Algebraische Kurven

Franz Halter-Koch

Inhaltsverzeichnis

KAPITEL 0

Grundlagen aus Ring- und Körpertheorie

0.1. Elementares über Ringe

Wir setzen $\mathbb{N} = \{1, 2, \ldots\}$ und $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. Für Mengen A, B schreiben wir $A \subset B$ (und nicht $A \subseteq B$) für echte oder unechte Inklusion und $A \subsetneq B$ für echte Inklusion. Wir schreiben häufig $\mathbf{0}$ an Stelle von $\{0\}$ oder auch an Stelle von $(0, \ldots, 0)$ oder sogar $\{(0, \ldots, 0)\}$, wenn klar ist, welche Null gemeint ist. Für eine Menge X bezeichnen wir mit $X^\bullet$ die Menge der von Null verschiedenen Elemente von X.

Ein *Ring* R ist ein kommutativer Ring mit Eins $1_R = 1 \in R$. Ringhomomorphismen bilden die Eins auf die Eins ab, und Teilringe enthalten die Eins. Ein Element $z \in R$ heißt

- *Nullteiler*, wenn $zu = 0$ für ein $u \in R^\bullet$;
- *invertierbar* oder *Einheit*, wenn $zu = 1$ für ein $u \in R$.

$n(R)$ bezeichne die Menge der Nullteiler und $R^\times$ die Einheitengruppe (= Gruppe der invertierbaren Elemente) von R. Ein Ring R heißt *nullteilerfrei* oder *Bereich*, wenn $n(R) = \{0\}$ (dann ist $1 \neq 0$). Ein Bereich R besitzt einen (bis auf Isomorphie) eindeutig bestimmten Quotientenkörper $\mathfrak{q}(R)$. Ist L ein Körper und $R \subset L$ ein Teilring, so können wir stets auch $\mathfrak{q}(R) \subset L$ annehmen. Ein Ring R heißt *Nullring*, wenn $R = \{0\}$ [äquivalent: $0 = 1$, oder $n(R) = \emptyset$].

Ist $\mathfrak{a}$ ein Ideal von R, so schreiben wir $\mathfrak{a} \lhd R$ und bezeichnen mit $R/\mathfrak{a}$ den Restklassenring. Genau dann ist $\mathfrak{a} = R$, wenn $1 \in \mathfrak{a}$ [äquivalent: $\mathfrak{a} \cap R^\times \neq \emptyset$], und dann ist $R/\mathfrak{a} = \mathbf{0}$. Für eine Teilmenge $A \subset R$ bezeichnen wir mit $(A) = {}_R(A)$ das von A erzeugte Ideal von R. Für $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in R$ sei $(a_1, \ldots, a_n) = {}_R(a_1, \ldots, a_n) = a_1R + \ldots + a_nR = {}_R(\{a_1, \ldots, a_n\})$, und für $a \in R$ sei $(a) = {}_R(a) = aR$ das von a erzeugte Hauptideal. R heißt *Hauptidealring*, wenn jedes Ideal von R ein Hauptideal ist. Jeder Bereich mit euklidischem Algorithmus (also mit einer Division mit Rest) ist ein Hauptidealbereich. Wichtigste Beispiele: $\mathbb{Z}$ und der Polynomring $K[X]$ über einem Körper K.

Ist $R \subset S$ ein Teilring und $\mathfrak{a} \lhd R$, so bezeichne

$$\mathfrak{a}S = {}_S(\mathfrak{a}) = \{a_1s_1 + \ldots + a_ns_n \mid n \in \mathbb{N},\ a_1, \ldots, a_n \in \mathfrak{a},\ s_1, \ldots, s_n \in S\}$$

das von $\mathfrak{a}$ erzeugte Ideal von S.

Sei R ein Bereich, $K = \mathfrak{q}(R)$ und $a \in K^\times$. Dann nennt man $aR = \{ax \mid x \in R\} \subset K$ das von a erzeugte *gebrochene Hauptideal*. Sind a, $b \in K^\times$, so ist genau dann $aR = bR$, wenn $a^{-1}b \in R^\times$.

Ein Ideal $\mathfrak{a} \lhd R$ heißt *maximales Ideal* wenn $\mathfrak{a} \neq R$ und es kein Ideal $\mathfrak{b} \lhd R$ mit $\mathfrak{a} \subsetneq \mathfrak{b} \subsetneq R$ gibt [äquivalent: $R/\mathfrak{a}$ is ein Körper]. Ein Ideal $\mathfrak{a} \lhd R$ heißt *Primideal*, wenn $R/\mathfrak{a}$ ein Bereich ist [äquivalent: $R \setminus \mathfrak{a}$ ist eine nicht-leere multiplikativ abgeschlossene Menge].

Für einen Ring R bezeichnen wir Polynomringe (in über R algebraisch unabhängigen Unbestimmten) mit $R[X]$, $R[X, Y]$, $R[X_1, \ldots, X_n]$ usw. Ist $R \subset S$ ein Teilring, wo werden wir häufig

stillschweigend annehmen, dass $(X_1, \ldots, X_n)$ auch über S algebraisch unabhängig ist, und dann ist $R[X_1, \ldots, X_n] \subset S[X_1, \ldots, X_n]$ ein Teilring. Ist $f \in R[X_1, \ldots, X_n]$ und $p = (p_1, \ldots, p_n) \in R^n$, so setzen wir $f(p) = f(p_1, \ldots, p_n)$.

Sei R ein Bereich und $K = \mathfrak{q}(R)$. Dann ist $R[X_1, \ldots, X_n]$ ein Bereich, $R[X_1, \ldots, X_n]^\times = R^\times$, und $K(X_1, \ldots, X_n) = \mathfrak{q}(R[X_1, \ldots, X_n])$ ist ein rationaler Funktionenkörper über K. Genau dann ist $R[X_1, \ldots, X_n]$ ein Hauptidealbereich, wenn $n = 1$ und R ein Körper ist. Ist $\mathfrak{a} \lhd R$, so ist

$$\mathfrak{a}[X_1, \ldots, X_n] = \Big\{ \sum_{\nu_1, \ldots, \nu_n \geq 0} a_{\nu_1, \ldots, \nu_n} X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} \;\Big|\; a_{\nu_1, \ldots, \nu_n} \in \mathfrak{a}, \;\; \text{fast alle} = 0 \Big\}$$

das von $\mathfrak{a}$ erzeugte Ideal in $R[X_1, \ldots, X_n]$, und die Abbildung

$$\Phi \colon R[X_1, \ldots, X_n]/\mathfrak{a}[X_1, \ldots, X_n] \to R/\mathfrak{a}\,[X_1, \ldots, X_n],$$

definiert durch

$$\Phi\Big(\sum_{\nu_1, \ldots, \nu_n \geq 0} a_{\nu_1, \ldots, \nu_n} X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} + \mathfrak{a}[X_1, \ldots, X_n] \Big) = \sum_{\nu_1, \ldots, \nu_n \geq 0} (a_{\nu_1, \ldots, \nu_n} + \mathfrak{a}) X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n},$$

ist ein Ringisomorphismus. Wir identifizieren: $R[X_1, \ldots, X_n]/\mathfrak{a}[X_1, \ldots, X_n] = R/\mathfrak{a}\,[X_1, \ldots, X_n]$.

Für ein Polynom

$$f = \sum_{\nu_1, \ldots, \nu_n \geq 0} a_{\nu_1, \ldots, \nu_n} X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} \in R[X_1, \ldots, X_n] \quad \text{mit} \;\; a_{\nu_1, \ldots, \nu_n} \in R, \;\; \text{fast alle} \;\; = 0$$

und $(i_1, \ldots, i_n) \in \mathbb{N}_0^n$ definieren wir die modifizierte partielle Ableitung $f_{i_1, \ldots, i_n} \in R[X_1, \ldots, X_n]$ durch

$$\begin{aligned} f_{i_1, \ldots, i_n} &= \sum_{\nu_1, \ldots, \nu_n \geq 0} a_{\nu_1, \ldots, \nu_n} \binom{\nu_1}{i_1} \cdots \binom{\nu_n}{i_n} X_1^{\nu_1 - i_1} \cdot \ldots \cdot X_n^{\nu_n - i_n} \\ &= \sum_{\nu_1 \geq i_1} \cdots \sum_{\nu_n \geq i_n} a_{\nu_1, \ldots, \nu_n} \binom{\nu_1}{i_1} \cdots \binom{\nu_n}{i_n} X_1^{\nu_1 - i_1} \cdot \ldots \cdot X_n^{\nu_n - i_n}. \end{aligned}$$

Der Zusammenhang mit den üblichen höheren partiellen Ableitungen ist gegeben durch

$$\frac{\partial^{i_1 + \ldots + i_n} f}{\partial X_1^{i_1} \ldots \partial X_n^{i_n}} = i_1! \cdot \ldots \cdot i_n! f_{i_1, \ldots, i_n}.$$

Satz und Definition 0.1.1 (Taylor'scher Satz und Ordnung)**.**

1. *Sei $f \in R[X_1, \ldots, X_n]$ und $p = (p_1, \ldots, p_n) \in R^n$. Dann ist*

$$f = \sum_{i_1, \ldots, i_n \geq 0} f_{i_1, \ldots, i_n}(p) (X_1 - p_1)^{i_1} \cdot \ldots \cdot (X_n - p_n)^{i_n},$$

   und man nennt $\operatorname{ord}_p(f) = \inf\{i_1 + \ldots + i_n \mid i_1, \ldots, i_n \geq 0, \; f_{i_1, \ldots, i_n}(p) \neq 0\}$ *die Ordnung von f in p.*

2. *Seien f, $g \in R[X_1, \ldots, X_n]$ und $p \in R^n$.*
   (a) *Genau dann ist $f(p) = 0$, wenn $\operatorname{ord}_p(f) > 0$.*
   (b) $\operatorname{ord}_p(fg) = \operatorname{ord}_p(f) + \operatorname{ord}_p(g)$
   (c) $\operatorname{ord}_p(f + g) \geq \min\{\operatorname{ord}_p(f), \operatorname{ord}_p(g)\}$, *mit Gleichheit, falls* $\operatorname{ord}_p(f) \neq \operatorname{ord}_p(g)$.

BEWEIS. 1. Sei

$$f = \sum_{\nu_1,\dots,\nu_n \geq 0} a_{\nu_1,\dots,\nu_n} X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} \in R[X_1,\dots,X_n] \quad \text{mit} \quad a_{\nu_1,\dots,\nu_n} \in R, \quad \text{fast alle} \quad = 0.$$

Dann folgt

$$\begin{aligned} f &= f\big(p_1 + (X_1 - p_1), \dots, p_n + (X_n - p_n)\big) \\ &= \sum_{\nu_1,\dots,\nu_n \geq 0} a_{\nu_1,\dots,\nu_n} [p_1 + (X_1 - p_1)]^{\nu_1} \cdot \ldots \cdot [p_n + (X_n - p_n]^{\nu_n} \\ &= \sum_{\nu_1,\dots,\nu_n \geq 0} a_{\nu_1,\dots,\nu_n} \sum_{i_1=0}^{\nu_1} \dots \sum_{i_n=0}^{\nu_n} \binom{\nu_1}{i_1} \dots \binom{\nu_n}{i_n} p_1^{\nu_1 - i_1} \cdot \ldots \cdot p_n^{\nu_n - i_n} (X_1 - p_1)^{i_1} \cdot \ldots \cdot (X_n - p_n)^{i_n} \\ &= \sum_{i_1,\dots,i_n \geq 0} \Big[\sum_{\nu_1 \geq i_1} \dots \sum_{\nu_n \geq i_n} a_{\nu_1,\dots,\nu_n} \binom{\nu_1}{i_1} \dots \binom{\nu_n}{i_n} p_1^{\nu_1 - i_1} \cdot \ldots \cdot p_n^{\nu_n - i_n} \Big] (X_1 - p_1)^{i_1} \cdot \ldots \cdot (X_n - p_n)^{i_n} \\ &= \sum_{i_1,\dots,i_n \geq 0} f_{i_1,\dots,i_n}(p) (X_1 - p_1)^{i_1} \cdot \ldots \cdot (X_n - p_n)^{i_n}. \end{aligned}$$

2. Offensichtlich. □

Für ein Polynom $f \in R[X]$ bezeichnen wir mit $\operatorname{gr}(f) \in \mathbb{N}_0 \cup \{-\infty\}$ den Grad von f und mit f', f'', $\dots$, $f^{(n)} \in R[X]$ die (gewöhnlichen) Ableitungen von f. Für $p \in R$ ist dann

$$\operatorname{ord}_p(f) = \inf\{n \in \mathbb{N}_0 \mid f^{(n)}(p) \neq 0\}.$$

Ein Polynom $f \in R[X_1,\dots,X_n]$ heißt *irreduzibel (über R)*, wenn $f \notin R$, und es gibt keine Faktorisierung $f = gh$ mit g, $h \in R[X_1,\dots,X_n] \setminus R$. Ist $R \subset S$ ein Teilring, so braucht ein über R irreduzibles Polynom über S nicht irreduzibel zu sein, aber jedes über S irreduzible Polynom $f \in R[X_1,\dots,X_n]$ ist auch über R irreduzibel.

Man sagt, ein Polynom $f \in R[X] \setminus R$ *zerfällt in Linearfaktoren* über R, wenn es ein $n \in \mathbb{N}$, $c \in R^\bullet$ und $\alpha_1,\dots,\alpha_n \in R$ gibt, so dass $f = c(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$.

0.2. Faktorielle Bereiche

Sei R ein Bereich. Sind a, $b \in R$, so heißt a ein *Teiler* von b, $a \mid b$, wenn $b = ac$ für ein $c \in R$ [äquivalent: $b \in aR$, oder $bR \subset aR$]. a und b heißen *assoziiert*, $a \simeq b$, wenn $aR = bR$ [äquivalent: $a \mid b$ und $b \mid a$, oder $b = au$ mit $u \in R^\times$].

Seien $n \in \mathbb{N}$ und $a_1,\dots,a_n \in R$. Ein Element $d \in R$ heißt *größter gemeinsamer Teiler* (ggT) von $a_1,\dots,a_n$, wenn gilt: **1)** $d \mid a_i$ für alle $i \in [1,n]$; **2)** Ist $g \in R$ und $g \mid a_i$ für alle $i \in [1,n]$, so folgt $g \mid d$. Genau dann ist d ein ggT von $a_1,\dots,a_n$, wenn (d) das kleinste $\{a_1,\dots,a_n\}$ umfassende Hauptideal ist. Insbesondere ist dadurch d bis auf Assoziierte eindeutig bestimmt. Ist R ein Hauptidealbereich, so ist d genau dann ein ggT von $a_1,\dots,a_n$, wenn $(d) = (a_1,\dots,a_n)$. Die Elemente $a_1,\dots,a_n$ heißen *teilerfremd*, $(a_1,\dots,a_n) = 1$, wenn 1 ein ggT von $a_1,\dots,a_n$ ist [äquivalent: Ist $c \in R$ and $c \mid a_i$ für alle $i \in [1,n]$, so ist $c \in R^\times$]. Ist R ein Hauptidealbereich, so ist genau dann $(a_1,\dots,a_n) = 1$, wenn es $x_1,\dots,x_n \in R$ gibt mit $a_1x_1 + \ldots + a_nx_n = 1$.

Ein Element $p \in R^\bullet$ heißt *Primelement*, wenn das Hauptideal $(p) = pR$ ein Primideal ist [äquivalent: Aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$ für alle a, $b \in R$].

Eindeutigkeit der Primzerlegung: Sind m, $n \in \mathbb{N}$ und $p_1, \ldots, p_n$, $q_1, \ldots, q_m$ Primelemente mit $p_1 \cdot \ldots \cdot p_n \simeq q_1 \cdot \ldots \cdot q_m$, so ist $n = m$, und es gibt eine Permutation $\sigma \in \mathfrak{S}_n$ so dass $p_i \simeq q_{\sigma(i)}$ für alle $i \in [1, n]$.

Ein Bereich R heißt *faktoriell*, wenn jedes $a \in R^\bullet \setminus R^\times$ ein Produkt von Primelementen ist. Ist R ein Hauptidealbereich, so ist R faktoriell, und jedes von $\mathbf{0}$ verschiedene Primideal ist maximal.

Satz 0.2.1 (Arithmetik in einem faktoriellen Bereich)**.** *Sei R ein faktorieller Bereich und $K = \mathsf{q}(R)$.*

1. *Je endlich viele Elemente von R besitzen einen* ggT.
2. *Sind a, b, $c \in R$, $a \,|\, bc$ und $(a, b) = 1$, so folgt $a \,|\, c$.*
3. *Jedes $x \in K$ hat eine Darstellung $x = a^{-1}b$ mit $a \in R^\bullet$, $b \in R$ und $(a, b) = 1$. Dabei sind a und b bis auf Assoziierte eindeutig bestimmt.*

Sei R ein faktorieller Bereich. Ein Polynom

$$f = \sum_{\nu_1, \ldots, \nu_n \geq 0} a_{\nu_1, \ldots, \nu_n} X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} \in R[X_1, \ldots, X_n]$$

heißt *primitiv*, wenn die Koeffizienten $\{a_{\nu_1, \ldots, \nu_n} \mid \nu_1, \ldots, \nu_n \geq 0\}$ teilerfremd sind. Zu jedem Polynum $f \in K[X_1, \ldots, X_n]^\bullet$ gibt es ein $c \in K^\times$, so dass $c^{-1}f$ ein primitives Polynom in $R[X_1, \ldots, X_n]$ ist. Jedes solche $c \in K^\times$ heißt *Inhalt* von f. Sind c, $c_1 \in K^\times$ Inhalte von f, so gibt es ein $u \in R^\times$ mit $c_1 = cu$. Ist $f \in K[X_1, \ldots, X_n]^\bullet$ und $c \in K^\times$ ein Inhalt von f, so gilt:

- Genau dann ist $f \in R[X_1, \ldots, X_n]$, wenn $c \in R$.
- Genau dann ist $f \in R[X_1, \ldots, X_n]$ primitiv, wenn $c \in R^\times$.
- Ist ein Koeffizient von f in $R^\times$, so ist $c^{-1} \in R$.

Satz 0.2.2 (Gauß'sches Lemma)**.** *Sei R ein faktorieller Bereich und $K = \mathsf{q}(R)$.*

1. *Seien f, $g \in K[X_1, \ldots, X_n]^\bullet$, $c \in K^\times$ ein Inhalt von f und $d \in K^\times$ ein Inhalt von g. Dann ist cd ein Inhalt von fg.*
2. *Ist $f \in R[X_1, \ldots, X_n]$ irreduzibel über R, so ist f auch irreduzibel über K.*
3. *Ein Polynom $p \in R[X_1, \ldots, X_n]$ ist genau dann ein Primelement von $R[X_1, \ldots, X_n]$, wenn*
   - *entweder $p \in R$ ist ein Primelement von R,*
   - *oder $p \in R[X_1, \ldots, X_n] \setminus R$ ist irreduzibel und primitiv.*
4. *$R[X_1, \ldots, X_n]$ ist faktoriell.*

Jeder Hauptidealbereich (und insbesondere jeder Körper) ist faktoriell. Ist K ein Körper, so ist $K[X]$ faktoriell, und ein Polynom $f \in K[X] \setminus K$ ist genau dann ein Primelement, wenn f irreduzibel ist. Dann ist $(f) \lhd K[X]$ ein maximales Ideal und $K[X]/(f)$ ein Körper.

Sei K ein Körper und $f \in K[X_1, \ldots, X_n]$. f heißt *reduziert* (über K), wenn $f = f_1 \cdot \ldots \cdot f_r$ mit $r \in \mathbb{N}$ und paarweise nicht-assoziierten irreduziblen Polynomen $f_1, \ldots, f_r \in K[X_1, \ldots, X_n]$ [äquivalent: $q^2 \nmid f$ für jedes (irreduzible) Polynom $q \in K[X_1, \ldots, X_n]$].

Lemma 0.2.3. *Sei R ein faktorieller Bereich, und seien f, $g \in R[X]$ Polynome ohne gemeinsamen Teiler in $R[X] \setminus R$. Dann gibt es Polynome p, $q \in R[X]$ mit $pf + qg \in R^\bullet$.*

BEWEIS. Wir zeigen zuerst, dass f und g in $K[X]$ teilerfremd sind. Wir nehmen im Gegenteil an, es gebe ein Polynom $h \in K[X]\backslash K$ mit $h \mid f$ und $h \mid g$. Sei $c \in K^\times$, so dass $h_0 = c^{-1}h \in R[X]\backslash R$ primitiv ist. Dann ist $f = h_0 f_1$ und $g = h_0 g_1$ mit Polynomen f_1, $g_1 \in K[X]$. Wegen $\mathfrak{I}(h_0) = R$ folgt $\mathfrak{I}(f_1) = \mathfrak{I}(f_1)\mathfrak{I}(h_0) = \mathfrak{I}(f) \subset R$, also $f_1 \in R[X]$, und in gleicher Weise $g_1 \in R[X]$. Daher ist h_0 ein gemeinsamer Faktor von f und g in $R[X]$, ein Widerspruch!

Da $K[X]$ ein Hauptidealbereich ist, gibt es Polynome p_1, $q_1 \in K[X]$, so dass $p_1 f + q_1 g = 1$. Sei $r \in R^\bullet$, so dass $p = rp_1$, $q = rq_1 \in R[X]$. Dann folgt $pf + qg = r$. □

0.3. Algebren

Sei K ein Körper. Eine *K-Algebra* ist ein Ring A mit einer K-Vektorraumstruktur

$$K \times A \to A, \quad (\lambda, x) \mapsto \lambda x,$$

so dass $\lambda(ab) = (\lambda a)b = a(\lambda b)$ für alle a, $b \in A$ und $\lambda \in K$. Man nennt $[A : K] = \dim_K(A)$ den *Grad* von A über K. Jeder Oberring von K und insbesondere jeder Polynomring $K[\boldsymbol{X}]$ ist eine K-Algebra. Ist A eine K-Algebra und $\mathfrak{a} \lhd A$, so ist auch $A/\mathfrak{a}$ eine K-Algebra. Ist A eine K-Algebra und X eine nicht-leere Menge, so ist $\mathrm{Abb}(X, A)$ eine K-Algebra bezüglich der wertweisen Verknüpfung von Abbildungen.

Ein *K-Algebrenhomomorphismus* ist ein Ringhomomorphismus, der auch ein Vektorraumhomomorphismus ist. Die Abbildung $\varepsilon_A \colon K \to A$, definiert durch $\varepsilon_A(\lambda) = \lambda 1_A$ für alle $\lambda \in K$, ist ein K-Algebrenhomomorphismus. Ist $A \neq \mathbf{0}$, so ist ε_A ein Monomorphismus, und wir werden häufig K mit $K1_A$ identifizieren und $K \subset A$ annehmen.

Sei A eine K-Algebra, $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$. Für ein Polynom

$$f = \sum_{\nu_1,\ldots,\nu_n \geq 0} \lambda_{\nu_1,\ldots,\nu_n} X_1^{\nu_1} \cdot \ldots \cdot X_n^{\nu_n} \in K[X_1, \ldots, X_n] \text{ sei } f(a_1, \ldots, a_n) = \sum_{\nu_1,\ldots,\nu_n \geq 0} \lambda_{\nu_1,\ldots,\nu_n} a_1^{\nu_1} \cdot \ldots \cdot a_n^{\nu_n},$$

und wir nennen

$$f^A \colon A^n \to A, \quad \text{definiert durch} \quad f^A(a_1, \ldots, a_n) = f(a_1, \ldots, a_n)$$

die durch f definierte polynomiale Abbildung auf A. Die Abbildung

$$K[X_1, \ldots, X_n] \to \mathrm{Abb}(A^n, A), \quad \text{definiert durch} \quad f \mapsto f^A,$$

ist ein K-Algebrenhomomorphismus. Für $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ ist

$$K[a_1, \ldots, a_n] = \{ f(a_1, \ldots, a_n) \mid f \in K[X_1, \ldots, X_n] \}$$

die kleinste K-Unteralgebra von A, die $a_1, \ldots, a_n$ enthält, und die Abbildung

$$\iota_{a_1,\ldots,a_n} \colon K[X_1, \ldots, X_n] \to A, \quad \text{definiert durch} \quad \iota_{a_1,\ldots,a_n}(f) = f(a_1, \ldots, a_n)$$

ist ein K-Algebrenhomomorphismus. Genauer gilt: $\iota_{(a_1,\ldots,a_n)}$ ist der eindeutig bestimmte K-Algebrenhomomorphismus $\varphi \colon K[X_1, \ldots, X_n] \to A$ mit $\varphi(X_i) = a_i$ für alle $i \in [1, n]$.

Eine K-Algebra A heißt *affin*, wenn $A = K[a_1, \ldots, a_n]$ mir $n \in \mathbb{N}$ und $a_1, \ldots, a_n \in A$ [äquivalent: Es gibt ein $n \in \mathbb{N}$ und einen K-Algebrenepimorphimus $K[X_1, \ldots, X_n] \to A$].

Ist M eine nicht-leere Menge, $n \in \mathbb{N}$, $f \in K[X_1, \ldots, X_n]$ und $(\varphi_1, \ldots, \varphi_n) \in \mathrm{Abb}(M, A)^n$, so ist auch $f(\varphi_1, \ldots, \varphi_n) \in \mathrm{Abb}(M, A)$, und $f(\varphi_1, \ldots, \varphi_n)(x) = f(\varphi_1(x), \ldots, \varphi_n(x)) \in A$ für alle $x \in M$.

0.4. Elementare Körpertheorie

Ist $\varphi\colon K \to K_1$ ein (Körper-)Homomorphismus, so ist φ injektiv und induziert einen Isomorphismus $\varphi\colon K \xrightarrow{\sim} \varphi(K)$. 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. Insbesondere ist L ein K-Algebra. Eine Körpererweiterung L/K heißt *endlich*, wenn $[L\colon K] = \dim_K(L) < \infty$. Für eine Teilmenge $S \subset L$ bezeichen $K[S]$ den kleinsten Teilring von L, der $K \cup S$ umfasst. Dann ist $K(S) = \mathsf{q}(K[S])$ der kleinste Teilkörper von L, der $K \cup S$ umfasst.

Seien L/K und L'/K Körpererweiterungen. Unter einem *K-Homomorphismus* $\varphi\colon L \to L'$ versteht man einen K-Algebrenhomomorphismus. Ein Körperhomomorphismus $\varphi\colon L \to L'$ ist genau dann ein K-Homomorphismus, von $\varphi \,|\, K = \mathrm{id}_K\,]$. Wir bezeichnen mit $\mathrm{Hom}_K(L, L')$ die Menge aller K-Homomorphismen $\varphi\colon L \to L'$, und mit $\mathsf{Gal}(L/K)$ die Menge aller K-Isomorphismen $\varphi\colon L \to L$. $\mathsf{Gal}(L/K)$ ist eine Gruppe und heißt *Galoisgruppe* von L/K. Ist $\varphi\colon L \to L'$ ein K-Isomorphismus, so ist $\varphi^*\colon \mathsf{Gal}(L'/K) \to \mathsf{Gal}(L/K)$, definiert durch $\varphi^*(\sigma) = \varphi^{-1} \circ \sigma \circ \varphi$, ein Gruppenisomorphismus.

Sei L/K eine Körpererweiterung, $\alpha \in L$ und $\phi_\alpha\colon K[X] \to K[\alpha] \subset L$ der eindeutig bestimmte K-Algebrenhomomorphismus mit $\phi_\alpha(X) = \alpha$. Das Element α heißt *algebraisch* über K, wenn $\mathrm{Ker}(\phi_\alpha) \neq \mathbf{0}$. In diesem Falle gibt es genau ein normiertes irreduzibles Polynom $f \in K[X]$ mit $\mathrm{Ker}(\phi_\alpha) = (f)$ [äquivalent: $f \in K[X]$ ist normiert, irreduzibel, und $f(\alpha) = 0$]. Dieses Polynom f heißt *Minimalpolynom* von α über K. Der Homomorphismus ϕ_α induziert einen Isomorphismus $\phi_\alpha^*\colon K[X]/(f) \xrightarrow{\sim} K[\alpha]$ vermöge $\phi(h + (f)) = h(\alpha)$ für alle $h \in K[X]$. Das Ideal $(f) \lhd K[X]$ ein maximales Ideal, also $K[X]/(f)$ und daher auch $K[\alpha]$ ein Körper, und es folgt $K[\alpha] = K(\alpha)$.

Ist α nicht algebraisch über K, so heißt α *transzendent über K*. In diesem Falle ist ϕ_α ein Isomorphismus und induziert einen K-Isomorphismus $\overline{\phi}_\alpha\colon K(X) \xrightarrow{\sim} K(\alpha)$ mit $\overline{\phi}_\alpha(X) = \alpha$.

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 M ein Zwischenkörper von L/K, so ist L/K genau dann algebraisch, wenn L/M und M/K beide algebraisch sind.

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

Sei K ein Körper, $f \in K[X] \setminus K$ und $L \supset K$ ein Oberkörper. L heißt *Zerfällungskörper* von f über K, wenn $f = c(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_n)$ mit $c \in K^\times$, $n \in \mathbb{N}$ und $\alpha_1, \ldots, \alpha_n \in L$, so dass $L = K(\alpha_1, \ldots, \alpha_n)$. Ist f irreduzibel über K, so heißt L ein *Stammkörper* von f über K, wenn es ein $\alpha \in L$ gibt mit $L = K(\alpha)$ und $f(\alpha) = 0$.

Satz 0.4.1 (Existenz und Eindeutigkeit von Stamm- und Zerfällungskörper)**.** *Sei K ein Körper. Jedes $f \in K[X] \setminus K$ besitzt einen bis auf K-Isomorphie eindeutig bestimmten Zerfällungskörper über K, und jedes über K irreduzible $f \in K[X] \setminus K$ besitzt einen bis auf K-Isomorphie eindeutig bestimmten Stammkörper über K.*

Sei L/K eine Körperweiterung. Die Menge $\overline{K}_L$ aller über K algebraischen Element von L ist ein Zwischenkörper von L/K und heißt *relativer algebraischer Abschluss von K in L*. K heißt *relativ algebraisch abgeschlossen in L*, wenn $\overline{K}_L = K$.

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 $K \subsetneq L$]. 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 0.4.2 (Hauptsatz über algebraische Hüllen)**.** *Sei K ein Körper.*

1. *K besitzt eine algebraische Hülle.*
2. *Ist L 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 $\varphi\colon K \to K_1$ ein Körperhomomorphismus, L/K eine algebraische Körpererweiterung und K_1^* ein algebraisch abgeschlossener Oberkörper von K. Dann gibt es einen Homomorphismus $\phi\colon L \to K_1^*$ mit $\phi \mid K = \varphi$.*
4. *Je zwei algebraischen Hüllen K_1 und K_2 von K sind K-isomorph.*

Sei K ein Körper und $\overline{K}$ eine algebraische Hülle von K. Dann ist $G_K = \mathsf{Gal}(\overline{K}/K)$ bis auf Isomorphie eindeutig durch K bestimmt und heißt *absolute Galoisgruppe* von K.

Lemma 0.4.3. *Sei K ein Körper und $\overline{K}$ eine algebraische Hülle von K. Dann ist*

$$G_K = \mathrm{Hom}_K(\overline{K}, \overline{K}), \quad \textit{und} \quad K = \{x \in \overline{K} \mid \sigma(x) = x \textit{ für alle } \sigma \in G_K\}.$$

Beweis. Offensichtlich ist $G_K \subset \mathrm{Hom}_K(\overline{K}, \overline{K})$. Ist nun $\sigma \in \mathrm{Hom}_K(\overline{K}, \overline{K})$, so 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 $\overline{K}$. Dann ist N endlich und $z \in N$. Für alle $y \in N$ ist $0 = \sigma(f(y)) = f(\sigma(y))$, also auch $\sigma(y) \in N$. Daher ist $\sigma(N) \subset N$, und da $\sigma \mid N\colon N \to N$ ist injektiv ist, folgt $N = \sigma(N)$, und es gibt ein $x \in N$ mit $\sigma(x) = z$.

Ist $x \in K$, so is definitionsgemäß $\sigma(x) = x$ 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 $\sigma_0 \in \mathrm{Hom}_K(K(x), \overline{K})$ mit $\sigma_0(x) = x'$. Dann gibt es ein $\sigma \in G_K$ mit $\sigma \mid K(x) = \sigma_0$, und es ist $\sigma(x) = x' \neq x$. □

$\mathbb{C}$ ist algebraisch abgeschlossen ("Fundamentalsatz der Algebra"). 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 $\mathbb{Q}$.

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

Satz 0.4.4. *Seien $K \subset L$ Körper, sei K relativ algebraisch abgeschlossen in L, und sei $\overline{L}$ eine algebraische Hülle von L.*

1. *Ist $f \in K[X] \setminus K$ irreduzibel, so ist f auch irreduzibel über L.*
2. *Ist $\alpha \in \overline{L}$ algebraisch über K, so ist $[L(\alpha)\colon L] = [K(\alpha)\colon K]$.*

Beweis. 1. Sei $f = c(X - \alpha_1) \cdot \ldots \cdot (x - \alpha_n)$ mit $n \in \mathbb{N}$, $c \in K^\times$ und $\alpha_1, \ldots, \alpha_n \in \overline{L}$, und sei f reduzibel über L. Dann it $f = gh$ mit $g, h \in L[X]$, und wir können annehmen, dass $g = c(X - \alpha_1) \cdot \ldots \cdot (X - \alpha_k)$ und $h = (X - \alpha_{k+1}) \cdot \ldots \cdot (X - \alpha_n)$ mit $k \in [1, n-1]$. Dann liegen

die Koeffizienten von g und von h in $K(\alpha_1,\dots,\alpha_n)\cap L$, sind also algebraisch über K und liegen daher in K, ein Widerspruch.

2. Sei $f\in K[X]$ das Minimalpolynom von α über K. Nach 1. ist f irreduzibel über L, also auch das Minimalpolynom von α über L, und es folgt $[K(\alpha):K]=\mathrm{gr}(f)=[L(\alpha):L]$. □

Primkörper. Sei K ein Körper. Der kleinste Teilkörper K_0 von K heißt *Primkörper* von K. Es ist entweder $K_0\cong\mathbb{Q}$ oder $K_0\cong\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ für eine Primzahl p (wir identifizieren). Man definiert die *Charakteristik* $\mathrm{char}(K)$ von K durch

$$\mathrm{char}(K)=\begin{cases}0, & \text{falls} \quad K_0\cong\mathbb{Q},\\ p & \text{falls} \quad K_0\cong\mathbb{F}_p.\end{cases}$$

Endliche Körper. Jeder endliche Bereich ist ein Körper. 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. Für $p\in\mathbb{P}$ ist $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$.

Sei $p\in\mathbb{P}$ und $e=fg$ mit $e,\ f\in\mathbb{N}$. Dann ist $F=\{x\in\mathbb{F}_{p^e}\colon x^{p^f}=x\}$ ein Teilkörper von $\mathbb{F}_{p^e}$ mit $|F|=p^f$, und wir identifizieren $F=\mathbb{F}_{p^f}$. Dann ist $\mathbb{F}_p\subset\mathbb{F}_{p^f}\subset\mathbb{F}_{p^e}$, $[\mathbb{F}_{p^e}:\mathbb{F}_{p^f}]=g$, $\mathbb{F}_{p^e}$ ist Zerfällungskörper von $X^{p^e}-X$ über $\mathbb{F}_p$, und $[\mathbb{F}_{p^e}:\mathbb{F}_p]=e$.

Sei F ein endlicher Köroper und $\overline{F}$ eine algebraische Hülle von F. Dann gibt es zu jedem $d\in\mathbb{N}$ genau einen Zwischenkörper E von $\overline{F}/F$ mit $[E:F]=d$, nämlich $E=\mathbb{F}_{q^d}$. Bezeichnet $\mathcal{K}$ die Menge aller Zwischenkörper $\mathbb{F}_q\subset E\subsetneq\overline{F}_q$, so definiert die Zuordnung $E\mapsto[E:\mathbb{F}_q]$ einen Verbandsisomorphismus $(\mathcal{K},\subset)\xrightarrow{\sim}(\mathbb{N},|)$. Für alle Körper E, E_1, $E_2\in\mathcal{K}$ gilt:

$$E_1\subset E_2 \iff [E_1:F]\,|\,[E_2:F],\qquad E=E_1E_2 \iff [E:F]=\mathrm{kgV}([E_1:F],[E_2:F])$$

und

$$[E_1\cap E_2:F]=\mathrm{ggT}([E_1:F],[E_2:F]).$$

$\overline{F}$ ist unendlich, und daher ist jeder algebraisch abgeschlossene Körper unendlich.

Separabilität. Sei K ein Körper.

Sei $f\in K[X]$, und $L\supset K$ ein Oberkörper. Ein Element $\alpha\in L$ heißt *mehrfache Nullstelle* von f, wenn es ein Polynom $g\in L[X]$ gibt mit $f=(X-\alpha)^2g$ [äquivalent: $f(\alpha)=f'(\alpha)=0$]. Ein Polynom $f\in K[X]$ heißt *separabel*, wenn es in keinem Oberkörper von K mehrfache Nullstellen besitzt [äquivalent: $(f,f')=1$]. 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 $\mathrm{char}(K)=0$ oder $\mathrm{char}(K)=p>0$ und $K=K^p$. 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 von f über K 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 M ein Zwischenkörper von L/K, so ist L/K genau dann separabel, wenn L/M und M/K beide separabel sind. Ist K vollkommen, so ist jede algebraische Körpererweiterung L/K separabel.

Satz und Definition 0.4.5. *Sei L/K eine endliche separable Körpererweiterung.*

1. (Satz vom primitiven Element) *Es gibt ein $\alpha\in L$ mit $L=K(\alpha)$.*

2. *Sei* $[L:K] = n$ *und* $\overline{L}$ *eine algebraische Hülle von* L*. Dann ist* $|\mathrm{Hom}_K(L,\overline{L})| = n$*. Explizit: Sei* $L = K(\alpha)$*,* $f \in K[X]$ *das Minimalpolynom von* α *über* K*, und seien* $\alpha = \alpha_1, \ldots, \alpha_n \in \overline{L}$ *die Nullstellen von* f*. Für* $i \in [1,n]$ *sei* $\varphi_i \colon L \to \overline{L}$ *der eindeutig bestimmte* K*-Homomorphismus mit* $\varphi_i(\alpha) = \alpha_i$*. Dann ist* $\mathrm{Hom}_K(L,\overline{L}) = \{\varphi_1, \ldots, \varphi_n\}$*. Der Körper* $L^* = K(\alpha_1, \ldots, \alpha_n)$ *ist ein Zerfällungskörper von* f*, er ist durch die Körpererweiterung* L/K *bis auf* L*-Isomorphie eindeutig bestimmt, und es gibt* $\varphi_1^*, \ldots, \varphi_n^* \in \mathsf{Gal}(L^*/L)$ *mit* $\varphi_i^* \mid L = \varphi_i$*.*

   L^* heißt *galoissche Hülle* von L/K*.*

Satz 0.4.6. *Sei* K *ein Körper,* $n \in \mathbb{N}$ *und* $f \in K[X_1, \ldots, X_n]$*.*

1. *Ist* K *vollkommen und* f *reduziert, so ist* f *absolut reduziert.*
2. *Sei*
$$\frac{\partial f}{\partial X_\nu} = 0 \quad \textit{für alle} \quad \nu \in [1,n].$$
   Dann ist entweder $f \in K$ *oder* $\mathrm{char}(K) = p > 0$ *und* $f = g(X_1^p, \ldots, X_n^p)$ *mit einem Polynom* $g \in K[X_1, \ldots, X_n]$*. Ist* K *algebraisch abgeschlossen und* $\mathrm{char}(K) = p > 0$*, so folgt* $f = g_1^p$ *mit einem Polynom* $g_1 \in K[X_1, \ldots, X_n]$*.*

Beweis. 1. Sei $f = f_1 \cdot \ldots \cdot f_k \in K[X_1, \ldots, X_n]$ mit $k \in \mathbb{N}$, paarweise nicht assoziierten irreduziblen $f_1, \ldots, f_k \in K[X_1, \ldots, X_n]$, und sei $q \in \overline{K}[X_1, \ldots, X_n]$ mit $q^2 \mid f$ in $\overline{K}[X_1, \ldots, X_n]$. Dann gibt es eine endliche Körpererweiterung L/K mit $q \in L[X_1, \ldots, X_n]$ und $q^2 \mid f$ in $L[X_1, \ldots, X_n]$. Da K vollkommen ist, ist $L = K(\alpha)$ mit über K separablem $\alpha \in L$. Sei (nach geeigneter Umnummerierung) $q \notin L[X_1, \ldots, X_{n-1}]$ und $l \in [1,k]$, so dass $f_1, \ldots, f_l \notin K[X_1, \ldots, X_{n-1}]$ und $f_{l+1}, \ldots, f_k \in K[X_1, \ldots, X_{n-1}]$. Sei $K^* = K(X_1, \ldots, X_{n-1})$, $L^* = L(X_1, \ldots, X_{n-1}) = K^*(\alpha)$ und $X = X_n$. Dann ist L^*/K^* separabel, $f_1, \ldots, f_l \in K^*[X]$ sind nach dem Gauß'schen Lemma paarweise nicht assoziiert und irreduzibel über K^*, $f_{l+1}, \ldots, f_k \in K^{*\times}$, und $q^2 \mid f = f_1 \cdot \ldots \cdot f_l \in L^*[X]$. Für $i, j \in [1,l]$ mit $i \neq j$ ist $(f_i, f_j) = 1$ in $K^*[X]$, es gibt φ, $\psi \in K^*[X]$ mit $\varphi f_i + \psi f_j = 1$, und daher gibt es höchstens ein $i \in [1,l]$ mit $q \mid f_i$ in $L^*[X]$, etwa $i = 1$, und dann ist auch $q^2 \mid f_1$ in $L^*[X]$. Daher ist f_1 inseparabel, $\mathrm{char}(K) = p > 0$ und $f_1 = g(X^{p^e})$ mit irreduziblem separablem $g \in K^*[X]$ und $e \in \mathbb{N}$. Dann ist $f_1 = c(X^{p^e} - \alpha_1) \cdot \ldots \cdot (X^{p^e} - \alpha_m)$, und die Polynome $X^{p^e} - \alpha_1, \ldots, X^{p^e} - \alpha_m \in L_1^*[X]$ sind irreduzibel und paarweise nicht assoziiert. Ist $q_1 \in L_1^*[X]$ irreduzibel mit $q_1 \mid q$, so folgt $q_1^2 \mid f_1$ in L_1^*, ein Widerspruch!

2. Induktion nach n. Sei
$$f = \sum_{\nu \geq 1} a_\nu X_n^\nu \quad \text{mit} \quad a_\nu \in K[X_1, \ldots, X_{n-1}], \ \text{falls} \ n \geq 2, \ \ a_n \in K, \ \ \text{falls} \ n = 1,$$
und $a_\nu = 0$ für fast alle $\nu \geq 0$. Dann ist
$$\frac{\partial f}{\partial X_n} = \sum_{\nu \geq 1} \nu a_\nu X_n^{\nu-1} = 0.$$

FALL 1: $\mathrm{char}(K) = 0$. Dann ist $a_\nu = 0$ für alle $\nu \geq 1$. Im Falle $n = 1$ folgt $f = a_0 \in K$. Im Falle $n \geq 1$ ist
$$\frac{\partial a_0}{\partial X_i} = 0 \ \text{ für alle } \ i \in [1, n-1]$$
und daher $a_0 \in K$ nach Induktionsvoraussetzung.

FALL 2: $\mathrm{char}(K) = p > 0$ und $f \notin K$. Dann ist $a_\nu = 0$ für alle $\nu \geq 1$ mit $p \nmid \nu$. Im Falle $n = 1$ folgt

$$f = g(X_n^p) \text{ mit } g = \sum_{\nu \geq 0} a_{p\nu} X^\nu.$$

Im Falle $n \geq 2$ ist

$$f = \sum_{\nu \geq 0} a_{p\nu} X_n^{p\nu} \text{ und } \frac{\partial f}{\partial X_i} = \sum_{\nu \geq 0} \frac{\partial a_{p\nu}}{\partial X_i} X_n^{p\nu} = 0 \text{ für alle } i \in [1, n-1],$$

also

$$\frac{\partial a_{p\nu}}{\partial X_i} = 0 \text{ für alle } \nu \geq 0 \text{ und } i \in [1, n-1].$$

Nach Induktionsvoraussetzung ist $a_{p\nu} = b_\nu(X_1^p, \ldots, X_{n-1}^p)$ mit $b_\nu \in K[X_1, \ldots, X_{n-1}]$ für alle $\nu \geq 0$ und daher

$$f = g(X_1^p, \ldots, X_n^p) \text{ mit } g = \sum_{\nu \geq 0} b_\nu X_n.$$

Ist K algebraisch abgeschlossen und $\mathrm{char}(K) = p > 0$, so ist

$$f = \sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n} X_1^{pi_1} \cdot \ldots \cdot X_n^{pi_n} = \Big(\sum_{i_1, \ldots, i_n \geq 0} a_{i_1, \ldots, i_n}^{1/p} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \Big)^p. \qquad \square$$

Satz 0.4.7. *Sei R ein faktorieller Bereich. Dann hat $R[X]$ unendlich viele Primelemente.*

BEWEIS. Sei $K = \mathsf{q}(R)$. Es genügt, zu zeigen: Es gibt unendlich viele normierte Polynome $f \in R[X]$, die über K irreduzibel sind. Ist R unendlich, so ist $\{X - a \mid a \in R\}$ eine unendliche Menge über K irreduzibler normierter Polynome. Ist R endlich, so ist R ein endlicher Körper, und zu jedem $n \in \mathbb{N}$ gibt es einen Oberkörper $L \supset R$ mit $[L : R] = n$. Da K vollkommen ist, ist L/R separabel, also $L = R(\alpha)$ mit $\alpha \in R$. Das Minimalpolynom von α über R ist ein normiertes irreduzibles Polynom vom Grade n. Daher gibt es zu jedem $n \in \mathbb{N}$ ein normiertes irreduzibles Polynom vom Grade n. $\square$

KAPITEL 1

Ebene affine Kurven

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

1.1. Definition und Beispiele

Definition 1.1.1. Für $n \in \mathbb{N}$ nennen wir $\mathbb{A}^n = \mathbb{A}^n(\overline{K}) = \overline{K}^n$ den *n-dimensionalen affinen Raum* über K und $\mathbb{A}^n(K) = K^n \subset \mathbb{A}^n$ die Menge der *K-wertigen Punkte* von $\mathbb{A}^n$. $\mathbb{A}^1$ heißt *affine Gerade* und $\mathbb{A}^2$ heißt *affine Ebene* über K.

Für ein Polynom $f \in K[X,Y]$ heißt $V(f) = \{p \in \mathbb{A}^2 \mid f(p) = 0\}$ das *Nullstellengebilde* von f. Eine Teilmenge $C \subset \mathbb{A}^2$ heißt (*ebene affine*) *über K definierte* (*algebraische*) *Kurve*, wenn es ein $f \in K[X,Y] \setminus K$ gibt mit $C = V(f)$. Die Menge $C(K) = C \cap K^2$ heißt Menge der *K-rationalen Punkte* von $C = C(\overline{K})$. Ist $K \subset L \subset \overline{K}$ ein Zwischenkörper, so ist jede über K definierte Kurve auch über L definiert.

Eine Teilmenge $L \subset \mathbb{A}^2$ 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.

Satz 1.1.2.

1. *Sei $p = (\alpha, \beta) \in \mathbb{A}^2(K)$. Für eine Teilmenge $L \subset \mathbb{A}^2$ sind äquivalent*:
   (a) *L ist eine über K definierte Gerade mit $p \in L$.*
   (b) *$L = V(a(X-\alpha) + b(Y-\beta))$ mit $(a,b) \in (K^2)^\bullet$.*
   (c) *Es gibt einen Vektor $u \in (K^2)^\bullet$ mit $L = p + \overline{K}u$.*
2. *Seien p, $q \in \mathbb{A}^2(K)$ und $p \neq q$. Dann gibt es genau eine über K definierte Gerade $L \subset \mathbb{A}^2$ mit $\{p,q\} \subset L$, nämlich $L = \{sp + tq \mid s, t \in \overline{K},\ s + t = 1\}$.*

Beweis. 1. (a) $\Rightarrow$ (b) Sei $L = V(aX + bY + c)$ mit a, b, $c \in K$ und $(a,b) \neq (0,0)$. Dann ist $a\alpha + b\beta + c = 0$ und daher $aX + bY + c = a(X-\alpha) + b(Y-\beta)$.

(b) $\Rightarrow$ (c) Für eine Punkt $(x,y) \in \mathbb{A}^2$ ist genau dann $a(x-\alpha) + b(y-\beta) = 0$, wenn es ein $\lambda \in \overline{K}$ gibt mit $(x-\alpha, y-\beta) = \lambda(-b,a)$. Mit $u = (-b,a) \in (K^2)^\bullet$ folgt $L = p + \overline{K}u$.

(c) $\Rightarrow$ (a) Seien a, $b \in K$ mi $u = (-b,a) \in (K^2)^\bullet$. Für einen Punkt $(x,y) \in \mathbb{A}^2$ gilt: Genau dann ist $(x,y) \in p + \overline{K}u$, wenn es ein $\lambda \in \overline{K}$ gibt mit $(x,y) = (\alpha,\beta) + \lambda(-b,a)$, und das ist genau dann der Fall, wenn $ax + by = a\alpha + b\beta$. Damit folgt $p + \overline{K}u = V(aX + bY - (a\alpha + b\beta))$, und offensichtlich ist $p \in p + \overline{K}u$.

2. Sei $p = (\alpha,\beta)$, $q = (\gamma,\delta)$, $a = \delta - \beta$, $b = \alpha - \gamma$ und $c = \beta\gamma - \alpha\delta$. Dann ist $(a,b) \neq (0,0)$ und $a\alpha + b\beta + c = a\gamma + b\delta + c = 0$, also $\{p,q\} \subset V(aX + bY + c)$. Sei nun $L \subset \mathbb{A}^2$ eine über K definierte Gerade mit $\{p,q\} \subset L$. Nach 1. ist $L = p + \overline{K}u$ mit $u \in (K^2)^\bullet$ und daher $q = p + \lambda u$

mit $\lambda \in \overline{K}^\times$. Es folgt $L = p + \overline{K}\lambda^{-1}(q-p) = p + \overline{K}(q-p) = \{p + t(q-p) \mid t \in \overline{K}\}$ und daher $L = \{sp + tq \mid s,\, t \in \overline{K},\ s+t = 1\}$. □

Beispiel 1.1.3 (Kreislinie)**.** Sei $a \in K$, $f_a = X^2+Y^2-a^2 \in K[X,Y]$ und $C_a = V(f_a) \subset \mathbb{A}^2$, also $C_a = \{\alpha, \beta) \in \mathbb{A}^2 \mid \alpha^2 + \beta^2 = a^2\}$. Ist $\mathrm{char}(K) = 2$, so ist $f_a = (X+Y+a)^2$ und $C_a = V(X+Y+a)$ eine Gerade.

Sei nun $\mathrm{char}(K) \neq 2$ und $\mathsf{i} \in \overline{K}$ mit $\mathsf{i}^2 = -1$. Dann ist $f_0 = X^2+Y^2 = (X+\mathsf{i}Y)(X-\mathsf{i}Y)$, und $C_0 = L_+ \cup L_-$ mit $L_\pm = V(X \pm \mathsf{i}Y) \subset \mathbb{A}^2$. Ist $\mathsf{i} \notin K$, so ist f_0 irreduzibel über K (aber nicht absolut irreduzibel), und $C_0(K) = \{(0,0)\}$. Ist $a \in K^\times$, so ist f_a absolut irreduzibel (Ü!), und $C_a = aC_1$.

Sei nun $a = 1$. Für $k \in \overline{K}$ sei $L_k = V(kX + Y - 1) \subset \mathbb{A}^2$ eine Gerader durch $(0,1)$. Ist $k \neq \pm\mathsf{i}$, so gilt für alle $(\alpha, \beta) \in \mathbb{A}^2$:

$$(\alpha,\beta) \in L_k \cap C_1 \iff (\alpha,\beta) = \Big(\frac{2k}{1+k^2}, \frac{1-k^2}{1+k^2}\Big).$$

Damit erhalten wir eine bijektive Abbildung

$$\tau\colon \overline{K} \setminus \{\pm\mathsf{i}\} \to C_1 \setminus \{(0,-1)\} \quad \text{vermöge} \quad \tau(k) = \Big(\frac{2k}{1+k^2}, \frac{1-k^2}{1+k^2}\Big).$$

Die Umkehrabbildung $\tau^{-1}\colon C_1 \setminus \{(0,-1)\} \to \overline{K} \setminus \{\pm\mathsf{i}\}$ ist gegeben durch

$$\tau^{-1}(\alpha,\beta) = \frac{1-\beta}{\alpha}, \ \text{ falls } \ \alpha \neq 0, \ \text{ und } \ \tau^{-1}(0,1) = 0.$$

Insbesondere ist auch $\tau \mid K \setminus \{\pm\mathsf{i}\}\colon K \setminus \{\pm\mathsf{i}\} \to C_1(K) \setminus \{(0,-1)\}$ bijektiv. Im Falle $K = \mathbb{Q}$ erhalten wir eine bijektive Abbildung $\mathbb{Q} \to \{(x,y) \in \mathbb{Q}^2 \mid x^2+y^2 = 1\} \setminus \{(0,-1)\}$ (Parametrisierung der rationalen 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 $c \neq 0$, und

$$\Big(\frac{a}{c}, \frac{b}{c}\Big) \in C_1(\mathbb{Q}) \cap \mathbb{Q}^2_{>0}.$$

Daher gibt es ein $k \in \mathbb{Q} \cap [0,1]$ mit

$$\frac{a}{c} = \frac{2k}{1+k^2}, \quad \frac{b}{c} = \frac{1-k^2}{1+k^2}, \ \text{ und es sei } \ k = \frac{n}{m} \ \text{ mit } \ m \in \mathbb{N}_0,\ n \in \mathbb{N},\ (n,m) = 1 \ \text{ und } \ n \leq m.$$

Es folgt $(m^2-n^2, m^2+n^2) \mid 2$,

$$\frac{a}{c} = \frac{2mn}{m^2+n^2}, \quad \frac{b}{c} = \frac{m^2-n^2}{m^2+n^2}, \ \text{ und wir behaupten } \ (m^2-n^2, m^2+n^2) = 1.$$

Wäre nämlich $(m^2-n^2, m^2+n^2) = 2$, so folgte $m \equiv n \equiv 1 \bmod 2$, $m^2-n^2 \equiv 0 \bmod 8$, $m^2+n^2 \equiv 2 \bmod 4$ und $2 \mid b$, ein Widerspruch. Also ist $(m^2-n^2, m^2+n^2) = 1$ und daher $(a,b,c) = (2mn, m^2-n^2, m^2+n^2)$. Wegen $2 \nmid b$ folgt $m \not\equiv n \bmod 2$, also

$$\mathcal{P} \subset \{(2mn, m^2-n^2, m^2+n^2) \mid m \in \mathbb{N}_0,\ n \in \mathbb{N},\ (m,n) = 1,\ m \not\equiv n \mod 2,\ m \geq n\},$$

und wir behaupten Gleichheit. Dazu ist zu zeigen: Sind $m\,n \in \mathbb{N}_0$, $(m,n) = 1$ und $m \not\equiv n \bmod 2$, so folgt $(2mn, m^2-n^2) = 1$. (Ü!)

