ARITHMETIK DER FUNKTIONENKÖRPER
(mit Anwendung auf Goppa Codes)

Literatur:

Stichtenoth, H., Algebraic function f ields and codes, Springer, 1993

Lütkebohmert, W., Codierungstheorie, Vieweg, 2003 (Algebraisch-geometrische Grundlagen)

Contents

1 Algebraische Grundbegriffe und Fakten 2

2 Reihen und Approximationssatz 24

3 Divisoren und Adéle 46

4 Duale Adéle-Räume und Residuen 77

5 Grundbegriffe der Codierung 106

6 Funktionale Goppa-Codes und Riemann-Rochscher Satz 113

7 Kanonische Goppa-Codes 126

8 Fehlerkorrektur-Algorithmus von Skorobogatov / Vladut 136

9 Vorträge 155

1 Algebraische Grundbegriffe und Fakten

Def inition 1.1 $\mathcal{F}$ *"algebraischer Funktionenkörper über (Konstantenkörper)* K*":*

- $\mathcal{F}$ endlich erzeugt über K;
- $\mathcal{F}$ vom Transzendenzgrad 1 über K;
- K algebraisch abgeschlossen in $\mathcal{F}$.

Es gilt: $t \in \mathcal{F}$ ist transzendent über K gdw. $\mathcal{F}/K(t)$ endliche Körpererweiterung.

Argument: Additivität der Transzendenzgrade Körpererweiterungen $M/L/K$.

Def inition 1.2 . *Eine* **diskrete Bewertung** *eines Körpers* $\mathcal{F}$ *ist eine Abbildung* $v : \mathcal{F} \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$, *die für alle* $a, b \in \mathcal{F}$ *folgende Eigenschaften erfüllt:*

(o) $v(a) = \infty \Leftrightarrow a = 0$;

(i) $v(ab) = v(a) + v(b)$;

(ii) $v(a + b) \geq \min\{v(a), v(b)\}$
(Dreiecks-Ungleichung für Bewertungen).

Es folgt

- $v(a+b) = \min\{v(a), v(b)\}$, falls $v(a) \neq v(b)$;
- $v(a-b) \geq \min\{v(a), v(b)\}$;
- $v(-1) = v(1) = 0$;
- $v(\zeta) = 0$ für Einheitswurzeln ζ;
- $v(\mathbb{F}^*) = \{0\}$ für endliche Teilkörper $\mathbb{F}$.

Def inition 1.3 *Der Integritätsbereich*

$$\mathcal{O} = \mathcal{O}_v := \{\varphi \in \mathcal{F};\ v(\varphi) \geq 0\}$$

heißt **"Bewertungsring"** *von* $\mathcal{F}$ *bzgl.* v.

Einheitengruppe: $\mathcal{O}^* = \{\varphi \in \mathcal{F};\ v(\varphi) = 0\}$

einziges Maximalideal:
$\mathfrak{m} = \mathfrak{m}_v := \{\varphi \in \mathcal{F};\ v(\varphi) > 0\}$

Damit ist $\mathcal{O}$ ein "lokaler Ring".

Theorem 1.4 *Der Bewertungsring $\mathcal{O}$ der diskreten Bewertung v hat die folgenden Eigenschaften:*

(i) $\mathcal{O}$ ist ein Hauptidealring;

(ii) $\mathcal{O}$ ist Ring mit eindeutiger Primzerlegung;

(iii) $t \in \mathcal{O}$ ist Primelement genau dann, wenn $v(t) = 1$.

Betrachten nur Bewertungen v von $\mathcal{F}/K$, d.h.

(iv) $v(c) = 0$ für alle $c \in K^*$.

Primelemente t heißen auch "lokale Parameter" von $\mathcal{F}$ bzgl. v.

Ferner gilt:

(1) $f \in \mathcal{O}$ oder $f^{-1} \in \mathcal{O}$ für alle $f \in \mathcal{F}$.

(2) $K \subseteq \mathcal{O} \subsetneqq \mathcal{F}$;

- $\Rightarrow \mathcal{O}$ ist maximaler echter Unterring von $\mathcal{F}$.

Def inition 1.5 *Jeder Unterring $\mathcal{O}$ von $\mathcal{F}$ mit den Eigenschaften (1), (2) heißt "Stellenring" in/von $\mathcal{F}$.*

Lemma 1.6 *Jeder Stellenring $\mathcal{O}$ ist lokaler Ring mit Maximalideal $\mathfrak{p} := \mathcal{O} \setminus \mathcal{O}^*$.*

Idealeigenschaften:

(i) $\mathcal{O}\mathfrak{p} \subseteq \mathfrak{p}$,

(ii) $\mathfrak{p} + \mathfrak{p} \subseteq \mathfrak{p}$.

Beweis.
(i): $f \in \mathcal{O}$, $m \in \mathfrak{p} \Rightarrow m \notin \mathcal{O}^* \Rightarrow fm \notin \mathcal{O}^*$
$\Rightarrow fm \in \mathfrak{p}$.
(ii): Seien $f, g \in \mathfrak{p}$, und z.B. $f/g \in \mathcal{O}$;
$\Rightarrow 1 + f/g \in \mathcal{O} \Rightarrow f + g = g(1 + f/g) \in \mathfrak{p}$.

Bemerkung 1.7 *Jedes* $0 \neq t \in \mathfrak{p}$ *ist transzendent (über* K*).*

Beweis.

Ann. t algebraisch $\Rightarrow t \in K^* \Rightarrow t \in \mathcal{O}^*$
$\Rightarrow t \notin \mathfrak{p}$, Widerspruch.

Lemma 1.8

Die Länge echt absteigender Teilerketten

$$...|f_n|...|f_1|f_0 = f \in \mathcal{O} \setminus K$$

ist beschränkt durch $n < [\mathcal{F} : K(f)] < \infty$.

Beweis.

Zeige: $f_0, ..., f_n$ sind $K(f)$-linear unabhängig:

Fall $f \in \mathcal{O}^*$ trivial, also sei $f \in \mathfrak{p}$ und

$\sum_{i=0}^{n} G_i f_i = 0$, $G_i = G_i(f) \in K[f]$

mit $ggT = 1$ in $K[f]$ (also auch in $\mathcal{O}$).

Sei j spätester Index mit $f | G_k$ für alle $k > j$.

$$0 = \sum_{i=0}^{j-1} G_i \frac{f_i}{f_j} + G_j + \sum_{k=j+1}^{n} \frac{f}{f_j} G'_k f_k$$

$\Rightarrow$ alle Summanden außer G_j in $\mathfrak{p}$,

Widerspruch, wenn gezeigt wird: $G_j \notin \mathfrak{p}$.

$G_j \notin \mathfrak{p}$:

Betrachte Zerlegung in $K[f]$:

$$G_j = a_0 + fH_j,\ a_0 \in K,\ H_j \in K[f];$$

Annahme, $G_j \in \mathfrak{p} \Rightarrow a_0 \in K \cap \mathfrak{p} = (0)$, $\Rightarrow f|G_j$,

Widerspruch zur Wahl von j.

$\square$

Theorem 1.9 *Sei $\mathcal{O}$ Stellenring mit Maximalideal $\mathfrak{p} = \mathcal{O} \setminus \mathcal{O}^*$. Dann gilt*

(a) $\mathfrak{p}$ *ist Hauptideal:* $\mathfrak{p} = \mathcal{O}t$*;*

(b) für alle $0 \neq f \in \mathcal{O}$ *gibt es eine eindeutige Zerlegung*

$$f = t^m \cdot u, \quad m \in \mathbb{N}, u \in \mathcal{O}^*;$$

(c) $v = v_t = v_{\mathfrak{p}}$*:* $\mathcal{O} \to \mathbb{N} \cup \{\infty\}, 0 \neq f \mapsto m$*,*
def iniert eine diskrete Bewertung von $\mathcal{F}$ *mit Bewertungsring* $\mathcal{O}$*.*

Beweis. (a) Annahme $\mathfrak{p}$ ist kein Hauptideal.
Bilde unendliche Folge: $0 \neq f = f_0 \in \mathfrak{p}$,

$$f_1 \in \mathfrak{p} \setminus \mathcal{O} f, \ldots, f_{j+1} \in \mathfrak{p} \setminus \mathcal{O} f_j, \ldots$$

$$\Rightarrow f_1/f_0 \notin \mathcal{O}, \ldots, f_{j+1}/f_j \notin \mathcal{O}, \ldots$$

$$\Rightarrow f_0/f_1 \in \mathfrak{p}, \ldots, f_j/f_{j+1} \in \mathfrak{p}, \ldots$$

liefert echte unendliche Teilerkette in $\mathcal{O}$

$$...|f_n|...|f_1|f_0 = f,$$

im Widerspruch zu Lemma 1.8.

(b) Fall: $f \in \mathcal{O}^* \Rightarrow f = t^0 \cdot f$.
Fall $f \in \mathfrak{p}$:
Ex. $m \in \mathbb{N}$ maximal mit $t^m | f$ (Lemma 1.8).

$$\Rightarrow f = t^m \cdot u,\ u \in \mathcal{O}^* \text{ eindeutig.}$$

(c) $\mathcal{F}^* \ni \varphi = f/g$, $f, g \in \mathcal{O}$.

$$v = v_t = v_{\mathfrak{p}} : \ \varphi \mapsto v_t(f) - v_t(g) =: \ v_t(\varphi).$$

Def inition 1.10 *Die Maximalideale von Stellenringen von $\mathcal{F}$ heißen "Stellen" von $\mathcal{F}$.*

Geometrische Bezeichnungen:

P (wie Punkt) statt $\mathfrak{p}$;
Menge aller Stellen von $\mathcal{F}$: $\mathbb{P}_{\mathcal{F}} = \mathbb{P}_{\mathcal{F}/K}$,

($\mathbb{P}$ wie projektiv).

Bijektive Korrespondenzen:

$$\begin{tikzcd}
\{\text{Stellen von } \mathcal{F}\} \arrow[r, "="] \arrow[d, "\wr"] & \mathbb{P}_{\mathcal{F}} \arrow[d, "\wr"] \\
\{\text{Stellenringe von } \mathcal{F}\} \arrow[r, "\sim"] & \{\text{diskr. Bewertungen von } \mathcal{F}\}
\end{tikzcd}$$

Stelle $P \mapsto$ Bewertung v_P:
$P = \mathfrak{p}$ hat erz. Element t;
$v_P : \ f = u \cdot t^k \mapsto k$ ($u \in \mathcal{O}^*$, $k \in \mathbb{Z}$).
(diskrete Bewertung);

Bewertung $v \mapsto \mathcal{O}_v$ (Bewertungsring);

Bewertungsring $\mathcal{O} \mapsto$ Max.ideal $\mathfrak{m} = \mathfrak{m}_P$
von Stellenring $\mathcal{O} = \mathcal{O}_P$.

Def inition 1.11 *Der Körper* $\mathfrak{k} = \mathcal{O}/\mathfrak{m}$ *heißt "Restklassenkörper" von* $\mathcal{O}$.

Bezeichnungen: $\mathfrak{k} = \mathfrak{k}_v = \mathfrak{k}_P$ für $\mathcal{O} = \mathcal{O}_v = \mathcal{O}_P$

"Restklassenhomomorphismus" ρ_P an Stelle P:

$$\rho_P : \ \mathcal{O}_P \twoheadrightarrow \mathfrak{k}_P \text{ mit Kern } \mathfrak{m}_P$$

Satz 1.12 *Der Restklassenkörper* $\mathfrak{k}$ *ist eine endliche Körpererweiterung von* K.

Def inition 1.13 *Der Körpergrad* $[\mathfrak{k}_P : K] < \infty$ *heißt "Grad der Stelle"* P.

$$\deg P = 1 \Leftrightarrow K = \mathfrak{k}_P.$$

$$\deg P \leq [\mathcal{F} : K(f)] < \infty$$

für alle $f \in \mathfrak{p}$.

Idee:

$n := [\mathcal{F} : K(f)] < \infty$,

$\Rightarrow z_0, z_1, .., z_n \in \mathcal{O}$ stets $K(f)$-lin. abh.,

$\Rightarrow$ Abhängigkeits-Relation mit Koeff. in $K[f]$, $ggT = 1$;

Reduktion mod $\mathfrak{p}$ liefert lin. Abhängigkeit der Restklassen $\bar{z}_0, \bar{z}_1, .., \bar{z}_n$ über $\mathfrak{k}$.

$\Rightarrow \deg P \leq n$.

Def inition 1.14 *Liegt f in $\mathcal{O}_P$, so wird das Bild von f in $\mathfrak{k}_P = \mathcal{O}_P/\mathfrak{m}_P$ beim Restklassen-Homomorphismus*

$$\mathcal{O}_P \twoheadrightarrow \mathfrak{k}_P$$

mit $f(P)$ bezeichnet und **"Funktionswert"** *von f an der Stelle P genannt.*
In diesem Falle heißt f **"regulär"** *an der Stelle P.*
Andernfalls wird P **"Polstelle"** *von f genannt und $f(P) = \infty$ gesetzt.*

Merke: P ist Nullstelle von f gdw. $f \in \mathfrak{m}_P$.

