KOMMUTATIVE ALGEBRAISCHE p-GRUPPEN

(MIT ANWENDUNGEN AUF p-DIVISIBLE GRUPPEN UND

ABELSCHE VARIETÄTEN)

Hanspeter Kraft

Sonderforschungsbereich
Theoretische Mathematik
Universität Bonn

53 Bonn

Wegelerstrasse 10

September 1975

Inhaltsverzeichnis

Einleitung

Bei vielen Problemen im Zusammenhang mit Abelschen Varietäten spielt die Untersuchung der <u>l-Teilungspunkte</u> eine wichtige Rolle. Dabei versteht man unter einem l-Teilungspunkt P der Abelschen Varietät A einen Punkt der Ordnung l, und die Gruppe ${}_lA$ der l-Teilungspunkte ist für l prim zur Charakteristik p des Grundkörpers k isomorph zu $(\mathbb{Z}/l\cdot\mathbb{Z})^{2d}$ mit d = Dimension der Abelschen Varietät A. Von entscheidender Bedeutung ist dabei das Studium der Operation der Galoisgruppe $Gal(\overline{k}/k)$ auf den l-Teilungspunkten und der damit zusammenhängenden Darstellungen.

Ist nun $l = p = \operatorname{char} k > 0$, so ist das <u>endliche k-Gruppenschema</u> ${}_pA = \operatorname{Ker} p\cdot Id_A$ nicht mehr reduziert; die rationalen Punkte bilden zwar wieder eine Gruppe der Gestalt $(\mathbb{Z}/p\mathbb{Z})^{\varrho}$, wobei hier aber ϱ alle Werte zwischen 0 und $d = \dim A$ annehmen kann und der <u>p-Rang von</u> A genannt wird, doch ist die Struktur von ${}_pA$ auch für algebraisch abgeschlossene Grundkörper k durch ϱ im allgemeinen nicht bestimmt : es fehlt die Beschreibung der <u>Zusammenhangskomponente der Null</u>, welche ein sogenanntes <u>infinitesimales</u> Gruppenschema ist, und speziell ihres unipotenten Bestandteiles, der für $\varrho < \dim A$ nicht verschwindet.

Im ersten Kapitel untersuchen wir nun etwas allgemeiner endliche kommutative k-Gruppenschemata $\mathfrak{G}$ mit $p\cdot Id_{\mathfrak{G}} = 0$ (im folgenden kurz <u>p-Gruppen</u> genannt). Mit Hilfe der Dieudonné-Theorie für unipotente k-Gruppen führt dies zum Studium von endlichdimensionalen k-Vektorräumen zusammen mit <u>zwei "semilinearen" nilpotenten Endomorphismen</u>, welche sich <u>gegenseitig annulieren.</u> Die hierzu notwendigen Grundlagen - eine Verallgemeinerung der Resultate [1] von <u>Gelfand-Ponomarev</u> - haben wir in einem Anhang zusammengestellt. Wir benützen dabei wesentlich eine unveröffentliche Darstellung dieser Resultate von P.Gabriel. Als Hauptergebnis erhalten wir eine <u>vollständige Klassifikation der p-Gruppen</u> und damit zusammenhängend eine explizite Beschreibung der Endomorphismenringe, der Cartier-Dualität, des Frobeniushomomorphismus und der Verschiebung,...

Im zweiten Kapitel kehren wir wieder zu unserem Ausgangsproblem zurück, wobei wir zunächst etwas allgemeiner die p-Kerne von p-divisiblen (formalen) Gruppen untersuchen. Speziell interessiert uns das Verhalten der p-Kerne in einer Isogenieklasse und die damit zusammenhängende Frage, wie stark durch den p-Kern die Isogenieklasse oder gar die Isomorphieklasse bestimmt ist. Man stellt dabei fest, dass die Antwort sehr stark von der Struktur dieses p-Kernes abhängt : ein gewisser Typ von p-Gruppen kommt in jeder Isogenieklasse vor, während ein anderer Typ sogar die Isomorphieklasse festlegt. Im Falle von Abelschen Varietäten geben wir eine vollständige Lösung dieser Frage für die Dimensionen ≤ 4. Mit den dabei entwickelten Methoden lassen sich auch noch weitere Fälle behandeln, doch dürfte eine dimensionsunabhängige allgemeine Lösung ziemlich schwierig sein. Wir haben hierzu nur einige wenige Resultate und Vermutungen.

Im folgenden arbeiten wir immer über einem festen Grundkörper k der Charakteristik $p>0$, welchen wir zudem perfekt voraussetzen. Ein wichtiger Aspekt der Theorie, nämlich das Studium von Familien von p-Gruppen, d.h. von p-Gruppen über einem Basisschema, und insbesondere das Problem der Spezialisierungen wird in der vorliegenden Arbeit nicht berührt. Gerade die hier studierten p-Gruppen bilden ein ausgezeichnetes Experimentierfeld für solche Probleme und man findet leicht viele interessante Beispiele (vgl. die Bemerkungen zu Beginn von Kapitel II). Wir hoffen, in einem späteren Zeitpunkt auf diese Probleme zurückzukommen.

Für die Theorie der algebraischen Gruppen und speziell die Dieudonné-Theorie der unipotenten k-Gruppen benutzen wir die "Groupes algébriques" von Demazure-Gabriel [GA] , für die p-divisiblen Gruppen die Lecture Notes "p-divisible Groups" von Demazure [PG] und für die Abelschen Varietäten die "Abelian Varieties" von Mumford [AV]. Den beiden Kapiteln haben wir eine kurze Inhaltsangabe vorangestellt.

P. Gabriel, F. Oort und C. Ringel danken wir für viele Gespräche und Anregungen im Zusammenhang mit dem vorliegenden Text.

Kapitel I : Klassifikation der p-Gruppen

Ist k ein perfekter Körper der Charakteristik $p > 0$, so ist ein endliches k-Gruppenschema $\mathfrak{g}$ nicht notwendig reduziert: Man hat eine Zerlegung

$$\mathfrak{g} = \mathfrak{g}_{red} \oplus \mathfrak{g}^{o}$$

wobei die Zusammenhangskomponente $\mathfrak{g}^{c}$ der Null ein sogenanntes infinitesimales k-Gruppenschema ist, d.h. von einer Potenz des Frobeniushomomorphismus annuliert wird. Dabei kann die Struktur von $\mathfrak{g}^{c}$ beliebig kompliziert sein; schon im kommutativen Falle besteht keine Hoffnung, diese Gruppen je im üblichen Sinne zu klassifizieren.

Betrachten wir nun kommutative endliche k-Gruppen $\mathfrak{g}$, welche von p = char k annuliert werden (im folgenden kurz p-Gruppen genannt), so führt dies unter Verwendung der Dieudonné-Theorie zum Studium von endlichdimensionalen k-Vektorräumen M mit zwei sich gegenseitig annulierenden "semilinearen" Endomorphismen. In ganz analoger Weise wie bei Gelfand-Ponomarev in [1] lässt sich in diesem Falle die Klassifikation durchführen; es handelt sich dabei um eine sogenannte "zahme Gattung", was im wesentlichen bedeutet, dass es bis auf Isomorphie nur endlich viele unzerlegbare Objekte einer festen Länge gibt.

Aus dieser Klassifikation erhalten wir zwei Typen von p-Gruppen: die Gruppen vom Typ T und diejenigen vom Typ Z, welche sich in verschiedener Hinsicht unterscheiden; z.B. ist bei den Gruppen vom Typ Z der Kern des Frobeniushomomorphismus gleich dem Bild der Verschiebung, während wir beim Typ T eine echte Inklusion haben. Ein weiteres Unterscheidungsmerkmal findet sich auch beim Studium der Endomorphismenringe.

Eine ausgezeichnete Rolle spielen die Gruppen vom Typ Z_1;

dies sind nach Definition direkte Summen von solchen Gruppen vom Typ Z, bei denen entweder der Frobeniushomomorphismus oder die Verschiebung einen einfachen Kern hat. Es zeigt sich nämlich, dass jede Untergruppe vom Typ Z einer solchen Gruppe ein direkter Summand ist und insbesondere wieder vom Typ Z_1 ist.

Wie wir schon in der Einleitung bemerkt haben, lassen wir hier alle Fragen über Familien von p-Gruppen und Spezialisierungen beiseite, obwohl es in diesem Zusammenhange viele interessante Probleme gibt. Man erhält z.B. aus jeder Familie von Abelschen Varietäten eines festen p-Ranges eine Familie von p-Gruppen vom Typ Z (vgl. Kap. II), und das Studium der Spezialisierungen der Gruppen vom Typ Z dürfte auch für die Theorie der Abelschen Varietäten von Interesse sein. Auf Grund der vorliegenden Resultate kann man zeigen, dass sich die Gruppen vom Typ Z in solche vom Typ T spezialisieren lassen, aber nicht umgekehrt, und man findet auch Beispiele von solchen Gruppen $\mathfrak{G}$ vom Typ Z, deren sämtliche Spezialisierungen vom Typ T oder isomorph zu $\mathfrak{G}$ sind. Der Katalog solcher Einzelresultate lässt sich beliebig vergrössern, doch fehlt bisher eine umfassende Theorie; wir hoffen jedoch in einem späteren Zeitpunkt auf diese Probleme zurückzukommen.

Obwohl in diesem Kapitel die Resultate des Anhanges ganz wesentlich benutzt werden, haben wir uns bemüht, eine in sich geschlossene Darstellung der Theorie zu geben. Insbesondere haben wir die dabei benötigten Begriffe aus dem Anhang schon hier exakt definiert und ausführlich diskutiert, so dass dieses Kapitel auch unabhängig vom Anhang gelesen und verstanden werden kann.

§1. Dieudonné-Theorie für p-Gruppen

Sei k ein perfekter Körper der Charakteristik $p > 0$. Dann verstehen wir unter einer p-Gruppe $\mathcal{G}$ ein endliches kommutatives k-Gruppenschema mit $p \cdot Id_{\mathcal{G}} = 0$. Jede solche p-Gruppe besitzt eine Zerlegung der Gestalt

$$\mathcal{G} = \mathcal{E} \oplus \mathcal{M} \oplus \mathcal{U}$$

wobei $\mathcal{E} = \mathcal{G}_{red}$ etal und eine k-Form von $(\mathbb{Z}/p\mathbb{Z})_k^r$ ist, $\mathcal{M}$ multiplikativ und eine k-Form von ${}_p\mu_k^s$ ist (${}_p\mu_k$ = Frobeniuskern der multiplikativen k-Gruppe μ_k) und $\mathcal{U}$ unipotent und infinitesimal ist (vgl. [GA] IV,§3,n°5). Ist insbesondere k algebraisch abgeschlossen, so hat $\mathcal{G}$ die Gestalt

$$\mathcal{G} = (\mathbb{Z}/p\mathbb{Z})_k^r \oplus {}_p\mu_k^s \oplus \mathcal{U} .$$

Für die Untersuchung der Struktur der unipotenten infinitesimalen p-Gruppe $\mathcal{U}$ verwenden wir nun die Dieudonné-Theorie:([GA] V,§1.): Sei D_k der Diedonné-Ring

$$D_k = \mathcal{W}(k)[F,V] \quad (FV=VF=p)$$

wobei $\mathcal{W}(k)$ der Ring der Wittschen Vektoren ist und die beiden Variablen F und V den folgenden Relationen unterliegen:

$$FV = VF = p \,, \qquad F\lambda = \lambda^{(p)}F \,, \qquad \lambda V = V\lambda^{(p)}$$

für $\lambda = (\lambda_0, \lambda_1, \lambda_2, \ldots) \in \mathcal{W}(k)$ und $\lambda^{(p)} = (\lambda_0^p, \lambda_1^p, \lambda_2^p, \ldots)$.
Der Ring D_k ist der Endomorphismenring des k-Gruppenschemas $\mathcal{W}_k$ der Wittschen Vektoren und der Funktor

$$\mathcal{G} \longmapsto M(\mathcal{G}) = \varinjlim_n \mathrm{Hom}(\mathcal{G}, \mathcal{W}_{nk})$$

§!

liefert eine Antiäquivalenz zwischen der Kategorie der unipotenten kommutativen k-Gruppen und der Kategorie der "auswischbaren" D_k-Moduln, d.h. derjenigen D_k-Moduln M, auf denen V lokal nilpotent operiert. Die <u>endlichen kommutativen unipotenten k-Gruppen</u> entsprechen dabei den auswischbaren D_k-<u>Moduln endlicher Länge</u>.

Das Studium der p-Gruppen, speziell der unipotenten infinitesimalen p-Gruppen führt nun zur Betrachtung der Ringe

$$\overline{D}_k = k[F,V]/(FV=VF=0)$$

und

$$\hat{D}_k = k[[F,V]]/(FV=VF=0)$$

wobei F und V den Relationen $F\lambda = \lambda^p F$ und $\lambda V = V\lambda^p$, $\lambda \in k$, unterliegen. Aus dem Vorangehenden erhalten wir dann folgendes Resultat:

<u>Satz:</u> <u>Die Kategorie der infinitesimalen unipotenten p-Gruppen ist antiäquivalent zur Kategorie der</u> $\hat{D}_k$-<u>Moduln endlicher Länge.</u>

Ein $\hat{D}_k$-Modul M endlicher Länge kann auch aufgefasst werden als ein endlichdimensionaler Vektorraum $_kM$ zusammen mit zwei nilpotenten, "semilinearen" Endomorphismen

$$F_M : M \longrightarrow M \quad \text{und} \quad V_M : M \longrightarrow M \quad , \; F_M V_M = V_M F_M = 0$$

$F_M(\lambda m) = \lambda^p \cdot F_M(m)$ und $V_M(\lambda m) = \lambda^{p^{-1}} \cdot V_M(m)$. Da k perfekt ist, sind F_M und V_M durch ihre Wirkung auf einer Basis des k-Vektorraumes M festgelegt.

Zu jeder natürlichen Zahl $n \geqslant 0$ und jedem Paar von nilpotenten Matrizen $\varphi, \psi \in M_n(k)$ mit $\varphi \circ \psi = \psi \circ \varphi = 0$ erhalten wir daher einen $\hat{D}_k$-Modul $M = M_{n,\varphi,\psi}$ in folgender Weise:

Der unterliegende k-Vektorraum ist k^n und die Endomorphismen F_M und V_M sind durch ihre Wirkung auf der natürlichen Basis des k^n gemäss φ und ψ festgelegt, dh. $F_M(x) = \varphi \circ x^p$ und $V_M(x) = \psi \circ x^{p^{-1}}$ für $x=(x_1,x_2,\dots,x_n) \in k^n$ und $x^p=(x_1^p,x_2^p,\dots,x_n^p)$. Offenbar ist jeder $\hat{D}_k$-Modul endlicher Länge isomorph zu einem Modul dieser Gestalt.

Das Studium der p-Gruppen und ihrer Eigenschaften, was in den folgenden Paragraphen durchgeführt werden soll, ist damit im wesentlichen äquivalent zum Studium der $\hat{D}_k$-Moduln endlicher Länge; die Übertragung der Definitionen und Eigenschaften der $\hat{D}_k$-Moduln auf die p-Gruppen werden oft stillschweigend durchgeführt unter Benützung des obigen Satzes.

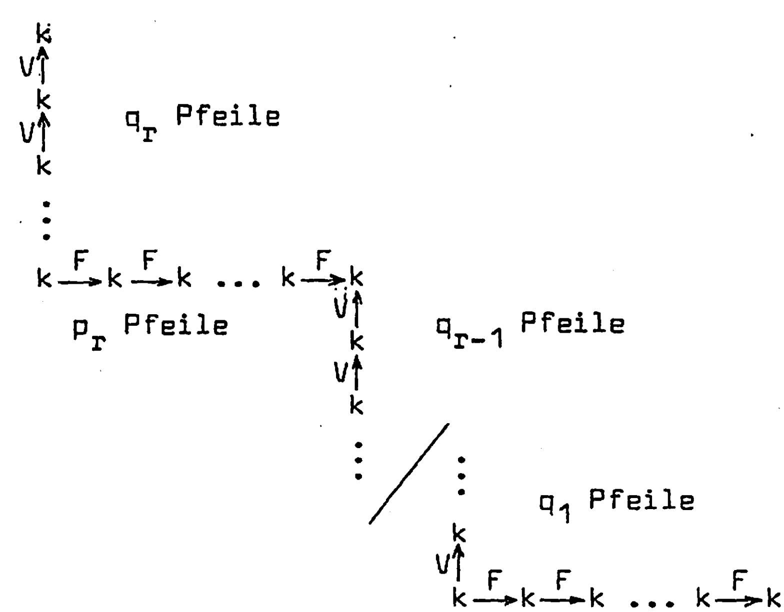
§2. Gruppen vom Typ T

Wir beginnen mit der Beschreibung von zwei speziellen Typen von p-Gruppen, den Gruppen vom Typ T in diesem Abschnitt und den Gruppen vom Typ Z im nachfolgenden Abschnitt. Man vergleiche hierzu auch die Darstellung im Anhang.

Sei $\mathcal{H}(F,V^{-1})$ die Halbgruppe mit 1 frei erzeugt von F und V^{-1}. Die Elemente $A \in \mathcal{H}(F,V^{-1})$ sind also Wörter (Monome) der Gestalt

$$A = F^{p_1}V^{-q_1}F^{p_2}V^{-q_2}\dots F^{p_r}V^{-q_r}$$

mit $p_i, q_i \in \mathbb{N}$, und zu jedem solchen Wort gehört ein $\hat{D}_k$-Modul M_A, welcher durch das folgende Diagramm beschrieben wird:



Der unterliegende k-Vektorraum von M_A ist die direkte Summe der im Diagramm vorkommenden Exemplare von k und die beiden nilpotenten semilinearen Endomorphismen F_M und V_M sind durch ihre Wirkung auf der kanonischen k-Basis von M gemäss den Pfeilen des Diagramms festgelegt.

Wir wählen ein für alle mal eine infinitesimale unipotente p-Gruppe mit Dieudonné-Modul isomorph zu M_A und bezeichnen diese mit $\mathcal{H}_A$.

Der Modul M_A und damit auch die Gruppe $\mathcal{H}_A$ ist unzerlegbar und hat die Länge

$$l(M_A) = l(\mathcal{H}_A) = l(A) + 1 = \sum_{i=1}^{r} p_i + \sum_{i=1}^{r} q_i + 1 ,$$

$$l(A) = \text{Wortlänge} = \text{Anzahl Pfeile im Diagramm.}$$

Unter der kanonischen Basis des Moduls M_A verstehen wir im folgenden immer die angeordnete kanonische Basis des unterliegenden Vektorraumes $k^{l(A)+1}$, wobei die Nummerierung der Exemplare von k in Richtung der F-Pfeile des Diagrammes erfolgt, beginnend "oben links" mit 1. Es ist leicht zu sehen, wie bei gegebenem Wort A die zu F und V zugehörigen Matrizen bezüglich der kanonischen Basis von M_A aussehen.

Definition: Eine p-Gruppe $\mathcal{H}$ heisst vom Typ T ("Treppe"), wenn $\mathcal{H}$ isomorph ist zu einer direkten Summe von Gruppen der Gestalt $\mathcal{H}_A$ mit $A \in \mathcal{H}(F,V^{-1})$.

Analog werden auch die $\hat{D}_k$-Moduln vom Typ T definiert.

Die p-Gruppen der Gestalt $\mathcal{H}_A$ sind also genau die unzerlegbaren Gruppen vom Typ T, und für $A' \neq A$ sind die beiden Gruppen $\mathcal{H}_A$ und $\mathcal{H}_{A'}$ nicht isomorph.

Bemerkung: In Verallgemeinerung des obigen Verfahrens kann man in folgender Weise weitere $\hat{D}_k$-Moduln konstruieren: Man startet wieder mit einem Wort A aus der Halbgruppe $\mathcal{H}(F,V^{-1})$ und betrachtet das zugehörige Diagramm aus Punkten und Pfeilen. Eine Belegung (Darstellung) des Diagrammes besteht nun darin, dass man jedem Punkt ein Exemplar eines k-Vektorraumes der Gestalt k^n, $n \in \mathbb{N}$, zuordnet und jedem Pfeil eine Matrix mit "richtiger" Zeilen- und Spaltenanzahl (Anzahl Zeilen = Dimension des Vektorraumes an der Pfeilspitze, und entsprechend für die Spalten). Wie vorher definiert eine solche Belegung einen $\hat{D}_k$-Modul M; es ergibt sich jedoch aus den nachfolgenden Resultaten (Struktursatz und Charakterisierung der Gruppen vom Typ Z), dass jeder solche $\hat{D}_k$-Modul M isomorph ist zu einer direkten Summe von Moduln der Gestalt $M_{A'}$, also wieder vom Typ T ist, was man übrigens auch unmittelbar direkt einsehen kann.

Für die speziellen Gruppen bzw. Moduln der Gestalt $\mathcal{H}_A$ bzw. M_A <u>definieren wir eine F-Länge und eine V-Länge</u> in folgender Weise:

$$l_F(\mathcal{H}_A) = l_F(M_A) = \sum_{i=1}^{r} p_i = \text{Anzahl F-Pfeile in } A,$$

$$l_V(\mathcal{H}_A) = l_V(M_A) = \sum_{i=1}^{r} q_i = \text{Anzahl V-Pfeile in } A,$$

($A = F^{p_1}V^{-q_1}F^{p_2}\dots F^{p_r}V^{-q_r}$ wie früher). Wir werden später sehen, wie sich diese Grössen mit Hilfe des Frobeniushomomorphismus und der Verschiebung ausdrücken lassen (§7.).

<u>Beispiele</u>: In den folgenden Beispielen steht zunächst der Modul M_A, dann das zugehörige Diagramm und anschliessend die zugehörige p-Gruppe. Dabei ist α_k die additive k-Gruppe, $\omega_{n,k}$ die k-Gruppe der Wittschen Vektoren der Länge n, und ${}_{F^m}\alpha_k$ bzw. ${}_{F^m}\omega_{n,k}$ die m-fachen Frobeniuskerne. Zur Beschreibung der k-Gruppen verwenden wir die funktorielle Schreibweise (R ist immer eine k-Algebra).

M_1 : $\bullet$ $\qquad\qquad {}_p\alpha_k$

M_{F^n} : $\bullet \xrightarrow{F} \bullet \xrightarrow{F} \cdots \xrightarrow{F} \bullet$ $\qquad\qquad {}_{p^{n+1}}\alpha_k$

$M_{V^{-m}}$:

$$\begin{tikzcd}
\bullet \\
\bullet \arrow[u, "V"'] \\
\vdots \arrow[u, "V"'] \\
\bullet \arrow[u, "V"']
\end{tikzcd}$$

$${}_F\omega_{m+1,k}$$

$M_{F^nV^{-m}}$:

$$\begin{tikzcd}
\bullet \\
\bullet \arrow[u, "V"'] \\
\vdots \arrow[u, "V"'] \\
\bullet \arrow[u, "V"'] \arrow[r, "F"'] & \bullet \arrow[r, "F"'] & \cdots \arrow[r, "F"'] & \bullet
\end{tikzcd}$$

$\mathcal{H} \subset \omega_{m+1,k}$:

$$\mathcal{H}(R) = \left\{ (r_0, r_1, \dots, r_m) / \ r_0^p = r_1^p = \dots = r_{m-1}^p = 0, \ r_m^{p^{n+1}} = 0 \right\}$$

$M_{V^{-m}F^n}$:

$$\begin{tikzcd}
\bullet \arrow[r, "F"] & \bullet \arrow[r, "F"] & \cdots \arrow[r, "F"] & \bullet \\
 & & & \bullet \arrow[u, "V"'] \\
 & & & \vdots \arrow[u, "V"'] \\
 & & & \bullet \arrow[u, "V"']
\end{tikzcd}$$

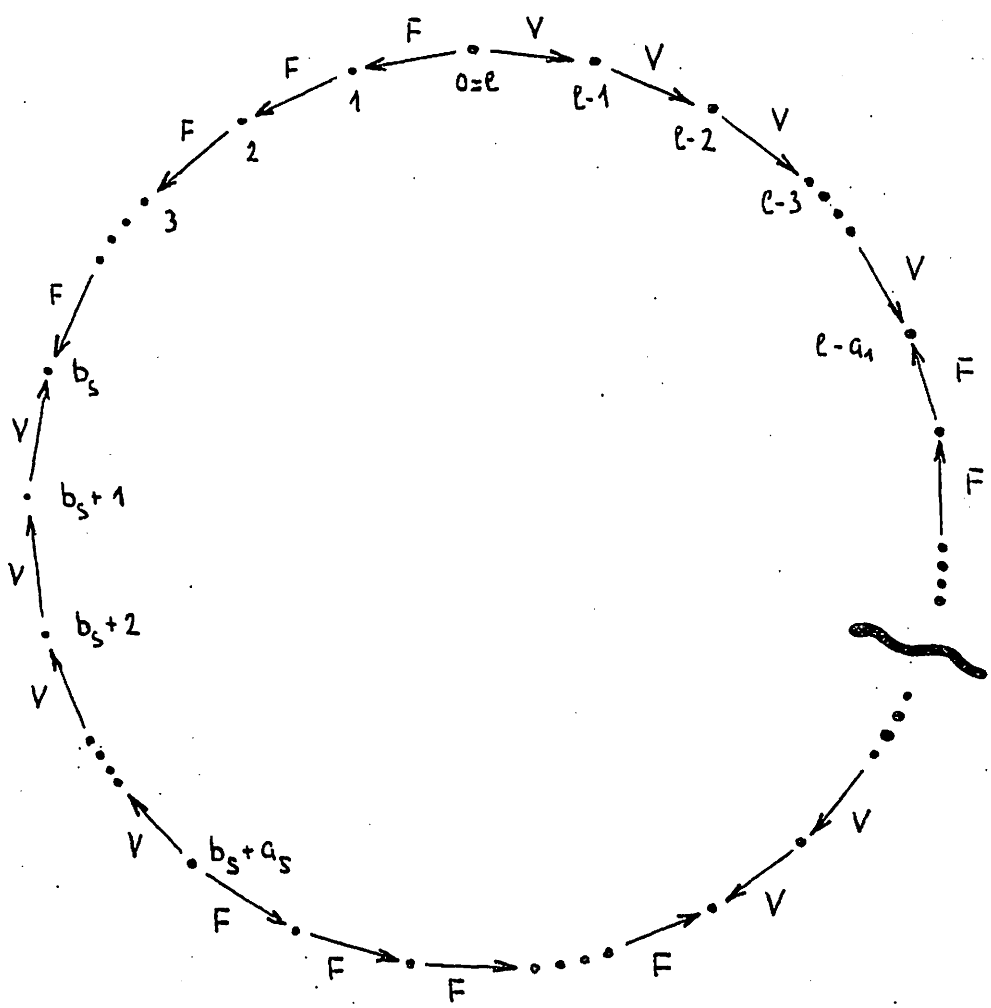
$\mathcal{H} \subset \alpha_k \oplus \omega_{m+1,k}$:

$$\mathcal{H}(R) = \left\{ (r, (r_0, r_1, \dots, r_m)) / \ r_0^p = \dots = r_m^p = 0, \ r^{p^n} = r_0 \right\}.$$

§3. Gruppen vom Typ Z

Hier betrachten wir nun die Halbgruppe $\mathcal{H}(V,F^{-1})$ und nennen ein Wort B zulässig, falls B verschieden von 1, V^n und F^{-n} mit $n \in \mathbb{N}$ ist, und nicht periodisch, falls B verschieden von C^n ist für alle $C \in \mathcal{H}(V,F^{-1})$ und $n > 1$.

