

Algebraische Kurven

Franz Halter-Koch

Contents

| | |
|---|----|
| Chapter 1. Ebene affine Kurven | 3 |
| 1.1. | 3 |
| 1.2. | 5 |
| 1.3. | 6 |
| 1.4. | 6 |
| 1.5. | 7 |
| 1.6. | 8 |
| 1.7. | 9 |
| Chapter 2. Ebene projektive Kurven | 13 |
| 2.1. | 13 |
| 2.2. | 13 |
| 2.3. | 14 |
| 2.4. | 16 |
| 2.5. | 18 |
| 2.6. | 19 |
| 2.7. | 21 |
| Chapter 3. Algebraische Funktionenkörper und diskrete Bewertungen | 23 |
| 3.1. | 23 |
| 3.2. | 24 |
| 3.3. | 24 |
| 3.4. | 25 |
| 3.5. | 26 |
| 3.6. | 27 |
| 3.7. | 30 |
| 3.8. | 32 |
| 3.9. | 33 |
| Chapter 4. Divisoren, Differenziale und der Satz von Riemann-Roch | 39 |
| 4.1. | 39 |
| 4.2. | 41 |
| 4.3. | 42 |
| 4.4. | 42 |
| 4.5. | 44 |
| 4.6. | 45 |
| 4.7. | 47 |
| Chapter 5. Algebraisch-geometrische Codes | 49 |
| 5.1. | 49 |
| 5.2. | 50 |

| | | |
|------------|---|----|
| Chapter 6. | Elliptische Funktionenkörper und elliptische Kurven | 53 |
| 6.1. | | 53 |
| 6.2. | | 54 |
| Chapter 7. | Endliche Erweiterungen algebraischer Funktionenkörper | 59 |
| 7.1. | | 59 |
| 7.2. | | 62 |
| 7.3. | | 62 |
| 7.4. | | 63 |
| 7.5. | | 64 |
| 7.6. | | 65 |
| Chapter 8. | Funktionenkörper über endlichem Konstantenkörper | 67 |
| 8.1. | | 67 |
| 8.2. | | 68 |
| 8.3. | | 70 |

Ebene affine Kurven

1.1

Ein *Ring* ist stets ein kommutativer Ring mit Eins, und ein *Ringhomomorphismus* soll stets die Eins auf die Eins abbilden. Ein nullteilerfreier Ring heißt *Bereich*. Ist R ein Bereich, so sei $R^\bullet = R \setminus \{0\}$, R^\times die *Einheitengruppe* und $\mathfrak{q}(R)$ ein Quotientenkörper von R . Wir schreiben häufig $\mathbf{0}$ an Stelle von $\{0\}$ oder auch an Stelle von $(0, \dots, 0)$ oder sogar $\{(0, \dots, 0)\}$, wenn klar ist, welche Null gemeint ist. Für einen Ring R bezeichnen wir Polynomringe mit $R[X]$, $R[X, Y]$, $R[X_1, \dots, X_n]$ usw. Ist $\mathbf{X} = (X_1, \dots, X_n)$, so ist $R[\mathbf{X}]^\times = R^\times$. Ist R ein Bereich und $K = \mathfrak{q}(R)$, so ist $K(\mathbf{X}) = \mathfrak{q}(R[\mathbf{X}])$ ein rationaler Funktionenkörper über K .

Ein Polynom $f \in R[\mathbf{X}]$ heißt *irreduzibel* (über R), wenn es keine Faktorisierung $f = gh$ mit $g, h \in R[\mathbf{X}] \setminus R$ besitzt. Wie in der elementaren Analysis üblich, bezeichnen wir mit

$$\frac{\partial^{i_1 + \dots + i_n} f}{\partial X_1^{i_1} \dots \partial X_n^{i_n}}$$

die höheren partiellen Ableitungen von f . Für $f \in R[X]$ bezeichne f' die gewöhnliche Ableitung von f . Ist $S \supset R$ ein Oberring, so induziert jedes $f \in R[X_1, \dots, X_n]$ eine Abbildung

$$f^S: S^n \rightarrow S, \quad \text{definiert durch} \quad f^S(x_1, \dots, x_n) = f(x_1, \dots, x_n).$$

Die Abbildung $f \mapsto f^S$ ist ein Ringhomomorphismus $R[X_1, \dots, X_n] \rightarrow \text{Abb}(S^n, S)$ (dabei ist $\text{Abb}(S^n, S)$ mit der wertweisen Verknüpfung versehen). Ist S ein unendlicher Bereich, so ist $f \mapsto f^S$ injektiv und wir brauchen nicht zwischen f und f^S zu unterscheiden. Ist $f \in R[X]$ und $\alpha \in S$ eine Nullstelle von f , so heißt α eine *mehrfache Nullstelle* von f , wenn $f'(\alpha) = 0$ [äquivalent: Es gibt ein $g \in S[X]$ mit $f = (X - \alpha)^2 g$].

Sei K ein Körper. Eine *K-Algebra* ist ein Ring A mit einer K -Vektorraumstruktur, so dass für alle $a, b \in A$ und $\lambda \in K$ das Assoziativgesetz $\lambda(ab) = (\lambda a)b = a(\lambda b)$ gilt. Ist A eine K -Algebra und X eine nicht-leere Menge, so ist $\text{Abb}(X, A)$ eine K -Algebra bezüglich der wertweisen Verknüpfung von Abbildungen. Ein *K-Algebrenhomomorphismus* ist ein Ringhomomorphismus, der auch ein Vektorraumhomomorphismus ist.

Ist L ein Körper und $K \subset L$ ein Teilkörper, so nennt man $K \subset L$ oder L/K eine *Körpererweiterung*, L einen *Oberkörper* von K und jeden Körper M mit $K \subset M \subset L$ einen *Zwischenkörper* von L/K . Ist $\varphi: K \rightarrow K_1$ ein (Körper-)Homomorphismus, so ist φ injektiv und induziert einen (Körper-)Isomorphismus $\varphi: K \xrightarrow{\sim} \varphi(K)$.

Ist L/K eine Körpererweiterung, so ist L eine K -Algebra, $[L:K] = \dim_K L \in \mathbb{N} \cup \{\infty\}$ heißt *Grad* der Körpererweiterung L/K , und L/K heißt *endlich*, wenn $[L:K] < \infty$. Für eine Teilmenge $S \subset L$ bezeichnen $K[S]$ den kleinsten Teilring von L , der $K \cup S$ umfasst, und es sei $K(S) = \mathfrak{q}(K[S])$.

Sind L/K und L'/K Körpererweiterungen, so ist ein *K-Homomorphismus* $\varphi: L \rightarrow L'$ ein *K-Algebrenhomomorphismus* [äquivalent: φ ist ein Körperhomomorphismus, und $\varphi|_K = \text{id}_K$].

Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *algebraisch über K* , wenn es ein $f \in K[X]$ gibt mit $f(\alpha) = 0$. Dann gibt es genau ein normiertes irreduzibles Polynom $g \in K[X]$ mit $g(\alpha) = 0$. Dieses heißt *Minimalpolynom* von α über K und induziert einen Isomorphismus

$$K[X]/_{\kappa[X]}(g) \xrightarrow{\sim} K(\alpha) = K[\alpha], \quad h + \kappa[X](g) \mapsto h(\alpha).$$

Ist α nicht algebraisch über K , so heißt α *transzendent über K* , und es bestehen Isomorphismen

$$K[X] \xrightarrow{\sim} K[\alpha], \quad f \mapsto f(\alpha), \quad \text{und} \quad K(X) \xrightarrow{\sim} K(\alpha).$$

Eine Körpererweiterung L/K heißt *algebraisch* wenn jedes $\alpha \in L$ über K algebraisch ist. Anderfalls heißt L/K *transzendent*. Ist L/K eine Körpererweiterung und $S \subset L$ eine Menge über K algebraischer Elemente, so ist $K(S)/K$ algebraisch. Ist \overline{K}_L die Menge aller über K algebraischen Elementen von L , so ist \overline{K}_L ein Zwischenkörper von L/K und heißt *relativer algebraischer Abschluss von K in L* . K heißt *relativ algebraisch abgeschlossen in L* , wenn $\overline{K}_L = K$.

Eine Körpererweiterung L/K heißt *endlich erzeugt*, wenn es ein $n \in \mathbb{N}$ und $\alpha_1, \dots, \alpha_n \in L$ gibt, so dass $L = K(\alpha_1, \dots, \alpha_n)$. Eine Körpererweiterung ist genau dann endlich, wenn sie endlich erzeugt und algebraisch ist.

Ein Körper K heißt *algebraisch abgeschlossen*, wenn jedes $f \in K[X] \setminus K$ in K eine Nullstelle besitzt [äquivalent dazu sind: **1)** Jedes $f \in K[X] \setminus K$ zerfällt über K in Linearfaktoren; **2)** Es gibt keine algebraische Körpererweiterung $K \subsetneq L$]. \mathbb{C} ist algebraisch abgeschlossen ("Fundamentalsatz der Algebra"). Ein Oberkörper $\overline{K} \supset K$ heißt *algebraischer Abschluss* oder *algebraische Hülle* von K , wenn \overline{K} algebraisch abgeschlossen und \overline{K}/K eine algebraische Körpererweiterung ist.

Satz 1.1.1 (Hauptsatz über algebraische Hüllen). *Sei K ein Körper.*

1. K besitzt eine algebraische Hülle.
2. Ist $L \subset K$ ein algebraisch abgeschlossener Oberkörper von K , so ist der relative algebraische Abschluss \overline{K}_L von K in L eine algebraische Hülle von K .
3. (Fortsetzungssatz für Homomorphismen) Sei $\varphi: K \rightarrow K_1$ ein Körperhomomorphismus, L/K eine algebraische Körpererweiterung und $K_1^* \supset K$ ein algebraisch abgeschlossener Oberkörper. Dann gibt es einen Homomorphismus $\phi: L \rightarrow K_1^*$ mit $\phi|_K = \varphi$.
4. Sind K_1 und K_2 algebraische Hüllen von K , so gibt es einen K -Isomorphismus $K_1 \xrightarrow{\sim} K_2$.

OHNE BEWEIS. □

Eine komplexe Zahl heißt *algebraisch*, wenn sie algebraisch über \mathbb{Q} ist. Der Körper $\overline{\mathbb{Q}}$ aller algebraischen Zahlen ist eine algebraische Hülle von \mathbb{Q} .

Ist F ein endlicher Körper, so ist $|F|$ eine Primzahlpotenz, und zu jeder Primzahlpotenz q gibt es bis auf Isomorphie genau einen Körper mit q Elementen, der mit \mathbb{F}_q bezeichnet wird. Ist $\overline{\mathbb{F}}_q$ eine algebraische Hülle von \mathbb{F}_q , so gibt es zu jedem $d \in \mathbb{N}$ genau einen Zwischenkörper E von $\overline{\mathbb{F}}_q/\mathbb{F}_q$ mit $[E:\mathbb{F}_q] = d$, und dieser ist isomorph zu \mathbb{F}_{q^d} .

Sei K ein Körper. Ein Polynom $f \in K[X]$ heißt *separabel*, wenn es in keinem Oberkörper von K mehrfache Nullstellen besitzt. Ein irreduzibles Polynom ist genau dann separabel, wenn $f' \neq 0$. K heißt *vollkommen*, wenn jedes irreduzible Polynom $f \in K[X]$ separabel ist. Genau dann ist K vollkommen, wenn entweder $\text{char}(K) = 0$ oder $\text{char}(K) = p > 0$ und $K = K^p$ ist. Jeder endliche und jeder algebraisch abgeschlossene Körper ist vollkommen.

Sei L/K eine Körpererweiterung. Ein Element $\alpha \in L$ heißt *separabel über K* , wenn α über K algebraisch und das Minimalpolynom separabel ist. Die Körpererweiterung L/K heißt *separabel*, wenn jedes $\alpha \in L$ über K separabel ist. Ist $L = K(S)$ mit einer Teilmenge $S \subset L$, so ist L/K genau dann separabel, wenn jedes $\alpha \in S$ über K separabel ist. Ist K vollkommen, so ist jede algebraische Körpererweiterung L/K separabel.

Satz 1.1.2 (Satz vom primitiven Element). *Sei L/K eine endliche separable Körpererweiterung. Dann ist $L = K(\alpha)$ mit $\alpha \in L$.*

Sei K ein Körper und \overline{K} eine algebraische Hülle von K . Ein Polynom $f \in K[\mathbf{X}]$ heißt *absolut irreduzibel*, wenn $f \in \overline{K}[\mathbf{X}]$ irreduzibel ist.

Für den Rest dieses Kapitels sei K ein Körper und \overline{K} eine algebraische Hülle von K .

1.2

Definition 1.2.1. Für ein Polynom $f \in K[X, Y]$ und $\mathbf{p} = (u, v) \in \overline{K}^2$ sei $f(\mathbf{p}) = f(u, v) \in \overline{K}^2$. Die Menge $V(f) = \{\mathbf{p} \in \overline{K}^2 \mid f(\mathbf{p}) = 0\}$ heißt *Nullstellengebilde* von f . Eine Teilmenge $C \subset \overline{K}^2$ heißt (*ebene affine*) *über K definierte (algebraische) Kurve*, wenn es ein $f \in K[X, Y] \setminus K$ gibt mit $C = V(f)$. Man schreibt dann auch $C: f = 0$ und spricht von der Kurve $f(x, y) = 0$.

Die Menge $C(K) = C \cap K^2$ heißt Menge der *K -rationalen Punkte* von $C = C(\overline{K})$. Ist $K \subset L \subset \overline{K}$, so ist jede über K definierte Kurve auch über L definiert.

Beispiele 1.2.2.

1. Eine Teilmenge $L \subset \overline{K}^2$ heißt *über K definierte Gerade*, wenn es $a, b, c \in K$ gibt mit $(a, b) \neq (0, 0)$ und $L = V(aX + bY + c)$. Dann ist $L(K) \subset K^2$ ein eindimensionaler affiner Teilraum im Sinne der Linearen Algebra.

2. Für $a \in K$ sei $f_a = X^2 + Y^2 - a \in K[X, Y]$ und $C_a = V(f_a) = \{(u, v) \in \overline{K}^2 \mid u^2 + v^2 = a\}$. Sei $\alpha \in \overline{K}$ mit $\alpha^2 = a$.

Ist $\text{char}(K) = 2$, so ist $f_a = (X + Y + \alpha)^2$ und $C_a = V(X + Y + \alpha)$ ist eine (doppelt zu zählende) Gerade. Ist $\alpha \notin K$, so ist $C_a(K) = \emptyset$.

Sei $\text{char}(K) \neq 2$ und $i \in \overline{K}$ mit $i^2 = -1$. Dann ist $f_0 = X^2 + Y^2 = (X + iY)(X - iY)$, und $C_0 = L_+ \cup L_-$ mit $L_{\pm} = V(X \pm iY) \subset \overline{K}^2$. Ist $i \notin K$, so ist f_0 irreduzibel über K und $C_0(K) = \{(0, 0)\}$.

Ist $\text{char}(K) \neq 2$ und $a \in K^2$, so ist f absolut irreduzibel (Ü!).

Sei nun $\text{char}(K) \neq 2$ und $a = 1$. Für $k \in \overline{K}$ sei $L_k = V(kX + Y - 1)$. Ist $k \neq \pm i$, so gilt für $(u, v) \in \overline{K}^2$:

$$(u, v) \in L_k \cap C_1 \iff (u, v) = \left(\frac{2k}{1+k^2}, \frac{1-k^2}{1+k^2} \right).$$

Damit erhalten wir eine bijektive Abbildung

$$\tau: \overline{K} \setminus \{\pm i\} \rightarrow C_1 \setminus \{(0, -1)\} \quad \text{vermöge} \quad \tau(k) = \left(\frac{2k}{1+k^2}, \frac{1-k^2}{1+k^2} \right).$$

Für $(u, v) \in C_1 \setminus \{(0, -1)\}$ ist

$$\tau^{-1}(u, v) = \frac{1-v}{u}, \quad \text{falls } u \neq 0, \quad \text{und } \tau^{-1}(0, 1) = 0.$$

Insbesondere ist auch $\tau|_{K \setminus \{\pm i\}} \rightarrow C_1(K) \setminus \{(0, -1)\}$ bijektiv. Im Falle $K = \mathbb{Q}$ erhalten wir eine bijektive Abbildung $\mathbb{Q} \rightarrow \{(x, y) \in \mathbb{Q}^2 \mid x^2 + y^2 = 1\}$ (rationale Punkte auf dem Einheitskreis).

Parametrisierung der pythagoräischen Tripel: Sei \mathcal{P} die Menge aller Tripel $(a, b, c) \in \mathbb{N}_0^3$ mit $a^2 + b^2 = c^2$, $(a, b) = 1$ und $2 \nmid b$. Ist $(a, b, c) \in \mathcal{P}$, so folgt

$$\left(\frac{a}{c}, \frac{b}{c} \right) \in C_1(\mathbb{Q}), \quad \text{also} \quad \frac{a}{c} = \frac{2k}{1+k^2}, \quad \frac{b}{c} = \frac{1-k^2}{1+k^2} \quad \text{mit eindeutig bestimmtem } k = \frac{n}{m} \in \mathbb{Q} \cap [0, 1],$$

wobei $m \in \mathbb{N}_0$, $n \in \mathbb{N}$, $(n, m) = 1$ und $n \leq m$. Es folgt $(m^2 - n^2, m^2 + n^2) \mid 2$, und

$$\frac{a}{c} = \frac{2mn}{m^2 + n^2}, \quad \frac{b}{c} = \frac{m^2 - n^2}{m^2 + n^2}.$$

Wäre $(m^2 - n^2, m^2 + n^2) = 2$, so folgte $m \equiv n \equiv 1 \pmod{2}$, $m^2 - n^2 \equiv 0 \pmod{8}$, $m^2 + n^2 \equiv 2 \pmod{4}$ und $2 \mid b$, ein Widerspruch. Also folgt $(m^2 - n^2, m^2 + n^2) = 1$ und daher $(a, b, c) = (2mn, m^2 - n^2, m^2 + n^2)$. Im Falle $K = \mathbb{R}$, $\overline{K} = \mathbb{C}$ und $a = -1$ ist $C_{-1} = \{(x, y) \in \mathbb{C}^2 \mid x^2 + y^2 = -1\} = iC_1$ und $C_{-1}(\mathbb{R}) = \emptyset$. Im Falle $K = \mathbb{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$ ist $\mathbb{F}_3^2 = \{\overline{0}, \overline{1}\}$, und $C_{-1}(\mathbb{F}_3) = \mathbb{F}_3^\times \times \mathbb{F}_3^\times$.

1.3

Satz 1.3.1. *Für jede Kurve $C \subset \overline{K}^2$ ist $|C| = |\overline{K}^2 \setminus C| = \infty$.*

BEWEIS. Ist $n \in \mathbb{N}$ und $\text{char}(K) \nmid n$, ist $X^n - 1 \in K[X]$ separabel und hat daher n Nullstellen. Daher ist $|\overline{K}| \geq n$ und folglich $|\overline{K}| = \infty$.

Sei nun $C = V(f)$ und

$$f = \sum_{i=0}^n a_i(Y)X^i \in K[X, Y] \quad \text{mit} \quad n \in \mathbb{N}_0, \quad a_i(Y) \in K[Y] \quad \text{und} \quad a_n(Y) \neq 0.$$

FALL 1: $n = 0$. Dann ist $f = a_0(Y) \in K[Y] \setminus K$. Seien $y_1, \dots, y_m \in \overline{K}$ die Nullstellen von f , und sei $y \in \overline{K}$ mit $f(y) \neq 0$. Dann folgt

$$C = \bigcup_{j=1}^m \overline{K} \times \{y_j\} \quad \text{und} \quad \overline{K} \times \{y\} \subset \overline{K}^2 \setminus C, \quad \text{also} \quad |C| = |\overline{K}^2 \setminus C| = \infty.$$

FALL 2: $n > 0$. Die Menge $N = \{y \in \overline{K} \mid a_n(y) = 0\}$ ist endlich, und für jedes $y \in \overline{K} \setminus N$ ist die Menge $M(y) = \{x \in \overline{K} \mid f(x, y) = 0\}$ endlich und nicht leer. Wegen

$$\bigcup_{y \in \overline{K} \setminus N} M(y) \subset C \quad \text{and} \quad \bigcup_{y \in \overline{K} \setminus N} (\overline{K} \setminus M(y)) \subset \overline{K} \setminus C \quad \text{folgt} \quad |C| = |\overline{K}^2 \setminus C| = \infty. \quad \square$$

Lemma 1.3.2. *Sei R ein faktorieller Bereich, und haben $f, g \in R[X]$ keinen nicht-konstanten gemeinsamen Teiler in $R[X]$. Dann gibt es Polynome $p, q \in R[X]$ mit $pf + qg \in R^\bullet$.*

BEWEIS Ü!. □

Satz 1.3.3. *Sind $f, g \in K[X, Y] \setminus K$ teilerfremd, so ist $|V(f) \cap V(g)| < \infty$.*

BEWEIS. $R_1 = K[X]$ ist ein faktorieller Bereich, und $f, g \in R_1[Y]$ sind Polynome ohne nicht-konstanten gemeinsamen Teiler in $R_1[Y]$. Nach Lemma 1.3.2 gibt es Polynome $p_1, q_1 \in R_1[Y] = K[X, Y]$ mit $p_1f + q_1g = d_1 \in R_1^\bullet = K[X]^\bullet$. Aus demselben Grund gibt es Polynome $p_2, q_2 \in K[X, Y]$ mit $p_2f + q_2g = d_2 \in K[Y]^\bullet$. Ist nun $(\alpha, \beta) \in V(f) \cap V(g)$, so folgt $d_1(\alpha) = d_2(\beta) = 0$ und daher $|V(f) \cap V(g)| \leq \text{gr}(d_1)\text{gr}(d_2) < \infty$. □

1.4

Sei $n \in \mathbb{N}$ und $K[\mathbf{X}]$ ein Polynomring in $\mathbf{X} = (X_1, \dots, X_n)$ über K . Dann ist $K[\mathbf{X}]$ faktoriell, und die Primelemente von $K[\mathbf{X}]$ sind genau die (über K) irreduziblen Polynome. Zwei Polynome $f, g \in K[\mathbf{X}]$ sind genau dann assoziiert [$f \simeq g$], wenn $f = cg$ mit $c \in K^\times$. Ein Polynom $f \in K[\mathbf{X}]$ heißt *reduziert* (über K), wenn $f = f_1 \cdot \dots \cdot f_k$ mit $k \in \mathbb{N}$ und über K irreduziblen paarweise nicht assoziierten Polynomen $f_1, \dots, f_k \in K[\mathbf{X}] \setminus K$ [äquivalent: $p^2 \nmid f$ für alle (irreduziblen) $p \in K[\mathbf{X}] \setminus K$].

Definition 1.4.1. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve. Eine Abbildung $u: C \rightarrow \overline{K}$ heißt eine *über K definierte reguläre Funktion* (auf C), wenn es ein Polynom $g \in K[X, Y]$ gibt, so dass $u(\mathbf{p}) = g(\mathbf{p})$ für alle $\mathbf{p} \in C$. Sei $K[C]$ die K -Algebra der über K definierten regulären Funktionen auf C (bezüglich wertweiser Verknüpfung). $K[C]$ heißt *Koordinatenring* von C . Wir betrachten die Elemente von K als konstante Abbildungen auf C und erhalten damit $K \subset K[C]$.

Wir identifizieren ein Polynom $f \in K[X, Y]$ mit der polynomialen Abbildung $f^{\overline{K}}: \overline{K}^2 \rightarrow \overline{K}$. Dann ist $K[C] = \{g \upharpoonright C \mid g \in K[X, Y]\}$, und die Abbildung

$$\theta_C: K[X, Y] \rightarrow K[C], \quad \text{definiert durch } \theta_C(f) = f \upharpoonright C,$$

ist ein K -Algebrenepimorphismus. Ist $x = \theta_C(X)$ und $y = \theta_C(Y)$, so ist $K[C] = K[x, y]$, und für jeden Punkt $\mathbf{p} = (\alpha, \beta) \in C$ ist $x(\mathbf{p}) = \alpha$ und $y(\mathbf{p}) = \beta$. x und y heißen die *Koordinatenfunktionen* von C . Das Ideal

$$I_K(C) = \text{Ker}(\theta_C) = \{g \in K[X, Y] \mid g \upharpoonright C = 0\} = \{g \in K[X, Y] \mid C \subset V(g)\} \triangleleft K[X, Y]$$

heißt *K -Verschwindungsideal* von C . Für $g \in K[X, Y]$ identifizieren wir die Restklasse $g + \mathcal{J}(C)$ mit der Funktion $g \upharpoonright C: C \rightarrow \overline{K}$.

Satz 1.4.2. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve, seien $x, y \in K[C]$ die Koordinatenfunktionen von C und $f \in K[X, Y]$. Genau dann ist $f \upharpoonright C = 0$, wenn $f(x, y) = 0 \in K[C]$.

PROOF. Für $\mathbf{p} = (\alpha, \beta) \in C$ ist $f(x, y)(\mathbf{p}) = f(x(\mathbf{p}), y(\mathbf{p})) = f(\alpha, \beta) = f(\mathbf{p})$. □

Satz 1.4.3. Sei $f = f_1^{e_1} \cdots f_k^{e_k} \in K[X, Y] \setminus K$ mit $k \in \mathbb{N}$, paarweise nicht-assozierten irreduziblen Polynomen $f_1, \dots, f_k \in K[X, Y] \setminus K$, $e_1, \dots, e_k \in \mathbb{N}$, $C = V(f) \subset \overline{K}^2$, und $f_0 = f_1 \cdots f_k$. Dann folgt

$$C = V(f_0) = \bigcup_{i=1}^k V(f_i) \quad \text{und} \quad \mathcal{J}_K(C) = \mathcal{J}_K(V(f_0)) = f_0 K[X, Y].$$

BEWEIS. Sei $\mathbf{p} \in \overline{K}^2$. Genau dann ist $\mathbf{p} \in V(f)$, wenn $0 = f(\mathbf{p}) = f_1(\mathbf{p})^{e_1} \cdots f_k(\mathbf{p})^{e_k}$, wenn also $f_i(\mathbf{p}) = 0$ für ein $i \in [1, k]$ und damit $\mathbf{p} \in V(f_i)$ ist. Daher ist $V(f) = V(f_0)$ die Vereinigung der $V(f_i)$.

Für alle $\mathbf{p} \in V(f)$ ist $f_0(\mathbf{p}) = 0$, also $f_0 \in \mathcal{J}_K(V(f))$ und daher $\mathcal{J}_K(V(f)) \subset \mathcal{J}_K(V(f_0))$. Für den Nachweis der umgekehrten Inklusion müssen wir zeigen: Ist $g \in \mathcal{J}_K(V(f_0))$, also $V(f) \subset V(g)$, so folgt $f_i \mid g$ für alle $i \in [1, k]$ [wegen der paarweisen Teilerfremdheit von f_1, \dots, f_k und da $K[X, Y]$ faktoriell ist, folgt dann $f_0 \mid g$ und daher $g \in \mathcal{J}_K(V(f_0))$]. Wir nehmen im Gegenteil an, es sei $i \in [1, k]$ und $f_i \nmid g$. Da f_i irreduzibel ist, sind f_i und g teilerfremd, und nach Satz 1.3.3 ist $|V(f_i) \cap V(g)| < \infty$. Wegen $V(f_i) \subset V(f) \subset V(g)$ folgt nun $|V(f_i)| < \infty$, ein Widerspruch zu Satz 1.3.1. □

1.5

Definition 1.5.1. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve.

1. C heißt *irreduzibel (über K)*, wenn C keine Zerlegung $C = C_1 \cup C_2$ mit über K definierten Kurven $C_1, C_2 \subsetneq C$ besitzt. C heißt *absolut irreduzibel*, wenn C über \overline{K} irreduzibel ist.
2. Sei $\mathcal{J}_K(C) = \mathcal{J}_K(V(f))$ und $f = f_1 \cdots f_k \in K[X, Y] \setminus K$ mit $k \in \mathbb{N}$ und paarweise nicht-assozierten irreduziblen $f_1, \dots, f_k \in K[X, Y] \setminus K$; dann ist $C = V(f) = V(f_1) \cup \dots \cup V(f_k)$. Die Kurven $V(f_1), \dots, V(f_k)$ heißen die *Komponenten* von C über K . Das Polynom f ist bis auf Faktoren aus K^\times eindeutig bestimmt und heißt *Minimalpolynom* von C über K .

Satz 1.5.2. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve.

1. Die folgenden Aussagen sind äquivalent:

- (a) Es gibt keine über K definierte Kurve C_1 mit $C_1 \subsetneq C$.
 (b) C ist irreduzibel über K .
 (c) $C = V(f)$ mit einem (über K) irreduziblen Polynom $f \in K[X, Y] \setminus K$.
 (d) $\mathcal{J}_K(C)$ ist ein Primideal von $K[X, Y]$.
 (e) $K[C]$ ist ein Bereich.
2. C hat eine (bis auf die Reihenfolge der Faktoren) eindeutige Zerlegung $C = C_1 \cup \dots \cup C_k$ mit paarweise verschiedenen über K definierten irreduziblen Kurven C_1, \dots, C_k ; diese sind die Komponenten von C über K .

BEWEIS. 1. (a) \Rightarrow (b) Offensichtlich.

(b) \Rightarrow (c) Sei $\mathcal{J}_K(C) = {}_{K[X, Y]}(f)$ mit $f \in K[X, Y] \setminus K$. Ist f nicht irreduzibel über K , so hat C mindestens zwei Komponenten über K und ist daher nicht irreduzibel.

(c) \Rightarrow (d) Ist $C = V(f)$ mit einem irreduziblen Polynom $f \in K[X, Y] \setminus K$, so ist (nach Satz 1.4.3) $\mathcal{J}_K(C) = {}_{K[X, Y]}(f)$ ein Primideal.

(d) \Leftrightarrow (e) Es ist $K[C] \cong K[X, Y]/\mathcal{J}_K(C)$.

(d) \Rightarrow (a) Sei C_1 eine über K definierte Kurve, $C_1 \subset C$, $\mathcal{J}_K(C) = {}_{K[X, Y]}(f)$ und $\mathcal{J}_K(C_1) = {}_{K[X, Y]}(f_1)$ mit $f, f_1 \in K[X, Y] \setminus K$. Da $\mathcal{J}_K(C)$ ein Primideal ist, ist f irreduzibel, und wegen $f \upharpoonright C_1 = 0$ ist $f \in \mathcal{J}_K(C_1)$, also $f_1 \mid f$. Damit folgt $f_1 \simeq f$ und $C_1 = V(f_1) = V(f) = C$.

2. Seien C_1, \dots, C_k die Komponenten von C über K . Diese sind nach Definition paarweise verschiedene über K definierte irreduzible Kurven, und es ist $C = C_1 \cup \dots \cup C_k$. Sei $C = C'_1 \cup \dots \cup C'_l$ eine weitere Zerlegung von C in paarweise verschiedene über K definierte irreduzible Kurven, und für $i \in [1, l]$ sei $\mathcal{J}_K(C'_i) = {}_{K[X, Y]}(f'_i)$. Dann sind $f'_1, \dots, f'_l \in K[X, Y]$ paarweise nicht-assoziierte irreduzible Polynome, es ist $f'_1 \cdots f'_l$ reduziert und $C = V(f'_1 \cdots f'_l)$, also $\mathcal{J}_K(C) = {}_{K[X, Y]}(f'_1 \cdots f'_l)$. Damit folgt $\{C'_1, \dots, C'_l\} = \{C_1, \dots, C_k\}$. \square

1.6

Definition 1.6.1. Sei $\mathbf{p} = (\alpha, \beta) \in \overline{K}^2$.

1. Sei $f \in K[X, Y]$. Dann ist

$$f = \sum_{i, j \geq 0} a_{i, j} [(X - \alpha) + \alpha]^i [(Y - \beta) + \beta]^j = \sum_{i, j \geq 0} \tilde{a}_{i, j} (X - \alpha)^i (Y - \beta)^j \quad \text{mit } \tilde{a}_{i, j} \in \overline{K},$$

und

$$\tilde{a}_{i, j} = \frac{1}{i!j!} \frac{\partial^{i+j} f}{\partial X^i \partial Y^j}(\mathbf{p}), \quad \text{falls } \text{char}(K) \nmid i!j! \quad (\ddot{U}!).$$

Insbesondere ist stets

$$\tilde{a}_{1,0} = \frac{\partial f}{\partial X}(\mathbf{p}) \quad \text{und} \quad \tilde{a}_{0,1} = \frac{\partial f}{\partial Y}(\mathbf{p}).$$

$\text{ord}_{\mathbf{p}}(f) = \inf\{i + j \mid i, j \geq 0, \tilde{a}_{i, j} \neq 0\} \in \mathbb{N}_0 \cup \{\infty\}$ heißt *Ordnung* von f in \mathbf{p} .

Für alle $c \in K^\times$ ist $\text{ord}_{\mathbf{p}}(cf) = \text{ord}_{\mathbf{p}}(f)$. Genau dann ist $f(\mathbf{p}) = 0$, wenn $\text{ord}_{\mathbf{p}}(f) > 0$.

Für $f, g \in K[X, Y]$ ist $\text{ord}_{\mathbf{p}}(fg) = \text{ord}_{\mathbf{p}}(f) + \text{ord}_{\mathbf{p}}(g)$, $\text{ord}_{\mathbf{p}}(f + g) \geq \min\{\text{ord}_{\mathbf{p}}(f), \text{ord}_{\mathbf{p}}(g)\}$, und im Falle $\text{ord}_{\mathbf{p}}(f) < \text{ord}_{\mathbf{p}}(g)$ ist $\text{ord}_{\mathbf{p}}(f + g) = \text{ord}_{\mathbf{p}}(f)$.

2. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve und $f \in K[X, Y]$ ein Minimalpolynom von C über K . Dann heißt $\text{ord}_{\mathbf{p}}(C) = \text{ord}_{\mathbf{p}, K}(C) = \text{ord}_{\mathbf{p}}(f)$ die *Ordnung* von C in \mathbf{p} über K . \mathbf{p} heißt *regulärer Punkt* von C über K , wenn $\text{ord}_{\mathbf{p}, K}(C) = 1$.

Genau dann ist $\mathbf{p} \in C$, wenn $\text{ord}_{\mathbf{p}}(C) > 0$. Ist $\mathbf{p} \in C$, so ist \mathbf{p} genau dann ein über K regulärer Punkt von C , wenn

$$\left(\frac{\partial f}{\partial X}(\mathbf{p}), \frac{\partial f}{\partial Y}(\mathbf{p}) \right) \neq (0, 0).$$

Ist $\mathbf{p} = (\alpha, \beta) \in C$ ein regulärer Punkt, so nennt man die Gerade

$$L = V\left(\frac{\partial f}{\partial X}(\mathbf{p})(X - \alpha) + \frac{\partial f}{\partial Y}(\mathbf{p})(Y - \beta)\right)$$

die *Tangente* von C im Punkte \mathbf{p} .

C heißt *regulär* oder *glatt* über K , wenn jeder Punkt von C über K regulär ist.

Satz 1.6.2. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve, $f \in K[X, Y]$ ein Minimalpolynom von C über K , $f = f_1 \cdot \dots \cdot f_k$ mit irreduziblen (nicht notwendig verschiedenen) Polynomen $f_1, \dots, f_k \in \overline{K}[X, Y]$ und $\mathbf{p} \in C$. Dann sind äquivalent:

- (a) \mathbf{p} ist regulärer Punkt von C über K .
- (b) Es gibt genau ein $i \in [1, k]$ mit $f_i(\mathbf{p}) = 0$, und für dieses i ist

$$\left(\frac{\partial f_i}{\partial X}(\mathbf{p}), \frac{\partial f_i}{\partial Y}(\mathbf{p}) \right) \neq (0, 0).$$

Insbesondere folgt:

1. Ist \mathbf{p} ein regulärer Punkt von C über K , so liegt \mathbf{p} in genau einer Komponente von C über \overline{K} und ist ein über \overline{K} regulärer Punkt dieser Komponente.
2. Ist f absolut irreduzibel, so ist \mathbf{p} genau dann ein regulärer Punkt von C über K , wenn \mathbf{p} ein regulärer Punkt von C über \overline{K} ist.

BEWEIS. Die Äquivalenz von (a) und (b) folgt aus den Formeln

$$\frac{\partial f}{\partial X}(\mathbf{p}) = \sum_{i=1}^k \frac{\partial f_i}{\partial X}(\mathbf{p}) \prod_{\substack{j=1 \\ j \neq i}}^r f_j(\mathbf{p}) \quad \text{und} \quad \frac{\partial f}{\partial Y}(\mathbf{p}) = \sum_{i=1}^k \frac{\partial f_i}{\partial Y}(\mathbf{p}) \prod_{\substack{j=1 \\ j \neq i}}^r f_j(\mathbf{p}).$$

Die übrigen Behauptungen sind offensichtlich. □

1.7

Definition 1.7.1. Sei $C \subset \overline{K}^2$ eine über K definierte irreduzible Kurve. Dann ist $K[C]$ ein Bereich; sei Quotientenkörper $K(C) = \mathfrak{q}(K[C])$ heißt *Funktionenkörper* von C über K , seine Elemente heißen *über K definierte rationale Funktionen auf C* .

Sei $J_K(C) = {}_{K[X, Y]}(f)$ und $\gamma \in K(C)$. Dann ist

$$\gamma = \frac{\varphi}{\psi} = \frac{g + {}_{K[X, Y]}(f)}{h + {}_{K[X, Y]}(f)}$$

mit $g, h \in K[X, Y]$, $h \notin {}_{K[X, Y]}(f)$, $\varphi = g + {}_{K[X, Y]}(f)$, $\psi = h + {}_{K[X, Y]}(f) \in K[C]$ und $\psi \neq 0$. Da $K[C]$ im Allgemeinen nicht faktoriell ist, ist diese Bruchdarstellung nicht eindeutig.

Ist $\gamma \in K(C)$ und $\mathbf{p} \in C$, so heißt γ *regulär* in \mathbf{p} , wenn es $g, h \in K[X, Y]$ gibt, so dass $h(\mathbf{p}) \neq 0$ und

$$\gamma = \frac{g + (f)}{h + (f)}. \quad \text{Dann heißt } \gamma(\mathbf{p}) = \frac{g(\mathbf{p})}{h(\mathbf{p})} \in \overline{K} \text{ der Wert von } \gamma \text{ an der Stelle } \mathbf{p}.$$

$\gamma(\mathbf{p})$ ist dann von der Bruchdarstellung unabhängig. Da f irreduzibel ist, ist genau dann $h \notin (f)$, wenn h und f teilerfremd sind, und daher ist die Menge $\{\mathbf{p} \in C \mid h(\mathbf{p}) = 0\} = V(f) \cap V(h)$ endlich. Daher ist jede rationale Funktion in fast allen Punkten regulär.

Satz 1.7.2. Sei $C \subset \overline{K}^2$ eine über K definierte irreduzible Kurve, $f \in K[X, Y] \setminus K$ ein Minimalpolynom von C über K , und seien $x, y \in K[C]$ die Koordinatenfunktionen von C . Dann ist $K(C) = K(x, y)$, $f(x, y) = 0$, und die Körpererweiterung $K(C)/K$ ist transzendent.

Ist x transzendent über K , so ist y algebraisch über $K(x)$. Ist $c \in K[x]^\bullet$ der höchste Koeffizient des Polynoms $f(x, Y) \in K(x)[Y]$, so ist $c^{-1}f(x, Y) \in K(x)[Y]$ das Minimalpolynom von y über $K(x)$.

BEWEIS. Nach Definition ist $K[C] = K[x, y]$ und daher $K(C) = K(x, y)$. Für alle $\mathbf{p} = (\alpha, \beta) \in C$ ist $f(x, y)(\mathbf{p}) = f(x(\mathbf{p}), y(\mathbf{p})) = f(\mathbf{p}) = 0$, also $f(x, y) = 0 \in K[C]$.

Angenommen, $K(x, y)/K$ sei algebraisch. Dann gibt es ein $g \in K[X] \setminus K$ mit $g(x) = g(y) = 0$. Für alle $\mathbf{p} = (\alpha, \beta) \in C$ ist dann $0 = g(x)(\mathbf{p}) = g(x(\mathbf{p})) = g(\alpha)$ und $0 = g(y)(\mathbf{p}) = g(y(\mathbf{p})) = g(\beta)$. Damit folgt $|C| < \infty$, ein Widerspruch zu Satz 1.3.1.

Ist x transzendent über K , so ist $K[X, Y] \cong K[x, Y] = K[x][Y]$. Daher ist $f(x, Y)$ irreduzibel über $K[x]$, also nach dem Gauß'schen Lemma auch über $K(x)$. Dann ist $c^{-1}f(x, Y) \in K(x)[Y]$ normiert und irreduzibel, und $c^{-1}f(x, y) = 0$. \square

Definition 1.7.3. Sei $C \subset \overline{K}^2$ eine über K definierte irreduzible Kurve und $\mathbf{p} \in C$. Dann heißt

$$\mathcal{O}_{\mathbf{p}}(C) = \mathcal{O}_{\mathbf{p}, K}(C) = K[C]_{\mathbf{p}} = \left\{ \frac{\varphi}{\psi} \in K(C) \mid \varphi, \psi \in K[C], \psi(\mathbf{p}) \neq 0 \right\}$$

der lokale Ring von C in \mathbf{p} über K , und

$$\mathcal{M}_{\mathbf{p}}(C) = \mathcal{M}_{\mathbf{p}, K}(C) = \left\{ \frac{\varphi}{\psi} \in K(C) \mid \varphi, \psi \in K[C], \psi(\mathbf{p}) \neq 0, \varphi(\mathbf{p}) = 0 \right\}$$

das maximale Ideal von C in \mathbf{p} über K .

Ist $\gamma \in \mathcal{O}_{\mathbf{p}}(C)$, so ist γ regulär in \mathbf{p} , $\gamma(\mathbf{p}) \in \overline{K}$, und $\mathcal{M}_{\mathbf{p}}(C) = \{\gamma \in \mathcal{O}_{\mathbf{p}}(C) \mid \gamma(\mathbf{p}) = 0\}$.

Definition 1.7.4 (Ringtheorie). Ein (kommutativer) Ring R heißt lokal, wenn $R \setminus R^\times$ ein Ideal ist (dann ist $P = R \setminus R^\times$ das größte echte Ideal von R , und R/P heißt Restklassenkörper von R).

Satz 1.7.5. Sei $C \subset \overline{K}^2$ eine über K definierte irreduzible Kurve, $\mathbf{p} = (\alpha, \beta) \in C$, und seien $x, y \in K[C]$ die Koordinatenfunktionen von C .

1. $\mathcal{O}_{\mathbf{p}}(C)$ ist ein lokaler Bereich mit maximalem Ideal $\mathcal{M}_{\mathbf{p}}(C)$, es ist $K[C] \subset \mathcal{O}_{\mathbf{p}}(C) \subset K(C)$, die Abbildung $\pi_{\mathbf{p}}: \mathcal{O}_{\mathbf{p}}(C) \rightarrow \overline{K}$, definiert durch $\pi_{\mathbf{p}}(\gamma) = \gamma(\mathbf{p})$, ist ein K -Algebrenhomomorphismus, $\text{Ker}(\pi_{\mathbf{p}}) = \mathcal{M}_{\mathbf{p}}(C)$ und $\text{Bi}(\pi_{\mathbf{p}}) = K(\alpha, \beta) = K[\alpha, \beta] \cong K[C]/K[C] \cap \mathcal{M}_{\mathbf{p}}(C) \cong \mathcal{O}_{\mathbf{p}}(C)/\mathcal{M}_{\mathbf{p}}(C)$. Insbesondere ist $K[C]/K[C] \cap \mathcal{M}_{\mathbf{p}}(C)$ ein maximales Ideal von $K[C]$.
2. Ist $\mathbf{p} \in C(K)$, so ist $\mathcal{M}_{\mathbf{p}}(C) = \mathcal{O}_{\mathbf{p}}(x - \alpha, y - \beta)$.

BEWEIS. 1. Offensichtlich ist $\mathcal{O}_{\mathbf{p}}(C) \subset K(C)$ ein Teilbereich, $\mathcal{M}_{\mathbf{p}}(C) \subset \mathcal{O}_{\mathbf{p}}(C)$ ein Ideal und $\pi_{\mathbf{p}}$ ein K -Algebrenhomomorphismus mit $\text{Ker}(\pi_{\mathbf{p}}) = \mathcal{M}_{\mathbf{p}}(C)$. Ist $\gamma \in \mathcal{O}_{\mathbf{p}}(C)$ so folgt

$$\gamma = \frac{\varphi}{\psi} \text{ mit } \varphi, \psi \in K[C], \varphi(\mathbf{p}) \neq 0, \text{ und aus } \gamma \notin \mathcal{M}_{\mathbf{p}}(C) \text{ folgt } \psi(\mathbf{p}) \neq 0, \text{ also } \frac{\psi}{\varphi} \in \mathcal{O}_{\mathbf{p}}(C).$$

Daher ist $\mathcal{O}_{\mathbf{p}}(C) \setminus \mathcal{M}_{\mathbf{p}}(C) = \mathcal{O}_{\mathbf{p}}(C)^\times$, also $\mathcal{O}_{\mathbf{p}}(C)$ ein lokaler Bereich mit maximalem Ideal $\mathcal{M}_{\mathbf{p}}(C)$ und $\pi_{\mathbf{p}}(\mathcal{O}_{\mathbf{p}}(C) \setminus \mathcal{M}_{\mathbf{p}}(C)) \cong \mathcal{O}_{\mathbf{p}}(C)/\mathcal{M}_{\mathbf{p}}(C)$ ein Körper. Es ist $\pi_{\mathbf{p}}(K[C]) = K[\pi_{\mathbf{p}}(x), \pi_{\mathbf{p}}(y)] = K[\alpha, \beta] \subset \overline{K}$, also $\pi_{\mathbf{p}}(K[C]) = K(\alpha, \beta)$ und daher $\text{Ker}(\pi_{\mathbf{p}}|K[C]) = K[C] \cap \mathcal{M}_{\mathbf{p}}(C)$ ein maximales Ideal von $K[C]$. Ist $\gamma = \psi^{-1}\varphi \in \mathcal{O}_{\mathbf{p}}(C)$ mit $\varphi, \psi \in K[C]$ und $\psi(\mathbf{p}) \neq 0$, so ist $\pi_{\mathbf{p}}(\gamma) = \psi(\mathbf{p})^{-1}\varphi(\mathbf{p}) \in \pi_{\mathbf{p}}(K[C])$, und daher folgt $\text{Bi}(\pi_{\mathbf{p}}) \cong \mathcal{O}_{\mathbf{p}}(C)/\mathcal{M}_{\mathbf{p}}(C) \cong K[C]/K[C] \cap \mathcal{M}_{\mathbf{p}}(C)$.

2. Seien $\alpha, \beta \in K$, und für $g \in K[X, Y]$ sei $\bar{g} = g|_C \in K[C]$. Sei $\gamma \in \mathcal{O}_{\mathbf{p}}(C)$,

$$\gamma = \frac{\bar{g}}{h} \text{ mit } g, h \in K[X, Y] \text{ und } h(\mathbf{p}) = h(\alpha, \beta) \neq 0.$$

Sei $g = c + (X - \alpha)g_1 + (Y - \beta)g_2$ mit $c \in K$ und $g_1, g_2 \in K[X, Y]$. Dann folgt

$$\bar{g} = c + (x - \alpha)\bar{g}_1 + (y - \beta)\bar{g}_2, \quad \gamma = \frac{c}{h} + (x - \alpha)\frac{\bar{g}_1}{h} + (y - \beta)\frac{\bar{g}_2}{h} \quad \text{und} \quad \gamma(\mathbf{p}) = h(\mathbf{p})^{-1}c.$$

Genau dann ist $\gamma \in \mathcal{M}_{\mathbf{p}}(C)$, wenn $c = 0$ und daher $\gamma \in \mathcal{O}_{\mathbf{p}}(x - \alpha, y - \beta)$ ist. □

Ebene projektive Kurven

Im ganzen Kapitel sei K ein Körper und \overline{K} eine algebraische Hülle von K .