Beispiel 1.15 $\mathcal{F} = K(X)$ *rationaler Funktionenkörper*

$\mathbb{P}_{K(X)}^{deg=1} \Leftrightarrow K \cup \{\infty\}$;

"endliche Stellen(ringe)": $X \in \mathcal{O}$;

$\mathbb{P}_{K(X)}^{fnt} \Leftrightarrow$ {normierte Primpolynome in $K[X]$};

Stelle ∞: $X' := 1/X \in \mathcal{O}, K[X'] \subset \mathcal{O}_\infty$

lokaler Parameter: Primpolynom X', $v_\infty = -deg$.

2 Reihen und Approximationssatz

$t \in \mathfrak{m}$ lokaler Parameter, (transzendent über K),

"formale Potenzreihenringe"

$$K[[t]] \subseteq k[[t]] \subseteq \bar{k}[[t]] = \bar{K}[[t]]$$

diskrete Bewertungsringe bzgl. t-Bewertung der Quotienten-Körper

$$K((t)) \subseteq k((t)) \subseteq \bar{k}((t)) = \bar{K}((t))$$

der "formalen Laurent-Reihen"

$$K \subseteq \mathfrak{k} = \mathcal{O}/\mathfrak{m} \subset \bar{K},$$

Potenzreihen-Entwicklung von $f \in \mathcal{O}$:

Fall $K = \mathfrak{k}$, $K[t] = \mathfrak{k}[t] \subset \mathfrak{k}[[t]]$

Näherungs-Polynome, induktiv:

$$f \equiv a_0 = f_0 \ := f(P) \quad \bmod t \text{ in } \mathfrak{k}[t],$$

$$f \equiv f_n = a_0 + a_1 t + \ldots + a_n t^n \quad \bmod t^{n+1};$$

$$a_{n+1} \ := \tfrac{f - f_n}{t^{n+1}}(P) \in \mathfrak{k}[t];$$

$$f_{n+1} \ := a_0 + a_1 t + \ldots + a_n t^n + a_{n+1} t^{n+1}.$$

$$f \mapsto \sum_{n=0}^{\infty} a_n t^n \in \mathfrak{k}[[t]]$$

liefert Ringeinbettung

$$\mathcal{O} \hookrightarrow \mathfrak{k}[[t]].$$

Allgemein: Zu Konstantenkörper-Erweiterung

$$\mathcal{F}_{\mathfrak{k}} := \mathfrak{k} \cdot \mathcal{F}, \quad \mathcal{O}_{\mathfrak{k}} := \mathfrak{k} \cdot \mathcal{O}$$

übergehen.

$$\mathcal{O} \subset \mathcal{O}_{\mathfrak{k}} \hookrightarrow \mathfrak{k}[[t]],$$
$$\mathcal{F} \subset \mathcal{F}_{\mathfrak{k}} \hookrightarrow \mathfrak{k}((t)).$$

Motivation. Fixiere lokalen Parameter t_P an jeder Stelle $P \in \mathbb{P}_{\mathcal{F}}$.

Laurentreihen-Entwicklungen

$$\mathcal{F} \ni \varphi = \sum_{i=-m}^{\infty} a_i t_P^i,\ a_i = a_{i,P} \in \mathfrak{k}_P \subset \bar{K}.$$

Hauptabschnitte von φ:

$$a_{-m}t_P^{-m} + ... + a_{-1}t_P^{-1},$$

echt, wenn $-m = v_P(\varphi) < 0$, ($a_{-m} \neq 0$);
sonst 0 (φ ist regulär, hat Potenzreihe in P).

Satz 2.1 *φ hat nur endlich viele Polstellen, also nur endlich viele (echte) Hauptabschnitte.*

Äquivalent: Jede Funktion $0 \neq f \in \mathcal{F}$ hat nur endlich viele Nullstellen P_i. Genauer gilt:

$$\sum_{Nullst.v.f} v_P(f) \deg P \leq [\mathcal{F} : K(f)] \qquad (1)$$

Zum Beweis benötigt man das folgende

Theorem 2.2 *(Approximations-Satz, auch Unabhängigkeits-Satz für Bewertungen)*

Zu gegebenen Bewertungen $v_1, ..., v_n$,
Funktionen $f_1, ..., f_n$,
ganzen Zahlen $a_1, ..., a_n$,

existiert stets eine Funktion $f \in \mathcal{F}$ mit

$$v_1(f - f_1) = a_1, ..., v_n(f - f_n) = a_n$$

Beweisschritte:

1) für zwei verschiedene Bewertungen v,w ex.

$$f \in \mathcal{F} \text{ mit } v(f) > 0,\ w(f) < 0:$$

nimm $f \in \mathcal{O}_v \setminus \mathcal{O}_w$, also $v(f) \geq 0,\ w(f) < 0.$

f durch $f^N t_v$ mit $N > w(t_v)$, ersetzen,

falls $v(f) = 0$. (t_v lokaler Parameter in v).

2) Zu verschiedenen Bewertungen $v_0, v_1, ..., v_n$ von $\mathcal{F}$ ex. $u \in \mathcal{F}$ mit

$$v_0(u) > 0,\ v_1(u), ..., v_n(u) < 0. \tag{2}$$

Induktion über n; Anfang $n = 1$, siehe 1).
$n \Rightarrow n + 1$: Setze $w\ := v_{n+1}$

u erfülle (2); falls $w(u) \geq 0$,
wähle f mit $v_0(f) > 0$, $w(f) < 0$;

$$u'\ := u^N + f,\ N >> 0.$$

leistet das Verlangte.

3) Zu jeder natürlichen Zahl N existert $f \in \mathcal{F}$ mit:

$$v_0(f-1), v_1(f), \ldots, v_n(f) \geq N.$$

Wähle u wie in 2), $f \; := 1/(1+u^N)$, $(N > 0)$;

$\Rightarrow$

$$v_i(1/f) = v_i(1+u^N) = v_i(u^N) \leq -N, \;\; i = 1, \ldots, n;$$

$$v_0(1-f) = v_0(u^N/(1+u^N)) = v_0(u^N) \geq N.$$

4) Zu vorgegebenen $g_1, ..., g_n \in \mathcal{F}$, und $a_1, ..., a_n \in \mathbb{Z}$ existiert $g \in \mathcal{F}$ mit

$$v_1(g - g_1) > a_1, \ ....., v_n(g - g_n) > a_n.$$

Wähle h_i, $i = 1, ..., n$ mit

$$v_1(h_1 - 1), v_2(h_1), ..., v_n(h_1) >> 0,$$

$$v_1(h_2), v_2(h_2 - 1), ..., v_n(h_2) >> 0,$$

$$...$$

$$v_1(h_n), v_2(h_n), ..., v_n(h_n - 1) >> 0,$$

Mit $g := \sum_{j=1}^{n} g_j h_j$ gilt

$$g - g_i = g_i(h_i - 1) + \sum_{j \neq i} g_j h_j,$$

$$v_i(g - g_i) \geq min\{v_i(g_i(h_i - 1)),\ v_i(g_j h_j), j \neq i\} >> 0,$$

weil

$$v_i(g_i(h_i - 1)) = v_i(g_i) + v_i(h_i - 1) >> 0$$

$$v_i(g_j h_j) = v_i(g_j) + v_i(h_j) >> 0,\ i \neq j = 1, ..., n.$$

5) Zweimalige Anwendung: Auf $t_1^{a_1}, ..., t_n^{a_n}$, ($t_i$ lokale Parameter in P_i), danach auf $f_1, ..., f_n$, liefert g' bzw. $g \in \mathcal{F}$ mit

$$v_i(g' - t_i^{a_i}) >> 0, \quad v_i(g - f_i) >> 0, \quad i = 1, ..., n.$$

Setze $f := g + g'$,

$$v_i(f - f_i) = v_i((g - f_i) + g') = v_i(g') = v_i(t_i^{a_i}) = a_i.$$

$\Rightarrow f$ ist gesuchte Approximation der f_i.

Approximationssatz $\Rightarrow$ obere Schranke (1) für Nullstellenanzahl von f:

A) Zu n vorgegebenen verschiedenen Stellen $P_1, ..., P_n$ existiert ein "System unabhängiger lokaler Parameter" $t_1, ..., t_n$:

$$v_i(t_i) = 1,\ v_j(t_i) = 0,\ \text{ für } 1 \leq i < j \leq n.$$

t_i nach Approximationssatz so wählbar:

$$v_i(t_i - 0) = 1,\ v_j(t_i - 0) = 0\ (j \neq i).$$

Seien $P_1, ..., P_n$ verschiedene Nullstellen von f,

$$e_i := v_i(f) > 0,\ d_i := deg P_i = [\mathfrak{k}_i : K],\ i = 1, ..., n.$$

B) Wähle für jedes i

$$\mathcal{O}_{P_i} \ni z_{i1}, ..., z_{id_i} \twoheadrightarrow K\text{-Basis von } \mathfrak{k}_i = \mathfrak{k}_{P_i},$$
$$(\Rightarrow v_i(z_{i1}), ..., v_i(z_{id_i}) = 0),$$

so daß (o.B.d.A.)

$$v_k(z_{i1}), ..., v_k(z_{id_i}) >> 0 \quad \forall k \neq i;$$

evtl. Änderung (Approximations-Satz) $z'_{ij} := z$ mit

$$v_i(z - z_{ij}) = 1,\ v_k(z - 0) >> 0,\ k \neq i,$$

$$\sum_{i=1}^{n} v_i(f) \cdot \deg\ P_i \leq [\mathcal{F} : K(f)]$$

folgt aus

C) $t_i^m z_{ij}$, $i = 1, ..., n$, $j = 1, ..., d_i$, $m = 0, ..., e_i - 1$ sind $K(f)$-linear unabhängig

Gegenteilige Annahme:

$$\sum_{mij} \varphi_{mij} \cdot t_i^m \cdot z_{ij} = 0,\ \varphi_{mij} \in K[f] \text{ mit } ggT = 1;$$

$$v_k(\varphi_{mij} \cdot t_i^m \cdot z_{ij}) = v_k(\varphi_{mij}) + v_k(t_i^m) + v_k(z_{ij})$$

$$\begin{cases} >> 0, & k \neq i \\ = v_k(\varphi_{mkj}) + m, & k = i \\ = m < e_k, & k = i,\ f \nmid \varphi_{mij} \end{cases}$$

Sei (μ, k, j_0) lexikographisch minimales Tripel (m, i, j) mit $f \nmid \varphi_{mij}$.

$\Rightarrow t_k^\mu \mid \varphi_{mij}$ für alle m, i, j;

$t_k^{\mu+1} \mid \varphi_{mij}$ falls $(m, i) \neq (\mu, k)$;

Abhängigkeits-Annahme der $t_i^m z_{ij}$

$$\Rightarrow t_k^{\mu+1} \mid \sum_{j=1}^{d_k} \varphi_{\mu kj} \cdot t_k^{\mu} \cdot z_{kj},$$

$$\Rightarrow t_k \mid \sum_{j=1}^{d_k} \varphi_{\mu kj} \cdot z_{kj},$$

Übergang zu Restklassen modulo $\mathfrak{m}_k = (t_k)$
$\Rightarrow \sum_j \bar{\varphi}_{\mu kj} \cdot \bar{z}_{kj} = 0$ in $\mathfrak{k}_{P_k}$,

im Widerspruch zur linearen Unabhängigkeit der $\bar{z}_{kj}$ (ein Koeff izient ist $\neq 0$, nämlich $\bar{\varphi}_{\mu kj_0}$).

Satz. Jede nichtkonstante Funktion hat mindestens eine Null- und eine Polstelle.

Beweis. Durch Übergang von f zu f^{-1} genügt der Nachweis einer Nullstelle.

Sei $f \in \mathcal{F} \setminus K$ und $\mathcal{R} = \mathcal{R}(f)$ die Menge der Ringerweiterungen R von $K[f]$ in $\mathcal{F}$ mit $Rf \neq R$.

Jede (total geordnete) Kette $(R_i)_{i \in I}$ in $\mathcal{R}$ wird von einem Ring $R \in \mathcal{R}$ dominiert, z.B. von $R = \bigcup_{i \in I} R_i$. Nach dem Zornschen Lemma existiert maximales Element $\mathcal{O}$ in $\mathcal{R}$.

$\mathcal{O}$ ist ein Stellenring (Def. 1.5) von $\mathcal{F}$:

(1) $z \notin \mathcal{O} \Rightarrow z^{-1} \in \mathcal{O}$;

(2) $K \subsetneqq \mathcal{O} \subsetneqq \mathcal{F}$;

(2) folgt direkt aus der Konstruktion.
Nachweis von (1): Annahme $z, z^{-1} \notin \mathcal{O}$.
Nacheinander folgt

$$\mathcal{O} \subsetneqq \mathcal{O}[z],\ \mathcal{O} \subsetneqq \mathcal{O}[z^{-1}]$$

$$\mathcal{O}[z],\ \mathcal{O}[z^{-1}] \notin \mathcal{R},$$

$$1 \in f\mathcal{O}[z],\ 1 \in f\mathcal{O}[z^{-1}],$$

$1 \in f\mathcal{O}[z]_n$, $1 \in f\mathcal{O}[z^{-1}]_m$ ($_n$ means Grad $\leq n$),

$$1 = \sum_{i=0}^{n} f a_i z^i, \; a_i \in \mathcal{O},$$

$$1 = \sum_{i=0}^{m} f b_i z^{-i}, \; b_i \in \mathcal{O},$$

Sei o.B.d.A. $m \leq n$. Multipliziere zweite Identität mit $f a_n z^n$, erste mit $1 - f b_0$:

$$1 - fb_0 = \sum_{i=0}^{n-1} (1 - fb_0) f a_i z^i + (1 - fb_0) f a_n z^n,$$

$$(1 - fb_0) f a_n z^n = f a_n z^n \sum_{j=1}^{m} f b_i z^{n-j};$$

Substitution von $(1 - b_0) f a_n z^n$ in obere Identität ergibt

$$1 \in f\mathcal{O}[z]_{n-1}$$

Abstieg von n, m zu Grad 0 führt zu

$$1 \in f\mathcal{O}[z]_0 = f\mathcal{O} = f\mathcal{O}[z^{-1}]_0$$

im Widerspruch zu $f\mathcal{O} \subsetneq \mathcal{O}$.

