Zum p-Rang von Kurven mit Automorphismen

Abschätzungen, Kongruenzformeln, Borne-Invarianten.

Nicolas Stalder

Diplomarbeit in Mathematik
ETH Zürich, 2003

Betreuer: Prof. Dr. Richard Pink

Inhaltsverzeichnis

Zum Geleit

Gegeben eine glatte projektive zusammenhängende Kurve über einem algebraisch abgeschlossenen Körper; welches sind die globalen Invarianten, die uns die Maschinerie der Cohomologietheorie liefert? Als erstes können wir die Cohomologie mit Koeffizienten in der Strukturgarbe berechnen und deren Dimension anschauen. Im Grad 0 erhalten wir einen 1-dimensionalen Vektorraum, da die Kurve zusammenhängend ist. Im Grad 1 haben wir einen g-dimensionalen Vektorraum, dabei ist g das *Geschlecht* der Kurve, ihre wichtigste Invariante überhaupt. In allen anderen Graden verschwindet die Cohomologie. Ist die Kurve darüber hinaus über einem Körper positiver Charakteristik definiert, so trägt sie einen kanonischen Endomorphismus, die *Frobenius-Abbildung*. Diese Abbildung induziert natürliche Endomorphismen der Cohomologie-Vektorräume, welche jedoch nicht linear, sondern *p-linear* sind. Eine solche Abbildung spaltet eindeutig in die direkte Summe einer bijektiven und einer nilpotenten Abbildung. Die Dimension des bijektiven Anteils heisst der *stabile Rang* der Abbildung. Angewandt auf die induzierte Frobenius-Abbildung im Grad 0 der Cohomologie erhalten wir nichts Neues, der stabile Rang des Frobenius im Grad 1 der Cohomologie hingegen ist eine *neue* Invariante, der *p-Rang* der Kurve.

Über diese neue Invariante soll in der vorliegenden Arbeit gesprochen werden. Es ist bekannt, dass der p-Rang einer hinreichend generischen Kurve mit dem Geschlecht übereinstimmt, und dass Automorphismen einer Kurve den p-Rang beeinflussen können. Was dieser Einfluss ist, welche Abschätzungen des p-Rangs wir aufgrund vorhandener Automorphismen angeben können, das wollen wir untersuchen, und das war der Ausgangspunkt dieser Diplomarbeit. Insbesondere interessiert uns der Zusammenhang zwischen dem p-Rang einer Kurve und dem p-Rang der Quotientenkurve nach einer endlichen Untergruppe der Automorphismengruppe. Erste Resultate wurden von Nakajima in [**Nak1**] durch findiges Kombinieren der Riemann-Hurwitz-Formel mit der Deuring-Schafarewitsch-Formel erzielt. In dieser Arbeit wird jedoch, wie in [**Nak2**] und [**Bor1**], ein anderer Ansatz verfolgt: Der bijektive Anteil der ersten Cohomologiegruppe, dessen Dimension der p-Rang ist, trägt eine Darstellung der endlichen Gruppe, welche mittels modularer Darstellungstheorie untersucht wird.

Leitfaden

Das erste Kapitel repetiert bekannte Tatsachen; die neuen Resultate, welche unter anderem *Kongruenzformeln* für den p-Rang zur Folge haben, werden in Kapitel 2 bis 4 dargestellt.

Im ersten Kapitel wiederholen wir einige Resultate der p-linearen Algebra, führen die Hasse-Witt-Matrix ein, definieren den p-Rang einer Kurve und zeigen die verschiedenen Bedeutungen auf, welche der p-Rang einer Kurve hat.

Im zweiten Kapitel wiederholen wir den Beweis der Deuring-Schafarewitsch-Formel im Rahmen der étalen Cohomologie. Dieses Kapitel ist von Pinks Darstellung im Artikel [**Pin1**] inspiriert, und zeigt den Einfluss des p-Rangs eines Galoisquotienten einer Kurve auf den p-Rang der Kurve selber auf. Wir finden hier eine *erste Kongruenzformel* für den p-Rang modulo einer Zahl N, die von der Gruppe G abhängt.

Im dritten Kapitel, das von Bornes Artikel [**Bor1**] inspiriert ist, untersuchen wir die Darstellung der Galoisgruppe, welche dem p-Rang zu Grunde liegt. Wir erhalten ein Kriterium für die Projektivität dieser Darstellung, und finden eine *zweite Kongruenzformel* für den p-Rang. Diese ist äquivalent zur ersten. Darüber hinaus ermitteln wir die *Seele* der obengenannten Darstellung, also den Isomorphietyp der Summe aller nicht-projektiven direkten Summanden einer Zerlegung der Darstellung in unzerlegbare direkte Summanden. Diese Seele hängt bloss von den Stabilisatoren der Operation von G auf der Kurve ab.

Im vierten Kapitel beweisen wir eine Verallgemeinerung eines Resultates von Borne. Es betrifft die Multiplizitäten der projektiven Summanden in einer Zerlegung der dem p-Rang zugrundeliegenden Darstellung, die wir *Borne-Invarianten* nennen. Das Resultat zeigt den Zusammenhang zwischen Kurven und ihren Galoisschen Quotientenkurven auf: Jede Borne-Invariante einer Quotientenkurve, zusammen mit Verzweigungsdaten, legt eine Borne-Invariante der ursprünglichen Kurve fest.

Im fünften Kapitel wird in sehr expliziter Weise eine Kurve X konstruiert, welche die Gruppe S_3 als Automorphismen zulässt. Anhand dieses und anderer Beispiele sehen wir die Auswirkungen der Resultate aus den Kapiteln 2 bis 4.

Im sechsten und letzten Kapitel stehen einige teils sehr spekulative Vermutungen – *quasi una fantasia*. Ich hoffe, einen gewissen Anteil dieser Vermutungen zu einem späteren Zeitpunkt präzisieren und beweisen zu können.

Im Anhang stehen zur Referenz einige Grundlagen der modularen Darstellungstheorie bereit, allerdings ohne Beweise, und ich erkläre, wie man mit einem Computeralgebrasystem den p-Rang von Kurven bestimmen kann.

Terminologie und Konventionen

Der Buchstabe p bezeichnet eine Primzahl. Der Buchstabe k bezeichnet, wenn nicht anders gekennzeichnet, einen algebraisch abgeschlossenen Körper der Charakteristik $p > 0$. Eine *Kurve* ist ein vollständiges, glattes, ganzes, zusammenhängendes Schema der Dimension 1 über k. Ist X eine Kurve, so ist mit der Notation $P \in X$ stets ein *abgeschlossener* k-wertiger Punkt von X gemeint, und v_P bezeichnet dann die Bewertung an diesem Punkt. Der Funktionenkörper einer Kurve X ist $k(X)$. Die Abbildung

$$\begin{aligned} \mathrm{Frob} : k &\longrightarrow k \\ x &\longmapsto x^p \end{aligned}$$

ist ein Automorphismus des Körpers k, den wir Frobenius nennen. Jede Kurve über k trägt als Endomorphismus den *absoluten Frobenius*, den wir mit Frob bezeichnen. Dieser ist auf dem topologischen Raum die Identität und erhebt Schnitte der Strukturgarbe zur p-ten Potenz. Mit Frob bezeichnen wir auch die Abbildungen, welche Frob auf den Cohomologiegruppen von X mit Koeffizienten in der Strukturgarbe induziert.

Eine *Überlagerung* einer Kurve Y durch eine Kurve X ist ein separabler endlicher Morphismus $\pi : X \longrightarrow Y$. Sie heisst *unverzweigt*, oder *étale*, falls jeder Punkt $y \in Y$ dieselbe Anzahl Urbilder in X hat; diese Anzahl stimmt dann mit dem Grad von π, also dem Grad der zugehörigen Körpererweiterung $k(Y) \subset k(X)$ überein. Die Überlagerung heisst Galoissch, falls die Körpererweiterung $k(Y) \subset k(X)$ Galoissch ist; das ist gleichbedeutend damit, dass G auf X operiert und dass sich Y als kategorischer Quotient X/G von X nach der Galoisgruppe $G = \mathrm{Gal}(X/Y) \subset \mathrm{Aut}_k(X)$ schreiben lässt.

Eine (endlich-dimensionale) Darstellung einer endlichen Gruppe G über einem Körper k ist dasselbe wie ein (endlich erzeugter) Modul M des Gruppenringes $k[G]$. Das Symbol $M \sim N$ bedeutet, dass M und N denselben modularen Charakter haben, dass sie also dieselben Kompositionsfaktoren besitzen. Ist k ein festgehaltener algebraisch abgeschlossener Grundkörper, so bezeichnet S_G ein Repräsentantensystem der Isomorphieklassen der irreduziblen Darstellungen von G über k.

Das Symbol $\therefore$ signalisiert das Ende eines Beweises.

Danksagung

Ich bedanke mich an dieser Stelle bei den folgenden Personen, welche in direkter oder indirekter Weise diese Diplomarbeit ermöglicht haben: Christian Ausoni, Paul Balmer, Simon Baumann, Claudia Biber, Gebhard Böckle, Theo Bühler, Ines Feller, Gilbert Durand, Andreas Felder, Martin Lotz, Srdjan Micic, Guido Mislin, Richard Pink, Arne

Schrenk, Aline Stalder, Bernard Stalder, Philippe Stalder, Beat Steiner, Matthias Traulsen, Tom Weinmann.

Motto

You may love representation theory, or probability and so on, but remember, the most beautiful area in mathematics is geometry.

(V.A. Rokhlin – Rat an A.M. Vershik).

KAPITEL 1

Bekanntes

1.1. p-lineare Algebra

Seien R, S zwei Ringe, M ein R-Modul, und N ein S-Modul. Ein *Dimorphismus* von M nach N ist ein Paar (f, g) bestehend aus einem Ringhomomorphismus $f : R \longrightarrow S$ und einem Gruppenhomomorphismus $g : M \longrightarrow N$, welcher die Bedingung $g(rm) = f(r)g(m)$ für alle $r \in R$ und $m \in M$ erfüllt. Der Spezialfall $R = S$ und $f = \mathrm{id}_R$ entspricht also einem Homomorphismus von R-Moduln; uns interessiert jedoch der Fall wo $R = k$ ein Körper positiver Charakteristik p ist, und $f = \mathrm{Frob}$ der Frobenius ist.

Definition 1.1.1 (p^n-lineare Abbildungen). Sei V ein Vektorraum über einem (falls n¡0 ist perfekten) Körper k der Charakteristik $p > 0$, und $n \in \mathbb{Z}$. Eine additive Abbildung $F : V \longrightarrow V$ heisst *p^n-linear*, falls für alle $\lambda \in k$ und $v \in V$ die folgende Gleichung gilt:

$$F(\lambda v) = \lambda^{p^n} v.$$

Ist V endlichdimensional und $\mathcal{B} = \{b_i\}$ eine Basis von V, so ist eine p-lineare Abbildung durch die Bilder der Basisvektoren festgelegt. Wir identifizieren vermittels $\mathcal{B}$ im folgenden V mit k^n. Die Matrix $A = (a_{ij})$ von F, entsteht wie in der linearen Algebra, indem man die Koordinaten der Bilder der Basisvektoren als Spalten von A schreibt. Beispielsweise entspricht die Einheitsmatrix der Abbildung $v \mapsto v^{(p)}$, welche die Koeffizienten der Basisdarstellung von v zur p-ten Potenz erhebt. Eine allgemeine p-lineare Abbildung hat auf k^n die Gestalt

$$F(v) = A \cdot v^{(p)},$$

wo rechts die gewöhnliche Matrixmultiplikation gemeint ist.

Ist $\mathcal{B}'$ eine zweite Basis, und S die Matrix der Koordinatentransformation, welche $\mathcal{B}'$-Koordinaten in $\mathcal{B}$-Koordinaten verwandelt, so ist die Matrix von F bezüglich der Basis $\mathcal{B}'$ durch $S^{-1}AS^{(p)}$ gegeben; dabei bezeichnet $S^{(p)}$ wieder die Matrix, welche aus S durch Erhebung ihrer Einträge zur p-ten Potenz entsteht. Die Matrix von F^n ist $A.A^{(p)}.A^{(p^2)}. \cdots .A^{(p^{n-1})} =: A^{[n]}$.

Der Begriff des Eigenwerts macht wenig Sinn für p-lineare Abbildungen, denn gilt $F(v) = \lambda v$ mit $\lambda \neq 0$, und ist $0 \neq \mu \in k$ beliebig, so gilt für $w := \mu v$ die Gleichung $F(w) = F(\mu v) = \mu^p F(v) = \mu^{p-1}\lambda w$; Eigenvektoren zu vorgegebenem Eigenwert bilden also keinen

k-Untervektorraum. Wir können aber immer noch zwischen dem Eigenraum zum Eigenwert 0 und dem Eigenraum *aller* Eigenwerte ungleich 0 unterscheiden.

PROPOSITION 1.1.2. *Sei V endlich dimensional der Dimension g, und $F : V \longrightarrow V$ p-linear. Setze $V^F = \{v \in V : F(v) = v\}$, sei V^s der von V^F aufgespannte k-Untervektorraum von V, und sei $V^n = \{v \in V : F^m(v) = 0$ für $m \gg 0\}$. Dann gilt*

(i) *V^F ist ein $\mathbb{F}_p$-Untervektorraum von V.*
(ii) $\dim_{\mathbb{F}_p} V^F = \dim_k V^s = \operatorname{rang} A^{[g]} \leq \dim_k V$
(iii) $V = V^s \oplus V^n$.
(iv) *Die Abbildung F operiert auf V^s bijektiv, auf V^n nilpotent.*
(v) *Es gilt $V^s = \bigcap_{m \geq 0} \operatorname{Bild}(F^m)$, und $V^n = \bigcup_{m \geq 0} \operatorname{Ker}(F^m)$.*

BEWEIS. Für den klassischen Beweis, siehe [**Has1**]. Ein moderner Beweis via der Korrespondenz von p-Liealgebren und endlichen Gruppenschemata findet sich in [**Mum1**], III.14. $\therefore$

Wir nennen V^s den *halbeinfachen* Anteil von V bezüglich F, und V^n den *nilpotenten* Anteil. Die Dimension von V^s heisst der *stabile Rang* von F.

BEMERKUNG 1.1.3 (Funktorialität). Die Zuordnungen $V \rightsquigarrow V^s$ und $V \rightsquigarrow V^n$ sind funktoriell: Paare (V, F) bestehend aus einem endlichdimensionalen Vektorraum V und einer p-linearen Abbildung F bilden die Objekte einer Kategorie, in welcher die Morphismen durch lineare Abbildungen $f : V \longrightarrow V'$ gegeben sind, welche zusätzlich mit den p-linearen Abbildungen kommutieren sollen: $fF = F'f$. Die Zuordnung $(V, F) \rightsquigarrow V^s$ ist dann ein *exakter* additiver Funktor von der obigen Kategorie nach der Kategorie der endlichdimensionalen Vektorräume.

Ist F eine p-lineare Abbildung auf V, so wird auf dem Dualraum $V' = \operatorname{Hom}_k(V, k)$ durch die Vorschrift $C(\psi)(v) := \psi(F(v))^p$ eine Abbildung C induziert, welche dann p^{-1}-linear ist. Zur Zerlegung von V gehört eine duale Zerlegung von V', dabei hat C denselben stabilen Rang wie F. Da sich jede p^{-1}-lineare Abbildung als duale einer p-linearen auffassen lässt, überträgt sich die Strukturtheorie der p-linearen auf p^{-1}-lineare Abbildungen.

1.2. Beispiel: Der p-Rang einer Kurve

Uns interessiert die folgende p-lineare Abbildung. Sei X eine Kurve, und sei $F = \operatorname{Frob}$ der Frobeniusendomorphismus von X. Auf jeder Cohomologiegruppe $H^i(X, \mathcal{O}_X)$ induziert Frob einen Gruppenhomomorphismus. Dieser ist p-linear, wie man z.B. via Cech-Cohomologie einsieht. Auf $H^0(X, \mathcal{O}_X) = k$ wird der gewöhnliche Frobenius induziert, und es gilt dann $k = k^s$. Interessant ist hingegen die erste Cohomologie.

Definition 1.2.1 (p-Rang). Der *p-Rang* h_X einer Kurve X ist der stabile Rang der induzierten Frobeniusabbildung auf $H^1(X, \mathcal{O}_X)$. In anderen Worten,

$$h_X = \dim_{\mathbb{F}_p} H^1(X, \mathcal{O}_X)^F.$$

Der p-Rang ist also eine ganze Zahl, und es gilt die Abschätzung

$$0 \leq h_X \leq g_X.$$

Bemerkung 1.2.2. Die Matrix von Frob^g bezüglich irgendeiner Basis von $H^1(X, \mathcal{O}_X)$ wird klassischerweise also *Hasse-Witt-Matrix* der Kurve X bezeichnet. Ihr Rang über k ist wegen Proposition 1.1.2.ii der stabile Rang des Frobenius, also der p-Rang von X.

