DIPLOMARBEIT

Algebraisch-geometrische Codes

ausgeführt am Institut für Geometrie

der Technischen Universität Wien

unter der Anleitung von Ao.Univ.Prof. Dr. Michael Drmota

durch

Clemens Fuchs

Novaragasse 24/15
1020 Wien

10. August 2000 .....

Vorwort

Durch den Eintritt der Industriestaaten in das Informationszeitalter und die revolutionären Erneuerungen im Bereich der Unterhaltungselektronik, haben in den letzten Jahrzehnten Methoden zur Fehlerbehandlung bei der Datenübertragung eine bedeutendere Rolle denn je erlangt. Diese sind das Forschungsgebiet der Codierungstheorie, dessen Ergebnisse jetzt von jedermann, ob beim Internetsurfen, Telefonieren oder beim Abspielen einer CD, bewusst oder unbewusst genutzt werden. Codes mit guten Fehlererkennungs- und -korrektureigenschaften werden benötigt, um die notwendigen Datenübertragungen möglich zu machen.

Es ist ein wohlbekanntes Problem der Codierungstheorie, dass lange Codes mit günstigen Eigenschaften schwierig zu konstruieren sind. Die Gilbert-Varshamov-Schranke besagt, dass eine Folge von Codes mit wachsender Blocklänge, hohen Informationsraten und entsprechend guten Fehlerkorrektureigenschaften existiert. Man nennt solche Familien von Codes „gut“. Der Beweis dieses Satzes ist allerdings nicht konstruktiv, er enthält also keinen Hinweis wie man derartige Codes konstruieren kann.

Einer der wichtigsten Fortschritte in der Theorie der fehlerkorrigierenden Codes war die Verwendung von Methoden aus der algebraischen Geometrie. Diese Entdeckung geht auf V. D. Goppa zurück der 1981 die Klasse der geometrischen Goppa-Codes (auch algebraisch-geometrische Codes genannt) eingeführt hat (siehe [7]). Geometrische Goppa-Codes haben hervorragende asymptotische Eigenschaften und Goppa konnte zeigen, dass diese Codes die Gilbert-Varshamov-Schranke erreichen. Das war der erste Fortschritt innerhalb von 30 Jahren. Tsfasman, Vlădut und Zink zeigten 1982, dass mit Hilfe von geometrischen Goppa-Codes, die Gilbert-Varshamov-Schranke sogar noch verbessert werden kann. Alle diese Ergebnisse waren aber nach wie vor nicht konstruktiv. Mittlerweile gibt es allerdings sogar schon die ersten expliziten Beschreibungen solcher Codes (siehe z.B. [18]).

In den letzten Jahren entdeckten Xing, Niederreiter und Lam neue Methoden um Codes mit Hilfe der algebraischen Geometrie zu konstruieren (siehe [15], [25] und [26]), indem sie ihre Konstruktionen im Zusammenhang

mit low-discrepancy sequences (siehe [13] und [24]) betrachteten. Dabei verwendeten sie Ansätze, die sich wesentlich von denen Goppas unterschieden. Özbudak und Stichtenoth fanden durch Verallgemeinerung dieser Konstruktionen eine äquivalente Beschreibung der geometrischen Goppa-Codes (siehe [16]). Neue Einblicke in die Natur dieser Codes ergeben sich durch die Betrachtung von Spezialklassen, die man durch die Konstruktionen von Xing, Niederreiter und Lam erhält (siehe [25]).

Insbesondere die letzten Konstruktionen von Xing, Niederreiter und Lam (siehe [15] und [26]), die eine echte Verallgemeinerung der geometrischen Goppa-Codes darstellen und daher den Namen verallgemeinerte algebraisch-geometrische Codes bekommen haben, scheinen sehr vielversprechend zu sein. Es handelt sich dabei zweifellos um eine weitreichende und sehr interessante Verallgemeinerung der geometrischen Goppa-Codes. Man kann mit ihrer Hilfe sehr gute - ja sogar bestmögliche - Beispiele für Codes über kleinen Alphabeten angeben, was mit Hilfe von geometrischen Goppa-Codes nicht möglich zu sein scheint.

Diese Arbeit soll die oben erwähnten Themen aufarbeiten und ist folgendermaßen gegliedert:

Im ersten Kapitel werden die Grundlagen der Codierungstheorie dargestellt. Die dazu notwendigen Begriffe, wie Codes, Gewicht und Distanz, Fehlererkennung und Fehlerkorrektur, etc., werden exakt eingeführt und die wichtigsten Eigenschaften bewiesen. Im Abschnitt 1.5 wird die Gilbert-Varshamov-Schranke formuliert und bewiesen und die Probleme, die sich daraus ergeben, aufgezeigt. In Abschnitt 1.6 behandeln wir die in den Anwendungen (bisher) am häufigsten verwendeten Codes, die BCH-Codes und geben dadurch weitere Motivation zur Suche nach guten Codes. Dieser Teil der Arbeit richtet sich vor allem nach dem Buch von Pretzel (siehe [17]).

Im zweiten Kapitel wird die Sprache entwickelt, um algebraisch-geometrische Codes betrachten zu können, nämlich die Theorie der algebraischen Funktionenkörper. Solche algebraische Objekte treten in natürlicher Weise in vielen Bereichen der Mathematik auf, wie etwa in der algebraischen Geometrie, der algebraischen Zahlentheorie oder in der komplexen Analysis. Tatsächlich ist die Theorie der algebraischen Funktionenkörper äquivalent zur Theorie der algebraischen Kurven. Wir wählen aber den rein algebraischen Zugang, da man dadurch relativ schnell zum Hauptergebnis, dem Satz von Riemann-Roch kommt, der in Abschnitt 2.6 behandelt wird. Durch diese Vorgangsweise erspart man sich viel Topologie, die beim Studium der algebraischen Kurven notwendig ist und die man zusätzlich zur Algebra benötigt. Dieses Kapitel stammt zum größten Teil aus dem Buch von Stichtenoth (siehe [19]) und zu einem kleineren Teil aus dem Buch von Pretzel

(siehe [18]).

Im dritten Kapitel können wir die geometrischen Goppa-Codes einführen und mit Hilfe des Satzes von Riemann-Roch deren Parameter abschätzen. Dabei werden wir zwei Beschreibungen von Goppa und eine Beschreibung nach Xing - Niederreiter - Lam und Özbudak - Stichtenoth kennenlernen. In Abschnitt 3.3 untersuchen wir spezielle Klassen von geometrischen Goppa-Codes: die rationalen Goppa-Codes, welche die BCH-Codes als Spezialfall enthalten, und die sogenannten XNL-Codes, welche auf den Konstruktionen von Xing, Niederreiter und Lam beruhen. Im Abschnitt 3.4 schließlich, werden wir die Beziehung zwischen den geometrischen Goppa-Codes und der asymptotischen Gilbert-Varshamov-Schranke kennenlernen und sehen, dass sie durch diese verbessert werden kann. Dieses Kapitel beruht hauptsächlich auf dem Buch von Stichtenoth (siehe [19]) und weiters auf den Arbeiten von Xing, Niederreiter, Lam und Özbudak, Stichtenoth (siehe [15],[25],[26] und [16]).

Das vierte und letzte Kapitel beschäftigt sich schlußendlich mit den verallgemeinerten algebraisch-geometrischen Codes, ihrer Konstruktion und es wird eine interessante Teilklasse vorgestellt, die eine offensichtliche Verallgemeinerung der geometrischen Goppa-Codes ist. Im Abschnitt 4.2 wird sich zeigen, dass wir dadurch Codes gewinnen können, die in einem gewissen Sinne Weltrekorde sind.

Abschließend möchte ich mich noch herzlich bei Herrn Prof. Niederreiter bedanken, der das Thema vorgeschlagen hat und bei der Literaturauswahl federführend war. Weiterer Dank gebührt meinem Betreuer Herrn Prof. Drmota und nicht zuletzt meinem Bruder Michael, für das sorgfältige Korrekturlesen.

Wien, August 2000 Clemens Fuchs

Inhaltsverzeichnis

Kapitel 1

Grundlagen der Codierungstheorie

1.1 Einführung

Die Anwendungsgebiete der Codierungstheorie sind sehr vielfältig, jedoch haben alle folgendes gemeinsam: Informationen sollen von einer Quelle über einen Informationskanal zu einem Empfänger geschickt werden. Dabei treten in der Regel Fehler auf. Ziel der Codierungstheorie ist es, Strategien zu entwickeln, die bei der Übertragung aufgetretenen Fehler zu erkennen und zu korrigieren. Beispiele für solche Übertragungen sind: gesprochene Nachrichten, Funk, Audiosysteme, Fernsehen, Computernetze, Satellitenkommunikation, Datenspeicherung, usw.

Um Fehler zu erkennen bzw. zu korrigieren, werden die folgenden beiden Prinzipien angewandt:

- Redundanz,
- Grammatik.

Diese Prinzipien sind uns von der natürlichen Sprache her wohlbekannt. Die Wörter in unserer Sprache bilden nur einen sehr kleinen Teil der möglichen Zeichenketten. Außerdem ergeben nur wenige Folgen von Wörtern einen Satz. Wir können sagen, dass mit sehr großer Wahrscheinlichkeit ein Fehler nur wenige Buchstaben betreffen wird. Da in der natürlichen Sprache die Anzahl der Worte, die man durch Änderung von nur wenigen Buchstaben ineinander überführen kann, gering ist, wird ein falsch geschriebenes Wort mit großer Wahrscheinlichkeit als solches erkannt, und da nur wenige mögliche Kandidaten als korrekte Version in Frage kommen, kann man es vielleicht sogar korrigieren. Insbesondere kann dazu die Grammatik nutzbringend eingesetzt werden.

Im folgenden wollen wir stets annehmen, dass eine Nachricht aus den *Symbolen* einer festen, endlichen Menge A aufgebaut ist, die wir das *Alphabet* nennen. Das Alphabet soll ein *Nullsymbol* besitzen, welches wir mit 0 bezeichnen.

Als erstes wollen wir den Kanal modellieren über den wir die Informationen senden. Dieses Modell wird natürlich umso komplizierter, je besser wir versuchen die Wirklichkeit nachzubilden. Das einfachste Modell erhält man unter der Annahme, dass es zu jedem Paar verschiedener Symbole a,$b \in A$ eine feste Wahrscheinlichkeit $p_{a,b}$ gibt, die angibt mit welcher Wahrscheinlichkeit b empfangen wird, wenn a gesendet wurde. Man spricht von einem *Zufallsfehler-Kanal*. Außerdem wollen wir noch annehmen, dass die Wahrscheinlichkeiten $p_{a,b}$ dieselben sind für alle Paare a, b mit $a \neq b$. Einen solchen Kanal nennt man *symmetrisch*. Im folgenden wollen wir stets annehmen, dass wir einen symmetrischen Zufallsfehler-Kanal haben.

Die nächste Stufe in unserem Modell ist der *Encoder*. Dieser wandelt die Eingangsnachricht um, sodass Fehler erkannt und korrigiert werden können. Zum Schluß benötigen wir noch einen *Decoder*, der die ursprüngliche Nachricht wieder herstellt, nachdem der *Fehler- Prozessor* die Nachricht auf eventuelle Fehler untersucht, diese korrigiert, oder mit einem Fehlersignal abgebrochen hat.

1.2 Blockcodes, Gewicht und Distanz

Wir wollen stets annehmen, dass unser Encoder (den wir gleich definieren werden) die Nachricht in *Wörter* bzw. *Blöcke* zerlegt, das heißt in Folgen von Symbolen fester Länge k. Der Encoder übersetzt jedes Wort in ein *Codewort* mit fester Länge n. Solche Codes nennt man *Blockcodes*.

Definition 1.2.1 Es sei A ein Alphabet. Eine Folge von n Symbolen aus A nennen wir ein *A-Wort* (oder kurz *Wort*) der Länge n. Die Menge aller A-Wörter der Länge n bezeichnen wir mit A^n.

Wenn A aus q Symbolen besteht, dann gibt es genau q^n A-Wörter der Länge n. Wir können jetzt Blockcodes formal definieren:

Definition 1.2.2 Ein $[n, k]$-*Blockcode* C über einem Alphabet A mit q Elementen ist eine Teilmenge von A^n bestehend aus genau q^k Codewörtern. Ein *Encoder* E für C ist eine bijektive Abbildung von A^k nach C, welche jedem A-Wort x der Länge k ein Codewort $u = E(x)$ zuordnet. Der dazugehörige *Decoder* D ist die zu E inverse Abbildung. Die Zahl n heißt *Länge* des Co-

des, k heißt der *Rang* oder die *Dimension* des Codes und k/n heißt die *Rate* des Codes C.

Der Encoder setzt das Codewort oft so zusammen, daß das Nachrichtenwort x der Anfang des Codewortes $E(x)$ ist. Einen solchen Encoder nennen wir *systematisch*. In diesem Fall besteht das Codewort aus dem Nachrichtenwort und den *Prüfziffern*. Der Decoder lässt lediglich die Prüfzeichen weg. Da $k \leq n$ ist, muss die Rate stets ≤ 1 sein.

Zunächst wollen wir die Methoden zur Fehlererkennung und Fehlerkorrektur betrachten, welche nur das Redundanzprinzip verwenden. Sei also $C \subseteq A^n$. Jedes $w \in A^n$ heißt ein *Empfangswort*. Ist $w \in F := A^n \backslash C$, so hat ein Übertragungsfehler stattgefunden. Ist $w \in C$, so kann man trotzdem die Möglichkeit eines Fehlers nicht ausschließen.

Definition 1.2.3 Für $v = (v_1, \ldots, v_n)$, $w = (w_1, \ldots, w_n) \in A^n$ heißt die Anzahl der Stellen $i \in \{1, \ldots, n\}$ mit $v_i \neq w_i$ (*Hamming-*) *Distanz* $d(v, w)$ von v, w. Das (*Hamming-*) *Gewicht* $\mathrm{wt}(v)$ von v ist die Anzahl der von 0 verschiedenen Einträge von v.

Satz 1.2.4 *Die Hamming-Distanz ist eine Metrik auf* A^n.

Beweis. Aus der Definition folgt sofort, dass $d(v, w)$ stets eine positive, reelle Zahl ist, dass $d(v, w) = 0 \Leftrightarrow v = w$ gilt und dass $d(v, w) = d(w, v)$ ist. Es bleibt also die Dreiecksungleichung zu zeigen: Sei $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$ und $z = (z_1, \ldots, z_n)$. Dann ist $d(x, z)$ gleich der Anzahl der Stellen in denen sich x und z unterscheiden. Sei U die Menge der Indizes dieser Stellen, dann ist

$$d(x, z) = |U| = |\{i \,|\, x_i \neq z_i\}|.$$

Sei $S = \{i \,|\, x_i \neq z_i \text{ und } x_i = y_i\}$ und $T = \{i \,|\, x_i \neq z_i \text{ und } x_i \neq y_i\}$. Dann ist U die disjunkte Vereinigung von S und T. Also gilt

$$d(x, z) = |S| + |T|.$$

Aus der Definition von $d(x, y)$ und T folgt daher, dass

$$|T| \leq d(x, y).$$

Andererseits gilt für $i \in S$, dass $y_i = x_i \neq z_i$ ist. Es folgt

$$|S| \leq d(y, z),$$

und damit insgesamt $d(x, z) \leq d(x, y) + d(y, z)$. □

Definition 1.2.5 Ein *Fehler-Prozessor* P für einen $[n, k]$-Code C über A

ist eine Abbildung, die einem Empfangswort w das Paar (a, u) zuordnet, wobei a die Werte „gut“ oder „schlecht“ annehmen kann und u ein Wort der Länge n ist. Dabei hat das Signal a hat den Wert „gut“, wenn w ein Codewort ist und sonst „schlecht“. Ein Fehler-Prozessor, der stets $u = w$ liefert, nennt man einen *Fehler-Detektor* und einen, der stets ein Codewort von C zurückliefert nennt man *perfekt*.

Das Prinzip der Decodierung ist das Folgende: Wird $w \in A^n$ empfangen, so werden wir annehmen, dass es von einem $c \in C$ stammt, für welches $d(c, w)$ minimal ist. Gibt es ein solches c, so wird w als dieses c decodiert. Gibt es mehr als ein solches c, dann erhält man keine eindeutige Entscheidung.

Definition 1.2.6 Es sei v ein gesendetes A-Wort und $w \in A^n$ das empfangene Wort. Weiters sei $t := d(v, w)$. Dann heißt t die *Anzahl der Übertragungsfehler* und wir sagen, dass t *Fehler aufgetreten sind*, oder dass ein *Fehler mit Gewicht* t stattgefunden hat.

Definition 1.2.7 Sei P ein Fehler-Prozessor für einen $[n, k]$-Code C über A. Wir sagen, P kann *alle Fehler vom Gewicht* $\leq t$ *erkennen*, wenn kein Codewort durch einen Fehler mit Gewicht $\leq t$ in ein anderes Codewort übergeführt werden kann. Wir sagen außerdem, P kann *alle Fehler vom Gewicht* $\leq t$ *korrigieren*, wenn zu jedem Empfangswort $w \in A^n$ genau ein Codewort c mit $d(w, c) \leq t$ existiert.

Ein Fehler-Prozessor überprüft also zuerst, ob das Empfangswort w ein Codewort ist oder nicht. Wenn w ein Codewort ist, dann ist die Aufgabe des Fehler-Prozessors beendet, dass Wort wird als „gut“ bewertet und weitergeleitet. Das bedeutet, wenn ein Fehler so auftritt, dass ein Codewort in ein anderes gestört wird, dann kann dieser Fehler nicht entdeckt und damit auch nicht korrigiert werden. Wenn wir alle Fehler bis zum Gewicht t erkennen wollen, ist es klarerweise notwendig, dass zwei verschiedene Codewörter mindestens Distanz $t + 1$ haben. Deshalb liegt es auf der Hand, folgendes Maß für den kleinstmöglichen Abstand zwischen verschiedenen Codewörtern einzuführen.

Definition 1.2.8 Sei C ein $[n, k]$-Code über A. Wir nennen

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

die *Minimaldistanz* von C. Dieses Maß ist so wichtig, dass wir C auch einen $[n, k, d]$-Code nennen.

Es gilt dann der folgende Satz:

Satz 1.2.9 *Sei C ein $[n,k]$-Code über A und $t \in \mathbb{N}$. Dann kann ein Fehler-Prozessor für C alle Fehler mit Gewicht $\leq t$ erkennen, genau dann wenn $d \geq t+1$ ist.*

Beweis. Wenn u und v Codewörter sind mit $u \neq v$ und $d(u,v) \leq t$, dann kann u in v durch einen Fehler vom Gewicht $\leq t$ übergeführt werden. In diesem Fall kann kein Fehler-Prozessor für C alle Fehler vom Gewicht $\leq t$ erkennen. Umgekehrt gilt, wenn je zwei Codewörter mindestens Distanz $t+1$ voneinander haben, dann führt ein Fehler vom Gewicht t ein Codewort in ein Wort über das kein Codewort ist. Der Fehler kann also entdeckt werden, indem man überprüft, ob das empfangene Wort ein Codewort ist. Also sind alle Fehler mit Gewicht $\leq t$ erkennbar. □

Satz 1.2.10 *Es gibt einen Fehler-Prozessor für den $[n,k]$-Code C über A, welcher alle Fehler bis zum Gewicht $t \in \mathbb{N}$ korrigiert, dann und nur dann, wenn $d \geq 2t+1$.*

Beweis. Angenommen es gibt Codewörter u und v mit $u \neq v$ und $d(u,v) \leq 2t$. Sei w ein Wort das mit u an allen Stellen übereinstimmt, an denen u mit v übereinstimmt. Weiters soll w mit u an den ersten t Stellen übereinstimmen, an denen u und v nicht übereinstimmen und an den restlichen Stellen soll w mit v übereinstimmen (wenn $d(u,v) < t$ dann wählen wir $w = u$). Dann gilt: $d(u,w) \leq t$ und $d(v,w) \leq t$. Angenommen w wird zusammen mit der Information empfangen, dass höchstens t Fehler aufgetreten sind. Dann kann sowohl u als auch v (oder ein ganz anderes Wort) gesendet worden sein. Also gibt es keinen Fehler-Prozessor der Fehler vom Gewicht $\leq t$ korrigieren kann.
Umgekehrt nehmen wir an, dass ein Wort w zusammen mit der Information empfangen wurde, dass höchstens t Fehler aufgetreten sind. Wenn es zwei Codewörter u und v mit $d(u,w) \leq t$ und $d(v,w) \leq t$ geben würde, dann müßte $d(u,v) \leq 2t$ gelten. Widerspruch zur Annahme, dass $d \geq 2t+1$ gilt. Also gibt es ein eindeutiges Wort u mit $d(u,w) \leq t$, und wir decodieren w durch u. □

1.3 Linearcodes

Als nächstes wollen wir das Prinzip der Grammatik nachbilden, indem wir dem Alphabet A und damit auch A^n, sowie dem Code C Struktur verleihen. Dies führt uns zum Begriff des *Linearcodes*.

Definition 1.3.1 Sei das Alphabet A der endliche Körper $\mathbb{F}_q$ mit q Ele-

menten. Dann heißt ein $[n,k]$-Code C über A ein *Linearcode*, wenn C ein Unterraum des Vektorraumes A^n ist.

Wenn C ein $[n,k]$-Linearcode über $\mathbb{F}_q$ ist, dann ist $k = \dim(C)$. Wir nützen diese Struktur um die Minimaldistanz eines Linearcodes zu charakterisieren.

Satz 1.3.2 *Für einen $[n,k]$-Linearcode C über $\mathbb{F}_q$ ist die Minimaldistanz gleich dem minimalen Gewicht aller vom Nullwort verschiedenen Codewörter.*

Beweis. Für Codewörter u und v gilt $d(u,v) = \mathrm{wt}(u-v)$. Aufgrund der Linearität ist $u-v$ wieder ein Codewort. □

Wenn ein Wort c gesendet und $y \in A^n$ empfangen worden ist, so heißt $e = y - c$ *Fehlerwort* (*Fehlermuster* oder kurz *Fehler*) von c. Es gilt:

$$\mathrm{wt}(e) = \mathrm{wt}(y-c) = d(y,c) = \text{Anzahl der Übertragungsfehler.}$$

Wenn wir mit Linearcodes arbeiten, dann werden wir stets verlangen, dass der Encoder die Linearität respektiert. Deshalb definieren wir:

Definition 1.3.3 Ein *linearer* Encoder E für einen $[n,k]$-Linearcode C über $\mathbb{F}_q$ ist ein Isomorphismus von $\mathbb{F}_q^k$ auf C.

Da wir nun nur mehr Linearcodes betrachten, sprechen wir in der Folge kurz von einem Encoder.

Definition 1.3.4 Sei C ein linearer $[n,k]$-Code über $\mathbb{F}_q$ mit Encoder E. Sei G jene $k \times n$ - Matrix, sodass $E(x) = xG$ für jedes Wort x mit Länge k ist. Dann heißt G eine *Generatormatrix* des Codes C.

Wenn wir also eine Generatormatrix G eines $[n,k]$-Codes C über $\mathbb{F}_q$ gegeben haben, dann ist durch $E(x) := xG$ eindeutig ein Encoder für C definiert. Wir haben einen Encoder systematisch genannt, wenn das Nachrichtenwort genau die ersten k Symbole des zugehörigen Codewortes sind. Diese Eigenschaft kann man sehr leicht an der Generatormatrix ablesen.

Satz 1.3.5 *Sei C ein linearer $[n,k]$-Code über $\mathbb{F}_q$ mit Generatormatrix G. Dann ist der zugehörige Encoder systematisch, dann und nur dann, wenn die ersten k Spalten von G die $k \times k$ Einheitsmatrix I_k bilden.*

Beweis. Die Spalten von G sind Gleichungen, mit deren Hilfe man aus den Symbolen eines Elementes x das Codewort u für x gewinnt. Deshalb sind die ersten k Symbole von u die Symbole von $x \Leftrightarrow$ wenn die ersten k Spalten

von G $(1,0,\ldots,0)^T, (0,1,0,\ldots,0)^T, \ldots, (0,\ldots,0,1)^T$ lauten. $\square$

Wir nennen eine Generatormatrix G daher *systematisch*, wenn der dazugehörige Encoder systematisch ist (also wenn die ersten k Spalten von G gleich I_k sind). Klarerweise kann ein Code mehrere verschiedene Generatormatrizen besitzen. Der folgende Satz gibt eine einfache, notwendige und hinreichende Bedingung um festzustellen, ob eine Matrix eine Generatormatrix eines Linearcodes ist.

Satz 1.3.6 *Sei C ein $[n,k]$-Linearcode über $\mathbb{F}_q$ und sei G eine $k \times n$-Matrix. Dann ist G eine Generatormatrix von C, dann und nur dann, wenn die Zeilen von G eine Basis von C bilden.*

Beweis.
$\Rightarrow$: Nach Voraussetzung ist E eine bijektive Abbildung von $\mathbb{F}_q^k$ nach C. Die Zeilen von G sind die Bilder der Nachrichtenwörter $(1,0,\ldots,0), (0,1,0,\ldots,0), \ldots, (0,\ldots,0,1)$ und bilden daher eine Basis von C.
$\Leftarrow$: Bezeichnen wir die Zeilen von G mit $g_1, \ldots g_k$. Multiplikation des Nachrichtenwortes $(a_1,\ldots,a_k)$ mit G gibt das Wort $a_1g_1 + \cdots + a_kg_k$. Nach Annahme ist das eine Linearkombination von Codewörtern. Da C ein Linearcode ist, handelt es sich dabei wieder um ein Codewort. G bildet $\mathbb{F}_q^k$ also auf einen Teilraum von C ab. Die Dimension dieses Teilraumes ist k, daher haben wir eine bijektive Zuordnung, also einen Encoder für C. $\square$

Einer der Hauptgründe, Linearcodes zu verwenden, ist die Tatsache, dass man sehr einfach überprüfen kann, ob ein Empfangswort ein Codewort ist oder nicht.

Definition 1.3.7 Eine *Kontrollmatrix* für einen $[n,k]$-Linearcode C über $\mathbb{F}_q$ ist eine $l \times n$-Matrix H, mit der Eigenschaft, dass für $v \in \mathbb{F}_q^n$ gilt:

$$Hv^T = 0 \Leftrightarrow v \in C$$

Die Zahl l ist zunächst beliebig. Wir werden sehen, dass der kleinstmögliche Wert $n-k$ ist. Wir sagen eine Kontrollmatrix sei *systematisch*, wenn sie von der Gestalt (D,J) ist, wobei J die $(n-k) \times (n-k)$ Einheitsmatrix ist. Es gilt die folgende, sehr einfache Beziehung zwischen systematischer Generator- und Kontrollmatrix.

Satz 1.3.8 *Es sei C ein $[n,k]$-Linearcode über $\mathbb{F}_q$. Dann gilt:*
Falls C eine systematische Generatormatrix G besitzt, dann auch eine systematische Kontrollmatrix H und umgekehrt. Insbesondere wird eine durch die andere eindeutig bestimmt, denn in diesem Fall gilt: Sei $G = (I, A)$ und

$H = (B, J)$, *dann ist* $A = -B^T$.

Beweis. Zunächst sollen systematische Generatormatrix G und systematische Kontrollmatrix H existieren. Dann haben sie die Form $G = (I, A)$ und $H = (B, J)$. Es gilt dann $HG^T = 0$, da die Zeilen von G Codewörter sind. Also erhalten wir $BI + JA^T = 0$. Also folgt $B = -A^T$. Deshalb wird G durch H bestimmt und umgekehrt, also sind beide eindeutig und sie haben die angegebene Form.
Wenn nun $G = (I, A)$ eine systematische Kontrollmatrix ist, dann zeigen wir, dass durch $H = (-A^T, J)$ eine systematische Kontrollmatrix definiert wird. Sei $v = uG$ für ein u. Wegen $HG^T = 0$ folgt aus $v = uG$, dass $Hv^T = HG^T u^T = 0u^T = 0$ ist. Daher ist H eine Kontrollmatrix und sie ist sytematisch. Umgekehrt sei $H = (B, J)$ gegeben. Wir setzen $G = (I, -B^T)$ und zeigen G ist eine Generatormatrix. Sei also $Hv^T = 0$. Wir zerlegen v in (u, w), wo u aus den ersten k Symbolen von v besteht. Dann gilt $Hv^T = 0 \Leftrightarrow -A^T u^T + Jw^T = -A^T u^T + w^T = 0$. Also gilt $w = uA$ und damit $v = (u, w) = (u, uA) = (I, A)u = uG$. □

Die Frage, ob jeder Code eine systematische Generatormatrix besitzt, beantwortet der folgende Satz:

Satz 1.3.9 *Sei C ein $[n, k]$-Linearcode über $\mathbb{F}_q$. Dann können die Codewörter so permutiert werden, dass der permutierte Code $\widetilde{C}$ eine systematische Generatormatrix besitzt.*

Beweis. Sei G eine Generatormatrix von C. Durch elementare Zeilenoperationen ist es möglich die Matrix G in eine Matrix G' überzuführen , sodass diese folgende Eigenschaften hat: Der erste Eintrag $\neq 0$ der $(i+1)$-ten Zeile erfolgt später als der von der i. Zeile. Der erste Eintrag $\neq 0$ jeder Zeile ist 1. Alle anderen Einträge in der Spalte, die die 1 enthält sind 0.
Die Zeilen von G' sind Linearkombinationen der Zeilen von G und daher Codewörter. Dann permutieren wir die Spalten von G', so dass die 1 in der i. Zeile in der i. Spalte steht. Die so erhaltene Matrix bezeichnen wir mit G''. Diese Permutation entspricht einer Permutation der Symbole der Codewörter von C. Den permutierten Code nennen wir $\widetilde{C}$. Nach Konstruktion beginnt G'' mit der $k \times k$ Einheitsmatrix und ist eine Generatormatrix für $\widetilde{C}$, da die Spalten eine Basis für $\widetilde{C}$ bilden. □

Nun wollen wir die Behauptung über die Größe der Kontrollmatrix zeigen:

Satz 1.3.10 *Sei C ein $[n, k]$-Linearcode über $\mathbb{F}_q$ und H eine Kontrollmatrix für C. Dann gilt:*

(a) rank $H = n - k$.
(b) *H hat mindestens $n - k$ Zeilen.*
(c) *Sei K eine Matrix, die aus H durch Hinzufügen von weiteren Zeilen entsteht, die Linearkombinationen der Zeilen von H sind, dann ist K ebenfalls eine Kontrollmatrix für C.*

Beweis.
(a) Da H eine Kontrollmatrix für C ist, folgt, dass C der Kern der linearen Abbildung H ist. Aus der Rangformel folgt rank $H = n - k$.
(b) Der Rang ist höchstens gleich der Anzahl der Zeilen einer Matrix.
(c) Trivial. □

Wir wollen noch eine andere Beschreibung der Kontrollmatrix eines Codes geben.

Definition 1.3.11 Das *kanonische innere Produkt* in $\mathbb{F}_q^n$ ist definiert durch

$$\langle a, b\rangle := \sum_{i=1}^{n} a_i b_i,$$

für $a = (a_1, \ldots, a_n)$ und $b = (b_1, \ldots, b_n) \in \mathbb{F}_q^n$. Offensichtlich liefert das eine nicht ausgeartete symmetrische Bilinearform auf $\mathbb{F}_q^n$.

Definition 1.3.12 Sei C ein $[n, k]$-Linearcode über $\mathbb{F}_q$. Dann heißt

$$C^\perp := \{u \in \mathbb{F}_q^n \mid \langle u, c\rangle = 0 \text{ für alle } c \in C\}$$

der zu C *duale Code.*

Aus der linearen Algebra wissen wir, dass der duale Code zu einem $[n, k]$-Linearcode über $\mathbb{F}_q$ ein $[n, n - k]$-Linearcode über $\mathbb{F}_q$ ist. Der duale Code lässt sich sehr einfach mit Hilfe der Kontrollmatrix von C beschreiben.

Satz 1.3.13 *Sei H eine Kontrollmatrix eines linearen $[n, k]$-Codes C über $\mathbb{F}_q$ mit $n - k$ Zeilen. Dann ist H eine Generatormatrix des zu C dualen Codes $C^\perp$.*

Beweis. Sei $U = \{vH \mid v \in \mathbb{F}_q^{n-k}\}$. Wir zeigen, dass $U = C^\perp$ gilt.
1. Klarerweise ist U ein Teilraum von $\mathbb{F}_q^n$ mit $\dim U = n - k$.
2. Sei G eine Generatormatrix von C. Jedes $u \in U$ ist orthogonal zu jedem $c \in C$, denn für $u = vH$ und $c = aG$ gilt, wegen $HG^T = 0$,

$$\langle u, c\rangle = uc^T = (vH)(aG)^T = v(HG^T)a^T = 0.$$

Also ist $U \subseteq C^\perp$.
Da der Unterraum $U \subseteq C^\perp$ und $\dim U = \dim C^\perp = n - k$ ist, folgt die

Behauptung. □

Zum Schluss zeigen wir, dass in der Kontrollmatrix die ganze Information über die Minimaldistanz des Codes steckt.

Satz 1.3.14 *Sei C ein $[n,k]$-Linearcode über $\mathbb{F}_q$ mit Kontrollmatrix H. C hat Minimaldistanz $> d$, dann und nur dann, wenn es keine Menge mit d Spalten von H gibt, die linear abhängig sind.*

Beweis. Wir bezeichnen die Spalten von H mit $h_1, \ldots, h_n$. Angenommen es existiert ein Codewort $c = (c_1, c_2, \ldots, c_n) \neq 0$ mit Gewicht $\leq d$. Wir müssen zeigen, dass H eine linear abhängige Menge von d Spalten besitzt. Da c ein Codewort ist, gilt

$$Hc^T = c_1h_1 + c_2h_2 + \cdots + c_nh_n = 0.$$

Wir wählen eine Menge von genau d Spalten von H, wo alle jene Spalten h_i vorkommen, in denen $c_i \neq 0$ ist. Diese Spalten seien o.B.d.A. $h_1, \ldots, h_d$. Wegen $c_i = 0$ für $i > d$, gilt dann

$$c_1h_1 + c_2h_2 + \cdots + c_dh_d = 0.$$

Da $c \neq 0$ ist, muß mindestens einer der Koeffizienten $c_i \neq 0$ sein. Die Menge $\{h_1, \ldots, h_d\}$ ist also linear abhängig.
Umgekehrt gilt für eine linear abhängige Menge von d Spalten von H (wir nehmen wieder o.B.d.A. an, dass sie wie oben numeriert sind), dass Koeffizienten $c_i, i = 1, \ldots d$ nicht alle 0 existieren, sodass

$$c_1h_1 + c_2h_2 + \cdots + c_dh_d = 0$$

gilt. Definieren wir $c_i = 0$ für $i > d$, dann haben wir ein Codewort $c = (c_1, \ldots, c_n)$ ungleich dem Nullwort gefunden, da gilt

$$Hc^T = c_1h_1 + \cdots + c_nh_n = 0.$$

Da $\mathrm{wt}(c) \leq d$ gilt, muss die Minimaldistanz $\leq d$ sein. □

Wenn wir also einen Linearcode C mit Generatormatrix G und Kontrollmatrix H gegeben haben, können wir den Encoder und den Decoder von C sehr leicht mit Hilfe der Operationen von $\mathbb{F}_q$ beschreiben. Ein Nachrichtenwort wird in ein Codewort umgewandelt, indem wir die Generatormatrix darauf anwenden. Ob ein Empfangswort ein Codewort ist, können wir überprüfen, indem wir es mit H multiplizieren. Wenn das Ergebnis 0 ist, dann ist es ein Codewort, sonst nicht. Falls G systematisch ist, wird decodiert, indem die Prüfzeichen weggelassen werden.

Wie man die Struktur des Codes ausnützen kann, um entstandene Fehler zu korrigieren, soll hier nicht behandelt werden. Informationen darüber findet man zum Beispiel in [17].

1.4 Äquivalente Codes

Wir wollen später Konstruktionen für Codes angeben. Dabei treten Codes auf, die im wesentlichen gleichwertig sind. Um diese Gleichheit exakt zu formulieren definieren wir:

Definition 1.4.1 Gegeben seien zwei Linearcodes C_1, $C_2 \subseteq \mathbb{F}_q^n$. C_1 und C_2 heißen *äquivalent*, wenn ein Vektor $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q \backslash \{0\})^n$ existiert, sodass $C_2 = a \cdot C_1$ ist, das heißt, dass

$$C_2 = \{(a_1 c_1, \ldots, a_n c_n) \mid (c_1, \ldots, c_n) \in C_1\}$$

gilt.

Äquivalente Codes haben viele qualitative Eigenschaften gemeinsam. Genauer gilt der folgende Satz:

Satz 1.4.2 *C_1 und C_2 seien äquivalente Codes über $\mathbb{F}_q$ der Länge n. Dann haben C_1 und C_2 dieselbe Dimension und dieselbe Minimaldistanz.*

Beweis. Da C_1 und C_2 äquivalent sind, gibt es ein $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q \backslash \{0\})^n$ mit $C_2 = a \cdot C_1$. Die Aussage über die Dimension folgt aus der Tatsache, dass die Abbildung

$$\alpha : \left\{ \begin{array}{ccc} \mathbb{F}_q^n & \longrightarrow & \mathbb{F}_q^n \\ (v_1, \ldots, v_n) & \longmapsto & (a_1 v_1, \ldots, a_n v_n) \end{array} \right.$$

ein Isomorphismus ist. Da nach Definition der Äquivalenz $C_2 = \alpha(C_1)$ ist, gilt $\dim C_2 = \dim C_1$.
Die zweite Aussage folgt sofort aus

$$\mathrm{wt}(a_1 c_1, \ldots, a_n c_n) = \mathrm{wt}(c_1, \ldots, c_n)$$

und Satz 1.3.2. □

Man beachte aber, dass äquivalente Codes nicht in allen interessanten Eigenschaften eines Codes übereinstimmen müssen. Zum Beispiel können äquivalente Codes nicht-isomorphe Automorphismengruppen besitzen (für eine Definition der Automorphismengruppe eines Codes siehe [19]).

1.5 Die Gilbert-Varshamov-Schranke

Ziel der Codierungstheorie ist es „gute“ Codes oder „gute“ Klassen von Codes zu konstruieren. Die meisten Schranken für Codes sind obere Schranken, die angeben, dass die Parameter eines Codes sich innerhalb gewisser Schranken bewegen müssen. Die Gilbert-Varshamov-Schranke ist eine untere Schranke. Sie besagt, dass Codes mit Parametern, die größer als gewisse Werte sind, existieren. Wir werden Codes, deren Parameter diese Schranke erreichen, „gut“ nennen. Die Gilbert-Varshamov-Schranke stellt also sicher, dass „gute“ Codes existieren.

