MATHEMATISCHES INSTITUT DER
UNIVERSITÄT BONN

DIPLOMARBEIT

Zur Inversen Galoisschen Theorie in positiver Charakteristik: Starrheitssätze

von Claus Diem

Unter der Betreuung von Prof. Dr. Florian Pop

Bonn, im Februar 1999

Dies ist meine Diplomarbeit aus dem Jahr 1999. Ich habe die Diagramme neu gesetzt. Außerdem habe einige Fußnoten eingefügt, wo ich Fehler gemacht hatte oder mir nun Änderungen sinnvoll erscheinen.

Leipzig, im November 2012, Claus Diem

Danksagung

Ich bedanke mich für die Betreuung der Arbeit bei Herrn Prof. Dr. Florian Pop. Beim Land Baden-Württemberg, der Provinz Ontario und dem Land Nordrhein-Westfalen bedanke ich mich für die guten Studienmöglichkeiten. Ich wurde mit einem Stipendium der Friedrich-Naumann-Stiftung unterstützt. Auch hier bedanke ich mich. Aber am meisten von allen danke ich meinen Eltern, die mich jahrelang unterstützt haben.

Inhaltsverzeichnis

Einleitung

Das Thema der vorliegenden Arbeit ist Inverse Galoissche Theorie in positiver Charakteristik. Allgemein ist es das Ziel der Inversen Galoisschen Theorie, die endlichen Quotienten der absoluten Galoisgruppe eines Körpers k zu bestimmen. D.h. man fragt sich, welche endlichen Gruppen als Galoisgruppen von galoisschen Körpererweiterungen $\lambda|k$ vorkommen.

Sei nun k ein globaler Körper, d.h. eine endliche Erweiterung von $\mathbf{Q}$ oder $\mathbf{F}_p(x)$. Dann gilt der Hilbertsche Irreduzibilitätssatz: Jede galoissche Erweiterung des rationalen Funktionenkörpers $k(t)$ kann unter Erhalt der Galoisgruppe auf eine galoissche Erweiterung von k spezialisiert werden.

Aus diesem Grund ist das sogenannte reguläre Inverse Galoissche Problem zentral: *Man realisiere alle endlichen Gruppen als Galoisgruppen einer über* $\mathbf{Q}$ *bzw.* $\mathbf{F}_p(x)$ *regulären, galoisschen Erweiterung* N *von* $\mathbf{Q}(t)$ *bzw. von* $\mathbf{F}_p(x)(t)$*!* (Regulär bedeutet in diesem Fall, dass $\mathbf{Q}$ bzw. $\mathbf{F}_p(x)$ algebraisch abgeschlossen in N ist.) Falls eine Gruppe Galoisgruppe einer solchen regulären Erweiterung ist, und k ein Zahlkörper respektive globaler Funktionenkörper ist, so ist G automatisch Galoisgruppe einer über k regulären, galoisschen Erweiterung von $k(t)$ und damit auch Galoisgruppe einer galoisschen Erweiterung von k.

Der *einfache* bzw der *starke Starrheitssatz* [MM, Theorem I.4.8, Theorem I.4.11] gibt Kriterien an, unter denen eine endliche Gruppe Galoisgruppe einer über k regulären galoisschen Erweiterung von $N|k(t)$ ist. Dabei ist k eine gewisse endliche abelsche Erweiterung von $\mathbf{Q}$, die unter weiteren Voraussetzungen gleich $\mathbf{Q}$ ist.

Diese Sätze gehen auf Belyi zurück. In [Belyi] wird gezeigt, dass die klassischen endlichen einfachen Gruppen vom Lie Typ als Galoisgruppen einer über $\mathbf{Q}^{ab}$ regulären, galoisschen Erweiterung über $\mathbf{Q}^{ab}(t)$ auftreten. Eine gute Übersicht über den Stand der Bemühungen, alle endlichen einfachen Gruppen als Galoisgruppen einer über $\mathbf{Q}$ regulären, galoisschen Erweiterung von $\mathbf{Q}(t)$ zu realisieren, bietet [MM, Kapitel I,2,3].

Das Ziel dieser Arbeit ist, die Starrheitssätze von Zahlkörpern auf globale Körper positiver Charakteristik zu übertragen. Dabei wird grundsätzlich vorausgesetzt, dass die *Charakteristik die Gruppenordnung nicht teilt.*

Zum einfachen Starrheitssatz

... in Charakteristik Null

Aufgrund der kontravarianten Äquivalenz der Kategorien der Funktionenkörper von Transzendenzgrad 1 über einem festen Grundkörper und der normalen, eigentlichen, irreduziblen Kurven (d.h. reduzierten, separierten Schemata von Dimension 1 über einem Körper) über demselben Grundkörper kann man Methoden der algebraischen Geometrie benutzen, um das reguläre Inverse Galoissche Problem anzugehen.

Sei $\mathbf{P}^1$ die (algebraische) projektive Gerade. Sei $\mathbf{Q}$ der Körper der rationalen Zahlen, $\overline{\mathbf{Q}}$ ein algebraischer Abschluss von $\mathbf{Q}$ und $\mathbf{C}$ der Körper der komplexen Zahlen. Sei S eine s-elementige Menge von rationalen Punkten aus $\mathbf{P}^1_{\mathbf{Q}}$. Sei $U = U_{\mathbf{Q}} := \mathbf{P}^1_{\mathbf{Q}} - S$. Sei für einen beliebigen Körper k in Charakteristik Null $U_k := U \times_{\mathbf{Q}} k$. Sei $\mathcal{U}$ die Analytifizierung von $U_{\mathbf{C}}$.

Ein erster Schritt zur Lösung des regulären Inversen Galoisschen Problems besteht im Riemannschen Existenzsatz. Dieser besagt insbesondere, dass die Kategorie der topologischen Überlagerungen von $\mathcal{U}$ äquivalent zur Kategorie der étalen Überlagerungen von $U_{\mathbf{C}}$ ist. Darüberhinaus ist bekannt, dass jede étale Überlagerung von $U_{\mathbf{C}}$ auch über $\overline{\mathbf{Q}}$ definiert werden kann. Daraus folgt, dass die étale Fundamentalgruppe von $U_{\overline{\mathbf{Q}}}$ kanonisch insomorph zur proendlichen Komplettierung der topologischen Fundamentalgruppe von $\mathcal{U}$ ist.

$$\pi_1(U_{\overline{\mathbf{Q}}}) =< \gamma_1, ..., \gamma_s | \gamma_1 \cdots \gamma_s = 1 > \hat{}$$

Sei nun G eine endliche Gruppe und $\underline{\sigma} = (\sigma_1, ..., \sigma_s)$ ein s-elementiges Erzeugendensystem von G mit $\sigma_1 \cdots \sigma_s = 1$. Dann definiert der surjektive stetige Homomorphismus $\pi_1(U_{\overline{\mathbf{Q}}}) \longrightarrow G, \gamma_i \mapsto \sigma_i$ eine galoissche Überlagerung von $U_{\overline{\mathbf{Q}}}$ mit Galoisgruppe G.

Die Frage ist nun, über welchen algebraischen Erweiterungen $k|\mathbf{Q}$ diese Überlagerung mit allen ihren Automorphismen definiert werden kann. Dazu betrachtet man die exakte Sequenz

$$1 \longrightarrow \pi_1(U_{\overline{\mathbf{Q}}}) \longrightarrow \pi_1(U_{\mathbf{Q}}) \longrightarrow \Gamma_{\mathbf{Q}} \longrightarrow 1 \tag{1}$$

Dabei ist $\Gamma_{\mathbf{Q}} := \mathrm{Gal}(\overline{\mathbf{Q}}|\mathbf{Q})$ die absolute Galoisgruppe von $\mathbf{Q}$. Die durch $\pi_1(U_{\overline{\mathbf{Q}}}) \longrightarrow G$ definierte galoissche Überlagerung ist genau dann mit allen Automorphismen über k definiert, wenn folgendes kommutatives Diagramm mit exakten Zeilen existiert:

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(U_{\overline{\mathbf{Q}}}) \arrow[r] \arrow[d] & \pi_1(U_k) \arrow[r] \arrow[d] & \Gamma_k \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & G \arrow[r] & G \times \Gamma_k \arrow[r] & \Gamma_k \arrow[r] & 1
\end{tikzcd} \tag{2}$$

Falls dies der Fall ist, definiert der Quotient $\pi_1(U_k) \longrightarrow G$ eine geometrisch irreduzible galoissche Überlagerung von U_k mit Galoisgruppe G. Durch Basiswechsel von k nach $\overline{\mathbf{Q}}$ erhält man die durch $\pi_1(U_{\overline{\mathbf{Q}}}) \longrightarrow G$ definierte Überlagerung und alle ihre Automorphismen. Die entsprechende Erweiterung von Funktionenkörpern ist dann die gesuchte reguläre galoissche Erweiterung von $k(t)$ mit Galoisgruppe G.

Sequenz 1 spaltet, da $U_{\mathbf{Q}}$ rationale Punkte enthält. Sei ein Schnitt fixiert. Dann operiert $\Gamma_{\mathbf{Q}}$ auf der freien proendlichen Gruppe auf $s-1$ Erzeugenden $\pi_1(U_{\overline{\mathbf{Q}}})$. Die Operation kann zur Zeit nicht effektiv angegeben werden. Bekannt ist allerdings: $\Gamma_{\mathbf{Q}}$ operiert auf den Konjugationsklassen der topologischen Erzeugenden γ_i mittels des cyklotomischen Charakters.

Die Idee des einfachen Starrheitssatzes besteht nun darin, diese Information auszunutzen und an die Gruppe G und das Erzeugendensystem $\underline{\sigma}$ gewisse Forderungungen zu stellen, so dass Diagramm 2 existiert.

Die Aussage des einfachen Starrheitssatzes lautet:

Sei G eine endliche Gruppe in der das Zentrum ein Komplement hat, und sei $\underline{C} = (C_1, ..., C_s)$ ein Vektor von Konjugationsklassen von G, welcher starr *ist. Dies heißt: Es gibt genau eine Konjugationsklasse $[\underline{\sigma}]$ von Erzeugendensystemen mit $\sigma_1 \cdots \sigma_s = 1$ und $\sigma_i \in C_i$. Dabei verstehen wir unter einer Konjugationsklasse von $\underline{\sigma}$ die Menge $[\underline{\sigma}] := \underline{\sigma}^G = \{(g\sigma_1 g^{-1}, ..., g\sigma_s g^{-1})|\ g \in G\}$.*

Sei $\mathbf{Q}_{\underline{C}} = \mathbf{Q}(\{\chi(C_i)|\chi$ irreduzibler Charakter von G mit Werten in $\overline{\mathbf{Q}}$, $i = 1, ..., s\})$.

Dann existiert eine über $\mathbf{Q}_{\underline{C}}$ reguläre, galoissche Erweiterung $N|\mathbf{Q}_{\underline{C}}(t)$ mit Galoisgruppe G.

Insbesondere, wenn für alle natürlichen Zahlen n mit $|G| \nmid n$ $\underline{C}^n = \underline{C}$ gilt, so gibt es eine über $\mathbf{Q}$ reguläre, galoissche Erweiterung $N|\mathbf{Q}(t)$ mit Galoisgruppe G.

... in positiver Charakteristik

Die Ergebnisse aus Charakteristik Null kann man auf positive Charakteristik übertragen, wenn man fordert, dass die Charakteristik die Gruppenordnung nicht teilt.

Der einfache Starrheitssatz hat zwei Versionen, je nachdem ob der Grundkörper ein endlicher Körper oder ein globaler Funktionenkörper ist. Der einfache Starrheitssatz für globale Funktionenkörper (siehe Satz 5.8) lautet:

Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung, in der das Zentrum ein Komplement hat. G besitze einen starren Klassenvektor $\underline{C}$ der Länge s.

Sei $(\mathbf{F}_p)_{\underline{C}} = \mathbf{F}_p(\{\chi(C_i)|\chi$ irreduzibler Charakter von G mit Werten in $\overline{\mathbf{F}}_p$, $i = 1, ..., s\})$.

Dann existiert eine über $(\mathbf{F}_p)_{\underline{C}}(x)$ reguläre, galoissche Erweiterung $N|(\mathbf{F}_p)_{\underline{C}}(x)(t)$ mit Galoisgruppe G.

Insbesondere, falls $\underline{C}^q = \underline{C}$ ist mit $q := p^e, e \geq 1$, so gibt es eine über $\mathbf{F}_q(x)$ reguläre, galoissche Erweiterung $N|\mathbf{F}_q(x)(t)$ mit Galoisgruppe G.

Für endliche Körper muss man nicht fordern, dass das Zentrum von G ein Komplement hat. Es gilt (siehe Satz 5.6):

Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung und einem $\underline{C}$ starren Klassenvektor der Länge s. Sei $e \geq 1$ und $q := p^e \geq s-1$.

Sei $(\mathbf{F}_q)_{\underline{C}} = \mathbf{F}_q(\{\chi(C_i)|\chi$ irreduzibler Charakter von G mit Werten in $\overline{\mathbf{F}}_p$, $i = 1, ..., s\})$.

Dann existiert eine über $(\mathbf{F}_q)_{\underline{C}}$ reguläre, galoissche Erweiterung $N|(\mathbf{F}_q)_{\underline{C}}(t)$ mit Galoisgruppe G.

Insbesondere, falls $\underline{C}^q = \underline{C}$ ist, so gibt es eine über $\mathbf{F}_q$ reguläre, galoissche Erweiterung $N|\mathbf{F}_q(t)$ mit Galoisgruppe G.

Für den *Beweis* sind folgende Punkte entscheidend:

- Der maximale p-primen Quotient der geometrischen Fundamentalgruppe einer Kurve über einem Körper in positiver Charakteristik ist bekannt.
- Sei k ein beliebiger Körper, $\overline{k}$ ein algebraischer Abschluss und k^{sep} ein separabler Abschluss von k, und sei U_k ein offener Teil der projektiven Geraden über k. Dann sind die étalen Fundamentalgruppen von $U_{\overline{k}}$ und $U_{k^{\text{sep}}}$ isomorph.
- Die maximale quasi-p-Untergruppe einer proendlichen Gruppe ist charakteristisch.

Diese Arbeit

Da die Kenntnis einiger Begriffe über Körper notwendig ist, um zu verstehen, was es heißt, eine Galoisgruppe sei über einem Teilkörper definiert, beginne ich mit einem Kapitel über diese Begriffe und einfache Eigenschaften.

Das zweite Kapitel hat endlich erzeugte Körpererweiterungen vom Transzendenzgrad 1, kurz Funktionenkörper, zum Inhalt. Insbesondere zeige ich dort, dass für einen regulären Funktionenkörper die Galoisgruppen der maximalen außerhalb S unverzeigten Erweiterungen von $\overline{k}K$ und von $k^{\text{sep}}K$ isomorph sind.

Im dritten Kapitel befasse ich mich mit algebraischen Kurven. Nach der Dedekind-Weber Äquivalenz ist die Kategorie der normalen, zusammenhängenden, eigentlichen k-Kurven isomporph zur Kategorie der Funktionenkörper (von Trandszendenzgrad 1) von k. Somit kann man mit Methoden aus der algebraischen Geometrie Einsichten über Funktionenkörper erlangen.

Im vierten Kapitel befindet sich der Beweis, dass die absolute Galoisgruppe Γ_k auf den Konjugationsklassen der Erzeugenden des p-primen Teils der algebraischen Fundamentalgruppe mittels des cyklotomischen Charakters operiert. Das Resultat lehnt sich stark an das entsprechende Resultat in Charakteristik Null an.

Im letzten Kapitel beweise ich den einfachen und den starken Starrheitssatz in positiver Charakteristik. Über endlichen Körpern kann der einfache Starrheitssatz insofern verbessert werden, als man nicht fordern muss, dass in der zu realisieren Gruppe das Zentrum ein Komplement besitzt.

In einem Anhang werden die in dieser Arbeit benutzten Begriffe und Tatsachen aus der Theorie der proendlichen Gruppen zusammengestellt.

Bezeichnungen und Definitionen

Sei k ein Körper. Dann vereinbaren wir die folgenden Bezeichnungen:

- k^{sep} ist ein separabler Abschluss von k
- k^{ins} ist ein rein inseparabler Abschluss von k
- $\overline{k}$ ist ein algebraischer Abschluss von k
- Γ_k ist die absolute Galoisgruppe von k, d.h. $\Gamma_k = \mathrm{Gal}(k^{\mathrm{sep}}|k)$
- Sei $K|k$ eine endlich erzeugte Körpererweiterung. Dann nennen wir $K|k$ einen *Funktionenkörper*, wenn der Transzendenzgrad von $K|k$ *gleich 1* ist.
- Sei $K|k$ ein Funktionenkörper, S eine endliche Menge von Primstellen von $K|k$. $M_S = M_S(K)$ ist eine maximale außerhalb S unverzweigte Erweiterung von K.

Für die algebraische Geometrie legen wir Folgendes fest:

- Alle Schemata seien noethersch und alle Morphismen seien von endlichem Typ
- Sei k ein beliebiger (*nicht* notwendig abgeschlossener Körper) Körper. Eine *k-Varietät* ist ein reduziertes, separiertes Schema über k (wie immer von endlichem Typ). Eine *k-Kurve* ist eine k-Varietät von Dimension 1.
- Ein Schema ist *ganz*, wenn es reduziert und irreduzibel ist
- Sei U ein normales, ganzes Schema.

  Sei X ein normales, ganzes Schema und $f : X \longrightarrow U$ ein endlicher, dominanter (und damit surjektiver) Morphismus. Dann nennen wir f eine *endliche, normale, ganze Überlagerung* von U. (Wir sagen dann auch, dass X eine normale, ganze Überlagerung von U ist.)

  Sei X ein normales Schema (nicht notwendiger Weise ganz). Dann nennen wir einen Morphismus $f : X \longrightarrow U$ eine *endliche, normale Überlagerung*, wenn f endlich und auf jeder Zusammenhangskomponente von X dominant (surjektiv) ist.

Außerdem vereinbaren wir:

- Vektoren werden stets unterstrichen.
- Die Konjugationsklasse eines Elementes x in einer Gruppe wird mit $[x]$ bezeichnet.
- Wenn wir über proendliche Gruppen reden, so meinen wir mit einem *Morphismus* stets einen stetigen Gruppenhomomorphismus, d.h. einen Morphismus in der Kategorie der proendlichen Gruppen.

Kapitel 1

Komposita von Körpern

1.1 Lineare Disjunktheit

Definition Sei F ein Körper. Seien $K|F$ und $L|F$ Körpererweiterungen. Ein *F-Kompositum von K und L* ist ein F-Algebrenmorphismus $K \otimes_F L \xrightarrow{\alpha} M$, wobei M das Körpererzeugnis des Bildes von α ist.

Ein *Morphismus von F-Komposita von K und L* $K \otimes_F L \xrightarrow{\alpha} M_1$ und $K \otimes_F L \xrightarrow{\beta} M_2$ ist ein Körpermorphismus $M_1 \xrightarrow{\psi} M_2$, so dass das Diagramm

$$\begin{tikzcd} K \otimes_F L \arrow[r, "\alpha"] \arrow[dr, "\beta"'] & M_1 \arrow[d, "\psi"] \\ & M_2 \end{tikzcd}$$

kommutiert. Jeder Morphismus von Komposita ist ein Isomorphismus, denn er ist nach Definition des Kompositums surjektiv und als Körpermorphismus injektiv.

Nach der universellen Eigenschaft des Tensorproduktes gibt es eine Bijektion zwischen F-Komposita einerseits und Paaren von Morphismen $K \hookrightarrow M$, $L \hookrightarrow M$, welche auf F die Identität sind, so dass M als Körper von Elementen aus K und L erzeugt wird, andererseits.

Definition Wenn die F-Erweiterungen K und L beide in einem Körper Ω eingebettet sind, so bezeichne KL das Körpererzeugnis von K und L in Ω. Das Kompositum $(K \overset{\iota_K}{\hookrightarrow} KL, L \overset{\iota_L}{\hookrightarrow} KL, KL)$, wobei ι_K und ι_L die Einbettungen von K und L nach Ω sind, ist dann *das Kompositum von K und L in Ω*.

Wenn $K \otimes_F L \longrightarrow M$ ein F-Kompositum ist, so ist M das Kompositum von K und L in M, wir schreiben deshalb auch $M = KL$. Dies bedeutet aber nicht, dass ein F-Kompositum von K und L durch M bis auf Isomorphie eindeutig definiert ist. Man betrachte dazu folgendes Beispiel:

Beispiel Der Körper $\mathbf{C}$ besitzt mit sich selbst als $\mathbf{R}$-Erweiterung genau zwei nichtisomorphe Komposita, die als Körper beide isomorph zu $\mathbf{C}$ sind. Das erste ist durch $\mathrm{id} : \mathbf{C} \longrightarrow \mathbf{C}$ und $\mathrm{id} : \mathbf{C} \longrightarrow \mathbf{C}$ gegeben. Das zweite hingegen durch die Identität $\mathrm{id} : \mathbf{C} \longrightarrow \mathbf{C}$ und die Konjugation $- : \mathbf{C} \longrightarrow \mathbf{C}$.

Definition Ein Kompositum $K \otimes_F L \longrightarrow KL$ ist *linear disjunkt*, falls der Morphismus injektiv ist.

Lineare Disjunktheit ist äquivalent zur folgenden, scheinbar unsymetrischen Bedingung:

Proposition 1.1 *Sei $\alpha : K \otimes_F L \longrightarrow KL$ ein Kompositum. Dann ist α genau dann linear disjunkt, wenn jede Teilmenge von K, die über F linear unabhängig ist, auch über L linear unabhängig ist.*

Beweis. Sei α injektiv. Seien $k_1, ...k_n$ über F linear unabhängige Elemente aus K. Dann sind $k_1 \otimes 1, ..., k_n \otimes 1 \in K \otimes_F L$ linear unabhängig über L. Da die Abbildung $K \otimes_F L \longrightarrow KL$ injektiv und K-linear ist, sind $k_1, ..., k_n$ linear unabhängig über L.

Sei andererseits jede Teilmenge aus K, die in KL über F linear unabhängig ist, auch über L linear unabhängig. Sei $x \in K \otimes_F L$. Dann gibt es K-linear unabhängige Elemente $k_1 ..., k_n \in K$ und Elemente $l_1, ..., l_n \in L$ mit $x = k_1 \otimes l_1 + \cdots + k_n \otimes l_n$. Wenn nun $k_1 l_1 + \cdots k_n l_n = 0$ in KL ist, so ist $l_1 = ... = l_n = 0$ nach Voraussetzung, also $x = 0$. $\square$

Damit sieht man sofort: Wenn M eine Körpererweiterung von K ist und M und L linear disjunkt über F sind, so sind auch K und L linear disjunkt über F.

Lineare Disjunktheit wird in dieser Arbeit durch folgendes Diagramm symbolisiert:

$$\begin{tikzcd}
KL \arrow[d, dash] \arrow[dr, dash] & \\
K \arrow[dr, dash] & L \arrow[d, dash] \\
& F
\end{tikzcd}$$

Das Bild eines Kompositums $K \otimes_F L \longrightarrow KL$ ist gleich

$$K[L] = L[K] = \{\sum_i k_i l_i | k_i \in K, l_i \in L\}$$

Wir werden uns nur mit linear disjunkten Körpererweiterungen beschäftigen, falls eine der beiden Erweiterungen algebraisch ist. In diesem Fall ist $KL = L[K] = K[L]$, und ein Kompositum $K \otimes_F L \longrightarrow KL$ ist stets surjektiv.

Proposition 1.2 *Sei $K|F$ algebraisch und $L|F$ beliebig. Dann sind äquivalent:*

1. *$K \otimes_F L \longrightarrow KL$ ist injektiv (und damit ein Isomorphismus), d.h. K und L sind über F linear disjunkt*
2. *$K \otimes_F L \longrightarrow KL$ ist ein Isomosphismus*
3. *$K \otimes_F L$ ist ein Körper*
4. *$K \otimes_F L$ ist ein Integritätsbereich*
5. *Jede über F linear unabhängige Teilmenge von K ist linear unabhängig über L*
6. *Jede Basis von $K|F$ ist eine Basis von $KL|L$*

Beweis. *1.* $\longrightarrow$ *2.*, *2.* $\longrightarrow$ *3.*, *3.* $\longrightarrow$ *4.* sind klar

4. $\longrightarrow$ *1.*: Sei $Q =$Quot$(K \otimes_F L)$ der Quotientenkörper. Q enthält durch $K \longrightarrow K \otimes_F L \longrightarrow Q$ und $L \longrightarrow K \otimes_F L \longrightarrow Q$ die Körper K und L. Das Bild der Abbildung $K \otimes_F L \longrightarrow Q$ ist gleich $L[K] = KL$. Somit ist $KL = Q$ und die Abbildung $K \otimes_F L \longrightarrow KL$ ist ein Isomorphismus, da $K \otimes_F L \longrightarrow Q$ injektiv ist. Also sind K und L über F linear disjunkt.

1. $\longrightarrow$ *5.*, *5.* $\longrightarrow$ *1.* siehe Proposition 1.1

5. $\longrightarrow$ *6.*: Jede Basis von $K|F$ ist linear unabhängig in $KL|L$ nach Voraussetzung. Sie ist aber auch ein Erzeugendensystem des L-Vektorraumes $K \otimes_F L$ und somit auch von $KL|L$.

6. $\longrightarrow$ *5.*: ist klar □

Dies wird falsch, wenn weder K noch L algebraisch über F sind. Sei beispielsweise $F(X,Y)$ der rationale Funktionenkörper in zwei Variabeln dann sind $F(X)$ und $F(Y)$ linear disjunkt über F in $F(X,Y)$. Sie sind aber nicht über F linear disjunkt bezüglich $F(X) \longrightarrow F(X), X \mapsto X$, $F(Y) \longrightarrow F(X), Y \mapsto X$.

Allerdings gilt aufgrund der universellen Eigenschaft des Quotientenkörpers: Wenn $K \otimes_F L$ ein Integritätsbereich ist, so ist $K \otimes_F L \longrightarrow$Quot$(K \otimes_F L)$ das eindeutige linear disjunkte Kompositum von K und L über F.

Deshalb definieren wir:

Definition Sei $K|F$ eine algebraische, $L|F$ eine beliebige Körpererweiterung. Dann sind K und L *linear disjunkt über F*, falls die F-Algebra $K \otimes_F L$ ein Körper ist. Falls dies der Fall ist, so ist die Identität $K \otimes_F L \longrightarrow K \otimes_F L$ *das Kompositum* von K und L über F.

Seien $K|F$ und $L|F$ beliebige Körpererweiterungen. Dann sind K und L *linear disjunkt über F*, falls die F-Algebra $K \otimes_F L$ ein Integritätsbereich ist. Falls dies der Fall ist, so ist der Morphismus von $K \otimes_F L$ auf den Quotientenkörper *das linear disjunkte Kompositum* von K und L über F.

Seien K und L über F linear disjunkt, KL das Kompositum von K und L über F. Sei L in einen Körper Ω eingebettet. Dann können F-Homomorphismen von K nach Ω zu L-Homomorphismen von KL nach Ω 'hochgehoben' werden: Sei dazu $\sigma \in \mathrm{Hom}_F(K, \Omega)$ beliebig. Dann definiert $k \otimes_F l \mapsto \sigma(k)l$ einen F-Algebrenmorphismus von $K \otimes_F L$ nach Ω. Nach Definition der linearen Disjunktheit ist die Abbildung $\widetilde{\sigma}$: $K[L] \longrightarrow \Omega, \sum_i k_i l_i \mapsto \sum_i \sigma(k_i) l_i$ $(k_i \in K, l_i \in L)$ wohldefiniert. Dies definiert dann einen eindeutigen Körperhomomorphismus von KL nach Ω.

Umgekehrt kann man L-Homomorphismen von KL nach Ω auf K einschränken. Wir erhalten dann einen F-Homomorphismus von K nach Ω. Die Abbildungen 'Hochheben' und 'Einschränken' sind invers zueinander. Daraus folgt:

Proposition 1.3 *Seien K und L über F linear disjunkt und sei L in Ω eingebettet. Dann definiert 'Hochheben' und 'Einschränken' eine Bijektion zwischen* $\mathrm{Hom}_F(K, \Omega)$ *und* $\mathrm{Hom}_L(KL, \Omega)$.

Wenn K und L über F linear disjunkt sind, so ist sicherlich $K \cap L = F$. Es ist interessant, Kriterien anzugeben, unter denen die Bedingung $K \cap L = F$ äquivalent zur linearen Disjunktheit ist.

Proposition 1.4 *Sei $\Omega|K$ eine Erweiterung. Sei $K|F$ ein galoisscher und $L|F$ ein algebraischer Teilkörper von $\Omega|K$. Dann sind K und L genau dann über F linear disjunkt, wenn $K \cap L = F$ ist.*

Beweis. Sei $K \cap L = F$.

1. Schritt Beweis für endliche Erweiterungen. Seien K und L endlich über F. Mit $K|F = K|K \cap L$ ist auch $KL|L$ galoissch (normal und separabel sind klar). Die Restriktion res: $\mathrm{Gal}(KL|L) \longrightarrow \mathrm{Gal}(K|K \cap L)$ definiert einen Isomorphismus. Die Injektivität ist klar. Die Surjektivität folgt aus folgender Überlegung: Sei $E|F$ der Körper mit Bild(res) $= \mathrm{Gal}(K|E)$. Man zeigt leicht, dass $E = F = K \cap L$ ist. Somit ist $[KL : L] = [K : K \cap L]$. Damit ist

$$\dim_F K \otimes_F L = \dim_F K \ \dim_F L =$$

$$[K : F][L : F] = [K : K \cap L][L : F] = [KL : L][L : F] = [KL : F]$$

Somit ist der Homomorphismus $K \otimes_F L \longrightarrow KL$ injektiv.

2. Schritt Beweis im allgemeinen Fall. Seien $k_1, ..., k_n \in K$ linear unabhängig über F. Seinen $l_1, ..., l_n \in L$ mit $l_1 k_1 + \cdots + l_n k_n = 0$. Dann sind die k_i in einer endlichen galoisschen Teilerweiterung von K und die l_i in einer endlichen algebraischen Teilerweiterung von $L|F$ enthalten. Diese sind nach Schritt 1 linear disjunkt. Also ist $l_1 = \cdots = l_n = 0$. Also sind K und L linear disjunkt über F. □

Separable algebraische und rein inseparable algebraische Erweiterungen sind immer linear disjunkt:

Proposition 1.5 *Sei $K|F$ separabel algebraisch und $L|F$ rein inseparabel. Dann sind K und L linear disjunkt über F.*

Beweis. Bette K und L in einen algebraisch abgeschlossenen Körper Ω ein. Sei K^n die normale Hülle von K. Dann ist $K^n|F$ galoissch. Außerdem ist $K^n \cap L = F$. Somit sind K^n und L linear disjunkt über F. Also sind auch K und L linear disjunkt über F. □

1.2 Definitionskörper

Definition

- Sei $M|K$ eine beliebige Körpererweiterung. Ein Teilkörper F von K ist ein *Definitionskörper* von $M|K$, falls eine zu K über F linear disjunkte Teilerweiterung L von $M|F$ existiert mit $M = KL$. L ist dann ein *Komplement* von $M|K$ über F.

- Sei $G =$Aut$(M|K)$. Ein *Definitionskörper von $M|K$ bezüglich der Automorphismengruppe G* ist ein Definitionskörper F, so dass G den Körper L invariant lässt, d.h. $G(L) \subseteq L$.

Falls F ein Definitionskörper zu $M|K$ ist, so sagen wir auch, $M|K$ sei *über F definiert.* Wenn G die Automorphismengruppe von $M|K$ ist und F ein Definitionskörper bezüglich der Automorphismengruppe ist, so sagen wir auch, $M|K$ sei *bezüglich G über F definiert.*

Bemerkungen

- Falls F ein Definitionskörper von $M|K$ mit Komplement L ist, so ist $M|K$ genau dann algebraisch, wenn $L|F$ algebraisch ist. Dies sieht man mit Hilfe von endlichen Teilerweiterungen.

- Sei nun F ein Definitionskörper von $M|K$ mit Komplement L.

  - Wie oben definiert können alle Elemente aus Aut$(L|F)$ zu Elementen aus Aut$(M|K)$ 'hochgehoben' werden. 'Hochheben' ist immer injektiv und genau dann ein Isomorphismus, wenn L ein Komplement von $M|K$ bezüglich G ist. Falls dies der Fall ist, ist die 'Einschränkung' Aut$(M|K) \longrightarrow$ Aut$(L|F)$ die Umkehrabbildung.

  - Falls $L|F$ algebraisch und normal ist, so ist F ein Definitionskörper bezüglich G.

  - Sei $M|K$ galoissch. Dann ist nach Proposition 1.3 (mit $\Omega = M$, Rollen von K und L vertauscht) F genau dann ein Definitionskörper bezüglich G, wenn $L|F$ galoissch ist.

Proposition 1.6 *Sei F ein Definitionskörper zur galoisschen Erweiterung $M|K$. Sei außerdem $K|F$ galoissch. Dann ist auch $M|F$ galoissch.*

Beweis. Sei L ein Komplement zu $M|K$ über F. Sei $x \in M$ fix unter $\mathrm{Aut}(M|F)$. Dann ist x fix unter $\mathrm{Gal}(M|K)$ und unter $\mathrm{Aut}(M|L)$. Ersteres bedeutet, dass $x \in K$ ist. Da $K|F$ galoissch ist, definiert Einschränken und Hochheben einen Isomorphismus von $\mathrm{Aut}(M|L)$ und $\mathrm{Gal}(K|F)$. Zweiteres besagt nun, dass x fix unter $\mathrm{Gal}(K|F)$ ist. D.h. $x \in F$. $\square$

Sehr übersichtlich ist die Frage, ob F ein Definitionskörper von $M|K$ oder gar ein Definitionskörper von $M|K$ bezüglich G ist, wenn $M|F$ und $K|F$ als galoissch vorausgesetzt wird.

Proposition 1.7 *Sei $M|F$ galoissch, $K|F$ eine galoissche Teilerweiterung mit $\mathrm{Gal}(M|K) = G$. Dann gilt:*

- *F ist genau dann ein Definitionskörper von $M|K$, wenn die Sequenz*

$$1 \longrightarrow \mathrm{Gal}(M|K) \longrightarrow \mathrm{Gal}(M|F) \longrightarrow \mathrm{Gal}(K|F) \longrightarrow 1$$

  spaltet.

- *F genau dann ein Definitionskörper von $M|K$ bezüglich G, wenn die Sequenz*

$$1 \longrightarrow \mathrm{Gal}(M|K) \longrightarrow \mathrm{Gal}(M|F) \longrightarrow \mathrm{Gal}(K|F) \longrightarrow 1$$

  spaltet und ein Schnitt gewählt werden kann, so dass die Operation von $\mathrm{Gal}(K|F)$ auf $\mathrm{Gal}(M|K)$ trivial ist.

Beweis. Sei F ein Definitionskörper von $M|K$ und L ein Komplement. Sei $H := \mathrm{Gal}(M|L)$. Die Aussagen $KL = M$ und $K \cap L = F$ sind äquivalent zu $H \cap G = 1, \mathrm{Gal}(M|F) = GH$. D.h. H ist ein abgeschlossenes Komplement zu G in $\mathrm{Gal}(M|F)$. Sei umgekehrt H ein abgeschlossenes Komplement zu G. Setze dann $L = M^H$. Nun gilt wieder $KL = M$ und $K \cap L = F$, also ist F ein Definitionskörper von $M|K$.

Sei F ein Definitionskörper von $M|K$ mit Komplement L. Dann gilt: F ein Definitionskörper bezüglich G mit Komplement $L \longleftrightarrow L|F$ ist normal $\longleftrightarrow$ $H = \mathrm{Gal}(M|L)$ ist normal in $\mathrm{Gal}(M|F) \longleftrightarrow H$ definiert einen Schnitt, so dass die Operation von $\mathrm{Gal}(K|F)$ auf $\mathrm{Gal}(M|K)$ trivial ist. $\square$

Die folgenden drei Propositionen sind direkte Anwendungen von Aussagen über semidirekte Produkte proendlicher Gruppen. Die entsprechenden gruppentheoretischen Aussagen werden im Anhang bewiesen. Dort werden auch die verwendeten Begriffe erläutert.