Bemerkung 1.2.3. Ein Element $t \in k(X)$ heisst *separierend*, falls es über k transzendent ist und die Körpererweiterung $k(t) \subset k(X)$ separabel ist. Dies ist gleichbedeutend damit, dass das Differential dt nicht verschwindet.

Definition 1.2.4 (Cartier-Operator). Sei X eine Kurve, und $k(X)$ der Funktionenkörper. Sei $t \in k(X)$ eine separierende Variable. Sei ferner $\omega = f \cdot dt$ ein meromorphes Differential, mit $f \in k(X)$. Dann lässt sich f in der Form

$$f = f_0^p + f_1^p t + \cdots + f_{p-1}^p t^{p-1}$$

mit $f_i \in k(X)$ schreiben. Der Cartier-Operator $\mathcal{C}$ ist dadurch definiert, dass er auf ω via

$$\mathcal{C}(\omega) = \mathcal{C}(f \cdot dt) = f_{p-1} dt = \left(\sqrt[p]{-\left(\frac{d}{dt}\right)^{p-1} f} \right) dt$$

wirkt. Diese Definition hängt nicht von der Wahl von t ab, und ist wohldefiniert [**Ser1**].

Proposition 1.2.5. *Der duale Vektorraum von $H^1(X, \mathcal{O}_X)$ ist nach Serre-Dualität der Vektorraum $H^0(X, \Omega_X)$. Der zum Frobenius-Operator auf $H^1(X, \mathcal{O}_X)$ duale p^{-1}-lineare Operator auf $H^0(X, \Omega_X)$ ist der Cartier-Operator.*

Beweis. [**Ser1**]. $\therefore$

Es ist häufig einfacher, mit dem Cartier-Operator statt dem Frobenius-Operator zu arbeiten, da holomorphe Differentiale konkreter als Elemente von $H^1(X, \mathcal{O}_X)$ sind. Wir werden das in Kapitel 3 so handhaben.

Bemerkung 1.2.6. Ist $\pi : X \longrightarrow Y$ ein rein inseparabler, endlicher Morphismus von Kurven, so gilt $h_X = h_Y$. Dies folgt zum Beispiel aus Lemma 1.4.5 und ist der Grund, weshalb wir uns stets auf separable Überlagerungen beschränken.

1.3. Des Kaisers Kleider

Wenn das Geschlecht einer Kurve der König all ihrer globalen diskreten Invarianten ist, so wäre ihr p-Rang gewissermassen der Kaiser: Er ist ebenso natürlich definiert, aber um vieles schwieriger zu kontrollieren. Jedenfalls hat der Kaiser eine grosse Garderobe, und tritt in vielen Erscheinungen auf. Wir erwähnen hier einige, ohne aber die Beweise zu geben, die sich in [**Bos1**], Chapitre 17, und [**Mur1**] finden.

PROPOSITION 1.3.1 (Étale Cohomologie). *Der p-Rang einer Kurve ist die Dimension von $H^1(X_{et}, \mathbb{F}_p)$, der ersten étalen Cohomologiegruppe mit konstanten Koeffizienten in $\mathbb{F}_p$.*

Die algebraische Fundamentalgruppe $\pi_1(X)$ einer Kurve X tritt bei der Untersuchung ihrer unverzweigten Überlagerungen auf. Der p-Rang hat mit zyklischen Überlagerungen der Ordnung p zu tun:

PROPOSITION 1.3.2 ($\mathbb{F}_p$-Überlagerungen). *Es gilt* $\mathrm{Hom}(\pi_1(X), \mathbb{F}_p) \cong \mathbb{F}_p^{h_X}$*. Folglich entsprechen Isomorphieklassen von Überlagerungen von X mit festgehaltener Galoisgruppe $\mathbb{F}_p$ auf natürlicher Weise den Elementen von $H^1(X, \mathcal{O}_X)^{\mathrm{Frob}}$.*

Ferner:

PROPOSITION 1.3.3 (abelsche Überlagerungen). *Es bezeichne $\pi_1(X)_{ab}$ den maximalen abelschen Quotienten der Fundamentalgruppe. Dann exisitert ein Isomorphismus*

$$\pi_1(X)_{ab} \cong \left(\prod_{p \neq \ell \ prim} \mathbb{Z}_\ell^{2g_X} \right) \times \mathbb{Z}_p^{h_X}.$$

PROPOSITION 1.3.4 (p-Überlagerungen). *Auch der maximale pro-p-Quotient $\pi_1(X)_p$ der Fundamentalgruppe von X wird vom p-Rang kontrolliert: $\pi_1(X)_p$ ist eine freie pro-p-Gruppe auf h_X Erzeugenden.*

1.4. A priori Abschätzungen

Sei $\pi : X \longrightarrow Y$ separabel. Es gibt globale Schranken für den p-Rang von X in Termen des Geschlechts g_X und Geschlecht und p-Rang der Kurve Y. In diesem Abschnitt skizzieren wir kurz die Form und den Beweis dieser Schranken.

DEFINITION/LEMMA 1.4.1. Zu jeder glatten projektiven Kurve X existiert eine abelsche Varietät Jac_X mit $\mathrm{Jac}_X(k) = \mathrm{Pic}^0(X)$. Diese heisst die *Jacobische Varietät* von X.

DEFINITION 1.4.2 (p-Rang einer abelschen Varietät). Der p-Rang einer abelschen Varietät A ist die Dimension über $\mathbb{F}_p$ des Kerns der Multiplikation mit p auf A, aufgefasst als Varietät. Er wird mit $h_p(A)$ bezeichnet.

PROPOSITION 1.4.3. *Sei X eine Kurve, und Jac_X ihre Jacobische. Es gilt $g_X = \dim \mathrm{Jac}_X$, und $h_X = h_p(\mathrm{Jac}_X)$.*

BEWEIS. [**Mum1**]. ∴

PROPOSITION 1.4.4. *Seien X, Y zwei Kurven, und sei $\pi : X \longrightarrow Y$ eine Überlagerung von Grad d. Es gibt induzierte Abbildungen $\pi_* : \mathrm{Jac}_X \longrightarrow \mathrm{Jac}_Y$ und $\pi^* : \mathrm{Jac}_Y \longrightarrow \mathrm{Jac}_X$, mit $\pi_*\pi^* = d\,\mathrm{id}$. Folglich ist die Abbildung*

$$\mathrm{Jac}_Y \times \ker(\pi_*)^\circ \longrightarrow \mathrm{Jac}_X$$

surjektiv mit endlichem Kern, also eine Isogenie.

LEMMA 1.4.5 (Isogenieinvarianz des p-Rangs). *Sei $A \longrightarrow A'$ eine Isogenie von abelschen Varietäten. Dann gilt $h_p(A) = h_p(A')$.*

BEWEIS. [**Mum1**], S.147. ∴

KOROLLAR 1.4.6. *Sei $\pi : X \longrightarrow Y$ ein endlicher Morphismus von Kurven. Dann gelten die folgenden Ungleichungen:*

(i) $g_X \geq g_Y$
(ii) $h_X \geq h_Y$
(iii) $g_X - h_X \geq g_Y - h_Y$

BEWEIS. Es gilt $g_X = \dim \mathrm{Jac}_X = \dim \mathrm{Jac}_Y + \dim \ker(\pi_*) \geq \dim \mathrm{Jac}_Y$. Wegen des vorangehenden Lemmas gilt auch

$$h_X = h_p(\mathrm{Jac}_X) = h_p(\mathrm{Jac}_Y) + h_p(\ker(\pi_*)^\circ).$$

Und schliesslich zeigt die Differenz dieser beiden Gleichungen zusammen mit der Tatsache $(\dim - h_p)(\ker(\pi_*)^\circ) \geq 0$ die dritte Behauptung des Korollars. ∴

KAPITEL 2

Deuring-Schafarewitsch

Wir beweisen in diesem Kapitel eine leichte Verallgemeinerung der *Deuring-Schafarewitsch-Formel*, welche die erste Kongruenzformel liefert. Dabei werden einige grundlegende Tatsachen aus der étalen Cohomologie verwendet, fehlende Beweise finden sich in den Standardreferenzen [**Mil1**] und [**Tam1**].

2.1. Lokalkonstante Garben

PROPOSITION 2.1.1 (Monodromie-Korrespondenz). *Sei $\varpi : U \longrightarrow V$ eine étale Galois-Überlagerung zusammenhängender Schemata mit Gruppe G, ferner $\overline{y}$ ein geometrischer Punkt von Y. Dann existiert eine Äquivalenz zwischen der Kategorie der lokalkonstanten étalen Garben von $\mathbb{F}_p$-Vektorräumen auf Y, welche auf X zurückgezogen konstant werden, und der Kategorie der endlichdimensionalen Vektorräume mit $\mathbb{F}_p$-linearer G-Operation. Diese Äquivalenz ordnet einer Garbe den Halm in $\overline{y}$, zusammen mit der Monodromieoperation der Galoisgruppe zu.*

BEWEIS. [**Mil1**] Theorem 5.3 und Chapter 5, §1. $\therefore$

Betrachten wir eine Galoisüberlagerung $\pi : X \longrightarrow Y$ von Kurven. Sei $D \subset X$ ein G-invarianter, reduzierter effektiver Divisor, $i : D \longrightarrow X$ die abgeschlossene Einbettung, $U = X \setminus D$ das offene Komplement und $j : U \longrightarrow X$ dessen Einbettung. Seien ferner $\widetilde{j} : S = \pi(D) \longrightarrow Y$ und $\widetilde{i} : V = Y \setminus S \longrightarrow Y$ die analogen Einbettungen. Dann induziert π eine étale Überlagerung $\varpi : U \longrightarrow V$.

DEFINITION 2.1.2. In der obigen Situation sei M ein $\mathbb{F}_p[G]$-Modul. Wir setzen

$$F_M := (M \otimes \varpi_* \mathbb{F}_p)^G.$$

Diese Zuordnung liefert einen exakten Funktor, der bis auf Äquivalenz Inverse zum Funktor der Proposition 2.1.1 liefert.

BEWEIS. Zur Exaktheit: Jede Äquivalenz von abelschen Kategorien ist exakt. $\therefore$

2.2. Eine exakte Formel

PROPOSITION 2.2.1. *Sei $\pi : X \longrightarrow Y$ eine Galoisüberlagerung von Kurven mit Gruppe G, ferner $D \subset X$ ein G-invarianter (reduzierter) effektiver Divisor von X, welcher alle verzweigten Punkte umfasst. Es* *gelte* $\mathbb{F}_p[G] \sim n_1\mathbb{F}_p + M$, *wobei* $\mathbb{F}_p$ *die triviale* G*-Operation trage. Dann gilt*

$$h_X - 1 + |D| = n_1 \cdot (h_Y - 1 + |\pi(D)|) + \chi_c(Y \setminus \pi(D), F_M).$$

BEWEIS. Die offene bzw. abgeschlossene Einbettung

$$X \setminus D \overset{j}{\hookrightarrow} X \overset{i}{\hookleftarrow} D$$

induziert eine kurze exakte Sequenz von Garben auf X_{et}:

$$0 \longrightarrow j_!\mathbb{F}_p \longrightarrow \mathbb{F}_p \longrightarrow i_*\mathbb{F}_p \longrightarrow 0.$$

Wegen der Additivität der Eulercharakteristik in kurzen exakten Sequenzen gilt also

$$\begin{aligned} \chi_c(X \setminus D, \mathbb{F}_p) &= \chi(X, j_!\mathbb{F}_p) \\ &= \chi(X, \mathbb{F}_p) - \chi(X, i_*\mathbb{F}_p) \\ &= 1 - h_X - |D|, \end{aligned}$$

und analog folgt

$$\chi_c(Y \setminus \pi(D), \mathbb{F}_p) = 1 - h_Y - |\pi(D)|.$$

Auf dem offenen Unterschema $Y \setminus \pi(D)$ ist $\pi_*\mathbb{F}_p$ die zur natürlichen Darstellung von G auf dem Gruppenring $\mathbb{F}_p[G]$ gehörige lokal-konstante Garbe. Wegen der Exaktheit des oben eingeführten Funktors $M \mapsto F_M$ und der Additivität der Eulercharakteristik folgt also schliesslich

$$\begin{aligned} \chi_c(X \setminus D, \mathbb{F}_p) &= \chi_c(Y \setminus \pi(D), \pi_*\mathbb{F}_p) \\ &= n_1 \cdot \chi_c(Y \setminus \pi(D), \mathbb{F}_p) + \chi_c(Y \setminus \pi(D), F_M). \end{aligned}$$

$\therefore$

KOROLLAR 2.2.2 (Deuring-Schafarewitsch-Formel). *Sei* $\pi : X \longrightarrow Y$ *eine Galoisüberlagerung von Kurven, deren Gruppe* G *eine* p*-Gruppe ist. Dann gilt*

$$h_X - 1 = (h_Y - 1) \cdot |G| + \sum_{x \in X} (|G_x| - 1),$$

wobei G_x *den Stabilisator* $\{g \in G : g(x) = x\}$ *von* x *in* G *bezeichnet.*

BEWEIS. Da G eine p-Gruppe ist, gilt $\mathbb{F}_p[G] \sim |G| \cdot \mathbb{F}_p$. Die Aussage folgt also aus der vorhergehenden Proposition und einer kurzen Rechnung, welche die Gleichheit $|\pi(D)| \cdot |G| = \sum_{x \in D} |G_x|$ nachweist. $\therefore$

BEISPIEL 2.2.3. Sei $\pi : X \longrightarrow Y$ eine Galoisüberlagerung in Charakteristik 2 mit Gruppe $G = S_3$. In diesem Fall gilt $R := \mathbb{F}_2[S_3] = \mathbb{F}_2[S_2] \oplus \mathrm{Mat}_2(\mathbb{F}_2)$ als Ring, und es folgt $R \sim 2\mathbb{F}_2 + 2M$ als S_3-Modul, wo M die eindeutige irreduzible 2-dimensionale Darstellung ist. Sei $D \subset X$ der effektive Divisor der Verzweigungspunkte. Es folgt, dass die linke Seite der Gleichung der Proposition, $1 - h_X - |D|$ gerade ist, da die rechte Seite es ist.

KOROLLAR 2.2.4. *Sei X eine Kurve in Charakteristik* 2 *mit* $S_3 \subset \mathrm{Aut}(X)$. *Dann gilt*

$$h_X \textit{ gerade} \iff \#\{\textit{Fixpunkte der Operation von } S_3 \textit{ auf } X\} \textit{ ungerade.}$$

Diese Beobachtung werden wir im nächsten Abschnitt verallgemeinern.

Die Ähnlichkeit der Deuring-Schafarewitsch-Formel zur Riemann-Hurwitz-Formel und die Unterschiede zwischen den beiden sind auffällig, und gleichzeitig verwirrend. Zur späteren Verwendung halte ich die Riemann-Hurwitz-Formel hier fest.

PROPOSITION 2.2.5 (Riemann-Hurwitz-Formel). *Sei $\pi : X \longrightarrow Y$ eine separable Überlagerung von Kurven. Dann gilt*

$$2(g_X - 1) = 2(g_Y - 1)\deg \pi + \sum_{x \in X} d_X.$$

Dabei ist d_X die Bewertung der Diskrimante der zugehörigen Körpererweiterung bei x.

BEWEIS. [**Har1**], Proposition IV.2.4, zusammen mit [**Ser3**], Proposition IV.2.4. ∴

2.3. Kongruenzformel 1

Sei G eine endliche Gruppe, und sei S_G ein Repräsentantensystem der irreduziblen Darstellungen von G über k. Im folgenden bezeichnet k auch die eindimensionale triviale Darstellung von G. Wir zerlegen den Gruppenring $k[G]$ gemäss seinen Kompositionsfaktoren, sei also

$$k[G] \sim n_k \cdot k + \sum_{k \neq M \in S_G} n_M \cdot M.$$

DEFINITION 2.3.1. Wir machen für spätere Zwecke in obiger Situation die folgende Definition: Es bezeichne $N = N_G$ den grössten gemeinsamen Teiler der n_M, für $M \in S_G$. Die Zahl N' ist als grösster gemeinsamer Teiler der n_M für alle $M \in S_G$ ausser k definiert.

BEMERKUNG 2.3.2. Eine andere, äquivalente Definition von N werden wir im nächsten Kapitel antreffen (Lemma 3.3.2). Aus dieser Definition ergibt sich auch (Korollar 3.3.3), dass die grösste Potenz von p, welche die Ordnung von G teilt (der *p-Anteil* von $|G|$), auch ein Teiler von N ist. Ob der p-Anteil von $|G|$ mit N übereinstimmt, und ob $N = N'$ gilt, ist mir nicht klar.

PROPOSITION 2.3.3 (Kongruenzformel 1). *Sei $\pi : X \longrightarrow Y$ eine Galoisüberlagerung von Kurven mit Gruppe G, ferner $D \subset X$ der effektive reduzierte Divisor der verzweigten Punkte von π. Dann gelten folgende Kongruenzen:*

(i) $h_X - 1 + |D| \equiv n_k\,(h_Y - 1 + |\pi(D)|) \pmod{N'}$

(ii) $h_X - 1 + |D| \equiv 0 \pmod{N}$

Insbesondere gelten diese Kongruenzen modulo dem p-Anteil von $|G|$.