$\square$

3 Divisoren und Adéle

Adéle: Jeder Stelle P wird Funktion f_P zugeordnet:

$$\mathfrak{f} = (f_P)_{P \in \mathbb{P}_{\mathcal{F}}};\ v_P(f_P) \geq 0 \text{ für fast alle } P$$

Adéle-Ring $\mathbb{A}_{\mathcal{F}}$ (kommutativ mit Einselement $\mathbf{1}$): Addition und Multiplikation komponentenweise:

$$\mathfrak{f} + \mathfrak{g} = (f_P)_{P \in \mathbb{P}_{\mathcal{F}}} + (g_P)_{P \in \mathbb{P}_{\mathcal{F}}} := (f_P + g_P)_{P \in \mathbb{P}_{\mathcal{F}}},$$

$$\mathfrak{f} \cdot \mathfrak{g} = (f_P)_{P \in \mathbb{P}_{\mathcal{F}}} \cdot (g_P)_{P \in \mathbb{P}_{\mathcal{F}}} := (f_P \cdot g_P)_{P \in \mathbb{P}_{\mathcal{F}}}.$$

$\mathbb{A}_{\mathcal{F}}$ ist ein unendlich-dimensionaler $\mathcal{F}$-Vektoraum:

$$g \cdot \mathfrak{f} = g \cdot (f_P)_{P \in \mathbb{P}_{\mathcal{F}}} := (g \cdot f_P)_{P \in \mathbb{P}_{\mathcal{F}}}$$

Diagonale Einbettung

$$Ad : \mathcal{F} \longrightarrow \mathbb{A}_{\mathcal{F}},$$

$$f \mapsto f \cdot \mathbf{1} = (f)_{P \in \mathbb{P}_{\mathcal{F}}} = (\ldots, f, \ldots)_P \text{ (konstant).}$$

Unterring der ganzen (überall regulären) Adéle:

$$\mathbb{A}_{\mathcal{F}}(O) := \{\mathfrak{f} = (f_P)_P \in \mathbb{A}_{\mathcal{F}};\ v_P(f_P) \geq 0 \quad \forall P \in \mathbb{P}_{\mathcal{F}}\}$$

Nächstes Ziel:

Theorem 3.1 *Für jeden Funktionenkörper $\mathcal{F}$ über einem Konstantenkörper K ist*

$$g = g_{\mathcal{F}} := \dim_K \mathbb{A}_{\mathcal{F}}/(\mathbb{A}_{\mathcal{F}}(O) + Ad(\mathcal{F})) < \infty,$$

also eine korrekt def inierte natürliche Zahl.

Def inition 3.2 *Diese Zahl $g_{\mathcal{F}}$ heißt "Geschlecht" des Funktionenkörpers $\mathcal{F}$.*

Interpretation der Elemente von $\mathbb{A}_{\mathcal{F}}/\mathbb{A}_{\mathcal{F}}(O)$:

Menge von Hauptabschnitten von Laurent-Reihen an endlich vielen Stellen.

Interpretation der Elemente von $\mathbb{A}_{\mathcal{F}}/(\mathbb{A}_{\mathcal{F}}(O) + Ad(\mathcal{F}))$:

nicht durch Funktionen realisierbare endliche Hauptabschnitts-Mengen.

Bei den Reihenentwicklungen werden lokale Parameter t_P an jeder Stelle P f ixiert.

"Divisorengruppe": freie abelsche Gruppe, erzeugt durch Stellen von $\mathcal{F}$:

$$Div\,\mathcal{F} \;:= \bigoplus_{P\in\mathbb{P}_{\mathcal{F}}} \mathbb{Z}\cdot P$$

"Grad eines Divisors" $D = \sum m_P \cdot P$:

$$\deg D \;:= \sum m_P \cdot \deg P = \sum m_P \cdot [\mathfrak{k}_P : K] \in \mathbb{Z}.$$

"Hauptdivisoren" von Funktionen $f \neq 0$:

$$(f) \;:= \sum_P v_P(f) \cdot P$$

$$\deg : \ Div\,\mathcal{F} \longrightarrow (\mathbb{Z}, +)$$

und

$$(\quad) : \ \mathcal{F}^* \longrightarrow Div\,\mathcal{F}, \text{ mit Kern } K^*,$$

sind Homomorphismen abelscher Gruppen:

$$\deg(D + E) = \deg D + \deg E$$
$$(f \cdot g) = (f) + (g),$$
$$(f^{-1}) = -(f).$$

Später wird gezeigt: $\deg(f) = 0$ für alle $f \in \mathcal{F}^*$.

Gruppe der Hauptdivisoren $Princ\,\mathcal{F} \subset Div\,\mathcal{F}$;

lineare Äquivalenz von Divisoren:

$$D \equiv D' \Leftrightarrow D - D' \in Princ\,\mathcal{F}$$

"Divisorenklassengruppe"

$$Pic\,\mathcal{F} \; := Div\,\mathcal{F}\,/\,Princ\,\mathcal{F}$$

"Effektive Divisoren", Schreibweise $D \geq O$:

$$D = m_1 P_1 + ... + m_k P_k, \; m_1, ..., m_k \geq 0,$$

bilden Halbgruppe $Div^+\mathcal{F}$.

Halbordnung in der Divisorengruppe:

$$D \geq D' \Leftrightarrow D - D' \geq O.$$

Raum polbeschränkter Funktionen eines Divisors $D = \sum v_P(D) \cdot P$:

$$\mathcal{L}(D) \ := \{f \in \mathcal{F};\ (f) \geq -D\}.$$

Raum abschnittsbeschränkter Adéle des Divisors D (ebenfalls K-Vektorraum):

$$\mathbb{A}(D) := \{\mathfrak{f} = (f_P) \in \mathbb{A}_{\mathcal{F}}; v_P(f_P) \geq -v_P(D), P \in \mathbb{P}_{\mathcal{F}}\}.$$

$\mathcal{L}(D) \hookrightarrow \mathbb{A}(D)$, via Diagonal-Einbettung.

Dimensions-Invarianten eines Divisors D:

$\mathfrak{l}(D) := \dim_K \mathcal{L}(D)$ ("Dimension")

$\mathfrak{l}^*(D) := \dim_K \mathbb{A}_{\mathcal{F}}/(\mathbb{A}(D) + Ad(\mathcal{F}))$ ("Kodimension")

$$D \leq E \Rightarrow \mathcal{L}(D) \subseteq \mathcal{L}(E),\ \mathbb{A}(D) \subseteq \mathbb{A}(E);$$
$$\Rightarrow \mathfrak{l}(D) \leq \mathfrak{l}(E),\ \mathfrak{l}^*(D) \geq \mathfrak{l}^*(E).$$

Bemerkungen.

$$\mathfrak{l}(O) = 1,$$
$$\mathfrak{l}(E) > 0, \text{ falls } E \text{ effektiv},$$
$$\mathfrak{l}(-E) = 0, \text{ falls } O \neq E \text{ effektiv},$$

$$D \equiv D' \Rightarrow \begin{cases} \mathcal{L}(D) \cong \mathcal{L}(D'), & \mathbb{A}(D) \cong \mathbb{A}(D'); \\ \mathfrak{l}(D) = \mathfrak{l}(D'), & \mathfrak{l}^*(D) = \mathfrak{l}^*(D'). \end{cases}$$

D ist linear äquivalent zu einem effektiven Divisor gdw $\mathfrak{l}(D) > 0$.

Lemma 3.3
$E \leq D \Rightarrow \mathfrak{l}(D) - \mathfrak{l}(E) \leq \deg D - \deg E$.

Satz 3.4 $\mathfrak{l}(D) \leq \deg D + 1 < \infty$, *falls* D *effektiv.*

Korollar. $\mathcal{L}(D)$ ist stets endlich-dimensional.

Lemma $\Rightarrow$ Satz $\Rightarrow$ Korollar.

Beweis des Lemmas:
Induktion über Grad-Differenz $\deg D - \deg E$.
Anfang: $D = E + P = (E' + mP) + P$,

$t = t_P$ lokaler Parameter.

$\mathfrak{l}(E+P) - \mathfrak{l}(E) \leq \deg P \; (= \deg D - \deg E)$:

$$\begin{tikzcd}
0 \arrow[r] & \mathcal{L}(E) \arrow[r] \arrow[d] & \mathcal{L}(E+P) \arrow[r] \arrow[d, "t^{m+1}\cdot"'] & \mathfrak{k}_P \arrow[d, "\|"] & \\
0 \arrow[r] & \mathfrak{m}_P \arrow[r] & \mathcal{O}_P \arrow[r] & \mathfrak{k}_P \arrow[r] & 0
\end{tikzcd}$$

Sei $(f) = (f)_0 - (f)_\infty$, (Nullst. - Poldivisor von f), $O \leq (f)_0,\ (f)_\infty$, teilerfremd.

Theorem . Für alle $f \in \mathcal{F} \setminus K$ gilt

$$\deg(f)_0 = \deg(f)_\infty = [\mathcal{F} : K(f)].$$

$\deg(f)_0 \leq n \; := [\mathcal{F} : K(f)]$ ist Satz 2.1.

Umkehrung, $\deg(f)_\infty = \deg(f)_0 \geq n$:

$u_1, ..., u_n$ $K(f)$-Basis von $\mathcal{F}$,
$1, f, .., f^k, ...$ K-Basis von $K[f]$,

rn K-linear unabhängige Funktionen:

$$f u_1, ..., f u_n$$

....

$$f^r u_1, ..., f^r u_n,$$

alle in $\mathcal{L}(r \cdot (f)_\infty + D)$

wobei $(u_1), ..., (u_n) \geq -D \in Div\,\mathcal{F}$, f ixiert.

Es folgt mit Satz 3.4

$$
\begin{aligned}
rn &\leq \mathfrak{l}(r \cdot (f)_\infty + D) \\
&\leq 1 + \deg(r \cdot (f)_\infty + D) \\
&= r \cdot \deg(f)_\infty + \deg D + 1
\end{aligned}
$$

$r \longrightarrow \infty$

$$\Rightarrow n \leq \deg(f)_\infty,$$

$\square$

Korollar 3.5 *Alle Hauptdivisoren sind vom Grad* 0.

Faktorisierung des Grad-Homomorphismus:

$$\deg : \; Div\,\mathcal{F}/Princ\,\mathcal{F} \longrightarrow \mathbb{Z}.$$

Korollar 3.6 *Für einen Divisor* D *vom Grad* 0 *sind folgende Eigenschaften äquivalent:*

(1) D ist Hauptdivisor;

(2) $\mathfrak{l}(D) \geq 1$;

(3) $\mathfrak{l}(D) = 1$.

Differenzabbildung, zwecks Vergleich von Grad und Dimension von Divisoren:

$$\delta : \; Div\,\mathcal{F} \longrightarrow \mathbb{Z}, \qquad D \mapsto \delta(D) \; := \deg D - \mathfrak{l}(D)$$

Satz 3.7 *δ ist nach oben beschränkt auf $Div\,\mathcal{F}$.*

Def inition 3.8

$$\chi = \chi_{\mathcal{F}} := \min\{-\delta(D); D \in Div\mathcal{F}\} = -\max_{D} \delta(D)$$

heißt "arithmetisches Geschlecht von $\mathcal{F}$.

Beweis des Satzes: Drei Schritte.

1.) δ ist monoton wachsend;

2.) δ ist beschränkt auf $\mathbb{Z} \cdot (f)_\infty$ für beliebiges $f \in \mathcal{F} \setminus K$;

3.) $\delta(Div\, \mathcal{F})$ wird von $\delta(\mathbb{N} \cdot (f)_\infty)$ dominiert.

1.) $E \leq D \Rightarrow \delta(E) \leq \delta(D)$
folgt aus $\mathfrak{l}(D) - \mathfrak{l}(E) \leq \deg D - \deg E$, was nach Lemma 3.3 gilt.