2.1

Definition 2.1.1. Sei $n \in \mathbb{N}$ und $K[X_1, \dots, X_n]$ ein Polynomring. Ein Polynom $F \in K[X_1, \dots, X_n]$ heißt *homogen* oder eine *Form* vom Grade $d \in \mathbb{N}_0$, wenn

$$F = \sum_{\substack{i_1, \dots, i_n \geq 0 \\ i_1 + \dots + i_n = d}} c_{i_1, \dots, i_n} X_1^{i_1} \cdot \dots \cdot X_n^{i_n}.$$

Ist dann T eine weitere Unbestimmte über K , so folgt $F(TX_1, \dots, TX_n) = T^d F(X_1, \dots, X_n)$. Ist $d > 0$, so sind die partiellen Ableitungen von F homogene Polynome vom Grade $d - 1$, und es ist

$$\sum_{i=1}^n X_i \frac{\partial f}{\partial X_i} = df.$$

Jedes Polynom $f \in K[X_1, \dots, X_n]$ hat eine eindeutige Darstellung $f = f_0 + f_1 + \dots + f_d$ mit Formen f_i vom Grade i für alle $i \in [0, d]$ und $f_d \neq 0$ (dann ist $d = \text{gr}(f)$). f_i heißt *i -te homogene Komponente* und f_d heißt *Leitform* von f .

Lemma 2.1.2. Seien $f, g \in K[X_1, \dots, X_n]$. Genau dann ist fg homogen, wenn f und g beide homogen sind.

BEWEIS. Sei $f = f_{d_1} + f_{d_1+1} + \dots + f_d$ und $g = g_{e_1} + g_{e_1+1} + \dots + g_e$ mit $d_1, d, e_1, e \in \mathbb{N}_0$, $d_1 \leq d$, $e_1 \leq e$ und Formen f_i vom Grade i und g_j vom Grade j für alle $i \in [d_1, d]$ und alle $j \in [e_1, e]$. Dann ist $fg = h_{d_1+e_1} + h_{d_1+e_1+1} + \dots + h_{d+e}$ mit Formen h_k vom Grade k , es ist $h_{d_1+e_1} = f_{d_1}g_{e_1} \neq 0$ und $h_{d+e} = f_d g_e \neq 0$. Genau dann ist fg homogen, wenn $d_1 + e_1 = d + e$, und das ist äquivalent mit $d = d_1$ und $e = e_1$, also der Homogenität von f und g . \square

2.2

Definition 2.2.1. Sei $n \in \mathbb{N}_0$. Die Menge \mathbb{P}_K^n die Menge aller eindimensionalen Untervektorräume von K^{n+1} heißt *n -dimensionaler projektiver Raum über K* .

Es ist $|\mathbb{P}_K^0| = 1$, \mathbb{P}_K^1 heißt *projektive Gerade* und \mathbb{P}_K^2 heißt *projektive Ebene* über K .

Für $(x_1, \dots, x_{n+1}) \in K^{n+1} \setminus \{\mathbf{0}\}$ sei $(x_1 : \dots : x_{n+1}) = K(x_1, \dots, x_{n+1}) \in \mathbb{P}_K^n$. Man nennt x_1, \dots, x_{n+1} die *homogenen Koordinaten* des (projektiven) Punktes $\mathbf{p} = (x_1 : \dots : x_{n+1})$.

Für $(x_1, \dots, x_{n+1}) = (x'_1, \dots, x'_{n+1}) \in K^{n+1} \setminus \{\mathbf{0}\}$ ist genau dann $(x_1 : \dots : x_{n+1}) = (x'_1 : \dots : x'_{n+1}) \in \mathbb{P}_K^n$, wenn es ein $\lambda \in K^\times$ gibt mit $x'_i = \lambda x_i$ für alle $i \in [1, n+1]$.

Für $i \in [1, n+1]$ heißt $\mathbb{P}_K^n(i) = \{(x_1 : \dots : x_{n+1}) \in \mathbb{P}_K^n \mid x_i \neq 0\} = \{(x_1 : \dots : x_{n+1}) \in \mathbb{P}_K^n \mid x_i = 1\}$ das *i -te affine Stück* von \mathbb{P}_K^n .

Für jedes $i \in [1, n+1]$ ist die Abbildung

$$\iota_i: K^n \rightarrow \mathbb{P}_K^n(i), \quad \text{definiert durch} \quad \iota_i(x_1, \dots, x_n) = (x_1 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_n),$$

bijektiv, und

$$\mathbb{P}_K^n = \bigcup_{i=1}^{n+1} \mathbb{P}_K^n(i).$$

Im Folgenden identifizieren wir K^n mit $\mathbb{P}_K^n(n+1)$ vermöge ι_{n+1} . Dann ist $(x_1, \dots, x_n) = (x_1 : \dots : x_n : 1)$ für alle $(x_1, \dots, x_n) \in K^n$, und $\mathbb{P}_K^n = K^n \cup \{(x_1 : \dots : x_n : 0) \mid (x_1, \dots, x_n) \in K^n \setminus \{\mathbf{0}\}\}$. Man nennt die Punkte $\mathbf{p} \in K^n$ die *endlichen Punkte* und die Punkte $\mathbf{p} \in \mathbb{P}_K^n \setminus K^n$ die *Fernpunkte* von \mathbb{P}_K^n .

Es ist $\mathbb{P}_K^1 = K \cup \{(1:0)\}$ und $\mathbb{P}_K^2 = K^2 \cup H_\infty$ mit $H_\infty = \{(x:y:0) \mid (x,y) \in K^2 \setminus \{(0,0)\}\}$. Man nennt $(1:0)$ den *Fernpunkt* der projektiven Geraden und H_∞ die *Ferngerade* der projektiven Ebene.

Definition 2.2.2. Sei $F \in K[X, Y, Z]$ eine Form vom Grade $d \in \mathbb{N}$. Ein Punkt $\mathbf{p} = (\alpha : \beta : \gamma) \in \mathbb{P}_K^2$ heißt *Nullstelle von F* , wenn $F(\alpha, \beta, \gamma) = 0$ (wegen $F(\lambda\alpha, \lambda\beta, \lambda\gamma) = \lambda^d F(\alpha, \beta, \gamma)$ ist diese Definition unabhängig von den gewählten homogenen Koordinaten von \mathbf{p}). Man schreibt $F(\mathbf{p}) = 0$, falls \mathbf{p} eine Nullstelle von F ist, und $F(\mathbf{p}) \neq 0$ andernfalls.

Die Menge $V_+(F) = \{\mathbf{p} \in \mathbb{P}_K^2 \mid F(\mathbf{p}) = 0\}$ heißt *projektives Nullstellengebilde* von F . Eine Teilmenge $\Gamma \subset \mathbb{P}_K^2$ heißt *über K definierte (ebene) projektive (algebraische) Kurve*, wenn $\Gamma = V_+(F)$ mit einer Form $F \in K[X, Y, Z] \setminus K$.

Eine über K definierte projektive Kurve $\Gamma \subset \mathbb{P}_K^2$ heißt *irreduzibel (über K)*, wenn Γ keine Zerlegung $\Gamma = \Gamma_1 \cup \Gamma_2$ mit über K definierten projektiven Kurven $\Gamma_1, \Gamma_2 \subsetneq \Gamma$ besitzt.

Ist $\Gamma \subset \mathbb{P}_K^2$ eine über K definierte projektive Kurve, so heißt $\Gamma(K) = \Gamma \cap \mathbb{P}_K^2$ die Menge der *K -rationalen Punkte* von Γ . Das Ideal $\mathcal{J}_K^+(\Gamma) = \mathcal{I}_{K[X,Y,Z]}(\Gamma)$ ($\{F \in K[X, Y, Z] \mid F \text{ ist eine Form mit } \Gamma \subset V_+(F)\}$) heißt *homogenes Verschwindungsideal* von Γ , der Restklassenring $K[\Gamma] = K[X, Y, Z]/\mathcal{J}_K^+(\Gamma)$ heißt *homogener Koordinatenring* von Γ , und die Restklassen $\hat{x} = X + \mathcal{J}_K^+(\Gamma)$, $\hat{y} = Y + \mathcal{J}_K^+(\Gamma)$, $\hat{z} = Z + \mathcal{J}_K^+(\Gamma)$ heißen *homogene Koordinaten* von Γ . Es ist $K[\Gamma] = K[\hat{x}, \hat{y}, \hat{z}]$.

Ist $F = F_1^{e_1} \cdots F_k^{e_k}$ mit $k \in \mathbb{N}$, paarweise nicht-assozierten irreduziblen Formen F_1, \dots, F_k und $e_1, \dots, e_k \in \mathbb{N}$, so ist $V_+(F) = V_+(F_1) \cup \dots \cup V_+(F_k)$, und die projektiven Kurven $V_+(F_1), \dots, V_+(F_k)$ heißt die *Komponenten* von $V_+(F)$ über K .

Eine Teilmenge $L \subset \mathbb{P}_K^2$ heißt eine über K definierte *projektive Gerade*, wenn $L = V_+(aX + bY + cZ)$ mit $(a, b, c) \in K^3 \setminus \{(0, 0, 0)\}$. Insbesondere ist $H_\infty = V_+(Z)$ die Ferngerade des \mathbb{P}_K^2 .

Satz 2.2.3. Seien $L_1, L_2 \subset \mathbb{P}_K^2$ über K definierte projektive Geraden. Dann ist $L_1(K) \cap L_2(K) \neq \emptyset$.

BEWEIS. Für $i \in \{1, 2\}$ sei $L_i = V_+(a_i X + b_i Y + c_i Z)$ mit $(a_i, b_i, c_i) \in K^3 \setminus \{\mathbf{0}\}$. Dann hat das lineare Gleichungssystem $a_i x + b_i y + c_i z$ ($i = 1, 2$) eine Lösung $(x, y, z) \in K^3 \setminus \{\mathbf{0}\}$, und es ist $(x:y:z) \in L_1(K) \cap L_2(K)$. \square

2.3

Definition 2.3.1.

1. Sei $f \in K[X, Y] \setminus K$, $\text{gr}(f) = d \in \mathbb{N}$ und $f = f_0 + f_1 + \dots + f_d$ mit Formen f_i vom Grade i für alle $i \in [0, d]$ und $f_d \neq 0$. Dann heißt

$$f^* = \sum_{i=0}^d Z^{d-i} f_i(X, Y) = Z^d f\left(\frac{X}{Z}, \frac{Y}{Z}\right) \in K[X, Y, Z]$$

die *Homogenisierung* von f . $f^* \in K[X, Y, Z]$ ist eine Form vom Grade d .

2. Für eine Form $F \in K[X, Y, Z]$ heißt $F(X, Y, 1) \in K[X, Y]$ die *Dehomogenisierung* von F .

Lemma 2.3.2. Seien $F, G \in K[X, Y, Z]$ Formen, $f, g \in K[X, Y]$ und $c \in K^\times$.

1. f^* ist eine Form, $\text{gr}(f^*) = \text{gr}(f)$, und $Z \nmid f^*$.
2. $(cf)^* = cf^*$ und $(cF)_* = cF_*$.
3. $(fg)^* = f^*g^*$, $(FG)_* = F_*G_*$, $(F+G)_* = F_* + G_*$, und $(f^*)_* = f$.
4. Ist $r \in [0, \text{gr}(F)]$ maximal mit $Z^r \mid F$, so ist $\text{gr}(F_*) = \text{gr}(F) - r$, und $F = Z^r (F_*)^*$.
5. Ist $f = f_1^{e_1} \cdot \dots \cdot f_r^{e_r}$ die Primzerlegung von f in $K[X, Y]$, so ist $f^* = f_1^{*e_1} \cdot \dots \cdot f_r^{*e_r}$ die Primzerlegung von f^* in $K[X, Y, Z]$. Insbesondere ist f genau dann irreduzibel, wenn f^* irreduzibel ist.
6. Sei $Z \nmid F$. Ist $F = F_1^{e_1} \cdot \dots \cdot F_r^{e_r}$ die Primzerlegung von F in $K[X, Y, Z]$, so ist $F_* = F_{1*}^{e_1} \cdot \dots \cdot F_{r*}^{e_r}$ die Primzerlegung von F_* in $K[X, Y]$. Insbesondere ist F genau dann irreduzibel, wenn F_* irreduzibel ist.

BEWEIS. Ü! □

Definition 2.3.3. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve und $f \in K[X, Y] \setminus K$ ein Minimalpolynom von C über K . Dann heißt $\overline{C} = V_+(f^*) \subset \mathbb{P}_{\overline{K}}^2$ der *projektive Abschluss* von C (unabhängig von der Wahl des Minimalpolynoms). Die Punkte $\mathbf{p} \in \overline{C} \setminus C$ heißen *Fernpunkte* von C (sie liegen in der Vereinigung der affinen Stücke $\mathbb{P}_{\overline{K}}^2(1) = \{(1:y:z \mid (y, z) \in \overline{K}^2\}$ und $\mathbb{P}_{\overline{K}}^2(2) = \{(x:1:z \mid (x, z) \in \overline{K}^2\}$) von $\mathbb{P}_{\overline{K}}^2$).

Satz 2.3.4. Sei $C \subset \overline{K}^2$ eine über K definierte Kurve, $f \in K[X, Y] \setminus K$ ein Minimalpolynom von C über K und $f = f_0 + \dots + f_d$ mit $d \in \mathbb{N}$, Formen f_i vom Grade i für alle $i \in [0, d]$, und $f_d \neq 0$. Dann ist $C = \overline{C} \cap \overline{K}^2$, und $\overline{C} \setminus C = \{(\alpha:\beta:0) \in \mathbb{P}_{\overline{K}}^2 \mid (\alpha, \beta) \in V(f_d) \setminus \{(0, 0)\}\} = \overline{C} \cap V_+(Z)$ ist endlich.

BEWEIS. Sei $\mathbf{p} = (\alpha:\beta:\gamma) \in \mathbb{P}_{\overline{K}}^2$. Genau dann ist $\mathbf{p} \in \overline{C} = V_+(f^*)$, wenn

$$\text{entweder } \gamma \neq 0 \text{ und } f\left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}\right) = 0 \text{ oder } \gamma = 0 \text{ und } f_d(\alpha, \beta) = 0.$$

Damit folgt:

$$\mathbf{p} \in \overline{C} \cap \overline{K}^2 \iff \gamma \neq 0 \iff \mathbf{p} = \left(\frac{\alpha}{\gamma}:\frac{\beta}{\gamma}:1\right) = \left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma}\right) \in V(f) = C.$$

Genau dann ist $\mathbf{p} \in \overline{C} \setminus C$, wenn $\mathbf{p} = (\alpha:\beta:0)$ mit $(0, 0) \neq (\alpha, \beta) \in V(f_d)$, und das ist genau dann der Fall, wenn entweder $\mathbf{p} = (\alpha:1:0)$ und $f_d(\alpha, 1) = 0$, oder $\mathbf{p} = (1:\beta:0)$ und $f_d(1, \beta) = 0$. Insbesondere ist $\overline{C} \setminus C = \overline{C} \cap V_+(Z)$ endlich, denn die Polynome $f_d(X, 1)$ und $f_d(1, Y)$ haben nur endlich viele Nullstellen (andernfalls wäre $f_d(X, 1) = 0$ und daher $Y - 1 \mid f_d$, ein Widerspruch, da f_d eine Form ist; bezüglich $f_d(1, Y)$ schließt man ebenso). □

Beispiele 2.3.5.

1. Sei L eine über K definierte Gerade, $L = V(aX + bY + c)$ mit $a, b, c \in K$ und $(a, b) \neq (0, 0)$. Dann ist $\overline{L} = V_+(aX + bY + cZ) \subset \mathbb{P}_{\overline{K}}^2$, und

$$\overline{L} \setminus L = \{(u:v:0) \mid (0, 0) \neq (u, v) \in \overline{K}^2, au + bv = 0\} = \{(-b:a:0)\}.$$

Der Fernpunkt $(-b:a:0)$ von L ist durch die "Steigung" der Geraden gegeben (jede zwei parallele Geraden gehen durch denselben Fernpunkt).

2. Kreislinie. Sei $\alpha \in \overline{K}$ mit $\alpha^2 = a \in K$, $\mathbf{m} = (u_0, v_0) \in K^2$ und

$$C_{\mathbf{m},a} = \{(u, v) \in \overline{K}^2 \mid (u - u_0)^2 + (v - v_0)^2 = \alpha^2\} = V((X - u_0)^2 + (Y - v_0)^2 - a).$$

Dann ist $\overline{C}_{\mathbf{m},a} = V_+((X - u_0Z)^2 + (Y - v_0Z)^2 - aZ^2) \subset \mathbb{P}_{\overline{K}}^2$, und

$$\overline{C}_{\mathbf{m},a} \setminus C_{\mathbf{m},a} = \{(u:v:0) \mid (0,0) \neq (u,v) \in \overline{K}^2, u^2 + v^2 = 0\} = \{(1:\pm i:0)\}$$

besteht aus den beiden "absoluten Kreispunkten", die allen Kreisen gemeinsam sind.

Betrachte speziell den Einheitskreis $C_1 = C_{0,1} = \{(u, v) \in \overline{K}^2 \mid u^2 + v^2 = 1\}$ und die Abbildung

$$\bar{\tau}: \mathbb{P}_{\overline{K}}^1 \rightarrow \overline{C}_1, \quad \text{definiert durch } \tau(k:l) = (2lk : l^2 - k^2 : l^2 + k^2).$$

Sei $\tau = \bar{\tau}|_{\overline{K}}$. Es ist $\tau(k) = \bar{\tau}(k:1) = (2k : 1 - k^2 : 1 + k^2)$, und im Falle $k \neq \pm i$ folgt

$$\tau(k) = \left(\frac{2k}{1+k^2}, \frac{1-k^2}{1+k^2} \right).$$

Nach Beispiel 2 in 1.2.2 ist $\tau|_{\overline{K} \setminus \{\pm i\}} \rightarrow C_1 \setminus \{(0, -1)\}$ bijektiv. Wegen $\tau(i) = (2i:2:0) = (1:-i:0)$, $\tau(-i) = (-2i:2:0) = (1:i:0)$ und $\tau(1:0) = (0:-1:1) = (0, -1)$ ist $\bar{\tau}$ bijektiv.

2.4

Satz 2.4.1.

1. Sei $F \in K[X, Y, Z] \setminus K$ eine Form, $\Gamma = V_+(F) \subset \mathbb{P}_{\overline{K}}^2$ und $C = \Gamma \cap \overline{K}^2$. Genau dann ist $\Gamma \neq V_+(Z)$, wenn $C \neq \emptyset$; dann ist $C = V(F_*) \subset \overline{K}^2$ eine Kurve, und im Falle $V_+(Z) \not\subset \Gamma$ ist $\overline{C} = \Gamma$.
2. Ist $\Gamma \subset \mathbb{P}_{\overline{K}}^2$ eine projektive Kurve, so ist $|\Gamma| = |\mathbb{P}_{\overline{K}}^2 \setminus \Gamma| = \infty$.
3. Seien $F, G \in K[X, Y, Z] \setminus K$ teilerfremde Formen. Dann ist $|V_+(F) \cap V_+(G)| < \infty$.
4. Sei $F = F_1^{e_1} \cdots F_k^{e_k}$ mit $k \in \mathbb{N}$, paarweise nicht-assoziierten irreduziblen Formen F_1, \dots, F_k , $e_1, \dots, e_k \in \mathbb{N}$ und $F_0 = F_1 \cdots F_k$. Dann ist $V_+(F) = V_+(F_0)$, $\mathcal{J}_K^+(V_+(F)) = {}_{\kappa[X, Y, Z]}(F_0)$, und im Falle $\Gamma \neq V_+(Z)$ ist $\mathcal{J}_K(\Gamma \cap \overline{K}^2) = {}_{\kappa[X, Y]}(F_{0*})$.

BEWEIS. 1. Sei $d = \text{gr}(F) \in \mathbb{N}$. Ist $F = Z^d$, so ist $\Gamma = V_+(Z)$ und $C = \emptyset$. Ist $F \neq Z^d$, so ist $F_* = F(X, Y, 1) \in K[X, Y] \setminus K$, und $C = \Gamma \cap \overline{K}^2 = \{(x, y) \in \overline{K}^2 \mid F(x, y, 1) = 0\} = V(F_*)$ eine Kurve. Insbesondere ist dann $C \neq \emptyset$ und $\Gamma \neq V_+(Z)$. Ist $V_+(Z) \not\subset \Gamma$, so ist $Z \nmid F$, also $(F_*)^* = F$ und $\overline{C} = V_+((F_*)^*) = \Gamma$.

2. Ist $\Gamma = V_+(Z)$, so ist $\mathbb{P}_{\overline{K}}^2 \setminus \Gamma = \overline{K}^2$ unendlich, und wegen $\Gamma \supset \{(x:1:0) \mid x \in \overline{K}\}$ ist auch Γ unendlich. Ist $\Gamma \neq V_+(Z)$, so ist $C \subset \overline{K}^2$ eine Kurve, und daher sind C und $\overline{K}^2 \setminus C$ unendlich. Wegen $\Gamma \supset \overline{K}^2 \cap C$ und $\mathbb{P}_{\overline{K}}^2 \setminus \Gamma \supset \overline{K}^2 \setminus C$ folgt die Behauptung.

3. Da F und G teilerfremd sind, können wir $Z \nmid G$ annehmen. Dann ist $V_+(G) = \overline{V(G_*)}$, und $V_+(F) \cap V_+(G) = [V_+(F) \cap \overline{K}^2 \cap \overline{V(G_*)}] \cup [V_+(Z) \cap \overline{V(G_*)}]$. Nach Satz 2.3.4 ist $V_+(Z) \cap \overline{V(G_*)}$ endlich. Ist $V_+(F) = V_+(Z)$, so ist $V_+(F) \cap \overline{K}^2 = \emptyset$, und wir sind fertig. Sei also $V_+(F) \neq V_+(Z)$. Dann folgt $V_+(F) \cap \overline{K}^2 \cap \overline{V(G_*)} = V(F_*) \cap V(G_*)$, und nach Satz 1.3.3 genügt es, die Teilerfremdheit von F_* und G_* zu zeigen. Sei $f \in K[X, Y]^\bullet$, $f|F_*$ und $f|G_*$. Dann folgt $f^*|(G_*)^* = G$ und $f^*|(F_*)^*|F$, also $f^* \in K$ und daher $f \in K$.

4. Offensichtlich ist $V_+(F) = V_+(F_0)$, $F_0 \in \mathcal{J}_K^+(V_+(F))$ und ${}_{\kappa[X, Y, Z]}(F_0) \subset \mathcal{J}_K^+(V_+(F))$. Da $\mathcal{J}_K^+(V_+(F))$ von allen Formen $G \in K[X, Y, Z] \setminus K$ mit $V_+(F) \subset V_+(G)$ erzeugt wird, genügt es, zu zeigen dass alle diese Formen in ${}_{\kappa[X, Y, Z]}(F_0)$ liegen. Sei also $G \in K[X, Y, Z] \setminus K$ eine Form mit $V_+(F) \subset V_+(G)$. Es genügt, $F_i|G$ für alle $i \in [1, k]$ zu zeigen, denn wegen der paarweisen Teilerfremdheit von F_1, \dots, F_k folgt dann $F_0|G$ und $G \in {}_{\kappa[X, Y, Z]}(F_0)$. Wir nehmen im Gegenteil an, es sei $i \in [1, k]$ und $F_i \nmid G$. Dann

sind F_i und G teilerfremd, und nach 2. ist $V_+(F_i) \cap V_+(G)$ endlich. Wegen $V_+(F_i) \subset V_+(F) \subset F_+(G)$ ist das ein Widerspruch zu $|V_+(F_i)| = \infty$.

Im Falle $\Gamma \neq V_+(Z)$ ist $\Gamma \cap \overline{K}^2 = V(F_{0*})$, und da F_{0*} reduziert ist, folgt $\mathcal{J}_K(\Gamma \cap \overline{K}^2) = \kappa_{[X,Y]}(F_{0*})$. \square

Satz 2.4.2. Sei $\Gamma \subset \mathbb{P}_{\overline{K}}^2$ eine über K definierte projektive Kurve.

1. Die folgenden Aussagen sind äquivalent:
 - (a) Es gibt keine über K definierte projektive Kurve Γ_1 mit $\Gamma_1 \subsetneq \Gamma$.
 - (b) Γ ist irreduzibel über K .
 - (c) $\Gamma = V_+(F)$ mit einer (über K) irreduziblen Form $F \in K[X, Y, Z] \setminus K$.
 - (d) $\mathcal{J}_K^+(\Gamma)$ ist ein Primideal von $K[X, Y, Z]$.
 - (e) $K[\Gamma]$ ist ein Bereich.
2. Γ hat eine (bis auf die Reihenfolge der Faktoren) eindeutige Zerlegung $\Gamma = \Gamma_1 \cup \dots \cup \Gamma_k$ mit paarweise verschiedenen über K definierten irreduziblen projektiven Kurven $\Gamma_1, \dots, \Gamma_k$; diese sind Komponenten von Γ über K . Ist $V_+(Z) \notin \{\Gamma_1, \dots, \Gamma_k\}$, so sind $\Gamma_1 \cap \overline{K}^2, \dots, \Gamma_k \cap \overline{K}^2$ die Komponenten von $\Gamma \cap \overline{K}^2$ über K . Insbesondere ist Γ genau dann irreduzibel, wenn entweder $\Gamma = V_+(Z)$ oder $\Gamma \cap \overline{K}^2$ eine irreduzible Kurve ist.
3. Sei $C \subset \overline{K}^2$ eine Kurve. Sind C_1, \dots, C_k die Komponenten von C über K , so sind $\overline{C}_1, \dots, \overline{C}_k$ die Komponenten von \overline{C} über K . Insbesondere ist \overline{C} genau dann irreduzibel, wenn C irreduzibel ist.

BEWEIS. 1. (a) \Rightarrow (b) Offensichtlich.

(b) \Rightarrow (c) Sei $\mathcal{J}_K^+(\Gamma) = \kappa_{[X,Y,Z]}(F)$ mit einer reduzierten Form F . Dann ist $\Gamma = V_+(F)$, und wir nehmen an, F sei nicht irreduzibel. Dann ist $F = F_1 F_2$ mit zueinander teilerfremden reduzierten Formen $F_1, F_2 \in K[X, Y, Z] \setminus K$, also $\Gamma = V_+(F_1) \cup V_+(F_2)$ und daher $\Gamma = V_+(F_1)$ oder $\Gamma = V_+(F_2)$. Sei $\Gamma = V_+(F_1)$. Dann folgt $\kappa_{[X,Y,Z]}(F) = \mathcal{J}_K^+(\Gamma) = \kappa_{[X,Y,Z]}(F_1)$, also $F \simeq F_1$ und $F_2 \in K$, ein Widerspruch.

(c) \Rightarrow (d) Ist $\Gamma = V_+(F)$ mit einer irreduziblen Form $F \in K[X, Y, Z] \setminus K$, so ist $\mathcal{J}_K^+(\Gamma) = \kappa_{[X,Y,Z]}(F)$ ein Primideal.

(d) \Leftrightarrow (e) Es ist $K[\Gamma] \cong K[X, Y, Z]/\mathcal{J}_K^+(\Gamma)$.

(d) \Rightarrow (a) Sei Γ_1 eine über K definierte projektive Kurve mit $\Gamma_1 \subset \Gamma$. Sei $\mathcal{J}_K^+(\Gamma) = \kappa_{[X,Y,Z]}(F)$ und $\mathcal{J}_K^+(\Gamma_1) = \kappa_{[X,Y,Z]}(F_1)$ mit $F, F_1 \in K[X, Y, Z] \setminus K$. Da $\mathcal{J}_K^+(\Gamma)$ ein Primideal ist, ist F irreduzibel, und wegen $\Gamma_1 \subset V_+(F)$ ist $F \in \mathcal{J}_K^+(\Gamma_1)$, also $F_1 \mid F$. Damit folgt $F_1 \simeq F$ und $\Gamma_1 = V_+(F_1) = V_+(F) = \Gamma$.

2. Seien $\Gamma_1, \dots, \Gamma_k$ die Komponenten von Γ über K . Diese sind nach Definition paarweise verschiedene über K definierte irreduzible projektive Kurven, und es ist $\Gamma = \Gamma_1 \cup \dots \cup \Gamma_k$. Sei $\Gamma = \Gamma'_1 \cup \dots \cup \Gamma'_l$ eine weitere Zerlegung von Γ in paarweise verschiedene über K definierte irreduzible projektive Kurven, und für $i \in [1, l]$ sei $\mathcal{J}_K^+(\Gamma'_i) = \kappa_{[X,Y,Z]}(F'_i)$. Dann sind $F'_1, \dots, F'_l \in K[X, Y, Z]$ paarweise nicht-assozierte irreduzible Formen, es ist $F'_1 \dots F'_l$ reduziert und $\Gamma = V(F'_1 \dots F'_l)$, also $\mathcal{J}_K^+(\Gamma) = \kappa_{[X,Y,Z]}(F'_1 \dots F'_l)$. Damit folgt $\{\Gamma'_1, \dots, \Gamma'_l\} = \{\Gamma_1, \dots, \Gamma_k\}$.

Sei $V_+(Z) \notin \{\Gamma_1, \dots, \Gamma_k\}$ und $\mathcal{J}_K^+(\Gamma) = \kappa_{[X,Y,Z]}(F_1 \dots F_k)$ mit paarweise nicht-assozierten irreduziblen Formen $F_1, \dots, F_k \in K[X, Y, Z]$. Dann ist $Z \nmid F = F_1 \dots F_k$, also $F_* = F_{1*} \dots F_{k*}$ die Primzerlegung von F_* . Wegen $\Gamma \cap \overline{K}^2 = V(F_*)$ und $\Gamma_i \cap \overline{K}^2 = V(F_{i*})$ für alle $i \in [1, k]$ sind $\Gamma_1 \cap \overline{K}^2, \dots, \Gamma_k \cap \overline{K}^2$ die Komponenten von $\Gamma \cap \overline{K}^2$ über K .

3. Für $i \in [1, k]$ sei $\mathcal{J}_K(C_i) = \kappa_{[X,Y]}(f_i)$, und $f = f_1 \dots f_k$. Dann sind $f_1, \dots, f_k \in K[X, Y]$ paarweise nicht-assoziiert und irreduzibel, es ist $C_i = V(f_i)$, $\overline{C}_i = V_+(f_i^*)$ für alle $i \in [1, k]$ und $C = V(f)$. Es folgt $f^* = f_1^* \dots f_k^*$, die Formen $f_1^*, \dots, f_k^* \in K[X, Y, Z]$ sind paarweise nicht-assoziiert und irreduzibel, und $\overline{C} = V_+(f^*)$. Daher sind $\overline{C}_1, \dots, \overline{C}_k$ die Komponenten von \overline{C} über K . \square

Satz 2.4.3 (Schwacher Satz von Bezout). *Sind $\Gamma, \Gamma_1 \subset \mathbb{P}_K^2$ über K definierte projektive Kurven, so ist $\Gamma_1 \cap \Gamma_2 \neq \emptyset$.*

BEWEIS. Jenseits unserer Möglichkeiten. □

2.5

Definition 2.5.1. Sei $\Gamma \subset \mathbb{P}_K^2$ eine über K definierte projektive Kurve, $\mathcal{J}_K^+(\Gamma) = {}_{K[X,Y,Z]}(F)$ mit einer Form $F \in K[X, Y, Z] \setminus K$ und $\mathbf{p} \in \Gamma$. \mathbf{p} heißt *regulärer Punkt* von Γ über K , wenn

$$\left(\frac{\partial F}{\partial X}(\mathbf{p}), \frac{\partial F}{\partial Y}(\mathbf{p}), \frac{\partial F}{\partial Z}(\mathbf{p}) \right) \neq (0, 0, 0)$$

(sinnvoll, da die partiellen Ableitungen ebenfalls homogene Polynome sind). Ist $\mathbf{p} = (\alpha : \beta : \gamma) \in \Gamma$ ein regulärer Punkt, so heißt die projektive Gerade

$$\Lambda = V_+ \left(\frac{\partial F}{\partial X}(\alpha, \beta, \gamma)X + \frac{\partial F}{\partial Y}(\alpha, \beta, \gamma)Y + \frac{\partial F}{\partial Z}(\alpha, \beta, \gamma)Z \right) \subset \mathbb{P}_K^2$$

(projektive) *Tangente* von Γ im Punkte \mathbf{p} (unabhängig von der Wahl von α, β, γ ; wegen

$$\frac{\partial F}{\partial X}(\alpha, \beta, \gamma)\alpha + \frac{\partial F}{\partial Y}(\alpha, \beta, \gamma)\beta + \frac{\partial F}{\partial Z}(\alpha, \beta, \gamma)\gamma = \text{gr}(F) F(\alpha, \beta, \gamma) = 0 \quad \text{ist } \mathbf{p} \in \Lambda).$$

Γ heißt *regulär* oder *glatt*, wenn jeder Punkt von Γ regulär ist.

Satz 2.5.2. *Sei $\Gamma \subset \mathbb{P}_K^2$ eine über K definierte projektive Kurve, $C = \Gamma \cap \overline{K}^2$ und $\mathbf{p} \in C$. Genau dann ist \mathbf{p} ein regulärer Punkt von Γ über K , wenn \mathbf{p} ein regulärer Punkt von C über K ist. Ist \mathbf{p} ein regulärer Punkt von C über K und $L \subset \overline{K}^2$ die Tangente von C in \mathbf{p} , so ist $\overline{L} \subset \mathbb{P}_K^2$ die projektive Tangente von Γ in \mathbf{p} .*

BEWEIS. Sei $\mathcal{J}_K^+(\Gamma) = {}_{K[X,Y,Z]}(F)$ mit einer Form $F \in K[X, Y, Z] \setminus K$ und $\mathbf{p} = (\alpha : \beta : 1) = (\alpha, \beta) \in C$. Dann ist $\mathcal{J}_K(C) = {}_{K[X,Y]}(F_*)$, und \mathbf{p} ist genau dann ein über K regulärer Punkt von C , wenn

$$\left(\frac{\partial F}{\partial X}(\alpha, \beta, 1), \frac{\partial F}{\partial Y}(\alpha, \beta, 1) \right) = \left(\frac{\partial F_*}{\partial X}(\alpha, \beta), \frac{\partial F_*}{\partial Y}(\alpha, \beta) \right) \neq (0, 0).$$

Wegen

$$\left(X \frac{\partial F}{\partial X} + Y \frac{\partial F}{\partial Y} + Z \frac{\partial F}{\partial Z} \right)(\alpha, \beta, 1) = \text{gr}(F) F(\alpha, \beta, 1) = 0$$

ist

$$\alpha \frac{\partial F}{\partial X}(\alpha, \beta, 1) + \beta \frac{\partial F}{\partial Y}(\alpha, \beta, 1) + \frac{\partial F}{\partial Z}(\alpha, \beta, 1) = 0$$

und daher

$$\left(\frac{\partial F}{\partial X}(\mathbf{p}), \frac{\partial F}{\partial Y}(\mathbf{p}) \right) \neq (0, 0) \quad \text{genau dann, wenn} \quad \left(\frac{\partial F}{\partial X}(\mathbf{p}), \frac{\partial F}{\partial Y}(\mathbf{p}), \frac{\partial F}{\partial Z}(\mathbf{p}) \right) \neq (0, 0, 0).$$

Dann ist

$$L = V \left(\frac{\partial F_*}{\partial X}(\alpha, \beta)(X - \alpha) + \frac{\partial F_*}{\partial Y}(\alpha, \beta)(Y - \beta) \right) \subset \overline{K}^2$$

und

$$\overline{L} = V_+ \left(\frac{\partial F_*}{\partial X}(\alpha, \beta)(X - \alpha Z) + \frac{\partial F_*}{\partial Y}(\alpha, \beta)(Y - \beta Z) \right) \subset \mathbb{P}_K^2.$$

Wegen

$$\frac{\partial F_*}{\partial X}(\alpha, \beta) = \frac{\partial F}{\partial X}(\alpha, \beta, 1), \quad \frac{\partial F_*}{\partial Y}(\alpha, \beta) = \frac{\partial F}{\partial Y}(\alpha, \beta, 1)$$

und

$$\alpha \frac{\partial F}{\partial X}(\alpha, \beta, 1) + \beta \frac{\partial F}{\partial Y}(\alpha, \beta, 1) + \frac{\partial F}{\partial Z}(\alpha, \beta, 1) = 0$$

folgt

$$\frac{\partial F^*}{\partial X}(\alpha, \beta)(X - \alpha Z) + \frac{\partial F^*}{\partial Y}(\alpha, \beta)(Y - \beta Z) = \frac{\partial F}{\partial X}(\mathbf{p})X + \frac{\partial F}{\partial Y}(\mathbf{p})Y + \frac{\partial F}{\partial Z}(\mathbf{p})Z,$$

und daher ist $\bar{L} \subset \mathbb{P}_{\bar{K}}^2$ die projektive Tangente von Γ in \mathbf{p} . \square

2.6

Definition 2.6.1. Sei $\Gamma \subset \mathbb{P}_{\bar{K}}^2$ eine über K definierte irreduzible projektive Kurve. Nach Satz 2.4.2 ist dann $\mathcal{J}_K^+(\Gamma) = {}_{\kappa[X,Y,Z]}(F)$ mit einer irreduziblen Form $F \in K[X, Y, Z] \setminus K$, und der homogene Koordinatenring $K[\Gamma] = K[X, Y, Z]/{}_{\kappa[X,Y,Z]}(F)$ ist ein Bereich. $K(\Gamma)$ bestehe aus allen Elementen

$$\gamma = \frac{G + {}_{\kappa[X,Y,Z]}(F)}{H + {}_{\kappa[X,Y,Z]}(F)} \in \mathfrak{q}(K[\Gamma]) \text{ mit Formen gleichen Grades } G, H \in K[X, Y, Z] \text{ und } H \notin {}_{\kappa[X,Y,Z]}(F).$$

$K(\Gamma)$ heißt *Funktionenkörper* von Γ über K . $K(\Gamma) \subset \mathfrak{q}(K[\Gamma])$ ist ein Teilkörper (nachrechnen!).

Sind $G, G_1, H, H_1 \in K[X, Y, Z]$ Formen mit $\text{gr}(G) = \text{gr}(H)$, $\text{gr}(G_1) = \text{gr}(H_1)$ und $H, H_1 \notin (F)$, so folgt

$$\frac{G + (F)}{H + (F)} = \frac{G_1 + (F)}{H_1 + (F)} \iff GH_1 - G_1H = FQ \text{ mit einer Form } Q \in K[X, Y, Z].$$

Sei $\gamma \in K(\Gamma)$ und $\mathbf{p} = (u:v:w) \in \Gamma$. Man nennt γ *regulär* in \mathbf{p} , wenn

$$\gamma = \frac{G + (F)}{H + (F)} \in K(C) \text{ mit Formen gleichen Grades } G, H \in K[X, Y, Z] \text{ so dass } H(\mathbf{p}) \neq 0,$$

und dann nennt man den nur von γ und \mathbf{p} abhängigen Quotienten

$$\gamma(\mathbf{p}) = \frac{G(u, v, w)}{H(u, v, w)} \in \bar{K} \text{ den Wert von } \gamma \text{ an der Stelle } \mathbf{p}.$$

Für $\mathbf{p} \in \Gamma$ sei

- $\mathcal{O}_{\mathbf{p}}(\Gamma) = \mathcal{O}_{\mathbf{p},K}(\Gamma)$ die Menge der in \mathbf{p} regulären $\gamma \in K(\Gamma)$, und
- $\mathcal{M}_{\mathbf{p}}(\Gamma) = \mathcal{M}_{\mathbf{p},K}(\Gamma) = \{\gamma \in \mathcal{O}_{\mathbf{p}}(\Gamma) \mid \gamma(\mathbf{p}) = 0\}$.

Man nennt $\mathcal{O}_{\mathbf{p}}(\Gamma)$ den *lokalen Ring* und $\mathcal{M}_{\mathbf{p}}(\Gamma)$ das *maximale Ideal* von Γ in \mathbf{p} über K .

Satz 2.6.2. Sei $\Gamma \subset \mathbb{P}_{\bar{K}}^2$ eine über K definierte irreduzible projektive Kurve und $\mathbf{p} \in \Gamma$. Dann ist $\mathcal{O}_{\mathbf{p},K}(\Gamma)$ ein lokaler Bereich mit maximalem Ideal $\mathcal{M}_{\mathbf{p},K}(\Gamma)$ und $\mathfrak{q}(\mathcal{O}_{\mathbf{p},K}(\Gamma)) = K(\Gamma)$.

BEWEIS. Es genügt, die folgenden (einfachen) Behauptungen nachzurechnen:

Sind $\gamma, \gamma' \in K(\Gamma)$ in \mathbf{p} regulär, so sind auch $\gamma + \gamma'$ und $\gamma\gamma'$ in \mathbf{p} regulär, $(\gamma + \gamma')(\mathbf{p}) = \gamma(\mathbf{p}) + \gamma'(\mathbf{p})$, $(\gamma\gamma')(\mathbf{p}) = \gamma(\mathbf{p})\gamma'(\mathbf{p})$, und im Falle $\gamma(\mathbf{p}) \neq 0$ ist auch γ^{-1} in \mathbf{p} regulär. \square

Satz 2.6.3. Sei $C \subset \bar{K}^2$ eine über K definierte irreduzible Kurve und $\mathcal{J}_K(C) = {}_{\kappa[X,Y]}(f)$ mit $f \in K[X, Y] \setminus K$. Dann ist die Abbildung

$$\tau: K(\bar{C}) \rightarrow K(C), \text{ definiert durch } \tau\left(\frac{G + (f^*)}{H + (f^*)}\right) = \frac{G_* + (f)}{H_* + (f)}$$

(für Formen gleichen Grades $G, H \in K[X, Y, Z]$ mit $H \notin (f^*)$), ein K -Isomorphismus.

Sind $\hat{x}, \hat{y}, \hat{z} \in K[\bar{C}]$ die homogenen Koordinaten von \bar{C} und $x, y \in K[C]$ die Koordinatenfunktionen von C , so folgt

$$x = \tau\left(\frac{\hat{x}}{\hat{z}}\right), \quad y = \tau\left(\frac{\hat{y}}{\hat{z}}\right), \quad \text{und} \quad K[C] = \tau\left(K\left[\frac{\hat{x}}{\hat{z}}, \frac{\hat{y}}{\hat{z}}\right]\right).$$

Ist $\mathbf{p} \in C$ und $\gamma \in K(\overline{C})$, so ist γ genau dann in \mathbf{p} regulär, wenn $\tau(\gamma)$ in \mathbf{p} regulär ist, und dann ist $\gamma(\mathbf{p}) = \tau(\gamma)(\mathbf{p})$. Insbesondere ist $\tau(\mathcal{O}_{\mathbf{p}}(\overline{C})) = \mathcal{O}_{\mathbf{p}}(C)$ und $\tau(\mathcal{M}_{\mathbf{p}}(\overline{C})) = \mathcal{M}_{\mathbf{p}}(C)$.

BEWEIS. Es sind die folgenden Eigenschaften nachzurechnen:

1) Ist $H \in K[X, Y, Z]$, so ist genau dann $H \notin (f^*)$, wenn $H_* \notin (f)$. Ist $\mathbf{p} = (\alpha, \beta) = (\alpha:\beta:1)$, so ist $H(\mathbf{p}) = H_*(\mathbf{p})$.

2) Sind $G, G_1, H, H_1 \in K[X, Y, Z]$ Formen mit $\text{gr}(G) = \text{gr}(H)$ und $\text{gr}(G_1) = \text{gr}(H_1)$, so folgt

$$\frac{G + (f^*)}{H + (f^*)} = \frac{G_1 + (f^*)}{H_1 + (f^*)} \iff \frac{G_* + (f)}{H_* + (f)} = \frac{G_{1*} + (f)}{H_{1*} + (f)}$$

(damit ist τ eine injektive Abbildung).

3) τ ist ein Ringhomomorphismus.

4) Sind $g, h \in K[X, Y]$, $\text{gr}(g) = d \in \mathbb{N}_0$, $\text{gr}(h) = e \in \mathbb{N}_0$ und $h \notin (f)$, so folgt

$$\frac{g + (f)}{h + (f)} = \tau\left(\frac{Z^e g^* + (f^*)}{Z^d h^* + (f^*)}\right). \quad \square$$

Definition und Bemerkung 2.6.4. Seien $\iota_1, \iota_2, \iota_3: \overline{K}^2 \rightarrow \mathbb{P}_{\overline{K}}^2$ die Einbettungen von \overline{K}^2 in die affinen Stücke von $\mathbb{P}_{\overline{K}}^2$, definiert durch

$$\iota_1(\beta, \gamma) = (1:\beta:\gamma) \in \mathbb{P}_{\overline{K}}^2(1), \quad \iota_2(\alpha, \gamma) = (\alpha:1:\gamma) \in \mathbb{P}_{\overline{K}}^2(2) \quad \text{und} \quad \iota_3(\alpha, \beta) = (\alpha:\beta:1) \in \mathbb{P}_{\overline{K}}^2(3).$$

Sei $\Gamma \subset \mathbb{P}_{\overline{K}}^2$ eine über K definierte projektive Kurve, $V_+(X) \not\subset \Gamma$, $V_+(Y) \not\subset \Gamma$, $V_+(Z) \not\subset \Gamma$, und sei $J_K^+(\Gamma) = \kappa_{[X,Y,Z]}(F)$ mit einer Form $F \in K[X, Y, Z] \setminus K$ (also $X \nmid F$, $Y \nmid F$ und $Z \nmid F$). Für $\nu \in \{1, 2, 3\}$ ist $C_\nu = \iota_\nu^{-1}(\Gamma) \subset \overline{K}^2$ eine über K definierte Kurve, und $\Gamma = \iota_1(C_1) \cup \iota_2(C_2) \cup \iota_3(C_3)$. Identifiziert man \overline{K}^2 mit dem affinen Stück $\mathbb{P}_{\overline{K}}^2(\nu)$ vermöge ι_ν , so ist $C_\nu = \Gamma \cap \overline{K}^2$, und Γ ist der projektive Abschluss von C_ν . Wir nennen die Kurven $C_1, C_2, C_3 \subset \overline{K}^2$ (oder auch ihre Bilder $\iota_1(C_1), \iota_2(C_2), \iota_3(C_3)$, mit denen wir sie identifizieren) die *affinen Stücke* von Γ .

Explizit: $J_K(C_1) = \kappa_{[Y,Z]}(F(1, Y, Z))$, $J_K(C_2) = \kappa_{[X,Z]}(F(X, 1, Z))$, $J_K(C_3) = \kappa_{[X,Y]}(F(X, Y, 1))$.