Beweis. Zunächst bemerken wir, dass für eine Erweiterung $\mathbb{F}_q|\mathbb{F}_p$ des Primkörpers in Charakteristik p folgendes gilt:

$$\dim_{\mathbb{F}_p} H^i(X, \mathbb{F}_p) = \dim_{\mathbb{F}_q} H^i(X, \mathbb{F}_q) \qquad \forall i.$$

In ähnlicher Weise können wir die Äquivalenz 2.1.1 auf $\mathbb{F}_q$-Vektorräume fortsetzen. Wir wählen nun $q = p^n$ gross genug, sodass die irreduziblen $\mathbb{F}_q[G]$-Moduln auch über $k[G]$ irreduzibel bleiben.

Der Beweis der Proposition 2.2.1 zeigt dann, dass die folgende Gleichheit gilt:

$$h_X - 1 + |D| = \sum_{M \in S_G} n_M \cdot \chi_c(Y \smallsetminus \pi(D), F_M).$$

Den Term $\chi_c(Y \smallsetminus \pi(D), F_k)$ haben wir mit $h_Y - 1 + |\pi(D)|$ identifiziert. Daraus folgen alle Behauptungen der Proposition. $\therefore$

KAPITEL 3

Galoismodulstruktur

In diesem Abschnitt wird die Struktur des halbeinfachen Anteils von $H^0(X, \Omega_X)$ bezüglich des Cartieroperators als $k[G]$-Modul untersucht, für eine beliebige endliche Untergruppe G der Automorphismengruppe einer Kurve X. Dazu beweisen wir zunächst mangels geeigneter Referenzen in der Literatur einige allgemein-psychiatrische Lemmata: Jede endlich-dimensionale Darstellung zerfällt in die direkte Summe einer Seele und eines projektiven Anteils. Wir bestimmen dann die Seele der oben genannten Darstellung – sie ist durch Fixpunktdaten der Operation von G bestimmt.

3.1. Loopspace und Seelen

Es sei im folgenden G immer eine endliche Gruppe, k ein algebraisch abgeschlossener Körper positiver Charakteristik p. Alle betrachteten Moduln seien endlich erzeugt.

Definition 3.1.1 (Projektive Hüllen). Sei M ein endlich erzeugter $k[G]$-Modul. Ein projektiver Modul P zusammen mit einer Surjektion $\pi_M : P \longrightarrow M$ heisst *projektive Hülle* von M, falls für jeden echten Untermodul P' von P die Einschränkung von π_M auf P' nicht mehr surjektiv ist.

Lemma 3.1.2. *Projektive Hüllen existieren und sind bis auf Isomorphismus eindeutig. Die projektive Hülle eines endlich erzeugten Moduls ist wieder endlich erzeugt. Ist M die endliche direkte Summe von endlich erzeugten $k[G]$-Moduln M_i, so ist die direkte Summe der projektiven Hüllen der M_i eine projektive Hülle von M.*

Beweis. [**Ser2**], Chapter 14, Proposition 41. $\therefore$

Mit $P_G(M)$ bezeichnen wir eine feste projektive Hülle von M. Falls die Gruppe G aus dem Kontext klar ist, schreiben wir auch einfach $P(M)$.

Proposition 3.1.3 (Universelle Eigenschaft der projektiven Hülle). *Die projektive Hülle hat folgende universelle Eigenschaft: Ist $P(M) \longrightarrow M$ die projektive Hülle von M, und ist $f : P \longrightarrow M$ eine weitere Surjektion eines projektiven Moduls P auf M, so existiert eine Faktorisierung*

$$P \longrightarrow P(M) \longrightarrow M$$

von f, in welcher ferner der erste Pfeil surjektiv ist.

Beweis. Dass eine Faktorisierung überhaupt existiert, folgt aus der universellen Eigenschaft des projektiven Moduls P. Das Bild von P in $P(M)$ ist ein Untermodul P'. Da das Bild von P' in M nach Voraussetzung M umfasst, folgt nach der Definition einer projektiven Hülle, dass $P' = P(M)$ ist. $\therefore$

Es ist bekannt, dass die Operation P_G eine Bijektion zwischen den Isomorphieklassen irreduzibler Moduln und den Isomorphieklassen projektiver, unzerlegbarer Moduln liefert (Proposition A.0.11). Für allgemeinere Moduln sagt die folgende Proposition, mit welchen Multiplizitäten die projektiven unzerlegbaren Moduln in der projektiven Hülle eines vorgegebenen Moduls vorkommen. Zum Voraus ein Lemma:

Lemma 3.1.4. *Ist M ein $k[G]$-Modul mit projektiver Hülle $P_G(M)$, ferner S ein irreduzibler Modul, so gilt*

$$\mathrm{Hom}_G(M, S) = \mathrm{Hom}_G(P_G(M), S).$$

Beweis. Wir wenden den Funktor $\mathrm{Hom}_G(-, S)$ auf die kurze exakte Sequenz $0 \longrightarrow \Omega(M) \xrightarrow{i} P(M) \xrightarrow{\pi_M} M \longrightarrow 0$ an und erhalten die exakte Sequenz

$$0 \longrightarrow \mathrm{Hom}_G(M, S) \longrightarrow \mathrm{Hom}_G(P(M), S) \xrightarrow{i^*} \mathrm{Hom}_G(\Omega(M), S).$$

Wir zeigen dass $i^* = 0$ ist, woraus die Behauptung dieses Lemmas folgt.

Wäre $i^* \neq 0$, so gäbe es eine Abbildung

$$0 \neq f : \Omega(M) \xrightarrow{i} P(M) \xrightarrow{F} S,$$

mit $f = i^*(F) = Fi$. Da S irreduzibel ist, müssen f und F surjektiv sein. Folglich ist die Abbildung

$$P(M) \xrightarrow{(\pi_M, F)} M \oplus S$$

immer noch surjektiv, somit auch $\ker F \xrightarrow{\pi_M} M$, was wegen $F \neq 0$, also $\ker F \subsetneq P(M)$ im Widerspruch zur Minimalität der projektiven Hülle $P(M)$ steht. $\therefore$

Proposition 3.1.5. *(Multiplizitäten der projektiven Hülle) Ist M ein $k[G]$-Modul und $P_G(M)$ seine projektive Hülle, so gilt*

$$P_G(M) \cong \bigoplus_{V \in S_G} P_G(V)^{m(V)},$$

dabei ist $m(V) := \dim_k \mathrm{Hom}_{k[G]}(M, V)$.

Beweis. Es sei $P_G(M) \cong \bigoplus_{V \in S_G} P_G(V)^{\ell(V)}$ eine Zerlegung von $P_G(M)$ in seine unzerlegbaren (projektiven) Summanden. Wir halten $S \in S_G$ fest und rechnen mit Lemma 3.1.4:

$$\begin{aligned}\operatorname{Hom}_G(M,S) &= \operatorname{Hom}_G(P(M),S)\\ &= \bigoplus_{V\in S_G} \operatorname{Hom}_G(P(V),S)^{\oplus\ell(V)}\\ &= \bigoplus_{V\in S_G} \operatorname{Hom}_G(V,S)^{\oplus\ell(V)}\end{aligned}$$

Nun ist nach dem Lemma von Schur $\operatorname{Hom}_G(V,S)=0$ für $V\neq S$, und $\operatorname{Hom}_G(S,S)=k$. Somit erhalten wir $m(S)=\dim_k \operatorname{Hom}_G(M,S) = \ell(S)\cdot\dim_k \operatorname{Hom}_G(S,S)=\ell(S)$, wie behauptet. $\therefore$

Definition 3.1.6 (Loopspace). Sei M ein endlich erzeugter $k[G]$-Modul. Wir definieren

$$\Omega_G(M) := \Omega^1_G(M) := \ker(P_G(M)\longrightarrow M)$$

und dann rekursiv $\Omega^i_G(M) := \Omega_G(\Omega^{i-1}_G(M))$ für $i>1$. Wir lassen den Index G weg, wenn klar ist, welche Gruppe gemeint ist.

Bemerkung 3.1.7. Der Name *Loopspace* für den Modul $\Omega(M)$ ist nicht zufällig gewählt. Es gibt Parallelen zwischen der stabilen Homotopietheorie und der Darstellungstheorie endlicher Gruppen. Die Anfänge dieser Theorie sind in [**KoZi1**] dargestellt. Nur soviel: Ω ist kein Funktor auf der Kategorie der endlich erzeugten $k[G]$-Moduln. Betrachtet man hingegen die *stabile Modulkategorie*, welche dieselben Objekte hat, in der jedoch zwei Morphismen identifiziert werden, falls ihre Differenz durch einen projektiven Modul faktorisiert, so wird Ω zu einem Funktor. Die stabile Modulkategorie trägt sogar die Struktur einer *triangulierten Kategorie*, in der Ω^{-1} der Translationsfunktor ist. Wir brauchen das aber nicht...

Definition 3.1.8. Sei M ein endlich erzeugter $k[G]$-Modul, und sei $M\cong\bigoplus M_i$ eine Zerlegung in unzerlegbare Moduln. Die direkte Summe der nicht-projektiven M_i heisst die *Seele* von M, die direkte Summe der projektiven M_i heisst der *projektive Anteil* von M. Da die Isomorphieklassen der M_i eindeutig bestimmt sind, ist auch die Seele und der projektive Anteil – bis auf Isomorphie – wohldefiniert. Wir bezeichnen die Seele von M mit $\operatorname{core}(M)$. Falls $M\cong\operatorname{core}(M)$ ist, nennen wir M selber eine Seele.

Lemma 3.1.9. *Die folgenden Aussagen sind äquivalent:*

(i) *M ist injektiv.*
(ii) *M ist projektiv.*
(iii) $\operatorname{core}(M)=0$.
(iv) *$\Omega_G(M)$ ist projektiv.*
(v) $\Omega_G(M)=0$.

Darüber hinaus ist $\Omega_G(M)$ stets eine Seele.

Beweis. Die Äquivalenz von (i) und (ii) gilt allgemein, da die duale Darstellung der regulären Darstellung zu dieser isomorph ist (Proposition A.0.17).

Klar ist die Äquivalenz von (ii) und (iii), nach Definition der Seele, ferner von (ii) und (v), denn $\Omega(M)$ ist Null genau dann, wenn $P(M) \longrightarrow M$ ein Isomorphismus ist, also wenn M projektiv ist.

Ein Loopspace, also ein Modul der Form $\Omega_G(M)$, kann keine nicht-trivialen projektiven Summanden enthalten, denn: Falls $0 \neq P \subset \Omega(M) \subset P(M)$ ein projektiver Untermodul ist, so zerlegt sich $P(M)$ in eine direkte Summe $P(M) \cong P \oplus Q$, da jeder projektive Modul auch injektiv ist. Der Summand P geht dann in der Projektion auf M nach 0, was im Widerspruch zur Minimalität der projektiven Hülle steht. Folglich enthält $\Omega(M)$ keine nicht-trivialen projektiven Untermoduln.

Damit ist auch die Äquivalenz von (iv) und (v), und die Behauptung dass jeder Loopspace eine Seele ist, klar und das Lemma bewiesen. $\therefore$

Proposition 3.1.10. *Sei $0 \longrightarrow N \longrightarrow P \longrightarrow M \longrightarrow 0$ eine kurze exakte Sequenz endlich erzeugter $k[G]$-Moduln, und sei P projektiv. Dann existiert ein Isomorphismus*

$$\operatorname{core}(N) \cong \Omega_G(M).$$

Beweis. Wir konstruieren zunächst das folgende kommutative Diagramm:

$$\begin{array}{ccccccccc}
0 & \longrightarrow & N & \longrightarrow & P & \longrightarrow & M & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \| & & \\
0 & \longrightarrow & \Omega(M) & \longrightarrow & P(M) & \longrightarrow & M & \longrightarrow & 0
\end{array}$$

Der mittlere senkrechte Pfeil existiert und ist surjektiv nach Lemma 3.1.3; der erste senkrechte Pfeil existiert wegen der universellen Eigenschaft des Kerns $\Omega(M)$. Sei Q der Kern des mittleren Pfeils. Da $P(M)$ projektiv ist, ist auch Q projektiv. Das Schlangenlemma zeigt nun einerseits, dass der erste senkrechte Pfeil surjektiv ist, und zweitens, dass der Kern dieses Pfeils isomorph zu Q ist. Also folgt die Isomorphie $N \cong \Omega(M) \oplus Q$. Da $\Omega(M)$ nach dem vorangehenden Lemma eine Seele ist, und Q projektiv ist, folgt schliesslich, dass $\Omega(M)$ die Seele von N ist. $\therefore$

3.2. Ermittlung der Seelen

In diesem Abschnitt betrachten wir folgende Situation: Sei G eine endliche Untergruppe der Automorphismengruppe einer Kurve X. Seien $D, \widetilde{D}, E, \ldots$ effektive, G-invariante Divisoren auf X. Aufgrund des Lemmas 3.2.2 werden wir oft annehmen, dass Divisoren reduziert sind.

Lemma 3.2.1. *Sei $D \geq 0$ ein effektiver Divisor. Der Cartieroperator operiert auf der Garbe $\Omega_X(D)$. Ist D darüber hinaus G-invariant, so* *operiert auch G auf dieser Garbe, und die Operationen von G und des Cartieroperators kommutieren. Insbesondere ist dann*

$$V_D := H^0(X, \Omega_X(D))^s,$$

der halbeinfache Anteil der globalen Schnitte bezüglich des Cartieroperators, eine Darstellung von G.

Beweis. Seien $U \subset X$ offen und $\omega \in \Omega_X(D)(U)$. Für einen Punkt $P \in U$ und einen lokalen Parameter t bei P schreiben wir

$$\omega = (f_0^p + f_1^p \cdot t + \cdots f_{p-1}^p \cdot t^{p-1})dt = f \cdot dt.$$

Es sei $n = v_P(D) \geq 0$. Nach Voraussetzung gilt $v_P(f) = v_P(\omega) \geq -n$. Da $v_P(f_i^p t^i) \equiv i \pmod p$ ist, sind $v_P(f_i^p t^i)$ und $v_P(f_j^p t^j)$ ungleich für $i \neq j$. Deshalb folgt die Abschätzung

$$p \cdot v_P(f_{p-1}) + p - 1 = v_P(f_{p-1}^p t^{p-1}) \geq v_P(f) = \min(v_P(f_i^p t^i)) \geq -n.$$

Somit gilt $v_P(\mathcal{C}(\omega)) = v_P(f_{p-1} \cdot dt) = v_P(f_{p-1}) \geq \lceil \frac{1-p-n}{p} \rceil \geq -n$, wobei $\lceil x \rceil$ die kleinste ganze Zahl grösser als x bezeichnet, und ingesamt, dass $\mathcal{C}(\omega) \in \Omega_X(D)(U)$ ist.

Anhand der Schreibweise von $\mathcal{C}$ in Termen der f_i ist es klar, dass die Operation von $\mathcal{C}$ mit der Operation von G vertauscht. Somit ist auch der halbeinfache Anteil V_D ein G-invarianter Unterraum, also eine Darstellung von G. $\therefore$

Für einen effektiven Divisor D sei D^{red} der zugehörige reduzierte Divisor mit demselben Träger.

Lemma 3.2.2. *Ist $D \geq 0$ ein effektiver Divisor, so gilt*

$$H^0(X, \Omega_X(D))^s = H^0(X, \Omega_X(D^{red})^s.$$

Anderseits gilt auch

$$H^0(X, \Omega_X(D^{red})^n = H^0(X, \Omega_X)^n.$$

Beweis. Zu zeigen ist, dass halbeinfache Differentiale höchstens einfache Polstellen haben. Es genügt wegen Lemma 1.1.2, die Aussage für Differentiale der Form $\omega = \mathcal{C}(\omega)$ zu beweisen. Es sei $v_P(\omega) = -n < 0$, dann ist wie im Beweis von Lemma 3.2.1 $v_P(\mathcal{C}(\omega)) \geq \lceil \frac{1-p-n}{p} \rceil$. Aus der elementaren Äquivalenz

$$\frac{1-p-n}{p} = -n \iff n = 1$$

folgt also schliesslich $n \geq -1$, die erste Aussage.

Zur zweiten Aussage: Es ist bekannt, dass für das Residuum an einem Punkt P die Aussage $\mathrm{Res}_P(\omega) = \mathrm{Res}_P(\mathcal{C}(\omega))^p$ gilt [**Ser1**]. Ein nilpotentes Differential kann also nur Residuum Null haben, und da es nach Voraussetzung nur Pole erster Ordnung hat, ist es sogar regulär. $\therefore$

Im folgenden nehmen wir immer an, dass Divisoren effektiv und G-invariant ist, je nach Bedarf auch, dass sie reduziert sind. Es geht uns darum, die Seelen der Darstellungen V_D zu bestimmen.

