Die Gaußsche Zahlenwelt

Von den Ursprüngen bis zum Brenn-Code

Prof. Dr. R.-P.Holzapfel,

seit 1958

Deutsche (Preußische) Akademie

der Wissenschaften, Berlin-Adlershof,

(gegr. v. W.Leibniz, gefördert v. L.Euler, A.Humboldt)

z.Z. Humboldt-Universität

1. Vorlesung (I): Von den Ursprüngen zu Gauß und öffentlicher Verschlüsselung

2. Vorlesung (II): Von Gauß zu Cauchy

3. Vorlesung (III): Von Gauß/Cauchy zu Goppa- und Brenn-Code

I. **Zusammenfassung der ersten Vorlesung (AlgebraischArithmetischGeometrischAnalytische Grundlagen)**

I.1 Algebraische Grundbegriffe, Caesar-Kryptographie

I.2 Heutige Anwendung: Öffentliche Verschlüsselung

II. Die Riemannsche Kugel über beliebigen Körpern

II.1 Geometrische Grundbegriffe

II.2 Bewertungen, Stellen und Funktionswerte

II.3 Potenzreihen

II.4 Divisoren und Funktionsräume

II.5 Algebraische Differentialformen

II.6 Kanonische Divisoren und Residuen

II.7 Riemann-Rochscher Satz

II.8 Logarithmische Differentialformen und der Residuen-Satz

III. **Anwendung in der Codierungstheorie**

III.1 Grundbegriffe der Codierungstheorie

III.2 Goppa-Codes auf $\mathbb{P}(\mathbb{F})$

III.3 Beispiel eines Brenn-Codes

1 Zusammenfassung der ersten Vorlesung

1.1 Agebraische Grundbegriffe und Cäsar-Kryptographie

AXIOME:

- Gruppe: $(G, \cdot)$ mit (Axiomen):
  (Ass), (Neut), (Inv) bzgl. $\cdot$ (Multiplikation)

- Abelsche Gruppe $(A, +)$ mit:
  (Ass), (Neut), (Inv), (Komm)
  bzgl. $+$ (Addition)
  Synonym: Additive Gruppe
  auch multiplikative Schreibweise möglich
  ($\cdot$ statt $+$)
  Synonym: Kommutative Gruppe

- Ring: $(R, +, \cdot)$ mit:
  (Ass $+$), (Neut $+$), (Inv $+$), (Komm $+$)
  bzgl. Addition
  (Ass $\cdot$) bzgl. Multiplikation
  ($\cdot$ Distr), (Distr $\cdot$) Distributivgesetze
- Kommutativer Ring: außerdem
  (Komm $\cdot$)

- Kommutativer Ring mit Einselement: außerdem
(Neut $\cdot$)
- Integritätsbereich: außerdem
(Kürz $\cdot$) $a \cdot b = a \cdot c,\ a \neq 0 \Longrightarrow b = c$
Kürzungsregel (der Multiplikation)

- Körper K: außerdem
  (Inv ·)* Existenz eines Inversen a^{-1} für alle
  $a \neq 0$
  äquivalent:
  $(K, +)$ ist eine abelsche Gruppe
  $(K^*, \cdot)$ ist eine abelsche Gruppe
  (mit $K^* := K \backslash \{0\}$)
  (Distr): (· Distr) $\Leftrightarrow$ (Distr ·)
  wegen Kommutativität der Multiplikation

Beispiel:
Ring der ganzen Zahlen $\mathbb{Z}$, genauer $(\mathbb{Z}, +, \cdot)$
Integritätsbereich

Satz 1.1 . *Jeder endliche Integritätsbereich ist ein Körper*

Beispiel:

Satz 1.2 . *Der Restklassenring* $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$ *der ganzen Zahlen modulo einer Primzahl* p *ist ein Körper, der aus* p *Elementen besteht: den Restklassen modulo* p*, repräsentiert durch die Reste*

$\{0, 1, 2, ..., p - 1\}$

Anmerkung 1.3 *In jedem Körper verfügen wir über die vier Grundrechenarten* **Addition**, **Subtraktion**, **Multiplikation**, **Division** *mit den elementaren Rechenregeln, die wir von den Körpern* $\mathbb{Q}$ *der rationalen Zahlen,* $\mathbb{R}$ *der reellen Zahlen und* $\mathbb{C}$ *der komplexen Zahlen kennen, und damit auch für die unendlich vielen* **Primkörper** $\mathbb{F}_p$, p *Primzahl:*

Körper:

(Ass $+$), (Neut $+$), (Inv $+$), (Komm $+$)

$\Leftrightarrow (K, +)$ ist abelsche Gruppe

(Ass $\cdot$), (Neut $\cdot$), (Inv $\cdot$)*, (Komm $\cdot$)

