Diplomarbeit

Satz von Belyi

im Studiengang Mathematik
der Universität Bremen
vorgelegt im

Januar 2008

von

Ralf Donau

Gutachter:
Prof. Dr. Jens Gamst
Prof. Dr. Eberhard Oeljeklaus

Inhaltsverzeichnis

1 Einleitung

Eine projektive Kurve X über einem algebraisch abgeschlossenen Körper C ist über einem Unterkörper $K \subset C$ definiert, falls X eine affine Überdeckung hat, so daß jeder affine Teil isomorph zu einer Lösungsmenge von algebraischen Gleichungen über K ist. Der Satz von Belyi sagt aus, daß eine komplexe projektive glatte Kurve X genau dann über einem Zahlkörper definiert ist, falls ein nicht konstanter Morphismus $X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ existiert, der höchstens drei kritische Werte besitzt. In dieser Arbeit werde ich einen Beweis dieses Satzes durchführen, dabei richte ich mich nach dem Artikel "Belyi's Theorem Revisited" von B. Köck.

Der Beweis des Satzes von Belyi hat zwei Richtungen. Einerseits müssen wir zu einer Kurve, die bereits über einem Zahlkörper definiert ist, einen Morphismus nach $\mathbb{P}^1_{\mathbb{C}}$ angeben, der höchstens drei kritische Werte hat. Das wird in Kapitel 6 durchgeführt. Andererseits, wenn ein Morphismus $X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ gegeben ist, der höchstens drei kritische Werte besitzt, ist zu zeigen, daß X über einer endlichen Erweiterung von $\mathbb{Q}$ definiert ist, also über einem Zahlkörper. Diese Richtung wird häufig als "obvious part" bezeichnet, was zutreffen mag, wenn einem die Resultate von Weil bekannt sind. Den Beweis dieser Richtung zerlegt B. Köck in zwei Teile, dazu benutzt er den Modulkörper von t, der in Kapitel 8 definiert wird, als Zwischenschritt. Im ersten Schritt zeigt er, daß der Modulkörper von t eine endliche Erweiterung von $\mathbb{Q}$ ist. Im zweiten Schritt wird gezeigt, daß die Kurve über einer endlichen Erweiterung des Modulkörpers definiert ist. Zuvor hatte J. Wolfart in seinem Beweis den absoluten Modulkörper der Kurve X verwendet, allerdings ist der Beweis von B. Köck mit dem Modulkörper von t einfacher.

Im Folgenden gebe ich eine kurze Übersicht über den Beweis, der in dieser Arbeit behandelt wird. Die einzelnen Schritte werden in der Sprache der Schemata durchgeführt, dazu verwende ich folgende Formulierung des Satzes von Belyi:

Theorem 1.0.1 *Sei X eine vollständige Kurve über $\mathbb{C}$. X ist genau dann über einem Zahlkörper definiert, wenn ein endlicher Morphismus $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ existiert, der höchstens 3 kritische Werte besitzt.*

Die einzelnen Schritte des Beweises werden in den Kapiteln 6, 8 und 10 ausgeführt.

Zuerst nehmen wir an, daß ein Morphismus $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ mit höchstens drei kritischen Werten existiert. Nachdem wir t eventuell mit einer gebrochenlinearen Transformation komponiert haben, können wir annehmen, daß die kritischen Werte von t in $\{0, 1, \infty\}$ liegen. Der Modulkörper $M(X, t)$ von t ist nach Lemma 8.2.3 eine endliche Erweiterung von $\mathbb{Q}$. X und t sind nach Theorem 10.0.12 über einer endlichen Erweiterung von $M(X, t)$ definiert, damit ist X insgesamt über einer endlichen Erweiterung von $\mathbb{Q}$, also einem Zahlkörper definiert.

Falls X über einem Zahlkörper definiert ist, liefert uns das Belyi Verfahren aus Kapitel 6 den gewünschten Morphismus.

Konventionen:

- Alle betrachteten Körper haben Charakteristik 0
- Ringe sind kommutativ mit Einselement
- Alle Kurven sind glatt

2 Vorbereitungen I

Im folgenden ist C ein algebraisch abgeschlossener Körper und alle auftretenden Körper haben Charakteristik 0.

2.1 Varietäten

Definition 2.1.1 *Ein Schema X heißt integral, falls für jedes offene $U \subset X$ der Ring $\mathcal{O}_{X,U}$ ein Integritätsring ist.*

Definition 2.1.2 *Eine Varietät über einem Körper K (kurz K-Varietät) ist ein integrales Schema X mit einem Strukturmorphismus*

$$X \xrightarrow{\varphi} \operatorname{Spec} K$$

welcher separiert und von endlichem Typ ist.

"von endlichem Typ" bedeutet in diesem Fall, daß X eine offene Überdeckung durch $(\operatorname{Spec} A_i)_{i=1\dots n}$ hat wobei jedes A_i eine endlich erzeugte K-Algebra ist. Schreibweise: Wenn wir von der Varietät $X \xrightarrow{\varphi} \operatorname{Spec} K$ sprechen, bezeichnen wir diese kurz mit X.

Bemerkung 2.1.3 *Sei $\mathcal{O}_X$ die Strukturgarbe von X, dann gilt für jede offene affine Teilmenge $U \subset X$:*

1. *$\mathcal{O}_X(U)$ ist eine endlich erzeugte K-Algebra.*
2. *Für $V \subset U$ offen ist die Restriktion $\mathcal{O}_X(U) \longrightarrow \mathcal{O}_X(V)$ ein K-Algebrenhomomorphismus.*

Beispiele

1. Affine Varietäten: Sei A eine endlich erzeugte K-Algebra, die ein Integritätsring ist, d.h. $A = K[X_1 \cdots X_n]/I$, wobei I ein Primideal in $K[X_1 \cdots X_n]$ ist. Dann ist das affine Schema $\operatorname{Spec} A$ zusammen mit dem durch die Inklusion $K \hookrightarrow A$ induzierten Morphismus $\operatorname{Spec} A \longrightarrow \operatorname{Spec} K$ eine K-Varietät.
2. $\mathbb{P}^1_C$ als projektives Schema zu einem algebraisch abgeschlossenen Körper C.

Definition 2.1.4 *Seien X und Y Varietäten über einem Körper K mit den Strukturmorphismen φ und ψ. Ein Morphismus von Schemata $f : X \longrightarrow Y$ heißt **Morphismus von K-Varietäten**, falls folgendes Diagramm kommutiert:*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "\varphi"'] & & Y \arrow[dl, "\psi"] \\ & \operatorname{Spec} K & \end{tikzcd}$$

Definition 2.1.5 *Sei X ein integrales Schema, $\mathcal{O}_X$ die zugehörige Strukturgarbe. Eine rationale Funktion auf X wird durch ein Paar (U, f) repräsentiert, wobei $U \subset X$ offen und nicht leer ist und $f \in O_{X,U}$ gilt. Wir identifizieren zwei durch (U, f) und (V, g) repräsentierte rationale Funktionen miteinander, falls $f_{|U\cap V} = g_{|U\cap V}$ gilt. Die Menge der rationalen Funktionen auf X bezeichnen wir mit $K(X)$.*

Man sieht leicht, daß die auf den Paaren (U, f) definierte Relation eine Äquivalenzrelation ist.

Bemerkung 2.1.6 *$K(X)$ ist ein Körper.*

Wenn X eine K-Varietät ist, so ist $K(X)$ eine K-Algebra. Die Einbettung $K \hookrightarrow K(X)$ hängt vom Strukturmorphismus $\varphi : X \longrightarrow \operatorname{Spec} K$ ab. $K(X)$ selbst hängt lediglich vom zugrunde liegenden Schema X ab.

Definition 2.1.7 *Seien X und Y irreduzibe Schemata. Eine rationale Abbildung von X nach Y wird durch ein Paar (U, f) repräsentiert, wobei U ein offenes Unterschema von X ist und $U \xrightarrow{f} Y$ ein Morphimus von Schemata. Wir identifizieren zwei durch (U, f) und (V, g) repräsentierte rationale Abbildungen miteinander, falls $f_{|U\cap V} = g_{|U\cap V}$. D.h. das Diagramm*

$$\begin{tikzcd}
& U \cap V \arrow[dl, hook'] \arrow[dr, hook] & \\
U \arrow[dr, "f"] & & V \arrow[dl, "g"'] \\
& Y &
\end{tikzcd}$$

kommutiert.

Definition 2.1.8 *Seien X und Y K-Varietäten und $X \xrightarrow{f} Y$ eine rationale Abbildung. f heißt über K definiert, falls f durch einen Morphismus von K-Varietäten repräsentiert wird.*

Jede rationale Abbildung $X \longrightarrow Y$, die durch einen Morphismus repräsentiert wird, dessen stetiges Bild dicht ist, induziert einen Körperhomomorphismus $K(Y) \longrightarrow K(X)$ zwischen den Funktionenkörpern. Jeden Morphismus zwischen Schemata kann man als rationale Abbildung auffassen.

In Kapitel 8 wird der Modulkörper eines endlichen Morphismus $X \longrightarrow \mathbb{P}^1_C$ definiert, dazu benötigen wir die folgende Definition:

Definition 2.1.9 *Sei $\sigma \in \operatorname{Aut}(K)$ ein Körperautomorphimus, und sei X eine K-Varietät mit dem Strukturmorphismus $\varphi : X \longrightarrow \operatorname{Spec} K$. Dann erhalten wir durch Kompositum mit $\operatorname{Spec} \sigma : \operatorname{Spec} K \longrightarrow \operatorname{Spec} K$ eine neue K-Varietät mit dem Strukturmorphismus $X \xrightarrow{\varphi} \operatorname{Spec} K \xrightarrow{\operatorname{Spec} \sigma} \operatorname{Spec} K$. Diese bezeichnen wir mit X^σ.*

Die zugrundeliegenden Schemata von X und X^σ sind identisch. Die K-Varietäten X und X^σ unterscheiden sich lediglich in den Strukturmorphismen nach $\operatorname{Spec} K$.

Sei $t : X \longrightarrow Y$ ein Morphismus zwischen K-Varietäten, und sei $\sigma \in \operatorname{Aut}(K)$. Dann ist auch $t : X^\sigma \longrightarrow Y^\sigma$ ein Morphismus zwischen K-Varietäten, wie man leicht sieht. Wir bezeichnen diesen Morphismus dann mit t^σ.

Beispiel:
Sei X eine affine Varietät, d.h. $X = \operatorname{Spec} A$ mit $A = K[X_1 \cdots X_n]/I$. Dann ist die Varietät X^σ isomorph zur Varietät $\operatorname{Spec} B$ mit $B = K[X_1 \cdots X_n]/\sigma^{-1}(I)$.

Definition 2.1.10 *Sei L ein Körper, und sei X eine Varietät über L. Sei $K \subset L$ ein Unterkörper, dann heißt X über K definiert, falls eine K-Varietät X_K existiert, so daß*

$$X = X_K \times_{\operatorname{Spec} K} \operatorname{Spec} L$$

gilt.

Bemerkung 2.1.11 *X und X_K haben die gleiche Dimension.*

Definition 2.1.12 *Seien X und Y Varietäten über L, die bereits über K definiert sind. Sei $f : X \longrightarrow Y$ ein Morphismus von L-Varietäten. Dann heißt f über K definiert, falls ein Morphismus $f_K : X_K \longrightarrow Y_K$ von K-Varietäten existiert, so daß folgendes Diagramm kommutiert:*

$$\begin{tikzcd} X_K \arrow[d, "f_K"'] & X \arrow[l] \arrow[d, "f"] \\ Y_K & Y \arrow[l] \end{tikzcd}$$

Definition 2.1.13 *Eine **(glatte) Kurve** über C ist eine C-Varietät X, deren zugrundeliegendes Schema eindimensional ist, wobei für jeden abgeschlossenen Punkt $x \in X$ der lokale Ring $\mathcal{O}_{X,x}$ ein diskreter Bewertungsring ist.*

Wir betrachten ausschließlich glatte Kurven, daher wird der Zusatz "glatt" weggelassen.

Sei X eine Kurve über C und $K(X)$ deren Körper der rationalen Funktionen von X, dann gilt $deg_{tr}(K(X) : C) = 1$. Die Körpererweiterung $K(X) : C(T)$ ist endlich, aus dem Satz vom primitiven Element folgt dann, daß $K(X)$ über C von höchstens zwei Elementen erzeugt wird, d.h. $K(X) = C(a, b)$ mit $a, b \in K(X)$. Umgekehrt existiert zu jeder endlich erzeugten Körpererweiterung $\widetilde{C}$ vom Transzendenzgrad 1 über C eine vollständige Kurve Y, so daß $K(Y) = \widetilde{C}$ gilt.

Definition 2.1.14 *Sei X ein (glatte) Kurve, dann heißt X **vollständig**, falls zu jedem diskreten Bewertungsring R, der zwischen K und $K(X)$ liegt, ein $x \in X$ existiert, so daß $R \cong \mathcal{O}_{X,x}$ gilt.*

Satz 2.1.15 *Seien X und Y vollständige Kurven über K, und sei $S \subset X$ eine endliche Teilmenge von abgeschlossenen Punkten. Sei $\varphi : X \setminus S \longrightarrow Y$ ein Morphismus von K-Varietäten, dann existiert eindeutig eine Fortsetzung $\widetilde{\varphi} : X \longrightarrow Y$ von φ.*

Folgerung 2.1.16 *Jede rationale Abbildung zwischen zwei vollständigen Kurven X und Y, die über C definiert ist, wird von einem Morphismus $X \longrightarrow Y$ repräsentiert. Ein Körperhomomorphismus $K(Y) \longrightarrow K(X)$ induziert einen Morphismus $X \longrightarrow Y$.*

2.2 Endliche Morphismen

Definition 2.2.1 *Seien X und Y C-Varietäten, und sei $f : X \longrightarrow Y$ ein Morphismus. Dann ist f ein* **endlicher Morphismus***, falls für jede offene affine Teilmenge $V \cong \operatorname{Spec} A \subset Y$ das Urbild $U := f^{-1}(V)$ affin ist, also $U \cong \operatorname{Spec} B$ gilt, und B vermöge dem induzierten Morphismus $A \longrightarrow B$ eine modulendliche A-Algebra ist.*

Sei $f : X \longrightarrow Y$ ein endlicher Morphismus zwischen Kurven über C, dann ist das Bild jeder offenen Teilmenge dicht in Y. Damit induziert f einen Körperhomomorphismus $f^* : K(Y) \longrightarrow K(X)$, dieser ist injektiv. Insbesondere sind damit die induzierten Ringhomomorphismen zwischen den affinen Koordinatenringen und auch die lokalen Ringhomomorphismen injektiv.

Satz 2.2.2 *Seien X und Y Kurven, und sei X vollständig. Sei $f : X \longrightarrow Y$ ein nicht-konstanter Morphismus. Dann gilt*

1. *f ist ein endlicher Morphismus*
2. *$f(X) = Y$*
3. *Y ist vollständig.*

Beweis: Proposition 6.8 auf S.137 in [Ha]

Seien X und Y vollständige Kurven, und sei f ein endlicher Morphismus. Dann ist der Grad der Körpererweiterung $K(X) : K(Y)$ endlich. Wir definieren den **Grad** von f als den Grad der Körpererweiterung $K(X) : K(Y)$. Wir wissen, daß sich Grade von Körpererweiterungen multiplizieren, d.h. seien $L : M$ und $M : K$ endliche Körpererweiterungen, dann gilt $[L : K] = [K : M] \cdot [M : K]$. Per Definition multiplizieren sich die Grade von endlichen Morphismen ebenfalls.

Definition 2.2.3 *Seien X und Y Kurven über C, und sei $t : X \longrightarrow Y$ ein endlicher Morphismus.* $\operatorname{Aut}(t)$ *bezeichne die Gruppe derjenigen Isomorphismen $f : X \longrightarrow X$, für die $t \circ f = t$ gilt.*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "t"'] & & X \arrow[dl, "t"] \\ & Y & \end{tikzcd}$$

Lemma 2.2.4 *Seien X und Y Kurven über C, und sei $t : X \longrightarrow Y$ ein endlicher Morphismus. Sei $P \in X$, so daß t unverzweigt in P ist. Sei $f : X \longrightarrow X$ aus* $\operatorname{Aut}(t)$ *mit $f(P) = P$, dann ist f die Identität.*

$$\begin{tikzcd} X \arrow[rr, "f"] \arrow[dr, "t"'] & & X \arrow[dl, "t"] \\ & Y & \end{tikzcd}$$

Beweis:
t bzw. f induziert einen lokalen C-Algebrenhomomorphismus
$\varphi_t : \mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$ bzw. $\varphi_f : \mathcal{O}_{X,P} \longrightarrow \mathcal{O}_{X,P}$ im Punkt P. Sei $r \in \mathcal{O}_{Y,f(P)}$ ein lokaler Parameter, dann ist $s := \varphi_t(r)$ ebenfalls ein lokaler Parameter, da t unverzweigt in P ist.

$$\begin{tikzcd} \mathcal{O}_{X,P} & & \mathcal{O}_{X,P} \arrow[ll, "\varphi_f"'] \\ & \mathcal{O}_{Y,f(P)} \arrow[ul, "\varphi_t"] \arrow[ur, "\varphi_t"'] & \end{tikzcd}$$

Es gilt
$$\varphi_f(s) = \varphi_f(\varphi_t(r)) = \varphi_t(r) = s$$
Damit ist φ_f die Identität, da φ_f durch das Bild des lokalen Parameters s eindeutig bestimmt ist. f induziert einen Körperhomomorphismus
$f^* : K(X) \longrightarrow K(X)$ dieser ist die Identität, da $K(X)$ der Quotientenkörper von $\mathcal{O}_{X,P}$ ist. Damit ist auch f die Identität.

$\square$

Definition 2.2.5 *Seien $p_1 : Y_1 \longrightarrow X$ und $p_2 : Y_1 \longrightarrow X$ endliche Morphismen zwischen Kurven über $\mathbb{C}$. (Y_1, p_1) und (Y_2, p_2) heißen isomorph als endliche Morphismen nach X, falls ein Isomorphismus $f : Y_1 \longrightarrow Y_2$ existiert, so daß $p_2 \circ f = p_1$ gilt.*

$$\begin{tikzcd} Y_1 \arrow[rr, "f"] \arrow[dr, "p_1"'] & & Y_2 \arrow[dl, "p_2"] \\ & X & \end{tikzcd}$$

Bemerkung 2.2.6 *Die soeben definierte Relation zwischen endlichen Morphismen ist eine Äquivalenzrelation.*

Die Begründung ist die gleiche wie die von Bemerkung 7.1.7.

$\square$

3 Differentiale

In diesem Abschnitt werden die kritischen Punkte von Morphismen zwischen Kurven definiert. Das Ziel ist dann, die Menge der kritischen Punkte eines endlichen Morphismus zu kennzeichnen. Wir werden sehen, daß diese mit dem Träger einer Garbe übereinstimmt und sogar endlich ist.

Ich erinnere daran, daß bei uns alle Körper Charakteristik 0 haben. Im Folgenden ist C ein algebraisch abgeschlossener Körper und K ein nicht notwendig algebraisch abgeschlossener Körper.

3.1 Tangential- und Cotangentialraum

Definition 3.1.1 *Sei A ein Ring, B eine A-Algebra und M ein B-Modul. Eine Abbildung $d : B \longrightarrow M$ heißt A-**Derivation**, falls folgendes gilt:*

1. *d ist additiv*
2. *d genügt der Produktregel*
3. *$d(a) = 0$ für alle $a \in A$*

Die Menge aller A-Derivationen $d : B \longrightarrow M$ bezeichnen wir mit $\mathrm{Der}_A(B, M)$.

Definition 3.1.2 *Sei A ein Ring, B eine A-Algebra, dann ist der **Modul der relativen Differentialformen** von B über A ein B-Modul $\Omega_{B/A}$ mit einer A-Derivation $d_{B/A} : B \longrightarrow \Omega_{B/A}$, welche folgende universelle Eigenschaft hat:*
Zu jeder A-Derivation v in einen B-Modul M existiert eindeutig eine B-lineare Abbildung $w : \Omega_{B/A} \longrightarrow M$, so daß $w \circ d_{B/A} = v$ gilt.

$$\begin{tikzcd} B \arrow[r, "d_{B/A}"] \arrow[dr, "v"'] & \Omega_{B/A} \arrow[d, dotted, "w"] \\ & M \end{tikzcd}$$

Eine solche Derivation $d_{B/A}$ kann man zu jeder A-Algebra B konstruieren.

Sei A eine lokale K-Algebra mit maximalem Ideal $\mathfrak{m}$, und sei $v : A \longrightarrow M$ eine K-Derivation, dann gilt nach der Produktregel $v(\mathfrak{m}^2) \subset \mathfrak{m}M$, denn

$$a, b \in \mathfrak{m} \Longrightarrow v(ab) = av(b) + bv(a) \in \mathfrak{m}M$$

Wenn nun $M = A/\mathfrak{m}$ gilt, ist der Körper M vermöge der Quotientenabbildung ein A-Modul, und es gilt $\mathfrak{m}M = 0$. Das heißt, die im Folgenden häufig auftretenden Derivationen $v : A \longrightarrow A/\mathfrak{m}$ verschwinden auf $\mathfrak{m}^2$.

Lemma 3.1.3 *Sei A eine lokale K-Algebra mit maximalem Ideal $\mathfrak{m}$. Sei $K \cong A/\mathfrak{m}$ als K-Algebren, dann hat jedes $a \in A$ eine eindeutige Darstellung $a = a_1 + a_2$ mit $a_1 \in K$ und $a_2 \in \mathfrak{m}$.*

Beweis:
Setze $a_1 := (a \bmod \mathfrak{m})$ (man denke an den K-Algebrenisomorphismus) und $a_2 := a - a_1$. Dann gilt $a_1 \in K$, und es gilt $a_2 \in \mathfrak{m}$, denn

$$(a_2 \bmod \mathfrak{m}) = (a \bmod \mathfrak{m}) - (a_1 \bmod \mathfrak{m}) = (a \bmod \mathfrak{m}) - (a \bmod \mathfrak{m}) = 0$$

Aus $K \cap \mathfrak{m} = \{0\}$ folgt die Eindeutigkeit dieser Darstellung.