Definition 3.2.3 (Hinreichend gross). Ein Divisor $\widetilde{D}$ heisst *hinreichend gross bezüglich* G, falls er G-invariant, reduziert, effektiv und nicht-leer ist, und ferner alle verzweigten Punkte der Operation von G enthält.

Proposition 3.2.4. *Ist $\widetilde{D}$ ein hinreichend grosser Divisor bezüglich G, so ist die Darstellung $V_{\widetilde{D}} = H^0(X, \Omega_X(\widetilde{D}))^s$ projektiv über $k[G]$.*

Beweis. Sei $P \subset G$ eine p-Sylowuntergruppe von G. Nach Nakajima ([**Nak1**], Theorem 1) wissen wir, dass der Modul $V_{\widetilde{D}}$ frei ist über $k[P]$. Aber das ist äquivalent dazu, dass er $k[G]$-projektiv ist. (Jeder Modul ist *relativ projektiv* bezüglich P, [**Ben1**], Corollary 3.6.10 oder Anhang A dieser Arbeit). $\therefore$

Bemerkung 3.2.5. Es lässt sich zeigen, dass $H^0(X, \Omega_X(D))$, also nicht bloss der halbeinfache Anteil $H^0(X, \Omega_X(D))^s$, dann und nur dann projektiv ist, wenn die Überlagerung $X \longrightarrow X/G$ zahm verzweigt ist [**Kan1**].

Definition 3.2.6 (Verzweigungsmodul). Sei $D \geq 0$ ein G-invarianter Divisor, und sei $\pi_G : X \longrightarrow Z = X/G$ die G-Galoisüberlagerung. Wir wählen einen genügend grossen Divisor $\widetilde{D} \supset D$, und für $z_i \in \pi_G(\widetilde{D})$ ein Urbild $x_i \in X$. Sei G_i der Stabilisator von x_i in G. Wir definieren

$$M_{G,\widetilde{D}} := \bigoplus k[G/G_i].$$

Falls $D \neq \varnothing$ ist, so definieren wir den *Verzweigungsmodul von V_D* (bezüglich $\widetilde{D}$) als

$$R_{G,D,\widetilde{D}} := M_{G,\widetilde{D}}.$$

Ist anderseits $D = \varnothing$, so definieren wir Augmentations-Abbildungen

$$\delta_i : k[G/G_i] \longrightarrow k, \quad \sum \lambda_\sigma \sigma \mapsto \sum \lambda_\sigma$$

und eine Abbildung

$$\delta = \Sigma \delta_i : M_{G,\widetilde{D}} = \bigoplus k[G/G_i] \longrightarrow k.$$

In diesem Fall sei der *Verzweigungsmodul von $V_\varnothing = H^0(X, \Omega_X)^s$* der Modul

$$R_{G,\varnothing,\widetilde{D}} := \ker \delta.$$

Bemerkung 3.2.7. Wir unterdrücken häufig die Wahl von $\widetilde{D}$ in der Notation der Verzweigungsmoduln $R_{G,D,\widetilde{D}}$ und schreiben bloss $R_{G,D}$, wenn wir nur an $\Omega^1(R_{G,D})$ interessiert sind. Dieser Modul hängt nicht mehr von der Wahl von $\widetilde{D}$ ab, denn wenn sich $\widetilde{D}$ vergrössert, so ändert sich $R_{G,\widetilde{D}}$ um direkte Summanden welche isomorph zu $k[G]$, also insbesondere projektiv sind. Insbesondere schreiben wir oft R_G für $R_{G,\varnothing,\widetilde{D}}$.

THEOREM 3.2.8. *Sei $\pi_G : X \longrightarrow Z = X/G$ die zu G gehörige Galois-Überlagerung, ferner D ein effektiver Divisor von X. Dann existiert ein projektiver $k[G]$-Modul P und ein Isomorphismus*

$$H^0(X, \Omega_X(D))^s \cong \Omega^1_G(R_{G,D}) \oplus P.$$

BEWEIS. Nach Lemma 3.2.2 dürfen wir annehmen, dass D reduziert ist. Sei $\widetilde{D} \supset D$ hinreichend gross. Dann ist auch $\widetilde{D} \smallsetminus D$ reduziert und G-invariant, und die Sequenz

$$0 \longrightarrow \mathcal{O}_X(-(\widetilde{D} \smallsetminus D)) \longrightarrow \mathcal{O}_X \xrightarrow{\text{Res}} \mathcal{O}_{\widetilde{D} \smallsetminus D} \longrightarrow 0$$

exakt. Sie geht durch Tensorieren mit $\Omega_X(\widetilde{D})$ in die exakte Sequenz

$$0 \longrightarrow \Omega_X(D) \longrightarrow \Omega_X(\widetilde{D}) \xrightarrow{\text{Res}} \mathcal{O}_{\widetilde{D} \smallsetminus D} \longrightarrow 0$$

über, welche schliesslich mit Lemma 3.2.4 die folgende lange exakte Cohomologiesequenz induziert:

$$\begin{aligned} 0 \quad &\longrightarrow \quad H^0(X, \Omega_X(D)) \longrightarrow H^0(X, \Omega_X(\widetilde{D})) \longrightarrow H^0(X, \mathcal{O}_{\widetilde{D} \smallsetminus D}) \\ &\xrightarrow{\ \delta\ } \quad H^1(X, \Omega_X(D)) \longrightarrow 0. \end{aligned}$$

Wir benutzen den Isomorphismus

$$M_{G,\widetilde{D}} \cong H^0(X, \mathcal{O}_{\widetilde{D} \smallsetminus D}),$$

die Tatsachen $H^1(X, \Omega_X(D)) = 0$ für $D \neq \varnothing$ und $H^1(X, \Omega_X) = k$, und bemerken, dass dann das δ aus der obigen exakten Sequenz in das δ von Definition 3.2.6 übergeht. In jedem Fall existiert also ein Isomorphismus $R_{G,D} \cong \ker \delta$. Nach dem zweiten Teil von Lemma 3.2.2 ist die Inklusion $H^0(X, \Omega_X(D) \subset H^0(X, \Omega_X(\widetilde{D}))$ auf den nilpotenten Anteilen ein Isomorphismus, die lange exakte Sequenz von oben liefert also eine kurze exakte Sequenz

$$0 \longrightarrow V_D \longrightarrow V_{\widetilde{D}} \longrightarrow R_{G,D,\widetilde{D}} \longrightarrow 0.$$

Und damit haben wir die Seele von V_D ermitteln können, denn nach Lemma 3.1.10 gilt nun

$$\operatorname{core}(V_D) \cong \Omega(R_{G,D}).$$

$\therefore$

KOROLLAR 3.2.9. *Der Modul $H^0(X, \Omega_X(D))^s$ ist projektiv als $k[G]$-Modul dann und nur dann, wenn $R_{G,D}$ projektiv ist.*

BEWEIS. Nach Lemma 3.1.9 ist der Modul V_D projektiv genau dann, wenn seine Seele trivial ist. Diese Seele ist nach Theorem 3.2.8 gleich $\Omega^1_G(R_{G,D})$. Mit demselben Lemma folgt die Aussage. $\therefore$

BEMERKUNG 3.2.10 (Unverzweigter Fall). Der Fall, in welchem G fixpunktfrei operiert, und $D = \varnothing$ gewählt wird, hat Borne [**Bor1**] behandelt und seine Darstellung hat dieses Kapitel überhaupt erst inspiriert. In diesem Fall ist $M_{G,\varnothing} = k[G]^n$ für ein $n \geq 1$, und $\Omega^1_G(R_G) =$

$\Omega^2_G(k)$. Man erhält also mit derselben Methode wie in der Proposition einen Isomorphismus

$$H^0(X, \Omega_X)^s \cong \Omega^2_G(k) \oplus P$$

für einen projektiven Modul P.

KOROLLAR 3.2.11. *Sind die Stabilisatoren der Operation von G auf X bekannt, so legt der modulare Charakter von V_D diesen Modul bis auf Isomorphie fest.*

BEWEIS. Wir schreiben $V_D \cong \Omega^1 R_{G,D} \oplus P$ mit P projektiv. Durch Kenntnis der Stabilisatoren der Operation lässt sich der modulare Charakter von $R_{G,D}$ bestimmen, somit ist der modulare Charakter von P unter den gemachten Voraussetzungen bekannt. Aber ein projektiver Modul ist durch seinen modularen Charakter bis auf Isomorphie festgelegt ([**Ser1**], Chapter 14, Theorem 35, Corollary 2), und deshalb folgt das Korollar. $\therefore$

3.3. Kongruenzformel 2

Wir betrachten in diesem Abschnitt dieselbe Situation wie im letzten, eine endliche Gruppe G operiere also auf einer Kurve X. Nachdem wir im letzten Abschnitt die Seele der Darstellungen V_D bestimmt haben, geht es nun darum, den projektiven Anteil von V_D zu untersuchen.

DEFINITION 3.3.1 (Borne-Invarianten). Die *Borne-Invarianten für $U \in S_G$ (bezüglich G und D)* werden mit $b(G, D, U)$ bezeichnet und sind dadurch definiert, dass ein Isomorphismus

$$H^0(X, \Omega_X(D))^s \cong \Omega_G(R_{G,D}) \oplus \bigoplus_{U \in S_G} P_G(U)^{\oplus b(G,D,U)}$$

existieren soll. Wegen des Satzes von Krull-Schmidt und Theorem 3.2.8 sind die Borne-Invarianten wohldefiniert. Ist $D = \varnothing$, so kürzen wir $b(G, \varnothing, U)$ mit $b(G, U)$ ab.

LEMMA 3.3.2. *Der grösste gemeinsame Teiler der Dimensionen der projektiven Hüllen $P_G(U)$ der Moduln $U \in S_G$ stimmt mit der Grösse N aus Definition 2.3.1 überein.*

BEWEIS. Es ist bekannt, dass $k[G]$ isomorph zu $\bigoplus_{U \in S_G} P_G(U)^{\oplus \dim U}$ ist (Proposition A.0.12). Die Cartan-Matrix C ([**Ser1**], Chapter 15), welche die Kompositionsfaktoren der projektiven Hüllen der irreduziblen Darstellungen in Termen der irreduziblen Darstellungen ausdrückt, ist symmetrisch ([**Ser1**], 15.4). Die Multiplizität μ_U von $U \in S_G$ als Kompositionsfaktor der regulären Darstellung $k[G]$ ist das gewichtete Mittel der U-ten Spalte, gewichtet mit den Dimensionen der irreduziblen Darstellungen. Die Dimension ν_U von $P(U)$ für $U \in S_G$ ist das gewichtete Mittel der U-ten Zeile, gewichtet mit denselben Gewichten. Aus der Symmetrie von C folgt also $\mu_U = \nu_U$ für alle U, und somit ist insbesondere der grösste gemeinsame Teiler der μ_U (nach Definition ist das N) derselbe wie der grösste gemeinsame Teiler der ν_U, um die es in diesem Lemma geht. $\therefore$

KOROLLAR 3.3.3. *Sei p^n der p-Anteil der Gruppenordnung, also $|G| = p^n k$ mit $k \in \mathbb{N}$ und $p \nmid k$. Dann gilt $p^n \mid N$.*

BEWEIS. Das ist Exercise 16.3 in [**Ser2**], und hier ist die Lösung: Ist M ein projektiver $k[G]$-Modul, und $P \subset G$ eine p-Sylowuntergruppe, so wissen wir bereits, dass M ein projektiver, und folglich freier $k[P]$-Modul ist. Folglich gilt $p^n = \dim_k k[P] \mid \dim_k M$, und somit teilt p^n auch N. $\therefore$

PROPOSITION 3.3.4 (Kongruenzformel 2). *Sei $\pi : X \longrightarrow Y$ eine Galoisüberlagerung von Kurven mit Gruppe G. Dann gilt die folgende Kongruenz:*

$$h_X \equiv \dim \Omega^1 R_G \pmod{N}.$$

Im Spezialfall, dass G fixpunktfrei operiert, gilt auch

$$h_X \equiv \dim \Omega^2 k \pmod{N}$$

.

BEWEIS. Die Aussagen folgen unmittelbar aus Proposition 3.2.8 bzw. Bemerkung 3.2.10, zusammen mit der Definition von N und dem vorangehenden Lemma. $\therefore$

BEMERKUNG 3.3.5. Nimmt man die Kongruenzformeln aus diesem und dem vorangehenden Kapital zusammen, so ergibt sich *keine* Restriktion für die Existenz von G-Operationen auf Kurven mit vorgegebenem Fixpunktverhalten. Die beiden Formeln sind vielmehr äquivalent.

BEISPIEL 3.3.6 (Fusion). Sei G eine endliche Gruppe, welche auf einer Kurve X operiert, und $|D|$ die Anzahl Fixpunkte dieser Operation. Dann gilt

$$\dim \Omega^1 R_G + |D| \equiv 1 \pmod{N}.$$

BEWEIS. Folgt aus dem Vergleich der Kongruenzformel 1 und 2. $\therefore$

Dieses Beispiel ist aber auch unabhängig von den Kongruenzformeln einzusehen, und zeigt damit die Äquivalenz von der Kongruenzformel 1 (Proposition 2.3.3.ii) und Kongruenzformel 2 (Proposition 3.3.4): Für die minimale Wahl von $\widetilde{D}$ gilt $|\widetilde{D}| = \dim M_{G,\varnothing}$, für eine grössere Wahl von $\widetilde{D}$ gilt eine Kongruenz modulo N. Ferner ist $\dim \Omega(M_G) + \dim M_G \equiv 0 \pmod{N}$ für jeden $k[G]$-Modul, und somit folgt die Aussage des vorangehenden Beispiels.

KAPITEL 4

Relative Erweiterungen

Wir behalten die Situation und die Notationen des vorangehenden Kapitels bei, betrachten aber zusätzlich einen Normalteiler N von G und die kurze exakte Sequenz

$$1 \longrightarrow N \longrightarrow G \longrightarrow H := G/N \longrightarrow 1.$$

Eine Darstellung von H liefert durch Zurückziehen eine Darstellung von G, und wir erhalten die Inklusion $S_H \subset S_G$ der irreduziblen Darstellungen.

Seien $Y := X/N$ und $Z := X/G = Y/H$ die zwei Quotientenkurven von X nach N respektive G. Es bezeichne $\pi : X \longrightarrow Y$ die kanonische Projektion. Unser Ziel ist es, den Zusammenhang zwischen den Borne-Invarianten von X und denjenigen von Y zu herzuleiten. Das gelingt für die Borne-Invarianten $b(G, V)$ für $V \in S_H$. Der Spezialfall $N = G$ legt insbesondere die Borne-Invariante $b(G, k)$ fest und liefert eine untere Abschätzung für den p-Rang von X in Termen des p-Ranges von X/G und lokaler Verzweigungsdaten.

4.1. Invariante Differentiale

Proposition 4.1.1. *Sei $D \subset X$ ein N-invarianter effektiver Divisor. Dann ist die Garbe $\pi_*\Omega_X(D)^N$ der N-invarianten Differentiale von der Form $\Omega_Y(E)$ für einen effektiven Divisor E auf $Y = X/N$. Dabei gilt*

$$E^{red} = \pi(D)^{red} \cup \{y \in Y \mid \pi \textit{ ist über } y \textit{ wild verzweigt}\}.$$

Darüber hinaus entspricht der vom Cartier-Operator auf X induzierte Cartier-Operator auf $\pi_*\Omega_X(D)^N$ dem Cartier-Operator auf $\Omega_Y(E)$.

