Hochschild-Homologie und Drinfeld-Moduln

Diplomarbeit
vorgelegt von
Stefan Wiedmann
aus
Ochsenhausen

angefertigt im
Mathematischen Institut
der Georg-August-Universität zu Göttingen

1998

Inhaltsverzeichnis

1 Einleitung

Die Untersuchung der *algebraischen Zahlkörper*, d. h. der endlichen algebraischen Körpererweiterungen von $\mathbf{Q}$ bildet die Grundlage der *algebraischen Zahlentheorie.* In Charakteristik p lassen sich den algebraischen Zahlkörpern die *Funktionenkörper*, d.h. endliche algebraische Körpererweiterungen des Körpers $\mathbf{F}_p(T)$ zur Seite stellen.
Der Ring $\mathbf{Z}$ und sein Quotientenkörper $\mathbf{Q}$ sind in enger Weise mit dem Polynomring $\mathbf{F}_p[T]$ und seinem Quotientenkörper $\mathbf{F}_p(T)$ verknüpft. Sowohl $\mathbf{Z}$ als auch $\mathbf{F}_p[T]$ sind Hauptidealringe und besitzen eine eindeutige Zerlegung in Primfaktoren. Den Primzahlen in $\mathbf{Z}$ entsprechen hierbei die normierten, irreduziblen Polynomen in $\mathbf{F}_p[T]$. In Analogie zur Situation in $\mathbf{Q}$ entstehen alle nicht archimedischen Bewertungen, mit Ausnahme der Gradbewertung, aus den irreduziblen Polynomen und alle auftretenden Restklassenringe sind endliche Körper.
Werden algebraische Körpererweiterungen von $\mathbf{F}_p(T)$ betrachtet, finden sich weitere Analogien zu den Zahlkörpern. Der ganze Abschluß von $\mathbf{F}_p[T]$ ist wiederum ein Dedekindring und auch die Gültigkeit der *Fundamentalen Gleichung*, $\sum e_i f_i =$ Grad der Körpererweiterung, bleibt erhalten. Darüberhinaus erfüllen auch die Bewertungen der Funktionenkörper eine Geschlossenheitsrelation.
Aufgrund der Analogien ist es nicht verwunderlich, daß die „großen“ Probleme der Zahlentheorie auf die Funktionenkörper übertragen worden sind. Als wohl schönstes Ergebnis konnte so die *Riemannsche Vermutung* über die Nullstellen der *Zeta-Funktion* im Falle der Funktionenkörper bewiesen werden.
Einen überraschenden Zugang zu den Problematiken der Zahlentheorie bildet die *algebraische Geometrie* bzw. das Studium von glatten, eindimensionalen Kurven. Eine Kurve heißt glatt, falls in allen abgeschlossenen Punkten ihre Residuenringe *regulär* sind. Im Falle von Kurven ist dies gleichbedeutend damit, daß die Residuenringe *diskrete Bewertungsringe* sind. Diese Beobachtung verknüpft die glatten Kurven mit der Bewertungstheorie und damit mit der Zahlentheorie.
Ziel des ersten Abschnitts der Arbeit ist die Verknüpfung der geometrischen Theorie der glatten Kurven in Charakteristik p mit den Funktionenkörpern zu formulieren.

Unter den glatten Kurven spielen die *elliptischen Kurven* eine zentrale Rolle. Von entscheidender Bedeutung ist die auf den elliptischen Kurven gegebene Gruppenstruktur, mit deren Hilfe sich viele Informationen über die Struktur von elliptischen Kurven gewinnen lassen. Im Rahmen einer modernen Formulierung der algebraischen Geometrie durch die Sprache der Schemata ist deshalb eine Übertragung des Gruppenbegriffs auf ein Schema wünschenswert und wird im zweiten Abschnitt ausführlich behandelt.

Wie zu Beginn erwähnt, spielt die Korrespondenz zwischen den algebraischen Zahlkörpern und den Funktionenkörpern eine wichtig Rolle in der Zahlentheorie. Dieselbe Idee wird auf die elliptischen Kurven angewandt und führt auf die Theorie der *Drinfeld-Moduln*, die die Rolle der elliptischen Kurven in Charakteristik p übernehmen.
In den Abschnitten 3 und 4 werden die Grundlagen für den Einstieg in die Theorie dieser wichtigen algebraischen Objekte geschaffen. Wie bei den Funktionenkörpern gibt es auch bei den Drinfeld-Moduln überaschende Analogien zu den elliptischen Kurven. Durch die Gruppenstruktur auf den elliptischen Kurven operiert $\mathbf{Z}$ auf den Punkten der Kurve und die Untersuchung des Torsionsverhaltens liefert die sogenannten *n-Teilungspunkte*. Die Übertragung dieses Konzepts auf die Drinfeld-Moduln führt zum Begriff der I-Teilungspunkte, und die in Abschnitt 4 vorgestellten Ergebnisse von *Drinfeld* ergeben eine wichtige Analogie zu den n-Teilungspunkten von elliptischen Kurven.

Wird die die elliptische Kurve definierende Gleichung modulo p betrachtet, entsteht in natürlicher Weise eine über dem endlichen Körper $\mathbf{F}_p$ definierte Kurve. Ein fundamentales Ergebnis dieses Reduktionsprozesses ist, daß fast alle entstehenden Kurven selbst wieder glatt sind. Dieses Verhalten zeigen auch die Drinfeld-Moduln, die ebenfalls außerhalb einer endlichen Menge ein gutes Reduktionsverhalten haben.

Die Formulierung und der Beweis dieser Analogie bilden das eigentliche Ziel der Arbeit. Für den Beweis des oben beschriebenen Sachverhalts werden in den Abschnitten 5-8 die nötigen Vorleistungen erbracht und zwei wichtige Techniken vorgestellt:
Die Theorie der *Hochschildhomologie* liefert Ergebnisse für *relative* Situationen. So ist beispielweise jeder R-Modul einer k-Algebra selbst in natürlicher Weise ein k-Modul. Mit Hilfe der Hochschildhomologie lassen sich einige wichtige Invarianten von k-Algebren beschreiben, und für die Zwecke dieser Arbeit ist vor allem der Zusammenhang der Hochschildhomologie mit *glatten* Algebren von Bedeutung.
Die *Deformationstheorie* bildet mit der Untersuchung von Fortsetzungen ein wichtiges Werkzeug zum Studium algebraischer Strukturen. Zunächst werden Strukturen über ‚einfachen' Objekten, z.B. endlichen Körpern untersucht, und dann die entsprechenden Ergebnisse auf ‚schwierigere' Objekte übertragen. In der Darstellungstheorie sieht das beispielsweise so aus:
Sei G Gruppe, $(R, \mathfrak{m})$ ein lokaler Ring und $k := R/\mathfrak{m}$. Sei $\varrho : G \longrightarrow \mathrm{GL}_n(k)$

eine Darstellung von G. Dies ergibt ein Diagramm:

$$\begin{tikzcd}
G \arrow[r, dashed, "?"] \arrow[dr, "\varrho"'] & \mathrm{GL}_n(R) \arrow[d, "\mathrm{mod}\,\mathfrak{m}"] \\
& \mathrm{GL}_n(k)
\end{tikzcd}$$

Gibt es solche Liftungen und wie sehen sie aus?
Einen Ansatz zur Lösung dieses Problems bildet die *Deformationstheorie*. Der ‚Abstand' zwischen k und R wird möglichst klein gewählt und das Liftungsproblem für lokale Ringe mit $\mathfrak{m}^2 = 0$ betrachtet.
Die *Deformationstheorie* wird in der vorliegenden Arbeit bei der Berechnung der Deformationen eines Drinfeld-Moduls eingesetzt. Das Ergebnis liefert einen engen Zusammenhang mit den Hochschildcohomologiegruppen.
Mit den beiden Theorien läßt sich jetzt die oben beschriebene fundamentale Analogie beweisen. Dies bildet den Abschluß der Arbeit.

2 Glatte Kurven in Charakteristik p

Eine sehr schöne Beziehung zwischen geometrischen und algebraischen Aspekten bildet der Begriff der Glattheit einer Kurve X. Auf der einen Seite steht die Rangbedingung an die Funktionalmatrix der Kurve im Punkt x, auf der anderen Seite die Bedingung an den lokalen Ring $\mathcal{O}_x$, im Punkt x ein diskreter Bewertungsring zu sein. Ist X eine projektive, zusammenhängende, glatte Kurve über dem endlichen Körper $\mathbf{F}_p$, dann lassen sich die abgeschlossenen Punkte von X als Bewertungen des Funktionenkörpers interpretieren. Insbesondere wird dadurch X den Methoden der Bewertungstheorie von Körpern zugänglich.

2.1 Bezeichnungen

Sei p Primzahl, X eine projektive, zusammenhängende, glatte Kurve über dem endlichen Körper $\mathbf{F}_p$. Sei η der generische Punkt von X, d.h. $\overline{\eta} = X$. Ist $F := \kappa(\eta)$ der Funktionenkörper von X, dann ist $F/\mathbf{F}_p$ endlich erzeugte Körpererweiterung vom Transzendenzgrad 1. Ist $\Omega_F := \{$*Menge der abgeschlossenen Punkte von*
so entsprechen die Elemente von Ω_F genau den normierten (diskreten) Bewertungen des Körpers F. Dies gibt Anlaß zu folgenden Notationen und Definitionen:

$\Omega_F \ni x : F \setminus \{0\} \longrightarrow \mathbb{Z}$ normierte, diskrete Bewertung auf F.

$\mathcal{O}_x$ Bewertungsring von x in F.

$\kappa(x) := \mathcal{O}_x/\mathfrak{p}_x$ Residuenkörper von x.

$\deg(x) := \dim_{\mathbf{F}_p} \kappa(x)$ Dimension des Residuenkörpers über $\mathbf{F}_p$.

2.2 Dedekindringe zu glatten Kurven in Charakteristik p

Sei $\infty \in X$ ein beliebiger abgeschlossener Punkt. Dann ist die offene Teilmenge $X \setminus \{\infty\}$ eine affine, glatte Kurve und identifiziert sich mit dem Spektrum eines eindimensionalen, noetherschen Integritätsringes A. Der Ring der regulären Funktionen auf $\operatorname{Spec}(A)$ ist wieder A [Har77, II, Prop. 2.2] und läßt sich mit Hilfe der Bewertungen folgendermaßen beschreiben:

$$\begin{aligned} A &= \bigcap_{x \neq \infty} \mathcal{O}_x \\ &= \{a \in F \mid x(a) \geq \mathit{0} \text{ \textit{für alle} } x \neq \infty\} \end{aligned}$$

Wunderbarerweise ist A nun sogar ein Dedekindring:

Theorem 2.1. *Sei A Ring der regulären Funktionen der affinen Kurve $X \setminus \{\infty\}$. Dann gilt:*

a) A ist ein Dedekindring.

b) A ist ein endlich erzeugter (damit freier) $\mathbf{F}_p[T]$-Modul

Beweis. Nach dem Satz von *Riemann-Roch* [Har77, Chapter IV] gibt es ein $T \in A$ mit $\infty(T) < 0$. Dann ist T notwendigerweise transzendent über $\mathbf{F}_p$ und $\mathbf{F}_p[T]$ ein Polynomring. Es ergibt sich folgendes Diagramm:

(2.1.1)
$$\begin{tikzcd} \mathbf{F}_p \arrow[r, hook, "\text{trgrad } 1"] & \mathbf{F}_p(T) \arrow[r, hook, "\text{endl. alg.}"] & F \\ & \mathbf{F}_p[T] \arrow[u, hook] \arrow[r, hook, "\text{ganzer}", "\text{Abschluß}"'] & A \arrow[u, hook] \end{tikzcd}$$

Insbesondere ist A als Schnitt über alle diskreten Bewertungsringe die $\mathbf{F}_p[T]$ enthalten der ganze Abschluß von $\mathbf{F}_p[T]$ in F [Mat80, §10 Theorem 10.4]. $\mathbf{F}_p[T]$ ist eine endlich erzeugte $\mathbf{F}_p$-Algebra und $F/\mathbf{F}_p(T)$ eine endlich algebraische Körpererweiterung. Daher ist nach einem Theorem von Emmy

Noether [Eis95, Theorem 4.14] der ganze Abschluß von $\mathbf{F}_p[T]$ in F ein endlich erzeugter (sogar freier) $\mathbf{F}_p[T]$-Modul und erbt damit die Dedekindeigenschaft von $\mathbf{F}_p[T]$. Siehe hierzu [Ser79, I §4 Prop. 8]. $\square$

In Analogie zu den algebraischen Zahlkörpern erfüllen die Bewertungen von F eine Geschlossenheitsrelation:

Satz 2.2. *Es gelten folgende Formeln:*

a) Für alle $a \in F \setminus \{0\}$ gilt:

$$\sum_{x \in \Omega_F} \deg(x) x(a) = 0 \tag{2.2.1}$$

b) Für alle $a \in A \setminus \{0\}$ gilt:

$$\deg(\infty)\infty(a) = -\dim_{\mathbf{F}_p} A/(a) \tag{2.2.2}$$

Beweis zu a). Fall 1. $\mathbf{F} = \mathbf{F_p}(\mathbf{T})$.
Sei Ω die Menge der diskreten, normierten Bewertungen von $\mathbf{F}_p(T)$. Diese entsprechen genau den normierten, irreduziblen Polynomen in $\mathbf{F}_p[T]$ und dem Negativen der Gradfunktion. Ist $y \in \Omega' := \Omega \setminus \{-\operatorname{grad}\}$ und p_y das zu y gehörige irreduzible Polynom, dann ist $\deg(y) = \dim_{\mathbf{F}_p} \mathbf{F}_p[T]/(p_y) = \operatorname{grad}(p_y)$. Für die Gradfunktion ist $\deg(-\operatorname{grad}) = 1$.
Da $y(p/q) = y(p) - y(q)$ ist, reicht es, die Behauptung für den Polynomring $\mathbf{F}_p[T]$ zu testen.
Sei $p \in \mathbf{F}_p[T]$ ein beliebiges Polynom, dann besitzt p eine eindeutige Zerlegung in Primfaktoren: $p = p_{y_1}^{e_1} \cdot \ldots \cdot p_{y_r}^{e_r}$. Es folgt:

$$\begin{aligned} \sum_{y \in \Omega'} \deg(y) y(p) &= \sum_{p_{y_i} | p} \operatorname{grad}(p_i) e_i \\ &= \operatorname{grad}(p) \end{aligned}$$

Fall 2. $\mathbf{F}/\mathbf{F_p}(\mathbf{T})$ **endliche, algebraische Körpererweiterung.**
Ist $x \in \Omega_F$, dann ist $x|_{\mathbf{F}_p(T)}$ eine (i. allg. nicht normierte) Bewertung von $\mathbf{F}_p(T)$. Insbesondere gibt es ein $y \in \Omega$ und eine natürliche Zahl e_x mit $x|_{\mathbf{F}_p(T)} = e_x y$. Die Bewertung x heißt *Fortsetzung* von y nach F. Die Fortsetzungen von y werden auch kurz mit $x|y$ bezeichnet.
Sei $N_{F/K} : F \longrightarrow K$ die Normabbildung und F_x bzw. K_y die Komplettierungen bezüglich x und y. Es gelten die Beziehungen (siehe [Ser79, II §2, §3]):

1. $\deg(x)x(a) = \deg(y)y(N_{F_x/K_y}(a))$

2. $N_{F/K}(a) = \prod_{x|y} N_{F_x/K_y}(a)$

Hieraus folgt:

$$\begin{aligned}
\sum_{x\in\Omega_F} \deg(x)x(a) &= \sum_{y\in\Omega}\sum_{x|y} \deg(x)x(a) \\
&= \sum_{y\in\Omega}\sum_{x|y} \deg(y)y(N_{F_x/K_y}(a)) \\
&= \sum_{y\in\Omega} \deg(y)y(N_{F/K}(a)) \\
&= 0 \quad \text{nach Fall 1.}
\end{aligned}$$

□

Beweis zu b). Sei $\Omega'_F := \Omega_F \setminus \{\infty\}$ und für jedes $x \in \Omega'_F$ sei $\mathfrak{p}_x$ das zu x gehörgige Primideal in A. Ist $a \in A$, $a \neq 0$ beliebig, dann hat das von a erzeugte Ideal (a) eine eindeutige Zerlegung:

$$(a) = \prod_{\mathfrak{p}_x|(a)} \mathfrak{p}_x^{x(a)}$$

Nach dem *Chinesischen Restsatz* gilt dann:

$$A/(a) \cong \prod_{\mathfrak{p}_x|(a)} A/\mathfrak{p}_x^{x(a)} \tag{2.2.3}$$

Zur Berechnung von $\dim_{\mathbf{F}_p} A/\mathfrak{p}_x^{x(a)}$ wird nun das folgende Lemma benötigt:

Lemma 2.3. Sei A ein Dedekindring und $\mathfrak{p}$ ein maximales Ideal in A. Für alle $i \geq 0$ gilt:

$$\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong A/\mathfrak{p}$$

Beweis. Sei $a \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ und $\mathfrak{a} := (a) + \mathfrak{p}^{i+1}$. Es folgt:

$$\begin{aligned}
& \mathfrak{p}^i \supseteq \mathfrak{a} \supsetneq \mathfrak{p}^{i+1} \\
\Rightarrow\quad & A \supseteq \mathfrak{a}\mathfrak{p}^{-i} \supsetneq \mathfrak{p} \\
\Rightarrow\quad & \mathfrak{a}\mathfrak{p}^{-i} \text{ ist echter Teiler von } \mathfrak{p} \\
\Rightarrow\quad & \mathfrak{a}\mathfrak{p}^{-i} = A \\
\Rightarrow\quad & \mathfrak{a} = \mathfrak{p}^i
\end{aligned}$$

Der $A/\mathfrak{p}$-Vektorraum $\mathfrak{p}^i/\mathfrak{p}^{i+1}$ wird vom Element a erzeugt. a ist damit eine Basis des Vektoraumes und induziert eine Isomorphie $\mathfrak{p}^i/\mathfrak{p}^{i+1} \cong A/\mathfrak{p}$ □

Mit Hilfe des Lemmas lassen sich jetzt die Dimensionen der $\mathbf{F}_p$-Vektorräume $A/\mathfrak{p}^i$ berechnen. Aus den exakten Sequenzen:

$$0 \longrightarrow \mathfrak{p}^{i-1}/\mathfrak{p}^i \longrightarrow A/\mathfrak{p}^i \longrightarrow A/\mathfrak{p}^{i-1} \longrightarrow 0 \quad \text{für } i > 0$$

ergibt sich für $x(a) > 0$:

$$\begin{aligned}
\dim_{\mathbf{F}_p} A/\mathfrak{p}_x^{x(a)} &= \dim_{\mathbf{F}_p} \mathfrak{p}_x^{x(a)-1}/\mathfrak{p}_x^{x(a)} + \dim_{\mathbf{F}_p} A/\mathfrak{p}_x^{x(a)-1} \\
&= \dim_{\mathbf{F}_p} A/\mathfrak{p}_x + \dim_{\mathbf{F}_p} A/\mathfrak{p}_x^{x(a)-1} \\
&\vdots \\
&= x(a) \deg(x)
\end{aligned}$$

Die Zerlegung von $A/(a)$ nach dem Chinesischen Restsatz (2.2.3) gilt insbesondere auch für den $\mathbf{F}_p$-Vektorraum $A/(a)$ und es folgt:

$$\begin{aligned}
\dim_{\mathbf{F}_p} A/(a) &= \sum_{\mathfrak{p}_x | (a)} x(a) \deg(x) \\
&= \sum_{x \in \Omega'_X} x(a) \deg(x) \quad \text{da } x(a) = 0 \text{ für } \mathfrak{p}_x \nmid (a)
\end{aligned}$$

Mit Teil a) folgt nun die Behauptung. □

Endgültig angelangt bei den Verwirrungen der Verzweigungstheorie sei der interessierte Leser bzw. die interessierte Leserin für weitere Ergebnisse an die Bücher von J.P. Serre [Ser79] und J. Neukirch [Neu92] verwiesen.

3 Gruppenschemata

Eine der auf den ersten Blick überraschensten Eigenschaften von elliptischen Kurven, d.h. Nullstellenmengen von Gleichungen der Form

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

ist die Existenz einer Gruppenstruktur. Nach Wahl eines „Nullpunktes“ wird die Addition zweier Punkte durch Bildung von Sekanten und Spiegelungen gegeben.
Durch die Verallgemeinerung von affinen und projektiven Nullstellenmengen (Varietäten) auf den Begriff des Schemas wird auch die Gruppenstruktur z.B einer elliptischen Kurve auf das zugehörige Schema transportiert. Im günstigsten Fall von algebraisch abgeschlossenen Körpern entsprechen die Punkte

einer affinen, elliptischen Kurve genau den maximalen Idealen des Koordinatenringes und die Gruppenstruktur wird einfach auf das Spektrum übertragen. Doch was passiert mit dem Nullideal? Was passiert im Falle eines nicht algebraisch abgeschlossenen Grundkörpers und wie sehen Gruppenstrukturen auf höherdimensionalen Ringen aus, in denen nicht abgeschlossenen Primideale auftreten?
Der folgende Abschnitt schafft die begrifflichen Grundlagen für die Beschreibung von Gruppenstrukturen auf Schemata und um es gleich ordentlich zu machen, wird auch der Grundkörper durch ein Basisschema ersetzt.

3.1 Die Kategorie **Sch**/S

Sei im folgenden S beliebiges Schema und $\Gamma(\,\_\,)$ der globale Schnittfunktor.

Definition 3.1. X heißt Schema über S oder S-Schema falls X Schema ist und es einen Morphismus von Schemata: $X \xrightarrow{\pi} S$ gibt. Ein Morphismus von S-Schemata ist ein Morphismus $X \longrightarrow Y$, so daß das Diagramm

(3.1.1)
$$\begin{tikzcd} X \arrow[rr] \arrow[dr, "\pi"'] & & Y \arrow[dl, "\tilde{\pi}"] \\ & S & \end{tikzcd}$$

kommutiert. Die Menge der S-Morphismen wird mit $\mathrm{Hom}_S(X, Y)$ bezeichnet. Der Funktor $\mathrm{Hom}_S(\,\_\,, X)$ heißt *Funktor der Punkte von X*. Ist R kommutativer Ring und $S = \mathrm{Spec}(R)$ so heißt X auch kurz R-Schema. Die Schemata über S bilden zusammen mit obigen Morphismen die Kategorie **Sch**/S.

Im Falle von affinen Schemata lassen sich mit Hilfe des folgenden Satzes die Morphismen genau beschreiben.

Satz 3.2. *Ist $X = \mathrm{Spec}(R)$ ein affines Schema und Y ein beliebiges Schema, so gilt:*
$$\mathrm{Hom}(Y, X) \cong \mathrm{Hom}_{Ring}(R, \Gamma(Y))$$

Beweis. siehe [Eis90, Theorem I-36] □

Folgerung 3.3. *Jedes Schema ist ein $\mathbb{Z}$-Schema. Insbesondere ist*
$$\mathrm{Hom}(X, Y) = \mathrm{Hom}_{\mathbb{Z}}(X, Y)$$

Beweis. Für jeden kommutativen Ring R gibt es genau einen Ringhomomorphismus $\mathbb{Z} \longrightarrow R$. Ist $R = \Gamma(X)$, so gibt es nach obigem Satz einen eindeutig bestimmten Morphismus $X \longrightarrow \mathrm{Spec}(\mathbb{Z})$. □

Eine der wichtigsten Eigenschaften von **Sch**$/S$ ist die Existenz von beliebigen Faserprodukten. Durch die beiden folgenden Beispiele soll die Bedeutung der Faserprodukte angedeutet werden, aber auch für die Definition der Gruppenschemata sind Faserprodukte eine unerläßliche Voraussetzung.