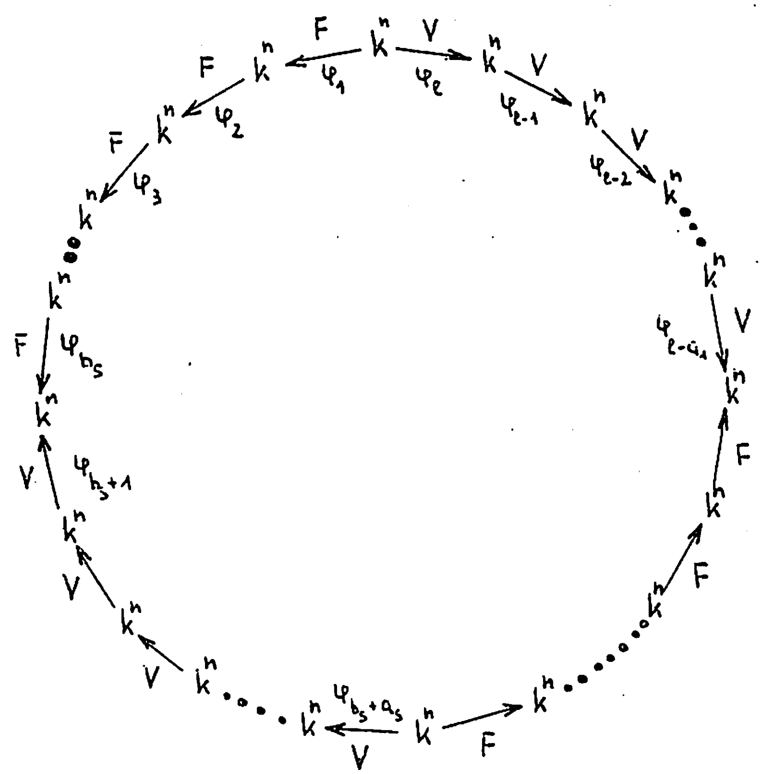
Ist $B = V^{a_1}F^{-b_1}V^{a_2}F^{-b_2}\dots V^{a_s}F^{-b_s}$ ein zulässiges Wort, so können wir B auch durch das folgende Diagramm beschreiben:



$l = l(B) = \sum_{i=1}^{s} a_i + \sum_{i=1}^{s} b_i$ ist die Wortlänge und wir denken uns immer die Punkte des Diagrammes in der angegebenen Weise durchnummeriert. Entsprechend werden auch die Pfeile des

Diagrammes nummeriert: der n-te Pfeil entspricht dem n-ten Buchstaben des Wortes B und ist der Pfeil zwischen den Punkten mit den Nummern n-1 und n.

Ist nun B ein zulässiges Wort der Länge $l = l(B)$, $n \geq 1$ eine natürliche Zahl und $\varphi_i \in Gl_n(k)$ $i=1,2,\ldots,l(B)$ invertierbare $n\times n$-Matrizen, so erhalten wir einen $\hat{D}_k$-Modul $N = N_{B,(\varphi_1,\ldots,\varphi_l)}$ beschrieben durch das folgende Diagramm:



Der unterliegende k-Vektorraum von N ist die direkte Summe der im Diagramm vorkommenden Exemplaren von k^n und die Endomorphismen F und V wirken auf der kanonischen Basis der einzelnen k^n gemäss der Belegung des Diagrammes durch die Matrizen φ_i .

Wiederum wählen wir eine <u>infinitesimale unipotente p-Gruppe mit Dieudonné-Modul isomorph zu</u> $N_{B,(\varphi_1,\varphi_2,\ldots,\varphi_l)}$ <u>und bezeichnen diese mit</u> $\mathfrak{G}_{B,(\varphi_1,\ldots,\varphi_l)}$.

Es ist klar, dass man durch geeignete Abänderung der Basis immer erreichen kann, dass alle φ_i ausser einem, etwa φ_1, gleich der Einheitsmatrix 1_n sind. Wir verwenden dafür die folgenden abkürzenden Schreibweisen:

$N_{B,\varphi}$

$$N_{B,\varphi} := N_{B,(\varphi,1_n,\dots,1_n)} \quad , \qquad N_B := N_{B,1}$$

und analog werden die Bezeichnungen $\mathfrak{G}_{B,\varphi}$ und $\mathfrak{G}_B$ definiert.
Für die speziellen Monome der Gestalt $B = V^aF^{-b}$ schreiben wir dann noch kürzer

$$N_{a,b} := N_{V^aF^{-b}} \quad , \qquad \mathfrak{G}_{a,b} := \mathfrak{G}_{V^aF^{-b}} \; .$$

Auf Grund der obigen Bemerkung wird es im folgenden meistens genügen, nur die Gruppen der Gestalt $\mathfrak{G}_{B,\varphi}$ zu betrachten.

Für die Länge der p-Gruppe $\mathfrak{G}_{B,\varphi}$ sowie auch des zugehörigen Moduls $N_{B,\varphi}$ erhalten wir

$$l(\mathfrak{G}_{B,\varphi}) = l(N_{B,\varphi}) = n\cdot l(B) = n\,(\sum_{i=1}^{s} a_i + \sum_{i=1}^{s} b_i)\,,$$
$$B = V^{a_1}F^{-b_1}V^{a_2}\dots V^{a_s}F^{-b_s} \quad , \quad \varphi \in Gl_n(k).$$

Wir definieren wiederum eine F-Länge und eine V-Länge für $\mathfrak{G}_{B,\varphi}$ bzw. $N_{B,\varphi}$:

$$l_F(\mathfrak{G}_{B,\varphi}) = l_F(N_{B,\varphi}) = n\cdot l_F(B) = n\cdot(\sum_{i=1}^{s} b_i),$$
$$l_V(\mathfrak{G}_{B,\varphi}) = l_V(N_{B,\varphi}) = n\cdot l_V(B) = n\cdot(\sum_{i=1}^{s} a_i).$$

Wir werden später diese beiden Grössen mit Hilfe des Frobeniushomomorphismus und der Verschiebung ausdrücken; insbesondere hängen sie nur vom Isomorphietyp der betrachteten Gruppe ab.

Definition: Eine p-Gruppe $\mathcal{G}$ heisst vom Typ Z ("Zykel"), wenn $\mathcal{G}$ isomorph ist zu einer direkten Summe von Gruppen der Gestalt $\mathcal{G}_{B,\varphi}$ mit zulässigem $B \in \mathcal{H}(V,F^{-1})$, $\varphi \in Gl_n(k)$ und $n \geq 1$.

Analog werden die $\hat{D}_k$-Moduln vom Typ Z definiert.

Bemerkung: Das Wort B ist durch den Isomorphietyp der Gruppe $\mathcal{G} = \mathcal{G}_{B,\varphi}$ nicht eindeutig bestimmt: Ist z.B. $B = C^m$, so lässt sich $\mathcal{G}$ auch in der Gestalt $\mathcal{G}_{C,\psi}$ schreiben.

Auch ein nicht periodisches B ist nur bis auf zyklische Vertauschung der Buchstaben von B bestimmt. Wie im Anhang könnte man eine Eindeutigkeit dadurch erzwingen, dass man unter Verwendung einer totalen Anordnung der Wörter B nur solche zulässt, welche nicht periodisch, zulässig und unter allen zyklisch vertauschten minimal sind. Es wird später im Zusammenhang mit der Cartier-Dualität klar werden, wieso wir uns hier nicht zum vorneherein auf solche Wörter beschränkt haben.

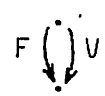
Die Frage der Unzerlegbarkeit der Gruppen $\mathcal{G}_{B,\varphi}$ werden wir im folgenden Paragraphen 4 behandeln. Wir können jedoch hier schon feststellen, dass die Gruppen $\mathcal{G}_{B,\lambda}$ mit $\lambda \in k^* = Gl_1(k)$ und zulässigem, nicht periodischem B sicher unzerlegbar sind. Etwas allgemeiner haben wir folgendes Resultat:

Lemma: Ist $B = C^m$ ein zulässiges Wort aus $\mathcal{H}(V,F^{-1})$ mit nicht periodischem C, so ist jeder direkte Summand der p-Gruppe $\mathcal{G}_{B,\varphi}$ isomorph zu einer Gruppe der Gestalt $\mathcal{G}_{C,\psi}$. Ist umgekehrt $\mathcal{G}_{C,\psi}$ isomorph zu einem direkten Summanden einer Gruppe $\mathcal{G}_{B',\varphi}$, so ist B' bis auf zyklische Vertauschung gleich einer Potenz von C.

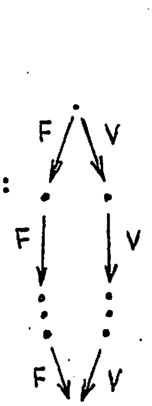
Dieses Lemma lässt sich ohne weiteres aus den allgemeinen Resultaten des Anhanges ableiten; es folgt jedoch auch unmittelbar aus den Ergebnissen der folgenden Paragraphen, so dass wir hier auf einen Beweis verzichten.

<u>Bemerkung</u>: Bei der Definition des Moduls $N_{B,(\varphi_1,\varphi_2,\dots,\varphi_t)}$ haben wir die Matrizen $\varphi_i \in Gl_n(k)$, also invertierbar vorausgesetzt. Verwenden wir beliebige Matrizen $\varphi_i \in M_n(k)$, so erhalten wir in analoger Weise einen $\hat{D}_k$-Modul, welcher jedoch im allgemeinen nicht mehr vom Typ Z ist.

<u>Beispiele</u> (vgl. die Bemerkungen zu den Beispielen am Ende des Paragraphen 2):

$N_{VF^{-1},\lambda}$:  $\mathcal{G}_\lambda \subset \omega_{2,k}$: $\mathcal{G}_\lambda(R) = \{(r_0,r_1)/\ r_0 = \lambda r_1^p,\ r_0^p = 0\}$

Bei diesen k-Gruppen handelt es sich um <u>Erweiterungen von</u> ${}_p\alpha_k$ <u>mit</u> ${}_p\alpha_k$, und zwar repräsentieren die k-Gruppen $\mathcal{G}_\lambda$, ${}_p\omega_{2k}$, ${}_{p^2}\alpha_k$ und ${}_p\alpha_k^2$ <u>alle Erweiterungsgruppen</u> von ${}_p\alpha_k$ mit ${}_p\alpha_k$, wobei $\mathcal{G}_\lambda$ und $\mathcal{G}_{\lambda'}$ genau dann isomorph sind, wenn $\lambda\cdot\lambda'^{-1} \in k^{*\,p^2-1}$ gilt (vgl. §4.).

$N_{a,b} = N_{V^aF^{-b}}$:  $\mathcal{G} \subset \omega_{a+1,k}$:

$$\mathcal{G}(R) = \{(r_0,r_1,\dots,r_a)/\ r_0^p = r_1^p = \dots = r_{a-1}^p = 0,\ r_a^{p^b} = r_0\}$$

?

§4. Unzerlegbare Gruppen vom Typ Z

k perfect

Es stellt sich nun die Frage, welche der p-Gruppen $\mathcal{G}_{B,\varphi}$ vom Typ Z unzerlegbar sind, wobei wir uns auf zulässige, nichtperiodische B beschränken können.

1

Wir betrachten hierzu die Ringe

$$R_t = k[T_t, T_t^{-1}], \qquad t \in \mathbb{N}, \ t > 0,$$

wobei die Unbestimmte T_t folgender Vertauschungsrelation genügt:

$$T_t \cdot \lambda = \lambda^{p^t} \cdot T_t \qquad \lambda \in k.$$

Ein R_t-Modul L endlicher Länge ist also ein endlichdimensionaler k-Vektorraum L zusammen mit einem semilinearen Automorphismus $\tau = \tau_L : L \longrightarrow L$ mit $\tau(\lambda v) = \lambda^{p^t} \cdot \tau(v)$.

Insbesondere definiert jede invertierbare Matrix $\alpha \in Gl_n(k)$ einen R_t-Modul L_α: der unterliegende Vektorraum ist der k^n und τ wirkt auf der kanonischen Basis wie α.

Nach dem Anhang Abschnitt 4 ist der $\hat{D}_k$-Modul $N_{B,\varphi}$ genau dann unzerlegbar, wenn der R_t-Modul L_φ unzerlegbar ist, $t = l(B)$. Genauer liefert jede Zerlegung von L_φ eine Zerlegung von $N_{B,\varphi}$.

Satz: a) Ist k algebraisch abgeschlossen, so gibt es genau einen einfachen R_t-Modul für jedes $t \in \mathbb{N}$, $t > 0$, nämlich L_1, und jeder R_t-Modul endlicher Länge ist halbeinfach. $k = \bar{k}$

b) Die Isomorphietypen von R_t-Moduln der Länge n werden klassifiziert durch $H^1(\Pi, Gl_n(\mathbb{F}_{p^t}))$ mit $\Pi = Gal(\bar{k}/k)$ und induzierter Operation von Π auf $\mathbb{F}_{p^t}$. Speziell sind die Isomorphieklassen der Moduln der Länge 1 gegeben durch die L_λ, falls $\lambda \in k^*$ ein vollständiges Repräsentantensystem mod k^{*p^t-1} durchläuft.

u für k kapp. wirkt

Beweis: Bekanntlich ist in R_t für $t > 0$ jedes Linksideal und jedes Rechtsideal ein Hauptideal (es gibt einen "linken" und einen "rechten" Euklidschen Algorithmus).

a) Ist k algebraisch abgeschlossen, so ist jedes maximale Linksideal von der Gestalt $R_t(T_t - \lambda)$ mit $\lambda \in k$ und die R_t-Moduln $L_\lambda =^t R_t/R_t(T_t - \lambda)$ sind alle untereinander isomorph : das Rechtsmultiplizieren mit $\mu \in k^*$ liefert einen Isomorphismus $L_\lambda \xrightarrow{\sim} L_{\lambda\mu^{1-p^t}}$. Es genügt daher noch zu zeigen, dass jede Erweiterung von der Gestalt

$$0 \longrightarrow L_1 \xrightarrow{i} M \xrightarrow{q} L_1 \longrightarrow 0$$

spaltet. Sei hierzu $e = i(1)$ das Bild der kanonischen Basis von L_1 unter i und $m \in M$ ein Urbild der kanonischen Basis von L_1 unter q. Dann gilt $T_t m = m + \varrho e$ für ein $\varrho \in k$; ist $\varrho = 0$, so ist km ein Untermodul von M und die Erweiterung spaltet. Für $\varrho \neq 0$ setzen wir $m' = m + \mu e$, wobei μ der Gleichung $X^{p^t} - X + \varrho = 0$ genügt und erhalten damit $T_t m' = m'$, wie eine einfache Rechnung zeigt, und damit die Behauptung.

b) Diese Behauptung ergibt sich mit den üblichen Methoden der Galoiscohomologie aus der Tatsache, dass der Endomorphismenring des R_t-Moduls L_1 gleich $\mathbb{F}_{p^t}$ ist.

Folgerung: Ist $k = \bar{k}$ algebraisch abgeschlossen, so ist jede unzerlegbare p-Gruppe vom Typ Z isomorph zu einer Gruppe $\mathcal{G}_B$ mit zulässigem nicht periodischem $B \in \mathcal{H}(V, F^{-1})$.

§5. Struktursatz

Der Beweis des folgenden Struktursatzes wird im Anhang gegeben, und zwar in der Formulierung für Moduln.

Struktursatz: Jede unipotente infinitesimale p-Gruppe ist eine direkte Summe von unzerlegbaren Gruppen vom Typ T und vom Typ Z.

Jeder $\hat{D}_k$-Modul endlicher Länge ist eine direkte Summe von Moduln vom Typ T und vom Typ Z.

Bemerkung: Die Eindeutigkeit der Zerlegung folgt aus dem bekannten Satz von Krull-Remak-Schmidt zusammen mit der Tatsache, dass der Endomorphismenring eines unzerlegbaren Objektes endlicher Länge immer ein lokaler Ring ist. Wir werden uns in §10 noch eingehend mit den Endomorphismenringen der unzerlegbaren Gruppen vom Typ T und Z beschäftigen.

Zusammen mit den Resultaten der vorangehenden Paragraphen erhalten wir noch folgenden Zusatz:

Zusatz: a) Jede k-Gruppe vom Typ T ist bereits über $\mathbb{F}_p$ definiert, und zwei solche Gruppen sind genau dann k-isomorph, wenn sie schon über $\mathbb{F}_p$ isomorph sind.

b) Ist $B \in \mathcal{H}(V,F^{-1})$ zulässig von der Länge $l = l(B)$ und n eine positive natürliche Zahl, so werden die Isomorphieklassen der p-Gruppen $\mathcal{G}_{B,\varphi}$ mit $\varphi \in Gl_n(k)$ durch die Menge $H^1(\Pi, Gl_n(\overline{\mathbb{F}}_{p^l}))$ mit $\Pi = Gal(\bar{k}/k)$ beschrieben. Für algebraisch abgeschlossene Körper k haben wir einen Isomorphismus $N_{B,\varphi} \cong N_B^n$; in diesem Falle ist jede Gruppe vom Typ Z bereits über $\mathbb{F}_p$ definiert.

Bemerkung: Ist $\mathcal{G} = \mathcal{G}_B$ eine Gruppe vom Typ Z mit $B = C^m$, so ist im algebraisch abgeschlossenen Falle $\mathcal{G}$ isomorph zu $\mathcal{G}_C^m$. Dies gilt auch noch für diejenigen Körper k, welche $\mathbb{F}_{p^l}$ enthalten, $l = l(C)$.

§6. Basiswechsel, Frobeniushomomorphismus und Verschiebung

Ist $\sigma : k \longrightarrow k'$ eine Körpererweiterung mit perfektem k', so entspricht dem Basiswechsel $\mathfrak{G}^{(\sigma)} = k' \otimes_{\sigma} \mathfrak{G}$ bei den p-Gruppen ein Funktor $M \longmapsto M^{(\sigma)} = k' \otimes_{\sigma} M$ von den $\hat{D}_k$-Moduln in die $\hat{D}_{k'}$-Moduln: Der unterliegende k'-Vektorraum von $M^{(\sigma)}$ ist $k' \otimes_{\sigma} M$ und die beiden k'-semilinearen Endomorphismen F und V von $M^{(\sigma)}$ sind durch

$$F(\lambda' \otimes m) = \lambda'^{p} F(m) , \qquad V(\lambda' \otimes m) = \lambda'^{p^{-1}} V(m)$$

eindeutig festgelegt.

Für $\sigma = ?^{p} : k \longrightarrow k$ setzen wir $M^{(\sigma)} =: M^{(p)}$, $\mathfrak{G}^{(\sigma)} =: \mathfrak{G}^{(p)}$ und entsprechend ist $M^{(p^n)}$ und $\mathfrak{G}^{(p^n)}$ definiert für alle $n \in \mathbb{Z}$. Ist z.B. $\mathfrak{G}$ über $\mathbb{F}_{p^n}$ definiert, so gilt in kanonischer Weise $\mathfrak{G}^{(p^n)} = \mathfrak{G}$.

Der Frobeniushomomorphismus $\mathcal{F}_{\mathfrak{G}} : \mathfrak{G} \longrightarrow \mathfrak{G}^{(p)}$ und die Verschiebung $\mathcal{V}_{\mathfrak{G}} : \mathfrak{G}^{(p)} \longrightarrow \mathfrak{G}$ bei den p-Gruppen lassen sich auf der Seite der $\hat{D}_k$-Moduln sehr einfach verstehen: Die beiden semilinearen Endomorphismen F_M und V_M induzieren in bekannter Weise $\hat{D}_k$-Modulhomomorphismen

contravariant

$$\mathcal{F}_M : M^{(p)} \longrightarrow M$$

$$\mathcal{V}_M : M \longrightarrow M^{(p)} .$$

$F : M \to M$

$V : M \to M$

Der Frobeniuskern ${}_{\mathcal{F}}\mathfrak{G} = \mathrm{Ker}\, \mathcal{F}_{\mathfrak{G}}$ und die grösste Untergruppe ${}_{\mathcal{V}}\mathfrak{G} \subset \mathfrak{G}$, welche von der Verschiebung annuliert wird, führen zu folgenden Definitionen:

$$_{\mathcal{F}}M = \mathrm{Coker}\, \mathcal{F}_M = M/\mathcal{F}(M^{(p)}) = M/F(M)$$

und

$$_{\mathcal{V}}M = \mathrm{Coker}\, \mathcal{V}_M^{(p^{-1})} = M/\mathcal{V}(M^{(p^{-1})}) = M/V(M) ;$$

${}_{\mathcal{F}}M$ ist der grösste Quotient von M, welcher von F annuliert wird und entsprechendes gilt für ${}_{\mathcal{V}}M$.

Es gilt also in kanonischer Weise

$$M(\mathcal{G}^{(\sigma)}) = M(\mathcal{G})^{(\sigma)} ,$$

$$M(\mathcal{F}_{\mathcal{G}}) = \mathcal{F}_{M(\mathcal{G})} \quad \text{und} \quad M(\mathcal{V}_{\mathcal{G}}) = \mathcal{V}_{M(\mathcal{G})} ;$$

$$M({}_{\mathcal{F}}\mathcal{G}) = {}_{\mathcal{F}}M(\mathcal{G}) \quad \text{und} \quad M({}_{\mathcal{V}}\mathcal{G}) = {}_{\mathcal{V}}M(\mathcal{G}) .$$

Man vergleiche hierzu [GA] II,§7,n°1, IV,§3,n°4, sowie V,§1,n°4.

Wir wollen nun alle diese Konstruktionen im Falle der speziellen Gruppen bzw. Moduln $\mathcal{H}_A$ bzw. M_A vom Typ T und $\mathcal{G}_{B,(\varphi_1,\varphi_2,\dots,\varphi_\ell)}$ bzw. $N_{B,(\varphi_1,\varphi_2,\dots,\varphi_\ell)}$ vom Typ Z, $l = l(B)$, $\varphi_i \in Gl_n(k)$, näher beschreiben:

Für einen Basiswechsel $\sigma : k \longrightarrow k'$ gilt in kanonischer Weise

$$\mathcal{H}^{(\sigma)}_{A,k} = \mathcal{H}_{A,k'} \qquad \mathcal{G}^{(\sigma)}_{B,(\varphi_1,\varphi_2,\dots,\varphi_\ell)} = \mathcal{G}_{B,(\varphi'_1,\dots,\varphi'_\ell)}$$

$$M^{(\sigma)}_{A,k} = M_{A,k'} \qquad N^{(\sigma)}_{B,(\varphi_1,\varphi_2,\dots,\varphi_\ell)} = N_{B,(\varphi'_1,\dots,\varphi'_\ell)}$$

mit $\varphi'_i = \sigma(\varphi_i)$ = Bild von φ_i in $Gl_n(k')$. Insbesondere erhalten wir

$$\mathcal{H}^{(p^n)}_A = \mathcal{H}_A , \qquad \mathcal{G}^{(p^n)}_{B,(\varphi_1,\dots,\varphi_\ell)} = \mathcal{G}_{B,(\varphi_1^{(p^n)},\dots,\varphi_\ell^{(p^n)})}$$

und entsprechend für die Moduln.

Die k-linearen Homomorphismen

$$\mathcal{F}_{M_A} : M_A \longrightarrow M_A , \qquad \mathcal{F}_{N_B} : N_{B,(\varphi_i)} \longrightarrow N_{B,(\varphi_i^{(p)})}$$

$$\mathcal{V}_{M_A} : M_A \longrightarrow M_A , \qquad \mathcal{V}_{N_B} : N_{B,(\varphi_i^{(p)})} \longrightarrow N_{B,(\varphi_i)}$$

wirken auf der kanonischen Basis von M_A und $N_{B,(\varphi_i)}$ (bzw. $N_{B,(\varphi_i^{(p)})}$) genau wie F und V. Hieraus geht hervor, dass man die Restklassen-Moduln ${}_{\mathcal{F}}M_A$ und ${}_{\mathcal{F}}N_{B,(\varphi_i)}$ (bzw. ${}_{\mathcal{V}}M_A$ und ${}_{\mathcal{V}}N_{B,(\varphi_i)}$) in folgender Weise erhält :

Im Diagramm dieser Moduln werden sämtliche Endpunkte von F-Pfeilen (bzw. V-Pfeilen) mit allen ankommenden und wegzeigenden Pfeilen weggelassen.
Dies ist natürlich auch die Beschreibung des Frobeniuskernes (bzw. des Kernes der Verschiebung) im Falle der p-Gruppen $\mathcal{H}_A$ und $\mathcal{G}_{B,(\varphi_i)}$.
Diese Moduln (oder Gruppen) zerfallen daher in eine direkte Summe von Moduln (oder Gruppen) vom Typ T, in deren Diagramme nur noch V-Pfeile (bzw. F-Pfeile) vorkommen. Man vergleiche hierzu die Klassifikation der kommutativen algebraischen k-Gruppen, welche vom Frobeniushomomorphismus bzw. der Verschiebung annuliert werden; [GA] II,§7,n°4 und IV,§3,n°6.