Beweis. Die Garbe $\pi_*\Omega_X(D)^N$ ist auf jeden Fall eine invertierbare Garbe, und somit von der Form $\Omega_X(E)$ für einen Divisor E auf Y, den wir im folgenden bestimmen werden. Sei $Q \in X$, dann gilt

$$\begin{aligned} \pi_*\Omega_X(D)^N \otimes_{\mathcal{O}_{Y,Q}} \widehat{\mathcal{O}_{Y,Q}} &= \left(\bigoplus_{P \in \pi^{-1}(Q)} \Omega_X(D) \otimes_{\mathcal{O}_{X,P}} \widehat{\mathcal{O}_{X,P}} \right)^N \\ &= \left(\Omega_X(D) \otimes_{\mathcal{O}_{X,P}} \widehat{\mathcal{O}_{X,P}} \right)^{N_P}. \end{aligned}$$

Sei also $P \in \pi^{-1}(Q)$, ferner x ein lokaler Parameter bei P und y ein lokaler Parameter bei Q. Es gilt $\widehat{\mathcal{O}_{X,P}} = k[[x]] =: R$ und $\widehat{\mathcal{O}_{Y,Q}} = k[[y]] = R^{N_P}$. Für y ergibt sich mit $n = |N_P|$ ein Ausdruck

$$y = x^n + \text{ höhere Terme in } x.$$

Der Differentialkalkül liefert

$$\frac{dy}{dx} = \begin{cases} n \cdot x^{n-1} + \text{ höhere}, & \text{falls } p \nmid n \\ * \cdot x^m + \text{ höhere}, & m \geq n, \text{ falls } p \mid n \end{cases}$$

wobei $v_P(*) = 0$ ist, also

$$m = v_P(\frac{dy}{dx}) = \begin{cases} n-1 & p \nmid n \\ \geq n & p \mid n \end{cases}$$

Nun sei

$$\Omega_P := \widehat{\Omega_{X,P}} = R \cdot dx = \frac{R}{\frac{dy}{dx}} \cdot dy$$

die Lokalisierung der Garbe der holomorphen Differentiale bei P, dann gilt mit $d = v_P(D)$ folglich

$$(\frac{1}{x^d}\Omega_P)^{N_P} = (\frac{1}{x^{d+m}}R)^{N_P} dy.$$

Wir schreiben $d + m = an + b$ mit $a, b \geq 0$ und $b \leq n - 1$. Es gilt

$$a \geq 1 \iff d + m \geq n \iff d \geq 1 \text{ oder } p \mid n.$$

Also folgt die Gleichheit

$$(\frac{1}{x^d}\Omega_P)^{N_P} = (\frac{1}{y^a x^b}R)^{N_P} dy = \frac{1}{y^a}(R^{N_P})dy,$$

was gleichbedeutend ist mit

$$\left(\pi_*\Omega_X(D) \otimes_{\mathcal{O}_{Y,Q}} \widehat{\mathcal{O}_{Y,Q}}\right)^N = \Omega_Y(E) \otimes_{\mathcal{O}_{Y,Q}} \widehat{\mathcal{O}_{Y,Q}}$$

falls wir nur $v_Q(E) = a$ setzen, wie behauptet.

Die Identifikation der Cartieroperatoren auf $\pi_*\Omega_X(D)^N$ und $\Omega_Y(E)$ unter dem Isomorphismus von Garben, welchen wir soeben konstruiert haben, ist klar, da sie auf beiden durch dieselben Formeln gegeben sind. $\therefore$

Definition 4.1.2 (Lokal-triviale Cohomologieklassen). Sei X eine Kurve, und $G \subset \mathrm{Aut}_k(X)$ eine endliche Gruppe von Automorphismen. Sei $V \in S_G$ eine irreduzible Darstellung von G, und bezeichne G_x für $x \in X$ den Stabilisator von x in G. Es sei $r_{G,G_x,V} : H^1(G, V) \longrightarrow H^1(G_x, V)$ die natürliche Restriktionsabbildung; wir definieren die globale Restriktionsabbildung

$$r_{G,X,V} : H^1(G, V) \longrightarrow \bigoplus_{x \in X} H^1(G_x, V)$$

als Summe der Restriktionsabbildungen $r_{G,G_x,V}$. Die *lokal-trivialen ersten Cohomologieklassen* von V bezüglich G und X bilden den Kern

$$H^1_{LT,X}(G,V) := \ker r_{G,X,V},$$

und wir definieren

$$d(G,X,V) := \dim_k H^1_{LT,X}(G,V).$$

THEOREM 4.1.3. *Seien*

$$H^0(X,\Omega_X)^s \cong \Omega_G R_G \oplus \bigoplus_{U\in S_G} P_G(U)^{b(G,U)}$$

und

$$H^0(Y,\Omega_Y)^s \cong \Omega_H R_H \oplus \bigoplus_{V\in S_H} P_H(V)^{b(H,V)}$$

die Zerlegungen in unzerlegbare Summanden. Sei $V \in S_H \subset S_G$. Dann gilt für die Borne-Invarianten die Gleichung

$$b(G,V) + d(G,X,V) = b(H,V) + d(H,Y,V).$$

BEWEIS. Sei $\widetilde{D}$ ein genügend grosser Divisor auf X. Mit Proposition 4.1.1 wissen wir, dass für $\widetilde{E} := \pi(\widetilde{D})$ ein Isomorphismus

$$\begin{aligned}\bigoplus_{V\in S_H} P_H(V)^{b(H,\widetilde{E},V)} \cong& H^0(Y,\Omega_Y(\widetilde{E}))^s \\ \cong& (H^0(X,\Omega_X(\widetilde{D}))^s)^N \cong \bigoplus_{U\in S_G} (P_G(V)^N)^{b(G,\widetilde{D},V)}\end{aligned}$$

existiert. Es ist bekannt ([**Bor1**], Lemma 2.7), dass $P_G(V)^N = P_H(V)$ für $V \in S_H$, hingegen $P_G(U)^N = 0$ für $U \in S_G \setminus S_H$ ist. Aus dem obigen Isomorphismus schliessen wir also, dass $b(G,\widetilde{D},V) = b(H,\widetilde{E},V)$ gilt, und dies wollen wir ausnützen.

Wir betrachten dazu die kurze exakte Sequenz

$$0 \longrightarrow H^0(X,\Omega_X)^s \longrightarrow H^0(X,\Omega_X(\widetilde{D}))^s \longrightarrow R_{G,\varnothing,\widetilde{D}} \longrightarrow 0.$$

Ähnlich wie im Beweis der Proposition 3.1.10 schliessen wir daraus mit dem Schlangenlemma auf einen Isomorphismus

$$\bigoplus_{U\in S_G} P_G(U)^{b(G,\widetilde{D},U)} \cong P_G(R_G) \oplus \bigoplus_{U\in S_G} P_G(U)^{b(G,U)},$$

und somit ist, für $U \in S_G$,

$$\begin{aligned} b(G,\widetilde{D},U) - b(G,U) &= \dim \operatorname{Hom}_G(P_G(R_{G,\varnothing,\widetilde{D}}),U) \\ &= \dim \operatorname{Hom}_G(R_{G,\varnothing,\widetilde{D}},U). \end{aligned}$$

Auf dieselbe Weise folgt auch, dass

$$b(H,\widetilde{E},V) - b(H,V) = \dim \operatorname{Hom}_H(R_{H,\varnothing,\widetilde{E}},V)$$

ist für $V \in S_H$. Somit erhalten wir

$$b(G,V) - b(H,V) = \dim \mathrm{Hom}_H(R_{H,\varnothing,\widetilde{E}}, V) - \dim \mathrm{Hom}_G(R_{G,\varnothing,\widetilde{D}}, V).$$

Um diese Differenz zu berechnen, untersuchen wir die folgende kurze exakte Sequenz von $k[G]$-Moduln

$$0 \longrightarrow R_{G,\varnothing,\widetilde{D}} \longrightarrow \bigoplus_{x\in\widetilde{D} \bmod G} k[G/G_x] \longrightarrow k \longrightarrow 0.$$

Sie induziert in der Gruppencohomologie durch Anwenden von $\mathrm{Hom}_G(-,V)$ die lange exakte Sequenz

$$\begin{aligned} 0 \quad \longrightarrow \quad & V^G \longrightarrow \bigoplus_{x\in\widetilde{D} \bmod G} V^{G_x} \longrightarrow \mathrm{Hom}_G(R_{G,\varnothing,\widetilde{D}}, V) \\ \longrightarrow \quad & H^1(G,V) \longrightarrow \bigoplus H^1(G_x,V). \end{aligned}$$

Dabei identifiziert sich die letzte Abbildung mit der Abbildung $r_{G,X,V}$ aus Definition 4.1.2.

Mit derselben Methode erhalten wir eine exakte Sequenz

$$0 \longrightarrow V^H \longrightarrow \bigoplus_{y\in\widetilde{E} \bmod H} V^{H_y} \longrightarrow \mathrm{Hom}_H(R_{H,\varnothing,\widetilde{E}}, V) \longrightarrow H^1_{LT,Y}(H,V) \longrightarrow 0.$$

Nun folgt mit der Gleichung $\dim V^G = \dim V^H$ und, für $y = \pi(x)$, der Gleichung $\dim V^{G_x} = \dim V^{H_y}$, die Aussage, denn

$$\begin{aligned} b(G,V) - b(H,V) &= \dim \mathrm{Hom}_H(R_{H,\varnothing,\widetilde{E}}, V) - \dim \mathrm{Hom}_G(R_{G,\varnothing,\widetilde{D}}, V) \\ &= (d(H,Y,V) + \sum \dim V^{H_y} - \dim V^H) \\ &\quad -(d(G,X,V) + \sum \dim V^{G_x} - \dim V^G) \\ &= d(H,Y,V) - d(G,X,V), \end{aligned}$$

wie in diesem Theorem behauptet wird. $\therefore$

Bemerkung 4.1.4. Falls der Normalteiler N eine p-Gruppe ist, so ist bekannt, dass $S_G = S_H$ gilt ([**Bor1**], Bemerkung nach Definition 2.5). Deshalb bestimmen in diesem Fall die Borne-Invarianten von Y *alle* Borne-Invarianten von X. In diesem Sinne ist Theorem 4.1.3 eine Verallgemeinerung von Nakajimas äquivarianter Deuring-Schafarewitsch-Formel [**Nak2**], welche als Spezialfall $N = G$ eine p-Gruppe, und $H = 1$ hervortritt. Insbesondere gilt im vorangehenden Korollar eine Gleichheit, und nicht bloss eine Kongruenz.

Beispiel 4.1.5. Sei $V = \{(12)(34), (13)(24), (14)(23)\} \subset S_4$ die Kleinsche Vierergruppe. Dann liefert die exakte Sequenz

$$1 \longrightarrow V \longrightarrow S_4 \longrightarrow S_3 \longrightarrow 1$$

in Charakteristik 2 ein Beispiel zur vorangehenden Bemerkung, welches wir in Beispiel 5.2.1 noch näher betrachten werden.

KOROLLAR 4.1.6. *Operiert G zahm auf X, so gilt für die Borne-Invarianten die Gleichung*

$$b(G,V) + \dim_k H^1(G,V) = b(H,V) + \dim_k H^1(H,V).$$

BEWEIS. Ist die Operation zahm, so teilt die Charakteristik von k die Ordnungen der Stabilisatoren G_x und H_y nicht. In diesem Fall sind deren Darstellung allesamt projektiv, und $H^1(K,V)$ ist gleich 0 für eine projektive Darstellung einer Gruppe K. Somit ist $H^1_{LT,X}(G,V) = H^1(G,V)$ und $H^1_{LT,Y}(H,V) = H^1(H,V)$, und die Aussage folgt. $\therefore$

BEMERKUNG 4.1.7. Dieses Korollar beweist die Vermutung, welche Borne in seinem Artikel [**Bor1**], nach Proposition 2.4, ausspricht.

Unter gewissen Umständen, welche das folgende Lemma aufführt, kann auf die Berechung der lokal-trivialen Cohomologiegruppen verzichtet werden:

LEMMA 4.1.8. *Es ist $H^1_{LT,Y}(H,V) = H^1_{LT,X}(G,V) \cap H^1(H,V)$, deshalb gilt stets die Abschätzung*

$$b(G,V) \le b(H,V).$$

Ferner:

(i) *Ist $p \nmid [G : G_x]$ für ein $x \in X$, so ist $H^1_{LT,X}(G,V) = H^1_{LT,Y}(H,V) = 0$.*
(ii) *Ist $p \nmid [N : N_x]$ für ein $x \in X$, so ist $H^1_{LT,X}(G,V) = H^1_{LT,Y}(H,V)$.*

In beiden Fällen gilt für alle $V \in S_H$ die Gleichheit

$$b(G,V) = b(H,V).$$

BEWEIS. Für $x \in X$ und $y = \pi(x) \in Y$ ist die Sequenz

$$1 \longrightarrow N_x \longrightarrow G_x \longrightarrow H_y \longrightarrow 1$$

exakt. Wir halten $V \in S_H$ fest und benutzen im folgenden die Notationen $LT_G := H^1_{LT,X}(G,V)$ und $LT_H := H^1_{LT,Y}(H,V)$. Die Inflations-Restriktions-Sequenz in der Gruppencohomologie zeigt für $V \in S_H$ dass die Sequenz

$$0 \longrightarrow H^1(H,V) \longrightarrow H^1(G,V) \longrightarrow H^1(N,V)^H$$

exakt ist. Daraus konstruieren wir folgendes kommutatives Diagramm:

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] \\
0 \arrow[r] & LT_H \arrow[r] \arrow[d, "i"'] & H^1(H,V) \arrow[r, "a"] \arrow[d] & \bigoplus_y H^1(H_y,V) \arrow[d] \\
0 \arrow[r] & LT_G \arrow[r] \arrow[d] & H^1(G,V) \arrow[r, "b"] \arrow[d] & \bigoplus_x H^1(G_x,V) \arrow[d] \\
 & \operatorname{Coker} i \arrow[r, "j"] \arrow[d] & H^1(N,V)^H \arrow[r, "c"] & \bigoplus_x H^1(N_x,V)^{H_y} \\
 & 0 & &
\end{tikzcd}$$

Die zwei rechten Spalten sind wegen der Inflations-Restriktions-Sequenz exakt. Die zwei oberen Zeilen sind exakt nach Definition der lokaltrivialen Cohomologieklassen. Die erste Spalte ist exakt wegen des Schlangenlemmas und nach Definition des Cokerns.

Sei $d : H^1(G,V)/H^1(H,V) \longrightarrow \bigoplus_x H^1(G_x,V)/H^1(H_y,V)$. Wir definieren j als Verkettung $j : \operatorname{Coker} i \longrightarrow \ker d \longrightarrow \ker c$. Somit ist j als Verkettung von injektiven eine injektive Abbildung, stimmt aber nicht notwendig mit $\ker c$ überein. Es gilt aber immer $\operatorname{Coker} i \subset \ker c$.

Die Kommutativität des gesamten Diagramms ist klar.

Nun zeigt eine Diagrammjagd, dass $LT_H = LT_G \cap H^1(H,V)$ ist, und somit folgt zunächst die Abschätzung $d(H,Y,V) \leq d(G,X,V)$ und daraus $b(G,V) = b(H,V) + d(H,Y,V) - d(G,X,V) \leq b(H,V)$.

Falls $p \nmid [G : G_x]$ gilt für ein x, so umfasst G_x eine p-Sylowgruppe von G, und die Restriktion $\operatorname{Res} : H^1(G,V) \longrightarrow H^1(G_x,V)$ ist injektiv, denn: Die Abbildung

$$\begin{aligned}
\operatorname{tr} : H^0(G_x,V) &\longrightarrow H^0(G,V) \\
v &\longmapsto \frac{1}{[G : G_x]} \sum_{g \in G/G_x} gv
\end{aligned}$$

ist eine Rechtsinverse zu $\operatorname{Res} : H^0(G,V) \longrightarrow H^0(G_x,V)$. Wegen der Universalität des Deltafunktors der Gruppencohomologie erhalten wir auch eine induzierte rechtsinverse Abbildung tr im Grad 1 der Cohomologie. Somit ist auch b injektiv, und $LT_G = \ker b = 0$. Schliesslich ist $LT_H \subset LT_G = 0$, also insgesamt $LT_H = LT_G = 0$.

Falls anderseits $p \nmid [N : N_x]$ gilt für ein x, so ist die Abibldung $H^1(N,V) \longrightarrow H^1(N_x,V)$ injektiv, und somit auch c. Da $\operatorname{Coker} i \subset \ker c = 0$ gilt, folgt also, dass $LT_G = LT_H$ ist. $\therefore$

KOROLLAR 4.1.9 (Untere Abschätzung). *Für den p-Rang von X ergibt sich folgende Abschätzung:*

$$h_X \geq \dim_k \Omega^1_G R_G + n_k \left(h_Y - d(G, X, k) + d(H, Y, k)\right).$$

Darüber hinaus ist die Differenz dieser Terme kongruent zu Null modulo N'.

BEWEIS. Wir betrachten den Spezialfall $N = G$ und $H = 1$ von Theorem 4.1.3. Es ist

$$h_X = \dim \Omega R_G + b(G, k) \dim P(k) + \sum_{k \neq V \in S_G} b(G, V) \dim P(V).$$

Nun ist $b(H, k) = h_Y$, ferner $b(G, k) = b(H, k) + d(H, Y, k) - d(G, X, k)$, und wie im Beweis von Lemma 3.3.2 folgt einerseits, dass $n_k = \dim P_G(k)$ ist, und anderseits dass N' mit dem grössten gemeinsamen Teiler der Dimensionen der projektiven Hüllen aller irreduzibler Darstellungen S_G ausser k übereinstimmt. Somit folgt das Korollar. $\therefore$

KAPITEL 5

Beispiele

5.1. S_3

Sei k ein algebraisch abgeschlossener Körper der Charakteristik 2. Wir werden eine Galoisüberlagerung des $\mathbb{P}^1$ mit Gruppe S_3 konstruieren, welche über $\mathbb{A}^1 \subset \mathbb{P}^1$ unverzweigt, über $\infty \in \mathbb{P}^1$ hingegen wild verzweigt ist.

