ccccc} X_f(\overline{k}) & \longrightarrow & \mathcal{V}(\overline{k}(X_f)/\overline{k}) & \longrightarrow & \mathcal{P}(\overline{k}(X_f)/\overline{k}) \\ P & \mapsto & v_P & \mapsto & \mathcal{O}_P \end{array}$$

bijektiv.

Beweis: siehe [Lor97, S.217]

4.4 Rationale Punkte

Für eine Zwischenerweiterung $k \subset F \subset \overline{k}$ läßt sich die Menge der F-rationalen Punkte $X_f(F)$ mit Hilfe der Galoisgruppe $G(\overline{k}/F)$ bestimmen. Dazu betrachtet man unter der Operation

$$\sigma(P) = (\sigma(p_0) : \sigma(p_1) : \sigma(p_2)) \qquad \text{für alle } \sigma \in G(\overline{k}/F)$$

der Gruppe $G(\overline{k}/F)$ den Stabilisator von P

$$\mathrm{Stab}(P) = \{\sigma \in G(\overline{k}/F) \mid \sigma(P) = P\}$$

und erhält den Körper

$$k(P) := \{c \in \overline{k} \mid \sigma(c) = c, \text{ für alle } \sigma \in \mathrm{Stab}(P)\}.$$

Die Menge

$$X_f(F) = \{P \in X_f(\overline{k}) \mid k(P) \subset F\}$$

heißt die Menge der *F-rationalen Punkte der Kurve X_f/k.*

Bemerkung 4.12. Der Grad eines Punktes P ist definiert durch

$$deg\, P = [k(P) : k]$$

und entspricht dem Grad $deg\, \mathfrak{P}$ des zugehörigen Primdivisors $\mathfrak{P}$. Die Menge der k-rationalen Punkte der Kurve $X_f(\overline{k})$ ist also gleich der Menge der Primdivisoren vom Grad eins.

Insbesondere sind wir an der Zahl der Elemente in $X_f(F)$ interessiert. Sei für $F = \mathbb{F}_{q^n}$ die Mächtigkeit der Menge $X_f(F)$ mit $\mathcal{N}(X_f(F))$ bezeichnet. Dann besagt ein Resultat von Weil, das auf der Riemannschen Vermutung im Fall der Funktionenkörper über einem endlichen Körper beruht, daß sich diese Zahl in Abhängigkeit vom Geschlecht g der Kurve abschätzen läßt. Diese Abschätzung konnte Serre etwas verbessern. In dieser verbesserten Form führe ich sie hier an:

$$|\mathcal{N}(X_f(F)) - (q^n + 1)| \leq g[2\sqrt{q^n}]$$

(siehe dazu auch [Sti93, S. 180]).

4.5 Projektive Transformationen

Die Automorphismen der projektiven Gerade $\mathbb{P}^1$ lassen sich mit Hilfe der regulären 2×2-Matrizen über k beschreiben, denn es gilt:

$$\mathrm{Aut}\, \mathbb{P}^1 \cong Gl(2, k)/k^* E,$$

wobei E die Einheitsmatrix ist.

Beweis: : [Hum91, S. 48]

Charakterisieren läßt sich jeder Automorphismus von $\mathbb{P}^1$ durch seine Wirkung auf das Trippel $((0:1), (1:1), (1:0)) =: (0, 1, \infty)$.

Beispiel 4.13. Sind $x = (x_1 : x_2)$ und $y = (y_1 : y_2)$ zwei Punkte, die verschieden und nicht ∞ sind, so kann das Trippel (x, y, ∞) mittels eines Automorphismus in $(0, 1, \infty)$ transformiert werden. Dazu wählen wir die Matrix

$$A := \begin{pmatrix} x_1 & x_2 \\ 0 & 1 \end{pmatrix}.$$

Dann bildet der zugeordente Automorphismus φ_A die Elemente x und y ab auf

$$x \mapsto (0:1), \quad y \mapsto (x_2y_1 - x_1y_2 : y_2) \quad \text{und} \quad \infty \mapsto \infty.$$

Der Automorphismus φ_B mit

$$B := \begin{pmatrix} (x_2y_1 - x_1y_2)^{-1} & 0 \\ 0 & y_2^{-1} \end{pmatrix}$$

transformiert $\varphi_A(y)$ in 1 und läßt 0 und ∞ fest. Die Hintereinanderausführung beider leistet nun das Gewünschte.

Sei mit $Gl(3, k)$ die Menge der k-linearen Automorphismen von k^3 bezeichnet. Dann induziert jedes Element $A = (a_{i,j})_{0 \leq i,j \leq 2} \in Gl(3, k)$ in der projektiven Ebene $\mathbb{P}^2(k)$ einen *Koordinatenwechsel*

$$\begin{array}{rcl} \phi_A : \mathbb{P}^2(k) & \longrightarrow & \mathbb{P}^2(k) \\ (p_0 : p_1 : p_2) & \mapsto & \left(\sum_{j=0}^{2} a_{0,j} \cdot p_j \; : \sum_{j=0}^{2} a_{1,j} \cdot p_j \; : \sum_{j=0}^{2} a_{2,j} \cdot p_j \right). \end{array}$$

Transformationen dieser Art erhalten zentrale Eigenschaften der projektiven Kurve, denn es gilt:

Lemma 4.14. *(i) Die Abbildung ϕ_A ist bijektiv.*

(ii) Die Gruppe $Gl(3, k)$ operiert auf $\mathbb{P}^2(k)$ vermittels $\phi_A \cdot P := \phi_A(P)$. Auf der Menge der Tripel von Punkten, die nicht colinear sind, operiert die Gruppe transitiv.

(iii) Sei $X_f(k)$ eine projektive, ebene Kurve. Dann induziert die Abbildung ϕ_A eine Bijektion $\phi_A : X_f(k) \to \phi_A(X_f(k))$. Die Menge $\phi_A(X_f(k))$ ist gleich der Menge der Punkte von $X_{f \circ \phi_A^{-1}}(k)$, also der durch das homogene Polynom

$$(f \circ \phi_A^{-1})(x_0, x_1, x_2) := f \left(\sum_{j=0}^{2} b_{0,j} \cdot x_j \; : \sum_{j=0}^{2} b_{1,j} \cdot x_j \; : \sum_{j=0}^{2} b_{2,j} \cdot x_j \right),$$

wobei $A^{-1} = (b_{i,j})_{0 \leq i,j \leq 2}$ ist. Insbesondere haben f und $f \circ \phi_A^{-1}$ den gleichen Grad.

(iv) Ein Punkt $P \in X_f(\overline{k})$ *ist nichtsingulär genau dann, wenn der Punkt* $\phi_A(P)$ *ein nichtsingulärer Punkt von* $X_{f\circ\phi_A^{-1}}(\overline{k})$ *ist.*

(v) ϕ_A *induziert nun weitere Abbildungen, nämlich*

$$\begin{array}{llccc}
\phi : X_f(\overline{k}) & \longrightarrow X_{f\circ\phi^{-1}}(\overline{k}) & \textit{mit} & P \mapsto & \phi(P), \\
\tilde{\phi} : \overline{k}(X_{f\circ\phi^{-1}}) & \longrightarrow \overline{k}(X_f) & \textit{mit} & \frac{\textit{Klasse von } g}{\textit{Klasse von } h} \mapsto & \frac{\textit{Klasse von } g\circ\phi}{\textit{Klasse von } h\circ\phi}, \\
\phi_{\mathcal{O}} : \mathcal{P}(\overline{k}(X_f/\overline{k})) & \longrightarrow \mathcal{P}(\overline{k}(X_{f\circ\phi^{-1}}/\overline{k})) & \textit{mit} & \mathcal{O} \mapsto & (\tilde{\phi})^{-1}(\mathcal{O}), \\
\phi_v : \mathcal{V}(\overline{k}(X_f)/\overline{k}) & \longrightarrow \mathcal{V}(\overline{k}(X_{f\circ\phi^{-1}})/\overline{k}) & \textit{mit} & v \mapsto & v\circ\tilde{\phi}.
\end{array}$$

Jede dieser Abbildungen ist bijektiv, und das daraus resultierende Diagramm

$$\begin{tikzcd}
X_f(\overline{k}) \arrow[r] \arrow[d, "\phi"] & \mathcal{P}(\overline{k}(X_f/\overline{k})) \arrow[r] \arrow[d, "\phi_{\mathcal{O}}"] & \mathcal{V}(\overline{k}(X_f)/\overline{k}) \arrow[d, "\phi_v"] \\
X_{f\circ\phi^{-1}}(\overline{k}) \arrow[r] & \mathcal{P}(\overline{k}(X_{f\circ\phi^{-1}}/\overline{k})) \arrow[r] & \mathcal{V}(\overline{k}(X_{f\circ\phi^{-1}})/\overline{k})
\end{tikzcd}$$

ist kommutativ.

Gewisse "Typen" von Kurven lassen sich also ineinander überführen, ohne daß sich dabei die Nichtsingularität wesentlich verändert.

Kapitel 5

Der Carlitz–Modul

In diesem Kapitel gebe ich eine kurze Beschreibung der Drinfeld–Moduln, um den dann zu betrachtenden Carlitz–Modul ρ in den theoretischen Kontext einzubetten. In Abschnitt 3 wird zudem eine rekursive Definition für ρ_n gegeben, die es ermöglicht, die Kapitel 6 und 7 auch ohne die beiden ersten Abschnitte dieses Kapitels zu verfolgen.

5.1 Der Ring $k\{\tau\}$

Definition 5.1. *Sei k ein Körper. Ein Polynom $f(X) \in k[X]$ heißt (absolut)* additiv *genau dann, wenn für alle Elemente $a, b \in \overline{k}$ gilt:*

$$f(a+b) = f(a) + f(b).$$

Direkt aus der Definition ergibt sich:

Proposition 5.2. *Ein Polynom $f(X) \in k[X]$ ist additiv genau dann, wenn*

$$\begin{cases} f(X) = \; const \cdot X, & falls \quad char\, k = 0 \\ f(X) = \sum\limits_{i=0}^{d} a_i X^{l^i}, \; a_i \in k, & falls \quad char\, k = l \neq 0 \text{ ist.} \end{cases}$$

Seien $f(X)$, $g(X) \in k[X]$ zwei additive Polynome und $a \in k$, dann sind

$$f(X) + g(X), \qquad a \cdot f(X) \quad und \quad f(g(X))$$

ebenfalls additiv.

Sei nun k ein Körper der Charakteristik $l \neq 0$, der den Körper $\mathbb{F}_q$, $q = l^v$, enthält. $\overline{k}$ sei ein fixierter algebraischer Abschluß von k. Für jede Erweiterung $k' \subset \overline{k}$ von k wird die *additive Gruppe* mit $\mathbb{G}_a(k') := (k', +)$ bezeichnet.
Dann ist

$$End_k(\mathbb{G}_a(k)) = \{f(X) \in k[X] \mid f(X) \text{ ist additiv}\}.$$

Definition 5.3. *Ein Polynom $f(X) \in k[X]$ heißt* $\mathbb{F}_q$-linear *genau dann, wenn $f(X)$ additiv ist und für alle $a \in \mathbb{F}_q$ gilt*

$$f(aX) = a \cdot f(X).$$

Lemma 5.4. *(i) Ein Polynom $f(X) \in k[X]$ ist genau dann $\mathbb{F}_q$-linear, wenn $f(X)$ von der Form*

$$f(X) = \sum_{i=0}^{d} a_i X^{q^i} \quad \textit{mit } a_i \in k \qquad \textit{ist.}$$

(ii) Ist $f(X) \in k[X]$ ein $\mathbb{F}_q$-lineares Polynom, so ist der Kern $ker(f)$ ein $\mathbb{F}_q$-Untervektorraum von k.

(iii) Ist $H \subset k$ ein endlich dimensionaler $\mathbb{F}_q$-Untervektorraum, so ist das Polynom

$$f_H(X) := \prod_{h \in H} (X - h)$$

$\mathbb{F}_q$-linear.

Wir setzen nun $\tau := X^q \in End_k(\mathbb{G}_a(k))$ und erhalten entsprechend für τ^i

$$\underbrace{\tau \circ \tau \circ \ldots \circ \tau}_{i \text{ Faktoren}} = X^{q^i} \quad \text{und insbesondere} \quad \tau^0 = X^{q^0} = X.$$

Satz 5.5. *Die Menge*

$$k\{\tau\} := \{\sum_{i=0}^{d} a_i \tau^i \mid d \in \mathbb{N},\ a_i \in k\}$$

ist mit den Verknüpfungen

(i) der komponentenweisen Addition und

(ii) der Multiplikation, definiert durch die Hintereinanderausführung von Polynomen:

$$\left(\sum_{i=0}^{d} a_i \tau^i\right) \cdot \left(\sum_{j=0}^{d} b_j \tau^j\right) = \sum_{k=0}^{d+d'} \left(\sum_{i+j=k} a_i\, b_j^{q^i}\right) \tau^k,$$

ein nichtkommutativer Ring mit Einselement.

Arithmetik in $k\{\tau\}$
Für ein Polynom

$$f = \sum_{i=0}^{d} a_i \tau^i \ \in k\{\tau\} \quad \text{mit } a_d \neq 0$$

wird $\quad D(f) = a_0, \quad deg_\tau f := d, \quad$ wobei $\quad deg_\tau 0 := -\infty \quad$ ist, gesetzt.
$f(\tau) \in k\{\tau\}$ heißt normiert genau dann, wenn $f(X) \in k[X]$ normiert ist.

Bemerkung 5.6. Die parallele Verwendung von $f(X)$ und $f(\tau)$ suggeriert, es handle sich hier um einen einfachen Einsetzungshomomorphismus, tatsächlich aber ist τ ein k-Endomorphismus über $\mathbb{G}_a(k)$.

Es gilt:

(i) $k\{\tau\}$ ist eine $\mathbb{F}_q$-Algebra $\mathbb{F}_q$-linearer Polynome.

(ii) $k\{\tau\}$ ist nullteilerfrei und $(k\{\tau\})^* = k^*$.

(iii) $deg\, f(X) = q^{deg_\tau(f(\tau))}$.

(iv) Für alle $f, g \in k\{\tau\}$ ist

$$deg_\tau(f+g) \leq deg_\tau(f) + deg_\tau(g), \quad deg_\tau(f \cdot g) = deg_\tau(f) \cdot deg_\tau(g),$$

$$D(f+g) = D(f) + D(g) \quad \text{und} \quad D(f \cdot g) = D(f) \cdot D(g).$$

Zusammenhang zwischen $k[X]$ und $k\{\tau\}$

(i) Für alle $f(X) \in k[X]$ existiert ein $g(\tau) \in k\{\tau\}$, so daß $g(X)$ von $f(X)$ geteilt wird.
(Beweis: siehe [Gos96, S.9])

(ii) Für alle $f(\tau), g(\tau) \in k\{\tau\}$ gilt:
ist $f(\tau) = h(\tau) \circ g(\tau)$ für ein $h(\tau) \in k\{\tau\}$, dann folgt daraus, daß $g(X) | f(X)$ in $k[X]$.
(Beweis: siehe [Gek97])

5.2 Drinfeld–Moduln

Bezeichnung 5.7. Mit A wird der Polynomring in einer Variablen, $\mathbb{F}_q[T]$, bezeichnet, der Quotientenkörper von A mit K. Es ist K_∞ die Vervollständigung von K bezüglich der ∞-Bewertung, C die Vervollständigung des algebraischen Abschlusses von K_∞.

Sei L eine endliche, separable Erweiterung von K und $\mathcal{O}$ der ganze Abschluß von A in L, also anschaulich:

$$\begin{tikzcd}
\mathcal{O} \arrow[r, hook] \arrow[d, dash] & L \arrow[d, dash] \\
A \arrow[r, hook] & K
\end{tikzcd} .$$

Definition 5.8. *Ein* $\mathcal{O}$-Körper k *ist ein Körper* k *versehen mit einem Ringhomomorphismus*

$$\gamma : \mathcal{O} \longrightarrow k.$$

Unter der $\mathcal{O}$*-Charakteristik des* $\mathcal{O}$*-Körpers* k *versteht man*

$$\begin{array}{llll} char_{\mathcal{O}}\, k := \infty, & \text{falls} & ker\,(\gamma) = \{0\} & \text{bzw.} \\ char_{\mathcal{O}}\, k := \mathfrak{p}, & \text{falls} & ker\,(\gamma) = \mathfrak{p} \neq \{0\} & \text{ist.} \end{array}$$

Dabei wird für $char_{\mathcal{O}}\, k = \infty$ *der Ausdruck* $(\mathfrak{a}, char_{\mathcal{O}}\, k) := 1$ *für alle* $\mathfrak{a} \subset \mathcal{O}$ *gesetzt.*

Zur Einführung der Drinfeld–Moduln betrachten wir nun die Ringhomomorphismen

$$\begin{array}{rcl} \phi : \mathcal{O} & \longrightarrow & k\{\tau\} \\ a & \mapsto & \phi_a \end{array}$$

mit den folgenden Eigenschaften:

(i) ϕ ist $\mathbb{F}_q$-linear, das heißt, für alle $c \in \mathbb{F}_q$ gilt: $\phi_{ca} = c \cdot \phi_a$,

(ii) $D \circ \phi = \gamma$ und

(iii) $\phi \neq \gamma$, es existiert also ein $a \in \mathcal{O}$ mit $\phi_a - \gamma(a) \neq 0$.

Proposition 5.9. *Ist* ϕ *wie oben beschrieben gegeben, so existiert ein* $r \in \mathbb{Q}$ *derart, daß für alle* $a \in \mathcal{O}$ *gilt:*

$$deg_{\tau}\phi_a = r \cdot deg\, a.$$

Beweis: siehe [Gek97].

Definition 5.10. *Ein* Drinfeld $\mathcal{O}$-Modul über k *ist eine* $\mathcal{O}$*-Modulstruktur auf* $\mathbb{G}_a(k)$*, vermittelt durch einen Ringhomomorphismus*

$$\begin{array}{rcl} \phi : \mathcal{O} & \longrightarrow & k\{\tau\} \\ a & \mapsto & \phi_a, \end{array}$$

der (i) bis (iii) genügt.
Die Zahl $r =:$ *Rang* $(\phi) \in \mathbb{Q}$ *aus* 5.9 *heißt der* Rang des Drinfeld–Moduls ϕ.
Ist L/k *eine Erweiterung von* k *und* $x \in L$*, so operiert* a *auf* x *durch*

$$a \underset{\phi}{*} x := \phi_a(x) = \gamma(a)x + g_1 x^q + \ldots + g_n x^{q^n},$$

mit $n \in \mathbb{N}$ *und* $g_i \in k$ *für alle* $i = 1, \ldots, n$.
Sei $a \in \mathcal{O}$*. Ein* $x \in \overline{k}$ *mit*

$$a \underset{\phi}{*} x = 0$$

heißt ein a-Torsionspunkt *oder* a-Teilungspunkt von ϕ*. Die Menge*

$${}_a\phi\ (k') := \{x \in k' \mid \phi_a(x) = 0\} \quad \textit{für} \quad k \subset k' \subset \overline{k}$$

heißt der Modul der k'-wertigen a-Teilungspunkte*.*
Ist $\mathfrak{a}$ *ein Ideal, so sei*

$${}_{\mathfrak{a}}\phi\ := \bigcap_{a \in \mathfrak{a}} {}_a\phi\ .$$

Bemerkung 5.11. (i) Die Verknüpfungsvorschrift $a \underset{\phi}{*} x$ für $a \in \mathcal{O}$ und $x \in k'$, wobei $k \subset k' \subset \overline{k}$ sein soll, macht jede additive Gruppe $(k', +) = \mathbb{G}_a(k')$ zu einem $\mathcal{O}$-Modul (k', ϕ), und es ist $(k', \phi) \subset (k'', \phi)$, falls $k \subset k' \subset k'' \subset \overline{k}$ ist.

(ii) Sei $\mathfrak{a} = (a)$ ein Hauptideal.

(a) Es ist ${}_{\mathfrak{a}}\phi\ = {}_a\phi\ .$

(b) Jedes ${}_a\phi\ $ ist sogar ein $(\mathcal{O}/\mathfrak{a})$-Modul.

(c) Für alle Erweiterungen k'/k und für alle $\mathfrak{a} \neq \{0\}$ ist ${}_{\mathfrak{a}}\phi\ (k')$ endlich.

(d) Ist $a \in \mathcal{O}$ mit ggT $(\mathfrak{a}, char_{\mathcal{O}}(k)) = 1$, so ist $\phi_a(X) \in k[X]$ separabel.

Beispiel 5.12. Sei $\mathcal{O} = \mathbb{F}_3[T, Y]$ und $Y^2 = -T^2 + T$.
Ein Drinfeld–Modul über $\overline{L}$, dem algebraischen Abschluß von $L =$ *Quot* $(\mathcal{O})$, ist gegeben durch ϕ_T und ϕ_Y mit

$$(\phi_Y)^2 = -(\phi_T)^2 + \phi_T \quad \text{in } \overline{L}\{\tau\}.$$

Der Ansatz

$$\begin{aligned}\phi_T &= T + a\tau + b\tau^2,\\ \phi_Y &= Y + c\tau + d\tau^2\end{aligned}$$

mit $a, b, c, d \in \mathcal{O}$ führt durch Koeffizientenvergleich auf das Gleichungssystem

$$\begin{aligned}c(Y + Y^q) &= a(1 - T - T^q)\\ c^{q+1} + d(Y + Y^{q^2}) &= -a^{q+1} + b(1 - T - T^{q^2})\\ cd^q + c^{q^2}d &= -(ab^q + a^{q^2}b)\\ d^{q^2+1} &= -b^{q^2+1}\end{aligned}$$

und mit $\varepsilon^2 := -1$, $\eta := 1 + T + \varepsilon Y$ auf die Lösungen

$$\begin{aligned}a &= \varepsilon Y, & c &= \eta(1 + T),\\ b &= 1 + T - \varepsilon Y, & d &= \eta(1 + T - \varepsilon Y).\end{aligned}$$

Satz 5.13. *Sei ϕ ein Drinfeld–Modul über k, $\{0\} \neq \mathfrak{a}$ ein Ideal von $\mathcal{O}$ und $r = Rang(\phi)$. Für den $\mathcal{O}$-Modul ${}_{\mathfrak{a}}\phi\ (\overline{k})$ gilt:*

(i) Falls $\mathrm{ggT}(\mathfrak{a}, char_{\mathcal{O}}(k)) = 1$ ist, dann ist ${}_{\mathfrak{a}}\phi\ (\overline{k})$ frei über $\mathcal{O}/\mathfrak{a}$ vom Rang r. Insbesondere ist $r \in \mathbb{N}$.