§7. Charakterisierung der Gruppen vom Typ Z

Aus der Beschreibung der Untergruppen ${}_{\mathfrak{F}}\mathcal{H}$ und ${}_{\mathfrak{V}}\mathcal{H}$ einer p-Gruppe $\mathcal{H} = \mathcal{H}_A$ vom Typ T, $A = F^{p_1}V^{-q_1}F^{p_2}\ldots F^{p_r}V^{-q_r}$, im vorangehenden Abschnitt erhalten wir für die Längen dieser Gruppen folgende Beziehungen:

$$l({}_{\mathfrak{F}}\mathcal{H}_A) = l(\mathcal{H}_A) - \sum_{i=1}^{r} p_i = \sum_{i=1}^{r} q_i + 1 = l_V(\mathcal{H}_A) + 1$$
$$l({}_{\mathfrak{V}}\mathcal{H}_A) = l(\mathcal{H}_A) - \sum_{i=1}^{r} q_i = \sum_{i=1}^{r} p_i + 1 = l_F(\mathcal{H}_A) + 1$$

Ebenso ergibt sich für die Gruppe $\mathcal{G} = \mathcal{G}_{B,\varphi}$ mit $\varphi \in Gl_n(k)$ und $B = V^{a_1}F^{-b_1}V^{a_2}\ldots V^{a_s}F^{-b_s}$:

$$l({}_{\mathfrak{F}}\mathcal{G}_{B,\varphi}) = n\cdot\sum_{i=1}^{s} a_i = l_V(\mathcal{G}_{B,\varphi})$$
$$l({}_{\mathfrak{V}}\mathcal{G}_{B,\varphi}) = n\cdot\sum_{i=1}^{s} b_i = l_F(\mathcal{G}_{B,\varphi}).$$

Die gleichen Formeln gelten natürlich auch für die speziellen Moduln M_A und $N_{B,\varphi}$.

Ebensoleicht erhält man folgende Beziehungen für diese Gruppen

$$l_F(\mathfrak{G}) = l(\operatorname{Im} \mathfrak{F}_{\mathfrak{G}}) \quad , \quad l_V(\mathfrak{G}) = l(\operatorname{Im} \mathfrak{V}_{\mathfrak{G}})$$

welche wir nun zur Definition der F-Länge und V-Länge für beliebige p-Gruppen benutzen:

Definition: Für eine p-Gruppe $\mathfrak{G}$ ist die F-Länge l_F und die V-Länge l_V definiert durch

$$l_F(\mathfrak{G}) = l(\operatorname{Im} \mathfrak{F}_{\mathfrak{G}}) \quad \text{und} \quad l_V(\mathfrak{G}) = l(\operatorname{Im} \mathfrak{V}_{\mathfrak{G}}).$$

Ebenso wird die F-Länge und die V-Länge von $\hat{D}_k$-Moduln endlicher Länge definiert.

Satz: Für eine unipotente infinitesimale p-Gruppe $\mathfrak{G}$ sind folgende Aussagen äquivalent:

(i) $\mathfrak{G}$ ist vom Typ Z;
(ii) $\operatorname{Im} \mathfrak{F}_{\mathfrak{G}} \xrightarrow{\sim} {}_{\mathfrak{V}}\mathfrak{G}$
(ii)' $\operatorname{Im} \mathfrak{V}_{\mathfrak{G}} \xrightarrow{\sim} {}_{\mathfrak{F}}\mathfrak{G}$
(iii) $l({}_{\mathfrak{F}}\mathfrak{G}) + l({}_{\mathfrak{V}}\mathfrak{G}) = l(\mathfrak{G})$;
(iv) $l_F(\mathfrak{G}) = l({}_{\mathfrak{V}}\mathfrak{G})$;
(iv)' $l_V(\mathfrak{G}) = l({}_{\mathfrak{F}}\mathfrak{G})$;

Bemerkung: Ist $\mathfrak{G}$ eine beliebige p-Gruppe, so sind die Aussagen (i),(ii) und (ii)' nach wie vor äquivalent. Die Bedingung (iii) charakterisiert diejenigen p-Gruppen, welche keinen direkten Summanden vom Typ T besitzen. Etwas allgemeiner gilt folgendes:

Für jede p-Gruppe $\mathfrak{G}$ ist $l({}_{\mathfrak{F}}\mathfrak{G}) + l({}_{\mathfrak{V}}\mathfrak{G}) - l(\mathfrak{G})$ gleich der Anzahl Faktoren vom Typ T in einer direkten Summenzerlegung von $\mathfrak{G}$ in unzerlegbare p-Gruppen. Ist $\mathfrak{G}$ zudem unipotent und infinitesimal, so ist diese Anzahl auch gleich $l({}_{\mathfrak{V}}\mathfrak{G}) - l_F(\mathfrak{G}) = l({}_{\mathfrak{F}}\mathfrak{G}) - l_V(\mathfrak{G})$.

Beweis: Nach dem folgenden Lemma sind die Aussagen (i), (ii) und (ii)' äquivalent. Zudem haben wir nach Definition die Implikationen (ii) $\Rightarrow$ (iv) und (ii)' $\Rightarrow$ (iv)', und offensichtlich folgt aus (iv) und (iv)' auch die Behauptung (iii). Da für eine p-Gruppe vom Typ T die Beziehung $l({}_{\mathfrak{F}}\mathfrak{G}) + l({}_{\mathfrak{V}}\mathfrak{G}) > l(\mathfrak{G})$ gilt, folgt mit dem Struktursatz auch die Implikation (iii) $\Rightarrow$ (i).

Lemma: Für einen $\hat{D}_k$-Modul endlicher Länge M sind folgende Aussagen äquivalent:

(i) M ist vom Typ Z ;

(ii) $\operatorname{Coim} \mathfrak{F}_M \xrightarrow{\sim} {}_{\mathfrak{V}}M$;

(ii)' $\operatorname{Coim} \mathfrak{V}_M \xrightarrow{\sim} {}_{\mathfrak{F}}M$.

Beweis: a) Ist M einer der speziellen Moduln M_A vom Typ T oder $N_{B,\varphi}$ vom Typ Z, so lässt sich nach §6 $\operatorname{Coim} \mathfrak{F}_M$ (bzw. $\operatorname{Coim} \mathfrak{V}_M$) folgendermassen beschreiben: Im Diagramm von M werden alle Punkte weggelassen, bei denen kein F-Pfeil (bzw. kein V-Pfeil) wegzeigt. Im Falle eines Moduls vom Typ Z sind das aber genau die Endpunkte von V-Pfeilen (bzw. F-Pfeilen), und wir erhalten daher in diesem Falle $\operatorname{Coim} \mathfrak{F}_M \xrightarrow{\sim} {}_{\mathfrak{V}}M$ (bzw. $\operatorname{Coim} \mathfrak{V}_M \xrightarrow{\sim} {}_{\mathfrak{F}}M$), womit die Implikationen (i) $\Rightarrow$ (ii) und (i) $\Rightarrow$ (ii)' bewiesen sind.

b) Ist $M = M_A$ ein Modul vom Typ T, so erhalten wir mit den Beziehungen zu Anfang dieses Abschnittes:

$$l(\operatorname{Coim} \mathfrak{F}_M) = l(\operatorname{Im} \mathfrak{F}_M) = l_F(M) = l({}_{\mathfrak{V}}M) - 1$$

$$l(\operatorname{Coim} \mathfrak{V}_M) = l(\operatorname{Im} \mathfrak{V}_M) = l_V(M) = l({}_{\mathfrak{F}}M) - 1$$

woraus mit Hilfe des Struktursatzes §5 die Implikationen (ii) $\Rightarrow$ (i) und (ii)' $\Rightarrow$ (i) folgen.

§8. Cartier-Dualität

Ist $\mathcal{G}$ eine endliche kommutative k-Gruppe, so ist die Cartier-duale Gruppe ${}^t\mathcal{G}$ definiert durch

$$ {}^t\mathcal{G} = \mathcal{H}om(\mathcal{G}, \mu_k) $$

([GA] II, §1, 2.10). Die Übertragung dieser Dualität auf die Dieudonné-Moduln führt zu folgender Definition des dualen Moduls ${}^tM$ zu einem $\hat{D}_k$-Modul M endlicher Länge : Der unterliegende k-Vektorraum ist $\mathrm{Hom}_k(M,k)$ und die Endomorphismen F und V sind definiert durch

$$ F(\alpha)(m) = \alpha(V(m))^p $$
$$ V(\alpha)(m) = \alpha(F(m))^{p^{-1}} $$

für $\alpha \in \mathrm{Hom}_k(M,k)$ und $m \in M$. Eine kleine Rechnung zeigt, dass die so definierten Abbildungen $F(\alpha)$ und $V(\alpha) : M \longrightarrow k$ k-linear sind und dass die Vertauschungsregeln $F(\lambda\alpha) = \lambda^p F(\alpha)$ und $V(\lambda\alpha) = \lambda^{p^{-1}} V(\alpha)$, $\lambda \in k$, gelten.

Für eine unipotente infinitesimale p-Gruppe $\mathcal{G}$ gilt dann in kanonischer Weise

$$ M({}^t\mathcal{G}) = {}^tM(\mathcal{G}). $$

Ist $\varphi : M \longrightarrow N$ ein $\hat{D}_k$-Modulhomomorphismus, so ist die duale Abbildung ${}^t\varphi : {}^tM \longrightarrow {}^tN$ wieder $\hat{D}_k$-linear, und wir erhalten einen funktoriellen Isomorphismus

$$ {}^t({}^tM) \xrightarrow{\sim} M . $$

Wir wollen nun die Cartier-Dualität im Falle der Gruppen $\mathcal{H}_A$ vom Typ T und $\mathcal{G}_{B,(\varphi_1,\ldots,\varphi_l)}$ vom Typ Z explizit beschreiben, $l = l(B)$, $\varphi_i \in Gl_n(k)$.

Ist A ein Wort aus der Halbgruppe $\mathcal{H}(F,V^{-1})$ (bzw. B ein zulässiges Wort aus $\mathcal{H}(V,F^{-1})$), so erhält man durch Vertauschen der Buchstaben F und V^{-1} (bzw. V und F^{-1}) ein neues Wort aus $\mathcal{H}(F,V^{-1})$ (bzw. ein zulässiges Wort aus $\mathcal{H}(V,F^{-1})$), welches wir mit ${}^tA$ (bzw. ${}^tB$) bezeichnen. Es gilt dann in kanonischer Weise

$${}^t\mathcal{H}_A = \mathcal{H}_{{}^tA}, \qquad {}^tM_A = M_{{}^tA},$$

$${}^t\mathcal{G}_{B,(\varphi_1,\dots,\varphi_l)} = \mathcal{G}_{{}^tB,({}^t\varphi_1,\dots,{}^t\varphi_l)}$$

$${}^tN_{B,(\varphi_1,\dots,\varphi_l)} = N_{{}^tB,({}^t\varphi_1,\dots,{}^t\varphi_l)}$$

Für das Diagramm bedeutet dies folgendes: Sämtliche vorkommenden Pfeile werden umgedreht und komplementär bezeichnet, wobei beim Typ Z gleichzeitig die Matrizen φ_i durch ihre Transponierten ersetzt werden.

Als letztes notieren wir noch folgendes:

1) ${}^t?$ vertauscht mit (perfektem) Basiswechsel

2) ${}^t\mathcal{F}_{\mathcal{G}} = \mathcal{V}_{{}^t\mathcal{G}}$ und ${}^t\mathcal{V}_{\mathcal{G}} = \mathcal{F}_{{}^t\mathcal{G}}$; insbesondere gilt

$${}^t({}_{\mathcal{F}}\mathcal{G}) = \mathrm{Coker}\,\mathcal{V}_{{}^t\mathcal{G}} \quad \text{bzw.} \quad {}^t({}_{\mathcal{F}}M) = \mathrm{Ker}\,\mathcal{V}_{{}^tM}$$

$${}^t({}_{\mathcal{V}}\mathcal{G}) = \mathrm{Coker}\,\mathcal{F}^{(p^{-1})}_{{}^t\mathcal{G}} \quad \text{bzw.} \quad {}^t({}_{\mathcal{V}}M) = \mathrm{Ker}\,\mathcal{F}^{(p^{-1})}_{{}^tM}$$

3) Der Typ (T oder Z) ändert sich beim Dualisieren nicht.

4) $l_F({}^t\mathcal{G}) = l_V(\mathcal{G})$ und $l_V({}^t\mathcal{G}) = l_F(\mathcal{G})$.

Alle diese Behauptungen ergeben sich unmittelbar aus den Definitionen.

§9. Sockel und Deckel

Bis auf Isomorphie ist der Frobeniuskern ${}_p\alpha_k$ der additiven k-Gruppe α_k die einzige einfache infinitesimale unipotente p-Gruppe; im Falle aller p-Gruppen kommen noch die k-Formen von $(\mathbb{Z}/p\mathbb{Z})_k$ und ${}_p\mu_k$ dazu.
Wir definieren nun den Sockel $\mathfrak{S}(\mathfrak{G}) \subset \mathfrak{G}$ einer p-Gruppe als die grösste halbeinfache Untergruppe von $\mathfrak{G}$ und den Deckel $\mathfrak{G} \longrightarrow \mathfrak{D}(\mathfrak{G})$ als den grössten halbeinfachen Quotienten von $\mathfrak{G}$. Die Länge von $\mathfrak{S}(\mathfrak{G})$ bzw. $\mathfrak{D}(\mathfrak{G})$ bezeichnen wir mit $\sigma(\mathfrak{G})$ bzw. $\delta(\mathfrak{G})$.
Für einen $\hat{D}_k$-Modul M definieren wir ebenfalls den Sockel $\mathfrak{S}(M) \subset M$ bzw. den Deckel $M \longrightarrow \mathfrak{D}(M)$ als den grössten halbeinfachen Untermodul bzw. den grössten halbeinfachen Quotienten von M; für die Längen setzen wir wiederum $\sigma(M)$ bzw. $\delta(M)$.
Ist $\mathfrak{G}$ infinitesimal und unipotent, so erhalten wir also in kanonischer Weise

$$M(\mathfrak{S}(\mathfrak{G})) = \mathfrak{D}(M(\mathfrak{G})), \qquad M(\mathfrak{D}(\mathfrak{G})) = \mathfrak{S}(M(\mathfrak{G}))$$

sowie

$$\sigma(\mathfrak{G}) = \delta(M(\mathfrak{G})), \qquad \delta(\mathfrak{G}) = \sigma(M(\mathfrak{G})).$$

Zudem ist $\mathfrak{S}(\mathfrak{G}) \xrightarrow{\sim} {}_p\alpha_k^{\sigma(\mathfrak{G})}$ und $\mathfrak{D}(\mathfrak{G}) \xrightarrow{\sim} {}_p\alpha_k^{\delta(\mathfrak{G})}$, und entsprechend $\mathfrak{S}(M) \xrightarrow{\sim} k^{\sigma(M)}$ und $\mathfrak{D}(M) \xrightarrow{\sim} k^{\delta(M)}$; insbesondere ist $\delta(M)$ die minimale Erzeugendenanzahl von M als $\hat{D}_k$-Modul.
Es ist leicht zu sehen, dass die beiden Funktoren $\mathfrak{S}$ und $\mathfrak{D}$ mit perfektem Basiswechsel vertauschen, wenn wir uns auf die unipotenten infinitesimalen p-Gruppen bzw. die $\hat{D}_k$-Moduln beschränken.

Im Falle der speziellen Moduln M_A vom Typ T bzw. $N_{B,(\varphi_1,\ldots,\varphi_\ell)}$ vom Typ Z lassen sich die Grössen $\sigma(M)$ und $\delta(M)$ aus dem Diagramm ablesen: σ ist die Anzahl der gemeinsamen Spitzen von V- und F-Pfeilen ($\xrightarrow{F}\cdot\xleftarrow{V}$) und δ ist die Anzahl der gemeinsamen Anfangspunkte von V- und F-Pfeilen ($\xleftarrow{F}\cdot\xrightarrow{V}$), wobei im Falle $N_{B,(\varphi_1,\ldots,\varphi_\ell)}$ mit $\varphi_i \in Gl_n(k)$ jeder Punkt mit der Vielfachheit n zu zählen ist.

Die Behauptungen des folgenden Lemmas ergeben sich unmittelbar aus den Definitionen:

Lemma: *Sei* $\mathfrak{G}$ *eine p-Gruppe. Dann gilt:*

(i) ${}^t\varphi(\mathfrak{G}) \xrightarrow{\sim} \mathcal{D}({}^t\mathfrak{G})$ *und* ${}^t\mathcal{D}(\mathfrak{G}) \xrightarrow{\sim} \varphi({}^t\mathfrak{G})$ *in kanonischer Weise; insbesondere ist* $\sigma({}^t\mathfrak{G}) = \delta(\mathfrak{G})$ *und* $\delta({}^t\mathfrak{G}) = \sigma(\mathfrak{G})$.

(ii) *Ist* $\mathfrak{G}$ *vom Typ Z, so ist* $\sigma(\mathfrak{G}) = \delta(\mathfrak{G})$.

(iii) *Ist* $\mathfrak{G}$ *unipotent und infinitesimal, so ist* $|\delta(\mathfrak{G}) - \sigma(\mathfrak{G})| \leq$ *Anzahl der unzerlegbaren Faktoren vom Typ T in einer direkten Summenzerlegung von* $\mathfrak{G}$ *in unzerlegbare Faktoren*.

Die gleichen Behauptungen gelten natürlich auch für $\hat{D}_k$-Moduln M endlicher Länge.

Wir untersuchen nun das *Verhalten der Grössen* σ, δ, l_F und l_V *bei exakten Sequenzen*, speziell für den Fall, wo der Kern oder der Cokern die Länge 1 hat. Wiederum formulieren wir die Behauptungen nur für p-Gruppen und überlassen die Übertragung auf $\hat{D}_k$-Moduln dem Leser.

Satz: a) *Sei* $0 \to \alpha_p \to \mathfrak{G} \to \overline{\mathfrak{G}} \to 0$ *eine exakte Sequenz von p-Gruppen. Dann gilt:*

(i) $\delta(\overline{\mathfrak{G}}) \leq \delta(\mathfrak{G}) \leq \delta(\overline{\mathfrak{G}}) + 1$ *mit* $\delta(\mathfrak{G}) = \delta(\overline{\mathfrak{G}}) + 1$ *genau dann, wenn die Folge spaltet*.

(ii) $\sigma(\overline{\mathfrak{G}})-1 \leq \sigma(\mathfrak{G}) \leq \sigma(\overline{\mathfrak{G}})+1$

(iii) *Ist* $\mathfrak{G}$ *vom Typ Z, so folgt* $l_F(\mathfrak{G}) = l_F(\overline{\mathfrak{G}}) + 1$ *und* $l_V(\mathfrak{G}) = l_V(\overline{\mathfrak{G}}) + 1$

b) <u>Sei</u> $0 \to \mathfrak{G}' \to \mathfrak{G} \to {}_p\alpha \to 0$ <u>eine exakte Sequenz von p-Gruppen</u>. <u>Dann gilt</u>:

(i) $\sigma(\mathfrak{G}') \leq \sigma(\mathfrak{G}) \leq \sigma(\mathfrak{G}') + 1$ <u>mit</u> $\sigma(\mathfrak{G}) = \sigma(\mathfrak{G}') + 1$ <u>genau dann</u>, <u>wenn die Folge spaltet</u>.

(ii) $\delta(\mathfrak{G}') - 1 \leq \delta(\mathfrak{G}) \leq \delta(\mathfrak{G}') + 1$.

(iii) <u>Ist</u> $\mathfrak{G}$ <u>vom Typ Z, so folgt</u> $l_F(\mathfrak{G}) = l_F(\mathfrak{G}') + 1$ <u>und</u> $l_V(\mathfrak{G}) = l_V(\mathfrak{G}') + 1$.

<u>Beweis</u>: Wir können ohne Einschränkung $\mathfrak{G}$ und $\mathfrak{G}'$ infinitesimal und unipotent voraussetzen und folglich k algebraisch abgeschlossen annehmen. Die einander entsprechenden Aussagen von a) und b) sind dual zueinander, und es genügt daher, je eine davon zu beweisen. Aus b) erhalten wir die exakte Sequenz $0 \to \mathcal{G}(\mathfrak{G}') \to \mathcal{G}(\mathfrak{G}) \to {}_p\alpha$ und damit die Behauptung (i).
Aus der Sequenz a) $0 \to {}_p\alpha \to \mathfrak{G} \xrightarrow{\varphi} \overline{\mathfrak{G}} \to 0$ erhalten wir die exakte Sequenz $0 \to {}_p\alpha \to \widetilde{\mathfrak{G}} \to \mathcal{G}(\overline{\mathfrak{G}}) \to 0$ mit $\widetilde{\mathfrak{G}} = \varphi^{-1}(\mathcal{G}(\overline{\mathfrak{G}})) \subset \mathfrak{G}$.
Spaltet diese Folge, so ergibt sich $\sigma(\mathfrak{G}) = \sigma(\widetilde{\mathfrak{G}}) = \sigma(\overline{\mathfrak{G}})+1$; andernfalls enthält $\widetilde{\mathfrak{G}}$ einen unzerlegbaren direkten Summanden $\mathfrak{G}_1$ der Länge ≥ 2. Es gilt dann $\operatorname{Ker} \varphi \subseteq \mathfrak{G}_1$ und wir erhalten eine exakte Sequenz $0 \to {}_p\alpha \to \mathfrak{G}_1 \to {}_p\alpha^s \to 0$ mit $1 \leq s \leq \sigma(\overline{\mathfrak{G}})$. Wegen der Unzerlegbarkeit von $\mathfrak{G}_1$ folgt aus dem vorangehenden Lemma (iii) die Abschätzung $s \leq 2$. Nach Konstruktion ist $\widetilde{\mathfrak{G}} = \mathfrak{G}_1 \oplus {}_p\alpha^r$ mit $r+s = \sigma(\overline{\mathfrak{G}})$, und daher

$$\sigma(\mathfrak{G}) = \sigma(\widetilde{\mathfrak{G}}) = r + 1 = \sigma(\overline{\mathfrak{G}}) - (s-1) ,$$

womit wegen $s \leq 2$ die Behauptung (ii) bewiesen ist.
Ist $\mathfrak{G}$ vom Typ Z, so gilt nach Definition $\mathcal{G}(\mathfrak{G}) \subseteq \operatorname{Im} \mathfrak{J}_{\mathfrak{G}}$ und $\mathcal{G}(\mathfrak{G}) \subseteq \operatorname{Im} \vartheta_{\mathfrak{G}}$ (man vergleiche die Beschreibung von Sockel und Deckel für die speziellen Gruppen $\mathfrak{G}_{B,\varphi}$ zu Beginn dieses Abschnittes). Wir erhalten daher aus der Sequenz a) (mit $\mathfrak{G}$ vom Typ Z) die beiden exakten Sequenzen

$$0 \to {}_p\alpha \to \operatorname{Im} \mathfrak{J}_{\mathfrak{G}} \to \operatorname{Im} \mathfrak{J}_{\overline{\mathfrak{G}}} \to 0$$

und

$$0 \to {}_p\alpha \to \operatorname{Im} \vartheta_{\mathfrak{G}} \to \operatorname{Im} \vartheta_{\overline{\mathfrak{G}}} \to 0 ,$$

woraus mit $l_F(\mathfrak{G}) = l(\mathrm{Im}\, \mathfrak{F}_{\mathfrak{G}})$ und $l_V(\mathfrak{G}) = l(\mathrm{Im}\, \mathfrak{V}_{\mathfrak{G}})$ (nach Definition §7) die Behauptung (iii) folgt.

Wir ziehen noch eine Folgerung aus diesem Satz, welche wir im Kapitel II benutzen werden.

Folgerung: Ist $0 \longrightarrow {}_p\alpha \longrightarrow \mathfrak{G} \longrightarrow \mathfrak{H} \longrightarrow {}_p\alpha \longrightarrow 0$ eine exakte Sequenz von p-Gruppen, $\mathfrak{G}$ und $\mathfrak{H}$ vom Typ Z, so gilt:

$$\text{(i)} \quad l_F(\mathfrak{G}) = l_F(\mathfrak{H}) \,, \quad l_V(\mathfrak{G}) = l_V(\mathfrak{H}) \,,$$

$$\text{(ii)} \quad |\delta(\mathfrak{G}) - \delta(\mathfrak{H})| \leq 1 \,, \quad |\sigma(\mathfrak{G}) - \sigma(\mathfrak{H})| \leq 1 \,.$$

§10. Endomorphismenringe

Ist $\mathfrak{G}$ eine p-Gruppe bzw. M ein $\hat{D}_k$-Modul endlicher Länge, so bezeichnen wir mit $\mathcal{E}_{\mathfrak{G}}$ bzw. $\mathcal{E}_M$ den Endomorphimenring

$$\mathcal{E}_{\mathfrak{G}} = \mathrm{End}\, \mathfrak{G} \qquad \text{bzw.} \qquad \mathcal{E}_M = \mathrm{End}_{\hat{D}_k}(M) \,.$$

$\mathcal{E}_M$ und damit auch $\mathcal{E}_{\mathfrak{G}}$ lässt sich in den Matrizenring $M_l(k)$, $l = l(M)$, oder $= l(\mathfrak{G})$, einbetten und kann als algebraischer k-Ring aufgefasst werden (vgl. z.B. [3]).

Der folgende Satz liefert einige Strukturaussagen für den Endomorphismenring; dabei beschränken wir uns bei der Formulierung auf den Fall der p-Gruppen und überlassen dem Leser die Übertragung der Resultate auf den Fall der $\hat{D}_k$-Moduln.

Satz: Ist k algebraisch abgeschlossen und $\mathfrak{g}$ eine unzerlegbare infinitesimale unipotente p-Gruppe, so erhalten wir für den Endomorphismenring $\mathcal{E}_{\mathfrak{g}}$ von $\mathfrak{g}$ folgende Strukturaussagen:

(i) $\mathcal{E}_{\mathfrak{g}}$ ist ein lokaler Ring mit nilpotentem Maximalideal $\mathfrak{m}$, und zwar gilt $\mathfrak{m}^n = 0$ für $n \geq l(\mathfrak{g})$.