Die Herleitung der Gilbert-Varshamov-Schranke beruht (so wie die meisten anderen Schranken auch) darauf, die Anzahl der Wörter zu zählen, die zu einem festen Wort eine vorgegebene Entfernung haben.

Definition 1.5.1 Sei A ein Alphabet mit q Elementen. Der *q-äre Ball* $B_q(u,r)$ um $u \in A^n$ mit Radius $r \in \mathbb{N}$, besteht aus allen Wörtern $v \in A^n$ mit $d(u,v) \leq r$. Die Anzahl der Wörter in $B_q(u,r)$ bezeichnen wir mit $V(q,n,r)$.

Satz 1.5.2 *Sei A ein Alphabet mit q Elementen und sei $B_q(u,r)$ ein q-ärer Ball um $u \in A^n$ mit Radius $r \in \mathbb{N}$. Dann gilt für die Anzahl der Wörter in $B_q(u,r)$ die Formel*

$$V(q,n,r) = \binom{n}{0} + \binom{n}{1}(q-1) + \cdots + \binom{n}{r}(q-1)^r = \sum_{k=0}^{r} \binom{n}{k}(q-1)^k.$$

Beweis. Der Ball $B_q(u,r)$ ist die disjunkte Vereinigung der Mengen $\{v \in A^n \mid d(u,v) = k\}$ für $k = 0, \ldots, r$. Um ein Wort mit Distanz k zu finden, müssen wir zuerst k Plätze wählen an denen sich v von u unterscheiden soll. Dafür gibt es $\binom{n}{k}$ Möglichkeiten. An jeder Stelle gibt es $q-1$ mögliche Symbole, die verschieden von jenem von u an dieser Stelle sind. Insgesamt gibt es $(q-1)^k$ Möglichkeiten, wenn man die k Stellen gewählt hat. Daher gibt es $\binom{n}{k}(q-1)^k$ Wörter mit Distanz k von u. □

Als sehr einfache Anwendung dieses Satzes erhält man die folgenden oberen Schranken für die Anzahl der Codewörter bei gegebener Länge und Minimaldistanz.

Satz 1.5.3 (Hamming-Schranke) *Sei C ein Code über dem q-elementigen Alphabet A mit Blocklänge n und Minimaldistanz $d = 2r+1$. Dann hat C höchstens $q^n/V(q,n,r)$ Codewörter.*

Beweis. Die Bälle mit Radius r um verschiedene Codewörter müssen disjunkt sein. Daher gilt $|C| \cdot V(q,n,r) \leq |A^n| = q^n$ und damit sofort die

Behauptung. □

Satz 1.5.4 (Singleton-Schranke) *Für einen linearen $[n, k, d]$-Code C über $\mathbb{F}_q$ gilt*

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

Beweis. Wenn wir die ersten $d-1$ Symbole in jedem Codewort von C entfernen, haben wir nach wie vor q^k verschiedene Wörter, da die Minimaldistanz d ist. Die Blocklänge reduziert sich dabei auf $n-d+1$. Also gilt $k \leq n-d+1$ und damit die Behauptung. □

Definition 1.5.5 Einen Code, der die Hamming-Schranke erreicht, nennt man *perfekt*. Einen Code, der die Singleton-Schranke erreicht, heißt *MDS-Code* (*maximum distance separable*-Code).

Die Gilbert-Varshamov-Schranke erhält man, wenn man die Anzahl der Bälle zählt, die man benötigt um den ganzen A^n zu überdecken.

Satz 1.5.6 (Gilbert-Varshamov-Schranke) *Es gibt einen Code C über dem q-elementigen Alphabet A mit Länge n und Minimaldistanz d mit $|C| \geq q^n / V(q, n, d-1)$.*

Beweis. Sei $C \subseteq A^n$ ein Code mit Minimaldistanz d. Wir können annehmen das C maximal ist, in dem Sinn, dass kein Wort zu C hinzugefügt werden kann ohne die Minimaldistanz zu verkleinern, denn wenn C nicht maximal in diesem Sinne wäre, könnten wir ein Codewort hinzufügen (ohne die Minimaldistanz zu verkleinern), usw. Die Maximalität von C impliziert, dass jedes Wort in A^n eine Distanz $\leq d-1$ von einem Codewort hat. Die Bälle mit Radius $d-1$ um Codewörter überdecken also den A^n. Es gilt daher

$$q^n = |A|^n \leq |C| V(q, n, d-1).$$

Daraus folgt

$$|C| \geq q^n / V(q, n, d-1),$$

und damit die Behauptung. □

Die Gilbert-Varshamov-Schranke kann durch lineare Codes stets erreicht werden. Es gilt der folgende Satz:

Satz 1.5.7 *Sei C ein Linearcode mit Blocklänge n über $\mathbb{F}_q$ und Minimaldistanz $\geq d$. Falls $|C| < q^n / V(q, n, d-1)$, dann existiert ein Linearcode $C' \supsetneq C$ in $\mathbb{F}_q^n$, sodass die Minimaldistanz von C' ebenfalls $\geq d$ ist.*

Beweis. Aus dem Beweis von Satz 1.5.6 folgt, dass wir ein Wort $v \in \mathbb{F}_q^n$ wählen können, dessen Distanz zu jedem Codewort mindestens d ist. Wir definieren

$$C' := \{u - av \mid u \in C \text{ und } a \in \mathbb{F}_q\}.$$

Offensichtlich ist C' linear, denn für $a, a', b, b' \in \mathbb{F}_q$ und $u, u' \in C$ gilt

$$b(u - av) - b'(u' - a'v) = (bu - b'u') - (ba - b'a')v,$$

wobei $bu - b'u' \in C$ ist, da C linear ist, und $ba - b'a' \in \mathbb{F}_q$. C' enthält C (indem man $a = 0$ setzt). Um zu zeigen, dass C' immer noch Minimaldistanz $\geq d$ hat verwenden wir Satz 1.3.2. Sei $w = u - av$ ein Codewort ungleich dem Nullwort. Wenn $a = 0$ gilt, dann ist $w \in C$ und damit ist in diesem Fall $\mathrm{wt}(w) \geq d$. Wenn $a \neq 0$ ist, setzen wir $b = a^{-1}$. Dann gilt

$$\mathrm{wt}(w) = \mathrm{wt}(bw) = \mathrm{wt}(bu - v) = d(bu, v).$$

Da C linear ist, ist bu ein Codewort von C und v war so gewählt, dass die Distanz zu jedem Codewort $\geq d$ ist. Es ist also $d(bu, v) \geq d$. Satz 1.3.2 impliziert die Behauptung. □

Folgerung 1.5.8 *Es gibt einen Linearcode $C \subseteq \mathbb{F}_q^n$ mit Minimaldistanz d, Rang $\geq n - \log_q(V(q, n, d-1))$ und daher Rate $\geq 1 - \log_q(V(q, n, d-1))/n$.*

Beweis. Man wähle einen Code der die Gilbert-Varshamov-Schranke erreicht. So einer existiert nach Satz 1.5.7. Dieser hat mindestens $q^n/V(q, n, d-1)$ Codewörter. Deshalb ist der Rang k mindestens

$$\log_q(q^n/V(q, n, d-1)) = n - \log_q(V(q, n, d-1)).$$

Die Aussage über die Rate folgt jetzt sofort aus der Definition der Rate als Quotient k/n. □

Für kurze Blocklängen gibt es viele Codes, die die Gilbert-Varshamov-Schranke erreichen. Mit zunehmender Blocklänge wird es dann aber immer schwieriger die Gilbert-Varshamov-Schranke zu erreichen.

Um eine Schranke für Familien von Codes zu erhalten, müssen wir Codes mit verschiedenen Blocklängen vergleichen können. Der Rang wird dabei durch die Rate ersetzt und wir verwenden folgendes Maß für die Minimaldistanz, welches nicht mehr von der Länge abhängt.

Definition 1.5.9 Für einen Code der Länge n und Minimaldistanz d über $\mathbb{F}_q$ nennen wir d/n die *relative Minimaldistanz*.

Wir benötigen auch noch eine Schätzung für den zweiten Term in der Gilbert-Varshamov-Schranke, die nicht von n abhängt. Dazu eignet sich die folgende Funktion:

Definition 1.5.10 Sei $q \in \mathbb{N}$. Für $0 \leq \delta \leq (q-1)/q$ definieren wir die *q-äre Entropie Funktion* $H_q(\delta)$ durch $H_q(0) = 0$ und,

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

Satz 1.5.11 *Sei $q \in \mathbb{N}$. Für alle $0 \leq \delta \leq (q-1)/q$ gilt $H_q(\delta) \leq \delta q/(q-1)$. Gleichheit gilt dann und nur dann, wenn $\delta = 0$ oder $\delta = q-1)/q$.*

Beweis. Für $0 < \delta \leq (q-1)/q$, gilt für die Ableitung von $H_q(\delta)$

$$\log_q(q-1) - \log_q(\delta/(1-\delta)) \geq 0.$$

Die zweite Ableitung ist

$$1/((\delta-1)\delta\ln(q)) < 0.$$

Die Kurve definiert durch $y = H_q(\delta)$ ist also konkav auf $(0,(q-1)/q]$. Für $\delta = (q-1)/q$ ist $H_q(\delta) = 1$. Deshalb muß die Gerade durch die Punkte $(0,0)$ und $((q-1)/q, 1)$ überall echt oberhalb der Kurve sein. □

Mit Hilfe dieser Funktion können wir die Funktion $V(q,n,d-1)$ in der Gilbert-Varshamov-Schranke ersetzen.

Hilfssatz 1.5.12 *Sei $0 \leq \delta \leq (q-1)/q$ und für $n \in \mathbb{N}$ sei $r = r(n)$ als die größte Zahl $\in \mathbb{N}$ definiert, sodass $r \leq \delta n$ ist. Dann gilt*
(a) $\log_q(V(q,n,r)) \leq nH_q(\delta)$ *und*
(b) $n^{-1}\log_q(V(q,n,r)) \longrightarrow H_q(\delta)$ *für $n \longrightarrow \infty$.*

Beweis. (a) Man beachte, dass $0 \leq 1/q = 1-(q-1)/q \leq 1-\delta$ gilt. Daher ist für jedes reelle $k \geq 0$,

$$\delta^k \leq (q-1)^k/q^k \leq (q-1)^k(1-\delta)^k.$$

Für $0 \leq i \leq \delta n$ erhalten wir daher mit $k = \delta n - i$

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

Umformen und Multiplikation mit $(1-\delta)^n$ ergibt

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

Mit Hilfe des Binomischen Lehrsatzes erhalten wir

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

Wenn wir den Logarithmus zur Basis q anwenden, erhalten wir

$$0 \geq \log_q(V(q,n,r)) - n \cdot H_q(\delta),$$

was die erste Aussage beweist.

(b) Für den Beweis der zweiten Aussage benötigen wir die Stirling'sche Formel für $\ln(n!)$:

$$\ln(n!) - 1/(12n) \leq (n+1/2)\ln(n) - n + K \leq \ln(n!),$$

wobei $K = \ln(2\pi)/2$ und damit eine Konstante ist. Wenn wir zum Logarithmus zur Basis q übergehen ändert sich die Konstante und wir erhalten

$$\log_q(n!) - \log_q(e)/(12n) \leq (n+1/2)\log_q(n) - n\log_q(e) + K' \leq \log_q(n!).$$

Aus Satz 1.5.2 folgt

$$V(q,n,r) \geq \binom{n}{r} (q-1)^r.$$

Wir setzen nun $\binom{n}{r} = n!/(r!(n-r)!)$, logarithmieren zur Basis q und verwenden die Stirling'sche Formel um die Faktoren abzuschätzen. Damit erhalten wir

$$\begin{aligned} \log_q(V(q,n,r)) \quad \geq \quad & (n+1/2)\log_q(n) - (r+1/2)\log_q(r) \\ & -(n-r+1/2)\log_q(n-r) + r\log_q(q-1) \\ & -n\log_q(e) + r\log_q(e) + (n-r)\log_q(e) - K' \\ & -\log_q(e)/(12r) - \log_q(e)/(12(n-r)). \end{aligned}$$

Wenn wir durch n dividieren und n gegen ∞ gehen lassen, können wir Terme die gegen 0 gehen vernachlässigen. Wir erhalten

$$\begin{aligned} &\lim_{n\to\infty} (n^{-1}\log_q(V(q,n,r))) \\ &\quad \geq \lim_{n\to\infty} (\log_q(n) - (r/n)\log_q(r) \\ &\qquad -((n-r)/n)\log_q(n-r) + (r/n)\log_q(q-1)). \end{aligned}$$

Aus der Definition für r folgt, dass $\delta n/r$ und $(1-\delta)n/(n-r)$ beide für $n \to \infty$ gegen 1 konvergieren. Also gilt

$$\begin{aligned}
&\lim_{n\to\infty}(n^{-1}\log_q(V(q,n,r))) \\
&\quad \geq \lim_{n\to\infty}(\log_q(n) - \delta\log_q(\delta n) - (1-\delta)\log_q((1-\delta)n) + \delta\log_q(q-1)) \\
&\quad = \lim_{n\to\infty}(\log_q(n) - \delta\log_q(\delta) - \delta\log_q(n) \\
&\qquad\qquad -(1-\delta)\log_q(1-\delta) - (1-\delta)\log_q(n) + \delta\log_q(q-1)) \\
&\quad = \lim_{n\to\infty}(-\delta\log_q(\delta) - (1-\delta)\log_q(1-\delta) + \delta\log_q(q-1)) \\
&\quad = H_q(\delta).
\end{aligned}$$

Aus der ersten Aussage folgt nun die Behauptung. □

Satz 1.5.13 (Asymptotische Gilbert-Varshamov-Schranke) *Für alle $\delta \leq (q-1)/q$ gibt es eine Folge von Linearcodes $C_n \subseteq \mathbb{F}_q^n$, sodass die relative Minimaldistanz von C_n gegen δ und die Rate gegen $1-H_q(\delta)$ konvergiert.*

Beweis. Sei r die größte Zahl $\in \mathbb{N}$ mit $r \leq \delta n$. Aus Folgerung 1.5.8 erhalten wir, dass ein Linearcode $C_n \subseteq \mathbb{F}_q^n$ mit Minimaldistanz $r+1$ und Rate $k/n \geq 1 - n^{-1}\log_q(V(q,n,r))$ existiert. Aus Hilfssatz 1.5.12 folgt, dass die Raten von C_n gegen $1-H_q(\delta)$ konvergieren. Es gilt $\delta n < r+1 \leq \delta n + 1$. Daraus folgt $\delta < (r+1)/n \leq \delta + 1/n$. Also konvergiert $(r+1)/n$ gegen δ, wenn n gegen ∞ geht. □

Mit Hilfe dieses Satzes definieren wir jetzt „gute“ und „schlechte“ Familien von Codes.

Definition 1.5.14 Sei W eine Familie von Linearcodes über $\mathbb{F}_q$. Wir nennen W *schlecht*, wenn für jede unendliche Folge von Codes in W, entweder die Rate oder die relative Minimaldistanz gegen 0 konvergiert. Wir nennen W *gut*, wenn es eine unendliche Folge von Codes in W gibt, die gegen die asymptotische Gilbert-Varshamov-Schranke konvergieren, das heißt, es gibt ein $\delta \leq (q-1)/q$, sodass die relativen Minimaldistanzen gegen δ und die Raten gegen $1-H_q(\delta)$ konvergieren.

Man beachte, dass es Familien von Codes gibt, die weder gut noch schlecht sind. Unter guten Familien von Codes verstehen wir also solche, in denen es lange Codes mit vernünftigen Raten bei nicht zu großer relativer Minimaldistanz gibt.

Satz 1.5.13 garantiert uns zwar, dass gute Familien von Codes existieren, leider ist der Beweis nicht konstruktiv. Er zeigt uns nicht, wie wir gute Familien von Codes konstruieren können. Die erste Frage, die sich stellt ist,

ob die Codes die am bekanntesten sind und die in den Anwendungen am häufigsten verwendet werden, gut oder schlecht oder keines von beiden sind? Dieser Frage soll im nächsten Kapitel kurz nachgegangen werden.

1.6 BCH-Codes

Die folgende wichtige Klasse von Codes wurde von R. C. Bose und D. K. Ray-Chaudhuri und unabhängig zur selben Zeit von A. Hocquenghem entdeckt (siehe [2] und [9]). Sie sind bekannt unter dem Namen BCH-Codes.

Definition 1.6.1 Sei $n|q^m-1$ und $\beta \in \mathbb{F}_{q^m}$ eine primitive n-te Einheitswurzel. Sei weiters $l \in \mathbb{Z}$ und $\delta \geq 2$. Wir definieren den Code $C(n,l,\delta)$ über $\mathbb{F}_{q^m}$ durch die Generatormatrix

$$H := \begin{pmatrix} 1 & \beta^l & \beta^{2l} & \dots & \beta^{(n-1)l} \\ 1 & \beta^{l+1} & \beta^{2(l+1)} & \dots & \beta^{(n-1)(l+1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{l+\delta-2} & \beta^{2(l+\delta-2)} & \dots & \beta^{(n-1)(l+\delta-2)} \end{pmatrix}. \tag{1.1}$$

Der Code $C := C(n,l,\delta)^\perp \cap \mathbb{F}_q^n$ wird ein *BCH-Code* mit *konstruierter Minimaldistanz* δ genannt. Mit anderen Worten,

$$C = \{c \in \mathbb{F}_q^n \mid H \cdot c^T = 0\},$$

wobei H die Generatormatrix von $C(n,l,\delta)$ ist.

Normalerweise definiert man BCH-Codes als spezielle zyklische Codes (siehe zum Beispiel [23]). Ihre Bedeutung liegt vor allem, in der für diese Codes einfachen und effizienten Fehlerkorrektur (siehe dazu [17]).

Für die Dimension k eines BCH-Codes C gilt offensichtlich:

$$k \geq n - m(\delta - 1).$$

Wir nennen $n-m(\delta-1)$ die *konstruierte Dimension* des BCH-Codes C. Der folgende Satz behauptet, dass eine untere Schranke für die Minimaldistanz durch δ gegeben ist.

Satz 1.6.2 *Sei C ein BCH-Code mit konstruierter Minimaldistanz δ. Dann gilt: $d \geq \delta$.*

Beweis. Der Beweis soll hier nicht geführt werden, da er aus einem allgemeineren Satz (siehe Folgerung 3.3.6) im Kapitel 4 folgt. Einen elementaren

Beweis findet man z.B. in [23]. □

Es gilt der folgende Satz:

Satz 1.6.3 *Sei C_k eine Folge von BCH-Codes über $\mathbb{F}_2$ der Länge $n = 2^k - 1$ mit konstruierter Minimaldistanz $\delta = 2t + 1 > \epsilon \cdot n$, wobei $\epsilon > 0$ ist. Dann folgt, dass die konstruierte Rate (=konstruierte Dimension/n) bei genügend großem n unter 0 fällt.*

Beweis. Die konstruierte relative Minimaldistanz ist $(2t+1)/n$. Wenn diese $> \epsilon$ sein soll, muß $t > (\epsilon n - 1)/2$ gelten. Da $k = \log_2(n+1)$ ist, folgt, dass die konstruierte Dimension $n - 2kt < n - (\epsilon n - 1)\log_2(n+1)$ sein muß. Wenn n genügend groß ist, gilt $\log_2(n+1) > 2/\epsilon$ und damit

$$\begin{aligned} n - (\epsilon n - 1)\log_2(n+1) &= n - \epsilon n \log_2(n+1) + \log_2(n+1) \\ &< n - 2n + \log_2(n+1) \\ &= \log_2(n+1) - n < 0. \end{aligned}$$

Damit fällt auch die konstruierte Rate unter 0. Es gilt also: Wenn die konstruierte Rate über 0 bleibt, kann die relative Minimaldistanz nicht größer als ϵ sein für großes n. □

Dieser Satz besagt zwar nur, dass diese spezielle Klasse von BCH-Codes entweder schlecht ist oder die Abschätzungen für Rang und Minimaldistanz schlecht sind. Man kann aber zeigen, dass die BCH-Codes insgesamt eine schlechte Familie von Codes bilden.

Satz 1.6.4 *Die BCH-Codes bilden eine schlechte Familie von Codes.*

Beweis. Einen Beweis findet man in [11] und soll hier entfallen. □

Die Frage, nach guten Familien von Codes bleibt zunächst noch offen. Der russische Mathematiker V. D. Goppa entdeckte 1970 eine Klasse von Codes (siehe [6]), welche die BCH-Codes als Spezialfall beinhalten. Von dieser Klasse konnte er zeigen, dass es sich um eine gute Klasse von Codes handelt. Allerdings konnte er keine explizite Konstruktion angeben. Im Jahr 1980 hat Goppa seine Definition nochmals erweitert (siehe [7]), indem er Kurven über endlichen Körpern betrachtete. In dieser Klasse von „geometrischen“ Codes, gibt es explizite Codes, die die Gilbert-Varshamov-Schranke sogar übertreffen.

Diese Codes werden im folgenden betrachtet. Das nächste Kapitel wird die dafür notwendige Sprache bereitstellen.

Kapitel 2

Algebraische Funktionenkörper

In diesem Kapitel sollen die grundlegenden Definitionen und Resultate der Theorie der algebraischen Funktionenkörper entwickelt werden. Wir setzen stets voraus:

Es sei K ein beliebiger Körper.

Ein algebraischer Funktionenkörper über K ist eine endliche und somit algebraische Erweiterung des rationalen Funktionenkörpers $K(x)$. Solche Typen von Körpererweiterungen treten in vielen verschiedenen Bereichen der Mathematik auf, wie zum Beispiel in der algebraischen Geometrie, in der Zahlentheorie und in der Theorie der kompakten Riemann'schen Flächen.

Wir wollen hier einen rein algebraischen Zugang zur Theorie der algebraischen Funktionenkörper geben. Diese Formulierung stammt ursprünglich hauptsächlich von Chevalley (1951, siehe [3]), wurde aufgenommen und weiterentwickelt von Roquette (1958) und seinen Schülern Deuring und Stichtenoth (siehe [4] und [19]). Der Vorteil dieses Zuganges ist, dass er sehr elementar ist, und dass man die wichtigen Sätze relativ schnell für beliebigen Körper K zeigen kann.

2.1 Funktionenkörper und Stellen

Definition 2.1.1 Ein Erweiterungkörper $F \supseteq K$ (wir schreiben auch F/K dafür) heißt ein *algebraischer Funktionenkörper in einer Variable über K* (oder kurz *Funktionenkörper*), falls es eine Element $x \in F$ gibt, welches transzendent über K ist, sodass F eine endliche und somit algebraische Erweiterung von $K(x)$ ist.

Im Spezialfall, dass $F = K(x)$ ist, für ein $x \in F$, welches transzendent über K ist, nennen wir F/K den *rationalen Funktionenkörper.*

Die Menge $\bar{K} := \{z \in F \mid z \text{ ist algebraisch über } K\}$ ist ein Unterkörper von F, da Summen, Produkte und Inverse algebraischer Elemente algebraisch sind. $\bar{K}$ wird *Konstantenkörper* von F/K genannt. Es gilt $K \subseteq \bar{K} \subset F$ und klarerweise ist $F/\bar{K}$ ein Funktionenkörper über $\bar{K}$. Wir nennen K *algebraisch abgeschlossen in* F (oder sagen K ist der *volle Konstantenkörper von* F), falls $\bar{K} = K$ ist. Außerdem nennen wir $\kappa = [\bar{K} : K]$ den *Konstantengrad* von F/K.

Der erste Satz zeigt uns, dass das Element x in der Definition des Funktionenkörpers keine besondere Rolle spielt. Wir können die transzendenten Elemente von F über K nämlich folgendermaßen charakterisieren:

Satz 2.1.2 *Sei F/K ein Funktionenkörper mit Konstantenkörper $\bar{K}$. Dann gilt:*

$$[F : K(y)] < \infty \iff y \in F \backslash \bar{K}.$$

Beweis.
$\Leftarrow$: Da $[F : K(x)] < \infty$ ist, sind die Potenzen von y nicht linear unabhängig über $K(x)$. Also ist y Nullstelle eines Polynomes $f(T) \in K(x)[T]$. Wenn wir mit dem gemeinsamen Nenner multiplizieren, können wir annehmen, dass die Koeffizienten von f Polynome in x sind. Wir können f also auffassen als $f(S,T) \in K[S,T]$, sodass $f(x,y) = 0$ gilt. Angenommen S kommt in $f(S,T)$ nicht vor, dann wäre y algebraisch über K und würde daher in $\bar{K}$ liegen. Widerspruch! Daher ist x algebraisch über $K(y)$ und daher gilt $[K(x,y) : K(y)] \leq \deg_{K(y)} f(S,y) < \infty$. Andererseits ist $[F : K(x,y)] \leq [F : K(x)]$. Insgesamt erhalten wir $[F : K(y)] = [F : K(x,y)] \cdot [K(x,y) : K(y)] < \infty$.
$\Rightarrow$: Nehmen wir indirekt an, dass $[F : K(y)] < \infty$ mit $y \in \bar{K}$ gilt. Klarerweise ist $[K(y) : K] < \infty$. Damit erhalten wir $[F : K] = [F : K(y)] \cdot [K(y) : K] < \infty$. Also ist F eine endliche und damit algebraische Erweiterung von K. Widerspruch zu F/K ein Funktionenkörper! □

Als nächstes wollen wir Bewertungsringe und Stellen definieren.

Definition 2.1.3 Ein *Bewertungsring* eines Funktionenkörpers F/K ist ein Unterring $\mathcal{O} \subseteq F$ mit den folgenden Eigenschaften:
(1) $K \subsetneq \mathcal{O} \subsetneq F$, und
(2) für jedes $z \in F$ gilt: $z \in \mathcal{O}$ oder $z^{-1} \in \mathcal{O}$.

Der folgende Satz liefert erste wichtige Einblicke in die Struktur von Bewertungsringen.

Satz 2.1.4 *Sei $\mathcal{O}$ ein Bewertungsring eines Funktionenkörpers F/K. Dann gilt:*
(a) *$\mathcal{O}$ ist ein lokaler Ring, das heißt $\mathcal{O}$ besitzt ein eindeutiges maximales Ideal $P = \mathcal{O}\backslash\mathcal{O}^*$, wobei $\mathcal{O}^* = \{z \in \mathcal{O} \mid \exists w \in \mathcal{O} \text{ mit } zw = 1\}$ die Gruppe der Einheiten von $\mathcal{O}$ bezeichnet.*
(b) *Für $0 \neq x \in F$ gilt: $x \in P \iff x^{-1} \notin \mathcal{O}$.*
(c) *Für den Konstantenkörper $\bar{K}$ von F/K gilt $\bar{K} \subseteq \mathcal{O}$ und $\bar{K} \cap P = \{0\}$.*

Beweis. (a) Wir brauchen nur zu zeigen, dass $P := \mathcal{O}\backslash\mathcal{O}^*$ ein Ideal ist. Daraus folgt nämlich sofort, dass es das eindeutige maximale Ideal sein muss, da ein echtes Ideal von $\mathcal{O}$ keine Einheit enthalten kann.
(1) Sei also $x \in P$, $z \in \mathcal{O}$. Dann ist $xz \notin \mathcal{O}^*$ (sonst wäre x eine Einheit), also gilt $xz \in P$.
(2) Seien $x, y \in P$. O.B.d.A. können wir annehmen, dass $x/y \in \mathcal{O}$ gilt. Dann ist $1 + x/y \in \mathcal{O}$ und damit $x + y = y(1 + x/y) \in P$ wegen (1). Also ist P ein Ideal von $\mathcal{O}$.
(b) Offensichtlich.
(c) Sei $z \in \bar{K}$. Angenommen $z \notin \mathcal{O}$. Dann ist $z^{-1} \in \mathcal{O}$, da $\mathcal{O}$ ein Bewertungsring ist. Da z^{-1} algebraisch über K ist, existieren Elemente $a_1, \ldots, a_r \in K$ mit $a_r(z^{-1})^r + \cdots + a_1 z^{-1} + 1 = 0$, also gilt $z^{-1}(a_r(z^{-1})^{r-1} + \cdots + a_1) = -1$. Daraus folgt $z = -(a_r(z^{-1})^{r-1} + \cdots + a_1) \in K[z^{-1}] \subseteq \mathcal{O}$, und damit $z \in \mathcal{O}$. Dass $\bar{K} \cap P = \{0\}$ gilt, folgt aus dem eben bewiesenen, denn es gilt $0 \neq z \in \bar{K} \cap P \Rightarrow z^{-1} \notin \mathcal{O} \Rightarrow z^{-1} \notin \bar{K}$. Dies widerspricht der Tatsache, dass $\bar{K}$ ein Körper ist. □

Zur Untersuchung der Eigenschaften des eindeutigen maximalen Ideals P benötigen wir den folgenden Hilfssatz:

Hilfssatz 2.1.5 *Sei $\mathcal{O}$ ein Bewertungsring eines Funktionenkörpers F/K, P das maximale Ideal und $0 \neq x \in P$. Seien $x_1, \ldots, x_n \in P$, sodass $x_1 = x$ und $x_i \in x_{i+1}P$ für $i = 1, \ldots, n-1$. Dann gilt: $n \leq [F : K(x)] < \infty$.*

Beweis. Aus den Sätzen 2.1.2 und 2.1.4 folgt, dass $[F : K(x)] < \infty$ ist. Es genügt also zu zeigen, dass $x_1, \ldots, x_n$ linear unabhängig über $K(x)$ sind. Zunächst gilt, aufgrund der Definition, dass alle $x_i \neq 0$ sind. Angenommen es gibt eine nicht triviale Linearkombination $\sum_{i=1}^{n} \varphi_i x_i = 0$ mit $\varphi_i \in K(x)$. Wir können annehmen, dass alle φ_i Polynome in x sind, und dass x nicht alle von ihnen teilt. Wir setzen $a_i := \varphi_i(0)$ und definieren $j \in \{1, \ldots, n\}$ durch die Bedingung $a_j \neq 0$, aber $a_i = 0$ für alle $i > j$. Wir erhalten

$$-\varphi_j x_j = \sum_{i \neq j} \varphi_i x_i \tag{2.1}$$

mit $\varphi_i \in \mathcal{O}$ für $i = 1, \ldots, n$ (da $x = x_1 \in P$), $x_i \in x_j P$ für $i < j$ und

$\varphi_i = xg_i$ für $i > j$, wobei g_i Polynome in x sind. Wenn wir (2.1) durch x_j dividieren, erhalten wir

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

Alle Summanden auf der rechten Seite gehören zu P, daher folgt $\varphi_j \in P$. Andererseits gilt $\varphi_j = a_j + xg_j$ mit $g_j \in K[x] \subseteq \mathcal{O}$ und $x \in P$, sodass $a_j = \varphi_j - xg_j \in P \cap K$ gilt. Da $a_j \neq 0$ gilt, ist das ein Widerspruch zu Satz 2.1.4 (c). □

Satz 2.1.6 *Sei $\mathcal{O}$ ein Bewertungsring eines Funktionenkörpers F/K und P das eindeutige maximale Ideal. Dann gilt:*
(a) *P ist ein Hauptideal.*
(b) *Falls $P = t\mathcal{O}$, dann hat jedes $0 \neq z \in F$ 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. Genauer, wenn $P = t\mathcal{O}$ und $\{0\} \neq I \subseteq \mathcal{O}$ ein Ideal ist, dann ist $I = t^n\mathcal{O}$ für ein $n \in \mathbb{N}$.*

Beweis. (a) Nehmen wir indirekt an, dass P kein Hauptideal wäre und wählen wir ein Element $0 \neq x_1 \in P$. Da $P \neq x_1\mathcal{O}$ ist, gibt es ein $x_2 \in P \backslash x_1\mathcal{O}$. Da $x_2 x_1^{-1} \notin \mathcal{O}$ ist, folgt aus Satz 2.1.4 (b) $x_2^{-1} x_1 \in P$, und daher gilt $x_1 \in x_2 P$. Durch Induktion erhält man eine Folge $x_1, x_2, x_3, \ldots$ aus P, sodass $x_i \in x_{i+1}P$ für jedes $i \geq 1$ gilt, was ein Widerspruch zu Hilfssatz 2.1.5 ist.
(b) Die Eindeutigkeit der Darstellung $z = t^n u$ mit $u \in \mathcal{O}^*$ und $n \in \mathbb{Z}$ ist trivial, sodass wir nur die Existenz einer solchen zeigen müssen. Da z oder z^{-1} in $\mathcal{O}$ liegt, können wir annehmen, dass $z \in \mathcal{O}$ gilt. Falls $z \in \mathcal{O}^*$, dann ist $z = t^0 z$. Es bleibt also der Fall $z \in P$. In diesem Fall gibt es ein maximales $m \geq 1$ mit $z \in t^m\mathcal{O}$, da die Länge der Sequenz

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

wegen Hilfssatz 2.1.5 beschränkt sein muß. Wir erhalten also $z = t^m u$ mit $u \in \mathcal{O}$. Angenommen u wäre keine Einheit von $\mathcal{O}$, dann würde $u \in P = t\mathcal{O}$ gelten, also $u = tw$ mit $w \in \mathcal{O}$ und daher $z = t^{m+1}w \in t^{m+1}\mathcal{O}$, was ein Widerspruch zur Maximalität von m ist. Daher ist $u \in \mathcal{O}^*$.
(c) Sei $\{0\} \neq I \subseteq \mathcal{O}$ ein Ideal. Die Menge $A := \{r \in \mathbb{N} \mid t^r \in I\}$ ist nicht leer, da für $0 \neq x \in I$ gilt: $x = t^r u$ mit $u \in \mathcal{O}^*$ und daher $t^r = xu^{-1} \in I$. Wir setzen $n := \min(A)$ und behaupten, dass $I = t^n\mathcal{O}$ gilt. Die Inklusion $I \supseteq t^n\mathcal{O}$ ist trivial, da $t^n \in I$ ist. Umgekehrt sei $y \in I$ und sei $y \neq 0$. Dann ist $y = t^s w$ mit $w \in \mathcal{O}^*$ und $s \geq 0$, woraus $t^s \in I$ und damit $s \geq n$ folgt. Daher gilt $y = t^n \cdot t^{s-n} w \in t^n\mathcal{O}$. □

Einen Ring mit den Eigenschaften des letzten Satzes nennt man auch einen *diskreten Bewertungsring.*

Definition 2.1.7
(a) Eine *Stelle* P eines Funktionenkörpers F/K ist das maximale Ideal eines Bewertungsringes $\mathcal{O}$ von F/K. Jedes Element $t \in P$, sodass $P = t\mathcal{O}$ gilt, wird ein *Primelement* von P (oder *lokaler Parameter* oder *Uniformisierungsvariable*) genannt.
(b) $\mathbb{P}_F := \{P \mid P \text{ ist eine Stelle von } F/K\}$.

Wenn $\mathcal{O}$ ein Bewertungsring von F/K und P sein maximales Ideal ist, dann wird $\mathcal{O}$ durch P eindeutig bestimmt, es gilt nämlich nach Satz 2.1.4 (b), dass $\mathcal{O} = \{z \in F\backslash\{0\} \mid z^{-1} \notin P\} \cup \{0\}$ ist. Deshalb nennen wir $\mathcal{O}_P := \mathcal{O}$ den *Bewertungsring der Stelle* P.

Sei jetzt P eine Stelle von F/K und $\mathcal{O}_P$ sein Bewertungsring. Da P ein maximales Ideal ist, ist der Restklassenring $\mathcal{O}_P/P$ ein Körper. Für $x \in \mathcal{O}_P$ definieren wir $x(P) \in \mathcal{O}_P/P$ als die Restklasse von x modulo P, für $x \in F\backslash\mathcal{O}_P$ setzen wir $x(P) := \infty$. Aus Satz 2.1.4 wissen wir, dass $K \subseteq \mathcal{O}_P$ und $K \cap P = \{0\}$, deshalb induziert die Restklassenabbildung $\mathcal{O}_P \longrightarrow \mathcal{O}_P/P$ eine kanonische Einbettung von K in $\mathcal{O}_P/P$. Über diese Einbettung wollen wir im folgenden K stets als einen Unterkörper von $\mathcal{O}_P/P$ auffassen. Man beachte, dass diese Beobachtung auch auf $\bar{K}$ anstatt K angewandt werden kann. Wir fassen also auch $\bar{K}$ als Unterkörper von $\mathcal{O}_P/P$ auf.

Definition 2.1.8 Sei $P \in \mathbb{P}_F$.
(a) $F_P := \mathcal{O}_P/P$ ist der *Restklassenkörper* von P. Die Abbildung

$$\begin{array}{ccc} F & \longrightarrow & F_P \cup \{\infty\} \\ x & \longmapsto & x(P) \end{array}$$

nennt man die *Restklassenabbildung* in Bezug auf P. Manchmal verwenden wir die Notation $x + P := x(P)$ für $x \in \mathcal{O}_P$.
(b) $\deg P := [F_P : K]$ nennen wir den *Grad* von P.

Der Grad einer Stelle ist stets endlich. Genauer gilt der folgende Satz:

Satz 2.1.9 *Sei P eine Stelle von F/K und $0 \neq x \in P$, dann gilt:*

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

Beweis. Zunächst bemerken wir, dass aus Satz 2.1.2 folgt, dass $[F : K(x)] < \infty$ ist. Seien $z_1, \ldots, z_n \in \mathcal{O}_P$, sodaß die Restklassen $z_1(P), \ldots, z_n(P) \in F_P$ linear unabhängig über K sind. Es genügt zu zeigen, dass die Elemente linear unabhängig über $K(x)$ sein müssen. Angenommen es gibt eine nicht triviale

Linearkombination

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

mit $\varphi_i \in K(x)$. O.B.d.A. können wir annehmen, dass die φ_i Polynome in x sind und dass nicht alle davon von x geteilt werden, das heißt $\varphi_i = a_i + xg_i$ mit $a_i \in K$, $g_i \in K[x]$, nicht alle $a_i = 0$. Wegen $x \in P$ und $g_i \in \mathcal{O}_P$ gilt $\varphi_i(P) = a_i(P) = a_i$. Wenn wir die Restklassenabbildung auf (2.2) anwenden erhalten wir

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

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

Definition 2.1.10 Eine Stelle P eines Funktionenkörpers F/K heißt *rational*, wenn $\deg P = 1$ ist, das heißt wenn $F_P = K$ ist.

Aus dieser Definition erhalten wir die nachstehende Folgerung. Sie ist ein einfaches Kriterium für den Grundkörper K eines Funktionenkörpers, um zu entscheiden, ob er der volle Konstantenkörper $\bar{K}$ ist.