$\square$

Bemerkung 3.1.4 *Sei A ein kommutativer Ring, $S \subset A$ ein multiplikatives System, A_S die Lokalisierung nach S und $j : A \longrightarrow A_S$ die kanonische "Einbettung". Dann gibt $\mathfrak{p} \longmapsto j(\mathfrak{p})A_S$ eine Bijektion zwischen den Primidealen $\mathfrak{p} \subset A$ mit $\mathfrak{p} \cap S = \emptyset$ und den Primidealen von A_S. Sei $q : A \longrightarrow A/\mathfrak{p}$ die Quotientenabbildung, dann gilt $A_S/j(\mathfrak{p})A_S \cong (A/\mathfrak{p})[q(S)]$.*

Definition 3.1.5 *Sei X eine C-Varietät, $x \in X$ ein abgeschlossener Punkt und $\mathcal{O}_{X,x}$ der Halm in x. Sei $\mathfrak{m}_x \subset \mathcal{O}_{X,x}$ das maximale Ideal, dann heißt*

1. *$\mathrm{Der}_C(\mathcal{O}_{X,x}, C)$ der **Tangentialraum** von X im Punkt x.*
2. *$\mathfrak{m}_x/\mathfrak{m}_x^2$ der **Cotangentialraum** von X im Punkt x.*

Bemerkung 3.1.6 *Es gilt $C \cong \mathcal{O}_{X,x}/\mathfrak{m}_x$ und damit ist C über die Quotientenabbildung $q : \mathcal{O}_{X,x} \longrightarrow C$ ein $\mathcal{O}_{X,x}$-Modul.*

Beweis:
$\mathcal{O}_{X,x}$ ist die Lokalisierung einer endlich erzeugten C-Algebra, d.h. $\mathcal{O}_{X,x} \cong A_\mathfrak{m}$, wobei A eine endlich erzeugte C-Algebra sei und $\mathfrak{m} \subset A$ ein maximales Ideal. Aus dem Hilbertschen Nullstellensatz folgt $C \cong A/\mathfrak{m}$. Nach Bemerkung 3.1.4 gilt

$$A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} \cong A/\mathfrak{m}$$

Insgesamt erhalten wir

$$\mathcal{O}_{X,x}/\mathfrak{m}_x \cong A_\mathfrak{m}/\mathfrak{m}A_\mathfrak{m} \cong A/\mathfrak{m}$$

$\square$

Satz 3.1.7 *Der Tangential- und Cotangentialraum sind C-Vektorräume und es gilt*

$$\mathrm{Hom}_C(\mathfrak{m}_x/\mathfrak{m}_x^2, C) = \mathrm{Der}_C(\mathcal{O}_{X,x}, C)$$

Beweis:
Sei $v \in \mathrm{Der}_C(\mathcal{O}_{X,x}, C)$, dann gilt $v(\mathfrak{m}_x^2) = 0$. Wir erhalten eine Linearform $v' : \mathfrak{m}_x/\mathfrak{m}_x^2 \longrightarrow C$, indem wir v repräsentantenweise operieren lassen. Man sieht leicht, daß diese Zuordnung C-linear ist.

Diese Zuordnung ist auch injektiv, denn sei $v' = 0$, dann gilt $v_{|\mathfrak{m}_x} = 0$. Zu zeigen ist nun $v = 0$. Sei $a \in \mathcal{O}_{X,x}$, dann können wir a nach Lemma 3.1.3 als Summe aus $a_1 \in C$ und $a_2 \in \mathfrak{m}_x$ schreiben. Also gilt

$$v(a) = v(a_1) + v(a_2) = 0 + 0 = 0$$

Jetzt müssen wir noch sehen, daß diese Zuordnung surjektiv ist. Sei $w : \mathfrak{m}_x/\mathfrak{m}_x^2 \longrightarrow C$ eine Linearform. Wir definieren eine Abbildung $v : \mathcal{O}_{X,x} \longrightarrow C$ wie folgt: Für $a = a_1 + a_2$ mit $a_1 \in C$ und $a_2 \in \mathfrak{m}_x$ setze $v(a) := w(\overline{a_2})$. Dann gilt trivialerweise $v(c) = 0$ für $c \in C$. Seien nun $a = a_1 + a_2$ und $b = b_1 + b_2$ aus $\mathcal{O}_{X,x}$. Dann gilt

$$\begin{aligned} v(ab) &= v((a_1 + a_2)(b_1 + b_2)) \\ &= v(a_1 b_2) + v(a_2 b_1) \\ &= a_1 v(b_2) + b_1 v(a_2) \\ &= av(b) + bv(a) \end{aligned}$$

Also ist v eine C-Derivation auf $\mathcal{O}_{X,x}$. Es gilt $v' = w$, damit ist die Surjektivität gezeigt.

$\square$

Folgerung 3.1.8 *Sei X eine Kurve (Erinnerung: wir betrachten ausschließlich glatte Kurven), $x \in X$ ein abgeschlossener Punkt, dann sind der Tangentialraum und der Cotangentialraum eindimensionale C-Vektorräume.*

Beweis:
$\mathcal{O}_{X,x}$ ist ein diskreter Bewertungsring, also ist $\mathfrak{m}/\mathfrak{m}^2$ ein eindimensionaler C-Vektorraum. Nach Satz 3.1.7 ist der Tangentialraum der Dualraum vom Cotangentialraum, also ist auch der Tangentialraum eindimensional.

$\square$

Sei $\varphi : A \longrightarrow B$ ein K-Algebrenhomomorphismus, und sei $v : B \longrightarrow M$ eine K-Derivation in einen B-Modul M. Vermöge φ ist M dann ein A-Modul, und $v \circ \varphi : A \longrightarrow M$ ist eine K-Derivation auf A, denn seien $a, b \in A$, dann gilt

$$v(\varphi(ab)) = v(\varphi(a)\varphi(b)) = \varphi(b)v(\varphi(a)) + \varphi(a)v(\varphi(b)) = bv(\varphi(a)) + av(\varphi(b))$$

und wegen der K-Linearität von φ gilt $v \circ \varphi(k) = 0$ für $k \in K$. Additivität gilt trivialerweise und damit ist gezeigt, daß $v \circ \varphi$ eine K-Derivation ist.

Seien A und B nun zusätzlich lokale K-Algebren, φ ein lokaler K-Algebrenhomomorphismus und seien $\mathfrak{m}_A$ und $\mathfrak{m}_B$ die entsprechenden maximalen Ideale. Es gelte $A/\mathfrak{m}_A \cong K \cong B/\mathfrak{m}_B$. K ist über die Quotientenabbildung $q_B : B \longrightarrow B/\mathfrak{m}_B$ ein B-Modul und ist vermöge φ ein A-Modul. Andererseits ist auf K eine A-Modulstruktur über die Quotientenabbildung $q_A : A \longrightarrow A/\mathfrak{m}_A$ erklärt. In beiden Fällen erhalten wir dieselbe A-Modulstruktur. Um das einzusehen, ist $q_A = q_B \circ \varphi$ zu zeigen (Gleichheit bezieht sich auf die kanonische Identifikation über die K-Algebrenisomorphismen). Sei $a \in A$, dann können wir a nach Lemma 3.1.3 als Summe aus $a_1 \in K$ und $a_2 \in \mathfrak{m}_A$ schreiben. Es gilt $\varphi(\mathfrak{m}_A) \subset \mathfrak{m}_B$, also $q_B \circ \varphi(a_2) = 0 = q_A(a_2)$. φ ist ein K-Algebrenhomomorphismus, also gilt auch $q_B \circ \varphi(a_1) = q_A(a_1)$. Daraus folgern wir, daß für $v \in \mathrm{Der}(B, K)$ die zurückgezogene Derivation $v \circ \varphi$ in $\mathrm{Der}(A, K)$ liegt. Wir können nun eine Abbildung

$$\begin{aligned} \mathrm{Der}(B, K) &\longrightarrow \mathrm{Der}(A, K) \\ v &\longmapsto v \circ \varphi \end{aligned}$$

definieren, diese Abbildung nennen wir **Tangentialabbildung**.

Seien X und Y C-Varietäten und sei $f : X \longrightarrow Y$ ein Morphismus von C-Varietäten. Sei $x \in X$ ein abgeschlossener Punkt, dann induziert f über die Strukturgarben einen lokalen C-Algebrenhomomorphismus

$$\varphi : \mathcal{O}_{Y,f(x)} \longrightarrow \mathcal{O}_{X,x}$$

Sei $\mathfrak{m}_x$ das maximale Ideal von $\mathcal{O}_{X,x}$ und $\mathfrak{m}_{f(x)}$ das maximale Ideal von $\mathcal{O}_{Y,f(x)}$. Es gilt $\varphi(\mathfrak{m}_{f(x)}) \subset \mathfrak{m}_x$, daraus folgt $\varphi(\mathfrak{m}^2_{f(x)}) \subset \mathfrak{m}^2_x$, also wird in natürlicher Weise eine C-lineare Abbildung

$$\widetilde{\varphi} : \mathfrak{m}_{f(x)}/\mathfrak{m}^2_{f(x)} \longrightarrow \mathfrak{m}_x/\mathfrak{m}^2_x$$

durch φ induziert. $\widetilde{\varphi}$ heißt dann die **Cotangentialabbildung** von f in x.

Bemerkung 3.1.9 *Die C-lineare Abbildung zwischen den Tangentialräumen*

$$\begin{array}{rcl} \mathrm{Der}_C(\mathcal{O}_{X,x}, C) & \longrightarrow & \mathrm{Der}_C(\mathcal{O}_{Y,f(x)}, C) \\ v & \longmapsto & v \circ \varphi \end{array}$$

ist die duale Abbildung zu $\widetilde{\varphi}$.

Diese Abbildung heißt **Tangentialabbildung** von f in x.
Beweis:
Sei $v \in \mathrm{Der}_C(\mathcal{O}_{X,x}, C)$, dann erhalten wir eine Linearform $v' : \mathfrak{m}_x/\mathfrak{m}^2_x \longrightarrow C$ (siehe Beweis von Satz 3.1.7). Zu zeigen: $v' \circ \widetilde{\varphi} = (v \circ \varphi)'$. Sei $\overline{\mu} \in \mathfrak{m}_{f(x)}/\mathfrak{m}^2_{f(x)}$ mit $\mu \in \mathfrak{m}_{f(x)}$, dann gilt $v \circ \varphi(\mu) = v' \circ \widetilde{\varphi}(\overline{\mu})$.

□

Der Cotangentialraum läßt sich auch anders beschreiben und zwar mit dem Modul der relativen Differentialformen. Dazu definieren wir die $\mathcal{O}_{X,x}$-lineare Abbildung

$$\begin{array}{rcl} \delta : \mathfrak{m}_x & \longrightarrow & \Omega_{\mathcal{O}_{X,x}/C} \\ m & \longmapsto & d_{\mathcal{O}_{X,x}/C}(m) \end{array}$$

wobei $\Omega_{\mathcal{O}_{X,x}/C}$ den Modul der relativen Differentialformen von $\mathcal{O}_{X,x}$ über C bezeichne und $d_{\mathcal{O}_{X,x}/C}$ die zugehörige Derivation. Es gilt $\delta(\mathfrak{m}^2_x) \subset \mathfrak{m}_x\Omega_{\mathcal{O}_{X,x}/C}$, also können wir eine Abbildung $\widetilde{\delta}$ definieren:

Satz 3.1.10 *Die C-lineare Abbildung*

$$\begin{array}{rcl} \widetilde{\delta} : \mathfrak{m}_x/\mathfrak{m}^2_x & \longrightarrow & \Omega_{\mathcal{O}_{X,x}/C}/\mathfrak{m}_x\Omega_{\mathcal{O}_{X,x}/C} \\ \overline{m} & \longmapsto & \overline{d_{\mathcal{O}_{X,x}/C}(m)} \end{array}$$

ist ein Isomorphismus.

Beweis:
Wir definieren eine C-Derivation $v : \mathcal{O}_{X,x} \longrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2$. Sei $a \in \mathcal{O}_{X,x}$, dann können wir a nach Lemma 3.1.3 als Summe aus $a_1 \in C$ und $a_2 \in \mathfrak{m}_x$ schreiben. Setze $v(a) := a_2 \bmod \mathfrak{m}_x^2$, dann ist v eine C-Derivation, denn per Definition gilt Additivität und $v(c) = 0$ für $c \in C$. Die Rechnung zum Nachweis der Produktregel ist analog zu der aus dem Beweis von Satz 3.1.7. Zu v existiert nun eindeutig ein $w : \Omega_{\mathcal{O}_{X,x/C}} \longrightarrow \mathfrak{m}_x/\mathfrak{m}_x^2$, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd}
\mathcal{O}_{X,x} \arrow[r, "d_{\mathcal{O}_{X,x/C}}"] \arrow[dr, "v"'] & \Omega_{\mathcal{O}_{X,x/C}} \arrow[d, dotted, "w"] \\
& \mathfrak{m}_x/\mathfrak{m}_x^2
\end{tikzcd}$$

$\Omega_{\mathcal{O}_{X,x/C}}$ wird von $\{d_{\mathcal{O}_{X,x/C}}(a) \mid a \in \mathfrak{m}_x\}$ erzeugt und es gilt $w(d_{\mathcal{O}_{X,x/C}}(a)) = v(a) = a \bmod \mathfrak{m}^2$. Wir schränken nun von $\mathcal{O}_{X,x}$ auf $\mathfrak{m}_x$ ein und betrachten dann erneut alles modulo $\mathfrak{m}_x^2$, damit erhalten wir folgende kommutative Diagramme:

$$\begin{tikzcd}
\mathfrak{m}_x \arrow[r, "\delta"] \arrow[dr, "v"'] & \Omega_{\mathcal{O}_{X,x/C}} \arrow[d, "w"] \\
& \mathfrak{m}_x/\mathfrak{m}_x^2
\end{tikzcd}
\qquad
\begin{tikzcd}
\mathfrak{m}_x/\mathfrak{m}_x^2 \arrow[r, "\widetilde{\delta}"] \arrow[dr, "\mathrm{id}"'] & \Omega_{\mathcal{O}_{X,x/C}}/\mathfrak{m}_x\Omega_{\mathcal{O}_{X,x/C}} \arrow[d, "\widetilde{w}"] \\
& \mathfrak{m}_x/\mathfrak{m}_x^2
\end{tikzcd}$$

Die Wohldefiniertheit von $\widetilde{w}$ folgt aus der $\mathcal{O}_{X,x}$-Linearität von w und daraus, daß $\mathfrak{m}_x \cdot \mathfrak{m}_x/\mathfrak{m}_x^2 = 0$ gilt. Nach dem obigen Diagramm ist $\widetilde{w}$ ein Linksinverses von $\widetilde{\delta}$. Man sieht leicht, daß $\widetilde{\delta} \circ \widetilde{w}$ auf den Erzeugenden die Identität ist, damit ist $\widetilde{w}$ ebenfalls ein Rechtsinverses.

□

Vermöge φ ist $\Omega_{\mathcal{O}_{X,x/C}}$ ein $\mathcal{O}_{Y,f(x)}$-Modul und $v := d_{\mathcal{O}_{X,x/C}} \circ \varphi$ ist eine C-Derivation auf $\mathcal{O}_{Y,f(x)}$. Es existiert eindeutig ein $\psi : \Omega_{\mathcal{O}_{Y,f(x)/C}} \longrightarrow \Omega_{\mathcal{O}_{X,x/C}}$, so daß folgendes Diagramm kommutiert.

$$\begin{tikzcd}
\mathcal{O}_{Y,f(x)} \arrow[r, "d_{\mathcal{O}_{Y,f(x)/C}}"] \arrow[dr, "v"'] & \Omega_{\mathcal{O}_{Y,f(x)/C}} \arrow[d, dotted, "\psi"] \\
& \Omega_{\mathcal{O}_{X,x/C}}
\end{tikzcd}$$

Auf den Erzeugenden $\{d_{\mathcal{O}_{Y,f(x)/C}}(a) \mid a \in \mathcal{O}_{Y,f(x)}\}$ von $\Omega_{\mathcal{O}_{Y,f(x)/C}}$ gilt nun

$$d_{\mathcal{O}_{Y,f(x)/C}}(a) \stackrel{\psi}{\longmapsto} d_{\mathcal{O}_{X,x/C}}(\varphi(a))$$

Es gilt $\psi(\mathfrak{m}_{f(x)}\Omega_{\mathcal{O}_{Y,f(x)}/C}) \subset \mathfrak{m}_x\Omega_{\mathcal{O}_{X,x}/C}$, denn sei $mv \in \mathfrak{m}_{f(x)}\Omega_{\mathcal{O}_{Y,f(x)}/C}$ mit $m \in \mathfrak{m}_{f(x)}$ und $v \in \Omega_{\mathcal{O}_{Y,f(x)}/C}$, dann gilt $\psi(mv) = \varphi(m)\psi(v) \in \mathfrak{m}_x\Omega_{\mathcal{O}_{X,x}/C}$, da φ ein lokaler Ringhomomorphismus ist. Wir können nun eine Abbildung

$$\widetilde{\psi} : \Omega_{\mathcal{O}_{Y,f(x)}/C}/\mathfrak{m}_{f(x)}\Omega_{\mathcal{O}_{Y,f(x)}/C} \longrightarrow \Omega_{\mathcal{O}_{X,x}/C}/\mathfrak{m}_x\Omega_{\mathcal{O}_{X,x}/C}$$

in naheliegender Weise definieren. Mit dem so definierten $\widetilde{\psi}$ kommutiert das folgende Diagramm.

$$\begin{tikzcd}
\mathfrak{m}_{f(x)}/\mathfrak{m}_{f(x)}^2 \arrow[r, "\widetilde{\varphi}"] \arrow[d, "\widetilde{\delta}"'] & \mathfrak{m}_x/\mathfrak{m}_x^2 \arrow[d, "\widetilde{\delta}"] \\
\Omega_{\mathcal{O}_{Y,f(x)}/C}/\mathfrak{m}_{f(x)}\Omega_{\mathcal{O}_{Y,f(x)}/C} \arrow[r, "\widetilde{\psi}"] & \Omega_{\mathcal{O}_{X,x}/C}/\mathfrak{m}_x\Omega_{\mathcal{O}_{X,x}/C}
\end{tikzcd}$$

Daher wissen wir nun, daß $\widetilde{\varphi}$ den gleichen Rang wie $\widetilde{\psi}$ hat. Seien X und Y Kurven, dann ist $\widetilde{\varphi}$ genau dann die Nullabbildung, wenn $\widetilde{\psi}$ die Nullabbildung ist. Das ist wiederum äquivalent dazu, daß die Tangentialabbildung im Punkt x die Nullabbildung ist.

3.2 Kritische Punkte

Definition 3.2.1 *Sei $f : X \longrightarrow Y$ ein Morphismus zwischen Kurven über C, und sei $x \in X$ ein abgeschlossener Punkt. Dann heißt x* ***kritischer Punkt*** *von f und $f(x)$ kritischer Wert von f, falls eine der folgenden äquivalenten Bedingungen erfüllt ist:*

1. *die Tangentialabbildung $\mathrm{Der}_C(\mathcal{O}_{X,x}, C) \longrightarrow \mathrm{Der}_C(\mathcal{O}_{Y,f(x)}, C)$ aus Satz 3.1.9 ist die Nullabbildung*
2. *Cotangentialabbildung $\widetilde{\varphi}$ ist die Nullabbildung*
3. *Cotangentialabbildung auf Differentialformen $\widetilde{\psi}$ ist die Nullabbildung*

Wir bezeichen die Menge aller kritischen Punkte von f mit $\mathrm{Crit}(f)$.

Bemerkung 3.2.2 *Ein Isomorphismus zwischen Kurven über C hat keine kritischen Punkte.*

Beweis:
Ein Isomorphismus zwischen lokal geringten Räumen induziert in jedem Punkt einen Isomorphismus zwischen den lokalen Ringen.

$\square$

Für den Beweis von Satz 3.2.5 benötigen wir eine bekannte Tatsache:

Satz 3.2.3 *Sei R ein Ring, und seien U, V, W R-Moduln. Dann ist die Sequenz von R-Moduln*

$$U \longrightarrow V \longrightarrow W \longrightarrow 0$$

genau dann exakt, falls für alle R-Moduln M die induzierte Sequenz

$$0 \longrightarrow \mathrm{Hom}_R(W, M) \longrightarrow \mathrm{Hom}_R(V, M) \longrightarrow \mathrm{Hom}_R(U, M)$$

exakt ist.

Beweis: Theorem 1 auf S.227 in [Bb]

Lemma 3.2.4 *Sei A ein lokaler Ring mit maximalem Ideal $\mathfrak{m}$, und sei M ein A-Modul, der von einem Element erzeugt wird. Ist $x \in M \setminus \mathfrak{m}M$, dann erzeugt x den Modul M.*

Beweis:
Sei $y \in M$ ein Erzeugendes von M, dann existiert $a \in A$ mit $x = ay$. Aus $x \notin \mathfrak{m}M$ folgt $a \notin \mathfrak{m}$, also ist a invertierbar. Nun gilt $y = a^{-1}x$ und damit ist x ein Erzeugendes von M.

□

Satz 3.2.5 *Seien $A \xrightarrow{f} B \xrightarrow{g} C$ Ringhomomorphismen, dann gibt es in natürlicher Weise eine exakte Sequenz von C-Moduln.*

$$\Omega_{B/A} \otimes_B C \xrightarrow{v} \Omega_{C/A} \xrightarrow{u} \Omega_{C/B} \longrightarrow 0$$

mit $v(d_{B/A}(b) \otimes 1) = d_{C/A}(b)$ und $u(d_{C/A}(c)) = d_{C/B}(c)$.

Beweis:
Gemäß Satz 3.2.3 zeigen wir, daß die exakte Sequenz von C-Moduln

$$0 \longrightarrow \mathrm{Hom}_C(\Omega_{C/B}, M) \xrightarrow{u^*} \mathrm{Hom}_C(\Omega_{C/A}, M) \xrightarrow{v^*} \mathrm{Hom}_C(\Omega_{B/A} \otimes_B C, M)$$

für alle C-Moduln M exakt ist.