Sei nun Γ irreduzibel. Für alle $\nu \in \{1, 2, 3\}$ ist dann auch C_ν irreduzibel, und nach Satz 2.6.3 erhalten wir Isomorphismen $\tau_\nu: K(\Gamma) \rightarrow K(C_\nu)$ wie folgt: Ist

$$\gamma = \frac{G + \kappa_{[X,Y,Z]}(F)}{H + \kappa_{[X,Y,Z]}(F)} \in K(\Gamma) \quad \text{mit Formen gleichen Grades } G, H \in K[X, Y, Z] \text{ mit } H \notin \kappa_{[X,Y,Z]}(F),$$

$$\text{so ist} \quad \tau_1(\gamma) = \frac{G(1, Y, Z) + \kappa_{[Y,Z]}(F(1, Y, Z))}{H(1, Y, Z) + \kappa_{[Y,Z]}(F(1, Y, Z))}, \quad \tau_2(\gamma) = \frac{G(X, 1, Z) + \kappa_{[X,Z]}(F(X, 1, Z))}{H(X, 1, Z) + \kappa_{[X,Z]}(F(X, 1, Z))}$$

$$\text{und} \quad \tau_3(\gamma) = \frac{G(X, Y, 1) + \kappa_{[X,Y]}(F(X, Y, 1))}{H(X, Y, 1) + \kappa_{[X,Y]}(F(X, Y, 1))}.$$

Identifiziert man $K(\Gamma)$ und $K(C_\nu)$ vermöge τ_ν , so ist $K[C_\nu] \subset K(\Gamma)$ ein Teilbereich. Sind $\hat{x}, \hat{y}, \hat{z}$ die homogenen Koordinaten von Γ , so folgt

$$K[C_1] = K\left[\frac{\hat{y}}{\hat{x}}, \frac{\hat{z}}{\hat{x}}\right], \quad K[C_2] = K\left[\frac{\hat{x}}{\hat{y}}, \frac{\hat{z}}{\hat{y}}\right] \quad \text{und} \quad K[C_3] = K\left[\frac{\hat{x}}{\hat{z}}, \frac{\hat{y}}{\hat{z}}\right].$$

Wir betrachten abschließend noch den Spezialfall $\Gamma = V_+(Z)$. Dann ist $K[\Gamma] = K[\hat{x}, \hat{y}]$, $\iota_3^{-1}(\Gamma) = \emptyset$, $C_1 = \iota_1^{-1}(\Gamma) = V(Z) \subset \overline{K}^2$ (wobei $Z \in K[Y, Z]$), und $C_2 = \iota_2^{-1}(\Gamma) = V(Z) \subset \overline{K}^2$ (wobei $Z \in K[X, Z]$). In $K(\Gamma)$ ist

$$K[C_1] = K\left[\frac{\hat{y}}{\hat{x}}\right] \quad \text{und} \quad K[C_2] = K\left[\frac{\hat{x}}{\hat{y}}\right].$$

Auch in diesem Falle nennt man die Geraden $C_1, C_2 \subset \overline{K}^2$ (oder auch ihre Bilder $\iota_1(C_1)$ und $\iota_2(C_2)$, mit denen wir sie identifizieren) die *affinen Stücke* von Γ .

2.7

Definitionen und Bemerkungen 2.7.1 (Projektive Koordinatentransformationen).

1. Für $A \in \mathrm{GL}_3(K)$ sei $\theta_A: \mathbb{P}_K^2 \rightarrow \mathbb{P}_K^2$ wie folgt definiert:

Ist $(\alpha, \beta, \gamma) \in \overline{K}^3 \setminus \{\mathbf{0}\}$ und $\mathbf{p} = (\alpha: \beta: \gamma) \in \mathbb{P}_K^2$, so ist $(\alpha', \beta', \gamma') = (\alpha, \beta, \gamma)A \in \overline{K}^3 \setminus \{\mathbf{0}\}$, $\mathbf{p}' = (\alpha': \beta': \gamma') \in \mathbb{P}_K^2$ hängt nur von $\mathbf{p} = (\alpha: \beta: \gamma)$ ab, und wir setzen $\theta_A(\mathbf{p}) = \mathbf{p}'$.

$\theta_A: \mathbb{P}_K^2 \rightarrow \mathbb{P}_K^2$ ist bijektiv, $\theta_A^{-1} = \theta_{A^{-1}}$, und für $A, B \in \mathrm{GL}_3(K)$ ist $\theta_{AB} = \theta_B \circ \theta_A$.

Eine Abbildung $\theta: \mathbb{P}_K^2 \rightarrow \mathbb{P}_K^2$ heißt eine über K definierte *projektive Koordinatentransformation*, wenn $\theta = \theta_A$ mit einer Matrix $A \in \mathrm{GL}_3(K)$.

2. Für $A \in \mathrm{GL}_3(K)$ sei $\theta_A^*: K[X, Y, Z] \rightarrow K[X, Y, Z]$ der eineutig bestimmt K -Algebrenhomomorphismus mit $(\theta_A^*(X), \theta_A^*(Y), \theta_A^*(Z)) = (X, Y, Z)A^{-1} \in K[X, Y, Z]^3$.

Explizit: Ist $F \in K[X, Y, Z]$ und

$$A^{-1} = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix},$$

so folgt

$$(\theta_A^*F)(X, Y, Z) = F((X, Y, Z)A^{-1}) = F(a_1X + b_1Y + c_1Z, a_2X + b_2Y + c_2Z, a_3X + b_3Y + c_3Z).$$

$\theta_A^*: K[X, Y, Z] \rightarrow K[X, Y, Z]$ ist ein Isomorphismus, $\theta_A^{*-1} = \theta_{A^{-1}}$, und für $A, B \in \mathrm{GL}_3(K)$ ist $\theta_{AB}^* = \theta_A^* \circ \theta_B^*$.

3. Sei $A \in \mathrm{GL}_3(K)$ und $F \in K[X, Y, Z] \setminus K$ eine Form vom Grade $d \in \mathbb{N}$. Dann ist auch $\theta_A^*(F)$ eine Form vom Grade d , und für $\mathbf{p} \in \mathbb{P}_K^2$ gilt:

$$(\theta_A^*F)(\theta_A(\mathbf{p})) = 0 \iff F(\mathbf{p}) = 0.$$

Insbesondere ist $V_+(\theta_A^*F) = \theta_A(V_+(F))$.

Beweis. Für $\mathbf{p} = (\alpha: \beta: \gamma) \in \mathbb{P}_K^2$ gilt:

$$(\theta_A^*F)(\theta_A(\mathbf{p})) = 0 \iff 0 = (\theta_A^*F)((\alpha, \beta, \gamma)A) = F((\alpha, \beta, \gamma)AA^{-1}) \iff F(\mathbf{p}) = 0$$

und

$$\begin{aligned} \mathbf{p} \in V_+(\theta_A^*(F)) &\iff (\theta_A^*F)(\mathbf{p}) = 0 \iff F(\theta_A^{-1}(\mathbf{p})) = 0 \\ &\iff \theta_{A^{-1}}(\mathbf{p}) \in V_+(F) \iff \mathbf{p} \in \theta_A(V_+(F)). \quad \square \end{aligned}$$

4. Sei $\Gamma \subset \mathbb{P}_K^2$ eine über K definierte projektive Kurve. Dann ist $\theta_A^*(\mathcal{J}_K^+(\Gamma)) = \mathcal{J}_K^+(\theta_A(\Gamma))$.

Beweis. Für eine Form $F \in K[X, Y, Z] \setminus K$ gilt:

$$\begin{aligned} F \in \mathcal{J}_K^+(\theta_A(\Gamma)) &\iff (\forall \mathbf{p} \in \Gamma) F(\theta_A(\mathbf{p})) = 0 \iff (\forall \mathbf{p} \in \Gamma) (\theta_A^{*-1}F)(\mathbf{p}) = 0 \\ &\iff \theta_A^{*-1}(F) \in \mathcal{J}_K^+(\Gamma) \iff F \in \theta_A^*(\mathcal{J}_K^+(\Gamma)). \quad \square \end{aligned}$$

Insbesondere induziert θ_A^* einen Isomorphismus

$$\theta_A^*: K[\Gamma] = K[X, Y, Z]/\mathcal{J}_K^+(\Gamma) \rightarrow K[X, Y, Z]/\mathcal{J}_K^+(\theta_A(\Gamma)) = K[\theta(\Gamma)].$$

Ist insbesondere Γ irreduzibel über K und $\mathcal{J}_K^+(\Gamma) = K[X, Y, Z](F)$ mit einer irreduziblen Form $F \in K[X, Y, Z] \setminus K$, so induziert θ_A^* auch einen Isomorphismus $\theta_A^*: K(\Gamma) \rightarrow K(\theta(\Gamma))$. Explizit:

$$\text{Ist } \gamma = \frac{G + (F)}{H + (F)}, \text{ so folgt } \theta_A^*(\gamma) = \frac{\theta_A^*(G) + (\theta_A^*(F))}{\theta_A^*(H) + (\theta_A^*(F))}.$$

Ist $\gamma \in K(\Gamma)$ und $\mathbf{p} \in \Gamma$, so ist γ genau dann in \mathbf{p} regulär, wenn $\theta_A^*(\gamma)$ in $\theta_A(\mathbf{p})$ regulär ist, und dann ist $\gamma(\mathbf{p}) = \theta_A^*(\gamma)(\theta_A(\mathbf{p}))$. Daher induziert θ_A^* auch einen Isomorphismus

$$\theta_A^* | \mathcal{O}_{\mathbf{p},K}(\Gamma): \mathcal{O}_{\mathbf{p},K}(\Gamma) \rightarrow \mathcal{O}_{\theta_A(\mathbf{p}),K}(\Gamma).$$

Satz 2.7.2.

1. Seien $H_1, H_2, H_3 \subset \mathbb{P}_{\overline{K}}^2$ drei über K definierte projektive Geraden mit $H_1 \cap H_2 \cap H_3 = \emptyset$. Dann gibt es eine über K definierte projektive Koordinatentransformation $\theta: \mathbb{P}_{\overline{K}}^2 \rightarrow \mathbb{P}_{\overline{K}}^2$, so dass $\theta(H_1) = V_+(X)$, $\theta(H_2) = V_+(Y)$ und $\theta(H_3) = V_+(Z)$, und insbesondere $\theta(\mathbb{P}_{\overline{K}}^2 \setminus H_i) = \mathbb{P}_{\overline{K}}^2(i)$ für alle $i \in \{1, 2, 3\}$.
2. Seien $\mathbf{p}, \mathbf{p}' \in \mathbb{P}_{\overline{K}}^2$. Dann gibt es eine über K definierte projektive Koordinatentransformation $\theta: \mathbb{P}_{\overline{K}}^2 \rightarrow \mathbb{P}_{\overline{K}}^2$, so dass $\{\theta(\mathbf{p}), \theta(\mathbf{p}')\} \subset \mathbb{P}_{\overline{K}}^2(3)$.

BEWEIS. 1. Für $i \in \{1, 2, 3\}$ sei $H_i = V_+(a_i X + b_i Y + c_i Z)$ mit $(a_i, b_i, c_i) \in K^3 \setminus \{\mathbf{0}\}$. Wegen $H_1 \cap H_2 \cap H_3 = \emptyset$ ist

$$A = \begin{pmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{pmatrix} \in \mathrm{GL}_3(K),$$

und wir betrachten $\theta = \theta_A: \mathbb{P}_{\overline{K}}^2 \rightarrow \mathbb{P}_{\overline{K}}^2$. Für $i \in \{1, 2, 3\}$ ist $\theta_A(H_i) = V_+(\theta_A^*(H_i))$, und

$$\theta_A^*(H_i) = (\theta_A^* H_i)(X, Y, Z) = H_i((X, Y, Z)A^{-1}) = (X, Y, Z) A^{-1} \begin{pmatrix} a_i \\ b_i \\ c_i \end{pmatrix},$$

also $(\theta_A^*(H_1), \theta_A^*(H_2), \theta_A^*(H_3)) = (X, Y, Z)$.

2. Sei $\mathbf{p} = (\alpha:\beta:\gamma)$ und $\mathbf{p}' = (\alpha':\beta':\gamma')$. Wir zeigen zuerst:

Es gibt ein Tripel $(a, b, c) \in K^3 \setminus \{\mathbf{0}\}$, so dass $a\alpha + b\beta + c\gamma \neq 0$ und $a\alpha' + b\beta' + c\gamma' \neq 0$ (also $V_+(aX + bY + cZ) \cap \{\mathbf{p}, \mathbf{p}'\} = \emptyset$).

Wir können $\alpha \neq 0$ annehmen. Ist dann auch $\alpha' \neq 0$, so leistet $(a, b, c) = (1, 0, 0)$ das Gewünschte. Ist $\alpha' = 0$, so ist $(\beta', \gamma') \neq (0, 0)$, und wir können $\beta' \neq 0$ annehmen. Im Falle $\beta \neq 0$ setzen wir $(a, b, c) = (0, 1, 0)$, und im Falle $\beta = 0$ setzen wir $(a, b, c) = (1, 1, 0)$.

Sei nun $(a, b, c) \in K^3 \setminus \{\mathbf{0}\}$ mit $V_+(aX + bY + cZ) \cap \{\mathbf{p}, \mathbf{p}'\} = \emptyset$. Seien $a', b', c', a'', b'', c'' \in K$, so dass

$$\begin{pmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{pmatrix} \in \mathrm{GL}_3(K).$$

Dann ist $V_+(aX + bY + cZ) \cap V_+(a'X + b'Y + c'Z) \cap V_+(a''X + b''Y + c''Z) = \emptyset$. Nach 1. gibt es eine über K definierte projektive Koordinatentransformation $\theta: \mathbb{P}_{\overline{K}}^2 \rightarrow \mathbb{P}_{\overline{K}}^2$, so dass $\theta(V_+(aX + bY + cZ)) = V_+(Z)$, und dann ist $\{\theta(\mathbf{p}), \theta(\mathbf{p}')\} \subset \mathbb{P}_{\overline{K}}^2(3)$. \square

Algebraische Funktionenkörper und diskrete Bewertungen

3.1

Definition 3.1.1. Eine Körpererweiterung L/K heißt (*algebraischer*) *Funktionenkörper* (*in einer Variablen*), wenn es ein über K transzendentes $x \in L$ gibt, so dass $[L:K(x)] < \infty$. Man sagt dann auch, L ist ein *Funktionenkörper über K* und nennt den relativen algebraischen Abschluss $\tilde{K} = \overline{K}_L$ aller über K algebraischen Elemente von L den *Konstantenkörper* von L/K .

Ist $x \in L$ transzendent über K , so ist x auch transzendent über \tilde{K} , und $[L:\tilde{K}(x)] \leq [L:K(x)]$. Daher ist L auch ein Funktionenkörper über \tilde{K} .

Ist $L = K(x)$ mit einem über K transzendenten x (also $L \cong K(X)$), so nennt man L eine *rationalen Funktionenkörper* über K .

Beispiel 3.1.2. Sei K ein Körper, \overline{K} eine algebraische Hülle von K und $C \subset \overline{K}$ eine über K definierte irreduzible Kurve. Dann ist $K(C) = K(x, y)$ nach Satz 1.7.2 ein Funktionenkörper über K .

Ist C absolut irreduzibel, so ist K der Konstantenkörper von $K(C)/K$.

Beweis: Sei C absolut irreduzibel und $f \in K[X, Y]$ ein Minimalpolynom von C . Dann ist C irreduzibel über \overline{K} und daher auch über jedem über K algebraischen Oberkörper $K_1 \supset K$. Seien $x, y \in K[C]$ die Koordinatenfunktionen und sei o. E. x transzendent über K . Sei \tilde{K} der Konstantenkörper von $K(C)/K$. Dann ist x auch transzendent über \tilde{K} , $K(C) = K(x, y) = \tilde{K}(x, y)$, und $f(x, y) = 0$. Sei $c \in K(x)^\times$ der führende Koeffizient von $f(x, Y) \in \tilde{K}[x, Y]$. Wegen $K[x, Y] \cong K[X, Y]$ ist $f(x, Y) \in K[x, Y]$ irreduzibel, also auch in $K(x)[Y]$, und daher ist $c^{-1}f \in K(x)[Y]$ das Minimalpolynom von y über $K(x)$. Aus dem selben Grund ist aber $c^{-1}f$ auch das Minimalpolynom von y über $\tilde{K}(x)$, und daher folgt $[K(x, y):\tilde{K}(x)] = [K(x, y):K(x)] = [K(x, y):\tilde{K}(x)][\tilde{K}(x):K(x)]$, also $[\tilde{K}:K] = [\tilde{K}(x):K(x)] = 1$ und daher $\tilde{K} = K$. \square

In obigem Beweis ist die absolute Irreduzibilität von f notwendig. Sei $K = \mathbb{R}$ und $C = V(X^2 + Y^2)$. Dann ist $C \subset \mathbb{C}^2$ eine über \mathbb{R} irreduzible Kurve, aber nicht absolut irreduzibel. Sind $x, y \in \mathbb{R}(C)$ die Koordinatenfunktionen von C , so ist $\mathbb{R}(C) = \mathbb{R}(x, y)$, $x^2 + y^2 = 0$, $x^{-1}y \in \mathbb{R}(C)$, und wegen $1 + (x^{-1}y)^2 = 0$ ist $x^{-1}y \notin \mathbb{R}$, aber algebraisch über \mathbb{R} .

Satz 3.1.3. Sei L/K ein Funktionenkörper, $x \in L$ transzendent über K , $[L:L(x)] < \infty$ und $y \in L$ mit $L = K(x, y)$. Dann gibt es ein bis auf Faktoren aus K^\times eindeutig bestimmtes irreduzibles Polynom $f \in K[X, Y] \setminus K$ mit $f(x, y) = 0$. Sei \overline{K} eine algebraische Hülle von K , $C = V(f) \subset \overline{K}^2$, und seien $x_C, y_C \in K(C)$ die Koordinatenfunktionen von C . Dann gibt es genau einen K -Isomorphismus $\Phi: L \rightarrow K(C)$ mit $\Phi(x) = x_C$ und $\Phi(y) = y_C$.

BEWEIS. Existenz und Eindeutigkeit von f : Es genügt, zu zeigen: $J = \{g \in K[X, Y] \mid g(x, y) = 0\}$ ist ein von einem irreduziblen Polynom erzeugtes Hauptideal von $K[X, Y]$. Da y über $K(x)$ algebraisch ist, gibt es ein $g_0 \in K(x)[Y]^\bullet$ mit $g_0(y) = 0$, und nach Hochmultiplizieren der Nenner kann man $g_0 \in K[x, Y]$ annehmen. Daher gibt es ein $g \in K[X, Y]^\bullet$ mit $g(x, Y) = g_0$. Es ist dann $g(x, y) = 0$, also auch

$f(x, y) = 0$ für ein irreduzibles Polynom $f \in K[X, Y]$ mit $f \mid g$. Daher ist $f \in J$, also $(f) \subset J$ und wir zeigen $J = (f)$.

Wir nehmen an, es gebe ein Polynom $g \in J \setminus (f)$. Sei $R = K[X]$. Dann sind g und f teilerfremd in $R[Y]$, und daher gibt es Polynome $p, q \in R[Y] = K[X, Y]$ mit $pf + qg = r \in R^\bullet = K[X]^\bullet$. Damit folgt $p(x, y)f(x, y) + q(x, y)g(x, y) = r(x) = 0$, ein Widerspruch zur Transzendenz von x .

Wegen $K[x, y] \cong K[X, Y]/(f) \cong K[x_C, y_C] = K[C]$ gibt es einen Isomorphismus $\Phi_0: K[x, y] \rightarrow K[C]$ mit $\Phi_0 \mid K = \text{id}K$, $\Phi_0(x) = x_C$ und $\Phi_0(y) = y_C$. Die Fortsetzung von Φ_0 auf die Quotientenkörper leistet das Gewünschte. Die Eindeutigkeit ist offensichtlich. \square

3.2

Satz 3.2.1. *Sei L/K ein Funktionenkörper. Ist $x_1 \in L$ transzendent über K , so ist $[L:K(x_1)] < \infty$.*

BEWEIS. Sei $x \in L$ transzendent über K mit $[L:K(x)] < \infty$. Dann ist x_1 algebraisch über $K(x)$, und es sei $f \in K(x)[X_1]^\bullet$ mit $f(x_1) = 0$. Nach Hochmultiplizieren der Nenner erhalten wir ein Polynom $F \in K[X, X_1]$ mit $F(x, x_1) = 0$. Sei

$$F = \sum_{\nu \geq 0} a_\nu(X_1)X^\nu \quad \text{mit} \quad a_\nu(X_1) \in K[X_1], \quad a_\nu(X_1) = 0 \quad \text{für fast alle } \nu \geq 0$$

Wegen $F \neq 0$ gibt es ein $\nu \geq 0$ mit $a_\nu(X_1) \neq 0$. Da x_1 über K transzendent ist, folgt $a_\nu(x_1) \neq 0$, also $F(x_1, X) \in K[X_1]^\bullet$ und $F(x_1, x) = 0$. Daher ist x algebraisch über $K(x_1)$, und

$$[L:K(x_1)] = [L:K(x_1, x)] [K(x_1, x):K(x_1)] \leq [L:K(x)] [K(x_1)(x):K(x_1)] < \infty. \quad \square$$

3.3

Definition 3.3.1. Sei L ein Körper und $\mathcal{O} \subsetneq L$ ein Teilring mit $L = \mathfrak{q}(\mathcal{O})$.

1. \mathcal{O} heißt *Bewertungsbereich* (von L), wenn gilt: Für alle $x \in L \setminus \mathcal{O}$ ist $x^{-1} \in \mathcal{O}$.
2. \mathcal{O} heißt *diskreter Bewertungsbereich* (von L), wenn \mathcal{O} faktoriell ist bis auf Assoziierte genau ein Primelement t besitzt (dann hat jedes $z \in L^\times$ eine eindeutige Darstellung $z = t^n u$ mit $n \in \mathbb{Z}$ und $u \in \mathcal{O}^\times$; insbesondere ist entweder $z \in \mathcal{O}$ (falls $n \geq 0$) oder $z^{-1} \in \mathcal{O}$ (falls $n < 0$), und daher ist \mathcal{O} ein Bewertungsbereich.

Satz 3.3.2. *Sei L ein Körper und $\mathcal{O} \subsetneq L$ ein Teilring mit $L = \mathfrak{q}(\mathcal{O})$.*

1. *Ist \mathcal{O} ein Bewertungsbereich, so ist \mathcal{O} lokal und $P = \mathcal{O} \setminus \mathcal{O}^\times = \{x^{-1} \mid x \in L \setminus \mathcal{O}\} \cup \{0\}$ sein maximales Ideal.*
2. *Sei \mathcal{O} ein diskreter Bewertungsbereich und $t \in \mathcal{O}$ ein Primelement.*
 - (a) *\mathcal{O} ist ein Hauptidealbereich, und $\{(t^n) \mid n \in \mathbb{N}\}$ ist die Menge aller von $\{0\}$ verschiedenen echten Ideale von \mathcal{O} . Insbesondere ist $(t) = \mathcal{O} \setminus \mathcal{O}^\times$ das maximale Ideal von \mathcal{O} .*
 - (b) *$\mathcal{O} \subsetneq L$ ist ein maximaler Teilring.*

BEWEIS. 1. Definitionsgemäß ist $\mathcal{O} \setminus \mathcal{O}^\times \supset \{x^{-1} \mid x \in L \setminus \mathcal{O}\} \cup \{0\}$. Ist umgekehrt $z \in \mathcal{O} \setminus \mathcal{O}^\times$ und $z \neq 0$, so ist $x = z^{-1} \in L \setminus \mathcal{O}$ und $z = x^{-1}$. Es bleibt also zu zeigen, dass $\mathcal{O} \setminus \mathcal{O}^\times$ ein Ideal von \mathcal{O} ist. Ist $a \in \mathcal{O} \setminus \mathcal{O}^\times$ und $r \in \mathcal{O}$, so ist auch $ra \in \mathcal{O} \setminus \mathcal{O}^\times$. Seien nun $a, b \in \mathcal{O} \setminus \mathcal{O}^\times$. Wir müssen $a + b \in \mathcal{O} \setminus \mathcal{O}^\times$ zeigen und können dafür $ab \neq 0$ annehmen. Dann ist $a^{-1}b \in \mathcal{O}$ oder $ab^{-1} \in \mathcal{O}$. Sei etwa $ab^{-1} \in \mathcal{O}$. Dann ist $a + b = b(ab^{-1} + 1) \in \mathcal{O} \setminus \mathcal{O}^\times$.

2. (a) Sei $\{0\} \neq I \triangleleft \mathcal{O}$. Ist $0 \neq a \in I$, so gibt es ein $m \in \mathbb{N}$ und ein $u \in \mathcal{O}^\times$ mit $a = t^m u$, also $t^m = u^{-1}a \in I$, und daher existiert $n = \min\{m \in \mathbb{N} \mid t^m \in I\}$. Es ist $(t^n) \subset I$, und wir behaupten Gleichheit. Sei $0 \neq a \in I$, $a = t^m u$ mit $m \in \mathbb{N}$ und $u \in \mathcal{O}^\times$. Dann ist $t^m = u^{-1}a \in I$, also $m \geq n$, und $a = t^n t^{m-n} u \in (t^n)$.

2. (b) Sei $\mathcal{O} \subsetneq \mathcal{O}' \subset L$ ein Teilring und $x \in \mathcal{O}' \setminus \mathcal{O}$. Dann ist $x = t^{-n}u$ mit $n \in \mathbb{N}$ und $u \in \mathcal{O}^\times$, also $t^{-1} = t^{n-1}u^{-1}x \in \mathcal{O}'$, und ist folgt $L = \mathcal{O}[t^{-1}] \subset \mathcal{O}'$, also $\mathcal{O}' = L$. \square

Satz 3.3.3 (Existenzsatz für Bewertungsbereiche). *Sei L ein Körper, $R \subsetneq L$ ein Teilbereich und $\{0\} \neq I \subsetneq R$ ein Ideal. Dann gibt es einen Bewertungsbereich \mathcal{O} von L mit maximalem Ideal $P = \mathcal{O} \setminus \mathcal{O}^\times$, so dass $R \subset \mathcal{O}$ und $I \subset P$.*

BEWEIS. Sei Ω die Menge aller Bereiche S mit $R \subset S \subset L$, so dass $S I \neq S$. Dann ist $R \in \Omega$, also $\Omega \neq \emptyset$, und wir zeigen mit Hilfe des Zorn'schen Lemmas, dass Ω ein maximales Element besitzt. Sei $(S_\lambda)_{\lambda \in \Lambda}$ eine Kette in Ω und $S = \bigcup_{\lambda \in \Lambda} S_\lambda$. Dann ist $S \subset L$ ein Teilring. Wäre $S = S I$, so folgte $1 = s_1 a_1 + \dots + s_r a_r$ mit $a_1, \dots, a_r \in I$ und $s_1, \dots, s_r \in S$. Da $(S_\lambda)_{\lambda \in \Lambda}$ eine Kette ist, gibt es ein $\nu \in \Lambda$ mit $\{s_1, \dots, s_r\} \subset S_\nu$, also $1 \in S_\nu(I)$, ein Widerspruch. Wegen $I \neq \{0\}$ ist $S \neq L$, also $S \in \Omega$.

Sei nun $\mathcal{O} \in \Omega$ maximal und $J = \mathcal{O}(I)$. Wegen $\{0\} \subsetneq J \subsetneq \mathcal{O}$ ist $\mathcal{O} \neq L$, und wir zeigen, dass \mathcal{O} ein Bewertungsbereich von L ist. Wir nehmen im Gegenteil an, es sei $z \in L^\times$ mit $z \notin \mathcal{O}$ und $z^{-1} \notin \mathcal{O}$. Dann ist $\mathcal{O} \subsetneq \mathcal{O}[z]$ und $\mathcal{O} \subsetneq \mathcal{O}[z^{-1}]$, und wegen der Maximalität von \mathcal{O} ist $\mathcal{O}_{[z]}(I) = \mathcal{O}_{[z]}(J) = \mathcal{O}[z]$ und $\mathcal{O}_{[z^{-1}]}(J) = \mathcal{O}[z^{-1}]$. Dann bestehen Gleichungen der Form

$$1 = \sum_{i=0}^n a_i z^i \quad \text{und} \quad 1 = \sum_{j=0}^m b_j (z^{-1})^j \quad \text{mit} \quad n, m \in \mathbb{N} \quad \text{und} \quad a_0, \dots, a_n, b_0, \dots, b_m \in J.$$

Wir nehmen an, m und n seien minimal mit dieser Eigenschaft, und es sei $m \leq n$ (Symmetrie von z und z^{-1}). Dann folgt

$$1 - b_0 = \sum_{i=0}^n (1 - b_0) a_i z^i \quad \text{und} \quad a_n z^n = \sum_{j=0}^m b_j a_n z^{n-j}, \quad \text{also} \quad (1 - b_0) a_n z^n = \sum_{j=1}^m a_n b_j z^{n-j},$$

und wir erhalten

$$1 = b_0 + (1 - b_0) a_0 + \sum_{i=1}^{n-1} (1 - b_0) a_i z^i + \sum_{j=1}^m a_n b_j z^{n-j} = \sum_{\nu=0}^{n-1} c_\nu z^\nu \quad \text{mit} \quad c_0, \dots, c_{n-1} \in J,$$

ein Widerspruch zur Minimalität von n . \square

3.4

Satz 3.4.1. *Sei L/K ein Funktionenkörper mit Konstantenkörper \tilde{K} und \mathcal{O} ein Bewertungsbereich von L mit maximalem Ideal P und $K \subset \mathcal{O}$.*

1. *Es ist $\tilde{K} \subset \mathcal{O}$ und $\tilde{K}^\times \subset \mathcal{O}^\times$.*
2. *Sei $n \in \mathbb{N}$, und seien $x_1, \dots, x_n \in P \setminus \{0\}$, so dass $x_i \in x_{i+1}P$ für alle $i \in [1, n-1]$. Dann ist $n \leq [L:K(x_1)] < \infty$. Insbesondere ist jedes $x \in P \setminus \{0\}$ transzendent über K .*
3. *\mathcal{O} ist ein diskreter Bewertungsbereich.*

PROOF. 1. Es genügt, $\tilde{K} \subset \mathcal{O}$ zu zeigen, und wir nehmen an, es sei $a \in \tilde{K} \setminus \mathcal{O}$. Dann folgt $a^{-1} \in \mathcal{O}$, also $K[a^{-1}] \subset \mathcal{O}$, und da a über K algebraisch ist, folgt $a \in K[a^{-1}] \subset \mathcal{O}$, ein Widerspruch.

2. Wegen $x_1 \in P \setminus \{0\}$ ist $x_1^{-1} \notin \mathcal{O}$, also $x_1^{-1} \notin \tilde{K}$. Daher ist x_1^{-1} und damit auch x_1 transzendent über K und $[L:K(x_1)] < \infty$ nach Satz 3.2.1.

Wegen $x_i \in x_{i+1}P$ für alle $i \in [1, n-1]$ ist $x_i \in x_j P$ für alle $i, j \in [1, n]$ mit $i < j$, und wir zeigen die lineare Unabhängigkeit von x_1, \dots, x_n über $K(x_1)$ (man beachte $K(x_1) \cong K[X]$). Wir nehmen im Gegenteil an, es bestehe eine Relation

$$\sum_{i=1}^n \varphi_i x_i \quad \text{mit} \quad \varphi_1, \dots, \varphi_n \in K(x_1) \quad \text{und} \quad (\varphi_1, \dots, \varphi_n) \neq (0, \dots, 0).$$

Wir können annehmen, dass $\varphi_1, \dots, \varphi_n \in K[x_1]$, und dass es ein $k \in [1, n]$ gibt, so dass $\varphi_k \notin x_1 K[x_1]$ und $\varphi_i \in x_1 K[x_1]$ für alle $i \in [k+1, n]$. Dann folgt

$$-\varphi_k = \sum_{i=1}^{k-1} \varphi_i x_k^{-1} x_i + \sum_{i=k+1}^n \varphi_i x_k^{-1} x_i.$$

Für $i \in [1, k-1]$ ist $x_i \in x_k P$, also $\varphi_i x_k^{-1} x_i \in K[x_1]P \subset \mathcal{O}P = P$. Für $i \in [k+1, n]$ ist $\varphi_i = x\psi_i$ mit $\psi_i \in K[x_1] \subset \mathcal{O}$, und $\varphi_i x_k^{-1} x_i = \psi_i x_i x_k^{-1} x_i \in P$. Daher ist $\varphi_k \in P$. Aber $\varphi_k = a + x_1\psi$ mit $a \in K^\times$ und $\psi \in K[x_1]$, und daher folgt $a = \varphi_k - x_1\psi \in P \cap K^\times$, ein Widerspruch.

3. Sei $(x_i)_{i \geq 1}$ eine Folge in $P \setminus \{0\}$, so dass für alle $i \geq 1$ gilt:

$$(x_1, \dots, x_i) \subsetneq (x_1, \dots, x_{i+1}), \quad \text{falls } (x_1, \dots, x_i) \subsetneq P, \quad \text{und } x_{i+1} = x_i \text{ sonst.}$$

Sei $n \in \mathbb{N}$, so dass $(x_1, \dots, x_i) \subsetneq (x_1, \dots, x_{i+1})$ für alle $i \in [1, n-1]$. Für alle $i \in [1, n-1]$ ist dann $x_{i+1} \notin x_i \mathcal{O}$, also $x_i^{-1} x_{i+1} \notin \mathcal{O}$ und daher $x_i x_{i+1}^{-1} \in P$, also $x_i \in x_{i+1} P$. Wegen 2. folgt $n \leq [L:K(x_1)]$. Daher gibt es ein $n \in \mathbb{N}$ mit $P = (x_1, \dots, x_n)$. Daher ist P endlich erzeugt.

Sei $\{y_1, \dots, y_m\}$ ein minimales Erzeugendensystem von P . Wäre $m \geq 2$, so folgte $y_2 \notin y_1 \mathcal{O}$, also $y_1^{-1} y_2 \notin \mathcal{O}$ und daher $y_1 y_2^{-1} \in \mathcal{O}$, folglich $y_1 \in y_2 \mathcal{O}$ und $P = (y_2, \dots, y_m)$ im Widerspruch zur Minimalität von m . Daher ist P ein Hauptideal, $P = (t)$ mit einem Primelement $t \in \mathcal{O}$.

Wir zeigen nun, dass jedes $x \in \mathcal{O}^\bullet$ eine eindeutige Darstellung $x = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}^\times$ besitzt (dann ist \mathcal{O} faktoriell und t ist bis auf Assoziierte das einzige Primelement). Die Eindeutigkeit ist klar, da t ein Primelement ist. Für den Nachweis der Existenz sei $x \in \mathcal{O}^\bullet$. Ist $x \in \mathcal{O}^\times$, so ist nichts zu zeigen. Sei also $x \in P$. Dann genügt es, die Existenz eines $n \in \mathbb{N}$ mit $t^n | x$ und $t^{n+1} \nmid x$ zu zeigen, denn dann ist $t^{-n} x \in \mathcal{O} \setminus (t) = \mathcal{O}^\times$. Wir nehmen im Gegenteil an, es sei $t^n | x$ für alle $n \in \mathbb{N}$. Für $i \in \mathbb{N}$ sei $x_i = t^{1-i} x$, also $x_i = t x_{i+1} \in x_{i+1} P$. Nach 2. folgt nun $n \leq [L:K(a)] < \infty$ für alle $n \in \mathbb{N}$, ein Widerspruch. \square

Satz 3.4.2. *Sei L/K ein Funktionenkörper und $K \subsetneq \mathcal{O} \subsetneq L$ ein lokaler Teilbereich mit maximalem Ideal $P = \mathcal{O} \setminus \mathcal{O}^\times$. Ist P ein Hauptideal, so ist \mathcal{O} ein diskreter Bewertungsbereich.*

BEWEIS. Sei $P = (t)$ mit einem Primelement $t \in \mathcal{O}$. Wir zeigen, dass jedes $a \in \mathcal{O}^\bullet$ eine Darstellung $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}^\times$ besitzt, und dafür genügt es, zu zeigen, dass es ein maximales $n \in \mathbb{N}$ mit $t^n | a$ gibt. Nach den Sätzen 3.3.3 und 3.3.2 gibt es einen diskreten Bewertungsbereich \mathcal{O}' von L mit maximalem Ideal $P' = (t')$, so dass $\mathcal{O} \subset \mathcal{O}'$ und $(t) \subset (t')$. Dann ist aber

$$\bigcap_{n \geq 0} (t^n) \subset \bigcap_{n \geq 0} (t'^n) = \{0\},$$

und daher gibt ein maximales $n \in \mathbb{N}$ mit $a \in (t^n)$, also $t^n | a$. \square

3.5

Satz 3.5.1. *Sei K ein Körper, \overline{K} eine algebraische Hülle von K , $C \subset \overline{K}^2$ eine über K definierte irreduzible Kurve und $\mathfrak{p} = (\alpha, \beta) \in C$.*

1. *Ist \mathfrak{p} ein über K regulärer Punkt von C , so ist $\mathcal{O}_{\mathfrak{p}, K}(C)$ ein diskreter Bewertungsbereich.*
2. *Ist $\mathcal{O}_{\mathfrak{p}, K}(C)$ ein diskreter Bewertungsbereich und $K(\alpha, \beta)/K$ separabel, so ist \mathfrak{p} ein regulärer Punkt von C .*

BEWEIS. Sei $\mathcal{J}_K(C) = {}_{K[X, Y]}(f)$ mit einem irreduziblen Polynom $f \in K[X, Y]$. Für $g \in K[X, Y]$ sei $\bar{g} = g + (f) = g | C \in K[C]$, und seien $x = \overline{X}$, $y = \overline{Y}$ die Koordinatenfunktionen von C .

1. Sei \mathbf{p} ein über K regulärer Punkt von C . Nach Satz 1.6.2 liegt \mathbf{p} in genau einer Komponente C_1 von C über \bar{K} und ist ein regulärer Punkt von C_1 . Sei $\mathcal{J}_{\bar{K}}(C_1) = \bar{K}[X, Y](f_0)$ mit einem irreduziblen Polynom $f_0 \in \bar{K}[X, Y]$. Dann ist $f_0 | f$ in $\bar{K}[X, Y]$, der kanonische Homomorphismus

$$K[X, Y] \rightarrow \bar{K}[C_1], \quad \text{definiert durch } g \mapsto g|_{C_1},$$

hat Kern $K[X, Y] \cap \bar{K}[C_1](f_0) = K[X, Y](f)$ und induziert einen Monomorphismus

$$K[C] \rightarrow \bar{K}[C_1], \quad \text{gegeben durch } \varphi \mapsto \varphi|_{C_1},$$

vermöge dessen wir $K[C] \subset \bar{K}[C_1]$ als Teilring auffassen. Dann ist auch $K(C) \subset \bar{K}(C_1)$, und

$$\mathcal{O}_{\mathbf{p}, K} = \left\{ \frac{u}{v} \mid u, v \in K[C], v(\mathbf{p}) \neq 0 \right\} = \mathcal{O}_{\mathbf{p}, \bar{K}}(C_1) \cap K(C).$$

Wir zeigen, dass $\mathcal{O}_{\mathbf{p}, \bar{K}}$ ein diskreter Bewertungsbereich von $\bar{K}(C_1)$ ist (dann ist $\mathcal{O}_{\mathbf{p}, K} = \mathcal{O}_{\mathbf{p}, \bar{K}}(C_1) \cap K(C)$ ein Bewertungsbereich von $K(C)$, also nach Satz 3.4.1 ein diskreter Bewertungsbereich. Da $\mathcal{O}_{\mathbf{p}, \bar{K}}(C)$ lokal ist, genügt es nach Satz 3.4.2 zu zeigen, dass das maximale Ideal $\mathcal{M}_{\mathbf{p}, \bar{K}}(C)$ ein Hauptideal ist.

Sei daher im Folgenden $K = \bar{K}$, $\mathcal{J}_K(C) = K[X, Y](f)$ und ohne Einschränkung $\frac{\partial f}{\partial Y}(\mathbf{p}) \neq 0$. Dann ist $f = (Y - \beta)f_1 - (X - \alpha)f_2$ mit $f_1, f_2 \in K[X, Y]$ und $f_1(\alpha, \beta) \neq 0$. Dann ist $\bar{f}_1(\mathbf{p}) \neq 0$ und

$$0 = \bar{f} = (y - \beta)\bar{f}_1 - (x - \alpha)\bar{f}_2, \quad \text{also } y - \beta = (x - \alpha) \frac{\bar{f}_2}{\bar{f}_1} \in \mathcal{O}_{\mathbf{p}}(C)(x - \alpha),$$

und daher $\mathcal{M}_{\mathbf{p}}(C) = \mathcal{O}_{\mathbf{p}}(C)(x - \alpha)$.

2. Sei $m_\alpha \in K[X]$ das Minimalpolynom von α und $m_\beta \in K[Y]$ das Minimalpolynom von β über K . Dann $\bar{m}_\alpha = m_\alpha(x)$ und $\bar{m}_\beta = m_\beta(y)$. Da $K(x, y)/K$ transzendent ist, folgt $(\bar{m}_\alpha, \bar{m}_\beta) \neq (0, 0)$. Da $\mathcal{O}_{\mathbf{p}}(C)$ ein Bewertungsbereich von $K(C)$ ist, folgt: Ist $\bar{m}_\alpha \bar{m}_\beta \neq 0$, so ist entweder $\bar{m}_\beta^{-1} \bar{m}_\alpha \in \mathcal{O}_{\mathbf{p}}(C)$ oder $\bar{m}_\alpha^{-1} \bar{m}_\beta \in \mathcal{O}_{\mathbf{p}}(C)$. Wir nehmen an, es sei $\bar{m}_\beta \neq 0$ und $\bar{m}_\beta^{-1} \bar{m}_\alpha \in \mathcal{O}_{\mathbf{p}}(C)$. Dann existieren Polynome $g, h \in K[X, Y]$ mit $h(\mathbf{p}) \neq 0$ und

$$\frac{\bar{m}_\alpha}{\bar{m}_\beta} = \frac{\bar{g}}{\bar{h}}, \quad \text{also } m_\alpha h - m_\beta g = Qf \quad \text{mit einem Polynom } Q \in K[X, Y].$$

Wir betrachten nun die partiellen Ableitungen nach X and der Stelle \mathbf{p} . Wegen

$$f(\mathbf{p}) = 0, \quad m_\alpha(\mathbf{p}) = m_\alpha(\alpha) = 0, \quad \frac{\partial m_\alpha}{\partial X}(\mathbf{p}) = m'_\alpha(\mathbf{p}) \neq 0, \quad m_\beta(\mathbf{p}) = m_\beta(\beta) = 0 \quad \text{und} \quad \frac{\partial m_\beta}{\partial X} = 0$$

folgt

$$m'_\alpha(\mathbf{p})h(\mathbf{p}) = Q(\mathbf{p}) \frac{\partial f}{\partial X}(\mathbf{p}) \neq 0 \quad \text{und daher} \quad \frac{\partial f}{\partial X}(\mathbf{p}) \neq 0. \quad \square$$

3.6

Definition 3.6.1. Sei L ein Körper und ∞ ein neues Symbol, für das wir folgende Konventionen vereinbaren: Für alle $k \in \mathbb{Z} \cup \{\infty\}$ ist $k + \infty = \infty + k = \infty$ und $k = \min\{k, \infty\} \leq \infty$.

Eine *diskrete Bewertung* oder *Exponentenbewertung* von L ist eine Abbildung $v: L \rightarrow \mathbb{Z} \cup \{\infty\}$, so dass für alle $a, b \in L$ gilt:

- $v(a) = \infty$ if and only if $a = 0$.
- $v(ab) = v(a) + v(b)$.
- $v(a + b) \geq \min\{v(a), v(b)\}$.

Ist v eine diskrete Bewertung von L , so heißt $\mathcal{O}_v = \{x \in L \mid v(x) \geq 0\}$ der *Bewertungsbereich* oder *Ganzheitsbereich* und $P_v = \{x \in L \mid v(x) > 0\}$ das *Bewertungsideal* von v .

Bemerkungen 3.6.2. Sei L ein Körper und $v: L \rightarrow \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung.

1. $v|L^\times: L^\times \rightarrow \mathbb{Z}$ ist ein Gruppenepimorphismus. Insbesondere ist $v(1) = 0$ und $v(a^{-1}) = -v(a)$ für alle $a \in L^\times$.
2. Für jede Einheitswurzel $z \in L$ ist $v(z) = 0$
[denn: Ist $n \in \mathbb{N}$ mit $z^n = 1$, so folgt $0 = v(z^n) = nv(z)$ und daher $v(z) = 0$].
3. Für alle $a, b \in K$ ist $v(-a) = v(a)$ und $v(a - b) \geq \min\{v(a), v(b)\}$.
4. Sind $a, b \in L$ mit $v(a) < v(b)$, so ist $v(a \pm b) = v(a)$.
[Beweis: Wäre $v(a + b) > v(a)$, so folgte $v(a) = v((a + b) + (-b)) \geq \min\{v(a + b), v(b)\} > v(a)$, ein Widerspruch].
5. Seien $n \in \mathbb{N}$ und $a_1, \dots, a_n \in L$. Dann gilt:
 - (a) Ist $v(a_1) < v(a_i)$ für alle $i \in [2, n]$, so ist $v(a_1 + \dots + a_n) = v(a_1)$.
 - (b) Ist $a_1 + \dots + a_n = 0$, so gibt es Indizes $i, j \in [1, n]$ mit $i \neq j$ und $v(a_i) = v(a_j)$.
 [Beweis Ü!]

Satz 3.6.3. Sei L ein Körper und v eine diskrete Bewertung von L . Dann ist \mathcal{O}_v ein diskreter Bewertungsbereich von L mit maximalem Ideal P_v , und $\mathcal{O}_v^\times = \mathcal{O}_v \setminus P_v = \{x \in L \mid v(x) = 0\}$. Für $t \in L$ sind die folgenden Aussagen äquivalent:

- a) t ist ein Primelement von \mathcal{O}_v ; b) $P_v = (t)$; c) $v(t) = 1$.

Ist $K \subset L$ ein Teilkörper, so ist genau dann $v|K^\times = 0$, wenn $K \subset \mathcal{O}_v$.

BEWEIS. Sind $a, b \in \mathcal{O}_v$, so folgt $v(a - b) \geq \min\{v(a), v(b)\} \geq 0$ und $v(ab) = v(a) + v(b) \geq 0$, also $a - b \in \mathcal{O}_v$ und $ab \in \mathcal{O}_v$. Daher ist $\mathcal{O}_v \subset L$ ein Teilbereich.

Ist $x \in L \setminus \mathcal{O}_v$, so ist $v(x) < 0$, also $v(x^{-1}) = -v(x) > 0$ und daher $x^{-1} \in \mathcal{O}_v$. Daher ist $L = \mathfrak{q}(\mathcal{O}_v)$. Ist $x \in L^\times$, so ist genau dann $x \in \mathcal{O}_v^\times$, wenn $x \in \mathcal{O}_v$ und $x^{-1} \in \mathcal{O}_v$, wenn also $v(x) \geq 0$ und $-v(x) = v(x^{-1}) \geq 0$. Damit folgt $\mathcal{O}_v^\times = \{x \in L^\times \mid v(x) = 0\} = \mathcal{O}_v \setminus P_v$.

Sind $a, b \in P_v$ und $c \in \mathcal{O}_v$, so folgt $v(a - b) \geq \min\{v(a), v(b)\} > 0$ und $v(ca) = v(c) + v(a) > 0$, also $a - b \in P_v$ und $ca \in P_v$. Daher ist $P_v \subset \mathcal{O}_v$ ein Ideal, und wegen $P_v = \mathcal{O}_v \setminus \mathcal{O}_v^\times$ ist \mathcal{O}_v lokal mit maximalem Ideal P_v .

Wir zeigen nun:

A. Ist $t \in K$ mit $v(t) = 1$, so hat jedes $a \in \mathcal{O}_v^\bullet$ eine eindeutige Darstellung $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}_v^\times$.

Beweis von A. Sei $t \in L$ mit $v(t) = 1$. Ist $a \in \mathcal{O}_v^\bullet$ und $v(a) = n$, so ist $v(t^{-n}a) = -nv(t) + v(a) = 0$, also folgt $u = t^{-n}a \in \mathcal{O}_v^\times$ und $a = t^n u$. Ist umgekehrt $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}_v^\times$, so folgt $v(a) = nv(t) + v(u) = n$. □[A]

Sei $t \in K$ mit $v(t) = 1$. Nach **A** ist \mathcal{O}_v faktoriell, und t ist bis auf Assoziierte das einzige Primelement von \mathcal{O}_v . Daher ist \mathcal{O}_v ein diskreter Bewertungsbereich, es folgt die Implikation **c**) \Rightarrow **a**), und nach Satz 3.3.2 ist **a**) \Leftrightarrow **b**). Für den Nachweis von **a**) \Rightarrow **c**) sei $a \in K^\times$ mit $v(a) = 1$. Dann ist $a \in \mathcal{O}_v^\bullet$, also $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}_v^\times$, es folgt $1 = nv(t)$ und $n = v(t) = 1$.