Folgerung 2.1.11 *Wenn der Funktionenkörper F/K eine rationale Stelle besitzt, dann ist $\bar{K} = K$ und daher ist der Konstantengrad $\kappa = 1$.*

Beweis. Sei $P \in \mathbb{P}_F$ die rationale Stelle. Aus Satz 2.1.4 (c) folgt dann, $\bar{K} \subseteq \mathcal{O}_P \backslash P$. Daher folgt $\bar{K} \subseteq \mathcal{O}_P / P = K$, und damit $\bar{K} = K$. □

Als nächstes wollen wir die Existenz von Stellen in einem Funktionenkörper beweisen. Wir werden sogar sehen, dass ein Funktionenkörper sehr viele Stellen besitzt.

Satz 2.1.12 *Sei F/K ein Funktionenkörper und R ein Unterring von F mit $K \subseteq R \subseteq F$. Angenommen $\{0\} \neq I \subsetneq R$ ist ein echtes Ideal von R. Dann gibt es eine Stelle $P \in \mathbb{P}_F$, sodass $I \subseteq P$ und $R \subseteq \mathcal{O}_P$ ist.*

Beweis. Wir betrachten die Menge

$$\mathcal{F} := \{S \mid S \text{ ist ein Untering von } F \text{ mit } R \subseteq S \text{ und } IS \neq S\},$$

wobei IS das Idealprodukt (die Menge aller endlichen Summen von Produkten as mit $a \in I$ und $s \in S$) bezeichnet. $\mathcal{F}$ ist nicht leer, da $R \in \mathcal{F}$ ist, und $\mathcal{F}$ ist mit der Inklusion induktiv geordnet. Sei nämlich $\mathcal{H} \subseteq \mathcal{F}$ eine total geordnete Teilmenge von $\mathcal{F}$, dann ist $T := \bigcup\{S \mid S \in \mathcal{H}\}$ ein Unterring von F mit $R \subseteq T$. Wir müssen zeigen, dass $IT \neq T$ ist. Angenommen das wäre

falsch, dann ist $1 = \sum_{\nu=1}^{n} a_\nu s_\nu$ mit $a_\nu \in I$, $s_\nu \in T$. Da $\mathcal{H}$ total geordnet ist, gibt es ein $S_0 \in \mathcal{H}$, sodass $s_1, \ldots, s_n \in S_0$ ist. Also gilt $1 = \sum_{\nu=1}^{n} a_\nu s_\nu \in IS_0$, womit ein Widerspruch erzielt wurde.
Mit Hilfe des Zornschen Lemmas folgt, dass $\mathcal{F}$ ein maximales Element besitzt, also gibt es einen Ring $\mathcal{O} \subseteq F$, sodass $R \subseteq \mathcal{O} \subseteq F$, $I\mathcal{O} \neq \mathcal{O}$ und $\mathcal{O}$ ist maximal mit diesen Eigenschaften. Wir wollen zeigen, dass $\mathcal{O}$ einen Bewertungsring von F/K bildet.
Aus $I \neq \{0\}$ und $I\mathcal{O} \neq \mathcal{O}$ folgt $\mathcal{O} \subsetneq F$ und $I \subseteq \mathcal{O}\backslash\mathcal{O}^*$. Außerdem ist $\mathcal{O} \supsetneq K$, denn angenommen $\mathcal{O}$ sei gleich K, dann wäre $K = R$ und damit würde kein echtes Ideal I existieren. Widerspruch! 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 $\mathcal{O}$ – $I\mathcal{O}[z] = \mathcal{O}[z]$ und $I\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$ und wir können $a_0, \ldots, a_n, b_0, \ldots, b_m \in I\mathcal{O}$ finden mit

$$1 = a_0 + a_1 z + \cdots + a_n z^n \quad \text{und} \tag{2.3}$$
$$1 = b_0 + b_1 z^{-1} + \cdots + b_m z^{-m}. \tag{2.4}$$

Klarerweise ist $n \geq 1$ und $m \geq 1$. Wir können annehmen, dass m,n in (2.3) und (2.4) minimal gewählt sind und $m \leq n$ gilt. Wenn wir (2.3) mit $1 - b_0$ und (2.4) mit $a_n z^n$ multiplizieren, erhalten wir

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

Wenn wir diese Gleichungen addieren, erhalten wir $1 = c_0 + c_1 z + \cdots + c_{n-1} z^{n-1}$ mit Koeffizienten $c_i \in I\mathcal{O}$. Das ist ein Widerspruch zur Minimalität von n in (2.3). Wir haben also gezeigt, dass $z \in \mathcal{O}$ oder $z^{-1} \in \mathcal{O}$ für jedes $z \in F$ gilt, also dass $\mathcal{O}$ ein Bewertungsring von F/K ist. □

Folgerung 2.1.13 *Sei F/K ein Funktionenkörper, $z \in F$ transzendent über K. Dann gilt:*
(a) *$z \in \mathcal{O}_P$ für eine Stelle P.*
(b) *Es gibt unendlich viele Stellen in F.*
Insbesondere gilt also $\mathbb{P}_F \neq \emptyset$.

Beweis. (a) Wende Satz 2.1.12 auf $R = K[z]$ und $I = zK[z]$ an.
(b) Wir zeigen zunächst: Seien R und I wie in Satz 2.1.12. Ist I ein Primideal, dann kann ein P mit $P \cap R = I$ gefunden werden.
Wir erweitern R und definieren B als den Ring $\{a/b \,|\, a \in R, b \in R\backslash I\}$. Dann ist $IB = \{a/b \,|\, a \in I, b \in R\backslash I\}$ ein Ideal von B. Da genau die Elemente, die nicht in IB liegen, ein inverses Element besitzen, ist IB das eindeutige maximale Ideal von B. Nach Konstruktion folgt $I \subseteq IB \cap R$ und $(R\backslash I) \cap IB = \emptyset$. Also $IB \cap R = I$. Wenn wir Satz 2.1.12 auf B anwenden, finden wir eine Stelle P mit $IB \subseteq P$. $P \cap B$ ist ein echtes Ideal von B, da

es die 1 nicht enthält, also gilt $P \cap B \subseteq IB$. Daraus folgt $P \cap B = IB$ und damit $P \cap R = IB \cap R = I$.
Die Behauptung ergibt sich jetzt folgendermaßen: In $K[z]$ gibt es unendlich viele verschiedene nicht assoziierte Primelemente p und jedes dieser Polynome erzeugt ein anderes Primideal $\langle p \rangle$. Zu jedem dieser Ideale gibt es eine andere Stelle P, sodass $P \cap K[z] = \langle p \rangle$ ist. □

Folgerung 2.1.14 *Der Konstantenkörper $\bar{K}$ von F/K ist eine endliche Erweiterung von K.*

Beweis. Wir wählen eine Stelle $P \in \mathbb{P}_F$. Da $\bar{K}$ in F_P eingebettet ist, folgt dass $[\bar{K} : K] \leq [F_P : K] = \deg P < \infty$ ist. □

Wenn P eine rationale Stelle des Funktionenkörper F/K ist, dann gilt $F_P = K$, und die Restklassenabbildung bildet F auf $K \cup \{\infty\}$ ab. Wenn wir voraussetzen K sei algebraisch abgeschlossen, dann ist jede Stelle rational. Deshalb können wir in diesem Fall ein Element $z \in F$ als Funktion

$$z : \begin{cases} \mathbb{P}_F & \longrightarrow & K \cup \{\infty\}, \\ P & \longmapsto & z(P) \end{cases} \tag{2.5}$$

auffassen. Aus diesem Grund heißt F/K ein *Funktionenkörper*. Interpretiert man die Elemente von K als Funktionen, so sind sie konstante Funktionen. Aus diesem Grund nennt man K den *Konstantenkörper* von F.

2.2 Bewertungen

Wir wollen noch eine andere nützliche Beschreibung von Stellen geben. Dazu definieren wir:

Definition 2.2.1 Eine *diskrete Bewertung* von F/K ist eine Funktion $\nu : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ mit den folgenden Eigenschaften:
(1) $\nu(x) = \infty \iff x = 0$.
(2) $\nu(xy) = \nu(x) + \nu(y)$ für alle $x, y \in F$.
(3) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ für alle $x, y \in F$.
(4) Es gibt ein Element $z \in F$ mit $\nu(z) = 1$.
(5) $\nu(a) = 0$ für alle $a \in K \backslash \{0\}$.

Das Symbol ∞ bezeichnet hier ein Element $\notin \mathbb{Z}$, sodass $\infty + \infty = \infty + n = n + \infty = \infty$ und $\infty > m$ für alle $m, n \in \mathbb{Z}$. Aus (2) und (4) folgt sofort, dass $\nu : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ surjektiv ist. Eigenschaft (3) wird Dreiecksungleichung genannt. Eine stärkere Version dieser Ungleichung liefert der folgende Hilfssatz:

Hilfssatz 2.2.2 (Strikte Dreiecksungleichung) *Sei ν eine diskrete Bewertung von F/K und $x, y \in F$ mit $\nu(x) \neq \nu(y)$. Dann gilt: $\nu(x+y) = \min\{\nu(x), \nu(y)\}$.*

Beweis. Aus (2) und (5) folgt, dass $\nu(ay) = \nu(y)$ für $0 \neq a \in K$. Speziell erhalten wir $\nu(-y) = \nu(y)$. Nach Voraussetzung ist $\nu(x) \neq \nu(y)$, also können wir o.B.d.A. $\nu(x) < \nu(y)$ annehmen. Falls $\nu(x+y) \neq \min\{\nu(x), \nu(y)\}$ ist, dann folgt $\nu(x+y) > \nu(x)$ aus (3) und wir erhalten $\nu(x) = \nu((x+y)-y) \geq \min\{\nu(x+y), \nu(y)\} > \nu(x)$, Widerspruch! □

Definition 2.2.3 Wir ordnen jeder Stelle $P \in \mathbb{P}_F$ eine Funktion $\nu_P : F \longrightarrow \mathbb{Z} \cup \{\infty\}$ auf folgende Art und Weise zu: Sei t ein Primelement für P. Dann hat jedes $0 \neq z \in F$ eine eindeutige Darstellung $z = t^n u$ mit $u \in \mathcal{O}_P^*$ und $n \in \mathbb{Z}$. Wir definieren $\nu_P(z) := n$ und $\nu_P(0) := \infty$.

Diese Funktion ν_P wird sich als diskrete Bewertung von F/K herausstellen. Man beachte, dass diese Definition nur von P, nicht aber von der Wahl von t abhängt. Sei nämlich t' ein anderes Primelement für P, dann gilt $P = t\mathcal{O} = t'\mathcal{O}$, sodass $t = t'w$ ist für ein $w \in \mathcal{O}_P^*$. Daraus folgt $t^n u = (t'^n w^n)u = t'^n(w^n u)$ mit $w^n u \in \mathcal{O}_P^*$.

Der folgende Satz liefert die Beziehung zwischen P, $\mathcal{O}_P$ und ν_P:

Satz 2.2.4 *Sei F/K ein Funktionenkörper.*
(a) *Für jede Stelle $P \in \mathbb{P}_F$ ist die Funktion ν_P eine diskrete Bewertung von F/K. Es gilt:*

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

Ein Element $x \in F$ ist ein Primelement von P, dann und nur dann, wenn $\nu_P(x) = 1$.
(b) *Umgekehrt gilt: Sei ν eine diskrete Bewertung von F/K. Dann ist die Menge $P := \{z \in F \mid \nu(z) > 0\}$ eine Stelle von F/K, und $\mathcal{O}_P = \{z \in F \mid \nu(z) \geq 0\}$ ist der dazugehörige Bewertungsring.*
(c) *Jeder Bewertungsring $\mathcal{O}$ von F/K bildet einen maximalen echten Unterring von F.*

Beweis. (a) Offensichtlich hat ν_P die Eigenschaften (1), (2), (4) und (5) in Definition 2.2.1. Um die Dreiecksungleichung (3) zu zeigen, nehmen wir Elemente $x, y \in F$ mit $\nu_P(x) = n$, $\nu_P(y) = m$. Wir können annehmen, dass $n \leq m < \infty$ ist. Wir haben $x = t^n u_1$ 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 $z \in \mathcal{O}_P$. Wenn $z = 0$ ist, dann gilt $\nu_P(x + y) = \infty > \min\{n, m\}$, sonst ist $z = t^k u$ mit $k \geq 0$ und $u \in \mathcal{O}_P^*$. Daher ist

$$\nu_P(x + y) = \nu_P(t^{n+k}u) = n + k \geq n = \min\{\nu_P(x), \nu_P(y)\}.$$

Wir haben also gezeigt, dass ν_P eine diskrete Bewertung von F/K ist. Die restlichen Aussagen von (a) sind trivial, genauso wie (b).
(c) Sei $\mathcal{O}$ ein Bewertungsring von F/K, P sein maximales Ideal, ν_P die diskrete Bewertung zu P und $z \in F \backslash \mathcal{O}$. Wir müssen zeigen, dass $F = \mathcal{O}[z]$ ist. Sei dazu $y \in F$ beliebig. Dann ist $\nu_P(yz^{-k}) \geq 0$ für hinreichend großes $k \geq 0$ (beachte $\nu_P(z^{-1}) > 0$, da $z \notin \mathcal{O}$). Daraus folgt $w := yz^{-k} \in \mathcal{O}$ und damit $y = wz^k \in \mathcal{O}[z]$. □

Dieser Satz besagt also, dass Stellen, Bewertungsringe und diskrete Bewertungen eines Funktionenkörpers im wesentlichen dasselbe Objekt beschreiben.

Die folgende Definition ist naheliegend, da wir uns, falls K algebraisch abgeschlossen ist, die Elemente eines Funktionenkörpers als Funktionen denken können.

Definition 2.2.5 Sei $z \in F$ und $P \in \mathbb{P}_F$. Wir sagen: P sei eine *Nullstelle* von z, wenn $\nu_P(z) > 0$ ist, und P sei ein *Pol* von z, wenn $\nu_P(z) < 0$ ist. Falls $\nu_P(z) = m > 0$ ist, nennen wir P eine Nullstelle *der Ordnung* m, falls $\nu_P(z) = -m < 0$ ist, sagen wir P ist ein Pol *der Ordnung* m.

Die nächste Folgerung kann man folgendermaßen interpretieren: jedes $z \in F$, welches nicht konstant ist, erzeugt eine nicht-konstante Funktion im Sinne von (2.5).

Folgerung 2.2.6 *Sei F/K ein Funktionenkörper, $z \in F$ nicht konstant. Dann hat z mindestens eine Nullstelle und einen Pol.*

Beweis. Betrachten wir den Ring $R = K[z]$ und das Ideal $I = zK[z]$. Satz 2.1.12 garantiert uns, dass eine Stelle $P \in \mathbb{P}_F$ mit $z \in P$ existiert, also ist P eine Nullstelle von z. Dasselbe Argument zeigt, dass z^{-1} eine Nullstelle $Q \in \mathbb{P}_F$ besitzt. Dieses Q ist ein Pol von z. □

Ein wichtiges Resultat ist die folgende Verallgemeinerung des Chinesischen Restsatzes. Dieser Satz stammt von Artin und Whaples (1967, siehe [1]) und ist unter anderem als schwacher Approximationssatz bekannt.

Satz 2.2.7 (Schwacher Approximationssatz) *Sei F/K ein Funktionenkörper, $P_1, \ldots, P_n \in \mathbb{P}_F$ paarweise verschiedene Stellen von F/K, x_1,*

$\ldots, x_n \in F$ *und* $r_1, \ldots, r_n \in \mathbb{Z}$. *Dann gibt es ein* $x \in F$ *mit*

$$\nu_{P_i}(x - x_i) = r_i \quad \textit{für} \quad i = 1, \ldots, n.$$

Beweis. Der Beweis ist in mehrere Schritte eingeteilt. Der Einfachheit halber schreiben wir ν_i anstatt ν_{P_i}.

1. Schritt: Es gibt ein $u \in F$ mit $\nu_1(u) > 0$ und $\nu_i(u) < 0$ für $i = 2, \ldots, n$.
Der Beweis dieser Behauptung erfolgt durch Induktion nach n. Für $n = 2$ beachten wir, dass $\mathcal{O}_{P_1} \not\subseteq \mathcal{O}_{P_2}$ gilt und umgekehrt, da Bewertungsringe nach Satz 2.2.4 (c) maximale Unterringe von F sind. Deshalb gibt es ein $y_1 \in \mathcal{O}_{P_1} \backslash \mathcal{O}_{P_2}$ und ein $y_2 \in \mathcal{O}_{P_2} \backslash \mathcal{O}_{P_1}$. Es gilt $\nu_1(y_1) \geq 0$, $\nu_2(y_1) < 0$, $\nu_1(y_2) < 0$ und $\nu_2(y_2) \geq 0$. Das Element $u := y_1/y_2$ hat also die gewünschte Eigenschaft: $\nu_1(u) > 0$, $\nu_2(u) < 0$.
Für $n > 2$ haben wir nach Induktionsannahme ein Element y mit $\nu_1(y) > 0, \nu_2(y) < 0, \ldots, \nu_{n-1}(y) < 0$. Wir müssen zeigen, dass $\nu_n(y) < 0$ ist. Im Fall $\nu_n(y) \geq 0$ wählen wir ein z mit $\nu_1(z) > 0$, $\nu_n(z) < 0$ und setzen $u := y + z^r$. Dabei ist $r \geq 1$ so gewählt, dass $r \cdot \nu_i(z) \neq \nu_i(y)$ für $i = 1, \ldots, n-1$ ist. Es folgt, dass $\nu_1(u) \geq \min\{\nu_1(y), r \cdot \nu_1(z)\} > 0$ und $\nu_i(u) = \min\{\nu_i(y), r \cdot \nu_i(z)\} < 0$ für $i = 2, \ldots, n$ ist.

2. Schritt: Es gibt ein $w \in F$, sodass $\nu_1(w - 1) > r_1$ und $\nu_i(w) > r_i$ für $i = 2, \ldots, n$ ist.
Wähle u aus dem 1. Schritt und setze $w := (1 + u^s)^{-1}$. Wir erhalten für genügend großes $s \in \mathbb{N}$, $\nu_1(w - 1) = \nu_1(-u^s(1 + u^s)^{-1}) = s \cdot \nu_1(u) > r_1$ und $\nu_i(w) = -\nu_i(1 + u^s) = -s \cdot \nu_i(u) > r_i$ für $i = 2, \ldots, n$.

3. Schritt: Bei gegebenen $y_1, \ldots, y_n \in F$ gibt es ein Element $z \in F$ mit $\nu_i(z - y_i) > r_i$ für $i = 1, \ldots, n$.
Wir wählen ein $s \in \mathbb{Z}$, sodass $\nu_i(y_j) \geq s$ für alle $i, j \in \{1, \ldots, n\}$ ist. Mit Hilfe von Schritt 2 erhalten wir $w_1, \ldots, w_n$ mit

$$\nu_i(w_i - 1) > r_i - s \quad \text{und} \quad \nu_j(w_i) > r_j - s \quad \text{für} \quad j \neq i.$$

Dann hat $z := \sum_{j=1}^{n} y_j w_j$ die gewünschten Eigenschaften.

Jetzt können wir den Beweis vervollständigen. Aus Schritt 3 erhalten wir ein $z \in F$ mit $\nu_i(z - x_i) > r_i$, $i = 1, \ldots, n$. Als nächstes wählen wir z_i mit $\nu_i(z_i) = r_i$, was trivialerweise möglich ist. Wieder finden wir aufgrund von Schritt 3 ein z' mit $\nu_i(z' - z_i) > r_i$ für $i = 1, \ldots, n$. Es folgt

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

Sei $x := z + z'$. Dann ist

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

womit die Behauptung gezeigt ist. □

Im Wesentlichen ist die Aussage des Approximationssatzes die Folgende: Wenn $v_1, \ldots, v_n$ paarweise verschiedene diskrete Bewertungen von F/K sind, $z \in F$ und wenn wir die Werte $v_1(z), \ldots, v_{n-1}(z)$ kennen, dann können wir nichts über den Wert $v_n(z)$ aussagen. Aus diesem Grund heißt Satz 2.2.7 auch manchmal *Satz von der Unabhängigkeit der Bewertungen.*

Wir erhalten mit Hilfe des schwachen Approximationssatzes 2.2.7 einen anderen Beweis von Folgerung 2.1.13 (b).

Folgerung 2.2.8 *Jeder Funktionenkörper hat unendlich viele Stellen.*

Beweis. Angenommen es gäbe nur endlich viele Stellen $P_1, \ldots, P_n$. Aufgrund des schwachen Approximationssatzes 2.2.7 könnten wir ein Element $0 \neq x \in F$ mit $\nu_{P_i}(x) > 0$ für $i = 1, \ldots, n$ finden. Dann muß x transzendent über K sein, da x Nullstellen besitzt. Widerspruch zu Folgerung 2.2.6, da x keine Pole besitzt. □

Wir können jetzt zeigen, dass die Anzahl der Nullstellen von $x \in F$ beschränkt ist. Später werden wir sehen, dass ein nicht konstantes x genauso viele Nullstellen, wie Polstellen besitzt, wenn man sie nur geeignet zählt. Ein wichtiger Schritt in diese Richtung wird der folgende Satz sein. Außerdem ist er eine Verschärfung der Resultate von Hilfssatz 2.1.5 und Satz 2.1.9.

Satz 2.2.9 (Nullstellensatz) *Sei F/K ein Funktionenkörper und $P_1, \ldots, P_r$ Nullstellen von einem Element $x \in F$. Dann gilt:*

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

Beweis. Wir setzen $\nu_i := \nu_{P_i}$, $f_i := \deg P_i$ und $e_i := \nu_i(x)$. Für jedes i gibt es ein Element t_i mit

$$\nu_i(t_i) = 1 \quad \text{und} \quad \nu_k(t_i) = 0 \quad \text{für} \quad k \neq i.$$

Als nächstes wählen wir $s_{i1}, \ldots, s_{if_i} \in \mathcal{O}_{P_i}$, sodass $s_{i1}(P_i), \ldots, s_{if_i}(P_i)$ eine Basis des Restklassenkörpers F_{P_i} über K bildet. Aufgrund des schwachen Approximationssatzes 2.2.7 können wir $z_{ij} \in F$ finden, sodass für alle i, j gilt:

$$\nu_i(s_{ij} - z_{ij}) > 0 \quad \text{und} \quad \nu_k(z_{ij}) \geq e_k \quad \text{für} \quad k \neq i. \tag{2.6}$$

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. Die Anzahl dieser Elemente ist $\sum_{i=1}^{r} f_i e_i = \sum_{i=1}^{r} \nu_{P_i}(x) \cdot \deg P_i$, sodass aus dieser Behauptung die Aussage des Satzes folgt.
Angenommen es gibt eine nicht triviale Linearkombination

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a z_{ij} = 0 \tag{2.7}$$

über $K(x)$. O.B.d.A. können wir annehmen, dass die $\varphi_{ija} \in K[x]$ sind und dass nicht alle φ_{ija} von x geteilt werden. Dann gibt es Indizes $k \in \{1, \ldots, r\}$ und $c \in \{0, 1, \ldots, e_k - 1\}$, sodass

$$\begin{aligned} &x \mid \varphi_{kja} \quad \text{für jedes} \quad a < c \quad \text{und jedes} \quad j \in \{1, \ldots, f_k\}, \\ &\text{und} \quad x \nmid \varphi_{kjc} \quad \text{für mindestens ein} \quad j \in \{1, \ldots, f_k\}. \end{aligned} \tag{2.8}$$

Wenn wir (2.7) mit t_k^{-c} multiplizieren, erhalten wir

$$\sum_{i=1}^{r} \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{ija} t_i^a t_k^{-c} z_{ij} = 0. \tag{2.9}$$

Für $i \neq k$ liegen alle Summanden von (2.9) in P_k da

$$\begin{aligned} \nu_k(\varphi_{ija} t_i^a t_k^{-c} z_{ij}) &= \nu_k(\varphi_{ija}) + a\nu_k(t_i) - c\nu_k(t_k) + \nu_k(z_{ij}) \\ &\geq 0 + 0 - c + e_k > 0. \end{aligned}$$

Für $i = k$ und $a < c$ folgt aus der Implikation $x \mid \varphi_{kja} \Rightarrow \nu_k(\varphi_{kja}) \geq e_k$, dass

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

ist. Für $i = k$ und $a > c$ gilt

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

Wenn wir das mit (2.9) kombinieren, erhalten wir

$$\sum_{j=1}^{f_k} \varphi_{kjc} z_{kj} \in P_k. \tag{2.10}$$

Wenn wir beachten, dass $\varphi_{kjc}(P_k) \in K$ ist, und dass aufgrund (2.8) nicht alle $\varphi_{kjc}(P_k) = 0$ sein können, erhalten wir aus (2.10) eine nicht triviale Linearkombination

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

über K. Das ist ein Widerspruch, dazu dass $z_{k1}(P_k), \ldots, z_{kf_k}(P_k)$ eine Basis von F_{P_k}/K bildet. □

Folgerung 2.2.10 *In einem Funktionenkörper F/K hat jedes Element $0 \neq x \in F$ nur endlich viele Nullstellen und Pole.*

Beweis. Wenn x konstant ist, besitzt x weder Nullstellen noch Pole. Wenn x transzendent über K ist, dann ist die Anzahl der Nullstellen $\leq [F : K(x)]$ aufgrund des Nullstellensatzes 2.2.9. Dasselbe Argument zeigt, dass x^{-1} nur endlich viele Nullstellen besitzt. □

Eine weitere unmittelbare Folgerung ist, dass verschiedene Elemente eines Funktionenkörpers verschiedene Funktionen auf den Stellen induzieren. Es gilt:

Folgerung 2.2.11 *Sei F/K ein Funktionenkörper und $x, y \in F$. Falls $x(P) = y(P)$ für alle Stellen P von F/K gilt, dann folgt $x = y$.*

Beweis. Die Bedingung impliziert, dass $\nu_P(x - y) > 0$ für alle Stellen P ist, also sind alle Stellen Nullstellen von $x - y$. Wegen Folgerung 2.1.13 (b) oder Folgerung 2.2.8 gibt es unendlich viele Stellen. Aus Folgerung 2.2.10 folgt nun, dass $x - y = 0$ gelten muss. □

2.3 Der rationale Funktionenkörper

Um ein besseres Verständnis für Bewertungen und Stellen zu bekommen, ist es wichtig eine genaue Vorstellung von ihnen zu haben, zumindest im einfachsten Fall, dem des rationalen Funktionenkörpers. Deshalb wollen wir jetzt den rationalen Funktionenkörper $F = K(x)$ betrachten, wobei x transzendent über K ist.

Gegeben sei ein irreduzibles Polynom $p(x) \in K[x]$. Wir betrachten die Menge

$$\mathcal{O}_{p(x)} := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x], p(x) \nmid g(x) \right\}. \tag{2.11}$$

Wie man sofort sieht, ist $\mathcal{O}_{p(x)}$ ein Bewertungsring von $K(x)/K$. Die dazugehörige Stelle lautet

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x], p(x) \mid f(x), p(x) \nmid g(x) \right\}. \tag{2.12}$$

Im Fall, dass $p(x) = x - \alpha$ linear ist, mit $\alpha \in K$, schreiben wir abkürzend

$$P_\alpha := P_{x-\alpha} \in \mathbb{P}_{K(x)}. \tag{2.13}$$

Ein weiterer Bewertungsring von $K(x)/K$ ist der folgende

$$\mathcal{O}_\infty := \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x], \deg f(x) \leq \deg g(x) \right\} \tag{2.14}$$

mit dem maximalen Ideal

$$P_\infty = \left\{ \frac{f(x)}{g(x)} \;\middle|\; f(x), g(x) \in K[x], \deg f(x) < \deg g(x) \right\}. \tag{2.15}$$

Diese Stelle nennt man auch die *unendliche* Stelle von $K(x)/K$. Man beachte, dass diese Bezeichnungen von der speziellen Wahl des erzeugenden Elementes x von $K(x)/K$ abhängen und dass die unendliche Stelle bezüglich $1/x$ die Stelle P_0 bezüglich x ist.

Ihre Eigenschaften sind im folgenden Satz zusammengefasst:

Satz 2.3.1 *Sei $F = K(x)$ der rationale Funktionenkörper.*
(a) *Sei $P = P_{p(x)} \in \mathbb{P}_{K(x)}$ die durch (2.12) definierte Stelle, wobei $p(x) \in K[x]$ ein irreduzibles Polynom ist. Dann ist $p(x)$ ein Primelement von P und die dazugehörige diskrete Bewertung ν_P kann folgendermaßen beschrieben werden: wenn $z \in K(x)\backslash\{0\}$ in der Form $z = p(x)^n \cdot (f(x)/g(x))$ mit $n \in \mathbb{Z}, f(x), g(x) \in K[x], p(x) \nmid f(x)$ und $p(x) \nmid g(x)$ geschrieben wird, dann ist $\nu_P(z) = n$.*
Der Restklassenkörper $K(x)_P = \mathcal{O}/P$ ist isomorph zu $K[x]/(p(x))$, ein Isomorphismus ist gegeben durch

$$\phi : \left\{ \begin{array}{ccc} K[x]/(p(x)) & \longrightarrow & K(x)_P, \\ f(x) \bmod p(x) & \longmapsto & f(x)(P) \end{array} \right.$$

Daraus folgt außerdem: $\deg P = \deg p(x)$.
(b) *Im Fall: $p(x) = x - \alpha$ mit $\alpha \in K$, ist der Grad von $P = P_\alpha$ eins und der Restklassenabbildung ist gegeben durch*

$$z(P) = z(\alpha) \quad \textit{für} \quad z \in K(x),$$

wobei $z(\alpha)$ folgendermaßen definiert ist: sei $z = f(x)/g(x)$ mit relativ primen Polynomen $f(x), g(x) \in K[x]$. Dann ist

$$z(\alpha) = \left\{ \begin{array}{cc} f(\alpha)/g(\alpha) & \textit{falls} \quad g(\alpha) \neq 0, \\ \infty & \textit{falls} \quad g(\alpha) = 0. \end{array} \right.$$

(c) *Sei $P = P_\infty$ die unendliche Stelle von $K(x)/K$ definiert durch (2.15).*

Dann gilt $\deg P_\infty = 1$. *Ein Primelement für* P_∞ *ist* $1/x$. *Die dazugehörige diskrete Bewertung ist gegeben durch*

$$\nu_\infty(f(x)/g(x)) = \deg g(x) - \deg f(x),$$

wobei $f(x), g(x) \in K[x]$ *sind. Die Restklassenabbildung zu* P_∞ *wird bestimmt durch* $z(P_\infty) = z(\infty)$ *für* $z \in K(x)$, *wobei* $z(\infty)$ *wie folgt definiert ist: falls*

$$z = \frac{a_n x^n + \cdots + a_0}{b_m x^m + \cdots + b_0} \quad \textit{mit} \quad a_n, b_m \neq 0,$$

dann ist

$$z(\infty) = \begin{cases} a_n/b_m & \textit{falls} \quad n = m, \\ 0 & \textit{falls} \quad n < m, \\ \infty & \textit{falls} \quad n > m. \end{cases}$$

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

Beweis. (a) Sei $P = P_{p(x)}, p(x) \in K[x]$ irreduzibel. Das Ideal $P_{p(x)} \subseteq \mathcal{O}_{p(x)}$ wird offensichtlich von $p(x)$ erzeugt, daher ist $p(x)$ ein Primelement für P. Die Beschreibung der zugehörigen diskreten Bewertung ist daher ebenfalls klar. Um die Aussage über den Restklassenkörper zu zeigen, betrachten wir den Ringhomomorphismus

$$\varphi : \begin{cases} K[x] & \longrightarrow & K(x)_P, \\ f(x) & \longmapsto & f(x)(P). \end{cases}$$

Der Kern von φ ist klarerweise das von $p(x)$ erzeugte Ideal. Die Abbildung ist surjektiv, denn wenn $z \in \mathcal{O}_{p(x)}$ ist – wir können $z = u(x)/v(x)$ und $u(x), v(x) \in K[x]$ mit $a(x)p(x) + b(x)v(x) = 1$ schreiben –, dann gilt

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

und $z(P) = (b(x)u(x))(P)$ liegt im Bild von φ. Deshalb induziert φ den behaupteten Isomorphismus ϕ von $K[x]/(p(x))$ auf $K(x)_P$.
(b) Jetzt sei $P = P_\alpha$ mit $\alpha \in K$. Falls $f(x) \in K[x]$ ist, dann gilt $(x - \alpha) \mid (f(x) - f(\alpha))$ und daher $f(x)(P) = (f(x) - f(\alpha))(P) + f(\alpha)(P) = f(\alpha)$. Ein beliebiges Element $z \in \mathcal{O}_P$ kann als $z = f(x)/g(x)$ mit Polynomen $f(x), g(x) \in K[x]$ und $(x - \alpha) \nmid g(x)$ geschrieben werden. Daher ist $g(x)(P) = g(\alpha) \neq 0$ und damit

$$z(P) = \frac{f(x)(P)}{g(x)(P)} = \frac{f(\alpha)}{g(\alpha)} = z(\alpha).$$

(c) Die erste Aussage folgt aus der Beobachtung, dass $F_{P_\infty} = \mathcal{O}_\infty / P_\infty = \{r + P_\infty \mid r \in K\} \cong K$ gilt. Das bedeutet: $\deg P_\infty = 1$. Wir zeigen als

nächstes, dass $1/x$ ein Primelement von P_∞ ist. Wir nehmen ein Element $z = f(x)/g(x) \in P_\infty$. Es gilt also $\deg f(x) < \deg g(x)$. Dann gilt

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

Daher ist $z \in (1/x)\mathcal{O}_\infty$ und somit $1/x$ ein P_∞-Primelement. Die Aussage über die zu P_∞ gehörige diskrete Bewertung folgt jetzt unmittelbar aus der Definition. Die letzte Aussage rechnet man direkt nach.
(d) Es gibt in $K(x)/K$ rationale Stellen, nämlich die Stellen $P = P_\alpha$ mit $\alpha \in K$. Daher folgt die Aussage sofort aus Folgerung 2.1.11. □

Satz 2.3.2 *Es gibt außer den Stellen $P_{p(x)}$ und P_∞, definiert durch (2.12) und (2.15), keine weiteren Stellen im rationalen Funktionenkörper $K(x)/K$.*

Beweis. Es genügt folgendes zu zeigen: Gegeben sei $P \in \mathbb{P}_{K(x)}$, dann ist entweder $P = P_\infty$, oder es gibt es ein irreduzibles Polynom $p(x) \in K[x]$ mit $\mathcal{O}_{p(x)} = \mathcal{O}_P$.
1. Fall: Sei $x \in \mathcal{O}_P$. Dann gilt $K[x] \subseteq \mathcal{O}_P$. Sei $I := K[x] \cap P$. Dann ist I ein Ideal von $K[x]$ und prim. Die Restklassenabbildung induziert eine Einbettung $K[x]/I \hookrightarrow K(x)_P$, daher ist nach Satz 2.1.9 $I \neq \{0\}$. Es folgt, dass ein eindeutig bestimmtes, irreduzibles, normiertes Polynom $p(x) \in K[x]$ existiert, mit $I = K[x] \cap P = p(x) \cdot K[x]$. Jedes $g(x) \in K[x]$ mit $p(x) \nmid g(x)$ ist nicht in I, daher ist $g(x) \notin P$ und damit $1/g(x) \in \mathcal{O}_P$ nach Satz 2.1.4. Wir schließen

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

Da Bewertungsringe nach Satz 2.2.4 maximale echte Unterringe von $K[x]$ sind, muß $\mathcal{O}_P = \mathcal{O}_{p(x)}$ gelten.
2. Fall: Angenommen $x \notin \mathcal{O}_P$. Wir können zunächst $K[x^{-1}] \subseteq \mathcal{O}_P, x^{-1} \in P \cap K[x^{-1}]$ und $P \cap K[x^{-1}] = x^{-1}K[x^{-1}]$ schließen. Wie im 1. Fall erhalten wir

$$\begin{aligned}
\mathcal{O}_P &\supseteq \left\{ \frac{f(x^{-1})}{g(x^{-1})} \,\middle|\, f(x^{-1}), g(x^{-1}) \in K[x^{-1}], x^{-1} \nmid g(x^{-1}) \right\} \\
&= \left\{ \frac{a_0 + a_1 x^{-1} + \cdots + a_n x^{-n}}{b_0 + b_1 x^{-1} + \cdots + b_m x^{-m}} \,\middle|\, b_0 \neq 0 \right\} \\
&= \left\{ \frac{a_0 x^{m+n} + \cdots + a_n x^m}{b_0 x^{m+n} + \cdots + b_m x^n} \,\middle|\, b_0 \neq 0 \right\} \\
&= \left\{ \frac{u(x)}{v(x)} \,\middle|\, u(x), v(x) \in K[x], \deg u(x) \leq \deg v(x) \right\} \\
&= \mathcal{O}_\infty.
\end{aligned}$$

Daraus folgt schließlich $\mathcal{O}_P = \mathcal{O}_\infty$ und damit $P = P_\infty$. □

Folgerung 2.3.3 *Die rationalen Stellen von $K(x)/K$ stehen in einer umgekehrt eindeutigen Beziehung mit $K \cup \{\infty\}$.*

Beweis. Unmittelbare Folgerung aus Satz 2.3.1 und Satz 2.3.2. □

2.4 Divisoren

Der Konstantenkörper $\bar{K}$ eines algebraischen Funktionenkörpers F/K ist nach Folgerung 2.1.14 eine endliche Erweiterung von K und wir können F auch als Funktionenkörper über $\bar{K}$ auffassen. Deshalb ist es uns problemlos möglich von nun an folgende Voraussetzung zu treffen:

F/K sei ein algebraischer Funktionenkörper in einer Variablen, sodass K der volle Konstantenkörper von F/K ist.

Wir definieren nun Folgendes:

Definition 2.4.1 Die (additiv geschriebene) freie abelsche Gruppe, welche durch die Stellen von F/K erzeugt wird, heißt die *Divisorengruppe* von F/K und wird mit $\mathcal{D}_F$ bezeichnet. Die Elemente von $\mathcal{D}_F$ heißen *Divisoren* von F/K.

Ein Divisor D ist also eine formale Summe

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

Der *Träger* von D ist definiert durch

$$\operatorname{supp} D := \{P \in \mathbb{P}_F \mid n_P \neq 0\}.$$

Die Addition von zwei Divisoren $D = \sum n_P P$ und $D' = \sum n'_P P$ erfolgt komponentenweise:

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

Das Nullelement der Divisorengruppe $\mathcal{D}_F$ ist der *Nulldivisor*

$$0 := \sum_{P \in \mathbb{P}_F} n_P P, \quad \text{mit allen} \quad n_P = 0.$$

Wir können die diskreten Bewertungen folgendermaßen auf Divisoren fortsetzen: Für $Q \in \mathbb{P}_F$ und $D = \sum n_P P \in \mathcal{D}_F$ definieren wir $\nu_Q(D) := n_Q$.