(ii) Ist $\{0\} \neq \mathfrak{p} = char_{\mathcal{O}}(k)$, so existiert ein $h \in \mathbb{Z}$, $1 \leq h \leq r$, so daß gilt: für alle $\mathfrak{a}$ von der Form $\mathfrak{a} = \mathfrak{p}^e$ mit $e \in \mathbb{N}$ ist ${}_{\mathfrak{a}}\phi\ (\overline{k})$ vom Rang $r - h$. In diesem Fall heißt h die Höhe von ϕ.

Beweis: siehe [Gek97].

Korollar 5.14. *Sei die Situation wie in 5.13 und $0 \neq \mathfrak{a} \subset \mathcal{O}$ ein Ideal mit $\mathrm{ggT}(\mathfrak{a}, char_{\mathcal{O}}(k)) = 1$. Dann ist die Erweiterung $k({}_{\mathfrak{a}}\phi\ )/k$ galoissch, und die Galoisgruppe $G(k({}_{\mathfrak{a}}\phi\ )/k)$ bettet sich vermöge*

$$\begin{aligned}G(k({}_{\mathfrak{a}}\phi\ )/k) &\longrightarrow Aut_{A/\mathfrak{a}}({}_{\mathfrak{a}}\phi\ ) \cong Gl(r, A/\mathfrak{a})\\ \sigma &\mapsto \sigma|_{{}_{\mathfrak{a}}\phi}\end{aligned}$$

in die Gruppe der invertierbaren Matrizen $Gl(r, \mathcal{O}/\mathfrak{a})$ mit $r = Rang(\phi)$ ein.

Beweis: siehe [Gek97].

5.3 Der Carlitz–Modul

Das klassische und zugleich "einfachste" Beispiel eines Drinfeld–Moduls ist der Carlitz–Modul. Er ist gegeben durch:

Definition 5.15. *Der Drinfeld A-Modul über K vom Rang* 1 *vermittelt durch den Ringhomomorphismus*

$$\begin{array}{rcll} \rho : A & \longrightarrow & K\{\tau\} & \\ T & \mapsto & \rho_T(\tau) := T + \tau & \textit{wobei} \\ & & \rho_T(X) = TX + X^q & \textit{und} \\ & & \gamma = id : A \hookrightarrow K & \textit{ist,} \end{array}$$

heißt Carlitz–Modul.

Bemerkung 5.16. Der Carlitz–Modul läßt sich auch mit Hilfe der Rechenregeln beschreiben:

(i) $\rho_T(X) = TX + X^q$,

(ii) $\rho_{T^i}(X) = \rho_T(\rho_{T^{i-1}}(X))$,

(iii) $\rho_{a+b}(X) = \rho_a(X) + \rho_b(X)$ mit $a, b \in A$ und

(iv) für alle $c \in \mathbb{F}_q$ ist $\rho_{cT^i}(X) = c \cdot \rho_{T^i}(X)$.

Wir verdeutlichen uns diese Rekursion an einem Beispiel.

Beispiel 5.17. Sei $c \in \mathbb{F}_q^*$. Dann ist

$$\begin{aligned} \rho_{T^2-c}(X) &= \rho_{T^2}(X) - \rho_c(X) \\ &= T^2X + (T + T^q)X^q + X^{q^2} - cX \\ &= (T^2 - c)X + (T + T^q)X^q + X^{q^2}. \end{aligned}$$

Seien $c_1, c_2 \in \mathbb{F}_q^*$, so ist

$$\rho_{(T-c_1)(T-c_2)}(X) = (T^2 - (c_1 + c_2)T + c_1c_2)X + (T + T^q - (c_1 + c_2))X^q + X^{q^2},$$

insbesondere ist für $T^2 - c = (T - c_1)(T - c_2)$

$$\rho_{T^2-c}(X) = f(X)\frac{\rho_{T-c_1}(X)}{X}\frac{\rho_{T-c_2}(X)}{X} \cdot X \quad \text{mit} \quad deg\, f(X) = q^2 - 2q + 1.$$

Proposition 5.18. *Ist $n \in A$ ein Polynom vom Grad $deg\, n = d$, so ist*

$$\rho_n(x) = \sum_{i=0}^{d} f_i(T) \cdot X^{q^i},$$

wobei jedes $f_i(T)$ ein Polynom aus A vom Grad $(d - i)q^i$ ist. Zudem ist $f_0(T) = n(T)$ und $f_d(T)$ ist der Leitkoeffizient von n.

Beweis: siehe [Hay74].

Bezeichnung 5.19. Sei $n \in A$ ein normiertes Polynom und

$$n = \prod_{\nu=1}^{s} p_\nu^{r_\nu}$$

wobei $s, r_\nu \in \mathbb{N}$ und $p_\nu \in A$ irreduzibel und normiert sind, die Zerlegung von n in irreduzible Faktoren.
Zur Bezeichnung der n-Torsionselemente von ρ verwende ich die abkürzende Schreibweise

$${}_n\rho \ := {}_n\rho\ (C)$$

und für den Zerfällungskörper in C von $\rho_n(X)$

$$K(n) := K({}_n\rho\ ).$$

Die multiplikative Gruppe des Ringes $A/(n)$ wird wie üblich $(A/(n))^*$ genannt.

Das Korollar zu Satz 5.13 sagt aus, daß die Erweiterung $K(n)/K$ eine abelsche Galoiserweiterung ist, deren Galoisgruppe sich in $(A/(n))^*$ einbetten läßt.

Darüber hinaus gilt der für meine Arbeit zentrale Satz:

Satz 5.20. *(i) Die Körpererweiterung $K(n)/K$ ist galoissch mit Galoisgruppe $(A/(n))^*$.*

(ii) Ist $n = p^r$ ein primäres Polynom, so ist die Erweiterung $K(n)/K$ vollverzweigt in $\mathfrak{p} = (p)$ und unverzweigt in allen anderen endlichen Stellen $\mathfrak{q} \neq \mathfrak{p}$, $\mathfrak{q} \neq \infty$.

(iii) Sei $K_+(n)$ der Fixkörper der Einbettung $\mathbb{F}_q^* \hookrightarrow (A/(n))^*$, also:

$$(A/(n))^* \left\{ \begin{array}{c} \left.\begin{array}{c} K(n) \\ | \\ K_+(n) \end{array}\right\} \mathbb{F}_q^* \\ | \\ K \end{array}\right. .$$

Dann ist die ∞-Stelle in $K_+(n)$ voll zerlegt, und jede über der ∞-Stelle von K liegende Stelle in $K_+(n)$ ist voll verzweigt in der Erweiterung $K(n)/K_+(n)$.

(iv) Sei n das Produkt von s primären Faktoren in A. Dann ist $K(n)$ das Kompositum der Körper $K(p_\nu^{r_\nu})$, $\nu = 1, \ldots, s$, und alle $K(p_\nu^{r_\nu})$ sind zueinander linear disjunkt.

(v) Sei $\mathcal{O}(n)$ der ganze Abschluß von A in $K(n)$ und $\lambda \in {}_n\rho$ ein primitiver n-Teilungspunkt von ρ. Dann ist

$$\mathcal{O}(n) = A[\lambda].$$

Bemerkung 5.21. Der Satz zeigt, daß die Erweiterungen des rationalen Funktionenkörpers, die aus der Adjunktion der n-Teilungspunkte eines Carlitz–Moduls hevorgehen, sehr viele der Eigenschaften der Kreisteilungserweiterungen des Körpers $\mathbb{Q}$ haben. Sie werden daher auch *Kreisteilungserweiterungen des rationalen Funktionenkörpers* genannt. Dem Körper $K_+(n)$ entspricht im Zahlkörperfall die maximale reelle Erweiterung von $\mathbb{Q}$, die in der Kreisteilungserweiterung enthalten ist. Der Ganzheitsring $\mathcal{O}(n)$ läßt sich mit dem Ring $\mathbb{Z}[\zeta_m]$ vergleichen, wobei ζ_m eine primitive m-te Einheitswurzel ist.

Beweis: Wir zeigen zunächst den Teil (ii), da sich daraus der Teil (iv) direkt und mit einer kleinen Ergänzung der Teil (i) folgern läßt.
Sei p ein irreduzibles Polynom vom Grad $deg\, p = d$ und $d \in \mathbb{N}$. Dann ist

$$\rho_{p^r}(X) = \prod_{\lambda \in_{p^r} \rho} (X - \lambda).$$

Der ganze Abschluß von A in $K(p^r)$ ist, da A ein Dedekindring ist, wiederum ein Dedekindring. Um jene endlichen Stellen zu bestimmen, die in der Erweiterung $K(p^r)/K$ verzweigen, genügt es zu ermitteln, welche Primideale von A die Diskriminante $D_{\mathcal{O}(p^r)/A}$ von $\mathcal{O}(p^r)$ über A teilen.

Sei $\lambda_0 \in {}_{p^r}\rho$ ein primitiver p^r-Teilungspunkt. Dann ist der Ring $A[\lambda_0]$ ein Unterring von $\mathcal{O}(p^r)$. Die Primteiler $\mathfrak{q}$ der Diskriminante $D_{A[\lambda_0]/A}$ sind diejenigen Primideale von A, die in $K(p^r)/K$ verzweigen oder für die gilt:

$$A[\lambda_0]_{(\mathfrak{q})} \subsetneq \mathcal{O}(p^r)_{(\mathfrak{Q})}$$

mit $\mathfrak{Q}|\mathfrak{q}$. Falls nun $f \in A[X]$ ein Polynom ist mit $f(\lambda_0) = 0$, so gilt:

$$D_{A[\lambda_0]/A} \mid N_K^{K(p^r)}(f'(\lambda_0)).$$

Wählen wir nun $f(X) = \rho_{p^r}(X)$, dann ist $f'(X) = \frac{d}{dX}\rho_{p^r}(X) = p^r$. Somit ist $(p) := \mathfrak{p}$ das einzige Primideal von A, das die Diskriminante $D_{A[\lambda_0]/A}$ teilt. Da aber $D_{\mathcal{O}(p^r)/A}$ ein Teiler von $D_{A[\lambda_0]/A}$ ist, ist $\mathfrak{p}$, abgesehen von der ∞-Stelle, über die hier keine Aussage gemacht wird, die einzige verzweigte Stelle in $K(p^r)/K$.

Sei nun

$$f_{p^r}(X) := \frac{\rho_{p^r}(X)}{\rho_{p^{r-1}}(X)} = \prod_{\substack{\lambda \in {}_{p^r}\rho \\ \lambda \text{ prim.TP.}}} (X - \lambda),$$

wobei λ alle primitiven p^r-Torsionspunkte durchläuft.
Setze $q^d := |p|$.
Dann ist der Grad von ρ_p gerade $|p|$, und der Grad von $f_{p^r}(X) \in A[X]$ ist

$$\begin{aligned} deg\,(f_{p^r}(X)) &= deg\,(\rho_{p^r}(X)) - deg\,(\rho_{p^{r-1}}(X)) \\ &= |p|^r - |p|^{r-1} = |p|^{r-1}(|p| - 1) \\ &= |\,(A/(p^r))^*| = |G(K(p^r)/K)|. \end{aligned}$$

Die Galoisgruppe von $K(p^r)/K$ ist also $(A/(p^r))^*$ selbst.
Die Operation der Galoisgruppe $G(K(n)/K)$ für ein primäres Polynom $p^r \in A$ ist gegeben durch

$$\sigma_{\bar{b}}(\lambda_0) = \rho_b(\lambda_0) \quad \text{für ein } \bar{b} \in (A/(p^r))^* \text{ mit Repräsentanten } b \in A.$$

Das Polynom $f_{p^r}(X)$ liegt in $A[X]$, denn die Koeffizienten sind ganz über A und liegen in K. Schreiben wir $f_{p^r}(X)$ in der Form

$$f_{p^r}(X) = X^{deg\, f_{p^r}} + \sum_{i=0}^{deg\,(f_{p^r})-1} a_i X^i,$$

so ist $a_0 = p$, denn wegen

$$\begin{aligned} \rho_{p^r}(X) &= p^r X + \{\text{ höhere Terme }\} \\ \rho_{p^{r-1}}(X) &= p^{r-1} X + \{\text{ höhere Terme }\} \end{aligned}$$

ist

$$\frac{\rho_{p^r}(X)}{\rho_{p^{r-1}}(X)} = p + \{\text{ höhere Terme }\}.$$

Daher ist

$$\pm p = \prod_{\substack{\lambda \in {}_{p^r}\rho \\ \lambda \text{ prim.TP.}}} \lambda = \prod_{\bar{b} \in (A(p^r))^*} \rho_b(\lambda_0).$$

Das Polynom

$$\rho_b(\lambda_0) = b \cdot \lambda_0 + (\dots)\lambda_0^q + \dots + \lambda_0^{q^{deg\, b}}$$

wird in $\mathcal{O}(p^r)$ von λ_0 geteilt. Aus Symmetriegründen folgt auch, $\rho_b(\lambda_0)$ teilt λ_0. Deswegen ist $\rho_b(\lambda_0) = \varepsilon \cdot \lambda_0$, wobei $\varepsilon \in \mathcal{O}$ eine Einheit ist. In die obige Gleichung eingesetzt liefert dies:

$$\pm p = \varepsilon \cdot \lambda_0^{|p|^{r-1}(|p|\,-1)}.$$

Der Verzweigungsindex von $\mathfrak{p} = (p)$ ist also größer gleich $|p|^{r-1}(|p|\,-1)$, zugleich muß er aber auch kleiner gleich dem Grad der Erweiterung sein, und somit gilt:

$$e_{\mathfrak{p}}(K(p^r)/K) = |p|^{r-1}(|p|\,-1) = |(A/(p^r))^*|.$$

Also ist $\mathfrak{p}$ in $K(p^r)/K$ voll verzweigt. Somit gilt (ii).

Zwei Körpererweiterungen L_1, L_2 über einem Körper K sind linear disjunkt, wenn es eine Stelle $\mathfrak{p} \in S(K)$ gibt, die voll verzweigt in L_1/K und unverzweigt in L_2/K ist (vergleiche 1.2.4).
Also ist (iv) bereits bewiesen.

Zusammen mit (ii) folgt (i), denn nach dem chinesischen Restsatz ist

$$(A/(n))^* = \prod_{\nu=1}^{s}(A/(p_\nu^{r_\nu}))^*.$$

Um nun (v) zu zeigen, betrachten wir zunächst wieder den primären Fall.
$f_{p^r}(X)$ ist ein Eisensteinpolynom, daher ist

$$\mathcal{O}(p^r)_{(\mathfrak{P})} = A[\lambda_0]_{(\mathfrak{p})}$$

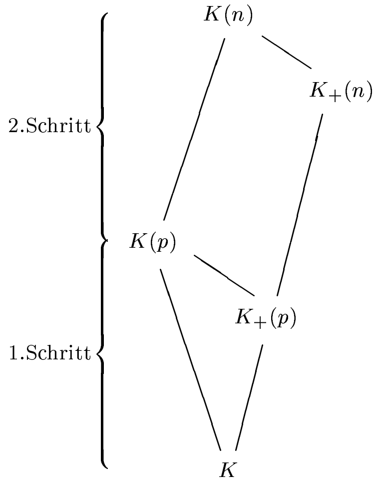
für $\mathfrak{P} \in S(K(p^r))$ mit $\mathfrak{P}|\mathfrak{p}$. Für $\mu, \nu \in \{1, \dots, s\}$ und $\mu \neq \nu$ sind die $K(p_\nu^{r_\nu})$ und $K(p_\mu^{r_\mu})$ linear disjunkt nach (iv). Zudem sind die Diskriminanten $D_{\mathcal{O}(p_\nu^{r_\nu})/A}$ und $D_{\mathcal{O}(p_\mu^{r_\mu})/A}$ teilerfremd. Somit ist

$$\mathcal{O}(n) = \prod_{\nu=1}^{s} \mathcal{O}(p_\nu^{r_\nu}) = A[\lambda],$$

wobei λ ein primitiver n-Teilungspunkt ist (vergleiche [Lan70, S.68]).

Schließlich ist noch (iii) zu zeigen.
Sei dazu $\mathfrak{P}' \in S(K(n))$ eine Stelle, die die ∞-Stelle von K teilt. Da die

Erweiterung galoissch ist, genügt es zu zeigen, daß der Verzweigungsindex $e_\infty(K(n)/K) = e_\infty(K(n)/K_+(n)) = q-1$ und der Trägheitsindex $f_\infty(K(n)/K) = 1$ ist. Dies zeigen wir in etwa dem Beweis von Hayes in [Hay74] folgend, indem wir zunächst die Erweiterung $K(p)/K$ für ein normiertes, irreduzibles Polynom $p|n$ betrachten und dann zeigen, daß jede Stelle $\mathfrak{P} \in S(K(p))$ mit $\mathfrak{P}|\infty$ in $K(n)/K$ voll zerlegt ist. Schematisch stellt sich dies so dar:



In beiden Schritten verwenden wir das Newton–Polygon. Nähere Angaben dazu finden sich in [Neu92, S.151 ff].
Schließlich zeigen wir noch, daß die Galoisgruppe von $K(n)/K_+(n)$ gerade die Einbettung von $\mathbb{F}_q^*$ in A ist.

1. Schritt: Für ein irreduzibles $p \in A$ vom Grad d haben wir nach Proposition 5.18 die Darstellung

$$\rho_p(X) = \sum_{i=0}^{d} h_i(T)\, X^{q^i} \quad \text{mit} \quad deg\, h_i = (d-i)q^i.$$

Mit $f_p(X) = \rho_p(X)/X$ und $f_p(X) = h(X^{q-1})$ für ein geeignetes $h(X) \in A$ erhalten wir

$$h(X) = \sum_{i=0}^{d} h_i(T) X^{\frac{q^i-1}{q-1}}.$$

Die Bewertung der $h_i(T)$ in K_∞ ist

$$v_\infty(h_i(T)) = -deg\, h_i(T) = -(d-i)q^i.$$

Nun wird das Newton–Polygon von $h(X)$ konstruiert.
Für die Punkte

$$\beta_i = \left(\frac{q^i-1}{q-1}, -(d-i)q^i\right), \quad i = 0, \dots, d$$

ist die Steigung der Strecke zwischen β_i und β_{i+1}, $i = 0, \ldots, d-1$, gegeben durch

$$\begin{aligned} \frac{-(d-i-1)q^{i+1} + (d-i)q^i}{\dfrac{q^{i+1}-1}{q-1} - \dfrac{q^i-1}{q-1}} &= \frac{-(d-i)q^i(q-1) + q^{i+1}}{q^i} \\ &= -(d-i)(q-1) + q. \end{aligned}$$

Mit wachsendem i wachsen auch die Steigungen strikt. Daher sind die β_i genau die Ecken des Newton–Polygons.
Zwischen β_0 und β_1 ist die Steigung $-d(q-1)+q$. Es existiert also eine Nullstelle θ von $h(X)$ in K_∞, die die Bewertung

$$v_\infty(\theta) = d(q-1) + q$$

hat.
Weil $h(X^{q-1}) = f_p(X)$ ist, ergibt sich die Vervollständigung von $K(p)$ bezüglich $\mathfrak{P}$ aus K_∞ durch Adjunktion einer Nullstelle λ' des Polynoms $X^{q-1} - \theta$:

$$(K(p))_{\mathfrak{P}} = K_\infty(\lambda').$$

Da nun $v_\infty(\theta)$ und $q-1$ relativ prim sind, ist $\mathfrak{P}$ in der Erweiterung $(K(p))_{\mathfrak{P}}/K_\infty$ voll verzweigt mit Verzweigungsindex $q-1$, und der Trägheitsindex ist 1.

2.Schritt: Nun bleibt noch zu zeigen, daß die Stelle $\mathfrak{P}$ in $K(n)/K(p)$ voll zerlegt ist.
Das Polynom $f_p(X)$ hat λ' als Nullstelle, dessen Bewertung in $(K(p))_{\mathfrak{P}}$

$$v_{\mathfrak{P}}(\lambda') = d(q-1) + q$$

ist. Wegen

$$\rho_n(X) = \rho_p(\rho_{\frac{n}{p}}(X)) = \rho_{\frac{n}{p}}(X) f_p(\rho_{\frac{n}{p}}(X))$$

erhalten wir $K(n)$ durch Adjunktion einer Nullstelle von $f_p(\rho_{\frac{n}{p}}(X))$. Deshalb ist $K(n)$ eine Erweiterung von $K(p)$, die durch Adjunktion einer Nullstelle des Polynoms $\rho_{\frac{n}{p}}(X) - \lambda'$ entsteht. Zur Bestimmung des Newton–Polygons wählen wir die Darstellung

$$\rho_{\frac{n}{p}}(X) = \sum_{i=0}^{deg(n)-d} g_i(T) X^{q^i}$$

mit $g_i(T) \in A$ und $deg\, g_i(T) = (deg(n) - d - i)q^i$ und setzen

$$\begin{aligned} &\gamma_{-1} = (0\,, \quad v_{\mathfrak{P}}(\lambda')\ ) = (0\,, \qquad d(q-1)+q \qquad) \\ \text{und} \qquad &\gamma_i \ = (q^i\,, v_{\mathfrak{P}}(g_i(T))) = (q^i\,, -(deg(n)-d-i)q^i(q-1)) \end{aligned}$$

für $0 \leq\ i \leq deg(n) - d$. Die Steigung der Strecke zwischen γ_{-1} und γ_0 ist

$$-(deg(n) - d)(q - 1) - d(q - 1) - q = -deg(n)(q - 1) - q,$$

und zwischen γ_i und γ_{i+1} ergibt sie sich aus

$$\begin{aligned}
\Delta y &= -(deg(n) - d - (i + 1))q^{i+1}(q - 1) + (deg(n) - d - i)q^i(q - 1) \\
&= q^i(q - 1)(-deg(n) + d + i)(q - 1) + q), \\
\Delta x &= q^i(q - 1)
\end{aligned}$$

zu

$$\frac{\Delta y}{\Delta x} = (-deg(n) + d + i)(q - 1) + q.$$

Wiederum wächst die Steigung strikt mit wachsendem i, so daß die Ecken des Newton–Polygons von $\rho_{\frac{n}{p}}(X) - \lambda'$ über $(K(p))_{\mathfrak{P}}$ eben die Punkte γ_i sind. Betrachten wir die Strecke zwischen γ_{-1} und γ_0, so ergibt sich daraus, daß $\rho_{\frac{n}{p}}(X) - \lambda'$ eine Nullstelle λ in $(K(p))_{\mathfrak{P}}$ hat. Da die Erweiterung galoissch ist, bedeutet dies, daß $\mathfrak{P}$ in $K(n)$ voll zerlegt ist.