Die B-Derivation $d_{C/B} : C \longrightarrow \Omega_{C/B}$ ist auch eine A-Derivation, also existiert eindeutig ein C-lineares $u : \Omega_{C/A} \longrightarrow \Omega_{C/B}$, so daß $u \circ d_{C/A} = d_{C/B}$ gilt, d.h. $u(d_{C/A}(c)) = d_{C/B}(c)$ für alle $c \in C$.

$$\begin{tikzcd} C \arrow[r, "d_{C/A}"] \arrow[d, "d_{C/B}"'] & \Omega_{C/A} \arrow[dl, dotted, "u"] \\ \Omega_{C/B} & \end{tikzcd}$$

Sei nun M ein C-Modul. Sei $x \in \mathrm{Hom}(\Omega_{C/B}, M)$, dann erhalten wir eine B-Derivation $x \circ d_{C/B} \in \mathrm{Der}_B(C, M)$. Aus der Definition des Moduls der relativen Differentialformen folgt, daß diese Zuordnung ein Isomorphismus ist, also gilt

$$\mathrm{Der}_B(C, M) \cong \mathrm{Hom}(\Omega_{C/B}, M)$$

Analog gilt

$$\mathrm{Der}_A(C, M) \cong \mathrm{Hom}(\Omega_{C/A}, M)$$

Sei $x \in \mathrm{Hom}(\Omega_{C/B}, M)$, dann gilt $x \circ d_{C/B} = x \circ (u \circ d_{C/A}) = u^*(x) \circ d_{C/A}$. Die durch x gegebene B-Derivation stimmt mit der durch $u^*(x)$ gegebenen A-Derivation überein, also entspricht u^* der Inklusionsabbildung
$\mathrm{Der}_B(C, M) \hookrightarrow \mathrm{Der}_A(C, M)$.

Die A-Derivation $d_{C/A} : C \longrightarrow \Omega_{C/A}$ gibt uns eine A-Derivation
$B \xrightarrow{g} C \xrightarrow{d_{C/A}} \Omega_{C/A}$. Es existiert eindeutig ein B-lineares $\widetilde{v}$, so daß
$\widetilde{v} \circ d_{B/A} = d_{C/A} \circ g$ gilt, d.h. $\widetilde{v}(d_{B/A}(b)) = d_{C/A}(b)$ für alle $b \in B$.

$$\begin{tikzcd} B \arrow[r, "d_{B/A}"] \arrow[d, "g"'] & \Omega_{B/A} \arrow[d, dotted, "\widetilde{v}"] \\ C \arrow[r, "d_{C/A}"] & \Omega_{C/A} \end{tikzcd}$$

Nun machen wir den B-Modul $\Omega_{B/A}$ über das Tensorprodukt zu einem C-Modul. Sei $i : \Omega_{B/A} \longrightarrow \Omega_{B/A} \otimes_B C$ die kanonische "Inklusion", dann existiert eindeutig ein C-lineares $v : \Omega_{B/A} \otimes_B C \longrightarrow \Omega_{C/A}$, so daß $v \circ i = \widetilde{v}$ gilt.

$$\begin{tikzcd} \Omega_{B/A} \arrow[r, "i"] \arrow[d, "\widetilde{v}"] & \Omega_{B/A} \otimes_B C \arrow[dl, dotted, "v"] \\ \Omega_{C/A} & \end{tikzcd}$$

Für v gilt dann $v(d_{B/A}(b) \otimes 1) = d_{C/A}(b)$ für alle $b \in B$.

Sei $x \in \mathrm{Hom}_C(\Omega_{B/A} \otimes_B C, M)$, dann gilt $x \circ i \in \mathrm{Hom}_B(\Omega_{B/A}, M)$. Diese Zuordnung ist ein Isomorphismus. Wir ordnen nun $x \in \mathrm{Hom}_C(\Omega_{B/A} \otimes_B C, M)$ eine A-Derivation auf B wie folgt zu: $x \circ i \circ d_{B/A}$.

Sei $x \in \mathrm{Hom}_C(\Omega_{C/A}, M)$, dann erhalten wir eine A-Derivation
$x \circ d_{C/A} \in \mathrm{Der}_A(C, M)$. Wir schränken diese Derivation auf B ein, dann gilt $x \circ (d_{C/A} \circ g) = x \circ (\widetilde{v} \circ d_{B/A}) = x \circ (v \circ i \circ d_{B/A}) = v^*(x) \circ i \circ d_{B/A}$. Wir sehen nun, daß v^* der Einschränkung $\mathrm{Der}_A(C, M) \longrightarrow \mathrm{Der}_A(B, M)$ entspricht.

Man sieht sehr leicht, daß

$$0 \longrightarrow \mathrm{Der}_B(C, M) \longrightarrow \mathrm{Der}_A(C, M) \longrightarrow \mathrm{Der}_A(B, M)$$

exakt ist.

$\square$

Satz 3.2.6 *Sei $f : X \longrightarrow Y$ ein Morphismus zwischen Kurven, und sei $x \in X$ ein abgeschlossener Punkt. x ist genau dann ein kritischer Punkt von f, wenn $\Omega_{\mathcal{O}_{X,x}/\mathcal{O}_{Y,f(x)}} \neq 0$ gilt.*

Beweis:
Wie haben die Ringhomomorphismen $C \longrightarrow \mathcal{O}_{Y,f(x)} \xrightarrow{\varphi} \mathcal{O}_{X,x}$. Nach Satz 3.2.5 erhalten wir folgende exakte Sequenz von $\mathcal{O}_{X,x}$-Moduln:

$$\Omega_{\mathcal{O}_{Y,f(x)}/C} \otimes_{\mathcal{O}_{Y,f(x)}} \mathcal{O}_{X,x} \xrightarrow{v} \Omega_{\mathcal{O}_{X,x}/C} \xrightarrow{u} \Omega_{\mathcal{O}_{X,x}/\mathcal{O}_{Y,f(x)}} \longrightarrow 0$$

wobei $v(d_{\mathcal{O}_{X,x}/C}(f) \otimes a) = d_{\mathcal{O}_{Y,f(x)}/C} \circ \varphi(f) \cdot a$ gilt.

x ist kein kritischer Punkt von f ist äquivalent dazu, daß $\widetilde{\psi}$ (siehe Definition 3.2.1) nicht die Nullabbildung ist. Das wiederum ist äquivalent dazu, daß ein m aus $\Omega_{\mathcal{O}_{X,x}/C} \setminus \mathfrak{m}_x \Omega_{\mathcal{O}_{X,x}/C}$ unter $\widetilde{\psi}$ getroffen wird. Nach Lemma 3.2.4 ist m ein Erzeugendes von $\Omega_{\mathcal{O}_{X,x}/C}$ und damit wäre v surjektiv. Wegen der Exaktheit ist v genau dann surjektiv, wenn u die Nullabbildung ist, und das ist äquivalent zu $\Omega_{\mathcal{O}_{X,x}/\mathcal{O}_{Y,f(x)}} = 0$.

□

3.3 Garben von Differentialformen

Definition 3.3.1 *Sei $\mathcal{F}$ eine Garbe (von Gruppen, Ringen, Moduln) auf einem topologischen Raum X, dann heißt*

$$\operatorname{supp} \mathcal{F} := \{P \in X \mid \mathcal{F}_P \neq 0\}$$

der ***Träger*** *von $\mathcal{F}$.*

Sei $U \subset X$ eine offene Teilmenge und $s \in \mathcal{F}(U)$, dann heißt

$$\operatorname{supp} s := \{P \in U \mid s_P \neq 0\}$$

der Träger von s.

Wir wissen, daß wir zu einem gegebenen Ring A einen topologischen Raum $\operatorname{Spec} A$ mit einer Garbe von Ringen $\mathcal{O}$ konstruieren können. Sei nun M ein A-Modul, dann können wir eine Garbe $\widetilde{M}$ von $\mathcal{O}_X$-Moduln, d.h. für $U \subset X$ offen ist $\widetilde{M}(U)$ ein $\mathcal{O}_X(U)$-Modul, auf $\operatorname{Spec} A$ in analoger Weise konstruieren, so daß für einen Punkt $\mathfrak{p} \in \operatorname{Spec} A$ der Halm von $\widetilde{M}$ im Punkt $\mathfrak{p}$ isomorph zu $M_{\mathfrak{p}}$ ist und für eine offene Basismenge $D(f) \subset \operatorname{Spec} A$ der Modul $\widetilde{M}(D(f))$ isomorph zu M_f ist. Mit den folgenden zwei Lemmata werden wir sehen, daß der Träger einer solchen Garbe abgeschlossen in $\operatorname{Spec} A$ ist.

Lemma 3.3.2 *Sei A ein Ring und M ein A-Modul. Sei $m \in M$ und $\operatorname{Ann} m$ das Ideal $\{a \in A \mid am = 0\}$, dann gilt*

$$\operatorname{supp} m = V(\operatorname{Ann} m)$$

Beweis:
Sei $\mathfrak{p} \in \operatorname{supp} m$, d.h. das Bild von m in $M_{\mathfrak{p}}$ ist ungleich 0. Nach der Definition der Lokalisierung von Moduln ist $\frac{m}{1} \in M_{\mathfrak{p}}$ genau dann ungleich $\frac{0}{1}$, wenn für alle $h \in A$ stets $h \notin \mathfrak{p} \Longrightarrow hm \neq 0$ gilt. Das ist äquivalent zu $hm = 0 \Longrightarrow h \in \mathfrak{p}$ für alle $h \in A$, und das ist eine andere Schreibweise für $\operatorname{Ann} m \subset \mathfrak{p}$. Also gilt $\mathfrak{p} \in V(\operatorname{Ann} m)$.

$\square$

Lemma 3.3.3 *Sei A ein Ring und M ein endlich erzeugter A-Modul. Sei* $\operatorname{Ann} M$ *das Ideal* $\{a \in A \mid am = 0 \text{ für alle } m \in M\}$, *dann gilt*

$$\operatorname{supp} \widetilde{M} = V(\operatorname{Ann} M)$$

Beweis:
Seien $m_1, \ldots, m_n$ die Erzeugenden von M. Es gilt

1. $\operatorname{Ann} M = \bigcap_{i=1}^{n} \operatorname{Ann}(m_i)$
2. $\bigcup_{i=1}^{n} \operatorname{supp}(m_i) = \operatorname{supp} \widetilde{M}$

Zu. 1
"$\subset$" ist klar, es bleibt "$\supset$" zu zeigen. Sei $a \in \bigcap \operatorname{Ann}(m_i)$ und $m \in M$, dann hat m eine Darstellung $m = \sum \lambda_i m_i$. Es gilt $a \cdot m = \sum \lambda_i a \cdot m_i = 0$. Damit ist $a \in \operatorname{Ann} M$ gezeigt.

Zu. 2
"$\subset$" ist klar, es bleibt "$\supset$" zu zeigen. Sei $\mathfrak{p} \in \operatorname{supp} \widetilde{M}$, dann existiert ein $x \in M$, dessen Bild in $M_{\mathfrak{p}}$ ungleich Null ist. Wir können x als $x = \sum \lambda_i m_i$ schreiben. Für ein i ist das Bild von m_i in $M_{\mathfrak{p}}$ ungleich Null, damit liegt $\mathfrak{p}$ im Träger von m_i. Also gilt $\mathfrak{p} \in \bigcup \operatorname{supp} m_i$.

Es gilt

$$V(\operatorname{Ann} M) = V(\bigcap_{i=1}^{n} \operatorname{Ann} m_i) = \bigcup_{i=1}^{n} V(\operatorname{Ann} m_i) = \bigcup_{i=1}^{n} \operatorname{supp} m_i = \operatorname{supp} \widetilde{M}$$

Die vorletzte Gleichheit folgt aus Lemma 3.3.2.

$\square$

Folgerung 3.3.4 *Sei A ein Ring und M ein endlich erzeugter A-Modul. Dann ist der Träger von $\widetilde{M}$ abgeschlossen in* $\operatorname{Spec} A$.

Definition 3.3.5 *Sei X ein Schema und $\mathcal{F}$ eine Garbe von $\mathcal{O}_X$-Moduln auf X, d.h. für $U \subset X$ offen ist $\mathcal{F}(U)$ ein $\mathcal{O}_X(U)$-Modul. Die Garbe $\mathcal{F}$ heißt **kohärent**, falls X eine offene affine Überdeckung* $(\operatorname{Spec} A_i)_{i \in I}$ *hat, so daß zu jedem $i \in I$ ein endlich erzeugter A_i-Modul M_i existiert, so daß $\mathcal{F}(\operatorname{Spec} A_i) \cong \widetilde{M_i}$ gilt.*

Der Träger einer kohärenten Garbe ist nach Folgerung 3.3.4 stets abgeschlossen, da Abgeschlossenheit eine lokale Eigenschaft ist.

Satz 3.3.6 *Seien A' und B A-Algebren, und sei $B' = B \otimes_A A'$. Dann gilt*

$$\Omega_{B'/A'} \cong \Omega_{B/A} \otimes_B B'$$

Insbesondere gilt für eine multiplikativ abgeschlossene Teilmenge $S \subset B$

$$\Omega_{S^{-1}B/A} \cong S^{-1}\Omega_{B/A}$$

ohne Beweis

Lemma 3.3.7 *Seien A und B Integritätsringe, $f : A \longrightarrow B$ ein Ringhomomorphismus und $S \subset B$ eine multiplikativ abgeschlossene Teilmenge. Setze $T := f^{-1}(S)$, dann gilt*

$$\Omega_{B_S/A} \cong \Omega_{B_S/A_T}$$

Beweis:
Jede A_T-Derivation auf B_S ist insbesondere eine A-Derivation. Umgekehrt ist auch jede A-Derivation auf B_S eine A_T-Derivation, denn sei $v : B_S \longrightarrow M$ eine A-Derivation in einen B_S-Modul M, und sei $\frac{a}{t} \in A_T$, d.h. $a \in A$ und $t \in T \subset A$. Es gilt

$$0 = \frac{1}{t} \cdot v(1) = \frac{1}{t} \cdot v\left(\frac{1}{t} \cdot t\right) = \frac{1}{t}\left(\frac{1}{t} \cdot v(t) + tv\left(\frac{1}{t}\right)\right) = v\left(\frac{1}{t}\right)$$

Aus der Produktregel folgt $v\left(\frac{a}{t}\right) = 0$. Damit ist gezeigt, daß v auch eine A_T-Derivation ist.

Wir wissen nun, daß $d_{B_S/A}$ und d_{B_S/A_T} beide universelle A_T-Derivationen sind. Aus der universellen Eigenschaft folgt damit die Isomorphie.

□

Sei $f : X \longrightarrow Y$ ein endlicher Morphismus zwischen Kurven. Sei $V \cong \operatorname{Spec} A$ eine affine Teilmenge von Y, dann ist $U := f^{-1}(V)$ affin, d.h. $U \cong \operatorname{Spec} B$. Wir erhalten dann eine Garbe $(\Omega_{B/A})^{\sim}$ von $\mathcal{O}_U$-Moduln auf dem affinen Unterschema U.

Nun können wir die Garbe $\Omega_{X/Y}$ von $\mathcal{O}_X$-Moduln auf X definieren, indem wir X und Y affin überdecken und die zugehörigen Garben $(\Omega_{B/A})^{\sim}$ zusammenkleben. $\Omega_{X/Y}$ ist insbesondere eine kohärente Garbe.

Lemma 3.3.8 *Seien A und B K-Algebren, und sei $f : A \longrightarrow B$ ein modulendlicher K-Algebrenhomomorphismus. Dann ist B vermöge f eine A-Algebra und es gilt $(\Omega_{B/A})_{(0)} = 0$.*

Beweis:
$\Omega_{B/A}$ wird von $\{d_{B/A}(b) \mid b \in B\}$ erzeugt, wir zeigen daß jedes dieser Erzeugenden ein Torsionselement ist, d.h. zu $b \in B$ existiert ein $0 \neq c \in B$, so daß $c \cdot d_{B/A}(b) = 0$ gilt. Wenn das gezeigt ist, folgt die Behauptung, denn es gilt $(\Omega_{B/A})_{(0)} \cong B_{(0)} \otimes_B \Omega_{B/A}$ nach Lemma 3.3.6 mit $S := B \setminus \{0\}$ und Lemma 3.3.7. Für $1 \otimes d_{B/A}(b)$ mit $b \in B$ gilt

$$1 \otimes d_{B/A}(b) = \left(\frac{1}{c} \cdot c\right) \otimes d_{B/A}(b) = \frac{1}{c} \otimes c d_{B/A}(b) = \frac{1}{c} \otimes 0 = 0$$

Es bleibt noch zu zeigen, daß $d_{B/A}(b)$ mit $b \in B$ ein Torsionselement ist. Jede modulendliche Ringerweiterung ist eine ganze Ringerweiterung. Sei nun $b \in B$, dann erfüllt b eine Ganzheitsgleichung über A, d.h. $\sum_{i=0}^{n} a_i b^i = 0$ mit $a_i \in A$ und $a_n = 1$. Wir nehmen an, daß die Ganzheitsgleichung so gewählt ist, daß n minimal ist. Man sieht leicht, daß $d_{B/A}(b^n) = nb^{n-1}d_{B/A}(b)$ gilt. Bei uns haben alle Körper Charakteristik 0, also hat n ein Inverses in B.

$$0 = \frac{1}{n} d_{B/A}\left(\sum_{i=0}^{n} a_i b^i\right) = \frac{1}{n}\sum_{i=1}^{n} a_i i b^{i-1} d_{B/A}(b) = \left(\sum_{i=0}^{n-1} a_{i+1}\frac{i+1}{n} b^i\right) d_{B/A}(b)$$

Aus der Minimalität von n und aus $a_n = 1$ folgt $c := \sum_{i=0}^{n-1} a_{i+1}\frac{i+1}{n} b^i \neq 0$. Damit ist gezeigt, daß $d_{B/A}(b)$ ein Torsionselement ist.

□

Folgerung 3.3.9 *Seien $X = \operatorname{Spec} B$ und $Y = \operatorname{Spec} A$ affine Kurven über $\mathbb{C}$, und sei $f : X \longrightarrow Y$ ein endlicher Morphismus. f wird von einem $\mathbb{C}$-Algebrenhomomorphismus $A \longrightarrow B$ induziert und es gilt*

$$\operatorname{Crit}(f) = \operatorname{supp} \Omega_{B/A}$$

Insbesondere ist $\operatorname{Crit}(f)$ abgeschlossen in $\operatorname{Spec} B$.

Beweis:
Nach Lemma 3.3.8 gilt $(0) \notin \operatorname{supp} \Omega_{B/A}$. Nun betrachten wir die abgeschlossenen Punkte.

Sei $\mathfrak{m}_B$ ein maximales Ideal in B, und sei $\mathfrak{m}_A \subset A$ das Bild von $\mathfrak{m}_B$ unter f. B ist in natürlicher Weise eine A-Algebra und es gilt nach Satz 3.3.6 mit $S := B \setminus \mathfrak{m}_B$

$$(\Omega_{B/A})_{\mathfrak{m}_B} \cong \Omega_{B_{\mathfrak{m}_B}/A}$$

$B_{\mathfrak{m}_B}$ ist eine $A_{\mathfrak{m}_A}$-Algebra vermöge dem induzierten lokalen Ringhomomorphismus. Nach Lemma 3.3.7 gilt

$$\Omega_{B_{\mathfrak{m}_B}/A} \cong \Omega_{B_{\mathfrak{m}_B}/A_{\mathfrak{m}_A}}$$

insgesamt erhalten wir dann

$$(\Omega_{B/A})_{\mathfrak{m}_B} \cong \Omega_{B_{\mathfrak{m}_B}/A_{\mathfrak{m}_A}}$$

Aus Satz 3.2.6 folgt damit die Behauptung.

□

Folgerung 3.3.10 *Sei $f : X \longrightarrow Y$ ein endlicher Morphismus zwischen Kurven. Dann ist die Menge der kritischen Punkte von f abgeschlossen und damit endlich.*

Denn: Sei $V \subset Y$ affin, dann ist auch $U := f^{-1}(V)$ affin. Die Menge der kritischen Punkte von $f_{|U}$ ist dann nach Folgerung 3.3.9 abgeschlossen in U. Nun ist Angeschlossenheit eine lokale Eigenschaft, damit ist die Menge der kritischen Punkte von f abgeschlossen.

Der generische Punkt ist kein kritischer Punkt, also ist die Menge der kritischen Punkte von f endlich.

□

4 Die projektive Gerade

Im Folgenden ist C ein algebraisch abgeschlossener Körper. In diesem Abschnitt werden einige Eigenschaften des projektiven Schemas $\mathbb{P}^1_C$, die wir später benötigen werden, betrachtet.

Wir betrachten den Polynomring in zwei Veränderlichen $C[X,Y]$. Sei $S_+ := (X,Y)$ das von X und Y erzeugte Ideal. Die zugrundeliegende Menge von

$$\mathbb{P}^1_{\mathbb{C}} := \operatorname{Proj} C[X,Y]$$

besteht aus denjenigen homogenen Primidealen $\mathfrak{p} \in C[X,Y]$, die echt in S_+ enthalten sind. Dazu gehört der nicht-abgeschlossene Punkt (0) und die abgeschlossenen Punkte $\mathfrak{p} \in \mathbb{P}^1_C$ von der Form $\mathfrak{p} = (aX+bY)$ mit $(a,b) \in C^2 \backslash \{(0,0)\}$.

Die abgeschlossenen Mengen in $\mathbb{P}^1_{\mathbb{C}}$ sind Teilmengen von der Form $V(I) = \{\mathfrak{p} \in \mathbb{P}^1_C \mid I \subset \mathfrak{p}\}$ mit einem homogenen Ideal $I \subset C[X,Y]$.

4.1 Polynome als Morphismen

Im Folgenden werden wir sehen, wie man ein nicht-konstantes Polynom $f \in C[X]$ als Morphismus $\mathbb{P}^1_C \longrightarrow \mathbb{P}^1_C$ auffassen kann. Zunächst betrachten wir den einfacheren Fall, indem wir zu einem gegebenen Polynom f einen Morphismus $\operatorname{Spec} C[X] \longrightarrow \operatorname{Spec} C[X]$ konstruieren. Anschließend werden wir diese Konstruktion auf $\mathbb{P}^1_C$ erweitern.

Sei $f \in C[X]$ ein Polynom. Wir definieren einen C-Algebrenhomomorphismus

$$\begin{array}{rcl} f^* : C[X] & \longrightarrow & C[X] \\ X & \longmapsto & f \end{array}$$

Dieser induziert einen Morphismus

$$\operatorname{Spec} f^* : \operatorname{Spec} C[X] \longrightarrow \operatorname{Spec} C[X]$$

Sei $(X-\lambda) \in \operatorname{Spec} C[X]$ ein abgeschlossener Punkt, dann gilt

$$\operatorname{Spec} f^*((X-\lambda)) = (X-\mu) \text{ mit } \mu = f(\lambda)$$

Denn: λ eine Nullstelle von $f-\mu$, also gilt $f-\mu \in (X-\lambda)$. $f-\mu$ ist das Bild von $X-\mu$ unter f^*, also umfaßt das Urbild vom Ideal $(X-\lambda)$ das Ideal $(X-\mu)$. Aus der Maximalität von $(X-\mu)$ folgt die Gleichheit. Man sieht genauso leicht, daß der generische Punkt (0) unter $\operatorname{Spec} f^*$ auf selbigen abgebildet wird.