Es ist dann

$$\operatorname{supp} D = \{P \in \mathbb{P}_F \mid \nu_P(D) \neq 0\} \quad \text{und} \quad D = \sum_{P \in \operatorname{supp} D} \nu_P(D) \cdot P.$$

Auf $\mathcal{D}_F$ kann man durch

$$D_1 \leq D_2 : \Longleftrightarrow \ \nu_P(D_1) \leq \nu_P(D_2) \quad \text{für alle} \quad P \in \mathbb{P}_F$$

eine partielle Ordnung definieren.

Definition 2.4.2 Ein Divisor der Form $D = P$ mit $P \in \mathbb{P}_F$ heißt ein *Primdivisor*. Ein Divisor $D \geq 0$ heißt *positiv* (oder *effektiv*).

Der Grad eines Divisors D wird definiert durch

$$\deg D := \sum_{P \in \mathbb{P}_F} \nu_P(D) \cdot \deg P.$$

Dadurch ist ein Homomorphismus $\deg : \mathcal{D}_F \to \mathbb{Z}$ definiert.

Nach Folgerung 2.2.10 hat jedes Element $0 \neq x \in F$ nur endlich viele Nullstellen und Pole in $\mathbb{P}_F$. Deshalb ist die folgende Definition sinnvoll.

Definition 2.4.3 Sei $0 \neq x \in F$ und bezeichne Z (bzw. N) die Menge der Nullstellen (bzw. Pole) von x in $\mathbb{P}_F$. Wir definieren

$$\begin{aligned}
(x)_0 &:= \sum_{P \in Z} \nu_P(x) P, \quad \text{den } \textit{Nullstellendivisor} \text{ von } \quad x, \\
(x)_\infty &:= \sum_{P \in N} (-\nu_P(x)) P, \quad \text{den } \textit{Polstellendivisor} \text{ von } \quad x, \\
(x) &:= (x)_0 - (x)_\infty, \quad \text{den } \textit{Hauptdivisor} \text{ von } \quad x.
\end{aligned}$$

Klarerweise ist $(x)_0 \geq 0, (x)_\infty \geq 0$ und es gilt

$$(x) = \sum_{P \in \mathbb{P}_F} \nu_P(x) P. \tag{2.16}$$

Hilfssatz 2.4.4 *Für $0 \neq x \in F$ gilt:*

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

Beweis. Folgt sofort aus Satz 2.1.4, Folgerung 2.2.6 und der Generalvoraussetzung, dass $K = \bar{K}$ ist. □

Hilfssatz 2.4.5 *Die Menge* $\{(x) \mid x \in F\backslash\{0\}\}$ *ist eine Untergruppe von* $\mathcal{D}_F$.

Beweis. Nach Hilfssatz 2.4.4 liegt der Nulldivisor in dieser Menge. Falls $0 \neq x, y \in F$ gegeben sind, dann gilt nach (2.16) $(xy) = (x) + (y)$ und damit die Behauptung. □

Definition 2.4.6

$$\mathcal{P}_F := \{(x) \mid x \in F\backslash\{0\}\}$$

heißt die *Gruppe der Hauptdivisoren* von F/K. Die Faktorgruppe

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

heißt die *Divisorklassengruppe*. Für einen Divisor $D \in \mathcal{D}_F$ schreiben wir $[D]$ für das zugehörige Element in der Faktorgruppe $\mathcal{C}_F$, und sprechen von der *Divisorklasse* von D. Zwei Divisoren $D, D' \in \mathcal{D}_F$ nennen wir äquivalent, wenn $[D] = [D']$ gilt, also wenn $D = D' + (x)$ für ein $x \in F\backslash\{0\}$ ist. Wir schreiben in diesem Fall

$$D \sim D'.$$

Wie man sofort sieht, ist $\sim$ eine Äquivalenzrelation.

Die nächste Definition spielt eine entscheidende Rolle in der weiteren Theorie.

Definition 2.4.7 Für einen Divisor $A \in \mathcal{D}_F$ setzen wir

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

und nennen $\mathcal{L}(A)$ den *Riemann-Roch-Raum* von A.

Diese Definition läßt sich folgendermaßen interpretieren: Es sei

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

mit $n_i > 0, m_j > 0$ dann enthält $\mathcal{L}(A)$ alle Elemente $x \in F$, die folgende Bedingungen erfüllen:
(1) x hat Nullstellen mit Ordnung $\geq m_j$ an den Stellen Q_j für $j = 1, \ldots, s$, und
(2) x darf nur an den Stellen $P_1, \ldots, P_r$ Pole haben, mit Polordnung höchstens n_i bei P_i $(i = 1, \ldots, r)$.

Zunächst wollen wir einige Eigenschaften und einfache Beobachtungen zusammenfassen.

Hilfssatz 2.4.8 *Sei $A \in \mathcal{D}_F$. Dann gilt:*
(a) $x \in \mathcal{L}(A) \iff \nu_P(x) \geq -\nu_P(A)$ *für alle* $P \in \mathbb{P}_F$.
(b) $\mathcal{L}(A) \neq \{0\} \iff$ *es gibt einen Divisor* $A' \sim A$ *mit* $A' \geq 0$.

Beweis. (a) Trivial.
(b) Folgt sofort aus $0 \neq x \in \mathcal{L}(A) \Leftrightarrow (x) \geq -A \Leftrightarrow A' := (x) + A \geq 0$ und der Definition von $\sim$. □

Hilfssatz 2.4.9 *Sei $A \in \mathcal{D}_F$. Dann gilt:*
(a) $\mathcal{L}(A)$ *ist ein Vektorraum über* K.
(b) *Wenn* A' *ein zu* A *äquivalenter Divisor ist, dann gilt* $\mathcal{L}(A) \cong \mathcal{L}(A')$ *(isomorph als Vektorräume über* K*).*

Beweis. (a) Sei $x, y \in \mathcal{L}(A)$ und $a \in K$. Für jedes $P \in \mathbb{P}_F$ gilt: $\nu_P(x+y) \geq \min\{\nu_P(x), \nu_P(y)\} \geq -\nu_P(A)$ und $\nu_P(ax) = \nu_P(a) + \nu_P(x) \geq -\nu_P(A)$. Daher sind nach Hilfssatz 2.4.8 $x+y$ und ax in $\mathcal{L}(A)$.
(b) Nach Annahme ist $A = A' + (z)$ mit $0 \neq z \in F$. Betrachte die Abbildung

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{L}(A) & \longrightarrow & F, \\ x & \longmapsto & xz. \end{array} \right.$$

Das ist eine K-lineare Abbildung, deren Bild in $\mathcal{L}(A')$ liegt. Genauso ist

$$\varphi' : \left\{ \begin{array}{ccc} \mathcal{L}(A') & \longrightarrow & F, \\ x & \longmapsto & xz^{-1} \end{array} \right.$$

eine K-lineare Abbildung von $\mathcal{L}(A')$ nach $\mathcal{L}(A)$. Diese Abbildungen sind zueinander invers, daher ist φ ein Isomorphismus zwischen $\mathcal{L}(A)$ und $\mathcal{L}(A')$. □

Hilfssatz 2.4.10 *Es gilt:*
(a) $\mathcal{L}(0) = K$.
(b) *Falls* $A < 0$, $A \in \mathcal{D}_F$ *ist, dann ist* $\mathcal{L}(A) = \{0\}$.

Beweis. (a) Wir haben $(x) = 0$ für $0 \neq x \in K$ nach Hilfssatz 2.4.4, daher ist $K \subseteq \mathcal{L}(0)$. Umgekehrt folgt aus $0 \neq x \in \mathcal{L}(0)$, dass $(x) \geq 0$ ist. Das bedeutet aber, dass x keine Pole besitzt. Aus Folgerung 2.2.6 erhalten wir, dass $x \in K$ sein muß.
(b) Angenommen es gibt ein Element $0 \neq x \in \mathcal{L}(A)$. Dann ist $(x) \geq -A > 0$, was zur Folge hat, dass x mindestens eine Nullstelle, aber keinen Pol besitzt, was unmöglich ist. □

Unser nächstes Ziel ist es zu zeigen, dass $\mathcal{L}(A)$ für alle $A \in \mathcal{D}_F$ endlichdimensional ist.

Hilfssatz 2.4.11 *Seien A, B Divisoren von F/K mit $A \leq B$. Dann haben wir $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ und*

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

Beweis. $\mathcal{L}(A) \subseteq \mathcal{L}(B)$ ist trivial. Um die zweite Aussage zu beweisen, können wir annehmen, dass $B = A + P$ für ein $P \in \mathbb{P}_F$ gilt. Der allgemeine Fall folgt dann durch vollständige Induktion. Wählen wir also ein Element $t \in F$ mit $\nu_P(t) = \nu_P(B) = \nu_P(A) + 1$. Für $x \in \mathcal{L}(B)$ gilt: $\nu_P(x) \geq -\nu_P(B) = -\nu_P(t)$. Daher ist $xt \in \mathcal{O}_P$. Wir erhalten durch

$$\psi : \begin{cases} \mathcal{L}(B) & \longrightarrow & F_P, \\ x & \longmapsto & (xt)(P) \end{cases}$$

eine K-lineare Abbildung. Es gilt: $x \in \ker(\psi) \Leftrightarrow \nu_P(xt) > 0$, das heißt $\nu_P(x) \geq -\nu_P(A)$. Daher ist $\ker(\psi) = \mathcal{L}(A)$, und ψ induziert eine K-lineare injektive Abbildung von $\mathcal{L}(B)/\mathcal{L}(A)$ nach F_P. Es folgt

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

□

Satz 2.4.12 *Für jeden Divisor $A \in \mathcal{D}_F$ ist der Riemann-Roch-Raum $\mathcal{L}(A)$ ein endlichdimensionaler Vektorraum über K. Genauer gilt: Wenn $A = A_+ - A_-$ mit positiven Divisoren A_+ und A_- ist, dann ist*

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

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

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

Da $0 \leq A_+$ gilt, folgt aus Hilfssatz 2.4.11, dass $\dim(\mathcal{L}(A_+)/\mathcal{L}(0)) \leq \deg A_+$ ist. Andererseits gilt $\dim \mathcal{L}(A_+) = \dim(\mathcal{L}(A_+)/\mathcal{L}(0)) + 1$, da nach Hilfssatz 2.4.10 (a) $\mathcal{L}(0) = K$ ist, und damit folgt die Behauptung. □

Definition 2.4.13 Für $A \in \mathcal{D}_F$ nennt man die Zahl $\dim A := \dim \mathcal{L}(A)$ die *Dimension* des Divisors A.

Eine der wichtigsten Fragen in der Theorie der algebraischen Funktionenkörper ist die Berechnung der Dimension eines Divisors. Die Antwort wird uns der Satz von Riemann-Roch geben.

Als erster Schritt in diese Richtung zeigen wir die folgende Verschärfung des Nullstellensatzes 2.2.9. Ihre Aussage ist im wesentlichen, dass jedes Element $0 \neq x \in F$ genauso viele Nullstellen wie Pole besitzt, wenn man sie nur richtig zählt.

Satz 2.4.14 *Jeder Hauptdivisor hat Grad* 0. *Genauer: Sei* $0 \neq x \in F/K$ *und* $(x)_0$ *bzw.* $(x)_\infty$ *bezeichne den Nullstellen- bzw. Poldivisor von* x. *Dann gilt:*

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

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

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

wo $P_1, \ldots, P_r$ alle Pole von x sind. Dann gilt nach dem Nullstellensatz 2.2.9

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

und daher bleibt zu zeigen, dass $n \leq \deg B$ ebenfalls gilt. Wählen wir eine Basis $u_1, \ldots, u_n$ von $F/K(x)$ und einen Divisor $C \geq 0$, sodass $(u_i) \geq -C$ für $i = 1, \ldots, n$ gilt. Wir erhalten

$$\dim(lB + C) \geq n(l+1) \quad \text{für alle} \quad l \geq 0, \tag{2.17}$$

was unmittelbar aus der Tatsache, dass $x^i u_j \in \mathcal{L}(lB + C)$ für $0 \leq i \leq l$, $1 \leq j \leq n$ gilt, folgt. Man beachte dabei, dass diese Elemente linear unabhängig über K sind, da $u_1, \ldots, u_n$ linear unabhängig über $K(x)$ sind. Wenn wir $c := \deg C$ setzen, erhalten wir nach Satz 2.4.12 $n(l+1) \leq \dim(lB + C) \leq l \cdot \deg B + c + 1$. Daher gilt

$$l(\deg B - n) \geq n - c - 1 \tag{2.18}$$

für alle $l \in \mathbb{N}$. Die rechte Seite von (2.18) ist unabhängig von l, daher ist (2.18) nur möglich, wenn $\deg B \geq n$ ist.
Wir haben also gezeigt, dass $\deg(x)_\infty = [F : K(x)]$ ist. Da $(x)_0 = (x^{-1})_\infty$ gilt, können wir nun schließen, dass $\deg(x)_0 = \deg(x^{-1})_\infty = [F : K(x^{-1})] = [F : K(x)]$ ist. □

Folgerung 2.4.15
(a) *Seien* A, A' *äquivalente Divisoren. Dann ist* $\dim A = \dim A'$ *und* $\deg A = \deg A'$.
(b) *Falls* $\deg A < 0$, *dann ist* $\dim A = 0$.
(c) *Für einen Divisor* A *mit Grad* 0 *sind die folgenden Aussagen äquivalent:*

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

Beweis. (a) Folgt sofort aus Hilfssatz 2.4.9 und Satz 2.4.14.
(b) Angenommen, dass $\dim A > 0$ gilt. Nach Hilfssatz 2.4.8 (b) gibt es einen Divisor $A' \sim A$ mit $A' \geq 0$. Daher ist $\deg A = \deg A' \geq 0$. Widerspruch!
(c) (1) $\Rightarrow$ (2): Falls $A = (x)$ ein Hauptdivisor ist, dann ist $x^{-1} \in \mathcal{L}(A)$ und daher gilt $\dim A \geq 1$.
(2) $\Rightarrow$ (3): Nach Voraussetzung gilt $\dim A \geq 1$ und $\deg A = 0$. Dann ist $A \sim A'$ für ein $A' \geq 0$. Die Bedingungen $A' \geq 0$ und $\deg A' = 0$ implizieren, dass $A' = 0$ ist, daher gilt nach Hilfssatz 2.4.10 (a) $\dim A = \dim A' = \dim 0 = 1$.
(3) $\Rightarrow$ (1): Nach Voraussetzung gilt $\dim A = 1$ und $\deg A = 0$. Wähle $0 \neq z \in \mathcal{L}(A)$, dann ist $(z) + A \geq 0$. Da $\deg((z) + A) = 0$ ist, folgt dass $(z) + A = 0$ ist. Daher ist $A = -(z) = (z^{-1})$ ein Hauptdivisor. □

In Satz 2.4.12 haben wir gesehen, dass

$$\dim A \leq 1 + \deg A \tag{2.19}$$

für jeden Divisor $A \geq 0$ ist. Tatsächlich gilt (2.19) für beliebige Divisoren mit Grad ≥ 0.

Hilfssatz 2.4.16 *Sei A ein Divisor mit $\deg A \geq 0$. Dann gilt:*

$$\dim A \leq 1 + \deg A.$$

Beweis. Wir können annehmen, dass $\dim A > 0$ ist. Nach Hilfssatz 2.4.8 (b) gilt $A \sim A'$ für einen Divisor $A' \geq 0$. Daher ist $\dim A = \dim A' \leq 1 + \deg A' = 1 + \deg A$ nach Folgerung 2.4.15 (a). □

Als nächstes wollen wir die Existenz einer unteren Schranke für $\dim A$ zeigen, die von ähnlicher Gestalt wie (2.19) ist.

Satz 2.4.17 *Es gibt eine Konstante $\gamma \in \mathbb{Z}$, sodass für alle Divisoren $A \in \mathcal{D}_F$ gilt:*

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

Beweis. Zunächst gilt nach Hilfssatz 2.4.11

$$A_1 \leq A_2 \Rightarrow \deg A_1 - \dim A_1 \leq \deg A_2 - \dim A_2. \tag{2.20}$$

Wir wählen ein Element $x \in F \backslash K$ fest und betrachten den Divisor $B := (x)_\infty$. Wie im Beweis von Satz 2.4.14 gibt es einen Divisor $C \geq 0$ (abhängig

von x), sodass $\dim(lB+C) \geq (l+1)\cdot \deg B$ für alle $l \geq 0$ gilt (siehe (2.17)). Andererseits gilt nach Hilfssatz 2.4.11 $\dim(lB+C) \leq \dim(lB) + \deg C$. Durch Kombination dieser beiden Ungleichungen erhalten wir

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

Daher gilt

$$\deg(lB) - \dim(lB) \leq \gamma \quad \text{für alle} \quad l \geq 0 \tag{2.21}$$

mit einem $\gamma \in \mathbb{Z}$. Wir wollen zeigen, dass (2.21) mit demselben γ auch dann noch gilt, wenn wir lB durch irgendeinen Divisor $A \in \mathcal{D}_F$ ersetzen. Dazu zeigen wir zunächst die folgende Behauptung:

Behauptung: Gegeben sei ein Divisor A. Dann existieren Divisoren A_1, D und eine ganze Zahl $l \geq 0$, sodass $A \leq A_1$, $A_1 \sim D$ und $D \leq lB$ ist.

Zum Beweis dieser Behauptung wählen wir $A_1 \geq A$, sodass $A_1 \geq 0$ ist. Dann gilt

$$\begin{array}{lll} \dim(lB - A_1) & \geq & \dim(lB) - \deg A_1 \qquad \text{(nach Hilfssatz 2.4.11)} \\ & \geq & \deg(lB) - \gamma - \deg A_1 \quad \text{(nach (2.21))} \\ & > & 0 \end{array}$$

für genügend großes l. Daher gibt es ein Element $0 \neq z \in \mathcal{L}(lB - A_1)$. Wenn wir $D := A_1 - (z)$ setzen, erhalten wir $A_1 \sim D$ und $D \leq A_1 - (A_1 - lB) = lB$, wie gewünscht.

Die Aussage des Satzes folgt jetzt so:

$$\begin{array}{lll} \deg A - \dim A & \leq & \deg A_1 - \dim A_1 \qquad \text{(nach (2.20))} \\ & = & \deg D - \dim D \qquad \text{(nach Folgerung 2.4.15)} \\ & \leq & \deg(lB) - \dim(lB) \quad \text{(nach (2.20))} \\ & \leq & \gamma \qquad \text{(nach (2.21)).} \end{array}$$

□

Besonders wichtig ist dabei die Tatsache, dass γ nicht von A, sondern nur vom Funktionenkörper F/K abhängt.

Definition 2.4.18 Das *Geschlecht* von F/K ist definiert durch

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

Man beachte, dass diese Definition aufgrund von Satz 2.4.17 sinnvoll ist. Es wird sich herausstellen, dass das Geschlecht die wichtigste Invariante eines Funktionenkörpers ist. Im Folgenden setzen wir stets voraus:

F/K sei ein algebraischer Funktionenkörper mit Geschlecht g.

Als erstes erhalten wir die nachstehende einfache Aussage über das Geschlecht.

Hilfssatz 2.4.19 *Das Geschlecht von F/K ist eine nicht negative ganze Zahl.*

Beweis. Wir setzen in der Definition des Geschlechtes $A = 0$. Dann erhalten wir $\deg(0) - \dim(0) + 1 = 0$, daher ist $g \geq 0$. □

Satz 2.4.20 (Satz von Riemann) *Sei F/K ein Funktionenkörper mit Geschlecht g.*
(a) *Für jeden Divisor $A \in \mathcal{D}_F$ gilt:*

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

(b) *Es gibt eine ganze Zahl c, die nur von F/K abhängt, sodass*

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

ist, wann immer $\deg A \geq c$ *ist.*

Beweis. (a) Folgt sofort aus der Definition des Geschlechts.
(b) Wähle einen Divisor A_0 mit $g = \deg A_0 - \dim A_0 + 1$ und setze $c := \deg A_0 + g$. Falls $\deg A \geq c$ ist, dann gilt

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

Daher gibt es ein Element $0 \neq z \in \mathcal{L}(A - A_0)$. Betrachten wir jetzt den Divisor $A' := A + (z)$, der $\geq A_0$ ist. Dann haben wir

$$\begin{array}{rcll} \deg A - \dim A & = & \deg A' - \dim A' & \text{(nach Folgerung 2.4.15)} \\ & \geq & \deg A_0 - \dim A_0 & \text{(nach Hilfssatz 2.4.11)} \\ & = & g - 1. & \end{array}$$

Daher ist $\dim A \leq \deg A + 1 - g$. □

Im Allgemeinen ist es sehr schwer, das Geschlecht eines Funktionenkörpers zu bestimmen. Als sehr einfaches Beispiel wollen wir das Geschlecht des rationalen Funktionenkörpers berechnen.

Satz 2.4.21 *Der rationale Funktionenkörper $K(x)/K$ hat Geschlecht $g = 0$.*

Beweis. Sei P_∞ der Poldivisor von x. Betrachte für $r \geq 0$ den Vektorraum $\mathcal{L}(rP_\infty)$. Offensichtlich sind die Elemente $1, x, \ldots, x^r$ in $\mathcal{L}(rP_\infty)$, daher gilt

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

für genügend großes r. Es ist also $g \leq 0$. Nach Hilfssatz 2.4.19 ist aber für jeden Funktionenkörper $g \geq 0$. Damit folgt die Behauptung. $\square$

2.5 Adèle und Weil-Differentiale

Am Beginn steht folgende Definition:

Definition 2.5.1 Für $A \in \mathcal{D}_F$, nennen wir

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

den *Spezialitätsindex* von A.

Der Satz von Riemann 2.4.20 zeigt uns, dass $i(A)$ eine nicht negative ganze Zahl ist, mit $i(A) = 0$ für $\deg A$ genügend groß. Wir werden in diesem Kapitel einige Interpretationen für $i(A)$ als Dimension gewisser Vektorräume besprechen.

Definition 2.5.2 Ein *Adèle* von F/K ist eine Abbildung

$$\alpha : \left\{ \begin{array}{ccc} \mathbb{P}_F & \longrightarrow & F, \\ P & \longmapsto & \alpha_P, \end{array} \right.$$

sodass $\alpha_P \in \mathcal{O}_P$ für fast alle $P \in \mathbb{P}_F$ ist. Wir wollen ein Adèle stets als Element des direkten Produktes $\prod_{P \in \mathbb{P}_F} F$ auffassen und verwenden daher die Notation $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ oder kürzer $\alpha = (\alpha_P)$. Die Menge

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

nennen wir den *Adèleraum* von F/K und fassen sie in offensichtlicher Weise als Vektorraum über K auf.

Das *Hauptadèle* eines Elementes $x \in F$ ist das Adèle, dessen Komponenten alle gleich x sind. Nach Folgerung 2.2.10 ist diese Definition sinnvoll. Es gibt also eine Einbettung $F \hookrightarrow \mathcal{A}_F$. Die Bewertungen ν_P von F/K können in natürlicher Weise auf $\mathcal{A}_F$ fortgesetzt werden, indem wir $\nu_P(\alpha) := \nu_P(\alpha_P)$ setzen (wo α_P die P-Komponente des Adèles α bezeichnet). Nach Definition ist $\nu_P(\alpha) \geq 0$ für fast alle $P \in \mathbb{P}_F$.

Definition 2.5.3 Für $A \in \mathcal{D}_F$ definieren wir

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

Offensichtlich ist $\mathcal{A}_F(A)$ ein K-Unterraum von $\mathcal{A}_F$.

Zunächst zeigen wir eine analoge Aussage zu Hilfssatz 2.4.11, wobei anstelle des Raumes $\mathcal{L}(A)$ nun $\mathcal{A}_F(A)$ gesetzt wird.

Hilfssatz 2.5.4 *Seien $A, B \in \mathcal{D}_F$ mit $A \leq B$. Dann gilt $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$ und*

$$\dim(\mathcal{A}_F(B)/\mathcal{A}_F(A)) = \deg B - \deg A.$$

Beweis. $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$ ist trivial. Es genügt die Aussage für den Fall zu beweisen, dass $B = A + P$ mit $P \in \mathbb{P}_F$ ist. Der allgemeine Fall folgt durch vollständige Induktion. Wir wählen ein $t \in F$ mit $\nu_P(t) = \nu_P(A) + 1$ und betrachten die K-lineare Abbildung

$$\varphi : \begin{cases} \mathcal{A}_F(B) & \longrightarrow & F_P, \\ \alpha & \longmapsto & (t\alpha_P)(P). \end{cases}$$

Wegen $\nu_P(t\alpha_P) = \nu_P(t) + \nu_P(\alpha_P) = \nu_P(A) + 1 + \nu_P(\alpha_P) \geq \nu_P(A) + 1 - \nu_P(B) = 0$ ist φ wohldefiniert. Genauso einfach sieht man, dass φ surjektiv ist, und dass der Kern von φ gleich $\mathcal{A}_F(A)$ ist. Daher folgt:

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

□

Man nennt den Raum $\mathcal{A}_F(A)$ den *Adèleraum über A*. Außerdem bezeichnet man $\mathcal{A}_F(A) + F$ als den *erweiterten Adèleraum über A*. Analog zum vorigen Hilfssatz erhalten wir:

Hilfssatz 2.5.5 *Seien $A, B \in \mathcal{D}_F$ mit $A \leq B$. Dann gilt:*

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

Beweis. Wir haben eine exakte Sequenz von linearen Abbildungen

$$\begin{aligned} 0 \longrightarrow \mathcal{L}(B)/\mathcal{L}(A) &\longrightarrow \mathcal{A}_F(B)/\mathcal{A}_F(A) \longrightarrow \\ &\longrightarrow (\mathcal{A}_F(B) + F)/(\mathcal{A}_F(A) + F) \longrightarrow 0, \end{aligned} \tag{2.22}$$

wobei die Abbildungen $\sigma_1 : \mathcal{L}(B)/\mathcal{L}(A) \to \mathcal{A}_F(B)/\mathcal{A}_F(A)$ und $\sigma_2 : \mathcal{A}_F(B)/\mathcal{A}_F(A) \to (\mathcal{A}_F(B)+F)/(\mathcal{A}_F(A)+F)$ in offensichtlicher Weise definiert sind. Die einzige nicht triviale Behauptung ist, dass der Kern von σ_2 im Bild von σ_1 enthalten ist. Es sei also $\alpha \in \mathcal{A}_F(B)$ mit $\sigma_2(\alpha + \mathcal{A}_F(A)) = 0$. Dann ist $\alpha \in \mathcal{A}_F(A) + F$, und daher gibt es ein $x \in F$ mit $\alpha - x \in \mathcal{A}_F(A)$. Da $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$ ist, können wir schließen, dass $x \in \mathcal{A}_F(B) \cap F = \mathcal{L}(B)$ gilt. Daher liegt $\alpha + \mathcal{A}_F(A) = x + \mathcal{A}_F(A) = \sigma_1(x + \mathcal{L}(A))$ im Bild von σ_1.

Aus der Exaktheit der Sequenz (2.22) erhalten wir

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

wobei wir Hilfssatz 2.5.4 verwendet haben. □

Der nächste Hilfssatz stellt eine Verbindung zwischen den Räumen $\mathcal{A}_F(A)$ und $\mathcal{A}_F$ her.

Hilfssatz 2.5.6 *Falls B ein Divisor mit $\dim B = \deg B + 1 - g$ ist, dann gilt:*

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

Beweis. Zunächst haben wir nach Hilfssatz 2.4.11 für $B_1 \geq B$

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

Andererseits gilt $\dim B_1 \geq \deg B_1 + 1 - g$ nach dem Satz von Riemann 2.4.20. Daher gilt

$$\dim B_1 = \deg B_1 + 1 - g \quad \text{für jeden Divisor} \quad B_1 \geq B. \tag{2.23}$$

Die Behauptung erhält man nun folgendermaßen: Sei $\alpha \in \mathcal{A}_F$. Offensichtlich kann man einen Divisor $B_1 \geq B$ finden, sodass $\alpha \in \mathcal{A}_F(B_1)$ ist. Aus Hilfssatz 2.5.5 und (2.23) folgt

$$\begin{aligned}&\dim(\mathcal{A}_F(B_1)+F)/(\mathcal{A}_F(B)+F)\\&\quad=(\deg B_1-\dim B_1)-(\deg B-\dim B)\\&\quad=(g-1)-(g-1)=0.\end{aligned}$$

Damit gilt: $\mathcal{A}_F(B) + F = \mathcal{A}_F(B_1) + F$. Da $\alpha \in \mathcal{A}_F(B_1)$ ist, folgt, dass $\alpha \in \mathcal{A}_F(B) + F$ ist. □

Man beachte, dass die Vektorräume $\mathcal{A}_F$, $\mathcal{A}_F(A)$ und F alle unendlichdimensionale Vektorräume sind. Der nächste Satz besagt, dass der Faktorraum $\mathcal{A}_F/(\mathcal{A}_F(A) + F)$ jedoch endliche Dimension hat.

Satz 2.5.7 (Schwacher Satz von Riemann-Roch) *Für den Spezialitätsindex eines Divisors A gilt:*

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

Beweis. Aus dem Satz von Riemann 2.4.20 (b) folgt, dass ein Divisor $A_1 \geq A$

mit $\dim A_1 = \deg A_1 + 1 - g$ existiert. Nach Hilfssatz 2.5.6 ist $\mathcal{A}_F = \mathcal{A}_F(A_1) + F$, und aus Hilfssatz 2.5.2 erhalten wir daher

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

□

Diesen Satz kann man auch so formulieren: Für jedes $A \in \mathcal{D}_F$ gilt:

$$\dim A = \deg A + 1 - g + \dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)). \tag{2.24}$$

Der Spezialitätsindex von A ist also das fehlende Glied im Satz von Riemann. Dieser Satz ist eine schwache Version des Satzes von Riemann-Roch, den wir im nächsten Kapitel beweisen werden. Leider ist der Spezialitätsindex ebenfalls schwer zu ermitteln. In der starken Form des Satzes von Riemann-Roch werden wir sehen, dass man den Spezialitätsindex von A als die Dimension des Divisors $W - A$ für einen geeigneten Divisor W berechnen kann.

Als Folgerung erhalten wir eine andere Charakterisierung des Geschlechtes von F/K.

Folgerung 2.5.8 $\quad g = \dim(\mathcal{A}_F/(\mathcal{A}_F(0) + F))$.

Beweis. $i(0) = \dim(0) - \deg(0) + g - 1 = 1 - 0 + g - 1 = g$. □

Als nächstes führen wir das Konzept der Weil-Differentiale ein, welches dann zu einer weiteren Interpretation des Spezialitätsindex eines Divisors führen wird.

Definition 2.5.9 Ein *Weil-Differential* von F/K ist eine K-lineare Abbildung $\omega : \mathcal{A}_F \to K$, die auf dem erweiterten Adèleraum $\mathcal{A}_F(A) + F$ über A für einen Divisor $A \in \mathcal{D}_F$ verschwindet. Wir nennen

$$\Omega_F := \{\omega \mid \omega \text{ ist ein Weil-Differential von } F/K\}$$

den *Raum der Weil-Differentiale* von F/K. Für $A \in \mathcal{D}_F$ sei

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

der *Raum der Weil-Differentiale über* A.

Zunächst sammeln wir die folgenden, sehr einfachen Eigenschaften über Ω_F und $\Omega_F(A)$ für einen Divisor A.

Hilfssatz 2.5.10
(a) Ω_F *ist ein Vektorraum über* K.
(b) $\Omega_F(A)$ *ist ein Teilraum von* Ω_F.
(c) *Seien* $A, B \in \mathcal{D}_F$ *mit* $A \leq B$, *dann ist* $\Omega_F(B) \subseteq \Omega_F(A)$.

Beweis. (a) Angenommen ω_1 verschwindet auf $\mathcal{A}_F(A_1) + F$ und ω_2 auf $\Omega_F(A_2) + F$, dann verschwindet $\omega_1 + \omega_2$ auf $\Omega_F(A_3) + F$ für jeden Divisor A_3 mit $A_3 \leq A_1$ und $A_3 \leq A_2$. Weiters verschwindet $a\omega_1$ auf $\Omega_F(A_1) + F$ für jedes $a \in K$.
(b) Klarerweise ist $\Omega_F(A)$ ein Teilraum von Ω_F.
(c) Wenn $A \leq B$ ist, dann ist $\mathcal{A}_F(A) + F \subseteq \mathcal{A}_F(B) + F$. Daher gilt, wenn ω auf $\mathcal{A}_F(B) + F$ verschwindet, dann erst recht auf $\mathcal{A}_F(A) + F$. □

Hilfssatz 2.5.11 *Für* $A \in \mathcal{D}_F$ *gilt* $\dim \Omega_F(A) = i(A)$.

Beweis. $\Omega_F(A)$ ist in natürlicher Weise isomorph zum Raum der Linearformen auf $\mathcal{A}_F/(\mathcal{A}_F(A)+F)$. Da nach dem schwachen Satz von Riemann-Roch 2.5.7 $\dim \mathcal{A}_F/(\mathcal{A}_F(A)+F) = i(A)$ ist, folgt sofort unsere Behauptung. □

Als einfache Folgerung aus Hilfssatz 2.5.11 erhalten wir:

Folgerung 2.5.12 $\Omega_F \neq 0$.

Beweis. Wähle einen Divisor A mit Grad ≤ -2. Dann gilt nach Hilfssatz 2.5.11

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

daher ist $\Omega_F(A) \neq 0$. □

Definition 2.5.13 Für $x \in F$ und $\omega \in \Omega_F$ definieren wir $x\omega : \mathcal{A}_F \longrightarrow K$ durch

$$(xw)(\alpha) := \omega(x\alpha).$$

Klarerweise ist dadurch eine K-lineare Abbildung von $\mathcal{A}_F \longrightarrow K$ definiert. Es handelt sich dabei sogar wieder um ein Weil-Differential:

Hilfssatz 2.5.14 $x\omega$ *ist ein Weil-Differential von* F/K. *Es gilt: Falls* ω *auf* $\mathcal{A}_F(A) + F$ *verschwindet, dann verschwindet* $x\omega$ *auf* $\mathcal{A}_F(A + (x)) + F$.

Beweis. Es genügt zu zeigen, dass $x\omega$ auf $\mathcal{A}_F(A+(x))+F$ verschwindet. Sei $\beta = \alpha + y \in \mathcal{A}_F(A + (x)) + F$ mit $\alpha \in \mathcal{A}_F(A + (x))$ und $y \in F$. Dann gilt $\nu_P(\alpha) + \nu_P(x) + \nu_P(A) \geq 0$. Daraus folgt, dass $x\beta = x\alpha + xy$ mit $xy \in F$ und $x\alpha \in \mathcal{A}_F(A)$ ist. Das heißt wiederum $\omega(x\beta) = 0$, woraus man aufgrund

der Definition $(x\omega)(\beta) = \omega(x\beta) = 0$ erhält. Daher gilt die Behauptung. $\square$

Durch diese Definition bekommt Ω_F die Struktur eines Vektorraumes über F. Als nächstes wollen wir die Dimension dieses Raumes untersuchen.

Satz 2.5.15 *Ω_F ist ein ein-dimensionaler Vektorraum über F.*

Beweis. Wir wählen ein $0 \neq \omega_1 \in \Omega_F$, was nach Folgerung 2.5.12 möglich ist. Wir müssen zeigen, dass für jedes Weil-Differential $\omega_2 \in \Omega_F$ ein $z \in F$ existiert, mit $\omega_2 = z\omega_1$. Wir können annehmen, es gelte $\omega_2 \neq 0$. Zunächst wählen wir Divisoren $A_1, A_2 \in \mathcal{D}_F$, sodass $\omega_1 \in \Omega_F(A_1)$ und $\omega_2 \in \Omega_F(A_2)$ ist. Für einen Divisor B (den wir später noch genauer spezifizieren werden) betrachten wir die K-linearen injektiven Abbildungen

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

Zuerst zeigen wir eine Behauptung:

Behauptung: Für eine geeignete Wahl von B gilt:

$$\varphi_1(\mathcal{L}(A_1 + B)) \cap \varphi_2(\mathcal{L}(A_2 + B)) \neq \{0\}.$$

Für den Beweis verwenden wir eine einfache, bekannte Tatsache aus der linearen Algebra (siehe z.B. [8]): U_1, U_2 seien Teilräume eines endlichdimensionalen Vektorraumes V, dann gilt:

$$\dim(U_1 \cap U_2) \geq \dim U_1 + \dim U_2 - \dim V. \tag{2.25}$$

Sei jetzt $B > 0$ ein Divisor mit genügend großem Grad, sodass

$$\dim(A_i + B) = \deg(A_i + B) + 1 - g$$

für $i = 1, 2$ ist. Das geht nach dem Satz von Riemann 2.4.20. Sei $U_i := \varphi_i(\mathcal{L}(A_i + B)) \subseteq \Omega_F(-B)$. Da

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

ist, erhalten wir

$$\begin{aligned} &\dim U_1 + \dim U_2 - \dim \Omega_F(-B) \\ &= \deg(A_1 + B) + 1 - g + \deg(A_2 + B) + 1 - g - (\deg B + g - 1) \\ &= \deg B + (\deg A_1 + \deg A_2 + 3(1 - g)). \end{aligned}$$

Der geklammerte Term ist unabhängig von B, daher ist

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

wenn $\deg B$ genügend groß ist. Mit (2.25) folgt $U_1 \cap U_2 \neq \{0\}$, was unsere Behauptung zeigt.

Der Rest des Beweises folgt jetzt sehr schnell: Wähle $x_1 \in \mathcal{L}(A_1 + B)$ und $x_2 \in \mathcal{L}(A_2 + B)$, sodass $x_1\omega_1 = x_2\omega_2 \neq 0$ ist. Dann ist $\omega_2 = (x_1 x_2^{-1})\omega_1$, was zu zeigen war. □

Als nächstes wollen wir jedem Weil-Differential $\omega \neq 0$ einen Divisor zuordnen. Dazu betrachten wir die folgende Menge von Divisoren

$$M(\omega) := \{A \in \mathcal{D}_F \mid \omega \text{ verschwindet auf } \mathcal{A}_F(A) + F\}. \tag{2.26}$$

Hilfssatz 2.5.16 *Sei $0 \neq \omega \in \Omega_F$. Dann gibt es einen eindeutig bestimmten Divisor $W \in M(\omega)$, für den $A \leq W$ für jedes $A \in M(\omega)$ gilt.*

Beweis. Nach dem Satz von Riemann 2.4.20 gibt es eine Konstante c, die nur vom Funktionenkörper F/K abhängt, mit der Eigenschaft: $i(A) = 0$, für alle $A \in \mathcal{D}_F$ mit Grad $\geq c$. Da nach dem schwachen Satz von Riemann-Roch 2.5.7 $\dim(\mathcal{A}_F/(\mathcal{A}_F(A) + F)) = i(A)$ ist, erhalten wir, dass $\deg A < c$ ist für alle $A \in M(\omega)$. Daher gibt es einen Divisor $W \in M(\omega)$ mit maximalem Grad.
Angenommen W habe nicht die gewünschte Eigenschaft. Dann gibt es einen Divisor $A_0 \in M(\omega)$ mit $A_0 \not\leq W$, das heißt $\nu_Q(A_0) > \nu_Q(W)$ für ein $Q \in \mathbb{P}_F$. Wir behaupten, es sei

$$W + Q \in M(\omega), \tag{2.27}$$

was ein Widerspruch zur Maximalität von W ist. Um diese Behauptung zu zeigen betrachten wir ein Adèle $\alpha = (\alpha_P) \in \mathcal{A}_F(W + Q)$. Wir können $\alpha = \alpha' + \alpha''$ schreiben mit

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

Dann ist $\alpha' \in \mathcal{A}_F(W)$ und $\alpha'' \in \mathcal{A}_F(A_0)$, daher gilt $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$. ω verschwindet also auf $\mathcal{A}_F(W + Q) + F$, und (2.27) ist damit bewiesen. Die Eindeutigkeit von W ist offensichtlich. □

Die folgende Definition ist jetzt nach dem Hilfssatz 2.5.16 sinnvoll.