Weitere Spezialfälle:

- $K = \mathbb{R},\ \overline{K} = \mathbb{C}\colon\ C_{-1} = \{(\alpha,\beta) \in \mathbb{C}^2 \mid \alpha^2 + \beta^2 = -1\} = \mathsf{i}C_1$ und $C_{-1}(\mathbb{R}) = \emptyset$.
- $K = \mathbb{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}\colon\ \overline{2} = -\overline{1},\ C_{\overline{2}}(\mathbb{F}_3) = \{(\alpha,\beta) \in \mathbb{F}_3^2 \mid \alpha^2 + \beta^2 = \overline{2}\} = \mathbb{F}_3^\times \times \mathbb{F}_3^\times$, also $|C_{\overline{2}}(\mathbb{F}_3)| = 4$, aber $|C_{\overline{2}}(\overline{F}_3^2)| = \infty$ (siehe Satz 1.2.1).

1.2. Unendlichkeit und Endlichkeit

Satz 1.2.1. *Für jede Kurve $C \subset \mathbb{A}^2$ ist $|C| = |\mathbb{A}^2 \setminus C| = \infty$.*

Beweis. Sei $C = V(f)$ und

$$f = \sum_{i=0}^{n} a_i(Y)X^i \in K[X,Y] \setminus K \quad \text{mit} \quad n \in \mathbb{N}_0\,,\ a_0(Y), \ldots, a_n(Y) \in K[Y] \ \text{ und } \ a_n(Y) \neq 0\,.$$

FALL 1: $n = 0$. Dann ist $f = a_0(Y) = c(Y - y_1) \cdot \ldots \cdot (Y - y_m)$ mit $c \in K^\times$, $m \in \mathbb{N}$ und $y_1, \ldots, y_m \in \overline{K}$. Ist $y \in \overline{K} \setminus \{y_1, \ldots, y_m\}$, so folgt

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

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

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

Satz 1.2.2. *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 gemeinsamen Teiler in $R_1[Y] \setminus R_1$. Nach Lemma 0.2.3 gibt es $p_1, q_1 \in R_1[Y] = K[X,Y]$ mit $p_1 f + q_1 g = d_1 \in R_1^\bullet = K[X]^\bullet$. Aus demselben Grund gibt es Polynome $p_2, q_2 \in K[X,Y]$ mit $p_2 f + q_2 g = d_2 \in K[Y]^\bullet$. Ist nun $(\alpha,\beta) \in V(f) \cap V(g)$, so folgt $d_1(\alpha) = d_2(\beta) = 0$ und daher $|V(f) \cap V(g)| \leq \mathrm{gr}(d_1)\mathrm{gr}(\mathrm{d}_2) < \infty$. $\square$

1.3. Reguläre Funktionen und Verschwindungsideale

Definition 1.3.1. Sei $C \subset \mathbb{A}^2$ eine über K definierte Kurve. Eine Abbildung $u\colon C \to \overline{K}$ heißt eine *über K definierte reguläre Funktion* (auf C), wenn es ein Polynom $g \in K[X,Y]$ gibt, so dass $u(p) = g(p)$ für alle $p \in C$. 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 $K \subset K[C]$.

Für ein Polynom $f \in K[X,Y]$ betrachten wir die polynomiale Abbildung $\overline{f}\colon \mathbb{A}^2 \to \overline{K}$, definiert durch $\overline{f}(\alpha,\beta) = f(\alpha,\beta)$. Da $\overline{K}$ unendlich ist, ist die Abbildung

$$K[X,Y] \ \to \ \mathrm{Abb}(\mathbb{A}^2, \overline{K}), \quad f \ \mapsto \ \overline{f}$$

ein K-Algebrenisomorphismus. Wir identifizieren das Polynom f mit der Abbildung $\overline{f}$. Dann ist $K[C] = \{g \restriction C \mid g \in K[X,Y]\}$, und die Abbildung $\theta_C\colon K[X,Y] \to K[C]$, definiert durch

$\theta_C(f) = f \restriction C$, ist ein K-Algebrenepimorphismus. Die Funktionen $x = \theta_C(X) \in K[C]$ und $y = \theta_C(Y) \in K[C]$ heißen die *Koordinatenfunktionen* von C. Es ist $K[C] = K[x, y]$, und für jeden Punkt $p = (\alpha, \beta) \in C$ ist $x(p) = \alpha$ und $y(p) = \beta$. Für $g \in K[X, Y]$ ist $\theta_C(g) = g(x, y)$, und für alle Punkte $p = (\alpha,\ \beta) \in C$ ist $\theta_C(g)(p) = g(x, y)(p) = g(x(p), y(p)) = g(\alpha, \beta)$. Insbesondere folgt: Genau dann ist $g \restriction C = 0$, wenn $g(x, y) = 0 \in K[C]$.

Das Ideal

$$\mathfrak{I}_K(C) = \mathrm{Ker}(\theta_C) = \{g \in K[X, Y] \mid g \restriction C = 0\} = \{g \in K[X, Y] \mid C \subset V(g)\} \ \lhd \ K[X, Y]$$

heißt *K-Verschwindungsideal* von C. θ_C induziert einen K-Algebrenisomorphismus

$$\theta_C^*\colon K[X, Y]/\mathfrak{I}_K(C) \ \xrightarrow{\sim}\ K[C] \quad \text{mit} \quad \theta_C^*(g + \mathfrak{I}_K(C)) = g \restriction C \quad \text{(wir identifizieren!)}.$$

Für Kurven C, $C_1 \subset \mathbb{A}^2$ mit $C \subset C_1$ ist $\mathfrak{I}_K(C) \supset \mathfrak{I}_K(C_1)$.

Satz und Definition 1.3.2. *Sei $f = f_1^{e_1} \cdot \ldots \cdot f_k^{e_k} \in K[X, Y] \setminus K$ mit $k \in \mathbb{N}$, paarweise nicht-assoziierten irreduziblen Polynomen $f_1, \ldots, f_k \in K[X, Y] \setminus K$ und $e_1, \ldots, e_k \in \mathbb{N}$. Sei $C = V(f) \subset \mathbb{A}^2$ und $f_0 = f_1 \cdot \ldots \cdot f_k$. Dann ist $f_0 \in K[X, Y]$ ein reduziertes Polynom,*

$$C = V(f_0) = \bigcup_{i=1}^{k} V(f_i), \quad \mathfrak{I}_K(C) = (f_0) \lhd K[X, Y] \quad \textit{und} \quad K[C] = K[X]/(f_0)\,.$$

Insbesondere sind die Polynome f_0, $f_1, \ldots, f_k$ durch C bis auf Faktoren aus $K^\times$ eindeutig bestimmt.

Die durch C eindeutig bestimmten Kurven $V(f_1), \ldots, V(f_k)$ heißen die *Komponenten* von C (über K).

Beweis. Offensichtlich ist f_0 ein reduziertes Polynom. Sei $p \in \mathbb{A}^2$. Genau dann ist $p \in C$, wenn $0 = f(p) = f_1(p)^{e_1} \cdot \ldots \cdot f_k(p)^{e_k}$, wenn also $f_i(p) = 0$ für ein $i \in [1, k]$ und damit $p \in V(f_i)$ ist. Daher folgt

$$C = V(f) = V(f_0) = \bigcup_{i=1}^{k} V(f_i)\,.$$

Für alle $p \in C$ ist $f_0(p) = 0$, also $f_0 \in \mathfrak{I}_K(C))$ und daher $(f_0) \subset \mathfrak{I}_K(C)$. Wir zeigen Gleichheit und nehmen dazu an, es $g \in \mathfrak{I}_K(C) \setminus (f_0)$, also $f_0 \nmid g$, und es sei f^* ein ggT von f_0 und g. Dann ist $f^* \mid f_0$, aber $f^* \not\simeq f_0$, und aus der Eindeutigkeit der Primzerlegung folgt

$$f^* \simeq \prod_{i \in I} f_i \quad \text{für eine Teilmenge} \quad I \subsetneq [1, k]\,.$$

Ist $i \in [1, k] \setminus I$, so folgt $f_1 \nmid f^*$, aber $f_i \mid f_0$, also $f_i \nmid g$. Da f_i irreduzibel ist, sind f_i und g teilerfremd, und daher ist $|V(f_i) \cap V(g)| < \infty$. Nun ist aber $V(f_i) \subset V(f) = C \subset V(g)$ und daher $V(f_i) \cap V(g) = V(f_i)$ unendlich, ein Widerspruch! Es ist also $\mathfrak{I}_K(C) = (f_0)$ und $K[C] = K[X]/\mathfrak{I}_K(C) = K[X]/(f_0)$. □

Korollar 1.3.3. *Seien f, $g \in K[X, Y] \setminus K$ reduziert. Genau dann ist $V(f) \subset V(g)$, wenn $(g) \subset (f)$ [oder $f \mid g$].*

BEWEIS. Offensichtlich ist genau dann $(g) \subset (f)$, wenn $f \mid g$, und dann ist $V(f) \subset V(g)$, denn aus $f(p) = 0$ folgt $g(p) = 0$ für alle $p \in \mathbb{A}^2$. Sei nun $V(f) \subset V(g)$. Nach Satz 1.3.2 ist dann

$$\begin{aligned}(g) &= \mathfrak{I}_K(V(g)) = \{h \in K[X,Y] \mid V(g) \subset V(h)\} \subset \{h \in K[X,Y] \mid V(f) \subset V(h)\} \\ &= \mathfrak{I}_K(V(f)) = (f).\end{aligned}$$ □

Satz 1.3.4. *Sei $f \in K[X,Y] \setminus K$. Dann ist das Hauptideal $(f) \lhd K[X,Y]$ nicht maximal. Insbesondere ist der Koordinatenring $K[C]$ einer über K definierten Kurve C kein Körper.*

BEWEIS. Sei C eine über K definierte Kurve. Dann ist $K[C] = K[X,Y]/(f)$ mit einem Polynom $f \in K[X,Y] \setminus K$. Es genügt also zu zeigen, dass (f) kein maximales Ideal ist, und dazu können wir annehmen, dass $f \notin K[Y]$.

$R = K[Y]$ ist ein faktorieller Bereich mit unendlich vielen Primelementen (Satz 0.4.7). Sei $f = a_n X^n + a_{n-1}X^{n-1} + \ldots + a_0 \in R[X] = K[X,Y]$ mit $n \in \mathbb{N}$, $a_n \neq 0$, und sei $p \in R$ ein Primelement mit $p \nmid a_n$. Wir zeigen $(f) \subsetneq (f,p) \subsetneq R[X]$. Wegen $p \notin (f)$ ist $(f) \subsetneq (f,p)$. Wir nehmen an, es seit $(f,p) = R[X]$. Dann gibt es Polynome g, $h \in R[X]$ mit $1 = pg + fh$. Sei $\pi\colon R[X] \to R/(p)[X]$, $g \mapsto \overline{g}$, die natürliche Fortsetzung des Restklassenhomomorphismus auf die Polynomringe. Dann ist $\overline{1} = \overline{f}\,\overline{g} \in R/(p)[X]$, ein Widerspruch da $\overline{f}$ ein Polynom vom Grade n ist. □

1.4. Irreduzible Kurven und Funktionenkörper

Definition 1.4.1. Eine über K definierte Kurve $C \subset \mathbb{A}^2$ heißt

- *irreduzibel* (über K), wenn C keine Zerlegung $C = C_1 \cup C_2$ in über K definierte Kurven C_1, $C_2 \subsetneq C$ besitzt;
- *absolut irreduzibel*, wenn C über $\overline{K}$ irreduzibel ist.

Satz 1.4.2. *Sei $C \subset \mathbb{A}^2$ 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) *$\mathfrak{I}_K(C)$ ist ein Primideal von $K[X,Y]$.*
   (e) *$K[C]$ ist ein Bereich.*
2. *Sind C und C_1 verschiedene über K definierte irreduzible Kurven, so ist $|C \cap C_1| < \infty$.*
3. *C hat eine (bis auf die Reihenfolge der Faktoren) eindeutige Zerlegung $C = C_1 \cup \ldots \cup C_k$ in verschiedene über K definierte irreduzible Kurven $C_1, \ldots, C_k$; diese sind die Komponenten von C über K.*

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

(b) $\Rightarrow$ (c) Nach Satz 1.3.2 ist $C = V(f_0)$ mit einem reduzierten Polynom $f_0 \in K[X,Y] \setminus K$, und wir nehmen an, f_0 sei nicht irreduzibel. Dann ist $f_0 = f_1 f_2$ mit f_1, $f_1 \in K[X,Y]$ und $(f_1, f_2) = 1$. Es folgt $C = V(f_1) \cup V(f_2)$, also $C = V(f_1)$ oder $C = V(f_2)$, etwa $C = V(f_1)$. Da f und f_1 reduziert sind, folgt $(f) = \mathfrak{I}_K(C) = (f_1)$, also $f \simeq f_1$ und daher $f_2 \in K^\times$, ein Widerspruch.

(c) $\Rightarrow$ (d) Ist $C = V(f)$ mit einem irreduziblen Polynom $f \in K[X,Y] \setminus K$, so ist (nach Satz 1.3.2) $\mathfrak{I}_K(C) = (f)$ ein Primideal.

(d) $\Leftrightarrow$ (e) Es ist $K[C] = K[X,Y]/\mathfrak{I}_K(C)$.

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

2. Sei $C_1 = V(f_1)$ und $C_2 = V(f_2)$ mit irreduziblen Polynomen f_1, $f_2 \in K[X,Y] \setminus K$. Ist $C_1 \neq C_2$, so folgt $f_1 \not\simeq f_2$, also $(f_1, f_2) = 1$ und daher $|C_1 \cap C_2| < \infty$.

3. Die Komponenten $C_1, \ldots, C_k$ von C sind k ürverschiedene über K definierte irreduzible Kurven mit $C = C_1 \cup \ldots \cup C_k$. Daher genügt es, die Eindeutigkeit zu zeigen.

Sei $l \in \mathbb{N}$ und $C = C'_1 \cup \ldots \cup C'_l$ eine Zerlegung von C in verschiedene über K definierte irreduzible Kurven. Für $i \in [1,k]$ ist $C_i = (C'_1 \cap C_i) \cup \ldots \cup (C'_l \cap C_i)$. Daher gibt es ein $j \in [1,l]$ mit $|C'_j \cap C_i| = \infty$, also $C'_j = C_i$ nach 2., und daher ist j durch i eindeutig bestimmt. Es gibt also eine Abbildung $\pi\colon [1,k] \to [1,l]$, so dass $C'_{\pi(i)} = C_i$ für alle $i \in [1,k]$. Ebenso gibt es eine Abbildung $\pi'\colon [1,l] \to [1,k]$, so dass $C_{\pi'(j)} = C'_j$ für alle $j \in [1,l]$. Für alle $i \in [1,k]$ ist $C_{\pi' \circ \pi(i)} = C'_{\pi(i)} = C_i$, also $\pi' \circ \pi(i) = i$ und daher $\pi' \circ \pi = \mathrm{id}_{[1,k]}$. Ebenso ist $\pi \circ \pi' = \mathrm{id}_{[1,l]}$. Es folgt $l = k$, $\pi \in \mathfrak{S}_k$, und $C'_{\pi(i)} = C_i$ für alle $i \in [1,k]$. $\square$

Definition 1.4.3. Sei $C \subset \mathbb{A}^2$ eine über K definierte irreduzible Kurve. Dann ist $K[C]$ ein Bereich; sein Quotientenkörper $K(C) = \mathfrak{q}(K[C])$ heißt *Funktionenkörper* von C über K, seine Elemente heißen (über K definierte) *rationale Funktionen* auf C.

Sei $\mathfrak{I}_K(C) = (f)$ mit irreduziblem $f \in K[X,Y] \setminus K$ und $\gamma \in K(C)$. Dann ist

$$\gamma = \frac{\varphi}{\psi} = \frac{g + (f)}{h + (f)} \text{ mit } g, h \in K[X,Y],\ h \notin (f),\ \varphi = g + (f) \in K[C] \text{ und } \psi = h + (f) \in K[C].$$

Da $K[C]$ im Allgemeinen nicht faktoriell ist, ist diese Bruchdarstellung nicht eindeutig. Ist $\gamma \in K(C)$ und $p \in C$, so heißt γ *regulär* in p, wenn es g, $h \in K[X,Y]$ gibt mit $h(p) \neq 0$ und

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

$\gamma(p)$ hängt nur von γ und p und nicht von der Bruchdarstellung von γ ab. Da f irreduzibel ist, ist genau dann $h \notin (f)$, wenn h und f teilerfremd sind. Daher ist die Menge

$$\{p \in C \mid h(p) = 0\} = V(f) \cap V(h)$$

endlich und γ in fast allen Punkten von C regulär.

Satz 1.4.4. *Sei $C \subset \mathbb{A}^2$ eine über K definierte irreduzible Kurve, und $\mathfrak{I}_K(C) = (f)$ mit $f \in K[X,Y]$. 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 $K(x)$. Ist f absolut irreduzibel, so ist K relativ algebraisch abgeschlossen in $K(C)$.

Beweis. Nach Definition ist $K[C] = K[x,y]$, also $K(C) = K(x,y)$, und $f(x,y) = 0$. 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 $p = (\alpha,\beta) \in C$ ist dann $0 = g(x)(p) = g(\alpha)$ und $0 = g(y)(p) = g(\beta)$. Damit folgt $|C| < \infty$, ein Widerspruch zu Satz 1.2.1.

Sei nun x transzendent über K. Dann ist $f \in K[X,Y] \setminus K[X]$ [denn aus $f \in K[X]$ folgt $f(x) = f(x,y) = 0$]. Es ist $K[x] \cong K[X]$, $K[X,Y] \cong K[x,Y] = K[x][Y]$, $f(x,Y) \in K[x][Y]$ ist irreduzibel über $K[x]$, also nach dem Gauß'schen Lemma auch über $K(x)$, und $f(x,y) = 0$. Dann ist $c^{-1}f(x,Y) \in K(x)[Y]$ normiert und irreduzibel, und $c^{-1}f(x,y) = 0$. Daher ist $f(x,Y)$ das Minimalpolynom von y über $K(x)$, und $[K(x,y)\colon K(x)] = \mathrm{gr}(f(x,Y)) = \mathrm{gr}_Y(f)$.

Sei nun C (also auch f) absolut irreduzibel und $\widetilde{K}$ der relative algebraische Abschluss von K in $K(C)$. Dann ist f irreduzibel über $\widetilde{K}$, x ist transzendent über $\widetilde{K}$, $K(C) = \widetilde{K}(x,y)$, $f(x,Y)$ ist irreduzibel über $\widetilde{K}[x]$, also auch über $\widetilde{K}(x)$, und $f(x,y) = 0$. Daher ist $c^{-1}f(x,Y) \in \widetilde{K}(x)[Y]$ auch das Minimalpolynom von y über $\widetilde{K}(x)$, es folgt $[K(C)\colon\widetilde{K}(x)] = \mathrm{gr}_Y(f)$, und

$$\mathrm{gr}_Y(f) = [K(x,y)\colon K(x)] = [K(x,y)\colon\widetilde{K}(x)]\,[\widetilde{K}(x)\colon K(x)] = \mathrm{gr}_Y(f)[\widetilde{K}\colon K],$$

also $[\widetilde{K}\colon K] = 1$ und daher $\widetilde{K} = K$. □

Beispiel 1.4.5. Sei $K = \mathbb{R}$ und $C = V(X^2 + Y^2) \subset \mathbb{C}^2$. Dann ist C 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 $\mathbb{R}$.

Definition 1.4.6. Sei $C \subset \mathbb{A}^2$ eine über K definierte irreduzible Kurve und $p \in C$. Dann heißt

$$\mathcal{O}_p(C) = \mathcal{O}_{p,K}(C) = \{\gamma \in K(C) \mid \gamma \text{ ist regulär in } p\}$$

der *lokale Ring* von C in p über K, und

$$\mathcal{M}_p(C) = \mathcal{M}_{p,K}(C) = \{\gamma \in \mathcal{O}_p(C) \mid \gamma(p) = 0\}$$

das *maximale Ideal* von C in p über K.

Definition 1.4.7 (Ringtheorie)**.** Ein Ring R heißt *lokal*, wenn $R \setminus R^\times$ ein Ideal ist. Dann ist $\mathfrak{m} = R \setminus R^\times$ das größte echte Ideal von R und das einzige maximale Ideal von R. Der Körper $k = R/\mathfrak{m}$ heißt *Restklassenkörper* von R .

Satz 1.4.8. *Sei $C \subset \mathbb{A}^2$ eine über K definierte (über K) irreduzible Kurve, $p = (\alpha, \beta) \in C$, $\mathfrak{I}_K(C) = (f)$, und seien x, $y \in K[C]$ die Koordinatenfunktionen von C.*

1. *$\mathcal{O}_p(C)$ ist eine lokale K-Algebra mit maximalem Ideal $\mathcal{M}_p(C)$, es ist $K[C] \subset \mathcal{O}_p(C)$, $\mathcal{M}_p(C) \cap K[C]$ ist ein maximales Ideal von $K[C]$, und die Einlagerung $K[C] \hookrightarrow \mathcal{O}_p(C)$ induziert einen Isomorphismus $K[C]/\mathcal{M}_p(C) \cap K[C] \xrightarrow{\sim} \mathcal{O}_p(C)/\mathcal{M}_p(C)$.*
2. *Die Abbildung $\pi_p \colon \mathcal{O}_p(C) \to \overline{K}$, definiert durch $\pi_p(\gamma) = \gamma(p)$, ist ein K-Algebrenhomomorphismus mit Kern $\operatorname{Ker}(\pi_p) = \mathcal{M}_p(C)$ und Bild*
$$\operatorname{Bi}(\pi_p) = K(\alpha,\beta) = K[\alpha,\beta] = \pi_p(K[C]) \cong K[C]/K[C] \cap \mathcal{M}_p(C) \cong \mathcal{O}_p(C)/\mathcal{M}_p(C).$$
Wir identifizieren: $K[C]/K[C] \cap \mathcal{M}_p(C) = \mathcal{O}_p(C)/\mathcal{M}_p(C) = K(\alpha,\beta)$.
3. *Ist $p \in C(K)$, so ist $\mathcal{M}_p(C) = {}_{\mathcal{O}_p(C)}(x-\alpha, y-\beta) \lhd \mathcal{O}_p(C)$.*

Beweis. 1. und 2. Sei $\lambda \in K$, und für $i \in \{1,2\}$ sei $\gamma_i \in \mathcal{O}_p(C)$,
$$\gamma_i = \frac{\varphi_i}{\psi_i} \in \mathcal{O}_p(C) \quad \text{mit} \quad \varphi_i,\, \psi_i \in K[C] \ \text{ und } \ \psi_i(p) \neq 0\,.$$
Dann ist $(\psi_1\psi_2)(p) = \psi_1(p)\psi_2(p) \neq 0$,
$$\lambda\gamma_1 = \frac{\lambda\varphi_1}{\psi_1} \in \mathcal{O}_p(C)\,, \quad \gamma_1+\gamma_2 = \frac{\varphi_1\psi_2+\varphi_2\psi_1}{\psi_1\psi_2} \in \mathcal{O}_p(C) \ \text{ und } \gamma_1\gamma_2 = \frac{\varphi_1\varphi_2}{\psi_1\psi_2} \in \mathcal{O}_p(C),$$
$$(\lambda\gamma_1)(p) = \lambda\gamma_1(p)\,, \quad (\gamma_1+\gamma_2)(p) = \gamma_1(p)+\gamma_2(p) \ \text{ und } \ (\gamma_1\gamma_2)(p) = \gamma_1(p)\gamma_2(p)\,.$$
Daher ist $\mathcal{O}_p(C) \subset K(C)$ eine K-Unteralgebra, und π_p ist ein K-Algebrenhomomorphismus. Ist $\varphi \in K[C]$, so ist
$$\varphi = \frac{\varphi}{1} \in \mathcal{O}_p(C)\,, \quad \text{also} \quad K[C] \subset \mathcal{O}_p(C)\,.$$
Wegen $\mathcal{M}_p(C) = \{\gamma \in \mathcal{O}_p(C) \mid \gamma(p) = 0\} = \operatorname{Ker}(\pi_p)$ ist $\mathcal{M}_p(C)$ ein Ideal von $\mathcal{O}_p(C)$. Ist $\gamma \in \mathcal{O}_p(C)$ so folgt
$$\gamma = \frac{\varphi}{\psi} \ \text{ mit } \ \varphi,\, \psi \in K[C]\,,\ \varphi(p) \neq 0\,, \ \text{ und aus } \ \gamma \notin \mathcal{M}_p(C) \ \text{ folgt } \psi(p) \neq 0\,, \text{ also } \frac{\psi}{\varphi} \in \mathcal{O}_p(C)\,.$$
Daher ist $\mathcal{O}_p(C) \setminus \mathcal{M}_p(C) \subset \mathcal{O}_p(C)^\times$, und da die umgekehrte Inklusion offensichtlich ist, folgt $\mathcal{M}_p(C) = \mathcal{O}_p(C) \setminus \mathcal{O}_p(C)^\times$. Daher ist $\mathcal{O}_p(C)$ ein lokaler Bereich mit maximalem Ideal $\mathcal{M}_p(C)$ und $\pi_p(\mathcal{O}_p(C) \cong \mathcal{O}_p(C)/\mathcal{M}_p(C)$ ein Körper. Wegen
$$\pi_p(K[C]) = K[\pi_p(x), \pi_p(y)] = K[\alpha,\beta] = K(\alpha,\beta)$$
ist $\pi_p(K[C]) = K(\alpha,\beta)$. Daher ist $\operatorname{Ker}(\pi_p \,|\, K[C]) = K[C] \cap \mathcal{M}_p(C)$ ein maximales Ideal von $K[C]$, und $K[C]/K[C] \cap \mathcal{M}_p(C) \cong K(\alpha,\beta)$.

3. Ist $p \in C(K)$, so ist $(\alpha,\beta) \in K^2$. Sei $\gamma \in \mathcal{O}_p(C)$,
$$\gamma = \frac{g(x,y)}{h(x,y)} \quad \text{mit} \quad g,\, h \in K[X,Y] \ \text{ und } \ h(p) = h(\alpha,\beta) \neq 0\,.$$
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
$$\gamma = \frac{g(x,y)}{h(x,y)} = \frac{c}{h(x,y)} + (x-\alpha)\frac{g_1(x,y)}{h(x,y)} + (y-\beta)\frac{g_2(x,y)}{h(x,y)} \in \frac{c}{h(x,y)} + {}_{\mathcal{O}_p(C)}(x-\alpha, y-\beta).$$
Genau dann ist $\gamma \in \mathcal{M}_p(C)$, wenn $c = 0$ und daher $\gamma \in {}_{\mathcal{O}_p(C)}(x-\alpha, y-\beta)$. □

KAPITEL 2

Ebene projektive Kurven

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

2.1. Homogene Polynome

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

$$F = \sum_{\substack{i_1,\ldots,i_n \geq 0 \\ i_1+\ldots+i_n=d}} c_{i_1,\ldots,i_n} X_1^{i_1} \cdot \ldots \cdot X_n^{i_n} \quad \text{mit Koeffizienten } c_{i_1,\ldots,i_n} \in K.$$

Insbesondere ist $F = 0$ homogen vom Grade d für jedes $d \in \mathbb{N}_0$. Ist $F \in K[X_1, \ldots, X_n]^\bullet$ eine Form vom Grade d, so ist $\operatorname{gr}(F) = d$. Ist T eine weitere Unbestimmte über K, so folgt $F(TX_1, \ldots, TX_n) = T^d F(X_1, \ldots, X_n)$, und

$$\sum_{i=1}^{n} X_i \frac{\partial F}{\partial X_i} = dF\,.$$

Für alle $(i_1, \ldots, i_n) \in \mathbb{N}_0^n$ ist die modifizierte höhere Ableitung $f_{i_1,\ldots,i_n}$ homogen vom Grade $d - (i_1 + \ldots + i_n)$. Daher folgt $\operatorname{ord}_{\lambda \boldsymbol{p}}(f) = \operatorname{ord}_{\boldsymbol{p}}(f)$ für jeden Punkt $\boldsymbol{p} \in K^n$ und $\lambda \in K^\times$.

Jedes Polynom $f \in K[X_1, \ldots, X_n]^\bullet$ mit $\operatorname{gr}(f) = d \in \mathbb{N}_0$ hat eine eindeutige Darstellung

$$f = f_0 + f_1 + \ldots + f_d \quad \text{mit Formen } f_i \text{ vom Grade } i \text{ für alle } i \in [0, d] \text{ und } f_d \neq 0.$$

Man nennt f_i die *i-te homogene Komponente* und f_d die *Leitform* von f.

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

Beweis. Sei $f = f_{d_1} + f_{d_1+1} + \ldots + f_d$ und $g = g_{e_1} + g_{e_1+1} + \ldots + g_e$ mit d_1, d, e_1, $e \in \mathbb{N}_0$, $d_1 \leq d$, $e_1 \leq e$, Formen f_i vom Grade i und g_j vom Grade j für alle $i \in [d_1, d]$ und alle $j \in [e_1, e]$, $f_{d_1} f_d \neq 0$ und $g_{e_1} g_e \neq 0$. Dann ist

$$fg = \sum_{j=d_1+e_1}^{d+e} h_j \quad \text{mit Formen } h_j \text{ vom Grade } j \text{ für alle } j \in [d_1 + e_1, d + e],$$

$h_{d_1+e_1} = f_{d_1} g_{e_1} \neq 0$ 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. □

Lemma 2.1.3. *Seien $m, n \in \mathbb{N}$, $d, e \in \mathbb{N}_0$, sei $F \in K[X_1, \ldots, X_n]$ eine Form vom Grade d, und seien $G_1, \ldots, G_n \in K[Y_1, \ldots, Y_m]$ Formen vom Grade e. Dann ist $F(G_1, \ldots, G_m)$ eine Form vom Grade de.*

Beweis. Für alle $(d_1, \ldots, d_n) \in \mathbb{N}_0^n$ mit $d_1 + \ldots + d_n = d$ ist $G_1^{d_1} \cdot \ldots \cdot G_n^{d_n}$ eine Form vom Grade d. Damit folgt die Behauptung. □

Satz 2.1.4. *Sei $F \in K[X, Y] \setminus K$ eine Form vom Grade d. Dann ist*

$$F = \prod_{i=1}^{d} (\alpha_i X + \beta_i Y) \quad \textit{mit} \quad \alpha_1, \beta_1, \ldots, \alpha_d, \beta_d \in \overline{K}.$$

Ist auch

$$F = \prod_{i=1}^{d} (\alpha_i' X + \beta_i' Y) \quad \textit{mit} \quad \alpha_1', \beta_1', \ldots, \alpha_d', \beta_d' \in \overline{K},$$

so gibt es eine Permutation $\sigma \in \mathfrak{S}_d$ und $\lambda_1, \ldots, \lambda_d \in \overline{K}$, so dass $(\alpha_i', \beta_i') = (\lambda \alpha_{\sigma(i)}, \lambda \beta_{\sigma(i)})$ für alle $i \in [1, d]$.

Beweis. Sei

$$F = \sum_{i=0}^{k} a_i X^i Y^{d-i} \text{ mit } k \in [0, d], \quad a_i, \ldots, a_k \in K, \ a_k \neq 0,$$

und

$$\widetilde{F} = \sum_{i=0}^{k} a_i T^i = a_k \prod_{i=1}^{k} (T - \xi_i) \quad \text{mit } \xi_1, \ldots, \xi_k \in \overline{K}.$$

Dann folgt

$$F = Y^d \sum_{i=0}^{k} a_i \Big(\frac{X}{Y}\Big)^i = Y^d \widetilde{F}\Big(\frac{X}{Y}\Big) = a^k Y^d \prod_{i=1}^{k} \Big(\frac{X}{Y} - \xi_i\Big) = a_k Y^{d-k} \prod_{i=^1}^{k} (X - \xi_i Y).$$

Insbesondere hat f die angegebene Gestalt. Die restliche Behauptung folgt aus der Eindeutigkeit der Primelementzerlegung in $K[X, Y]$. □

2.2. Ebene projektive Kurven

Definition 2.2.1. Sei $n \in \mathbb{N}_0$. Unter dem *n-dimensionalen projektiven Raum $\mathbb{P}^n = \mathbb{P}^n(\overline{K})$ über K* versteht man die Menge aller eindimensionalen Untervektorräume von $\overline{K}^{n+1}$. Es ist $|\mathbb{P}^0| = 1$, $\mathbb{P}^1$ heißt *projektive Gerade*, und $\mathbb{P}^2$ heißt *projektive Ebene* über K.

Für einen Vektor $\boldsymbol{x} = (x_1, \ldots, x_{n+1}) \in (\overline{K}^{n+1})^\bullet$ sei $[\boldsymbol{x}] = (x_1 : \ldots : x_{n+1}) = \overline{K}\boldsymbol{x} \in \mathbb{P}^n$. Man nennt dann $\boldsymbol{x}$ einen *homogenen Koordinatenvektor* des (projektiven) Punktes $[\boldsymbol{x}] \in \mathbb{P}^n$. Für $\boldsymbol{x}, \boldsymbol{x}' \in (\overline{K}^{n+1})^\bullet$ ist genau dann $[\boldsymbol{x}] = [\boldsymbol{x}']$, wenn es ein $\lambda \in \overline{K}^\times$ gibt mit $\boldsymbol{x}' = \lambda \boldsymbol{x}$. Für $i \in [1, n+1]$ heißt

$$\mathbb{P}^n(i) = \{(x_1 : \ldots : x_{n+1}) \in \mathbb{P}^n \mid x_i \neq 0\} = \{(x_1 : \ldots : x_{n+1}) \in \mathbb{P}^n \mid x_i = 1\}$$

das *i-te affine Stück* von $\mathbb{P}^n$. Für jedes $i \in [1, n+1]$ ist die Abbildung

$$\iota_i \colon \mathbb{A}^n \to \mathbb{P}^n(i), \quad \text{definiert durch} \quad \iota_i(x_1, \ldots, x_n) = (x_1 : \ldots : x_{i-1} : 1 : x_i : \ldots : x_n),$$

bijektiv, und

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

Man nennt $\mathbb{P}^n(K) = \{[\boldsymbol{x}] \in \mathbb{P}^n \mid \boldsymbol{x} \in (K^{n+1})^\bullet\}$ die Menge der K-wertigen Punkte von $\mathbb{P}^n$. Offensichtlich ist $\iota_i(\mathbb{A}^n(K)) = \mathbb{P}^n(i) \cap \mathbb{P}^n(K)$ für alle $i \in [1, n+1]$.

Definition 2.2.2. Sei $n \in \mathbb{N}$ und $F \in K[\boldsymbol{X}] = K[X_1, \ldots, X_n]$ eine Form. Ein Punkt $p = [\boldsymbol{p}] \in \mathbb{P}^n$ mit $\boldsymbol{p} \in (K^{n+1})^\bullet$ heißt *Nullstelle* von F, wenn $F(\boldsymbol{p}) = 0$. Diese Definition hängt nur von p und nicht vom homogenen Koordinatenvektor $\boldsymbol{p}$ ab. Ist nämlich $\boldsymbol{p}' = \lambda\boldsymbol{p}$ mit $\lambda \in \overline{K}^\times$ und F vom Grade d, so folgt $F(\boldsymbol{p}') = \lambda^d F(\boldsymbol{p})$, also $F(\boldsymbol{p}') = 0$ genau dann, wenn $F(\boldsymbol{p}) = 0$. Ist p Nullstelle von F, so schreiben wir $F(p) = 0$, andernfalls $F(p) \neq 0$

Definition 2.2.3. Sei $F \in K[X, Y, Z]$ eine Form. Die Menge $V_+(F) = \{p \in \mathbb{P}^2 \mid F(p) = 0\}$ heißt *projektives Nullstellengebilde* von F. Eine Teilmenge $\Gamma \subset \mathbb{P}^2$ heißt eine *über K definierte* (*ebene*) *projektive* (*algebraische*) *Kurve*, wenn $\Gamma = V_+(F)$ mit einer Form $F \in K[X, Y, Z] \setminus K$. Die Menge $\Gamma(K) = \Gamma \cap \mathbb{P}^2(K)$ heißt *Menge der K-rationalen Punkte* von Γ.

Eine Teilmenge $\Lambda \subset \mathbb{P}^2$ heißt eine (*über K definierte*) *projektive Gerade*, wenn

$$\Lambda = V_+(aX + bY + cZ) \quad \text{mit} \quad (a, b, c) \in (K^3)^\bullet.$$

Satz und Definition 2.2.4.

1. *Für $i \in \{1, 2\}$ sei $\Lambda_i = V_+(a_iX + b_iY + c_iZ) \subset \mathbb{P}^2$ mit $(a_i, b_i, c_i) \in (K^3)^\bullet$, und*

$$r = \operatorname{rg} \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}.$$

   Ist $r = 1$, so ist $\Lambda_1 = \Lambda_2$. Ist $r = 2$, so ist $\Lambda_1 \cap \Lambda_2 = \{p\}$ mit $p \in \mathbb{P}^2(K)$. p heißt *Schnittpunkt* von Λ_1 und Λ_2.

2. *Seien $p = [\boldsymbol{p}]$, $q = [\boldsymbol{q}] \in \mathbb{P}^2(K)$ mit $\boldsymbol{p}, \boldsymbol{q} \in (K^3)^\bullet$ und $p \neq q$. Dann gibt es genau eine über K definierte projektive Gerade $\Lambda \subset \mathbb{P}^2$ mit $\{p, q\} \subset \Lambda$, nämlich*

$$\Lambda = \{[s\boldsymbol{p} + t\boldsymbol{q}] \mid (s, t) \in (\mathbb{A}^2)^\bullet\}.$$

   Die Abbildung $\phi\colon \mathbb{P}^1 \to \Lambda$, definiert durch $\phi(s:t) = [s\boldsymbol{p} + t\boldsymbol{q}]$ für alle $(s, t) \in (\mathbb{A}^2)^\bullet$, ist bijektiv, und $\phi(\mathbb{P}^1(K)) = \Lambda(K)$. Λ heißt *Verbindungsgerade* von $[\boldsymbol{p}]$ und $[\boldsymbol{q}]$.

Beweis. 1. Im Falle $r = 1$ gibt es ein $\lambda \in K^\times$ mit $(a_2, b_2, c_2) = (\lambda a_1, \lambda b_1, \lambda c_1)$, und daher ist $\Lambda_1 = \Lambda_2$.

Sei $r = 2$ und $\boldsymbol{p} = (p_1, p_2, p_3) \in (\overline{K}^3)^\bullet$. Genau dann ist $[\boldsymbol{p}] \in \Lambda_1 \cap \Lambda_2$, wenn $\boldsymbol{p}$ eine Lösung des linearen Gleichungssystems $a_ip_1 + b_ip_2 + c_ip_3 = 0$ für $i \in \{1, 2\}$ ist. Für jeden Körper K' mit $K \subset K' \subset \overline{K}$ ist die Lösungsmenge dieses linearen Gleichungssystems über K' ein 1-dimensionaler K'-Vektorraum. Ist nun $\boldsymbol{p}_0 \in (K^3)^\bullet$ eine Lösung des Gleichungssystems, so folgt $\Lambda_1 \cap \Lambda_2 = \{[\boldsymbol{p}] \in \mathbb{P}^2 \mid \boldsymbol{p} \in \overline{K}\boldsymbol{p}_0\} = [\boldsymbol{p}_0] \in \mathbb{P}^2(K)$.

2. Sei $\boldsymbol{p} = (p_1, p_2, p_3)$ und $\boldsymbol{q} = (q_1, q_2, q_3)$. Wegen $[\boldsymbol{p}] \neq [\boldsymbol{q}]$ ist

$$\operatorname{rg} \begin{pmatrix} p_1 & p_2 & p_3 \\ q_1 & q_2 & q_3 \end{pmatrix} = 2\,.$$

Für $(a,b,c) \in (K^3)^\bullet$ ist genau dann $\{[\boldsymbol{p}],[\boldsymbol{q}]\} \subset V_+(aX+bY+cZ)$, wenn (a,b,c) das lineare Gleichungssystem $ap_1+bp_2+cp_3 = aq_1+bq_2+cq_3 = 0$ erfüllt. Die Lösungsmenge dieses linearen Gleichungssystems über K ist ein 1-dimensionaler K-Vektorraum. Ist daher $(a,b,c) \in (K^3)^\bullet$ eine Lösung dieses linearen Gleichunssystems, so ist $\Lambda = V_+(aX+bY+cZ)$ ist die einzige projektive Gerade mit $\{[\boldsymbol{p}],[\boldsymbol{q}]\} \subset \Lambda$.

Ist $\boldsymbol{z} = (z_1,z_2,z_3) \in (\overline{K}^3)^\bullet$, so ist genau dann $[\boldsymbol{z}] \in \Lambda$, wenn $az_1+bz_2+cz_3 = 0$. Die Lösungsmenge W dieser homogenen Gleichung über $\overline{K}$ ist ein 2-dimensionaler $\overline{K}$-Vektorraum. Wegen $\{\boldsymbol{p},\boldsymbol{q}\} \subset W$ ist $W = \{s\boldsymbol{p}+t\boldsymbol{q} \mid (s,t) \in \overline{K}^2\}$ und daher $\Lambda = \{[s\boldsymbol{p}+t\boldsymbol{q}] \mid (s,t) \in (\overline{K}^2)^\bullet\}$.

Es bleibt zu zeigen: Sind (s,t), $(s',t') \in (\overline{K}^2)^\bullet$, so ist genau dann $[s\boldsymbol{p}+t\boldsymbol{q}] = [s'\boldsymbol{p}+t'\boldsymbol{q}]$, wenn $(s\!:\!t) = (s'\!:\!t')$. Ist $(s\!:\!t) = (s'\!:\!t')$, so gibt es eine $\lambda \in \overline{K}^\times$, so dass $s' = \lambda s$ und $t' = \lambda t$. Dann ist $s'\boldsymbol{p}+t'\boldsymbol{q} = \lambda(s\boldsymbol{p}+t\boldsymbol{q})$ und daher $[s\boldsymbol{p}+t\boldsymbol{q}] = [s'\boldsymbol{p}+t'\boldsymbol{q}]$. Ist umgekehrt $[s\boldsymbol{p}+t\boldsymbol{q}] = [s'\boldsymbol{p}+t'\boldsymbol{q}]$, so gibt es ein $\lambda \in \overline{K}^\times$, so dass $s'\boldsymbol{p}+t'\boldsymbol{q} = \lambda(s\boldsymbol{p}+t\boldsymbol{q})$. Aus der linearen Unabhängigkeit von $\boldsymbol{p}$ und $\boldsymbol{q}$ folgt $s' = \lambda s$ und $t' = \lambda t$, also $(s\!:\!t) = (s'\!:\!t')$. □

Beispiel 2.2.5.

1. Wir betrachten die projektive Ebene $\mathbb{P}^2 = \mathbb{P}^2(1) \cup \mathbb{P}^2(2) \cup \mathbb{P}^2(3)$ gemeinsam mit ihren drei affinen Stücken.

- $\mathbb{P}^2(1) = \{(1\!:\!y\!:\!z) \mid (y,z) \in \mathbb{A}^2\} = \mathbb{P}^2 \setminus V_+(X)$. Identifiziert man $\mathbb{P}^2(1)$ mit $\mathbb{A}^2$ vermöge $(1:y:z) = (y,z)$, so nennt man $\mathbb{A}^2$ die affine (y,z)-Ebene von $\mathbb{P}^2$ und $V_+(X)$ die *Ferngerade* der (y,z)-Ebene.

  Sei nun $\Lambda = V_+(aX+bY+cZ) \subset \mathbb{P}^2$ mit $(a,b,c) \in (\overline{K}^3)^\bullet$, und sei $\Lambda \neq V_+(X)$, also $(b,c) \neq (0,0)$. Dann ist

  $$L = \Lambda \cap \mathbb{P}^2(1) = \{(y,z) \in \mathbb{A}^2 \mid a+by+cz = 0\} = V(a+bY+cZ) \subset \mathbb{A}^2$$

  das erste affine Stück von Λ, und

  $$\Lambda \setminus L = \Lambda \cap V_+(X) = \{(0\!:\!y\!:\!z) \in \mathbb{P}^2 \mid by+cz = 0\} = \{(0\!:\!-c\!:\!b)\}\,.$$

  Man nennt den Punkt $(0:-c:b) \in V_+(X)$ den *Fernpunkt der Geraden L* bei der Einbettung $\mathbb{A}^2 = \mathbb{P}^2(1) \subset \mathbb{P}^2$.

  Ist umgekehrt $p \in V_+(X)$, so gibt es ein Paar $(b,c) \in (\overline{K}^2)^\bullet$ mit $p = (0\!:\!-c\!:\!b)$, und dann ist $\mathcal{B}(p) = \{V(\lambda+bY+cZ) \mid \lambda \in \overline{K}\}$ die Menge aller Geraden in $\mathbb{A}^2 = \mathbb{P}^2(1)$ mit Fernpunkt p. Man nennt $\mathcal{B}(p)$ die *durch den Fernpunkt p bestimmte Parallelenschar von* $\mathbb{A}^2 = \mathbb{P}^2(1)$. Die Zuordnung $p \mapsto \mathcal{B}(p)$ definiert eine Bijektion von der Menge $V_+(X)$ der Fernpunkte von $\mathbb{A}^2 = \mathbb{P}^2(1) \subset \mathbb{P}^2$ auf die Menge der Parallelenscharen von $\mathbb{A}^2 = \mathbb{P}^2(1)$.
- $\mathbb{P}^2(2) = \{(x\!:\!1\!:\!z) \mid (x,z) \in \mathbb{A}^2\} = \mathbb{P}^2 \setminus V_+(Y)$. Identifiziert man $\mathbb{P}^2(2)$ mit $\mathbb{A}^2$ vermöge $(x:1:z) = (x,z)$, so nennt man $\mathbb{A}^2$ die affine (x,z)-Ebene von $\mathbb{P}^2$ und $V_+(Y)$ die *Ferngerade* der (x,z)-Ebene.

  Sei nun $\Lambda = V_+(aX+bY+cZ) \subset \mathbb{P}^2$ mit $(a,b,c) \in (\overline{K}^3)^\bullet$, und sei $\Lambda \neq V_+(Y)$, also $(a,c) \neq (0,0)$. Dann ist

  $$L = \Lambda \cap \mathbb{P}^2(2) = \{(x,z) \in \mathbb{A}^2 \mid ax+b+cz = 0\} = V(aX+b+cZ) \subset \mathbb{A}^2$$

  das zweite affine Stück von Λ, und

  $$\Lambda \setminus L = \Lambda \cap V_+(Y) = \{(x\!:\!0\!:\!z) \in \mathbb{P}^2 \mid ax+cz = 0\} = \{(-c\!:\!0\!:\!a)\}\,.$$

  Man nennt den Punkt $(-c:0:a) \in V_+(Y)$ den *Fernpunkt der Geraden L* bei der Einbettung $\mathbb{A}^2 = \mathbb{P}^2(2) \subset \mathbb{P}^2$.

Ist umgekehrt $p \in V_+(Y)$, so gibt es ein Paar $(a,c) \in (\overline{K}^2)^\bullet$ mit $p = (-c:0:a)$, und dann ist $\mathcal{B}(p) = \{V(aX + \lambda + cZ) \mid \lambda \in \overline{K}\}$ die Menge aller Geraden in $\mathbb{A}^2 = \mathbb{P}^2(2)$ mit Fernpunkt p. Man nennt $\mathcal{B}(p)$ die *durch den Fernpunkt p bestimmte Parallelenschar von* $\mathbb{A}^2 = \mathbb{P}^2(2)$. Die Zuordnung $p \mapsto \mathcal{B}(p)$ definiert eine Bijektion von der Menge $V_+(X)$ der Fernpunkte von $\mathbb{A}^2 = \mathbb{P}^2(2) \subset \mathbb{P}^2$ auf die Menge der Parallelenscharen von $\mathbb{A}^2 = \mathbb{P}^2(2)$.

- $\mathbb{P}^2(3) = \{(x:y:1) \mid (x,y) \in \mathbb{A}^2\} = \mathbb{P}^2 \setminus V_+(Z)$. Identifiziert man $\mathbb{P}^2(3)$ mit $\mathbb{A}^2$ vermöge $(x:y:1) = (x,y)$, so nennt man $\mathbb{A}^2$ die affine (x,y)-Ebene von $\mathbb{P}^2$ und $V_+(Z)$ die *Ferngerade* der (x,y)-Ebene.

  Sei nun $\Lambda = V_+(aX + bY + cZ) \subset \mathbb{P}^2$ mit $(a,b,c) \in (\overline{K}^3)^\bullet$, und sei $\Lambda \neq V_+(Z)$, also $(a,b) \neq (0,0)$. Dann ist

  $$L = \Lambda \cap \mathbb{P}^2(3) = \{(x,y) \in \mathbb{A}^2 \mid ax + by + c = 0\} = V(aX + bY + c) \subset \mathbb{A}^2$$

  das dritte affine Stück von Λ, und

  $$\Lambda \setminus L = \Lambda \cap V_+(Z) = \{(x:y:0) \in \mathbb{P}^2 \mid ax + by = 0\} = \{(-b:a:0)\}\,.$$

  Man nennt den Punkt $(-b:a:0) \in V_+(Z)$ den *Fernpunkt der Geraden L* bei der Einbettung $\mathbb{A}^2 = \mathbb{P}^2(3) \subset \mathbb{P}^2$.

  Ist umgekehrt $p \in V_+(Z)$, so gibt es ein Paar $(a,b) \in (\overline{K}^2)^\bullet$ mit $p = (-b:a:0)$, und dann ist $\mathcal{B}(p) = \{V(aX + bY + \lambda) \mid \lambda \in \overline{K}\}$ die Menge aller Geraden in $\mathbb{A}^2 = \mathbb{P}^2(3)$ mit Fernpunkt p. Man nennt $\mathcal{B}(p)$ die *durch den Fernpunkt p bestimmte Parallelenschar von* $\mathbb{A}^2 = \mathbb{P}^2(3)$. Die Zuordnung $p \mapsto \mathcal{B}(p)$ definiert eine Bijektion von der Menge $V_+(X)$ der Fernpunkte von $\mathbb{A}^2 = \mathbb{P}^2(3) \subset \mathbb{P}^2$ auf die Menge der Parallelenscharen von $\mathbb{A}^2 = \mathbb{P}^2(3)$.

2. Sei $F = Y^2Z - X^3 \in K[X,Y,Z]$ und $\Gamma = V_+(F) \subset \mathbb{P}^2$. Für $i \in \{1,2,3\}$ nennt man $C_i = \Gamma \cap \mathbb{P}^2(i) \subset \mathbb{A}^2$ das i-te affine Stück von Γ. Die Punkte in $\Gamma \setminus C_i$ heißen Fernpunkte von C_i. Im Detail:

- $C_1 = \{(y,z) \in \mathbb{A}^2 \mid y^2z - 1 = 0\} = V(Y^2Z - 1) \subset \mathbb{A}^2$, und $\Gamma \setminus C_1 = \{(0:1:0),\ (0:0:1)\}$.
- $C_2 = \{(x,z) \in \mathbb{A}^2 \mid z - x^3 = 0\} = V(Z - X^3) \subset \mathbb{A}^2$, und $\Gamma \setminus C_2 = \{(0:0:1)\}$.
- $C_3 = \{(x,y) \in \mathbb{A}^2 \mid y^2 - x^3 = 0\} = V(Y^2 - X^3) \subset \mathbb{A}^2$, und $\Gamma \setminus C_3 = \{(0:1:0)\}$.

2.3. Projektiver Abschluss

Konvention. Im Folgenden identifizieren wir $\mathbb{A}^n$ mit dem affinen Stück $\mathbb{P}^n(n+1)$ vermöge ι_{n+1}. Dann ist $\mathbb{A}^n \subset \mathbb{P}^n$, $(x_1,\ldots,x_n) = (x_1:\ldots:x_n:1)$ für alle $(x_1,\ldots,x_n) \in \mathbb{A}^n$, und

$$\mathbb{P}^n = \mathbb{A}^n \cup \{(x_1:\ldots:x_n:0) \mid (x_1,\ldots,x_n) \in (\overline{K}^n)^\bullet\}.$$

Man nennt die Punkte von $\mathbb{A}^n$ die *endlichen Punkte* und die von $\mathbb{P}^n \setminus \mathbb{A}^n$ die *Fernpunkte* von $\mathbb{A}^n$. Insbesondere ist $\mathbb{P}^1 = \mathbb{A}^1 \cup \{(1:0\}$ und $\mathbb{P}^2 = \mathbb{A}^2 \cup H_\infty$ mit $H_\infty = \{(x:y:0) \mid (x,y) \in (\overline{K}^2)^\bullet\}$. Man nennt $(1:0)$ den *Fernpunkt* von $\mathbb{A}^1$ und H_∞ die *Ferngerade* von $\mathbb{A}^2$.

Definition 2.3.1.

1. Sei $f \in K[X,Y]$, $\operatorname{gr}(f) = d \in \mathbb{N}_0$ und $f = f_0 + f_1 + \ldots + f_d$ mit Formen f_i vom Grade i für alle $i \in [0,d]$ und $f_d \neq 0$. Dann heißt

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

die *Homogenisierung* von f.

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

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

1. *f^* ist eine Form, $\mathrm{gr}(f^*) = \mathrm{gr}(f)$, und $Z \nmid f^*$.*
2. *$c^* = c_* = c$, $(fg)^* = f^*g^*$, $(FG)_* = F_*G_*$, $(F+G)_* = F_* + G_*$, und $(f^*)_* = f$.*
3. *Ist $r \in [0, \mathrm{gr}(F)]$ maximal mit $Z^r \mid F$, so ist $\mathrm{gr}(F_*) = \mathrm{gr}(F) - r$, und $F = Z^r\,(F_*)^*$.*
4. *Sei $f = f_1^{e_1} \cdot \ldots \cdot f_r^{e_r}$ mit $r \in \mathbb{N}$, paarweise nicht-assoziierten irreduziblen Polynomen $f_1, \ldots, f_r \in K[X,Y]$ und $e_1, \ldots, e_r \in \mathbb{N}$. Dann ist $f^* = f_1^{*e_1} \cdot \ldots \cdot f_r^{*e_r}$, und $f_1^*, \ldots, f_r^*$ sind paarweise nicht-assoziierte irreduzible Formen in $K[X,Y,Z]$. Insbesondere ist f genau dann irreduzibel, wenn f^* irreduzibel ist.*
5. *Sei $Z \nmid F$ und $F = F_1^{e_1} \cdot \ldots \cdot F_r^{e_r}$ mit $r \in \mathbb{N}$, paarweise nicht-assoziierten irreduziblen Formen $F_1, \ldots, F_r \in K[X,Y,Z]$ und $e_1, \ldots, e_r \in \mathbb{N}$. Dann ist $F_* = F_{1*}^{e_1} \cdot \ldots \cdot F_{r*}^{e_r}$, und $F_{1*}, \ldots, F_{r*}$ sind paarweise nicht-assoziierte irreduzible Polynome in $K[X,Y]$. Insbesondere ist F genau dann irreduzibel, wenn F_* irreduzibel ist.*

Beweis. 1. und 2. Trivial.