2.) Sei $f \in \mathcal{F} \setminus K$, $n := \deg(f)_\infty = [\mathcal{F} : K(f)]$;
Nach Theorem 57 existiert D mit

$$\mathfrak{l}(r \cdot (f)_\infty + D) \geq r \cdot n \quad \forall\, r > 0;$$

Es gilt nach Lemma 3.3 auch:

$$\begin{aligned} &\mathfrak{l}(r \cdot (f)_\infty + D) - \mathfrak{l}(r \cdot (f)_\infty) \\ &\leq \deg(r \cdot (f)_\infty + D) - \deg(r \cdot (f)_\infty) = \deg D, \end{aligned}$$

folglich

$$\mathfrak{l}(r \cdot (f)_\infty) \geq r \cdot n - \deg D = \deg(r \cdot (f)_\infty) - \deg D,$$

also $\delta(r \cdot (f)_\infty) \leq \deg D$ (fest, bei festem f).

3.) Zeigen: zu jedem $E \in Div\,\mathcal{F}$ existiert ein $r \in \mathbb{N}$ mit $\delta(E) \leq r \cdot (f)_\infty$.

O.B.d.A. E effektiv (da δ nach 1.) monoton wachsend ist). Nacheinander folgt:

$$r \cdot (f)_\infty - E \leq r \cdot (f)_\infty,$$

$$\mathfrak{l}(r \cdot (f)_\infty) - \mathfrak{l}(r \cdot (f)_\infty - E) \leq$$
$$\deg(r \cdot (f)_\infty) - \deg(r \cdot (f)_\infty - E) = \deg E,$$

$$
\begin{aligned}
\mathfrak{l}(r\cdot(f)_\infty - E) &\geq -\deg E + \mathfrak{l}(r\cdot(f)_\infty)\\
&= -\deg E + \deg(r\cdot(f)_\infty) - \delta(r\cdot(f)_\infty)\\
&> 0 \qquad \text{für } r >> 0.
\end{aligned}
$$

da $-\delta(\mathbb{N}\cdot(f)_\infty)$ nach unten beschränkt ist.
Also existiert $z \in \mathcal{L}(r\cdot(f)_\infty - E)$, d.h.
$(z) \geq -r\cdot(f)_\infty + E$, also $E - (z) \leq r\cdot(f)_\infty$,
mithin

$$\delta(E) = \delta(E-(z)) \leq \delta(r\cdot(f)_\infty) \leq \deg D.$$

$\square$

Korollar. Folgende Grad-Abschätzungen der Dimension von Divisoren sind richtig:

$$\chi + \deg D \leq \mathfrak{l}(D) \qquad \forall\, D \in \mathit{Div}\, \mathcal{F},$$
$$\mathfrak{l}(D) \leq \deg D + 1 \qquad \forall\, D \in \mathit{Div}^{\,+} \mathcal{F}.$$

Wegen $\chi = \min_D\{\mathfrak{l}(D) - \deg D\}$ und Satz 3.4.

$\square$

Satz (Riemann). Sei M Divisor mit mit maximalem δ. Dann gilt $\mathfrak{l}(M) = \chi + \deg M$ und

$$\mathfrak{l}(D) = \chi + \deg D \qquad \forall\, D \text{ mit } \deg D > \chi + \deg M.$$

Beweis. Die erste Ungleichung des Korollars angewandt auf D-M ergibt

$$\mathfrak{l}(D-M) \geq \deg(D-M)+\chi = \deg D - \deg M + \chi > 0$$

Nacheinander folgt:

$D - M \equiv D' - M$ effektiv, $M \leq D' \equiv D$;

$$-\chi = \delta(M) \leq \delta(D') = \delta(D) \leq -\chi,$$

$$\deg D - \mathfrak{l}(D) = \delta(D) = -\chi.$$

$\square$

Satz von Riemann-Roch (Adéle-Version).
Für alle Divisoren $D \in Div\mathcal{F}$ gilt
$(\mathfrak{l} - \mathfrak{l}^*)(D) - (\mathfrak{l} - \mathfrak{l}^*)(O) = \deg D = (\mathfrak{l} - \mathfrak{l}^*)(D) - \chi$
(Doppeldifferenz = Grad)

Erste Identität folgt aus zweiter, für $D = O$:

$$\chi = \mathfrak{l}(O) - \mathfrak{l}^*(O) = 1 - g.$$

Korollar. Die Kodimension $\mathfrak{l}^*(D)$ eines jeden Divisors ist endlich. Sie verschwindet für alle Divisoren $D \geq M$, M Divisor mit maximalem δ.

Beweis-Schritte. $D \leq E \Rightarrow$

1.)

$$\dim \mathbb{A}(E)/\mathbb{A}(D) = \deg E - \deg D;$$

2.)

$$\dim(\mathbb{A}(E) + Ad(\mathcal{F}))/(\mathbb{A}(D) + Ad(\mathcal{F}))$$
$$= \delta(E) - \delta(D);$$

3.)

$$Div\,\mathcal{F} \ni M \text{ maximal bzgl. } \delta$$
$$\Downarrow$$
$$\mathbb{A}_{\mathcal{F}} = \mathbb{A}(M) + Ad(\mathcal{F}), \text{ d.h. } \ell^*(M) = 0.$$

2.), 3.) $\Rightarrow$ Riemann-Roch:

Sei M maximal bzgl. δ, $M \geq D$
(M existiert nach Satz von Riemann).

$$\mathbb{A}_{\mathcal{F}} = \mathbb{A}(M) + Ad(\mathcal{F}) \text{ nach 3.),} \quad \Longrightarrow$$

$$\begin{aligned}
\mathfrak{l}^*(D) &= \dim \mathbb{A}_{\mathcal{F}}/(\mathbb{A}(D) + Ad(\mathcal{F})) \\
&= \dim(\mathbb{A}(M) + \mathbb{A}_{\mathcal{F}})/(\mathbb{A}(D) + Ad(\mathcal{F})) \\
&\overset{2.)}{=} \delta(M) - \delta(D) = -\chi - (\deg D - \mathfrak{l}(D))
\end{aligned}$$

1.) Induktiv, schrittweise Punktaddition,

$$E = D + P = (D' + mP) + P,\ P \notin supp\, D',$$

$t = t_P$ lokaler Parameter in P,

$$\tau : \mathfrak{f} = (f_P)_P \mapsto t^{m+1} \cdot f_P \mod \mathfrak{m}_P$$

$$0 \longrightarrow \mathbb{A}(D) \longrightarrow \mathbb{A}(E) \xrightarrow{\tau} \mathfrak{k}_P \longrightarrow 0 \text{ exakt;}$$

$$\dim \mathbb{A}(E)/\mathbb{A}(D) = \dim_K \mathfrak{k}_P = \deg P = \deg E - \deg D.$$

Nun wird 1.) $\Rightarrow$ 2.) gezeigt.

Behauptung: Im kommutativen Diagramm

$$\begin{tikzcd}
\mathcal{L}(D) \arrow[r] \arrow[d] & \mathcal{L}(E) \arrow[r] \arrow[d] & \mathcal{L}(E)/\mathcal{L}(D) \arrow[d, "\cap"'] \\
\mathbb{A}(D) \arrow[r] \arrow[d] & \mathbb{A}(E) \arrow[r] \arrow[d] \arrow[dr, "s"] & \mathbb{A}(E)/\mathbb{A}(D) \arrow[d, "\sigma"'] \\
\mathbb{A}(D) + Ad(\mathcal{F}) \arrow[r] & \mathbb{A}(E) + Ad(\mathcal{F}) \arrow[r] & \overline{\mathbb{A}(E) + Ad(\mathcal{F})}
\end{tikzcd}$$

ist die rechte Spalte eine kurze exakte Folge.

Def inition von σ:

$$s : \mathbb{A}(E) \longrightarrow (\mathbb{A}(E) + \mathcal{F})/(\mathbb{A}(D) + \mathcal{F}),$$
$$\alpha \mapsto \alpha \mod (\mathbb{A}(D) + \mathcal{F})$$

faktorisiert durch

$$\sigma : \ \mathbb{A}(E)/\mathbb{A}(D) \longrightarrow (\mathbb{A}(E) + \mathcal{F})/(\mathbb{A}(D) + \mathcal{F})$$

$$Ker\ s = \mathbb{A}(E) \cap (\mathbb{A}(D) + \mathcal{F}) = \mathbb{A}(D) + \mathcal{L}(E),$$
$$Ker\ \sigma = (\mathbb{A}(D) + \mathcal{L}(E))/\mathbb{A}(D)$$
$$= \mathcal{L}(E)/\mathbb{A}(D) \cap \mathcal{L}(E) = \mathcal{L}(E)/\mathcal{L}(D)$$

Daraus folgt dann 2.) mit Hilfe von 1.):

$$\begin{aligned} &\dim(\mathbb{A}(E) + Ad(\mathcal{F}))/(\mathbb{A}(D) + Ad(\mathcal{F})) \\ = &\dim \mathbb{A}(E)/\mathbb{A}(D) - \dim \mathcal{L}(E)/\mathcal{L}(D) \\ \overset{1.)}{=} &\deg E - \deg D - (\mathfrak{l}(E) - \mathfrak{l}(D)) = \delta(E) - \delta(D). \end{aligned}$$

Beweis von 3.): Zu zeigen: $\mathbb{A}_{\mathcal{F}} \subseteq \mathbb{A}(M) + Ad(\mathcal{F})$.
Sei $\mathfrak{a} \in \mathbb{A}_{\mathcal{F}}$, $\mathfrak{a} \in \mathbb{A}(D)$, o.B.d.A. $D \geq M$. Es gilt

$$\delta(D) = \delta(M) = -\chi,$$

nach Riemann's Satz.

folglich

$$\dim(\mathbb{A}(D)+\mathcal{F})/(\mathbb{A}(M)+\mathcal{F}) \overset{2.)}{=} \delta(D)-\delta(M)=0,$$

also

$$\mathfrak{a} \in \mathbb{A}(D)+\mathcal{F}=\mathbb{A}(M)+\mathcal{F}.$$

Der Satz von Riemann-Roch in der Adéle-Version ist bewiesen.

$\square$

Klassische Fassung, mit Geschlecht g von $\mathcal{F}$:

$$\mathfrak{l}(D)-\mathfrak{l}^*(D)=\deg D+1-g.$$

Homogene Fassung: $|D,E|_{\mathfrak{l}-\mathfrak{l}^*} = |D,E|_{\deg}$, d.h.

$$(\mathfrak{l}-\mathfrak{l}^*)(D) - (\mathfrak{l}-\mathfrak{l}^*)(E) = \deg D - \deg E$$

$$\text{Dimensionsdifferenz-Abstand} \ = \ \text{Grad-Abstand} \tag{3}$$

allgemein $w: \ Div\,\mathcal{F} \longrightarrow \mathbb{R}$ (Wichtung),
"w-Abstand" zweier Divisoren:

$$|D,E|_w \ := w(D) - w(E).$$

auch "Raumabstände" bzgl. Dimension:

$$|\mathbb{A}(D),\mathbb{A}(E)|_{\dim} = |D,E|_{\deg}, \ \text{für } D \geq E,$$

$$|\mathbb{A}(D)+\mathcal{F},\mathbb{A}(E)+\mathcal{F}|_{\dim} = |D,E|_{\delta} = |D,E|_{\deg-\mathfrak{l}}$$

4 Duale Adéle-Räume und Residuen

Sei $\mathcal{F}$ Funktionenkörper mit Konstantenkörper K. Lineare Adéle-Funktionale $\omega : \mathbb{A}_{\mathcal{F}} \longrightarrow K$ mit

- $\omega(\mathcal{F}) = 0$,
- $\omega(\mathbb{A}(D)) = 0$ für einen Divisor D.

nennen wir "Differentiale" auf $\mathbb{A}_{\mathcal{F}}$;
Bezeichnung: $\mathbf{\Omega}_{\mathcal{F}}$
K-Vektorraum aller $\mathbb{A}_{\mathcal{F}}$-Differentiale.

Dualität:

$$\mathbb{A}_{\mathcal{F}} \times \check{\mathbb{A}}_{\mathcal{F}} = \mathbb{A}_{\mathcal{F}} \times Hom_K(\mathbb{A}_{\mathcal{F}}, K) \longrightarrow K$$
$$(\mathfrak{a}, \varphi) \mapsto < \mathfrak{a}, \varphi > := \varphi(\mathfrak{a})$$

Auf $\mathbb{A}(D) = \mathbb{A}_{\mathcal{F}}(D)$ verschwindende $\mathbf{\Omega}$-Funktionale:

$$\mathbf{\Omega}(D) = (\mathbb{A}(D) + \mathcal{F})^{\perp} \subset \mathbf{\Omega}_{\mathcal{F}} \subset \check{\mathbb{A}}_{\mathcal{F}}$$

$\mathcal{F}$-Vektorraum-Struktur überträgt sich von $\mathbb{A}_{\mathcal{F}}$ auf $\check{\mathbb{A}}_{\mathcal{F}}$:

$$f \cdot \varphi \ := \varphi \circ f \cdot$$

$$< \mathfrak{a}, f\varphi > = f\varphi(\mathfrak{a}) = \varphi(f\mathfrak{a}) = < f\mathfrak{a}, \varphi >$$

$$
\begin{tikzcd}
\mathbb{A}(D) + \mathcal{F} \arrow[r] \arrow[dr, "0"] & \mathbb{A}_{\mathcal{F}} \arrow[r] \arrow[d, "\omega"] & \mathbb{A}_{\mathcal{F}}/(\mathbb{A}(D) + \mathcal{F}) \arrow[dl] \\
& K &
\end{tikzcd}
$$

$$
\omega \in \mathbf{\Omega}_{\mathcal{F}}(D) \cong Hom_K(\mathbb{A}_{\mathcal{F}}/(\mathbb{A}(D) + \mathcal{F}), K),
$$

$$
\dim \mathbf{\Omega}_{\mathcal{F}}(D) = \dim \mathbb{A}_{\mathcal{F}}/(\mathbb{A}(D) + \mathcal{F}) = \mathfrak{l}^*(D),
$$

endlich nach Riemann-Rochschem Satz.