Definition 2.5.17
(a) Der *Divisor* (ω) eines Weil-Differentiales $\omega \neq 0$ ist der eindeutig bestimmte Divisor von F/K, der die folgenden Eigenschaften erfüllt:
(1) ω verschwindet auf $\mathcal{A}_F((\omega)) + F$.
(2) Falls ω auf $\mathcal{A}_F(A) + F$ verschwindet, dann ist $A \leq (\omega)$.
(b) Für $0 \neq \omega \in \Omega_F$ und $P \in \mathbb{P}_F$ definieren wir $\nu_P(\omega) := \nu_P((\omega))$.

(c) Eine Stelle P heißt *Nullstelle* (bzw. *Pol*) von $\omega \neq 0$, falls $\nu_P(\omega) > 0$ (bzw. $\nu_P(\omega) < 0$) ist. $\omega \neq 0$ heißt *regulär bei* P, wenn $\nu_P(\omega) \geq 0$ ist, und ω heißt *regulär* (oder *holomorph*), wenn ω regulär ist für alle $P \in \mathbb{P}_F$.

Als unmittelbare Konsequenz aus diesen Definitionen erhalten wir

$$\Omega_F(A) = \{\omega \in \Omega_F \,|\, \omega = 0 \text{ oder } (\omega) \geq A\} \tag{2.28}$$

und

$$\Omega_F(0) = \{\omega \in \Omega_F \,|\, \omega \text{ ist regulär}\}.$$

Als Folgerung aus Definition 2.5.1 und Hilfssatz 2.5.11 ergibt sich

$$\dim \Omega_F(0) = g.$$

Bis jetzt haben wir die sogenannte *Diagonaleinbettung* $F \hookrightarrow \mathcal{A}_F$ betrachtet, die jedem $x \in F$ das dazugehörige Hauptadèle zuordnet. Es gibt aber noch andere Möglichkeiten F in den Raum der Adèle einzubetten. Wir wollen jetzt, für jede Stelle $P \in \mathbb{P}_F$ eine andere Einbettung $\iota_P : F \hookrightarrow \mathcal{A}_F$ betrachten.

Definition 2.5.18 Sei $P \in \mathbb{P}_F$.
(a) Für $x \in F$ sei $\iota_P(x) \in \mathcal{A}_F$ das Adèle, dessen P-Komponente x ist, und dessen andere Komponenten alle 0 sind.
(b) Für ein Weil-Differential $\omega \in \Omega_F$ definieren wir seine *lokale Komponente* $\omega_P : F \longrightarrow K$ durch

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

Klarerweise ist ω_P eine K-lineare Abbildung.

Satz 2.5.19 *Sei $\omega \in \Omega_F$ und $\alpha = (\alpha_P) \in \mathcal{A}_F$. Dann ist $\omega_P(\alpha_P) \neq 0$ für höchstens endlich viele Stellen P und es gilt*

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

Insbesondere gilt:

$$\sum_{P \in \mathbb{P}_F} \omega_P(1) = 0. \tag{2.29}$$

Beweis. Wir können $\omega \neq 0$ annehmen und wir setzen $W := (\omega)$ gleich dem Divisor von ω. Es gibt eine endliche Menge $S \subseteq \mathbb{P}_F$, sodass

$$\nu_P(W) = 0 \quad \text{und} \quad \nu_P(\alpha_P) \geq 0 \quad \text{für alle} \quad P \notin S.$$

Definieren wir $\beta = (\beta_P) \in \mathcal{A}_F$ durch

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

Dann ist $\beta \in \mathcal{A}_F(W)$ und $\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P)$, daher haben wir $\omega(\beta) = 0$ und schließlich

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

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 jede seiner lokalen Komponenten eindeutig bestimmt wird.

Satz 2.5.20
(a) *Sei $\omega \neq 0$ ein Weil-Differential von F/K und $P \in \mathbb{P}_F$. Dann gilt*

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

Insbesondere ist $\omega_P \neq 0$.
(b) *Falls $\omega, \omega' \in \Omega_F$ gegeben sind und $\omega_P = \omega'_P$ für ein $P \in \mathbb{P}_F$ gilt, dann folgt $\omega = \omega'$.*

Beweis. (a) Zur Erinnerung, es gilt laut Definition $\nu_P(\omega) = \nu_P(W)$, wobei $W = (\omega)$ den Divisor von ω bezeichnet. Sei $s := \nu_P(\omega)$. Für $x \in F$ mit $\nu_P(x) \geq -s$ erhalten wir $\iota_P(x) \in \mathcal{A}_F(W)$, daher gilt $\omega_P(x) = \omega(\iota_P(x)) = 0$. Wir nehmen jetzt an, dass $\omega_P(x) = 0$ ist, für jedes $x \in F$ mit $\nu_P(x) \geq -s-1$. 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 $\nu_P(\alpha_P) \geq -s - 1$. Daher ist

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

Aus diesem Grund verschwindet ω auf $\mathcal{A}_F(W + P)$, was ein Widerspruch zur Definition von W ist.
(b) Falls $\omega_P = \omega'_P$ gilt, dann ist $(\omega - \omega')_P = 0$, und daher nach (a) $\omega - \omega' = 0$.
□

2.6 Der Satz von Riemann-Roch und Anwendungen

In diesem Abschnitt wollen wir den Satz von Riemann-Roch zeigen, der wohl einer der wichtigsten Sätze in der Theorie der algebraischen Funktionenkörper ist. Der Schlüssel zu seinem Beweis liegt in der Betrachtung von

Divisoren, die von Weil-Differentialen kommen.

Definition 2.6.1 Ein Divisor W heißt ein *kanonischer Divisor* von F/K, wenn $W = (\omega)$ für ein $\omega \in \Omega_F$ ist.

Satz 2.6.2
(a) *Für* $0 \neq x \in F$ *und* $0 \neq \omega \in \Omega_F$ *gilt:* $(x\omega) = (x) + (\omega)$.
(b) *Je zwei kanonische Divisoren von* F/K *sind äquivalent.*

Beweis. Falls ω auf $\mathcal{A}_F(A) + F$ verschwindet, dann verschwindet $x\omega$ nach Hilfssatz 2.5.14 auf $\mathcal{A}_F(A + (x)) + F$, daher ist

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

Genauso sieht man $(x\omega) + (x^{-1}) \leq (x^{-1}x\omega) = (\omega)$. Die Kombination dieser beiden Unlgeichungen ergibt:

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

Das zeigt (a). Die Aussage (b) folgt aus (a) und aus Satz 2.5.15. □

Eine einfache Folgerung aus diesem Satz lautet: Die kanonischen Divisoren von F/K bilden eine ganze Klasse der Divisorenklassengruppe $\mathcal{C}_F$. Diese Divisorenklasse nennt man die *kanonische Klasse* von F/K.

Der entscheidende Schritt zum Beweis des Satzes von Riemann-Roch ist der folgende Satz. Das wichtigste Resultat für den Beweis ist der Satz 2.5.15.

Satz 2.6.3 *Sei* A *ein beliebiger Divisor, und* $W = (\omega)$ *ein kanonischer Divisor von* F/K. *Dann ist die Abbildung*

$$\mu : \left\{ \begin{array}{ccc} \mathcal{L}(W - A) & \longrightarrow & \Omega_F(A), \\ x & \longmapsto & x\omega \end{array} \right.$$

ein Isomorphismus zwischen K*-Vektorräumen. Insbesondere gilt:*

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

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

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

daher ist nach (2.28) $x\omega \in \Omega_F(A)$. Die Abbildung μ bildet also $\mathcal{L}(W - A)$ in $\Omega_F(A)$ ab. Klarerweise ist μ linear und injektiv. Um zu zeigen, dass μ

auch surjektiv ist, betrachten wir ein Weil-Differential $\omega_1 \in \Omega_F(A)$. Nach Satz 2.5.15 gilt $w_1 = x\omega$ für ein $x \in F$. Da

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

ist, erhalten wir $(x) \geq -(W - A)$, daher ist $x \in \mathcal{L}(W - A)$ und $\omega_1 = \mu(x)$. Wir haben gezeigt, dass $\dim \Omega_F(A) = \dim(W - A)$ ist. Da nach Hilfssatz 2.5.11 $\dim \Omega_F(A) = i(A)$ ist, folgt $i(A) = \dim(W - A)$. □

Die Zusammenfassung aller erhaltenen Resultate liefert den Satz von Riemann-Roch.

Satz 2.6.4 (Satz von Riemann-Roch) *Sei W ein kanonischer Divisor von F/K. Dann gilt für jedes $A \in \mathcal{D}_F$*

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

Beweis. Unmittelbare Folgerung aus Satz 2.6.3 und der Definition 2.5.1 von $i(A)$. □

Folgerung 2.6.5 *Für einen kanonischen Divisor W gilt*

$$\deg W = 2g - 2 \quad \textit{und} \quad \dim W = g.$$

Beweis. Für $A = 0$ folgt aus dem Satz von Riemann-Roch 2.6.4 und Hilfssatz 2.4.10

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

Daher ist $\dim W = g$. Wenn wir $A = W$ setzen, erhalten wir

$$g = \dim W = \deg W + 1 - g + \dim(W - W) = \deg W + 2 - g.$$

Es folgt $\deg W = 2g - 2$. □

Aus dem Satz von Riemann 2.4.20 wissen wir bereits, dass es eine Konstante c gibt, sodass $i(A) = 0$, wann immer $\deg A \geq c$ gilt. Wir können nun eine genauere Beschreibung geben, wie diese Konstante zu wählen ist.

Satz 2.6.6 *Wenn A ein Divisor von F/K vom Grad $\geq 2g - 1$ ist, dann gilt*

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

Beweis. Wir wissen $\dim A = \deg A + 1 - g + \dim(W - A)$, wobei W ein kanonischer Divisor ist. Da $\deg A \geq 2g - 1$ und $\deg W = 2g - 2$ gilt, folgt

$\deg(W - A) < 0$. Aus Folgerung 2.4.15 erhalten wir $\dim(W - A) = 0$. $\square$

Man beachte, dass die Schranke $2g - 1$ im letzten Satz bestmöglich ist, da für einen kanonischen Divisor W nach Folgerung 2.6.5

$$\dim W > \deg W + 1 - g$$

gilt.

Wir können jetzt den Satz von Riemann-Roch 2.6.4 so formulieren, wie wir ihn später stets brauchen werden (wir werden trotzdem stets auf den Satz 2.6.4 verweisen):
Für jeden Divisor $A \in \mathcal{D}_F$ gilt

$$\dim A \geq \deg A + 1 - g,$$

mit Gleichheit, wenn $\deg A \geq 2g - 1$ ist.

Wir wollen jetzt noch einige Anwendungen des Satzes von Riemann-Roch 2.6.4 diskutieren. Unser erstes Ziel ist zu zeigen, dass wir mit Hilfe des Satzes von Riemann-Roch 2.6.4 sowohl das Geschlecht, als auch die kanonische Klasse von F/K charakterisieren können.

Satz 2.6.7 *Angenommen $g_0 \in \mathbb{Z}$ und $W_0 \in \mathcal{D}_F$ erfüllen*

$$\dim A = \deg A + 1 - g_0 + \dim(W_0 - A) \tag{2.30}$$

für jedes $A \in \mathcal{D}_F$. Dann ist $g_0 = g$ und W_0 ein kanonischer Divisor.

Beweis. Indem wir $A = 0$ bzw. $A = W_0$ in (2.30) setzen, erhalten wir so wie im Beweis von Folgerung 2.6.5 $\dim W_0 = g_0$ und $\deg W_0 = 2g_0 - 2$. Sei W ein kanonischer Divisor von F/K. Wir wählen einen Divisor A mit $\deg A > \max\{2g-2, 2g_0-2\}$. Dann ist nach Satz 2.6.6 $\dim A = \deg A + 1 - g$ und nach (2.30) $\dim A = \deg A + 1 - g_0$. Daher gilt $g = g_0$.
Wenn wir $A = W$ in (2.30) substituieren, erhalten wir

$$g = (2g - 2) + 1 - g + \dim(W_0 - W).$$

Daher ist $\dim(W_0 - W) = 1$. Da $\deg(W_0 - W) = 0$ ist, folgt nach Hilfssatz 2.4.15 $W_0 - W$ ist ein Hauptdivisor, und daher gilt $W_0 \sim W$. $\square$

Eine nützliche Charakterisierung der Klasse der kanonischen Divisoren ist die Folgende:

Satz 2.6.8 *Ein Divisor B ist kanonisch, dann und nur dann, wenn* $\deg B = 2g - 2$ *und* $\dim B \geq g$ *ist.*

Beweis. Man nehme an, dass $\deg B = 2g-2$ und $\dim B \geq g$ ist, und wähle einen kanonischen Divisor W. Dann gilt

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

Daher gilt $\dim(W-B) \geq 1$. Da $\deg(W-B) = 0$ ist, impliziert die Folgerung 2.4.15 $W \sim B$ und damit die Behauptung. □

Die nächste Anwendung ist eine Verschärfung des schwachen Approximationssatzes 2.2.7.

Satz 2.6.9 (Starker Approximationssatz) *Sei $S \subsetneq \mathbb{P}_F$ eine echte Teilmenge von $\mathbb{P}_F$ und $P_1, \ldots, P_r \in S$ paarweise verschiedene Stellen von F/K. Es seien die Elemente $x_1, \ldots, x_r \in F$ und $n_1, \ldots, n_r \in \mathbb{Z}$ gegeben. Dann gibt es ein Element $x \in F$, sodass*

$$\nu_{P_i}(x - x_i) = n_i \quad (i = 1, \ldots, r), \quad \textit{und}$$

$$\nu_P(x) \geq 0 \quad \textit{für alle} \quad P \in S \backslash \{P_1, \ldots, P_r\}.$$

Beweis. Betrachte das Adèle $\alpha = (\alpha_P)_{P \in \mathbb{P}_F}$ mit

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

Wähle eine Stelle $Q \in \mathbb{P}_F \backslash S$. Für genügend großes $m \in \mathbb{N}$ erhalten wir mit dem schwachen Satz von Riemann-Roch 2.5.7 in Kombination mit Satz 2.6.6

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

Daher gibt es ein Element $z \in F$ mit $z - \alpha \in \mathcal{A}_F(mQ - \sum_{i=1}^{r}(n_i+1)P_i)$. Das bedeutet

$$\nu_{P_i}(z - x_i) > n_i \quad \text{für} \quad i = 1, \ldots, r, \tag{2.31}$$

$$\nu_P(z) \geq 0 \quad \text{für} \quad P \in S \backslash \{P_1, \ldots, P_r\}. \tag{2.32}$$

Wir wählen jetzt $y_1, \ldots, y_r \in F$ mit $\nu_{P_i}(y_i) = n_i$. In derselben Weise wie oben, konstruieren wir ein $y \in F$ mit

$$\nu_{P_i}(y - y_i) > n_i \quad \text{für} \quad i = 1, \ldots, r, \tag{2.33}$$

$$\nu_P(y) \geq 0 \quad \text{für} \quad P \in S \backslash \{P_1, \ldots, P_r\}. \tag{2.34}$$

Wir haben also für $i = 1, \ldots, r$

$$\nu_{P_i}(y) = \nu_{P_i}((y - y_i) + y_i) = n_i \tag{2.35}$$

aufgrund (2.33) und der strikten Dreiecksungleichung 2.2.2. Setzen wir $x := y + z$, dann erhalten wir mit (2.35)

$$\nu_{P_i}(x - x_i) = \nu_{P_i}(y + (z - x_i)) = n_i \quad (i = 1, \ldots, r).$$

Für $P \in S \backslash \{P_1, \ldots, P_r\}$ gilt nach (2.32) und (2.34) $\nu_P(x) = \nu_P(y+z) \geq 0$. □

Als Beispiel berechnen wir einen kanonischen Divisor im rationalen Funktionenkörper $K(x)$.

Satz 2.6.10 *Für den rationalen Funktionenkörper $F = K(x)$ gelten die folgenden Aussagen:*
(a) *Der Divisor $-2P_\infty$ ist kanonisch.*
(b) *Es gibt ein eindeutiges Weil-Differential $\eta \in \Omega_{K(x)}$ mit $(\eta) = -2P_\infty$ und $\eta_{P_\infty}(x^{-1}) = -1$.*
(c) *Die lokalen Komponenten η_{P_∞} bzw. η_{P_a} des obigen Weil-Differentials η erfüllen:*

$$\eta_{P_\infty}((x-a)^n) = \begin{cases} 0 & \text{für} \quad n \neq -1, \\ -1 & \text{für} \quad n = -1, \end{cases}$$

$$\eta_{P_a}((x-a)^n) = \begin{cases} 0 & \text{für} \quad n \neq -1, \\ 1 & \text{für} \quad n = -1. \end{cases}$$

Beweis. (a) $\deg(-2P_\infty) = -2 = 2g - 2 < 0$, daher ist $\dim(-2P_\infty) = 0 = g$, und damit ist $-2P_\infty$ nach Satz 2.6.8 kanonisch.
(b) Wähle ein Weil-Differential ω mit Divisor $(\omega) = -2P_\infty$. Dann verschwindet ω auf dem Raum $\mathcal{A}_{K(x)}(-2P_\infty)$ und ω verschwindet nicht identisch auf $\mathcal{A}_{K(x)}(-P_\infty)$. Nach Hilfssatz 2.5.4 ist

$$\dim \mathcal{A}_{K(x)}(-P_\infty)/\mathcal{A}_{K(x)}(-2P_\infty) = 1.$$

Außerdem gilt

$$\iota_{P_\infty}(x^{-1}) \in \mathcal{A}_{K(x)}(-P_\infty) \backslash \mathcal{A}_{K(x)}(-2P_\infty).$$

Mit den letzten beiden Formeln können wir schließen, dass

$$\omega_{P_\infty}(x^{-1}) = \omega(\iota_{P_\infty}(x^{-1})) =: c \neq 0.$$

Wir setzen $\eta := c^{-1}\omega$ und erhalten $(\eta) = -2P_\infty$ und $\eta_{P_\infty}(x^{-1}) = -1$.
Die Eindeutigkeit von η erhalten wir folgendermaßen: Falls η^* dieselben Eigenschaften wie η hat, dann verschwindet $\eta - \eta^*$ auf dem Raum $\mathcal{A}_{K(x)}(-P_\infty)$. Wegen $\deg -P_\infty = -1 = 2g - 1$ folgt aus Satz 2.6.6 und Hilfssatz 2.5.6 $\mathcal{A}_{K(x)}(-P_\infty) + K(x) = \mathcal{A}_{K(x)}$. Dies hat $\eta - \eta^* = 0$ zur Folge.
(c) Da Weil-Differentiale auf Hauptadèlen verschwinden, gilt nach Satz 2.5.19

$$0 = \eta((x-a)^n) = \sum_{P \in \mathbb{P}_{K(x)}} \eta_P((x-a)^n). \tag{2.36}$$

Für $P \neq P_\infty$ und $P \neq P_a$ ist $\nu_P((x-a)^n) = 0$, daher folgt nach Satz 2.5.20 $\eta_P((x-a)^n) = 0$ und (2.36) impliziert

$$\eta_{P_\infty}((x-a)^n) + \eta_{P_a}((x-a)^n) = 0. \tag{2.37}$$

Im Fall $n \leq -2$, erhalten wir $\nu_{P_\infty}((x-a)^n) \geq 2 = -\nu_{P_\infty}(\eta)$, daher ist nach Satz 2.5.20 $\eta_{P_\infty}((x-a)^n) = 0$ und (2.37) hat zur Folge, dass auch $\eta_{P_a}((x-a)^n) = 0$ ist. Im Fall $n \geq 0$, gilt nach Satz 2.5.20 $\eta_{P_a}((x-a)^n) = 0 = -\nu_{P_a}(\eta)$ und wir erhalten das Ergebnis für $\eta_{P_\infty}((x-a)^n)$ wieder durch (2.37).
Zum Schluss betrachten wir den Fall $n = -1$. Da

$$\frac{1}{x-a} = \frac{a}{x(x-a)} + \frac{1}{x} \text{ und } \iota_{P_\infty}\left(\frac{a}{x(x-a)}\right) \in \mathcal{A}_{K(x)}(-2P_\infty),$$

sehen wir, dass $\eta_{P_\infty}((x-a)^{-1}) = \eta_{P_\infty}(x^{-1}) = -1$ nach Definition von η gilt und aus (2.37) folgt, dass $\eta_{P_a}((x-a)^{-1}) = 1$ ist. □

Für einen Divisor A mit Grad < 0 gilt $\dim A = 0$ nach Hilfssatz 2.4.10. Andererseits gilt nach Satz 2.6.6, dass $\dim A = \deg A + 1 - g$ ist, falls $\deg A > 2g - 2$. Die Dimension von A hängt in diesen Fällen also nur von $\deg A$ (und dem Geschlecht) ab. Im Fall $0 \leq \deg A \leq 2g-2$, ist die Situation komplizierter, aber trotzdem kann man allgemeine Resultate ableiten. Wir führen zunächst eine Bezeichnung für Divisoren mit Spezialitätsindex 0 ein.

Definition 2.6.11 Ein Divisor $A \in \mathcal{D}_F$ heißt *nicht speziell*, wenn $i(A) = 0$ ist, und sonst wird A *speziell* genannt.

Wir sammeln einige Eigenschaften, die sofort aus dieser Definition folgen:

Hilfssatz 2.6.12 *Sei $A \in \mathbb{P}_F$.*
(a) *A ist nicht speziell* $\iff \dim A = \deg A + 1 - g$.
(b) $\deg A > 2g - 2 \Rightarrow$ *A ist nicht speziell.*
(c) *Die Eigenschaft eines Divisors A speziell oder nicht speziell zu sein, hängt nur von der Klasse $[A]$ von A in der Divisorklassengruppe ab.*
(d) *Kanonische Divisoren sind speziell.*
(e) *Jeder Divisor A mit $\dim A > 0$ und $\deg A < g$ ist speziell.*
(f) *Falls A nicht speziell ist und $B \geq A$, dann ist auch B nicht speziell.*

Beweis. (a) ist klar aufgrund der Definition von $i(A)$, (b) ist Satz 2.6.6 und (c) folgt aus der Tatsache, dass $\dim A$ und $\deg A$ nur von der Divisorklasse $[A]$ abhängen.
(d) Für einen kanonischen Divisor W haben wir $i(W) = \dim(W - W) = 1$ nach Satz 2.6.3, daher ist W speziell.
(e) $1 \leq \dim A = \deg A + 1 - g + i(A) \Rightarrow i(A) \geq g - \deg A > 0$, da $\deg A < g$

ist. Daher ist A speziell.
(f) Nach dem schwachen Satz von Riemann-Roch 2.5.7 ist A nicht speziell $\Leftrightarrow \mathcal{A}_F = \mathcal{A}_F(A) + F$. Falls $B \geq A$, dann ist $\mathcal{A}_F(A) \subseteq \mathcal{A}_F(B)$ nach Hilfssatz 2.5.4 und daher folgt die Aussage. □

Satz 2.6.13 *Angenommen $T \subseteq \mathbb{P}_F$ sei eine Menge von Stellen vom Grad eins, sodass $|T| \geq g$. Dann gibt es einen nicht speziellen Divisor $B \geq 0$ mit* $\deg B = g$ *und* $\operatorname{supp} B \subseteq T$.

Beweis. Der wesentliche Schritt im Beweis besteht darin, die folgende Behauptung zu zeigen:

> Gegeben seien g verschiedene Stellen $P_1, \ldots, P_g \in T$ und ein Divisor $A \geq 0$ mit $\dim A = 1$ und $\deg A \leq g - 1$. Dann gibt es einen Index $j \in \{1, \ldots, g\}$, sodass $\dim(A + P_j) = 1$ ist.

Angenommen diese Behauptung sei falsch. Dann ist $\dim(A + P_j) > 1$ und es gibt Elemente $z_j \in \mathcal{L}(A + P_j) \backslash \mathcal{L}(A)$ für $j = 1, \ldots, g$. Da

$$\nu_{P_j}(z_j) = -\nu_{P_j}(A) - 1 \quad \text{und} \quad \nu_{P_i}(z_j) \geq -\nu_{P_i}(A) \quad \text{für} \quad i \neq j,$$

folgt mit der strikten Dreiecksungleichung 2.2.2, dass die $g + 1$ Elemente $1, z_1, \ldots, z_g$ linear unabhängig über K sind. Wähle einen Divisor $D \geq A + P_1 + \cdots + P_g$ mit $\deg D = 2g - 1$. Dann sind $1, z_1, \ldots, z_g \in \mathcal{L}(D)$, daher ist $\dim D \geq g + 1$. Andererseits ist $\dim D = \deg D + 1 - g = g$ nach dem Satz von Riemann-Roch 2.6.4. Das ist ein Widerspruch.
Aufgrund dieser Behauptung finden wir Divisoren $0 < P_{i_1} < P_{i_1} + P_{i_2} < \ldots < P_{i_1} + P_{i_2} + \cdots + P_{i_g} =: B$ (mit $i_\nu \in \{1, \ldots, g\}$), sodass $\dim(P_{i_1} + \cdots + P_{i_j}) = 1$ ist für $j = 1, \ldots, g$. Insbesondere ist daher $\dim B = 1$. Der Divisor B ist nicht speziell, da

$$\deg B + 1 - g = g + 1 - g = 1 = \dim B$$

aufgrund Hilfssatz 2.6.12 (a). □

Das einzige Beispiel eines algebraischen Funktionenkörpers, das wir kennengelernt haben, ist der rationale Funktionenkörper, und der ist aus algebraischer Sicht ein Trivialbeispiel. Häufig hat ein nicht rationaler Funktionenkörper F/K für ein irreduzibles Polynom $\varphi(T) \in K(x)[T]$ eine Darstellung der Form

$$F = K(x, y) \quad \text{mit} \quad \varphi(y) = 0.$$

Damit kann F als eine endliche algebraische Erweiterung des rationalen Funktionenkörpers $K(x)$ aufgefasst werden. Viele Probleme liegen dabei auf der Hand:

- Ist K der volle Konstantenkörper von F?

- Berechne das Geschlecht von F.
- Beschreibe die Stellen von F explizit. Wie sehen insbesondere die rationalen Stellen aus?
- Konstruiere eine Basis des Raumes $\mathcal{L}(G)$, zumindest in Spezialfällen.

Diese Probleme zu beantworten ist das Hauptziel der Theorie der algebraischen Funktionenkörper. Wir werden uns damit hier nicht beschäftigen. Eine ausführliche Behandlung dieser Probleme findet man in [19] und [18].

2.7 Die P-adische Vervollständigung

In diesem Kapitel wollen wir einen bewertungstheoretischen Aspekt ins Spiel bringen. Wir werden die Vervollständigung eines Funktionenkörpers F/K bezüglich einer Stelle $P \in \mathbb{P}_F$ betrachten. Zunächst verallgemeinern wir Definition 2.2.1 auf einen beliebigen Körper.

Definition 2.7.1 Eine *diskrete Bewertung* eines Körper T ist eine surjektive Abbildung $\nu : T \longrightarrow \mathbb{Z} \cup \{\infty\}$, die folgende Bedingungen erfüllt:
(1) $\nu(x) = \infty \iff x = 0$.
(2) $\nu(xy) = \nu(x) + \nu(y)$ für alle $x, y \in T$.
(3) $\nu(x + y) \geq \min\{\nu(x), \nu(y)\}$ für alle $x, y \in T$ (Dreiecksungleichung).
Das Paar (T, ν) nennt man einen *bewerteten Körper*.

Wie in Hilfssatz 2.2.2 kann man leicht zeigen, dass die strikte Dreiecksungleichung

$$\nu(x + y) = \min\{\nu(x), \nu(y)\} \quad \text{falls } x, y \in T \text{ und } \nu(x) \neq \nu(y)$$

auch hier gilt.

Definition 2.7.2 Sei (T, ν) ein bewerteter Körper. Wir sagen, die Folge $(x_n)_{n \geq 0}$ *konvergiert* in T, falls ein Element $x \in T$ (genannt der *Grenzwert* der Folge) existiert, mit

$$\forall c \in \mathbb{R} \ \exists n_0 \in \mathbb{N} : \nu(x - x_n) \geq c \ \ \forall n \geq n_0.$$

Eine Folge $(x_n)_{n \geq 0}$ heißt eine *Cauchy Folge*, wenn sie die folgende Eigenschaft hat:

$$\forall c \in \mathbb{R} \ \exists n_0 \in \mathbb{N} : \nu(x_n - x_m) \geq c \ \ \forall n, m \geq n_0.$$

Wie in der reellen Analysis zeigt man:

(a) Sei $(x_n)_{n\geq 0}$ eine konvergente Folge in T. Dann ist sein Grenzwert $x \in T$ eindeutig bestimmt. Daher schreiben wir: $x = \lim_{n\to\infty} x_n$.
(b) Jede konvergente Folge ist eine Cauchy Folge.

Bekanntlich gilt im Allgemeinen die Umkehrung der letzten Aussage nicht. Wir führen die folgende Notation ein.

Definition 2.7.3
(a) Ein bewerteter Körper (T, ν) heißt *vollständig*, wenn jede Cauchy Folge in T konvergent ist.
(b) Sei (T, ν) ein bewerteter Köper. Die *Vervollständigung* von T ist ein bewerteter Körper $(\hat{T}, \hat{\nu})$ mit den folgenden Eigenschaften:
   (1) $T \subseteq \hat{T}$ und ν ist die Einschränkung von $\hat{\nu}$ auf T.
   (2) $(\hat{T}, \hat{\nu})$ ist vollständig.
   (3) T ist dicht in $\hat{T}$, das heißt für jedes $z \in \hat{T}$ gibt es eine Folge $(x_n)_{n\geq 0}$ in T mit $\lim_{n\to\infty} x_n = z$.

Ohne Beweis führen wir den folgenden Satz an:

Satz 2.7.4 (Vervollständigungssatz) *Für jeden bewerteten Körper (T, ν) gibt es eine Vervollständigung $(\hat{T}, \hat{\nu})$. Sie ist eindeutig im folgenden Sinne: Falls $(\tilde{T}, \tilde{\nu})$ eine andere Vervollständigung von (T, ν) ist, dann gibt es einen eindeutigen Isomorphismus $f : \hat{T} \to \tilde{T}$, sodass $\hat{\nu} = \tilde{\nu} \circ f$. Daher nennen wir $(\hat{T}, \hat{\nu})$ die Vervollständigung von (T, ν).*

Beweis. Einen Beweis findet man z. B. in [19]. □

Häufig ist es zweckmäßiger konvergente Reihen anstatt Folgen zu betrachten. Sei $(z_n)_{n\geq 0}$ eine Folge in einem bewerteten Körper (T, ν) und $s_m := \sum_{i=0}^{m} z_i$. Wir sagen, die unendliche Reihe $\sum_{i=0}^{\infty} z_i$ ist konvergent, wenn die Folge der Paritalsummen $(s_m)_{m\geq 0}$ konvergiert. In diesem Fall schreiben wir, wie üblich,

$$\sum_{i=0}^{\infty} z_i := \lim_{m\to\infty} s_m.$$

In einem vollständigen bewerteten Körper gibt es ein sehr einfaches Kriterium für die Konvergenz einer unendlichen Reihe.

Hilfssatz 2.7.5 *Sei $(z_n)_{n\geq 0}$ eine Folge in einem vollständigen, bewerteten Körper (T, ν). Dann gilt: Die unendliche Reihe $\sum_{i=0}^{\infty} z_i$ ist konvergent, dann und nur dann, wenn die Folge $(z_n)_{n\geq 0}$ gegen 0 konvergiert.*

Beweis. Angenommen $(z_n)_{n\geq 0}$ konvergiert gegen 0. Betrachte die m-te Pa-

rialsumme $s_m := \sum_{i=0}^{m} z_i$. Für $n > m$ ist

$$\nu(s_n - s_m) = \nu\left(\sum_{i=m+1}^{n} z_i\right) \geq \min\{\nu(z_i) \,|\, m < i \leq n\} \geq \min\{\nu(z_i) \,|\, i > m\}.$$

$\nu(z_i) \to \infty$ für $i \to \infty$ impliziert, dass die Folge $(s_n)_{n\geq 0}$ eine Cauchy Folge in T und damit konvergent ist.
Die umgekehrte Richtung zeigt man genauso wie in der Analysis. □

Wir spezialisieren diese Resultate jetzt auf den Fall eines algebraischen Funktionenkörpers F/K.

Definition 2.7.6 Sei P eine Stelle von F/K. Die Vervollständigung von F bezüglich der Bewertung ν_P nennen wir die *P-adische Vervollständigung* von F. Wir bezeichnen diese Vervollständigung mit $\hat{F}_P$ und die Bewertung von $\hat{F}_P$ wieder mit ν_P.

Es gilt jetzt der folgende Satz.

Satz 2.7.7 *Sei $P \in \mathbb{P}_F$ eine rationale Stelle und $t \in F$ ein P-primes Element. Dann hat jedes Element $z \in \hat{F}_P$ eine eindeutige Darstellung der Form*

$$z = \sum_{i=n}^{\infty} a_i t^i \quad \textit{mit} \quad \nu_P(z) \geq n \in \mathbb{Z} \quad \textit{und} \quad a_i \in K. \tag{2.38}$$

Diese Darstellung heißt die P-adische Potenzreihe von z bezüglich t.

Umgekehrt gilt: Sei $(c_i)_{i\geq n}, n \in \mathbb{Z}$ eine Folge in K, dann ist die Reihe $\sum_{i=n}^{\infty} c_i t^i$ in $\hat{F}_P$ konvergent, und es gilt

$$\nu_P\left(\sum_{i=n}^{\infty} c_i t^i\right) = \min\{i \,|\, c_i \neq 0\}.$$

Beweis. Zunächst beweisen wir die Existenz einer Darstellung der Form (2.38). Sei also $z \in \hat{F}_P$ gegeben. Wir wählen ein $n \in \mathbb{Z}$ mit $n \leq \nu_P(z)$. Da F in $\hat{F}_P$ dicht ist, gibt es ein Element $y \in F$ mit $\nu_P(z - y) > n$. Aufgrund der Dreiecksungleichung gilt $\nu_P(y) \geq n$ und daher $\nu_P(yt^{-n}) \geq 0$. Da P eine rationale Stelle ist, gibt es ein Element $a_n \in K$ mit $\nu_P(yt^{-n} - a_n) > 0$, und

$$\nu_P(z - a_n t^n) = \nu_P\left((z - y) + (y - a_n t^n)\right) > n.$$

Genauso finden wir ein $a_{n+1} \in K$ mit

$$\nu_P(z - a_n t^n - a_{n+1} t^{n+1}) > n + 1.$$

Wenn wir diese Konstruktion iterieren, erhalten wir eine unendliche Folge $a_n, a_{n+1}, a_{n+2}, \ldots$ in K, sodass

$$\nu_P\left(z - \sum_{i=n}^{m} a_i t^i\right) > m$$

für alle $m \geq n$. Das zeigt, dass

$$z = \sum_{i=n}^{\infty} a_i t^i$$

gilt.
Um die Eindeutigkeit dieser Darstellung zu zeigen, betrachten wir eine andere Folge $(b_i)_{i \geq m}$ in K, welche folgende Bedingung erfüllt:

$$z = \sum_{i=n}^{\infty} a_i t^i = \sum_{i=m}^{\infty} b_i t^i.$$

Wir können $n = m$ annehmen, denn wenn $n < m$ ist, definieren wir $b_i := 0$ für alle $n \leq i < m$. Angenommen es gibt ein j mit $a_j \neq b_j$. Dann wählen wir ein minimales j mit dieser Eigenschaft und erhalten für alle $k > j$

$$\nu_P\left(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\right) = \nu_P\left((a_j - b_j)t^j + \sum_{i=j+1}^{k} (a_i - b_i)t^i\right) = j. \quad (2.39)$$

Die letzte Gleichheit gilt, da $\nu_P((a_j - b_j)t^j) = j$, und damit ist die strikte Dreiecksungleichung 2.2.2 anwendbar. Andererseits gilt

$$\begin{aligned}\nu_P\left(\sum_{i=n}^{k} a_i t^i - \sum_{i=n}^{k} b_i t^i\right) &= \nu_P\left(\sum_{i=n}^{k} a_i t^i - z + z - \sum_{i=n}^{k} b_i t^i\right) \\ &\geq \min\left\{\nu_P\left(z - \sum_{i=n}^{k} a_i t^i\right), \nu_P\left(z - \sum_{i=n}^{k} b_i t^i\right)\right\}. \quad (2.40)\end{aligned}$$

Für $k \to \infty$, strebt (2.40) gegen unendlich. Das ist ein Widerspruch zu (2.39) und zeigt, dass die Darstellung (2.38) eindeutig ist.
Um die letzte Aussage des Satzes zu zeigen, betrachten wir eine beliebige Folge $(c_i)_{i \geq n}, n \in \mathbb{Z}$ in K. Da $\nu_P(c_i t^i) \geq i$ für alle i gilt, strebt die Folge $(c_i t^i)_{i \geq n}$ gegen 0. Daher konvergiert nach Hilfssatz 2.7.5 die Reihe $\sum_{i=n}^{\infty} c_i t^i$ in $\hat{F}_P$, wir definieren:

$$\sum_{i=n}^{\infty} c_i t^i =: y \in \hat{F}_P.$$

Setze $j_0 := \min\{i \mid c_i \neq 0\}$. Im Fall $j_0 = \infty$ sind alle $c_i = 0$ und daher ist hier $y = 0$ und $\nu_P(y) = \infty$. Im Fall $j_0 < \infty$, gilt nach der strikten Dreiecksungleichung 2.2.2 für alle $k \geq j_0$

$$\nu_P\left(\sum_{i=n}^{k} c_i t^i\right) = j_0.$$

Da für genügend großes k

$$\nu_P\left(y - \sum_{i=n}^{k} c_i t^i\right) > j_0$$

ist, folgt

$$\nu_P(y) = \nu_P\left(y - \sum_{i=n}^{k} c_i t^i + \sum_{i=n}^{k} c_i t^i\right)$$

$$= \min\left\{\nu_P\left(y - \sum_{i=n}^{k} c_i t^i\right), \nu_P\left(\sum_{i=n}^{k} c_i t^i\right)\right\} = j_0,$$

und damit die Behauptung. □

Wie man aus dem Beweis des letzten Satzes sieht, läßt sich die P-adische Potenzreihenentwicklung sofort folgendermaßen verallgemeinern:

Satz 2.7.8 *Es sei $P \in \mathbb{P}_F$ eine rationale Stelle und $(t_r)_{r\in\mathbb{Z}}$ eine Folge von Elementen in F mit $\nu_P(t_r) = r$ für alle $r \in \mathbb{Z}$. Dann besitzt jedes Element $z \in \hat{F}_P$ eine eindeutige Darstellung der Form*

$$z = \sum_{i=n}^{\infty} a_i t_i \quad \textit{mit} \quad \nu_P(z) \geq n \in \mathbb{Z} \quad \textit{und} \quad a_i \in K.$$

Diese Darstellung nennen wir die P-adische Potenzreihe von z bezüglich der Folge $(t_r)_{r\in\mathbb{Z}}$.