Satz 3.4 (Faserprodukte). *Seien X, Y S-Schemata. Dann gibt es ein Faserprodukt von X und Y über S:*

$$\begin{array}{ccc} X \times_S Y & \xrightarrow{p_1} & X \\ {\scriptstyle p_2}\downarrow & & \downarrow \\ Y & \longrightarrow & S \end{array}$$

mit der universellen Eigenschaft:
Ist Z ein S-Schema und $f : Z \longrightarrow X$, $g : Z \longrightarrow Y$ gegeben, dann gibt es genau einen Morphismus $Z \longrightarrow X \times_S Y$, so daß das Diagramm

(3.4.1)
$$\begin{tikzcd} Z \arrow[dr] \arrow[drr, bend left, "f"] \arrow[ddr, bend right, "g"'] & & \\ & X \times_S Y \arrow[r, "p_1"] \arrow[d, "p_2"] & X \arrow[d] \\ & Y \arrow[r] & S \end{tikzcd}$$

kommutiert.

Beweis. Für $X = \operatorname{Spec}(R_1)$, $Y = \operatorname{Spec}(R_2)$, $S = \operatorname{Spec}(k)$ ist $X \times_S Y = \operatorname{Spec}(R_1 \otimes_k R_2)$. Für den allgemeinen Fall siehe [Har77] oder [Eis90]. $\square$

Beispiel 3.5. Ist $s \in S$, $\kappa(s) := \mathcal{O}_{S,s}/\mathfrak{m}_{S,s}$ Residuenkörper in s und $Y = \{s\} := \operatorname{Spec}(\kappa(s))$ Unterschema von S, so heißt das Faserprodukt $X_s := X \times_S \{s\}$ Faser von X über s und ist insbesondere ein $\kappa(s)$-Schema.

Beispiel 3.6. Ist $\mathrm{id} : X \longrightarrow X$, so ergibt sich nach Satz 3.4 ein eindeutiger Morphismus

$$\delta_X : X \longrightarrow X \times_S X$$

δ_X heißt *Diagonalmorphismus.*

Für die moderne Formulierung der algebraischen Geometrie ist das Studium der Kategorie **Sch**$/S$ von grundlegender Bedeutung. Eine Einführung in die Sprache der Schemata findet sich im sehr gut lesbaren Buch von David Eisenbud [Eis90].

3.2 Gruppenstrukturen auf Schemata

Definition 3.7 (Gruppenschema). Ein Gruppenschema G über S ist ein S-Schema mit S-Morphismen:

$$\sigma : S \longrightarrow G \quad i : G \longrightarrow G \quad \mu : G \times_S G \longrightarrow G$$

so daß die folgenden Diagramme kommutieren:

i) *Neutrales Element*

$$\begin{tikzcd} & G \times_S G \arrow[d, "\mu"] \\ S \times_S G \arrow[ur, "\sigma \times \mathrm{id}"] \arrow[r, "p_2"] & G \end{tikzcd} \qquad \begin{tikzcd} & G \times_S G \arrow[d, "\mu"] \\ G \times_S S \arrow[ur, "\mathrm{id} \times \sigma"] \arrow[r, "p_1"] & G \end{tikzcd}$$

ii) *inverses Element*

$$\begin{tikzcd} G \times_S G \arrow[rr, "\mathrm{id} \times i"] & & G \times_S G \arrow[d, "\mu"] \\ G \arrow[u, "\delta_G"] \arrow[r, "\pi"] & S \arrow[r, "\sigma"] & G \end{tikzcd} \quad \begin{tikzcd} G \times_S G \arrow[rr, "i \times \mathrm{id}"] & & G \times_S G \arrow[d, "\mu"] \\ G \arrow[u, "\delta_G"] \arrow[r, "\pi"] & S \arrow[r, "\sigma"] & G \end{tikzcd}$$

iii) *assoziativ*

$$\begin{tikzcd} G \times_S G \times_S G \arrow[r, "\mu \times \mathrm{id}"] \arrow[d, "\mathrm{id} \times \mu"'] & G \times_S G \arrow[d, "\mu"] \\ G \times_S G \arrow[r, "\mu"] & G \end{tikzcd}$$

Gilt zusätzlich:

iv) *kommutativ*

$$\begin{tikzcd} G \times_S G \arrow[r, "p_2 \times p_1"] \arrow[d, "\mu"'] & G \times_S G \arrow[d, "\mu"] \\ G \arrow[r, "\mathrm{id}"] & G \end{tikzcd}$$

So heißt G ein *abelsches* Gruppenschema über S.

Definition 3.8 (Morphismen von Gruppenschemata). Seien G_1, G_2 Gruppenschemata über S. Ein S-Morphismus $f : G_1 \longrightarrow G_2$ heißt Morphismus von Gruppenschemata über S, falls das folgende Diagramm kommutiert:

$$\begin{tikzcd} G_1 \times_S G_1 \arrow[r, "f \times f"] \arrow[d, "\mu_1"'] & G_2 \times_S G_2 \arrow[d, "\mu_2"] \\ G_1 \arrow[r, "f"] & G_2 \end{tikzcd}$$

Definition 3.9. Sei G abelsches Gruppenschema über S.

$$\mathrm{End}_S(G) := \{f \in \mathrm{Hom}_S(G, G) \mid f \text{ ist Morphismus von Guppenschemata}\}$$

heißt *Endomorphismenring* von G. Die additive Struktur ist wie folgt gegeben:
Sind $f, g \in \mathrm{End}_S(G)$, dann ist $f * g$ gegeben durch:

$$\begin{tikzcd} G \times_S G \arrow[r, "f \times g"] & G \times_S G \arrow[d, "\mu"] \\ G \arrow[u, "\delta_G"] \arrow[r, dashed, "f * g"] & G \end{tikzcd}$$

Als Nullelement fungiert $G \xrightarrow{\sigma\pi} G$ und als Inverses der Addition $G \xrightarrow{i} G$. Die multiplikative Struktur liefert wie gewöhnlich die Komposition von Morphismen. Eine genauere Beschreibung des Endomorphismenrings im Falle $G = \mathbf{G}_{a/k}$ (Bsp 3.10) findet sich in Abschnitt 3.

Nach diesen trockenen Definitionen dienen die beiden folgenden Beispiele der Anschauung und sind für die weiteren Kapitel grundlegend.

Beispiel 3.10 (Additives Gruppenschema). Sei $\mathbf{G}_a := \mathrm{Spec}(\mathbb{Z}[T])$. $\mathbf{G}_a$ ist ein abelsches Gruppenschema durch:

$\boldsymbol{\sigma}$ **:** Der durch den Ringhomomorphismus

$$\begin{aligned} \mathbb{Z}[T] &\longrightarrow \mathbb{Z} \\ T &\longmapsto 0 \end{aligned}$$

induzierte Morphismus $\mathrm{Spec}(\mathbb{Z}) \xrightarrow{\sigma} \mathbf{G}_a$.

$\boldsymbol{\mu}$ **:** Der durch den Ringhomomorphismus

$$\begin{aligned} \mathbb{Z}[T] &\longrightarrow \mathbb{Z}[T_1, T_2] \\ T &\longmapsto T_1 + T_2 \end{aligned}$$

induzierte Morphismus $\mathrm{Spec}(\mathbb{Z}[T] \bigotimes_{\mathbb{Z}} \mathbb{Z}[T]) = \mathbf{G}_a \times_{\mathbb{Z}} \mathbf{G}_a \xrightarrow{\mu} \mathbf{G}_a$.

i : Der durch den Ringhomomorphismus

$$\begin{aligned} \mathbb{Z}[T] &\longrightarrow \mathbb{Z}[T] \\ T &\longmapsto -T \end{aligned}$$

induzierte Morphismus $\mathbf{G}_a \xrightarrow{i} \mathbf{G}_a$.

Für ein beliebiges Schema S wird das *additive Gruppenschema* über S definiert durch: $\mathbb{G}_{a/S} := \mathbf{G}_a \times_{\mathbb{Z}} S$. Für $S = \operatorname{Spec}(R)$ ist $\mathbb{G}_{a/R} = \operatorname{Spec}(R[T])$.

Beispiel 3.11 (Konstantes Gruppenschema). Sei M endliche Gruppe und $\mathbf{Z}[M]$ die Gruppenalgebra über $\mathbb{Z}$. $\operatorname{Hom}_{\mathbb{Z}}(\mathbb{Z}[M], \mathbb{Z})$ ist dann ein kommutativer Ring, isomorph zu

$$\underbrace{\mathbb{Z} \times \cdots \times \mathbf{Z}}_{|M|-\text{Stück}} := \mathbf{Z}^M$$

mit kanonischer Basis $\varepsilon_m := (0, \dots, 1_m, \dots, 0)$.
$M_{\mathbf{Z}} := \operatorname{Spec}(\mathbf{Z}^M)$ wird ein Gruppenschema über $\mathbf{Z}$ durch:

σ : Der durch den Ringhomomorphismus

$$\begin{aligned} \mathbf{Z}^M &\longrightarrow \mathbf{Z} \\ (\alpha_m) &\longmapsto \alpha_e \quad e \text{ neutrales Element in } M \end{aligned}$$

induzierte Morphismus $\operatorname{Spec}(\mathbf{Z}) \xrightarrow{\sigma} M_{\mathbf{Z}}$.

μ : Der durch den Ringhomomorphismus

$$\begin{aligned} \mathbf{Z}^M &\longrightarrow \mathbf{Z}^M \otimes_{\mathbf{Z}} \mathbf{Z}^M \\ \varepsilon_m &\longmapsto \sum_{n \in M} \varepsilon_{mn^{-1}} \otimes \varepsilon_n \end{aligned}$$

induzierte Morphismus $M_{\mathbf{Z}} \times_{\mathbf{Z}} M_{\mathbf{Z}} \xrightarrow{\mu} M_{\mathbf{Z}}$.

i : Der durch den Ringhomomorphismus

$$\begin{aligned} \mathbf{Z}^M &\longrightarrow \mathbf{Z}^M \\ (\alpha_m) &\longmapsto (\alpha_{m^{-1}}) \end{aligned}$$

induzierte Morphismus $M_{\mathbf{Z}} \xrightarrow{i} M_{\mathbf{Z}}$

Ist M sogar abelsche Gruppe, so ist $M_{\mathbf{Z}}$ abelsches Gruppenschema. Für ein beliebiges Schema S wird das *konstante Gruppenschema* über S definiert durch:

$$M_S := M_{\mathbf{Z}} \times_{\mathbf{Z}} S$$

3.3 Alternative Definition von Gruppenschemata

Eine kompakte Beschreibung der Gruppenschemata bietet die folgende, alternative Definition. Beide Definitionen werden im weiteren gleichberechtigt nebeneinander verwendet.

Definition 3.12 (Alternativ). Sei $\mathcal{E} : \mathbf{Sch}/S \longrightarrow \mathbf{Men}$ ein kovarianter Funktor. $\mathcal{E}$ heißt *Gruppenschema* falls:

1. $\mathcal{E}$ faktorisiert über $\mathbf{Ab}$, d.h.:

$$\begin{tikzcd} \mathbf{Sch}/S \arrow[rr, "\mathcal{E}"] \arrow[dr] & & \mathbf{Men} \\ & \mathbf{Ab} \arrow[ur, "\mathcal{V}"'] & \end{tikzcd}$$

   wobei $\mathcal{V}$ der *Vergißfunktor* ist.

2. $\mathcal{E}$ ist darstellbar, d.h. es gibt ein Schema E/S, mit $\mathcal{E} \cong \mathrm{Hom}_S(\_\,, E)$.

Also ist $\mathcal{E}(X)$ eine abelsche Gruppe für alle Schemata X/S und für $f \in \mathrm{Hom}_S(X, Y)$ ist $\mathcal{E}(Y) \longrightarrow \mathcal{E}(X)$ ein Gruppenhomomorphismus.

Bemerkung 3.13 (Zusammenhang der beiden Definitionen).

- Ist E ein Gruppenschema, und $\mathcal{E} := \mathrm{Hom}_S(\_\,, E)$. Ist dann X/S ein Schema, und sind ϕ, $\psi \in \mathrm{Hom}_S(X, E)$, so ist die Gruppenstruktur $\phi * \psi$ auf $\mathrm{Hom}_S(X, E)$ gegeben durch Komposition der Morphismen:

(3.13.1)
$$\begin{tikzcd} X \times_S X \arrow[r, "\phi \times \psi"] & E \times_S E \arrow[d, "\mu"] \\ X \arrow[u, "\delta_X"] \arrow[r, dashed, "\phi * \psi"] & E \end{tikzcd}$$

- Ist das Gruppenschema als Funktor $\mathcal{E}$ gegeben und E/S ein darstellendes Objekt, so finden sich μ, σ, i wie folgt:

  1. Sind $p_1, p_2 \in \mathrm{Hom}_S(E \times_S E, E)$ die kanonischen Projektionen, so setze
     $\mu := p_1 + p_2$.
  2. σ wird definiert als neutrales Element in $\mathrm{Hom}_S(S, E)$.
  3. Ist $\mathrm{id} \in \mathrm{Hom}_S(E, E)$, so $i := -\mathrm{id}$.

Beispiel 3.14. Als Funktoren lassen sich nun das *additive* und das *konstante* Gruppenschema sehr einfach beschreiben:

$$\begin{aligned} \mathbf{G}_a : \mathbf{Sch}/S &\longrightarrow \mathbf{Ab} \\ X &\longmapsto (\Gamma(X), +) \end{aligned}$$

Darstellendes Objekt ist $S \times_{\mathrm{Spec}(\mathbb{Z})} \mathrm{Spec}(\mathbb{Z}[T])$.

Ist M beliebige abelsche Gruppe.

$$\begin{aligned} M_S : \mathbf{Sch}/S &\longrightarrow \mathbf{Ab} \\ X &\longmapsto M \end{aligned}$$

Darstellendes Objekt ist $S \times_{\mathrm{Spec}(\mathbf{Z})} \mathrm{Spec}(\mathbb{Z}^M)$.

Auch das Konzept von Faserprodukten läßt sich auf Funktoren übertragen:

Definition 3.15 (Faserprodukte von Funktoren). Sei $\mathcal{S} := \mathrm{Hom}_S(\_\,, S)$ und $\mathcal{F}, \mathcal{G} : \mathbf{Sch}/S \longrightarrow \mathbf{Men}$ kontravariante Funktoren und $\mathcal{F} \longrightarrow \mathcal{S}$ bzw. $\mathcal{G} \longrightarrow \mathcal{S}$ natürliche Transformationen, so wird $(\mathcal{F} \times_S \mathcal{G})(X) := \mathcal{F}(X) \times_{\mathcal{S}(X)} \mathcal{G}(X)$

Satz 3.4 auf Seite 12 liest sich dann wie folgt:
Sind $\mathcal{F} = \mathrm{Hom}_S(\_\,, X)$ und $\mathcal{G} = \mathrm{Hom}_S(\_\,, Y)$ darstellbare Funktoren, dann ist auch $\mathcal{F} \times_S \mathcal{G}$ darstellbar durch das Schema $X \times_S Y$.

4 Der Endomorphismenring von $\mathbf{G}_{a/k}$

Wie im letzten Abschnitt versprochen, folgt nun die Berechnung des Endomorphismenringes für ein additives Gruppenschema über einem kommutativen Ring.

4.1 Additive Polynome

Sei k kommutativer Ring und $\mathbf{G}_{a/k} = \mathrm{Spec}(k[T])$ das additive Gruppenschema über k.
Ist $f \in \mathrm{Hom}_k(\mathbf{G}_{a/k}, \mathbf{G}_{a/k})$ so ist f gegeben durch einen k-Algebren-Homomorphismus

$$\begin{aligned} k[T] &\longrightarrow k[T] \\ T &\longrightarrow F \end{aligned}$$

Der Einfachheit halber sei dieser ebenfalls mit F bezeichnet.
Ist $f \in \mathrm{Hom}_k(\mathbf{G}_{a/k}, \mathbf{G}_{a/k})$, dann ist nach Definition 3.9 auf Seite 14

$f \in \mathrm{End}_k(\mathbf{G}_{a/k})$, falls f mit der Gruppenstruktur verträglich ist. Dies heißt explizit:

$$f \in \mathrm{End}_k(\mathbf{G}_{a/k}) \quad \Longleftrightarrow \quad f \circ \mu = \mu \circ (f \times_k f)$$

Mit Hilfe des Funktors Γ folgt:

$$\begin{tikzcd} \mathbf{G}_{a/k} \times_S \mathbf{G}_{a/k} \arrow[r, "f \times f"] \arrow[d, "\mu"'] & \mathbf{G}_{a/k} \times_S \mathbf{G}_{a/k} \arrow[d, "\mu"] \\ \mathbf{G}_{a/k} \arrow[r, "f"] & \mathbf{G}_{a/k} \end{tikzcd} \quad \xrightarrow{\Gamma} \quad \begin{tikzcd} k[T] \arrow[r, "\Gamma(\mu)"] \arrow[d, "F"'] & k[T_1, T_2] \arrow[d, "F \otimes_k F"] \\ k[T] \arrow[r, "\Gamma(\mu)"] & k[T_1, T_2] \end{tikzcd}$$

Aus dem Diagramm folgt:

$$\begin{aligned} (F \otimes_k F) \circ \Gamma(\mu)(T) &= (F \otimes_k F)(T_1 + T_2) \\ &= F(T_1) + F(T_2) \\ &\overset{!}{=} F(T_1 + T_2) \\ &= \Gamma(\mu) \circ F(T) \end{aligned}$$

Das heißt: $f \, \mathrm{End}_k(\mathbf{G}_{a/k}) \Longleftrightarrow F(T_1) + F(T_2) = F(T_1 + T_2)$.

Definition 4.1. Ein Polynom $F \in k[T]$ heißt *additiv*, falls $F(T_1) + F(T_2) = F(T_1 + T_2)$.

Folgerung 4.2. $f \in \mathrm{End}_k(\mathbf{G}_{a/k}) \Longleftrightarrow F$ *ist additives Polynom.*

Lemma 4.3. Einfach zu zeigen sind die folgenden Eigenschaften additiver Polynome:

a) Sind F, G additive Polynome, so auch $F + G$ und $F \circ G$.

b) $F = T$ ist additives Polynom.

Folgerung 4.4. *Die additiven Polynome bilden einen Ring. Dieser wird mit* $\mathrm{Add}(k[T])$ *bezeichnet.*

Der folgende Satz verknüpft die Struktur des Endomorphismenrings mit den additiven Polynomen.

Satz 4.5. *Es gibt einen kanonischen Isomorphismus von Ringen:*

$$\mathrm{End}_k(\mathbf{G}_{a/k}) \cong \mathrm{Add}(k[T])$$

Beweis. Der Funktor Γ und Folgerung 4.2 auf der vorherigen Seite induzieren einen bijektiven Morphismus von $\mathrm{End}_k(\mathbf{G}_{a/k})$ mit $\mathrm{Add}(k[T])$. Zu zeigen bleibt, daß die durch Γ induzierte Ringstruktur mit der Ringstruktur nach Lemma 4.3 auf der vorherigen Seite übereinstimmt.
Sind also $f, g \in \mathrm{End}_k(\mathbf{G}_{a/k})$, so ist $f * g$ gegeben durch das linke Diagramm analog zu (3.13.1). Anwendung von Γ induziert dann:

$$\begin{tikzcd} \mathbf{G}_{a/k} \times_S \mathbf{G}_{a/k} \arrow[r, "f \times g"] & \mathbf{G}_{a/k} \times_S \mathbf{G}_{a/k} \arrow[d, "\mu"] \\ \mathbf{G}_{a/k} \arrow[u, "\delta_{\mathbf{G}_{a/k}}"] \arrow[r, dashed, "f * g"] & \mathbf{G}_{a/k} \end{tikzcd} \xrightarrow{\quad\Gamma\quad} \begin{tikzcd} k[T_1, T_2] \arrow[d, "\Gamma(\delta_{k[T]})"'] & k[T_1, T_2] \arrow[l, "F \otimes_k G"'] \\ k[T] & k[T] \arrow[l, dashed, "F * G"'] \arrow[u, "\Gamma(\mu)"'] \end{tikzcd}$$

Das bedeutet explizit:

$$T \overset{\Gamma(\mu)}{\longmapsto} T_1 + T_2 \overset{F \otimes_k G}{\longmapsto} F(T_1) + G(T_2) \overset{\Gamma(\delta_{k[T]})}{\longmapsto} F(T) + G(T) \overset{!}{=} (F+G)(T)$$

$F * G$ stimmt also mit der additiven Struktur auf $\mathrm{Add}(k[T])$ überein. Γ ist als Funktor verträglich mit der Komposition von Morphismen und $\Gamma(\mathrm{id}) = T$. $\square$

4.2 Der Schiefpolynomring $k\{\tau\}$

Für $\mathrm{char}(k) = 0$ ist $\mathrm{Add}(k[T]) = \{aT \mid a \in k\} \cong k$ und liefert damit nichts Neues.
Für $\mathrm{char}(k) = p$ mit p Primzahl ist auch T^p nach dem *Satz vom kleinen Moritz*:

$$(T_1 + T_2)^p = T_1^p + T_2^p \quad \text{siehe [tD95, Notiz (5.6)]}$$

ein additives Polynom. Die additiven Polynome lassen sich in diesem Fall durch einen sogenannten Schiefpolynomring beschreiben.

Sei im folgenden k kommutativer Ring mit $\mathrm{char}(k) = p$, p Primzahl. Wird k als $\mathbf{Z}$-Modul aufgefaßt, dann läßt sich auf dem $\mathbf{Z}$-Modul $k \otimes_{\mathbf{Z}} \mathbf{Z}[T]$ eine im allgemeinen nicht kommutative Ringstruktur definierien.

Lemma 4.6. Ist $\tau := 1 \otimes T \in k \otimes_{\mathbf{Z}} \mathbf{Z}[T]$, dann hat jedes $\varphi \in k \otimes_{\mathbf{Z}} \mathbf{Z}[T]$ eine eindeutige Darstellung der Form: $\varphi = \sum_{i=0}^{n} a_i \tau^i$ mit $a_i \in k$.

Beweis. Als $\mathbf{Z}$-Modul ist $\mathbf{Z}[T] \cong \bigoplus_{i=0}^{\infty} \mathbf{Z}$. Da Tensorprodukte mit direkten Summen verträglich sind, folgt:

$$\begin{aligned} k \otimes_{\mathbf{Z}} \mathbf{Z}[T] &\cong k \otimes_{\mathbf{Z}} \bigoplus_{i=0}^{\infty} \mathbf{Z} \\ &\cong \bigoplus_{i=0}^{\infty} k \end{aligned}$$

Insbesondere ist mit $(T^i)_{i\in\mathbf{N}_0}$ als Basis von $\mathbf{Z}[T]$ auch $(\tau^i = 1\otimes T^i)_{i\in\mathbf{N}_0}$ eine Basis von $k\otimes_{\mathbf{Z}}\mathbf{Z}[T]$. □

Das Lemma motiviert die Bezeichnung: $k\{\tau\} := k\otimes_{\mathbf{Z}}\mathbf{Z}[T]$

Satz 4.7. *Auf $k\{\tau\}$ ist eine im allgemeinen nicht kommutative Ringstruktur gegeben durch:*

$$a\tau^i b\tau^j := ab^{p^i}\tau^{i+j} \quad a,b\in k \tag{4.7.1}$$

und die lineare Fortsetzung dieser Vertauschungsrelation auf $k\{\tau\}$.

Beweis. Nicht ganz trivial ist nur das Distributivgesetz:

$$\begin{aligned} a\tau^i(b\tau^j + c\tau^j) &= a\tau^i(b+c)\tau^j \\ &= a(b+c)^{p^i}\tau^{i+j} \\ &= (ab^{p^i} + ac^{p^i})\tau^{i+j} \\ &= ab^{p^i}\tau^{i+j} + ac^{p^i}\tau^{i+j} \\ &= a\tau^i b\tau^j + a\tau^i c\tau^j \quad \text{für alle } a,b,c\in k \end{aligned}$$

□

Die folgende Bemerkung liefert neben der Vertauschungsrelation die grundlegenden Hilfsmittel zur Beschreibung von $k\{\tau\}$.

