

Die approbierte Originalversion dieser Diplom-/Masterarbeit ist an der Hauptbibliothek der Technischen Universität Wien aufgestellt (<http://www.ub.tuwien.ac.at>).

The approved original version of this diploma or master thesis is available at the main library of the Vienna University of Technology (<http://www.ub.tuwien.ac.at/englweb/>).



D I P L O M A R B E I T

# Asymptotik von Goppa Codes

ausgeführt am Institut für  
Diskrete Mathematik und Geometrie  
der Technischen Universität Wien

unter Anleitung von Ao. Univ-Prof. Dr. Gerhard Dorfer

durch  
Philipp Grohs  
Nussdorferstraße, 33/2/15  
1090 Wien

---

Datum

---

Unterschrift



# Inhaltsverzeichnis

<b>1</b>	<b>Lineare Codes</b>	<b>1</b>
1.1	Einführung . . . . .	1
1.2	Lineare Codes . . . . .	3
1.3	Polynomcodes . . . . .	4
1.4	Zyklische Codes . . . . .	5
1.5	Schranken für Codes . . . . .	6
1.6	Reed-Solomon Codes . . . . .	10
<b>2</b>	<b>Algebraische Funktionenkörper</b>	<b>13</b>
2.1	Stellen . . . . .	13
2.2	Der rationale Funktionenkörper . . . . .	21
2.3	Der schwache Approximationssatz . . . . .	24
2.4	Divisoren . . . . .	27
2.5	Das Geschlecht . . . . .	32
2.6	Motivation: Riemannsche Flächen . . . . .	34
2.7	Der Satz von Riemann-Roch . . . . .	37
2.8	Einige Konsequenzen aus dem Satz von Riemann-Roch . . . . .	44
2.9	Lokale Komponenten von Weil Differentialen . . . . .	46
<b>3</b>	<b>Goppa Codes</b>	<b>49</b>
3.1	Kurven und Funktionenkörper . . . . .	49
3.2	Geometrische Goppa Codes . . . . .	51
3.3	Asymptotische Eigenschaften . . . . .	57
<b>4</b>	<b>Erweiterungen von Funktionenkörpern</b>	<b>61</b>
4.1	Algebraische Erweiterungen . . . . .	61
4.2	Die Fundamentalgleichung von Hilbert . . . . .	66
4.3	Unterringe von Funktionenkörpern . . . . .	70
4.4	Lokale Ganzheitsbasen . . . . .	75
4.5	Die Cospur . . . . .	78
4.6	Die Differenten . . . . .	85
4.7	Konstantenkörpererweiterungen . . . . .	96
4.8	Galoiserweiterungen . . . . .	101

4.9	Verzweigungsgruppen . . . . .	108
4.10	Die Drinfeld-Vladut Schranke . . . . .	115
4.10.1	Die Hasse-Weil Schranke . . . . .	115
4.10.2	Die Drinfeld-Vladut Schranke . . . . .	118
<b>5</b>	<b>Funktionskörpertürme</b>	<b>121</b>
5.1	Grundlagen und Definitionen . . . . .	121
5.2	Zahme Türme . . . . .	124
5.3	Ein zahmer optimaler Turm . . . . .	127
5.4	Ein wilder optimaler Turm . . . . .	132
5.5	Ausblick . . . . .	142

# Vorwort

Die algebraische Codierungstheorie ist eines der wichtigsten Gebiete der Algebra. Beispielsweise basiert die Codierung von CD's auf dieser Theorie, sowie jeglicher digitale Datenaustausch zwischen einem Sender und einem Empfänger, ja sogar die Raumfahrt bedient sich der Theorie der algebraischen Codes; zur Kommunikation mit Raumsonden werden oft Reed-Solomon Codes benützt (1985 Voyager 2 nach Umprogrammierung, 1989 Galileo zum Jupiter, 1989 Magellan zur Venus und 1990 Ulysses zur Sonne).

Dies ist einer der beiden Aspekte, die das Thema dieser Arbeit für mich so reizvoll machen. Der andere ist die sehr interessante und anspruchsvolle Theorie dahinter. Waren die ersten Codes noch relativ einfach, so zieht die heutige Codierungstheorie alle Register der modernen Mathematik im Bestreben immer bessere Codes zu finden. Die wohl schönste und wichtigste Entwicklung in dieser Richtung in den letzten Jahrzehnten ist die Konstruktion von V.D. Goppa, der mit Mitteln der algebraischen Geometrie eine Verallgemeinerung der Reed-Solomon Codes finden konnte. Diese sogenannten Algebraisch Geometrischen Codes, oder Geometrischen Goppa Codes, bestechen durch ihre hervorragenden asymptotischen Eigenschaften.

Im Jahre 1957 fanden Gilbert und Varshamov eine Schranke (die asymptotische Gilbert-Varshamov Schranke), die die Existenz von Codes sicherte, deren Parameter gewisse „gute“ Eigenschaften haben. Ob es Codes mit „besseren“ Parameter gibt stand damals noch in den Sternen, und nachdem man gut 30 Jahre keine solchen Codes finden konnte, regierte der allgemeine Glaube, dass es keine besseren Codes gäbe, dass die Gilbert-Varshamov Schranke also optimal sei. V.D. Goppa war überhaupt der erste, der explizit Codes angeben konnte, die die Gilbert-Varshamov Schranke erreichen.

Man glaubte jedoch immer noch an die Optimalität der Gilbert-Varshamov Schranke bis Tsfasman und Zink mit tiefliegenden Methoden aus der Algebraischen Geometrie (Uniformisierungstheorie von Shimura-Kurven) schließlich zeigen konnten, dass Goppa Codes existieren, die die Gilbert-Varshamov Schranke brechen.

Diese bahnbrechende Entdeckung hatte nur einen Nachteil: Man wusste zwar von der Existenz solcher Codes, jedoch war in dem Beweis kein Hinweis enthalten, wie man nun solche Codes konstruieren könne. Von diesem Zeitpunkt an arbeiteten zahlreiche

Forschungsgruppen an einer Lösung dieses Problems und H. Stichtenoth und A. Garcia konnten schließlich im Jahre 1996 eine explizite Folge von Codes angeben, die die Gilbert-Varshamov Schranke bricht, und die in einem gewissen Sinne optimal ist. Obwohl nun endlich ein Beispiel einer expliziten optimalen Codefolge gefunden wurde, war der Mathematikwelt immer noch nicht ganz klar, was eigentlich der Trick hinter der Konstruktion von Stichtenoth und Garcia war, es funktionierte ganz einfach.

Im Anschluss an ihr erstes Paper [14] folgten noch einige Arbeiten, die die Konstruktion erklärten und weitere optimale Codefolgen angaben. Es ist bis dato immer noch nicht ganz klar warum die Konstruktion für gewisse Kurven funktioniert und für andere nicht.

Ziel dieser Arbeit ist es diese Ergebnisse aufzuarbeiten und Beispiele von optimalen Codefolgen explizit anzugeben. Im ersten Kapitel beginnen wir mit einigen Grundlegenden Definitionen und Eigenschaften von linearen Codes. Zudem leiten wir die asymptotische Gilbert-Varshamov Schranke her, die eine wichtige Rolle in der vorliegenden Arbeit spielt. Ich habe mich in diesem Kapitel an keine spezielle Arbeit gehalten, vielmehr wird mein in diversen Vorlesungen über Codierungstheorie erworbenes Wissen widergegeben. Der Beweis der Gilbert-Varshamov Schranke stammt aus dem Buch von Oliver Pretzel [31].

Das zweite Kapitel soll eine Einführung in die Theorie der algebraischen Funktionenkörper geben, welche eine gänzlich algebraische Theorie zum Studium algebraischer Kurven bereitstellt. Wir folgen hier dem Buch von H. Stichtenoth [38], der ein Schüler von P. Roquette, einem Vorreiter auf diesem Gebiet, war. Einzig der zur Motivation dienende Abschnitt über Riemannsche Flächen stammt im Wesentlichen aus dem Buch von M. Rosen [34].

Das dritte Kapitel führt nun endlich die Geometrischen Goppa Codes ein. Im ersten Abschnitt werden noch einige Grundlagen über algebraische Kurven besprochen, sowie der Zusammenhang zwischen algebraischen Funktionenkörpern und Kurven. Ich habe mich hier wieder an kein spezielles Buch gehalten, am ehesten noch an das Buch von O. Pretzel [31] und das Buch von R. Hartshorne [21]. Es ist mir ein Anliegen diese Zusammenhänge zu erwähnen, denn so effizient der Zugang über Funktionenkörper auch sein mag, um die Idee hinter den Goppa Codes zu verstehen, muss man sich mit Kurven beschäftigen. Die Abschnitte über die Goppa Codes stammen wieder im Grossen und Ganzen aus dem Buch von H. Stichtenoth.

Das vierte Kapitel behandelt Erweiterungen von Funktionenkörpern. Es ist das längste und wahrscheinlich auch das anspruchvollste Kapitel dieser Arbeit. Hier werden die Werkzeuge bereitgestellt, mit denen man optimale Codes konstruieren kann. Ich habe mich auch hier an das Buch von H. Stichtenoth gehalten, das an manchen Stellen zwar sehr technisch ist, aber andererseits auch den kürzesten Weg ans Ziel bietet. Eine andere Möglichkeit wäre es gewesen, dieses Kapitel mit Hilfe der Theorie von Dedekindringen

zu erarbeiten, was aber mit einem erheblich grösserem Zeitaufwand verbunden gewesen wäre, da ich dann ja auch ein Kapitel über Dedekindringe schreiben hätte müssen. Es ist jedoch meiner Meinung nach lehrreich, sich die Ergebnisse dieses Kapitels auch von diesem Standpunkt her zu überlegen.

Das fünfte und letzte Kapitel behandelt schließlich Funktionenkörpertürme. In diesem Kapitel werden wir, unter Verwendung der Ergebnisse aus Kapitel vier, zwei Beispiele von optimalen Codes angeben können, und die aktuellen Probleme der Forschung auf diesem Gebiet illustrieren.

Schlussendlich möchte ich mich noch bei Herrn Prof. Gerhard Dorfer für dieses interessante Thema und die sehr sorgfältige Betreuung bedanken.

Wien, am 13.03.2006

Philipp Grohs



# Kapitel 1

## Lineare Codes

Dieses Kapitel soll eine Einführung in die Theorie der linearen Codes geben, zusammen mit einigen Beispielen. Eine Einführung in dieses Thema bietet beispielsweise [28].

### 1.1 Einführung

Das Kommunikationsmodell, welches wir verwenden besteht aus einem Sender, einem Kommunikationskanal und einem Empfänger. Der Sender sendet eine Information  $I$  über den Kommunikationskanal und der Empfänger erhält die Information  $I'$ . Ziel der Codierungstheorie ist es nun erstens, festzustellen ob bei der Übertragung ein Fehler passiert ist, und zweitens, etwaige Fehler richtig zu korrigieren. In unserem Fall besteht die Information aus einer endlichen Folge von Symbolen aus einem **Alphabet**  $A$ .  $A$  sei zunächst nur irgendeine endliche Menge.

Diese endliche Folge von Symbolen teilen wir nun in gleichlange Blöcke und erhalten sogenannte **Nachrichtenwörter**.

**Definition 1.1.1** *Ein Nachrichtenwort der Länge  $k$  über dem Alphabet  $A$  ist ein Element der Menge  $A^k$ .*

Ein solches Nachrichtenwort wollen wir nun so codieren, dass eventuelle Übertragungsfehler erkannt, bzw. korrigiert werden können. Dazu fügt man dem Nachrichtenwort noch zusätzliche Symbole hinzu, die sogenannten **Kontrollsymbole**. Wir können nun den Begriff des Codewortes definieren:

**Definition 1.1.2** *Ein Codewort der Länge  $n$  besteht aus einem Nachrichtenwort der Länge  $k$  und aus  $n - k$  Kontrollsymbolen. Die Menge aller Codewörter heißt **Code** und wird mit  $C$  bezeichnet.  $C$  heißt  $[n, k]$ -Code wenn die Nachrichtenwörter  $k$  Symbole besitzen und wenn  $n - k$  Kontrollsymbole hinzugefügt werden. Die sogenannte **Codierungsvorschrift** ist die Abbildung  $f_C$ , die den Nachrichtenwörtern die Kontrollsymbole hinzufügt:*

$$f_C : N \subseteq A^k \rightarrow C \subseteq A^n \quad \text{bijektiv.}$$

$N$  ist dabei die Menge der zulässigen Nachrichtenwörter. Der Code heißt **systematisch**, wenn die Kontrollsymbole entweder vorne oder hinten angehängt werden.

Erhält der Empfänger nun ein  $w \in A^n \setminus C$ , dann liegt ein Übertragungsfehler vor.

**Definition 1.1.3** Wir definieren eine Abbildung  $d : A^n \times A^n \rightarrow \mathbb{N}$ , indem wir zwei Elementen  $u = (u_1, \dots, u_n), v = (v_1, \dots, v_n) \in A^n$  die Anzahl der Indizes  $i$  zuordnen, für die  $v_i \neq u_i$ . Wir nennen  $d(u, v)$  die Hammingdistanz von  $v$  zu  $u$ .

Der Beweis des folgenden Satzes ist einfach.

**Satz 1.1.4** Die Hammingdistanz ist eine Metrik auf  $A^n$ .

Korrigieren heißt nun, dass man einem fehlerbehafteten Empfangswort sein nächstgelegenes Codewort zuordnet (bezüglich der Hammingdistanz). Diese Decodierungsvorschrift nennt man **Maximum Likelihood Decodierung**. Sie basiert auf der Annahme

$$P(a \text{ erhalten} \mid a \text{ gesendet}) > P(b \text{ erhalten} \mid a \text{ gesendet}),$$

für alle  $b \neq a$ .

**Definition 1.1.5** Man nennt

$$d := \min\{d(x, y) : x, y \in C; x \neq y\}$$

die **Minimaldistanz** von  $C$ .

Man kann also um jedes Codewort eine Kugel mit Radius  $d$  legen, ohne dass ein anderes Codewort in der Kugel liegt. Diese Überlegung, die die Codierungstheorie übrigens mit der Theorie der Kreispackungen in Verbindung bringt, macht den Beweis des folgenden Satzes offensichtlich.

**Satz 1.1.6** Sei  $C$  ein Code mit Minimaldistanz  $d$ . Dann gilt:

- (a)  $C$  kann genau dann  $t$  oder weniger Fehler erkennen, wenn  $d \geq t + 1$  gilt.
- (b)  $C$  kann genau dann  $t$  oder weniger Fehler korrigieren, wenn  $d \geq 2t + 1$  gilt.

*Beweis:* (a) ist trivial.

(b) Man mache sich klar, dass die Tatsache, dass  $t$  oder weniger Fehler korrigiert werden können, nichts anderes heisst, als dass sich keine zwei Kugeln mit Radius  $t$  schneiden, wenn man sie um zwei Codewörter legt. Daraus folgt unmittelbar die Behauptung. □

**Definition 1.1.7** Sei  $C$  ein  $[n, k]$ -Code mit Minimaldistanz  $d$ . Dann nennen wir  $C$  einen  $[n, k, d]$ -Code.

## 1.2 Lineare Codes

Genauso wie wir in unserer Sprache eine Grammatik haben, also gewisse Regeln, wie man Wörter „manipulieren“ kann, wollen wir nun auch gewisse Regeln auf unserem Code einführen. Eine Möglichkeit ist es, auf  $A$  eine abelsche Gruppenstruktur zu legen und zu fordern, dass der Code eine Untergruppe von  $A^n$  ist. Solche Codes heißen **Gruppencodes**. Wir gehen noch weiter: Wir fordern dass  $A = \mathbb{F}_q$  der Körper mit  $q$  Elementen ist, und dass die Abbildung

$$f_C : \mathbb{F}_q^k \rightarrow \mathbb{F}_q^n$$

ein  $\mathbb{F}_q$ -Vektorraummonomorphismus (also linear und injektiv) ist. Als Nachrichtenwörter sind also alle Elemente aus  $\mathbb{F}_q^k$  zugelassen.

**Definition 1.2.1** *Ein linearer  $[n, k]$  Code über dem Alphabet  $\mathbb{F}_q$  ist ein  $k$ -dimensionaler Unterraum von  $\mathbb{F}_q^n$ .*

**Definition 1.2.2** *Sei  $a = (a_1, \dots, a_n) \in A^n$ . Das **Hamminggewicht**  $w(a)$  von  $a$  ist die Anzahl der von Null verschiedenen Elemente  $a_i$ ,  $i = 1, \dots, n$ .*

Wir bringen nun die Minimaldistanz mit dem Hamminggewicht in Zusammenhang.  $C$  sei im Folgenden immer ein  $[n, k, d]$ -Linearcode.

**Satz 1.2.3** *Die Minimaldistanz von  $C$  ist gleich dem minimalen Gewicht aller von Null verschiedenen Codewörter.*

*Beweis:*

$$\begin{aligned} d &= \min\{d(x, y) : x, y \in C, x \neq y\} = \min\{w(x - y) : x, y \in C, x \neq y\} \\ &= \min\{w(c) : c \in C \setminus \{0\}\}. \end{aligned}$$

□

Man kann übrigens die Codierungsvorschrift  $f_C$  eines jeden Linearcode „systematisch machen“ indem man geeignete Basistransformationen anwendet. Der Code wird durch die Matrix der Abbildung  $f_C$  dargestellt.

**Definition 1.2.4** *Die  $k \times n$  Matrix der injektiven Abbildung  $f_C$  heißt **Generatormatrix** von  $C$ .*

Zu jedem  $[n, k]$  Code  $C$  kann man den sogenannten **dualen Code** assoziieren:

**Definition 1.2.5** *Der zu  $C$  duale Unterraum von  $A^n$  (bezüglich des kanonischen inneren Produktes  $\langle \cdot, \cdot \rangle$ ) heißt **dualer Code** von  $C$  und wir schreiben dafür  $C^\perp$ .*

Aus der Definition folgt direkt

**Satz 1.2.6** *Der zu einem  $[n, k]$  Code  $C$  duale Code,  $C^\perp$ , ist ein  $[n, n - k]$ -Code und es gilt für die Generatormatrix  $H$  von  $C^\perp$ :*

$$x \in C \Leftrightarrow xH^T = 0 \in A^{n-k}.$$

Es ist bis dato kein Zusammenhang bekannt zwischen der Minimaldistanz von  $C$  und der Minimaldistanz von  $C^\perp$ .

**Definition 1.2.7** *Die Generatormatrix von  $C^\perp$  heißt **Kontrollmatrix** von  $C$ .*

**Bemerkung 1.2.8** *Wir haben hier Codes als  $k$ -dimensionale Unterräume von  $\mathbb{F}_q^n$  definiert. Dadurch ist die Codierungsvorschrift  $f_C$  natürlich nur bis auf eine Basistransformation in  $\mathbb{F}_q^k$  definiert. Wenn wir also, wie oben, einem Code  $C$  seine Codierungsvorschrift zuordnen, meinen wir genau genommen eine Äquivalenzklasse von Abbildungen modulo Basistransformationen (in  $\mathbb{F}_q^k$ ).*

### 1.3 Polynomcodes

Wir wollen nun eine spezielle Klasse von Linearcodes genauer studieren: die Polynomcodes. Da Operationen mit Polynomen sehr einfach implementierbar sind, sind Polynomcodes insbesondere für die Anwendung wichtig. Sehr viele in der Praxis verwendeten Codes sind Polynomcodes. Als Alphabet dient uns wieder der Körper  $\mathbb{F}_q$ .

Zunächst ordnen wir einem Vektor in naheliegender Weise ein Polynom zu:

**Definition 1.3.1** *Sei  $c = (c_1, \dots, c_m) \in \mathbb{F}_q^m$ . Wir definieren*

$$p_c(x) := c_1 + c_2x + \dots + c_mx^{m-1}.$$

**Definition 1.3.2** *Sei  $C$  ein  $[n, k]$  Linearcode über  $\mathbb{F}_q$  und  $g(x) \in \mathbb{F}_q[x]$  mit  $\deg(g(x)) = n - k$ .  $C$  heißt **Polynomcode** mit **Generatorpolynom**  $g(x)$ , falls die Menge*

$$P_C := \{p_c(x) : c \in C\}$$

*genau aus den Vielfachen von  $g(x)$  vom Grad  $< n$  besteht.*

**Lemma 1.3.3** *Für einen Polynomcode  $C$  mit Generatorpolynom  $g(x)$  gilt*

$$c \in C \Leftrightarrow p_c(x) \equiv 0 \pmod{g(x)}.$$

## 1.4 Zyklische Codes

**Definition 1.4.1** Ein linearer  $[n, k]$ -Code  $C$  heißt **zyklisch**, wenn mit jedem Codewort  $c = (c_1, \dots, c_n) \in C$  auch jene Wörter, die durch zyklische Vertauschung der Symbole von  $c$  entstehen, in  $C$  liegen.

**Satz 1.4.2** Jeder zyklische Linearcode  $C$  ist ein Polynomcode.

*Beweis:* Sei

$$P_C := \{p_c(x) = c_1 + c_2x + \dots + c_nx^{n-1} : c = (c_1, \dots, c_n) \in C\}.$$

Wir wählen  $0 \neq g(x) \in P_C$  mit minimalem Grad.

**1.Behauptung:**  $g(x)$  teilt jedes  $p(x) \in P_C$ :

Sei  $p(x) \in P_C$ . Dann gilt

$$p(x) = q(x)g(x) + r(x) \text{ mit } \deg(r(x)) < \deg(g(x)) \text{ oder } r(x) = 0.$$

Es gilt also  $r(x) \notin P_C$  oder  $r(x) = 0$ , da der Grad von  $g(x)$  minimal ist. Angenommen  $r(x) \neq 0$ . Es gilt

$$r(x) = p(x) - q(x)g(x),$$

und  $q(x)g(x) \in P_C$  weil  $C$  zyklisch. Also würde folgen, dass  $r(x) \in P_C$  gilt, Widerspruch. Damit ist die Behauptung gezeigt.

**2.Behauptung:** Sei  $p(x)$  ein Polynom vom Grad  $< n$  mit  $g(x)|p(x)$ . Dann gilt  $p(x) \in P_C$ :

Es gilt  $p(x) = g(x)v(x) \in P_C$  weil  $C$  zyklisch ist. Daraus folgt, dass  $C$  ein Polynomcode mit Generatorpolynom  $g(x)$  ist.

□

**Satz 1.4.3** Ein  $[n, k]$ -Polynomcode ist genau dann zyklisch, wenn sein Generatorpolynom  $g(x)$  das Polynom  $x^n - 1$  teilt.

*Beweis:* Nehmen wir zuerst an, dass  $g(x)|x^n - 1$ . Sei  $f(x) := x^n - 1$ ,  $c \in C$  und  $p(x)$  beliebig. Dann ist  $p_c(x)p(x) \bmod(f(x)) \in P_C$ . Daher gilt

$$xp_c(x) \bmod(f(x)), x^2p_c(x) \bmod(f(x)), \dots \in P_C.$$

Führt man eine Division mit Rest durch  $x^n - 1$  durch, so sieht man, dass diese Polynome gerade den zyklische Vertauschung des Codevektors  $c$  entsprechen. Daher ist  $C$  zyklisch.

Zu zeigen bleibt die andere Richtung. Sei also  $C$  zyklisch. Dann ist  $x^k p_c(x) \bmod(f(x)) \in P_C$  für  $c \in C$  und  $f(x) = x^n - 1$ , da dieses Polynom ja der  $k$ -fachen zyklischen Verschiebung von  $c$  entspricht. Da  $\deg(x^k g(x)) = n$  gilt  $x^k g(x) \bmod(f(x)) \equiv x^k g(x) - x^n - 1 \in P_C$  und daher  $g(x)|x^k g(x) - (x^n - 1)$ , also gilt  $g(x)|x^n - 1$ .

□

## 1.5 Schranken für Codes

Wir wollen nun einige Schranken für die Codeparameter herleiten. Zunächst ist klar, dass, wenn  $k$  gross ist,  $d$  klein ist (bei festem  $n$ ). Diese Überlegung wird mit der Singleton Schranke präzisiert.

**Proposition 1.5.1 (Singleton Schranke)** *Für einen  $[n, k, d]$ -Linearcode gilt*

$$k + d \leq n + 1.$$

*Beweis:* Betrachten wir den Teilraum  $W \subseteq \mathbb{F}_q^n$  gegeben durch

$$W := \{(a_1, \dots, a_n) \in \mathbb{F}_q^n : a_i = 0 \text{ für alle } i \geq d\}.$$

Da jedes  $a \in W$  ein Hamminggewicht kleiner als  $d$  hat, gilt  $W \cap C = 0$ . Da  $\dim(W) = d - 1$ , gilt

$$\begin{aligned} k + (d - 1) &= \dim(C) + \dim(W) \\ &= \dim(C + W) + \dim(C \cap W) = \dim(C + W) \leq n. \end{aligned}$$

□

**Definition 1.5.2** *Ein  $[n, k, d]$ -Code  $C$  mit der Eigenschaft  $k + d = n + 1$ , heißt  $C$  MDS-Code<sup>1</sup>.*

Die Singletonsschranke liefert eine obere Schranke für  $d$ . Wir wollen nun eine „untere“ Schranke herleiten, in dem Sinne, dass ein Code existiert, der einen bestimmten Wert von  $d$  übertrifft. Um eine solche Schranke herzuleiten, zählen wir zunächst die Wörter in  $\mathbb{F}_q^n$ , die in einer Kugel  $K_r(u)$  mit Radius  $r$  um ein  $u \in \mathbb{F}_q^n$  liegen.

**Lemma 1.5.3** *Es gilt für  $V_r(n) := \text{card}(K_r(u))$*

$$V_r(n) = \sum_{k=0}^r \binom{n}{k} (q-1)^k.$$

*Beweis:* Betrachten wir die Anzahl der Wörter, deren Distanz zu  $u$  gleich  $k$  ist. Dann sind  $k$  Komponenten ungleich denen von  $u$ , dafür gibt es  $\binom{n}{k}$  Möglichkeiten, und zu jeder Komponente existieren  $q-1$  Möglichkeiten den Eintrag zu ändern. Aufsummieren über  $k$  liefert das Ergebnis.

□

**Proposition 1.5.4** *Sei  $C$  ein linearer  $[n, k, d]$ -Code über  $\mathbb{F}_q$ . Gelte  $\text{card}(C) < q^n/V_{d-1}(n)$ , dann existiert ein linearer  $[n, k+1, d]$ -Code  $C'$ , der  $C$  echt enthält.*

<sup>1</sup>maximum distance separable Code

*Beweis:* Unsere Voraussetzung besagt, dass ein  $v \in \mathbb{F}_q^n$  existieren muss mit  $d(v, c) \geq d$  für alle  $c \in C$ . Definieren wir  $C' := C \oplus \{v\}$ . Zu zeigen ist, dass das Hamminggewicht eines Codewortes aus  $C'$  grösser gleich  $d$  ist. Sei  $u = c + av \in C'$  mit  $c \in C, a \in \mathbb{F}_q$ . Für  $a = 0$  ist die Aussage trivial. Sei also  $a \neq 0$ . Dann gilt

$$w(u) = w(-a^{-1}u) = w(-a^{-1}c - v) = d(-a^{-1}c, v) \geq d$$

nach Konstruktion von  $v$ .

□

**Korollar 1.5.5 (Gilbert-Varshamov Schranke)** Für alle  $n$  und  $d < n$  existiert ein linearer  $[n, k, d]$ -Code über  $\mathbb{F}_q$  mit  $k \geq n - \log_q(V_{d-1}(n))$ .

Wir wollen noch ein asymptotisches Resultat herleiten. Dazu müssen wir das Verhalten von  $V_{d-1}(n)$  für  $n$  gegen unendlich kennen. Zunächst eine Definition.

**Definition 1.5.6** Sei  $C$  ein  $[n, k, d]$  Code. Wir definieren die **Übertragungsrate** von  $C$  durch

$$R(C) := \frac{k}{n}$$

und die **relative Minimaldistanz** durch

$$\delta(C) := \frac{d}{n}.$$

Die Gilbert-Varshamov Schranke besagt, dass ein  $[n, k, d]$ -Code existiert mit  $R \geq 1 - \log_q(V_{d-1}(n))/n$ . Wir studieren nun das asymptotische Verhalten von  $\log_q(V_{d-1}(n))/n$  mit Hilfe der sogenannten  $q$ -ären Entropiefunktion:

**Definition 1.5.7** Für  $0 \leq \delta \leq (q-1)/q$  definieren wir die  **$q$ -äre Entropiefunktion**  $H_q(\delta)$  durch  $H_q(0) := 0$  und

$$H_q(\delta) := \delta \log_q(q-1) - \delta \log_q(\delta) - (1-\delta) \log_q(1-\delta).$$

**Lemma 1.5.8** Sei  $0 \leq \delta \leq (q-1)/q$  und für  $n \in \mathbb{Z}$  sei  $r = r(n)$  die größte ganze Zahl mit  $r \leq \delta n$ . Dann gilt

$$(a) \log_q(V_r(n)) \leq nH_q(\delta).$$

$$(b) \lim_{n \rightarrow \infty} \frac{1}{n} \log_q(V_r(n)) = H_q(\delta).$$

*Beweis:* (a) Es gilt  $0 \leq 1/q = 1 - (q-1)/q \leq 1 - \delta$ . Also gilt für jedes  $k \geq 0$

$$\delta^k \leq \frac{(q-1)^k}{q^k} \leq (q-1)^k (1-\delta)^k.$$

Sei nun  $0 \leq i \leq \delta n$  und  $k := \delta n - i$ . Dann bekommen wir

$$\delta^{\delta n - i} \leq (q - 1)^{\delta n - i} (1 - \delta)^{\delta n - i}.$$

Multiplikation mit  $(1 - \delta)^n$  liefert

$$\frac{\delta^i (1 - \delta)^{n - i}}{(q - 1)^i} \geq \frac{\delta^{\delta n} (1 - \delta)^{n - \delta n}}{(q - 1)^{\delta n}} = q^{-nH_q(\delta)}. \quad (1.1)$$

Es gilt nun

$$\begin{aligned} 1 &= 1^n = (\delta + (1 - \delta))^n \\ &= \sum_{i=0}^n \binom{n}{i} \delta^i (1 - \delta)^{n - i} \\ &= \sum_{i=0}^n \binom{n}{i} (q - 1)^i \left(\frac{\delta}{q - 1}\right)^i (1 - \delta)^{n - i} \\ &\geq \sum_{i=0}^r \binom{n}{i} (q - 1)^i \left(\frac{\delta}{q - 1}\right)^{\delta n} (1 - \delta)^{n - \delta n} \quad \text{wegen (1.1)} \\ &= V_r(n) q^{-nH_q(\delta)}. \end{aligned}$$

Wendet man nun  $\log_q$  an, so erhält man das Gewünschte.

(b) Wir verwenden die Stirlingsche Formel für  $\ln(n!)$ :

$$\ln(n!) - \frac{1}{12n} \leq \left(n + \frac{1}{2}\right) \ln(n) - n + K \leq \ln(n!)$$

mit  $K := \frac{\ln(2\pi)}{2}$ . Daraus folgt

$$\log_q(n!) - \frac{\log_q(e)}{12n} \leq \left(n + \frac{1}{2}\right) \log_q(n) - n \log_q(e) + K' \leq \log_q(n!)$$

mit einer anderen Konstante  $K'$ . Klarerweise gilt wegen der Summendarstellung von  $V_r(n)$

$$V_r(n) \geq \binom{n}{r} (q - 1)^r$$

und wenn wir  $\binom{n}{r} = \frac{n!}{r!(n-r)!}$  mit der Stirlingschen Formel abschätzen, so erhalten wir (wir schreiben  $\log$  statt  $\log_q$ )

$$\begin{aligned} \log(V_r(n)) &\geq \left(n + \frac{1}{2}\right) \log(n) - \left(r + \frac{1}{2}\right) \log(r) \\ &\quad - \left(n - r + \frac{1}{2}\right) \log(n - r) + r \log(q - 1) \\ &\quad - n \log(e) + r \log(e) + (n - r) \log(e) - K' \\ &\quad - \frac{\log(e)}{12r} - \frac{\log(e)}{12(n - r)}. \end{aligned}$$

Dividieren wir nun durch  $n$  und ignorieren wir die Terme von der Größenordnung  $O(1)$  (für  $n \rightarrow \infty$ ), so erhalten wir

$$\begin{aligned} & \lim_{n \rightarrow \infty} \left( \frac{\log(V_r(n))}{n} \right) \\ & \geq \lim_{n \rightarrow \infty} \left( \log(n) - \frac{r}{n} \log(r) - \frac{n-r}{n} \log(n-r) + \frac{r}{n} \log(q-1) \right). \end{aligned} \quad (1.2)$$

Nach der Definition von  $r$  gilt  $\lim_{n \rightarrow \infty} \frac{r}{n} = \delta$ . Nützt man dies aus, so folgt nach kurzer Rechnung aus (1.2)

$$\lim_{n \rightarrow \infty} \left( \frac{\log(V_r(n))}{n} \right) \geq H_q(\delta).$$

Zusammen mit (a) folgt daraus (b). □

Wir können nun unser asymptotisches Resultat beweisen.

**Satz 1.5.9 (Asymptotische Gilbert-Varshamov Schranke)** Für  $0 \leq \delta \leq \frac{q-1}{q}$  existiert eine Folge von linearen Codes der Länge  $n$  über  $\mathbb{F}_q$  mit  $\lim_{n \rightarrow \infty} \delta(C_n) = \delta$  und  $\lim_{n \rightarrow \infty} R(C_n) = 1 - H_q(\delta)$ .

*Beweis:* Sei  $r$  die größte ganze Zahl mit  $r \leq n\delta$ . Nach der Gilbert-Varshamov Schranke existiert ein Code  $C_n$  der Länge  $n$  mit Minimaldistanz  $r+1$  und

$$1 - \frac{\log(V_r(n)) - 1}{n} \geq R(C_n) \geq 1 - \frac{\log(V_r(n))}{n}.$$

Die linke Ungleichung erhält man indem man  $k$  unter Beibehaltung von  $d$  verkleinert. Nach dem vorigen Lemma gilt

$$\lim_{n \rightarrow \infty} R(C_n) = 1 - H_q(\delta).$$

Um den Grenzwert der relativen Minimaldistanzen zu berechnen beachte man, dass

$$\delta n < r + 1 \leq \delta n + 1$$

gilt. Also gilt

$$\delta < \frac{r+1}{n} \leq \delta + \frac{1}{n},$$

und folglich

$$\lim_{n \rightarrow \infty} \delta(C_n) = \lim_{n \rightarrow \infty} \frac{r+1}{n} = \delta. \quad \square$$

## 1.6 Reed-Solomon Codes

Wir wollen uns abschliessend eine prominente Familie von Codes ansehen: die Reed-Solomon Codes [33]. Sie werden zum Beispiel bei der Codierung von CD's verwendet. Ihre herausragende Eigenschaft ist die hervorragende Korrektur von gebündelten Fehlern. So kann man beispielsweise in eine CD ein kleines Loch bohren und die CD wird immer noch fehlerfrei abgespielt. Wir gehen jedoch auf diese Eigenschaft in dieser Arbeit nicht ein, in diesem ersten Zugang beschreiben wir die Reed-Solomon Codes als zyklische MDS-Codes. Wir verwenden als Alphabet  $\mathbb{F}_q$ .

**Definition 1.6.1** Sei  $\alpha$  ein primitives Element von  $\mathbb{F}_q$  und  $n = q - 1$ . Dann heisst der  $[n, k]$ -Code mit Generatorpolynom  $g(x) = (x - \alpha) \dots (x - \alpha^{d-1})$  mit  $d = n - k + 1$  **Reed-Solomon Code** der Länge  $n$  und wird mit  $RS(n, d)$  bezeichnet.

Offensichtlich ist dieser Code zyklisch, da sein Generatorpolynom das Polynom  $x^n - 1$  teilt. Wir zeigen, dass  $RS(n, d)$  ein Code mit Minimaldistanz  $d$  ist. Daraus folgt aus der Beziehung  $d = n - k + 1$ , dass  $RS(n, d)$  ein MDS-Code ist. Zunächst ein Lemma.

**Lemma 1.6.2** Sei  $C$  ein linearer Code der Länge  $n$  mit Kontrollmatrix  $H$ . Dann gilt für die Minimaldistanz  $d$

$$d \geq r \Leftrightarrow \text{je } r - 1 \text{ Spalten von } H \text{ sind linear unabhängig.}$$

*Beweis:* Sei  $d \geq r$  und  $H = (h_1, \dots, h_n)$ . Angenommen  $r - 1$  Spalten wären linear abhängig. Seien o.B.d.A. die ersten  $r - 1$  Spalten  $h_1, \dots, h_{r-1}$  von  $H$  linear abhängig. Dann gilt  $\sum_{i=1}^{r-1} c_i h_i = 0$  für einen Vektor  $0 \neq c = (c_1, \dots, c_i, 0, \dots, 0) \in \mathbb{F}_q^n$ . Es gilt  $Hc = 0$ , also  $c \in C$  und  $w(c) \leq r - 1$ . Widerspruch zu  $d \geq r$ .

Seien umgekehrt je  $r - 1$  Spalten linear unabhängig und  $c \in \mathbb{F}_q^n$  ein Vektor vom Gewicht kleiner als  $r$ , sagen wir  $r - l$ . Seien  $c_{i_1}, \dots, c_{i_{r-l}}$  die Einträge von  $c$  ungleich Null. Dann gilt wegen  $Hc = 0$

$$\sum_{j=1}^{r-l} c_{i_j} h_{i_j} = 0,$$

also sind die  $r - l$  Spalten  $h_{i_1}, \dots, h_{i_{r-l}}$  linear abhängig. Widerspruch. □

**Satz 1.6.3** Reed-Solomon Codes sind MDS-Codes.

*Beweis:* Wir überlegen uns nun wie die Kontrollmatrix des Reed-Solomon Codes  $C = RS(n, d)$  aussieht. Sei  $c = (c_1, \dots, c_n) \in \mathbb{F}_q^n$ . Dann gilt für  $c(x) = c_1 + c_2x + \dots + c_nx^{n-1}$

$$\begin{aligned} c \in C &\Leftrightarrow (x - \alpha) \dots (x - \alpha^{d-1}) | c(x) \\ &\Leftrightarrow c(\alpha^i) = 0 \text{ für } i = 1, \dots, d - 1. \end{aligned}$$

Da andererseits

$$c \in C \Leftrightarrow Hc = 0$$

gilt, muss  $H$  die folgende Gestalt haben:

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \dots & \alpha^n \\ 1 & \alpha^2 & (\alpha^2)^2 & \dots & \dots & (\alpha^2)^n \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \alpha^{d-1} & (\alpha^{d-1})^2 & \dots & \dots & (\alpha^{d-1})^n \end{pmatrix}$$

Aufgrund der Formel für die Vandermondsche Unterdeterminante gilt, dass je  $d - 1$  Spalten von  $H$  linear unabhängig sind, daher ist die Minimaldistanz  $d(C)$  mindestens  $d$ . Nach der Definition gilt also

$$d(C) \geq n - k + 1$$

und wegen der Singleton Schranke gilt sogar

$$d(C) = n - k + 1 = d,$$

daher sind Reed-Solomon Codes MDS-Codes.

□



# Kapitel 2

## Algebraische Funktionenkörper

In dieser Arbeit werden die Goppa Codes über die Theorie der algebraischen Funktionenkörper konstruiert. Ursprünglich hat V.D. Goppa diese Codes mit Mitteln der algebraischen Geometrie, genauer nichtsingulären projektiven Kurven, hergeleitet. Die Sprache der algebraischen Funktionenkörper (in einer Variablen) ist äquivalent zu der der nichtsingulären projektiven Kurven. Der Zugang über algebraische Funktionenkörper hat zwei Vorteile: zum einen ist er erheblich direkter, zum zweiten ist die Verzweigungstheorie mit einem algebraischen Zugang etwas einfacher zu handhaben. Was man dabei einbüßt ist die Anschauung, die aber bei algebraischer Geometrie über endlichen Körpern (und nur dafür interessieren wir uns im Wesentlichen) ohnehin sehr begrenzt und zum Teil irreführend ist. Ziel dieses Kapitels ist eine Einführung in die Theorie der algebraischen Funktionenkörper, die im Satz von Riemann-Roch ihren Höhepunkt findet.

### 2.1 Stellen

Kommen wir zur ersten wichtigen Definition:

**Definition 2.1.1** *Ein algebraischer Funktionenkörper  $F/K$  in einer Variable über einem Körper  $K$  ist eine endliche Körpererweiterung  $F \supseteq K(x)$ , wobei  $x$  transzendent über  $K$  ist.*

Im folgenden werden wir  $F/K$  kurz als Funktionenkörper bezeichnen. Die Menge

$$\tilde{K} := \{z \in F : z \text{ ist algebraisch über } K\}$$

bezeichnet man als **Konstantenkörper**.  $\tilde{K}$  ist ein Körper und es gilt  $K \subseteq \tilde{K} \subseteq F$ .  $F/\tilde{K}$  ist klarerweise ein Funktionenkörper.

Wir sagen:  $K$  ist **algebraisch abgeschlossen** in  $F$ , falls  $K = \tilde{K}$  gilt.

**Bemerkung 2.1.2** *Es gilt, dass  $z \in F$  genau dann transzendent über  $K$  ist, falls  $[F : K(z)] < \infty$ .*

**Beispiel 2.1.3** Das einfachste Beispiel eines Funktionenkörpers über  $K$  ist der sogenannte **rationale Funktionenkörper**  $K(x)$  für ein über  $K$  transzendentes Element  $x$ .

Warum der rationale Funktionenkörper den Namen „Funktionenkörper“ trägt, ist offensichtlich. Wir wollen nun sehen wie man die Elemente eines jeden beliebigen Funktionenkörpers als Funktionen auffassen kann. Dazu benötigen wir die Begriffe des Bewertungsringes und der Stellen.

**Definition 2.1.4** Ein **Bewertungsring** eines Funktionenkörpers  $F/K$  ist ein Ring  $\mathcal{O} \subseteq F$  mit den folgenden Eigenschaften:

- (1)  $K \subset \mathcal{O} \subset F$ , und
- (2) es gilt  $z \in \mathcal{O}$  oder  $z^{-1} \in \mathcal{O}$  für alle  $z \in F \setminus \{0\}$ .

**Proposition 2.1.5** Für einen Bewertungsring  $\mathcal{O}$  eines Funktionenkörpers  $F/K$  gilt:

- (a)  $\mathcal{O}$  ist lokal mit maximalem Ideal  $P = \mathcal{O} \setminus \mathcal{O}^*$ , wobei  $\mathcal{O}^*$  die Einheitengruppe von  $\mathcal{O}$  bezeichne.
- (b) Für  $0 \neq x \in F$  gilt:  $x \in P \Leftrightarrow x^{-1} \notin \mathcal{O}$ .
- (c) Für  $\tilde{K}$  gilt:  $\tilde{K} \subseteq \mathcal{O}$  und  $\tilde{K} \cap P = \{0\}$ .

*Beweis:* (a) Es genügt zu zeigen, dass  $P := \mathcal{O} \setminus \mathcal{O}^*$  ein Ideal ist.

- (1) Sei  $x \in P$  und  $z \in \mathcal{O}$ . Dann ist  $xz$  keine Einheit in  $\mathcal{O}$ , also  $xz \in P$ .
- (2) Sei  $x, y \in P \setminus \{0\}$ . Nach Definition 2.1.4 (2) ist  $x/y \in \mathcal{O}$  oder  $y/x \in \mathcal{O}$ . Gelte o.B.d.A  $x/y \in \mathcal{O}$ . Dann ist  $1 + x/y \in \mathcal{O}$  und nach (1) auch  $y(1 + x/y) = y + x$ .  $P$  ist also ein Ideal von  $\mathcal{O}$ .

(b) ist klar.

(c) Sei  $z \in \tilde{K}$ . Angenommen  $z \notin \mathcal{O}$ . Dann ist  $z^{-1} \in \mathcal{O}$ . Da  $z^{-1}$  algebraisch über  $K$  ist, existieren Elemente  $a_1, \dots, a_r \in K$  mit  $a_r(z^{-1})^r + \dots + a_1 z^{-1} + 1 = 0$ , also  $-1 = z^{-1}(a_r(z^{-1})^{r-1} + \dots + a_1)$ . Es gilt also  $z = -(a_r(z^{-1})^{r-1} + \dots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}$ , also  $z \in \mathcal{O}$ . Die Aussage  $\tilde{K} \cap P = \{0\}$  ist trivial.

□

**Satz 2.1.6** Sei  $\mathcal{O}$  ein Bewertungsring eines Funktionenkörpers  $F/K$  mit maximalem Ideal  $P$ . Dann gilt:

- (a)  $P$  ist Hauptideal.

- (b) Sei  $P = t\mathcal{O}$ . Dann hat jedes Element  $0 \neq z \in F$  eine eindeutige Darstellung der Form  $z = t^n u$ , für ein  $n \in \mathbb{Z}$ ,  $u \in \mathcal{O}^*$ .
- (c)  $\mathcal{O}$  ist ein Hauptidealring. Es gilt: falls  $P = t\mathcal{O}$  und  $\{0\} \neq I \subseteq \mathcal{O}$  ein Ideal, so ist  $I = t^n \mathcal{O}$  für ein  $n \in \mathbb{N}$ .

**Definition 2.1.7** Ein diskreter Bewertungsring ist ein lokaler Hauptidealring.

Satz 2.1.6 besagt also nichts anderes, als dass  $\mathcal{O}$  ein **diskreter Bewertungsring** ist. Um ihn beweisen zu können, benötigen wir das folgende Lemma:

**Lemma 2.1.8** Sei  $\mathcal{O}$  ein Bewertungsring eines Funktionenkörpers  $F/K$ ,  $P$  sein maximales Ideal, und  $0 \neq x \in P$ . Sei  $x_1, \dots, x_n \in P$  so, dass  $x_1 = x$  und  $x_i \in x_{i+1}P$  für  $i = 1, \dots, n-1$ . Dann gilt  $n \leq [F : K(x)] < \infty$ .

*Beweis:* Aus Bemerkung 2.1.2 und Proposition 2.1.5 (c) folgt sofort die Relation  $[F : K(x)] < \infty$ . Es genügt also zu zeigen, dass  $x_1, \dots, x_n$  linear unabhängig über  $K(x)$  sind. Nehmen wir an, es existierte eine nichttriviale Linearkombination  $\sum_{i=1}^n \varphi_i x_i = 0$  mit  $\varphi_i \in K(x)$ . Durch Multiplikation mit einem gemeinsamen Nenner können wir uns auf den Fall  $\varphi_i \in K[x]$  beschränken. Weiters können wir annehmen, dass  $x$  nicht alle Polynome  $\varphi_i$  teilt. Setze  $a_i := \varphi_i(0)$  und definiere  $j \in \{1, \dots, n\}$  durch die Bedingung  $a_j \neq 0$ , aber  $a_i = 0$  für alle  $i > j$ . Wir erhalten

$$-\varphi_j x_j = \sum_{i \neq j} \varphi_i x_i \quad (2.1)$$

mit  $\varphi_i \in \mathcal{O}$  für  $i = 1, \dots, n$  (da  $x = x_1 \in P$ ),  $x_i \in x_j P$  für  $i < j$  und  $\varphi_i = x g_i$  für  $i > j$ , wobei  $g_i$  ein Polynom in  $x$  ist. Dividiert man (2.1) durch  $x_j$ , so erhält man

$$-\varphi_j = \sum_{i < j} \varphi_i \frac{x_i}{x_j} + \sum_{i > j} \frac{x}{x_j} g_i x_i.$$

Da alle Summanden auf der rechten Seite in  $P$  liegen, liegt  $\varphi_j$  in  $P$ . Andererseits gilt  $\varphi_j = a_j + x g_j$  mit  $g_j \in K[x] \subseteq \mathcal{O}$  und  $x \in P$ , also haben wir  $a_j \in P \cap K$ , was aufgrund unserer Voraussetzung  $a_j \neq 0$  ein Widerspruch zu Proposition 2.1.5 (c) ist.

□

*Beweis von Satz 2.1.6:* (a) Angenommen  $P$  wäre kein Hauptideal. Wähle ein Element  $0 \neq x_1 \in P$ . Da nach Voraussetzung  $x_1 \mathcal{O} \neq P$ , gibt es ein Element  $x_2 \in P \setminus x_1 \mathcal{O}$ . Es gilt  $x_2 x_1^{-1} \notin \mathcal{O}$ , also  $x_2^{-1} x_1 \in P$  nach Proposition 2.1.5 (b), also  $x_1 \in x_2 P$ . Iteriert man diese Konstruktion, so erhält man eine unendliche Folge  $x_1, x_2, \dots \in P$  mit  $x_i \in x_{i+1} P$  für alle  $i \geq 1$ , ein Widerspruch zu Lemma 2.1.8!

(b) Zur Eindeutigkeit der Darstellung  $z = t^n u$ ,  $n \in \mathbb{Z}$  und  $u \in \mathcal{O}^*$ : Sei  $t^m v$  eine andere Darstellung mit  $m \in \mathbb{Z}$  und  $v \in \mathcal{O}^*$ . Gelte o.B.d.A  $n \geq m$ . Dann

gilt  $1 = t^{n-m}uv^{-1} \in P$  falls  $n \neq m$ , Widerspruch. Also gilt  $n = m$ , und damit  $1 = uv^{-1}$ , also  $u = v$ .

Zu zeigen bleibt die Existenz einer solchen Darstellung: Da  $\mathcal{O}$  ein Bewertungsring ist, brauchen wir die Existenz nur für  $z \in \mathcal{O}$  zeigen. Für  $z \in \mathcal{O}^*$  haben wir schon eine Darstellung:  $z = t^0z$ . Wir müssen also nur noch den Fall  $z \in P$  behandeln.

**Behauptung:** Es existiert ein maximales  $m \geq 1$  mit  $z \in t^m\mathcal{O}$ .

Um dies einzusehen betrachtet man die Folge

$$x_1 = z, x_2 = t^{m-1}, x_3 = t^{m-2}, \dots, x_m = t.$$

Es gilt  $x_i \in x_{i+1}P$  und nach Lemma 2.1.8 gilt also, dass  $m$  beschränkt ist. Das beweist die Behauptung. Sei also  $z = t^m u$  mit  $u \in \mathcal{O}$ .

**Behauptung:**  $u$  ist Einheit.

Sonst wäre nämlich  $u \in P$ , also  $u \in t\mathcal{O}$ , und damit  $z \in t^{m+1}\mathcal{O}$ , was ein Widerspruch zur Maximalität von  $m$  wäre.

(c) Sei  $\{0\} \neq I \subseteq \mathcal{O}$  ein Ideal. Betrachte die Menge  $A := \{r \in \mathbb{N} : t^r \in I\}$ .  $A$  ist nichtleer, da für  $x \in I$  eine Darstellung  $x = t^r u$  gilt mit  $r \in \mathbb{N}$  und  $u \in \mathcal{O}^*$ . Es gilt  $t^r = xu^{-1} \in I$ . Setze  $n := \min(A)$ . Dann gilt klarerweise  $I \supseteq t^n\mathcal{O}$  weil  $t^n \in I$ . Umgekehrt sei  $0 \neq y \in I$ . Wir können  $y$  schreiben als  $y = t^s w$ ,  $s \in \mathbb{N}$ ,  $w \in \mathcal{O}^*$ , daher gilt  $t^s \in I$ , also  $s \geq n$  und  $y = t^n t^{s-n} w \in t^n\mathcal{O}$ .

□

**Definition 2.1.9** Sei  $F/K$  ein Funktionenkörper.

(a) Eine **Stelle** von  $F/K$  ist ein maximales Ideal  $P$  eines Bewertungsringes  $\mathcal{O}$  von  $F/K$ . Jedes Erzeugendenelement von  $P$  heißt **primes Element** für  $P$ .

(b)  $\mathbb{P}_F := \{P : P \text{ ist Stelle von } F/K\}$ .

Es existiert eine eindeutige Beziehung zwischen Stellen und Bewertungsringen eines Funktionenkörpers  $F/K$ . Man kann nämlich zu jeder Stelle  $P$  den dazugehörigen Bewertungsring  $\mathcal{O}_P$  durch die Relation  $\mathcal{O}_P = \{z \in F : z^{-1} \notin P\}$  zurückgewinnen.  $\mathcal{O}_P$  heißt **der Bewertungsring der Stelle  $P$** .

Man kann Stellen bzw. Bewertungsringe auch anders charakterisieren, und zwar, wie der Name schon vermuten lässt, durch Bewertungen.

**Definition 2.1.10** Eine **diskrete Bewertung** von  $F/K$  ist ein surjektiver Gruppenhomomorphismus  $v$  der multiplikativen Gruppe  $F^*$  auf die additive Gruppe  $\mathbb{Z}$ , vermöge der Relation  $v(0) := \infty$  auf ganz  $F$  ausgedehnt, mit den folgenden Eigenschaften:

(1)  $v(x + y) \geq \min\{v(x), v(y)\}$  für  $x, y \in F$ .

(2)  $v$  verschwindet auf  $K$ .

(1) heißt auch Dreiecksungleichung. Eine Verschärfung liefert das folgende Lemma.

**Lemma 2.1.11 (Starke Dreiecksungleichung)** *Sei  $v$  eine diskrete Bewertung von  $F/K$  und  $x, y \in F$  mit  $v(x) \neq v(y)$ . Dann gilt  $v(x + y) = \min\{v(x), v(y)\}$ .*

*Beweis:* Aus der Definition einer diskreten Bewertung folgt, dass  $v(ay) = v(y)$  für alle  $0 \neq a \in K$ . Es gilt also  $v(-y) = v(y)$ . Da  $v(x) \neq v(y)$  können wir o.B.d.A annehmen, dass  $v(x) < v(y)$  gilt. Angenommen  $v(x + y) \neq \min\{v(x), v(y)\}$ . Dann gilt also  $v(x + y) > v(x)$  und es gilt

$$v(x) = v((x + y) - y) \geq \min\{v(y), v(x + y)\} > v(x),$$

ein Widerspruch. □

Wir wollen nun jeder Stelle, bzw. jedem Bewertungsring in bijektiver Weise eine diskrete Bewertung zuordnen:

**Definition 2.1.12** *Sei  $P \in \mathbb{P}_F$ . Definiere eine Funktion  $v_P : F \rightarrow \mathbb{Z} \cup \{\infty\}$  wie folgt: Wähle ein primes Element  $t$  von  $P$ . Dann besitzt jedes  $0 \neq z \in F$  eine eindeutige Darstellung der Form  $z = t^n u$ ,  $u \in \mathcal{O}_P^*$ . Definiere  $v_P(z) := n$  und  $v_P(0) := \infty$ .*

Wie man leicht sieht hängt diese Definition nicht von der Wahl des primen Elementes von  $P$  ab.

**Satz 2.1.13** *Sei  $F/K$  ein Funktionenkörper.*

(a) *Für jede Stelle  $P \in \mathbb{P}_F$  ist die oben definierte Funktion  $v_P$  eine diskrete Bewertung von  $F/P$ . Es gilt*

$$\begin{aligned} \mathcal{O}_P &= \{z \in F : v_P(z) \geq 0\}, \\ \mathcal{O}_P^* &= \{z \in F : v_P(z) = 0\}, \\ P &= \{z \in F : v_P(z) > 0\}. \end{aligned}$$

*Ein Element  $x \in F$  ist primes Element für  $P$  genau, wenn  $v_P(x) = 1$  gilt.*

(b) *Umgekehrt, sei  $v$  eine diskrete Bewertung von  $F/K$ . Dann ist die Menge  $P := \{z \in F : v(z) > 0\}$  eine Stelle von  $F/K$  und  $\mathcal{O}_P = \{z \in F : v(z) \geq 0\}$ .*

(c) *Jeder Bewertungsring von  $F/K$  ist ein maximaler echter Unterring von  $F$  bezüglich der Inklusionsrelation.*

*Beweis:* (a) Um zu zeigen, dass  $v_P$  eine diskrete Bewertung ist, genügt es die Dreiecksungleichung zu zeigen; die anderen Aussagen sind offensichtlich. Betrachten wir  $x, y \in F$  mit  $v_P(x) = n$  und  $v_P(y) = m$ . Nehmen wir an  $n \leq m < \infty$ . Wir haben also  $x = t^n u_1$  und  $y = t^m u_2$ , mit  $u_1, u_2 \in \mathcal{O}_P^*$ . Dann gilt  $x + y = t^n(u_1 + t^{m-n}u_2) = t^n z$  mit  $z \in \mathcal{O}_P$ . Für  $z = 0$  ist die Aussage trivial, für  $z \neq 0$  können wir eine Darstellung  $z = t^k u$ , mit  $u \in \mathcal{O}_P^*, k \geq 0$ , finden. Daraus folgt  $x + y = t^{n+k}u$  und daraus folgt die

Dreiecksungleichung.