Beweis. Der Beweis läuft genauso wie in Satz 2.7.7. □

2.8 Die Hasse-Weil-Schranke

In den letzten Abschnitten haben wir die Theorie der algebraischen Funktionenkörper über einem beliebigen Körper entwickelt. Im Hinblick auf die codierungstheoretischen Anwendungen wollen wir den Fall eines endlichen Konstantenkörpers genauer beleuchten. Deshalb setzen wir ab jetzt und für alles weitere voraus:

$F/\mathbb{F}_q$ sei ein algebraischer Funktionenkörper mit Geschlecht g, dessen Konstantenkörper der endliche Körper $\mathbb{F}_q$ ist.

Besonders sind wir an rationalen Stellen, also an Stellen deren Grad eins ist, interessiert. Ihre Anzahl ist endlich und kann durch die Hasse-Weil-Schranke abgeschätzt werden. Diese Schranke spielt eine wesentliche Rolle bei den Anwendungen der algebraischen Funktionenkörper in der Codierungstheorie. Da die Beweise der in diesem Abschnitt vorkommenden Sätze ein wesentlich tieferes Verständnis der Theorie der algebraischen Funktionenkörper verlangen, als wir entwickeln konnten, sollen sie in diesem Kapitel gänzlich entfallen. Eine vollständige Darstellung dieser Theorie findet man in [19].

Wir wollen im Folgenden die Zahl

$$A_n := |\{A \in \mathcal{D}_F \mid A \geq 0 \text{ und } \deg A = n\}| \tag{2.41}$$

untersuchen. Diese Zahl ist stets endlich. Zum Beispiel ist $A_0 = 1$ und A_1 die Anzahl der rationalen Stellen $P \in \mathbb{P}_F$. Wir codieren diese Information in die folgende Potenzreihe:

Definition 2.8.1 Die Potenzreihe

$$Z(t) := Z_F(t) := \sum_{n=0}^{\infty} A_n t^n \in \mathbb{C}[[t]]$$

heißt die *Zetafunktion* von $F/\mathbb{F}_q$.

Man beachte, dass t hier als komplexe Variable und $Z(t)$ als Potenzreihe über $\mathbb{C}$ aufgefasst wird, und nicht etwa eine P-adische Potenzreihe ist, wie sie im vorigen Kapitel betrachtet wurde. Diese Potenzreihe konvergiert in einer Umgebung von 0:

Satz 2.8.2 *Die Potenzreihe $Z(t) = \sum_{n=0}^{\infty} A_n t^n$ konvergiert für $|t| < q^{-1}$.*

Satz 2.8.3 *$Z(t)$ kann zu einer rationalen Funktion, die genau bei $t = q^{-1}$ und bei $t = 1$ einfache Pole besitzt, fortgesetzt werden.*

Als nächstes definieren wir:

Definition 2.8.4 Das Polynom $L(t) := L_F(t) := (1-t)(1-qt)Z(t)$ nennt man *L-Polynom* von $F/\mathbb{F}_q$.

Man beachte, dass $L(t)$ die ganze Information über die Zahlen A_n $(n \geq 0)$ beinhaltet, da

$$L(t) = (1-t)(1-qt)\sum_{n=0}^{\infty} A_n t^n$$

gilt. Die Eigenschaften von $L(t)$ sind im folgenden Satz zusammengefasst:

Satz 2.8.5
(a) $L(t) \in \mathbb{Z}[t]$ *und* $\deg L(t) = 2g$.
(b) *Sei* $L(t) = a_0 + a_1 t + \cdots + a_{2g} t^{2g}$. *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 rationalen Stellen* $P \in \mathbb{P}_F$ *bezeichnet.*
(c) $L(t)$ *faktorisiert über* $\mathbb{C}[t]$ *in*

$$L(t) = \prod_{i=1}^{2g} (1 - \alpha_i t).$$

Die komplexen Zahlen $\alpha_1, \ldots, \alpha_{2g}$ *können in einer Weise angeordnet werden, sodass* $\alpha_i \alpha_{g+i} = q$ *für* $i = 1, \ldots, g$ *gilt.*

Der letzte Satz zeigt, dass die Zahl

$$N(F) := N = |\{P \in \mathbb{P}_F \mid \deg P = 1\}|$$

sehr einfach mit Hilfe des L-Polynomes $L(t)$ von $F/\mathbb{F}_q$ berechnet werden kann.

Folgerung 2.8.6 *Für* $N(F)$ *gilt:*

$$N(F) = q + 1 - \sum_{i=1}^{2g} \alpha_i.$$

Das Hauptresultat zum Beweis der Hasse-Weil-Schranke ist der folgende Satz:

Satz 2.8.7 (Satz von Hasse-Weil) *Für die Reziprokwerte der Nullstellen von* $L_F(t)$ *gilt:*

$$|\alpha_i| = q^{1/2} \quad \text{für} \quad i = 1, \ldots, 2g.$$

Der Satz von Hasse-Weil 2.8.7 wird auch oft die *Riemann'sche Vermutung für algebraische Funktionenkörper* genannt. Diese Notation wollen wir kurz erläutern:

Man kann die Zetafunktion $Z_F(t)$ als ein Analogon zur klassischen Riemann'schen ζ-Funktion

$$\zeta(s) := \sum_{n=1}^{\infty} n^{-s} \tag{2.42}$$

(wobei $s \in \mathbb{C}$ und $\mathrm{Re}(s) > 1$ ist) auffassen. Definiere die *absolute Norm* eines Divisors $A \in \mathcal{D}_F$ durch

$$\mathcal{N}(A) := q^{\deg A}.$$

Die absolute Norm $\mathcal{N}(P)$ eines Primdivisors $P \in \mathbb{P}_F$ ist zum Beispiel die Kardinalität seines Restklassenkörpers F_P. Dann kann die Funktion

$$\zeta_F(s) := Z_F(q^{-s})$$

in der Form

$$\zeta_F(s) = \sum_{n=0}^{\infty} A_n q^{-sn} = \sum_{A \in \mathcal{D}_F, A \geq 0} \mathcal{N}(A)^{-s}$$

geschrieben werden, was ein geeignetes Analogon zu (2.42) darstellt. Es ist eine wohl bekannte Tatsache (siehe z.B. [20]), dass die Riemann'sche ζ-Funktion (2.42) eine analytische Fortsetzung zu einer meromorphen Funktion auf $\mathbb{C}$ besitzt. Die klassische Riemann'sche Vermutung (eines der wichtigsten ungelösten Probleme) besagt, dass - abgesehen von den sogenannten trivialen Nullstellen $s = -2, -4, -6, \ldots$ - alle Nullstellen von $\zeta(s)$ auf der Geraden $\mathrm{Re}(s) = 1/2$ liegen.

Der Satz von Hasse-Weil 2.8.7 impliziert, dass

$$\zeta_F(s) = 0 \Rightarrow Z_F(q^{-s}) = 0 \Rightarrow |q^{-s}| = q^{-1/2}$$

gilt. Da $|q^{-s}| = q^{-\mathrm{Re}(s)}$ ist, bedeutet die vorige Implikation Folgendes:

$$\zeta_F(s) = 0 \Rightarrow \mathrm{Re}(s) = 1/2.$$

Deshalb kann der Satz von Hasse-Weil 2.8.7 als Analogon zur klassischen Riemann'schen Vermutung aufgefasst werden.

Als direkte Folgerung aus dem Satz von Hasse-Weil 2.8.7 erhalten wir den nachstehenden Satz:

Satz 2.8.8 (Hasse-Weil-Schranke) *Die Zahl $N = N(F)$ der rationalen Stellen von $F/\mathbb{F}_q$ kann durch*

$$|N - (q+1)| \leq 2gq^{1/2}$$

abgeschätzt werden.

Beweis. Aus Folgerung 2.8.6 erhalten wir

$$N - (q+1) = -\sum_{i=1}^{2g} \alpha_i.$$

Daher ist die Hasse-Weil-Schranke eine sofortige Folgerung aus dem Satz von Hasse-Weil 2.8.7. □

Die Hasse-Weil-Schranke ist scharf, man kann Beispiele für Funktionenkörper $F/\mathbb{F}_q$ angeben, wo sie angenommen wird. Mit ihrer Hilfe können auch Abschätzungen für die Anzahl der Stellen von festem Grad r

$$B_r := B_r(F) := |\{P \in \mathbb{P}_F \mid \deg P = r\}|$$

angegeben werden. Solche Untersuchungen findet man zum Beispiel in [19].

Kapitel 3

Geometrische Goppa-Codes

In diesem Kapitel wollen wir Linearcodes betrachten, die Goppa um 1981 basierend auf algebraischen Funktionenkörper $F/\mathbb{F}_q$ konstruiert hat. Heute nennt man diese Codes *algebraisch-geometrische Codes* (kurz *AG-Codes*) oder *geometrische Goppa-Codes.*

In Goppas Konstruktion wählt man einen Divisor G und n rationale Stellen. Dann bildet die Auswertung der Funktionen von $\mathcal{L}(G)$ an diesen rationalen Stellen einen Code der Länge n. Goppa hat zwei duale Klassen von Codes definiert. Diese beiden Klassen sind aber verschiedene Beschreibungen für dieselben Codes. Später werden wir eine weitere äquivalente Methode kennenlernen, geometrische Goppa-Codes zu konstruieren. Diese ist erst kürzlich entdeckt worden und zeigt ganz neue Perspektiven von AG-Codes auf.

3.1 Konstruktion nach Goppa

Wir wollen einige Notationen für diesen Abschnitt festhalten:

> $F/\mathbb{F}_q$ *sei ein algebraischer Funktionenkörper mit Geschlecht* g.
> $P_1, \ldots, P_n$ *seien paarweise verschiedene rationale Stellen von* $F/\mathbb{F}_q$.
> $D = P_1 + \cdots + P_n$.
> G *sei ein Divisor von* $F/\mathbb{F}_q$ *mit* $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$.

Dann definieren wir:

Definition 3.1.1 Der *geometrische Goppa-Code* (oder *algebraisch-geometrische Code*) $C_{\mathcal{L}}(D, G)$ assoziiert mit den Divisoren D und G ist definiert durch

$$C_{\mathcal{L}}(D, G) := \{(x(P_1), \ldots, x(P_n)) \mid x \in \mathcal{L}(G)\} \subseteq \mathbb{F}_q^n.$$

Man beachte, dass diese Definition aus folgendem Grund sinvoll ist: für $x \in \mathcal{L}(G)$ gilt $\nu_{P_i}(x) \geq 0$ $(i = 1, \ldots, n)$, da $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$ ist. Die Restklasse $x(P_i)$ von x modulo P_i ist ein Element des Restklassenkörpers von P_i. Wegen $\deg P_i = 1$, ist der Restklassenkörper der Körper $\mathbb{F}_q$, daher gilt $x(P_i) \in \mathbb{F}_q$.

Wir können die *Auswertungsabbildung* $ev_D : \mathcal{L}(G) \to \mathbb{F}_q^n$ betrachten, die gegeben ist durch

$$ev_D(x) := (x(P_1), \ldots, x(P_n)) \in \mathbb{F}_q^n. \tag{3.1}$$

Die Auswertungsabbildung ist $\mathbb{F}_q$-linear und $C_{\mathcal{L}}(D, G)$ ist das Bild von $\mathcal{L}(G)$ unter dieser Abbildung.

Tatsächlich stellt Definition 3.1.1 eine komplizierte Möglichkeit dar, einen speziellen Unterraum von $\mathbb{F}_q^n$ zu definieren. Der nächste Satz zeigt, warum diese Codes interessant sind. Mit Hilfe des Satzes von Riemann-Roch 2.6.4 kann man nämlich die Paramter k und d dieses Codes berechnen oder zumindest abschätzen.

Satz 3.1.2 *$C_{\mathcal{L}}(D, G)$ ist ein $[n, k, d]$-Code mit den Parametern*

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

Beweis. Die Auswertungsabbildung (3.1) ist eine surjektive lineare Abbildung von $\mathcal{L}(G)$ nach $C_{\mathcal{L}}(D, G)$ mit dem Kern

$$\ker(ev_D) = \{x \in \mathcal{L}(G) \mid \nu_{P_i}(x) > 0 \text{ für } i = 1, \ldots, n\} = \mathcal{L}(G - D).$$

Es folgt, dass $k = \dim C_{\mathcal{L}}(D, G) = \dim \mathcal{L}(G) - \dim \mathcal{L}(G - D)$ ist. Die Behauptung über die Minimaldistanz d macht nur dann Sinn, wenn $C_{\mathcal{L}}(D, G) \neq \{0\}$ gilt, daher nehmen wir das an. Wähle $x \in \mathcal{L}(G)$ mit $\operatorname{wt}(ev_D(x)) = d$. Dann sind genau $n - d$ Stellen $P_{i_1}, \ldots, P_{i_{n-d}}$ im Träger von D Nullstellen von x, daher ist

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

Nach Folgerung 2.4.15 (b) können wir schließen, dass

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

gilt. Daher ist $d \geq n - \deg G$. □

Folgerung 3.1.3 *Angenommen, der Grad von G sei echt kleiner als n.*

Dann ist die Auswertungsabbildung $ev_D : \mathcal{L}(G) \to C_{\mathcal{L}}(D,G)$ *injektiv und es gilt:*
(a) $C_{\mathcal{L}}(D,G)$ *ist ein* $[n,k,d]$*-Code mit*

$$d \geq n - \deg G \quad \textit{und} \quad k = \dim G \geq \deg G + 1 - g.$$

Daher gilt

$$k + d \geq n + 1 - g. \tag{3.2}$$

(b) *Falls zusätzlich* $2g - 2 < \deg G < n$ *gilt, dann ist* $k = \deg G + 1 - g$.
(c) *Falls* $\{x_1, \ldots, x_k\}$ *eine Basis von* $\mathcal{L}(G)$ *ist, dann ist die Matrix*

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

eine Generatormatrix für $C_{\mathcal{L}}(D,G)$.

Beweis. Nach Annahme sei $\deg(G-D) = \deg G - n < 0$, daher ist $\mathcal{L}(G-D) = 0$. Da $\mathcal{L}(G-D)$ den Kern der Auswertungsabbildung bildet, ist diese Abbildung injektiv. Die verbleibenden Aussagen sind triviale Folgerungen aus Satz 3.1.2 und dem Satz von Riemann-Roch 2.6.4. □

Man beachte, dass die untere Schranke für die Minimaldistanz (3.2), einer oberen Schranke, nämlich der Singelton-Schranke 1.5.4, sehr ähnlich ist. Wenn wir diese beiden Schranken zusammensetzen, erhalten wir für $\deg G < n$

$$n + 1 - g \leq k + d \leq n + 1. \tag{3.3}$$

Falls das Geschlecht g des Funktionenkörpers F gleich 0 ist, dann gilt $k + d = n + 1$. Daher sind geometrische Goppa-Codes, die über dem rationalen Funktionenkörper $\mathbb{F}_q(z)$ konstruiert werden, nach Satz 2.4.21 im Fall $\deg G < n$ stets MDS-Codes.

Um eine sinnvolle Schranke für die Minimaldistanz von $C_{\mathcal{L}}(D,G)$ und der Dimension k zu bekommen, setzen wir deshalb oft $g \leq \deg G < n$ voraus.

Definition 3.1.4 Die Zahl $d^* := n - \deg G$ nennt man die *konstruierte Distanz* des Codes $C_{\mathcal{L}}(D,G)$.

Satz 3.1.3 besagt, dass die Minimaldistanz d eines geometrischen Goppa-Codes nicht kleiner als seine konstruierte Distanz sein kann. Die Frage, ob $d^* = d$ oder $d^* < d$ gilt, wird durch den folgenden Hilfssatz beantwortet:

Hilfssatz 3.1.5 *Angenommen es gelte* $\dim G > 0$ *und* $d^* = n - \deg G > 0$.

So gilt $d^* = d$ dann und nur dann, wenn ein Divisor D' mit $0 \leq D' \leq D$, $\deg D' = \deg G$ und $\dim(G - D') > 0$ existiert.

Beweis. Zunächst nehmen wir $d^* = d$ an. Dann gibt es ein Element $0 \neq x \in \mathcal{L}(G)$, sodass das Codewort $(x(P_1), \ldots, x(P_n)) \in C_{\mathcal{L}}(D, G)$ genau $n - d = n - d^* = \deg G$ Komponenten hat, die 0 sind, sagen wir $x(P_{i_j}) = 0$ für $j = 1, \ldots, \deg G$. Setzen wir

$$D' := \sum_{j=1}^{\deg G} P_{i_j}.$$

Dann gilt: $0 \leq D' \leq D$, $\deg D' = \deg G$ und $\dim(G - D') > 0$ (da $x \in \mathcal{L}(G - D')$ ist).
Umkehrung: Falls D' die obigen Eigenschaften hat, wählen wir ein Element $0 \neq y \in \mathcal{L}(G - D')$. Das Gewicht des dazugehörigen Codewortes $(y(P_1), \ldots, y(P_n))$ ist $\leq n - \deg G = d^*$, daher gilt $d = d^*$. □

Mit Hilfe der lokalen Komponenten von Weil-Differentialen kann auch ein anderer Code zu den Divisoren G und D assoziiert werden.

Definition 3.1.6 Seien G und $D = P_1 + \cdots + P_n$ Divisoren wie zuvor. Dann definieren wir den Code $C_\Omega(D, G) \subseteq \mathbb{F}_q^n$ durch

$$C_\Omega(D, G) := \{(\omega_{P_1}(1), \ldots, \omega_{P_n}(1)) \,|\, \omega \in \Omega_F(G - D)\}.$$

Unser erstes Resultat ist ein Analogon zu Satz 3.1.2.

Satz 3.1.7 *$C_\Omega(D, G)$ ist ein $[n, k', d']$-Code mit den Parametern*

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

Unter der zusätzlichen Voraussetzung, dass $\deg G > 2g - 2$ ist, gilt $k' = i(G - D) \geq n + g - 1 - \deg G$. Falls $2g - 2 < \deg G < n$ ist ,dann gilt

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

Beweis. Sei $P \in \mathbb{P}_F$ eine rationale Stelle und ω ein Weil-Differential mit $\nu_P(\omega) \geq -1$. Wir behaupten

$$\omega_P(1) = 0 \iff \nu_P(\omega) \geq 0. \tag{3.4}$$

Um diese Aussage zu zeigen, verwenden wir Satz 2.5.20 (a), der besagte, dass für eine ganze Zahl $r \in \mathbb{Z}$ Folgendes gilt:

$$\nu_P(\omega) \geq r \iff \omega_P(x) = 0 \quad \text{für alle} \quad x \in F \quad \text{mit} \quad \nu_P(x) \geq -r. \tag{3.5}$$

Die Implikation $\Leftarrow$ von (3.4) ist eine offensichtliche Folgerung aus (3.5). Umgekehrt nehmen wir an, dass $\omega_P(1) = 0$ sei. Sei nun $x \in F$ mit $\nu_P(x) \geq 0$. Da $\deg P = 1$ ist, können wir $x = a + y$ mit $a \in \mathbb{F}_q$ und $\nu_P(y) \geq 1$ schreiben. Dann ist

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

Aus (3.5) folgt nämlich $\omega_P(y) = 0$, da $\nu_P(\omega) \geq -1$ und $\nu_P(y) \geq 1$ gilt. Damit ist (3.4) gezeigt.
Wir betrachten jetzt die $\mathbb{F}_q$-lineare Abbildung

$$\rho_D : \begin{cases} \Omega_F(G-D) & \longrightarrow & C_\Omega(D,G), \\ \omega & \longmapsto & (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)). \end{cases}$$

ρ_D ist surjektiv, und nach (3.4) ist $\Omega_F(G)$ ihr Kern. Daraus ergibt sich

$$k' = \dim \Omega_F(G-D) - \dim \Omega_F(G) = i(G-D) - i(G). \tag{3.6}$$

Sei $\rho_D(\omega) \in C_\Omega(D,G)$ ein Codewort mit Gewicht $m > 0$. Dann ist $\omega_{P_i}(1) = 0$ für gewisse Indizes $i = i_1, \ldots, i_{n-m}$, daher gilt nach (3.4)

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

Da $\Omega_F(A) \neq 0$ nach Satz 2.6.6 $\deg A \leq 2g-2$ impliziert, erhalten wir

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

Daher gilt für die Minimaldistanz d' von $C_\Omega(D,G)$ die Ungleichung $d' \geq \deg G - (2g-2)$.
Wenn wir noch $\deg G > 2g-2$ annehmen, erhalten wir nach Satz 2.6.6 $i(G) = 0$. Deshalb impliziert (3.6)

$$k' = i(G-D) = \dim(G-D) - \deg(G-D) - 1 + g$$

$$= \dim(G-D) + n + g - 1 - \deg G.$$

Die verbleibenden Aussagen des Satzes folgen jetzt sofort. □

In Analogie zu Definition 3.1.4 nennt man $\deg G - (2g-2)$ die *konstruierte Distanz* von $C_\Omega(D,G)$.

Die enge Verbindung, die es zwischen $C_\mathcal{L}(D,G)$ und $C_\Omega(D,G)$ gibt, zeigt der folgende Satz:

Satz 3.1.8 *Die Codes $C_\mathcal{L}(D,G)$ und $C_\Omega(D,G)$ sind dual zueinander, das heißt es gilt*

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

Beweis. Wir bemerken zunächst die folgende Tatsache: Man betrachte eine rationale Stelle $P \in \mathbb{P}_F$, ein Weil-Differential ω mit $\nu_P(\omega) \geq -1$ und ein Element $x \in F$ mit $\nu_P(x) \geq 0$. Dann gilt

$$\omega_P(x) = x(P) \cdot \omega_P(1). \tag{3.7}$$

Um dies zu zeigen, schreiben wir $x = a+y$ mit $a = x(P) \in \mathbb{F}_q$ und $\nu_P(y) > 0$. Dann gilt nach (3.5) $\omega_P(x) = \omega_P(a) + \omega_P(y) = a \cdot \omega_P(1) + 0 = x(P) \cdot \omega_P(1)$. Als nächstes zeigen wir, dass $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$. Sei dazu $\omega \in \Omega_F(G-D)$ und $x \in \mathcal{L}(G)$. Wir erhalten

$$\begin{aligned}
0 &= \omega(x) = \sum_{P \in \mathbb{P}_F} \omega_P(x) && (3.8)\\
&= \sum_{i=1}^{n} \omega_{P_i}(x) && (3.9)\\
&= \sum_{i=1}^{n} x(P_i) \cdot \omega_{P_i}(1) && (3.10)\\
&= \langle (\omega_{P_1}(1), \ldots, \omega_{P_n}(1)), (x(P_1), \ldots, x(P_n)) \rangle,
\end{aligned}$$

wobei $\langle , \rangle$ das kanonische innere Produkt von $\mathbb{F}_q^n$ bezeichnet (siehe Definition 1.3.11). Wir müssen noch die einzelnen Schritte in der obigen Rechnung rechtfertigen. (3.8) folgt aus Satz 2.5.19 und der Tatsache, dass Weil-Differentiale auf Hauptadèlen verschwinden. Für $P \in \mathbb{P}_F \backslash \{P_1, \ldots, P_n\}$ gilt $\nu_P(x) \geq -\nu_P(\omega)$, da $x \in \mathcal{L}(G)$ und $\omega \in \Omega_F(G-D)$ ist, deshalb folgt aus (3.5) $\omega_P(x) = 0$. Das beweist (3.9). Schlussendlich folgt (3.10) aus (3.7). Daher ist $C_\Omega(D,G) \subseteq C_\mathcal{L}(D,G)^\perp$.
Es genügt jetzt zu zeigen, dass die Codes $C_\Omega(D,G)$ und $C_\mathcal{L}(D,G)^\perp$ dieselbe Dimension haben. Aus den Sätzen 3.1.2, 3.1.7 und aus der Definition des Spezialitätsindex 2.5.1 folgt:

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

□

Als nächstes wollen wir zeigen, dass $C_\Omega(D,G)$ als $C_\mathcal{L}(D,H)$ mit einem geeigneten Divisor H dargestellt werden kann. Daraus wird dann ersichtlich, dass die beiden Definitionen ein und dieselbe Klasse von Codes, nämlich die

geometrischen Goppa-Codes, beschreiben. Für diesen Zweck benötigen wir zunächst den folgenden Hilfssatz.

Hilfssatz 3.1.9 *Es gibt ein Weil-Differential η mit den folgenden Eigenschaften:*

$$\nu_{P_i}(\eta) = -1 \quad \textit{und} \quad \eta_{P_i}(1) = 1 \quad \textit{für} \quad i = 1, \ldots, n.$$

Beweis. Wähle ein beliebiges Weil-Differential $\omega_0 \neq 0$. Nach dem schwachen Approximationssatz 2.2.7 gibt es ein Element $z \in F$ mit $\nu_{P_i}(z) = -\nu_{P_i}(\omega_0) - 1$ für $i = 1, \ldots, n$. Setze $\omega := z\omega_0$, dann erhalten wir $\nu_{P_i}(\omega) = -1$. Daher gilt nach (3.4) $a_i := \omega_{P_i}(1) \neq 0$. Wieder gibt es nach dem schwachen Approximationssatz 2.2.7 ein Element $y \in F$, sodass $\nu_{P_i}(y - a_i) > 0$ ist. Es folgt: $\nu_{P_i}(y) = 0$ und $y(P_i) = a_i$. Wir setzen $\eta := y^{-1}\omega$ und erhalten $\nu_{P_i}(\eta) = \nu_{P_i}(\omega) = -1$ und

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

□

Satz 3.1.10 *Sei η ein Weil-Differential mit $\nu_{P_i}(\eta) = -1$ und $\eta_{P_i}(1) = 1$ für $i = 1, \ldots, n$. Dann gilt*

$$C_{\mathcal{L}}(D, G)^{\perp} = C_{\Omega}(D, G) = C_{\mathcal{L}}(D, D - G + (\eta)).$$

Beweis. Beachte, dass $\operatorname{supp}(D - G + (\eta)) \cap \operatorname{supp} D = \emptyset$ ist, da $\nu_{P_i}(\eta) = -1$ für $i = 1, \ldots, n$ gilt. Daher ist $C_{\mathcal{L}}(D, D - G + (\eta))$ wohldefiniert. Nach Satz 2.6.3 gibt es einen Isomorphismus $\mu : \mathcal{L}(D - G + (\eta)) \to \Omega_F(G - D)$ definiert durch $\mu(x) := x\eta$. Für $x \in \mathcal{L}(D - G + (\eta))$ gilt nach (3.7)

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

Daraus folgt $C_{\Omega}(D, G) = C_{\mathcal{L}}(D, D - G + (\eta))$. □

Wir könnten Satz 3.1.10 zum Beispiel dazu verwenden um einen anderen Beweis von Satz 3.1.7 – und zwar als direkte Folgerung aus Satz 3.1.2 – zu geben. Als Nächstes wollen wir noch zeigen, dass zu G äquivalente Divisoren, diesselben geometrischen Goppa-Codes definieren.

Satz 3.1.11
(a) *Angenommen G_1 und G_2 sind Divisoren mit $G_1 \sim G_2$ und*

$$\operatorname{supp} G_1 \cap \operatorname{supp} D = \operatorname{supp} G_2 \cap \operatorname{supp} D = \emptyset.$$

Dann sind die Codes $C_{\mathcal{L}}(D, G_1)$ und $C_{\mathcal{L}}(D, G_2)$ äquivalent. Dasselbe gilt für $C_\Omega(D, G_1)$ und $C_\Omega(D, G_2)$.
(b) *Umgekehrt gilt: Wenn $C \subseteq \mathbb{F}_q^n$ ein zu $C_{\mathcal{L}}(D, G)$ (bzw. zu $C_\Omega(D, G)$) äquivalenter Code ist, dann gibt es einen Divisor $G' \sim G$, sodass* $\operatorname{supp} G' \cap \operatorname{supp} D = \emptyset$ *und $C = C_{\mathcal{L}}(D, G')$ (bzw. $C = C_\Omega(D, G')$) ist.*

Beweis. (a) Nach Annahme ist $G_2 = G_1 - (z)$ mit $\nu_{P_i}(z) = 0$ für $i = 1, \ldots, n$. Daher ist $a := (z(P_1), \ldots, z(P_n)) \in (\mathbb{F}_q \backslash \{0\})^n$. Außerdem ist die Abbildung $x \mapsto xz$ von $\mathcal{L}(G_1)$ nach $\mathcal{L}(G_2)$ bijektiv (nach Hilfssatz 2.4.9). Das zeigt $C_{\mathcal{L}}(D, G_2) = a \cdot C_{\mathcal{L}}(D, G_1)$. Die Äquivalenz von $C_\Omega(D, G_1)$ und $C_\Omega(D, G_2)$ beweist man ähnlich.
(b) Sei $C = a \cdot C_{\mathcal{L}}(D, G)$ mit $a = (a_1, \ldots, a_n) \in (\mathbb{F}_q \backslash \{0\})^n$. Nach dem Approximationssatz 2.2.7 gibt es ein $z \in F$ mit $z(P_i) = a_i$ $(i = 1, \ldots, n)$ und setze $G' := G - (z)$. Dann ist $C = C_{\mathcal{L}}(D, G')$. □

Dieser Satz hat die folgende Konsequenz: Falls G ein Divisor ist, dessen Träger nicht disjunkt zu $\operatorname{supp} D$ ist, können wir immer noch einen geometrischen Goppa-Code $C_{\mathcal{L}}(D, G)$ assoziiert zu D und G definieren. Wähle nämlich einen Divisor $G' \sim G$ mit $\operatorname{supp} G' \cap \operatorname{supp} D = \emptyset$ (das ist nach dem schwachen Approximationssatz 2.2.7 möglich) und setze $C_{\mathcal{L}}(D, G) := C_{\mathcal{L}}(D, G')$. Die Wahl von G' ist nicht kanonisch, daher ist nach Satz 3.1.11 $C_{\mathcal{L}}(D, G)$ nur bis auf Äquivalenz wohldefiniert.

3.2 Konstruktion nach Xing - Niederreiter - Lam und Özbudak - Stichtenoth

Kürzlich haben C. P. Xing, H. Niederreiter und K. Y. Lam eine Reihe von neuen Konstruktionen von Linearcodes, basierend auf algebraischen Funktionenkörpern, entdeckt (siehe [15], [25] und [26]). Diese neuen Konstruktionen unterscheiden sich wesentlich von Goppas Konstruktion der geometrischen Goppa-Codes, die wir im letzten Kapitel kennengelernt haben. Während Goppa nur die Auswertung von Funktionen (bzw. von Weil-Differentialen bei 1) verwendet, machen Xing, Niederreiter und Lam wesentlichen Gebrauch von P-adischen Potenzreihenentwicklungen, nicht speziellen Divisoren, usw.

Diese neuen Codes haben sich als äquivalent zu gewissen geometrischen Goppa-Codes herausgestellt. Wir werden sie im nächsten Abschnitt kennenlernen. In diesem Abschnitt wollen wir eine Verallgemeinerung der Konstruktion von Xing, Niederreiter und Lam betrachten, die äquivalent zu Goppas Konstruktion ist, und von F. Özbudak und H. Stichtenoth stammt (siehe

[16]).

Die grundsätzliche Idee dabei ist recht einfach: Seien G_1 und G_2 zwei Divisoren eines algebraischen Funkionenkörpers über $\mathbb{F}_q$ mit $G_1 \leq G_2$. Dann ist $\mathcal{L}(G_1)$ ein Unterraum des Vektorraumes $\mathcal{L}(G_2)$ über $\mathbb{F}_q$. Wenn wir daher eine Basis von $\mathcal{L}(G_2)$ wählen, dann bilden die Koordinatenvektoren der Elemente von $\mathcal{L}(G_1)$ einen linearen Code über $\mathbb{F}_q$ der Länge $n = \dim(\mathcal{L}(G_2))$ und mit Dimension $k = \dim(\mathcal{L}(G_1))$. Wir werden eine leicht verbesserte Variante dieser Idee verwenden. Klarerweise müssen dabei die Basis, sowie die Divisoren G_1 und G_2 geeignet gewählt werden, denn nimmt man zum Beispiel eine Basis von $\mathcal{L}(G_1)$ und erweitert diese zu einer Basis von $\mathcal{L}(G_2)$, dann erhält man einen uninteressanten Linearcode mit Minimaldistanz 1.

Es sei $F/\mathbb{F}_q$ ein algebraischer Funktionenkörper mit Geschlecht g. Wir wählen einen nicht speziellen Divisor B und n verschiedene rationale Stellen $P_1, \ldots, P_n$. Für $1 \leq j \leq n$ betrachten wir den Vektorraum

$$\mathcal{L}(B + P_j).$$

Dann ist $\mathcal{L}(B + P_j) \backslash \mathcal{L}(B)$ nichtleer. Da nämlich B als nicht speziell vorausgesetzt war, folgt mit Hilfsatz 2.6.12

$$\dim(B + P_j) = \dim(B) + 1.$$

Wir wählen Elemente

$$f_j \in \mathcal{L}(B + P_j) \backslash \mathcal{L}(B) \tag{3.11}$$

für jedes $1 \leq j \leq n$. Dann gilt der folgende Hilfssatz:

Hilfssatz 3.2.1 *Seien $f_1, f_2, \ldots, f_n$ wie in (3.11), dann hat jedes $f \in \mathcal{L}(B + \sum_{i=1}^{n} P_i)$ eine eindeutige Darstellung der Form*

$$f = \sum_{i=1}^{n} c_i f_i + w, \quad \textit{mit} \quad c_i \in \mathbb{F}_q \quad \textit{und} \quad w \in \mathcal{L}(B).$$

Beweis. Es sei $s := \dim B$ und $g_1, \ldots, g_s$ eine Basis von $\mathcal{L}(B)$. Zunächst gilt wieder mit Hilfssatz 2.6.12

$$\dim\left(B + \sum_{i=1}^{n} P_i\right) = \dim(B) + n.$$

Es genügt also zu zeigen, dass $f_1, \ldots, f_n, g_1, \ldots, g_s$, linear unabhängig über $\mathbb{F}_q$ sind.
Sei dazu

$$\sum_{i=1}^{n} a_i f_i + \sum_{j=1}^{s} b_j g_j = 0$$

mit $a_i, b_j \in \mathbb{F}_q$. Angenommen $a_h \neq 0$ für ein $1 \leq h \leq n$. Dann gilt

$$-a_h f_h = \sum_{i \neq h} a_i f_i + \sum_{j=1}^{s} b_j g_j. \tag{3.12}$$

Nach Konstruktion der f_i, g_j erhalten wir die Ungleichungen

$$\nu_{P_h}(-a_h f_h) = \nu_{P_h}(f_h) \leq -\nu_{P_h}(B) - 1$$

und

$$\nu_{P_h}\left(\sum_{i \neq h} a_i f_i + \sum_{j=1}^{s} b_j g_j\right) \geq -\nu_{P_h}(B).$$

Diese zwei Ungleichungen sind ein Widerspruch zu (3.12). Daher ist $a_1 = a_2 = \cdots = a_n = 0$ und nach Wahl der g_j ist daher auch $b_1 = \cdots = b_s = 0$. Daraus folgt die Behauptung. □

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

$$\alpha : \begin{cases} \mathcal{L}(B + \sum_{i=1}^{n} P_i) & \longrightarrow & \mathbb{F}_q^n, \\ f & \longmapsto & (c_1, \ldots, c_n). \end{cases} \tag{3.13}$$

Diese Abbildung ist klarerweise surjektiv und besitzt den Kern $\ker(\alpha) = \mathcal{L}(B)$.

Sei A ein weiterer Divisor mit den folgenden Eigenschaften:

$$A \geq 0 \quad \text{und} \quad \operatorname{supp} A \cap \{P_1, \ldots, P_n\} = \emptyset. \tag{3.14}$$

Dann definieren wir den folgenden Code:

Definition 3.2.2 Seien $B, P_1, \ldots, P_n, A$ und die Abbildung α wie vorher. Dann definieren wir den Code $C_{\mathcal{NS}}(B; P_1, \ldots, P_n; A) \subseteq \mathbb{F}_q^n$ durch

$$C_{\mathcal{NS}} := C_{\mathcal{NS}}(B; P_1, \ldots, P_n; A) = \alpha\left(\mathcal{L}\left(B + \sum_{i=1}^{n} P_i - A\right)\right).$$

Wir wollen als Nächstes zeigen, dass die so erhaltenen Codes in Wirklichkeit geometrische Goppa-Codes sind.