3. Sei $F = Z^r G$ mit $r \in [0, \mathrm{gr}(F)]$, einer Form $G \in K[X,Y,Z]$, so dass $Z \nmid G$, und sei $d = \mathrm{gr}(G)$. Dann ist

$$G = \sum_{i=0}^{d} Z^{d-i} G_i(X,Y) \quad \text{mit Formen } G_i \in K[X,Y] \text{ vom Grade } i \text{ für alle } i \in [0,d] \text{ und } G_d \neq 0.$$

Es folgt

$$G_* = \sum_{i=0}^{d} G_i(X,Y), \quad \text{also } \mathrm{gr}(G_*) = d \text{ und } (G_*)^* = G.$$

Somit erhalten wir $F_* = G_*$, $\mathrm{gr}(F_*) = d = \mathrm{gr}(F) - r$ und $Z^r (F_*)^* = Z^r (G_*)^* = Z^r G = F$.

4. Nach 2. genügt es, zu zeigen: **1)** Ist $f \in K[X,Y] \setminus K$ irreduzibel, so ist auch f^* irreduzibel; **2)** Sind $f, g \in K[X,Y] \setminus K$, so ist genau dann $f \simeq g$, wenn $f^* \simeq g^*$.

1) Sei $f \in K[X,Y] \setminus K$ irreduzibel und $f^* = GH$ mit Formen $G, H \in K[X,Y,Z] \setminus K$. Wegen $Z \nmid f^*$ folgt $f = (f^*)_* = G_* H_*$, $\mathrm{gr}(G_*) = \mathrm{gr}(G) \geq 1$ und $\mathrm{gr}(H_*) = \mathrm{gr}(H) \geq 1$, im Widerspruch zur Irreduzibilität von f.

2) Für $c \in K^\times$ ist genau dann $f = cg$, wenn $f^* = cg^*$.

5. Nach 2. genügt es, zu zeigen: **1)** Ist $F \in K[X,Y,Z] \setminus K$ irreduzibel und $Z \nmid F$, so ist auch F_* irreduzibel; **2)** Sind $F, G \in K[X,Y,Z] \setminus K$, so ist genau dann $F \simeq G$, wenn $F_* \simeq G_*$.

1) Sei $F \in K[X,Y,Z] \setminus K$ irreduzibel, $Z \nmid F$ und $F_* = gh$ mit Polynomen $g, h \in K[X,Y] \setminus K$. Dann folgt $F = (F_*)^* = g^* h^*$, $\mathrm{gr}(g^*) = \mathrm{gr}(g) \geq 1$ und $\mathrm{gr}(h^*) = \mathrm{gr}(h) \geq 1$, im Widerspruch zur Irreduzibilität von F.

2) Für $c \in K^\times$ ist genau dann $F = cG$, wenn $F_* = cG_*$. □

Definition 2.3.3. Sei $C \subset \mathbb{A}^2$ eine über K definierte Kurve, $f \in K[X,Y]$ und $\mathfrak{I}_K(C) = (f)$. Dann heißt $\overline{C} = V_+(f^*) \subset \mathbb{P}^2$ der *projektive Abschluss* von C (diese Definition ist unabhängig von der Wahl von f). Die Punkte $p \in \overline{C} \setminus C$ heißen *Fernpunkte* von C.

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

Beweis. Sei $p = (\alpha,\beta) = (\alpha:\beta:1) \in \mathbb{A}^2$. Dann ist $f(p) = f(\alpha,\beta) = f^*(\alpha,\beta,1)$, also genau dann $p \in C$, wenn $p \in \overline{C}$. Damit folgt $C = \overline{C} \cap \mathbb{A}^2$.

Ist $p = (\alpha:\beta:0) \in \mathbb{P}^2 \setminus \mathbb{A}^2$ mit $(\alpha,\beta) \in (\overline{K}^2)^\bullet$, so ist genau $p \in \overline{C}$, wenn $f^*(\alpha,\beta,0) = 0$. Wegen $f^* = Z^d f_0 + Z^{d-1} f_1 + \ldots + Z f_{d-1} + f_d$ ist $f^*(\alpha,\beta,0) = f_d(\alpha,\beta)$, also

$$\begin{aligned}\overline{C} \setminus C &= \{(\alpha:\beta:0) \mid (\alpha,\beta) \in (\overline{K}^2)^\bullet,\ f_d(\alpha,\beta) \neq 0\} \\ &= \{(\alpha:1:0) \mid \alpha \in \overline{K},\ f_d(\alpha,1) = 0\} \cup \{(1:\beta:0) \mid \alpha \in \overline{K},\ f_d(1,\beta) = 0\}.\end{aligned}$$

$\overline{C} \setminus C$ ist endlich, denn aus

$$f_d = \sum_{i=0}^{d} c_i X^i Y^{d-i} \neq 0 \quad \text{folgt} \quad f_d(X,1) = \sum_{i=0}^{d} c_i X^i \neq 0 \quad \text{und} \quad f_d(1,Y) = \sum_{i=0}^{d} c_i Y^{d-i} \neq 0. \quad \square$$

Korollar 2.3.5.

1. *Sei $L = V(aX + bY + c) \subset \mathbb{A}^2$ eine Gerade mit $(a,b,c) \in \overline{K}^3$ und $(a,b) \neq (0,0)$. Dann ist $\overline{L} = V_+(aX + bY + cZ) \subset \mathbb{P}^2$ und $\overline{L} \setminus L = \{(b:-a:0)\}$.*
2. *Sei $\Lambda = V_+(aX + bY + cZ) \subset \mathbb{P}^2$ eine projektive Gerade mit $(a,b,c) \in \overline{(K^3)}^\bullet$. Genau dann ist $\Lambda \neq V_+(Z)$, wenn $(a,b) \neq (0,0)$, und dann ist $\Lambda \cap \mathbb{A}^2 = V(aX + bY + c)$.*

Beweis. Trivial. $\square$

Beispiel 2.3.6 (Kreislinie)**.** Sei $\mathrm{char}(K) \neq 2$ und $\mathsf{i} \in \overline{K}$ mit $\mathsf{i}^2 = -1$. Sei $\boldsymbol{m} = (u_0, v_0) \in \mathbb{A}^2$, $a \in K$, und

$$C_{\boldsymbol{m},a} = \{(u,v) \in \mathbb{A}^2 \mid (u-u_0)^2 + (v-v_0)^2 = a^2\} = V\big((X-u_0)^2 + (Y-v_0)^2 - a^2\big) \subset \mathbb{A}^2$$

die Kreislinie mit Radius a und Mittelpunkt $\boldsymbol{m}$. Dann ist

$$\overline{C}_{\boldsymbol{m},a} = V_+\big((X-u_0Z)^2 + (Y-v_0Z)^2 - a^2Z^2\big) \subset \mathbb{P}^2,$$

und

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

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

Spezialfall $C_1 = C_{\mathbf{0},1} = \{(u,v) \in \mathbb{A}^2 \mid u^2 + v^2 = 1\}$. Sei

$$\overline{\tau}\colon \mathbb{P}^1 \ \to\ \overline{C}_1 \ \text{ definiert durch } \ \tau(k:l) = (2lk : l^2 - k^2 : l^2 + k^2),$$

und sei $\tau = \overline{\tau} \,|\, \mathbb{A}^1$. Dann ist $\tau(k) = \overline{\tau}(k:1) = (2k : 1 - k^2 : 1 + k^2)$. Im Falle $k \neq \pm\mathsf{i}$ folgt

$$\tau(k) = \Big(\frac{2k}{1+k^2}, \frac{1-k^2}{1+k^2}\Big), \quad \text{und} \quad \tau \,|\, \mathbb{A}^1 \setminus \{\pm\mathsf{i}\}\colon \mathbb{A}^1 \setminus \{\pm\mathsf{i}\} \to C_1 \setminus \{(0,-1)\} \ \text{ ist bijektiv}$$

nach 1.1.3.2. Wegen $\tau(\mathsf{i}) = (2\mathsf{i} : 2 : 0) = (1 : -\mathsf{i} : 0)$, $\tau(-\mathsf{i}) = (-2\mathsf{i} : 2 : 0) = (1 : \mathsf{i} : 0)$ und $\tau(1:0) = (0:-1:1) = (0,-1)$ ist $\overline{\tau}$ bijektiv.

Definition 2.3.7. Sei $\Gamma \subset \mathbb{P}^2$ eine über K definierte projektive Kurve.

1. Γ 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.
2. Das von allen Formen $F \in K[X,Y,Z]$ mit $\Gamma \subset V_+(F)$ erzeugte Ideal $\mathfrak{I}_K^+(\Gamma) \lhd K[X,Y,Z]$ heißt *homogenes Verschwindungsideal*, der Restklassenring $K[\Gamma] = K[X,Y,Z]/\mathfrak{I}_K^+(\Gamma)$ heißt *homogener Koordinatenring*, und die Restklassen $\hat{x} = X + \mathfrak{I}_K^+(\Gamma)$, $\hat{y} = Y + \mathfrak{I}_K^+(\Gamma)$, $\hat{z} = Z + \mathfrak{I}_K^+(\Gamma)$ heißen *homogene Koordinaten* von Γ. Es ist $K[\Gamma] = K[\hat{x}, \hat{y}, \hat{z}]$. Die Elemente von $K[\Gamma]$ sind keine Funktionen. Sind $\Gamma, \Gamma_1 \subset \mathbb{P}^2$ projektive Kurven mit $\Gamma \subset \Gamma_1$, so ist $\mathfrak{I}_K^+(\Gamma_1) \subset \mathfrak{I}_K^+(\Gamma)$.

Satz und Definition 2.3.8.

1. *Sei $F \in K[X,Y,Z] \setminus K$ eine Form, $\Gamma = V_+(F) \subset \mathbb{P}^2$ und $C = \Gamma \cap \mathbb{A}^2$. Ist $\Gamma \neq V_+(Z)$, so ist $C = V(F_*) \subset \mathbb{A}^2$ eine Kurve, und im Falle $V_+(Z) \not\subset \Gamma$ ist $\overline{C} = \Gamma$.*
2. *Für jede projektive Kurve $\Gamma \subset \mathbb{P}^2$ ist $|\Gamma| = |\mathbb{P}^2 \setminus \Gamma| = \infty$.*
3. *Seien $F, G \in K[X,Y,Z] \setminus K$ teilerfremde Formen. Dann ist $|V_+(F) \cap V_+(G)| < \infty$.*
4. *Sei $F = F_1^{e_1} \cdot \ldots \cdot F_k^{e_k}$ mit $k \in \mathbb{N}$, paarweise nicht-assoziierten irreduziblen Formen $F_1, \ldots, F_k \in K[X,Y,Z]$, $e_1, \ldots, e_k \in \mathbb{N}$, $F_0 = F_1 \cdot \ldots \cdot F_k$ und $\Gamma = V_+(F) \subset \mathbb{P}^2$. Dann ist $F_0 \in K[X,Y,Z]$ eine reduzierte Form,*

$$\Gamma = V_+(F_0) = \bigcup_{i=1}^{k} V_+(F_i)\,,$$

$\mathfrak{I}_K^+(\Gamma) = (F_0) \lhd K[X,Y,Z]$, und im Falle $\Gamma \neq V_+(Z)$ ist $\mathfrak{I}_K(\Gamma \cap \mathbb{A}^2) = (F_{0*}) \lhd K[X,Y]$. Die Kurven $V_+(F_1), \ldots, V_+(F_k)$ heißen die Komponenten von Γ über K.

Beweis. 1. Sei $d = \mathrm{gr}(F)$. Ist $\Gamma \neq V_+(Z)$, so ist $F \neq Z^d$, $F_* = F(X,Y,1) \in K[X,Y] \setminus K$, und $C = \Gamma \cap \mathbb{A}^2 = \{(x,y) \in \mathbb{A}^2 \mid F(x,y,1) = 0\} = V(F_*) \subset \mathbb{A}^2$ ist eine Kurve. Sei nun $V_+(Z) \not\subset \Gamma$. Dann gibt es ein Paar $(\alpha, \beta) \in (\overline{K}^2)^\bullet$ mit $F(\alpha, \beta, 0) \neq 0$. Daher ist $Z \nmid F$, also $(F_*)^* = F$ und $\overline{C} = V_+((F_*)^*) = \Gamma$.

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

3. Da F und G teilerfremd sind, können wir $Z \nmid G$ annehmen. Dann ist $V_+(G) = \overline{V(G_*)}$, und $V_+(F) \cap V_+(G) = [V_+(F) \cap \mathbb{A}^2 \cap \overline{V(G_*)}\,] \cup [V_+(Z) \cap \overline{V(G_*)}\,]$. Nach Satz 2.3.4 ist $V_+(Z) \cap \overline{V(G_*)}$ endlich. Ist $V_+(F) = V_+(Z)$, so ist $V_+(F) \cap \mathbb{A}^2 = \emptyset$. Sei also $V_+(F) \neq V_+(Z)$. Dann folgt $V_+(F) \cap \mathbb{A}^2 \cap \overline{V(G_*)} = V(F_*) \cap V(G_*)$, und nach Satz 1.2.2 genügt es, die Teilerfremdheit von F_* und G_* zu zeigen. Sei $f \in K[X,Y]^\bullet$, $f \mid F_*$ und $f \mid G_*$. Dann folgt $f^* \mid (G_*)^* = G$ und $f^* \mid (F_*)^* \mid F$, also $f^* \in K$ und daher $f \in K$.

4. Offensichtlich ist $\Gamma = V_+(F) = V_+(F_0) = V_+(F_1) \cup \ldots \cup V_+(F_k)$, $F_0 \in \mathfrak{I}_K^+(\Gamma)$ und daher $(F_0) \subset \mathfrak{I}_K^+(\Gamma)$. Da $\mathfrak{I}_K^+(\Gamma))$ 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 (F_0) liegen. Sei also $G \in K[X,Y,Z] \setminus K$ eine Form mit $V_+(F) = V_+(F_0) \subset V_+(G)$, und sei $G \notin (F_0)$, also $F_0 \nmid G$. Sei F_0^* ein ggT von F_0 und G. Dann it $F_0^* \not\simeq F_0$, und daher gibt es eine Teilmenge $I \subsetneq [1,k]$ mit

$$F_0^* \simeq \prod_{i \in I} F_i.$$

Sei $i \in [1,k] \setminus I$. Dann ist $F_i \nmid F_0^*$, also $F_i \nmid G$ und daher $(F_i, G) = 1$. Nach 3. ist $V_+(F_i) \cap V_+(G)$ endlich, ein Widerspruch zu 2., da $V_+(F_i) \subset V_+(F) \subset V_+(G)$.

Im Falle $\Gamma \neq V_+(Z)$ ist $\Gamma \cap \mathbb{A}^2 = V(F_{0*})$, und da mit F_0 auch F_{0*} reduziert ist, folgt $\mathfrak{I}_K(\Gamma \cap \mathbb{A}^2) = (F_{0*})$. □

Korollar 2.3.9.

1. *Seien $F, G \in K[X,Y,Z] \setminus K$ reduzierte Formen. Genau dann ist $V_+(F) \subset V_+(G)$, wenn $(G) \subset (F)$ [oder $F \mid G$].*
2. *Sei $C \subset \mathbb{A}^2$ eine Kurve und $\Gamma \subset \mathbb{P}^2$ eine projektive Kurve mit $C \subset \Gamma$. Dann ist auch $\overline{C} \subset \Gamma$.*

Beweis. 1. Genau dann ist $(G) \subset (F)$, wenn $F \mid G$, und dann ist $V_+(F) \subset V_+(G)$. Ist umgekehrt $V_+(F) \subset V_+(G)$, so folgt $(F) = \mathfrak{I}_K^+(V_+(F)) \supset \mathfrak{I}_K^+(V_+(G)) = (G)$.

2. Sei $\mathfrak{I}_K(C) = (f)$ mit einem reduzierten Polynom $f \in K[X,Y]$ und $\mathfrak{I}_K^+(\Gamma) = (F)$ mit einer reduzierten Form $F \in K[X,Y,Z]$. Wegen $C \subset \Gamma \cap \mathbb{A}^2$ ist $(f) = \mathfrak{I}_K(C) \supset \mathfrak{I}_K(\Gamma \cap \mathbb{A}^2) = (F_*)$, also $f \mid F_*$ und daher $f^* \mid (F_*)^* \mid F$. Damit folgt $\Gamma = V_+(F) \supset V_+(f^*) = \overline{C}$. □

Satz 2.3.10. *Sei $\Gamma \subset \mathbb{P}^2$ 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) *$\mathfrak{I}_K^+(\Gamma)$ 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 $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_k$ in verschiedene über K definierte irreduzible projektive Kurven $\Gamma_1, \ldots, \Gamma_k$; diese sind die Komponenten von Γ über K. Ist $\Gamma \neq V_+(Z)$, so sind die Kurven $\Gamma_i \cap \mathbb{A}^2$ für $i \in [1,k]$ mit $\Gamma_i \neq V_+(Z)$ die Komponenten von $\Gamma \cap \mathbb{A}^2$ über K. Insbesondere ist Γ genau dann irreduzibel, wenn entweder $\Gamma = V_+(Z)$ oder $\Gamma \cap \mathbb{A}^2$ eine irreduzible Kurve ist.*
3. *Sei $C \subset \mathbb{A}^2$ eine Kurve. Sind $C_1, \ldots, C_k$ die Komponenten von C über K, so sind $\overline{C}_1, \ldots, \overline{C}_k$ die Komponenten von $\overline{C}$ über K. Insbesondere ist $\overline{C}$ genau dann irreduzibel über K, wenn C irreduzibel über K ist.*

Beweis. 1. (a) $\Rightarrow$ (b) Offensichtlich.

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

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

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

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

2. Sei $\mathfrak{I}_K^+(\Gamma) = (F)$ mit einer reduzierten Form $F \in K[X,Y,Z] \setminus K$, $F = F_1 \cdot \ldots \cdot F_k$ mit $k \in \mathbb{N}$ und paarweise nicht-assoziierten über K irreduziblen Formen $F_1, \ldots, F_k \in K[X,Y,Z]$, und für $i \in [1,k]$ sei $\Gamma_i = V_+(F_i)$. Dann sind $\Gamma_1, \ldots, \Gamma_k$ die Komponenten von Γ über K. Diese sind verschiedene über K definierte irreduzible projektive Kurven, und $\Gamma = \Gamma_1 \cup \ldots \cup \Gamma_k$. Sei $\Gamma = \Gamma_1' \cup \ldots \cup \Gamma_l'$ eine weitere Zerlegung von Γ in verschiedene über K definierte irreduzible projektive Kurven, und für $i \in [1,l]$ sei $\mathfrak{I}_K^+(\Gamma_i') = (F_i')$. Dann sind $F_1', \ldots, F_l' \in K[X,Y,Z]$ paarweise nicht-assoziierte irreduzible Formen, $F_1' \cdot \ldots \cdot F_l'$ ist reduziert und $\Gamma = V(F_1' \cdot \ldots \cdot F_l')$. Daher ist $\mathfrak{I}_K^+(\Gamma) = (F_1' \cdot \ldots \cdot F_l')$, es folgt $F_1' \cdot \ldots \cdot F_l' \simeq F \simeq F_1 \cdot \ldots \cdot F_k$. Wegen der Eindeutigkeit der Primzerlegung ist $l = k$, und es gibt eine Permutation $\pi \in \mathfrak{S}_k$, so dass $F_i' \simeq F_{\pi(i)}$ und daher $\Gamma_i' = \Gamma_{\pi(i)}$).

Sei nun $\Gamma \neq V_+(Z)$. Ist $V_+(Z) \in \{\Gamma_1, \ldots, \Gamma_k\}$, so sei $V_+(Z) = \Gamma_k$, $F_k = Z$ und $l = k-1$; andernfalls sei $l = k$. Dann ist $l \geq 1$, $\Gamma \cap \mathbb{A}^2 = V(F_*)$, $Z \nmid F_i$ und $\Gamma_i \cap \mathbb{A}^2 = V(F_{i*})$ für alle $i \in [1,l]$, und $F_* = F_{1*} \cdot \ldots \cdot F_{l*}$. Nach Lemma 2.3.2 sind $F_{1*}, \ldots, F_{l*} \in K[X,Y]$ paarweise nicht assoziierte irreduzible Polynome, und daher sind $\Gamma_1 \cap \mathbb{A}^2, \ldots, \Gamma_l \cap \mathbb{A}^2$ die Komponenten von $\Gamma \cap \mathbb{A}^2$ über K.

3. Für $i \in [1,k]$ sei $\mathfrak{I}_K(C_i) = (f_i)$, und $f = f_1 \cdot \ldots \cdot f_k$. Dann sind $f_1, \ldots, f_k \in K[X,Y]$ 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 $f^* = f_1^* \cdot \ldots \cdot f_k^*$, die Formen $f_1^*, \ldots, f_k^* \in K[X,Y,Z]$ sind paarweise nicht-assoziiert und irreduzibel, und $\overline{C} = V_+(f^*)$. Daher sind $\overline{C}_1, \ldots, \overline{C}_k$ die Komponenten von $\overline{C}$ über K. □

Satz 2.3.11 (Schwacher Satz von Bezout)**.** *Sind $\Gamma_1, \Gamma_2 \subset \mathbb{P}^2$ über K definierte projektive Kurven, so ist $\Gamma_1 \cap \Gamma_2 \neq \emptyset$.*

Beweis. Jenseits unserer Möglichkeiten. □

2.4. Vielfachheiten und Tangenten

Definitionen und Bemerkungen 2.4.1. Sei $\Gamma \subset \mathbb{P}^2$ eine über K definierte projektive Kurve, $\mathfrak{I}_K^+(\Gamma) = (F)$ mit einem homogenen Polynom $F \in K[X,Y,Z]$ vom Grade d, $\Lambda \subset \mathbb{P}^2$ eine projektive Gerade, $\Lambda \not\subset \Gamma$, $p = [\boldsymbol{p}] \in \Gamma \cap \Lambda$ und $q = [\boldsymbol{q}] \in \Lambda \setminus \{p\}$ (mit $\boldsymbol{p}$, $\boldsymbol{q} \in (\overline{K}^3)^\bullet$). Dann ist $F(\boldsymbol{p} + T\boldsymbol{q}) \in \overline{K}[T]$ ein Polynom, $\operatorname{gr}(F(\boldsymbol{p} + T\boldsymbol{q})) \leq d$, wegen $\Lambda \not\subset \Gamma$ ist $F(\boldsymbol{p} + T\boldsymbol{q}) \neq 0$, und wegen $F(\boldsymbol{p}) = 0$ ist $F(\boldsymbol{p} + T\boldsymbol{q}) = T^k \Phi(T)$ mit $k \in [1,d]$, $\Phi \in \overline{K}[T]$ und $\Phi(0) \neq 0$. Dabei hängt k nur von Γ, Λ und p ab.

Beweis. Sei $p = [\boldsymbol{p}_1]$ und $q_1 = [\boldsymbol{q}_1] \in \Lambda \setminus \{p\}$ mit $\boldsymbol{p}_1$, $\boldsymbol{q}_1 \in (\overline{K}^3)^\bullet$. Dann ist $\boldsymbol{p}_1 = \lambda \boldsymbol{p}$ und $\boldsymbol{q}_1 = s\boldsymbol{p} + t\boldsymbol{q}$ mit $\lambda, t \in \overline{K}^\times$ und $s \in \overline{K}$. Damit folgt

$$F(\boldsymbol{p}_1 + T\boldsymbol{q}_1) = F((\lambda + sT)\boldsymbol{p} + Tt\boldsymbol{q}) = (\lambda + sT)^d F\Big(\boldsymbol{p} + \frac{Tt}{\lambda + sT}\,\boldsymbol{q}\Big)$$
$$= (\lambda + sT)^d \Big(\frac{Tt}{\lambda + sT}\Big)^k \Phi\Big(\frac{Tt}{\lambda + sT}\Big) = T^k \Phi_1(T) \text{ mit } \Phi_1 \in \overline{K}[T],\ \Phi_1(0) \neq 0. \quad \square$$

Man nennt $k = \mu_p(\Gamma, \Lambda)$ die *Schnittmultiplizität* von Γ mit Λ in p.

Satz 2.4.2. *Sei $\Gamma \subset \mathbb{P}^2$ eine projektive Kurve, $\mathfrak{I}_K^+(\Gamma) = (F)$ mit einem homogenen Polynom $F \in K[X,Y,Z]$ vom Grade d, $\Lambda \subset \mathbb{P}^2$ eine projektive Gerade, $\Lambda \not\subset \Gamma$ und $\boldsymbol{p}, \boldsymbol{q} \in (\overline{K}^3)^\bullet$ mit $[\boldsymbol{p}], [\boldsymbol{q}] \in \Lambda$ und $[\boldsymbol{p}] \neq [\boldsymbol{q}]$). Dann ist $F(S\boldsymbol{p}+T\boldsymbol{q}) \in \overline{K}[S,T]$ ein homogenes Polynom vom Grade d, und es gibt Paare $(\alpha_1,\beta_1),\ldots,(\alpha_d,\beta_d) \in (K^2)^\bullet$, so dass*

$$F(S\boldsymbol{p}+T\boldsymbol{q}) = \prod_{i=1}^{d}(\alpha_i S + \beta_i T).$$

Die Zuordnung $(s,t) \mapsto s\boldsymbol{p}+t\boldsymbol{q}$ für alle $(s,t) \in (\overline{K}^2)^\bullet$ induziert eine bijektive Abbildung

$$\Phi\colon \Big\{(s\!:\!t) \in \mathbb{P}^1_K \;\Big|\; \prod_{i=1}^{d}(s\alpha_i + t\beta_i) = 0\Big\} \;\to\; \Lambda \cap \Gamma, \quad \textit{definiert durch} \;\; \Phi(s\!:\!t) = [s\boldsymbol{p}+t\boldsymbol{q}].$$

Ist $p \in \Lambda \cap \Gamma$ und $|\Phi^{-1}(p)| = (s\!:\!t) \in \mathbb{P}^1$, so ist $\mu_p(\Gamma,\Lambda)$ die Anzahl der Indizes $i \in [1,d]$ mit $s\alpha_i + t\beta_i = 0$. Insbesondere folgt

$$\sum_{p \in \Lambda\cap\Gamma} \mu_p(\Gamma,\Lambda) = d.$$

Beweis. Nach Lemma 2.1.4, Satz 2.1.3 und wegen $\Lambda \not\subset \Gamma$ ist $F(S\boldsymbol{p}+T\boldsymbol{q}) \in \overline{K}[S,T]$ eine Form vom Grade d der behaupteten Gestalt. Sind (s,t), $(s',t') \in (\overline{K}^2)^\bullet$ mit $(s\!:\!t) = (s'\!:\!t')$, so folgt $[s'\boldsymbol{p}+t'\boldsymbol{q}] = [s\boldsymbol{p}+t\boldsymbol{q}]$, und für $i \in [1,d]$ ist genau dann $s\alpha_i + t\beta_i = 0$, wenn $s'\alpha_i + t'\beta_i = 0$. Für alle $(s,t) \in (\overline{K}^2)^\bullet$ ist

$$F(s\boldsymbol{p}+t\boldsymbol{q}) = \prod_{i=1}^{d}(s\alpha_i + t\beta_i),$$

und $\Lambda \cap \Gamma = \{[s\boldsymbol{p}+t\boldsymbol{q}] \mid (s,t) \in (\overline{K}^2)^\bullet\}$. Damit folgt, dass die Zuordnung $(s,t) \mapsto s\boldsymbol{p}+t\boldsymbol{q}$ eine surjektive Abbildung Φ wie in der Behauptung des Satzes induziert. Zum Nachweis der Injektivität seien (s,t), $(s',t') \in (\overline{K}^2)^\bullet$ mit $[s\boldsymbol{p}+t\boldsymbol{q}] = [s'\boldsymbol{p}+t'\boldsymbol{q}]$. Dann gibt es ein $\lambda \in \overline{K}^\times$ mit $s'\boldsymbol{p}+t'\boldsymbol{q} = \lambda s\boldsymbol{p} + \lambda t\boldsymbol{q}$, und aus der linearen Unabhängigkeit von $\boldsymbol{p}$ und $\boldsymbol{q}$ folgt $(s',t') = (\lambda s, \lambda t)$, also $(s'\!:\!t') = (s\!:\!t)$.

Sei nun $p \in \Gamma \cap \Lambda$, $\Phi^{-1}(p) = (s\!:\!t) \in \mathbb{P}^1$ und $\{i \in [1,d] \mid s\alpha_i + t\beta_i = 0\} = [1,k]$ mit $k \in \mathbb{N}$. Wir müssen nun $\mu_p(\Gamma,\Lambda) = k$ zeigen. Nach Definition ist $p = [s\boldsymbol{p}+t\boldsymbol{q}]$, und es sei $\boldsymbol{q}_1 \in (\overline{K}^2)^\bullet$ mit $[\boldsymbol{q}_1] \in \Lambda \setminus \{p\}$. Dann ist $\boldsymbol{q}_1 = s_1\boldsymbol{p} + t_1\boldsymbol{q}$ mit $(s_1,t_1) \in (\overline{K}^2)^\bullet$, $(s\!:\!t) \neq (s_1\!:\!t_1)$, und es folgt

$$\begin{aligned} F(\boldsymbol{p}_1 + T\boldsymbol{q}_1) &= F\big((s+Ts_1)\boldsymbol{p} + (t+Tt_1)\boldsymbol{q}\big) = \prod_{i=1}^{d}\big(\alpha_i(s+Ts_1) + \beta_i(t+Tt_1)\big) \\ &= \prod_{i=1}^{d}[(\alpha_i s + \beta_i t) + T(\alpha_i s_1 + \beta_i t_1)] \\ &= T^k \prod_{i=1}^{k}(\alpha_i s_1 + \beta_i t_1) \prod_{i=k+1}^{d}[(\alpha_i s + \beta_i t) + T(\alpha_i s_1 + \beta_i t_1)] = T^k G(T) \end{aligned}$$

mit einem Polynom $G \in \overline{K}[T]$, so dass

$$G(0) = \prod_{i=1}^{k}(\alpha_i s_1 + \beta_i t_1) \prod_{i=k+1}^{d}(\alpha_i s + \beta_i t),$$

und wir zeigen $G(0) \neq 0$. Für $i \in [k+1, d]$ ist $\alpha_i s + \beta_i t) \neq 0$ nach Definition. Wäre $i \in [1, k]$ und $\alpha_i s_1 + \beta_i t_1 = 0$, so folgte $\Phi(s_1 : t_1) = [s_1 \boldsymbol{p} + t_1 \boldsymbol{q}] = [\boldsymbol{q}_1] = p$, ein Widerspruch. □

Definition 2.4.3.

1. Sei $\Gamma \subset \mathbb{P}^2$ eine über K definierte projektive Kurve und $p \in \Gamma$. Dann nennt man $\operatorname{ord}_p(\Gamma) = \min\{\mu_p(\Gamma, \Lambda) \mid \Lambda \subset \mathbb{P}^2$ projektive Gerade mit $p \in \Lambda\}$ die *Ordnung* von p auf Γ. Ist $\operatorname{ord}_p(\Gamma) = 1$, so heißt p *einfach* oder *regulär* oder *glatt* und andernfalls *singulär*. Die projektive Kurve Γ heißt *glatt*, wenn alle Punkte von Γ glatt sind. Eine projektive Gerade $\Lambda \subset \mathbb{P}^2$ heißt *Tangente* in p an Γ, wenn $p \in \Lambda$ und $\mu_p(\Gamma, \Lambda) > \operatorname{ord}_p(\Gamma)$.
2. Sei $C \subset \mathbb{A}^2$ eine über K definierte Kurve, $L \subset \mathbb{A}^2$, $\Gamma = \overline{C} \subset \mathbb{P}^2$, $\Lambda = \overline{L} \subset \mathbb{P}^2$ und $p \in C \cap L$. Dann nennt man $\mu_p(C, L) = \mu_p(\Gamma, \Lambda)$ die *Schnittmultiplizität* von C mit L in p und $\operatorname{ord}_{\boldsymbol{p}}(C) = \operatorname{ord}_p(\Gamma)$ die *Ordnung* von $\boldsymbol{p}$ auf C. Offensichtlich ist $\operatorname{ord}_p(C) = \min\{\mu_p(C, L) \mid L \subset \mathbb{A}^2$ Gerade mit $p \in L\}$. Ist $\operatorname{ord}_p(C) = 1$, so heißt p *einfach* oder *regulär* oder *glatt* und anderfalls *singulär*. Die Kurve C heißt *glatt*, wenn alle Punkte von C glatt sind. Eine Gerade $L \subset \mathbb{A}^2$ heißt *Tangente* in p an C, wenn $p \in L$ und $\mu_p(C, L) > \operatorname{ord}_p(C)$. Genau dann ist L eine Tangente in p an C, wenn $\overline{L}$ eine Tangente in p an $\overline{C}$ in p ist.

Satz 2.4.4. *Sei $\Gamma \subset \mathbb{P}^2$ eine über K definierte projektive Kurve, $\Gamma \neq V_+(Z)$, $\mathfrak{I}_K^+(\Gamma) = (F)$ mit einer Form $F \in K[X, Y, Z]$, und $f = F_* \in K[X, Y]$. Sei $C = \Gamma \cap \mathbb{A}^2$, also $\mathfrak{I}_K(C) = (f)$, $p = (\alpha, \beta) = (\alpha : \beta : 1) \in C$ und $m = \operatorname{ord}_p(C) = \operatorname{ord}_p(\Gamma)$.*

1. *Sei $\Lambda \subset \mathbb{P}^2$ eine projektive Gerade, $\Lambda \not\subset \Gamma$, $p \in \Lambda$, $k = \mu_p(\Gamma, \Lambda)$ und $\Lambda \cap \mathbb{A}^2 = p + \overline{K}u$ mit $u \in (\overline{K}^2)^\bullet$. Dann ist $f(p + Tu) = T^k \varphi(T)$ mit einem Polynom $\varphi \in \overline{K}[T]$, so dass $\varphi(0) \neq 0$.*
2. *Es ist $\operatorname{ord}_p(f) = m$, und*

$$f = \prod_{j=1}^{m} \big(a_j(X - \alpha) + b_j(Y - \beta)\big) + \overline{f}$$

mit $(a_1, b_1), \ldots, (a_m, b_m) \in (\overline{K}^2)^\bullet$ und $\overline{f} \in \overline{K}[X, Y]$, so dass $\operatorname{ord}_p(\overline{f}) > m$. Für $j \in [1, m]$ sei $L_j = V(a_j(X - \alpha) + b_j(Y - \beta))$ und $\Lambda_j = \overline{L}_j \subset \mathbb{P}^2$. Dann ist $\mu_p(\Gamma, \Lambda_j) > m$ für alle $j \in [1, m]$, und $\mu_p(\Gamma, \Lambda) = m$ für alle projektiven Geraden $\Lambda \subset \mathbb{P}^2$ mit $\Lambda \notin \{\Lambda_1, \ldots, \Lambda_m\}$. Insbesondere sind die projektiven Geraden $\Lambda_1, \ldots, \Lambda_m$ genau die Tangenten an Γ in p.
3. *Für $r \in \mathbb{N}$ ist genau dann*

$$\frac{\partial^{i+j+k} F}{\partial X^i \partial Y^j \partial Z^k}(\alpha, \beta, 1) = 0 \quad \text{für alle} \quad i, j, k \in \mathbb{N}_0 \quad \text{mit} \quad i + j + k < r,$$

wenn

$$\frac{\partial^{i+j} f}{\partial X^i \partial Y^j}(\alpha, \beta) = 0 \quad \text{für alle} \quad i, j \in \mathbb{N}_0 \quad \text{mit} \quad i + j < r.$$

Ist $r \in \mathbb{N}$ und $\operatorname{char}(K) \nmid r!$, so gibt es ein größtes $r \in \mathbb{N}$, so dass diese Bedingungen erfüllt sind, und für dieses ist $r = \operatorname{ord}_p(C)$.

4. *Genau dann ist p ein regulärer Punkt von Γ (bzw. C), wenn*

$$\Big(\frac{\partial F}{\partial X}(p), \frac{\partial F}{\partial Y}(p), \frac{\partial F}{\partial Z}(p)\Big) \neq (0,0,0) \quad \Big[\ \textit{äquivalent:} \quad \Big(\frac{\partial f}{\partial X}(\alpha,\beta), \frac{\partial f}{\partial Y}(\alpha,\beta)\Big) \neq (0,0)\ \Big].$$

In diesem Falle besitzt Γ genau eine Tangente in p, nämlich

$$\Lambda = V_+\Big(\frac{\partial F}{\partial X}(p)X + \frac{\partial F}{\partial Y}(p)Y + \frac{\partial F}{\partial Z}(p)Z\Big),$$

und es ist

$$\Lambda \cap \mathbb{A}^2 = V\Big(\frac{\partial f}{\partial X}(\alpha,\beta)(X-\alpha) + \frac{\partial f}{\partial Y}(\alpha,\beta)(Y-\beta)\Big)$$

BEWEIS. 1. Sei $d = \mathrm{gr}(F)$, $u = (\gamma,\delta) \in (\overline{K}^2)^\bullet$, $\boldsymbol{p} = (\alpha,\beta,1)$ und $\boldsymbol{q} = (\alpha+\gamma, \beta+\delta, 1)$. Dann ist $p = [\boldsymbol{p}]$ und $[\boldsymbol{q}] \in \Lambda \setminus \{p\}$. Nach Definition ist $f(p+Tu) \in \overline{K}[T]$, wegen $\Lambda \not\subset \Gamma$ ist $p + \overline{K}u \not\subset C = V(f)$, und wegen $f(p) = 0$ ist $f(p+Tu) = T^l\varphi(T)$ mit $l \in \mathbb{N}$, $\varphi \in \overline{K}[T]$, $\varphi(0) \neq 0$. Wir müssen $l = k$ zeigen.

Nach Definition von k ist $F(\boldsymbol{p} + T\boldsymbol{q}) = T^k\Phi(T)$ mit $\Phi \in \overline{K}[T]$ und $\Phi(0) \neq 0$. Nun folgt

$$\begin{aligned} T^k\Phi(T) &= F(\alpha + T(\alpha+\gamma), \beta + T(\beta+\delta), 1+T) = (1+T)^d F\Big(\alpha + \frac{T}{1+T}\,\gamma, \beta + \frac{T}{1+T}\,\delta, 1\Big) \\ &= (1+T)^d f\Big(p + \frac{T}{1+T}\,u\Big) = (1+T)^d\Big(\frac{T}{1+T}\Big)^l \varphi\Big(\frac{T}{1+T}\Big) = T^l(1+T)^{d-l}\varphi\Big(\frac{T}{1+T}\Big), \end{aligned}$$

also $k = l$.

2. Sei $\mathrm{ord}_p(f) = n \in \mathbb{N}$. Dann folgt $f = f_1(X-\alpha, Y-\beta) + \overline{f}$ mit einer Form $f_1 \in K[X,Y]^\bullet$ vom Grade n und $\overline{f} \in K[X,Y]$ mit $\mathrm{ord}_p(\overline{f}) > n$. Nach Lemma 2.1.4 ist

$$f_1 = \prod_{j=1}^{n}\big(a_j(X-\alpha) + b_j(Y-\beta)\big)$$

mit $(a_1,b_1), \ldots, (a_n,b_n) \in (\overline{K}^2)^\bullet$. Nach Definition ist

$$L_j = V\big(a_j(X-\alpha) + b_j(Y-\beta)\big) = p + \overline{K}u_j \quad \text{mit} \quad u_j = (-b_j, a_j).$$

Sei nun $\Lambda \subset \mathbb{P}^2$ eine projektive Gerade mit $p \in \Lambda$ und $\Lambda \cap \mathbb{A}^n = p + \overline{K}u$ mit $u = (\gamma,\delta) \in (\overline{K}^2)^\bullet$. Wegen $\mathrm{ord}_p(\overline{f}) > n$ ist $\overline{f}(p+Tu) = T^{n+1}\psi_u(T)$ mit $\psi_u \in \overline{K}[T]$, und mit 1. folgt

$$\begin{aligned} f(p+Tu) = f(\alpha+T\gamma, \beta+T\delta) &= \prod_{j=1}^{n}(a_jT\gamma + b_jT\delta) + \overline{f}(p+Tu) \\ &= T^n\prod_{j=1}^{n}(a_j\gamma + b_j\delta) + T^{n+1}\psi_u(T) = T^{\mu_p(\Gamma,\Lambda)}\varphi(T) \ \text{ mit } \ \varphi \in \overline{K}[T],\ \varphi(0) \neq 0. \end{aligned}$$

Daher ist $\mu_p(\Gamma,\Lambda) \geq n$, und genau dann ist $\mu_p(\Gamma,\Lambda) = n$, wenn es ein $j \in [1,n]$ gibt mit $a_j\gamma + b_j\delta = 0$. Für $j \in [1,n]$ ist genau dann $a_j\gamma + b_j\delta = 0$, wenn $(\gamma,\delta) = (-\lambda b_j, \lambda a_j)$ mit einem $\lambda \in \overline{K}^\times$, wenn also $\Lambda \cap \mathbb{A}^2 = L_j$ und daher $\Lambda = \Lambda_j$ ist.

Insbesondere folgt $n = \min\{\mu_p(\Gamma,\Lambda) \mid \Gamma \subset \mathbb{P}^2 \text{ projektive Gerade mit } p \in \Lambda\} = m$, und $\Lambda_1, \ldots, \Lambda_m$ sind die Tangenten an Λ in p.

3. Sei $r \in \mathbb{N}$ und zuerst

$$\frac{\partial^{i+j+k}F}{\partial X^i \partial Y^j \partial Z^k}(\alpha,\beta,1) = 0 \ \text{ für alle } \ i,\, j,\, k \in \mathbb{N}_0 \ \text{ mit } \ i+j+k < r.$$

Für alle $i,\, j \in \mathbb{N}_0$ mit $i+j<r$ ist dann auch

$$\frac{\partial^{i+j} f}{\partial X^i \partial Y^j}\,(\alpha,\beta) = \frac{\partial^{i+j+0} F}{\partial X^i \partial Y^j \partial Z^0}(\alpha,\beta,1) = 0.$$

Die Umkehrung beweisen wir durch Widerspruch. Sei

$$\frac{\partial^{i+j} f}{\partial X^i \partial Y^j}\,(\alpha,\beta) = 0 \;\text{ für alle }\; i,\, j \in \mathbb{N}_0 \;\text{ mit }\; i+j<r,$$

und sei $k \in [0, r-1]$ minimal,so dass es $i,\, j \in \mathbb{N}_0$ mit $i+j+k<r$ gibt mit

$$\frac{\partial^{i+j+k} F}{\partial X^i \partial Y^j \partial Z^k}\,(\alpha,\beta,1) \neq 0.$$

Dann ist $k \geq 1$, und

$$G = \frac{\partial^{i+j+k-1} F}{\partial X^i \partial Y^j \partial Z^{k-1}} \;\text{ ist eine Form vom Grade }\; d-i-j-k+1.$$

Es folgt

$$\begin{aligned} 0 &= (d-i-j-k+1)G(\alpha,\beta,1) = \alpha\frac{\partial G}{\partial X}(\alpha,\beta,1) + \beta\frac{\partial G}{\partial y}(\alpha,\beta,1) + \frac{\partial G}{\partial Z}(\alpha,\beta,1) \\ &= \alpha\,\frac{\partial^{i+j+k} F}{\partial X^{i+1}\partial Y^j \partial Z^{k-1}}(\alpha,\beta,1) + \beta\,\frac{\partial^{i+j+k} F}{\partial X^i \partial Y^{j+1} \partial Z^{k-1}}(\alpha,\beta,1) + \frac{\partial^{i+j+k} F}{\partial X^i \partial Y^j \partial Z^k}(\alpha,\beta,1) \\ &= \frac{\partial^{i+j+k} F}{\partial X^i \partial Y^j \partial Z^k}(\alpha,\beta,1), \quad \text{ein Widerspruch.} \end{aligned}$$

Nach Satz 0.1.1 ist

$$f = \sum_{i,j\geq 0} f_{i,j}(p)(X-\alpha)^i (Y-\beta)^j$$

mit modifizierten höheren partiellen Ableitungen $f_{i,j}$, es ist

$$\frac{\partial^{i+j} f}{\partial X^i \partial Y^j} = i!\, j!\, f_{i,j} \;\text{ für alle }\; i,\, j \geq 0,$$

und wegen $f(p)=0$ ist $\operatorname{ord}_p(f) = \operatorname{ord}_p(C) = \min\{i+j \mid i,\, j \in \mathbb{N}_0,\; f_{i,j}(p) \neq 0\} \in \mathbb{N}$.

Ist $r = \operatorname{ord}_p(C)$ und $\operatorname{char}(K) \nmid r!$, so gibt es Indizes $i_1,\, j_1 \geq 0$ mit $i_1 + j_1 = r$,

$$\frac{\partial^{i_1+j_1} f}{\partial X^{i_1} \partial Y^{j_1}}(p) \neq 0 \;\text{ und }\; \frac{\partial^{i+j} f}{\partial X^i \partial Y^j}(p) = 0 \;\text{ für alle }\; i,\, j \geq 0 \;\text{ mit }\; i+j<r.$$

Ist umgekehrt $r \in \mathbb{N}$ maximal, so dass

$$\frac{\partial^{i+j} f}{\partial X^i \partial Y^j}(p) = 0 \;\text{ für alle }\; i,\, j \geq 0 \;\text{ mit }\; i+j<r,$$

so gibt es Indizes $i,\, j \geq 0$ mit $i+j=r$ und $f_{i,j}(p) \neq 0$. Ist außerdem $\operatorname{char}(K) \nmid r!$, so folgt $f_{i,j}(p) = 0$ für alle $i,\, j \geq 0$ mit $i+j<r$, und daher ist $\operatorname{ord}_p(C) = r$.

4. Genau dann ist p ein regulärer Punkt von Γ, wenn $\operatorname{ord}_p(\Gamma) = 1$, nach 3. ist das äquivalent mit den angegebenen Bedingungen. Dann besitzt Γ genau eine Tangente in $p = (\alpha,\beta) = (\alpha:\beta:1)$, nämlich $\Lambda = \overline{L}$ mit

$$L = V\Big(\frac{\partial f}{\partial X}(p)(X-\alpha) + \frac{\partial f}{\partial Y}(p)(Y-\beta)\Big), \;\text{ also }\; \Lambda = V_+\Big(\frac{\partial f}{\partial X}(p)(X-\alpha Z) + \frac{\partial f}{\partial Y}(p)(Y-\beta Z)\Big).$$

Nun ist aber

$$\frac{\partial f}{\partial X}(p)(X-\alpha Z)+\frac{\partial f}{\partial Y}(p)(Y-\beta Z)=\frac{\partial F}{\partial X}(p)X+\frac{\partial F}{\partial Y}(p)Y-\Big[\alpha\frac{\partial F}{\partial X}(p)+\beta\frac{\partial F}{\partial Y}(p)\Big]$$

und

$$\alpha\frac{\partial F}{\partial X}(p)+\beta\frac{\partial F}{\partial Y}(p)=\Big(X\frac{\partial F}{\partial X}+Y\frac{\partial F}{\partial Y}\Big)(\alpha,\beta,1)=\Big(dF-Z\frac{\partial F}{\partial Z}\Big)(\alpha,\beta-1)=-\frac{\partial F}{\partial Z}(p),$$

also

$$\frac{\partial f}{\partial X}(p)(X-\alpha Z)+\frac{\partial f}{\partial Y}(p)(Y-\beta Z)=\frac{\partial F}{\partial X}(p)X+\frac{\partial F}{\partial Y}(p)Y+\frac{\partial F}{\partial Z}(p)Z. \qquad \square$$

Satz 2.4.5. *Sei $\Gamma\subset\mathbb{P}^2$ eine über K definierte projektive Kurve, $p\in\Gamma$ und $\mathfrak{I}_K^+(\Gamma)=(F)$ mit einer absolut reduzierten Form $F\in K[X,Y,Z]$. Genau dann ist p ein regulärer Punkt von Γ, wenn p in genau einer Komponente von Γ über $\overline{K}$ liegt und ein regulärer Punkt dieser Komponente über $\overline{K}$ ist. Insbesondere besitzt Γ nur endlich viele singuläre Punkte.*

Beweis. Sei $p=[\boldsymbol{p}]$ mit $\boldsymbol{p}\in(\overline{K}^3)^\bullet$, $(X,Y,Z)=(X_1,X_2,X_3)$ und $F=F_1\cdot\ldots\cdot F_k$ mit $k\in\mathbb{N}$ und paarweise nicht assoziierten über $\overline{K}$ irreduziblen Formen $F_1,\ldots,F_k\in\overline{K}[X_1,X_2,X_3]$. Dann sind $V_+(F_1),\ldots,V_+(F_k)$ die Komponenten von Γ über $\overline{K}$. Für $\nu\in[1,3]$ ist

$$\frac{\partial F}{\partial X_\nu}(\boldsymbol{p})=\sum_{i=1}^{k}\frac{\partial F_i}{\partial X_\nu}(\boldsymbol{p})\prod_{\substack{j=1\\ j\neq i}}^{r}F_j(\boldsymbol{p}).$$

Liegt p in zwei verschiedenen Komponenten von Γ über $\overline{K}$, so gibt es $i,\,j\in[1,k]$ mit $i\neq j$ und $F_i(\boldsymbol{p})=F_j(\boldsymbol{p})=0$. Damit folgt

$$\frac{\partial F}{\partial X_\nu}(\boldsymbol{p})=0\ \text{ für alle }\ \nu\in[1,3],$$

und daher ist p nicht regulär. Liegt p in genau einer Komponente von Γ über $\overline{K}$, etwa in $V_+(F_i)$, so folgt für alle $\nu\in[1,3]$

$$\frac{\partial F}{\partial X_\nu}(\boldsymbol{p})=\lambda\,\frac{\partial F_i}{\partial X_\nu}(\boldsymbol{p})\quad\text{mit}\quad\lambda=\prod_{\substack{j=1\\ j\neq i}}^{n}F_j(\boldsymbol{p})\neq 0.$$

Daher ist p genau dann ein regulärer Punkt von Γ, wenn p ein regulärer Punkt von $V_+(F_i)$ ist.

Für die Menge S der singulären Punkte von Γ gilt

$$S\subset\bigcup_{\substack{i,j=1\\ i\neq j}}^{k}V_+(F_i)\cap V_+(F_j)\ \cup\ \bigcup_{i=1}^{k}V_+(F_i)\cap V_+\Big(\frac{\partial F_i}{\partial X_1}\Big)\cap V_+\Big(\frac{\partial F_i}{\partial X_2}\Big)\cap V_+\Big(\frac{\partial F_i}{\partial X_3}\Big)$$

Ist $i\in[1,k]$, so ist F_i irreduzibel über $\overline{K}$, also

$$\frac{\partial F_i}{\partial X_\nu}\neq 0\ \text{ und daher }\ \Big(F_i,\frac{\partial F_i}{\partial X_\nu}\Big)=1\ \text{ für ein }\ \nu\in[1,3]$$

Die Endlichkeit von S folgt nun aus Satz 2.3.8.3. $\square$

Beispiel 2.4.6. Sei K nicht vollständig, $\mathrm{char}(K) = p$ und $a \in K \setminus K^p$. Dann ist das Polynom $f = X^p + Y^p + a \in K[X,Y]$ irreduzibel, aber wegen $f = (X + Y + a^{1/p})^p \in \overline{K}[X,Y]$ ist f nicht absolut reduziert. Daher ist auch $F = f^* = X^p + Y^p + aZ^p$ irreduzibel, nicht absolut irreduzibel und nicht absolut reduziert. $V_+(F)$ ist eine über K definierte irreduzible projektive Kurve, alle Punkte von $V_+(F)$ sind über K singulär, aber es ist auch $V_+(F) = V_+(X + Y + a^{1/p}Z)$ eine über $\overline{K}$ definierte projektive Gerade.

Satz 2.4.7. *Sei* $\mathrm{char}(K) \neq 2$, $A = (a_{i,j})_{i,j\in[1,3]} \in \mathsf{M}_n(K)$ *eine symmetrische Matrix* (*also* $a_{i,j} = a_{j,i}$ *für alle* i, $j \in [1,3]$),

$$Q = \sum_{i,j=1}^{3} a_{i,j} X_i X_j \in K[X_1, X_2, X_3]^\bullet \quad \textit{und} \quad \Sigma = V_+(Q) \subset \mathbb{P}^2.$$

1. *Ist* $\det A \neq 0$, *so ist* Q *irreduzibel, und* Σ *ist glatt.*
2. *Ist* $\det A = 0$, *so ist* $Q = GG_1$ *mit Linearformen* G, $G_1 \in K[X_1, X_2, X_3]$ *und* $\Sigma = \Lambda \cup \Lambda_1$ *mit projektiven Geraden* Λ, $\Lambda_1 \subset \mathbb{P}^2$.

Beweis. Für i, $j \in [1,3]$ ist

$$\frac{\partial Q}{\partial X_i} = 2\sum_{j=1}^{3} a_{i,j} X_j \quad \text{und} \quad \frac{\partial^2 Q}{\partial X_i \partial X_j} = 2a_{i,j}.$$

Wir zeigen zuerst:

A. Genau dann ist $\det A = 0$, wenn es eine projektive Gerade $\Lambda \subset \mathbb{P}^2$ gibt mit $\Lambda \subset \Sigma$.

Beweis von **A.** Sei zuerst $\det A = 0$. Dann gibt es einen Vektor $\boldsymbol{p} = (p_1, p_2, p_3) \in (K^3)^\bullet$, so dass

$$\sum_{j=1}^{3} a_{i,j} p_j = 0 \ \text{ für alle } \ i \in [1,3], \ \text{ also auch } \ \sum_{i,j=1}^{3} a_{i,j} p_i p_j = \sum_{i=1}^{3} p_i \sum_{j=1}^{3} a_{i,j} p_j = 0,$$

und daher ist $p = [\boldsymbol{p}] \in \Sigma$. Sei nun $q = [\boldsymbol{q}] \in \Sigma \setminus \{p\}$ mit $\boldsymbol{q} = (q_1, q_2, q_3) \in (\overline{K}^3)^\bullet$. Für alle $(s,t) \in (\overline{K}^2)^\bullet$ ist dann

$$\begin{aligned} Q(s\boldsymbol{p} + t\boldsymbol{q}) &= Q(s\boldsymbol{p}) + \sum_{i=1}^{3} \frac{\partial Q}{\partial X_i}(s\boldsymbol{p}) t q_i + \frac{1}{2} \sum_{i,j=1}^{3} \frac{\partial^2 Q}{\partial X_i \partial X_j)}(s\boldsymbol{p}) t^2 q_i q_j \\ &= s^2 Q(\boldsymbol{p}) + 2st \sum_{i=1}^{3} \sum_{j=1}^{3} a_{i,j} p_j q_i + t^2 \sum_{i,j=1}^{3} a_{i,j} q_i q_j = 0, \end{aligned}$$

und daher liegt die Verbindungsgerade Λ von p und q in Σ.