Wir können also die Punkte aus C mit den abgeschlossenen Punkten aus $\operatorname{Spec} C[X]$ identifizieren, so daß diese Identifikation mit $f \longmapsto \operatorname{Spec} f^*$ verträglich ist. Mit dem folgenden Lemma erhalten wir eine Kennzeichung der kritischen Punkte von $\operatorname{Spec} f^*$. Für den Beweis wird eine Bemerkung aus Kapitel 9.1 benötigt.

Lemma 4.1.1 *Sei* $(X-\lambda) \in \operatorname{Spec} C[X]$ *ein abgeschlossener Punkt, dann ist* $(X-\lambda)$ *genau dann ein kritischer Punkt von* $\operatorname{Spec} f^*$*, wenn* $f'(\lambda) = 0$ *gilt.*

Beweis:
Setze $\mu := f(\lambda)$, dann ist λ eine Nullstelle von $f-\mu$, d.h. $f-\mu \in (X-\lambda)$. Es gilt $f-\mu \in (X-\lambda)^2$ genau dann, wenn λ eine mehrfache Nullstelle von $f-\mu$ ist. Nun ist allgemein bekannt, daß λ genau dann eine mehrfache Nullstelle von $f-\mu$ ist, wenn $f'(\lambda) = (f-\mu)'(\lambda) = 0$ gilt.

Spec f^* induziert einen lokalen Ringhomomorphismus

$$\begin{array}{rcl} \varphi : C[X]_{(X-\mu)} & \longrightarrow & C[X]_{(X-\lambda)} \\ X & \longmapsto & f \end{array}$$

zwischen nach maximalen Idealen lokalisierten Polynomringen. $X-\mu$ und $X-\lambda$ sind die Erzeugenden der entsprechenden maximalen Ideale.

Nun gilt $f'(\lambda) = 0$ genau dann, wenn $X-\mu$ unter φ nach $(X-\lambda)^2$ abgebildet wird. Nach Bemerkung 9.1.2 ist daß äquivalent dazu, daß $(X-\lambda)$ ein kritischer Punkt von Spec f^* ist.

$\square$

Nun werden wir f einen Morphismus $\mathbb{P}^1_C \longrightarrow \mathbb{P}^1_C$ zuordnen. Sei n der Grad von $f(X)$, und sei $F(X,Y) := Y^n f\left(\frac{X}{Y}\right)$ die Homogenisierung nach Y. Es gilt $n \geq 1$, da f nicht-konstant ist. Wir definieren einen C-Algebrenhomomorphismus

$$\begin{array}{rcl} F^* : C[X,Y] & \longrightarrow & C[X,Y] \\ X & \longmapsto & F \\ Y & \longmapsto & Y^n \end{array}$$

F^* ist injektiv, und homogene Polynome werden unter F^* auf homogene Polynome abgebildet. Umgekehrt sind auch die Urbilder homogener Polynome homogen. Wir betrachten nun die Urbilder homogener Primideale. Das Urbild von (Y) ist (Y). Wegen der Injektivität von von F^* ist das Urbild von (0) ebenfalls (0). Es fehlt noch das Urbild von $(X-\lambda Y)$ mit $\lambda \in C$.

Setze $\mu := f(\lambda)$, dann ist $X-\lambda$ ein Teiler von $f-\mu$, d.h. es existiert ein $g \in C[X]$ mit

$$f-\mu = g\cdot(X-\lambda)$$

Wir homogenisieren beide Seiten der Gleichung nun nach Y:

$$\begin{array}{rcl} Y^n \cdot \left(f\left(\dfrac{X}{Y}\right) - \mu\right) & = & Y^n \cdot g\left(\dfrac{X}{Y}\right)\cdot\left(\dfrac{X}{Y}-\lambda\right) \\ \Longleftrightarrow F(X,Y) - \mu Y^n & = & Y^{n-1}\cdot g\left(\dfrac{X}{Y}\right)\cdot(X-\lambda Y) \end{array}$$

Also ist $X-\lambda Y$ ein Teiler von $F(X,Y)-\mu Y^n$, damit gilt

$$F(X,Y)-\mu Y^n \in (X-\lambda Y)$$

Damit ist $(X-\mu Y)$ im Urbild von $(X-\lambda Y)$ enthalten. Nun ist $(X-\mu Y)$ ein maximales homogenes Ideal, daraus folgt die Gleichheit.

Wir erhalten damit eine stetige Abbildung

$$\operatorname{Proj} F^* : \operatorname{Proj} C[X,Y] \longrightarrow \operatorname{Proj} C[X,Y]$$

Als nächstes werden wir die kritischen Punkte von $\operatorname{Proj} F^*$ kennzeichnen. Wir betrachten das affine Unterschema $D_+(Y) \subset \mathbb{P}^1_C$, das sind alle Punkte bis auf den Punkt im unendlichen (Y). Es gilt $\operatorname{Spec} C[X] \cong D_+(Y)$, und der Morphismus $\operatorname{Proj} F^*_{|D_+(Y)}$ entspricht dem Morphismus $\operatorname{Spec} f^*$. Wir erhalten folgendes Resultat:

Folgerung 4.1.2 $(X - \lambda Y)$ *ist genau dann ein kritischer Punkt von* $\operatorname{Proj} F^*$*, wenn* $f'(\lambda) = 0$ *gilt.*

4.2 Gebrochen-lineare Transformationen als Morphismen

Wir betrachten bijektive gebrochen-lineare Transformationen $\frac{ax+b}{cx+d}$, d.h. es gilt

$$\det \begin{bmatrix} a & b \\ c & d \end{bmatrix} \neq 0$$

Zu einer gegebenen gebrochen-linearen Transformation definieren wir einen C-Algebrenhomomorphismus

$$\begin{array}{rcl} C[X,Y] & \longrightarrow & C[X,Y] \\ X & \longmapsto & aX + bY \\ Y & \longmapsto & cX + dY \end{array}$$

Nun betrachten wir die Urbilder von Punkten aus $D_+(Y)$, also Punkte der Form $(X - \lambda Y)$ mit $\lambda \in C$. Dazu unterscheiden wir zwei Fälle:

$\lambda \neq -\frac{d}{c}$**:**
Das Urbild von $(X - \lambda Y)$ ist das Ideal $(X - \mu Y)$ mit $\mu = \frac{a\lambda+b}{c\lambda+d}$. Denn: Das Bild von $X - \mu Y$ ist $(aX + bY) - \mu(cX + dY)$. Wir multiplizieren mit der Einheit $c\lambda + d$:

$$\begin{aligned} & (c\lambda + d)(aX + bY) - (a\lambda + b)(cX + dY) \\ = \; & (ac\lambda + ad - ac\lambda - bc)X + (bc\lambda + bd - ad\lambda - bd)Y \\ = \; & (ad - bc)X + (bc\lambda - ad\lambda)Y \\ = \; & (ad - bc)X - \lambda(ad - bc)Y \end{aligned}$$

Wir dividieren nochmal durch $ad - bc \neq 0$, dann wird $X - \lambda Y$ getroffen.

$\lambda = -\frac{d}{c}$**:**
Das Urbild von $(X - \lambda Y) = (cX + dY)$ ist das Ideal (Y).

Wir können gebrochen-lineare Transformationen also als Morphismen $\mathbb{P}^1_C \longrightarrow \mathbb{P}^1_C$ betrachten. Diese sind sogar Isomorphismen und haben deshalb keine kritischen Punkte.

Satz 4.2.1 *Seien $x_1, x_2, x_3 \in \mathbb{P}^1_C$ paarweise verschiedene abgeschlossene Punkte. Dann existiert eine gebrochen-lineare Transformation q mit*

$$x_1 \longmapsto 0,\ x_2 \longmapsto 1,\ x_3 \longmapsto \infty$$

Beweis:
Setze

$$q(x) := \frac{x - x_1}{x - x_3} \cdot \frac{x_2 - x_3}{x_2 - x_1}$$

q ist bijektiv, da $\det \begin{bmatrix} 1 & x_1 \\ 1 & x_3 \end{bmatrix} \neq 0$ gilt.

□

4.3 K-rationale Punkte

Sei $\sigma \in \mathrm{Aut}(C)$, wir definieren einen Ringhomomorphismus

$$\begin{array}{rcl} C[X,Y] & \longrightarrow & C[X,Y] \\ \sum a_{ij} X^i Y^j & \longmapsto & \sum \sigma(a_{ij}) X^i Y^j \end{array}$$

indem wir auf den Koeffizienten der Polynome operieren. Das Urbild vom Punkt $(aX + bY) \in \mathbb{P}^1_C$ ist $(\sigma^{-1}(a)X + \sigma^{-1}(b)Y)$. Wir erhalten einen Isomorphismus

$$\mathrm{Proj}(\sigma) : (\mathbb{P}^1_C)^\sigma \longrightarrow \mathbb{P}^1_C$$

Das folgende Diagramm kommutiert:

$$\begin{tikzcd}
(\mathbb{P}^1_C)^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"] \arrow[d] & \mathbb{P}^1_C \arrow[d] \\
C^\sigma \arrow[r, "\mathrm{Spec}(\sigma)"'] & C
\end{tikzcd}$$

Also ist die C-Varietät $(\mathbb{P}^1_C)^\sigma$ isomorph zur C-Varietät $\mathbb{P}^1_C$. Der Funktionenkörper $K(\mathbb{P}^1_C)$ ist isomorph zum Körper der rationalen Funktionen in einer Veränderlichen, also $C(X)$. Der durch $\mathrm{Proj}(\sigma)$ induzierte Körperautomorphismus ist

$$\begin{array}{rcl} \mathrm{Proj}(\sigma)^* : C(X) & \longrightarrow & C(X) \\ a \in C & \longmapsto & \sigma(a) \\ X & \longmapsto & X \end{array}$$

Definition 4.3.1 *Sei $K \subset C$ ein Unterkörper, dann heißt ein abgeschlossener Punkt $(aX + bY) \in \mathbb{P}^1_C$ K-rational, falls ein $\lambda \in C$ existiert, so daß $\lambda a, \lambda b \in K$ gilt.*

Bemerkung 4.3.2 *Für* $\sigma \in \mathrm{Aut}(C:K)$ *sind* K*-rationale Punkte invariant unter* $\mathrm{Proj}(\sigma)$.

Denn: sei $(aX + bY) \in \mathbb{P}^1_C$ ein K-rationaler Punkt, d.h. es existiert ein $\lambda \in C$ mit $\lambda a, \lambda b \in K$. Es gilt

$$\lambda a \in K \Longrightarrow \sigma^{-1}(\lambda a) \in K \Longrightarrow \sigma^{-1}(\lambda)\sigma^{-1}(a) \in K$$

Analog gilt $\sigma^{-1}(\lambda)\sigma^{-1}(b) \in K$, also ist auch $(\sigma^{-1}(a)X + \sigma^{-1}(b)Y)$ K-rational.

Bemerkung 4.3.3 *Sei* $(aX+bY) \in \mathbb{P}^1_C$ *ein* K*-rationaler Punkt, dann existiert im lokalen Ring* $C[X,Y]_{((aX+bY))}$ *ein lokaler Parameter, der invariant unter* $\mathrm{Aut}(C:K)$ *ist.*

5 Galois Überlegungen

Im Folgenden ist C ein algebraisch abgeschlossener Körper und alle auftretenden Körper haben Charakteristik 0.

5.1 Galois Korrespondenz

Satz 5.1.1 (Fortsetzungssatz) *Sei K ein Körper, C ein algebraisch abgeschlossener Körper und $\sigma : K \longrightarrow C$ ein Körperhomomorphismus. Für jede algebraische Erweiterung L von K existiert eine Fortsetzung zu einem Körperhomomorphismus $\widetilde{\sigma} : L \longrightarrow C$.*

Beweis mit Zornschem Lemma.

□

Lemma 5.1.2 *Sei $K \subset C$ ein Unterkörper, dann kann jeder Körperautomorphismus $\sigma \in \mathrm{Aut}(K)$ zu einem Automorphismus auf ganz C fortgesetzt werden.*

Beweis:
Sei τ eine Transzendenzbasis von $C : K$. Nun läßt sich jedes $x \in K(\tau)$ als rationale Funktion in $x_1, \ldots, x_s \in \tau$ mit Koeffizienten aus K auffassen. Also können wir einen Körperautomorphismus $\widetilde{\sigma} : K(\tau) \longrightarrow K(\tau)$ definieren, wobei σ für jedes $x \in K(\tau)$ auf den Koeffizienten operiert. Es gilt $\widetilde{\sigma}_{|K} = \sigma$ und $\widetilde{\sigma}_{|\tau} = \mathrm{id}_\tau$, also ist $\widetilde{\sigma}$ eine Fortsetzung von σ auf $K(\tau)$. Als nächstes müssen wir $\widetilde{\sigma}$ zu einem Automorphismus auf C fortsetzen. $C : K(\tau)$ ist eine algebraische Erweiterung und $\widetilde{\sigma}$ ist ein Körperhomomorphismus von $K(\tau)$ nach C. Nach Satz 5.1.1 existiert eine Fortsetzung $\overline{\sigma} : C \longrightarrow C$ von $\widetilde{\sigma}$. Das Bild von $\overline{\sigma}$ ist ein algebraisch abgeschlossener Unterkörper von C, da C algebraisch abgeschlossen ist. Also gilt $\mathrm{Im}\,\overline{\sigma} = C$, damit ist $\overline{\sigma}$ ein Körperautomorphismus.

□

Anwendung von Lemma 5.1.2:

Satz 5.1.3 *Sei $K \subset C$ Unterkörper, dann gilt*

$$C^{\mathrm{Aut}(C:K)} = K$$

Beweis:

„$\subset$"

Sei $x \in C \setminus K$. Es ist zu zeigen, daß ein $\sigma \in \mathrm{Aut}(C : K)$ existiert, so daß $\sigma(x) \neq x$ gilt.

Fall 1: x ist transzendent über K
Wähle $\sigma \in \mathrm{Aut}(K(x) : K)$ mit $\sigma(x) = -x$. σ kann nach Lemma 5.1.2 zu einem Automorphismus auf ganz C fortgesetzt werden.

Fall 2:

x hat ein Minimalpolynom $m_x \in K[X]$. Sei

$$N := \{x \in C \mid m_x(x) = 0\}$$

die Nullstellenmenge von m_x, dann ist $K(N)$ der Zerfällungskörper von m_x. m_x ist separabel, also können wir ein $\sigma \in \mathrm{Aut}(K(N) : K)$ mit $\sigma(x) \neq x$ wählen. σ kann zu einem Automorphismus auf ganz C fortgesetzt werden.

„$\supset$"

klar per Definition

$\square$

Definition 5.1.4 *Eine Untergruppe $U \subset \mathrm{Aut}(C)$ heißt abgeschlossen, falls ein Unterkörper $K \subset C$ mit $U = \mathrm{Aut}(C : K)$ existiert.*

Bemerkung 5.1.5 $U \subset \mathrm{Aut}(C)$ *abgeschlossen* $\Longrightarrow$ $U = \mathrm{Aut}(C : C^U)$

Beweis:
Sei U abgeschlossen, d.h. $U = \mathrm{Aut}(C : L)$ mit einem Unterkörper $L \subset C$. Nach Satz 5.1.3 gilt $C^U = L$ und daraus folgt $U = \mathrm{Aut}(C : C^U)$.

$\square$

Wir erhalten damit eine Galois Korrespondenz zwischen den abgeschlossenen Untergruppen von $\mathrm{Aut}(C)$ und den Unterkörpern von C:

$$\begin{array}{ccc} K & \longmapsto & \mathrm{Aut}(C : K) \\ U & \longmapsto & C^U \end{array}$$

5.2 Unendliche Körpererweiterungen

Lemma 5.2.1 *Sei $U \subset \mathrm{Aut}(C)$ eine Untergruppe und $K : C^U$ eine endliche Körpererweiterung mit $\mathrm{Aut}(C : K) \subset U$. Dann ist U abgeschlossen.*

Beweis:
Wenn wir K durch seinen normalen Abschluß ersetzen, gelten die Voraussetzungen weiterhin, also können wir annehmen, daß $K : C^U$ eine normale und damit galoissche Körpererweiterung ist. Wir haben nun den Einschränkungshomomorphismus

$$\begin{array}{rcl} \varphi : \mathrm{Aut}(C : C^U) & \longrightarrow & \mathrm{Aut}(K : C^U) \\ \sigma & \longmapsto & \sigma_{|K} \end{array}$$

Per Definition gilt $U \subset \mathrm{Aut}(C : C^U)$. Sei $\varphi(U)$ das Bild von U, dann gilt $K^{\varphi(U)} = C^U$ und daraus folgt $\varphi(U) = \mathrm{Aut}(K : C^U)$, da die Körpererweiterung $K : C^U$ galoissch und endlich ist.

Es gilt $\ker\varphi = \mathrm{Aut}(C:K)$ und $\mathrm{Aut}(C:K) \subset U \subset \mathrm{Aut}(C:C^U)$, also erhalten wir einen Isomorphismus

$$\mathrm{Aut}(C:C^U)/\,\mathrm{Aut}(C:K) \cong \mathrm{Aut}(K:C^U)$$

und damit gilt $U = \mathrm{Aut}(C:C^U)$.

□

Bemerkung 5.2.2 *Sei $U \subset \mathrm{Aut}(C)$ eine Untergruppe, und sei $\sigma \in \mathrm{Aut}(C)$ ein Körperautomorphismus. Dann gilt*

$$C^{\sigma U \sigma^{-1}} = \sigma(C^U)$$

Beweis:

$$\begin{aligned} x \in C^{\sigma U \sigma^{-1}} &\iff \forall \tau \in U\colon x = \sigma\tau\sigma^{-1}(x) \\ &\iff \forall \tau \in U\colon \sigma^{-1}(x) = \tau(\sigma^{-1}(x)) \\ &\iff \sigma^{-1}(x) \in C^U \\ &\iff x \in \sigma(C^U) \end{aligned}$$

□

Lemma 5.2.3 *Sei G eine Gruppe, $H \subset G$ eine Untergruppe von endlichem Index. Dann existiert eine Untergruppe $N \subset G$, die normal und von endlichem Index ist, so daß $N \subset H$ gilt.*

Beweis:
Zuerst zeigen wir, daß für Untergruppen H_1, H_2 von endlichem Index die Untergruppe $H_1 \cap H_2$ endlichen Index hat. Sei $a \in G$, dann gilt
$a(H_1 \cap H_2) = aH_1 \cap aH_2$. Nun haben H_1, H_2 nur endlich viele Nebenklassen, daraus folgt, daß $H_1 \cap H_2$ endlich viele Nebenklassen hat. Wir betrachten für alle $\sigma \in G$ die konjugierten $\sigma H \sigma^{-1}$ von H, dann folgt induktiv, daß

$$N := \bigcap_{\sigma \in G} \sigma H \sigma^{-1}$$

endlichen Index in G hat. Es bleibt zu zeigen, daß N normal in G ist. Für $\tau \in G$ gilt

$$\tau N \tau^{-1} = \tau \left(\bigcap_{\sigma \in G} \sigma H \sigma^{-1} \right) \tau^{-1} = \bigcap_{\sigma \in G} (\tau\sigma) H (\tau\sigma)^{-1} = \bigcap_{\sigma \in G} \sigma H \sigma^{-1} = N$$

□

Satz 5.2.4 *Sei L ein Körper, $G \subset \mathrm{Aut}(L)$ eine endliche Untergruppe, und sei $K := L^G$ der Fixkörper von G. Dann ist die Körpererweiterung $L:K$ endlich und galoissch.*

Beweis: Satz 4 auf S.140 in [Bo]

Lemma 5.2.5 *Sei $U \subset \operatorname{Aut}(C)$ eine Untergruppe und $V \subset U$ eine Untergruppe von endlichem Index. Dann ist die Körpererweiterung $C^V : C^U$ endlich algebraisch. Falls V normal in U oder U abgeschlossen ist, gilt*

$$[C^V : C^U] \leq [U : V]$$

Beweis:
Nach Lemma 5.2.3 existiert eine Untergruppe $W \subset U$, die normal und von endlichem Index ist, so daß $W \subset V$ gilt. Wegen Bemerkung 5.2.2 gilt $\sigma(C^W) = C^W$ für alle $\sigma \in U$. Nun können wir folgenden Gruppenhomomorphismus definieren:

$$\begin{array}{rcl} \varphi : U & \longrightarrow & \operatorname{Aut}(C^W : C^U) \\ \sigma & \longmapsto & \sigma_{|C^W} \end{array}$$

Es gilt $W \subset \ker \varphi$, damit erhalten wir kanonisch

$$\widetilde{\varphi} : U/W \quad \longrightarrow \quad \operatorname{Aut}(C^W : C^U)$$

Nun gilt $(C^W)^{\varphi(U)} = C^U$, und aus U/W endlich folgt $\varphi(U)$ endlich. Also ist $C^U \subset C^W$ Fixkörper einer endlichen Gruppe, damit ist die Körpererweiterung $C^W : C^U$ nach Satz 5.2.4 endlich und galoissch. Daraus folgt
$\varphi(U) = \operatorname{Aut}(C^W : C^U)$. Insbesondere ist $C^V : C^U$ endlich, da C^V ein Zwischenkörper von $C^W : C^U$ ist. $\widetilde{\varphi}$ ist surjektiv, also gilt

$$[C^W : C^U] = \# \operatorname{Aut}(C^W : C^U) \leq \#U/W = [U : W]$$

Damit gilt $[C^V : C^U] \leq [U : V]$, falls V bereits normal in U ist.

W ist normal und von endlichem Index in V, also ist auch $[C^W : C^V]$ mit dem gleichen Argument wie oben endlich und galoissch. Nun gilt allgemein:

$$[C^V : C^U] = \frac{[C^W : C^U]}{[C^W : C^V]} = \frac{\# \operatorname{Aut}(C^W : C^U)}{\# \operatorname{Aut}(C^W : C^V)} = \#(\operatorname{Aut}(C : C^U)/ \operatorname{Aut}(C : C^V))$$

Sei U abgeschlossen, dann gilt $U = \operatorname{Aut}(C : C^U)$ und $V \subset \operatorname{Aut}(C : C^V)$. Daraus folgt $[C^V : C^U] \leq \#U/V = [U : V]$.