$\Leftrightarrow (K^*, \cdot)$ ist abelsche Gruppe

(Distr), verbindet Addition und Multiplikation

Anmerkung 1.4 *Integritätsbereiche sind Gegenstand der Teilbarkeitslehre. In jedem Integritätsbereich verfügen wir über die drei Grundrechenarten* **Addition**, **Subtraktion**, **Multiplikation**, *mit den elementaren Rechenregeln, die wir von den Ringen* $\mathbb{Z}$ *der ganzen (rationalen) Zahlen und* $K[X]$ *der Polynome über einem Körper* K *kennen:*

(Ass $+$), (Neut $+$), (Inv $+$), (Komm $+$),
(Ass $\cdot$), (Neut $\cdot$), (Kürz $\cdot$), (Komm $\cdot$),
(Distr)

Anmerkung 1.5 *In jedem Ring mit Einselement verfügen wir über die drei Grundrechenarten* **Addition**, **Subtraktion**, **Multiplikation**, *mit den elementaren Rechenregeln, die wir von den Ringen* $Mat_n(K)$ *der* n*-reihigen quadratischen Matrizen mit Koeff izienten in einem Körper* K *kennen:*

(Ass $+$), (Neut $+$), (Inv $+$), (Komm $+$),
(Ass $\cdot$), (Neut $\cdot$),
($\cdot$ Distr), (Distr $\cdot$)

Homomorphismen

multiplikativ:

$h: A \longrightarrow B$, A, B mit Multiplikation

$$h(a \cdot b) = h(a) \cdot h(b)$$

Bild des Produktes $=$ Produkt der Bilder

additiv:

$h: A \longrightarrow B$, A, B mit Addition

$$h(a + b) = h(a) + h(b)$$

Bild der Summe $=$ Summe der Bilder

z.B. Gruppen-Homomorphismen.

Ringhomomorphismen:
sowohl additiv als auch multiplikativ.
Für Ringe mit Einselement, speziell für Integritätsbereiche, wird zusätzlich

$$h(1_A) = 1_B$$

gefordert.

Bild der Eins $=$ Eins des Bildringes

Beispiel 1.6 . Restklassen-Homomorphismus*:*

$\mathbb{Z} \longrightarrow \mathbb{F}_p, \; g \mapsto \bar{g} := g \,mod\, p$ *Restklasse modulo* p

ist ein Homomorphismus von Integritätsbereichen.

allgemeiner, $n \in \mathbb{N}$ (natürliche Zahl):

Beispiel 1.7 .

$$\mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}, \; g \mapsto \bar{g} := g \bmod n$$

(Restklasse modulo n)

ist ein surjektiver Homomorphismus von kommutativen Ringen mit Einselement.

Resultierende Rechenregeln:

$$(a+b) \, mod \, n = (a \, mod \, n) + (b \, mod \, n)$$
$$(a \cdot b) \, mod \, n = (a \, mod \, n) \cdot (b \, mod \, n)$$

auch

$$\overline{a+b} = \bar{a} + \bar{b}$$
$$\overline{a \cdot b} = \bar{a} \cdot \bar{b}$$

Def inition 1.8 *.* $\mathbb{Z}/n\mathbb{Z}$ *heißt* **Ring der Restklassen modulo** n*.*

Er besteht aus n Elementen, repräsentiert durch die kleinsten natürlichen Reste modulo n

$$\{0, 1, 2, ..., n-2, n-1\}$$

Cäsar-Verschlüsselung:

Eineindeutige Zuordnung, z.B. $n = 27$

$$\begin{aligned} \mathbb{Z}/27\mathbb{Z} &\Leftrightarrow \{\text{Reste modulo } 27\} \\ &\Leftrightarrow \{\text{Leerzeichen und Buchstaben}\} \end{aligned}$$

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & .... & 21 & 22 & 23 & 24 & 25 & 26 \\ & A & B & C & D & E & F & G & H & I & J & K & L & M & N & O & .... & U & V & W & X & Y & Z \end{pmatrix}$$

Schlüssel k:

Verschlüsselung:

Verschiebung der Buchstaben um k Stellen nach rechts, modulo n

Übersetzung in Zahlen:

$$\bar{x} \mapsto \bar{x} + \bar{k} = \overline{x + k} =: \bar{y}$$

Entschlüsselung:
Rück-Verschiebung der Buchstaben um k Stellen nach links, modulo n
Übersetzung in Zahlen:

$$\bar{y} \mapsto \bar{y} - \bar{k} = \overline{y - k}$$

gewinnt x zurück:

$$\bar{x} \mapsto \bar{x} + \bar{k} = \bar{y} \mapsto \bar{y} - \bar{k} = (\bar{x} + \bar{k}) - \bar{k} = \bar{x}$$

Wortverschlüsselung:
KLARTEXT $\mapsto$ Ziffernfolge (Reste)
$\mapsto$ Restklassenfolge $\mapsto$ verschobene Restklassenfolge
$\mapsto$ Restfolge $\mapsto$ GEHEIMTEXT

Entschlüsselung:
GEHEIMTEXT $\mapsto$ Ziffernfolge (Reste)
$\mapsto$ Restklassenfolge $\mapsto$ rückverschobene Restklassenfolge
$\mapsto$ Restfolge $\mapsto$ KLARTEXT
MAPLE-Beispiel