LEMMA 5.1.1. *Sei $f \in k[x]$ ein Polynom von ungeradem Grad $n = 2g+1$. Das Polynom*

$$F(x,y) = y^2 + y + f(x)$$

ist separabel und irreduzibel über $k(x)$. Die assoziierte glatte projektive Kurve Y_f hat Geschlecht $g_X = g$ und p-Rang $h_X = 0$. Die Überlagerung $\pi = x : Y_f \longrightarrow \mathbb{P}^1$ ist eine Galoiserweiterung der Ordnung 2, und ausserhalb von $\infty \in \mathbb{P}^1$ unverzweigt.

BEWEIS. Das Polynom F ist separabel, da $\frac{d}{dy}F = 1$ ist. Wäre F reduzibel, also von der Form $F = (y-a)(y-b) = y^2 + (a+b)y + ab$ für $a, b \in k(x)$, so wäre durch Koeffizientenvergleich $b = a+1$, und also $f = ab = a^2 + a$ von der Form $a^2 + a$, hätte also insbesondere geraden Grad. Aber f hat ungeraden Grad, deshalb ist F irreduzibel.

Die Abbildung $(x,y) \mapsto (x, y+1)$ liefert den Galoisautomorphismus von $k(x,y)$ über $k(x)$.

Wir betrachten die Projektion $\pi : Y_f \longrightarrow \mathbb{P}^1$, gegeben durch die Funktion x. Ausserhalb von $\infty \in \mathbb{P}^1$ ist π unverzweigt, denn für festes $x_0 \in k$ hat die Gleichung $y^2 + y = f(x_0)$ zwei verschiedene Lösungen, da eine Lösung y_0 eine neue Lösung $y_0 + 1$ zur Folge hat. Über ∞ ist π verzweigt, da $\mathbb{P}^1$ keine nicht-trivialen unverzweigten Überlagerungen besitzt.

Nach der Deuring-Schafarewitsch-Formel gilt $h_{Y_f} - 1 = 2(h_{\mathbb{P}^1} - 1) + (e_\infty - 1) = 2(0-1) + (2-1) = -1$, also auch $h_{Y_f} = 0$.

Sei $\widetilde{\infty} \in Y_f$ der (eindeutige) Punkt über $\infty \in \mathbb{P}^1$. Um das Geschlecht von Y_f mittels der Riemann-Hurwitz-Formel zu bestimmen, müssen wir die Bewertung der Diskriminante bei $\widetilde{\infty}$ berechnen, sei also v die Bewertung bei $\widetilde{\infty}$. Wir sind im total verzweigten Fall, also genügt es, die Bewertung der Ableitung des Minimalpolynoms ϕ eines lokalen Parameters t bei $\widetilde{\infty}$ zu bestimmen: Es gilt ([**Sti1**], Proposition III.5.12)

$$d(\widetilde{\infty}|\infty) = v\left(\phi'(t)\right).$$

Es gilt $v(x) = -e_{\widetilde{\infty}} = -2$, und folglich $2v(y) = v(y^2 + y) = v(f) = -2(2g+1)$. Somit ist $v(y) = -(2g+1)$, und $t := y/x^{g+1}$ ist ein lokaler Parameter bei $\widetilde{\infty}$. Das Minimalpolynom von t über $k(x)$ ist

$$\phi(T) = (T - \frac{y}{x^{g+1}})(T - \frac{y+1}{x^{g+1}}) \in kx[T],$$

also ist

$$\phi'(t) = \frac{y}{x^{g+1}} + \frac{y+1}{x^{g+1}} = \frac{1}{x^{g+1}}.$$

Nun ist schliesslich $d(\widetilde{\infty}|\infty) = v(\phi'(t)) = -(g+1)v(x) = 2g+2$. Endlich gilt mit der Riemann-Hurwitz-Formel , dass $2(g_{Y_f} - 1) = 2 \cdot 2(g_{\mathbb{P}^1} - 1) + d(\widetilde{\infty}|\infty) = -4 + 2g + 2$, also gilt $2g_{Y_f} - 2 = 2g - 2$, und schliesslich $g_{Y_f} = g$. $\therefore$

Die Strategie ist nun, Y_f für geeignet gewähltes f um eine unverzweigte Galoisüberlagerung $X|Y_f$ von Grad 3 so zu erweitern, dass die resultierende Überlagerung $X|\mathbb{P}^1$ Galoissch mit Gruppe S_3 ist.

Lemma 5.1.2. *Sei $L|K$ eine Galoiserweiterung von Körpern in Charakteristik ungleich* 3, *mit Gruppe $C_2 = \langle\tau|\tau^2 = 1\rangle$, und umfasse K die dritten Einheitswurzeln μ_3. Sei $u \in L^*$. Die Erweiterung $L(\sqrt[3]{u})|K$ ist Galoissch mit Gruppe $S_3 = \langle\tau,\sigma|\tau^2 = \sigma^3 = (\tau\sigma)^2 = 1\rangle$ genau dann, wenn*

(i) $u \notin (L^*)^3$
(ii) $u \cdot \tau(u) \in (L^*)^3$

Beweis. Die erste Bedingung bedeutet, dass $L(\sqrt[3]{u})|L$ nicht-trivial ist. Falls sie erfüllt ist, ist das nach Kummer-Theorie eine Galoiserweiterung mit Gruppe $C_3 = \langle\sigma|\sigma^3 = 1\rangle$. Sei $z := \sqrt[3]{u}$ eine feste Wahl einer dritten Wurzel aus u. Wir haben dann den Isomorphismus

$$\mathrm{Gal}(L(z)|L) \longrightarrow \mu_3, \quad \sigma \mapsto \frac{\sigma(z)}{z}.$$

Um sicherzustellen, dass $L(z)|K$ Galoissch mit Gruppe S_3 ist, benötigen wir eine Fortsetzung von τ zu einem Automorphismus von $L(z)$ über K, so dass $(\tau\sigma)^2 = 1$ gilt. Diese Fortsetzung nennen wir wieder τ.

Angenommen, so eine Fortsetzung existiert, rechnen wir:

$$\frac{\sigma(\tau z)}{\tau z} = \tau\left(\frac{\tau\sigma\tau z}{z}\right) = \frac{\tau\sigma\tau z}{z} = \frac{\sigma^2 z}{z} = \left(\frac{\sigma z}{z}\right)^2 = \frac{z}{\sigma z},$$

dabei benutzt die zweite Gleichheit, dass $\mu_3 \subset K$ ist, und in der dritten Gleichung benutzen wir die Relation $(\tau\sigma)^2 = 1$. Somit erhalten wir

$$1 = \frac{\sigma z}{z} \cdot \frac{\sigma\tau z}{\tau z} = \frac{\sigma(z \cdot \tau(z))}{z \cdot \tau(z)},$$

also $z \cdot \tau(z) \in L^*$. Dies ist äquivalent mit der zweiten Bedingung des Lemmas, nämlich $u \cdot \tau(u) \in (L^*)^3$.

Anderseits, angenommen die zweite Bedingung gilt, so können wir durch

$$\tau(z) := \frac{\sqrt[3]{u \cdot \tau(u)}}{z}$$

eine Fortsetzung von τ auf $L(z)$ definieren. Auf die Wahl der dritten Wurzel kommt es dabei nicht an. $\therefore$

Soweit so gut. Wie aber sollen wir $u \in k(Y_f)$ wählen, um eine unverzweigte Überlagerung zu erhalten?

Lemma 5.1.3. *Sei Y_f eine Kurve wie in Lemma 5.1.1. Sei $L = k(Y_f) = k(x,y)$ der zugehörige Funktionenkörper. Sei $u \in L^*$ und X die zum Funktionenkörper $k(Y_f)(\sqrt[3]{u})$ assoziierte Kurve. Die Überlagerung $X \longrightarrow Y_f$ ist unverzweigt genau dann, wenn der Divisor $D = (u) \in \mathrm{Div}(Y)$ an jeder Stelle durch 3 teilbar ist.*

Beweis. Sei $z := \sqrt[3]{u}$, und $P' \in X$ ein Punkt, welcher auf $P \in Y_f$ abgebildet wird. Angenommen $3 \nmid v_P(u)$. Dann ist $3v_{P'}(z) = v_{P'}(u) = e(P'|P)v_P(u)$, und es folgt $3 \mid e(P'|P)$, also ist P verzweigt.

Anderseits, angenommen $3 \mid v_P(u)$. Sei also $v_P(u) = 3\ell$ für $\ell \in \mathbb{Z}$, und wähle $t \in k(Y_f)$ mit $v_P(t) = \ell$. Wir setzen $y_1 := t^{-1}y$ und $u_1 := t^{-3}u$. Dann ist natürlich $y_1^3 = u_1$, ferner $0 = v_P(u_1) = v_{P'}(y_1)$, und $\sqrt[3]{u_1} = t^{-1}z$ erzeugt denselben Funktionenkörper wie z. Durch Ersetzen von (y,u) durch (y_1,u_1) können wir also den allgemeinen Fall $3 \mid v_P(u)$ auf den Spezialfall $v_P(u) =$ reduzieren. Für diesen letzteren ist die Aussage aber klar. Also ist P unverzweigt. $\therefore$

Lemma 5.1.4. *Ist Y eine Kurve von Geschlecht g, ferner $D \in \mathrm{Div}(Y)$ ein Divisor vom Grad 0, und $P_\infty \in Y$ ein beliebiger Punkt, so existieren Punkte $P_1, \dots, P_g \in Y$, sodass $D \sim P_1 + \cdots + P_g - gP_\infty$.*

Beweis. Folgt direkt aus dem Satz von Riemann-Roch. $\therefore$

Lemma 5.1.5. *Sei $D := 3g \cdot \widetilde{\infty}$. Der Vektorraum $H^0(Y_f, \mathcal{O}(D))$ hat als Basis die Funktionen x^i, mit $0 \leq i \leq 3g/2$, und $x^j y$, mit $0 \leq j \leq (g+1)/2$. Insbesondere ist für $g = 2$ die Menge $\{1, x, x^2, x^3, y\}$ eine Basis.*

Beweis. Mit Hilfe des Satzes von Riemann-Roch erhalten wir

$$h^0(Y_f, \mathcal{O}(D)) = 3g + 1 - g + h^0(Y_f, \mathcal{O}(K - D)) = 2g + 1.$$

Der zweite h^0-Term verschwindet, da der Divisor $K - D$ negativen Grad $2g - 2 - 3g < 0$ hat. Wir wissen bereits, dass $v_{\widetilde{\infty}}(x) = -2$, und $v_{\widetilde{\infty}} = -2g - 1$. Die angegebenen Funktionen liegen also in $H^0(Y_f, \mathcal{O}(D))$, sind linear unabhängig, und aus Dimensionsgründen bilden sie auch eine Basis. $\therefore$

Sei u wie in Lemma 5.1.2. Wir können für $v \in (L^*)^3$ immer noch die Ersetzung $u \mapsto uv$ vornehmen, dabei geht $1/3(u)$ in $1/3(u) + (v)$ über, an der Divisorenklasse ändert sich also nichts. Mittels Lemma

5.1.4 dürfen wir oBdA annehmen, dass $(u) = 3(P_1 + \cdots + P_g - g\widetilde{\infty})$ für geeignete Punkte P_i gilt, und nach Lemma 5.1.5 ist $u = a + by$ für $a, b \in k[x]$ mit $\deg a \leq 3g/2$ und $\deg b \leq (g+1)/2$. Nachfolgend zur Übersicht nochmals die Situation:

$$\begin{array}{lll}
X: & z^3 = u(x,y) = a(x) + b(x)y, & \deg a \leq \dfrac{3g}{2}, \deg b \leq \dfrac{g+1}{2} \\
\quad | & & \\
\widetilde{\infty} \in Y_f: & y^2 + y = f(x), & \deg f = 2g+1 \\
\quad | & & \\
\infty \in \mathbb{P}^1 & &
\end{array}$$

Wir setzen $\psi := u \cdot \tau(u) = (a + by)(a + b(y+1)) = a^2 + ab + b^2 f$. Wir wollen vorerst die Polynome f, a und b als Freiheitsgrade lassen, und den Divisor von ψ vorgeben. Um dann sicherzustellen, dass die resultierende Überlagerung $X \longrightarrow Y_f$ tatsächlich étale ist, fehlt uns bloss noch das folgende Lemma.

Lemma 5.1.6. *Falls $(\psi) = 6x_1 + \cdots + 6x_g - 6g\infty \in \mathrm{Div}(\mathbb{P}^1)$, wobei $x_i \neq x_j$ für $i \neq j$, und falls die Polynome a und b teilerfremd sind, so gilt*

$$(u) = 3P_1 + \cdots + 3P_g - 3g\widetilde{\infty} \in \mathrm{Div}(Y_f)$$

für geeignete Punkte $P_i \in Y_f$, mit $P_i \neq P_i^\tau$ und $P_i \neq P_j, P_j^\tau$ (für $i \neq j$).

Beweis. Sei $(u) = \sum n_i Q_i \in \mathrm{Div}(Y_f)$. Dann ist $(\psi) = (u) + (u)^\tau = \sum n_i Q_i + \sum n_i Q_i^\tau$. Die Annahme, dass a und b teilerfremd sind, impliziert dass u und $\tau(u)$ disjunkte Divisoren haben, denn: Gilt $u(Q) = 0$, also $a(x_Q) = b(x_Q)y_Q$, und angenommen $u(Q^\tau) = 0$, also $a(x_Q) = b(x_Q)y_Q + b(x_Q)$, so folgt zuerst $b(x_Q) = 0$, und dann $a(x_Q) = b(x_Q)y_Q = 0 \cdot y_Q = 0$. Also hätten a und b eine gemeinsame Nullstelle x_Q, und wären nicht teilerfremd. Aus der Disjunktheit der Divisoren (u) und $(u)^\tau$ folgen alle Behauptungen des Lemmas. $\therefore$

Wir wählen also Punkte $x_1, \ldots, x_g \in \mathbb{A}^1 \subset \mathbb{P}^1$. Der Ansatz ist

$$\psi = (x - x_1)^3 \cdots (x - x_g)^3 = a^2 + ab + b^2 f;$$

das liefert ein Gleichungssystem in den Koeffizienten von a, b und f.

Kommen wir zu unserem ersten Beispiel. In diesem wollen wir f vom Grad 5 wählen, also $g(Y_f) = 2$. Wir nehmen als Ansatz $\psi = x^3(x+1)^3$ – das ist fast der allgemeine Fall, da der $\mathbb{P}^1$ für jedes Tripel (P_1, P_2, P_3) einen Automorphismus zulässt, welcher das Tripel durch $(0, 1, \infty)$ ersetzt. Das Polynom $a(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3$ hat dann Grad kleiner gleich 3, und $b(x)$ ist eine Konstante λ. Zu lösen ist also

$$a^2 + \lambda a + \lambda^2 f = x^3(x+1)^3 = x^6 + x^5 + x^4 + x^3.$$

Als erstes folgt $a_3 = 1$. Die Teilerfremdheit von a und b bedeutet einfach, dass $b = \lambda \in k^*$ ein nicht-verschwindender Skalar ist. Eine partikuläre Lösung ist nun $b(x) = 1$ und $a(x) = x^3 + x^2$, sodass $f(x) = x^5 + x^2$. Man überprüft schnell, dass $u = a + by = x^3 + x^2 + y$ keine dritte Potenz ist, also die Voraussetzung von Lemma 5.1.2.i erfüllt.

Beispiel 5.1.7 ($g_X = 4, h_X = 2, g_Y = 2, h_Y = 0$).

$$X: \quad z^3 = x^2(x+1) + y$$
$$Y: \quad y^2 - y = x^2(x^3+1)$$

Die Überlagerung $X|Y$ ist étale, wohingegen $Y|\mathbb{P}^1$ genau über ∞ verzweigt ist. Die Kurve X kann auch durch

$$X: \quad z^3(z^3+1) = x^3(x+1)^3$$

beschrieben werden. S_3 operiert via $\tau(z) = x(x+1)/z$, und $\sigma(z) = \zeta_3 z$, wobei ζ_3 eine primitive Einheitswurzel ist.

Die Darstellung von G auf $H^0(X, \Omega_X)^s$ hat modularen Charakter $\phi(e) = 2$ und $\phi(\sigma) = -1$. Die Darstellung ist also die irreduzible zweidimensionale Darstellung M von S_3 in Charakteristik 2. Eine explizite Basis von $H^0(X, \Omega_X)^s$ ist $z \cdot dx$ und $\mathcal{C}(z \cdot dx) = (x^2 + x)/z \cdot dx$. Es gilt $\Omega(R_{S_3}) = 0$, ferner $b(S_3, k) = 0$ und $b(S_3, M) = 1$.

Beweis. Wir wissen dass σ auf x und y trivial operiert, auf z hingegen durch Multiplikation mit einer primitiven dritten Einheitswurzel. Anderseits operiert τ auf x trivial, auf y hingegen durch $\tau(y) = y + 1$. Daraus folgt dass

$$z^3 \cdot \tau(z^3) = \psi = x^3(x+1)^3.$$

Wir können also durch $\tau(z) := \frac{x(x+1)}{z}$ die Operation von τ in kompatibler Weise auf z ausdehnen.