□

5.3 Anhang: Untergruppen von festem Index

Bemerkung 5.3.1 *Sei G eine Gruppe und X eine Menge, auf der G operiere. Sei $x_0 \in X$, dann erhalten wir eine bijektive Abbildung*

$$\varphi_{x_0} : G/\operatorname{Stab}(x_0) \longrightarrow Gx_0$$

Insbesondere ist der Orbit Gx_0 von x_0 genau dann endlich, wenn $\operatorname{Stab}(x_0)$ endlichen Index in G hat.

Satz 5.3.2 *Sei G eine endlich erzeugte Gruppe. Sei $d \in \mathbb{N} \setminus \{0\}$, dann ist die Anzahl der Untergruppen vom Index d endlich.*

Beweis:
Sei $U \subset G$ eine Untergruppe, dann erhalten wir eine Gruppenoperation

$$\begin{array}{rcl} G \times G/U & \longrightarrow & G/U \\ (g, xU) & \longmapsto & (gx)U \end{array}$$

auf den Restklassen von G/U. Die Operation ist transitiv und der Stabilisator der Restklasse U ist U selbst. G operiert nun auf einer endlichen Menge, wir numerieren die Restklassen durch, wobei wir U die 1 zuordnen. G operiert dann transitiv auf $\{1, \ldots, d\}$, wobei $\mathrm{Stab}(1) = U$ gilt. Wir erhalten also eine surjektive Zuordnung, wenn wir jeder transitiven Operation von G auf $\{1, \ldots, d\}$ die Untergruppe $\mathrm{Stab}(1)$ vom Index d zuordnen.

Sei F eine freie Gruppe vom Rang r, dann ist ein Gruppenhomomorphismus $F \longrightarrow S_d$, wobei S_d die Permutationsgruppe einer d-elementigen Menge bezeichnet, durch die Bilder der freien Erzeugenden eindeutig bestimmt, d.h. es gilt

$$\# \operatorname{Hom}(F, S_d) = (d!)^r$$

Eine Operation von G auf $\{1, \ldots, d\}$ ist das gleiche wie ein Gruppenhomomorphismus $G \longrightarrow S_d$. Nun ist G endlich erzeugt, also gilt

$$\# \operatorname{Hom}(G, S_d) \leq (d!)^r$$

□

Satz 5.3.3 *Sei G eine freie Gruppe vom Rang r. Sei $d \in \mathbb{N} \setminus \{0\}$, dann ist die Anzahl $M_{r,d}$ der Untergruppen vom Index d durch folgende Rekursionsformel gegeben:*

$$\begin{array}{rcl} N_{r,1} & = & 1 \\ N_{r,d} & = & d(d!)^{r-1} - \displaystyle\sum_{i=1}^{d-1} (d-i)!^{r-1} N_{r,i} \end{array}$$

Beweis: Theorem 7.2.9 auf S.105 in [Hal]

6 Belyi Verfahren

In diesem Abschnitt werden wir zu einer Kurve X über C, die bereits über $\mathbb{Q}^{\text{alg}}$ definiert ist, einen endlichen Morphismus $t : X \longrightarrow \mathbb{P}^1_C$ konstruieren, so daß dessen kritische Werte in $\{0, 1, \infty\}$ liegen. Damit wäre für $C = \mathbb{C}$ eine Richtung des Satzes von Belyi bewiesen.

Sei X eine Kurve über C, die bereits über $\mathbb{Q}^{\text{alg}}$ definiert ist, dann existiert nach Lemma 6.1.3 ein endlicher Morphismus $t_1 : X \longrightarrow \mathbb{P}^1_C$, dessen kritische Werte $\mathbb{Q}^{\text{alg}}$-rational sind. Sei S_1 die Menge der kritischen Werte von t_1, diese ist nach Folgerung 3.3.10 endlich. Nach Lemma 6.2.7 existiert ein endlicher Morphismus $t_2 : \mathbb{P}^1_C \longrightarrow \mathbb{P}^1_C$, der jeden Punkt aus S_1 auf einen $\mathbb{Q}$-rationalen Punkt abbildet und dessen kritische Werte $\mathbb{Q}$-rational sind. Sei nun S_2 die Menge der kritischen Werte von t_2, dann existiert nach Lemma 6.3.2 ein endlicher Morphismus $t_3 : \mathbb{P}^1_C \longrightarrow \mathbb{P}^1_C$, der $S_2 \cup t_2(S_1)$ nach $\{0, 1, \infty\}$ abbildet und dessen kritische Werte in $\{0, 1, \infty\}$ liegen. $t := t_3 \circ t_2 \circ t_1$ ist schließlich der gesuchte Morphismus.

6.1 Erster Schritt

Zu einer Kurve X über C, die bereits über einem algebraisch abgeschlossenen Unterkörper $N \subset C$ definiert ist, existiert ein nicht-konstanter Morphismus $t : X \longrightarrow \mathbb{P}^1_C$, der über N definiert ist. Denn: Es existiert eine Varietät X_N über N, so daß $X = X_N \times_{\operatorname{Spec} N} \operatorname{Spec} C$ gilt. X_N ist dann nach Bemerkung 2.1.11 eine Kurve. Wir wählen einen nicht-konstanten Morphismus $t_N : X_N \longrightarrow \mathbb{P}^1_N$, dieser induziert einen Morphismus $t : X \longrightarrow \mathbb{P}^1_C$. Ich erinnere daran, daß ein Morphismus zwischen vollständigen Kurven nach Satz 2.2.2 genau dann endlich ist, wenn er nicht-konstant ist. Wir zeigen nun, daß die kritischen Werte von t N-rational sind.

Für das Belyi Verfahren ist der Spezialfall $N = \mathbb{Q}^{\text{alg}}$ interessant.

Lemma 6.1.1 *Sei $K' : K$ eine Körpererweiterung, A eine K-Algebra und B eine A-Algebra. Setze $A' := A \otimes_K K'$ und $B' := B \otimes_K K'$.*
Sei $\pi : \operatorname{Spec} B' \longrightarrow \operatorname{Spec} B$ die durch die Inklusion $B \hookrightarrow B'$ induzierte Projektion, dann gilt

$$\pi(\operatorname{supp} \Omega_{B'/A'}) \subset \operatorname{supp} \Omega_{B/A}$$

Beweis:
Es gilt

$$B \otimes_A A' = B \otimes_A (A \otimes_K K') = (B \otimes_A A) \otimes_K K' = B \otimes_K K' = B'$$

Nach Satz 3.3.6 gilt $\Omega_{B'/A'} \cong \Omega_{B/A} \otimes_B B'$. Sei $\mathfrak{p} \in \operatorname{Spec} B'$ ein abgeschlossener Punkt, dann induziert π einen lokalen Ringhomomorphismus $\varphi : B_{\pi(\mathfrak{p})} \longrightarrow B'_{\mathfrak{p}}$. $B'_{\mathfrak{p}}$ ist damit ein $B_{\pi(\mathfrak{p})}$-Modul, also gilt $B'_{\mathfrak{p}} = B_{\pi(\mathfrak{p})} \otimes_{B_{\pi(\mathfrak{p})}} B'_{\mathfrak{p}}$.

$$\begin{aligned}
(\Omega_{B'/A'})_{\mathfrak{p}} &\cong \Omega_{B'/A'} \otimes_{B'} B'_{\mathfrak{p}} \\
&\cong (\Omega_{B/A} \otimes_B B') \otimes_{B'} B'_{\mathfrak{p}}
\end{aligned}$$

$$
\begin{aligned}
&\cong \Omega_{B/A} \otimes_B (B' \otimes_{B'} B'_{\mathfrak{p}}) \\
&\cong \Omega_{B/A} \otimes_B B'_{\mathfrak{p}} \\
&\cong \Omega_{B/A} \otimes_B (B_{\pi(\mathfrak{p})} \otimes_{B_{\pi(\mathfrak{p})}} B'_{\mathfrak{p}}) \\
&\cong (\Omega_{B/A} \otimes_B B_{\pi(\mathfrak{p})}) \otimes_{B_{\pi(\mathfrak{p})}} B'_{\mathfrak{p}} \\
&\cong (\Omega_{B/A})_{\pi(\mathfrak{p})} \otimes_{B_{\pi(\mathfrak{p})}} B'_{\mathfrak{p}}
\end{aligned}
$$

Aus $(\Omega_{B'/A'})_{\mathfrak{p}} \neq 0$ folgt damit $(\Omega_{B/A})_{\pi(\mathfrak{p})} \neq 0$, d.h.

$$\mathfrak{p} \in \operatorname{supp} \Omega_{B'/A'} \Longrightarrow \pi(\mathfrak{p}) \in \operatorname{supp} \Omega_{B/A}$$

□

Lemma 6.1.2 *Sei $N \subset C$ ein algebraisch abgeschlossener Unterkörper. Es gilt $C \otimes_N N[X] = C[X]$ und die durch $N[X] \hookrightarrow C[X]$ induzierte Projektion* $\operatorname{Spec} C[X] \longrightarrow \operatorname{Spec} N[X]$ *bildet alle nicht N-rationalen Punkte auf* $(0) \in \operatorname{Spec} N[X]$ *ab.*

Beweis:
Sei $(X - \lambda) \in \operatorname{Spec} C[X]$ ein nicht N-rationaler Punkt, d.h. $\lambda \notin N$ und damit ist λ transzendent über N. Dann ist $X - \lambda$ für alle $0 \neq p \in N[X]$ kein Teiler von p. Also wird unter der Inklusion $N[X] \hookrightarrow C[X]$ kein Element aus $(X - \lambda)$ außer der Null getroffen.

□

Lemma 6.1.3 *Sei X eine Kurve über C, und sei $t : X \longrightarrow \mathbb{P}^1_C$ ein endlicher Morphismus. Seien X und t über einem algebraisch abgeschlossenen Unterkörper $N \subset C$ definiert. Dann sind die kritischen Werte von t N-rational.*

Beweis:
X ist über N definiert, d.h. es existiert eine N-Varietät X_N, so daß

$$X = X_N \times_{\operatorname{Spec} N} \operatorname{Spec} C$$

gilt. $\mathbb{P}^1_C$ ist über N definiert, es gilt

$$\mathbb{P}^1_C \cong \mathbb{P}^1_N \times_{\operatorname{Spec} N} \operatorname{Spec} C$$

Seien $\alpha : X \longrightarrow X_N$ und $\beta : \mathbb{P}^1_C \longrightarrow \mathbb{P}^1_N$ die kanonischen Projektionen. t ist über N definiert, d.h. es existiert ein Morphismus $t_N : X_N \longrightarrow \mathbb{P}^1_N$ von N-Varietäten, so daß folgendes Diagramm kommutiert.

$$
\begin{tikzcd}
X_N \arrow[d, "t_N"'] & X \arrow[l, "\alpha"'] \arrow[d, "t"] \\
\mathbb{P}^1_N & \mathbb{P}^1_C \arrow[l, "\beta"]
\end{tikzcd}
$$

Nach Bemerkung 2.1.11 hat X_N die gleiche Dimension wie X, ist also eindimensional und ist damit eine vollständige Kurve. t ist ein nicht-konstanter Morphismus, damit ist auch t_N nicht-konstant. Also ist t_N ein endlicher Morphismus.

Wir betrachten das affine Unterschema $\mathbb{P}^1_N \setminus \{\infty\} \cong \operatorname{Spec} N[X]$, dann gilt

$$\beta^{-1}(\mathbb{P}^1_N \setminus \{\infty\}) = \mathbb{P}^1_C \setminus \{\infty\} \cong \operatorname{Spec} C[X]$$

$U := t_N^{-1}(\mathbb{P}^1_N \setminus \{\infty\})$ ist wegen der Endlichkeit von t_N ebenfalls affin, d.h. $U \cong \operatorname{Spec} B$. Das Urbild U' von U unter der Projektion α ist isomorph zu $\operatorname{Spec} B'$ mit $B' = B \otimes_N C$. Wir betrachten nun die kritischen Werte von $t_{|U'}$, denn $\infty \in \mathbb{P}^1_C$ ist ein N-rationaler Punkt und daher brauchen wir ihn nicht zu betrachten. Wir können uns nun auf affine Teile beschränken und erhalten folgendes kommutative Diagramm, wobei wir die Bezeichnungen für die Morphismen beibehalten.

$$\begin{tikzcd} U \arrow[d, "t_N"'] & U' \arrow[l, "\alpha"'] \arrow[d, "t"] \\ \mathbb{P}^1_N \setminus \{\infty\} & \mathbb{P}^1_C \setminus \{\infty\} \arrow[l, "\beta"] \end{tikzcd}$$

Es wird ein kommutives Diagramm von Ringhomomorphismen induziert:

$$\begin{tikzcd} B \arrow[r] & B' = B \otimes_N C \\ N[X] \arrow[u] \arrow[r] & C[X] \arrow[u] \end{tikzcd}$$

Wir haben nun die C bzw. N-Algebrenhomomorphismen $C[X] \longrightarrow B'$ und $N[X] \longrightarrow B$. Die Menge der kritischen Punkte von t stimmt nach Folgerung 3.3.9 mit $\operatorname{supp} \Omega_{B'/C[X]}$ überein. Nach Lemma 6.1.1 gilt

$$\alpha(\operatorname{supp} \Omega_{B'/C[X]}) \subset \operatorname{supp} \Omega_{B/N[X]}$$

Daraus folgt

$$\operatorname{supp} \Omega_{B'/C[X]} \subset \alpha^{-1}(\operatorname{supp} \Omega_{B/N[X]})$$

Die Menge der kritischen Werte von t stimmt mit $t(\operatorname{supp} \Omega_{B'/C[X]})$ überein. Es gilt

$$t(\operatorname{supp} \Omega_{B'/C[X]}) \subset t(\alpha^{-1}(\operatorname{supp} \Omega_{B/N[X]})) \subset \beta^{-1}(t_N(\operatorname{supp} \Omega_{B/N[X]}))$$

Für die letzte Inklusion brauchen wir die Morphismen nur als Abbildungen zu betrachten. Es gilt $\beta \circ t = t_N \circ \alpha$, insbesondere gilt dann

$$\begin{aligned} & \beta \circ t(\alpha^{-1}(\operatorname{supp} \Omega_{B/N[X]})) = t_N \circ \alpha(\alpha^{-1}(\operatorname{supp} \Omega_{B/N[X]})) \\ \Longrightarrow \quad & \beta \circ t(\alpha^{-1}(\operatorname{supp} \Omega_{B/N[X]})) \subset t_N(\operatorname{supp} \Omega_{B/N[X]}) \\ \Longrightarrow \quad & \beta^{-1}(\beta \circ t(\alpha^{-1}(\operatorname{supp} \Omega_{B/N[X]}))) \subset \beta^{-1}(t_N(\operatorname{supp} \Omega_{B/N[X]})) \\ \Longrightarrow \quad & t(\alpha^{-1}(\operatorname{supp} \Omega_{B/N[X]})) \subset \beta^{-1}(t_N(\operatorname{supp} \Omega_{B/N[X]})) \end{aligned}$$

Damit sind nun alle Inklusionen in der obigen Kette gezeigt. Nach Lemma 3.3.8 ist (0) nicht in $\operatorname{supp}\Omega_{B/N[X]}$ enthalten, und aus Lemma 6.1.2 folgt damit, daß $\beta^{-1}(t_N(\operatorname{supp}\Omega_{B/N[X]}))$ ausschließlich aus N-rationalen Punkten besteht.

$\square$

6.2 Zweiter Schritt

Als nächstes werden wir zu einer endlichen Teilmenge $S \subset \mathbb{P}^1_C$ von $\mathbb{Q}^{\text{alg}}$-rationalen Punkten einen nicht-konstanten und damit nach Satz 2.2.2 endlichen Morphismus von $\mathbb{P}^1_C$ nach $\mathbb{P}^1_C$ konstruieren, der jeden Punkt aus S auf einen $\mathbb{Q}$-rationalen Punkt abbildet und dessen kritische Werte $\mathbb{Q}$-rational sind.

Definition 6.2.1 *Sei $S \subset \mathbb{Q}^{\text{alg}}$ eine Teilmenge. S heißt gegen Konjugationen abgeschlossen, falls für jedes $s \in S$ und jeden Automorphismus $\sigma \in \operatorname{Aut}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$ stets $\sigma(s) \in S$ gilt. D.h. $\sigma(S) = S$ für alle $\sigma \in \operatorname{Aut}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$.*

Bemerkung 6.2.2 *Aus $S \subset \mathbb{Q}^{\text{alg}}$ einelementig und gegen Konjugationen abgeschlossen folgt $S \subset \mathbb{Q}$*

Bemerkung 6.2.3 *Sei $p \in \mathbb{Q}[X]$, dann ist $p(S)$ gegen Konjugationen abgeschlossen, falls S gegen Konjugationen abgeschlossen ist.*

Beweis:
Sei $x \in p(S)$, d.h. es existiert $s \in S$ mit $p(s) = x$. Es gilt

$$\sigma(x) = \sigma(p(s)) = p(\sigma(s))$$

S ist gegen Konjugationen abgeschlossen, also gilt $\sigma(s) \in S$ und daraus folgt $\sigma(x) \in p(S)$.

$\square$

Bemerkung 6.2.4 *Sei $p \in \mathbb{Q}[X]$, dann ist $N(p) := \{x \in \mathbb{Q}^{\text{alg}} \mid p(x) = 0\}$ gegen Konjugationen abgeschlossen.*

Beweis:
Sei $x \in \mathbb{Q}^{\text{alg}}$ mit $p(x) = 0$ und sei $\sigma \in \operatorname{Aut}(\mathbb{Q}^{\text{alg}}/\mathbb{Q})$. Es gilt

$$p(\sigma(x)) = \sigma(p(x)) = \sigma(0) = 0$$

$\square$

Bemerkung 6.2.5 *Sei $S \subset \mathbb{Q}^{\text{alg}}$ eine endliche Teilmenge, dann existiert eine endliche Teilmenge $\overline{S} \subset \mathbb{Q}^{\text{alg}}$ mit $S \subset \overline{S}$, so daß $\overline{S}$ gegen Konjugationen abgeschlossen ist.*

Beweis:
Für $s \in S$ bezeichne $m_s \in \mathbb{Q}[X]$ das Minimalpolynom von s über $\mathbb{Q}$. Wir definieren ein Polynom

$$p := \prod_{s \in S} m_s$$

Es gilt $p \in \mathbb{Q}[X]$ und $S \subset N(p)$. Setze $\overline{S} := N(p)$, dann ist $\overline{S}$ nach Bemerkung 6.2.4 gegen Konjugationen abgeschlossen.

□

Bemerkung 6.2.6 *Sei $S \subset \mathbb{Q}^{\mathrm{alg}}$ endlich und gegen Konjugationen abgeschlossen. Setze $n := \#S$, dann existiert ein nicht-konstantes Polynom $p \in \mathbb{Q}[X]$ vom Grad n, so daß $p(S) = \{0\}$ gilt.*

Beweis:
Setze

$$p := \prod_{s \in S} (X - s)$$

Sei $\sigma \in \mathrm{Aut}(\mathbb{Q}^{\mathrm{alg}}/\mathbb{Q})$, dann ist $\sigma_{|S} : S \longrightarrow S$ eine Permutation auf S, und damit gilt $\sigma(p) = p$. Daraus folgt $p \in \mathbb{Q}[X]$.

□

Das folgende Lemma gibt uns den gewünschten Morphismus, da wir Polynome nach Abschnitt 4.1 als Morphismen von $\mathbb{P}^1_C$ nach $\mathbb{P}^1_C$ auffassen können.

Lemma 6.2.7 *Sei $S \subset \mathbb{Q}^{\mathrm{alg}}$ eine endliche Teilmenge. Es existiert ein nicht-konstantes Polynom $p \in \mathbb{Q}[X]$, so daß $p(S) \subset \mathbb{Q}$ gilt und alle kritischen Werte von p in $\mathbb{Q}$ liegen.*

Beweis:
Nach Bemerkung 6.2.5 können wir annehmen, daß S gegen Konjugationen abgeschlossen ist. Induktion nach $n = \#S$:

$n \leq 1$:
Setze $p(X) := X$, dann hat p keine kritischen Werte und nach Bemerkung 6.2.2 gilt $p(S) = S \subset \mathbb{Q}$.

$n > 1$:
Nach Bemerkung 6.2.6 existiert ein nicht-konstantes Polynom $p_1 \in \mathbb{Q}[X]$ vom Grad n mit $p_1(S) = \{0\}$. ${p_1}'$ hat höchstens $n - 1$ Nullstellen. Also hat

$$S_1 := p_1\{r \in \mathbb{Q}^{\mathrm{alg}} \mid {p_1}'(r) = 0\}$$

höchstens $n - 1$ Elemente und ist nach Bemerkung 6.2.3 und 6.2.4 gegen Konjugationen abgeschlossen. Nach Induktionsvoraussetzung existiert ein nicht-konstantes Polynom $p_2 \in \mathbb{Q}[X]$, so daß $p_2(S_1) \subset \mathbb{Q}$ gilt und alle kritischen Werte von p_2 in $\mathbb{Q}$ liegen. Setze $p := p_2 \circ p_1$, damit gilt

$p(S) = p_2\{0\} \subset \mathbb{Q}$. Es bleibt zu zeigen, daß alle kritischen Werte von p in $\mathbb{Q}$ liegen. Es gilt

$$p'(X) = p_2{}'(p_1(X)) \cdot p_1{}'(X)$$

Sei z eine Nullstelle von p', d.h. $p_2(p_1(z))$ ist ein kritischer Wert von p.

Fall 1:
$p_1{}'(z) = 0 \implies p_1(z) \in S_1 \implies p_2(p_1(z)) \in p_2(S_1) \subset \mathbb{Q}$

Fall 2:
$p_2{}'(p_1(z)) = 0 \implies p_1(z)$ ist ein kritischer Punkt von $p_2 \implies p_2(p_1(z))$ ist ein kritischer Wert von $p_2 \implies p_2(p_1(z)) \in \mathbb{Q}$.