3. Schritt: Andererseits gilt hier nun, daß $K(\lambda^{q-1}) = K_+(n)$ ist. Denn für alle $c \in \mathbb{F}_q^*$ gilt $\sigma_{\bar{c}}(\lambda) = \rho_c(\lambda) = c\lambda$, deshalb ist $\sigma_{\bar{c}}(\lambda^{q-1}) = \lambda^{q-1}$, daraus folgt $K(\lambda^{q-1}) \subset K_+(n)$. Und wegen $K(n) = K(\lambda)$ ist

$$[K(n) : K(\lambda^{q-1})] = [K(\lambda) : K(\lambda^{q-1})] \leq q - 1.$$

$\square$

Da der Trägheitsindex $f_\infty(K(n)/K) = 1$ ist, ergibt sich sofort:

Korollar 5.22. *Der Körper $\mathbb{F}_q$ ist in $K(n)$ algebraisch abgeschlossen.*

Kapitel 6

Kreisteilungserweiterungen

6.1 Bezeichnungen und Voraussetzungen

Da wir von nun an ausschließlich Kreisteilungserweiterungen des rationalen Funktionenkörpers sowie geeignete Zwischenerweiterungen betrachten werden, führe ich die folgenden Notationen ein, die für den gesamten Rest der Arbeit gelten.

Es ist $A := \mathbb{F}_q[T]$ der Polynomring über $\mathbb{F}_q$ in einer Unbestimmten T.
Mit $K := \mathbb{F}_q(T)$ wird der Quotientenkörper von A bezeichnet und die Erweiterung des Konstantenkörpers durch den Übergang zu dem algebraischen Abschluß $\overline{\mathbb{F}}_q \subset C$ von $\mathbb{F}_q$ mit

$$K' := \overline{\mathbb{F}}_q \, K = \overline{\mathbb{F}}_q(T).$$

Sei $n \in A$ ein normiertes Polynom. Dann hat n eine eindeutige Zerlegung in Primfaktoren, nämlich:

$$n = \prod_{\nu=1}^{s} p_\nu^{r_\nu},$$

wobei s, r_ν in $\mathbb{N}$ liegen und die $p_\nu \in A$ normierte, irreduzible, paarweise verschiedene Polynome vom Grad ≥ 1 sind. Desweiteren sind

$$\begin{aligned} d_\nu &:= deg(p_\nu)\,, & q_\nu &:= q^{d_\nu}, \\ n_\nu &:= \quad p_\nu^{r_\nu} \quad , & m_\nu &:= \frac{n}{n_\nu} \end{aligned}$$

und

$$\varphi(n) := |(A/(n))^*|.$$

Da nach dem chinesischen Restsatz

$$(A/(n))^* \cong \prod_{\nu=1}^{s} (A/(n_\nu))^*$$

ist, ergibt sich

$$\varphi(n) = \prod_{\nu=1}^{s} \varphi(n_\nu) \quad \text{mit} \quad \varphi(n_\nu) = (q_\nu - 1) q_\nu^{r_\nu - 1}.$$

Die Analogie zur Eulerschen φ-Funktion spiegelt sich in der Bezeichnung wider.

Entsprechend werden auch die Hauptideale mit $\mathfrak{p}_\nu := (p_\nu)$ für alle $\nu = 1, \ldots, s$ bezeichnet, und für $1 \leq \alpha \leq r_\nu$ sei

$$G(n_\nu)^\alpha := \{ b \in (A/(n_\nu))^* \mid b \equiv 1 \bmod p_\nu^\alpha \}.$$

Weiterhin sind

$$_n\rho \ := {}_n\rho \ (C)$$

die Menge der n-Torsionselemente von ρ in C und

$$K(n) := K({}_n\rho \ )$$

der Zerfällungskörper in C von $\rho_n(X)$. Die entsprechende Konstantenerweiterung von $K(n)$ bezeichne ich mit

$$K'(n) := \overline{\mathbb{F}}_q \, K(n).$$

Im weiteren Verlauf werden wir einige Unterkörper von $K(n)$ betrachten. Auch für solche Körper $K \subset K_*(n) \subset K(n)$, wobei "$*$" an geeigneter Stelle definiert wird, wird der Übergang zum algebraischen Abschluß herangezogen, die Konstantenerweiterung bezeichne ich dann mit

$$K'_*(n) := \overline{\mathbb{F}}_q \, K_*(n).$$

Nach Kapitel 3 ändern sich der Grad, die Verzweigungsindizes und das Geschlecht einer solchen Erweiterung nicht unter Konstantenerweiterung, da $\mathbb{F}_q$ nach Korollar 5.22 der volle Konstantenkörper von $K(n)$ ist. Ebenso ändern sich die Mächtigkeiten der Verzweigungsgruppen einer galoisschen Erweiterung eines algebraischen Funktionenkörpers unter Konstantenerweiterung nicht.
Es ergibt sich also:

$$\begin{aligned} [K'(n) : K'] &= [K(n) : K] = \varphi(n) \quad \text{und} \\ e_{\mathfrak{p}'}(K'(n)/K') &= e_{\mathfrak{p}}(K(n)/K) \qquad \text{sowie} \quad g(K'(n)) = g(K(n)), \end{aligned}$$

wobei $\mathfrak{p}' \in S(K')$ mit $\mathfrak{p}'|\mathfrak{p}$ ist. Für $K(n_\nu)/K$ bedeutet dies anschaulich

$$\begin{array}{ccccccccc} \mathfrak{P}_\nu & K(n_\nu) & \text{———} & K'(n_\nu) & \mathfrak{P}_{\nu,1} & \dots & \mathfrak{P}_{\nu,d_\nu} \\ \Big| & \Big| & & \Big| & \Big| & & \Big| \\ \mathfrak{p}_\nu & K & \text{———} & K' & \mathfrak{p}_{\nu,1} & \dots & \mathfrak{p}_{\nu,d_\nu} \end{array},$$

wobei die Primzerlegung $p_\nu = \prod_{\alpha=1}^{d_\nu} p_{\nu,\alpha} \in \overline{\mathbb{F}}_q[T]$ die Stellen $\mathfrak{p}_{\nu,\alpha} = (p_{\nu,\alpha})$ bestimmt.

Bemerkung 6.1. Die Erweiterung des Konstantenkörpers ist "sehr groß" gewählt. Um eine Vereinfachung der Berechnung zu erreichen, würde eine "kleinere" Erweiterung bereits genügen.
Wählen wir nämlich statt des algebraischen Abschlusses $\overline{\mathbb{F}}_q$ den Restkörper einer Stelle $\mathfrak{P}$ in $K(n)/K$, so ist der Grad jeder $\mathfrak{p}$ bzw. $\mathfrak{P}$ teilenden Stelle bereits 1.
Und auch wenn dieses Verfahren iteriert und der Konstantenkörper um alle Restkörper erweitert wird, die in unserer Situation relevant sind, d.h. für alle Stellen $\mathfrak{P} \in S(K(n))$ mit $\mathfrak{P}|(p_\nu)$ für ein $\nu \in \{1, \dots, s\}$, bleibt die Erweiterung endlich und somit auch die Konstanten– und Restkörper. Letzteres würde insbesondere gewährleisten, daß die Komplettierungen der dann zu betrachtenden Körper in der Tat lokale Körper sind.
Die Erweiterung des Konstantenkörpers dient hier vor allem der technischen Vereinfachung der Berechnung, da in der Riemann–Hurwitz–Formel nun nicht mehr zwischen Trägheits- und Zerlegungsgraden unterschieden werden muß. Folglich ist die konkrete Wahl der Erweiterung des Konstantenkörpers für die Inhalte dieser Arbeit nicht essentiell.

Sei nun $K \subset L \subset K(n)$. Für eine Stelle $\mathfrak{q} \in S(L)$ und $S(L') \ni \mathfrak{q}'|\mathfrak{q}$ mit $L' := \overline{\mathbb{F}}_q L$ bezeichne stets

$$g_i(\mathfrak{q}') := |(G(K'(n)/L'))_i(\mathfrak{q}')| = |(G(K(n)/L))_i(\mathfrak{q})|$$

die Mächtigkeit der i-ten Verzweigungsgruppe in der Erweiterung $K'(n)/L'$.

Ziel der folgenden Berechnungen ist es, eine geschlossene Formel zur Berechnung des Geschlechtes $g(K(n))$ anzugeben. Dazu betrachten wir zunächst den primären Fall und folgern den allgemeinen Fall rekursiv unter Ausnutzung der linearen Disjunktheit der Erweiterungen $K(n_\nu)$ und $K(m_\nu)$.

6.2 Das Geschlecht von $K(p^r)$

Da hier in der oben angegebenen Schreibweise $s = 1$ ist, setze ich zur verbesserten Übersichtlichkeit $p_1 = p$, $r_1 = r$ und $d_1 = d$, die Galoisgruppe bezeichne ich mit G.

Das Geschlecht des Körpers $K(p^r)$ läßt sich mit Hilfe der Riemann–Hurwitz–Formel

$$2g(K(p^r)) - 2 = [K(p^r) : K](2g(K) - 2) + \sum_{\mathfrak{p} \in S(K')} \sum_{i=0}^{\infty} (g_i(\mathfrak{p}) - 1),$$

aus Satz 3.9 berechnen. Dazu werden allerdings die Mächtigkeiten der höheren Vezweigungsgruppen benötigt.

6.2.1 Höhere Verzweigungsgruppen von $K(p^r)$

Aus Satz 5.20 folgt, daß in $K(p^r)$ jede über ∞ liegende Stelle zahm verzweigt mit Verzweigungsindex $e_\infty(K(p^r)/K) = q-1$. Die höheren Verzweigungsgruppen sind somit trivial und die Berechnung der Bewertung der lokalen Differente vereinfacht sich stark:

$$\sum_{i=0}^{\infty} (g_i(\infty) - 1) = e_\infty(K(p^r)_{\mathfrak{Q}}/K_\infty) - 1 = q - 2,$$

wobei $\mathfrak{Q} \in S(K(p^r))$ eine ∞ teilende Stelle ist.
Eine weitere Aussage des Satzes 5.20 ist, daß die Stelle $\mathfrak{p} = (p)$ die einzige endliche Stelle ist, die in dieser Erweiterung verzweigt. Da sie voll verzweigt, ist der Index

$$e_{\mathfrak{p}}(K(p^r)/K) = |(A/\mathfrak{p})^*| = \varphi(p^r) = q^{d(r-1)}(q^d - 1).$$

Bezeichnen $K_{\mathfrak{p}}$ bzw. $K(p^r)_{\mathfrak{P}}$ die Vervollständigungen von K bzw. $K(p^r)$ bezüglich $\mathfrak{p}$ bzw. $\mathfrak{P}$, wobei $\mathfrak{P}|\mathfrak{p}$ gilt, so ist nach Kapitel 1 die Galoisgruppe von $K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ gleich der Zerlegungsgruppe von $\mathfrak{P}$:

$$G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) = Z_{\mathfrak{P}}(K(p^r)/K).$$

Da $\mathfrak{p}$ in der Erweiterung voll verzweigt, stimmen die Galoisgruppen von $K(p^r)/K$ und $K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ überein und die Trägheitsgruppe von $\mathfrak{P}$ ist gleich der Galoisgruppe.

Die i-te Verzweigungsgruppe von $\mathfrak{P}$ für in $K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ sei mit

$$G_i := \{\sigma \in G \mid v_{\mathfrak{P}}(\sigma(a) - a) \geq i + 1 \text{ für alle } a \in \mathcal{O}_{(\mathfrak{P})}\}$$

bezeichnet für alle $i \in \mathbb{Z}$ und $i \geq -1$. Dann gilt:

Proposition 6.2. *Die Verzweigungsgruppen von $K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}$ sind*

$$\begin{array}{lrclcrcll}
 & & & & & G_0 & = & G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}), & \\
\textit{für} & 1 & \leq i \leq & q^d-1 & \textit{ist} & G_i & \cong & G(p^r)^1, & \\
\textit{für} & q^d & \leq i \leq & q^{2d}-1 & \textit{ist} & G_i & \cong & G(p^r)^2, & \\
\multicolumn{9}{l}{\textit{und allgemein}} \\
\textit{für} & q^{d(\alpha-1)} & \leq i \leq & q^{d\alpha}-1 & \textit{ist} & G_i & \cong & G(p^r)^\alpha, & 1 \leq \alpha \leq r-1, \\
\textit{für} & q^{d(r-1)} & \leq i & & \textit{ist} & G_i & \cong & G(p^r)^r = \{1\}. &
\end{array}$$

Beweis: Daß $G_0 = T_{\mathfrak{P}}(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) = G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}})$ ist, ist klar.
Sei nun R^* ein minimales Repräsentantensystem für $(A/(p^r))^*$ und λ_0 ein Erzeuger des A-Moduls ${}_{p^r}\rho$.
Dann ist die Abbildung

$$\begin{array}{rccc}
 & R^* & \longrightarrow & G(K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}) \\
 & b & \mapsto & \sigma_{\overline{b}} \\
\text{mit} & & & \sigma_{\overline{b}}(\lambda_0) = \rho_b(\lambda_0)
\end{array}$$

eine Bijektion. Für $b \in R^*$ ist

$$\begin{array}{lrcl}
 & \rho_b(\lambda_0) & = & b\cdot\lambda_0 + (\dots)\lambda_0^q + \dots + \lambda_0^{q^{deg(b)}}. \\
\text{Weiter ist} & \rho_b(\lambda_0) - \lambda_0 & = & \rho_{b-1}(\lambda_0) \\
\text{und} & v_{\mathfrak{P}}(\rho_b(\lambda_0) - \lambda_0) & = & v_{\mathfrak{P}}(\rho_{b-1}(\lambda_0)).
\end{array}$$

Behauptung: Ist für ein $0 \leq \alpha \leq r-1$ nun $b \equiv 1 \bmod p^\alpha$ und $b \not\equiv 1 \bmod p^{\alpha+1}$, so ist $\rho_{b-1}(\lambda_0)$ ein primitiver $\rho_{p^{r-\alpha}}$-Torsionspunkt.

Beweis: Seien

$$f_{p^r}(X) := \frac{\rho_{p^r}(X)}{\rho_{p^{r-1}}(X)} = \prod_{\substack{\lambda\in{}_{p^r}\rho \\ \lambda\text{ prim.TP.}}} (X-\lambda)$$

und

$$f_{p^{r-\alpha}}(X) := \frac{\rho_{p^{r-\alpha}}(X)}{\rho_{p^{r-\alpha-1}}(X)} = \prod_{\substack{\lambda\in{}_{p^{r-\alpha}}\rho \\ \lambda\text{ prim.TP.}}} (X-\lambda).$$

Beide Polynome sind Eisenstein–Polynome und Minimal–Polynome der Erweiterungen $K(p^r)$ bzw. $K(p^{r-\alpha})$.
Da $p^\alpha|(b-1)$ und $p^{\alpha+1}\nmid(b-1)$ gilt, existiert ein $\tilde{b} \in R^*$, so daß $b-1 = \tilde{b}\cdot p^\alpha$ und

$\mathrm{ggT}(\tilde{b}, p) = 1$ ist.
Damit erhalten wir

$$\rho_{p^{r-\alpha}}(\rho_{b-1}(\lambda_0)) = \rho_{(b-1)p^{r-\alpha}}(\lambda_0) = \rho_{\tilde{b}p^r}(\lambda_0) = \rho_{p^r}(\rho_{\tilde{b}}(\lambda_0)) = 0$$

und

$$\rho_{p^{r-\alpha-1}}(\rho_{b-1}(\lambda_0)) = \rho_{\tilde{b}p^{r-1}}(\lambda_0) \neq 0,$$

da $\rho_{\tilde{b}}(\lambda_0)$ ein primitiver ρ_{p^r}-Torsionspunkt ist. Also ist $f_{p^{r-\alpha}}(\rho_{b-1}(\lambda_0)) = 0$ und somit ist $\rho_{b-1}(\lambda_0)$ ein primitiver $\rho_{p^{r-\alpha}}$-Torsionspunkt.

Unter Beachtung der vollen Verzweigung ergibt sich dann

$$v_{\mathfrak{P}}(\rho_{b-1}(\lambda_0)) = \underbrace{[K(p^r)_{\mathfrak{P}} : K(p^{r-\alpha})_{\mathfrak{q}}]}_{q^{d\alpha}} \cdot \underbrace{v_{\mathfrak{q}}(\rho_{b-1}(\lambda_0))}_{1} = q^{d\alpha},$$

wobei $\mathfrak{q}$ das Primideal im Ganzheitsring von $K(p^{r-\alpha})$ bezeichnet, daß $\mathfrak{p}$ teilt, also $\mathfrak{p} \subset \mathfrak{q} \subset \mathfrak{P}$. Daher ist $\sigma_{\overline{b-1}} \in G_i$ für alle $i \leq q^{d\alpha} - 1$ und für $i \geq q^{d\alpha}$ ist $\sigma_{\overline{b-1}} \notin G_i$. Somit ist die Proposition gezeigt. □

Nun berechnen wir die Mächtigkeit der Verzweigungsgruppen.

Behauptung 6.3. Für alle $1 \leq \alpha \leq r$ gilt

$$|G(p^r)^\alpha| = q^{d(r-\alpha)}.$$

Beweis: Die Projektionsabbildung

$$(A/(p^r))^* \longrightarrow (A/(p^\alpha))^*$$

hat als Kern die Gruppe $G(p^r)^\alpha$. Daher ist die Sequenz

$$1 \longrightarrow G(p^r)^\alpha \longrightarrow (A/(p^r))^* \longrightarrow (A/(p^\alpha))^* \longrightarrow 1$$

exakt. Also ist

$$|G(p^r)^\alpha| = \frac{\varphi(p^r)}{\varphi(p^\alpha)} = q^{d(r-\alpha)}.$$

□

Bemerkung 6.4. Die in der Proposition 6.2 beschriebene Gruppenfiltration stimmt mit der oberen Numerierung der Verzweigungsgruppen überein:

$$G_i = G^\alpha = G(p^r)^\alpha \quad \text{mit} \quad \varphi_{K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(i) = \alpha$$

(vergleiche Abschnitt 2.3).

Beweis: Ist G^v eine Sprungstelle der Filtration (G^v), so ist nach dem Satz von Hasse – Arf, Satz 2.11, die Zahl v ganz. Es sind also zunächst jene $v \in \mathbb{R}$ zu bestimmen, die ganzzahlig sind.
Die Herbrand'sche φ-Funktion

$$\varphi_{K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(u) = \int_0^u \frac{dt}{|G_0 : G_t|}$$

liefert mit $g_i := |G_i|$ für ein $m \in \mathbb{N}$

$$\varphi_{K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(m) + 1 = \frac{1}{g_0} \sum_{i=0}^{m} g_i.$$

Es ist hier also für $q^{d(\alpha-1)} \leq m \leq q^{d\alpha} - 1$

$$\begin{aligned}
\varphi_{K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(m) &= \frac{1}{g_0} \left(\sum_{k=1}^{\alpha-1} \sum_{i=q^{d(k-1)}}^{q^{kd}-1} q^{d(r-k)} + \sum_{i=q^{d(\alpha-1)}}^{m} q^{d(r-\alpha)} \right) \\
&= \frac{1}{g_0} \left((\alpha-1)(q^d-1)q^{d(k-1)}q^{d(r-k)} + (m - q^{d(\alpha-1)} + 1)q^{d(r-\alpha)} \right) \\
&= \alpha - 1 + \frac{m - q^{d(\alpha-1)} + 1}{(q^d-1)q^{d(r-1)}} \cdot q^{d(r-\alpha)} \\
& \begin{cases} = & \alpha, \quad \text{für } m = q^{d\alpha} - 1 \\ \notin & \mathbb{N}, \quad \text{sonst.} \end{cases}
\end{aligned}$$

Die Sprungstellen stimmen demnach überein:

$$G_{q^{d\alpha}-1} \;=\; G^{\alpha} \;\cong\; G(p^r)^{\alpha} \quad \text{für } 1 \leq \alpha \leq r-1,$$

da $\varphi_{K(p^r)_{\mathfrak{P}}/K_{\mathfrak{p}}}(q^{d\alpha} - 1) = \alpha$ ist. □

Bezeichnung 6.5. Im folgenden werde ich $(A/(n))^*$ mit $G(n)$ bezeichnen und auch die Galoisgruppe $G(K(n)/K)$ mit $G(n)$ unter Ausnutzung der gegebenen Isomorphie identifizieren.