(b) Zunächst ist  $\mathcal{O}_P$  ein Bewertungsring, da für ein  $z \in F$  entweder  $v(z) \geq 0$  oder  $v(z^{-1}) = -v(z) \geq 0$  gilt. Ausserdem ist  $\mathcal{O}_P$  ein Ring, aufgrund der Homomorphieeigenschaft einer Bewertung und es gilt  $K \subseteq \mathcal{O}_P$  wegen Definition 2.1.10 (2). Zu zeigen ist noch, dass  $P = \mathcal{O}_P \setminus \mathcal{O}^*$  gilt. Da aber für ein  $z \in \mathcal{O}_P$  gilt, dass  $z^{-1} \in \mathcal{O}_P$  genau dann, wenn  $v_P(z) = 0$ , ist das offensichtlich.

(c) Sei  $\mathcal{O}$  ein Bewertungsring von  $F/K$ ,  $P$  sein maximales Ideal,  $v_P$  die dazugehörige diskrete Bewertung und  $z \in F \setminus \mathcal{O}$ . Wir zeigen  $F = \mathcal{O}[z]$ . Wegen  $z \notin \mathcal{O}$  gilt  $v_P(z^{-1}) > 0$ . Also existiert für ein beliebiges  $y \in F$  ein  $k \geq 0$  mit  $v_P(yz^{-k}) \geq 0$ , d.h.  $w := yz^{-k} \in \mathcal{O}$ , also  $y = wz^k \in \mathcal{O}[z]$ .

□

Wir haben also gezeigt, dass Stellen, Bewertungsringe und Bewertungen im wesentlichen auf dasselbe hinauslaufen. Sei  $P$  eine Stelle, also ein maximales Ideal von  $\mathcal{O}_P$ , dann ist  $\mathcal{O}_P/P$  ein Körper. Für  $x \in \mathcal{O}_P$  schreiben wir  $x(P)$  für die Restklasse  $x+P$ . Für  $x \notin \mathcal{O}_P$  definieren wir  $x(P) := \infty$ . Wegen Proposition 2.1.5 (c) liefert die kanonische Restklassenabbildung von  $\mathcal{O}_P$  nach  $\mathcal{O}_P/P$  eine kanonische Einbettung von  $K$  (sogar  $\tilde{K}$ ) in  $\mathcal{O}_P/P$ . Auf diese Weise können wir  $K$  als Unterkörper von  $\mathcal{O}_P/P$  betrachten.

**Definition 2.1.14** Sei  $P \in \mathbb{P}_F$ .

(a)  $F_P := \mathcal{O}_P/P$  heißt **Restklassenkörper** von  $P$ . Die Abbildung  $x \mapsto x(P)$  von  $F$  auf  $F_P \cup \{\infty\}$  heißt **Restklassenabbildung** von  $P$ .

(b)  $\deg(P) := [F_P : K]$  heißt **Grad** von  $P$ .

**Proposition 2.1.15** Sei  $P$  eine Stelle von  $F/K$  und  $0 \neq x \in P$ , dann gilt

$$\deg(P) \leq [F : K(x)] < \infty.$$

*Beweis:* Da  $x \in P$ , ist  $x$  transzendent über  $K$ , also  $[F : K(x)] < \infty$ , nach Bemerkung 2.1.2. Zu zeigen bleibt  $\deg(P) \leq [F : K(x)]$ . Seien  $z_1, \dots, z_n \in \mathcal{O}_P$ , sodass die Restklassen  $z_1(P), \dots, z_n(P)$  linear unabhängig über  $K$  sind. Wir zeigen, dass dann  $z_1, \dots, z_n$  linear unabhängig über  $K(x)$  sind. Angenommen es existierte eine nichttriviale Darstellung

$$\sum_{i=1}^n \varphi_i z_i = 0, \tag{2.2}$$

mit  $\varphi_i \in K(x)$ . O.B.d.A. können wir annehmen, dass  $\varphi_i \in K[x]$  und dass nicht alle  $\varphi_i$ 's durch  $x$  teilbar sind. Wir setzen also voraus, dass  $\varphi_i = a_i + xg_i$ , mit  $a_i \in K$ ,  $g_i \in K[x]$

und nicht alle  $a_i = 0$ . Klarerweise gilt  $\varphi_i(P) = a_i$ . Die Restklassenabbildung auf (2.2) angewendet ergibt

$$0 = 0(P) = \sum_{i=1}^n \varphi_i(P) z_i(P) = \sum_{i=1}^n a_i z_i(P).$$

Das ist ein Widerspruch zur linearen Unabhängigkeit von  $z_1(P), \dots, z_n(P)$  über  $K$ .

□

Unter der noch nicht bewiesenen Annahme, dass  $\mathbb{P}_F \neq \emptyset$ , kann man das Folgende zeigen:

**Korollar 2.1.16**  $\tilde{K}$  ist eine endliche Körpererweiterung von  $K$ .

*Beweis:* Wähle ein  $P \in \mathbb{P}_F$ . Wie wir später sehen werden geht das, da  $\mathbb{P}_F \neq \emptyset$  gilt.  $\tilde{K}$  ist vermöge der Restklassenabbildung in  $F_P$  eingebettet und es gilt

$$[\tilde{K} : K] \leq [F_P : K] < \infty.$$

□

**Bemerkung 2.1.17** Sei  $\deg(P) = 1$ . Dann haben wir  $F_P = K$  und die Restklassenabbildung bildet  $F$  auf  $K \cup \{\infty\}$  ab. Wenn  $K$  algebraisch abgeschlossen ist, dann ist insbesondere jede Stelle vom Grad 1 und man kann jedes Element  $z \in F$  in folgendem Sinne als Funktion auffassen:

$$z : \begin{cases} \mathbb{P}_F & \rightarrow & K \cup \{\infty\} \\ P & \mapsto & z(P) \end{cases} \quad (2.3)$$

Aus dieser Beziehung leitet sich der Name Funktionenkörper ab. Die Elemente von  $\tilde{K}$  sind konstant im Sinne von (2.3) und das ist auch der Grund warum  $\tilde{K}$  Konstantenkörper heißt. Auch die folgende Definition ist durch (2.3) gerechtfertigt:

**Definition 2.1.18** Sei  $v_P$  die Bewertung, die  $P$  zugeordnet ist und  $z \in F$ . Dann heisst  $P$

- (a) Nullstelle der Ordnung  $m$  von  $z$ , falls  $v_P(z) = m \geq 0$ .
- (b) Pol der Ordnung  $m$  von  $z$ , falls  $v_P(z) = -m < 0$ .

Nun wollen wir uns mit Hilfe des Lemmas von Zorn überlegen, warum es überhaupt Stellen gibt:

**Satz 2.1.19** Sei  $F/K$  ein Funktionenkörper und  $R$  ein Unterring von  $F$  mit  $K \subseteq R \subseteq F$ . Sei  $I$  ein nichttriviales Ideal von  $R$ . Dann existiert eine Stelle  $P \in \mathbb{P}_F$  mit  $I \subseteq P$  und  $R \subseteq \mathcal{O}_P$ .

*Beweis:* Betrachte die Menge

$$\mathfrak{F} := \{S : S \text{ ist Unterring von } F \text{ mit } R \subseteq S \text{ und } IS \neq S\}^1.$$

Es gilt  $R \in \mathfrak{F}$ , also  $\mathfrak{F} \neq \emptyset$ . Betrachten wir eine Kette  $\mathfrak{H}$  in  $\mathfrak{F}$  bezüglich der Inklusionsrelation. Dann ist  $T := \bigcup \mathfrak{H}$  ein Unterring von  $F$  mit  $R \subseteq T$ . Wir wollen zeigen, dass  $IT \neq T$ . Angenommen es gelte  $IT = T$ , dann gäbe es eine Darstellung  $1 = \sum_{\nu=1}^n a_\nu s_\nu$  mit  $a_\nu \in I$  und  $s_\nu \in T$ . Da  $\mathfrak{H}$  totalgeordnet ist, gibt es ein  $S_0 \in \mathfrak{H}$ , sodass  $s_1, \dots, s_n \in S_0$ , also gilt  $1 \in IS_0$ , d.h.  $IS_0 = S_0$ , und das ist ein Widerspruch. Nach dem Lemma von Zorn existiert also ein maximales Element  $\mathcal{O}$  in  $\mathfrak{F}$ . Wir zeigen, dass  $\mathcal{O}$  ein Bewertungsring ist:

Da  $I \neq \{0\}$  und  $I\mathcal{O} \neq \mathcal{O}$ , haben wir  $\mathcal{O} \subset F$  und  $I \subseteq \mathcal{O} \setminus \mathcal{O}^*$ . Angenommen es gibt ein Element  $z \in F$  mit  $z \notin \mathcal{O}$  und  $z^{-1} \notin \mathcal{O}$ . Dann gilt wegen der Maximalität von  $\mathcal{O}$ , dass  $I\mathcal{O}[z] = \mathcal{O}[z]$  und  $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$  und wir können  $a_0, \dots, a_n, b_0, \dots, b_m \in I\mathcal{O}$  finden, sodass

$$1 = a_0 + a_1 z + \dots + a_n z^n \text{ und} \quad (2.4)$$

$$1 = b_0 + b_1 z^{-1} + \dots + b_m z^{-m} \quad (2.5)$$

Klarerweise gilt  $n, m \geq 1$  und wir wählen  $m$  und  $n$  zusätzlich minimal und fordern o.B.d.A.  $n \geq m$ . Multipliziert man (2.4) mit  $1 - b_0$  und (2.5) mit  $a_n z^n$ , dann erhält man

$$\begin{aligned} 1 - b_0 &= (1 - b_0)a_0 + (1 - b_0)a_1 z + \dots + (1 - b_0)a_n z^n \text{ und} \\ 0 &= (b_0 - 1)a_n z^n + b_1 a_n z^{n-1} + \dots + b_m a_n z^{n-m} \end{aligned}$$

Addiert man diese beiden Gleichungen, so erhält man eine Gleichung der Form

$$1 = c_0 + c_1 z + \dots + c_{n-1} z^{n-1}$$

mit Koeffizienten  $c_i \in I\mathcal{O}$ . Das ist ein Widerspruch zur Minimalität von  $n$  in (2.4). Es gilt also  $z \in \mathcal{O}$  oder  $z^{-1} \in \mathcal{O}$  und  $\mathcal{O}$  ist ein Bewertungsring von  $F/K$ . □

**Korollar 2.1.20** *Sei  $F/K$  ein Funktionenkörper und  $z \in F$  transzendent über  $K$ . Dann hat  $z$  mindestens eine Nullstelle und einen Pol. Insbesondere gilt  $\mathbb{P}_F \neq \emptyset$ .*

*Beweis:* Betrachte den Ring  $R = K[z]$  und das Ideal  $zK[z]$ . Wegen Satz 2.1.19 gibt es eine Stelle  $P \in \mathbb{P}_F$  mit  $z \in P$ , also ist  $P$  Nullstelle von  $z$ . Dieselbe Argumentation auf  $z^{-1}$  angewendet zeigt die Existenz eines Pols von  $z$ . □

---

<sup>1</sup> $IS$  sei hier die lineare Hülle von  $I$  als  $S$ -Modul aufgefasst.

## 2.2 Der rationale Funktionenkörper

Wir diskutieren im Folgenden die zentralen Eigenschaften des einfachsten Funktionenkörpers, des rationalen Funktionenkörpers über einem Körper  $K$ . Ein Verständnis des rationalen Funktionenkörpers ist notwendig wenn man die Theorie verstehen möchte, speziell im Hinblick auf Funktionenkörpertürme. An dieser Stelle sei auch auf eine Parallele zur algebraischen Zahlentheorie hingewiesen, wo man ja algebraische Zahlkörper, also endliche Erweiterungen von  $\mathbb{Q} = \mathbb{Q}(\mathbb{Z})$  betrachtet. Wir betrachten endliche Erweiterungen von  $K(x) = \mathbb{Q}(K[x])$ . Bekannterweise haben die Ringe  $\mathbb{Z}$  und  $K[x]$ , der Polynomring in einer Variablen über einem Körper  $K$ , sehr viele ringtheoretische Eigenschaften gemein. Wir interessieren uns hier für Stellen des rationalen Funktionenkörpers  $K(x)/K$ . Die Stellen sind nichts anderes als Bewertungen. Im Falle  $\mathbb{Q}$  existieren genau die  $p$ -adischen Bewertungen und der Betrag. Ein analoges Resultat gilt auch für den rationalen Funktionenkörper, der Beweis ist im Grunde derselbe, er basiert darauf, dass der Ring  $K[x]$ , genau wie der Ring  $\mathbb{Z}$ , ein Hauptidealring ist.

Betrachten wir also für ein normiertes, irreduzibles Polynom  $p(x) \in K[x]$  den Bewertungsring

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \quad (2.6)$$

von  $K(x)/K$  mit dem maximalen Ideal

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\} \quad (2.7)$$

Dass der durch (2.6) definierte Unterring von  $K(x)$  tatsächlich ein Bewertungsring ist, ist trivial, ebenso wie die Tatsache, dass das durch (2.7) Ideal die dazugehörige Stelle ist. Im Fall  $p(x) = x - \alpha$ ,  $\alpha \in K$ , schreiben wir abkürzend

$$P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}. \quad (2.8)$$

Diese Stellen entsprechen den  $p$ -adischen Bewertungen auf  $\mathbb{Q}$ , wenn man statt eines irreduziblen Polynoms eine Primzahl heranzieht. Analog zum Betrag auf  $\mathbb{Q}$  existiert noch ein weiterer Bewertungsring von  $K(x)/K$ , und zwar

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg(f(x)) \leq \deg(g(x)) \right\} \quad (2.9)$$

mit maximalem Ideal

$$P_\infty := \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], \deg(f(x)) < \deg(g(x)) \right\}. \quad (2.10)$$

$P_\infty$  heißt die **Unendlichkeitsstelle** von  $K(x)$ . Es sei darauf hingewiesen, dass diese Definition von der Wahl des Elementes  $x$  in  $K(x)/K$  abhängt. Es gilt klarerweise  $K(x) = K(\frac{1}{x})$ , aber die Unendlichkeitsstelle  $P_\infty$  in  $K(x)/K$  ist genau die Stelle  $P_0$  in  $K(\frac{1}{x})/K$ .

**Proposition 2.2.1** Sei  $F = K(x)$  der rationale Funktionenkörper.

- (a) Sei  $P = P_{p(x)}$  die Stelle definiert durch (2.7),  $p(x)$  sei ein normiertes, irreduzibles Polynom aus  $K[x]$ . Dann ist  $p(x)$  ein primitives Element von  $P$  und die dazugehörige diskrete Bewertung lässt sich wie folgt beschreiben: Sei  $0 \neq z \in K(x)$ . Hat  $z$  die Darstellung  $z = p(x)^n \frac{f(x)}{g(x)}$  mit  $n \in \mathbb{Z}$ ,  $f(x), g(x) \in K[x]$ ,  $p(x) \nmid f(x)$ ,  $p(x) \nmid g(x)$ , dann gilt  $v_P(z) = n$ . Es gilt  $F_P \cong K[x]/(p(x))$ , vermöge

$$\Phi : \begin{cases} K[x]/(p(x)) & \rightarrow K(x)_P \\ f(x) \bmod p(x) & \mapsto f(x)(P). \end{cases}$$

Insbesondere gilt  $\deg(P) = \deg(p(x))$ .

- (b) Speziell im Fall  $P(x) = x - \alpha$ ,  $\alpha \in K$ , ist  $\deg(P) = \deg(P_\alpha) = 1$  und die Restklassenabbildung ist gegeben durch

$$z(P) = z(\alpha) \text{ für } \alpha \in K,$$

wobei  $z(\alpha)$  durch den Einsetzungshomomorphismus von  $K(x)$  auf  $K(\alpha)$  definiert ist, falls  $z = \frac{f(x)}{g(x)}$  mit  $g(\alpha) \neq 0$ , ansonsten gilt  $z(\alpha) = \infty$ .

- (c) Betrachten wir  $P = P_\infty$ . Dann gilt  $\deg(P) = 1$  und  $\frac{1}{x}$  ist ein primes Element von  $P$ . Die Bewertung  $v_P$  ist gegeben durch:

$$v_P \left( \frac{f(x)}{g(x)} \right) = \deg(g(x)) - \deg(f(x)),$$

$f(x), g(x) \in K[x]$ . Die Restklassenabbildung lautet wie folgt: Sei  $z = f(x)/g(x) \in K(x)$ , dann ist  $z(P) = \lim_{x \rightarrow \infty} f(x)/g(x)$ .

- (d)  $K$  ist der volle Konstantenkörper von  $K(x)/K$ .

*Beweis:* Der Beweis hat den Charakter eines Algebra-Übungsbeispiels. Ich möchte daher nur die wichtigsten Aussagen zeigen:

- (a) Die Aussage über die Bewertung  $v_P$  ist klar. Um zu zeigen, dass  $\Phi$  ein Isomorphismus ist, betrachte die Abbildung  $\varphi$  definiert durch

$$\varphi : \begin{cases} K[x] & \rightarrow K(x)_P \\ f(x) & \mapsto f(x)(P) \end{cases}$$

Klarerweise gilt  $\ker(\varphi) = (p(x))$ . Wir zeigen, dass  $\varphi$  surjektiv ist: Sei  $z \in \mathcal{O}_P$ . Schreibe  $z = u(x)/v(x)$ , mit  $u(x), v(x) \in K[x]$  und  $p(x) \nmid v(x)$ . Aus der Hauptidealringeneigenschaft von  $K[x]$  folgt die Existenz von Polynomen  $a(x), b(x) \in K[x]$  mit  $a(x)p(x) + b(x)v(x) = 1$ . Es folgt

$$z = 1 \cdot z = \frac{a(x)u(x)}{v(x)}p(x) + b(x)u(x),$$

und  $z(P) = \varphi(b(x)u(x))$ , also ist  $\varphi$  surjektiv. Wir haben

$$\begin{array}{ccc} K[x] & \xrightarrow{\varphi} & K(x)_P \\ \downarrow \pi & \nearrow \Phi & \\ K[x]/(p(x)) & & \end{array}$$

$\pi$  ist die kanonische Restklassenabbildung modulo  $(p(x))$ . Aus dem Homomorphiesatz folgt die behauptete Isomorphie.

(b) Für  $f(x) \in K[x]$  gilt  $(x - \alpha) \mid (f(x) - f(\alpha))$ , also gilt  $f(x)(P) = (f(x) - f(\alpha))(P) + f(\alpha)(P) = f(\alpha)$ . Der Rest ist klar.

(c) Wir zeigen nur, dass  $\frac{1}{x}$  ein primes Element von  $P_\infty$  ist. Betrachte ein Element  $z = \frac{f(x)}{g(x)} \in P_\infty$ , d.h.  $\deg(f(x)) < \deg(g(x))$ . Dann gilt

$$z = \frac{1}{x} \cdot \frac{xf(x)}{g(x)}, \quad \text{mit } \deg(xf(x)) \leq \deg(g(x)),$$

und daraus folgt  $z \in \frac{1}{x}\mathcal{O}_\infty$ , also ist  $\frac{1}{x}$  ein primes Element.

(d) Wähle eine Stelle  $P = P_\alpha$ . Es gilt  $K \subseteq \tilde{K} \subseteq K(x)_P = K$ .

□

Proposition 2.2.1 besagt im Grunde genommen, dass unsere Interpretation von Elementen eines Funktionenkörpers als Funktionen mit der offensichtlichen Interpretation von Elementen aus  $K(x)$  als rationale Funktionen, übereinstimmt.

**Satz 2.2.2** Die Stellen  $P_{p(x)}$  und  $P_\infty$ , definiert durch (2.7) und (2.10) sind alle Stellen von  $K(x)/K$ .

*Beweis: 1. Fall:*  $x \in \mathcal{O}_P$ : Dann gilt  $K[x] \subseteq \mathcal{O}_P$ . Setze  $I := P \cap K[x]$ . Dann ist  $I$  ein Primideal von  $K[x]$ .  $I \neq \{0\}$ , da die Restklassenabbildung eine Einbettung von  $K[x]/I$  in  $K(x)_P$ , eine endliche Körpererweiterung von  $K$  induziert. Daraus folgt die Existenz eines irreduziblen Polynoms  $p(x) \in K[x]$  mit  $I = P \cap K[x] = p(x)K[x]$ . Jedes  $g(x)$  mit  $p(x) \nmid g(x)$  ist nicht in  $I$ , also auch nicht in  $P$ , daher ist  $1/g(x) \in \mathcal{O}_P$ . Wir fassen zusammen:

$$\mathcal{O}_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) \nmid g(x) \right\} \subseteq \mathcal{O}_P.$$

Da Bewertungsringe maximale Unterringe sind, gilt Gleichheit.

**2. Fall:**  $x \notin \mathcal{O}_P$ : Dann gilt  $K[x^{-1}] \subseteq \mathcal{O}_P$ ,  $x^{-1} \in P \cap K[x^{-1}]$  und  $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$ . Wie im ersten Fall hat man

$$\begin{aligned} \mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} : f(x^{-1}), g(x^{-1}) \in K[x^{-1}], x^{-1} \nmid g(x^{-1}) \right\} \\ &= \left\{ \frac{a_0 + a_1x^{-1} + \dots + a_nx^{-n}}{b_0 + b_1x^{-1} + \dots + b_mx^{-m}} : b_0 \neq 0 \right\} \\ &= \left\{ \frac{a_0x^{m+n} + \dots + a_nx^m}{b_0x^{m+n} + \dots + b_mx^n} : b_0 \neq 0 \right\} \\ &= \left\{ \frac{u(x)}{v(x)} : u(x), v(x) \in K[x], \deg(u(x)) \leq \deg(v(x)) \right\} \\ &= \mathcal{O}_\infty. \end{aligned}$$

Also gilt  $\mathcal{O}_P = \mathcal{O}_\infty$ . □

**Korollar 2.2.3** *Die Stellen vom Grad 1 von  $K(x)/K$  stehen in bijektivem Zusammenhang mit  $K \cup \{\infty\}$*

Der Beweis dieses Korollars ist nach dem Vorangegangenen trivial.

## 2.3 Der schwache Approximationssatz

Ziel dieses Abschnitts ist die Herleitung des schwachen Approximationssatzes für Bewertungen. Die Aussage dieses Satzes ist im Wesentlichen, dass man für  $n$  paarweise verschiedene Bewertungen  $v_1, \dots, v_n$  eines Funktionenkörpers  $F/K$  aus den Werten  $v_1(z), \dots, v_{n-1}(z)$  für ein Element  $z \in F/K$ , nichts über den Wert  $v_n(z)$  aussagen kann. Darum wird der schwache Approximationssatz manchmal auch als Unabhängigkeitssatz bezeichnet.

**Satz 2.3.1 (Schwacher Approximationssatz)** *Sei  $F/K$  ein Funktionenkörper,  $P_1, \dots, P_n \in \mathbb{P}_F$  paarweise verschiedene Stellen von  $F/K$ ,  $x_1, \dots, x_n \in F$  und  $r_1, \dots, r_n \in \mathbb{Z}$ . Dann existiert ein  $x \in F$  mit*

$$v_{P_i}(x - x_i) = r_i \text{ für } i = 1, \dots, n.$$

*Beweis:* Da der Beweis eher technischer Natur ist, zerlegen wir ihn in mehrere Schritte. Wir bezeichnen mit  $v_i$  die Bewertung  $v_{P_i}$ .

**Schritt 1:** Es existiert ein  $u \in F$  mit  $v_1(u) > 0$  und  $v_i(u) < 0$  für  $i = 2, \dots, n$ .

*Beweis von Schritt 1:* Wir beweisen diese Aussage durch Induktion über  $n$ . Sei  $n = 2$ . Da  $\mathcal{O}_{P_1} \not\subseteq \mathcal{O}_{P_2}$  und umgekehrt (wegen der Maximalität von Bewertungsringen), können

wir ein  $y_1 \in \mathcal{O}_{P_1} \setminus \mathcal{O}_{P_2}$  und ein  $y_2 \in \mathcal{O}_{P_2} \setminus \mathcal{O}_{P_1}$  finden. Das Element  $u := y_1/y_2$  hat die gewünschte Eigenschaft.

Sei  $n > 2$ . Nach Induktionsvoraussetzung existiert ein  $y \in F$  mit  $v_1(y) > 0$  und  $v_i(y) < 0$  für  $i = 2, \dots, n-1$ . Wenn  $v_n(y) < 0$ , dann sind wir fertig. Betrachten wir also den Fall  $v_n(y) \geq 0$ . Wähle ein  $z \in F$  mit  $v_1(z) > 0$  und  $v_n(z) < 0$  und setze  $u := y + z^r$ , wobei  $r \geq 1$  so gewählt wird, dass  $r \cdot v_i(z) \neq v_i(y)$  für  $i = 1, \dots, n-1$ . Es gilt  $v_1(u) \geq \min\{v_1(y), r \cdot v_1(z)\} > 0$  und  $v_i(u) = \min\{v_i(y), r \cdot v_i(z)\} < 0$  für  $i = 2, \dots, n$  wegen der strikten Dreiecksungleichung. Das beweist die Behauptung.

**Schritt 2:** Es existiert ein  $w \in F$  mit  $v_1(w-1) > r_1$  und  $v_i(w) > r_i$  für  $i = 2, \dots, n$ .

*Beweis von Schritt 2:* Wähle  $u \in F$  wie in Schritt 1 und setze  $w := (1 + u^s)^{-1}$ . Für  $s \in \mathbb{N}$  gross genug haben wir  $v_1(w-1) = v_1(-u^s(1 + u^s)^{-1}) = s \cdot v_1(u) > r_1$ , und  $v_i(w) = -v_i(1 + u^s) = -s \cdot v_i(u) > r_i$  für  $i = 2, \dots, n$ .

**Schritt 3:** Seien  $y_1, \dots, y_n \in F$  gegeben. Dann existiert ein Element  $z \in F$  mit  $v_i(z - y_i) > r_i$  für  $i = 1, \dots, n$ .

*Beweis von Schritt 3:* Wähle  $s \in \mathbb{Z}$ , sodass  $v_i(y_j) \geq s$  für alle  $i, j \in \{1, \dots, n\}$ . Nach Schritt 2 existieren  $w_1, \dots, w_n$  mit

$$v_i(w_i - 1) > r_i - s \text{ und } v_i(w_j) > r_i - s \text{ für } i \neq j.$$

$z := \sum_{j=1}^n y_j w_j$  erfüllt die behauptete Eigenschaft.

**Schritt 4:** Nach Schritt 3 können wir ein  $z \in F$  finden mit  $v_i(z - x_i) > r_i$ ,  $i = 1, \dots, n$ . Wählen wir  $z_i$  mit  $v_i(z_i) = r_i$ . Dann existiert, wieder nach Schritt 3, ein Element  $z'$  mit  $v_i(z' - z_i) > r_i$ , für  $i = 1, \dots, n$ . Es folgt:

$$v_i(z') = v_i((z' - z_i) + z_i) = \min\{v_i(z' - z_i), v_i(z_i)\} = r_i.$$

Setze  $x := z + z'$ . Dann gilt

$$v_i(x - x_i) = v_i((z - x_i) + z') = \min\{v_i(z - x_i), v_i(z')\} = r_i.$$

□

**Korollar 2.3.2** *Jeder Funktionenkörper  $F/K$  hat unendlich viele Stellen.*

*Beweis:* Angenommen es existierten nur endlich viele Stellen  $P_1, \dots, P_n$ . Nach dem schwachen Approximationssatz können wir ein Element  $0 \neq x \in F$  finden, mit  $v_{P_i}(x) > 0$ , für  $i = 1, \dots, n$ .  $x$  ist transzendent über  $K$ , da es Nullstellen besitzt.  $x$  hat aber keine Pole und das ist ein Widerspruch zu Korollar 2.1.20.

□

**Proposition 2.3.3** Sei  $F/K$  ein Funktionenkörper und  $P_1, \dots, P_r$  Nullstellen eines Elements  $x \in F$ . Dann gilt

$$\sum_{i=1}^r v_{P_i}(x) \cdot \deg(P_i) \leq [F : K(x)].$$

*Beweis:* Setze  $v_i := v_{P_i}$ ,  $f_i := \deg(P_i)$  und  $e_i := v_{P_i}(x)$ . Für jedes  $i$  existiert ein Element  $t_i$  mit

$$v_i(t_i) = 1 \text{ und } v_k(t_i) = 0 \text{ für } k \neq i.$$

Wähle  $s_{i1}, \dots, s_{if_i} \in \mathcal{O}_{P_i}$  sodass  $s_{i1}(P_i), \dots, s_{if_i}(P_i)$  eine Basis von  $F_{P_i}$  über  $K$  bilden. Aus dem schwachen Approximationssatz folgt, dass man Elemente  $z_{ij} \in F$  finden kann mit

$$v_i(s_{ij} - z_{ij}) > 0 \text{ und } v_k(z_{ij}) \geq e_k \text{ für } k \neq i. \quad (2.11)$$

Wir behaupten, dass die Elemente

$$t_i^a \cdot z_{ij}, \quad 1 \leq i \leq r, \quad 1 \leq j \leq f_i, \quad 0 \leq a < e_i$$

linear unabhängig über  $K(x)$  sind. Daraus folgt dann die Proposition. Nehmen wir also an es existierte eine nichttriviale Linearkombination

$$\sum_{i=1}^r \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a z_{ij} = 0 \quad (2.12)$$

über  $K(x)$ . O.B.d.A. können wir annehmen, dass  $\varphi_{ija} \in K[x]$ , und nicht alle  $\varphi_{ija}$  sind durch  $x$  teilbar. Dann finden wir Indizes  $k \in \{1, \dots, r\}$  und  $c \in \{0, \dots, e_k - 1\}$  mit

$$x \mid \varphi_{kja} \text{ für alle } a < c \text{ und alle } j \in \{1, \dots, f_k\},$$

$$\text{und } x \nmid \varphi_{kjc} \text{ für ein } j \in \{1, \dots, f_k\}. \quad (2.13)$$

Multipliziert man (2.12) mit  $t_k^{-c}$ , so erhält man

$$\sum_{i=1}^r \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} = 0. \quad (2.14)$$

Für  $i \neq k$  sind alle Summanden von (2.14) in  $P_k$ , da

$$v_k(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) \geq 0 + 0 - c + e_k > 0.$$

Für  $i = k$  und  $a < c$  haben wir

$$v_k(\varphi_{kja} t_k^a t_k^{-c} z_{kj}) \geq e_k + a - c \geq e_k - c > 0.$$

Es gilt nämlich  $x \mid \varphi_{kja}$  und daher  $v_k(\varphi_{kja}) \geq e_k$ . Sei nun  $i = k$  und  $a > c$ . Dann gilt

$$v_k(\varphi_{kja} t_k^a t_k^{-c} z_{kj}) \geq a - c > 0.$$

Kombiniert man diese Ergebnisse mit (2.14), so erhält man

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \in P_k. \quad (2.15)$$

Es gilt  $\varphi_{kjc}(P_k) \in K$  und nicht alle  $\varphi_{kjc}(P_k) = 0$  wegen (2.13) also ergibt (2.15) eine nichttriviale Linearkombination

$$\sum_{j=1}^{f_k} \varphi_{kjc}(P_k) \cdot z_{kj}(P_k) = 0$$

über  $K$ . Das ist ein Widerspruch, da  $z_{k1}(P_k), \dots, z_{kf_k}(P_k)$  eine Basis von  $F_{P_k}/K$  bilden. □

Die folgende Aussage ist eine triviale Konsequenz der obigen Proposition:

**Korollar 2.3.4** *In einem Funktionenkörper hat jedes Element  $0 \neq x \in F$  nur endlich viele Nullstellen und Pole.*

## 2.4 Divisoren

Im folgenden setzen wir voraus, dass  $K$  der volle Konstantenkörper ist.  $\tilde{K}$  ist eine endliche Körpererweiterung von  $K$  und  $F$  kann als Funktionenkörper über  $\tilde{K}$  aufgefasst werden. Die obige Forderung ist also keine große Einschränkung.

**Definition 2.4.1** *Die freie abelsche Gruppe, die von den Stellen von  $F/K$  erzeugt wird, heißt **Divisorgruppe** und wird mit  $\mathcal{D}_F$  bezeichnet. Die Elemente von  $\mathcal{D}_F$  heißen **Divisoren**. Sei ein Divisor*

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ mit } n_P \in \mathbb{Z}, \text{ fast alle } n_P = 0,$$

gegeben. Dann definieren wir den **Träger** von  $P$  durch:

$$\text{supp}(D) := \{P \in \mathbb{P}_F : n_P \neq 0\}.$$

Weiters definieren wir  $v_Q(D) := n_Q$  für  $Q \in \mathbb{P}_F$ . Wir definieren eine partielle Ordnung auf  $\mathcal{D}_F$  durch

$$D_1 \leq D_2 :\Leftrightarrow v_P(D_1) \leq v_P(D_2) \text{ für alle } P \in \mathbb{P}_F.$$

Ein Divisor  $D$  heißt **positiv**, falls  $D \geq 0$  gilt. Die Gradabbildung  $\text{deg} : \mathbb{P}_F \rightarrow \mathbb{Z}$  wird mittels der universellen Eigenschaft der freien abelschen Gruppe auf  $\mathcal{D}_F$  fortgesetzt.

Da ein Element  $0 \neq x \in F$  nur endlich viele Nullstellen und Pole hat, macht die folgende Definition Sinn:

**Definition 2.4.2** Sei  $0 \neq x \in F$  und bezeichne mit  $Z$  (bzw.  $N$ ) die Menge der Nullstellen (bzw. Pole) von  $x$ . Dann definieren wir

$$(x)_0 := \sum_{P \in Z} v_P(x)P, \text{ den Nullstellendivisor von } x,$$

$$(x)_\infty := \sum_{P \in N} -v_P(x)P, \text{ den Poldivisor von } x,$$

$$(x) := (x)_0 - (x)_\infty, \text{ den Hauptdivisor von } x.$$

Offensichtlich gilt (wegen unserer Annahme  $K = \tilde{K}$  und Korollar 2.1.20)

$$x \in K \Leftrightarrow (x) = 0.$$

**Definition 2.4.3** Wir definieren die **Hauptdivisorengruppe**

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

Da  $(xy) = (x) + (y)$  für  $x, y \in F$ , ist  $\mathcal{P}_F$  tatsächlich eine Gruppe. Die Faktorgruppe

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

heißt **Divisorklassengruppe**. Liegen zwei Divisoren  $D_1$  und  $D_2$  in derselben Nebenklasse bzgl.  $\mathcal{P}_F$ , so schreiben wir

$$D_1 \sim D_2.$$

Die folgende Definition ist von fundamentaler Bedeutung in der Theorie der Funktionenkörper.

**Definition 2.4.4** Für einen Divisor  $A \in \mathcal{D}_F$  definieren wir den **Riemann-Roch Raum**

$$\mathcal{L}(A) := \{x \in F : (x) \geq -A\} \cup \{0\}.$$

Für

$$A = \sum_{i=1}^r n_i P_i - \sum_{j=1}^s m_j Q_j,$$

mit  $n_i, m_j > 0$ , besteht  $\mathcal{L}(A)$  also genau aus jenen Elementen  $x \in F$  mit

- (1)  $x$  hat Nullstellen der Ordnung  $\geq m_j$  bei  $Q_j$ , für  $j = 1, \dots, s$ , und
- (2)  $x$  kann nur Polstellen bei  $P_1, \dots, P_r$  haben, wobei die Ordnung der Polstelle bei  $P_i$  durch  $n_i$  beschränkt ist für  $i = 1, \dots, r$ .

Die folgende Bemerkung ist eine einfache Folgerung aus Definition 2.4.4, die uns später immer wieder wertvolle Dienste leisten wird.

**Bemerkung 2.4.5** Sei  $A \in \mathcal{D}_F$ . Dann gilt:

- (a)  $x \in \mathcal{L}(A) \Leftrightarrow v_P(x) \geq -v_P(A)$  für alle  $P \in \mathbb{P}_F$ .
- (b)  $\mathcal{L}(A) \neq \{0\} \Leftrightarrow \exists A' \sim A : A' \geq 0$ .

**Lemma 2.4.6** Sei  $A, A' \in \mathcal{D}_F$ . Dann gilt

- (a)  $\mathcal{L}(A)$  ist ein Vektorraum über  $K$ .
- (b) Wenn  $A \sim A'$ , dann sind  $\mathcal{L}(A)$  und  $\mathcal{L}(A')$  isomorph als  $K$ -Vektorräume.

*Beweis:* (a) Sei  $x, y \in \mathcal{L}(A)$  und  $a \in K$ . Dann gilt für  $P \in \mathbb{P}_F$ :

$$v_P(x + y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(A),$$

und

$$v_P(ax) = v_P(a) + v_P(x) = v_P(x) \geq -v_P(A).$$

Wegen Bemerkung 2.4.5 (a) gilt also  $x + y, ax \in \mathcal{L}(A)$ .

(b) Sei  $A' = A + (z)$ . Die Abbildung  $\varphi : x \mapsto x \cdot z$  liefert den gesuchten Isomorphismus von  $\mathcal{L}(A')$  auf  $\mathcal{L}(A)$ .

□

**Lemma 2.4.7** Es gilt:

- (a)  $\mathcal{L}(0) = K$ .
- (b) Sei  $A < 0$ , dann ist  $\mathcal{L}(A) = \{0\}$ .

*Beweis:* (a) Für jedes  $x \in K$  gilt  $(x) = 0$ , also ist  $K \subseteq \mathcal{L}(0)$ . Sei umgekehrt  $x \in \mathcal{L}(0)$ . Dann gilt  $(x) \geq 0$ . Also hat  $x$  keine Polstelle und liegt daher in  $K$  nach Korollar 2.1.20.

(b) Sei  $x \in \mathcal{L}(A) \setminus \{0\}$ . Dann gilt  $(x) \geq -A > 0$ . Daher liegt  $x$  nicht in  $K$  und hat aber keinen Pol. Widerspruch!

□

Wir machen eine erste (einfache) Aussage über die Dimension des Riemann-Roch Raums:

**Lemma 2.4.8** Seien  $A, B \in \mathcal{D}_F$  mit  $A \leq B$  für einen Funktionenkörper  $F/K$ . Dann gilt  $\mathcal{L}(A) \subseteq \mathcal{L}(B)$  und

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \deg(B) - \deg(A).$$

*Beweis:*  $\mathcal{L}(A) \subseteq \mathcal{L}(B)$  ist klar. Um die zweite Aussage zu beweisen betrachten wir den Fall  $B = A + P$  für ein  $P \in \mathbb{P}_F$ . Der allgemeine Fall folgt dann durch Induktion. Wähle nun ein Element  $t \in F$  mit  $v_P(t) = v_P(B) = v_P(A) + 1$ . Sei  $x \in \mathcal{L}(B)$ . Dann gilt  $v_P(x) \geq -v_P(B) = -v_P(t)$ . Wir haben daher  $xt \in \mathcal{O}_P$  und bekommen eine lineare Abbildung

$$\psi : \begin{cases} \mathcal{L}(B) & \rightarrow & F_P \\ x & \mapsto & (xt)(P). \end{cases}$$

Es ist  $x \in \ker(\psi)$  genau dann, wenn  $v_P(xt) > 0$ , d.h.  $v_P(x) \geq -v_P(A)$ . Daher gilt  $\ker(\psi) = \mathcal{L}(A)$ . Wir haben

$$\begin{array}{ccc} \mathcal{L}(B) & \xrightarrow{\psi} & \text{Im}(\psi) \subseteq F_P \\ \downarrow \pi & \nearrow \bar{\psi} := \psi \circ \pi^{-1} & \\ \mathcal{L}(B)/\mathcal{L}(A) & & \end{array}$$

wobei  $\pi$  die Restklassenabbildung modulo  $\mathcal{L}(A)$  bezeichnet.  $\bar{\psi}$  ist ein  $K$ -Vektorraumisomorphismus und daher gilt

$$\dim(\mathcal{L}(B)/\mathcal{L}(A)) \leq \dim(F_P) = \deg(B) - \deg(A).$$

□

**Proposition 2.4.9** *Für  $A \in \mathcal{D}_F$  ist  $\mathcal{L}(A)$  ein endlichdimensionaler  $K$ -Vektorraum. Genauer gilt für  $A = A_+ - A_-$ , wobei  $A_+, A_-$  positiv sind,*

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

*Beweis:* Da  $\mathcal{L}(A) \subseteq \mathcal{L}(A_+)$ , genügt es zu zeigen, dass

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

Wegen  $0 \leq A_+$  gilt nach Lemma 2.4.8

$$\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) = \dim(\mathcal{L}(A_+)/K) = \dim(\mathcal{L}(A_+)) - 1 \leq \deg(A_+).$$

□

**Definition 2.4.10** *Sei  $A \in \mathcal{D}_F$ . Wir definieren die **Dimension** von  $A$  durch  $\dim(A) := \dim(\mathcal{L}(A))$ .*

Nun zeigen wir, dass die Anzahl der Nullstellen gleich der Anzahl der Pole ist, wenn man sie nur richtig zählt:

**Satz 2.4.11** *Sei  $x \in F$  nicht konstant. Dann gilt*

$$\deg(x)_0 = \deg(x)_\infty = [F : K(x)].$$

*Insbesondere gilt, dass jeder Hauptdivisor Grad Null hat.*

*Beweis:* Sei  $n := [F : K(x)]$  und

$$B := (x)_\infty = \sum_{i=1}^r -v_{P_i}(x)P_i,$$

wobei  $P_1, \dots, P_r$  alle Pole von  $x$  sind. Dann gilt

$$\deg(B) = \sum_{i=1}^r v_{P_i}(x^{-1}) \cdot \deg(P_i) \leq [F : K(x)] = n$$

nach Proposition 2.3.3. Wir müssen noch zeigen, dass  $n \leq \deg(B)$  gilt. Wählen wir also eine Basis  $u_1, \dots, u_n$  von  $F$  über  $K(x)$  und einen Divisor  $C \geq 0$  sodass  $(u_i) \geq -C$  für  $i = 1, \dots, n$ .

**Behauptung:** Es gilt

$$\dim(lB + C) \geq n(l + 1) \text{ für alle } l \geq 0. \quad (2.16)$$

Die Elemente  $x^i u_j$  liegen in  $\mathcal{L}(lB + C)$  für  $0 \leq i \leq l$ ,  $0 \leq j \leq n$ , da

$$v_P(x^i u_j) = i v_P(x) + v_P(u_j) = -i v_P(B) + v_P(u_j) \geq -l v_P(B) - v_P(C)$$

für alle  $0 \leq i \leq l$ ,  $0 \leq j \leq n$  gilt. Sie sind weiters linear unabhängig über  $K$ , weil die Elemente  $u_1, \dots, u_n$  linear unabhängig über  $K(x)$  sind. Das beweist die Behauptung.

Setze  $c := \deg(C)$ . Dann gilt nach (2.16) und Proposition 2.4.9

$$n(l + 1) \leq \dim(lB + C) \leq l \cdot \deg(B) + c + 1.$$

Also haben wir

$$l(\deg(B) - n) \geq n - c - 1 \text{ für alle } l \geq 0.$$

Das ist nur möglich für  $\deg(B) \geq n$ . Also gilt

$$\deg(x)_\infty = [F : K(x)] = [F : K(x^{-1})] = \deg(x^{-1})_\infty = \deg(x)_0.$$

□

**Korollar 2.4.12** Sei  $A \in \mathcal{D}_F$ .

- (a) Für  $A' \sim A$  gilt  $\dim(A') = \dim(A)$  und  $\deg(A') = \deg(A)$ .
- (b) Wenn  $\deg(A) < 0$ , dann gilt  $\dim(A) = 0$ .
- (c) Wenn  $\deg(A) = 0$ , dann sind die folgenden Aussagen äquivalent:

- (1)  $A$  ist Hauptdivisor.
- (2)  $\dim(A) \geq 1$ .
- (3)  $\dim(A) = 1$ .

*Beweis:* (a) folgt aus dem obigen Satz und Lemma 2.4.6.

(b) Angenommen es gelte  $\dim(A) > 0$ . Nach Bemerkung 2.4.5 existiert dann ein Divisor  $A' \sim A$  mit  $A' \geq 0$ . Daraus folgt  $\deg(A) = \deg(A') \geq 0$ , Widerspruch.

(c) (1) $\Rightarrow$ (2): Sei  $A = (x)$ , dann ist  $(x^{-1}) \in \mathcal{L}(A)$ , also  $\dim(A) \geq 1$ .

(2) $\Rightarrow$ (3) Angenommen  $\dim(A) \geq 1$ . Dann existiert ein  $A' \geq 0$  mit  $A' \sim A$ , also gilt  $\deg(A') = \deg(A) = 0$  nach Voraussetzung. Daraus folgt  $A' = 0$ , also  $\dim(A) = \dim(A') = \dim(0) = 1$ . Aus  $A \sim 0$  folgt auch die Implikation (2) $\Rightarrow$ (1). (3) $\Rightarrow$ (2) ist trivial. □

## 2.5 Das Geschlecht

In diesem Abschnitt wollen wir einen zentralen Begriff im Zusammenhang mit algebraischen Funktionenkörpern einführen: das Geschlecht. Die Bestimmung des Geschlechts eines gegebenen Funktionenkörpers wird sich als das wichtigste Problem der folgenden Kapitel herausstellen. Wir beginnen mit einer wichtigen Proposition:

**Proposition 2.5.1** *Sei  $F/K$  ein Funktionenkörper. Dann existiert eine Konstante  $\gamma \in \mathbb{Z}$ , sodass für alle Divisoren  $A \in \mathcal{D}_F$  gilt*

$$\deg(A) - \dim(A) \leq \gamma.$$

*Beweis:* Zunächst folgt aus Lemma 2.4.8 die Beziehung

$$A_1 \leq A_2 \Rightarrow \deg(A_1) - \dim(A_1) \leq \deg(A_2) - \dim(A_2). \quad (2.17)$$

Wir wählen ein nichtkonstantes  $x \in F$  und betrachten den Divisor  $B := (x)_\infty$ . Wie im Beweis von Satz 2.4.11 und unter Verwendung der Aussage selbigen Satzes zeigt man die Existenz eines positiven Divisors  $C$  mit

$\dim(lB + C) \geq (l + 1) \cdot \deg(B)$  für alle  $l \geq 0$ . Andererseits gilt wegen Lemma 2.4.8  $\dim(lB + C) \leq \dim(lB) + \deg(C)$ . Man erhält also

$$\dim(lB) \geq (l + 1)\deg(B) - \deg(C) = \deg(lB) + ([F : K(x)] - \deg(C)).$$

Also

$$\deg(lB) - \dim(lB) \leq \gamma \text{ für alle } l > 0. \quad (2.18)$$

für ein  $\gamma \in \mathbb{Z}$ . Wir zeigen nun, dass (2.18) nicht nur für  $lB$ , sondern für jeden beliebigen Divisor  $A \in \mathcal{D}_F$  gilt.

**Behauptung:** Sei  $A \in \mathcal{D}_F$ . Dann existieren Divisoren  $A_1, D$  und eine positive ganze

Zahl  $l$  sodass  $A \leq A_1$ ,  $A_1 \sim D$  und  $D \leq lB$ .

*Beweis:* Wähle  $A_1 \geq A$ , sodass  $A_1 \geq 0$ . Dann gilt nach Lemma 2.4.8 und (2.18)

$$\begin{aligned} \dim(lB - A_1) &\geq \dim(lB) - \deg(A_1) \\ &\geq \deg(lB) - \gamma - \deg(A_1) \\ &> 0 \end{aligned}$$

für  $l$  gross genug. Es existiert also ein Element  $0 \neq z \in \mathcal{L}(lB - A_1)$ . Setze  $D := A_1 - (z)$ . Dann gilt  $A_1 \sim D$  und  $D \leq A_1 - (A_1 - lB) = lB$ . Das beweist die Behauptung.

Nun gilt wegen (2.17) und (2.18)

$$\begin{aligned} \deg(A) - \dim(A) &\leq \deg(A_1) - \dim(A_1) \\ &= \deg(D) - \dim(D) \\ &\leq \deg(lB) - \dim(lB) \\ &\leq \gamma. \end{aligned}$$

□

Nun sind wir in der Lage das Geschlecht sinnvoll zu definieren:

**Definition 2.5.2** Sei  $F/K$  ein Funktionenkörper. Wir definieren das **Geschlecht**  $g$  von  $F/K$  durch

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

Aufgrund der obigen Proposition ist das Geschlecht wohldefiniert und endlich.  $g$  ist auch positiv, denn wählt man  $A = 0$ , so bekommt man

$$\deg(A) - \dim(A) + 1 = \deg(0) - \dim(0) + 1 = 0.$$

**Satz 2.5.3 (Satz von Riemann)** Sei  $F/K$  ein Funktionenkörper vom Geschlecht  $g$ . Dann gilt:

(a) Für jeden Divisor  $A \in \mathcal{D}_F$  gilt

$$\dim(A) \geq \deg(A) + 1 - g.$$

(b) Es existiert eine ganze Zahl  $c$ , abhängig von  $F/K$ , sodass

$$\dim(A) = \deg(A) + 1 - g$$

für alle  $A \in \mathcal{D}_F$  mit  $\deg(A) \geq c$ .

*Beweis:* (a) folgt aus der Definition des Geschlechts.

(b) Wähle einen Divisor  $A_0$  mit  $g = \deg(A_0) - \dim(A_0) + 1$  und setze  $c := \deg(A_0) + g$ . Sei  $\deg(A) \geq c$ . Dann gilt

$$\dim(A - A_0) \geq \deg(A - A_0) + 1 - g \geq c - \deg(A_0) + 1 - g \geq 1.$$

Es existiert also ein Element  $0 \neq z \in \mathcal{L}(A - A_0)$ . Betrachte den Divisor  $A' := A + (z)$ . Es gilt  $A' \geq A_0$ , und

$$\begin{aligned} \deg(A) - \dim(A) &= \deg(A') - \dim(A') \\ &\geq \deg(A_0) - \dim(A_0) \\ &= g - 1. \end{aligned}$$

Zusammen mit (a) folgt daraus  $\dim(A) = \deg(A) + 1 - g$ .

□

**Lemma 2.5.4** *Der rationale Funktionenkörper  $K(x)/K$  hat Geschlecht 0.*

*Beweis:* Es gilt klarerweise  $\{1, x, \dots, x^r\} \subseteq \mathcal{L}(rP_\infty)$ . Wir haben also

$$r + 1 \leq \dim(rP_\infty) = \deg(rP_\infty) + 1 - g = r + 1 - g$$

für  $r$  gross genug (nach Satz 2.5.3).

□

## 2.6 Motivation: Riemannsche Flächen

In der Einleitung des ersten Abschnitts war die Rede davon, dass wir den Satz von Riemann-Roch beweisen möchten. Bekannterweise ist dieser Satz ursprünglich ein Resultat über kompakte Riemannsche Flächen. Dabei werden gewisse Divisoren betrachtet, die zu einem Differential gehören und daraus wird eine Formel für  $\mathcal{L}(A)$  für einen Divisor  $A$  gewonnen. Wir wollen ein analoges Resultat für algebraische Funktionenkörper formulieren. Dazu wäre es hilfreich wenn man ein Analogon zu einem Differential auf einer kompakten Riemannschen Fläche für algebraische Funktionenkörper hätte. Ein solches Analogon existiert und wird im Abschnitt 1.7 definiert und mit dessen Hilfe lässt sich dann tatsächlich ein Satz von Riemann-Roch für Funktionenkörper beweisen. Ziel dieses Abschnitt ist es diese Definition zu motivieren. Für das Verständnis der restlichen Arbeit ist dieser Abschnitt nicht notwendig, vielmehr soll vermittelt werden, dass die Definitionen nicht vom Himmel fallen, sondern sehr geschickt adaptiert sind. Einige der Begriffe, die im folgenden Erwähnung finden, können im Rahmen dieser Arbeit nicht genauer erläutert werden. Eine gute Einführung in die Theorie der

Riemannschen Flächen bietet der Klassiker [41]. Moderne Darlegungen der Theorie liefern etwa die Bücher [26] und [12]. Diese Motivation stammt im Wesentlichen aus [34].

Sei also  $X$  eine kompakte Riemannsche Fläche vom Geschlecht  $g$ ,  $M$  der Körper der meromorphen Funktionen auf  $X$ , und  $\Omega$  der Raum der meromorphen Differentiale auf  $X$ . Wir fixieren uns einen Punkt  $x \in X$  und ein Differential  $0 \neq \omega \in \Omega$ . Sei  $t$  eine lokale Koordinatenabbildung um  $x$ . Dann kann man  $\omega$  lokal um  $x$  schreiben als

$$\omega = \sum_{i=-N}^{\infty} a_i t^i dt. \quad (2.19)$$

Sei  $M_x$  der Körper der meromorphen Funktionenkeime um  $x$  und  $f \in M_x$ . Wir können  $f\omega$  um einen hinreichend kleinen Kreis um  $x$  integrieren und erhalten  $2\pi i \operatorname{Res}_x(f\omega)$ . Schreibt man  $f$  als  $f = \sum_{j=-M}^{\infty} b_j t^j$ , so erhält man

$$\operatorname{Res}_x(f\omega) = \sum_{i+j=-1} a_i b_j \quad (2.20)$$

Definieren wir die  $\mathbb{C}$ -lineare Abbildung

$$\omega_x : \begin{cases} M_x & \rightarrow \mathbb{C} \\ f & \mapsto \operatorname{Res}_x(f\omega) \end{cases}$$

und betrachten die Menge  $\{\omega_x : x \in X\}$  linearer Funktionale. Was muss für eine mit  $X$  durchindizierte Menge von linearen Funktionalen gelten, wenn sie von einem Differential kommen? Um das beantworten zu können, rufen wir uns zunächst den Begriff der **Ordnung** von  $\omega$  an der Stelle  $x$  ins Gedächtnis: Sie ist definiert als das Minimum aller ganzen Zahlen  $i$  mit  $a_i \neq 0$ . Diese Definition ist, wie man leicht zeigen kann, unabhängig von der Wahl der Koordinaten und definiert eine endliche ganze Zahl  $\operatorname{ord}_x(\omega)$ . Es gilt  $\operatorname{ord}_x(\omega) = 0$  für fast alle  $x \in X$ . Man kann also jedem Differential  $\omega$  in eindeutiger Weise einen Divisor (also ein Element der freien abelschen Gruppe, die von  $X$  erzeugt wird)  $(\omega)$  zuordnen:

$$(\omega) = \sum_{x \in X} \operatorname{ord}_x(\omega) x.$$

Wir wollen nun einen Zusammenhang zwischen Funktionenkörpern und kompakten Riemannschen Flächen herstellen:  $M$  ist eine endliche Körpererweiterung von  $\mathbb{C}(x)$ , also ein Funktionenkörper. Die Punkte von  $X$  entsprechen den Stellen von  $M$  als Funktionenkörper. Sei  $O_x \subseteq M_x$  der Ring der holomorphen Funktionenkeime um  $x$ . Dann ist  $O_x$  ein diskreter Bewertungsring.  $M \cap O_x$  ist übrigens ein Bewertungsring des Funktionenkörpers  $M$ . Jedes Element aus  $O_x$  kann in eine Potenzreihe in einer Koordinatenabbildung entwickelt werden, wobei alle negativen Koeffizienten verschwinden. Das maximale Ideal  $P_x$  von  $O_x$  ist das Ideal, welches von  $t_x$ , der (oder einer) Koordinatenabbildung um  $x$ , erzeugt wird. Jedes Ideal von  $O_x$  wird von  $t_x^m$  erzeugt für ein  $m \in \mathbb{N}$  (siehe Abschnitt 1.1).

**Lemma 2.6.1** Sei  $0 \neq \omega \in \Omega$  ein meromorphes Differential,  $x \in X$  und  $\omega_x$  das lineare Funktional auf  $M_x$  wie wir es oben definiert haben. Dann existiert eine ganze Zahl  $N$  sodass  $\omega_x$  auf  $P_x^N$  verschwindet, aber nicht auf  $P_x^{N-1}$ . Es gilt

$$\text{ord}_x(\omega) = -N.$$

*Beweis:* Wählt man eine Darstellung wie in (2.19) für  $\omega$  und wählt man  $t_x = t$ , so erhält man trivialerweise die Aussage. □

**Korollar 2.6.2**  $\omega_x$  verschwindet auf  $O_x$  aber nicht auf  $P_x^{-1}$  für fast alle  $x \in X$ .

*Beweis:* Folgt aus obigem Lemma und der Tatsache, dass  $\text{ord}_x(\omega) = 0$  für fast alle  $x \in X$ . □

Damit haben wir eine lokale Bedingung für  $\omega_x$ . Eine globale können wir uns auch herleiten. Es gilt, dass auf einer kompakten Riemannschen Fläche die Summe der Residuen eines meromorphen Differentials gleich Null ist.