(ii) Der Restklassenring $\mathcal{E}_{\mathfrak{g}}/\mathfrak{m}$ ist ein kommutativer Körper:

$$\mathcal{E}_{\mathfrak{g}}/\mathfrak{m} \xrightarrow{\sim} \begin{cases} k & \text{falls } \mathfrak{g} \text{ vom Typ I}, \\ \mathbb{F}_{p^l} & \text{falls } \mathfrak{g} \text{ vom Typ Z}, \ l = l(\mathfrak{g}) \end{cases}$$

Zudem besitzt die kanonische Projektion $pr\colon \mathcal{E}_{\mathfrak{g}} \longrightarrow \mathcal{E}_{\mathfrak{g}}/\mathfrak{m}$ einen Schnitt, welcher ein Ringhomomorphismus ist.

(iii) Ist $l(\mathfrak{g}) > 1$, so ist das Zentrum von $\mathcal{E}_{\mathfrak{g}}$ gleich $\mathbb{F}_p$.

(iv) $\mathfrak{g}$ besitzt eine unter $\mathcal{E}_{\mathfrak{g}}$ stabile Kompositionsreihe $\mathfrak{g} = \mathfrak{g}_0 \supset \mathfrak{g}_1 \supset \mathfrak{g}_2 \supset \ldots \supset \mathfrak{g}_{l-1} \supset \mathfrak{g}_l = 0$ mit $\mathfrak{m}\mathfrak{g}_i \subseteq \mathfrak{g}_{i+1}$; insbesondere lässt sich $\mathcal{E}_{\mathfrak{g}}$ in den Ring $T_l \subset M_l(k)$ der unteren Dreiecksmatrizen einbetten.

Beweis: Wir beweisen den Satz in der entsprechenden Formulierung für einen unzerlegbaren $\hat{D}_k$-Modul M anstelle der unipotenten infinitesimalen p-Gruppe $\mathfrak{g}$.

a) Die Behauptung (i) gilt ganz allgemein für den Endomorphismenring eines unzerlegbaren Moduls endlicher Länge (vgl. [BA8] §2, Exercice 3, Seite 27): es gibt eine Kompositionsreihe

$$M = M_0 \supset M_1 \supset M_2 \supset \ldots \supset M_{l-1} \supset M_l = 0$$

mit $\mathfrak{m} M_i \supset M_{i+1}$.

b) Ist $M = M_A$ unzerlegbar vom Typ T, so erhalten wir einen Ringhomomorphismus $\iota : k \longrightarrow \mathcal{E}_M$ folgendermassen: $\iota(\lambda)$ wirkt auf das i-te Exemplar von k in M_A durch Multiplizieren mit λ^{p^i}, dh. bezüglich der kanonischen Basis von M_A hat $\iota(\lambda)$ die Gestalt

$$\begin{pmatrix} \lambda & & & 0 \\ & \lambda^{p} & & \\ & & \ddots & \\ 0 & & & \lambda^{p^{e-1}} \end{pmatrix}$$

(vgl. §2.). Nach dem folgenden Lemma gibt es einen unter $\mathcal{E}_M$ stabilen Untermodul $M' = ke$ mit $e = e_i$ aus der kanonischen Basis von M_A. Wir erhalten daher einen Ringhomomorphismus

$\rho : \mathcal{E}_M \longrightarrow \mathrm{End}_{\hat{D}_k}(M') = k$ mit $\rho \circ \iota = ?^{p^i}$; ρ ist daher surjektiv, besitzt einen Schnitt und $\mathcal{E}_M / \mathfrak{M} \xrightarrow{\sim} k$, womit die eine Hälfte der Behauptung (ii) bewiesen ist.

c) Im Falle $M = N_B$ unzerlegbar vom Typ Z finden wir eine Einbettung $\iota : \mathbb{F}_{p^e} \longrightarrow \mathcal{E}_M$ wie oben gegeben durch

$$\iota(\lambda) = \begin{pmatrix} \lambda & & & 0 \\ & \lambda^{p} & & \\ & & \ddots & \\ 0 & & & \lambda^{p^{e-1}} \end{pmatrix}, \qquad l = l(B),$$

bezüglich der kanonischen Basis von N_B. Wie unter b) folgt auch hier unter Verwendung des nachfolgenden Lemmas, dass $\mathcal{E}_M / \mathfrak{M}$ sich in k einbetten lässt und daher ein kommutativer Körper ist, und wir werden unter e) zeigen, dass die Komposition $\mathbb{F}_{p^e} \xrightarrow{\iota} \mathcal{E}_M \xrightarrow{pr} \mathcal{E}_M / \mathfrak{M}$ ein Isomorphismus ist. Da $\mathcal{E}_M / \mathfrak{M}$ ein algebraischer Ring ist, ist $\mathcal{E}_M / \mathfrak{M}$ entweder ein endlicher Körper oder isomorph zu k (vgl. [3])

d) Wir beweisen nun (iv) durch Induktion und haben hierzu folgendes zu zeigen: Ist $\varphi : M \longrightarrow \overline{M}$ ein unter $\mathcal{E}_M$ invarianter Restklassenmodul von der Länge ≥ 1 und ist $\overline{\mathcal{E}} \subseteq \mathcal{E}_{\overline{M}}$ das Bild des Endomorphismenringes $\mathcal{E}_M$ in $\mathcal{E}_{\overline{M}}$, so gibt es in $\overline{M}$ einen unter $\overline{\mathcal{E}}$ stabilen eindimensionalen Untermodul. Sei hierfür $N \subset \varphi(\overline{M})$ der grösste Untermodul des Sockels, welcher vom Bild des Maximalideals $\mathfrak{M}$ von $\mathcal{E}_M$ in $\mathcal{E}_{\overline{M}}$ annuliert wird. Dann faktorisiert die Abbildung

$\mathcal{E}_M \longrightarrow \mathrm{End}_{\hat{D}_k}(N) = \mathcal{E}_N$ über den kommutativen Restklassenkörper $k_0 = \mathcal{E}_M/\mathfrak{M}$ und wir erhalten eine Einbettung $k_0 \hookrightarrow \mathcal{E}_N \simeq M_s(k)$ mit $s = l(N)$. Da alle vorkommenden Ringe und Homomorphismen algebraisch sind, lässt sich diese Einbettung diagonalisieren, womit (iv) bewiesen ist.

e) Wir wollen nun noch den fehlenden Teil des Beweises von (ii) beenden. Sei hierzu wieder $M = N_B$ unzerlegbar vom Typ Z. Nach d) gibt es dann eine k-Vektorraumbasis $\{f_0, f_1, .., f_{l-1}\}$ von M, bezüglich welcher die Endomorphismen aus $\mathcal{E}_M$ durch Dreiecksmatrizen dargestellt werden:

$$\mathcal{E}_M \hookrightarrow T_l = \{(a_{ij}) \in M_l(k) \mid a_{ij} = 0 \text{ für } i < j\}$$

Ist nun die Komposition $\mathbb{F}_{p^\ell} \xrightarrow{\iota} \mathcal{E}_M \xrightarrow{pr} \mathcal{E}_M/\mathfrak{M} = k_0$ nicht surjektiv, so gibt es ein Element $\alpha \in \mathcal{E}_M$ derart, dass $pr(\alpha) = \bar{\alpha} \notin \mathbb{F}_{p^\ell}$, aber α algebraisch über $\mathbb{F}_{p^\ell}$ ist. Die Potenzen α^{p^s} haben die gleiche Eigenschaft und sind für genügend grosses s Diagonalmatrizen. Hieraus folgt, dass $\iota(\mathbb{F}_{p^\ell})$ aus Diagonalmatrizen besteht, aber echt in $\mathcal{E}_M \cap \Delta_\ell$ enthalten ist (Δ_ℓ = Diagonalmatrizen in $M_l(k)$). Da die Darstellungen von $\mathbb{F}_{p^\ell}$ auf den ke_i (e_i aus der kanonischen Basis von M_A) gegeben durch $\lambda \longmapsto \lambda^{p^i} \cdot ? \in \mathrm{End}_{\hat{D}_k}(ke_i)$ für $i=0,1,..,l-1$ paarweise nicht isomorph sind, handelt es sich bei der obigen Basis $\{f_0, f_1, .., f_{l-1}\}$ bis auf Reihenfolge und skalare Vielfache um die kanonische Basis von M_A. Es ist nun aber leicht zu sehen, dass eine bezüglich der kanonischen Basis diagonale Matrix α genau dann einen $\hat{D}_k$-Modulendomorphismus induziert, wenn $\alpha \in \iota(\mathbb{F}_{p^\ell})$ gilt.

f) Um (iii) zu beweisen, denken wir uns wieder den Endomorphismenring $\mathcal{E}_M$ in die Dreiecksmatrizen eingebettet: $\mathcal{E}_M \hookrightarrow T_l(k) \subset M_l(k)$. Ist nun $\alpha \in \mathrm{Zent}\, \mathcal{E}_M$, so vertauscht α mit allen Diagonalmatrizen in $\mathcal{E}_M$ und daher auch mit der von diesen Matrizen erzeugten k-Unteralgebra von $M_l(k)$, welche aus allen Diagonalmatrizen besteht (beachte die Definition von ι : k bzw. $\mathbb{F}_p \longrightarrow \mathcal{E}_M$). Das Zentrum von $\mathcal{E}_M$ muss daher aus Diagonalmatrizen bestehen. Ist zudem $\mathfrak{F}_M$ oder $\mathfrak{V}_M$ nicht trivial (dh. $l(M) > 1$), so erhält man aus

$$\mathfrak{F}_M \circ \iota(\lambda) = \iota(\lambda^p) \circ \mathfrak{F}_M \quad \text{bzw.} \quad \iota(\lambda) \circ \mathfrak{V}_M = \mathfrak{V}_M \circ \iota(\lambda^p)$$

unmittelbar $\lambda = \lambda^p$ für ein Zentrumselement $\iota(\lambda)$ und damit die Behauptung.

Lemma: Ist k algebraisch abgeschlossen, $M = M_A$ bzw. $= N_B$ ein unzerlegbarer $\hat{D}_k$-Modul vom Typ T bzw. Z, so gibt es ein Element e aus der kanonischen Basis von M derart, dass ke ein unter $\mathcal{E}_M$ invarianter Untermodul von M ist.

Beweis: Wir führen den Beweis für den Fall $M = M_A$ vom Typ T; der Fall $M = N_B$ ergibt sich genau gleich (man verwendet am Schluss die Tatsache, dass B nicht periodisch ist).
Sei $\mathcal{B} = \{e_0, e_1, \ldots, e_{l-1}\}$ die kanonische Basis von M und $e \in \mathcal{B} \cap \mathcal{G}(M)$ ein Basiselement aus dem Sockel von M. Zu e gehört eine Zerlegung $A = A' \cdot A_e$ des Wortes A, welche dem Aufschneiden des Diagrammes von A bei e entspricht.
In $\mathcal{H}(F, V^{-1})$ betrachten wir nun die lexikographische Anordnung: $A = F^{p_1} V^{-q_1} F^{p_2} V^{-q_2} \ldots \geqslant A' = F^{p_1'} V^{-q_1'} F^{p_2'} V^{-q_2'} \ldots$ genau dann, wenn $(p_1, -q_1, p_2, -q_2, \ldots) \geqslant (p_1', -q_1', p_2', -q_2', \ldots)$ gilt in der üblichen lexikographischen Anordnung. Sei nun $e \in \mathcal{B} \cap \mathcal{G}(M)$ wie oben und $\varphi \in \mathcal{E}_M$ ein Endomorphismus von M. Besitzt nun $\varphi(e)$ eine von Null verschiedene Komponente in ke', $e' \in \mathcal{B}$, so gilt $e' \in \mathcal{G}(M)$ und $A_e \leqslant A_{e'}$: Sei hierzu $A_e = F^{p_1} V^{-q_1} \ldots$, $A_{e'} = F^{p_1'} V^{-q_1'} \ldots$ und $e = F^{p_1}(e_1)$; wäre nun $p_1' < p_1$, so hätte $\varphi(e) = F^{p_1}(\varphi(e_1))$ keine Komponente in ke'. Im Falle $p_1' = p_1$ hat aber $\varphi(e_1)$ eine nicht triviale Komponente in ke_1' mit $e_1' \in \mathcal{B}$ gegeben durch $F^{p_1'} e_1' = e'$. Wegen $V^{q_1+1}(e_1) = 0$ folgt daher $V^{q_1+1}\varphi(e_1) = 0$ und folglich $q_1 \geqslant q_1'$ dh. $-q_1 \leqslant -q_1'$. Durch Induktion folgt hieraus

sofort die Beziehung $(p_1,-q_1,\dots) \leq (p_1',-q_1',\dots)$, also $A_e \leq A_{e'}$. Da die A_e für $e \in \mathfrak{B} \cap \mathcal{Y}(M)$ alle verschieden sind, gibt es unter ihnen ein grösstes: A_{e_0}. Nach obigen Überlegungen kann dann $\varphi(e_0)$ für jeden Endomorphismus $\varphi \in \mathcal{E}_M$ nur in ke_0 von Null verschiedene Komponenten haben, dh. ke_0 ist stabil unter allen Endomorphismen von M.

Bemerkung: Im Falle eines beliebigen perfekten Grundkörpers k kann man noch folgendes zeigen:

1) Der Satz gilt nach wie vor für p-Gruppen der Gestalt $\mathcal{G}_{B,\lambda}$ mit zulässigem nicht periodischen B und $\lambda \in k^*$, sowie für alle unzerlegbaren p-Gruppen vom Typ T.

2) Für eine p-Gruppe $\mathcal{G} = \mathcal{G}_{B,\varphi}$ mit zulässigem und nicht periodischem B und $\varphi \in Gl_n(k)$ gelten immer noch die Aussagen (i) und (iii), (i) sogar mit $l = l(B)$. Wie im Beweis des Satzes erhalten wir auch hier eine Einbettung

$$\iota \; : \; End_{R_l}(L_\varphi) \hookrightarrow \mathcal{E}_{\mathcal{G}} \quad , \qquad l = l(B)$$

und die Komposition $pr \circ \iota : End_{R_l}(L_\varphi) \to \mathcal{E}_{\mathcal{G}}/\mathfrak{M}$ ist surjektiv. Dabei ist $End_{R_l}(L_\varphi)$ eine endlichdimensionale lokale Algebra über $\mathbb{F}_{p^l}$ und lässt sich in $M_n(\mathbb{F}_{p^l})$ einbetten.

§11. Gruppen vom Typ Z_1

Die p-Gruppen der Gestalt $\mathcal{G}_{r,1} = \mathcal{G}_{V^rF^{-1}}$ und $\mathcal{G}_{1,s} = \mathcal{G}_{VF^{-s}}$ spielen beim Studium der p-Kerne p-divisibler Gruppen und Abelscher Varietäten eine ausgezeichnete Rolle. Diese beruht auf einer interessanten Eigenschaft dieser Gruppen bezüglich Untergruppen, welche im folgenden Satz zum Ausdruck kommt: Zunächst führen wir folgende Bezeichnung ein:

Definition: Eine p-Gruppe $\mathcal{G}$ heisst vom Typ Z_1, wenn $\mathcal{G}$ isomorph ist zu einer direkten Summe von Gruppen der Gestalt $\mathcal{G}_{r,1}$ und $\mathcal{G}_{1,s}$.

Analog werden die Moduln vom Typ Z_1 definiert.

Satz: Ist $\mathcal{G}$ eine Gruppe vom Typ Z_1, $\mathcal{H} \subset \mathcal{G}$ eine Untergruppe vom Typ Z, so ist $\mathcal{H}$ ein direkter Summand von $\mathcal{G}$ und insbesondere auch vom Typ Z_1.

Beweis: a) Sei zunächst k algebraisch abgeschlossen. Sind dann $\mathcal{G} = \bigoplus_\mu \mathcal{G}_\mu$ und $\mathcal{H} = \bigoplus_\nu \mathcal{H}_\nu$ direkte Zerlegungen in unzerlegbare Faktoren, so gibt es zu jedem ν ein μ derart, dass die Komposition $\varphi_\mu^\nu : \mathcal{H}_\nu \xrightarrow{in_\nu} \mathcal{H} \hookrightarrow \mathcal{G} \xrightarrow{pr_\mu} \mathcal{G}_\mu$ nicht den ganzen Sockel $\mathcal{S}(\mathcal{H}_\nu)$ im Kern enthält. Nach dem folgenden Lemma ist dann φ_μ^ν ein Isomorphismus, woraus die Behauptung folgt.

b) Ist nun k beliebig perfekt, so machen wir Induktion über $n = \sigma(\mathcal{G}) - \sigma(\mathcal{H})$. Ist $n = 0$, so folgt mit a) durch Übergang zum algebraischen Abschluss $\bar{k}$ von k unmittelbar $\mathcal{H} = \mathcal{G}$ und somit die Behauptung. Ist $n > 0$, so gibt es einen direkten Summanden $\mathcal{G}'$ von $\mathcal{G}$ der Gestalt $\mathcal{G}_{r,1}$ oder $\mathcal{G}_{1,s}$ mit der Eigenschaft, dass die Komposition $\varphi : \mathcal{H} \hookrightarrow \mathcal{G} \xrightarrow{pr} \mathcal{G}/\mathcal{G}'$ injektiv ist. Da $\mathcal{G}/\mathcal{G}'$ wieder vom Typ Z_1 ist mit $\sigma(\mathcal{G}/\mathcal{G}') = \sigma(\mathcal{G}) - 1$, folgt die Behauptung durch Induktion.

<u>Lemma</u>: <u>Sei</u> k <u>algebraisch abgeschlossen und</u> N <u>ein</u> $\hat{D}_k$<u>-Modul vom Typ Z. Ist dann</u> $\varrho : N_{1,s} \longrightarrow N$ <u>ein Homomorphismus, welcher auf dem Deckel einen nicht trivialen Homomorphismus</u> $\mathfrak{D}(\varrho) : \mathfrak{D}(N_{1,s}) \longrightarrow \mathfrak{D}(N)$ <u>induziert, so ist</u> ϱ <u>ein Isomorphismus auf einen direkten Summanden von</u> N. <u>Die gleiche Aussage gilt auch für</u> $N_{r,1}$ <u>an Stelle von</u> $N_{1,s}$.

<u>Beweis</u>: Sei zunächst $N = N_B$ unzerlegbar, und sei $\{e_{\nu_1}, e_{\nu_2}, \ldots, e_{\nu_t}\}$ bzw. $\{e\}$ das minimale Erzeugendensystem von N bzw. $N_{1,s}$ (als $\hat{D}_k$-Modul), welches in der kanonischen Basis von N enthalten ist. Im Diagramm der Moduln entsprechen diese Elemente den gemeinsamen Anfangspunkten $(\xleftarrow{F} \cdot \xrightarrow{V})$ von F- und V-Pfeilen. Nach Voraussetzung besitzt $\varrho(e)$ eine nicht-triviale Komponente in einem der direkten Summanden $k \cdot e_i$, und es gilt daher $F^s(\varrho(e)) = \varrho(F^s e) = \varrho(Ve) = V(\varrho(e)) \neq 0$; insbesondere ist $V(\varrho(e))$ im Sockel von N_B enthalten. Es folgt hieraus unmittelbar, dass alle zusammenhängenden V-Pfeil-Folgen im Diagramm die Länge 1 und alle zusammenhängenden F-Pfeil-Folgen die Länge s haben müssen, d.h. $B = (VF^{-s})^d$ mit einem $d > 0$, welches wegen der Unzerlegbarkeit von N_B gleich 1 sein muss. Folglich ist ϱ ein Isomorphismus.

Ist nun $N = \bigoplus_i N_i$ eine Zerlegung in unzerlegbare Faktoren vom Typ Z, welche nach dem Struktursatz alle von der Gestalt N_B sind (§5, Zusatz b)), so ist für eine der Kompositionen

$$pr_i \circ \varrho \; : \; N_{1,s} \longrightarrow N \xrightarrow{pr_i} N_i$$

die induzierte Abbildung auf dem Deckel $\mathcal{D}(pr_i \circ \varrho) : \mathcal{D}(N_{1,s}) \longrightarrow \mathcal{D}(N_i)$ nicht trivial ist. Nach dem vorangehenden ist dann $pr_i \circ \varrho$ ein Isomorphismus, womit das Lemma bewiesen ist.

<u>Bemerkung</u>: Sowohl vom Satz als auch vom Lemma gelten auch die <u>dualen Aussagen</u>, wie man mit Hilfe der Cartier-Dualität sofort einsieht. Wir erhalten damit folgendes Resultat:
<u>Ist</u> $\pi : \mathcal{G} \longrightarrow \mathcal{H}$ <u>ein Epimorphismus von Gruppen vom Typ Z und</u> <u>ist</u> $\mathcal{G}$ <u>vom Typ</u> Z_1, <u>so besitzt</u> π <u>einen Schnitt und</u> $\mathcal{H}$ <u>ist</u> <u>auch vom Typ</u> Z_1.

Kapitel II : Anwendungen auf p-divisible Gruppen und Abelsche Varietäten.

Ist $\underrightarrow{\mathfrak{G}}$ eine p-divisible (formale) Gruppe, so ist der p-Kern $_p\underrightarrow{\mathfrak{G}} = \operatorname{Ker} p\cdot \mathrm{Id}_{\underrightarrow{\mathfrak{G}}}$ eine p-Gruppe im Sinne von Kapitel I. Es zeigt sich nun, dass diese p-Gruppen vom Typ Z sind und dass alle Gruppen vom Typ Z als p-Kerne p-divisibler Gruppen auftreten. Hierzu konstruieren wir unter Benützung der Dieudonné-Theorie einige spezielle p-divisible Gruppen und zwar in ähnlicher Weise, wie wir das in Kapitel I für die Gruppen vom Typ Z getan haben.

Anschliessend untersuchen wir das Verhalten der p-Kerne in einer Isogenieklasse einer p-divisiblen Gruppe. Durchläuft $\underrightarrow{\mathfrak{G}}$ eine solche Isogenie-klasse, so nimmt die Länge des Sockels von $\underrightarrow{\mathfrak{G}}$ alle Werte zwischen 1 inklusive und einem Maximum m an, welches sich leicht aus den Isogenieinvarianten von $\underrightarrow{\mathfrak{G}}$ berechnen lässt. Dieses Resultat geht zurück auf eine Vermutung von F. Oort, welche zum Teil von M. Poletti bewiesen wurde; einer mündlichen Mitteilung von F. Oort verdanken wir den Beweis für die Tatsache, dass das Minimum angenommen wird. Es folgt hieraus auch, dass ein gewisser Typ von Gruppen vom Typ Z (die Gruppen $\mathfrak{G}_{r,r}$, $r>0$) in jeder Isogenieklasse vorkommt. Auf der andern Seite gibt es zu den Gruppen vom Typ Z_1 (aus §11) bis auf Isomorphie nur eine p-divisible Gruppe mit diesem p-Kern.

Betrachten wir nun eine Abelsche Varietät A, so ergeben sich aus der Existenz einer Isogenie zwischen A und ihrer dualen Varietät $\hat{A}$ gewisse Symmetrieeigenschaften für die Struktur des p-Kernes $_pA = \operatorname{Ker} p\cdot\mathrm{Id}_A$; wir zeigen jedoch an Beispielen, dass diese Bedingungen nicht hinreichend sind. Es ist also nach wie vor ein offenes Problem, welche Gruppen vom Typ Z p-Kerne von Abelschen Varietäten sind. Wir geben zum Schluss eine vollständige Liste dieser p-Kerne für Abelsche Varietäten der Dimension $\leqslant 4$, sowie deren Zugehörigkeit zu den Isogenieklassen.

§12. Dieudonné-Theorie p-divisibler Gruppen

Wie bisher bezeichnen wir mit k einen perfekten Körper der Charakteristik $p > 0$. Für die Definitionen und die folgenden Eigenschaften der p-divisiblen k-Gruppen (auch Barsotti-Tate-Gruppen genannt) verweisen wir auf [PG].

Eine p-divisible k-Gruppe ist eine kommutative formale p-Torsionsgruppe definiert über k, bei der das Multiplizieren mit p ein Epimorphismus ist und deren p^n-Kerne endliche k-Gruppen sind. Für die p-divisiblen Gruppen verwenden wir im folgenden immer Symbole der Art $\underset{\rightarrow}{\mathfrak{G}}$, $\underset{\rightarrow}{\mathfrak{H}}$, ..., wobei der daruntergesetzte Pfeil daran erinnern soll, dass $\underset{\rightarrow}{\mathfrak{G}}$ der induktive Limes der p^n-Kerne ist : $\underset{\rightarrow}{\mathfrak{G}} = \varinjlim_n {}_{p^n}\underset{\rightarrow}{\mathfrak{G}}$ mit ${}_{p^n}\underset{\rightarrow}{\mathfrak{G}} = \operatorname{Ker} p^n \cdot \mathrm{Id}_{\underset{\rightarrow}{\mathfrak{G}}}$.

Die Länge von ${}_p\underset{\rightarrow}{\mathfrak{G}}$ heisst auch die Höhe von $\underset{\rightarrow}{\mathfrak{G}}$:

$$h(\underset{\rightarrow}{\mathfrak{G}}) = l({}_p\underset{\rightarrow}{\mathfrak{G}}),$$

und die Dimension von $\mathfrak{G}$ ist gegeben durch

$$\dim \underset{\rightarrow}{\mathfrak{G}} = l({}_{\mathfrak{F}}\underset{\rightarrow}{\mathfrak{G}})$$

mit ${}_{\mathfrak{F}}\underset{\rightarrow}{\mathfrak{G}} = \operatorname{Ker} \mathfrak{F}_{\underset{\rightarrow}{\mathfrak{G}}}$ = Frobeniuskern. Es gilt:

$$h(\underset{\rightarrow}{\mathfrak{G}}) = \dim \underset{\rightarrow}{\mathfrak{G}} + \dim {}^t\underset{\rightarrow}{\mathfrak{G}}$$

wobei ${}^t\underset{\rightarrow}{\mathfrak{G}}$ die Serre-duale p-divisible Gruppe zu $\mathfrak{G}$ ist, welche man folgendermassen erhält: Das Multiplizieren mit p induziert eine unendliche Folge von Epimorphismen

$$\cdots \longrightarrow {}_{p^n}\underset{\rightarrow}{\mathfrak{G}} \longrightarrow {}_{p^{n-1}}\underset{\rightarrow}{\mathfrak{G}} \longrightarrow \cdots\cdots \longrightarrow {}_{p^2}\underset{\rightarrow}{\mathfrak{G}} \longrightarrow {}_p\underset{\rightarrow}{\mathfrak{G}}$$

und damit durch Dualisieren eine unendliche Folge von Monomorphismen

$${}^t_p\underset{\rightarrow}{\mathfrak{G}} \longrightarrow {}^t_{p^2}\underset{\rightarrow}{\mathfrak{G}} \longrightarrow \cdots \longrightarrow {}^t_{p^{n-1}}\underset{\rightarrow}{\mathfrak{G}} \longrightarrow {}^t_{p^n}\underset{\rightarrow}{\mathfrak{G}} \longrightarrow \cdots\cdots$$

und es gilt dann ${}^t\underset{\rightarrow}{\mathfrak{G}} = \varinjlim_n {}^t_{p^n}\underset{\rightarrow}{\mathfrak{G}}$ und ${}_{p^n}({}^t\underset{\rightarrow}{\mathfrak{G}}) = {}^t_{p^n}\underset{\rightarrow}{\mathfrak{G}}$.