$\mathbf{\Omega}_{\mathcal{F}}$ ist ein $\mathcal{F}$-Vektorraum ($\mathcal{F}$-Unterraum von $\mathbb{A}_{\mathcal{F}}$):

$$(f) \geq -E,\ \mathfrak{a} \in \mathbb{A}(D-E) \Rightarrow f\mathfrak{a} \in \mathbb{A}(D)$$

$$\begin{tikzcd}
\mathbb{A}(D-E) \arrow[r] \arrow[d] & \mathbb{A} \arrow[r, "f\omega"] \arrow[d, "f\cdot"'] & K \arrow[d, "\|"] \\
\mathbb{A}(D) \arrow[r] & \mathbb{A} \arrow[r, "\omega"] & K
\end{tikzcd}$$

$$f\cdot : \mathbf{\Omega}(D) \longrightarrow \mathbf{\Omega}(D-E),\ f \in \mathcal{L}(E);$$
$$f\cdot : \mathbf{\Omega}(D) \xrightarrow{\sim} \mathbf{\Omega}(D+(f)),\ (\text{via } E = -(f)). \tag{4}$$

Lemma 4.1 *Zu jedem Ω-Funktional $\omega \neq 0$ existiert ein eindeutig bestimmter Divisor $W \in Div\,\mathcal{F}$ mit*

$$\omega \in \mathbf{\Omega}(W), W \text{ maximal}$$

a) $\omega \in \mathbf{\Omega}(D), \mathbf{\Omega}(E) \Rightarrow \omega \in \mathbf{\Omega}(kgV(D,E))$;

b) für jede aufsteigende Folge von Divisoren

$$D_1 \leq D_2 \leq \ldots \leq D_n \leq \ldots$$

stagniert von einem Index an die Folge von K-Vektorräumen

$$\mathbf{\Omega}(D_1) \geq \mathbf{\Omega}(D_2) \geq \ldots \geq \mathbf{\Omega}(D_n) \geq \ldots$$

Anwendung auf $D, E, D'_n s$ mit

$$\omega \in \mathbf{\Omega}(D), \mathbf{\Omega}(E), \mathbf{\Omega}(D_n) \qquad \text{liefert } W.$$

zu a):

$$\mathbb{A}(D) + \mathbb{A}(E) = \mathbb{A}(kgV(D, E)),$$

$$D, E \leq kgV(D, E) \; := \sum_P \max\{v_P(D), v_P(E)\} \cdot P$$

zu b): Die K-Vektorräume $\mathbf{\Omega}(D_n)$ haben endliche Dimension.

Def inition 4.2 *Der in Lemma 4.1 gefundene Divisor W heißt "kanonischer Divisor" von ω*

Bezeichnung: $(\omega) := W$

Charakterisierung:

$$\omega \in \mathbf{\Omega}(D) \Leftrightarrow (\omega) \geq D \qquad \forall\, D \in Div\, \mathcal{F}.$$

Es gilt:

$$(f\omega) = (f) + (\omega) \qquad \forall\, f \in \mathcal{F}^*,\ 0 \neq \omega \in \mathbf{\Omega}_{\mathcal{F}}; \quad (5)$$

Beweis.
Fixiere $f \in \mathcal{F}^*$, $0 \neq \omega \in \mathbf{\Omega}_{\mathcal{F}}$, $W = (\omega)$.

$$\begin{aligned} D \leq W = (\omega) &\Leftrightarrow \omega \text{ annulliert } D, \\ &\Leftrightarrow f\omega \text{ annulliert } D + (f) \text{ nach (4)}, \\ &\Leftrightarrow D + (f) \leq (f\omega), \\ &\Rightarrow (\omega) + (f) = W + (f) \leq (f\omega); \end{aligned}$$

ebenso: $\quad (f\omega) + (f^{-1}) \leq (f^{-1} \cdot f\omega) = (\omega)$,
also auch $\quad (f\omega) \leq (\omega) - (f^{-1}) = (\omega) + (f)$.

Satz 4.3 *Der Raum der Differentiale $\mathbf{\Omega}_\mathcal{F}$ ist ein eindimensionaler $\mathcal{F}$-Vektorraum.*
Die kanonischen Divisoren bilden eine vollständige Divisorenklasse:

"kanonische Klasse" von $Div\,\mathcal{F}$.

Aus der zweiten Behauptung folgt die erste:
Fixiere $0 \neq \omega$. Sei $0 \neq \eta \in \mathbf{\Omega}_\mathcal{F} = \mathcal{F}\omega$ beliebig, $\eta = f\omega$, also $(\eta) = (f) + (\omega) \equiv (\omega)$.
Umgekehrt folgt aus $D \equiv (\omega)$ sofort

$$D = (f) + (\omega) = (f\omega) \in \mathbf{\Omega}_\mathcal{F}.$$

Beweis der ersten Behauptung. Es ist die Surjektivität der offensichtlich injektiven Abbildung

$$\mathcal{F} \xrightarrow{\cdot\omega} \mathbf{\Omega},\ f \mapsto f\omega\ (0 \neq \omega \in \mathbf{\Omega}(D) \text{ fixiert}),$$

zu verifizieren. Sei $\eta \in \mathbf{\Omega}(E)$. Wir vergrößern D, E zu $D' := D + B$ bzw. $E' := E + B$ mit geeignetem effektiven Divisor B (Existenz ist zu zeigen), so daß

$$\mathcal{L}(D') \cdot \omega \ \cap\ \mathcal{L}(E') \cdot \eta \neq O. \tag{6}$$

Aus (6) folgt die Surjektivität: Sei

$$0 \neq f\omega = g\eta \in \mathcal{L}(D') \cdot \omega \ \cap \ \mathcal{L}(E') \cdot \eta;$$

dann ist $\eta = \frac{f}{g}\omega \in \mathcal{F}\omega$.

Nach Riemanns Satz gilt für hinr. großes B

$$\mathfrak{l}(D') - \deg(D') = \chi = \mathfrak{l}(E') - \deg(E'),$$

und nach Riemann-Roch auch

$$-\mathfrak{l}^*(-B) = \deg(-B) + \chi.$$

$$
\begin{aligned}
&\dim \mathcal{L}(D') \cdot \omega + \dim \mathcal{L}(E') \cdot \eta - \dim \boldsymbol{\Omega}(-B) \\
&= \mathfrak{l}(D') + \mathfrak{l}(E') - \mathfrak{l}^*(-B) \\
&= (\deg D' + \chi) + (\deg E' + \chi) + (\deg(-B) + \chi) \\
&= (\deg D + \deg E + 2 \cdot \deg B) + \deg(-B) + 3 \cdot \chi \\
&= \deg B + \deg D + \deg E + 3\chi \\
&> 0 \text{ für große } B.
\end{aligned}
$$

Wegen (4) gilt

$$\mathcal{L}(D') \cdot \omega,\ \mathcal{L}(E') \cdot \eta \ \subseteq \ \boldsymbol{\Omega}(-B) = \begin{cases} D - D' \\ E - E' \end{cases}$$

und nach der Dimensionsformel für Durchschnitte von Unterräumen

$$\dim(\mathcal{L}(D') \cdot \omega \ \cap \ \mathcal{L}(E') \cdot \eta) \geq$$
$$\dim \mathcal{L}(D') \cdot \omega + \dim \mathcal{L}(E') \cdot \eta - \dim \boldsymbol{\Omega}(-B) > 0,$$

womit (6) und damit auch Satz 4.3 bewiesen sind.

Serre-Dualität:

$$\cdot\omega : \mathcal{L}(W-D) \xrightarrow{\sim} \mathbf{\Omega}(D), \ \ f \mapsto f\omega,$$

ist ein K-linearer Isomorphismus.

Beweis. Nach (4) bilden wir ab

$$\mathcal{L}(E) \times \mathbf{\Omega}(D) \xrightarrow{\cdot} \mathbf{\Omega}(D-E), \quad \text{folglich}$$

$$\mathcal{L}(W-D) \times \mathbf{\Omega}(W) \longrightarrow \mathbf{\Omega}((W-(W-D)) = \mathbf{\Omega}(D),$$

$$\mathcal{L}(W-D) \times \{\omega\} \xrightarrow{\cdot\omega} \mathbf{\Omega}(D), \quad (f,\omega) \mapsto f\cdot\omega.$$

Surjektivität: $\mathbf{\Omega}(D) \ni \eta = f\omega$ nach Satz 4.3,

$$f\omega \in \mathbf{\Omega}(D) \Leftrightarrow (f) + (\omega) = (f\omega) \geq D \Leftrightarrow$$

$$(f) \geq D - (\omega) = D - W \Leftrightarrow f \in \mathcal{L}(W-D).$$

Nullstellen und Pole von Differentialen

Schreibe: $(\omega) = \sum_{P \in \mathbb{P}_{\mathcal{F}}} v_P(\omega) \cdot P$.

Def initionen 4.4

$v_P(\omega)$ heißt "Nullstellenordnung" von ω in P.
Das $\mathbb{A}_{\mathcal{F}}$-Differential ω ist "regulär" an der Stelle P gdw. $v_P(\omega) \geq 0$.

Andernfalls heißt P "Polstelle" von ω und $-v_P(\omega) > 0$ die "Polordnung" von ω an dieser Stelle.

Satz 4.5 *Für jeden kanonischen Divisor* $W = (\omega)$ *gilt*

(i) $\mathfrak{l}(W) = g = 1 - \chi_{\mathcal{F}}$,

(ii) $\mathfrak{l}^*(W) = 1$,

(iii) $\deg W = 2g - 2$.

Für alle Divisoren $D \in Div\mathcal{F}$, $D^* := W - D$, *gilt*

(iv) $\mathfrak{l}^*(D) = \mathfrak{l}(D^*) = \mathfrak{l}(W - D)$,

(v) $\mathfrak{l}^*(D) = 0$ *falls* $\deg D > 2g - 2$,
(dies sind δ*-maximale Divisoren.)*

Beweis. (iv) folgt aus $L(W-D) \cong \Omega(D)$ und

$$\dim \Omega(D) = \mathfrak{l}^*(D).$$

(iv) $\Rightarrow$ (i): mit $D = O$;
(iv) $\Rightarrow$ (ii): $\mathfrak{l}^*(W) = \mathfrak{l}(W^*) = \mathfrak{l}(O) = 1$;
(i),(ii) $\Rightarrow$ (iii): benutze Riemann-Rochschen Satz:

$$\begin{aligned} \deg W &= deg(W-O) = (\mathfrak{l}-\mathfrak{l}^*)(W) - (\mathfrak{l}-\mathfrak{l}^*)(O) \\ &= (g-1)-(1-g) = 2g-2. \end{aligned}$$

(v): $\deg(W-D) < 0 \;\Rightarrow\; \mathfrak{l}^*(D) = \mathfrak{l}(W-D) = 0$;
sonst wäre $W - D \equiv E \geq O$ und dann
$\deg(W-D) \geq 0$, Widerspruch.

Satz 4.6 *(Kanonische Version des Riemann-Rochschen Satzes)*

$$\mathfrak{l}(D) - \mathfrak{l}(D^*) = \deg D + 1 - g,$$

$$\mathfrak{l}(D) - \mathfrak{l}(W - D) = \deg D + 1 - g.$$

* bzgl. (beliebigen) f ixierten kanonischen Divisor $W = (\omega)$,

$$Div\,\mathcal{F} \xrightarrow{\ *\ } Div\,\mathcal{F},$$

$$D \mapsto D^* = W - D$$

$$D' \equiv D \Rightarrow D'^{*} \equiv D^{*}$$
$$D^{**} = D$$

Spiegelung von $Div\,\mathcal{F}$ an einen kanonischen Divisor induziert
Spiegelung von $Pic\,\mathcal{F}$ an der kanonischen Klasse:

$$\begin{array}{ccc} Div\,\mathcal{F} & \xrightarrow{*} & Div\,\mathcal{F} \\ \downarrow & & \downarrow \\ Pic\,\mathcal{F} & \xrightarrow{*} & Pic\,\mathcal{F} \end{array}$$

Lokale Adéle:

$$\mathbb{I} := (\delta_{P,P})_{P\in\mathbb{P}_{\mathcal{F}}} = (..1..,1,..1..)$$

$$\mathbb{I}_P := (\delta_{P,Q})_{Q\in\mathbb{P}_{\mathcal{F}}} = (..0..,1,..0..)$$

$$\delta_{P,Q} := \begin{cases} 1, & P = Q \\ 0, & P \neq Q \end{cases}$$

$$\mathbb{A}_P := \mathcal{F}\cdot\mathbb{I}_P = \{f\cdot\mathbb{I}_P;\ f\in\mathcal{F}\} = \mathbb{I}_P\cdot\mathbb{A}$$

$$= \{(..0..,f,..0..);\ \mathcal{F}\ni f \text{ an } P\text{-ter Stelle}\}$$

$$\mathcal{F} \xrightarrow{\cdot\mathbb{I}_P} \mathbb{A}_P \xhookrightarrow{\iota_P} \mathbb{A} \overset{\cdot\mathbb{I}_P}{\twoheadrightarrow} \mathbb{A}_P$$

Lokale Differentiale:

$$\omega_P \;:= \omega \circ \mathbb{I}_P : \; \mathbb{A} \longrightarrow \mathbb{A}_P \longrightarrow K$$

Global-Lokal-Zerlegung:

$$\omega = \sum_P \omega_P, \qquad \text{meint:}$$

$$\omega(\mathfrak{a}) = \sum_P \omega_P(\mathfrak{a}) \qquad \forall\, \mathfrak{a} \in \mathbb{A}.$$

$\omega_P(\mathfrak{a}) = 0$ für fast alle P:

$\omega \in \mathbf{\Omega}(D)$, verschwindet auf $\mathbb{A}(D)$.