Bemerkung 4.8.

a) $k\{\tau\}$ ist i. allg. keine k-Algebra, da k nicht im Zentrum von $k\{\tau\}$ liegen muß. Aus $\tau a = a^p\tau$ folgt:
$$k\subseteq \text{Zentrum}(k\{\tau\}) \iff a^p = a \quad \forall a\in k$$

b) Es gibt eine *Gradabbildung*
$$\begin{aligned} \deg : k\{\tau\}\setminus\{0\} &\longrightarrow \mathbf{N} \\ \sum_{n=0}^{N} a_n\tau^n &\longmapsto N \quad (a_N\neq 0) \end{aligned}$$
Für $\varphi,\psi\in k\{\tau\}$ gilt: $\deg(\varphi+\psi)\leq \max(\deg\varphi,\deg\psi)$.
Ist k sogar ein Integritätsring so ist $\deg(\varphi\psi) = \deg\varphi + \deg\psi$.

c) Es gibt einen Ringhomomorphismus
$$\begin{aligned} \partial : k\{\tau\} &\longrightarrow k \\ \sum_{n=0}^{N} a_n\tau^n &\longmapsto a_0 \end{aligned}$$

Wegen diesen Analogien zu Polynomringen wird $k\{\tau\}$ auch als *Schiefpolynomring* bezeichnet.

4.3 $\mathrm{End}_k(\mathbf{G}_{a/k})$ in Primzahlcharakteristik

Sei im folgenden wiederum k kommutativer Ring mit $\mathrm{char}(k) = p$ und p Primzahl.
Das wichtigste Ergebnis des Abschnitts lautet:

Satz 4.9. *Es gibt einen kanonischen Isomorphismus von Ringen:*

$$\mathrm{End}_k(\mathbf{G}_{a/k}) \cong k\{\tau\}$$

Der Beweis des Satzes stützt sich auf die folgenden Lemmata:

Lemma 4.10. Jedes additive Polynom $F \in \mathrm{Add}(k[T])$ ist von der Form:

$$F = \sum_{n=0}^{N} a_n T^{p^n}$$

Beweis. Ist $F = \sum_{n=0}^{N} a_n T^n \in \mathrm{Add}(k[T])$ so gilt:

$$\begin{aligned} & F(T_1) + F(T_2) = F(T_1 + T_2) \\ \Rightarrow \quad & \sum_{n=0}^{N} a_n T_1^n + \sum_{n=0}^{N} a_n T_2^n = \sum_{n=0}^{N} a_n (T_1 + T_2)^n \\ & \qquad = \sum_{n=0}^{N} \sum_{k=0}^{n} a_n \binom{n}{k} T_1^k T_2^{n-k} \end{aligned}$$

Koeffizientenvergleich der beiden Polynome ergibt:

$$F \in \mathrm{Add}(k[T]) \iff a_n \binom{n}{k} = 0 \quad \text{für} \quad \begin{matrix} 0 < k < n \\ 0 \leq n \leq N \end{matrix} \tag{4.10.1}$$

Zu zeigen bleibt also:

$$a_n = 0 \quad \text{für} \quad n \neq p^s$$

□

Dies ergibt sich aus den folgenden beiden Lemmata:

Lemma 4.11. Sei $z \in \mathbf{Z}$, $a \in k$ mit $za = 0$. Dann gilt: $p|z$ oder $a = 0$

Beweis. Annahme: $p \nmid z$. Dann gibt es $n, m \in \mathbb{Z}$ mit $1 = mp + nz$. Es folgt:

$$\begin{aligned} 0 &= mpa + nza \\ &= 1a \\ &= a \end{aligned}$$

□

Lemma 4.12. Sei $N \in \mathbf{N}$, $N > 1$. Sei $\binom{N}{k} \equiv 0 \bmod p$ für $0 < k < N$, dann ist $N = p^s$ für ein $s \in \mathbf{N}$.

Beweis. Aus $\binom{N}{1} = N$ folgt $p|N$ d.h., $N = p^s t$ für $s, t \in \mathbf{N}$ und $(t, p) = 1$. Nach (4.10.1) ist $T^N \in \mathrm{Add}(k[T])$ und es folgt:

$$\begin{aligned} T_1^N + T_2^N &= (T_1 + T_2)^N \\ &= (T_1 + T_2)^{p^s t} \\ &= ((T_1 + T_2)^{p^s})^t \\ &= (T_1^{p^s} + T_2^{p^s})^t \\ &= \sum_{k=0}^{t} \binom{t}{k} T_1^{p^s k} T_2^{p^s (t-k)} \end{aligned}$$

Annahme: $t \neq 1$, dann ergibt der Koeffizientenvergleich:

$$\begin{aligned} &\binom{t}{k} \equiv 0 \bmod p \quad \text{für } 0 < k < t \\ \Rightarrow \quad t = &\binom{t}{1} \equiv 0 \bmod p \end{aligned}$$

im Widerspruch zu $(t, p) = 1$. $\square$

Ende des Beweises zu Lemma 4.10. Ist $a_n \neq 0$, so gilt nach Lemma 4.11 auf der vorherigen Seite

$$\binom{n}{k} \equiv 0 \bmod p \quad \text{für} \quad 0 < k < n$$

Nach Lemma 4.12 ist dann aber $n = p^s$ für ein $s \in \mathbf{N}$ und es folgt die Behauptung. $\square$

Beweis von Satz 4.9. Nach Satz 4.5 auf Seite 18 ist $\mathrm{End}_k(\mathbf{G}_{a/k}) \cong \mathrm{Add}(k[T])$. Zu zeigen ist also, $k\{\tau\} \cong \mathrm{Add}(k[T])$.
Ist $F \in \mathrm{Add}(k[T]$, so hat F nach Lemma 4.10 auf der vorherigen Seite die Gestalt: $F = \sum_{n=0}^{N} a_n T^{p^n}$. Dies legt die Definition des folgenden Morphismus nahe:

$$\begin{aligned} \phi : \mathrm{Add}(k[T]) &\longrightarrow k\{\tau\} \\ \sum_{n=0}^{N} a_n T^{p^n} &\longmapsto \sum_{n=0}^{N} a_n \tau^n \end{aligned}$$

ϕ ist additiv und bijektiv, daher bleibt die Verträglichkeit mit den multiplikativen Strukturen zu zeigen, d.h.:

$$\phi(F \circ G) = \phi(F)\phi(G) \text{ für } F, G \in \mathrm{Add}(k[T])$$

Es reicht, die Bedingung für Monome zu prüfen:

$$\begin{aligned} \phi(aT^{p^n} \circ bT^{p^m}) &= a\tau^n b\tau^m \\ \phi(a(bT^{p^m})^{p^n}) &= \\ \phi(ab^{p^n} T^{p^{n+m}}) &= ab^{p^n}\tau^{n+m} \end{aligned}$$

Dies stimmt mit der Definition der multiplikativen Struktur auf $k\{\tau\}$ überein und ϕ ist als Isomorphismus von Ringen entlarvt. □

5 Drinfeld-Moduln

5.1 Modulstrukturen auf abelschen Gruppenschemata

Eines der wichtigsten Hilfsmittel zur Untersuchung der Struktur einer abelschen Gruppe M ist die Interpretation von M als $\mathbf{Z}$-Modul. Ist M endlich erzeugt, dann ist die Struktur von M nach dem *Hauptsatz über endlich erzeugte abelsche Gruppen* eindeutig festgelegt. Das wesentliche Strukturmerkmal bilden hierbei die p-Torsionspunkte bzw. die torsionsfreien Punkte von M. Dieses Konzept wird nun auf abelsche Gruppenschemata übertragen.
Sei R Ring und M abelsche Gruppe. M ist R-Modul genau dann, falls es einen Ringhomomorphismus $R \longrightarrow \mathrm{End}_{\mathbf{Z}}(M)$ gibt. Diese Beobachtung legt die folgende Definition nahe:

Definition 5.1. Sei E/S abelsches Gruppenschema. E heißt *Schema von R-Moduln* oder kurz ein R-Modul, falls es einen Ringhomomorphismus $R \longrightarrow \mathrm{End}_S(E)$ gibt.

5.2 Drinfeld-Moduln

Sei im folgenden p eine Primzahl, S ein Schema über $\mathbf{F}_p$ und A der Dedekindring aus Abschnitt 2.

Ein Drinfeld-Modul ist ein Spezialfall der Definition 5.1.

Definition 5.2 (Drinfeld-Moduln). Sei $d \in \mathbf{Z}$, $d > 0$. Ein *Drinfeld A-Modul vom Rang d* ist ein Paar (E, φ) mit:

$E \xrightarrow{\pi} S$	$\varphi : A \longrightarrow \mathrm{End}_S(E)$
ist ein abelsches Gruppenschema	Ringhomomorphismus

und den weiteren Daten:

1.) E ist lokal isomorph zu $\mathbf{G}_{a/S}$ bezüglich der Zariskitopologie auf S, d.h.:

   1.a) für alle $s \in S$ gibt es eine offene Umgebung $U(s) \subseteq S$ mit

$$E|_{U(s)} \cong \mathbf{G}_{a/U(s)}$$

   als Gruppenschemata über $U(s)$, wobei $E|_{U(s)} := E|_{\pi^{-1}(U(s))}$ die kanonische Einschränkung von E auf $\pi^{-1}(U(s))$ ist.

   1.b) Sind $U, V \subseteq S$ mit $E|_U \xrightarrow{\psi_1} \mathbf{G}_{a/U}$ und $E|_V \xrightarrow{\psi_2} \mathbf{G}_{a/V}$ Isomorphien und $\mathrm{Spec}(k) \subseteq U \cap V$ offene, affine Teilmenge, so ist $\psi_2\psi_1^{-1}|_{\mathrm{Spec}(k)} \in \mathrm{End}_k(\mathbf{G}_{a/k})$.

2.) Ist $U = \mathrm{Spec}(k)$ offene, affine Teilmenge von S und $E|_U \xrightarrow{\psi} \mathbf{G}_{a/k}$ ein Isomorphismus von Gruppenschemata über U, so erfüllt das Element:

$$\psi \circ \varphi(a) \circ \psi^{-1} = \sum_n \alpha_n(a)\tau^n \in k\{\tau\}$$

   die für alle $a \in A \setminus \{0\}$ die Bedingungen:

   2.a) $\alpha_n(a)$ ist invertierbar in k für $n = -d\deg(\infty)\infty(a)$.

   2.b) $\alpha_n(a)$ ist nilpotent für $n > -d\deg(\infty)\infty(a)$.

Satz 5.3. *Sei (E, d) ein Drinfeld-Modul, dann gibt es einen kanonischen Ringhomomorphismus:*

$$\partial : \mathrm{End}_S(E) \longrightarrow \Gamma(S)$$

und damit einen Morphismus von Schemata:

$$\theta : S \longrightarrow X \setminus \{\infty\}$$

Dieser Morphismus heißt Charakteristik des Drinfeld-Modul E.

Beweis. Sei $\mathrm{Spec}(k) = U \subseteq S$ eine offene, affine Teilmenge mit $E|_U \cong \mathbf{G}_{a/k}$. Dann ist $\mathrm{End}_U(E|_U) \cong k\{\tau\}$, und die Abbildung $\partial : k\{\tau\} \longrightarrow k$ aus Bemerkung 4.8 auf Seite 20 liefert einen Ringhomomorphismus nach $k = \Gamma(U, \mathcal{O}_S)$. Ist $\mathrm{End}_S(E) \longrightarrow \mathrm{End}_U(E|_U)$ die kanonische Einschränkung, so ergibt sich ein Ringhomomorphsimus $\mathrm{End}_S(E) \longrightarrow \Gamma(U, \mathcal{O}_S)$. Dieser Morphismus ist nach Bedingung 1.b) mit der Bildung von Durchschnitten verträglich und so lassen sich die lokalen Schnitte in $\Gamma(U, \mathcal{O}_S)$ nach dem Garbenaxiom zu einem Schnitt in $\Gamma(S)$ zusammenkleben. $\square$

Bemerkung 5.4. Ist k ein Körper und $S = \mathrm{Spec}(k)$, dann werden die Definitionen wesentlich einfacher. Ein Drinfeld-Modul vom Rang d ist ein Ringhomomorphismus

$$\varphi : A \longrightarrow k\{\tau\}$$

mit $\deg(\varphi(a)) = -d \deg(\infty)\infty(a)$.
Die Charakteristik θ ergibt sich aus dem Diagramm:

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[dr, "\theta"'] & k\{\tau\} \arrow[d, "\partial"] \\ & k \end{tikzcd}$$

5.3 Teilungspunkte

Wie am Anfang beschrieben, liefern Torsionen wichtige Informationen über die Struktur von $\mathbf{Z}$-Moduln. Dieses Konzept führt im Falle eines Drinfeld-Moduln zum Begriff der I-Teilungspunkte.

Definition 5.5. Sei (E, φ) ein Drinfeld Modul, dann heißt der Funktor:

$$\begin{aligned} E_a : \mathbf{Sch}/S &\longrightarrow \mathbf{Ab} \\ X &\longmapsto \mathrm{Ker}(\mathrm{Hom}_S(X, E) \xrightarrow{\varphi(a)} \mathrm{Hom}_S(X, E)) \end{aligned}$$

Schema der a-Teilungspunkte von E.
Ist I ein Ideal in A, so wird analog der Funktor

$$\begin{aligned} E_I : \mathbf{Sch}/S &\longrightarrow \mathbf{Ab} \\ X &\longmapsto \bigcap_{a \in I} \mathrm{Ker}(\mathrm{Hom}_S(X, E) \xrightarrow{\varphi(a)} \mathrm{Hom}_S(X, E)) \end{aligned}$$

definiert. Sinnigerweise wird er dann als *Schema der I-Teilungspunkte* bezeichnet.

Eigenschaften 5.6.

1. Ist (a) das von $a \in A$ erzeugte Ideal, so ist $E_{(a)} = E_a$.

2. Ist I erzeugt von $a_1, \ldots, a_s \in A$, so ist $E_I = E_{a_1} \cap \cdots \cap E_{a_s}$.

3. Ist X/S ein Schema, so annuliert jedes $a \in I$ nach Definition den A-Modul $E_I(X)$, d.h. $E_I(X)$ ist A/I-Modul.

4. Sind I_1, I_2 teilerfremde Ideale in A, dann gibt es eine kanonische Isomorphie:
$$E_I \cong E_{I_1} \times_S E_{I_2}$$
als Schemata von $A/I \cong A/I_1 \times A/I_2$-Moduln.

Lokal lassen sich die I-Teilungspunkte sehr gut beschreiben. Dies zeigt der folgende Satz.

Satz 5.7 (Drinfeld). *Sei (E, φ) ein Drinfeld Modul vom Rang d. Die Einschränkung des Schemas von A/I-Moduln E_I auf $S \setminus \theta^{-1}(V(I))$ ist lokal konstant mit Wert $(A/I)^d$ bezüglich der étalen Topologie auf $S \setminus \theta^{-1}(V(I))$.*

Bemerkung 5.8 (zum Satz).

1. Die *Grothendieck* Topologie verallgemeinert den Begriff einer Topologie auf einem Schema X. Offene Teilmengen $U \subseteq X$ werden durch Morphismen von Schemata $f : U \longrightarrow X$ mit bestimmten Eigenschaften ersetzt. Bsp:

   - f Zariski offene Immersionen $\rightarrow$ *Zariskitopologie.*
   - f étale von endlichem Typ $\rightarrow$ *étale Topologie*
   - f flach, lokal von endlichem Typ $\rightarrow$ *flache Topologie*
     Genaueres findet sich in [Art62].

2. Sei $U := S \setminus \theta^{-1}(V(I)) \subseteq S$ eine offene Teilmenge von S. Ist $\mathcal{F}$: $\mathbf{Sch}/S \longrightarrow \mathbf{Men}$ ein Funktor, so wird
$$\begin{aligned} \mathcal{F}|_{\mathcal{U}} : \mathbf{Sch}/U &\longrightarrow \mathbf{Men} \\ X/U &\longrightarrow \mathcal{F}(X/S) \end{aligned}$$
als Einschränkung von $\mathcal{F}$ auf U definiert.

3. Die Aussage des Satzes liest sich nun wie folgt:
   Es gibt $U_i \longrightarrow U$ offene Überdeckung von U im Sinne der étalen Grothendieck Topologie, so daß $E_a|_{U_i}(X) \cong (A/I)^d$ ist.

4. Ist $S = \mathrm{Spec}(k)$, k Körper und $\theta^{-1}(V(I)) = \emptyset$, so ist jede separable, algebraische Körpererweiterung von k eine Überdeckung von $\mathrm{Spec}(k)$ im Sinne der étalen Topologie. Sei $I = (a)$ und $E = \mathbf{G}_{a/k}$ und $\varphi(a) \in k\{\tau\}$ gegeben. Da $\theta^{-1}(V(I)) = \emptyset$ ist, ist $\partial(\varphi(a)) \neq 0$ und $\varphi(a)$ aufgefaßt als additives Polynom in $k[T]$ separabel. Der Zerfällungskörper ist dann die gesuchte étale Überdeckung. Genaueres findet sich in [DH87] und in [Lau91].

Der Satz gibt nun Anlaß zu der folgenden Definition:

Definition 5.9 (Drinfeld). Sei (E, φ) ein Drinfeld-Modul und I Ideal in A. Sei
$\theta^{-1}(V(I)) = \emptyset$. Eine *$I$-Level-Struktur* auf (E, φ) ist ein Isomorphismus von Schemata von A/I-Moduln über S:

$$\iota : (A/I)^d_S \xrightarrow{\sim} E_I$$

Hierbei ist $(A/I)^d_S$ das konstante Schema (Bsp 3.11 auf Seite 15) von A/I-Moduln mit Wert $(A/I)^d$.

5.4 Faserkategorien

Der folgende Abschnitt gibt eine kleine Einführung in die Sprache der *Faserkategorien* und verfolgt zwei Zwecke:
Zum einen verallgemeinern Faserkategorien den Begriff von darstellbaren Funktoren auf $\mathbf{Sch}/S$, indem auch das Basisschema S als Variable angesehen wird. Zum andern bieten Faserkategorien die Grundlage für die Definition von *algebraischen Stacks*.
Algebraische Stacks sind spezielle Faserkategorien über der Kategorie **Sch** mit einigen zusätzlich geforderten Daten. Sie verallgemeinern die Kategorie **Sch** und erlauben die Lösung von Darstellungsproblemen, die über **Sch** nicht lösbar sind.
Die folgenden Grundlagen über Faserkategorien wurden dem Artikel [DM69, §4] von *Deligne* und *Mumford* entnommen. Für eine weiterführende Darstellung des Themas, insbesondere die Definition von *algebraischen Stacks* und deren Anwendungen, sei auf diesen Artikel verwiesen.

Seien im folgenden A, B beliebige Kategorien und C ein Kategorie mit beliebigen Faserprodukten.

Definition 5.10. Sei $\mathcal{F} : \mathbf{A} \longrightarrow \mathbf{C}$ ein covarianter Funktor. Für alle $X \in \mathrm{Obj}(\mathbf{C})$ wird $\mathcal{F}(X)$ Kategorie durch:

Objekte: $x \in \mathrm{Obj}(\mathbf{A})$ mit $\mathcal{F}(x) = X$

Morphismen: $f \in \mathrm{Mor}_{\mathbf{A}}(x, y)$ mit $\mathcal{F}(f) = \mathrm{id}_X\}$

Die Kategorie $\mathcal{F}(X)$ heißt *Faser* über X.

Definition 5.11 (Faserkategorie). Sei $\mathcal{F} : \mathbf{A} \longrightarrow \mathbf{C}$ ein covarianter Funktor. $\mathcal{F}$ heißt *Faserkategorie*, falls gilt:

Zu jedem Pfeil $F : X \longrightarrow Y$ in $\mathbf{C}$ und jedem $y \in \mathcal{F}(Y)$ gibt es einen Pfeil $f : x \longrightarrow y$ mit der universellen Eigenschaft:

$$\begin{tikzcd} x' \arrow[d, dashed, "f'"'] \arrow[dr, "h"] & & & X \arrow[d, equal] \arrow[dr, "F"] & \\ x \arrow[r, "f"] & y & \arrow[r, "\mathcal{F}"] & X \arrow[r, "F"] & Y \end{tikzcd}$$

Das heißt, für jedes $x' \in \mathcal{F}(X)$ und jedes $h \in \mathrm{Mor}_{\mathbf{A}}(x', y)$ mit $\mathcal{F}(h) = F$ gibt es genau einen Morphismus $f' \in \mathrm{Mor}_{\mathcal{F}(X)}(x', x)$, so daß das linke Diagramm kommutiert.
x ist dann bis auf Isomorphie eindeutig definiert und liefert einen Funktor:

$$\begin{aligned} F^* : \mathcal{F}(Y) &\longrightarrow \mathcal{F}(X) \\ y &\longmapsto F^*(y) \end{aligned}$$

Es gilt (falls definiert): $(F_1F_2)^* = F_2^*F_1^*$

Beispiel 5.12. Sei $\mathbf{A}$ Kategorie der Schemata über einem Basisschema und

$$\begin{aligned} \mathcal{F} : \mathbf{A} &\longrightarrow \mathbf{Sch} \\ X/S &\longmapsto S \end{aligned}$$

Funktor durch Ausstoßen des Basisschemas. $\mathcal{F}$ ist eine Faserkategorie mit $\mathcal{F}(S) = \mathbf{Sch}/S$ und für $F : T \longrightarrow S$ ist $F^*(E) = E \times_S T$.

Definition 5.13 (Morphismen zwischen Faserkategorien). Seien $\mathcal{F}_1 : \mathbf{A} \longrightarrow \mathbf{C}$ und $\mathcal{F}_2 : \mathbf{B} \longrightarrow \mathbf{C}$ zwei Faserkategorien. Ein Morphismus zwischen Faserkategorien ist ein Funktor $\mathcal{T} : \mathbf{A} \longrightarrow \mathbf{B}$, so daß das Diagramm

$$\begin{tikzcd} \mathbf{A} \arrow[dd, "\mathcal{T}"'] \arrow[dr, "\mathcal{F}_1"] & \\ & \mathbf{C} \\ \mathbf{B} \arrow[ur, "\mathcal{F}_2"'] & \end{tikzcd}$$

kommutiert.
Die Morphismen zwischen Faserkategorien bilden selbst eine Kategorie:

Objekte: $\mathcal{T} : \mathbf{A} \longrightarrow \mathbf{B}$ Morphismen von Faserkategorien.

Morphismen: $t : \mathcal{T}_1 \longrightarrow \mathcal{T}_2$ Transformationen von Funktoren.

Diese Kategorie wird mit $\mathrm{Hom}(\mathbf{A}, \mathbf{B})$ bezeichnet.

Definition 5.14 (Darstellbare Faserkategorien). Sei $X \in \mathrm{Obj}(\mathbf{C})$. Zu X wird die folgende Kategorie definiert:

Objekte: Pfeile $U \longrightarrow X$ in $\mathbf{C}$

Morphismen: Kommutative Diagramme:

$$\begin{tikzcd} U \arrow[d] \arrow[dr] & \\ U' \arrow[r] & X \end{tikzcd}$$

Diese Kategorie wird mit $\mathbf{C}/X$ bezeichnet.
Sei $\mathcal{F}$ der folgende Funktor:

$$\mathcal{F} : \mathbf{C}/X \longrightarrow \mathbf{C}$$
$$(U \longrightarrow X) \longmapsto U$$

mit

$$\mathcal{F}\left(\begin{tikzcd} U \arrow[d, "f"'] \arrow[dr] & \\ U' \arrow[r] & X \end{tikzcd}\right) = U \xrightarrow{f} U'$$

$\mathcal{F}$ wird dadurch zu einer Faserkategorie über $\mathbf{C}$ und wird schlicht mit X bezeichnet.
Eine zu X isomorphe Faserkategorie heißt *darstellbar*.
Ist $Y \in \mathrm{Obj}(\mathbf{C})$ dann läßt sich die Faser $\mathcal{F}(Y)$ einfach beschreiben: Objekte sind die Elemente in $\mathrm{Hom}_{\mathbf{C}}(Y, X)$ und Identitäten die einzigen Morphismen. Kategorien mit Identitäten als den einzigen Morphismen heißen *diskret* und demzufolge heißt eine Faserkategorie mit diskreten Fasern *diskrete Faserkategorie*. Insbesondere sind darstellbare Faserkategorien diskret.