6.2.2 Geschlechtsberechnung

Nun müssen nur noch die entsprechenden Werte in die Riemann–Hurwitz–Formel eingesetzt werden. Es ist

$$\begin{aligned}
2g(K(p^r)) - 2 &= [K(p^r) : K](2g(K) - 2) + \sum_{\mathfrak{q} \in S(K')} \sum_{i=o}^{\infty} (g_i(\mathfrak{q}) - 1), \\
&= \varphi(p^r)(2g(K) - 2) + \frac{\varphi(p^r)}{q-1}(e_\infty(K(p^r)/K) - 1) + d \cdot \sum_{i=0}^{\infty} (g_i(\mathfrak{p}) - 1) \\
&= -2 \cdot \varphi(p^r) + \frac{\varphi(p^r)}{q-1}(q-2) + d \cdot \sum_{i=0}^{\infty} (g_i(\mathfrak{p}) - 1),
\end{aligned}$$

da das Geschlecht des rationalen Funktionenkörpers 0 ist (vergleiche Beispiele 3.5). Aus den obigen Überlegungen ergibt sich

$$\begin{aligned}
\sum_{i=0}^{\infty}(g_i(\mathfrak{p})-1) &= \sum_{i=0}^{q^{d(r-1)}}(g_i(\mathfrak{p})-1), \\
&\qquad \text{da für } i \geq q^{d(r-1)} \qquad G_i(\mathfrak{P}) = \{1\} \text{ ist,} \\
&= |g_0(\mathfrak{p})| - 1 + \sum_{\alpha=1}^{r-1}\sum_{i=q^{d(\alpha-1)}}^{q^{d\alpha}-1}(|G(p^r)^\alpha|-1), \\
&\qquad \text{da für } q^{d(\alpha-1)} \leq i \leq q^{d\alpha}-1 \qquad G_i(\mathfrak{P}) = G(p^r)^\alpha \text{ ist,} \\
&= |g_0(\mathfrak{p})| - 1 + \sum_{\alpha=1}^{r-1}(q^{d\alpha}-q^{d(\alpha-1)})(q^{d(r-\alpha)}-1), \\
&\qquad \text{da } |G(p^r)^\alpha| = q^{d(r-\alpha)} \text{ ist,} \\
&= |g_0(\mathfrak{p})| - 1 + \sum_{\alpha=1}^{r-1}(q^{d\alpha}-q^{d(\alpha-1)})q^{d(r-\alpha)} - \sum_{\alpha=1}^{r-1}(q^{d\alpha}-q^{d(\alpha-1)}) \\
&= q^{d(r-1)}(q^d-1) - 1 + (r-1)q^{d(r-1)}(q^d-1) - (q^{d(r-1)}-1) \\
&= q^{d(r-1)}(rq^d-r-1).
\end{aligned}$$

Eingesetzt liefert dies

$$2g(K(p^r)) - 2 = -2(q^d-1)q^{d(r-1)} + \frac{q-2}{q-1}(q^d-1)q^{d(r-1)} + dq^{d(r-1)}(rq^d-r-1)$$

bzw.

$$\begin{aligned}
g(K(p^r)) &= 1 + \frac{1}{2}q^{d(r-1)}\left(-2(q^d-1) + \frac{q-2}{q-1}(q^d-1) + d(rq^d-r-1)\right) \\
&= 1 + \frac{1}{2}q^{d(r-1)}(q^d-1)\left(-2 + \frac{q-2}{q-1} + d\frac{rq^d-r-1}{q^d-1}\right).
\end{aligned}$$

Somit gilt

Satz 6.6. *Das Geschlecht des Körpers $K(p^r)$ ist*

$$\boxed{g(K(p^r)) = 1 + \frac{1}{2}\,\varphi(p^r)\left(-2 + \frac{q-2}{q-1} + d\frac{rq^d-r-1}{q^d-1}\right).}$$

6.3 Das Geschlecht von $K(n)$

Satz 6.7. *Für das Geschlecht von $K(n)$ gilt:*

$$2g(K(n)) - 2 = \varphi(n)\left(-2 + \frac{q-2}{q-1} + \sum_{\nu=1}^{s} d_\nu \frac{r_\nu q_\nu - r_\nu - 1}{q_\nu - 1}\right).$$

Beweis: Es gilt:

(i) Die Berechnung kann rekursiv erfolgen:

$$\begin{aligned} g(K(n)) &= [K(n) : K(m_\nu)](2g(K(m_\nu)) - 2) \\ &\quad + \sum_{\tilde{\mathfrak{p}} \in S(K'(m_\nu))} \sum_{i=o}^{\infty} (g_i(\tilde{\mathfrak{p}}) - 1). \end{aligned}$$

(ii) Die $K(n_\nu)$ sind linear disjunkt nach Satz 5.20, und von den endlichen Stellen verzweigt in $K(n_\nu)$ nur die Stelle $\mathfrak{p}_\nu$, diese ist $K(m_\nu)$ unverzweigt. In $K'(m_\nu)$ sind die $\mathfrak{p}_\nu$ teilenden Stellen von K' voll zerlegt, so daß sich für jede Stelle $\mathfrak{p}_\nu$ mit $\nu = 1, \ldots, s$ in $K'(n)$ der Zerlegungsgrad $d_\nu \cdot \varphi(m_\nu)$ ergibt (vergleiche: Abschnitt 1.2.4).

(iii) Die Verzweigungsindizes der ∞-Stelle in $K(n)$ und $K(m_\nu)$ stimmen für $s \geq 2$ überein, also findet dann in der Erweiterung $K(n)/K(m_\nu)$ keine weitere Verzweigung an der ∞-Stelle statt.

(iv) Bezeichnet $H_i(\mathfrak{P}_\nu)$ die i-te Verzweigungsgruppe einer Stelle $\mathfrak{P}_\nu \in S(K(n))$, die die Stelle $\mathfrak{p}_\nu$ teilt, dann gilt

$$H_i(\mathfrak{P}_\nu) = G(K(n)/K(m_\nu)) \cap G_i(\mathfrak{P}_\nu) = G_i(\mathfrak{P}_\nu),$$

da $G(K(n)/K(m_\nu)) = G(K(n_\nu)/K) = G(n_\nu)$ ist.

(v) Die obige Gleichung ergibt sich also für $s \geq 2$ zu

$$2g(K(n)) - 2 = \varphi(n_\nu)(2g(K(m_\nu)) - 2) + d_\nu\, \varphi(m_\nu) \sum_{i=0}^{\infty} g_i(\mathfrak{p}_\nu).$$

Nun läßt sich der Satz induktiv beweisen.

(vi) Die Verankerung für $s = 1$ ist im vorangegangenen Abschnitt bereits gezeigt worden. Der Schritt von $s-1$ nach s erfolgt mit (v):

$$\begin{aligned}
2g(K(n))-2 &= \varphi(n_s)(2g(K(m_s))-2)+d_s\,\varphi(m_s)\sum_{i=0}^{\infty}(g_i(\mathfrak{p}_s)-1)\\
&= \varphi(n_s)\,\varphi(m_s)\left(-2+\frac{q-2}{q-1}+\sum_{\nu=1}^{s-1}d_\nu\frac{r_\nu q_\nu-r_\nu-1}{q_\nu-1}\right)\\
&\quad +d_s\,\varphi(m_s)q_s^{r_s-1}(r_sq_s-r_s-1)\\
&= \varphi(n)\left(-2+\frac{q-2}{q-1}+\sum_{\nu=1}^{s-1}d_\nu\frac{r_\nu q_\nu-r_\nu-1}{q_\nu-1}\right)\\
&\quad +d_s\,\varphi(n)\frac{r_sq_s-r_s-1}{q_s-1}\\
&= \varphi(n)\left(-2+\frac{q-2}{q-1}+\sum_{\nu=1}^{s}d_\nu\frac{r_\nu q_\nu-r_\nu-1}{q_\nu-1}\right).
\end{aligned}$$

□

Das Geschlecht von $K(n)$ ist also

$$\boxed{g(K(n))=1+\frac{1}{2}\,\varphi(n)\left(-2+\frac{q-2}{q-1}+\sum_{\nu=1}^{s}d_\nu\frac{r_\nu q_\nu-r_\nu-1}{q_\nu-1}\right).}$$

6.4 Der Fixkörper von $\mathbb{F}_q^*$

Mit $K_+(n)$ wird der Fixkörper der Einbettung $\mathbb{F}_q^*\hookrightarrow(A/(n))^*$ bezeichnet.

Bemerkung 6.8. Da $\mathbb{F}_q^*$ "diagonal" in $G(n)\cong G(n_1)\times\ldots\times G(n_s)$ liegt, kann hier die lineare Disjunktheit der $K(n_\nu)$ zur Berechnung des Geschlechtes von $K_+(n)$ nicht genutzt werden. Insbesondere ist das Körperkompositum $\prod_{\nu=1}^s K_+(n_\nu)$ im allgemeinen ein echter Unterkörper von $K_+(n)$, wie man leicht sieht. Denn der Grad der Erweiterung $K_+(n_\nu)/K$ ist

$$[K_+(n_\nu):K]=\frac{\varphi(n_\nu)}{q-1}$$

und somit ist

$$\left[\prod_{\nu=1}^{s}K_+(n_\nu)\,:K\right]=\prod_{\nu=1}^{s}\frac{\varphi(n_\nu)}{q-1}=\frac{1}{(q-1)^s}\prod_{\nu=1}^{s}\varphi(n_\nu).$$

Wir erhalten also

$$\left[K_+(n) : \prod_{\nu=1}^{s} K_+(n_\nu)\right] = \left(\frac{1}{(q-1)^s}\prod_{\nu=1}^{s}\varphi(n_\nu)\right)^{-1}\cdot\frac{\varphi(n)}{q-1} = (q-1)^{s-1}.$$

Das Geschlecht des Körpers $K_+(n)$ wird daher “von oben“ berechnet.

$$G(n)\left\{\begin{array}{c} K(n) \\ \Big| \\ K_+(n) \\ \Big| \\ K \end{array}\right. \begin{array}{l} \left.\begin{array}{c} \\ \\ \end{array}\right\}\mathbb{F}_q^* \\ \left.\begin{array}{c} \\ \\ \end{array}\right\}G(n)/\mathbb{F}_q^* \end{array}$$

Die Verzweigungsgruppen der Erweiterung $K(n)/K_+(n)$ ergeben sich aus den Schnitten der Verzweigungsgruppen der Erweiterung $K(n)/K$ mit der Galoisgruppe $G(K(n)/K_+(n)) \cong \mathbb{F}_q^*$.
Da $|\mathbb{F}_q^*| = q-1$ ist, ist der Verzweigungsindex jeder Stelle prim zur Charakteristik des Restklassenkörpers. Daher ist jede Stelle in der Erweiterung zahm, und alle höheren Verzweigungsgruppen sind trivial. Es genügt, die Trägheitsgruppen der in $K(n)$ verzweigenden Stellen zu betrachten.
Für eine (fixierte) endliche Stelle $\mathfrak{P}$ in $K(n)$ mit $\mathfrak{P}|\mathfrak{p}_\nu$ für ein $\nu = 1, \dots, s$ ist die Trägheitsgruppe

$$T_{\mathfrak{P}}(K(n)/K_+(n)) = T_{\mathfrak{P}}(K(n)/K) \cap G(K(n)/K_+(n)).$$

Ihre Mächtigkeit ist gleich dem Verzweigungsindex von $\mathfrak{P}$ in der Erweiterung $K(n)/K_+(n)$. Wegen

$$T_{\mathfrak{P}}(K(n)/K) \cong G(n_\nu) \quad \text{und} \quad G(K(n)/K_+(n)) \cong \mathbb{F}_q^*$$

erhalten wir

$$\begin{array}{lrcl} & T_{\mathfrak{P}}(K(n)/K) & \cong & \{b \in G(n) \mid b \equiv 1 \bmod m_\nu\} \\ \text{und} & G(K(n)/K_+(n)) & \cong & \{b \in G(n) \mid \exists \varepsilon \in \mathbb{F}_q^* \text{ mit } b \equiv \varepsilon \bmod n\} \end{array}$$

und somit

$$T_{\mathfrak{P}}(K(n)/K) \cap G(K(n)/K_+(n)) \cong \begin{cases} \mathbb{F}_q^*, & \text{falls} \quad s = 1 \\ \{1\}, & \text{falls} \quad s > 1 \end{cases}.$$

Nach Satz 5.20 haben die $\frac{\varphi(n)}{q-1}$ Stellen in $K_+(n)$, die über der ∞-Stelle liegen, den Verzweigungsindex $q-1$.
Aus

$$2g(K(n)) - 2 = (q-1)(2g(K_+(n)) - 2) + \sum_{\mathfrak{q} \in S(K'_+(n))} (g_0(\mathfrak{q}) - 1)$$

ergibt sich:

Satz 6.9. *Das Geschlecht von $K_+(n)$ ist*

$$
\boxed{
\begin{aligned}
g(K_+(n)) &= 1 + \frac{1}{q-1}\left(g(K(n)) - 1 - \frac{1}{2}\left(\varphi(n)\frac{q-2}{q-1} + d_1(q-2)\right)\right) \\
&\text{für } s = 1 \qquad \text{und} \\
g(K_+(n)) &= 1 + \frac{1}{q-1}\left(g(K(n)) - 1 - \frac{1}{2}\,\varphi(n)\frac{q-2}{q-1}\right) \quad \text{für } s > 1.
\end{aligned}
}
$$

Kapitel 7

Zwischenerweiterungen

Voraussetzung: Von nun an sei das normierte Polynom $n \in A$ stets teilerfremd zu den Polynomen T und $T-1$ gewählt.

Von der Erweiterung $K(n)/K$ ausgehend lassen sich nun Zwischenerweiterungen bestimmen, in der eine gewisse Zahl rationaler Punkte sicher vorhanden ist. Betrachten wir nämlich eine rationale Stelle $\mathfrak{q}$ des Körpers K und bestimmen ihre Zerlegungsgruppe $Z = Z_{\mathfrak{q}}(K(n)/K)$, so ist in dem Fixkörper $K(n)^Z$ die Stelle $\mathfrak{q}$ voll zerlegt. Somit hat der Körper K^Z mindestens Grad der Erweiterung viele rationale Stellen. Auf diese Weise können wir uns "von unten" der Serre–Schranke (siehe Seite 41) nähern.

Betrachten wir nun zwei in K rationale Stellen (a) und (b), so lassen sich diese mittels einer affinen linearen Transformation, die die ∞-Stelle fest läßt, in die ebenfalls rationalen Stellen (T) und $(T-1)$ überführen, wobei dann auch die Erweiterung $K(n)/K$ in eine ihr isomorphe Erweiterung $K(n')/K$ überführt wird (vergleiche Abschnitt 4.5).

Beschränken wir nun unsere Betrachtungen auf die beiden Stellen (T) und $(T-1)$ und wählen n teilerfremd zu T und $T-1$, so ist dies keine echte Einschränkung.

Nun lassen sich für die Fixkörper

$$K_T(n) := K(n)^{Z_{(T)}(K(n)/K)} \quad \text{und} \quad K_{T-1}(n) := K(n)^{Z_{(T-1)}(K(n)/K)}$$

sowie für die Schnitte von Zwischenkörpern

$$\begin{aligned} K_{T,+}(n) &:= K_T(n) \cap K_+(n), \quad & K_{T,T-1}(n) &:= K_T(n) \cap K_{T-1}(n), \\ \text{und} & & K_{T,T-1,+}(n) &:= K_{T,T-1}(n) \cap K_+(n) \end{aligned}$$

die Geschlechter ermitteln.

Dazu wird es wiederum notwendig sein, die Mächtigkeiten höherer Verzweigungsgruppen zu ermitteln. Nach Kapitel 2 können diese für einen Zwischenkörper $K \subset L \subset K(n)$ mit $L = K(n)^H$ sowohl von "unten", wobei gewisse Quotienten von Gruppe betrachtet werden, als auch von "oben", indem die

Schnittbildung mit den Verzweigungsgruppen der Erweiterung $K(n)/K$ mit der Gruppe H benutzt wird, berechnet werden. Die letztgenannte Methode bietet in dieser Situation den Vorteil relativ einfacher Berechnungen, wie sich im Abschnitt 7.3 zeigen wird.

7.1 Zerlegungsgruppen

Seien $n \in A$ ein normiertes und $a \in A$ ein normiertes, irreduzibles Polynom, so daß $\mathrm{ggT}(a,n) = 1$ ist. Der Grad von a sei mit $\alpha := deg(a)$ und das von a erzeugte Hauptideal mit $\mathfrak{a}$ bezeichnet.
Dann ist $\mathfrak{A}$ mit $\mathfrak{A}|\mathfrak{a}$ in der Erweiterung $K(n)/K$ unverzweigt. Die Trägheitsgruppe ist $T_{\mathfrak{a}}(K(n)/K) = \{1\}$ und die Zerlegungsgruppe

$$Z_{\mathfrak{a}}(K(n)/K) \cong G\left(\mathcal{O}(n)/\mathfrak{A}\Big/ A/\mathfrak{a}\right).$$

Die Galoisgruppe der Resterweiterung ist zyklisch und erzeugt von der Abbildung

$$x \mapsto x^{q^\alpha}.$$

Ist $\sigma \in Z_{\mathfrak{a}}(K(n)/K)$ der korrespondierende Erzeuger, so ist σ charakterisiert durch

$$\sigma(x) \equiv x^{q^\alpha} \bmod \mathfrak{A} \qquad \text{für alle } x \in \mathcal{O}_{(\mathfrak{A})}.$$

Dieses Element der Galoisgruppe heißt der *Frobenius–Automorphismus von* $\mathfrak{a}$.

Proposition 7.1. *Der zu* $\mathfrak{a}$ *gehörige Frobenius–Automorphismus ist gleich* $\sigma_{\overline{a}}$.

Beweis: Da $\sigma_{\overline{a}}(\lambda_0) = \rho_a(\lambda_0)$ ist, ist zu zeigen, daß für alle $x \in \mathcal{O}_{(\mathfrak{A})}$

$$\rho_a(x) \equiv x^{q^\alpha} \bmod \mathfrak{A}$$

ist. Es ist

$$\rho_a(\tau) = \sum_{i=0}^{\alpha} a_i\tau^i \quad \text{bzw.} \quad \rho_a(\tau) - \tau^\alpha = \sum_{i=0}^{\alpha-1} a_i\tau^i.$$

Behauptung: Es gilt $a|\left(\rho_a(\tau) - \tau^\alpha\right)$.
Beweis: Durch vollständige Induktion über den Vergleich der $(\alpha-1)$-ten Koeffizienten von

$$\rho_T(\tau)\rho_a(\tau) = (T+\tau)\sum_{i=0}^{\alpha} a_i\tau^i = \sum_{i=0}^{\alpha} a_i\tau^i\,(T+\tau) = \rho_a(\tau)\rho_T(\tau)$$

zeigen wir, daß a die a_i für $i = 0, \ldots \alpha - 1$ teilt.

(i) Für $i = 0$ ist die Behauptung wahr, denn es ist $a_0 = a$ und somit gilt $a|a_0$.

(ii) Die Behauptung gelte für alle $i \leq k-1$. Die k-ten Koeffizienten sind

$$Ta_k + a_{k-1}^q = a_k T^{q^k} + a_{k-1}.$$

Einfaches Umstellen der Gleichung liefert

$$(T^{q^k} - T)a_k = a_{k-1} - a_{k-1}^q,$$

woraus folgt, daß $a_{k-1}|(T^{q^k} - T)a_k$ gilt. Zu zeigen ist nun also, daß a den Term $(T^{q^k} - T)$ für $k < \alpha$ nicht teilt. Dazu zeigen wir die Gleichheit

$$(T^{q^k} - T) = \prod_{\substack{f \in A \\ \text{irred.,norm.} \\ deg(f)|k}} f.$$

Der Zerfällungskörper des Polynoms $T^{q^k} - T$ ist $\mathbb{F}_{q^k}$. Ist nun f ein irreduzibles Polynom vom Grad d, so sind alle Nullstellen in dem Körper $\mathbb{F}_{q^d}$ enthalten. Der Körper $\mathbb{F}_{q^d}$ ist ein Unterkörper von $\mathbb{F}_{q^k}$ genau dann, wenn k von d geteilt wird (siehe [Wol96, Seite 168 f]). Somit ist für jedes irreduzible Polynom f

$$T^{q^k} - T \equiv 0 \bmod f$$

genau dann, wenn der Grad von f die Zahl k teilt. Da

$$\frac{d}{dT}(T^{q^k} - T) = -1 \neq 0,$$

$T^{q^k} - T$ also quadratfrei ist, gilt die obige Aussage.
Somit muß nun für alle $0 \leq k \leq \alpha - 1$ das Polynom a die Koeffizienten a_k teilen. Ist $k = \alpha$, so ist $a_k = 1$, und a teilt $T^{q^k} - T$.

Also ist $\rho_a(\tau) - \tau^\alpha \equiv 0 \bmod a$, und da $a \in \mathfrak{a} \subset \mathfrak{A}$ ist, folgt die Aussage der Proposition. □

Bezeichnung 7.2. Sei $a \in G(n)$. Mit $\langle\, a \,\rangle_{G(n)}$ bezeichne ich das Erzeugnis des Elementes a in der Gruppe $G(n)$.

Als Zerlegungsgruppen der Stellen T und $T-1$ ergeben sich demnach

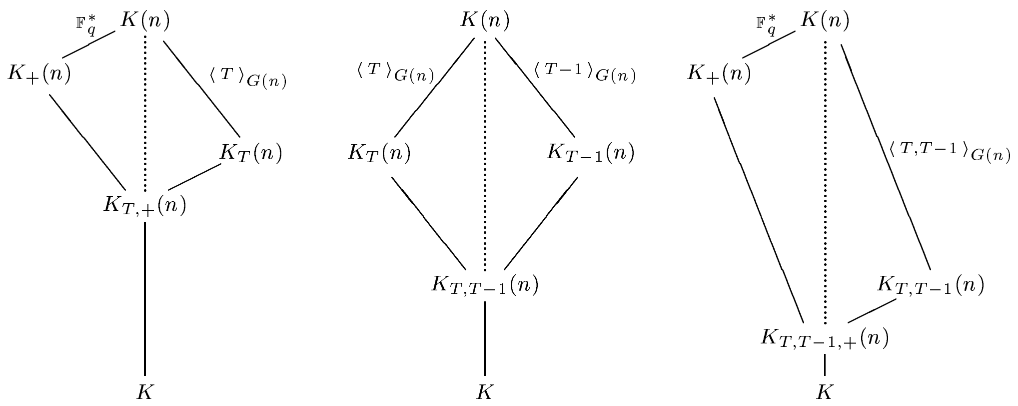
$$Z_{(T)}(K(n)/K) = \langle \sigma_{\overline{T}} \rangle \cong \langle\, T \,\rangle_{G(n)}$$

und

$$Z_{(T-1)}(K(n)/K) = \langle \sigma_{\overline{T-1}} \rangle \cong \langle\, T-1 \,\rangle_{G(n)}.$$

7.2 Galoisgruppen

Nun lassen sich die Galoisgruppen der zu Beginn des Kapitels genannten Körper bestimmen.



Aus der Galoistheorie wissen wir: sei k ein beliebiger Körper und L/k eine Galoiserweiterung mit Galoisgruppe $G = G(L/k)$. Weiter seien H und H' Untergruppen von G und L^H bzw. $L^{H'}$ die entsprechenden Zwischenerweiterungen, also $G(L/L^H) = H$ bzw. $G(L/L^{H'}) = H'$. Dann ist dem Zwischenkörper $L^H \cap L^{H'}$ die kleinste Untergruppe zugeordnet, die H und H' enthält (vergleiche [Lan93, S. 263]).