Wir betrachten also den Code

$$C_{\mathcal{NS}} = C_{\mathcal{NS}}(B; P_1, \ldots, P_n; A),$$

wobei B ein nicht spezieller Divisor ist, $P_1, \ldots, P_n$ verschiedene rationale Stellen sind und A ein positiver Divisor mit $\operatorname{supp} A \cap \{P_1, \ldots, P_n\} = \emptyset$ ist. Mit Hilfe des schwachen Approximationssatzes 2.2.7 finden wir ein Element $z \in F$ mit

$$\nu_{P_i}(z - f_i^{-1}) = -\nu_{P_i}(f_i) + 1, \quad i = 1, \ldots, n.$$

Es gilt dann

$$\nu_{P_i}(zf_i) = 0 \quad \text{und} \quad (zf_i)(P_i) = 1,$$

für $i = 1, \ldots, n$. Wir definieren den Divisor:

$$G := B + \sum_{i=1}^{n} P_i - A - (z).$$

Es gilt dann der folgende Satz:

Satz 3.2.3 *Seien $A, B, P_1, \ldots, P_n$, und G wie vorhin. Dann gilt*

$$C_{\mathcal{NS}}(B; P_1, \ldots, P_n; A) = C_{\mathcal{L}}(P_1 + \cdots + P_n, G).$$

Beweis. Zunächst sei bemerkt, dass

$$\nu_{P_i}(G) = \nu_{P_i}(B) + 1 - \nu_{P_i}(z) = -\nu_{P_i}(f_i) - \nu_{P_i}(z) = 0$$

für $i = 1, \ldots, n$ gilt, daher ist $\operatorname{supp} G \cap \{P_1, \ldots, P_n\} = \emptyset$. Betrachte die Auswertungsabbildung

$$ev : \begin{cases} \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n, \\ h & \longmapsto & (h(P_1), \ldots, h(P_n)) \end{cases}$$

und die Abbildung

$$\varphi : \begin{cases} \mathcal{L}\left(B + \sum_{i=1}^{n} P_i - A\right) & \longrightarrow & \mathcal{L}(G), \\ f & \longmapsto & zf. \end{cases}$$

Die Abbildung φ ist ein $\mathbb{F}_q$-linearer Isomorphismus (siehe Hilfssatz 2.4.9 (b)). Wir betrachten jetzt das folgende Diagramm:

$$\begin{array}{ccc} \mathcal{L}\left(B + \sum_{i=1}^{n} P_i - A\right) & \longrightarrow & \mathcal{L}(G) \\ & \searrow \quad \swarrow & \\ & \mathbb{F}_q^n & \end{array}$$

wobei $\alpha : \mathcal{L}(B + \sum_{i=1}^{n} P_i - A) \to \mathbb{F}_q^n$ durch (3.13) definiert ist. Wie man leicht sieht ist dieses Diagramm kommutativ. Sei nämlich

$$f \in \mathcal{L}\left(B + \sum_{i=1}^{n} P_i - A\right),$$

dann erhalten wir

$$f = \sum_{i=1}^{n} c_i f_i + w$$

mit $c_1, \ldots, c_n \in \mathbb{F}_q$ und $w \in \mathcal{L}(B)$ (das geht nach Hilfssatz 3.2.1). Daher ist $(c_1, \ldots, c_n) = \alpha(f)$. Andererseits gilt

$$(zf)(P_j) = \left(\sum_{i=1}^{n} c_i z f_i + zw \right)(P_j) = c_j (zf_j)(P_j) = c_j$$

für alle $1 \leq j \leq n$, nach Wahl von z und da $\nu_{P_j}(zf_i) = \nu_{P_j}(z) + \nu_{P_j}(f_i) \geq -\nu_{P_j}(B) + 1 + \nu_{P_j}(B) = 1 > 0$ und genauso $\nu_{P_j}(zw) \geq 1 > 0$ ist. Also gilt $ev(\varphi(f)) = \alpha(f)$. Daher folgt

$$C_{\mathcal{NS}} = \alpha\left(\mathcal{L}\left(B + \sum_{i=1}^{n} P_i - A \right) \right) = ev(\mathcal{L}(G)) = C_{\mathcal{L}}(P_1 + \cdots + P_n, G).$$

□

Als Folgerung erhalten wir sofort Abschätzungen für die Parameter des Codes $C_{\mathcal{NS}}(B; P_1, \ldots, P_n; A)$.

Satz 3.2.4 *Es sei B ein nicht spezieller Divisor, $P_1, \ldots, P_n$ verschiedene rationale Stellen, sowie A ein Divisor mit (3.14). Zusätzlich gelte* $\deg A > \deg B$. *Dann ist $C_{\mathcal{NS}}(B; P_1, \ldots, P_n; A)$ ein $[n, k, d]$-Code mit*

$$k \geq \deg B - \deg A + n + 1 - g \quad \textit{und} \quad d \geq \deg A - \deg B.$$

Beweis. Folgt sofort aus Satz 3.2.3 und Satz 3.1.3. □

Aus dem Beweis von Satz 3.2.3 sieht man außerdem leicht, dass jeder geometrische Goppa-Code als ein Code $C_{\mathcal{NS}}$, mit geeigneten Divisoren, dargestellt werden kann. In diesem Sinne sind diese beiden Konstruktionen äquivalent.

3.3 Einige spezielle Klassen von Goppa-Codes

In diesem Abschnitt wollen wir zunächst geometrische Goppa-Codes untersuchen, die mit Hilfe von Divisoren des rationalen Funktionenkörpers definiert werden.

Definition 3.3.1 Ein geometrischer Goppa-Code $C_{\mathcal{L}}(D, G)$ assoziiert mit

Divisoren G und D des rationalen Funktionenkörpers $\mathbb{F}_q(z)/\mathbb{F}_q$ nennt man *rational* (wir nehmen wieder stets an, dass $D = P_1 + \cdots + P_n$ mit paarweise verschiedenen rationalen Stellen und $\operatorname{supp} G \cap \operatorname{supp} D = \emptyset$ gilt).

Beachte, dass die Länge von $C_{\mathcal{L}}(D, G)$ durch $q+1$ beschränkt ist, da $\mathbb{F}_q(z)$ nur $q+1$ rationale Stellen besitzt, nämlich den Pol P_∞ von z und für jedes $\alpha \in \mathbb{F}_q$ die Nullstelle P_α von $z - \alpha$ (siehe Satz 2.3.1). Das folgende Resultat ist eine sofortige Konsequenz aus Abschnitt 3.1.

Satz 3.3.2 *Sei $C = C_{\mathcal{L}}(D, G)$ ein rationaler geometrischer Goppa-Code über $\mathbb{F}_q$, und seien n, k, d die Parameter von C. Dann gilt:*
(a) $n \leq q + 1$.
(b) $k = 0 \iff \deg G < 0$, *und* $k = n \iff \deg G > n - 2$.
(c) *Für* $0 \leq \deg G \leq n - 2$ *gilt,*

$$k = 1 + \deg G \quad \textit{und} \quad d = n - \deg G.$$

Insbesondere ist C daher ein MDS Code.
(d) *$C^\perp$ ist ebenfalls ein rationaler geometrischer Goppa-Code.*

Als nächstes berechnen wir die Generatormatrix eines rationalen geometrischen Goppa-Codes.

Satz 3.3.3 *Sei $C = C_{\mathcal{L}}(D, G)$ ein rationaler geometrischer Goppa-Code über $\mathbb{F}_q$ mit Parametern n, k und d.*
(a) *Falls $n \leq q$ ist, gibt es paarweise verschiedene Elemente $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ und $v_1, \ldots, v_n \in \mathbb{F}_q \backslash \{0\}$ (nicht notwendig verschieden), sodass*

$$C = \{(v_1 \cdot f(\alpha_1), v_2 \cdot f(\alpha_2), \ldots, v_n \cdot f(\alpha_n)) \mid f \in \mathbb{F}_q[z] \textit{ und } \deg f \leq k - 1\}.$$

Die Matrix

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_n \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_n \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_n \\ \vdots & \vdots & & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_n \end{pmatrix} \tag{3.15}$$

ist eine Generatormatrix von C.
(b) *Falls $n = q + 1$ ist, hat C die folgende Generatormatrix*

$$M = \begin{pmatrix} v_1 & v_2 & \cdots & v_{n-1} & 0 \\ \alpha_1 v_1 & \alpha_2 v_2 & \cdots & \alpha_n v_{n-1} & 0 \\ \alpha_1^2 v_1 & \alpha_2^2 v_2 & \cdots & \alpha_n^2 v_{n-1} & 0 \\ \vdots & \vdots & & \vdots & \vdots \\ \alpha_1^{k-1} v_1 & \alpha_2^{k-1} v_2 & \cdots & \alpha_n^{k-1} v_{n-1} & 1 \end{pmatrix} \tag{3.16}$$

wobei $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_{n-1}\}$ *und* $v_1, \ldots, v_{n-1} \in \mathbb{F}_q \backslash \{0\}$.

Beweis. (a) Sei $D = P_1 + \cdots + P_n$. Da $n \leq q$ ist, gibt es eine rationale Stelle P, die nicht im Träger von D liegt. Wähle eine rationale Stelle $Q \neq P$ (z.B. $Q = P_1$). Nach dem Satz von Riemann-Roch 2.6.4 gilt $\dim(Q - P) = 1$, daher ist nach Folgerung 2.4.15 $Q - P$ ein Hauptdivisor. Sei $Q - P = (z)$. Dann ist z ein erzeugendes Element des rationalen Funktionenkörpers über $\mathbb{F}_q$, und P ist ein Poldivisor von z. Wie gewöhnlich schreiben wir $P = P_\infty$. Nach Satz 3.3.2 können wir annehmen, dass $\deg G = k - 1 \geq 0$ sei, denn der Fall $k = 0$ ist trivial. Der Divisor $(k-1)P_\infty - G$ hat Grad 0, daher ist er ein Hauptdivisor (wieder nach dem Satz von Riemann-Roch 2.6.4 und Folgerung 2.4.15). Sei $(k-1)P_\infty - G = (u)$ mit $0 \neq u \in F$. Die k Elemente $u, z \cdot u, \ldots, z^{k-1} \cdot u$ sind in $\mathcal{L}(G)$, und sie sind linear unabhängig über $\mathbb{F}_q$. Da $\dim G = k$ ist, bilden sie eine Basis von $\mathcal{L}(G)$, das heißt

$$\mathcal{L}(G) = \{u \cdot f(z) \mid f \in \mathbb{F}_q[z] \text{ und } \deg f \leq k-1\}.$$

Wir setzen $\alpha_i := z(P_i)$ und $v_i := u(P_i)$ und erhalten

$$(u \cdot f(z))(P_i) = u(P_i) \cdot f(z(P_i)) = v_i \cdot f(\alpha_i)$$

für $i = 1, \ldots, n$. Daher gilt

$$C = C_{\mathcal{L}}(D, G) = \{(v_1 \cdot f(\alpha_1), \ldots, v_n \cdot f(\alpha_n)) \mid \deg f \leq k-1\}.$$

Das Codewort in C, das zu $u \cdot z^j$ gehört, ist $(v_1\alpha_1^j, v_2\alpha_2^j, \ldots, v_n\alpha_n^j)$, daher ist die Matrix (3.15) eine Generatormatrix von C.
(b) Der Beweis ist im Wesentlichen derselbe wie der im Fall $n \leq q$. Doch jetzt gilt $n = q+1$, und wir können ein Element z so wählen, dass $P_n = P_\infty$ der Pol von z ist. Wie oben haben wir $(k-1)P_\infty - G = (u)$ mit $0 \neq u \in F$ und $\{u, z \cdot u, \ldots, z^{k-1} \cdot u\}$ ist eine Basis von $\mathcal{L}(G)$. Für $1 \leq i \leq n-1 = q$ sind die Elemente $\alpha_i := z(P_i) \in \mathbb{F}_q$ paarweise verschieden, daher gilt $\mathbb{F}_q = \{\alpha_1, \ldots, \alpha_{n-1}\}$. Weiters ist $v_i := u(P_i) \in \mathbb{F}_q \backslash \{0\}$ für $i = 1, \ldots, n-1$. Für $0 \leq j \leq k-2$ erhalten wir

$$((uz^j)(P_1), \ldots, (uz^j)(P_n)) = (\alpha_1^j v_1, \ldots, \alpha_{n-1}^j v_{n-1}, 0),$$

aber für $j = k-1$ folgt

$$((uz^{k-1})(P_1), \ldots, (uz^{k-1})(P_n)) = (\alpha_1^{k-1} v_1, \ldots, \alpha_{n-1}^{k-1} v_{n-1}, \gamma)$$

mit einem Element $0 \neq \gamma \in \mathbb{F}_q$. Wenn wir u durch $\gamma^{-1}u$ ersetzen, erhalten wir die Generatormatrix (3.16). □

Um den zum rationalen geometrischen Goppa-Code $C = C_{\mathcal{L}}(D, G)$ dualen Code zu berechnen, benötigen wir nach Satz 3.1.8 und 3.1.10 ein Weil-Differential ω von $\mathbb{F}_q(z)$, sodass

$$\nu_{P_i}(\omega) = -1 \quad \text{und} \quad \omega_{P_i}(1) = 1 \quad \text{für} \quad i = 1, \ldots, n. \tag{3.17}$$

Hilfssatz 3.3.4 *Betrachte den rationalen Funktionenkörper $F = \mathbb{F}_q(z)$ und n verschiedene Elemente $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$. Sei $P_i \in \mathbb{P}_F$ eine Nullstelle von $z - \alpha_i$ und $h(z) := \prod_{i=1}^{n}(z - \alpha_i)$. Angenommen y ist ein Element von F mit $y(P_i) = 1$ für $i = 1, \ldots, n$. Dann gibt es ein Weil-Differential ω von $F/\mathbb{F}_q$ mit der Eigenschaft (3.17) und dem Divisor*

$$(\omega) = (y) + (h'(z)) - (h(z)) - 2P_\infty$$

(wobei $h'(z) \in \mathbb{F}_q[z]$ die Ableitung des Polynomes $h(z)$ bezeichnet).

Beweis. Nach Satz 2.6.10 gibt es ein Weil-Differential η von F mit $(\eta) = -2P_\infty$ und $\eta_{P_\infty}(z^{-1}) = -1$. Wir setzen

$$\omega := y \cdot (h'(z)/h(z)) \cdot \eta.$$

Der Divisor von ω ist $(\omega) = (y) + (h'(z)) - (h(z)) - 2P_\infty$, insbesondere gilt $\nu_{P_i}(\omega) = -1$ für $i = 1, \ldots, n$. Wir müssen zeigen, dass $\omega_{P_i}(1) = 1$ ist. Dazu schreiben wir $h(z) = (z - \alpha_i)g_i(z)$. Dann folgt

$$y \cdot \frac{h'(z)}{h(z)} = (1 + (y-1)) \cdot \left(\frac{g_i'(z)}{g_i(z)} + \frac{1}{z - \alpha_i} \right) = \frac{1}{z - \alpha_i} + u$$

mit $u \in F$ und $\nu_{P_i}(u) \geq 0$ (da $\nu_{P_i}(y-1) > 0$ und $\nu_{P_i}(g_i(z)) = 0$ ist). Da nach Satz 2.6.10 (c) und Satz 2.5.20 (a) $\eta_{P_i}((z - \alpha_i)^{-1}) = 1$ und $\eta_{P_i}(u) = 0$ ist, erhalten wir

$$\omega_{P_i}(1) = \eta_{P_i}\left(y \cdot \frac{h'(z)}{h(z)} \right) = \eta_{P_i}\left(\frac{1}{z - \alpha_i} + u \right) = 1.$$

□

Beachte, dass man mit Hilfe von Hilfssatz 3.3.4 - kombiniert mit den Sätzen 3.1.8, 3.1.10 und 3.3.3 - eine Kontrollmatrix für $C_{\mathcal{L}}(D, G)$ angeben kann.

Beispiele für rationale geometrische Goppa-Codes kennen wir bereits: BCH-Codes. Der nächste Satz stellt die Verbindung her.

Satz 3.3.5 *Sei $n | q^m - 1$ und $\beta \in \mathbb{F}_{q^m}$ eine n-te primitive Einheitswurzel. Sei $F = \mathbb{F}_{q^m}(z)$ der rationale Funktionenkörper über $\mathbb{F}_{q^m}$ und P_0 (bzw. P_∞) die Nullstelle (bzw. der Pol) von z. Für $i = 1, \ldots, n$ bezeichne P_i die Nullstelle von $z - \beta^{i-1}$, und wir setzen $D_\beta := P_1 + \cdots + P_n$. Angenommen $a, b \in \mathbb{Z}$ sind ganze Zahlen mit $0 \leq a + b \leq n - 2$. Dann gilt:*
(a) *$C_{\mathcal{L}}(D_\beta, aP_0 + bP_\infty) = C(n, l, \delta)$ mit $l = -a$ und $\delta = a + b + 2$ (für*

$C(n,l,\delta)$ siehe Definition 1.6.1).
(b) *Der zu $C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)$ duale Code ist gegeben durch*

$$C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)^\perp = C_{\mathcal{L}}(D_\beta, rP_0+sP_\infty)$$

mit $r=-(a+1)$ und $s=n-b-1$. Daher ist der BCH-Code $C(n,l,\delta)^\perp|_{\mathbb{F}_q}$ die Einschränkung des Codes $C_{\mathcal{L}}(D_\beta, rP_0+sP_\infty)$ auf $\mathbb{F}_q$, mit $r=l-1$ und $s=n+1-\delta-l$.

Beweis. (a) Wir betrachten den Code $C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)$, wobei $0 \le a+b \le n-2$ ist. Die Elemente $z^{-a}\cdot z^j$ mit $0 \le j \le a+b$ bilden eine Basis von $\mathcal{L}(aP_0+bP_\infty)$. Daher ist die Matrix

$$\begin{pmatrix} 1 & \beta^{-a} & \beta^{-2a} & \dots & (\beta^{n-1})^{-a} \\ 1 & \beta^{-a+1} & \beta^{-2a+2} & \dots & (\beta^{n-1})^{-a+1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \beta^{-a+(a+b)} & \beta^{-2a+2(a+b)} & \dots & (\beta^{n-1})^{-a+(a+b)} \end{pmatrix}$$

eine Generatormatrix von $C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)$. Setzen wir $l := -a$ und $\delta := a+b+2$, dann erhalten wir (1.1), daher ist $C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty) = C(n,l,\delta)$.
(b) Wir verwenden die Bezeichnungen von Hilfssatz 3.3.4 und setzen

$$y := z^{-n} \text{ und } h(z) := \prod_{i=1}^{n}(z-\beta^{i-1}) = z^n - 1.$$

Nach Satz 3.1.10 ist $C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)^\perp = C_{\mathcal{L}}(D_\beta, B)$ mit

$$\begin{aligned} B &= D_\beta - (aP_0+bP_\infty) + (z^{-n}) + (h'(z)) - (h(z)) - 2P_\infty \\ &= D_\beta - (aP_0+bP_\infty) + n(P_\infty - P_0) + (n-1)(P_0-P_\infty) \\ &\qquad -(D_\beta - nP_\infty) - 2P_\infty \\ &= (-a-1)P_0 + (n-b-1)P_\infty. \end{aligned}$$

Da nach (a) $l=-a$ und $\delta = a+b+2$ ist, finden wir $C_{\mathcal{L}}(D_\beta, aP_0+bP_\infty)^\perp = C_{\mathcal{L}}(D_\beta, rP_0+sP_\infty)$ mit $s = n-b-1 = n-(\delta-a-2)-1 = n+1-\delta-l$ und $r = -a-1 = l-1$. □

Satz 1.6.2, der eine Schranke für die Minimaldistanz eines BCH-Codes angab, erhalten wir nun als einfache Folgerung.

Folgerung 3.3.6 *Die Minimaldistanz eines BCH-Codes mit konstruierter Minimaldistanz δ ist mindestens δ.*

Beweis. Nach Satz 3.3.5 können wir einen BCH-Code in der Form $C =$

$C_{\mathcal{L}}(D_\beta, rP_0+sP_\infty)|_{\mathbb{F}_q}$ darstellen. Die Minimaldistanz von $C_{\mathcal{L}}(D_\beta, rP_0+sP_\infty)$ ist nach Satz 3.3.2 und Satz 3.3.5 (b)

$$d = n - \deg(rP_0 + sP_\infty) = n - ((l-1) + (n+1-\delta-l)) = \delta.$$

Da die Minimaldistanz bei der Einschränkung auf $\mathbb{F}_q$ nicht kleiner werden kann, ist die Minimaldistanz von $C \geq \delta$. □

Als nächstes wollen wir zwei Klassen von geometrischen Goppa-Codes betrachten, die auf der P-adischen Potenzreihenentwicklung beruhen, wobei $P \in \mathbb{P}_F$ eine rationale Stelle ist. Die Konstruktionen dieser Codes stammen von Xing, Niederreiter und Lam (siehe [25]), deshalb werden wir sie *XNL-Codes* nennen.

Ab jetzt sei also $F/\mathbb{F}_q$ wieder ein beliebiger algebraischer Funktionenkörper mit Geschlecht g. Gegeben seien $n+1$ verschiedene rationale Stellen $P_\infty, P_1, \ldots, P_n$ und ein Divisor $E \geq 0$ mit $\deg E = 2g$ und $P_\infty \notin \operatorname{supp} E$. Als erstes wollen wir eine spezielle Basis von $\mathcal{L}(E)$ wählen.

Hilfssatz 3.3.7 *Es gibt eine Basis $w_0, w_1, \ldots, w_g$ von $\mathcal{L}(E)$, sodass*

$$\nu_{P_\infty}(w_l) = n_l \quad \textit{mit} \quad 0 = n_0 < n_1 < \cdots < n_g \leq 2g.$$

Beweis. Zunächst gilt nach dem Satz von Riemann-Roch 2.6.4, dass

$$\dim E = g + 1. \tag{3.18}$$

Außerdem folgt $\dim(E - P_\infty) = g$ und $\dim(E - (2g+1)P_\infty) = 0$. Deshalb existieren ganze Zahlen

$$0 = n_0 < n_1 < \cdots < n_g \leq 2g,$$

sodass

$$\dim(E - n_l P_\infty) = \dim(E - (n_l + 1)P_\infty) + 1,$$

für $0 \leq l \leq g$ ist. Für jedes $0 \leq l \leq g$ wählen wir ein Element

$$w_l \in \mathcal{L}(E - n_l P_\infty) \backslash \mathcal{L}(E - (n_l + 1)P_\infty).$$

Nach Konstruktion gilt $\nu_{P_\infty}(w_l) = n_l$. Wegen (3.18) genügt es zu zeigen, dass $w_0, \ldots, w_g$ linear unabhängig über $\mathbb{F}_q$ sind. Angenommen wir haben

$$\sum_{l=0}^{g} a_l w_l = 0$$

mit $a_l \in \mathbb{F}_q$ und $a_k \neq 0$ für ein $0 \leq k \leq g$. Wir nehmen an, dass k minimal mit dieser Eigenschaft ist. Dann gilt

$$a_k w_k = -\sum_{l=k+1}^{g} a_l w_l \neq 0.$$

Nun gilt einerseits: $\nu_{P_\infty}(a_k w_k) = n_k$, andererseits:

$$\nu_{P_\infty}\left(-\sum_{l=k+1}^{g} a_l w_l\right) \geq \min_{k+1 \leq l \leq g} \{\nu_{P_\infty}(w_l)\} = n_{k+1} > n_k.$$

Das ist ein Widerspruch, und damit ist der Hilfssatz bewiesen. □

Wie in der Konstruktion in Kapitel 3.2 (siehe (3.11)) wählen wir für $1 \leq j \leq n$ Elemente

$$f_j \in \mathcal{L}(E + P_j) \backslash \mathcal{L}(E). \tag{3.19}$$

Das ist – genauso wie dort – möglich nach dem Satz von Riemann-Roch 2.6.4, indem wir beachten, dass $\deg E = 2g$ ist.

Hilfssatz 3.3.8 *Die Elemente $w_0, w_1, \ldots, w_g, f_1, f_2, \ldots, f_n$ aus Hilfssatz 3.3.7 bzw. (3.19) sind linear unabhängig über $\mathbb{F}_q$.*

Beweis. Man zeigt dies genauso wie im Beweis von Hilfssatz 3.2.1. □

Wir wählen nun einen lokalen Parameter t für P_∞ und setzen

$$t_r := \begin{cases} t^r & \text{für} \quad r \notin \{n_0, \ldots, n_g\}, \\ w_l & \text{für} \quad r = n_l \in \{n_0, \ldots, n_g\} \end{cases}$$

für $r = 0, 1, 2, \ldots$, wobei $n_0, \ldots, n_g$ wie in Hilfssatz 3.3.7 sind. Dann gilt $\nu_{P_\infty}(t_r) = r$ für alle $r \geq 0$. Jedes f_j besitzt nach Satz 2.7.8 eine P_∞-Potenzreihenentwicklung bezüglich der Folge $(t_r)_{r \geq 0}$ der Form

$$f_j = \sum_{r=0}^{\infty} a_{rj} t_r \tag{3.20}$$

mit $a_{rj} \in \mathbb{F}_q$ (man beachte: wegen $P_\infty \notin \operatorname{supp}(E + P_j)$ für $1 \leq j \leq n$ ist $\nu_{P_\infty}(f_j) \geq 0$).

Wir wählen eine feste ganze Zahl m mit $g \leq m < n$ und definieren den Vektor $c_j \in \mathbb{F}_q^m$ für $1 \leq j \leq n$ durch

$$c_j = (\widehat{a_{n_0 j}}, a_{1j}, \ldots, \widehat{a_{n_1 j}}, \ldots, \widehat{a_{n_g j}}, \ldots, a_{m+g\ j}),$$

wobei $\widehat{\ }$ bedeutet, dass der zugehörige Eintrag weggelassen wird. Der Einfachheit halber schreiben wir

$$c_j = (c_{1j}, c_{2j}, \ldots, c_{mj}).$$

Definieren wir jetzt eine $m \times n$-Matrix H über $\mathbb{F}_q$ durch

$$H = (c_1^T, c_2^T, \ldots, c_n^T) = \begin{pmatrix} c_{11} & c_{12} & \cdots & c_{1n} \\ c_{21} & c_{22} & \cdots & c_{2n} \\ \vdots & \vdots & & \vdots \\ c_{m1} & c_{m2} & \cdots & c_{mn} \end{pmatrix}.$$

Definition 3.3.9 Wir bezeichnen mit $C_F = C_F(P_\infty, P_1, \ldots, P_n; E; m)$ den Linearcode mit Kontrollmatrix H und nennen ihn einen *XNL-Code 1.Art.*

Der Code C_F ist ein Linearcode der Länge n. Wir zeigen zunächst, dass er in die Klasse der geometrischen Goppa-Codes fällt, indem wir ihn auf die Konstruktion in Kapitel 3.2 zurückführen.

Satz 3.3.10 *Gegeben seien $n+1$ verschiedene rationale Stellen $P_\infty, P_1, \ldots, P_n$, ein positiver Divisor E mit $\deg E = 2g$ und $P_\infty \notin \operatorname{supp} E$ und eine positive ganze Zahl m mit $g \leq m < n$. Dann gilt*

$$C_F(P_\infty, P_1, \ldots, P_n; E; m) = C_{\mathcal{NS}}(E; P_1, \ldots, P_n; (m+g+1)P_\infty).$$

Beweis. Seien f_j wie in (3.19) und betrachte ihre P_∞- Potenzreihenentwicklung (3.20). Aus der Definition des Codes C_F wissen wir, dass der Vektor $c = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ genau dann ein Codewort von C_F ist, wenn

$$\sum_{i=1}^{n} a_{ji} c_i = 0 \quad \text{für alle } j \in \{0, \ldots, m+g\} \backslash \{n_0, \ldots, n_g\},$$

wobei die n_i wie in Hilfssatz 3.3.7 definiert werden. Daraus folgt

$$\begin{aligned} \sum_{i=1}^{n} c_i f_i &= \sum_{i=1}^{n} c_i \left(\sum_{r=0}^{\infty} a_{ri} t_r \right) = \sum_{r=0}^{\infty} \left(\sum_{i=1}^{n} c_i a_{ri} \right) t_r \\ &= \sum_{r \in \{n_0, \ldots, n_g\}} \left(\sum_{i=1}^{n} a_{ri} c_i \right) w_r + \sum_{r \geq m+g+1} \left(\sum_{i=1}^{n} a_{ri} c_i \right) t_r \\ &= w + u, \end{aligned}$$

mit $w \in \mathcal{L}(E)$ und u mit $\nu_{P_\infty}(u) \geq m+g+1$. Es folgt, dass

$$u \in \mathcal{L}(E + \sum_{i=1}^{n} P_i - (m+g+1)P_\infty).$$

Daher ist c ein Codewort von $C_{\mathcal{NS}}$.
Umgekehrt sei $c = (c_1, \ldots, c_n)$ ein Codewort von $C_{\mathcal{NS}}$. Dann gibt es ein $f \in \mathcal{L}(E + \sum_{i=1}^{n} P_i - (m+g+1)P_\infty)$, welches sich in der Form

$$f = \sum_{i=1}^{n} c_i f_i + w$$

darstellen läßt, wobei $c_i \in \mathbb{F}_q$ für $i = 1, \ldots, n$ und $w \in \mathcal{L}(E)$ ist. Man beachte, dass nach Hilfssatz 3.3.8 $w_0, \ldots, w_g, f_1, \ldots, f_n$ eine Basis von $\mathcal{L}(D + \sum_{i=1}^{n} P_i)$ bilden. Daher kann jedes Element von

$$\mathcal{L}\left(E + \sum_{i=1}^{n} P_i - (m+g+1)P_\infty\right) \subseteq \mathcal{L}\left(E + \sum_{i=1}^{n} P_i\right)$$

eindeutig in obiger Form geschrieben werden. Betrachten wir die P_∞-Potenzreihenentwicklung von f bezüglich der Folge $(t_r)_{r\in\mathbb{Z}}$, dann erhalten wir mit Hilfe von (3.20)

$$\begin{aligned} f &= \sum_{i=1}^{n} c_i \left(\sum_{r=0}^{\infty} a_{ri} t_r\right) + w = \sum_{r=0}^{\infty} \left(\sum_{i=1}^{n} c_i a_{ri}\right) t_r + w \\ &= \sum_{r \notin \{n_0,\ldots,n_g\}} \left(\sum_{i=1}^{n} c_i a_{ri}\right) t_r + w + \sum_{r \in \{n_0,\ldots,n_g\}} \left(\sum_{i=1}^{n} c_i a_{ri}\right). \end{aligned}$$

Da $\nu_{P_\infty}(f) \geq (m+g+1) - \nu_{P_\infty}(E) = m+g+1$ ist, erhalten wir

$$\sum_{i=1}^{n} c_i a_{ri} = 0$$

für $r \in \{0, \ldots, m+g\} \backslash \{n_0, \ldots, n_g\}$ und

$$w = -\sum_{r \in \{n_0,\ldots,n_g\}} \left(\sum_{i=1}^{n} c_i a_{ri}\right).$$

Damit ist c ein Codewort von C_F und somit der Beweis geführt. □

Folgerung 3.3.11 *Der Linearcode $C_F(P_\infty, P_1, \ldots, P_n; E; m)$ ist ein $[n,k,d]$-Code über $\mathbb{F}_q$ mit*

$$k \geq n - m \quad \textit{und} \quad d \geq m - g + 1.$$

Beweis. Folgt sofort aus Satz 3.3.10 und Satz 3.2.4. □

Wir wollen noch eine zweite Konstruktion betrachten, die ebenfalls auf der Potenzreihenentwicklung an einer rationalen Stelle beruht. Anstatt des Divisors E vom Grad $2g$ verwenden wir diesmal einen nicht speziellen Divisor $D \geq 0$ mit $\deg D = g$, das heißt wir haben $\dim D = 1$. Der folgende Hilfssatz sichert die Existenz eines solchen Divisors.

Hilfssatz 3.3.12 *Der algebraische Funktionenkörper $F/\mathbb{F}_q$ besitzt einen nicht speziellen Divisor $D \geq 0$ mit $\deg D = g$ in jedem der folgenden Fälle:*
(a) *$F/\mathbb{F}_q$ ist der rationale Funktionenkörper.*
(b) *$F/\mathbb{F}_q$ hat Geschlecht $g = 1$ (in diesem Fall nennt man F einen elliptischen Funktionenkörper).*
(c) *$F/\mathbb{F}_q$ hat mindestens vier rationale Stellen, wenn $q = 2$ ist, und mindestens zwei rationale Stellen, wenn $q \geq 3$ gilt.*

Beweis. (a) Wähle D gleich dem Nulldivisor.
(b) Nach der Hasse-Weil-Schranke 2.8.8 besitzt $F/\mathbb{F}_q$ mindestens eine rationale Stelle P. Wähle $D = P$, dann gilt $\deg D = 1 = g$ und $\dim D = 1$ (nach dem Satz von Riemann-Roch 2.6.4).
(c) Einen Beweis findet man z.B. in [13]. □

Seien $P_\infty, P_1, \ldots, P_n$ $n+1$ verschiedene rationale Stellen. Wie vorhin wählen wir für $1 \leq j \leq n$ Elemente

$$g_j \in \mathcal{L}(D + P_j) \backslash \mathcal{L}(D). \tag{3.21}$$

Dies ist aufgrund des Satzes von Riemann-Roch möglich, da D nicht speziell ist (siehe (3.11) und (3.19)). Dann gilt

Hilfssatz 3.3.13 *Die Elemente $1, g_1, \ldots, g_n$ aus (3.21) bilden eine Basis von $\mathcal{L}(D + \sum_{i=1}^{n} P_i)$.*

Beweis. Zeigt man genauso wie im Beweis von Hilfssatz 3.2.1. □

Wähle einen lokalen Parameter t von P_∞ und betrachte die P_∞- adische Potenzreihe von g_j bezüglich t

$$g_j = t^{-v} \cdot \sum_{r=0}^{\infty} b_{rj} t^r$$

wo $v = \nu_{P_\infty}(D) \geq 0$ und alle Koeffizienten $b_{rj} \in \mathbb{F}_q$ sind. Für $1 \leq j \leq n$ definieren wir

$$c_{rj} = \begin{cases} b_{r-1\ j} & \text{für} \quad 1 \leq r \leq v, \\ b_{rj} & \text{für} \quad r \geq v+1. \end{cases}$$

Wir wählen wieder ein festes m mit $g \leq m < n$ und setzen

$$c_j = (c_{1j}, c_{2j}, \ldots, c_{mj}) \in \mathbb{F}_q^m.$$

Schlussendlich definieren wir die $m \times n$-Matrix H durch

$$H = (c_1^T, c_2^T, \ldots, c_n^T).$$

Definition 3.3.14 Der Code $C_S = C_S(P_\infty, P_1, P_2, \ldots, P_n; D; m) \subseteq \mathbb{F}_q^n$ ist der Linearcode mit Kontrollmatrix H. Wir nennen ihn *XNL-Code 2.Art.*

Wie vorhin erhalten wir die folgenden Aussagen:

Satz 3.3.15 *Gegeben seien $n+1$ verschiedene rationale Stellen $P_\infty, P_1, \ldots, P_n$, ein nichtspezieller Divisor $D \geq 0$ mit $\deg D = g$ und eine positive ganze Zahl m mit $g \leq m < n$. Dann gilt*

$$C_S(P_\infty, P_1, \ldots, P_n; D; m) = C_{\mathcal{NS}}(D; P_1, \ldots, P_n; (m+1)P_\infty).$$

Beweis. Der Nachweis verläuft genauso wie Satz 3.3.10. □

Folgerung 3.3.16 *Der Linearcode $C_S(P_\infty, P_1, \ldots, P_n; D; m)$ ist ein $[n, k, d]$-Code über $\mathbb{F}_q$ mit*

$$k \geq n - m \quad \textit{und} \quad d \geq m - g + 1.$$

Beweis. Dies ist eine unmittelbare Folgerung aus Satz 3.3.15 und Satz 3.2.4. □

3.4 Geometrische Goppa-Codes und die asymptotische Gilbert-Varshamov-Schranke

In diesem Abschnitt werden wir sehen, dass geometrische Goppa-Codes eine gute Familie von Codes sind (siehe Definition 1.5.14). Um gute Codes zu konstruieren, benötigen wir lange Codes. Betrachten wir also lange geometrische Goppa-Codes. Gegeben sei ein algebraischer Funktionenkörper $F/\mathbb{F}_q$ mit $N = N(F)$ rationalen Stellen. Dann ist die Länge eines geometrischen Goppa-Codes $C_{\mathcal{L}}(D, G)$ assoziiert zu den Divisoren D und G von F beschränkt durch N, da D die Summe von rationalen Stellen ist. Tatsächlich stellt dies die einzige Einschränkung an die Länge eines geometrischen Goppa-Codes dar.

Hilfssatz 3.4.1 *Seien $P_1, \ldots, P_n$ verschiedene rationale Stellen von $F/\mathbb{F}_q$. Dann gibt es für jedes $r \geq 0$ einen Divisor G mit $\deg G = r$ und $P_i \notin \operatorname{supp} G$*

für $i = 1, \ldots, n$.

Beweis. Der Hilfssatz ist trivial, falls eine weitere rationale Stelle Q existiert, die verschieden von $P_1, \ldots, P_n$ ist. In diesem Fall setzen wir $G := rQ$. Falls $P_1, \ldots, P_n$ alle rationalen Stellen von $F/\mathbb{F}_q$ sind, wählen wir einen Divisor $G \sim rP_1$, sodass $\nu_{P_i}(G) = 0$ ist, für $i = 1, \ldots, n$. Dies ist möglich nach dem schwachen Approximationssatz 2.2.7. □

Die Hasse-Weil-Schranke gibt uns eine Schranke für die Anzahl der rationalen Stellen von $F/\mathbb{F}_q$ an.

Tsfasman, Vlădut und Zink gaben 1982 eine „explizite" Beschreibung einer Folge von geometrischen Goppa-Codes über $\mathbb{F}_{p^2}$, deren Rate und relative Minimaldistanz gegen die asymptotische Gilbert-Varshamov-Schranke konvergieren (siehe [22]). Ihre Konstruktion verwendet so genannte Shimura-Modular-Kurven und benötigt viel algebraische Geometrie. Die Funktionenkörper, die von Tsfasman, Vlădut und Zink verwendet wurden, sind Beispiele für die Richtigkeit des folgenden Satzes, den wir nicht beweisen.

Satz 3.4.2 *Es sei* $q = p^2$ *mit* $p \geq 7$ *eine Primzahl. Dann gibt es eine Familie algebraischer Funktionenkörper* $F^{(\nu)}/\mathbb{F}_{p^2}$ *mit Geschlecht* $g^{(\nu)} = g(F^{(\nu)}) \longrightarrow \infty$ *so, dass die Anzahl* $N^{(\nu)} = N(F^{(\nu)})$ *der rationalen Stellen gegen unendlich konvergiert, aber* $g^{(\nu)}/N^{(\nu)}$ *gegen* $1/(p-1)$ *geht.*

Beweis. Einen Beweis findet man in [21]. □

Mit Hilfe dieses Satzes kann man die Existenz einer guten Familie von geometrischen Goppa-Codes sofort ableiten. Zunächst definieren wir:

Definition 3.4.3
(a) $N_q(g) := \max\{N(F) \mid F$ ist ein algebraischer Funktionenkörper über $\mathbb{F}_q$ mit Geschlecht $g\}$.
(b) $A(q) := \limsup_{g \to \infty} N_q(g)/g$.

Satz 3.4.4 (Drinfeld-Vlădut-Schranke) $A(q) \leq q^{1/2} - 1$.

Beweis. Einen Beweis, der den Satz von Hasse-Weil 2.8.7 verwendet, findet man z.B. in [19]. □

Folgerung 3.4.5 $A(q) = q^{1/2} - 1$, *falls* $q = p^2$ *mit* $p \geq 7$ *eine Primzahl ist.*

Beweis. Folgt aus Satz 3.4.2 und der Drinfeld-Vlădut-Schranke 3.4.4. □

Es sei bemerkt, dass Satz 3.4.2 und Folgerung 3.4.5 bereits dann gelten, wenn q ein Quadrat ist.