Mit Hilfe der Dieudonné-Theorie für endliche Gruppen (vgl. §1) konstruiert man zu jeder p-divisiblen Gruppe $\underrightarrow{\mathfrak{G}}$ einen D_k-Modul $M(\underrightarrow{\mathfrak{G}})$, und der Funktor $\underrightarrow{\mathfrak{G}} \longmapsto M(\underrightarrow{\mathfrak{G}})$ liefert eine Antiäquivalenz zwischen den p-divisiblen Gruppen und den torsionsfreien, über $\mathcal{W}(k)$ endlich erzeugten D_k-Moduln; dabei entspricht der endlichen Untergruppe ${}_{p^n}\underrightarrow{\mathfrak{G}}$ der D_k-Modul $M(\underrightarrow{\mathfrak{G}})/p^n M(\underrightarrow{\mathfrak{G}})$. $M(\underrightarrow{\mathfrak{G}})$ ist also ein freier $\mathcal{W}(k)$-Modul vom Rang $n = h(\underrightarrow{\mathfrak{G}}) = l({}_p\underrightarrow{\mathfrak{G}})$, und es gilt nach Definition $\dim \underrightarrow{\mathfrak{G}} = l(M(\underrightarrow{\mathfrak{G}})/FM(\underrightarrow{\mathfrak{G}}))$.

Analog zu den p-Gruppen besitzt auch jede p-divisible Gruppe eine Zerlegung der Gestalt

$$\underrightarrow{\mathfrak{G}} = \underrightarrow{\mathcal{E}} \oplus \underrightarrow{\mathcal{M}} \oplus \underrightarrow{\mathcal{U}}$$

wobei $\underrightarrow{\mathcal{E}}$ etal, $\underrightarrow{\mathcal{M}}$ multiplikativ und $\underrightarrow{\mathcal{U}}$ zusammenhängend und unipotent ist; dabei heisst $\underrightarrow{\mathfrak{G}}$ etal bzw. multiplikativ bzw. zusammenhängend bzw. unipotent, falls dies für ${}_p\underrightarrow{\mathfrak{G}}$ (und damit für alle ${}_{p^n}\underrightarrow{\mathfrak{G}}$) gilt. Eine p-divisible Gruppe $\underrightarrow{\mathfrak{G}}$ ist genau dann etal bzw. multiplikativ, wenn im Dieudonné-Modul $M(\underrightarrow{\mathfrak{G}})$ das Multiplizieren mit F bzw. V bijektiv ist. Die duale Gruppe einer etalen p-divisiblen Gruppe ist multiplikativ und umgekehrt. Dies erkennt man zum Beispiel aus der Beschreibung der Serre-Dualität auf der Seite der Dieudonné-Moduln : Der duale Modul zu M ist gegeben durch

$$^tM = \mathrm{Hom}_{\mathcal{W}(k)}(M, \mathcal{W}(k))$$

mit

$$(F_{^tM}\varphi)(m) = \varphi(V_M m)^{(p)}$$

$$(V_{^tM}\varphi)(m) = \varphi(F_M m)^{(p^{-1})} \quad , \quad \varphi \in {}^tM \ , \quad m \in M \ .$$

(vgl. Cartier-Dualität für p-Gruppen §8.)

Für algebraisch abgeschlossenen Grundkörper $k = \bar{k}$ ist jede etale p-divisible Gruppe isomorph zu einem Produkt $(\mathbb{Q}_p/\mathbb{Z}_p)_k^r$ und jede multiplikative p-divisible Gruppe isomorph zu einem Produkt $\mu_k(p)^s$; dabei ist $(\mathbb{Q}_p/\mathbb{Z}_p)_k = \varinjlim_n (p^{-n}\mathbb{Z}/\mathbb{Z})_k$ mit Dieudonné-Modul $M = \mathcal{W}(k)$, $F_M = \varphi$, $V_M = p\,\varphi^{-1}$, und $\mu_k(p) = \varinjlim_n {}_{p^n}\mu_k$ mit Dieudonné-Modul

$M = \mathcal{W}(k)$, $F_M = p\cdot\varphi$, $V_M = \varphi^{-1}$, wobei wie früher $\varphi: \mathcal{W}(k) \longrightarrow \mathcal{W}(k)$ die Bijektion $(\lambda_0, \lambda_1, \lambda_2, \ldots) \mapsto (\lambda_0, \lambda_1, \lambda_2, \ldots)^{(p)} = (\lambda_0^p, \lambda_1^p, \lambda_2^p, \ldots)$ ist. Aus der obigen Beschreibung der Serre-Dualität sieht man auch, dass diese beiden Gruppen zueinander dual sind.

Ähnlich wie in §1 können wir einen D_k-Modul M auch auffassen als einen $\mathcal{W}(k)$-Modul M zusammen mit zwei Endomorphismen

$$F_M : M \longrightarrow M \quad \text{und} \quad V_M : M \longrightarrow M$$

mit den Relationen

$$\begin{aligned} F_M V_M &= V_M F_M = p\cdot \mathrm{Id}_M \\ F_M(\lambda m) &= \lambda^{(p)} F_M(m) \qquad\qquad (*) \\ V_M(\lambda m) &= \lambda^{(p^{-1})} V_M(m) , \quad \lambda \in \mathcal{W}(k). \end{aligned}$$

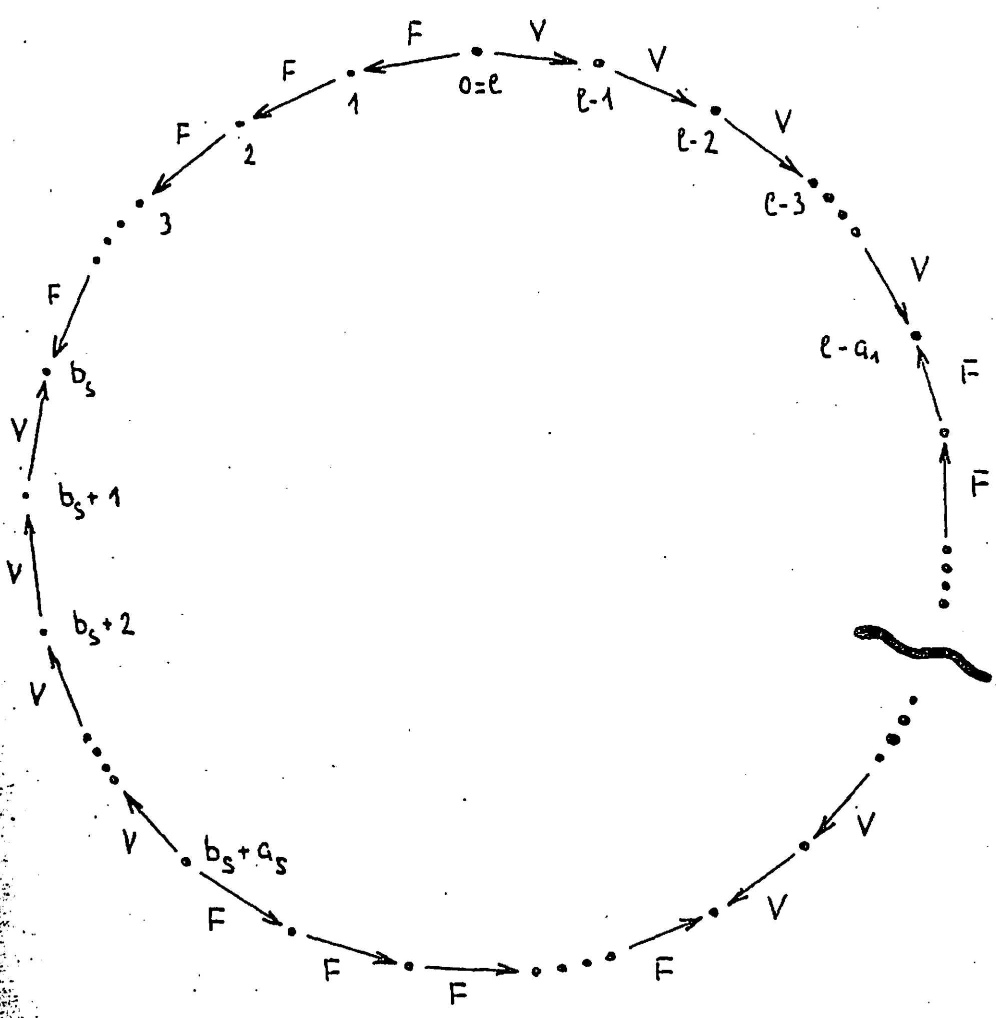
Insbesondere ist für einen torsionsfreien, über $\mathcal{W}(k)$ endlich erzeugten D_k-Modul M der Endomorphimus F_M durch V_M eindeutig festgelegt und umgekehrt.

Ist n eine natürliche Zahl ≥ 1 und sind $\varphi, \psi \in M_n(\mathcal{W}(k))$ zwei $n\times n$-Matrizen mit Koeffizienten in $\mathcal{W}(k)$ mit $\varphi\psi = \psi\varphi = p\cdot 1_n$, so erhalten wir einen D_k-Modul $M = M_{\varphi,\psi}$, indem wir auf dem freien $\mathcal{W}(k)$-Modul $M = \mathcal{W}(k)^n$ die Endomorphismen F_M und V_M durch ihre Wirkung auf der kanonischen Basis von M gemäss den Matrizen φ und ψ festlegen (unter Benützung von (*)). Offensichtlich ist jeder torsionsfreie und über $\mathcal{W}(k)$ endlich erzeugte D_k-Modul isomorph zu einem Modul dieser Gestalt.

§13. Einige spezielle p-divisible Gruppen

Es geht im folgenden darum, einige spezielle torsionsfreie D_k-Moduln zu konstruieren, und damit auch einige p-divisible Gruppen, und zwar in ähnlicher Weise, wie wir in §3 die Moduln und Gruppen vom Typ Z definiert haben.

Sei hierzu $B \in \mathcal{H}(V,F^{-1})$ ein <u>zulässiges Wort</u>, d.h. $B = V^{a_1}F^{-b_1}V^{a_2}F^{-b_2}\dots V^{a_s}F^{-b_s}$, $B \neq 1, V^a, F^b$, von der <u>Wortlänge</u> $l = l(B) = \sum_{i=1}^{s} a_i + \sum_{i=1}^{s} b_i$, <u>beschrieben durch das Diagramm</u>



Sei weiter n eine natürliche Zahl ≥ 1 und $\varphi_i \in Gl_n(\mathcal{W}(k))$ invertierbare Matrizen für $i = 1,2,..,l$. Dann definieren wir den D_k-Modul $\widetilde{N} = \widetilde{N}_{B,(\varphi_1,\varphi_2,..,\varphi_l)}$ in folgender Weise:
Für jeden Punkt des Diagramms nehmen wir ein Exemplar W_i des freien $\mathcal{W}(k)$-Moduls $\mathcal{W}(k)^n$ und setzen $\widetilde{N} = \bigoplus_{i=1}^{l} W_i$ für den unterliegenden $\mathcal{W}(k)$-Modul; die Endomorphismen $F = F_{\widetilde{N}}$ und $V = V_{\widetilde{N}}$ definieren wir durch ihre Einschränkungen

$$F_i = F\big|_{W_{i-1}} : W_{i-1} \longrightarrow W_i \quad , \quad V_i = V\big|_{W_i} : W_i \longrightarrow W_{i-1}$$

$(i=1,2,..,l,\ W_0 = W_l)$, wobei F_i (bzw. V_i) auf der kanonischen Basis von W_{i-1} (bzw. W_i) wirkt wie φ_i (bzw. $p\cdot\varphi_i^{-1}$), falls der i-te Pfeil ein F-Pfeil ist, und wie $p\cdot\varphi_i^{-1}$ (bzw. φ_i), falls der i-te Pfeil ein V-Pfeil ist.

Aus der Konstruktion folgt unmittelbar $F_{\widetilde{N}} V_{\widetilde{N}} = V_{\widetilde{N}} F_{\widetilde{N}} = p\cdot Id_{\widetilde{N}}$, und zudem gilt in kanonischer Weise

$$\widetilde{N}_{B,(\varphi_1,\varphi_2,...,\varphi_l)} \Big/ p\cdot\widetilde{N}_{B,(\varphi_1,\varphi_2,...,\varphi_l)} \cong N_{B,(\overline{\varphi_1},\overline{\varphi_2},...,\overline{\varphi_l})}$$

wobei $N_{B,(\overline{\varphi_1},\overline{\varphi_2},..,\overline{\varphi_l})}$ der in §3 eingeführte Modul vom Typ Z ist mit $\overline{\varphi_i}$ = Restklasse von φ_i in $Gl_n(k)$ bezüglich der kanonischen Projektion $\mathcal{W}(k) \longrightarrow k$, $\lambda = (\lambda_0,\lambda_1,...) \longmapsto \lambda_0$.

Wir wählen wiederum eine p-divisible Gruppe mit Dieudonné-Modul isomorph zu $\widetilde{N}_{B,(\varphi_1,...)}$ und bezeichnen diese mit $\underset{\to}{G}_{B,(\varphi_1,...)}$. Wie früher führen wir auch wieder die abkürzenden Bezeichnungen ein:

$$\widetilde{N}_{B,\varphi} = \widetilde{N}_{B,(\varphi,1_n,..,1_n)} \qquad \widetilde{N}_B = \widetilde{N}_{B,1},\ 1 \in Gl_1(k),$$

und

$$\widetilde{N}_{r,s} = \widetilde{N}_{V^rF^{-s}},$$

und analog für die Gruppen.

Es gilt dann nach Konstruktion:

$$h(\underset{\rightarrow}{\mathcal{G}}_{B,(\varphi_1,\dots,\varphi_l)}) = h(\underset{\rightarrow}{\mathcal{G}}_{B,\varphi}) = n\cdot l(B) \;, \quad h(\underset{\rightarrow}{\mathcal{G}}_B) = l(B),$$

$$\dim \underset{\rightarrow}{\mathcal{G}}_{B,(\varphi_1,\dots,\varphi_l)} = \dim \underset{\rightarrow}{\mathcal{G}}_{B,\varphi} = n\cdot l_V(B) \;,$$

$$\dim \underset{\rightarrow}{\mathcal{G}}_B = l_V(B);$$

Zudem ist leicht zu sehen, dass die Serre-duale Gruppe zu $\underset{\rightarrow}{\mathcal{G}}_{B,(\varphi_1,\dots)}$ wieder diese Gestalt hat, nämlich $\underset{\rightarrow}{\mathcal{G}}_{{}^tB,({}^t\varphi_1,\dots)}$ (vgl. §8).

Im Falle $B = V^rF^{-s}$ erhalten wir speziell:

$$h(\underset{\rightarrow}{\mathcal{G}}_{r,s}) = r+s \;, \quad \dim \underset{\rightarrow}{\mathcal{G}}_{r,s} = r \;, \quad {}^t\underset{\rightarrow}{\mathcal{G}}_{r,s} = \underset{\rightarrow}{\mathcal{G}}_{s,r} \,.$$

Setzen wir noch $\underset{\rightarrow}{\mathcal{G}}_{1,o} = \mu(p)_k$ und $\underset{\rightarrow}{\mathcal{G}}_{o,1} = (\mathbb{Q}_p/\mathbb{Z}_p)_k$, so gelten diese Beziehungen auch noch im Falle $(r,s) = (1,o),(o,1)$.

Lemma: Ist $k = \overline{k}$ algebraisch abgeschlossen, so ist $\underset{\rightarrow}{\mathcal{G}}_{B,(\varphi_1,\dots,\varphi_l)}$ isomorph zu $\underset{\rightarrow}{\mathcal{G}}_B^n$.

Beweis: Wir beweisen die entsprechende Aussage für Moduln und können ohne Einschränkung $\tilde{N} = \tilde{N}_{B,\varphi_l}$ annehmen.

Nach Konstruktion haben wir $\tilde{N} = \bigoplus_{i=1}^{l} W_i$, W_i Exemplar von $\mathcal{W}(k)^n$, und ein Basiswechsel in W_2 mit einer Matrix $\rho \in Gl_n(\mathcal{W}(k))$ transformiert φ in $\rho^{-1}\circ\varphi\circ\rho^{(p^l)}$, $l = l(B)$. Gesucht ist also eine Matrix ρ mit $\varphi\circ\rho^{(p^l)} = \rho$.

Hierzu betrachten wir das affine k-Ringschema $M_n(\mathcal{W}_k)$ und den Morphismus

$$\phi = \varphi\circ\mathcal{F}^l - \mathrm{Id} : M_n(\mathcal{W}_k) \longrightarrow M_n(\mathcal{W}_k)$$

($\mathcal{F}: \mathcal{W}_k \longrightarrow \mathcal{W}_k$ Frobeniusmorphismus des k-Ringschemas $\mathcal{W}_k$ der Wittschen Vektoren, [GA] V,§1,n°1).

Mit Hilfe der kanonischen Projektion $pr : \omega_k \longrightarrow \alpha_k$ erhalten wir das kommutative Diagramm

$$\begin{tikzcd} M_n(\omega_k) \arrow[r, "\Phi"] \arrow[d] & M_n(\omega_k) \arrow[d] \\ M_n(\alpha_k) \arrow[r, "\bar{\Phi}"] & M_n(\alpha_k) \end{tikzcd}$$

mit $\bar{\Phi} = \bar{\varphi}\cdot\tilde{\mathfrak{F}}^{\ell} - \mathrm{Id} : M_n(\alpha_k) \longrightarrow M_n(\alpha_k)$, $\bar{\varphi}$ = Restklasse von φ in $M_n(k)$ unter $\omega(k) \longrightarrow k$. Nach den Ergebnissen von Kap. I (insbesondere §5) gilt das obige Lemma in der Formulierung für Gruppen vom Typ Z anstelle der p-divisiblen Gruppen, woraus wir die Existenz einer Matrix $\sigma \in Gl_n(k) \subset M_n(k)$ mit $\bar{\Phi}(\sigma) = 0$ folgern. Insbesondere ist $\bar{\Phi}$ isomorph zur Abbildung $\tilde{\mathfrak{F}}^{\ell} - \mathrm{Id}$ und folglich ein Epimorphismus mit endlichem Kern, welcher nicht zusammenhängend ist. Dann ist aber auch Φ ein Epimorphismus: $\mathrm{Im}\,\Phi$ ist ein ω_k-Untermodul von $M_n(\omega_k)$, welcher unter $pr : M_n(\omega_k) \longrightarrow M_n(\alpha_k)$ epimorph auf $M_n(\alpha_k)$ abgebildet wird, was nur für $\mathrm{Im}\,\Phi = M_n(\omega_k)$ möglich ist (betrachte die rationalen Punkte!). Da Φ damit auch den Kern von pr epimorph auf sich abbildet, induziert pr einen Epimorphismus $\mathrm{Ker}\,\Phi \longrightarrow \mathrm{Ker}\,\bar{\Phi}$. Wir finden daher ein Urbild $\rho \in (\mathrm{Ker}\,\Phi)(k)$ von $\sigma \in (\mathrm{Ker}\,\bar{\Phi})(k)$. Wegen $\overline{\det \rho} = \det \sigma \neq 0$ ist $\det \rho$ eine Einheit in $\omega(k)$ und folglich $\rho \in Gl_n(\omega(k))$, was zu zeigen war.

§14. Isogenieklassen

Ein Homomorphismus $\varphi : \underrightarrow{\mathcal{G}} \longrightarrow \underrightarrow{\mathcal{H}}$ zwischen zwei p-divisiblen Gruppen heisst eine Isogenie, wenn Ker φ und Coker φ endliche Gruppen sind; ein solcher Homomorphismus ist immer ein Epimorphismus, und wir nennen $\underrightarrow{\mathcal{G}}$ und $\underrightarrow{\mathcal{H}}$ isogen, wenn es eine Isogenie zwischen $\underrightarrow{\mathcal{G}}$ und $\underrightarrow{\mathcal{H}}$ gibt. Man sieht leicht, dass dies eine Äquivalenzrelation ist.

Auf der Seite der Moduln bedeutet das folgendes: $\underrightarrow{\mathcal{G}}$ und $\underrightarrow{\mathcal{H}}$ sind genau dann isogen, wenn sich $M(\underrightarrow{\mathcal{G}})$ in $M(\underrightarrow{\mathcal{H}})$ einbetten lässt mit einem Cokern endlicher Länge. Wir sprechen in diesem Falle von isogenen D_k-Moduln. Man folgert hieraus, dass die Isogenieklassen den Moduln über dem Quotientenring $D_k[p^{-1}]$ von D_k entsprechen und erhält daraus die folgende Klassifikation (Dieudonné-Manin):

Struktursatz: Ist $k = \overline{k}$ algebraisch abgeschlossen, so ist jede p-divisible Gruppe $\underrightarrow{\mathcal{G}}$ isogen zu einer Gruppe der Gestalt

$$\bigoplus_i \underrightarrow{\mathcal{G}}_{r_i,s_i} \qquad \text{mit} \quad (r_i,s_i) = 1 .$$

Dabei sind die teilerfremden Paare (r_i,s_i) durch $\underrightarrow{\mathcal{G}}$ eindeutig bestimmt.

Für den Beweis vergleiche man [PG]. Wir sprechen im folgenden oft von den Isogenieinvarianten (r_i,s_i) der Gruppe $\underrightarrow{\mathcal{G}}$.

Die p-divisible Gruppe $\underrightarrow{\mathcal{G}}$ heisst einfach, wenn jede echte Untergruppe von $\underrightarrow{\mathcal{G}}$ endlich ist. Für $k = \overline{k}$ ist dies äquivalent zur Aussage, dass $\underrightarrow{\mathcal{G}}$ isogen zu einem $\underrightarrow{\mathcal{G}}_{r,s}$ mit $(r,s) = 1$ ist; insbesondere gibt es zwischen zwei verschiedenen $\underrightarrow{\mathcal{G}}_{r,s}$ mit $(r,s) = 1$ keine nicht trivialen Homomorphismen.

Bemerkung: Die Höhe $h(\underset{\rightarrow}{G})$ und die Dimension $\dim \underset{\rightarrow}{G}$ sind Isogenieinvarianten und lassen sich aus den Isogenieinvarianten (r_i, s_i) folgendermassen bestimmen:

$$h(\underset{\rightarrow}{G}) = \sum_i r_i + \sum_i s_i \quad , \quad \dim \underset{\rightarrow}{G} = \sum_i r_i$$

Für den Beweis verwende man die Tatsache, dass $p \cdot Id_{\underset{\rightarrow}{G}}$ und $\mathcal{F}_{\underset{\rightarrow}{G}}$ Epimorphismen sind.
Wenn der Grundkörper nicht algebraisch abgeschlossen ist, reden wir dennoch von den Isogenieinvarianten (r_i, s_i) von $\underset{\rightarrow}{G}$ und meinen damit die Isogenieinvarianten von $\underset{\rightarrow}{G} \otimes_k \bar{k}$.

Es stellt sich nun die Frage, wie diese Isogenieinvarianten für die in §13 eingeführten Gruppen $\underset{\rightarrow}{G}_{B,(\varphi_1, \varphi_2, \ldots, \varphi_l)}$ aussehen. Wegen des Lemmas von §13 genügt es hierzu, die Gruppen der Gestalt $\underset{\rightarrow}{G}_B$ zu untersuchen.

Satz: Zwei p-divisible Gruppen $\underset{\rightarrow}{G}_B$ und $\underset{\rightarrow}{G}_{B'}$ sind genau dann isogen, wenn $l_F(B) = l_F(B')$ und $l_V(B) = l_V(B')$ gilt. Insbesondere ist $\underset{\rightarrow}{G}_B$ isogen zur Gruppe $\underset{\rightarrow}{G}_{r,s}$ mit $r = l_V(B)$ und $s = l_F(B)$ und hat folglich die Isogenieinvarianten $d \times (\frac{r}{d}, \frac{s}{d})$ mit $d = (r,s)$.

Beweis: Wir beweisen die entsprechende Behauptung für die zugehörigen D_k-Moduln und zeigen zunächst folgendes:
Ist $B = V^{a_1}F^{-b_1}V^{a_2}\ldots F^{-b_s}$ mit $a_1, b_s \neq 0$ und ist

$B' = F^{-1}V^{a_1-1}F^{-b_1}\ldots V^{a_s}F^{1-b_s}V$, so ist $\tilde{N}_{B'}$ isogen zu $\tilde{N}_B$.
Dies sieht man folgendermassen: Ist $\tilde{N}_B = \bigoplus_i W_i$ gemäss Konstruktion (W_i Exemplar von $\mathcal{W}(k)$), so ist der $\mathcal{W}(k)$-Untermodul $\tilde{N}' = pW_1 \oplus W_2 \oplus \ldots \oplus W_l$ ein D_k-Untermodul, welcher in kanonischer Weise isomorph zu $\tilde{N}_{B'}$ ist : es gilt nämlich nach Definition $V(W_2) = pW_1$ und $F(W_l) = pW_1$, $l = l(B)$.
Es ist nun leicht zu sehen, dass man jedes Wort B' mit

$l_F(B') = l_F(B)$ und $l_V(B') = l_V(B)$ aus B durch sukzessive Anwendung dieser Operation sowie zyklischer Vertauschungen erhält, womit die eine Richtung der Behauptung des Satzes bewiesen ist. Die andere Richtung folgert man unmittelbar aus der obigen Bemerkung.