Sei umgekehrt $\Lambda = V_+(G) \subset \Sigma$ mit einer Linearform $G \in \overline{K}[X_1, X_2, X_3]^\bullet$. Dann ist $Q = GG_1$ mit einer weiteren Linearform $G_1 \in \overline{K}[X_1, X_2, X_3]^\bullet$. Dann gibt es ein $\boldsymbol{p} = (p_1, p_2, p_3) \in (\overline{K}^3)^\bullet$ mit $G(\boldsymbol{p}) = G_1(\boldsymbol{p}) = 0$, und für alle $i \in [1,3]$ ist

$$\frac{\partial Q}{\partial X_i}(\boldsymbol{p}) = G(\boldsymbol{p}) \frac{\partial G_1}{\partial X_i}(\boldsymbol{p}) + G_1(\boldsymbol{p}) \frac{\partial G}{\partial X_i}(\boldsymbol{p}) = 0, \ \text{ also } \ \sum_{j=1}^{3} a_{i,j} p_j = 0 \ \text{ und daher } \det A = 0. \quad \square[\mathbf{A}.]$$

1. Sei $\det A \neq 0$. Wäre Q reduzibel, so gäbe es eine Form $G \in K[X_1, X_2, X_3]$ mit $G \,|\, Q$, und dann wäre $\Lambda = V_+(G) \subset \Sigma$, im Widerspruch zu **A**. Daher ist Q irreduzibel. Wäre Σ nicht glatt und $p = [\boldsymbol{p}] \in \Sigma$ ein singulärer Punkt mit $\boldsymbol{p} = (p_1, p_2, p_3) \in (\overline{K}^3)^\bullet$, so folgte

$$\frac{\partial Q}{\partial X_i}(\boldsymbol{p}) = 2\sum_{j=1}^{3} a_{i,j}p_j = 0 \;\text{ für alle }\; i \in [1,3], \quad \text{also} \quad \det A = 0.$$

2. Sei $\det A = 0$. Nach **A** gibt es eine projektive Gerade $\Lambda \subset \mathbb{P}^2$ mit $\Lambda \subset \Sigma$. Ist $\mathfrak{I}_K^+(\Lambda) = (G)$ mit einer Linearform G, so ist $G \,|\, Q$ und daher $Q = GG_1$ mit einer Linearform G_1. Damit folgt $\Sigma = V_+(G) \cup V_+(G_1)$. □

Definition 2.4.8. Sei $\Gamma \subset \mathbb{P}^2$ eine projektive Kurve, $p \in \Gamma$ ein reguärer Punkt und Λ die Tangente an p (dann ist $\operatorname{ord}_p(\Gamma) = 1$ und $\mu_p(\Gamma, \Lambda) \geq 2$). Ist $\mu_p(\Gamma, \Lambda) \geq 3$, so heißt p ein *Wendepunkt* und Λ eine *Wendetangente*.

Satz 2.4.9. *Sei* $\operatorname{char}(K) \neq 2$, $\Gamma \subset \mathbb{P}^2$ *eine projektive Kurve,* $\mathfrak{I}_K^+(\Gamma) = (F)$ *mit einer Form* $F \in K[X_1, X_2, X_3]$, $\boldsymbol{p} \in (\overline{K}^3)^\bullet$ *und* $p = [\boldsymbol{p}] \in \Gamma$ *ein regulärer Punkt. Genau dann ist* p *ein Wendepunkt von* Γ*, wenn*

$$\det\Big(\frac{\partial^2 F}{\partial X_i \partial X_j}(\boldsymbol{p})\Big) = 0\,.$$

Beweis. Sei Λ die Tangente an Γ in p und $q = [\boldsymbol{q}] \in \Lambda \setminus \{p\}$ mit $\boldsymbol{q} = (q_1, q_2, q_3) \in (\overline{K}^3)^\bullet$. Dann ist

$$\begin{aligned} F(\boldsymbol{p} + T\boldsymbol{q}) &= F(\boldsymbol{p}) \sum_{i=1}^{3} \frac{\partial F}{\partial X_i} T q_i + \frac{1}{2} \sum_{i,j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(\boldsymbol{p}) T^2 q_i q_j + T^3 \Psi(T) \\ &= \frac{T^2}{2} \sum_{i,j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(\boldsymbol{p}) q_i q_j + T^3 \Psi(T) \quad \text{mit einem Polynom} \;\; \Psi \in \overline{K}[T]. \end{aligned}$$

Genau dann ist p ein Wendepunkt, wenn $\mu_p(\Gamma, \Lambda) \geq 3$, wenn also $F(\boldsymbol{p} + T\boldsymbol{q}) = T^3\Phi(T)$ mit $\Phi \in \overline{K}[T]$ für jeden Punkt $q = [\boldsymbol{q}] \in \Lambda \setminus \{p\}$, und das ist genau dann der Fall, wenn

$$\Lambda \subset V_+\Big(\sum_{i,j=1}^{2} \frac{\partial^2 F}{\partial X_i \partial X_j}(\boldsymbol{p}) X_i X_j\Big).$$

Nun folgt die Behauptung aus Satz 2.4.7. □

2.5. Funktionenkörper projektiver Kurven

Definition 2.5.1. Sei $\Gamma \subset \mathbb{P}^2$ eine über K definierte irreduzible projektive Kurve. Nach Satz 2.3.10 ist dann $\mathfrak{I}_K^+(\Gamma) = (F)$ mit einer irreduziblen Form $F \in K[X, Y, Z]$, der homogene Koordinatenring $K[\Gamma] = K[X, Y, Z]/(F)$ ist ein Bereich, und wir bezeichnen mit $K(\Gamma)$ die Menge aller Quotienten

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

$K(\Gamma)$ ist ein Teilkörper von $\mathfrak{q}(K[\Gamma])$.

Beweis. Seien R, $R_1 \in K(\Gamma)$,

$$R = \frac{G+(F)}{H+(F)} \quad \text{und} \quad R_1 = \frac{G_1+(F)}{H_1+(F)}$$

mit Formen G, $H \in K[X,Y,Z]$ vom Grade d, Formen G_1, $H_1 \in K[X,Y,Z]$ vom Grade e, und H, $H_1 \notin (F)$. Dann sind GG_1, HH_1 und $GH_1 + G_1H$ Formen vom Grade $d+e$, $HH_1 \notin (F)$,

$$R + R_1 = \frac{GH_1 + G_1H + (F)}{HH_1 + (F)} \in K(\Gamma), \quad RR_1 = \frac{GG_1+(F)}{HH_1+(F)} \in K(\Gamma).$$

Genau dann ist $R \neq 0$, wenn $G \notin (F)$, und dann ist

$$R^{-1} = \frac{H+(F)}{G+(F)} \in K(\Gamma). \qquad \square$$

Der Körper $K(\Gamma)$ heißt *Funktionenkörper* von Γ über K. Seine Elemente heißen *rationale Funktionen* auf Γ.

Eine rationale Funktion $R \in K(\Gamma)$ heißt *reguär* in einem Punkt $p = (\alpha:\beta:\gamma) \in \Gamma$, wenn

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

Dann hängt der Quotient

$$R(p) = \frac{G(\alpha,\beta,\gamma)}{H(\alpha,\beta,\gamma)} \in \overline{K}$$

nur von R und p ab (nachrechnen!) und heißt *Wert* von R an der Stelle p.

Für $a \in K$ ist

$$\frac{a+(F)}{1+(F)} \in K(\Gamma) \text{ regulär in jedem Punkte } p \in \Gamma \text{ mit Wert } a.$$

Die Zuordnung

$$a \mapsto \frac{a+(F)}{1+(F)} \text{ ist ein Körpermonomorphismus, und wir identifizieren } K \subset K(\Gamma).$$

Für $p \in \Gamma$ sei

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

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

Satz 2.5.2. *Sei $C \subset \mathbb{A}^2$ eine über K definierte irreduzible Kurve und $\mathfrak{I}_K(C) = (f)$ mit $f \in K[X,Y]$. Dann ist die Abbildung*

$$\tau\colon K(\overline{C}) \ \to \ K(C), \quad \textit{definiert durch} \quad \tau\Big(\frac{G+(f^*)}{H+(f^*)}\Big) = \frac{G_*+(f)}{H_*+(f)}$$

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

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

$$x = \tau\Big(\frac{\hat{x}}{\hat{z}}\Big), \qquad y = \tau\Big(\frac{\hat{y}}{\hat{z}}\Big), \quad \textit{und} \quad K[C] = \tau\Big(K\Big[\frac{\hat{x}}{\hat{z}}, \frac{\hat{y}}{\hat{z}}\Big]\Big).$$

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

Im Folgenden identifizieren wir (bei fester Einbettung $\mathbb{A}^2 \subset \mathbb{P}^2$) vermöge τ:

$$K(C) = K(\overline{C}), \quad \mathcal{O}_{p,K}(C) = \mathcal{O}_{p,K}(\overline{C}), \quad \mathcal{M}_{p,K}(C) = \mathcal{M}_{p,K}(\overline{C}).$$

BEWEIS. Es sind die folgenden Eigenschaften nachzurechnen (Übung!):

1) Ist $H \in K[X,Y,Z]$, so ist genau dann $H \notin (f^*)$, wenn $H_* \notin (f)$.

2) Sind $G, G_1 \in K[X,Y,Z]$ Formen gleichen Grades und $H, H_1 \in K[X,Y,Z]$ Formen gleichen Grades, so gilt:

$$\text{Aus} \quad \frac{G+(f^*)}{H+(f^*)} = \frac{G_1+(f^*)}{H_1+(f^*)} \quad \text{folgt} \quad \frac{G_*+(f)}{H_*+(f)} = \frac{G_{1*}+(f)}{H_{1*}+(f)}$$

(damit ist τ eine Abbildung).

3) Für $R, R' \in K(\overline{C})$ ist $\tau(R+R') = \tau(R)+\tau(R')$ und $\tau(RR') = \tau(R)\tau(R')$. Also τ ist ein Ringhomomorphismus, und da $K(\overline{C})$ ein Körper ist, ist τ injektiv.

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

$$\frac{g+(f)}{h+(f)} = \tau\Big(\frac{Z^e g^*+(f^*)}{Z^d h^*+(f^*)}\Big).$$

Daher ist τ surjektiv. Nach Definition ist dann

$$\tau\Big(\frac{\hat{x}}{\hat{z}}\Big) = \tau\Big(\frac{X+(f^*)}{Z+(f^*)} = \frac{X+(f)}{1+(f)} = X+(f) = x, \quad \text{und ebenso} \quad \tau\Big(\frac{\hat{y}}{\hat{z}}\Big) = y.$$

5) Ist $p = (\alpha,\beta) = (\alpha:\beta:1) \in C$ und

$$R = \frac{G+(f^*)}{H+(f^*)} \quad \text{mit Formen gleichen Grades } G, H \in K[X,Y,Z],$$

so ist genau dann $H(\alpha,\beta,1) \neq 0$, wenn $H_*(\alpha,\beta) \neq 0$, und dann ist

$$R(p) = \frac{G(\alpha,\beta,1)}{H(\alpha,\beta,1)} = \frac{G_*(\alpha,\beta)}{H_*(\alpha,\beta)} = \tau(R)(p). \qquad \square$$

Satz 2.5.3. *Sei $\Gamma \subset \mathbb{P}^2$ eine über K definierte irreduzible projektive Kurve und $p \in \Gamma$. Dann ist $\mathcal{O}_{p,K}(\Gamma)$ eine lokaler K-Unteralgebra von $K(C)$ mit maximalem Ideal $\mathcal{M}_{p,K}(\Gamma)$ und $\mathfrak{q}(\mathcal{O}_{p,K}(\Gamma)) = K(\Gamma)$. Die Abbildung $\varepsilon_p\colon \mathcal{O}_p(\Gamma) \to \overline{K}$, definiert durch $\varepsilon_p(R) = R(p)$ für alle $R \in \mathcal{O}_p(\Gamma)$, ist ein K-Algebrenhomomorphismus mit Kern $\operatorname{Ker}(\varepsilon_p) = \mathcal{M}_p(\Gamma)$.*

BEWEIS. p liegt in einem affinen Stück von Γ, und wir können $p \in C = \Gamma \cap \mathbb{A}^2$ annehmen. Dann ist C eine über K definierte irreduzible Kurve und $\Gamma = \overline{C}$. Nach Satz 2.5.2 besteht ein Isomorphismus $\tau\colon K(\overline{C}) \xrightarrow{\sim} K(C)$ mit $\tau(\mathcal{O}_p(\Gamma)) = \mathcal{O}_p(C)$, und $\varepsilon_p = \pi_p \circ \tau$ mit dem K-Algebrenhomomorphismus $\pi_p\colon \mathcal{O}_p(C) \to \overline{K}$ aus Satz 1.4.8. Daher folgen die Behauptungen aus Satz 1.4.8. $\square$

Definition und Bemerkung 2.5.4. Seien ι_1, ι_2, $\iota_3 \colon \mathbb{A}^2 \to \mathbb{P}^2$ die Einbettungen von $\mathbb{A}^2$ in die affinen Stücke von $\mathbb{P}^2$, definiert durch

$$\iota_1(\beta,\gamma) = (1:\beta:\gamma) \in \mathbb{P}^2(1) = \mathbb{P}^2 \setminus V_+(X) \quad (\text{die } (\mathsf{y},\mathsf{z})\text{-Ebene}),$$

$$\iota_2(\alpha,\gamma) = (\alpha:1:\gamma) \in \mathbb{P}^2(2) = \mathbb{P}^2 \setminus V_+(Y) \quad (\text{die } (\mathsf{x},\mathsf{z})\text{-Ebene}),$$

$$\iota_3(\alpha,\beta) = (\alpha:\beta:1) \in \mathbb{P}^2(3) = \mathbb{P}^2 \setminus V_+(Z) \quad (\text{die } (\mathsf{x},\mathsf{y})\text{-Ebene}).$$

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

Sei nun Γ irreduzibel. Für alle $\nu \in \{1, 2, 3\}$ ist dann auch C_ν irreduzibel, und nach Satz 2.5.2 erhalten wir Isomorphismen $\tau_\nu \colon K(\Gamma) \to K(C_\nu)$ wie folgt: Ist

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

so ist

$$\tau_1(R) = \frac{G(1,Y,Z)+(F(1,Y,Z))}{H(1,Y,Z)+(F(1,Y,Z))}\,, \quad \tau_2(R) = \frac{G(X,1,Z)+(F(X,1,Z))}{H(X,1,Z)+(F(X,1,Z))}$$

und

$$\tau_3(R) = \frac{G(X,Y,1)+(F(X,Y,1))}{H(X,Y,1)+(F(X,Y,1))}\,.$$

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

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

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

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

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

2.6. Projektive Koordinatentransformationen

Definitionen und Bemerkungen 2.6.1 (Projektive Koordinatentransformationen)**.**

1. Sei $A \in \mathsf{GL}_3(K)$, $\boldsymbol{p} \in (\overline{K}^3)^\bullet$, $\boldsymbol{p}' = \boldsymbol{p}A$, $p = [\boldsymbol{p}] \in \mathbb{P}^2$ und $p' = [\boldsymbol{p}'] \in \mathbb{P}^2$. Dan hängt p' nur von A und p ab, und wir setzen $\theta_A(p) = p'$. Die Abbildung $\theta_A \colon \mathbb{P}^2 \to \mathbb{P}^2$ heißt *die durch A definierte projektive Koordinatentransformation.* Für alle $\lambda \in \overline{K}^\times$ und A, $B \in \mathsf{GL}_3(K)$ ist θ_A bijektiv, $\theta_A^{-1} = \theta_{A^{-1}}$, $\theta_{\lambda A} = \theta_A$, und $\theta_{AB} = \theta_B \circ \theta_A$.

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

2. Für $A \in \mathsf{GL}_3(K)$ sei $\theta_A^* \colon K[X,Y,Z] \to K[X,Y,Z]$ der eineutigig bestimme K-Algebrenhomomorphismus mit $(\theta_A^*(X), \theta_A^*(Y), \theta_A^*(Z)) = (X,Y,Z)\,A^{-1}$. Ist $F \in K[X,Y,Z]$ eine Form vom Grade d, so ist $\theta_A^*(F) = F(\theta_A^*(X), \theta_A^*(Y), \theta_A^*(Z))$ ebenfalls eine Form vom Grade d, θ_A^* ist ein K-Algebrenisomorphismus, $\theta_A^{*-1} = \theta_{A^{-1}}$, und für A, $B \in \mathsf{GL}_3(K)$ ist $\theta_{AB}^* = \theta_A^* \circ \theta_B^*$.

3. Sei $A \in \mathsf{GL}_3(K)$ und $F \in K[X,Y,Z] \setminus K$ eine Form. Für $p \in \mathbb{P}^2$ ist genau dann $\theta_A^*(F)(\theta_A(p)) = 0$, wenn $F(p) = 0$, und $V_+(\theta_A^*(F)) = \theta_A(V_+(F))$.

   Beweis. Sei $p = [\boldsymbol{p}]$ mit $\boldsymbol{p} \in (\overline{K}^3)^\bullet$.

   $$\theta_A^*(F)(\theta_A(p)) = 0 \iff 0 = \theta_A^*(F)(\boldsymbol{p}A) = F(\boldsymbol{p}AA^{-1}) = F(\boldsymbol{p}) \iff F(p) = 0$$

   und

   $$\begin{aligned} p \in V_+(\theta_A^*(F)) &\iff 0 = \theta_A^*(F)(\boldsymbol{p}) = F(\boldsymbol{p}A^{-1}) \\ &\iff \theta_A^{-1}(p) = \theta_{A^{-1}}(p) = [\boldsymbol{p}A^{-1}] \in V_+(F) \iff p \in \theta_A(V_+(F)). \end{aligned}$$ □

4. Ist $\Lambda \subset \mathbb{P}^2$ eine über K definierte projektive Gerade, so ist auch $\theta_A(\Lambda)$ eine über K definierte projektive Gerade.

   Beweis. Ist $\Lambda = V_+(F)$ mit einer Linearform $F \in K[X,Y,Z]$, so folgt (nach 3.) $\theta_A(\Lambda) = V_+(\theta_A^*(F)$, und auch $\theta_A^*(F) \in K[X,Y,Z]$ ist eine Linearform. □

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

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

   $$\begin{aligned} F \in \mathfrak{I}_K^+(\theta_A(\Gamma)) &\iff \theta_A(\Gamma) \subset V_+(F) \iff \Gamma \subset \theta_A^{-1}(V_+(F)) = V_+(\theta_A^{*-1}(F)) \\ &\iff \theta_A^{*-1}(F) \in \mathfrak{I}_K^+(\Gamma) \iff F \in \theta_A^*(\mathfrak{I}_K^+(\Gamma))\,. \end{aligned}$$ □

   Insbesondere induziert θ_A^* einen Isomorphismus

   $$\theta_A^\# \colon K[\Gamma] = K[X,Y,Z]/\mathfrak{I}_K^+(\Gamma) \to K[X,Y,Z]/\mathfrak{I}_K^+(\theta_A(\Gamma)) = K[\theta_A(\Gamma)]\,.$$

   Ist Γ irreduzibel und $\mathfrak{I}_K^+(\Gamma) = (F)$ mit einer irreduziblen Form $F \in K[X,Y,Z]$, so ist $\mathfrak{I}_K^+(\theta_A(\Gamma)) = (\theta_A^*(F))$, und $\theta_A^\#$ induziert einen Isomorphismus der Quotientenkörper $\theta_A^\# \colon K(\Gamma) \to K(\theta(\Gamma))$. Explizit:

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

   Ist $R \in K(\Gamma)$ und $p \in \Gamma$, so ist R genau dann in p regulär, wenn $\theta_A^\#(R)$ in $\theta_A(p)$ regulär ist. Dann ist $R(p) = \theta_A^\#(R)(\theta_A(p))$, und es folgt $\theta_A^\#(\mathcal{O}_p(\Gamma)) = \mathcal{O}_{\theta_A(p)}(\theta_A(\Gamma))$.

Definition 2.6.2.

1. Drei Punkte p_1, p_2, $p_3 \in \mathbb{P}^2$ heißen *kollinear*, wenn es eine projektive Gerade $\Lambda \subset \mathbb{P}^2$ gibt mit $\{p_1, p_2, p_3\} \subset \Lambda$. Ein Quadrupel (p_1, p_2, p_3, p_4) von Punkten in $\mathbb{P}^2$ heißt *Basis* von $\mathbb{P}^2$, wenn je drei dieser Punkte nicht kollinear sind.
2. Drei projektive Geraden Λ_1, Λ_2, $\Lambda_3 \subset \mathbb{P}^2$ heißen *kopunktal*, wenn $\Lambda_1 \cap \Lambda_2 \cap \Lambda_3 \neq \emptyset$. Ein Quadrupel $(\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4)$ projektiver Geraden in $\mathbb{P}^2$ heißt *Dualbasis* von $\mathbb{P}^2$, wenn je drei dieser projektiven Geraden nicht kopunktal sind.

Lemma 2.6.3.

1. *Für $i \in [1,3]$ sei $\boldsymbol{p}_i \in (\overline{K}^3)^\bullet$ und $p_i = [\boldsymbol{p}_i] \in \mathbb{P}^2$. Genau dann sind p_1, p_2, p_3 kollinear, wenn $\boldsymbol{p}_1$, $\boldsymbol{p}_2$, $\boldsymbol{p}_3$ über $\overline{K}$ linear abhängig sind.*
2. *Für $i \in [1,3]$ sei $\Lambda_i = V_+(a_iX + b_iY + c_iZ) \subset \mathbb{P}^2$ mit $\boldsymbol{u}_i = (a_i, b_i, c_i) \in (\overline{K}^3)^\bullet$, und sei $u_i = [\boldsymbol{u}_i] \in \mathbb{P}^2$. Genau dann sind Λ_1, Λ_2, Λ_3 kopunktal, wenn u_1, u_2, u_3 kollinear sind.*

Beweis. 1. Für $i \in [1,3]$ sei $\boldsymbol{p}_i = (\alpha_i, \beta_i, \gamma_i)$, und

$$P = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{pmatrix} \in \mathsf{M}_3(\overline{K}).$$

Sind p_1, p_2, p_3 kollinear, so gibt es eine projektive Gerade $\Lambda \subset \mathbb{P}^2$ mit $\{p_1, p_2, p_3\} \subset \Lambda$. Ist $\Lambda = V_+(aX + bY + cZ)$ mit $(a, b, c) \in (\overline{K}^3)^\bullet$, so ist $a\alpha_i + b\beta_i + c\gamma_i = 0$ für alle $i \in [1,3]$ und daher $\det P = 0$. Dann sind $\boldsymbol{p}_1$, $\boldsymbol{p}_2$, $\boldsymbol{p}_3$ die Zeilenvektoren von P und daher linear abhängig.

Sind umgekehrt $\boldsymbol{p}_1$, $\boldsymbol{p}_2$, $\boldsymbol{p}_3$ linear abhängig, so ist $\det P = 0$, und es gibt $(a, b, c) \in (\overline{K}^3)^\bullet$, so dass $a\alpha_i + b\beta_i + c\gamma_i = 0$ und daher $\{p_1, p_2, p_3\} \subset V_+(aX + bY + cZ)$ für alle $i \in [1,3]$.

2. Genau dann sind Λ_1, Λ_2, Λ_3 kopunktal, wenn es einen Punkt $p = (\alpha : \beta : \gamma) \in \Lambda_1 \cap \Lambda_2 \cap \Lambda_3$ mit $(\alpha, \beta, \gamma) \in (\overline{K}^3)^\bullet$ gibt, und das ist genau dann der Fall, wenn $a_i\alpha + b_i\beta + c_i\gamma = 0$, also $u_i = [\boldsymbol{u}_i] \in V_+(\alpha X + \beta Y + \gamma Z)$ für alle $i \in [1,3]$. □

Satz 2.6.4.

1. *Seien (p_1, p_2, p_3, p_4), $(p'_1, p'_2, p'_3, p'_4) \in \mathbb{P}^2(K)^4$ Basen von $\mathbb{P}^2$. Dann gibt es eine Matrix $A \in \mathsf{GL}_3(K)$, so dass $\theta_A(p_i) = p'_i$ für alle $i \in [1,3]$.*
2. *Seien $(\Lambda_1, \Lambda_2, \Lambda_3, \Lambda_4)$ und $(\Lambda'_1, \Lambda'_2, \Lambda'_3, \Lambda'_4)$ über K definierte Dualbasen von $\mathbb{P}^2$. Dann gibt es eine Matrix $A \in \mathsf{GL}_3(K)$, so dass $\theta_A(\Lambda_i) = \Lambda'_i$ für alle $i \in [1,3]$.*

Beweis. 1. Für $i \in [1,4]$ sei $p_i = [\boldsymbol{p}_i]$ und $p'_i = [\boldsymbol{p}'_i]$ mit $\boldsymbol{p}_i$, $\boldsymbol{p}'_i \in (K^3)^\bullet$. Dann ist $(\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3)$ eine Basis von K^3, und da auch $(\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_4)$, $(\boldsymbol{p}_1, \boldsymbol{p}_3, \boldsymbol{p}_4)$ und $(\boldsymbol{p}_2, \boldsymbol{p}_3, \boldsymbol{p}_4)$ linear unabhängig sind, folgt $\boldsymbol{p}_4 = \lambda_1\boldsymbol{p}_1 + \lambda_2\boldsymbol{p}_2 + \lambda_3\boldsymbol{p}_3$ mit λ_1, λ_2, $\lambda_3 \in K^\times$.

In gleicher Weise erhalten wir $\boldsymbol{p}'_4 = \lambda'_1\boldsymbol{p}'_1 + \lambda'_2\boldsymbol{p}'_2 + \lambda'_3\boldsymbol{p}'_3$ mit λ'_1, λ'_2, $\lambda'_3 \in K^\times$. Für alle $i \in [1,3]$ ist $p'_i = [\lambda_i^{-1}\lambda'_i\boldsymbol{p}'_i]$, und da $(\boldsymbol{p}_1, \boldsymbol{p}_2, \boldsymbol{p}_3)$ und $(\lambda_1^{-1}\lambda'_1\boldsymbol{p}'_1, \lambda_2^{-1}\lambda'_2\boldsymbol{p}'_2, \lambda_3^{-1}\lambda'_3\boldsymbol{p}'_3)$ Basen von K^3 sind, gibt es eine Matrix $A \in \mathsf{GL}_3(K)$, so dass $\lambda_i^{-1}\lambda'_i\boldsymbol{p}'_i = \boldsymbol{p}_iA$ für alle $i \in [1,3]$, und dann folgt auch

$$\boldsymbol{p}'_4 = \sum_{i=1}^{3} \lambda'_i\boldsymbol{p}'_i = \sum_{i=1}^{3} \lambda_i(\lambda_i^{-1}\lambda'_i)\boldsymbol{p}'_i = \sum_{i=1}^{3} \lambda_i\boldsymbol{p}_iA = \boldsymbol{p}_4A,$$

also $p'_i = \theta_A(p_i)$ für alle $i \in [1,4]$.

2. Wir zeigen zuerst:

A. Sei $\Lambda = V_+(aX + bY + cZ,\ \Lambda' = V_+(a'X + b'Y + c'Z)$ mit $(a, b, c), (a', b', c') \in (K^3)^\bullet$ und $A \in \mathsf{GL}_3(K)$ mit $(a', b', c') = (a, b, c)A$ und $A' = (A^{-1})^{\mathsf{t}}$. Dann ist $\Lambda' = \theta_{A'}(\Lambda)$.

Beweis von **A.** Nach den Bemerkungen 2.6.1.3 ist $\theta_{A'}(\Lambda) = V_+(\theta^*_{A'}(aX + bY + cZ))$, und $\theta^*_{A'}(aX+bY+cZ) = a\theta^*_{A'}(X)+b\theta^*_{A'}(Y)+c\theta^*_{A'}(Z)$ und $(\theta^*_{A'}(X), \theta^*_{A'}(Y), \theta^*_{A'}(Z)) = (X, Y, Z)A'^{-1}$. Sei

$$A'^{-1} = A^{\mathsf{t}} = \begin{pmatrix} \alpha_1 & \beta_1 & \gamma_1 \\ \alpha_2 & \beta_2 & \gamma_2 \\ \alpha_3 & \beta_3 & \gamma_3 \end{pmatrix} \in \mathsf{M}_3(\overline{K}).$$

Dann ist $a' = a\alpha_1 + b\beta_1 + c\gamma_1,\ b' = a\alpha_2 + b\beta_2 + c\gamma_2$ und $c' = a\alpha_3 + b\beta_3 + c\gamma_3$,

$$(\theta^*_{A'}(X), \theta^*_{A'}(Y), \theta^*_{A'}(Z)) = (\alpha_1X + \alpha_2Y + \alpha_3Z, \beta_1X + \beta_2Y + \beta_3Z, \gamma_1X + \gamma_2Y + \gamma_3Z),$$

$\theta^*_{A'}(aX+bY+cZ) = (a\alpha_1+b\beta_1+c\gamma_1)X+(a\alpha_2+b\beta_2+c\gamma_2)Y+(a\alpha_3+b\beta_3+c\gamma_3)Z = a'X+b'Y+c'Z$ und daher $\theta_{A'}(\Lambda) = \Lambda'$. □[**A.**]

Für $i \in [1, 4]$ sei $\Lambda_i = V_+(a_iX+b_iY+c_iZ),\ \Lambda'_i = V_+(a'_iX+b'_iY+c'_iZ),\ \boldsymbol{u}_i = (a_i, b_i, c_i),\ \boldsymbol{u}'_i = (a'_i, b'_i, c'_i) \in (K^3)^\bullet$ und $u_i = [\boldsymbol{u}_i]$, $u'_i = [\boldsymbol{u}'_i] \in \mathbb{P}^2(K)$. Nach Lemma 2.6.3.2 sind (u_1, u_2, u_3, u_4) und (u'_1, u'_2, u'_3, u'_4) Basen von $\mathbb{P}^2$ in $\mathbb{P}^2(K)$, und nach 1. gibt es eine Matrix $A \in \mathsf{GL}_3(K)$, so dass $\theta_A(u_i) = u'_i$ und daher $\boldsymbol{u}'_i = \boldsymbol{u}_iA$ für alle $i \in [1, 4]$. Nach **A** folgt $\Lambda'_i = \theta_{A'}(\Lambda_i)$ mit $A' = (A^{-1})^{\mathsf{t}}$. □

Definition und Bemerkung 2.6.5. Eine Abbildung $\sigma\colon \mathbb{A}^2 \to \mathbb{A}^2$ heißt eine über K definierte *affine Koordinatentransformation*, wenn es a_1, b_1, c_1, a_2, b_2, $c_2 \in K$ gibt, so dass $a_1b_2 - a_2b_1 \neq 0$ und

$$\sigma(x, y) = (a_1x + b_1y + c_1, a_2x + b_2y + c_2) \quad \text{für alle } x, y \in \mathbb{A}^2.$$

Man nennt

$$C(\sigma) = \begin{pmatrix} a_1 & a_2 & 0 \\ b_1 & b_2 & 0 \\ c_1 & c_2 & 1 \end{pmatrix}$$

die Matrix und $\theta_{C(\sigma)}$ die *projektive Fortsetzung* von σ.

Es ist $\theta_{C(\sigma)} \,|\, \mathbb{A}^2 = \sigma$ und $\theta_{C(\sigma)} \,|\, V_+(Z) = \mathrm{id}_{V_+(Z)}$. Ist umgekehrt $\theta\colon \mathbb{P}^2 \to \mathbb{P}^2$ eine über K definierte projektive Koordinatentransformation mit $\theta \,|\, V_+(Z) = \mathrm{id}_{V_+(Z)}$, so ist $\theta \,|\, \mathbb{A}^2\colon \mathbb{A}^2 \to \mathbb{A}^2$ eine über K definierte affine Koordinatentransformation, und θ ist die projektive Fortsetzung von $\theta \,|\, \mathbb{A}^2$.

KAPITEL 3

Algebraische Funktionenkörp er und diskrete Bewertungen

3.1. Algebraische Funktionenkörper

Definition 3.1.1. Eine Körpererweiterung L/K heißt (*algebraischer*) *Funktionenkörper* (*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 $\widetilde{K}$ von K in L den *Konstantenkörper* von L/K.

Ist $x \in L$ transzendent über K, so ist x auch transzendent über $\widetilde{K}$, und $[L:\widetilde{K}(x)] \leq [L:K(x)]$. Daher ist L auch ein Funktionenkörper über $\widetilde{K}$. Ist $L = K(x)$ mit einem über K transzendenten x (also $L \cong K(X)$), so nennt man L einen *rationalen Funktionenkörper* über K.

Beispiel 3.1.2. Sei K ein Körper, C eine über K definierte irreduziblen Kurve und $K(C)$ ihr Funktionenkörper. Nach Satz 1.4.4 ist $K(C)/K$ ein Funktionenkörper. Ist C absolut irreduzibel, so ist K der Konstantenkörper von $K(C)/K$.

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

Beweis. Sei $J = \{g \in K[X, Y] \mid g(x, y) = 0\} \lhd K[X, Y]$. Wir zeigen: Es gibt ein irreduzibles Polynom $f \in K[X, Y]$ mit $J = (f)$. Dann ist $f(x, y) = 0$, und für jedes irreduzible Polynom $f_1 \in K[X, Y]$ mit $f_1(x, y) = 0$ ist $f \mid f_1$, also $f_1 = cf$ mit einem $c \in K^\times$.

Da y über $K(x)$ algebraisch ist, gibt es ein Polynom $g_0 \in K(x)[Y]^\bullet$ mit $g_0(y) = 0$, und nach Hochmultiplizieren der Nenner kann man $g_0 \in K[x, Y]$ annehmen. Ist nun $g \in K[X, Y]^\bullet$ mit $g(x, Y) = g_0$, so ist $g(x, y) = 0$ und daher auch $f(x, y) = 0$ für einen irreduziblen Faktor f von g. Dann ist $f \in J$, also $(f) \subset J$ und wir zeigen $J = (f)$. Wir nehmen im Gegenteil an, es gebe ein Polynom $g \in J \setminus (f)$. Ist $R = K[X]$, so sind g und f ohne nicht-konstanten gemeinsamen Faktor in $R[Y] = K[X, Y]$. Nach Lemma 0.2.3 gibt es Polynome p, $q \in R[Y] = K[X, Y]$ mit $pf + qg = r \in R^\bullet = K[X]^\bullet$. Damit folgt $r(x) = p(x, y)f(x, y) + q(x, y)g(x, y) = 0$, ein Widerspruch zur Transzendenz von x.

Sei $\phi\colon K[X, Y] \to K[x, y]$ der K-Algebrenhomomorphismus mit $\phi(X) = x$ und $\phi(Y) = y$. Dann ist $\mathrm{Ker}(\phi) = (f)$, und ϕ induziert einen Isomorphismus $\phi^*\colon K[X, Y]/(f) \xrightarrow{\sim} K[x, y]$. Sei $C = V(f) \subset \mathbb{A}^2$. Dann ist $\theta_C\colon K[X, Y] \to K[x_C, y_C]$ ein K-Algebrenepimorphismus mit $\theta_C(X) = x_C$, $\theta_C(Y) = y_C$ und $\mathrm{Ker}(\theta_C) = \mathfrak{I}_K(C) = (f)$. θ_C induziert einen Isomorphismus

$\theta_C^*\colon K[X,Y]/(f) \xrightarrow{\sim} K[C]$, und $\Phi_0 = \theta_C^* \circ \phi^{*-1}\colon K[x,y] \to K[x_C, y_C]$ ist ein K-Algebrenisomorphismus mit $\Phi_0(x) = x_C$ und $\Phi_0(y) = y_C$. Sei $\Phi\colon L = K(x,y) \to K(C)$ die Fortsetzung von Φ_0 auf die Quotientenkörper. Dann leistet Φ das Gewünschte, und die Eindeutigkeit ist offensichtlich. □

Satz 3.1.4. *Sei L/K ein Funktionenkörper, und sei $t \in L$ transzendent über K. Dann ist $[L\colon K(t)] < \infty$.*

Beweis. 1. Sei $x \in L$ transzendent über K mit $[L : K(x)] < \infty$. Dann ist t algebraisch über $K(x)$, und es gibt ein Polynom $f \in K(x)[T]^\bullet$ mit $f(t) = 0$. Nach Hochmultiplizieren der Nenner können wir $f \in K[x][T]^\bullet$ annehmen, und dann gibt es ein Polynom $F \in K[X,T]^\bullet$ mit $F(x,t) = 0$. Sei

$$F = \sum_{\nu=0}^{n} a_\nu(T) X^\nu \quad \text{mit} \quad n \in \mathbb{N}_0,\ a_\nu(T) \in K[T] \ \text{ für alle } \nu \in [0,n] \ \text{ und } \ a_n(T) \neq 0.$$

Da x über K transzendent ist, folgt $a_n(t) \neq 0$, also $F(X,t) \in K(t)[X]^\bullet$, und wegen $F(t,x) = 0$ ist x algebraisch über $K(t)$. Damit folgt

$$[L\colon K(t)] = [L\colon K(t,x)]\,[K(t,x)\colon K(t)] \leq [L\colon K(x)]\,[K(t)(x)\colon K(t)] < \infty\,. \qquad \square$$

3.2. Bewertungsbereiche

Definition 3.2.1. Sei L ein Körper und $\mathcal{O} \subsetneq L$ ein Teilring mit $L = \mathsf{q}(\mathcal{O})$.

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 und 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 dann 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 3.2.2. *Sei L ein Körper, $\mathcal{O} \subsetneq L$ ein Teilring, $L = \mathsf{q}(\mathcal{O})$ und $P = \mathcal{O} \setminus \mathcal{O}^\times$.*

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

$$\bigcap_{n \in \mathbb{N}} P^n = \{0\}.$$

Beweis. 1. Sei $\mathcal{O}$ ein Bewertungsbereich. Dann ist offensichtlich $P \supset \{x^{-1} \mid x \in L \setminus \mathcal{O}\} \cup \{0\}$. Ist umgekehrt $z \in P$ und $z \neq 0$, so ist $z^{-1} \in L \setminus \mathcal{O}$ und $z = (z^{-1})^{-1}$. Es bleibt zu zeigen, dass P ein Ideal ist. Seien dazu a, $b \in P$ und $r \in \mathcal{O}$. Dann ist auch $ra \in P$, und für den Nachweis von $a + b \in P$ können wir $ab \neq 0$ annehmen. Dann ist $a^{-1}b \in \mathcal{O}$ oder $ab^{-1} \in \mathcal{O}$, etwa $ab^{-1} \in \mathcal{O}$, und es folgt $a + b = b(ab^{-1} + 1) \in \mathcal{O} \setminus \mathcal{O}^\times$.

2. (a) Sei $\{0\} \neq I \subsetneq \mathcal{O}$ ein Ideal. Ist $a \in I^\bullet$, 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 es sei $n = \min\{m \in \mathbb{N} \mid t^m \in I\}$. Dann ist $(t^n) \subset I$, und wir zeigen Gleichheit. Sei $a \in I^\bullet$, $a = t^m u$ 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) Ist $z \in L^\times \setminus \mathcal{O}$, so ist $z = t^{-n}u = (t^{-1})^n u$ mit $n \in \mathbb{N}$ und $u \in \mathcal{O}^\times$. Damit folgt $L = \mathcal{O}[t^{-1}]$. 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 daher $L = \mathcal{O}[t^{-1}] \subset \mathcal{O}'$, also $\mathcal{O}' = L$.

3. Sei $P = (t)$. Ist $\mathcal{O}$ ein diskreter Bewertungsbereich und $a \in \mathcal{O}^\bullet$, so ist $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}^\times$, und daher $t^{n+1} \nmid a$, also $a \notin (t^n) = P^n$ und daher

$$\bigcap_{n\in\mathbb{N}} P^n = \{0\}.$$

Sei nun

$$\bigcap_{n\in\mathbb{N}} P^n = \bigcap_{n\in\mathbb{N}} (t^n) = \{0\}.$$

Wir zeigen: Jedes $a \in \mathcal{O}^\bullet$ hat eine eindeutige Darstellung $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}^\times$ (dann ist $\mathcal{O}$ ein faktorieller Bereich und t is bis auf Assoziierte das einzige Primelement). Ist $a \in \mathcal{O}^\times$, so gibt es ein $n \in \mathbb{N}_0$, so dass $a \in (t^n) \setminus (t^{n+1})$, und dann ist $a = t^n u$ mit $u \in \mathcal{O}^\times$. Die Eindeutigkeit der Darstellung folgt, da t ein Primelement ist. □

Satz 3.2.3 (Existenzsatz für Bewertungsbereiche)**.** *Sei L ein Körper, $R \subsetneq L$ ein Teilring und $\mathbf{0} \neq I \subsetneq R$ ein Ideal. Dann gibt es einen Bewertungsbereich $\mathcal{O}$ von L mit maximalem Ideal P, 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 $IS \neq S$. Dann ist $R \in \Omega$, also $\Omega \neq \emptyset$. Wir zeigen, dass die Vereinigung jeder Kette in Ω wieder zu Ω gehört. Mit Hilfe des Zorn'schen Lemmas folgt dann, dass Ω ein maximales Element besitzt. Sei also $(S_\lambda)_{\lambda\in\Lambda}$ eine Kette in Ω und

$$S = \bigcup_{\lambda\in\Lambda} S_\lambda.$$

Dann ist S ein Teilring von L und wir behaupten $IS \subsetneq S$. Wäre $IS = S$, also $1 \in IS$, so folgte $1 = s_1a_1 + \ldots + s_ra_r$ mit $a_1, \ldots, a_r \in I$ und $s_1, \ldots s_r \in S$. Da $(S_\lambda)_{\lambda\in\Lambda}$ eine Kette ist, gibt es ein $\nu \in \Lambda$ mit $\{s_1, \ldots, s_r\} \subset S_\nu$, also $1 \in IS_\nu$ und $IS_\nu = S_\nu$, ein Widerspruch]. Daher ist $S \in \Omega$.

Sei nun $\mathcal{O} \in \Omega$ maximal und $J = I\mathcal{O}$. 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 $J\mathcal{O}[z] = I\mathcal{O}[z] = \mathcal{O}[z]$ und $J\mathcal{O}[z^{-1}] = \mathcal{O}[z^{-1}]$. Dann bestehen Gleichungen der Form

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

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

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

und wir erhalten

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

ein Widerspruch zur Minimalität von n. □

3.3. Bewertungsbereiche in Funktionenkörpern

Satz 3.3.1. *Sei L/K ein Funktionenkörper mit Konstantenkörper $\widetilde{K}$ und $\mathcal{O}$ ein Bewertungsbereich von L mit maximalem Ideal P und $K \subset \mathcal{O}$.*

1. *$\widetilde{K} \subset \mathcal{O}$ und $\widetilde{K}^\times \subset \mathcal{O}^\times$.*
2. *Seien $n \in \mathbb{N}$, $x_1,\dots,x_n \in P^\bullet$ und $x_i \in x_{i+1}P$ für alle $i \in [1,n-1]$. Dann ist $n \le [L\colon K(x_1)] < \infty$. Insbesondere ist jedes $x \in P^\bullet$ transzendent über K.*
3. *$\mathcal{O}$ ist ein diskreter Bewertungsbereich.*

Beweis. 1. Wir nehmen an, es sei $a \in \widetilde{K} \setminus \mathcal{O}$. Dann ist $a^{-1} \in \mathcal{O}$, 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. Daher ist $\widetilde{K} \subset \mathcal{O}$, und folglich auch $\widetilde{K}^\times \subset \mathcal{O}^\times$.

2. Sei $x_1 \in P^\bullet$. Dann ist $x_1^{-1} \notin \mathcal{O}$, also $x_1^{-1} \notin \widetilde{K}$. Daher ist x_1^{-1} und damit auch x_1 transzendent über K und $[L\colon K(x_1)] < \infty$ nach Satz 3.1.4.

Seien nun $x_1,\dots,x_n \in P^\bullet$ und $x_i \in x_{i+1}P$ für alle $i \in [1,n-1]$. Dann folgt $x_i \in x_jP$ für alle $i,\,j \in [1,n]$ mit $i<j$, und wir zeigen: $(x_1,\dots,x_n)$ ist linear unabhängig über $K(x_1)$. 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 $\varphi_k \notin x_1K[x_1]$ und $\varphi_i \in x_1K[x_1]$ 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 $x_i \in x_kP$, 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 $\varphi x_k^{-1} x_i = \psi_i x_i x_k^{-1} x_1 \in P$. 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. Wir zeigen zuerst, dass P endlich erzeugt ist, und nehmen im Gegenteil an, es gebe eine Folge $(x_i)_{i\ge1}$ in $P^\bullet$, so dass $(x_1,\dots,x_i) \subsetneq (x_1,\dots,x_{i+1})$ für alle $i \ge 1$. Für alle $i \ge 1$ ist dann $x_{i+1} \notin x_i\mathcal{O}$, folglich $x_i^{-1}x_{i+1} \in L \setminus \mathcal{O}$ und daher $x_ix_{i+1}^{-1} \in P$, also $x_i \in x_{i+1}P$. Wegen 2. folgt $n \le [L\colon K(x_1)]$ für alle $n \in \mathbb{N}$, ein Widerspruch.

Sei nun $\{y_1,\dots,y_m\}$ ein minimales Erzeugendensystem von P. Wäre $m \ge 2$, so folgte $y_2 \notin y_1\mathcal{O}$, also $y_1^{-1}y_2 \notin \mathcal{O}$ und daher $y_1y_2^{-1} \in \mathcal{O}$, 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 $t \in \mathcal{O}$. Nach Satz 3.2.2.3 genügt es, zu zeigen: Für jedes $x \in \mathcal{O}^\bullet$ gibt es ein $n \in \mathbb{N}$ mit $x \notin (t^n)$. Wir nehmen im Gegenteil an, es sei $x \in \mathcal{O}^\bullet$ und $x \in (t^n)$ für alle $n \in \mathbb{N}$. Dann ist $x \in P$,

und für $i \in \mathbb{N}$ sei $x_i = t^{1-i}x$, also $x_i = tx_{i+1} \in x_{i+1}P$. Nach 2. folgt nun $n \leq [L:K(x)] < \infty$ für alle $n \in \mathbb{N}$, ein Widerspruch. □

Satz 3.3.2. *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. Nach Satz 3.2.3 gibt es einen Bewertungsbereich $\mathcal{O}'$ von L mit maximalem Ideal P', so dass $\mathcal{O} \subset \mathcal{O}'$ und $P \subset P'$. Nach Satz 3.3.1.3 ist $\mathcal{O}'$ ein diskreter Bewertungsbereich, und wegen

$$\bigcap_{n\in\mathbb{N}} P^n \subset \bigcap_{n\in\mathbb{N}} P'^n = \{0\}$$

ist nach Satz 3.2.2 auch $\mathcal{O}$ ein diskreter Bewertungsbereich. □

3.4. Kennzeichnung regulärer Punkte

Satz 3.4.1. *Sei K ein Körper, $\overline{K}$ eine algebraische Hülle von K, $C \subset \mathbb{A}^2$ eine über K definierte irreduzible Kurve und $\boldsymbol{p} = (\alpha, \beta) \in C$.*

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

Beweis. Sei $\mathfrak{I}_K(C) = (f)$ mit irreduziblem $f \in K[X,Y]$, und seien x, $y \in K[C]$ die Koordinatenfunktionen von C.

1. Sei $\boldsymbol{p} = (\alpha, \beta) \in K^2$ ein über K regulärer Punkt von C, und sei

$$\frac{\partial f}{\partial Y}(\alpha,\beta) \neq 0\,.$$

Nach Satz 1.4.4 ist $\mathcal{M}_{\boldsymbol{p},K}(C) = {}_{\mathcal{O}_{\boldsymbol{p},K}}(x-\alpha, y-\beta)$, und wegen $f(\boldsymbol{p}) = f(\alpha,\beta) = 0$ folgt $f = (X-\alpha)f_1 + (Y-\beta)f_2$ mit f_1, $f_2 \in K[X,Y]$. Dann ist

$$\frac{\partial f}{\partial Y} = (X-\alpha)\frac{\partial f_1}{\partial Y} + (Y-\beta)\frac{\partial f_2}{\partial Y} + f_2\,, \quad \text{also} \quad \frac{\partial f}{\partial Y}(\alpha,\beta) = f_2(\alpha,\beta) = f_2(x,y)(\alpha,\beta) \neq 0\,.$$

Wegen $0 = f(x,y) = (x-\alpha)f_1(x,y) + (y-\beta)f_2(x,y)$ folgt

$$y - \beta = \frac{-(x-\alpha)f_1(x,y)}{f_2(x,y)} \in {}_{\mathcal{O}_{\boldsymbol{p},K}}(x-\alpha) \quad \text{und daher} \quad \mathcal{M}_{\boldsymbol{p},K}(C) = {}_{\mathcal{O}_{\boldsymbol{p},K}}(x-\alpha)\,.$$

Nach Satz 3.3.2 ist $\mathcal{O}_{\boldsymbol{p},K}$ ein diskreter Bewertungsbereich.

2. Sei $m_\alpha \in K[X]$ das Minimalpolynom von α und $m_\beta \in K[Y]$ das Minimalpolynom von β über K. Da $K(x,y)/K$ transzendent ist, folgt $(m_\alpha(x), m_\beta(y)) \neq (0,0)$, und wegen der Separabilität ist $m'_\alpha(\alpha)m'_\beta(\beta) \neq 0$. Ist nun $m_\alpha(x)m_\beta(y) \neq 0$, so ist entweder $m_\alpha(x)m_\beta(y)^{-1} \in \mathcal{O}_{\boldsymbol{p},K}(C)$ oder $m_\alpha(x)^{-1}m_\beta(y) \in \mathcal{O}_{\boldsymbol{p},K}(C)$. Daher können wir annehmen, dass

$$m_\beta(y) \neq 0 \quad \text{und} \quad \frac{m_\alpha(x)}{m_\beta(y)} \in \mathcal{O}_{\boldsymbol{p},K}(C).$$

Dann existieren Polynome $g,\, h \in K[X,Y]$ mit $h(\alpha,\beta) \neq 0$ und

$$\frac{m_\alpha(x,y)}{m_\beta(x,y)} = \frac{g(x.y)}{h(x,y)}\,, \quad \text{also} \quad \frac{m_\alpha + (f)}{m_\beta + (f)} = \frac{g + (f)}{h + (f)},$$

und daher $m_\alpha h - m_\beta g = Qf$ mit einem Polynom $Q \in K[X,Y]$. Es folgt

$$\frac{\partial(Qf)}{\partial X} = \frac{\partial Q}{\partial X} f + Q\frac{\partial f}{\partial X} = m'_\alpha h + m_\alpha \frac{\partial h}{\partial X} - m_\beta \frac{\partial g}{\partial X}\,,$$

und wegen $f(\boldsymbol{p}) = m_\alpha(\boldsymbol{p}) = m_\alpha(\alpha) = 0$, $m'_\alpha(\boldsymbol{p}) \neq 0$ und $h(\boldsymbol{p}) \neq 0$ folgt

$$\frac{\partial f}{\partial X}(\boldsymbol{p}) \neq 0\,. \qquad \square$$

3.5. Diskrete Bewertungen

Definition 3.5.1. 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 surjektive Abbildung $v\colon L \to \mathbb{Z} \cup \{\infty\}$, so dass für alle $a,\, b \in L$ gilt:

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

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

Bemerkungen 3.5.2. Sei L ein Körper und $v\colon L \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung.

1. $v \,|\, L^\times\colon L^\times \to \mathbb{Z}$ ist ein Gruppenepimorphismus, $v(1) = 0$ und $v(a^{-1}) = -v(a)$ für alle $a \in L^\times$.
2. Für jede Einheitswurzel $z \in L$ ist $v(z) = 0$.
   Beweis. Ist $n \in \mathbb{N}$ mit $z^n = 1$, so folgt $0 = v(z^n) = nv(z)$ und daher $v(z) = 0$. $\square$
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. Aus $v(a+b) > v(a)$ folgte $v(a) = v((a+b)+(-b)) \geq \min\{v(a+b),\, v(b)\} > v(a)$, ein Widerspruch. $\square$
5. Sei $n \in \mathbb{N}_{\geq 2}$, und seien $a_1, \ldots, a_n \in L$.
   (a) Ist $v(a_1) < v(a_i)$ für alle $i \in [2,n]$, so ist $v(a_1 + \ldots + a_n) = v(a_1)$
   Beweis. Es ist $v(a_2 + \ldots + a_n) \geq \min\{v(a_2, \ldots, v(a_n)\} > v(a_1)$, und daher folgt $v(a_1 + (a_2 + \ldots + a_n)) = v(a_1)$. $\square$
   (b) Ist $a_1 + \ldots + a_n = 0$, so gibt es Indizes $i,\, j \in [1,n]$ mit $i \neq j$ und $v(a_i) = v(a_j)$.
   Beweis. Sind $v(a_1), \ldots, v_(a_n)$ alle verschieden, so können wir (nach Umnummerierung) annehmen, dass $v(a_1) < v(a_i)$ für alle $i \in [2,n]$, und nach (a) folgt dann $\infty = v(a_1 + \ldots + a_n) = v(a_1)$, ein Widerspruch. $\square$

Satz 3.5.3. *Sei L ein Körper und v eine diskrete Bewertung von L.*

1. *$\mathcal{O}_v$ ist ein diskreter Bewertungsbereich mit maximalem Ideal P_v. Es ist $\mathsf{q}(\mathcal{O}_v) = L$, und $\mathcal{O}_v^\times = \{x \in L \mid v(x) = 0\}$.*
2. *Für $t \in L$ sind die folgenden Aussagen äquivalent:*
   (a) *t ist ein Primelement von $\mathcal{O}_v$;*
   (b) *$P_v = (t)$;*
   (c) *$v(t) = 1$.*
3. *Ist K ein Teilkörper von L, so ist genau dann $v \mid K^\times = 0$, wenn $K \subset \mathcal{O}_v$.*

BEWEIS. 1. Sind $a, b \in \mathcal{O}_v$, so ist $v(a-b) \geq \min\{v(a), v(b)\} \geq 0$ 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 $L = \mathsf{q}(\mathcal{O}_v)$. 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 ist $v(a-b) \geq \min\{v(a), v(b)\} > 0$ und $v(ca) = v(c)+v(a) > 0$, also $a - b \in P_v$ und $ca \in P_v$. Daher ist P_v ein Ideal von $\mathcal{O}_v$, und wegen $P_v = \mathcal{O}_v \setminus \mathcal{O}_v^\times$ ist $\mathcal{O}_v$ lokal mit maximalem Ideal P_v.

Sei nun $t \in L$ mit $v(t) = 1$. Wir zeigen, dass jedes $a \in \mathcal{O}_v^\bullet$ eine eindeutige Darstellung $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in \mathcal{O}_v^\times$ besitzt (dann ist $\mathcal{O}_v$ ein diskreter Bewertungsbereich und t ist bis auf Assoziierte sein einziges Primelement). Sei also $a \in \mathcal{O}_v^\bullet$. Dann ist $v(a) = n \in \mathbb{N}_0$, und es folgt $v(t^{-n}a) = -nv(t) + v(a) = 0$, also $u = t^{-n}a \in \mathcal{O}_v^\times$ 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 $v(a) = nv(t) + v(u) = n$.

2. (a) $\Leftrightarrow$ (b) Nach Satz 3.2.2.2.

(b) $\Rightarrow$ (c) Wegen $P_v = (t) = t\mathcal{O}_v$ ist $v(x) \geq v(t)$ für alle $x \in P_v$, und da v surjektiv ist, folgt $v(t) = \min\{v(x) \mid x \in P_v\} = 1$.

(c) $\Rightarrow$ (b) Nach Definition ist $t \in P_v$, also $(t) \subset P_v$. Ist $a \in P_v^\bullet$, so ist $v(a) \geq 1$ und daher $v(t^{-1}a) = -v(t) + v(a) \geq 0$. Es folgt $t^{-1}a \in \mathcal{O}_v$ und $a \in t\mathcal{O}_v = (t)$.

3. Sei K ein Teilkörper von L. Genau dann ist $K \subset \mathcal{O}_v$, wenn $K^\times \subset \mathcal{O}_v^\times$, und das ist äquivalent mit $v \mid K^\times = 0$. □

Satz und Definition 3.5.4. *Sei R ein faktorieller Bereich, $L = \mathsf{q}(R)$ und $t \in R^\bullet$ ein Primelement. Dann hat jedes $x \in L^\times$ eine Darstellung $x = t^n u^{-1} v$ mit $n \in \mathbb{Z}$ und $u, v \in R \setminus (t)$. Dabei hängt $n = v_t(x)$ nur von x und dem Primideal (t) ab. Setzt man noch $v_t(0) = \infty$, so ist $v_t \colon L \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung und $v_t(t) = 1$.*

$v_t \colon L \to \mathbb{Z} \cup \{\infty\}$ heißt *t-adische Bewertung* von L. Für $x \in L$ heißt $v_t(x)$ der *t-adische Wert* von x.