Die globale Bedingung lautet

**Lemma 2.6.3** Für jedes  $f \in M$  gilt

$$\sum_{x \in X} \omega_x(f) = 0.$$

*Beweis:* Aus  $f \in M$  folgt klarerweise  $f \in M_x$ . Die Summe macht also Sinn. Da  $X$  kompakt ist, hat  $f$  höchstens endlich viele Polstellen, also  $f \in O_x$  für fast alle  $x \in X$ . Da wegen des obigen Korollars  $\omega_x(f) = 0$  für fast alle  $x \in X$  gilt, ist die Summe sogar endlich.  $f\omega$  ist auch ein meromorphes Differential. Es gilt

$$\sum_{x \in X} \omega_x(f) = \sum_{x \in X} \text{Res}_x(f\omega) = 0$$

nach den vorangegangenen Bemerkungen. □

Nun sind wir in der Lage die sogenannten **Weil Differentiale** zu definieren: Sei zunächst der **Adeleraum**  $A(X) \subseteq \prod_{x \in X} M_x$  die Teilmenge von  $\prod_{x \in X} M_x$  mit fast allen  $x$ -Komponenten in  $O_x$ .<sup>2</sup>  $A(X)$  ist ein  $\mathbb{C}$ -Vektorraum. Schreibt man nämlich ein

<sup>2</sup>Im folgenden Abschnitt werden wir den Adeleraum etwas anders definieren:  $M_x$  ist die Vervollständigung von  $M$  bezüglich der Bewertung die dem Bewertungsring  $M \cap O_x$  zugeordnet ist. Wir werden uns später diese Vervollständigung ersparen und einfach ein Adele als ein Element von  $\prod_{x \in X} M$  auffassen mit fast allen  $x$ -Komponenten in  $M \cap O_x$ .

Element  $\Phi \in A(X)$  in offensichtlicher Weise als  $\Phi = (f_x)$ , so definiert man die Multiplikation mit einem Skalar  $a \in \mathbb{C}$  durch  $a\Phi := a(f_x) := (af_x)$ . Wir ordnen nun jedem  $\omega \in \Omega$  ein lineares Funktional  $\tilde{\omega}$  auf  $A(X)$  zu, und zwar in folgender Art:

$$\tilde{\omega} : \begin{cases} A(X) & \rightarrow \mathbb{C} \\ \Phi = (f_x) & \mapsto \sum_{x \in X} \omega_x(f_x). \end{cases}$$

Aus Lemma 2.6.3 folgt, dass  $\tilde{\omega}$  auf  $M$  verschwindet, wenn man  $M$  diagonal in  $A(X)$  einbettet, also  $f \in M$  auf  $(f_x)$  abbildet mit  $f_x = f$  für alle  $x$ .

Sei  $D = \sum_{x \in X} n_x x$  ein Divisor auf  $X$ . Definiere

$$A(D) := \{(f_x) \in A(X) : \text{ord}_x(f_x) \geq -n_x \text{ für alle } x \in X\} \cup \{0\}.$$

Nun sieht man sofort, dass folgendes gilt:

**Lemma 2.6.4** *Das Funktional  $\tilde{\omega}$  verschwindet auf  $M$  und auf  $A((\omega))$ . Weiters gilt: wenn  $\tilde{\omega}$  auf  $A(D)$  verschwindet, dann gilt  $A(D) \subseteq A((\omega))$ .*

Wichtig ist nun, dass auch die Umkehrung gilt: Sei  $\lambda$  ein Funktional auf  $A(X)$ , welches auf  $M$  und auf  $A(D)$  verschwindet für einen Divisor  $D$ , so gibt es ein Differential  $\omega \in \Omega$  mit  $\tilde{\omega} = \lambda$ . Damit haben wir eine rein algebraische Charakterisierung eines Differentials, und zwar als lineare Funktionale auf gewissen Räumen. Diese Charakterisierung stammt von Weil und kann im Prinzip eins zu eins auf algebraische Funktionenkörper übertragen werden. Damit sind wir mit unserer Motivation am Ende und wenden uns wieder den algebraischen Funktionenkörpern zu.

## 2.7 Der Satz von Riemann-Roch

*Im Folgenden sei  $F/K$  ein Funktionenkörper vom Geschlecht  $g$ .*

Wir wollen in diesem Abschnitt Differentiale auf Funktionenkörpern einführen und den Satz von Riemann-Roch beweisen. Die Definitionen sind durch das vorige Kapitel motiviert, die Analogien sind offensichtlich.

**Definition 2.7.1** *Ein Adele<sup>3</sup> auf einem Funktionenkörper ist eine Abbildung*

$$\alpha : \begin{cases} \mathbb{P}_F & \rightarrow F \\ P & \mapsto \alpha_P, \end{cases}$$

*mit der Eigenschaft, dass  $\alpha_P \in \mathcal{O}_P$  für fast alle  $P \in \mathbb{P}_F$ . Wir können also ein Adele als ein Element des direkten Produktes  $\prod_{P \in \mathbb{P}} F$  auffassen. Wir benützen daher die Schreibweise  $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ , oder kürzer  $\alpha = (\alpha_P)$ . Die Menge*

$$\mathcal{A}_F := \{\alpha : \alpha \text{ ist ein Adele von } F/K\}$$

*heißt Adeleraum.*

---

<sup>3</sup>Manchmal definiert man ein Adele als Abbildung mit Werten in  $\hat{F}_P$ , der Vervollständigung von  $F$  bezüglich der Bewertung, die der Stelle  $P$  zugeordnet ist. Wir benötigen das im folgenden nicht, daher nehmen wir mit unserer etwas einfacheren Definition vorlieb.

$\mathcal{A}_F$  ist ein  $K$ -Vektorraum, die Skalarmultiplikation ist in offensichtlicher Weise definiert. Wir können  $F$  in  $\mathcal{A}_F$  einbetten, indem wir einem  $x \in F$  das Adele, welches in jeder Komponente gleich  $x$  ist, zuordnen, das sogenannte **Hauptadele** von  $x$ . Wegen Korollar 2.3.4 macht diese Definition Sinn. Die Bewertungen  $v_P$  dehnen sich auf den Adeleraum aus, indem man  $v_P(\alpha) := v_P(\alpha_P)$  setzt. Definitionsgemäß gilt für ein Adele  $\alpha$  von  $F/K$ , dass  $v_P(\alpha) \geq 0$  für fast alle  $P \in \mathbb{P}_F$ .

**Definition 2.7.2** Für  $A \in \mathcal{D}_F$  definieren wir

$$\mathcal{A}_F(A) := \{\alpha \in \mathcal{A}_F : v_P(\alpha) \geq -v_P(A) \text{ für alle } P \in \mathbb{P}_F\}.$$

**Definition 2.7.3** Für  $A \in \mathcal{D}_F$  heißt

$$i(A) := \dim(A) - \deg(A) + g - 1$$

**Spezialitätenindex** von  $A$ .

**Satz 2.7.4** Sei  $A \in \mathcal{D}_F$ . Dann gilt

$$i(A) = \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)).$$

*Beweis:* Um den Beweis übersichtlicher zu gestalten, unterteilen wir ihn in mehrere Schritte.

**Schritt 1:** Sei  $A_1, A_2 \in \mathcal{A}_F$  mit  $A_1 \leq A_2$ . Dann gilt  $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$  und

$$\dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) = \deg(A_2) - \deg(A_1). \quad (2.21)$$

*Beweis:* Die Inklusion  $\mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$  ist trivial. Zu zeigen bleibt (2.21). Wir nehmen an, dass  $A_2 = A_1 + P$  für ein  $P \in \mathbb{P}_F$  gilt. Der allgemeine Fall folgt dann leicht durch Induktion. Wählen wir ein Element  $t \in F$  mit  $v_P(t) = v_P(A_1) + 1 = v_P(A_2)$  und betrachten die  $K$ -lineare Abbildung

$$\varphi : \begin{cases} \mathcal{A}_F(A_2) & \rightarrow & F_P \\ \alpha & \mapsto & (t\alpha_P)(P). \end{cases}$$

$\varphi$  ist klarerweise surjektiv und  $\ker(\varphi) = \mathcal{A}_F(A_1)$ . Es gilt also

$$\deg(A_2) - \deg(A_1) = \deg(P) = [F_P : K] = \dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)).$$

**Schritt 2:** Seien  $A_1, A_2$  wie in Schritt 1. Dann gilt

$$\dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) = (\deg(A_2) - \dim(A_2)) - (\deg(A_1) - \dim(A_1)). \quad (2.22)$$

*Beweis:* Wir haben eine exakte Sequenz linearer Abbildungen

$$0 \rightarrow \mathcal{L}(A_2)/\mathcal{L}(A_1) \begin{array}{l} \xrightarrow{\sigma_1} \mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \\ \xrightarrow{\sigma_2} (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F) \end{array} \rightarrow 0, \quad (2.23)$$

mit  $\sigma_1(x + \mathcal{L}(A_1)) := (x)_{P \in \mathbb{P}_F} + \mathcal{A}_F(A_1)$  und  $\sigma_2((\alpha_P)_{P \in \mathbb{P}_F} + \mathcal{A}_F(A_1)) := (\alpha_P)_{P \in \mathbb{P}_F} + \mathcal{A}_F(A_1) + F$ . Klarerweise ist  $\sigma_1$  injektiv und  $\sigma_2$  surjektiv. Zu zeigen bleibt  $Im(\sigma_1) = ker(\sigma_2)$ . Wir zeigen zunächst  $Im(\sigma_1) \subseteq ker(\sigma_2)$ . Sei  $x + \mathcal{L}(A_1) \in \mathcal{L}(A_2)/\mathcal{L}(A_1)$ . Dann gilt

$$\sigma_2(\sigma_1(x + \mathcal{L}(A_1))) = \sigma_2((x)_{P \in \mathbb{P}_F} + \mathcal{A}_F(A_1)) = (x)_{P \in \mathbb{P}_F} + \mathcal{A}_F(A_1) + F = 0 + \mathcal{A}_F(A_1).$$

$ker(\sigma_2) \subseteq Im(\sigma_1)$ : Sei also  $\alpha \in \mathcal{A}_F(A_2)$  mit  $\sigma_2(\alpha + \mathcal{A}_F(A_1)) = 0$ . Dann ist  $\alpha \in \mathcal{A}_F(A_1) + F$ , also existiert ein  $x \in F$  mit  $\alpha - x \in \mathcal{A}_F(A_1) \subseteq \mathcal{A}_F(A_2)$ . Es gilt also  $x \in \mathcal{A}_F(A_2) \cap F = \mathcal{L}(A_2)$ . Es gilt  $\alpha + \mathcal{A}_F(A_1) = x + \mathcal{A}_F(A_1) = \sigma_1(x + \mathcal{L}(A_1))$ . Das beweist die Exaktheit.

Aus der Exaktheit von (2.23) folgt nun wiederum, dass

$$\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1) \cong \mathcal{L}(A_2)/\mathcal{L}(A_1) \oplus (\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F).$$

Wir erhalten

$$\begin{aligned} \dim((\mathcal{A}_F(A_2) + F)/(\mathcal{A}_F(A_1) + F)) &= \dim(\mathcal{A}_F(A_2)/\mathcal{A}_F(A_1)) - \dim(\mathcal{L}(A_2)/\mathcal{L}(A_1)) \\ &= (\deg(A_2) - \deg(A_1)) - (\dim(A_2) - \dim(A_1)) \end{aligned}$$

nach (2.21).

**Schritt 3:** Sei  $B \in \mathcal{D}_F$  mit  $\dim(B) = \deg(B) + 1 - g$ . Dann gilt

$$\mathcal{A}_F = \mathcal{A}_F(B) + F. \quad (2.24)$$

*Beweis:* Wegen Lemma 2.4.8 haben wir für einen Divisor  $B_1 \geq B$ :

$$\dim(B_1) \leq \deg(B_1) + \dim(B) - \deg(B) = \deg(B_1) + 1 - g.$$

Wegen des Satzes von Riemann gilt aber auch die umgekehrte Ungleichung und wir erhalten

$$\dim(B_1) = \deg(B_1) + 1 - g \text{ für alle } B_1 \geq B. \quad (2.25)$$

Wir beweisen nun (2.24): Sei  $\alpha \in \mathcal{A}_F$ . Wir wählen einen Divisor  $B_1 \geq B$  mit  $\alpha \in \mathcal{A}_F(B_1)$ . Nach (2.22) und (2.25) gilt

$$\dim((\mathcal{A}_F(B_1) + F)/(\mathcal{A}_F(B) + F)) = 0.$$

Daher gilt  $\mathcal{A}_F(B_1) + F = \mathcal{A}_F(B) + F$  und da  $\alpha \in \mathcal{A}_F(B_1)$ , folgt  $\alpha \in \mathcal{A}_F(B) + F$ .

**Schritt 4:** Wählen wir nun einen beliebigen Divisor  $A \in \mathcal{D}_F$ . Nach dem Satz von Riemann (Satz 2.5.3) gibt es einen Divisor  $A_1 \geq A$  mit  $\dim(A_1) = \deg(A_1) + 1 - g$ . Wegen (2.24) gilt  $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$  und daher (wegen (2.22))

$$\begin{aligned} \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) &= \dim((\mathcal{A}_F(A_1) + F)/(\mathcal{A}_F(A) + F)) \\ &= (\deg(A_1) - \dim(A_1)) - (\deg(A) - \dim(A)) = (g - 1) + \dim(A) - \deg(A) = i(A). \end{aligned}$$

□

Die Aussage des vorigen Satzes nennt man auch „schwacher Satz von Riemann-Roch“.

Nun wollen wir den Begriff des Weil Differentials einführen.

**Definition 2.7.5** Ein Weil Differential auf  $F/K$  ist ein lineares Funktional  $\omega$  auf  $\mathcal{A}_F$  (als  $K$ -Vektorraum), welches auf  $\mathcal{A}_F(A) + F$  verschwindet für ein  $A \in \mathcal{D}_F$ . Wir nennen

$$\Omega_F := \{\omega : \omega \text{ ist Weil Differential auf } F/K\}$$

den Modul der Weil Differentiale auf  $F/K$ . Für  $A \in \mathcal{D}_F$  definieren wir

$$\Omega_F(A) := \{\omega \in \Omega_F : \omega \text{ verschwindet auf } \mathcal{A}_F(A) + F\}.$$

Der Beweis des folgenden Lemmas ist trivial.

**Lemma 2.7.6**  $\Omega_F$  ist ein  $K$ -Vektorraum. Sei  $a \in K$  und  $\omega_1, \omega_2 \in \Omega_F$ , sodass  $\omega_i$  auf  $\mathcal{A}_F(A_i) + F$  verschwindet ( $i = 1, 2$ ), dann verschwindet  $a\omega_1 + \omega_2$  auf  $\mathcal{A}_F(A_3) + F$  für jeden Divisor  $A_3$  mit  $A_3 \leq \min\{A_1, A_2\}$ .

**Lemma 2.7.7** Für  $A \in \mathcal{D}_F$  gilt  $\dim(\Omega_F(A)) = i(A)$ .

*Beweis:* Betrachten wir die Abbildung

$$\Phi : \begin{cases} \Omega_F(A) & \rightarrow & (\mathcal{A}_F/(\mathcal{A}_F(A) + F))^* \\ \omega & \mapsto & \bar{\omega}. \end{cases}$$

mit  $\bar{\omega}((\alpha_P) + (\mathcal{A}_F(A) + F)) := \omega((\alpha))$ . Man sieht leicht, dass  $\Phi$  ein  $K$ -Vektorraumisomorphismus ist.  $(\mathcal{A}_F/(\mathcal{A}_F(A) + F))^*$  hat als endlichdimensionaler Vektorraum dieselbe Dimension wie der Raum  $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ , also folgt die Aussage aus dem schwachen Satz von Riemann-Roch.

□

Daraus folgt übrigens, dass  $\Omega_F \neq \{0\}$ . Nehmen wir einen Divisor  $A$  mit  $\deg(A) \leq -2$ , dann gilt

$$\dim(\Omega_F(A)) = i(A) = \dim(A) - \deg(A) + g - 1 \geq 1,$$

also ist  $\Omega_F(A) \neq \{0\}$  und damit auch  $\Omega_F \neq \{0\}$ .

Wir wollen  $\Omega_F$  auch als Vektorraum über  $F$  auffassen.

**Definition 2.7.8** Sei  $x \in F$  und  $\omega \in \Omega_F$ . Dann definieren wir die Abbildung

$$x\omega : \begin{cases} \mathcal{A}_F & \rightarrow & K \\ \alpha & \mapsto & \omega(x\alpha). \end{cases}$$

**Bemerkung 2.7.9**

(a) Klarerweise ist  $x\omega$  ein Weil Differential: verschwindet  $\omega$  auf  $\mathcal{A}_F(A) + F$ , so verschwindet  $x\omega$  auf  $\mathcal{A}_F(A + (x)) + F$ . Mit unserer Definition haben wir also auf  $\Omega_F$  die Struktur eines  $F$ -Vektorraums.

(b) Die Abbildung  $x \rightarrow x\omega$  ist injektiv für  $x \in F$  und  $\omega \in \Omega_F$ . Angenommen es gelte  $x\omega = 0$  für alle  $x \in F$ . Dann wäre  $\omega(x\alpha) = 0$  für alle  $\alpha = (\alpha_P) \in \mathcal{A}_F$ . Setzen wir  $\tilde{\alpha} := (x^{-1}\alpha_P)$ . Dann gilt  $\omega(\alpha) = \omega(x\tilde{\alpha}) = 0$ . Daraus folgt  $\omega = 0$ .

**Proposition 2.7.10**  $\Omega_F$  ist ein eindimensionaler  $F$ -Vektorraum.

*Beweis:* Wir wissen, dass  $\Omega_F \neq \{0\}$ , also wählen wir ein  $\omega_1 \in \Omega_F \setminus \{0\}$ . Sei  $0 \neq \omega_2 \in \Omega_F$ . Zu zeigen ist, dass ein  $z \in F$  existiert mit  $\omega_2 = z\omega_1$ . Wählen wir  $A_i \in \mathcal{D}_F$  mit  $\omega_i \in \Omega_F(A_i)$  ( $i = 1, 2$ ). Für einen Divisor  $B \in \mathcal{D}_F$  betrachten wir die beiden  $K$ -linearen, injektiven Abbildungen

$$\varphi_i : \begin{cases} \mathcal{L}(A_i + B) & \rightarrow \Omega_F(-B) \\ x & \mapsto x\omega_i. \end{cases} \quad (i = 1, 2).$$

Aufgrund von Bemerkung 2.7.9 (b) ist diese Abbildung injektiv. Sie ist auch wohldefiniert: Nach Bemerkung 2.7.9 (a) verschwindet  $x\omega_i$  auf  $\mathcal{A}_F(A_i + (x))$ , und da  $x \in \mathcal{L}(A_i + B)$  gilt, verschwindet  $x\omega_i$  auf  $\mathcal{A}_F(-B)$ .

**Behauptung:** Es existiert ein  $B \in \mathcal{D}_F$  mit

$$\bigcap_{i=1,2} \varphi_i(\mathcal{L}(A_i + B)) \neq \{0\}.$$

*Beweis:* Wähle  $B > 0$  mit

$$\dim(A_i + B) = \deg(A_i + B) + 1 - g \quad (i = 1, 2).$$

Nach dem Satz von Riemann ist das möglich. Noch eine kleine Trivialität: Seien  $U_1, U_2$  Unterräume eines Vektorraums  $V$ , so gilt

$$\dim(U_1 \cap U_2) \geq \dim(U_1) + \dim(U_2) - \dim(V). \quad (2.26)$$

Setzen wir  $U_i := \varphi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$ ,  $i = 1, 2$ . Es gilt

$$\begin{aligned} \dim(\Omega_F(-B)) &= i(-B) = \dim(-B) - \deg(-B) + g - 1 \\ &= \deg(B) - 1 + g. \end{aligned}$$

Daher bekommen wir

$$\dim(U_1) + \dim(U_2) - \dim(\Omega_F(-B))$$

$$\begin{aligned}
&= \deg(A_1 + B) + 1 - g + \deg(A_2 + B) + 1 - g - (\deg(B) + g - 1) \\
&= \deg(B) + (\deg(A_1) + \deg(A_2) + 3(1 - g)).
\end{aligned}$$

Der Ausdruck in Klammern ist unabhängig von  $B$ , also gilt für  $\deg(B)$  groß genug

$$\dim(U_1) + \dim(U_2) - \dim(\Omega_F(-B)) > 0,$$

und wegen (2.26) beweist das die Behauptung.

Nach der Behauptung existieren also  $x_i \in \mathcal{L}(A_i + B)$ ,  $i = 1, 2$ , mit  $x_1\omega_1 = x_2\omega_2 \neq 0$ , woraus dann folgt  $\omega_2 = (x_1x_2^{-1})\omega_1$ .

□

Wir wollen nun jedem Weil Differential  $\omega \neq 0$  einen Divisor zuordnen. Dazu definieren wir die Menge

$$M(\omega) := \{A \in \mathcal{D}_F : \omega \text{ verschwindet auf } \mathcal{A}_F(A) + F\}.$$

**Lemma 2.7.11** *Sei  $0 \neq \omega \in \Omega_F$ . Dann existiert ein eindeutig bestimmter Divisor  $W \in M(\omega)$  mit  $A \leq W$  für alle  $A \in M(\omega)$ , d.h.  $W = \max M(\omega)$ .*

*Beweis:* Nach dem Satz von Riemann existiert eine Konstante  $c$  mit  $i(A) = 0$  für alle  $A \in \mathcal{D}_F$  mit  $\deg(A) \geq c$ . Da  $\dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$  nach Satz 2.7.4, gilt  $\deg(A) < c$  für alle  $A \in M(\omega)$ . Wir können also einen Divisor  $W \in M(\omega)$  mit maximalem Grad wählen. Angenommen  $W$  erfüllt nicht die Eigenschaften, die wir verlangen. Dann existiert ein  $A_0 \in M(\omega)$  mit  $A_0 \not\leq W$ , also existiert ein  $Q \in \mathbb{P}_F$  mit  $v_Q(A_0) > v_Q(W)$ . Wir behaupten

$$W + Q \in M(\omega),$$

ein Widerspruch zur Maximalität des Grades von  $W$ . Betrachten wir ein Adele  $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$ . Dann kann man  $\alpha$  auch schreiben als  $\alpha = \alpha' + \alpha''$  mit

$$\alpha'_P := \begin{cases} \alpha_P & \text{für } P \neq Q \\ 0 & \text{für } P = Q \end{cases} \quad \text{und}$$

$$\alpha''_P := \begin{cases} 0 & \text{für } P \neq Q \\ \alpha_Q & \text{für } P = Q \end{cases}$$

Es gilt  $\alpha' \in \mathcal{A}_F(W)$  und  $\alpha'' \in \mathcal{A}_F(A_0)$ , also gilt  $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$  und damit verschwindet  $\omega$  auf  $\mathcal{A}_F(W + Q) + F$ . Widerspruch! Die Eindeutigkeit ist damit auch bewiesen.

□

Nach dem vorangegangenen Lemma ist die folgende Definition sinnvoll.

**Definition 2.7.12** Sei  $F/K$  ein Funktionenkörper und  $\omega \in \Omega_F \setminus \{0\}$ .

- (a) Der **Divisor der Weil Differentials**  $\omega$  ist der eindeutig bestimmte Divisor  $(\omega)$  von  $F/K$  mit
- (1)  $\omega$  verschwindet auf  $\mathcal{A}_F((\omega))$ .
  - (2) Verschwindet  $\omega$  auf  $\mathcal{A}_F(A) + F$ , so gilt  $A \leq (\omega)$ .
- (b) Für  $P \in \mathbb{P}_F$  definieren wir  $v_P(\omega) := v_P((\omega))$ .
- (c) Eine Stelle  $P \in \mathbb{P}_F$  heißt **Nullstelle (Pol)** von  $\omega$ , falls  $v_P(\omega) > 0$  ( $v_P(\omega) < 0$ ).  $\omega$  heißt **regulär** (oder **holomorph**) an der Stelle  $P$ , falls  $v_P(\omega) \geq 0$ .
- (d) Ein Divisor  $W$  heißt **kanonischer Divisor** von  $F/K$ , falls  $W = (\omega)$  für ein  $\omega \in \Omega_F$ .

**Proposition 2.7.13** Sei  $F/K$  ein Funktionenkörper.

- (a) Für  $0 \neq x \in F$  und  $0 \neq \omega \in \Omega_F$  gilt  $(x\omega) = (x) + (\omega)$ .
- (b) Je zwei kanonische Divisoren sind äquivalent.

*Beweis:* Verschwindet  $\omega$  auf  $\mathcal{A}_F(A) + F$ , so verschwindet  $x\omega$  auf  $\mathcal{A}_F(A + (x)) + F$ , also gilt

$$(\omega) + (x) \leq (x\omega).$$

Gleichermaßen gilt  $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$ . Kombiniert man die beiden Ungleichungen, so erhält man

$$(\omega) + (x) \leq (x\omega) \leq -(x^{-1}) + (\omega) = (\omega) + (x).$$

Das beweist (a). (b) folgt aus (a) und der Tatsache, dass  $\Omega_F$  ein eindimensionaler  $F$ -Vektorraum ist.

□

Aus dem obigen Lemma folgt also, dass die kanonischen Divisoren eine Klasse in der Divisorklassengruppe  $\mathcal{C}_F$  bilden, die sogenannte **kanonische Klasse**.

**Satz 2.7.14** Sei  $A \in \mathcal{D}_F$  ein Divisor und  $W = (\omega)$  ein kanonischer Divisor von  $F/K$ . Dann ist die Abbildung

$$\mu : \begin{cases} \mathcal{L}(W - A) & \rightarrow \Omega_F(A) \\ x & \mapsto x\omega \end{cases}$$

ein  $K$ -Vektorraumisomorphismus. Insbesondere gilt

$$i(A) = \dim(W - A).$$

*Beweis:* Für  $x \in \mathcal{L}(W - A)$  gilt

$$(x\omega) = (x) + (\omega) \geq -(W - A) + W = A,$$

also ist die Abbildung wohldefiniert.  $\mu$  ist auch linear und injektiv, wie man sofort sieht. Um zu zeigen, dass  $\mu$  surjektiv ist, wählen wir ein  $\omega_1 \in \Omega_F(A) \setminus \{0\}$ . Nach Proposition 2.7.10 gilt  $\omega_1 = x\omega$  für ein  $x \in F$ . Da

$$(x) + W = (x) + (\omega) = (x\omega) = (\omega_1) \geq A,$$

folgt  $x \in \mathcal{L}(W - A)$  und  $\omega_1 = \mu(x)$ . □

Nun können wir, die bisherigen Ergebnisse zusammenfassend, den Satz von Riemann-Roch beweisen.

**Satz 2.7.15 (Riemann-Roch)** *Sei  $W$  ein kanonischer Divisor von  $F/K$ . Dann gilt für alle  $A \in \mathcal{D}_F$ ,*

$$\dim(A) = \deg(A) + 1 - g + \dim(W - A).$$

*Beweis:* Die Aussage folgt direkt aus Satz 2.7.14 und der Definition von  $i(A)$ . □

## 2.8 Einige Konsequenzen aus dem Satz von Riemann-Roch

**Lemma 2.8.1** *Sei  $W$  ein kanonischer Divisor. Dann gilt*

$$\deg(W) = 2g - 2 \text{ und } \dim(W) = g.$$

*Beweis:* Zum Beweis der Aussage über die Dimension setze man in den Satz von Riemann-Roch  $A = 0$  ein und für die Aussage über den Grad von  $W$  setze man  $A = W$  in den Satz von Riemann-Roch ein und benütze  $\dim(W) = g$ . □

**Satz 2.8.2** *Sei  $A \in \mathcal{D}_F$  mit  $\deg(A) \geq 2g - 1$ . Dann gilt*

$$\dim(A) = \deg(A) + 1 - g.$$

*Beweis:* Wir haben nach dem Satz von Riemann-Roch

$$\dim(A) = \deg(A) + 1 - g + \dim(W - A)$$

für einen kanonischen Divisor  $W$ . Wegen  $\deg(A) \geq 2g - 1$  und  $\deg(W) = 2g - 2$  gilt  $\deg(W - A) < 0$ . Daher folgt wegen Korollar 2.4.12  $\dim(W - A) = 0$ .

□

**Proposition 2.8.3** Sei  $P \in \mathbb{P}_F$ . Dann existiert für jedes  $n \geq 2g$  ein Element  $x \in F$  mit  $(x)_\infty = nP$ .

*Beweis:* Nach dem vorigen Satz gilt

$$\dim((n-1)P) = (n-1)\deg(P) + 1 - g$$

und

$$\dim(nP) = n \cdot \deg(P) + 1 - g.$$

Daraus folgt

$$A := \mathcal{L}(nP) \setminus \mathcal{L}((n-1)P) \neq \emptyset.$$

Jedes  $x \in A$  erfüllt die gewünschte Eigenschaft.

□

Der folgende Satz liefert eine Verschärfung des schwachen Approximationssatzes.

**Satz 2.8.4 (starker Approximationssatz)** Sei  $S \subset \mathbb{P}_F$ ,  $P_1, \dots, P_r \in S$ ,  $x_1, \dots, x_r \in F$ , und  $n_1, \dots, n_r \in \mathbb{Z}$ . Dann existiert ein  $x \in F$  mit

$$v_{P_i}(x - x_i) = n_i \text{ für } i = 1, \dots, r \text{ und}$$

$$v_P(x) \geq 0 \text{ für alle } P \in S \setminus \{P_1, \dots, P_r\}.$$

*Beweis:* Betrachten wir das Adele  $(\alpha_P)$  mit

$$\alpha_P := \begin{cases} x_i & \text{falls } P = P_i, i = 1, \dots, r \\ 0 & \text{sonst.} \end{cases}$$

Wählen wir eine Stelle  $Q \in \mathbb{P}_F \setminus S$ . Für  $m \in \mathbb{N}$  groß genug haben wir wegen Satz 2.7.4 und Satz 2.8.2

$$\mathcal{A}_F = \mathcal{A}_F \left( mQ - \sum_{i=1}^r (n_i + 1)P_i \right) + F.$$

Es existiert also ein  $z \in F$  mit  $z - \alpha \in \mathcal{A}_F(mQ - \sum_{i=1}^r (n_i + 1)P_i)$ . Das heißt

$$v_{P_i}(z - x_i) > n_i \text{ für } i = 1, \dots, r \text{ und} \quad (2.27)$$

$$v_P(z) \geq 0 \text{ für } P \in S \setminus \{P_1, \dots, P_r\}. \quad (2.28)$$

Nun wählen wir Elemente  $y_1, \dots, y_r \in F$  mit  $v_{P_i}(y_i) = n_i$ . Genau wie vorhin konstruieren wir ein Element  $y \in F$  mit

$$v_{P_i}(y - y_i) > n_i \text{ für } i = 1, \dots, r \text{ und} \quad (2.29)$$

$$v_P(y) \geq 0 \text{ für } P \in S \setminus \{P_1, \dots, P_r\}. \quad (2.30)$$

Dann haben wir für  $i = 1, \dots, r$  wegen (2.29) und der starken Dreiecksungleichung

$$v_{P_i}(y) = v_{P_i}((y - y_i) + y_i) = n_i. \quad (2.31)$$

Setzen wir nun  $x := y + z$ , so erhalten wir

$$v_{P_i}(x - x_i) = v_{P_i}(y + (z - x_i)) = n_i \text{ für } i = 1, \dots, r$$

wegen (2.31), und für  $P \in \mathbb{P}_F \setminus S$  gilt  $v_P(x) = v_P(y + z) \geq 0$  wegen (2.28) und (2.30).  $\square$

## 2.9 Lokale Komponenten von Weil Differentialen

Mit der Definition des Hauptadeles eines Elements  $x \in F$  haben wir schon eine Einbettung  $F \hookrightarrow \mathcal{A}_F$  kennengelernt. Analog zur Residuenabbildung existiert noch eine andere lokale Einbettung  $\iota_P : F \hookrightarrow \mathcal{A}_F$ :

**Definition 2.9.1** Sei  $P \in \mathbb{P}_F$ .

(a) Sei  $x \in F$ . Dann ist  $\iota_P(x) \in \mathcal{A}_F$  jenes Adele, welches an der Stelle  $P$  gleich  $x$  ist, und auf allen anderen Stellen verschwindet.

(b) Für ein Weil Differential  $\omega \in \Omega_F$  definieren wir seine **lokale Komponente**  $\omega_P : F \rightarrow K$  durch

$$\omega_P(x) := \omega(\iota_P(x)).$$

Klarerweise ist diese Abbildung  $K$ -linear.

**Proposition 2.9.2** Sei  $\omega \in \Omega_F$  und  $\alpha = (\alpha_P) \in \mathcal{A}_F$ . Dann gilt  $\omega_P(\alpha_P) = 0$  für fast alle Stellen  $P$ , und

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_F} \omega_P(\alpha_P).$$

Insbesondere gilt

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0.$$

*Beweis:* Wir können  $\omega \neq 0$  annehmen und setzen  $W := (\omega)$ . Es existiert eine endliche Menge  $S \subset \mathbb{P}_F$  mit  $v_P(W) = 0$  und  $v_P(\alpha_P) \geq 0$  für alle  $P \notin S$ . Definieren wir  $\beta = (\beta_P) \in \mathcal{A}_F$  durch

$$\beta_P = \begin{cases} \alpha_P & \text{für } P \notin S \\ 0 & \text{für } P \in S. \end{cases}$$

Dann gilt  $\beta \in \mathcal{A}_F(W)$  und  $\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P)$ , also gilt  $\omega(\beta) = 0$  und

$$\omega(\alpha) = \sum_{P \in S} \omega_P(\alpha_P).$$

Für  $P \notin S$  gilt  $\iota_P(\alpha_P) \in \mathcal{A}_F(W)$ , und daher  $\omega_P(\alpha_P) = 0$ .

□

Wir zeigen noch, dass ein Weil Differential durch eine einzelne lokale Komponente eindeutig bestimmt ist.

**Proposition 2.9.3**

(a) Sei  $0 \neq \omega \in \Omega_F$  und  $P \in \mathbb{P}_F$ . Dann gilt

$$v_P(\omega) = \max\{r \in \mathbb{Z} : \omega_P(x) = 0 \text{ für alle } x \in F \text{ mit } v_P(x) \geq -r\}.$$

Speziell gilt  $\omega_P \neq 0$ .

(b) Sei  $\omega, \omega' \in \Omega_F$  und  $\omega_P = \omega'_P$  für ein  $P \in \mathbb{P}_F$ . Dann gilt  $\omega = \omega'$ .

*Beweis:* (a) Sei wieder  $W := (\omega)$ . Dann gilt definitionsgemäß  $v_P(\omega) = v_P(W)$ . Sei  $s := v_P(\omega)$ . Für  $x \in F$  mit  $v_P(x) \geq -s$  gilt  $\iota_P(x) \in \mathcal{A}_F(W)$ , also  $\omega_P(x) = \omega(\iota_P(x)) = 0$ . Nehmen wir nun an, dass  $\omega_P(x) = 0$  für ein  $x \in F$  mit  $v_P(x) \geq -s - 1$ . Sei  $\alpha = (\alpha_Q)_{Q \in \mathbb{P}_F} \in \mathcal{A}_F(W + P)$ . Dann gilt

$$\alpha = (\alpha - \iota_P(\alpha_P)) + \iota_P(\alpha_P)$$

mit  $\alpha - \iota_P(\alpha_P) \in \mathcal{A}_F(W)$  und  $v_P(\alpha_P) \geq -s - 1$ , also

$$\omega(\alpha) = \omega(\alpha - \iota_P(\alpha_P)) + \omega_P(\alpha_P) = 0.$$

Also verschwindet  $\omega$  auf  $\mathcal{A}_F(W + P)$ , Widerspruch zur Definition von  $W$ .

(b) Gelte  $\omega_P = \omega'_P$ , dann gilt  $(\omega - \omega')_P = 0$ , also  $\omega - \omega' = 0$  wegen (a).

□



# Kapitel 3

## Goppa Codes

In diesem Kapitel wollen wir die geometrischen Goppa Codes motivieren, definieren und ihre zentralen Eigenschaften herleiten.

### 3.1 Kurven und Funktionenkörper

In diesem Abschnitt sollen Zusammenhänge zwischen Kurven und algebraischen Funktionenkörpern skizziert werden. Beweise und (weit) umfangreichere Abhandlungen finden sich in [21, 31].

Sei  $K$  ein Körper mit algebraischem Abschluss  $\overline{K}$ .

**Definition 3.1.1** *Eine affine Kurve  $C : f(x, y) = 0$  über  $K$  ist die Menge  $\{(x, y) \in \overline{K}^2 : f(x, y) = 0\}$ , wobei  $f(x, y) \in K[x, y]$  ein irreduzibles Polynom ist. Die Elemente aus  $K^2 \cap C$  heißen **rationale Punkte** von  $C$ .*

Indem wir Fernpunkte hinzunehmen erhalten wir den projektiven Abschluss einer affinen Kurve: Der zweidimensionale projektive Raum über  $K$  ist die Menge

$$P^2(K) := K^3 \setminus \{(0, 0, 0)\} / \sim,$$

wobei

$$(a_1, a_2, a_3) \sim (b_1, b_2, b_3) :\Leftrightarrow b_i = \lambda a_i \text{ für ein } \lambda \in K^* \text{ und } i = 1, 2, 3.$$

Sei  $f(x, y, z) \in K[x, y, z]$ . Um sinnvoll sagen zu können, dass  $f$  im Punkt  $(x, y, z) \in P^2(K)$  eine Nullstelle besitzt, muss man fordern, dass  $f$  homogen ist, d.h.  $f(\lambda x, \lambda y, \lambda z) = \lambda^n f(x, y, z)$  für alle  $\lambda \in K$ . Damit hängt die Aussage „ $(x, y, z)$  ist Nullstelle von  $f$ “ nur von der Äquivalenzklasse von  $(x, y, z)$  ab.

**Definition 3.1.2** *Eine projektive Kurve  $C : f(x, y, z) = 0$  über  $K$  ist die Menge  $\{(x, y, z) \in P^2(\overline{K}) : f(x, y, z) = 0\}$ , wobei  $f(x, y, z) \in K[x, y, z]$  ein irreduzibles homogenes Polynom ist. Die Elemente aus  $C \cap P(K)^2$  heißen **rationale Punkte** von  $C$ .*

Sei  $C : f(x, y, z) = 0$  eine projektive Kurve über  $K$ . Dann kann man dieser Kurve ihre drei **affinen Komponenten**  $C_1 : f(1, y, z) = 0$ ,  $C_2 : f(x, 1, z) = 0$ ,  $C_3 : f(x, y, 1) = 0$  zuordnen. Umgekehrt kann man einer affinen Kurve  $C : f(x, y) = 0$  ihren **projektiven Abschluss**  $\overline{C} : z^{\deg(f(x,y))} f\left(\frac{x}{z}, \frac{y}{z}\right) = 0$  zuordnen.

**Definition 3.1.3** Sei eine affine Kurve  $C : f(x, y) = 0$  gegeben. Dann definieren wir den **Funktionskörper**  $K(C)$  von  $C$  als den Quotientenkörper von  $K[x, y]/(f(x, y))$ . Ist  $K(C)$  isomorph zum Körper der rationalen Funktionen  $\frac{h(t)}{g(t)}$  in einer Variablen, so heißt die Kurve **rational**. Sei  $C : f(x, y, z) = 0$  eine projektive Kurve. Dann ist der Funktionskörper  $K(C)$  von  $C$  definiert als der Funktionskörper einer affinen Komponente von  $C^1$ . Eine projektive Kurve heißt **rational**, wenn ihre affinen Komponenten rational sind.

**Definition 3.1.4** Ein Punkt  $(u, v)$  einer affinen Kurve  $C : f(x, y) = 0$  heißt **singulär**, wenn  $f_x(u, v) = f_y(u, v) = 0$ . Andernfalls heißt  $(u, v)$  **regulär**. Sei  $C : f(x, y, z) = 0$  eine projektive Kurve und  $(u, v, w) \in C$ . Dann heißt  $(u, v, w)$  **singulär**, falls  $(1, v, w)$  ein singulärer Punkt von  $C_1$  ist,  $(u, 1, w)$  ein singulärer Punkt von  $C_2$  ist, und  $(u, v, 1)$  ein singulärer Punkt von  $C_3$  ist. Andernfalls heißt  $(u, v, w)$  **regulär**.

**Definition 3.1.5** Eine affine, bzw. projektive Kurve heißt **regulär** oder **nichtsingulär**, falls jeder Punkt der Kurve regulär ist.

Sei nun eine projektive Kurve  $C$  gegeben, zusammen mit einem Punkt  $P \sim (u, v, 1) \in C$ . Wir definieren  $K[x, y]_P$  als die Menge aller rationalen Funktionen  $g(x, y)/h(x, y)$  mit  $h(u, v) \neq 0$ . Sei  $Q \sim (u, 1, w) \in C$ , dann geht die Definition analog mit  $h(u, w) \neq 0$  und für  $R \sim (1, v, w) \in C$  mit  $h(v, w) \neq 0$ . Diese Definitionen sind, wie man zeigen kann, verträglich.

**Definition 3.1.6** Sei  $C$  eine projektive Kurve und  $P$  ein Punkt auf  $C$ . Dann definieren wir den **lokalen Koordinatenring**  $K(C)_P$  als die Elemente von  $K(C)$ , die durch rationale Funktionen aus  $K[x, y]_P$  dargestellt werden können.

**Satz 3.1.7** Sei  $C$  eine nichtsinguläre projektive Kurve. Dann ist  $K(C)$  ein Funktionskörper und  $K(C)_P$  ein Bewertungsring. Alle Bewertungsringe von  $K(C)$  sind von dieser Form.

Umgekehrt kann man zu jedem Funktionskörper  $F/K$  eine nichtsinguläre projektive Kurve  $C$  konstruieren mit  $K(C) = F/K$  (siehe etwa [21]). Wir haben also den versprochenen Zusammenhang zwischen Kurven und Funktionskörpern hergestellt. Die Stellen vom Grad 1 sind genau die rationalen Punkte der zugehörigen Kurve.

<sup>1</sup>Die Funktionskörper der verschiedenen affinen Komponenten von  $C$  sind, wie man zeigen kann, isomorph.

## 3.2 Geometrische Goppa Codes

Um die Idee hinter den Goppa Codes zu verstehen, interpretieren wir zunächst die Reed-Solomon Codes auf eine andere Art. Die Goppa Codes sind dann nur eine naheliegende Verallgemeinerung. Sei also  $\mathbb{F}_q = \{0, \alpha, \alpha^2, \dots, \alpha^n = 1\}$  ein Körper mit  $q$  Elementen und  $n = q - 1$ .

**Satz 3.2.1** Sei  $1 \leq k \leq n$  und

$$\mathcal{L}_k := \{f \in \mathbb{F}_q[x] : \deg(f(x)) < k\}.$$

Betrachten wir die lineare Auswertungsabbildung  $ev : \mathcal{L}_k \rightarrow \mathbb{F}_q^n$  gegeben durch

$$ev(f) := (f(\alpha), f(\alpha^2), \dots, f(\alpha^n)) \in \mathbb{F}_q^n.$$

Dann gilt mit  $d = n - k + 1$

$$RS(n, d) = ev(\mathcal{L}_k).$$

*Beweis:* Zunächst gilt klarerweise  $\dim(ev(\mathcal{L}_k)) = k$ , da die Auswertungsabbildung auf  $\mathcal{L}_k$  injektiv ist. Der Reed Solomon Code  $RS(n, d)$  ist der Polynomcode mit Generatorpolynom  $g(x) = (x - \alpha) \dots (x - \alpha^{n-k})$ . Betrachten wir den Vektor

$$c := (f(\alpha), \dots, f(\alpha^n))$$

mit einem Polynom  $f$  vom Grad kleiner  $k$ . Das Polynom, welches diesem Vektor zugeordnet wird ist

$$c_f(x) = f(\alpha) + f(\alpha^2)x + \dots + f(\alpha^n)x^{n-1}.$$

Wir wollen zeigen, dass  $c \in RS(n, d)$  liegt. Dazu genügt es zu zeigen, dass jedes Polynom  $(x - \alpha^i)$ ,  $i \leq n - k$ , das Polynom  $c_f(x)$  teilt, also  $c_f(\alpha^i) = 0$  gilt. Aufgrund der Linearität der Abbildung  $f \mapsto c_f(x)$ , genügt es  $f = x^l$ ,  $l < k$  zu betrachten. Es gilt

$$c_{x^l}(\alpha^i) = \alpha^l + \alpha^{2l}\alpha^i + \alpha^{3l}\alpha^{2i} + \dots + \alpha^{nl}\alpha^{(n-1)i} = \alpha^l \frac{1 - \alpha^{n(i+l)}}{1 - \alpha} = 0$$

wegen der geometrischen Summenformel.  $ev(\mathcal{L}_k)$  ist also ein Teilraum von  $RS(n, d)$  der gleichen Dimension, also sind die beiden gleich. □

Interpretieren wir nun die Punkte  $\alpha, \alpha^2, \dots, \alpha^n$  als Punkte der projektiven nichtsingulären Kurve  $C : y = 0$ . Zu den obigen Punkten kommt dann noch der Punkt  $(0, 0, 1)$  dazu, der als unendlich ferner Punkt  $\infty$  agiert. Die Funktionen aus  $\mathcal{L}_k$  sind genau diejenigen Funktionen aus  $K(C) = \mathbb{F}_q(x)$ , die an der Stelle  $\infty$  einen Pol vom Grad kleiner als  $k$  haben. Übersetzen wir das auf die Sprache der Funktionenkörper, dann bekommen wir den rationalen Funktionenkörper  $\mathbb{F}_q(x)/\mathbb{F}_q$  und  $\mathcal{L}_k$  entspricht dem

Riemann-Roch Raum  $\mathcal{L}(kP_\infty)$ . Die wesentliche Einschränkung der Reed-Solomon Codes ist, dass man über einem Körper mit  $q$  Elementen nur einen Code mit Länge  $q - 1$  definieren kann. Dieser besitzt zwar gute Eigenschaften, ist aber auch sehr kurz. Es lassen sich auch keine asymptotischen Aussagen machen, da man die Codelänge nicht losgelöst von der Anzahl der Elemente des Alphabets betrachten kann. Nun kann man sich aber folgendes überlegen: wir haben im Prinzip gewisse Funktionen auf Punkten der Kurve  $C : y = 0$  ausgewertet und einen Code der Länge  $\text{card}(C)$  erhalten. Leider gilt  $\text{card}(C) = q - 1$ , was diese Codes sehr kurz macht. Es existieren jedoch Kurven  $D : g(x, y, z) = 0$  mit viel mehreren (rationalen) Punkten, und was liegt daher näher, als die obige Konstruktion auf solche Kurven  $D$  zu verallgemeinern um einen Code der Länge  $\text{card}(D)$  zu erhalten? Das ist die Idee hinter den geometrischen Goppa Codes, die wir im folgenden exakt formulieren werden. Wir bedienen uns dazu der Sprache der algebraischen Funktionenkörper.

Für das Weitere seien folgende Begriffsbezeichnungen festgehalten:

- $F/\mathbb{F}_q$  ein Funktionenkörper vom Geschlecht  $g$
- $P_1, \dots, P_n$  paarweise verschiedene Stellen vom Grad 1
- $D := P_1 + \dots + P_n$
- $G \in \mathcal{D}_F$  mit  $\text{supp}(G) \cap \text{supp}(D) = \emptyset$

Definieren wir die Auswertungsabbildung  $ev_D : \mathcal{L}(G) \rightarrow \mathbb{F}_q^n$  durch

$$ev_D(x) := (x(P_1), \dots, x(P_n)) \in \mathbb{F}_q^n.$$

Diese Definition macht Sinn, da wegen  $\text{supp}(G) \cap \text{supp}(D) = \emptyset$  für  $x \in \mathcal{L}(G)$  die Beziehung  $v_{P_i}(x) \geq 0$  folgt und daher  $x(P_i) \in \mathbb{F}_q$  für  $i = 1, \dots, n$ . Nun sind wir in der Lage den geometrischen Goppa Code zu definieren:

**Definition 3.2.2** *Der zu  $D$  und  $G$  gehörige geometrische Goppa Code ist definiert durch*

$$\mathcal{C}_{\mathcal{L}}(D, G) := ev_D(\mathcal{L}(G)).$$

Nun ist die Codelänge nur noch durch die Anzahl der Stellen vom Grad 1 beschränkt.

**Satz 3.2.3**  $\mathcal{C}_{\mathcal{L}}(D, G)$  ist ein  $[n, k, d]$  Code mit

$$k = \dim(G) - \dim(G - D) \text{ und } d \geq n - \deg(G).$$

*Beweis:*  $ev_D$  ist eine surjektive lineare Abbildung von  $\mathcal{L}(D)$  nach  $\mathcal{C}_{\mathcal{L}}(D, G)$  mit Kern

$$\text{Ker}(ev_D) = \{x \in \mathcal{L}(D) : v_{P_i}(x) > 0 \text{ für } i = 1, \dots, n\} = \mathcal{L}(G - D).$$

Also gilt  $k = \dim(\mathcal{C}_{\mathcal{L}}(D, G)) = \dim(G) - \dim(G - D)$ . Wir nehmen an, dass  $\mathcal{C}_{\mathcal{L}}(D, G) \neq 0$ , sonst würde die Aussage über die Minimaldistanz keinen Sinn machen. Sei  $x \in \mathcal{L}(D)$  mit  $w(\text{ev}_D(x)) = d$ . Dann sind genau  $n - d$  Stellen  $P_{i_1}, \dots, P_{i_{n-d}} \in \text{supp}(D)$  Nullstellen von  $x$ , also gilt

$$0 \neq x \in \mathcal{L}(G - (P_{i_1} + \dots + P_{i_{n-d}})).$$

Es gilt wegen Korollar 2.4.12 (b)

$$0 \leq \deg(G - (P_{i_1} + \dots + P_{i_{n-d}})) = \deg(G) - (n - d).$$

Wir haben also

$$d \geq n - \deg(G).$$

□

**Satz 3.2.4** *Gelte  $\deg(G) < n$ . Dann ist die Abbildung  $\text{ev}_D$ , die jedem  $x \in \mathcal{L}(G)$  den Vektor  $(x(P_1), \dots, x(P_n))$  zuordnet, injektiv und es gilt:*

(a)  $\mathcal{C}_{\mathcal{L}}(D, G)$  ist ein  $[n, k, d]$  Code mit

$$d \geq n - \deg(G) \text{ und } k = \dim(G) \geq \deg(G) + 1 - g,$$

$$\text{also } k + d \geq n + 1 - g.$$

(b) Gilt zusätzlich  $2g - 2 < \deg(G) < n$ , so folgt

$$k = \deg(G) + 1 - g.$$

(c) Sei  $\{x_1, \dots, x_k\}$  eine Basis von  $\mathcal{L}(G)$ , dann ist die Matrix

$$M = \begin{pmatrix} x_1(P_1) & x_1(P_2) & \dots & x_1(P_n) \\ \vdots & \vdots & & \vdots \\ x_k(P_1) & x_k(P_2) & \dots & x_k(P_n) \end{pmatrix}$$

eine Generatormatrix von  $\mathcal{C}_{\mathcal{L}}(D, G)$ .

*Beweis:* Nach Voraussetzung gilt  $\deg(G - D) = \deg(G) - n < 0$ , also ist  $\mathcal{L}(G - D) = 0$  und  $\text{ev}_D$  injektiv. Die restlichen Aussagen folgen aus dem vorigen Satz und dem Satz von Riemann-Roch.

□

Mit Hilfe von lokalen Komponenten von Weil Differentialen kann man den Divisoren  $G$  und  $D$  noch einen anderen Code zuordnen:

**Definition 3.2.5** *Seien  $G$  und  $D$  wie vorhin. Wir definieren den Code  $\mathcal{C}_{\Omega}(D, G) \subseteq \mathbb{F}_q^n$  durch*

$$\mathcal{C}_{\Omega}(D, G) := \{(\omega_{P_1}(1), \dots, \omega_{P_n}(1)) : \omega \in \Omega_F(G - D)\}.$$

**Satz 3.2.6**  $\mathcal{C}_\Omega(D, G)$  ist ein  $[n, k', d']$ -Code mit

$$k' = i(G - D) - i(G) \text{ und } d' \geq \deg(G) - (2g - 2).$$

Unter der Voraussetzung  $\deg(G) > 2g - 2$  gilt  $k' = i(G - D) \geq n + g - 1 - \deg(G)$ . Gilt  $2g - 2 < \deg(G) < n$ , dann haben wir

$$k' = n + g - 1 - \deg(G).$$

*Beweis:* Sei  $P \in \mathbb{P}_F$  eine Stelle vom Grad 1 und  $\omega \in \Omega_F$  mit  $v_P(\omega) \geq -1$ .

**Behauptung:**

$$\omega_P(1) = 0 \Leftrightarrow v_P(\omega) \geq 0. \quad (3.1)$$

Um das zu beweisen, verwenden wir Proposition 2.9.3, die besagt, dass für eine ganze Zahl  $r$  gilt

$$v_P(\omega) \geq r \Leftrightarrow \omega_P(x) = 0 \text{ für alle } x \in F \text{ mit } v_P(x) \geq -r. \quad (3.2)$$

Die Implikation von Rechts nach Links in (3.1) folgt sofort aus (3.2). Für die andere Richtung nehmen wir an, dass  $\omega_P(1) = 0$  und sei  $x \in F$  mit  $v_P(x) \geq 0$ . Da  $\deg(P) = 1$  kann man  $x$  schreiben als  $x = a + y$  mit  $a = x(P) \in \mathbb{F}_q$  und  $v_P(y) \geq 1$ . Dann gilt

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P(1) + 0 = 0$$

weil  $v_P(\omega) \geq -1$  und  $v_P(y) \geq 1$ . Das beweist die Behauptung.

Als nächstes betrachten wir die  $\mathbb{F}_q$ -lineare Abbildung

$$\varrho_D : \begin{cases} \Omega_F(G - D) & \rightarrow & \mathcal{C}_\Omega(D, G), \\ \omega & \mapsto & (\omega_{P_1}(1), \dots, \omega_{P_n}(1)). \end{cases}$$

$\varrho_D$  ist surjektiv und nach (3.1) ist sein Kern gegeben durch  $\Omega_F(G)$ . Deshalb gilt

$$k' = \dim(\Omega_F(G - D)) - \dim(\Omega_F(G)) = i(G - D) - i(G). \quad (3.3)$$

Sei  $\varrho_D(\omega)$  ein Codewort vom Hamminggewicht  $m > 0$ . Dann gilt  $\omega_{P_i}(1) = 0$  für gewisse Indizes  $i = i_1, \dots, i_{n-m}$ , also gilt

$$\omega \in \Omega_F \left( G - \left( D - \sum_{j=1}^{n-m} P_{i_j} \right) \right)$$

wegen (3.1). Nach Satz 2.8.2 folgt aus  $\Omega_F(A) \neq 0$ , dass  $\deg(A) \leq 2g - 2$  ist. Wir erhalten

$$2g - 2 \geq \deg(G) - (n - (n - m)) = \deg(G) - m.$$

Es gilt also

$$d' \geq \deg(G) - (2g - 2).$$

Nehmen wir nun  $\deg(G) > 2g - 2$  an. Dann folgt aus Satz 2.8.2  $i(G) = 0$  und aus (3.3) und dem Satz von Riemann-Roch folgt

$$\begin{aligned} k' &= i(G - D) = \dim(G - D) - \deg(G - D) - 1 + g \\ &= \dim(G - D) + n + g - 1 - \deg(G). \end{aligned}$$

Alle weiteren Aussagen folgen nun sofort. □

Der folgende Satz beschreibt den Zusammenhang zwischen  $\mathcal{C}_\Omega(D, G)$  und  $\mathcal{C}_\mathcal{L}(D, G)$ .