Bemerkung: Ist das Wort B periodisch, d.h. $B = C^d$ mit zulässigem C und gilt zudem $\mathbb{F}_{p^l} \subset k$ mit $l = l(B)$, so gibt es einen Isomorphismus $\underset{\rightarrow}{G}_B \xrightarrow{\sim} \underset{\rightarrow}{G}_C^d$. Dass die beiden Gruppen isogen sind, folgt schon aus dem vorangehenden Satz, und zudem findet man mit dem Lemma von §13 auch sofort einen Isomorphismus über $\bar{k}$. Mit ähnlichen Methoden wie im Beweis von diesem Lemma kann man die Behauptung auch auf die entsprechende Behauptung bei p-Gruppen vom Typ Z reduzieren. Wir überlassen dem Leser eine genaue Beweisführung.

§15. p-Kerne von p-divisiblen Gruppen

Für jede endliche kommutative k-Gruppe G haben wir die Zerlegung

$$G = \mathcal{E} \oplus \mathcal{M} \oplus \mathcal{U} ,$$

wobei $\mathcal{E} = G_{red}$ isomorph zur k-Gruppe $\pi_0(G)$ der Zusammenhangskomponenten und etal ist, $\mathcal{M}$ bzw. $\mathcal{U}$ der multiplikative bzw. unipotente Bestandteil der Zusammenhangs komponente G^0 der Null von G ist (vgl.§1).

Im Falle einer p-divisiblen Gruppe $\underset{\rightarrow}{G}$ erhalten wir nun für den p-Kern $_p\underset{\rightarrow}{G}$ folgendes Resultat:

Satz: Ist $\underrightarrow{\mathfrak{G}}$ eine p-divisible Gruppe und $\mathfrak{U} \subset {}_p\underrightarrow{\mathfrak{G}}$ der unipotente infinitesimale Bestandteil des p-Kernes ${}_p\underrightarrow{\mathfrak{G}}$ von $\underrightarrow{\mathfrak{G}}$, so ist $\mathfrak{U}$ eine Gruppe vom Typ Z.

Beweis: Wir betrachten die exakte Sequenz

$$0 \longrightarrow {}_{\mathcal{F}}\underrightarrow{\mathfrak{G}} \longrightarrow \underrightarrow{\mathfrak{G}} \xrightarrow{\mathcal{F}} \underrightarrow{\mathfrak{G}}^{(p)} \longrightarrow 0$$

gegeben durch den Frobeniushomomorphismus $\mathcal{F} = \mathcal{F}_{\underrightarrow{\mathfrak{G}}}$ und setzen $\mathcal{H} = \mathcal{F}^{-1}({}_{\mathcal{V}}\underrightarrow{\mathfrak{G}}^{(p)})$ mit ${}_{\mathcal{V}}\underrightarrow{\mathfrak{G}}^{(p)} = \operatorname{Ker} \mathcal{V}_{\underrightarrow{\mathfrak{G}}}$. Die endliche Gruppe $\mathcal{H}$ ist offensichtlich in ${}_p\underrightarrow{\mathfrak{G}} = \operatorname{Ker} p \cdot \mathrm{Id}_{\underrightarrow{\mathfrak{G}}}$ enthalten, und folglich enthält $\mathfrak{U}$ den unipotenten infinitesimalen Bestandteil $\mathcal{H}'$ von $\mathcal{H}$. Da $\mathcal{F}$ ein Epimorphismus ist, erhalten wir daraus die exakte Sequenz

$$0 \longrightarrow {}_{\mathcal{F}}\mathfrak{U} \longrightarrow \mathfrak{U} \longrightarrow {}_{\mathcal{V}}\mathfrak{U}^{(p)} \longrightarrow 0$$

und damit $l(\mathfrak{U}) = l({}_{\mathcal{F}}\mathfrak{U}) + l({}_{\mathcal{V}}\mathfrak{U})$, woraus die Behauptung mit Satz (iii) aus §7 folgt.

Aus §13 erhalten wir noch die folgende Umkehrung der obigen Behauptung:

Zusatz: Jede p-Gruppe vom Typ Z ist isomorph zum p-Kern einer p-divisiblen Gruppe.   bass fehl?

Wir haben bereits gesehen, dass die Höhe, die Dimension, die Länge von Frobeniuskern und Kern der Verschiebung Isogenieinvarianten sind. Es ist leicht an Beispielen zu sehen, dass dies für die Grössen $\sigma(\underrightarrow{\mathfrak{G}}) := \sigma({}_p\underrightarrow{\mathfrak{G}})$ und $\delta(\underrightarrow{\mathfrak{G}}) := \delta({}_p\underrightarrow{\mathfrak{G}})$ nicht gilt, was schon von Barsotti festgestellt wurde (vgl.

x / K

auch Oort [6]). Das Verhalten dieser Grössen in einer Isogenieklasse wird durch folgenden Satz geklärt:

Satz (Poletti-Oort): Ist $k = \bar{k}$ algebrisch abgeschlossen und $\underset{\to}{G}$ eine unipotente zusammenhängende p-divisible Gruppe mit den Isogenieinvarianten (r_i, s_i), so gilt

$$1 \leq \sigma(\underset{\to}{G}) \leq \sum_i \min(r_i, s_i) \leq h(\underset{\to}{G}),$$

und alle Werte zwischen 1 und $\sum_i \min(r_i, s_i)$ inklusive kommen in der Isogenieklasse vor.

Bemerkung: Die Abschätzung $\sigma(\underset{\to}{G}) \leq \sum_i \min(r_i, s_i)$ wurde von F.Oort in [6] vermutet und von M.Poletti in [9] bewiesen, inklusive der Tatsache, dass dieses Maximum angenommen wird. Einer mündlichen Mitteilung von F.Oort verdanken wir den Beweis dafür, dass auch das Minimum 1 angenommen wird.

Beweis: a) Ist $\underset{\to}{G}$ isogen zu $\underset{\to}{G}_{r,s}$, so gilt

$$\begin{aligned}\sigma(\underset{\to}{G}) \leq \min(l(_{\mathfrak{f}}\underset{\to}{G}), l(_{\upsilon}\underset{\to}{G})) &= \min(l(_{\mathfrak{f}}\underset{\to}{G}_{r,s}), l(_{\upsilon}\underset{\to}{G}_{r,s})) \\ &= \min(r,s)\end{aligned}$$

(vgl. §14 und §7).

Sei nun $\varphi : \bigoplus_i \underset{\to}{G}_{r_i,s_i} \longrightarrow \underset{\to}{G}$ eine Isogenie und $\underset{\to}{G}_i \subseteq \underset{\to}{G}$ das Bild von $\underset{\to}{G}_{r_i,s_i}$ unter φ, so erhalten wir $\underset{\to}{G} = \sum_i \underset{\to}{G}_i$ und $\underset{\to}{G}_i$ ist isogen zu $\underset{\to}{G}_{r_i,s_i}$. Es gilt nun $\sigma(\underset{\to}{G}) \leq \sum_i \sigma(\underset{\to}{G}_i)$:

$$\sigma(\underset{\to}{G}) = \sigma(_p\underset{\to}{G}) = \delta(_p\underset{\to}{G}) \leq \sum_i \delta(_p\underset{\to}{G}_i) = \sum_i \sigma(_p\underset{\to}{G}_i) = \sum_i \sigma(\underset{\to}{G}_i),$$

denn $_p\underset{\to}{G}$ ist vom Typ Z (vgl. den vorangehenden Satz sowie §9 Lemma (ii)). Nach obigem folgt daher $\sigma(\underset{\to}{G}) \leq \sum_i \min(r_i, s_i)$. Dieses Maximum wird aber auch angenommen: Ist $r_i \geq s_i$, so setzen wir $B_i = (VF^{-1})^{s_i} F^{-r_i+s_i}$, und für $r_i \leq s_i$ analog

$B_i = (VF^{-1})^{r_i} V^{s_i - r_i}$ und erhalten nach §9 $\sigma(\underset{\to}{G}_{B_i}) = \min(r_i, s_i)$. Zudem ist $\underset{\to}{G}_{B_i} \sim \underset{\to}{G}_{r_i,s_i}$ isogen nach §14, woraus die Behauptung folgt.

b) Jede Isogenieklasse von unipotenten zusammenhängenden p-divisiblen Gruppen enthält eine Gruppe mit $\sigma(\underset{\to}{G}) = 1$. Wir machen Induktion über die Höhe $h(\underset{\to}{G})$ von $\underset{\to}{G}$; der Fall $h(\underset{\to}{G}) = 2$ ist klar. Wir betrachten nun die Isogenieklasse der Gruppe $\underset{\to}{G} = \bigoplus_i \underset{\to}{G}_{r_i,s_i}$ mit $r_i, s_i > 0$, $(r_i, s_i) = 1$, und setzen voraus, dass für alle Isogenieklassen echt kleinerer Höhe die Behauptung schon bewiesen ist. Ist nun $(r_i, s_i) = (r, s)$ für alle i, so ist $\underset{\to}{G}$ isogen zu $\underset{\to}{G}_{nr,ns}$ (vgl. die Bemerkung am Ende von §14), womit die Behauptung bewiesen ist. Andernfalls gibt es eine echte Zerlegung $\underset{\to}{G} = \underset{\to}{G}' \oplus \underset{\to}{G}''$ mit $\mathrm{Hom}(\underset{\to}{G}', \underset{\to}{G}'') = \mathrm{Hom}(\underset{\to}{G}'', \underset{\to}{G}') = 0$. Nach Induktionsvoraussetzung gibt es dann Gruppen $\underset{\to}{H}'$ und $\underset{\to}{H}''$ isogen zu $\underset{\to}{G}'$ und $\underset{\to}{G}''$ mit $\sigma(\underset{\to}{H}') = \sigma(\underset{\to}{H}'') = 1$, und folglich ist $\underset{\to}{H} = \underset{\to}{H}' \oplus \underset{\to}{H}''$ isogen zu $\underset{\to}{G}$ mit $\sigma(\underset{\to}{H}) = 2$. Wir finden daher eine Isogenie $\varphi_1 : \underset{\to}{H} \to \underset{\to}{H}_1$ mit $l(\mathrm{Ker}\,\varphi_1) = 1$ und $\mathrm{Ker}\,\varphi_1 \cap \underset{\to}{H}' = \mathrm{Ker}\,\varphi_1 \cap \underset{\to}{H}'' = 0$. Ist nun wiederum $\sigma(\underset{\to}{H}_1) > 1$, so gibt es eine weitere Isogenie $\varphi_2 : \underset{\to}{H}_1 \to \underset{\to}{H}_2$ mit $l(\mathrm{Ker}\,\varphi_2) = 1$ und $\mathrm{Ker}\,\varphi_2 \circ \varphi_1 \cap \underset{\to}{H}' = \mathrm{Ker}\,\varphi_2 \circ \varphi_1 \cap \underset{\to}{H}'' = 0$. Enthält daher die Isogenieklasse von $\underset{\to}{G}$ keine Gruppe mit einfachem Sockel, so erhalten wir eine unendlich lange Kette von Isogenien

$$\underset{\to}{H} \xrightarrow{\varphi_1} \underset{\to}{H}_1 \xrightarrow{\varphi_2} \underset{\to}{H}_2 \xrightarrow{\varphi_3} \underset{\to}{H}_3 \longrightarrow \cdots \qquad (*)$$

mit $\mathrm{Ker}(\varphi_n \circ \varphi_{n-1} \cdots \varphi_1) \cap \underset{\to}{H}' = \mathrm{Ker}(\varphi_n \circ \varphi_{n-1} \cdots \varphi_1) \cap \underset{\to}{H}'' = 0$ für alle n. Ist dann $\underset{\to}{H}_\infty = \varinjlim_i \underset{\to}{H}_i$ der induktive Limes der $\underset{\to}{H}_i$, $\varphi : \underset{\to}{H} \to \underset{\to}{H}_\infty$ der induzierte Homomorphismus, so ist

$\operatorname{Ker}\varphi \cap \underset{\to}{\mathcal{H}}' = \operatorname{Ker}\varphi \cap \underset{\to}{\mathcal{H}}'' = 0$: gefilterte induktive Limiten existieren in der Kategorie der p-divisiblen Gruppen und sind exakt (betrachte die Dieudonné-Moduln und verwende z.B. [GA] V,§2,n^{o}1 und 2). Zudem ist φ eine Isogenie: Die Projektionen auf die Faktoren induzieren Einbettungen $\operatorname{Ker}\varphi \hookrightarrow \underset{\to}{\mathcal{H}}'$ und $\operatorname{Ker}\varphi \hookrightarrow \underset{\to}{\mathcal{H}}''$, und wegen $\operatorname{Hom}(\underset{\to}{\mathcal{H}}', \underset{\to}{\mathcal{H}}'') = 0$ muss $\operatorname{Ker}\varphi$ endlich sein. Dies steht aber im Widerspruch zur Tatsache, dass die Kette (*) unendlich lang ist : $l(\operatorname{Ker}\varphi) \geq l(\operatorname{Ker}\varphi_n \circ \varphi_{n-1} \ldots) = n$ für alle n. Damit ist die Behauptung b) bewiesen.

c) Alle Werte zwischen 1 und $\sum_i \min(r_i, s_i)$ werden angenommen. Sei hierzu $\varphi : \underset{\to}{\mathcal{G}} \longrightarrow \underset{\to}{\mathcal{H}}$ eine Isogenie mit einfachem Kern, $l(\operatorname{Ker}\varphi) = 1$. Dann gilt nach §9 Folgerung, dass $|\sigma(\underset{\to}{\mathcal{G}}) - \sigma(\underset{\to}{\mathcal{H}})| \leq 1$ ist, d.h. die Sockel-Länge kann sich höchstens um 1 ändern. Da jede Isogenie Komposition von solchen "einfachen" Isogenien ist, folgt die Behauptung aus a) und b).

Bemerkung: a) Aus der Struktur der etalen und der multiplikativen p-divisiblen Gruppen ist leicht zu entnehmen, wie sich der Satz auf beliebige p-divisible Gruppen verallgemeinert : Jeder einfache multiplikative Faktor liefert noch einen Beitrag der Länge 1 zum Sockel.

b) Ist $\underset{\to}{\mathcal{G}}$ eine p-divisible Gruppe definiert über einem beliebigen Körper k mit den Isogenieinvarianten (r_i, s_i) $r_i, s_i > 0$ und teilerfremd, so gilt nach wie vor die Abschätzung des Satzes. Zudem folgt aus obigem Beweis b), dass das Minimum 1 angenommen wird.

Problem: Sind die p-Kerne einfacher p-divisibler Gruppen unzerlegbar? (vgl. hierzu §16.)

§16. p-Kerne in Isogenieklassen

Betrachten wir eine Isogenieklasse von p-divisiblen Gruppen, so stellt sich die Frage, welche Gruppen vom Typ Z als p-Kerne von Elementen dieser Isogenieklasse auftreten.

Der Einfachheit halber wollen wir in diesem Paragraphen den Grundkörper k algebraisch abgeschlossen voraussetzen. Mit Hilfe des Struktursatzes und des vorangehenden Abschnittes erhalten wir zunächst folgendes Resultat:

Satz 1: Ist $\underrightarrow{\mathfrak{G}}$ eine zusammenhängende unipotente p-divisible Gruppe, so gibt es eine zu $\underrightarrow{\mathfrak{G}}$ isogene Gruppe $\underrightarrow{\mathfrak{H}}$ mit dem p-Kern ${}_p\mathfrak{H} \xrightarrow{\sim} \mathfrak{G}_{r,s}$, $r = l_V(\underrightarrow{\mathfrak{G}})$ und $s = l_F(\underrightarrow{\mathfrak{G}})$.

Ist daher $\underrightarrow{\mathfrak{G}}$ eine p-divisible Gruppe mit ${}_p\underrightarrow{\mathfrak{G}} \xrightarrow{\sim} \mathfrak{G}_{r,s}$, so erhalten wir hieraus im allgemeinen keine Informationen über die Isogenieklasse oder gar den Isomorphietyp von $\underrightarrow{\mathfrak{G}}$.

Die Situation ist ganz anders, wenn der p-Kern Gruppen der Gestalt $\mathfrak{G}_{r,1}$ und $\mathfrak{G}_{1,s}$ als direkte Faktoren enthält, wie man aus den folgenden beiden Sätzen erkennt.

Satz 2 (Manin): Ist $\underrightarrow{\mathfrak{G}}$ eine p-divisible Gruppe und r (bzw. s) eine positive natürliche Zahl, so sind folgende Aussagen äquivalent:

(i) $\underrightarrow{\mathfrak{G}}$ ist isogen zu $\underrightarrow{\mathfrak{G}}_{r,1}$ (zu $\underrightarrow{\mathfrak{G}}_{1,s}$);

(ii) $\underrightarrow{\mathfrak{G}}$ ist isomorph zu $\underrightarrow{\mathfrak{G}}_{r,1}$ (zu $\underrightarrow{\mathfrak{G}}_{1,s}$);

(iii) ${}_p\underrightarrow{\mathfrak{G}}$ ist isomorph zu $\mathfrak{G}_{r,1}$ (zu $\mathfrak{G}_{1,s}$);

(iv) $\underrightarrow{\mathfrak{G}}$ ist unipotent zusammenhängend von der Dimension 1 (bzw. s) und der Höhe $r+1$ (bzw. $s+1$).

Beweis: Der Sockel $\mathfrak{S}(\underrightarrow{\mathfrak{G}})$ von $\underrightarrow{\mathfrak{G}} = \underrightarrow{\mathfrak{G}}_{r,1}$ hat die Länge 1 und $\underrightarrow{\mathfrak{G}}_{r,1} / \mathfrak{S}(\underrightarrow{\mathfrak{G}}_{r,1})$ ist isomorph zu $\underrightarrow{\mathfrak{G}}_{r,1}$, wie man unmittelbar

Dieses Resultat lässt sich nun wesentlich verschärfen:

Satz 3: Sei $\underrightarrow{\mathfrak{G}}$ eine p-divisible Gruppe und ${}_p\underrightarrow{\mathfrak{G}} = \mathfrak{G}' \oplus \mathfrak{G}''$ eine direkte Summenzerlegung des p-Kernes mit $\mathfrak{G}'$ vom Typ Z_1, $\mathfrak{G}' \xrightarrow{\sim} \bigoplus_i \mathfrak{G}_{r_i,1} \oplus \bigoplus_j \mathfrak{G}_{1,s_j}$. Dann gibt es eine direkte Zerlegung $\underrightarrow{\mathfrak{G}} = \underrightarrow{\mathfrak{G}}' \oplus \underrightarrow{\mathfrak{G}}''$ mit $\underrightarrow{\mathfrak{G}}' \xrightarrow{\sim} \bigoplus_i \underrightarrow{\mathfrak{G}}_{r_i,1} \oplus \bigoplus_j \underrightarrow{\mathfrak{G}}_{1,s_j}$.

Beweis: Es genügt offensichtlich, den Fall $\mathfrak{G}' \xrightarrow{\sim} \mathfrak{G}_{r,1}$ zu behandeln. Wir zeigen zunächst folgendes: Ist mit den Bezeichnungen des Satzes $\mathfrak{H} \subseteq \mathfrak{G}''$ eine Untergruppe, so induziert die Projektion $\varphi : \underrightarrow{\mathfrak{G}} \longrightarrow \underrightarrow{\mathfrak{G}}_1 = \underrightarrow{\mathfrak{G}}/\mathfrak{H}$ einen Isomorphismus von $\mathfrak{G}'$ auf einen direkten Summanden von ${}_p\underrightarrow{\mathfrak{G}}_1$. Hierzu können wir natürlich annehmen, dass $l(\mathfrak{H}) = 1$ ist, d.h. $\mathfrak{H} \xrightarrow{\sim} {}_p\alpha$. Nach der Bemerkung §7 ist dann $\mathfrak{G}''_1 = \mathfrak{G}''/\mathfrak{H} = \mathfrak{Z} \oplus \mathfrak{T}$ mit $\mathfrak{Z}$ vom Typ Z und $\mathfrak{T}$ unzerlegbar vom Typ T. Aus der exakten Sequenz

$$0 \longrightarrow \mathfrak{G}' \oplus \mathfrak{Z} \oplus \mathfrak{T} \xhookrightarrow{{}_p\varphi} {}_p\underrightarrow{\mathfrak{G}}_1 \longrightarrow {}_p\alpha \longrightarrow 0$$

ergibt sich die induzierte exakte Sequenz

$$\mathcal{D}(\mathfrak{G}') \oplus \mathcal{D}(\mathfrak{Z}) \oplus \mathcal{D}(\mathfrak{T}) \xrightarrow{\mathcal{D}({}_p\varphi)} \mathcal{D}({}_p\underrightarrow{\mathfrak{G}}_1) \longrightarrow {}_p\alpha \longrightarrow 0$$

auf den Deckeln. Nach dem Lemma §11 genügt es für obige Behauptung zu zeigen, dass $\mathcal{D}(\mathfrak{G}') \nsubseteq \operatorname{Ker} \mathcal{D}({}_p\varphi)$ ist. Unter Verwendung des folgenden Lemmas erhalten wir für die Längen der Bilder unter $\mathcal{D}({}_p\varphi) =: \varepsilon$:

$$\begin{aligned}
\delta({}_p\underrightarrow{\mathfrak{G}}_1) - 1 &\leqslant l(\varepsilon\,\mathcal{D}(\mathfrak{G}' \oplus \mathfrak{Z})) + l(\varepsilon\,\mathcal{D}(\mathfrak{T})) \\
&\leqslant \delta(\mathfrak{G}') + \delta(\mathfrak{Z}) + (\sigma(\mathfrak{T}) - 1) = \\
&= \sigma(\mathfrak{G}') + \sigma(\mathfrak{Z}) + \sigma(\mathfrak{T}) - 1 = \sigma({}_p\underrightarrow{\mathfrak{G}}_1) - 1 .
\end{aligned}$$

Es steht also überall das Gleichheitszeichen und insbesondere ist $l(\varepsilon\mathcal{D}(\underset{\rightarrow}{G}')) = \delta(\underset{\rightarrow}{G}')$, d.h. $\mathcal{D}(\underset{\rightarrow}{G}')$ wird injektiv abgebildet.

Wir erhalten damit eine unendliche Sequenz

$$\underset{\rightarrow}{G} = \underset{\rightarrow}{G}_0 \xrightarrow{\varphi_1} \underset{\rightarrow}{G}_1 \xrightarrow{\varphi_2} \underset{\rightarrow}{G}_2 \xrightarrow{\varphi_3} \underset{\rightarrow}{G}_3 \longrightarrow \cdots$$

von Isogenien mit der Eigenschaft, dass die induzierte Sequenz auf den p-Kernen folgende Gestalt hat:

$$G' \oplus G''_0 \xrightarrow{\mathrm{Id}\oplus 0} G' \oplus G''_1 \xrightarrow{\mathrm{Id}\oplus 0} G' \oplus G''_2 \longrightarrow \cdots$$

Setzen wir $\underset{\rightarrow}{H} = \varinjlim_i \underset{\rightarrow}{G}_i$, so ist die induzierte Abbildung $\varphi : \underset{\rightarrow}{G} \longrightarrow \underset{\rightarrow}{H}$ ein Epimorphismus mit $\varphi|G'$ injektiv und mit Kern $\underset{\rightarrow}{K} = \bigcup_i \phi_i^{-1}(G''_i)$, $\phi_i = \varphi_i \circ \varphi_{i-1} \circ \cdots \varphi_1$.

Wir behaupten, dass $\underset{\rightarrow}{K}$ p-divisibel ist : Der Homomorphismus $p\cdot\mathrm{Id} : \underset{\rightarrow}{G}_i \longrightarrow \underset{\rightarrow}{G}_i$ faktorisiert über φ_{i+1}

$$p\cdot\mathrm{Id} = \mu_i \circ \varphi_{i+1} : \underset{\rightarrow}{G}_i \xrightarrow{\varphi_{i+1}} \underset{\rightarrow}{G}_{i+1} \xrightarrow{\mu_i} \underset{\rightarrow}{G}_i$$

mit $\mathrm{Ker}\,\mu_i = G' \subseteq {}_p\underset{\rightarrow}{G}_{i+1}$, und μ_i induziert daher einen Isomorphismus $G''_{i+1} \xrightarrow{\sim} G''_i$. Es ist also $p\cdot\phi_{i+1}^{-1}(G''_{i+1}) = \phi_i^{-1}(G''_i)$ und folglich $\underset{\rightarrow}{K}$ p-divisibel. Man erkennt hieraus auch, dass $\varphi|_{G'} : G' \xrightarrow{\sim} {}_p\underset{\rightarrow}{H}$ ein Isomorphismus ist und daher $\underset{\rightarrow}{H} \cong \underset{\rightarrow}{G}_{r,1}$ ist nach Satz 2.

Wenden wir nun das vorangehende auf die Serre-duale Gruppe ${}^t\underset{\rightarrow}{G}$ an, so finden wir einen Monomorphismus $\psi : \underset{\rightarrow}{H} \hookrightarrow \underset{\rightarrow}{G}$ mit der Eigenschaft, dass $pr_{G'} \circ {}_p\psi : {}_p\underset{\rightarrow}{H} \rightarrow G' \oplus G'' \longrightarrow G'$ ein Isomorphismus ist. Die Komposition

$$\varphi \circ \psi : \underset{\rightarrow}{H} \longrightarrow \underset{\rightarrow}{G} \longrightarrow \underset{\rightarrow}{H}$$

induziert folglich einen Isomorphismus auf den p-Kernen, und ist daher selbst ein Isomorphismus : $\underrightarrow{\mathcal{G}} \xrightarrow{\sim} \underrightarrow{\mathcal{H}} \oplus \operatorname{Ker} \varphi$.

Folgerung (Oort): Ist $\mathcal{G}$ eine unipotente zusammenhängende p-divisible Gruppe mit $h(\underrightarrow{\mathcal{G}}) = 2\cdot\sigma(\underrightarrow{\mathcal{G}})$, so gibt es einen Isomorphismus

$$\underrightarrow{\mathcal{G}} \xrightarrow{\sim} \underrightarrow{\mathcal{G}}^{d}_{1,1}$$

$d = \sigma(\underrightarrow{\mathcal{G}}) = \dim \underrightarrow{\mathcal{G}}$.

Beweis: Die Voraussetzung impliziert offensichtlich ${}_p\underrightarrow{\mathcal{G}} \xrightarrow{\sim} \mathcal{G}^{d}_{1,1}$ mit $d = \sigma(\underrightarrow{\mathcal{G}})$, woraus mit Satz 3 die Behauptung folgt.