Multiplikative Cäsar-Verschlüsselung
Entschlüsselung mit multiplikativem Inversem k'
von k modulo p,
Finde Gegen-Schlüssel $1 < k' < p - 1$ mit

$$k \cdot k' \equiv 1 \, mod \, p$$

Multiplikative Rück-Verschiebung der
Buchstaben mit Faktor k' modulo p

Übersetzung in Zahlen:

$$\bar{y} \mapsto \bar{k}' \cdot \bar{y} = \overline{k' \cdot y}$$

gewinnt x zurück:

$$\bar{x} \mapsto \overline{k \cdot x} = \bar{y} \mapsto \overline{k' \cdot y} = \overline{k' \cdot k \cdot x} = \bar{x}$$

MAPLE-Beispiel

1.2 Öffentliche Verschlüsselung

Def inition 1.9 . *Zwei ganze Zahlen* a, b *heißen* **kongruent modulo n** *genau dann, wenn sie bei der Division durch* n *denselben Rest haben.*

Schreibweise: $a \equiv b\, mod\, n \Leftrightarrow n \mid b - a$

Satz 1.10 (Chinesischer Restsatz). *Seien m, n zueinander teilerfremde natürliche Zahlen und a, b beliebige ganze Zahlen. Dann hat das Kongruenzsystem*

$$x \equiv a \bmod m$$
$$x \equiv b \bmod n$$

stets eine Lösung. Ist x_0 eine, so erhält man mit

$$\bar{x}_0 = x_0 + \mathbb{Z} \cdot mn$$

alle Lösungen. (Restklasse modulo mn)

Hintergrund: Produkt zweier Ringe R, S:

$$R \times S \ := \{(r, s);\ r \in R,\ s \in S\}$$

Addition und Multiplikation komponentenweise:

$$(r, s) + (r', s') \ := (r + r', s + s')$$

$$(r, s) \cdot (r', s') \ := (r \cdot r', s \cdot s')$$

Satz 1.11 *Falls m, n teilerfremd sind, gilt*

$$\mathbb{Z}/mn\mathbb{Z} \cong (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/n\mathbb{Z})$$

(Isomorphie von kommutativen Ringen mit Einselement)

via

$$g \bmod mn \mapsto \ (g \bmod m \ , \ g \bmod n)$$

Beispiel 1.12 . *Seien p, q zwei verschiedene Primzahlen; dann gilt*

$$\mathbb{Z}/pq\mathbb{Z} \cong \mathbb{F}_p \times \mathbb{F}_q$$

Einheiten eines kommutativen Ringes R mit Einselement

Def inition 1.13 . *Ein Element $r \in R$ heißt* **Einheit** *von R genau dann, wenn ein Element $r' \in R$ existiert mit $r \cdot r' = 1$.*
Falls r Einheit ist, so ist r' eindeutig durch r bestimmt und wird mit r^{-1} bezeichnet. Dieses Element wird **Inverses** *von r genannt.*
Die Einheiten von R bilden eine Gruppe, die mit R^* bezeichnet wird.

Satz 1.14 *Für das Produkt* $R \times S$ *zweier kommutativer Ringe mit Einselement gilt*

$$(R \times S)^* \cong R^* \times S^*$$

(Isomorphie abelscher Gruppen)

Korollar 1.15

$$(\mathbb{Z}/mn\mathbb{Z})^* \cong (\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$$

speziell

$$(\mathbb{Z}/pq\mathbb{Z})^* \cong \mathbb{F}_p^* \times \mathbb{F}_q^*$$

(Isomorphie abelscher Gruppen; p,q verschiedene Primzahlen)

Anzahl der Elemente der Einheitsgruppen

Euler-Funktion

$$\varphi(n) \ := \# \left(\mathbb{Z}/n\mathbb{Z}\right)^*$$

Satz 1.16 . *Falls m, n teilerfremd sind, so gilt*

$$\varphi(mn) = \varphi(m) \cdot \varphi(n).$$

Ferner

$$\varphi(p^k) = (p-1)p^{k-1} \ , \ p \text{ Primzahl}$$

Korollar 1.17 . *Sei* $n = p_1^{k_1} p_2^{k_2} ... p_r^{k_r}$ *die Primzerlegung von* n*. Dann gilt*

$$\varphi(n) = (p_1 - 1)(p_2 - 1)...(p_r - 1) p_1^{k_1 - 1} p_2^{k_2 - 1} ... p_r^{k_r - 1},$$

speziell

$$\varphi(pq) = (p-1)(q-1),$$

p,q *verschiedene Primzahlen*

Potenz-Verschlüsselung:

Wahl einer Primzahl $p > 27$, $\#\mathbb{F}_p^* = p - 1$

z.B. $p = 29$, $\#\mathbb{F}_{29}^* = 29 - 1 = 28 =$ Anzahl der Gruppenelemente

Eineindeutige Zuordnung

$$\mathbb{F}_{29}^* \Leftrightarrow \{\text{zu 29 prime Reste modulo } 29\}$$
$$\Leftrightarrow \{\text{Leerzeichen und Buchstaben}\}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & .... & 21 & 22 & 23 & 24 & 25 & 26 & 27 & 28 \\ A & B & C & D & E & F & G & H & I & J & K & L & M & N & .... & U & V & W & X & Y & Z & \_ & \circ \end{pmatrix}$$

Schlüssel k, $1 < k < p - 1$:
Verschlüsselung:
Potentielle Verschiebung der Buchstaben modulo p
Übersetzung in Zahlen:

$$\bar{x} \mapsto \bar{x}^k = \overline{x^k} =: \; y$$

MAPLE-Beispiel

zur Entschlüsselung:

Satz 1.18 *Ist G eine endliche abelsche Gruppe und $n = \#G$ die Gruppenordnung, so gilt*

$$a^n = 1 \text{ für alle Gruppenelemente } a \in G.$$

Korollar 1.19 *(Kleiner Fermatscher Satz). Für jede Primzahl p gilt*

$$a^{p-1} \equiv 1 \, mod \, p$$

für alle zu p teilerfremden ganzen Zahlen a.

Öffentliche Verschlüsselung
(Publik Key Cryptography)
RSA-Verfahren (Revest, Shamir, Adleman)

Transaktionszahl (TAN), längere Zeit f ixiert:

Produkt zweier (großer) Primzahlen $n = p \cdot q$

n öffentlich bekannt; p, q geheim

Persönliche Identif ikationszahl (PIN):

öffentlich bekannt:
Alice: Rest $a \; modulo \; n$, teilerfremd zu n
Bob: Rest $b \; modulo \; n$, teilerfremd zu n

PIN's, geheim, nur dem PC des Nutzers bekannt:
Alice: inverser Rest a' zu $a \; modulo \; n$
Bob: inverser Rest b' zu $b \; modulo \; n$

f ixierte Zuordnung:
Buchstaben/Zeichen $\mapsto$ Reste $mod\, n$, injektiv

Verschlüsselung:

Alice's PC verschlüsselt Nachrichts-Ziffer
N zu $Y \equiv N^{a'b}\, mod\, n$
und versendet Y zu Bob

Bob's PC entschlüsselt mittels ab'-Potenz:
$Y^{ab'} \equiv (N^{a'b})^{ab'} \equiv N^{(aa')(bb')} \equiv N^{1 \cdot 1} = N\, mod\, n$

2 Die Riemannsche Kugel über beliebigen Körpern

2.1 Geometrische Grundbegriffe

Def inition (Wiederholung). Euklidischer Ring: Integritätsbereich R mit euklidischer Wertung

$$w: \; R^{\bullet} \; := R \setminus \{o\} \longrightarrow \mathbb{N}$$

Zu jedem Paar $0 \neq g,\ f \in R$ existieren $q,\ r \in R$, so daß

$$f = q \cdot g + r \text{ mit: } w(r) < w(g) \text{ oder } r = 0.$$

(Division mit Rest)

Beispiel 2.1 *Die Gradwertung*

$$f(X) = a_n X^n + \dots. + a_1 X + a_0 \mapsto n = deg\ f$$

des Polynomringes $K[X]$ ist euklidisch ($a_n \neq 0$, K ein Körper).

Die Gradwertung ist auch **additiv**, d.h. es gilt:

$$deg(f(X) \cdot h(X)) = deg\, f + deg\, h, \quad f, h \in K[X]^{\bullet}$$

Haupt-Satz 2.2 *Im Polynomring K[X] gilt der Existenz- und Eindeutigkeits-Satz für Primzerlegungen. Speziell ist jedes normierte Polynom eindeutig (bis auf Reihenfolge der Faktoren) in ein Produkt normierter Primpolynome zerlegbar.*

(gilt allgemeiner für alle euklidischen Ringe)

$K \Leftrightarrow$ aff ine K-Gerade $\mathbb{A}(K)$ (Punktmenge)
$\mathfrak{F}(K) :=$ Vektorraum der Funktionen
$f : \mathbb{A}(K) \to K$
polynomiale Funktionen:
$f(X) \mapsto f(x) \in \mathfrak{F}(K)$ (Einsetz-Funktion)
Der **Einsetz-Homomorphismus** ($X \mapsto x$)

$$K[X] \twoheadrightarrow K[x]$$

ist ein surjektiver Homomorphismus von kommutativen Ringen mit Einselement.