**Satz 3.2.7** *Der Code  $\mathcal{C}_\Omega(D, G)$  ist der Dualcode von  $\mathcal{C}_\mathcal{L}(D, G)$ , d.h.*

$$\mathcal{C}_\Omega(D, G) = \mathcal{C}_\mathcal{L}(D, G)^\perp.$$

*Beweis:*

**1. Behauptung:** Sei  $P \in \mathbb{P}_F$  eine Stelle vom Grad 1,  $\omega \in \Omega_F$  mit  $v_P(\omega) \geq -1$  und  $x \in F$  mit  $v_P(x) \geq 0$ . Dann gilt

$$\omega_P(x) = x(P) \cdot \omega_P(1). \quad (3.4)$$

Um dies einzusehen schreiben wir  $x = a + y$ ,  $a = x(P) \in \mathbb{F}_q$  und  $y \in P$ , d.h.  $v_P(y) > 0$ . Dann gilt wegen (3.2)

$$\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P(1) + 0 = x(P) \cdot \omega_P(1).$$

**2. Behauptung:**  $\mathcal{C}_\Omega(D, G) \subseteq \mathcal{C}_\mathcal{L}(D, G)^\perp$ .

Sei  $\omega \in \Omega(G - D)$  und  $x \in \mathcal{L}(G)$ . Wir erhalten

$$\begin{aligned} 0 &= \omega(x) = \sum_{P \in \mathbb{P}_F} \omega_P(x) \\ &= \sum_{i=1}^n \omega_{P_i}(x) \end{aligned} \quad (3.5)$$

$$\begin{aligned} &= \sum_{i=1}^n x(P_i) \cdot \omega_{P_i}(1) \\ &= \langle (\omega_{P_1}(1), \dots, \omega_{P_n}(1)), (x(P_1), \dots, x(P_n)) \rangle. \end{aligned} \quad (3.6)$$

(3.5) folgt aus (3.2) und der Tatsache, dass für  $P \in \mathbb{P}_F \setminus \{P_1, \dots, P_n\}$   $v_P(x) \geq -v_P(\omega)$  gilt (da  $x \in \mathcal{L}(G)$  und  $\omega \in \Omega_F(G - D)$ ). (3.6) folgt aus (3.4). Das beweist die 2. Behauptung.

**3. Behauptung:**  $\dim(\mathcal{C}_\Omega(D, G)) = \dim(\mathcal{C}_\mathcal{L}(D, G)^\perp)$ .

Es gilt nach dem Satz von Riemann-Roch

$$\dim(\mathcal{C}_\Omega(G, D)) = i(G - D) - i(G)$$

$$\begin{aligned}
&= \dim(G - D) - \deg(G - D) - 1 + g - (\dim(G) - \deg(G) - 1 + g) \\
&= \deg(D) + \dim(G - D) - \dim(G) \\
&= n - (\dim(G) - \dim(G - D)) \\
&= n - \dim(\mathcal{C}_{\mathcal{L}}(D, G)) = \dim(\mathcal{C}_{\mathcal{L}}(D, G)^\perp).
\end{aligned}$$

Das beweist die 3.Behauptung und den Satz. □

Unser nächstes Ziel ist es zu zeigen, dass die Codes  $\mathcal{C}_{\Omega}(D, G)$  als Goppa Codes  $\mathcal{C}_{\mathcal{L}}(D, H)$  dargestellt werden können, mit einem geeigneten Divisor  $H$ . Dazu benötigen wir das folgende Lemma.

**Lemma 3.2.8** *Es existiert ein  $\eta \in \Omega_F$  mit*

$$v_{P_i}(\eta) = -1 \text{ und } \eta_{P_i}(1) = 1 \text{ für } i = 1, \dots, n.$$

*Beweis:* Sei  $0 \neq \omega_0 \in \Omega_F$ . Nach dem schwachen Approximationssatz existiert ein  $z \in F$  mit

$$v_{P_i}(z) = -v_{P_i}(\omega_0) - 1 \text{ für } i = 1, \dots, n.$$

Setzen wir  $\omega := z\omega_0$ , dann gilt  $v_{P_i}(\omega) = -1$ . Also gilt  $a_i := \omega_{P_i}(1) \neq 0$  wegen (3.1). Wieder nach dem schwachen Approximationssatz existiert ein  $y \in F$  mit  $v_{P_i}(y - a_i) > 0$ . Es folgt  $v_{P_i}(y) = 0$  und  $y(P_i) = a_i$ . Wir setzen  $\eta := y^{-1}\omega$  und erhalten  $v_{P_i}(\eta) = v_{P_i}(\omega) = -1$  und

$$\eta_{P_i}(1) = \omega_{P_i}(y^{-1}) = y^{-1}(P_i) \cdot \omega_{P_i}(1) = a_i^{-1} \cdot a_i = 1.$$

□

**Proposition 3.2.9** *Sei  $\eta$  das Weil Differential aus dem vorigen Lemma. Dann gilt*

$$\mathcal{C}_{\mathcal{L}}(D, G)^\perp = \mathcal{C}_{\Omega}(D, G) = \mathcal{C}_{\mathcal{L}}(D, H) \text{ mit } H := D - G + (\eta).$$

*Beweis:* Der Code  $\mathcal{C}_{\mathcal{L}}(D, H)$  ist wohldefiniert, da wegen  $v_{P_i}(\eta) = -1$  für  $i = 1, \dots, n$   $\text{supp}(D - G + (\eta)) \cap \text{supp}(D) = \emptyset$  gilt. Wegen Satz 2.7.14 existiert ein Isomorphismus  $\mu : \mathcal{L}(D - G + (\eta)) \rightarrow \Omega_F(G - D)$  gegeben durch  $\mu(x) := x\eta$ . Für  $x \in \mathcal{L}(D - G + (\eta))$  gilt

$$(x\eta)_{P_i}(1) = \eta_{P_i}(x) = x(P_i) \cdot \eta_{P_i}(1) = x(P_i)$$

wegen (3.4). Daher gilt  $\mathcal{C}_{\Omega}(D, G) = \mathcal{C}_{\mathcal{L}}(D, D - G + (\eta))$ . □

### 3.3 Asymptotische Eigenschaften

Wir wenden uns den asymptotischen Eigenschaften von Goppa Codes zu. Ein asymptotisches Resultat haben wir schon kennengelernt: Die asymptotische Gilbert-Varshamov Schranke. Wir werden sie nun etwas anders formulieren und dann zeigen wir man mit Goppas Konstruktion Codes konstruieren kann, die die Gilbert-Varshamov Schranke übertreffen. Wir beginnen mit einem Resultat, das auf Yu. I. Manin zurückgeht.

**Definition 3.3.1** *Wir definieren die folgenden Teilmengen von  $[0, 1] \times [0, 1]$ :*

$$U_q := \{(\delta, R) : \text{Es existiert ein Linearcode } C \text{ über } \mathbb{F}_q \text{ mit } \delta = \delta(C) \text{ und } R = R(C)\}$$

und  $V_q$  sei die Menge der Häufungspunkte von  $U_q$ .

**Satz 3.3.2 (Manin)** *Es existiert eine stetige Funktion  $\alpha_q(\delta)$ ,  $\delta \in [0, 1]$  mit*

$$U_q = \{(\delta, R) : 0 \leq \delta \leq 1 \text{ und } 0 \leq R \leq \alpha_q(\delta)\}^2.$$

Weiters ist die Funktion  $\alpha_q(\delta)$  monoton fallend.

*Beweis:* Findet sich in [29].

□

Die Gilbert-Varshamov Schranke besagt nichts anderes, als

$$\alpha_q(\delta) \geq 1 - H_q(\delta).$$

Lange Zeit dachte man, dass sogar

$$\alpha_q(\delta) = 1 - H_1(\delta)$$

gilt. Wir zeigen jedoch mit Hilfe von geometrischen Goppa Codes, dass das nicht gilt. Zunächst wollen wir eine andere untere Schranke für  $\alpha_q(\delta)$  herleiten. Dazu brauchen wir das folgende Lemma:

**Lemma 3.3.3** *Seien  $P_1, \dots, P_n$  paarweise verschiedene Stellen von  $F/\mathbb{F}_q$  vom Grad 1. Dann existiert für jedes  $r \geq 0$  ein Divisor  $G \in \mathcal{D}_F$  mit  $\deg(G) = r$  und  $P_i \notin \text{supp}(G)$  ( $i = 1, \dots, n$ ).*

*Beweis:* Falls eine Stelle  $Q$  vom Grad 1 existiert mit  $Q \neq P_i$  für alle  $i = 1, \dots, n$ , dann leistet  $G := rQ$  das Gewünschte. Seien also  $P_1, \dots, P_n$  alle Stellen vom Grad 1. Nach dem Approximationssatz existiert ein  $x \in F$  mit  $v_{P_i}(x) = 0$  für  $i = 2, \dots, n$ , und  $v_{P_1}(x) = -r$ . Setzen wir  $G := rP_1 + (x)$ . Dann gilt  $\deg(G) = \deg(rP_1 + (x)) = r \cdot \deg(P_1) + \deg((x)) = r$  nach Satz 2.4.11 und der Voraussetzung  $\deg(P_1) = 1$ . Weiters gilt  $v_{P_i}(G) = v_{P_i}(rP_1 + (x)) = r \cdot v_{P_i}(P_1) + v_{P_i}(x) = 0$  für  $i = 1, \dots, n$ , aufgrund der Wahl von  $x$ .

---

<sup>2</sup>Es ist bis dato unbekannt, ob die Funktion  $\alpha_q(\delta)$  differenzierbar ist.

□

**Definition 3.3.4** Für einen Funktionenkörper  $F/\mathbb{F}_q$  definieren wir

$$N(F) := \text{card}(\{P \in \mathbb{P}_F : \text{deg}(P) = 1\}).$$

Weiters definieren wir

$$N_q(g) := \max\{N(F) : F \text{ ist ein Funktionenkörper über } \mathbb{F}_q \text{ vom Geschlecht } g\}$$

und

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

Wir beweisen nun eine zweite untere Schranke für  $\alpha_q(\delta)$ .

**Proposition 3.3.5** Sei  $A(q) > 1$ . Dann gilt für  $0 \leq \delta \leq 1 - A(q)^{-1}$

$$\alpha_q(\delta) \geq (1 - A(q)^{-1}) - \delta.$$

*Beweis:* Sei  $\delta \in [0, 1 - A(q)^{-1}]$ . Wählen wir eine Folge von Funktionenkörpern  $F_i/\mathbb{F}_q$  vom Geschlecht  $g_i$  mit

$$g_i \rightarrow \infty \text{ und } \frac{n_i}{g_i} \rightarrow A(q), \quad (3.7)$$

mit  $n_i := N(F_i)$ . Wählen wir zusätzlich Zahlen  $r_i > 0$  mit

$$\frac{r_i}{n_i} \rightarrow 1 - \delta. \quad (3.8)$$

Sei  $D_i$  die Summe über alle Stellen von  $F_i/\mathbb{F}_q$  vom Grad 1, also  $\text{deg}(D_i) = n_i$ . Nach dem obigen Lemma existiert ein Divisor  $G_i \in \mathcal{D}_F$  mit  $\text{deg}(G_i) = r_i$  und  $\text{supp}(G_i) \cap \text{supp}(D_i) = \emptyset$ . Betrachten wir den  $[n_i, k_i, d_i]$ -Code  $C_i := \mathcal{C}_{\mathcal{L}}(D_i, G_i)$ . Es gilt nach Satz 3.2.4

$$k_i \geq \text{deg}(G_i) + 1 - g_i = r_i + 1 - g_i \text{ und } d_i \geq n_i - \text{deg}(G_i) = n_i - r_i.$$

Daraus folgt

$$R_i := R(C_i) \geq \frac{r_i + 1}{n_i} - \frac{g_i}{n_i} \text{ und } \delta_i := \delta(C_i) \geq 1 - \frac{r_i}{n_i}. \quad (3.9)$$

Durch Übergang zu Teilfolgen können wir annehmen, dass die Folgen  $(R_i)_{i \geq 1}$  und  $(\delta_i)_{i \geq 1}$  konvergent sind, wir schreiben

$$R_i \rightarrow R \text{ und } \delta_i \rightarrow \tilde{\delta}.$$

Aus (3.7), (3.8) und (3.9) folgt, dass  $R \geq 1 - \delta - A(q)^{-1}$  und  $\tilde{\delta} \geq \delta$ . Es gilt also

$$\alpha_q(\tilde{\delta}) \geq R \geq 1 - \delta - A(q)^{-1}.$$

Da  $\alpha_q(\delta)$  fallend ist, folgt

$$\alpha_q(\delta) \geq \alpha_q(\tilde{\delta}) \geq 1 - \delta - A(q)^{-1}.$$

□

Untere Schranken für  $A(q)$  ergeben also untere Schranken für  $\alpha_q(\delta)$ . Mit Hilfe von Uniformisierungstheorie von Shimurakurven haben Tsfasman und Zink das folgende zeigen können:

**Satz 3.3.6** *Für ein Quadrat  $q$  gilt*

$$A(q) \geq q^{1/2} - 1.$$

Aus der Drinfeld-Vladut Schranke, die wir im nächsten Kapitel (aufbauend auf dem Satz von Hasse-Weil) beweisen werden, folgt sogar

**Satz 3.3.7 (Tsfasman-Vladut-Zink)** *Für ein Quadrat  $q$  gilt*

$$A(q) = q^{1/2} - 1.$$

Mit dem Satz von Tsfasman-Vladut-Zink haben wir eine neue Schranke für  $\alpha_q(\delta)$ :

**Satz 3.3.8**

$$\alpha_q(\delta) \geq \left(1 - \frac{1}{q^{1/2} - 1}\right) - \delta \text{ für } 0 \leq \delta \leq 1 - \frac{1}{q^{1/2} - 1}.$$

Man sieht leicht, dass das eine echte Verbesserung der Gilbert-Varshamov Schranke ist. Ziel dieser Arbeit ist es den Satz von Tsfasman-Vladut-Zink zu beweisen. Wir werden dazu sogar explizite Folgen von Kurven, bzw. Funktionenkörpern  $F_i/\mathbb{F}_q$  vom Geschlecht  $g_i$  konstruieren mit  $\lim_{i \rightarrow \infty} \frac{N(F_i)}{g_i} = q^{1/2} - 1$ . Dazu müssen wir zunächst im folgenden Kapitel Erweiterungen von Funktionenkörpern genauer studieren.

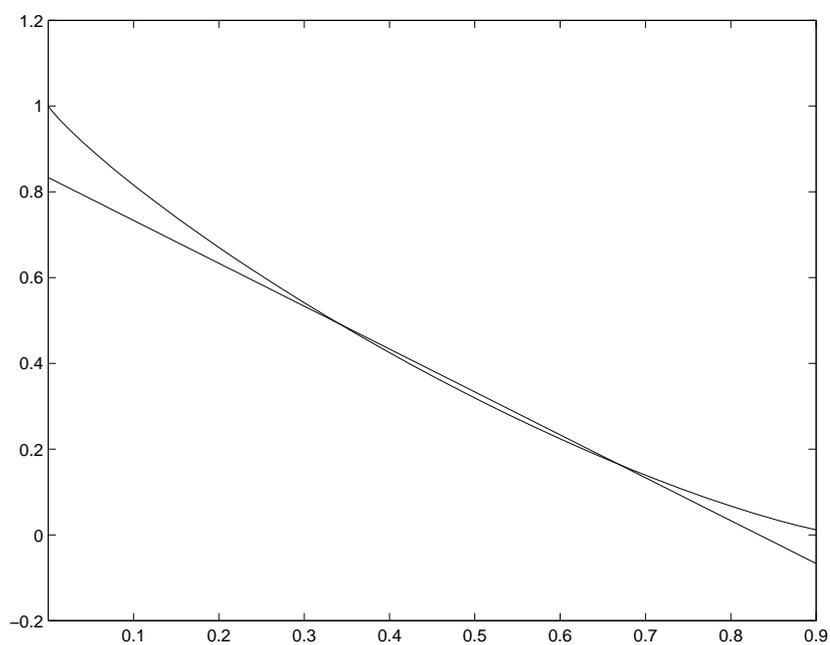


Abbildung 3.1: Die Asymptotische Gilbert-Varshamov Schranke im Vergleich mit der linearen Tsfasman-Vladut-Zink Schranke.

# Kapitel 4

## Erweiterungen von Funktionskörpern

Dieses Kapitel ist das technische Herzstück dieser Arbeit. Hier werden die Werkzeuge entwickelt mit denen man geeignete Funktionskörpertürme konstruieren kann. Aufgrund der sehr komplexen Verzweigungstheorie von Funktionskörpererweiterungen ist dieses Kapitel sehr umfangreich und auch teilweise technisch. Wer mit Bewertungstheorie und Dedekindringen vertraut ist, wird viele bekannte Sachverhalte entdecken, im Wesentlichen ist die Theorie der Funktionskörpererweiterungen ja auch eine Anwendung der Verzweigungstheorie von Bewertungen. Gerne hätte ich dieses Kapitel von diesem Standpunkt her beleuchtet, jedoch würde das dann ein Kapitel über Dedekindringe und Bewertungen erforderlich machen und das würde den Rahmen dieser Arbeit sprengen. Ein klassisches Werk über Bewertungstheorie ist [37]. In [34, 30] wird die Theorie der Funktionskörper mit Hilfe der Theorie von Dedekindringen aufgebaut. Wir beschäftigen uns hier nur mit algebraischen Erweiterungen, da nur diese für die Anwendungen interessant sind. Um dieses Kapitel gänzlich verstehen zu können, muss man mit Galoistheorie vertraut sein.

### 4.1 Algebraische Erweiterungen

Für das folgende wollen wir einige Voraussetzungen treffen:

- $K$  ist der volle Konstantenkörper von  $F/K$ .
- $K$  ist vollkommen, d.h. jede algebraische Erweiterung von  $K$  ist separabel.

Wir beginnen mit einigen wichtigen Definitionen.

**Definition 4.1.1** Sei  $F/K$  ein Funktionskörper.

- (a) Ein algebraischer Funktionskörper  $F'/K'$  heißt **algebraische Erweiterung** von  $F/K$ , falls  $F' \supseteq F$  eine algebraische Körpererweiterung ist und  $K' \supseteq K$  gilt.

- (b) Eine algebraische Funktionenkörpererweiterung  $F'/K'$  von  $F/K$  heißt **Konstantenkörpererweiterung**, falls  $F' = FK'$  durch Komposition der Körper  $F$  und  $K'$  entsteht.
- (c) Eine algebraische Funktionenkörpererweiterung  $F'/K'$  von  $F/K$  heißt **endlich**, falls  $[F' : F] < \infty$ .

**Lemma 4.1.2** Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$ . Dann gilt:

- (a)  $K'/K$  ist algebraisch und  $F \cap K' = K$ .
- (b)  $F'/K'$  ist eine endliche Erweiterung von  $F/K$ , genau wenn  $[K' : K] < \infty$ .
- (c) Sei  $F_1 := FK'$ . Dann ist  $F_1/K'$  eine Konstantenkörpererweiterung von  $F/K$  und  $F'/K'$  ist eine endliche Erweiterung von  $F_1/K'$ .

*Beweis:* (a) Klarerweise ist die Körpererweiterung  $K'(x) \supseteq K(x)$  algebraisch, da ja  $F' \supseteq F$  und  $F \supseteq K(x)$  algebraische Körpererweiterungen sind. Es gilt also für jedes  $a \in K'$ , dass ein Polynom  $\psi(T) = \psi_0(x) + \psi_1(x)T + \dots + \psi_n(x)T^n \in K(x)[T]$  existiert mit  $\psi(a) = 0$ . Wir haben also

$$\psi_0(x) + \psi_1(x)a + \psi_2(x)a^2 + \dots + \psi_n(x)a^n = 0.$$

Seien o.B.d.A die Koeffizienten  $\psi_i(x)$  Polynome aus  $K[x]$ , wobei nicht alle durch  $x$  teilbar sind, also  $\psi_i(x) = xg_i(x) + b_i, b_i \in K$ , nicht alle  $b_i = 0$  ( $i = 1, \dots, n$ ). Dann bekommen wir eine Relation der Form

$$xg_0(x) + xg_1(x)a + \dots + xg_n(x)a^n + b_0 + b_1a + b_na^n = 0. \quad (4.1)$$

Diese Relation ist eine Relation im Ring  $K[x]$ . Wenden wir den Einsetzungshomomorphismus an der Stelle  $x = 0$  auf (4.1) an, so erhalten wir eine algebraische Gleichung für  $a$ .  $K' \supseteq K$  ist also eine algebraische Körpererweiterung und da  $K$  der volle Konstantenkörper von  $F/K$  ist, gilt  $K' \cap F \subseteq K$ . Die umgekehrte Inklusion ist trivial.

(b) Sei  $F'/K'$  eine endliche Erweiterung von  $F/K$ . Dann kann  $F'$  als Funktionenkörper über  $K$  aufgefasst werden. Es gilt also  $[K' : K] < \infty$  nach Korollar 2.1.16. Nehmen wir umgekehrt an, dass  $[K' : K] < \infty$  gilt. Für ein  $x \in F' \setminus K$  gilt wegen (a), dass  $x$  transzendent über  $K'$  ist und daher  $[F' : K'(x)] < \infty$ . Ausserdem gilt

$$[K'(x) : K(x)] \leq [K' : K] < \infty,$$

nach Voraussetzung. Also gilt

$$[F' : K(x)] = [F' : K'(x)] \cdot [K'(x) : K(x)] < \infty.$$

Daraus folgt  $[F' : F] < \infty$ .

(c) folgt aus (b).

□

**Definition 4.1.3** Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$ . Eine Stelle  $P' \in \mathbb{P}_{F'}$  liegt über  $P \in \mathbb{P}_F$ , falls  $P \subseteq P'$ . Man sagt auch: „ $P'$  ist eine **Erweiterung** von  $P$ “, oder „ $P$  liegt unter  $P'$ “ und schreibt  $P'|P$ .

**Proposition 4.1.4** Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$ ,  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$ . Dann sind die folgenden Aussagen äquivalent:

- (1)  $P'|P$ .
- (2)  $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$ .
- (3) Es existiert eine ganze Zahl  $e \geq 1$  mit  $v_{P'}(x) = e \cdot v_P(x)$  für alle  $x \in F$ .

Ausserdem gilt

$$P = P' \cap F \text{ und } \mathcal{O}_P = \mathcal{O}_{P'} \cap F,$$

falls  $P'|P$ .  $P$  heißt deshalb auch die **Einschränkung** von  $P'$  auf  $F$ .

*Beweis:*

(1)  $\Rightarrow$  (2): Angenommen es gelte  $P'|P$  und  $\mathcal{O}_P \not\subseteq \mathcal{O}_{P'}$ . Dann existiert ein  $u \in F$  mit  $v_P(u) \geq 0$  und  $v_{P'}(u) < 0$ . Wegen  $P'|P$  gilt sogar  $v_P(u) = 0$ . Sei  $t \in F$  mit  $v_P(t) = 1$ . Dann gilt mit  $r := v_{P'}(t) > 0$ :

$$v_P(u^r t) = r \cdot v_P(u) + v_P(t) = 1$$

und

$$v_{P'}(u^r t) = r \cdot v_{P'}(u) + v_{P'}(t) \leq -r + r = 0.$$

Es gilt also  $u^r t \in P \setminus P'$  und das ist ein Widerspruch zu  $P'|P$ .

(2)  $\Rightarrow$  (3): Sei  $t$  ein primes Element von  $P$  und  $t'$  ein primes Element von  $P'$ .  $\mathcal{O}_{P'} P = \mathcal{O}_{P'} \mathcal{O}_P \cdot t = \mathcal{O}_{P'} \cdot t$  ist ein nichttriviales (Haupt-) Ideal von  $\mathcal{O}_{P'}$  weil  $t \in \mathcal{O}_{P'}$  und daher existiert wegen Satz 2.1.6 ein  $1 \leq e \in \mathbb{Z}$  mit  $\mathcal{O}_{P'} t = \mathcal{O}_{P'} (t')^e$ . Also gilt  $t = (t')^e u$  für ein  $u \in \mathcal{O}_{P'}^*$ , und daraus folgt (3) unmittelbar.

(3)  $\Rightarrow$  (1): Sei  $x \in P$ . Dann ist  $v_P(x) \geq 1$  und damit auch  $v_{P'}(x) = e \cdot v_P(x) \geq 1$ , also gilt  $x \in P'$ .

Die restlichen Aussagen folgen nun trivialerweise.

□

**Lemma 4.1.5** Es existiert eine kanonische Einbettung von  $F_P$  in  $F'_{P'}$ , falls  $P'|P$ .

*Beweis:* Man ordne einer Restklasse  $x + P \in F_P = F/\mathcal{O}_P$  einfach die Restklasse  $x + P' \in F'_{P'} = F'/\mathcal{O}_{P'}$  zu. Diese Abbildung ist wohldefiniert, nach Voraussetzung, und injektiv nach der vorangegangenen Proposition. □

Man kann also  $F_P$  als Unterkörper von  $F'_{P'}$  auffassen.

**Definition 4.1.6** Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$ ,  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$ .

(a) Die Zahl  $e(P'|P) := e$  mit <http://student.tuwien.ac.at/>

$$v_{P'}(x) = e \cdot v_P(x) \text{ für } x \in F$$

heißt **Verzweigungsindex** von  $P'$  über  $P$ . Ist  $e(P'|P) > 1$ , so sagen wir  $P'|P$  ist **verzweigt**, andernfalls ist  $P'|P$  **unverzweigt**.

(b)  $f(P'|P) := [F'_{P'} : F_P]$  heißt **relativer Grad** von  $P'|P$ .

**Proposition 4.1.7** Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$  und  $P'$  eine Stelle von  $F'/K'$ , die über einer Stelle  $P$  von  $F/K$  liegt. Dann gilt

(a)  $f(P'|P) < \infty \Leftrightarrow [F' : F] < \infty$ .

(b) Sei  $F''/K''$  eine algebraische Erweiterung von  $F'/K'$  und  $P'' \in \mathbb{P}_{F''}$  mit  $P''|P'$ . Dann gilt

$$\begin{aligned} e(P''|P) &= e(P''|P') \cdot e(P'|P) \text{ und} \\ f(P''|P) &= f(P''|P') \cdot f(P'|P). \end{aligned}$$

*Beweis:* (a) Betrachte die kanonischen Einbettungen  $K \subseteq F_P \subseteq F'_{P'}$  und  $K \subseteq K' \subseteq F'_{P'}$ , wobei  $[F_P : K] < \infty$  und  $[F'_{P'} : K'] < \infty$ . Es folgt

$$[F'_{P'} : F_P] < \infty \Leftrightarrow [K' : K] < \infty.$$

Wegen Lemma 4.1.2 ist aber die letztere Bedingung äquivalent zu  $[F' : F] < \infty$ .

(b) folgt direkt aus der Definition. □

Als nächstes wollen wir uns überlegen, ob überhaupt Erweiterungen von einer gegebenen Stelle existieren, und wenn ja, wieviele.

**Proposition 4.1.8** Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$ .

(a) Für jede Stelle  $P' \in \mathbb{P}_{F'}$  existiert genau eine Stelle  $P \in \mathbb{P}_F$  mit  $P'|P$ , und zwar gilt  $P = P' \cap F$ .

(b) Umgekehrt hat jede Stelle  $P \in \mathbb{P}_F$  zumindest eine und höchstens endlich viele Erweiterungen  $P' \in \mathbb{P}_{F'}$ .

*Beweis:* (a) **Behauptung:** Es existiert ein  $z \in F$  mit

$$z \neq 0 \text{ und } v_{P'}(z) \neq 0. \quad (4.2)$$

Angenommen das wäre falsch. Wähle ein  $t \in F'$  mit  $v_{P'}(t) = 1$ . Dann genügt  $t$  einer algebraischen Gleichung über  $F$ :

$$c_n t^n + c_{n-1} t^{n-1} + \dots + c_1 t + c_0 = 0, \quad c_i \in F, \quad c_n \neq 0, \quad c_0 \neq 0.$$

Nach unserer Annahmen muss  $v_{P'}(c_0) = 0$  gelten und  $v_{P'}(c_i t^i) = v_{P'}(c_i) + i \cdot v_{P'}(t) > 0$  für  $i > 0$ . Wir haben einen Widerspruch zur starken Dreiecksungleichung und damit (4.2) bewiesen.

Setzen wir  $\mathcal{O} := \mathcal{O}_{P'} \cap F$  und  $P := P' \cap F$ . Nach (4.2) ist  $\mathcal{O}$  ein Bewertungsring, da trivialerweise alle Bedingungen aus Definition 2.1.4 bis auf  $\mathcal{O} \subset F$  erfüllt sind. Wegen (4.2) gilt aber  $z^{-1} \notin \mathcal{O}$  und das beweist  $\mathcal{O} \subset F$ .  $P := P' \cap F$  ist ein Ideal von  $\mathcal{O}$  und da für jedes Ideal  $I$  von  $\mathcal{O}$  gelten muss, dass  $I \subseteq P$ , ist  $P$  die zu  $\mathcal{O}$  gehörige Stelle. Die Eindeutigkeit ist klar.

(b) Sei  $P \in \mathbb{P}_F$ . wähle ein  $x \in F \setminus K$  sodass  $P$  die einzige Nullstelle von  $x$  ist (siehe Proposition 2.8.3).

**Behauptung:** Für  $P' \in \mathbb{P}_{F'}$  gilt

$$P'|P \Leftrightarrow v_{P'}(x) > 0. \quad (4.3)$$

Sei  $P'|P$ , dann gilt  $v_{P'}(x) = e \cdot v_P(x) > 0$ . Nehmen wir umgekehrt an  $v_{P'}(x) > 0$ . Sei  $Q$  die eindeutige Stellen von  $F/K$ , die unter  $P'$  liegt (hier verwenden wir (a)). Dann gilt  $v_Q(x) > 0$ , also  $P = Q$ , da  $P$  die einzige Nullstelle von  $x$  ist.

Da  $x \notin K'$  mindestens eine und höchstens endlich viele Nullstellen in  $F'/K'$  hat, folgt (b). □

Wir sind nun in der Lage, einen Homomorphismus von der Divisorgruppe  $\mathcal{D}_F$  auf die Divisorgruppe  $\mathcal{D}_{F'}$  anzugeben.

**Definition 4.1.9** Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$  und  $P \in \mathbb{P}_F$ . Wir definieren die **Conorm** von  $P$  als den Divisor

$$\text{Con}_{F'/F}(P) := \sum_{P'|P} e(P'|P) \cdot P.$$

Diese Abbildung ist zunächst nur auf  $\mathbb{P}_F$  definiert und wird durch die universelle Eigenschaft der Divisorgruppe auf ganz  $\mathcal{D}_F$  ausgedehnt.

**Proposition 4.1.10** *Sei  $F'/K'$  eine algebraische Erweiterung von  $F/K$ . Für  $0 \neq x \in F$  sei  $(x)_0^F, (x)_\infty^F, (x)^F$  bzw.  $(x)_0^{F'}, (x)_\infty^{F'}, (x)^{F'}$  der Nullstellen-, Pol- und Hauptdivisor von  $x$  in  $\mathcal{D}_F$  bzw.  $\mathcal{D}_{F'}$ . Dann gilt*

$$\text{Con}_{F'/F}((x)_0^F) = (x)_0^{F'}, \text{Con}_{F'/F}((x)_\infty^F) = (x)_\infty^{F'}, \text{ und } \text{Con}_{F'/F}((x)^F) = (x)^{F'}.$$

*Beweis:*

$$\begin{aligned} (x)^{F'} &= \sum_{P' \in \mathbb{P}_{F'}} v_{P'}(x) \cdot P' = \sum_{P \in \mathbb{P}_F} \sum_{P'|P} e(P'|P) \cdot v_P(x) \cdot P' \\ &= \sum_{P \in \mathbb{P}_F} v_P(x) \cdot \text{Con}_{F'/F}(P) = \text{Con}_{F'/F}((x)^F). \end{aligned}$$

Die restlichen Aussagen folgen daraus unmittelbar. □

## 4.2 Die Fundamentalgleichung von Hilbert

In diesem Abschnitt werden wir die sogenannte Fundamentalgleichung von Hilbert beweisen. Daraus ergibt sich eine Formel für den Grad der Conorm eines Divisors. Zudem werden wir mit Hilfe des Satzes von Kummer sehen, wie man einige Stellen explizit faktorisieren kann. Zunächst ein einfaches Lemma:

**Lemma 4.2.1** *Sei  $K'/K$  eine endliche Körpererweiterung und  $x$  transzendent über  $K$ . Dann gilt*

$$[K'(x) : K(x)] = [K' : K].$$

*Beweis:* Wir wählen ein  $\alpha \in K'$  mit  $K' = K(\alpha)$ . Dies ist möglich aufgrund unserer Annahme, dass  $K$  vollkommen ist und des Satzes vom primitiven Element (siehe z.B. [27]). Daraus folgt  $K'(x) = K(\alpha)(x)$ , also gilt  $[K'(x) : K(x)] \leq [K' : K]$ . Um die umgekehrte Ungleichung zu zeigen, beweisen wir, dass das irreduzible Polynom  $\varphi(T) \in K[T]$  von  $\alpha$  über  $K$  irreduzibel über  $K(x)$  ist. Angenommen dem wäre nicht so. Dann hätten wir  $\varphi(T) = g(T) \cdot h(T)$  mit normierten Polynomen  $g(T), h(T) \in K(x)[T]$  von kleinerem Grad als  $\varphi$ . Es gilt  $\varphi(\alpha) = 0$ , wir können also o.B.d.A. annehmen, dass  $g(\alpha) = 0$ . Wir schreiben

$$g(T) = T^r + c_{r-1}(x)T^{r-1} + \dots + c_0(x),$$

$c_i(x) \in K(x)$  und  $r < \deg(\varphi)$ . Setzen wir  $\alpha$  ein, so erhalten wir

$$\alpha^r + c_{r-1}(x)\alpha^{r-1} + \dots + c_0(x) = 0.$$

Multiplizieren wir mit einem gemeinsamen Nenner, so erhalten wir

$$g_r(x)\alpha^r + g_{r-1}(x)\alpha^{r-1} + \dots + g_0(x) = 0.$$

Die Koeffizienten  $g_i(x)$  sind nun Polynome in  $K[x]$  und wir nehmen o.B.d.A. an, dass nicht alle  $g_i(x)$  durch  $x$  teilbar sind. Setzen wir  $x = 0$ , so erhalten wir eine nichttriviale algebraische Gleichung für  $\alpha$  über  $K$  vom Grad kleiner als  $\varphi$ . Widerspruch!

□

Nun sind wir in der Lage die **Fundamentalgleichung von Hilbert** zu beweisen:

**Satz 4.2.2** *Sei  $F'/K'$  eine endliche Erweiterung von  $F/K$ ,  $P$  eine Stelle von  $F/K$  und  $P_1, \dots, P_m$  alle Stellen von  $F'/K'$ , die über  $P$  liegen. Sei  $e_i := e(P_i|P)$  und  $f_i := f(P_i|P)$ . Dann gilt*

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

*Beweis:* Wähle ein  $x \in F$  mit  $P$  als einziger Nullstelle in  $F/K$  (siehe Proposition 2.8.3) und sei  $v_P(x) =: r > 0$ . Die Stellen  $P_1, \dots, P_r$  sind genau die Nullstellen von  $x$  in  $F'/K'$  wegen (4.3). Wir berechnen  $[F' : K(x)]$  auf zwei Arten:

$$\begin{aligned} [F' : K(x)] &= [F' : K'(x)] \cdot [K'(x) : K(x)] \\ &= \left( \sum_{i=1}^m v_{P_i}(x) \cdot \deg(P_i) \right) \cdot [K' : K] \\ &= \sum_{i=1}^n (e_i \cdot v_P(x)) \cdot ([F'_{P_i} : K'] \cdot [K' : K]) \\ &= r \cdot \sum_{i=1}^m e_i \cdot [F'_{P_i} : F_P] \cdot [F_P : K] \\ &= r \cdot \deg(P) \cdot \sum_{i=1}^m e_i f_i. \end{aligned}$$

Hier haben wir das obige Lemma und Satz 2.4.12 und Lemma 2.1.8 verwendet. Andererseits gilt

$$[F' : K(x)] = [F' : F] \cdot [F : K(x)] = [F' : F] \cdot r \cdot \deg(P),$$

da ja  $rP$  der Nulldivisor von  $x$  in  $F/K$  ist. Durch Vergleich der beiden Formeln folgt die Hilbertsche Fundamentalgleichung.

□

**Korollar 4.2.3** *Sei  $F'/K'$  eine endliche Erweiterung von  $F/K$  und  $P \in \mathbb{P}_F$ . Dann gilt*

$$(a) \text{ card}(\{P' \in \mathbb{P}_{F'} : P'|P\}) \leq [F' : F].$$

$$(b) \text{ Für } P'|P \text{ gilt } e(P'|P) \leq [F' : F] \text{ und } f(P'|P) \leq [F' : F].$$

**Korollar 4.2.4** Sei  $F'/K'$  eine endliche Erweiterung von  $F/K$ . Dann gilt für jeden Divisor  $A \in \mathcal{D}_F$ ,

$$\deg(\text{Con}_{F'/F}(A)) = \frac{[F' : F]}{[K' : K]} \cdot \deg(A).$$

*Beweis:* Es reicht den Fall  $A = P$ ,  $P \in \mathbb{P}_F$  zu betrachten. Es gilt

$$\begin{aligned} \deg(\text{Con}_{F'/F}(P)) &= \deg \left( \sum_{P'|P} e(P'|P) \cdot P' \right) \\ &= \sum_{P'|P} e(P'|P) \cdot [F_{P'} : K'] \\ &= \sum_{P'|P} e(P'|P) \cdot \frac{[F_{P'} : K]}{[K' : K]} \\ &= \frac{1}{[K' : K]} \sum_{P'|P} e(P'|P) \cdot [F_{P'} : F_P] \cdot [F_P : K] \\ &= \frac{1}{[K' : K]} \sum_{P'|P} e(P'|P) \cdot f(P'|P) \cdot \deg(P) \\ &= \frac{[F' : F]}{[K' : K]} \deg(P), \end{aligned}$$

wegen der Hilbertschen Fundamentalgleichung. □

Für die folgenden Betrachtungen benötigen wir noch eine Definition.

**Definition 4.2.5** Sei  $B$  ein Ring und  $A \subseteq B$  ein Unterring.  $x \in B$  heißt **ganz** über  $A$ , falls  $x$  Nullstelle eines normierten Polynoms mit Koeffizienten in  $A$  ist. Die Menge  $ic_B(A) := \{z \in B : z \text{ ist ganz über } A\}$  heißt **ganzer Abschluß** von  $A$  in  $B$ .  $A$  heißt **ganz abgeschlossen**, falls  $A = ic_{Q(A)}(A)$  gilt, wobei  $Q(A)$  den Quotientenkörper von  $A$  bezeichne.

Wir behandeln nun eine Methode, um alle Erweiterungen einer Stelle  $P \in \mathbb{P}_F$  in  $F'$  zu beschreiben. Dazu führen wir zunächst einige Schreibweisen ein:

$$\begin{aligned} \bar{F} &:= F_P, \text{ der Restklassenkörper von } P; \\ \bar{a} &:= a(P), \text{ die Restklasse von } a \in \mathcal{O}_P; \\ \text{für } \Psi(T) &= \sum c_i T^i \text{ ein Polynom mit Koeffizienten } c_i \in \mathcal{O}_P, \text{ sei} \end{aligned}$$

$$\bar{\Psi}(T) := \sum \bar{c}_i T^i \in \bar{F}[T].$$

**Satz 4.2.6 (Kummer)** Sei  $F' = F(y)$ , wobei  $y$  ganz über  $\mathcal{O}_P$  ist mit Minimalpolynom  $\varphi(T) \in \mathcal{O}_P[T]$ . Sei

$$\bar{\varphi}(T) = \prod_{i=1}^r \gamma_i(T)^{\varepsilon_i}$$

die Zerlegung von  $\bar{\varphi}$  in normierte, irreduzible Polynome über  $\bar{F}$ . Wählen wir normierte Polynome  $\varphi_i(T) \in \mathcal{O}_P[T]$  mit

$$\bar{\varphi}_i(T) = \gamma_i(T) \text{ und } \deg(\varphi_i(T)) = \deg(\gamma_i(T)).$$

Dann gilt:

(a) Für  $1 \leq i \leq r$  existieren paarweise verschiedene Stellen  $P_i \in \mathbb{P}_{F'}$  mit

$$P_i|P, \quad \varphi_i(y) \in P_i \text{ und } f(P_i|P) \geq \deg(\gamma_i(T)).$$

(b) Gilt  $\varepsilon_i = 1$  für alle  $i = 1, \dots, r$ , dann existiert für jedes  $i$  genau eine Stelle  $P_i|P$  mit  $\varphi_i(y) \in P_i$ . Diese Stellen sind alle Stellen, die über  $P$  liegen und es gilt

$$\text{Con}_{F'/F}(P) = \sum_{i=1}^r P_i.$$

Die Erweiterungen sind also unverzweigt. Weiters ist der Restklassenkörper  $F'_i$  isomorph zu  $\bar{F}[T]/(\gamma_i(T))$ , es gilt also  $f(P_i|P) = \deg(\gamma_i(T))$ .

*Beweis:* (a) Sei  $\bar{F}_i := \bar{F}[T]/(\gamma_i(T))$ .  $\bar{F}_i$  ist ein Erweiterungskörper von  $\bar{F}$  und es gilt  $[\bar{F}_i : \bar{F}] = \deg(\gamma_i(T))$ .

Sei  $\rho : \mathcal{O}_P[T] \rightarrow \mathcal{O}_P[y]$  der Auswertungshomomorphismus bei  $y$  und  $\pi_i : \mathcal{O}_P[T] \rightarrow \bar{F}_i$  die kanonische Restklassenabbildung. Wegen  $\ker(\rho) \subseteq \ker(\pi_i)$  ist die Abbildung  $\sigma_i := \pi_i \circ \rho^{-1}$  wohldefiniert und surjektiv. Wir haben

$$\begin{array}{ccc} \mathcal{O}_P[T] & & \\ \downarrow \rho & \searrow \pi_i & \\ \mathcal{O}_P[y] & \xrightarrow{\sigma_i} & \bar{F}_i \\ \downarrow \pi & \cong & \nearrow \\ \mathcal{O}_P[y]/(\ker(\sigma_i)) & & \end{array}$$

Nach Satz 2.1.19 existiert eine Stelle  $P_i \in \mathbb{P}_{F'}$  mit  $\ker(\sigma_i) \subseteq P_i$  und  $\mathcal{O}_P[y] \subseteq \mathcal{O}_{P_i}$ , also gilt  $P_i|P$  und  $\varphi_i(y) \in P_i$ .  $\mathcal{O}_{P_i}/P_i$  enthält  $\bar{F}_i \cong \mathcal{O}_P[y]/(\ker(\sigma_i))$ , also gilt

$$f(P_i|P) \geq [\bar{F}_i : \bar{F}] = \deg(\gamma_i(T)).$$

Für  $i \neq j$  sind die Polynome  $\gamma_i(T) = \bar{\varphi}_i(T)$  und  $\gamma_j(T) = \bar{\varphi}_j(T)$  relativ prim in  $\bar{F}[T]$ , also haben wir Polynome  $\lambda_i(T), \lambda_j(T) \in \mathcal{O}_P[T]$  mit

$$1 = \bar{\varphi}_i(T)\bar{\lambda}_i(T) + \bar{\varphi}_j(T)\bar{\lambda}_j(T).$$

Klarerweise gilt  $\varphi_i(y)\lambda_i(y) \in \ker(\sigma_i)$  und  $\varphi_j(y)\lambda_j(y) \in \ker(\sigma_j)$ , also gilt  $1 \in \ker(\sigma_i) + \ker(\sigma_j) \subseteq P_i + P_j$ . Das kann nur sein, wenn  $P_i \neq P_j$ .

(b) Nach Voraussetzung haben wir

$$\begin{aligned} [F' : F] &= \deg(\varphi(T)) = \sum_{i=1}^r \deg(\varphi_i(T)) \\ &\leq \sum_{i=1}^r f(P_i|P) \leq \sum_{i=1}^r e(P_i|P)f(P_i|P) \\ &\leq \sum_{P'|P} e(P'|P)f(P'|P) = [F' : F]. \end{aligned}$$

Daraus folgen alle Behauptungen sofort. □

### 4.3 Unterringe von Funktionenkörpern

Um in der Erweiterungstheorie weiterkommen zu können, müssen wir zunächst Unterringe von Funktionenkörpern studieren.

**Definition 4.3.1** *Ein Unterring eines Funktionenkörpers  $F/K$  ist ein Ring  $R$  mit  $K \subseteq R \subseteq F$ , wobei  $R$  kein Körper sein darf.*

Wir betrachten nun spezielle Unterringe:

**Definition 4.3.2** *Für  $\emptyset \neq S \subset \mathbb{P}_F$  sei*

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

*der Durchschnitt aller Bewertungsringe  $\mathcal{O}_P$  mit  $P \in S$ . Jeder Ring von dieser Form heißt **Holomorphierung** von  $F/K$ .*

Dass Holomorphieringe tatsächlich Unterringe sind ist noch zu zeigen:

**Lemma 4.3.3** *Sei  $F/K$  ein Funktionenkörper.*

- (a) *Jeder Bewertungsring  $\mathcal{O}_P$  ist ein Holomorphierung. Es gilt  $\mathcal{O}_P = \mathcal{O}_S$  mit  $S = \{P\}$ .*
- (b) *Jeder Holomorphierung  $\mathcal{O}_S$  ist ein Unterring von  $F/K$ .*

(c) Für  $P \in \mathbb{P}_F$  und  $\emptyset \neq S \subset \mathbb{P}_F$  gilt

$$\mathcal{O}_S \subseteq \mathcal{O}_P \Leftrightarrow P \in S.$$

Also gilt  $\mathcal{O}_S = \mathcal{O}_T \Leftrightarrow S = T$ .

*Beweis:* (a) ist klar!

(b) Wir müssen nur zeigen, dass  $\mathcal{O}_S$  kein Körper ist. Wählen wir nun eine beliebige Stelle  $P_1 \in S$ . Nach dem starken Approximationssatz existiert ein Element  $0 \neq x \in F$  mit

$$v_{P_1}(x) > 0 \text{ und } v_P(x) \geq 0 \text{ für alle } P \in S.$$

Wir verwenden hier, dass  $S \neq \mathbb{P}_F$ . Es gilt klarerweise  $x \in \mathcal{O}_S$  und  $x^{-1} \notin \mathcal{O}_S$ , also ist  $\mathcal{O}_S$  kein Körper.

(c) **Behauptung:** Sei  $P \notin S$ . Dann existiert ein  $z \in F$  mit

$$v_P(z) < 0 \text{ und } v_Q(z) \geq 0 \text{ für alle } Q \in S. \quad (4.4)$$

Falls  $S \cup \{P\} \neq \mathbb{P}_F$ , so braucht man nur den starken Approximationssatz anzuwenden. Gilt  $S \cup \{P\} = \mathbb{P}_F$ , so wählen wir ein  $z \in \mathcal{O}_S$  mit mindestens einer Nullstelle in  $S$ . Da  $z$  auch eine Polstelle haben muss, die nicht in  $S$  liegt, gilt  $v_P(z) < 0$ . Damit ist die Behauptung gezeigt.

Jedes Element, welches (4.4) erfüllt ist in  $\mathcal{O}_S$ , aber nicht in  $\mathcal{O}_P$ . Wir haben also gezeigt: aus  $P \notin S$  folgt  $\mathcal{O}_S \not\subseteq \mathcal{O}_P$ , und das beweist (c). □

**Proposition 4.3.4** Sei  $\mathcal{O}_S$  ein Holomorphiering von  $F/K$ . Dann gilt

(a)  $F$  ist der Quotientenkörper von  $\mathcal{O}_S$ .

(b)  $\mathcal{O}_S$  ist ganz abgeschlossen.

*Beweis:* (a) Sei  $x \in F \setminus \{0\}$ . Dann existiert nach dem starken Approximationssatz ein Element  $z \in F$  mit

$$v_P(z) \geq \max\{0, v_P(x^{-1})\} \text{ für alle } P \in S.$$

Klarerweise gilt dann  $z \in \mathcal{O}_S$  und  $y := xz \in \mathcal{O}_S$ , also ist  $x = yz^{-1}$  im Quotientenkörper von  $\mathcal{O}_S$ .

(b) Sei  $u \in F$  ganz über  $\mathcal{O}_S$ . Dann erfüllt  $u$  eine Gleichung der Form

$$u^n + a_{n-1}u^{n-1} + \cdots + a_0 = 0, \quad (4.5)$$

wobei alle Koeffizienten  $a_i$  in  $\mathcal{O}_S$  liegen. Wir zeigen, dass  $v_P(u) \geq 0$  für alle  $P \in S$ . Angenommen das wäre falsch, also  $v_P(u) < 0$  für ein  $P \in S$ . Dann hätten wir wegen  $v_P(a_i) \geq 0$

$$v_P(u^n) = nv_P(u) < v_P(a_i u^i) \text{ für } i = 0, \dots, n-1.$$

Mit der starken Dreiecksungleichung erhält man einen Widerspruch zu (4.5).

□

**Satz 4.3.5** Sei  $R$  ein Unterring von  $F/K$  und

$$S(R) := \{P \in \mathbb{P}_F : R \subseteq \mathcal{O}_P\}.$$

Dann gilt:

(a)  $\emptyset \neq S(R) \subset \mathbb{P}_F$ .

(b)  $ic_F(R) = \mathcal{O}_{S(R)}$ .

*Beweis:* (a) Da  $R$  kein Körper ist, gibt es ein nichttriviales Ideal  $I \subset R$  und nach Satz 2.1.19 existiert eine Stelle  $P \in \mathbb{P}_F$  mit  $I \subseteq P$  und  $R \subseteq \mathcal{O}_P$ . Daraus folgt  $S(R) \neq \emptyset$ . Betrachten wir andererseits ein Element  $x \in R$  welches transzendent über  $K$  ist. Jede Polstelle von  $x$  liegt nicht in  $S(R)$ , also gilt  $S(R) \neq \mathbb{P}_F$ .

(b)  $ic_F(R) \subseteq \mathcal{O}_{S(R)}$  ist klar. Wir zeigen die umgekehrte Inklusion.

**Behauptung:** Sei  $z \in \mathcal{O}_{S(R)}$ . Dann gilt

$$z^{-1} \cdot R[z^{-1}] = R[z^{-1}]. \quad (4.6)$$

Angenommen die Behauptung wäre falsch, dann wäre  $z^{-1} \cdot R[z^{-1}]$  ein echtes Ideal von  $R[z^{-1}]$ . Nach Satz 2.1.19 können wir eine Stelle  $Q \in \mathbb{P}_F$  finden mit

$$R[z^{-1}] \subseteq \mathcal{O}_Q \text{ und } z^{-1} \in Q.$$

Es folgt  $Q \in S(R)$  und  $z \notin \mathcal{O}_Q$ . Widerspruch!

Nach (4.6) haben wir eine Darstellung der Eins

$$1 = z^{-1} \cdot \sum_{i=0}^s a_i (z^{-1})^i \quad (4.7)$$

mit  $a_0, \dots, a_s \in R$ . Multipliziert man (4.7) mit  $z^{s+1}$ , so erhält man eine Ganzheitsgleichung für  $z$  über  $R$ .

□

**Korollar 4.3.6** *Ein Unterring  $R$  von  $F/K$  mit Quotientenkörper  $F$  ist ganz abgeschlossen genau dann, wenn  $R$  ein Holomorphiering ist.*

**Proposition 4.3.7** *Sei  $\mathcal{O}_S$  ein Holomorphiering von  $F/K$ . Dann existiert ein eindeutiger Zusammenhang zwischen  $S$  und der Menge von maximalen Idealen von  $\mathcal{O}_S$ , gegeben durch*

$$P \mapsto M_P := P \cap \mathcal{O}_S \quad (\text{für } P \in S).$$

*Darüber hinaus ist die Abbildung*

$$\varphi : \begin{cases} \mathcal{O}_S/M_P & \rightarrow F_P = \mathcal{O}_P/P \\ x + M_P & \mapsto x + P \end{cases}$$

*ein Isomorphismus.*

*Beweis:* Betrachten wir für ein  $P \in S$  den Ringhomomorphismus

$$\Phi : \begin{cases} \mathcal{O}_S & \rightarrow F_P \\ x & \mapsto x + P. \end{cases}$$

**Behauptung:**  $\Phi$  ist surjektiv.

Sei  $z + P \in F_P$  mit  $z \in \mathcal{O}_P$ . Nach dem starken Approximationssatz existiert ein  $x \in F$  mit

$$v_P(x - z) > 0 \text{ und } v_Q(x) \geq 0 \text{ für alle } Q \in S \setminus \{P\}.$$

$x$  liegt also in  $\mathcal{O}_S$  und  $\Phi(x) = z + P$ . Das beweist die Behauptung.

Der Kern von  $\Phi$  ist  $M_P$ , also ist  $\varphi$  ein Isomorphismus. Da  $F_P$  ein Körper ist, ist  $M_P$  ein maximales Ideal von  $\mathcal{O}_S$ . Mit Hilfe des starken Approximationssatzes kann man wie oben zeigen, dass  $M_P \neq M_Q$  für  $P \neq Q$  aus  $S$ .

Zu zeigen bleibt, dass jedes maximale Ideal von  $\mathcal{O}_S$  als  $P \cap \mathcal{O}_S$  geschrieben werden kann für ein  $P \in S$ . Sei also  $M$  ein maximales Ideal. Nach Satz 2.1.19 existiert eine Stelle  $P \in \mathcal{P}_F$  mit

$$M \subseteq P \text{ und } \mathcal{O}_S \subseteq \mathcal{O}_P.$$

Es gilt also  $P \in S$ . Da  $M \subseteq P \cap \mathcal{O}_S$  und  $M$  maximales Ideal ist, folgt  $M = P \cap \mathcal{O}_S$ .

□

**Definition 4.3.8** *Ein Ring  $R$  heißt **Dedekindring**, falls er*

- (i) *noethersch,*
- (ii) *ganz abgeschlossen, und*
- (ii) *von Dimension 1 ist, d.h. jedes Primideal von  $R$  ist maximal.*

**Lemma 4.3.9** Sei  $\emptyset \neq S \subset \mathbb{P}$ . Dann ist  $\mathcal{O}_S$  ein Dedekindring.

*Beweis:*  $\mathcal{O}_S$  ist ganz abgeschlossen wegen Korollar 4.3.6. Wir zeigen, dass die Lokalisierung bezüglich eines maximalen Ideals ein diskreter Bewertungsring ist. Sei ein maximales Ideal  $M_P = P \cap \mathcal{O}_S$  gegeben mit  $P \in S$ . Wir zeigen

$$(\mathcal{O}_S \setminus M_P)^{-1} \mathcal{O}_S = \mathcal{O}_P. \quad (4.8)$$

Sei  $z/u \in (\mathcal{O}_S \setminus M_P)^{-1} \mathcal{O}_S$ . Dann gilt  $v_P(z/u) = v_P(z) - v_P(u) = v_P(z) \geq 0$ , also  $z/u \in \mathcal{O}_P$ . Sei umgekehrt  $x \in \mathcal{O}_P$ . Nach dem starken Approximationssatz existiert ein  $u \in F$  mit  $v_P(u) = 0$  und  $v_Q(u) \geq \max\{0, -v_Q(x)\}$  für alle  $Q \in S \setminus \{P\}$ . Dann gilt aber  $u \notin P$ ,  $v_P(xu) = v_P(x) \geq 0$ , also  $xu \in \mathcal{O}_P$  und damit  $x = (xu)/u \in (\mathcal{O}_S \setminus M_P)^{-1} \mathcal{O}_S$ . Das beweist (4.8).

Sei nun  $0 \neq I \subset \mathcal{O}_S$  ein Primideal. Dann existiert ein  $P \in S$  mit  $I \subseteq M_P$  nach Satz 4.3.7. Es gilt

$$(\mathcal{O}_S \setminus M_P)^{-1} \mathcal{O}_S \subseteq (\mathcal{O}_S \setminus I)^{-1} \mathcal{O}_S, \quad (4.9)$$

und da  $(\mathcal{O}_S \setminus M_P)^{-1}$  ein Bewertungsring, und daher ein maximaler Unterring von  $F/K$  ist, gilt Gleichheit in (4.9). Daraus folgt  $I = M_P$ .

Zu zeigen bleibt, dass  $\mathcal{O}_S$  noethersch ist. Das folgt unmittelbar aus Lemma 9.4 in [9], und der Tatsache, dass jedes Element in  $F \setminus \{0\}$  nur endlich viele Nullstellen besitzt. □

Abschließend noch eine Proposition, die dem Leser, der mit Dedekindringen oder Riemannschen Flächen vertraut ist, nicht überraschend erscheinen wird:

**Proposition 4.3.10** Sei  $S \subseteq \mathbb{P}_F$  eine nichtleere endliche Menge von Stellen von  $F/K$ . Dann ist  $\mathcal{O}_S$  ein Hauptidealring.