Falls $\mathrm{Gal}(K|F)$ eine projektive proendliche Gruppe ist, erhalten wir das folgende optimale Resultat. [MM, I, Theorem 3.4]

Proposition 1.8 *Sei $K|F$ galoissch mit projektiver Galoisgruppe. Sei $M|K$ galoissch mit $\mathrm{Gal}(M|K) = G$. Dann gilt:*

- *F ist genau dann ein Definitionskörper von $M|K$, wenn $M|F$ galoissch ist.*
- *F ist genau dann ein Definitionskörper von $M|K$ bezüglich G, wenn darüberhinaus* $\mathrm{Gal}(K|F)$ *auf G durch innere Automorphismen aus G operiert.*

Beweis. Wenn F ein Definitionskörper von $M|K$ ist, dann ist $M|F$ galoissch nach Proposition 1.6. Wenn andererseits $M|F$ galoissch ist, dann spaltet die exakte Sequenz

$$1 \longrightarrow \mathrm{Gal}(M|K) \longrightarrow \mathrm{Gal}(M|F) \longrightarrow \mathrm{Gal}(K|F) \longrightarrow 1\ ,$$

weil $\mathrm{Gal}(K|F)$ als projektiv vorausgesetzt wurde. Der zweite Teil folgt aus Proposition 2 im Anhang. □

Bemerkung Die Voraussetzungen dieser Proposition sind insbesondere dann erfüllt, wenn $\mathrm{Gal}(K|F)$ isomorph zu der Galoisgruppe eines endlichen Körpers ist. (z.B. $F = \mathbf{F}_p(t), K = \overline{\mathbf{F}}_p(t)$.)

Das folgende Resultat gibt eine hinreichende Bedingung dafür, dass F ein Definitionskörper von $M|K$ bezüglich G ist, wenn man schon weiß, dass $M|K$ über F definiert ist.

Proposition 1.9 *Sei $M|K$ eine galoissche Erweiterung mit Galoisgruppe G, in der das Zentrum ein (abgeschlossenes) Komplement hat. Sei $K|F$ galoissch und sei F ein Definitionskörper von $M|K$.* $\mathrm{Gal}(K|F)$ *operiere auf G durch innere Automorphismen aus G. Dann ist F ein Definitionskörper von $M|K$ bezüglich G.*

Beweis. Dies folgt sofort aus Proposition 4 im Anhang. □

Dieses Resultat lässt sich noch verschärfen:

Proposition 1.10 *Sei $M|K$ eine galoissche Erweiterung mit Galoisgruppe G und Zentrum $Z(G)$. Sei $K|F$ galoissch und sei F ein Definitionskörper von $M|K$. Sei H eine Untergruppe von G, in der $H \cap Z(G)$ ein (abgeschlossenes) Komplement hat. Es gebe ein (abgeschlossenes) Komplement von* $\mathrm{Gal}(K|F)$ *in* $\mathrm{Gal}(M|F)$*, so dass* $\mathrm{Gal}(K|F)$ *auf G durch innere Automorphismen, die durch Elemente aus H gebenen sind, operiert. Dann ist F ein Definitionskörper von $M|K$ bezüglich G.*

Beweis. Dies folgt aus Proposition 5 im Anhang. □

Wir kommen nun zur Frage, wann eine Teilerweiterung einer über F definierten Erweiterung selbst über F definiert ist.

Proposition 1.11 *Sei $M|F$ galoissch, $K|F$ eine galoissche Teilerweiterung von $M|F$, so dass F ein Definitionskörper zu $M|K$ ist. Sei $N|K$ eine galoissche Teilerweiterung von $M|K$. Dann ist F genau dann ein Definitionskörper zu $N|K$, wenn $N|F$ galoissch ist.*

Beweis. Falls F ein Definitionskörper von $N|K$ ist, so ist $N|F$ galoissch nach Proposition 1.6. Ist andererseits $N|F$ galoissch, so erhalten wir folgendes Diagramm mit exakten Zeilen:

$$\begin{tikzcd}
1 \arrow[r] & \mathrm{Gal}(M|K) \arrow[r] \arrow[d] & \mathrm{Gal}(M|F) \arrow[r] \arrow[d] & \mathrm{Gal}(K|F) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \mathrm{Gal}(N|K) \arrow[r] & \mathrm{Gal}(N|F) \arrow[r] & \mathrm{Gal}(K|F) \arrow[r] & 1
\end{tikzcd}$$

Weil die obere Sequenz spaltet, spaltet auch die untere. Deshalb ist F ein Definitionskörper zu $N|K$. $\square$

Sei F ein Definitionskörper zu $M|K$, und sei $M|F$ galoissch. Die Frage, ob $N|F$ galoissch ist, ist äquivalent zu der Frage, ob $\mathrm{Gal}(M|N)$ normal in $\mathrm{Gal}(M|F)$ ist. Dies ist genau dann der Fall, wenn $\mathrm{Gal}(M|N)$ invariant unter der Operation von $\mathrm{Gal}(K|F)$ auf $\mathrm{Gal}(M|K)$ ist. Eine Umformulierung hiervon ist:

Sei F ein Definitionskörper der galoisschen Erweiterung $M|K, \pi = \mathrm{Gal}(M|K)$. Sei $\psi : \pi \longrightarrow G$ ein surjektiver Morphismus. ψ definiert eine galoissche Zwischenerweiterung $N := M^{\mathrm{Kern}\,\psi}$ von $M|K$ mit Galoisgruppe G. Dann ist F genau dann ein Definitionskörper von $N|K$, wenn $\mathrm{Kern}(\psi)$ invariant unter der Operation von $\mathrm{Gal}(K|F)$ auf $\mathrm{Gal}(M|K)$ ist. Dies ist insbesondere immer dann der Fall, wenn $\mathrm{Kern}(\psi)$ in G charakteristisch ist.

1.3 Tensorprodukte von Körpern

Sei $K|F$ endlich algebraisch, $L|F$ beliebig. Dann ist $K = F[X_1, ..., X_n]/\mathbf{m}$, wobei $\mathbf{m}$ ein maximales Ideal in $F[X_1, ..., X_n]$ ist. Mit dem Chinesischen Restsatz erhalten wir einen F-Algebrenmorphismus

$$\begin{array}{c} K \otimes_F L = (F[X_1, ..., X_n]/\mathbf{m}) \otimes_F L = L[X_1, ..., X_n]/(\mathbf{m}) = \\ L[X_1, ..., X_n]/\mathbf{P}_1 \oplus \cdots \oplus L[X_1, ..., X_n]/\mathbf{P}_r \end{array} , \tag{1.1}$$

wobei die $\mathbf{P}_i$ die Primärideale zu $(\mathbf{m})$ sind. Sei jeweils $\mathbf{m}_i = \mathrm{rad}(\mathbf{P}_i)$ das assoziierte Primideal. Sei p_i die Projektion von $K \otimes_F L$ auf $L[X_1, ..., X_n]/\mathbf{m}_i$. Dieser Integritätsbereich enthält die Körper K und L. Sei Q der Quotientenkörper von $L[X_1, ..., X_n]/\mathbf{m}_i$. Dann ist das Bild von $L[X_1, ..., X_n]/\mathbf{m}_i$ in $KL \subseteq Q$ enthalten. Somit ist $L[X_1, ..., X_n]/\mathbf{m}_i = KL = Q$. Es ist also

$$(K \otimes_F L)^{\mathrm{red}} = (KL)_1 \oplus \cdots \oplus (KL)_r,$$

wobei jeder Körper $(KL)_i$ mit der Abbildung $p_i : K \otimes_F L \longrightarrow (KL)_i$ ein Kompositum von K und L ist.

Wir zeigen nun, dass jedes Kompositum von K und L isomorph zu einem $(KL)_i$ ist. Sei $K \otimes_F L \longrightarrow KL$ ein Kompositum. Wir erhalten einen surjektiven Ringmorphismus $(KL)_1 \oplus \cdots \oplus (KL)_r = (K \otimes_F L)^{\mathrm{red}} \longrightarrow KL$. Dabei werden die idempotenten Elemente der Form $e_i := (0, ..., 0, 1, 0, ..., 0)$ entweder auf 0 oder auf 1 abgebildet. Aus den Gleichungen $e_i e_j = 0$ $(i \neq j)$ folgt, dass höchstens eines dieser Elemente auf 1 abgebildet wird. Da aber das 1-Element $(1, ..., 1)$ auf 1 abgebildet wird, wird genau ein Element $(0, ..., 0, 1, 0, ..., 0)$ auf 1 abgebildet. Damit erhalten wir ein kommutatives Diagramm von F-Morphismen

$$\begin{tikzcd} K \otimes_F L \arrow[r] \arrow[d] & (K \otimes_F L)^{\mathrm{red}} \arrow[r, equal] & (KL)_1 \oplus \cdots \oplus (KL)_r \arrow[d, "p_i"] \\ KL \arrow[rr, "\sim"] & & (KL)_i \end{tikzcd}$$

Jedes Kompositum ist zu einem Faktor $(KL)_i$ (genauer gesagt zu genau einer Projektion $p_i : K \otimes_F L \longrightarrow (KL)_i$) isomorph. Es ist aber auch zu genau einer Projektion isomorph, da ansonsten die Faktoren untereinander isomorph wären, was angesichts der Gleichung $p_i(e_j) = \delta_{ij}$ unmöglich ist.

Daraus folgt:

Proposition 1.12 *Sei $K|F$ endlich und $L|F$ beliebig. Seien $p_i : L \otimes_F K \longrightarrow (KL)_i$ $(i = 1, ..., r)$ Repräsentanten aus den (endlich vielen) Isomorphieklassen der F-Komposita von K und L. Dann induziert der Homomorphismus*

$$p_1 \oplus \cdots \oplus p_r : K \otimes_F L \longrightarrow (KL)_1 \oplus \cdots \oplus (KL)_r$$

einen Isomorphismus von F-Algebren

$$(K \otimes_F L)^{\mathrm{red}} \cong (KL)_1 \oplus \cdots \oplus (KL)_r.$$

Falls $K|F$ endlich separabel ist, so ist

$$K \otimes_F L \cong (KL)_1 \oplus \cdots \oplus (KL)_r$$

und die Körper $(KL)_i$ sind endliche separable Erweiterungen von L.

Beispiel Wir wissen bereits, dass der Körper $\mathbf{C}$ mit sich selbst als $\mathbf{R}$-Körpererweiterung genau zwei nichtisomorphe Komposita besitzt. Es ist $\mathbf{C} \otimes_{\mathbf{R}} \mathbf{C} \cong \mathbf{C} \oplus \mathbf{C}$. Der Isomorphismus wird durch $(\mathrm{id}, \mathrm{id}) : \mathbf{C} \longrightarrow \mathbf{C} \oplus \mathbf{C}$ und $(\mathrm{id}, -) : \mathbf{C} \longrightarrow \mathbf{C} \oplus \mathbf{C}$ induziert.

Somit entspricht dem ersten Kompositum die Projektion auf den ersten Faktor, während dem zweiten Kompositum die Projektion auf den zweiten Faktor entspricht.

Wir beschäftigen uns nun wieder mit einer nicht notwendigerweise endlichen algebraischen Erweiterung $K|F$.

Proposition 1.13 *Sei $K|F$ algebraisch. Dann sind die unter 1. bis 3. angegebenen Punkte jeweils äquivalent*

- 1. *$K|F$ ist separabel*
  2. *$K \otimes_F \overline{F}$ ist reduziert, d.h. das Nilradikal ist Null*
  3. *$K \otimes_F L$ ist für alle Erweiterungen $L|K$ reduziert*
- 1. *$K|F$ ist rein inseparabel*
  2. *$K \otimes_F \overline{F}$ ist irreduzibel, d.h. das Nilradikal ist ein Primideal*
  3. *$K \otimes_F L$ ist für alle Erweiterungen $L|K$ irreduzibel*

Beweis. Im Fall, dass $K|F$ eine einfache Erweiterung ist, folgen alle Äquivalenzen sofort aus Gleichung 1.1.

Wir zeigen 1. $\longrightarrow$ 3. Sei $K|F$ eine beliebige algebraische, $L|K$ eine beliebige Erweiterung. Dann ist K induktiver Limes von gewissen einfachen Erweiterungen $F(\alpha_i)$. Da das Tensorprodukt mit induktivem Limes vertauscht, ist

$$K \otimes_F L = \varinjlim_i F(\alpha_i) \otimes_F L.$$

Da auch das Radikalbilden mit induktivem Limes vertauscht, ist

$$\mathrm{rad}(K \otimes_F L) = \varinjlim_i \mathrm{rad}(F(\alpha_i) \otimes_F L).$$

Falls $K|F$ separabel bzw. rein inseparabel ist, so sind alle $F(\alpha_i) \otimes_F L$ reduziert bzw. irreduzibel und $K \otimes_F L$ ist reduziert bzw. irreduzibel.

3. $\longrightarrow$ 2. ist klar.

2. $\longrightarrow$ 1. Sei nun $K \otimes_F \overline{F}$ reduziert bzw. irreduzibel. Sei $F(\alpha_i)$ eine einfache Teilereiterung von $K|F$. Da Körpererweiterungen flach sind, ist der Morphismus $F(\alpha_i) \otimes_F \overline{F} \longrightarrow K \otimes_F \overline{F}$ injektiv. Somit sind alle einfachen Teilerweiterungen von $K|F$ reduziert bzw. irreduzibel. Es folgt, dass $K|F$ separabel bzw. irreduzibel ist. $\square$

1.4 Separable, primäre und reguläre Erweiterungen

Die letzte Proposition legt es nahe, die Begriffe separabel bzw. rein inseparabel auf beliebige Erweiterungen auszudehnen. Anstatt von rein inseparablen Erweiterungen spricht man allerdings von primären Erweiterungen.

Definition Sei $K|F$ eine beliebige Körpererweiterung. Dann ist

- $K|F$ *separabel*, falls $K \otimes_F L$ für alle Erweiterungen $L|F$ reduziert ist
- $K|F$ *primär*, falls $K \otimes_F L$ für alle Erweiterungen $L|F$ irreduzibel ist
- $K|F$ *regulär*, falls $K \otimes_F L$ für alle Erweiterungen $L|F$ ein Integritätsbereich ist, d.h. K und L sind über F linear disjunkt

Eine Körpererweiterung ist also genau dann regulär, wenn sie separabel und primär ist. Erinnerung: Wenn $K|F$ regulär ist und $L|F$ eine beliebige Körpererweiterung ist, dann ist $\mathrm{Quot}(K \otimes_F L)$ *das* linear disjunkte Kompositum von K und L über F.

Proposition 1.14 *Sei $K|F$ endlich erzeugt. Dann sind äquivalent*

- 1. *$K|F$ ist separabel*
  2. *$K \otimes_k F^{\mathrm{ins}}$ ist reduziert*
  3. *$K|F$ ist separabel erzeugt, d.h. es existeriert eine Transzendenzbasis $\mathfrak{T} \subset K$, so dass $K|F(\mathfrak{T})$ algebraisch separabel ist*

  Desweiteren sind äquivalent

- 1. *$K|F$ ist primär*
  2. *$K \otimes_F F^{\mathrm{sep}}$ ist irreduzibel*
  3. *F ist separabel abgeschlossen in K, d.h. alle Elemente aus K, die algebraisch separabel über F sind, sind schon in F enthalten*

  und es sind äquivalent

- 1. *$K|F$ ist regulär*
  2. *$K \otimes_F \overline{F}$ ist ein Integritätsbereich*
  3. *K und $\overline{F}$ sind linear disjunkt über F*
  4. *$K|F$ ist separabel erzeugt und F ist separabel abgeschlossen in K*
  5. *$K|F$ ist separabel erzeugt und F ist algebraisch abgeschlossen in K*

Beweis. siehe [Bo, 7.3. Sätze 7,12,13] □

Insbesondere sieht man, dass eine Erweiterung $K|F$ genau dann separabel ist, wenn sie zu F^{ins} linear disjunkt ist, während sie genau dann primär ist, wenn sie zu F^{sep} linear disjunkt ist. In diesen Fällen sind nach Proposition 1.2 die Tensorprodukte $K \otimes_F F^{\mathrm{ins}}$ bzw. $K \otimes_F F^{\mathrm{sep}}$ sogar Körper.

Proposition 1.15 *Sei $K|F$ regulär und sei $L|K$ eine Erweiterung. Dann ist $L|F$ genau dann regulär, wenn L linear disjunkt zu $\overline{F}K$ über K ist.*

Beweis. Dies ist ein Spezialfall von [La, VIII,3,Proposition 3.1.]. Mit den hier verwendeten Notationen lautet dieser Satz: Seien $E|F$, $K|F$ und $L|K$ Erweiterungen. Dann gilt: E und L sind genau dann linear disjunkt über F, wenn E und K linear disjunkt über F und EK und L linear disjunkt über K sind. Setze nun $E := \overline{F}$. □

$$\begin{tikzcd}
EL \arrow[d, dash] \arrow[dr, dash] & & \\
L \arrow[dr, dash] & EK \arrow[d, dash] \arrow[dr, dash] & \\
& K \arrow[dr, dash] & E \arrow[d, dash] \\
& & F
\end{tikzcd}$$

Definition Sei $K|F$ regulär. Eine Erweiterung $L|K$ ist *regulär über* F, wenn L über F regulär ist.

Nach obiger Proposition ist eine Erweiterung $L|K$ genau dann regulär über F, wenn L und $\overline{F}K$ über K linear disjunkt sind.

Definition Sei $K|F$ eine reguläre Körpererweiterung und $M|\overline{F}K$ eine algebraische Körpererweiterung. Dann ist $M|\overline{F}K$ *über* F *definiert*, wenn es eine über F reguläre Teilerweiterung L von $M|\overline{F}K$ mit $M = \overline{F}L$ gibt.

In diesem Fall haben wir folgendes kommutatives Diagramm von linear disjunkten Erweiterungen:

$$\begin{tikzcd}
M = \overline{F}L \arrow[d, dash] \arrow[dr, dash] & & \\
L \arrow[dr, dash] & \overline{F}K \arrow[d, dash] \arrow[dr, dash] & \\
& K \arrow[dr, dash] & \overline{F} \arrow[d, dash] \\
& & F
\end{tikzcd}$$

Eine Erweiterung $M|\overline{F}K$ ist also genau dann über F definiert ist, wenn sie über K definiert ist.

Definition Sei mit obigen Bezeichnungen die algebraische Erweiterung $M|\overline{F}K$ über F definiert. Wenn dann der Morphismus $\mathrm{Aut}(L|K) \longrightarrow \mathrm{Aut}(M|\overline{F}K)$,

$\alpha \mapsto \alpha \otimes_F \mathrm{id}_{\overline{F}}$ ein Isomorphismus ist, so ist $M|\overline{F}K$ *bezüglich der Automorphismengruppe über* F *definiert.*

Nun ist $\alpha \otimes_F \mathrm{id}_{\overline{F}} = \alpha \otimes_K \mathrm{id}_{\overline{F}K}$, und somit ist die Erweiterung $M|\overline{F}K$ genau dann bezüglich der Automorphismengruppe über F definiert, wenn sie bezüglich der Automorphismengruppe über K definiert ist.

Kapitel 2

Funktionenkörper

2.1 Zerlegungstheorie

In diesem Kapitel fixieren wir einen Grundkörper k. Sei $K|k$ eine beliebige Körpererweiterung. Alle folgenden Erweiterungen seien in einen festen algebraisch abgeschlossenen Oberkörper Ω eingebettet.

In diesem Abschnitt werden kurz die Grundbegriffe der Zerlegungstheorie dargestellt und insbesondere auf Funktionenkörper (*immer von Transzendenzgrad 1*) angewendet.

Bewertungsringe und Bewertungen

Ein *Bewertungsring* von $K|k$ ist ein Ring $\mathcal{O}$, der k enthält und folgende Eigenschaft hat: $\forall x \in K : x \notin \mathcal{O} \longrightarrow x^{-1} \in \mathcal{O}$. Ein Bewertungsring ist ganz abgeschlossen, lokal mit maximalem Ideal $\mathfrak{p} = \{x \in K^*|x^{-1} \notin \mathcal{O}\} \cup \{0\}$ und Einheitengruppe $\mathcal{O}^* = \mathcal{O} - \mathfrak{p}$, wie man leicht sieht. Die kommutative Gruppe $\Gamma := K^*/\mathcal{O}^*$ heißt *Wertegruppe*. Die Operation auf Γ wird stets additiv geschrieben. Auf Γ ist durch $\overline{x} \leq \overline{x'} :\Longleftrightarrow x'x^{-1} \in \mathcal{O}^*$ eine Totalordnung definiert. Dadurch wird Γ eine geordnete Gruppe. Falls $\Gamma \cong \mathbf{Z}$ ist, nennen wir Γ einen *diskreten* Bewertungsring. Dies ist äquivalent dazu, dass das maximale Ideal $\mathfrak{p}$ ein Hauptideal ist und der Bewertungsring Höhe 1 hat. Die kanonischen Projektion $K^* \longrightarrow \Gamma$ ist eine *(nicht-archimedische) Bewertung* von $K|k$. Darunter verstehen wir eine Abbildung $K^* \longrightarrow \Gamma$ in eine geordnete Gruppe mit den folgenden Eigenschaften:

- $v(x) = 0$ für alle $x \in k^*$
- $v(xy) = v(x) + v(y)$ für alle $x, y \in K^*$
- $v(x) \geq \min\{v(x), v(y)\}$ für alle $x, y \in K^*$

Wenn $v : K^* \longrightarrow \Gamma$ eine Bewertung ist, so wählen wir ein Element $\infty \notin \Gamma$ und erweitern Γ mit $x + \infty := \infty, \infty + \infty = \infty$ zu einem Monoid $\Gamma \cup \infty$. Wir setzen

$v(0) := \infty$, $x < \infty$ für alle $x \in \Gamma$.

Wenn v eine Bewertung zu einem Bewertungsring ist, können $\mathcal{O}$ und $\mathfrak{p}$ aus v zurückgewonnen werden. Es ist

$$\mathcal{O} = \{x \in K | v(x) \geq 0\} \tag{2.1}$$

und außerdem

$$\mathfrak{p} = \{x \in K | v(x) > 0\}. \tag{2.2}$$

Andererseits kann durch Gleichung 2.1 jeder Bewertung von $K|k$ ein Bewertungsring zugeordnet werden. Das Primideal ist dann durch Gleichung 2.2 gegeben.

Zwei Bewertungen $v : K^* \longrightarrow \Gamma$ und $w : K^* \longrightarrow \Gamma'$ heißen *äquivalent*, falls es einen ordnungstreuen Isomorphismus $\gamma : v(K^*) \longrightarrow w(K^*)$ zwischen den Bildern der Bewertungen gibt mit $\gamma v = w$.

Äquivalente Bewertungen definieren den gleichen Bewertungsring. Dies motiviert folgende Definition:

Primstellen

Eine *Primstelle* einer Körpererweiterung $K|k$ ist eine Klasse von äquivalenten Bewertungen von $K|k$. Wir nennen eine Primstelle *diskret*, wenn die enthaltenen Bewertungen diskret sind. Zu jeder diskreten Primstelle $\mathfrak{p}$ gibt es eine eindeutig bestimmte surjektive Bewertung $v_\mathfrak{p} : K \longrightarrow \mathbf{Z}$, welche die *normierte* Bewertung zu $\mathfrak{p}$ genannt wird.

Jeder Primstelle $\mathfrak{p}$ ist eineindeutig ein Bewertungsring

$$\mathcal{O}_\mathfrak{p} = \{x \in K | v(x) \geq 0 \text{ für ein (und damit alle) } v \in \mathfrak{p}\}$$

von $K|k$ zugeordnet. Das maximale Ideal in $\mathcal{O}_\mathfrak{p}$ bezeichnen wir wieder mit $\mathfrak{p}$. Also

$$\mathfrak{p} = \{x \in K | v(x) > 0 \text{ für ein (und damit alle) } v \in \mathfrak{p}\}.$$

Definitionsgemäß ist eine Primstelle genau dann diskret, wenn der zugehörige Bewertungsring diskret ist. Der Körper $\kappa = \kappa(\mathfrak{p}) := \mathcal{O}_\mathfrak{p}/\mathfrak{p}$ heißt der *Restklassenkörper* zu $\mathfrak{p}$. Wir bezeichnen die Charakteristik des Restklassenkörpers stets mit p.

Erweiterungen

Sei $L|K$ eine algebraische Körpererweiterung. Falls $\mathfrak{P}$ eine Primstelle von L ist, deren Bewertungen beim Einschränken auf K in $\mathfrak{p}$ liegen, so sagen wir, $\mathfrak{P}$ sei eine Primstelle in L *über* $\mathfrak{p}$ oder eine *Erweiterung* von $\mathfrak{p}$ und schreiben $\mathfrak{P}|\mathfrak{p}$. Analog sagen wir, ein Bewertungsring $\mathcal{O}_\mathfrak{P}$ von L liege *über* $\mathcal{O}_\mathfrak{p}$, wenn $\mathcal{O}_\mathfrak{P} \cap K = \mathcal{O}_\mathfrak{p}$ ist. Man sieht, dass $\mathfrak{P}$ genau dann über $\mathfrak{p}$ liegt, wenn $\mathcal{O}_\mathfrak{P}$ über $\mathcal{O}_\mathfrak{p}$ liegt.

Wenn A eine nullteilerfreie k-Algebra mit Quotientenkörper K und $L|K$ eine algebraische Erweiterung ist, so bezeichnen wir die *Normalisierung* von A in L mit $\mathcal{N}_A(L)$, also

$$\mathcal{N}_A(L) = \{x \in L | x \text{ ganz über } A\}.$$

Der Körper L ist dann der Quotientenkörper von $\mathcal{N}_A(L)$.

Sei im Folgenden $K|k$ stets eine endlich erzeugte Körpererweiterung von Transzendenzgrad 1, kurz ein Funktionenkörper.

Endliche Erweiterungen

Wir überlegen uns zuerst, dass alle Primstellen eines Funktionenkörpers diskret sind. Für $k(t)|k$ ist das klar. Jeder Funktionenkörper $K|k$ ist endliche Erweiterung des rationalen Funktionenkörpers $k(t)|k$. Somit liegt jede Primstelle von $K|k$ über einer von $k(t)|k$.

Wir studieren allgemeiner Erweiterungen von diskreten Primstellen in endlichen Erweiterungen von Funktionenkörpern und zeigen dabei, dass Erweiterungen von diskreten Primstellen diskret sind. Sei $L|K$ eine endliche Erweiterung von Funktionenkörpern. Diskrete Bewertungsringe sind Spezialfälle von *Dedekindringen*, also noetherschen, ganz abgeschlossenen Ringen von Höhe 1. Die Normalisierung $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ eines diskreten Bewertungsringes $\mathcal{O}_\mathfrak{p}$ in L ist ein Dedekindring. [Ne, I, Satz (8.1)] Ein entscheidender Beweisschritt ist, dass im Falle von Funktionenkörpern $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ ein *endlicher* $\mathcal{O}_\mathfrak{p}$-Modul ist. [ZS, vol I,V,4, Theorem 9] (Es ist sogar die Normalisierung eines Dedekindringes in einer beliebigen endlichen Körpererweiterung ein Dedekindring (Satz von Krull-Akizuki) [Ne, I,Satz (12.8)])

Eine diskrete Primstelle $\mathfrak{p}$ von $K|k$ besitzt Erweiterungen in L. Alle diese erhält man folgendenmaßen: Das Ideal $\mathfrak{p}$ zerfällt im Dedekindring $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ in Primideale. [Ne, I, Korollar (3.9)]

$$(\mathfrak{p}) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r} \;\; (\mathfrak{P}_i \neq \mathfrak{P}_j \text{ für } i \neq j)$$

Die Lokalisierung von $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ an jedem dieser Primideale $\mathfrak{P}_i$ ist ein Bewertungsring, der über $\mathcal{O}_p$ liegt. So erhält man auch alle Bewertungsringe über $\mathcal{O}_\mathfrak{p}$, da diese als normale Ringe $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ enthalten und lokal sind. Da die Normalisierung $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ ein Dedekindring ist, ist jeder Bewertungsring von $L|k$ als Lokalisierung der Normalisierung ein Dedekindring [Ne, I, Satz (11.4)] und somit diskret. Dies zeigt insbesondere, dass *alle* Primstellen von Funktionenkörpern diskret sind, da alle Funktionenkörper über k endliche Erweiterungen von $k(t)$ sind.

Seien κ, λ die Restklassenkörper von $\mathfrak{p}$ und $\mathfrak{P}$. Die Körpererweiterung $\lambda|\kappa$ ist endlich, da die Erweiterung der Dedekindringe $\mathcal{O}_\mathfrak{p} \hookrightarrow \mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ endlich ist. Wir setzen $f = f_{\mathfrak{P}|\mathfrak{p}} := [\lambda : \kappa]$ und nennen diese Zahl den *Trägheitsgrad* von $\mathfrak{P}|\mathfrak{p}$. Die Zahl $e_{\mathfrak{P}|\mathfrak{p}}$ mit $v_\mathfrak{P}(a) = e_{\mathfrak{P}|\mathfrak{p}} v_\mathfrak{p}(a)$ für $a \in K^*$ heißt *Verzweigungsindex*. Wenn $\mathfrak{P} = \mathfrak{P}_i$ aus obiger Zerlegung von $\mathfrak{p}$ in $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L)$ ist, so ist $e_{\mathfrak{P}|\mathfrak{p}} = e_i$.

Wir vereinbaren die folgenden Begriffe: So ist $\mathfrak{p}$ *unzerlegt* in $L|K$, wenn über $\mathfrak{p}$ genau eine Primstelle liegt und *voll zerlegt*, wenn die Anzahl der Erweiterungen von $\mathfrak{p}$ gleich dem Grad der Erweiterung $L|K$ ist. Eine Erweiterung $\mathfrak{P}|\mathfrak{p}$ ist *unverzeigt*, wenn $e_{\mathfrak{P}|\mathfrak{p}} = 1$ ist und die Restklassenkörpererweiterung separabel ist. Andererseits ist $\mathfrak{P}|\mathfrak{p}$ *rein verzeigt*, wenn die Restklassenkörpererweiterung rein inseparabel ist und *rein wild verzweigt*, wenn zusätzlich $e_{\mathfrak{P}|\mathfrak{p}}$ eine p-Potenz (p Charakteristik des Restklassenkörpers) ist.

Für endliche Erweiterungen von Funktionenkörpern gilt die fundamentale Gleichung

$$\sum_{\mathfrak{P}|\mathfrak{p}} e_{\mathfrak{P}|\mathfrak{p}} f_{\mathfrak{P}|\mathfrak{p}} = [L:K].$$

Denn: Die Normalisierung des Ringes $\mathcal{O}_\mathfrak{p}$ in der endlichen K-Erweiterung L ist ein endlicher $\mathcal{O}_\mathfrak{p}$-Modul. [ZS, vol I,V,4, Theorem 9] Nach [En, Theorem 18.6] gilt die fundamentale Gleichung. Falls darüberhinaus die Erweiterung $L|K$ normal ist, so operiert die Automorphismengruppe von $L|K$ transitiv auf der Menge der Primstellen über $\mathfrak{p}$ und alle Trägheitsgrade und alle Verzeigungsindices von Primstellen über $\mathfrak{p}$ sind gleich.

Beliebige algebraische Erweiterungen

Sei $L|K$ nun eine beliebige algebraische Erweiterung, $\mathfrak{p}$ eine Primstelle von $K|k$. Dann besitzt die Bewertung $v_\mathfrak{p}$ Erweiterungen auf jede endliche Zwischenerweiterung. Die Erweiterungen sind bezüglich $(L', w') \leq (L'', w'') :\Longleftrightarrow L' \subseteq L'', w''|_{L'} = w'$ partiell geordnet. Offensichtlich existieren obere Schranken für jede total geordnete Teilmenge. Nach dem Zornschen Lemma gibt es Erweiterungen $\mathfrak{P}$ von $\mathfrak{p}$ auf L. Diese sind jedoch im Allgemeinen nicht diskret. Es gibt insbesondere keine normierte Bewertung $v_\mathfrak{P}$.

Sei $\mathfrak{P}|\mathfrak{p}$ eine solche Erweiterung. Wir sagen dann, $\mathfrak{P}|\mathfrak{p}$ sei *unverzweigt / rein verzweigt / rein wild verzweigt* in L, wenn die Einschränkung von $\mathfrak{P}|\mathfrak{p}$ auf jede endliche Teilerweiterung von $L|K$ diese Eigenschaft hat. Analog sei $\mathfrak{p}$ unzerlegt / voll zerlegt in L, wenn $\mathfrak{p}$ diese Eigenschaft in jeder endlichen Teilerweiterung von $L|K$ hat. Insbesondere ist eine Primstelle $\mathfrak{p}$ in L genau dann unzerlegt, wenn über ihr in L genau eine Primstelle liegt.

Hilbertsche Zerlegungstheorie

Sei $L|K$ eine beliebige galoissche Erweiterung. Die Galoisgruppe von $L|K$ hat für alle $\mathfrak{P}|\mathfrak{p}$ die abgeschlossenen Untergruppen $G_{\mathfrak{P}|\mathfrak{p}}(L|K)$ - *Zerlegungsgruppe*,

$I_{\mathfrak{P}|\mathfrak{p}}(L|K)$ - *Trägheitsgruppe*, $R_{\mathfrak{P}|\mathfrak{p}}(L|K)$ - *Verzeigungsgruppe*, wobei

$$\begin{aligned}
G_{\mathfrak{P}|\mathfrak{p}}(L|K) &= \{\sigma \in \mathrm{Gal}(L|K)| \quad \sigma(\mathfrak{P}) = \mathfrak{P}\} \\
I_{\mathfrak{P}|\mathfrak{p}}(L|K) &= \{\sigma \in G_{\mathfrak{P}|\mathfrak{p}}(L|K)| \quad \forall x \in \mathcal{N}_{\mathcal{O}_\mathfrak{p}}(L) : \sigma x \equiv x \bmod \mathfrak{P}\} \\
R_{\mathfrak{P}|\mathfrak{p}}(L|K) &= \{\sigma \in G_{\mathfrak{P}|\mathfrak{p}}(L|K)| \quad \forall x \in L^* : \tfrac{\sigma x}{x} \equiv 1 \bmod \mathfrak{P}\}\ .
\end{aligned}$$

Durch $\overline{\sigma}(\overline{x}) := \overline{\sigma(x)}$ wird ein stetiger Homomorphismus $G_{\mathfrak{P}|\mathfrak{p}}(L|K) \longrightarrow \mathrm{Gal}(\lambda|\kappa)$ definiert. Nach Definition ist die Trägheitsgruppe der Kern dieses Homomorphismus. Man zeigt, dass die Verzweigungsgruppe die (einzige) p-Sylowgruppe in der Trägheitsgruppe ist. [Ne, II,Satz (9.12)]

Durch diese Gruppen (und die höheren Verzweigungsgruppen) kann das Verzweigungsverhalten von $\mathfrak{P}|\mathfrak{p}$ bestimmt werden. Dies ist die soganannte Hilbertsche Verzweigungstheorie. So ist $\mathfrak{p}$ genau dann unzerlegt in $L|K$, wenn für eine Primstelle $\mathfrak{P}|\mathfrak{p}$ $G_{\mathfrak{P}|\mathfrak{p}}(L|K) = \mathrm{Gal}(L|K)$ ist, und voll zerlegt, wenn $G_{\mathfrak{P}|\mathfrak{p}}(L|K) = 1$ ist. Weiterhin ist $\mathfrak{P}|\mathfrak{p}$ genau dann *unverzweigt*, wenn $I_{\mathfrak{P}|\mathfrak{p}}(L|K) = 1$ ist, *rein verzeigt*, wenn $G_{\mathfrak{P}|\mathfrak{p}}(L|K) = I_{\mathfrak{P}|\mathfrak{p}}(L|K)$ ist und *rein wild verzweigt*, wenn $G_{\mathfrak{P}|\mathfrak{p}}(L|K) = R_{\mathfrak{P}|\mathfrak{p}}(L|K)$ ist.