Es ist $\mathcal{O}_{v_t} = \{u^{-1}c \mid c \in R,\ u \in R \setminus (t)\}$, $P_{v_t} = \{u^{-1}c \mid c \in (t),\ u \in R \setminus (t)\}$, $R \subset \mathcal{O}_{v_t}$, und $P_{v_t} \cap R = (t) \lhd R$. Die Einbettung $R \hookrightarrow \mathcal{O}_{v_t}$ induziert einen Ringmonomorphismus

$$j \colon R/(t) \to \mathcal{O}_{v_t}/P_{v_t}, \quad \text{so dass} \quad j(a + (t)) = a + P_{v_t S} \quad \text{für alle } a \in R.$$

Identifiziert man $R/(t)$ mit seinem Bild unter j, so ist $R/(t) \subset \mathcal{O}_{v_t}/P_{v_t}$ ein Teilring, und $\mathcal{O}_{v_t}/P_{v_t} = \mathsf{q}(R/(t))$. Ist insbesondere R ein Hauptidealbereich, so ist $R/(t) = \mathcal{O}_{v_t}/P_{v_t}$.

BEWEIS. Da R faktoriell ist, ist jedes $a \in R^\bullet \setminus R^\times$ ein Produkt von Primelementen, und dabei können wir zu t assoziierte Primelemente zusammenfassen. Dann hat jedes $a \in R^\bullet$ eine Darstellung $a = t^n u p_1 \cdot \ldots \cdot p_r$ mit $n \in \mathbb{N}_0$, $u \in R^\times$, $r \in \mathbb{N}_0$ und zu t nicht assoziierten

Primelementen $p_1, \ldots, p_r$. Insbesondere ist dann $t \nmid up_1 \cdot \ldots \cdot p_r$, und daher hat jedes $a \in R^\bullet$ eine Darstellung $a = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in R \setminus (t)$. Ist $x \in L^\times$, so ist $x = a^{-1}b$ mit $a, b \in R^\bullet$, $a = t^n u$ und $b = t^m v$ mit $n, m \in \mathbb{N}_0$ und $u, v \in R \setminus (t)$, und es folgt $x = t^{m-n}u^{-1}v$.

Zum Nachweis der Eindeutigkeit von n sei $t_1 \in R^\bullet$ ein weiteres Primelement, es sei $(t_1) = (t)$, also $t_1 = t\varepsilon$, und es sei $x = t^n u^{-1}v = t_1^{n_1}u_1^{-1}v_1$ mit $n, n_1 \in \mathbb{Z},\ n \geq n_1$ und $u, v, u_1, v_1 \in R \setminus (t)$. Dann folgt $t^n v u_1 = t_1^{n_1} v_1 u = t^{n_1}\varepsilon^{n_1} v_1 u$, also $t^{n-n_1} v u_1 = \varepsilon^{n_1} v_1 u \notin (t)$ und daher $n = n_1$.

Nach Definition ist $v_t(t) = 1,\ v_t \colon L \to \mathbb{Z} \cup \{\infty\}$ surjektiv, und genau dann $v_t(x) = \infty$, wenn $x = 0$. Für $a \in R$ ist $v_t(a) \geq 0$, und genau dann ist $v_t(a) > 0$, wenn $a \in (t)$. Wir zeigen nun:

$$v_t(x_1x_2) = v_t(x_1) + v_t(x_2) \quad \text{und} \quad v_t(x_1 + x_2) \geq \min\{v_t(x_1), v_t(x_2)\} \quad \text{für alle } x_1, x_2 \in L.$$

Ist $x_1x_2 = 0$, so ist nichts zu zeigen. Sei also $x_i = t^{n_i}u_i^{-1}v_i$ mit $n_i = v_t(x_i) \in \mathbb{Z},\ u_i, v_i \in R \setminus (t)$ für $i \in \{1, 2\}$ und $n_1 \geq n_2$. Dann folgt $x_1x_2 = t^{n_1+n_2}(u_1u_2)^{-1}v_1v_2$ und $u_1u_2v_1v_2 \notin (t)$, also $v_t(x_1x_2) = n_1 + n_2$. Es ist $x_1 + x_2 = t^{n_2}(u_1u_2)^{-1}w$ mit $w = t^{n_1-n_2}u_2v_1 + u_1v_2 \in R$ und daher $v_t(x_1 + x_2) = n_2 + v_t(w) \geq n_2$.

Ist $x \in \mathcal{O}_{v_t}$ und $v_t(x) = n \geq 0$, so ist $x = u^{-1}(t^n v)$ mit $u, v \in R \setminus (t)$ und $c = t^n v \in R$. Ist umgekehrt $x = u^{-1}c$ mit $u \in R$ und $c \in R \setminus (t)$, so ist $v_t(x) = v_t(c) - v_t(u) = v_t(c) \geq 0$ und daher $x \in \mathcal{O}_{v_t}$. Ist $x = u^{-1}c \in \mathcal{O}_{v_t}$ mit $c \in R$ und $u \in R \setminus (t)$, so ist wegen $v_t(x) = v_t(c)$ genau dann $x \in P_{v_t}$, wenn $v_t(c) \geq 1$, also $c \in (t)$. Daher ist $\mathcal{O}_{v_t} = \{u^{-1}c \mid c \in R,\ u \in R \setminus (t)\}$ und $P_{v_t} = \{u^{-1}c \mid c \in (t)$. Für alle $x \in R^\bullet$ ist $x = t^n u$ mit $n \in \mathbb{N}_0$ und $u \in R \setminus (t)$, also $x \in \mathcal{O}_{v_t}$, und genau dann ist $x \in P_{v_t}$, wenn $n > 0$. Damit folgt $R \subset \mathcal{O}_{v_t},\ P_{v_t} \cap R = (t)$, und die Einlagerung $R \hookrightarrow \mathcal{O}_{v_t}$ induziert einen Ringmonomorphismus $j \colon R/(t) \to \mathcal{O}_{v_t}/P_{v_t}$. Identifiziert man $R/(t)$ mit dem Bild unter j, so gilt für $\xi = u^{-1}c + P_{v_t} \in \mathcal{O}_{v_t}/P_{v_t}$ (mit $c \in R$ und $u \in R \setminus (t)$, also $u + (t) \in (R/(t))^\bullet$)

$$\xi = \frac{c + P_{v_t}}{u + P_{v_t}} = \frac{c + (t)}{u + (t)} \in \mathfrak{q}(R/(t)).$$

Es folgt $\mathcal{O}_{v_t}/P_{v_t} = \mathfrak{q}(R/(t))$. Ist R ein Hauptidealbereich, so ist (t) ein maximales Ideal, also $R/(t)$ ein Körper und daher $\mathcal{O}_{v_t}/P_{v_t} = R/(t)$. □

.

Korollar 3.5.5. *Sei L ein Körper.*

1. *Seien $v, v' \colon L \to \mathbb{Z} \cup \{\infty\}$ diskrete Bewertungen mit $\mathcal{O}_v = \mathcal{O}_{v'}$. Dann ist $v = v'$.*
2. *Sei $v \colon L \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung und $t \in L$ mit $v(t) = 1$. Dann ist $v = v_t$.*
3. *Sei R ein Hauptidealbereich, $L = \mathfrak{q}(R)$ und $v \colon L \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung mit $R \subset \mathcal{O}_v$. Dann gibt es ein Primelement t von R mit $v = v_t$.*
4. *Sei $\mathcal{O}$ ein diskreter Bewertungsbereich und $t \in \mathcal{O}$ ein Primelement. Dann ist $\mathcal{O} = \mathcal{O}_{v_t}$.*

Beweis. 1. Ist $\mathcal{O}_v = \mathcal{O}_{v'}$, so ist $P_v = P_{v'} = (t)$ mit $t \in L$ und $v(t) = v'(t) = 1$. Ist nun $x \in L^\times$, so folgt $x = t^n u$ mit $n \in \mathbb{Z}$ und $u \in \mathcal{O}_v^\times = \mathcal{O}_{v'}^\times$, also $v(x) = n = v'(x)$.

2. t ist ein Primelement von $\mathcal{O}_v$, und daher ist $v_t(x) \geq 0$ für alle $x \in \mathcal{O}_v$. Damit folgt $\mathcal{O}_v \subset \mathcal{O}_{v_t}$, also $\mathcal{O}_v = \mathcal{O}_{v_t}$ nach Satz 3.2.2.2, und daher $v = v_t$ nach 1.

3. Wäre $P_v \cap R = \{0\}$, so folgte $v(x) = 0$ für alle $x \in R^\bullet$ und daher $v(x) = 0$ für alle $x \in L^\times$, ein Widerspruch. Daher ist $P_v \cap R$ ein von $\{0\}$ verschiedenes Primideal von R, also $P_v \cap R = (t)$ mit einem Primelement t von R, und es folgt $R \setminus (t) \subset \mathcal{O}_v \setminus P_v = \mathcal{O}_v^\times$. Ist $x \in \mathcal{O}_{v_t}$, so ist $x = u^{-1}c$ mit $c \in R$ und $u \in R \setminus (t)$, und wir erhalten $v(x) = v(c) - v(u) = v(c) \geq 0$, also $x \in \mathcal{O}_v$. Wegen $\mathcal{O}_{v_t} \subset \mathcal{O}_v$ folgt $\mathcal{O}_v = \mathcal{O}_{v_t}$ nach Satz 3.2.2.2, und daher $v = v_t$ nach 1.

4. Wegen $\mathcal{O} \subset \mathcal{O}_{v_t}$ folgt Gleichheit nach Satz 3.2.2.2. □

Satz 3.5.6 (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) $\{x \in L \mid v(x) \geq 0\} \subset \{x \in L \mid v'(x) \geq 0\}$.
(e) $\{x \in L \mid v(x) > 0\} \subset \{x \in L \mid v'(x) > 0\}$.

Beweis. (a) $\Rightarrow$ (b) $\Leftrightarrow$ (d) und (a) $\Rightarrow$ (c) $\Leftrightarrow$ (e) Offensichtlich.

(b) $\Rightarrow$ (a) Nach Satz 3.2.2.2 und Korollar 3.5.5.

(e) $\Rightarrow$ (d) 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 $t \in L$ mit $v(t) = 1$. Dann ist $v'(t) = r > 0$, $v(x^r t) = rv(x) + v(t) = 1$ und

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

Satz 3.5.7 (Schwacher Approximationssatz)**.** *Sei L ein Körper, $n \in \mathbb{N}$, und seien $v_1, \ldots, v_n$ verschiedene diskrete Bewertungen von L. Seien $(x_1, \ldots, x_n) \in L^n$ und $(r_1, \ldots, r_n) \in \mathbb{Z}^n$. 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 3.5.6 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 $v_2(u_1^{-1}u_2) = -v_2(u_1) + v_2(u_2) < 0$.

$n \geq 3,\ n - 1 \to n$: 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 $v_i(u) = \min\{v_i(y),\ rv_i(z)\} < 0$. □[**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 $s \gg 1$. □[**B**]

C. Für alle $(y_1, \ldots, y_n) \in L^n$ 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 $(y_1, \ldots, y_n) \in L^n$ und $s \in \mathbb{Z}$, so dass $v_i(y_j) \geq s$ für alle $i,\ j \in [1, n]$. Nach **B** gibt es $w_1, \ldots, w_n \in L$, 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 $z = y_1w_1 + \ldots + y_nw_n$. Für alle $i \in [1, n]$ folgt dann

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

Für $j \in [1, n]$ mit $j \neq i$ ist $v_i(y_jw_j) > s + (r_i - s) = r_i$, und daher ist auch $v_i(z - y_i) > r_i$. □[**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 $v_i(x - x_i) = v_i\big((z - x_i) + (z' - z_i) + z_i\big) = \min\{v_i(z - x_i),\, v_i(z' - z_i),\, v_i(z_i)\} = r_i$. □

3.6. Stellen eines Funktionenkörpers

Definition 3.6.1. 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 3.2.2 ist dann $\mathcal{O}$ ein diskreter Bewertungsbereich und $P = (t)$ ist ein Hauptideal von $\mathcal{O}$. Nach Korollar 3.5.5 ist $v = v_t$, also $\mathcal{O} = \mathcal{O}_v$ und $P = \mathcal{P}_v$. Nach Satz 3.5.3 ist $v \,|\, K^\times = 0$, und nach Satz 3.5.6 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. Jedes Primelement t von $\mathcal{O}_P$ heitß *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 $\widetilde{K}$ der Konstantenkörper von L/K und $P \in \mathbb{P}_L$. Nach Satz 3.3.1 ist $\widetilde{K} \subset \mathcal{O}_P$ und $P \cap \widetilde{K} = \mathbf{0}$. Die Einbettung $\widetilde{K} \hookrightarrow \mathcal{O}_P$ induziert einen K-Monomorphismus $\widetilde{K} \to L_P$, wir identifizieren die Elemente $a \in \widetilde{K}$ mit den Restklassen $a + P \in L_P$, und betrachten fürderhin $\widetilde{K}$ als in L_P eingebettet. Dann ist $K \subset \widetilde{K} \subset L_P$, und wir nennen $\deg(P) = [L_P : K]$ den *Grad* von P (in Satz 3.6.3 werden wir $\deg(P) < \infty$ zeigen). 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

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

und wir nennen $z(P)$ den *Wert* der Funktion z an der Stelle P. Aufgrund der Einbettung $\widetilde{K} \hookrightarrow L_P$ ist $z(P) = z$ für alle $z \in \widetilde{K}$ und alle $P \in \mathbb{P}_L$ (das rechtfertigt die Terminologie *Konstantenkörper*). Die Abbildung $z \mapsto z(P)$ ist ein $\widetilde{K}$-Algebrenepimorphismus $\mathcal{O}_P \to L_P$. 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.

Sei $z \in L$ und $P \in \mathbb{P}_{L/K}$. Man nennt P eine *Nullstelle* von z, wenn $z(P) = 0$ [äquivalent: $z \in P$ oder $v_P(z) > 0$], und dann heißt $v_P(z)$ die *Nullstellenordnung* von z in P. Man nennt P eine *Polstelle* von z, wenn $z(P) = \infty$ [äquivalent: $z \in L \setminus \mathcal{O}_P$ oder $v_P(z) < 0$], und dann heißt $-v_P(z)$ 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. Für $z \in L^\times$ ist offensichtlich $\mathcal{P}(z) = \mathcal{N}(z^{-1})$.

Satz 3.6.2. *Sei L/K ein Funktionenkörper, $R \subset L$ ein Bereich mit $K \subset R$ und $\mathbf{0} \neq I \subsetneq R$ ein Ideal. Dann gibt es eine Stelle $P \in \mathbb{P}_L$ mit $R \subset \mathcal{O}_P$ und $I \subset P$.*

Beweis. Nach Satz 3.2.3. □

Satz 3.6.3. *Sei L/K ein Funktionenkörper mit Konstantenkörper $\widetilde{K}$.*

1. *Sei $x \in L \setminus \widetilde{K}$, $r \in \mathbb{N}$, und seien $P_1, \ldots, P_r \in \mathbb{P}_L$ 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* $[\widetilde{K} : K] \leq \deg(P) \leq [L : K(x)] < \infty$. *Ist insbesondere* $\mathbb{P}_L^1 \neq \emptyset$, *so ist* $\widetilde{K} = K$.
3. *Für* $x \in L \setminus \widetilde{K}$ *ist* $0 < |\mathcal{N}(x)| \leq [L:K(x)] < \infty$ *und* $0 < |\mathcal{P}(x)| \leq [L:K(x)] < \infty$.
4. *Sei* $x \in L^\times$. *Dann ist die Menge* $\{P \in \mathbb{P}_L \mid v_P(x) \neq 0\}$ *endlich, und genau dann ist* $x \in \widetilde{K}^\times$, *wenn* $v_P(x) = 0$ *für alle* $P \in \mathbb{P}_L$.
5. $|\mathbb{P}_L| = \infty$.

Beweis. Nach Satz 3.1.4 ist $[L:K(x)] < \infty$. Für $i \in [1,r]$ sei $v_i = v_{P_i}$, $e_i = v_i(x)$, also $e_i \geq 1$, da $x \in P_i$, und $f_i \in \mathbb{N}$ mit $f_i \leq \deg(P_i)$. Seien $s_{i,1}, \ldots, s_{i,f_i} \in \mathcal{O}_{P_i}$, so dass die Werte $s_{i,1}(P_i), \ldots, s_{i,f_i}(P_i) \in L_{P_i}$ über K linear unabhängig sind. Nach Satz 3.5.7 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 $v_i(s_{i,j} - z_{i,j}) > 0$ und $v_k(z_{i,j}) \geq e_k$ 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 $v_i(z_{i,j}) \geq 0$. Wir zeigen:

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

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

Beweis von **A.** 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). Wir fixieren einen Index $k \in [1,r]$, fr den es ein $c \in [0,e_k-1]$ und ein $j \in [1,f_k]$ gibt, so dass $\varphi_{k,j,c} \notin xK[x]$, und es sei $c \in [0,e_k-1]$ minimal mit dieser Eigenschaft. Dann folgt $\varphi_{k,j,a} \in xK[x]$ für alle $a \in [0,c-1]$ und $j \in [1,f_k]$, es 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 $v_k(\varphi_{k,j,a}) \geq e_k$, 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

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

da $v_k(z_{k,j} - s_{k,j}) > 0$ für alle $j \in [1,f_k]$. 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 auch $\varphi_{k,j,c} = a_j + x\psi_j = x\psi_j \in xK[x]$ für alle $j \in [1,k]$, ein Widerspruch.

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

3. Ist $x \in L^\times$, so ist $\mathcal{P}(x) = \mathcal{N}(x^{-1})$ und $K(x) = K(x^{-1})$. 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.

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

und daher $|\mathcal{N}(x)| \le [L\colon K(x)]$. Ist $x \in L \setminus \widetilde{K}$, so ist $\mathbf{0} \ne xK[x] \subsetneq K[x]$ ein Ideal, und nach Satz 3.6.2 gibt es eine Stelle $P \in \mathbb{P}_L$ mit $x \in P$ und daher $P \in \mathcal{N}(x)$.

4. Für jedes $x \in L^\times$ ist die Menge $\{P \in \mathcal{P}_L \mid v_P(x) \ne 0\} = \mathcal{N}(x) \cup \mathcal{P}(x)$ 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 $x \in \widetilde{K}^\times$. Ist umgekehrt $x \in \widetilde{K}^\times$, so folgt $x \in \mathcal{O}_P^\times$ und daher $v_P(x) = 0$ für alle $P \in \mathbb{P}_L$ nach Satz 3.3.1.

5. Nach 3. ist $\mathbb{P}_L \ne \emptyset$. Wir nehmen an, es sei $\mathbb{P}_L = \{P_1, \dots, P_r\}$ mit $r \in \mathbb{N}$. Nach Satz 3.5.7 gibt es ein $z \in L$ mit $v_{P_i}(z) > 0$ für alle $i \in [1, r]$. Dann ist aber $z \notin \widetilde{K}$ und $\mathcal{P}(z) = \emptyset$, ein Widerspruch. □

Satz 3.6.4. *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 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. □

3.7. Die Stellen des rationalen Funktionenkörpers

Definition und Bemerkung 3.7.1. Sei K ein Körper und $L = K(x)$ ein rationaler Funktionenkörper. Dann ist $L = \mathfrak{q}(K[x])$, und $K[x] \cong K[X]$ ist ein Hauptidealbereich. Zur Beschreibung von $\mathbb{P}_{K(x)}$ bestimmen wir alle diskreten Bewertungen $v\colon K(x) \to \mathbb{Z} \cup \{\infty\}$ mit $v \mid K^\times = 0$.

Sei also $v\colon K(x) \to \mathbb{Z} \cup \{\infty\}$ eine diskrete Bewertung von $K(x)$ mit $v \mid K^\times = 0$.

FALL 1: $v(x) \ge 0$. Dann ist $K[x] \subset \mathcal{O}_v$, und nach Satz 3.5.4 gibt es ein Primelement $t \in K[x]$ mit $v = v_t$. Dann ist $t = p(x)$ für ein (eindeutig bestimmtes) normiertes irreduzibles Polynom $p \in K[X]$, wir setzen $v_p = v_t$, $\mathcal{O}_p = \mathcal{O}_{v_p}$, und $P_p = P_{v_p} \in \mathbb{P}_{K(x)}$. Explizit ist

$$\mathcal{O}_p = \Big\{ \frac{g(x)}{h(x)} \;\Big|\; g,\, h \in K[X],\ p \nmid h \Big\} \quad \text{und} \quad P_p = \Big\{ \frac{g(x)}{h(x)} \;\Big|\; g,\, h \in K[X],\ p \mid g,\ p \nmid h \Big\}.$$

Nach Satz 3.5.4 ist $K(x)_p = K(x)_{P_p} = \mathcal{O}_p/P_p \cong K[x]/(p(x)) \cong K[X]/(p) = K(\xi)$ mit $p(\xi) = 0$. Identifiziert man $K(x)_p = K(\xi)$ vermöge $x + P_p = \xi$, so gilt für alle $z \in \mathcal{O}_p$:

$$\text{Ist} \quad z = \frac{g(x)}{h(x)} \ \text{ mit } \ g,\, h \in K[X] \ \text{ und } \ p \nmid h, \ \text{ also } \ h(\xi) \ne 0, \quad z(P_p) = \frac{g(\xi)}{h(\xi)}.$$

Es ist $\deg(P_p) = [K(\xi)\colon K] = \operatorname{gr}(p)$.

Für $c \in K$ sei $p_c = X - c$ und $P_c = P_{p_c}$. Dann ist $K(x)_{P_c} = K$, also $\deg(P_c) = 1$, und für

$$z = \frac{g(x)}{h(x)} \ \text{ mit } \ g,\, h \in K[X],\ h(c) \ne 0 \ \text{ ist } \ z(P_c) = z(c) = \frac{g(c)}{h(c)}.$$

Wegen $\mathbb{P}^1_{K(x)} \neq \emptyset$ ist K der Konstantenkörper von $K(x)$, also K relativ algebraisch abgeschlossen in $K(x)$.

FALL 2: $v(x) < 0$. Sei $t = x^{-1}$. Dann ist $K[t] \cong K[T]$, $K[t] \subset \mathcal{O}_v$, und daher ist $v = v_q$ mit einem Primelement $q \in K[t]$. Wegen $v(t) = -v(x) > 0$ ist $t \in (q)$, und da t ein Primelement von $K[t]$ ist, folgt $(t) = (q)$ und $v = v_t$. Wir zeigen nun:

$$\text{Ist } \; z = \frac{g(x)}{h(x)} \in K(x) \;\; \text{mit } \; g,\, h \in K[x]^\bullet, \;\; \text{so folgt } \; v_t(z) = \operatorname{gr}(g) - \operatorname{gr}(f).$$

Sei dazu

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

Dann ist

$$z = \frac{x^n(a_n + a_{n-1}x^{-1} + \ldots + a_0 x^{-n})}{x^m(b_m + b_{m-1}x^{-1} + \ldots + b_0 x^{-m})} = t^{m-n}\,\frac{a_n + a_{n-1}t + \ldots + a_0 t^n}{b_m + b_{m-1}t + \ldots + b_0 t^m} = t^{m-n}\frac{f_0}{g_0}$$

mit $f_0,\, g_0 \in K[t] \setminus (t)$, also $v_t(h) = m - n = \operatorname{gr}(h) - \operatorname{gr}(g)$.

Man nennt $v_\infty = v_t \colon K(x) \to \mathbb{Z} \cup \{\infty\}$ die *negative Gradbewertung* von $K(x)$ und $P_\infty = P_{v_t}$ die *unendliche Stelle* von $K(x)$ (bezüglich x).

Es ist $\deg(P_\infty) = 1$, $\mathcal{P}(x) = \{P_\infty\}$ und $\mathcal{N}(x) = \{P_0\}$

Damit haben wir folgenden Satz gezeigt:

Satz 3.7.2. *Sei K ein Körer und $K(x)$ ein rationaler Funktionenkörper über K. Dann ist*

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

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

3.8. Stellen und Punkte

Sei K ein vollkommener Körper, $\overline{K}$ eine algebraische Hülle und $G_K = \mathsf{Gal}(\overline{K}/K)$ die absolute Galoisgruppe von K.

Definition 3.8.1. Sei $\sigma \in G_K$. Für einen Punkt $p = (\alpha : \beta : \gamma) \in \mathbb{P}^2$ mit $(\alpha, \beta, \gamma) \in (\overline{K}^3)^\bullet$ definieren wir $\sigma(p) = (\sigma(\alpha) : \sigma(\beta) : \sigma(\gamma))$. Diese Definition ist unabhängig von der Wahl der projektiven Koordinaten, denn für $\lambda \in \overline{K}^\times$ ist $(\sigma(\lambda\alpha) : \sigma(\lambda\beta) : \sigma(\lambda\gamma)) = (\sigma(\alpha) : \sigma(\beta) : \sigma(\gamma))$. Wegen $\sigma(1) = 1$ lät σ die affinen Stücke von $\mathbb{P}^2$ invariant: Für alle $\nu \in [1, 3]$ ist $\sigma(\mathbb{P}^2(\nu)) = \mathbb{P}^2(\nu)$. Insbesondere gilt: Ist $p = (\alpha, \beta) = (\alpha : \beta : 1) \in \mathbb{A}^2$, so ist $\sigma(p) = (\sigma(\alpha) : \sigma(\beta) : 1) = (\sigma(\alpha), \sigma(\beta)$.

Zwei Punkte $p,\, p' \in \mathbb{P}^2$ heißen *K-äquivalent*, $p \sim_K p'$, wenn es ein $\sigma \in G_K$ gibt mit $p' = \sigma(p)$. $\sim_K$ ist eine Äquivalenzrelation auf $\mathbb{P}^2$ und auf $\mathbb{A}^2$, und

$$\mathbb{P}^2(K) = \{p \in \mathbb{P}^2 \mid \sigma(p) = p \text{ für alle } \sigma \in G_K\}.$$

Satz 3.8.2.

1. *Für zwei Punkte $p,\, p' \in \mathbb{A}^2$ sind die folgenden Aussagen sind äquivalent*:
   (a) $p \sim_K p'$.

(b) *Für alle* $f \in K[X,Y]$ *gilt: Genau dann ist* $f(p') = 0$*, wenn* $f(p) = 0$*.*

(c) *Für jede über* K *definierte Kurve* $C \subset \mathbb{A}^2$ *gilt: Genau dann ist* $p' \in C$*, wenn* $p \in C$*.*

2. *Für zwei Punkte* $p, p' \in \mathbb{P}^2$ *sind die folgenden Aussagen sind äquivalent:*
   (a) $p \sim_K p'$*.*
   (b) *Für jede über* K *definierte projektive Kurve* $\Gamma \subset \mathbb{P}^2$ *gilt: Genau dann ist* $p' \in \Gamma$*, wenn* $p \in \Gamma$*.*
3. *Sei* $\sigma \in G_K$*. Dann ist* $\sigma(C) = C$ *für jede über* K *definierte Kurve* $C \subset \mathbb{A}^2$ *und* $\sigma(\Gamma) = \Gamma$ *für jede über* K *definierte projektive Kurve* $\Gamma \subset \mathbb{P}^2$*.*

BEWEIS. 1. (a) $\Rightarrow$ (b) Sei $p = (\alpha, \beta)$ und $\sigma \in G_K$ mit $p' = \sigma(p) = (\sigma(\alpha), \sigma(\beta)$. Für jedes Polynom $f \in K[X,Y]$ ist dann $f(p') = f(\sigma(\alpha), \sigma(\beta)) = \sigma(f(\alpha, \beta)) = \sigma(f(p))$, also genau dann $f(p') = 0$, wenn $f(p) = 0$.

(b) $\Rightarrow$ (c) Offensichtlich.

(c) $\Rightarrow$ (a) Sei $p = (\alpha, \beta)$, $p' = (\alpha', \beta')$, und seien $\varphi, \varphi' \colon K[X,Y] \to \overline{K}$ definiert durch $\varphi(f) = f(p)$ und $\varphi'(f) = f(p')$. φ und φ' sind K-Algebrenhomomorphismen, $\mathrm{Bi}(\varphi) = K(\alpha, \beta)$, $\mathrm{Bi}(\varphi') = K(\alpha', \beta')$ und

$$J = \mathrm{Ker}(\varphi) = \{f \in K[X,Y] \mid p \in V(f)\} = \{f \in K[X,Y] \mid p' \in V(f)\} = \mathrm{Ker}(\varphi').$$

φ und φ' induzieren K-Isomorphismen

$$\varphi_1 \colon K[X,Y]/J \xrightarrow{\sim} K(\alpha, \beta) \quad \text{und} \quad \varphi_1' \colon K[X,Y]/J \xrightarrow{\sim} K(\alpha', \beta')$$

mit $\varphi_1(X + J) = \alpha$, $\varphi_1(Y + J) = \beta$, $\varphi_1'(X + J) = \alpha'$ und $\varphi_1'(Y + J) = \beta'$. Dann ist

$$\sigma_0 = \varphi_1' \circ \varphi_1^{-1} \colon K(\alpha, \beta) \to K(\alpha', \beta')$$

ein K-Isomorphismus mit $\sigma_0(\alpha) = \alpha'$ und $\sigma_0(\beta) = \beta'$. Ist $\sigma \in G_K$ mit $\sigma \mid K(\alpha, \beta) = \sigma_0$, so folgt $\sigma(p) = p'$ und daher $p \sim_K p'$.

2. (a) $\Rightarrow$ (b) Sei $\Gamma = V_+(F) \subset \mathbb{P}^2$ mit einer Form $F \in K[X,Y,Z]$ und $p = (\alpha : \beta : \gamma) \in \Gamma$. Sei $\sigma \in G_K$ mit $p' = \sigma(p) = (\sigma(\alpha) : \sigma(\beta) : \sigma(\gamma))$. Dann ist $F(\sigma(\alpha), \sigma(\beta), \sigma(\gamma)) = \sigma(F(\alpha, \beta, \gamma))0$, also $F(p') = 0$ und damit $p' \in \Gamma$ genau dann, wenn $F(p) = 0$ und damit $p \in \Gamma$.

(b) $\Rightarrow$ (a) Sei $p = (\alpha : \beta : \gamma)$, $p' = (\alpha' : \beta' : \gamma')$, und sei $\gamma \neq 0$. Dann ist $p \notin V_+(Z)$, also auch $p' \notin V_+(Z)$ und $\gamma' \neq 0$. Daher können wir $\gamma = \gamma' = 1$ annehmen, und nach 1. genügt es, zu zeigen: Für jede über K definierte Kurve $C \subset \mathbb{A}^2$ gilt: Genau dann ist $p = (\alpha, \beta) = (\alpha : \beta : 1) \in C$, wenn $p' = (\alpha', \beta') = (\alpha' : \beta' : 1) \in C$. Sei also $C \subset \mathbb{A}^2$ eine über K definierte Kurve und $\overline{C} \subset \mathbb{P}^2$ ihr projektiver Abschluss. Wegen $C = \overline{C} \cap \mathbb{A}^2$ ist genau dann $p' \in C$, wenn $p \in C$.

3. Offensichtlich nach 1. und 2. □

Satz 3.8.3. *Sei* $C \subset \mathbb{A}^2$ *eine über* K *definierte irreduzible Kurve.*

1. *Für* $p \in C$ *sei* $\pi_p \colon K[C] \to \overline{K}$ *definiert durch* $\pi_p(\varphi) = \varphi(p)$ *für alle* $\varphi \in K[C]$*. Dann ist* $\mathrm{Ker}(\pi_{\boldsymbol{p}}) = \mathcal{M}_{p,K}(C) \cap K[C]$ *ein maximales Ideal von* $K[C]$*, und zu jedem maximalen Ideal* $\mathfrak{m}$ *von* $K[C]$ *gibt es einen Punkt* $p \in C$ *mit* $\mathfrak{m} = \mathrm{Ker}(\pi_p) = \mathcal{M}_{p,K}(C) \cap K[C]$*.*
2. *Für zwei Punkte* $p, p' \in C$ *ist genau dann* $\mathcal{O}_{p,K}(C) = \mathcal{O}_{p',K}(C)$*, wenn* $p \sim_K p'$*.*
3. *Die Zuordnung* $p \mapsto \mathcal{M}_{p,K}(C) \cap K[C]$ *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. Für $p \in C$ ist π_p nach Satz 1.4.8 ist π_p ein K-Algebrenhomomorphismus, $\mathrm{Bi}(\pi_p) = K[\alpha,\beta] = K(\alpha,\beta)$ ist ein Körper, und daher ist $\mathrm{Ker}(\pi_{\boldsymbol{p}}) = \mathcal{M}_{\boldsymbol{p},K}(C) \cap K[C]$ ein maximales Ideal von $K[C]$.

Sei nun $\mathfrak{m}d$ ein maximales Ideal von $\max(K[C])$ und seien x, $y \in K[C]$ die Koordinatenfunktionen. Dann ist $K[C]/\mathfrak{m} = K[x+\mathfrak{m}, y+\mathfrak{m}]$ ein Körper, nach Satz 3.6.4 ist $K[C]/K$ algebraisch, und daher gibt es einen K-Homomorphismus $\sigma\colon K[C] \to \overline{K}$. Sei $\pi\colon K[C] \to \overline{K}$ definiert durch $\pi(\varphi) = \sigma(\varphi+\mathfrak{m})$, und sei $\alpha = \pi(x)$, $\beta = \pi(y)$. π ist ein K-Algebrenhomomorphismus, $\mathrm{Ker}(\pi) = \mathfrak{m}$, wegen $f(\alpha,\beta) = \pi(f(x,y)) = 0$ ist $p = (\alpha,\beta) \in C$. Ist $\varphi = g(x,y) \in K[C]$ mit $g \in K[X,Y]$, so folgt $\pi(\varphi) = g(\pi(x),\pi(y)) = g(\alpha,\beta) = \varphi(p)$. Daher ist $\pi = \pi_p$ und $\mathfrak{m} = \mathrm{Ker}(\pi_p)$.

2. Sei $\mathfrak{I}_K(C) = (f) \lhd K[X,Y]$ mit irreduziblem $f \in K[X,Y]$, und seien p, $p' \in C$. Ist $p \sim_K p'$, so folgt

$$\begin{aligned}\mathcal{O}_{p,K}(C) &= \left\{ \frac{g+(f)}{h+(f)} \;\middle|\; g,\, h \in K[X,Y]\,,\ h(p) \neq 0 \right\} \\ &= \left\{ \frac{g+(f)}{h+(f)} \;\middle|\; g,\, h \in K[X,Y]\,,\ h(p') \neq 0 \right\} = \mathcal{O}_{p',K}(C)\,.\end{aligned}$$

Sei nun $\mathcal{O}_{p,K}(C) = \mathcal{O}_{p',K}(C)$. Nach Satz 3.8.2 genügt es, zu zeigen: Für jedes Polynom $h \in K[X,Y]$ mit $h(p) \neq 0$ ist auch $h(p') \neq 0$. Sei $h \in K[X,Y]$ und $h(p) \neq 0$. Dann ist

$$\frac{1}{h+(f)} \in \mathcal{O}_{p,K}(C) = \mathcal{O}_{p',K}(C)\,, \quad \text{also} \quad \frac{1}{h+(f)} = \frac{g_1+(f)}{h_1+(f)}$$

mit g_1, $h_1 \in K[X,Y]$ und $h_1(p') \neq 0$. Es folgt $hg_1 + (f) = h_1 + (f)$, also $h(p')g_1(p') = h_1(p') \neq 0$ und daher $h(p') \neq 0$.

3. Nach 1. definiert $p \mapsto \mathcal{M}_{p,K}(C) \cap K[C]$ eine surjektive Abbildung $C \to \max(K[C])$. Daher ist zu zeigen: Für p, $p' \in C$ ist genau dann $p \sim_K p'$, wenn $\mathcal{M}_{p,K}(C) \cap K[C] = \mathcal{M}_{p',K}(C) \cap K[C]$.

Sind p, $p' \in C$ mit $p \sim_K p'$, so folgt $\mathcal{O}_{p,K}(C) = \mathcal{O}_{p',K}(C)$, also $\mathcal{M}_{p,K}(C) = \mathcal{M}_{p',K}(C)$ und daher $\mathcal{M}_{p,K}(C) \cap K[C] = \mathcal{M}_{p',K}(C) \cap K[C]$.

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

$$\begin{aligned}\mathcal{O}_{p,K}(C) &= \{\varphi^{-1}\psi \mid \psi \in K[C]\,,\ \varphi \in K[C] \setminus \mathcal{M}_{p,K}(C)\} \\ &= \{\varphi^{-1}\psi \mid \psi \in K[C]\,,\ \varphi \in K[C] \setminus \mathcal{M}_{p',K}(C)\} = \mathcal{O}_{p',K}(C), \quad \text{und daher } \ p \sim_K p'. \quad \square\end{aligned}$$

Lemma 3.8.4. *Sei $\Gamma \subset \mathbb{P}^2$ 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 2.5.4 besitzt Γ die affinen Stücke $C_1 = V_+(Z) \setminus V_+(X)$ und $C_2 = V_+(Z) \setminus V_+(Y)$, es ist $\hat{z} = 0$,

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

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

FALL 2: $\Gamma \notin \{V_+(X), V_+(Y), V_+(Z)\}$. Seien $C_1 = C \setminus V_+(X)$, $C_2 = C \setminus V_+(Y)$ und $C_3 = C \setminus V_+(Z)$ die affinen Stücke von C. Dann ist nach Bemerkung 2.5.4

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

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

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

und

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

also in jedem Fall $K[C_3] \subset \mathcal{O}_P$. □

Definition 3.8.5. Seien R und R' lokale Ringe mit maximalen Idealen $P = R \setminus R^\times$ und $P' = R' \setminus R'^\times$. Man sagt, R' *dominiert* R und schreibt $R \prec R'$, wenn $R \subset R'$ und $P \subset P'$.

Satz 3.8.6. *Sei $\Gamma \subset \mathbb{P}^2$ eine über K definierte irreduzible projektive Kurve.*

1. *Sei $p \in \Gamma$.*
   (a) *Es gibt eine Stelle $P \in \mathbb{P}_{K(\Gamma)/K}$ mit $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$, und für jede solche Stelle P ist $\mathcal{M}_{p,K}(\Gamma) = P \cap \mathcal{O}_{p,K}(\Gamma)$. Ist $p \in \Gamma(K)$ regulär, so ist $\mathcal{M}_{p,K}(\Gamma) = P \in \mathbb{P}^1_{K(\Gamma)}$ und $\mathcal{O}_{p,K}(\Gamma) = \mathcal{O}_P$.*
   (b) *Sei $p = (\alpha, \beta) \in \Gamma \cap \mathbb{A}^2$ und $P \in \mathbb{P}_{K(\Gamma)}$ mit $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$. Dann induziert die Einbettung $\mathcal{O}_{p,K}(\Gamma) \hookrightarrow \mathcal{O}_P$ einen K-Monomorphismus*
   $$K(\alpha, \beta) = \mathcal{O}_{p,K}(\Gamma)/\mathcal{M}_{p,K}(\Gamma) \to K(C)_P = \mathcal{O}_P/P.$$
   Wir identifizieren: $K(\alpha, \beta) \subset K(C)_P$. Insbesondere ist $[K(\alpha, \beta) : K] \leq \deg(P)$, mit Gleichheit, falls $\mathcal{O}_{p,K}(\Gamma) = \mathcal{O}_P$.
2. *Zu jeder Stelle $P \in \mathbb{P}_{K(\Gamma)}$ gibt es einen bis auf K-Konjugierte eindeutig bestimmten Punkt $p \in \Gamma$, so dass $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$. Ist C ein affines Stück von Γ, so ist genau dann $p \in C$, wenn $K[C[\subset \mathcal{O}_P$.*
3. *Ist Γ regulär, so definiert die Zuordnung $p \mapsto \mathcal{M}_{p,K}(\Gamma)$ eine Bijektion $\Psi\colon \Gamma(K) \to \mathbb{P}^1_{K(\Gamma)}$.*

BEWEIS. *Vorbemerkung.* Ist $C = \mathbb{A}^2 \cap \Gamma$ ein affines Stück von Γ, so ist C nach Satz 2.3.10 eine über K definierte irreduzible Kurve, $\Gamma = \overline{C}$, und nach Satz 2.5.2 ist $K(C) = K(\Gamma)$, $\mathcal{O}_{p,K}(C) = \mathcal{O}_{p,K}(\Gamma)$ und $\mathcal{M}_{p,K}(C) = \mathcal{M}_{p,K}(\Gamma)$.

1. (a) Nach Satz 3.2.3 gibt es eine Stelle $P \in \mathbb{P}_{K(\Gamma)/K}$ mit $\mathcal{O}_{\boldsymbol{p},K}(\Gamma) \prec \mathcal{O}_P$. Ist P eine solche Stelle, so ist $\mathcal{M}_{p,K}(\Gamma) \subset P \cap \mathcal{O}_{p,K}(\Gamma)$, und da $\mathcal{M}_{p,K}(\Gamma)$ ein maximales Ideal von $\mathcal{O}_{p,K}(\Gamma)$ ist, folgt $\mathcal{M}_{p,K}(\Gamma) = P \cap \mathcal{O}_{p,K}(\Gamma)$.

Ist $p \in \Gamma(K)$ regulär, so ist $\mathcal{O}_{p,K}(\Gamma)$ ein diskreter Bewertungsbereich und daher nach Satz 3.2.2 ein maximaler Teilbereich von $K(\Gamma)$. Ist nun $P \in \mathbb{P}_{K(\Gamma)}$ mit $\mathcal{O}_{p,K}(\Gamma) \subset \mathcal{O}_P$, so folgt $\mathcal{O}_{\boldsymbol{p},K}(C) = \mathcal{O}_P$ und daher $\mathcal{M}_{\boldsymbol{p},K}(\Gamma) = P$. Da p in einem affinen Stück von Γ liegt, können wir $p = (\alpha, \beta) \in K^2$ annehmen, und dann folgt $\deg(P) = 1$ nach (b).

(b) $C = \Gamma \cap \mathbb{A}^2$ ist ein affines Stück von Γ. Nach Satz 1.4.8 ist $K(\alpha,\beta) = \mathcal{O}_{p,K}(\Gamma)/\mathcal{M}_{p,K}(\Gamma)$, und wegen $\mathcal{M}_{p,K}(\Gamma) = P \cap \mathcal{O}_{p,K}(\Gamma)$ induziert die Einbettung $\mathcal{O}_{p,K}(\Gamma) \hookrightarrow \mathcal{O}_P$ eine K-Monomorphismus $\varphi\colon \mathcal{O}_{p,K}(\Gamma)/\mathcal{M}_{p,K}(\Gamma) \to \mathcal{O}_P/P$. Ist $\mathcal{O}_{p,K}(\Gamma) = \mathcal{O}_P$, so ist φ ein Isomorphismus. Die weiteren Behauptungen sind nun offensichtlich.

2. Sei $P \in \mathbb{P}_{K(\Gamma)}$. Wir zeigen zunächst die folgenden Behauptungen:

A. Ist C ein affines Stück von Γ und $K[C] \subset \mathcal{O}_P$, so gibt es einen Punkt $p \in C$ mit $K[C] \cap P = \mathcal{M}_{p,K}(\Gamma) \cap P$ und $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$.

B. Sind p, $p' \in \Gamma$, so dass $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$ und $\mathcal{O}_{p',K}(\Gamma) \prec \mathcal{O}_P$, so ist $p \sim_K p'$.

Seien **A** und **B** gezeigt. Nach Lemma 3.8.4 gibt es ein affines Stück C von Γ, so dass $K[C] \subset \mathcal{O}_P$, nach **A** gibt es einen Punkt $p \in C$ mit $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$, und nach **B** ist dieser bis auf K-Konjugierte eindeutig bestimmt.

Sei nun $p \in \Gamma$, $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$, und sei C ein affines Stück von Γ, etwa $C = \Gamma \cap \mathbb{A}^2$. Ist $p \in C$, so folgt $K[C] \subset \mathcal{O}_{p,K}(\Gamma) \subset \mathcal{O}_P$. Ist umgekehrt $K[C] \subset \mathcal{O}_P$, so gibt es nach **A** eine Punkt $p' \in C$ mit $\mathcal{O}_{p',K}(\Gamma) \prec \mathcal{O}_P$, nach **B** ist $p' \sim_K p$, und daher auch $p \in \Gamma \cap \mathbb{A}^2 = C$. □

Beweis von **A.** Sei C ein affines Stück von Γ, etwa $C = \Gamma \cap \mathbb{A}^2$. Dann ist $K(\Gamma) = K(C)$, $\mathcal{O}_{p,K}(\Gamma) = \mathcal{O}_{p,K}(C)$ und $\mathcal{M}_{p,K}(\Gamma) = \mathcal{M}_{p,K}(C)$. Seien x, y die Koordinatenfunktionen von C, und sei $K[C] = K[x,y] \subset \mathcal{O}_P$. Sei nun $\pi\colon K[C] \hookrightarrow \mathcal{O}_P \to \mathcal{O}_P/P = K(C)_P$ definiert durch $\pi(\varphi) = \varphi(P) \in K(C)_P$ für alle $\varphi \in K[C]$. Dann ist $\mathrm{Bi}(\pi) = K[x(P), y(P)] \subset K(C)_P$, und wegen $[K(C)_P : K] = \deg(P) < \infty$ sind $x(P)$ und $y(P)$ algebraisch über K. Daher ist $\mathrm{Bi}(\pi)$ ein Körper, $\mathrm{Ker}(\pi) = K[C] \cap P$ ist ein maximales Ideal von $K[C]$, und nach Satz 3.8.3.3 gibt es einen Punkt $p \in C$, so dass $K[C] \cap P = K[C] \cap \mathcal{M}_{p,K}(C)$.

Wir zeigen nun $\mathcal{O}_{p,K}(C) \prec \mathcal{O}_P$. Sei $\gamma = \psi^{-1}\varphi \in \mathcal{O}_{p,K}(C)$ mit φ, $\psi \in K[C]$ und $\psi(p) \neq 0$. Dann ist $\psi \in K[C] \setminus \mathcal{M}_{p,K}(C) \subset \mathcal{O}_P \setminus P = \mathcal{O}_P^\times$, und wegen $K[C] \subset \mathcal{O}_P$ folgt $\gamma \in \mathcal{O}_P$. Ist $\gamma \in \mathcal{M}_{p,K}(C)$, so ist $\gamma = \psi^{-1}\varphi$ mit φ, $\psi \in K[C]$, $\varphi(p) = 0$ und $\psi(p) \neq 0$. Dann ist $\varphi \in \mathcal{M}_{p,K}(C) \cap K[C] \subset P$ und (wie eben) $\psi \in \mathcal{O}_P^\times$, also $\gamma \in P$. □[**A.**]

Beweis von **B.** Seien p, $p' \in \Gamma$ mit $\mathcal{O}_{p,K}(\Gamma) \prec \mathcal{O}_P$ und $\mathcal{O}_{p',K}(\Gamma) \prec \mathcal{O}_P$, und sei C ein affines Stück von Γ mit $p \in C$, etwa $C = \Gamma \cap \mathbb{A}^2$. Dann ist $K[C] \cap \mathcal{M}_{p,K}(\Gamma) \subset K[C] \cap P$, nach Satz 3.8.3 ist $K[C] \cap \mathcal{M}_{p,K}(\Gamma)$ ein maximales Ideal von $K[C]$, und daher folgt $K[C] \cap \mathcal{M}_{p,K}(\Gamma) = K[C] \cap P$. Ist nun $p' \in C$, so ist auch $K[C] \cap P = K[C] \cap \mathcal{M}_{p',K}(C)$, also $K[C] \cap \mathcal{M}_{p',K}(C) = K[C] \cap \mathcal{M}_{p,K}(C)$ und daher $p \sim_K p'$ nach Satz 3.8.3.3.

Wir nehmen nun an, es sei $p' \notin C$. Seien $\hat{x}$, $\hat{y}$, $\hat{z}$ die homogenen Koordinaten von Γ, und sei $p' = (\alpha : \beta : 0)$ mit $(\alpha,\beta) \in (\overline{K}^2)^\bullet$, etwa $\alpha \neq 0$. Dann ist die Funktion $\hat{x}^{-1}\hat{z} \in K(\Gamma)$ regulär in p', und wegen $(\hat{x}^{-1}\hat{z})(p') = 0$ folgt $\hat{x}^{-1}\hat{z} \in \mathcal{M}_{p',K}(\Gamma) \subset P$. Wegen $K[C] \subset \mathcal{O}_{p,K}(\Gamma) \subset \mathcal{O}_P$ ist $\hat{z}^{-1}\hat{x} \in \mathcal{O}_P$ und daher $1 = (\hat{x}^{-1}\hat{z})(\hat{z}^{-1}\hat{x}) \in P$, ein Widerspruch. □[**B.**]

3. Ist $p \in \Gamma(K)$, so ist $\mathcal{M}_{p,K}(\Gamma) \in \mathbb{P}_{K(\Gamma)/K}$ nach 1.

Ψ ist injektiv: Seien p, $p' \in \Gamma(K)$ mit $\mathcal{M}_{p,K}(\Gamma) = \mathcal{M}_{p',K}(\Gamma)$. Nach Satz 3.5.6 ist dann $\mathcal{O}_{p,K}(\Gamma) = \mathcal{O}_{p',K}(\Gamma)$, also $p \sim_K p'$ nach Satz 3.8.3 und daher $p = p'$.

Ψ ist surjektiv: Sei $P \in \mathbb{P}^1_{K(\Gamma)/K}$. Nach 2. gibt es einen Punkt $p \in \Gamma$ mit $\mathcal{M}_{p,K}(\Gamma) \subset P$, und wir können $p = (\alpha,\beta) \in \Gamma \cap \mathbb{A}^2$ annehmen. Nach 1.(b) ist $K(\alpha,\beta) \subset K(\Gamma)_P = K$ und daher $p = (\alpha,\beta) \in \Gamma(K)$. □

Satz 3.8.7. *Seien Γ, $\Gamma_1 \subset \mathbb{P}^2$ projektive Kurven.Dann ist $\Gamma \cap \Gamma_1 \neq \emptyset$.*

BEWEIS. Es genügt, die Behauptung für irreduzible projektive Kurven zu beweisen. Ist Γ oder Γ_1 eine projektive Gerade, so folgt die Behauptung aus Satz 2.4.2. Wir nehmen an, es sei Γ irreduzibelt, $\Gamma \neq V_+(Z)$, $\Gamma_1 \neq V_+(Z)$ und $\Gamma \cap \Gamma_1 \cap V_+(Z) = \emptyset$, und wir zeigen $\Gamma \cap \Gamma_1 \cap \mathbb{A}^2 \neq \emptyset$.

Sei $C = \Gamma \cap \mathbb{A}^2$ und $C_1 = \Gamma_1 \cap \mathbb{A}^2$, also $\Gamma = \overline{C}$ und $\Gamma_1 = \overline{C}_1$. Sei $\mathfrak{I}_K(C) = (f)$ mit einem irreduziblen Polynom $f \in K[X,Y]$ und $\mathfrak{I}_K(C_1) = (g)$ mit einem Polynom $g \in K[X,Y] \setminus K$. Seien x, $y \in K[C]$ die Koordinatenfunktionen von C. Dann ist $g(x,y) = g + (f) \in K[C]$ und wir behaupten:

A. $g(x,y) \notin K$.

Beweis von **A.** Wir nehmen an, es sei $g(x,y) = c \in K$. Dann ist $g - c \in (f)$, also $g - c = fh$ mit $h \in K[X,Y]$. Ist f_1 die Leitform von f und h_1 die Leitform von h, so ist $g_1 = f_1 h_1$ die Leitform von g. Nach Satz 2.4.2 ist $\Gamma \cap V_+(Z) \neq \emptyset$. Ist $p = (\alpha : \beta : 0) \in \Gamma \cap V_+(Z)$, so ist $f_1(\alpha,\beta) = 0$, also auch $g_1(\alpha,\beta) = 0$ und daher $p \in \Gamma_1 \cap V_+(Z)$, im Widerspruch zur Annahme $\Gamma \cap \Gamma_1 \cap V_+(Z) = \emptyset$. □[**A.**]

Nach **A** ist $\mathbf{0} \neq (g(x,y)) \subsetneq K[C]$, und nach Satz 3.6.2 gibt es eine Stelle $P \in \mathbb{P}_{K(C)}$ mit $K[C] \subset \mathcal{O}_P$ und $g(x,y) \in P$. Nach Satz 3.8.6 gibt es einen Punkt $p = (\alpha,\beta) \in C$, so dass $\mathcal{M}_{p,K}(C) = P \cap \mathcal{O}_{p,K}(C)$. Dann ist $g(x,y) \in P \cap K[C] = \mathcal{M}_{p,K}(C) \cap K[C]$, und nach Satz 3.8.3 ist $\mathcal{M}_{p,K}(C) \cap K[C] = \{\varphi \in K[C] \mid \varphi(p) = 0$. Damit folgt $g(x,y)(p) = g(\alpha,\beta) = g(p) = 0$, also $p \in C_1$. □

Satz 3.8.8. *Sei $C \subset \mathbb{A}^2$ eine über K definierte irreduzible Kurve, seien x, $y \in K[C]$ die Koordinatenfunktionen, und sei $p = (\alpha,\beta) \in C(K)$ ein regulärer Punkt von C. Dann ist $\mathcal{O}_{p,K}(C)$ ein diskreter Bewertungsbereich, $P_p = \mathcal{M}_{p,K}(C) \in \mathbb{P}^1_{K(C)}$, und es sei $v_p = v_{P_p}$ die zugehörige diskrete Bewertung von $K(C)$. Sei $L = V(a(X-\alpha) + b(Y-\beta)) \subset \mathbb{A}^2$ eine über K definierte Gerade mit $(a,b) \in (K^2)^\bullet$ und $p \in L$, und sei $\varphi = y(x-\alpha) + b(y-\beta) \in K(C)$.*

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

BEWEIS. Sei $\mathfrak{I}_K(C) = (f)$ mit einem irreduziblem Polynom $f \in K[X,Y]$. Nach Satz 3.4.1 ist $\mathcal{O}_{p,K}(C)$ ein diskreter Bewertungsbereich, nach Satz 1.4.8 ist $\mathcal{M}_{p,K}(C) = {}_{\mathcal{O}_{p,K}(C)}(x-\alpha, y-\beta)$, und nach Satz 3.8.6 ist $P_p = \mathcal{M}_{p,K}(C) \in \mathbb{P}^1_{K(C)}$. Wegen

$$1 = \min\{v_p(z) \mid z \in P_p\} = \min\{v_p(x-\alpha),\, v_p(y-\beta)\} \quad \text{folgt} \quad v_p(\varphi) \geq 1.$$

Sei nun

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

Dann ist $T = V(a_0(X-\alpha)+b_0(Y-\beta))$ die Tangente an C in p, und $f = a_0(X-\alpha)+b_0(X-\beta)+f_2$ mit einem Polynom $f_2 \in K[X,Y]$, so dass $\operatorname{ord}_p(f_2) \geq 2$. Wegen

$$0 = f(x,y) = a_0(x-\alpha) + b_0(y-\beta) + f_2(x,y) \quad \text{und} \quad v_p(f_2(x,y)) \geq 2$$

folgt $v_p(a_0(x-\alpha) + b_0(y-\beta)) \geq 2$. Wäre nun $v_p(y-\beta) \geq 2$, so folgte wegen $a_0 \neq 0$ auch $v_p(x-\alpha) \geq 2$, ein Widerspruch. Daher ist $v_p(y-\beta) = 1$.