Die Gruppe $G(K(n)/K) \cong G(n)$ ist abelsch, also ist das Produkt zweier Untergruppen selbst wieder eine Gruppe, und es ergibt sich für die zugehörigen Zwischenkörper:

Lemma 7.3. *Die Galoisgruppen sind*

$$\begin{aligned} G(K(n)/K_{T,+}(n)) &\cong \langle T \rangle_{G(n)} \mathbb{F}_q^*, \\ G(K(n)/K_{T,T-1}(n)) &\cong \langle T \rangle_{G(n)} \langle T-1 \rangle_{G(n)} = \langle T, T-1 \rangle_{G(n)}, \\ G(K(n)/K_{T,T-1,+}(n)) &\cong \langle T, T-1 \rangle_{G(n)} \mathbb{F}_q^*. \end{aligned}$$

Bemerkung 7.4. (i) Da diese Gruppen als Untergruppen einer abelschen Gruppe Normalteiler sind, sind die beschriebenen Zwischenkörper galoissche Erweiterungen des rationalen Funktionenkörpers K.

(ii) Interessant sind hier nur jene Fälle, bei denen die aus den Schnitten resultierenden Körper eine echte Erweiterung des rationalen Funktionenkörpers K darstellen, die Produkte der Untergruppen also ungleich der ganzen Galoisgruppe sind.

7.3 Projektionsabbildungen

Um die Verzweigungsgruppen der Erweiterung $K(n)/L$ zu bestimmen, wobei L einer der Körper $K_T(n)$, $K_{T,+}(n)$, $K_{T,T-1}(n)$ oder $K_{T,T-1,+}(n)$ ist, muß die entsprechende Galoisgruppe mit den Verzweigungsgruppen der Erweiterung $K(n)/K$ geschnitten werden.
Die i-te Verzweigungsgruppe einer Stelle $\mathfrak{P}$ mit $\mathfrak{P}|\mathfrak{p}_\nu$ für ein $\nu = 1, \ldots, s$ ist nach Proposition 6.2 und Kapitel 2 mit $q_\nu^{\alpha-1} \le i \le q_\nu^\alpha - 1$

$$\begin{aligned}(G(K(n)/K))^\alpha(\mathfrak{P}) &= (G(K(n)_\mathfrak{P}/K_\mathfrak{p}))^\alpha \\ &\cong \begin{cases} G(n_\nu), & \alpha = 0 \\ G(n_\nu)^\alpha = \{b \in G(n_\nu) \,|\, b \equiv 1 \bmod p_\nu^\alpha\}, & \alpha \ge 1. \end{cases}\end{aligned}$$

In einem ersten Schritt werden wir nun diese Gruppen in die Gruppe $G(n)$ einbetten. Dort werden dann die entsprechenden Schnitte

$$(G(K(n)/L))_i(\mathfrak{P}) = (G(K(n)/K))_i(\mathfrak{P}) \cap G(K(n)/L)$$

für $i \ge 0$ gebildet.
Da nur die Mächtigkeiten dieser Gruppen von Interesse sind, werden wir sie als Kern gewisser Abbildungen auffassen, die eben solche Gruppen aufeinander abbilden, deren Mächtigkeiten bekannt sind bzw. sich einfach berechnen lassen.

7.3.1 Einbettungen

Mittels der Einbettung $\iota : G(n_\nu) \hookrightarrow G(n)$ läßt sich die Trägheitsgruppe einer Stelle $\mathfrak{P}$ mit $\mathfrak{P}|\mathfrak{p}_\nu$ beschreiben als

$$(G(K(n)/K))^0(\mathfrak{P}) = \iota(G(n_\nu)) = \{b \in G(n) \,|\, b \equiv 1 \bmod m_\nu\} =: H(n_\nu).$$

Entsprechend erhalten wir für die höheren Verzweigungsgruppen dieser Stelle

$$(G(K(n)/K))^\alpha(\mathfrak{P}) = \{b \in G(n) \,|\, b \equiv 1 \bmod m_\nu p_\nu^\alpha\} =: H(n_\nu)^\alpha$$

für $\alpha = 1, \ldots, r_\nu$.
Die Einbettung von $\mathbb{F}_q^*$ in die Gruppe $G(n)$, also

$$\{b \in G(n) \,|\, \exists \varepsilon \in \mathbb{F}_q^* \text{ mit } b \equiv \varepsilon \bmod n\},$$

wird im folgenden Abschnitt mit F_n bezeichnet.

Proposition 7.5. *Somit erhalten wir als Verzweigungsgruppen in den verschiedenen Teilerweiterungen $K(n)/L$ für jedes $\nu \in \{1, \ldots, s\}$, eine Stelle $\mathfrak{P}|\mathfrak{p}_\nu$ und*

$q_\nu^{\alpha-1} \leq i \leq q_\nu^\alpha - 1$:

$$\begin{aligned}
(G(K(n)/K_T(n))_i(\mathfrak{P}) &= \langle T \rangle_{G(n)} \cap H(n_\nu)^\alpha, \\
(G(K(n)/K_{T,+}(n))_i(\mathfrak{P}) &= \langle T \rangle_{G(n)} F_n \cap H(n_\nu)^\alpha, \\
(G(K(n)/K_{T,T-1}(n))_i(\mathfrak{P}) &= \langle T, T-1 \rangle_{G(n)} \cap H(n_\nu)^\alpha, \\
(G(K(n)/K_{T,T-1,+}(n))_i(\mathfrak{P}) &= \langle T, T-1 \rangle_{G(n)} F_n \cap H(n_\nu)^\alpha.
\end{aligned}$$

7.3.2 Projektionen

Sei $s > 1$. Für jedes $\nu = 1, \ldots, s$ und jedes $\alpha = 0, \ldots r_s$ ist die Projektion

$$\begin{aligned}
\pi_{\nu,\alpha} : G(n) &\longrightarrow G(m_\nu p_\nu^\alpha) \\
b \bmod n &\mapsto b \bmod m_\nu p_\nu^\alpha
\end{aligned}$$

gegeben. Der Kern der Abbildung $\pi_{\nu,\alpha}$ ist $H(n_\nu)^\alpha$.
Schränken wir nun diese Projektion auf die Gruppen ein, die zu den Galoisgruppen der betrachteten Erweiterungen isomorph sind, so sind die Kerne der jeweiligen Einschränkungen gerade die gewünschten Verzweigungsgruppen.

Zu bestimmen bleiben nun noch die Bilder dieser Einschränkungen. Es ergeben sich:

$$\begin{aligned}
\pi_{\nu,\alpha}(F_n) &= F_{m_\nu p_\nu^\alpha} \\
\pi_{\nu,\alpha}(\langle T \rangle_{G(n)}) &= \langle T \rangle_{G(m_\nu p_\nu^\alpha)}, \\
\pi_{\nu,\alpha}(\langle T \rangle_{G(n)} F_n) &= \langle T \rangle_{G(m_\nu p_\nu^\alpha)} F_{m_\nu p_\nu^\alpha}, \\
\pi_{\nu,\alpha}(\langle T, T-1 \rangle_{G(n)}) &= \langle T, T-1 \rangle_{G(m_\nu p_\nu^\alpha)}, \\
\pi_{\nu,\alpha}(\langle T, T-1 \rangle_{G(n)} F_n) &= \langle T, T-1 \rangle_{G(m_\nu p_\nu^\alpha)} \mathbb{F}_{m_\nu p_\nu^\alpha}.
\end{aligned}$$

Somit ist die folgende Aussage gezeigt.

Proposition 7.6. *Die Sequenzen*

$$1 \longrightarrow F_n \cap H(n_\nu)^\alpha \longrightarrow F_n \longrightarrow F_{m_\nu p_\nu^\alpha} \longrightarrow 1$$

$$1 \longrightarrow \langle T \rangle_{G(n)} \cap H(n_\nu)^\alpha \longrightarrow \langle T \rangle_{G(n)} \longrightarrow \langle T \rangle_{G(m_\nu p_\nu^\alpha)} \longrightarrow 1$$

$$1 \longrightarrow \langle T \rangle_{G(n)} F_n \cap H(n_\nu)^\alpha \longrightarrow \langle T \rangle_{G(n)} F_n \longrightarrow \langle T \rangle_{G(m_\nu p_\nu^\alpha)} F_{m_\nu p_\nu^\alpha} \longrightarrow 1$$

$$1 \longrightarrow \langle T, T-1 \rangle_{G(n)} \cap H(n_\nu)^\alpha \longrightarrow \langle T, T-1 \rangle_{G(n)} \longrightarrow \langle T, T-1 \rangle_{G(m_\nu p_\nu^\alpha)} \longrightarrow 1$$

sind exakt.

Und die Mächtigkeiten der höheren Verzweigungsgruppen können nun bestimmt werden.

7.3.3 Mächtigkeiten der Verzweigungsgruppen

Da die Mächtigkeiten der verschiedenen Gruppen in den Geschlechtsberechnungen immer wieder gebraucht werden, führe ich zunächst abkürzende Schreibweisen ein.

Bezeichnungen 7.7. Es seien für $s > 1$ und $f = n$ bzw. $f = m_\nu p_\nu^\alpha$ mit $\nu = 1, \dots, s$ und $\alpha = 1, \dots, r_\nu - 1$

$$\begin{array}{rr} & e_T(f) := |\langle T \rangle_{G(f)}|, \\ \tilde{e}_{T,+}(f) := |\langle T \rangle_{G(f)} \cap F_f|, & e_{T,+}(f) := |\langle T \rangle_{G(f)} F_f|, \\ \tilde{e}_{T,T-1}(f) := |\langle T \rangle_{G(f)} \cap \langle T-1 \rangle_{G(f)}|, & e_{T,T-1}(f) := |\langle T, T-1 \rangle_{G(f)}|, \\ \tilde{e}_{T,T-1,+}(f) := |\langle T, T-1 \rangle_{G(f)} \cap F_f|, & e_{T,T-1,+}(f) := |\langle T, T-1 \rangle_{G(f)} F_f|. \end{array}$$

Ist $s = 1$, so setzen wir $\tilde{e}_*(m_\nu) = 1$ und $e_*(m_\nu) := 1$.

Daraus ergibt sich nun

Korollar 7.8.

$$\begin{array}{rcl} |(G(K(n)/K_T(n))_i(\mathfrak{P})| & = & \frac{e_T(n)}{e_T(m_\nu p_\nu^\alpha)} \quad , \\ |(G(K(n)/K_{T,+}(n))_i(\mathfrak{P})| & = & \frac{e_{T,+}(n)}{e_{T,+}(m_\nu p_\nu^\alpha)} \quad , \\ |(G(K(n)/K_{T,T-1}(n))_i(\mathfrak{P})| & = & \frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu p_\nu^\alpha)} \quad , \\ |(G(K(n)/K_{T,T-1,+}(n))_i(\mathfrak{P})| & = & \frac{e_{T,T-1,+}(n)}{e_{T,T-1,+}(m_\nu p_\nu^\alpha)} \quad . \end{array}$$

Bemerkung 7.9. (i) Zur Berechnung von beispielsweise $e_{T,T-1}(n)$ kann hier nun die Beziehung

$$|\langle T, T-1 \rangle_{G(n)}| = \frac{|\langle T \rangle_{G(n)}||\langle T-1 \rangle_{G(n)}|}{|\langle T \rangle_{G(n)} \cap \langle T-1 \rangle_{G(n)}|} = \frac{e_T(n) \cdot e_{T-1}(n)}{\tilde{e}_{T,T-1}(n)}$$

genutzt werden. Dies vereinfacht die Berechnung einzelner konkreter Beispiele sehr (vergleiche Anhang A).

(ii) Die in Kapitel 6 elementar ausgerechneten Trägheitsgruppen von $K(n)/K_+(n)$ lassen also auch mit dieser Methode berechnen, denn als Verzweigungsindex einer endlichen Stelle $\mathfrak{q}$ mit $\mathfrak{q}|\mathfrak{p}_\nu$ für ein $\nu = 1, \dots, s$ ergibt sich hier für $s > 1$

$$e_{\mathfrak{p}_\nu}(K(n)/K_+(n)) = \left| ker(\pi_{\nu,0}\big|_{F_n}) \right| = \frac{|F_n|}{|F_n|} = 1.$$

(iii) Auch für den Fixkörper $K_T(n)$ können diese Größen elementar bestimmt werden. Diese Berechnung werde ich im folgenden Absatz vorstellen.

(iv) Die Mächtigkeiten der übrigen Gruppen lassen sich jedoch nicht mehr auf solch elementaren Wegen berechnen.

7.3.4 Elementare Berechnung von $|H(n_\nu)^\alpha \cap \langle T \rangle_{G(n)}|$

Der Schnitt $H(n_\nu)^\alpha \cap \langle T \rangle_{G(n)}$ ist gerade die Menge der Potenzen von T, für die gilt:

$$T^k \equiv 1 \bmod m_\nu \quad \text{und} \quad T^k \equiv 1 \bmod p_\nu^\alpha.$$

Dies gilt genau dann, wenn sowohl $e_T(m_\nu)$ als auch $e_T(p_\nu^\alpha)$ Teiler von k sind, d.h.

$$k \equiv 0 \begin{cases} \bmod & e_T(m_\nu) \\ \bmod & e_T(p_\nu^\alpha) \end{cases}.$$

Dazu äquivalent ist die Forderung, daß

$$k \equiv 0 \bmod M$$

ist, wobei $M = \mathrm{kgV}(e_T(p_\nu^\alpha), e_T(m_\nu))$ ist.
Ohne Einschränkung können wir $k \leq e_T(n)$ wählen und in einem minimalen Repräsentantensytem von $\mathbb{Z}/e_T(n)\mathbb{Z}$ die Zahl jener Repräsentanten k ermitteln, die $k \equiv 0 \bmod e_T(p_\nu^\alpha)$ sind. Beachten wir nun, daß M ein Teiler von $e_T(n)$ ist, so erhalten wir $\frac{e_T(n)}{M}$ Repräsentanten, die diese Bedingung erfüllen.
Aus dem chinesichen Restsatz folgt, daß $e_T(m_\nu p_\nu^\alpha) = M$ ist, was im Anhang A näher beschrieben wird. Somit ergibt sich

$$|H(n_\nu)^\alpha \cap \langle T \rangle_{G(n)}| = \frac{e_T(n)}{e_T(m_\nu p_\nu^\alpha)}.$$

7.4 Geschlechtsberechnungen

Nun lassen sich Formeln zur Berechnung der Geschlechter dieser Zwischenkörper angeben, die mehr oder weniger "geschlossen" sind.
Während sich das Geschlecht von $K(n)$ und $K_+(n)$ allein durch Berücksichtigung bereits bekannter Daten ermitteln läßt, treten hier nun Größen auf, die nicht im Vorfeld gegeben oder direkt zu ermitteln sind.
So sind die nun folgenden Formeln insofern nicht geschlossen, als in jedem Fall die Erzeugnisse von T und gegebenenfalls $T-1$ als Elemente verschiedener Gruppen betrachtet werden müssen, die stets nur als empirische Daten zur Verfügung stehen, deren numerischen Berechnung wir uns in Anhang A widmen werden.
Zugleich sind die Formeln aber so explizit, daß sie ein sofortiges Ausrechnen einiger Beispiele oder auch die Erstellung eines Computerprogrammes ermöglichen.

Sei L einer der Körper $K_T(n)$, $K_{T,+}(n)$, $K_{T,T-1}(n)$ oder $K_{T,T-1,+}(n)$ und $L' = \overline{\mathbb{F}}_q L$ die entsprechende Konstantenerweiterung.

Aus der Riemann–Hurwitz–Formel

$$2g(K(n))-2=[K(n):L](2g(L)-2)+\sum_{\mathfrak{q}\in S(L')}\sum_{i=0}^{\infty}(g_i(\mathfrak{q})-1)$$

ergibt sich für das Geschlecht von L

$$g(L)=1+\frac{1}{[K(n):L]}\left(g(K(n))-1-\frac{1}{2}\sum_{\mathfrak{q}\in S(L')}\sum_{i=0}^{\infty}(g_i(\mathfrak{q})-1)\right).$$

Wählen wir nun für jedes $\nu=1,\dots,s$ ein $\mathfrak{q}_\nu\in S(L')$ mit $\mathfrak{q}_\nu|\mathfrak{p}_\nu$ und bezeichnen

$$a_\nu(L'):=\sum_{i=0}^{\infty}(g_i(\mathfrak{q}_\nu)-1),$$

so erhalten wir

$$\begin{aligned} g(L) &= 1+\frac{1}{[K(n):L]}\Bigg(g(K(n))-1 \\ &\quad -\frac{1}{2}\left[\frac{\varphi(n)}{q-1}\left(e_\infty(K(n)/L)-1\right)+\sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(L')\right]\Bigg). \end{aligned}$$

Unter Verwendung der Ergebnisse und Bezeichnungen des vorangegangenen Abschnittes lassen sich nun die Geschlechter der verschiedenen Fixkörper ermitteln.

Formel 7.10. Für $K_T(n)$ erhalten wir

$$\begin{aligned} g(K_T(n)) &= 1+\frac{1}{[K(n):K_T(n)]}\Bigg(g(K(n))-1-\frac{1}{2}\Bigg[\frac{\varphi(n)}{q-1}\left(|\langle\, T\,\rangle_{G(n)}\cap F_n|-1\right) \\ &\quad +\sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(K'_T(n))\Bigg]\Bigg) \\ &= 1+\frac{1}{e_T(n)}\Bigg(g(K(n))-1-\frac{1}{2}\Bigg[\frac{\varphi(n)}{q-1}\left(\tilde{e}_{T,+}(n)-1\right) \\ &\quad +\sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(K'_T(n))\Bigg]\Bigg) \end{aligned}$$

mit

$$\begin{aligned}
a_\nu(K'_T(n)) &= \sum_{i=0}^{\infty}(g_i(\mathfrak{q}_\nu)-1) = \sum_{i=0}^{q_\nu^{r_\nu-1}-1}(g_i(\mathfrak{q}_\nu)-1) \\
&= \left|H(n_\nu)\cap\langle T\rangle_{G(n)}\right| - 1 + \sum_{\alpha=1}^{r_\nu-1}\sum_{i=q_\nu^{\alpha-1}}^{q_\nu^{\alpha}-1}\left(\left|H(n_\nu)^\alpha\cap\langle T\rangle_{G(n)}\right|-1\right) \\
&= \frac{e_T(n)}{e_T(m_\nu)} - 1 + \sum_{\alpha=1}^{r_\nu-1}(q_\nu - q_\nu^{\alpha-1})\left(\frac{e_T(n)}{e_T(m_\nu p_\nu^\alpha)}-1\right) \\
&= \frac{e_T(n)}{e_T(m_\nu)} - 1 + (q_\nu-1)\sum_{\alpha=1}^{r_\nu-1} q_\nu^{\alpha-1}\left(\frac{e_T(n)}{e_T(m_\nu p_\nu^\alpha)}\right) - q_\nu^{r_\nu-1}.
\end{aligned}$$

Formel 7.11. Der Schnitt von $K_T(n)$ mit $K_+(n)$ hat das Geschlecht

$$\begin{aligned}
g(K_{T,+}(n)) &= 1 + \frac{1}{e_{T,+}(n)}\Bigg(g(K(n)) - 1 - \frac{1}{2}\Bigg[\frac{\varphi(n)}{q-1}(q-2) \\
&\qquad + \sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(K'_{T,+}(n))\Bigg]\Bigg)
\end{aligned}$$

mit

$$a_\nu(K'_{T,+}(n)) = \frac{e_{T,+}(n)}{e_{T,+}(m_\nu)} + (q_\nu-1)\left(\sum_{\alpha=1}^{r_\nu-1} q_\nu^{\alpha-1}\frac{e_{T,+}(n)}{e_{T,+}(m_\nu p_\nu^\alpha)}\right) - q_\nu^{r_\nu-1}.$$

Formel 7.12. Das Geschlecht von $K_{T,T-1}(n)$ ist

$$\begin{aligned}
g(K_{T,T-1}(n)) &= 1 + \frac{1}{e_{T,T-1}(n)}\Bigg(g(K(n)) - 1 - \frac{1}{2}\Bigg[\frac{\varphi(n)}{q-1}(\tilde{e}_{T,T-1,+}(n)-1) \\
&\qquad + \sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(K'_{T,T-1}(n))\Bigg]\Bigg)
\end{aligned}$$

mit

$$a_\nu(K'_{T,T-1}(n)) = \frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu)} + (q_\nu-1)\left(\sum_{\alpha=1}^{r_\nu-1} q_\nu^{\alpha-1}\frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu p_\nu^\alpha)}\right) - q_\nu^{r_\nu-1}.$$

Formel 7.13. Für den Körper $K_{T,T-1,+}(n)$ ergibt sich

$$\begin{aligned}
g(K_{T,T-1,+}(n)) &= 1 + \frac{1}{e_{T,T-1,+}(n)}\Bigg(g(K(n)) - 1 - \frac{1}{2}\Bigg[\frac{\varphi(n)}{q-1}(q-2) \\
&\qquad + \sum_{\nu=1}^{s}\varphi(m_\nu)d_\nu\cdot a_\nu(K'_{T,T-1,+}(n))\Bigg]\Bigg)
\end{aligned}$$

mit

$$a_\nu(K'_{T,T-1,+}(n)) = \frac{e_{T,T-1,+}(n)}{e_{T,T-1,+}(m_\nu)} + (q_\nu - 1)\left(\sum_{\alpha=1}^{r_\nu-1} q_\nu^{\alpha-1}\frac{e_{T,T-1,+}(n)}{e_{T,T-1,+}(m_\nu p_\nu^\alpha)}\right) - q_\nu^{r_\nu-1}.$$

7.5 Rationale Punkte

Nach Kapitel 4 entsprechen den rationalen Punkten der Kurve, die einem algebraischen Funktionenkörper zugeordnet werden kann, gerade die rationalen Stellen dieses Körpers. Die Anzahl der "sicheren" rationalen Stellen läßt sich nun allein aus der Wahl des Zwischenkörpers und dem Grad der Erweiterung von $K_*(n)/K$ ermitteln, wobei $*$ für einen der Indizes "T", "$T,+$", "$T, T-1$" oder "$T, T-1, +$" steht. Da (T), $(T-1)$ und ∞ im Körper K rationale Stellen sind, sind alle über diesen Stellen in ihren Zerlegungskörpern liegende Stellen ebenfalls rational. Gleiches gilt dann auch für die entsprechenden Schnitte. Sei die Zahl der so bestimmten rationalen Stellen mit $N(K_*(n))$ bezeichnet. Es ist

$$\begin{aligned}[K_*(n):K] &= [K(n):K_*(n)]^{-1}\cdot[K(n):K]\\ &= e_*(n)^{-1}\cdot\varphi(n).\end{aligned}$$

Proposition 7.14. *Für $q \neq 2$ ergibt sich:*

$$\begin{aligned}N(K_T(n)) &= \tfrac{\varphi(n)}{e_T(n)},\\ N(K_{T,+}(n)) &= 2\cdot\tfrac{\varphi(n)}{e_{T,+}(n)},\\ N(K_{T,T-1}(n)) &= 2\cdot\tfrac{\varphi(n)}{e_{T,T-1}(n)},\\ N(K_{T,T-1,+}(n)) &= 3\cdot\tfrac{\varphi(n)}{e_{T,T-1,+}(n)}.\end{aligned}$$

Bemerkung 7.15. Ist $q = 2$, so ist die ∞-Stelle voll zerlegt in der Erweiterung $K(n)/K$, so daß sich in diesem Spezialfall

$$\begin{aligned}N(K_T(n)) &= 2\cdot\frac{\varphi(n)}{e_T(n)} \qquad \text{und}\\ N(K_{T,T-1}(n)) &= 3\cdot\frac{\varphi(n)}{e_{T,T-1}(n)}\end{aligned}$$

ergibt.