Ist $K \subset L$ ein Teilkörper, so ist genau dann $K \subset \mathcal{O}_v$, wenn $K^\times \subset \mathcal{O}_v^\times$, wenn also $v|K^\times = 0$. □

Definition und Satz 3.6.4. Sei R ein faktorieller Bereich, $L = \mathfrak{q}(R)$ und $t \in R^\bullet$ ein Primelement von R . Dann hat jedes $x \in K^\times$ eine Darstellung $x = t^n u^{-1} v$ mit $n \in \mathbb{Z}$ und $u, v \in R \setminus (t)$. Dabei ist n durch x und das Primideal ${}_R(t)$ eindeutig bestimmt und heißt t -adischer Wert von x . Wir setzen $v_t(x) = n$ und $v_t(0) = \infty$. Dann ist $v_t: L \rightarrow \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung von L , $v_t(t) = 1$, $\mathcal{O}_{v_t} = \{u^{-1}c \mid u, c \in R, u \notin (t)\} \supset R$ und $P_{v_t} = \{u^{-1}c \mid u, c \in R, u \notin (t), c \in (t)\} = \mathfrak{o}_{v_t}(t)$.

Ist R ein Hauptidealbereich, so ist (t) ein maximales Ideal von R , und die Einbettung $R \hookrightarrow \mathcal{O}_{v_t}$ induziert einen Isomorphismus $R/R(t) \xrightarrow{\sim} \mathcal{O}_{v_t}/\mathcal{P}_{v_t}$.

Die diskrete Bewertung v_t heißt t -adische Bewertung von L (sie hängt nur vom Primideal $R(t)$ ab.)

BEWEIS. Die Existenz einer Darstellung für $x \in L^\times$ wie behauptet ist klar. Zum Nachweis der Eindeutigkeit von n sei ${}_R(t) = {}_R(t')$, $x = t^n u^{-1} v = t^{n'} u'^{-1} v'$ mit $n, n' \in \mathbb{Z}$, $u, v, u', v' \in R \setminus {}_R(t)$, und es sei $n \geq n'$. Dann gibt es ein $e \in R^\times$ mit $t' = et$, und es folgt $t^{n-n'} e^{-n'} u' v = uv' \notin {}_R(t)$, also $n = n'$.

Um v_t als diskrete Bewertung nachzuweisen, genügt es, zu zeigen, dass $v_t(x_1 x_2) = v_t(x_1) + v_t(x_2)$ und $v_t(x_1 + x_2) \geq \min\{v_t(x_1), v_t(x_2)\}$ für alle $x_1, x_2 \in L^\times$. Für $i \in \{1, 2\}$ sei $x_i = t^{n_i} u_i^{-1} v_i$ mit $n_i = v_t(x_i) \in \mathbb{Z}$, $u_i, v_i \in R \setminus (t)$ und $n_1 \geq n_2$. Dann folgt $x_1 x_2 = t^{n_1+n_2} (u_1 u_2)^{-1} v_1 v_2$ mit $u_1 u_2 v_1 v_2 \notin (t)$, also $v_t(x_1 x_2) = n_1 + n_2$, und $x_1 + x_2 = t^{n_2} (t^{n_1-n_2} u_2 v_1 + u_1 v_2) (u_1 u_2)^{-1} = t^{n_2+\delta} w (u_1 u_2)^{-1}$ mit $\delta \in \mathbb{N}_0$ und $w \in R \setminus (t)$, also $v_t(x_1 + x_2) = n_2 + \delta \geq n_2$.

Nach Definition ist $R \subset \mathcal{O}_{v_t}$ und $t \in P_{v_t}$, also auch $\mathcal{O}_{v_t}(t) \subset P_{v_t}$. Ist $x = u^{-1}c$ mit $u \in R \setminus (t)$ und $c \in R$, so ist $v_t(x) = v_t(c) \geq 0$, also $x \in \mathcal{O}_{v_t}$, und im Falle $c \in (t)$ ist $v_t(x) = v_t(c) \geq v_t(t) = 1$, also $x \in P_{v_t}$. Ist $x \in \mathcal{O}_{v_t}$, so ist $x = t^n u^{-1}v$ mit $n = v(x) \geq 0$ und $u, v \in R \setminus (t)$, also $x = u^{-1}c$ mit $c = t^n v \in R$. Ist $x \in P_{v_t}$, so ist $n > 0$, also $c \in (t)$ und daher $x \in \mathcal{O}_{v_t}(t) \subset P_{v_t}$. Damit sind die Behauptungen über \mathcal{O}_{v_t} und P_{v_t} gezeigt.

Sei nun R ein Hauptidealbereich. Ist $u \in R$ mit $(t) \subset (u) \subsetneq R$, so folgt $u \notin R^\times$ und $u \mid t$, also $u \simeq t$ und $(u) = (t)$. Daher ist (t) maximal, und wegen $\mathcal{O}_{v_t}(t) \cap R = \{x \in R \mid v_t(x) > 0\} = {}_R(t)$ induziert die Einbettung $R \hookrightarrow \mathcal{O}_{v_t}$ einen Monomorphismus $\varphi: R/R(t) \rightarrow \mathcal{O}_{v_t}/\mathcal{O}_{v_t}(t)$ mit $\varphi(b + {}_R(t)) = b + \mathcal{O}_{v_t}(t)$. Ist $x = u^{-1}c \in \mathcal{O}_v$ mit $u, c \in R$ und $u \notin (t)$, so ist $R = {}_R(u, t)$, und daher gibt es $m, n \in R$ mit $c = um + tn$ und daher $x + \mathcal{O}_{v_t}(t) = \varphi(m + {}_R(t))$. Folglich ist φ ein Isomorphismus. \square

Satz 3.6.5. Sei L ein Körper.

1. Sei \mathcal{O} ein diskreter Bewertungsbereich von L und $t \in \mathcal{O}$ ein Primelement. Dann ist die t -adische Bewertung v_t von L eine diskrete Bewertung mit $\mathcal{O}_{v_t} = \mathcal{O}$.
2. Sei $v: L \rightarrow \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung und $t \in \mathcal{O}_v$ ein Primelement. Dann ist $v = v_t$.

BEWEIS. 1. Nach Satz 3.6.4 ist v_t eine diskrete Bewertung von L , und nach Satz 3.3.2 genügt es, $\mathcal{O}_{v_t} \subset \mathcal{O}$ zu zeigen. Ist $x \in \mathcal{O}_{v_t}$, so ist $x = u^{-1}c$ mit $u, c \in \mathcal{O}$ und $u \in \mathcal{O} \setminus (t) = \mathcal{O}^\times$ und daher $x \in \mathcal{O}$.

2. Nach Satz 3.6.3 ist $v(t) = 1$. Ist $x \in L^\times$, so ist $x = t^n u$ mit $n \in \mathbb{Z}$ und $u \in \mathcal{O}_v^\times = \mathcal{O}_v \setminus (t)$, und daher folgt $v(x) = n = v_t(x)$. \square

Satz 3.6.6 (Vergleichssatz für diskrete Bewertungen). Sei L ein Körper, und seien v und v' diskrete Bewertungen von L . Dann sind die folgenden Aussagen äquivalent:

- (a) $v = v'$.
- (b) $\mathcal{O}_v \subset \mathcal{O}_{v'}$.
- (c) $P_v \subset P_{v'}$.
- (d) $\{x \in L \mid v(x) > 0\} \subset \{x \in L \mid v'(x) > 0\}$.
- (e) $\{x \in L \mid v(x) \geq 0\} \subset \{x \in L \mid v'(x) \geq 0\}$.

BEWEIS. (a) \Rightarrow (b), (c) \Rightarrow (d) und (e) \Rightarrow (b) Offensichtlich.

(b) \Rightarrow (a) und (b) \Rightarrow (c) Nach Satz 3.3.2.2(b) ist $\mathcal{O}_v = \mathcal{O}_{v'}$ und daher $P_v = P_{v'} = (t)$ mit $t \in \mathcal{O}_v$. Nach Satz 3.6.5.2. ist dann $v = v_t = v'$.

(d) \Rightarrow (e) Wir nehmen an, es sei $x \in L$ mit $v(x) \geq 0$ und $v'(x) < 0$. Dann ist $v(x) = 0$, und es sei $t \in P$ mit $v(t) = 1$. Dann ist $v'(t) = r \in \mathbb{N}$, $v(x^r t) = rv(x) + v(t) = 1$ und

$$v'(x^r t) = rv'(x) + v'(t) \leq -r + r = 0, \quad \text{ein Widerspruch.} \quad \square$$

Satz 3.6.7 (Schwacher Approximationssatz). *Sei L ein Körper, $n \in \mathbb{N}$, und seien v_1, \dots, v_n verschiedene diskrete Bewertungen von L . Seien $(x_1, \dots, x_n) \in L^n$ und $(r_1, \dots, r_n) \in \mathbb{Z}^n$. Dann gibt es ein $x \in L$, so dass $v_i(x - x_i) = r_i$ für alle $i \in [1, n]$.*

BEWEIS. Wir beginnen mit drei Zwischenbehauptungen **A**, **B** und **C**.

A. Es gibt ein $u \in L$, so dass $v_1(u) > 0$ und $v_i(u) < 0$ für alle $i \in [2, n]$.

Beweis von A. Induktion nach n . Für $n = 1$ ist nichts zu zeigen.

$n = 2$: Nach Satz 3.6.6 gibt es $u_1, u_2 \in L^\times$ mit $v_1(u_1) < 0$, $v_2(u_1) \geq 0$, $v_1(u_2) \geq 0$ und $v_2(u_2) < 0$. Dann ist $v_1(u_1^{-1}u_2) = -v_1(u_1) + v_1(u_2) > 0$ und $v_2(u_1^{-1}u_2) = -v_2(u_1) + v_2(u_2) < 0$.

$n \geq 3$, $n-1 \rightarrow n$: Sei $y \in L^\times$ mit $v_1(y) > 0$ und $v_i(y) < 0$ für alle $i \in [2, n-1]$. Ist dann $v_n(y) < 0$, so sind wir fertig. Sei also $v_n(y) \geq 0$, und sei $z \in L^\times$ mit $v_1(z) > 0$ und $v_n(z) < 0$. Da $v_i(y) \neq 0$ für alle $i \in [1, n-1]$, gibt es ein $r \in \mathbb{N}$ mit $rv_i(z) \neq v_i(y)$ für alle $i \in [1, n-1]$. Sei nun $u = y + z^r$. Dann ist $v_1(u) \geq \min\{v_1(y), rv_1(z)\} > 0$, und für alle $i \in [2, n]$ ist $v_i(u) = \min\{v_i(y), rv_i(z)\} < 0$. \square [A]

B. Es gibt ein $w \in L$ mit $v_1(w-1) > r_1$ und $v_i(w) > r_i$ für alle $i \in [2, n]$.

Beweis von B. Sei $u \in L$ mit $v_1(u) > 0$ und $v_i(u) < 0$ für alle $i \in [2, n]$. Für $s \in \mathbb{N}$ sei $w = (1 + u^s)^{-1}$, also $w - 1 = -u^s(1 + u^s)^{-1}$. Dann ist $v_1(w-1) = sv_1(u) - v_1(1 + u^s) = sv_1(u) > r_1$ für $s \gg 1$. Für $i \in [2, n]$ ist $v_i(w) = -v_i(1 + u^s) = -sv_i(u) > r_i$ für $s \gg 1$. \square [B]

C. Für alle $(y_1, \dots, y_n) \in L^n$ gibt es ein $z \in L$, so dass $v_i(z - y_i) > r_i$ für alle $i \in [1, n]$.

Beweis von C. Sei $(y_1, \dots, y_n) \in L^n$ und $s \in \mathbb{Z}$, so dass $v_i(y_j) \geq s$ für alle $i, j \in [1, n]$. Nach **B** gibt es $w_1, \dots, w_n \in L$, so dass $v_i(w_i - 1) > r_i - s$ und $v_i(w_j) > r_i - s$ für alle $i, j \in [1, n]$ mit $j \neq i$. Sei nun $z = y_1w_1 + \dots + y_nw_n$. Für alle $i \in [1, n]$ folgt dann

$$z - y_i = \sum_{\substack{j=1 \\ j \neq i}}^n y_j w_j + y_i(w_i - 1) \quad \text{und} \quad v_i(y_i(w_i - 1)) > s + (r_i - s).$$

Für $j \in [1, n]$ mit $j \neq i$ ist $v_i(y_j w_j) > s + (r_i - s) = r_i$, und daher ist auch $v_i(z - y_i) > r_i$. \square [C]

Eigentlicher Beweis. Für $i \in [1, n]$ sei $z_i \in L$ mit $v_i(z_i) = r_i$. Nach **C** gibt es $z, z' \in L$, so dass $v_i(z - x_i) > r_i$ und $v_i(z' - z_i) > r_i$ für alle $i \in [1, n]$. Sei $x = z + z'$. Für alle $i \in [1, n]$ folgt dann

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

3.7

Definition 3.7.1. Sei L/K ein Funktionenkörper. Eine Teilmenge $P \subset L$ heißt *Stelle* von L/K , wenn P das maximale Ideal eines Bewertungsbereiches \mathcal{O} von L mit $K \subset \mathcal{O}$ ist. Nach Satz 3.3.2 ist dann \mathcal{O} ein diskreter Bewertungsbereich, $P = (t)$ ist ein Hauptideal von \mathcal{O} , nach Satz 3.6.5 ist $\mathcal{O} = \mathcal{O}_{v_t}$, und nach Satz 3.6.3 ist $v|K^\times = 0$. Nach Satz 3.6.6 sind \mathcal{O} und v durch P eindeutig bestimmt.] Man nennt $\mathcal{O} = \mathcal{O}_P$ den Bewertungsbereich und $v = v_P$ die Bewertung zur Stelle P (es ist dann $\mathcal{O}_P = \mathcal{O}_{v_P}$ und $P = P_{v_P}$). Jedes Primelement t von \mathcal{O}_P heißt *Ortsuniformisierende* oder *lokaler Parameter* von P . Der Körper $L_P = \mathcal{O}_P/P$ heißt *Restklassenkörper* von P . Es bezeichne $\mathbb{P}_L = \mathbb{P}_{L/K}$ die Menge aller Stellen von L/K .

Sei \tilde{K} der Konstantenkörper von L/K und $P \in \mathbb{P}_L$. Nach Satz 3.4.1 ist $\tilde{K} \subset \mathcal{O}_P$ und $P \cap \tilde{K} = \{0\}$. Die Einbettung $\tilde{K} \hookrightarrow \mathcal{O}_P$ induziert einen Monomorphismus $\tilde{K} \rightarrow L_P$, und wir betrachten fernerhin \tilde{K} als in L_P eingebettet. Dann ist $K \subset \tilde{K} \subset L_P$, und nach Satz 3.7.2 ist $\deg(P) = [L_P : K] < \infty$. Man nennt $\deg(P)$ den *Grad* von P . Für $d \in \mathbb{N}$ bezeichne \mathbb{P}_L^d die Menge aller Stellen vom Grade d .

Für $P \in \mathbb{P}_L$ und $z \in L$ definieren wir $z(P) \in L_P \cup \{\infty\}$ durch

$$z(P) = z + P \in L_P, \quad \text{falls } z \in \mathcal{O}_P, \quad \text{und} \quad z(P) = \infty, \quad \text{falls } z \in L \setminus \mathcal{O}_P,$$

und wir nennen $z(P)$ den Wert der Funktion z an der Stelle P . Aufgrund der Einbettung $\tilde{K} \hookrightarrow L_P$ gilt für $z(P) = z$ für alle $z \in \tilde{K}$ und alle $P \in \mathbb{P}_L$. Die Abbildung $z \mapsto z(P)$ ist ein \tilde{K} -Algebrenepimorphismus $\mathcal{O}_P \rightarrow L_P$.

Sei $z \in L$ und $P \in \mathbb{P}_L$. Ist $z(P) = 0$, so nennt man P eine Nullstelle von z ; es ist dann $v_P(z) > 0$, und man nennt $v_P(z)$ die Nullstellenordnung von z in P . Ist $z(P) = \infty$, so nennt man P eine Polstelle von z ; es ist dann $v_P(z) < 0$, und man nennt $-v_P(z)$ die Polstellenordnung von z in P . Es bezeichne $\mathcal{N}(z)$ die Menge der Nullstellen und $\mathcal{P}(z)$ die Menge der Polstellen von z . Offensichtlich ist $\mathcal{P}(z) = \mathcal{N}(z^{-1})$.

Satz 3.7.2. Sei L/K ein Funktionenkörper mit Konstantenkörper \tilde{K} .

1. Sei $x \in L \setminus \tilde{K}$, $r \in \mathbb{N}$, und seien $P_1, \dots, P_r \in \mathbb{P}_L$ verschiedene Nullstellen von x . Dann ist

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

2. Sei $P \in \mathbb{P}_L$ und $0 \neq x \in P$. Dann ist $[\tilde{K}:K] \leq \deg(P) \leq [L:K(x)] < \infty$. Ist insbesondere $\mathbb{P}_L^1 \neq \emptyset$, so ist $\tilde{K} = K$.

3. Für $x \in L \setminus \tilde{K}$ ist $0 < |\mathcal{N}(x)| \leq [L:K(x)] < \infty$ und $0 < |\mathcal{P}(x)| \leq [L:K(x)] < \infty$.

4. Für jedes $x \in L^\times$ ist $v_P(x) = 0$ für fast alle (das heißt, für alle bis auf endlich viele) $P \in \mathbb{P}_L$, und $\tilde{K}^\times = \{x \in L^\times \mid v_P(x) = 0 \text{ für alle } P \in \mathbb{P}_L\}$.

5. $|\mathbb{P}_L| = \infty$.

BEWEIS. Nach Satz 3.2.1 ist $[L:K(x)] < \infty$. Für $i \in [1, r]$ sei $v_i = v_{P_i}$, $e_i = v_i(x) \in \mathbb{N}$ (da $x \in P_i$) und $f_i \in \mathbb{N}$ mit $f_i \leq \deg(P_i)$. Seien $s_{i,1}, \dots, s_{i,f_i} \in \mathcal{O}_{P_i}$, so dass die Werte $s_{i,1}(P_i), \dots, s_{i,f_i}(P_i) \in L_{P_i}$ über K linear unabhängig sind. Nach Satz 3.6.7 gibt es ein $t_i \in L$ mit $v_i(t_i) = 1$ und $v_k(t_i) = 0$ für alle $k \in [1, r] \setminus \{i\}$. Für alle $i \in [1, r]$ und $j \in [1, f_i]$ gibt es Funktionen $z_{i,j} \in L$ mit

$$v_i(s_{i,j} - z_{i,j}) > 0 \quad \text{und} \quad v_k(z_{i,j}) \geq e_k \quad \text{für alle } k \in [1, r] \setminus \{i\}.$$

Dann ist $z_{i,j} = s_{i,j} - (s_{i,j} - z_{i,j}) \in \mathcal{O}_{P_i}$, also $v_i(z_{i,j}) \geq 0$. Nun zeigen nun:

Die Menge $\{t_i^a z_{i,j} \mid i \in [1, r], j \in [1, f_i], a \in [0, e_i - 1]\}$ ist linear unabhängig über $K(x)$.

Damit folgt dann

$$[L:K(x)] \geq \sum_{i=1}^r e_i f_i = \sum_{i=1}^r v_{P_i}(x) f_i \quad \text{und daher auch} \quad [L:K(x)] \geq \sum_{i=1}^r v_{P_i}(x) \deg(P_i).$$

Wir nehmen im Gegenteil an, es bestehe eine Relation der Form

$$\sum_{i=1}^r \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{i,j,a} t_i^a z_{i,j} = 0 \quad \text{mit} \quad \varphi_{i,j,a} \in K(x), \quad \text{nicht alle} = 0.$$

Wir können annehmen, dass $\varphi_{i,j,a} \in K[x] \subset \mathcal{O}_{P_i}$ für alle i, j, a , aber $\varphi_{i,j,k} \notin xK[x]$ für mindestens ein Indextripel (i, j, a) . Sei $k \in [1, r]$, $l \in [1, f_k]$ und $c \in [0, e_k - 1]$, so dass $\varphi_{k,l,c} \notin xK[x]$, aber $\varphi_{k,j,a} \in xK[x]$ für alle $a \in [0, c - 1]$ und $j \in [1, f_k]$. Dann ist

$$y = \sum_{i=1}^r \sum_{j=1}^{f_i} \sum_{a=0}^{e_i-1} \varphi_{i,j,a} t_i^a t_k^{-c} z_{i,j} = 0, \quad \text{und wir betrachten} \quad y(P_k).$$

- Für alle $i \in [1, r] \setminus \{k\}$, $j \in [1, f_i]$ und $a \in [0, e_i - 1]$ ist $v_k(\varphi_{i,j,a} t_i^a t_k^{-c} z_{i,j}) \geq -c + e_k > 0$.
- Für alle $j \in [1, f_k]$ und $a \in [0, c - 1]$ ist $\varphi_{k,j,a} \in xK[x] \subset x\mathcal{O}_{P_k}$, also $v_k(\varphi_{k,j,a}) \geq v_k(x) = e_k$, und daher $v(\varphi_{k,j,a} t_k^{a-c} z_{k,j}) \geq e_k + a - c > 0$.
- Für alle $j \in [1, f_k]$ und $a \in [c + 1, e_k - 1]$ ist $v(\varphi_{k,j,a} t_k^{a-c} z_{k,j}) \geq a - c > 0$.

Daher folgt

$$0 = y(P_k) = \sum_{j=1}^{f_k} \varphi_{k,j,c}(P_k) z_{k,j}(P_k) = \sum_{j=1}^{f_k} \varphi_{k,j,c}(P_k) s_{k,j}(P_k).$$

Für $j \in [1, f_k]$ sei $\varphi_{k,j,c} = a_j + x\psi_j$ mit $a_j \in K$ und $\psi_j \in K[x] \subset \mathcal{O}_{P_k}$ also $\varphi_{k,j,c}(P_k) = a_j \in K$ für alle $j \in [1, f_k]$, und damit folgt $a_j = 0$ für alle $j \in [1, f_k]$ wegen der linearen Unabhängigkeit der $s_{k,j}(P_k)$ über K . Insbesondere ist dann aber $\varphi_{k,l,c} = a_l + x\psi_l = x\psi_l \in xK[x]$, ein Widerspruch.

2. Ist $x \in P$, so ist P eine Nullstelle von x , und aus 1. folgt $\deg(P) \leq v_P(x) \deg(P) \leq [L:K(x)]$. Wegen $K \subset \tilde{K} \subset L_P$ ist $[\tilde{K}:K] \leq [L_P:K] = \deg(P)$.

3. Ist $x \in L^\times$, so ist $\mathcal{P}(x) = \mathcal{N}(x^{-1})$ und $K(x) = K(x^{-1})$, und daher genügt es, die Aussagen für $\mathcal{N}(x)$ zu beweisen. Sind $P_1, \dots, P_r \in \mathcal{N}(x)$ verschieden, so folgt aus 1.

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

und daher $|\mathcal{N}(x)| \leq [L:K(x)]$. Ist $x \in L \setminus \tilde{K}$, so ist $\{0\} \neq I = xK[x] \subsetneq K[x]$ ein echtes Ideal, und nach Satz 3.3.3 gibt es einen Bewertungsbereich \mathcal{O} von L mit maximalem Ideal P , so dass $x \in P$. Dann ist aber $P \in \mathcal{N}(x)$.

4. Für jedes $x \in L^\times$ ist die Menge $\{P \in \mathcal{P}_L \mid v_P(x) \neq 0\} = \mathcal{N}(x) \cup \mathcal{P}(x)$ endlich und daher $v_P(x) = 0$ für fast alle $P \in \mathbb{P}_L$. Ist $x \in L^\times$ und $v_P(x) = 0$ für alle $P \in \mathbb{P}_L$, so ist $\mathcal{N}(x) = \mathcal{P}(x) = \emptyset$ und daher $x \in \tilde{K}^\times$. Ist umgekehrt $x \in \tilde{K}^\times$, so folgt $x \in \mathcal{O}_P^\times$ und daher $v_P(x) = 0$ für alle $P \in \mathbb{P}_L$ nach Satz 3.4.1.

5. Nach 3. ist $\mathbb{P}_L \neq \emptyset$. Wir nehmen an, es sei $\mathbb{P}_L = \{P_1, \dots, P_r\}$ mit $r \in \mathbb{N}$. Nach Satz 3.6.7 gibt es ein $z \in L$ mit $v_{P_i}(z) > 0$ für alle $i \in [1, r]$. Dann ist aber $z \notin \tilde{K}$ und $\mathcal{P}(z) = \emptyset$, ein Widerspruch. \square

Satz 3.7.3. *Sei K^*/K eine Körpererweiterung, und seien $x, y \in K^*$, so dass $K[x, y]$ ein Körper ist. Dann ist $K[x, y]/K$ algebraisch.*

BEWEIS. Sei $L = K[x, y] = K(x, y)$, und sei x nicht algebraisch über K . Dann ist $L = K(x)[y]$ und daher y algebraisch über $K(x)$ (sonst wäre $K(x)[y]$ ein Polynomring über $K(x)$, also kein Körper). Daher ist L/K ein Funktionenkörper. Ist $P \in \mathbb{P}_L$, so $K[x, y] \not\subset \mathcal{O}_P$ und daher $v_P(x) < 0$ oder $v_P(y) < 0$. Daher folgt $\mathbb{P}_L = \mathcal{P}(x) \cup \mathcal{P}(y)$, also ist \mathbb{P}_L endlich, ein Widerspruch. \square

3.8

Definition und Bemerkung 3.8.1. Sei K ein Körper und $K(x)$ ein rationaler Funktionenkörper. Dann ist $R = K[x] \cong K[X]$, also x eine Unbestimmte über K . $R[x]$ ist ein Hauptidealbereich, und die normierten irreduziblen Polynome sind ein Repräsentantensystem paarweise nicht-assoziierter Primelemente von $K[x]$.

1. Sei $p \in K[x]$ normiert und irreduzibel und $v_p: K(x) \rightarrow \mathbb{Z} \cup \{\infty\}$ die p -adische Bewertung von $K(x)$ (siehe Satz 3.6.4). Es ist dann

$$\mathcal{O}_p = \mathcal{O}_{v_p} = \left\{ \frac{f}{g} \mid f, g \in K[x], p \nmid g \right\} \quad \text{und} \quad P_p = P_{v_p} = \left\{ \frac{f}{g} \mid f, g \in K[x], p \mid f, p \nmid g \right\}.$$

Man nennt P_p die zum Primpolynom p gehörige Stelle von $K(x)$. Sei $K(x)_p = \mathcal{O}_p/P_p$ der Restklassenkörper von P_p . Nach Satz 3.6.4 induziert die Einbettung $K[x] \hookrightarrow \mathcal{O}_p$ einen Isomorphismus $K[x]/(p) \xrightarrow{\sim} \mathcal{O}_p/P_p = K(x)_p$. Daher ist $\deg(P_p) = [K(x)_p:K] = \dim_K K[x]/(p) = \text{gr}(p)$. Insbesondere ist $\mathbb{P}_{K(x)}^1 \neq \emptyset$, und daher ist K der Konstantenkörper von $K(x)$.

2. Sei $v_\infty: K(x) \rightarrow \mathbb{Z} \cup \{\infty\}$ definiert durch

$$v_\infty\left(\frac{f}{g}\right) = \text{gr}(g) - \text{gr}(f) \quad (\text{unabhängig von der Bruchdarstellung}).$$

v_∞ ist eine diskrete Bewertung von $K(x)/K$ (nachrechnen!). Es ist $v_\infty(x^{-1}) = 1$,

$$\mathcal{O}_\infty = \mathcal{O}_{v_\infty} = \left\{ \frac{f}{g} \mid f, g \in K[x], g \neq 0, \text{gr}(f) \leq \text{gr}(g) \right\}$$

und

$$P_\infty = P_{v_\infty} = \left\{ \frac{f}{g} \mid f, g \in K[x], \text{gr}(f) < \text{gr}(g) \right\} = \mathcal{o}_\infty(x^{-1}).$$

Die Stelle $P_\infty = P_{v_\infty} = x^{-1}\mathcal{O}_\infty$ heißt *unendliche Stelle* von $K(x)$.

Sei nun $t = x^{-1}$. Dann ist $K(x) = K(t) \supset K[t]$, t ist ein Primelement von $K[t]$, und wir zeigen $v_\infty = v_t: K(x) \rightarrow \mathbb{Z} \cup \{\infty\}$ (dann folgt auch $\deg(P_\infty) = \deg(P_t) = 1$. Sei dazu

$$f = \sum_{\nu=0}^n a_\nu x^\nu, \quad g = \sum_{\mu=1}^m b_\mu x^\mu \quad \text{mit } m, n \in \mathbb{N}_0, a_n b_m \neq 0, \quad \text{und } h = \frac{f}{g} \in K(x)^\times.$$

Dann ist $v_\infty(h) = m - n$, und

$$h = \frac{x^n(a_n + a_{n-1}x^{-1} + \dots + a_0x^{-n})}{x^m(b_m + b_{m-1}x^{-1} + \dots + b_0x^{-m})} = t^{m-n} \frac{a_n + a_{n-1}t + \dots + a_0t^n}{b_m + b_{m-1}t + \dots + b_0t^m} = t^{m-n} \frac{f_0}{g_0}$$

mit $f_0, g_0 \in K[t] \setminus (t)$, also $v_t(h) = m - n = v_\infty(h)$.

Satz 3.8.2. *Sei K ein Körper und $K(x)$ ein rationaler Funktionenkörper über K . Dann ist*

$$\mathbb{P}_{K(x)} = \{P_p \mid p \in K[x] \text{ normiert und irreduzibel}\} \cup \{P_\infty\}.$$

Es ist $\deg(P_\infty) = 1$, und für ein normiertes irreduzibles Polynom $p \in K[x]$ ist $\deg(P_p) = \text{gr}(p)$.

BEWEIS. Nach den Bemerkungen 3.8.1 genügt es, zu zeigen:

Ist $v: K(x) \rightarrow \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung von $K(x)$ mit $v|K^\times = 0$, so ist entweder $v = v_p$ mit einem normierten irreduziblen Polynom $p \in K[x]$, oder $v = v_\infty$.

Sei also $v: K(x) \rightarrow \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung mit $v|K^\times = 0$.

FALL 1: $v(x) \geq 0$. Dann ist $K[x] \subset \mathcal{O}_v$, und $P_v \cap K[x]$ ist ein Primideal von $K[x]$. Wäre $P_v \cap K[x] = \{0\}$, so folgte $v(z) = 0$ für alle $z \in K[x]^\bullet$ und daher $v|K(x)^\times = 0$, ein Widerspruch. Daher ist $P_v \cap K[x] = (p)$ mit einem normierten irreduziblen Polynom $p \in K[x]$, und für alle $g \in K[x] \setminus (p)$ ist $v(g) = 0$. Damit folgt

$$\mathcal{O}_{v_p} = \left\{ \frac{f}{g} \mid f, g \in K[x], g \notin (p) \right\} \subset \mathcal{O}_v$$

und daher $v = v_p$ nach Satz 3.6.6.

FALL 2: $v(x) < 0$. Sei $t = x^{-1}$. Dann ist $K(x) = K(t)$, $v(t) > 0$, und nach FALL 1 gibt es ein Primelement $q \in K[t]$ mit $v = v_q$. Wegen $v(t) > 0$ folgt $t \in (q)$ und daher $q = t$, also $v = v_t = v_\infty$. \square

3.9

*In diesem Abschnitt sei K ein vollkommener Körper,
 \overline{K} eine algebraische Hülle von K und $G_K = \text{Hom}_K(\overline{K}, \overline{K})$.*

Lemma 3.9.1.

1. Jedes $\sigma \in G_K$ ist bijektiv, und G_K ist eine Gruppe.
2. $K = \{x \in \overline{K} \mid \sigma(x) = x \text{ für alle } \sigma \in G_K\}$.

BEWEIS. 1. Sei $\sigma \in G_K$. Dann ist σ injektiv. Für den Nachweis der Surjektivität sei $z \in \overline{K}$, $f \in K[X]$ das Minimalpolynom von z über K , und $N \subset \overline{K}$ die Menge der Nullstellen von f in \overline{K} . Für alle $y \in N$ ist $0 = \sigma(f(y)) = f(\sigma(y))$ und daher $\sigma(y) \in N$. Die Abbildung $\sigma|_N: N \rightarrow N$ ist injektiv, also auch surjektiv, und daher ist $z \in N = \sigma(N) \subset \sigma(\overline{K})$.

Daher ist jedes $\sigma \in G_K$ bijektiv. Sind $\sigma, \sigma' \in G_K$, so folgt $\sigma' \circ \sigma \in G_K$ und $\sigma^{-1} \in G_K$. Daher ist G_K eine Gruppe.

2. Ist $x \in K$, so ist $\sigma(x) = x$ für alle $\sigma \in G_K$ nach Definition. Ist $x \in \overline{K} \setminus K$, so hat das Minimalpolynom $f \in K[X]$ von x über K in \overline{K} eine Nullstelle $x' \neq x$, und es gibt ein $\sigma_0 \in \text{Hom}_K(K(x), \overline{K})$ mit $\sigma_0(x) = x'$. Dann gibt es ein $\sigma \in G_K$ mit $\sigma|_{K(x)} = \sigma_0$, und es ist $\sigma(x) = x' \neq x$. \square

Definition und Satz 3.9.2.

1. Für zwei Punkte $\mathbf{p}, \mathbf{p}' \in \overline{K}^2$ sind die folgenden Aussagen sind äquivalent:

- (a) Es gibt ein $\sigma \in G_K$, so dass gilt: Ist $\mathbf{p} = (\alpha, \beta)$, so ist $\mathbf{p}' = (\sigma(\alpha), \sigma(\beta))$.
- (b) Für alle $f \in K[X, Y]$ gilt: $f(\mathbf{p}) = 0 \iff f(\mathbf{p}') = 0$.
- (c) Für jede über K definierte Kurve $C \subset \overline{K}^2$ gilt: $\mathbf{p} \in C \iff \mathbf{p}' \in C$.

Sind diese Bedingungen erfüllt, so heißen \mathbf{p} und \mathbf{p}' K -konjugiert, $\mathbf{p} \sim_K \mathbf{p}'$. \sim_K ist eine Äquivalenzrelation auf \overline{K}^2 , und K^2 ist die Menge aller Punkte, die nur zu sich selbst K -konjugiert sind.

2. Für zwei Punkte $\mathbf{p}, \mathbf{p}' \in \mathbb{P}_{\overline{K}}^2$ sind die folgenden Aussagen sind äquivalent:

- (a) Es gibt ein $\sigma \in G_K$, so dass gilt; Ist $\mathbf{p} = (\alpha:\beta:\gamma)$, so ist $\mathbf{p}' = (\sigma(\alpha):\sigma(\beta):\sigma(\gamma))$.
- (b) Für jede über K definierte projektive Kurve $\Gamma \subset \mathbb{P}_{\overline{K}}^2$ gilt: $\mathbf{p} \in \Gamma \iff \mathbf{p}' \in \Gamma$.

Sind diese Bedingungen erfüllt, so liegen \mathbf{p} und \mathbf{p}' in denselben affinen Stück von $\mathbb{P}_{\overline{K}}^2$ und heißen K -konjugiert, $\mathbf{p} \sim_K \mathbf{p}'$.

Ist $\theta: \mathbb{P}_{\overline{K}}^2 \rightarrow \mathbb{P}_{\overline{K}}^2$ eine über K definierte projektive Koordinatentransformation und $\mathbf{p}, \mathbf{p}' \in \mathbb{P}_{\overline{K}}^2$ mit $\mathbf{p} \sim_K \mathbf{p}'$, so folgt $\theta(\mathbf{p}) \sim_K \theta(\mathbf{p}')$.

\sim_K stimmt auf den affinen Stücken mit der in 1. definierten Äquivalenzrelation überein, wenn man diese mit \overline{K}^2 identifiziert.

3. Sei $C \subset \overline{K}^2$ eine über K definierte irreduzible Kurve.

- (a) Für zwei Punkte $\mathbf{p}, \mathbf{p}' \in C$ ist genau dann $\mathcal{O}_{\mathbf{p},K}(C) = \mathcal{O}_{\mathbf{p}',K}(C)$, wenn $\mathbf{p} \sim_K \mathbf{p}'$.
- (b) Die Zuordnung $\mathbf{p} \mapsto \mathcal{M}_{\mathbf{p},K}(C) \cap K[C]$ definiert eine Bijektion von der Menge C/\sim_K der Klassen K -konjugierter Punkte von C auf die Menge $\max(K[C])$ der maximalen Ideale von $K[C]$.

BEWEIS. 1. (a) \Rightarrow (b) \Leftrightarrow (c) Offensichtlich.

(b) \Rightarrow (a) Sei $\mathbf{p} = (\alpha, \beta)$, $\mathbf{p}' = (\alpha', \beta')$, und seien $\varphi: K[X, Y] \rightarrow \overline{K}$ und $\varphi': K[X, Y] \rightarrow \overline{K}$ definiert durch $\varphi(f) = f(\mathbf{p})$ und $\varphi'(f) = f(\mathbf{p}')$. Dann ist $\text{Ker}(\varphi) = \text{Ker}(\varphi')$, und daher gibt es einen K -Isomorphismus $\sigma_0: K(\alpha, \beta) \rightarrow K(\alpha', \beta')$ mit $\sigma_0(\alpha) = \alpha'$ und $\sigma_0(\beta) = \beta'$. Da \overline{K} eine algebraische Hülle von K ist, gibt es ein $\sigma \in G_K$ mit $\sigma|_{K(\alpha, \beta)} = \sigma_0$. Offensichtlich ist \sim_K eine Äquivalenzrelation.

2. (a) \Rightarrow (b) Offensichtlich.

(b) \Rightarrow (a) Sei $\mathbf{p} = (\alpha:\beta:\gamma)$ und $\mathbf{p}' = (\alpha':\beta':\gamma')$, und sei ohne Einschränkung $\gamma \neq 0$ (sonst betrachte man einen anderen affinen Teil von $\mathbb{P}_{\overline{K}}^2$). Mit $\Gamma = V_+(Z)$ folgt dann $\gamma' \neq 0$. Dann ist aber

$$\mathbf{p} = \left(\frac{\alpha}{\gamma}, \frac{\beta}{\gamma} \right), \quad \mathbf{p}' = \left(\frac{\alpha'}{\gamma'}, \frac{\beta'}{\gamma'} \right), \quad \text{und für jede Kurve } C \subset \overline{K}^2 \text{ gilt: } \mathbf{p} \in C \iff \mathbf{p}' \in C.$$

Nach 1. gibt es ein $\sigma \in G_K$, so dass

$$\sigma\left(\frac{\alpha}{\gamma}\right) = \frac{\alpha'}{\gamma'} \quad \text{und} \quad \sigma\left(\frac{\beta}{\gamma}\right) = \frac{\beta'}{\gamma'}, \quad \text{also} \quad \alpha' = \frac{\gamma'}{\sigma(\gamma)} \sigma(\alpha) \quad \text{und} \quad \beta' = \frac{\gamma'}{\sigma(\gamma)} \sigma(\beta).$$

Daher folgt $(\alpha':\beta':\gamma') = (\sigma(\alpha):\sigma(\beta):\sigma(\gamma))$. Die übrigen Behauptungen sind nun offensichtlich.

3. Sei $\mathcal{J}_K(C) = {}_{K[X,Y]}(f)$ mit irreduziblem $f \in K[X, Y]$.

(a) Seien $\mathbf{p}, \mathbf{p}' \in C$. Ist $\mathbf{p} \sim_K \mathbf{p}'$, so folgt

$$\mathcal{O}_{\mathbf{p},K}(C) = \left\{ \frac{g+(f)}{h+(f)} \mid g, h \in K[X, Y], h(\mathbf{p}) \neq 0 \right\} = \left\{ \frac{g+(f)}{h+(f)} \mid g, h \in K[X, Y], h(\mathbf{p}') \neq 0 \right\} = \mathcal{O}_{\mathbf{p}',K}(C).$$

Sei nun $\mathcal{O}_{\mathbf{p},K}(C) = \mathcal{O}_{\mathbf{p}',K}(C)$ und $h \in K[X, Y]$ mit $h(\mathbf{p}) \neq 0$. Dann ist

$$[h+(f)]^{-1} \in \mathcal{O}_{\mathbf{p},K}(C) = \mathcal{O}_{\mathbf{p}',K}(C), \quad \text{also} \quad [h+(f)]^{-1} = \frac{g_1+(f)}{h_1+(f)} \quad \text{mit} \quad g_1, h_1 \in K[X, Y] \quad \text{und} \quad h_1(\mathbf{p}') \neq 0.$$

Damit folgt $hg_1 + (f) = h_1 + (f)$, also $h(\mathbf{p}')g_1(\mathbf{p}') = h_1(\mathbf{p}') \neq 0$ und daher auch $h(\mathbf{p}') \neq 0$.

(b) Seien $x, y \in K[C]$ die Koordinatenfunktionen von C . Sei $\mathbf{p} = (\alpha, \beta) \in C$ und $\pi_{\mathbf{p}}: K[C] \rightarrow \overline{K}$ definiert durch $\pi_{\mathbf{p}}(\varphi) = \varphi(\mathbf{p})$ für alle $\varphi \in K[C]$. Dann ist $\pi_{\mathbf{p}}$ ein K -Algebrenhomomorphismus, $\text{Bi}(\pi_{\mathbf{p}}) = K[\alpha, \beta] = K(\alpha, \beta)$ ist ein Körper, und daher ist $\text{Ker}(\pi_{\mathbf{p}}) = \mathcal{M}_{\mathbf{p},K}(C) \cap K[C]$ ein maximales Ideal (siehe Satz 1.7.5).

Ist $\mathbf{p} \sim_K \mathbf{p}'$, so folgt $\mathcal{O}_{\mathbf{p},K}(C) = \mathcal{O}_{\mathbf{p}',K}(C)$, also $\mathcal{M}_{\mathbf{p},K}(C) = \mathcal{M}_{\mathbf{p}',K}(C)$ und

$$\mathcal{M}_{\mathbf{p},K}(C) \cap K[C] = \mathcal{M}_{\mathbf{p}',K}(C) \cap K[C].$$

Ist umgekehrt $\mathcal{M}_{\mathbf{p},K}(C) \cap K[C] = \mathcal{M}_{\mathbf{p}',K}(C) \cap K[C]$, so folgt

$$\begin{aligned} \mathcal{O}_{\mathbf{p},K}(C) &= \{\varphi^{-1}\psi \mid \psi \in K[C], \varphi \in K[C] \setminus \mathcal{M}_{\mathbf{p},K}(C)\} \\ &= \{\varphi^{-1}\psi \mid \psi \in K[C], \varphi \in K[C] \setminus \mathcal{M}_{\mathbf{p}',K}(C)\} = \mathcal{O}_{\mathbf{p}',K}(C) \end{aligned}$$

Nach (a) genügt es nun, zu zeigen, dass jedes maximale Ideal in $K[C]$ von der Form $\text{Ker}(\pi_{\mathbf{p}})$ mit $\mathbf{p} \in C$ ist. Sei also $\mathfrak{m} \subset K[C]$ ein maximales Ideal. Dann ist $K[C]/\mathfrak{m} = K[x+\mathfrak{m}, y+\mathfrak{m}]$ ein Körper, und nach Satz 3.7.3 ist $K[x+\mathfrak{m}, y+\mathfrak{m}]/K$ algebraisch. Daher gibt es einen K -Homomorphismus $\sigma: K[x+\mathfrak{m}, y+\mathfrak{m}] \rightarrow \overline{K}$, es sei $\pi: K[C] \rightarrow \overline{K}$ definiert durch $\pi(\varphi) = \sigma(\varphi+\mathfrak{m})$, $\alpha = \pi(x)$ und $\beta = \pi(y)$. π ist ein K -Algebrenhomomorphismus, $\text{Ker}(\pi) = \mathfrak{m}$, wegen $f(\alpha, \beta) = \pi(f(x, y)) = 0$ ist $\mathbf{p} = (\alpha, \beta) \in C$. Ist $\varphi = g(x, y) \in K[C]$ mit $g \in K[X, Y]$, so folgt $\pi(\varphi) = g(\pi(x), \pi(y)) = g(\alpha, \beta) = \varphi(\mathbf{p})$. Daher ist $\pi = \pi_{\mathbf{p}}$ und $\mathfrak{m} = \text{Ker}(\pi_{\mathbf{p}})$. \square

Lemma 3.9.3. Sei $\Gamma \subset \mathbb{P}_{\overline{K}}^2$ eine irreduzible projektive Kurve und $P \in \mathbb{P}_{K(\Gamma)/K}$. Dann gibt es ein affines Stück C von Γ mit $K[C] \subset \mathcal{O}_P$.

BEWEIS. Seien $\hat{x}, \hat{y}, \hat{z} \in K[\Gamma]$ die homogenen Koordinaten von Γ .

FALL 1: $\Gamma \in \{V_+(X), V_+(Y), V_+(Z)\}$. Wir betrachten den Fall $\Gamma = V_+(Z)$. Nach Bemerkung 2.6.4 besitzt Γ die affinen Stücke $C_1 = V_+(Z) \setminus V_+(X)$ und $C_2 = V_+(Z) \setminus V_+(Y)$, es ist $\hat{z} = 0$,

$$K[C_1] = K\left[\frac{\hat{y}}{\hat{x}}\right] \quad \text{und} \quad K[C_2] = K\left[\frac{\hat{x}}{\hat{y}}\right], \quad \text{und} \quad \frac{\hat{x}}{\hat{y}} \in \mathcal{O}_P \quad \text{oder} \quad \frac{\hat{y}}{\hat{x}} \in \mathcal{O}_P.$$

Daher ist $K[C_1] \subset \mathcal{O}_P$ oder $K[C_2] \subset \mathcal{O}_P$.