Bemerkung 5.15. Seien $\mathcal{F} : \mathbf{A} \longrightarrow \mathbf{C}$ und $X \in \mathrm{Obj}(\mathbf{C})$ Faserkategorien über $\mathbf{C}$. Dann ist die Kategorie $\mathrm{Hom}(X, \mathbf{A})$ kanonisch isomorph zur Faser $\mathcal{F}(X)$.

Beweis. Der gesuchte Isomorphismus wird gegeben durch:

$$\begin{aligned} \mathcal{F}(X) &\longrightarrow \mathrm{Hom}(X, \mathbf{A}) \\ x &\longmapsto \begin{pmatrix} \mathcal{T} : X \longrightarrow \mathbf{A} \\ (U \xrightarrow{f} X) \longmapsto f^*(x) \end{pmatrix} \end{aligned} \qquad \begin{aligned} \mathrm{Hom}(X, \mathbf{A}) &\longrightarrow \mathcal{F}(X) \\ \mathcal{T} &\longmapsto \mathcal{T}(X \xrightarrow{\mathrm{id}} X) \end{aligned}$$

□

Definition 5.16 (Faserkategorien und mengenwertige Funktoren). Jedem kontravarianten, mengenwertigen Funktor läßt sich in kanonischer Weise eine Faserkategorie zuordnen, andererseits definiert jede Faserkategorie einen solchen Funktor.

1. Sei $\mathcal{F} : \mathbf{A} \longrightarrow \mathbf{C}$ eine Faserkategorie. Der zugehörige mengenwertige Funktor $[\mathcal{F}]$ wird nun wie folgt definiert:

$$\begin{aligned}[\mathcal{F}] : \mathbf{C} &\longrightarrow \mathbf{Men} \\ X &\longmapsto \{\text{Isomorphieklassen in } \mathcal{F}(X)\}\end{aligned}$$

   Ist $F : X \longrightarrow Y$ Morphismus und $[y]$ eine Klasse in $\mathcal{F}(Y)$, so $[\mathcal{F}](F)[y] := [F^*y]$

2. Ist andererseits $\mathcal{G} : \mathbf{C} \longrightarrow \mathbf{Men}$ ein kontravarianter Funktor, so läßt sich eine Faserkategorie hierzu definieren:

   Sei $\mathbf{A}$ Kategorie definiert durch:

   Objekte: Paare (X, a) mit $X \in \mathrm{Obj}(\mathbf{C})$ und $a \in \mathcal{G}(X)$

   Morphismen: $\mathrm{Mor}((X, a), (Y, b)) := \{F \in \mathrm{Mor}_{\mathbf{C}}(X, Y) \text{ mit } \mathcal{G}(F)(b) = a\}$

   Die Faserkategorie ergibt sich nun durch Ausstoßen:

$$\begin{aligned}\mathcal{F} : \mathbf{A} &\longrightarrow \mathbf{C} \\ (X, a) &\longmapsto X\end{aligned}$$

   Wird die Menge $\mathcal{G}(X)$ als diskrete Kategorie interpretiert (Identitäten sind die einzigen Morphismen), dann ist die Faser $\mathcal{F}(X) = \mathcal{G}(X)$ für alle $X \in \mathrm{Obj}(\mathbf{C})$. Insbesondere sind die durch mengenwertige Funktoren definierten Faserkategorien diskret.

Bemerkung 5.17.

a) Ist $\mathcal{F} : \mathbf{A} \longrightarrow \mathbf{C}$ diskrete Faserkategorie, dann sind die Isomorphieklassen der Fasern nach 5.14 trivial und der zugehörige mengenwertige Funktor ist:

$$\begin{aligned}[\mathcal{F}] : \mathbf{C} &\longrightarrow \mathbf{Men} \\ U &\longmapsto \mathrm{Obj}(\mathcal{F}(U))\end{aligned}$$

   Ist $\mathbf{A}$ sogar darstellbar durch ein $X \in \mathrm{Obj}(\mathbf{C})$, dann ist $[\mathcal{F}](\_\,) \cong \mathrm{Hom}_{\mathbf{C}}(\_\,, X)$ und damit selbst darstellbar.

b) Ist andererseits $\mathcal{G} : \mathbf{C} \longrightarrow \mathbf{Men}$ ein darstellbarer Funktor, d.h. $\mathcal{G}(\_) \cong \mathrm{Hom}_{\mathbf{C}}(\_, X)$ für ein $X \in \mathbf{C}$, dann ist auch die zugehörige Faserkategorie darstellbar mit darstellendem Objekt X.

Definition 5.18 (Basiswechsel). Sei $\mathcal{T} : \mathbf{S}_1 \longrightarrow \mathbf{S}_2$ Morphismus von Faserkategorien über $\mathbf{C}$. Für jedes $X \in \mathrm{Obj}(\mathbf{C})$ und jeden Morphismus $x : X \longrightarrow \mathbf{S}_2$ wird eine Faserkategorie $X \times_{\mathbf{S}_2} \mathbf{S}_1$ wie folgt definiert:

$$\textbf{Objekte: } \text{Tripel} \begin{pmatrix} Y \xrightarrow{F} X \\ y \in \mathrm{Obj}(\mathbf{S}_1(Y)) \\ f : \mathcal{T}(y) \xrightarrow{\sim} F^*(x) \\ \quad \in \mathrm{Mor}_{\mathbf{S}_2(Y)}(\mathcal{T}(y), F^*(x)) \end{pmatrix}$$

Morphismen: Paare $\begin{pmatrix} \alpha \in \mathrm{Hom}_{\mathbf{C}/X}(Y, Y') \\ \beta \in \mathrm{Hom}_{\mathbf{S}_1}(y, y') \end{pmatrix}$, so daß das folgende Diagramm kommutiert:

$$\begin{array}{ccc} y & \xrightarrow{f} & F^*(x) \\ {\scriptstyle\beta}\downarrow & & \downarrow{\scriptstyle\alpha^*} \\ y' & \xrightarrow{f'} & F'^*(x) \end{array}$$

Die Projektionsmorphismen werden gegeben durch:

$$\begin{aligned} X \times_{\mathbf{S}_2} \mathbf{S}_1 &\longrightarrow \mathbf{C}/X \\ (Y \longrightarrow X, y, f) &\longmapsto (Y \longrightarrow X) \end{aligned}$$

und

$$\begin{aligned} X \times_{\mathbf{S}_2} \mathbf{S}_1 &\longrightarrow \mathbf{S}_1 \\ (Y \longrightarrow X, y, f) &\longmapsto y \end{aligned}$$

Definition 5.19 (Darstellbare Morphismen). Ein Morphismus $\mathcal{T} : \mathbf{S}_1 \longrightarrow \mathbf{S}_2$ von Faserkategorien heißt *darstellbar*, falls für jedes Objekt $X \in \mathrm{Obj}(\mathbf{C})$ und jeden Morphismus $x : X \longrightarrow \mathbf{S}_2$ gilt: $X \times_{\mathbf{S}_2} \mathbf{S}_1$ ist darstellbar als Faserkategorie über $\mathbf{C}/X$.

Beispiel 5.20. Sei $\mathbf{S}$ Faserkategorie über $\mathbf{C}$. Sei $Y \in \mathrm{Obj}\,\mathbf{C}$. Ist $\mathcal{T} : \mathbf{S} \longrightarrow Y$ darstellbarer Morphismus, dann ist $\mathbf{S}$ darstellbar über $\mathbf{C}/Y$.

Beweis. Setze $X = Y$ und $x = \mathrm{id}$, den identischen Funktor auf X. Nach Definition ist dann $Y \times_Y \mathbf{S} = \mathbf{S}$ darstellbar. $\square$

Nach diesen Vorarbeiten lassen sich die Eigenschaften von Morphismen zwischen Schemata auf Faserkategorien verallgemeinern:

Definition 5.21. Sei $\mathbf{C} = \mathbf{Sch}$ und $\mathcal{T} : \mathbf{S}_1 \longrightarrow \mathbf{S}_2$ darstellbarer Morphismus. $\mathcal{T}$ heißt flach, glatt, étale, von endlichem Typ, etc., falls für jedes Schema X und jeden Morphismus $x : X \longrightarrow \mathbf{S}_2$ das darstellende Objekt $(Z \longrightarrow X)$ von $X \times_{\mathbf{S}_2} \mathbf{S}_1$ die entsprechende Eigenschaft hat.

5.5 Modulare Varietäten

Das Konzept der I-Teilungspunkte von Drinfeld Moduln wird nun in die Sprache der Faserkategorien übertragen:

Definition 5.22. Sei I Ideal in A und $d \in \mathbb{N}$. Sei S ein Schema über $\mathbf{F}_p$. Es wird nun die folgende Faserkategorie definiert. Sei $\mathbf{A}$ eine Kategorie gegeben durch:

Objekte: Tripel $(E/S, \varphi, \iota)$, wobei (E, φ) ist Drinfeld-Modul vom Rang d mit
$\theta^{-1}(V(I)) = \emptyset$ und einer I-Level-Struktur ι.

Morphismen: Sind $(E/S, \varphi, \iota)$ und $(F/T, \varphi', \iota')$ zwei Objekte, so sind die Morphismen Paare:

$(T \longrightarrow S, F \longrightarrow E \times_S T)$ verträglich mit den Modul- und I-Level-Strukturen.

Die Faserkategorie $\mathcal{M}_I^d$ ergibt sich nun wie folgt:

$$\begin{aligned} \mathcal{M}_I^d : \mathbf{A} &\longrightarrow \mathbf{Sch}/\mathbf{F}_p \\ (E/S, \varphi, \iota) &\longmapsto S \end{aligned}$$

Bemerkung 5.23. Ist $(E/S, \varphi)$ ein Drinfeld-Modul, so definiert die Charakteristik einen Morphismus von Schemata: $\theta : S \longrightarrow X \setminus (\{\infty\} \cup V(I))$. Dieser induziert wiederum einen Morphismus von Faserkategorien:

$$\begin{aligned} \Theta : \mathcal{M}_I^d &\longrightarrow X \setminus (\{\infty\} \cup V(I)) \\ (E/S, \varphi, \iota) &\longmapsto (S, \theta) \end{aligned}$$

Satz 5.24 (Drinfeld). *Ist $I \neq A$, dann ist die Faserkategorie $\mathcal{M}_I^d$ darstellbar durch ein affines Schema M_I^d von endlichem Typ über $\mathbf{F}_p$.*

Beweis. siehe [Lau91]. □

Bemerkung 5.25. Für $I = A$ sind die Teilungspunkte trivial und $\mathcal{M}_A^d$ ist einfach die Faserkategorie der Drinfeld-Moduln vom Rang d. Leider ist diese Kategorie i. allg. nicht durch ein Schema darstellbar.
Abhilfe schafft, wie oben erwähnt, die Erweiterung des Begriffs eines Schemas durch *algebraische Stacks*. Die Kategorie der Drinfeld Moduln ist dann darstellbar durch einen *algebraischen Stack* M_A^d von endlichem Typ über $\mathbf{F}_p$.

6 Hochschild-Homologie

6.1 Relative Homologie und Cohomologietheorie

Ist G eine Gruppe und M ein G-Modul, dann ist M selbst abelsche Gruppe (ein $\mathbf{Z}$-Modul). Analog ist für einen R-Modul M mit einer k-Algebra R auch M ein k-Modul. Allgemein lassen sich solche relativen Gegebenheiten als Paare zueinander adjungierter Funktoren beschreiben. Ziel des Unterabschnitts ist die Entwicklung einer mit diesen Funktoren verträglichen Homologietheorie.

Seien $\mathcal{C}_k$ und $\mathcal{C}_R$ abelsche Kategorien. Zur besseren Unterscheidung seien die Morphismen in $\mathcal{C}_R$ mit „ $\longrightarrow$ “ und die Morphismen in $\mathcal{C}_k$ mit „ $\dashrightarrow$ “ bezeichnet.

Definition 6.1. Die Kategorien $\mathcal{C}_k$ und $\mathcal{C}_R$ heißen zueinander relativ oder einfach *relative Kategorie*, falls es zwei Funktoren $\Box$, F mit den folgenden Eigenschaften gibt:

$$\begin{aligned} \Box : \mathcal{C}_R &\longrightarrow \mathcal{C}_k \\ A &\longmapsto A_\Box \end{aligned}$$

ein *exakter, linearer* und *volltreuer* Funktor, d.h.:

exakt: Ist
$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$
exakte Sequenz in $\mathcal{C}_R$, so ist auch
$$0 \dashrightarrow A_\Box \dashrightarrow B_\Box \dashrightarrow C_\Box \dashrightarrow 0$$
eine exakte Sequenz in $\mathcal{C}_k$.

linear: Sind $\varphi_1, \varphi_2 : A \longrightarrow B$ Morphismen in $\mathcal{C}_R$, so gilt:
$$\varphi_{1\Box} + \varphi_{2\Box} = (\varphi_1 + \varphi_2)_\Box$$

volltreu: $\alpha_\Box = 0 \iff \alpha = 0$. Insbesondere ist mit $A_\Box$ dann auch $A = 0$.

$$\begin{aligned} F : \mathcal{C}_k &\longrightarrow \mathcal{C}_R \\ M &\longmapsto FM \end{aligned}$$

ein zu $\Box$ *linksadjungierter* Funktor F, d.h.:
Es gibt einen Isomorphismus von Funktoren:

(6.1.1) $\quad \mathrm{Hom}_{\mathcal{C}_R}(F(\_\,), \_\,) \cong \mathrm{Hom}_{\mathcal{C}_k}(\_\,, \Box(\_\,)) : \mathcal{C}_k^{\mathrm{op}} \times \mathcal{C}_R \longrightarrow \mathbf{Men}$

Insbesondere also einen Isomorphismus von Mengen:

(6.1.2) $\quad \varphi : \mathrm{Hom}_R(FM, A) \cong \mathrm{Hom}_k(M, \Box A)$

für alle M in $\mathcal{C}_k$ und A in $\mathcal{C}_R$ (Mit $\mathcal{C}_k^{\mathrm{op}}$ sei die zu $\mathcal{C}_k$ opponierte Kategorie bezeichnet).

Lemma 6.2. Sei M in $\mathcal{C}_k$. Sei $e_M := \varphi(\mathrm{id}_{FM}) : M \dashrightarrow \Box FM$. Sei $M \overset{u}{\dashrightarrow} A_\Box$ ein Morphismus in $\mathcal{C}_k$, dann gibt es genau einen Morphismus $FM \xrightarrow{\alpha} A$ in $\mathcal{C}_R$, so daß das Diagramm

$$\begin{tikzcd} & \Box FM \arrow[d, dashed, "\alpha_\Box"] \\ M \arrow[ur, "e_M"] \arrow[r, dashed, "u"] & A_\Box \end{tikzcd}$$

kommutiert.

Beweis. Nach (6.1.1) kommutiert für $M \in \mathcal{C}_k$, $A \in \mathcal{C}_R$ und $FM \xrightarrow{\alpha} A$ das Diagramm:

$$\begin{tikzcd} \mathrm{Hom}_{\mathcal{C}_R}(FM, FM) \arrow[r, "\varphi"] \arrow[d, "\alpha_*"'] & \mathrm{Hom}_{\mathcal{C}_k}(M, \Box FM) \arrow[d, "\alpha_{\Box *}"] \\ \mathrm{Hom}_{\mathcal{C}_R}(FM, A) \arrow[r, "\varphi"] & \mathrm{Hom}_{\mathcal{C}_k}(M, \Box A) \end{tikzcd}$$

Dabei ist α_* die von α induzierte Abbildung. Ist $e_M = \varphi(\mathrm{id}_{FM})$, so folgt aus der Bijektivität von φ für jedes $M \overset{u}{\dashrightarrow} A_\Box$ die eindeutige Existenz eines $FM \xrightarrow{\alpha} A$ mit $\alpha_\Box e_M = \varphi(\alpha) = u$. $\Box$

Die *relativen projektiven* Objekte spielen die entscheidende Rolle bei der Entwicklung einer relativen Homologietheorie:

Definition 6.3.

1. Ein Morphismus $A \xrightarrow{\alpha} B$ heißt *zulässig* falls es einen Morphismus $B_\Box \overset{s}{\dashrightarrow} A_\Box$ in $\mathcal{C}_k$ gibt mit $\alpha_\Box s \alpha_\Box = \alpha_\Box$.

2. Ein Modul P in $\mathcal{C}_R$ heißt *relativ projektiv* falls gilt:

   Für jedes Diagramm mit zulässigem α und beliebigem β

$$\begin{tikzcd} & P \arrow[d, "\beta"] \arrow[dl, dotted, "\tilde{\beta}"'] & \\ A \arrow[r, "\alpha"] & B \arrow[r] & 0 \end{tikzcd}$$

   gibt es einen Morphismus $P \xrightarrow{\tilde{\beta}} A$, so daß das Diagramm kommutiert.

Bemerkung 6.4.

- Ist $A \xrightarrow{\alpha} B$ zulässig, so sind die beiden exakten Sequenzen

$$0 \longrightarrow \operatorname{Ker}\alpha \longrightarrow A \longrightarrow \operatorname{Im}\alpha \longrightarrow 0$$
$$0 \longrightarrow \operatorname{Im}\alpha \longrightarrow B \longrightarrow \operatorname{Coker}\alpha \longrightarrow 0$$

  nach Anwendung von $\Box$ als Sequenzen in $\mathcal{C}_k$ spaltend.

- Ist $P \in \mathcal{C}_R$ projektives Objekt, dann ist P auch relativ projektiv.

Satz 6.5.

1. *Ist M in $\mathcal{C}_k$, so ist $F(M)$ relativ projektiv.*

2. *Ist A in $\mathcal{C}_R$, dann gibt es einen zulässigen, surjektiven Morphismus: $F(A_\Box) \xrightarrow{\alpha} A$. $\mathcal{C}_R$ hat also genügend viele relativ projektive Objekte.*

Beweis.

zu 1. Sei

$$\begin{tikzcd} & F(M) \arrow[d, "\gamma"] \arrow[dl, dotted, "?\ \tilde{\gamma}"'] & \\ A \arrow[r, shift left, "\alpha"] & B \arrow[l, dashed, shift left, "s"] \arrow[r] & 0 \end{tikzcd}$$

Diagramm mit zulässigem α. Anwendung von (6.1.2) auf γ liefert die Existenz eines Morphismus: $M \overset{u}{\dashrightarrow} B_\square$. Sei $\tilde{u} := su : M \dashrightarrow A_\square$:

$$\begin{tikzcd} & M \arrow[dl, "\tilde{u}"'] \arrow[d, dashed, "u"] \\ A_\square & B_\square \arrow[l, dashed, "s"] \end{tikzcd}$$

Wiederum mit (6.1.1) angewandt auf $\tilde{u}$ ergibt sich ein Morphismus $F(M) \xrightarrow{\tilde{\gamma}} A$, der das Diagramm kommutativ ausfüllt.

zu 2. Mit (6.1.2) gibt es zu $A_\square \overset{\mathrm{id}}{\dashrightarrow} A_\square$ einen Morphismus $F(A_\square) \xrightarrow{\alpha} A$. Zu zeigen bleibt: α ist surjektiv und zulässig.

surjektiv: Sei $A \xrightarrow{\beta} B$ ein Pfeil in $\mathcal{C}_R$ mit $\beta\alpha = 0$. Es ergibt sich das kommutative Diagramm:

$$\begin{tikzcd} \mathrm{Hom}(F(A_\square), A) \arrow[r, "\varphi"] \arrow[d, "\beta_*"'] & \mathrm{Hom}(A_\square, A_\square) \arrow[d, "\beta_{\square *}"] \\ \mathrm{Hom}(F(A_\square), B) \arrow[r, "\varphi"] & \mathrm{Hom}(A_\square, B_\square) \end{tikzcd}$$

Mit $\beta\alpha$ ist also auch $\beta_\square \, \mathrm{id} = 0$, d.h. $\beta_\square = 0$. Mit der Volltreuheit von $\square$ ist dann aber auch $\beta = 0$. Es folgt die Behauptung.

zulässig: Sei $t := e_{A_\square} : A_\square \dashrightarrow \square F A_\square$ Nach Definition gilt dann:

$$\begin{aligned} & \mathrm{id}_{A_\square} = \alpha_\square e_{A_\square} = \alpha_\square t \\ \Longrightarrow \quad & \alpha_\square = \alpha_\square t \alpha_\square \end{aligned}$$

und α stellt sich damit als zulässig heraus.

$\square$

Um die Homologiemaschinerie ordentlich zum Laufen zu bringen, noch einige Definitionen:

Definition 6.6. Sei A in $\mathcal{C}_R$

1. Eine Auflösung $X \xrightarrow{\varepsilon} A$ heißt *zulässige Auflösung*, falls alle $X_n \xrightarrow{\partial_n} X_{n-1}$ und $X_0 \xrightarrow{\varepsilon} A$ zulässige Morphismen sind.

2. Eine zulässige Auflösung heißt *relativ projektiv*, falls alle X_n relativ projektive Objekte in $\mathcal{C}_R$ sind.

3. Eine zulässige Auflösung $X \xrightarrow{f} A$ heißt *relativ freie Auflösung*, falls $X_n = F(M_n)$, so daß für alle n aus $\mathbf{N}$ ein M_n aus $\mathcal{C}_k$ existiert.

Satz 6.7 (Vergleichstheorem). *Ist $X \xrightarrow{\varepsilon} A$ eine relativ projektive, $Y \xrightarrow{\varepsilon'} B$ eine beliebige zulässige Auflösung und $A \xrightarrow{\alpha} B$ ein beliebiger Morphismus, dann läßt sich α zu einer Kettentransformation φ fortsetzen:*

$$\begin{tikzcd}
{} \arrow[r] & X_2 \arrow[r] \arrow[d, "\varphi_2"'] & X_1 \arrow[r] \arrow[d, "\varphi_1"'] & X_0 \arrow[r] \arrow[d, "\varphi_0"'] & A \arrow[r] \arrow[d, "\alpha"'] & 0 \\
{} \arrow[r] & Y_2 \arrow[r] & Y_1 \arrow[r] & Y_0 \arrow[r] & B \arrow[r] & 0
\end{tikzcd}$$

Beweis. Der Beweis funktioniert wie im nicht relativen Fall und findet sich im Buch [Mac69, Chapter IX Theorem 6.2]. $\square$

In der relativen Situation gibt es immer eine kanonische Auflösung. Dies zeigt der folgende Satz:

Satz 6.8 (Bar-Auflösung). *Sei $\tilde{F} := F(\square(\_))$ und C in $\mathcal{C}_R$.*
Sei

$$\beta_n := \tilde{F}^n \tilde{F} \quad \text{für} \quad n = 0, 1, 2, \ldots$$

d.h.

$$\begin{aligned}
\beta_0(C) &= \tilde{F}C \\
\beta_n(C) &= \tilde{F}^n \tilde{F}(C)
\end{aligned}$$

Es gibt Morphismen ε, ∂ in $\mathcal{C}_R$

$$\tilde{F}C \xrightarrow{\varepsilon} C$$
$$\beta_n(C) \xrightarrow{\partial_n} \beta_{n-1}(C)$$

und Morphismen s in $\mathcal{C}_k$

$$C_\square \overset{s_{-1}}{\dashrightarrow} \beta_0(C)_\square$$
$$\beta_{n-1}(C)_\square \overset{s_{n-1}}{\dashrightarrow} \beta_n(C)_\square$$

so daß

$$
0 \underset{}{\overset{}{\leftrightarrows}} C \underset{s_{-1}}{\overset{\varepsilon}{\leftrightarrows}} \beta_0(C) \underset{s_0}{\overset{\partial_1}{\leftrightarrows}} \beta_1(C) \underset{s_1}{\overset{\partial_2}{\leftrightarrows}} \cdots
$$

eine relativ freie, zulässige Auflösung von C ist und s eine zusammenziehbare Homotopie, d.h. $\partial s + s\partial = 1$ in $\mathcal{C}_k$. Diese Auflösung $(=: \beta(C))$ heißt Bar-Auflösung von C.