Lemma 2.3 *Ist* $\mathbb{F}$ *ein endlicher Körper, so ist der Raum* $\mathbb{F}[x]$ *der polynomialen Funktionen auf* $\mathbb{A}(\mathbb{F})$ *ein endlich-dimensionaler* $\mathbb{F}$*-Vektorraum, und damit endlich als Menge.*

Satz 2.4 *Es gibt unendlich viele Primpolynome in* $\mathbb{F}[X]$*. Insbesondere ist* $\mathbb{F}[X]$ *nicht endlich-dimensional über* $\mathbb{F}$*.*

Def inition 2.5 *Projektive K-Gerade:*

$$\mathbb{P}(K) := \mathbb{A}(K) \cup \{\infty\}$$

Beispiele 2.6 *Reelle und komplexe projektive Geraden:*

$\mathbb{P}(\mathbb{R}) \Leftrightarrow$ *Kreis-Peripherie*

$\mathbb{P}(\mathbb{C}) \Leftrightarrow$ *Kugel-Oberf läche*

Riemannsche Zahlenkugel

Def inition 2.7 *Der Quotientenkörper $K(X)$ des Polynomringes $K[X]$ heißt* **Körper der rationalen Funktionen** *über K.*

Jede Rationale Funktion $r(X) = \frac{f(X)}{g(X)}$, $0 \neq g(X), f(X) \in K[X]$, teilerfremd, liefert eine Funktion $r(X)$ auf der aff inen Geraden $\mathbb{A}(\bar{K})$ mit Werten in $\bar{K} \cup \{\infty\}$:
Man setze $r(a) = \infty$, falls $a \in \bar{K}$ Nullstelle des Nenners $g(X)$ ist. Solche Punkte heißen **Pole** von $r(X)$;

$r(X)$ hat nur endlich viele Null- und Polstellen auf der aff inen Geraden $\mathbb{A}(\bar{K})$.

2.2 Bewertungen, Stellen und Funktionswerte

Ziel: Ausdehnung des Wertebereiches rationaler Funktionen von der aff inen Geraden auf die projektive Gerade $\mathbb{P}(\bar{\mathbb{F}})$

Def inition 2.8 . *Eine* **diskrete Bewertung** *eines Körpers* L *ist eine Abbildung* $v:\ L \twoheadrightarrow \mathbb{Z} \cup \{\infty\}$, *die für alle* $a, b \in L$ *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* $v(a) \neq v(b)$;
- $v(e) = 0$, e *Einh.W.;* $v(a-b) \geq \min\{v(a), v(b)\}$

Beispiel 2.9 Prim-Bewertungen. *$p(X)$ sei Primpolynom in $K[X]$.*

$$r(X) = p(X)^k \frac{f_1(X)}{g_1(X)}, \; f_1, g_1 \text{ teilerfremd zu } p$$

$$v_p(r(X)) := k$$

$$\mathbb{A}(K) \subset \{\text{Primbewertungen von} K[X]\} :$$

$$K \ni c \mapsto v_{(X-c)}$$

Bewertung in ∞ via $X' := \frac{1}{X}$, $K(X) = K(X')$

$$v_\infty =_{Def} v'_0 = v_{X'} : K(X') \longrightarrow \mathbb{Z} \cup \{\infty\}$$

$\mathbb{P}(K) \subset$ {Primbewertungen von $K[X]$} $\cup \{v_\infty\}$

Satz 2.10 *Die Primbewertungen v_p, $p = p(X)$ Primpolynom, und v_∞ sind diskrete Bewertungen des rationalen Funktionenkörpers $K(X)$. Die* **"endlichen Bewertungen"** v_p *korrespondieren eineindeutig mit den normierten Primpolynomen von $K[X]$.*

Bezeichnungen.
endliche Bewertungen: $\mathbb{A}_{K(X)}$;
alle Bewertungen: $\mathbb{P}_{K(X)}$

Beispiel.

- Gaußsche Zahlenebene:
  $\mathbb{R} \subset \mathbb{C} \Leftrightarrow \mathbb{A}(\mathbb{C}) \Leftrightarrow \mathbb{A}_{\mathbb{C}(X)} \twoheadrightarrow \mathbb{A}_{\mathbb{R}(X)}$
- Riemannsche Zahlenkugel:
  $\mathbb{R} \cup \{\infty\} \subset \mathbb{C} \cup \{\infty\} \Leftrightarrow \mathbb{P}(\mathbb{C}) \Leftrightarrow \mathbb{P}_{\mathbb{C}(X)} \twoheadrightarrow \mathbb{P}_{\mathbb{R}(X)}$

Bemerkung 2.11 *Die unendliche Bewertung von $K(X)$ ist die Fortsetzung der negativen Gradwertung von $K[X]^\bullet$ auf den rationalen Funktionenkörper $K(X)$:*

$$-\deg f(X) = v_\infty(f),\ 0 \neq f = f(X) \in K[X]$$

Def inition 2.12 *Die Elemente von $\mathbb{P}_{K(X)}$ heißen* **"Stellen"** *von $K(X)$. Synonym dazu werden die Primideale von $K[X]$ als endliche Stellen und ∞ als unendliche Stelle bezeichnet.*

Def inition 2.13 *Sei v_P die Bewertung der Stelle P ($= p(X)$ oder ∞). Der Integritätsbereich*

$$\mathcal{O}_P := \{\varphi \in K(X);\ v_P(\varphi) \geq 0\}$$

heißt **"Stellenring"** *von K(X) in P.*

Einheitengruppe: $\mathcal{O}_P^* = \{\varphi \in K(X);\ v_P(\varphi) = 0\}$

einziges nichttriviales Primideal (Maximalideal):
$\mathfrak{m}_P := \{\varphi \in K(X);\ v_P(\varphi) > 0\}$

Theorem 2.14 *Der Stellenring* $\mathcal{O} = \mathcal{O}_P$ *der diskreten Bewertung* $v = v_P$ *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* $v(t) = 1$.