*Beweis:* Sei  $S = \{P_1, \dots, P_s\}$  und  $\{0\} \neq I \subseteq \mathcal{O}_S$  ein Ideal von  $\mathcal{O}_S$ . Für  $i = 1, \dots, s$  wählen wir  $x_i \in I$  mit

$$v_{P_i}(x_i) =: n_i \leq v_{P_i}(u) \text{ für alle } u \in I.$$

Nach dem Approximationssatz können wir  $z_i \in F$  finden mit

$$v_{P_i}(z_i) = 0 \text{ und } v_{P_j}(z_i) > n_j \text{ für alle } j \neq i.$$

Offensichtlich ist  $z_i \in \mathcal{O}_S$ , also gilt  $x := \sum_{i=1}^s x_i z_i \in I$ . Nach der starken Dreiecksungleichung gilt  $v_{P_i}(x) = n_i$  für  $i = 1, \dots, s$ . Wir wollen zeigen, dass  $I \subseteq x\mathcal{O}_S$ . Die umgekehrte Inklusion ist ja trivial, da  $x \in I$ . Betrachten wir ein Element  $z \in I$ . Setze  $y := x^{-1}z$ , dann gilt

$$v_{P_i}(y) = v_{P_i}(z) - n_i \geq 0 \text{ für } i = 1, \dots, s.$$

Also gilt  $y \in \mathcal{O}_S$  und damit  $z \in x\mathcal{O}_S$ . □

## 4.4 Lokale Ganzheitsbasen

In diesem Abschnitt wollen wir den Begriff der lokalen Ganzheitsbasis einführen. Wir verwenden hier einige Eigenschaften der Spurabbildung, sie können in jedem Algebrabuch nachgelesen werden (z.B. in [27]). Der (einfache) Beweis des folgenden Lemmas findet sich in [27].

**Lemma 4.4.1** *Sei  $Tr_{F'/F}$  die Spurabbildung der Erweiterung  $F'/F$ ,  $R$  ein ganz abgeschlossener Unterring von  $F/K$  mit  $Q(R) = F$ , und  $z \in ic_{F'}(R)$ . Dann gilt  $Tr_{F'/F}(z) \in R$ .*

**Satz 4.4.2** *Sei  $R$  ein ganz abgeschlossener Unterring von  $F/K$  mit Quotientenkörper  $F$  und  $F'/K'$  eine endliche, separable Erweiterung von Grad  $n$ . Sei  $R' = ic_{F'}(R)$ . Dann gilt:*

- (a) *Für jede Basis  $\{x_1, \dots, x_n\}$  von  $F'/F$  existieren Elemente  $a_i \in R \setminus \{0\}$  mit  $a_1x_1, \dots, a_nx_n \in R'$ . Es gibt also Basen von  $F'/F$ , die in  $R'$  enthalten sind.*
- (b) *Sei  $\{z_1, \dots, z_n\} \subseteq R'$  eine Basis von  $F'/F$  und  $\{z_1^*, \dots, z_n^*\}$  die duale Basis bezüglich der Spurabbildung der Erweiterung  $F'/F$ . Dann gilt*

$$\sum_{i=1}^n Rz_i \subseteq R' \subseteq \sum_{i=1}^n Rz_i^*.$$

- (c) *Sei  $R$  zusätzlich ein Hauptidealring. Dann existiert eine Basis  $\{u_1, \dots, u_n\}$  von  $F'/F$  mit*

$$R' = \sum_{i=1}^n Ru_i.$$

*Beweis:* (a) ist ein bekanntes Resultat aus der algebraischen Zahlentheorie (siehe z.B. [27], Kapitel VII, Prop. 1.1).

- (b) Jedes  $z \in F'$  kann dargestellt werden als

$$z = e_1z_1^* + \dots + e_nz_n^* \text{ mit } e_i \in F.$$

Falls  $z \in R'$  ist, dann ist  $zz_j \in R'$  für  $j = 1, \dots, n$ , und daher gilt  $Tr_{F'/F}(zz_j) \in R$  wegen Lemma 4.4.1. Es gilt

$$Tr_{F'/F}(zz_j) = Tr_{F'/F} \left( \sum_{i=1}^n e_iz_jz_i^* \right) = e_j,$$

also  $e_j \in R$ , daher gilt  $R' \subseteq \sum_{i=1}^n Rz_i^*$ .

(c) Wähle eine Basis  $\{w_1, \dots, w_n\}$  von  $F'/F$  mit  $R' \subseteq \sum_{i=1}^n R w_i$  (nach (b) ist das möglich). Setzen wir für  $1 \leq k \leq n$

$$R_k := R' \cap \sum_{i=1}^k R w_i.$$

Wir konstruieren induktiv  $u_1, \dots, u_n$  mit  $R_k = \sum_{i=1}^k R u_i$ . Sei  $k = 1$ . Dann ist  $R_1 = R' \cap R w_1$ . Wir setzen

$$I_1 := \{a \in F : a w_1 \in R'\}.$$

Da  $R' \subseteq \sum_{i=1}^n R w_i$ , gilt  $I_1 \subseteq R$ .  $I_1$  ist sogar ein Ideal von  $R$ , also gilt  $I = a_1 R$  für ein  $a_1 \in R$ . Setzen wir  $u_1 := a_1 w_1$ , so erhalten wir  $R_1 = R u_1$ .

Sei  $k \geq 2$  und  $u_1, \dots, u_{k-1}$  mit  $R_{k-1} = \sum_{i=1}^{k-1} R u_i$ . Sei

$$I_k := \{a \in F : \text{es existieren } b_1, \dots, b_{k-1} \in R \\ \text{mit } b_1 w_1 + \dots + b_{k-1} w_{k-1} + a w_k \in R'\}.$$

$I_k$  ist ein Ideal von  $R$ , also  $I_k = a_k R$ . Wähle  $u_k \in R'$  mit

$$u_k = c_1 w_1 + \dots + c_{k-1} w_{k-1} + a_k w_k.$$

Klarerweise gilt  $R_k \supseteq \sum_{i=1}^k R u_i$ . Um die umgekehrte Inklusion zu zeigen, wählen wir ein  $w \in R_k$ , also

$$w = d_1 w_1 + \dots + d_k w_k \text{ mit } d_i \in R.$$

Dann gilt  $d_k \in I_k$ , also  $d_k = d a_k$  mit  $d \in R$  und

$$w - d a_k \in R' \cap \sum_{i=1}^{k-1} R w_i = R_{k-1} = \sum_{i=1}^{k-1} R u_i.$$

Also gilt  $w \in \sum_{i=1}^k R u_i$ . Wir haben gezeigt, dass  $R' = \sum_{i=1}^n R u_i$ . Da nach (a) eine Basis von  $F'/F$  existiert, die in  $R'$  liegt, sind die Elemente  $u_1, \dots, u_n$  linear unabhängig über  $F$  und damit bilden sie eine Basis von  $F'/F$ .

□

**Korollar 4.4.3** Sei  $F'/F$  eine endliche, separable Erweiterung von  $F/K$  und  $P \in \mathbb{P}_F$ . Sei  $\mathcal{O}'_P := i_{F'}(\mathcal{O}_P)$ . Dann gilt

$$\mathcal{O}'_P = \bigcap_{P'|P} \mathcal{O}_{P'}.$$

Es existiert eine Basis  $\{u_1, \dots, u_n\}$  von  $F'/F$  mit

$$\mathcal{O}'_P = \sum_{i=1}^n \mathcal{O}_P \cdot u_i.$$

Eine solche Basis heißt **Ganzheitsbasis** von  $\mathcal{O}'_P$  über  $\mathcal{O}_P$  (oder auch **lokale Ganzheitsbasis** von  $F'/F$  für die Stelle  $P$ ).

*Beweis:* Wenn man sich den Beweis von Satz 4.3.5 ansieht, dann merkt man, dass nirgends verwendet wird, dass  $K$  der volle Konstantenkörper ist. Wir betrachten also den Funktionenkörper  $F'/K$  und wenden Satz 4.3.5 an. Daraus folgt die erste Behauptung. Die zweite ist eine unmittelbare Folgerung aus dem Satz 4.4.2 (c), weil  $\mathcal{O}_P$  ein Hauptidealring ist.

□

Das folgende Korollar zeigt, dass lokale Ganzheitsbasen nicht nur existieren, sondern dass jede Basis fast überall eine lokale Ganzheitsbasis ist.

**Korollar 4.4.4** *Sei  $F/K$  ein Funktionenkörper,  $F'/F$  eine endliche, separable Erweiterung und  $\{z_1, \dots, z_n\}$  irgendeine Basis von  $F'/F$ . Dann ist  $\{z_1, \dots, z_n\}$  eine lokale Ganzheitsbasis für fast alle  $P \in \mathbb{P}_F$ .*

*Beweis:* Betrachten wir die duale Basis  $\{z_1^*, \dots, z_n^*\}$ . Die Menge der Koeffizienten der Minimalpolynome von  $z_1, \dots, z_n, z_1^*, \dots, z_n^*$  ist endlich. Sei  $S \subseteq \mathbb{P}_F$  die Menge aller Pole dieser Koeffizienten. Dann ist  $S$  endlich und für  $P \notin S$  gilt

$$z_1, \dots, z_n, z_1^*, \dots, z_n^* \in \mathcal{O}'_P,$$

mit  $\mathcal{O}'_P = i_{C_{F'}}(\mathcal{O}_P)$ . Also gilt

$$\sum_{i=1}^n \mathcal{O}_P z_i \subseteq \mathcal{O}'_P \subseteq \sum_{i=1}^n \mathcal{O}_P z_i^* \subseteq \mathcal{O}'_P \subseteq \sum_{i=1}^n \mathcal{O}_P z_i$$

wegen Satz 4.4.2 (b) und der Tatsache, dass  $\{z_1, \dots, z_n\}$  die Dualbasis von  $\{z_1^*, \dots, z_n^*\}$  ist.

□

An dieser Stelle erwähnen wir noch einen Zusatz zum Satz von Kummer. Da dieses Resultat im Folgenden nicht benötigt wird, verzichten wir auf den Beweis (siehe [38] Kaptitel III.3).

**Satz 4.4.5** *Voraussetzungen wie in Satz 4.2.6. Gelte weiters, dass  $\{1, y, \dots, y^{n-1}\}$  eine lokale Ganzheitsbasis bei  $P$  ist. Dann sind  $P_1, \dots, P_r$  wie in Satz 4.2.6 (b) die einzigen Stellen, die über  $P$  liegen, und es gilt*

$$\text{Con}_{F'/F}(P) = \sum_{i=1}^r \varepsilon_i P_i.$$

*Ausserdem ist  $F'_P$  isomorph zu  $\overline{F}[T]/(\gamma_i(T))$ , also gilt  $f(P_i|P) = \deg(\gamma_i(T))$ .*

## 4.5 Die Cospur

Wir betrachten in diesem Abschnitt nur endliche, separable Erweiterungen  $F'/K'$  von  $F/K$ . Wir wollen jedem Weil Differential von  $F/K$  ein Weil Differential von  $F'/K'$  zuordnen. Damit werden wir eine sehr nützliche Formel für das Geschlecht von  $F'$  herleiten, die Hurwitzsche Geschlechtsformel. Zuerst müssen wir aber noch den Begriff der Differente einführen. Da die Erweiterung  $F'/F$  separabel ist, ist die Spurabbildung nicht identisch Null.

**Definition 4.5.1** Für  $P \in \mathbb{P}_F$ , sei wie zuvor  $\mathcal{O}'_P = i_{C_{F'}}(\mathcal{O}_P)$ . Dann heißt die Menge

$$\mathcal{C}_P := \{z \in F : \text{Tr}_{F'/F}(z \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P\}$$

**Komplementärmodul** über  $\mathcal{O}_P$ .

**Proposition 4.5.2** Es gilt

- (a)  $\mathcal{C}_P$  ist ein  $\mathcal{O}'_P$ -Modul, und  $\mathcal{O}'_P \subseteq \mathcal{C}_P$ .  
 (b) Sei  $\{z_1, \dots, z_n\}$  eine Ganzheitsbasis von  $F'/F$  über  $\mathcal{O}_P$ . Dann gilt

$$\mathcal{C}_P = \sum_{i=1}^n \mathcal{O}_P \cdot z_i^*.$$

- (c) Es existiert ein Element  $t \in F'$  (abhängig von  $P$ ) mit  $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ . Für dieses Element gilt

$$v_{P'}(t) \leq 0 \text{ für alle } P' | P,$$

und für  $t' \in F'$  gilt

$$\mathcal{C}_P = t' \cdot \mathcal{O}'_P \Leftrightarrow v_{P'}(t') = v_{P'}(t) \text{ für alle } P' | P.$$

- (d)  $\mathcal{C}_P = \mathcal{O}'_P$  für fast alle  $P \in \mathbb{P}_F$ .

*Beweis:* (a) folgt unmittelbar aus Lemma 4.4.1.

(b) Betrachten wir zuerst ein Element  $z \in \mathcal{C}_P$ . Da  $\{z_1^*, \dots, z_n^*\}$  eine Basis von  $F'/F$  ist, gibt es  $x_1, \dots, x_n \in F$  mit  $z = \sum_{i=1}^n x_i z_i^*$ . Da  $z \in \mathcal{C}_P$  und  $z_1, \dots, z_n \in \mathcal{O}'_P$ , gilt  $x_j = \text{Tr}_{F'/F}(z z_j) \in \mathcal{O}_P$  für  $1 \leq j \leq n$ . Es gilt also  $z \in \sum_{i=1}^n \mathcal{O}_P z_i^*$ . Sei umgekehrt  $z \in \sum_{i=1}^n \mathcal{O}_P z_i^*$  und  $u \in \mathcal{O}'_P$ . Schreiben wir  $z = \sum_{i=1}^n x_i z_i^*$  und  $u = \sum_{j=1}^n y_j z_j$  mit  $x_i, y_j \in \mathcal{O}_P$ . Dann gilt  $\sum_{i=1}^n x_i y_i = \text{Tr}_{F'/F}(zu) \in \mathcal{O}_P$ , also  $z \in \mathcal{C}_P$ .

(c) Nach (b) wissen wir, dass  $\mathcal{C}_P = \sum_{i=1}^n \mathcal{O}_P u_i$  mit gewissen  $u_i \in F'$ . Wählen wir ein  $x \in F$  mit

$$v_P(x) \geq 0 \text{ und } v_{P'}(x) \geq -v_{P'}(u_i)$$

für alle  $P'|P$  und  $i = 1, \dots, n$ . Daraus folgt sofort  $x \cdot \mathcal{C}_P \subseteq \mathcal{O}'_P$ . Wie man leicht sieht, ist  $x \cdot \mathcal{C}_P$  ein Ideal von  $\mathcal{O}'_P$  und nach Proposition 4.3.10 ein Hauptideal. Es gilt also  $x \cdot \mathcal{C}_P = y \cdot \mathcal{O}'_P$ . Setzen wir  $t := x^{-1}y$ , so erhalten wir  $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ . Da  $\mathcal{O}'_P \subseteq \mathcal{C}_P$ , gilt  $v_{P'}(t) \leq 0$  für alle  $P'|P$ . Schlussendlich haben wir

$$\begin{aligned} t \cdot \mathcal{O}'_P &= t' \cdot \mathcal{O}'_P \\ \Leftrightarrow tt'^{-1} &\in \mathcal{O}'_P \text{ und } t^{-1}t' \in \mathcal{O}'_P \\ \Leftrightarrow v_{P'}(tt'^{-1}) &\geq 0 \text{ und } v_{P'}(t^{-1}t') \geq 0 \text{ für alle } P'|P \\ \Leftrightarrow v_{P'}(t) &= v_{P'}(t') \text{ für alle } P'|P. \end{aligned}$$

(d) Sei  $\{z_1, \dots, z_n\}$  eine Basis von  $F'/F$ .  $\{z_1, \dots, z_n\}$  und  $\{z_1^*, \dots, z_n^*\}$  sind für fast alle  $P$  eine lokale Ganzheitsbasis. Aus (b) folgt dann, dass  $\mathcal{C}_P = \mathcal{O}'_P$  für fast alle  $P$ .

□

**Definition 4.5.3** Betrachten wir eine Stelle  $P \in \mathbb{P}_F$  und den ganzen Abschluss  $\mathcal{O}'_P$  in  $F'$ . Sei  $\mathcal{C}_P = t \cdot \mathcal{O}'_P$  der Komplementärmodul über  $\mathcal{O}_P$ . Dann definieren wir für  $P'|P$  den **Differenzenexponenten** von  $P'$  über  $P$  durch

$$d(P'|P) := -v_{P'}(t).$$

Nach der obigen Proposition macht diese Definition Sinn und es gilt  $d(P'|P) \geq 0$ . Weiters gilt, da  $\mathcal{C}_P = 1 \cdot \mathcal{O}'_P$  für fast alle  $P$ , dass  $d(P'|P) = 0$  ist, für fast alle  $P \in \mathbb{P}_F$  und  $P'|P$ . Wir können daher den Divisor

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

definieren. Dieser Divisor heißt **Differente** von  $F'/F$ .

**Lemma 4.5.4** Für  $z \in F'$  gilt

$$z \in \mathcal{C}_P \Leftrightarrow v_{P'}(z) \geq -d(P'|P) \text{ für alle } P'|P.$$

Ausserdem gilt  $\text{Diff}(F'/F) \geq 0$ .

*Beweis:*  $\text{Diff}(F'/F) \geq 0$  ist klar. Aus  $\mathcal{C}_P = t \cdot \bigcap_{P'|P} \mathcal{O}'_{P'}$  folgt sofort die andere Behauptung.

□

**Definition 4.5.5** Sei

$$\mathcal{A}_{F'/F} := \{\alpha \in \mathcal{A}_{F'} : \alpha_{P'} = \alpha_{Q'} \text{ falls } P' \cap F = Q' \cap F\}.$$

Wir dehnen die Spurabbildung  $Tr_{F'/F}$  auf eine Abbildung  $\mathcal{A}_{F'/F} \rightarrow \mathcal{A}_F$  aus, vermöge

$$(Tr_{F'/F}(\alpha))_P := Tr_{F'/F}(\alpha_{P'}) \text{ für } \alpha \in \mathcal{A}_{F'/F},$$

wobei  $P'|P$  gilt.

Für einen Divisor  $A' \in \mathcal{D}_{F'}$ , setzen wir

$$\mathcal{A}_{F'/F}(A') := \mathcal{A}_{F'}(A') \cap \mathcal{A}_{F'/F}.$$

Dass  $Tr_{F'/F} : \mathcal{A}_{F'/F} \rightarrow \mathcal{A}_F$  wohldefiniert ist, zeigt das folgende Lemma:

**Lemma 4.5.6**  $Tr_{F'/F}(\alpha) \in \mathcal{A}_F$  für  $\alpha \in \mathcal{A}_{F'/F}$ . Die Spur eines Hauptadeles von  $z \in F'$  ist das Hauptadele von  $Tr_{F'/F}(z)$ .

*Beweis:* Es gilt  $\alpha_{P'} \in \mathcal{O}_{P'}$  für fast alle  $P' \in \mathbb{P}_{F'}$ . Da ja der ganze Abschluss von  $\mathcal{O}_P$  gleich  $\bigcap_{P'|P} \mathcal{O}_{P'}$  ist, gilt  $Tr_{F'/F}(\alpha_{P'}) \in \mathcal{O}_P$  für fast alle  $P \in \mathbb{P}_F$ , also erhalten wir ein Adele von  $F/K$ . Die zweite Aussage ist trivial. □

Wir sind nun in der Lage, jedem Weil Differential auf  $F/K$  ein spezielles Weil Differential auf  $F'/K'$  zuzuordnen zu können, die sogenannte **Cospur**.

**Satz 4.5.7** Für jedes Weil Differential  $\omega$  auf  $F/K$  existiert ein eindeutig bestimmtes Weil Differential  $\omega'$  auf  $F'/K'$  mit

$$Tr_{K'/K}(\omega'(\alpha)) = \omega(Tr_{F'/F}(\alpha)) \quad (4.10)$$

für alle  $\alpha \in \mathcal{A}_{F'/F}$ . Dieses Weil Differential heißt **Cospur** von  $\omega$  in  $F'/F$ , und wird mit  $Cotr_{F'/F}(\omega)$  bezeichnet. Falls  $\omega \neq 0$  und  $(\omega) \in \mathcal{D}_F$  der Divisor von  $\omega$  ist, dann gilt

$$(Cotr_{F'/F}(\omega)) = Con_{F'/F}((\omega)) + Diff(F'/F). \quad (4.11)$$

Um diesen Satz beweisen zu können, benötigen wir zwei Lemmata:

**Lemma 4.5.8** Für jedes  $C' \in \mathcal{D}_{F'}$  gilt  $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(C')$ .

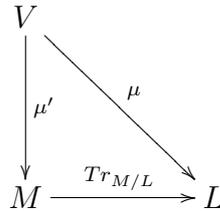
*Beweis:* Sei  $\alpha = (\alpha_{P'})_{P' \in \mathbb{P}_{F'}}$  ein Adele von  $F'$ . Nach dem Approximationssatz existiert für alle  $P \in \mathbb{P}_F$  ein Element  $x_P \in F'$  mit

$$v_{P'}(\alpha_{P'} - x_P) \geq -v_P(C') \text{ für alle } P'|P.$$

Setzen wir nun  $\beta = (\beta_{P'})_{P' \in \mathbb{P}_{F'}}$  mit  $\beta_{P'} := x_P$  für  $P'|P$ . Dann gilt  $\beta \in \mathcal{A}_{F'/F}$  und  $\alpha - \beta \in \mathcal{A}_{F'}(C')$  und daher  $\alpha \in \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(C')$ .

□

**Lemma 4.5.9 (Liftungslemma)** *Sei  $M/L$  eine endliche, seperable Körpererweiterung,  $V$  ein  $M$ -Vektorraum und  $\mu : V \rightarrow L$  eine  $L$ -lineare Abbildung. Dann existiert eine eindeutig bestimmte  $M$ -lineare Abbildung  $\mu' : V \rightarrow M$  mit  $Tr_{M/L} \circ \mu' = \mu$ .*



*Beweis:* Betrachten wir den Raum  $M^*$  der  $L$ -Linearformen auf  $M$ . Dann ist  $M^*$  ein eindimensionaler  $M$ -Vektorraum, wenn man  $(z \cdot \lambda)(w) := \lambda(z \cdot w)$  definiert. Definieren wir für  $v \in V$  die Abbildung  $\lambda_v : M \rightarrow L$  durch  $\lambda_v(a) := \mu(av)$ . Diese Abbildung ist  $L$ -linear, es existiert also ein Element  $z_v \in M$  mit  $\lambda_v = z_v \cdot Tr_{M/L}$ . Man prüft leicht nach, dass  $\mu'(v) := z_v$  das Gewünschte leistet.

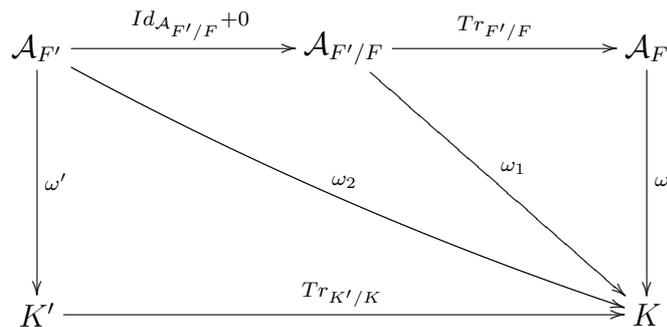
□

Nun können wir uns an den Beweis von Satz 4.5.7 machen.

*Beweis von Satz 4.5.7:* Sei

$$W' := Con_{F'/F}(\omega) + Diff(F'/F).$$

Nach Lemma 4.5.8 gilt  $\mathcal{A}_{F'} = \mathcal{A}_{F'/F} + \mathcal{A}_{F'}(W')$ .



Die Strategie des Beweises ist nach der Graphik klar. Man muss nur noch nachrechnen, dass man damit auch wirklich Weil Differentiale erhält und dass die Gleichung (4.11) gilt.

**Schritt 1:** Wir definieren  $\omega_1$  in naheliegender Weise Als  $\omega_1 = \omega \circ Tr_{F'/F}$ . Dann gilt:

(a<sub>1</sub>)  $\omega_1(\alpha) = 0$  für  $\alpha \in \mathcal{A}_{F'/F}(W') + F'$ .

(b<sub>1</sub>) Sei  $B' \in \mathcal{D}_{F'}$  mit  $B' \not\leq W'$ . Dann existiert ein  $\beta \in \mathcal{A}_{F'/F}(B')$  mit  $\omega_1(\beta) \neq 0$ .

*Beweis von Schritt 1:* (a<sub>1</sub>):  $\omega_1$  verschwindet klarerweise auf  $F'$ , da  $\omega$  auf  $F$  verschwindet. Um zu beweisen, dass  $\omega_1(\alpha) = 0$  für alle  $\alpha \in \mathcal{A}_{F'}(W')$ , genügt es zu zeigen, dass für alle  $P \in \mathbb{P}_F$  und alle  $P'|P$  gilt, dass

$$v_P(\text{Tr}_{F'/F}(\alpha_{P'})) \geq -v_P(\omega). \quad (4.12)$$

Wählen wir ein Element  $x \in F$  mit  $v_P(x) = v_P(\omega)$ . Dann gilt

$$\begin{aligned} v_{P'}(x\alpha_{P'}) &= v_{P'}(x) + v_{P'}(\alpha_{P'}) \geq e(P'|P)v_P(\omega) - v_{P'}(W') \\ &= v_{P'}(\text{Con}_{F'/F}((\omega)) - W') = -v_{P'}(\text{Diff}(F'/F)) = -d(P'|P). \end{aligned}$$

Daher gilt  $x\alpha_{P'} \in \mathcal{C}_P$  und daher  $v_P(\text{Tr}_{F'/F}(x\alpha_{P'})) \geq 0$ . Es gilt  $\text{Tr}_{F'/F}(x\alpha_{P'}) = x \cdot \text{Tr}_{F'/F}(\alpha_{P'})$  und  $v_P(x) = v_P(\omega)$  und daraus folgt (4.12).

(b<sub>1</sub>): Wir haben also einen Divisor  $B'$  gegeben mit  $B' \not\leq W'$ . Daher existiert eine Stelle  $P_0 \in \mathbb{P}_F$  mit

$$v_{P^*}(\text{Con}_{F'/F}((\omega)) - B') < -d(P^*|P_0) \quad (4.13)$$

für ein  $P^*|P_0$ . Betrachten wir die Menge

$$J := \{z \in F' : v_{P^*}(z) \geq v_{P^*}(\text{Con}_{F'/F}((\omega)) - B') \text{ für alle } P^*|P_0\}.$$

Nach dem Approximationssatz existiert ein Element  $u \in J$  mit

$$v_{P^*}(u) = v_{P^*}(\text{Con}_{F'/F}((\omega)) - B') \text{ für alle } P^*|P_0.$$

Nach Lemma 4.5.4 liegt  $u$  nicht in  $\mathcal{C}_{P_0}$ . Da  $J \cdot \mathcal{O}'_{P_0} \subseteq J$ , haben wir

$$\text{Tr}_{F'/F}(J) \not\subseteq \mathcal{O}_{P_0}. \quad (4.14)$$

Wählen wir nun ein  $t \in F$  mit  $v_{P_0}(t) = 1$ . Nach der Definition von  $J$  existiert ein  $r \geq 0$  mit  $t^r \cdot J \subseteq \mathcal{O}'_{P_0}$ , also gilt

$$t^r \cdot \text{Tr}_{F'/F}(J) = \text{Tr}_{F'/F}(t^r \cdot J) \subseteq \mathcal{O}_{P_0}.$$

$t^r \cdot \text{Tr}_{F'/F}(J)$  ist ein Ideal von  $\mathcal{O}_{P_0}$ , also gibt es ein  $s \geq 0$  mit  $t^r \cdot \text{Tr}_{F'/F}(J) = t^s \cdot \mathcal{O}_{P_0}$ . Wir haben also  $\text{Tr}_{F'/F}(J) = t^m \cdot \mathcal{O}_{P_0}$  für ein  $m \in \mathbb{Z}$ . Wegen (4.14) gilt  $m \leq -1$ , daher gilt

$$t^{-1} \cdot \mathcal{O}_{P_0} \subseteq \text{Tr}_{F'/F}(J). \quad (4.15)$$

Nach Proposition 2.9.3 (a) können wir ein Element  $x \in F$  finden mit

$$v_{P_0}(x) = -v_{P_0}(\omega) - 1 \text{ und } \omega_{P_0}(x) \neq 0. \quad (4.16)$$

Wir wählen  $y \in F$  mit  $v_{P_0}(y) = v_{P_0}(\omega)$ , also  $xy \in t^{-1} \cdot \mathcal{O}_{P_0}$ . Nach (4.15) gibt es ein  $z \in J$  mit  $Tr_{F'/F}(z) = xy$ . Wir definieren uns ein Adele  $\beta \in \mathcal{A}_{F'/F}$  durch

$$\beta_{P'} := \begin{cases} 0 & \text{für } P' \nmid P_0 \\ y^{-1}z & \text{für } P' | P_0 \end{cases}$$

Aus der Definition von  $J$  folgt für  $P' | P_0$

$$\begin{aligned} v_{P'}(\beta) &= -v_{P'}(y) + v_{P'}(z) \\ &\geq -v_{P'}(\text{Con}_{F'/F}(\omega)) + v_{P'}(\text{Con}_{F'/F}(\omega) - B') \\ &= -v_{P'}(B'). \end{aligned}$$

Also gilt  $\beta \in \mathcal{A}_{F'/F}(B')$ . Ausserdem haben wir  $\omega_1(\beta) = \omega(Tr_{F'/F}(\beta)) = \omega_{P_0}(x) \neq 0$  wegen (4.16). Das beweist  $(b_1)$ .

**Schritt 2:** Wir definieren  $\omega_2 : \mathcal{A}_{F'} \rightarrow K$  wie folgt. Für  $\alpha \in \mathcal{A}_{F'}$  existieren nach Lemma 4.5.8 Adele  $\beta \in \mathcal{A}_{F'/F}$  und  $\gamma \in \mathcal{A}_{F'}(W')$  mit  $\alpha = \beta + \gamma$ . Wir setzen

$$\omega_2(\alpha) := \omega_1(\beta).$$

$\omega_2$  ist damit wohldefiniert; sei  $\alpha = \beta_1 + \gamma_1$  eine andere Darstellung, so gilt

$$\beta_1 - \beta = \gamma - \gamma_1 \in \mathcal{A}_{F'/F} \cap \mathcal{A}_{F'}(W') = \mathcal{A}_{F'/F}(W').$$

Nach  $(a_1)$  gilt also  $\omega_1(\beta) - \omega_1(\beta_1) = 0$ . Das einzige Problem ist jetzt noch, dass  $K'$  nicht gleich  $K$  ist. Dazu haben wir das Liftungslemma:

**Schritt 3:** Nach dem Liftungslemma gibt es eine  $K'$ -lineare Abbildung  $\omega' : \mathcal{A}_{F'} \rightarrow K'$  mit  $Tr_{K'/K} \circ \omega' = \omega_2$ . Daraus folgt unmittelbar (4.10). Zu zeigen bleibt noch:

$$(a_3) \quad \omega'(\alpha) = 0 \text{ für } \alpha \in \mathcal{A}_{F'/F}(W') + F'.$$

$$(b_3) \quad \text{Sei } B' \in \mathcal{D}_{F'} \text{ nicht kleiner als } W', \text{ dann existiert ein Adele } \beta \in \mathcal{A}_{F'}(B') \text{ mit } \omega'(\beta) \neq 0.$$

Ad  $(a_3)$ : Da  $\omega'$   $K'$ -linear ist, ist das Bild von  $\mathcal{A}_{F'}(W') + F'$  entweder 0 oder ganz  $K'$ . In letzterem Fall gibt es ein  $\alpha \in \mathcal{A}_{F'}(W')$  mit  $Tr_{K'/K}(\omega'(\alpha)) \neq 0$ , da die Spurabbildung  $Tr_{K'/K}$  nicht verschwindet. Damit gilt aber  $\omega_2(\alpha) \neq 0$  und das ist ein Widerspruch.

Ad  $(b_3)$ : Wir wissen schon nach Schritt 2, dass ein  $\beta \in \mathcal{A}_{F'}(B')$  existiert mit  $\omega_2(\beta) \neq 0$ . Also gilt  $Tr_{K'/K}(\omega'(\beta)) \neq 0$  und das zeigt die Behauptung.

Damit haben wir die Existenz von  $\omega'$  gezeigt. Es bleibt noch die Eindeutigkeit:

Nehmen wir also an, wir hätten ein  $\omega^* \in \Omega_{F'}$  mit der Eigenschaft (4.10). Setzen wir  $\nu := \omega^* - \omega'$ , so erhalten wir

$$\text{Tr}_{K'/K}(\nu(\alpha)) = 0 \text{ für alle } \alpha \in \mathcal{A}_{F'/F}. \quad (4.17)$$

Da  $\nu$  ein Weil Differential ist, existiert ein Divisor  $C' \in \mathcal{D}_{F'}$  mit der Eigenschaft, dass  $\nu$  auf  $\mathcal{A}_{F'}(C')$  verschwindet. Aus Lemma 4.5.8 folgt  $\text{Tr}_{K'/K}(\nu(\alpha)) = 0$  für alle  $\alpha \in \mathcal{A}_{F'}$ . Daraus folgt  $\nu = 0$ , also  $\omega^* = \omega'$ . □

Wir beweisen noch einige Eigenschaften der Cospur.

**Proposition 4.5.10**

(a) Seien  $\omega, \omega_1$  und  $\omega_2$  Weil Differentiale von  $F/K$  und sei  $x \in F$ . Dann gilt

$$\text{Cotr}_{F'/F}(\omega_1 + \omega_2) = \text{Cotr}_{F'/F}(\omega_1) + \text{Cotr}_{F'/F}(\omega_2)$$

und

$$\text{Cotr}_{F'/F}(x\omega) = x\text{Cotr}_{F'/F}(\omega).$$

(b) Sei  $F''/F'$  eine weitere endliche, separable Erweiterung. Dann gilt

$$\text{Cotr}_{F''/F}(\omega) = \text{Cotr}_{F''/F'}(\text{Cotr}_{F'/F}(\omega))$$

für jedes  $\omega \in \Omega_F$ .

*Beweis:* Wegen der Eindeutigkeitsaussage in Satz 4.5.7 genügt es zu zeigen, dass die der Gleichung (4.10) entsprechenden Relationen erfüllt sind. Das rechnet man aber unmittelbar nach. □

**Korollar 4.5.11** Sei ein Turm  $F'' \supseteq F' \supseteq F$  von endlichen, separablen Funktionenkörpererweiterungen gegeben. Dann gilt:

(a)  $\text{Diff}(F''/F) = \text{Con}_{F''/F'}(\text{Diff}(F'/F)) + \text{Diff}(F''/F')$ .

(b)  $d(P''|P) = e(P''|P')d(P'|P) + d(P''|P')$ , falls  $P''|P'|P$ .

*Beweis:* (b) ist nur eine Umformulierung von (a). Wir beweisen also nur (a):

Wählen wir ein Weil Differential  $\omega \in \Omega_F \setminus \{0\}$ . Dann gilt

$$(\text{Cotr}_{F''/F}(\omega)) = \text{Con}_{F''/F}(\omega) + \text{Diff}(F''/F).$$

Andererseits gilt

$$\begin{aligned} (\text{Cotr}_{F''/F}(\omega)) &= (\text{Cotr}_{F''/F'}(\text{Cotr}_{F'/F}(\omega))) \\ &= \text{Con}_{F''/F'}(\omega) + \text{Con}_{F''/F'}(\text{Diff}(F'/F)) + \text{Diff}(F''/F'). \end{aligned}$$

Hier haben wir die Transitivität der Conorm benützt. Vergleicht man die beiden Darstellungen von  $(\text{Cotr}_{F''/F}(\omega))$ , so erhält man die Behauptung.

□

Wir zeigen noch eine sehr wichtige Folgerung aus Satz 4.5.7, die **Hurwitzsche Geschlechtsformel**:

**Satz 4.5.12** *Sei  $F/K$  ein Funktionenkörper vom Geschlecht  $g$  und  $F'/F$  eine endliche, separable Erweiterung. Sei  $K'$  der Konstantenkörper von  $F'$  und  $g'$  das Geschlecht von  $F'/K'$ . Dann gilt*

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

*Beweis:* Wählen wir ein Weil Differential  $\omega \neq 0$  auf  $F/K$ . Nach Satz 4.5.7 gilt

$$(\text{Cotr}_{F'/F}(\omega)) = \text{Con}_{F'/F}(\omega) + \text{Diff}(F'/F).$$

Der Grad eines kanonischen Divisors in  $F/K$  bzw.  $F'/K'$  ist  $2g - 2$  bzw.  $2g' - 2$ , also haben wir

$$\begin{aligned} 2g' - 2 &= \deg(\text{Con}_{F'/F}(\omega)) + \deg(\text{Diff}(F'/F)) \\ &= \frac{[F' : F]}{[K' : K]}(2g - 2) + \deg(\text{Diff}(F'/F)) \end{aligned}$$

wegen Korollar 4.2.4.

□

## 4.6 Die Differente

Wir haben nun mit der Hurwitzschen Geschlechtsformel ein gutes Werkzeug zur Hand, um das Geschlecht einer endlichen, separablen Erweiterung zu bestimmen. Etwas fehlt uns dabei aber noch: Wir haben bisher keine Methode kennengelernt, wie man die Differente explizit berechnet. Diesem Problem widmet sich dieser Abschnitt.

Wir beginnen mit dem zentralen Resultat dieses Abschnitts, der **Dedekindschen Differenzenformel**.

**Satz 4.6.1** *Es gilt für alle  $P'|P$ :*

- (a)  $d(P'|P) \geq e(P'|P) - 1$ .
- (b)  $d(P'|P) = e(P'|P) - 1$  genau dann, wenn  $\text{char}(K) \nmid e(P'|P)$  (z.B. wenn  $\text{char}(K) = 0$ ).

Um diesen Satz zu beweisen, benötigen wir Einiges an Vorarbeit:

**Lemma 4.6.2** Sei  $F^*/F$  eine algebraische Funktionenkörpererweiterung,  $P \in \mathbb{P}_F$  und  $P^* \in \mathbb{P}_{F^*}$  mit  $P^*|P$ . Betrachten wir einen Automorphismus  $\sigma$  von  $F^*/F$ . Dann ist  $\sigma(P^*) := \{\sigma(z) : z \in P^*\}$  eine Stelle von  $F^*$  und es gilt

$$(a) \quad v_{\sigma(P^*)}(y) = v_{P^*}(\sigma^{-1}(y)) \text{ für alle } y \in F^*.$$

$$(b) \quad \sigma(P^*)|P.$$

$$(c) \quad e(\sigma(P^*)|P) = e(P^*|P) \text{ und } f(\sigma(P^*)|P) = f(P^*|P).$$

*Beweis:*  $\sigma(\mathcal{O}_{P^*})$  ist klarerweise ein Bewertungsring von  $F'/K'$  und  $\sigma(P^*)$  sein maximales Ideal. Ist  $t^*$  ein primitives Element von  $P^*$ , so ist  $\sigma(t^*)$  ein primes Element von  $\sigma(P^*)$ .

(a) Sei  $0 \neq y \in F^*$  und  $y = \sigma(z)$ . Schreiben wir  $z = (t^*)^r \cdot u$  mit  $u \in (\mathcal{O}_{P^*})^*$ , dann ist  $\sigma(u) \in (\mathcal{O}_{\sigma(P^*)})^*$  und  $y = \sigma(t^*)^r \cdot \sigma(u)$ , also ist  $v_{P^*}(z) = v_{\sigma(P^*)}(y)$ .

(b) klar, da  $\sigma(P) = P$ .

(c) Die Aussage über die Verzweigungsindizes ist klar. Jeder Automorphismus  $\sigma$  induziert einen Isomorphismus  $\bar{\sigma} : F_{P^*}^* \rightarrow F_{\sigma(P^*)}^*$ , vermöge

$$\bar{\sigma}(z + P^*) := \sigma(z) + \sigma(P^*).$$

Daraus folgt die Aussage über die relativen Grade. □

Nun sind wir in der Lage Satz 4.6.1 (a) zu zeigen:

*Beweis von Satz 4.6.1 (a):* Wir müssen zeigen, dass

$$\text{Tr}_{F'/F}(t \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P \tag{4.18}$$

für alle  $t \in F'$  mit

$$v_{P'}(t) = 1 - e(P'|P) \text{ für alle } P'|P. \tag{4.19}$$

Betrachten wir eine endliche Galoiserweiterung  $F^*$  von  $F$  mit  $F \subseteq F' \subseteq F^*$ . Wählen wir nun  $n := [F' : F]$  Automorphismen  $\sigma_1, \dots, \sigma_n$  von  $F^*/F$  die, auf  $F'$  eingeschränkt, paarweise verschieden sind. Wir haben für  $z \in \mathcal{O}'_P$

$$\text{Tr}_{F'/F}(t \cdot z) = \sum_{i=1}^n \sigma_i(t \cdot z). \tag{4.20}$$

Sei  $P^*$  irgendeine Stelle von  $F^*$ , die über  $P$  liegt und setzen wir  $P_i^* := \sigma_i^{-1}(P^*)$  und  $P'_i := P_i^* \cap F'$ .  $\sigma_i(z)$  ist ganz über  $\mathcal{O}_P$ , da  $z \in \mathcal{O}'_P$ . Also gilt  $v_{P^*}(\sigma_i(z)) \geq 0$ . Wir erhalten

$$v_{P^*}(\sigma_i(t \cdot z)) = v_{P^*}(\sigma_i(t)) + v_{P^*}(\sigma_i(z))$$

$$\begin{aligned}
&\geq v_{P^*}(\sigma_i(t)) = v_{P_i^*}(t) \\
&= e(P_i^*|P_i')(1 - e(P_i'|P)) \\
&> -e(P_i^*|P_i')e(P_i'|P) = -e(P_i^*|P) \\
&= -e(P^*|P).
\end{aligned}$$

Wir haben das vorige Lemma und die Voraussetzung (4.19) benützt. Nun sehen wir mit (4.20)

$$-e(P^*|P) < v_{P^*}(Tr_{F'/F}(t \cdot z)) = e(P^*|P) \cdot v_P(Tr_{F'/F}(t \cdot z)).$$

Daher gilt  $v_P(Tr_{F'/F}(t \cdot z)) \geq 0$  und (4.18) folgt. □

Um Satz 4.6.1 (b) beweisen zu können, brauchen wir das folgende Lemma:

**Lemma 4.6.3** *Sei  $P \in \mathbb{P}_P$  und seien  $P_1, \dots, P_r \in \mathbb{P}_{F'}$  alle Erweiterungen von  $P$  in  $F'/F$ . Betrachten wir die Restklassenkörper  $k := \mathcal{O}_P/P$  bzw.  $k_i := \mathcal{O}_{P_i}/P_i \supseteq k$  und die dazugehörigen kanonischen Restklassenabbildungen  $\pi : \mathcal{O}_P \rightarrow k$  bzw.  $\pi_i : \mathcal{O}_{P_i} \rightarrow k_i$  ( $i=1, \dots, r$ ). Dann gilt für jedes  $u \in \mathcal{O}'_P$*

$$\pi(Tr_{F'/F}(u)) = \sum_{i=1}^r e(P_i|P) \cdot Tr_{k_i/k}(\pi_i(u)).$$

*Beweis von Satz 4.6.1 (b):* Wir behalten die Notation von Lemma 4.6.3 bei und wir schreiben abkürzend  $e_i := e(P_i|P)$ . Sei  $P'|P$  und  $e := (P'|P)$ . Wir wollen zeigen, dass

$$d(P'|P) = e - 1 \Leftrightarrow \text{char}(K) \nmid e. \quad (4.21)$$

Wir zeigen zuerst die Implikation von Rechts nach Links. Gelte also  $\text{char}(K) \nmid e$ . Angenommen  $d(P'|P) \geq e$ . Dann existiere ein  $w \in F'$  mit

$$v_{P'}(w) \leq -e \text{ und } Tr_{F'/F}(w \cdot \mathcal{O}'_P) \subseteq \mathcal{O}_P. \quad (4.22)$$

Da  $K$  vollkommen ist, ist die Erweiterung  $k_1/k$  separabel und wir können ein  $y_0 \in \mathcal{O}_{P'}$  finden mit  $Tr_{k_1/k}(\pi_1(y_0)) \neq 0$ . Nach dem Approximationssatz existiert ein Element  $y \in F'$  mit

$$v_{P'}(y - y_0) > 0$$

und

$$v_{P_i}(y) \geq \max\{1, e_i + v_{P_i}(w)\} \text{ für } 2 \leq i \leq r. \quad (4.23)$$

Daraus folgt  $y \in \mathcal{O}'_P$ , und nach Lemma 4.6.3 gilt

$$\pi(Tr_{F'/F}(y)) = e \cdot Tr_{k_1/k}(\pi_1(y)) + \sum_{i=2}^r e_i \cdot Tr_{k_i/k}(\pi_i(y))$$

$$= e \cdot \text{Tr}_{k_1/k}(\pi_1(y)) \neq 0.$$

Hier verwenden wir, dass  $\text{char}(K) \nmid e$ . Wir erhalten

$$v_P(\text{Tr}_{F'/F}(y)) = 0.$$

Wählen wir nun ein  $x \in F$  mit  $v_P(x) = 1$ . Dann gilt

$$\text{Tr}_{F'/F}(x^{-1}y) = x^{-1} \cdot \text{Tr}_{F'/F}(y) \notin \mathcal{O}_P. \quad (4.24)$$

Andererseits gilt  $x^{-1}yw^{-1} \in \mathcal{O}'_P$ , da

$$v_{P'}(x^{-1}yw^{-1}) = -e + v_{P'}(y) - v_{P'}(w) \geq 0$$

und

$$v_{P_i}(x^{-1}yw^{-1}) = v_{P_i}(y) - (e_i + v_{P_i}(w)) \geq 0, \quad i = 2, \dots, r,$$

nach (4.22) und (4.23). Also gilt  $x^{-1}y \in w \cdot \mathcal{O}'_P$  und  $\text{Tr}_{F'/F}(x^{-1}y) \in \mathcal{O}_P$  nach (4.22), was ein Widerspruch zu (4.24) ist. Wir haben damit also die Implikation von Rechts nach Links gezeigt.

Wir zeigen noch die Implikation von Links nach Rechts von (4.21). Nehmen wir also an  $\text{char}(K) \mid e$  und zeigen, dass dann  $d(P'|P) \geq e$ . Wähle  $u \in F'$  mit

$$v_{P'}(u) = -e \text{ und } v_{P_i}(u) \geq -e_i + 1 \quad (i = 2, \dots, r). \quad (4.25)$$

Sei  $x \in F$  ein  $P$ -primes Element. Für jedes  $z \in \mathcal{O}'_P$  gilt

$$v_{P'}(xuz) \geq 0 \text{ und } v_{P_i}(xuz) > 0$$

für  $i = 2, \dots, r$ . Also ist  $xuz \in \mathcal{O}'_P$  und nach Lemma 4.6.3 gilt

$$\begin{aligned} \pi(\text{Tr}_{F'/F}(xuz)) &= e \cdot \text{Tr}_{k_1/k}(\pi_1(xuz)) + \sum_{i=2}^r e_i \cdot \text{Tr}_{k_i/k}(\pi_i(xuz)) \\ &= e \cdot \text{Tr}_{k_1/k}(\pi_1(xuz)) = 0. \end{aligned}$$

Daraus folgern wir, dass  $x \cdot \text{Tr}_{F'/F}(uz) \in P = x \cdot \mathcal{O}_P$ , also  $\text{Tr}_{F'/F}(uz) \in \mathcal{O}_P$  für jedes  $z \in \mathcal{O}'_P$ . Das impliziert  $u \in \mathcal{C}_P$  und  $-e = v_{P'}(u) \geq -d(P'|P)$  wegen (4.25).

□

*Beweis von Lemma 4.6.3:* Wie man zeigen kann, gilt  $\text{Tr}_{F'/F}(u)$  ist die Spur der  $F$ -linearen Abbildung  $\mu : F' \rightarrow F'$ , definiert durch  $\mu(z) := u \cdot z$  (siehe Appendix A in [38], oder [1]).

Sei  $t$  ein primes Element von  $P$ . Wir versehen  $V := \mathcal{O}'_P/t\mathcal{O}'_P$  mit einer  $k$ -Vektorraumstruktur vermöge der Skalarmultiplikation

$$(x + P) \cdot (z + t\mathcal{O}'_P) := xz + t\mathcal{O}'_P \quad (x \in \mathcal{O}_P, z \in \mathcal{O}'_P).$$

Wählen wir eine Ganzheitsbasis  $\{z_1, \dots, z_n\}$  von  $\mathcal{O}'_P$  über  $\mathcal{O}_P$ ,  $n = [F' : F]$ . Dann ist  $\{z_1 + t\mathcal{O}'_P, \dots, z_n + t\mathcal{O}'_P\}$  eine Basis von  $V$  über  $k$ , also gilt  $\dim_k(V) = n$ . Definieren wir eine  $k$ -lineare Abbildung  $\bar{\mu} : V \rightarrow V$  durch

$$\bar{\mu}(z + t\mathcal{O}'_P) := u \cdot z + t\mathcal{O}'_P. \quad (4.26)$$

Sei  $A = (a_{ij})$  die Koordinatenmatrix von  $\mu$  bezüglich  $\{z_1, \dots, z_n\}$ . Da  $u \in \mathcal{O}'_P$  und  $\{z_1, \dots, z_n\}$  Ganzheitsbasis ist, sind die Koeffizienten  $a_{ij} \in \mathcal{O}_P$ .  $\bar{A} := (\pi(a_{ij}))$  ist die Koordinatenmatrix von  $\bar{\mu}$  bezüglich  $\{z_1 + t\mathcal{O}'_P, \dots, z_n + t\mathcal{O}'_P\}$ , und daher

$$\pi(\text{Tr}_{F'/F}(u)) = \pi(\text{Tr}(A)) = \text{Tr}(\bar{A}) = \text{Tr}(\bar{\mu}). \quad (4.27)$$

Wir definieren für  $1 \leq i \leq r$  die Faktorräume  $V_i := \mathcal{O}_{P_i}/P_i^{e_i}$  und die Abbildungen  $\mu_i : V_i \rightarrow V_i$  durch

$$\mu_i(z + P_i^{e_i}) := u \cdot z + P_i^{e_i}.$$

Wir versehen  $V_i$  in derselben Art wie  $V$  mit einer  $k$ -Vektorraumstruktur. Bezüglich dieser Struktur sind die Abbildungen  $\mu_i$  linear. Nun existiert ein kanonischer Isomorphismus

$$f : V \rightarrow \bigoplus_{i=1}^r V_i,$$

gegeben durch

$$f(z + t\mathcal{O}'_P) := (z + P_1^{e_1}, \dots, z + P_r^{e_r}).$$

Nach dem Approximationssatz ist  $f$  surjektiv.  $f$  ist auch injektiv: nehmen wir an  $f(z + t\mathcal{O}'_P) = 0$ . Dann gilt  $v_{P_i}(z) \geq e_i$ , also  $v_{P_i}(z \cdot t^{-1}) \geq 0$  für  $i = 1, \dots, r$ . Das impliziert  $z \cdot t^{-1} \in \mathcal{O}'_P$ , also  $z \in t\mathcal{O}'_P$  (nur nebenbei bemerkt: Diese Isomorphie würde auch aus der Zerlegung der Ideale  $P$  in Primideale im Dedekindring  $\mathcal{O}'_P$  und dem Chinesischen Restsatz folgen). Wir haben ein kommutatives Diagramm:

$$\begin{array}{ccc} V & \xrightarrow{\bar{\mu}} & V \\ \downarrow f & & \downarrow f \\ \bigoplus_{i=1}^r V_i & \xrightarrow{(\mu_1, \dots, \mu_n)} & \bigoplus_{i=1}^r V_i \end{array}$$

Nach (4.27) gilt daher

$$\pi(\text{Tr}_{F'/F}(u)) = \sum_{i=1}^r \text{Tr}(\mu_i). \quad (4.28)$$

Wir müssen jetzt nur noch zeigen, dass

$$\text{Tr}(\mu_i) = e_i \cdot \text{Tr}_{k_i/k}(\pi_i(u)).$$

Betrachten wir die Kette von  $k$ -Unterräumen

$$V_i = V_i^{(0)} \supseteq V_i^{(1)} \supseteq \dots \supseteq V_i^{(e_i)} = 0,$$

mit  $V_i^{(j)} := P_i^j / P_i^{e_i} \subseteq V_i$ . Diese Räume sind invariant unter  $\mu_i$ , also induziert  $\mu_i$  lineare Abbildungen

$$\sigma_{ij} : \begin{cases} V_i^{(j)} / V_i^{(j+1)} & \rightarrow V_i^{(j)} / V_i^{(j+1)} \\ [z + P_i^{e_i}] & \mapsto [u \cdot z + P_i^{e_i}] \end{cases}, \quad j = 0, \dots, e_i - 1.$$

$[z + P_i^{e_i}]$  bezeichnet dabei die Restklasse in  $V_i^{(j)} / V_i^{(j+1)}$ . Man sieht leicht, dass

$$\text{Tr}(\mu_i) = \sum_{j=0}^{e_i-1} \text{Tr}(\sigma_{ij}). \quad (4.29)$$

Wir wissen, dass

$$\text{Tr}_{k_i/k}(\pi_i(u)) = \text{Tr}(\gamma_i) \quad (4.30)$$

wobei  $\gamma_i$  die  $k$ -lineare Abbildung von  $k_i$  auf  $k_i$  ist, die durch  $\gamma_i(z + P_i) := u \cdot z + P_i$  definiert ist. Wir konstruieren nun für  $1 \leq j < e_i - 1$  einen  $k$ -Vektorraumisomorphismus  $h : k_i \rightarrow V_i^{(j)} / V_i^{(j+1)}$ , sodass das folgende Diagramm kommutiert:

$$\begin{array}{ccc} k_i & \xrightarrow{\gamma_i} & k_i \\ \downarrow h & & \downarrow h \\ V_i^{(j)} / V_i^{(j+1)} & \xrightarrow{\sigma_{ij}} & V_i^{(j)} / V_i^{(j+1)} \end{array}$$

Aus diesem Diagramm folgt  $\text{Tr}(\gamma_i) = \text{Tr}(\sigma_{ij})$  und daraus folgt dann das Lemma aus (4.29) und (4.30).

$h$  ist wie folgt definiert: Sei  $t_i \in F'$  ein primes Element von  $P_i$ . Dann definieren wir

$$h(z + P_i) := [t_i^j z + P_i^{e_i}].$$

Dass  $h$  wohldefiniert und ein Isomorphismus ist, rechnet man leicht nach.

□

Wir können nun Verzweigungen genauer charakterisieren.

**Definition 4.6.4** Sei  $F'/F$  eine algebraische Funktionenkörpererweiterung und  $P \in \mathbb{P}_F$ .

- (a) Eine verzweigte Erweiterung  $P'|P$  heißt **zahm verzweigt**, falls  $\text{char}(K) \nmid e(P'|P)$ .  
Andernfalls heißt  $P'|P$  **wild verzweigt**.
- (b)  $P$  heißt **verzweigt** in  $F'/F$ , falls ein  $P'|P$  existiert, sodass  $P'|P$  verzweigt ist.  
Andernfalls heißt  $P$  **unverzweigt**.
- (c) Eine verzweigte Stelle  $P$  heißt **zahm verzweigt**, falls alle Erweiterungen  $P'|P$  zahm sind. Andernfalls heißt  $P$  **wild verzweigt**.
- (d)  $P$  heißt **total verzweigt**, falls nur eine Stelle  $P'$  über  $P$  liegt und  $e(P'|P) = [F' : F]$  gilt.
- (e)  $F'/F$  heißt **verzweigt**, falls zumindest eine Stelle verzweigt ist.
- (f)  $F'/F$  heißt **zahm**, falls keine Stelle wild verzweigt ist.

Das nächste Korollar ist eine unmittelbare Folgerung aus der Dedekindschen Differentenformel.

**Korollar 4.6.5** Sei  $F'/F$  eine endliche, separable Funktionenkörpererweiterung.

- (a) Sei  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$ . Dann ist  $P'|P$  genau dann verzweigt, wenn  $P' \leq \text{Diff}(F'/F)$  gilt.  
Falls  $P'|P$  verzweigt ist, gilt

$$d(P'|P) = e(P'|P) - 1 \Leftrightarrow P'|P \text{ ist zahm verzweigt,}$$

$$d(P'|P) \geq e(P'|P) \Leftrightarrow P'|P \text{ ist wild verzweigt.}$$

- (b) Fast alle Stellen sind unverzweigt in  $F'/F$ .