□

6.3 Dritter Schritt

Als letztes konstruieren wir einen nicht-konstanten und damit endlichen Morphismus $\mathbb{P}^1_C \longrightarrow \mathbb{P}^1_C$, der eine endliche Teilmenge $S \subset \mathbb{P}^1_C$ von $\mathbb{Q}$-rationalen Punkten nach $\{0, 1, \infty\}$ abbildet, so daß die kritischen Werte in $\{0, 1, \infty\}$ liegen.

Da wir Polynome und gebrochen-lineare Transformationen als Morphismen auffassen können[1], können wir die folgenden Beweise ein wenig einfacher formulieren.

Lemma 6.3.1 *Sei $x \in \mathbb{P}^1_C - \{0, 1, \infty\}$ ein $\mathbb{Q}$-rationaler Punkt. Dann existiert ein nicht-konstanter Morphismus q, der $\{0, 1, \infty, x\}$ nach $\{0, 1, \infty\}$ abbildet und dessen kritische Werte in $\{0, 1, \infty\}$ liegen.*

Als erstes wählen wir eine gebrochen-lineare Transformation q_2, die $\{0, 1, \infty, x\}$ nach $\{0, 1, \infty, x'\}$ abbildet, wobei $x' \in (0, 1)$ gilt. Wenn x bereits in $(0, 1)$ liegt, setzen wir $q_2 := \mathrm{id}$. Falls x dies nicht erfüllt, gibt es zwei Fälle:

Fall $x < 0$:
Setze $q_2 := \frac{1}{1-x}$

Fall $x > 1$:
Setze $q_2 := \frac{1}{x}$

Als nächstes wählen wir ein Polynom q_1, das $\{0, 1, \infty, x'\}$ nach $\{0, 1, \infty\}$ abbildet und dessen kritische Werte in $\{0, 1, \infty\}$ liegen. Nun gilt $x' \in (0, 1)$, also hat x' eine Darstellung $x' = \frac{m}{m+n}$ mit $m, n \in \mathbb{N}^+$. Setze

$$q_1(z) := \frac{(m+n)^{m+n}}{m^m n^n} z^m (1-z)^n$$

[1] siehe Abschnitt 4.1 und 4.2

Es gilt:

1. $q_1(0) = 0$
2. $q_1(1) = 0$
3. $q_1(\infty) = \infty$
4. $q_1(x') = 1$

Die Rechnung zu 4.:

$$x'^m(1-x')^n = \left(\frac{m}{m+n}\right)^m \left(\frac{n}{m+n}\right)^n = \frac{m^m n^n}{(m+n)^{m+n}}$$

Nun müssen wir noch die kritischen Werte von q_1 bestimmen.

$$\begin{aligned} q_1'(z) &= konst \cdot mz^{m-1}(1-z)^n - z^m n(1-z)^{n-1} \\ &= konst \cdot z^{m-1}(1-z)^{n-1}(m(1-z) - zn) \\ &= konst \cdot z^{m-1}(1-z)^{n-1}(m - (m+n)z) \end{aligned}$$

Als kritische Punkte kommen also $0, 1, \infty, x'$ in Frage, damit liegen die kritischen Werte von q_1 in $\{0, 1, \infty\}$.

Den gesuchten Morphismus q erhalten wir schließlich durch das Kompositum aus q_1 und q_2.

$$q := q_1 \circ q_2$$

□

Lemma 6.3.2 *Sei $S \subset \mathbb{Q} \cup \{\infty\}$ eine endliche Teilmenge. Es existiert ein nicht-konstanter Morphismus $q : \mathbb{P}^1_{\mathbb{C}} \longrightarrow \mathbb{P}^1_{\mathbb{C}}$, so daß $q(S) \subset \{0, 1, \infty\}$ und alle kritischen Werte von q in $\{0, 1, \infty\}$ liegen.*

Beweis per Induktion nach $n = \#S$

$n \leq 3$:
Wir wählen eine gebrochen-lineare Transformation q, die S nach $\{0, 1, \infty\}$ abbildet. (siehe Satz 4.2.1)

$n > 3$:
Wir können annehmen, daß $\{0, 1, \infty\} \subset S$ gilt. Sei $x \in S \setminus \{0, 1, \infty\}$ ein weiterer Punkt, dann existiert nach Lemma 6.3.1 ein nicht-konstanter Morphismus q_1, der $\{0, 1, \infty, x\}$ nach $\{0, 1, \infty\}$ abbildet und dessen kritische Werte in $\{0, 1, \infty\}$ liegen. Es gilt dann $\#q_1(S) < n$. Nach Induktionsvoraussetzung existiert ein nicht-konstanter Morphismus q_2, der $q_1(S)$ nach $\{0, 1, \infty\}$ abbildet und dessen kritische Werte in $\{0, 1, \infty\}$ liegen. $q := q_2 \circ q_1$ ist schließlich der gesuchte Morphismus.

□

7 Vorbereitungen II

7.1 Überlagerungstheorie

Eine zusammenhängende Mannigfaltigkeit ist ein zusammenhängender topologischer Raum, der lokal homöomorph zum $\mathbb{R}^n$ ist, d.h. eine n-dimensionale reelle C^0-Mannigfaltigkeit. Eine zusammenhängende Mannigfaltigkeit ist insbesondere wegweise und lokal wegweise zusammenhängend.

Definition 7.1.1 *Seien X und Y zusammenhängende Mannigfaltigkeiten. Eine stetige Abbildung $p : Y \longrightarrow X$ heißt* ***Überlagerung****, falls folgendes gilt:*

Jedes $x \in X$ hat eine offene Umgebung U, so daß sich $p^{-1}(U)$ als Vereinigung von paarweise disjunkten offenen Teilmengen $V_j \subset X$, wobei j ein Element aus einer Indexmenge J ist, darstellen läßt:

$$p^{-1}(U) = \bigcup_{j \in J} V_j$$

Zusätzlich sind für alle $j \in J$ die Einschränkungen $p_{|V_j} : V_j \longrightarrow U$ Homöomorphismen.
Sprechweise: *Y ist eine Überlagerung von X.*

Für $y_1, y_2 \in Y$ haben $p^{-1}(y_1)$ und $p^{-1}(y_2)$ die gleiche Mächtigkeit. Falls diese endlich ist, d.h. $\#p^{-1}(y_1) = n$ mit $n \in \mathbb{N}$, bezeichnet n den **Grad** von p. Insbesondere ist eine Überlagerung $p : Y \longrightarrow X$ surjektiv, da Y nicht-leer ist.[2]

Definition 7.1.2 *Seien X und Y zusammenhängende Mannigfaltigkeiten, und sei $p : Y \longrightarrow X$ eine Überlagerung. Dann heißt das Paar (Y, p) eine universelle Überlagerung von X, falls für jede Überlagerung $q : Z \longrightarrow X$, wobei Z eine zusammenhängende Mannigfaltigkeit ist, und jedes Paar $y \in Y$, $z \in Z$ mit $p(y) = q(z)$ genau eine Überlagerung $f : Y \longrightarrow Z$ existiert, so daß $f(y) = z$ und $q \circ f = p$ gilt, d.h. folgendes Diagramm kommutiert:*

$$\begin{tikzcd}
Y \arrow[rr, dotted, "f"] \arrow[dr, "p"'] & & Z \arrow[dl, "q"] \\
& X &
\end{tikzcd}$$

Aus der universellen Eigenschaft folgt, daß eine universelle Überlagerung bis auf Homöomorphie eindeutig ist.

Zu jeder zusammenhängenden Mannigfaltigkeit existiert eine zusammenhängende, einfach zusammenhängende Mannigfaltigkeit $\widetilde{X}$ mit einer Überlagerung $p : \widetilde{X} \longrightarrow X$. Nun ist jede einfach zusammenhängende Überlagerung eine universelle Überlagerung, also ist $(\widetilde{X}, p)$ eine universelle Überlagerung von X.[3]

[2] siehe Theorem 4.16 auf S.26 in [Fo]
[3] siehe Theorem 5.2, 5.3 auf S.32 in [Fo]

Definition 7.1.3 *Seien X und Y zusammenhängende Mannigfaltigkeiten, und sei $p : Y \longrightarrow X$ eine Überlagerung. Eine* ***Decktransformation*** *der Überlagerung p ist ein Homöomorphismus $f : Y \longrightarrow Y$, für den $p = p \circ f$ gilt.*

$$\begin{tikzcd} Y \arrow[rr, "f"] \arrow[dr, "p"'] & & Y \arrow[dl, "p"] \\ & X & \end{tikzcd}$$

Die Decktransformationen von p bilden eine Gruppe, diese bezeichnen wir mit $\mathrm{Aut}(p)$.

Theorem 7.1.4 *Sei $(\widetilde{X}, p)$ eine universelle Überlagerung von X, dann ist* $\mathrm{Aut}(p)$ *isomorph zur Fundamentalgruppe $\pi_1(X)$ von X.*

Beweis: Theorem 5.6 auf S.34 in [Fo]

Sei X eine zusammenhängende Mannigfaltigkeit und $(\widetilde{X}, p)$ eine universelle Überlagerung von X. Sei $q : Y \longrightarrow X$ eine weitere Überlagerung, wobei auch Y eine zusammenhängende Mannigfaltigkeit sei. Dann existiert eine Überlagerung $f : \widetilde{X} \longrightarrow Y$ mit $p = q \circ f$.

$$\begin{tikzcd} \widetilde{X} \arrow[rr, "f"] \arrow[dr, "p"'] & & Y \arrow[dl, "q"] \\ & X & \end{tikzcd}$$

$\widetilde{X}$ ist eine einfach zusammenhängende Überlagerung von Y, also eine universelle Überlagerung. $\mathrm{Aut}(f)$ ist eine Untergruppe von $\mathrm{Aut}(p)$, denn für $\varphi \in \mathrm{Aut}(f)$ gilt per Definition $f = f \circ \varphi$. Wegen $p = q \circ f$ erhalten wir

$$p = q \circ f = q \circ f \circ \varphi = p \circ \varphi$$

$\square$

Sei $(\widetilde{X}, p)$ eine universelle Überlagerung von X, dann existiert zu $x, y \in \widetilde{X}$ mit $p(x) = p(y)$ ein $f \in \mathrm{Aut}(p)$ mit $f(x) = y$, d.h. $\mathrm{Aut}(p)$ operiert transitiv auf den Fasern von p. Dies sieht man leicht, wenn man die universelle Eigenschaft von p gemäß Definition 7.1.2 ausnutzt, indem man $Y := \widetilde{X}$ und $Z := \widetilde{X}$ setzt. Wir nennen eine Überlagerung mit dieser Eigenschaft **galoissch**.

Wir führen auf $\widetilde{X}$ eine Äquivalenzrelation ein, indem wir zwei Punkte $x, y \in Y$ identifizieren, falls ein $\varphi \in \mathrm{Aut}(p)$ mit $\varphi(x) = y$ existiert. Den Quotientenraum bezeichnen wir mit $\widetilde{X}/\mathrm{Aut}(p)$. Nun gilt

$$p(x) = p(y) \Longleftrightarrow \exists \varphi \in \mathrm{Aut}(p) \colon \varphi(x) = y$$

Also induziert p eine bijektive Abbildung

$$\widetilde{p} : \widetilde{X}/\mathrm{Aut}(p) \longrightarrow X$$

Bemerkung 7.1.5 *$\widetilde{p}$ ist ein Homöomorphismus.*

Beweis:

$$\begin{tikzcd} \widetilde{X}/\operatorname{Aut}(p) \arrow[r, "\widetilde{p}"] & X \\ Y \arrow[u, "q"] \arrow[ur, "p"'] & \end{tikzcd}$$

Die Stetigkeit von $\widetilde{p}$ folgt aus der Finalität der Quotientenabbildung q. Es bleibt zu zeigen, daß $\widetilde{p}^{-1}$ stetig ist. Dazu zeigen wir, daß für jedes $\overline{x} \in \widetilde{X}/\operatorname{Aut}(p)$ das Bild einer Umgebung von $\overline{x}$ unter $\widetilde{p}$ eine Umgebung von $\widetilde{p}(x)$ ist. Sei nun $\overline{x} \in \widetilde{X}/\operatorname{Aut}(p)$, dann hat $p(x)$ eine Umgebung U, so daß $p^{-1}(U) = \bigcup_{j\in J} V_j$ disjunkte Vereinigung offener Mengen ist und die $p_{|V_j}$ Homöomorphismen sind. Nun liegt x in einem dieser V_j, daher fixieren wir von nun an dieses V_j.

Sei O eine Umgebung von $\overline{x}$ in $\widetilde{X}/\operatorname{Aut}(p)$, dann ist $q^{-1}(O)$ eine Umgebung von x, und $W := q^{-1}(O) \cap V_j$ ist ebenfalls eine Umgebung von x. $p(W)$ ist eine Umgebung von $p(x)$, da $p_{|V_j}$ ein Homöomorphismus ist und ist enthalten in $\widetilde{p}(O)$, damit ist $\widetilde{p}(O)$ eine Umgebung von $\widetilde{p}(\overline{x})$.

$\square$

Wir wissen nun:

Sei $(\widetilde{X}, p)$ eine universelle Überlagerung einer zusammenhängenden Mannigfaltigkeit X, dann gilt $\widetilde{X}/\operatorname{Aut}(p) \cong X$.

Definition 7.1.6 *Seien $p_1 : Y_1 \longrightarrow X$ und $p_2 : Y_1 \longrightarrow X$ Überlagerungen. (Y_1, p_1) und (Y_2, p_2) heißen homöomorph als Überlagerungen von X, falls ein Homöomorphismus $f : Y_1 \longrightarrow Y_2$ existiert, so daß $p_2 \circ f = p_1$ gilt.*

$$\begin{tikzcd} Y_1 \arrow[rr, "f"] \arrow[dr, "p_1"'] & & Y_2 \arrow[dl, "p_2"] \\ & X & \end{tikzcd}$$

Einfacher gesagt: Jedes $y_1 \in Y_1$, das über einem $x \in X$ liegt, wird unter f auf ein $y_2 \in Y_2$ abgebildet, das über x liegt.

Bemerkung 7.1.7 *Die soeben definierte Relation zwischen Überlagerungen ist eine Äquivalenzrelation.*

Denn: Für die Reflexivität setzt man $f := \mathrm{id}$, Transitivität erhält man durch komponieren. Für die Symmetrie formt man wie folgt um:

$$p_2 \circ f = p_1 = p_1 \circ f^{-1} \circ f \Longrightarrow p_2 = p_1 \circ f^{-1}$$

$\square$

Sei $(\widetilde{X}, p)$ eine universelle Überlagerung von X, und sei $q : Y \longrightarrow X$ eine weitere Überlagerung. Dann existiert eine Überlagerung $f : \widetilde{X} \longrightarrow Y$ mit $p = q \circ f$.

Seien $\overline{x}, \overline{y} \in \widetilde{X}/\operatorname{Aut}(f)$ mit $\overline{x} = \overline{y}$, dann gilt $f(x) = f(y)$ und wegen $p = q \circ f$ gilt auch $p(x) = p(y)$. Wir können folgende Abbildungen in naheliegender Weise repräsentantenweise definieren:

$$\begin{array}{rcl} \widetilde{p} : \widetilde{X}/\operatorname{Aut}(f) & \longrightarrow & X \\ \widetilde{f} : \widetilde{X}/\operatorname{Aut}(f) & \longrightarrow & Y \end{array}$$

Wegen Bemerkung 7.1.5 ist $\widetilde{f} : \widetilde{X}/\operatorname{Aut}(f) \longrightarrow Y$ ein Homöomorphismus, also ist $\widetilde{p} = q \circ \widetilde{f}$ eine Überlagerung, die homöomorph zu q ist.

Unser Resultat ist nun, daß jede Überlagerung von X homöomorph zu $\widetilde{X}/H$ ist, wobei H eine Untergruppe von $\operatorname{Aut}(p)$ ist.

Satz 7.1.8 *Sei $p : \widetilde{X} \longrightarrow X$ eine universelle Überlagerung von X, und sei $q : Y \longrightarrow X$ eine weitere Überlagerung vom Grad n. Dann existiert eine Überlagerung $f : \widetilde{X} \longrightarrow Y$ mit $p = q \circ f$.* $\operatorname{Aut}(f)$ *hat dann endlichen Index in* $\operatorname{Aut}(p)$, *und es gilt* $[\operatorname{Aut}(p) : \operatorname{Aut}(f)] = n$.

$$\begin{tikzcd} \widetilde{X} \arrow[rr, "f"] \arrow[dr, "p"'] & & Y \arrow[dl, "q"] \\ & X & \end{tikzcd}$$

Beweis:
Sei M die Menge der Überlagerungen $\varphi : \widetilde{X} \longrightarrow Y$, für die $p = q \circ \varphi$ gilt. $\operatorname{Aut}(p)$ operiert auf M via

$$\begin{array}{rcl} \operatorname{Aut}(p) \times M & \longrightarrow & M \\ (\tau, \varphi) & \longmapsto & \varphi \circ \tau \end{array}$$

Es gilt $f \in M$, der Stabilisator von f ist per Definition $\operatorname{Aut}(f)$. Die Operation ist transitiv, denn seien $\varphi_1, \varphi_2 \in M$, und sei $y \in Y$. Wähle $x_1 \in \varphi_1^{-1}(y)$ und $x_2 \in \varphi_2^{-1}(y)$, dann existiert ein $\tau \in \operatorname{Aut}(p)$ mit $\tau(x_1) = x_2$, da p galoissch ist. Es gilt $\varphi_2 \circ \tau(x_1) = \varphi_1(x_1)$, daraus folgt $\varphi_2 \circ \tau = \varphi_1$.

Sei $x \in \widetilde{X}$, dann existiert wegen der Universalität von p zu jedem $y \in q^{-1}(p(x))$ genau eine Überlagerung $\varphi : \widetilde{X} \longrightarrow Y$ mit $\varphi(x) = y$ und $p = q \circ \varphi$. Die Menge $q^{-1}(p(x))$ hat nach Voraussetzung genau n Elemente, damit hat auch M genau n Elemente.

Nun operiert $\operatorname{Aut}(p)$ transitiv auf M, also hat der Orbit von f genau n Elemente. Nach Bemerkung 5.3.1 gilt $[\operatorname{Aut}(p) : \operatorname{Aut}(f)] = n$.

$\square$

7.2 Riemannsche Flächen

Seien X und Y kompakte Riemannsche Flächen, und sei $f : X \longrightarrow Y$ eine nicht-konstante holomorphe Abbildung. Sei A die Menge der kritischen Punkte von f, dann ist A endlich und

$$f_{|A} : X \setminus A \longrightarrow Y \setminus f(A)$$

ist eine Überlagerung.[4] Wir nennen f eine **verzweigte holomorphe Überlagerung**.

Nun kommt eine fundamentale Tatsache aus der Theorie der Riemannsche Flächen, die wir später benötigen werden und deren Beweis nicht trivial ist:

Theorem 7.2.1 *Seien X, Y und Z kompakte Riemannsche Flächen und seien $\pi : Y \longrightarrow X$, $\tau : Z \longrightarrow X$ verzweigte holomorphe Überlagerungen. Sei $S \subset X$ eine endliche Teilmenge. Dann kann jede faser-erhaltende biholomorphe Abbildung*

$$\varphi : Y \setminus \pi^{-1}(S) \longrightarrow Z \setminus \tau^{-1}(S)$$

zu einer faser-erhaltenden biholomorphen Abbildung $\widetilde{\varphi} : Y \longrightarrow Z$, d.h. $\tau \circ \widetilde{\varphi} = \pi$, fortgesetzt werden.

Beweis: Theorem 8.5 auf S.52 in [Fo]

Sei X eine vollständige Kurve über $\mathbb{C}$, dann können wir diese als kompakte Riemannsche Fläche auffassen, und jeder Morphismus zwischen vollständigen Kurven gibt eine holomorphe Abbildung. Umgekehrt läßt sich jede kompakte Riemannsche Fläche als vollständige Kurve realisieren. Jede holomorphe Abbildung zwischen kompakten Riemannsche Flächen ist algebraisch, d.h. ein Morphismus zwischen vollständigen Kurven.

In naheliegender Weise können wir einer verzweigten Überlagerung einen **Grad** zuordnen. Der Körper der meromorphen Funktionen $\mathcal{M}(X)$ ist isomorph zum Körper der rationalen Funktionen $K(X)$. Aus dem folgenden Theorem folgt damit, daß uns ein endlicher Morphismus vom Grad d eine verzweigte holomorphe Überlagerung vom Grad d gibt.

Theorem 7.2.2 *Sei $\pi : Y \longrightarrow X$ eine holomorphe Überlagerung vom Grad d, dann induziert diese einen Körperhomomorphismus*

$$\begin{array}{rcl} \pi^* : \mathcal{M}(X) & \longrightarrow & \mathcal{M}(Y) \\ f & \longmapsto & f \circ \pi \end{array}$$

Die Körpererweiterung $\mathcal{M}(Y) : \mathcal{M}(X)$ ist eine algebraische Erweiterung vom Grad d.

Beweis: Theorem 8.3 auf S.50 in [Fo]

[4] siehe S.29 in [Fo]

8 Modulkörper

In diesem Abschnitt wird der Modulkörper eines endlichen Morphismus $t : X \longrightarrow \mathbb{P}^1_C$ definiert. Wir interessieren uns hauptsächlich für den Fall $C = \mathbb{C}$. Das Hauptresultat dieses Abschnitts wird sein, daß der Modulkörper eines Morphismus $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ein Zahlkörper ist, falls dessen kritische Werte in $\{0, 1, \infty\}$ liegen.

Zur Definition des Modulkörpers erinnere ich an die Definition 2.1.9.

Definition 8.0.3 *Sei X eine Varietät über C. Setze*

$$U(X) := \{\sigma \in \mathrm{Aut}(C) \mid X^\sigma \cong X\}$$

*Der Fixkörper $M(X) := C^{U(X)}$ heißt **absoluter Modulkörper** von X.*

8.1 Modulkörper eines endlichen Morphismus

Definition 8.1.1 *Sei $t : X \longrightarrow \mathbb{P}^1_C$ ein endlicher Morphismus zwischen Kurven über C. $U(X, t) \subset \mathrm{Aut}(C)$ besteht aus denjenigen Körperautomorphismen σ, für die ein Isomorphismus f_σ existiert, so daß folgendes Diagramm kommutiert.*

$$\begin{tikzcd} X^\sigma \arrow[r, "f_\sigma"] \arrow[d, "t^\sigma"'] & X \arrow[d, "t"] \\ (\mathbb{P}^1_C)^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"'] & \mathbb{P}^1_C \end{tikzcd}$$

*Der Fixkörper $M(X, t) := C^{U(X,t)}$ heißt **Modulkörper** von (X, t).*

Insbesondere gilt $U(X, t) \subset U(X)$.