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 $v_p(\varphi) = v_p(a_0(x-\alpha) + b_0(y-\beta)) \geq 2$.

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 $v_p(\varphi) = v_p(y-\beta) = 1$. 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 $v_p(\varphi) = 1$. $\square$

KAPITEL 4

Divisoren, Diffenerziale und der Satz von Riemann-Roch

In diesem Kapitel sei L/K ein Funktionenkörper mit Konstantenkörper K.

4.1. Freie abelsche Gruppen

Definition und Bemerkung 4.1.1. Sei D eine (additive) abelsche Gruppe und $P \subset D$. Dann heißt D *frei mit Basis* P, wenn jedes $a \in D$ eine eindeutige Darstellung

$$a = \sum_{p \in P} n_p p \quad \text{mit} \quad n_p \in \mathbb{Z},\ n_p = 0 \ \text{ für fast alle } \ p \in P$$

besitzt. Insbesondere ist dann P ein Erzeugendensystem von D.
Es sei $\mathbb{Z}^{(P)} = \{(n_p)_{p\in P} \in \mathbb{Z}^P \mid n_p = 0 \text{ für fast alle } p \in P\}$. Dann ist $\mathbb{Z}^{(P)} \subset \mathbb{Z}^P$ eine Untergruppe bezüglich komponentenweiser Addition, und für $q \in P$ sei $e^{(q)} = (\delta_{p,q})_{p\in P} \in \mathbb{Z}^{(P)}$ der q-te Einheitsvektor. Ist $(n_p)_{p\in P} \in \mathbb{Z}^{(P)}$, so ist

$$(n_p)_{p\in P} = \sum_{p\in P} n_p e^{(p)},$$

und daher ist $\mathbb{Z}^{(P)}$ eine freie abelsche Gruppe mit Basis $\{e^{(p)} \mid p \in P\}$.

Eine abelsche Gruppe D ist genau dann frei mit Basis $P \subset D$, wenn die Abbildung

$$\chi\colon \mathbb{Z}^{(P)} \to D, \quad \text{definiert durch} \quad \chi\big((n_p)_{p\in P}\big) = \sum_{p\in P} n_p p$$

ein Isomorphismus ist.

Satz 4.1.2 (Existenz und Eindeutigkeit freier abelscher Gruppen)**.**

1. *Sei D eine freie abelsche Gruppe mit Basis P, A eine abelsche Gruppe und $f_0\colon P \to A$ eine Abbildung. Dann gibt es genau einen Gruppenhomomorphismus $f\colon D \to A$ mit $f \mid P = f_0$.*
2. *Sei P eine Menge. Dann gibt es eine freie abelsche Gruppe D mit Basis P.*
3. *Sind D und D' freie abelsche Gruppen mit Basis P, so gibt es genau einen Isomorphismus $\Phi\colon D \to D'$ mit $\Phi \mid P = \mathrm{id}_P$.*

Beweis. 1. *Existenz:* Definiere $f\colon D \to A$ durch

$$f\Big(\sum_{p\in P} n_p p\Big) = \sum_{p\in P} n_p f_0(p) \quad \text{für alle} \quad (n_p)_{p\in P} \in \mathbb{Z}^{(P)}.$$

Dann ist f offensichtlich ein Gruppenhomomorphismus mit $f \mid P = f_0$. Ist $f'\colon D \to A$ ein weiterer Gruppenhomomorphismus mit $f' \mid P = f_0$, so folgt $f = f'$ da P ein Erzeugendensystem von D ist.

2. $\mathbb{Z}^{(P)}$ ist eine freie abelsche Gruppe mit Basis $P' = \{(e^{(p)} \mid p \in P\}$, und die Zuordnung $p \mapsto e^{(p)}$ definiert eine bijektive Abbildung $P \to P'$. Ersetzt man in $\mathbb{Z}^{(P)}$ die Basis P' durch P, so erhält man eine freie abelsche Gruppe mit Basis P.

3. Nach 1. gibt es Homomorphismen $\Phi\colon D \to D'$ und $\Phi'\colon D' \to D$ mit $\Phi \mid P = \Phi' \mid P = \mathrm{id}_P$. Dann sind $\mathrm{id}_D\colon D \to D$ und $\Phi' \circ \Phi\colon D \to D$ Homomorphismen mit $\mathrm{id}_D \mid P = \Phi' \circ \Phi \mid P = \mathrm{id}_P$, und es folgt $\mathrm{id}_D = \Phi' \circ \Phi$. Ebenso folgt $\mathrm{id}_{D'} = \Phi \circ \Phi'$, und daher ist Φ ein Isomorphismus. Die Eindeutigkeit von Φ folgt wieder aus 1. □

4.2. Divisoren und ihre Vielfachenräume

Definitionen und Bemerkungen 4.2.1. $\mathbb{D}_L = \mathbb{D}_{L/K}$ sei die (bis auf Isomorphie eindeutig bestimmte) freie abelsche Gruppe mit Basis $\mathbb{P}_L$. Nach Definition hat jedes $D \in \mathbb{D}_L$ eine eindeutige Darstellung

$$D = \sum_{P \in \mathbb{P}_L} n_P P \quad \text{mit} \quad (n_P)_{P \in \mathbb{P}_L} \in \mathbb{Z}^{(P)}, \quad \text{und man definiert} \quad v_P(D) = n_P \quad \text{für alle} \quad P \in \mathbb{P}_L.$$

Die Objekte $D \in \mathbb{D}_L$ heißen *Divisore*, die Stellen $P \in \mathbb{P}_L$ nennt man auch *Primdivisoren*. Für $D \in \mathbb{D}_L$ und $P \in \mathbb{P}_L$ heißt $v_P(D) \in \mathbb{Z}$ der *P-adische Wert von D*. Für $P \in \mathbb{P}_L$ ist $v_P\colon \mathbb{D}_L \to \mathbb{Z}$ der eindeutig bestimmte kGruppenhomomorphismus mit $v_P(P) = 1$ und $v_P(P') = 0$ für alle $P' \in \mathbb{P}_L \setminus \{P\}$. Die Null $0 \in \mathbb{D}_L$ heißt *Nulldivisor*.

Für Divisoren $D_1, D_2 \in \mathbb{D}_L$ definiert man $D_1 \le D_2$, wenn $v_P(D_1) \le v_P(D_2)$ für alle $P \in \mathbb{P}_L$. Genau dann ist $D_1 \le D_2$, wenn $D_2 - D_1 \ge 0$, und aus $D_1 \le D_2$ folgt $D_1 + D \le D_2 + D$ für alle $D \in \mathbb{D}_L$. Ein Divisor $D \in \mathbb{D}_L$ heißt *effektiv*, wenn $D \ge 0$.

Für einen Divisor $D \in \mathbb{D}_L$ sei

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

D_+ heißt *Positivteil* und D_- heißt *Negativteil* von D. Nach Definition ist $D_+ \ge 0$, $D_- \ge 0$ und $D = D_+ - D_-$.

Für einen Divisor $D \in \mathbb{D}_L$ nennt man

$$\deg(D) = \sum_{P \in \mathbb{P}_L} v_P(D) \deg(P)$$

den *Grad* von D. Nach Definition ist $\deg\colon \mathbb{D}_L \to \mathbb{Z}$ ein Gruppenhomomorphismus, also insbesondere $\deg(0) = 0$ und $\deg(-D) = -\deg(D)$ für alle $D \in \mathbb{D}_L$

Wir setzen $\mathrm{Bi}(\deg) = \partial_L \mathbb{Z}$ mit $\partial_L \in \mathbb{N}$. Dann ist $\partial_L = \mathrm{ggT}(\{\deg(D) \mid D \in \mathbb{D}_L\})$. Die Gruppe $\mathbb{D}_L^0 = \mathrm{Ker}(\deg)$ heißt *Divisorengruppe 0-ten Grades*.

Für $x \in L^\times$ definieren wir

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

$(x)_0$ heißt *Nullstellendivisor*, $(x)_\infty$ heißt *Polstellendivisor* und (x) heißt *Hauptdivisor* von x. Es ist $(x) = (x)_0 - (x)_\infty$, $(x)_0 = (x)_+$, $(x)_\infty = (x)_-$, $(x)_\infty = (x^{-1})_0$, und für alle $P \in \mathbb{P}_L$ ist

$v_P((x)) = v_P(x)$. Die Abbildung

$$\delta\colon L^\times \to \mathbb{D}_L, \quad \text{definiert durch} \quad \delta(x) = (x) = \sum_{P\in\mathbb{P}_L} v_P(x)P,$$

ist ein Gruppenhomomorphismus und $\mathrm{Ker}(\delta) = K^\times$. Die Gruppe $(L^\times) = \mathrm{Bi}(\delta) \subset \mathbb{D}_L$ heißt *Gruppe der Hauptdivisoren* von L. Der Epimorphismus $\delta\colon L^\times \to (L^\times)$ induziert einen Isomorphismus $L^\times/K^\times \xrightarrow{\sim} (L^\times)$. Die Faktorgruppe $\mathcal{C}_L = \mathbb{D}_L/(L^\times)$ heißt *Divisorenklassengruppe* von L. Für einen Divisor $D \in \mathbb{D}_L$ bezeichne $[D] = D + (L^\times) \in \mathcal{C}_L$ 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: $D_2 = D_1 + (x)$ mit einem $x \in L^\times$]. $\sim$ ist eine Kongruenzrelation auf $\mathbb{D}_L$, und ein Divisor $D \in \mathbb{D}_L$ ist genau dann ein Hauptdivisor, wenn $D \sim 0$.

Für einen Divisor $D \in \mathbb{D}_L$ sei

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

$\mathcal{L}(D)$ ist ein K-Vektorraum und heißt *Vielfachenraum von* $-D$, und $\dim(D) = \dim_K \mathcal{L}(D)$ heißt *Dimension* von D. Genau dann ist $\dim(D) > 0$, wenn es ein $x \in L^\times$ mit $(x) \geq -D$ gibt.
Beweis der Vektorraumeigenschaft:
Seien $x, y \in \mathcal{L}(D)$ und $c \in K$. Für alle $P \in \mathbb{P}_L$ ist $v_P(x+y) \geq \min\{v_P(x), v_P(y)\} \geq -v_P(D)$ und $v_P(cx) = v_P(c) + v_P(x) = v_P(x) \geq -v_P(D)$. Daher ist $x + y \in \mathcal{L}(D)$ und $cx \in \mathcal{L}(D)$.

Satz 4.2.2. *Seien D, $D' \in \mathbb{D}_L$.*

1. *Ist $D \sim D'$, so ist $\dim(D) = \dim(D')$.*
2. *$\mathcal{L}(0) = K$ und $\dim(0) = 1$.*
3. *Ist $D < 0$, so ist $\mathcal{L}(D) = \{0\}$ und $\dim(D) = 0$.*
4. *Genau dann ist $\dim(D) > 0$, wenn es einen zu D äquivalenten effektiven Divisor gibt.*

Beweis. 1. Sei $D = D' + (z)$ mit $z \in L^\times$. Dann ist die Abbildung $\mu_z\colon \mathcal{L}(D) \to L$, definiert durch $\mu_z(x) = xz$, ein K-Vektorraummonomorphismus, und wir zeigen $\mu_z(\mathcal{L}(D)) = \mathcal{L}(D')$. Dann folgt $\dim_K(\mathcal{L}(D)) = \dim_K(\mathcal{L}(D'))$.

Sei $x \in \mathcal{L}(D)^\bullet$. Dann ist $(x) \geq -D$ und daher $(xz) = (x) + (z) \geq -D + (z) = -D'$, also $xz \in \mathcal{L}(D')$. Ist umgekehrt $y \in \mathcal{L}(D')^\bullet$, so ist $(y) \geq -D' = -D + (z)$, also $yz^{-1} = (y) - (z) \geq -D$, es folgt $yz^{-1} \in \mathcal{L}(D)$ und $y = \mu_z(yz^{-1})$.

2. Sei $x \in L^\times$. Genau dann ist $(x) \geq 0$, wenn $\mathcal{P}(x) = \emptyset$, und das ist genau dann der Fall, wenn $x \in K$. Daher ist $\mathcal{L}(0) = K$ und $\dim(0) = 1$.

3. Sei $D < 0$ und $x \in \mathcal{L}(D)^\times$. Dann ist $v_P(x) \geq -v_P(D) \geq 0$ für alle $P \in \mathbb{P}_L$, also $x \in K$, und es gibt ein $P \in \mathbb{P}_L$ mit $v_P(x) \geq -x_P(D) > 0$. Daher ist $x = 0$. Also folgt $\mathcal{L}(D) = \{0\}$ und $\dim(D) = 0$.

4. Ist $\dim(D) > 0$ und $z \in \mathcal{L}(D)^\bullet$, so ist $(z) \geq -D$, also $D_1 = D + (z) \geq 0$ und $D_1 \sim D$. Sei nun $D_1 \in \mathbb{D}_L$, $D_1 \geq 0$ und $D_1 \sim D$, etwa $D_1 = D + (z)$ mit $z \in L^\times$. Dann ist $(z) = D_1 - D \geq -D$, also $z \in \mathcal{L}(D)$ und daner $\dim(D) > 0$. □

Satz 4.2.3. *Seien D, $D' \in \mathbb{D}_L$.*

1. *$\dim(D) \leq \deg(D_+) + 1 < \infty$.*
2. *Sei $D \leq D'$. Dann gilt:*

(a) $\mathcal{L}(D) \subset \mathcal{L}(D')$ *und* $\dim(D) \leq \dim(D')$.

(b) $\dim_K\big(\mathcal{L}(D')/\mathcal{L}(D)\big) \leq \deg(D'-D)$.

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

3. *Ist* D' *effektiv, so ist* $\dim(D+D') \leq \dim(D) + \deg(D')$.

BEWEIS. 2.(a) Ist $x \in \mathcal{L}(D)^\bullet$, so ist $(x) \geq -D \geq -D'$, also $x \in \mathcal{L}(D')$. Damit erhalten wir $\mathcal{L}(D) \subset \mathcal{L}(D')$ und $\dim(D) \leq \dim(D')$.

2.(b) *Spezialfall*: $D' = D + P$ mit $P \in \mathbb{P}_L$.
Wir müssen zeigen: $\dim_K \mathcal{L}(D+P)/\mathcal{L}(D) \leq \deg(P)$. Sei dazu $t \in L$ mit $v_P(t) = v_P(D)+1$. Ist $x \in \mathcal{L}(D+P)$, o ist $v_P(tx) = v_P(t) + v_P(x) \geq v_P(t) + v_P(-D-P) = v_P(t) - v_P(D) - 1 \geq 0$ und daher $tx \in \mathcal{O}_P$. Sei nun

$$\psi\colon \mathcal{L}(D+P) \to L_P \quad \text{definiert durch} \quad \psi(x) = (xt)(P).$$

Sei $x \in \mathcal{L}(D+P)$. Dann gilt:

$$x \in \operatorname{Ker}(\psi) \iff v_P(xt) \geq 1 \iff v_P(x) \geq 1 - v_P(t) = -v_P(D) \iff x \in \mathcal{L}(D).$$

Es folgt $\operatorname{Ker}(\psi) = \mathcal{L}(D+P) \cap \mathcal{L}(D) = \mathcal{L}(D)$. Daher induziert ψ einen K-Vektorraummonomorphismus $\mathcal{L}(D+P)/\mathcal{L}(D) \to L_P$, und es folgt $\dim_K \mathcal{L}(D+P)/\mathcal{L}(D) \leq \dim_K(L_P) = \deg(P)$.

Allgemeiner Fall: Sei $D' = D + P_1 + \ldots + P_r$ mit $r \in \mathbb{N}$. Dann ist

$$\mathcal{L}(D') = \mathcal{L}(D+P_1+\ldots+P_r) \supset \ldots \supset \mathcal{L}(D+P_1+\ldots+P_i) \supset \mathcal{L}(D+P_1+\ldots+P_{i-1}) \supset \ldots \supset \mathcal{L}(D)$$

eine Folge von K-Untervektorräumen, und es folgt nach dem Spezialfall

$$\begin{aligned}\dim_K \mathcal{L}(D')/\mathcal{L}(D) = \sum_{i=1}^{r} \dim_K \mathcal{L}(D+P_1+\ldots+P_i)/\mathcal{L}(D+P_1+\ldots+P_{i-1}) &= \sum_{i=1}^{r} \deg(D_i) \\ &= \deg(D'-D).\end{aligned}$$

1. Es ist $D_+ \geq 0$ und daher $\dim_K \mathcal{L}(D_+)/\mathcal{L}(0) \leq \deg(D_+)$. Wegen $\dim_K \mathcal{L}(0) = \dim(0) = 1$ folgt $\dim(D_+) = \dim_K \mathcal{L}(D_+) \leq \deg(D_+) + 1$, und wegen $D \leq D_+$ ist $\dim(D) \leq \dim(D_+)$.

2.(c) Aus $D \leq D'$ folgt

$$\dim(D') - \dim(D) = \dim_K \mathcal{L}(D')/\mathcal{L}(D) \leq \deg(D'-D) = \deg(D') - \deg(D),$$

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

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

4.3. Definition des Geschlechts und Satz von Riemann

Satz 4.3.1. *Sei* $x \in L^\times$.

1. *Ist* $x \notin K$, *so ist* $\deg(x)_0 = \deg(x)_\infty = [L\colon K(x)]$, *und es gibt einen effektiven Divisor* $C \in \mathbb{D}_L$, *so dass* $\dim(l(x)_\infty + C) \geq (l+1)\deg(x)_\infty$ *für alle* $l \in \mathbb{N}_0$.
2. $\deg(x) = 0$.
3. *Für je zwei linear äquivalente Divisoren* D, $D' \in \mathbb{D}_L$ *ist* $\deg(D) = \deg(D')$.

BEWEIS. 1. Sei $x \in L \setminus K$. Dann ist $n = [L : K(x)] < \infty$, und es sei $(u_1, \ldots, u_n)$ eine $K(x)$-Basis von L. Sei $C \in \mathbb{D}_L$ ein effektiver Divisor, so dass $(u_i) \geq -C$ für alle $i \in [1, n]$. Für alle $i \in [1, n]$ und $j \in [0, l]$ ist dann $(x^j u_i) = j(x) + (u_i) \geq -j(x)_\infty - C \geq -[l(x)_\infty + C]$ und daher $x^j u_i \in \mathcal{L}((x)_\infty + C)$. Da x über K transzendent ist, ist $\{x^j u_i \mid j \in [0, l],\ i \in [1, n]\}$ linear unabhängig über K, und es folgt $\dim(l(x)_\infty + C) \geq (l+1)n$. Nach Satz 4.2.3.1 erhalten wir

$$\begin{aligned}(l+1)n \leq \dim(l(x)_\infty + C) &\leq \deg(l(x)_\infty + C)_+ + 1 = \deg(l(x)_\infty + C) + 1 \\ &= l \deg(x)_\infty + \deg(C) + 1\end{aligned}$$

und daher

$$l\,[\deg(x)_\infty - n] \geq n - \deg(C) - 1.$$

Für $l \gg 1$ folgt $\deg(x)_\infty \geq n$. Nach Satz 3.6.3.1 ist

$$\deg(x)_\infty = \sum_{P \in \mathcal{P}(x)} -v_P(x) \deg(P) = \sum_{P \in \mathcal{N}(x^{-1})} v_P(x^{-1}) \deg(P) \leq [L : K(x^{-1})] = [L : K(x)] = n.$$

Es folgt $\deg(x)_\infty = n = [L : K(x)]$, $\dim(l(x)_\infty + C) \geq (l+1)n = (l+1)\deg(x)_\infty$, und $\deg(x)_0 = \deg(x^{-1})_\infty = [L : K(x^{-1})] = [L : K(x)]$.

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

3. Seien D, $D' \in \mathbb{D}_L$ linear äquivalent, und sei $x \in L^\times$ mit $D' = D + (x)$. Dann folgt $\deg(D') = \deg(D) + \deg(x) = \deg(D)$. □

Korollar 4.3.2. *Für $D \in \mathbb{D}_L^0$ sind äquivalent*:

(a) $D \in (L^\times)$.

(b) $\dim(D) > 0$.

(c) $\dim(D) = 1$.

BEWEIS. (a) $\Rightarrow$ (b) Ist $D \in (L^\times)$, so ist $D \sim 0$ und daher $\dim(D) > 0$ nach Satz 4.2.2.4.

(b) $\Rightarrow$ (c) und (a) Nach Satz 4.2.2 gibt es einen effektiven Divisor $D_1 \in \mathbb{D}_L$ mit $D_1 \sim D$. Dann ist $\deg(D_1) = \deg(D) = 0$, also $D_1 = 0$, $D \sim 0$, also $D \in (L^\times)$, und $\dim(D) = \dim(0) = 1$.

(c) $\Rightarrow$ (b) Offensichtlich. □

Definition 4.3.3. Sei $\mathfrak{d} = [D] \in \mathcal{C}_L$. Dann nennt man $\deg(\mathfrak{d}) = \deg(D)$ den *Grad* und $\dim(\mathfrak{d}) = \dim(D)$ die *Dimension* der Divisorenklasse $\mathfrak{d}$.

Satz und Definition 4.3.4 (Satz von Riemann)**.**

1. *Es ist*
$$g_L = \sup\{\deg(D) - \dim(D) + 1 \mid D \in \mathbb{D}_L\} < \infty.$$
$g_L = g_{L/K}$ heißt *Geschlecht* von L.

2. *Sei $D \in \mathbb{D}_L$. Dann ist*
$$\dim(D) \geq \deg(D) - g_L + 1 \quad \textit{und} \quad i(D) = \dim(D) - \deg(D) + g_L - 1 \geq 0.$$
$i(D)$ heißt *Spezialitätsindex* von D. *Es ist $i(0) = g_L$, und es gibt einen Divisor $D_0 \in \mathbb{D}_L$ mit $i(D_0) = 0$.*

3. *Sei $D_0 \in \mathbb{D}_L$ mit $i(D_0) = 0$ und $D \in \mathbb{D}_L$ mit $\deg(D) \geq \deg(D_0) + g_L$. Dann ist auch $i(D) = 0$. Insbesondere gilt: Es gibt ein $c \in \mathbb{N}$, so dass $i(D) = 0$ für alle $D \in \mathbb{D}_L$ mit $\deg(D) > c$.*

BEWEIS. 1. Sei $x \in L \setminus K$ und $B = (x)_\infty$. Nach Satz 4.3.1 gibt es einen effektiven Divisor $C \in \mathbb{D}_L$, so dass $\dim(lB + C) \geq (l+1)\deg(B) \geq \deg(lB)$ für alle $l \in \mathbb{N}_0$, und wir zeigen

$$\deg(D) - \dim(D) \leq \deg(C) \quad \text{für alle} \quad D \in \mathbb{D}_L.$$

Sei $l \in \mathbb{N}_0$, $D \in \mathbb{D}_L$, und sei $C_1 \in D_L$ effektiv mit $C_1 \geq D$. Nach Satz 4.2.3.2(c) ist

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

und aus Satz 4.2.3.3 folgt

$$\dim(lB) = \dim(lB - C_1 + C_1) \leq \dim(lB - C_1) + \deg(C_1),$$

und daher

$$\begin{aligned}\dim(lB - C_1) &\geq \dim(lB) - \deg(C_1) \geq \deg(lB) - \deg(C) - \deg(C_1) = l\deg(B) - \deg(C + C_1) \\ &\geq 1 \quad \text{für} \quad l \gg 1.\end{aligned}$$

Sei $l \in \mathbb{N}$ mit $\dim(lB - C_1) \geq 1$, $z \in \mathcal{L}(lB - C_1)^\bullet$, also $(z) \geq -lB + C_1$, und $D_1 = C_1 - (z)$. Dann ist $D_1 \leq C_1 + lB - C_1 = lB$, und wegen $D_1 \sim C_1$ und $D \leq C_1$ folgt nach Satz 4.2.3.2(c)

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

2. Definitionsgemäß gibt es einen Divisor $D_0 \in \mathbb{D}_L$ mit $g_L = \deg(D_0) - \dim(D_0) + 1$, also $i(D_0) = 0$, und für alle $D \in \mathbb{D}_L$ ist

$$\dim(D) \geq \deg(D) - g_L + 1, \quad i(D) = \dim(D) - \deg(D) + g_L - 1 \geq 0,$$

und $i(0) = \dim(0) - \deg(0) + g_L - 1 = g_L$.

3. Nach 2. ist $\dim(D - D_0) \geq \deg(D - D_0) - g_L + 1 = \deg(D) - \deg(D_0) - g_L + 1 \geq 1$. Sei nun $z \in \mathcal{L}(D - D_0)^\bullet$ und $D' = D + (z)$. Dann ist $D' \geq D - (D - D_0) = D_0$ und $D' \sim D$. Mit Satz 4.2.3.2(c) folgt

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

und daher $i(D) = \dim(D) - \deg(D) + g_L - 1 \leq 0$, also $i(D) = 0$. □

4.4. Adele

Definitionen und Bemerkungen 4.4.1. Eine Familie $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in L^{\mathbb{P}_L}$ heißt (*unvollständiges*) *Adel* von L/K, wenn $\alpha_P \in \mathcal{O}_P$ für fast alle $P \in \mathbb{P}_L$. Es sei $\mathbb{A}_L = \mathbb{A}_{L/K}$ die Menge aller Adele von L/K mit komponentenweiser Addition, Multiplikation und Skalarmultiplikation mit Elementen aus K. Explizit: Für $\alpha, \beta \in \mathbb{A}_L$ und $c \in K$ sind die Adele $\alpha + \beta$, $\alpha\beta$ und $c\alpha$ definiert durch $(\alpha + \beta)_P = \alpha_P + \beta_P$, $(\alpha\beta)_P = \alpha_P\beta_P$ und $c\alpha)_P = c\alpha_P$ für alle $P \in \mathbb{P}_L$. Damit wird $\mathbb{A}_L$ zur K-Algebra.

Für ein Adel $\alpha \in \mathbb{A}_L$ und $Q \in \mathbb{P}_L$ sei $v_Q(\alpha) = v_Q(\alpha_Q)$. Für alle $\alpha, \beta \in \mathbb{A}_L$ und $Q \in \mathbb{P}_L$ ist dann $v_Q(\alpha + \beta) \geq \min\{v_Q(\alpha), v_Q(\beta)\}$ und $v_Q(\alpha\beta) = v_Q(\alpha) + v_Q(\beta)$. Ist $x \in L$, so ist $v_P(x) = 0$ (also insbesondere $x \in \mathcal{O}_P$) für fast alle $P \in \mathbb{P}$, und daher $[x] = (x)_{P \in \mathbb{P}} \in \mathbb{A}_L$ und $v_Q(x) = v_Q([x])$ für alle $Q \in \mathbb{P}_L$. Die Abbildung $L \to \mathbb{A}_L$, $x \mapsto [x]$, ist ein K-Algebrenmonomorphismus, wir identifizieren und schreiben $x = [x]$. Damit ist $L \subset \mathbb{A}_L$ eine K-Unteralgebra.

Für einen Divisor $D \in \mathbb{D}_L$ sei

$$\mathbb{A}_L(D) = \{\alpha \in \mathbb{A}_L \mid v_Q(\alpha) \geq -v_Q(D) \ \text{ für alle } \ Q \in \mathbb{P}_L\}.$$

Dann ist $\mathbb{A}_L(D) \subset \mathbb{A}_L$ ein K-Untervektorraum, und $\mathbb{A}_(D) \cap L = \mathcal{L}(D)$.

Satz 4.4.2. *Seien D_1, $D_2 \in D_L$ und $D_1 \leq D_2$. Dann ist*

$$\mathbb{A}_L(D_1) \subset \mathbb{A}_L(D_2), \quad \dim_K \mathbb{A}_L(D_2)/\mathbb{A}_L(D_1) = \deg(D_2 - D_1)$$

und

$$\dim_K(\mathbb{A}_L(D_2) + L)/(\mathbb{A}_L(D_1) + L) = [\deg(D_2) - \dim(D_2)] - [\deg(D_1) - \dim(D_1)].$$

Beweis. Ist $\alpha \in \mathbb{A}_L(D_1)$, so folgt $v_Q(\alpha) \geq -v_Q(D_1) \geq -v_Q(D_2)$ für alle $Q \in \mathbb{P}_L$ und daher $\alpha \in \mathbb{A}_L(D_2)$. Wir zeigen nun zuerst:

A. Ist $D \in \mathbb{D}_L$ und $Q \in \mathbb{P}_L$, so folgt $\dim_K \mathbb{A}_L(D+Q)/\mathbb{A}_L(D) = \deg(Q)$.

Beweis von **A.** Sei $t \in L$ mit $v_Q(t) = v_Q(D) + 1 = v_Q(D+Q)$. Für ein Adel $\alpha \in \mathbb{A}_L(D+Q)$ ist $v_Q(t\alpha) = v_Q(t) + v_Q(\alpha_Q) \geq v_Q(D) + 1 - v_Q(D+Q) = 0$, also $t\alpha_Q \in \mathcal{O}_Q$. Wir definieren

$$\varphi\colon \mathbb{A}_L(D+Q) \to L_Q \quad \text{durch} \quad \varphi(\alpha) = (t\alpha_Q)(Q).$$

Dann ist φ ein K-Vektorraumhomomorphismus, und wir zeigen, dass φ surjektiv ist. Sei dazu $c = z(Q) \in L_Q$ mit $z \in \mathcal{O}_Q$. Sei $\alpha_Q = t^{-1}z \in L$, also $v_Q(\alpha_Q) = -v_Q(t) + v_Q(z) \geq -v_Q(D+Q)$, und für $P \in \mathbb{P}_L \setminus \{Q\}$ sei $\alpha_P \in L$ mit $v_P(\alpha_P) = -v_P(D) = -v_P(D+Q)$. Damit erhalten wir $\alpha = (\alpha_P)_{P \in \mathbb{P}_L} \in \mathbb{A}_L(D+Q)$ und $\varphi(\alpha) = (t\alpha_Q)(Q) = z(Q) = c$.

Ist $\alpha \in \mathbb{A}_L(D+Q)$, so ist genau dann $\varphi(\alpha) = 0$, wenn $v_Q(t\alpha) \geq 1$, also genau dann, wenn $v_Q(\alpha) \geq 1 - v_Q(t) = -v_Q(D)$. Daher ist $\operatorname{Ker}(\varphi) = \mathbb{A}_L(D)$, φ induziert einen K-Vektorraumisomorphismus $\mathbb{A}_L(D+Q)/\mathbb{A}_L(D) \xrightarrow{\sim} L_Q$, und damit folgt die Behauptung. $\square[\mathbf{A}]$

Sei nun $D_2 = D_1 + P_1 + \ldots + P_r$ mit $r \in \mathbb{N}$ und $P_1, \ldots, P_r \in \mathbb{P}_L$. Dann ist

$$\mathbb{A}_L(D_2) \supset \ldots \supset \mathbb{A}_L(D_1 + P_1 + \ldots + P_i) \supset \mathbb{A}_L(D_1 + P_1 + \ldots + P_{i-1}) \supset \ldots \supset \mathbb{A}_L(D_1)$$

eine Folge von K-Untervektorräumen, und nach **A** ist

$$\begin{aligned}\dim_K \mathbb{A}_L(D_2)/\mathbb{A}_L(D_1) &= \sum_{i=1}^{r} \dim_K \mathbb{A}_L(D_1 + P_1 + \ldots + P_i)/\mathbb{A}_L(D_1 + P_1 + \ldots + P_{i-1}) \\ &= \sum_{i=1}^{r} \deg(P_i) = \deg(D_2 - D_1).\end{aligned}$$

Zum Nachweis der zweiten Dimensionsaussage betrachten wir den natürlichen K-Vektorraumisomorphismus

$$\sigma_0\colon \mathbb{A}_L(D_2) \to (\mathbb{A}_L(D_2) + L)/(\mathbb{A}_L(D_1) + L), \quad \text{definiert durch} \quad \sigma_0(\alpha) = \alpha + (\mathbb{A}_L(D_1) + L).$$

Wegen $\mathbb{A}_L(D_1) \subset \operatorname{Ker}(\sigma_0)$ induziert σ_0 einen K-Vektorraumepimorphismus

$$\sigma\colon \mathbb{A}_L(D_2)/\mathbb{A}_L(D_1) \to (\mathbb{A}_L(D_2) + L)/(\mathbb{A}_L(D_1) + L),$$

und es folgt

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

Wegen $\mathcal{L}(D_2) \subset \mathbb{A}_L(D_2)$ und $\mathcal{L}(D_1) = \mathbb{A}_L(D_1) \cap \mathcal{L}(D_2)$ gibt es einen K-Vektorraummonomorphismus

$$\tau\colon \mathcal{L}(D_2)/\mathcal{L}(D_1) \to \mathbb{A}_L(D_2)/\mathbb{A}_L(D_1) \quad \text{mit} \quad \tau(x + \mathcal{L}(D_1)) = x + \mathbb{A}_L(D_1) \text{ für alle } x \in \mathcal{L}(D_2),$$

und wir zeigen:

B. $\operatorname{Bi}(\tau) = \operatorname{Ker}(\sigma)$.

Mit **B** folgt $\dim_K \mathrm{Ker}(\sigma) = \dim_K \mathrm{Bi}(\tau) = \dim_K \mathcal{L}(D_2)/\mathcal{L}(D_1) = \dim(D_2) - \dim(D_1)$ und daher

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

Beweis von **B.** $\subset$: Sei $x \in \mathcal{L}(D_2)$ und $\tau(x + \mathcal{L}(D_1)) = x + \mathbb{A}_L(D_1) \in \mathrm{Bi}(\tau)$. Dann ist $\sigma(x + \mathbb{A}_L(D_1)) = x + (\mathbb{A}_L(D_1) + L) = \mathbb{A}_L(D_1) + L$, also $x + \mathbb{A}_L(D_1) \in \mathrm{Ker}(\sigma)$.

$\supset$: Sei $\alpha \in \mathbb{A}_L(D_2)$ und $\alpha + \mathbb{A}_L(D_1) \in \mathrm{Ker}(\sigma)$. Dann is $\alpha \in \mathbb{A}_L(D_1) + L$, und daher gibt es ein $x \in L$ mit $\alpha - x \in \mathbb{A}_L(D_1) \subset \mathbb{A}_L(D_2)$. Es folgt $x = \alpha - (\alpha - x) \in \mathbb{A}_L(D_2) \cap L = \mathcal{L}(D_2)$ und $\alpha = x + \mathbb{A}_L(D_1) = \tau(x + \mathcal{L}(D_1)) \in \mathrm{Bi}(\tau)$. □

Satz 4.4.3. *Sei $D \in \mathbb{D}_L$. Dann ist $i(D) = \dim_K \mathbb{A}_L/(\mathbb{A}_L(D) + L)$. Insbesondere folgt*

$$\dim(D) = \deg(D) + 1 - g_L + \dim_K \mathbb{A}_L/(\mathbb{A}_L(0)+L) \quad \textit{und} \quad g_L = \dim_K \mathbb{A}_L/(\mathbb{A}_L(0)+L).$$

Beweis. Nach Satz 4.3.4 ist $\dim(D) = \deg(D) + 1 - g_L + i(D)$ und $g_L = i(0)$. Daher genügt es, $i(D) = \dim_K \mathbb{A}_L/(\mathbb{A}_L(0)+L)$ zu zeigen.

Spezialfall $i(D) = 0$: Dann ist $\deg(D) - \dim(D) = g_L - 1$, und wir müssen $\mathbb{A}_L = \mathbb{A}_L(D) + L$ zeigen. Sei $\alpha \in \mathbb{A}_L$. Es gibt es einen Divisor $D_1 \in \mathbb{D}_L$ mit $D_1 \geq D$ und $\alpha \in \mathbb{A}_L(D_1)$. Dann ist $D_1 = D + (D_1 - D)$ und $D_1 - D$ ist ein effektiver Divisor. Nach Satz 4.2.3.3 und Satz 4.3.4.2 folgt

$$\dim(D_1) \leq \dim(D) + \deg(D_1 - D) = \deg(D_1) + \dim(D) - \deg(D) = \deg(D_1) - g_L + 1 \leq \dim(D_1),$$

also $\dim(D_1) = \deg(D_1) - g_L + 1$. Aus Satz 4.4.2 folgt

$$\begin{aligned}\dim_K(\mathbb{A}_L(D_1)+L)/(\mathbb{A}_L(D)+L) &= [\deg(D_1) - \dim(D_1)] - [\deg(D) - \dim(D)]\\ &= (g_L - 1) - (g_L - 1) = 0.\end{aligned}$$

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

Allgemeiner Fall: Nach Satz 4.3.4.3 gibt es einen Divisor $D_1 \in \mathbb{D}_L$ mit $D_1 \geq D$ und $i(D_1) = 0$. Dann ist $\mathbb{A}_L = \mathbb{A}_L(D_1) + L$, und es folgt

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

4.5. Differenziale und der Satz von Riemann - Roch

Definitionen und Bemerkungen 4.5.1. Sei $\mathbb{A}_L^* = \mathrm{Hom}_K(\mathbb{A}_L, K)$ der K-Dualraum von $\mathbb{A}_L$. Für einen Divisor $D \in \mathbb{D}_L$ sei

$$\Omega_L(D) = \{\omega \in \mathbb{A}_L^* \mid \omega \restriction (\mathbb{A}_L(D) + L) = 0\}.$$

Offensichtlich ist $\Omega_L(D) \subset \mathbb{A}_L^*$ ein K-Untervektorraum, und $\Omega_L(D)$ ist isomorph zum K-Dualraum von $\mathbb{A}_L/(\mathbb{A}_L(D)+L)$. Damit folgt

$$\dim_K \Omega_L(D) = \dim_K \mathbb{A}_L/(\mathbb{A}_L(D)+L) = i(D).$$

Für Divisoren D, $D' \in \mathbb{D}_L$ mit $D \leq D'$ ist $\mathbb{A}_L(D) \subset \mathbb{A}_L(D')$ und daher $\Omega_L(D) \supset \Omega_L(D')$. Zu je zwei Divisoren D_1, $D_2 \in \mathbb{D}_L$ gibt es einen Divisor $D \in \mathbb{D}_L$ mit $D \leq D_1$ und $D \leq D_2$, und

dann ist $\Omega_L(D_1) \cup \Omega_L(D_2) \subset \Omega_L(D)$. Daher ist $\{\Omega_L(D) \mid D \in \mathbb{D}_L\}$ eine gerichtete Menge von K-Untervektorräumen von $\mathbb{A}_L^*$, und daher ist

$$\Omega_L = \bigcup_{D \in \mathbb{D}_L} \Omega_L(D) \subset \mathbb{A}_L^* \quad \text{ein} \quad K\text{-Untervektorraum.}$$

Der K-Vektorraum $\Omega_L = \Omega_{L/K}$ heißt *Differenzialmodul* von L, die Elemente $\omega \in \Omega_L$ heißen (*Weil'sche*) *Differenziale*.

Jedes $\omega \in \Omega_L$ ist ein K-Vektorraumhomomorphismus $\omega\colon \mathbb{A}_L \to K$ mit $\omega \,|\, L = 0$, und für jeden Divisor $D \in \mathbb{D}_L$ ist $\Omega_L(D) = \{\omega \in \Omega_L \colon \omega \restriction \mathbb{A}_L(D) = 0\}$.

Für $\omega \in \Omega_L$ und $x \in L$ definiert man

$$x\omega\colon \mathbb{A}_L \to K \quad \text{durch} \quad (x\omega)(\alpha) = \omega(x\alpha) \quad \text{für alle} \quad \alpha \in \mathbb{A}_L.$$

Dann ist $x\omega \in \mathbb{A}_L^*$. Der nächste Satz zeigt, dass mit dieser Skalarmultiplikation Ω_L zum L-Vektorraum wird.

Satz 4.5.2.

1. *Sei $D \in \mathbb{D}_L$ und $\omega \in \Omega_L(D)$.*
   (a) *Ist $B \in \mathbb{D}_L$ und $x \in \mathcal{L}(B)$, so ist $x\omega \in \Omega_L(D - B)$.*
   (b) *Ist $x \in L^\times$, so ist $x\omega \in \Omega_L(D + (x))$.*
2. *Für alle $x \in L$ und $\omega \in \Omega_L$ ist $x\omega \in \Omega_L$, und vermöge*

$$L \times \Omega_L \;\to\; \Omega_L, \quad (x, \omega) \;\mapsto\; x\omega$$

ist Ω_L ein eindimensionaler L-Vektorraum.

Beweis. 1.(a) Sei $B \in \mathbb{D}_L$ und $x \in \mathcal{L}(B)$. Wir zeigen: $x\omega \,|\, (\mathbb{A}_L(D - B) + L) = 0$. Sei dazu $\alpha \in \mathbb{A}_L(D - B)$ und $z \in L$. Dann ist $(x\omega)(\alpha + z) = \omega(x\alpha + xz) = \omega(x\alpha)$. Für alle $P \in \mathbb{P}_L$ ist $v_P(x\alpha) = v_P(x) + v_P(\alpha) \geq -v_P(B) - v_P(D - B) = -v_P(D)$, also $x\alpha \in \mathbb{A}_L(D)$ und daher $\omega(x\alpha) = 0$.

(b) Nach (a) mit $B = -(x)$.

2. Für $x = 0$ ist nichts zu zeigen. Sei also $x \in L^\times$ und $\omega \in \Omega_L$. Dann gibt es ein $D \in \mathbb{D}_L$ mit $\omega \in \Omega_L(D)$, und nach 1.(b) folgt $x\omega \in \Omega_L(D + (x)) \subset \Omega_L$. Sine ω, $\omega' \in \Omega_L$ und x, $x' \in L$, so ist offensichtlich $x(\omega + \omega') = x\omega + x\omega'$, $(x + x')\omega = x\omega + x'\omega$ und $(xx')\omega = x(x'\omega)$. Daher ist Ω_L ein L-Vektorraum.

Es bleibt zu zeigen: $\dim_L(\Omega_L) = 1$. Seien ω_1, $\omega_2 \in \Omega_L^\bullet$. Wir müssen zeigen, dass es ein $x \in L$ mit $\omega_2 = x\omega_1$ gibt. Für $i \in \{1, 2\}$ sei $D_i \in \mathbb{D}_L$ mit $\omega_i \in \Omega_L(D_i)$. Für einen effektiven Divisor $B \in \mathbb{D}_L$ mit $\deg(B) \gg 1$ ist dann $i(D_i + B) = 0$, und es sei

$$\varphi_i\colon \mathcal{L}(D_i + B) \to \Omega_L(D_i - (D_i + B)) = \Omega_L(-B) \quad \text{definiert durch} \quad \varphi_i(x) = x\omega_i.$$

φ_i ist ein K-Vektorraummonomorphismus, und es sei $U_i = \mathrm{Bi}(\varphi_i) \subset \Omega_L(-B)$. Dann folgt

$$\dim_K(U_i) = \dim(D_i + B) = \deg(D_i + B) - g_L + 1.$$

Wegen

$$\begin{aligned} \dim_K(U_1 + U_2) &\leq \dim_K(\Omega_L(-B)) = i(-B) \\ &= \dim(-B) - \deg(-B) + g_L - 1 = \deg(B) + g_L - 1 \end{aligned}$$

folgt

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

Daher gibt es Elemente $x_1 \in \mathcal{L}(D_1 + B)$ und $x_2 \in \mathcal{L}(D_2 + B)$ mit $\varphi_1(x_1) = \varphi_2(x_2) \neq 0$, also $x_1\omega_1 = x_2\omega_2 \neq 0$. □

Satz und Definition 4.5.3.

1. *Sei $\omega \in \Omega_L^\bullet$. Dann gibt es einen (eindeutig bestimmten) größten Divisor $W \in \mathbb{D}_L$ mit $\omega \in \Omega_L(W)$ (für jeden Divisor $D \in \mathbb{D}_L$ mit $\omega \in \Omega_L(D)$ ist dann $D \leq W$).*

   Man nennt $W = (\omega)$ den *Divisor* von ω. *Für alle $D \in \mathbb{D}_L$ ist dann*

   $$\Omega_L(D) = \{\omega \in \Omega_L^\bullet \mid (\omega) \geq D\} \cup \{0\} \subset \Omega_L.$$

2. *Für alle $x \in L^\times$ und $\omega \in \Omega_L^\bullet$ ist $(x\omega) = (x) + (\omega)$.*
3. *Sei $D \in \mathbb{D}_L$, $\omega \in \Omega_L^\bullet$ und $W = (\omega)$. Dann ist die Abbildung*

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

   ein K-Vektorraumisomorphismus.

Beweis. 1. Nach Satz 4.3.4 gibt es ein $c \in \mathbb{N}$, so dass $i(D) = 0$ für alle $D \in \mathbb{D}_L$ mit $\deg(D) > c$. Ist nun $D \in \mathbb{D}_L$ mit $\omega \in \Omega_L(D)$, so ist $0 \neq \dim_K \Omega_L(D) = i(D)$ und daher $\deg(D) \leq c$. Daher gibt es einen Divisor $W \in \mathbb{D}_L$ maximalen Grades mit $\omega \in \Omega_L(W)$, und wir zeigen: Für eine Divisor $D \in \mathbb{D}_L$ ist genau dann $\omega \in \Omega_L(D)$, wenn $D \leq W$.

Sei $D \in \mathbb{D}_L$. Ist $D \leq W$, so ist $\Omega_L(W) \subset \Omega_L(D)$ und daher $\omega \in \Omega_L(D)$. Sei nun $\omega \in \Omega_L(D)$ und $D \not\leq W$. Dann gibt es ein $Q \in \mathbb{P}_L$ mit $v_Q(D) > v_Q(W)$, und wir zeigen $\omega \,|\, \mathbb{A}_L(Q + W) = 0$ (dann ist $\omega \in \Omega_L(Q + W)$ und $\deg(Q + W) = \deg(W) + \deg(Q) > \deg(W)$, ein Widerspruch). Sei $\alpha \in \mathbb{A}_L(Q + W)$, und definiere Adele α', $\alpha'' \in \mathbb{A}_L$ durch

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

Dann folgt $v_P(\alpha') = v_P(\alpha) \geq -v_P(Q + W) = -v_P(W)$ für alle $P \in \mathbb{P}_L \setminus \{Q\}$, und wegen $v_Q(\alpha') = \infty \geq -v_Q(W)$ folgt $\alpha' \in \mathbb{A}_L(W)$. Es ist $v_P(\alpha'') = \infty \geq -v_Q(D)$ für alle $P \in \mathbb{P}_L \setminus \{Q\}$, und $v_Q(\alpha'') = v_Q(\alpha) \geq -v_Q(Q + W) = -[v_Q(W) + 1] \geq -v_Q(D)$, also $\alpha'' \in \mathbb{A}_L(D)$. Damit folgt $\omega(\alpha) = \omega(\alpha') + \omega(\alpha'') = 0$.

2. Sei $x \in L^\times$ und $\omega \in \Omega_L^\bullet$. Nach Definition ist $\omega \in \Omega_L((\omega))$, und nach Satz 4.5.2.1(b) ist $x\omega \in \Omega_L((\omega) + (x))$. Daher folgt $(x\omega) \geq (\omega) + (x)$. In gleicher Weise ist

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

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

3. Ist $x \in \mathcal{L}(W - D)$, so ist $x\omega \in \Omega_L(W - (W - D)) = \Omega_L(D)$, und offensichtlich ist μ ein K-Vektorraummonomorphismus. Für den Beweis der Surjektivität sei $\omega_1 \in \Omega_L(D)^\bullet$. Nach Satz 4.5.2.2 ist $\omega_1 = x\omega$ für ein $x \in L^\times$ und $\omega \in \Omega_L$. Wegen $D \leq (\omega_1) = (x) + (\omega) = (x) + W$ folgt $(x) \geq D - W$ und daher $x \in \mathcal{L}(W - D)$. □

Definition 4.5.4.

1. Für eine Stelle $P \in \mathbb{P}_L$ definiert man $v_P\colon \Omega_L \to \mathbb{Z} \cup \{\infty\}$ durch $v_P(\omega) = v_P((\omega))$, falls $\omega \neq 0$, und $v_P(0) = \infty$. Man nennt P eine *Nullstelle* (*Polstelle*) von ω, wenn $v_P(\omega) > 0$ ($v_P(\omega) < 0$). ω heißt *regulär* in P, wenn $v_P(\omega) \geq 0$. ω heißt *holomorph*, wenn ω in allen Stellen von L regulär ist [äquivalent, $\omega \in \Omega_L(0)$].
2. Ein Divisor $W \in \mathbb{D}_L$ heißt *kanonischer Divisor*, wenn $W = (\omega)$ für ein Differenzial $\omega \in \Omega_L^\bullet$. Nach den Sätzen 4.5.2.2 und 4.5.3.2 sind je zwei kanonische Divisoren äquivalent. Eine Divisorenklasse $\mathfrak{d} \in \mathcal{C}_L$ heißt *kanonische Klasse*, wenn sie einen kanonischen Divisor enthält. Nach dem Vorangegangenen gibt es genau eine kanonische Klasse, und diese besteht aus allen kanonischen Divisoren.

Satz 4.5.5 (Riemann - Roch)**.** *Sei $W \in \mathbb{D}_L$ ein kanonischer Divisor und $D \in \mathbb{D}_L$.*

1. *$i(D) = \dim(W - D)$, und $\dim(D) = \deg(D) + 1 - g_L + \dim(W - D)$.*
2. *$\deg(W) = 2g_L - 2$, und $\dim(W) = g_L$.*
3. *Ist $\deg(D) \geq 2g_L - 1$, so ist $i(D) = 0$.*
4. *Genau dann ist D ein kanonischer Divisor, wenn $\deg(D) = 2g_L - 2$ und $\dim(D) \geq g_L$.*

Beweis. Sei $\omega \in \Omega_L^\bullet$ und $W = (\omega)$.

1. Nach Satz 4.5.3.3 gibt es einen K-Vektorraumisomorphismus $\mu\colon \mathcal{L}(W - D) \xrightarrow{\sim} \Omega_L(D)$. Daher ist $i(D) = \dim_K \Omega_L(D) = \dim(W - D)$, und (nach Satz 4.3.4)

$$\dim(D) = \deg(D) + 1 - g_L + i(D) = \deg(D) + 1 - g_L + \dim(W - D).$$

2. Nach Satz 4.3.4 und 1. ist

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

und daher $\deg(W) = 2g_L - 2$.

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

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

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

und daher $\dim(W - D) \geq 1$. Wegen $\deg(W - D) = \deg(W) - \deg(D) = 0$ folgt $W - D \in (L^\times)$ nach Korollar 4.3.2, also $W \dim D$, und D ist kanonisch. □

Satz 4.5.6 (Starker Approximationssatz)**.** *Sei $r \in \mathbb{N}_0$, seien $P_0, P_1, \ldots, P_r \in \mathbb{P}_L$ verschieden, $x_1, \ldots, x_r \in L$ und $n_1, \ldots, n_r \in \mathbb{Z}$. Dann gibt es ein $x \in L$, so dass $v_{P_i}(x) = n_i$ für alle $i \in [1, r]$, und $v_P(x) \geq 0$ für alle $P \in \mathbb{P}_L \setminus \{P_0, \ldots, P_r\}$. Insbesondere gibt es ein $x \in L^\times$, so dass P_0 die einzige Polstelle von x ist.*

Beweis. Sei $\alpha \in \mathbb{A}_L$ definiert durch $\alpha_{P_i} = x_i$ für alle $i \in [1, r]$ und $\alpha_P = 0$ für alle $P \in \mathbb{P}_L \setminus \{P_1, \ldots, P_r\}$. 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 4.5.5.3 ist dann

$$0 = i(D_m) = \dim_K(\mathbb{A}_L/(\mathbb{A}_L(D_m) + L)), \quad \text{also} \quad \mathbb{A}_L = \mathbb{A}_L(D_m) + L.$$

Daher gibt es ein $z \in L$ mit $z - \alpha \in \mathbb{A}_L(D_m)$, und dann ist $v_{P_i}(z - x_i) \geq n_i + 1$ für alle $i \in [1, r]$ und $v_P(z) \geq 0$ für alle $P \in \mathbb{P}_L \setminus \{P_0, P_1, \ldots, P_r\}$.

Für $i \in [1, r]$ sei $y_i \in L$ mit $v_{P_i}(y_i) = n_i$, und es sei $\beta \in \mathbb{A}_L$ definiert durch $\beta_{P_i} = y_i$ für alle $i \in [1, r]$ und $\beta_P = 0$ für alle $P \in \mathbb{P}_L \setminus \{P_1, \ldots, P_r\}$. Sei $y \in L$ mit $y - \beta \in \mathbb{A}_L(D_m)$. Dann ist $v_{P_i}(y - y_i) \geq n_i + 1$ für alle $i \in [1, r]$ und $v_P(y) \geq 0$ für alle $P \in \mathbb{P}_L \setminus \{P_0, P_1, \ldots, P_r\}$.

Sei $x = y + z$. Für alle $i \in [1, r]$ ist dann $v_{P_i}(x - x_i) = v_{P_i}((z - x_i) + (y - y_i) + y_i) = n_i$, und für alle $P \in \mathbb{P}_L \setminus \{P_0, P_1, \ldots, P_r\}$ ist $v_P(x) \geq 0$. □

Satz 4.5.7 (Kennzeichnung rationaler Funktionenkörper)**.** *Genau dann ist L ein rationaler Funktionenkörper über K, (also $L = K(x)$), wenn $g_L = 0$ und $\mathbb{P}_L^1 \neq \emptyset$. Für jeden Divisor $P \in \mathbb{P}_L^1$ ist dann $-2P$ ein kanonischer Divisor.*

Beweis. Sei $L = K(x)$. Dann ist $\mathbb{P}_L = \{P_p \mid p \in K[X] \text{ normiert und irreduzibel}\} \cup \{P_\infty\}$. Für jedes normiert irreduzible Polynom $p \in K[X]$ ist $\deg(P_p) = \operatorname{gr}(p)$, $\deg(P_\infty) = 1$, $(x)_0 = P_X$ und $(x)_\infty = P_\infty \in \mathbb{P}_L^1$. Sei $r \in \mathbb{N}$, $r \geq 2g_L - 1$. Dann ist $\deg(rP_\infty) = r \geq 2g_L - 1$ und daher $\dim(rP_\infty) = r \deg(P_\infty) - g_L + 1 = r - g_L + 1$. Für alle $n \in [0, r]$ ist $(x^n) \geq -n(x)_\infty \geq -nP_\infty$, also $\{x^n \mid n \in [0, r]\} \subset \mathcal{L}(rP_\infty)$ und daher $r + 1 \leq \dim(rP_\infty) = r - g_L + 1$. Wegen $g_L \geq 0$ folgt $g_L = 0$.

Sei nun $g_L = 0$ und $P \in \mathbb{P}_L^1$. Wegen $\deg(P) = 1 \geq 2g_L - 1$ folgt $\dim(P) = \deg(P) + 1 - g_L = 2$ und daher $\mathcal{L}(P) \supsetneq K$. Ist $x \in \mathcal{L}(P) \setminus K$, so ist $(x) \geq -P$, $(x) \neq 0$, und daher $(x)_\infty = P$. Damit folgt $[L : K(x)] = \deg(x)_\infty = 1$ und $L = K(x)$.