Die Aussagen über die Verzweigung folgen aus den vorangegangenen Lemmata, ferner ist klar dass $g(Y) = 2$ und $h(Y) = 0$ gilt. Da $X|Y$ unverzweigt ist, folgt mit der Riemann-Hurwitz-Formel $g(X) = 3g(Y) - 2 = 6 - 2 = 4$. Die S_3-Operation hat auf X drei Fixpunkte; Korollar 2.2.4 sagt uns also, dass $h(X)$ gerade sein muss. Die globale Abschätzung $g_X - h_X \le g_Y - h_Y = 2$ liefert schliesslich $h_X \in \{0, 2\}$.

Zum Schluss müssen wir explizit eine Basis von $H^0(X, \Omega_X)^s$ bestimmen. Das Differential dx ist ein meromorphes Differential. Da die Überlagerung $\pi : X \longrightarrow \mathbb{P}^1$ über $\mathbb{A}^1$ unverzweigt ist, gilt $v_P(dx) = 0$ für $P \in \pi^{-1}(\mathbb{A}^1)$. Wir haben $\pi^{-1}(\{\infty\}) = \{\infty_1, \infty_2, \infty_3\}$. Aus Symmetrie folgt $(dx) = \ell(\infty_1 + \infty_2 + \infty_3)$, wir müssen ℓ bestimmen. Wir wissen dass $3\ell = \deg(dx) = 2g_X - 2 = 8 - 2 = 6$ gilt, also $\ell = 2$ ist.

Das heisst also, dass $D := (dx) = 2(\infty_1 + \infty_2 + \infty_3)$ und

$$H^0(X, \Omega_X) = H^0(X, \mathcal{O}_X(D)) \cdot dx.$$

Ich behaupte, dass $z \in H^0(X, \mathcal{O}_X(D))$ liegt. Denn z kann wegen der Gleichheit $z^3 = x^3 + x^2 + y$ höchstens dort Pole haben, wo x oder y

welche haben, also bei den ∞_i. Der Term x^3 dominiert, also gilt

$$v_{\infty_i}(z) = \frac{1}{3} v_{\infty_i}(x^3) = \frac{-6}{3} = -2.$$

Betrachten wir nun $\omega := z \cdot dx \in H^0(X, \Omega_X)$. Es ist dann

$$\mathcal{C}(\omega) = \sqrt{\frac{dz}{dx}} dx = \frac{x^2 + x}{z} dx,$$

denn:

$$z^2 dz = d(z^3) = d(x^3 + x^2 + y) = x^2 dx + dy = x^2 dx + x^4 dx = (x^4 + x^2) dx,$$

also auch

$$\frac{dz}{dx} = \frac{x^4 + x^2}{z^2}.$$

Zufälligerweise ist also jetzt gerade $\mathcal{C}(\omega) = \tau(\omega)$. Das erspart uns eine weitere Rechung; und wir erhalten $\mathcal{C}(\mathcal{C}(\omega)) = \tau^2(\omega) = \omega$. Da z und $\tau(z)$ k-linear unabhängig sind, haben wir in $\{\omega, \tau(\omega)\}$ eine Basis von $H^0(X, \Omega_X)^s$ gefunden. Es ist jetzt ein leichtes, den modularen Charakter dieser Darstellung von S_3 explizit zu bestimmen. Sei M die (projektive) zweidimensionale Darstellung von S_3. In Termen der Kapitel 3 und 4 gilt $R_{S_3} = \ker(k[S_3/S_2] \longrightarrow k) = M$, also $\Omega^1 R_{S_3} = 0$, und $b(S_3, k) = b(S_2, k) = 0$. Was uns Theorem 4.1.3 nicht sagt, wir folglich berechnen mussten, war $b(S_3, M) = 1$.

Ausserdem ist $H^0(X, \Omega_X)^n = H^0(Y, \Omega_Y)$, mit Basis $\{dx, x \cdot dx\}$. $\therefore$

Im nächsten Beispiel möchte ich die Gruppe S_3 beibehalten, aber auf der Stufe von Y anstatt $g = 2$ und $h = 0$ die Vorgaben $g_Y = 2$ und $h_Y = 1$ machen. Das lässt sich nur erreichen, wenn $Y|\mathbb{P}^1$ über *zwei* Punkten erreicht ist. Wir wollen dann wieder eine dreifache unverzweigte Überlagerung $X|Y$ konstruieren, sodass $X|\mathbb{P}^1$ Galoissch mit Gruppe S_3 ist. Dieses Mal lasse ich die expliziten Rechnungen weg.

Beispiel 5.1.8 ($G = S_3, g_X = 4, h_X = 3, g_Y = 2, h_Y = 1$). Hier sei ζ eine dritte Einheitswurzel.

$$\begin{aligned} X: \quad & z^3 = x^3 + \zeta^2 x^2 + \zeta x + 1 + \zeta xy \\ Y: \quad & y^2 - y = \zeta x^3 + 1/x \end{aligned}$$

Die Überlagerung $X|Y$ ist unverzweigt, wohingegen $Y|\mathbb{P}^1$ genau über 0 und ∞ verzweigt ist. Hier ist $\Omega(R_{S_3}) = k$, daneben $b(S_3, k) = 0$ und $b(S_3, M) = 1$, dabei ist M die irreduzible zweidimensionale Darstellung von S_3.

Wir haben hier $a(x) = x^3 + \zeta^2 x^2 + \zeta x + 1$, $b(x) = \zeta x$ und $f(x) = \zeta x^3 + 1/x$ gesetzt, also $\psi = a^2 + ab + b^2 f = x^6 + x^5 + x^3 + x + 1 = (x + \zeta)^3 (x + \zeta^2)^3$.

5.2. S_4

Wir betrachten eine Kurve in Charakteristik 2, deren Automorphismengruppe S_4 umfasst, um Bemerkung 4.1.4 zu verdeutlichen. Es sei $V \subset S_4$ die Kleinsche Vierergruppe; wir identifizieren S_3 mit S_4/V. Es gilt $S_{S_4} = S_{S_3} = \{k, M_2\}$, dabei bezeichnet k die triviale eindimensionale Darstellung, und M_2 die zwei-dimensionale irreduzible Darstellung von S_3.

Beispiel 5.2.1 ($G = S_4, g = 13, h = 5$). Sei T eine Kurve, auf welcher S_4 operiert, und zwar so, dass die Quotientenkurve $X := T/V$ zusammen mit der induzierten S_3-Operation mit der Kurve X aus Beispiel 5.1.7 und der dort definierten S_3-Operation übereinstimmt. Wir erinnern daran, dass $g_X = 4$ und $h_X = 2$ ist, und dass

$$H^0(X, \Omega_X)^s \cong P_{S_3}(M_2) = M_2$$

gilt. Wir nehmen an, dass $T \longrightarrow X$ unverzweigt ist. Dann folgt, dass $g_T = 4(g_X - 1) + 1 = 13$ ist. Da X drei verzweigte Punkte hat, existieren auf T deren 12, und somit gilt

$$h_T \equiv 1 - 12 \equiv 5 \pmod 8$$

nach unserer Kongruenzformel, da $|S_4| = 24 = 8 \cdot 3$ ist. Die globalen Abschätzungen zeigen, dass auch

$$2 = h_X \leq h_T \leq g_T - (g_X - h_X) = 11$$

gilt, und somit folgt, dass $h_T = 5$ ist. Wir hätten den p-Rang von T auch mittels der Deuring-Schafarewitsch-Formel aus dem p-Rang von X bestimmen können: $h_T = 4(h_X - 1) + 1 = 5$.

Da die Dimensionen aller projektiven Darstellungen der S_4 durch 8 teilbar sind, müssen alle Borne-Invarianten von T bezüglich S_4 verschwinden, es gilt also $b(S_4, k) = b(S_4, M_2) = 0$, und somit

$$H^0(T, \Omega_T)^s \cong \Omega_{S_4}(R_{S_4}).$$

5.3. D_n

Anstelle von Beispielen mit Gruppe $S_3 = D_3$ lassen sich auch leicht Beispiele mit Gruppe D_n für $n > 3$ produzieren. Wir schreiben

$$D_n = \langle \tau, \sigma \mid \tau^2 = \sigma^n = (\tau\sigma)^2 = 1 \rangle.$$

Hier ist eines:

Beispiel 5.3.1 ($G = D_5, g_X = 6, h_X = 4, g_Y = 2, h_Y = 0$).

$$\begin{aligned} X: \quad z^5 &= x^4(x+1) + (1 + x + x^2)y \\ Y: \quad y^2 - y &= x^4(x+1) \end{aligned}$$

Die Überlagerung $X|Y$ ist unverzweigt, wohingegen $Y|\mathbb{P}^1$ genau über ∞ verzweigt ist. Die Kurve X lässt sich alternativ als

$$X : z^5(z^5 + 1 + x + x^2) = x^5(x+1)^5$$

schreiben. Deshalb operiert D_5 via

$$\tau(x,y,z) = (x, y+1, \frac{x(x+1)}{z}), \qquad \sigma(x,y,z) = (x,y,\zeta_5 z),$$

dabei ist ζ_5 eine primitive fünfte Einheitswurzel.

Eine Basis von $H^0(X, \Omega_X)^s$ ist

$$\left\{ z \cdot dx, \mathcal{C}(z \cdot dx) = (x^3 + x^2 + y)/z^2 \cdot dx, \tau(z) \cdot dx, \mathcal{C}(\tau(z) \cdot dx) \right\}.$$

Der modulare Charakter ist $\phi(e) = 4$, $\phi(\sigma) = \phi(\sigma) = -1$. Die Darstellung hat also als Kompositionsfaktoren genau die zwei irreduziblen zweidimensionalen Darstellungen M_2 und $M_{2'}$ von D_5. Wir haben $\Omega(R_{D_5}) = 0$, ferner $b(D_5, M_2) = b(D_5, M_{2'}) = 1$, und die Borne-Invarianten verschwinden für die eindimensionale Darstellung k.

Hier ist eine Serie von Beispielen:

Beispiel 5.3.2 (D_n-Überlagerungen des $\mathbb{P}^1$). Sei n ungerade.

$$X_n : \quad z^n(z^n + 1 + x + \cdots + x^{n-3}) = x^n(x+1)^n$$

Die Kurve X_n ist eine D_n-Überlagerung des $\mathbb{P}^1$. Wir haben $g_{13} = 144$, $g_{11} = 78$, $g_9 = 64$, $g_7 = 36$, $g_5 = 6$ und $g_3 = 4$. In all diesen Fällen gilt $g_n - h_n = 2$. Allerdings ist der Quotient von X_n nach $C_n = \langle\sigma\rangle$ für $n \geq 7$ nicht mehr unverzweigt.

Bemerkung 5.3.3. Diese letzte Serie wurde nicht von Hand, sondern mit dem Computeralgebrasystem KASH/KANT 2.2 berechnet. In Anhang B wird kurz erklärt, wie das geht.

KAPITEL 6

Vermutungen

6.1. Relative Maximalität

Was Theorem 4.1.3 frei lässt, sind die Borne-Invarianten für Darstellungen, die nicht von Quotientengruppen induziert werden können. Aufgrund der Berechnung der Beispiele aus dem letzten Kapitel mache ich folgende Beobachtung: Eine (separable) Überlagerung $\pi : X \longrightarrow Y$ von Kurven muss, wie wir wissen, a priori die Abschätzung $g_X - h_X \geq g_Y - h_Y$ erfüllen.

Definition 6.1.1 (Relative Gewöhnlichkeit (provisorische Form)). Eine Kurve X heisst *relativ gewöhnlich* bezüglich einer Überlagerung $\pi : X \longrightarrow Y$, falls die Gleichung

$$g_X - h_X = g_Y - h_Y$$

erfüllt ist. Die Überlagerung π heisst dann ebenfalls *relativ gewöhnlich*.

Eine Galoisüberlagerung durch eine p-Gruppe in Charakteristik wird im allgemeinen nicht relativ gewöhnlich sein. Durch Vergleich der Riemann-Hurwitz-Formel und der Deuring-Schafarewitsch-Formel sehen wir, dass wilde Verzweigung zwar zum Geschlecht, nicht aber zum p-Rang beiträgt.

Es stellt sich die Frage, wie der aus dem Grad der Überlagerung und der Verzweigung entstehende Beitrag an das Geschlecht einer überlagernden Kurve sich auf den p-Rang auswirkt. Wird der halbeinfache oder der nilpotente Anteil grösser?

Vermutung 6.1.2 (naive Form). *Ist $\pi : X \longrightarrow Y$ eine Überlagerung von Grad d, der kein Vielfaches der Charakteristik ist, so wird* im allgemeinen *π relativ gewöhnlich sein.*

Wieso könnte diese Vermutung richtig sein?

Beispiel 6.1.3 (Elliptische Kurven). In Charakteristik $p \neq 2$ lässt sich jede elliptische Kurve durch eine Gleichung der Form

$$E_\lambda : y^2 = x(x-1)(x-\lambda) \quad \lambda \in k \setminus \{0, 1\}$$

schreiben, also als zweifache Überlagerung des $\mathbb{P}^1$, verzweigt genau über $\{0, 1, \lambda, \infty\}$. Für eine offene, Zariski-dichte Teilmenge von k wird E_λ gewöhnlich sein, also relativ gewöhnlich bezüglich der Projektion via x. In Termen von Galois-Moduln, mit $G = S_2$, ist aus Charakteristik-Gründen stets $\Omega(R_G) = 0$ und $P_G(V) = V$. Mit Theorem 4.1.3 ist

$b(G,k) = 0$, und wenn S die nicht-triviale eindimensionale Darstellung ist, gilt $b(G,S) = 0,1$, dabei entspricht $b(G,S) = 1$ dem generischen, relativ gewöhnlichen Fall.

Beispiel 6.1.4 (S_3-Überlagerungen von $\mathbb{P}^1$, étale über $\mathbb{A}^1$). In den Beispielen des vorherigen Abschnitts mit Gruppe S_3 können wir $\pi : X \longrightarrow X/S_3 = \mathbb{P}^1$ in zwei Überlagerungen $X \longrightarrow X/A_3$ und $X/A_3 \longrightarrow X/S_3$ aufspalten. Die zweite ist eine verzweigte p-Überlagerung, und folglich *nicht* relativ maximal. Die Überlagerung $X \longrightarrow X/A_3$ jedoch ist in allen von mir bislang berechneten Beispielen relativ-maximal, sowohl in den unverzweigten Fällen, wie auch in den verzweigten (Beispiel 5.3.2).

Die Vermutung erscheint als relativer Fall des klassischen Resultats, dass eine offene, Zariski-dichte Teilmenge des Moduliraums $\mathcal{M}_g$ der Kurven von Geschlecht g gewöhnlich ist [**Kob1**].

6.2. Eine Verfeinerung

Spezialisieren wir uns auf den Fall von unverzweigten Galois-Überlagerungen $\pi : X \longrightarrow Y$ von Grad n, lassen dabei aber beliebige n zu, und betrachten die bekannten globalen Abschätzungen $h_X \geq h_Y$ und $g_X - h_X \geq g_Y - h_Y$. Durch Umschreiben erhalten wir die äquivalenten Formen

$$h_X - 1 \geq h_Y - 1$$

und

$$h_X - 1 \leq (h_Y - 1) + (n-1)(g_Y - 1).$$

In Kapitel 2 haben wir einen Term $n_k(h_Y - 1)$ in $h_X - 1$ identifiziert, wobei n_k die Multiplizität der trivialen in der regulären Darstellung der Galoisgruppe in der gegebenen Charakteristik des Grundkörpers bezeichnet.

Proposition 6.2.1. *Ist $\pi : X \longrightarrow Y = X/G$ eine unverzweigte Galoisüberlagerung mit Gruppe G, und ist $M \in S_G$ eine irreduzible Darstellung von G, so gilt (in der Notation von Kapitel 2) eine Abschätzung*

$$\chi(Y \smallsetminus \pi(D), F_M) \leq \dim_k(M) \cdot (g_Y - 1).$$

Beweis. Diese Vermutung erscheint aus dem obigen recht natürlich, denn die Summe dieser Abschätzungen über alle irreduziblen Darstellungen, gewichtet mit ihrer Multiplizität in der regulären Darstellungen, ist gültig – sie bedeutet ja gerade $g_X - h_X \geq g_Y - h_Y$. Sie lässt sich mit [**Pin1**], Proposition 7.1 beweisen. $\therefore$

Korollar 6.2.2 (Obere Abschätzung). *Ist $\pi : X \longrightarrow Y/G$ eine unverzweigte Galois-Überlagerung mit Gruppe G der Ordnung n, und n_k wie oben, so gilt die Abschätzung*

$$h_X - 1 \leq n_k(h_Y - 1) + (n - n_k)(g_Y - 1).$$

Beweis. Mit der Proposition und den Methoden aus Kapitel 2. $\therefore$

Eine verbesserte Definition von *relativer Gewöhnlichkeit* einer Galoisüberlagerung, welche sinnvoll ist auch für Überlagerungen, deren Grad durch die Charakteristik teilbar ist, müsste dieses Korollar miteinbeziehen.