Darüber hinaus ist dann auch die Methode des Abstiegs von $K(n)$ zu Schnitten von Zerlegungskörpern $\mathbb{F}_2(T)$-rationaler Stellen voll ausgeschöpft, da der Körper $\mathbb{F}_2(T)$ nur drei rationale Stellen hat.

7.6 Beispiele

In den einzelnen Beispielen werden wir die Zahl der rationalen Stellen eines Körpers L immer wieder mit oberen Schranken für die maximale Anzahl rationaler Stellen vergleichen. Eine Schranke ist die Serre–Schranke

$$|\mathcal{N}(X_f(F)) - (q+1)| \leq g[2\sqrt{q}]$$

(vergleiche Seite 41). Verschiedene Autoren arbeiteten an einer Verbesserung dieser Schranke, was beispielsweise in [NX99] beschrieben ist. Als obere Schranken ziehe ich für $q = 2$ die von Frau Seibert in [Sei98] ermittelten heran. Sie verwendete dabei die Methode von Serre, die die expliziten Formeln von Weil nutzt. Für kleinere Geschlechter finden sich Tabellen in [NX99] und [XN96]. Dort finden sich für $q = 3$ ebenfalls untere Schranken.

Wir betrachten zunächst zwei Beispiele über dem Körper $\mathbb{F}_3(T)$.

Beispiel 7.16. Für $n = T^4 + 2T^3 + T^2 + 2T + 1$ erhalten wir den Körper $K(n)$ vom Geschlecht 99. Der Zerlegungskörper der ∞-Stelle hat das Geschlecht $g(K_{T,+}(n)) = 7$ und 16 rationale Stellen, eine obere Schranke ist hier 17. Der Schnitt der drei betrachteten Zerlegunsgkörper $K_{T,T-1,+}(n)$ hat das Gechlecht 1 und nach unserer Rechnung mindestens 6 rationale Stellen, optimal sind 7.

Beispiel 7.17. Ist $n = T^3 + 2T^2 + 2T + 1$, so ist $g(K(n)) = 19$. Der Körper $K_+(n)$ hat das Geschlecht $g(K_+(n)) = 6$ und wenigstens 13 rationale Stellen. Demgegenüber steht 15 als obere Schranke für die Maximalzahl der rationalen Punkte.

Binäre Funktionenkörper

Über dem Körper $K := \mathbb{F}_2(T)$ ergeben sich nun einige interessante Beispiele. Das Polynom n ist im folgenden stets in der Primfaktorzerlegung angegeben.

Für kleinere Geschlechter finden sich Kurven, die genau eine obere Schranke erreichen.

Beispiel 7.18. Der Körper $K_{T,T-1}(n)$ mit

$$n = (T^3 + T^2 + 1)^2 (T^{14} + T^{13} + T^{10} + T^9 + T^8 + T^7 + 1)$$

hat das Geschlecht 2 und 6 rationale Stellen.
Dabei ist $\varphi(n) = 917448$ und $e_{T,T-1}(n) = 458724$, so daß der Erweiterungsgrad $[K_{T,T-1}(n) : K] = 2$ ist. Das Geschlecht von $K(n)$ ist $g(K(n)) = 8060045$. Aus

$$\begin{aligned} g(K_{T,T-1}(n)) &= 1 + \frac{1}{e_{T,T-1}(n)} \Bigg(g(K(n)) - 1 \\ &\quad - \frac{1}{2} \left[\sum_{\nu=1}^{s} \varphi(m_\nu) d_\nu \cdot a_\nu(K'_{T,T-1}(n)) \right] \Bigg) \end{aligned}$$

mit

$$a_\nu(K'_{T,T-1}(n)) = \frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu)} + (q_\nu - 1)\sum_{\alpha=1}^{r_\nu - 1} q_\nu^{\alpha-1}\left(\frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu p_\nu^\alpha)}\right) - q_\nu^{r_\nu - 1},$$

also

$$\begin{aligned}
a_1(K'_{T,T-1}(n)) &= \frac{e_{T,T-1}(n)}{e_{T,T-1}(m_1)} + (2^3-1)\frac{e_{T,T-1}(n)}{e_{T,T-1}(m_1 p_1)} - 2^3 \\
&= \frac{458724}{16383} + 7 \cdot \frac{458724}{114681} - 8 \\
&= 48, \\
a_2(K'_{T,T-1}(n)) &= \frac{e_{T,T-1}(n)}{e_{T,T-1}(m_2)} - 1 \\
&= \frac{458724}{28} - 1 \\
&= 16382,
\end{aligned}$$

ergibt sich hier

$$\begin{aligned}
g(K_{T,T-1}(n)) &= 1 + \frac{1}{458724}(8060045 - 1 \\
&\quad -\frac{1}{2}[3 \cdot 16383 \cdot 48 + 14 \cdot 56 \cdot 16382]) \\
&= 2.
\end{aligned}$$

Beispiel 7.19. Der Körper $K_{T,T-1}(n)$ mit

$$n = (T^4+T+1)^2(T^5+T^4+T^2+T+1)(T^7+T^5+T^4+T^3+T+1)$$

hat das Geschlecht 9 und 12 rationale Stellen. Hier ist $\varphi(n) = 944880$ und $e_{T,T-1}(n) = 236220$, der Grad der Erweiterung daher $[K_{T,T-1}(n) : K] = 4$.

Beispiel 7.20. Der Körper $K_{T,T-1}(n)$ mit

$$n = (T^3+T^2+1)(T^8+T^6+T^5+T+1)(T^9+T+1)$$

hat das Geschlecht 21 und 21 rationale Stellen. Dabei ist $\varphi(n) = 912135$ und $e_{T,T-1}(n) = 130305$ und somit $[K_{T,T-1}(n) : K] = 7$.

Daneben erhalten wir mit dieser Methode auch solche Beispiele, die sich oberen Schranken annähern.

Beispiel 7.21. Sei nun

$$n = (T^2+T+1)^4(T^6+T^3+1)(T^6+T^5+T^4+T^2+1).$$

Dann ist $\varphi(n) = 762048$ und $e_{T,T-1}(n) = 63504$. Der Körper $K_{T,T-1}(n)$ hat das Geschlecht 51 und 36 rationale Stellen. Dies ist ein weiteres Beispiel für die bisher bekannte beste untere Schranke für die Maximalzahl der rationalen Stellen einer Kurve mit Geschlecht 51 über einem rationalen binären Funktionenkörper. Eine obere Schranke ist hier $N_2(g) = 41$.

Des weiteren lassen sich mit dieser Methode drei bekannte untere Schranken verbessern.

Beispiel 7.22. Wählen wir das Polynom

$$n = (T^4+T^3+1)(T^4+T^3+T^2+T^1+1)$$

mit $\varphi(n) = 225$ und $e_T(n) = 15$, so hat der Körper $K_T(n)$ das Geschlecht 38 und 30 rationale Punkte. Hier ist eine obere Schranke $N_2(g) = 33$.

Beispiel 7.23. Der Körper $K_{T,T-1}(n)$ mit

$$n = (T^3+T^2+1)^3(T^2+T+1)^2,$$

wobei $\varphi(n) = 5376$ und $e_{T,T-1}(n) = 336$ ist, hat das Geschlecht 66 und 48 rationale Stellen. Als obere Schranke betrachten wir hier $N_2(66) = 50$.

Beispiel 7.24. Ist nun

$$n = (T^3+T^2+1)^2(T^3+T+1)(T^{11}+T^{10}+T^9+T^7+1),$$

so ist $\varphi(n) = 802424$ und $e_T(n) = 28658$, und der Körper $K_T(n)$ hat das Geschlecht 81 und 56 rationale Stellen. Eine obere Schranke ist $N_2(81) = 59$.

Auch im Bereich grösserer Geschlechter finden sich einige interessante Beispiele, die ich in Anhang B anführe.

7.7 Weitere Aussichten

Die Methode des Abstieges ist auch für $q = 2$ mit dieser Arbeit keineswegs voll ausgeschöpft. Betrachten wir nämlich das Erzeugnis $U := \langle T, T-1, f \rangle_{G(n)}$, wobei $f \in A$ ein beliebiges, zu n teilerfremdes Polynom ist, und den zugehörigen Fixkörper $L := K(n)^U$, so liegt dieser zwischen $K_{T,T-1}(n)$ und K.

Auch hier sind die drei in K rationalen Stellen voll zerlegt, so daß die Zahl der sicheren rationalen Stellen recht "groß" ist. In einigen Fällen wird auch das Geschlecht $g(L)$ soviel kleiner werden, daß sich gute Beispiele für untere Schranken ergeben können.

Ebenso kann ein Körper $K \subset L \subset K_T(n)$ bestimmt werden, für den die Erweiterung $K(n)/L$ die Galoisgruppe $\langle T, f \rangle_{G(n)}$ hat. Insbesondere dann, wenn das Erzeugnis $\langle T, T-1 \rangle_{G(n)}$ "sehr groß" ist, der Körper $K_{T,T-1}(n)$ nur noch eine kleine oder keine Erweiterung des Körpers K darstellt, und $\langle T \rangle_{G(n)}$ "weniger groß" ist, können auf diese Weise unter Umständen interessante Beispiele zu finden sein.

Wir können zudem die Erweiterung $K_{T,T-1}(n)/K$ betrachten und hier ohne Berücksichtigung der oberen Erweiterung Zwischenkörpern ermitteln sowie deren Geschlecht berechnen. Für diese Methoden möchte ich je ein Beispiel angeben.

Beispiel 7.25. Dazu betrachten wir nun zunächst

$$G(n)/\langle T,T-1\rangle_{G(n)} \left\{ \begin{array}{c} K_{T,T-1}(n) \\ | \\ L \\ | \\ K \end{array} \right. \begin{array}{l} \left.\begin{array}{c} \\ \\ \end{array}\right\} V \\ \left.\begin{array}{c} \\ \\ \end{array}\right\} (G(n)/\langle T,T-1\rangle_{G(n)})/V \end{array}$$

In $K_{T,T-1}(n)$ gilt für eine Stelle $\mathfrak{p}'_\nu$ mit $\mathfrak{p}'_\nu | \mathfrak{p}_\nu$ für ein $\nu = 1, \ldots, s$ nach Proposition 2.9

$$\begin{aligned} (G(n)/\langle T,T-1\rangle_{G(n)})^\alpha &= {(G(n)^\alpha \langle T,T-1\rangle_{G(n)})}/{\langle T,T-1\rangle_{G(n)}} \\ &= {(H(n_\nu)^\alpha \langle T,T-1\rangle_{G(n)})}/{\langle T,T-1\rangle_{G(n)}} \end{aligned}$$

für $\alpha = 0, \ldots, r_\nu$. Die angegebenen Beispiele im vorangegangenen Teil zeigen, daß die verschiedenen Gruppen, die hier zu betrachten sind, teilweise recht groß sind und sich somit nur schlecht berechnen lassen.
Berücksichtigen wir jedoch, daß der Verzweigungsindex einer Stelle in L/K stets auch zugleich Teiler der Ordnung der Galoisgruppe sein muß und zudem auch den Verzweigungsindex der Erweiterung $K_{T,T-1}(n)/K$ teilen muß, können wir in speziellen Situationen allein aus den Gruppenmächtigkeiten Aussagen über das Verzweigungsverhalten machen.
Gilt nämlich $2 \nmid t$, wobei $[K_{T,T-1}(n) : K] =: t$ sein soll, so tritt keine höhere Verzweigung in der Erweiterung $K_{T,T-1}(n)/K$ auf. Existiert darüber hinaus eine Primzahl $m > 2$ mit $m | t$ und $m | e_{\mathfrak{p}_\nu}(K_{T,T-1}(n)/K)$ sowie $m^2 \nmid t$ für ein

$\nu = 1, \dots, s$, so verzweigt eben jene Stelle $\mathfrak{p}_\nu$ in der Erweiterung L/K vom Grad m voll.
Aus der Gruppentheorie folgt

$$\begin{aligned} |H(n_\nu)\langle T, T-1\rangle_{G(n)}| &= \frac{|H(n_\nu)||\langle T, T-1\rangle_{G(n)}|}{|H(n_\nu) \cap \langle T, T-1\rangle_{G(n)}|} \\ &= \frac{\varphi(n_\nu) e_{T,T-1}(n)}{\frac{e_{T,T-1}(n)}{e_{T,T-1}(m_\nu)}} \qquad = \varphi(n_\nu) e_{T,T-1}(m_\nu) \end{aligned}$$

und somit

$$e_{\mathfrak{p}_\nu}(K_{T,T-1}(n)/K) = |(G(n)/\langle T, T-1\rangle_{G(n)})^0| = \frac{\varphi(n_\nu) e_{T,T-1}(m_\nu)}{e_{T,T-1}(n)}.$$

Der Verzweigungsindex läßt sich also in speziellen Fällen aus bereits bekannten Daten ermitteln.

Für $n = \prod_{\nu=1}^{5} n_\nu$ mit

$$\begin{aligned} &n_1 = (T^2 + T + 1)^2, \quad n_2 = (T^3 + T^2 + 1), \quad n_3 = (T^4 + T^3 + 1), \\ &n_4 = (T^4 + T + 1), \quad n_5 = \ (T^4 + T^3 + T^2 + T + 1) \end{aligned}$$

führen wir nun diese Berechnungen explizit aus.
Aus der Tabelle in Anhang B erhalten wir die Daten $g(K_{T,T-1}(n)) = 238$ und $[K_{T,T-1}(n) : K] = 45$. Zudem liefert das Programm, mit dessen Hilfe die Daten erechnet wurden, noch

$$\begin{aligned} e_{T,T-1}(n) = 6300, \quad e_{T,T-1}(m_1) = 1575, \quad e_{T,T-1}(m_2) = 900, \\ e_{T,T-1}(m_3) = 6300, \quad e_{T,T-1}(m_4) = 6300, \quad e_{T,T-1}(m_5) = 6300. \end{aligned}$$

Für die Verzweigungsindizes der verzweigten Stellen ergibt sich daraus

$$\begin{aligned} e_{\mathfrak{p}_1}(K_{T,T-1}(n)/K) &= \tfrac{2^2\cdot(2^2-1)\cdot 1575}{6300} = 3, \\ e_{\mathfrak{p}_2}(K_{T,T-1}(n)/K) &= \tfrac{(2^3-1)\cdot 900}{6300} = 1, \\ e_{\mathfrak{p}_3}(K_{T,T-1}(n)/K) &= \tfrac{(2^4-1)\cdot 6300}{6300} = 15, \\ e_{\mathfrak{p}_4}(K_{T,T-1}(n)/K) &= \tfrac{(2^4-1)\cdot 6300}{6300} = 15, \\ e_{\mathfrak{p}_5}(K_{T,T-1}(n)/K) &= \tfrac{(2^4-1)\cdot 6300}{6300} = 15. \end{aligned}$$

Wählen wir nun $[K_{T,T-1}(n) : L] = 5$, dann ist

$$e_{\mathfrak{p}_\nu}(K_{T,T-1}(n)/L) = \begin{cases} 1 & \text{für} \quad \nu = 1, 2 \\ 5 & \text{für} \quad \nu = 3, 4, 5 \end{cases}$$

und die Zerlegung der $\mathfrak{p}_\nu$ für $\nu = 3, 4, 5$ ist 15. Nun läßt sich das Geschlecht des Körpers L berechnen:

$$g(L) = 1 + \frac{1}{5}(238 - 1 - \frac{1}{2} \cdot 3 \cdot 3 \cdot 4 \cdot (5 - 1)) = 34.$$

Die Zahl der K-rationalen Stellen ist $27 = 3 \cdot [L : K]$.

Beispiel 7.26. Wählen wir die Methode des weiteren Abstieges, so lassen sich die Erkenntnisse aus Abschnitt 7.3 nutzen, um die Mächtigkeiten der höheren Verzweigungsgruppen in einer Erweiterung $K(n)/L$ mit Galoisgruppe $\langle\, T, T - 1, f\,\rangle_{G(n)}$ zu berechnen.
Betrachten wir die exakte Sequenz

$$1 \to \langle\, T, T-1, f\,\rangle_{G(n)} \cap H(n_\nu)^\alpha \to \langle\, T, T-1, f\,\rangle_{G(n)} \to \langle\, T, T-1, f\,\rangle_{G(m_\nu p_\nu^\alpha)} \to 1,$$

so ergibt sich für die Verzweigungsgruppen

$$|\langle\, T, T-1, f\,\rangle_{G(n)} \cap H(n_\nu)^\alpha| = \frac{|\langle\, T, T-1, f\,\rangle_{G(n)}|}{|\langle\, T, T-1, f\,\rangle_{G(m_\nu p_\nu^\alpha)}|} := \frac{e(n)}{e(m_\nu p_\nu^\alpha)}.$$

Wir erhalten also in

$$g(L) = 1 + \frac{1}{[K(n) : L]} \left(g(K(n)) - 1 - \frac{1}{2} \sum_{\nu=1}^{s} \varphi(m_\nu) \cdot d_\nu \cdot a_\nu(L') \right)$$

für alle $a_\nu(L')$, wobei mit $L' = \overline{\mathbb{F}}_q L$ ist,

$$a_\nu(L') = \frac{e(n)}{e(m_\nu)} + (q_\nu - 1) \sum_{\alpha=1}^{r_\nu - 1} q_\nu^{\alpha-1} \frac{e(n)}{e(m_\nu p_\nu^\alpha)} - q_\nu^{r_\nu - 1}.$$

Nun führen wir dies an einem konkreten Beispiel durch.
Für $n = (T^2 + T + 1)^4 (T^3 + T^2 + 1)^2 = n_1 n_2$ ist

$$g(K(n)) = 58625, \quad g(K_{T,T-1}(n)) = 161 \quad \text{und} \quad [K_{T,T-1}(n) : K] = 32.$$

Als dritten Erzeugenden wählen wir nun $f = (T^6 + T^5 + T^4 + T^3 + T + 1)^{21}$. Dabei ist die Wahl von $\widetilde{f} = (T^6 + T^5 + T^4 + T^3 + T + 1)$ zufällig gewesen. Dieses Polynom hat in $G(n)$ die Ordnung $42 = 2 \cdot 3 \cdot 7$. Der Erweiterungsgrad $K_{T,T-1}(n)/K$ ist eine Potenz von 2. Also genügt es, $\widetilde{f}^{21}$ zu betrachten. Wir erhalten nun

$$\begin{array}{rcrrcrrcr}
\varphi(n) & = & 10752, & \varphi(n_2) & = & 56, & \varphi(n_1) & = & 192, \\
e(n) & = & 672, & e(m_2) & = & 96, & e(m_1) & = & 28, \\
 & & & e(m_2 p_2) & = & 672, & e(m_1 p_1) & = & 84, \\
 & & & & & & e(m_1 p_2) & = & 168, \\
 & & & & & & e(m_1 p_3) & = & 672.
\end{array}$$

Daraus ergibt sich

$$a_1(L') = 80, \quad a_2(L') = 6$$

und das Geschlecht $g(L) = 79$. Dieses Geschlecht hat keiner der betrachteten Zerlegungskörper (vergleiche Anhang B). Die Zahl der sicheren rationalen Punkte ist hier $N(L) = 48$.

Beispiel 7.27. Analog zu Beispiel 7.26 erhalten wir hier aus der exakten Sequenz

$$1 \to \langle T, f \rangle_{G(n)} \cap H(n_\nu)^\alpha \to \langle T, f \rangle_{G(n)} \to \langle T, f \rangle_{G(m_\nu p_\nu^\alpha)} \to 1$$

die Mächtigkeiten der höheren Verzweigungsgruppen:

$$|\langle T, f \rangle_{G(n)} \cap H(n_\nu)^\alpha| = \frac{|\langle T, f \rangle_{G(n)}|}{|\langle T, f \rangle_{G(m_\nu p_\nu^\alpha)}|} := \frac{e'(n)}{e'(m_\nu p_\nu^\alpha)} .$$

Hieraus läßt sich nun das Geschlecht eines Körpers L mit $G(K(n)/L) = \langle T, f \rangle_{G(n)}$ berechnen.
Auch hier betrachten wir zur Veranschaulichung ein "Zahlenbeispiel".
Sei $n = (T^4 + T + 1)(T^4 + T^3 + T^2 + T^1 + 1)^2 = n_1 n_2$. Dann ist

$$g(K(n)) = 17041, \quad g(K_T(n)) = 521 \quad \text{und} \quad [K_T(n) : K] = 120.$$

Nun wählen wir das Polynom $f = T^2 + T + 1$ und betrachten den zu $\langle T, f \rangle_{G(n)}$ gehörenden Zwischenkörper L. Aus den Daten

$$\begin{array}{rclrrclrrcl} \varphi(n) &=& 3600, & \varphi(n_1) &=& 15, & \varphi(n_2) &=& 240, \\ e'(n) &=& 900, & e'(m_1) &=& 60, & e'(m_2) &=& 15, \\ &&&&&& e'(m_2 p_2) &=& 225, \end{array}$$

läßt sich nun das Geschlecht von L sowie die Zahl der rationalen Punkte berechnen:

$$g(L) = 67 \quad \text{und} \quad N(L) = 42.$$

Eine systematische Suche nach geeigneten Beispielen gestaltet sich nun jedoch schwieriger als dies für die von mir betrachteten Körper der Fall ist, da nun die Berechnung und Verwaltung der Daten, insbesondere des Erzeugnisses $\langle T, T-1 \rangle_{G(n)}$, teilweise sehr aufwendig wird. Zudem ist eine "geschickte" Wahl des hinzutretenden dritten Erzeugers von einem Computerprogamm nur schlecht zu realisieren.