Sei $\mathfrak{a} = (a_P)_{P \in \mathbb{P}_{\mathcal{F}}} \in \mathbb{A}(E)$,

$$\omega_P(\mathfrak{a}) = \omega(..0.., a_P, ..0..) = 0$$

falls $v_P(a_P) \geq -v_P(D)$. Ist für fast alle P erfüllt, da fast immer $v_P(a_P) \geq 0$ und $v_P(D) = 0$. Sei $S \subset \mathbb{P}_{\mathcal{F}}$ die endliche Ausnahmemenge. Mit

$$\begin{aligned} \mathfrak{a}_P &:= \mathbb{I}_P \cdot \mathfrak{a} = (..0.., a_P, ..0..) \\ \mathfrak{a}_S &:= \sum_{P \in S} \mathfrak{a}_P \end{aligned}$$

$$\mathfrak{a} = \mathfrak{a}_S + \mathfrak{a}'_S, \ \mathfrak{a}'_S \in \mathbb{A}(D) \subseteq \omega^{\perp},$$

erhält man

$$\begin{aligned}\omega(\mathfrak{a}) &= \omega(\mathfrak{a}_S + \mathfrak{a}'_S) = \omega(\mathfrak{a}_S) + \omega(\mathfrak{a}'_S) \\ &= \omega(\mathfrak{a}_S) + 0 = \sum_{P\in S} \omega(\mathfrak{a}_P) \\ &= \omega\left(\sum_{P\in S} \mathfrak{a}_P\right) = \sum_{P\in S} \omega_P(\mathfrak{a}).\end{aligned}$$

Verschwindungs-Satz für Summen lokaler Differentiale auf $\mathcal{F}$.

$$\sum_{P\in\mathbb{P}_\mathcal{F}} \omega_P(\mathfrak{f}) = 0, \quad \forall\, \mathfrak{f} = Ad(f),\ f \in \mathcal{F}. \tag{7}$$

denn: Summe $= \omega(Ad(f)) = 0$ nach Def. von $\boldsymbol{\Omega}_{\mathcal{F}}$.

Def inition 4.7

$$res_P(\omega) \;:= \omega_P(1) = \omega_P(\mathbb{I}) = \omega(..0..,1,..0..) \in K$$

heißt "Residuum" des Differentials ω an der Stelle P.

Aus (7) angewandt auf $f = 1$ folgt unmittelbar der

Residuensatz 4.8 $\sum\limits_{P \in \mathbb{P}_{\mathcal{F}}} res_P(\omega) = 0.$

Identif izieren:

$$\mathcal{F} \ni f = Ad(f) = f \cdot \mathbb{I} = \mathfrak{f} \in \mathbf{\Omega}$$, also auch

$$\omega_P(f) := \omega_P(Ad(f)) = \omega_P(f \cdot \mathbb{I}) = \omega_P(\mathfrak{f}).$$

Eigenschaften:

a) $\omega_P(\mathfrak{a}) = 0 \Leftrightarrow v_P(\mathfrak{a}) \geq -v_P(\omega)$;

b) $\omega_P(f) = 0 \Leftrightarrow f\omega$ regulär in P;

c) $\omega_P(1) = 0 \Leftrightarrow \omega$ regulär in P;

d) $v_P(\omega) \geq k \Leftrightarrow \omega_P(f) = 0 \quad \forall\, f \in \mathfrak{p}^{-k}$;

e) $(f\omega)_P(\mathfrak{a}) = \omega_P(f\mathfrak{a})$;

f) $res_P(f\omega) = \omega_P(f) = f(P) \cdot \omega_P(1) f(P) \cdot res_P\omega$
falls P Punkt ist, f regulär in P und
$v_P(\omega) \geq -1$.

Beweise. a) Mit $W = (\omega)$ gilt

$$0 = \omega_P(\mathfrak{a}) = \omega(\mathfrak{a}_P) \Leftrightarrow \mathfrak{a}_P \in \mathbb{A}(W)$$
$$\Leftrightarrow v_P(\mathfrak{a}_P) \geq -v_P(W) = -v_P(\omega).$$

b),c):

$$\omega_P(f) = 0 \Leftrightarrow v_P(f) \overset{a)}{\geq} -v_P(\omega) \Leftrightarrow v_P(f\omega) \geq 0.$$

d) $v_P(\omega) \geq k \Leftrightarrow v_P(f\omega) \geq 0 \quad \forall\, f \in \mathfrak{p}^{-k}$

$$\overset{b)}{\Leftrightarrow} \omega_P(f) = 0 \quad \forall\, f \in \mathfrak{p}^{-k} = t_P^{-k}\mathcal{O}_P.$$

e) $(f\omega)_P(\mathfrak{a}) = f\omega(\mathfrak{a}_P) = \omega(f\mathfrak{a}_P)$

$$= \omega((f\mathfrak{a})_P) = \omega_P(f\mathfrak{a}).$$

f) $f = c + f_1,\ c = f(P) \in K,\ f_1 \in \mathfrak{p}$;

$$\omega_P(f) = \omega_P(c) + \omega_P(f_1) \overset{d)}{=} \text{(mit } k = -1\text{)}$$

$$= \omega_P(c \cdot 1) = f(P) \cdot \omega_P(1).$$

Satz 4.9 *Zu vorgegebenen Punkten $P_1, ..., P_n$ existiert ein Differential $\eta \in \mathbf{\Omega}_{\mathcal{F}}$ mit einfachen Polen und Residuen 1 an diesen Stellen.*

Beweis. Wähle $\omega \in \mathbf{\Omega}_{\mathcal{F}}$ mit einfachen Polen in den P_i. Dies ist nach dem Approximationssatz 2.2 möglich: Nämlich zu beliebigem $0 \neq \omega \in \mathbf{\Omega}$ existiert $f \in \mathcal{F}$ mit $v_i(f) = -v_i(\omega) - 1$. Dann gilt

$$v_i(f\omega) = v_i(f) + v_i(\omega) = -1, \ i = 1, .., n, \ (v_i = v_{P_i}).$$

Sei $$r_i \ := res_{P_i}\omega = \omega_{P_i}(1) \overset{c)}{\in} K^*.$$

Wieder mit Hilfe des Approximationssatzes nehmen wir eine Funktion g mit $v_i(g - r_i) > 0$, $i = 1, .., n$. Es folgt

$$g \in \mathcal{O}_{P_i},\ g \equiv r_i \mod \mathfrak{p}_i,\ \Rightarrow v_i(g) = 0.$$

Setzen $\eta := g^{-1}\omega$; dann gilt

$$v_i(\eta) = v_i(g^{-1}) + v_i(\omega) = v_i(\omega) = -1;$$

$$res_{P_i}(\eta) = \eta_{P_i}(1) = (g^{-1}\omega)_{P_i}(1) = \omega_{P_i}(g^{-1})$$

$$\overset{f)}{=} g^{-1}(P_i) \cdot \omega_{P_i}(1) = r_i^{-1} \cdot r_i = 1.$$

$\square$

5 Grundbegriffe der Codierung

"Alphabet": $\mathbb{F} = \mathbb{F}_q$ endlicher Körper, $q = p^r$;
"Wörter" (der Länge n): Elemente von $\mathbb{F}^n$;

"Code" (linear): $\mathbb{F}$-linearer Unterraum C von $\mathbb{F}^n$;

Code-"Dimension": $k = k_C = \dim C = \dim_{\mathbb{F}} C$;

"Hamming-Gewicht" eines Wortes $c = (c_1, ..., c_n)$:

$$w(c) \ := \#\{i;\ c_i \neq 0\};$$

"Hamming-Abstand" zweier Wörter:

$$\delta(a, b) \ := w(a - b);$$

"Minimalabstand" (-"Distanz") in/von C:

$$d = d_C \ := \min\{w(c);\ 0 \neq c \in C\};$$

"Fehlerkorrektur-Index": $e = e_C = \left[\frac{d-1}{2}\right]$.

Eigenschaften:

- $w(a) = 0 \Leftrightarrow a = 0$;
- $w(a + b) \leq w(a) + w(b)$;
- $\delta(a, b) = 0 \Leftrightarrow a = b$;
- $\delta(b, a) = \delta(a, b) = \delta(a + c, b + c) = w(a - b)$;
- $\delta(a, c) \leq \delta(a, b) + \delta(b, c)$ (Dreiecksungleichung).

Beweis.
$$w(a - c) = w((a - b) + (b - c)) \leq w(a - b) + w(b - c).$$

Gebrauch des Fehlerkorrektur-Indexes:

Ist $a \in \mathbb{F}^n$ ein Wort, das von einem Wort $c \in C$ höchstens an e Stellen abweicht, so ist $c \in C$ durch diese Eigenschaft eindeutig bestimmt.

Beweis. Sei auch $\delta(a, c') \leq e$, $c' \in C$. Dann gilt

$$\begin{aligned} w(c - c') = \delta(c, c') &\leq \delta(c, a) + \delta(a, c') \\ &\leq 2e \leq 2 \cdot \frac{d-1}{2} < d, \end{aligned}$$

also $c - c' = 0$, letztlich $c' = c$.

"Typ" des Codes: $(n, k, d) = (n, k_C, d_C)$.

Lemma 5.1 *(Singleton). Für Codes C vom obigen Typ gilt stets*

$$d = d_C \leq n - k + 1 \text{ "Singleton-Schranke".}$$

Beweis.

$$V := \mathbb{F}^{d-1} \times O \subseteq \mathbb{F}^n, \; V \cap C = O,$$

$$k + (d-1) = \dim C + \dim V = \dim(C + V) \leq n.$$

Def inition 5.2 *Der Code C heißt "optimal" (auch MDS-code) genau dann, wenn d_C den Wert dieser Schranke annimmt.*

"Inneres Produkt" $\mathbb{F}^n \times \mathbb{F}^n \longrightarrow \mathbb{F}$:
nichtentartete symmetrische Bilinearform

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

$$a = (a_1, .., a_n), b = (a_1, .., b_n) \in \mathbb{F}^n$$

"Orthogonalität": $a \perp b$ gdw. $< a, b >= 0$.
Dualer Code

$$C^{\perp} \ := \{a \in \mathbb{F}^n;\ a \perp c \quad \forall\, c \in C\}.$$

$$\dim C^\perp = n - \dim C \quad , \quad C^{\perp\perp} = C.$$

"Generatormatrix" $G \in Mat_{d\times n}(\mathbb{F})$ des Codes C: Basis von C in den Zeilen.

"Prüfmatrix" $P \in Mat_{(n-d)\times n}(\mathbb{F})$ von C: Generatormatrix von $C^\perp$.

$$c \in C \Leftrightarrow c \cdot {}^tP = O$$

P heißt auch "Kontrollmatrix" von C.

6 Funktionale Goppa-Codes und Riemann-Rochscher Satz

Vorgaben:

- Funktionenkörper $\mathcal{F}$ über endlichem Körper $\mathbb{F}$;
- "Punkt-Divisor" (reduziert)

$$D = P_1 + P_2 + \cdots + P_n,$$

$$P_i \in \mathbb{P}(\mathbb{F}),\ P_i \neq P_j,\ i \neq j;$$

- "Polschranken-Divisor":

$$G = \sum_j m_j Q_j \in Div\,\mathcal{F},$$

separiert von D, d.h. $P_i \neq Q_j \,\forall\, i, j$.

(Funktionaler) "Goppa-Code" in $\mathbb{F}^n$:

$$C(D,G) \;:= \{f(D) = (f(P_1), .., f(P_n));\; f \in \mathcal{L}(G)\}$$

Bild der Werte-Abbildung

$$\mathcal{L}(G) \longrightarrow \mathbb{F}^n,\; f \mapsto f(D).$$

Exakte Folge von $\mathbb{F}$-Vektorräumen:

$$O \to \mathcal{L}(G-D) \to \mathcal{L}(G) \to C(D,G) \to O \tag{8}$$

$\Rightarrow$ Dimensions-Formel

$$k = \dim C(D,G) = l(G) - l(G-D) \tag{9}$$

Minimaldistanz-Abschätzung

$$d \geq \delta \ := n - \deg G; \tag{10}$$

Beweis. Sei $c = f(D) \in C = C(D,G)$ Wort mit minalem Hamming-Gewicht d, o.B.d.A. $f(P_1), .., f(P_d) \neq 0,$

$$f(P_{d+1}) = \ldots = f(P_n) = 0.$$

$$\Rightarrow$$

$$0 \neq f \in \mathcal{L}(G - (P_{d+1} + \ldots + P_n)),$$

$$\deg(G - (P_{d+1} + \ldots + P_n)) \geq 0,$$

$$\deg G - (n - d) \geq 0.$$

$\square$

Def inition 6.1 $\delta = n - \deg G$ *heißt "designierte Minimaldistanz" des Goppa-Codes* $C(D, G)$.