Satz 3.4.6 *Es sei $A(q) > 1$. Dann gibt es für alle $0 \leq \delta \leq 1 - A(q)^{-1}$ eine Folge von Linearcodes $C_n \subseteq \mathbb{F}_q^n$, sodass die relative Minimaldistanz gegen eine Zahl $\geq \delta$ und die Rate gegen eine Zahl $\geq (1 - A(q)^{-1}) - \delta$ konvergieren.*

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

$$g_i \longrightarrow \infty \quad \text{und} \quad n_i/g_i \longrightarrow A(q), \tag{3.22}$$

wobei $n_i := N(F_i)$ ist. Das ist möglich, sofern $n_i \to \infty$ für $i \to \infty$ strebt. Wähle $r_i > 0$, sodass

$$r_i/n_i \longrightarrow 1 - \delta. \tag{3.23}$$

Sei D_i die Summe aller rationalen Stellen von $F_i/\mathbb{F}_q$, dann ist $\deg D_i = n_i$. Nach Hilfssatz 3.4.1 gibt es einen Divisor G_i von $F_i/\mathbb{F}_q$ mit $\deg G_i = r_i$ und $\operatorname{supp} G_i \cap \operatorname{supp} D_i = \emptyset$. Betrachte die Codes $C_i := \mathcal{L}(D_i, G_i)$. Diese C_i sind $[n_i, k_i, d_i]$-Codes, deren Parameter k_i und d_i nach Folgerung 3.1.3 folgendermaßen abgeschätzt werden können:

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

Daher gilt

$$R_i := \frac{k_i}{n_i} \geq \frac{r_i + 1}{n_i} - \frac{g_i}{n_i} \quad \text{und} \quad \delta_i := \frac{d_i}{n_i} \geq 1 - \frac{r_i}{n_i}. \tag{3.24}$$

Wir können o.B.d.A. annehmen, dass die Folgen $(R_i)_{i \geq 1}$ und $(\delta_i)_{i \geq 1}$ konvergieren, andernfalls betrachten wir geeigenete Teilfolgen. Gelte $R_i \to R$ und $\delta_i \to \tilde{\delta}$. Aus (3.22), (3.23) und (3.24) folgt $R \geq 1 - \delta - A(q)^{-1}$ und $\tilde{\delta} \geq \delta$ und damit die Behauptung. □

Als unmittelbare Folgerung erhalten wir:

Satz 3.4.7 (Tsfasman-Vlădut-Zink-Schranke) *Es sei $q = p^2$ mit $p \geq 7$ eine Primzahl. Dann gibt es für alle $0 \leq \delta \leq 1 - 1/(p-1)$ eine Folge von Linearcodes $C_n \subseteq \mathbb{F}_q^n$ so, dass die relative Minimaldistanz gegen eine Zahl $\geq \delta$ und die Rate gegen eine Zahl $\geq (1 - 1/(p-1)) - \delta$ konvergieren.*

Beweis. Folgt sofort aus Satz 3.4.5 und Satz 3.4.6. □

Falls $q = p^2 \geq 49$ ist, dann ist die Tsfasman-Vlădut-Zink-Schranke in einem gewissen Intervall besser als die Gilbert-Varshamov-Schranke. Das

heißt, dass geometrische Goppa-Codes die Gilbert-Varshamov-Schranke nicht nur erreichen, sondern sie sogar noch übertreffen.

Satz 3.4.8 *Sei $q = p^2$ mit $p \geq 7$ eine Primzahl. Dann ist für $\delta = (q - 1)/(2q-1)$ die Tsfasman-Vlădut-Zink-Schranke besser als die Gilbert-Varshamov-Schranke.*

Beweis. Für $p = 7$ berechnen wir $\log_{49}(97) \approx 1.1755 > 7/6$. Daher ist $1/(p-1) < \log_q(2q-1) - 1$. Da die linke Seite dieser Ungleichung mit wachsendem p stärker fällt als die rechte Seite, bleibt die Ungleichung für größer werdende p richtig. Daher gilt in diesem Fall,

$$(1 - 1/(p-1)) - \delta > 1 - \delta - \log_q(2q-1) + 1 = 1 - H_q(\delta),$$

woraus die Behauptung folgt. □

H. Niederreiter und C. P. Xing konnten im Jahr 1998 sogar noch eine weitere Verbesserung erzielen: Sie zeigten, dass für q kein Quadrat und keine Primzahl die asymptotische Gilbert-Varshamov-Schranke, mit Hilfe von geometrischen Goppa-Codes, immer noch gebrochen werden kann. Details dazu findet man in [14].

Die Bedeutung der AG-Codes liegt also darin, dass sie hervorragende asymptotische Eigenschaften besitzen. Um diese nützen zu können benötigt man aber möglichst viele rationale Stellen. Wenn der Funktionenkörper $F/\mathbb{F}_q$ Geschlecht $g = 0$ hat, dann gibt es nach der Hasse-Weil-Schranke 2.8.8 genau $q + 1$ rationale Stellen. Wir müssen also Funktionenkörper mit Geschlecht $g > 0$ betrachten. Der Preis den man aber dafür zu zahlen hat, ist der, dass das Rechnen in einem solchen Funktionenkörper wesentlich schwieriger ist. Insbesondere die Berechnung des Geschlechts stellt ein großes Problem dar. Aus diesem Grund haben wir auch keine explizite Angabe von Codes, welche die asymptotische Gilbert-Varshamov-Schranke erreichen, kennengelernt (solche expliziten Darstellungen gibt es z.B. seit kurzem auch von Garcia und Stichtenoth, siehe [18]).

Kapitel 4

Verallgemeinerte AG-Codes

In diesem Kapitel wollen wir Goppas Methode, Codes mit Hilfe von algebraischen Funktionenkörpern zu konstruieren, in dem Sinn verallgemeinern, dass die Verwendung von Stellen beliebig hohen Grades zugelassen wird. Damit ist es möglich Linearcodes zu konstruieren, die alle bisher dagewesenen übertreffen. Diese Resultate stammen von Xing, Niederreiter und Lam (siehe [15], [26] und [16]).

4.1 Konstruktion nach Xing - Niederreiter - Lam

Die Idee dieser Konstruktion besteht darin, einige „innere“ Codes mit einem „äußeren“ Code - einem AG-Code - zu verknüpfen, um einen neuen Code zu gewinnen.

Wir betrachten also wieder einen algebraischen Funktionenkörper $F/\mathbb{F}_q$ mit Geschlecht g. Gegeben seien s verschieden Stellen $P_1, \ldots, P_s$ und ein Divisor G von F mit $\operatorname{supp} G \cap \{P_1, \ldots, P_s\} = \emptyset$. Für $i = 1, \ldots, s$ seien lineare $[n_i, k_i = \deg P_i, d_i]$-Codes $C_i \subseteq \mathbb{F}_q^{n_i}$ gegeben. Weiters seien $\pi_i : F_{P_i} \to C_i$ fest gewählte $\mathbb{F}_q$-lineare Isomorphismen vom Restklassenkörper F_{P_i} auf den Linearcode C_i. Wir betrachten jetzt die Abbildung

$$\pi : \begin{cases} \mathcal{L}(G) & \longrightarrow & \mathbb{F}_q^n, \\ f & \longmapsto & (\pi_1(f(P_1)), \ldots, \pi_s(f(P_s))), \end{cases} \tag{4.1}$$

wobei $n = \sum_{i=1}^{s} n_i$ gilt. Klarerweise ist π eine $\mathbb{F}_q$-lineare Abbildung. Wir definieren:

Definition 4.1.1 Wir nennen

$$C(P_1, \ldots, P_s; G; C_1, \ldots, C_s) := \pi(\mathcal{L}(G))$$

einen *verallgemeinerten AG-Code.*

Offensichtlich ist $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ ein Linearcode über $\mathbb{F}_q$ der Länge n. Außerdem ist klar, dass, falls alle Stellen P_i rational und $n_i = k_i = d_i = 1$ für $1 \leq i \leq s$ gewählt werden, $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ ein geometrischer Goppa-Code ist. Wenn man nämlich $\pi_i = id_{\mathbb{F}_q}$ wählt für $i = 1, \ldots, s$, dann ist $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s) = C_{\mathcal{L}}(P_1 + \cdots + P_n, G)$. In jedem anderen Fall erhält man einen zu $C_{\mathcal{L}}(P_1 + \cdots + P_n, G)$ äquivalenten Code.

Als nächstes wollen wir Abschätzungen für die Parameter von $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ herleiten. Wir zeigen zuerst den folgenden Hilfssatz:

Hilfssatz 4.1.2 *Mit den Notationen von oben gilt: Falls*

$$\deg G < \sum_{i=1}^{n} k_i,$$

dann ist π injektiv.

Beweis. Sei $h \in \mathcal{L}(G)$ mit $\pi(h) = 0$. Dann ist auch

$$\pi_i(h(P_i)) = 0 \quad \text{für alle } 1 \leq i \leq s.$$

Damit ist $h(P_i) = 0$ für alle $1 \leq i \leq s$, da die π_i Isomorphismen sind. Es folgt

$$h \in \mathcal{L}\left(G - \sum_{i=1}^{s} P_i\right).$$

Wegen

$$\deg G < \sum_{i=1}^{s} k_i = \deg\left(\sum_{i=1}^{s} P_i\right)$$

folgt $h = 0$ und damit die Behauptung. □

Satz 4.1.3 *Seien die Bezeichnungen wie oben. Außerdem gelte wieder*

$$\deg G < \sum_{i=1}^{s} k_i.$$

Dann ist $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ ein $[n, k, d]$-Code mit den Parametern

$$\begin{aligned} k &\geq \deg G + 1 - g, \\ d &\geq \sum_{i=1}^{s} d_i - \deg G - \max_{R}\left\{\sum_{i \in R}(d_i - k_i)\right\}, \end{aligned}$$

wobei das Maximum über alle Teilmengen R von $\{1, 2, \ldots, s\}$ gebildet, und eine leere Summe, wie gewöhnlich, als 0 definiert wird.
Weiters gilt: $k = \deg G + 1 - g$, falls $\deg G \geq 2g - 1$.

Beweis. Es folgt sofort aus Hilfssatz 4.1.2 und dem Satz von Riemann-Roch 2.6.4, dass

$$k = \dim \mathcal{L}(G) = \dim G \geq \deg G + 1 - g,$$

mit Gleichheit, falls $\deg G \geq 2g - 1$ ist.
Wählen wir jetzt ein Element $f \in \mathcal{L}(G)$ so, dass das Codewort $\pi(f)$ Gewicht d hat. Wir können annehmen, dass $f \neq 0$ sei, da sonst der Code trivial ist. Sei

$$S = \{i \in \{1, 2, \ldots, s\} \mid f(P_i) = 0\}. \tag{4.2}$$

Da $0 \neq f \in \mathcal{L}(G - \sum_{i \in S} P_i)$ gilt, folgt

$$\deg G \geq \deg \left(\sum_{i \in S} P_i \right) = \sum_{i \in S} k_i = \sum_{i \in S} d_i - \sum_{i \in S} (d_i - k_i).$$

Andererseits gilt

$$d = \mathrm{wt}(\pi(f)) = \sum_{i=1}^{s} \mathrm{wt}(\pi_i(f(P_i))) = \sum_{i \notin S} \mathrm{wt}(\pi_i(f(P_i))) \geq \sum_{i \notin S} d_i.$$

Wenn wir diese beiden Ungleichungen kombinieren, erhalten wir

$$\mathrm{wt}(\pi(f)) + \deg G \geq \sum_{i=1}^{s} d_i - \sum_{i \in S} (d_i - k_i)$$

und daraus folgt die gewünschte Schranke für d. □

Folgerung 4.1.4 *Zusätzlich zu den Voraussetzungen in Satz 4.1.3 gelte $k_i \geq d_i$ für $1 \leq i \leq s$. Dann gilt für die Minimaldistanz d von $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$*

$$d \geq \sum_{i=1}^{s} d_i - \deg G.$$

Beweis. Folgt sofort aus Satz 4.1.3. □

Folgerung 4.1.5 *Es gelten die Voraussetzungen von Satz 4.1.3. Für die Minimaldistanz d von $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ folgt dann*

$$d \geq \delta := \min \left\{ \sum_{i \notin S} d_i \;\middle|\; S \in X \right\},$$

wobei die Menge X folgendermaßen definiert ist:

$$X := \left\{ S \subseteq \{1, 2, \ldots, s\} \;\middle|\; \sum_{i \in S} k_i \leq \deg G \right\}.$$

Beweis. Sei $0 \neq f \in \mathcal{L}(G)$, sodass das Codewort $\pi(f)$ Gewicht d hat. Im Beweis des letzten Satzes haben wir folgende Ungleichungen gezeigt:

$$\deg G \geq \sum_{i \in S} k_i \quad \text{und} \quad d \geq \sum_{i \notin S} d_i,$$

wobei S durch (4.2) definiert ist. Daraus folgt die Behauptung. □

Man beachte, dass die Folgerung 3.1.3, welche die Abschätzungen für die Parameter eines geometrischen Goppa-Codes $C_{\mathcal{L}}(D, G)$ – im Fall, dass $\deg G < n$ ist – liefert, jetzt ein Spezialfall von Satz 4.1.3 ist. Außerdem sei bemerkt, dass sich jeder lineare $[n, k, d]$-Code über $\mathbb{F}_q$ in trivialer Weise als ein verallgemeinerter AG-Code realisieren läßt: Sei $F = \mathbb{F}_q(x)$ der rationale Funktionenkörper, P_∞ der Pol von x und wähle eine Stelle $P \in \mathbb{P}_F$ mit Grad $\deg P = k$. Sei $\pi : F_P \to C$ ein $\mathbb{F}_q$-linearer Isomorphismus. Dann gilt

$$C = C(P; (k-1)P_\infty; C),$$

da die Abbildung $\mathcal{L}((k-1)P_\infty) \to C \subseteq \mathbb{F}_q^n$ definiert durch $f \mapsto \pi(f(P))$ nach Hilfssatz 4.1.2 injektiv, und nach dem schwachen Approximationssatz 2.2.7 surjektiv ist.

Wir wollen noch eine spezielle Klasse von Codes untersuchen, die eine Verallgemeinerung der Konstruktion von Xing - Niederreiter - Lam und Özbudak - Stichtenoth ist und von Xing, Niederreiter und Lam stammt (siehe [15]). Auch bei dieser Konstruktion werden Stellen beliebigen Grades verwendet. Wir werden sehen, dass es sich dabei um spezielle verallgemeinerte AG-Codes handelt.

Wie immer sei $F/\mathbb{F}_q$ ein algebraischer Funktionenkörper mit Geschlecht g. Wir wählen einen nicht speziellen Divisor B und s verschiedene Stellen $P_1, \ldots, P_s$ vom Grad $\deg P_i = k_i$ $(i = 1, \ldots, s)$. Weiters setzen wir

$$n = \sum_{i=1}^{s} k_i.$$

Da B nicht speziell ist und $B + P_i \geq B$ für $1 \leq i \leq s$ folgt nach Hilfssatz 2.6.12

$$\dim(B + P_i) = \dim B + k_i.$$

Daher können wir k_i Elemente $f_{i,1}, \ldots, f_{i,k_i} \in \mathcal{L}(B + P_i)$ finden, die linear unabhängig modulo $\mathcal{L}(B)$ sind. Es gilt dann der folgende Hilfssatz:

Hilfssatz 4.1.6 *Die n Elemente $f_{1,1}, \ldots, f_{1,k_1}, f_{2,1}, \ldots, f_{s,k_s}$ bilden eine Basis von $\mathcal{L}(B + \sum_{i=1}^{s} P_i)$ modulo $\mathcal{L}(B)$.*

Beweis. Mit demselben Argument wie zuvor sieht man:

$$\dim\left(B + \sum_{i=1}^{s} P_i\right) = \dim B + n.$$

Daher genügt es zu zeigen, dass $f_{1,1}, \ldots, f_{1,k_1}, f_{2,1}, \ldots, f_{s,k_s}$ linear unabhängig modulo $\mathcal{L}(B)$ über $\mathbb{F}_q$ sind. Angenommen, dass

$$w + \sum_{i=1}^{s} h_i = 0,$$

wobei $w \in \mathcal{L}(B)$ und h_i eine $\mathbb{F}_q$-Linearkombination von $f_{i,1}, \ldots, f_{i,k_i}$ für $1 \leq i \leq s$ ist. Wir können $h_j \notin \mathcal{L}(B)$ für mindestens ein $1 \leq j \leq s$ annehmen. Dann schreiben wir die letzte Gleichung um in

$$-h_j = w + \sum_{i=1, i\neq j}^{s} h_i.$$

Es ist $h_j \in \mathcal{L}(B + P_j) \backslash \mathcal{L}(B)$ und daher

$$\nu_{P_j}(-h_j) = \nu_{P_j}(h_j) \leq -\nu_{P_j}(B) - 1.$$

Andererseits erhalten wir aus $h_i \in \mathcal{L}(B + P_i)$ für $1 \leq i \leq s$

$$\nu_{P_j}\left(w + \sum_{i=1, i\neq j}^{s} h_i\right) \geq -\nu_{P_j}(B),$$

was ein Widerspruch ist. Damit gilt die Behauptung. □

Aus Hilfssatz 4.1.6 folgt nun, dass jedes $f \in \mathcal{L}(B + \sum_{i=1}^{s} P_i)$ eine eindeutige Darstellung der Form

$$f = \sum_{i=1}^{s} \sum_{j=1}^{k_i} c_{i,j} f_{i,j} + w$$

mit $c_{i,j} \in \mathbb{F}_q$ und $w \in \mathcal{L}(B)$ besitzt. Wie in Abschnitt 3.2 erhalten wir eine surjektive $\mathbb{F}_q$-lineare Abbildung

$$\alpha : \left\{ \begin{array}{ccc} \mathcal{L}(B + \sum_{i=1}^{s} P_i) & \longrightarrow & \mathbb{F}_q^n, \\ f & \longmapsto & (c_{1,1}, \ldots, c_{s,k_s}) \end{array} \right. \tag{4.3}$$

mit dem Kern $\ker(\alpha) = \mathcal{L}(B)$.

Sei A ein weiterer Divisor, sodass

$$A \geq 0 \quad \text{und} \quad \operatorname{supp} A \cap \{P_1 \ldots, P_s\} = \emptyset$$

gilt. Der Grad von A sei m mit $g < m \leq n$. Wir definieren:

Definition 4.1.7 Seien $B, P_1, \ldots, P_s, A$ und die Abbildung α wie oben festgelegt. Dann definieren wir den Code $C_{V\text{-}\mathcal{NS}}(B; P_1, \ldots, P_s; A) \subseteq \mathbb{F}_q^n$ durch

$$C_{V\text{-}\mathcal{NS}} := C_{V\text{-}\mathcal{NS}}(B; P_1, \ldots, P_n; A) = \alpha\left(\mathcal{L}\left(B + \sum_{i=1}^{s} P_i - A\right)\right).$$

Diese Konstruktion ist eine offensichtliche Verallgemeinerung der Konstruktion in Abschnitt 3.2. Wir zeigen jetzt, dass es sich beim Code $C_{V\text{-}\mathcal{NS}}(B; P_1 \ldots, P_s; A)$ um einen verallgemeinerten AG-Code handelt.

Satz 4.1.8 *Seien $A, B, P_1, \ldots, P_s$ wie vorhin. Dann ist $C_{V\text{-}\mathcal{NS}}(B; P_1, \ldots, P_s; A)$ äquivalent zu $C(P_1, \ldots, P_s; G; C_1, \ldots, C_s)$ mit*

$$C_i = \mathbb{F}_q^{k_i} \quad \textit{und} \quad [n_i, k_i, d_i] = [k_i, k_i, 1],$$

wobei $k_i = \deg P_i$ für $i = 1, \ldots, s$ ist und

$$G \sim B + \sum_{i=1}^{s} P_i - A.$$

Beweis. Zunächst findet man mit dem schwachen Approximationssatz 2.2.7 ein Element z mit

$$\nu_{P_i}(z) = \nu_{P_i}(B + P_i), \quad \text{für} \quad i = 1, \ldots, s.$$

Dann ist $\nu_{P_i}(zf_{i,j}) = \nu_{P_i}(z) + \nu_{P_i}(f_{i,j}) = 0$ und die Restklassen

$$(zf_{i,j})(P_i), \quad j = 1, \ldots, k_i$$

bilden eine Basis des Restklassenkörpers F_{P_i} über $\mathbb{F}_q$. Angenommen wir haben nämlich eine nicht triviale $\mathbb{F}_q$-Linearkombination

$$\sum_{j=1}^{k_i} a_j (zf_{i,j})(P_i) = 0$$

mit $a_j \in \mathbb{F}_q$. Dann gilt einerseits

$$\sum_{j=1}^{k_i} a_j (z f_{i,j}) \in P_i.$$

Andererseits ist aber, wegen $a_j(zf_{i,j}) \in \mathcal{O}_{P_i}^*$,

$$\sum_{j=1}^{k_i} a_j (z f_{i,j}) \in \mathcal{O}_{P_i}^*,$$

was nicht gleichzeitig möglich sein kann.
Wir definieren die lineare Abbildung

$$\pi_i : \left\{ \begin{array}{ccc} F_{P_i} & \longrightarrow & C_i := \mathbb{F}_q^{k_i}, \\ (zf_{i,j})(P_i) & \longmapsto & e_j^{(i)} \end{array} \right.$$

wobei $e_j^{(i)} = (0, \ldots, 0, 1, 0, \ldots, 0) \in \mathbb{F}_q^{k_i}$ den j-ten Vektor der kanonischen Basis von $\mathbb{F}_q^{k_i}$ bezeichnet. Weiters sei der Divisor

$$G := B + \sum_{i=1}^{s} P_i - A - (z).$$

Offensichtlich ist G äquivalent zu $B + \sum_{i=1}^{s} P_i - A$. Weiters definieren wir die Abbildung

$$\varphi : \left\{ \begin{array}{ccc} \mathcal{L}(B + \sum_{i=1}^{s} P_i - A) & \longrightarrow & \mathcal{L}(G) \\ f & \longmapsto & zf. \end{array} \right.$$

Die Abbildung φ ist ein $\mathbb{F}_q$-linearer Isomorphismus (siehe Hilfssatz 2.4.9 (b)). Wie im Beweis von Satz 3.2.3 betrachten wir das Diagramm

$$\begin{array}{ccc} \mathcal{L}\left(B + \sum_{i=1}^{s} P_i - A\right) & \longrightarrow & \mathcal{L}(G) \\ & \searrow \quad \swarrow & \\ & \mathbb{F}_q^n & \end{array}$$

wobei $\alpha : \mathcal{L}(B + \sum_{i=1}^{s} P_i - A) \to \mathbb{F}_q^n$ durch (4.3) und $\pi : \mathcal{L}(G) \to \mathbb{F}_q^n$ durch (4.1) definiert sind. Wie man leicht sieht ist dieses Diagramm kommutativ. Sei nämlich

$$f \in \mathcal{L}\left(B + \sum_{i=1}^{n} P_i - A\right).$$

Wir setzen

$$f = \sum_{i=1}^{s} \sum_{j=1}^{k_i} c_{i,j} f_{i,j} + w$$

mit $c_{i,j} \in \mathbb{F}_q$ und $w \in \mathcal{L}(B)$ (das geht nach Hilfssatz 4.1.6). Dann ist $(c_{1,1}, \ldots, c_{s,k_s}) = \alpha(f)$. Andererseits gilt

$$\begin{aligned} \pi_l((zf)(P_l)) &= \pi_l\left(\left(\sum_{i=1}^{s}\sum_{j=1}^{k_i} c_{i,j}(zf_{i,j}) + zw\right)(P_l)\right) \\ &= \pi_l\left(\sum_{j=1}^{k_l} c_{l,j}(zf_{l,j})(P_l)\right) \\ &= \sum_{j=1}^{k_l} c_{l,j}e_j^{(l)} = (c_{l,1}, \ldots, c_{l,k_l}) \end{aligned}$$

für alle $1 \leq l \leq s$, nach Wahl von z und da $\nu_{P_l}(zf_{i,j}) = \nu_{P_l}(z) + \nu_{P_l}(f_{i,j}) \geq \nu_{P_l}(B) + 1 - \nu_{P_l}(B) = 1 > 0$ für $l \neq i$ und genauso $\nu_{P_l}(zw) \geq 1 > 0$ ist. Also ist $\pi(\varphi(f)) = \alpha(f)$. Daher gilt

$$\begin{aligned} C_{V\text{-}\mathcal{NS}} = \alpha\left(\mathcal{L}\left(B + \sum_{i=1}^{s} P_i - A\right)\right) &= \pi(\mathcal{L}(G)) \\ &= C(P_1, \ldots, P_s; G; \mathbb{F}_q^{k_1}, \ldots, \mathbb{F}_q^{k_s}). \end{aligned}$$

□

Als Folgerung können wir jetzt die Parameter des Codes $C_{V\text{-}\mathcal{NS}}(B; P_1, \ldots, P_s; A)$ abschätzen. Man beachte auch hier wieder, die offensichtliche Verallgemeinerung von Satz 3.2.4.

Satz 4.1.9 *Sei B ein nicht spezieller Divisor, und $P_1, \ldots, P_s$ verschiedene Stellen von $F/\mathbb{F}_q$. Weiters sei A ein positiver Divisor von F mit $g < \deg A \leq n$ und $\operatorname{supp} A \cap \{P_1, \ldots, P_s\} = \emptyset$. Dann ist $C_{V\text{-}\mathcal{NS}}(B; P_1, \ldots, P_s; A)$ ein linearer $[n, k, d]$-Code über $\mathbb{F}_q$ mit*

$$n = \sum_{i=1}^{s} k_i, \quad k \geq \deg B - \deg A + n + 1 - g, \quad d \geq \delta,$$

wobei $k_i = \deg P_i$ für $1 \leq i \leq s$ und δ die kleinste Kardinalität einer Teilmenge R von $\{1, \ldots, s\}$ ist, für welche $\sum_{i \in R} k_i \geq \deg A - \deg B$ gilt. Weiters folgt: $k = \deg B - \deg A + n + 1 - g$, falls $\deg B - \deg A + n + 1 - g \geq g$.

Beweis. Folgt sofort aus Satz 4.1.8, Satz 4.1.3 und Folgerung 4.1.5. □

Eine weitere untere Schranke für δ erhält man, indem man $R \subseteq \{1, \ldots, s\}$ mit $\sum_{i \in R} k_i \geq \deg A - \deg B$ und $|R| = \delta$ nimmt und beachtet, dass

$$\deg A - \deg B \leq \sum_{i \in R}((k_i - 1) + 1) \leq \sum_{i=1}^{s}(k_i - 1) + \delta.$$

Dann gilt nämlich

$$\delta \geq \deg A - \deg B - \sum_{i=1}^{s}(k_i - 1).$$

Im nächsten Abschnitt werden wir sehen, welchen Gewinn verallgemeinerten AG-Codes gegenüber Goppas Konstruktion bedeuten.

4.2 Gewinn gegenüber Goppas Konstruktion

In diesem Abschnitt wollen wir zunächst zeigen, dass verallgemeinerte AG-Codes besser sind als geometrische Goppa-Codes. Indem wir Stellen höheren Grades verwenden, können wir nämlich mit der letzten Konstruktion in Abschnitt 4.1, Codes gewinnen, die eine bessere Schranke für $k + d$ haben, als geometrische Goppa-Codes.

Wir bezeichnen mit $g_q(N)$ das kleinste g, sodass ein algebraischer Funktionenkörper $F/\mathbb{F}_q$ mit Geschlecht g und mit mindestens N rationalen Stellen existiert. Der hier verwendete Wert für $g_q(N)$ stammt aus einer Tabelle von [12].

Sei F der rationale Funktionenkörper über $\mathbb{F}_2$. Für $P_1, \ldots, P_s$ wählen wir drei rationale Stellen von $F/\mathbb{F}_2$, eine Stelle vom Grad 2, und zwei Stellen vom Grad 3. A sei eine Stelle von $F/\mathbb{F}_2$ vom Grad 7 und B sei ein nicht spezieller Divisor von $F/\mathbb{F}_2$, zum Beispiel einer dessen Existenz nach Satz 3.3.12 gesichert ist. Dann erhalten wir einen binären Linearcode $C_{V\text{-}\mathcal{NS}}(B; P_1, \ldots, P_s; A)$ der Länge 11 und nach Satz 4.1.9 gilt $k + d \geq 8$. Goppas Konstruktion liefert uns – zum Vergleich – nur einen binären Linearcode der Länge 11 mit $k + d \geq 11 - g_2(11) + 1 = 4$.

Auf diese Art und Weise lassen sich leicht weiter Beispiele erzeugen, welche die Schwäche Goppas Konstruktion aufzeigen.

Zum Schluß wollen wir noch einige Beispiele für verallgemeinerte AG-Codes präsentieren, welche die derzeit besten mit diesen Parametern sind. Dabei betrachten wir q-äre Linearcodes für $q = 2, 3$. Bekanntlich ist es schwierig, gute q-äre geomtetrische Goppa-Codes für kleine q zu bekommen.

Wir denken uns die Stellen von $F/\mathbb{F}_q$ mit nichtabsteigendem Grad aufgelistet und es seien $P_1, P_2, \ldots, P_s$ die ersten s Stellen von dieser Liste. Wir

wählen stets einen Divisor G mit $\deg G = m$ und $\operatorname{supp} G \cap \{P_1, \ldots, P_s\} = \emptyset$. Die abgeschätzten Parameter erhält man bei allen Beispielen aus Satz 4.1.3 und Folgerung 4.1.4.

1. Beispiel: Sei $F = \mathbb{F}_2(x, y)$ der durch

$$y^2 + xy = x^3 + x$$

definierte Funktionenkörper. Das Geschlecht von F ist 1 und die Zetafunktion von F lautet

$$Z(t) = \frac{2t^2 + t + 1}{(1-t)(1-2t)}.$$

Außerdem gilt $B_1 = 4, B_2 = 2, B_3 = 0, B_4 = 2$ (B_r bezeichnet die Anzahl der Stellen von Grad r).

(a) Wenn wir $s = 6$, $[n_i, k_i, d_i] = [1, 1, 1]$ für $1 \leq i \leq 4$, und $[n_i, k_i, d_i] = [3, 2, 2]$ für $i = 5, 6$ setzen, erhalten wir einen binären Linearcode $C(P_1, \ldots, P_6; G; C_1, \ldots, C_6)$ mit Parametern

$$[10, m, 8 - m], \quad \text{für} \quad 1 \leq m \leq 7.$$

(b) Wenn wir $s = 7$, $[n_i, k_i, d_i] = [1, 1, 1]$ für $1 \leq i \leq 4$, $[n_i, k_i, d_i] = [3, 2, 2]$ für $i = 5, 6$ und $[n_7, k_7, d_7] = [8, 4, 4]$ setzen, erhalten wir einen binären Linearcode $C(P_1, \ldots, P_7; G; C_1, \ldots, P_7)$ mit Parametern

$$[18, m, 12 - m], \quad \text{für} \quad 1 \leq m \leq 11.$$

2. Beispiel: Sei $F = \mathbb{F}_3(x, y)$ der durch

$$y^2 = 2x^4 + x^2 + 1$$

definierte Funktionenkörper. Das Geschlecht von F ist 1 und die Zetafunktion von F lautet

$$Z(t) = \frac{3t^2 + 2t + 1}{(1-t)(1-3t)}.$$

Außerdem gilt $B_1 = 6, B_2 = 3, B_3 = 4$.

(a) Wenn wir $s = 7$, $[n_i, k_i, d_i] = [1, 1, 1]$ für $1 \leq i \leq 6$ und $[n_7, k_7, d_7] = [3, 2, 2]$ wählen, erhalten wir einen Linearcode $C(P_1, \ldots, P_7; G; C_1, \ldots, C_7)$ über $\mathbb{F}_3$ mit Parametern

$$[9, m, 8 - m], \quad \text{für} \quad 1 \leq m \leq 7.$$

(b) Wenn wir $s = 9$, $[n_i, k_i, d_i] = [1, 1, 1]$ für $1 \leq i \leq 6$ und $[n_i, k_i, d_i] = [3, 2, 2]$ für $7 \leq i \leq 9$ wählen, erhalten wir einen Linearcode $C(P_1, \ldots, P_9; G; C_1, \ldots, C_9)$ über $\mathbb{F}_3$ mit den Parametern

$$[15, m, 12 - m], \quad \text{für} \quad 1 \leq m \leq 11.$$

Die folgende Tabelle gibt eine Reihe von Codes aus den letzten Beispielen an, die bestmöglich sind, in dem Sinne, dass die Minimaldistanz eine bekannte obere Schranke für die Minimaldistanz d eines q-ären Linearcodes von gegebener Länge n und Dimension k erreicht.

q	$[n, k, d]$	Beispiel
2	$[10, 2, 6]$	1(a)
2	$[10, 3, 5]$	1(a)
2	$[10, 4, 4]$	1(a)
2	$[18, 4, 8]$	1(b)
3	$[9, 2, 6]$	2(a)
3	$[15, 3, 9]$	2(b)

Weitere Beispiele, welche zeigen wie gut verallgemeinerte AG-Codes sind, findet man in [5] und [26].

Die verallgemeinerten AG-Codes sind also eine effektive und weitreichende Verallgemeinerung der geometrischen Goppa-Codes. Es bleibt die Hoffnung, dass damit in Zukunft Linearcodes mit guten Fehlerkorrektureigenschaften konstruiert werden können. Dabei sind natürlich noch viele Probleme offen:

- Für die Konstruktion von verallgemeinerten AG-Codes benötigt man Funktionenkörper mit einer ausgewogenen Balance zwischen der Anzahl der Stellen kleinen Grades. Nach einem bekannten Prinzip (siehe [21]) besitzt nämlich ein Funktionenkörper mit maximal vielen rationalen Stellen bei gegebenen Geschlecht nur wenige Stellen anderer kleiner Grade. Wie kann man also geeignete Funktionenkörper wählen?
- Wie sehen Decodierungsalgorithmen für verallgemeinerte AG-Codes aus? Können damit auch interessante Rückschlüsse auf geometrische Goppa-Codes gemacht werden?
- Gibt es eine einfachere Theorie für geometrische Goppa-Codes und verallgemeinerte AG-Codes?
- Was passiert, wenn man andere bekannte Methoden der Codierungstheorie auf geometrische Goppa-Codes oder verallgemeinerte AG-Codes anwendet?

Wenn diese Probleme gelöst sind, könnten Codes, die von algebraischen Funktionenkörpern kommen, in Zukunft vielleicht die entscheidende Rolle in der Codierungstheorie spielen.

Literaturverzeichnis

[1] E. Artin: *Algebraic numbers and algebraic functions*, Gordon and Breach, New York, 1967.

[2] R. C. Bose and D. K. Ray-Chaudhuri: "On a class of error correcting binary group codes", *Info. and Control* **3**, 68 - 79, 1960.

[3] C. Chevalley: *Introduction to the theory of algebraic functions of one variable*, American Mathematical Society, Providence, RI, 1951.

[4] M. Deuring: *Lectures on the theory of algebraic functions of one variable*, Lecture Notes in Mathematics 314, Springer-Verlag, Berlin, 1973.

[5] C. Ding - H. Niederreiter - C. P. Xing: "Some New Codes from Algebraic Curves", erscheint in *IEEE Trans. Inform. Theory*, 2000.

[6] V. D. Goppa: "A new class of linear error-correcting codes", *Problems of Info. Transmission* **8**(3), 207 - 212, 1970.

[7] V. D. Goppa: "Codes on algebraic curves", *Dokl. Akad. Nauk SSSR* **259**, 1289 - 1290, 1981, (in russischer Sprache).

[8] H. Havlicek: *Lineare Algebra und Analytische Geometrie I, II*, TU Wien, 1995-96.

[9] A. Hocquenghem: "Codes correcteurs d'erreurs", *Chiffres* **2**, 147 - 156, 1959.

[10] R. Lidl und H. Niederreiter: *Finite Fields*, Addison-Wesley, Reading, Mass., 1983.

[11] F. J. MacWilliams - N. J. A. Sloane: *Theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[12] H. Niederreiter: "Nets, (t, s)-sequences, and algebraic curves over finite fields with many rational points", *Proc. International Congress of Mathematicians (Berlin, 1998)*, *Documenta Math. Extra Volume* **ICM III**, 337 - 386, 1998.

[13] H. Niederreiter and C. P. Xing: "Low-discrepancy sequences and global function fields with many rational places", *Finite Fields Appl.* **2**, 241 - 273, 1996.

[14] H. Niederreiter and C. P. Xing: "Towers of global funktion fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound", *Math. Nachrichtentech.* **195**, 171 - 186, 1998.

[15] H. Niederreiter - C. P. Xing - K. Y. Lam: "A New Construction of Algebraic-Geometry Codes", *Applicable Algebra Engrg. Comm. Comput.* **9**, 373 - 381, 1999.

[16] F. Özbudak - H. Stichtenoth: "Constructing Codes from Algebraic Curves", *IEEE Trans. Inform. Theory* **45**, 2502 - 2505, 1999.

[17] O. Pretzel: *Error-Correcting Codes and Finite Fields*, Oxford University Press, Oxford, 1992.

[18] O. Pretzel: *Codes and Algebraic Curves*, Oxford University Press, Oxford, 1998.

[19] H. Stichtenoth: *Algebraic Function Fields and Codes*, Springer-Verlag, Berlin, 1993.

[20] E. C. Titchmarsh: *The Zeta-function of Riemann*, Stechert-Hafner Verlag, New York, 1964.

[21] M. A. Tsfasman - S. G. Vlădut: *Algebraic-Geometric Codes*, Kluwer Academic Publishers, Dordrecht-Boston-London, 1991.

[22] M. A. Tsfasman - S. G. Vlădut - T. Zink: "Modular curves, Shimura curves and Goppa codes better than the Varshamov-Gilbert bound", *Math. Nachr.* **109**, 21 - 28, 1982.

[23] J. H. van Lint: *Introduction to Coding Theory*, Springer-Verlag, New York, 1999.

[24] C. P. Xing and H. Niederreiter: "A construction of low-discrepancy sequences using global function fields", *Acta Arith.* **73**, 87 - 102, 1995.

[25] C. P. Xing - H. Niederreiter - K. Y. Lam: "Constructions of Algebraic-Geometry Codes", *IEEE Trans. Inform. Theory* **45**, 1186 - 1193, 1999.

[26] C. P. Xing - H. Niederreiter - K. Y. Lam: "A Generalization of Algebraic-Geometry Codes", *IEEE Trans. Inform. Theory* **45**, 2498 - 2501, 1999.