8.2 Modulkörper im Komplexen

Sei X eine vollständige Kurve und $f : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ein endlicher Morphismus. f gibt uns eine verzweigte holomorphe Überlagerung. Sei $S \subset \mathbb{P}^1_{\mathbb{C}}$ die Menge der kritischen Werte von f, dann ist

$$t_S : X \setminus t^{-1}(S) \longrightarrow \mathbb{P}^1_{\mathbb{C}} \setminus S$$

wobei t_S die naheliegende Einschränkung von t sei, eine holomorphe Überlagerung. Der Grad der Überlagerung t_S stimmt mit dem Grad des endlichen Morphismus t überein.

Lemma 8.2.1 *Seien $t_1 : X_1 \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ und $t_2 : X_2 \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ endliche Morphismen zwischen vollständigen Kurven, und sei $S \subset \mathbb{P}^1_{\mathbb{C}}$ eine endliche Teilmenge, so daß die kritischen Werte von t_1 und t_2 in S enthalten sind. Dann sind t_1 und t_2 genau dann isomorph, wenn die zugeordneten holomorphen Überlagerungen t_{1S} und t_{2S} homöomorph sind.*

Beweis:
Der Übergang vom algebraischen zum analytischen ist funktoriell, also folgt aus t_1 isomorph zu t_2, daß t_{1S} und t_{2S} homöomorph sind.

Sei nun umgekehrt t_{1S} homöomorph zu t_{2S}, d.h. es existiert ein Homöomorphismus $f : X_1 \setminus t_1^{-1}(S) \longrightarrow X_2 \setminus t_2^{-1}(S)$ mit $t_{2S} \circ f = t_{1S}$. Nun sind t_{1S} und t_{2S} als Überlagerungen lokal biholomorphe Abbildungen. Daraus folgt, daß auch f lokal biholomorph ist, denn sei $x \in X_1 \setminus t_1^{-1}(S)$, dann hat $y := t_{1S}(x) \in \mathbb{P}^1_{\mathbb{C}} \setminus S$ gemäß Definition 7.1.1 Umgebungen U_1, U_2, so daß x eine Umgebung V_1 und $f(x)$ eine Umgebung V_2 hat mit $t_{1S|V_1} : V_1 \longrightarrow U_1$ und $t_{2S|V_2} : V_2 \longrightarrow U_2$ biholomorph. Wir können annehmen, daß $U := U_1 = U_2$ gilt, da wir ansonsten kleinere Umgebungen wählen können.

$$\begin{tikzcd} V_1 \arrow[rr, "f_{|V_1}"] \arrow[dr, "t_{1S|V_1}"'] & & V2 \arrow[dl, "t_{2S|V_2}"] \\ & U & \end{tikzcd}$$

Nun gilt $t_{2S|V_2} \circ f_{|V_1} = t_{1S|V_1}$, daraus folgt $f_{|V_1} = t_{1S|V_1} \circ t_{2S|V_2}^{-1}$. f ist lokal biholomorph und ein Homöomorphismus, also ist f biholomorph. Nach Theorem 7.2.1 existiert eine Fortsetzung $\widetilde{f} : X_1 \longrightarrow X_2$ von f, die faser-erhaltend, d.h. $t_2 \circ \widetilde{f} = t_1$, und biholomorph ist. Jede holomorphe Abbildung zwischen vollständigen Kurven ist algebraisch, also ist $\widetilde{f}$ der gesuchte Isomorphismus.

□

Lemma 8.2.2 *Sei $S \subset \mathbb{P}^1_{\mathbb{C}}$ eine endliche Teilmenge von abgeschlossenen Punkten und sei $d \geq 1$ eine natürliche Zahl. Dann existieren nur endlich viele Isomorphieklassen von Paaren (X, t), wobei X eine vollständige Kurve und $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ein endlicher Morphismus vom Grad d, dessen kritische Werte in S liegen, ist.*

Beweis:
Sei $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ein endlicher Morphismus, dessen kritische Werte in S liegen, dann erhalten wir eine holomorphe Überlagerung $t_S : X \setminus t^{-1}(S) \longrightarrow \mathbb{P}^1_{\mathbb{C}} \setminus S$. Wir ordnen nun jeder Isomorphieklasse (X, t) die Homöomorphieklasse $(X \setminus t^{-1}(S), t_S)$ zu. Diese Zuordnung ist nach Lemma 8.2.1 injektiv.

Nun ist zu zeigen, daß es nur endlich viele Homöomorphieklassen von Überlagerungen von $\mathbb{P}^1_{\mathbb{C}} \setminus S$ vom Grad d gibt. Sei $p : \widetilde{S} \longrightarrow \mathbb{P}^1_{\mathbb{C}} \setminus S$ eine universelle Überlagerung von $\mathbb{P}^1_{\mathbb{C}} \setminus S$, und sei $t : Y \longrightarrow \mathbb{P}^1_{\mathbb{C}} \setminus S$ eine Überlagerung von $\mathbb{P}^1_{\mathbb{C}} \setminus S$, dann ist die Überlagerung $\widetilde{S}/\operatorname{Aut}(t) \longrightarrow \mathbb{P}^1_{\mathbb{C}} \setminus S$ isomorph zu $t : Y \longrightarrow \mathbb{P}^1_{\mathbb{C}} \setminus S$. Nach Satz 7.1.8 stimmt der Grad der Überlagerung t mit dem Index von $\operatorname{Aut}(t)$ in $\operatorname{Aut}(p)$ überein. Wir interessieren uns nun für Überlagerungen vom Grad d, von denen es höchstens so viele Homöomorphieklassen gibt, wie $\operatorname{Aut}(p)$ Untergruppen vom Index d hat.

Nach Theorem 7.1.4 ist die Fundamentalgruppe $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus S)$ von $\mathbb{P}^1_{\mathbb{C}} \setminus S$ isomorph zu $\operatorname{Aut}(p)$. $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus S)$ ist eine endlich erzeugte freie Gruppe[5] vom

[5] siehe Aufgabe 5.7.A2 in [SZ]

Rang $\#S - 1$, nach Satz 5.3.2 hat diese nur endlich viele Untergruppen vom Index d.

$\square$

Lemma 8.2.3 *Sei X eine vollständige Kurve über $\mathbb{C}$, $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ein endlicher Morphismus und K ein Unterkörper von $\mathbb{C}$, so daß alle kritischen Werte von t K-rational sind. Dann ist die Körpererweiterung $M(X,t) : K$ endlich algebraisch.*

Beweis:
Sei $\sigma \in \mathrm{Aut}(\mathbb{C} : K)$, dann erhalten wir einen endlichen Morphismus

$$t(\sigma) := \mathrm{Proj}(\sigma) \circ t^\sigma$$

d.h. das folgende Diagramm kommutiert:

$$\begin{tikzcd} X^\sigma \arrow[d, "t^\sigma"'] \arrow[dr, "t(\sigma)"] & \\ {\mathbb{P}^1_{\mathbb{C}}}^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"'] & \mathbb{P}^1_{\mathbb{C}} \end{tikzcd}$$

$\mathrm{Proj}(\sigma)$ hat nach Bemerkung 3.2.2 keine kritischen Werte und ist ein endlicher Morphismus vom Grad 1. Nach Bemerkung 4.3.2 sind K-rationale Punkte invariant unter $\mathrm{Proj}(\sigma)$, also sind die kritischen Werte von $t(\sigma)$ die gleichen wie die von t. Sei d der Grad von t, dann hat $t(\sigma)$ ebenfalls den Grad d. Wir erhalten also eine Gruppenoperation von $\mathrm{Aut}(\mathbb{C} : K)$ auf den Isomorphieklassen.

t hat nach Folgerung 3.3.10 nur endlich viele kritische Punkte. Sei S die Menge der kritischen Werte von t, dann existieren nach Lemma 8.2.2 nur endlich viele Isomorphieklassen von endlichen Morphismen nach $\mathbb{P}^1_{\mathbb{C}}$ vom Grad d, deren kritische Werte in S liegen. Insbesondere ist der Orbit der Isomorphieklasse (X,t) unter der Operation von $\mathrm{Aut}(\mathbb{C} : K)$ endlich. Der Stabilisator von (X,t) hat nach Bemerkung 5.3.1 endlichen Index in $\mathrm{Aut}(\mathbb{C} : K)$. Nun besteht der Stabilisator von (X,t) aus denjenigen $\sigma \in \mathrm{Aut}(\mathbb{C} : K)$, für die ein Isomorphismus f_σ existiert, so daß folgendes Diagramm kommutiert:

$$\begin{tikzcd} X^\sigma \arrow[r, "f_\sigma"] \arrow[dr, "t(\sigma)"'] & X \arrow[d, "t"] \\ & \mathbb{P}^1_{\mathbb{C}} \end{tikzcd}$$

Wie man nun leicht sieht, gilt $\mathrm{Stab}(X,t) \subset U(X,t)$.[6] Insbesondere hat $U(X,t)$ damit endlichen Index in $\mathrm{Aut}(\mathbb{C} : K)$. Nach Satz 5.1.3 gilt $\mathbb{C}^{\mathrm{Aut}(\mathbb{C}/K)} = K$, und nach Lemma 5.2.5 ist die Körpererweiterung $\mathbb{C}^{U(X,t)} : \mathbb{C}^{\mathrm{Aut}(\mathbb{C}/K)}$ endlich algebraisch.

[6] siehe Definition 8.1.1

□

Nun kommen wir zu unserem Hauptresultat, das ein Spezialfall von Lemma 8.2.3 ist: Inbesondere ist $M(X,t)$ eine endliche Erweiterung von $\mathbb{Q}$, also ein Zahlkörper, falls die kritischen Werte von t in $\{0,1,\infty\}$ liegen.

Als nächstes suchen wir eine Abschätzung für den Grad der Körpererweiterung $M(X,t) : \mathbb{Q}$. Sei G eine freie Gruppe vom Rang 2, dann berechnet sich die Anzahl M_d der Untergruppen vom Index d nach Satz 5.3.3 mit der folgenden Rekursionsformel:

$$\begin{aligned} M_1 &= 1 \\ M_d &= d(d!) - \sum_{i=1}^{d-1} (d-i)! M_i \end{aligned}$$

Bemerkung 8.2.4 *Sei X eine vollständige Kurve über $\mathbb{C}$, $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ein endlicher Morphismus vom Grad d, dessen kritische Werte in $\{0,1,\infty\}$ liegen. Dann gilt*

$$[M(X,t) : \mathbb{Q}] \leq M_d$$

Der Beweis greift auf Einzelheiten der Beweise von Lemma 8.2.2 und Lemma 8.2.3 zurück.

Beweis:
$\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\})$ ist eine freie Gruppe vom Rang 2. Es gibt höchstens so viele Homöomorphieklassen von Überlagerungen von $\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\}$ vom Grad d, wie $\pi_1(\mathbb{P}^1_{\mathbb{C}} \setminus \{0,1,\infty\})$ Untergruppen vom Index d hat. Insbesondere hat der Orbit von (X,t) unter der Operation von $\mathrm{Aut}(\mathbb{C} : \mathbb{Q})$ höchstens M_d Elemente. Es gilt $\mathrm{Stab}(X,t) = U(X,t)$, wie man leicht sieht, damit ist der Index von $U(X,t)$ in $\mathrm{Aut}(\mathbb{C} : \mathbb{Q})$ nach Bemerkung 5.3.1 höchstens M_d. Nach Lemma 5.2.5 gilt

$$[M(X,t) : \mathbb{Q}] \leq [\mathrm{Aut}(\mathbb{C} : \mathbb{Q}) : U(X,t)] \leq M_d$$

□

9 Vorbereitungen III

9.1 Verzweigung

Sei X eine Kurve über C, dann ist für jeden abgeschlossenen Punkt $x \in X$ der lokale Ring $\mathcal{O}_{X,x}$ ein diskreter Bewertungsring. Sei $K(X)$ der Körper der rationalen Funktionen auf X, dann gilt $K(X) \cong Q(\mathcal{O}_{X,x})$. Im Folgenden fasse ich $\mathcal{O}_{X,x}$ als Unterring von $K(X)$ auf. Es existiert eine Bewertung v_x auf $K(X)$ mit $v_x(c) = 0$ für alle $c \in C$, so daß

$$\mathcal{O}_{X,x} = \{f \in K(X) \mid v_x(f) \geq 0\} \cup \{0\}$$

gilt. Sei $\mathfrak{m}_x$ das maximale Ideal von $\mathcal{O}_{X,x}$, dann gilt

$$\mathfrak{m}_x = \{f \in K(X) \mid v_x(f) > 0\} \cup \{0\}$$

Sei $t \in \mathfrak{m}_x \setminus \mathfrak{m}_x^2$, dann wird $\mathfrak{m}_x$ nach Lemma 3.2.4 von t erzeugt. Für $0 \neq f \in \mathfrak{m}_x$ existiert ein $g \in \mathcal{O}_{X,x}$, so daß $f = g \cdot t$ gilt. Per Definition einer diskreten Bewertung gilt $v_x(f) = v_x(g) + v_x(t)$. Da das für alle $0 \neq f \in \mathfrak{m}_x$ gilt, muß $v_x(t) = 1$ gelten. Ein solches t heißt **lokaler Parameter** in x.

$\mathfrak{m}_x^n$ wird von t^n erzeugt, für $f \in \mathcal{O}_{X,x} \setminus \{0\}$ gilt $v_x(f) = \max\{n \in \mathbb{N} \mid f \in \mathfrak{m}_x^n\}$. Wir nennen $v_x(f)$ die **Nullstellenordnung** von f in x. Sei nun $f \in K(X) \setminus \{0\}$, dann existieren $a, b \in \mathcal{O}_{X,x} \setminus \{0\}$, so daß $f = \frac{a}{b}$ gilt. Es gilt

$$v_x(f) = v_x(a) - v_x(b)$$

Wir nennen $\operatorname{ord}_x(f) := v_x(f)$ die **Ordnung** von f in x und sagen, daß f einen **Pol** in x hat, falls $\operatorname{ord}_x(f) < 0$ gilt, in diesem Fall ist $-\operatorname{ord}_x(f)$ die **Polordnung**.

Definition 9.1.1 *Seien X und Y vollständige Kurven über C, und sei $f : X \longrightarrow Y$ ein endlicher Morphismus. Sei $P \in X$ ein abgeschlossener Punkt, dann induziert f einen lokalen C-Algebrenhomomorphismus*

$$\varphi : \mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$$

Sei $t \in \mathcal{O}_{Y,f(P)}$ ein lokaler Parameter in $f(P)$. $\mathcal{O}_{X,P}$ ist ein diskreter Bewertungsring, sei v_P die zugehörige Bewertung, dann heißt

$$e_P := v_P(\varphi(t))$$

*der **Verzweigungsindex** von f in P. f heißt verzweigt in P, falls $e_P > 1$ gilt, und unverzweigt in P, falls $e_P = 1$ gilt.*

e_P ist wohldefiniert, da φ injektiv ist, also insbesondere $\varphi(t) \neq 0$ gilt.

Bemerkung 9.1.2 *f ist genau dann in P verzweigt, wenn P ein kritischer Punkt von f ist.*

Beweis:
Sei $\varphi : \mathcal{O}_{Y,f(P)} \longrightarrow \mathcal{O}_{X,P}$ der durch f induzierte lokale Ringhomomorphismus, und sei $t \in \mathcal{O}_{Y,f(P)}$ ein lokaler Parameter $f(P)$. Zu zeigen: $e_P > 1$ gilt genau dann, wenn die Cotangentialabbildung $\widetilde{\varphi} : \mathfrak{m}_{f(P)}/\mathfrak{m}^2_{f(P)} \longrightarrow \mathfrak{m}_P/\mathfrak{m}^2_P$ die Nullabbildung ist. (siehe Definition 3.2.1)

Nun ist $e_P > 1$ äquivalent zu $\varphi(t) \in \mathfrak{m}^2_P$. Das wiederum ist äquivalent dazu, daß $\widetilde{\varphi}$ die Nullabbildung ist.

□

Bemerkung 9.1.3 *Seien X, Y und Z Kurven über C und seien $f : X \longrightarrow Y$ und $g : Y \longrightarrow Z$ endliche Morphismen von C-Varietäten. Ist $P \in X$ ein abgeschlossener Punkt, dann ist der Verzweigungsindex von $g \circ f$ in P das Produkt der Verzweigungsindizes von f in P und von g in $f(P)$.*

Dies sieht man leicht, wenn man die lokalen Ringhomomorphismen komponiert.

□

Der folgende Satz ist ein Resultat, das wir bereits aus der Theorie der Riemannschen Flächen kennen:

Eine nicht-konstante meromorphe Funktion auf einer kompakten Riemannschen Fläche nimmt jeden Wert mit Vielfachheiten gleich oft an.

Satz 9.1.4 *Sei $f : X \longrightarrow Y$ ein endlicher Morphismus zwischen Kurven über C vom Grad n. Sei $Q \in Y$ ein abgeschlossener Punkt, dann gilt*

$$\sum_{P \in f^{-1}(Q)} e_P = n$$

e_P bezeichnet den Verzweigungsindex von f im Punkt P.

Ein endlicher Morphismus vom Grad n nimmt also jeden Wert mit Vielfachheiten genau n-mal an. Falls Q kein kritischer Wert von f ist, hat Q genau n Urbilder (siehe Bemerkung 9.1.2). Wir folgern weiterhin, daß der Grad eines endlichen Morphismus eine obere Schranke für den Verzweigungsindex in einem Punkt ist, d.h. $e_P \leq n$.

Definition 9.1.5 *Sei $f : X \longrightarrow Y$ ein endlicher Morphismus zwischen Kurven über C vom Grad n. Sei $P \in X$ ein abgeschlossener Punkt, dann heißt f in P* ***total verzweigt****, falls $e_P = n$ gilt.*

9.2 Satz von Riemann-Roch

Das Ziel von diesem Abschnitt ist, zu einer gegebenen vollständigen Kurve X und einem abgeschlossenen Punkt P eine nicht-konstante rationale Funktion zu finden, die ihren einzigen Pol im Punkt P hat.

Definition 9.2.1 *Sei X eine Kurve über C und $\widetilde{X} \subset X$ die Menge aller abgeschlossenen Punkte von X. Sei*

$$\operatorname{Div}(X) := \bigoplus_{x \in \widetilde{X}} \mathbb{Z}$$

die von den Elementen aus $\widetilde{X}$ erzeugte freie abelsche Gruppe. Ein ***Divisor*** *auf X ist dann ein Element aus* $\operatorname{Div}(X)$.

Ein Divisor D auf X ist also eine formale endliche Linearkombination von abgeschlossen Punkten, d.h.

$$D = \sum_{x \in \widetilde{X}} n_x \cdot x$$

mit $n_x \in \mathbb{Z}$ und $n_x \neq 0$ für endlich viele $x \in \widetilde{X}$. Seien $D = \sum n_x \cdot x$ und $D' = \sum n'_x \cdot x$ zwei Divisoren auf X. Wir setzen

$$D \leq D' :\Longleftrightarrow n_x \leq n'_x \text{ für alle } x \in \widetilde{X}$$

Wir erhalten damit eine partielle Ordnungrelation auf $\operatorname{Div}(X)$.

Sei $f \in K(X)$ eine rationale Funktion, dann gilt $\operatorname{ord}_x(f) \neq 0$ für endlich viele $x \in \widetilde{X}$. Wir erhalten also einen Divisor (f) auf X:

$$(f) := \sum_{x \in \widetilde{X}} \operatorname{ord}_x(f) \cdot x$$

Ein Divisor der Form (f) heißt **Hauptdivisor**.

Definition 9.2.2 *Sei D ein Divisor auf X. Dann bezeichnet*

$$\deg(D) := \sum_{x \in \widetilde{X}} n_x$$

den ***Grad*** *von D.*

Bemerkung 9.2.3 *Sei X eine vollständige Kurve, und sei D ein Hauptdivisor auf X, dann gilt* $\deg D = 0$.

Definition 9.2.4 *Sei X eine vollständige Kurve, dann ist der C-Vektorraum $\Omega_{X/\operatorname{Spec} C}$ endlich-dimensional. Die natürliche Zahl*

$$g := \dim_C \Omega_{X/\operatorname{Spec} C}$$

heißt das ***Geschlecht*** *von X.*

Der folgende Satz ist eine Abschätzung, die direkt aus dem Satz von Riemann-Roch folgt.

Satz 9.2.5 *Sei X eine vollständige Kurve vom Geschlecht g, und sei D ein Divisor auf X. Setze*

$$L(D) := \{f \in K(X) \mid (f) + D \geq 0\}$$

dann ist $L(D)$ ein endlich-dimensionaler C-Vektorraum und es gilt

$$\dim_C L(D) \geq \deg(D) + 1 - g$$

□

Nun können wir unser Hauptresultat formulieren:

Folgerung 9.2.6 *Sei X eine vollständige Kurve vom Geschlecht g, und sei $P \in X$ ein abgeschlossener Punkt. Dann existiert eine nicht-konstante rationale Funktion $z \in K(X) \setminus C$, die P als einzigen Pol, wobei die Polordnung in P höchstens $g + 1$ ist, hat. Das heißt*

$$\mathrm{ord}_P(z) \geq -(g+1)$$

und für einen abgeschlossenen Punkt $Q \in X$ gilt

$$\mathrm{ord}_Q(z) \geq 0$$

Beweis:
Setze $D := (g+1) \cdot P$, dann gilt $\deg(D) = g + 1$. Aus Satz 9.2.5 folgt

$$\dim_C L(D) \geq (g+1) + 1 - g = 2$$

Also existiert ein $z \in K(X) \setminus C$ mit $(f) \geq -D$.

□

10 Definitionskörper

Im Folgenden ist C ein algebraisch abgeschlossener Körper. In diesem Abschnitt werden wir sehen, daß für einen Morphismus $t : X \longrightarrow \mathbb{P}^1_C$ die Kurve X und der Morphismus t über einer endlichen Erweiterung des Modulkörpers definiert sind.

Für den Beweis des Satzes von Belyi benötigen wir den Spezialfall $C = \mathbb{C}$.