Es folgt noch ein nützliches Korollar aus der Dedekindschen Differentenformel und der Hurwitzschen Geschlechtsformel.

**Korollar 4.6.6** Sei  $F'/F$  eine endliche, separable Funktionenkörpererweiterung mit gleichem Konstantenkörper  $K$ . Sei  $g$  das Geschlecht von  $F/K$  und  $g'$  das Geschlecht von  $F'/K$ . Dann gilt

$$(a) \quad 2g' - 2 \geq [F' : F](2g - 2) + \sum_{P \in \mathbb{P}_F} \sum_{P'|P} (e(P'|P) - 1) \deg(P').$$

$$(b) \quad g \leq g'.$$

Wir wollen uns noch eine andere Art überlegen, wie man die Differente abschätzen kann.

**Satz 4.6.7** Sei  $F' = F(y)$  eine endliche, separable Funktionenkörpererweiterung vom Grad  $[F' : F] =: n$ . Sei  $P \in \mathbb{P}_F$ , sodass  $y$  ganz über  $\mathcal{O}_P$  ist und  $\varphi(T) \in \mathcal{O}_P[T]$  das Minimalpolynom von  $y$ . Seien  $P_1, \dots, P_r \in \mathbb{P}_{F'}$  alle Stellen, die über  $P$  liegen. Dann gilt

$$(a) \quad d(P_i|P) \leq v_{P_i}(\varphi'(y)) \text{ für } 1 \leq i \leq r.$$

(b)  $\{1, \dots, y^r\}$  ist eine lokale Ganzheitsbasis bei  $P$  genau dann, wenn in (a) Gleichheit gilt.

Um diesen Satz zu beweisen, benötigen wir zunächst zwei Lemmata. Definitionsgemäss läßt sich das Polynom  $\varphi(T)$  in  $F'$  als

$$\varphi(T) = (T - y)(c_{n-1}T^{n-1} + \dots + c_1T + c_0),$$

mit  $c_{n-1} = 1$  faktorisieren. Es gilt

**Lemma 4.6.8**  $\{\frac{c_0}{\varphi'(y)}, \dots, \frac{c_{n-1}}{\varphi'(y)}\}$  ist die duale Basis zu  $\{1, y, \dots, y^{n-1}\}$ .

*Beweis:* Betrachten wir die  $n$  Einbettungen  $\sigma_1, \dots, \sigma_n$  von  $F'/F$  in einen algebraischen Abschluss  $\Phi$  von  $F$ . Setzen wir  $y_j = \sigma_j(y)$ , so erhalten wir

$$\varphi(T) = \prod_{j=1}^n (T - y_j).$$

Ableiten und  $T = y_\nu$  setzen ergibt

$$\varphi'(y_\nu) = \prod_{j \neq \nu} (y_\nu - y_j).$$

Betrachten wir nun für  $0 \leq l \leq n - 1$  die Polynome

$$\varphi_l(T) := \left( \sum_{j=1}^n \frac{\varphi(T)}{T - y_j} \cdot \frac{y_j^l}{\varphi'(y_j)} \right) - T^l \in \Phi[T].$$

Klarerweise ist  $\varphi_l(y_\nu) = 0$  für  $\nu = 1, \dots, n$  und daher ist  $\varphi_l(T)$  das Nullpolynom für alle  $l = 0, \dots, n - 1$ . Es gilt also

$$T^l = \sum_{j=1}^n \frac{\varphi(T)}{T - y_j} \cdot \frac{y_j^l}{\varphi'(y_j)} \text{ für } 0 \leq l \leq n - 1.$$

Indem wir  $\sigma_i(T) = T$  setzen, dehnen wir nun die Einbettungen  $\sigma_i$  auf Abbildungen  $\sigma_i : F'(T) \rightarrow \Phi(T)$  aus. Wir erhalten

$$\begin{aligned} T^l &= \sum_{j=1}^n \sigma_j \left( \frac{\varphi(T)}{T-y} \cdot \frac{y^l}{\varphi'(y)} \right) \\ &= \sum_{j=1}^n \sigma_j \left( \sum_{i=0}^{n-1} c_i T^i \cdot \frac{y^l}{\varphi'(y)} \right) \\ &= \sum_{i=0}^{n-1} \text{Tr}_{F'/F} \left( \frac{c_i}{\varphi'(y)} \cdot y^l \right) T^i. \end{aligned}$$

Koeffizientenvergleich liefert die gewünschte Aussage. □

**Lemma 4.6.9** *Es gilt*

- (a)  $c_j \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i$  für  $j = 0, \dots, n-1$ .
- (b)  $y^j \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i$  für  $j = 0, \dots, n-1$ .

*Beweis:* (a) Sei

$$\varphi(T) = T^n + a_{n-1}T^{n-1} + \dots + a_1T + a_0$$

mit  $a_i \in \mathcal{O}_P$ . Definitionsgemäß haben wir die folgende Rekursionsformel:

$$c_{n-1} = 1, \quad c_0 y = -a_0, \quad \text{und } c_i y = c_{i-1} - a_i \text{ für } 1 \leq i \leq n-1. \quad (4.31)$$

Die Aussage (a) gilt klarerweise für  $j = n-1$ . Angenommen es gilt also für ein  $j \in \{1, \dots, n-1\}$

$$c_j = \sum_{i=0}^{n-1} s_i y^i \text{ mit } s_i \in \mathcal{O}_P.$$

Dann erhalten wir aus (4.31)

$$\begin{aligned} c_{j-1} &= a_j + c_j y = a_j + \sum_{i=0}^{n-2} s_i y^{i+1} + s_{n-1} y^n \\ &= a_j + \sum_{i=0}^{n-2} s_i y^{i+1} - s_{n-1} \sum_{i=0}^{n-1} a_i y^i \in \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i. \end{aligned}$$

Induktive Anwendung des obigen Arguments liefert (a).

(b) Wir gehen ähnlich vor, wie beim Beweis von (a). Diesmal gilt die Aussage offensichtlich für  $j = 0$ . Angenommen es gilt für ein  $j \geq 0$

$$y^j = \sum_{i=0}^{n-1} r_i c_i \text{ mit } r_i \in \mathcal{O}_P.$$

Wenden wir (4.31) an, so erhalten wir

$$\begin{aligned} y^{j+1} &= \sum_{i=0}^{n-1} r_i c_i y = \sum_{i=1}^{n-1} r_i (c_{i-1} - a_i) - r_0 a_0 \\ &= \sum_{i=0}^{n-2} r_{i+1} c_i - \left( \sum_{i=0}^{n-1} r_i a_i \right) \cdot c_{n-1} \in \sum_{i=0}^n \mathcal{O}_P \cdot c_i. \end{aligned}$$

□

Nun können wir uns an den Beweis von Satz 4.6.7 machen:

*Beweis von Satz 4.6.7:* (a) Wir bezeichnen wieder mit  $\mathcal{O}'_P$  den ganzen Abschluss von  $\mathcal{O}_P$  in  $F'$ . Wir müssen zeigen, dass die folgende Aussage gilt:

$$z \in \mathcal{C}_P \Rightarrow v_{P_i}(z) \geq -v_{P_i}(\varphi'(y)) \text{ für } i = 1, \dots, r.$$

$z \in \mathcal{C}_P$  kann geschrieben werden als

$$z = \sum_{i=0}^{n-1} r_i \cdot \frac{c_i}{\varphi'(y)} \text{ mit } r_i \in F.$$

Da  $y^l$  ganz über  $\mathcal{O}_P$  und  $z \in \mathcal{C}_P$  ist, gilt  $Tr_{F'/F}(z \cdot y^l) \in \mathcal{O}_P$ . Aufgrund von Lemma 4.6.8 gilt

$$Tr_{F'/F}(z \cdot y^l) = r_l \in \mathcal{O}_P.$$

Aus Lemma 4.6.9 (a) folgt nun

$$z = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} r_i c_i \in \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i \subseteq \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P.$$

Das beweist die Behauptung.

(b) Nach Lemma 4.6.9 wissen wir, dass

$$\sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i = \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i.$$

Sei nun  $\{1, \dots, y^{n-1}\}$  eine Ganzheitsbasis bei  $P$ . Es folgt

$$\begin{aligned} \mathcal{C}_P &= \sum_{i=0}^{n-1} \mathcal{O}_P \cdot \frac{c_i}{\varphi'(y)} = \frac{1}{\varphi'(y)} \cdot \sum_{i=0}^{n-1} \mathcal{O}_P \cdot c_i \\ &= \frac{1}{\varphi'(y)} \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i = \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P. \end{aligned}$$

Das beweist

$$d(P_i|P) = v_{P_i}(\varphi'(y)) \text{ für } i = 1, \dots, r. \quad (4.32)$$

Wir müssen noch zeigen, dass umgekehrt aus (4.32) folgt, dass  $\{1, \dots, y^{n-1}\}$  eine Ganzheitsbasis bei  $P$  ist. Dabei müssen wir nur zeigen, dass

$$\mathcal{O}'_P \subseteq \sum_{i=0}^{n-1} \mathcal{O}_P \cdot y^i.$$

Die umgekehrte Inklusion ist ja trivial. Sei also  $z \in \mathcal{O}'_P$ . Wir können  $z$  schreiben als

$$z = \sum_{i=0}^{n-1} t_i y^i \text{ mit } t_i \in F.$$

Wegen Lemma 4.6.9 (a) gilt  $c_j \in \mathcal{O}'_P$  und nach Voraussetzung gilt  $\mathcal{C}_P = \frac{1}{\varphi'(y)} \cdot \mathcal{O}'_P$ , also folgt

$$t_j = \text{Tr}_{F'/F} \left( \frac{1}{\varphi'(y)} \cdot c_j \cdot z \right) \in \mathcal{O}_P.$$

Das beweist den Satz. □

**Proposition 4.6.10** *Sei  $F'/F$  eine endliche separable Erweiterung von Funktionenkörpern,  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$ . Sei  $P'|P$  total verzweigt (also  $e(P'|P) = [F' : F] =: n$ ) und  $t \in F'$  ein primes Element von  $P'$  mit Minimalpolynom  $\varphi(T) \in F[T]$  über  $F$ . Dann gilt  $d(P'|P) = v_{P'}(\varphi'(t))$  und  $\{1, t, \dots, t^{n-1}\}$  ist eine Ganzheitsbasis von  $F'/F$  bei  $P$ .*

*Beweis:* Zuerst zeigen wir, dass  $\{1, t, \dots, t^{n-1}\}$  linear unabhängig über  $F$  ist. Angenommen wir hätten eine Linearkombination

$$\sum_{i=0}^{n-1} r_i t^i = 0 \text{ mit } r_i \in F, \text{ nicht alle } r_i = 0.$$

Für  $r_i \neq 0$  gilt

$$v_{P'}(r_i t^i) = v_{P'}(t^i) + e(P'|P) \cdot v_P(r_i) \equiv i \pmod{n}.$$

Also gilt  $v_{P'}(r_i t^i) \neq v_{P'}(r_j t^j)$  für  $i \neq j$  und  $r_i \neq 0$ ,  $r_j \neq 0$ . Die Starke Dreiecksungleichung impliziert

$$v_{P'} \left( \sum_{i=0}^{n-1} r_i t^i \right) = \min\{v_{P'}(r_i t^i) : r_i \neq 0\} < \infty,$$

und das ist ein Widerspruch.  $\{1, t, \dots, t^{n-1}\}$  ist also eine Basis von  $F'/F$ . Aus der Hilbertschen Fundamentalformel folgt, dass  $P'$  die einzige Stelle ist, die über  $P$  liegt, also gilt  $i_{CF'}(\mathcal{O}_P) = \mathcal{O}_{P'}$ . Wir wollen zeigen, dass

$$\mathcal{O}_{P'} = \sum_{i=0}^{n-1} \mathcal{O}_P \cdot t^i.$$

Sei  $z \in \mathcal{O}_{P'}$  und schreiben wir

$$z = \sum_{i=0}^{n-1} x_i t^i \text{ mit } x_i \in F.$$

Dann gilt mit dem obigen Argument  $0 \leq v_{P'}(z) = \min\{n \cdot v_P(x_i) + i : 0 \leq i \leq n-1\}$ , also muß  $v_P(x_i) \geq 0$  sein, und die Behauptung folgt. Die Aussage über den Differentenindex folgt aus dem vorigen Satz.

□

## 4.7 Konstantenkörpererweiterungen

Im folgenden versuchen wir Konstantenkörpererweiterungen genauer zu verstehen. In diesem Kapitel ist es nun erstmals unerlässlich, einen vollkommenen Konstantenkörper  $K$  zu fordern. Wie immer bezeichne  $\Phi \supseteq F$  einen algebraischen Abschluss von  $F$ .

Sei  $K' \supseteq K$  eine algebraische Körpererweiterung (mit  $K' \subseteq \Phi$ ). Dann ist  $F' := FK'$  ein Funktionenkörper über  $K'$  und daher ist sein Konstantenkörper eine endliche Erweiterung von  $K'$ . Wir wissen allerdings a priori nicht, ob  $K'$  schon der volle Konstantenkörper ist. Mit dieser Frage beschäftigen wir uns zunächst.

Zuerst aber ein einfaches Lemma.

**Lemma 4.7.1** *Sei  $\alpha \in \Phi$  algebraisch über  $K$ . Dann gilt  $[K(\alpha) : K] = [F(\alpha) : F]$ .*

*Beweis:*  $[F(\alpha) : F] \leq [K(\alpha) : K]$  ist trivial. Zu zeigen ist nur, dass das Minimalpolynom  $\varphi(T) \in K[T]$  von  $\alpha$  über  $K$  irreduzibel über  $F$  bleibt. Angenommen wir hätten eine Faktorisierung  $\varphi(T) = g(T)h(T)$  über  $F$ .  $g$  und  $h$  sind normierte Polynome vom Grad  $\geq 1$  aus  $F[T]$ . Jede Nullstelle von  $g(T)$  und  $h(T)$  in  $\Phi$  ist eine Nullstelle von  $\varphi$ , also

algebraisch über  $K$ . Also sind alle Koeffizienten von  $g(T)$  und  $h(T)$  algebraisch über  $K$ , da sie ja mit Hilfe der elementarsymmetrischen Funktionen also Polynomausdrücken in den Nullstellen dargestellt werden können. Andererseits sind die Koeffizienten in  $F$ . Da  $K$  algebraisch abgeschlossen in  $F$  ist, gilt  $g(T), h(T) \in K[T]$ . Widerspruch.

□

Nun können wir die Frage über den Konstantenkörper von einer Konstantenkörpererweiterung beantworten:

**Proposition 4.7.2** *Sei  $F' = FK'$  eine algebraische Konstantenkörpererweiterung von  $F/K$ . Dann gilt:*

- (a)  $K'$  ist der volle Konstantenkörper von  $F'$ .
- (b) Jede Teilmenge von linear unabhängigen Elementen über  $K$  bleibt linear unabhängig über  $K'$ .
- (c)  $[F : K(x)] = [F' : K'(x)]$  für alle  $x \in F \setminus K$ .

*Beweis:* (a) Sei  $\gamma \in F'$  algebraisch über  $K'$ . Dann ist  $\gamma$  algebraisch über  $K$  und es existieren endlich viele Elemente  $\alpha_1, \dots, \alpha_r \in K'$ , sodass  $\gamma \in F(\alpha_1, \dots, \alpha_r)$ . Nach dem Satz vom primitiven Element existiere ein  $\alpha \in K'$ , mit  $K(\alpha_1, \dots, \alpha_r) = K(\alpha)$ . Hier geht ein, dass  $K$  perfekt ist, also die Erweiterung  $K(\alpha_1, \dots, \alpha_r)/K$  separabel ist. Da  $\gamma$  algebraisch über  $K$  ist, können wir ein  $\beta \in F'$  finden, mit  $K(\alpha, \gamma) = K(\beta)$ . Daher gilt  $F(\beta) = F(\alpha, \gamma) = F(\alpha)$ , da  $\gamma \in F(\alpha)$ . Wir erhalten aufgrund des vorigen Lemmas

$$[K(\beta) : K] = [F(\beta) : F] = [F(\alpha) : F] = [K(\alpha) : K].$$

Daraus folgt  $K(\alpha) = K(\beta)$  und daher gilt  $\gamma \in K(\alpha) \subseteq K'$ .

(b) Sei  $y_1, \dots, y_r \in F$  linear unabhängig über  $K$ . Betrachten wir eine Linearkombination

$$\sum_{i=1}^r \gamma_i y_i = 0 \text{ mit } \gamma_i \in K'.$$

Wählen wir wieder ein  $\alpha \in K'$  mit  $K(\gamma_1, \dots, \gamma_r) = K(\alpha)$ . Wir schreiben

$$\gamma_i = \sum_{j=0}^{n-1} c_{ij} \alpha^j \text{ mit } c_{ij} \in K, n = [K(\alpha) : K].$$

Wir erhalten

$$0 = \sum_{i=1}^r \sum_{j=0}^{n-1} (c_{ij} \alpha^j) y_i = \sum_{j=0}^{n-1} \left( \sum_{i=1}^r c_{ij} y_i \right) \alpha^j,$$

wobei  $\sum c_{ij}y_j \in F$ . Da nach dem obigen Lemma  $[F(\alpha) : F] = [K(\alpha) : K]$  gilt, sind die Elemente  $1, \alpha, \dots, \alpha^{n-1}$  linear unabhängig über  $F$  und daher gilt

$$\sum_{i=1}^r c_{ij}y_i = 0 \text{ für } j = 0, \dots, n-1.$$

Da aber  $y_1, \dots, y_r$  linear unabhängig über  $K$  sind, gilt  $c_{ij} = 0$  für alle  $i, j$ . Daher ist  $\gamma_i = 0$  für  $i = 1, \dots, r$ .

(c) Klarerweise gilt  $[F' : K'(x)] \leq [F : K(x)]$ . Wir zeigen, dass alle Elemente  $z_1, \dots, z_s$ , die linear unabhängig über  $K(x)$  sind, auch linear unabhängig über  $K'(x)$  bleiben. Angenommen, das gelte nicht, dann hätten wir

$$\sum_{i=1}^s f_i(x) \cdot z_i = 0,$$

und o.B.d.A. gelte  $f_i(x) \in K'[x]$  und  $f_i(x) \neq 0$  für zumindest ein  $i$ . Daher existiert eine lineare Abhängigkeit in der Menge  $\{x^j z_i : 1 \leq i \leq s, j \geq 0\}$  über  $K'$ . Nach Teil (b) unserer Proposition ist die Menge auch linear abhängig über  $K$ , also sind  $z_1, \dots, z_s$  linear abhängig über  $K(x)$ . Widerspruch. □

**Satz 4.7.3** Sei  $F' = FK'$  eine algebraische Konstantenkörpererweiterung von  $F/K$ . Dann gilt:

- (a)  $F'/F$  ist unverzweigt.
- (b)  $F'/K'$  hat dasselbe Geschlecht wie  $F/K$ .
- (c) Für jeden Divisor  $A \in \mathcal{D}_F$  gilt  $\deg(\text{Con}_{F'/F}(A)) = \deg(A)$ .
- (d) Für jeden Divisor  $A \in \mathcal{D}_F$  gilt

$$\dim(\text{Con}_{F'/F}(A)) = \dim(A).$$

Jede Basis von  $\mathcal{L}(A)$  ist auch Basis von  $\mathcal{L}(\text{Con}_{F'/F}(A))$ <sup>1</sup>.

- (e) Ist  $W$  ein kanonischer Divisor von  $F/K$ , so ist  $\text{Con}_{F'/F}(W)$  ein kanonischer Divisor von  $F'/K'$ .
- (f) Die Conormabbildung  $\text{Con}_{F'/F} : \mathcal{C}_F \rightarrow \mathcal{C}_{F'}$  ist injektiv.
- (g) Für  $P' \in \mathbb{P}_{F'}$  gilt

$$F'_{P'} = F_P K' \text{ wobei } P := P' \cap F.$$

<sup>1</sup>Wir betrachten dabei  $\mathcal{L}(A)$  als  $K$ -Vektorraum, und  $\mathcal{L}(\text{Con}_{F'/F}(A))$  als  $K'$ -Vektorraum.

(h) *Ist die Erweiterung  $K'/K$  endlich, so ist jede Basis von  $K'/K$  eine Ganzheitsbasis von  $F'/F$  für alle  $P \in \mathbb{P}_F$ .*

*Beweis:* Da wir den Rest nicht benötigen, beweisen wir hier nur die Aussagen (a) und (b) für endliche Erweiterungen. Der restliche Beweis findet sich in [38].

Sei also  $K' = K(\alpha)$  eine endliche Erweiterung von  $K$  und  $\varphi(T)$  das Minimalpolynom von  $\alpha$  über  $K$ . Nach dem Lemma 4.7.1 ist  $\varphi(T)$  irreduzibel über  $F$ . Sei  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$ . Nach Satz 4.6.7 gilt

$$0 \leq d(P'|P) \leq v_{P'}(\varphi'(\alpha)).$$

Da  $\alpha$  separabel ist, gilt  $\varphi'(\alpha) \neq 0$  und da  $\varphi'(\alpha) \in K'$  liegt, gilt  $v_{P'}(\varphi'(\alpha)) = 0$ . Nach der Dedekindschen Differentenformel ist  $P'|P$  unverzweigt. Nach Lemma 4.7.1 gilt  $[F' : F] = [K' : K]$ . Damit, und aus der eben gezeigten Tatsache, dass  $\deg(\text{Diff}(F'/F)) = 0$  ist, folgt die Aussage (b) sofort mit der Hurwitzschen Geschlechterformel. □

**Proposition 4.7.4** *Sei  $F/K$  ein Funktionenkörper mit Konstantenkörper  $K$ . Sei  $F'/F$  eine endliche Körpererweiterung mit Konstantenkörper  $K'$ . Sei  $\bar{K} \subseteq \Phi$  ein algebraischer Abschluss von  $K$ . Dann gilt*

$$[F' : F] = [F'\bar{K} : F\bar{K}] \cdot [K' : K] \tag{4.33}$$

Für den Spezialfall  $F' = F(y)$  erhalten wir: Sei  $\varphi(T) \in F[T]$  das Minimalpolynom von  $y$  über  $F$ . Dann sind folgende Aussagen äquivalent:

- (1)  $K' = K$ .
- (2)  $\varphi(T)$  ist irreduzibel in  $F\bar{K}[T]$ .

*Beweis:* Wegen  $F \subseteq FK' \subseteq F'$ , gilt

$$[F' : F] = [F' : FK'] \cdot [FK' : F]. \tag{4.34}$$

Da die Erweiterung  $K'/K$  separabel und endlich ist, gilt  $K' = K(\alpha)$  für ein  $\alpha \in K'$  und wir erhalten wegen Lemma 4.7.1, dass

$$[FK' : F] = [K' : K]. \tag{4.35}$$

Aufgrund von Proposition 4.7.2 (c) gilt für jedes  $x \in F \setminus K$ ,

$$[FK' : K'(x)] = [F\bar{K} : \bar{K}(x)] \text{ und } [F' : K'(x)] = [F'\bar{K} : \bar{K}(x)].$$

Daraus folgt

$$[F' : FK'] = [F'\bar{K} : F\bar{K}]. \tag{4.36}$$

Setzt man nun (4.35) und (4.36) in (4.34) ein, so erhält man (4.33).

Betrachten wir nun den Fall  $F' = F(y)$ . Es gilt  $\deg(\varphi(T)) = [F' : F]$  und  $[F'\bar{K} : F\bar{K}]$  ist gleich dem Grad des Minimalpolynoms von  $y$  über  $F\bar{K}$ , welches ein Teiler von  $\varphi(T)$  in  $F\bar{K}[T]$  ist. Die Äquivalenz von (1) und (2) folgt nun sofort aus (4.33).

□

Noch ein nützlicher Satz, der eine Verallgemeinerung des Eisensteinschen Kriteriums darstellt:

**Satz 4.7.5 (Eisensteinsches Kriterium)** Sei  $F/K$  ein Funktionenkörper und

$$\varphi(T) = a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0$$

ein Polynom mit Koeffizienten in  $F$ . Angenommen es existiert eine Stelle  $P \in \mathbb{P}_F$  sodass die Bedingung (1) oder (2) erfüllt ist:

$$(1) \quad v_P(a_n) = 0, \quad v_P(a_i) \geq v_P(a_0) > 0 \text{ für } i = 1, \dots, n-1, \text{ und } ggT(n, v_P(a_0)) = 1.$$

$$(2) \quad v_P(a_n) = 0, \quad v_P(a_i) \geq 0 \text{ für } i = 1, \dots, n-1, \quad v_P(a_0) < 0, \text{ und } ggT(n, v_P(a_0)) = 1.$$

Dann ist  $\varphi(T)$  irreduzibel in  $F[T]$ . Sei  $F' = F(y)$ , wobei  $y$  eine Nullstelle von  $\varphi(T)$  ist. Dann hat  $P$  genau eine Erweiterung  $P' \in \mathbb{P}_{F'}$  und es gilt  $e(P'|P) = n$  und  $f(P'|P) = 1$ . Weiters ist  $K$  der volle Konstantenkörper von  $F'$ .

*Beweis:* Betrachten wir einen Erweiterungskörper  $F' = F(y)$ , mit  $\varphi(y) = 0$ . Es gilt  $[F' : F] \leq \deg(\varphi(T)) = n$ . Gleichheit gilt genau dann, wenn  $\varphi(T)$  irreduzibel in  $F[T]$  ist. Wählen wir eine Erweiterung  $P'|P$ . Aus  $\varphi(y) = 0$  folgt

$$-a_n y^n = a_0 + a_1 y + \dots + a_{n-1} y^{n-1}. \quad (4.37)$$

Nehmen wir zunächst (1) an: Aus  $v_{P'}(a_n) = 0$  und  $v_{P'}(a_i) > 0$  für  $i = 0, \dots, n-1$  folgt  $v_{P'}(y) > 0$ . Sei  $e := e(P'|P)$ . Dann gilt  $v_{P'}(a_0) = e \cdot v_P(a_0)$  und  $v_{P'}(a_i y^i) = e \cdot v_P(a_i) + i \cdot v_{P'}(y) > e \cdot v_P(a_0)$  für  $i = 1, \dots, n-1$ . Mit (4.37) und der starken Dreiecksungleichung folgt

$$n \cdot v_{P'}(y) = e \cdot v_P(a_0).$$

Aus  $ggT(n, v_P(a_0)) = 1$  folgt  $n|e$ , also  $n \leq e$ . Andererseits gilt  $n \geq [F' : F] \geq e$  wegen der Hilbertschen Fundamentalgleichung. Also gilt

$$n = e = [F' : F].$$

Die restlichen Aussagen sind triviale Folgerungen aus der Hilbertschen Fundamentalgleichung und Proposition 4.7.4. Der Beweis mit der Voraussetzung (2) ist sehr ähnlich und kann daher ausgelassen werden.

□

## 4.8 Galoisweiterungen

In diesem Abschnitt behandeln wir Galoisweiterungen  $F'/F$  und nennen dann  $F'/K'$  eine Galoisweiterung von  $F/K$ . Zunächst werden wir einige allgemeine Resultate herleiten, zum Beispiel dass die Automorphismengruppe von  $F'/F$  transitiv auf der Menge der Stellen  $P' \in \mathbb{P}_{F'}$  operiert, die über einer Stelle  $P \in \mathbb{P}_F$  liegen. Daraus werden wir einige Folgerungen ziehen. Danach wenden wir uns zwei Spezialfällen zu: Kummer Erweiterungen und Artin-Schreier Erweiterungen. Erweiterungen dieser Art werden uns später asymptotisch optimale Familien von Goppa Codes liefern.

**Satz 4.8.1** *Sei  $F'/K'$  eine Galoisweiterung von  $F/K$  und  $P_1, P_2 \in \mathbb{P}_{F'}$  Erweiterungen von  $P \in \mathbb{P}_F$ . Dann gilt  $P_2 = \sigma(P_1)$  für ein  $\sigma \in \text{Gal}(F'/F)$ .*

*Beweis:* Angenommen  $\sigma(P_1) \neq P_2$  für alle  $\sigma \in G := \text{Gal}(F'/F)$ . Nach dem Approximationssatz existiert ein  $z \in F'$  mit  $v_{P_2}(z) > 0$  und  $v_Q(z) = 0$  für alle  $Q \in \mathbb{P}_{F'}$  mit  $Q \neq P_2$  und  $Q|P$ . Sei  $Nm_{F'/F} : F' \rightarrow F$  die Normabbildung (siehe Appendix A in [38], bzw. [27] oder [1]). Wir erhalten

$$\begin{aligned} v_{P_1}(Nm_{F'/F}(z)) &= v_{P_1} \left( \prod_{\sigma \in G} \sigma(z) \right) = \sum_{\sigma \in G} v_{P_1}(\sigma(z)) \\ &= \sum_{\sigma \in G} v_{\sigma^{-1}(P_1)}(z) = \sum_{\sigma \in G} v_{\sigma(P_1)}(z) = 0 \end{aligned} \quad (4.38)$$

weil  $P_2 \neq \sigma(P_1)$  für alle  $\sigma \in G$ . Ausserdem gilt

$$v_{P_2}(Nm_{F'/F}(z)) = \sum_{\sigma \in G} v_{\sigma(P_2)}(z) > 0. \quad (4.39)$$

Es gilt  $Nm_{F'/F}(z) \in F$ , und daher

$$v_{P_1}(Nm_{F'/F}(z)) = 0 \Leftrightarrow v_P(Nm_{F'/F}(z)) = 0 \Leftrightarrow v_{P_2}(Nm_{F'/F}(z)) = 0.$$

Das ist ein Widerspruch zu (4.38) und (4.39). □

**Korollar 4.8.2** *Voraussetzungen wie in Satz 4.8.1. Seien  $P_1, \dots, P_r \in \mathbb{P}_{F'}$  alle Stellen, die über  $P \in \mathbb{P}_F$  liegen. Dann gilt:*

(a)  $e(P_i|P) = e(P_j|P)$  und  $f(P_i|P) = f(P_j|P)$  für alle  $i, j$ . Wir schreiben daher auch

$$e(P) := e(P_i|P) \text{ und } f(P) := f(P_i|P)$$

und nennen  $e(P)$  (bzw.  $f(P)$ ) den Verzweigungsindex (bzw. den relativen Grad) von  $P$  in  $F'/F$ .

$$(b) e(P) \cdot f(P) \cdot r = [F' : F].$$

$$(c) d(P_i|P) = d(P_j|P) \text{ für alle } i, j.$$

*Beweis:* (a) ist klar wegen Lemma 4.6.2 und Satz 4.8.1.

(b) folgt aus (a) und der Fundamentalungleichung von Hilbert.

(c) Betrachten wir

$$\mathcal{O}'_P = \bigcap_{i=1}^r \mathcal{O}_{P_i},$$

den ganzen Abschluss von  $\mathcal{O}_P$  in  $F'$ . Sei  $\sigma \in \text{Gal}(F'/F)$ . Dann gilt  $\sigma(\mathcal{O}'_P) = \mathcal{O}'_P$  und  $\sigma(\mathcal{C}_P) = \mathcal{C}_P$ , da  $\text{Tr}_{F'/F}(\sigma(u)) = \text{Tr}_{F'/F}(u)$ . Sei  $\mathcal{C}_P = t \cdot \mathcal{O}'_P$ . Dann haben wir

$$\sigma(t) \cdot \mathcal{O}'_P = \sigma(\mathcal{C}_P) = \mathcal{C}_P = t \cdot \mathcal{O}'_P.$$

Betrachten wir nun zwei Stellen  $P_i, P_j$ , die über  $P$  liegen. Dann gibt es  $\sigma \in \text{Gal}(F'/F)$  mit  $\sigma(P_j) = P_i$ , woraus folgt

$$-d(P_i|P) = v_{P_i}(\sigma(t)) = v_{\sigma^{-1}(P_i)}(t) = v_{P_j}(t) = -d(P_j|P).$$

□

Nun wollen wir uns zyklische Erweiterungen genauer ansehen. Die einzigen zyklischen Galoiserweiterungen sind Artin-Schreier Erweiterungen und Kummer Erweiterungen (siehe [27] bzw. [1]). Wir wollen diese Erweiterungen im Zusammenhang mit Funktionenkörpern betrachten. Diese Ergebnisse gehen auf H. Hasse zurück, siehe [24]. Zuerst betrachten wir **Kummer Erweiterungen**.

**Proposition 4.8.3** *Sei  $F/K$  ein algebraischer Funktionenkörper sodass  $K$  eine primitive  $n$ -te Einheitswurzel enthalte ( $n > 1$  relativ prim zu  $\text{char}(K)$ ). Sei  $u \in F$  mit  $u \neq w^d$  für alle  $w \in F$  und  $d > 1$  mit  $d|n$ . Sei*

$$F' := F(y) \text{ mit } y^n = u.$$

*Eine solche Erweiterung heißt **Kummer Erweiterung**. Es gilt:*

(a) *Das Polynom  $\Phi(T) = T^n - u$  ist das Minimalpolynom von  $y$  über  $F$ . Die Erweiterung  $F'/F$  ist galoissch, die Galoisgruppe ist zyklisch und alle Automorphismen sind von der Gestalt  $\sigma(y) = \zeta y$ , wobei  $\zeta$  eine  $n$ -te Einheitswurzel ist.*

(b) *Sei  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$  eine Erweiterung von  $P$ . Dann gilt*

$$e(P'|P) = \frac{n}{r_P} \text{ und } d(P'|P) = \frac{n}{r_P} - 1$$

*mit  $r_P := \text{ggT}(n, v_P(u)) > 0$ .*

(c) Sei  $K'$  der Konstantenkörper von  $F'$  und  $g$  (bzw.  $g'$ ) das Geschlecht von  $F/K$  (bzw.  $F'/K'$ ). Dann gilt

$$g' = 1 + \frac{n}{[K' : K]} \left( g - 1 + \frac{1}{2} \sum_{P \in \mathbb{P}_F} \left( 1 - \frac{r_P}{n} \right) \deg(P) \right).$$

*Beweis:* (a) folgt aus Hilbert's Theorem 90, siehe [27] bzw. [1].

(b) **1. Fall:**  $r_P = 1$ .

Es gilt

$$n \cdot v_{P'}(y) = v_{P'}(y^n) = v_{P'}(u) = e(P'|P) \cdot v_P(u).$$

Daraus folgt, da  $n$  und  $v_P(u)$  relativ prim sind, dass  $e(P'|P) = n$ . Da  $\text{char}(K) \nmid n$  gilt, ist nach der Dedekindschen Differentenformel der Differentenexponent gegeben durch  $d(P'|P) = n - 1$ .

**2. Fall:**  $r_P = n$ .

Dann gilt  $v_P(u) = l \cdot n$  für ein  $l \in \mathbb{Z}$ . Wählen wir ein  $t \in F$  mit  $v_P(t) = l$  und setzen

$$y_1 := t^{-1}y \text{ und } u_1 := t^{-n}u.$$

Dann gilt  $y_1^n = u_1$ ,  $v_{P'}(y_1) = v_P(u_1) = 0$ , und das Minimalpolynom von  $y_1$  über  $F$  ist

$$\Psi(T) = T^n - u_1 \in F[T].$$

$y_1$  ist also ganz über  $\mathcal{O}_P$  und daher gilt nach Satz 4.6.7

$$0 \leq d(P'|P) \leq v_{P'}(\Psi'(y_1)).$$

Es ist  $\Psi'(y_1) = n \cdot y_1^{n-1}$ , und daher gilt  $v_{P'}(\Psi'(y_1)) = (n-1) \cdot v_{P'}(y_1) = 0$ , und damit  $d(P'|P) = 0$ . Nach der Dedekindschen Differentenformel haben wir  $e(P'|P) = 1$ .

**3. Fall:**  $1 < r_P < n$ .

Betrachten wir den Zwischenkörper

$$F_0 := F(y_0) \text{ mit } y_0 := y^{n/r_P}.$$

Dann gilt  $[F' : F_0] = n/r_P$  und  $[F_0 : F] = r_P$ . Das Element  $y_0$  erfüllt die Gleichung

$$y_0^{r_P} = u$$

über  $F$  und mit  $P_0 := P' \cap F_0$  können wir den 2. Fall auf  $F_0/F$  anwenden und erhalten  $e(P_0|P) = 1$ . Daraus folgt

$$v_{P_0}(y_0) = \frac{v_P(u)}{r_P},$$

und da dieser Wert relativ prim zu  $n/r_P$  ist, können wir Fall 1 auf die Erweiterung  $F' = F_0(y) \supseteq F_0$  anwenden (da  $y^{n/r_P} = y_0$ ) und erhalten  $e(P'|P_0) = n/r_P$ . Aufgrund der Multiplikativität des Verzweigungsindex gilt daher  $e(P'|P) = n/r_P$ . Wieder folgt aus der Dedekindschen Differentenformel  $d(P'|P) = \frac{n}{r_P} - 1$ .

(c) Es gilt

$$\begin{aligned} \deg(\text{Diff}(F'/F)) &= \sum_{P \in \mathbb{P}_F} \sum_{P'|P} d(P'|P) \cdot \deg(P') \\ &= \sum_{P \in \mathbb{P}_F} \left( \frac{n}{r_P} - 1 \right) \cdot \sum_{P'|P} \deg(P'). \end{aligned}$$

Die zweite Summe können wir noch vereinfachen, da wir ja wissen, dass bei einer Galoiserweiterung die Verzweigungsindizes nicht von der Stelle abhängen, die über  $P$  liegen. Wir haben also

$$\begin{aligned} \sum_{P'|P} \deg(P') &= \frac{1}{e(P)} \cdot \deg \left( \sum_{P'|P} e(P'|P) \cdot P' \right) \\ &= \frac{1}{e(P)} \cdot \deg(\text{Con}_{F'/F}(P)) = \frac{r_P}{n} \cdot \frac{n}{[K' : K]} \cdot \deg(P) \\ &= \frac{r_P}{[K' : K]} \cdot \deg(P). \end{aligned}$$

Fassen wir nun zusammen, so erhalten wir

$$\begin{aligned} \deg(\text{Diff}(F'/F)) &= \sum_{P \in \mathbb{P}_F} \frac{n - r_P}{r_P} \cdot \frac{r_P}{[K' : K]} \cdot \deg(P) \\ &= \frac{n}{[K' : K]} \cdot \sum_{P \in \mathbb{P}_F} \left( 1 - \frac{r_P}{n} \right) \cdot \deg(P). \end{aligned}$$

Aus der Hurwitzschen Geschlechtsformel folgt nun (c). □

Die zweite Klasse von Erweiterungen, die wir näher studieren wollen, sind die sogenannten **Artin-Schreier Erweiterungen**. Dazu benötigen wir jedoch zuvor noch ein kleines Lemma.

**Lemma 4.8.4** *Sei  $F/K$  ein algebraischer Funktionenkörper der Charakteristik  $p > 0$ ,  $u \in F$  und  $P \in \mathbb{P}_F$ . Dann gilt entweder (a) oder (b):*

(a) *es existiert ein  $z \in F$  mit  $v_P(u - (z^p - z)) \geq 0$ ,*

(b) es existiert ein  $z \in F$  mit

$$v_P(u - (z^p - z)) = -m < 0 \text{ und } m \neq 0 \text{ mod } p.$$

Im Fall (b) ist  $m$  eindeutig bestimmt durch

$$-m = \max\{v_P(u - (w^p - w)) : w \in F\}. \quad (4.40)$$

*Beweis:* Wir beginnen mit einer

**Behauptung:** Seien  $x_1, x_2 \in F \setminus \{0\}$  und  $v_P(x_1) = v_P(x_2)$ . Dann existiert ein  $y \in F$  mit

$$v_P(y) = 0 \text{ und } v_P(x_1 - y^p x_2) > v_P(x_1). \quad (4.41)$$

Es gilt  $(x_1/x_2)(P) \neq 0$ , also gilt  $(x_1/x_2)(P) = y(P)^p$  für ein  $y \in \mathcal{O}_P \setminus P$ . Hier haben wir die Vollkommenheit von  $\mathcal{O}_P/P$  benützt. Klarerweise gilt  $v_P(y) = 0$  und  $v_P((x_1/x_2) - y^p) > 0$ . Daraus folgt (4.41).

**Behauptung:** Gelte  $v_P(u - (z_1^p - z_1)) = -lp < 0$ . Dann existiert ein Element  $z_2 \in F$  mit

$$v_P(u - (z_2^p - z_2)) > -lp. \quad (4.42)$$

Wählen wir ein Element  $t \in F$  mit  $v_P(t) = -l$ . Dann gilt

$$v_P(u - (z_1^p - z_1)) = v_P(t^p).$$

Nach (4.41) existiert ein  $y \in F$  mit  $v_P(y) = 0$  und

$$v_P(u - (z_1^p - z_1) - (yt)^p) > -lp.$$

Da  $v_P(yt) = v_P(t) = -l > -lp$ , gilt

$$v_P(u - (z_1^p - z_1) - ((yt)^p - yt)) > -lp.$$

Setzen wir  $z_2 := z_1 + yt$ , so erhalten wir (4.42).

Damit ist aber schon bewiesen, dass entweder (a) oder (b) gelten muss! Zu zeigen bleibt im Fall (b) noch (4.40). Für jedes  $w \in F$  gilt  $p \cdot v_P(w - z) \neq -m$ , da  $m \neq 0 \text{ mod } p$ .

**1. Fall:**  $p \cdot v_P(w - z) > -m$ .

Dann gilt  $v_P((w - z)^p - (w - z)) > -m$  und  $v_P(u - (w^p - w)) = v_P(u - (z^p - z) - ((w - z)^p - (w - z))) = -m$  nach der strikten Dreiecksungleichung.

**2. Fall:**  $p \cdot v_P(w - z) < -m$ .

Dann erhalten wir  $v_P(u - (w^p - w)) = v_P(u - (z^p - z) - ((w - z)^p - (w - z))) < -m$ . In jedem Fall gilt  $v_P(u - (w^p - w)) \leq -m$ , und das beweist (4.40).

□

Nun sind wir in der Lage Artin-Schreier Erweiterungen zu behandeln.

**Satz 4.8.5** Sei  $F/K$  algebraischer Funktionenkörper und  $\text{char}(K) = p > 0$ . Sei  $u \in F$  mit  $u \neq w^p - w$  für alle  $w \in F$ . Sei

$$F' = F(y) \text{ mit } y^p - y = u.$$

Eine solche Erweiterung heißt **Artin-Schreier Erweiterung**.

Definiere für  $P \in \mathbb{P}_F$

$$m_P := \begin{cases} m & \text{falls ein } z \in F \text{ existiert mit} \\ & v_P(u - (z^p - z)) = -m < 0 \text{ und } m \not\equiv 0 \pmod{p}, \\ -1 & \text{falls ein } z \in F \text{ existiert mit } v_P(u - (z^p - z)) \geq 0. \end{cases}$$

Nach dem vorangegangenen Lemma ist  $m_P$  wohldefiniert. Es gilt:

(a)  $F'/F$  ist eine zyklische Galoiserweiterung vom Grad  $p$ . Die Automorphismen sind gegeben durch  $\sigma(y) = y + \nu$ ,  $\nu = 0, 1, \dots, p-1$ .

(b)  $P$  ist genau dann unverzweigt, wenn  $m_P = -1$ .

(c)  $P$  ist genau dann total verzweigt, wenn  $m_P > 0$ . Sei  $P'$  die Stelle über  $P$ . Dann gilt

$$d(P'|P) = (p-1)(m_P + 1).$$

(d) Gelte  $m_Q > 0$  für ein  $Q \in \mathbb{P}_F$ . Dann ist  $K$  algebraisch abgeschlossen in  $F'$  und es gilt

$$g' = p \cdot g + \frac{p-1}{2} \left( -2 + \sum_{P \in \mathbb{P}_F} (m_P + 1) \cdot \deg(P) \right).$$

wobei  $g'$  (bzw.  $g$ ) das Geschlecht von  $F'/K'$  (bzw.  $F/K$ ) bezeichne.

*Beweis:* (a) folgt aus der additiven Form von Hilbert's Theorem 90, siehe [27] oder [1].

(b) und (c): **1. Fall:**  $m_P = -1$ .

Dann existiert also ein  $z \in F$  mit  $v_P(u - (z^p - z)) \geq 0$ . Sei  $y_1 := y - z$  und  $u_1 := u - (z^p - z)$ . Dann gilt  $F' = F(y_1)$  und  $\varphi_1(T) = T^p - T - u_1$  ist das Minimalpolynom von  $y_1$  über  $F$ . Da  $v_P(u_1) \geq 0$ , ist  $y_1$  ganz über  $\mathcal{O}_P$  und es gilt für jede Erweiterung  $P'|P$

$$0 \leq d(P'|P) \leq v_{P'}(\varphi_1'(y_1)) = 0,$$

da  $\varphi_1'(T) = -1$ . Also gilt  $d(P'|P) = 0$  und  $P'|P$  ist unverzweigt.

**2. Fall:**  $m_P > 0$ .

Wählen wir ein  $z \in F$  mit  $v_P(u - (z^p - z)) = -m_P$ . Betrachten wir die Elemente  $y_1 := y - z$  und  $u_1 := u - (z^p - z)$ . Es gilt wieder  $F' = F(y_1)$  und das Minimalpolynom

von  $y_1$  über  $F$  ist  $\varphi_1(T) = T^p - T - u_1$ . Sei  $P'$  eine Erweiterung von  $P$ . Da  $y_1^p - y_1 = u_1$ , erhalten wir

$$v_{P'}(u_1) = e(P'|P) \cdot v_P(u_1) = -m_P \cdot e(P'|P)$$

und

$$v_{P'}(u_1) = v_{P'}(y_1^p - y_1) = p \cdot v_{P'}(y_1).$$

Da  $p$  und  $m_P$  relativ prim sind, und  $e(P'|P) \leq [F' : F] = p$  gilt, haben wir

$$e(P'|P) = p \text{ und } v_{P'}(y_1) = -m_P.$$

Insbesondere ist  $P'|P$  total verzweigt.

Sei nun  $x$  ein primes Element von  $P$ . Wählen wir ganze Zahlen  $i, j \geq 0$  mit  $1 = ip - jm_P$ . Dann ist das Element  $t := x^i y_1^j$  ein primes Element von  $P'$ , da  $v_{P'}(t) = 1$ . Nach Proposition 4.6.10 gilt

$$d(P'|P) = v_{P'}(\psi'(t)),$$

wobei  $\psi$  das Minimalpolynom von  $t$  über  $F$  bezeichnet. Sei  $G := \text{Gal}(F'/F)$ . Klarerweise gilt

$$\psi(T) = \prod_{\sigma \in G} (T - \sigma(t)) = (T - t)h(T)$$

mit

$$h(T) = \prod_{\sigma \neq id} (T - \sigma(t)) \in F'[T].$$

Also gilt  $\psi'(T) = h(T) + (T - t)h'(T)$  und  $\psi'(t) = h(t)$ . Wir haben nun

$$d(P'|P) = v_{P'} \left( \prod_{\sigma \neq id} (t - \sigma(t)) \right) = \sum_{\sigma \neq id} v_{P'}(t - \sigma(t)).$$

Wir wissen, dass jedes  $\sigma \neq id$  aus  $G$  von der Form  $\sigma(y_1) = y_1 + \mu$  für ein  $\mu \in \{1, \dots, p-1\}$  ist. Es gilt also

$$t - \sigma(t) = x^i y_1^j - x^i (y_1 + \mu)^j = -x^i \sum_{l=1}^j \binom{j}{l} y_1^{j-l} \mu^l.$$

Da  $v_{P'}(y_1^{j-1}) < v_{P'}(y_1^{j-l})$  gilt für  $l \geq 2$ , folgt aus der starken Dreiecksungleichung

$$\begin{aligned} v_{P'}(t - \sigma(t)) &= v_{P'}(x^i) + v_{P'}(j\mu y_1^{j-1}) \\ &= ip + (j-1) \cdot (-m_P) = ip - jm_P + m_P = m_P + 1. \end{aligned}$$

Zusammenfassend erhalten wir

$$d(P'|P) = (p-1)(m_P + 1)$$

und das beweist (b) und (c). Die Formel für das Geschlecht  $g'$  in (d) folgt direkt aus der Hurwitzschen Geschlechtsformel.

Wir müssen nur noch zeigen, dass  $K$  algebraisch abgeschlossen ist, falls eine total verzweigte Stelle  $Q$  existiert. Angenommen  $K$  wäre nicht algebraisch abgeschlossen. Sei  $K'$  der algebraische Abschluß in  $F'$ . Dann ist  $K'F/F$  eine Konstantenkörpererweiterung vom Grad  $> 1$  in der  $Q$  unverzweigt ist nach Satz 4.7.3. Das ist aber ein Widerspruch zur Multiplikativität der Verzweigungsindizes.

□

## 4.9 Verzweigungsgruppen

Wir betrachten wieder eine Galoiserweiterung  $F'/F$  von algebraischen Funktionenkörpern mit Galoisgruppe  $G := \text{Gal}(F'/F)$ . Sei  $P$  eine Stelle von  $F/K$  und  $P'$  eine Erweiterung von  $P$  in  $F'$ .

### Definition 4.9.1

- (a)  $G_Z(P'|P) := \{\sigma \in G : \sigma(P') = P'\}$  heißt **Zerlegungsgruppe** von  $P'$  über  $P$ .
- (b)  $G_T(P'|P) := \{\sigma \in G : v_{P'}(\sigma z - z) > 0 \text{ für alle } z \in \mathcal{O}_{P'}\}$  heißt **Trägheitsgruppe** von  $P'$  über  $P$ .
- (c) Der Fixkörper  $Z := Z(P'|P)$  von  $G_Z(P'|P)$  heißt **Zerlegungskörper**, und der Fixkörper  $T := T(P'|P)$  von  $G_T(P'|P)$  heißt **Trägheitskörper** von  $P'$  über  $P$ .

Klarerweise gilt  $G_T(P'|P) \subseteq G_Z(P'|P)$  und sowohl  $G_T(P'|P)$ , als auch  $G_Z(P'|P)$  sind Untergruppen von  $G$ .

**Satz 4.9.2** *Mit der obigen Notation gilt:*

- (a) Die Zerlegungsgruppe  $G_Z(P'|P)$  hat Ordnung  $e(P'|P) \cdot f(P'|P)$ .
- (b) Die Trägheitsgruppe  $G_T(P'|P)$  hat Ordnung  $e(P'|P)$  und ist ein Normalteiler von  $G_Z(P'|P)$ .
- (c) Die Körpererweiterung  $F'_{P'}/F_P$  ist galoissch. Jeder Automorphismus  $\sigma \in G_Z(P'|P)$  induziert einen Automorphismus  $\bar{\sigma}$  von  $F'_{P'}$  über  $F_P$  indem man  $\bar{\sigma}(z(P')) = \sigma(z)(P')$  setzt für ein  $z \in \mathcal{O}_{P'}$ . Die Abbildung

$$\Phi : \begin{cases} G_Z(P'|P) & \rightarrow & \text{Gal}(F'_{P'}/F_P) \\ \sigma & \mapsto & \bar{\sigma} \end{cases}$$

ist ein surjektiver Gruppenhomomorphismus mit Kern  $G_T(P'|P)$ . Insbesondere ist  $\text{Gal}(F'_{P'}/F_P)$  isomorph zu der Faktorgruppe  $G_Z(P'|P)/G_T(P'|P)$ .

(d) Sei  $P_Z := P' \cap Z$  und  $P_T := P' \cap T$ . Dann gilt  $P'|P_T|P_Z|P$ . Weiters gilt

$$e(P'|P_T) = e(P'|P) = [F' : T] \text{ und } f(P'|P_T) = 1,$$

$$f(P_T|P_Z) = f(P'|P) = [T : Z] \text{ und } e(P_T|P_Z) = 1,$$

und

$$e(P_Z|P) = f(P_Z|P) = 1.$$

*Beweis:* (a)  $G$  operiert transitiv auf der Menge der Erweiterungen von  $P$ , also existieren  $\sigma_1, \dots, \sigma_r \in G$  so wählen, dass alle Erweiterungen von  $P$  durch  $\sigma_1(P'), \dots, \sigma_r(P')$  gegeben sind, wobei  $\sigma_i(P') \neq \sigma_j(P')$  für  $i \neq j$ , d.h.  $\sigma_1, \dots, \sigma_r$  ist ein vollständiges Repräsentantensystem von  $G/G_Z(P'|P)$ , also gilt  $[F' : F] = \text{ord}(G) = r \cdot \text{ord}(G_Z(P'|P))$ . Andererseits gilt  $[F' : F] = e(P'|P) \cdot f(P'|P) \cdot r$ . Das beweist (a).

Wir betrachten nun  $P_Z$ . Offensichtlich ist die Zerlegungsgruppe von  $P'$  über  $P_Z$  durch  $G_Z(P'|P)$  gegeben, also gilt  $e(P'|P_Z) \cdot f(P'|P_Z) = \text{ord}(G_Z(P'|P)) = e(P'|P) \cdot f(P'|P)$  wegen (a). Da  $e(P'|P) = e(P'|P_Z) \cdot e(P_Z|P)$  und  $f(P'|P) = f(P'|P_Z) \cdot f(P_Z|P)$ , gilt

$$e(P_Z|P) = f(P_Z|P) = 1. \quad (4.43)$$

Insbesondere ist  $P'$  die einzige Erweiterung von  $P_Z$  in  $F'$ .

Als nächstes beweisen wir (c): Zuerst eine Notation: Für  $z \in \mathcal{O}_{P'}$  sei  $\bar{z} := z(P') \in F'_{P'}$ , und für  $\psi(T) = \sum z_i T^i \in \mathcal{O}_{P'}[T]$  sei  $\bar{\psi}(T) := \sum \bar{z}_i T^i \in F'_{P'}[T]$ . Nun kommen wir zum eigentlichen Beweis: Da nach unserer generellen Annahme  $K$  vollkommen ist, ist die Erweiterung  $F'_{P'}/F_P$  separabel, also  $F'_{P'} = F_P(\bar{u})$  für ein  $u \in \mathcal{O}_{P'}$ . Die Erweiterung ist galoissch, wenn wir zeigen können, dass  $F'_{P'}$  der Zerfällungskörper eines Polynoms über  $F_P$  ist.  $P'$  ist die einzige Erweiterung von  $P_Z$ , also ist  $\mathcal{O}_{P'}$  der ganze Abschluss von  $\mathcal{O}_{P_Z}$  in  $F'$  und das Minimalpolynom  $\varphi(T) \in Z[T]$  von  $u$  über  $Z$  hat Koeffizienten in  $\mathcal{O}_{P_Z}$ . Da nach (4.43)  $f(P_Z|P) = 1$ , liegt  $\bar{z} \in F_P$  für alle  $z \in \mathcal{O}_{P_Z}$ . Also gilt  $\bar{\varphi}(T) \in F_P[T]$ . Da die Erweiterung  $F'/Z$  galoissch ist, zerfällt  $\varphi(T)$  in Linearfaktoren,  $\varphi(T) = \prod (T - u_i)$  mit  $u_i \in \mathcal{O}_{P'}$ , also gilt

$$\bar{\varphi}(T) = \prod (T - \bar{u}_i) \text{ mit } \bar{u}_i \in F'_{P'}. \quad (4.44)$$

Eine der Nullstellen von  $\bar{\varphi}(T)$  ist  $\bar{u}$ , also ist  $F'_{P'}$  der Zerfällungskörper von  $\bar{\varphi}$  über  $F_P$ .

Sei  $\sigma \in G_Z(P'|P)$  und  $y, z \in \mathcal{O}_{P'}$  mit  $\bar{y} = \bar{z}$ . Dann gilt  $y - z \in P'$ , also gilt  $\sigma(y) - \sigma(z) = \sigma(y - z) \in \sigma(P') = P'$  und  $\sigma(y)(P') = \sigma(z)(P')$ .  $\Phi$  ist also wohldefiniert und ein Homomorphismus. Der Kern von  $\Phi$  ist  $G_T(P'|P)$  entsprechend der Definition der Trägheitsgruppe. Zu zeigen bleibt, dass  $\Phi$  surjektiv ist:

Jeder Automorphismus  $\alpha \in \text{Gal}(F'_{P'}/F_P)$  ist durch das Bild von  $\bar{u}$  eindeutig bestimmt und es muss  $\alpha(\bar{u}) = \bar{u}_i$  (siehe (4.44)). Da  $F'/Z$  galoissch ist, existiert ein  $\sigma \in \text{Gal}(F'/Z) =$

$G_Z(P'|P)$  mit  $\sigma(u) = u_i$  und folglich gilt  $\bar{\sigma} = \alpha$ , also ist  $\Phi$  surjektiv.