Henselisierungen

Ein wichtiges Hilfsmittel zur Untersuchung des Verzweigungsverhaltens einer Primstelle in einer Körpererweiterung sind *Hensilisierungen.* Sei $\mathfrak{p}$ eine Primstelle von K. Diese erweitert sich zu einer Primstelle $\mathfrak{P}$ in einem separablen Abschluss K^{sep} von K. Wir bezeichnen den Zerlegungskörper dieser Erweiterung mit $K_\mathfrak{p}$ und nennen diesen Körper eine *Henselisierung* von K *an* $\mathfrak{p}$. Aus der Hilbertschen Zerlegungstheorie folgt, dass zwei Henselisierungen zu derselben Primstelle $\mathfrak{p}$ isomorph sind. Die Einschränkung von $\mathfrak{P}$ auf $K_\mathfrak{p}$ bezeichnen wir wieder mit $\mathfrak{p}$. Nach Konstruktion ist die Primstelle $\mathfrak{p}$ in jeder algebraischen Erweiterung von $K_\mathfrak{p}$ unzerlegt.

Der Körper $K_\mathfrak{p}$ erfüllt das *Henselsche Lemma* [Ne, II, 6]: Sei $f \in \mathcal{O}_\mathfrak{p}[x]$ ein primitives Polynom, dass über dem Restklassenkörper $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$ eine Zerlegung in teilerfremde Polynome $\overline{g}, \overline{h} \in \kappa[x]$ besitzt. Dann besitzt f eine Zerlegung in Polynome $g, h \in \mathcal{O}_\mathfrak{p}[x]$, wobei die Polynome g, h auf $\overline{g}, \overline{h}$ reduziert werden.

Sei $L|K$ eine algebraische Körpererweiterung, $\mathfrak{P}|\mathfrak{p}$ eine Erweiterung von Primstellen und $\mathfrak{p}$ diskret. Dann ist $LK_\mathfrak{p}$ eine Hensilisierung von L an $\mathfrak{P}$, Bezeichnung $L_\mathfrak{P}$. Da $\mathfrak{p}$ und $\mathfrak{P}$ in den Erweiterungen $K_\mathfrak{p}|K$ und $L_\mathfrak{P}|L$ voll zerlegt sind, ist der Verzeigungsindex und der Trägheitsgrad von $\mathfrak{P}|\mathfrak{p}$ in $L|K$ und in der Erweiterung der Henselisierungen $L_\mathfrak{P}|K_\mathfrak{p}$ gleich.

Sei nun $L|K$ galoissch. Dann ist auch die Erweiterung der Henselisierungen $L_\mathfrak{P}|K_\mathfrak{p}$ galoissch. Die Einbettung $\tau : L \hookrightarrow L_\mathfrak{P}$ definiert eine Restriktion

$\mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}}) \longrightarrow \mathrm{Gal}(L|K)$. Es gilt [Ne, II, Satz (9.6)]

$$G_{\mathfrak{P}|\mathfrak{p}}(L|K) \cong \mathrm{Gal}(L_{\mathfrak{P}}|K_{\mathfrak{p}})$$

$$I_{\mathfrak{P}|\mathfrak{p}}(L|K) \cong I(L_{\mathfrak{P}}|K_{\mathfrak{p}})$$

$$R_{\mathfrak{P}|\mathfrak{p}}(L|K) \cong R(L_{\mathfrak{P}}|K_{\mathfrak{p}}) .$$

Dabei ist $I(L_{\mathfrak{P}}|K_{\mathfrak{p}})$ und $R(L_{\mathfrak{P}}|K_{\mathfrak{p}})$ die Trägheitsgruppe bzw. die Verzweigungsgruppe von $\mathfrak{p}$ in $L_{\mathfrak{P}}|K_{\mathfrak{p}}$.

2.2 Rein inseparable Erweiterungen

Mit der Hilbertsche Zerlegungstheorie können nur separable Körpererweiterungen untersucht werden. Deshalb beschäftigen wir uns nun mit rein inseparablen Erweiterungen. Weiterhin sei $K|k$ ein Funktionenkörper (von Transzendenzgrad 1).

Proposition 2.1 *Sei $L|K$ eine rein inseparable Erweiterung, $\mathfrak{p}$ eine Primstelle von $K|k$. Dann ist $\mathfrak{p}$ in $L|K$ unzerlegt und rein wild verzeigt.*

Beweis. Da diese Aussagen genau dann gelten, wenn sie für alle endlichen Zwischenerweiterungen gelten, können wir uns auf endliche Erweiterungen beschränken.

Die Primstelle $\mathfrak{p}$ ist in $L|K$ unzerlegt: Sei w eine Fortsetzung von $v_{\mathfrak{p}}$ in L. Sei $x \in L$ beliebig. Dann gibt es ein $i \in \mathbf{N}$ mit $x^{p^i} = a \in K$. Dementsprechend ist $p^i w(x) = w(x^{p^i}) = w(a) = v_{\mathfrak{p}}(a)$, also $w(x) = p^{-i} v_{\mathfrak{p}}(a)$. Damit ist w durch $v_{\mathfrak{p}}$ eindeutig bestimmt.

Außerdem ist die Restklassenkörpererweiterung $\lambda|\kappa$ rein inseparabel. Denn da alle Elemente $x \in L$ eine Gleichung der Form $x^{p^i} - a = 0$ mit $a \in K$ erfüllen, gilt für $\overline{x} \in \lambda$: $x^{p^i} - \overline{a} = 0$ mit $\overline{a} \in \kappa$. Die fundamentale Gleichung lautet $n = ef$. Da der Grad von $L|K$ eine Potenz von p ist, ist auch der Verzweigungsindex eine Potenz von p. □

Proposition 2.2 *Sei $L|K$ eine algebraische Erweiterung, $\mathfrak{p}$ eine Primstelle von $K|k$, die eine Fortsetzung $\mathfrak{P}$ auf L besitzt, welche unverzweigt ist. Dann ist $L|K$ separabel.*

Beweis. Wieder können wir uns auf endliche Erweiterungen beschränken.

Sei K' die maximale separable Teilerweiterung von $L|K$, $\mathfrak{p}'$ die Fortsetzung von $\mathfrak{p}$ auf K'. Dann ist $\mathfrak{P}|\mathfrak{p}'$ nach Voraussetzung unverzweigt, d.h. der Verzweigungsindex ist gleich 1 und die Restklassenkörpererweiterung ist separabel. Nach der vorigen Proposition ist $\mathfrak{p}'$ in L aber auch unzerlegt und die Restklassenkörpererweiterung ist rein inseparabel. Aus der fundamentalen Gleichung folgt $L = K'$. □

Sei $L|K$ galoissch und sei $K'|K$ rein inseparabel. Dann sind nach Proposition 1.5 L und K' linear disjunkt über K. Sei L' das Kompositum. Dann ist $L'|K$ normal, L ist die maximale separable, K' die maximale rein inseparable Teilerweiterung und $L'|K'$ ist galoissch.

Wir wollen zeigen, dass die Verzweigungsgruppen und die Trägheitsgruppen der galoisschen Erweiterungen $L'|K'$ und $L|K$ kanonisch isomorph sind.

Sei $\mathfrak{p}$ eine Primstelle von K, $\mathfrak{P}$ eine Erweiterung in L, $\mathfrak{p}'$ die eindeutige Erweiterung von $\mathfrak{p}$ nach K', $\mathfrak{P}'$ die Erweiterung von $\mathfrak{P}$ nach L'. Seien $\kappa, \lambda, \kappa', \lambda'$ die entsprechenden Restklassenkörper.

Die Restriktion definiert einen Isomorphismus auf den Zerlegungsgruppen, da die Fortsetzungen der Bewertungen und der Automorphismen eindeutig sind.

$$G_{\mathfrak{P}'|\mathfrak{p}'}(L'|K') \longrightarrow G_{\mathfrak{P}|\mathfrak{p}}(L|K)$$

Dieser setzt sich fort zu einem kommutativen Diagramm

$$\begin{tikzcd}
1 \arrow[r] & I_{\mathfrak{P}'|\mathfrak{p}'}(L'|K') \arrow[r] \arrow[d] & G_{\mathfrak{P}'|\mathfrak{p}'}(L'|K') \arrow[r] \arrow[d] & \mathrm{Aut}(\lambda'|\kappa') \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I_{\mathfrak{P}|\mathfrak{p}}(L|K) \arrow[r] & G_{\mathfrak{P}|\mathfrak{p}}(L|K) \arrow[r] & \mathrm{Aut}(\lambda|\kappa) \arrow[r] & 1
\end{tikzcd}$$

mit exakten Zeilen. Die Kommutativität folgt aus der Kommutativität des rechten Vierecks. Außerdem ist $\mathrm{Aut}(\lambda'|\kappa') \cong \mathrm{Aut}(\lambda|\kappa)$, da die Erweiterungen $\lambda'|\lambda$ und $\kappa'|\kappa$ rein inseparabel sind. Also sind auch die Trägheitsgruppen isomorph.

Proposition 2.3 *Jede algebraisch separable Erweiterung $M|k^{\mathrm{ins}}K$ ist mit ihrer Automorphismengruppe über K definiert. Die maximale separable Teilerweiterung $L|K$ ist das eindeutige Komplement. Eine Primstelle $\mathfrak{p}$ von $K|k$ ist genau dann unzerlegt/ rein zerlegt in $L|K$, wenn die eindeutige Fortsetzung unzerlegt/ voll zerlegt in $M|k^{\mathrm{ins}}K$ ist. Eine Erweiterung $\mathfrak{P}|\mathfrak{p}$ ist genau dann unverzweigt in $L|K$, wenn die eindeutige Fortsetzung auf $M|k^{\mathrm{ins}}K$ unverzeigt ist.*

Falls $M|k^{\mathrm{ins}}K$ galoissch ist, definiert die Restriktion einen Isomorphismus auf den Zerlegungsgruppen und den Trägheitsgruppen.

Beweis. Es ist noch zu zeigen: Eine Erweiterung $\mathfrak{P}|\mathfrak{p}$ ist genau dann unverzweigt in $L|K$, wenn die eindeutige Fortsetzung auf $M|k^{\mathrm{ins}}K$ unverzeigt ist. Dies folgt aus folgendem Lemma, nach dem man nur den galoisschen Fall betrachten muss. □

Lemma 2.4 *Seien $L_1|K$, $L_2|K$ endliche Erweiterungen, L ein Kompositum von L_1 und L_2, $\mathfrak{p}$ eine Primstelle von K, $\mathfrak{P}|\mathfrak{p}$ eine Erweiterung von $\mathfrak{p}$ auf L. Seien die Einschränkungen $\mathfrak{P}_1, \mathfrak{P}_2$ von $\mathfrak{P}$ auf L_1, L_2 unverzeigt über $\mathfrak{p}$. Dann ist auch $\mathfrak{P}|\mathfrak{p}$ unverzweigt.*

Beweis. Sei $K_\mathfrak{p}$ eine Henselisierung von K an $\mathfrak{p}$, $L_\mathfrak{P} = LK_\mathfrak{p}$. Dann ist $L_\mathfrak{P}$ Kompositum von $L_1K_\mathfrak{p}$ und $L_2K_\mathfrak{p}$, und die Erweiterungen $L_1K_\mathfrak{p}|K_\mathfrak{p}$ und $L_2K_\mathfrak{p}|K_\mathfrak{p}$ sind unverzweigt. Nach [Ne, II, (7.3)] ist $L_\mathfrak{P}|K_\mathfrak{p}$ unverzeigt. Damit ist auch $L|K$ unverzweigt. □

2.3 Die maximale außerhalb S unverzeigte Erweiterung

Definition Sei S eine endliche Menge von Primstellen des Funktionenkörpers $K|k$. Sei $\mathcal{K}_S(K)$ die Kategorie der endlichen, außerhalb S unverzweigten Erweiterungen von K in Ω. Nach obigem Lemma hat $\mathcal{K}_S(K)$ die Eigenschaft, dass es mit zwei Objekten auch deren Kompositum in Ω enthält. Die Objekte von $\mathcal{K}_S(K)$ bilden also bezüglich der Inklusion in Ω ein direktes System. Wir setzen

$$M_S = M_S(K) := \varinjlim_{L \in \mathcal{K}_S(K)} L.$$

$M_S(K)$ heißt die *maximale außerhalb S unverzweigte Erweiterung von K.*

Proposition 2.5 *Die maximale außerhalb S unverzweigte Erweiterung M_S ist separabel über K.*

Beweis. Jeder Funktionenkörper $K|k$ hat unendlich viele Primstellen, denn der rationale Funktionenkörper $k(t)|k$ hat schon unendlich viele Primstellen. Da S endlich ist, gibt es eine Primstelle $\mathfrak{p} \notin S$. Die Behauptung folgt aus Proposition 2.2 □

$M_S|K$ ist galoissch, da $\mathcal{K}_S(K)$ mit einem Objekt auch dessen galoissche Hülle enthält. Es gilt:

$$\mathrm{Gal}(M_S|K) = \varprojlim_{\substack{L \in \mathcal{K}_S(K) \\ L|K \mathrm{galoissch}}} \mathrm{Gal}(L|K).$$

M_S ist Durchschnitt über alle maximalen in $\mathfrak{p}$ unverzweigten Erweiterungen, wobei $\mathfrak{p} \notin S$, also

$$M_S = \bigcap_{p \notin S, \mathfrak{P}|\mathfrak{p}} T_{\mathfrak{P}|\mathfrak{p}},$$

wobei $T_{\mathfrak{P}|\mathfrak{p}} = \mathrm{Gal}(K^{\mathrm{sep}}|K)^{I_{\mathfrak{P}|\mathfrak{p}}(K^{\mathrm{sep}}|K)}$ die maximale unverzweigte Teilerweiterung von $\mathfrak{P}|\mathfrak{p}$ in $\overline{K}$ ist.

Da über jeder Primstelle von K genau eine Primstelle von $k^{\mathrm{ins}}K$ liegt, schreiben wir auch S für die über S liegende Menge von Primstellen von $k^{\mathrm{ins}}K$. Aus Proposition 2.3 folgt insbesondere

Satz 2.6 *Sei $M_S(k^{\mathrm{ins}}K)$ die maximale außerhalb S unverzweigte Erweiterung von $k^{\mathrm{ins}}K$. Dann ist K mit Komplement $M_S(K)$ ein Definitionskörper zu $M_S(k^{\mathrm{ins}}K)|k^{\mathrm{ins}}K$ bezüglich der Galoisgruppe* $\mathrm{Gal}(M_S(k^{\mathrm{ins}}K)|k^{\mathrm{ins}}K)$*. Dabei definiert die Restriktion einen Isomorphismus auf den Trägheitsgruppen.*

Nach dem eben bewiesenen Satz erhalten wir folgendes Diagramm linear disjunkter Erweiterungen:

$$\begin{tikzcd}
M_S(k^{\mathrm{ins}}K) \arrow[d, dash] \arrow[dr, dash] & \\
k^{\mathrm{ins}}K \arrow[dr, dash] & M_S(K) \arrow[d, dash] \\
& K
\end{tikzcd}$$

und somit einen kanonischen Isomorphismus

$$\mathrm{Gal}(M_S(k^{\mathrm{ins}}K)|k^{\mathrm{ins}}K) \cong \mathrm{Gal}(M_S(K)|K)\ .$$

2.4 Separable Konstantenerweiterungen

Wir wollen zeigen, dass algebraisch separable Konstantenerweiterungen stets unverzweigt sind.

Proposition 2.7 *Sei $K|k$ eine beliebige primäre Erweiterung. Sei A eine normale k-Algebra in K. Sei $l|k$ eine algebraische separable Erweiterung. Dann ist die Normalisierung von A in $Kl = K \otimes_k l$ gerade $Al = A \otimes_k l$.*

Beweis. Wir behandeln zuerst den Fall, dass $l|k$ endlich ist.

Sei $\mathcal{N}_A(Kl)$ der ganze Abschluss von A in Kl. Dann ist sicherlich $Al \subseteq \mathcal{N}_A(Kl)$. Es ist noch die umgekehrte Inklusion $\mathcal{N}_A(Kl) \subseteq Al$ zu zeigen.

Sei $l_1, ...l_n$ eine Basis von $l|k$. Da nach Voraussetzung K und l linear disjunkt über k sind, ist $l_1, ..., l_n$ eine Basis von $Kl|K$. Sei d die Diskriminante von $l_1, ..., l_n$ in $Kl|K$,

$$d = d(l_1, ..., l_n) = (det(\sigma_i l_j)_{ij})^2,$$

wobei σ_i die K-Einbettungen von Kl in den algebraisch abgeschlossenen Körper Ω durchläuft. Nach Proposition 1.3 durchläuft $\sigma_i|l$ genau die Einbettungen von l nach Ω. Damit ist d die Diskriminante von $l_1, ..., l_n$ in der Erweiterung $l|k$. Insbesondere ist $d \in k$ und ungleich 0, da die Erweiterung $l|k$ als separabel vorausgesetzt ist.

Nach [Ne, I, Lemma (2.9)] ist

$$\mathcal{N}_A(Kl) \subseteq \frac{1}{d}(Al_1 + \cdots + Al_n) = Al.$$

Der unendliche Fall folgt nun durch

$$\mathcal{N}_A(L) = \varinjlim_{\substack{l' \text{endl. Teilerw.} \\ \text{von } l|k}} \mathcal{N}_A(Kl') = \varinjlim_{\substack{l' \text{endl. Teilerw.} \\ \text{von } l|k}} Al' =$$

$$A \qquad \underset{\substack{l' \text{endl. Teilerw.} \\ \text{von } l|k}}{\varinjlim} \qquad l' = Al$$

□

Bemerkung Diese Aussage ist für separable (oder auch reguläre Funktionenkörper) und rein inseparable Konstantenerweiterungen i.A. nicht richtig. Man betrachte das folgende Beispiel:

Sei $p > 2$ eine ungerade Primzahl, $k = \mathbf{F}_p(t)$ (allgemeiner sei k ein beliebiger Körper mit $t \in k$, $\sqrt[p]{t} \notin k$). Sei $K := k(y)[X]/(f)$ mit $f(X) = X^p - X - ty^p, x := X \bmod f$ (y tranzendent über k). Sei $\alpha = \sqrt[p]{t}, l = k(\alpha)$. Sei A=(Normalisierung von $k[\frac{1}{y}]_{\frac{1}{y}} = \mathcal{O}_{\frac{1}{y}}$ in K). Dann ist $K|k$ regulär und $l|k$ rein inseparabel.

Behauptung Al ist nicht ganz abgeschlossen in Kl; das Element $u = \frac{1}{x-\alpha y} \in Kl$ ist normal über Al aber nicht in Al enthalten.

Dazu: Es ist $u^{-p} - u^{-1} - \alpha y = x^p - ty^p - x + \alpha y - \alpha y = 0$, somit $u^p + \frac{u^{p-1}}{\alpha y} - \frac{1}{\alpha y} = 0$. Folglich ist u normal über Al.

Annahme: $u \in Al$. Dann gibt es eindeutig bestimmte $u_i \in A$ mit $u = \sum_{i=0}^{p-1} \alpha^i u_i$. Daraus folgt:

$$1 = \sum_{i=0}^{p-1} x\alpha^i u_i - \sum_{i=0}^{p-1} y\alpha^{i+1} u_i = \sum_{i=1}^{p-1} \alpha^i (xu_i - yu_{i-1}) + xu_0 - ytu_{p-1}$$

Aus der Eindeutigkeit der u_i folgt:

$$1 = xu_0 - ytu_{p-1}, \forall i = 1, ..., p-1 : xu_i = yu_{i-1}, \text{ also } u_i = \frac{y}{x} u_{i-1}$$

Einsetzen ergibt:

$$1 = xu_0 - yt(\frac{y}{x})^{p-1} u_0 = u_0(x - \frac{ty^p}{x^{p-1}})$$

$$\begin{aligned} \Longrightarrow u_0 &= (x - \tfrac{ty^p}{x^{p-1}})^{-1} = (x - \tfrac{x^p - x}{x^{p-1}})^{-1} \\ &= (\tfrac{x^p - x^p + x}{x^{p-1}})^{-1} = (\tfrac{x}{x^{p-1}})^{-1} = x^{p-2} \end{aligned}$$

Es ist noch zu zeigen, dass $x^{p-2} \notin A$ ist. Der Ring $k[\frac{1}{y}]_{\frac{1}{y}}$ ist der diskrete Bewertungsring zu $v_\infty = v_{\frac{1}{y}}$. Aus der Gleichung $(\frac{x}{y})^p - \frac{1}{y^{p-1}} \frac{x}{y} - t = 0$ folgt, dass das Element $\frac{x}{y}$ in A enthalten und eine Einheit ist. Es wird im Restklassenkörper auf eine p-te Wurzel von t abgebildet. Nach der Fundamentalen Gleichung ist v_∞ in der Erweiterung $K|k(y)$ unzerlegt und rein wild verzweigt. Insbesondere ist A ein Dedekindring. Sei w die eindeutige Fortsetzung von v_∞ auf K. Dann ist $w(x) = w(\frac{x}{y})w(y) = v_\infty(y) = -1$. Somit ist $x^{p-2} \notin A$ und damit auch $u_0 \notin A$ *Widerspruch!*. □

Sei $K|k$ ein primärer Funktionenkörper, $l|k$ algebraisch separabel. Sei $\mathfrak{p}$ eine Primstelle von K, $\mathcal{O}_\mathfrak{p}$ der Bewertungsring, $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(Kl)$ die Normalisierung des Bewertungsrings in Kl. Sei κ der Restklassenkörper von $\mathfrak{p}$.

Die Primstelle $\mathfrak{p}$ zerfällt in $\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(Kl)$ in $(\mathfrak{p}) = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_r^{e_r}$ mit maximalen Idealen $\mathfrak{P}_i$. Damit ist

$$\kappa \otimes_k l = \mathcal{O}_\mathfrak{p}/\mathfrak{p} \otimes_k l = (\mathcal{O}_\mathfrak{p} \otimes_k l)/(\mathfrak{p}) = \mathcal{N}_{\mathcal{O}_\mathfrak{p}}(Kl)/(\mathfrak{p}) =$$

$$\mathcal{N}_{\mathcal{O}_\mathfrak{p}}(Kl)/\mathfrak{P}_1^{e_1} \oplus \cdots \oplus \mathcal{N}_{\mathcal{O}_\mathfrak{p}}(Kl)/\mathfrak{P}_r^{e_r}$$

Da $l|k$ algebraisch separabel ist, ist $\kappa \otimes_k l$ reduziert. Genauer ist $\kappa \otimes_k l = (\kappa l)_1 \oplus \cdots \oplus (\kappa l)_r$, wobei $(\kappa l)_i$ alle nicht-isomorphen k-Komposita von κ und l durchläuft. Somit sind alle Restklassenkörpererweiterungen separabel und alle Verzweigungsindices gleich 1. Wir fassen zusammen:

Proposition 2.8 *Sei $K|k$ ein beliebiger Funktionenkörper. Dann ist jede Primstelle von $K|k$ in $k^{\mathrm{sep}}K|k$ unverzweigt.*

Beweis. Soeben haben wir den Fall einer primären Erweiterung $K|k$ behandelt. Der allgemeine Fall folgt, wenn man zuerst von k zum algebraischen Abschluss von k in K übergeht. Über diesem ist dann K primär nach Proposition 1.14. □

Es folgt, dass die Erweiterung $k^{\mathrm{sep}}K|K$ ein Teilkörper von $M_S = M_S(K)$ ist. Insbesondere ist $M_S = M_S(K) = M_S(k^{\mathrm{sep}}K)$. Wir erhalten eine exakte Sequenz

$$1 \longrightarrow \mathrm{Gal}(M_S|k^{\mathrm{sep}}K) \longrightarrow \mathrm{Gal}(M_S|K) \longrightarrow \mathrm{Gal}(k^{\mathrm{sep}}K|K) \longrightarrow 1 .$$

Sei $\overline{S}$ die in $k^{\mathrm{sep}}K$ bzw. $\overline{k}K$ über S liegende Menge von Primstellen. Nach Satz 2.6 gilt

$$\mathrm{Gal}(M_S|k^{\mathrm{sep}}K) \cong \mathrm{Gal}(M_{\overline{S}}(\overline{k}K)|\overline{k}K)$$

Sei nun $K|k$ *primär*. Dann ist k mit Komplement k^{sep} ein Definitionskörper von $k^{\mathrm{sep}}K|K$ bezüglich der Galoisgruppe. Also ist

$$\mathrm{Gal}(k^{\mathrm{sep}}K|K) \cong \Gamma_k$$

Insgesamt erhalten wir eine exakte Sequenz

$$1 \longrightarrow \mathrm{Gal}(M_S(\overline{k}K)|\overline{k}K) \longrightarrow \mathrm{Gal}(M_S(K)|K) \longrightarrow \Gamma_k \longrightarrow 1 \qquad (2.3)$$

Wir beschäftigen uns nun mit Erweiterungen, die eine Primstelle mit Grad 1 - d.h. mit Restklassenkörper k - besitzen. In diesem Fall muss man gar nicht fordern, dass $K|k$ primär ist.

Proposition 2.9 *Wenn K eine Primstelle von Grad 1 hat, so ist $K|k$ regulär.*

Beweis. Sei v Bewertung von Grad 1. Seien $a_1, ..., a_n \in \overline{k}$ linear unabhängig über k. *Annahme:* Es gibt $b_1, ..., b_n \in K$ mit $\sum_i a_i b_i = 0$, nicht alle $b_i = 0$.

Durch Multiplizieren mit einer Potenz einer Uniformisierenden an v kann man erreichen, dass alle b_i nicht-negative Bewertung haben und mindestens ein b_i Bewertung 0 hat, d.h. eine Einheit in $\mathcal{O}_p$ ist. Durch die Restklassenabbildung erhalten wir die Relation $\sum_i a_i \overline{b_i} = 0$ in $\overline{k}$. Nach Konstruktion und Voraussetzung liegen alle $\overline{b_i}$ in k und mindestens ein $\overline{b_i}$ ist ungleich 0. *Widerspruch!*
□

Proposition 2.10 *Wenn $K|k$ eine Primstelle mit Grad 1 besitzt, dann spaltet die Sequenz 2.3 immer.*

Zuerst ein Lemma

Lemma 2.11 *Sei $M|K$ eine galoissche Erweiterung, $\mathfrak{p}$ eine Primstelle von K (wie immer diskret), $\mathfrak{P}$ eine Fortsetzung von $\mathfrak{p}$ auf M. Sei $\lambda|\kappa$ die Erweiterung der Restklassenkörper. λ sei abgeschlossen unter Wurzelziehen. Dann spaltet die Sequenz*

$$1 \longrightarrow I_{\mathfrak{P}|\mathfrak{p}}(M|K) \longrightarrow G_{\mathfrak{P}|\mathfrak{p}}(M|K) \longrightarrow \mathrm{Aut}(\lambda|\kappa) \longrightarrow 1\ .$$

Beweis. Nach [Ne, II, Satz (9.4)] können wir annehmen, dass $M|K$ henselsch ist.

Aufgrund des exakten Diagramms

$$\begin{tikzcd}
 & 1 \arrow[d] & 1 \arrow[d] & 1 \arrow[d] & \\
1 \arrow[r] & R(M|K) \arrow[r] \arrow[d] & R(M|K) \arrow[r] \arrow[d] & 1 \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I(M|K) \arrow[r] \arrow[d] & \mathrm{Gal}(M|K) \arrow[r] \arrow[d] & \mathrm{Aut}(\lambda|\kappa) \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & I(M|K)/R(M|K) \arrow[r] \arrow[d] & \mathrm{Gal}(M|K)/R(M|K) \arrow[r] \arrow[d] & \mathrm{Aut}(\lambda|\kappa) \arrow[r] \arrow[d] & 1 \\
 & 1 & 1 & 1 &
\end{tikzcd}$$

müssen wir nur zeigen, dass die exakten Sequenzen

$$1 \longrightarrow I(M|K)/R(M|K) \longrightarrow \mathrm{Gal}(M|K)/R(M|K) \longrightarrow \mathrm{Aut}(\lambda|\kappa) \longrightarrow 1$$

und

$$1 \longrightarrow R(M|K) \longrightarrow \mathrm{Gal}(M|K) \longrightarrow \mathrm{Gal}(M|K)/R(M|K) \longrightarrow 1$$

spalten.

Zur ersten Sequenz: Sei $V = M^{R(M|K)}$ die maximale zahm verzweigte Teilerweiterung, $T = M^{I(M|K)}$ die maximale unverzweigte Teilerweiterung von $M|K$. Dann ist die Sequenz nichts anderes als

$$1 \longrightarrow \mathrm{Gal}(V|T) \longrightarrow \mathrm{Gal}(V|K) \longrightarrow \mathrm{Aut}(\lambda|\kappa) \longrightarrow 1.$$

Dabei ist λ der Restklassenkörper von V und T. Sei $\pi \in K$ eine fest gewählte Uniformisierende. Sei $V_n|T$ eine endliche Teilerweiterung von Grad n. Dann gilt $p \nmid n$ und $V_n = T(\sqrt[n]{t_n})$, wobei $t_n \in T$ eine Uniformisierende ist. (Siehe [Ne, II, Satz (7.7)] und beachte, dass die Bewertung als diskret vorausgesetzt wurde.) π ist auch Uniformisierende in T. Damit ist $\alpha_n := \frac{t_n}{\pi}$ eine Einheit in T. Nach Voraussetzung sind die n-ten Wurzeln von $\overline{\alpha_n}$ in λ enthalten. Nach dem Henselschen Lemma sind auch die n-ten Wurzeln von α in T enthalten. Damit gilt $V_n = T(\sqrt[n]{\pi})$. Die Erweiterungen $K(\sqrt[n]{\pi})$ mit $\sqrt[n]{\pi} \in V$ bilden ein induktives System. Sei $L := \lim_{\longrightarrow n \text{ mit } \sqrt[n]{\pi}\in V} K(\sqrt[n]{\pi})$. Dann ist L ein Komplement zu $V|T$ über K und die Sequenz spaltet.

Zur zweiten Sequenz: Beweis nach [KPR]. Sei die Charakteristik p der Restklassenkörper positiv. Die Gruppe $I(M|K)/R(M|K) = \mathrm{Gal}(V|T)$ hat Ordnung prim zu p. Somit sind die p-Sylowgruppen von $\mathrm{Gal}(L|K)/R(L|K)$ und $\mathrm{Gal}(L|K)/I(L|K) = \mathrm{Aut}(\lambda|\kappa)$ isomorph. Die p-Sylowgruppen von Körpern mit Charakteristik p haben kohomologische Dimension ≤ 1. Dies folgt aus der Artin-Schreier Theorie. [Se2, II, 2.2. Proposition 3 mit Beweis]. Somit hat $\mathrm{Gal}(M|K)/R(M|K)$ kohomologische p-Dimension ≤ 1 [Se2, I, 3.3. Proposition 14 mit Corollaire 1] und jede Sequenz mit pro-p-Kern spaltet. □

Beweis von Proposition 2.10. Sei weiterhin $\mathfrak{p}$ eine Primstelle von K mit Grad 1 und sei $\mathfrak{P}$ eine Fortsetzung auf M_S. Seien λ und κ die Restklassenkörper von M_S und K. Die Sequenz

$$1 \longrightarrow I_{\mathfrak{P}|\mathfrak{p}}(M_S(K)|K) \longrightarrow G_{\mathfrak{P}|\mathfrak{p}}(M_S(K)|K) \longrightarrow \mathrm{Aut}(\lambda|\kappa) \longrightarrow 1$$

spaltet nach dem Lemma. Die Restklassenkörper κ und λ können mit k bzw. k^{sep} identifiziert werden. Die Identifikation ist gegeben durch $k \overset{\iota}{\hookrightarrow} K \xrightarrow{p} \kappa \cup \{\infty\}$ und analog für k^{sep} und λ. Wir erhalten ein kommutatives Diagramm

$$\begin{tikzcd}
1 \arrow[r] & I_{\mathfrak{P}|\mathfrak{p}}(M_S(K)|K) \arrow[r] \arrow[d] & G_{\mathfrak{P}|\mathfrak{p}}(M_S(K)|K) \arrow[r] \arrow[d] & \mathrm{Aut}(\lambda|\kappa) \arrow[r] \arrow[d, "\cong"] & 1 \\
1 \arrow[r] & \mathrm{Gal}(M_S(K)|k^{\mathrm{sep}}K) \arrow[r] & \mathrm{Gal}(M_S(K)|K) \arrow[r] & \Gamma_k \arrow[r] & 1 .
\end{tikzcd}$$

Dies definiert einen Schnitt. □

Sei eine Primstelle $\mathfrak{p}$ und ein Schnitt $\Gamma_k \hookrightarrow G_{\mathfrak{P}|\mathfrak{p}}(M_S(K)|K)$ wie im Beweis fest gewählt. Falls $\mathfrak{p} \notin S$ ist, so ist

$$G_{\mathfrak{P}|\mathfrak{p}}(M_S(K)|K) \xrightarrow{\sim} \mathrm{Aut}(\lambda|\kappa)$$

ein Isomorphismus, und der Schnitt ist durch $\mathfrak{P}|\mathfrak{p}$ eindeutig bestimmt. In jedem Fall ist das Komplement in $G_{\mathfrak{P}|\mathfrak{p}}(M_S(K)|K)$ enthalten.

Sei M eine außerhalb S unverzweigte galoissche Erweiterung über $\overline{k}K$. Sei G ihre Galoisgruppe. Dann ist $M|\overline{k}K$ über k definiert.

Nach Konstruktion bleibt $I_{\mathfrak{P}|\mathfrak{p}}(M|\overline{k}K)$ unter der Operation von Γ_k invariant. Wenn nun Γ_k auf G durch innere Automorphismen aus G operiert, dann sind diese in $N_G(I_{\overline{\mathfrak{P}}|\overline{\mathfrak{p}}}(M|\overline{k}K))/Z(G)$ ($N_G(I_{\overline{\mathfrak{P}}|\overline{\mathfrak{p}}}(M|\overline{k}K))$ = Normalisator von $I_{\overline{\mathfrak{P}}|\overline{\mathfrak{p}}}(M|K)$ in G) enthalten. Wir können Proposition 1.10 anwenden und erhalten:

Proposition 2.12 *Sei $K|k$ ein (regulärer) Funktionenkörper, $\mathfrak{p}$ eine Primstelle mit Grad 1. Sei M eine außerhalb S unverzweigte galoissche Erweiterung von $\overline{k}K$, die normal über K ist. Dann ist $M|\overline{k}K$ über k definiert. Sei $G = \mathrm{Gal}(M|\overline{k}K)$. Sei $\overline{\mathfrak{P}}$ eine Fortsetzung von $\mathfrak{p}$ auf M. Sei H eine Untergruppe von G, die die Gruppe $N_G(I_{\overline{\mathfrak{P}}|\overline{\mathfrak{p}}}(M|\overline{k}K))$ enthält. Es gelte:*

- *Das Zentrum von G hat ein Komplement in H.*
- *Γ_k operiert auf G durch innere Automorphismen aus G.*

Dann ist die Erweiterung $M|\overline{k}K$ mit ihrer Galoisgruppe über k definiert.

Siehe auch [MM, I,Theorem 3.9] für einen anderen Beweis.

In diesem Zusammenhang lautet Proposition 1.8:

Proposition 2.13 *Sei k ein endlicher Körper, $K|k$ ein regulärer Funktionenkörper. Sei $M|\overline{k}K$ eine galoissche Erweiterung mit Galoisgruppe G, die über K galoissch ist. Dann ist M über k definiert. Wenn darüberhinaus Γ auf G durch innere Automorphismen aus G operiert, dann ist die Erweiterung $M|\overline{k}K$ mit ihrer Galoisgruppe über k definiert.*

Kapitel 3

Kurven

3.1 Die Fundamentalgruppe normaler Schemata

Wir beginnen mit einer Zusammenstellung der grundlegenden Definitionen und Ergebnisse über étale Überlagerungen normaler Schemata und die Fundamentalgruppe. Die Darstellung ist an das erste Kapitel von [Popp] angelehnt. Alle Schemata seien noethersch und alle Morphismen seinen von endlichem Typ. Schemata werden im Folgenden mit X, Y oder U bezeichnet. Die Strukturgarbe eines Schemas X wird mit $\mathcal{O}_X$, die lokalen Ringe mit $\mathcal{O}_{X,x}$, die entsprechenden maximalen Ideale mit $\mathfrak{m}_x$ bezeichnet. Falls X reduziert und irreduzibel ist, so soll $\kappa(X)$ der Funktionenkörper sein.