FALL 2: $\Gamma \notin \{V_+(X), V_+(Y), V_+(Z)\}$. Sind C_1, C_2, C_3 , so ist nach Bemerkung 2.6.4

$$K[C_1] = K\left[\frac{\hat{y}}{\hat{x}}, \frac{\hat{z}}{\hat{x}}\right] \subset K(\Gamma), \quad K[C_2] = K\left[\frac{\hat{x}}{\hat{y}}, \frac{\hat{z}}{\hat{y}}\right] \subset K(\Gamma) \quad \text{und} \quad K[C_3] = K\left[\frac{\hat{x}}{\hat{z}}, \frac{\hat{y}}{\hat{z}}\right] \subset K(\Gamma),$$

und wir nehmen an, es sei $K[C_1] \not\subset \mathcal{O}_P$, $K[C_2] \not\subset \mathcal{O}_P$ und $K[C_3] \not\subset \mathcal{O}_P$.

$$\text{FALL 1: } \frac{\hat{y}}{\hat{x}} \notin \mathcal{O}_P \implies \frac{\hat{x}}{\hat{y}} \in \mathcal{O}_P \implies \frac{\hat{z}}{\hat{y}} \notin \mathcal{O}_P \implies \frac{\hat{y}}{\hat{z}} \in \mathcal{O}_P \implies \frac{\hat{x}}{\hat{z}} = \frac{\hat{x}}{\hat{y}} \frac{\hat{y}}{\hat{z}} \in \mathcal{O}_P \implies K[C_3] \subset \mathcal{O}_P,$$

ein Widerspruch.

$$\text{FALL 2: } \frac{\hat{y}}{\hat{x}} \in \mathcal{O}_P \implies \frac{\hat{z}}{\hat{x}} \notin \mathcal{O}_P \implies \frac{\hat{x}}{\hat{z}} \in \mathcal{O}_P \implies \frac{\hat{y}}{\hat{z}} \notin \mathcal{O}_P \implies \frac{\hat{z}}{\hat{y}} \in \mathcal{O}_P \implies \frac{\hat{y}}{\hat{x}} \frac{\hat{z}}{\hat{y}} = \frac{\hat{z}}{\hat{x}} \in \mathcal{O}_P,$$

ebenfalls ein Widerspruch. \square

Satz 3.9.4. *Sei $\Gamma \subset \mathbb{P}_K^2$ eine über K definierte irreduzible projektive Kurve.*

1. Sei $\mathfrak{p} \in \Gamma$.

(a) *Es gibt eine Stelle $P \in \mathbb{P}_{K(\Gamma)/K}$ mit $\mathcal{M}_{\mathfrak{p},K}(\Gamma) \subset P$, und für jede solche Stelle P ist $\mathcal{M}_{\mathfrak{p},K}(\Gamma) = P \cap \mathcal{O}_{\mathfrak{p},K}(\Gamma)$.*

(b) *Sei \mathfrak{p} regulär über K . Dann ist $\mathcal{M}_{\mathfrak{p},K}(\Gamma) = P$, und genau dann ist $\mathfrak{p} \in \Gamma(K)$, wenn $\deg(P) = 1$.*

2. *Zu jeder Stelle $P \in \mathbb{P}_{K(\Gamma)/K}$ gibt es einen (bis auf K -Konjugierte eindeutig bestimmten) Punkt $\mathfrak{p} \in \Gamma$ mit $\mathcal{M}_{\mathfrak{p},K}(\Gamma) \subset P$.*

3. *Ist Γ regulär, so definiert die Zuordnung $\mathfrak{p} \mapsto \mathcal{M}_{\mathfrak{p},K}(\Gamma)$ bijektive Abbildungen*

$$\Psi: \Gamma/\sim_K \rightarrow \mathbb{P}_{K(\Gamma)/K} \quad \text{und} \quad \Psi^1: \Gamma(K) \rightarrow \mathbb{P}_{K(\Gamma)/K}^1.$$

BEWEIS. 1. Sei $\mathfrak{p} \in \Gamma$. Dann liegt \mathfrak{p} in einem affinen Stück C von Γ , und es ist $K(C) = K(\Gamma)$, $\mathcal{O}_{\mathfrak{p},K}(C) = \mathcal{O}_{\mathfrak{p},K}(\Gamma)$ und $\mathcal{M}_{\mathfrak{p},K}(C) = \mathcal{M}_{\mathfrak{p},K}(\Gamma)$. Daher können wir annehmen, dass $C \subset \overline{K}^2$ eine irreduzible über K definierte Kurve und $\mathfrak{p} \in C$ ist. Nach Satz 3.3.3 gibt es eine Stelle $P \in \mathbb{P}_{K(C)/K}$ mit $\mathcal{O}_{\mathfrak{p},K}(C) \subset \mathcal{O}_P$ und $\mathcal{M}_{\mathfrak{p},K}(C) \subset P$.

Sei nun $P \in \mathbb{P}_{K(C)/K}$ mit $\mathcal{M}_{\mathfrak{p},K}(C) \subset P$. Dann ist $\mathcal{M}_{\mathfrak{p},K}(C) \subset P \cap \mathcal{O}_{\mathfrak{p},K}(C)$, und da $\mathcal{M}_{\mathfrak{p},K}(C)$ ein maximales Ideal von $\mathcal{O}_{\mathfrak{p},K}(C)$ ist, folgt $\mathcal{M}_{\mathfrak{p},K}(C) = P \cap \mathcal{O}_{\mathfrak{p},K}(C)$. Ist \mathfrak{p} über K regulär, so ist $\mathcal{O}_{\mathfrak{p},K}(C)$ ein diskreter Bewertungsbereich, also nach Satz 3.3.2 ein maximaler Teilbereich von $K(C)$. Daher folgt $\mathcal{O}_{\mathfrak{p},K}(C) = \mathcal{O}_P$ und $\mathcal{M}_{\mathfrak{p},K}(C) = P$. Ist $\mathfrak{p} = (\alpha, \beta)$, so ist $\mathcal{O}_P/P = \mathcal{O}_{\mathfrak{p},K}(C)/\mathcal{M}_{\mathfrak{p},K}(C) \cong K(\alpha, \beta)$ nach Satz 1.7.5 und daher genau dann $\mathfrak{p} \in C(K)$ (also $\mathfrak{p} \in \Gamma(K)$), wenn $\deg(P) = 1$.

2. Sei $P \in \mathbb{P}_{K(\Gamma)/K}$. Nach Lemma 3.9.3 gibt es ein affines Stück $C \subset \Gamma$ mit $K[C] \subset \mathcal{O}_P$, und wir nehmen an, es sei $C = \Gamma \setminus V_+(Z)$, also $K[C] = K[x, y]$ mit $x = \hat{z}^{-1}\hat{x}$ und $y = \hat{z}^{-1}\hat{y}$. Wir zeigen:

A. $K[C] \cap P$ ist ein maximales Ideal von $K[C]$.

B. Ist $\mathfrak{p} \in C$, so ist genau dann $K[C] \cap P = K[C] \cap \mathcal{M}_{\mathfrak{p},K}(C)$, wenn $\mathcal{M}_{\mathfrak{p},K}(C) \subset P$.

Beweis von **A.** Sei $\pi: K[x, y] \hookrightarrow \mathcal{O}_P \rightarrow K(C)_P = \mathcal{O}_P/P$ definiert durch $\pi(\varphi) = \varphi(P) \in K(C)_P$. Dann ist $\text{Bi}(\pi) = K[x(P), y(P)] \subset K(C)_P$ ein Teilkörper, also $\text{Ker}(\pi) = K[C] \cap P$ ein maximales Ideal von $K[C]$. \square [**A.**]

Beweis von **B.** Sei $\mathfrak{p} \in C$. Sei zuerst $K[C] \cap P = K[C] \cap \mathcal{M}_{\mathfrak{p},K}(C)$ und $\gamma = \psi^{-1}\varphi \in \mathcal{M}_{\mathfrak{p},K}(C)$. Dann ist $\gamma = \psi^{-1}\varphi \in \mathcal{M}_{\mathfrak{p},K}(C)$ mit $\varphi, \psi \in K[C]$, $\varphi(\mathfrak{p}) = 0$ und $\psi(\mathfrak{p}) \neq 0$. Es folgt $\varphi \in \mathcal{M}_{\mathfrak{p},K}(C) \cap K[C] \subset P$, $\psi \in K[C] \setminus \mathcal{M}_{\mathfrak{p},K}(C) \subset \mathcal{O}_P \setminus P = \mathcal{O}_P^\times$ und daher $\gamma \in P$. \square [**B.**]

Sei nun $P \in \mathbb{P}_{K(\Gamma)/K}$ und $K[C] \subset \mathcal{O}_P$. Nach **A** ist $K[C] \cap P$ ein maximales Ideal von $K[C]$ und daher $K[C] \cap P = \mathcal{M}_{\mathfrak{p},K}(C) \cap K[C]$ für eine Punkt $\mathfrak{p} \in C$ nach Satz 3.9.2.3. Nun folgt $\mathcal{M}_{\mathfrak{p},K}(C) \subset P$ nach **B**.

Es bleibt zu zeigen, dass \mathfrak{p} bis auf K -Konjugierte eindeutig bestimmt ist. Sei also $\mathfrak{p}' \in \Gamma$ ein weiterer Punkt mit $\mathcal{M}_{\mathfrak{p}',K}(\Gamma) \subset P$. Ist $\mathfrak{p}' \in C$, so ist $K[C] \cap P = K[C] \cap \mathcal{M}_{\mathfrak{p}',K}(C) = K[C] \cap \mathcal{M}_{\mathfrak{p},K}(C)$ ein maximales Ideal von $K[C]$ nach **A** und **B** und daher $\mathfrak{p} \sim_K \mathfrak{p}'$ nach Satz 3.9.2.3. Wir nehmen nun an, es sei $\mathfrak{p}' \notin C$. Dann ist $\mathfrak{p}' = (\alpha:\beta:0)$ mit $(\alpha, \beta) \in \overline{K}^2 \setminus \{0\}$, und wir können $\alpha \neq 0$ annehmen. Dann ist die Funktion $\hat{x}^{-1}\hat{z} \in K(\Gamma)$ regulär in \mathfrak{p}' , und wegen $(\hat{x}^{-1}\hat{z})(\mathfrak{p}') = 0$ folgt $\hat{x}^{-1}\hat{z} \in \mathcal{O}_{\mathfrak{p}',K}(\Gamma) \subset P$. Nun ist aber $\hat{z}^{-1}\hat{x} \in \mathcal{O}_P$ und daher $1 = (\hat{x}^{-1}\hat{z})(\hat{z}^{-1}\hat{x}) \in P$, ein Widerspruch.

3. Klar nach 1., 2. und Satz 3.9.2. \square

Satz 3.9.5. Sei $C \subset \overline{K}^2$ eine über K definierte irreduzible Kurve, seien $x, y \in K[C]$ die Koordinatenfunktionen und $\mathfrak{p} = (\alpha, \beta) \in C(K)$ ein regulärer Punkt von C . Dann ist $\mathcal{O}_{\mathfrak{p}}(C)$ ein diskreter Bewertungsbereich, $P_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p},K}(C) = \mathcal{O}_{\mathfrak{p}}(C)(x - \alpha, y - \beta) \in \mathbb{P}_{K(C)}^1$, und es sei $v_{\mathfrak{p}} = v_{P_{\mathfrak{p}}}$ die zugehörige diskrete Bewertung von $K(C)$. Sei $L \subset \overline{K}^2$ eine über K definierte Gerade, $\mathfrak{p} \in L$, $(a, b) \in K^2 \setminus \{(0, 0)\}$ mit $L = V(a(X - \alpha) + b(Y - \beta))$ und $\varphi = y(x - \alpha) + b(y - \beta) \in K(C)$.

Dann ist $v_{\mathfrak{p}}(\varphi) \geq 1$, und genau dann ist $v_{\mathfrak{p}}(\varphi) \geq 2$, wenn L eine Tangente von C in \mathfrak{p} ist.

BEWEIS. Sei $\mathcal{J}_K(C) = (f)$ mit einem irreduziblem Polynom $f \in K[X, Y]$. Nach Satz 3.5.1 ist $\mathcal{O}_{\mathfrak{p}}(C)$ ein diskreter Bewertungsbereich, nach Satz 1.7.5 ist $\mathcal{M}_{\mathfrak{p},K}(C) = \mathcal{O}_{\mathfrak{p}}(C)(x - \alpha, y - \beta)$, und nach Satz 3.9.4 ist $P_{\mathfrak{p}} = \mathcal{M}_{\mathfrak{p},K}(C) \in \mathbb{P}_{K(C)}^1$. Wegen $1 = \min\{v_{\mathfrak{p}}(z) \mid z \in P_{\mathfrak{p}}\} = \min\{v_{\mathfrak{p}}(x - \alpha), v_{\mathfrak{p}}(y - \beta)\}$ folgt $v_{\mathfrak{p}}(\varphi) \geq 1$. Sei nun

$$a_0 = \frac{\partial f}{\partial X}(\mathfrak{p}), \quad b_0 = \frac{\partial f}{\partial Y}(\mathfrak{p}), \quad \text{und sei } a_0 \neq 0.$$

Dann ist $T = V(a_0(X - \alpha) + b_0(Y - \beta))$ die Tangente an C in \mathfrak{p} , und $f = a_0(X - \alpha) + b_0(Y - \beta) + f_2$ mit einem Polynom $f_2 \in K[X, Y]$, so dass $\text{ord}_{\mathfrak{p}}(f_2) \geq 2$. Wegen $0 = f(x, y) = a_0(x - \alpha) + b_0(y - \beta) + f_2(x, y)$ und $v_{\mathfrak{p}}(f_2(x, y)) \geq 2$ folgt $v_{\mathfrak{p}}(a_0(x - \alpha) + b_0(y - \beta)) \geq 2$. Wäre nun $v_{\mathfrak{p}}(y - \beta) \geq 2$, so folgte wegen $a_0 \neq 0$ auch $v_{\mathfrak{p}}(x - \alpha) \geq 2$, ein Widerspruch. Daher ist $v_{\mathfrak{p}}(y - \beta) = 1$.

Ist $L = T$, so gibt es ein $\lambda \in K^\times$ mit $a(X - \alpha) + b(Y - \beta) = \lambda[a_0(X - \alpha) + b_0(Y - \beta)]$, und es folgt $\varphi = \lambda[a_0(x - \alpha) + b_0(y - \beta)]$, also $v_{\mathfrak{p}}(\varphi) = v_{\mathfrak{p}}(a_0(x - \alpha) + b_0(y - \beta)) \geq 2$.

Ist $L \neq T$, so ist entweder $a = 0$, oder $a \neq 0$ und $a^{-1}b \neq a_0^{-1}b_0$. Ist $a = 0$, so ist $b \neq 0$, und wegen $\varphi = b(y - \beta)$ ist $v_{\mathfrak{p}}(\varphi) = v_{\mathfrak{p}}(y - \beta) = 1$. Ist $a \neq 0$, so folgt

$$\varphi = aa_0^{-1}[a_0(x - \alpha) + b_0(y - \beta)] + (b - aa_0^{-1}b_0)(y - \beta),$$

und wegen $b - aa_0^{-1}b_0 \neq 0$ ist $v_{\mathfrak{p}}(\varphi) = 1$. □

Divisoren, Differenziale und der Satz von Riemann-Roch

Im ganzen Kapitel sei L/K ein Funktionenkörper mit Konstantenkörper K .

4.1

Definition 4.1.1. Die von \mathbb{P}_L erzeugte freie abelsche Gruppe $\mathbb{D}_L = \mathbb{D}_{L/K}$ heißt *Divisorengruppe* von L/K , ihre Elemente heißen *Divisoren*.

Jedes $D \in \mathbb{D}_L$ hat eine eindeutige Darstellung als (formale) Summe

$$D = \sum_{P \in \mathbb{P}_L} n_P P \quad \text{mit} \quad n_P \in \mathbb{Z}, \quad n_P = 0 \quad \text{für fast alle } P \in \mathbb{P}_L, \quad \text{und es sei } v_P(D) = n_P \quad \text{für alle } P \in \mathbb{P}_L.$$

Für $D_1, D_2 \in \mathbb{D}_L$ sei $D_1 \leq D_2$, wenn $v_P(D_1) \leq v_P(D_2)$ für alle $P \in \mathbb{P}_L$. Die Null $0 \in \mathbb{D}_L$ heißt *Nulldivisor*.

Für zwei Divisoren D_1, D_2 ist $D_1 = D_2$ genau dann, wenn $v_P(D_1) = v_P(D_2)$ für alle $P \in \mathbb{P}_L$. Für $D \in \mathbb{D}_L$ ist genau dann $D = D_1 + D_2$, wenn $v_P(D) = v_P(D_1) + v_P(D_2)$ für alle $P \in \mathbb{P}_L$.

Für einen Divisor $D \in \mathbb{D}_L$ definieren wir seinen *Positivteil* $D_+ \in \mathbb{D}_L$, seinen *Negativteil* $D_- \in \mathbb{D}_L$, und seinen *Grad* $\deg(D) \in \mathbb{Z}$ durch

$$D_+ = \sum_{\substack{P \in \mathbb{P}_L \\ v_P(D) > 0}} v_P(D)P, \quad D_- = \sum_{\substack{P \in \mathbb{P}_L \\ v_P(D) < 0}} -v_P(D)P \quad \text{und} \quad \deg(D) = \sum_{P \in \mathbb{P}_L} v_P(D) \deg(P).$$

Offensichtlich ist $D = D_+ - D_-$, und $\deg: \mathbb{D}_L \rightarrow \mathbb{Z}$ ist ein Gruppenhomomorphismus. Die Gruppe $\mathbb{D}_L^0 = \text{Ker}(\deg)$ heißt *Divisorengruppe 0-ten Grades* von L/K .

Für $x \in L^\times$ sind nach Satz 3.7.2 die Mengen $\mathcal{N}(x) = \mathcal{N}^L(x)$ der Nullstellen und $\mathcal{P}(x) = \mathcal{P}^L(x)$ der Polstellen von x nicht-leere endliche Mengen. Man definiert den *Nullstellendivisor* $(x)_0 = (x)_0^L$ und den *Polstellendivisor* $(x)_\infty = (x)_\infty^L$ von x durch

$$(x)_0 = \sum_{P \in \mathcal{N}(x)} v_P(x)P \quad \text{und} \quad (x)_\infty = \sum_{P \in \mathcal{P}(x)} -v_P(x)P.$$

Der Divisor

$$(x) = (x)^L = (x)_0 - (x)_\infty = \sum_{P \in \mathbb{P}_L} v_P(x)P \quad \text{heißt} \quad \textit{Hauptdivisor} \quad \text{von } x.$$

Offensichtlich ist $(x)_0 = (x)_+$ und $(x)_\infty = (x)_-$. Die Abbildung $\partial: L^\times \rightarrow \mathbb{D}_L$, definiert durch $\partial(x) = (x) \in \mathbb{D}_L$, ist ein Gruppenhomomorphismus. Nach Satz 3.7.2 ist $\text{Ker}(\partial) = K^\times$. Die Gruppe $(L^\times) = \text{Bi}(\partial) = \{(x) \mid x \in L^\times\} \cong L^\times / K^\times$ heißt *Gruppe der Hauptdivisoren*, und die Faktorgruppe $\mathcal{C}_L = \mathcal{C}_{L/K} = \mathbb{D}_L / (L^\times)$ heißt *Divisorenklassengruppe* von L . Für $D \in \mathbb{D}_L$ heißt $[D] = D + (L^\times) \in \mathcal{C}_L$ die *Klasse* von D . Zwei Divisoren $D_1, D_2 \in \mathbb{D}_L$ heißen *linear äquivalent*, $D_1 \sim D_2$, wenn $[D_1] = [D_2]$ (äquivalent: $D_1 - D_2 \in (L^\times)$).

Für $D \in \mathbb{D}_L$ sei

$$\mathcal{L}(D) = \{x \in L^\times \mid (x) \geq -D\} \cup \{0\} = \{x \in L \mid v_P(x) + v_P(D) \geq 0 \text{ für alle } P \in \mathbb{P}_L\}$$

der Vielfachenraum von $-D$. $\mathcal{L}(D)$ ist ein endlich-dimensionaler K -Vektorraum (siehe Satz 4.1.2 und Satz 4.1.3). $\dim(D) = \dim_K \mathcal{L}(D)$ heißt *Dimension* von D .

Satz 4.1.2. *Seien $D, D' \in \mathbb{D}_L$.*

1. $\mathcal{L}(D)$ ist ein K -Vektorraum.
2. Ist $D \sim D'$, so folgt $\dim(D) = \dim(D')$.
3. $\mathcal{L}(0) = K$, und $\dim(0) = 1$.
4. Ist $D < 0$, so ist $\mathcal{L}(D) = \{0\}$, und $\dim(D) = 0$.
5. Die folgenden Aussagen sind äquivalent:
 - (a) $\dim(D) > 0$.
 - (b) Es gibt einen Divisor $D_1 \in \mathbb{D}_L$ mit $D_1 \sim D$ und $D_1 \geq 0$.

BEWEIS. 1. Sind $x, y \in \mathcal{L}(D)$ und $c \in K^\times$, so gilt für alle $P \in \mathbb{P}_L$:
 $v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(D)$ und $v_P(cx) = v_P(x) \geq -v_P(D)$, also $x+y \in \mathcal{L}(D)$ und $cx \in \mathcal{L}(D)$.

2. Sei $z \in L^\times$ mit $D = D' + (z)$. Ist $0 \neq x \in \mathcal{L}(D)$, so folgt $(xz) = (x) + (z) \geq -D + (z) = -D'$, also $xz \in \mathcal{L}(D')$. Daher definiert $x \mapsto xz$ einen K -Vektorraummonomorphismus $\mathcal{L}(D) \rightarrow \mathcal{L}(D')$, und es folgt $\dim(D) \leq \dim(D')$. Wegen der Symmetrie folgt Gleichheit.

3. Genau dann ist $x \in \mathcal{L}(0)$, wenn $v_P(x) \geq 0$ für alle $P \in \mathbb{P}_L$, wenn also $\mathcal{P}(x) = \emptyset$, also $x \in K$.

4. Ist $D < 0$ und $x \in \mathcal{L}(D)$, so ist $v_P(x) \geq 0$ für alle $P \in \mathbb{P}_L$, also $x \in K$, und $v_P(x) > 0$ für mindestens ein $P \in \mathbb{P}_L$, also $x = 0$.

5. (a) \Rightarrow (b) Sei $0 \neq x \in \mathcal{L}(D)$. Dann ist $(x) \geq -D$ und daher $D_1 = D + (x) \sim D$ und $D_1 \geq 0$.

(b) \Rightarrow (a) Sei $D_1 \in \mathbb{D}_L$ mit $D_1 \geq 0$ und $x \in L^\times$ mit $D_1 = D + (x)$. Dann ist $(x) \geq -D$ und daher $\mathcal{L}(D) \neq \{0\}$. \square

Satz 4.1.3. *Seien $D, D' \in \mathbb{D}_L$.*

1. $\dim(D) \leq \deg(D_+) + 1 < \infty$.
2. Ist $D \leq D'$, so ist $\mathcal{L}(D) \subset \mathcal{L}(D')$,

$$\dim_K(\mathcal{L}(D')/\mathcal{L}(D)) \leq \deg(D' - D) \quad \text{und} \quad \deg(D) - \dim(D) \leq \deg(D') - \dim(D').$$
3. Ist $D' \geq 0$, so ist $\dim(D + D') \leq \dim(D) + \deg(D')$.

BEWEIS. 1. und 2. Ist $D \leq D'$, so ist nach $-D' \leq -D$ und daher $\mathcal{L}(D) \subset \mathcal{L}(D')$. Für den Nachweis von $\dim_K(\mathcal{L}(D')/\mathcal{L}(D)) \leq \deg(D' - D)$ sei $D' = D + P_1 + \dots + P_r$ mit $r \in \mathbb{N}_0$ und $P_1, \dots, P_r \in \mathbb{P}_L$. Dann ist

$$\mathcal{L}(D') = \mathcal{L}(D + P_1 + \dots + P_r) \supset \mathcal{L}(D + P_1 + \dots + P_{r-1}) \supset \dots \supset \mathcal{L}(D + P_1) \supset \mathcal{L}(D),$$

also

$$\dim_K(\mathcal{L}(D')/\mathcal{L}(D)) = \sum_{i=1}^r \dim_K(\mathcal{L}(D + P_1 + \dots + P_i)/\mathcal{L}(D + P_1 + \dots + P_{i-1}))$$

und $\deg(D' - D) = \deg(P_1) + \dots + \deg(P_r)$. Daher genügt es, die Behauptung im Falle $D' = D + P$ mit $P \in \mathbb{P}_L$ zu zeigen. Der allgemeine Fall folgt dann durch Induktion nach r .

Sei also $D' = D + P$ mit $P \in \mathbb{P}_L$, und sei $t \in L$ mit $v_P(t) = v_P(D) + 1$. Ist $x \in \mathcal{L}(D + P)$, so folgt $v_P(xt) = v_P(x) + v_P(t) \geq -v_P(D + P) + v_P(D) + 1 = 0$, also $xt \in \mathcal{O}_P$, und wir definieren $\psi: \mathcal{L}(D + P) \rightarrow L_P$ durch $\psi(x) = (xt)(P)$. ψ ist ein K -Vektorraumhomomorphismus mit Kern

$\text{Ker}(\psi) = \{x \in \mathcal{L}(D+P) \mid v_P(xt) > 0\} = \{x \in \mathcal{L}(D+P) \mid v_P(x) \geq v_P(D)\} = \mathcal{L}(D)$ und induziert einen K -Vektorraummonomorphismus $\mathcal{L}(D+P)/\mathcal{L}(D) \rightarrow L_P$. Daher folgt

$$\dim_K(\mathcal{L}(D+P)/\mathcal{L}(D)) \leq \dim_K L_P = \deg(P).$$

Jetzt können wir 1. zeigen. Wegen $D \leq D_+$ und $\dim_K(\mathcal{L}(0)) = 1$ folgt

$$\dim(D) \leq \dim(D_+) = \dim_K(\mathcal{L}(D_+)/\mathcal{L}(0)) + \dim_K(\mathcal{L}(0)) \leq \deg(D_+) + 1.$$

Nun ist $\dim(D') - \dim(D) = \dim_K(\mathcal{L}(D')/\mathcal{L}(D)) \leq \deg(D' - D) = \deg(D') - \deg(D)$ und daher auch

$$\deg(D) - \dim(D) \leq \deg(D') - \dim(D').$$

3. Nach 2. ist $\dim(D+D') - \dim(D) = \dim_K(\mathcal{L}(D+D')/\mathcal{L}(D)) \leq \deg(D')$, und daher folgt $\dim(D+D') \leq \dim(D) + \deg(D')$. \square

4.2

Satz 4.2.1.

1. Sei $x \in L \setminus K$. Dann ist $\deg(x)_0 = \deg(x)_\infty = [L:K(x)]$, und es gibt einen Divisor $C \in \mathbb{D}_L$, so dass $C \geq 0$ und $\dim(l(x)_\infty + C) \geq (l+1)\deg(x)_\infty$ für alle $l \in \mathbb{N}_0$.
2. Für alle $x \in L^\times$ ist $\deg(x) = 0$, und für alle $D, D' \in \mathbb{D}_L$ mit $D \sim D'$ ist $\deg(D) = \deg(D')$.
3. Für $D \in \mathbb{D}_L^0$ sind die folgenden Aussagen äquivalent:

$$(a) \quad D \in (L^\times); \quad (b) \quad \dim(D) \geq 1; \quad (c) \quad \dim(D) = 1.$$

BEWEIS. 1. Sei $n = [L:K(x)]$, (u_1, \dots, u_n) eine $K(x)$ -Basis von L . Sei $C \in \mathbb{D}_L$, so dass $C \geq 0$ und $(u_i) \geq -C$ für alle $i \in [1, n]$, und sei $l \in \mathbb{N}_0$. Für alle $i \in [1, n]$ und $j \in [0, l]$ ist

$$(x^j u_i) = j(x)_0 - j(x)_\infty + (u_i) \geq -j(x)_\infty - C \geq -(l(x)_\infty + C),$$

also $x^j u_i \in \mathcal{L}(l(x)_\infty + C)$. Dann ist $\{x^j u_i \mid j \in [0, l], i \in [1, n]\}$ linear unabhängig über K , denn

aus $\sum_{i=1}^n \sum_{j=0}^l c_{j,i} x^j u_i = 0$ mit $c_{j,i} \in K$ folgt $\sum_{j=0}^l c_{j,i} x^j = 0$ für alle $i \in [1, n]$, also $c_{j,i} = 0$ für alle i, j .

Damit folgt

$$n(l+1) \leq \dim(l(x)_\infty + C) \leq \deg(l(x)_\infty + C) + 1 = l \deg(x)_\infty + \deg(C) + 1$$

nach Satz 4.1.3, da $l(x)_\infty + C \geq 0$, und wir erhalten $l[\deg(x)_\infty - n] \geq n - \deg(C) - 1$. Für $l \gg 1$ folgt daraus $\deg(x)_\infty \geq n$. Nach Satz 3.7.2 ist aber

$$\deg(x)_\infty = \sum_{\substack{P \in \mathbb{P}_L \\ v_P(x) < 0}} -v_P(x) \deg(P) = \sum_{\substack{P \in \mathbb{P}_L \\ v_P(x) < 0}} v_P(x^{-1}) \deg(P) \leq [L:K(x^{-1})] = n,$$

also $\deg(x)_\infty = n$, und daher auch $\dim(l(x)_\infty + C) \geq (l+1)n = (l+1)\deg(x)_\infty$ für alle $l \in \mathbb{N}_0$. Wegen $(x)_0 = (x^{-1})_\infty$ folgt auch $\deg(x)_0 = [L:K(x)]$.

2. Für $x \in L^\times$ ist $\deg(x) = \deg(x)_0 - \deg(x)_\infty = 0$ nach 1.

3. (a) \Rightarrow (b) Sei $D = (x)$ mit $x \in L^\times$. Wegen $(x^{-1}) = -D$ ist dann $x^{-1} \in \mathcal{L}(D)$, also $\dim(D) \geq 1$.

(b) \Rightarrow (c) und (c) \Rightarrow (a) Nach Satz 4.1.2 gibt es einen Divisor $D_1 \in \mathbb{D}_L$, so dass $D_1 \geq 0$ mit $D_1 \sim D$. Wegen $\deg(D_1) = \deg(D) = 0$ ist $D_1 = 0$, $\dim(D) = \dim(D_1) = 1$, und $D \in (L^\times)$. \square

Definition 4.2.2. Sei $\mathfrak{d} = [D] \in \mathcal{C}_L$ eine Divisorenklasse mit $D \in \mathbb{D}_L$. Dann definiert man ihren Grad und ihre Dimension durch

$$\deg(\mathfrak{d}) = \deg(D) \quad \text{und} \quad \dim(\mathfrak{d}) = \dim(D).$$

$\deg: \mathcal{C}_L \rightarrow \mathbb{Z}$ ist ein Gruppenepimorphismus. Sein Kern $\mathcal{C}_L^0 = C_{L/K}^0 = \{\mathfrak{d} \in \mathcal{C}_L \mid \deg(\mathfrak{d}) = 0\} = \mathbb{D}_L^0 / (L^\times)$ heißt *Divisorenklassengruppe 0-ten Grades*.

4.3

Definition und Satz 4.3.1 (Satz von Riemann).

1. $g_L = \sup\{\deg(D) - \dim(D) + 1 \mid D \in \mathbb{D}_L\} \in \mathbb{N}_0$. $g_L = g_{L/K}$ heißt *Geschlecht* von L/K .
Für $D \in \mathbb{D}_L$ ist $\dim(D) \geq \deg(D) - g_L + 1$, also $i(D) = \dim(D) - \deg(D) + g_L - 1 \geq 0$, und insbesondere $i(0) = g_L$.
 $i(D)$ heißt *Spezialitätsindex* von D .
2. Sei $D_0 \in \mathbb{D}_L$ mit $g_L = \deg(D_0) - \dim(D_0) + 1$. Ist dann $D \in \mathbb{D}_L$ und $\deg(D) \geq \deg(D_0) + g_L$, so folgt $\dim(D) = \deg(D) + 1 - g_L$, also $i(D) = 0$.

BEWEIS. 1. Nach Definition ist $g_L \geq \deg(0) - \dim(0) + 1 = 0$. Sei $x \in L \setminus K$ und $B = (x)_\infty$. Nach Satz 4.2.1 gibt es ein $C \in \mathbb{D}_L$, so dass $C \geq 0$ und $\dim(lB + C) \geq (l+1)\deg(B) \geq \deg(lB)$ für alle $l \in \mathbb{N}_0$. Für alle $l \in \mathbb{N}_0$ ist (nach Satz 4.1.3.6) $\dim(lB + C) \leq \dim(lB) + \deg(C)$ und daher

$$\deg(lB) - \dim(lB) \leq \deg(lB) - \dim(lB + C) + \deg(C) \leq \deg(C).$$

Wir zeigen nun: Für alle $D \in \mathbb{D}_L$ ist $\deg(D) - \dim(D) \leq \deg(C)$. Damit folgt dann $g_L < \infty$ und $\dim(D) \geq \deg(D) + 1 - g_L$ für alle $D \in \mathbb{D}_L$ nach Definition von g_L .

Sei $D \in \mathbb{D}_L$, und sei $C_1 \in \mathbb{D}_L$ mit $C_1 \geq 0$ und $C_1 \geq D$. Für alle $l \in \mathbb{N}_0$ ist dann (nach Satz 4.1.3.3) $\dim(lB) = \dim(lB - C_1 + C_1) \leq \dim(lB - C_1) + \deg(C_1)$ und daher

$$\dim(lB - C_1) \geq \dim(lB) - \deg(C_1) \geq \deg(lB) - \deg(C) - \deg(C_1) = l \deg(B) - \deg(C + C_1).$$

Wegen $\deg(B) > 0$ gibt es ein $l \in \mathbb{N}$ mit $\dim(lB - C_1) > 0$. Es sei $0 \neq z \in \mathcal{L}(lB - C_1)$ und $D_1 = C_1 - (z)$. Dann ist $D_1 \sim C_1$, und wegen $(z) \geq -lB + C_1$ ist $D_1 \leq C_1 + lB - C_1 = lB$. Wegen $D_1 \sim C_1$ und $D \leq C_1$ folgt mit Satz 4.1.3.2

$$\deg(D) - \dim(D) \leq \deg(C_1) - \dim(C_1) = \deg(D_1) - \dim(D_1) \leq \deg(lB) - \dim(lB) \leq \deg(C).$$

2. Sei $D \in \mathbb{D}_L$ mit $\deg(D) \geq \deg(D_0) + g_L$. Dann ist

$$\dim(D - D_0) \geq \deg(D - D_0) + 1 - g_L = \deg(D) - \deg(D_0) + 1 - g_L \geq 1,$$

es sei $0 \neq z \in \mathcal{L}(D - D_0)$ und $D' = D + (z)$. Dann ist $D' \geq D_0$, $D' \sim D$, und nach Satz 4.1.3 folgt $\deg(D) - \dim(D) = \deg(D') - \dim(D') \geq \deg(D_0) - \dim(D_0) = g_L - 1$ und daher

$$\dim(D) \leq \deg(D) - g_L + 1.$$

Mit 1. folgt die Gleichheit. □

4.4

Definition 4.4.1. Ein Vektor $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in L^{\mathbb{P}_L}$ heißt *Repartition* oder (*unvollständiges*) *Adel* von L/K , wenn $\alpha_P \in \mathcal{O}_P$ für fast alle (das heißt, bis auf endlich viele) $P \in \mathbb{P}_L$. $\mathbb{A}_L = \mathbb{A}_{L/K}$ bezeichne die Menge der Repartitionen von L/K . Versehen mit wertweiser Addition und Multiplikation, ist \mathbb{A}_L ein Ring.

Für $\alpha = (\alpha_P)_{P \in \mathbb{P}_L}$ und $Q \in \mathbb{P}_L$ sei $v_Q(\alpha) = v_Q(\alpha_Q) \in \mathbb{Z} \cup \{\infty\}$ [also $v_Q(\alpha) \geq 0$ für fast alle $Q \in \mathbb{P}_L$].

Für $x \in L$ ist $v_P(x) \geq 0$ für fast alle $P \in \mathbb{P}_L$ nach Satz 3.7.2, daher ist $(x)_{P \in \mathbb{P}_L} \in \mathbb{A}_L$, die Abbildung $x \mapsto (x)_{P \in \mathbb{P}_L}$ ist ein Ringmonomorphismus $L \rightarrow \mathbb{A}_L$, und für alle $Q \in \mathbb{P}_L$ ist $v_Q(x) = v_Q((x)_{P \in \mathbb{P}_L})$. Wir identifizieren $x \in L$ mit $(x)_{P \in \mathbb{P}_L} \in \mathbb{A}_L$ (damit wird $L \subset \mathbb{A}_L$ ein Teilring und \mathbb{A}_L eine L -Algebra).

Für $D \in \mathbb{D}_L$ sei $\mathbb{A}_L(D) = \{\alpha \in \mathbb{A}_L \mid v_P(\alpha) \geq -v_P(D) \text{ für alle } P \in \mathbb{P}_L\}$. Dann ist $\mathbb{A}_L(D) \subset \mathbb{A}_L$ ein K -Untervektorraum, und $\mathbb{A}_L(D) \cap L = \mathcal{L}(D)$.

Satz 4.4.2. *Seien $D, D_1, D_2 \in \mathbb{D}_L$ und $D_1 \leq D_2$.*

1. $\mathbb{A}_L(D_1) \subset \mathbb{A}_L(D_2)$, und $\dim_K(\mathbb{A}_L(D_2)/\mathbb{A}_L(D_1)) = \deg(D_2 - D_1)$.
2. $\dim_K(\mathbb{A}_L(D_2) + L/\mathbb{A}_L(D_1) + L) = (\deg(D_2) - \dim(D_2)) - (\deg(D_1) - \dim(D_1))$.
3. $i(D) = \dim_K(\mathbb{A}_L/\mathbb{A}_L(D) + L)$. Insbesondere folgt:
 $\dim(D) = \deg(D) + 1 - g_L + \dim_K(\mathbb{A}_L/\mathbb{A}_L(D) + L)$, und $g_L = i(0) = \dim_K(\mathbb{A}_L/\mathbb{A}_L(0) + L)$.

BEWEIS. 1. Nach Definition ist $\mathbb{A}_L(D_1) \subset \mathbb{A}_L(D_2)$, und wie im Beweis von Satz 4.1.3.5 genügt es, den Fall $D_2 = D_1 + Q$ mit $Q \in \mathbb{P}_L$ zu betrachten. Sei $t \in L$ mit $v_Q(t) = v_Q(D_1) + 1 = v_Q(D_2)$. Wir behaupten:

$$\varphi_0: \mathbb{A}_L(D_2) \rightarrow \mathcal{O}_Q, \quad \text{definiert durch } \varphi_0(\alpha) = t\alpha_Q,$$

ist ein K -Vektorraumepimorphismus.

Ist $\alpha \in \mathbb{A}_L(D_2)$, so ist $v_Q(t\alpha_Q) = v_Q(D_2) + v_Q(\alpha_Q) \geq 0$, also $t\alpha_Q \in \mathcal{O}_Q$, und daher ist $\varphi_0: \mathbb{A}_L(D_2) \rightarrow \mathcal{O}_Q$ ein K -Vektorraumhomomorphismus. Für den Nachweis der Surjektivität sei $z \in \mathcal{O}_Q$. Sei $\alpha_Q = t^{-1}z \in L$, und für alle $P \in \mathbb{P}_L \setminus \{Q\}$ sei $\alpha_P \in L$ mit $v_P(\alpha_P) = -v_P(D_2)$. Wegen $v_Q(\alpha_Q) \geq -v_Q(t) = -v_Q(D_2)$ und $v_P(\alpha_P) = 0$ für fast alle $P \in \mathbb{P}_L$ ist $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in \mathbb{A}_L(D_2)$ und $\varphi_0(\alpha) = z$.

φ_0 induziert einen K -Vektorraumepimorphismus $\varphi: \mathbb{A}_L(D_2) \rightarrow L_Q$, definiert durch $\varphi(\alpha) = (t\alpha_Q)(Q)$. Ist $\alpha \in \mathbb{A}_L(D_2)$, so ist genau dann $\varphi(\alpha) = 0$, wenn $v_Q(t\alpha_Q) \geq 1$, also $v_Q(\alpha) \geq -v_Q(t) + 1 = -v_Q(D_1)$. Für $P \in \mathbb{P}_L \setminus \{Q\}$ ist aber $v_P(\alpha) \geq -v_P(D_2) = -v_P(D_1)$. Daher ist $\text{Ker}(\varphi) = \mathbb{A}_L(D_1)$, φ induziert einen Isomorphismus $\mathbb{A}_L(D_2)/\mathbb{A}_L(D_1) \xrightarrow{\sim} L_Q$, und es folgt $\dim_K(\mathbb{A}_L(D_2)/\mathbb{A}_L(D_1)) = \dim_K L_Q = \deg(Q)$.

2. Der K -Vektorraumepimorphismus $\mathbb{A}_L(D_2) \rightarrow \mathbb{A}_L(D_2) + L/\mathbb{A}_L(D_1) + L$, $\alpha \mapsto \alpha + (\mathbb{A}_L(D_1) + L)$, induziert einen K -Vektorraumepimorphismus

$$\sigma_1: \mathbb{A}_L(D_2)/\mathbb{A}_L(D_1) \rightarrow \mathbb{A}_L(D_2) + L/\mathbb{A}_L(D_1) + L.$$

Die Abbildung $\tau: \mathcal{L}(D_2) \rightarrow \mathbb{A}_L(D_2)/\mathbb{A}_L(D_1)$, definiert durch $\tau(x) = x + \mathbb{A}_L(D_1)$, ist ein K -Vektorraumhomomorphismus mit $\text{Ker}(\tau) = \mathcal{L}(D_2) \cap \mathbb{A}_L(D_1) = \mathcal{L}(D_1)$ und $\text{Bi}(\tau) \subset \text{Ker}(\sigma_1)$. Es genügt nun, $\text{Bi}(\tau) = \text{Ker}(\sigma_1)$ zu zeigen, denn dann ist $\mathcal{L}(D_2)/\mathcal{L}(D_1) \cong \text{Ker}(\sigma_1)$ und

$$\begin{aligned} \dim_K(\mathbb{A}_L(D_2) + L/\mathbb{A}_L(D_1) + L) &= \dim_K(\mathbb{A}_L(D_2)/\mathbb{A}_L(D_1)) - \dim_K \mathcal{L}(D_2)/\mathcal{L}(D_1) \\ &= (\deg(D_2) - \dim(D_2)) - (\deg(D_1) - \dim(D_1)). \end{aligned}$$

Für den Nachweis von $\text{Ker}(\sigma_1) \subset \text{Bi}(\tau)$ sei $\alpha \in \mathbb{A}_L(D_2)$ mit $\alpha + \mathbb{A}_L(D_1) \in \mathbb{A}_L(D_1) + L$. Dann gibt es ein $x \in L$ mit $\alpha = x + \mathbb{A}_L(D_1)$. Für alle $P \in \mathbb{P}_L$ ist

$$v_P(x) \geq \min\{v_P(\alpha_P), v_P(\alpha_P - x)\} \geq \min\{-v_P(D_2), -v_P(D_1)\} = -v_P(D_2).$$

Also folgt $x \in \mathcal{L}(D_2)$ und $\alpha + \mathbb{A}_L(D_1) = \tau(x)$.

3. Sei zuerst $i(D) = 0$. Wir müssen $\mathbb{A}_L(D) + L = \mathbb{A}_L$ zeigen. Sei $\alpha \in \mathbb{A}_L$ und $D_1 \in \mathbb{D}_L$, so dass $D_1 \geq D$ und $\alpha \in \mathbb{A}_L(D_1)$. Nach Satz 4.1.2.3 und Satz 4.3.1.1 ist dann

$$\begin{aligned} \dim(D_1) &= \dim(D + (D_1 - D)) \leq \dim(D) + \deg(D_1 - D) \\ &= \deg(D_1) + \dim(D) - \deg(D) = \deg(D_1) + 1 - g_L \leq \dim(D_1), \end{aligned}$$

also $\dim(D_1) = \deg(D_1) + 1 - g_L$. Aus 2. folgt

$$\dim_K(\mathbb{A}_L(D_1) + L/\mathbb{A}_L(D) + L) = (\deg(D_1) - \dim(D_1)) - (\deg(D) - \dim(D)) = (g_L - 1) - (g_L - 1) = 0,$$

also $\mathbb{A}_L(D) + L = \mathbb{A}_L(D_1) + L$ und daher $\alpha \in \mathbb{A}_L(D) + L$.

Sei nun $D \in \mathbb{D}_L$ beliebig. Nach Satz 4.3.1 gibt es ein $D_1 \in \mathbb{D}_L$ mit $D_1 \geq D$ und $i(D) = 0$. Dann ist nach dem eben Bewiesenen $\mathbb{A}_L = \mathbb{A}_L(D_1) + L$, und es folgt

$$\begin{aligned} \dim_K(\mathbb{A}_L/\mathbb{A}_L(D) + L) &= \dim_K(\mathbb{A}_L(D_1) + L/\mathbb{A}_L(D) + L) \\ &= (\deg(D_1) - \dim(D_1)) - (\deg(D) - \dim(D)) = g_L - 1 + \dim(D) - \deg(D) = i(D). \quad \square \end{aligned}$$

4.5

Definitionen und Bemerkungen 4.5.1. Für $D \in \mathbb{D}_L$ sei $\Omega_L(D)$ die Menge aller K -Vektorraumhomomorphismen $\omega: \mathbb{A}_L \rightarrow K$ mit $\omega|_{\mathbb{A}_L(D) + L} = 0$. $\Omega_L(D) \subset \text{Hom}_K(\mathbb{A}_L, K)$ ist ein K -Untervektorraum, und

$$\Omega_L(D) \cong \text{Hom}_K(\mathbb{A}_L/\mathbb{A}_L(D) + L, K), \quad \text{also} \quad \dim_K(\Omega_L(D)) = \dim_K(\mathbb{A}_L/\mathbb{A}_L(D) + L) = i(D).$$

Für $D, D' \in \mathbb{D}_L$ mit $D' \leq D$ ist $\mathbb{A}_L(D') + L \subset \mathbb{A}_L(D) + L$ und daher $\Omega_L(D) \subset \Omega_L(D')$. Da es zu je zwei Divisoren $D_1, D_2 \in \mathbb{D}_L$ ein $D \in \mathbb{D}_L$ gibt mit $D \leq D_1$ und $D \leq D_2$, ist $\{\Omega_L(D) \mid D \in \mathbb{D}_L\}$ eine gerichtete Menge von K -Untervektorräumen von $\text{Hom}_K(\mathbb{A}_L, K)$, und

$$\Omega_L = \Omega_{L/K} = \bigcup_{D \in \mathbb{D}_L} \Omega_L(D) \subset \text{Hom}_K(\mathbb{A}_L, K)$$

ist ein K -Vektorraum. Die $\omega \in \Omega_L$ heißen (*Weil'sche*) *Differenziale* von L/K . Für alle $\omega \in \Omega_L$ ist $\omega|_L = 0$, und für $D \in \mathbb{D}_L$ ist $\Omega_L(D) = \{\omega \in \Omega_L \mid \omega|_{\mathbb{A}_L(D)} = 0\}$.

Für $\omega \in \Omega_L$ und $x \in L$ sei $x\omega: \mathbb{A}_L \rightarrow K$ definiert durch $(x\omega)(\alpha) = \omega(x\alpha)$. Dann ist $x\omega \in \Omega_L$, und vermöge $(x, \omega) \mapsto x\omega$ ist Ω_L ein L -Vektorraum.

Genauer gilt: Sind $B, D \in \mathbb{D}_L$, $\omega \in \Omega_L(D)$ und $x \in \mathcal{L}(B)$. Dann ist $x\omega \in \Omega_L(D - B)$. [Beweis: Wir müssen $x\omega|_{\mathbb{A}_L(D - B) + L} = 0$ zeigen. Sei $\alpha = \beta + z \in \mathbb{A}_L(D - B) + L$ mit $\beta \in \mathbb{A}_L(D - B)$ und $z \in L$. Für $P \in \mathbb{P}_L$ ist dann

$$v_P(x\beta) = v_P(x) + v_P(\beta) \geq -v_P(B) - v_P(D - B) = -v_P(D),$$

also $x\alpha = x\beta + xz \in \mathbb{A}_L(D) + L$ und daher $x\omega(\alpha) = \omega(x\alpha) = 0$.]

Insbesondere gilt: Aus $\omega \in \Omega_L(D)$ und $x \in L^\times$ folgt $x\omega \in \Omega_L(D + (x))$ [wegen $x \in \mathcal{L}(-(x))$].

Definition und Satz 4.5.2.

1. $\dim_L(\Omega_L) = 1$.
2. Sei $0 \neq \omega \in \Omega_L$. Dann gibt es genau einen Divisor $W \in \mathbb{D}_L$, so dass für alle $D \in \mathbb{D}_L$ gilt:
 - * Genau dann ist $\omega \in \Omega_L(D)$, wenn $D \leq W$

$W = (\omega)$ heißt *Divisor von ω* .

Sei $\omega \in \Omega_L$. Für $P \in \mathbb{P}_L$ sei $v_P(\omega) = v_P((\omega))$, falls $\omega \neq 0$, und $v_P(0) = \infty$. Eine Stelle $P \in \mathbb{P}_L$ heißt *Nullstelle* von ω , wenn $v_P(\omega) > 0$, und *Polstelle* von ω , wenn $v_P(\omega) < 0$. ω heißt *regulär in P* , wenn $v_P(\omega) \geq 0$. ω heißt *global regulär* oder *holomorph*, wenn ω in jeder Stelle $P \in \mathbb{P}_L$ regulär ist.