Ist $L = K(x)$ und $P \in \mathbb{P}_L^1$, so ist $\deg(-2P) = -2 = 2g_L - 2$ und $\dim(-2P) = 0 = g_L$, also $-2P$ kanonisch. □

KAPITEL 5

Elliptische Funktionenkörper und elliptische Kurven

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

5.1. Elliptische Funktionenkörper

Definition 5.1.1. Ein Funktionenkörper L/K heißt *elliptisch*, wenn $g_L = 1$ und $\mathbb{P}_L^1 \neq \emptyset$.

Satz 5.1.2. *Sei L/K ein elliptischer Funktionenkörper.*

1. *Zu jedem $A \in \mathbb{D}_L$ mit $\deg(A) = 1$ gibt es genau ein $P \in \mathbb{P}_L$ 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*

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

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

$$P \oplus Q = R \iff P + Q \sim R + O \quad \text{und} \quad P \oplus Q \oplus R = O \iff P + Q + R \sim 3O\,.$$

Beweis. 1. Sei $A \in \mathbb{D}_L$ mit $\deg(A) = 1 = 2g_L - 1$. Dann ist $\dim(A) = \deg(A) + 1 - g_L = 1$ nach Satz 4.5.5, und nach Korollar 4.3.2 gibt es ein $A_1 \in \mathbb{D}_L$ mit $A_1 \geq 0$ und $A \sim A_1$. Wegen $\deg(A_1) = 1$ und $A_1 \geq 0$ ist $A_1 = P \in \mathbb{P}_L^1$. Zum Nachweis der Eindeutigkeit nehmen wir an, es seien $P, P' \in \mathbb{P}_L$ mit $P \neq P'$, $A \sim P \sim P'$. Dann folgt $\deg(P) = \deg(P') = 1$ und $0 \neq P - P' = (x)$ mit $x \in L^\times$, $(x)_\infty = P'$ und $[L\colon(x)] = \deg(x)_\infty = 1$, also $L = K(x)$, ein Widerspruch.

2. Φ ist bijektiv: Sei $\mathfrak{c} \in \mathcal{C}_L^0$ und $C \in \mathfrak{c}$, also $\deg(C) = 0$. 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 $P \in \mathbb{P}_L^1$.

Definiert man $\oplus$ auf $\mathbb{P}_L^1$ durch $P \oplus Q = R \iff \Phi(P) + \Phi(Q) = \Phi(R)$, so ist $(\mathbb{P}_L^1, \oplus)$ eine abelsche Gruppe, Φ ein Gruppenisomorphismus, $\Phi(O) = [O - O] = [0] = 0 \in \mathcal{C}_L$, und für alle P, Q, $R \in \mathbb{P}_L^1$ gilt:

$$P \oplus Q = R \iff [P-O]+[Q-O] = [R-O] \iff P+Q-2O \sim R-O \iff P+Q = R+O,$$

und wegen $\Phi(O) = 0$ auch

$$\begin{aligned} P \oplus Q \oplus R = O \iff [P - O] + [Q - O] + [R - O] = 0 &\iff P + Q + R - 3O \sim 0 \\ &\iff P + Q + R \sim 3O. \qquad \square \end{aligned}$$

Definitionen und Bemerkungen 5.1.3. 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 $\operatorname{char}(K) \neq 2$,
- $a_1 = 0$ oder $(a_1, a_3) = (1,0)$, falls $\operatorname{char}(K) = 2$.

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

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

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

$$\begin{aligned} f = f(p) &+ \frac{\partial f}{\partial X}(p)(X-\alpha) + \frac{\partial f}{\partial Y}(p)(Y-\beta) \\ &+ a_1(X-\alpha)(Y-\beta) - (a_2+3\alpha)(X-\alpha)^2 + (Y-\beta)^2 - (X-\alpha)^3\,. \end{aligned}$$

Satz 5.1.4. *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 $P \in \mathbb{P}^1_L$. Für $n \in \mathbb{N}$ ist $\deg(nP) = n \geq 1 = 2g_L - 1$, und aus Satz 4.5.5 folgt $\dim(nP) = \deg(nP) + 1 - g_L = n$, also insbesondere $K = \mathcal{L}(P) \subsetneq \mathcal{L}(2P) \subsetneq \mathcal{L}(3P)$. 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 4.3.1.1 folgt $[L\!:\!K(x_1)] = \deg(2P) = 2$, $[L\!:\!K(y_1)] = \deg(3P) = 3$, und wegen $[L\!:\!K(x_1,y_1)] \,|\, [L\!:\!K(x_1)]$ und $[L\!:\!K(x_1,y_1)] \,|\, [L\!:\!K(y_1)]$ folgt $L = K(x_1,y_1)$. Es ist $\{y_1^2, x_1y_1, y_1, x_1^3, x_1^2, x_1, 1\} \subset \mathcal{L}(6P)$ und $\dim \mathcal{L}(6P) = 6$. Daher besteht eine Relation $ay_1^2 + \alpha_1x_1y_1 + \alpha_3y_1 - bx_1^3 - \alpha_2x_1^2 - \alpha_4x_1 - \alpha_6 = 0$ mit $(a, \alpha_1, \alpha_3, b, \alpha_2, \alpha_4, \alpha_6) \in (K^7)^\bullet$. 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^3b^2 und setzen $y_2 = a^2by_1$, $x_2 = abx_1$. Dann erhalten wir $L = K(x_2,y_2)$ und

$$y_2^2 + \alpha_1x_2y_2 + \alpha_3aby_2 - x_2^3 - \alpha_2ax_2^2 - \alpha_4a^2bx_2 - \alpha_6 = 0.$$

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

$$x = x_2 \quad \text{und} \quad y = y_2 + \frac{\alpha_1x + \alpha_3ab}{2}.$$

Dann folgt $L = K(x,y)$, und es besteht eine Relation der Form $y^2 - x^3 - a_2x^2 - a_4x - a_6 = 0$ mit $a_2, a_4, a_6 \in K$.

FALL 2: $\operatorname{char}(K) = 2$ 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 $y^2 + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0$ mit $a_2, a_3, a_4, a_6 \in K$.

FALL 3: $\operatorname{char}(K) = 2$ und $\alpha_1 \neq 0$. Wir setzen $y = y_2$ und $x = \alpha_1 x_2 + \alpha_3 ab$. Dann ist $L = K(x, y)$, und es besteht eine Relation der Form $y^2 + xy - x^3 - a_2x^2 - a_4x - a_6 = 0$ mit $a_2, a_4, a_6 \in K$. □

5.2. Elliptische Kurven

Satz 5.2.1. *Sei $f \in K[X, Y]$ ein Weierstraß-Polynom und $\Delta = \Delta_f$ seine Diskriminante. Sei $C = V(f) \subset \mathbb{A}^2$, $E = \overline{C} \subset \mathbb{P}^2_{\overline{K}}$, $o = (0:1:0)$, und seien $x, y \in K[C]$ die Koordinatenfunktionen von C.*

1. *f ist absolut irreduzibel.*
2. *$E \setminus C = \{o\}$, und 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*

$$\Psi\colon E(K) \to \mathbb{P}^1_{K(E)}, \quad \text{definiert durch} \quad \Psi(p) = \mathcal{M}_p(E),$$

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

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

BEWEIS. Sei $f = Y^2 + a_1XY + a_3Y - g$ mit $g = X^3 + a_2X^2 + a_4X + a_6 \in K[X]$.

1. Wir nehmen an, $f = Y^2 + (a_1X + a_3)Y - g \in \overline{K}[X][Y]$ sei reduzibel. Dann hat f eine Faktorisierung $f = (Y - h_1)(Y - h_2)$ mit $h_1, h_2 \in K[X]$ und $\operatorname{gr}(h_1) \geq \operatorname{gr}(h_2)$. Damit folgt $h_1h_2 = -g$ und $h_1 + h_2 = -(a_1X + a_3)$, also $(\operatorname{gr}(h_1), \operatorname{gr}(h_2)) \in \{(3, 0), (2, 1)\}$ und $\operatorname{gr}(h_1 + h_2) \leq 1$, ein Widerspruch.

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

$$f^* = Y^2Z + a_1XYZ + a_3YZ^2 - X^3 - a_2X^2Z - a_4XZ^2 - a_6Z^3$$

und wegen

$$\frac{\partial f^*}{\partial Z}(0, 1, 0) = 1 \quad \text{ist } o \text{ ein regulärer Punkt von } E.$$

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

FALL 1: $\operatorname{char}(K) \neq 2$. 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 $p = (\alpha, \beta) \in \mathbb{A}^2$, wenn $2\beta = 0$ 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: $\operatorname{char}(K) = 2$ und $a_1 = 0$. Dann ist $f = Y^2 + a_3Y - g$,

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

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

FALL 3: $\mathrm{char}(K) = 2$ 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 $p = (\alpha, \beta) \in \mathbb{A}^2$, 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 $K(C) = K(E) = K(x, y)$ mit $f(x, y) = 0$. y ist algebraisch über $K(x)$, x ist algebraisch über $K(y)$, und x und y sind 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 $K(x)$. Daher folgt $[K(C) : K(x)] = 2$ und $[K(C) : K(y)] = 3$.

Wegen $o \in E(K)$ ist $O = \mathcal{M}_{o,K}(E) \in \mathbb{P}^1_{K(C)}$, und nach Satz 3.8.6 ist Ψ eine bijektive Abbildung. Ist $P \in \mathbb{P}_{K(C)}$ und $p \in C$ mit $\mathcal{O}_{p,K}(C) \subset \mathcal{O}_P$, so ist $\{x, y\} \subset K[C] \subset \mathcal{O}_P$. Daher ist O die einzige Polstelle von x und von y, und nach Satz 4.3.1 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 $\{1, x, \ldots, x^m, y, yx, \ldots, yx^{m-2}\} \subset \mathcal{L}(nO)$. Ist $n \in \mathbb{N}$ ungerade, $n = 2m + 1 \geq 3$, so ist $\{1, x, \ldots, x^m, y, yx, \ldots, yx^{m-1}\} \subset \mathcal{L}(nO)$. 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 4.5.5. 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 4.5.5), 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 $P \in \mathbb{P}^1_{K(C)}$. 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 v_O ist die negative Gradbewertung von $K(t)$ bezüglich t. Daher gibt es Polynome $p, q \in K[X]$ mit $x = p(t)$, $y = q(t)$, $\mathrm{gr}(p) = -v_O(x) = 2$ und $\mathrm{gr}(q) = -v_O(y) = 3$, woraus wir nun einen Widerspruch herleiten. Es ist $f(x, y) = f(p(t), q(t)) = 0$, und da t über K transzendent ist, folgt $f(p, q) = 0 \in K[X]$.

FALL 1: $\mathrm{char}(K) \neq 2$. Dann ist $q^2 = g(p)$, also $2qq' = g'(p)p'$, 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 $\mathrm{gr}(p') = 1$, ein Widerspruch.

FALL 2: $\mathrm{char}(K) = 2$, $a_1 = 0$. Dann ist $\Delta = a_3^4 \neq 0$, also $a_3 \neq 0$ und $q^2 + a_3 q = g(p)$. Wegen $2qq' = 0$ folgt $a_3 q' = g'(p)p'$, $\mathrm{gr}(a_3 q') = 2$ und $\mathrm{gr}(g'p) = 4$, ein Widerspruch.

FALL 3: $\mathrm{char}(K) = 2$, $(a_1, a_3) = (1, 0)$. Dann ist $\Delta = a_4^2 + a_6 \neq 0$, also $a_4^2 \neq a_6$, und $q^2 + pq = g(p)$. Es folgt $pq' + p'q = g'(p)p'$, und wegen $pq' \in 0$ ist $p' = c \in K^\times$. Sei $\tau \in \overline{K}$ mit $p(\tau) = 0$. Dann ist $cq(\tau) = cg'(0)$, also $q(\tau) = a_4$, und $q(\tau)^2 = g(0) = a_6$, ein Widerspruch.

5. Sei $p \in E(K)$ ein singulärer Punkt von E. Dann ist $p = (\alpha, \beta) \in C(K) \subset K^2$, und die Taylorentwicklung von f in p degeneriert zu

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

Wegen $f(x,y)=0$ folgt

$$t=\frac{y-\beta}{x-\alpha}\in K(x,y)\,,\quad x=t^2+\frac{a_1}{2}t-2\alpha-a_2\,,\quad y=t(x-\alpha)+\beta\,,$$

und $K(C)=K(x,y)=K(t)$. □

Definition und Bemerkung 5.2.2. Eine über K definierte *elliptische Kurve* ist eine über K definierte irreduzible projektive glatte Kurve $E\subset\mathbb{P}^2$, so dass $K(E)$ ein elliptischer Funktionenkörper ist. Dann ist die Abbildung

$$\Psi\colon E\to\mathbb{P}_{K(E)/K}\,,\quad \text{definiert durch}\quad \Psi(p)=P_p=\mathcal{M}_{p,K}(E)\,,$$

bijektiv, und $\Psi(E(K))=\mathbb{P}^1_{K(E)}$. Für $p\in E$ sei $v_p=v_{P_p}\colon K(E)\to\mathbb{Z}\cup\{\infty\}$.

Sei zunächst $o\in E(K)$ beliebig. Nach Satz 5.1.2 wird $\mathbb{P}^1_{K(E)}$ zur abelschen Gruppe mit Nullelement P_o vermöge

$$P\oplus Q=R\iff P+Q\sim R+P_o\qquad\text{für alle } P,Q,R\in\mathbb{P}^1_{K(E)}\,,$$

und dann ist die Abbildung $\mathbb{P}^1_{K(E)}\to\mathcal{C}^0_{K(E)}\,,\ P_p\mapsto[P_p-P_o]$, ein Gruppenisomorphismus. Mittels Ψ wird dann auch $E(K)$ zur abelschen Gruppe mit Nullelement o vermöge

$$p\oplus q=r\iff P_p\oplus P_q\sim P_r+P_o\quad\text{für alle } p,q,r\in E(K)\,.$$

Man nennt $\oplus$ die *Addition mit Basis* o auf $E(K)$. Für $p\in E(K)$ und $m\in\mathbb{Z}$ bezeichnet man das m-fache von p in $E(K)$ mit $[m]\,p$.

Sei nun $E=\overline{V(f)}$ mit $f=Y^2+a_1XY+a_3Y-X^3-a_2X^2-a_4X-a_6\in K[X,Y]$ und $C=V(f)=E\cap\mathbb{A}^2=E\setminus\{o\}$ mit $o=(0:1:0)$. Sei $K[C]=K[x,y]$ mit $f(x,y)=0$, also $K(C)=K(E)=K(x,y)$. Dann gilt:

A. $\mathcal{P}(x)=\mathcal{P}(y)=\{P_o\}$, $v_o(x)=-2$ und $v_o(y)=-3$.

Beweis von **A.** Sei $P\in\mathbb{P}_{K(E)}\setminus\{P_o\}$ und $p\in E$ mit $\mathcal{O}_{p,K}(E)\prec\mathcal{O}_P$. Dann ist $p\neq o$, denn aus $p=o$ folgte $P_o=\mathcal{M}_{p,K}(E)\subset P$, also $P=P_o$. Daher ist $p\in C$ und $\{x,y\}\subset K[C]\subset\mathcal{O}_{p,K}(E)\subset\mathcal{O}_P$, also $P\notin\mathcal{P}(x)\cup\mathcal{P}(y)$. Wegen $\mathcal{P})(x)\neq\emptyset$ und $\mathcal{P}(y)\neq\emptyset$ folgt $\mathcal{P}(x)=\mathcal{P}(y)=\{P_o$. Wegen $[K(x,y):K(x)]=2=\deg(x)_\infty$ und $[K(x,y):K(y)]=3=\deg(y)_\infty$ folgt $(x)_\infty=2P_o$ und $(y)_\infty=3P_o$, also $v_o(x)=-2$ und $v_o(y)=-3$. □[**A**]

Satz 5.2.3. *Sei $E\subset\mathbb{P}_{\overline{K}}$ eine elliptische Kurve, $E=\overline{V(f)}$ mit*

$$f=Y^2+a_1XY+a_3Y-X^3-a_2X^2-a_4X-a_6\in K[X,Y]\,,$$

$o=(0:1:0)$, $C=E\cap\mathbb{A}^2=E\setminus\{o\}$, $K[C]=K[x,y]$ mit $f(x,y)=0$, also $K(E)=K(x,y)$ und $\oplus$ die Addition mit Basis o auf $E(K)$.

1. *Seien $p,q\in C(K)$. Im Falle $p\neq q$ sei $L\subset\mathbb{A}^2$ die Verbindungsgerade von p und q, und im Falle $p=q$ sei L die Tangente an C in p. Dann gibt es einen eindeutig bestimmten Punkt $r\in E(K)$ mit folgenden Eigenschaften:*
   - $\overline{L}\cap E(K)=\{p,q,r\}$.
   - *Im Falle $p\neq q$ ist*
     - *entweder $r\notin\{p,q\}$;*
     - *oder $r=p$ und L ist Tangente an C in p;*

– *oder* $r = q$ *und* L *ist Tangente an* C *in* q.

Für diesen Punkt r *ist* $p \oplus q \oplus r = o$. *Insbesondere folgt* $q = \ominus p$, *falls* $o \in \overline{L}$, *und das ist genau dann der Fall, wenn* $L = V(X - \alpha)$ *mit* $\alpha \in K$.

2. *Seien* $p = (\alpha, \beta)$, $p' = (\alpha', \beta') \in C(K)$. *Dann ist* $\ominus p = (\alpha, -\beta - a_1\alpha - a_3)$, *und genau dann ist* $\alpha = \alpha'$, *wenn* $p' \in \{p, \ominus p\}$.

Im Falle $p' \neq \ominus p$ *ist* $p \oplus p' = (\alpha'', \beta'')$, *wobei*

$$\alpha'' = \lambda^2 + a_1\lambda - a_2 - \alpha - \alpha' \quad \textit{und} \quad \beta'' = -(\lambda + a_1)\alpha'' - \nu - a_3$$

mit

$$\lambda = \frac{\beta' - \beta}{\alpha' - \alpha}, \quad \nu = \frac{\beta\alpha' - \beta'\alpha}{\alpha' - \alpha}, \qquad \textit{falls} \quad p \neq p' \quad (\textit{und dann auch} \quad \alpha \neq \alpha')$$

und

$$\lambda = \frac{3\alpha^2 + 2a_2\alpha + a_4 - a_1\beta}{2\beta + a_1\alpha + a_3}, \quad \nu = \frac{-\alpha^3 + a_4\alpha + 2a_6 - a_3\beta}{2\beta + a_1\alpha + a_3}, \qquad \textit{falls} \quad p = p'$$

(*im Falle* $p = p' \neq \ominus p$ *ist* $2\beta + a_1\alpha + a_3 \neq 0$).

BEWEIS. 1. Sei $p = (\alpha, \beta) \in C(K) \subset K^2$ und $L \subset \mathbb{A}^2$ eine über K definierte Gerade mit $p \in L$, also $L = V(a(X - \alpha) + b(Y - \beta))$ mit $(a, b) \in (K^2)^\bullet$, und sei

$$\varphi = a(x - \alpha) + b(y - \beta) \in K[C].$$

Nach Satz 3.8.8 ist $v_p(\varphi) \geq 1$, und genau dann ist $v_p(\varphi) \geq 2$, wenn L die Tangente von C in p ist. Für einen Punkt $z = (\alpha', \beta') \in C(K)$ ist $\varphi = a(x - \alpha') + b(y - \beta') + a(\alpha' - \alpha) + b(\beta' - \beta)$, also $v_z(\varphi) \geq 0$. Genau dann ist $v_z(\varphi) \geq 1$, wenn $z \in L$, und genau dann ist $v_z(\varphi) \geq 2$, wenn L Tangente von C in z ist. Nach Satz 4.3.1 ist

$$(\varphi) = \sum_{P \in \mathbb{P}_{K(C)}} v_P(\varphi)P = v_o(\varphi)P_o + \sum_{z \in C(K)} v_z(\varphi)P_z + T \quad \text{mit} \quad T = \sum_{\substack{P \in \mathbb{P}_{K(E)} \\ \deg(P) \geq 2}} v_P(\varphi)P,$$

also entweder $T = 0$ oder $\deg(T) \geq 2$, und

$$0 = \deg(\varphi) = \sum_{P \in \mathbb{P}_{K(C)}} v_P(\varphi)\deg(P) = v_o(\varphi) + \sum_{z \in C(K)} v_z(\varphi) + \deg(T).$$

FALL 1: $b = 0$. Dann ist $a \neq 0$ und $o \in \overline{L}$. Wegen $v_o(x) = -2$ ist $v_o(\varphi) = -2$ und daher

$$\sum_{z \in C(K)} v_z(\varphi) + \deg(T) = 2.$$

FALL 1a: $p \neq q$. Dann ist $v_p(\varphi) \geq 1$, $v_q(\varphi) \geq 1$, also $v_p(\varphi) = v_q(\varphi) = 1$, $T = 0$ und $v_z(\varphi) = 0$ für alle $z \in C(K) \setminus \{p, q\}$. Es folgt $\overline{L} \cap E(K) = \{p, q, o\}$ und $(\varphi) = -2P_o + P_p + P_q$, also $P_p + P_{lq} + P_o \sim 3P_o$ und daher $q = \ominus p$.

FALL 1b: $p = q$. Dann ist $v_p(\varphi) \geq 2$, also $v_p(\varphi) = 2$, $T = 0$ und $v_z(\varphi) = 0$ für alle $z \in C(K) \setminus \{p\}$. Es folgt $\overline{L} \cap E(K) = \{p, o\}$ und $(\varphi) = -2P_o + 2P_p$, also $2P_p + P_o \sim 3P_o$, und $2[p] = o$.

FALL 2: $b \neq 0$. Dann ist $o \notin \overline{L}$. Wegen $v_o(x) = -2$ und $v_o(y) = -3$ ist $v_o(\varphi) = -3$, und

$$\sum_{z \in C(K)} v_z(\varphi) + \deg(T) = 3.$$

FALL 2a: $p \neq q$. Dann ist $v_p(\varphi) \geq 1$ und $v_q(\varphi) \geq 1$. Ist L die Tangente von C in p, so ist $v_p(\varphi) \geq 2$, also $v_p(\varphi) = 2$, $v_q(\varphi) = 1$, $T = 0$ und $v_z(\varphi) = 0$ für alle $z \in C(K) \setminus \{p, q\}$. Daher folgt $L \cap E(K) = \{p, q\}$ und $(\varphi) = -3P_o + 2P_p + P_q$, also $2P_p + P_q \sim 3P_o$ und daher $[2]p \oplus q = o$. Ist L die Tangente von C in q, so folgt in gleicher Weise $P_p + 2P_q \sim 3P_o$ und daher $p \oplus [2]q = o$.

Ist L nicht die Tangente von C in p und auch nicht in q, so ist $v_p(\varphi) = v_q(\varphi) = 1$, also wieder $T = 0$, und es gibt einen Punkt $r \in C(K) \setminus \{p, q\}$ mit $v_r(\varphi) = 1$. Es folgt $L \cap E(K) = \{p, q, r\}$ und $(\varphi) = -3P_o + P_p + P_q + P_r$, also $P_p + P_q + P_r \sim 3P_o$ und daher $p \oplus q \oplus r = o$.

FALL 2b: $p = q$. Dann ist $v_p(\varphi) \geq 2$. Ist $v_p(\varphi) \geq 3$, so ist $T = 0$ und $v_z(\varphi) = 0$ für alle $z \in C(K) \setminus \{p\}$. Daher folgt $L \cap E(K) = \{p\}$ und $(\varphi) = -3P_o + 3P_p$, also $3P_p \sim 3P_o$ und daher $[3]p = o$. Ist $v_p(\varphi) = 2$, so ist wieder $T = 0$, und es gibt einen Punkt $r \in C(K) \setminus \{p\}$ mit $v_r(\varphi) = 1$. Es folgt $L \cap E(K) = \{p, r\}$ und $(\varphi) = -3P_o + 2P_p + P_r$, also $2P_p + P_r \sim 3P_o$ und daher $[2]p \oplus r = o$.

2. Genau dann ist $\alpha = \alpha'$, wenn $\{p, p'\} \subset V(X - \alpha)$, und nach 1. ist das genau dann der Fall, wenn entweder $p = p'$ oder $p \oplus p' = o$. Genau dann ist $p \oplus p' = o$ (also $p' = \ominus p$), wenn $p' = (\alpha, \beta')$ und β, β' die einzigen Nullstellen von $f(\alpha, Y)$ sind. Dann gibt es ein $c \in K^\times$ mit

$$f(\alpha, Y) = c(Y - \beta)(Y - \beta'), \quad \text{also} \quad Y^2 - a_1\alpha Y - a_3 Y - g(\alpha) = cY^2 - c(\beta + \beta')Y + c\beta\beta',$$

es folgt $c = 1$ und $\beta + \beta' = -a_1\alpha - a_3$.

Sei nun $p' \neq \ominus p$. Sei L die Verbindungsgerade von p und p', falls $p \neq p'$, und sei L die Tangente von C in p, falls $p = p'$. Wegen $p \oplus p' \neq o$ ist dann $o \notin L$ und $L = V(Y - \lambda X - \nu)$ mit den angegebenen Werten für $\lambda, \nu \in K$. Genau dann ist $p \oplus p' = p'' = (\alpha'', \beta'')$, wenn $L \cap C = \{p, p', \ominus p''\}$. Das ist genau dann der Fall, wenn α, α', α'' die einzigen Nullstellen von $f(X, \lambda X + \nu)$ sind, und dann ist $\beta'' = -(\lambda\alpha'' + \nu) - a_1\alpha'' - a_3 = -(\lambda + a_1)\alpha'' - \nu - a_3$. Wir erhalten $f(X, \lambda X + \nu) = c(X - \alpha)(X - \alpha')(X - \alpha'')$ mit $c \in K^\times$ und daher

$$\begin{aligned} f(X, \lambda X + \nu) &= (\lambda X + \nu)^2 + a_1 X(\lambda X + \nu) + a_3(\lambda X + \nu) - X^3 - a_2 X^2 - a_4 X - a_6 \\ &= cX^3 - c(\alpha + \alpha' + \alpha'')X^2 + c(\alpha\alpha' + \alpha\alpha'' + \alpha'\alpha'')X - c\alpha\alpha'\alpha''. \end{aligned}$$

Es folgt $c = -1$ und $\alpha + \alpha' + \alpha'' = \lambda^2 + a_1\lambda - a_2$. □

5.3. Was ist an elliptischen Kurven elliptisch?

Wir berechnen nach klassischen Methoden der Integralrechnung den Umfang einer Ellipse mit Halbachsen $a > b$. Ein Viertelbogen ist gegeben durch die Gleichung

$$y = \frac{b}{y}\sqrt{a^2 - x^2} \quad \text{mit} \quad x \in [a, b],$$

und seine Länge berechnet sich zu

$$L = \int_0^a \sqrt{1 + y'^2}\, dx = \int_0^a \sqrt{\frac{a^4 - (a^2 - b^2)x^2}{a^2(a^2 - x^2}}\, dx = \int_0^a \frac{a^4 - (a^2 - b^2)x^2}{\sqrt{a^2(a^2 - x^2)(a^4 - (a^2 - b^2)x^2)}}\, dx.$$

Man hat also Integrale der Form

$$\int \frac{A_1 + B_1 x^2}{\sqrt{cx^4 + px^2 + q}}\, dx \quad \text{mit geeigneten Parametern } A_1, B_1, c, p, q \in \mathbb{R}$$

zu berechnen. Die Substitution

$$x = \sqrt{\frac{u - \frac{p}{3}}{\sqrt{c}}}$$

führt zu einem Integral der Form

$$\int \frac{A + Bu}{\sqrt{P(u)}}\, du = A \int \frac{du}{\sqrt{P(u)}} + B \int \frac{u\, du}{\sqrt{P(u)}}$$

mit A, $B \in \mathbb{R}$ und $P(u) = u^3 + au + b \in \mathbb{R}[u]$. Man nennt

$$\int \frac{du}{\sqrt{P(u)}} \quad \text{und} \quad \int \frac{u\, du}{\sqrt{P(u)}} \quad \textit{elliptische Integrale 1. und 2. Gattung.}$$

Wir betrachten elliptische Integrale 1. Gattung. Sei dazu $I = [d, e]$ ein Intervall mit $P(x) > 0$ für alle $x \in I$. Dann ist die Funktion

$$g\colon I \to \mathbb{R}, \quad \text{definiert durch} \quad g(y) = \int_d^y \frac{du}{\sqrt{P(u)}}$$

streng monoton wachsend, differenzierbar, und es sei $G\colon g(I) \to \mathbb{R}$ die (ebenfalls differenzierbare) Umkehrfunktion. Fr $y \in I$ und $g(y) = x$ ist dann

$$g'(y) = \frac{1}{\sqrt{P(y)}} \quad \text{und} \quad G'(x) = \frac{1}{g'(y)} = \sqrt{P(y)} = \sqrt{P(G(x))}.$$

Daher genügt G der Differenzialgleichung

$$G'^2 = P(G) = G^3 + aG + b,$$

und für alle $x \in g(I)$ ist

$$(G(x), G'(x)) \in V(Y^2 - X^3 - aX - b), \quad \text{liegt also auf einer elliptischen Kurve.}$$

KAPITEL 6

Endliche Erweiterungen algebraischer Funktionenkörper

In diesem Kapitel sei K ein vollkommener Körper.

6.1. Fortsetzung von Stellen

Definition 6.1.1. Seien L/K und L'/K' Funktionenkörper. Man nennt L'/K' eine (*endliche*) *Funktionenköpererweiterung* 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 6.1.2. *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 $\overline{L}$ eine algebraische Hülle von L, und sei $K \subset K' \subset \overline{L}$ ein Zwischenkörper mit $[K' : K] < \infty$. Dann ist $[K'L : L] = [K' : K]$, und $K'L/K'$ ist ein Funktionenkörper mit Konstanenkörper K'. Insbesondere ist $K'L/K'$ eine Konstantenerweiterung von L/K.*

Beweis. 1. Sei $x \in L$ transzendent über K und $[L : K(x)] < \infty$. Dann ist $[L' : K(x)] < \infty$ 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 3.6.3 ist $[K' : K] < \infty$.

2. Da K vollkommen ist, ist K'/K endlich separabel und daher $K' = K(\alpha)$ mit $\alpha \in K'$. Nach Satz 0.4.4 ist $[L(\alpha) : L] = \mathrm{gr}(f) = [K(\alpha) : K]$, und es bleibt zu zeigen, dass $K(\alpha)$ der Konstantenkörper von $L(\alpha)$ ist. Sei also $\beta \in L(\alpha)$ algebraisch über $K(\alpha)$. Dann ist $K(\alpha, \beta)/K$ endlich separabel, und es gibt ein $\gamma \in K(\alpha, \beta)$ mit $K(\alpha, \beta) = K(\gamma)$. Dann ist $L(\alpha) = L(\gamma)$ und $[L(\gamma) : L] = [K(\gamma) : K] \geq [K(\alpha) : K] = [L(\alpha) : L] = [L(\gamma) : L]$. Daher folgt $\beta \in K(\gamma) = K(\alpha)$. □

Satz 6.1.3. *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.*
3. *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 $v_{P'} \mid L = e\, v_P : L \to \mathbb{Z} \cup \{\infty\}$.*

(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* $L_P \to L'_{P'}$, *und wir identifizieren* L_P *mit seinem Bild in* $L'_{P'}$. *Es ist dann* $L_P \subset L'_{P'}$, $f(P'/P) = [L'_{P'} : L_P] < \infty$,

$$\deg(P') = \frac{\deg(P) f(P'/P)}{[K' : K]} .$$

und $x(P') = x(P)$ *für alle* $x \in L$.

BEWEIS. 1. Sei $P' \in \mathbb{P}_{L'}$. Wir zeigen zuerst:

A. $L \not\subset \mathcal{O}_{P'}$.

Beweis von **A.** Wir nehmen an, es sei $L \subset \mathcal{O}_{P'}$ und $z \in L' \setminus \mathcal{O}_{P'}$. Dann ist $v_{P'}(z) < 0$, und z ist algebraisch über L. Daher besteht eine Gleichung der Form $z^n + a_{n-1} z^{n-1} + \ldots + a_1 z + a_0 = 0$ mit $n \in \mathbb{N}$ und $a_0, \ldots, a_{n-1} \in L$, und dann ist $v_{P'}(a_\nu z^\nu) = \nu v_{P'}(z) + v_{P'}(a_\nu) > n v_{P'}(z) = v_{P'}(z^n)$ für alle $\nu \in [0, n-1]$, ein Widerspruch. □[**A.**]

Nach **A** ist $L \cap \mathcal{O}_{P'} \subsetneq L$, und für $x \in L \setminus \mathcal{O}_{P'}$ ist $x^{-1} \in L \cap \mathcal{O}_{P'}$. Daher ist $L \cap \mathcal{O}_{P'}$ ein Bewertungsbereich von L, und es gibt eine Stelle $P_1 \in \mathbb{P}_L$ mit $L \cap \mathcal{O}_{P'} = \mathcal{O}_{P_1}$. Dann ist $P = P' \cap L \subsetneq O_{P'} \cap L = \mathcal{O}_{P_1}$ ein Ideal, also $P \subset P_1$. Ist $x \in P_1$, so ist $x^{-1} \in L \setminus \mathcal{O}_{P_1} \subset L' \setminus \mathcal{O}_{P'}$ und daher $x \in L \cap P' = P$. Daher folgt $P = P_1 \in \mathbb{P}_L$ und $\mathcal{O}_P = \mathcal{O}_{P_1} = \mathcal{O}_{P'} \cap L$.

Zum Beweis der Einzigkeit von P sei $P_1 \in \mathbb{P}_L$ mit $P_1 \subset P'$. Dann folgt $P_1 \subset P' \cap L = P$ und daher $P_1 = P$ nach Satz 3.5.6.

2. Sei $P \in \mathbb{P}_L$. Nach Satz 4.5.6 gibt es ein $x \in L^\times$ mit $\mathcal{N}^L(x) = \{P\}$. Ist $P' \in \mathbb{P}_{L'}$, so ist genau dann $P' \in \mathcal{N}^{L'}(x)$, wenn $P' \cap L \in \mathcal{N}^L(x)$, also wenn $P' \cap L = P$ ist. Daher folgt $\mathcal{N}^{L'}(x) = \{P' \in \mathbb{P}_{L'} \mid P' \supset P\}$, und letztere Menge ist endlich und nicht leer.

3. (a) $\Rightarrow$ (c) $v_{P'} \,|\, L^\times \colon L^\times \to \mathbb{Z}$ ist ein Gruppenhomomorphismus, und für $a \in P^\bullet$ ist $v_{P'}(a) \in \mathbb{N}$. Daher ist $v_{P'}(L^\times) = e\mathbb{Z}$ mit $e \in \mathbb{N}$, und $v_0 = e^{-1} v_{P'} \,|\, L \colon L \to \mathbb{Z} \cup \{\infty\}$ ist 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 3.5.6 folgt $v_0 = v_P$, also $v_{P'} \,|\, L = e\, v_P$.

(c) $\Rightarrow$ (d) $P = \{x \in L \mid v_P(x) > 0\} = \{x \in L \mid v_{P'}(x) > 0\} = P' \cap L$.

(c) $\Rightarrow$ (e) $\mathcal{O}_P = \{x \in L \mid v_P(x) \geq 0\} = \{x \in L \mid v_{P'}(x) \geq 0\} = \mathcal{O}_{P'} \cap L$.

(d) $\Rightarrow$ (a) und (e) $\Rightarrow$ (b) Offensichtlich.

(b) $\Rightarrow$ (a) Nach 1. 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 äquivalenten 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 $L_P = \mathcal{O}_P / P \to \mathcal{O}_{P'} / P' = L'_{P'}$. Nach Identifizierung ist $K \subset L_P \subset L'_{P'}$, $[L'_{P'} : K] = [L'_{P'} : K'][K' : K] < \infty$, und

$$f(P'/P) = [L'_{P'} : L_P] = \frac{[L'_{P'} : K]}{[L_P : K]} = \frac{[L'_{P'} : K'] \, [K' : K]}{[L_P : K]} = \frac{\deg(P') \, [K' : K]}{\deg(P)} .$$

Ist $x \in \mathcal{O}_P$, so ist $x + P' = x + P \in \mathcal{L}_P \subset L'_{P'}$ aufgrund der Einbettung $K_L \subset K'_{L'}$ und daher $x(P) = x(P')$. Ist $x \in L \setminus \mathcal{O}_P \subset L' \setminus \mathcal{O}_{P'}$, so folgt $v_P(x) = v_{P'}(x) = \infty$. □

Definition 6.1.4. Sei L'/K' eine Funktionenkörpererweiterung von L/K.

1. Sei $P \in \mathbb{P}_L$, $P' \in \mathbb{P}_{L'}$ und $P' \supset P$. Man sagt dann, P' *liegt über* P, mand nennt nennt P die *Einschränkung* von P' auf L, P' eine *Fortsetzung* von P auf L' und $f(P'/P)$ den *Restklassengrad* von $P' \supset P$. Ist $v_{P'} \mid L = e v_P \colon L \to \mathbb{Z} \cup \{\infty\}$ mit $e \in \mathbb{N}$, so nennt man $e = e(P'/P)$ die *Verzweigungsordnung* von $P' \supset P$. Ist $e(P'/P) > 1$, so nennt man $P' \supset P$ *verzweigt*, andernfalls *unverzweigt*.
2. Die Abbildung $\mathsf{j}_{L'/L} \colon \mathbb{D}_L \to \mathbb{D}_{L'}$, definiert durch

$$j_{L'/L}(D) = \sum_{P \in \mathbb{P}_L} v_P(D) \sum_{\substack{P' \in \mathbb{P}_{L'} \\ P' \mid P}} e(P'/P) P' \quad \text{für alle} \quad P \in \mathbb{P}_L \,,$$

heißt *Konorm* oder *Einbettung der Divisoren*.

Satz 6.1.5. *Sei L'/K' eine Funktionenkörpererweiterung von L/K, $P \in \mathbb{P}_L$, $P' \in \mathbb{P}_{L'}$ und $P' \supset P$.*

1. *Sei $\sigma \in \mathsf{Gal}(L'/L)$. Dann ist $\sigma(P') \in \mathbb{P}_{L'}$, $\sigma(P') \supset P$, $v_{\sigma(P')} \circ \sigma = v_{P'} \colon L' \to \mathbb{Z} \cup \{\infty\}$, $f(\sigma(P')/P) = f(P'/P)$ und $f(\sigma(P')/P) = e(P'/P)$.*
2. *Sei L''/K'' eine Funktionenkörpererweiterung von L'/K', $P'' \in \mathbb{P}_{L''}$ und $P'' \supset P'$. Dann ist $e(P''/P) = e(P''/P')e(P'/P)$ und $f(P''/P) = f(P''/P')f(P'/P)$.*

Beweis. 1. $\sigma \mid \mathcal{O}_P \colon \mathcal{O}_P \to \sigma(\mathcal{O}_P)$ ist ein Ringisomorphismus. Daher ist $\sigma(\mathcal{O}_P$ ein zu $\mathcal{O}_P$ isomorpher Bewertungsbereich von L' mit maximalem Ideal $\sigma(P')$. Folglich ist $\sigma(P') \in \mathbb{P}_{L'}$, $\sigma(\mathcal{O}_P) = \mathcal{O}_{\sigma(P)}$, und $P = \sigma(P) \subset \sigma(P')$. Sei $t \in L'^{\times}$ mit $v_{P'}(t) = 1$. Dann ist $P' = t\mathcal{O}_{P'}$, also $\sigma(P') = \sigma(t)\sigma(\mathcal{O}_{P'}) = \sigma(t)\mathcal{O}_{\sigma(P'}$ und daher $v_{\sigma(P')}(\sigma(t)) = 1$. Sei $x \in L'^{\times}$ und $v_{P'}(x) = n \in \mathbb{Z}$. Dann ist $x = t^n u$ mit $u \in \mathcal{O}_{P'}^{\times}$, $\sigma(x) = \sigma(t)^n \sigma(u)$, $\sigma(u) \in \sigma(\mathcal{O}_{P'}^{\times}) = \mathcal{O}_{\sigma(P')}^{\times}$, und daher $v_{\sigma(P')}(\sigma(x)) = n = v_{P'}(x)$.

Wegen $\sigma \mid \mathcal{O}_P = \mathrm{id}_{\mathcal{O}_P}$ induziert $\sigma \colon \mathcal{O}_{P'} \to \mathcal{O}_{\sigma(P')}$ einen L_P-Isomorphismus $L'_{P'} \to L'_{\sigma(P')}$, und daher ist $f(P'/P) = f(\sigma(P')/P)$.

Ist $t \in L$ mit $v_P(t) = 1$, so ist $e(P'/P) = v_{P'}(t) = v_{\sigma(P')}(\sigma(t)) = v_{\sigma(P)}(t) = e(\sigma(P')/P)$.

2. Aus $e(P''/P)\, v_P = v_{P''} \mid L = (v_{P''} \mid L') \mid L = e(P''/P')\, v_{P'} \mid L = e(P''/P')e(P'/P)\, v_P$ folgt $e(P''/P) = e(P''/P')e(P'/P)$, und wegen $L_P \subset L'_{P'} \subset L''_{P''}$ ist $f(P''/P) = f(P''/P')f(P'/P)$. □

Satz 6.1.6. *Sei L'/K' eine Funktionenkörpererweiterung von L/K.*

1. *$\mathsf{j}_{L'/L}$ ist ein Monomorphismus. Für alle $x \in L^{\times}$ ist*

$$\mathsf{j}_{L'/L}((x)^L) = (x)^{L'}, \quad \mathsf{j}_{L'/L}((x)_0^L) = (x)_0^{L'} \quad \text{und} \quad \mathsf{j}_{L'/L}((x)_\infty^L) = (x)_\infty^{L'} .$$

2. *Für alle $P \in \mathbb{P}_L$ ist*

$$[L' : L] = \sum_{\substack{P' \in \mathbb{P}_{L'} \\ P' \supset P}} e(P'/P)\, f(P'/P) \,.$$

Insbesondere folgt

$$|\{P' \in \mathbb{P}_{L'} \mid P' \supset P\}| \le [L' : L] \,, \quad e(P'/P) \le [L' : L] \quad \text{und} \quad f(P'/P) \le [L' : L]$$

für alle $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$.

3. *Für alle $D \in \mathbb{D}_L$ ist*

$$\deg(\mathsf{j}_{L'/L}(D)) = \frac{\deg(D)\,[L'\!:\!L]}{[K'\!:\!K]}\,,$$

BEWEIS. 1. Offensichtlich ist $\mathsf{j}_{L'/L}$ ein Gruppenmmonomorphismus. Sei $x \in L^\times$. Für $P \in \mathbb{P}_L$ und $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$ ist genau dann $v_P(x) > 0$, wenn $v_{P'} > 0$. Daher folgt

$$(x)_0^{L'} = \sum_{\substack{P' \in \mathbb{P}_{L'} \\ v_{P'}(x)>0}} v_{P'}(x)\,P' = \sum_{\substack{P\in\mathbb{P}_L \\ v_P(x)>0}} \sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} e(P'/P)v_P(x)P' = \sum_{\substack{P\in\mathbb{P}_L \\ v_P(x)>0}} v_P(x)\,\mathsf{j}_{L'/L}(P) = \mathsf{j}_{L'/L}((x)_0^L)\,.$$

Nun ist aber $(x)_\infty^{L'} = -(x^{-1})_0^{L'} = -j_{L'/L}((x^{-1})_0^L) = -j_{L'/L}(-(x)_\infty^L) = j_{L'/L}((x)_\infty^L)$, und

$$(x)^{L'} = (x)_0^{L'} - (x)_\infty^{L'} = j_{L'/L}((x)_0^L) - j_{L'/L}((x)_\infty^L) = j_{L'/L}((x)_0^L - (x)_\infty^L) = j_{L'/L}((x)^L)\,.$$

2. Sei $P \in \mathbb{P}_L$. Nach Satz 4.5.6 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 $P' \supset P$ genau die Nullstellen von x in L. Aus Satz 4.3.1 folgt

$$\begin{aligned}[L'\!:\!K'(x)] = \deg((x)_0^{L'}) &= \sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} v_{P'}(x)\deg(P') = \sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} e(P'/P)v_P(x)\frac{\deg(P)f(P'/P)}{[K'\!:\!K]} \\ &= \frac{\deg((x)_0^L)}{[K'\!:\!K]} \sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} e(P'/P)f(P'/P) = \frac{[L\!:\!K(x)]}{[K'\!:\!K]} \sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} e(P'/P)f(P'/P)\end{aligned}$$

und daher

$$\sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} e(P'/P)f(P'/P) = \frac{[L'\!:\!K'(x)]\,[K'\!:\!K]}{[L\!:\!K(x)]} = \frac{[L'\!:\!K'(x)]\,[K'(x)\!:\!K(x)]}{[L\!:\!K(x)]} = [L'\!:\!L]\,.$$

3. Es genügt, die Formel für $D = P \in \mathbb{P}_L$ zu zeigen. Es ist

$$\deg(\mathsf{j}_{L'/L}(P)) = \sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} e(P'/P)\deg(P') = \sum_{\substack{P'\in\mathbb{P}_{L'} \\ P'\supset P}} e(P'/P)\frac{\deg(P)f(P'/P)}{[K'\!:\!K]} = \frac{\deg(P)\,[L'\!:\!L]}{[K'\!:\!K]}\,.\ \square$$

6.2. Ganze Größen und Holomorphiebereiche

Definition 6.2.1. Sei L/K ein Funktionenkörper mit Konstantenkörper K. Für eine Teilmenge $S \subset \mathbb{P}_L$ sei

$$\mathcal{O}_S = \bigcap_{P\in S} \mathcal{O}_P \qquad (\text{also } \mathcal{O}_S = K, \text{ falls } S = \mathbb{P}_L, \text{ und } \mathcal{O}_S = L, \text{ falls } S = \emptyset\,).$$

$\mathcal{O}_S$ 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 $\emptyset \neq S \subsetneq \mathbb{P}_L$. Insbesondere ist jeder Bewertungsbereich $\mathcal{O}$ mit $K \subsetneq \mathcal{O} \subsetneq L$ ein Holomorphiebereich.

Definition 6.2.2. 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 ist $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ mit $n \in \mathbb{N}$ und $a_0, \ldots, a_{n-1} \in R$. Jede solche Gleichung heißt *ganze Gleichung* von x über R.]
2. Eine *ganz-algebraische Zahl* ist eine komplexe Zahl, die ganz über $\mathbb{Z}$ ist.
3. $\mathrm{cl}_L(R) = \{x \in L \mid x \text{ ist ganz über } R\}$ heißt *ganzer Abschluss* von R in L.
4. R heißt *ganz-abgeschlossen*, wenn $\mathrm{cl}_{\mathsf{q}(R)}(R) = R$.

Satz 6.2.3. *Sei L/K ein Funktionenkörper und $\emptyset \neq S \subsetneq \mathbb{P}_L$.*

1. *$L = \mathsf{q}(\mathcal{O}_S)$.*
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 $\mathcal{O}_S \subset \mathcal{O}_T$.*

Beweis. 1. Sei $x \in L^\times$. Nach Satz 4.5.6 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 $x = z^{-1}(xz) \in \mathsf{q}(\mathcal{O}_S)$.

2. Wir nehmen an, $x \in L \setminus \mathcal{O}_S$ sei ganz über $\mathcal{O}_S$. Dann gibt es ein $P \in S$ mit $v_P(x) < 0$, und es besteht eine ganze Gleichung $x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0 = 0$ mit $n \in \mathbb{N}$ und $a_0, \ldots, a_{n-1} \in S$. Dann ist aber $v_P(x^n) = nv_P(x) < v_P(a_ix^i)$ für alle $i \in [0, n-1]$, ein Widerspruch.

3. Sei $S = \{P_1, \ldots, P_n\}$ und $\{0\} \neq \mathfrak{a} \lhd \mathcal{O}_S$. 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 3.5.7 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 $z_1, \ldots, z_n \in \mathcal{O}_S$, $a = a_1z_1 + \ldots + a_nz_n \in \mathfrak{a}$, und wir zeigen $\mathfrak{a} = a\mathcal{O}_S$. Für $i \in [1, n]$ ist $v_{P_i}(a_iz_i) = n_i$, und für alle $j \in [1, n] \setminus \{i\}$ ist $v_{P_i}(a_jz_j) > n_i$. Daher folgt $v_{P_i}(a) = n_i$, also insbesondere $a \neq 0$. Ist nun $x \in \mathfrak{a}$, so folgt $v_{P_i}(a^{-1}x) = -m_i + v_{P_i(x)} \geq 0$ für alle $i \in [1, n]$, also $a^{-1}x \in \mathcal{O}_S$ und $x \in a\mathcal{O}_S$.

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 4.5.6 gibt es ein $x \in L$ mit $v_Q(x) < 0$ und $v_P(x) \geq 0$ für alle $P \in S$, also $x \in \mathcal{O}_S \setminus \mathcal{O}_T$. □

Satz 6.2.4. *Sei L/K ein Funktionenkörper mit Konstantenkörper K, sei R ein Bereich mit $K \subset R \subset L$, und sei R kein Körper. Dann ist $\emptyset \neq S(R) = \{P \in \mathbb{P}_L \mid R \subset \mathcal{O}_P\} \subsetneq \mathbb{P}_L$, und*

$$\mathcal{O}_{S(R)} \bigcap_{\substack{P \in \mathbb{P}_L \\ R \subset \mathcal{O}_P}} \mathcal{O}_P = \mathrm{cl}_L(R).$$

Insbesondere ist $\mathrm{cl}_L(R)$ ein ganz-abgeschlossener Teilbereich von L und $\mathsf{q}(\mathrm{cl}_L(R)) = L$.

Beweis. Da R kein Körper ist, gibt es ein Ideal $\{0\} \neq I \subsetneq R$, und nach Satz 3.2.3 gibt es ein $P \in \mathbb{P}_L$ mit $R \subset \mathcal{O}_P$, also $P \in S(R)$. Ist $x \in R \setminus K$, so gibt es ein $P \in \mathbb{P}_L$ mit $v_P(x) < 0$ und daher $P \notin S(R)$. Damit folgt $\emptyset \neq S(R) \subsetneq \mathbb{P}_L$.

Offensichtlich ist $R \subset \mathcal{O}_{S(R)}$ und $\mathrm{cl}_L(R) \subset \mathrm{cl}_L(\mathcal{O}_{S(R)} = \mathcal{O}_{S(R)}$. Sei nun $0 \neq z \in \mathcal{O}_{S(R)}$. Dann ist $z^{-1}R[z^{-1}] \lhd R[z^{-1}]$, und es genügt, $z^{-1}R[z^{-1}] = R[z^{-1}]$ zu zeigen. Dann besteht nämlich eine Gleichung der Form $1 = z^{-1}(a_0 + a_1z^{-1} + \ldots + a_nz^{-n})$ mit $n \in \mathbb{N}$, $a_0, \ldots, a_n \in R$, und es folgt $z^{n+1} - a_0z^n - a_1z^{n-1} - \ldots - a_n = 0$, also $z \in \mathrm{cl}(R)$.

Wir nehmen nun an, es sei $z^{-1}R[z^{-1}] \subsetneq R[z^{-1}]$. Nach Satz 3.2.3 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. □

Bemerkung 6.2.5. Teile von Satz 6.2.4 sind ein Spezialfall des folgenden allgemeineren Satzes, den wir hier nicht beweisen:

Sei L ein Körper und $R \subset L$ ein Teilring. Dann ist $R' = \mathrm{cl}_L(R)$ ein ganz-abgeschlossener Bereich.

Satz und Definition 6.2.6. *Sei L'/L eine separable Körpererweiterung, $[L':L] = n \in \mathbb{N}$ und $\mathrm{Hom}_L(L', \overline{L'}) = \{\sigma_1, \ldots, \sigma_n\}$.*

Für $x \in L'$ definieren wir die *Spur* von x über L durch $\mathsf{S}_{L'/L}(x) = \sigma_1(x) + \ldots + \sigma_n(x)$.

1. *Ist $(u_1, \ldots, u_n)$ eine L-Basis von L', so gibt es genau eine L-Basis $(u_1^*, \ldots, u_n^*)$ von L', so dass $\mathsf{S}_{L'/L}(u_i u_j^*) = \delta_{i,j}$ für alle $i, j \in [1,n]$. $(u_1^*, \ldots, u_n^*)$* heißt die zu *$(u_1, \ldots, u_n)$ komplementäre* Basis. *$(u_1, \ldots, u_n)$ ist die zu $(u_1^*, \ldots, u_n^*)$ komplementäre Basis.*
2. *$\mathsf{S}_{L'/L}\colon L' \to L$ ist ein L-Vektorraumepimorphismus, und für $a \in L$ ist $\mathsf{S}_{L'/L}(a) = na$.*
3. *Sei $L \subset M \subset L'$ ein Zwischenkörper. Dann ist $\mathsf{S}_{L'/L} = \mathsf{S}_{M/L} \circ \mathsf{S}_{L'/M}$.*
4. *Sei $x \in L'$, $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1 X + a_0 \in L[X]$ das Minimalpolynom von x über L und $m = [L':L(x)]$. Dann ist $\mathsf{S}_{L'/L}(x) = -m a_{d-1}$.*
5. *Sei $a \in L'$ und $\mu_a\colon L' \to L'$ definiert durch $\mu_a(x) = ax$. Dann ist $\mu_a \in \mathrm{End}_L(L')$, und $\mathsf{S}_{L'/L}(a) = \mathsf{S}(\mu_a)$ ist die Spur des L-Vektorraumendomorphismus μ_a.*

Beweis. 1. Sei $L' = L(\alpha)$ und $A = (\sigma_i(\alpha^{\nu-1}))_{i,\nu\in[1,n]}$. Dann ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine L-Basis von L', und (Vandermonde'sche Determinante)

$$\det(A) = \prod_{1\le i<j\le n} (\sigma_j(\alpha) - \sigma_i(\alpha)) \neq 0\,.$$

Sei $(u_1, \ldots, u_n) \in L'^n$ eine L-Basis von L' und $(u_1^*, \ldots, u_n^*) \in L'^n$. Dann gibt es Matrizen $T, T^* \in \mathsf{M}_n(L)$ mit $(u_1, \ldots, u_n) = (1, \alpha, \ldots, \alpha^{n-1})T$, $(u_1^*, \ldots, u_n^*) = (1, \alpha, \ldots, \alpha^{n-1})T^*$ 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

$$(\mathsf{S}_{L'/L}(u_i u_j^*))_{i,\,j\in[1,n]} = U^{\mathsf{t}}U^* = T^{\mathsf{t}}A^{\mathsf{t}}AT^*$$

Daher gibt es genau eine Matrix $T^* \in \mathsf{GL}_n(L)$, so dass $\mathsf{S}_{L'/L}(u_i u_j^*) = \delta_{i,j}$ für alle $i, j \in [1,n]$, und damit folgt die Existenz und Eindeutigkeit von $(u_1^*, \ldots, u_n^*)$.