Etale und endliche, normale Überlagerungen

Definition Sei $f : X \longrightarrow U$ ein Morphismus von Schemata, $x \in X$ ein topologischer Punkt und $u = f(x)$. Dann ist f

- *unverzweigt* in x, falls
  1. $f^{\#}(\mathfrak{m}_u)\mathcal{O}_{X,x} = \mathfrak{m}_x$ und
  2. die Restklassenkörpererweiterung $\kappa(x)|\kappa(u)$ endlich separabel ist.
- *flach* in x, falls $\mathcal{O}_{X,x}$ (mittels $f^{\#}$) ein flacher $\mathcal{O}_{U,u}$-Modul ist.
- *étale* in x, falls f unverzweigt und flach in x ist.

Ein Morphismus $f : X \longrightarrow U$ ist *unverzweigt* / *flach* / *étale*, wenn er es an jedem Punkt $x \in X$ ist.

Ein Morphismus $f : X \longrightarrow U$ ist eine *étale Überlagerung*, falls er étale und endlich ist.

Definition Wir nennen ein Schema X *ganz*, falls X irreduzibel und reduziert ist. Wir erinnern daran, dass dies äquivalent zu der Bedingung ist, dass für alle offenen $U \subseteq X$ der Ring $\mathcal{O}_X(U)$ ein Integritätsbereich ist.

Im Folgenden werden wir uns nur mit endlichen, normalen Überlagerungen von normalen, zusammenhängenden Schemata beschäftigen. (Ein Schema ist *normal*, wenn alle seine lokalen Ringe normale Integritätsbereiche sind. Falls das Schema ganz ist, ist dies äquivalent dazu, dass alle affinen Teilschemata durch normale Ringe definiert sind. [Mu, III, 8, Text nach Definition 1, Fußnote]) Ein normales Schema ist insbesondere reduziert und seine Zusammenhangskomponenten sind irreduzibel. Ein Schema ist also genau dann normal und zusammenhängend wenn es normal und ganz ist. Anstelle von normalen, zusammenhängenden Schemata sprechen wir im Folgenden von normalen, ganzen Schemata.

Sei im Folgenden U stets ein normales, ganzes Schema. Sei $K = \kappa(U)$ der Funktionenkörper.

Definition Sei X ein normales, ganzes Schema und $f : X \longrightarrow U$ ein endlicher, dominanter Morphismus. Dann nennen wir f eine *endliche, normale, ganze Überlagerung* von U. (Wir sagen dann auch, dass X eine endliche, normale, ganze Überlagerung von U ist.)

Sei X ein normales Schema (nicht notwendiger Weise ganz). Dann nennen wir einen Morphismus $f : X \longrightarrow U$ eine *endliche, normale Überlagerung*, wenn f endlich und auf jeder Zusammenhangskomponente von X dominant ist.

Bemerkung Aus dem Going-up Theorem [Ei, Proposition 4.15] folgt, dass ein endlicher Morphismus abgeschlossen ist. Somit ist eine endliche, normale Überlagerung stets surjektiv auf jeder ihrer Zusammenhangskomponenten.

Da 'endlich' stabil unter Basiswechsel ist, ist eine endliche, normale Überlagerung $X \longrightarrow U$ sogar universell abgeschlossen. Aus dem Bewertungskriterium folgt, dass affine Morphismen separiert sind. Eine endliche, normale Überlagerung ist also eigentlich. Komposita von separierten Morphismen sind separiert und Komposita von eigentlichen Morphismen sind eigentlich. (Bewertungskriterium) Wenn U ein separiertes S-Schema ist, so ist auch X ein separiertes S-Schema. Analog ist X ein eigentliches S-Schema, wenn U eines ist.

Folgendes Lemma ist im Weiteren fundamental:

Lemma 3.1 *Sei $f : X \longrightarrow U$ unverzweigt und auf jeder Zusammenhangskomponente von X dominant. Dann ist f étale. Weiterhin ist dann X normal.*

Beweis. Ohne Einschränkung kann man annehmen, dass X zusammenhängend ist. Siehe nun [SGA I, I, Corollaire 9.10, Corollaire 9.11]. □

Flache (und somit auch étale Morphismen) sind offen. [SGA I, IV, Théorème 6.6] Aus dem zweiten Teil des Lemmas folgt, dass étale Überlagerungen über dem normalen ganzen Schema U endliche, normale Überlagerungen im Sinne obiger Definition sind.

Normalisierungen in endlichen Körpererweiterungen

Definition (Nach [Mu, III.8, Definition 3]) Sei $K \longrightarrow L$ eine endliche Erweiterung des Funktionenkörpers von U. Eine *Normalisierung* von U in L ist eine endliche, normale, ganze Überlagerung $X \longrightarrow U$, mit $\kappa(X) = L$, so dass die induzierte Abbildung $\kappa(U) \hookrightarrow \kappa(X)$ gleich der vorgegebenen Inklusion $K \hookrightarrow L$ ist.

Proposition 3.2 *Falls die Normalisierung existiert, ist sie eindeutig im folgenden Sinne: Wenn $X_1 \longrightarrow U$ und $X_2 \longrightarrow U$ zwei Normalisierungen von U in L sind, dann gibt es einen U-Isomorphismus zwischen X_1 und X_2, der auf L die Identität induziert.*

Die Normalisierung existiert in den folgenden Fällen:

- *$L|\kappa(U)$ ist endlich separabel*
- *U ist ein k-Schema (k ein Körper) und $L|\kappa(U)$ ist endlich beliebig (dabei muss U nicht normal sein)*

Beweis. Skizze nach [Mu, III.8 Theorem 3]:

Eindeutigkeit Es ist klar, dass für affine Schemata Spek(R) die Normalisierung durch die Normalisierung von R in L zu definieren ist. Dies ist die Eindeutigkeit für affine Schemata. Da jedes Schema durch affine Schemata überdeckt wird, ergibt sich daraus die Eindeutigkeit für beliebige Schemata.

Existenz Für affine Schemata ist zu zeigen, dass die Normalisierung eines Ringes in einem Körper unter den angegebenen Bedingungen endlich ist. Dies folgt aus dem Beweis von [Ne, I, Satz (8.1) mit Lemma (2.9)] und [ZS, vol I,V,4, Theorem 9]. Aus der Existenz und Eindeutigkeit für affine Schemata ergibt sich die Existenz für beliebige Schemata. Denn die Normalisierungen von offenen affinen Teilen können aufgrund der Eindeutigkeit 'zusammengeklebt' werden. □

Aufgrund der Eindeutigkeit bezeichnen wir die Normalisierung von U in L mit $\mathcal{N}_U(L)$. Aus der Eindeutigkeit der Normalisierung folgt, dass jede endliche, normale, ganze Überlagerung $X \longrightarrow U$ isomorph zur Normalisierung von U im Funktionenkörper $\kappa(X)$ ist. Aus der Eindeutigkeit folgt ferner, dass die Normalisierung in den beiden angegebenen Fällen einen kontravarianten Funktor definiert. Genauer gilt im ersten Fall:

Sei $K = \kappa(U)$ der Funktionenkörper des normalen, ganzen Schemas U. Normalisierung definiert einen Funktor von der Kategorie der endlichen separablen Körpererweiterungen von K in die Kategorie der endlichen, normalen, ganzen Überlagerungen von U, deren Funktionenkörper separabel ist. Die letzte Bedingung besagt gerade, dass die endlichen, normalen, ganzen Überlagerungen unverzweigt am generischen Punkt sein sollen. Normalisierung definiert nach Konstruktion zusammen mit dem Funktionenkörperfunktor eine kontravariante Äquivalenz von Kategorien.

$$\left\{\begin{array}{l}\text{Objekte:}\\ \text{Endliche, normale, ganze}\\ U\text{-Überlagerungen,}\\ \text{unv. am generischen Punkt}\\ \text{Morphismen:}\\ \text{Überlagerungen, die}\\ U\text{-Schemamorphismen sind}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Objekte:}\\ \text{Endliche, separable}\\ \text{Erweiterungen von } K\\ \text{Morphismen:}\\ \text{endliche}\\ K\text{-Körperhomomorphismen}\end{array}\right\}$$

$$\begin{array}{ccc} \mathcal{F}_K : X \longrightarrow U & \to & K \longrightarrow \kappa(X) \\ \mathcal{N}_U(L) \longrightarrow U & \leftarrow & K \longrightarrow L : \mathcal{N}_U \end{array}$$

Sei Ω ein algebraisch abgeschlossener Oberkörper von $K = \kappa(U)$. Wenn man auf der linken Seite zusätzlich fordert, dass die Funktionenkörper der Überlagerungen in Ω eingebettet sind, und auf der rechten Seite fordert, dass die endlichen Körpererweiterungen alle in Ω liegen, so erhält man wieder eine kontravariante Äquivalenz von Kategorien.

Wenn X und Y étale U-Überlagerungen sind und $X \longrightarrow Y$ ein U-Morphismus ist, so ist $X \longrightarrow Y$ nach [SGA I, I, Corollaire 4.8.] étale und auch endlich, wie man sich leicht überlegt.

Sei $\mathcal{E}t(U)$ die Kategorie mit Objekten: zusammenhängende, étale Überlagerungen von U und Morphismen: étale Überlagerungen, welche U-Morphismen sind, wobei die Funktionenkörper in Ω liegen. Sei $\mathcal{K}(U)$ die Kategorie der endlichen Erweiterungungen L von K in Ω, wobei die Normalisierung von U in L über U unverzweigt ist. (Diese Erweiterungen sind automatisch separabel.)

Die Kategorie $\mathcal{E}t(U)$ ist eine volle Unterkategorie der obigen linken Kategorie, während $\mathcal{K}(U)$ eine volle Unterkategorie der rechten Kategorie ist. Die Funktoren $\mathcal{F}_K$ und $\mathcal{N}_U$ definieren eine Äquivalenz zwischen den beiden Kategorien:

- Eine étale Überlagerung $X \longrightarrow U$ ist insbesondere unverzweigt, und die Erweiterung der Funktionenkörper liegt demnach in $\mathcal{K}(U)$.

- Wenn andererseits $K \longrightarrow L$ in $\mathcal{K}(U)$ liegt, definiert die Normalisierung eine étale Überlagerung von U. Denn: Die Normalisierung ist dominant und außerdem unverzweigt nach Voraussetzung. Das Resultat folgt aus Lemma 3.1.

Sei Y normal und ganz, und sei S ein abgeschlossenes Teilschema. Dann ist die Kategorie $\mathcal{E}t(Y - S)$ der zusammenhängenden, étalen Überlagerungen von $Y - S$ auch äquivalent zur Kategorie der endlichen, normalen, ganzen, außerhalb S étalen Überlagerungen von Y (wobei die Funktionenkörper in Ω liegen).

Die Äquivalenz ist auf Objekten folgendermaßen gegeben: Sei $X \longrightarrow Y - S$ zusammenhängend, étale. Bilde die Normalisierung von Y in $\kappa(X)$. Sei andererseits $X \longrightarrow Y$ normal, ganz und étale außerhalb S. Schränke dies auf $Y - S$

ein. Auf Morphismen ist die Äquivalenz analog durch Einschränken bzw. über den Umweg des Funktionenkörpers gegeben.

Die Äquivalenz ist klar, da beide Funktoren die entsprechenden Erweiterungen der Funktionenkörper nicht ändern, endliche, normale, ganze Überlagerungen von normalen Schemata aber durch die Erweiterungen der Funktionenkörper eindeutig bestimmt sind.

Wir wollen zeigen, dass $\mathcal{K}(U)$ mit zwei Körpern auch deren Kompositum in Ω enthält. Dann bilden die Objekte in $\mathcal{K}(U)$ mit Inklusionen in Ω ein direktes System.

Normalisierungen in reduzierten endlichen Algebren

Definition Sei X ein reduziertes aber nicht notwendigerweise irreduzibles Schema. Der *Ring der rationalen Funktionen* oder kürzer der *Funktionenring* von X ist der induktive Limes aller Ringe $\mathcal{O}_X(V), V$ offen in X.

$$\mathcal{F}(X) := \varinjlim \mathcal{O}_X(V)$$

Man sieht sofort: Falls X die irreduziblen Komponenten $X_1, ..., X_r$ hat, so ist $\mathcal{F}(X) = \kappa(X_1) \oplus \cdots \oplus \kappa(X_k)$.

Wir erweitern die Definition der Normalisierung:

Definition Sei weiterhin U ein normales, ganzes Schema, $K := \kappa(U) \longrightarrow A$ eine endliche reduzierte Algebra, (d.h. das Nilradikal von A ist Null). Dann ist eine *Normalisierung* von U in A eine endliche, normale Überlagerung mit Funktionenring A.

Dabei sei noch einmal betont, dass eine endliche, normale Überlagerung des normalen, ganzen Schemas U nach Definition auf jeder Irreduzibilitätskomponente dominant ist.

Sei A eine endliche, separable K-Algebra, d.h. $A \otimes_K \overline{K}$ sei reduziert. Nach dem Chinesischen Restsatz ist A als K-Algebra isomorph zu $L_1 \oplus \cdots \oplus L_r$, wobei die L_i irreduzible, geometrisch reduzierte, endliche K-Algebren, mit einem Wort: endliche, separable Körpererweiterungen von K sind.

In diesem Fall existiert die Normalisierung stets und ist eindeutig. Die disjunkte Summe der Normalisierungen von U in den Körpererweiterungen $L_i|K$ hat die gewünschten Eigenschaften. Auf affinen, offenen Teilen Spek$R \subseteq U$ ist die Normalisierung genau wie im Fall einer endlichen Körpererweiterung des Funktionenkörpers durch die Normalisierung von R im Ring A definiert.

Die Funktoren 'Funktionenring' und 'Normalisierung' definieren eine kontravariante Äquivalenz zwischen den Kategorien der endlichen, normalen Überlagerungen von U, die an den generischen Punkten unverzweigt sind, und der Kategorie der endlichen separablen Algebren über K.

Definition der Fundamentalgruppe normaler Schemata

Proposition 3.3 *Die Menge der Objekte von $\mathcal{K}(U)$ hat die Eigenschaft, dass sie mit zwei Körpererweiterungen auch deren Kompositum in Ω enthält. Insbesondere enthält sie mit einer Erweiterung auch deren galoissche Hülle.*

Beweis. Wenn U ein normales, ganzes Schema ist und L_1 und L_2 endliche Erweiterungen vom Funktionenkörper K sind, wobei $L_2|K$ separabel ist, so ist nach Proposition 1.12 $L_1 \otimes_K L_2$ eine endliche Summe von endlichen separablen Körpererweiterungen von L_1.

Die Bedingung 'étale' ist stabil unter Basiswechsel. [SGA I, I, Proposition 4.6.] Sei U ein normales, ganzes Schema mit Funktionenkörper K. Seien X_1, X_2 endliche, normale, ganze Überlagerungen von U, wobei $X_2 \longrightarrow U$ unverzeigt (étale) sei. Dann ist der Morphismus $X_1 \times_U X_2 \longrightarrow X_1$ étale und somit (weil auch endlich) eine étale Überlagerung.

Seien L_1, L_2 die Funktionenkörper von $\kappa(X_1), \kappa(X_2)$. Dann ist die étale (und somit normale) Überlagerung $X_1 \times_U X_2 \longrightarrow X_1$ gleich der Normalisierung von X_1 in der Algebra $L_1 \otimes_K L_2$. (Dies ist die 'Propriété de translation' in [SGA I, Proposition 1.10.4. (iii)].)

Nach Proposition 1.12 ist jedes Kompositum L_1L_2 von L_1 und L_2 gleich einer irreduziblen Komponente von $L_1 \otimes_K L_2$. Damit ist die Normalisierung X von X_1 in L_1L_2 gleich einer Zusammenhangskomponente von $X_1 \times_U X_2 \longrightarrow X_1$ und somit unverzeigt über X_1. Wenn nun außerdem $X_1 \longrightarrow U$ als unverzweigt vorausgesetzt wird, so ist X über U unverzeigt. $\Box$

Sei $M(U)$ das Kompositum aller Körper aus $\mathcal{K}(U)$ im festen algebraisch abgeschlossenen Körper Ω. Also

$$M(U) := \varinjlim_{L \in \mathcal{K}(U)} L = \varinjlim_{\substack{L \in \mathcal{K}(U) \\ L|K \text{ galoissch}}} L,$$

wobei die Morphismen des direkten Limes die Inklusionen in Ω sind. $M(U)|K$ ist galoissch. Wir definieren nun die *étale Fundamentalgruppe von U mit Werten in* Ω durch

$$\pi_1(U) = \pi_1(U, \Omega) := \mathrm{Gal}(M(U)|K) = \varprojlim_{\substack{L \in \mathcal{K}(U) \\ L|K \text{ galoissch}}} \mathrm{Gal}(L|K)$$

Falls der Grundkörper k algebraisch abgeschlossen ist, so sprechen wir anstatt von der étalen Fundamentalgruppe auch von der *geometrischen Fundamentalgruppe von U*.

Nach Konstruktion gibt es eine Bijektion zwischen den Isomorphieklassen der étalen zusammenhängenden Überlagerungen von U und den Konjugationsklassen der offenen Untergruppen (abgeschlossenen Untergruppen mit endlichem Index) von $\pi_1(U)$.

Die Fundamentalgruppe von Kurven

Sei k ein beliebiger Körper. Eine k-*Varietät* ist ein reduziertes, separiertes Schema über k (wie immer von endlichem Typ). Eine k-*Kurve* ist eine k-Varietät von Dimension 1.

Der Funktor 'Funktionenkörper' definiert eine kontravariante Äquivalenz zwischen der Kategorie der normalen, ganzen, eigentlichen k-Kurven und der Kategorie der Funktionenkörper, d.h. der endlich erzweugten Erweiterungen von Transzendenzgrad 1. (Dedekind-Weber Äquivalenz) Den Umkehrfunktor bezeichnen wir in Anlehnung an die Normalisierung mit $\mathcal{N}$.

$$\left\{\begin{array}{l}\text{Eigentliche, normale,}\\ \text{ganze } k\text{-Kurven mit}\\ \text{nicht konstanten}\\ k\text{-Morphismen}\end{array}\right\} \longleftrightarrow \left\{\begin{array}{l}\text{Funktionenkörper}\\ \text{über } k \text{ mit}\\ k\text{-Körper-}\\ \text{homomorphismen}\end{array}\right\}$$

$$\mathcal{F} : X \qquad \mapsto \qquad \kappa(X)$$

Insbesondere kann man jedem Funktionenkörper K ein *Modell* zuordnen. Dies ist eine eigentliche, normale, ganze k-Kurve Y mit $\kappa(Y) \cong_k K$. Nach Proposition 3.2 kann man ein Modell zu $K|k$ folgendermaßen konstruieren: Wähle ein transzendentes Element $t \in K|k$. Damit erhält man eine Erweiterung $K|k(t)$. Der rationale Funktionenkörper $k(t)|k$ ist der Funktionenkörper der projektiven Geraden. Sei Y die Normalisierung von $\mathbf{P}^1_k$ in K.

Sei $K|k$ ein Funktionenkörper, Y ein Modell von $K|k$. Wenn y ein abgeschlossener Punkt von Y ist, so ist der lokale Ring $\mathcal{O}_{Y,y}$ ein Bewertungsring und definiert eine Primstelle von $K|k$. Die Zuordnung $y \mapsto \mathcal{O}_{Y,y}$ definiert eine Bijektion zwischen der Menge der abgeschlossenen Punkte von Y und der Menge der Primstellen von $K|k$. Eine endliche Erweiterung $K \longrightarrow L$ ist genau dann an einer Primstelle verzweigt, wenn die zugehörige endliche, normale, ganze Überlagerung $\mathcal{N}_Y(L) \longrightarrow Y$ am entsprechenden Punkt verzweigt ist.

Sei S eine endliche Menge von abgeschlossenen Punkten in einer eigentlichen, normalen, ganzen Kurve Y. Sei $U := Y - S$ das Komplement von S. Die zu S gehörige Menge von Primstellen werde wieder mit S bezeichnet. Sei wie in Kapitel 2 $\mathcal{K}_S(K)$ die Kategorie der in Ω enthaltenen endlichen außerhalb S unverzweigten Erweiterungen. Wir wiederholen, dass die außerhalb S unverzweigten Erweiterungen $L|K$ automatisch separabel sind. Die Normalisierung von U in L ist also unverzweigt am generischen Punkt. Damit ist $\mathcal{K}_S(K) = \mathcal{K}(U)$. Sei wie im vorigen Kapitel $M_S(K)$ die maximale außerhalb S unverzweigte Erweiterung von K. Dann ist $M_S(K) = M(U)$ und somit

$$\pi_1(U) = \varprojlim_{\substack{L \in \mathcal{K}_S(Y) \\ L|K \text{ galoissch}}} \operatorname{Gal}(L|K) = \operatorname{Gal}(M_S(K)|K).$$

3.2 Die Fundamentalgruppe beliebiger Schemata

Die Fundamantalgruppe in der algebraischen Topologie

In der algebraischen Topologie definiert man die Fundamentalgruppe eines wegzusammenhängenden, lokal wegzusammenhängenden, semi-lokal-einfachzusammenhängenden topologischen Raumes U - z.B. einer zusammenhängenden Mannigfaltigkeit - entweder durch Homotopieklassen von punktierten Wegen oder als das Opunierte der Automorphismengruppe (über U) einer universellen Überlagerung. Wenn man zwei verschiedene universelle Überlagerungen wählt, steht die Menge der Homöomorphismen zwischen diesen universellen Überlagerungen in Bijektion zur Menge der Elemente der Fundamentalgruppe. Wenn man einen Homöomorphismus fest wählt, definiert jeder andere einen inneren Automorphismus auf der Fundamentalgruppe. Diese Nichteindeutigkeit wird beseitigt, wenn man die Fundamentalgruppe in der Kategorie der punktierten Räume definiert. Es gibt bis auf eindeutige Homöomorphie genau eine punktierte universelle Überlagerung. Nach Wahl einer solchen punktierten universellen Überlagerung ist die Fundamentalgruppe eindeutig bestimmt.

Ein anderer Zugang zur topologischen Fundamentalgruppe besteht im sogenannten *Faserfunktor*. Hierzu wählt man wieder einen Punkt $a \in U$. $F_a : \mathcal{E}t(U) \longrightarrow \mathcal{E}ns$ ordnet jeder Überlagerung $X \longrightarrow U$ die Faser $F_a(X)$ über a zu. U-Überlagerungen $X \longrightarrow Y$ werden dabei die Faser eingeschränkt. Der Faserfunktor ist treu. Eine universelle Überlagerung $\widetilde{U}$ ist ein darstellendes Objekt, es gilt also $F_a \cong \mathrm{Hom}_U(\widetilde{U}, .)$, wobei der Isomorphismus wieder durch einen fest gewählten Punkt $\widetilde{a} \in F_a(\widetilde{U})$ gegeben ist. Damit ist die Automorphismengruppe des Faserfunktors isomorph zur Automorphismengruppe des Funktors $\mathrm{Hom}_U(\widetilde{U}, .)$, also $\mathrm{Aut}(\widetilde{U}\ |U)$, dem Opunierten der Fundamentalgruppe von U (Yoneda-Lemma).

Geometrische Punkte auf Schemata

Sei U ein beliebiges zusammenhängendes Schema. Sei $u \in U$ ein topologischer Punkt. Der Faserfunktor F_u von der Kategorie der étalen Überlagerungen in die Kategorie der endlichen Mengen ist nun i.A. nicht treu. (Z.B. wenn U das Spektrum eines nicht-separabel abgeschlossenen Körpers ist). Dies wird anders, wenn man den Faserfunktor anstatt mittels eines topologischen Punktes mittels eines geometrischen Punktes definiert.

Definition Sei U ein beliebiges Schema, Ω ein algebraisch abgeschlossener Körper. Ein *geometrischer Punkt* ist ein Morphismus $\mathrm{Spek}(\Omega) \longrightarrow U$. Dies ist nichts anderes als ein topologischer Punkt $u \in U$ mit einer Einbettung $\kappa(u) \hookrightarrow \Omega$.

Allgemeiner ist ein *T-wertiger* Punkt (T ein beliebiges Schema) ein Morphismus $T \longrightarrow U$. Die Menge der T-wertigen Punkte wird mit $U(T)$=Hom(T, U) bezeichnet. Für festes T definiert das Bilden der T-wertigen Punkte einen kovarianten Funktor.

Die Idee eines punktierten Raumes überträgt sich von der algebraischen Topologie auf die algebraische Geometrie. Sei Ω ein algebraisch abgeschlossener Körper. Ein *punktiertes Schema* ist ein Tupel (U, a), wobei a ein geometrischer Punkt ist. Dementsprechend ist ein Morphismus von punktierten Schemata ein Diagramm

$$\begin{tikzcd} \mathrm{Spek}(\Omega) \arrow[r] \arrow[d, equal] & X \arrow[d] \\ \mathrm{Spek}(\Omega) \arrow[r] & U. \end{tikzcd}$$

Definition der Fundamentalgruppe beliebiger Schemata

Definition Sei U ein festes zusammenhängendes Schema und a ein geometrischer (Ω-wertiger) Punkt. Sei $f : X \longrightarrow U$ eine étale Überlagerung. Die *Faser von a in X* ist das Urbild von a in $X(\Omega)$.

$$F_a(U) := f(\Omega)^{-1}(a)$$

Der *Faserfunktor* F_a von U an a ist ein Funktor von der Kategorie der étalen Überlagerungen von U in die Kategorie der endlichen Mengen. Er ordnet jeder étalen Überlagerung von U die Faser über a zu. Etale Überlagerungen $g : X \longrightarrow Y$ über U werden auf die Einschränkung von $g(\Omega)$ auf $F_a(X)$ abgebildet.[1]

Der Faserfunktor ist treu (Wenn X eine étale U-Überlagerung ist, so liegt in jeder Zusammenhangskomponente von X ein geometrischer Punkt über a. Damit kann man [SGA I, I, Corollaire 5.4.] anwenden.)

Man definiert in Analogie zur topologischen Fundamentalgruppe:

Definition Sei (U, a) ein zusammenhängendes, punktiertes (noethersches) Schema. Dann ist die *Fundamentalgruppe von U mit Basispunkt a* die zur Automorphismengruppe des Faserfunktors F_a opunierte Gruppe.

$$\pi_1(U, a) := \mathrm{Aut}(F_a)^{op}$$

Da étale Überlagerungen definitionsgemäß endlich sind, gibt es i.A. keine universelle étale Überlagerung, und deshalb ist der Faserfunktor i.A. auch nicht darstellbar. Er ist aber strikt pro-darstellbar, d.h. es gibt ein projektives System $P = (P_i)_{i \in I}$ mit

$$F_a \cong \varinjlim_i \mathrm{Hom}_U(P_i, .), \tag{3.1}$$

[1] Die Notation $f(\Omega)$ ist nicht Standard. Meine Idee war: Wenn ...(Ω) ein Funktor ist, sollte man die von f induzierte Abbildung von $X(\Omega)$ nach $U(\Omega)$ mit $f(\Omega)$ bezeichnen. Das ist natürlich problematisch, da $f(\Omega)$ schon das Bild von Ω unter f bezeichnet. Die Bezeichnung f_* wäre in Ordnung, man schreibt aber einfach f.

wobei dieser Isomorphismus durch ein Element

$$\rho \in \varprojlim_i F_a(P_i)$$

gegeben ist. Dabei sind die Morphismen des projektiven Systems P epi. [SGA I, V, 3 c)]

Um auszunutzen, dass der Faserfunktor pro-darstellbar ist, müssen wir wissen, was eine galoissche Überlagerung ist. [SGA I, Exposé V 1-3]

Galoissche Überlagerungen

Definition Sei X ein Schema, G eine endliche Gruppe, die auf X operiert. Ein *Quotientenschema von X nach G* ist ein Schema X/G mit einem G-invarianten Morphismus $X \longrightarrow X/G$ und folgender universeller Eigenschaft: Wenn $f : X \longrightarrow Z$ ein G-invarianter Morphismus ist, so gibt es genau einen Morphismus $X/G \longrightarrow Z$, so dass das Diagramm

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d] & Z \\ X/G \arrow[ur] & \end{tikzcd}$$

kommutiert.

Wenn $X \longrightarrow U$ ein G-invarianter affiner Morphismus ist, so existiert das Quotientenschema stets. (Man kann X durch G-invariante affine Mengen überdecken - nämlich die Urbilder von affinen Mengen von U. Die Existenz folgt aus [SGA I, IV, Proposition 1.8].) Falls $X \longrightarrow U$ eine étale Überlagerung ist, dann sind auch die Morphismen $X \longrightarrow X/G$ und $X/G \longrightarrow U$ étale Überlagerungen. [SGA I, V, Proposition 2.2., Corollaire 1.5.; Corollaire 3.4.]

Definition Sei $X \longrightarrow U$ ein G-invarianter Morphismus. Der Stabilisator eines topologischen Punktes $x \in X$ heißt *Zerlegungsgruppe* von x, Bezeichnung $G(x)$. Der Stabilisator eines geometrischen Punktes über x heißt *Trägheitsgruppe* von x (Definition ist unabhängig von der Wahl des geometrischen Punktes über x), Bezeichung $I(x)$.

Wenn $K|k$ ein Funktionenkörper, $L|K$ eine galoissche Erweiterung und $X \longrightarrow U$ die entsprechende endliche, normale, ganze Überlagerung von Modellen ist, so stimmen diese Gruppen unter der Bijektion von Primstellen und Punkten genau mit den in der Bewertungstheorie definierten überein.

Definition Sei $X \longrightarrow U$ eine G-invariante étale Überlagerung, U das Quotientenschema von X nach G, und es gelte: Wenn X_0 eine Zusammenhangskomponente von X ist und für ein $g \in G$ $g|_{X_0} = id_{X_0}$ gilt, so ist g das neutrale Element in G. Wir sagen dann, der Morphismus $X \longrightarrow U$ sei eine *galoissche Überlagerung* mit *Galoisgruppe G*.

Dies ist äquivalent zu Definition 2.7. (eigentlich 2.8.) in [SGA I, Exposé V]. Dort heißt ein endlicher G-invarianter Morphismus $X \longrightarrow U$ galoissch mit Galoisgruppe G, wenn $X/G = U$ ist und alle Trägheitsgruppen trivial sind. Die Äquivalenz dieser beiden Definitionen folgt aus dem Spezialfall, dass X zusammenhängend ist, siehe dazu [SGA I, V, Corollaire 2.4.] Falls X zusammenhängend ist, dann ist die Automorphismengruppe von $X \longrightarrow U$ gleich G. [SGA I, V, Corollaire 2.4.]

Sei nun U ein *normales*, ganzes Schema und $X \longrightarrow U$ eine étale, ganze G-invariante Überlagerung. Dann ist die Inklusion $\kappa(X/G) \longrightarrow \kappa(X)$ $\kappa(G)$-invariant, d.h ihr Bild liegt in $\kappa(X/G)^{\kappa(G)}$. Andererseits ist die Überlagerung $X \longrightarrow \mathcal{N}(\kappa(X)^{\kappa(G)})$ G-invariant. Daraus folgen die kommutativen Diagramme

$$\begin{tikzcd} \kappa(X)^{\kappa(G)} \arrow[r] & \kappa(X) \\ \kappa(U) \arrow[u] \arrow[r] & \kappa(X/G) \arrow[u] \arrow[ul] \end{tikzcd} \qquad \begin{tikzcd} \mathcal{N}_U(\kappa(X)^{\kappa(G)}) \arrow[d] & X \arrow[l] \arrow[d] \\ U & X/G. \arrow[l] \arrow[ul] \end{tikzcd}$$

Durch Anwenden des Funktionenkörperfunktors auf das zweite Diagramm erhalten wir $\kappa(X/G) = \kappa(X)^{\kappa(G)}$. Aus dem ersten Diagramm folgt mit dem Normalisierungsfunktor $\mathcal{N}_U(\kappa(X)^{\kappa(G)}) = X/G$. Es gilt also $X \longrightarrow U$ ist galoissch mit Galoisgruppe $G \longleftrightarrow U = X/G \longleftrightarrow \kappa(X/G) = \kappa(U) \longleftrightarrow \kappa(X)^{\kappa(G)} = \kappa(U) \longleftrightarrow \kappa(X)|\kappa(U)$ ist galoissch mit Galoisgruppe $\kappa(G)$.

Also ist eine étale zusammenhängende Überlagerung $X \longrightarrow U$ über einem *normalen* Schema U genau dann galoissch, wenn die entsprechende Körpererweiterung galoissch ist. Die Galoisgruppe der Überlagerung stimmt mit der Automorphismengruppe überein und ist gleich dem Opunierten der Galoisgruppe der Körpererweiterung.

Berechnung der Fundamentalgruppe

Die étalen Überlagerungen in 3.1 können als galoissche Überlagerungen gewählt werden. Es ist

$$\pi_1(U,a) = \mathrm{Aut}(F_a)^{op} \cong \varprojlim_i \mathrm{Aut}(P_i)^{op}.$$

(siehe [SGA I, V,3 h) und V,7]) Insbesonderes ist die Fundamentalgruppe eine proendliche Gruppe. Sie werde mit der proendlichen Topologie versehen.

Die Fundamentalgruppe operiert auf der Faser jeder Überlagerung. Aus [SGA I, I, V f), g)] folgt, dass die Operation stetig ist. In [SGA I, I,V] wird gezeigt, dass die Kategorie der étalen Überlagerungen von U mittels dem Faserfunktor F_a kanonisch isomorph zur Kategorie der endlichen Mengen mit diskreter $\pi_1(U,a)$-Operation ist. (Diskret heißt, dass der Stabilisator jedes Elements offen ist.)

Die Fundamentalgruppen zu zwei verschiedenen geometrischen Punkten eines zusammenhängenden Schemas sind isomorph. Der Isomorphismus ist eindeutig bestimmt bis auf einen stetigen inneren Isomorphismus. [SGA I, I, Text nach Corollaire 5.7., 7] In dieser Arbeit ist mit *der* Fundamentalgruppe eines irreduziblen Schemas immer die Fundamentalgruppe bezüglich eines durch $\kappa(U) \longrightarrow \Omega$ gegebenen geometrischen Punktes über dem generischen Punkt gemeint.

Die Fundamentalgruppe als Funktor

Man kann das Bilden der étale Fundamentalgruppe zu einem Funktor von der Kategorie der punktierten, zusammenhängenden Schemata in die Kategorie der proendlichen Gruppen machen. Sei dazu $\alpha : (U, a) \longrightarrow (V, a')$ ein Morphismus punktierter Schemata. Aus der universellen Eigenschaft des Produkts folgt die dem Morphismus $U \longrightarrow V$ kanonisch zugeondnete natürliche Transformation

$$\mathrm{Hom}_U(\mathrm{Spek}(\Omega), U \times_V .) \cong \mathrm{Hom}_V(\mathrm{Spek}(\Omega), .)$$

und daraus eine $\alpha : (U, a) \longrightarrow (V, a')$ kanonisch zugeordnete natürliche Transformation

$$F_a(U \times_V .) \cong F_{a'}.$$

Sei $f = f_\alpha$ der Funktor, der einer étalen Überlagerung $Y \longrightarrow V$ die étale Überlagerung $U \times_V Y \longrightarrow U$ zuordnet. Es gibt also eine dem Morphismus $(U, a) \longrightarrow (V, a')$ kanonisch zugeondnete natürliche Transformation

$$F_a \circ f \cong F_{a'}, \tag{3.2}$$

Jeder Automorphismus von F_a definiert durch 'Einschränkung' auf Objekte der Form $f(Y \longrightarrow V) = (U \times_V Y \longrightarrow U)$ auch einen Automorphismus von $F_a \circ f$ und aufgrund von 3.2 auch eine natürliche Transformation von $F_{a'}$. 'Einschränken' ist verträglich mit der Gruppenstruktur der Automorphismengruppe des Faserfunktors. Man erhält einen Gruppenhomomorphismus

$$\pi_1(\alpha) : \pi_1(U, a) \longrightarrow \pi_1(V, a')$$

In [SGA I, V,6 und 7] wird gezeigt, dass dieser Homomorphismus *stetig* ist. Man überlegt sich, dass π_1 nun ein Funktor ist.