Ein Divisor $W \in \mathbb{D}_L$ heißt *kanonischer Divisor*, wenn $W = (\omega)$ für ein $\omega \in \Omega_L$.

3. Für $D \in \mathbb{D}_L$ ist $\Omega_L(D) = \{\omega \in \Omega_L \mid \omega \neq 0, (\omega) \geq D\} \cup \{0\}$. Insbesondere ist $\Omega_L(0)$ die Menge der holomorphen Differenziale, und $\dim_K \Omega_L(0) = g_L$.
4. Für $x \in L^\times$ und $0 \neq \omega \in \Omega_L$ ist $(x\omega) = (x) + (\omega)$.

Eine Divisorenklasse $\mathfrak{w} \in \mathcal{C}_L$ heißt *kanonische Klasse*, wenn $\mathfrak{w} = [W]$ für einen kanonischen Divisor $W \in \mathbb{D}_L$.

Insbesondere gibt es genau eine kanonische Klasse; diese ist die Menge aller kanonischen Divisoren.

5. Sei $D \in \mathbb{D}_L$, $0 \neq \omega \in \Omega_L$ und $W = (\omega)$. Dann ist die Abbildung

$$\mu: \mathcal{L}(W - D) \rightarrow \Omega_L(D), \quad \text{definiert durch } \mu(x) = x\omega,$$

ein K -Vektorraumisomorphismus.

BEWEIS. 1. Seien $\omega_1, \omega_2 \in \Omega_L \setminus \{0\}$. Wir zeigen, dass es ein $x \in L^\times$ gibt mit $\omega_2 = x\omega_1$. Für $i \in \{1, 2\}$ sei $D_i \in \mathbb{D}_L$ mit $\omega_i \in \Omega_L(D_i)$. Für einen Divisor $B \in \mathbb{D}_L$ und $i \in \{1, 2\}$ sei

$$\varphi_i: \mathcal{L}(D_i + B) \rightarrow \Omega_L(-B) \quad \text{definiert durch } \varphi_i(x) = x\omega_i, \quad \text{und } U_i = \varphi_i(\mathcal{L}(D_i + B)) \subset \Omega_L(-B).$$

φ_i ist ein K -Vektorraummonomorphismus, $U_i \subset \Omega_L(-B)$ ist ein K -Untervektorraum, und

$$\dim_K(U_1 + U_2) = \dim_K(U_1) + \dim_K(U_2) - \dim_K(U_1 \cap U_2) \leq \dim_K(\Omega_L(-B)) = i(-B).$$

Ist nun $B \geq 0$, so folgt $i(-B) = \dim(-B) - \deg(-B) + g_L - 1 = \deg(B) + g_L - 1$. Ist außerdem $\deg(B) \gg 1$, so folgt nach Satz 4.3.1

$$\begin{aligned} \dim_K(U_1 \cap U_2) &\geq \dim(D_1 + B) + \dim(D_2 + B) - i(-B) \\ &= [\deg(D_1 + B) + 1 - g_L] + [\deg(D_2 + B) + 1 - g_L] - [\deg(B) + g_L - 1] \\ &= \deg(B) + \deg(D_1 + D_2) + 3(1 - g_L) > 0. \end{aligned}$$

Daher existieren $x_1 \in \mathcal{L}(D_1 + B) \setminus \{0\}$ und $x_2 \in \mathcal{L}(D_2 + B) \setminus \{0\}$ mit $\varphi_1(x_1) = \varphi_2(x_2)$, also $x_1\omega_1 = x_2\omega_2$ und daher $\omega_2 = (x_2^{-1}x_1)\omega_1$.

2. Nach Satz 4.3.1 gibt es ein $c \in \mathbb{N}$, so dass $i(D) = 0$ für alle $D \in \mathbb{D}_L$ mit $\deg(D) \geq c$. Ist nun $0 \neq \omega \in \Omega_L(D)$, so ist $1 \leq \dim_K \Omega_L(D) = i(D)$, also $\deg(D) < c$, und daher gibt es einen Divisor W maximalen Grades mit $\omega \in \Omega_L(W)$, und wir zeigen, dass W die gewünschte Eigenschaft hat (die Eindeutigkeit ist offensichtlich).

Sei also $D \in \mathbb{D}_L$, $\omega \in \Omega_L(D)$, und es sei $D \not\leq W$. Dann gibt es ein $Q \in \mathbb{P}_L$ mit $v_Q(D) > v_Q(W)$, und wir zeigen $\omega|_{\mathbb{A}_L(Q+W)} = 0$ (das ist dann ein Widerspruch zur Maximalität von $\deg(W)$). Sei also $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in \mathbb{A}_L(Q+W)$. Dann ist $\alpha = \alpha' + \alpha''$ mit

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

Dann ist $\alpha' \in \mathbb{A}_L(W)$, $\alpha'' \in \mathbb{A}_L(D)$, und daher $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$.

3. Nach Definition.

4. Sei $x \in L^\times$ und $0 \neq \omega \in \Omega_L$. Dann ist $\omega \in \Omega_L((\omega))$, also $x\omega \in \Omega_L((\omega) + (x))$ und daher $(x\omega) \geq (x) + (\omega)$. Mit x^{-1} an Stelle von x folgt $(\omega) = (x^{-1}(x\omega)) \geq (x^{-1}) + (x\omega) = -(x) + (x\omega)$ und daher $(x\omega) \leq (x) + (\omega)$.

5. Ist $0 \neq x \in \mathcal{L}(W - D)$, so ist $x\omega \in \Omega_L(W - (W - D)) = \Omega_L(D)$. Offensichtlich ist μ ein K -Vektorraummonomorphismus. Zum Nachweis der Surjektivität sei $0 \neq \omega_1 \in \Omega_L(D)$. Nach 1. gibt es ein $\omega \in \Omega_L \setminus \{0\}$ mit $\omega_1 = x\omega$, und es folgt $(x) = (\omega_1) - (\omega) \geq D - W$, also $x \in \mathcal{L}(W - D)$ und $\omega_1 = \mu(x)$. \square

4.6

Satz 4.6.1 (Satz von Riemann-Roch). Sei $W \in \mathbb{D}_L$ ein kanonischer Divisor und $D \in \mathbb{D}_L$.

1. $i(D) = \dim(W - D)$ (also $\dim(D) = \deg(D) + 1 - g_L + \dim(W - D)$).
2. $\deg(W) = 2g_L - 2$ und $\dim(W) = g_L$.
3. Ist $\deg(D) \geq 2g_L - 1$, so ist $i(D) = 0$ (also $\dim(D) = \deg(D) + 1 - g_L$ und $\mathbb{A}_L = \mathbb{A}_L(D) + L$).
4. D ist genau dann ein kanonischer Divisor, wenn $\deg(D) = 2g_L - 2$ und $\dim(D) \geq g_L$.

BEWEIS. 1. Nach Satz 4.5.2.5 ist $\mu: \mathcal{L}(W - D) \rightarrow \Omega_L(D)$ ein K -Vektorraumisomorphismus und daher $i(D) = \dim_K \Omega_L(D) = \dim_K \mathcal{L}(W - D) = \dim(W - D)$.

2. Nach 1. ist $g_L = i(0) = \dim(W) = \deg(W) + 1 - g_L + \dim(0) = \dim(W) + 2 - g_L$.

3. Ist $\deg(D) \geq 2g - 1$, so folgt $\deg(W - D) < 0$ und daher $i(D) = \dim(W - D) = 0$.

4. Ist D kanonisch, so ist $D \sim W$ und daher $\deg(D) = 2g_L - 2$ und $\dim(D) = g_L$. Sei also $\deg(D) = 2g_L - 2$ und $\dim(D) \geq g_L$. Dann folgt

$$g_L \leq \dim(D) = \deg(D) + 1 - g_L + \dim(W - D) = g_L - 1 + \dim(W - D),$$

also $\dim(W - D) \geq 1$ und $\deg(W - D) = 0$. Nach Satz 4.2.1 ist $W - D \in \mathbb{H}_L$, also $D \sim W$ und daher D kanonisch. \square

Satz 4.6.2 (Starker Approximationsatz). *Sei $r \in \mathbb{N}_0$, und seien $P_0, P_1, \dots, P_r \in \mathbb{P}_L$ verschieden. Seien $x_1, \dots, x_r \in L$ und $n_1, \dots, n_r \in \mathbb{Z}$. Dann gibt es ein $x \in L$, so dass $v_{P_i}(x - x_i) = n_i$ für alle $i \in [1, r]$, und $v_P(x) \geq 0$ für alle $P \in \mathbb{P}_L \setminus \{P_0, \dots, P_r\}$.*

Insbesondere gilt: Es gibt ein $x \in L^\times$, so dass P_0 die einzige Polstelle von x (und die einzige Nullstelle von x^{-1}) ist.

BEWEIS. Sei $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in \mathbb{A}_L$ mit $\alpha_{P_i} = x_i$ für alle $i \in [1, r]$ und $\alpha_P = 0$ für alle $P \in \mathbb{P}_L \setminus \{P_1, \dots, P_r\}$. Für $m \in \mathbb{N}$ sei

$$D_m = mP_0 - \sum_{i=1}^r (n_i + 1)P_i \in \mathbb{D}_L,$$

und es sei m so groß, dass $\deg(D_m) \geq 2g_L - 1$. Nach Satz 4.6.1 ist dann $\mathbb{A}_L = \mathbb{A}_L(D_m) + L$, und daher gibt es ein $z \in L$ mit $z - \alpha \in \mathbb{A}_L(D_m)$. Für alle $i \in [1, r]$ ist dann $v_{P_i}(z - x_i) \geq n_i + 1$, und für alle $P \in \mathbb{P}_L \setminus \{P_0, \dots, P_r\}$ ist $v_P(z) \geq 0$.

Für $i \in [1, r]$ sei $y_i \in L$ mit $v_{P_i}(y_i) = n_i$. Obiges Argument (mit y_i an Stelle von x_i) beweist die Existenz eines $y \in L$, so dass $v_{P_i}(y - y_i) \geq n_i + 1$ für alle $i \in [1, r]$ und $v_P(y) \geq 0$ für alle $P \in \mathbb{P}_L \setminus \{P_0, \dots, P_r\}$. Ist nun $x = y + z$, so folgt $x - x_i = (z - x_i) + (y - y_i) + y_i$ und daher $v_{P_i}(x - x_i) = n_i$ für alle $i \in [1, r]$, und $v_P(x) \geq \min\{v_P(y), v_P(z)\} \geq 0$ für alle $P \in \mathbb{P}_L \setminus \{P_0, \dots, P_r\}$. Im Falle $r = 0$ ist P_0 die einzige Polstelle von x . \square

Satz 4.6.3 (Kennzeichnung rationaler Funktionenkörper). *Die folgenden Aussagen sind äquivalent:*

- (a) L/K ist ein rationaler Funktionenkörper (also $L = K(x)$ mit über K transzendentem x).
- (b) $g_L = 0$ und $\mathbb{P}_L^1 \neq \emptyset$.

Ist L/K ein rationaler Funktionenkörper und $P \in \mathbb{P}_L^1$, so ist $-2P$ ein kanonischer Divisor.

BEWEIS. (a) \Rightarrow (b) Sei $L = K(x)$. Für jedes normierte irreduzible Polynom $p \in K[x]$ sein $P_p \in \mathbb{P}_L$ die zugehörige Stelle, und $P_\infty \in \mathbb{P}_L$ sei die unendliche Stelle. Dann ist $v_{P_x}(x) = 1$, $v_{P_\infty}(x) = -1$ und $v_P(x) = 0$ für alle $P \in \mathbb{P}_L \setminus \{P_x, P_\infty\}$, also $(x)_0 = P_x$, $(x)_\infty = P_\infty$, und $\deg(P_x) = \deg(P_\infty) = 1$.

Sei nun $r \in \mathbb{N}$. Für $n \in [0, r]$ ist $(x^n) = n(x)_0 - n(x)_\infty \geq -r(x)_\infty$, also $x^n \in \mathcal{L}(r(x)_\infty)$. Da $(1, x, \dots, x^r)$ über K linear unabhängig ist, folgt $r + 1 \leq \dim(r(x)_\infty)$, und für $r \gg 1$ ist nach Satz 4.3.1 $\dim(r(x)_\infty) = \deg(r(x)_\infty) + 1 - g_L = r + 1 - g_L$, und es folgt $g_L = 0$.

(b) \Rightarrow (a) Sei $P \in \mathbb{P}_L$ mit $\deg(P) = 1$. Wegen $\deg(P) \geq 2g - 1$ folgt $\dim(P) = \deg(P) + 1 - g = 2$ nach Satz 4.6.1, also $\mathcal{L}(P) \supseteq K$. Ist $x \in \mathcal{L}(P) \setminus K$, so ist $(x) \geq -P$ und $(x) \neq 0$, also $(x)_\infty = P$ und $[L:K(x)] = \deg(x)_\infty = \deg(P) = 1$. Damit folgt $L = K(x)$.

Ist L/K ein rationaler Funktionenkörper, $P \in \mathbb{P}_L$ und $\deg(P) = 1$, so ist $\deg(-2P) = -2 = 2g_L - 2$ und $\dim(-2P) = 0 = g_L$. Nach Satz 4.6.1.4 ist $-2P$ kanonisch. \square

4.7

Definition 4.7.1. Sei $P \in \mathbb{P}_L$.

1. Die *lokale Einbettung* $\iota_P: L \rightarrow \mathbb{A}_L$ sei definiert durch

$$\iota_P(x) = (\iota_P(x)_Q)_{Q \in \mathbb{P}_L} \quad \text{mit} \quad \iota_P(x)_Q = \begin{cases} x, & \text{falls } P = Q, \\ 0, & \text{falls } P \neq Q. \end{cases}$$

ι_P ist ein L -Algebrenmonomorphismus.

2. Sei $\omega \in \Omega_L$. Dann heißt der K -Vektorraumhomomorphismus $\omega_P = \omega \circ \iota_P: L \rightarrow K$ die *lokale Komponente* und das Element $\text{res}_P(\omega) = \omega_P(1) \in K$ das *Residuum* von ω an der Stelle P .

Satz 4.7.2. Sei $\omega \in \Omega_L$.

1. Sei $P \in \mathbb{P}_L$. Für alle $x, z \in L$ ist dann $(x\omega)_P(z) = \omega_P(xz)$, $\text{res}_P(x\omega) = \omega_P(x)$, und $\text{res}_P: \Omega_L \rightarrow K$ ist ein K -Vektorraumhomomorphismus.
2. Sei $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in \mathbb{A}_L$. Dann ist $\omega_P(\alpha_P) = 0$ für fast alle $P \in \mathbb{P}_L$, $\text{res}_P(\omega) = 0$ für fast alle $P \in \mathbb{P}_L$,

$$\omega(\alpha) = \sum_{P \in \mathbb{P}_L} \omega_P(\alpha_P) \quad \text{und} \quad \sum_{P \in \mathbb{P}_L} \text{res}_P(\omega) = 0.$$

3. Ist $\omega \neq 0$ und $P \in \mathbb{P}_L$, so folgt $\omega_P \neq 0$, und $v_P(\omega) = \max\{r \in \mathbb{Z} \mid \omega_P \upharpoonright \mathcal{L}(rP) = 0\}$.
4. Sei $P \in \mathbb{P}_L^1$ und $v_P(\omega) \geq -1$. Dann ist $\text{res}_P(x\omega) = \omega_P(x) = x(P) \text{res}_P(\omega)$ für alle $x \in \mathcal{O}_P$. Insbesondere ist genau dann $\text{res}_P(\omega) = 0$, wenn $v_P(\omega) \geq 0$.

BEWEIS. Sei $\omega \neq 0$ und $W = (\omega)$.

1. Für $x, z \in L$ ist $(x\omega)_P(z) = (x\omega)(\iota_P(z)) = \omega(x\iota_P(z)) = \omega(\iota_P(xz)) = \omega_P(xz)$ und daher $\text{res}_P(x\omega) = (x\omega)_P(1) = \omega_P(x)$.

Ist $\omega' \in \Omega_L$ und $x \in K$, so folgt $\text{res}_P(\omega + \omega') = (\omega + \omega') \circ \iota_P(1) = \omega \circ \iota_P(1) + \omega' \circ \iota_P(1) = \text{res}_P(\omega) + \text{res}_P(\omega')$, und $\text{res}_P(x\omega) = (x\omega)_P(1) = \omega_P(x) = x\omega_P(1) = x \text{res}_P(\omega)$.

2. Sei $S = \{P \in \mathbb{P}_L \mid v_P(W) \neq 0 \text{ oder } v_P(\alpha_P) < 0\}$. Dann ist $S \subset \mathbb{P}_L$ endlich, und wir definieren $\beta = (\beta_P)_{P \in \mathbb{P}_L}$ durch $\beta_P = \alpha_P$, falls $P \notin S$, und $\beta_P = 0$, falls $P \in S$. Für $P \notin S$ ist dann $v_P(\beta_P) = v_P(\alpha_P) \geq 0 = -v_P(W)$, und für $P \in S$ ist $v_P(\beta_P) = \infty \geq -v_P(W)$. Daher ist $\beta \in \mathbb{A}_L(W)$, und für alle $P \notin S$ ist $\iota_P(\alpha_P) \in \mathbb{A}_L(W)$. Damit folgt $\omega(\beta) = 0$, $\omega(\iota_P(\alpha_P)) = 0$ für alle $P \notin S$, und

$$\alpha = \beta + \sum_{P \in S} \iota_P(\alpha_P), \quad \text{also} \quad \omega(\alpha) = \omega(\beta) + \sum_{P \in S} \omega(\iota_P(\alpha_P)) = \sum_{P \in \mathbb{P}_L} \omega_P(\alpha_P).$$

Insbesondere ist

$$\sum_{P \in \mathbb{P}_L} \text{res}_P(\omega) = \sum_{P \in \mathbb{P}_L} \omega_P(1) = \omega(1) = 0, \quad \text{da} \quad \omega \upharpoonright L = 0.$$

3. Sei $r = v_P(W)$. Ist $x \in \mathcal{L}(rP)$, so ist $v_P(x) \geq -r = -v_P(W)$, also $\iota_P(x) \in \mathbb{A}_L(W)$ und daher $\omega_P(x) = \omega(\iota_P(x)) = 0$. Nach Definition von W gibt es ein $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in \mathbb{A}_L(W + P)$ mit $\omega(\alpha) \neq 0$. Wegen $\alpha \notin \mathbb{A}_L(W)$ ist $v_P(\alpha_P) = -(r+1)$ und daher $\alpha_P \in \mathcal{L}((r+1)P)$. Wegen $\alpha = \alpha - \iota_P(\alpha_P) + \iota_P(\alpha_P)$ und $\alpha - \iota_P(\alpha_P) \in \mathbb{A}_L(W)$ folgt $0 \neq \omega(\alpha) = \omega(\alpha - \iota_P(\alpha_P)) + \omega(\iota_P(\alpha_P)) = \omega_P(\alpha_P)$. Also ist $\omega_P \upharpoonright \mathcal{L}((r+1)P) \neq 0$ und daher auch $\omega_P \upharpoonright \mathcal{L}(sP) \neq 0$ für alle $s > r$. Insbesondere ist $\omega_P \neq 0$.

4. Sei $\deg(P) = 1$ (also $L_P = K$), $x \in \mathcal{O}_P$ und $v_P(\omega) \geq -1$. Dann ist $v_P(x - x(P)) \geq 1$, also $x - x(P) \in \mathcal{L}(-P)$, und wegen $v_P(\omega) \geq -1$ folgt $\omega_P(x - x(P)) = 0$. Daher ist

$$\text{res}_P(x\omega) = \omega_P(x) = \omega_P(x - x(P)) + \omega_P(x(P)) = x(P)\omega_P(1) = x(P) \text{res}_P(\omega).$$

Genau dann ist $\text{res}_P(\omega) = \omega_P(1) = 0$, wenn $\omega_P \upharpoonright K = 0$, und das ist wegen $K = \mathcal{L}(0)$ nach 3. genau dann der Fall, wenn $v_P(\omega) \geq 0$. \square

Satz 4.7.3. *Seien $P_1, \dots, P_n \in \mathbb{P}_L^1$ verschieden. Dann gibt es ein $\eta \in \Omega_L$, so dass $v_{P_i}(\eta) = -1$ und $\text{res}_{P_i}(\eta) = 1$ für alle $i \in [1, n]$.*

BEWEIS. Sei $0 \neq \omega \in \Omega_L$. Nach Satz 3.6.7 gibt es ein $z \in L$, so dass $v_{P_i}(z) = -v_{P_i}(\omega) - 1$ und daher $v_{P_i}(z\omega) = -1$ für alle $i \in [1, n]$. Nach Satz 4.7.2 ist dann $a_i = \text{res}_{P_i}(z\omega) \neq 0$, und nach Satz 3.6.7 gibt es ein $y \in L$ mit $v_{P_i}(y - a_i) > 0$ für alle $i \in [1, n]$. Damit folgt $y(P_i) = a_i$, $v_{P_i}(y) = 0$, $v_{P_i}(y^{-1}z\omega) = -v_{P_i}(y) + v_{P_i}(z\omega) = -1$ und $\text{res}_{P_i}(y^{-1}z\omega) = y^{-1}(P_i) \text{res}_{P_i}(z\omega) = a_i^{-1} \text{res}_{P_i}(z\omega) = 1$. \square

Algebraisch-geometrische Codes

Im diesem Kapitel sei q eine Primzahlpotenz, \mathbb{F}_q ein Körper mit q Elementen, und wir schreiben \dim an Stelle von $\dim_{\mathbb{F}_q}$.

5.1

Definition 5.1.1. Sei $n \in \mathbb{N}$. Für $\mathbf{a} = (a_1, \dots, a_n)$, $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$ sei

$$\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^n a_i b_i, \quad w(\mathbf{a}) = |\{i \in [1, n] \mid a_i \neq 0\}| \in [0, n] \quad \text{und} \quad d(\mathbf{a}, \mathbf{b}) = w(\mathbf{a} - \mathbf{b}) \in [0, n].$$

Man nennt $w(\mathbf{a})$ das *Gewicht* von \mathbf{a} und $d(\mathbf{a}, \mathbf{b})$ die *Hamming-Distanz* von \mathbf{a} und \mathbf{b} . Für eine Teilmenge $C \subset \mathbb{F}_q^n$ sei $C^\perp = \{\mathbf{u} \in \mathbb{F}_q^n \mid \langle \mathbf{u}, \mathbf{c} \rangle = 0 \text{ für alle } \mathbf{c} \in C\}$. $C^\perp \subset \mathbb{F}_q^n$ ist ein Untervektorraum.

Ist $C \subset \mathbb{F}_q^n$ ein Untervektorraum und $k = \dim_{\mathbb{F}_q}(C)$, so ist $\dim_{\mathbb{F}_q}(C^\perp) = n - k$, und $(C^\perp)^\perp = C$. Ist $H \in M_{n-k, n}(\mathbb{F}_q)$ eine Matrix, deren Zeilen eine Basis von C^\perp bilden so ist $C = \{\mathbf{u} \in \mathbb{F}_q^n \mid H\mathbf{u}^t = \mathbf{0}\}$, und man nennt H eine *Testmatrix* für C .

Lemma 5.1.2. Sei $n \in \mathbb{N}$.

1. Für alle $\mathbf{a}, \mathbf{b} \in \mathbb{F}_q^n$ ist $w(\mathbf{a} + \mathbf{b}) \leq w(\mathbf{a}) + w(\mathbf{b})$.
2. $d: \mathbb{F}_q^n \times \mathbb{F}_q^n \rightarrow [0, n] \subset \mathbb{R}_{\geq 0}$ ist eine Metrik.

BEWEIS. 1. Sei $\mathbf{a} = (a_1, \dots, a_n)$, $\mathbf{b} = (b_1, \dots, b_n) \in \mathbb{F}_q^n$. Dann ist

$$\begin{aligned} w(\mathbf{a} + \mathbf{b}) &= |\{i \in [1, n] \mid a_i + b_i \neq 0\}| \leq |\{i \in [1, n] \mid a_i \neq 0 \text{ oder } b_i \neq 0\}| \\ &\leq |\{i \in [1, n] \mid a_i \neq 0\}| + |\{i \in [1, n] \mid b_i \neq 0\}| = w(\mathbf{a}) + w(\mathbf{b}). \end{aligned}$$

2. Definitheit und Symmetrie sind offensichtlich. Für $\mathbf{a}, \mathbf{b}, \mathbf{c} \in \mathbb{F}_q^n$ ist

$$d(\mathbf{a}, \mathbf{c}) = w(\mathbf{c} - \mathbf{a}) = w((\mathbf{b} - \mathbf{a}) + (\mathbf{c} - \mathbf{b})) \leq w(\mathbf{b} - \mathbf{a}) + w(\mathbf{c} - \mathbf{b}) = d(\mathbf{a}, \mathbf{b}) + d(\mathbf{b}, \mathbf{c}). \quad \square$$

Definition 5.1.3. Seien $n \in \mathbb{N}$ und $k \in [0, n]$.

1. Ein (*linearer*) $[n, k]$ -Code C über \mathbb{F}_q ist ein Untervektorraum $C \subset \mathbb{F}_q^n$ mit $k = \dim_{\mathbb{F}_q}(C)$. Man nennt \mathbb{F}_q das *Alphabet*, die Elemente $\mathbf{c} \in C$ die *Codewörter*, k die *Dimension* und n die *Länge* von C . Im Falle $C \neq \{\mathbf{0}\}$ nennt man

$$d = \min w(C \setminus \{\mathbf{0}\}) = \min\{d(\mathbf{a}, \mathbf{b}) \mid \mathbf{a}, \mathbf{b} \in C, \mathbf{a} \neq \mathbf{b}\} \in [0, n]$$

die *Minimaldistanz* von C , und im Falle $C = \{\mathbf{0}\}$ setzt man $d = 0$.

2. Ein $[n, k, d]$ -Code ist ein $[n, k]$ -Code mit Minimaldistanz d .
3. Sei C ein $[n, k]$ -Code. Der $[n, n - k]$ -Code C^\perp heißt der zu C *duale Code*.
4. Sei $t \in \mathbb{N}$. Ein $[n, k]$ -Code $C \subset \mathbb{F}_q^n$ heißt *t-fehlerkorrigierend*, wenn für alle $\mathbf{u} \in \mathbb{F}_q^n$ gilt: $|\{\mathbf{c} \in C \mid d(\mathbf{u}, \mathbf{c}) \leq t\}| \leq 1$.

Ein $[n, k, d]$ -Code ist *t-fehlerkorrigierend* für jedes $t \in \mathbb{N}$ mit $2t < d$.

Definition und Satz 5.1.4 (Satz von der Singleton-Schranke). *Sei C ein $[n, k, d]$ -Code. Dann ist $k + d \leq n + 1$. Gilt Gleichheit, so nennt man C einen MDS-Code oder Code mit Maximaldistanz.*

BEWEIS. Im Falle $d \leq 1$ ist nichts zu zeigen. Sei also $d \geq 2$ und $W = \mathbb{F}_q^{d-1} \times \{0\}^{n-d+1} \subset \mathbb{F}_q^n$. Für alle $\mathbf{a} \in W$ ist $d(\mathbf{a}, \mathbf{0}) = w(\mathbf{a}) \leq d - 1$ und daher $W \cap C = \{\mathbf{0}\}$. Es folgt

$$k + (d - 1) = \dim C + \dim W = \dim(C + W) + \dim(C \cap W) = \dim(C + W) \leq n. \quad \square$$

Definition und Bemerkung 5.1.5. Sei $n = q - 1$, $k \in [1, n]$ und $\mathbb{F}_q^\times = \langle \beta \rangle = \{\beta, \beta^2, \dots, \beta^n = 1\}$. Sei $L_k = \{f \in \mathbb{F}_q[X] \mid \text{gr}(f) \leq k - 1\}$, und sei

$$\mathbf{e}: L_k \rightarrow \mathbb{F}_q^n \quad \text{definiert durch} \quad \mathbf{e}(f) = (f(\beta), f(\beta^2), \dots, f(\beta^n)).$$

L_k ist ein \mathbb{F}_q -Vektorraum, $\dim(L_k) = k$, und \mathbf{e} ist ein \mathbb{F}_q -Monomorphismus [denn: Ist $f \in \text{Ker}(\mathbf{e})$, so ist $\text{gr}(f) \leq k - 1 < n$, und f hat n Nullstellen, also folgt $f = 0$]. Daher ist $C_k = \mathbf{e}(L_k) \subset \mathbb{F}_q^n$ ein $[n, k]$ -Code. Für $\mathbf{c} = \mathbf{e}(f) \in C \setminus \{\mathbf{0}\}$ ist $w(\mathbf{c}) = n - |\{i \in [1, n] \mid f(\beta^i) = 0\}| \geq n - \text{gr}(f) \geq n - (k - 1)$. Ist d die Minimaldistanz von C , so folgt $d \leq n - k + 1$, also $k + d \leq n + 1$, und nach Satz 5.1.4 gilt Gleichheit.

Der Code C_k heißt RS-Code (*Reed Solomon Code*). Jeder RS-Code ist ein MDS-Code. Wegen $n = q - 1$ sind RS-Codes "kurz".

5.2

Definition 5.2.1. Sei L/\mathbb{F}_q ein Funktionenkörper mit Konstantenkörper \mathbb{F}_q und $n \in \mathbb{N}$. Seien $P_1, \dots, P_n \in \mathbb{P}_L^1$ verschieden, $D = P_1 + \dots + P_n$ und $G \in \mathbb{D}_L$, so dass $v_{P_i}(G) = 0$ für alle $i \in [1, n]$ (für $x \in \mathcal{L}(G)$ ist dann $x \in \mathcal{O}_{P_i}$ und $x(P_i) \in L_{P_i} = \mathbb{F}_q$ für alle $i \in [1, n]$).

1. Die Abbildung

$$\mathbf{e} = \mathbf{e}_{D,G}: \mathcal{L}(G) \rightarrow \mathbb{F}_q^n \quad \text{sei definiert durch} \quad \mathbf{e}(x) = (x(P_1), \dots, x(P_n)).$$

Dann ist \mathbf{e} ein \mathbb{F}_q -Vektorraumhomomorphismus, und $C_{\mathcal{L}}(D, G) = \text{Bi}(\mathbf{e}) \subset \mathbb{F}_q^n$ heißt (*geometrischer*) *Goppa-Code* zu den Divisoren D und G .

2. Die Abbildung

$$\mathbf{e}^* = \mathbf{e}_{D,G}^*: \Omega_L(G - D) \rightarrow \mathbb{F}_q^n \quad \text{sei definiert durch} \quad \mathbf{e}^*(\omega) = (\text{res}_{P_1}(\omega), \dots, \text{res}_{P_n}(\omega)).$$

Dann ist \mathbf{e}^* ein \mathbb{F}_q -Vektorraumhomomorphismus, und $C_{\Omega}(D, G) = \text{Bi}(\mathbf{e}^*) \subset \mathbb{F}_q^n$ heißt (*residueller*) *Goppa-Code* zu den Divisoren D und G .

Satz 5.2.2. *Sei L/\mathbb{F}_q ein Funktionenkörper mit Konstantenkörper \mathbb{F}_q und $n \in \mathbb{N}$. Seien $P_1, \dots, P_n \in \mathbb{P}_L^1$ verschieden, $D = P_1 + \dots + P_n$ und $G \in \mathbb{D}_L$, so dass $v_{P_i}(G) = 0$ für alle $i \in [1, n]$ (für $x \in \mathcal{L}(G)$ ist dann $x \in \mathcal{O}_{P_i}$ und $x(P_i) \in L_{P_i} = \mathbb{F}_q$ für alle $i \in [1, n]$). $D = P_1 + \dots + P_n$ mit verschiedenen $P_1, \dots, P_n \in \mathbb{P}_L^1$ und $G \in \mathbb{D}_L$, so dass $v_{P_i}(G) = 0$ für alle $i \in [1, n]$.*

1. $C_{\mathcal{L}}(D, G)$ ist ein $[n, k, d]$ -Code mit

$$k = \dim(G) - \dim(G - D), \quad \text{und} \quad d \geq n - \deg(G) \quad \text{im Falle} \quad k > 0.$$

Ist insbesondere $\deg(G) < n$, so gilt:

$\mathbf{e}_{D,G}$ ist ein Monomorphismus, $k = \dim(G) \geq \deg(G) + 1 - g_L$ mit Gleichheit, falls $\deg(G) \geq 2g_L - 1$, und im Falle $k > 0$ ist $k + d \geq n + 1 - g_L$.

2. Sei $\eta \in \Omega_L$, so dass $v_{P_i}(\eta) = -1$ und $\text{res}_{P_i}(\eta) = 1$ für alle $i \in [1, n]$ (existiert nach Satz 4.7.3), und sei $W = (\eta)$. Dann ist $v_{P_i}(D - G + W) = 0$ für alle $i \in [1, n]$, und es ist $C_{\Omega}(D, G) = C_{\mathcal{L}}(D, D - G + W)$.

3. $C_\Omega(G, D)$ ist ein $[n, k^*, d^*]$ -Code mit

$$k^* = i(G - D) - i(G) = n - \dim C_{\mathcal{L}}(D, G), \quad \text{und} \quad d^* \geq \deg(G) - 2g_L + 2 \quad \text{im Falle} \quad k^* > 0.$$

Ist insbesondere $\deg(G) \geq 2g_L - 1$, so gilt:

$e_{D,G}^*$ ist ein Monomorphismus, $k^* = i(G - D) \geq n + g_L - 1 - \deg(G)$ mit Gleichheit, falls $\deg(G) < n$, und im Falle $k^* > 0$ ist $k^* + d^* \geq n + 1 - g_L$.

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

BEWEIS. 1. Es ist $\text{Ker}(e) = \{x \in \mathcal{L}(G) \mid v_{P_i}(x) > 0 \text{ für alle } i \in [1, n]\} = \mathcal{L}(G - D)$ und daher $k = \dim C_{\mathcal{L}}(D, G) = \dim(G) - \dim(G - D)$. Sei nun $k > 0$, und sei $x \in \mathcal{L}(G) \setminus \mathcal{L}(G - D)$, so dass $d = w(e(x))$ die Minimaldistanz von $C_{\mathcal{L}}(D, G)$ ist. Dann ist $n - d = |\{i \in [1, n] \mid x \in P_i\}|$, und es sei (nach geeigneter Ummummerierung) $x \in P_i$ für alle $i \in [d + 1, n]$. Dann ist $x \in \mathcal{L}(G - (P_{d+1} + \dots + P_n)) \setminus \{0\}$ und daher $0 \leq \deg(G - (P_{d+1} + \dots + P_n)) = \deg(G) - (n - d)$, also $d \geq n - \deg(G)$.

Sei nun $\deg(G) < n$. Wegen $\deg(G - D) = \deg(G) - n < 0$ ist dann $\mathcal{L}(G - D) = \{0\}$, also e ein Monomorphismus, $k = \dim \text{Bi}(e) = \dim G \geq \deg(G) + 1 - g_L$ nach Satz 4.3.1, und nach Satz 4.6.1 gilt Gleichheit, falls $\deg(G) \geq 2g_L - 1$. Im Falle $k > 0$ folgt insbesondere $k + d \geq n + 1 - g_L$.

2. Für alle $i \in [1, n]$ ist $v_{P_i}(W) = v_{P_i}(\eta) = -1$ und daher $v_{P_i}(D - G + W) = 0$. Nach Satz 4.5.2.5 definiert die Zuordnung $x \mapsto x\eta$ einen K -Vektorraumisomorphismus $\mu: \mathcal{L}(D - G + W) \rightarrow \Omega_L(G - D)$. Für alle $i \in [1, n]$ und $x \in \mathcal{L}(D - G + W)$ ist $\text{res}_{P_i}(x\eta) = x(P_i)\text{res}_{P_i}(\eta) = x(P_i)$. Daher folgt $e_{D, D-G+W} = e_{D, G}^* \circ \mu$ und $C_\Omega(D, G) = C_{\mathcal{L}}(D, D - G + W)$.

3. Nach 1. und 2. ist $C_\Omega(D, G) = C_{\mathcal{L}}(D, D - G + W)$ ein $[n, k^*, d^*]$ -Code mit

$$k^* = \dim(D - G + W) - \dim(-G + W), \quad \text{und} \quad d^* \geq n - \deg(D - G + W), \quad \text{falls} \quad k^* > 0.$$

Nach Satz 4.5.2.5 ist

$$\begin{aligned} k^* &= \dim(D - G + W) - \dim(-G + W) = \dim \Omega_L(G - D) - \dim \Omega_L(G) = i(G - D) - i(G) \\ &= [\dim(G - D) - \deg(G - D) + g_L - 1] - [\dim(G) - \deg(G) + g_L - 1] \\ &= \dim(G - D) - \dim(D) + n = n - \dim C_{\mathcal{L}}(D, G), \end{aligned}$$

und mit Satz 4.6.1 folgt (falls $k^* > 0$)

$$d^* \geq n - \deg(D - G + W) = n - \deg(D) + \deg(G) - \deg(W) = \deg(G) - 2g_L + 2.$$

Ist $\deg(G) \geq 2g_L - 1$, so ist $\deg(D - G + W) \leq n - 2g_L + 1 + 2g_L - 2 < n$, also $e_{D, D-G+W}$ ein Monomorphismus nach 1., und daher ist auch $e_{D, G}^*$ ein Monomorphismus. Ferner ist in diesem Falle $i(G) = 0$, also

$k^* = i(G - D) = \dim(G - D) - \deg(G - D) + g_L - 1 = \dim(G - D) - \deg(G) + n + g_L - 1 \geq n + g_L - 1 - \deg(G)$ mit Gleichheit, falls $\deg(G) < n$, denn dann ist $\deg(G - D) < 0$ und $\dim(G - D) = 0$. Im Falle $k^* > 0$ folgt $k^* + d^* \geq n + 1 - g_L$.

4. Sei $x \in \mathcal{L}(G)$ und $\omega \in \Omega_L(G - D)$. Dann ist $(x\omega) = (x) + (\omega) \geq -G + (G - D) = D$, also $v_P(x\omega) \geq -1$ für alle $P \in \mathbb{P}_L$ und $v_P(x\omega) \geq 0$ für alle $P \in \mathbb{P}_L \setminus \{P_1, \dots, P_n\}$. Mit Satz 4.7.2 folgt nun

$$\langle e(x), e^*(\omega) \rangle = \sum_{i=1}^n \text{res}_{P_i}(\omega)x(P_i) = \sum_{i=1}^n \text{res}_{P_i}(x\omega) = \sum_{P \in \mathbb{P}_L} \text{res}_P(x\omega) = 0.$$

Daher ist $C_\Omega(D, G) \subset C_{\mathcal{L}}(D, G)^\perp$, und wegen $\dim C_\Omega(D, G) = n - \dim C_{\mathcal{L}}(D, G)$ folgt Gleichheit. \square

Elliptische Funktionenkörper und elliptische Kurven

In diesem Kapitel sei K ein Körper und \overline{K} eine algebraische Hülle von K .

6.1

Definition 6.1.1. Ein Funktionenkörper L/K heißt *elliptisch*, wenn $g_L = 1$ und $\mathbb{P}_L^1 \neq \emptyset$.

Satz 6.1.2. Sei L/K ein elliptischer Funktionenkörper.

1. Zu jedem $A \in \mathbb{D}_L$ mit $\deg(A) = 1$ gibt es genau ein $P \in \mathbb{P}_L^1$ mit $A \sim P$ (und dann ist $P \in \mathbb{P}_L^1$).
2. Sei $O \in \mathbb{P}_L^1$. Dann ist die Abbildung

$$\Phi: \mathbb{P}_L^1 \rightarrow \mathcal{C}_L^0, \quad \text{definiert durch } \Phi(P) = [P - O],$$

bijektiv, und es gibt genau eine Verknüpfung \oplus auf \mathbb{P}_L^1 , für die \mathbb{P}_L^1 zur abelschen Gruppe und Φ zum Isomorphismus wird. Für diese ist O das Nullelement, und für alle $P, Q, R \in \mathbb{P}_L^1$ gilt:

$$P \oplus Q = R \iff [P - O] + [Q - O] = [R - O] \iff P + Q \sim R + O$$

und

$$P \oplus Q \oplus R = O \iff P + Q + R \sim 3O.$$

BEWEIS. 1. Sei $A \in \mathbb{D}_L$ mit $\deg(A) = 1$. Nach Satz 4.6.1 ist $\dim(A) = \deg(A) + 1 - g_L = 1$, und nach Satz 4.1.2.5 gibt es ein $A_1 \in \mathbb{D}_L$ mit $A_1 \geq 0$ und $A \sim A_1$. Dann ist $\deg(A_1) = \deg(A) = 1$ und daher $A_1 = P \in \mathbb{P}_L^1$. Zum Nachweis der Eindeutigkeit nehmen wir an, es seien $P, P' \in \mathbb{P}_L^1$ mit $P \neq P'$, $A \sim P$ und $A \sim P'$, so folgt $\deg(P) = \deg(P')$ und $P \sim P'$. Dann ist $0 \neq P - P' = (x)$ mit $x \in L^\times$, $(x)_\infty = P'$ und $[L:(x)] = \deg(x)_\infty = 1$, also $L = K(x)$, ein Widerspruch.

2. Es genügt, die Bijektivität von Φ zu zeigen. Sei also $\mathfrak{c} \in \mathcal{C}_L^0$ und $C \in \mathfrak{c}$. Dann ist $\deg(C) = 0$, und für $P \in \mathbb{P}_L^1$ ist genau dann $\Phi(P) = \mathfrak{c}$, wenn $[P - O] = [C]$, also $P \sim O + C$. Wegen $\deg(O + C) = 1$ gibt es nach 1. genau ein solches $P \in \mathbb{P}_L^1$. \square

Definitionen und Bemerkungen 6.1.3. Ein Polynom $f \in K[X, Y]$ heißt *Weierstraß-Polynom*, wenn

$$f = Y^2 + a_1XY + a_3Y - g \quad \text{mit} \quad g = X^3 + a_2X^2 + a_4X + a_6$$

und

- $a_1 = a_3 = 0$, falls $\text{char}(K) \neq 2$,
- $a_1 = 0$ oder $(a_1, a_3) = (1, 0)$, falls $\text{char}(K) = 2$.

Ist $g = (X - \xi_1)(X - \xi_2)(X - \xi_3)$ mit $\xi_1, \xi_2, \xi_3 \in \overline{K}$, so heißt

$$D = [(\xi_1 - \xi_2)(\xi_1 - \xi_3)(\xi_2 - \xi_3)]^2 = -4a_2^3a_6 + a_2^2a_4^2 - 4a_4^3 - 27a_6^2 + 18a_2a_4a_6 \in K$$

die *Diskriminante* von g (nachrechnen! Genau dann ist $D \neq 0$, wenn g keine mehrfachen Nullstellen besitzt).

Die *Diskriminante* $\Delta = \Delta_f$ des Weierstraß-Polynoms f ist definiert durch

$$\Delta = \begin{cases} 16D, & \text{falls } a_1 = a_3 = 0, \\ a_3^4, & \text{falls } \text{char}(K) = 2 \text{ und } a_1 = 0, \\ a_4^2 + a_6, & \text{falls } \text{char}(K) = 2 \text{ und } (a_1, a_3) = (1, 0). \end{cases}$$

Ist $\mathbf{p} = (\alpha, \beta) \in K^2$, so besitzt das Weierstraß-Polynom in \mathbf{p} die Taylorentwicklung

$$f = f(\mathbf{p}) + \frac{\partial f}{\partial X}(\mathbf{p})(X - \alpha) + \frac{\partial f}{\partial Y}(\mathbf{p})(Y - \beta) + a_1(X - \alpha)(Y - \beta) - (a_2 + 3\alpha)(X - \alpha)^2 + (Y - \beta)^2 - (X - \alpha)^3.$$

Satz 6.1.4. *Sei L/K ein elliptischer Funktionenkörper. Dann gibt es ein Weierstraß-Polynom $f \in K[X, Y]$, so dass $L = K(x, y)$ und $f(x, y) = 0$.*

BEWEIS. Sei $P \in \mathbb{P}_L^1$. Für $n \in \mathbb{N}$ ist dann $\deg(nP) = n \geq 1 = 2g_L - 1$, und aus Satz 4.6.1 folgt $\dim(nP) = \deg(nP) + 1 - g_L = n$. Daher ist $K = \mathcal{L}(P) \subsetneq \mathcal{L}(2P) \subsetneq \mathcal{L}(3P)$. Sei $x_1 \in \mathcal{L}(2P) \setminus K$ und $y_1 \in \mathcal{L}(3P) \setminus \mathcal{L}(2P)$. Dann ist $(x_1)_\infty = 2P$, $(y_1)_\infty = 3P$, aus Satz 4.2.1 folgt $[L : K(x_1)] = \deg(2P) = 2$, $[L : K(y_1)] = \deg(3P) = 3$, und wegen $[L : K(x_1, y_1)] \mid [L : K(x_1)]$ und $[L : K(x_1, y_1)] \mid [L : K(y_1)]$ folgt $L = K(x_1, y_1)$. Die 7 Elemente $y_1^2, x_1 y_1, y_1, x_1^3, x_1^2, x_1, 1$ liegen in $\mathcal{L}(6P)$ und sind wegen $\dim \mathcal{L}(6P) = 6$ linear abhängig über K . Daher besteht eine Relation $ay_1^2 + \alpha_1 x_1 y_1 + \alpha_3 y_1 - bx_1^3 - \alpha_2 x_1^2 - \alpha_4 x_1 - \alpha_6 = 0$ mit $(a, \alpha_1, \alpha_3, b, \alpha_2, \alpha_4, \alpha_6) \in K^7 \setminus \{\mathbf{0}\}$. Wegen $[K(x_1)(y_1) : K(x_1)] = 2$ ist $a \neq 0$, und wegen $[K(y_1)(x_1) : K(y_1)] = 3$ ist $b \neq 0$. Nun multiplizieren wir die Relation mit $a^3 b^2$ und setzen $y_2 = a^2 b y_1$, $x_2 = a b x_1$. Dann erhalten wir $L = K(x_2, y_2)$ und $y_2^2 + \alpha_1 x_2 y_2 + \alpha_3 a b y_2 - x_2^3 - \alpha_2 a x_2^2 - \alpha_4 a^2 b x_2 - \alpha_6 = 0$.

FALL 1: $\text{char}(K) \neq 2$. Wir setzen

$$y = y_2 + \frac{\alpha_1 x_2 + \alpha_3 a b}{2} \quad \text{und} \quad x = x_2.$$

Dann folgt $L = K(x, y)$, und es besteht eine Relation der Form $y^2 - x^3 - a_2 x^2 - a_4 x - a_6 = 0$ mit $a_2, a_4, a_6 \in K$.

FALL 2: $\text{char}(K) = 2$ und $\alpha_1 = 0$. Wir setzen $y = y_2$ und $x = x_2$. Dann ist $L = K(x, y)$, und es besteht eine Relation der Form $y^2 + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6 = 0$ mit $a_2, a_3, a_4, a_6 \in K$.

FALL 3: $\text{char}(K) = 2$ und $\alpha_1 \neq 0$. Wir setzen $y = y_2$ und $x = \alpha_1 x_2 + \alpha_3 a b$. Dann ist $L = K(x, y)$, und es besteht eine Relation der Form $y^2 + x y - x^3 - a_2 x^2 - a_4 x - a_6 = 0$ mit $a_2, a_4, a_6 \in K$. \square

6.2

Satz 6.2.1. *Sei $f \in K[X, Y]$ ein Weierstraß-Polynom, Δ seine Diskriminante, $C = V(f) \subset \overline{K}^2$, $E = \overline{C} \subset \mathbb{P}_{\overline{K}}^2$, $\mathbf{o} = (0 : 1 : 0)$, und seien $x, y \in K[C]$ die Koordinatenfunktionen von C .*

1. f ist absolut irreduzibel.
2. $E \setminus V(f) = \{\mathbf{o}\}$, und \mathbf{o} ist ein regulärer Punkt von E .
3. Genau dann ist E glatt, wenn $\Delta \neq 0$.
4. Sei $\Delta \neq 0$. Dann ist $K(E)$ ein elliptischer Funktionenkörper, und

$$\Psi: E(K) \rightarrow \mathbb{P}_{K(E)}^1, \quad \text{definiert durch} \quad \Psi(\mathbf{p}) = \mathcal{M}_{\mathbf{p}}(E),$$

eine bijektive Abbildung. Ist $O = \Psi(\mathbf{o})$, so ist $(x)_\infty = 2O$ und $(y)_\infty = 3O$.