Lemma: Ist $\varrho : \mathcal{H} \longrightarrow \mathcal{G}$ ein Homomorphismus von p-Gruppen mit $\mathcal{G}$ vom Typ Z und $\mathcal{H}$ vom Typ T, so gilt für die auf dem Deckel induzierte Abbildung $\mathcal{D}(\varrho) : \mathcal{D}(\mathcal{H}) \longrightarrow \mathcal{D}(\mathcal{G})$:

$$l(\operatorname{Im}\mathcal{D}(\varrho)) \leq \sigma(\mathcal{H}) - 1 .$$

Beweis: Wir beweisen die entsprechende Aussage für Moduln und betrachten einen Homomorphismus $\varrho : M \longrightarrow N$ mit $M = M_A$ vom Typ T und N vom Typ Z (§2 und §3). Es ist nun leicht zu sehen, dass diejenigen beiden Exemplare von k, welche in den beiden Endpunkten des Diagrammes von M_A stehen, im Kern der Komposition

$$M \xrightarrow{\text{kan.}} \mathcal{D}(M) \xrightarrow{\mathcal{D}(\varrho)} \mathcal{D}(N)$$

liegen (diese werden entweder von F oder von V annuliert). Durch die Fallunterscheidung $\delta(M) - \sigma(M) = 0, 1$ oder -1 ergibt sich hieraus sofort die Behautung.

Es dürfte im allgemeinen recht schwierig sein, bei einer vorgegebenen Isogenieklasse die darin vorkommenden p-Kerne zu bestimmen.

Aus dem Vorangehenden erhalten wir z.B. folgende Aussage:

Ist $\underrightarrow{G}$ einfach von der Dimension ≤ 3, so ist ${}_p\underrightarrow{G}$ unzerlegbar (vgl. Problem am Ende von §15).

Wahrscheinlich gilt diese Aussage ganz allgemein für beliebige Dimensionen. Damit wäre das obige Problem wenigstens für die einfachen Isogenieklassen gelöst (verwende den Satz §14).

Der folgende Satz beschreibt eine weitere Situation, wo wir die vollständige Antwort kennen:

Satz 4: Ist $\underrightarrow{G}$ isogen zu $\underrightarrow{G}_{r,1} \oplus \underrightarrow{G}_{1,s}$ mit $r,s \geq 1$, so ist ${}_p\underrightarrow{G}$ entweder zu $\underrightarrow{G}_{r,1} \oplus \underrightarrow{G}_{1,s}$ oder zu $\underrightarrow{G}_{r+1,s+1}$ isomorph.

Genauer: Unter obigen Voraussetzungen gibt es eine Isogenie

$$\varphi : \underrightarrow{G}_{r,1} \oplus \underrightarrow{G}_{1,s} \longrightarrow \underrightarrow{G}$$

mit $l(\operatorname{Ker}\varphi) \leq 1$.

Beweis: Seien $\iota_1 : {}_p\alpha \hookrightarrow \underrightarrow{G}_{r,1}$ und $\iota_2 : {}_p\alpha \hookrightarrow \underrightarrow{G}_{1,s}$ zwei nicht triviale Einbettungen und

$$0 \longrightarrow {}_p\alpha \xrightarrow{\iota = (\iota_1,\iota_2)} \underrightarrow{G}_{r,1} \oplus \underrightarrow{G}_{1,s} \xrightarrow{\varphi_\iota} \underrightarrow{G}_\iota \longrightarrow 0$$

die zugehörige exakte Sequenz. Man folgert hieraus leicht $\sigma(\underrightarrow{G}_\iota) = 1$ (vgl. den Beweis von Satz §9.) und erhält folglich ${}_p\underrightarrow{G}_\iota \cong \underrightarrow{G}_{r+1,s+1}$.

Ist nun $\varphi : \underrightarrow{G}_{r,1} \oplus \underrightarrow{G}_{1,s} \longrightarrow \underrightarrow{G}$ eine Isogenie mit nicht trivialem Kern, so faktorisiert φ über ein geeignetes φ_ι , $\iota = (\iota_1,\iota_2)$, wobei wir ohne Einschränkung ι_1 und ι_2 nicht trivial voraussetzen können : $\varphi = \varphi' \circ \varphi_\iota : \underrightarrow{G}_{r,1} \oplus \underrightarrow{G}_{1,s} \xrightarrow{\varphi_\iota} \underrightarrow{G}' \xrightarrow{\varphi'} \underrightarrow{G}$.

Ist dann φ' kein Isomorphismus, so ist $\mathcal{S}(\underrightarrow{G}') \subseteq \operatorname{Ker}\varphi'$, und insbesondere gilt $\operatorname{Ker}\varphi \supseteq \varphi_\iota^{-1}(\mathcal{S}(\underrightarrow{G}')) = \mathcal{S}(\underrightarrow{G}_{r,1} \oplus \underrightarrow{G}_{1,s})$.

φ faktorisiert daher über den Endomorphismus $\mathcal{V} \oplus \mathcal{F}$ von $\underset{\rightarrow}{G}_{r,1} \oplus \underset{\rightarrow}{G}_{1,s}$, und die Behauptung des Satzes folgt durch Induktion über die Länge $l = l(\operatorname{Ker}\varphi)$.

Mit ähnlichen Methoden lassen sich auch noch weitere Spezialfälle klären. Zum Beispiel enthält die Isogenieklasse von $\underset{\rightarrow}{G}_{2,1} \oplus \underset{\rightarrow}{G}_{r,1}$ die p-Kerne $G_{2,1} \oplus G_{r,1}$, $G_{r+2,2}$ und $G_{VF^{-1}VF^{-r-1}}$.

Wir können auch die "duale" Frage stellen:

In welchen Isogenieklassen kommt eine vorgegebene p-Gruppe als p-Kern vor?

Auch hier kennen wir die Antwort nur in einigen Spezialfällen: falls G vom Typ Z_1 ist (Satz 3) und für $\sigma(G) = 1$ (Satz 2 §15.)

Wir werden in §18 im Zusammenhang mit den Abelschen Varietäten nochmals auf diesen Problemkreis zurückkommen.

Bemerkung: Wir haben zu Beginn dieses Paragraphen den Grundkörper algebraisch abgeschlossen vorausgestzt. Die Sätze 2, 3 und 4 gelten aber auch für einen beliebigen perfekten Grundkörper k; man braucht hierzu eine Aussage der folgenden Art :

Ist $\underset{\rightarrow}{G}$ eine k-Form der p-divisiblen Gruppe $\underset{\rightarrow}{G}_B$ mit zulässigem nicht periodischem B und ist ${}_p\underset{\rightarrow}{G}$ k-isomorph zu G_B, so ist $\underset{\rightarrow}{G}$ k-isomorph zu $\underset{\rightarrow}{G}_B$.

(Zum Beweis verwendet man folgende Eigenschaft der Endomorphismenringe : Die kanonische Projektion $\operatorname{End}(\underset{\rightarrow}{G}_B) \longrightarrow \operatorname{End}(G_B)$ induziert eine Bijektion auf den Restklassenkörpern dieser Endomorphismenringe)

§17. p-adische Tate-Gruppen von Abelschen Varietäten

In diesem Abschnitt setzen wir $k = \bar{k}$ algebraisch abgeschlossen voraus.

Wie üblich verstehen wir im folgenden unter einer Abelschen Varietät A eine vollständige zusammenhängende reduzierte algebraische Gruppe. Das Multiplizieren mit p : $p\,\mathrm{Id}_A : A \longrightarrow A$ und damit auch der Frobeniushomomorphismus $\mathcal{F}_A : A \longrightarrow A^{(p)}$ und die Verschiebung $\mathcal{V}_A : A^{(p)} \longrightarrow A$ sind Epimorphismen mit endlichen Kernen.

Wir definieren wie früher ${}_pA = \mathrm{Ker}\; p\cdot\mathrm{Id}_A$, ${}_{\mathcal{F}}A = \mathrm{Ker}\;\mathcal{F}_A$ und ${}_{\mathcal{V}}A = \mathrm{Ker}\;\mathcal{V}_A^{(p^{-1})}$ (= grösste Untergruppe von A, welche von der Verschiebung annuliert wird).

Die Vereinigung der p^n-Kerne ${}_{p^n}A = \mathrm{Ker}\; p^n\cdot\mathrm{Id}_A$ bildet eine p-divisible Gruppe, die sogenannte p-adische Tate-Gruppe von A, welche wir mit $\underrightarrow{\mathcal{T}}A$ bezeichnen :

$$\underrightarrow{\mathcal{T}}A = \varinjlim_n {}_{p^n}A \;.$$

Es gilt dabei $\dim \underrightarrow{\mathcal{T}}A = \dim A$ und $h(\underrightarrow{\mathcal{T}}A) = 2\cdot\dim A$.

Betrachten wir die duale Varietät $\hat{A}$ zu A, so ist der p-Kern ${}_p\hat{A}$ die Cartier-duale Gruppe zu ${}_pA$, und das gleiche gilt für alle p^n-Kerne. Wir erhalten daher einen kanonischen Isomorphismus

$$\underrightarrow{\mathcal{T}}\hat{A} \xrightarrow{\sim} {}^t(\underrightarrow{\mathcal{T}}A) \;;$$

da A und $\hat{A}$ isogen sind, ergibt sich hieraus der folgende Satz:

Satz: Die Isogenieklasse der p-adischen Tate-Gruppe $\underrightarrow{\mathcal{T}}A$ einer Abelschen Varietät A der Dimension d ist selbstdual, d.h. $\underrightarrow{\mathcal{T}}A$ ist isogen zu einer Gruppe der Gestalt

$$(\underrightarrow{\mathcal{G}}_{1,0} \oplus \underrightarrow{\mathcal{G}}_{0,1})^{\varrho} \oplus \underrightarrow{\mathcal{G}}_{1,1}^{\,n} \oplus \bigoplus_{\substack{r>1\\(r,s)=1}} (\underrightarrow{\mathcal{G}}_{r,s} \oplus \underrightarrow{\mathcal{G}}_{s,r})^{m_{r,s}}$$

In der Arbeit [5] vermutet Manin, dass alle selbstdualen Isogenieklassen p-divisibler Gruppen "algebroid" sind, d.h. eine p-adische Tate-Gruppe einer Abelschen Varietät enthalten.
Dies wurde von Serre [11] und Honda [2] bewiesen, und unter Benützung der Klassifikation der Isogenieklassen Abelscher Varietäten über einem endlichen Körper nach Honda [2] (vgl. auch Tate [12] [13]) wurde dieses Resultat von Lenstra-Oort [4] folgendermassen vervollständigt:

Zusatz 1: Jede selbstduale Isogenieklasse von p-divisiblen Gruppen enthält die p-adische Tate-Gruppe einer Abelschen Varietät A. Ist diese Klasse verschieden von der Isogenieklasse einer Gruppe der Gestalt $\mathfrak{G}^d_{1,1}$, so kann A einfach gewählt werden.

Dieses Resultat besagt also unter anderm, dass man von einer Zerlegung der p-adischen Tate-Gruppe im allgemeinen nicht auf das entsprechende Zerlegen der Abelschen Varietät schliessen kann. Nur im oben nicht betrachteten Falle der Isogenieklasse von $\mathfrak{G}_{1,1}$ hat man das folgende Ergebnis von Oort [7] [8]:

Zusatz 2: Ist A eine Abelsche Varietät mit $\mathfrak{T}A$ isogen zu $\mathfrak{G}^d_{1,1}$, $d = \dim A$, so ist A isogen zu E^d mit einer supersingulären elliptischen Kurve E. Zudem sind folgende Aussagen äquivalent:

(i) A ist isomorph zu E^d,

(ii) $\mathfrak{T}A$ ist isomorph zu $\mathfrak{G}^d_{1,1}$,

(iii) ${}_pA$ ist isomorph zu $\mathfrak{G}^d_{1,1}$,

(iv) $\sigma(A) = d$.

§18. p-Kerne Abelscher Varietäten

Betrachten wir nun wieder die Frage, welche p-Gruppen als p-Kerne Abelscher Varietäten auftreten können, so erhalten wir aus dem Satz von §17 zunächst folgendes Resultat (der Einfachheit halber setzen wir auch in diesem Abschnitt k algebraisch abgeschlossen voraus):

Satz: Ist A eine Abelsche Varietät, so erhalten wir für den p-Kern von A folgende Zerlegung:

$$_pA \cong (\mathbb{Z}/p\mathbb{Z})_k^{\varrho} \oplus {_p\mu_k^{\varrho}} \oplus \mathfrak{U}_A$$

mit $\mathfrak{U}_A$ infinitesimal und unipotent.

Die Grösse ϱ heisst auch der p-Rang der Abelschen Varietät A, ϱ = p-rg A, und ist eine Isogenieinvariante. Die Anzahl der Punkte des p-Kernes ist gegeben durch p^{ϱ}.

Für einen beliebigen perfekten Grundkörper k erhält man eine etwas schwächere Form des Satzes, deren Formulierung wir dem Leser überlassen.

Zusatz: Der unipotente infinitesimale Bestandteil $\mathfrak{U}_A$ des p-Kernes einer Abelschen Varietät A ist eine p-Gruppe vom Typ Z mit $l_F(\mathfrak{U}_A) = l_V(\mathfrak{U}_A) = \dim A - \text{p-rg}\, A$.

Beweis: Nach Konstruktion ist $\mathfrak{U}_A$ der p-Kern des unipotenten zusammenhängenden Bestandteiles der p-adischen Tate-Gruppe $\underrightarrow{T}A$, deren Isogenieklasse nach §17 selbstdual ist. Da l_F und l_V Isogenieinvarianten sind, folgt die Behauptung aus §8 .

Wir werden aber gleich sehen, dass die im Zusatz gegebene Bedingung nicht hinreichend ist dafür, dass eine p-Gruppe als p-Kern einer Abelschen Varietät auftritt.

Es bleibt also nach wie vor das schwierige Problem, die p-Kerne einer selbstdualen Isogenieklasse von p-divisiblen Gruppen zu bestimmen.

In der Tabelle zu Ende dieses Abschnittes geben wir eine vollständige Lösung für die Dimensionen ≤ 4; man beachte, dass die p-Gruppe $\mathfrak{g}_{VF-2} \oplus \mathfrak{g}_{V^2F-1_{VF-1}}$ und ihre duale nicht vorkommen (es folgt sofort aus Satz 3 §17, dass eine p-divisible Gruppe mit diesem p-Kern isogen zu $\underset{\to}{\mathfrak{g}}_{2,1} \oplus \underset{\to}{\mathfrak{g}}_{2,3}$ ist.). Man findet leicht weitere Beispiele von p-Gruppen $\mathfrak{g}$ mit $l_F(\mathfrak{g}) = l_V(\mathfrak{g})$, welche nicht als p-Kerne Abelscher Varietäten auftretem ($\mathfrak{g}_{1,r} \oplus \mathfrak{g}'$ mit unzerlegbarem $\mathfrak{g}'$ vom Typ Z, $l_V(\mathfrak{g}') = r+1$, $l_F(\mathfrak{g}') = 2$ und $\mathfrak{g}' \not\cong \mathfrak{g}_{r+1,2}$).

Wir wollen nun noch erläutern, wie man diese Tabelle erhält und welche Methoden dabei benutzt wurden. Zunächst haben wir die beiden folgenden allgemeinen Resultate:

Satz 1: Jede direkte Summe $\underset{\nu}{\oplus} \mathfrak{U}_\nu$ von unzerlegbaren p-Gruppen $\mathfrak{U}_\nu$ vom Typ Z mit $l_F(\mathfrak{U}_\nu) = l_V(\mathfrak{U}_\nu) = d_\nu$ kommt als p-Kern einer Abelschen Varietät vor, und zwar kann man diese isogen zu E^d wählen mit einer supersingulären elliptischen Kurve E und $d = \sum_\nu d_\nu$.

Beweis: Nach dem Satz §14 ist $\underset{\to}{\mathfrak{g}}_B$ mit $l_F(B) = l_V(B) = d$ isogen zu $\underset{\to}{\mathfrak{g}}^{d}_{1,1}$, woraus die Behauptung folgt.

Satz 2: Ist A eine Abelsche Varietät mit ${}_pA \cong \mathfrak{g}_{d-1,1} \oplus \mathfrak{g}_{1,d-1}$ so ist A einfach und für jede zu A isogene Varietät B ist ${}_pB$ isomorph entweder zu ${}_pA$ oder zu $\mathfrak{g}_{d,d}$.

Dieser Satz ist ein Spezialfall von Satz 4 §16.

<u>Bemerkung</u>: In Ergänzung zu Satz 1 entnimmt man der Tabelle, dass <u>die meisten der unzerlegbaren Gruppen nur in der Isogenieklasse von</u> E^d <u>vorkommen</u>. Es wäre interessant zu wissen, ob dies auf einem allgemeinen Prinzip beruht.

Mit den obigen beiden Sätzen lässt sich der grösste Teil der Tabelle klären. Die noch verbleibenden Einzelfälle ergeben sich mit Hilfe der <u>Methode der "generischen</u> ${}_p\alpha$ <u>-Quotienten"</u> :

<u>Man betrachte eine generische Einbettung</u> $\iota : {}_p\alpha \hookrightarrow \mathfrak{S}(\underset{\to}{\mathfrak{g}})$ <u>in den Sockel von</u> $\underset{\to}{\mathfrak{g}}$ <u>und bestimme den p-Kern des Quotienten</u> $\underset{\to}{\mathfrak{g}}/\iota({}_p\alpha)$, unter Benützung der Resultate von §9.

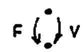
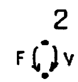
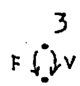
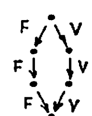
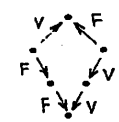
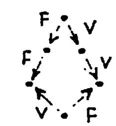
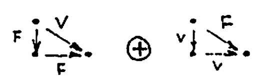
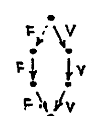
Dieses Verfahren führt in der obigen Situation zum Ziel, da man hier schon nach wenigen Schritten wieder auf etwas schon bekanntes trifft; zum Beispiel haben wir folgende Kette der p-Kerne von generischen ${}_p\alpha$-Quotienten:

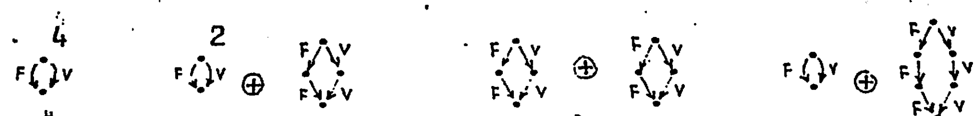
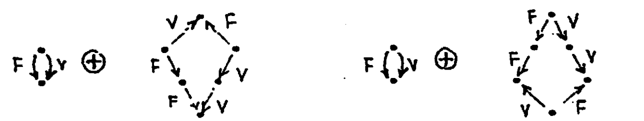
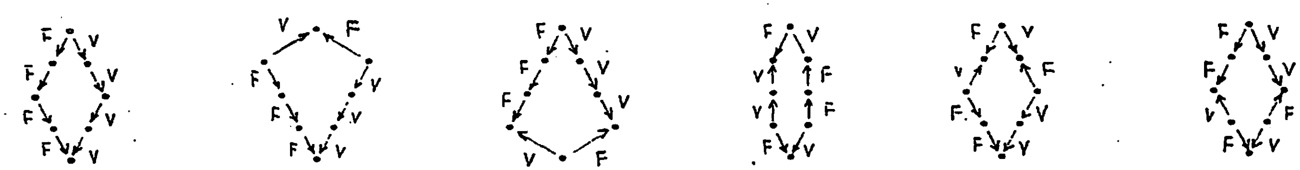
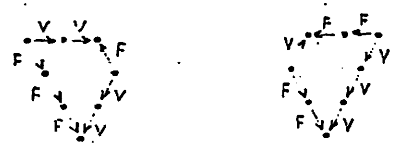
$$\mathfrak{g}_{VF-2} \oplus \mathfrak{g}_{V^3F-2} \longmapsto \mathfrak{g}_{V^3F-1VF-3} \longmapsto \mathfrak{g}_{V^4F-4} \longmapsto \mathfrak{g}_{V-3F^3V-1F}$$

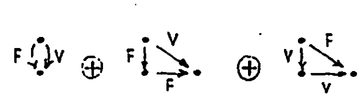
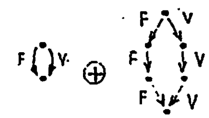
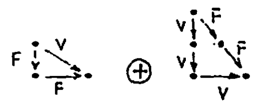
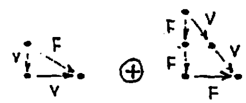
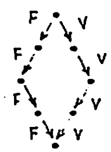
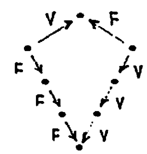
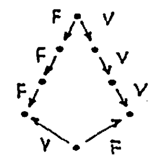
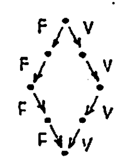
und die letzte Gruppe ist zugleich der p-Kern des generischen ${}_p\alpha$ -Quotienten von $\underset{\to}{\mathfrak{g}}_{1,1} \oplus \underset{\to}{\mathfrak{g}}_{1,2} \oplus \underset{\to}{\mathfrak{g}}_{2,1}$

Diese Methode führt auch in vielen andern Spezialfällen zum Ziel.

Tabelle : p-Kerne Abelscher Varietäten der Dimension ≤ 4

dim	Isogenieklasse	
1	(1, 1)	 $\mathcal{G}_{1,1}$
2	2x(1, 1)	 $\mathcal{G}^2_{1,1}$  $\mathcal{G}_{2,2}$
3	3x(1, 1)	 $\mathcal{G}^3_{1,1}$  $\mathcal{G}_{1,1} \oplus \mathcal{G}_{2,2}$  $\mathcal{G}_{3,3}$  $\mathcal{G}_{VF^{-2}V^2F^{-1}}$  $\mathcal{G}_{VF^{-1}V^2F^{-2}}$
3	(1,2)+(2,1)	 $\mathcal{G}_{1,2} \oplus \mathcal{G}_{2,1}$  $\mathcal{G}_{3,3}$

dim	Isogenieklasse	
4	$4\times(1,1)$	 $\mathcal{G}_{1,1}^{4}$ $\mathcal{G}_{1,1}^{2}\oplus\mathcal{G}_{2,2}$ $\mathcal{G}_{2,2}^{2}$ $\mathcal{G}_{1,1}\oplus\mathcal{G}_{3,3}$  $\mathcal{G}_{1,1}\oplus\mathcal{G}_{V^2F^{-1}VF^{-2}}$ $\mathcal{G}_{1,1}\oplus\mathcal{G}_{V^2F^{-2}VF^{-1}}$  $\mathcal{G}_{4,4}$ $\mathcal{G}_{VF^{-3}V^3F^{-1}}$ $\mathcal{G}_{V^3F^{-3}VF^{-1}}$ $\mathcal{G}_{V^2F^{-1}VF^{-2}VF^{-1}}$ $\mathcal{G}_{V^2F^{-1}VF^{-1}VF^{-2}}$ $\mathcal{G}_{V^2F^{-2}VF^{-1}VF^{-1}}$  $\mathcal{G}_{V^2F^{-3}V^2F^{-1}}$ $\mathcal{G}_{V^3F^{-2}VF^{-2}}$

dim	Isogenieklasse	
4	(1,1)+(1,2)+(2,1)	 $G_{1,1} \oplus G_{1,2} \oplus G_{2,1}$  $G_{1,1} \oplus G_{3,3}$
		 $G_{1,2} \oplus G_{2,2}$  $G_{2,1} \oplus G_{2,3}$
		 $G_{4,4}$  $G_{VF^{-3}V^{3}F^{-1}}$  $G_{V^{3}F^{-3}VF^{-1}}$
4	(1,3)+(3,1)	 $G_{1,3} \oplus G_{3,1}$  $G_{4,4}$

Anhang : Endlichdimensionale Darstellungen des Ringes $k_\sigma[\![a,b]\!]/(a\cdot b)$

Die folgende Klassifikation der Moduln endlicher Länge über dem Ring $\mathcal{A} = k_\sigma[\![a,b]\!]/(a\cdot b)$ ist eine leichte Verallgemeinerung der Resultate von Gelfand-Ponomarev [1]. Dabei benutzen wir eine von P. Gabriel gegebene funktorielle Interpretation dieser Resultate und folgend auch weitgehend seinen unveröffentlichten Aufzeichnungen. Ihm und auch C. Ringel danken wir für die Bemerkungen zum Text. Man vergleiche hierzu auch die Arbeit [14].

1. Unterfunktoren des Vergissfunktors

Sei k ein Körper, $\lambda \longmapsto \lambda^\sigma$ ein Automorphismus von k und $\mathcal{A} = k_\sigma[\![a,b]\!]/(a\cdot b)$ der (eventuell nicht kommutative) Ring, welcher über k von a,b erzeugt wird mit den Relationen

$$a\cdot b = b\cdot a = 0\,, \quad a\lambda = \lambda^\sigma a \quad \text{und} \quad \lambda b = b\lambda^\sigma \quad \text{für} \quad \lambda\in k.$$

Eine Abbildung $\varphi : V \longrightarrow W$ zwischen zwei k-Vektorräumen heisst σ-semilinear (oder semilinear bezüglich σ), wenn für alle $\lambda \in k$ und $v\in V$ gilt : $\varphi(\lambda\cdot v) = \lambda^\sigma\cdot\varphi(v)$.

Jedem $\mathcal{A}$-Modul M ordnen wir den unterliegenden k-Vektorraum $V(M) = M$ zu und wollen gewisse Unterfunktoren des Vergissfunktors V betrachten.

Sei $\mathcal{H} = \mathcal{H}(b,a^{-1})$ die von b und a^{-1} frei erzeugte Halbgruppe mit 1; ihre Elemente sind also Monome z.B. von der Gestalt $a^{-4}b^3a^{-1}b^2$. Auf $\mathcal{H}$ führen wir eine totale Ordnung ein (lexikographisch), so dass gilt :

a) $bD < 1 < a^{-1}D$ für alle $D\in\mathcal{H}$, ?

b) Aus $A < B$ folgt $AD < BD$ für alle $D\in\mathcal{H}$.

Jedem Monom D ordnen wir schliesslich zwei Unterfunktoren D^- und D^+ zu, welche folgendermassen definiert werden:

$D^-(M)$: ...