Äquivalenz der beiden Definitionen der Fundamentalgruppe normaler Schemata

Sei U ein normales, ganzes Schema, K der Funktionenkörper. Dann wird die oben angegebene Definition der Fundamentalgruppe für normale, ganze Schemata ein Spezialfall der abstrakteren Definition, wenn man als Basispunkt einen geometrischen Punkt über dem generischen Punkt, d.h eine Einbettung $a : K \longrightarrow \Omega$ festlegt. Als projektives System $(P_i)_{i \in I}$ wählt man alle zusammenhängenden, galoisschen Überlagerungen von U, deren Funktionenkörper in Ω liegt. Diese entsprechen genau den galoisschen, endlichen Erweiterungen L des

Funktionenkörpers K in Ω, wobei die Normalisierung von U in L unverzweigt ist - also den Objekten aus $\mathcal{K}(U)$. Somit gilt:

$$\pi_1(U,a) = \varprojlim_i \mathrm{Aut}(P_i)^{op} = \varprojlim_i \mathrm{Gal}(\kappa(P_i)|K) = \mathrm{Gal}(M(U)|K)$$

Beachte: $\mathcal{G}_r \longrightarrow \mathcal{G}_r, G \mapsto G^{op}, f \mapsto f$ definiert einen *kovarianten* Funktor auf der Kategorie der Gruppen.

Es gibt noch eine andere Möglichkeit, um die Isomorphie zu zeigen. (siehe [SGA I, V.8]) Sei wieder $a : K \longrightarrow \Omega$ ein geometrischer Punkt über dem generischen Punkt von U. Dann definiert $\mathrm{Spek}(\Omega) \longrightarrow \mathrm{Spek}(K)$ einen geometrischen Punkt a'. Damit ist $\pi_1(\mathrm{Spek}(K), a')$ kanonisch isomorph zu Γ_K. Man erhält einen Morphismus von punktierten Räumen $(\mathrm{Spek}(K), a') \longrightarrow (X, a)$. Dies definiert einen Morphismus

$$\Gamma_K = \pi_1(\mathrm{Spek}(K), a') \longrightarrow \pi_1(X, a).$$

Der Morphismus ist surjektiv und induziert einen Isomorphismus auf $\mathrm{Gal}(M(U)|K)$.

Trägheitsgruppen in der Fundamentalgruppe

Sei Y ein normales ganzes Schema, K der Funktionenkörper, S ein abgeschlossenes Unterschema aus Y und $U := Y - S$. Sei $P = (P_i)_{i \in I}$ das System von außerhalb S unverzweigten, endlichen, normalen, ganzen Überlagerungen von Y, deren Funktionenkörper in Ω liegt und galoissch über K ist. Dann gilt wieder $\pi_1(U) \cong \varprojlim_i \mathrm{Aut}(P_i)^{op}$.

Sei nun $y \in S$. Dann gibt es nach dem Zornschen Lemma ein System von Elementen $x = (x_i)_i \in (P_i)_{i \in I}$, so dass die Morphismen des projektiven Systems die x_i aufeinander abbilden und alle Elemente über y liegen. Die Gruppe $I(x) := \varprojlim_i I(x_i)$ heißt eine *Trägheitsgruppe von y (in der Fundamentalgruppe).*

Falls Y eine normale, ganze, eigentliche k-Kurve ist, so entspricht der endlichen Menge von abgeschlossenen Punkten S eine Menge von Primstellen auf $K|k$, die zu y gehörende Primstelle sei $\mathfrak{p}$. Dann stehen die projektiven Systeme von Punkten x über y in Bijektion zu den Erweiterungen $\mathfrak{P}$ von $\mathfrak{p}$ in $M_S|K$. Wenn $\mathfrak{P}$ die x entsprechende Erweiterung ist, so ist $I(x) = I_{\mathfrak{P}|\mathfrak{p}}(M_S|K)$.

3.3 Der Riemannsche Existenzsatz

Der Riemannsche Existenzsatz für vollständige Kurven

Wir studieren die Funktionenkörper und die normalen, ganzen Kurven über $\mathbf{C}$, dem Körper der komplexen Zahlen. Es sei daran erinnert, dass eine Kurve genau dann normal ist, wenn sie regulär ist (d.h. alle lokalen Ringe sind regulär). Über einen algebraisch abgeschlossenen Körper ist dies äquivalent dazu, dass die Kurve glatt ist, d.h. das Jacobi-Kriterium gilt. [Ha, I, Theorem 5.1.] (siehe auch

Proposition 3.10 in dieser Arbeit) Anstelle von normalen bzw. regulären Kurven spricht man dann auch von nicht-singulären Kurven.

Sei $\mathcal{K}$ die Kategorie der Funktionenkörper (von Transzendenzgrand 1) über $\mathbf{C}$. Sei $\mathcal{U}$ die Kategorie der eigentlichen (projektiven), normalen (nicht-sigulären) zusammenhängenden (ganzen) algebraischen $\mathbf{C}$-Kurven mit nicht-konstanten (dominanten) Morphismen. Sei $\mathcal{U}^{\text{klassisch}}$ die Kategorie der klassischen projektiven, nicht-singulären, irreduziblen Kurven, d.h. der in gewissen $\mathbf{P}^n_{\mathbf{C}}$ eingebetteten projektiven, nicht-singulären, irreduziblen algebraischen Mengen von Dimension 1. Sei schließlich $\mathcal{U}^{\text{an}}$ die Kategorie der kompakten Riemannschen Flächen (der kompakten, zusammenhängenden, 1-dimensionalen, komplexen Mannigfaltigkeiten) mit analytischen (verzweigten) Überlagerungen.

Es gibt mehrere natürliche Funktoren zwischen diesen Kategorien.

Der Funktionenkörperfunktor definiert eine kontravariante Äquivalenz zwischen $\mathcal{K}$ und $\mathcal{U}$. (Dedekind-Weber Äquivalenz) Der Funktionenkörperfunktor wird mit $\mathcal{F}$ und sein Inverses mit $\mathcal{N}$ bezeichnet.

Die Kategorie $\mathcal{U}$ ist äquivalent zur Kategorie $\mathcal{U}^{\text{klassisch}}$. Es gibt einen volltreuen essentiell surjektiven Funktor $\mathcal{U}^{\text{klassisch}} \longrightarrow \mathcal{U}$. [Ha, II, Proposition 4.10] Nach [Ja, Proposition 1.3] definiert das Einbetten jeder eigentlichen, glatten, ganzen $\mathbf{C}$-Kurve in einen $\mathbf{P}^n_{\mathbf{C}}$ einen Funktor, Bezeichnung $(\ )^{\text{klassisch}}$. (Insbesondere sind zwei Einbettungen derselben eigentlichen, glatten, ganzen $\mathbf{C}$-Kurve in der Kategorie $\mathcal{U}^{\text{klassisch}}$ isomorph.)

Man kann jede projektive, nicht-singuläre, irreduzible klassische Kurve *analytifizieren*. Der projektive Raum $\mathbf{P}^n_{\mathbf{C}}$ ist in natürlicher Weise eine komplexe Mannigfaltigkeit. Sei $X^{\text{klassisch}} \subseteq \mathbf{P}^n_{\mathbf{C}}$ eine projektive, nicht-singuläre, irreduzible klassische Kurve. Dann induziert die komplexe Struktur von $\mathbf{P}^n_{\mathbf{C}}$ eine komplexe Struktur auf $X^{\text{klassisch}}$.

Wir bezeichnen die Analytifizierung von $X^{\text{klassisch}}$ mit X^{an}. Da $X^{\text{klassisch}}$ als nicht-singulär und irreduzibel vorausgesetzt war, ist X^{an} eine kompakte Riemannsche Fläche.[2]

[2] Die Definition der komplexen Struktur und der Beweis, dass man eine Riemannsche Fläche erhält, ist nicht ganz einfach. Wir gehen deshalb genauer darauf ein: Wir bezeichnen der Einfachheit halber $X^{\text{klassisch}}$ mit X. Wir betrachten $\mathbf{P}^n_{\mathbf{C}}$ mit der starken Topologie (auch komplexe oder reelle Topologie genannt). Diesen Raum bezeichnen wir mit $(\mathbf{P}^n_{\mathbf{C}})^{\text{top}}$. Die starke Topologie induziert eine Topologie auf X; den entsprechenden topologischen Raum bezeichnen wir mit X^{top}. Es ist offensichtlich, dass X^{top} abgeschlossen in $(\mathbf{P}^n_{\mathbf{C}})^{\text{top}}$ und somit kompakt ist. Die komplexe Struktur auf X^{top} kann man mittels der folgenden beiden Zugänge erhalten:

Der erste Zugang beruht auf der Theorie der analytischen Räume (siehe beispielsweise Serre: Géometrie algébrique et géométrie analytique, Annales de l'Institut Fourier 6 (1959), p. 1 - 42 [Serre] und Exposé XII in SGA I in der Ausgabe von Springer (1971)). Man kann X in offensichtlicher Weise einen analytischen Raum X^{an} zuordnen. Dieser Raum ist genau wie X regulär und ein-dimensional (siehe Exposé XII, Proposition 2.1 in SGA I). Ein solcher Raum ist eine Riemannsche Fläche, siehe hierzu Abschnitt 4 in [Serre].

Der zweite Zugang benutzt weniger Theorie: Wir betrachten zuerst einen Punkt P auf

Auch Morphismen kann man analytifizieren: Seien $X^{\text{klassisch}} \subset \mathbf{P}^n, Y^{\text{klassisch}} \subset \mathbf{P}^m$ klassische, projektive, nicht-singuläre, irreduzible Kurven. Dann ist ein Morphismus zwischen $X^{\text{klassisch}}$ und $Y^{\text{klassisch}}$ durch einen Morphismus zwischen $\mathbf{P}^n_{\mathbf{C}}$ und $\mathbf{P}^m_{\mathbf{C}}$ gegeben, d.h. durch ein Tupel homogener Polynome gleichen Grades $(f_0, ..., f_m) \in k[X_0, ..., X_n]$. Diese definieren analytische Morphismen zwischen X^{an} und Y^{an}.[3]

Insgesamt haben wir einen Funktor $\mathcal{U}^{\text{klassisch}} \longrightarrow \mathcal{U}^{\text{an}}$. Durch Verknüpfung dieses Funktors mit dem Einbettungsfunktor $(\ )^{\text{klassisch}}$ erhalten wir einen Funktor $(\ )^{\text{an}} : \mathcal{U} \longrightarrow \mathcal{U}^{\text{an}}$, den *Analytifizierungsfunktor.*

Desweiteren gibt es den kontravarianten Funktor $\mathcal{M}$, der jeder kompakten Riemannschen Fläche den Körper der meromorphen Funktionen (also der holomorphen Abbildungen auf die Riemannsche Zahlenkugel $\boldsymbol{\mathcal{P}}^1$) zuordnet. Ein Morphismus $\phi : \mathcal{X} \longrightarrow \mathcal{Y}$ wird auf den 'Rückziehmorphismus' $\mathcal{M}(\phi) : \mathcal{M}(\mathcal{Y}) \longrightarrow \mathcal{M}(\mathcal{X}) : g \mapsto g \circ \phi$ abgebildet.

Insgesamt erhalten wir folgendes Diagramm:

$$\begin{tikzcd}
\mathcal{U}^{\text{an}} \arrow[rr, bend left, "\mathcal{M}"] & \mathcal{U} \arrow[l, "(\ )^{\text{an}}"'] \arrow[r, shift left, "\mathcal{F}"] & \mathcal{K} \arrow[l, shift left, "\mathcal{N}"]
\end{tikzcd}$$

Sei X eine projektive, nicht-singuläre zusammenhängende Kurve. Dann sind alle analytischen Morphismen von X^{an} nach $\boldsymbol{\mathcal{P}}^1$ algebraisch. Dies sieht man fol-

---

X und ein uniformisierendes Element f an P. Dieses Element definiert einen Morphismus $f : X \longrightarrow \mathbf{P}^1_{\mathbf{C}}$, der an P étale ist. Somit gibt es eine Umgebung U von $f(P)$, Polynome $f_1, \ldots, f_m \in \mathbf{C}[z][y_1, \ldots, x_m]$ und offene Einbettungen $U \hookrightarrow \mathbf{A}^1_{\mathbf{C}}$, $f^{-1}(U) \hookrightarrow V(f_1, \ldots, f_m)$, so dass das Diagramm

$$\begin{tikzcd}
f^{-1}(U) \arrow[r, hook] \arrow[d, "f"] & V(f_1, \ldots, f_m) \arrow[d, "z"] \\
U \arrow[r, hook] & \mathbf{A}^1_{\mathbf{C}}
\end{tikzcd}$$

kommutiert und das Jacobi-Kriterium im Bild von P gilt, d.h. $\det(((\frac{\partial f_i}{\partial y_j}))_{i,j})(P) \neq 0$ ist (siehe [Mu, III.5]). Wir bezeichnen hier das Bild von P in $V(f_1, \ldots, f_m)$ wieder mit P. Nach dem Satz über implizit definierte Funktionen (siehe Theorem 7.6 in Fritzsche, Grauert: From Holomorphic Functions to Complex Manifolds, Springer Verlag, 2002) gibt es offene Mengen U_1, U_2 in $\mathbf{C}$ bzw. in $\mathbf{C}^m$ und eine holomorphe Abbildung $g : U_1 \longrightarrow (U_2 \cap V(f_1, \ldots, f_m))$, so dass $U_1 \times U_2$ eine Umgebung von P in $\mathbf{C}^{m+1}$ und $V(f_1, \ldots, f_m) \cap (U_1 \times U_2) = \text{Graph}(g)$ ist. Somit ist $(z, g) : U_1 \longrightarrow U_1 \times U_2$ ein lokales Inverses zu z bezüglich der starken Topologie. Dies zeigt, dass f auf einer Umgebung von P in X^{top} eine bijektive Abbildung definiert. Die Abbildung f entsteht durch Einschränkung einer holomorphen Abbildung auf einer offenen Teilmenge von $(\mathbf{P}^1_{\mathbf{C}})^{\text{top}}$, und die (lokale) Umkehrabbildung ist holomorph. Wir fixieren nun für jeden Punkt eine geeingete Umgebung und so ein f. Diese definieren einen Atlas auf X^{top}. Die Verknüpfungen des Inversen einer Kartenabbildung mit einer Kartenabbildung (auf dem entsprechend eingeschränkten Definitionsbereich) ist offensichtlich wieder holomorph. Somit haben wir einen holomorphen Atlas auf X^{top}. Wir erhalten eine Riemannsche Fläche.

[3]Dies stimmt nicht ganz: Morpismen sind lokal so gegeben. Dies macht hier jedoch keinen Unterschied.

gendermaßen: Die Aussage ist für die projektive Gerade richtig. Es ist $\mathcal{M}(\mathcal{P}^1) = \mathcal{F}(\mathbf{P}^1_{\mathbf{C}}) \cong \mathbf{C}(t)$. (Dabei entspricht t der Identität auf $\mathbf{P}^1_{\mathbf{C}}$, wenn die Elemente aus dem Funktionenkörper einer ganzen $\mathbf{C}$-Kurve mit Morphismen nach $\mathbf{P}^1_{\mathbf{C}}$ identifiziert werden.) Wähle eine endliche, normale, ganze Überlagerung $\pi : X \longrightarrow \mathbf{P}^1_{\mathbf{C}}$ (mittels der Dedekind-Weber Äquivalenz). Diese endliche, normale, ganze Überlagerung habe Grad n. Dann hat auch die entsprechende Erweiterung $\mathcal{F}(X)|\mathbf{C}(t)$ Grad n. Die Überlagerung $\pi^{\mathrm{an}} : X^{\mathrm{an}} \longrightarrow \mathcal{P}^1$ hat auch Grad n, da sich der Grad der Überlagerung beim Analytifizieren nicht ändert. Jedes Element $f \in \mathcal{M}(X^{\mathrm{an}})$ erfüllt eine Polynomgleichung von Grad n:

$$f^n + (\mathcal{M}(\pi^{\mathrm{an}}))(c_1)f^{n-1} + \cdots + (\mathcal{M}(\pi^{\mathrm{an}}))(c_{n-1})f + (\mathcal{M}(\pi^{\mathrm{an}}))(c_n) = 0$$

Dabei sind die c_i die elementarsymmetrischen Funktionen zu f [Fo, 8.1, Theorem I.8.3.]. Demnach hat die (separable) Erweiterung $\mathcal{M}(X^{\mathrm{an}})|\mathbf{C}(t)$ höchstens Grad n. Sicherlich ist aber $\mathcal{F}(X) \leq \mathcal{M}(X^{\mathrm{an}})$. Somit sind beide Körper gleich, $\mathcal{M}(X^{\mathrm{an}})= \mathcal{F}(X)$.

Für einen algebraischen Morphismus $\theta : X \longrightarrow Y$ ist $\mathcal{F}(\theta)$ - genau wie $\mathcal{M}(\theta^{\mathrm{an}})$ - durch Zurückziehen von rationalen Funktionen definiert. Es ist also $\mathcal{M} \circ (\ )^{\mathrm{an}} = \mathcal{F}$. Daraus folgt $\mathcal{M} \circ (\ )^{\mathrm{an}} \circ \mathcal{N} = \mathrm{id}$. Insbesondere ist $\mathcal{M}$ surjektiv auf den Objekten und $(\ )^{\mathrm{an}}$ injektiv. Die Injektivität von $(\ )^{\mathrm{an}}$ ist jedoch trivial.

Das Ziel ist nun zu zeigen, dass $\mathcal{M}$ und $(\ )^{\mathrm{an}} \circ \mathcal{N}$ eine Äquivalenz von Kategorien definieren. Dazu betrachten wir den Funktor $\mathcal{M}$ genauer. Es ist noch zu zeigen, dass $\mathcal{M}$ Bijektionen auf den Morphismenmengen definiert.

Wir verwenden folgenden Spezialfall des Satzes von Riemann-Roch: Zu jedem Punkt auf einer kompakten Riemannschen Fläche gibt es eine meromorphe Funktion, die genau und ausschließlich an diesem Punkt eine Polstelle hat. Daraus folgt relativ einfach folgende 'Trennungseigenschaft': Seien x_1, x_2 zwei verschiedene Punkte auf einer kompakten Riemannschen Fläche. Seien c_1, c_2 zwei komplexe Zahlen. Dann gibt es eine meromorphe Funktion f mit $f(x_1) = c_1, f(x_2) = c_2$. [Fo, 2, Theorem 14.12 und Corollary 14.13].

Seien nun $\mathcal{X}, \mathcal{Y}$ kompakte Riemannsche Flächen. Zur Injektivität von $\mathrm{Hom}(\mathcal{X}, \mathcal{Y}) \longrightarrow \mathrm{Hom}(\mathcal{M}(\mathcal{Y}), \mathcal{M}(\mathcal{X}))$: Seien $\phi, \phi' : \mathcal{X} \longrightarrow \mathcal{Y}$ analytische Morphismen. Sei $\phi \neq \phi'$. Dann gibt es einen Punkt $x \in \mathcal{X}$ mit $\phi(x) \neq \phi'(x)$. Nach der 'Trennungseigenschaft' gibt es eine meromorphe Funktion f mit $f\phi(x) \neq f\phi'(x)$. Also ist $\mathcal{M}(\phi)(f) = f\phi \neq f\phi' = \mathcal{M}(\phi')(f)$.

Die Surjektivität von $\mathrm{Hom}(\mathcal{X}, \mathcal{Y}) \longrightarrow \mathrm{Hom}(\mathcal{M}(\mathcal{Y}), \mathcal{M}(\mathcal{X}))$ ist schwieriger. Wir verweisen auf [Re, Theorem 7.2.]. Ein Hauptschritt des Beweises ist: Wenn $\mathcal{X}$ eine kompakte Riemannsche Fläche ist, so definiert die Zuordnung $x \mapsto v_x$, wobei v_x die Bewertung an x ist, eine Bijektion zwischen der Menge der Punkte von $\mathcal{X}$ und der Menge der Primstellen von $\mathcal{M}(\mathcal{X})|\mathbf{C}$.

Bemerkung Die soeben bewiesene Äquivalenz der Kategorien $\mathcal{U}^{\mathrm{an}}$ und $\mathcal{U}$ wird in der Algebra *Riemannscher Existenzsatz* genannt. In der Analysis wird die oben benutzte Aussage, dass es zu jedem Punkt auf einer kompakten Riemannschen Fläche eine meromorphe Funktion gibt, die genau und ausschließlich an diesem Punkt einen Pol hat, Riemannscher Existenzsatz genannt.

Grob gesagt besagt der (algebraische) Riemannsche Existenzsatz, dass man alle analytischen kompakten 'Flächen' (besser: Kurven) und die entsprechenden Morphismen auch algebraisch (d.h. mit Hilfe von Polynomen) definieren kann. Dies ist das sogenannte GAGA-Prinzip von Serre. Kurz: analytisch + kompakt = algebraisch.

Der Riemannsche Existenzsatz für nicht-vollständige Kurven

Sei U eine normale, ganze Kurve über $\mathbf{C}$. U ist eine offene Teilmenge einer projektiven, normalen, ganzen Kurve Y. Sei $S := Y - U$. Sei $\mathcal{E}t(U)$ die Kategorie der zusammenhängenden, étalen Überlagerungen von U. Sei $K|\mathbf{C}$ der Funktionenkörper zu U. Der Menge S entspricht dann eine Menge von Primstellen auf K. Sei $\mathcal{K}_S(K)$ die Kategorie der endlichen außerhalb S unverzweigten Körpererweiterungen von K. Nach Dedekind-Weber-Äquivalenz sind diese beiden Kategorien kontravariant äquivalent. Sei U^{an} die Analytifizierung von U, $\mathcal{E}t^{\mathrm{an}}(U^{\mathrm{an}})$ die Kategorie der zusammenhängenden, unverzeigten, endlichen analytischen Überlagerungen von U^{an}.

Einer étalen Überlagerung von U entspricht eine außerhalb S unverzweigte endliche, normale Überlagerung von Y. Genauso verhält es sich mit U^{an}. Denn nach dem Riemannschen Hebbarkeitssatz kann man jede unverzeigte analytische Überlagerung von U^{an} zu einer außerhalb S^{an} unverzeigten Überlagerung von Y^{an} fortsetzen [Fo, Theorem I.8.4.]. Dabei kommutiert offensichtlich Analytifizieren und Einschränken einer Überlagerung von Y auf U und deshalb auch Analytifizieren und Fortsetzen.

Wir können den Riemannschen Existenzsatz anwenden, der sich zuerst nur auf vollständige, normale Kurven bezieht. Es folgt, dass alle drei Kategorien $\mathcal{K}_S(K), \mathcal{E}t(U), \mathcal{E}t^{\mathrm{an}}(U^{\mathrm{an}})$ äquivalent sind.

$$\mathcal{K}_S(K) \cong \mathcal{E}t(U) \cong \mathcal{E}t^{\mathrm{an}}(U^{\mathrm{an}})$$

Struktur der geometrischen Fundamentalgruppe von Kurven über C

Wir wollen nun die geometrische Fundamentalgruppe durch die topologische Fundamentalgruppe ausdrücken. Sei U^{top} der unterliegende topologische Raum von U^{an}. Neben dem Riemannschen Existenzsatz benutzen wir die Tatsache, dass die Kategorie der topologischen Überlagerungen von U^{top} äquivalent zur Kategorie der unverzeigten Überlagerungen von U^{an} ist. Der Funktor von U^{an} nach U^{top} ist der Vergissfunktor. Der entgegengesetze Funktor ist durch 'Hochheben' der analytischen Struktur von U^{an} auf eine Überlagerung definiert. Die Morphismen (Überlagerungen) werden dabei zu unverzweigten analytischen Überlagerungen. Insbesondere existiert in der Kategorie der unverzweiten analytischen Überlagerungen von U^{an} eine maximale unverzweigte Überlagerung

$\widetilde{U^{\mathrm{an}}}$. Mit ihrer Hilfe können wir eine *analytische Fundamentalgruppe* definieren.

$$\pi_1^{\mathrm{an}}(U^{\mathrm{an}}) := \mathrm{Aut}^{\mathrm{an}}(\widetilde{U^{\mathrm{an}}}\,|U^{\mathrm{an}})^{\mathrm{op}}$$

Diese ist kanonisch isomorph zur topologischen Fundamentalgruppe.

$$\pi_1^{\mathrm{an}}(U^{\mathrm{an}}) = \mathrm{Aut}^{\mathrm{an}}(\widetilde{U^{\mathrm{an}}}\,|U^{\mathrm{an}})^{op} = \mathrm{Aut}^{\mathrm{top}}(\widetilde{U^{\mathrm{top}}}\,|U^{\mathrm{top}})^{op} = \pi_1^{\mathrm{top}}(U^{\mathrm{top}})$$

Wir fixieren eine universelle (unverzeigte) Überlagerung $\widetilde{U^{\mathrm{an}}}$ von U^{an} und eine maximale unverzweigte Überlagerung M_S von K. Nach dem Riemannschen Existenzsatz ist die Kategorie der Quotienten von $\widetilde{U^{\mathrm{an}}}$ nach einer Untergruppe von $\mathrm{Aut}(\widetilde{U}\,|U)$ mit endlichem Index und mit Projektionen als Morphismen kontravariant äquivalent zur Kategorie der endlichen Erweiterungen von K in M_S. Das Gleiche gilt, wenn man nur endliche galoissche Quotienten und endliche galoissche Erweiterungen (also solche, die durch Normalteiler von endlichem Index definiert sind) zulässt. Denn eine endliche Überlagerung / separable Körpererweiterung ist genau dann galoissch, wenn die Kardinalität der Automorphismengruppe gleich dem Grad der Überlagerung / Körpererweiterung ist. Diese Kategorien bilden projektive bzw. induktive Systeme. (Durchschnitte von Normalteilern mit endlichem Index sind Normalteiler mit endlichem Index.) Es folgt, dass die geometrische Fundamentalgruppe gleich der proendlichen Komplementierung der topologischen Fundamentalgruppe ist.

$$\pi_1^{\mathrm{top}}(U^{\mathrm{top}})\hat{} = \pi_1^{\mathrm{an}}(U^{\mathrm{an}})\hat{} = \varprojlim_{\substack{N \text{ Normalteiler} \\ \text{mit endlichem Index}}} \pi_1^{\mathrm{an}}(U^{\mathrm{an}})/N =$$

$$\varprojlim_{\substack{\mathfrak{X} \text{ Quotient von } \widetilde{U^{\mathrm{an}}} \text{ über} \\ U^{\mathrm{an}} \text{ mit endlichem Index}}} \mathrm{Aut}(\mathfrak{X}|U^{\mathrm{an}})^{op} = \varprojlim_{\substack{L \text{ endliche galoissche} \\ \text{Erweiterung von } K \text{ in } M_S}} \mathrm{Gal}(L|K) =$$

$$\mathrm{Gal}(M_S|K) = \pi_1(U)$$

Oben haben wir gesehen, dass der Analytifizierungsfunktor injektiv ist. Genauso ist der 'Topologisierungsfunktor' $U \mapsto U^{\mathrm{top}}$ injektiv. Allein aus dieser Aussage und ohne den Riemannschen Existenzsatz erhält man immerhin eine surjektive Abbildung $\pi_1^{\mathrm{top}}(U^{\mathrm{top}})\hat{} \longrightarrow \pi_1(U)$.

Struktur der geometrischen Fundamentalgruppe von Kurven in Charakteristik Null

Für eine normale, ganze **C**-Kurve von Geschlecht g mit s 'Löchern' ist somit

$$\pi_1(U) \cong < a_1, b_1, ..., a_g, b_g, \gamma_1, ..., \gamma_s | [a_1 b_1][a_2 b_2] \cdots [a_g b_g] \gamma_1 \cdots \gamma_s = 1 > \hat{}$$

Dabei korrespondieren die γ_i zu 'Trägheitselementen' an $y_i \in S$. D.h.: Es gibt eine zu $\hat{\mathbf{Z}} = \lim_{\longleftarrow} \mathbf{Z}/n\mathbf{Z}$ isomorphe Trägheitsgruppe über y_i in der Fundamentalgruppe, welche als prozyklische Gruppe von γ_i topologisch erzeugt ist. [Ab, Theorem T], [MM, Theorem I.1.4] Es ist ein algebraisches Resultat, dass die Trägheitsgruppen alle (nicht-kanonisch) isomorph zu $\hat{\mathbf{Z}}$ sind. Nach [Ne, II, Satz (9.6)] folgt dies aus [Se1, IV, Proposition 8].

Man sieht: Wenn $U = \mathbf{P}^1_{\mathbf{C}} - S$ ist, so wird $\pi_1(U)$ von ihren Trägheitsgruppen erzeugt. Insbesondere gibt es keine étalen, zusammenhängenden (nicht-trivialen) Überlagerungen von $\mathbf{P}^1_{\mathbf{C}}$. Dies folgt auch aus der Hurwitz-Formel: Wenn Y eine normale, eigentliche, zusammenhängende Kurve über einem algebraisch abgeschlossenen Körper ist und $X \longrightarrow Y$ eine étale Überlagerung mit Grad n ist, so gilt

$$2 - 2g(X) = n(2 - 2g(Y)).$$

Dabei ist $g(Y) = H^0(Y, \Omega_{Y|k}) = H^1(Y, \mathcal{O}_Y)$ das Geschlecht der nicht-singulären Kurve Y und analog $g(X)$ das Geschlecht der nicht-singulären Kurve X. Für $Y = \mathbf{P}^1$ ist das Geschlecht gleich 0 und somit muss $n = 1$ sein. [Ha, IV, Corollary 2.4]

Sei $\overline{k}$ ein algebraisch abgeschlossener Körper mit Charakteristik Null, $\overline{K}$ ein algebraisch abgeschlossener Oberkörper. Sei Y eine eigentliche $\overline{k}$-Kurve, S eine endliche Menge von Punkten aus Y und $U = Y - S$. Dann definiert der Funktor

$$\mathcal{E}t(U) \longrightarrow \mathcal{E}t(U \otimes_{\overline{k}} \overline{K}), X \mapsto X \otimes_{\overline{k}} \overline{K}$$

eine Äquivalenz von Kategorien. Dabei sind die Trägheitsgruppen über Punkten aus S und über den entsprechenden Punkten aus $Y \times_{\overline{k}} \overline{K}$ kanonisch isomorph. Insbesondere sind die geometrischen Fundamentalgruppen $\pi_1(U)$ und $\pi_1(U \times_{\overline{k}} \overline{K})$ und die einander entsprechenden Trägheitsgruppen in der Fundamentalgruppe kanonisch isomorph. Die Struktur der geometrischen Fundamentalgruppe einer normalen, ganzen Kurve hängt *in Charakteristik Null* also nur vom Geschlecht der Kurve und der Anzahl der 'Löcher' ab. (siehe [SGA I, X,Corollaire 1.8] für den eigentlichen Fall und ansonsten [Popp, Satz (11.1)])

Der $\frac{1}{2}$-Riemannsche Existenzsatz

Es ist kein Beweis der Struktur der geometrischen Fundamentalgruppe von Kurven bekannt, der ohne topologische und analytische Methoden auskommt. Man weiß noch nicht einmal, wie man bei einer eigentlichen, normalen, ganzen Kurve positiven Geschlechts 'kanonische' Erzeugende aus der geometrischen Fundamentalgruppe auswählen kann.

Es ist nun interessant, mit algebraischen Methoden 'große' Quotienten der Fundamentalgruppe anzugeben. In [Pop] wird mit Methoden der rigiden analytischen Goemetrie Folgendes bewiesen: Sei k ein beliebiger Körper mit Charakteristik Null, $S = \{y_1, z_1, ..., y_s, z_s\}$ eine $2s$-elementige Menge von Punkten aus $\mathbf{P}^1_{\overline{k}}, U := \mathbf{P}^1_{\overline{k}} - S$.

Dann hat $\pi_1(U)$ eine freie proendliche Gruppe auf n Erzeugenden als Quotienten.

$$\pi_1(U) \longrightarrow \Pi := < \gamma_1, \tau_1, ..., \gamma_n, \tau_n | \forall i : \gamma_i \tau_i = 1 > \hat{}$$

Dabei sind die Erzeugenden γ_i, τ_i Trägheitselemente zu s_i, t_i.

Aus diesem Resultat folgt insbesondere, dass jede endliche Gruppe Galoisgruppe einer galoisschen Erweiterung von $\overline{k}(t)$ oder $k^{\mathrm{sep}}(t)$ ist.

Der Spezialisierungsmorphismus

Sei nun R ein vollständiger diskreter Bewertungsring mit algebraisch abgeschlossenem Restklassenkörper k mit Charakteristik $p > 0$ und Quotientenkörper K mit Charakteristik Null. Sei Y eine eigentliche, normale, ganze Kurve über R. Y hat über R zwei Fasern, die *allgemeine Faser* $Y_\eta = Y \times_R K$ und die *spezielle Faser* $Y_k = Y \times_R k$. Sei $\overline{Y_\eta} := Y_\eta \times_K \overline{K}$. Grothendieck betrachtet einen *Spezialisierungsmorphismus*

$$\pi_1(\overline{Y_\eta}) \longrightarrow \pi_1(Y_k)$$

Dieser Morphismus ist surjektiv und bijektiv auf dem maximalen p-primen Quotienten. [SGA I, X,Corollaire 3.9]

$$\pi_1^{(p')}(\overline{Y_\eta}) \xrightarrow{\sim} \pi_1^{(p')}(Y_k)$$

Seien $r_1, ..., r_s$ R-wertige Punkte in Y. Jedes r_i definiert einen topologischen Punkt in der allgemeinen Faser und einen topologischen Punkt in der speziellen Faser, $r_{i,\eta}$ und $r_{i,k}$. Die Punkte $r_{i,k}$ (und damit auch die Punkte $r_{i,\eta}$) seien für alle i verschieden. Sei $U := Y - \{r_{1,\eta}, r_{1,k}, ..., r_{s,\eta}, r_{s,k}\}$. Dann ist der Spezialisierungsmorphismus

$$\pi_1(\overline{U_\eta}) \longrightarrow \pi_1(U_k)$$

wieder ein Isomorphismus auf dem maximalen p-primen Quotienten. [Popp, 11.2]

$$\pi_1^{(p')}(\overline{U_\eta}) \xrightarrow{\sim} \pi_1^{(p')}(U_k)$$

Aus [Fu, 9 und Theorem 4.10] folgt, dass die Trägheitsgruppen isomorph sind. Dort wird ferner bewiesen, dass die 'zahme Fundamentalgruppe' über U_k (die analog zur étalen Fundamentalgruppe die étalen Überlagerungen von U_k klassifiziert, welche in den Punkten $y_{i,k}$ zahm verzweigt sind) ein Quotient der étalen Fundamentalgruppe von $\overline{U_\eta}$ ist. In dieser Arbeit wird aber nur die Struktur des maximalen p-primen Quotienten der geometrischen Fundamentalgruppe benötigt.

Zu jedem vollkommenen Körper in positiver Charakteristik gibt es einen vollständigen Bewertungsring, der diesen Körper als Restklassenkörper hat und dessen Quotientenkörper Charakteristik Null hat - nämlich den Ring der Wittvektoren. [Se1, II,5, 3] Somit ist durch den Riemannschen Existenzsatz der maximale p-prime Quotient der geometrischen Fundamentalgruppe in Charakteristik p stets bekannt.

3.4 Abstieg

Proposition 3.4 *Sei X ein ganzes k-Schema, K der Funktionenkörper von X. $l|k$ eine Erweiterung. Dann sind die unter* 1. *und* 2. *abgegebenen Aussagen zueinander äquivalent*

- *1. $X \times_k l$ ist reduziert*
  2. $K \otimes_k l$ ist reduziert
- *1. $X \times_k l$ ist irreduzibel*
  2. $K \otimes_k l$ ist irreduzibel
- *1. $X \times_k l$ ist ganz*
  2. $K \otimes_k l$ ist ein Integritätsbereich

Beweis.
zu 1. Für affine Schemata X =Spek(R) (wobei R ein Integritätsbereich ist) ist Folgendes zu zeigen: $R \otimes_k l$ ist reduziert $\longleftrightarrow$ $K \otimes_k l$ ist reduziert. Sei $S = \{a \otimes 1 | a \in R\}$. S ist ein Multiplikatives System von nicht-Nullteilern und $K \otimes_k l = S^{-1}(R \otimes_k l)$. Die Aussage folgt nun aus folgender einfachen Tatsache: Sei A ein Ring, S ein multiplikatives System von nicht-Nullteilern. Dann gilt: $\mathrm{rad}(S^{-1}A) = S^{-1}\mathrm{rad}(A)$. Insbesondere ist $\mathrm{rad}(A) = 0 \longleftrightarrow \mathrm{rad}(S^{-1}A) = 0$. Die Aussage folgt für allgemeine Schemata, da Reduziertheit eine lokale Eigenschaft ist.

zu 2. Sei X =Spek(R) wieder affin, S wie bei *1.* Allgemein gilt $\mathrm{rad}(S^{-1}A) = S^{-1}\mathrm{rad}(A)$ und $\mathrm{rad}(A) = \mathrm{rad}(S^{-1}A) \cap A$. Daraus folgt: $\mathrm{rad}(A)$ ist prim $\longleftrightarrow \mathrm{rad}(S^{-1}A)$ ist prim.