Def inition 2.15 *Der Körper* $\mathfrak{k} = \mathcal{O}/\mathfrak{m}$ *heißt Restklassenkörper von* $\mathcal{O}$.

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

Def inition 2.16 *Liegt* $r(X)$ *in* $\mathcal{O}_P$*, so wird das Bild von* $r(X)$ *in* $\mathfrak{k}_P = \mathcal{O}_P/\mathfrak{m}_P$ *beim Restklassen-Homomorphismus* $\mathcal{O}_P \twoheadrightarrow \mathfrak{k}_P$ *mit* $r(P)$ *bezeichnet und* **"Funktionswert"** *von* r *an der Stelle* P *genannt. In diesem Falle heißt* $r(X)$ **"regulär"** *an der Stelle* P*. Andernfalls wird* P **"Polstelle"** *von* $r(X)$ *genannt und* $r(P) = \infty$ *gesetzt.*

Merke: P ist Nullstelle von $r(X)$ gdw. $r(X) \in \mathfrak{m}_P$.

Satz 2.17 *Der Restklassenkörper* $\mathfrak{k} = \mathfrak{k}_P$ *ist eine endliche Körpererweiterung (d.h. endlichen Grades) des Grundkörpers* K *und damit eine algebraische Erweiterung.*

$$K \subseteq \mathfrak{k}_P \subseteq \bar{K} \text{ für alle Stellen } P.$$

Damit liegen alle Funktionswerte in $\bar{K} \cup \{\infty\}$.

WICHTIG: Ist $K = \mathbb{F}$ ein endlicher Körper, so liegen die Funktionswerte im endlichen Körper $\mathfrak{k}_P \supseteq \mathbb{F}$, sind also PC-berechenbar.

Def inition 2.18 *Die Primelemente* t *von* $\mathcal{O} = \mathcal{O}_P$ *werden* **"lokale Parameter"** *von* $K(X)$ *in* P *genannt.*

PRIMZERLEGUNG in $\mathcal{O}_P$: $0 \neq \varphi = \varepsilon \cdot t^k$,
$\varepsilon \in \mathcal{O}^*$ Einheit, $k = v_P(\varphi)$

lokale Parameter: $t' = \varepsilon \cdot t$.

Ziel:

Satz 2.19 *Jedes Element von* $\mathcal{O}$ *läßt sich eindeutig in eine Potenzreihe von* t *mit Koeff. im Restklassenkörper* $\mathfrak{k} = \mathcal{O}/\mathfrak{m}$ *entwickeln.*

Lemma 2.20 *(i)* $P \sim p(X)$ *ist eine* "Nullstelle" *von* $\varphi = \frac{f(X)}{g(X)}$ *gdw.* $\varphi(P) = 0$

$$\iff \varphi \in \mathfrak{m}_P \iff v_P(\varphi) > 0 \iff p(X) \mid f(X)$$

(ii) P *ist ein* "Pol" *von* φ *gdw.* P *eine Nullstelle von* $\frac{1}{\varphi} = \frac{g(X)}{f(X)}$ *ist.*

$$\iff \frac{1}{\varphi} \in \mathfrak{m}_P \iff v_P(\varphi) < 0 \iff p(X) \mid g(X)$$

($P = \infty \sim X' = 1/X \in K(X') = K(X)$*)*

Def initionen 2.21 *(i)* $v_P(\varphi)$ *heißt* **"Nullstellenordnung"** *von* φ *in* P*;* $v_P(1/\varphi)$ *heißt* **"Polordnung"** *von* φ *in* P*.*

(ii) Der Erweiterungsgrad $[\mathfrak{k}_P : K] =: \deg P$ *heißt* **"Grad der Stelle"** P*.*

Die Punkte der projektiven Geraden identif izieren wir mit den Stellen vom Grad 1:

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

2.3 Potenzreihen

Integritätsbereich $\mathfrak{k}[[t]]$ der formalen Potenzreihen über dem Körper $\mathfrak{k}$ (t Unbestimmte, transzendent über $\mathfrak{k}$):

$$\mathfrak{k}[[t]] := \{c_0+c_1t+c_2t^2+\ldots+c_nt^n+\ldots;\ c_i \in \mathfrak{k}\} \supset \mathfrak{k}[t]$$