(b) Dass  $G_T(P'|P)$  ein Normalteiler von  $G_Z(P'|P)$  ist, ist klar, da es Kern eines Homomorphismus' ist (nach (c)). Wegen (c) und (a) gilt

$$\begin{aligned} f(P'|P) = [F'_{P'} : F_P] &= \text{ord}(\text{Gal}(F'_{P'}/F_P)) \\ &= \text{ord}(G_Z(P'|P))/\text{ord}(G_T(P'|P)) \\ &= (e(P'|P) \cdot f(P'|P))/\text{ord}(G_T(P'|P)). \end{aligned}$$

Also gilt  $\text{ord}(G_T(P'|P)) = e(P'|P)$ .

(d) Direkt aus der Definition folgt, dass die Trägheitsgruppe von  $P'$  über  $P_T$  gleich  $G_T(P'|P)$  ist. Wenden wir (b) zuerst auf die Erweiterung  $F'/T$  und dann auf  $F'/F$  an, so erhalten wir

$$e(P'|P_T) = \text{ord}(G_T(P'|P)) = e(P'|P). \quad (4.45)$$

(d) folgt nun leicht aus (4.43) und (4.45) und der Multiplikativität des Verzweigungsgrades und der relativen Grade. □

Eine andere Charakterisierung des Zerlegungskörpers und der Trägheitskörpers liefert der folgende Satz.

**Satz 4.9.3** *Sei  $F'/F$  eine Galoiserweiterung von Funktionenkörpern,  $P \in \mathbb{P}_F$  eine Stelle und  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$ . Für einen Zwischenkörper  $F \subseteq M \subseteq F'$  sei  $P_M := P' \cap M$ . Dann gilt:*

- (a)  $M \subseteq Z(P'|P) \Leftrightarrow e(P_M|P) = f(P_M|P) = 1$ .
- (b)  $M \supseteq Z(P'|P) \Leftrightarrow P'$  ist die einzige Stelle von  $F'$ , die über  $P_M$  liegt.
- (c)  $M \subseteq T(P'|P) \Leftrightarrow e(P_M|P) = 1$ .
- (d)  $M \supseteq T(P'|P) \Leftrightarrow P_M$  ist total verzweigt in  $F'/M$ .

*Beweis:* Nach Satz 4.9.2 sind alle Implikationen von links nach rechts trivial. Bevor wir uns die Umkehrung überlegen, sei noch bemerkt, dass die Zerlegungsgruppe von  $P'$  über  $P_M$  in  $G_Z(P'|P)$  enthalten ist und gleiches gilt für die Trägheitsgruppe. Dies folgt direkt aus der Definition dieser Gruppen. Hier soll nur (a) bewiesen werden, die anderen Beweise gehen ganz ähnlich.

(a) Angenommen  $e(P_M|P) = f(P_M|P) = 1$ . Dann gilt  $e(P'|P_M) \cdot f(P'|P_M) = e(P'|P) \cdot f(P'|P)$ , also hat die Zerlegungsgruppe von  $P'$  über  $P_M$  dieselbe Ordnung wie  $G_Z(P'|P)$  nach Satz 4.9.2 (a). Aus der obigen Bemerkung folgt, dass  $G_Z(P'|P)$  gleich der Zerlegungsgruppe von  $P'$  über  $P_M$  ist. Insbesondere folgt  $G_Z(P'|P) \subseteq \text{Gal}(F'/M)$ , also gilt  $Z(P'|P) \supseteq M$ .

□

**Definition 4.9.4** Sei  $P \in \mathbb{P}_F$ . Dann heißt  $P$  **vollständig zerlegt** in  $F'$ , wenn  $e(Q|P) = f(Q|P) = 1$  gilt, für alle  $Q \in \mathbb{P}_{F'}$  mit  $Q|P$ .

**Korollar 4.9.5** Sei  $F'/F$  eine endliche, seperable Erweiterung von Funktionenkörpern und seinen  $F_1, F_2$  Zwischenkörper mit  $F' = F_1F_2$ . Dann gilt für  $P \in \mathbb{P}_F$

- (a) Falls  $P$  vollständig zerlegt ist in  $F_1/F$  und  $F_2/F$ , dann zerfällt  $P$  in  $F'/F$ .
- (b) Ist  $P$  unverzweigt in  $F_1/F$  und  $F_2/F$ , dann ist  $P$  unverzweigt in  $F'/F$ .

*Beweis:* (a) Wählen wir eine Galoiserweiterung  $\tilde{F}/F$  mit  $\tilde{F} \supseteq F' \supseteq F$ . Sei  $P'$  eine Stelle von  $F'$ , die über  $P$  liegt. Wählen wir eine Erweiterung  $\tilde{P} \in \mathbb{P}_{\tilde{F}}$  von  $P'$ . Sei  $P_i := P' \cap F_i$  ( $i = 1, 2$ ). Da  $P$  in  $F_i/F$  vollständig zerfällt, gilt  $e(P_i|P) = f(P_i|P) = 1$  für  $i = 1, 2$ . Also gilt  $F_i \subseteq Z(\tilde{P}|P)$  und daher  $F' \subset Z(\tilde{P}|P)$ , also gilt  $e(P'|P) = f(P'|P) = 1$  nach Satz 4.9.3(a). Der Beweis von (b) geht sehr ähnlich und wird daher nicht geführt.

□

Wir wollen nun auf eine ähnliche Art wilde Verzweigungen studieren.

**Definition 4.9.6** Sei  $F'/F$  eine Galoiserweiterung von Funktionenkörpern mit Galoisgruppe  $G = \text{Gal}(F'/F)$ . Betrachten wir eine Stelle  $P \in \mathbb{P}_F$  und eine Erweiterung  $P' \in \mathbb{P}_{F'}$  von  $P$ . Für jedes  $i \geq -1$  definieren wir die  **$i$ -te Verzweigungsgruppe** von  $P'|P$  durch

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

$G_i(P'|P)$  ist klarerweise eine Untergruppe von  $G$ .

**Proposition 4.9.7** Sei  $F'/F$  eine Galoiserweiterung,  $P \in \mathbb{P}_F$ ,  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$  und  $G_i := G_i(P'|P)$ . Dann gilt

- (a)  $G_{-1} = G_Z(P'|P)$  und  $G_0 = G_T(P'|P)$ . Insbesondere gilt  $\text{ord}(G_0) = e(P'|P)$ .
- (b)  $G_{-1} \supseteq G_0 \supseteq \dots \supseteq G_i \supseteq G_{i+1} \supseteq \dots$  und  $G_m = \{id\}$  für  $m$  gross genug.
- (c) Sei  $\sigma \in G_0$ ,  $i \geq 0$  und  $t$  ein primes Element von  $P'$ . Dann gilt

$$\sigma \in G_i \Leftrightarrow v_{P'}(\sigma t - t) \geq i + 1.$$

- (d) Sei  $\text{char}(F) = 0$ . Dann gilt  $G_i = \{id\}$  für alle  $i \geq 1$ . Weiters ist  $G_0 = G_T(P'|P)$  zyklisch.
- (e) Sei  $\text{char}(F) = p > 0$ . Dann ist  $G_1$  ein Normalteiler von  $G_0$ . Die Ordnung von  $G_1$  ist eine Potenz von  $p$  und die Faktorgruppe  $G_0/G_1$  ist zyklisch mit einer Ordnung relativ prim zu  $p$ .

(f) Sei  $\text{char}(F) = p > 0$ . Dann ist  $G_{i+1}$  ein Normalteiler von  $G_i$  für alle  $i \geq 1$ . Die Faktorgruppe  $G_i/G_{i+1}$  ist isomorph zu einer additiven Untergruppe von  $F'_{P'}$ .

*Beweis:* (a) und (b) sind klar.

(c) Betrachten wir  $T$ , den Trägheitskörper von  $P'$  über  $P$  und setzen wir  $P_T = P' \cap T$ ,  $e := e(P'|P)$ , und  $\mathcal{O}_{P_T} = \mathcal{O}_{P'} \cap T$ . Da  $P'|P_T$  total verzweigt ist, bilden die Elemente  $1, t, \dots, t^{e-1}$  eine Ganzheitsbasis für  $F'/P$  bei  $P_T$ . Sei nun  $\sigma \in G_0 = \text{Gal}(F'/T)$  mit  $v_{P'}(\sigma t - t) \geq i+1$  und  $z \in \mathcal{O}_{P'}$ . Wir können  $z$  schreiben als  $z = \sum_{i=0}^{e-1} x_i t^i$  mit  $x_i \in \mathcal{O}_{P_T}$  und erhalten

$$\sigma z - z = \sum_{i=1}^{e-1} x_i ((\sigma t)^i - t^i) = (\sigma t - t) \sum_{i=1}^{e-1} x_i u_i,$$

mit  $u_i = ((\sigma t)^i - t^i)/(\sigma t - t) \in \mathcal{O}_{P'}$ . Daraus folgt  $v_{P'}(\sigma z - z) \geq v_{P'}(\sigma t - t) \geq i+1$ . Also gilt  $\sigma \in G_i$  und das beweist (c).

Im folgenden bezeichne  $(F'_{P'})^*$  die multiplikative Gruppe des Restklassenkörpers, sowie  $F'_{P'}$  die additive. Wir zeigen die Existenz eines Homomorphismus'

$$\chi : G_0 \rightarrow (F'_{P'})^* \text{ mit } \text{Ker}(\chi) = G_1, \quad (4.46)$$

sowie für alle  $i \geq 1$  die Existenz von

$$\psi_i : G_i \rightarrow F'_{P'} \text{ mit } \text{Ker}(\psi_i) = G_{i+1}. \quad (4.47)$$

Die Aussagen (d),(e) und (f) folgen sofort aus der Existenz dieser Homomorphismen. Für (d) beachte man noch, dass keine endliche Untergruppe von  $F'_{P'}$  existiert und daher  $G_i = G_{i+1}$  für alle  $i \geq 1$  gelten muss. Da  $G_i = \{id\}$  ab einem Index, folgt (d).

Wir zeigen zunächst (4.46). Wählen wir ein primes Element  $t$  von  $P'$  und setzen wir für  $\sigma \in G_0$

$$\chi(\sigma) := \frac{\sigma(t)}{t} + P' \in (F'_{P'})^*.$$

$\chi$  hängt nicht von der spezifischen Wahl von  $t$  ab: Sei  $t^* = u \cdot t$  ein anderes primes Element von  $P'$  (also  $v_{P'}(u) = 0$ ). Dann gilt

$$\frac{\sigma(t^*)}{t^*} - \frac{\sigma(t)}{t} = \frac{\sigma(t) \cdot \sigma(u)}{t \cdot u} - \frac{\sigma(t)}{t} = \frac{\sigma(t)}{t} \cdot u^{-1} \cdot (\sigma(u) - u) \in P'.$$

Man beachte, dass wegen  $\sigma \in G_0$  gilt, dass  $\sigma(u) - u \in P'$ . Wir zeigen, dass  $\chi$  ein Homomorphismus ist: Sei  $\sigma, \tau \in G_0$ . Dann ist  $\tau(t)$  ein primes Element von  $P'$  und daher

$$\chi(\sigma\tau) = \frac{(\sigma\tau)(t)}{t} + P' = \frac{\sigma(\tau(t))}{\tau(t)} \cdot \frac{\tau(t)}{t} + P' = \chi(\sigma)\chi(\tau).$$

Ein Element  $\sigma \in G_0$  liegt im Kern von  $\chi$  genau dann, wenn  $(\sigma(t)/t) - 1 \in P'$ , also  $v_{P'}(\sigma(t) - t) \geq 2$  gilt. Also gilt  $\text{ker}(\chi) = G_1$ . Das beweist (4.46).

Wir wollen noch (4.47) zeigen: Sei  $i \geq 1$  und  $\sigma \in G_i$ . Dann ist  $\sigma(t) = t + t^{i+1} \cdot u_\sigma$  für ein  $u_\sigma \in \mathcal{O}_{P'}$ . Wir definieren  $\psi_i$  durch

$$\psi_i(\sigma) := u_\sigma + P'.$$

Die Homomorphieeigenschaft von  $\psi_i$  rechnet man unmittelbar nach, die Aussage über den Kern ist klar. □

Das folgende Korollar erwähne ich ohne Beweis (der Beweis ist dem von Satz 4.9.3 sehr ähnlich):

**Korollar 4.9.8** *Sei  $F'/F$  eine Galoiserweiterung mit  $\text{char}(F) = p > 0$ ,  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$ . Sei weiters  $V_1(P'|P)$  der Fixkörper der ersten Verzweigungsgruppe  $G_1(P'|P)$  und  $P_M := P' \cap M$  für einen Zwischenkörper  $F \subseteq M \subseteq F'$ . Dann gilt:*

$$(a) \quad M \subseteq V_1(P'|P) \Leftrightarrow \text{ggT}(e(P_M|P), p) = 1.$$

$$(b) \quad M \supseteq V_1(P'|P) \Leftrightarrow P_M \text{ ist total verzweigt in } F'/M \text{ und } e(P'|P_M) \text{ ist eine Potenz von } p.$$

Ohne Beweis möchte ich noch den folgenden Satz erwähnen. Der Beweis findet sich z.B. in [38].

**Satz 4.9.9 (Hilbertsche Differentenformel)** *Sei  $F'/F$  eine Galoiserweiterung von Funktionenkörpern,  $P \in \mathbb{P}_F$  und  $P' \in \mathbb{P}_{F'}$  mit  $P'|P$ . Dann gilt*

$$d(P'|P) = \sum_{i=0}^{\infty} (\text{ord}(G_i(P'|P)) - 1).$$

Wir wollen nun das **Lemma von Abhyankar** beweisen. Dazu benötigen wir zuerst ein gruppentheoretisches Lemma. Die hier verwendeten gruppentheoretischen Begriffe werden z.B. in [27] oder [1] erklärt.

**Lemma 4.9.10** *Sei  $G$  eine endliche Gruppe und  $U$  ein Normalteiler, sodass  $\text{ord}(U) = p^n$ , wobei  $p$  eine Primzahl oder 1 ist. Weiters soll  $G/U$  eine zyklische Gruppe sein mit  $\text{ggT}(\text{ord}(G/U), p) = 1$ . Angenommen  $H_1$  sei eine Untergruppe von  $G$  mit  $p^n | \text{ord}(H_1)$ . Dann gilt für jede Untergruppe  $H_2 \subseteq G$*

$$\text{ord}(H_1 \cap H_2) = \text{ggT}(\text{ord}(H_1), \text{ord}(H_2)).$$

*Beweis:* Es gilt klarerweise, dass sowohl die Ordnung von  $H_1$ , also auch die Ordnung von  $H_2$  von der Ordnung von  $H_1 \cap H_2$  geteilt werden, also gilt

$$\text{ord}(H_1 \cap H_2) \mid \text{ggT}(\text{ord}(H_1), \text{ord}(H_2)).$$

$U$  ist ein Normalteiler von  $G$  und daher die einzige  $p$ -Sylow-Untergruppe von  $G$ . Es gilt  $\text{ord}(H_1) = p^n a_1$  mit  $ggT(a_1, p) = 1$  und  $\text{ord}(H_2) = p^m a_2$  mit  $ggT(a_2, p) = 1$  und  $m \leq n$ . Daraus folgt  $ggT(\text{ord}(H_1), \text{ord}(H_2)) = p^m d$  mit  $d := ggT(a_1, a_2)$ . Es genügt zu zeigen, dass

$$H_1 \cap H_2 \text{ enthält eine Untergruppe der Ordnung } p^m, \text{ und} \quad (4.48)$$

$$H_1 \cap H_2 \text{ enthält ein Element, dessen Ordnung ein Vielfaches von } d \text{ ist.} \quad (4.49)$$

Wir zeigen zuerst (4.48): Da  $p^n \mid \text{ord}(H_1)$  existiert eine  $p$ -Sylow Untergruppe von  $H_1$  der Ordnung  $p^n$ . Da aber  $\text{ord}(U) = p^n$  und  $U$  die einzige  $p$ -Sylowgruppe von  $G$  ist, gilt  $U \subseteq H_1$ . Wählen wir eine  $p$ -Sylowgruppe  $V$  von  $H_2$ . Dann gilt  $\text{ord}(V) = p^m$  und  $V \subseteq U \subseteq H_1$ . Damit ist (4.48) bewiesen.

Um (4.49) zu zeigen, betrachten wir die kanonische Restklassenprojektion  $\pi$  von  $G$  auf  $G/U$ . Es gilt  $\text{ord}(\pi(H_1)) = a_1$  und  $\text{ord}(\pi(H_2)) = a_2$ . Da  $G/U$  zyklisch ist, gilt  $\text{ord}(\pi(H_1) \cap \pi(H_2)) = d$ . Wählen wir nun  $g_1 \in H_1$  und  $g_2 \in H_2$  sodass  $\pi(g_1) = \pi(g_2)$  die Untergruppe  $\pi(H_1) \cap \pi(H_2)$  erzeugt. Dann gilt  $g_1^{-1}g_2 \in U \subseteq H_1$ , also  $g_2 \in H_1 \cap H_2$  und die Ordnung von  $g_2$  ist ein Vielfaches von  $d$ .

□

**Satz 4.9.11 (Lemma von Abhyankar)** *Sei  $F'/F$  eine endliche, separable Funktionenkörpererweiterung. Seien  $F_1, F_2$  Unterkörper von  $F'$  mit  $F' = F_1 F_2$  und  $F \subseteq F_1, F_2$ . Sei  $P' \in \mathbb{P}_{F'}$  eine Erweiterung von  $P \in \mathbb{P}_F$  und  $P_i := P' \cap F_i$ ,  $i = 1, 2$ . Sei zumindest eine der Erweiterungen  $P_1|P$  oder  $P_2|P$  zahm. Dann gilt*

$$e(P'|P) = kgV(e(P_1|P), e(P_2|P)).$$

*Beweis:* Wählen wir eine Galoiserweiterung  $F^*/F$  mit  $F' \subseteq F^*$  und eine Erweiterung  $P^* \in \mathbb{P}_{F^*}$  von  $P'$ . Sei  $G := G_T(P^*|P)$  und  $H_i := G_T(P^*|P_i)$ . Da zumindest eine Erweiterung  $P_i|P$  zahm ist, können wir o.B.d.A. annehmen, dass  $ggT(e(P_1|P), p) = 1$  gilt. Die Gruppen  $G, H_1$  und  $H_2$  erfüllen die Voraussetzungen von Lemma 4.9.10 und daher gilt

$$\text{ord}(H_1 \cap H_2) = ggT(\text{ord}(H_1), \text{ord}(H_2)).$$

Wegen  $F' = F_1 F_2$  gilt  $\text{Gal}(F^*/F') = \text{Gal}(F^*/F_1) \cap \text{Gal}(F^*/F_2)$  und  $G_T(P^*|P') = G_T(P^*|P_1) \cap G_T(P^*|P_2) = H_1 \cap H_2$ . Wir haben

$$\begin{aligned} e(P^*|P') &= \text{ord}(G_T(P^*|P')) = \text{ord}(H_1 \cap H_2) \\ &= ggT(\text{ord}(H_1), \text{ord}(H_2)) = ggT(e(P^*|P_1), e(P^*|P_2)) \\ &= ggT(e(P^*|P') \cdot e(P'|P_1), e(P^*|P') \cdot e(P'|P_2)) \\ &= e(P^*|P') \cdot ggT(e(P'|P_1), e(P'|P_2)). \end{aligned}$$

Es gilt also

$$ggT(e(P'|P_1), e(P'|P_2)) = 1. \quad (4.50)$$

Andererseits gilt

$$e(P'|P) = e(P'|P_1) \cdot e(P_1|P) = e(P'|P_2) \cdot e(P_2|P). \quad (4.51)$$

Aus (4.50) und (4.51) folgt

$$e(P'|P) = kgV(e(P_1|P), e(P_2|P)).$$

□

## 4.10 Die Drinfeld-Vladut Schranke

### 4.10.1 Die Hasse-Weil Schranke

Im Folgenden nehmen wir an, dass  $F/\mathbb{F}_q$  ein Funktionenkörper über einem endlichen Körper  $\mathbb{F}_q$  vom Geschlecht  $g$  ist. Beweise zu den in diesem Abschnitt getätigten Aussagen findet man in [38] oder in [34]. Sei

$$A_n := \text{card}(\{A \in \mathcal{D}_F : A \geq 0 \text{ und } \deg(A) = n\}).$$

**Definition 4.10.1** Wir definieren die **Zetafunktion** eines Funktionenkörpers  $F/\mathbb{F}_q$  durch

$$Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]].$$

Zur Motivation: Die klassische Zetafunktion ist definiert durch

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s}, \quad s \in \mathbb{C}, \text{Re}(s) > 1.$$

Wir fassen  $Z(t)$  als Analogon zu der klassischen Zetafunktion auf, indem wir die **absolute Norm** eines Divisors  $A \in \mathcal{D}_F$  definieren durch

$$\mathcal{N}(A) := q^{\deg(A)}.$$

Die Funktion

$$\zeta_F(s) := Z_F(q^{-s})$$

lässt sich dann schreiben als

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in \mathcal{D}_F, A \geq 0} \mathcal{N}(A)^{-s}.$$

Weitere motivierende Beispiele liefert die Theorie der Zetafunktionen algebraischer Zahlkörper.

**Definition 4.10.2** Sei  $\mathcal{C}_F^0 := \{[A] \in \mathcal{C}_F : \deg[A] = 0\}$ . Dann heißt  $h := \text{ord}(\mathcal{C}_F^0)$  **Klassenzahl** von  $F/\mathbb{F}_q$ .

Man kann zeigen, dass mit unseren Voraussetzungen immer  $h < \infty$  gilt, siehe [38], Kap. V. Wir listen einige grundlegende Eigenschaften der Zetafunktion auf:

**Proposition 4.10.3**

(a) Die Potenzreihe  $Z(t)$  ist konvergent für  $|t| < q^{-1}$ , und für diese  $t$  gilt

$$Z(t) = \frac{1}{(1-t)(1-qt)}, \quad \text{falls } g = 0, \text{ und}$$

$Z(t) = F(t) + G(t)$  mit

$$F(t) = \frac{1}{q-1} \sum_{\substack{[C] \in \mathcal{C}_F \\ 0 \leq \deg[C] \leq 2g-2}} q^{\dim[C]} \cdot t^{\deg[C]}, \text{ und}$$

$$G(t) = \frac{h}{q-1} \left( q^g t^{2g-1} \frac{1}{1-qt} - \frac{1}{1-t} \right).$$

(b) Es gilt  $Z(t) = \prod_{P \in \mathbb{P}_F} (1 - t^{\deg(P)})^{-1}$ .

(c) Es gilt  $Z(t) = q^{g-1} t^{2g-2} Z\left(\frac{1}{qt}\right)$ .

(d)  $Z(t)$  besitzt eine meromorphe Fortsetzung auf  $\mathbb{C}$ .

**Definition 4.10.4** Die Funktion

$$L(T) := (1-t)(1-qt)Z(t)$$

heißt **L-Polynom** von  $F/\mathbb{F}_q$ .

**Satz 4.10.5** Es gilt

(a)  $L(t)$  ist ein Polynom vom Grad  $2g$ .

(b)  $L(t) = q^g t^{2g} L\left(\frac{1}{qt}\right)$ .

(c) Wir schreiben  $L(t) = a_0 + a_1 t + \dots + a_{2g} t^{2g}$ . Dann gilt

(1)  $a_0 = 1$  und  $a_{2g} = q^g$ .

(2)  $a_{2g-i} = q^{g-i} a_i$  für  $0 \leq i \leq g$ .

(3)  $a_1 = N - (q+1)$ , wobei  $N$  die Anzahl der Stellen vom Grad 1 ist.

(d)

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t).$$

Die Zahlen  $\alpha_i$  sind ganzzahligebräusche Zahlen und sie können in einer Reihenfolge angeordnet werden, sodass  $\alpha_i \alpha_{g+i} = q$  für  $i = 1, \dots, g$ .

(e) Sei  $L_r(t)$  das  $L$ -Polynom der Konstantenkörpererweiterung  $F_r = F\mathbb{F}_{q^r}$ . Dann gilt

$$L_r(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t),$$

wobei die  $\alpha_i$ 's dieselben sind, wie in (d).

Sei  $F_r := F\mathbb{F}_{q^r}$ . Dann definieren wir

$$N_r := N_r(F) := \text{card}\{P \in \mathbb{P}_{F_r} : \text{deg}(P) = 1\}.$$

**Korollar 4.10.6** Es gilt für  $r \geq 1$

$$N_r = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r,$$

wobei die  $\alpha_i$ 's wie in Satz 4.10.5 definiert sind. Insbesondere gilt

$$N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

*Beweis:* Nach Satz 4.10.5 (c) (3) ist der Koeffizient bei  $t$  von  $L_r(t)$  gleich  $N_r - (q^r + 1)$ . Andererseits folgt aus der Faktorisierung in Satz 4.10.5 (e), dass der Koeffizient gleich  $-\sum_{i=1}^{2g} \alpha_i^r$  ist.

□

Nun kommen wir zum **Satz von Hasse-Weil**. Dieser Satz ist auch als die Riemannsche Vermutung für Funktionenkörper bekannt und lautet wie folgt:

**Satz 4.10.7 (Hasse-Weil)** Sei  $F/\mathbb{F}_q$  ein Funktionenkörper,  $L(t)$  sein  $L$ -Polynom, und  $\alpha_1, \dots, \alpha_{2g}$  die Reziprokwerte seiner Nullstellen. Dann gilt:

$$|\alpha_i| = q^{1/2} \text{ für } i = 1, \dots, 2g.$$

Aus dem Satz von Hasse-Weil folgt

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2}.$$

Da  $|q^{-s}| = q^{-\operatorname{Re}(s)}$  heißt das

$$\zeta_F(s) = 0 \Rightarrow \operatorname{Re}(s) = 1/2.$$

Damit sollte die Bezeichnung „Riemannsche Vermutung für Funktionenkörper“ klar sein. Eine direkte Konsequenz aus dem Satz von Hasse-Weil ist die sogenannte **Hasse-Weil Schranke**.

**Satz 4.10.8 (Hasse-Weil Schranke)** Für die Anzahl  $N = N(F)$  der Stellen von Grad 1 gilt

$$|N - (q + 1)| \leq 2gq^{1/2}.$$

*Beweis:* Folgt direkt aus dem Satz von Hasse-Weil und dem Korollar 4.10.6. □

## 4.10.2 Die Drinfeld-Vladut Schranke

Wir wollen einige Folgerungen aus dem Satz von Hasse-Weil ziehen. Dazu schreiben wir für  $i = 1, \dots, 2g$

$$w_i := \alpha_i q^{-1/2},$$

$\alpha_1, \dots, \alpha_i$  sind dabei die Reziprokwerte der Nullstellen des L-Polynoms von  $F/\mathbb{F}_q$ . Es gilt  $|w_i| = 1$  nach dem Satz von Hasse-Weil und wir können annehmen (siehe Satz 4.10.5 (d)), dass

$$w_{g+i} = \overline{w_i} = w_i^{-1} \text{ für } i = 1, \dots, g.$$

Nach dem Korollar 4.10.6 folgt

$$N_r q^{-r/2} = q^{r/2} + q^{-r/2} - \sum_{i=1}^g (w_i^r + w_i^{-r}). \quad (4.52)$$

Seien reelle Zahlen  $c_1, \dots, c_g$  gegeben. Multiplizieren wir (4.52) mit  $c_r$ , so erhalten wir

$$N_1 c_r q^{-r/2} = c_r q^{r/2} + c_r q^{-r/2} - \sum_{i=1}^g c_r (w_i^r + w_i^{-r}) - (N_r - N_1) c_r q^{-r/2}. \quad (4.53)$$

Summiert man nun (4.53) für  $r = 1, \dots, m$  auf, so erhält man

$$\begin{aligned} & N_1 \lambda_m(q^{-1/2}) = \\ & = \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g - \sum_{i=1}^g f_m(w_i) - \sum_{r=1}^m (N_r - N_1) c_r q^{-r/2}, \end{aligned} \quad (4.54)$$

wobei

$$\lambda_m(t) := \sum_{r=1}^m c_r t^r$$

und

$$f_m(t) := 1 + \lambda_m(t) + \lambda_m(t^{-1})$$

für  $t \in \mathbb{C}$ . Es gilt  $f_m(t) \in \mathbb{R}$  für  $|t| = 1$ .

Indem wir die Werte  $c_i$  klug wählen, leiten wir nun die **Drinfeld-Vladut Schranke** her. Zuvor wollen wir uns noch einige Definitionen aus dem Kapitel 3.3 in Erinnerung rufen. Für einen Funktionenkörper  $F$  über  $\mathbb{F}_q$  sei

$$N(F) := \text{card}(\{P \in \mathbb{P}_F : \text{deg}(P) = 1\}),$$

und

$$N_q(g) := \max\{N(F) : F \text{ ist ein Funktionenkörper über } \mathbb{F}_q \text{ vom Geschlecht } g.\}$$

Weiters sei

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

Aus der Hasse-Weil Schranke folgt sofort  $\frac{N}{g} \leq 2q^{1/2}$ , und damit

$$A(q) \leq 2q^{1/2}.$$

Diese Abschätzung wollen wir verbessern.

**Proposition 4.10.9** *Seien  $c_1, \dots, c_m \in \mathbb{R}$  mit*

- (1)  $c_r \geq 0$  für alle  $r = 1, \dots, m$ , und es existiert ein  $i$  mit  $c_i > 0$ .
- (2)  $f_m(t) \geq 0$  für alle  $t \in \mathbb{C}$  mit  $|t| = 1$ .

Dann gilt

$$N \leq \frac{g}{\lambda_m(q^{-1/2})} + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + 1. \quad (4.55)$$

*Beweis:* Es gilt  $N = N_1 \leq N_r$  für alle  $r \geq 1$ , also gilt nach (4.54) und den Annahmen (1) und (2)

$$N \cdot \lambda_m(q^{-1/2}) \leq \lambda_m(q^{1/2}) + \lambda_m(q^{-1/2}) + g.$$

Dividiert man durch  $\lambda_m(q^{-1/2})$ , so erhält man das Gewünschte (man beachte, dass wegen (1)  $\lambda_m(q^{-1/2}) > 0$  gilt).

□

**Satz 4.10.10 (Drinfeld-Vladut Schranke)**

$$A(q) \leq q^{1/2} - 1.$$

*Beweis:* Setzen wir

$$c_r := 1 - \frac{r}{m} \quad (r = 1, \dots, m).$$

Es gilt für  $t \neq 1$ ,

$$\lambda_m(t) = \sum_{r=1}^m \left(1 - \frac{r}{m}\right) t^r = \frac{t}{(1-t)^2} \left(\frac{t^m - 1}{m} + 1 - t\right) \quad (4.56)$$

und

$$f_m(t) = 1 + \lambda_m(t) + \lambda_m(t^{-1}) = \frac{2 - (t^m + t^{-m})}{m(t-1)(t^{-1}-1)}. \quad (4.57)$$

Da  $t^{-1} = \bar{t}$  für  $|t| = 1$  gilt, folgt aus (4.57)  $f_m(t) \geq 0$  für alle  $t \in \mathbb{C}$  mit  $|t| = 1$ . Wir können also die obige Proposition anwenden und erhalten

$$\frac{N}{g} \leq \frac{1}{\lambda_m(q^{-1/2})} + \frac{1}{g} \left(1 + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})}\right). \quad (4.58)$$

Aus (4.56) folgt sofort

$$\lim_{m \rightarrow \infty} \lambda_m(q^{-1/2}) = \frac{1}{q^{1/2} - 1}.$$

Daher existiert für alle  $\varepsilon > 0$  ein  $m_0$  mit

$$\lambda_{m_0}(q^{-1/2})^{-1} < q^{1/2} - 1 + \varepsilon/2.$$

Wählen wir nun  $g_0$  so, dass

$$\frac{1}{g_0} \left(1 + \frac{\lambda_{m_0}(q^{1/2})}{\lambda_{m_0}(q^{-1/2})}\right) < \varepsilon/2.$$

Dann gilt für jedes  $g \geq g_0$  wegen (4.58)

$$\frac{N}{g} < q^{1/2} - 1 + \varepsilon,$$

und daher

$$A(q) \leq q^{1/2} - 1.$$

□

# Kapitel 5

## Funktionskörpertürme

Dieses Kapitel soll eine Einführung in die Theorie der Funktionskörpertürme geben. Wir haben im Kapitel 3 die Grösse  $A(q)$  betrachtet, im speziellen für gerade Primzahlpotenzen  $q$ , und gesehen, dass man mit einer Folge von Funktionskörpern  $F_n$ , die die Gleichung

$$\lim_{n \rightarrow \infty} \frac{N(F_n)}{g(F_n)} = \sqrt{q} - 1$$

erfüllt ( $g(F_n)$  bezeichne im Folgenden das Geschlecht von  $F_n$ ), Codes konstruieren kann, die die Gilbert-Varshamov Schranke übertreffen. Ziel dieses Kapitels ist es, zwei Beispiele für derartige Folgen von Funktionskörpern zu geben.

### 5.1 Grundlagen und Definitionen

Wir beginnen mit der Definition eines Funktionskörperturmes. Die Definitionen gehen im wesentlichen auf H. Stichtenoth und A. Garcia zurück (siehe [16]).

**Definition 5.1.1** *Ein Funktionskörperturn über  $\mathbb{F}_q$  ist eine unendliche Folge  $\mathcal{F} = (F_n)_{n \in \mathbb{N}}$  von Funktionskörpern  $F_n/\mathbb{F}_q$  mit vollem Konstantenkörper  $\mathbb{F}_q$ , sodass*

(i)  $F_0 \subseteq F_1 \subseteq F_2 \subseteq \dots$  und für jedes  $n \geq 1$  ist die Körpererweiterung  $F_n/F_{n-1}$  separabel und es gilt  $[F_n : F_{n-1}] > 1$ ,

(ii)  $g(F_j) > 1$  für ein  $j \geq 0$ .

**Bemerkung 5.1.2** *Diese Definition ist nicht immer einheitlich, so benützen sowohl H. Stichtenoth, als auch J. Wulftange zeitweise eine etwas andere, im Wesentlichen äquivalente Definition, siehe [43, 15].*

Das erste, was wir zeigen werden, ist, dass für einen gegebenen Funktionskörperturn  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  der Grenzwert  $\lim_{i \rightarrow \infty} N(F_i)/g(F_i)$  immer existiert.

**Definition 5.1.3** *Sei  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  ein Turm über  $\mathbb{F}_q$ . Dann heißt*

(i)

$$\nu(\mathcal{F}) := \lim_{i \rightarrow \infty} \frac{N(F_i)}{[F_i : F_0]}$$

die **Zerfällungsrate** von  $\mathcal{F}$ , und

(ii)

$$\gamma(\mathcal{F}) := \lim_{i \rightarrow \infty} \frac{g(F_i)}{[F_i : F_0]}$$

das **Geschlecht** von  $\mathcal{F}$ .

Eine direkte Folgerung aus der Hilbertschen Fundamentalgleichung ist das folgende Lemma.

**Lemma 5.1.4** Sei  $E/\mathbb{F}_q$  eine Funktionenkörpererweiterung eines Funktionenkörpers  $F/\mathbb{F}_q$  und sei  $t$  die Anzahl der Stellen vom Grad 1 von  $F/\mathbb{F}_q$ , die in  $E/F$  vollständig zerfallen. Dann gilt:

$$t[E : F] \leq N(E) \leq [E : F]N(F).$$

Damit können wir nun das Folgende beweisen:

**Lemma 5.1.5** Die Limiten  $\nu(\mathcal{F})$ , und  $\gamma(\mathcal{F})$  existieren, und es gilt

$$0 \leq \nu(\mathcal{F}) < \infty \text{ und } 0 < \gamma(\mathcal{F}) \leq \infty.$$

*Beweis:* Wir beweisen zuerst die Existenz von  $\nu(\mathcal{F})$ . Für  $i \geq 1$  haben wir

$$\frac{N(F_i)/[F_i : F_0]}{N(F_{i-1})/[F_{i-1} : F_0]} \leq \frac{N(F_i)}{[F_i : F_{i-1}]N(F_{i-1})} \leq 1$$

wegen Lemma 5.1.4, also ist die Folge  $\left(\frac{N(F_i)}{[F_i : F_0]}\right)_{i \geq 0}$  monoton fallend und folglich konvergent. Weiters gilt klarerweise  $0 \leq \nu(\mathcal{F}) < \infty$ .

Für die Aussage zum Geschlecht, betrachten wir die Folge  $\left(\frac{g(F_i)-1}{[F_i : F_0]}\right)_{i \geq 0}$ . Wegen der Hurwitzschen Geschlechtsformel gilt

$$\begin{aligned} g(F_{i+1}) - 1 &= [F_{i+1} : F_i](g(F_i) - 1) + \frac{1}{2} \deg(\text{Diff}(F_{i+1}/F_i)) \\ &\geq \frac{[F_{i+1} : F_0]}{[F_i : F_0]}(g(F_i) - 1). \end{aligned}$$

Die Folge  $\left(\frac{g(F_i)-1}{[F_i : F_0]}\right)_{i \geq 0}$  ist also monoton wachsend, und hat denselben Grenzwert  $\gamma(\mathcal{F})$  wie  $\left(\frac{g(F_i)}{[F_i : F_0]}\right)_{i \geq 0}$ . Die Aussage  $0 < \gamma(\mathcal{F}) \leq \infty$  ist trivial.

□

Nun macht die folgende Definition Sinn:

**Definition 5.1.6** Sei  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  ein Funktionenkörperturm. Wir definieren

$$\lambda(\mathcal{F}) := \lim_{i \rightarrow \infty} \frac{N(F_i)}{g(F_i)} = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})}.$$

**Lemma 5.1.7** Es gilt für einen Funktionenkörperturm  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  über  $\mathbb{F}_q$

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

*Beweis:* Die linke Abschätzung folgt aus dem Lemma 5.1.5, die rechte ist nichts anderes als die Drinfeld-Vladut Schranke.

□

**Definition 5.1.8** Sei  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  ein Funktionenkörperturm über  $\mathbb{F}_q$ . Dann heißt  $\mathcal{F}$

- (i) **asymptotisch schlecht**, falls  $\lambda(\mathcal{F}) = 0$ ,
- (ii) **asymptotisch gut**, falls  $\lambda(\mathcal{F}) > 0$ , und
- (iii) **asymptotisch optimal**, falls  $\lambda(\mathcal{F}) = \sqrt{q} - 1$ .

**Definition 5.1.9** Ein Funktionenkörperturm  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  heißt

- (i) **zahm**, falls alle Erweiterungen  $F_n/F_0$  zahm sind.
- (ii) **wild**, falls  $\mathcal{F}$  nicht zahm ist.

Meistens betrachtet man rekursive Türme:

**Definition 5.1.10** Sei  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  ein Funktionenkörperturm über  $\mathbb{F}_q$ .  $\mathcal{F}$  heißt **rekursiv**, falls ein  $f(x, y) \in \mathbb{F}_q[x, y]$  existiert, mit

$$F_{i+1} = F_i(x_{i+1}) \text{ mit } f(x_i, x_{i+1}) = 0 \text{ für } i \geq 0,$$

und  $F_0 = \mathbb{F}_q(x_0)$ .

$\mathcal{F}$  heißt **gerade**, falls  $\deg_x(f) = \deg_y(f)$ , ansonsten heißt  $\mathcal{F}$  **schief**.

**Bemerkung 5.1.11** Man kann zeigen, dass schiefe Türme immer asymptotisch schlecht sind (siehe [17]).

**Bemerkung 5.1.12** *Es ist eine schwierige Aufgabe, zu bestimmen ob eine Folge von Funktionenkörpern  $(F_n)_{n \geq 0}$ , die durch  $F_{i+1} = F_i(x_{i+1})$  gegeben ist, mit  $f(x_i, x_{i+1}) = 0$  tatsächlich einen Turm definiert, d.h. dass  $f$  immer irreduzibel bleibt. Es existieren in diese Richtung keine allgemeinen Resultate, ausser für gewisse Klassen von Türmen (z.B. Fermattürme, siehe [43], oder auch gewisse Kummertürme vom Grad 2, siehe [15]). Man beweist solche Resultate meistens, indem man zeigt, dass in jeder Erweiterung  $F_{n+1}/F_n$  eine Stelle verzweigt.*

**Definition 5.1.13** *Sei  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  ein Funktionenkörperturm. Dann definieren wir:*

- (i)  $V(\mathcal{F}/F_0) := \{P \in \mathbb{P}_{F_0} : P \text{ ist verzweigt in einer Erweiterung } F_n/F_0 \text{ für ein } n \geq 0\}$ , den **Verzweigungsort**, und
- (ii)  $S(\mathcal{F}/F_0) := \{P \in \mathbb{P}_{F_0} : \deg(P) = 1 \text{ und } P \text{ zerfällt vollständig in allen Erweiterungen } F_n/F_0\}$ , den **Zerfallungsort**

von  $\mathcal{F}$ .

Entsprechend sind der  $F_k$ -Verzweigungsort  $V(\mathcal{F}/F_k)$ , und der  $F_k$ -Zerfallungsort  $S(\mathcal{F}/F_k)$  für  $k \in \mathbb{N}$  definiert.

**Lemma 5.1.14** *Sei  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  ein Funktionenkörperturm über  $\mathbb{F}_q$  und gelte  $S(\mathcal{F}/F_0) \neq \emptyset$ . Dann gilt*

$$\nu(\mathcal{F}) \geq t > 0,$$

mit  $t := \text{card}(S(\mathcal{F}/F_0))$ .

*Beweis:* Sei  $P \in S(\mathcal{F}/F_0)$ . Dann liegen  $[F_n : F_0]$  Stellen vom Grad 1 von  $F_n$  über  $P$  in der Erweiterung  $F_n/F_0$  für alle  $n \geq 0$ . Also gilt  $N(F_n) \geq t[F_n : F_0]$ . Die Aussage folgt nun direkt aus der Definition von  $\nu(\mathcal{F})$ .

□

## 5.2 Zahme Türme

Wir behandeln einige Resultate über zahme Funktionenkörpertürme. Der wesentliche Vorteil eines zahmen Turmes ist, dass man mit der Dedekindschen Differentenformel ein wichtiges Werkzeug zur Bestimmung der Differenten und damit des Geschlechts in der Hand hat. Für wilde Türme hat man das nicht und man muss in der Regel um einiges mehr an Rechenarbeit investieren um das Geschlecht berechnen zu können. Wir wollen uns für diesen Abschnitt einen zahmen Funktionenkörperturm  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  über  $\mathbb{F}_q$  fixieren.

**Definition 5.2.1** *Sei die Menge  $V(\mathcal{F}/F_0)$  endlich. Dann heißt  $\mathcal{F}$  von **endlichem Verzweigungstyp**.*

**Lemma 5.2.2** *Sei  $\mathcal{F}$  ein zahmer Turm von endlichem Verzweigungstyp. Dann gilt*

$$\gamma(\mathcal{F}) \leq g(F_0) + \frac{s-2}{2},$$

mit  $s := \sum_{P \in V(\mathcal{F}/F_0)} \deg(P)$ .

*Beweis:* Sei  $P \in \mathbb{P}_{F_0}$  und  $Q \in \mathbb{P}_{F_n}$  mit  $Q|P$ . Da der Turm zahm ist, gilt  $d(Q|P) = e(Q|P) - 1$ . Wir erhalten

$$\begin{aligned} \deg(\text{Diff}(F_n/F_0)) &= \sum_{P \in V(\mathcal{F}/F_0)} \sum_{Q|P} d(Q|P) \deg(Q) \\ &\leq \sum_{P \in V(\mathcal{F}/F_0)} \left( \sum_{Q|P} e(Q|P) f(Q|P) \right) \deg(P) \\ &= [F_n : F_0] s. \end{aligned}$$

Aus der Hurwitzschen Geschlechtsformel folgt

$$2g(F_n) - 2 \leq [F_n : F_0](2g(F_0) - 2 + s)$$

und daraus folgt die Behauptung. □

**Korollar 5.2.3** *Sei  $\mathcal{F}$  ein zahmer Turm von endlichem Verzweigungstyp und gelte  $S(\mathcal{F}/F_0) \neq \emptyset$ . Dann gilt mit  $s := \sum_{P \in V(\mathcal{F}/F_0)} \deg(P)$  und  $t := \text{card}(S(\mathcal{F}/F_0))$*

$$\lambda(\mathcal{F}) \geq \frac{2t}{2g(F_0) + s - 2}.$$

*Insbesondere ist  $\mathcal{F}$  asymptotisch gut.*

*Beweis:* Die Aussage ist eine direkte Folgerung aus Lemma 5.1.14 und Lemma 5.2.2. □

Es gilt auch eine Umkehrung unter der Voraussetzung, dass alle Erweiterungen  $F_n/F_0$  galoissch sind. Mann nennt dann  $\mathcal{F}$  **galoissch**.

**Satz 5.2.4** *Sei  $\mathcal{F}$  ein asymptotisch guter, zahmer, galoisscher Turm. Dann ist  $\mathcal{F}$  von endlichem Verzweigungstyp und es gilt  $S(\mathcal{F}/F_n) \neq \emptyset$  für ein  $n \geq 0$ .*

*Beweis:* Angenommen, der Verzweigungsort sei unendlich. Dann gibt es Stellen  $P_{n_1}, P_{n_2}, \dots \in \mathbb{P}_{F_0}$  ( $n_1 \leq n_2 \leq \dots$ ), sodass  $P_{n_i}$  verzweigt ist in der Erweiterung  $F_{n_i}/F_0$ . Sei  $Q_i$  eine Stelle aus  $F_{n_i}$  mit  $Q_i|P_{n_i}$ . Dann gilt

$$\begin{aligned}
 \deg(\text{Diff}(F_{n_i}/F)) &= \sum_{P \in \mathbb{P}_{F_0}} \sum_{P'|P} d(P'|P) \deg(P') \\
 &= \sum_{P \in \mathbb{P}_{F_0}} \sum_{P'|P} (e(P'|P) - 1) \cdot \deg(P') \\
 &= \sum_{P \in \mathbb{P}_{F_0}} r_P \cdot (e(P) - 1) \cdot f(P) \cdot \deg(P) \\
 &= [F_{n_i} : F_0] \sum_{P \in \mathbb{P}_{F_0}} \frac{(e(P) - 1)}{e(P)} \cdot \deg(P) \\
 &\geq [F_{n_i} : F_0] \sum_{j=1}^i \frac{(e(P_{n_j}) - 1)}{e(P_{n_j})} \geq \frac{i}{2} [F_{n_i} : F_0].
 \end{aligned}$$

Die zweite Zeile folgt aus der Dedekindschen Differentenformel, die dritte Zeile folgt aus Korollar 4.8.2, man beachte auch die Notation wie in Kapitel 4.8. Die vierte Zeile folgt aus der Hilbertschen Fundamentalformel. Der Rest ist klar. Aus der Hurwitzschen Geschlechtsformel folgt

$$2g(F_{n_i}) - 2 \geq [F_{n_i} : F_0](2g(F_0) - 2) + \frac{i}{2}[F_{n_i} : F_0]$$

und daraus folgt  $\gamma(\mathcal{F}) = \infty$ . Das impliziert aber  $\lambda(\mathcal{F}) = 0$ . Widerspruch.

Nun zeigen wir, dass  $S(\mathcal{F}/F_n) \neq \emptyset$  für ein  $n \geq 0$ .

Sei  $M$  die Menge der Stellen vom Grad 1 von  $F_0$ . Für  $P \in M$  und  $i \in \mathbb{N}$  definieren wir  $r_i(P)$  als die Anzahl an Stellen vom Grad 1, die über  $P$  in der Erweiterung  $F_i/F_0$  liegen und setzen

$$\mu(P) := \lim_{i \rightarrow \infty} \frac{r_i(P)}{[F_i : F_0]}.$$

Dann gilt

$$\nu(\mathcal{F}) = \sum_{P \in M} \mu(P) > 0,$$

weil nach Voraussetzung  $\lambda(\mathcal{F}) = \frac{\nu(\mathcal{F})}{\gamma(\mathcal{F})} > 0$  gilt. Also muss ein  $P \in M$  existieren mit  $\mu(P) > 0$ . Da alle Erweiterungen galoissch sind, liegen nur rationale Stellen über  $P$  in  $F_i$ , d.h. alle relativen Grade  $f_i(P)$  müssen 1 sein für alle  $i \geq 1$ , und wir haben

$$r_i(P) = \frac{[F_i : F_0]}{e_i(P)},$$

wobei  $e_i(P)$  der Verzweigungsindex von  $P$  in der Erweiterung  $F_i/F_0$  ist. Es gilt

$$0 < \mu(P) = \lim_{i \rightarrow \infty} \frac{1}{e_i(P)}.$$

Die Folge  $(e_i(P))_{i \geq 1}$  ist also ab einem Index konstant, sagen wir ab dem Index  $n$  und daher zerfallen die Stellen in  $F_n$ , die über  $P$  liegen vollständig in allen Erweiterungen  $F_m/F_n$  mit  $m > n$ .

□

**Bemerkung 5.2.5** In [13] wird gezeigt, dass ein galoisscher Turm dessen Galoisgruppen  $\text{Gal}(F_n/F_0)$  abelsch sind, asymptotisch schlecht ist. Der Beweis basiert auf der Theorie höherer Verzweigungsgruppen, siehe Kapitel 4.9.

### 5.3 Ein zahmer optimaler Turm

Hier wollen wir das erste Beispiel eines asymptotisch optimalen Turmes präsentieren (siehe [15]). Diese Konstruktion funktioniert jedoch nur über  $\mathbb{F}_q$  mit einem Primzahlquadrat  $q = p^2$ ,  $p \neq 2$ . Wir fixieren ein Element  $i \in \mathbb{F}_q$  mit  $i^2 = -1$ .

**Definition 5.3.1** Wir betrachten das Polynom  $f(x, y) := 2xy^2 - x^2 - 1 \in \mathbb{F}_q[x, y]$  und den dazugehörigen rekursiven Funktionenkörperturm  $\mathcal{F} = (F_0, F_1, F_2, \dots)$ .

Wir haben also in jedem Rekursionsschritt eine Kummererweiterung. Dass dadurch auch tatsächlich ein Turm definiert wird, müssen wir erst zeigen.

**Lemma 5.3.2** Sei  $F := \mathbb{F}_q(x, y)$  mit  $f(x, y) = 0$ . Dann gilt:

- (i)  $[F : \mathbb{F}_q(x)] = [F : \mathbb{F}_q(y)] = 2$ , und  $\mathbb{F}_q$  ist der volle Konstantenkörper von  $F$ .
- (ii) In der Erweiterung  $F/\mathbb{F}_q(x)$  verzweigen genau die Stellen mit  $x = 0$ ,  $x = \infty$ ,  $x = i$ ,  $x = -i$ .
- (iii) Sei  $Q \in \mathbb{P}_F$  mit  $x(Q) = \infty$  (nach (ii) existiert genau eine solche Stelle). Dann gilt  $y(Q) = \infty$ , und  $Q$  ist unverzweigt in der Erweiterung  $F/\mathbb{F}_q(y)$ .

*Beweis:* (ii) und  $[F : \mathbb{F}_q(X)] = 2$  folgt sofort aus dem Satz 4.8.3. Da total verzweigte Stellen existieren, folgt auch, dass  $\mathbb{F}_q$  der volle Konstantenkörper von  $F$  ist. Wir zeigen nun (iii): Wegen (ii) ist  $v_Q(x) = -2$  und daraus folgt  $v_Q(y) = -2$ , also  $y(Q) = \infty$ . Sei  $Q_1 := Q \cap \mathbb{F}_q(y)$ . Dann liegt sowohl die Stelle  $P_1 \in \mathbb{P}_F$  mit  $x(P_1) = 0$ ,  $y(P_1) = \infty$ , als auch die Stelle  $Q$  über  $Q_1$  in der Erweiterung  $F/\mathbb{F}_q(y)$ . Daher zerfällt die Stelle  $Q_1$  in dieser Erweiterung, also ist  $Q$  unverzweigt in  $F/\mathbb{F}_q(y)$ . Aus dieser Tatsache folgt auch  $F \neq \mathbb{F}_q(y)$  und  $[F : \mathbb{F}_q(y)] = 2$ .

□

**Korollar 5.3.3** *Es gilt:*

- (i)  $[F_n : F_0] = 2^n$ , für alle  $n \geq 0$ .
- (ii) Der Pol von  $x_0$  ist total verzweigt in der Erweiterung  $F_n/F_0$  und  $\mathbb{F}_q$  ist algebraisch abgeschlossen in  $F_n$ .
- (iii) Sei  $Q \in \mathbb{P}_{F_n}$  der (nach (ii) eindeutig bestimmte) Pol von  $x_0$  in  $F_n$ . Dann ist  $Q$  unverzweigt in der Erweiterung  $F_n/\mathbb{F}_q(x_n)$ .

*Beweis:* Nach dem Lemma 5.3.2 ist der Fall  $n = 1$  erledigt. Wir nehmen an, die Aussagen gelten für  $n$ . Sei  $Q \in \mathbb{P}_{F_{n+1}}$  mit  $x_0(Q) = \infty$ ,  $Q_1 := Q \cap F_n$ ,  $Q_2 := Q \cap \mathbb{F}_q(x_n, x_{n+1})$  und  $P := Q \cap \mathbb{F}_q(x_n)$ .  $Q_1$  ist die Polstelle von  $x_0$  in  $F_n$  und nach Induktionsvoraussetzung gilt  $e(Q_1|P) = 1$  und  $x_n(P) = \infty$ . Ausserdem ist  $Q_2$  eine einfache Polstelle von  $x_{n+1}$  und  $Q_2|P$  ist total verzweigt. Nun wenden wir das Lemma von Abhyankar (Satz 4.9.11) an und erhalten zusammen mit Lemma 5.3.2 alle Aussagen für  $n + 1$ . □

**Lemma 5.3.4** *Die Stellen  $P_{x_0=0}$ ,  $P_{x_0=\infty}$ ,  $P_{x_0=i}$ , und  $P_{x_0=-i}$  sind total verzweigt in der Erweiterung  $F_2/F_0$ , und daher gilt  $g(F_2) \geq 3$ .*

*Beweis:* Folgt aus Satz 4.8.3 und der Hurwitzschen Geschlechtsformel. □

Damit ist gezeigt, dass  $\mathcal{F}$  tatsächlich ein Turm ist. Wir bestimmen nun den Verzweigungsort unseres Turmes:

**Lemma 5.3.5** *Es gilt*

$$V(\mathcal{F}/F_0) = \{P \in \mathbb{P}_{F_0} : \text{mit } x_0(P) \in A\}, \text{ mit} \quad (5.1)$$

$$A := \{0, \infty, 1, -1, i, -i\}.$$

*Beweis:* Wir zeigen nur „ $\subseteq$ “ in (5.1), da wir nur diese Inklusion benötigen. Die andere Inklusion kann man ganz problemlos nachrechnen.

Sei  $P \in V(\mathcal{F}/F_0)$ . Dann existiert ein  $n \geq 1$  und eine Stelle  $Q \in \mathbb{P}_{F_n}$ , sodass  $Q$  über  $P$  liegt und in der Erweiterung  $F_n/F_{n-1}$  verzweigt ist. Fassen wir nun  $F_n$  als das Kompositum von  $F_{n-1}$  und  $F_2 := \mathbb{F}_q(x_n, x_{n-1})$  auf, so erhalten wir mit dem Lemma von Abhyankar (Satz 4.9.11), dass  $Q$  in der Erweiterung  $\mathbb{F}_q(x_{n-1}, x_n)/\mathbb{F}_q(x_{n-1})$  verzweigt. Es gilt also nach Lemma 5.3.2, dass  $x_{n-1}(Q) \in A$ . Wir wollen zeigen, dass  $x_0(Q) \in A$  gilt. Dazu genügt es zu zeigen, dass wenn  $x_i(Q) \in A$  liegt, auch  $x_{i-1}(Q) \in A$  liegt für alle  $i \geq 1$ . Um das zu zeigen betrachten wir unsere definierende Gleichung

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

Nun sieht man sofort die folgenden Implikationen:

$$\begin{aligned} x_i(Q) = 0 &\Rightarrow x_{i-1}(Q) \in \{i, -i\}, \\ x_i(Q) = \infty &\Rightarrow x_{i-1}(Q) \in \{0, \infty\}, \\ x_i(Q) = \pm 1 &\Rightarrow x_{i-1}(Q) = 1, \\ x_i(Q) = \pm i &\Rightarrow x_{i-1}(Q) = -1. \end{aligned}$$

Das beweist unser Lemma. □

Wir wollen nun den Zerfällungsort von  $\mathcal{F}$  bestimmen. Dazu benötigen wir einige Resultate über sogenannte Deuring Polynome. Diese Polynome sind von Deuring eingeführt worden um supersinguläre elliptische Kurven zu klassifizieren (siehe [7] oder [32]) und sind definiert durch

$$H(X) := \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j} X^j \in \mathbb{F}_p[X].$$

Sei

$$\Omega := \{\alpha \in \overline{\mathbb{F}}_p : H(\alpha^4) = 0\}.$$

$\overline{\mathbb{F}}_p$  sei dabei ein algebraischer Abschluss von  $\mathbb{F}_p$ .