5. Besitzt E einen singulären Punkt $\mathbf{p} \in E(K)$, so ist $K(E)$ ein rationaler Funktionenkörper.

BEWEIS. Sei $f = Y^2 + a_1XY + a_3Y - g$ mit $g = X^3 + a_2X^2 + a_4X + a_6 \in K[X]$. Dann ist $f^* = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$, $E = \overline{C} = V_+(f^*)$, $f^*(\mathbf{o}) = 0$, und $f_3 = -X^3$ ist die Leitform von f .

1. Da K beliebig war, genügt es, die Irreduzibilität von f über K nachzuweisen. Wir nehmen an, $f = Y^2 + (a_1X + a_3)Y - g \in K[X][Y]$ sei reduzibel. Dann besitzt f , aufgefasst als Polynom in Y über $K[X]$, eine Faktorisierung $f = (Y - h_1)(Y - h_2)$ mit Polynomen $h_1, h_2 \in K[X]$. Wegen $g = -h_1h_2$ ist dann entweder $\{\text{gr}(h_1), \text{gr}(h_2)\} = \{0, 3\}$ oder $\{\text{gr}(h_1), \text{gr}(h_2)\} = \{1, 2\}$, und beides ist wegen $a_1X + a_3 = -(h_1 + h_2)$ unmöglich.

2. Es ist $E \setminus C = \{(\alpha : \beta : 0) \in \mathbb{P}_{\overline{K}}^2 \mid \alpha = 0\} = \{\mathbf{o}\}$, und wegen

$$\frac{\partial f^*}{\partial Z}(\mathbf{o}) = 1 \quad \text{ist } \mathbf{o} \text{ ein regulärer Punkt von } E.$$

3. Nach 2. ist E genau dann regulär, wenn C regulär ist.

FALL 1: $\text{char}(K) \neq 2$. Dann ist $f = Y^2 - g$,

$$\frac{\partial f}{\partial X} = -g' \quad \text{und} \quad \frac{\partial f}{\partial Y} = 2Y.$$

Genau dann ist E singulär in einem Punkt $\mathbf{p} = (\alpha, \beta) \in \overline{K}^2$, wenn $\beta = 0$ und $g(\alpha) = g'(\alpha) = 0$. Daher besitzt E genau dann einen singulären Punkt, wenn g eine mehrfache Nullstelle besitzt, und das ist genau dann der Fall, wenn $D = 0$. Daher ist E genau dann glatt, wenn $\Delta \neq 0$.

FALL 2: $\text{char}(K) = 2$ und $a_3 \neq 0$. Dann ist $a_1 = 0$, $f = Y^2 + a_3Y - g$,

$$\frac{\partial f}{\partial X} = -g' \quad \text{und} \quad \frac{\partial f}{\partial Y} = a_3.$$

Ist $\Delta = a_3^4 \neq 0$, so ist E glatt. Ist $\Delta = a_3 = 0$ und $\mathbf{p} = (\alpha, \beta) \in \overline{K}^2$ mit $g'(\alpha) = \alpha^2 + a_4 = 0$ und $f(\alpha, \beta) = \beta^2 + a_3\beta - g(\alpha) = 0$, so ist \mathbf{p} ein singulärer Punkt von E .

FALL 3: $\text{char}(K) = 2$ und $(a_1, a_3) = (1, 0)$. Dann ist $f = Y^2 + XY - g$,

$$\frac{\partial f}{\partial X} = Y - g' \quad \text{und} \quad \frac{\partial f}{\partial Y} = X.$$

Genau dann ist E singulär in einem Punkt $\mathbf{p} = (\alpha, \beta) \in \overline{K}^2$, wenn $\alpha = 0$, $f(\beta, 0) = \beta^2 - a_6 = 0$ und $\beta = g'(0) = a_4$. Daher besitzt E genau dann einen singulären Punkt, wenn $a_4^2 = a_6$, also $\Delta = 0$ ist.

4. Sei $\Delta \neq 0$. Es ist $K(C) = K(E) = K(x, y)$, und wegen $f(x, y) = 0$ ist y algebraisch über $K(x)$ und x algebraisch über $K(y)$. Daher sind x und y beide transzendent über K , $f(X, Y)$ ist das Minimalpolynom von x über $K(y)$ und $f(x, Y)$ ist das Minimalpolynom von y über $K(x)$. Insbesondere folgt $[K(C) : K(x)] = 2$ und $[K(C) : K(y)] = 3$. Wegen $\mathbf{o} \in E(K)$ ist $O = \mathcal{M}_{\mathbf{o}}(E) \in \mathbb{P}_{K(C)}^1$, und nach Satz 3.9.4 ist Ψ eine bijektive Abbildung. Für alle $\mathbf{p} \in C$ ist $P_{\mathbf{p}} = \mathcal{M}_{\mathbf{p}}(C) = \mathcal{M}_{\mathbf{p}}(E) \in \mathbb{P}_{K(C)}$ und $\mathcal{O}_{P_{\mathbf{p}}} \supset K[x, y]$. Daher ist O die einzige Polstelle von x und von y , und nach Satz 4.2.1 ist $(x)_{\infty} = 2O$ und $(y)_{\infty} = 3O$. Da $(1, y)$ über $K(x)$ linear unabhängig ist, ist $\{x^k, x^k y \mid k \in \mathbb{N}_0\}$ eine über K linear unabhängige Menge. Ist $n \in \mathbb{N}$ gerade, $n = 2m \geq 4$, so ist $\{1, x, \dots, x^m, y, yx, \dots, yx^{m-2}\} \subset \mathcal{L}(nO)$. Ist $n \in \mathbb{N}$ ungerade, $n = 2m + 1 \geq 3$, so ist $\{1, x, \dots, x^m, y, yx, \dots, yx^{m-1}\} \subset \mathcal{L}(nO)$. In jedem Falle folgt $\dim(nO) \geq n$, und für $n \gg 1$ ist $n \leq \dim(nO) = \deg(nO) + 1 - g_{K(C)} = n + 1 - g_{K(C)}$, also $g_{K(C)} \leq 1$ nach Satz 4.6.1. Wir müssen $g_{K(C)} = 1$ zeigen, und wir nehmen an, es sei $g_{K(C)} = 0$.

Wegen $\deg(O) = 1 \geq 2g_{K(C)} - 1$ ist $\dim(O) = \deg(O) + 1 - g_{K(C)} = 2$ (nach Satz 4.6.1), also $K \subsetneq \mathcal{L}(O)$. Ist $t \in \mathcal{L}(O) \setminus K$, so folgt $(t)_{\infty} = O$ und daher $(t) = P - O$ mit $P \in \mathbb{P}_{K(C)}^1$. Dann ist $[K(C) : K(t)] = \deg(t)_{\infty} = 1$, also $K(C) = K(t)$, und $K[t]$ besteht aus allen $z \in K(t)$, die höchstens in O einen Pol besitzen. Insbesondere folgt $x, y \in K[t]$, und daher gibt es Polynome $p, q \in K[X]$ mit $x = p(t)$, $y = q(t)$, $\text{gr}(p) = 2$ und $\text{gr}(q) = 3$, woraus wir nun einen Widerspruch herleiten.

FALL 1: $\text{char}(K) \neq 2$. Dann ist $q(t)^2 = g(p(t))$, also $2q(t)q'(t) = g'(p(t))p'(t)$, und wegen $\Delta \neq 0$ ist $g(t) = (t - \beta_1)(t - \beta_2)(t - \beta_3)$ mit verschiedenen $\beta_1, \beta_2, \beta_3 \in \overline{K}$. Für $i \in [1, 3]$ sei $\tau_i \in \overline{K}$ mit $p(\tau_i) = \beta_i$, also $q(\tau_i) = 0$ und daher $0 = g'(\beta_i)p'(\tau_i)$. Da g keine mehrfachen Nullstellen besitzt, ist $g'(\beta_i) \neq 0$, also $p'(\tau_i) = 0$. Nun sind aber τ_1, τ_2, τ_3 verschieden, und es ist $\text{gr}(p') = 1$, ein Widerspruch.

FALL 2: $\text{char}(K) = 2$, $a_3 \neq 0$. Dann ist $a_1 = 0$ und $q(t)^2 + a_3q(t) = g(p(t))$. Wegen $2q(t)q'(t) = 0$ folgt $a_3q'(t) = g'(p(t))p'(t)$. Wegen $a_3 \neq 0$ ist $a_3q'(t)$ ein Polynom vom Grade 2, aber $g'(p(t))$ ist vom Grade 4, ein Widerspruch.

FALL 3: $\text{char}(K) = 2$, $(a_1, a_3) = (1, 0)$. Dann ist $q(t)^2 + p(t)q(t) = g(p(t))$, und durch Differenzieren erhalten wir $p(t)q'(t) + p'(t)q(t) = g'(p(t))p'(t)$. Sei $\tau \in \overline{K}$ mit $p(\tau) = 0$.

FALL 3a: $p'(\tau) = 0$. Dann ist τ eine mehrfache Nullstelle von $p(t)$, also $p(t) = c(t - \tau)^2$ mit $c \in K^\times$ und daher $p'(t) = 0$. Es folgt $p(t)q'(t) = 0$, ein Widerspruch.

FALL 3b: $p'(\tau) \neq 0$. Dann ist $q(\tau) = g'(p(\tau)) = g'(0) = a_4$ und $q(\tau)^2 = g(p(\tau)) = g(0) = a_6$, also $a_4^2 = a_6$ und $\Delta = 0$, ein Widerspruch.

5. Sei $\mathbf{p} = (\alpha, \beta)E(K) \subset K^2$ ein singulärer Punkt von E . Dann degeneriert die Taylorentwicklung von f in \mathbf{p} zu $f = (Y - \beta)^2 + a_1(X - \alpha)(Y - \beta) - (a_2 + 3\alpha)(X - \alpha)^2 - (X - \alpha)^3$, und wegen $f(x, y) = 0$ folgt

$$t = \frac{y - \beta}{x - \alpha} \in K(x, y), \quad x = t^2 + a_1t - 2\alpha - a_2, \quad y = t(x - \alpha)^2 + \beta, \quad \text{und} \quad K(C) = K(x, y) = K(t). \quad \square$$

Definition und Bemerkung 6.2.2. Eine über K definierte *elliptische Kurve* ist eine über K definierte irreduzible projektive glatte Kurve $E \subset \mathbb{P}_{\overline{K}}^2$, so dass $K(E)$ ein elliptischer Funktionenkörper ist. Dann ist

$$\Psi: E \rightarrow \mathbb{P}_{K(E)}, \quad \text{definiert durch} \quad \Psi(\mathbf{p}) = P_{\mathbf{p}} = \mathcal{M}_{\mathbf{p}, K(E)},$$

bijektiv, und $\Psi(E(K)) = \mathbb{P}_{K(E)}^1$. Für $\mathbf{p} \in E$ sei $v_{\mathbf{p}} = v_{P_{\mathbf{p}}}: K(E) \rightarrow \mathbb{Z} \cup \{\infty\}$.

Sei $\mathbf{o} \in E(K)$. Nach Satz 6.1.2 wird $\mathbb{P}_{K(E)}^1$ zur abelschen Gruppe mit Nullelement $P_{\mathbf{o}}$ vermöge

$$P \oplus Q = R \iff P + Q \sim R + P_{\mathbf{o}} \quad \text{für alle } P, Q, R \in \mathbb{P}_{K(E)}^1,$$

und dann ist die Abbildung $\mathbb{P}_{K(E)}^1 \rightarrow \mathcal{C}_{K(E)}^0$, $P_{\mathbf{p}} \mapsto [P_{\mathbf{p}} - P_{\mathbf{o}}]$, ein Gruppenisomorphismus.

Mittels Ψ wird dann auch $E(K)$ zur abelschen Gruppe mit Nullelement \mathbf{o} vermöge

$$\mathbf{p} \oplus \mathbf{q} = \mathbf{r} \iff P_{\mathbf{p}} \oplus P_{\mathbf{q}} \sim P_{\mathbf{r}} + P_{\mathbf{o}} \quad \text{für alle } \mathbf{p}, \mathbf{q}, \mathbf{r} \in E(K).$$

Man nennt \oplus die *Addition mit Basis* \mathbf{o} auf $E(K)$. Für $\mathbf{p} \in E(K)$ und $m \in \mathbb{Z}$ bezeichnet man das m -fache von \mathbf{p} in $E(K)$ mit $[m]\mathbf{p}$.

Satz 6.2.3. Sei $E \subset \mathbb{P}_{\overline{K}}$ eine elliptische Kurve, $E = \overline{V(f)}$ mit

$$f = Y^2 + a_1XY + a_3Y - X^3 - a_2X^2 - a_4X - a_6 \in K[X, Y],$$

$C = E \cap \overline{K}^2$, $\mathbf{o} = (0:1:0)$ der Fernpunkt von C und \oplus die Addition mit Basis \mathbf{o} auf $E(K)$.

1. Seien $\mathbf{p}, \mathbf{q} \in C(K) = E(K) \setminus \{\mathbf{o}\}$. Im Falle $\mathbf{p} \neq \mathbf{q}$ sei $L \subset \overline{K}^2$ die Verbindungsgerade von \mathbf{p} und \mathbf{q} , und im Falle $\mathbf{p} = \mathbf{q}$ sei L die Tangente an C in \mathbf{p} . Dann gibt es einen eindeutig bestimmten Punkt $\mathbf{r} \in E(K)$, so dass $\overline{L} \cap E(K) = \{\mathbf{p}, \mathbf{q}, \mathbf{r}\}$, und im Falle $\mathbf{p} \neq \mathbf{q}$ ist

- entweder $\mathbf{r} \notin \{\mathbf{p}, \mathbf{q}\}$
- oder $\mathbf{r} = \mathbf{p}$ und L ist Tangente an C in \mathbf{p}
- oder $\mathbf{r} = \mathbf{q}$ und L ist Tangente an C in \mathbf{q} .

Für diesen Punkt \mathbf{r} ist $\mathbf{p} \oplus \mathbf{q} \oplus \mathbf{r} = \mathbf{o}$.

Insbesondere folgt $\mathbf{q} = \ominus \mathbf{p}$, falls $\mathbf{o} \in \overline{L}$ (also $L = V(X - \alpha)$ mit $\alpha \in K$).

2. Seien $\mathbf{p} = (\alpha, \beta)$, $\mathbf{p}' = (\alpha', \beta') \in E \cap K^2$. Dann ist $\ominus \mathbf{p} = (\alpha, -\beta - a_1\alpha - a_3)$, und genau dann ist $\alpha = \alpha'$, wenn $\mathbf{p}' \in \{\mathbf{p}, \ominus \mathbf{p}\}$.

Im Falle $\mathbf{p}' \neq \ominus \mathbf{p}$ ist $\mathbf{p} \oplus \mathbf{p}' = (\alpha'', \beta'')$, wobei

$$\alpha'' = \lambda^2 + a_1\lambda - a_2 - \alpha - \alpha' \quad \text{und} \quad \beta'' = -(\lambda + a_1)\alpha'' - \nu - a_3$$

mit

$$\lambda = \frac{\beta' - \beta}{\alpha' - \alpha}, \quad \nu = \frac{\beta\alpha' - \beta'\alpha}{\alpha' - \alpha}, \quad \text{falls } \mathbf{p} \neq \mathbf{p}' \quad (\text{und dann auch } \alpha \neq \alpha'),$$

und

$$\lambda = \frac{3\alpha^2 + 2a_2\alpha + a_4 - a_1\beta}{2\beta + a_1\alpha + a_3}, \quad \nu = \frac{-\alpha^3 + a_4\alpha + 2a_6 - a_3\beta}{2\beta + a_1\alpha + a_3}, \quad \text{falls } \mathbf{p} = \mathbf{p}'.$$

BEWEIS. 1. Seien $x, y \in K[C]$ die Koordinatenfunktionen von C , $\mathbf{p} = (\alpha, \beta) \in C(K) \subset K^2$ und $L \subset \bar{K}$ eine über K definierte Gerade mit $\mathbf{p} \in L$,

$$L = V(a(X - \alpha) + b(Y - \beta)) \quad \text{mit} \quad (a, b) \in K^2 \setminus \{(0, 0)\}, \quad \text{und} \quad \varphi = a(x - \alpha) + b(y - \beta) \in K[C].$$

Nach Satz 3.9.5 ist $v_{\mathbf{p}}(\varphi) \geq 1$, und genau dann ist $v_{\mathbf{p}}(\varphi) \geq 2$, wenn L die Tangente von C in \mathbf{p} ist. Für einen Punkt $\mathbf{z} = (\alpha', \beta') \in C$ ist $\varphi = a(x - \alpha') + b(y - \beta') + a(\alpha' - \alpha) + b(\beta' - \beta)$, also $v_{\mathbf{z}}(\varphi) \geq 0$. Genau dann ist $v_{\mathbf{z}}(\varphi) \geq 1$, wenn $\mathbf{z} \in L$, und genau dann ist $v_{\mathbf{z}}(\varphi) \geq 2$, wenn L Tangente von C in \mathbf{z} ist. Nach Satz 4.2.1 ist

$$0 = \deg(\varphi) = \sum_{P \in \mathbb{P}_{K(C)}} v_P(\varphi)P = v_{\mathbf{o}}(\varphi) + \sum_{\mathbf{z} \in C} \deg(P_{\mathbf{z}})v_{\mathbf{z}}(\varphi).$$

FALL 1: $b = 0$. Dann ist $a \neq 0$, $\mathbf{o} \in \bar{L}$, und wegen $v_{\mathbf{o}}(x) = -2$ ist $v_{\mathbf{o}}(\varphi) = -2$ und daher

$$\sum_{\mathbf{z} \in C} \deg(P_{\mathbf{z}})v_{\mathbf{z}}(\varphi) = 2.$$

FALL 1a: $\mathbf{p} \neq \mathbf{q}$. Dann ist $v_{\mathbf{p}}(\varphi) \geq 1$, $v_{\mathbf{q}}(\varphi) \geq 1$, also $v_{\mathbf{p}}(\varphi) = v_{\mathbf{q}}(\varphi) = 1$ und $v_{\mathbf{z}}(\varphi) = 0$ für alle $\mathbf{z} \in C \setminus \{\mathbf{p}, \mathbf{q}\}$. Daher folgt $L \cap E = \{\mathbf{p}, \mathbf{q}, \mathbf{o}\}$ und $(\varphi) = -2P_{\mathbf{o}} + P_{\mathbf{p}} + P_{\mathbf{q}}$, also $P_{\mathbf{p}} + P_{\mathbf{q}} + P_{\mathbf{o}} \sim 3P_{\mathbf{o}}$ und daher $\mathbf{q} = \ominus \mathbf{p}$.

FALL 1b: $\mathbf{p} = \mathbf{q}$. Dann ist $v_{\mathbf{p}}(\varphi) \geq 2$, also $v_{\mathbf{p}}(\varphi) = 2$ und $v_{\mathbf{z}}(\varphi) = 0$ für alle $\mathbf{z} \in C \setminus \{\mathbf{p}\}$. Daher folgt $L \cap E = \{\mathbf{p}, \mathbf{o}\}$ und $(\varphi) = -2P_{\mathbf{o}} + 2P_{\mathbf{p}}$, also $2P_{\mathbf{p}} + P_{\mathbf{o}} \sim 3P_{\mathbf{o}}$, und $2[\mathbf{p}] = \mathbf{o}$.

FALL 2: $b \neq 0$. Dann ist $\mathbf{o} \notin \bar{L}$. Wegen $v_{\mathbf{o}}(x) = -2$ und $v_{\mathbf{o}}(y) = -3$ ist $v_{\mathbf{o}}(\varphi) = -3$, und daher

$$\sum_{\mathbf{z} \in C} \deg(P_{\mathbf{z}})v_{\mathbf{z}}(\varphi) = 3.$$

FALL 2a: $\mathbf{p} \neq \mathbf{q}$. Dann ist $v_{\mathbf{p}}(\varphi) \geq 1$ und $v_{\mathbf{q}}(\varphi) \geq 1$. Ist L die Tangente von C in \mathbf{p} , so ist $v_{\mathbf{p}}(\varphi) \geq 2$, also $v_{\mathbf{p}}(\varphi) = 2$, $v_{\mathbf{q}}(\varphi) = 1$ und $v_{\mathbf{z}}(\varphi) = 0$ für alle $\mathbf{z} \in C \setminus \{\mathbf{p}, \mathbf{q}\}$. Daher folgt $L \cap E = \{\mathbf{p}, \mathbf{q}\}$ und $(\varphi) = -3P_{\mathbf{o}} + 2P_{\mathbf{p}} + P_{\mathbf{q}}$, also $2P_{\mathbf{p}} + P_{\mathbf{q}} \sim 3P_{\mathbf{o}}$ und daher $[2]\mathbf{p} \oplus \mathbf{q} = \mathbf{o}$. Ist L die Tangente von C in \mathbf{q} , so folgt in gleicher Weise $P_{\mathbf{p}} + 2P_{\mathbf{q}} \sim 3P_{\mathbf{o}}$ und daher $\mathbf{p} \oplus [2]\mathbf{q} = \mathbf{o}$. Ist L nicht die Tangente von C in \mathbf{q} , so ist $v_{\mathbf{q}}(\varphi) = 1$, und daher gibt es einen Punkt $\mathbf{r} \in C \setminus \{\mathbf{p}, \mathbf{q}\}$ mit $\deg(P_{\mathbf{r}}) = v_{\mathbf{r}}(\varphi) = 1$. Es folgt $L \cap E = \{\mathbf{p}, \mathbf{q}, \mathbf{r}\}$ und $(\varphi) = -3P_{\mathbf{o}} + P_{\mathbf{p}} + P_{\mathbf{q}} + P_{\mathbf{r}}$, also $P_{\mathbf{p}} + P_{\mathbf{q}} + P_{\mathbf{r}} \sim 3P_{\mathbf{o}}$ und daher $\mathbf{p} \oplus \mathbf{q} \oplus \mathbf{r} = \mathbf{o}$.

FALL 2b: $\mathbf{p} = \mathbf{q}$. Dann ist $v_{\mathbf{p}}(\varphi) \geq 2$. Ist $v_{\mathbf{p}}(\varphi) \geq 3$, so ist $v_{\mathbf{z}}(\varphi) = 0$ für alle $\mathbf{z} \in C \setminus \{\mathbf{p}\}$. Daher folgt $L \cap E = \{\mathbf{p}\}$ und $(\varphi) = -3P_{\mathbf{o}} + 3P_{\mathbf{p}}$, also $3P_{\mathbf{p}} \sim 3P_{\mathbf{o}}$ und daher $[3]\mathbf{p} = \mathbf{o}$. Ist $v_{\mathbf{p}}(\varphi) = 2$, so gibt es einen Punkt $\mathbf{r} \in C \setminus \{\mathbf{p}\}$ mit $\deg(P_{\mathbf{r}}) = v_{\mathbf{r}}(\varphi) = 1$. Es folgt $\mathbf{r} \in C(K)$, $L \cap E = \{\mathbf{p}, \mathbf{r}\}$ und $(\varphi) = -3P_{\mathbf{o}} + 2P_{\mathbf{p}} + P_{\mathbf{r}}$, also $2P_{\mathbf{p}} + P_{\mathbf{r}} \sim 3P_{\mathbf{o}}$ und daher $[2]\mathbf{p} \oplus \mathbf{r} = \mathbf{o}$.

2. Genau dann ist $\alpha = \alpha'$, wenn $\mathbf{p}, \mathbf{p}' \in V(X - \alpha)$, und nach 1. ist das genau dann der Fall, wenn entweder $\mathbf{p} = \mathbf{p}'$ oder $\mathbf{p} + \mathbf{p}' = \mathbf{o}$. Genau dann ist $\mathbf{p} + \mathbf{p}' = \mathbf{o}$ (also $\mathbf{p}' = \ominus \mathbf{p}$), wenn $\mathbf{p}' = (\alpha, \beta')$ und

β, β' die einzigen Nullstellen von $f(\alpha, Y)$ sind. Dann ist aber $f(\alpha, Y) = c(Y - \beta)(Y - \beta')$ mit $c \in K^\times$, also $Y^2 - a_1\alpha Y - a_3Y - g(\alpha) = cY^2 - c(\beta + \beta')Y + c\beta\beta'$. Damit folgt $c = 1$ und $\beta + \beta' = -a_1\alpha - a_3$.

Sei nun $\mathbf{p}' \neq \ominus\mathbf{p}$. Sei L die Verbindungsgerade von \mathbf{p} und \mathbf{p}' , falls $\mathbf{p} \neq \mathbf{p}'$, und sei L die Tangente von C in \mathbf{p} , falls $\mathbf{p} = \mathbf{p}'$. Wegen $\mathbf{p} + \mathbf{p}' \neq \mathbf{o}$ ist dann $\mathbf{o} \notin L$ und daher $L = V(Y - \lambda X - \nu)$ mit den angegebenen Werten für $\lambda, \nu \in K$. Genau dann ist $\mathbf{p} \oplus \mathbf{p}' = \mathbf{p}'' = (\alpha'', \beta'')$, wenn $L \cap C = \{\mathbf{p}, \mathbf{p}', \ominus\mathbf{p}''\}$, und das ist genau dann der Fall, wenn $\alpha, \alpha', \alpha''$ die einzigen Nullstellen von $f(X, \lambda X + \nu)$ sind, und dann $\beta'' = -(\lambda\alpha'' + \nu) - a_1\alpha'' - a_3 = -(\lambda + a_1)\alpha'' - \nu - a_3$. Wir erhalten $f(X, \lambda X + \nu) = c(X - \alpha)(X - \alpha')(X - \alpha'')$ mit $c \in K^\times$ und daher

$$\begin{aligned} f(X, \lambda X + \nu) &= (\lambda X + \nu)^2 + a_1X(\lambda X + \nu) + a_3(\lambda X + \nu) - X^3 - a_2X^2 - a_4X - a_6 \\ &= cX^3 - c(\alpha + \alpha' + \alpha'')X^2 + c(\alpha\alpha' + \alpha\alpha'' + \alpha'\alpha'')X - c\alpha\alpha'\alpha''. \end{aligned}$$

Es folgt $c = -1$ und $\alpha + \alpha' + \alpha'' = \lambda^2 + a_1\lambda - a_2$. □

Endliche Erweiterungen algebraischer Funktionenkörper

In diesem Kapitel sei K ein vollkommener Körper.

7.1

Definition 7.1.1. Seien L/K und L'/K' Funktionenkörper. Man nennt L'/K' eine (endliche) *Funktionenkörpererweiterung* von L/K , wenn gilt: $L' \supset L$ ist eine endliche Körpererweiterung, $K' \supset K$, K ist der Konstantenkörper von L und K' ist der Konstantenkörper von L' . Insbesondere ist dann $K'L \subset L'$, und im Falle $K'L = L'$ nennt man L'/K' eine *Konstantenerweiterung* von L/K .

Satz 7.1.2. Sei L/K ein Funktionenkörper mit Konstantenkörper K .

1. Sei $L' \supset L$ eine endliche Körpererweiterung. Dann ist auch L'/K ein Funktionenkörper. Ist K' der Konstantenkörper von L'/K , so ist L'/K' eine Funktionenkörpererweiterung von L/K , $K' \cap L = K$, und $[K':K] < \infty$.
2. Sei $\bar{L} \supset L$ eine algebraische Hülle von L , $K \subset K' \subset \bar{L}$ ein Zwischenkörper und $[K':K] < \infty$. Dann ist $[K'L:L] = [K':K]$, und $K'L/K'$ ist ein Funktionenkörper mit Konstantenkörper K' . Insbesondere $K'L/K'$ eine Konstantenerweiterung von L/K .

(also die relative algebraische Hülle von K in L'), .

BEWEIS. 1. Sei $x \in L$ transzendent über K und $[L:K(x)] < \infty$. Dann ist $[L':K(x)] = [L':L][L:K(x)] < \infty$ und daher L'/K ein Funktionenkörper. Da K' die relative algebraische Hülle von K in L' ist, folgt $K' \cap L = K$, und nach Satz 3.7.2 ist $[K':K] < \infty$.

2. Sei $K' = K(\alpha)$ und $f \in K[X]$ das Minimalpolynom von α über K . Dann ist $LK' = L(\alpha)$, und wir zeigen, dass f irreduzibel über L ist (dann folgt $[L(\alpha):L] = \text{gr}(f) = [K(\alpha):K]$). Wir nehmen im Gegenteil an, es sei $f = gh$ mit $g, h \in L[X] \setminus L$. Sind $\alpha = \alpha_1, \dots, \alpha_n \in L$ die Nullstellen von f in \bar{L} , so liegen die Koeffizienten von g und h in $K(\alpha_1, \dots, \alpha_n) \cap L = K$, ein Widerspruch zur Irreduzibilität von f über K .

Es bleibt zu zeigen, dass $K(\alpha)$ der Konstantenkörper von $L(\alpha)$ ist. Sei also $\beta \in L(\alpha)$ algebraisch über $K(\alpha)$. Wegen der Vollkommenheit von K gibt es nach dem Satz vom primitiven Element ein Element $\gamma \in K(\alpha, \beta)$ mit $K(\alpha, \beta) = K(\gamma)$. Dann ist $L(\alpha) = L(\gamma)$, und nach dem eben Gezeigten folgt $[L(\gamma):L] = [K(\gamma):K] \geq [K(\alpha):K] = [L(\alpha):L] = [L(\gamma):L]$. Daher ist $\beta \in K(\gamma) = K(\alpha)$. \square

Satz 7.1.3. Sei L'/K' eine Funktionenkörpererweiterung von L/K .

1. Sei $P' \in \mathbb{P}_{L'}$ und $P = P' \cap L$. Dann ist $P \in \mathbb{P}_L$, $\mathcal{O}_P = \mathcal{O}_{P'} \cap L$, und P ist die einzige Stelle von L mit $P \subset P'$.
2. Ist $P \in \mathbb{P}_L$, so ist die Menge $\{P' \in \mathbb{P}_{L'} \mid P \subset P'\}$ endlich und nicht leer.

BEWEIS. 1. Sei $P' \in \mathbb{P}_{L'}$. Wir nehmen an, es sei $L \subset \mathcal{O}_{P'}$. Ist dann $z \in L' \setminus \mathcal{O}_{P'}$, also $v_{P'}(z) < 0$, so ist z algebraisch über L , und es besteht eine Gleichung $z^n + a_{n-1}z^{n-1} + \dots + a_1z + a_0 = 0$ mit $n \in \mathbb{N}$ und $a_0, \dots, a_{n-1} \in L$. Für $\nu \in [0, n-1]$ ist aber $v_{P'}(a_\nu z^\nu) = \nu v_{P'}(z) + v_{P'}(a_\nu) > \nu v_{P'}(z) = v_{P'}(z^\nu)$,

ein Widerspruch. Daher ist $L \cap \mathcal{O}_{P'} \subsetneq L$, und für $x \in L \setminus \mathcal{O}_{P'}$ ist $x^{-1} \in L \cap \mathcal{O}_{P'}$, also ist $L \cap \mathcal{O}_{P'}$ ein Bewertungsbereich von L , es gibt eine Stelle $P_1 \in \mathbb{P}_L$ mit $L \cap \mathcal{O}_{P'} = \mathcal{O}_{P_1}$, und wir zeigen $P_1 = P$. Ist $x \in P_1$, so ist $x^{-1} \in L \setminus \mathcal{O}_{P_1} \subset L' \setminus \mathcal{O}_{P'}$ und daher $x \in L \cap P' = P$. Nun ist aber $P = P' \cap L \subsetneq \mathcal{O}_{P'} \cap L = \mathcal{O}_{P_1}$ ein Ideal und daher $P \subset P_1$.

Ist $P_1 \in \mathbb{P}_L$ mit $P_1 \subset P'$, so folgt $P_1 \subset P$ und daher $P = P_1$ nach Satz 3.6.6.

2. Sei $P \in \mathbb{P}_L$. Nach Satz 4.6.2 gibt es ein $x \in L^\times$ so dass P die einzige Nullstelle von x ist. Ist $P' \in \mathbb{P}_{L'}$, so ist P' genau dann Nullstelle von x , wenn $x \in P' \cap L$, wenn also $P \subset P'$. Daher ist $\mathcal{N}^{L'}(x) = \{P' \in \mathbb{P}_{L'} \mid P' \supset P\}$, und diese Menge ist endlich und nicht leer. \square

Definition und Satz 7.1.4. Sei L'/K' eine Funktionkörpererweiterung von L/K .

1. Sei $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L'}$. Dann sind die folgenden Aussagen äquivalent:

- (a) $P \subset P'$.
- (b) $\mathcal{O}_P \subset \mathcal{O}_{P'}$.
- (c) Es gibt ein $e \in \mathbb{N}$, so dass $v_{P'} \mid L = e v_P: L \rightarrow \mathbb{Z} \cup \{\infty\}$.
- (d) $P = P' \cap L$.
- (e) $\mathcal{O}_P = \mathcal{O}_{P'} \cap L$.

Sind diese Bedingungen erfüllt, so ist $P' \cap \mathcal{O}_P = P$, und die Inklusion $\mathcal{O}_P \hookrightarrow \mathcal{O}_{P'}$ induziert einen Monomorphismus $L_P \rightarrow L'_{P'}$, vermöge dessen wir $L_P \subset L'_{P'}$ annehmen. Es ist dann $f(P'/P) = [L'_{P'}:L_P] < \infty$,

$$\deg(P') = \frac{\deg(P)f(P'/P)}{[K':K]}.$$

und $x(P') = x(P)$ für alle $x \in L$.

Man sagt, P' liegt über P , schreibt $P' \mid P$, nennt P die *Einschränkung* von P' auf L und $f(P'/P)$ den *Restklassengrad* von $P' \mid P$. Die Zahl $e = e(P'/P)$ in (c) heißt *Verzweigungsordnung* von $P' \mid P$. Ist $e(P'/P) > 1$, so nennt man $P' \mid P$ *verzweigt*, andernfalls *unverzweigt*.

2. Die Abbildung $j_{L'/L}: \mathbb{D}_L \rightarrow \mathbb{D}_{L'}$ sei wie folgt definiert: Für $P \in \mathbb{P}_L$ sei

$$j_{L'/L}(P) = \sum_{P' \mid P} e(P'/P) P' \quad (\text{Summe über alle } P' \in \mathbb{P}_{L'} \text{ mit } P' \mid P),$$

und für

$$D = \sum_{P \in \mathbb{P}_L} v_P(D) P \in \mathbb{D}_L \text{ sei } j_{L'/L}(D) = \sum_{P \in \mathbb{P}_L} v_P(D) j_{L'/L}(P) \in \mathbb{D}_{L'}.$$

Die Abbildung $j_{L'/L}$ heißt *Konorm* oder *Einbettung der Divisoren*.

$j_{L'/L}$ ist ein Monomorphismus, und für alle $x \in L^\times$ ist $j_{L'/L}((x)^L) = (x)^{L'}$, $j_{L'/L}((x)_0^L) = (x)_0^{L'}$ und $j_{L'/L}((x)_\infty^L) = (x)_\infty^{L'}$.

3. Für alle $P \in \mathbb{P}_L$ ist

$$[L':L] = \sum_{P' \mid P} e(P'/P) f(P'/P) \quad (\text{Summe über alle } P' \in \mathbb{P}_{L'} \text{ mit } P' \mid P),$$

also insbesondere $e(P'/P) \leq [L':L]$ und $f(P'/P) \leq [L':L]$ für alle $P' \mid P$.

4. Für alle $D \in \mathbb{D}_L$ ist

$$\deg(j_{L'/L}(D)) = \frac{\deg(D) [L':L]}{[K':K]},$$

5. Sei L''/K'' eine Funktionenkörpererweiterung von L'/K' . Dann ist L''/K'' auch eine Funktionenkörpererweiterung von L/K , $j_{L''/L} = j_{L''/L'} \circ j_{L'/L}$, und für $P \in \mathbb{P}_L$, $P' \in \mathbb{P}_{L'}$, $P'' \in \mathbb{P}_{L''}$ mit $P'' | P' | P$ ist $e(P''/P) = e(P''/P')e(P'/P)$ und $f(P''/P) = f(P''/P')f(P'/P)$.

BEWEIS. 1. (a) \Rightarrow (c) Für $0 \neq a \in P$ ist $v_{P'}(a) > 0$. Es folgt $v_{P'}(L^\times) = e\mathbb{Z}$ mit $e \in \mathbb{N}$, und daher ist $v_0 = e^{-1}v_{P'} | L: L \rightarrow \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung von L mit

$$P_{v_0} = \{x \in L \mid v_{P'}(x) > 0\} = P' \cap L \supset P = P_{v_P}.$$

Aus Satz 3.6.6 folgt $v_0 = v_P$, also $v_{P'} | L = e v_P$.

$$(c) \Rightarrow (d) \quad P = \{x \in L \mid v_P(x) > 0\} = \{x \in L \mid v_{P'}(x) > 0\} = P' \cap L.$$

$$(c) \Rightarrow (e) \quad \mathcal{O}_P = \{x \in L \mid v_P(x) \geq 0\} = \{x \in L \mid v_{P'}(x) \geq 0\} = \mathcal{O}_{P'} \cap L.$$

$$(d) \Rightarrow (a) \text{ und } (e) \Rightarrow (b) \text{ Offensichtlich.}$$

(b) \Rightarrow (a) Nach Satz 7.1.3 gibt es eine Stelle $P_1 \in \mathbb{P}_L$ mit $P_1 \subset P'$, und für diese ist $\mathcal{O}_{P_1} = \mathcal{O}_{P'} \cap L$, also $\mathcal{O}_P \subset \mathcal{O}_{P_1}$. Damit folgt $\mathcal{O}_P = \mathcal{O}_{P_1}$ und $P = P_1 \subset P'$.

Sind diese Bedingungen erfüllt, so ist $P' \cap \mathcal{O}_P = P' \cap L \cap \mathcal{O}_P = P$, und daher induziert $\mathcal{O}_P \hookrightarrow \mathcal{O}_{P'}$ einen Monomorphismus $L_P = \mathcal{O}_P/P \rightarrow \mathcal{O}_{P'}/P' = L'_{P'}$. Nach Identifizierung ist $K \subset L_P \subset L'_{P'}$, und $[L'_{P'}:K] = [L'_{P'}:K'] [K':K] < \infty$. Nun ist

$$f(P'/P) = [L'_{P'}:L_P] = \frac{[L'_{P'}:K]}{[L_P:K]} = \frac{[L'_{P'}:K'] [K':K]}{[L_P:K]} = \frac{\deg(P') [K':K]}{\deg(P)}.$$

2. Offensichtlich ist $j_{L'/L}$ ein Gruppenmonomorphismus. Für $x \in L^\times$ ist

$$(x)^{L'} = \sum_{P' \in \mathbb{P}_{L'}} v_{P'}(x) P' = \sum_{P \in \mathbb{P}_L} \sum_{P' | P} e(P'/P) v_P(x) P' = \sum_{P \in \mathbb{P}_L} v_P(x) j_{L'/L}(P) = j_{L'/L}((x)^L).$$

Für $x \in L$, $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L'}$ mit $P' | P$ ist genau dann $v_P(x) \geq 0$, wenn $v_{P'} \geq 0$. Daher folgen die Aussagen über den Nullstellen- und Polstellendivisor.

3. Sei $P \in \mathbb{P}_L$. Nach Satz 4.6.2 gibt es ein $x \in L$, so dass P die einzige Nullstelle von x in L ist. Dann sind die $P' \in \mathbb{P}_{L'}$ mit $P' | P$ genau die Nullstellen von x in L . Aus Satz 4.2.1 folgt

$$\begin{aligned} [L':K'(x)] &= \deg((x)_0^{L'}) = \sum_{P' | P} v_{P'}(x) \deg(P') = \sum_{P' | P} e(P'/P) v_P(x) \frac{\deg(P) f(P'/P)}{[K':K]} \\ &= \frac{\deg((x)_0^L)}{[K':K]} \sum_{P' | P} e(P'/P) f(P'/P) = \frac{[L:K(x)]}{[K':K]} \sum_{P' | P} e(P'/P) f(P'/P) \end{aligned}$$

und daher

$$\sum_{P' | P} e(P'/P) f(P'/P) = \frac{[L':K'(x)] [K':K]}{[L:K(x)]} = \frac{[L':K'(x)] [K'(x):K(x)]}{[L:K(x)]} = [L':L].$$

4. Es genügt, die Formel für $D = P \in \mathbb{P}_L$ zu zeigen. Es ist

$$\deg(j_{L'/L}(P)) = \sum_{P' | P} e(P'/P) \deg(P') = \sum_{P' | P} e(P'/P) \frac{\deg(P) f(P'/P)}{[K':K]} = \frac{\deg(P) [L':L]}{[K':K]}.$$

5. Offensichtlich. □

7.2

Definition 7.2.1. Sei L/K ein Funktionenkörper mit Konstantenkörper \tilde{K} . Für eine Teilmenge $S \subset \mathbb{P}_L$ sei

$$\mathcal{O}_S = \bigcap_{P \in S} \mathcal{O}_P \quad (\text{also } \mathcal{O}_S = \tilde{K}, \text{ falls } S = \mathbb{P}_L, \text{ und } \mathcal{O}_S = L, \text{ falls } S = \emptyset).$$

\mathcal{O}_S ist die Menge aller Funktionen $x \in L$, die an allen Stellen $P \in S$ regulär sind.

Ein Teilbereich $R \subset K$ heißt *Holomorphiebereich* von L/K , wenn $R = \mathcal{O}_S$ mit einer Menge $\emptyset \neq S \subsetneq \mathbb{P}_L$.

Insbesondere ist jeder Bewertungsbereich \mathcal{O} mit $K \subsetneq \mathcal{O} \subsetneq L$ ein Holomorphiebereich.

Definition 7.2.2. Sei L ein Körper und $R \subset L$ ein Teilbereich.

1. Ein Element $x \in L$ heißt *ganz* über R , wenn es ein normiertes Polynom $f \in R[X]^\bullet$ gibt mit $f(x) = 0$ [äquivalent: Es besteht eine Relation $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ mit $n \in \mathbb{N}$ und $a_0, \dots, a_{n-1} \in R$. Jede solche Relation heißt *ganze Gleichung* von x über R .]
2. Eine *ganz-algebraische Zahl* ist eine komplexe Zahl, die ganz über \mathbb{Z} ist.
3. $\text{cl}_L(R) = \{x \in L \mid x \text{ ist ganz über } R\}$ heißt *ganzer Abschluss* von R in L .
4. R heißt *ganz-abgeschlossen*, wenn $\text{cl}_{\mathfrak{q}(R)}(R) = R$.

Satz 7.2.3. Sei L/K ein Funktionenkörper und $\emptyset \neq S \subsetneq \mathbb{P}_L$.

1. $L = \mathfrak{q}(\mathcal{O}_S)$.
2. \mathcal{O}_S ist ganz-abgeschlossen.
3. Ist S endlich, so ist \mathcal{O}_S ein Hauptidealbereich.
4. Sei $\emptyset \neq T \subsetneq \mathbb{P}_L$. Genau dann ist $T \subset S$, wenn $\mathcal{O}_S \subset \mathcal{O}_T$.

Insbesondere gilt: Ist $P \in \mathbb{P}_L$, so ist genau dann $P \in S$, wenn $\mathcal{O}_S \subset \mathcal{O}_P$.

BEWEIS. 1. Sei $x \in L^\times$. Nach Satz 4.6.2 gibt es ein $z \in L$ mit $v_P(z) \geq \max\{0, -v_P(x)\}$ für alle $P \in S$. Dann ist $v_P(z) \geq 0$ und $v_P(xz) \geq 0$ für alle $P \in S$, also $z, xz \in \mathcal{O}_S$ und $x = z^{-1}(xz) \in \mathfrak{q}(\mathcal{O}_S)$.

2. Wir nehmen an, es sei $x \in L \setminus \mathcal{O}_S$ ganz über \mathcal{O}_S . Dann gibt es ein $P \in S$ mit $v_P(x) < 0$, und es besteht eine ganze Gleichung $x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 = 0$ mit $n \in \mathbb{N}$ und $a_0, \dots, a_{n-1} \in \mathcal{O}_S$. Dann ist aber $v_P(x^n) = nv_P(x) < v_P(a_i x^i)$ für alle $i \in [0, n-1]$, ein Widerspruch.

3. Sei $S = \{P_1, \dots, P_n\}$ und $\{0\} \neq \mathfrak{a} \triangleleft \mathcal{O}_S$. Für $i \in [1, n]$ ist $n_i = \min v_{P_i}(\mathfrak{a}) \in \mathbb{N}_0$, und es sei $a_i \in \mathfrak{a}$ mit $v_{P_i}(a_i) = n_i$. Nach Satz 3.6.7 gibt es zu jedem $i \in [1, n]$ ein $z_i \in L$ mit $v_{P_i}(z_i) = 0$ und $v_{P_j}(z_i) > n_j$ für alle $j \in [1, n] \setminus \{i\}$. Insbesondere folgt $z_1, \dots, z_n \in \mathcal{O}_S$, $a = a_1 z_1 + \dots + a_n z_n \in \mathfrak{a}$, und wir zeigen $\mathfrak{a} = \mathcal{O}_S(a)$. Für $i \in [1, n]$ ist $v_{P_i}(a_i z_i) = n_i$, für alle $j \in [1, n] \setminus \{i\}$ ist $v_{P_j}(a_j z_j) > n_j$, und daher folgt $v_{P_i}(a) = n_i$, also insbesondere $a \neq 0$. Ist nun $x \in \mathfrak{a}$, so folgt $v_{P_i}(a^{-1}x) = -n_i + v_{P_i}(x) \geq 0$ für alle $i \in [1, n]$, also $a^{-1}x \in \mathcal{O}_S$ und $x \in (a)$.

4. Aus $T \subset S$ folgt $\mathcal{O}_S \subset \mathcal{O}_T$. Sei also $T \not\subset S$ und $Q \in T \setminus S$. Nach Satz 4.6.2 gibt es ein $x \in L$ mit $v_Q(x) < 0$ und $v_P(x) \geq 0$ für alle $P \in S$. Dann ist aber $x \in \mathcal{O}_S \setminus \mathcal{O}_T$. \square

7.3

Satz 7.3.1. Sei L/K ein Funktionenkörper mit Konstantenkörper \tilde{K} , und sei $R \subset L$ ein Teilbereich, so dass $\tilde{K} \subset R$ und R kein Körper ist. Dann ist $\emptyset \neq S(R) = \{P \in \mathbb{P}_L \mid R \subset \mathcal{O}_P\} \subsetneq \mathbb{P}_L$, und $\mathcal{O}_{S(R)} = \text{cl}_L(R)$. Insbesondere ist $\text{cl}_L(R)$ ein ganz-abgeschlossener Teilbereich von L und $\mathfrak{q}(\text{cl}_L(R)) = L$.

BEWEIS. Da R kein Körper ist, gibt es ein Ideal $\{0\} \neq I \subsetneq R$, und nach Satz 3.3.3 gibt es ein $P \in \mathbb{P}_L$ mit $R \subset \mathcal{O}_P$, also $P \in S(R)$. Ist $x \in R \setminus \tilde{K}$, so gibt es ein $P \in \mathbb{P}_L$ mit $v_P(x) < 0$ und daher $P \notin S(R)$.