Definition 10.0.7 *Sei $t : X \longrightarrow \mathbb{P}^1_C$ ein endlicher Morphismus, und sei $P \in X$ ein abgeschlossener Punkt. $U(X,t,P)$ bezeichnet diejenigen Körperautomorphismen $\sigma \in \mathrm{Aut}(C)$, für die ein Isomorphismus $f_\sigma : X \longrightarrow X$ existiert, so daß $f_\sigma(P) = P$ gilt und folgendes Diagramm kommutiert.*

$$\begin{tikzcd} X^\sigma \arrow[r, "f_\sigma"] \arrow[d, "t^\sigma"'] & X \arrow[d, "t"] \\ (\mathbb{P}^1_C)^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"] & \mathbb{P}^1_C \end{tikzcd}$$

Ich erinnere daran, daß die zugrundeliegenden Schemata von X und X^σ identisch sind. Auch die Morphismen t und t^σ sind als Morphismen zwischen Schemata identisch.

Insbesondere gilt $U(X,t,P) \subset U(X,t)$[7]. Den Fixkörper von $U(X,t,P)$ bezeichnen wir mit $M(X,t,P)$.

Bemerkung 10.0.8 *Für $\sigma \in U(X,t,P)$ ist f_σ sogar eindeutig bestimmt.*

Denn: Sei g_σ ein weiterer Isomorphismus mit den beiden Eigenschaften von f_σ. Dann gilt $f_\sigma \circ g_\sigma^{-1}(P) = P$ und $g_\sigma^{-1} \circ f_\sigma(P) = P$.

$$\begin{tikzcd} X \arrow[r, "g_\sigma^{-1}"] \arrow[d, "t"] & X^\sigma \arrow[r, "f_\sigma"] \arrow[d, "t^\sigma"] & X \arrow[d, "t"] \\ \mathbb{P}^1_C \arrow[r, "\mathrm{Proj}(\sigma)^{-1}"] & (\mathbb{P}^1_C)^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"] & \mathbb{P}^1_C \end{tikzcd} \qquad \begin{tikzcd} X \arrow[rr, "f_\sigma \circ g_\sigma^{-1}"] \arrow[dr, "t"'] & & X \arrow[dl, "t"] \\ & \mathbb{P}^1_C & \end{tikzcd}$$

Nach Lemma 2.2.4 gilt $f_\sigma \circ g_\sigma^{-1} = \mathrm{id}$ und $g_\sigma^{-1} \circ f_\sigma = \mathrm{id}$, daraus folgt $g_\sigma = f_\sigma$.

□

Bemerkung 10.0.9 *Sei $\sigma \in U(X,t,P)$, dann induziert das eindeutig gegebene f_σ einen Körperautomorphsimus $f_\sigma^* : K(X) \longrightarrow K(X)$. Insbesondere kommutiert das folgende Diagramm:*

$$\begin{tikzcd} K(X) & K(X) \arrow[l, "f_\sigma^*"'] \\ C(T) \arrow[u, "t^*"] & C(T) \arrow[l, "\sigma"] \arrow[u, "t^*"'] \end{tikzcd}$$

[7]siehe Definition 8.1.1

Wir erhalten also eine Gruppenoperation von $U(X,t,P)$ auf $K(X)$.

Lemma 10.0.10 *Sei $t : X \longrightarrow \mathbb{P}^1_C$ ein endlicher Morphismus, und sei $Q \in \mathbb{P}^1_C$ ein $\mathbb{Q}$-rationaler Punkt. Sei $P \in t^{-1}(Q)$, dann ist die Körpererweiterung $M(X,t,P) : M(X,t)$ endlich algebraisch.*

Beweis:
Sei $\sigma \in U(X,t)$. Q ist $\mathbb{Q}$-rational, also ist Q nach Bemerkung 4.3.2 invariant unter $\mathrm{Proj}(\sigma)$. Zu σ existiert ein Morphismus $f_\sigma : X^\sigma \longrightarrow X$, so daß das Diagramm

$$\begin{tikzcd} X^\sigma \arrow[r, "f_\sigma"] \arrow[d, "t^\sigma"'] & X \arrow[d, "t"] \\ (\mathbb{P}^1_C)^\sigma \arrow[r, "\mathrm{Proj}(\sigma)"'] & \mathbb{P}^1_C \end{tikzcd}$$

kommutiert, damit ist $t^{-1}(Q)$ invariant unter f_σ. Ich erinnere daran, daß die Morphismen t und t^σ als Morphismen zwischen Schemata identisch sind.

Wir betrachten den Quotienten $t^{-1}(Q)/\operatorname{Aut}(t)$, wobei wir zwei Punkte P_1 und P_2 aus der Faser von Q identifizieren, falls ein $\varphi \in \operatorname{Aut}(t)$ existiert, so daß $\varphi(P_1) = P_2$ gilt. $U(X,t)$ operiert auf $t^{-1}(Q)/\operatorname{Aut}(t)$ via

$$\begin{array}{ccc} U(X,t) \times t^{-1}(Q)/\operatorname{Aut}(t) & \longrightarrow & t^{-1}(Q)/\operatorname{Aut}(t) \\ (\sigma, \overline{P}) & \longmapsto & \overline{f_\sigma(P)} \end{array}$$

Diese Definition ist unabhängig von der Wahl von P und f_σ, denn sei $\overline{P}_1 = \overline{P}_2$ und seien f_σ und g_σ gemäß der Definition von $U(X,t)$ gewählt. Es existiert ein $r \in \operatorname{Aut}(t)$ mit $r(P_1) = P_2$. Setze $s := g_\sigma \circ r \circ f_\sigma^{-1}$, dann ist s ein Isomorphismus. Zu zeigen ist $s \in \operatorname{Aut}(t)$ und $s(f_\sigma(P_1)) = g_\sigma(P_2)$, damit wäre die Wohldefiniertheit gezeigt. In den folgenden Umformungen werde ich nicht zwischen t und t^σ unterscheiden.

$$\begin{aligned} t \circ s &= t \circ (g_\sigma \circ r \circ f_\sigma^{-1}) \\ &= (t \circ g_\sigma) \circ r \circ f_\sigma^{-1} \\ &= (\mathrm{Proj}(\sigma) \circ t) \circ r \circ f_\sigma^{-1} \\ &= \mathrm{Proj}(\sigma) \circ (t \circ r) \circ f_\sigma^{-1} \\ &= \mathrm{Proj}(\sigma) \circ t \circ f_\sigma^{-1} \\ &= t \end{aligned}$$

Damit ist $s \in \operatorname{Aut}(t)$ gezeigt. Es fehlt noch $s(f_\sigma(P_1)) = g_\sigma(P_2)$.

$$s \circ f_\sigma(P_1) = (g_\sigma \circ r \circ f_\sigma^{-1}) \circ f_\sigma(P_1) = g_\sigma \circ r(P_1) = g_\sigma(P_2)$$

Damit ist die Wohldefiniertheit gezeigt. Man sieht leicht, daß wir eine Gruppenoperation erhalten haben.

$U(X,t,P)$ ist der Stabilisator von $\overline{P}$, denn: Jedes Element aus $U(X,t,P)$ läßt insbesondere $\overline{P}$ invariant. Sei nun $\sigma \in \operatorname{Stab}(\overline{P})$ dann steht P in relation mit $f_\sigma(P)$, d.h. es existiert $r \in \mathrm{Aut}(t)$ mit $r(f_\sigma(P)) = P$. $g_\sigma := r \circ f_\sigma$ ist dann der gesuchte Isomorphismus, d.h. $g_\sigma(P) = P$. Damit gilt $U(X,t,P) = \mathrm{Stab}(\overline{P})$. Nach Bemerkung 5.3.1 hat $U(X,t,P)$ endlichen Index in $U(X,t)$, und nach Lemma 5.2.5 ist die Körpererweiterung $M(X,t,P) : M(X,t)$ endlich algebraisch.

$\square$

Lemma 10.0.11 *Sei $P \in X$ ein abgeschlossener Punkt und $s \in \mathcal{O}_{X,P}$ ein lokaler Paramter. Sei $f \in K(X)$ mit $n := -\mathrm{ord}_P(f) \geq 1$, d.h. f hat einen Pol der Ordnung n in P. Dann hat f eine eindeutige Darstellung*

$$f = \frac{a_{-n}}{s^n} + \frac{a_{-(n-1)}}{s^{n-1}} + \ldots + a_o + r$$

mit $a_{-n}, \ldots, a_0 \in C$ und $r \in \mathfrak{m}_P$.

Beweis:
Es gilt $K(X) = Q(\mathcal{O}_{X,P})$, also hat f eine Darstellung $f = \frac{a}{b}$ mit $a, b \in \mathcal{O}_{X,P}$. Wir können annehmen, daß der Bruch soweit gekürzt ist, daß $v_p(a) = 0$ und $v_P(b) = n$ gilt. Außerdem können wir annehmen, daß der Bruch mit einer Einheit erweitert wurde, so daß $b = s^n$ gilt. Wir erhalten damit $f = \frac{a}{s^n}$ mit $a \in \mathcal{O}_{X,P}$.

Nach Lemma 3.1.3 hat a eine eindeutige Darstellung $a = a_{-n} + b$ mit $a_{-n} \in C$ und $b \in \mathfrak{m}_P$. Wir erhalten $f = \frac{a_{-n}}{s^n} + \frac{b}{s^n}$. Wegen $v_p(b) > 0$ gilt $-\mathrm{ord}_P(\frac{b}{s^n}) < n$, also hat f eine eindeutige Darstellung $f = \frac{a_{-n}}{s^n} + f'$ mit $-\mathrm{ord}_P(f') < n$. Diese Zerlegung führen wir mit f' erneut durch, bis schließlich $v_p(f') > 0$ gilt, d.h. $f' \in \mathfrak{m}_P$.

$\square$

Theorem 10.0.12 *Sei $t : X \longrightarrow \mathbb{P}^1_C$ ein endlicher Morphismus, dann sind X und t über einer endlichen Erweiterung von $M(X,t)$ definiert.*

Der Funktionenkörper von $\mathbb{P}^1_{\mathbb{C}}$ ist isomorph zum Körper der rationalen Funktionen in einer Veränderlichen $C(T)$. Sei $K(X)$ der Funktionenkörper von X, dann induziert $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ einen Körperhomomorphismus $t^* : C(T) \longrightarrow K(X)$.

Nach Folgerung 3.3.10 ist die Menge der kritischen Werte von t endlich, wir wählen einen $\mathbb{Q}$-rationalen Punkt $Q \in \mathbb{P}^1_{\mathbb{C}}$, der kein kritischer Wert von t ist. Wir wählen ein $P \in t^{-1}(Q)$, dann ist P kein kritischer Punkt von t und nach Bemerkung 9.1.2 ist t unverzweigt in P.

Nach Folgerung 9.2.6 existiert eine nicht-konstante rationale Funktion $\mathfrak{z} \in K(X) \setminus C$, so daß P der einzige Pol von $\mathfrak{z}$ ist. Wir wählen $\mathfrak{z}$ so, daß die Polordnung $n := -\mathrm{ord}_P(\mathfrak{z})$ im Punkt P minimal ist.

Nach Bemerkung 4.3.3 können wir einen lokalen Parameter $r \in \mathfrak{m}_Q$ so wählen, daß r invariant unter $\mathrm{Aut}(C)$, also insbesondere invariant unter $U(X,t,P)$ ist. Sei φ der durch t induzierte lokale Ringhomomorphismus im Punkt P, dann ist $s := \varphi(r) \in \mathfrak{m}_P$ ebenfalls invariant unter $U(X,t,P)$, wie man anhand des

Diagramms aus Bemerkung 10.0.9 erkennen kann. Nach Lemma 10.0.11 hat $\mathfrak{z}$ eine eindeutige Darstellung

$$\mathfrak{z} = \frac{a_{-n}}{s^n} + \frac{a_{-(n-1)}}{s^{n-1}} + \ldots + a_o + r \text{ mit } r \in \mathfrak{m}_p$$

Setze $\mathfrak{z}' := \frac{1}{a_{-n}} \cdot \mathfrak{z} - \frac{a_0}{a_{-n}}$. Seien a'_i die Koeffizienten von $\mathfrak{z}'$, dann gilt $a'_{-n} = 1$ und $a'_0 = 0$.

$\mathfrak{z}'$ ist damit eindeutig bestimmt, denn sei $\mathfrak{z}'' \in K(X)$, so daß P der einzige Pol von $\mathfrak{z}''$ ist, wobei die Polordnung minimal ist und $a''_{-n} = 1$, $a''_0 = 0$ gilt. Dann hat $\mathfrak{z}' - \mathfrak{z}''$ keinen Pol $n-ter$ Ordnung in P und ist wegen der Minimalität von n damit konstant. Nun gilt $\mathfrak{z}' - \mathfrak{z}'' \in \mathfrak{m}_p \cap C$, also $\mathfrak{z}' - \mathfrak{z}'' = 0$. Von nun an nehmen wir an, daß $\mathfrak{z}$ diese Eigenschaften hat, d.h. es gilt $\mathfrak{z} = \mathfrak{z}'$.

Der durch den Körperhomomorphismus

$$\begin{array}{rcl} z^* : C(T) & \longrightarrow & K(X) \\ T & \longmapsto & z \end{array}$$

induzierte Morphismus z ist nach Satz 9.1.4 in P total verzweigt. Setze $\mathfrak{t} := t^*(T) \in K(X) \setminus C$, dann gilt $C(\mathfrak{t}, \mathfrak{z}) \cong K(X)$. Um das zu sehen, zeigen wir, daß die Körpererweiterung $K(X) : C(\mathfrak{t}, \mathfrak{z})$ Grad 1 hat. Es existiert eine Kurve Y über C, so daß $C(\mathfrak{t}, \mathfrak{z}) \cong K(Y)$ gilt. Die Inklusion $\pi^* : C(\mathfrak{t}, \mathfrak{z}) \hookrightarrow K(X)$ induziert einen endlichen Morphismus $\pi : X \longrightarrow Y$. Wir erhalten insgesamt folgendes kommutative Diagramm:

$$\begin{tikzcd}
\mathbb{P}^1_C & & \\
& Y \arrow[ul] \arrow[dl] & X \arrow[l, "\pi"'] \arrow[ull, "t"'] \arrow[dll, "z"] \\
\mathbb{P}^1_C & &
\end{tikzcd}$$

Nach Bemerkung 9.1.3 multiplizieren sich die Verzweigungsindizes beim Kompositum. t ist unverzweigt in P, d.h. der Verzweigungsindex in P ist 1. Der Verzweigungsindex von π in P ist damit ebenfalls 1. z ist total verzweigt in P, d.h. der Verzweigungsindex in P stimmt mit dem Grad von z überein. Da sich die Grade von endlichen Morphismen zwischen vollständigen Kurven ebenfalls multiplizieren, ist auch π in P total verzweigt. Damit hat π Grad 1 und es gilt $[K(X) : K(Y)] = 1$.

Der lokale Parameter s aus $\mathcal{O}_{X,P}$ wurde so gewählt, daß er invariant unter $U(X,t,P)$ ist. $\sigma \in U(X,t,P)$ induziert einen lokalen Ringisomorphismus $\mathcal{O}_{X,P} \longrightarrow \mathcal{O}_{X,P}$, es gilt $v_P(\mathfrak{z}) = v_P(\sigma(\mathfrak{z}))$. In Punkten $\neq P$ ist die Bewertung größer gleich 0, also hat $\sigma(\mathfrak{z})$ einen Pol minimaler Ordnung in P als einzigen Pol. Seien a_i die Koeffizienten von $\sigma(\mathfrak{z})$, dann gilt $a_{-n} = 1$ und $a_0 = 0$. Wir hatten vorher gesehen, daß $\mathfrak{z}$ mit diesen Eigenschaften eindeutig bestimmt ist, also gilt $\sigma(\mathfrak{z}) = \mathfrak{z}$. Wir wissen nun, daß $\mathfrak{z}$ invariant unter $U(X,t,P)$ ist. $\mathfrak{t}$ ist per Konstruktion ebenfalls invariant unter $U(X,t,P)$[8], d.h. $\mathfrak{t}, \mathfrak{z} \in K(X)^{U(X,t,P)}$.

Setze $k := M(X,t,P)$. Es gilt $C(\mathfrak{t})^{U(X,t,P)} = k(\mathfrak{t})$. $\mathfrak{z}$ ist algebraisch über $k(\mathfrak{t})$, denn $\mathfrak{z}$ hat ein normiertes Minimalpolynom $m_{\mathfrak{z}} = \sum a_i X^i \in C(\mathfrak{t})[X]$. Für $\sigma \in U(X,t,P)$ gilt $\sigma(m_{\mathfrak{z}})(\mathfrak{z}) = \sum \sigma(a_i)\mathfrak{z}^i = \sigma(\sum a_i \mathfrak{z}^i) = \sigma(m_{\mathfrak{z}}(\mathfrak{z})) = 0$. Also ist $\sigma(m_{\mathfrak{z}})$ auch ein normiertes Minimalpolynom von $\mathfrak{z}$ und damit gilt wegen der Eindeutigkeit des Minimalpolynoms $m_{\mathfrak{z}} = \sigma(m_{\mathfrak{z}})$. Daraus folgt $m_{\mathfrak{z}} \in k(\mathfrak{t})[X]$.

Wir betrachten den Integritätsring $C[\mathfrak{t}, \mathfrak{z}] \cong C[X_1, X_2]/(m_{\mathfrak{z}})$. Dann ist $k[\mathfrak{t}, \mathfrak{z}]$ ebenfalls ein Integritätsring und es gilt $k[\mathfrak{t}, \mathfrak{z}] \otimes_k C \cong C[\mathfrak{t}, \mathfrak{z}]$. Damit ist die affine Kurve $\operatorname{Spec} C[\mathfrak{t}, \mathfrak{z}]$ über k definiert, $K(X)$ ist birational äquivalent zu dieser, also ist $K(X)$ über k definiert. t wird von dem Körperhomomorphismus t^* induziert, dieser wird wiederum von dem Körperhomomorphismus $k(T) \longrightarrow k(\mathfrak{t}, \mathfrak{z})$ induziert. Nach Lemma 10.0.10 ist die Körpererweiterung $k : M(X,t)$ endlich algebraisch.

□

Als nächstes suchen wir eine Abschätzung für den Grad der Körpererweiterung $k : M(X,t)$. Dazu betrachten wir die Beweise von Lemma 10.0.10 und Theorem 10.0.12.

Bemerkung 10.0.13 *Sei d der Grad von t, und sei a die Anzahl der Elemente in* $\operatorname{Aut}(t)$*, dann gilt* $[M(X,t,P) : M(X,t)] \leq \frac{d}{a}$.

Beweis:
Die Faser $t^{-1}(Q)$ hat nach Satz 9.1.4 genau d Elemente, da Q im Beweis von Theorem 10.0.12 so gewählt wurde, daß Q kein kritischer Wert von t ist. Wir betrachten nun $t^{-1}(Q)/\operatorname{Aut}(t)$. Sei $P \in t^{-1}(Q)$, dann gilt nach Lemma 2.2.4 genau dann $f(P) = P$ für $f \in \operatorname{Aut}(t)$, wenn $f = \mathrm{id}$ gilt. Nach dem Burnside Lemma hat $t^{-1}(Q)/\operatorname{Aut}(t)$ dann genau $\frac{d}{a}$ Elemente. $U(X,t)$ operiert auf $t^{-1}(Q)/\operatorname{Aut}(t)$, der Stabilisator von $\overline{P}$ ist $U(X,t,P)$. Nach Bemerkung 5.3.1 ist der Index von $U(X,t,P)$ in $U(X,t)$ höchstens $\frac{d}{a}$. Die Kurve X und der Morphismus t sind über $k = M(X,t,P)$ definiert, damit gilt $\operatorname{Aut}(C : k) \subset U(X,t)$. Nach Lemma 5.2.1 ist $U(X,t)$ damit abgeschlossen, und nach Lemma 5.2.5 gilt $[M(X,t,P) : M(X,t)] \leq [U(X,t,P) : U(X,t)] \leq \frac{d}{a}$.

□

Nun können wir aus den Bemerkungen 8.2.4 und 10.0.13 eine weitere Gradabschätzung folgern:

Folgerung 10.0.14 *Sei X eine vollständige Kurve über $\mathbb{C}$, $t : X \longrightarrow \mathbb{P}^1_{\mathbb{C}}$ ein endlicher Morphismus vom Grad d, dessen kritische Werte in $\{0, 1, \infty\}$ liegen. Sei a die Anzahl der Elemente in* $\operatorname{Aut}(t)$*, dann sind X und t über einem Zahlkörper k definiert mit*

$$[k : \mathbb{Q}] \leq \frac{d}{a} M_d$$

[8]siehe Diagramm aus Bemerkung 10.0.9

Literatur

[Kö] Bernhard Köck, “Belyi's Theorem Revisited”, arXiv:math.AG/0108222, 2001.

[Kö2] Bernhard Köck, “Belyi's Theorem Revisited”, Beiträge zur Algebra und Geometrie, Volume **45**, 2004.

[Ha] R. Hartshorne, “Algebraic Geometry”, Graduate Texts in Mathematics **52**, Springer-Verlag, New York 1977.

[Fo] O. Forster, “Lectures on Riemann Surfaces”, Graduate Texts in Mathematics **81**, Springer-Verlag, New York 1981.

[Bo] S. Bosch, “Algebra”, 4. Auflage, Springer-Verlag, Berlin 2001.

[Wi] D. J. Winter, “The Structure of Fields”, Graduate Texts in Mathematics **16**, Springer-Verlag, New York 1974.

[Ma] H. Matsumura, “Commutative algebra”, Second Edition, Mathematics lecture note series **56**, The Benjamin/Cumming Publishing Co., 1980.

[Hal] M. Hall, “The theory of groups”, Second Edition, Macmillian Co., New York 1968.

[Bb] N. Bourbaki, “Algebra I”, Chapters 1-3, Elements of Mathematics, Addison-Wesley Publishing Co., Great Britain 1973.

[EH] D. Eisenbud, J. Harris, “The Geometry of Schemes”, Graduate Texts in Mathematics **197**, Springer-Verlag, New York 2000.

[Lüt] W. Lütkebohmert, “Codierungstheorie”, 1. Auflage, Vieweg, 2003.

[Wa] F. Warner, “Foundations of Differentiable Manifolds and Lie Groups”, Graduate Texts in Mathematics **94**, Springer-Verlag, New York 1983.

[SZ] R. Stöcker, H. Zieschang, “Algebraische Topologie”, Mathematische Leitfäden, B. G. Teubner, Stuttgart 1988.