Unter der speziellen Voraussetzung

$$0 < \deg G < n \qquad \text{(sp)}$$

gilt

i) $\mathcal{L}(G) \to \mathbb{F}^n$ ist injektiv;

ii) $k = \dim C(D, G) = \mathfrak{l}(G)$;

iii) $k \geq \deg G + 1 - g$;

iv) $d + k \geq n + 1 - g$;

v) $k = \deg G + 1 - g$ falls $\deg G > 2g - 2$;

vi) $C(D,G)$ ist optimal vom Typ $(\deg D, 1+\deg G, n-\deg G)$ falls $g=0$;

vii) $\delta = d$ gilt genau dann, wenn ein effektiver Divisor $D' \leq D$ existiert, der linear äquivalent zu G ist.

Beweis. i),ii): $\deg(G-D)<0 \Rightarrow O = \mathcal{L}(G-D)$ (Kern der Funtionswert-Abbildung);
iii) folgt aus Riemann-Rochschem Satz;
iv): addiere $d \geq \delta = n - \deg G$ in iii);
v): folgt aus $\mathfrak{l}^*(G)=0$, $k=\mathfrak{l}(G)$ und Riemann-Roch angewandt auf $G \in Div\,\mathcal{F}$;

vi): nach iv) gilt $d \geq n+1-k$;
aber auch $d \leq n+1-k$ (Singleton-Schranke);
$k = 1 + \deg G$ nach v); $d = n+1-k = n - \deg G$.

vii), ($\Rightarrow$): Nach Voraussetzung gilt

$$n - d = n - \delta = n - (n - \deg G) = \deg G.$$

Wähle Wort $f(D) \in C(D,G)$ mit Minimalgewicht d, o.B.d.A.

$$f(P_1), .., f(P_{\deg G}) = 0; \;\; f(P_j) \neq 0, \; n - d < j \leq n.$$

Für $D' := \sum_{i=1}^{n-d} P_i \leq D$ gilt $\deg D' = n - d = \deg G$.

also $\deg(G - D') = 0$ und $f \in \mathcal{L}(G - D') \neq O$, also ist $G - D'$ Hauptdivisor nach Lemma 3.6, mithin $G \equiv D'$.

($\Leftarrow$): Sei o.B.d.A. $D' = P_1 + \ldots + P_{\deg G}$. In $\mathcal{L}(G - D')$ existiert $f \neq 0$. Nach i) gilt $O \neq f(D) \in C(D; G)$, ferner $w(f(D)) \leq n - \deg G$ wegen $f(P_1) = \ldots = f(P_{\deg G}) = 0$, also $d \leq n - \deg G = \delta \leq d$, somit $d = \delta$.

Satz 6.2 *Zu jedem Punkt-Divisor* $D = P_1 + ...P_n$ *und Teildivisor* $O < D' < D$ *existiert ein Goppa-Code* $C(D, G)$*, dessen Minimaldistanz* d *mit der designierten* $\delta = n - \mathfrak{l}(G)$ *übereinstimmt.*

Beweis . Nach vii) braucht nur ein Divisor $G \equiv D'$ gefunden zu werden, der separiert zu D ist. Die Existenz folgt aus dem folgenden

Moving Lemma 6.3 . *Zu jedem Divisorenpaar* D*,* E *existiert ein von* D *separierter Divisor* E' *in der Divisorenklasse von* E*.*

Beweis . (mit Approximations-Satz). Seien

$$D = \sum_{i=1}^{r} k_i P_i;$$

$$E = \sum_{i=1}^{r} m_i P_i + \sum_{j=1}^{s} n_j Q_j;$$

$$k_i, m_i,\ n_j \in \mathbb{Z},\ \ P_i \neq Q_j \quad \forall\, i, j;$$

t_i lokaler Parameter in P_i, $i = 1, ..., r$.

Nach dem Approximationssatz existiert $h \in \mathcal{F}$ mit

$$v_i(h - t_i^{-m_i}) = N >> 0, \; i = 1, ..., n.$$

Daraus folgt $v_i(h) = -m_i$. Für $E' := E + (h)$ gilt dann

$$v_i(E') = v_i(E + (h)) = v_i(E) + v_i(h) = m_i - m_i = 0$$

für alle i, also $supp\, E' \cap supp\, D = \emptyset$.

$\square$

Satz 6.4 . *Zu jedem Punktdivisor $D = P_1 + ... + P_n$ und jeder Divisorenklasse $\mathcal{G}$ existieren Goppa-Divisoren $C(D, G)$ mit $G \in \mathcal{G}$. Je zwei solcher Goppa-Divisoren $C(D, G)$ und $C(D, G')$, sind einander ähnlich.*

Def inition 6.5 *Zwei Codes $C, C' \subseteq \mathbb{F}^n$ heißen "ähnlich" genau dann, wenn ein $\mathbb{F}$-linearer Isomorphismus von $\mathbb{F}^n$ auf sich existiert, der C in C' überführt und der bzgl. der kanonischen Basis durch eine Diagonalmatrix repräsentiert wird.*

Bemerkung 6.6 . *Ähnliche Codes sind vom gleichen Typ.*

Beweis von Satz 6.4. Sei $G \equiv G'$, $G' = G - (h)$, $h \in \mathcal{F}$. Da G und G' von D separiert sind, trifft dies auch für $(h) = G - G'$ zu. Daher ist $H := diag(h(P_1), ..., h(P_n))$ eine invertierbare Diagonalmatrix. Nun betrachte

$$\begin{tikzcd}
\mathcal{L}(G-D) \arrow[r] \arrow[d, "\wr"] & \mathcal{L}(G) \arrow[r] \arrow[d, "\cdot h"] & C(D,G) \arrow[r] \arrow[d, "\wr"] & \mathbb{F}^n \arrow[d, "\cdot H"] \\
\mathcal{L}(G'-D) \arrow[r] & \mathcal{L}(G') \arrow[r] & C(D,G') \arrow[r] & \mathbb{F}^n
\end{tikzcd}$$

7 Kanonische Goppa-Codes

Sei $C(D,G)$ ein Goppa-Code, W ein kanonischer Divisor, o.B.d.A. (nach Satz 6.4) $W-(G-D)$ separiert von $D = P_1 + ... + P_n$.

Def inition 7.1 . *"kanonischer Goppa-Code"* $C^*(D,G) := C(D,(G-D)^*) = C(D,W-(G-D))$, *zu D,G gehörig; genauer $C^*_\omega(D,G)$, mit $W=(\omega)$.*

Bemerkung 7.2 . *Der kanonische Goppa-Code $C^*(D,G)$ ist bis auf Ähnlichkeit eindeutig durch D, G bestimmt; sein Typ (n,k^*,d^*) sogar eindeutig.*

"Designierter Typ" von $C^*(D,G)$

$$(n^*, k^*, \delta^*) = (n, n-k, (n-\delta) - (2g-2)) =$$
$$(\deg D, \deg D - \mathfrak{l}(G) + \mathfrak{l}(G-D), \deg G - (2g-2)) : \tag{11}$$

$$\begin{aligned} k^* &= \mathfrak{l}((G-D)^*) - \mathfrak{l}((G-D)^* - D) \\ &= \mathfrak{l}^*(G-D) - \mathfrak{l}(W-G) = \mathfrak{l}^*(G-D) - \mathfrak{l}^*(G) \\ &= \mathfrak{l}(G-D) - \mathfrak{l}(G) + \deg D = -k + n, \end{aligned}$$

unter Verwendung der homogenen Riemann-Roch-Formel (3), Seite 75.

$$\delta^* = n - \deg(G-D)^* = n - \deg(W - G + D)$$
$$= \deg G - (2g-2).$$

Goppa-Residuen-Codes

$D = P_1 + ... + P_n$, $G \in Div\mathcal{F}$ wie bisher.

$Res_D : \mathbf{\Omega} \longrightarrow \mathbb{F}^n$, $\mathbb{F}$-linear

$$\omega \mapsto Res_D(\omega) \ := (res_{P_1}(\omega), .., res_{P_n}(\omega))$$

Def inition 7.3 *Die Codes*

$$C^{\Omega}(D,G) \ := Res_D(\Omega(G-D)) \subseteq \mathbb{F}^n$$

heißen "Goppa-Residuen-Codes".

Bemerkung 7.4 . *Für rationale Funktionenkörper $\mathcal{F} = \mathbb{F}(X)$ waren dies die originalen von Goppa eingeführten Codes.*

Theorem 7.5 . *Sei $\eta \in \mathbf{\Omega}_{\mathcal{F}}$ Differential mit*

$$v_i(\eta) = -1,\ res_{P_i}\eta = \eta_{P_i}(1) = 1,\ i = 1, .., n,$$

welches nach Satz 4.9 existiert. Für den kanonischen Goppa Code bzgl. $W = (\eta)$

$$C^*_\eta(D, G) = C(D, (G - D)^*) = C(D, (\eta) - (G - D))$$

gilt $$C^\Omega(D, G) = C^*_\eta(D, G).$$

Beweis . $\omega \in \Omega(G-D) \Leftrightarrow (\omega) \geq G-D$;

$$\omega = f\eta \in \Omega(G-D) \Leftrightarrow (f)+(\eta) \geq G-D$$
$$\Leftrightarrow (f) \geq -(\eta)+G-D \Leftrightarrow f \in \mathcal{L}((G-D)^*)$$

Wegen $-1 \leq v_i(\omega) = v_i(f\eta) = v_i(f)-1$ ist f regulär in den Punkten P_i. Folglich gilt nach f) auf Seite 101

$$\begin{aligned}(res_{P_1}\omega, ..., res_{P_n}\omega) &= (res_{P_1}(f\eta), ..., res_{P_n}(f\eta)) \\ &= (f(P_1)\cdot res_{P_1}\eta, ..., f(P_1)\cdot res_{P_n}\eta) \\ &= (f(P_1), ..., f(P_n)) = f(D).\end{aligned}$$

Durchläuft $\omega = f\eta$ den Raum $\Omega(G-D)$, so durchläuft f den Raum $\mathcal{L}((G-D)^*)$, woraus nun insgesamt

$$C^{\Omega}(D,G) = Res_D(\Omega(G-D)) = C^*(D,G) \qquad (12)$$

folgt.

□

Korollar 7.6 *Die Ähnlichkeitsklassen von Goppa-Residuen-Codes, kanonischen Goppa-Codes und funktionalen Goppa-Codes stimmen überein.*

Aus (12) folgt die Übereinstimmung für Residuen- und kanonische Codes. Jeder kanonische Code ist nach Def inition ein funktionaler Code. Darum braucht nur noch gezeigt zu werden, daß die funktionalen Goppa-Codes bis auf Ähnlichkeit kanonisch sind:

$$\begin{aligned} C(D,G) &= C(D, W-(W-(G-D))-D) \\ &= C(D, W-((G-D)^{*}-D)) \\ &= C^{*}(D,(G-D)^{*}). \end{aligned}$$

Theorem 7.7 . *Der funktionale Goppa-Code $C(D,G)$ ist der zum kanonischen Goppa-Code $C^{\Omega}(D,G) \sim C^{*}(D,G)$ duale Code in $\mathbb{F}^n$.*

Beweis (über Residuensatz). Sei $f \in \mathcal{L}(G)$, $\omega \in \Omega(G-D)$, somit $f\omega \in \Omega(-D)$ und wegen f), Seite 101,

$$res_{P_i}(f \cdot \omega) = f(P_i) \cdot res_{P_i}\omega, \;\; i = 1, ..., n.$$

Es folgt weiterhin, da $f\omega$ außerhalb D regulär ist, daß $f\omega$ außerhalb D kein Residuum hat, also

$$< f(D), Res_D\,\omega > = \sum_{i=1}^{n} f(P_i) \cdot res_{P_i}\,\omega$$

$$= \sum_{i=1}^{n} res_{P_i}(f \cdot \omega) = \sum_{P} res_P(f\omega) = 0,$$

unter Verwendung des Residuensatzes 4.8. Nun erhält man die Orthogonalitäts-Relationen

$$f(D) \perp Res_D\,\omega \quad \forall\, f \in \mathcal{L}(G),\ \omega \in \Omega(G-D);$$
$$C(D,G) \perp C^{\Omega}(D,G),\ C^{\Omega}(D,G) \subseteq C(D,G)^{\perp}.$$

Die Dimensionsgleichheit

$$\begin{aligned}\dim C^{\Omega}(D,G) &= \dim C^{*}(D,D) = k^{*} \overset{(11)}{=} n-k \\ &= n - \dim C(D,G) = \dim C(D,G)^{\perp}\end{aligned}$$

führt schließlich zu $C^{\Omega}(D,G) = C(D,G)^{\perp}$.