Der allgemeine Fall folgt nun nicht so leicht wie unter *1.* Schließlich ist Irreduzibilität keine lokale Eigenschaft. Wenn allerdings Spek(R) in X dicht liegt, so liegt Spek$(R \otimes_k l)$ dicht in $X \times_k l$. *Denn*: Sei V eine offene, nichtleere Teilmenge von $X \times_k l$. Dann ist die Teilmenge $\mathrm{Aut}(l|k)V = \bigcup_{\sigma \in \mathrm{Aut}(l|k)} \mathrm{id}_X \times_k \sigma^{-1}(V)$ offen, nichtleer. Sei $p : X \times_k l \longrightarrow X$ die Projektion. Dann ist $\mathrm{Aut}(l|k)V = p^{-1}p(V)$. Die Projektion ist offen. Also ist $p(V) \cap \mathrm{Spek}(R) \neq \emptyset$. Somit ist auch $\mathrm{Aut}(l|k)V \cap \mathrm{Spek}(R \otimes_k l) \neq \emptyset$. Es gibt also ein $x \in V$ und ein $\sigma \in \mathrm{Aut}(l|k)$ mit $(\mathrm{id}_X \otimes \sigma^{-1})(x) \in \mathrm{Spek}(R \otimes_k l)$. Da $\mathrm{Spek}(R \otimes_k l)$ $\mathrm{Aut}(l|k)$-invariant ist, folgt $x \in \mathrm{Spek}(R \otimes_k l)$. Damit ist $V \cap \mathrm{Spek}(R \otimes_k l) \neq \emptyset$. (Siehe [Mu, Theorem II.4.1] für die verwendeten Eigenschaften von p.)

Da Irreduzibilität nur auf einer dichten Teilmenge nachgeprüft werden muss, kann man von X zu einer affinen offenen (und damit dichten) Teilmenge Spek(R) übergehen.

zu 3. Folgt aus *1.* und *2.*. □

Insbesondere folgt aus Propostion 3.4 und Proposition 1.14:

Proposition 3.5 *Sei X ein ganzes k-Schema, K der Funktionenkörper von X. Dann sind die unter 1., bis 4. angegebenen Aussagen zueinander äquivalent:*

- *1. X ist geometrisch reduziert, d.h. $\overline{X} := X \times_k \overline{k}$ ist reduziert*

  2. Für alle Erweiterungen $l|k$ ist $X \times_k l$ reduziert

  3. $X^{\text{ins}} := X \times_k k^{\text{ins}}$ ist ganz

  4. $K|k$ ist separabel

- *1. X ist geometrisch irreduzibel, d.h. $\overline{X} := X \times_k \overline{k}$ ist irreduzibel*

  2. Für alle Erweiterungen $l|k$ ist $X \times_k l$ irreduzibel

  3. $X^{\text{sep}} := X \times_k k^{\text{sep}}$ ist ganz

  4. $K|k$ ist primär

- *1. X ist geometrisch ganz, d.h. $\overline{X} := X \times_k \overline{k}$ ist ganz*

  2. Für alle Erweiterungen $l|k$ ist $X \times_k l$ ganz

  3. $K|k$ ist regulär

Proposition 3.6 *Sei X eine normales k-Schema, $l|k$ eine algebraische Körpererweiterung. Ist $X \times_k l$ normal, so ist auch X normal.*

Beweis. Wir können annehmen, dass X ganz ist. Seien $Z_i, i = 1, ..., n$ die Irreduzibilitätskomponenten von $X \times_k l$.

Sei Spek(A) ein affines Teilschema von X. Dann ist Spek$(A) \times_k l$ =Spek$(A \otimes_k l)$ ein affines Teilschema von $X \times_k l$. $A \otimes_k l$ hat die Form $B_1 \oplus \cdots \oplus B_n$, wobei B_i ganz abgeschlossen in $\kappa(Z_i)$ ist. Damit ist $A \otimes_k l$ ganz abgeschlossen *in* $\kappa(Z_1) \oplus \cdots \oplus \kappa(Z_n) \cong \kappa(X) \otimes_k l$, dem Funktionenring von $X \times_k l$.

Nun ist A normal nach dem folgenden Lemma. □

Lemma 3.7 *Sei $K|k$ eine beliebige Körpererweiterung. Sei $l|k$ eine beliebige algebraische Erweiterung. Sei A ein Teilring von K, der k enthält. Sei $A \otimes_k l$ ganz abgeschlossen in $K \otimes_k l$. Dann ist A normal.*

Beweis. Sei $l_i, i \in I$ eine Basis von $l|k$, welche die 1 enthält. Sei $l_0 = 1$. Sei $x \in K$ ganz über A. Dann ist auch $x \otimes_k 1 \in K \otimes_k l$ ganz über $A \otimes_k l$ und somit ein Element von $A \otimes_k l$. Es gibt eindeutig bestimmte $a_i \in A$ mit $x \otimes_k 1 = \sum_i a_i \otimes_k l_i$, denn die Basis $(l_i)_{i \in I}$ von $l|k$ ist auch eine Basis des freien A-Modul $A \otimes_k l$. Die l_i bilden auch eine K-Basis von $K \otimes_k l$. Aufgrund der Eindeutigkeit der Darstellung ist $x \otimes_k 1 = a_0 \otimes_k 1$ und somit $x = a_0 \in A$. □

Proposition 3.8 *Sei X eine normales k-Schema, $l|k$ eine algebraische separable Körpererweiterung. Dann ist die Konstantenerweiterung $X \times_k l$ normal.*

Beweis. Der Morphismus Spek$(l) \longrightarrow$Spek(k) ist étale. Da étale stabil unter Basiswechsel ist, ist auch $X \times_k l \longrightarrow X$ étale. Wenn X normal ist, so ist auch $X \times_k l$ normal nach Lemma 3.1. □

Daraus folgt insbesondere:

Proposition 3.9 *Sei X eine normale, ganze k-Kurve, $l|k$ eine algebraische separable Körpererweiterung. Sei der Funktionenkörper $K|k$ primär. Dann ist die Konstantenerweiterung $X \times_k l$ gleich der Normalisierung von X in Kl.*

Diese Aussage folgt auch aus Proposition 2.7.

Nach [Ha, III, Theorem 10.2] ist ein k-Schema genau dann glatt, wenn $X \times_k \overline{k}$ regulär ist. Aus den Propositionen 3.6 und 3.8 folgt:

Proposition 3.10 *Eine glatte Kurve ist immer normal. Wenn k vollkommen ist, dann ist eine k-Kurve genau dann normal, wenn sie glatt ist.*

Wenn X ein geometrisch ganzes, separiertes k-Schema ist, dann ist definitionsgemäß $\overline{X} = X \times_k \overline{k}$ eine ganze Varietät. In unserem Kontext ist die umgekehrte Problemstellung (Abstiegsproblem) entscheidend: Gegeben eine Körpererweiterung $l|k$ und eine ganze Varietät X' über l, kann man X' *über k definieren*? D.h. gibt es ein k-Schema X (wie immer von endlichem Typ) mit $X' = X \times_k l$?

Sei U ein ganzes k-Schema, so dass auch $U' := U \times_k l$ ganz ist, $X' \longrightarrow U'$ sei eine étale, zusammenhängende Überlagerung. Wir fragen uns, ob es eine étale Überlagerung $X \longrightarrow U$ gibt mit $X' = X \times_k l$, so dass das Diagramm

$$\begin{array}{ccc} X \times_k l = X' & \longrightarrow & U' \\ \big\downarrow{\scriptstyle p_1} & & \big\downarrow \\ X & \longrightarrow & U \end{array}$$

kommutiert. Falls dies der Fall ist, sagen wir, dass die étale Überlagerung $X' \longrightarrow U'$ *über k definiert* ist.[4]

Wir behandeln das Abstiegsproblem, falls U eine normale, ganze Kurve ist und $U' := U \times_k l$ normal, ganz ist. Falls $l = k^{\text{sep}}$ ist, so bedeutet letzteres, dass der Funktionenkörper primär ist. Falls $l = k^{\text{ins}}$ ist, so lassen sich die Voraussetzungen damit zusammenfassen, dass U glatt und ganz sein soll. (Dies impliziert, dass der Funktionenkörper separabel ist.) Nun ist U' die Normalisierung von U in $\kappa(U)l$.

Seien S' und S die Menge der 'fehlenden Punkte' auf U' und U bei einer Einbettung in eine normale, eigentliche, ganze Kurve.

Sei eine étale, zusammenhängende Überlagerung $X' \longrightarrow U'$ gegeben. Falls die étale Überlagerung $X' \longrightarrow U'$ über k definiert ist, so ist $\kappa(X)|\kappa(U)$ unverzeigt außerhalb S, $\kappa(X)$ und l sind linear disjunkt über k und $\kappa(X') = \kappa(X)l$.

Sei andererseits die Erweiterung $\kappa(X')|\kappa(U')$ als außerhalb S unverzweigte Erweiterung über k definiert, d.h. es existiere eine außerhalb S unverzweigte

[4] Dieser Wortgebrauch von "über k definiert" ist etwas problemathsch: Manche Autoren benutzen den Begriff "über k definiert" im Sinne von "über k", d.h. sie sagen wollen, dass man Schemata über k betrachtet. In diesem Sinne wird er auch oftmals benutzt, wenn auf Schemata verzichtet wird, z.B. in Silverman: The arithmetic of elliptic curves, Springer (2009). Außerdem legt der Begriff eine Eindeutigkeit eines Models über k nahe, die nicht gegeben ist. Aus diesen Gründen sollte man lieber den zuvor benutzten Begriff "über k definierbar" benutzen. Gleiches gilt für den weiter unten benutzen Begriff, dass eine galoissche Überlagerung "mit ihrer Galoisgruppe über k definiert" sei.

Erweiterung $L|\kappa(U)$, wobei L und l über k linear disjunkt sind und $Ll = \kappa(X')$ ist. Dann ist die Normalisierung X von U in L eine étale, zusammenhängende Überlagerung von U. Da L und l über k linear disjunkt sind, ist $X \times_k l$ ganz. Da 'étale' stabil unter Basiswechsel ist, ist $X \times_k l \longrightarrow U'$ étale. Insbesondere ist $X \times_k l$ normal. Ferner ist die Erweiterung der Funktionenkörper $\kappa(X \times_k l)|\kappa(U')$ gleich $\kappa(X')|\kappa(U')$. Damit ist $X \times_k l \longrightarrow U'$ gleich der (eindeutig bestimmten) Normalisierung $X' \longrightarrow U'$ von U' in $\kappa(X')$. Also ist die étale Überlagerung $X' \longrightarrow U'$ über k definiert.

Nach diesen Überlegungen können wir auf die Resultate aus dem zweiten Kapitel zurückgreifen, um die Frage zu beantworten, wann eine étale Überlagerung über einem Körper definiert ist.

Sei $l = k^{\text{ins}}$. In diesem Fall können wir eine vollständige Antwort auf das Abstiegsproblem geben. Die Frage ist, ob $X' \longrightarrow U^{\text{ins}} := U \times_k k^{\text{ins}}$ über k definiert werden kann. Wir haben Folgendes gesehen: Die Erweiterung $\kappa(X')|\kappa(U^{\text{ins}})$ ist über k definiert, die entsprechende Erweiterung $L|\kappa(U)$ ist unverzweigt außerhalb S. Deshalb kann eine étale Überlagerung über k^{ins} immer über k definiert werden.

Sei die galoissche Überlagerung $X' \longrightarrow U'$ über k definiert. Wir sagen, die galoissche Überlagerung $X' \longrightarrow U'$ sei *mit ihrer Galoisgruppe* über k definiert, wenn die étale Überlagerung $X \longrightarrow U$ galoissch ist. Wir wiederholen, dass dies im Falle von étalen, zusammenhängenden Überlagerungen von normalen Kurven nichts anderes heißt, als dass die Erweiterung der Funktionenkörper galoissch ist. (Siehe auch die abstrakte Definition in Abschnitt 'Die Fundamentalgruppe beliebiger Schemata'.) Diese Definition entspricht der für Körper gegebenen. (Siehe Bemerkungen nach der Definition von 'Definitionskörper' in Kapitel 2.) Das 'Hochheben' $\sigma \longrightarrow \sigma \times_k \mathrm{id}_l$ induziert dann einen Isomorphismus von $\mathrm{Gal}(X|U)$ und $\mathrm{Gal}(X'|U')$.

Die Ergebnisse aus der Betrachtung der analogen Situation für Körper lassen sich direkt auf Kurven übertragen, da die Automorphismengruppe einer étalen Überlagerung gleich der Automorphismengruppe der entsprechenden Erweiterung von Funktionenkörpern ist. Eine galoissche Überlagerung $X' \longrightarrow U'$ ist genau dann mit ihrer Galoisgruppe über k definiert, wenn die entsprechende Erweiterung von Funktionenkörpern als außerhalb S unverzweigte Erweiterung mit ihrer Galoisgruppe über k definiert ist. Insbesondere sind (unter den gegebenen Voraussetzungen) alle galoisschen Überlagerungen über k^{ins} mit ihrer Galoisgruppe über k definiert.

Aus der Äquivalenz der Kategorie der Funktionenkörper über k mit der Kategorie der normalen, ganzen, eigentlichen k-Kurven folgt für die Fundamentalgruppen:

Sei $K|k$ ein *primärer* Funktionenkörper. Sei Y das Modell zu $K|k$. Nach Proposition 3.9 ist $Y^{\text{sep}} := Y \times_k k^{\text{sep}}$ die Normalisierung von Y in $k^{\text{sep}}K$. Damit ist Y^{sep} das Modell zu $k^{\text{sep}}K|k^{\text{sep}}$. Sei S eine endliche Menge von Primstellen von $K|k$ bzw. von Punkten von Y. Sei $U := Y - S$. Es ist $U^{\text{sep}} := U \times k^{\text{sep}} =$

$Y^{\mathrm{sep}} - S^{\mathrm{sep}}$.

Aus der exakten Sequenz

$$1 \longrightarrow \mathrm{Gal}(M_S(K)|k^{\mathrm{sep}}K) \longrightarrow \mathrm{Gal}(M_S(K)|K) \longrightarrow \Gamma_k \longrightarrow 1$$

erhalten wir die exakte Sequenz

$$1 \longrightarrow \pi_1(U^{\mathrm{sep}}) \longrightarrow \pi_1(U) \longrightarrow \Gamma_k \longrightarrow 1\ . \tag{3.3}$$

Sei nun $K|k$ ein *separabler* Funktionenkörper, Y das Modell, $S \subseteq Y$ endlich und $U = Y - S$. Sei Y über k glatt. (z.B. $K = k(t), Y = \mathbf{P}^1_k$) Dann ist $Y^{\mathrm{ins}} := Y \times_k k^{\mathrm{ins}}$ normal und somit das Modell zu $k^{\mathrm{ins}}K|k^{\mathrm{ins}}$ und aus

$$\mathrm{Gal}(M_S(k^{\mathrm{ins}}K)|k^{\mathrm{ins}}K) \cong \mathrm{Gal}(M_S(K)|K)$$

folgt

$$\pi_1(U^{\mathrm{ins}}) \cong \pi_1(U) \tag{3.4}$$

Dieser Isomorphismus induziert einen Isomorphismus auf den Trägheitsgruppen nach Proposition 2.3.

Sei nun $K|k$ ein *regulärer* Funktionenkörper. Sei weiterhin Y das Modell zu $K|k$, Y über k glatt, $S \subseteq Y$ endlich, $U = Y - S$. Dann lässt sich die exakte Sequenz 3.3 mit dem Isomorphismus 3.4 zu der exakten Sequenz

$$t\ 1 \longrightarrow \pi_1(\overline{U}) \longrightarrow \pi_1(U) \longrightarrow \Gamma_k \longrightarrow 1 \tag{3.5}$$

zusammenfassen. Wenn man auf die abstrakte Definition der Fundamentalgruppe als Automorphismengruppe des Faserfunktors zurückgreift, sind die Morphismen in der Sequenz 3.5 die durch den Faserfunktor induzierten Morphismen der Sequenz $\overline{U} \longrightarrow U \longrightarrow \mathrm{Spek}(k)$ bezüglich eines über dem generischen Punkt von $\overline{U}$ liegenden geometrischen Punktes. Dies sieht man folgendermaßen: Die Inklusionen auf die generischen Punkte ergeben ein kommutatives Diagramm

$$\begin{tikzcd}
\mathrm{Spek}(\overline{k}K) \arrow[r] \arrow[d] & \mathrm{Spek}(K) \arrow[r] \arrow[d] & \mathrm{Spek}(k) \arrow[d] \\
\overline{U} \arrow[r] & U \arrow[r] & \mathrm{Spek}(k)\ .
\end{tikzcd}$$

Dies induziert ein Diagramm

$$\begin{tikzcd}
\Gamma_{\overline{k}K} \arrow[r] \arrow[d] & \Gamma_K \arrow[r] \arrow[d] & \Gamma_k \arrow[d] \\
\pi_1(\overline{U}) \arrow[r] & \pi_1(U) \arrow[r] & \pi_1(\mathrm{Spek}(k))\ .
\end{tikzcd}$$

Daraus folgt das Diagramm

$$\begin{tikzcd}
\mathrm{Gal}(M_S(\overline{k}K)|\overline{k}K) \arrow[r] \arrow[d, equal] & \mathrm{Gal}(M_S(K)|K) \arrow[r] \arrow[d, equal] & \Gamma_k \arrow[d, equal] \\
\pi_1(\overline{U}) \arrow[r] & \pi_1(U) \arrow[r] & \pi_1(\mathrm{Spek}(k))\ .
\end{tikzcd}$$

Damit wird Sequenz 3.5 ein Spezialfall von [SGA I, IX, Théorème 6.1].

Nach Proposition 2.10 wissen wir bereits, dass die Sequenz 3.5 spaltet, wenn Y einen rationalen Punkt enthält. Wenn U einen rationalen Punkt enthält, folgt dies auch aus der Funktorialität von π_1, da es dann eine abgeschlossene Inklusion $\mathrm{Spek}(k) \longrightarrow U$ gibt, so dass $U \longrightarrow \mathrm{Spek}(k)$ kommutiert.

Kapitel 4

Die Galoisoperation auf der geometrischen Fundamentalgruppe

Sei k ein beliebiger Körper mit Charakteristik $p \geq 0$. Sei $n \in \mathbf{N}$ mit $p \nmid n$. Sei $\zeta_n \in k^{\mathrm{sep}}$ eine primitive n-te Einheitswurzel. Für $\delta \in \Gamma_k$, der absoluten Galoisgruppe von k, definieren wir $c_n(\zeta) \in (\mathbf{Z}/n\mathbf{Z})^*$ als Lösung der Gleichung $\delta(\zeta_n) = \zeta_n^{c_n(\delta)}$. Man sieht: c_n definiert einen stetigen Homomorphismus $\Gamma_k \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*$, welcher unabhängig von der Wahl der primitiven n-ten Eineitswurzel ist. Wir nennen c_n den *cyclotomischen Charakter von k zur Ordnung n.*

Die Morphismen $c_n : \Gamma_k \longrightarrow \mathbf{Z}/n\mathbf{Z}$ definieren einen Morphismus

$$c : \Gamma_k \longrightarrow (\hat{\mathbf{Z}}/p(\hat{\mathbf{Z}}))^* = (\prod_{\substack{l \neq p \\ l \text{ prim}}} \mathbf{Z}_l)^*,$$

den *cyclotomischen Charakter* von k.

Im Falle $k = \mathbf{Q}$ ist der cylotomische Charakter surjektiv und der Satz von Kronecker-Weber besagt, dass sein Kern die absolute Galoisgruppe von $\mathbf{Q}^{ab}$ ist. Also $c : \mathrm{Gal}(\mathbf{Q}^{ab}|\mathbf{Q}) \xrightarrow{\sim} \hat{\mathbf{Z}}^*$.

Sei p eine Primzahl und $k = \mathbf{F}_p$. Die absolute Galoisgruppe $\Gamma_{\mathbf{F}_p}$ ist durch Frob$\mapsto (1)_{n\in\mathbf{N}}$ kanonisch isomorph zu $\hat{\mathbf{Z}}$, und es stellt sich die Frage, wie die Abbildung $c : \hat{\mathbf{Z}} \longrightarrow (\hat{\mathbf{Z}}/p(\hat{\mathbf{Z}}))^*$ aussieht. Nach Definition bildet c_n den Frobenius auf $p \in (\mathbf{Z}/n\mathbf{Z})^*$ ab. Entsprechend wird $(1)_{n\in\mathbf{N}}$ auf $(p)_{n\in\mathbf{N}}$ abgebildet. Da es sich um einen stetigen Homomorphismus handelt, wird $\alpha \in \hat{\mathbf{Z}}$ auf $p^\alpha = (p^{\alpha_n})_n$ abgebildet.

Sei nun k ein beliebiger Körper mit Charakteristik $p > 0$. Da alle Einheitswurzeln schon in $\overline{\mathbf{F}}_p$ liegen, faktorisiert der cyclotomische Charakter über die Restriktion $\Gamma_k \longrightarrow \Gamma_{k\cap\overline{\mathbf{F}}_p}$. Der Kern des cyklotomischen Charakters von k ist gleich $\Gamma_{\overline{F_p}k}$. Dies ist sozusagen das Analogon zum Satz von Kronecker-Weber in positiver Charakteristik.

Insbesondere sieht man, dass der cyklotomische Charakter für Körper positiver Charakteristik *nicht* surjektiv ist. Das Bild von c_n ist stets in $\{p^i | p^i \in (\mathbf{Z}/n\mathbf{Z})^*\}$ enthalten. Für endliche Körper $\mathbf{F}_q, q = p^n$ ist das Bild gleich $\{q^i | q^i \in (\mathbf{Z}/n\mathbf{Z})^*\}$.

Sei der endliche Körper $\mathbf{F}_q, q = p^m$ algebraisch abgeschlossen in k. Dann ist $k|\mathbf{F}_q$ regulär, da alle Erweiterungen von vollkommenen Körpern separabel sind. Die Restriktion $\Gamma_k \longrightarrow \Gamma_{k\cap\overline{\mathbf{F}}_p}$ ist surjektiv, und somit ist das Bild des cyklotomischen Charakters von k gleich der Menge $\{q^i | q^i \in (\mathbf{Z}/n\mathbf{Z})^*\}$

Sei weiterhin k ein beliebiger Körper mit Charakteristik $p > 0$, $\mathbf{P}^1_k$ die projektive Gerade über k. Sei S eine endliche Menge von abgeschlossenen Punkten aus $\mathbf{P}^1_k$. Sei $U := \mathbf{P}^1_k - S$. Sei $\overline{S} = S \times_k \overline{k} = \{y_1, ..., y_s\}$ die Menge der Punkte, die über S in $\mathbf{P}^1_{\overline{k}}$ liegen. Dann ist $\overline{U} = \mathbf{P}^1_{\overline{k}} - \overline{S}$. Γ_k operiert auf $\mathbf{P}^1_{\overline{k}}$ durch $\delta \mapsto \mathrm{id}_{\mathbf{P}^1_k} \times_k \delta^{-1}$. Dies induziert eine Operation auf $\overline{S}$. Sei $\delta^{-1}(y_i) =: y_{\delta(i)}$. Damit operiert die Gruppe Γ_k auch auf der Menge der Zahlen $\{1, ..., s\}$.

Die Punkte $y_1, ..., y_s$ entsprechen gewissen Primstellen von $\overline{k}(t)|\overline{k}$, die mit $\mathfrak{p}_1, ..., \mathfrak{p}_s$ bezeichnet werden. Mittels des Isomorphismus $\mathrm{Gal}(\overline{k}(t)|k(t)) \xrightarrow{\sim} \Gamma_k$ operiert Γ_k auf der Menge der Primstellen. Mit der soeben definierten Operation von Γ_k auf der Menge $\{1, ..., s\}$ gilt $\delta(\mathfrak{p}_i) = \mathfrak{p}_{\delta(i)}$.

Da $\mathbf{P}^1_k$ einen rationalen Punkt enthält, hat die Sequenz

$$1 \longrightarrow \pi_1(U^{\mathrm{sep}}) \longrightarrow \pi_1(U) \longrightarrow \Gamma_k \longrightarrow 1 \tag{4.1}$$

nach Proposition 2.10 einen Schnitt.

Wir wiederholen, dass die Fundamentalgruppe über dem separablen Abschluss k^{sep} gleich der über dem algebraischen Abschluss $\overline{k}$ ist. Sei $\pi := \pi(\overline{U}) \cong \pi(U^{\mathrm{sep}})$ die geometrische Fundamentalgruppe und $\pi^{(p')} = \pi_1^{(p')}(\overline{U}) \cong \pi_1^{(p')}(U^{\mathrm{sep}})$ der maximale p-prime Quotient der geometrischen Fundamentalgruppe.

Sei ein Schnitt in Sequenz 4.1 fixiert. Da die maximale quasi-p-Untergruppe $p(\pi_1(\overline{U}))$ charakteristisch ist, erhalten wir eine exakte spaltende Sequenz

$$1 \longrightarrow \pi^{(p')} \longrightarrow \pi^{(p')} \rtimes \Gamma_k \longrightarrow \Gamma_k \longrightarrow 1 \tag{4.2}$$

Sei $M_S^{(p')}$ die maximale außerhalb S unverzeigte und zu p prime Erweiterung von $k^{\mathrm{sep}}(t)$, also $M_S^{(p')} = M_S^{p(\mathrm{Gal}(M_S|k^{\mathrm{sep}}(t)))}$, wobei $p(\mathrm{Gal}(M_S|k^{\mathrm{sep}}(t)))$ die maximale quasi-p-Untergruppe von $\mathrm{Gal}(M_S|k^{\mathrm{sep}}(t))$ ist. Dann ist $\mathrm{Gal}(M_S^{(p')}|k^{\mathrm{sep}}(t))$ isomorph zu $\pi^{(p')}$. $M_S^{(p')}$ ist galoissch über $k(t)$, da $p(\mathrm{Gal}(M_S|k^{\mathrm{sep}}(t)))$ charakteristisch in $\mathrm{Gal}(M_S|k^{sep}(t))$ ist. Die exakte spaltende Sequenz 4.2 ist nun nichts anderes als

$$1 \longrightarrow \mathrm{Gal}(M_S^{(p')}|k^{sep}(t)) \longrightarrow \mathrm{Gal}(M_S^{(p')}|k(t)) \longrightarrow \Gamma_k \longrightarrow 1 \tag{4.3}$$

Nachdem wir bereits einen Schnitt in Sequenz 4.1 fixiert haben, setzen wir uns nun das Ziel, in Sequenz 4.2 bzw. 4.3 die Operation von Γ_k auf $\pi^{(p')}$=Gal

$(M_S^{(p')}|k^{\mathrm{sep}}(t))$ zu untersuchen. Γ_k operiert in kanonischer Weise auf den Konjugationsklassen der Elemente. Das heißt, das Bild der Operation hängt nicht von der Wahl des Schnitts ab, wie eine einfache Rechnung zeigt.

Wir wissen nach dem Riemannschen Existenzsatz und dem Spezialisierungsmorphismus: $\pi^{(p')}$ ist die freie p-prime proendliche Gruppe auf $s-1$ Erzeugenden.

$$\pi^{(p')} \cong < \gamma_1, ..., \gamma_s | \gamma_1 \cdots \gamma_s = 1 > \hat{}^{(p')} \tag{4.4}$$

Dabei sind die topologischen Erzeugenden γ_i Trägheitselemente über $\mathfrak{p}_i$ bzw. y_i. Es gilt der folgende Satz, der sich an das entsprechende Resultat in Charakteristik Null [MM, I,Theorem 2.6] anlehnt:

Satz 4.1 *Sei k ein Körper mit Charakteristik $p > 0$. Sei S eine endliche Menge von Primstellen von $k(t)$. Sei $\pi := \mathrm{Gal}(M_S|k^{\mathrm{sep}}(t))$. Dann operiert Γ_k auf den Konjugationsklassen der durch den topologischen Erzeugenden von $\pi^{(p')}$ in Gleichung 4.4 mittels des cyklotomischen Charakters. Es gilt für jedes i und alle $\delta \in \Gamma_k$:*

$$[\gamma_i]^\delta = [\gamma_{\delta(i)}^{c(\delta)}]$$

Beweis. Wir wählen ein festes Komplement von $\pi^{(p')}$ in $\mathrm{Gal}(M_S^{(p')}|k(t))$. Jedes Element $\delta \in \Gamma_k$ setzt sich dann eindeutig zu einem $\overline{\delta} \in \mathrm{Gal}(M_S^{(p')}|k(t))$ fort.

Wir wissen, dass die Erzeugenden γ_i von $\pi^{(p')}$ Trägheitselemente an gewissen Primstellen $\mathfrak{P}_i|\mathfrak{p}_i$ von $M_S^{(p')}|k^{\mathrm{sep}}(t)$ sind. Es gilt für jedes Element $\delta \in \Gamma_k$:

$$< \gamma_i^{\overline{\delta}} > \hat{} = I_{\mathfrak{P}_i|\mathfrak{p}_i}^{\overline{\delta}} = I_{\sigma(\mathfrak{P}_{\delta(i)})|\mathfrak{p}_{\delta(i)}} = \sigma I_{\mathfrak{P}_{\delta(i)}|\mathfrak{p}_{\delta(i)}} \sigma^{-1} = \sigma < \gamma_{\delta(i)} > \hat{}\sigma^{-1}$$

mit einem gewissen $\sigma \in \pi^{(p')}$. Es existiert also ein $d^{(i)} = d^{(i)}(\delta) \in (\hat{\mathbf{Z}}/p(\hat{\mathbf{Z}}))^*$ mit

$$[\gamma_i]^\delta = [\gamma_{\delta(i)}^{d^{(i)}(\delta)}].$$

Die genaue Bestimmung der $d^{(i)}(\delta)$ erfolgt durch Übergang zur Abelisierung $(\pi^{(p')})^{ab}$. Da die (abgeschlossene) Kommutatoruntergruppe von $\pi^{(p')}$ charakteristisch ist, operiert Γ_k auch auf der Abelisierung. Die Gruppe $(\pi^{(p')})^{ab} = (\pi^{ab})^{(p')}$ ist die freie abelsche proendliche p-prime Gruppe auf $s-1$ topologischen Erzeugenden.

Andererseits hat die Gruppe die topologischen Erzeugenden $\overline{\gamma_1}, ..., \overline{\gamma_s}$ ($\overline{\gamma_i}$ = Einschränkung von γ_i) und die beiden Relationen $\overline{\gamma_1} \cdots \overline{\gamma_s} = 1$ und $\overline{\gamma_{\delta(1)}}^{d^{(1)}(\delta)} \cdots \overline{\gamma_{\delta(s)}}^{d^{(s)}(\delta)} = 1$. Die Gruppe $(\pi^{(p')})^{ab}$ ist also isomorph zu der Gruppe

$$< \overline{\gamma_1}, ..., \overline{\gamma_{s-1}} | \overline{\gamma_{\delta(1)}}^{d^{(1)}(\delta)-d^{(s)}(\delta)} \cdots \overline{\gamma_{\delta(s-1)}}^{d^{(s-1)}(\delta)-d^{(s)}(\delta)} = 1 > \hat{}^{(p')}_{\text{abelsch}}.$$

Folglich muss die Relation trivial sein in der freien abelschen p-primen Gruppe auf $s-1$ Erzeugenden $< \overline{\gamma_1}, ..., \overline{\gamma_{s-1}} >^{(p')}_{\text{abelsch}}$. Also ist $d^{(1)}(\delta) = \cdots = d^{(s)}(\delta) := d(\delta)$. Nun müssen wir noch zeigen, dass $d(\delta) = c(\delta)$ ist.

Ohne Einschränkung nehmen wir an, dass S zwei Bewertungen von Grad 1 enthält, sagen wir $\mathfrak{p}_1$ und $\mathfrak{p}_s$. (Da wir uns nur mit der Abelisierung beschäftigen, spielt die Nummerierung keine Rolle.) Falls dies nicht der Fall ist, können wir zwei solche Punkte zu S hinzunehmen. Durch die Hinzunahme von Primstellen ändert sich $d(\delta)$ nicht. *Denn:* Seien S und S' endliche Mengen von Primstellen mit $S \subseteq S'$. Seien π, π'; $d(\delta), d'(\delta)$ entsprechend definiert. Aus dem kanonischen Diagramm

$$\begin{tikzcd}
\Gamma_k \arrow[r] \arrow[d, equal] & \mathrm{Aut}(\pi'^{(p')}) \arrow[d] \\
\Gamma_k \arrow[r] & \mathrm{Aut}(\pi^{(p')})
\end{tikzcd}$$

folgt $d_n(\delta) = d'_n(\delta)$ für alle $p \nmid n$.

Sei M der Fixkörper von $< \overline{\gamma_2}, ..., \overline{\gamma_{s-1}} > \hat{}$ in M_S^{ab}. Dann ist M die maximale außerhalb $\mathfrak{p}_1$ und $\mathfrak{p}_s$ unverzeigte p-prime abelsche Erweiterung von $k^{\mathrm{sep}}(t)$. Die maximale p-prime außerhalb zweier Punkten unverweigte Erweiterung ist aber sowieso abelsch, und M ist die maximale außerhalb y_1 und y_s unverzeigte p-prime Erweiterung von $k^{\mathrm{sep}}(t)$.

Die endlichen Teilerweiterungen von M haben die Form $k^{\mathrm{sep}}(z_n)$ mit $z_n = \sqrt[n]{t}$, wobei t den Divisor $\mathfrak{p}_1 - \mathfrak{p}_s$ hat und n prim zu p ist. Man sieht, dass M Kompositum der zwei über $k(t)$ linear disjunkten Erweiterungen $k^{\mathrm{sep}}(t)$ und $k(z_n | n \in \mathbf{N})$ ist. Daher besitzt jedes $\delta \in \Gamma_k$ eine Fortsetzung $\overline{\delta}$ auf M mit $\overline{\delta}(z_n) = z_n$ für alle $n \in \mathbf{N}$. Sei $\overline{\gamma}$ die Einschränkung von $\overline{\gamma_1}$ auf die galoissche Erweiterung $k^{\mathrm{sep}}(z_n)|k^{\mathrm{sep}}(t)$. Dann erzeugt $\overline{\gamma}$ die Galoisgruppe von $k^{\mathrm{sep}}(z_n)|k^{\mathrm{sep}}(t)$. Es existiert also eine primitive n-te Einheitswurzel $\zeta_n \in k^{\mathrm{sep}}$ mit $\overline{\gamma}(z_n) = \zeta_n z_n$. Daraus folgt:

$$\zeta_n^{c_n(\overline{\delta})} = \overline{\delta}(\zeta_n) = \frac{\overline{\delta}(\overline{\gamma}(z_n))}{\overline{\delta}(z_n)} = \frac{\overline{\delta}\overline{\gamma}\overline{\delta}^{-1}\overline{\delta}(z_n))}{\overline{\delta}(z_n)} =$$

$$\frac{\overline{\gamma}^{\overline{\delta}}\overline{\delta}(z_n)}{\overline{\delta}(z_n)} = \frac{\overline{\gamma}^{\delta}(z_n)}{z_n} = \frac{\overline{\gamma}^{d_n(\delta)}(z_n)}{z_n} = \frac{\zeta_n^{d_n(\delta)} z_n}{z_n} = \zeta_n^{d_n(\delta)}$$

Also ist $c(\delta) = d(\delta)$ und somit $[\gamma_i]^\delta = [\gamma_{\delta(i)}^{c(\delta)}]$. $\square$

Kapitel 5

Starrheit

5.1 s-Erzeugendensysteme

Definition Sei G eine endliche Gruppe. Ein *s-Erzeugendensystem* von G ist ein Erzeugendensystem $\underline{\sigma} = (\sigma_1, ..., \sigma_s)$ mit $\sigma_1 \cdots \sigma_s = 1$. Die Menge aller s-Erzeugendensysteme werde mit $\Sigma_s(G)$ bezeichnet.