Beweis.

- Definition von s: Mit Hilfe von Lemma 6.2 auf Seite 34 ergibt sich s folgendermaßen:

$$
\begin{aligned}
s_{-1} &:= e_{C_\square} : C_\square \dashrightarrow \beta_0(C)_\square \\
s_n &:= e_{\beta_n(C)_\square} : \beta_n(C)_\square \dashrightarrow \beta_{n+1}(C)_\square
\end{aligned}
$$

- Konstruktion von ε: In Analogie zu der Konstruktion nach Satz 6.5 auf Seite 35 ergibt sich ε als $\varphi^{-1}(\mathrm{id}_{C_\square}) : \beta_0(C) = F(C_\square) \longrightarrow C$. ε ist surjektiv und es gilt: $\varepsilon_\square s_{-1} = \mathrm{id}_{C_\square}$, d.h. ε ist zulässig.

- Konstruktion von ∂ durch Induktion: Ist

$$
1 - s_{-1}\varepsilon_\square : \beta_0(C)_\square \dashrightarrow \beta_0(C)_\square
$$

so induziert diese Abbildung mit Hilfe von φ wieder einen Morphismus

$$
\beta_1(C) \xrightarrow{\partial_1} \beta_0(C)
$$

und es gilt:

$$
\begin{aligned}
& \partial_{1\square} e_{\beta_0(C)} = \varphi(\partial_1) = 1 - s_{-1}\varepsilon_\square \\
\Longrightarrow \quad & \partial_{1\square} s_0 = 1 - s_{-1}\varepsilon_\square
\end{aligned}
$$

Es folgt:

$$
\begin{aligned}
& \varepsilon_\square \partial_{1\square} s_0 = \varepsilon_\square - \varepsilon_\square s_{-1}\varepsilon_\square \\
\Longrightarrow \quad & (\varepsilon\partial_1)_\square s_0 = 0 \\
\Longrightarrow \quad & (\varepsilon\partial_1)_\square = 0 \quad \text{nach Eindeutigkeit der Faktorisierung in Lemma 6.2} \\
\Longrightarrow \quad & \varepsilon\partial_1 = 0 \quad \text{nach Volltreuheit von } \square
\end{aligned}
$$

Ist ∂_n konstruiert, so ergibt sich ∂_{n+1} aus:

$$1 - s_{n-1}\partial_{n\Box} : \beta_n(C)_\Box \dashrightarrow \beta_n(C)_\Box$$

also

$$\partial_{n+1} : \beta_{n+1}(C) \longrightarrow \beta_n(C)$$

mit

$$\partial_{n+1\Box} s_n = 1 - s_{n-1}\partial_{n\Box}$$

Es folgt:

$$\begin{aligned} \partial_{n\Box}\partial_{n+1\Box} s_n &= \partial_{n\Box} - \partial_{n\Box} s_{n-1}\partial_{n\Box} \\ &= \partial_{n\Box} - (1 - s_{n-2}\partial_{n-1\Box})\partial_{n\Box} \\ &= s_{n-2}\partial_{n-1\Box}\partial_{n\Box} \\ &= 0 \end{aligned}$$

$\Longrightarrow \quad \partial_n\partial_{n+1} = 0$ wieder nach Eindeutigkeit der Faktorisierung und der Volltreuheit von $\Box$.

$\Longrightarrow \quad \partial_{n\Box} - \partial_{n\Box} s_{n-1}\partial_{n\Box} = 0$, also insbesondere ist ∂_n zulässig.

Nach Konstruktion gilt:

$$\varepsilon_\Box s_{-1} = \mathrm{id}_{C_\Box}$$

und

$$\partial_{n+1\Box} s_n = 1 - s_{n-1}\partial_{n\Box}$$

Damit ist s als zusammenziehbare Homotopie in $\mathcal{C}_k$ erkannt. Es folgt die Behauptung.

$\Box$

Die kanonische Auflösung bildet die Grundlage für die Definition von relativen Extensionsfunktoren.

Definition 6.9 (Relative Extensionsfunktoren). Sei $A, C \in \mathcal{C}_R$.
Sei $\beta(C)$ Bar-Auflösung von C, dann heißen

$$\mathrm{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C, A) := H^n(\mathrm{Hom}_{\mathcal{C}_R}(\beta(C), A))$$

relative Extensionsfunktoren.

Wie in der nicht relativen Homologietheorie ergibt sich nun:

Folgerung 6.10.
1.) Ist $X \xrightarrow{\varepsilon} C$ *zulässige, relativ projektive Auflösung von* C*, so gilt:*

$$\operatorname{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C, A) \cong H^n(\operatorname{Hom}_{\mathcal{C}_R}(X, A))$$

2.) Sind

$$0 \longrightarrow C^{‘} \longrightarrow C \longrightarrow C^{“} \longrightarrow 0$$

$$0 \longrightarrow A^{‘} \longrightarrow A \longrightarrow A^{“} \longrightarrow 0$$

exakte, $\square$*-spaltende Sequenzen in* $\mathcal{C}_R$*, so gibt es lange exakte Sequenzen:*

$$\cdots\cdots\to \operatorname{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C^{''}, A) \longrightarrow \operatorname{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C, A) \longrightarrow \operatorname{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C^{'}, A) \longrightarrow \operatorname{Ext}^{n+1}_{\mathcal{C}_R/\mathcal{C}_k}(C^{''}, A) \cdots\cdots\to$$

$$\cdots\cdots\to \operatorname{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C, A^{'}) \longrightarrow \operatorname{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C, A) \longrightarrow \operatorname{Ext}^n_{\mathcal{C}_R/\mathcal{C}_k}(C, A^{''}) \longrightarrow \operatorname{Ext}^{n+1}_{\mathcal{C}_R/\mathcal{C}_k}(C, A^{'}) \cdots\cdots\to$$

6.2 Relative Homologietheorie und Cohomologietheorie für Algebren

Die Ergebnisse aus 6.1 werden nun auf k-Algebren angewandt.
Sei k kommutativer Ring, R eine k-Algebra. Es seien mit $\mathcal{C}_R$ die Kategorie der links-R-Moduln und mit $\mathcal{C}_k$ die Kategorie der k-Moduln bezeichnet. **Im folgenden sei $\otimes_k$ kurz mit $\otimes$ bezeichnet. Ebenso sei im folgenden $\mathbf{R}^{\otimes \mathbf{n}} := \underbrace{R \otimes \cdots \otimes R}_{\text{n-Stück}}$ wobei $\mathbf{R}^{\otimes \mathbf{0}} := \mathbf{k}$.**

Satz 6.11. *Es gibt Funktoren:*

$$\square : \mathcal{C}_R \longrightarrow \mathcal{C}_k \quad \textit{und} \quad F : \mathcal{C}_k \longrightarrow \mathcal{C}_R$$

die die Bedingungen aus Abschnitt 6.1 erfüllen.

Beweis. Sei

$$\begin{aligned} \square : \mathcal{C}_R &\longrightarrow \mathcal{C}_k \\ A &\longmapsto A_\square \quad \text{„Vergißfunktor“} \end{aligned}$$

und

$$\begin{aligned} F : \mathcal{C}_k &\longrightarrow \mathcal{C}_R \\ M &\longmapsto R \otimes_k M \end{aligned}$$

Offenbar ist $\square$ linear, exakt und volltreu. Zu zeigen bleibt die Adjungiertheitseigenschaft, also die Existenz eines Isomorphismus

$$\varphi : \operatorname{Hom}_R(FM, A) \longrightarrow \operatorname{Hom}_k(M, A_\square) \quad \text{für alle } M \in \mathcal{C}_k \text{ und } A \in \mathcal{C}_R.$$

Ist $\alpha \in \mathrm{Hom}_R(R \otimes_k M, A)$, so setze

$$\begin{aligned} \varphi(\alpha) : M &\longrightarrow A_\square \\ m &\longmapsto \alpha(1 \otimes m) \end{aligned}$$

Ist $s \in \mathrm{Hom}_k(M, A_\square)$, so setze

$$\begin{aligned} \psi(s) : R \otimes_k M &\longrightarrow A \\ \lambda \otimes m &\longmapsto \lambda s(m) \end{aligned}$$

Es folgt:

$$\begin{aligned} \psi(\varphi(\alpha)) : R \otimes_k M &\longrightarrow A \\ \lambda \otimes m &\longmapsto \lambda\varphi(\alpha)(m) = \lambda\alpha(1 \otimes m) = \alpha(\lambda \otimes m) \end{aligned}$$

und

$$\begin{aligned} \varphi(\psi(s)) : M &\longrightarrow A_\square \\ m &\longmapsto \psi(s)(1 \otimes m) = 1s(m) = s(m) \end{aligned}$$

$\Rightarrow$ φ und ψ sind zueinander inverse Isomorphismen. Die funktorielle Verträglichkeit ergibt sich durch eine analoge Rechnung. $\square$

Folgerung 6.12. *Nach Lemma 6.2 auf Seite 34 ergibt sich ein Morphismus*

$$\begin{aligned} e_M = \varphi(\mathrm{id}_{FM}) : M &\longrightarrow \square FM = R \otimes_k M \\ m &\longmapsto 1 \otimes m \end{aligned}$$

Satz 6.13 (Bar-Auflösung). *Sei C links-R-Modul, dann gibt es eine relativ freie, zulässige Auflösung (Bar-Auflösung) $\beta(C)$:*

$$0 \longleftarrow C \underset{s_{-1}}{\overset{\varepsilon}{\rightleftarrows}} \underbrace{R \otimes_k C}_{\beta_0(C)} \underset{s_0}{\overset{\partial_1}{\rightleftarrows}} \underbrace{R \otimes_k R \otimes_k C}_{\beta_1(C)} \underset{s_1}{\overset{\partial_2}{\rightleftarrows}} \cdots \tag{6.13.1}$$

mit

$$\begin{aligned} \varepsilon : R \otimes_k C &\longrightarrow C \\ \lambda \otimes c &\longmapsto \lambda c \end{aligned}$$

$$\begin{aligned} s_{-1} : C &\longrightarrow R \otimes_k C \\ c &\longmapsto 1 \otimes c \end{aligned}$$

$$\begin{aligned} s_n : \beta_n(C) &\longrightarrow R \otimes_k \beta_n(C) = \beta_{n+1}(C) \\ r_0 \otimes \cdots \otimes r_n \otimes c &\longmapsto 1 \otimes r_0 \otimes \cdots \otimes r_n \otimes c \end{aligned}$$

und

$$\partial_n : \beta_n(C) \longrightarrow \beta_{n-1}(C)$$
$$\partial_n := \sum_{i=0}^{n} (-1)^i \triangle_i$$

wobei $\triangle_i$ definiert ist durch:

$$\begin{aligned} \triangle_i : \beta_n(C) &\longrightarrow \beta_{n-1}(C) \\ r_0 \otimes \cdots \otimes r_n \otimes c &\longmapsto \begin{cases} r_0 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n \otimes c & \textit{für } i \neq n \\ r_0 \otimes \cdots \otimes r_n c & \textit{für } i = n \end{cases} \end{aligned}$$

Beweis. Zu zeigen ist die Übereinstimmung der angegebenen Morphismen mit den Konstruktionen nach Satz 6.8 auf Seite 37. Für ε und s_i folgt dies direkt aus den Definitionen. Für ∂_n liefert eine Induktion nach n das gewünschte Ergebnis:

$n = 1$: Zu berechnen ist $\psi(1 - s_{-1}\varepsilon_{\square})$, also

$$\begin{aligned} R \otimes R \otimes C &\longrightarrow R \otimes C \\ r_0 \otimes r_1 \otimes c &\longmapsto r_0(r_1 \otimes c - 1 \otimes r_1 c) = r_0 r_1 \otimes c - r_0 \otimes r_1 c = \partial_1(r_0 \otimes r_1 \otimes c) \end{aligned}$$

$n > 1$: Induktiv berechnet sich ∂_{n+1} nun als $\psi(1 - s_{n-1}\partial_{n\square})$:

$$\begin{aligned} \beta_{n+1}(C) &\longrightarrow \beta_n(C) \\ r_0 \otimes \cdots \otimes r_{n+1} \otimes c &\longmapsto r_0\Big(r_1 \otimes \cdots \otimes r_{n+1} \otimes c \\ &\qquad - 1 \otimes \sum_{i=0}^{n} (-1)^i \triangle_i(r_1 \otimes \cdots \otimes r_{n+1} \otimes c)\Big) \\ &= r_0 r_1 \otimes \cdots \otimes r_{n+1} \otimes c \\ &\qquad + r_0 \sum_{i=1}^{n+1} (-1)^i \triangle_i(1 \otimes r_1 \otimes \cdots \otimes r_{n+1} \otimes c) \\ &= \partial_{n+1}(r_0 \otimes \cdots \otimes r_{n+1} \otimes c) \end{aligned}$$

□

Bemerkung 6.14. Ist G ein rechts-R-Modul, so ergibt sich analog eine Bar-Auflösung $\beta(G)$ der Form:

(6.14.1) $$0 \longleftarrow G \underset{s_{-1}}{\overset{\varepsilon}{\leftrightarrows}} \underbrace{G \otimes_k R}_{\beta_0(C)} \underset{s_0}{\overset{\partial_1}{\leftrightarrows}} \underbrace{G \otimes_k R \otimes_k R}_{\beta_1(C)} \underset{s_1}{\overset{\partial_2}{\leftrightarrows}} \cdots$$

Definition 6.15.

1. Nach Definition 6.9 auf Seite 39 ergeben sich nun *relative Extensionsfunktoren*
$$\mathrm{Ext}^n_{R/k}(C, A) := H^n(\mathrm{Hom}_R(\beta(C), A))$$
für C, A links-R-Moduln.

2. Es lassen sich nun auch relative Torsionsfunktoren definieren: Ist G rechts-R-Modul und C links-R-Modul, so heißen
$$\mathrm{Tor}^{R/k}_n(G, C) := H_n(\beta(G) \otimes_R C) \cong H_n(G \otimes_R \beta(C)$$
relative Torsionsfunktoren.

Zur Definition der Hochschild-Homologie werden noch einige technische Hilfsmittel benötigt:

Bi-Moduln

Sei k kommutativer Ring, R eine k-Algebra. M heißt R-Bi-Modul falls M sowohl links als auch rechts R-Modul ist und es gilt:
$$\lambda(m\mu) = (\lambda m)\mu \quad \text{für alle } \lambda, \mu \in R, m \in M$$
Eine Abbildung $f : M \longrightarrow N$ ist ein Morphismus von Bi-Moduln, falls gilt:
$$f(\lambda m \mu) = \lambda f(m)\mu$$
Die Menge aller solcher Morphismen wird mit $\mathrm{Hom}_{R-R}(M, N)$ bezeichnet. Die Bi-Moduln über R werden dadurch zu einer Kategorie. Diese wird mit $\mathcal{C}_{R-R}$ bezeichnet.

Definition 6.16 (Tensorprodukte). Sind M, N R-Bi-Moduln, so wird das Tensorprodukt $M \otimes_{R-R} N$ definiert als Quotient des k-Moduls $M \otimes_k N$ mit den Relationen:
$$\begin{aligned} m\lambda \otimes n &= m \otimes \lambda n \\ \lambda m \otimes n &= m \otimes n\lambda \end{aligned} \tag{6.16.1}$$

Lemma 6.17. Ist M R-Bi-Modul, N k-Modul, so gibt es einen kanonischen Isomorphismus von Bi-Moduln:
$$\begin{aligned} \theta : M \otimes_{R-R} (R \otimes N \otimes R) &\longrightarrow M \otimes N \\ m \otimes (\lambda \otimes n \otimes \mu) &\longmapsto \mu m \lambda \otimes n \end{aligned}$$

Beweis. Die Abbildung θ ist verträglich mit den Gleichungen (6.16.1) und die Umkehrabbildung wird gegeben durch $\theta^{-1}(m \otimes n) = m \otimes (1 \otimes n \otimes 1)$. □

Die einhüllende Algebra R^e

Definition 6.18 (opponierter Ring). Ist R beliebiger Ring, so ist der *opponierte* Ring R^{op} gegeben durch:

1. Als abelsche Gruppe ist $R^{\mathrm{op}} = R$.
2. Sind $\lambda^*, \mu^* \in R^{\mathrm{op}}$, so gelte: $\lambda^*\mu^* := (\lambda\mu)^*$.

Definition 6.19 (einhüllende Algebra). Ist R eine k-Algebra, so ist die *einhüllende Algebra* R^e definiert durch:

$$R^e := R \otimes R^{\mathrm{op}}$$

insbesondere gilt:

$$\begin{aligned}(a \otimes b^*)(c \otimes d^*) &= ac \otimes b^*d^* \\ &= ac \otimes (db)^*\end{aligned}$$

Satz 6.20. *Die Kategorien Bi-Moduln über R, links-R^e-Moduln, rechts-R^e-Moduln sind äquivalent.*

Beweis. Ist M R-Bi-Modul, so definiere $(a \otimes b^*)m := amb$. Es folgt:

$$\begin{aligned}(a \otimes b^*)(c \otimes d^*)m &= (a \otimes b^*)cmd \\ &= acmdb \\ &= (ac \otimes (db)^*)m\end{aligned}$$

Dies zeigt die Wohldefiniertheit der links-R^e-Modul Struktur. Für die Rechts-Modul-Struktur definiere $m(a \otimes b^*) := bma$. Es ergibt sich die Assoziativität aus:

$$\begin{aligned}m(a \otimes b^*)(c \otimes d^*) &= bma(c \otimes d^*) \\ &= dbmac \\ &= m(ac \otimes (db)^*)\end{aligned}$$

Ist andererseits M ein links-R^e-Modul, so wird dieser zu einem Bi-Modul durch:

$$amb := (a \otimes b^*)m$$

Analog wird aus einem rechts-R^e-Modul ein Bi-Modul durch:

$$amb := m(b \otimes a^*)$$

Und schließlich wird aus einem rechts-R^e-Modul ein links-R^e-Modul durch:

$$(a \otimes b^*)m := m(b \otimes a^*)$$

□

Folgerung 6.21. *Die Kategorie der R-Bi-Moduln $\mathcal{C}_{R-R}$ ist eine abelsche Kategorie.*

6.3 Hochschild(Co-)homologie-Gruppen

R selbst ist in kanonischer Weise sowohl R^e-links- als auch R^e-rechts-Modul.

Satz 6.22. *Die Bar-Auflösung $\beta(R)$ von R bezüglich $\mathcal{C}_R/\mathcal{C}_k$ ist eine relativ freie, zulässige Auflösung von R bezüglich $\mathcal{C}_{R^e}/\mathcal{C}_k$.*

Zunächst das folgende Lemma:

Lemma 6.23. Ist M k-Modul, so gibt es einen Isomorphismus von links-R^e-Modul:

$$\begin{aligned} R^e \otimes M &\longrightarrow R \otimes M \otimes R \\ a \otimes b^* \otimes m &\longmapsto a \otimes m \otimes b \end{aligned}$$

Beweis. Fraglich ist nur, ob die R^e-Linearität gegeben ist:

$$\begin{array}{ccc} (c \otimes d^*)a \otimes b^* \otimes m & \longmapsto & (c \otimes d^*)a \otimes m \otimes b \\ \| & & \| \\ ca \otimes (bd)^* \otimes m & \longmapsto & ca \otimes m \otimes bd \end{array}$$

Paßt also. $\square$

Beweis von Satz 6.22. Nach Definition ist

$$\beta_0(R) = R \otimes R \cong R^e \otimes k$$

und

$$\beta_n(R) = R \otimes R^{\otimes n} \otimes R \cong R^e \otimes R^{\otimes n}$$

Die $\beta_n(R)$ sind damit relativ freie R^e/k-Moduln. Mit Hilfe der expliziten Formeln für die Abbildungen ε und ∂_n nach Satz 6.13 ergibt sich, daß diese Abbildungen Bi-Modul-Homomorphismen oder äquivalent R^e-linear sind. Die s_i bleiben natürlich weiterhin k-linear, und $\beta(R)$ wird dadurch zu einer relativ freien, zulässigen Auflösung von R bezüglich $\mathcal{C}_{R^e}/\mathcal{C}_k$. $\square$

Es folgt:

$$H^n_{R^e/k}(R, M) = H^n(\mathrm{Hom}_{R^e}(\beta(R), M))$$

und

$$H_n^{R^e/k}(R, M) = H_n(M \otimes_{R^e} \beta(R))$$

Definition 6.24. Die k-Moduln $H^n_{R^e/k}(R, M)$ und $H_n^{R^e/k}(R, M)$ heißen *Hochschildcohomologiegruppen* bzw. *Hochschildhomologiegruppen.*

6.4 Hochschildkomplexe

Lemma 6.25. Sei M ein R-Bi-Modul, dann gibt es Isomorphismen von k-Moduln:

1. $\mathrm{Hom}_{R^e}(R^{\otimes n+2}, M) \cong \mathrm{Hom}_k(R^{\otimes n}, M)$
2. $M \otimes_{R^e} R^{\otimes n+2} \cong M \otimes R^{\otimes n}$

Beweis. Die gesuchten Isomorphismen lauten:

$$\begin{aligned} \alpha : \mathrm{Hom}_{R^e}(R^{\otimes n+2}, M) &\longrightarrow \mathrm{Hom}_k(R^{\otimes n}, M) \\ f &\longmapsto \alpha(f) \quad \text{mit} \\ &\qquad \alpha(f)(r_1 \otimes \cdots \otimes r_n) := f(1 \otimes r_1 \otimes \cdots \otimes r_n \otimes 1) \end{aligned}$$

α^{-1} ergibt sich dann mit:

$$\begin{aligned} \alpha^{-1} : \mathrm{Hom}_k(R^{\otimes n}, M) &\longrightarrow \mathrm{Hom}_{R^e}(R^{\otimes n+2}, M) \\ F &\longmapsto \alpha^{-1}(F) \quad \text{mit} \\ &\qquad \alpha^{-1}(F)(r_0 \otimes \cdots \otimes r_{n+1}) := r_0 F(r_1 \otimes \cdots \otimes r_n) r_{n+1} \end{aligned}$$

und

$$\begin{aligned} \gamma : M \otimes_{R^e} R^{\otimes n+2} &\longrightarrow M \otimes R^{\otimes n} \\ m \otimes (r_0 \otimes \cdots \otimes r_{n+1}) &\longmapsto r_{n+1} m r_0 \otimes r_1 \otimes \cdots \otimes r_n \end{aligned}$$

und für γ^{-1} ergibt sich:

$$\begin{aligned} \gamma^{-1} : M \otimes R^{\otimes n} &\longrightarrow M \otimes_{R^e} R^{\otimes n+2} \\ m \otimes r_1 \otimes \cdots \otimes r_n &\longmapsto m \otimes (1 \otimes r_1 \otimes \cdots \otimes r_n \otimes 1) \end{aligned}$$

□

Satz 6.26. *Mit Hilfe des Lemmas lassen sich die Komplexe* $\mathrm{Hom}_{R^e}(\beta(R), M)$ *und*
$M \otimes_{R^e} \beta(R)$ *noch ein wenig kompakter beschreiben:*

1. $\mathrm{Hom}_{R^e}(\beta(R), M)$:

$$(6.26.1)\quad 0 \longrightarrow M \xrightarrow{\delta^1} \mathrm{Hom}_k(R, M) \xrightarrow{\delta^2} \mathrm{Hom}_k(R^{\otimes 2}, M) \longrightarrow \cdots$$

mit

$$(\Delta^{i''} f)(r_1 \otimes \cdots \otimes r_n) = \begin{cases} r_1 f(r_2 \otimes \cdots \otimes r_n) & i = 0 \\ f(r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n) & 0 < i < n \\ f(r_1 \otimes \cdots \otimes r_{n-1}) r_n & i = n \end{cases}$$

und

$$\delta^n = \sum_{i=0}^{n} (-1)^i \Delta^{i''}$$

Beweis. Nach Lemma 6.25 auf der vorherigen Seite und Satz 6.13 auf Seite 41 ergibt sich mit $\Delta^{i'} := \mathrm{Hom}_{R^e}(\Delta_i, \mathrm{id}_M)$ das kommutative Diagramm:

$$\begin{tikzcd} \mathrm{Hom}_{R^e}(R^{\otimes n+1}, M) \arrow[r, "\Delta^{i'}"] \arrow[d, "\alpha"'] & \mathrm{Hom}_{R^e}(R^{\otimes n+2}, M) \arrow[d, "\alpha"] \\ \mathrm{Hom}_k(R^{\otimes n-1}, M) \arrow[r, "\Delta^{i''}"] & \mathrm{Hom}_k(R^{\otimes n}, M) \end{tikzcd}$$