$\square$

8 Fehlerkorrektur-Algorithmus von Skorobogatov / Vladut

Fehlerkorrektur (ca. 1990) für kanonischen Goppa-Code

Minicode-Beispiel: Tonleiter-Code $C^* \subset \mathbb{F}_2^7$ def iniert durch Generator-Matrix

$$P = \begin{pmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix} \in Mat_{3\times 7}(\mathbb{F}_2).$$

P prüft Zugehörigkeit zum dualen Code

$$C \ := C^{*\perp} \subset \mathbb{F}_2^7.$$

und korrigiert einen Fehler: Sei $a = c + e \in \mathbb{F}_2^7$ fehlerhaftes Wort, $c \in C$; mit "Fehlervektor"

$$e = e_k = (0, .., 0, 1, 0, ..0),$$

1 an k-ter Stelle; k unbekannt. Ermittlung von k liefert das richtige Wort $c = a - e_k$.

"P-Syndrom" von a:

$$S_P(a) \ := P^t a = P^t e = S_P(e) = k\text{-te Spalte von } P.$$

$$k = (2^0, 2^1, 2^2) \cdot S(a) \text{ in } \mathbb{Z}^3.$$

$a \in \mathbb{F}^n$, fehlerhaftes Wort, $a = c + e \in \mathbb{F}^n$, $c \in C$, $e \in \mathbb{F}^n$ Fehler;

Arbeits-Hypothese: $\qquad w(e) \leq t$, $t \in \mathbb{N}_+$, fest gewählt,

Fehler-Korrektur-Algorithmus von Vladut / Skorobogatov (1990):

A) Fehlerstellen in a ermitteln;

B) Fehlervektor e und damit korrigiertes Code-Wort $c = a - e$ ermitteln;

für Wörter in kanonischen Goppa-Codes

$$C^* = C^\Omega(D, G) = C(D, G)^\perp = C^\perp.$$

(jeder Goppa-Code ist bis auf Ähnlichkeit so darstellbar).

1. Wahl von t (maximal zulässige Zahl von Fehlerstellen)
2. Wahl eines Goppa-Codes $C = C(D, G)$ mit designiertem dualem (d.h. von C^*) Fehlerkorrektur-Index

$$(\delta^* - 1)/2 \leq (d^* - 1)/2,$$

so daß :

(W) $0 < t \leq (\delta^* - 1)/2 - g/2$;

und Wahl eines Hilfsdivisor G' mit

(W') $\deg G' = g + t$

Resultierende Grundeigenschaften:

(I) $supp\, G' \cap supp\, D = \emptyset$
(o.B.d.A. nach Moving-Lemma);

(II) $\deg G' < \delta^* - t = \deg G - (2g - 2) - t$;

(III) $\mathfrak{l}(G') > t$;

(W) $\Rightarrow$ (III):

$$l(G') \overset{RR}{\geq} \deg G' + 1 - g \overset{(W)}{=} g + t + 1 - g = t + 1 > t;$$

(W),(W′) $\Rightarrow$ (II):

$$\delta^* - t - \deg G' \overset{(W')}{=} \delta^* - t - (t + g)$$
$$= \delta^* - 2t - g \overset{(W)}{\geq} 1 > 0.$$

A) Fehler-Lokalisierung

$$a = c + e,\ c \in C^*,\ e = (e_1, ..., e_n),\ w(e) \leq t.$$

"Fehlerdivisor" E (von a)

$$E := \sum_{e_i \neq 0} P_i \leq D = P_1 + ... + P_n.$$

"Fehlerlokalisierende Funktion" aus $\mathcal{L}(G')$ für $a = c + e$ bzgl. $C(D, G)$:

$$0 \neq f \in \mathcal{L}(G') \text{ mit } f(E) = O,$$

"Nullstellendivisor" von f auf D:

$$N(f) = N_D(f) \;:= \sum_{f(P_j)=0} P_j \leq D.$$

Äquivalenz:

$0 \neq f \in \mathcal{L}(G')$ fehlerlokalisierende Funktion
$\Leftrightarrow E \leq N(f) \Leftrightarrow f \in \mathcal{L}(G' - E)$.

Existenz. Zu zeigen:

(III′) $\mathfrak{l}(G' - E) > 0$, unter der Voraussetzung
$\deg E = w(E) \leq t$ (Fehlerschranke),

Erinnerung: $\quad \mathfrak{l}(A-P) \geq \mathfrak{l}(A) - 1$
für Divisoren A und Punkte $P \notin supp\ A$:

$$\begin{tikzcd}
\mathfrak{m}_P \arrow[r] & \mathcal{O}_P \arrow[r] & \mathfrak{k}_P = \mathbb{F} \\
\mathcal{L}(A-P) \arrow[r] \arrow[u] & \mathcal{L}(A) \arrow[r] \arrow[u] & \mathcal{L}(A)/\mathcal{L}(A-P) \arrow[u]
\end{tikzcd}$$

Anw. auf $A = G'$ und Punkte von E liefert (III′):

$$\mathfrak{l}(G'-E) \overset{(III)}{>} t - \deg E \geq t - t = 0.$$

Def inition 8.1 *Für $g \in \mathcal{L}(G)$ sei*

$$S_g(a) \;:= < a, g(D) > \in \mathbb{F}$$

das "g-Syndrom" von a.

Wegen $C^* \ni c = a - e \perp C(D, G)$ stimmen die Syndrome von a und seines Fehlervektors e für alle $g \in \mathcal{L}(D)$ überein:

$$S_g(a) = < a, g(D) > = < e, g(D) > = S_g(e).$$

Speziell für $g = fh$, $f \in \mathcal{L}(G')$, $h \in \mathcal{L}(G - G')$ gilt:

$$S_{fh}(a) = < a, hf(D) > = < e, hf(D) > = S_{fh}(e);$$

und falls f fehlerlokalisierende Funktion ist:

$$< a, fh(D) > = < e, hf(D) > = \sum_{i=1}^{n} e_i h(P_i) f(P_i) = 0.$$

Da eine fehlerlokalisierende Funktion

$$0 \neq f = x_1 b_1 + \ldots + x_l b_l,\ \ b_1, \ldots b_l$$ Basis von $\mathcal{L}(G')$,

existiert, ist das folgende homogene lineare "Syndrom-Gleichungssystem" echt lösbar.

$$
\begin{aligned}
< a, b_1 h_1(D) > \cdot X_1 + ... + < a, b_l h_1(D) > \cdot X_l &= 0,\\
< a, b_1 h_2(D) > \cdot X_1 + ... + < a, b_l h_2(D) > \cdot X_l &= 0,\\
\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\\
< a, b_1 h_r(D) > \cdot X_1 + ... + < a, b_l h_r(D) > \cdot X_l &= 0,
\end{aligned}
\tag{13}
$$

mit Basis $h_1, ..., h_r$ von $\mathcal{L}(G - G')$.

Es gilt die wichtige Umkehrung:

Satz 8.2 *Jede echte Lösung* $x_1, ..., x_l$ *des Syndrom-Gleichungssystems (13) liefert eine fehlerlokalisierende Funktion* $f = x_1 b_1 + ... + x_l b_l$ *für* a*.*

Beweis Nach (II) gilt

$$\deg(G - G' - E) \geq \deg G - \deg G' - t > 2g - 2,$$

daher (und erst recht)

$$\mathfrak{l}^*(G{-}G'{-}E) = 0 = \mathfrak{l}^*(G{-}G'{-}E'), \qquad \forall O \leq E' \leq E$$

Nach dem Riemann-Rochschen Satz sind die Dimenensionen $\mathcal{L}(G - G' - E')$ exakt berechenbar. Speziell gilt

$$\mathfrak{l}(G - G') - \#E' = \mathfrak{l}(G - G' - E'),$$
$$\mathfrak{l}(G - G' - E) + 1 = \mathfrak{l}(G - G' - (E - P)),$$

für alle Fehlerstellen $P \in supp\, E$. Damit gilt

Lemma 8.3 *Zu jeder Fehlerstelle P existiert eine Funktion $h = h_P \in \mathcal{L}(G - G')$ mit*

$$h(P) \neq 0, \;\; h(P_j) = 0 \quad \forall\, P_j \in supp\,(E - P). \tag{14}$$

Entstamme nun $f = x_1 b_1 + ... + x_l b_l$ einer Lösung des Gleichungssystems (13). Dieses verkürzt sich mit offensichtlichen Bezeichnungen zu

$$< a, fh(D) > = < e, fh(D) > = < e|_E, fh(E) > = 0$$

für alle $h \in \mathcal{L}(G - G')$. Speziell ergibt sich für h aus (14)

$$0 = < e|_E, fh(E) > = e_P \cdot fh(P) = e_P h(P) \cdot f(P),$$

also $f(P) = 0$ wegen $e_P h(P) \neq 0$.

Da f(P) = 0 für alle Trägerpunkte P von E gilt, ist f eine fehlerlokalisierende Funktion.

$\square$

B) Fehler-Korrektur

Sei f fehlerlokalisierende Funktion für $a = c + e \in \mathbb{F}^n$, also mit D-Nullstellendivisor

$$D \geq N \;:= N(f) = N_D(f) \geq E.$$

Für alle $g \in \mathcal{L}(G)$ gilt

$$\begin{aligned} < e|_N, g(N) > &= < e, g(D) > \\ &= < c + e, g(D) > = < a, g(D) > \end{aligned}$$

Damit ist der Vektor $e|_N \in \mathbb{F}^s$, $s := \# supp\, N$, eine Lösung des "inhomogenen linearen Syndrom-Gleichungssystems" von a bzgl. N.

$$< (Z_1, ..., Z_s), g(N) > = < a, g(D) >, \qquad (15)$$

wobei g eine Basis von $\mathcal{L}(G)$ durchläuft.

Lemma 8.4 *Das obige Gleichungssystem (15) ist eindeutig lösbar.*

Beweis Sei $(z_1, .., z_s) \in \mathbb{F}^s$ eine weitere Lösung, $z \ := (z_1, .., z_s, 0, .., 0) \in \mathbb{F}^n$. Das zugehörige homogene Gleichungssystem liefert

$$< z - e, g(D) > = < (z - e)|_N, g(N) > = 0 \quad \forall g \in \mathcal{L}(G)$$

und damit $b - e \perp C(D, G)$, also $b - e \in C^*$. Es genügt nun zu zeigen, daß $w(z - e) < \delta^*$ ist, weil das nur für $z - e = 0$ möglich sein kann.

Es sei daran erinnert, daß $N = N(f)$, $0 \neq f \in \mathcal{L}(G' - N)$, also $\deg(G' - N) \geq 0$ und somit $\deg N \leq \deg G'$ gilt. Nun folgt

$$
\begin{aligned}
w(z - e) = w(z|_N - e|_N) \leq s = \deg N \\
\leq \deg G' \overset{(II)}{<} \delta^* - t < \delta^* \leq d^*.
\end{aligned}
$$

$\square$

Fazit: Die Fehlerkorrektur kann durch Lösen zweier linearer Gleichungssysteme durchgeführt werden. Genauer hat man den folgenden

Fehlerkorrektur-Algorithmus

Man löst das homogene Syndrom-Gleichungs-system (13),
erhält als beliebige nichttriviale Lösung eine fehlerlokalisierende Funktion f mit D-Nulldivisor N der Länge s;
löst danach das inhomogene Syndrom-Gleichungssystem (15),
erhält als einzige Lösung den Fehlerkorrektur-vektor e.

Damit wird das korrigierte Wort $c = a - e$ gewonnen.

9 Vorträge

- 1.1 Diskrete Bewertungsringe eines Funktionenkörpers, 1 - 8;
- 1.2 Stellenringe, 8 - 16;
- 1.3 Grad von Stellen und Funktionswerte, 17 - 23;
- 2.1 Potenz- und Laurent-Reihen algebraischer Funktionen, 24 - 27;
- 2.2 Der Approximationssatz, 28 - 35;
- 2.3 Endliche Anzahl der Null- und Polstellen einer algebraischen Funktion, 36 - 45;
- 3.1 Adéle, Geschlecht und Divisoren, 45 - 52;
- 3.2 Endliche Dimension polbeschränkter Funktionen, 53 - 59;
- 3.3 Satz von Riemann, 60 - 66;
- 3.4 Satz von Riemann-Roch, 68 - 75;
- 4.1 Differentiale und kanonische Divisoren, 76 - 83
- 4.2 Serre-Dualität, 84 - 91

- 4.3 Invarianten von Divisorenklassen und Riemann-Rochscher Satz, 92 - 99;
- 4.4 Der Residuensatz und spezielle Diferentialformen, 99 - 105;
- 5.1 Hamming-Distanz von Code-Wörtern und Orthogonalität, 106 - 112;
- 6.1 Funktionale Goppa-Codes und Typ-Bestimmung, 113 - 121
- 6.2 Moving-Lemma und Ähnlichkeitsklassen, 121 - 124
- 7.1 Kanonische und duale Goppa-Codes, 125 - 135;
- 8.1 Fehler-Lokalisierung, 136 - 145;
- 8.2 Der Korrektur-Algorithmus, 145 - 155