Anhang A

Numerische Berechnung der $e_*(n)$

Die Ordnung $e_T(n)$ des Polynoms T in der Gruppe

$$G(n) := (A/(n))^*$$

mit $n = \prod_{\nu=1}^{s} p_\nu^{r_\nu}$, wobei $s \in \mathbb{N}$ und $p_\nu \in A$ irreduzible und normierte Polynome vom Grad $deg\ p_\nu = d_\nu$ sowie $q_\nu := q^{d_\nu}$ sind, und mit $n_\nu = p_\nu^{r_\nu}$ die primären Faktoren bezeichnet werden sollen, kann numerisch wie folgt berechnet werden.

Die Ideale (n_ν) und (n_μ) sind für $\nu \neq \mu$ in A komaximal. Daher gilt nach dem chinesischen Restsatz, daß

$$G(n) = (A/(n))^* = \prod_{\nu=1}^{s} (A/(n_\nu))^* = \prod_{\nu=1}^{s} G(n_\nu)$$

ist. Somit ist die Ordnung $e_T(n)$ von T in $G(n)$ gerade

$$e_T(n) = \mathrm{kgV}\left\{e_T(n_\nu)\,,\, i = 1, \ldots , s\right\}.$$

Nun bleibt also nur noch für den primären Fall eine möglichst effektive Berechnung zu ermitteln.

Wir setzen für ein ν nun $p := p_\nu$ und $r := r_\nu$.
Zunächst wird $e_T(p)$ berechnet. Die Mächtigkeit von $G(p)$ ist $q_\nu - 1$. Zur Ermittlung von $e_T(p)$ die Potenzen von T nacheinander berechnet.

Dies liefert dann ein $b = e_T(p) \in \mathbb{N}$ mit $T^b \equiv 1 \bmod p$. Sei $T^b = x$.
Dann läßt sich x "p-adisch" entwickeln mit f_i vom Grad $< q_\nu$

$$x \equiv 1 + f_1 p + f_2 p^2 + \cdots + f_{r-1} p^{r-1} \bmod p^r.$$

Sind alle $f_i = 0$, so ist $e_T(p) = e_T(p^2) = \ldots = e_T(p^{r-1}) = b$. Andernfalls gilt:

Lemma A.1. *Sei β die kleinste Zahl in obiger Darstellung, für die f_β ungleich 0 ist. Dann ist die Ordnung von T in den verschiedenen $G(p^\alpha)$ gleich*

$$e_T(p^\alpha) = l^j b \quad \textit{für} \quad l^{j-1}\beta < \alpha \leq l^j \beta$$

mit $j = 1, \ldots, r$.

Beweis: O.E. rechnen wir mit x statt mit T. Es ist nämlich

$$G(p^\alpha) \cong G(p) \times Q,$$

wobei Q eine l-Gruppe ist (vergleiche Kapitel 2 und 7). Daher ergibt sich die Ordnung von T aus

$$e_T(p^\alpha) = b \cdot e_x(p^\alpha).$$

Es ist

$$x \equiv 1 + f_\beta p^\beta + \ldots + f_{r-1} p^{r-1} \bmod p^r.$$

Sei $k \in \mathbb{N}$ mit $k = l^j m$ mit $j, m \in \mathbb{N}$ und $\mathrm{ggT}(m, l) = 1$, dann ist

$$\begin{aligned} x^k = (x^{l^j})^m \quad & \equiv 1 + m f_\beta^{l^j} p^{\beta l^j} + \{\text{ Terme höherer } p\text{-Potenzen }\} \bmod p^\alpha \\ & \begin{cases} \equiv 1 \bmod p^\alpha, \ \alpha \leq \beta \cdot l^j \\ \not\equiv 1 \bmod p^\alpha, \ \alpha > \beta \cdot l^j. \end{cases} \end{aligned}$$

Daraus ergibt sich für ein fest gewähltes $\alpha \leq r$ mit $\beta \cdot l^{j-1} < \alpha \leq \beta \cdot l^j$

$$e_x(p^\alpha) = \min \{k | x^k \equiv 1 \bmod p^\alpha\} = l^j$$

und somit $e_T(p^\alpha) = b \cdot l^j$. □

Analog wird $e_{T^{-1}}(n)$ berechnet.

Bei der Berechnung von $\tilde{e}_{T,+}(n) = |\langle T \rangle_{G(n)} \cap F_n|$ kann nun genutzt werden, daß nur solche Potenzen von T in Betracht kommen, deren Exponent bereits von der höchsten l-Potenz, die in $e_T(n)$ enthalten ist, geteilt werden.

Gilt also $l^\gamma | e_T(n)$ und $l^{\gamma+1} \not| e_T(n)$, so erhalten wir

$$\{T^{l^\gamma k} \,|\, l^\gamma k \leq e_T(n)\}$$

als Menge der zu überprüfenden Kandidaten.

Zur Berechnung von $\tilde{e}_{T,T-1}(n)$ wird mittels Ausprobieren ein minimales $c \in \mathbb{N}$ bestimmt mit $(T-1)^c \in \langle\, T \,\rangle_{G(n)}$. Daraus erhalten wir dann

$$\tilde{e}_{T,T-1}(n) = \frac{e_{T-1}(n)}{\mathrm{ggT}(e_{T-1}(n), c)}\,.$$

Die Kenntnis eines solchen c läßt sich nun nutzen, um $\tilde{e}_{T,T-1,+}(n)$ zu berechnen. Mit der Darstellung

$$\langle\, T, T-1 \,\rangle_{G(n)} = \{T^x (T-1)^y \mid 0 \leq y < c \text{ und } 0 \leq x < e_T(n)\}$$

erhalten wir für geeignete "Kandidaten", die zugleich in F_n liegen, mit $e_T(n) = l^\delta d$ und $e_{T-1}(n) = l^\varepsilon e$ Ausdrücke der Form

$$T^x (T-1)^y \quad \text{mit} \quad \left\{ \begin{array}{cc} 0 \leq x \leq e_T(n), & 0 \leq y < c \\ l^\delta | x, & l^\varepsilon | y. \end{array} \right\}.$$

Aus diesen Daten lassen sich nun alle anderen Grössen $e_*(n)$ einfach ermitteln, denn es gilt:

$$e_{T,+}(n) = \frac{e_T(n)(q-1)}{\tilde{e}_{T,+}(n)} \quad \text{und} \quad e_{T,T-1}(n) = \frac{e_T(n) e_{T-1}(n)}{\tilde{e}_{T,T-1}(n)}\,.$$

Anhang B

Ausgewählte Beispiele

In Zusammenhang mit dieser Arbeit wurde ein Programm entwickelt, das für Kreisteilungserweiterungen des Körpers $\mathbb{F}_2(T)$ sowohl das Geschlecht als auch die Zahl der sicheren K-rationalen Punkte mittels der angegebenen Formeln berechnete. Ausgewertet wurden die Körper $K_T(n)$, $K_{T-1}(n)$ und $K_{T,T-1}(n)$, wobei der Grad von n kleiner gleich 20 und n teilerfremd zu T und $T-1$ war. Diese Daten wurden dann verglichen mit oberen Schranken, die ich der Staatsexamensarbeit [Sei98] entnommen habe und mit $N_2(g)$ bezeichne.

Insgesamt wurden 1572861 Beispiele gerechnet. Danach wurden eben jene Geschlechter kleiner 1000, für die Beispiele mit

$$\frac{N(L)}{N_2(g)} \geq 0,8$$

errechnet wurden, ermittelt. Aus der Fülle dieser Daten wurden nun zu jedem auftretenden Geschlecht willkürlich zwei konkrete Beispiele ausgewählt, die ich nun im folgenden anführen werde.

Um einen Eindruck von der Menge der Daten zu geben, sei hier ein Beispiel genannt. Für das Geschlecht 9 wurden insgesamt 7010 Körper ermittelt, die alle 12 rationale Stellen haben.
Es ist davon auszugehen, daß zahlreiche der Kurven, die sowohl gleiches Geschlecht als auch gleiche Zahl sicherer rationaler Punkte haben, abstrakt isomorph zueinander sind.

In der nachfolgenden Tabelle ist mit $|G|$ stets die Mächtigkeit der Galoisgruppe von L/K und mit z die Zahl der in K liegenden und in L/K voll zerlegten rationalen Stellen bezeichnet.

g	$N_2(g)$	Polynom in faktorisierter Form	Körper	$\|G\|$	z
2	6	$(T^3+T^2+1)^2(T^{14}+T^{13}+T^{10}+T^9+T^8+T^7+1)$	$K_{T,T-1}(n)$	2	3
		$(T^4+T^3+1)(T^5+T^2+1)\cdot$ $(T^{11}+T^9+T^8+T^6+T^4+T^3+T^2+T+1)$	$K_{T-1}(n)$	3	2
5	9	$(T^2+T+1)^3$	$K_T(n)$	4	2
		$(T^2+T+1)^3$	$K_{T-1}(n)$	4	2
6	10	$(T^2+T+1)(T^3+T^2+1)(T^7+T^4+1)\cdot$ $(T^8+T^7+T^6+T^4+T^2+T+1)$	$K_{T,T-1}(n)$	3	3
		$(T^8+T^6+T^5+T^4+T^3+T+1)\cdot$ $(T^{12}+T^{11}+T^9+T^8+T^4+T^3+T^2+T+1)$	$K_{T,T-1}(n)$	3	3
8	11	$(T^2+T+1)(T^8+T^7+T^3+T^2+1)\cdot$ $(T^{10}+T^9+T^8+T^5+1)$	$K_{T,T-1}(n)$	3	3
		$(T^4+T^3+1)(T^6+T+1)(T^{10}+T^8+T^3+T+1)$	$K_{T,T-1}(n)$	3	3
9	12	$(T^4+T+1)^2(T^5+T^4+T^2+T+1)\cdot$ $(T^7+T^5+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	4	3
		$(T^2+T+1)^2(T^4+T^3+T^2+T^1+1)\cdot$ $(T^5+T^4+T^3+T+1)(T^7+T^6+T^5+T^2+1)$	$K_T(n)$	6	2
11	14	$(T^2+T+1)^2(T^4+T+1)$	$K_T(n)$	6	2
		$(T^2+T+1)^2(T^4+T+1)$	$K_{T-1}(n)$	6	2
12	15	$(T^3+T+1)(T^6+T^4+T^3+T+1)\cdot$ $(T^{11}+T^{10}+T^9+T^8+T^6+T^5+T^3+T+1)$	$K_{T-1}(n)$	7	2
		$(T^3+T+1)(T^6+T^3+1)\cdot$ $(T^{11}+T^{10}+T^7+T^5+T^4+T^3+T^2+T+1)$	$K_T(n)$	7	2
20	21	$(T^3+T^2+1)^2(T^8+T^6+T^5+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	6	3
		$(T^3+T+1)^2(T^2+T+1)(T^6+T^5+T^3+T^2+1)$	$K_{T,T-1}(n)$	6	3
21	21	$(T^2+T+1)(T^9+T^8+T^7+T^3+T^2+T+1)(T^9+T^8+1)$	$K_{T,T-1}(n)$	7	3
		$(T^3+T^2+1)(T^8+T^6+T^5+T+1)(T^9+T+1)$	$K_{T,T-1}(n)$	7	3
22	22	$(T^2+T+1)(T^5+T^3+1)\cdot$ $(T^6+T^5+T^4+T^2+1)(T^7+T^6+T^5+T^4+1)$	$K_T(n)$	9	2
		$(T^2+T+1)(T^5+T^4+T^3+T^2+1)\cdot$ $(T^6+T^5+T^4+T+1)(T^7+T^5+T^3+T+1)$	$K_{T-1}(n)$	9	2
26	25	$(T^2+T+1)^2(T^3+T+1)^2$	$K_{T,T-1}(n)$	8	3
		$(T^2+T+1)^2(T^3+T^2+1)^2$	$K_{T,T-1}(n)$	8	3
28	26	$(T^5+T^4+T^3+T^2+1)^2\cdot$ $(T^3+T+1)(T^7+T^6+T^5+T^2+1)$	$K_{T,T-1}(n)$	8	3
		$(T^5+T^2+1)^2(T^4+T^3+T^2+T^1+1)(T^6+T+1)$	$K_{T,T-1}(n)$	8	3
29	27	$(T^2+T+1)^3(T^4+T^3+1)$	$K_{T-1}(n)$	12	2
		$(T^2+T+1)^3(T^4+T^3+T^2+T^1+1)$	$K_T(n)$	12	2
31	28	$(T^2+T+1)^3(T^4+T^3+1)$	$K_T(n)$	12	2
		$(T^2+T+1)^3(T^4+T^3+T^2+T^1+1)$	$K_{T-1}(n)$	12	2

g	$N_2(g)$	Polynom in faktorisierter Form	Körper	$\lvert G\rvert$	z
32	29	$(T^3+T+1)^2(T^4+T^3+1)$	$K_{T-1}(n)$	12	2
		$(T^3+T^2+1)^2(T^4+T^3+T^2+T^1+1)$	$K_T(n)$	12	2
34	30	$(T^2+T+1)(T^5+T^4+T^2+T+1)\cdot$ $(T^6+T^5+T^3+T^2+1)(T^6+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	9	3
		$(T^2+T+1)(T^5+T^3+T^2+T+1)\cdot$ $(T^6+T^3+1)(T^6+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	9	3
37	32	$(T^2+T+1)^2(T^3+T^2+1)\cdot$ $(T^3+T+1)(T^7+T^5+T^2+T+1)$	$K_{T-1}(n)$	14	2
		$(T^2+T+1)^2(T^3+T^2+1)\cdot$ $(T^3+T+1)(T^7+T^5+T^2+T+1)$	$K_T(n)$	14	2
38	33	$(T^4+T^3+1)(T^4+T^3+T^2+T^1+1)$	$K_T(n)$	15	2
*		$(T^4+T^3+1)(T^4+T^3+T^2+T^1+1)$	$K_{T-1}(n)$	15	2
41	35	$(T^2+T+1)^4$	$K_T(n)$	16	2
*		$(T^2+T+1)^4$	$K_{T-1}(n)$	16	2
42	35	$(T^8+T^5+T^4+T^3+1)$	$K_T(n)$	15	2
		$(T^8+T^5+T^3+T^2+1)$	$K_{T-1}(n)$	15	2
48	39	$(T^3+T+1)^3$	$K_T(n)$	16	2
		$(T^3+T+1)^3$	$K_{T-1}(n)$	16	2
51	41	$(T^2+T+1)^5(T^4+T^3+T^2+T^1+1)\cdot$ $(T^6+T^5+T^3+T^2+1)$	$K_{T,T-1}(n)$	12	3
		$(T^2+T+1)^4(T^6+T^3+1)(T^6+T^5+T^4+T^2+1)$	$K_{T,T-1}(n)$	12	3
53	42	$(T^4+T^3+1)^2(T^2+T+1)(T^4+T^3+T^2+T^1+1)$	$K_{T,T-1}(n)$	12	3
		$(T^4+T^3+T^2+T^1+1)^2(T^6+T^4+T^2+T+1)$	$K_{T,T-1}(n)$	12	3
54	43	$(T^2+T+1)(T^6+T^3+1)$	$K_T(n)$	21	2
		$(T^2+T+1)(T^6+T^4+T^3+T+1)$	$K_{T-1}(n)$	21	2
55	43	$(T^2+T+1)^2(T^6+T^4+T^2+T+1)\cdot$ $(T^7+T^6+T^5+T^4+T^2+T+1)$	$K_T(n)$	18	2
		$(T^2+T+1)^2(T^6+T^5+T^4+T^2+1)\cdot$ $(T^7+T^5+T^4+T^3+T+1)$	$K_T(n)$	18	2
62	48	$(T^3+T^2+1)(T^4+T^3+1)(T^6+T^4+T^3+T+1)\cdot$ $(T^7+T^6+T^5+T^4+1)$	$K_{T-1}(n)$	21	2
		$(T^3+T+1)(T^4+T^3+T^2+T^1+1)\cdot$ $(T^6+T^3+1)(T^7+T^5+T^3+T+1)$	$K_T(n)$	21	2
65	50	$(T^4+T^3+T^2+T^1+1)^2$	$K_T(n)$	24	2
		$(T^4+T^3+1)^2$	$K_{T-1}(n)$	24	2
66	50	$(T^3+T^2+1)^3(T^2+T+1)^2$	$K_{T,T-1}(n)$	16	3
*		$(T^3+T+1)^3(T^2+T+1)^2$	$K_{T,T-1}(n)$	16	3

g	$N_2(g)$	Polynom in faktorisierter Form	Körper	$\|G\|$	z
67	51	$(T^3+T^2+1)(T^6+T^5+T^4+T+1)$	$K_{T-1}(n)$	21	2
		$(T^3+T^2+1)(T^6+T^5+T^4+T^2+1)$	$K_T(n)$	21	2
68	51	$(T^4+T+1)(T^6+T^4+T^3+T+1)$	$K_{T-1}(n)$	21	2
		$(T^4+T+1)(T^6+T^3+1)$	$K_T(n)$	21	2
69	52	$(T^2+T+1)^6(T^8+T^7+T^4+T^3+T^2+T+1)$	$K_{T,T-1}(n)$	16	3
		$(T^4+T^3+1)^3(T^3+T^2+1)(T^5+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	16	3
70	53	$(T^3+T^2+1)(T^4+T^3+1)(T^4+T+1)\cdot$ $(T^4+T^3+T^2+T^1+1)(T^5+T^3+1)$	$K_{T,T-1}(n)$	15	3
*		$(T^3+T^2+1)(T^5+T^4+T^3+T+1)\cdot$ $(T^{12}+T^{11}+T^{10}+T^9+T^8+T^6+T^4+T+1)$	$K_{T,T-1}(n)$	15	3
75	56	$(T^6+T^3+1)^2$	$K_{T,T-1}(n)$	16	3
		$(T^6+T+1)^2$	$K_{T,T-1}(n)$	16	3
76	56	$(T^2+T+1)(T^3+T^2+1)(T^3+T+1)\cdot$ $(T^4+T+1)(T^8+T^7+T^3+T^2+1)$	$K_{T,T-1}(n)$	15	3
		$(T^2+T+1)(T^3+T^2+1)(T^3+T+1)\cdot$ $(T^4+T^3+T^2+T^1+1)(T^8+T^6+T^5+T^2+1)$	$K_{T,T-1}(n)$	15	3
81	59	$(T^3+T^2+1)^2(T^3+T+1)(T^{11}+T^{10}+T^9+T^7+1)$	$K_{T-1}(n)$	28	2
*		$(T^3+T^2+1)^2(T^3+T+1)(T^{11}+T^{10}+T^9+T^7+1)$	$K_T(n)$	28	2
105	73	$(T^2+T+1)^5$	$K_T(n)$	32	2
*		$(T^2+T+1)^5$	$K_{T-1}(n)$	32	2
108	75	$(T^2+T+1)(T^3+T^2+1)\cdot$ $(T^3+T+1)(T^6+T^3+1)$	$K_{T,T-1}(n)$	21	3
*		$(T^2+T+1)(T^3+T^2+1)(T^3+T+1)\cdot$ $(T^6+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	21	3
128	87	$(T^2+T+1)^2(T^3+T+1)^2(T^6+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	24	3
		$(T^2+T+1)^2(T^3+T^2+1)^2(T^6+T^3+1)$	$K_{T,T-1}(n)$	24	3
135	91	$(T^2+T+1)^2(T^3+T^2+1)\cdot$ $(T^6+T^4+T^3+T+1)(T^7+T^5+T^2+T+1)$	$K_{T-1}(n)$	42	2
		$(T^2+T+1)^2(T^3+T^2+1)(T^6+T^3+1)\cdot$ $(T^7+T^3+T^2+T+1)$	$K_T(n)$	42	2
149	99	$(T^3+T^2+1)^4(T^8+T^7+T^6+T^5+T^2+T+1)$	$K_{T,T-1}(n)$	32	3
		$(T^3+T^2+1)^4(T^3+T+1)(T^5+T^4+T^2+T+1)$	$K_{T,T-1}(n)$	32	3
154	101	$(T^2+T+1)(T^3+T+1)(T^4+T^3+T^2+T^1+1)\cdot$ $(T^4+T+1)(T^7+T^6+T^5+T^3+T^2+T+1)$	$K_{T-1}(n)$	45	2
		$(T^2+T+1)(T^3+T+1)(T^4+T^3+T^2+T^1+1)\cdot$ $(T^4+T+1)(T^7+T^6+T^5+T^3+T^2+T+1)$	$K_T(n)$	45	2
161	105	$(T^2+T+1)^4(T^3+T^2+1)^2$	$K_{T,T-1}(n)$	32	3
*		$(T^2+T+1)^4(T^3+T+1)^2$	$K_{T,T-1}(n)$	32	3