G operiert auf der Menge der s-Erzeugendensysteme durch Konjugation genauso wie auf G^s. Wir schreiben

$$\underline{\sigma}^g := (g\sigma_1 g^{-1}, ..., g\sigma_s g^{-1})$$

Analog schreiben wir Operationen von Automorphismen von rechts. Sei also für $\alpha \in \mathrm{Aut}(G)$

$$\underline{\sigma}^\alpha := (\alpha(\sigma_1), ..., \alpha(\sigma_s))$$

Sei

$$[\underline{\sigma}] = \underline{\sigma}^G = \{(g\sigma_1 g^{-1}, ..., g\sigma_s g^{-1}) |\ g \in G\} \in \Sigma_s(G)/\mathrm{Inn}(G)$$

die Bahn von $\underline{\sigma}$ unter Konjugation.

Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung $n := |G|$.

Sei k ein Körper der Charakteristik p. Sei S eine Menge von abgeschlossenen Punkten aus $\mathbf{P}^1_k$, so dass die Menge $\overline{S} = S \times_k \overline{k}$ genau s Elemente hat. Wir verwenden nun die Bezeichnungen aus dem vorhergeganenen Kapitel. Insbesondere ist $U = \mathbf{P}^1_k - S$ das Komplement von S und $\pi = \pi_1(\overline{U}) \cong \pi_1(U^{\mathrm{sep}}), \pi^{(p')} = \pi_1^{(p')}(\overline{U}) \cong \pi_1^{(p')}(U^{\mathrm{sep}})$. Die absolute Galoisgruppe Γ_k operiert auf $\pi^{(p')}$, und wir wissen, dass die Operation auf den Konjugationsklassen der topologischen Erzeugenden γ_i durch den cyklotomischen Charakter gegeben ist.

Jedem s-Erzeugendensystem $\underline{\sigma} = (\sigma_1, ..., \sigma_s)$ von G ist durch $\gamma_i \mapsto \sigma_i$ ein surjektiver stetiger Homomorphismus $\psi_{\underline{\sigma}}$ zugeordnet. Die Zuordnung $\underline{\sigma} \mapsto \psi_{\underline{\sigma}}$

definiert eine Bijektion zwischen den s-Erzeugendensystemen und den stetigen surjektiven Morphismen $\pi^{(p')} \longrightarrow G$. Deshalb schreiben wir auch Kern($\underline{\sigma}$) anstatt Kern($\psi_{\underline{\sigma}}$).

Seien $\underline{\sigma}, \underline{\tau}$ zwei s-Erzeugendensysteme. Dann gilt: Kern($\underline{\sigma}$)=Kern($\underline{\tau}$) $\longleftrightarrow$ es existiert ein $\alpha \in$Aut(G) mit $\underline{\sigma}^{\alpha} = \underline{\tau}$. Deshalb kann man Kern($[\underline{\sigma}]$) := Kern($\underline{\sigma}$) setzen.

Dazu: Sei Kern($\underline{\sigma}$)=Kern($\underline{\tau}$). Definiere $\alpha(g) := \psi_{\underline{\tau}}(\psi_{\underline{\sigma}}^{-1}(g))$. Dies ist ein wohldefinierter Isomorphismus mit Umkehrabbildung $\beta(g) := \psi_{\underline{\sigma}}(\psi_{\underline{\tau}}^{-1}(g))$.

Sei andererseits $\alpha \in \operatorname{Aut} G$ mit $\underline{\sigma}^{\alpha} = \underline{\tau}$. Dann ist $\psi_{\underline{\sigma}^{\alpha}} = \psi_{\underline{\tau}}$. Es ist $\psi_{\underline{\sigma}^{\alpha}} = \alpha\psi_{\underline{\sigma}}$. Somit $\alpha\psi_{\underline{\sigma}} = \psi_{\underline{\tau}}$. Daraus folgt Kern($\underline{\sigma}$)=Kern($\underline{\tau}$). □

Die Menge der Normalteiler von $\pi^{(p')} = \text{Gal}(M_S^{(p')}|k(t))$ mit zu G isomorphem Quotient steht in Bijektion zur Menge der galoisschen Teilerweiterungen von $M_S^{(p')}|k(t)$ mit Galoisgruppe G. Diese wiederum steht in Bijektion zur Menge der Isomorphieklassen von außerhalb S unverzweigten Erweiterungen mit Galoisgruppe G. Daraus folgt:

Proposition 5.1 (Hurwitz-Klassifikation) *Die Zuordnung*

$$\begin{array}{ccc} \Sigma_s(G)/Aut(G) & \longrightarrow & \left\{ \begin{array}{c} \textit{Außerhalb } S \textit{ unverzweigte Körpererweiterungen} \\ \textit{von } k(t) \textit{ (bis auf } k(t)\textit{-Isomorphie) mit} \\ \textit{Galoisgruppe } G \end{array} \right\} \\ \sigma^{Aut(G)} & \mapsto & M_S^{Kern(\sigma)} \end{array}$$

ist eine Bijektion.

□

Sei $\underline{\gamma} = (\gamma_1, ..., \gamma_s)$ das fest gewählte topologische Erzeugendensystem von $\pi^{(p')}$ aus Gleichung 4.4 und $[\underline{\gamma}] = \underline{\gamma}^{\pi^{(p')}}$ die Bahn von $\underline{\gamma}$ unter Konjugation. Wir fixieren einen Schnitt $\delta \mapsto \overline{\delta}$ in $\pi^{(p')} \rtimes \Gamma_k$. Nun setzen wir für $\delta \in \Gamma_k$ und $\underline{\sigma} \in \Sigma_s(G)$

$$\underline{\sigma}^{\overline{\delta}} := \psi_{\underline{\sigma}}(\underline{\gamma}^{\overline{\delta}}).$$

Dann ist $\psi_{\underline{\sigma}}((.)^{\overline{\delta}}) = \psi_{\underline{\sigma}^{\overline{\delta}}}$. Daraus folgt

$$\underline{\sigma}^{\overline{\delta_1}\,\overline{\delta_2}} = \psi_{\underline{\sigma}^{\overline{\delta_1}\,\overline{\delta_2}}}(\underline{\gamma}) = \psi_{\underline{\sigma}}(\underline{\gamma}^{\overline{\delta_1}\,\overline{\delta_2}}) = \psi_{\underline{\sigma}}((\underline{\gamma}^{\overline{\delta_2}})^{\overline{\delta_1}}) = \psi_{\underline{\sigma}^{\overline{\delta_1}}}(\underline{\gamma}^{\overline{\delta_2}}) = \psi_{(\underline{\sigma}^{\overline{\delta_1}})^{\overline{\delta_2}}}(\underline{\gamma}) = (\underline{\sigma}^{\overline{\delta_1}})^{\overline{\delta_2}}$$

Also operiert Γ_k auf der Menge der s-Erzeugendensysteme von G.

Genauso ist die Operation auf den Konjugationsklassen $[\underline{\sigma}]$ definiert. Da die Operation von Γ_k auf $\pi^{(p')}$ aber bis auf einen inneren Automorphismus eindeutig ist, ist das Bild von $[\underline{\sigma}]$ nur von δ abhängig. Wir setzen

$$[\underline{\sigma}]^{\delta} := \psi_{[\underline{\sigma}]}([\underline{\gamma}]^{\delta}).$$

Nach Definition gilt nun

$$\psi_{[\underline{\sigma}]^{\delta}}([\underline{\gamma}]) = \psi_{[\underline{\sigma}]}([\underline{\gamma}]^{\delta})$$

Daraus folgt

$$\psi_{[\underline{\sigma}]^\delta}([x]) = \psi_{[\underline{\sigma}]}([x]^\delta)$$

für alle $x \in \pi^{(p')}$ und somit

$$\mathrm{Kern}([\underline{\sigma}]^\delta) = \mathrm{Kern}([\underline{\sigma}])^{\delta^{-1}} \tag{5.1}$$

Sei σ ein fest gewähltes s-Erzeugendensystem von G. Im Folgenden wollen wir erreichen, dass die durch ψ definierte étale Überlagerung von U^{sep} schon über einer 'möglichst kleinen' Erweiterung l von k definiert ist. D.h. wir wollen folgendes Diagramm zu einem kommutativen Diagramm mit exakten Zeilen vervollständigen.

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(U^{\mathrm{sep}}) \arrow[r] \arrow[d] & \pi_1(U \times_k l) \arrow[r] \arrow[d] & \Gamma_l \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \pi_1^{(p')}(U^{\mathrm{sep}}) \arrow[r] \arrow[d, "\psi"] & \pi^{(p')} \rtimes \Gamma_l \arrow[r] & \Gamma_l \arrow[r] \arrow[d] & 1 \\
 & G & & \Gamma_l &
\end{tikzcd}$$

Dann wollen wir einen Schnitt finden, so dass die Γ_l-Operation auf G trivial ist, d.h., dass auch alle Automorphismen der étalen Überlagerung über l definiert sind. (In der Sprache von [Pop] bedeutet dies, dass der Quotient l-rational ist.) In Bezug auf Körper bedeutet letzteres, dass G Galoisgruppe einer regulären Erweiterung von $l(t)$ ist, welche nur an S verzeigt ist.

5.2 Operation auf dem Klassenvektor

Ein *Klassenvektor* ist ein Tupel von Konjugationsklassen von G. Zu $[\underline{\sigma}] \in \Sigma_s(G)/\mathrm{Inn}(G)$ ist durch $C_i := [\sigma_i]$ ein Klassenvektor $\underline{C} = (C_i)_i$ zugeordnet. Zu $\delta \in \Gamma_k$ sei $\underline{C}^\delta$ definiert durch $C_i^\delta := ([\sigma]^\delta)_i$. Damit gilt:

Proposition 5.2

$$C_i^\delta = C_{\delta(i)}^{c_n(\delta)}$$

Dabei ist c_n der cyklotomische Charakter von k zur Ordnung $n = |G|$.

Beweis. Es ist nach Satz 4.1

$$C_i^\delta = ([\sigma]^\delta)_i = \psi([\gamma_i]^\delta) = \psi([\gamma_{\delta(i)}^{c(\delta)}]) = [\sigma_{\delta(i)}^{c_n(\delta)}] = C_{\delta(i)}^{c_n(\delta)} \square$$

Sei nun S eine s-elementige Menge von k-rationalen Punkten von $\mathbf{P}_k^1$. (Insbesondere muss k mindestens die Kardinalität $s-1$ haben.)

Dann gilt

$$\underline{C}^{\delta} = \underline{C}^{c(\delta)} \tag{5.2}$$

Sei

$$\underline{C}_p^* := \{\underline{C}^{p^i} | i \in \mathbf{N}\}$$

Wegen Gleichung 5.2 operiert Γ_k mittels des cyklotomischen Charakters auf $\underline{C}_p^*$. Sei $k_{\underline{C}}$ der Fixkörper von $\{\delta \in \Gamma_k | \underline{C}^{c(\delta)} = \underline{C}\}$ in k^{sep}. Dann ist $k_{\underline{C}}$ der kleinste Oberkörper von k, so dass die Operation auf $\underline{C}_p^*$ trivial ist.

Sei $d_p(\underline{C}) := |\underline{C}_p^*|$. Dann ist d_p die kleinste Zahl $i > 0$, für die $\underline{C}^{p^i} = \underline{C}$ ist. Wir nennen $d_p(\underline{C})$ den *p-Irrationalitätsgrad* von $\underline{C}$. Wir sagen, dass ein Klassenvektor *p-rational* ist, wenn $d_p(\underline{C}) = 1$, d.h. wenn $\underline{C}^p = \underline{C}$ ist.

Wie schon gesagt wurde, faktorisiert der cyklotomische Charakter von Γ_k über $\Gamma_{\mathbf{F}_p}$. Deshalb untersuchen wir zuerst die Operation von $\Gamma_{\mathbf{F}_p}$ auf $\underline{C}_p^*$. Diese Operation ist transitiv. Genau die $d_p(\underline{C})$-fachen Potenzen des Frobenius von $\mathbf{F}_p$ operieren trivial auf $\underline{C}_p^*$. Also ist

$$(\mathbf{F}_p)_{\underline{C}} = \mathbf{F}_{p^{d_p(\underline{C})}}.$$

Dieses Ergebnis überträgt sich von $\mathbf{F}_p$ auf k.

Proposition 5.3 *Es ist* $k_{\underline{C}} = \mathbf{F}_{p^{d_p(\underline{C})}} k$.

Beweis. Wir bemerken, dass $\Gamma_{\mathbf{F}_{p^{d_p(\underline{C})}} k}$ trivial auf $\underline{C}_p^*$ operiert. Nun müssen wir noch zeigen, dass $\mathbf{F}_{p^{d_p(\underline{C})}} k$ der kleinste Oberkörper von k mit dieser Eigenschaft ist. Sei l ein Oberkörper von k, der trivial auf $\underline{C}_p^*$ operiert. Sei F der algebraische Abschluss von $\mathbf{F}_p$ in l. Dann ist l über F regulär, da alle Erweiterungen der endlichen Körper separabel sind. Die Restriktion definiert also einen Isomorphismus $\mathrm{Gal}(l\overline{F}|l) \cong \Gamma_F$. Da die Operation von $\mathrm{Gal}(l\overline{F}|l)$ trivial ist (es ist sogar die Operation von Γ_l trivial) ist auch die Operation von Γ_F trivial. Da $\mathbf{F}_{p^{d_p(\underline{C})}}$ der kleinste Körper mit dieser Eigenschaft ist, folgt $\mathbf{F}_{p^{d_p(\underline{C})}} \leq F \leq l$ und somit $\mathbf{F}_{p^{d_p(\underline{C})}} k \leq l$. $\square$

Bemerkung In [MM] ist in Charakteristik Null der *Irrationalitätsgrad* $d(\underline{C})$ definiert. Mit

$$\underline{C}^* := \{\underline{C}^m | m \in (\mathbf{Z}/n\mathbf{Z})^*\}$$

ist $d(\underline{C}) = |\underline{C}^*|$. Aus der Definition ist sofort klar, dass $d_p(\underline{C})$ den Irrationalitätsgrad $d(\underline{C})$ teilt. Der Körper $k_{\underline{C}}$ ist also ein Teilkörper von $\mathbf{F}_{p^{d(\underline{C})}} k$. Insbesondere ist ein Klassenvektor auf jeden Fall dann p-rational, wenn er rational ist. Es können also alle Ergebnisse über Rationalität von Klassenvektoren von Charakteristik Null auf Charakteristik p übertragen werden.

In Analogie zu [MM, I,Proposition 4.4.] gilt:

Proposition 5.4 $k_{\underline{C}}$ *wird von den Werten der irreduziblen Charaktäre von* G *(mit Werten in* $\overline{\mathbf{F}}_p$*) erzeugt.*

$k_{\underline{C}} = k(\{\chi(C_i) | \chi$ *irreduzibler Charakter von* G *mit Werten in* $\overline{\mathbf{F}}_p, i = 1, ..., s\})$

Beweis. Der Beweis folgt aus folgenden zwei Tatsachen:

1. Sei C eine beliebige Konjugationsklasse von G, χ ein beliebiger Charakter von G mit Werten in $\overline{\mathbf{F}}_p$. Dann ist für alle $\delta \in \Gamma_k$: $\delta(\chi(C)) = \chi(C^{c_n(\delta)})$.

2. Seien C und D zwei Konjugationsklassen von G. Dann folgt aus $\chi(C) = \chi(D)$ für alle irreduziblen Charaktäre von G, dass $C = D$ ist.

Denn nun gilt für alle $\delta \in \Gamma_k$:

$$\delta \in \Gamma_{k_{\underline{C}}} \longleftrightarrow \underline{C}^{c_n(\delta)} = \underline{C} \longleftrightarrow$$
$$\text{Für alle irreduziblen Charaktäre } \chi \text{ ist } \chi(\underline{C}^{c_n(\delta)}) = \chi(\underline{C}) \longleftrightarrow$$
$$\text{Für alle irreduziblen Charaktäre } \chi \text{ ist } \delta(\chi(\underline{C})) = \chi(\underline{C}).$$

Zu 1. Sei C eine Konjugationsklasse von G, χ ein Charakter. Sei $\sigma \in C$. Dann ist $\chi|_{<\sigma>} = \sum_i a_i\chi_i$ mit $a_i \in \mathbf{F}_p$ und irreduziblen Charaktären χ_i. Somit ist $\delta(\chi(C)) = \sum_i a_i\delta(\chi_i(\sigma)) = \sum_i a_i\chi_i(\sigma^{c_n(\delta)}) = \chi(C^{c_n(\delta)})$.

Zu 2. Sei für beliebige Konjugationsklassen A, B:

$$< A, B >:= \frac{1}{n} \sum_{\chi \text{ irred.}} \chi(A)\chi(B^{-1}).$$

(Beachte, dass die Charakteristik die Gruppenordnung n nicht teilt.) Dann gilt nach [La, XVIII, Theorem 5.5]: $< A, B >= h_A\delta_{AB}$, wobei h_A die Anzahl der Elemente in der Klasse A ist. Dabei teilt h_A die Gruppenordnung, ist also prim zur Charakteristik. 'Die Konjugationsklassen sind orthogonal zueinander.' Nun ist nach Voraussetzung $< C, D >=< C, C >= h_C$ und somit $C = D$. □

5.3 Starrheitssätze

Definition Ein *starres s-Erzeugendensystem* ist ein s-Ezeugendensystem σ mit: Für jedes $\underline{\tau} = (\tau_1, ..., \tau_s) \in G^s$ mit der Eigenschaft, dass $\underline{\tau\sigma\tau}^{-1} = (\tau_i\sigma_i\tau_i^{-1})_i$ ein s-Erzeugendensystem von G ist, gibt es ein $\tau \in G$ mit $\tau_i\sigma_i\tau_i^{-1} = \tau\sigma_i\tau^{-1}$ für alle i.

Weiter sagen wir, ein Klassenvektor $\underline{C}$ der Länge s sei *starr*, wenn es bis auf Konjugation genau ein s-Erzeugendensystem $\underline{\sigma}$ von G mit $\sigma_i \in C_i$ gibt.

Mit diesen Definitionen ist ein s-Erzeugendensystem $\underline{\sigma}$ genau dann starr, wenn $[\underline{\sigma}]$ durch den zugehörigen Klassenvektor $\underline{C}$ eindeutig bestimmt ist.

Wir nehmen nun an, dass $\underline{\sigma}$ ein solches starres Erzeugendensystem ist. Dann folgt aus $\underline{C}^\delta = \underline{C}$, dass $[\underline{\sigma}]^\delta = [\underline{\sigma}]$ ist. Wir erhalten also folgendes Resultat:

Proposition 5.5 *Sei $\underline{C}$ ein starrer Klassenvektor. Dann ist der Kern von ψ invariant unter der Operation von $\Gamma_{k_{\underline{C}}}$.*

Beweis. Aus $\underline{C}^\delta = \underline{C}$ folgt $[\underline{\sigma}]^\delta = [\sigma]$ und daraus mit Gleichung 5.1

$$\mathrm{Kern}([\sigma]) = \mathrm{Kern}([\underline{\sigma}]^\delta) = \mathrm{Kern}([\underline{\sigma}])^{\delta^{-1}}.$$

□

Alle $\delta \in \Gamma_{k_{\underline{C}}}$ operieren auf G durch innere Automorphismen. Denn aufgrund der Starrheit von $\underline{\sigma}$ ist $\underline{\sigma}^\delta = \underline{\sigma}^\alpha$ mit einem $\alpha \in G$. Somit gilt für alle $g \in G$ $g^\delta = g^\alpha$.

Wir können nun die Propositionen 2.12 und 2.13 anwenden. Unter den Voraussetzungen, dass k endlich ist, bzw. dass das Zentrum von G ein Komplement in G besitzt, kann die Operation von $\Gamma_{k_{\underline{C}}}$ auf G trivial gewählt werden.

Wir erhalten folgendes Diagramm:

$$\begin{tikzcd}
1 \arrow[r] & \pi_1(U^{\mathrm{sep}}) \arrow[r] \arrow[d] & \pi_1(U \times_k k_{\underline{C}}) \arrow[r] \arrow[d] & \Gamma_{k_{\underline{C}}} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & \pi_1^{(p')}(U^{\mathrm{sep}}) \arrow[r] \arrow[d, "\psi"] & \pi^{(p')} \rtimes \Gamma_{k_{\underline{C}}} \arrow[r] \arrow[d] & \Gamma_{k_{\underline{C}}} \arrow[r] \arrow[d] & 1 \\
1 \arrow[r] & G \arrow[r] & G \times \Gamma_{k_{\underline{C}}} \arrow[r] & \Gamma_{k_{\underline{C}}} \arrow[r] & 1
\end{tikzcd}$$

Es ergeben sich die beiden folgenden Sätze:

Satz 5.6 (Einfacher Starrheitssatz für endliche Körper) *Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung und einem starren Klassenvektor $\underline{C}$ der Länge s. Sei $e \geq 1$ und $q := p^e \geq s - 1$. Sei S eine s-elementige Menge von Primstellen mit Grad 1 auf $\mathbf{F}_q(t)|\mathbf{F}_q$.*

Sei $(\mathbf{F}_q)_{\underline{C}} = \mathbf{F}_q(\{\chi(C_i)|\chi$ irreduzibler Charakter von G mit Werten in $\overline{\mathbf{F}}_p$, $i = 1, ..., s\})$.

Dann existiert eine über $(\mathbf{F}_q)_{\underline{C}}$ reguläre, galoissche Erweiterung $N|(\mathbf{F}_q)_{\underline{C}}(t)$ mit Galoisgruppe G, unverzweigt außerhalb von S, wobei die Trägheitsgruppen von Elementen $\sigma_i \in C_i$ erzeugt werden.

Insbesondere, falls $\underline{C}^q = \underline{C}$ ist, so gibt es eine über $\mathbf{F}_q$ reguläre, galoissche Erweiterung $N|\mathbf{F}_q(t)$ mit Galoisgruppe G, unverzweigt außerhalb von S, wobei die Trägheitsgruppen von Elementen $\sigma_i \in C_i$ erzeugt werden.

Bemerkung Ein ähnliches aber schwächeres Resultat kann auch durch Anwendung des einfachen Starrheitssatzes in Charakteristik Null und 'Spezialisieren' gewonnen werden: (siehe [Beck, Proposition 2.3, Proposition 3.7.], siehe auch [MM, I,Proposition 10.9].)

Wenn die endliche Gruppe G mit dem starren Klassenvektor $\underline{C}$ der Länge s *triviales Zentrum* hat und f so gewählt wird, dass $q := p^{fd(\underline{C})} \geq s - 1$ ist, (wobei $d(\underline{C})$ der Irreduzibilitätsgrad von $\underline{C}$ ist), so existiert eine über $\mathbf{F}_q$ reguläre, galoissche Erweiterung $N|\mathbf{F}_q(t)$ mit Galoisgruppe G, unverzweigt außerhalb einer vorgegebenen s-elementigen Menge von Primstellen von Grad 1, wobei die Trägheitsgruppen von Elementen $\sigma_i \in C_i$ erzeugt werden.

Sei nun k ein beliebiger Körper mit Charakteristik p, der den Körper $(\mathbf{F}_q)_{\underline{C}}$ enthält. Dann sind N (im obigen Satz) und k linear disjunkt über $(\mathbf{F}_q)_{\underline{C}}$ im linear disjunkten Kompositum $Nk := \mathrm{Quot}(N \otimes_{(\mathbf{F}_q)_{\underline{C}}} k)$. Aus dem Diagramm

$$\begin{tikzcd}
Nk \arrow[d, dash] \arrow[dr, dash] & & \\
N \arrow[dr, dash] & k(t) \arrow[d] \arrow[dr, dash] & \\
& (\mathbf{F}_q)_{\underline{C}}(t) \arrow[dr, dash] & k \arrow[d, dash] \\
& & (\mathbf{F}_q)_{\underline{C}}
\end{tikzcd}$$

folgt, dass $Nk|k(t)$ eine galoissche Erweiterung mit Galoisgruppe G ist, wobei Nk über k regulär ist. Die Primstellen von $\mathbf{F}_q(t)$ setzen sich auf eindeutig $k(t)$, wenn man $v_{\mathfrak{p}}|_k = 0$ fordert. Daraus folgt:

Korollar 5.7 *Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung und einem $\underline{C}$ starren Klassenvektor der Länge s. Sei $e \geq 1$ und $q := p^e$ mit $q \geq s-1$. Sei S eine s-elementige Menge von Primstellen mit Grad 1 auf $\mathbf{F}_q(t)|\mathbf{F}_q$ Sei k ein beliebiger Körper mit Charakteristik p, der den Körper $(\mathbf{F}_q)_{\underline{C}}$ enthält.*

Dann existiert eine über k reguläre, galoissche Erweiterung $N|k(t)$ mit Galoisgruppe G, unverzweigt außerhalb der eindeutigen Fortsetzungen von S, wobei die Trägheitsgruppen von Elementen $\sigma_i \in C_i$ erzeugt werden.

Wenn man anstelle von Körpern mit Kurven arbeitet, ergibt sich der *Beweis* des Korollars auch aus folgender Überlegung:

Nach dem Starrheitssatz für endliche Körper existiert eine galoissche, geometrisch ganze Überlagerung $X \longrightarrow U_{(\mathbf{F}_q)_{\underline{C}}}$ mit Galoisgruppe G. Nun ist die Bedingung 'galoissch mit Galoisgruppe G' invariant unter flachem Basiswechsel nach [SGA I, Proposition 1.9.] und [SGA I, Proposition 2.1.]. Somit ist $X \times_{(\mathbf{F}_q)_{\underline{C}}} k \longrightarrow U_k$ eine galoissche Überlagerung mit Galoisgruppe G, welche automatisch geometrisch ganz ist. □

Satz 5.8 (Einfacher Starrheitssatz für globale Funktionenkörper) *Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung, in der das Zentrum ein Komplement hat. G besitze einen starren Klassenvektor $\underline{C}$ der Länge s. Sei S eine s-elementige Menge von Primstellen mit Grad 1 auf $\mathbf{F}_p(x)(t)|\mathbf{F}_p(x)$.*

Sei $(\mathbf{F}_p)_{\underline{C}} = \mathbf{F}_p(\{\chi(C_i)|\chi$ irreduzibler Charakter von G mit Werten in $\overline{\mathbf{F}}_p$, $i = 1, ..., s\})$.

Dann existiert eine über $(\mathbf{F}_p)_{\underline{C}}(x)$ reguläre, galoissche Erweiterung $N|(\mathbf{F}_p)_{\underline{C}}(x)(t)$ mit Galoisgruppe G, unverzweigt außerhalb von S, wobei die Trägheitsgruppen von Elementen $\sigma_i \in C_i$ erzeugt werden.

Insbesondere, falls $\underline{C}^q = \underline{C}$ ist mit $q := p^e, e \geq 1$, so gibt es eine über $\mathbf{F}_q(x)$ reguläre, galoissche Erweiterung $N|\mathbf{F}_q(x)(t)$ mit Galoisgruppe G, unverzweigt außerhalb von S, wobei die Trägheitsgruppen von Elementen $\sigma_i \in C_i$ erzeugt werden.

Bemerkung Sei $\sigma_1 \in C_1$. Dann bleibt der einfache Starrheitssatz für globale Funktionenkörper richtig, wenn das Zentrum von G kein Komplement in G sondern in einer beliebigen Untergruppe von G, welche $N_G(<\sigma_1>)$ enthält, hat. Man wähle dazu die Primstelle $\mathfrak{p}$ in Proposition 2.12 gleich $\mathfrak{p}_1 \in S$.

Genau wie über $\mathbf{Q}(t)$ gilt auch über $\mathbf{F}_p(x)(t)$ ein *starker Starrheitssatz.* Die Idee ist, dass auf die p-Rationalität des Klassenvektors verzichtet werden kann, wenn dieser gewisse Symmetrien aufweist und man nicht mit rationalen Punkten sondern mit wohl gewählten Bahnen von Punkten arbeitet.

Satz 5.9 (Starker Starrheitssatz für globale Funktionenkörper) *Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung, in der das Zentrum ein Komplement hat. G besitze einen starren Klassenvektor $\underline{C}$.*

Sei $e \geq 1$ und $q := p^e$. Es gebe einen (nicht notwendigerweise starren) Klassenvektor $\underline{D}$ der Länge r von G, so dass der starre Klassenvektor $\underline{C}$ die folgende Form hat:

$$C = (D_1, D_1^q, ..., D_1^{q^{b_1-1}}, ..., D_r, D_r^q, ..., D_r^{q^{b_r-1}})$$

Dabei ist $b_i := \frac{d_p(D_i)}{\mathrm{ggT}(d_p(D_i),e)}$ die Länge der Bahn $D_i, D_i^q, ...$

Dann existiert eine über $\mathbf{F}_q(x)$ reguläre, galoissche Erweiterung $N|\mathbf{F}_q(x)(t)$ mit Galoisgruppe G, welche außerhalb von r Primstellen unverzweigt ist.

Beweis. Sei wie im Satz $b_i = \frac{d_p(D_i)}{\mathrm{ggT}(d_p(D_i),e)}$ die Länge der Bahn $D_1, D_1^q, ...$ Seien $a_i \in \mathbf{F}_{q^{b_i}} \backslash \mathbf{F}_{q^{b_i-1}}$ $(\mathbf{F}_0 = 0)$, $x_i \in \mathbf{F}_q(x)$, wobei die Bahnen $\{a_i^{q^j} x_i | j \in \mathbf{N}\}$ paarweise disjunkt seien $(i = 1, ..., r)$. Wir schreiben $\underline{C} = (C_{11}, C_{12}, ..., C_{1b_1}, ..., C_{r1}, ..., C_{rb_r})$ mit $C_{ij} = D_i^{q^j}$. Sogleich werden wir die Notation $C_{i,-a} = C_{i,r-a}$ verwenden.

Seien für $i = 1, ..., r, j = 1, ..., b_i : \mathfrak{p}_{ij} := (t - a_i^{q^{-j}} x_i)$ Primstellen auf $\overline{\mathbf{F}_q(x)}(t)|\overline{\mathbf{F}_q(x)}$. Sei $\overline{S}$ die $\Gamma_{\mathbf{F}_q(x)}$-invariante Menge, welche die s Primstellen $\mathfrak{p}_{ij}$ zum Inhalt hat. Sei S die darunterliegende Menge von Primstellen auf $\mathbf{F}_q(x)(t)|\mathbf{F}_q(x)$. Dann hat S die Kardinalität r.

Sei $\delta \in \Gamma_{\mathbf{F}_q(x)}$ beliebig. Sei die Restriktion von δ auf $\overline{\mathbf{F}}_q$ gleich $Frob^{de}$. Dann ist $\delta(\mathfrak{p}_{ij}) = \mathfrak{p}_{i,j-d}$. Somit ist nach Proposition 5.2

$$C_{ij}^{\delta} = C_{i,j-d}^{q^d} = (D_i^{(q^{(j-d)})^{(q^d)}} = D_i^{q^{(j-d)+d}} = D_i^{q^j} = C_{ij}$$

und aus der Starrheit von $\underline{C}$ folgt die Behauptung wie beim einfachen Starrheitssatz mit Proposition 2.12.

Genauer gilt: Es gibt eine über $\mathbf{F}_q(x)$ reguläre, galoissche Erweiterung $N|\mathbf{F}_q(x)(t)$ mit Galoisgruppe G, unverzweigt außerhalb von S, wobei die Trägheitsgruppen von Elementen $\sigma_i \in C_i$ erzeugt werden. □

Mit diesem Resultat sieht man auch, dass alle endlichen abelschen Gruppen mit zu p primer Ordnung Galoisgruppen einer über $\mathbf{F}_p(x)$ regulären, galoisschen Erweiterung $N|\mathbf{F}_p(x)(t)$ sind. Man braucht nur ein Erzeugendensystem in der Form des starken Starrheitssatzes mit $e = 1$ zu wählen. Dieses ist automatisch starr.

Proposition 5.10 *Sei k ein beliebiger Körper in Charakteristik p. Dann sind alle endlichen abelschen p-Gruppen Galoisgruppen einer über k regulären, galoisschen Erweiterung von $k(t)$.*

Beweis. Sei $G = \mathbf{Z}/p^{e_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{e_r}\mathbf{Z}$ eine beliebige endliche abelsche p-Gruppe.

1. Schritt Konstruktion von regulären, galoisschen Erweiterungen von $k(t)$ mit Galoisgruppe $\mathbf{Z}/p\mathbf{Z}$. Es sei beliebiges transzendentes Element $u \in k(t)|k$ fixiert. Sei $L|k(t)$ die durch die Gleichung $v^p - v = u$ gegebene Artin-Schreier Erweiterung. Diese hat Galoisgruppe $\mathbf{Z}/p\mathbf{Z}$. Außerdem ist $v \notin \overline{k}$, da ansonsten $u \in \overline{k}$ wäre. Nun ist die Erweiterung $L|k(t)$ über k regulär, da die Ordnung von $\mathbf{Z}/p\mathbf{Z}$ eine Primzahl ist.

2.Schritt Konstruktion von regulären, galoisschen Erweiterungen von $k(t)$ mit Galoisgruppe $\mathbf{Z}/p\mathbf{Z} \times \cdots \times \mathbf{Z}/p\mathbf{Z}$. Seien $\alpha_1, ..., \alpha_r$ verschiedene Elemente aus k. Dann liegen die Elemente $\alpha_i u$ in verschiedenen Nebenklassen von $\{y - y^p | y \in k(t)\}$ in $k(t)$. Nach der Artin-Schreier Theorie definieren die $\alpha_i u$ verschiedene (linear disjunkte) galoissche Erweiterungen $L_i|k(t)$ mit zu $\mathbf{Z}/p\mathbf{Z}$ isomorpher Galoisgruppe. Das Kompositum L der L_i (in einem algebraischen Abschluss von $k(t)$) hat somit Galoisgruppe $\mathbf{Z}/p\mathbf{Z} \times \cdots \times \mathbf{Z}/p\mathbf{Z}$. Die Elemente $\alpha_i u$ definieren auch über $\overline{k}(t)$ linear disjunkte Erweiterungen $L_i\overline{k}|\overline{k}(t)$ (da die $\alpha_i u$ in verschieden Nebenklassen von $\{y - y^p | y \in \overline{k}(t)\}$ in $\overline{k}(t)$ liegen). Somit ist $[L\overline{k} : \overline{k}(t)] = p^r = [L : k(t)]$ und L ist über $k(t)$ linear disjunkt zu $\overline{k}(t)$, d.h. $L|k(t)$ ist regulär über k.[1]

3. Schritt Konstruktion von regulären, galoisschen Erweiterungen von $k(t)$ mit Galoisgruppe $G = \mathbf{Z}/p^{e_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{e_r}\mathbf{Z}$. Der maximale p-Quotient der absoluten Galoisgruppe von $k(t)$ ist eine freie pro-p-Gruppe. [Se2, II, 2.2. Proposition 3 mit Corollaire 1] Deshalb faktoriert der Morphismus $\Gamma_{k(t)} \longrightarrow \mathbf{Z}/p\mathbf{Z} \times$

[1] Hier sind zwei Fehler: Erstens müsste man für die angegebene Konstruktion voraussetzen, dass k unendliche Kardinalität hat. Zweitens muss man einen r-dimensionalen $\mathbf{F}_p$-Untervektorraum U von $k(t)/\mathcal{P}(k(t))$ wählen, wobei $\mathcal{P}$ der Artin-Schreier Operator sei. Damit die Erweiterung reguär ist, muss außerdem das Bild von U in $\overline{k}(t)/\mathcal{P}(\overline{k}(t))$ r-dimensional sein.

Eine einfache Möglichkeit für so eine Untergruppe U ist diese: Betrachte den von t^{ip+1} mit $i = 0, \ldots, r-1$ erzeugten $\mathbf{F}_p$-Untervektorraum von $k(t)/\mathcal{P}(k(t))$. Dieser Vektorraum hat in der Tat die Dimension r und sein Bild in $\overline{k}(t)/\mathcal{P}(\overline{k}(t))$ hat auch die Dimension r.