Das definiert $\Delta^{i''}$ und es folgt:

$$\begin{aligned} (\Delta^{i''} f)(r_1 \otimes \cdots \otimes r_n) &= (\alpha \Delta^{i'} \alpha^{-1} f)(r_1 \otimes \cdots \otimes r_n) \\ &= (\Delta^{i'} \alpha^{-1} f)(1 \otimes r_1 \otimes \cdots \otimes r_n \otimes 1) \\ &= \begin{cases} (\alpha^{-1} f)(r_1 \otimes \cdots \otimes r_n \otimes 1) & i = 0 \\ (\alpha^{-1} f)(1 \otimes r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n \otimes 1) & 0 < i < n \\ (\alpha^{-1} f)(1 \otimes r_1 \otimes \cdots \otimes r_n) & i = n \end{cases} \\ &= \begin{cases} r_1 f(r_2 \otimes \cdots \otimes r_n) & i = 0 \\ f(r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n) & 0 < i < n \\ f(r_1 \otimes \cdots \otimes r_{n-1}) r_n & i = n \end{cases} \end{aligned}$$

□

2. $M \otimes_{R^e} \beta(R)$:

(6.26.2) $$0 \longleftarrow M \xleftarrow{d_1} R \xleftarrow{d_2} R^{\otimes 2} \xleftarrow{d_3} \cdots$$

mit

$$\nabla_i''(m \otimes r_1 \otimes \cdots \otimes r_n) = \begin{cases} m r_1 \otimes r_2 \otimes \cdots \otimes r_n & i = 0 \\ m \otimes r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_2 r_n & 0 < i < n \\ r_n m \otimes r_1 \otimes \cdots \otimes r_{n-1} & i = n \end{cases}$$

und

$$d_n = \sum_{i=0}^{n} (-1)^i \nabla_i''$$

Beweis. Wiederum mit Lemma 6.25 und Satz 6.13 ergibt sich das ∇_i'' definierende Diagramm mit $\nabla_i' := \mathrm{id}_M \otimes_{R^e} \Delta_i$:

$$\begin{tikzcd}
M \otimes_{R^e} R^{\otimes n+2} \arrow[r, "\nabla_i'"] \arrow[d, "\gamma"'] & M \otimes_{R^e} R^{\otimes n+1} \arrow[d, "\gamma"] \\
M \otimes R^{\otimes n} \arrow[r, "\nabla_i''"] & M \otimes R^{\otimes n-1}
\end{tikzcd}$$

Also

$$\begin{aligned}
\nabla_i''(m \otimes r_1 \otimes \cdots \otimes r_n) &= \gamma \nabla_i' \gamma^{-1}(m \otimes r_1 \otimes \cdots \otimes r_n) \\
&= \gamma \nabla_i'(m \otimes 1 \otimes r_1 \otimes \cdots \otimes r_n \otimes 1) \\
&= \begin{cases} \gamma(m \otimes r_1 \otimes \cdots \otimes r_n \otimes 1) & i = 0 \\ \gamma(m \otimes 1 \otimes r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n \otimes 1) & 0 < i < n \\ \gamma(m \otimes 1 \otimes r_1 \otimes \cdots \otimes r_n) & i = n \end{cases} \\
&= \begin{cases} m r_1 \otimes r_2 \otimes \cdots \otimes r_n & i = 0 \\ m \otimes r_1 \otimes \cdots \otimes r_i r_{i+1} \otimes \cdots \otimes r_n) & 0 < i < n \\ r_n m \otimes r_1 \otimes \cdots \otimes r_{n-1} & i = n \end{cases}
\end{aligned}$$

□

Folgerung 6.27. *Die Hochschildhomologie- bzw. Cohomologiegruppen ergeben sich als n-te (Co-)Homologie der beiden* Hochschild-Komplexe (6.26.1) *und* (6.26.2)*. Sie wurden von Hochschild ursprünglich zur Definition „seiner“ Gruppen benutzt.*

Folgerung 6.28.

1. $H_0(R, M) = M/[M, R]$. *Hierbei ist* $[M, R]$ *der von Elementen der Form* $mr - rm$ *mit* $m \in M$, $r \in R$ *erzeugte* k*-Untermodul von* M.

2. $H^0(R, M) = \{m \in M : rm = mr \; \forall \, r \in R\}$

Algebren über Körpern

Ist k ein Körper, wird alles wieder ein wenig einfacher:

Satz 6.29. *Für einen Körper k stimmen die Hochschild(co)homolgien mit den absoluten* Ext *und* Tor *Gruppen überein:*

$$H_*(R,M) \cong \operatorname{Tor}_*^{R^e}(M,R)$$
$$H^*(R,M) \cong \operatorname{Ext}_{R^e}^*(R,M)$$

Zum Beweis wird das folgende Lemma benötigt:

Lemma 6.30. Sei k kommutativer Ring. Seien P, Q k-Moduln, so gilt:

1. P, Q flach $\Rightarrow P \otimes Q$ flach.
2. P, Q projektiv $\Rightarrow P \otimes Q$ projektiv.

Beweis.

1. Zu zeigen ist die Exaktheit des Funktors $(P \otimes Q) \otimes \_$. Diese ergibt sich aus der Isomorphie:
$$(P \otimes Q) \otimes \_ \cong P \otimes (Q \otimes \_)$$
2. Die Exaktheit des Funktors $\operatorname{Hom}(P \otimes Q, \_)$ ergibt sich aus der Isomorphie
$$\operatorname{Hom}(P \otimes Q, \_) \cong \operatorname{Hom}(P, \operatorname{Hom}(Q, \_))$$

□

Beweis von Satz 6.29. Zu zeigen ist, daß die Bar-Auflösung 6.13.1 auf Seite 41 nach Satz 6.13 auf Seite 41 eine flache, bzw. projektive Auflösung des R^e-Moduls R ist, falls R flacher bzw. projektiver k-Modul ist.

1. Sei zunächst R projektiver k-Modul. Nach Lemma 6.30 ist auch $\beta(R)_n = R^{\otimes n+2}$ projektiver k-Modul. Daraus folgt die Exaktheit der Funktoren
$$\operatorname{Hom}_k(R^{\otimes n-2}, \_) \cong \operatorname{Hom}_{R^e}(R^{\otimes n}, \_)$$
und die Projektivität der R^e-Moduln $\beta(R)_n$.
2. Ist R flacher k-Modul, so folgt die Behauptung analog aus der Isomorphie
$$R^{\otimes n+2} \otimes_{R^e} \_ \cong R^{\otimes n} \otimes \_$$
Ist k sogar Körper, so ist R (und jeder andere k-Modul) flach und projektiv. Es folgt die Behauptung.

$\square$

Die Hochschildhomolgie bildet ein wichtiges Werkzeug zur Beschreibung von k-Algebren. Mit ihrer Hilfe läßt sich beispielsweise ein homologischer Dimensionsbegriff formulieren. Für eine gründliche Einführung in die Theorie der Hochschildhomolgie sei an die „Klassiker“ [Mac69, Chapter X] und [CE56, Chapter IX] verwiesen.

7 $\mathbf{H^2(R, M)}$ und glatte Algebren

Ziel des Abschnitts ist die Beschreibung der zweiten Cohomologie einer k-Algebra R. Es stellt sich heraus, daß die Elemente von $H^2(R, M)$ genau einem besonderen Typ von Extensionen, den sogenannten *Hochschildextensionen*, entsprechen.
Ist k Körper und $H^2(R, M) = 0$ für alle Bi-Moduln M, dann erfüllt R eine Liftungseigenschaft. R heißt in diesem Fall *glatte* k-Algebra.

7.1 Hochschildextensionen

Definition 7.1. Sei R eine k-Algebra. Eine *singuläre Extension* von R ist ein surjektiver Algebrenhomomorphismus $\sigma : E \longrightarrow R$ einer k-Algebra E mit $\ker(\sigma)^2 = 0$.

$J := \ker(\sigma)$ ist R-Bi-Modul durch

$$\begin{aligned} rj &:= \sigma^{-1}(r)j \quad \text{bzw.} \\ jr &:= j\sigma^{-1}(r) \end{aligned}$$

Dies ist wohldefiniert, denn sind $e_1, e_2 \in \sigma^{-1}(r)$, so folgt $e_1 = e_2 + j'$ mit $j' \in J$.

$$\begin{aligned} \Rightarrow e_1 j &= (e_2 + j')j \\ &= e_2 j + \underbrace{j'j}_{=0} \end{aligned}$$

Analoges gilt für je_1.

Definition 7.2.

1. Sei $0 \longrightarrow J \longrightarrow E \longrightarrow R \longrightarrow 0$ singuläre Extension von R. Sei M ein R-Bi-Modul mit $M \cong J$ als R-Bi-Modul, dann heißt

   $0 \longrightarrow M \longrightarrow E \longrightarrow R \longrightarrow 0$ *singuläre Extension* von R durch M.

2. Ist die Sequenz $0 \longrightarrow M \longrightarrow E \longrightarrow R \longrightarrow 0$ sogar k-spaltend, so heißt sie *Hochschildextension* von R durch M.

3. Zwei Hochschildextensionen von R durch M heißen *äquivalent*, falls es einen Ring-Isomorphismus $\varphi : E \longrightarrow E'$ gibt, so daß das folgende Diagramm kommutiert:

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r] \arrow[d, equal] & E \arrow[r] \arrow[d, "\varphi"'] & R \arrow[r] \arrow[d, equal] & 0 \\ 0 \arrow[r] & M \arrow[r] & E' \arrow[r] & R \arrow[r] & 0 \end{tikzcd}$$

Beispiel 7.3. Sei $R \oplus M$ direkte Summe als k-Modul. $R \oplus M$ wird Ring durch:

$$(r_1, m_1)(r_2, m_2) := (r_1 r_2, r_1 m_2 + m_1 r_2)$$

Die Hochschildextension

$$0 \longrightarrow M \longrightarrow R \oplus M \longrightarrow R \longrightarrow 0$$

heißt *triviale Hochschildextension* von R durch M.

Die Hochschildextensionen beschreiben die zweite Cohomologie vollständig. Dies zeigt der folgende Satz:

Satz 7.4. *Sei R k-Algebra, M R-Bi-Modul. Es gibt eine kanonische Bijektion von Mengen:*

$$\{\text{\textit{Äquivalente Hochschildextensionen von } } R \text{ \textit{durch} } M\} \cong H^2(R, M)$$

Das triviale Element von $H^2(R, M)$ entspricht hierbei der trivialen Extension.

Beweis.

1. Sei

$$\begin{tikzcd} 0 \arrow[r] & M \arrow[r, "\chi"] & E \arrow[r, shift left, "\sigma"] & R \arrow[l, shift left, dashed, "s"] \arrow[r] & 0 \end{tikzcd}$$

eine Hochschildextension mit einem k-linearen Schnitt s. Die Abbildung s ist i. allg. kein Ringhomomorphismus. Die *Faktorabbildung* f beschreibt diese Abweichung:

$$\begin{aligned} f : R \times R &\longrightarrow M \\ (r_1, r_2) &\longmapsto s(r_1)s(r_2) - s(r_1 r_2) \end{aligned}$$

definiert. f ist k-bilinear und wohldefiniert:

$$\begin{aligned}\sigma(s(r_1)s(r_2) - s(r_1r_2)) &= \sigma s(r_1)\sigma s(r_2) - \sigma s(r_1r_2)\\ &= r_1r_2 - r_1r_2 = 0\end{aligned}$$

wobei der Einfachheit halber M mit $\chi(M)$ identifiziert wird. Die E-Modul-Struktur wird durch $em := \sigma(e)m$, bzw. $me := m\sigma(e)$ gegeben . Mit Hilfe von f läßt sich nun die multiplikative Struktur von $E \cong R \oplus M$ beschreiben:

$$(r_1, m_1)(r_2, m_2) = (r_1r_2, r_1m_2 + m_1r_2 + f(r_1, r_2)) \tag{7.4.1}$$

Dies ergibt sich aus der folgenden Betrachtung:

Sind $e_1 = \sigma(r_1) + m_1$ und $e_2 = \sigma(r_2) + m_2$ gegeben, so folgt:

$$\begin{aligned}e_1e_2 &= \sigma(r_1)\sigma(r_2) + \sigma(r_1)m_2 + m_1\sigma(r_2) + \underbrace{m_1m_2}_{=0}\\ &= \sigma(r_1r_2) + f(r_1, r_2) + r_1m_2 + m_1r_2\end{aligned}$$

2. Ist $\varphi : E \longrightarrow E'$ Äquivalenz zweier Hochschildextensionen:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r, "\chi_1"] \arrow[d, equal] & E \arrow[r, shift left, "\sigma_1"] \arrow[d, "\varphi"'] & R \arrow[l, dashed, shift left, "s_1"] \arrow[r] \arrow[d, equal] & 0 \\
0 \arrow[r] & M \arrow[r, "\chi_2"] & E' \arrow[r, shift left, "\sigma_2"] & R \arrow[l, dashed, shift left, "s_2"] \arrow[r] & 0
\end{tikzcd}$$

so gilt:

$$\begin{aligned}\chi_2(m') &:= s_2(r_1)s_2(r_2) - s_2(r_1r_2)\\ &= \varphi s_1(r_1)\varphi s_1(r_2) - \varphi s_1(r_1r_2)\\ &= \varphi(s_1(r_1)s_1(r_2) - s_1(r_1r_2)) = \varphi(\chi_1(m))\end{aligned}$$

mit geeigneten m und m'. Weiterhin gilt: $\chi_2(m) = \varphi\chi_1(m) = \chi_2(m')$. Aus der Injektivität von χ_2 folgt $m = m'$, insbesondere $f_1(r_1, r_2) = f_2(r_1, r_2)$.

$\Rightarrow$ Zwei äquivalente Extensionen haben dieselbe Faktorabbildung.

3. Ist f eine Faktorabbildung, so folgt aus der Assoziativität des Produkts in E folgende Zusatzbedingung für f:

$$\begin{aligned}s(r_0)(s(r_1)s(r_2)) &= s(r_0)(f(r_1, r_2) + s(r_1r_2))\\ &= r_0f(r_1, r_2) + s(r_0r_1r_2) + f(r_0, r_1r_2)\end{aligned}$$

und

$$
\begin{aligned}
(s(r_0)s(r_1))s(r_2) &= (s(r_0r_1) + f(r_0, r_1))s(r_2) \\
&= s(r_0r_1r_2) + f(r_0r_1, r_2) + f(r_0, r_1)r_2
\end{aligned}
$$

Also insgesamt:

$$
r_0 f(r_1, r_2) - f(r_0r_1, r_2) + f(r_0, r_1r_2) - f(r_0, r_1)r_2 = 0 \tag{7.4.2}
$$

4. Ist andererseits $f \in \mathrm{Hom}_k(R^{\otimes 2}, M)$ und erfüllt 7.4.2, so definiert f eine Extension:
$$0 \longrightarrow M \longrightarrow R \oplus M \longrightarrow R \longrightarrow 0$$
mit Ringstruktur auf $R \oplus M$ gegeben durch (7.4.1).

5. Ist $0 \longrightarrow M \longrightarrow E \longrightarrow R \longrightarrow 0$ Extension und s_1, s_2 zwei Schnitte, so ist $s_2 = s_1 + (s_2 - s_1) = s_1 + g$ mit $g \in \mathrm{Hom}_k(R, M)$. Sind f_1, f_2 die zugehörigen Faktorabbildungen, so folgt:
$$
\begin{aligned}
f_2(r_1, r_2) &= (s_1 + g)(r_1)(s_1 + g)(r_2) - (s_1 + g)(r_1r_2) \\
&= f_1(r_1, r_2) + r_1 g(r_2) + g(r_1)r_2 - g(r_1r_2) + \underbrace{g(r_1)g(r_2)}_{=0} \\
&= f_1(r_1, r_2) + \delta^2 g(r_1, r_2)
\end{aligned}
$$
mit $\delta^2 : \mathrm{Hom}_k(R, M) \longrightarrow \mathrm{Hom}_k(R^{\otimes 2}, M)$ aus 6.26.1 auf Seite 46.

6. Mit derselben Formeln nach läßt sich nun $H^2(R, M)$ beschreiben:

   Co-Ränder: $f \in \mathrm{Hom}_k(R^{\otimes 2}, M)$ mit
$$r_0 f(r_1, r_2) - f(r_0r_1, r_2) + f(r_0, r_1r_2) - f(r_0, r_1)r_2 = 0$$

   Co-Bilder: Ist $f \in \mathrm{Hom}_k(R, M)$ so gilt für $\delta^2 f$:
$$\delta^2 f(r_1, r_2) = r_1 f(r_2) - f(r_1, r_2) + f(r_1)r_2$$

7. Zusammengefaßt sind also alle Faktorabbildungen Co-Ränder und diese liefern dieselbe Extension falls sie sich um ein Co-Bild unterscheiden. Es folgt die Behauptung.

$\square$

7.2 Glatte Algebren

Definition 7.5. Sei R eine k-Algebra. R heißt k-glatt, falls es für jede singuläre Erweiterung einer k-Algebra T mit einem T-Bi-Modul M und für jeden Algebrahomomorphismus $\alpha : R \longrightarrow T$ eine Liftung $\beta : R \longrightarrow E$ von k-Algebren gibt, so daß das Diagramm

$$\begin{tikzcd}
 & & k \arrow[r] \arrow[d] & R \arrow[dl, "\beta"'] \arrow[d, "\alpha"] & \\
0 \arrow[r] & M \arrow[r] & E \arrow[r] & T \arrow[r] & 0
\end{tikzcd}$$

kommutiert.

Ist k ein Körper, dann stellt der folgende Satz den Zusammenhang zwischen der zweiten Hochschildcohomolgie und glatten Algebren her:

Satz 7.6. *Ist k Körper, R eine k-Algebra, so gilt:*

$$R \text{ ist glatte } k\text{-Algebra} \iff H^2(R, M) = 0 \text{ für alle } R\text{-Bi-Moduln } M$$

Beweis.

„⇒“ Sei R glatte k-Algebra und $0 \longrightarrow M \longrightarrow E \longrightarrow R \longrightarrow 0$ Hochschildextension. Es ergibt sich das Diagramm:

$$\begin{tikzcd}
 & & k \arrow[r] \arrow[d] & R \arrow[dl, "\beta"'] \arrow[d, equal, "\mathrm{id}"] & \\
0 \arrow[r] & M \arrow[r] & E \arrow[r] & R \arrow[r] & 0
\end{tikzcd}$$

mit einer Liftung β. Insbesondere ist β ein Ringhomomorphismus und die Extension damit trivial.

„⇐“ Ist $H^2(R, M) = 0$ für alle Bi-Moduln M und $0 \longrightarrow M \longrightarrow E \xrightarrow{\sigma} T \longrightarrow 0$ singuläre Extension von T und $\alpha : R \longrightarrow T$ ein Ringhomomorphismus. Sei D der Algebren-Pullback von R und Eüber T, d.h. $D := \{(r, e) \in R \times E \text{ mit } \alpha(r) = \sigma(e)\}$. Dann ist M isomorph zum Kern der kanonischen Abbildung $\pi_1 : D \longrightarrow R$. Da k Körper ist, spaltet die Sequenz $0 \longrightarrow M \longrightarrow D \longrightarrow R \longrightarrow 0$ und ist damit eine Hochschildextension. Es ergibt sich das Diagramm:

$$\begin{tikzcd}
0 \arrow[r] & M \arrow[r] \arrow[d, equal] & D \arrow[r, shift left, "\pi_1"] \arrow[d, "\pi_2"'] & R \arrow[l, dashed, shift left, "s"] \arrow[r] \arrow[d, "\alpha"] & 0 \\
0 \arrow[r] & M \arrow[r] & E \arrow[r, "\sigma"] & T \arrow[r] & 0
\end{tikzcd}$$

Da $H^2(R,M)=0$, gibt es einen Schnitt s mit trivialer Faktorabbildung. s ist dann ein Ringhomomorphismus und $\beta := \pi_2 s$ die gesuchte Liftung von α.

$\square$

Glattheit ist transitiv und verträglich mit Lokalisierung und Konstantenerweiterung. Dies zeigt der folgende Satz:

Satz 7.7.

1. *Sei R glatt über k und $1 \in S \subseteq R$ multiplikativ abgeschlossene Teilmenge $\Rightarrow S^{-1}R$ ist glatt über k.*

2. *Sei R glatte k-Algebra, Q glatte R-Algebra $\Rightarrow Q$ ist glatte k-Algebra.*

3. *Ist R glatt über k und $k \longrightarrow l$ Ringhomomorphismus $\Rightarrow R \otimes_k l$ ist glatte l-Algebra.*

Beweis.

1. Sei $0 \longrightarrow M \longrightarrow E \longrightarrow R \longrightarrow 0$ singuläre Extension der k-Algebra T. Die Glattheitseigenschaft führt auf das Diagramm:

$$\begin{tikzcd}
 & k \arrow[r] \arrow[dr] & R \arrow[r] \arrow[d, dashed, "\beta"'] & S^{-1}R \arrow[d, "\alpha"] & \\
0 \arrow[r] & M \arrow[r] & E \arrow[r] & T \arrow[r] & 0
\end{tikzcd}$$

Aus R glatt über k folgt die Existenz von $\beta : R \longrightarrow E$. Für $s \in S$, ist $\beta(s)$ mod M invertierbar und da $M^2 = 0$, ist $\beta(s)$ selbst invertierbar. Nach der universellen Eigenschaft des Rings $S^{-1}R$ faktorisiert β über $S^{-1}R$, und dies gibt die gesuchte Liftung von α.

2. Mit obiger Extension ergibt sich das Diagramm:

$$\begin{tikzcd}
 & k \arrow[r] \arrow[dr] & R \arrow[r] \arrow[d, dashed, "\beta"'] & Q \arrow[d, "\alpha"] \arrow[dl, "\gamma"'] & \\
0 \arrow[r] & M \arrow[r] & E \arrow[r] & T \arrow[r] & 0
\end{tikzcd}$$

R glatt über $k \Rightarrow \exists\ \beta : R \longrightarrow E$. Via β ist E dann auch R-Algebra, und da Q glatt über R ist, folgt die Existenz der gesuchten Liftung γ.

3. Ist $0 \longrightarrow M \longrightarrow E \longrightarrow T \longrightarrow 0$ singuläre Extension einer l-Algebra T, dann folgt:

$$\begin{tikzcd}
 & & k \arrow[r] \arrow[d] & R \arrow[d] \arrow[ddl, "\beta"'] & \\
 & & l \arrow[r] \arrow[d] & R \otimes_k l \arrow[d, "\alpha"] \arrow[dl, "\gamma"] & \\
0 \arrow[r] & M \arrow[r] & E \arrow[r] & T \arrow[r] & 0
\end{tikzcd}$$

R glatt über $k \Rightarrow \exists\ \beta : R \longrightarrow E$. Nach der universellen Eigenschaft des Tensorproduktes gibt es dann einen Ringhomomorphismus γ der α wie gewünscht liftet.