Natürlich ist $R \subset \mathcal{O}_{S(R)}$. Ist $x \in L$ ganz über R , so ist x auch ganz über $\mathcal{O}_{S(R)}$, also $x \in \mathcal{O}_{S(R)}$, und daher folgt $\text{cl}_L(R) \subset \mathcal{O}_{S(R)}$. Sei nun $0 \neq z \in \mathcal{O}_{S(R)}$. Dann ist $z^{-1}R[z^{-1}] \triangleleft R[z^{-1}]$, und wir zeigen $z^{-1}R[z^{-1}] = R[z^{-1}]$. Dann besteht nämlich eine Gleichung $1 = z^{-1}(a_0 + a_1z^{-1} + \dots + a_nz^{-n})$ mit $n \in \mathbb{N}$ und $a_0, \dots, a_n \in R$, und es folgt $z^{n+1} - a_0z^n - a_1z^{n-1} - \dots - a_n = 0$, also eine ganze Gleichung von z über R und damit $z \in \text{cl}(R)$.

Wir nehmen nun an, es sei $z^{-1}R[z^{-1}] \subsetneq R[z^{-1}]$. Nach Satz 3.3.3 gibt es dann ein $Q \in \mathbb{P}_L$ mit $R[z^{-1}] \subset \mathcal{O}_Q$ und $z^{-1} \in Q$, also $Q \in S(R)$ und $z \notin \mathcal{O}_Q$, ein Widerspruch. \square

7.4

Definition und Satz 7.4.1. Sei L/K eine endliche separable Körpererweiterung, $[L:K] = n$ und \overline{K} eine algebraische Hülle von L . Dann gibt es genau n K -Homomorphismen $\sigma_1, \dots, \sigma_n: L \rightarrow \overline{K}$, die man wie folgt erhält:

Sei $L = K(\alpha)$, $f \in K[X]$ das Minimalpolynom von α über K , und seien $\alpha_1, \dots, \alpha_n \in \overline{K}$ die verschiedenen Nullstellen von f in \overline{K} . Dann ist $\sigma_i: L \rightarrow \overline{K}$ der eindeutig bestimmte K -Homomorphismus mit $\sigma_i(\alpha) = \alpha_i$.

Für $x \in L$ definieren wir die *Spur* von x durch $S_{L/K}(x) = \sigma_1(x) + \dots + \sigma_n(x)$.

1. $S_{L/K}: L \rightarrow K$ ist ein K -Vektorraumepimorphismus, und für $a \in K$ ist $S_{L/K}(a) = na$.
2. Ist (u_1, \dots, u_n) eine K -Basis von L , so gibt es eindeutig bestimmte Elemente $u_1^*, \dots, u_n^* \in L$, so dass $S_{L/K}(u_i u_j^*) = \delta_{i,j}$ für alle $i, j \in [1, n]$, und (u_1^*, \dots, u_n^*) ist eine K -Basis von L . (u_1^*, \dots, u_n^*) heißt die zu (u_1, \dots, u_n) komplementäre Basis.
3. Ist $K \subset M \subset L$ ein Zwischenkörper, so ist $S_{L/K} = S_{M/K} \circ S_{L/M}$.
4. Sei $x \in L$, $f = X^d + a_{d-1}X^{d-1} + \dots + a_1X + a_0 \in K[X]$ das Minimalpolynom von x über K und $m = [L:K(x)]$. Dann ist $S_{L/K}(x) = -ma_{d-1}$.

BEWEIS. 1. Für $x, y \in L$ und $a \in K$ ist $sS_{L/K}(x+y) = S_{L/K}(x) + S_{L/K}(y)$, $S_{L/K}(ax) = aS_{L/K}(x)$ und $S_{L/K}(a) = na$. Daher ist $S_{L/K}: L \rightarrow L$ ein K -Vektorraumhomomorphismus. Sei nun $x \in L$. Für den Nachweis von $S_{L/K}(x) \in K$ zeigen wir $\sigma(S_{L/K}(x)) = S_{L/K}(x)$ für alle K -Homomorphismus $\sigma: L \rightarrow \overline{K}$. Sei also $\sigma: L \rightarrow \overline{K}$ ein K -Homomorphismus und $\bar{\sigma}: \overline{K} \rightarrow \overline{K}$ ein Isomorphismus mit $\bar{\sigma}|_L = \sigma$. Dann ist $(\bar{\sigma} \circ \sigma_1, \dots, \bar{\sigma} \circ \sigma_n) = (\sigma_1, \dots, \sigma_n)$ und daher $\sigma(S_{L/K}(x)) = \bar{\sigma}(S_{L/K}(x)) = S_{L/K}(x)$. $S_{L/K} \neq 0$ folgt aus 2.

2. Sei $L = K(\alpha)$ und $A = (\sigma_i(\alpha^{\nu-1}))_{i,\nu \in [1,n]}$. Dann ist $(1, \alpha, \dots, \alpha^{n-1})$ ist eine K -Basis von L , und

$$\det(A) = \prod_{1 \leq i < j \leq n} (\sigma_j(\alpha) - \sigma_i(\alpha)) \neq 0.$$

Sei $(u_1, \dots, u_n) \in L^n$ eine K -Basis von L und $(u_1^*, \dots, u_n^*) \in L^n$. Dann gibt es Matrizen $T, T^* \in M_n(K)$ mit $(u_1, \dots, u_n) = (1, \alpha, \dots, \alpha^{n-1})T$, $(u_1^*, \dots, u_n^*) = (1, \alpha, \dots, \alpha^{n-1})T^*$ und $\det(T) \neq 0$. Sei nun $U = (\sigma_i(u_\nu))_{i,\nu \in [1,n]} = AT$ und $U^* = (\sigma_i(u_\nu^*))_{i,\nu \in [1,n]} = AT^*$. Dann ist

$$(S_{L/K}(u_i u_j^*))_{i,j \in [1,n]} = U^t U^* = T^t A^t A T^*$$

Daher gibt es genau eine Matrix $T^* \in \text{GL}_n(K)$, so dass $S_{L/K}(u_i u_j^*) = \delta_{i,j}$ für alle $i, j \in [1, n]$, und damit folgt die Existenz und Eindeutigkeit von (u_1^*, \dots, u_n^*) .

3. Sei $\text{Hom}_K(M, \overline{K}) = \{\tau_1, \dots, \tau_d\}$ und $\text{Hom}_M(L, \overline{K}) = \{\sigma_1, \dots, \sigma_m\}$. Für $i \in [1, d]$ sei $\bar{\tau}_i: \overline{K} \rightarrow \overline{K}$ ein Isomorphismus mit $\bar{\tau}_i|_M = \tau_i$. Dann ist $\text{Hom}_K(L, \overline{K}) = \{\bar{\tau}_i \circ \sigma_j \mid i \in [1, d], j \in [1, m]\}$, und für

$x \in L$ folgt

$$\mathcal{S}_{L/K}(x) = \sum_{i=1}^d \sum_{j=1}^m \bar{\tau}_i \circ \sigma_j(x) = \sum_{i=1}^d \bar{\tau}_i(\mathcal{S}_{L/M}(x)) = \sum_{i=1}^d \tau_i(\mathcal{S}_{L/M}(x)) = \mathcal{S}_{M/K} \circ \mathcal{S}_{L/M}(x).$$

4. Es ist $n = [L:K(x)][K(x):K] = md$. Sei $\text{Hom}_K(K(x), \bar{K}) = \{\sigma_1, \dots, \sigma_d\}$. Dann ist

$$f = \prod_{i=1}^d (X - \sigma_i(x)), \quad \text{also} \quad a_{d-1} = -\sum_{i=1}^d \sigma_i(x)$$

und daher $\mathcal{S}_{L/K}(x) = \mathcal{S}_{K(x)/K} \circ \mathcal{S}_{L/K(x)}(x) = \mathcal{S}_{K(x)/K}(mx) = m\mathcal{S}_{K(x)/K}(x) = -ma_{d-1}$. \square

Satz 7.4.2. Sei L/K eine endliche separable Körpererweiterung, $n = [L:K]$, $R \subset K$ ein ganz-abgeschlossener Teilbereich mit $K = \mathfrak{q}(R)$ und $R' = \text{cl}_L(R)$.

1. Sei $x \in L$ und $f \in K[X]$ das Minimalpolynom von x über K . Genau dann ist $x \in R'$, wenn $f \in R[X]$, und dann ist auch $\mathcal{S}_{L/K}(x) \in R$.
2. $L = \{a^{-1}x \mid a \in R^\bullet, x \in R'\}$. Insbesondere enthält R' eine K -Basis von L .
3. Sei $(u_1, \dots, u_n) \in R'^n$ eine K -Basis von L und (u_1^*, \dots, u_n^*) die zu (u_1, \dots, u_n) komplementäre Basis. Dann ist $R' \subset Ru_1^* + \dots + Ru_n^*$.
4. Ist R ein Hauptidealbereich, so gibt es eine K -Basis (u_1, \dots, u_n) von L mit $R' = Ru_1 + \dots + Ru_n$.

BEWEIS. Algebra. \square

Definition und Satz 7.4.3. Sei L'/K' eine Funktionenkörpererweiterung von L/K . Für $P \in \mathbb{P}_L$ sei $\mathcal{O}'_P = \text{cl}_{L'}\mathcal{O}_P$.

Eine L -Basis (u_1, \dots, u_n) von L' heißt *Ganzheitsbasis* von L'/L für P , wenn $\mathcal{O}'_P = \mathcal{O}_P u_1 + \dots + \mathcal{O}_P u_n$.

1. Sei $P \in \mathbb{P}_L$. Dann ist

$$\mathcal{O}'_P = \text{cl}_{L'}\mathcal{O}_P = \bigcap_{P' \mid P} \mathcal{O}_{P'}, \quad \text{und es gibt eine Ganzheitsbasis von } L'/L \text{ für } P.$$

2. Jede L -Basis von L' ist eine Ganzheitsbasis für fast alle $P \in \mathbb{P}_L$.

BEWEIS. 1. Nach den Sätzen 7.3.1 und 7.4.2.

2. Sei (u_1, \dots, u_n) eine L -Basis von L' und (u_1^*, \dots, u_n^*) die komplementäre Basis. Dann gibt es eine endliche Menge $S \subset \mathbb{P}_L$, so dass alle Polstellen der Koeffizienten der Minimalpolynome von $u_1, \dots, u_n, u_1^*, \dots, u_n^*$ in S liegen. Für alle $P \in \mathbb{P}_L \setminus S$ ist dann $\{u_1, \dots, u_n, u_1^*, \dots, u_n^*\} \subset \mathcal{O}'_P$, und aus Satz 7.4.2 folgt

$$\mathcal{O}'_P \subset \sum_{i=1}^n \mathcal{O}_P u_i^* \subset \mathcal{O}'_P, \quad \text{also Gleichheit.} \quad \square$$

7.5

Definition und Satz 7.5.1. Sei L'/K' eine Funktionenkörpererweiterung von L/K , $P \in \mathbb{P}_L$ und $\mathcal{O}'_P = \text{cl}_{L'}(\mathcal{O}_P)$.

Dann heißt $\mathcal{C}_P = \{z \in L \mid \mathcal{S}_{L'/L}(z\mathcal{O}'_P) \subset \mathcal{O}_P\}$ der *Komplementärmodul* von L'/L über \mathcal{O}_P .

1. Sei (u_1, \dots, u_n) eine Ganzheitsbasis von L'/L für P und (u_1^*, \dots, u_n^*) die komplementäre Basis. Dann ist $\mathcal{C}_P = \mathcal{O}_P u_1^* + \dots + \mathcal{O}_P u_n^* \supset \mathcal{O}'_P$, und $\mathcal{O}'_P \mathcal{C}_P = \mathcal{C}_P$.

2. Es gibt ein $t \in L'$ mit $\mathcal{C}_P = t\mathcal{O}'_P$. Für alle $P' \in \mathbb{P}_L$ mit $P' | P$ ist $v_{P'}(t) \leq 0$ und hängt nur von P' ab. Insbesondere ist $\mathcal{C}_P = \mathcal{O}'_P$ für fast alle $P \in \mathbb{P}_L$.

Die Zahl $d(P'/P) = -v_{P'}(t) \in \mathbb{N}_0$ heißt *Differentenexponent* von $P' | P$, und der Divisor

$$D_{L/L'} = \sum_{P \in \mathbb{P}_L} \sum_{P' | P} d(P'/P) P' \in \mathbb{D}_{L'}$$

heißt *Differente* von L'/L .

Für $z \in L'$ ist genau dann $z \in \mathcal{C}_P$, wenn $v_{P'}(z) \geq -d(P'/P)$ für alle $P' | P$.

BEWEIS. 1. Sei $z = c_1 u_1^* + \dots + c_n u_n^* \in L'$ mit $c_1, \dots, c_n \in L$. Wegen $\mathcal{O}'_P = \mathcal{O}_P u_1 + \dots + \mathcal{O}_P u_n$ gilt:

$$z \in \mathcal{C}_P \iff S_{L'/L}(z\mathcal{O}'_P) \subset \mathcal{O}_P \iff S_{L'/L}(z u_i) = \sum_{\nu=1}^n c_\nu S_{L'/L}(u_\nu^* u_i) = c_i \in \mathcal{O}_P \text{ für alle } i \in [1, n].$$

Also ist genau dann $z \in \mathcal{C}_P$, wenn $z \in \mathcal{O}_P u_1^* + \dots + \mathcal{O}_P u_n^*$, und es folgt $\mathcal{C}_P \supset \mathcal{O}'_P$ nach Satz 7.4.2. Ist $x \in \mathcal{O}'_P$ und $z \in \mathcal{C}_P$, so folgt $S_{L'/L}(xz\mathcal{O}'_P) \subset S_{L'/L}(z\mathcal{O}'_P) \subset \mathcal{O}_P$ und daher $xz \in \mathcal{C}_P$.

2. Nach Satz 7.4.2 gibt es ein $a \in \mathcal{O}'_P$, so dass $au_i^* \in \mathcal{O}'_P$ für alle $i \in [1, n]$ und daher $a\mathcal{C}_P \subset \mathcal{O}'_P$. Dann ist $a\mathcal{C}_P$ ein Ideal von \mathcal{O}'_P , und nach den Sätzen 7.2.3 und 7.4.3 ist \mathcal{O}'_P ein Hauptidealbereich. Daher gibt es ein $t_1 \in \mathcal{O}'_P$ mit $a\mathcal{C}_P = t_1\mathcal{O}'_P$. Ist $t = a^{-1}t_1$, so folgt $\mathcal{C}_P = t\mathcal{O}'_P$, und wegen $\mathcal{O}'_P \subset \mathcal{C}_P$ gibt es ein $s \in \mathcal{O}'_P$ mit $st = 1$, also $v_{P'}(t) = -v_{P'}(s) \leq 0$ für alle $P' | P$. Ist $t' \in L$ mit $\mathcal{C}_P = t\mathcal{O}'_P = t'\mathcal{O}'_P$, so folgt $t' = te$ mit $e \in \mathcal{O}'_P \times \subset \mathcal{O}'_P \times$ für alle $P' | P$ und daher $v_{P'}(t) = v_{P'}(t')$. \square

7.6

Satz 7.6.1 (Dedekind'scher Differentensatz). Sei L'/K' eine Funktionenkörpererweiterung von L/K , sei L'/L separabel, $L' = L(y)$, $f \in L[X]$ das Minimalpolynom von y über L und $P \in \mathbb{P}_L$.

1. Sei $P' \in \mathbb{P}_{L'}$ mit $P' | P$.
 - (a) $e(P'/P) - 1 \leq d(P'/P) \leq v_{P'}(f'(y))$.
 - (b) Genau dann ist $d(P'/P) = e(P'/P) - 1$, wenn $\text{char}(K) \nmid e(P' | P)$.
2. Sei $[L' : L] = n$ und $d(P'/P) = v_{P'}(f'(y))$ für alle $P' \in \mathbb{P}_L$ mit $P' | P$. Dann ist $(1, y, \dots, y^{n-1})$ eine Ganzheitsbasis von L'/L für P .

OHNE BEWEIS. \square

Satz 7.6.2 (Hurwitz'sche Geschlechtsformel). Sei L'/K' eine Funktionenkörpererweiterung von L/K , und sei L'/L separabel. Dann ist

$$2g_{L'} - 2 = \frac{[L' : L]}{[K' : K]} (2g_L - 2) + \deg(D_{L'/L}).$$

OHNE BEWEIS. \square

Satz 7.6.3. Sei L'/K' eine Funktionenkörpererweiterung von L/K , und sei $L' = LK'$.

1. Für alle $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L'}$ mit $P' | P$ ist $e(P'/P) = 1$ und $L'_{P'} = L_P K'$.
2. $g_{L'} = g_L$.

BEWEIS. 1. Sei $K' = K(\alpha)$ und $f \in K[X]$ das Minimalpolynom von α über K . Dann ist $L' = L(\alpha)$ und f ist auch das Minimalpolynom von α über L . Wegen $f'(\alpha) \in K'$ ist $v_{P'}(f(\alpha)) = 0$ für alle $P' \in \mathbb{P}_{L'}$. Nach Satz 7.6.1 ist $(1, \alpha, \dots, \alpha^{n-1})$ eine Ganzheitsbasis von L'/L für alle $P \in \mathbb{P}_L$, und $e(P'/P) = 0$ für alle $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L'}$ mit $P' | P$.

Sei nun $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L'}$ mit $P' | P$. Wir zeigen $z(P') \in L_P K'$ für alle $z \in L'$ (damit folgt dann $L_{P'} = L_P K'$). Sei also $z \in L'$, seien P_2, \dots, P_r die übrigen Stellen von L' über P und $\mathcal{O}'_P = \text{cl}_{L'}(\mathcal{O}_P) = \mathcal{O}_{P'} \cap \mathcal{O}_{P_2} \cap \dots \cap \mathcal{O}_{P_r} = \mathcal{O}_P + \mathcal{O}_P \alpha + \dots + \mathcal{O}_P \alpha^{n-1}$. Nach Satz 3.6.7 gibt es ein $u \in L'$ mit $v_{P'}(u - z) > 0$ und $v_{P_i}(u) \geq 0$ für alle $i \in [2, r]$. Dann ist $u \in \mathcal{O}'_P$, also

$$u = \sum_{i=0}^{n-1} \gamma_i \alpha^i, \quad \text{und daher} \quad z(P') = u(P') = \sum_{i=0}^{n-1} \gamma_i(P') \alpha^i = \sum_{i=0}^{n-1} \gamma_i(P) \alpha^i \in L_P K'.$$

2. Nach Satz 7.6.2. □

Funktionenkörper über endlichem Konstantenkörper

Im diesem Kapitel sei q eine Primzahlpotenz, \mathbb{F}_q ein Körper mit q Elementen und L/\mathbb{F}_q ein Funktionenkörper mit Konstantenkörper \mathbb{F}_q und Geschlecht $g_L = g$.

8.1

Lemma 8.1.1. Seien $F \subset E_1, E_2 \subset E$ endliche Körper und $E = E_1E_2$. Dann ist

$$[E:F] = \text{kgV}([E_1:F], [E_2:F]).$$

BEWEIS. Sei \bar{F} eine algebraische Hülle von F und $E \subset F$. Sei Ω die Menge aller Zwischenkörper $F \subset K \subset \bar{F}$. Dann ist die Abbildung $\Phi: (\Omega, \subset) \rightarrow (\mathbb{N}, |)$, definiert durch $\Phi(K) = [K:F]$, ein Verbandsisomorphismus. Für alle $K_1, K_2 \in \Omega$ ist genau dann $K_1 \subset K_2$, wenn $\Phi(K_1) \mid \Phi(K_2)$, also auch $[K_1K_2:F] = \text{kgV}([K_1:F], [K_2:F])$ und $[K_1 \cap K_2:F] = \text{ggT}([K_1:F], [K_2:F])$. \square

Definition und Satz 8.1.2. Sei \bar{L} eine algebraische Hülle von L . Für $r \in \mathbb{N}$ sei $\mathbb{F}_q \subset \mathbb{F}_{q^r} \subset \bar{L}$ und $L_r = L\mathbb{F}_{q^r}$. L_r heißt *Konstantenerweiterung r -ten Grades* von L .

1. $[L_r:L] = r$, \mathbb{F}_{q^r} ist der Konstantenkörper von L_r , und $g_{L_r} = g$.
2. Sei $P \in \mathbb{P}_L$, $\deg(P) = m$ und $d = \text{ggT}(m, r)$. Dann ist $j_{L_r/L}(P) = P_1 + \dots + P_d$ mit verschiedenen $P_1, \dots, P_d \in \mathbb{P}_{L_r}$, und für alle $i \in [1, d]$ ist $\deg(P_i) = \frac{m}{d}$.

BEWEIS. Nach Satz 7.1.2 ist $[L_r:L] = [\mathbb{F}_{q^r}:\mathbb{F}_q] = r$, und \mathbb{F}_{q^r} ist der Konstantenkörper von L_r . Nach Satz 7.6.3 ist $g_{L_r} = g$ und $e(P'/P) = 1$ für alle $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L_r}$ mit $P' \mid P$.

Sei nun $P \in \mathbb{P}_L$, und seien P_1, \dots, P_d die über P liegenden Stellen von L' . Für alle $i \in [1, r]$ ist $(L_r)_{P_i} = \mathbb{F}_{q^r}L_P$ nach Satz 7.6.3, also

$$\deg(P_i) = [(L_r)_{P_i}:\mathbb{F}_{q^r}] = \frac{[(L_r)_{P_i}:\mathbb{F}_q]}{r} = \frac{\text{kgV}([\mathbb{F}_{q^r}:\mathbb{F}_q], [L_P:\mathbb{F}_q])}{r} = \frac{\text{kgV}(m, r)}{r} = \frac{m}{\text{ggT}(m, r)}.$$

Nach Satz 7.1.4 ist

$$\deg(P_i) = \frac{\deg(P)f(P_i/P)}{r} = \frac{mf(P_i/P)}{r}, \quad \text{also} \quad f(P_i/P) = \frac{r}{\text{ggT}(m, r)}$$

und

$$r = [L_r:L] = \sum_{i=1}^d e(P_i/P)f(P_i/P) = d \frac{r}{\text{ggT}(m, r)}, \quad \text{also} \quad d = \text{ggT}(m, r). \quad \square$$

Definition 8.1.3. Für $n \in \mathbb{N}_0$ sei $\mathbb{D}_L^n = \{D \in \mathbb{D}_L \mid \deg(D) = n\}$, $\mathcal{C}_L^n = \{[D] \in \mathcal{C}_L \mid \deg(D) = n\}$, $\partial = \text{ggT}(\{\deg(P) \mid P \in \mathbb{P}_L\}) = \min\{\deg(D) \mid D \in \mathbb{D}_L, D > 0\}$ und $A_n = |\{D \in \mathbb{D}_L^n \mid D \geq 0\}|$.

Insbesondere ist $A_0 = 1$ und $A_1 = |\mathbb{P}_L^1|$. Es ist $\deg(\mathbb{D}_L) = \deg(\mathcal{C}_L) = \partial\mathbb{Z}$, und für alle $n \in \mathbb{N}$ mit $\partial \nmid n$ ist $A_n = 0$.

Nach Satz 4.2.2 ist $\mathcal{C}_L^0 = \mathbb{D}_L^0/(L^\times)$. $h = h_L = |\mathcal{C}_L^0|$ heißt *Klassenzahl* von L . Für alle $n \in \partial\mathbb{N}_0$ ist $|\mathcal{C}_L^n| = |\deg^{-1}(n\mathbb{Z})| = h_L$.

Satz 8.1.4.

1. Für alle $n \in \mathbb{N}_0$ ist $A_n < \infty$.
2. $h < \infty$, und aus $g = 0$ folgt $h = 1$.

BEWEIS. 1. Sei $x \in L \setminus \mathbb{F}_q$. Für $P \in \mathbb{P}_{\mathbb{F}_q(x)}$ und $P' \in \mathbb{P}_L$ mit $P' | P$ folgt aus Satz 7.1.4

$$\deg(P') = \deg(P)f(P'/P) \leq \deg(P) [\mathbb{F}_q:K(x)].$$

Für jedes $n \in \mathbb{N}$ gibt es nur endlich viele normierte irreduzible Polynome vom Grade n . Daher ist $\mathbb{P}^n d_{\mathbb{F}_q(x)}$ endlich. Folglich sind auch alle Mengen \mathbb{P}_L^n endlich. Ist $n \in \mathbb{N}$ und $D \in \mathbb{D}_L^n$ mit $D \geq 0$, so ist

$$D = \sum_{P \in \mathbb{P}_L} n_P P \quad \text{mit } n_P \in \mathbb{N}_0 \quad \text{und} \quad \sum_{P \in \mathbb{P}_L} n_P = n.$$

Daher ist auch $A_n = |\{D \in \mathbb{D}_L^n \mid D \geq 0\}| < \infty$.

2. Sei $C \in \mathbb{D}_L$ mit $n = \deg(C) \geq g_L$. Die Abbildung $\tau: \mathcal{C}_L^0 \rightarrow \mathcal{C}_L^n$, definiert durch $\tau(\mathfrak{c}) = \mathfrak{c} + [C]$, ist bijektiv, und daher genügt es, die Endlichkeit von \mathcal{C}_L^n zu zeigen. Wir zeigen: In jeder Klasse $\mathfrak{c} \in \mathcal{C}_L^n$ gibt es einen Divisor A mit $A \geq 0$. Wegen $\deg(A) = \deg(\mathfrak{c}) = n$ gibt es nach 1. nur endlich viele solcher Divisoren. Sei $C \in \mathfrak{c}$. Nach Satz 4.3.1 ist $\dim(C) \geq \deg(C) + 1 - g_L \geq 1$, und nach Satz 4.1.2 gibt es ein $A \in \mathbb{D}_L$ mit $A \geq 0$ und $A \sim C$.

Sei nun $g = 0$. Wir müssen $\mathbb{D}_L^0 = (L^\times)$ zeigen. Ist $A \in \mathbb{D}_L^0$, so folgt $\dim(A) = \deg(A) + g - 1 = 1$ nach Satz 4.6.1 und $A \in (L^\times)$ nach Satz 4.2.1. \square

8.2

Definition und Satz 8.2.1. Für $\mathfrak{c} \in \mathcal{C}_L$ ist

$$|\{A \in \mathfrak{c} \mid A \geq 0\}| = \frac{q^{\dim(\mathfrak{c})} - 1}{q - 1}, \quad \text{und für alle } n > 2g - 2 \text{ mit } \partial | n \text{ ist } A_n = \frac{h(q^{n+1-g} - 1)}{q - 1}.$$

Die Potenzreihe

$$\mathcal{Z}_L(t) = \sum_{n \geq 0} A_n t^n \quad \text{konvergiert absolut für } |t| < q^{-1}.$$

Die Funktion \mathcal{Z}_L heißt *Zetafunktion* von L/\mathbb{F}_q .

BEWEIS. Sei $\mathfrak{c} \in \mathcal{C}$, $n = \dim(\mathfrak{c})$ und $C \in \mathfrak{c}$. Für $A \in \mathbb{D}_L$ gilt: Genau dann ist $A \in \mathfrak{c}$ und $A \geq 0$, wenn $A = C + (x)$ mit $x \in \mathcal{L}(C) \setminus \{0\}$. Nun ist $|\mathcal{L}(C) \setminus \{0\}| = q^n - 1$, und für $x, x' \in \mathcal{L}(C) \setminus \{0\}$ ist genau dann $(x) = (x')$, wenn $x' \in x\mathbb{F}_q^\times$. Daher folgt

$$|\{A \in \mathfrak{c} \mid A \geq 0\}| = \frac{q^n - 1}{q - 1}.$$

Sei nun $n > 2g - 2$. Für $\mathfrak{c} \in \mathcal{C}_L^n$ ist (nach Satz 4.6.1)

$$|\{A \in \mathfrak{c} \mid A \geq 0\}| = \frac{q^{\dim(\mathfrak{c})} - 1}{q - 1} = \frac{q^{n+1-g} - 1}{q - 1},$$

und wegen $|\mathcal{C}_L^n| = h$ folgt die Formel für A_n . Wegen $|A_n| \ll q^n$ konvergiert die Potenzreihe $\mathcal{Z}(t)$ absolut für alle $t \in \mathbb{C}$ mit $|t| < q^{-1}$. \square

Definition und Bemerkung 8.2.2. Für $r \in \mathbb{N}$ sei $\mu_r = \{\zeta \in \mathbb{C} \mid \zeta^r = 1\}$ die Gruppe der r -ten Einheitswurzeln. Ist $m \in \mathbb{N}$ und $d = \text{ggT}(r, m)$ so ist

$$(1 - t^{mr/d})^d = \prod_{\zeta \in \mu_r} (1 - (\zeta t)^m) \quad \text{für alle } t \in \mathbb{C}^\times.$$

[Beweis: Für $\zeta \in \mu_r$ ist

$$\text{ord}(\zeta^m) = \frac{\text{ord}(\zeta)}{\text{ggT}(\text{ord}(\zeta), m)}; \text{ daher ist die Abbildung } \theta: \begin{cases} \mu_r & \rightarrow \mu_{r/d} \\ \zeta & \mapsto \zeta^m \end{cases} \text{ surjektiv mit } \text{Ker}(\theta) = \mu_d.$$

Es folgt

$$(T^{r/d} - 1)^d = \prod_{\zeta \in \mu_{r/d}} (T - \zeta)^d = \prod_{\zeta \in \mu_r} (T - \zeta^m) \in \mathbb{C}[T].$$

Substituiert man $T = t^{-m}$ und multipliziert mit t^{mr} , so folgt die Behauptung.]

Satz 8.2.3. Für $t \in \mathbb{C}$ mit $|t| < q^{-1}$ und $r \in \mathbb{N}$ ist

$$\mathcal{Z}_L(t) = \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} \neq 0, \quad \text{und} \quad \mathcal{Z}_{L_r}(t^r) = \prod_{\zeta \in \mu_r} \mathcal{Z}_L(\zeta t).$$

BEWEIS. Für $t \in \mathbb{C}$ mit $|t| < q^{-1}$ ist

$$\sum_{P \in \mathbb{P}_L} |t|^{\deg(P)} \leq \sum_{\substack{D \in \mathbb{D}_L \\ D \geq 0}} |t|^{\deg(D)} = \sum_{n=0}^{\infty} A_n |t|^n < \infty,$$

und daher ist das unendliche Produkt absolut konvergent (also insbesondere non 0 verschieden). Sei nun $t \in \mathbb{C}$ mit $|t| < q^{-1}$, $\varepsilon \in \mathbb{R}_{>0}$ beliebig und $X \in \mathbb{N}$, so dass

$$\left| \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} - \prod_{\substack{P \in \mathbb{P}_L \\ \deg(P) < X}} \frac{1}{1 - t^{\deg(P)}} \right| < \frac{\varepsilon}{2} \quad \text{und} \quad \sum_{n=X}^{\infty} A_n |t|^n < \frac{\varepsilon}{2}.$$

Sei $\mathbb{D}_L(X)$ die Menge aller Divisoren $D \in \mathbb{D}_L$, so dass $D \geq 0$ und $v_P(D) = 0$ für alle $P \in \mathbb{P}_L$ mit $\deg(P) \geq X$. Ist $D \in \mathbb{D}_L$, $D \geq 0$ und $D \notin \mathbb{D}_L(X)$, so ist $\deg(D) \geq X$. Damit folgt

$$\prod_{\substack{P \in \mathbb{P}_L \\ \deg(P) < X}} \frac{1}{1 - t^{\deg(P)}} = \prod_{\substack{P \in \mathbb{P}_L \\ \deg(P) < X}} \sum_{n=0}^{\infty} t^{\deg(nP)} = \sum_{D \in \mathbb{D}_L(X)} t^{\deg(D)}$$

und

$$\begin{aligned} \left| \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} - \mathcal{Z}_L(t) \right| &\leq \left| \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} - \prod_{\substack{P \in \mathbb{P}_L \\ \deg(P) < X}} \frac{1}{1 - t^{\deg(P)}} \right| + \left| \sum_{D \in \mathbb{D}_L(X)} t^{\deg(D)} - \sum_{\substack{D \in \mathbb{D}_L \\ D \geq 0}} t^{\deg(D)} \right| \\ &\leq \frac{\varepsilon}{2} + \sum_{\substack{D \in \mathbb{D}_L, D \geq 0 \\ D \notin \mathbb{D}_L(X)}} |t|^{\deg(D)} \leq \frac{\varepsilon}{2} + \sum_{n=X}^{\infty} A_n |t|^n < \varepsilon. \end{aligned}$$

Sei nun $r \in \mathbb{N}$, $P \in \mathbb{P}_L$ mit $\deg(P) = m$ und $d = \text{ggT}(m, r)$. Nach Satz 8.1.2 ist dann d die Anzahl der $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$, und für jedes solche P' ist $\deg(P') = m/d$. Damit folgt für $t \in \mathbb{C}^\times$

$$\prod_{P' \supset P} (1 - t^{r \deg(P')}) = (1 - t^{rm/d})^d = \prod_{\zeta \in \mu_r} (1 - (\zeta t)^m),$$

und für $|t| < q^{-1}$ ist

$$\mathcal{Z}_{L_r}(t^r) = \prod_{P \in \mathbb{P}_L} \prod_{P' \supset P} \frac{1}{1 - t^{r \deg(P')}} = \prod_{P \in \mathbb{P}_L} \prod_{\zeta \in \mu_r} \frac{1}{1 - (\zeta t)^{\deg(P)}} = \prod_{\zeta \in \mu_r} \mathcal{Z}_L(\zeta t). \quad \square$$

8.3

Definition und Satz 8.3.1.

1. $\partial = 1$, und

$$\lim_{t \rightarrow 1} (1-t)\mathcal{Z}_L(t) = \frac{h}{1-q}.$$

2. Sei $t \in \mathbb{C}$ und $|t| < q^{-1}$.

(a) Im Falle $g = 0$ ist

$$\mathcal{Z}_L(t) = \frac{1}{(1-t)(1-qt)}.$$

(b) Im Falle $g \geq 1$ ist $\mathcal{Z}_L(t) = F(t) + G(t)$ mit

$$F(t) = \frac{1}{q-1} \sum_{n=0}^{2g-2} \left(\sum_{\substack{c \in \mathcal{C}_L \\ \deg(c)=n}} q^{\dim(c)} \right) t^n \quad \text{und} \quad G(t) = \frac{h}{q-1} \left[\frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t} \right].$$

3. $\mathcal{Z}_L(t)$ ist eine in $\mathbb{C} \setminus \{1, q^{-1}\}$ definierte rationale Funktion. $\mathcal{L}_L(t) = (1-t)(1-qt)\mathcal{Z}_L(t) \in \mathbb{Z}[t]$ und $\mathcal{L}_L(1) = h$. $\mathcal{L}_L = \mathcal{L}_{L/\mathbb{F}_q}$ heißt das \mathcal{L} -Polynom von L/\mathbb{F}_q .

BEWEIS. Wir geben zuerst vorläufige Formeln für $\mathcal{Z}_L(t)$, beweisen damit $\partial = 1$ und leiten erst dann die endgültigen Formeln her.

Im Falle $g = 0$ ist $h = 0$ nach Satz 8.1.4 und mit Satz 8.2.1 folgt

$$\mathcal{Z}_L(t) = \sum_{\substack{n=0 \\ \partial | n}} \frac{q^{n+1} - 1}{q-1} t^n = \frac{1}{q-1} \left[q \sum_{n=0}^{\infty} (qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n} \right] = \frac{1}{q-1} \left[\frac{q}{1-(qt)^\partial} - \frac{1}{1-t^\partial} \right].$$

Sei nun $g \geq 1$. Nach Satz 8.2.1 folgt

$$\begin{aligned} \mathcal{Z}_L(t) &= \sum_{\substack{n=0 \\ \partial | n}}^{2g-2} \sum_{\substack{c \in \mathcal{C}_L \\ \deg(c)=n}} \frac{q^{\dim(c)} - 1}{q-1} t^n + \sum_{\substack{n=2g-1 \\ \partial | n}}^{\infty} \frac{h(q^{n+1-g} - 1)}{q-1} t^n \\ &= \frac{1}{q-1} \sum_{n=0}^{2g-2} \left(\sum_{\substack{c \in \mathcal{C}_L \\ \deg(c)=n}} q^{\dim(c)} \right) t^n - \frac{h}{q-1} \sum_{\substack{n=0 \\ \partial | n}}^{2g-2} t^n + \frac{hq^{1-g}}{q-1} \sum_{\substack{n=2g-1 \\ \partial | n}}^{\infty} q^n t^n - \frac{h}{q-1} \sum_{\substack{n=2g-1 \\ \partial | n}}^{\infty} t^n \\ &= F(t) - \frac{h}{q-1} \sum_{n=0}^{\infty} t^{\partial n} + \frac{hq^{1-g+\partial k} t^{\partial k}}{q-1} \sum_{n=0}^{\infty} q^{n\partial} t^{n\partial} \quad \left(\text{mit } k = \left\lceil \frac{2g-1}{\partial} \right\rceil \right) \\ &= F(t) + \frac{h}{q-1} \left[\frac{q^{1-g+\partial k} t^{\partial k}}{1-(qt)^\partial} - \frac{1}{1-t^\partial} \right] = F(t) + G(t). \end{aligned}$$

In beiden Fällen ist

$$\lim_{t \rightarrow 1} (1-t)\mathcal{Z}_L(t) = \frac{h}{\partial(1-q)} \quad \text{und} \quad \mathcal{L}_L(1) = \lim_{t \rightarrow 1} (1-t)(1-qt)\mathcal{Z}_L(t) = \frac{h}{\partial}.$$

Wenn wir nun noch $\partial = 1$ zeigen können, folgen alle Behauptungen des Satzes.

Wegen $A_n =$ für alle $n \in \mathbb{N}_0$ mit $\partial \nmid n$ ist $\mathcal{Z}_L(\zeta t) = \mathcal{Z}_L(t)$ für alle $\zeta \in \mu_\partial$. Nach Satz 8.2.3 ist

$$\mathcal{Z}_{L_\partial}(t^\partial) = \prod_{\zeta \in \mu_\partial} \mathcal{Z}_L(\zeta t) = \mathcal{Z}_L(t)^\partial \quad \text{und} \quad 0 \neq \lim_{t \rightarrow 1} \frac{(1-t)^\partial \mathcal{Z}_L(t)^\partial}{(1-t^\partial) \mathcal{Z}_{L_\partial}(t^\partial)} = \lim_{t \rightarrow 1} \frac{(1-t)^\partial}{1-t^\partial},$$

und daraus folgt $\partial = 1$. □

Satz 8.3.2.

1. Es bestehen die Funktionalgleichungen

$$\mathcal{Z}_L(t) = q^{g-1}t^{2g-2}\mathcal{Z}_L\left(\frac{1}{qt}\right) \text{ f\"ur alle } t \in \mathbb{C}^\times \setminus \{1, q^{-1}\},$$

und

$$\mathcal{L}_L(t) = q^g t^{2g} \mathcal{L}_L\left(\frac{1}{qt}\right) \text{ f\"ur alle } t \in \mathbb{C}^\times.$$

2. $\text{gr}(\mathcal{L}_L) = 2g$. Ist $\mathcal{L}_L(t) = a_0 + a_1 t + \dots + a_{2g} t^{2g}$, so folgt $a_0 = 1$, $a_1 = |\mathbb{P}_L^1| - (q+1)$, $a_{2g} = q^g$, und $a_{2g-i} = q^{g-i} a_i$ f\"ur alle $i \in [0, g]$.
3. Es gibt ganz-algebraische Zahlen $\alpha_1, \dots, \alpha_{2g}$, so dass $\alpha_i \alpha_{g+i} = q$ f\"ur alle $i \in [1, g]$, und f\"ur alle $r \in \mathbb{N}$ ist

$$\mathcal{L}_{L_r}(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t), \quad q^r + 1 - |\mathbb{P}_{L_r}^1| = \sum_{i=1}^{2g} \alpha_i^r \quad \text{und} \quad q^g = \prod_{i=1}^{2g} \alpha_i.$$

Satz von Hasse -Weil (ohne Beweis):

$$\text{F\"ur alle } i \in [1, 2g] \text{ ist } |\alpha_i| = \sqrt{q}, \quad \text{und} \quad |q^r + 1 - |\mathbb{P}_{L_r}^1|| \leq 2gq^{r/2}.$$

BEWEIS. 1. Sei $\mathfrak{w} \in \mathcal{C}_L$ die kanonische Klasse. Dann ist $\text{deg}(\mathfrak{w}) = 2g - 2$, und die Zuordnung $\mathfrak{c} \mapsto \mathfrak{w} - \mathfrak{c}$ definiert eine Bijektion der Menge $\{\mathfrak{c} \in \mathcal{C}_L \mid \text{deg}(\mathfrak{c}) \in [0, 2g - 2]\}$ auf sich. Nach Satz 8.3.1 folgt

$$\begin{aligned} (q-1)F(t) &= \sum_{\substack{\mathfrak{c} \in \mathcal{C}_L \\ \text{deg}(\mathfrak{c}) \in [0, 2g-2]}} q^{\dim(\mathfrak{c})} t^{\text{deg}(\mathfrak{c})} = \sum_{\substack{\mathfrak{c} \in \mathcal{C}_L \\ \text{deg}(\mathfrak{c}) \in [0, 2g-2]}} q^{\text{deg}(\mathfrak{c})+1-g+\dim(\mathfrak{w}-\mathfrak{c})} t^{\text{deg}(\mathfrak{c})} \\ &= q^{g-1} t^{2g-2} \sum_{\substack{\mathfrak{c} \in \mathcal{C}_L \\ \text{deg}(\mathfrak{c}) \in [0, 2g-2]}} q^{\text{deg}(\mathfrak{c})-(2g-2)+\dim(\mathfrak{w}-\mathfrak{c})} t^{\text{deg}(\mathfrak{c})-(2g-2)} \\ &= q^{g-1} t^{2g-2} \sum_{\substack{\mathfrak{c} \in \mathcal{C}_L \\ \text{deg}(\mathfrak{c}) \in [0, 2g-2]}} q^{\dim(\mathfrak{w}-\mathfrak{c})} \left(\frac{1}{qt}\right)^{\text{deg}(\mathfrak{w}-\mathfrak{c})} = q^{g-1} t^{2g-2} (q-1)F\left(\frac{1}{qt}\right). \end{aligned}$$

Ferner ist

$$\begin{aligned} (q-1)q^{g-1}t^{2g-2}G\left(\frac{1}{qt}\right) &= hq^{g-1}t^{2g-2} \left[\frac{q^g \left(\frac{1}{qt}\right)^{2g-1}}{1 - q\left(\frac{1}{qt}\right)} - \frac{1}{1 - \frac{1}{qt}} \right] = hq^{g-1}t^{2g-2} \left[\frac{q^{-g+1}t^{-2g+1}t}{t-1} - \frac{qt}{qt-1} \right] \\ &= h \left[\frac{q^g t^{2g-1}}{1-qt} - \frac{1}{1-t} \right] = (q-1)G(t). \end{aligned}$$

Damit folgt

$$\mathcal{Z}_L(t) = F(t) + G(t) = q^{g-1}t^{2g-2} \left[F\left(\frac{1}{qt}\right) + G\left(\frac{1}{qt}\right) \right] = q^{g-1}t^{2g-2} \mathcal{Z}_L\left(\frac{1}{qt}\right)$$

und

$$\begin{aligned} q^g t^{2g} \mathcal{L}_L\left(\frac{1}{qt}\right) &= q^g t^{2g} \left(1 - \frac{1}{qt}\right) \left(1 - \frac{1}{t}\right) \mathcal{Z}_L\left(\frac{1}{qt}\right) = q^g t^{2g} \left(1 - \frac{1}{qt}\right) \left(1 - \frac{1}{t}\right) q^{1-g} t^{2-2g} \mathcal{Z}_L(t) \\ &= (1-qt)(1-t) \mathcal{Z}_L(t) = \mathcal{L}_L(t) \end{aligned}$$

2. Nach Definition ist $\text{gr}(\mathcal{L}_L) \leq 2g$, und aus

$$\mathcal{L}_L(t) = \sum_{i=0}^{2g} a_i t^i = (1-t)(1-qt) \sum_{n=0}^{\infty} A_n t^n = A_0 + [A_1 - (q+1)A_0]t + \sum_{i=2}^{2g} a_i t^i$$

und daher $a_0 = A_0 = 1$ und $a_1 = A_1 - (q+1)A_0 = |\mathbb{P}_L^1| - (q+1)$. Nach 1. ist

$$\mathcal{L}_L(t) = q^g t^{2g} \sum_{i=0}^{2g} a_i \left(\frac{1}{qt}\right)^i = \sum_{i=0}^{2g} a_i q^{g-i} t^{2g-i} = \sum_{i=0}^{2g} a_{2g-i} t^{2g-i}$$

und daher $a_{2g-i} = a_i q^{g-i}$ für alle $i \in [0, g]$. Insbesondere folgt $a_{2g} = q^g$ und daher $\text{gr}(\mathcal{Z}_L) = 2g$.

3. Es ist

$$\mathcal{L}_L^\perp(t) = t^{2g} \mathcal{L}_L\left(\frac{1}{t}\right) = \sum_{i=0}^{2g} a_i t^{2g-i} = t^{2g} + a_1 t^{2g-1} + \dots + q^g = \prod_{i=1}^{2g} (t - \alpha_i)$$

mit ganz-algebraischen Zahlen $\alpha_1, \dots, \alpha_{2g} \in \mathbb{C}$, so dass

$$-a_1 = q + 1 - |\mathbb{P}_L^1| = \sum_{i=1}^{2g} \alpha_i \quad \text{und} \quad q^g = \prod_{i=1}^{2g} \alpha_i.$$

Mit Hilfe der Funktionalgleichung folgt

$$\mathcal{L}_L(t) = t^{2g} \mathcal{L}_L^\perp\left(\frac{1}{t}\right) = \prod_{i=1}^{2g} (1 - \alpha_i t) = q^g \prod_{i=1}^{2g} \left(t - \frac{1}{\alpha_i}\right) = q^g t^{2g} \mathcal{L}_L\left(\frac{1}{qt}\right) = q^g \prod_{i=1}^{2g} \left(t - \frac{\alpha_i}{q}\right),$$

und daher gibt es eine Permutation $\sigma \in \mathfrak{S}_{2g}$, so dass $\alpha_i \alpha_{\sigma(i)} = q$ für alle $i \in [1, 2g]$, und nach geeigneter Ummummerierung ist

$$\mathcal{L}_L(t) = \prod_{i=1}^k (1 - \alpha_i t) \left(1 - \frac{q}{\alpha_i} t\right) (1 - \sqrt{q} t)^l (1 + \sqrt{q} t)^m$$

mit $k, l, m \in \mathbb{N}_0$, so dass $2k + l + m = 2g$. Der führende Koeffizient von \mathcal{L}_L ist $q^g = q^k (-1)^l \sqrt{q}^{l+m}$. Daher ist $l = 2l'$ und $m = 2m'$ mit $l', m' \in \mathbb{N}_0$. Mit $\alpha_i = \sqrt{q}$ für $i \in [k+1, k+l']$ und $\alpha_i = -\sqrt{q}$ für $i \in [k+l'+1, k+l'+m']$ folgt die Behauptung.

Sei nun $r \in \mathbb{N}$. Dann folgt

$$\begin{aligned} \mathcal{L}_{L_r}(t^r) &= (1 - t^r)(1 - q^r t^r) \mathcal{Z}_{L_r}(t^r) = \prod_{\zeta \in \mu_r} (1 - \zeta t)(1 - \zeta q t) \mathcal{Z}_L(\zeta t) = \prod_{\zeta \in \mu_r} \mathcal{L}_L(\zeta t) = \prod_{i=1}^{2g} \prod_{\zeta \in \mu_r} (1 - \alpha_i \zeta t) \\ &= \prod_{i=1}^{2g} (1 - \alpha_i^r t^r), \quad \text{also} \quad \mathcal{L}_{L_r}(t) = \prod_{i=1}^{2g} (1 - \alpha_i^r t) \quad \text{und daher} \quad |\mathbb{P}_{L_r}^1| = q^r + 1 - \sum_{i=1}^{2g} \alpha_i^r. \quad \square \end{aligned}$$