**Satz 5.3.6**

- (i) Das Polynom  $H(X)$  ist separabel.
- (ii)  $\Omega \subseteq \mathbb{F}_{p^2}$  und  $\text{card}(\Omega) = 2(p-1)$ .

*Beweis:* Der Beweis zu (i) findet sich in [7] und [32]. Da  $H(0) \neq 0$  und  $\deg(H(X)) = (p-1)/2$ , folgt aus (i) sofort  $\text{card}(\Omega) = 2(p-1)$ . Der Beweis der Behauptung  $\Omega \subseteq \mathbb{F}_{p^2}$  findet sich im Appendix von [15]. □

Wir zeigen den folgenden Satz, aus dem die Optimalität des Turmes  $\mathcal{F}$  folgt.

**Satz 5.3.7** Sei  $\alpha \in \Omega$  und  $\beta \in \overline{\mathbb{F}}_p$  mit  $\beta^2 = \frac{\alpha^2+1}{2\alpha}$ . Dann gilt  $\beta \in \Omega$ .

Der Satz 5.3.7 ist eine direkte Folgerung der folgenden Proposition.

**Proposition 5.3.8** Es gilt

$$H(X^4) = X^{p-1} \cdot H\left(\left(\frac{X^2+1}{2X}\right)^2\right).$$

*Beweis (Skizze):* Wir haben

$$\begin{aligned} X^{p-1} \cdot H \left( \left( \frac{X^2 + 1}{2X} \right)^2 \right) &= X^{p-1} \cdot \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 \cdot \left( \frac{X^2 + 1}{2X} \right)^{2j} \\ &= \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 \cdot \frac{1}{4^j} \cdot (X^2 + 1)^{2j} \cdot X^{p-1-2j} \\ &= \sum_{k=0}^{p-1} c_k \cdot X^{2k}, \end{aligned}$$

mit

$$c_k = \sum_{j=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{j}^2 \cdot \frac{1}{4^j} \cdot \binom{2j}{k+j-\frac{p-1}{2}}.$$

Nach einiger Rechnung erhält man

$$c_k \equiv S_k \pmod{p} \text{ für } 0 \leq k \leq p-1 \text{ und}$$

$$S_k := (-1)^k \sum_{j=0}^k \frac{(-1)^j}{4^j} \cdot \binom{2j}{j}^2 \cdot \binom{k+j}{2j}.$$

Da  $p \neq 2$  gilt, ist  $S_k$  in  $\mathbb{F}_p$  wohldefiniert, da  $4^j \neq 0$  in  $\mathbb{F}_p$ .

**Behauptung:** Es gilt für  $S_k$  wie oben definiert:

- (i)  $S_k = 0$  für  $k$  ungerade, und
- (ii)  $S_k = \frac{1}{4^k} \binom{k}{k/2}^2$  für  $k$  gerade.

Zum Beweis verwenden wir die Gaußsche hypergeometrische Funktion  $G(z) := {}_2F_1\left(\frac{1}{2}, \frac{1}{2}; 1; z\right)$  (siehe [20]). Diese Funktion erfüllt bekannterweise die Differentialgleichung

$$z(1-z) \cdot y'' + (1-2z) \cdot y' - \frac{1}{4} \cdot y = 0,$$

und besitzt die Potenzreihenentwicklung

$$G(z) = \sum_{n \geq 0} \frac{1}{4^{2n}} \cdot \binom{2n}{n}^2 \cdot z^n.$$

Eine kurze Rechnung zeigt, dass dann die Funktionen  $G(z^2)$  und  $\frac{1}{1-z} \cdot G\left(\frac{-4z}{(1-z)^2}\right)$  Lösungen der Differentialgleichung

$$z(z^2 - 1) \cdot y'' + (3z^2 - 1) \cdot y' + z \cdot y = 0$$

sind, und daraus folgt

$$G(z^2) = \frac{1}{1-z} \cdot G\left(\frac{-4z}{(1-z)^2}\right). \quad (5.2)$$

Nun gilt, da der Koeffizient von  $z^{n-k}$  in der Summe  $(\sum_{m=0}^n z^m)^{2k+1}$  gleich  $\binom{n+k}{2k}$  ist, dass

$$\frac{1}{1-z} G\left(\frac{-4z}{(1-z)^2}\right) = \sum_{n \geq 0} (-1)^n \cdot S_n \cdot z^n,$$

und wegen (5.2) gilt daher

$$\sum_{n \geq 0} (-1)^n \cdot S_n \cdot z^n = \sum_{n \geq 0} \frac{1}{4^{2n}} \cdot \binom{2n}{n}^2 \cdot z^{2n}. \quad (5.3)$$

Das beweist unsere Behauptungen (i) und (ii).

**Behauptung:**  $c_k \equiv \binom{\frac{p-1}{2}}{k/2}^2 \pmod{p}$  für  $k$  gerade und  $0 \leq k \leq p-1$ .

Durch vollständige Induktion rechnet man das Folgende nach:

$$4^k \cdot \binom{\frac{p-1}{2}}{k/2}^2 \equiv \binom{k}{k/2}^2 \pmod{p} \text{ für } k \text{ gerade und } 0 \leq k \leq p-1.$$

Daraus und aus (5.3) folgt sofort die Behauptung.

Setzt man diese Ergebnisse in die Definition von  $c_k$  ein, so erhält man die Aussage der Proposition. □

**Satz 5.3.9** *Der Turm  $\mathcal{F}$  ist asymptotisch optimal.*

*Beweis:* Sei  $P := P_\alpha \in \mathbb{P}_{F_0}$  mit  $\alpha \in \Omega$ . Nach Satz 5.3.6 gilt  $\deg(P) = 1$ . Nach Satz 5.3.7 besitzt die Gleichung

$$\beta^2 = \frac{\alpha^2 + 1}{2\alpha}$$

zwei verschiedene Nullstellen  $\beta$  in  $\Omega$ . Aus dem Satz von Kummer (Satz 4.2.6) folgt, dass die Stelle  $P$  in der Erweiterung  $F_1/F_0$  vollständig zerfällt. Durch Induktion folgt, dass  $P$  in allen Erweiterungen  $F_n/F_{n-1}$  vollständig zerfällt, und daraus folgt

$$\Omega \subseteq S(\mathcal{F}/F_0).$$

Wir verwenden nun die Notation von Korollar 5.2.3 und sehen, dass

$$t \geq \text{card}(\Omega) = 2(p-1) \text{ und } s \leq 6.$$

Setzt man in Korollar 5.2.3 ein, so erhält man unter Verwendung der Tatsache  $g(F_0) = 0$

$$\lambda(\mathcal{F}) \geq \frac{4(p-1)}{6-2} = p-1 = A(p^2)$$

und das beweist die Optimalität von  $\mathcal{F}$ .

□

## 5.4 Ein wilder optimaler Turm

Für wilde Türme kann man keine Resultate in der Art von Satz 5.2.3 herleiten, da man keine Kontrolle über die Differenten besitzt. Es genügt dann nicht den Verzweigungsort zu bestimmen, man muss vielmehr in jedem Schritt  $F_n/F_{n-1}$  die Differenten kennen und dann die Transitivität der Differenten ausnützen. Das werden wir als erstes tun und erhalten den folgenden Satz.

**Satz 5.4.1** *Sei  $\mathcal{F} = (F_0, F_1, F_2, \dots)$  ein Turm über  $\mathbb{F}_q$ . Gelte*

$$\deg(\text{Diff}(F_{n+1}/F_n)) \leq \varepsilon \cdot [F_{n+1} : F_n] \cdot \deg(\text{Diff}(F_n/F_{n-1}))$$

für alle  $n \geq 1$  mit  $0 \leq \varepsilon < 1$ . Sei weiters der  $S(\mathcal{F}/F_0) \neq \emptyset$ . Dann gilt mit  $t := \text{card}(S(\mathcal{F}/F_0))$

$$\lambda(\mathcal{F}) \geq \frac{2(1-\varepsilon)[F_1 : F_0] \cdot t}{\deg(\text{Diff}(F_1/F_0)) + (1-\varepsilon)[F_1 : F_0](2g(F_0) - 2)},$$

falls  $\deg(\text{Diff}(F_1/F_0)) + (1-\varepsilon)[F_1 : F_0](2g(F_0) - 2) > 0$ .

*Beweis:* Wir setzen  $D_{n+1} := \deg(\text{Diff}(F_{n+1}/F_n))$  für  $n \geq 0$ .

Aus  $D_{n+1} \leq \varepsilon[F_{n+1} : F_n] \cdot D_n$  folgt

$$D_{i+1} \leq \varepsilon^i [F_{i+1} : F_1] \cdot D_1 \text{ für alle } i \geq 1. \quad (5.4)$$

Wir erhalten wegen der Hurwitzschen Geschlechtsformel, (5.4) und Korollar 4.5.11

$$\begin{aligned} 2g(F_{n+1}) - 2 &= [F_{n+1} : F_0](2g(F_0) - 2) + \deg(\text{Diff}(F_{n+1}/F_0)) \\ &= [F_{n+1} : F_0](2g(F_0) - 2) + \sum_{i=0}^n [F_{n+1} : F_{i+1}] \cdot D_{i+1} \\ &\leq [F_{n+1} : F_0](2g(F_0) - 2) + \sum_{i=0}^n \varepsilon^i [F_{n+1} : F_1] \cdot D_1 \\ &= [F_{n+1} : F_0] \left( (2g(F_0) - 2) + \frac{D_1}{[F_1 : F_0]} \cdot \frac{1 - \varepsilon^{n+1}}{1 - \varepsilon} \right) \\ &\leq [F_{n+1} : F_n] \left( (2g(F_0) - 2) + \frac{D_1}{(1-\varepsilon)[F_1 : F_0]} \right). \end{aligned}$$

Unter Verwendung von Lemma 5.1.14 sieht man

$$\lambda(\mathcal{F}) \geq \frac{2t}{2g(F_0) - 2 + \frac{D_1}{(1-\varepsilon)[F_1:F_0]}} = \frac{2(1-\varepsilon)[F_1:F_0] \cdot t}{D_1 + (1-\varepsilon)[F_1:F_0](2g(F_0) - 2)}.$$

□

**Bemerkung 5.4.2** Die Forderung  $\deg(\text{Diff}(F_1/F_0)) + (1-\varepsilon)[F_1:F_0](2g(F_0) - 2) > 0$  stellt keine Einschränkung dar, da  $g(F_n) \geq 2$  ab einem Index  $n$  gilt, und wenn man  $\mathcal{F}$  durch den Turm  $\tilde{\mathcal{F}} = (\tilde{F}_0, \tilde{F}_1, \tilde{F}_2, \dots) := (F_n, F_{n+1}, F_{n+2}, \dots)$  ersetzt gilt  $\deg(\text{Diff}(\tilde{F}_1/\tilde{F}_0)) + (1-\varepsilon)[\tilde{F}_1:\tilde{F}_0](2g(\tilde{F}_0) - 2) > 0$  und man kann den Satz anwenden.

Wir wollen nun ein Beispiel eines optimalen, wilden Turmes über  $\mathbb{F}_{q^2}$  angeben, wobei  $q$  eine Primzahlpotenz ist (siehe [16]).

**Definition 5.4.3**  $\mathcal{F}$  sei der durch das Polynom

$$f(x, y) = (x^{q-1} + 1)y^q + (x^{q-1} + 1)y - x^q \in \mathbb{F}_{q^2}[x, y]$$

definierte rekursive Turm.

Die folgenden Teilmengen von  $\mathbb{F}_{q^2}$  werden wir zur Analyse dieses Turmes benötigen:

$$\Omega := \{\alpha \in \mathbb{F}_{q^2} : \alpha^q + \alpha = 0\} \text{ und } \Omega^* := \Omega \setminus \{0\}.$$

Klarerweise besteht die Menge  $\Omega$  aus  $q$  Elementen.

Wie man mittels einer Substitution  $y_1 := \alpha y$  mit  $\alpha \in \Omega^*$  sofort sieht, besteht dieser Turm aus Artin-Schreier Erweiterungen

$$F_{i+1} = F_i(x_{i+1}) \text{ mit } x_{i+1}^q + x_{i+1} = \frac{x_i^q}{x_i^{q-1} + 1}.$$

**Lemma 5.4.4** Sei  $F = \mathbb{F}_{q^2}(x, y)$  mit  $f(x, y) = 0$  und  $P \in \mathbb{P}_{\mathbb{F}_{q^2}(x)}$  mit  $x(P) \in \Omega^* \cup \{\infty\}$ . Dann ist  $P$  in der Erweiterung  $F/\mathbb{F}_{q^2}(x)$  total verzweigt.

*Beweis:* Die Aussage folgt sofort aus dem Satz über Artin-Schreier Erweiterungen (Satz 4.8.5).

□

Wir berechnen den Zerfällungsort:

**Lemma 5.4.5**  $S(\mathcal{F}/F_0) = \{P_\alpha \in \mathbb{P}_{F_0} : \alpha \in \mathbb{F}_{q^2} \setminus \Omega\}$ .

*Beweis:* Sei  $P \in \mathbb{P}_{F_i}$  mit  $x_i(P) \notin \Omega$ . Dann gilt

$$f(x_{i+1}) := x_{i+1}^q + x_{i+1} - \frac{x_i^q}{x_i^{q-1} + 1} \in \mathcal{O}_P[x_{i+1}]$$

und

$$f(x_{i+1}) \equiv x_{i+1}^q + x_{i+1} - \frac{\alpha^{q+1}}{\alpha^q + \alpha} =: \bar{f}(x_{i+1}) \pmod{(P)},$$

(wir haben den konstanten Koeffizienten mit  $\alpha \neq 0$  erweitert). Es gilt

$$Nm_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha^{q+1}$$

und

$$Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha^q + \alpha.$$

Daher gilt

$$\gamma := \frac{\alpha^{q+1}}{\alpha^q + \alpha} \in \mathbb{F}_q \setminus \{0\}.$$

Alle  $q$  Nullstellen von  $\bar{f}(x_{i+1})$  liegen in  $\mathbb{F}_{q^2}$ , da die Spurabbildung  $Tr_{\mathbb{F}_{q^2}/\mathbb{F}_q}$  eine  $\mathbb{F}_q$ -lineare, und surjektive Abbildung ist. Da  $\bar{f}$  separabel ist, zerfällt  $\bar{f}$  in Linearfaktoren über  $\mathbb{F}_{q^2}$  und nach dem Satz von Kummer (Satz 4.2.6) zerfällt  $P$  total in der Erweiterung  $F_{i+1}/F_i$ . Wir zeigen noch, dass  $x_{i+1}(P') \notin \Omega$  für  $P'|P$ . Dafür genügt es aber wieder nach dem Satz von Kummer zu zeigen, dass keine Nullstelle von  $\bar{f}$  in  $\Omega$  liegt. Das ist jedoch unmittelbar klar, da  $\gamma \neq 0$  gilt. □

Unser nächstes Ziel ist es, den Verzweigungsort zu berechnen.

**Lemma 5.4.6** Sei  $P \in \mathbb{P}_{\mathbb{F}_{q^2}(x_1)}$ .

- (i) Sei  $x_1(P) \in \Omega$ . Dann ist  $P$  total verzweigt in der Erweiterung  $\mathbb{F}_{q^2}(x_0, x_1)/\mathbb{F}_{q^2}(x_1)$ .
- (ii) Sei  $x_1(P) = \infty$ . Dann ist  $P$  unverzweigt in der Erweiterung  $\mathbb{F}_{q^2}(x_0, x_1)/\mathbb{F}_{q^2}(x_1)$ .

*Beweis:* Wir haben als definierende Gleichung

$$x_1^q + x_1 = \frac{x_0^q}{x_0^{q-1} + 1}.$$

Setzen wir  $\tilde{x}_0 := \frac{1}{x_0}$ , so erhalten wir

$$x_1^q + x_1 = \frac{1}{\tilde{x}_0 + \tilde{x}_0^q} \tag{5.5}$$

und daher

$$\tilde{x}_0^q + \tilde{x}_0 = \frac{1}{x_1^q + x_1}.$$

Es gilt klarerweise  $\mathbb{F}_{q^2}(x_0) = \mathbb{F}_{q^2}(\tilde{x}_0)$ , und wegen (5.5) und dem Satz über Artin-Schreier Erweiterungen folgt die Behauptung, da

$$v_P\left(\frac{1}{x_1^q + x_1}\right) = -v_P(x_1^q + x_1) = -1 \text{ f\"ur } x_1(P) \in \Omega,$$

und

$$v_P\left(\frac{1}{x_1^q + x_1}\right) = -v_P(x_1^q + x_1) = q \text{ f\"ur } x_1(P) = \infty.$$

□

**Lemma 5.4.7** *F\"ur ein  $P \in \mathbb{P}_{F_n}$  mit  $x_0(P) \in \Omega^* \cup \{\infty\}$  gilt*

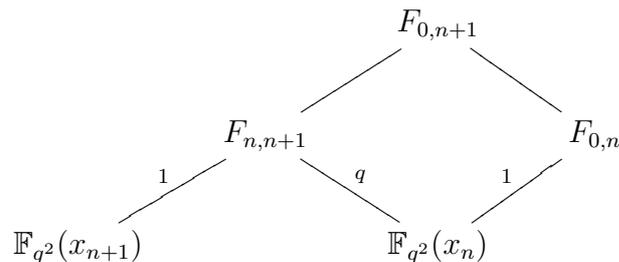
- (i)  $P \cap F_{n-1}$  ist total verzweigt in  $F_n/F_{n-1}$  f\"ur alle  $n$  und  $d(P/P \cap F_{n-1}) = 2(q-1)$ .
- (ii)  $x_i(P) = \infty$  f\"ur alle  $i \geq 1$ .
- (iii)  $P \cap \mathbb{F}_{q^2}(x_n)$  ist unverzweigt in der Erweiterung  $F_n/\mathbb{F}_{q^2}(x_n)$
- (iv)  $\mathcal{F}$  definiert einen Turm \"uber  $\mathbb{F}_{q^2}$ .

*Beweis:* (ii) folgt sofort aus der definierenden Gleichung.

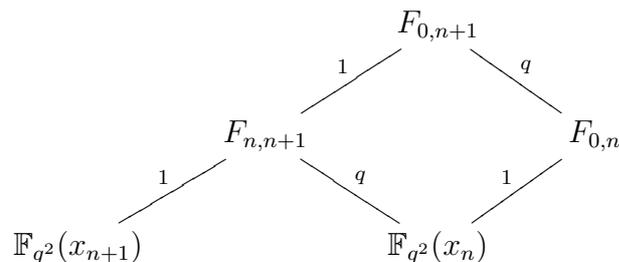
(iii) Um \"Ubersichtlichkeit zu gew\"ahrleisten verwenden wir die folgende Notation:

$$F_{k,l} := \mathbb{F}_{q^2}(x_k, x_{k+1}, \dots, x_l).$$

Der Fall  $n = 1$  ist bereits durch Lemma 5.4.6 erledigt. Nehmen wir an, die Einschr\"ankung von  $P$  sei in der Erweiterung  $F_{0,n}/F_{n,n}$  unverzweigt. Wieder nach dem Lemma 5.4.6 und dem Lemma 5.4.4 haben wir dann das folgende Diagramm f\"ur  $P$  (die Zahlen bezeichnen die Verzweigungsindizes):



Das Lemma von Abhyankar liefert:



$P$  ist also unverzweigt in der Erweiterung  $F_{0,n+1}/F_{n+1,n+1}$ , und das beweist (iii).

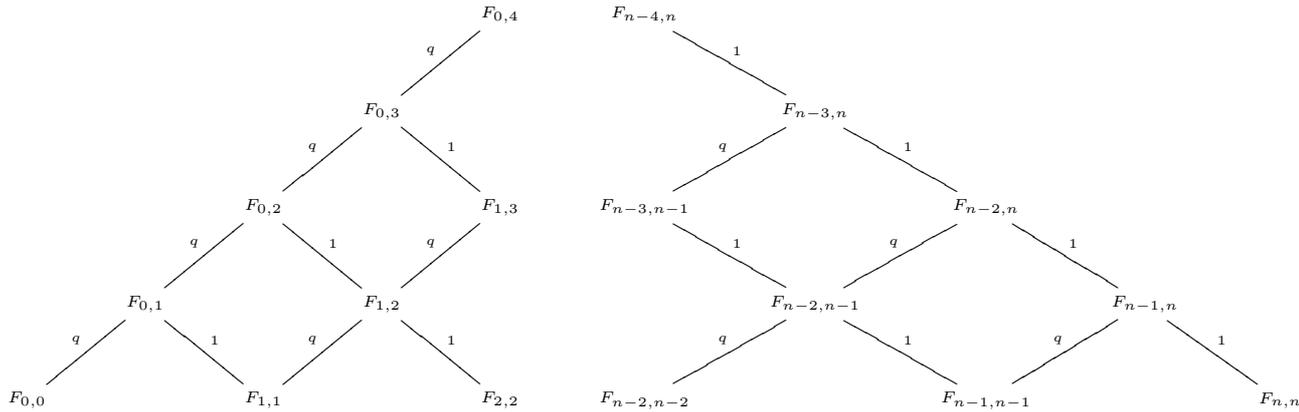
(i) Es gilt für  $n \geq 2$

$$v_{P \cap F_{n-1}}(x_{n-1}^q / (x_{n-1}^{q-1} + 1)) = -1 \cdot e(P \cap F_{n-1} | P \cap \mathbb{F}_{q^2}(x_{n-1})).$$

Aus (ii) und (iii) folgt  $e(P \cap F_{n-1} | P \cap \mathbb{F}_{q^2}(x_{n-1})) = 1$ , also ist nach dem Satz über Artin-Schreier Erweiterungen (Satz 4.8.5) die Stelle  $P \cap F_{n-1}$  total verzweigt in der Erweiterung  $F_n/F_{n-1}$ . Die Aussage über den Differentenindex folgt auch aus Satz 4.8.5.

(iv) folgt aus (i) und der Formel für das Geschlecht im Satz über Artin-Schreier Erweiterungen. □

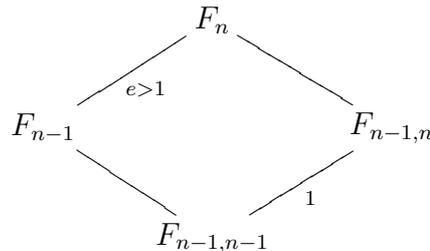
Aus diesen Betrachtungen folgt, dass wir alles über die Stellen  $P$  mit  $x_0(P) \in \Omega^* \cup \{\infty\}$  wissen. Ihr Verzweigungsverhalten lässt sich wie folgt beschreiben (wir verwenden wieder das Lemma von Abhyankar und die Tatsache, dass  $x_i(P) = \infty$  für alle  $i \geq 1$  gilt).



Wir kennen außerdem den Differentenindex  $d(P/P \cap F_{n-1})$ . Dieser ist  $2(q - 1)$  nach dem Satz über Artin-Schreier Erweiterungen. Nun wollen wir alle Stellen bestimmen, die in einer Erweiterung  $F_n/F_{n-1}$  verzweigen können.

**Lemma 5.4.8** *Angenommen  $P$  ist in  $F_n/F_{n-1}$  verzweigt. Dann ist  $P$  in  $F_{n-1,n}/F_{n-1,n-1}$  verzweigt. Insbesondere gilt  $x_{n-1}(P) \in \Omega^* \cup \{\infty\}$ .*

*Beweis:* Angenommen  $P$  ist unverzweigt in  $F_{n-1,n}/F_{n-1,n-1}$ . Dann haben wir das folgende Bild:



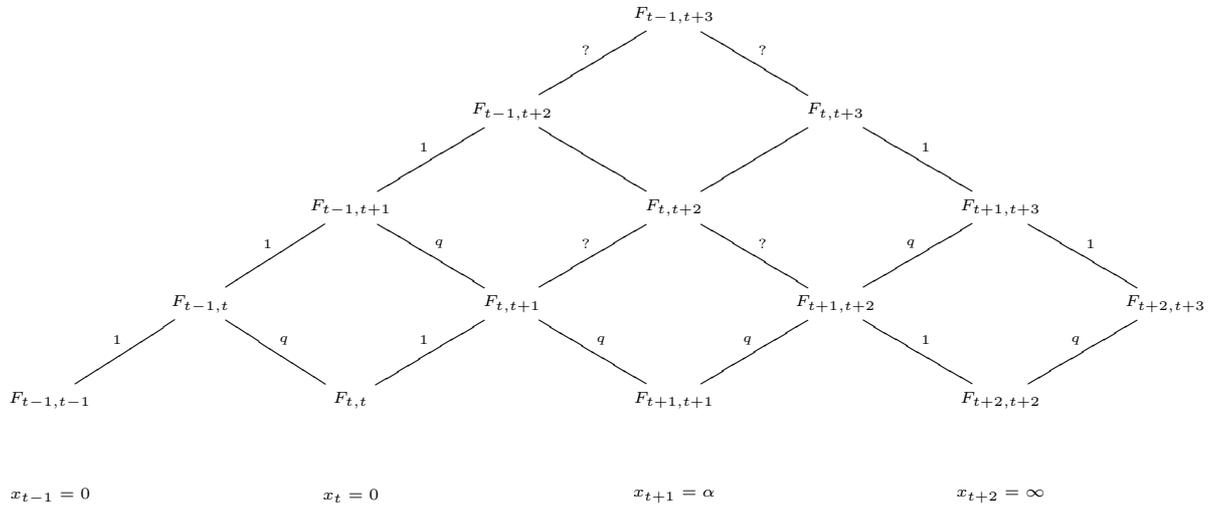
Das ist aber ein Widerspruch zum Lemma von Abhyankar.

□

Die Stellen, die theoretisch verzweigen können, sind also jene, mit

- (a)  $x_0(P) \in \Omega^* \cup \{\infty\}$ ,
- (b)  $x_0(P) = x_1(P) = \dots = x_t(P) = 0$  und  $x_{t+1}(P) = \alpha \in \Omega^*$

Fall (a) haben wir unter Kontrolle. Wenden wir uns nun dem Fall (b) zu: Sei  $P$  eine Stelle mit  $x_0(P) = x_1(P) = \dots = x_t(P) = 0$  und  $x_{t+1}(P) = \alpha \in \Omega^*$ . Dann folgt wie in Lemma 5.4.7 (ii)  $x_{t+k}(P) = \infty$  für alle  $k \geq 2$  und nach dem Lemma von Abhyankar haben wir das folgende Bild:



Das folgende Lemma zeigt, dass wir die Fragezeichen immer durch 1 ersetzen können.

**Lemma 5.4.9** Sei  $1 \leq k \leq t$  und sei  $Q \in \mathbb{P}_{F_{t+1-k,t+k}}$  mit  $x_{t+1}(Q) = \alpha \in \Omega^*$ . Dann ist  $Q$  unverzweigt in der Erweiterung  $F_{t+1-k,t+k+1}/F_{t+1-k,t+k}$ .

Für den Beweis wollen wir eine neue Notation einführen (siehe [14, 16]):

**Definition 5.4.10** Sei  $F/K$  ein Funktionenkörper,  $P \in \mathbb{P}_F$ , und  $x, y, z \in F$ . Wir schreiben

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

wenn

$$x = y + t \cdot z \text{ mit } v_P(t) \geq 0.$$

*Beweis von Lemma 5.4.9:* Wir setzen  $H_k := F_{t+1-k,t+1+k}$  und  $E_k := F_{t+1-k,t+k}$ . Wir zeigen induktiv

$$Q \text{ ist unverzweigt in } H_k/E_k \tag{5.6}$$

und

$$x_{t+k+1} = \alpha^{q+1} x_{t+1-k}^{-1} + \mathcal{O}(1) \text{ an der Stelle } Q. \quad (5.7)$$

Sei  $k = 1$ . Dann gilt  $E_1 = \mathbb{F}_{q^2}(x_t, x_{t+1})$  und  $H_1 = E_1(x_{t+2})$ ,  $x_t(Q) = 0$ , und  $x_{t+1}(Q) = \alpha$ . Es gilt also an der Stelle  $Q$

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

Daraus folgt

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

und daher gilt (an der Stelle  $Q$ )

$$\frac{1}{x_{t+1} - \alpha} = x_t^{-q} (1 + x_t^{q-1} + \mathcal{O}(x_t^q)) = x_t^{-q} + x_t^{-1} + \mathcal{O}(1). \quad (5.8)$$

Weiters gilt

$$x_{t+2}^q + x_{t+2} = \frac{(x_{t+1} - \alpha)^q + \alpha^q}{x_{t+1}^{q-1} + 1} = \frac{\alpha^q}{x_{t+1}^{q-1} + 1} + \mathcal{O}(1). \quad (5.9)$$

Wir schreiben  $x_{t+1}^{q-1} + 1 = (x_{t+1} - \alpha) \cdot h(x_{t+1})$ , wobei  $h$  ein Polynom vom Grad  $q - 2$  ist. Leiten wir diese Gleichung ab, so erhalten wir

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

also gilt  $h(\alpha) = -\alpha^{q-2}$ . Es folgt

$$\frac{\alpha^q}{x_{t+1}^{q-1} + 1} - \frac{\alpha^{q+1}}{x_{t+1} + 1} = \alpha^q \cdot \frac{1 - \alpha \cdot h(x_{t+1})}{x_{t+1}^{q-1} + 1} = \mathcal{O}(1) \quad (5.10)$$

an der Stelle  $Q$ , da  $1 - \alpha \cdot h(\alpha) = 1 - \alpha \cdot (-\alpha^{q-2}) = 1 + \alpha^{q-1} = 0$  gilt. Aus (5.8), (5.9) und (5.10) folgt, dass an der Stelle  $Q$  gilt

$$\begin{aligned} x_{t+2}^q + x_{t+2} &= \frac{\alpha^{q+1}}{x_{t+1} - \alpha} + \mathcal{O}(1) \\ &= \frac{\alpha^{q+1}}{x_t^q} + \frac{\alpha^{q+1}}{x_t} + \mathcal{O}(1). \end{aligned}$$

Aus der Relation  $(\alpha^{q+1})^q = \alpha^{q+1}$  folgt

$$\left( x_{t+2} - \frac{\alpha^{q+1}}{x_t} \right)^q + \left( x_{t+2} - \frac{\alpha^{q+1}}{x_t} \right) = \mathcal{O}(1). \quad (5.11)$$

(5.11) heißt nichts anderes als

$$0 \leq v_Q \left( \left( x_{t+2} - \frac{\alpha^{q+1}}{x_t} \right)^q + \left( x_{t+2} - \frac{\alpha^{q+1}}{x_t} \right) \right)$$

und daraus folgt wegen der (starken) Dreiecksungleichung

$$0 \leq v_Q \left( x_{t+2} - \frac{\alpha^{q+1}}{x_t} \right)$$

und das heißt wiederum genau

$$x_{t+2} = \alpha^{q+1} x_t^{-1} + \mathcal{O}(1),$$

und das ist (5.7).

Weiters folgt aus (5.11), dass

$$0 \leq v_Q \left( x_{t+2}^q + x_{t+2} - \left( \left( \frac{\alpha^{q+1}}{x_t} \right)^q + \frac{\alpha^{q+1}}{x_t} \right) \right) = v_Q \left( \frac{x_{t+1}^q}{x_{t+1}^{q-1} + 1} - \left( \left( \frac{\alpha^{q+1}}{x_t} \right)^q + \frac{\alpha^{q+1}}{x_t} \right) \right).$$

Aus dem Satz über Artin-Schreier Erweiterungen folgt, dass  $Q$  unverzweigt in  $H_1/E_1$  ist.

Nun sei  $k \geq 2$ . An der Stelle  $Q$  hat man

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

Es folgt (man verwende, dass  $x_{t+k}^{-1}(Q) = 0$  gilt)

$$x_{t+k+1}^q + x_{t+k+1} = x_{t+k} + \mathcal{O}(1). \quad (5.12)$$

Andererseits gilt an der Stelle  $Q$

$$\begin{aligned} x_{t+2-k}^q + x_{t+2-k} &= \frac{x_{t+1-k}^q}{x_{t+1-k}^{q-1} + 1} \\ &= x_{t+1-k}^q (1 - x_{t+1-k}^{q-1} + \mathcal{O}(x_{t+1-k}^q)), \end{aligned}$$

und daher

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

(man beachte, dass  $x_{t+1-k}(Q) = 0$ ). Wir erhalten

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

und daher

$$x_{t+2-k}^{-1} = x_{t+1-k}^{-q} + x_{t+1-k}^{-1} + \mathcal{O}(1). \tag{5.13}$$

Nach Induktionsvoraussetzung (Formel (5.7)) gilt

$$x_{t+k} = \alpha^{q+1} x_{t+2-k}^{-1} + \mathcal{O}(1). \tag{5.14}$$

Kombinieren wir nun (5.12), (5.13) und (5.14), so erhalten wir

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

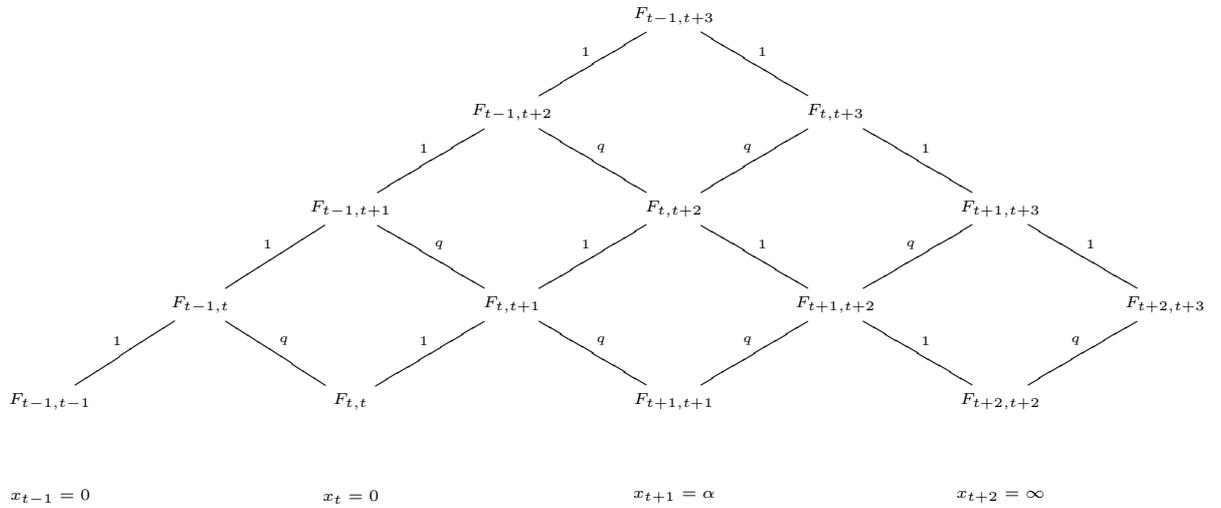
Wir haben also

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

Analog, zum Fall  $k = 1$  sieht man, dass  $Q$  unverzweigt ist in der Erweiterung  $H_k/E_k$ .

□

Wir können jetzt also unser Verzweigungsdiagramm komplettieren:



Wir wollen nun unsere Erkenntnisse in Form eines Lemmas zusammenfassen:

**Lemma 5.4.11** Sei  $0 \leq t < n$  und  $Q \in \mathbb{P}_{F_n}$  mit

$$x_i(Q) = \begin{cases} 0 & \text{für } 0 \leq i \leq t, \\ \alpha \in \Omega^* & \text{für } i = t + 1 \\ \infty & \text{für } t + 2 \leq i < n. \end{cases}$$

Dann gilt

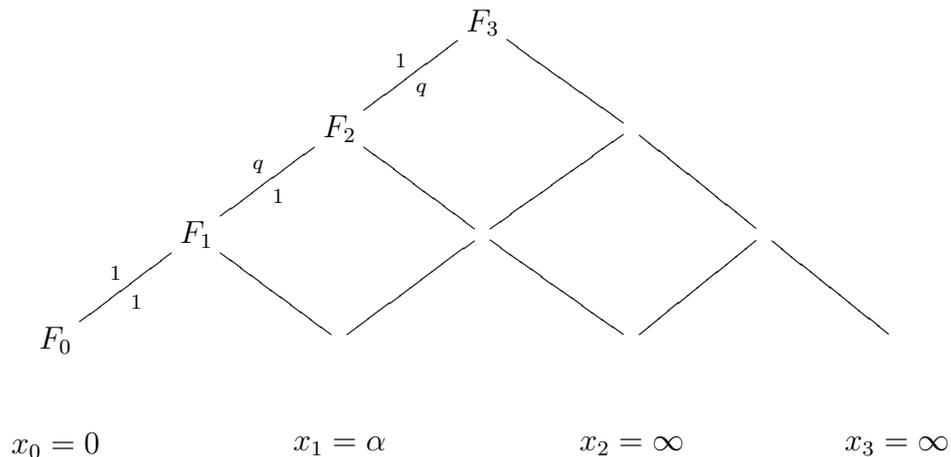
- (i) Die Einschränkung von  $Q$  ist unverzweigt in  $F_n/F_{n-1}$ , falls  $n \leq 2t + 2$ ,
- (ii) Die Einschränkung von  $Q$  ist total verzweigt in  $F_n/F_{2t+1}$ , falls  $n > 2t + 2$  und der Differentenexponent ist  $2(q - 1)$ .

*Beweis:* Die Aussagen über die Verzweigungen folgen durch „diagram chasing“ im obigen Verzweigungsdiagramm. Die Aussage über den Differentenexponenten folgt direkt aus dem Satz über Artin-Schreier Erweiterungen.

□

**Lemma 5.4.12** Sei  $n > 2t + 2$ . Dann gilt für die Stelle  $Q$  aus dem obigen Lemma  $\text{deg}(Q) = q^{t+1}$ .

*Beweis:* Am besten versteht man die Aussage, wenn man ein Beispiel betrachtet. Sei  $t = 0$  und  $n = 3$ .



Die Zahlen links von den Linien bezeichnen die relativen Grade, die Zahlen rechts davon die Verzweigungsindizes. In der Erweiterung  $F_1/F_0$  zerfällt die Stelle total, der relative Grad ist also 1. In der Erweiterung  $F_2/F_1$  ist die Stelle unverzweigt und es liegt genau eine Stelle über ihr. Daher gilt nach der Hilbertschen Fundamentalformel, dass der relative Grad gleich  $q$  ist. In der Erweiterung  $F_3/F_2$  ist die Stelle total verzweigt, daher ist der relative Grad gleich 1. Nun sollte auch der allgemeine Fall klar sein.

□

Nun sind wir endlich in der Lage den Grad der Differente explizit anzugeben.

**Lemma 5.4.13** Sei  $n \geq 1$ . Dann gilt

$$\text{deg}(\text{Diff}(F_n/F_{n-1})) = 2 \cdot (q - 1) \cdot q^{\lfloor \frac{n+1}{2} \rfloor}.$$

*Beweis:* Zuerst leisten die Stellen mit  $x_0(P) \in \Omega^* \cup \{\infty\}$  einen Beitrag. Es gibt  $q$  solche Stellen und jede hat den Differentenindex  $2(q-1)$ . Der zweite Beitrag kommt von den Stellen, die in den vorherigen Lemmata betrachtet wurden. Für jedes  $\alpha \in \Omega^*$  und jedes  $0 \leq t \leq \lfloor \frac{n-3}{2} \rfloor$  existiert eine solche Stelle und der Differentenindex ist  $2(q-1)$ . Wir haben also

$$\begin{aligned}
 \deg(\text{Diff}(F_n/F_{n-1})) &= q \cdot 2 \cdot (q-1) + \sum_{t=0}^{\lfloor (n-3)/2 \rfloor} \sum_{\alpha \in \Omega^*} q^{t+1} \cdot 2 \cdot (q-1) \\
 &= q \cdot 2 \cdot (q-1) + \sum_{t=0}^{\lfloor (n-3)/2 \rfloor} q^{t+1} \cdot 2 \cdot (q-1)^2 \\
 &= 2q(q-1)(1 + (q^{\lfloor (n-1)/2 \rfloor} - 1)) \\
 &= 2 \cdot (q-1) \cdot q^{\lfloor \frac{n+1}{2} \rfloor}.
 \end{aligned}$$

□

Wir zeigen, dass  $\mathcal{F}$  asymptotisch optimal ist.

**Satz 5.4.14** *Es gilt*

$$\lambda(\mathcal{F}) = q - 1.$$

*Beweis:* Wir ersetzen den Turm  $\mathcal{F}$  durch den Turm  $\mathcal{F}' := (F'_0, F'_1, \dots)$  mit  $F'_i := F_{2i}$ . Klarerweise gilt  $\lambda(\mathcal{F}) = \lambda(\mathcal{F}')$  und nach Lemma 5.4.13 und Korollar 4.5.11 gilt

$$\begin{aligned}
 D_n &:= \deg(\text{Diff}(F'_n/F'_{n-1})) = \deg(\text{Diff}(F_{2n}/F_{2n-2})) \\
 &= 2(q-1)q^{\lfloor (2n+1)/2 \rfloor} + 2q(q-1)q^{\lfloor 2n/2 \rfloor} \\
 &= 2(q^2-1)q^n.
 \end{aligned}$$

Die Voraussetzungen von Satz 5.4.1 sind also erfüllt mit  $\varepsilon := q^{-1}$  und  $t := \text{card}(S(\mathcal{F}'/F'_0)) = \text{card}(S(\mathcal{F}/F_0)) = q^2 - 1$ . Wir bekommen

$$\lambda(\mathcal{F}') \geq \frac{2(1-q^{-1})q^2(q^2-q)}{2(q^2-1)q + (1-q^{-1})q^2(-2)} = q - 1.$$

□

**Bemerkung 5.4.15** *Durch diesen Turm ist der Satz von Tsfasman-Vladut-Zink mit Hilfe einer expliziten Konstruktion bewiesen.*

## 5.5 Ausblick

Die Forschung auf dem Gebiet der Funktionenkörpertürme ist noch lange nicht abgeschlossen. Nachdem man über Funktionenkörpern mit Konstantenkörper quadratischer

Ordnung optimale Türme konstruieren kann, ist sehr wenig bekannt über Funktionenkörper mit Konstantenkörper nicht quadratischer Ordnung. Es existieren jedoch einige Ergebnisse, so konnte J. P. Serre mit Klassenkörpertürmen und dem Golod-Shaverevic Theorem zeigen, dass eine Konstante  $c > 0$  (unabhängig von  $q$ ) existiert mit

$$A(q) \geq c \log(q) > 0.$$

Für  $q = p^3$  ( $p$  Primzahl) existiert eine bessere Schranke. T. Zink bewies, dass

$$A(p^3) \geq \frac{2(p^2 - 1)}{p + 2}. \quad (5.15)$$

J. Bezerra, A. Garcia und H. Stichtenoth konnten in [6] zeigen, dass (5.15) auch gilt, wenn man statt  $p$  eine beliebige Primzahlpotenz  $q$  einsetzt. Der Beweis liefert auch einen expliziten Turm, der diese Schranke erreicht und ist mit den in dieser Arbeit entwickelten Methoden zu verstehen. Diese Schranke liefert übrigens wieder eine Verbesserung der Gilbert-Varshamov Schranke.

Ein anderes offenes Problem ist die Klassifizierung von Funktionenkörpertürmen. Zwar wurden schon einige spezielle Ergebnisse erzielt, z.B. in [5] oder [43], ein vollständiges Verständnis der verschiedenen Typen von (rekursiven) Funktionenkörpertürmen ist jedoch noch nicht vorhanden.

In [4] wird die Theorie der Funktionenkörper mit Graphentheorie in Verbindung gebracht. Dieses Paper ist sehr interessant und trägt sehr zum Verständnis der Verzweigungstheorie bei.

Ein weiteres Problem, auf das in dieser Arbeit gar nicht eingegangen wird, ist die Konstruktion eines effizienten Codierungsalgorithmus<sup>7</sup>. Ein Hauptproblem ist dabei das Finden einer Basis für den Vektorraum  $\mathcal{L}(G)$  (siehe Kapitel 3). Ein wirklich praktikabler Algorithmus wurde bis heute noch nicht gefunden.

Man kann Geometrische Goppa Codes dahingehend verallgemeinern, dass man auch bei Stellen höheren Grades auswertet. Diese Codes heißen XNL-Codes und wurden von Xing, Niederreiter und Lam erfunden. Eine Einführung in diese Codes findet sich in [30]. Man hat diese Codes auch auf ihre asymptotischen Eigenschaften überprüft, signifikante Verbesserungen gegenüber den Geometrischen Goppa Codes fand man dabei bisher nicht.

Es gibt Bestrebungen, die Konstruktion von Goppa Codes mit elementaren Mitteln zu erklären, siehe [11], jedoch können diese Überlegungen nur auf eine spezielle Klasse von Goppa Codes angewendet werden.

Die Theorie der Funktionenkörpertürme findet auch in anderen Gebieten der Mathematik Anwendung. In der Finanzmathematik verwendet man oft sogenannte Quasi

Monte-Carlo Verfahren zur Numerischen Integration von Funktionen. Diese Verfahren werten die Funktion an gewissen Punkten aus und bilden dann das Mittel. Die Konvergenz dieses Verfahrens hängt wesentlich von der Verteilung der Punkte, genauer von der Sterndiskrepanz der Punktmenge, ab. Punktfolgen mit geringer Sterndiskrepanz heißen **low-discrepancy sequences** und solche Folgen können mit Mitteln der Theorie der algebraischen Funktionenkörper konstruiert werden (siehe z.B. [30]).

# Literaturverzeichnis

- [1] S. Bosch, Algebra, Springer Verlag, Berlin/Heidelberg/New York, 4. Auflage, 2001.
- [2] P. Beelen, A. Garcia, H. Stichtenoth, On ramification and genus of recursive towers, preprint.
- [3] P. Beelen, A. Garcia, H. Stichtenoth, On towers of function fields of Artin-Schreier type, erscheint in *Bulletin Braz. Math. Soc.*.
- [4] P. Beelen, A. Garcia, H. Stichtenoth, On towers of function fields over finite fields, preprint.
- [5] P. Beelen, A. Garcia, H. Stichtenoth, Towards a classification of recursive towers of function fields over finite fields, preprint.
- [6] J. Bezerra, A. Garcia, H. Stichtenoth, An explicit tower of function fields over cubic finite fields and Zink's lower bound, preprint.
- [7] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, *Abh. Math. Sem. Hamburg* **14** (1941), 197-272.
- [8] G. Dorfer, H. Maharaj, Generalized AG codes and generalized duality, *Finite Fields Appl.* **9** (2003), 194-210.
- [9] D. Eisenbud, Commutative algebra with a view towards algebraic geometry, Graduate Texts in Mathematics, Springer Verlag, Berlin/Heidelberg/New York, 1995.
- [10] N. Elkies, Explicit modular towers, Proceedings of the 35<sup>th</sup> Annual Allerton Conference on Communication, Control and Computing, Urbana, IL, 1997.
- [11] G. L. Feng, T. R. N. Rao, V.K. Wei, Simplified understanding and efficient decoding of a class of algebraic-geometric codes, *IEEE Trans. Inf. Theor.* **40** (1994), 981-1002.
- [12] O. Forster, Riemannsche Flächen, Springer-Verlag, Berlin/Heidelberg/New York, 1977.

- [13] G. Frey, M. Perret, H. Stichtenoth, On the different of Abelian extensions of global Function Fields, "Coding Theory and Algebraic Geometry. Proceedings, Luminy, 1991" Lecture Notes in Math., Vol. 1518, 26-32.
- [14] A. Garcia, H. Stichtenoth, A tower of Artin-Schreier extensions of function fields attaining the Drinfeld-Vladut bound, *Invent. Math.* **121** (1995), 211-222.
- [15] A. Garcia, H. Stichtenoth, On tame towers over finite fields, *J. Reine Angew. Math.* **557** (2003), 53-80.
- [16] A. Garcia, H. Stichtenoth, On the asymptotic behaviour of some towers of function fields over finite fields, *J. Number Theory* **61** (1996), 248-273.
- [17] A. Garcia, H. Stichtenoth, Skew pyramids of function fields are asymptotically bad, Coding Theory, Cryptography and Related Topics, Proceedings of the conference in Guanajuato 1998, Springer-Verlag, Berlin (2000).
- [18] A. Garcia, H. Stichtenoth, M. Thomas, On towers and composita of towers of function fields over finite fields, *Finite Fields Appl.* **3** (1997), 257-274.
- [19] V. D. Goppa, Geometry and Codes, Mathematics and its Applications, **24**, Kluwer Academic Publishers, 1988.
- [20] R. L. Graham, D. E. Knuth, O. Patashnik, Concrete Mathematics, Addison-Weseley, 1990.
- [21] R. Hartshorne, Algebraic Geometry, Graduate Texts in Mathematics, Springer Verlag, Berlin/Heidelberg/New York, 1977.
- [22] H. Hasse, Existenz seperabler zyklischer unverzweigter Erweiterungskörper vom Primzahlgrade  $p$  über elliptischen Funktionenkörpern der Charakteristik  $p$ , *J. Reine Angew. Math.* **172** (1934), 77-85.
- [23] H. Hasse, Theorie der Differentiale in algebraischen Funktionenkörpern mit vollkommenem Konstantenkörper, *J. Reine Angew. Math.* **172** (1934), 55-76.
- [24] H. Hasse, Theorie der relativ zyklischen algebraischen Funktionenkörper, *J. Reine Angew. Math.* **172** (1934), 37-54.
- [25] J. Ihara, Some remarks on the number of rational points of algebraic curves over finite fields, *J. Fac. Sci. Tokyo* **28** (1981), 721-724.
- [26] K. Lamotke, Riemannsche Flächen, Springer Verlag, Berlin/Heidelberg/New York, 2005.
- [27] S. Lang, Algebra, Graduate Texts in Mathematics, Springer Verlag, Berlin/Heidelberg/New York, 2002.

- [28] W. Lütkebohmert, Codierungstheorie. Algebraisch-geometrische Grundlagen und Algorithmen, Vieweg-Studium, 2003.
- [29] Yu. I. Manin, What is the maximum number of points on a curve over  $\mathbb{F}_2$ ?, *J. Fac. Sci. Tokyo* **28** (1981), 715-720.
- [30] H. Niederreiter, C. P. Xing, Rational points on curves over finite fields, London Mathematical Society Lecture Notes Series **285**, Cambridge University Press, 2001.
- [31] O. Pretzel, Codes and Algebraic Curves, Oxford Lecture Series in Mathematics and its Applications, Vol. **8**, Oxford Science Publications, 1998.
- [32] J. H. Silverman, The arithmetic of elliptic curves, *Frad. Texts Math.* **106**, Springer Verlag, Berlin/Heidelberg/New York, 1986.
- [33] I. Reed, G. Solomon, Polynomial Codes over certain finite fields, *SIAM J.*, **8** (1960), 300-304.
- [34] M. Rosen, Number Theory in Function Fields, Graduate Texts in Mathematics, Springer Verlag, Berlin/Heidelberg/New York, 2002.
- [35] P. Samuel, O. Zariski, Commutative Algebra I, University Series in higher Mathematics, D. Van Nostrand Company, Inc., 1958.
- [36] P. Samuel, O. Zariski, Commutative Algebra II, University Series in higher Mathematics, D. Van Nostrand Company, Inc., 1960.
- [37] J. P. Serre, Local Fields, Graduate Texts in Mathematics, Springer Verlag, Berlin/Heidelberg/New York, 1995.
- [38] H. Stichtenoth, Algebraic Function Fields and Codes. Springer Universitext, Springer Verlag, Berlin/Heidelberg/New York, 1993.
- [39] M. A. Tsfasman, S. G. Vladut, T. Zink, Modular curves, Shimura curves and codes, better than the Varshamov-Gilbert bound, *Math. Nachr.* **109** (1982), 21-28.
- [40] M. A. Tsfasman, S. G. Vladut, Algebraic-geometric codes, Kluwer Acad. Publ., Dordrecht-Boston-London 1991.
- [41] H. Weyl, Die Idee der Riemannschen Fläche, Teubner Verlag, 1913,
- [42] E. Witt, Über die Invarianz des Geschlechts eines algebraischen Funktionenkörpers, *J. Reine Angew. Math.* **172** (1934), 75-76.
- [43] J. Wulftange, Zahme Türme algebraischer Funktionenkörper, Doktorarbeit an der Universität Essen, 2003.

# Index

- $\mathcal{O}$ -Notation, 137
- $q$ -näre Entropiefunktion, 7
- Übertragungsrate, 7
  
- absolute Norm, 115
- Adele, 37
- Adeleraum, 37
- affine Komponenten, 50
- affine Kurve, 49
- algebraische Funktionenkörpererweiterung, 61
- algebraischer Funktionenkörper, 13
- Alphabet, 1
- Artin-Schreier Erweiterung, 106
- asymptotisch gut, 123
- asymptotisch optimal, 123
- asymptotisch schlecht, 123
- asymptotische Gilbert-Varshamov Schranke, 9
  
- Bewertungsring, 14
  
- Code, 1
- Codewort, 1
- Conorm, 65
- Cospur, 80
  
- Dedekindring, 73
- Dedekindsche Differentenformel, 85
- Differente, 79
- Differentenexponent, 79
- Dimension eines Divisors, 30
- diskrete Bewertung, 16
- diskreter Bewertungsring, 15
- Divisor, 27
- Divisor eines Weil Differentials, 43
- Divisorgruppe, 27
  
- Divisorklassengruppe, 28
- dualer Code, 3
  
- Eisensteinsches Kriterium, 100
- endliche Funktionenkörpererweiterung, 62
- endlicher Verzweigungstyp, 124
  
- Fundamentalgleichung von Hilbert, 67
- Funktionenkörper einer Kurve, 50
- Funktionenkörperturn, 121
  
- galoisscher Turm, 125
- ganz, 68
- ganz abgeschlossen, 68
- ganzer Abschluß, 68
- Ganzheitsbasis, 76
- Generatormatrix, 3
- Generatorpolynom, 4
- geometrischer Goppa Code, 52
- gerader Turm, 123
- Geschlecht, 33
- Grad einer Stelle, 18
- Gruppencodes, 3
  
- Hammingdistanz, 2
- Hamminggewicht, 3
- Hasse-Weil, 117
- Hauptadele, 38
- Hauptdivisor, 28
- Hauptdivisorengruppe, 28
- Hilbertsche Differentenformel, 113
- Holomorphierung, 70
- Hurwitzsche Geschlechtsformel, 85
  
- kanonischer Divisor, 43
- Klassenzahl, 116
- Komplementärmodul, 78

- Konstantenkörper, 13
- Konstantenkörpererweiterung, 62
- Kontrollmatrix, 4
- Kummer Erweiterungen, 102
  
- L-Polynom, 116
- Linearcode, 3
- lokale Komponente, 46
- lokaler Koordinatenring, 50
- low-discrepancy Sequence, 144
  
- Maximum Likelihood Decodierung, 2
- MDS-Code, 6
- Minimaldistanz, 2
  
- Nachrichtenwort, 1
- Nullstellendivisor, 28
  
- Poldivisor, 28
- Polynomcode, 4
- positiver Divisor, 27
- primes Element, 16
- projektive Kurve, 49
- projektiver Abschluss, 50
  
- rationale Kurve, 50
- rationale Punkte, 49
- rationaler Funktionenkörper, 14
- rekursiver Turm, 123
- relative Minimaldistanz, 7
- relativer Grad, 64
- Restklassenabbildung einer Stelle, 18
- Restklassenkörper, 18
- Riemann-Roch Raum, 28
  
- Satz von Riemann-Roch, 44
- Satz von Tsfasman-Vladut-Zink, 59
- schiefer Turm, 123
- singulärer Punkt; regulärer Punkt, 50
- Spezialitätenindex, 38
- starker Approximationssatz, 45
- Stelle, 16
- systematischer Code, 2
  
- Träger eines Divisors, 27
  
- Trägheitsgruppe, 108
- Trägheitskörper, 108
  
- Unendlichkeitsstelle, 21
- Unterring, 70
  
- Verzweigungsgruppe, 111
- Verzweigungsindex, 64
- Verzweigungsort, 124
- vollständig zelegt, 111
  
- Weil Differential, 40
- wilder Turm, 123
- wildverzweigt, 91
  
- zahmer Turm, 123
- zahnverzweigt, 91
- Zerfallungsort, 124
- Zerlegungsgruppe, 108
- Zerlegungskörper, 108
- Zetafunktion, 115
- zyklische Codes, 5