□

Im Falle von Körpererweiterungen gibt es ein schönes Ergebnis:

Satz 7.8. *Ist K/k endliche, separable Körpererweiterung, dann ist K eine glatte k-Algebra.*

Beweis. Ist K/k endlich und separabel, dann gibt es ein $x \in K$ mit $K = k(x)$ und ist $f \in k[X]$ Minimalpolynom von x, so ist $f'(x) \neq 0$. Ist eine Extension der k-Algebra T gegeben, so folgt:

$$\begin{tikzcd}
 & & k \arrow[r] \arrow[d] & K = k(x) \arrow[d, "\alpha"] & \\
0 \arrow[r] & M \arrow[r] & E \arrow[r, "\sigma"] & T \arrow[r] & 0
\end{tikzcd}$$

Die gesuchte Liftung existiert, falls es ein $e \in E$ gibt mit $f(e) = 0$ und $e \bmod M = \alpha(x)$. Schauen wir genauer hin:
Sei $y \in E$ Urbild von $\alpha(x)$ und $m \in M$. Es gilt mit Hilfe der Taylorentwicklung:
$f(y+m) = f(y) + f'(y)m + \underbrace{f''(y)m^2/2 + \ldots}_{=0}$
Weiterhin gilt:
$\sigma f(y) = f(\sigma(y)) = f(\alpha(x)) = \alpha f(x) = 0 \Rightarrow f(y) \in M$.
Analog ist $\sigma f'(y) = \alpha f'(x)$. Insbesondere ist $f'(y) \bmod M$ eine Einheit in T und mit $M^2 = 0$ auch $f'(y)$ Einheit in E.
Setze $m := -f(y)/f'(y) \in M \Rightarrow f(y+m) = 0$. Es folgt die Behauptung. □

Wie dem Beweis zu entnehmen ist, hängt die Konstruktion der Liftung entscheidend von der Separabilität des Minimalpolynoms ab. Dies macht plausibel, daß nur separable Erweiterungen glatte k-Algebren liefern. Dieses Ergebnis läßt sich sogar auf beliebige Körpererweiterungen übertragen.

Definition 7.9. Eine beliebige Körpererweiterung K/k heißt *separabel*, falls es eine Transzendentsbasis Γ gibt, so daß $K/k(\Gamma)$ eine (endliche) separable Erweiterung ist.

Als Ergebnis ergibt sich mit Hilfe dieser Definition:

Theorem 7.10. *Sei K/k beliebige Körpererweiterung, dann gilt:*

$$K/k \text{ ist separabel} \quad \Longleftrightarrow \quad K \text{ ist glatte } k\text{-Algebra}$$

Beweis. siehe [Mat80, §26, insbesondere Theorem 26.9] □

8 Glattheit von Dedekindringen

Neben den separablen Körpererweiterungen erweisen sich auch die in Abschnitt 2 definierten Dedekindringe A als glatte $\mathbf{F}_p$-Algebren. Dies wird (mit einiger Mühe) im folgenden bewiesen.

Sei im ganzen Abschnitt die Situation wie in Abschnitt 2 mit den entsprechenden Notationen und Definitionen.

8.1 Eigenschaften des Dedekindringes A

Satz 8.1.

1. *$A \otimes_{\mathbf{F}_p} A$ ist noethersch.*

2. *Ist $0 \neq \mathfrak{p} \in \operatorname{Spec} A$, $A_\mathfrak{p}$ die Lokalisierung von A nach $\mathfrak{p}$ und $\hat{A}_\mathfrak{p}$ Komplettierung, so ist $\hat{A}_\mathfrak{p} \cong \mathbf{F}_q[|X|]$ mit $\mathbf{F}_q \cong A/\mathfrak{p}$ und $q = p^n$.*

3. *Sei $\mathfrak{p} \in \operatorname{Spec} A$ und $S := A \setminus \mathfrak{p}$. Mit S ist dann auch $T := S \otimes S = \{a \otimes b \in A \otimes_{\mathbf{F}_p} A\}$ multiplikativ abgeschlossen. Es gilt: $A_\mathfrak{p} \otimes_{\mathbf{F}_p} A_\mathfrak{p} \cong T^{-1}(A \otimes A)$, insbesondere ist also auch $A_\mathfrak{p} \otimes_{\mathbf{F}_p} A_\mathfrak{p}$ noethersch.*

Beweis.

1. A ist nach Abschnitt 2 eine endlich erzeugte $\mathbf{F}_p$-Algebra, d.h. $A \cong \mathbf{F}_p[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$. Es folgt:

$$\begin{aligned} A \otimes_{\mathbf{F}_p} A &\cong A \otimes_{\mathbf{F}_p} \mathbf{F}_p[X_1, \ldots, X_n]/(f_1, \ldots f_m) \\ &\cong A[X_1, \ldots, X_n]/(f_1, \ldots f_m) \end{aligned}$$

Da A noethersch ist, ist $A \otimes_{\mathbf{F}_p} A$ als Quotient eines noetherschen Ringes selbst wieder noethersch.

2. Ist π uniformisierendes Element in $\hat{A}_{\mathfrak{p}}$, dann hat jedes Element in $\hat{A}_{\mathfrak{p}}$ eine eindeutige π-adische Entwicklung. Dies induziert den gesuchten Isomorphismus. Genaueres findet sich in [Ser79, II §4 Theorem 2]

3. Die Abbildung $T^{-1}(A \otimes A) \longrightarrow A_{\mathfrak{p}} \otimes_{\mathbf{F}_p} A_{\mathfrak{p}}$ existiert, da T in $A_{\mathfrak{p}} \otimes_{\mathbf{F}_p} A_{\mathfrak{p}}$ invertierbar ist. Unter den beiden Abbildungen

$$\begin{array}{rcl} A & \longrightarrow & T^{-1}(A \otimes A) \\ a & \longmapsto & 1 \otimes a \end{array} \quad \text{und} \quad \begin{array}{rcl} A & \longrightarrow & T^{-1}(A \otimes A) \\ a & \longmapsto & a \otimes 1 \end{array}$$

wird S auf invertierbare Elemente abgebildet. Dies induziert die gesuchte Umkehrabbildung.

$\square$

8.2 Berechnung von $\mathbf{H^2(A, M)}$

Theorem 8.2. *Für die $\mathbf{F}_p$-Algebra A ist $H^2(A, M) = 0$ für alle A-Bi-Moduln M.*

Der Beweis des Satzes gliedert sich nun wie folgt: Zunächst wird die Behauptung für den einfachsten Fall $A = \mathbf{F}_p[X]$ gezeigt (Schritt I). Dann wird die Glattheitseigenschaft auf die Komplettierungen $\mathbf{F}_q[|X|]$ der Lokalisierungen von A übertragen (Schritt II, III). Dies ergibt dann die Aussage für die lokalen Ringe $A_{\mathfrak{p}}$ (Schritt IV). In den letzten beiden Schritten wird durch ein lokal-global Argument der Beweis abgeschlossen (Schritte V, VI).

Für Schritt I zunächst die folgende Definition:

Definition 8.3. Sei R Ring; M, N R-Moduln, P_i projektive R-Moduln. Eine *projektive Auflösung von M der Länge n* ist eine Auflösung der Form:

$$0 \longleftarrow M \longleftarrow P_0 \longleftarrow \dots \longleftarrow P_n \longleftarrow 0$$

Insbesondere ist $\mathrm{Ext}^i_R(M, N) = 0$ für $i > n$.

Schritt I. *Sei K beliebiger Körper, dann gilt für die K-Algebra $K[X]$:*

$$H^2(K[X], M) = 0 \quad \textit{für alle Bi-Moduln } M$$

Beweis. Da K Körper ist gilt nach Satz 6.29 auf Seite 49

$$H^2(K[X],M) = \mathrm{Ext}_{K[X]^e}(K[X],M)$$

Es wird nun eine projektive Auflösung der Länge 1 des $K[X]^e$-Moduls $K[X]$ konstruiert.
Sei I der Kern der Abbildung

$$\begin{aligned} K[X] \otimes_K K[X] &\longrightarrow K[X] \\ f(X) \otimes g(X) &\longmapsto f(X)g(X) \end{aligned}$$

Es ergibt sich die exakte Sequenz:

$$0 \longrightarrow I \longrightarrow K[X] \otimes_K K[X] \longrightarrow K[X] \longrightarrow 0$$

$K[X]^e$ ist selbst natürlich projektiver $K[X]^e$-Modul. Die Projektivität von I ergibt sich aus der Feststellung, daß I ein Hauptideal im Integritätsring $K[X]^e \cong K[X,Y]$ ist. I wird erzeugt von $X \otimes 1 - 1 \otimes X$. Dies wird im folgenden bewiesen:

Beh. 1: I wird erzeugt von Elementen der Form $f \otimes 1 - 1 \otimes f$:

$$\begin{aligned} &\text{Ist } \sum f_i \otimes g_i \in I \\ &\Rightarrow \sum f_i g_i = 0 \\ &\Rightarrow \sum f_i \otimes g_i = \sum 1 \otimes g_i(f_i \otimes 1 - 1 \otimes f_i) \end{aligned}$$

Beh. 2: Elemente der Form $f \otimes 1 - 1 \otimes f$ werden vom Element $\alpha := X \otimes 1 - 1 \otimes X$ erzeugt: Sei $f = \sum_{i=0}^{n} a_i X^i$. Es folgt:

$$\begin{aligned} &\sum_{i=0}^{n} a_i X^i \otimes 1 - 1 \otimes \sum_{i=0}^{n} a_i X^i \\ &\quad = (\sum_{k=0}^{n} a_{k+1} \sum_{i+j=k} X^i \otimes X^j)(X \otimes 1 - 1 \otimes X) \end{aligned}$$

Wobei Œ $a_0 = 0$ gewählt werden kann, da $a_0 \otimes 1 - 1 \otimes a_0 = 0$.

□

Schritt II. *Sei K beliebiger Körper, dann gilt für die K-Algebra $K[|X|]$:*

$$H^2(K[|X|],M) = 0 \quad \textit{für alle Bi-Moduln } M$$

Zunächst das folgende Lemma:

Lemma 8.4. $K[|X|]\otimes_K K[|X|]$ ist ein Unterring von $K[|X,Y|]$. Mit $K[|X,Y|]$ ist damit auch $K[|X|]\otimes_K K[|X|]$ ein Integritätsring.

Beweis. Sei ε der K-Algebrenhomomorphismus

$$\begin{aligned} \varepsilon : K[|X|]\otimes_K K[|X|] &\longrightarrow K[|X,Y|] \\ f(X)\otimes g(X) &\longmapsto f(X)g(Y) \end{aligned}$$

Die Abbildung ist injektiv, falls das folgende Kriterium erfüllt ist (Siehe [Bou71]): Ist $(f_i)_{i\in I}$ eine K-Basis von $K[|X|]$, dann ist ε injektiv, falls die $(\varepsilon(f_i))_{i\in I}$ linear unabhängig über $K[|Y|]$ sind.

$$\begin{aligned} \text{Ist also } \sum_{\text{endlich}} g_i(Y)f_i(X) &= 0 \\ \Rightarrow \sum g_i(0)f_i(X) &= 0 \\ \Rightarrow\ g_i(0) = 0\ \forall\, i \text{ da die } f_i \text{ nach Vorausetzung linear unabhängig sind.}& \end{aligned}$$

Aus den Potenzreihen $g_i(Y)$ läßt sich nun ein Y ausklammern:

$$\begin{aligned} \Rightarrow\ Y\sum \tilde{g}_i(Y)f_i(X) &= 0 \\ \Rightarrow \sum \tilde{g}_i(Y)f_i(X) &= 0 \end{aligned}$$

Aufsteigende Induktion liefert nun die lineare Unabhängigkeit der $f_i(X)$ über $K[|Y|]$ □

Beweis von Schritt II. Analog zu Schritt I wird eine projektive Auflösung der Länge 1 von $K[|X|]$ als $K[|X|]^e$-Modul konstruiert: Sei

$$0 \longrightarrow (\alpha) \longrightarrow K[X]\otimes_K K[X] \longrightarrow K[X] \longrightarrow 0 \tag{8.4.1}$$

die Auflösung aus Schritt I. $K[|X|]$ ist Komplettierung von $K[X]$ bezüglich des Primideals (X) und damit nach Satz 8.7 auf der nächsten Seite eine flache $K[X]$-Algebra. Der Funktor
$K[|X|]\otimes_{K[X]} \_ \otimes_{K[X]} K[|X|]$ ist damit exakt. Anwendung des Funktors auf die Sequenz (8.4.1) ergibt deshalb:

$$0 \longrightarrow K[|X|]\otimes_K (\alpha)\otimes_K K[|X|] \longrightarrow K[|X|]\otimes_K K[|X|] \xrightarrow{\mu} K[|X|] \longrightarrow 0$$

Insbesondere ist der Kern der Abbildung μ erzeugt von α, und damit als Hauptideal im Integritätsring $K[|X|]^e$ ein projektiver $K[|X|]^e$-Modul. Es folgt die Behauptung. □

Bemerkung 8.5. Aus Schritt II ergibt sich, daß Potenzreihenringe in einer Veränderlichen glatte K-Algebren sind. Dies ist für Potenzreihenringe in mehreren Veränderlichen im allgemeinen nicht mehr richtig. Genauer gilt: Ist $\operatorname{char} k = p$ und $[K : K^p] < \infty$, dann ist $K[|X_1, \ldots X_n|]$ glatt über K. Vergleiche hierzu [Mat80, §28 Bemerkung zu Theorem 28.2]

Schritt III. *Ist L/K endliche, separable Körpererweiterung, so ist auch für die K-Algebra $L[|X|]$ die Hochschildcohomologie*

$$H^2_{L[|X|]/K}(L[|X|], M) = 0 \quad \textit{für alle Bimoduln } M$$

Beweis. Nach Satz 7.6 auf Seite 54 reicht es zu zeigen, daß $L[|X|]$ eine glatte K-Algebra ist. Da L/K separabel, ist nach Satz 7.8 auf Seite 56 L glatte K-Algebra. Nach Schritt II ist $L[|X|]$ glatte L-Algebra. Aus der Transitivität der Glattheitseigenschaft (vgl. Satz 7.7 auf Seite 55) folgt, daß auch $L[|X|]$ eine glatte K-Algebra ist. □

Für den nächsten Schritt werden nun einige Weisheiten aus der kommutativen Algebra benötigt, die im folgenden ohne Beweis aufgelistet werden. Genaueres findet sich z.B. in [Mat80].

Satz 8.6. *Ist R noetherscher Ring, M endlich erzeugter R-Modul und S flache R-Algebra, so gilt:*

$$\operatorname{Ext}^i_R(M, N) \otimes_R S = \operatorname{Ext}^i_S(M \otimes_R S, N \otimes_R S)$$

Satz 8.7.

1. *Sei R Ring, $S \subseteq A$ eine multiplikativ abgeschlossene Teilmenge, dann ist*

   $S^{-1}A$ eine flache A-Algebra.

2. *Ist R noetherscher, lokaler Ring und $\hat{R}$ die Komplettierung von R, so ist $\hat{R}$* treuflacher *R-Modul, d.h. für alle R-Moduln M, N gilt:*

   $$M \longrightarrow N \quad \textit{ist injektiv} \quad \Longleftrightarrow \quad M \otimes_R \hat{R} \longrightarrow N \otimes_R \hat{R} \quad \textit{ist injektiv}$$

3. *Ist R noetherscher Ring, $\mathfrak{p}$ Primideal in R, dann ist die Komplettierung $\hat{R}_\mathfrak{p}$ bezüglich $\mathfrak{p}$ eine flache R-Algebra.*

Lemma 8.8. Sei R Ring, G ein R-Modul und S eine treuflache R-Algebra, dann gilt:

$$G = 0 \quad \Longleftrightarrow \quad G \otimes_R S = 0$$

Beweis. Es ist $G \otimes_R S = 0 \longrightarrow 0$ injektiv, also auch $G \longrightarrow 0$. $\square$

Schritt IV. *Sei M ein A-Bi-Modul und die beiden Abbildungen*

$$\begin{aligned} \mu : A \otimes A &\longrightarrow A \\ a \otimes b &\longmapsto ab \end{aligned} \qquad \begin{aligned} \Delta : \operatorname{Spec} A &\longrightarrow \operatorname{Spec}(A \otimes A) \\ \mathfrak{p} &\longmapsto \mu^{-1}(\mathfrak{p}) \end{aligned}$$

gegeben. Es gilt:

$$H^2(A, M)_{\mathfrak{P}} = 0 \quad \textit{für alle } \mathfrak{P} \in \Delta(\operatorname{Spec} A)$$

Beweis. Nach Satz 8.7 auf der vorherigen Seite ist $\hat{A}^e_{\mathfrak{p}}$ eine treuflache $A^e_{\mathfrak{p}}$-Algebra. Daraus folgt für einen beliebigen $A_{\mathfrak{p}}$-Bimodul N:

$$\begin{aligned} \operatorname{Ext}^2_{A^e_{\mathfrak{p}}}(A_{\mathfrak{p}}, N) \otimes_{A^e_{\mathfrak{p}}} \hat{A}^e_{\mathfrak{p}} &\cong \operatorname{Ext}^2_{\hat{A}^e_{\mathfrak{p}}}(\hat{A}_{\mathfrak{p}}, N \otimes_{A^e_{\mathfrak{p}}} \hat{A}^e_{\mathfrak{p}}) && \text{nach Satz 8.6} \\ &\cong \operatorname{Ext}^2_{\mathbf{F}_q[|X|]^e}(\mathbf{F}_q[|X|], N \otimes_{A^e_{\mathfrak{p}}} \mathbf{F}_q[|X|]^e) && \text{nach Satz 8.1} \\ &= H^2_{\mathbf{F}_q[|X|]/\mathbf{F}_p}(\mathbf{F}_q[|X|], N \otimes_{A^e_{\mathfrak{p}}} \hat{A}^e_{\mathfrak{p}}) && \text{nach Satz 6.29} \\ &= 0 && \text{nach Schritt III} \end{aligned}$$

Nach Lemma 8.8 auf der vorherigen Seite ist damit $\operatorname{Ext}^2_{A^e_{\mathfrak{p}}}(A_{\mathfrak{p}}, N) = 0$.
Sei $S = A \setminus \mathfrak{p}$ und $T = S \otimes S$ wie in Satz 8.1 auf Seite 57. Wiederum nach Satz 8.7 auf der vorherigen Seite ist $A_{\mathfrak{p}}$ eine flache A-Algebra und es folgt:

$$\begin{aligned} T^{-1} H^2(A, M) &= T^{-1} \operatorname{Ext}^2_{A^e}(A, M) \\ &\cong \operatorname{Ext}^2_{A^e}(A, M) \otimes_{A^e} A^e_{\mathfrak{p}} && \text{nach Satz 8.1} \\ &\cong \operatorname{Ext}^2_{A^e_{\mathfrak{p}}}(A_{\mathfrak{p}}, M \otimes_{A^e} A^e_{\mathfrak{p}}) && \text{nach Satz 8.6} \\ &= 0 \end{aligned}$$

Da $\mu^{-1}(S) \supseteq T$ ist, ist $H^2(A, M)_{\mathfrak{P}}$ eine Lokalisierung von $T^{-1}H^2(A, M)$ und mit letzterem Modul selbst Null. $\square$

Schritt V. *Ist $\mathfrak{P} \notin \Delta(\operatorname{Spec} A)$, dann ist $A_{\mathfrak{P}} = 0$ und damit auch*

$$H^2(A, M)_{\mathfrak{P}} \cong \operatorname{Ext}_{A^e_{\mathfrak{P}}}(A_{\mathfrak{P}}, M \otimes_{A^e} A^e_{\mathfrak{P}}) = 0$$

Beweis. Es reicht zu zeigen, daß es ein $a \in A$ gibt, so daß $a \otimes 1 - 1 \otimes a \notin \mathfrak{P}$ ist: Einerseits ist das Element $a \otimes 1 - 1 \otimes a$ eine Einheit in $A^e_{\mathfrak{P}}$, andererseits liegt es im Annulator des A^e-Moduls A. Damit ist $A_{\mathfrak{P}} = 0$.
Annahme: $a \otimes 1 - 1 \otimes a \in \mathfrak{P}$ für alle $a \in A$.

Da $\ker(\mu)$ von den $a\otimes 1 - 1\otimes a$ erzeugt wird, ist $\ker(\mu) \subseteq \mathfrak{P}$ und die kanonische Projektion nach $A^e/\mathfrak{P}$ faktorisiert über μ. Es ergeben sich die Diagramme:

$$\begin{tikzcd} A^e \arrow[rr, "\pi"] \arrow[dr, "\mu"'] & & A^e/\mathfrak{P} \\ & A \arrow[ur, "\tilde{\pi}"'] & \end{tikzcd} \xrightarrow{\text{Spec}} \begin{tikzcd} \operatorname{Spec} A^e & & \operatorname{Spec} A^e/\mathfrak{P} \arrow[ll, "\theta"'] \arrow[dl, "\tilde{\theta}"] \\ & \operatorname{Spec} A \arrow[ul, "\Delta"] & \end{tikzcd}$$

Insbesondere gilt:

$$\begin{aligned} \mathfrak{P} &= \theta(\overline{0}) \\ &= \Delta\tilde{\theta}(\overline{0}) \end{aligned}$$

$\Rightarrow \mathfrak{P} \in \Delta(\operatorname{Spec} A)$ im Widerspruch zur Voraussetzung. □

Schritt VI. $H^2(A, M) = 0$ *für alle Bi-Moduln* M.

Beweis. Nach Schritt IV und V ist $\operatorname{Ext}^2_{A^e}(A, M)_{\mathfrak{P}} = 0$ für alle Primideale $\mathfrak{P}$ aus A^e. Es folgt die Behauptung, da ein Modul, dessen sämtliche Lokalisierungen verschwinden, trivial ist. □

9 Deformationen von Drinfeld-Moduln

Ziel des folgenden Abschnitts ist die Beschreibung der Deformationen von Drinfeld-Moduln, die, wie sich herausstellt, in engem Zusammenhang mit der Hochschildcohomologie steht.

Sei im folgenden k Körper mit Charakteristik p.
Als Musterexemplar eines lokalen Ringes $(R, \mathfrak{m})$ mit $\mathfrak{m}^2 = 0$ dient der folgende Ring:

Definition 9.1. Sei $\mathcal{O} := k[\varepsilon]$ mit $\varepsilon^2 = 0$. Der Ring $\mathcal{O}$ ist ein lokaler Ring mit maximalem Ideal (ε) und $\mathcal{O}/(\varepsilon) \cong k$.

Definition 9.2 (Deformationen von Drinfeld-Modul). Sei $\varphi : A \longrightarrow k\{\tau\}$ ein Drinfeld-Modul vom Rang d:

$$\begin{tikzcd} A \arrow[rr, "\varphi"] \arrow[dr, "\theta"'] & & k\{\tau\} \arrow[dl, "\partial"] \\ & k & \end{tikzcd}$$

mit θ der Charakteristik des Drinfeld Moduls und $\partial(\sum a_i\tau^i) = a_0$.

Eine *Deformation* von φ ist ein Drinfeld-Modul $\psi : A \longrightarrow \mathcal{O}\{\tau\}$ und ein kommutatives Diagramm:

$$\begin{tikzcd} A \arrow[r, "\psi"] \arrow[dr, "\varphi"'] & \mathcal{O}\{\tau\} \arrow[d, "\bmod \varepsilon"] \\ & k\{\tau\} \end{tikzcd}$$

Von entscheidender Bedeutung ist das folgende Ideal:
Sei $\mathfrak{m}\{\tau\} := \{\sum \alpha_i \tau^i \in \mathcal{O}\{\tau\} \mid \alpha_i \in \varepsilon k\}$ das von ε erzeugte Ideal in $\mathcal{O}\{\tau\}$.

Lemma 9.3. $\mathfrak{m}\{\tau\}$ ist in natürlicher Weise ein A-Bi-Modul.