6.3. Moduli von Galoisüberlagerungen

Um die Vermutung 6.1.2 präziser zu formulieren, müsste man sich Gedanken über die Moduli von Galoisüberlagerungen machen. Wir halten eine Kurve Y fest, daneben eine gewünschte Galoisgruppe G und suchen eine G-Überlagerung von X. Dabei wollen wir alle diskreten Invarianten festhalten, insbesondere also die Stabilisatoren über Punkten $y \in Y$, und die Hilbertsche Untergruppenkette dieser Stabilisatoren. Aus diesen Überlagerungen wäre ein Modulschema zu produzieren, das wohl im allgemeinen nicht irreduzibel wäre, und auf dem Modulschema wären *relativ maximale* Punkte zu suchen, und die Oberhalbstetigkeit des p-Ranges in Familien auszunützen.

Das ist ein offenes Forschungsprojekt, welches für zyklische Galoiserweiterungen am machbarsten erscheint.

ANHANG A

Modulare Darstellungstheorie

Wir wiederholen in diesem Abschnitt einige Resultate der Darstellungstheorie einer endlichen Gruppe G über einem Körper k der Charakteristik p zur Referenz des Lesers. Anstelle der in Charakteristik 0 klassischen Korrespondenz zwischen Isomorphieklassen von Darstellungen und ihren zugehörigen Charakteren treten die *modularen Charaktere*, welche nicht mehr den Isomorphietyp, sondern bloss die Kompositionsreihe der Darstellung bestimmen.

Definition A.0.1. Eine *Darstellung* von G ist ein (Links-)$k[G]$-Modul M endlicher Dimension über k. Die Darstellung heisst *einfach* oder *irreduzibel*, falls M keine nicht-trivialen $k[G]$-Untermodulen besitzt. Sie heisst *unzerlegbar*, falls M nicht in eine direkte Summe $M = M_1 \oplus M_2$ von nicht-trivialen $k[G]$-Untermoduln M_i von M zerlegt werden kann.

Beispiel A.0.2. Ist P eine p-Gruppe, und k ein Körper der Charakteristik $p > 0$, so existiert nur ein einfacher kP-Modul, nämlich der eindimensionale triviale Modul k. Denn: Der vom Orbit eines beliebigen nicht-trivialen Elements aufgespannte $\mathbb{F}_p$-Untervektorraum X ist eine endliche Menge, auf welcher P operiert. Nach einer elementaren Kongruenzformel (s. [**Ser2**], Lemma 8.3) gilt für die Fixpunktmenge X^G

$$0 \equiv |X| \equiv |X^G| \pmod p.$$

Da $0 \in X^G$ liegt, gilt also $|X^G| \geq p$, insbesondere existiert ein nicht-trivialer Fixpunkt von X, welcher den gesuchten eindimensionalen P-invarianten Untermodul aufspannt.

Definition A.0.3. Eine Darstellung heisst *halbeinfach*, falls sie in eine (endliche) direkte Summe einfacher Darstellungen zerlegt werden kann. Der Ring $k[G]$ heisst *halbeinfach*, falls alle Darstellungen halbeinfach sind.

Die Problematik der Darstellungstheorie ist, dass über einem Körper positiver Charakteristik der Ring $k[G]$ im allgemeinen *nicht* halb-einfach ist.

Proposition A.0.4 (Satz von Maschke). *Der Ring $k[G]$ ist halbeinfach genau dann, wenn p die Ordnung von G nicht teilt.*

Beweis. Corollary 3.6.12, S. 72 [**Ben1**]. $\therefore$

A.0.1. Gute Eigenschaften der Gruppenringe $k[G]$.

PROPOSITION A.0.5. *Der Ring $k[G]$ ist Noethersch, Artinsch, und eine kokommutative Hopf-Algebra bezüglich der Komultiplikation*

$$\Delta : k[G] \longrightarrow k[G] \otimes_k k[G], \qquad g \mapsto g \otimes g$$

und der Antipodenabbildung

$$\eta : k[G] \longrightarrow k[G], \qquad g \mapsto g^{-1}.$$

PROPOSITION A.0.6 (Fitting-Lemma). *Für eine Darstellung M und einen $k[G]$-Endomorphismus f von M gilt, für n gross genug, dass $M = \mathrm{Bild}(f^n) \oplus \mathrm{Ker}(f^n)$.*

BEWEIS. Lemma 1.4.4, S. 8 [**Ben1**]. ∴

PROPOSITION A.0.7 (Krull-Schmidt). *Jede Darstellung M hat die* eindeutige Zerlegungseigenschaft *(*Krull-Schmidt-Eigenschaft*), nämlich:*

(i) *M ist eine endliche direkte Summe unzerlegbarer Moduln.*
(ii) *Für zwei solche Zerlegungen $M = \oplus_{i=1}^m M_i = \oplus_{i=1}^n N_i$ mit jedem M_i und jedem N_i nicht-verschwindend und unzerlegbar gilt $m = n$, und nach eventueller Umordnung auch $M_i \cong N_i$.*

BEWEIS. Theorem 1.4.6, S. 8 [**Ben1**]. ∴

Unter allen Darstellungen sind die $k[G]$-projektiven ausgezeichnet.

DEFINITION/LEMMA A.0.8 (projektive Hüllen). Zu jedem $k[G]$-Modul M existiert eine *projektive Hülle* P_M, das heisst ein projektiver Modul P_M und ein Epimorphismus $P_M \longrightarrow M$, mit P_M minimal bezüglich Zerlegung in direkte Summen.

Wir definieren $\Omega(M)$ als Kern dieser Abbildung, und setzen dann für $i > 1$ induktiv $\Omega^i(M) := \Omega(\Omega^{i-1}(M))$.

BEWEIS. [**Ser2**], Chapter 14, Proposition 41. ∴

DEFINITION A.0.9. Das *Radikal* von M ist der Durchschnitt aller maximaler echter Untermoduln von M, und wird mit $\mathrm{Rad}(M)$ bezeichnet.

Der *Sockel* von M ist die Summe aller irreduzibler Untermoduln von M, und wird mit $\mathrm{Soc}(M)$ bezeichnet.

LEMMA A.0.10. *Der Modul M ist halbeinfach genau dann, wenn* $\mathrm{Soc}(M) = M$. *Falls M projektiv und unzerlegbar ist, so gilt $Soc(M) \cong M/\mathrm{Rad}(M)$.*

BEWEIS. Die erste Aussage folgt sogar für nicht endlich-erzeugte Moduln mit dem Lemma von Zorn. Die zweite ist [**Ben1**], Theorem 1.6.3. ∴

Proposition A.0.11. *Die Abbildung $M \mapsto P_M$ liefert eine Bijektion zwischen Isomorphieklassen einfacher $k[G]$-Moduln und Isomorphieklassen unzerlegbarer projektiver $k[G]$-Moduln. Die inverse Abbildung ist gegeben durch $P \mapsto P/\operatorname{Rad}(P)$ gegeben.*

Beweis. [**Ben1**], S. 14. ∴

Proposition A.0.12. *Die projektive Hülle $P(V)$ eines einfachen $k[G]$-Moduls V tritt in der regulären Darstellung mit Multiplizität* $\dim_k V$ *auf. Genauer: Es existiert ein Isomorphismus*

$$k[G] \cong \bigoplus_{V \in S_G} P(V)^{\dim_k(V)}.$$

Beweis. [**Bor1**], Lemma 2.7. ∴

Beispiel A.0.13. Ist P eine p-Gruppe, und k ein Körper der Charakteristik p, so existiert nur ein projektiver unzerlegbarer kP-Modul, nämlich die projektive Hülle des trivialen Moduls k. Es gilt also $k[P] \cong P(k)$ als $k[P]$-Moduln, und eine Darstellung ist $k[P]$-projektiv genau dann, wenn sie $k[P]$-frei ist.

A.0.2. Blöcke. Im klassischen Fall wo die Charakteristik p des Körpers die Ordnung der Gruppe G nicht teilt, ist $k[G]$ halbeinfach und zerfällt nach dem Struktursatz von Wedderburn in eine direkte Summe von Matrizenringen. Im allgemeinen Fall können wir $k[G]$ immer noch (als Ring) in unzerlegbare zwei-seitige Ideale B_i zerlegen,

$$k[G] = B_1 \oplus \cdots \oplus B_s.$$

Diese B_i werden die *Blöcke* von $k[G]$ genannt.

Für einen unzerlegbaren $k[G]$-Modul M gilt

$$M \cong k[G] \otimes_{k[G]} M = \bigoplus_{i=1}^{s} B_i \otimes M = B_j \otimes M$$

für ein j. Wir sagen dann, dass M *zum Block B_j gehört*. Offensichtlich gehören dann auch alle Kompositionsfaktoren von M zum Block B_j.

Beispiel A.0.14. Sei k ein Körper der Charakteristik 2, und sei $G = S_3$ die symmetrische Gruppe auf 3 Elementen. Dann ist die Blockzerlegung von $k[G]$ durch

$$k[G] \cong k[\varepsilon]/(\varepsilon^2) \oplus \operatorname{Mat}_{2\times 2}(k)$$

gegeben. Die triviale eindimensionale Darstellung gehört zum ersten Block; zum (halbeinfachen) zweiten Block gehört eine irreduzible zweidimensionale Darstellung.

Es gilt auch $k[\varepsilon]/(\varepsilon^2) \cong kS_2$; falls τ das Erzeugende von S_2 bezeichnet, geht dabei ε auf $\tau + 1$.

Bemerkung A.0.15. Man sagt, dass ein Block *Defekt* 0 hat, falls alle Darstellungen im Block projektiv sind. Eine irreduzible Darstellung gehört zu einem Block von Defekt 0 genau dann, wenn ihre Dimension durch die grösste Potenz von p teilbar ist, welche die Gruppenordnung teilt. Sie ist dann auch die einzige irreduzible Darstellung in ihrem Block.

A.0.3. Darstellungen von Untergruppen.

Definition A.0.16 (Restriktion, Induktion). Sei H eine Untergruppe von G. Dann ist $k[H]$ ein Unterring von $k[G]$, und eine Darstellung M von G liefert durch Einschränkung eine Darstellung von H. Wir schreiben $M \downarrow_H$ für den entstandenen $k[H]$-Modul, und nennen diese Operation *Restriktion*.

Umgekehrt liefert ein kH-Modul N zwei $k[G]$-Moduln, $N \uparrow^G := k[G] \otimes_{k[H]} N$ und $N \Uparrow^G := \mathrm{Hom}_{k[H]}(k[G], N)$. Wir nennen diese Operationen *Induktion* und *Koinduktion*.

Proposition A.0.17. *Es gibt einen Isomorphismus $k[G] \cong (k[G])^* = \mathrm{Hom}_k(k[G], k)$ als $k[G]$-$k[G]$-Bimoduln. Insbesondere sind für einen kH-Modul N die Induktion $N \uparrow^G$ und Koinduktion $N \Uparrow^G$ isomorph. Daneben ist eine Darstellung projektiv genau dann, wenn sie injektiv ist.*

Beweis. Es bezeichne e das triviale Element von G. Wir definieren

$$\lambda : k[G] \longrightarrow k, \qquad \sum_{g\in G} \lambda_g g \mapsto \lambda_e.$$

Der erste Isomorphismus ist eine Abbildung $\phi : k[G] \longrightarrow (k[G])^*$, welche für $x, y \in k[G]$ durch $\phi(x)(y) := \lambda(yx)$ gegeben ist. Der zweite folgt aus

$$N \uparrow^G = k[G] \otimes_{kH} N \cong (k[G])^* \otimes_{kH} N \cong \mathrm{Hom}_{kH}(k[G], N) = N \Uparrow^G .$$

$\therefore$

Definition A.0.18 (Relative Projektivität). Ein $k[G]$-Modul M heisst *projektiv relativ zu H*, falls für jedes Paar M_1 und M_2 von $k[G]$-Moduln, jede Abbildung $\lambda : M \longrightarrow M_1$ und jeden Epimorphismus $\mu : M_2 \longrightarrow M_1$ aus der Existenz einer Abbildung $\nu : M \downarrow_H \longrightarrow M_2 \downarrow_H$ mit $\lambda = \mu \circ \nu$ die Existenz einer Abbildung $\nu' : M \longrightarrow M_2$ mit $\lambda = \mu \circ \nu'$ folgt.

Für $H = 1$ ist ein Modul also projektiv relativ zu H genau dann, wenn er projektiv ist.

Proposition A.0.19. *Angenommen, der Index $[G : H]$ ist in k invertierbar. Dann ist jeder $k[G]$-Modul projektiv relativ zu H.*

Beweis. Corollary 3.6.9, S.72 [**Ben1**]. $\therefore$

Bemerkung A.0.20. Dies beweist insbesondere die eine Richtung des Satzes von Maschke.

ANHANG B

p-Ränge mit KASH berechnen

Wir beschreiben, wie man das Computeralgebrasystem KANT/KASH 2.2 den p-Rang einer Kurve, die über einem endlichen Körper definiert ist, ausrechnen lassen kann.

Beispiel B.0.21.

```
AlffInit(FF(2,1),"x","z");
f:=z^3*(z^3+1)+x^3*(x+1)^3;
AlffPolyIsIrrSep(f);
AlffOrders(f);
AlffHasseWittInvariant(F);
quit;
```

Die erste Zeile initialisiert das System, dabei erzeugt `FF(p,n)` einen endlichen Körper der Ordnung p^n. Der zweite Befehl prüft ein Polynom auf Irreduzibilität und Separabilität in z. Der dritte Befehl erzeugt den gewünschten Funktionenkörper, und `AlffHasseWittInvariant` bestimmt schliesslich den p-Rang.

Das obige Beispiel bestimmt also den p-Rang des Hauptbeispiels 5.1.7 aus Kapitel 4.

Die Beispielserie 5.3.2 wurde mit KASH berechnet.

Literaturverzeichnis

[Ben1] D.J. Benson: Representations and cohomology. Cambridge studies in advanced mathematics 30, 2nd edition (1997).

[Bor1] N. Borne: A relative Shafarevich theorem. Preprint math.AG/0204088 (2002).

[Bos1] J.-B. Bost: Courbes semi-stables et groupe fondamental en géométrie algébrique. Birkhäuser Progress in Mathematics 187, 2000.

[Cre1] R. Crew: Etale p-covers in characteristic p. Comp. Math. 52, 31-45 (1984).

[Har1] R. Hartshorne: Algebraic geometry. Springer GTM 52, 1977.

[Has1] H. Hasse: Zyklische unverzweigte Erweiterungskörper vom Primzahlgrad p über einem algebraischen Funktionenkörper der Charakteristik p. Monatshefte für Mathematik und Physik 43, 477-492 (1936).

[Kan1] E. Kani: The Galois-module structure of the space of holomorphic differentials of a curve. Journ. f. d. reine u. angew. Mathem. 367 (1986).

[Kob1] N. Koblitz: p-adic variation of the zeta-function. Comp. Math. Vol. 31, Fasc. 2, pp. 119-218 (1975).

[KoZi1] S. König, A. Zimmermann: Derived Equivalences for Group Rings. Springer Lecture Notes in Mathematics 1685 (1991).

[Mil1] J. Milne: Étale cohomology. Princeton UP, Princeton Mathematical Series 33 (1980).

[Mum1] D. Mumford: Abelian varieties. Tata institute of fundamental research, Studies in mathematics 5 (1970).

[Mur1] J. Murre: Lectures on an introduction to Grothendieck's theory of the fundamental group. Tata institute of fundamental research, Lectures on Mathematics and Physics 40, 1967.

[Nak1] S. Nakajima: p-ranks and automorphims groups of algebraic curves. Trans. AMS 303, 595-607 (1987).

[Nak2] S. Nakajima: Equivariant form of the Deuring-Shafarevich formula for Hasse-Witt invariants. Math. Z. 190, no. 4, 559-556 (1985).

[Pin1] R. Pink: Euler-Poincare formula in equal characteristic under ordinariness assumptions. manuscripta math. 102, 1-24 (2000).

[Ser1] J.-P. Serre: Sur la topologie des variétés algébriques en caractéristique p. Symp. Int. Top. Alg. Mexico, 24-53 (1958).

[Ser2] J.-P. Serre: Linear representations of finite groups. Springer GTM 42 (1977).

[Ser3] J.-P. Serre: Local fields. Springer GTM 67, 1979.

[Sti1] H. Stichtenoth: Algebraic Function Fields and Codes. Springer universitext (1993).

[Sti2] H. Stichtenoth: Die Hasse-Witt-Invariante eines Kongruenzfunktionenkörpers. Arch. Math 33, 357-360 (1979).

[Sub1] D. Subrao: The p-rank of Artin-Schreier curves. manuscripta math. 16, 169-193 (1975).

[Tam1] G. Tamme: Introduction to Étale Cohomology. Universitext, Springer (1994).