Addition:

$$\sum_{i=0}^{\infty} a_i t^i + \sum_{i=0}^{\infty} b_i t^i := \sum_{i=0}^{\infty} (a_i + b_i) t^i$$

Multiplikation:

$$(\sum_{i=0}^{\infty} a_i t^i) \cdot (\sum_{j=0}^{\infty} b_j t^j) := \sum_{k=0}^{\infty} \left(\sum_{i+j=k} a_i b_j \right) t^k$$

diskrete Bewertung $v : \mathfrak{k}[[t]] \longrightarrow \mathbb{N}$

$$a_m t^m + a_{m+1} t^{m+1} + \ldots \quad \mapsto \quad m \quad (a_m \neq 0)$$

Theorem 2.22 *Der Potenzreihen-Ring $\mathfrak{k}[[t]]$ ist ein diskreter Bewertungsring und hat daher die folgenden Eigenschaften:*

(i) $\mathfrak{k}[[t]]$ *ist ein Hauptidealring;*

(ii) $\mathfrak{k}[[t]]$ *ist Ring mit eindeutiger Primzerlegung;*

(iii) $\pi \in \mathfrak{k}[[t]]$ *ist Primelement genau dann, wenn* $v(\pi) = 1$*, z.B.* $\pi = t$*;*

(iv) *Einheitengruppe:* $\mathfrak{k}[[t]]^* = v^{-1}(0)$*;*

(v) *einziges Primideal (maximal):* $\mathfrak{m} = (\pi) = (t) = t \cdot \mathfrak{k}[[t]] = v^{-1}(\mathbb{N}_+)$*;*

außerdem:

(vi) π Primelement $\iff \pi = \varepsilon \cdot t,\ \varepsilon$ Einheit;

(vii) Restklassenkörper: $\mathfrak{k}[[t]]/\mathfrak{m} \cong \mathfrak{k}$.

$$\begin{array}{rcl} \varphi = a_0 + a_1 t + \cdots + a_n t^n + \dots & \mapsto & a_0 \\ t & \mapsto & 0 \end{array}$$

Kern-Bild-Folge:

$$\mathfrak{m} \hookrightarrow \mathfrak{k}[[t]] \twoheadrightarrow \mathfrak{k}$$

Abschnitte $\varphi_n := a_0 + a_1 t + \cdots + a_n t^n$ der Potenzreihe φ sind:

- Polynome in $\mathfrak{k}[t]$,
- polynomiale Funktionen φ_n auf $\mathfrak{k}$,
- Reste von φ modulo t^{n+1}

Jede Potenzreihe def iniert eine unendliche polynomiale **"Abschnittsfolge"**

$$\varphi_0, \varphi_1, \varphi_2, \dots, \varphi_n, \dots,$$

Umgekehrt def iniert jede unendliche **"Abschnittsfolge"** von Polynomen

$$f_0 = a_0, f_1 = a_0 + a_1 t, f_2 = a_0 + a_1 t + a_2 t^2,$$

$$\ldots$$

$$f_n = a_0 + a_1 t + a_2 t^2 + \cdots + a_n t^n \in \mathfrak{k}[t]$$

$$\ldots$$

eine eindeutig bestimmte Potenzreihe

$$\varphi = \lim f_n \ := a_0 + a_1 t + \cdots + a_n t^n + \cdots \in \mathfrak{k}[[t]]$$

$f(X) \in K(X)$, sei regulär an der Stelle $P \in \mathbb{P}_{K(X)}$.
Rekursive Konstruktion einer zugehörigen unendlichen Abschnittsfolge $(f_n)_{n=0}^{\infty}$ von Polynomen aus $\mathfrak{k}[t]$, wobei

$$\mathfrak{k} = \mathfrak{k}_P = \mathcal{O}_{\mathcal{P}}/\mathfrak{m}_{\mathcal{P}} \supseteq \ K \text{ (algebraische Erweiterung)},$$

bzgl. eines fest gewählten lokalen Parameters

$t \in \mathcal{O} = \mathcal{O}_{\mathcal{P}}$ (ist stets transzendent über K und $\mathfrak{k}$):

$$\begin{aligned} f_0 = a_0 &\equiv f \mod t,\; a_0 = f(P) \in \mathfrak{k} \\ f_1 = a_0 + a_1 t &\equiv f \mod t^2,\; a_1 := \frac{f - a_0}{t}(P) \\ f_2 = a_0 + a_1 t + a_2 t^2 &\equiv f \mod t^3,\; a_2 := \frac{f - f_1}{t^2}(P) \end{aligned}$$

u.s.w.