Beweis. Als $\mathbf{F}_p$-Algebren sind A, $k\{\tau\}$ und $\mathcal{O}\{\tau\}$ insbesondere $\mathbf{F}_p$-Vektorräume. Sei ψ nun eine Liftung von φ als $\mathbf{F}_p$-Vektorraumhomomorphismus:

$$\begin{tikzcd} & A \arrow[dl, "\psi"'] \arrow[d, "\varphi"] & \\ \mathcal{O}\{\tau\} \arrow[r, "\bmod \varepsilon"'] & k\{\tau\} \arrow[r] & 0 \end{tikzcd}$$

Ist $f(\tau) \in \mathfrak{m}\{\tau\}$, so ergibt sich die Bimodulstruktur durch $af(\tau)b := \psi(a)f(\tau)\psi(b)$. Die Bimodulstruktur ist unabhängig von der Wahl der Liftung ψ:
Seien ψ_1, ψ_2 zwei Liftungen von φ. Es folgt:

$$\psi_1(a)f(\tau)\psi_1(b) - \psi_2(a)f(\tau)\psi_2(b) =$$
$$\underbrace{(\psi_1(a) - \psi_2(a))}_{\in\mathfrak{m}\{\tau\}} f(\tau)\psi_1(b) + \psi_2(a)f(\tau) \underbrace{(\psi_1(b) - \psi_2(b))}_{\in\mathfrak{m}\{\tau\}} = 0$$

Da $\tau\varepsilon = \varepsilon^p\tau = 0$, hängt die links-Modulstruktur nur von θ ab. Andererseits läßt sich jedes $\psi(a)$ schreiben als $\psi(a) = \varphi(a) + g(\tau)$ mit einem $g(\tau) \in \mathfrak{m}\{\tau\}$. Es folgt:

$$\begin{aligned} f(\tau)\psi(a) &= f(\tau)\varphi(a) + f(\tau)g(\tau) \\ &= f(\tau)\varphi(a) \end{aligned}$$

Es folgt für die Bimodulstruktur:

$$af(\tau)b = \theta(a)f(\tau)\varphi(b) \tag{9.3.1}$$

□

Es ergeben sich nun die beiden Fragen:

- Gibt es zu jedem φ eine Deformation?
- Wie sehen die Isomorphieklassen dieser Fortsetzungen aus?

Beide Fragen stehen, wie im folgenden gezeigt wird, in engem Zusammenhang mit den Hochschildcohomologiegruppen des A-Bi-Moduls $\mathfrak{m}\{\tau\}$.

Theorem 9.4.

1. *Jeder Drinfeld-Modul besitzt Deformationen.*
2. *Die Isomorphieklassen der Deformationen sind isomorph zu* $H^1(A, \mathfrak{m}\{\tau\})$.
3. *Die Automorphismengruppe einer Deformation* ψ *ist isomorph zu* $H^0(A, \mathfrak{m}\{\tau\})$.

Zunächst einige Lemmata:

Lemma 9.5. Sei ψ eine Liftung von φ. ψ ist Ringhomomorphismus, falls

$$\psi(a_1 a_2) = \psi(a_1)\psi(a_2) \text{ für alle } a_1, a_2 \in A$$

Beweis. Zu zeigen: $\psi(1) = 1$
Es gilt: $\psi(1) = \psi(1 \cdot 1) = \psi(1)^2$ und $\psi(1) - 1 \in (\varepsilon)$. Es folgt:

$$\begin{aligned} 0 = (\psi(1) - 1)^2 &= \psi(1)^2 - 2\psi(1) + 1 \\ &= -\psi(1) + 1 \\ \Rightarrow \quad \psi(1) &= 1 \end{aligned}$$

$\square$

Als „Maß“ wie gut oder schlecht eine Liftung ψ ein Ringhomomorphismus ist, wird die folgende Bilinearform definiert:

$$\begin{aligned} T : A \times A &\longrightarrow \mathfrak{m}\{\tau\} \\ a_1, a_2 &\longmapsto \psi(a_1)\psi(a_2) - \psi(a_1 a_2) \end{aligned}$$

Da $\psi(a_1)\psi(a_2) - \psi(a_1 a_2) \equiv 0 \mod \varepsilon$ ist, landet T in $\mathfrak{m}\{\tau\}$ und ist nach Definition $\mathbf{F}_p$-bilinear.

Lemma 9.6. Es gilt:

$$a_1 T(a_2, a_3) - T(a_1 a_2, a_3) + T(a_1, a_2 a_3) - T(a_1, a_2) a_3 = 0$$

Beweis. Einsetzen der Definition liefert die Behauptung. $\square$

Seien ψ_1, ψ_2 zwei Liftungen von φ. Sei $t := \psi_2 - \psi_1$. Die Abbildung t landet nach Definition wieder in $\mathfrak{m}\{\tau\}$ und ist $\mathbf{F}_p$-linear.
t induziert die $\mathbf{F}_p$-bilineare Abbildung:

$$\begin{aligned} \delta t : A \times A &\longrightarrow \mathfrak{m}\{\tau\} \\ a_1, a_2 &\longmapsto a_1 t(a_2) - t(a_1 a_2) + t(a_1) a_2 \end{aligned}$$

Lemma 9.7. Sind T_1, T_2 die zu ψ_1 bzw. ψ_2 gehörenden bilinearen Abbildungen, so gilt:

$$T_2 - T_1 = \delta t$$

Beweis.

$$\begin{aligned} T_2(a_1, a_2) &= (\psi_1 + t)(a_1)(\psi_1 + t)(a_2) - (\psi_1 + t)(a_1 a_2) \\ &= \psi_1(a_1)\psi_1(a_2) + t(a_1)\psi_1(a_2) + \psi_1(a_1)t(a_2) + 0 - \psi_1(a_1 a_2) - t(a_1 a_2) \\ &= (T_1 + \delta t)(a_1, a_2) \end{aligned}$$

□

Definition 9.8. Seien φ_1, φ_2 Drinfeld-Moduln über k. Ein Morphismus von $\varphi_1 \longrightarrow \varphi_2$ ist gegeben durch ein $u \in k\{\tau\}$, mit

$$\varphi_1(a)u = u\varphi_2(a) \text{ für alle } a \in A$$

Ist u invertierbar, dann vermittelt u einen Isomorphismus.

Nützlich ist nun das folgende Lemma:

Lemma 9.9. Sei k Ring in Charakteristik p und $u := \sum a_i \tau^i \in k\{\tau\}$, dann gilt:
u invertierbar $\Longleftrightarrow$ a_0 invertierbar und a_i ist nilpotent für alle $i > 0$.

Beweis. siehe [Lau91, (1.1)] □

Zur Erinnerung nochmals die Cozykel- und Coränderrelationen der Hochschildcohomologie nach 6.26 auf Seite 46 für den Komplex $\mathrm{Hom}_{R^e}(\beta(R), M)$:

$$0 \longrightarrow M \xrightarrow{\delta^1} \mathrm{Hom}_k(R, M) \xrightarrow{\delta^2} \mathrm{Hom}_k(R^{\otimes 2}, M) \xrightarrow{\delta^3} \cdots$$

mit

$$\begin{aligned} \delta^1(m)(a) &= am - ma \\ \delta^2(f)(a_1, a_2) &= a_1 f(a_2) - f(a_1, a_2) + f(a_1) a_2 \\ \delta^3(f)(a_1, a_2, a_3) &= a_1 f(a_2, a_3) - f(a_1 a_2, a_3) + f(a_1, a_2 a_3) - f(a_1, a_2) a_3 \end{aligned}$$

Nach diesen Vorleistungen nun zum Beweis von Theorem 9.4:

Beweis.

1. Sei ψ eine beliebige Liftung mit zugehöriger Bilinearform T. Nach Lemma 9.6 auf Seite 65 ist T ein Cozykel in $H^2(A, \mathfrak{m}\{\tau\})$. Da $H^2(A, \mathfrak{m}\{\tau\}) = 0$ nach Theorem 8.2 auf Seite 58, folgt die Existenz eines $t \in \mathrm{Hom}(A, \mathfrak{m}\{\tau\})$ mit $\delta(t) = T$.

   Setze $\tilde{\psi} := \psi - t$ und sei $\tilde{T}$ zugehörige Bilinearform. Es folgt:

   $$\begin{array}{lll} & \tilde{T} - T &= \delta(\tilde{\psi} - \psi) \quad \text{nach Lemma 9.7} \\ \Rightarrow & \tilde{T} - \delta(t) &= \delta(-t) \\ \Rightarrow & \tilde{T} &= 0 \end{array}$$

   Damit ist $\tilde{\psi}$ nach Lemma 9.5 auf Seite 65 ein Ringhomomorphismus und dadurch eine Deformation von φ.

2. Seien ψ_1, ψ_2 zwei Deformationen von φ. Insbesondere ist dann $T_1 = T_2 = 0$, und es folgt für $t := \psi_2 - \psi_1$, daß $\delta(t) = T_2 - T_1 = 0$. Damit ist $t \in \mathrm{Hom}(A, \mathfrak{m}\{\tau\})$ ein Cozykel.

   Ist $\psi_1 \cong \psi_2$, dann gibt es ein invertierbares $u := \sum (a_i + b_i\varepsilon)\tau^i \in \mathcal{O}\{\tau\}$ mit $\psi_1(a)u = u\psi_2(a)$ für alle $a \in A$. Nach Lemma 9.9 auf der vorherigen Seite ist u invertierbar, falls $a_0 + b_0\varepsilon$ eine Einheit ein $\mathcal{O}$ ist und die $a_i + b_i\varepsilon$ für $i > 0$ nilpotent sind. Da k Körper, ist $a_i + b_i\varepsilon$ nilpotent $\Longleftrightarrow a_i = 0$. Es folgt:

   $$u \text{ ist invertierbar} \quad \Longleftrightarrow \quad u = \lambda + f \quad \text{mit } \lambda \in k^\times, f \in \mathfrak{m}\{\tau\}$$

   a) *Ist $\psi_1 \cong \psi_2$, dann unterscheiden sie sich um ein Cobild.*
      Ist ein Isomorphismus $u = \lambda + f$ gegeben, so gilt:

      $$\begin{array}{lr} & \psi_1(a)(\lambda + f) \bmod \varepsilon = (\lambda + f)\psi_2(a) \bmod \varepsilon \\ \Rightarrow & \varphi(a)\lambda = \lambda\varphi(a) \end{array}$$

      d.h. λ vermittelt einen Automorphismus des Drinfeld-Moduls φ. Da k ein Körper ist, ergibt ein Koeffizientenvergleich, daß $\lambda \in \mathbf{F}_p$ ist. Nun folgt:

      $$\begin{array}{lrl} & \psi_1(a)(\lambda + f) &= (\lambda + f)\psi_2(a) \\ \Rightarrow & \psi_1(a)\lambda + \psi_1(a)f &= \lambda\psi_2(a) + f\psi_2(a) \\ \Rightarrow & \lambda(\psi_2(a) - \psi_1(a)) &= f\psi_2(a) - \psi_1(a)f \\ \Rightarrow & t(a) &= \delta(\lambda^{-1}f)(a) \end{array}$$

      ψ_1 und ψ_2 unterscheiden sich damit um ein Cobild.

b) *Unterscheiden sich ψ_1 und ψ_2 um ein Cobild, dann sind sie isomorph.*

Es gilt:

$$\begin{aligned} & t(a) = \delta(f)(a) \\ \Rightarrow \quad & \psi_2(a) - \psi_1(a) = fa - af \\ \Rightarrow \quad & \psi_1(a)(1+f) = (1+f)\psi_2(a) \end{aligned}$$

Da $1+f$ eine Einheit ist, sind ψ_1 und ψ_2 isomorph.

3. Analog zum vorigen Fall sind die Automorphismen einer festen Deformation ψ gegeben durch ein invertierbares $u \in \mathcal{O}\{\tau\}$ mit $\psi(a)u = u\psi(a)$ und $u = \lambda + f$. Es ergibt sich:

$$\begin{aligned} & \psi(a)(\lambda+f) = (\lambda+f)\psi(a) \\ \Rightarrow \quad & 0 = f\psi(a) - \psi(a)f \\ \Rightarrow \quad & f \in H^0(A, \mathfrak{m}\{\tau\}) \end{aligned}$$

Andererseits induziert jedes $f \in H^0(A, \mathfrak{m}\{\tau\})$ wieder einen Automorphismus durch $u := 1 + f$.

□

10 Generische Glattheit der Charakteristik

Nach Abschnitt 5 induziert die Charakteristik eines Drinfeld-Moduls einen Morphismus

$$\Theta : M_I^d \longrightarrow X$$

von Schemata (Algebraische Stacks für $I = A$). In Analogie zum Fall der elliptischen Kurven ist dieser Morphismus glatt außerhalb der „verbotenen Menge“ $V(I) \cup \{\infty\}$. In diesem Abschnitt wird mit Hilfe des Ergebnisses aus Abschnitt 9 die Beweisidee erläutert.

Sei im folgenden I Ideal in A, d > 0 ganzzahlig und $\mathcal{M}_\mathbf{I}^\mathbf{d}$ die Faserkategorie nach Definition 5.22 auf Seite 32.

Theorem 10.1 (Drinfeld). *Der Morphismus von Algebraischen Stacks (Schemata für $I \neq A$)*

$$\Theta : M_I^d \longrightarrow X \setminus (\{\infty\} \cup V(I))$$

ist glatt von relativer Dimension $d - 1$.

Im ersten Schritt des Beweises wird nun alles auf den Fall $I = A$, d.h. $\Theta : M_A^d \longrightarrow X \setminus \{\infty\}$ zurückgeführt:

Lemma 10.2. Sind $J \subseteq I$ Ideale, dann gibt es einen kanonischen Morphismus von Faserkategorien:

$$r_{I,J} : \mathcal{M}_J^d \longrightarrow \mathcal{M}_I^d$$

so daß das Diagramm

$$\begin{tikzcd} \mathcal{M}_J^d \arrow[r, "r_{I,J}"] \arrow[d, "\theta"'] & \mathcal{M}_I^d \arrow[d, "\theta"] \\ X \setminus (\{\infty\} \cup V(J)) \arrow[r, hook] & X \setminus (\{\infty\} \cup V(I)) \end{tikzcd}$$

kommutiert.

Beweis. Zu zeigen ist, daß eine J-Level-Struktur eine I-Level-Struktur induziert, d.h.:

$$M := \bigcap_{i \in I} \operatorname{Ker}((A/J)^d \xrightarrow{\cdot i} (A/J)^d)$$

ist freier A/I-Modul vom Rang d. Es reicht die Behauptung für $d = 1$ zu prüfen. Es gilt:

$$M = (0 : I/J)_{A/J} = (J : I)_A / J$$

Sei $\mathfrak{p} \neq 0$ Primideal in A, dann gilt:

$$((J : I)_A)_{\mathfrak{p}} = (A_{\mathfrak{p}} J : A_{\mathfrak{p}} I)_{A_{\mathfrak{p}}} = ((\pi^m) : (\pi^n))_{A_{\mathfrak{p}}} = (\pi^{m-n})$$

für $m \geq n$ und π uniformisierendes Element in $A_{\mathfrak{p}}$.

$$\Rightarrow \quad M_{\mathfrak{p}} = (\pi^{m-n})/(\pi^m) \cong A_{\mathfrak{p}}/(\pi^n) = (A/I)_{\mathfrak{p}}$$

$M_{\mathfrak{p}}$ ist also freier $(A/I)_{\mathfrak{p}}$-Modul vom Rang 1 und damit M selbst freier A/I-Modul. □

Satz 10.3. *Der Morphismus von Faserkategorien:*

$$r_{I,J} : \mathcal{M}_J^d \longrightarrow \mathcal{M}_I^d|_{X \setminus (\{\infty\} \cup V(J))}$$

ist darstellbar, endlich und étale (d.h. glatt von relativer Dimension 0*).*

Beweis. Siehe [Lau91, (1.4)]. □

Mit Hilfe von Satz 10.3 und der Transitivität der Glattheitseigenschaft reicht es nun, das Theorem für den Fall $I = A$ zu zeigen.

10.1 Der Tangentialraum von $\mathcal{M}_A^d$

Im zweiten Schritt wird der Tangentialraum von $\mathcal{M}_A^d$ berechnet.

Definition 10.4 (Tangentialraum). Sei $\mathbf{S}$ Faserkategorie über $\mathbf{Sch}/\mathbf{F}_p$ und $[\mathbf{S}]$ der zur Faserkategorie zugehörige kontravariante, mengenwertige Funktor nach 5.16 auf Seite 30:

$$\begin{aligned} [\mathbf{S}] : \mathbf{Sch}/\mathbf{F}_p &\longrightarrow \mathbf{Men} \\ S &\longmapsto \{\text{Isomorphiklassen in } \mathbf{S}(S)\} \end{aligned}$$

Sei k Ring mit Charakteristik p Primzahl. Sei $k[\varepsilon] := k[X]/(X^2)$.
$t_{\mathbf{S}}(k) := [\mathbf{S}](k[\varepsilon])$ heißt *Tangentialraum* von $\mathbf{S}$ in k.
Der Ringhomomorphismus:

$$\begin{aligned} k[\varepsilon] &\longrightarrow k \\ \varepsilon &\longmapsto 0 \end{aligned}$$

vermittelt eine Abbildung $\pi : [\mathbf{S}](k[\varepsilon]) \longrightarrow [\mathbf{S}](k)$. Ist $\varphi \in [\mathbf{S}](k)$, dann heißt

$$t_{\mathbf{S}(k),\varphi} := \{\psi \in t_{\mathbf{S}}(k) \mid \pi(\psi) \cong \varphi\}$$

der *Tangentialraum des k-wertigen Punktes φ.*

Satz 10.5. *Sei k Körper mit Charakteristik p. Sei $T_{A/\mathbf{F}_p} := \mathrm{Hom}_A(\Omega_{A/\mathbf{F}_p}, A)$ und*
$A^e := A \otimes_{\mathbf{F}_p} A$. Wird dem A-Modul $T_{A/\mathbf{F}_p}$ die A^e-Modul-Struktur durch die Abbildung $A^e \longrightarrow A$ gegeben, so gilt:
Für einen k-wertigen Punkt, d.h. einen Drinfeld-Modul $\varphi : A \longrightarrow k\{\tau\}$ vom Rang d, ist der Tangentialraum kanonisch isomorph zu $T_{A/\mathbf{F}_p} \otimes_{A^e} k\{\tau\}$.

Für den Beweis des Satzes wird das folgende Lemma benötigt:

Lemma 10.6. Es gibt einen Isomorphismus $H^1(A, \mathfrak{m}\{\tau\}) \cong T_{A/\mathbf{F}_p} \otimes_{A^e} \mathfrak{m}\{\tau\}$ von A^e-Moduln.

Beweis. Beweis siehe [Lau91] □

Beweis des Satzes. Nach Abschnitt 9 ist der Tangentialraum für einen k-wertigen Punkt, d.h. einen Drinfeld-Modul $\varphi : A \longrightarrow k\{\tau\}$ vom Rang d, isomorph zu $H^1(A, \mathfrak{m}\{\tau\})$. Aus dem Lemma und den Isomorphismen von A^e-Moduln $\mathfrak{m}\{\tau\} \cong \varepsilon k\{\tau\} \cong k\{\tau\}$ folgt die Behauptung. □

Zurück zum Theorem, dessen Beweis nun in greifbarer Nähe liegt. Das letzte Hindernis beseitigt das folgende Lemma:

Lemma 10.7. Sei $k\{\tau\}$ ein $k \otimes_{\mathbf{F}_p} A$-Modul durch $\lambda f(\tau) b := \lambda f(\tau)\varphi(b)$, dann ist $k\{\tau\}$ lokal frei von konstantem Rang d über $k \otimes_{\mathbf{F}_p} A$.

Beweis. Zum Beweis siehe wiederum [Lau91] $\square$

Beweis des Theorems. Die Abbildung $\Theta : M_A^d \longrightarrow X \backslash \{\infty\}$ ist glatt, falls die induzierte Abbildung in den Tangentialträumen für alle k-wertigen Punkte über $\mathbf{F}_p$ surjektiv ist. Die Abbildung ist gegeben durch:

$$\begin{aligned} T_{A/\mathbf{F}_p} \otimes_{A^e} k\{\tau\} &\longrightarrow T_{A/\mathbf{F}_p} \otimes_{A^e} k \\ t \otimes f(\tau) &\longmapsto t \otimes \partial(f(\tau)) \end{aligned}$$

und damit surjektiv. Nach Lemma 10.7 ist der Tangentialraum von M_A^d lokal frei vom Rang d. Da $X \setminus \{\infty\}$ glatt über $\mathbf{F}_p$ von relativer Dimension 1 ist, ist damit Θ glatt von relativer Dimension $d-1$. $\square$

Zu guter Letzt

Neben den beschriebenen Aussagen gibt es zur Theorie der Drinfeld-Moduln viele weitere Ergebnisse. Literatur findet sich, neben den Orginalarbeiten von Drinfeld, bei Laumond [Lau91], Deligne und Husemöller [DH87] und bei Gekeler [Gek80].
Im Hinblick auf den Beweis der *Fermatschen Vermutung* war die Deformationstheorie ein wichtiges Hilfsmittel. Eine intensive Einführung in diese Theorie hätte den Rahmen dieser Arbeit überschritten. Mit dem Unterabschnitt über die Faserkategorien liegt jedoch eine ausreichend einführende Basis vor, obschon auf einige grundlegende Definitionen verzichtet wurde.
Ich gehe davon aus, daß dieser Umstand dem Verständnis des Prinzips deformationstheoretischer Methoden in den Abschnitten 9 und 10 keinen Abbruch tut.

Ein Schlußwort

Je prie les patriotes, mes amis, de ne pas me reprocher de mourir autrement que pour le pays.

Je meurs victime d'une infâme coquette, et de deux dupes de cette coquette. C'est dans un misérable cancan que s'éteint ma vie.

Oh! pourquoi mourir pour si peu de chose, mourir pour quelque chose d'aussi méprisable!

Je prends le ciel à témoin que c'est contraint et forcé que j'ai cédé à une provocation que j'ai conjureé par tous les moyens.

Je me repens d'avoir dit une vérité funeste à des hommes si peu en état de l'entendre de sang-froid. Mais enfin j'ai dit la vérité. J'emporte au tombeau une conscience nette de mensonge, nette de sang patriote.

Adieu! j'avais bien de la vie pour le bien public.

Pordon pour ceux qui m'ont tué, ils sont de bonne foi.

E. Galois *Paris, 29. V. 1832*

Literatur

[Art62] M. Artin, *Grothendieck topologies*, Harvard University, 1962.

[Bou71] Nicolas Bourbaki, *Éléments de mathématique, Algèbre*, nouvelle ed., Actualités scientifiques et industrielles, vol. 1044a, Hermann, Paris, 1971 (French), Fascicule VII, Chapitre III.

[CE56] Henri Cartan and Samuel Eilenberg, *Homological Algebra*, Princton University Press, Princton, 1956, Princton Mathematical Series.

[DH87] Pierre Deligne and Dale Husemöller, *Survey of drinfeld modules*, Contemporary Mathematics **67** (1987), 25–91.

[DM69] Pierre Deligne and David Mumford, *The irreducibility of the space of given genus*, Publ. Math. I.H.C.S **36** (1969), 75–110.

[Eis90] David Eisenbud, *Schemes*, Springer Verlag, New York, 1990.

[Eis95] David Eisenbud, *Commutative algebra with a View Toward Algebraic Geometry*, Springer Verlag, New York, 1995.

[Gek80] Ernst-Ulrich Gekeler, *Drinfeld modular curves*, no. 1231, Springer-Verlag, Bonn, 1980, Lecture notes in Mathematics.

[Har77] Robin Hartshorne, *Algebraic geometry*, Graduate Texts in Mathematics, vol. 52, Springer-Verlag, New York, 1977.

[Lau91] Gérard Laumond, *Cohomology with compact supports of drinfeld modular varieties*, J. Algebra **152** (1991), no. 2, 520–524.

[Mac69] Saunders Mac Lane, *Homology*, Springer-Verlag, Berlin, 1969.

[Mat80] Hideyuki Matsumura, *Commutative ringtheory*, Cambrige University Press, New York, 1980, Cambrige studies in advanced mathematics 8.

[Neu92] Jürgen Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 1992, Grundlehren der Mathematischen Wissenschaften.

[Ser79] Jean-Pierre Serre, *Local fields*, no. 67, Springer-Verlag, New York, 1979.

[tD95] Tammo tom Dieck, *Lineare Algebra und Algebra*, Mathematisches Institut der Universität Göttingen, 1995.