$\cdots \times \mathbf{Z}/p\mathbf{Z}$ über einen surjektiven Morphismus nach $\mathbf{Z}/p^{e_1}\mathbf{Z} \times \cdots \times \mathbf{Z}/p^{e_r}\mathbf{Z}$. Dies definiert eine Erweiterung $M|k(t)$ mit Galoisgruppe G, welche L enthält und außerdem regulär über $k(t)$ ist. *Annahme:* $M|k(t)$ ist nicht regulär über $k(t)$. Sei $\widetilde{M} := M \cap \overline{k(t)}$. Da $\widetilde{M}\ |k(t)$ nicht-trivial ist, enthält $\widetilde{M}\ |k(t)$ eine Teilerweiterung von Grad p. Diese ist gleich $L_i|k(t)$ für ein $i = 1, ..., r$ und somit regulär. *Widerspruch!* □

Zwei galoissche Teilerweiterungen $N_1|k(t), N_2|k(t)$ von $\overline{k(t)}|k(t)$ mit teilerfremden Grad sind linear disjunkt, da sie $k(t)$ als Durchschnitt haben. Das Kompositum hat somit das Produkt der Galoisgruppen von $N_1|k(t)$ und $N_2|k(t)$ als Galoisgruppe. Wenn nun die Erweiterungen $N_1|k(t)$ und $N_2|k(t)$ regulär sind, sind auch $N_1\overline{k}|\overline{k}(t)$ und $N_2\overline{k}|\overline{k}(t)$ linear disjunkt und $N_1N_2|k(t)$ ist regulär.

Insgesamt folgt:

Korollar 5.11 *Alle endlichen abelschen Gruppen sind Galoisgruppen einer über $\mathbf{F}_p(x)$ regulären, galoisschen Erweiterung von $\mathbf{F}_p(x)(t)$.* □

Nun sind alle globalen Körper Hilbertsche Körper [FJ, Corollary 12.8], d.h. der Hilbertsche Irreduzibilitätssatz gilt. Man kann also 'spezialisieren' [FJ, Lemma 12.12]. Genauer gilt:

Sei k ein globaler Körper und $N|k(t)$ eine galoissche Erweiterung mit Galoisgruppe G. Dann gibt es eine Primstelle von $k(t)|k$ mit Grad 1, die in $N|k(t)$ unverzweigt und unzerlegt ist. Insbesondere ist die Restklassenkörpererweiterung eine galoissche Erweiterung von k mit Galoisgruppe G.

Aus Korollar 5.7 folgt:

Korollar 5.12 *Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung und einem starren Klassenvektor $\underline{C}$ der Länge s. Sei $e \geq 1, q := p^e$ mit $q \geq s-1$. Sei k ein globaler Körper mit Charakteristik p, der den Körper $(\mathbf{F}_q)_{\underline{C}}$ enthält. Dann existiert eine galoissche Erweiterung $\lambda|k$ mit Galoisgruppe G.*

Aus dem einfachen Starrheitssatz für globale Funktionenkörper folgt:

Korollar 5.13 *Sei p eine Primzahl. Sei G eine endliche Gruppe mit zu p primer Ordnung, in der das Zentrum ein Komplement hat. G enthalte einen starren Klassenvektor $\underline{C}$. Sei k ein globaler Körper mit Charakteristik p, der den Körper $(\mathbf{F}_p)_{\underline{C}}$ enthält. Dann existiert eine galoissche Erweiterung $\lambda|k$ mit Galoisgruppe G.*

Aus Korollar 5.11 folgt:

Korollar 5.14 *Alle endlichen abelschen Gruppen können als Galoisgruppen über jedem globalen Körper positiver Charakteristik realisiert werden.*

Anhang

Proendliche Gruppen

Eine proendliche Gruppe ist eine topologische Gruppe, welche projektiver Limes von endlichen Gruppen ist. Dabei seien die endlichen Gruppen mit der diskreten Topologie versehen. Die Homomorphismen des projektiven Systems können surjektiv gewählt werden. In dieser Arbeit treten proendliche Gruppen nur als Galoisgruppen auf. Dann sind die Homomorphismen des projektiven Systems sowieso surjektiv.

Die proendlichen Gruppen bilden mit den stetigen Homomorphismen eine Kategorie, wobei die stetigen Gruppenhomomorphisen die Morphismen sind.

Aus dem Satz von Tychonoff folgt, dass der projektive Limes von kompakten Räumen kompakt ist. Der projektive Limes von kompakten nicht-leeren Räumen ist kompakt und nicht-leer. Dies liegt daran, dass der projektive Limes der Räume X_i als Teilraum von $\prod_i X_i$ Durchschnitt der abgeschlossenen - und damit kompakten - nicht-leeren Teilmengen $X_{ij} := \{\alpha = (\alpha_i) \in \prod_i X_i | p_{ij}(\alpha_i) = \alpha_j\}$ ist $(i > j)$. (Siehe auch [Ne, IV, Satz (2.3)].)

Außerdem sieht man leicht, dass der projektive Limes von total unzusammenhängenden Räumen total unzusammenhängend ist. Eine proendliche Gruppe ist also kompakt und total unzusammenhängend. Diese notwendigen Bedingungen sind auch schon hinreichend. Insbesondere folgt daraus, dass projektive Limites von proendlichen Gruppen proendlich sind. Außerdem sieht man, dass eine Untergruppe einer proendlichen Gruppe genau dann proendlich ist, wenn sie abgeschlossen (also kompakt) ist.

Proposition 1 *Sei $(G_i)_{i \in I}$ ein projektives System von proendlichen Gruppen mit surjektiven Homomorphismen $p_{ij} : G_i \longrightarrow G_j$. Sei $\pi := \lim_{\longleftarrow} G_i$. Dann sind die natürlichen Morphismen $p_i : \pi \longrightarrow G_i$ surjektiv.*

Beweis. Sei $i \in I$ fest gewählt, und sei $x_i \in G_i$. Sei $H_j := p_{ij}^{-1}(x_i)$. Dann bilden die H_j ein projektives System von nicht-leeren abgeschlossenen (und damit kompakten) Teilräumen von G_j. Sei $H := \lim_{\longleftarrow} H_i \subseteq \pi$. H ist nicht-leer, da projektive Limites kompakter nicht-leerer Räume nie leer sind. Jedes Element aus H wird auf x_i abgebildet. □

Einige gruppentheoretische Aussagen

Definition Eine proendliche Gruppe Γ ist *projektiv*, wenn für jeden surjektiven Morphismus proendlicher Gruppen

$$G \xrightarrow{p} Q \longrightarrow 1$$

und jeden Morphismus $\Gamma \longrightarrow Q$ genau ein Morphismus $\Gamma \longrightarrow G$ existiert, so dass das Diagramm

$$\begin{tikzcd} & \Gamma \arrow[dl] \arrow[d] & \\ G \arrow[r, "p"] & Q \arrow[r] & 1 \end{tikzcd}$$

kommutiert.

Definition Seien G und Γ proendliche Gruppen, S ein semidirektes Produkt von G mit Γ. Dann ist ein *direktes abgeschlossenes Komplement von G in S* ein abgeschlossener Normalteiler $H \leq S$ mit $G \cap H = 1$, $GH = S$.

In Kapitel 1 haben wir benutzt:

Proposition 2 *Sei G eine proendliche Gruppe, Γ eine proendliche projektive Gruppe. Sei S ein semidirektes Produkt von G mit Γ. Dann hat G in S genau dann ein direktes abgeschlossenes Komplement, wenn Γ auf G durch innere Automorphismen aus G operiert.*

Beweis. Sei S semidirektes Produkt von G und Γ, Γ operiere auf G durch innere Automorphismen. (Diese Bedingung hängt nicht von der Wahl eines Komplements ab. Sie besagt nichts anderes als dass der *kanonische* Morphismus $\Gamma \longrightarrow \mathrm{Out}(G)$ trivial ist.) Sei $\overline{\Gamma} \cong \Gamma$ ein abgeschlossenes Komplement von G in S.

Sei $C_S(G) = \{s \in S | \forall g \in G : sg = gs\}$ der Zentralisator von G in S. Da nach Voraussetzung Γ auf G durch innere Automorphismen operiert, ist $< G \cup C_S(G) >= S$. (*Denn:* Sei $s = g\overline{\delta} \in S, g \in g, \overline{\delta} \in \overline{\Gamma}$. Dann gibt es ein $\alpha \in G$, so dass für alle $h \in G$ gilt: $\alpha^{-1}h\alpha = \overline{\delta}^{-1}h\overline{\delta}$. D.h. $\alpha^{-1}\overline{\delta} \in C_G(S)$. Somit ist $s = (g\alpha)(\alpha^{-1}\overline{\delta}) \in < G \cup C_S(G) >$.)

Es ist $Z(G) = G \cap C_S(G)$ und $C_S(G)/Z(G) = C_S(G)/(G \cap C_S(G)) \cong (C_S(G) \cup G)/G = S/G = \Gamma$. Das Diagramm

$$\begin{tikzcd} 1 \arrow[r] & Z(G) \arrow[r] \arrow[d] & C_S(G) \arrow[r] \arrow[d] & \Gamma \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & G \arrow[r] & S \arrow[r] & \Gamma \arrow[r] & 1 \end{tikzcd}$$

kommutiert. Auch die obere Zeile spaltet, da Γ als projektiv vorausgesetzt wurde. Ein (direktes) abgeschlossenes Komplement von $Z(G)$ in $C_S(G)$ ist auch ein direktes abgeschlossenes Komplement von G in S. $\square$

Proposition 3 *Sei π eine proendliche Gruppe, E eine Teilmenge. Dann ist der Zentralisator $C_\pi(E)$ von E in π eine abgeschlossene Untergruppe von π. Insbesondere ist das Zentrum von π abgeschlossen.*

Beweis. Die Aussage muss nur für einelementige Mengen E nachgewiesen werden, da beliebige Durchschnitte von abgeschlossenen Untergruppen abgeschlossen sind. Sei also $E = \{x\}$.

Seien $p_i : \pi \longrightarrow G_i$ die endlichen Quotienten von π. Dann ist genau dann $x \in C_\pi(x)$, wenn für alle $i \in I$ $x_i \in C_{G_i}(x_i)$ ist. Die Gruppen $C_{G_i}(x_i)$ bilden ein projektives System von endlichen Gruppen, welches $C_{\pi(x)}$ definiert. □

Proposition 4 *Sei G eine proendliche Gruppe, in der das Zentrum ein abgeschlossenes Komplement hat. Sei S ein semidirektes Produkt von G mit einer proendlichen Gruppe Γ. Γ operiere auf G durch innere Automorphismen aus G. Dann hat G in S ein direktes abgeschlossenes Komplement.*

Beweis. Sei C ein abgeschlossenes Komplement von $Z(G)$ in G. Dann hat C selbst triviales Zentrum. Es ist $\mathrm{Inn}(G) \cong G/Z(G) \cong C \cong \mathrm{Inn}(C)$. Nach Wahl eines Schnittes erhalten wir das Diagramm

$$\begin{tikzcd} \Gamma \arrow[r] \arrow[d] & \mathrm{Inn}(C) \arrow[d] \\ \Gamma \arrow[r] & \mathrm{Inn}(G)\ . \end{tikzcd}$$

Daraus folgt das Diagramm mit exakten Zeilen:

$$\begin{tikzcd} 1 \arrow[r] & C \arrow[r] \arrow[d] & C \rtimes \Gamma \arrow[r] \arrow[d] & \Gamma \arrow[r] \arrow[d, equal] & 1 \\ 1 \arrow[r] & G \arrow[r] & S \arrow[r] & \Gamma \arrow[r] & 1 \end{tikzcd}$$

Da C triviales Zentrum hat und die Operation von Γ auf C durch innere Automorphismen gegeben ist, ist der Zentralisator von C in $C \rtimes \Gamma$ ein direktes abgeschlossenes Komplement von C in $C \rtimes \Gamma$. Da die Operation von Γ auf G durch innere Automorphismen aus G gegeben ist, ist sie auf dem Zentrum von G trivial. Deshalb ist der Zentralisator von C in $C \rtimes \Gamma$ nun auch ein direktes abgeschlossenes Komplement von G in S. □

Eine Verschärfung hiervon ist:

Proposition 5 *Sei G eine proendliche Gruppe mit Zentrum $Z(G)$, und sei H eine Untergruppe von G. Die Gruppe $H \cap Z(G)$ besitze ein abgeschlossenes Komplement in H. Sei S ein semidirektes Produnkt von G mit einer proendlichen Gruppe Γ bezüglich eines Morphismus* $\Gamma \longrightarrow \mathrm{Aut}(G)$. *Das Bild dieses Morphismus liege in der Gruppe* $H/(H \cap Z(G)) \hookrightarrow \mathrm{Inn}(G)$.

$$(*) \qquad \begin{tikzcd} \Gamma \arrow[d] \arrow[rrd] & & \\ H/(H \cap Z(G)) \arrow[r, hook] & \mathrm{Inn}(G) \arrow[r, hook] & \mathrm{Aut}(G) \end{tikzcd}$$

Dann hat G in S ein direktes abgeschlossenes Komplement.

Beweis. Wir zeigen Folgendes: Es gibt einen surjektiven Morphismus $\pi : S \longrightarrow G$, so dass die Komposition $\pi\iota : G \longrightarrow G$ ein Isomorphismus ist. Dabei ist $\iota : G \hookrightarrow S$ die Inklusion. Dann ist $K :=$Kern(π) ein direktes abgeschlossenes Komplement von G in S. *Denn*: K ist ein Komplement von G in S und K ist normal und abgeschlossen in S, weil Kerne immer normal und abgeschlossen sind.

Die Inklusion $H/(H \cap Z(G)) \hookrightarrow \operatorname{Aut} G$ definiert ein semidirektes Produkt $G \rtimes H/(H \cap Z(G))$. Das folgende kommutative Diagramm ist nur eine Umformulierung der Bedingung $(*)$.

$$\begin{tikzcd} \Gamma \arrow[r] \arrow[d] & \operatorname{Aut}(G) \arrow[d, equal] \\ H/(H \cap Z(G)) \arrow[r] & \operatorname{Aut}(G) \end{tikzcd}$$

Es definiert einen Morphismus $S \longrightarrow G \rtimes H/(H \cap Z(G))$.

$$\begin{tikzcd} 1 \arrow[r] & G \arrow[r] \arrow[d, equal] & S \arrow[r] \arrow[d] & \Gamma \arrow[r] \arrow[d] & 1 \\ 1 \arrow[r] & G \arrow[r] & G \rtimes H/(H \cap Z(G)) \arrow[r] & H/(H \cap Z(G)) \arrow[r] & 1 \end{tikzcd}$$

Sei C ein (direktes) Komlement von $H \cap Z(G)$ in H. Es ist $H/(H \cap Z(G)) = C$. Somit ist

$$G \rtimes H/(H \cap Z(G)) = G \rtimes C,$$

wobei C auf G durch Konjugation operiert.

Nun ist $G \rtimes C$ isomorph zu $G \times C$. Der Isomorphismus ist durch

$$\phi : G \rtimes C \longrightarrow G \times C, (g, c) \mapsto (gc, c)$$

gegeben. Es induziert die Identität auf G. Surjektivität und Injektivität von ϕ ist klar. Bleibt noch zu zeigen, dass es sich um einen Isomorphismus handelt. Es ist

$$\phi((g_1, c_1)(g_2, c_2)) = \phi(g_1 c_1 g_2 c_1^{-1}, c_1 c_2) = (g_1 c_1 g_2 c_1^{-1} c_1 c_2, c_1 c_2) =$$

$$(g_1 c_1, c_1)(g_2 c_2, c_2) = \phi(g_1, c_1)\phi(g_2, c_2)$$

Somit gibt es einen surjektiven Morphismus

$$\pi : \; S \longrightarrow G \rtimes H/(Z(G) \cap H) \cong G \times C \longrightarrow G \, .$$

Der Morphismus $\pi\iota : G \hookrightarrow S \longrightarrow G$ ist die Identität. $\square$

pro-p-Gruppen

Definition Sei π eine proendliche Gruppe und p eine Primzahl. Wir sagen, π habe *Ordnung p* oder sei eine *pro-p-Gruppe*, wenn alle endlichen Quotienten von π p-Gruppen sind. Falls alle endlichen Quotienten von π quasi-p-Gruppen sind, d.h. von Elementen der Ordnung p bzw. ihren p-Sylowgruppen erzeugt werden, so nennen wir π eine *proendliche quasi-p-Gruppe*. Falls alle endlichen Quotienten eine zu p prime Ordnung haben, so sagen wir die Gruppe habe *Ordnung prim zu p* oder sei eine *proendliche zu p prime Gruppe*.

Die *maximale quasi-p-Untergruppe* $p(\pi)$ von π ist definiert als

$$p(\pi) = \varprojlim_{\substack{G \text{ endlicher Quotient} \\ \text{von } \pi}} p(G).$$

Dabei ist $p(G)$ die Untergruppe von G, die von allen p-Sylowgruppen von G (von allen Elementen, deren Ordnung eine p-Potenz ist) erzeugt wird. $p(\pi)$ ist eine proendliche quasi-p-Gruppe. Die Inklusionen $p(G) \longrightarrow G$ induzieren eine Injektion $\pi \longrightarrow p(\pi)$. Definitionsgemäß ist $p(\pi)$ kompakt und damit abgeschlossen in π.

Die maximale quasi-p-Untergruppe von π hat folgende universelle Eigenschaft: Sei $\psi : \Pi \longrightarrow \pi$ ein Morphismus, wobei Π eine proendliche quasi-p-Gruppe ist. Dann faktorisiert ψ eindeutig über $p(\pi)$.
Beweis. Sei $\pi \longrightarrow G$ ein endlicher Quotient. Dann gibt es aufgrund der Stetigkeit von ψ einen endlichen Quotienten $\Pi \longrightarrow H$, so dass das Diagramm

$$\begin{tikzcd} \Pi \arrow[r, "\psi"] \arrow[d] & \pi \arrow[d] \\ H \arrow[r] & G \end{tikzcd}$$

kommutiert. Dabei ist das Bild der quasi-p-Gruppe H in $p(G)$ enthalten. Insgesamt ist das Bild von ψ in $\varprojlim p(G) = p(\pi)$ enthalten. □

Mit dieser Betrachtung sieht man, dass $p(\pi)$ die größte quasi-p-Untergruppe von π ist. Daraus folgt, dass $p(\pi)$ charakteristisch ist.

Der *maximale p-prime Quotient* von π ist der Quotient $\pi^{(p')} := \pi/p(\pi)$. Es ist

$$\pi^{(p')} = \varprojlim_{\substack{G \text{ endlicher Quotient} \\ \text{von } \pi}} G/p(G),$$

denn der Funktor $\varprojlim -$ ist auf projektiven Systemen von endlichen Gruppen (allgemeiner kompakten topologischen Gruppen) exakt ([Ne, IV, (2.7)]). In unserem Kontext bedeutet dies, dass die Sequenz

$$1 \longrightarrow \lim_{\longleftarrow} p(G) \longrightarrow \lim_{\longleftarrow} G \longrightarrow \lim_{\longleftarrow} G/p(G) \longrightarrow 1$$

exakt ist. Schwierig ist nur die Surjektivität der Abbildung $\lim_{\longleftarrow} G \longrightarrow \lim_{\longleftarrow} G/p(G)$. Diese wird mit Hilfe der Kompaktheit von π bewiesen. Sei $(x_G)_{G \text{ endl. Quotient von} \pi} \in \lim_{\longleftarrow} G/p(G)$. Sei U_G die Urbildmenge von x_G in π. Die U_G sind nicht-leer und haben die Eigenschaft, dass alle endlichen Schnitte nicht-leer sind. Die U_G sind abgeschlossen und als Teilmenge eines kompakten Raumes kompakt. Damit ist der Schnitt $U := \bigcap_{G \text{ endl. Quotient von } \pi} U_G$ nicht-leer. Ein beliebiges Element aus U wird auf x abgebildet.

$\pi^{(p')}$ hat folgende universelle Eigenschaft: Sei Π eine proendliche Gruppe mit Ordnung prim zu p und sei $\psi : \pi \longrightarrow \Pi$ ein Morphismus. Dann faktorisiert ψ eindeutig über $\pi^{(p')}$. Der *Beweis* ist genauso einfach wie der der universellen Eigenschaft von $p(\pi)$.

Sei π eine proendliche Gruppe. Dann ist eine *p-Sylowgruppe* von π eine abgeschlossene Untergruppe π_p, deren endliche Quotienten p-Sylowgruppen der entsprechenden Quotienten von π sind, d.h. für jeden surjektiven Morphismus $\phi : \pi \longrightarrow G$ in eine endliche Gruppe G ist $\phi(\pi_p)$ eine p-Sylowgruppe von G. Wir zeigen nun, dass analog zu endlichen Gruppen p-Sylowgruppen immer existieren, zwei p-Sylowgruppen immer konjugiert sind und dass die maximale quasi-p-Untergruppe von den p-Sylowgruppen topologisch erzeugt wird.

Proposition 6 *Jede proendliche Gruppe besitzt eine p-Sylowgruppe.*

Beweis. Sei $\pi = \lim_{\longleftarrow} G_i$, eine proendliche Gruppe, wobei die G_i die endlichen Quotienten seien. Sei jeweils S_i eine p-Sylowgruppe von G_i. Wir betrachten für $i > j$

$$A_{ij} := \{\alpha = (\alpha_i)_i \in \prod_i G_i | p_{ij}(\alpha_i S_i \alpha_i^{-1}) = \alpha_j S_j \alpha_j^{-1}\}.$$

Die A_{ij} sind abgeschlossen in der kompakten Menge $\prod_i G_i$. Sie sind nicht-leer, da p-Sylowgruppen in endlichen Gruppen stets konjugiert sind. Auch endliche Durchschnitte von verschiedenen A_{ij} sind nicht-leer. Dies sieht man folgendermaßen: Seien $i_1, ..., i_l, j_1, ..., j_l$ endlich viele Elemente aus der Indexmenge mit $i_k > j_k$. Sei $A^* := \bigcap_k A_{i_k j_k}$. Wähle ein n mit $n \geq i_k$ für alle k. Wähle nun für alle $i < n$ ein $\alpha_i \in G_i$ mit $p_{ni}(S_n) = \alpha_i S_i \alpha_i^{-1}$. Ergänze dies zu einem $\alpha \in \prod_i G_i$. Dann ist für alle k:

$$p_{i_k j_k}(\alpha_{i_k} S_{i_k} \alpha_{i_k}^{-1}) = p_{n j_k}(S_n) = \alpha_{j_k} S_{j_k} \alpha_{j_k}^{-1}$$

Also $\alpha \in A^*$.

Aufgrund der Kompaktheit des Produkts ist $A := \bigcap_{i>j} A_{ij}$ nicht-leer. Für $\alpha \in A$ definiert das projektive System $(\alpha_i S_i \alpha_i^{-1})_i$ eine p-Sylowgruppe in π. $\square$

Proposition 7 *Je zwei p-Sylowgruppen einer proendlichen Gruppe π sind konjugiert.*

Beweis. Seien S, S' zwei p-Sylowgruppen von π. Sei für alle endlichen Quotienten G_i von π: $T_i := \{\alpha_i \in G_i | \alpha_i S_i \alpha_i^{-1} = S_i'\}$. Diese Mengen bilden ein projektives System von nicht-leeren endlichen Mengen. Damit ist $T := \lim_{\longleftarrow} T_i \leq \pi$ nichtleer. Für ein beliebiges Element $\alpha \in T$ gilt $\alpha S \alpha^{-1} = S$. □

Proposition 8 *Die maximale quasi-p-Untergruppe einer proendlichen Gruppe wird von den p-Sylowgruppen topologisch erzeugt, d.h. der maximale p-prime Quotient ist die abgeschlossene Hülle des Erzeugnisses der p-Sylowgruppen.*

Beweis. Es ist zu zeigen, dass für alle endlichen Quotienten G_i der proendlichen Gruppe π gilt: Die Quotienten des topologischen Erzeugnisses der p-Sylowgruppen erzeugen $p(G_i)$.

Nach Definition sind alle p-Sylowgruppen in der maximalen quasi-p-Untergruppe enthalten. Andererseits gibt es zu jeder p-Sylowgruppe $S_i \leq G_i$ eine p-Sylowgruppe von π, die mit p_i auf S_i abgebildet wird. Dies sieht man folgendermaßen: Sei π_p eine feste p-Sylowgruppe von π. Es ist $p_i(\pi_p) = \alpha_i S_i \alpha_i^{-1}$ mit einem $\alpha_i \in G_i$. Sei $\alpha \in \pi$ ein Urbild von α_i. Dann ist $\alpha^{-1}\pi_p\alpha$ die gesuchte p-Sylowgruppe. □

Analog zur maximalen quasi-p-Untergruppe einer proendlichen Gruppe ist die *maximale quasi-p-prime Untergruppe* definiert. Sei π eine proendliche Gruppe. Dann ist

$$p'(\pi) := \lim_{\substack{\longleftarrow \\ G \text{ endlicher Quotient} \\ \text{von } \pi}} p'(G).$$

Dabei ist $p'(G)$ die Untergruppe von G, die von allen l-Sylowgruppen ($l \neq p$) (von allen Elementen, deren Ordnung nicht von p geteilt wird) erzeugt wird. Analog zu $p(\pi)$ wird $p'(\pi)$ von allen l-Sylowgruppen ($l \neq p$) von π topologisch erzeugt.

Der *maximale p-Quotient* von π ist nun $\pi^{(p)} := \pi/p'(\pi)$. Es ist

$$\pi^{(p)} = \lim_{\substack{\longleftarrow \\ G \text{ endlicher Quotient} \\ \text{von } \pi}} G/p'(G).$$

Auch die maximale quasi-p-prime Untergruppe bzw. der maximale p-Quotient erfüllen die offensichtlichen universellen Eigenschaften.

Freie Objekte

Definition (nach [Se2, I,1.5.]) Sei $\mathcal{C}$ eine Unterkategorie der Kategorie der proendlichen Gruppen. Sei I eine beliebige Menge. Ein *freies Objekt* auf der Menge

I ist eine proendliche Gruppe $\hat{F}_{\mathcal{C}}(I)$ auf $\mathcal{C}$ mit einer Abbildung $I \longrightarrow \hat{F}_{\mathcal{C}}(I)$, so dass in jeder Umgebung der Null fast alle Bilder von I liegen (d.h. das Bild des durch die Komplemente von endlichen Mengen definierten Filters konvergiert gegen Null) und folgender universeller Eigenschaft: Für jede proendliche Gruppe Π definiert die Zuordnung $(f : F_{\mathcal{C}}(I) \longrightarrow \Pi) \mapsto (I \longrightarrow f(i))$ eine Bijektion zwischen der Menge der Morphismen von $\hat{F}_{\mathcal{C}}(I)$ nach Π und der Menge der gegen Null konvergenten Abbildungen von I nach $\hat{F}_{\mathcal{C}}(I)$. Man sieht sofort, dass ein freies Objekt bis auf eindeutige Isomorphie eindeutig bestimmt ist.

Sei $\mathcal{C}$ die volle Kategorie der proendlichen Gruppen. Sei $F(I)$ die freie Gruppe auf I. Dann ist $\hat{F}(I)$, die *freie proendliche Gruppe auf* I, die proendliche Gruppe, die durch das projektive System $F(I)/N$, N Normalteiler in $F(I)$ bestimmt wird, wobei $F(I)/N$ endlich ist *und* fast alle Erzeugenden aus I enthält. Insbesondere, falls I endlich ist, so ist $\hat{F}(I)$ die proendliche Komplettierung von $F(I)$. Die universelle Eigenschaft von $\lim_{\longleftarrow} F(I)/N$ folgt aus der von $F(I)$.

Weiterhin sieht man sofort: Der maximale p-prime Quotient von $\hat{F}(I)$ ist ein freies Objekt auf I in der Kategorie der p-primen proendlichen Gruppen, der maximale p-Quotient von $F(I)$ ist ein freies Objekt auf I in der Kategorie der proendlichen p-Gruppen. Man spricht von freien proendlichen p-primen Gruppen bzw. freien pro-p-Gruppen.

Die *freie abelsche proendliche Gruppe* auf I, d.h. das freie Objekt in der Kategorie der abelschen proendlichen Gruppen, ist die Abelisierung der freien proendlichen Gruppe auf I. Man kann sie auch analog zur Konstruktion der freien proendlichen Gruppe auf I direkt aus der freien abelschen Gruppe auf I konstruieren. Die freie abelsche proendliche p-prime Gruppe ist einerseits der maximale p-prime Quotient der freien abelschen proendlichen Gruppe, andererseits die Abelisierung der freien proendlichen p-primen Gruppe. Analoges gilt für freie abelsche pro-p-Gruppen.

Kohomologie proendlicher Gruppen

Es folgt eine kurze Darstellung der verwendeten Definitionen und Ergebnisse über die Kohomologie proendlicher Gruppen. Dabei wird die Kohomologie endlicher Gruppen als bekannt vorausgesetzt.

Definition Sei π eine proendliche Gruppe. Ein *diskreter π-Modul* ist ein Modul A mit einer π-Operation, so dass der Stabilisator jeden Elementes eine offene Untergruppe in π ist, d.h.

$$A = \bigcup A^U,$$

wobei U die offenen Untergruppen von π durchläuft.

Für solche Moduln kann man wie für Moduln endlicher Gruppen Kohomologiegruppen definieren. [Se2, I, 2] Die inhomogenen n-Ketten $C^q(\pi, A)$ sind die *stetigen* Abbildungen von π^n nach A und die Kohomologiegruppen von π mit Werten in A die Kohomologiegruppen des mit der üblichen Korandabbildung definierten Komplexes. Es ist

$$H^n(\pi, A) = \varinjlim H^n(\pi/U, A^U).$$

Jede abelsche Torsionsgruppe ist direkte Summe ihrer p-Primärbestandteile. Die *kohomologische p-Dimension von π*, Bezeichnung $cd_p(\pi)$ ist das Minimum über alle n, die folgende Bedingung erfüllen:

Für alle diskreten π-Torsionsmoduln A und für alle $q > n$
ist die p-Primärkomponente von $H^q(\pi, A)$ gleich Null

(Die kohomologische Dimension ist ∞, falls es keine solche untere Schranke gibt.) Die *kohomologische Dimension von π* ist analog definiert als das Minimum über alle n, für die stets $H^q(\pi, A)$ gleich Null ist ($q > n$). Es ist $cd(\pi) = \sup_p cd_p(\pi)$.

Aus [Se2, I, 3.1. Proposition 11 und Proposition 12] folgt:

Proposition 9 *Sei π eine pro-p-Gruppe. Dann ist $cd_p(\pi) = cd(\pi)$.*

Proposition 10 *[Se2, I, 3.3. Proposition 14] Sei π eine proendliche Gruppe und Π eine Untergruppe. Dann ist $cd_p(\Pi) \leq cd_p(\pi)$. Gleichheit gilt insbesondere dann, wenn die alle Indices $(\pi/U : \Pi/(\Pi \cap U))$ - wobei U alle offenen Untergruppen von π durchläuft - prim zu p sind.*

Daraus folgt:

Korollar 1 *Sei π_p eine p-Sylowgruppe von π. Dann ist $cd(\pi_p) = cd_p(\pi_p) = cd_p(\pi)$.*

Und es folgt:

Korollar 2 *Es ist genau dann $cd_p(\pi) = 0$, wenn π zu p prime Ordnung hat. Insbesondere ist eine p-Gruppe genau dann trivial, wenn sie kohomologische Dimension Null hat.*

Proposition 11 *[Se2, I,3.4. Proposition 16] Sei π proendliche Gruppe. Dann sind äquivalent :*

- *Jede Sequenz*
$$1 \longrightarrow A \longrightarrow E \longrightarrow \pi \longrightarrow 1\ ,$$
wobei A eine abelsche pro-p-Gruppe ist, spaltet.
- *Jede Sequenz*
$$1 \longrightarrow A \longrightarrow E \longrightarrow \pi \longrightarrow 1\ ,$$
wobei A eine beliebige pro-p-Gruppe ist, spaltet.
- *π hat kohomologische p-Dimension ≤ 1*

Proposition 12 *[Se2, I, 4.2., Corollaire 2 zu Proposition 24] Sei π eine pro-p-Gruppe. Dann ist $cd_p(\pi) = cd(\pi)$. Es sind äquivalent*

- *π ist eine freie pro-p-Gruppe*
- *π hat kohomologische Dimension ≤ 1*

Sei k ein Körper, Γ_k die absolute Galoisgruppe von k. Die kohomologische Untersuchung von Γ_k wird *Galoiskohomologie* genannt. Γ_k operiert diskret auf der additiven Gruppe $(k^{\text{sep}}, +)$ und der multiplikativen Gruppe $(k^{\text{sep}\,*}, *)$.

Proposition 13 *[Se1, X, Proposition 1, Proposition 2] Es ist*

- $H^n(\Gamma_k, k^{\text{sep}}) = 0$ *für alle* $n \geq 1$
- $H^1(\Gamma_k, k^{\text{sep}\,*}) = 0$

Dies impliziert den Satz Hilbert 90 und die Kummer- und Artin-Schreier-Theorie. [Se1, X, 3]

Es folgt auch:

Proposition 14 *[Se2, II,2.2. Proposition 3 (mit Beweis), Corollaire 1] Sei k ein Körper mit Charakteristik p. Sei π_p eine p-Sylowgruppe von Γ_k. Dann ist $cd(\pi_p) \leq 1, cd_p(\Gamma_k) \leq 1, cd(\Gamma_k^{(p)}) \leq 1$. D.h. jede p-Sylowgruppe und der maximale p-Quotient der absoluten Galoisgruppe eines Körper mit Charakteristik p sind freie pro-p-Gruppen.*

Literaturverzeichnis

[Ab] Abhyankar, S. , Coverings of Algebraic Curves, Amer.J.Math. **79** (1957) 825-856

[Beck] Beckmann, S., On Extensions of Number Fields obtained by specializing Branched Coverings, Journal für die reine und angewandte Mathematik **419** (1991) 27-53

[Belyi] Belyi, G.V., On Galois Extensions of a Maximal Cyclotomic Field, Math. USSR Izvestija **14** (1980) 247-256 (englische Übersetzung des russischen Originals)

[Bo] Bosch, S., Algebra, Springer-Verlag, Berlin (1991)

[KPR] Kuhlmann, F.-V., Pank, M., Roquette, P., Immediate and Purly Wild Extentions of Valued Fields, Manuscripta Mathematica **55** (1986) 39-67

[Ei] Eisenbud, D., Commutative Algebra with a View Toward Algebraic Geometry , Springer-Verlag, New York (1994)

[En] Endler, O., Valuation Theory, Springer-Verlag, Berlin (1970)

[Ja] Jacobson, N., Basic Algebra II, W.H.Freeman and Company, New York (1989)

[FJ] Fried, M., Jarden, M., Field Arithmetics, Springer-Verlag, Berlin (1986)

[Fo] Forster, O., Lectures on Riemann Surfaces, Springer-Verlag, Berlin (1993)

[Fu] Fulton, W., Hurwitz Schemes and Irreducibility of Moduli of Algebraic Curves, Ann. Math. **90** (1969) 542-575

[Ha] Hartshorne, R., Algebraic Geometry, Springer-Verlag, New-York (1977)

[La] Lang, S., Algebra, Third Edition, Addison-Wesley, Reading (1993)

[MM] Malle, G., Matzat, B.H., Inverse Galois Theory, Springer-Verlag, Berlin (erscheint demnächst)

[Mu] Mumford, D., The Red Book of Varieties and Schemes, Springer-Verlag, Berlin (1994)

[Ne] Neukirch, J., Algebraische Zahlentheorie, Springer-Verlag, Berlin (1992)

[Pop] Pop, F., $\frac{1}{2}$ Riemann Existence Theorem with Galois Action, in Algebra and Number Theory, ed. Frey, G., Ritter, J., de Gruyter Proceedings in Mathematics, Berlin (1994)

[Popp] Popp, H., Fundamentalgruppen algebraischer Mannigfaltigkeiten, Springer-Verlag, Berlin (1970)

[Re] Reyssat, E., Quelques Aspects des Surfaces de Riemann, Birkhäuser, Boston (1989)

[SGA I] Grothendieck, A., Séminaire de Geometrie Algebrique 1960-61: Revêtements Etales et Groupe Fondamentale (SGA I), Institut des Hautes Etudes Scientifiques, Paris (1961)

[Se1] Serre, J.-P., Corps Locaux, Hermann, Paris (1962)

[Se2] Serre, J.-P., Cohomologie Galoisienne, Springer-Verlag, Berlin (1965)

[ZS] Zariski, O., Samuel, P., Commutative Algebra, D. van Nostrand Company, Princeton (1960)