2. Für $x, y \in L'$ und $a \in L$ ist

$$\mathsf{S}_{L'/L}(x+y) = \mathsf{S}_{L'/L}(x) + \mathsf{S}_{L'/L}(y)\,, \quad \mathsf{S}_{L'/L}(ax) = a\mathsf{S}_{L'/L}(x) \quad \text{und} \quad \mathsf{S}_{L'/L}(a) = na\,.$$

Für jeden L-Homomorphismus $\sigma\colon L' \to \overline{L'}$ gibt es ein $\overline{\sigma} \in G_L$ mit $\overline{\sigma}\,|\,L = \sigma$, und dann ist $(\overline{\sigma}\circ\sigma_1, \ldots, \overline{\sigma}\circ\sigma_n) = (\sigma_1, \ldots, \sigma_n)$. Es folgt $\sigma(\mathsf{S}_{L'/L}(x) = \overline{\sigma}(\mathsf{S}_{L'/L}(x) = \mathsf{S}_{L'/L}(x)$, also $\mathsf{S}_{L'/L}(x) \in L$. Daher ist $\mathsf{S}_{L'/L}\colon L' \to L$ ein L-Vektorraumhomomorphismus. Nach 2. ist $\mathsf{S}_{L'/L} \neq 0$, und daher ist $\mathsf{S}_{L'/L}$ ein Epimorphismus.

3. Sei $\mathrm{Hom}_L(M, \overline{L'}) = \{\tau_1, \ldots, \tau_d\}$ und $\mathrm{Hom}_M(L', \overline{L'}) = \{\sigma_1, \ldots, \sigma_m\}$. Für $i \in [1,d]$ sei $\overline{\tau}_i \in G_L$ mit $\overline{\tau}_i\,|\,M = \tau_i$. Dann ist $\mathrm{Hom}_L(L', \overline{L'}) = \{\overline{\tau}_i\circ\sigma_j \mid i \in [1,d]\,,\ j \in [1,m]\,\}$, und für $x \in L'$ folgt

$$\mathsf{S}_{L'/L}(x) = \sum_{i=1}^{d}\sum_{j=1}^{m} \overline{\tau}_i\circ\sigma_j(x) = \sum_{i=1}^{d} \overline{\tau}_i(\mathsf{S}_{L'/M}(x)) = \sum_{i=1}^{d} \tau_i(\mathsf{S}_{L'/M}(x)) = \mathsf{S}_{M/L}\circ\mathsf{S}_{L'/M}(x)\,.$$

4. Es ist $n = [L'\!:\!L(x)]\,[L(x)\!:\!L] = md$. Sei $\mathrm{Hom}_L(L(x), \overline{L'}) = \{\sigma_1, \ldots, \sigma_d\}$. 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 $\mathsf{S}_{L'/L}(x) = \mathsf{S}_{L(x)/L} \circ \mathsf{S}_{L'/L(x)}(x) = \mathsf{S}_{L(x)/L}(mx) = m\mathsf{S}_{L(x)/L}(x) = -ma_{d-1}$.

5. Sei $[L'\!:\!L(a)] = m$, $L(a)\!:\!L] = d$ und $f = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in L[X]$ das Minimalpolynom von a über L. Dann ist $(1, a, \ldots, a^{d-1})$ eine L-Basis von $L(a)$, und

$$a\,(1, a, \ldots, a^{d-1}) = (1, a, \ldots, a^{d-1})\,T \quad \text{mit} \quad T = \begin{pmatrix} 0 & 0 & \ldots & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & \ldots & 0 & -a_1 \\ 0 & 1 & \ldots & \ldots & 0 & -a_2 \\ . & . & \ldots & \ldots & . & . \\ 0 & 0 & \ldots & \ldots & 1 & -a_{d-1} \end{pmatrix}.$$

T ist die Matrix des Endomorphismus $\mu'_a = \mu_a \,|\, L(a)$ bezüglich der Basis $(1, a, \ldots, a^{n-1})$, und daher ist $\mathsf{S}(\mu'_a) = \mathsf{S}(T) = -a_{d-1}$. Sei $(v_1, \ldots, v_m)$ eine $L(a)$-Basis von L'. Dann erhalten wir einen L-Vektorraumisomorphismus $\phi\colon L(a)^m \to L'$, definiert durch $\phi(x_1, \ldots, x_m) = x_1v_1 + \ldots + x_mv_m$, und ein kommutatives Diagramm

$$\begin{array}{ccc} L(a)^m & \xrightarrow{\ \phi\ } & L' \\ {\scriptstyle \mu_a'^m}\downarrow & & \downarrow{\scriptstyle \mu_a} \\ L(a)^m & \xrightarrow{\ \phi\ } & L' \end{array}$$

Damit folgt $\mathsf{S}(\mu_a) = \mathsf{S}(\mu_a'^m) = m\mathsf{S}(\mu'_a) = -ma_{d-1} = \mathsf{S}_{L'/L}(a)$ nach 4. □

Satz 6.2.7. *Sei L'/L eine separable Körpererweiterung, $[L' : L] = n \in \mathbb{N}$, $R \subset L$ ein ganz-abgeschlossener Teilbereich, $L = \mathsf{q}(R)$ und $R' = \mathrm{cl}_{L'}(R)$.*

1. *Sei $x \in L'$ und $f \in L[X]$ das Minimalpolynom von x über L. Genau dann ist $x \in R'$, wenn $f \in R[X]$, und dann ist $\mathsf{S}_{L'/L}(x) \in R$.*
2. *$L' = \{a^{-1}x \mid a \in R^\bullet,\ x \in R'\}$. Insbesondere enthält R' eine L-Basis von L'.*
3. *Sei $(u_1, \ldots, u_n) \in R'^n$ eine L-Basis von L' und $(u_1^*, \ldots, u_n^*)$ die zu $(u_1, \ldots, u_n)$ komplementäre Basis. Dann ist $R' \subset Ru_1^* + \ldots + Ru_n^*$.*
4. *Ist R ein Hauptidealbereich, so gibt es eine K-Basis $(u_1, \ldots, u_n)$ von L mit*

$$R' = Ru_1 + \ldots + Ru_n\,.$$

Beweis. 1. Ist $f \in R[X]$, so ist $f(x) = 0$ eine ganze Gleichung für x über R, also $x \in R'$, und nach Satz 6.2.6 ist $\mathsf{S}_{L'/L}(x) \in R$.

Sei nun $x \in R'$ und $g \in R[X]$ ein normiertes Polynom mit $g(x) = 0$. Sei L^* ein Zerfällungskörper von f über L, seien $x_1, \ldots, x_n$ die Nullstellen von f in L^*, und seien $\sigma_1, \ldots, \sigma_n\colon L' \to L^*$ die eindeutig bestimmten L-Homomorphismen mit $\sigma_i(x) = x_i$ für alle $i \in [1, n]$. Nach Bemerkung 6.2.5 ist $R^* = \mathrm{cl}_{L^*}(R)$ ein ganz-abgeschlossener Bereich. Wegen $g(x_i) = \sigma_i(g(x)) = 0$ für alle $i \in [1, n]$ ist $\{x_1, \ldots, x_n\} \subset R^*$, und daher liegen die Koeffizienten von f in $R^* \cap K = R$.

2. Offensichtlich ist $\{a^{-1}x \mid a \in R^\bullet,\ x \in R'\} \subset L'$. Sei nun $x \in L'$ und

$$f = X^d + a_{d-1}X^{d-1} + \ldots + a_1X + a_0 \in L[X]$$

das Minimalpolynom von x über L. Sei $a \in R^\bullet$, so dass $aa_i \in R$ für alle $i \in [0, d-1]$. Dann folgt

$$(ax)^d + \sum_{i=1}^{d-1} a^i a_{d-i} (ax)^{d-i} = 0\,,$$

also $ax \in R'$, und $x = a^{-1}(ax)$.

3. Sei $a \in R'$, $a = c_1 u_1^* + \ldots + c_n u_n^*$ mit $c_1, \ldots, c_n \in L$. Dann folgt $au_i \in R'$ für alle $i \in [1, r]$, und

$$\mathsf{S}_{L'/L}(au_i) = \sum_{\nu=1}^{n} c_\nu \mathsf{S}_{L'/L}(u_i^* u_\nu) = c_i \in R$$

für alle $i \in [1, r]$. Daher ist $a \in Ru_1^* + \ldots + Ru_n^*$.

4. Nach 3. ist R' Untermodul eines endlich erzeugten freien R-Moduls, also selbst frei (nach dem Hauptsatz für endlich erzeugte Moduln über Hauptidealbereichen). □

Satz und Definition 6.2.8. *Sei L'/K' eine Funktionenkörpererweiterung von L/K.*

1. *Sei $P \in \mathbb{P}_L$. Dann ist*

$$\mathcal{O}'_P = \mathrm{cl}_{L'} \mathcal{O}_P = \bigcap_{P' \mid P} \mathcal{O}_{P'}\,,$$

und es gibt eine L-Basis $(u_1, \ldots, u_n)$ von L', so dass $\mathcal{O}'_P = \mathrm{cl}_{L'}\mathcal{O}_P = \mathcal{P}_P u_1 + \ldots + \mathcal{O}_P u_n$.
Eine L-Basis $(u_1, \ldots, u_n)$ von L' mit $\mathcal{O}'_P = \mathrm{cl}_{L'}\mathcal{O}_P = \mathcal{P}_P u_1 + \ldots + \mathcal{O}_P u_n$ heißt *P-Ganzheitsbasis von L'/L.*

2. *Jede L-Basis von L' ist eine P-Ganzheitsbasis für fast alle $P \in \mathbb{P}_L$.*

Beweis. 1. Nach den Sätzen 6.2.4 und 6.2.7.

2. Sei $(u_1, \ldots, u_n)$ eine L-Basis von L' und $(u_1^*, \ldots, u_n^*)$ die komplementäre Basis. Dann gibt es eine endliche Menge $S \subset \mathbb{P}_L$, so dass alle Polstellen der Koeffizienten der Minimalpolynome von $u_1, \ldots, u_n$, $u_1^*, \ldots, u_n^*$ in S liegen. Für alle $P \in \mathbb{P}_L \setminus S$ ist dann $\{u_1, \ldots, u_n, u_1^*, \ldots u_n^*\} \subset \mathcal{O}'_P$, und aus Satz 6.2.7 folgt

$$\mathcal{O}'_P \subset \sum_{i=1}^{n} \mathcal{O}_P u_i^* \subset \mathcal{O}'_P\,, \quad \text{also Gleichheit.}$$ □

Satz 6.2.9. *Sei L'/K' eine Funktionenkörpererweiterung von L/K, $P \in \mathbb{P}_L$ und $u \in \mathcal{O}'_P$. Dann ist*

$$\mathsf{S}_{L'/L}(u)(P) = \sum_{\substack{P' \in \mathbb{P}_{L'} \\ P' \supset P}} e(P'/P)\, \mathsf{S}_{L'_{P'}/L_P}(u(P')) \in L_P$$

Beweis. Sei $\{P_1, \ldots, P_r\} = \{P' \in \mathbb{P}_{L'} \mid P' \supset P$ und $t \in L$ mit $v_P(t) = 1$. Für alle $i \in [1, r]$ ist dann $v_{P_i}(t) = e_i = e(P_i/P)$, $t\mathcal{O}_{P_i} = P_i^{e_i}$, , und die Restklassenringe $V = \mathcal{O}'_P/t\mathcal{O}'_P$ und $V_i = \mathcal{O}_{P_i}/t\mathcal{O}_{P_i}$ sind endlich-dimensionale L_P-Vektorräume. Sei

$$\chi\colon \mathcal{O}'_P \to \bigoplus_{i=1}^{r} V_i \quad \text{definiert durch} \quad \chi(x) = (x + t\mathcal{O}_{P_1}, \ldots, x + t\mathcal{O}_{P_r}).$$

Dann ist χ ein L_P-Vektorraumisomorphismus. Wir zeigen:

A. χ is surjektiv, und $\mathrm{Ker}(\chi) = t\mathcal{O}'_P$.

Beweis von **A.** Nach Satz 6.2.8 ist

$$\mathrm{Ker}(\chi) = \bigcap_{i=1}^{r} t\mathcal{O}_{P_i} = t\mathcal{O}'_P.$$

Zum Nachweis der Surjektivität sei $(x_1, \ldots, x_r) \in \mathcal{O}_{P_1} \times \ldots \times \mathcal{O}_{P_r} \subset L'^r$. Nach Satz 3.5.7 gibt es ein $x \in L'$ mit $v_{P_i}(x - x_i) \geq e_i = v_{P_i}(t)$, also $v_{P_i}(x) \geq \min\{v_{P_i}(x - x_i), v_{P_i}(x_i)\} \geq 0$ für alle $i \in [1, r]$. Damit folgt $x \in \mathcal{O}_{P_1} \cap \ldots \cap \mathcal{O}_{P_r} = \mathcal{O}'_P$ und

$$\chi(x) = (x + t\mathcal{O}_{P_1}, \ldots, x + t\mathcal{O}_{P_r}) = (x_1 + t\mathcal{O}_{P_1}, \ldots, x_r + t\mathcal{O}_{P_r}). \qquad \square[\mathbf{A}]$$

χ induziert einen L_P-Vektorraumisomorphismus

$$\overline{\chi}\colon V \ \to \ \bigoplus_{i=1}^{r} V_i.$$

Seien nun $\mu\colon V \to V$ und $\mu_i\colon V_i \to V_i$ für alle $i \in [1, r]$ definiert durch $\mu(x + t\mathcal{O}'_P) = ux + t\mathcal{O}'_P$ und $\mu_i(x + t\mathcal{O}_{P_i}) = ux + t\mathcal{O}_{P_i}$. μ und μ_i sincd L_P-Vektorraumendomorphismen und induzieren ein kommutatives Diagramm

$$\begin{array}{ccc} V & \xrightarrow{\overline{\chi}} & \bigoplus_{i=1}^{r} V_i \\ {\scriptstyle\mu}\big\downarrow & & \big\downarrow{\scriptstyle\bigoplus_{i=1}^{r}\mu_i} \\ V & \xrightarrow{\overline{\chi}} & \bigoplus_{i=1}^{r} V_i \ . \end{array}$$

Damit folgt $\mathsf{S}(\mu) = \mathsf{S}(\mu_1) + \ldots + \mathsf{S}(\mu_r)$.

Sei nun $(u_1, \ldots, u_n) \in \mathcal{O}'^n_P$ eine P-Ganzheitsbasis und

$$uu_j = \sum_{\nu=1}^{n} c_{j,\nu} u_\nu \quad \text{mit} \quad c_{j,\nu} \in \mathcal{O}_P \quad \text{für alle} \quad j \in [1, n].$$

Dann ist $(u_1 + t\mathcal{O}'_P, \ldots, u_n + t\mathcal{O}'_P)$ eine L_P-Basis von V, und

$$\mu(u_j + t\mathcal{O}'_P) = uu_j + t\mathcal{O}'_P = \sum_{\nu=1}^{n} c_{j,\nu}(u_\nu + t\mathcal{O}'_P) = \sum_{\nu=1}^{n} c_{j,\nu}(P)(u_\nu + t\mathcal{O}'_P) \quad \text{für alle} \quad j \in [1, n].$$

Damit folgt

$$\mathsf{S}(\mu) = \sum_{\nu=1}^{n} c_{\nu,\nu}(P) = \mathsf{S}_{L'/L}(u)(P),$$

und es bleibt zu zeigen: Für alle $i \in [1, r]$ ist $\mathsf{S}(\mu_i) = e_i \mathsf{S}_{L'_{P_i}/L_P}(u(P_i))$.

Sei $i \in [1, r]$ fest. Sei $t_i \in L'$ mit $v_{P_i}(t_i) = 1$, und sei $\mu_i^*\colon L'_{P_i} \to L'_{P_i}$ definiert durch

$$\mu_i^*(x(P_i)) = ux(P_i) = u(P_i)(x(P_i) \quad (\text{für} \quad x \in \mathcal{O}_{P_i}).$$

Dann ist μ_i^* ein L_P-Vektorraumhomomorphismus, und $\mathsf{S}(\mu_i^*) = \mathsf{S}_{L'_{P_i}/L_P}(u(P_i))$. Daher müssen wir zeigen:

$$e_i \mathsf{S}(\mu_i^*) = \mathsf{S}(\mu_i).$$

Wir betrachten die Folge von L_P-Untervektorräumen

$$V_i = V_i^{(0)} \supset V_i^{(1)} \supset \ldots \supset V_i^{(e_i)} = \{0\} \quad \text{mit} \quad V_i^{(j)} = P_i^j / t\mathcal{O}_{P_i} \quad \text{für alle} \quad j \in [0, e_i].$$

Für $j \in [0, e_i - 1]$ ist $\mu_i(V_i^{(j)}) \subset V_i^{(j)}$, $\mu_i(V_i^{(j+1)}) \subset V_i^{(j+1)}$, und daher induziert μ_i einen L_P-Vektorraumhomomorphismus $\mu_i^{(j)} \colon V_i^{(j)}/V_i^{(j+1)} \to V_i^{(j)}/V_i^{(j+1)}$. Seien die L_P-Vektorraumisomorphismen $\beta_j' \colon V_i^{(j)}/V_i^{(j+1)} \xrightarrow{\sim} P_i^j/P_i^{j+1}$ und $\beta_j'' \colon P_i^j/P_i^{j+1} \xrightarrow{\sim} L'_{P_i}$ wie folgt definiert: Für eine Restklasse $\gamma = (x + t\mathcal{O}_{P_i}) + V_i^{(j+1)} \in V_i^{(j)}/V_i^{(j+1)}$ (mit $x \in P_i^j$) sei $\beta_j'(\gamma) = x + P_i^{j+1}$, und für eine Restklasse $t_i^j w + P_i^{j+1} \in P_i^j/P_i^{j+1}$ (mit $w \in \mathcal{O}_{P_i}$) sei $\beta_j''(t_i^j w + P_i^{j+1}) = w + P_i \in L'_{P_i}$. Dann ist $\beta_j = \beta_j'' \circ \beta_j' \colon V_i^{(j)}/V_i^{(j+1)} \to L'_{P_i}$ ein Isomorphismus, wir erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} V_i^{(j)}/V_i^{(j+1)} & \xrightarrow{\beta_j} & L'_{P_i} \\ {\scriptstyle \mu_i^{(j)}}\big\downarrow & & \big\downarrow{\scriptstyle \mu_i^*} \\ V_i^{(j)}/V_i^{(j+1)} & \xrightarrow{\beta_j} & L'_{P_i}\ . \end{array}$$

Insbesondere ist $\dim_{L_P}(V_i^{(j)}/V_i^{(j+1)} = \dim_{L_P} L'_{P_i} = f(P_i/P) = f_i$ unabhängig von j, und $\mathsf{S}(\mu_i^{(j)}) = \mathsf{S}(\mu_i^*)$. Daher müssen wir zeigen:

$$\sum_{j=0}^{e_i-1} \mathsf{S}(\mu_i^{(j)}) = \mathsf{S}(\mu_i).$$

Sei $\boldsymbol{v}^{(j)} = (v_1^{(j)}, \ldots, v_{f_i}^{(j)}) \in (V_i^{(j)})^{f_i}$ ein Repräsentantensystem einer L_P-Basis von $V_i^{(j)}/V_i^{(j+1)}$. Dann it $(\boldsymbol{v}^{(0)}, \ldots, \boldsymbol{v}^{(e_i-1)})$ eine L_P-Basis von V_i und

$$(u\boldsymbol{v}^{(0)}, \ldots, u\boldsymbol{v}^{(e_i-1)}) = (\boldsymbol{v}^{(0}, \ldots, \boldsymbol{v}^{(e_i-1)}) \quad \begin{pmatrix} T_0 & 0 & \ldots & 0 & 0 \\ T_{0,1} & T_1 & \ldots & 0 & 0 \\ . & . & . & . & . \\ T_{0,e_i-2} & T_{1,e_i-2} & \ldots & T_{e_i-2} & 0 \\ T_{0,e_i-1} & T_{1,e_i-1} & \ldots & T_{e_i-2,e_i-1} & T_{e_i-1} \end{pmatrix}$$

mit Matrizen T_i, $T_{i,j} \in \mathsf{M}_{f_i}(L_P)$. Für alle $j \in [0, e_i - 1]$ ist $\mu_i(\boldsymbol{v}^{(j)}) = u\boldsymbol{v}^{(j)}$, und daher folgt $\mathsf{S}(\mu_i) = \mathsf{S}(T_0) + \ldots + \mathsf{S}(T_{e_i-1})$. Es bleibt zu zeigen: Für alle $j \in [0, e_i - 1]$ ist $\mathsf{S}(\mu_i^{(j)}) = \mathsf{S}(T_j)$.

Sei $j \in [0, e_i - 1]$ und $\pi_j \colon V_i^{(j)} \to V_i^{(j)}/V_i^{(j+1)}$ der natürliche Restklassenhomomorphismus von L_P-Vektorräumen. Dann ist $\pi_j(\boldsymbol{v}^{(j)} = (\pi_j(v_1^{(j)}), \ldots, \pi_j(v_{f_i}^{(j)}))$ eine L_P-Basis von $V_i^{(j)}/V_i^{(j+1)}$, und für alle $\nu \in [1, f_j]$ ist $\mu_i^{(j)}(\pi_j(v_\nu^{(j)})) = \pi_j(uv_\nu^{(j)})$. Damit folgt

$$\big(\mu_i^{(j)}(\pi_j(v_1^{(j)})), \ldots, \mu_i^{(j)}(\pi_j(v_{f_i}^{(j)}))\big) = \pi_j(u\boldsymbol{v}^{(j)}) = \pi_j\Big(\boldsymbol{v}^{(j)}T_j + \sum_{\nu=j+1}^{e_i-1} \boldsymbol{v}^{(\nu)}T_{j,\nu}\Big) = \pi_j(\boldsymbol{v}^{(j)})T_j,$$

da $\pi_j(\boldsymbol{v}^{(\nu)}) = \mathbf{0}$ für alle $\nu \in [j+1, e_i - 1]$, und wir erhalten $\mathsf{S}(\mu_i^{(j)}) = \mathsf{S}(T_j) \in L_P$. □

6.3. Differententheorie

Satz und Definition 6.3.1. *Sei L'/K' eine Funktionenkörpererweiterung von L/K, $P \in \mathbb{P}_L$ und $\mathcal{O}'_P = \mathrm{cl}_{L'}(\mathcal{O}_P)$.*
Dann heißt $\mathcal{C}_P = \{z \in L' \mid \mathsf{S}_{L'/L}(z\mathcal{O}'_P) \subset \mathcal{O}_P\}$ der *Komplementärmodul* von L'/L über $\mathcal{O}_P$.

1. *Sei* $(u_1, \ldots, u_n)$ *eine* P*-Ganzheitsbasis von* L'/L *und* $(u_1^*, \ldots, u_n^*)$ *die komplementäre Basis. Dann ist* $\mathcal{C}_P = \mathcal{O}_P u_1^* + \ldots + \mathcal{O}_P u_n^* \supset \mathcal{O}'_P$*, 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* $P' \supset P$ *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 $d(P') = -v_{P'}(t) \in \mathbb{N}_0$ heißt *Differentenexponent* von P', und der Divisor

$$D_{L/L'} = \sum_{P \in \mathbb{P}_L} \sum_{\substack{P' \in \mathbb{P}_{L'} \\ P' \supset P}} d(P') P' \in \mathbb{D}_{L'}$$

   heißt *Differente* von L'/L.

   Für $z \in L'$ *ist genau dann* $z \in \mathcal{C}_P$*, wenn* $v_{P'}(z) \geq -d(P')$ *für alle* $P' \in \mathbb{P}_{L'}$ *mit* $P' \supset P$.

Beweis. 1. Sei $z = c_1 u_1^* + \ldots + c_n u_n^* \in L'$ mit $c_1, \ldots, c_n \in L$. Wegen $\mathcal{O}'_P = \mathcal{O}_P u_1 + \ldots + \mathcal{O}_P u_n$ gilt:

$$\begin{aligned} z \in \mathcal{C}_P &\iff \mathsf{S}_{L'/L}(z\mathcal{O}'_P) \subset \mathcal{O}_P \\ &\iff \mathsf{S}_{L'/L}(zu_i) = \sum_{\nu=1}^{n} c_\nu \mathsf{S}_{L'/L}(u_\nu^* u_i) = c_i \in \mathcal{O}_P \text{ für alle } i \in [1, n]\,. \end{aligned}$$

Also ist genau dann $z \in \mathcal{C}_P$, wenn $z \in \mathcal{O}_P u_1^* + \ldots + \mathcal{O}_P u_n^*$, und es folgt $\mathcal{C}_P \supset \mathcal{O}'_P$ nach Satz 6.2.7. Ist $x \in \mathcal{O}'_P$ und $z \in \mathcal{C}_P$, so folgt $\mathsf{S}_{L'/L}(xz\mathcal{O}'_P) \subset \mathsf{S}_{L'/L}(z\mathcal{O}'_P) \subset \mathcal{O}_P$ und daher $xz \in \mathcal{C}_P$.

2. Nach Satz 6.2.7 gibt es ein $a \in \mathcal{O}_P^\bullet$, so dass $au_i^* \in \mathcal{O}'_P$ für alle $i \in [1, n]$ und daher $a\mathcal{C}_P \subset \mathcal{O}'_P$. Folglich ist $a\mathcal{C}_P$ ein Ideal von $\mathcal{O}'_P$, und nach den Sätzen 6.2.3 und 6.2.8 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 $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$. Ist $t' \in L$ mit $\mathcal{C}_P = t\mathcal{O}'_P = t'O'_P$, so folgt $t' = te$ mit $e \in \mathcal{O}'^\times_P \subset \mathcal{O}^\times_{P'}$ für alle $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$ und daher $v_{P'}(t) = v_{P'}(t')$.

Sei $z \in L'$ und $t \in L'$ mit $\mathcal{C}_P = t\mathcal{O}'_P$. Genau dann ist $z \in \mathcal{C}_P$, wenn $z \in t\mathcal{O}_{P'}$, also $v_{P'}(z) \geq v_{P'}(t) = -d(P')$ für alle $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$. □

Satz 6.3.2 (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* $P' \supset P$.
   (a) $e(P'/P) - 1 \leq d(P') \leq v_{P'}(f'(y))$.
   (b) *Genau dann ist* $d(P') = e(P'/P) - 1$*, wenn* $\mathrm{char}(K) \nmid e(P' \mid P)$.
2. *Sei* $[L' : L] = n$ *und* $d(P') = v_{P'}(f'(y))$ *für alle* $P' \in \mathbb{P}_{L'}$ *mit* $P' \supset P$*. Dann ist* $(1, y, \ldots, y^{n-1})$ *eine* P*-Ganzheitsbasis von* L'/L.

Beweis. 1. (a) Nach Satz 3.5.7 gibt es ein $t \in L'$, so dass $v_{P'}(t) = 1 - e(P'/P)$ für alle $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$. Es genügt, zu zeigen:

A. Für alle $z \in \mathcal{O}'_P$ ist $\mathsf{S}(tz) \in \mathcal{O}_P$.

Aus **A** folgt $t \in \mathcal{C}_P$, und dann ist $1 - e(P'/P) = v_{P'}(t) \geq -d(P')$, also $d(P') \leq e(P'/P) - 1$ für alle $P' \in \mathbb{P}_{L'}$ mit $P' \supset P$ nach Satz 6.3.1.2.

Beweis von **A.** Sei L^* eine galoissche Hülle von L'/L, und seien $\sigma_1, \dots, \sigma_n \in \mathsf{Gal}(L^*/L)$, so dass $\mathrm{Hom}_L(L', \overline{L'}) = \{\sigma_1 \,|\, L', \dots, \sigma_n \,|\, L'\}$, und sei $z \in \mathcal{O}'_P$. Dann ist

$$\mathsf{S}_{L'/L}(tz) = \sum_{i=1}^{n} \sigma_i(tz).$$

Sei $P^* \in \mathbb{P}_{L^*}$, $P^* \supset P$ und $i \in [1,n]$. Nach Satz 6.1.5 ist $P_i^* = \sigma_i^{-1}(P^*) \in \mathbb{P}_{L^*}$, $P_i^* \supset P$, $P'_i = P_i^* \cap L' \in \mathbb{P}_{L'}$, $P'_i \supset P$, $e(P_i^*/P) = e(P_i^*/P'_i)e(P'_i/P)$ und $v_{P^*} \circ \sigma_i = v_{P_i^*}$. Da $z \in L' \subset L^*$ über $\mathcal{O}_P$ ganz ist, folgt $z \in \mathcal{O}_{P_i^*}$, also $v_{P_i^*}(z) \geq 0$ und

$$\begin{aligned} v_{P^*}(\sigma_i(tz)) = v_{P_i^*}(tz) = v_{P_i^*}(t) + v_{P_i^*}(z) \geq v_{P_i^*}(t) = e(P_i^*/P'_i)v_{P'_i}(t) = e(P_i^*/P'_i)(1 - e(P'_i/P)) \\ > -e(P_i^*/P'_i)e(P'_i/P) = -e(P_i^*/P) = -e(P^*/P). \end{aligned}$$

Daher ist auch $-e(P^*/P) < v_{P^*}(\mathsf{S}_{L'/L}(tz)) = e(P^*/P)v_P(\mathsf{S}_{L'/L}(tz))$, also $v_P(\mathsf{S}_{L'/L}(tz)) \geq 0$ und $\mathsf{S}_{L'/L}(tz) \in \mathcal{O}_P$.

1. (b) Seien $P' = P_1, \dots P_r \in \mathbb{P}_{L'}$ (mit $r \in \mathbb{N}$) die verschiedenen Fortsetzungen von P auf L'.

Sei zuerst $\mathrm{char}(K) \nmid e(P'/P)$, aber $e(P'/P) \geq d(P')$. Sei $t \in L'$ mit $\mathcal{C}_P = t\mathcal{O}'_P$. Dann ist $v_{P'}(t) = -d(P') \leq -e(P'/P)$ und $\mathsf{S}_{L'/L}(t\mathcal{O}'_P) \subset \mathcal{O}_P$. Da K vollkommen ist, ist $L'_{P'}/L_P$ separabel, und daher gibt es ein $y_0 \in \mathcal{O}_{P'}$ mit $\mathsf{S}_{L'_{P'}/L_P}(y_0(P')) \neq 0$. Nach Satz 3.5.7 gibt es ein $y \in L'$, so dass $v_{P'}(y - y_0) \geq 1$ und $v_{P_i}(y) \geq \max\{1, e(P_i/P) + v_{P_i}(t)\}$ für alle $i \in [2,r]$. Dann ist $y \in \mathcal{O}'_P$, $y(P_i) = 0$ für alle $i \in [2,r]$, und mit Satz 6.2.9 folgt

$$\begin{aligned} \mathsf{S}_{L'/L}(y)(P) &= e(P'/P)\mathsf{S}_{L'_{P'}/L_P}(y(P')) + \sum_{i=2}^{r} e(P_i/P)\mathsf{S}_{L'_{P_i}/L_P}(y(P_i)) \\ &= e(P'/P)\mathsf{S}_{L'_{P'}/L_P}(y(P')) \neq 0, \quad \text{da } \mathrm{char}(K) \nmid e(P'/P). \end{aligned}$$

Sei $x \in L$ mit $v_P(x) = 1$. Dann ist

$$v_{P'}(x^{-1}yt^{-1} = -e(P'/P) + v_{P'}(y) - v_{P'}(t) \geq 0$$

und

$$v_{P_i}(x^{-1}yt^{-1} = -e(P_i/P) + v_{P_i}(y) - v_{P_i}(t) \geq 0 \text{ für alle } i \in [2,r],$$

also $x^{-1}yt^{-1} \in \mathcal{O}'_P$, $x^{-1}y \in t\mathcal{O}'_P = \mathcal{C}_P$ und daher $\mathsf{S}_{L'/L}(x^{-1}y) = x^{-1}\mathsf{S}_{L'/L}(y) \in \mathcal{O}_P$. Es folgt $\mathsf{S}_{L'/L}(y) \in x\mathcal{O}_P = P$, im Widerspruch zu $\mathsf{S}_{L'/L}(y)(P) \neq 0$. □

Satz 6.3.3 (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. □

Satz 6.3.4. *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 6.3.2 ist $(1, \alpha, \ldots, \alpha^{n-1})$ eine Ganzheitsbasis von L'/L für alle $P \in \mathbb{P}_L$, und $e(P'/P) = 1$ 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 $P_2, \ldots, P_r$ die übrigen Stellen von L' über P und $\mathcal{O}'_P = \mathrm{cl}_{L'}(\mathcal{O}_P) = \mathcal{O}_{P'} \cap \mathcal{O}_{P_2} \cap \ldots \cap \mathcal{O}_{P_r} = \mathcal{O}_P + \mathcal{O}_P\alpha + \ldots + \mathcal{O}_P\alpha^{n-1}$. Nach Satz 3.5.7 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 6.3.3. □

KAPITEL 7

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 $g_L = g$.

7.1

Lemma 7.1.1. *Seien $F \subset E_1$, $E_2 \subset E$ endliche Körper und $E = E_1E_2$. Dann ist*

$$[E:F] = \mathrm{kgV}([E_1:F],\, [E_2:F])\,.$$

Beweis. Sei $\overline{F}$ eine algebraische Hülle von F und $E \subset F$. Sei Ω die Menge aller Zwischenkörper $F \subset K \subset \overline{F}$. Dann ist die Abbildung $\Phi\colon (\Omega, \subset) \to (\mathbb{N}, |\,)$, 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 $\Phi(K_1) \,|\, \Phi(K_2)$, also auch $[K_1K_2 : F] = \mathrm{kgV}([K_1 : F], [K_2 : F])$ und $[K_1 \cap K_2 : F] = \mathrm{ggT}([K_1:F], [K_2:F])$. □

Satz und Definition 7.1.2. *Sei $\overline{L}$ eine algebraische Hülle von L. Für $r \in \mathbb{N}$ sei $\mathbb{F}_q \subset \mathbb{F}_{q^r} \subset \overline{L}$ 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 $d = \mathrm{ggT}(m, r)$. Dann ist $\mathsf{j}_{L_r/L}(P) = P_1 + \ldots + P_d$ mit verschiedenen $P_1, \ldots, P_d \in \mathbb{P}_{L_r}$, und für alle $i \in [1, d]$ ist $\deg(P_i) = \frac{m}{d}$.*

Beweis. Nach Satz 6.1.2 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 6.3.4 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 $P' \,|\, P$.

Sei nun $P \in \mathbb{P}_L$, und seien $P_1, \ldots, P_d$ 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 6.3.4, also

$$\deg(P_i) = [(L_r)_{P_i} : \mathbb{F}_{q^r}] = \frac{[(L_r)_{P_i} : \mathbb{F}_q]}{r} = \frac{\mathrm{kgV}\big([\mathbb{F}_{q^r}:\mathbb{F}_q],\, [L_P:\mathbb{F}_q]\big)}{r} = \frac{\mathrm{kgV}(m,r)}{r} = \frac{m}{\mathrm{ggT}(m,r)}\,.$$

Nach Satz 6.1.6 ist

$$\deg(P_i) = \frac{\deg(P)f(P_i/P)}{r} = \frac{mf(P_i/P)}{r}\,, \quad \text{also} \quad f(P_i/P) = \frac{r}{\mathrm{ggT}(m,r)}$$

und

$$r = [L_r:L] = \sum_{i=1}^{d} e(P_i/P)f(P_i/P) = d\,\frac{r}{\mathrm{ggT}(m,r)}\,, \quad \text{also} \quad d = \mathrm{ggT}(m,r)\,. \qquad \square$$

Definition 7.1.3. Für $n \in \mathbb{N}_0$ sei $\mathbb{D}_L^n = \{D \in \mathbb{D}_L \mid \deg(D) = n\}$, $\mathcal{C}_L^n = \{[D] \in \mathcal{C}_L \mid \deg(D) = n\}$ und $A_n = |\{D \in \mathbb{D}_L^n \mid D \geq 0\}|$. Insbesondere ist $A_0 = 1$ und $A_1 = |\mathbb{P}_L^1|$.
Sei $\deg(\mathbb{D}_L) = \deg(\mathcal{C}_L) = \partial\mathbb{Z}$ mit $\partial = \min\{\deg(D) \mid D \in \mathbb{D}_L\,,\ \deg(D) > 0\}$. Für alle $n \in \mathbb{N}$ mit $\partial \nmid n$ ist $A_n = 0$.
$h = h_L = |\mathcal{C}_L^0|$ heißt *Klassenzahl* von L.

Satz 7.1.4.

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 $P' \mid P$ folgt aus Satz 6.1.6

$$\deg(P') = \deg(P) f(P'/P) \leq \deg(P)\,[\,\mathbb{F}_q : K(x)]\,.$$

Für jedes $n \in \mathbb{N}$ gibt es nur endlich viele normierte irreduzible Polynome vom Grade n. Daher ist $\mathbb{P}^n_{\mathbb{F}_q(x)}$ endlich. Folglich sind auch alle Mengen $\mathbb{P}_L^d$ endlich. Ist $n \in \mathbb{N}$ und $D \in \mathbb{D}_L^n$ mit $D \geq 0$, so ist

$$D = \sum_{P \in \mathbb{P}_L} n_P P \quad \text{mit} \quad n_P \in \mathbb{N}_0 \quad \text{und} \quad \sum_{P \in \mathbb{P}_L} n_P = n\,.$$

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 $\tau\colon \mathcal{C}_L^0 \to \mathcal{C}_L^n$, 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 4.3.4 ist $\dim(C) \geq \deg(C) + 1 - g_L \geq 1$, und nach Satz 4.2.2 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 4.5.5 und $A \in (L^\times)$ nach Satz 4.3.1. □

7.2

Satz und Definition 7.2.1. *Für $\mathfrak{c} \in \mathcal{C}_L$ ist*

$$|\{A \in \mathfrak{c} \mid A \geq 0\}| = \frac{q^{\dim(\mathfrak{c})} - 1}{q - 1},$$

und für alle $n > 2g - 2$ mit $\partial \mid n$ ist

$$A_n = \frac{h(q^{n+1-g} - 1)}{q - 1}\,.$$

Die Potenzreihe

$$\mathcal{Z}_L(t) = \sum_{n \geq 0} A_n t^n \quad \textit{konvergiert absolut für } |t| < q^{-1}.$$

Die Funktion $\mathcal{Z}_L$ heißt *Zetafunktion* von $L/\mathbb{F}_q$.

BEWEIS. Sei $\mathfrak{c} \in \mathcal{C}$, $d = \dim(\mathfrak{c})$ 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 $|\mathcal{L}(C) \setminus \{0\}| = q^d - 1$, 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

$$|\{A \in \mathfrak{c} \mid A \geq 0\}| = \frac{q^d - 1}{q - 1}\,.$$

Sei nun $n = \deg(\mathfrak{c}) > 2g - 2$. Für $\mathfrak{c} \in \mathcal{C}_L^n$ ist (nach Satz 4.5.5)

$$|\{A \in \mathfrak{c} \mid A \geq 0\}| = \frac{q^{\dim(\mathfrak{c})} - 1}{q - 1} = \frac{q^{n+1-g} - 1}{q - 1}\,,$$

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 $|t| < q^{-1}$. □

Definition und Bemerkung 7.2.2. 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 $d = \mathrm{ggT}(r, m)$ so ist

$$\big(1 - t^{mr/d}\big)^d = \prod_{\zeta \in \mu_r} \big(1 - (\zeta t)^m\big) \quad \text{für alle} \quad t \in \mathbb{C}^\times\,.$$

[Beweis: Für $\zeta \in \mu_r$ ist

$$\mathrm{ord}(\zeta^m) = \frac{\mathrm{ord}(\zeta)}{\mathrm{ggT}(\mathrm{ord}(\zeta), m)}.$$

Daher ist die Abbildung

$$\theta\colon \begin{cases} \mu_r & \to & \mu_{r/d} \\ \zeta & \mapsto & \zeta^m \end{cases} \quad \text{surjektiv mit } \mathrm{Ker}(\theta) = \mu_d.$$

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 7.2.3. *Für $t \in \mathbb{C}$ mit $|t| < q^{-1}$ und $r \in \mathbb{N}$ ist*

$$\mathcal{Z}_L(t) = \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} \;\neq\; 0\,, \quad \textit{und} \quad \mathcal{Z}_{L_r}(t^r) = \prod_{\zeta \in \mu_r} \mathcal{Z}_L(\zeta t)\,.$$

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

$$\Big| \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} - \prod_{\substack{P \in \mathbb{P}_L \\ \deg(P) < X}} \frac{1}{1 - t^{\deg(P)}} \Big| < \frac{\varepsilon}{2} \quad \text{und} \quad \sum_{n=X}^{\infty} A_n |t|^n \;<\; \frac{\varepsilon}{2}\,.$$

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

$$\begin{aligned} &\Big| \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} - \mathcal{Z}_L(t) \Big| \\ &\quad \leq \Big| \prod_{P \in \mathbb{P}_L} \frac{1}{1 - t^{\deg(P)}} - \prod_{\substack{P \in \mathbb{P}_L \\ \deg(P) < X}} \frac{1}{1 - t^{\deg(P)}} \Big| + \Big| \sum_{D \in \mathbb{D}_L(X)} t^{\deg(D)} - \sum_{\substack{D \in \mathbb{D}_L \\ D \geq 0}} t^{\deg(D)} \Big| \\ &\quad \leq \frac{\varepsilon}{2} + \sum_{\substack{D \in \mathbb{D}_L,\ D \geq 0 \\ D \notin \mathbb{D}_L(X)}} |t|^{\deg(D)} \leq \frac{\varepsilon}{2} + \sum_{n=X}^{\infty} A_n |t|^n < \varepsilon \,. \end{aligned}$$

Sei nun $r \in \mathbb{N}$, $P \in \mathbb{P}_L$ mit $\deg(P) = m$ und $d = \mathrm{ggT}(m, r)$. Nach Satz 7.1.2 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 $t \in \mathbb{C}^\times$

$$\prod_{P' \mid P} \big(1 - t^{r \deg(P')}\big) = \big(1 - t^{rm/d}\big)^d = \prod_{\zeta \in \mu_r} \big(1 - (\zeta t)^m\big) \,,$$

und für $|t| < q^{-1}$ ist

$$\mathcal{Z}_{L_r}(t^r) = \prod_{P \in \mathbb{P}_L} \prod_{P' \mid P} \frac{1}{1 - t^{r \deg(P')}} = \prod_{P \in \mathbb{P}_L} \prod_{\zeta \in \mu_r} \frac{1}{1 - (\zeta t)^{\deg(P)}} = \prod_{\zeta \in \mu_r} \mathcal{Z}_L(\zeta t) \,. \qquad \square$$

7.3

Satz und Definition 7.3.1.

1. $\partial = 1$, *und*
$$\lim_{t \to 1} (1 - t) \mathcal{Z}_L(t) = \frac{h}{1 - q} \,.$$
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*
   $$F(t) = \frac{1}{q - 1} \sum_{n=0}^{2g-2} \Big(\sum_{\substack{\mathfrak{c} \in \mathcal{C}_L \\ \deg(\mathfrak{c}) = n}} q^{\dim(\mathfrak{c})} \Big) t^n \quad \text{und} \quad G(t) = \frac{h}{q - 1} \Big[\frac{q^g t^{2g-1}}{1 - qt} - \frac{1}{1 - t} \Big] \,.$$

3. $\mathcal{Z}_L(t)$ *ist eine in* $\mathbb{C} \setminus \{1, q^{-1}\}$ *definierte rationale Funktion,*

$$\mathcal{L}_L(t) = (1-t)(1-qt)\mathcal{Z}_L(t) \in \mathbb{Z}[t], \quad \textit{und} \quad \mathcal{L}_L(1) = h.$$

$\mathcal{L}_L = \mathcal{L}_{L/\mathbb{F}_q}$ 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 7.1.4 und mit Satz 7.2.1 folgt

$$\mathcal{Z}_L(t) = \sum_{\substack{n=0 \\ \partial \mid n}} \frac{q^{n+1}-1}{q-1}\, t^n = \frac{1}{q-1}\Big[q\sum_{n=0}^{\infty}(qt)^{\partial n} - \sum_{n=0}^{\infty} t^{\partial n}\Big] = \frac{1}{q-1}\Big[\,\frac{q}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\,\Big].$$

Sei nun $g \geq 1$. Nach Satz 7.2.1 folgt

$$\begin{aligned}
\mathcal{Z}_L(t) &= \sum_{\substack{n=0 \\ \partial \mid n}}^{2g-2} \sum_{\substack{\mathfrak{c} \in \mathcal{C}_L \\ \deg(\mathfrak{c})=n}} \frac{q^{\dim(\mathfrak{c})}-1}{q-1}\, t^n + \sum_{\substack{n=2g-1 \\ \partial \mid n}}^{\infty} \frac{h(q^{n+1-g}-1)}{q-1}\, t^n \\
&= \frac{1}{q-1}\sum_{n=0}^{2g-2}\Big(\sum_{\substack{\mathfrak{c} \in \mathcal{C}_L \\ \deg(\mathfrak{c})=n}} q^{\dim(\mathfrak{c})}\Big)t^n - \frac{h}{q-1}\sum_{\substack{n=0 \\ \partial \mid n}}^{2g-2} t^n + \frac{hq^{1-g}}{q-1}\sum_{\substack{n=2g-1 \\ \partial \mid n}}^{\infty} q^n t^n - \frac{h}{q-1}\sum_{\substack{n=2g-1 \\ \partial \mid n}}^{\infty} t^n \\
&= F(t) - \frac{h}{q-1}\sum_{n=0}^{\infty} t^{\partial n} + \frac{hq^{1-g+\partial k}t^{\partial k}}{q-1}\sum_{n=0}^{\infty} q^{n\partial}t^{n\partial} \qquad \Big(\text{mit} \quad k = \Big\lceil \frac{2g-1}{\partial} \Big\rceil\Big) \\
&= F(t) + \frac{h}{q-1}\Big[\,\frac{q^{1-g+\partial k}t^{\partial k}}{1-(qt)^{\partial}} - \frac{1}{1-t^{\partial}}\,\Big] = F(t) + G(t)\,.
\end{aligned}$$

In beiden Fällen ist

$$\lim_{t\to 1}(1-t)\mathcal{Z}_L(t) = \frac{h}{\partial(1-q)} \quad \text{und} \quad \mathcal{L}_L(1) = \lim_{t\to 1}(1-t)(1-qt)\mathcal{Z}_L(t) = \frac{h}{\partial}\,.$$

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 7.2.3 ist

$$\mathcal{Z}_{L_\partial}(t^\partial) = \prod_{\zeta \in \mu_\partial} \mathcal{Z}_L(\zeta t) = \mathcal{Z}_L(t)^\partial \quad \text{und} \quad 0 \neq \lim_{t\to 1}\frac{(1-t)^\partial \mathcal{Z}_L(t)^\partial}{(1-t^\partial)\mathcal{Z}_{L_\partial}(t^\partial)} = \lim_{t\to 1}\frac{(1-t)^\partial}{1-t^\partial}\,,$$

und daraus folgt $\partial = 1$. □

Satz 7.3.2.

1. *Es bestehen die Funktionalgleichungen*

$$\mathcal{Z}_L(t) = q^{g-1}t^{2g-2}\mathcal{Z}_L\Big(\frac{1}{qt}\Big) \quad \textit{für alle} \quad t \in \mathbb{C}^\times \setminus \{1, q^{-1}\}\,,$$

und

$$\mathcal{L}_L(t) = q^g t^{2g}\mathcal{L}_L\Big(\frac{1}{qt}\Big) \quad \textit{für alle} \quad t \in \mathbb{C}^\times\,.$$

2. $\mathrm{gr}(\mathcal{L}_L) = 2g$. *Ist* $\mathcal{L}_L(t) = a_0 + a_1 t + \ldots + a_{2g}t^{2g}$, *so folgt* $a_0 = 1$, $a_1 = |\mathbb{P}^1_L| - (q+1)$, $a_{2g} = q^g$, *und* $a_{2g-i} = q^{g-i}a_i$ *für alle* $i \in [0,g]$.
3. *Es gibt ganz-algebraische Zahlen* $\alpha_1, \ldots, \alpha_{2g}$, *so dass* $\alpha_i\alpha_{g+i} = q$ *für alle* $i \in [1,g]$, *und für alle* $r \in \mathbb{N}$ *ist*

$$\mathcal{L}_{L_r}(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t)\,, \quad q^r + 1 - |\mathbb{P}^1_{L_r}| = \sum_{i=1}^{2g}\alpha_i^r \quad \textit{und} \quad q^g = \prod_{i=1}^{2g}\alpha_i\,.$$

Satz von Hasse -Weil (ohne Beweis):

$$\textit{Für alle}\ \ i \in [1,2g] \ \ \textit{ist} \ \ |\alpha_i| = \sqrt{q}\,, \quad \textit{und} \quad \big|\, q^r + 1 - |\mathbb{P}^1_{L_r}|\,\big| \le 2gq^{r/2}\,.$$

Beweis. Im Falle $g = 0$ sind alle Behauptungen trivialerweise richtig. Sei also im Folgenden $g \ge 1$.

1. Sei $\mathfrak{w} \in \mathcal{C}_L$ die kanonische Klasse. Dann ist $\deg(\mathfrak{w}) = 2g-2$, und die Zuordnung $\mathfrak{c} \mapsto \mathfrak{w}-\mathfrak{c}$ definiert eine Bijektion der Menge $\{\mathfrak{c} \in \mathcal{C}_L \mid \deg(\mathfrak{c}) \in [0,2g-2]\}$ auf sich. Nach Satz 7.3.1 folgt

$$\begin{aligned}(q-1)F(t) &= \sum_{\substack{\mathfrak{c}\in\mathcal{C}_L\\ \deg(\mathfrak{c})\in[0,2g-2]}} q^{\dim(\mathfrak{c})}t^{\deg(\mathfrak{c})} = \sum_{\substack{\mathfrak{c}\in\mathcal{C}_L\\ \deg(\mathfrak{c})\in[0,2g-2]}} q^{\deg(\mathfrak{c})+1-g+\dim(\mathfrak{w}-\mathfrak{c})}t^{\deg(\mathfrak{c})}\\ &= q^{g-1}t^{2g-2}\sum_{\substack{\mathfrak{c}\in\mathcal{C}_L\\ \deg(\mathfrak{c})\in[0,2g-2]}} q^{\deg(\mathfrak{c})-(2g-2)+\dim(\mathfrak{w}-\mathfrak{c})}t^{\deg(\mathfrak{c})-(2g-2)}\\ &= q^{g-1}t^{2g-2}\sum_{\substack{\mathfrak{c}\in\mathcal{C}_L\\ \deg(\mathfrak{c})\in[0,2g-2]}} q^{\dim(\mathfrak{w}-\mathfrak{c})}\Big(\frac{1}{qt}\Big)^{\deg(\mathfrak{w}-\mathfrak{c})} = q^{g-1}t^{2g-2}(q-1)F\Big(\frac{1}{qt}\Big)\,.\end{aligned}$$

Ferner ist

$$\begin{aligned}(q-1)q^{g-1}t^{2g-2}G\Big(\frac{1}{qt}\Big) &= hq^{g-1}t^{2g-2}\Big[\frac{q^g\big(\frac{1}{qt}\big)^{2g-1}}{1-q\big(\frac{1}{qt}\big)} - \frac{1}{1-\frac{1}{qt}}\Big]\\ &= hq^{g-1}t^{2g-2}\Big[\frac{q^{-g+1}t^{-2g+1}t}{t-1} - \frac{qt}{qt-1}\Big]\\ &= h\Big[\frac{q^gt^{2g-1}}{1-qt} - \frac{1}{1-t}\Big] = (q-1)G(t)\,.\end{aligned}$$

Damit folgt

$$\mathcal{Z}_L(t) = F(t) + G(t) = q^{g-1}t^{2g-2}\Big[F\Big(\frac{1}{qt}\Big) + G\Big(\frac{1}{qt}\Big)\Big] = q^{g-1}t^{2g-2}\mathcal{Z}_L\Big(\frac{1}{qt}\Big)$$

und

$$\begin{aligned}q^gt^{2g}\mathcal{L}_L\Big(\frac{1}{qt}\Big) &= q^gt^{2g}\Big(1-\frac{1}{qt}\Big)\Big(1-\frac{1}{t}\Big)\mathcal{Z}_L\Big(\frac{1}{qt}\Big) = q^gt^{2g}\Big(1-\frac{1}{qt}\Big)\Big(1-\frac{1}{t}\Big)q^{1-g}t^{2-2g}\mathcal{Z}_L(t)\\ &= (1-qt)(1-t)\mathcal{Z}_L(t) = \mathcal{L}_L(t)\end{aligned}$$

2. Nach Definition ist $\mathrm{gr}(\mathcal{L}_L) \le 2g$, und aus

$$\mathcal{L}_L(t) = \sum_{i=0}^{2g}a_it^i = (1-t)(1-qt)\sum_{n=0}^{\infty}A_nt^n = A_0 + [\,A_1 - (q+1)A_0\,]t + \sum_{i=2}^{2g}a_it^i$$

und daher $a_0 = A_0 = 1$ und $a_1 = A_1 - (q+1)A_0 = |\mathbb{P}^1_L| - (q+1)$. Nach 1. ist

$$\mathcal{L}_L(t) = q^g t^{2g} \sum_{i=0}^{2g} a_i \Big(\frac{1}{qt}\Big)^i = \sum_{i=0}^{2g} a_i q^{g-i} t^{2g-i} = \sum_{i=0}^{2g} a_{2g-i} t^{2g-i}$$

und daher $a_{2g-i} = a_i q^{g-i}$ für alle $i \in [0,g]$. Insbesondere folgt $a_{2g} = q^g$ und daher $\operatorname{gr}(\mathcal{Z}_L) = 2g$.

3. Es ist

$$\mathcal{L}^*_L(t) = t^{2g}\mathcal{L}_L\Big(\frac{1}{t}\Big) = \sum_{i=0}^{2g} a_i t^{2g-i} = t^{2g} + a_1 t^{2g-1} + \ldots + q^g = \prod_{i=1}^{2g}(t-\alpha_i)$$

mit ganz-algebraischen Zahlen $\alpha_1, \ldots, \alpha_{2g} \in \mathbb{C}$, so dass

$$-a_1 = q + 1 - |\mathbb{P}^1_L| = \sum_{i=1}^{2g} \alpha_i \quad \text{und} \quad q^g = \prod_{i=1}^{2g} \alpha_i \,.$$

Mit Hilfe der Funktionalgleichung folgt

$$\mathcal{L}_L(t) = t^{2g}\mathcal{L}^*_L\Big(\frac{1}{t}\Big) = \prod_{i=1}^{2g}(1-\alpha_i t) = q^g \prod_{i=1}^{2g}\Big(t - \frac{1}{\alpha_i}\Big) = q^g t^{2g}\mathcal{L}_L\Big(\frac{1}{qt}\Big) = q^g \prod_{i=1}^{2g}\Big(t - \frac{\alpha_i}{q}\Big)\,,$$

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 Umnummerierung ist

$$\mathcal{L}_L(t) = \prod_{i=1}^{k}(1-\alpha_i t)\Big(1 - \frac{q}{\alpha_i}t\Big)(1-\sqrt{q}\,t)^l(1+\sqrt{q}\,t)^m$$

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

$$\begin{aligned}\mathcal{L}_{L_r}(t^r) &= (1-t^r)(1-q^r t^r)\mathcal{Z}_{L_r}(t^r) = \prod_{\zeta\in\mu_r}(1-\zeta t)(1-\zeta q t)\mathcal{Z}_L(\zeta t) = \prod_{\zeta\in\mu_r}\mathcal{L}_L(\zeta t)\\ &= \prod_{i=1}^{2g}\prod_{\zeta\in\mu_r}(1-\alpha_i\zeta t) = \prod_{i=1}^{2g}(1-\alpha_i^r t^r),\end{aligned}$$

also

$$\mathcal{L}_{L_r}(t) = \prod_{i=1}^{2g}(1-\alpha_i^r t) \quad \text{und daher} \quad |\mathbb{P}^1_{L_r}| = q^r + 1 - \sum_{i=1}^{2g}\alpha_i^r\,. \qquad \square$$