Beweis von Satz 2.19.

$$f \mapsto \varphi = \varphi(t) = \lim f_n = a_0 + a_1 t + \cdots + a_n t^n + \cdots \in \mathfrak{k}[[t]].$$

$\square$

Satz 2.23 *Die Potenzreihen-Entwicklungen def. einen injektiven Ring-Homomorphismus.*

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

Def inition 2.24 *Sei* $\mathfrak{k}$ *ein Körper,* t "transzendent" *über* $\mathfrak{k}$*. Die unendlichen Reihen*

$$a_{-m}t^{-m}+a_{-m+1}t^{-m+1}+\ldots.+a_{-1}t^{-1}+a_0+\ldots.+a_Nt^N+\ldots.$$

heißen **"formale Laurent-Reihen"** *mit Koeff izienten* a_j *in* $\mathfrak{k}$*.*

Satz 2.25 *Die formalen Laurent-Reihen über* $\mathfrak{k}$ *bilden einen Erweiterungskörper* $\mathfrak{k}((t))$ *von* $\mathfrak{k}$*, der auch den rationalen Funktionenkörper* $\mathfrak{k}(t)$ *(isomorph) enthält.* $\mathfrak{k}((t))$ *ist der Quotientenkörper des Integritätsbereiches* $\mathfrak{k}[[t]]$ *der formalen Potenzreihen über* $\mathfrak{k}$*.*

Satz 2.26 *Sei P eine Stelle des rationalen Funktionenkörpers $K(X)$, $\mathfrak{k}_P$ der zugehörige Restklassenkörper und t ein lokaler Parameter in P. Jede Funktion $\varphi(X) \in K(X)$ läßt sich eindeutig in eine Laurentreihe mit Koeff izienten in $\mathfrak{k}_P$ entwickeln:*

$$\varphi = a_{-m}t^{-m} + \ldots . + a_0 + a_1 t + \ldots . + a_N t^N + \ldots . \in \mathfrak{k}_P((t)),$$

$a_{-m} \neq 0$ falls $\varphi \neq 0$,

$-m = v_P(\varphi)$ Nullstellenordnung von φ,

m Polordnung von φ.

Korollar 2.27 *Die Laurent-Reihen-Entwicklungen def inieren eine Körpereinbettung*

$$Ser_t : \; K(X) \hookrightarrow \mathfrak{k}_P((t)).$$

("Ser" von series, engl. für "Reihe")

2.4 Divisoren und Funktionsräume

Def inition 2.28 *Die freie abelsche Gruppe erzeugt durch alle Stellen P von $\mathbb{P} = \mathbb{P}_{K(X)}$ heißt* "Divisorengruppe" *des Funktionenkörpers $K(X)$.*

$$Div\,\mathbb{P} \;:= \sum_{P\in\mathbb{P}} \mathbb{Z}\cdot P$$

Elemente: $D = m_1P_1 + m_2P_2 \cdots + m_rP_r$, $P_i \in \mathbb{P}$, Addition koeff izientenweise:

$$\sum_P m_P \cdot P + \sum_P n_P \cdot P \ := \sum_P (m_P + n_P) \cdot P$$

$$(m_1 P_1 + \cdots + m_r P_r) + (n_1 P_1 + \cdots + n_r P_r)$$
$$= (m_1 + n_1) P_1 + \cdots + (m_r + n_r) P_r$$

Halbordnung:

$$D = m_1 P_1 + \ldots m_r P_r \geq 0 \Longleftrightarrow m_1, \ldots, m_r \geq 0$$
$$D \geq D' \Longleftrightarrow D - D' \geq 0$$

Divisoren von Funktionen $0 \neq \varphi \in K(X)$ (*"Hauptdivisoren"*):

$$(\varphi) := \sum_P v_P(\varphi) \cdot P \qquad \text{(endliche Summe)}$$

Def inition 2.29 *Die Hauptdivisoren bilden eine Untergruppe $Princ\,\mathbb{P}$ der Divisorengruppe $Div\,\mathbb{P}$. Sie wird* "Gruppe der Hauptdivisoren" *auf $\mathbb{P}$ genannt.*

Funktionsräume mit vorgeschriebener Beschränkung von Polstellen und Polordnungen

$$\mathcal{L}(D) \ := \{\varphi \in K(X);\ (\varphi) \geq -D\} \cup \{0\}$$

für jeden Divisor $D \in Div\, \mathbb{P}$ (Polbeschränkungs-Divisor).

$\mathcal{L}(D) \subset K(X)$ ist ein K-Vektorraum.

Ziel: $\mathcal{L}(D)$ ist endlich-dimensional, genaue Bestimmung der Dimension.

Beispiele 2.30

(i) $\mathcal{L}(O) = K$;

(ii) $\mathcal{L}(D) = O$, *falls* $D < O$;

(iii) $\mathcal{L}(n \cdot \infty) = K[X]_{deg \leq n}$; $n \geq 0$;

(iv) $\dim \mathcal{L}(n \cdot P) = n + 1$, *falls* $P \in \mathbb{P}(K)$;

(v) $\dim \mathcal{L}(D) = \dim \mathcal{L}(D')$, *falls* $D - D' \in Princ\, \mathbb{P}$.

Def inition 2.31 *Zwei Divisoren* D, D' *heißen* "linear äquivalent" *genau dann, wenn* $D - D' \in Princ\, \mathbb{P}$; *Schreibweise:* $D \equiv D'$.