g	$N_2(g)$	Polynom in faktorisierter Form	Körper	$\lvert G\rvert$	z
167	109	$(T^3+T^2+1)^3(T^3+T+1)^2(T^5+T^2+1)$	$K_{T,T-1}(n)$	32	3
*		$(T^3+T+1)^3(T^3+T^2+1)^2(T^5+T^4+T^3+T+1)$	$K_{T,T-1}(n)$	32	3
172	112	$(T^2+T+1)^2(T^5+T^4+T^3+T+1)^2$	$K_{T,T-1}(n)$	32	3
		$(T^2+T+1)^2(T^5+T^4+T^2+T+1)^2$	$K_{T,T-1}(n)$	32	3
173	112	$(T^3+T+1)^2(T^4+T+1)^2$	$K_{T,T-1}(n)$	32	3
		$(T^3+T^2+1)^2(T^4+T^3+T^2+T^1+1)^2$	$K_{T,T-1}(n)$	32	3
185	119	$(T^2+T+1)^4(T^3+T+1)(T^4+T^3+1)(T^5+T^2+1)$	$K_{T-1}(n)$	48	2
		$(T^2+T+1)^4(T^3+T^2+1)\cdot$ $(T^4+T^3+1)(T^5+T^4+T^2+T+1)$	$K_{T-1}(n)$	48	2
186	119	$(T^7+T^3+T^2+T+1)^2(T^3+T^2+1)(T^3+T+1)$	$K_{T,T-1}(n)$	32	3
		$(T^7+T^3+1)^2(T^3+T^2+1)(T^3+T+1)$	$K_{T,T-1}(n)$	32	3
238	148	$(T^2+T+1)^2(T^3+T^2+1)(T^4+T^3+1)\cdot$ $(T^4+T+1)(T^4+T^3+T^2+T^1+1)$	$K_{T,T-1}(n)$	45	3
*		$(T^2+T+1)(T^3+T^2+1)(T^3+T+1)\cdot$ $(T^4+T^3+1)(T^4+T+1)(T^4+T^3+T^2+T^1+1)$	$K_{T,T-1}(n)$	45	3
244	151	$(T^2+T+1)(T^3+T+1)(T^4+T+1)\cdot$ $(T^5+T^3+1)(T^6+T^3+1)$	$K_T(n)$	63	2
		$(T^2+T+1)(T^3+T^2+1)(T^4+T^3+1)\cdot$ $(T^5+T^3+T^2+T+1)(T^6+T^3+1)$	$K_T(n)$	63	2
247	153	$(T^2+T+1)(T^3+T+1)\cdot$ $(T^6+T^5+T^4+T+1)$	$K_{T-1}(n)$	63	2
		$(T^2+T+1)(T^3+T^2+1)(T^6+T+1)$	$K_{T-1}(n)$	63	2
250	155	$(T^2+T+1)(T^6+T^5+T^4+T+1)\cdot$ $(T^{12}+T^{11}+T^8+T^6+T^4+T^3+T^2+T+1)$	$K_{T,T-1}(n)$	45	3
		$(T^2+T+1)(T^6+T^5+T^4+T^2+1)\cdot$ $(T^{12}+T^{11}+T^8+T^6+T^4+T^3+T^2+T+1)$	$K_{T,T-1}(n)$	45	3
251	155	$(T^3+T^2+1)^2(T^2+T+1)\cdot$ $(T^3+T+1)(T^6+T^5+T^3+T^2+1)$	$K_{T,T-1}(n)$	42	3
		$(T^3+T+1)^2(T^2+T+1)(T^3+T^2+1)(T^6+T^3+1)$	$K_{T,T-1}(n)$	42	3
261	161	$(T^6+T^3+1)^2(T^2+T+1)(T^6+T+1)$	$K_{T,T-1}(n)$	48	3
		$(T^6+T^4+T^3+T+1)^2(T^2+T+1)(T^6+T+1)$	$K_{T,T-1}(n)$	48	3
281	171	$(T^2+T+1)^2(T^4+T^3+1)^2(T^4+T+1)$	$K_{T,T-1}(n)$	48	3
		$(T^2+T+1)^2(T^4+T^3+T^2+T^1+1)^2(T^4+T+1)$	$K_{T,T-1}(n)$	48	3
293	178	$(T^6+T^5+T^2+T+1)^2(T^4+T+1)$	$K_{T,T-1}(n)$	48	3
		$(T^6+T^5+1)^2(T^4+T+1)$	$K_{T,T-1}(n)$	48	3
339	202	$(T^2+T+1)^3(T^6+T^4+T^3+T+1)$	$K_{T-1}(n)$	84	2
		$(T^2+T+1)^3(T^6+T^3+1)$	$K_T(n)$	84	2

g	$N_2(g)$	Polynom in faktorisierter Form	Körper	$\|G\|$	z
357	212	$(T^3+T+1)^5(T^5+T^4+T^2+T+1)$	$K_{T,T-1}(n)$	64	3
*		$(T^3+T^2+1)^5(T^5+T^3+T^2+T+1)$	$K_{T,T-1}(n)$	64	3
367	217	$(T^2+T+1)^2(T^4+T^3+1)\cdot$ $(T^4+T^3+T^2+T^1+1)$	$K_T(n)$	90	2
		$(T^2+T+1)^2(T^4+T^3+1)\cdot$ $(T^4+T^3+T^2+T^1+1)$	$K_{T-1}(n)$	90	2
368	218	$(T^{10}+T^9+T^8+T^7+T^6+T^5$ $+T^4+T^3+T^2+T+1)$	$K_T(n)$	93	2
		$(T^{10}+T^9+T^8+T^7+T^2+T+1)$	$K_{T-1}(n)$	93	2
369	218	$(T^2+T+1)^2(T^3+T^2+1)^2\cdot$ $(T^3+T+1)^2(T^4+T^3+1)$	$K_{T,T-1}(n)$	64	3
		$(T^2+T+1)^2(T^3+T^2+1)^2\cdot$ $(T^3+T+1)^2(T^4+T^3+T^2+T^1+1)$	$K_{T,T-1}(n)$	64	3
373	220	$(T^4+T+1)^2(T^3+T^2+1)\cdot$ $(T^4+T^3+1)(T^4+T^3+T^2+T^1+1)$	$K_{T,T-1}(n)$	60	3
		$(T^4+T^3+1)^2(T^3+T+1)\cdot$ $(T^4+T+1)(T^4+T^3+T^2+T^1+1)$	$K_{T,T-1}(n)$	60	3
378	223	$(T^2+T+1)^3(T^3+T+1)^3(T^5+T^2+1)$	$K_{T,T-1}(n)$	64	3
		$(T^2+T+1)^3(T^3+T^2+1)^3(T^5+T^4+T^3+T^2+1)$	$K_{T,T-1}(n)$	64	3
381	225	$(T^4+T^3+1)^3(T^2+T+1)^2(T^3+T+1)$	$K_{T,T-1}(n)$	64	3
		$(T^4+T+1)^3(T^2+T+1)^2(T^3+T^2+1)$	$K_{T,T-1}(n)$	64	3
392	231	$(T^5+T^3+1)^3(T^2+T+1)(T^3+T+1)$	$K_{T,T-1}(n)$	64	3
		$(T^5+T^4+T^3+T+1)^3(T^5+T^3+T^2+T+1)$	$K_{T,T-1}(n)$	64	3
393	231	$(T^2+T+1)^4(T^4+T^3+T^2+T^1+1)^2(T^3+T^2+1)$	$K_{T,T-1}(n)$	64	3
		$(T^2+T+1)^4(T^4+T^3+1)^2(T^3+T^2+1)$	$K_{T,T-1}(n)$	64	3
405	237	$(T^3+T+1)^3(T^4+T^3+T^2+T^1+1)^2$	$K_{T,T-1}(n)$	64	3
		$(T^3+T+1)^3(T^4+T^3+1)^2$	$K_{T,T-1}(n)$	64	3
483	278	$(T^3+T^2+1)^3(T^3+T+1)$	$K_T(n)$	112	2
		$(T^3+T^2+1)^3(T^3+T+1)$	$K_{T-1}(n)$	112	2
521	298	$(T^4+T^3+1)^2(T^4+T+1)$	$K_{T-1}(n)$	120	2
		$(T^4+T^3+T^2+T^1+1)^2(T^4+T+1)$	$K_T(n)$	120	2
652	366	$(T^3+T^2+1)(T^3+T+1)\cdot$ $(T^6+T^4+T^2+T+1)(T^7+T^5+T^2+T+1)$	$K_T(n)$	147	2
		$(T^3+T^2+1)(T^3+T+1)\cdot$ $(T^6+T^5+T^4+T^2+1)(T^7+T^6+T^4+T+1)$	$K_T(n)$	147	2
655	367	$(T^3+T^2+1)(T^5+T^4+T^2+T+1)\cdot$ $(T^{12}+T^{11}+T^8+T^6+T^4+T^3+T^2+T+1)$	$K_{T,T-1}(n)$	105	3
		$(T^3+T+1)(T^5+T^3+T^2+T+1)\cdot$ $(T^{12}+T^{11}+T^{10}+T^9+T^8+T^6+T^4+T+1)$	$K_{T,T-1}(n)$	105	3

g	$N_2(g)$	Polynom in faktorisierter Form	Körper	$\|G\|$	z
794	438	$(T^3+T+1)^4(T^2+T+1)^2$	$K_{T,T-1}(n)$	128	3
		$(T^3+T^2+1)^4(T^2+T+1)^2$	$K_{T,T-1}(n)$	128	3
857	470	$(T^3+T^2+1)^3(T^2+T+1)^2(T^3+T+1)^2$	$K_{T,T-1}(n)$	128	3
		$(T^3+T+1)^3(T^2+T+1)^2(T^3+T^2+1)^2$	$K_{T,T-1}(n)$	128	3

Vergleichen wir nun diese Beispiele mit jenen, die von Niederreiter und Xing, [XN95], [NX96], [XN96], [NX97], und von van der Geer und van der Vlugt, [VdGVdV93], [VdGVdV97], so ergeben sich für die mit "*" gekennzeichneten Geschlechter neue untere Schranken. Jedoch wird in keinem der vorliegenden Beispiele, in denen eine untere Schranke verbessert wird, die obere Schranke erreicht. Dabei bleibt jedoch unklar, ob dies im gewählten Beispiel oder der Ungenauigkeit der Schranke begründet liegt.

Symbolverzeichnis

	Kapitel 1	
q	$:= l^v$, wobei l eine Primzahl und v eine natürliche Zahl ist,	11
K	rationaler Funktionenkörper,	11
$S(K)$	Menge der Stellen des Körpers K,	11
$\mathfrak{p}$	eine Stelle von K,	11
$v_{\mathfrak{p}}$	diskrete, normierte Bewertung, der Stelle $\mathfrak{p}$ zugehörig,	11
$o_{(\mathfrak{p})}$	Bewertungsring der Stelle $\mathfrak{p}$ in K,	11
$\mathfrak{P}$	eine Stelle von L in der endlichen, separablen Erweiterung L/K,	11
$S(L)$	Menge der Stellen des Körpers L,	11
$v_{\mathfrak{P}}$	diskrete, normierte Bewertung, der Stelle $\mathfrak{P}$ zugehörig,	11
$\mathcal{O}_{(\mathfrak{P})}$	Bewertungsring der Stelle $\mathfrak{P}$ in L,	11
$e_{\mathfrak{P}}(L/K)$	Verzweigungsindex von $v_{\mathfrak{P}}$ in L/K ,	13
$f_{\mathfrak{P}}(L/K)$	Trägheitsindex von $v_{\mathfrak{P}}$ in L/K,	13
$K_{\mathfrak{p}}$	Vervollständigung von K bzgl. $\mathfrak{p}$,	14
$o_{\mathfrak{p}}$	der Bewertungsring von $K_{\mathfrak{p}}$ bezüglich $\mathfrak{p}$,	14
$\mathcal{D}_{L/K}$	Differente von L/K,	15
$G(L/K)$	Galoisgruppe der Erweiterung L/K,	16
$e_{\mathfrak{p}}(L/K)$	Verzweigungsindex von $\mathfrak{p}$ in Galoiserweiterung L/K,	16
$f_{\mathfrak{p}}(L/K)$	Trägheitsindex von $\mathfrak{p}$ in Galoiserweiterung L/K,	16
$r_{\mathfrak{p}}(L/K)$	Zahl der über $\mathfrak{p}$ liegenden Primdivisoren in der Erweiterung L/K,	16
$Z_{\mathfrak{P}}(L/K)$	Zerlegungsgruppe von $\mathfrak{P}$ in L/K,	16
$T_{\mathfrak{P}}(L/K)$	Trägheitsgruppe von $\mathfrak{P}$ in L/K,	16
$Z_{\mathfrak{p}}(L/K)$	Zerlegungsgruppe von $\mathfrak{P}$ mit $\mathfrak{P}\vert\mathfrak{p}$ in der abelschen Galoiserweiterung L/K,	17
A	Polynomring in einer Unbestimmten T über $\mathbb{F}_q$,	19

v_∞	“unendlich-“Bewertung,	20
A_∞	diskreter Bewertungsring der ∞-Stelle,	20
$\mathfrak{m}_\infty$	Bewertungsideal der ∞-Stelle,	20
$\mathbb{F}_q(T)_\infty$	Vervollständigung von $\mathbb{F}_q(T)$ an der ∞-Stelle,	21
C	Vervollständigung des algebraischen Abschlusses von $\mathbb{F}_q(T)_\infty$,	21
$D_{\mathcal{O}/A}$	Diskriminante von $\mathcal{O}/A$,	22
	Kapitel 2	
G_i	i-te Verzweigungsgruppe in einer lokalen Erweiterung,	24
$\|M\|$	Elementanzahl der Menge M,	24
$G_i(\mathfrak{P})$	i-te Verzweigungsgruppe von $\mathfrak{P}$ in einer globalen Galoiserweiterung mit Galoisgruppe G,	25
$g_i(\mathfrak{p})$	Mächtigkeit der i-ten Verzweigungsgruppe von $\mathfrak{P}$ mit $\mathfrak{P}\|\mathfrak{p}$ in einer globalen Galoiserweiterung ,	25
$\varphi_{L/k}$	Herbrand'sche φ-Funktion in der Galoiserweiterung L/k ,	26
$\psi_{L/k}$	die zur Herbrand-Funktion inverse Funktion,	27
G^v	obere Numerierung der Vezweigungsgruppen,	27
$G^v(\mathfrak{P})$	obere Numerierung der Verzweigungsgruppen von $\mathfrak{P}$ in einer globalen Galoiserweiterung,	27
	Kapitel 3	
$deg\ \mathfrak{a}$	Grad des Divisors $\mathfrak{a}$,	29
$Con_{L'/L}(\mathfrak{A})$	Conorm des Divsors $\mathfrak{A}$ in der Erweiterung L'/L ,	29
$g(L)$	Geschlecht des Funktionenkörpers L,	31
	Kapitel 4	
$Z_f(\overline{k})$	affine, ebene Kurve,	35
$\mathcal{V}(L/k)$	Menge aller Stellen von L, die auf k trivial sind,	36
$(X, k(X))$	vollständig nichtsinguläre Kurve über k,	37
$\mathbb{P}^1/k$	projektive Gerade,	37
$\mathbb{P}^2(k)$	projektive Ebene über k,	38
$X_f(\overline{k})$	ebene projektive Kurve,	39

$X_f(k)$	die Menge der k-rationalen Punkten der projektiven Kurve $X_f(\overline{k})$,	39
$\overline{k}(X_f)$	Körper der rationalen Funktionen von $X_f(\overline{k})$,	40
$\mathcal{P}(\overline{k}(X_f)/\overline{k})$	die Menge aller lokalen Hauptidealringe $\mathcal{O} \subset \overline{k}(X_f)$, die ein echtes Ideal enthalten,	40
$X_f(F)$	die Menge der F-rationalen Punkte der projektiven Kurve $X_f(\overline{k})$, wobei $k \subset F \subset \overline{k}$ ist,	41
$\mathcal{N}(X_f(F))$	Zahl der rationalen Punkte der Kurve $X_f(F)$,	41
	Kapitel 5	
τ	$:= X^q$, wobei X eine Unbestimmte ist,	46
$k\{\tau\}$	nichtkommutativer Polynomring über dem Körper k mit $\mathbb{F}_q \subset k$,	46
K	$:= \mathbb{F}_q(T)$,	47
ρ	Carlitz–Modul,	51
${}_n\rho$	die n-Torsionselemente von ρ ,	52
$K(n)$	Zerfällungskörper von ρ_n,	52
$K_+(n)$	Zerlegungskörper der ∞-Stelle in $K(n)/K$,	52
	Kapitel 6	
A	$:= \mathbb{F}_q[T]$,	59
K	$:= \mathbb{F}_q(T)$,	59
K'	$:= \overline{\mathbb{F}}_q(T)$,	59
n	$:= \prod_{\nu=1}^{s} p_\nu^{r_\nu}$ mit $s, r_\nu \in \mathbb{N}$ und $p_\nu \in A$ normierte, irreduzible, paarweise verschiedene Polynome,	59
d_ν	$:= deg(p_\nu)$,	59
q_ν	$:= q^{d_\nu}$,	59
n_ν	$:= p_\nu^{r_\nu}$,	59
m_ν	$:= \frac{n}{n_\nu}$,	59
$\varphi(n)$	$:= \lvert (A/(n))^* \rvert$,	59
$G(n_\nu)^\alpha$	$:= \{b \in (A/(n_\nu))^* \mid b \equiv 1 \bmod p_\nu^\alpha\}$,	60
$K(n)$	$:= K({}_n\rho\ )$, der Zerfällungskörper in C von $\rho_n(X)$,	60
$K'(n)$	$:= \overline{\mathbb{F}}_q\, K(n)$,	60

$K'_*(n)$	$:= \overline{\mathbb{F}}_q\, K_*(n)$, $*$ stellvertretend für verschiedene Indizes,	60
$g_i(\mathfrak{q}')$	$:= \lvert (G(K'(n)/L'))_i(\mathfrak{q}') \rvert$ mit $K \subset L \subset K(n)$ und $L' := \overline{\mathbb{F}}_q\, L$,	61
$G(n)$	$:= (A/(n))^*$,	65
$K_+(n)$	Fixkörper von $\mathbb{F}_q^*$,	68
	Kapitel 7	
n	$= \prod_{\nu=1}^{s} p_\nu^{r_\nu}$ wie oben und $T \nmid n$ sowie $(T-1) \nmid n$	71
$K_T(n)$	der Zerlegungskörper der Stelle (T) in $K(n)$,	71
$K_{T-1}(n)$	der Zerlegungskörper der Stelle $(T-1)$ in $K(n)$,	71
$K_{T,+}(n)$	$:= K_T(n) \cap K_+(n)$,	71
$K_{T,T-1}(n)$	$:= K_T(n) \cap K_{T-1}(n)$,	71
$K_{T,T-1,+}(n)$	$:= K_{T,T-1}(n) \cap K_+(n)$,	71
$\langle\, a \,\rangle_{G(n)}$	Erzeugnis des Elementes $a \in A$ in der Gruppe $G(n)$,	73
$H(n_\nu)^\alpha$	$:= (G(K(n)/K))^\alpha(\mathfrak{P})$ mit $\mathfrak{P} \in S(K(n))$	
	und $\mathfrak{P} \vert \mathfrak{p}_\nu$ für alle $\alpha = 0, \dots r_\nu$,	75
F_n	Einbettung von $\mathbb{F}_q^*$ in $G(n)$,	75
$e_T(n)$	$:= \lvert \langle\, T \,\rangle_{G(n)} \rvert$,	77
$\tilde{e}_{T,+}(n)$	$:= \lvert \langle\, T \,\rangle_{G(n)} \cap F_n \rvert$,	77
$e_{T,+}(n)$	$:= \lvert \langle\, T \,\rangle_{G(n)} F_n \rvert$,	77
$\tilde{e}_{T,T-1}(n)$	$:= \lvert \langle\, T \,\rangle_{G(n)} \cap \langle\, T-1 \,\rangle_{G(n)} \rvert$,	77
$e_{T,T-1}(n)$	$:= \lvert \langle\, T, T-1 \,\rangle_{G(n)} \rvert$,	77
$\tilde{e}_{T,T-1,+}(n)$	$:= \lvert \langle\, T, T-1 \,\rangle_{G(n)} \cap F_n \rvert$,	77
$e_{T,T-1,+}(n)$	$:= \lvert \langle\, T, T-1 \,\rangle_{G(n)} F_n \rvert$,	77
$N(K_*(n))$	Zahl der “sicheren“ rationalen Stellen,	81

Literaturverzeichnis

[Bea86] Simone de Beauvoir. *Das andere Geschlecht.* rororo, Hamburg 1986.

[Coh91] P.M. Cohn. *Algebraic Numbers and Algebraic Functions.* Chapman & Hall, London 1991.

[Gek97] E.-U. Gekeler. Drinfeld–Moduln. Vorlesung, Saarbrücken, SS 1997.

[Gos96] David Goss. *Basic Structures of Function Field Arithmetic.* Springer, Berlin 1996.

[Hay74] D.R. Hayes. Explicit class field theory for rational function fields. *Trans.Am.Math.Soc.*, 1974.

[Hum91] James E. Humphreys. *Linear Algebraic Groups.* Springer, New York 1991.

[Koc97] Helmut Koch. *Zahlentheorie.* Vieweg, Braunschweig/Wiesbaden 1997.

[Lan70] S. Lang. *Algebraic Number Theory.* Addison-Wesley, 1970.

[Lan93] S. Lang. *Algebra.* Addison-Wesley, third edition, New York 1993.

[Lau99] K. Lauter. Deligne–Lusztig curves as ray class fields. *Manuscripta Math. 98*, 1999.

[Lor97] Dino Lorenzini. *An Invitation to Arithmetic Geometry.* American Mathematical Society, Rhode Island 1997.

[Neu92] Jürgen Neukirch. *Algebraische Zahlentheorie.* Springer, Berlin 1992.

[NX96] H. Niederreiter and C. Xing. Explicit global function fields over the binary field with many rational places. *Acta Arith. 75*, 1996.

[NX97] H. Niederreiter and C. Xing. Drinfeld modules of rank I and algebraic curves with many rational points II. *Acta Arith. 81*, 1997.

[NX99] H. Niederreiter and C. Xing. Global function fields with many rational places and their applications. *Contemporary Mathematics 225*, 1999.

[Sei98] Jessica Seibert. Obere Schranken für die Punktzahl algebraischer Kurven über endlichen Körpern. Staatsexamensarbeit, Universität des Saarlandes, 1998.

[Ser79] J-P. Serre. *Local Fields.* Springer, New York 1979.

[Sti93] Henning Stichtenoth. *Algebraic Function Fields and Codes.* Springer, Berlin 1993.

[VdGVdV93] G. Van der Geer and M. Van der Vlugt. Curves over finite fields of characteristic 2 with many rational points. *C.R. Acad. Sci. Paris Sér. I Math. 317*, 1993.

[VdGVdV97] G. Van der Geer and M. Van der Vlugt. How to construct curves over finite fields with many rational points. *Cambridge University Press Symp. Math 37*, 1997.

[Wol96] Jürgen Wolfart. *Einführung in die Zahlentheorie und Algebra.* vieweg, Wiesbaden 1996.

[XN95] C. Xing and H. Niederreiter. Modules de Drinfeld et courbes algébriques ayant beaucoup de points rationels. *C.R. Acad. Sci. Paris Sér. I Math. 322*, 1995.

[XN96] C. Xing and H. Niederreiter. Drinfeld modules of rank I and algebraic curves with many rational points. Preprint, 1996.