Satz: Die Menge der Unterfunktoren der Gestalt $D^- \subset D^+$ mit $D \in \mathcal{H}$ ist total angeordnet. Aus $D < E$ folgt $D^- \subset D^+ \subset E^- \subset E^+$.

Beweis: Die Behauptung folgt unmittelbar aus

$$(AbB)^+(M) = AbBa^{-1}(0) \subseteq Ab(M) \subseteq Aa^{-1}(0) \subseteq Aa^{-1}Cb(M) = (Aa^{-1}C)^-(M)$$

Damit erhalten wir eine Filtrierung des Vergissfunktors durch die Unterfunktoren D^+, D^- mit $D \in \mathcal{H}(b,a^{-1})$.

In genau gleicher Weise führt die Betrachtung der Halbgruppe $\mathcal{H}(a,b^{-1})$ zu einer weiteren Filtrierung des Vergissfunktors, welche wir zum Unterschied "zweite Filtrierung" nennen.

2. Moduln erster Art

Wir betrachten nun die zweite Filtrierung, sowie die dadurch auf $a^{-1}(0_M)/b(M)$ induzierte Filtrierung. Schreiben wir kurz b^{-1} für den Funktor $M \longmapsto b^{-1}(0_M)$ und a für den Funktor $M \longmapsto a(M)$ (und entsprechend für b und a^{-1}), so können wir jedem Monom

$$D = a^{p_1}b^{-q_1}a^{p_2} \dots a^{p_r}b^{-q_r} \in \mathcal{H}(a,b^{-1})$$

die beiden Unterfunktoren

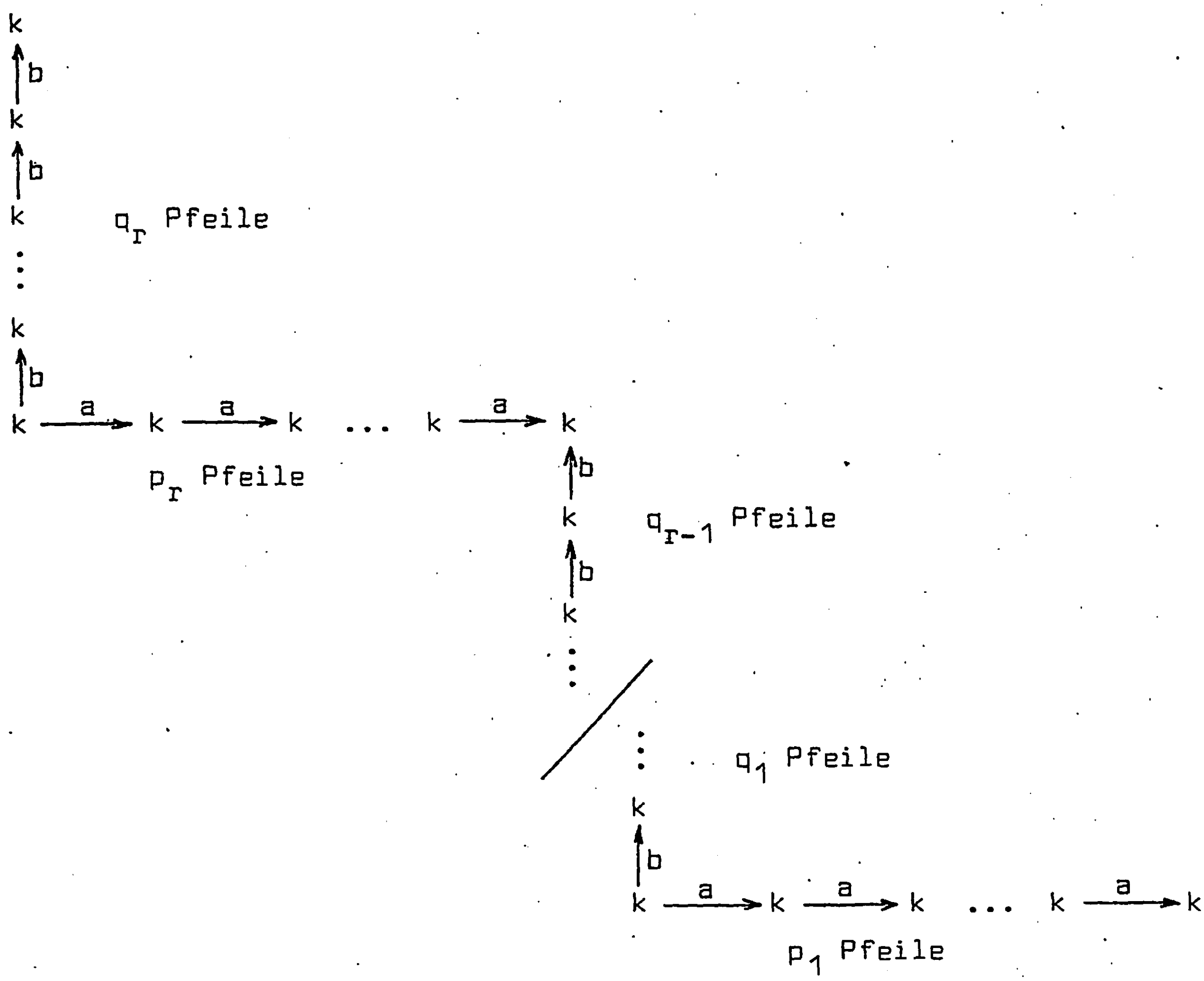
$$Da \cap a^{-1}/Da \cap b \subseteq Db^{-1} \cap a^{-1}/Db^{-1} \cap b \subseteq a^{-1}/b$$

von a^{-1}/b zuordnen, sowie den entsprechenden Faktor (= Unterrestklassenfunktor) V_D des Vergissfunktors V :

$$V_D = Db^{-1} \cap a^{-1}/Db^{-1} \cap b + Da \cap a^{-1} =$$

$$= (Db^{-1} \cap a^{-1}/Db^{-1} \cap b) \;/\; (Da \cap a^{-1}/Da \cap b) .$$

Zu jedem solchen D gehört auch ein Modul M_D, welcher unzerlegbar ist und Modul erster Art genannt wird, beschrieben durch das folgende Diagramm:



<u>Satz</u>: a) <u>Es ist</u> $V_D(M_D) = k$ <u>und</u> $V_D(M_E) = 0$ <u>für</u> $D \neq E \in \mathcal{H}(a,b^{-1})$.

b) <u>Sei</u> $v_D \in V_D(M_D)$, $v_D \neq 0$. <u>Dann gibt es für jeden</u> $\mathcal{A}$-<u>Modul</u> M <u>und jedes</u> $v \in V_D(M)$ <u>ein</u> $\mu: M_D \longrightarrow M$ <u>mit</u> $V_D(\mu)(v_D) = v$.

<u>Beweis</u>: a) Es ist offensichtlich $a^{-1}(0_M)/b(M_D) = ke$, wobei e im obigen Diagramm die Kopie von k ganz unten rechts erzeugt. Zudem ist auch $V_D(M_D) = ke$, d.h.

$$0 = (Da \cap a^{-1}/Da \cap b)(M_D) \text{ und } (Db^{-1} \cap a^{-1}/Db^{-1} \cap b)(M_D) = (a^{-1}/b)(M_D).$$

Für $E < D$ gilt daher $(Eb^{-1} \cap a^{-1}/Eb^{-1} \cap b)(M_D) = 0$ und folglich

$V_E(M_D) = 0$. Für $E > D$ erhalten wir analog $(Ea \cap a^{-1}/Ea \cap b)(M_D) =$
$= (a^{-1}/b)(M_D)$ und daher $V_E(M_D) = 0$.

b) Dies folgt unmittelbar aus den Definitionen.

Bemerkung: Für $E \in \mathcal{H}(a,b^{-1})$ gilt $E^+(M_D)/E^-(M_D) = k$ oder 0, je nach dem ob $D = D_1E$ ist oder nicht. Eine entsprechende Aussage gilt für Monome $A \in \mathcal{H}(b,a^{-1})$.

3. Moduln zweiter Art

Sei nun $A \in \mathcal{H}(b,a^{-1})$ ein Monom, aber keine Potenz, d.h. verschieden von B^m für alle $m > 1$. Zudem sei A auch verschieden von b, 1, a^{-1}. Als Beispiel nehmen wir $A = ba^{-1}ba^{-2}$.

Es seien nun
$$A_0 = A \ , \ A_1 \ , \ A_2 \ , \ \dots \ , \ A_{n-1} \ , \ A_n = A_0 = A$$
die Monome, die man aus A durch zyklische Vertauschung der "Buchstaben" erhält, n = Wortlänge. In unserem Beispiel erhalten wir
$$A_0 = A_5 = ba^{-1}ba^{-2} \ , \ A_1 = a^{-1}ba^{-2}b \ , \ A_2 = ba^{-2}ba^{-1} \ ,$$
$$A_3 = a^{-2}ba^{-1}b \ , \ A_4 = a^{-1}ba^{-1}ba^{-1} \ .$$

Für jedes solche A_i und jeden $\mathcal{A}$-Modul M setzen wir nun
$$A_i^\infty(0_M) = \bigcup_r A_i^r(0_M) \quad \text{und} \quad A_i^\infty(M) = \bigcap_r A_i^r(M)$$
sowie
$$W_{A_i}(M) = A_i^\infty(0_M) \,/\, A_i^\infty(M) \ .$$

Zwischen den verschiedenen Räumen, die wir so erhalten, induzieren die Multiplikationen mit a oder b semilineare Abbildungen (bezüglich σ oder σ^{-1}), die wir im Falle unseres Beispieles wie folgt spezifizieren ($W_i = W_{A_i}(M)$):

$A^r 0 \subset A^{r+1} 0 \quad \subset \quad A^{r+1} \cap \subset A^r \cap$

$A^{r-1} 0 \subset A^r 0 \qquad\qquad A^r \cap \subset A^{r-1} \cap$

$$\begin{tikzcd}
& W_0 & \\
W_1 \arrow[ur, "b"] \arrow[d, "a"'] & & W_4 \arrow[ul, "a"'] \\
W_2 & & W_3 \arrow[ll, "b"] \arrow[u, "a"']
\end{tikzcd}$$

Lemma: Die Abbildungen a,b des obigen Diagrammes sind bijektiv.

Beweis: Aus den Definitionen folgt unmittelbar, dass die Abbildungen b alle surjektiv, die Abbildungen a alle injektiv sind. Wenn nicht alle bijektiv wären, müsste die Dimension streng steigen, wenn man im Gegenuhrzeigersinn herumliefe.

Wir können ohne weiteres annehmen, dass A_o minimal nicht-periodisch ist (das heisse: $A_o \neq b,\ 1,\ a^{-1},\ B^r$ für $r > 1$, und $A_o < A_i$ für $i = 1,2,..,n-1$). Dann induziert die Komposition

$$W_o \xrightarrow{a^{-1}} W_4 \xrightarrow{a^{-1}} W_3 \xrightarrow{b} W_2 \xrightarrow{a^{-1}} W_1 \xrightarrow{b} W_o$$

einen σ^{-n}-semilinearen Automorphismus φ_{A_o} von W_o.

Setzen wir $R_{-n} = k_\tau[T,T^{-1}]$, wobei die Unbestimmte T den Vertauschungsregeln $T\lambda = \lambda^{\sigma^n} T$ genügt, so kann (W_o, φ_{A_o}) auch als R_{-n}-Modul aufgefasst werden und wir bezeichnen diesen mit $W_A(M)$.

Umgekehrt gehört zu jedem R_{-n}-Modul W ein $\mathcal{A}$-Modul $M_A(W)$, welchen wir folgendermassen konstruieren: Wir wählen einen σ-semilinearen Automorphismus σ_W von W und setzen $M_A(W) = W^n$ n = Wortlänge von A, wobei a und b auf den Faktoren W_o, W_1, $W_2, .., W_{n-1}$ entsprechend dem folgenden Diagramm operieren:

$$\begin{tikzcd}
 & & W = W_0 & & \\
W = W_1 \arrow[urr, "b = T\circ\sigma_W^{n-1}"] \arrow[dr, "a=\sigma_W"'] & & & & W_4 = W \arrow[ull, "a=\sigma_W"'] \\
 & W = W_2 & & W_3 = W \arrow[ll, "b=\sigma_W^{-1}"] \arrow[ur, "a=\sigma_W"'] &
\end{tikzcd}$$

Es ist leicht zu sehen, dass der Isomorphietyp dieses Moduls nicht von der Wahl von σ_W abhängt.

Satz: a) Es ist $W_A(M_A(W)) = W$, sowie $W_A(M_D) = 0$ und $V_D(M_A(W)) = W_B(M_A(W)) = 0$ für alle weiteren B und alle D.

b) Für jeden $\mathcal{A}$-Modul M existiert ein $\nu : M_A(W_A(M)) \longrightarrow M$ mit invertierbarem $W_A(\nu)$.

Den Beweis dieses Satzes geben wir in Abschnitt 6.

4. Struktursatz

Satz: Der Funktor

$$((V_D),(W_A)) \quad : \quad \mathrm{mod}_{\mathcal{A}} \longrightarrow \coprod_D \mathrm{mod}_k \times \coprod_A \mathrm{mod}_{R_{-n_A}}$$

ist eine Darstellungsspiegelung. Dabei bezeichnet $\mathrm{mod}_{\mathcal{A}}$ die Kategorie der $\mathcal{A}$-Moduln endlicher Länge, und entsprechend mod_k und $\mathrm{mod}_{R_{-n_A}}$, D durchläuft alle Monome in $\mathcal{H}(a,b^{-1})$ und A alle minimalen nicht-periodischen Monome in $\mathcal{H}(b,a^{-1})$, und n_A ist die Wortlänge von A.

Ein Funktor $F : \mathcal{C} \to \mathcal{D}$ heisst Darstellungsspiegelung, wenn er surjektiv auf den Objekten (bis auf Isomorphie), surjektiv auf den Morphismen ist und wenn aus $Ff = \mathrm{Iso}$ auch $f = \mathrm{Iso}$ folgt.

Korollar: Jeder $\mathcal{A}$-Modul endlicher Länge ist direkte Summe von Moduln erster und zweiter Art. Die Moduln M_D sind unzerlegbar, und ein Modul $M_A(W)$ ist genau dann unzerlegbar, wenn der Modul W unzerlegbar ist.

Beginn des Beweises: Sei $F : \mathcal{C} \longrightarrow \mathcal{D}$ ein additiver Funktor, und es habe $\mathcal{D}$ die Eigenschaft, dass jedes Objekt $D \in \mathcal{D}$ direkte Summe von unzerlegbaren ist. Um nachzuweisen, dass F eine Darstellungsspiegelung ist, genügt es, folgendes zu zeigen:

1) Jedes unzerlegbare Objekt $D \in \mathcal{D}$ ist isomorph zu einem FD' mit $D' \in \mathcal{C}$.

2) Zu jedem Objekt $C \in \mathcal{C}$ und jedem Morphismus $f : D \longrightarrow FC$ gibt es einen Morphismus $g : D' \longrightarrow C$ mit $Fg = f$, D und D' wie in 1).

3) Aus $Ff = \mathrm{Iso}$ folgt schon $f = \mathrm{Iso}$.

Die Bedingungen 1) und 2) folgen aus den Sätzen von Abschnitt 2 und 3. Es bleibt die Bedingung 3), deren Nachweis in Abschnitt 8 erbracht wird.

5. Unendliche Wörter

Wir betrachten die Menge $\mathcal{H}^{\infty}(b,a^{-1})$ der Wörter

$$A = x_1x_2x_3\ldots x_nx_{n+1}\ldots$$

unendlicher Länge in b und a^{-1} ($x_i = b$ oder $= a^{-1}$). Diese Wörter werden wieder lexikographisch durch $b < a^{-1}$ total geordnet. Die n-te Approximation von A ist das Monom A_n endlicher Länge

$$A_n = x_1x_2x_3\ldots x_{n-1}x_n \in \mathcal{H}(a,b_{-1})$$

Jedem solchen Wort A ordnen wir zwei Unterfunktoren A', A'' des Vergissfunktors V zu:

$A'(M) =$ [illegible]

Lemma: a) *Für* $A < B$ *gilt* : $A' \subseteq A'' \subseteq B' \subseteq B''$.

b) *Für* $D \in \mathcal{H}(b,a^{-1})$ *ist* $D^{-} = (Dba^{-\infty})' = (Dba^{-\infty})''$ *und* $D^{+} = (Da^{-1}b^{\infty})' = (Da^{-1}b^{\infty})''$.

Beweis: Die Behauptung a) ergibt sich wie beim Lemma von Abschnitt 1, und b) folgt aus den Definitionen.

Satz: *Es gilt* $A' \neq A''$ *nur dann, wenn* $A = D^{\infty}$ *mit* $D \in \mathcal{H}(b,a^{-1})$, $D \neq b,a^{-1}$ *ist.*

Beweis: Sei $A = CB$ eine Zerlegung mit $C \in \mathcal{H}(b,a^{-1})$ und $B \in \mathcal{H}^{\infty}(b,a^{-1})$. Aus $A' \neq A''$ folgt dann unmittelbar $B' \neq B''$. Ist nun M ein $\mathcal{A}$-Modul mit $A'(M) \neq A''(M)$, so folgt auch $B'(M) \neq B''(M)$, und dies kann nur für endlich viele verschiedene Wörter B vorkommen. Wir erhalten daher $A = CD^{\infty}$ mit endlichen C und D, und wir wollen zeigen, dass $C = 1$ gilt.
Sei $C \neq 1$ minimal gewählt und $D = Eb$, $C = Fa^{-1}$ um ein Beispiel zu wählen. Dann ist $A = Fa^{-1}D^{\infty} = Fa^{-1}EbD^{\infty}$, d.h. es ist sowohl $a^{-1}D^{\infty}(O_M) \neq a^{-1}D^{\infty}(M)$, als auch $bD^{\infty}(O_M) \neq bD^{\infty}(M)$. Nach dem folgenden Lemma ist

$$\dim D^{\infty}(M)/D^{\infty}(O_M) \geqslant \dim bD^{\infty}(M)/bD^{\infty}(O_M) + \dim a^{-1}D^{\infty}(M)/a^{-1}D^{\infty}(O_M).$$

Wie in Abschnitt 3 ist wegen $D = Eb$ die Multiplikation mit b ein Isomorphismus

$$D^{\infty}(M)/D^{\infty}(O_M) \xrightarrow{\sim} bD^{\infty}(M)/bD^{\infty}(O_M),$$

woraus $a^{-1}D^{\infty}(M)/a^{-1}D^{\infty}(O_M) = 0$ folgt, also ein Widerspruch.

Lemma: *Aus* $ba = 0$ *und* $P \subseteq N \subseteq M$ *folgt*

$$\dim N/P \geqslant \dim bN/bP + \dim a^{-1}N/a^{-1}P .$$

Beweis: Es ist $P \subseteq (N \cap I)+P \subseteq (N \cap K)+P \subseteq N \cap (K+P) \subseteq N$ mit $I = \operatorname{Im} a$ und $K = \operatorname{Ker} b$. Die Behauptung folgt dann aus den beiden Isomorphismen

$$(N \cap I)+P/P \cong N \cap I/P \cap I \cong a^{-1}N/a^{-1}P$$

und

$$N/N \cap (K+P) \cong N+K/P+K \cong \dots$$

Wir werden diese Resultate vor allem im letzten Abschnitt benützen, wo wir eine genauere Beschreibung des Verbandes der eben konstruierten Unterfunktoren A', A'' von V geben.

6. Beweis des Satzes von Abschnitt 3

a) Wir zeigen zunächst $W_A(M_A(W)) = W$. Dazu nehmen wir wieder den Spezialfall $A = ba^{-1}ba^{-2}$, geben jedoch einen Beweis, der sich leicht auf den allgemeinen Fall übertragen lässt.

Der Modul $M = M_A(W)$ ist durch das folgende Diagramm gegeben:

$$\begin{tikzcd}
 & & W_0 & & \\
W_1 \arrow[urr, "b", "\sim"'] \arrow[dr, "a"', "\wr"] & & & & W_4 \arrow[ull, "a"', "\sim"] \\
 & W_2 & & W_3 \arrow[ll, "\sim", "b"'] \arrow[ur, "\wr", "a"'] &
\end{tikzcd}$$

Für die zyklischen Vertauschungen A_i von A haben wir folgende lexikographische Anordnung:

$$A_0^\infty < A_2^\infty < A_4^\infty < A_1^\infty < A_3^\infty .$$

Man zeigt nun ohne weiteres, dass $W_i \subseteq A_i^\infty(M) = (A_i^\infty)''(M)$ und dass

$$0 = W_i \cap A_i^\infty(0_M) = W_i \cap (A_i^\infty)''(M)$$

gilt. Wegen

$$\dim M = \sum_i \dim W_i = \sum_i \dim(A_i^{\infty\,''}(M)/A_i^{\infty\,'}(M) \leq \dim M$$

erhalten wir

$$0 = A_0^{\infty\,'}(M) \subseteq A_0^{\infty\,''}(M) = A_2^{\infty\,'}(M) \subseteq A_2^{\infty\,''}(M) = A_4^{\infty\,'}(M) \subseteq \ldots \subseteq A_3^{\infty\,''}(M) = M$$

sowie

$$W_i = A_i^\infty(M)/A_i^\infty(0_M) ,$$

Mit ähnlichen Überlegungen ergeben sich auch die restlichen Behauptungen von a).

b) Für den Beweis dieser Behauptung brauchen wir einige Eigenschaften von (semilinearen) Relationen, welche im folgenden Abschnitt 7 zusammengestellt sind. Wir führen den Beweis wieder am Beispiel $A = ba^{-1}ba^{-2}$.

Wir betrachten die durch A definierte Relation auf M. Für diese Relation gilt $x \mapsto y$ genau dann, wenn es Elemente $z_1, z_2, z_3, z_4 \in M$ gibt mit

$$\begin{tikzcd}
x & & & y \\
z_1 \arrow[u, mapsto, "b"] \arrow[dr, mapsto, "a"'] & & & z_4 \arrow[u, mapsto, "a"'] \\
& z_2 & z_3 \arrow[l, mapsto, "b"] \arrow[ur, mapsto, "a"'] &
\end{tikzcd}$$

Nach dem Zerlegungssatz (Abschnitt 7) gibt es eine Vektorraumzerlegung
$$A_0^{\infty''}(M) = \mathrm{Def}^{\infty} A^{-1} = \mathrm{Ker}^{\infty} A^{-1} \oplus N = A_0^{\infty'}(M) \oplus N$$

derart dass zu jedem $y \in N$ genau ein $x \in N$ existiert mit $x \mapsto y$. Man findet hieraus leicht semilineare Abbildungen

$$z_i : N \longrightarrow A_i^{\infty''}(M) \qquad (\text{bezüglich } \sigma^{-n+i})$$

und

$$x : N \longrightarrow N \qquad (\text{bezüglich } \sigma^{-n})$$

mit der Eigenschaft, dass für alle $y \in N$ die Beziehungen

$$\begin{tikzcd}
x(y) & & & y \\
z_2(y) \arrow[u, mapsto, "b"] & & & z_4(y) \arrow[u, mapsto, "a"'] \\
& z_2(y) \arrow[ul, mapsto, "a"] & z_3(y) \arrow[l, mapsto, "b"'] \arrow[ur, mapsto, "a"] &
\end{tikzcd}$$

gelten. Nach Konstruktion ist der R_{-n}-Modul $W_A(M)$ gegeben durch (N, x), und man sieht sofort, dass die durch

$$\nu(w_0, w_1, w_2, \ldots) = w_0 + z_1(\sigma_W^{n-1}(w_1)) + z_2(\sigma_W^{n-2}(w_2)) + \ldots$$

gegebene lineare Abbildung $\nu : M_A(N) = N^n \longrightarrow M$ ein $\mathfrak{A}$-Modulhomomorphismus mit den gesuchten Eigenschaften ist.

7. Semilineare Relationen

Unter einer semilinearen Relation R (bezüglich σ^n) auf einem endlichdimensionalen k-Vektorraum V verstehen wir eine additiv abgeschlossene Teilmenge $R \subseteq V \times V$ mit der Eigenschaft, dass für $(x,y) \in R$ und $\lambda \in k$ auch $(\lambda x, \lambda^{\sigma^n} y) \in R$ gilt. Wir schreiben $x \mapsto y$ anstelle von $(x,y) \in R$, und definieren für $n > 0$

$$\mathrm{Def}^n R = \{x \in V \mid \exists \text{ Sequenz } x \mapsto x_1 \mapsto x_2 \mapsto \ldots \mapsto x_n\}$$

$$\mathrm{Ker}^n R = \{x \in V \mid \exists \text{ Sequenz } x \mapsto x_1 \mapsto \ldots \mapsto x_{n-1} \mapsto 0\},$$

sowie $\mathrm{Def}^\infty R = \bigcap_n \mathrm{Def}^n R$ und $\mathrm{Ker}^\infty R = \bigcup_n \mathrm{Ker}^n R.$

Die $D^i = \mathrm{Def}^i R$ und $K^i = \mathrm{Ker}^i R$ sind k-Vektorräume $\subseteq V$ und wir erhalten

$$V \supseteq D^1 \supseteq D^2 \supseteq \ldots \supseteq D^\infty \supseteq K^\infty \supseteq \ldots \supseteq K^2 \supseteq K^1 \supseteq 0 .$$

Insbesondere ist $D^n = D^\infty$ und $K^n = K^\infty$ für genügend grosses n.

Lemma 1: Für alle $x \in D^\infty$ gibt es ein $y \in D^\infty$ mit $x \mapsto y$.

Beweis: klar.

Lemma 2: Sind $x, y, y' \in D^\infty$ mit $x \mapsto y$ und $x \mapsto y'$, so gilt $y' - y \in K^\infty$.

Beweis: Sei $B = \{y \in D^\infty \mid \exists x \in D^\infty \text{ mit } x \mapsto y\}$. Aus $y \in B$ und $x \mapsto y$, $x' \mapsto y$ folgt dann $x' - x \in K^\infty$, und wir erhalten eine semilineare Abbildung

$$f : B \longrightarrow D^\infty/K^\infty$$

gegeben durch $f(y) = \overline{x}$ für $x \mapsto y$. Nach Lemma 1 ist f surjektiv und wegen $f(K^\infty) = 0$ faktorisiert f in der Gestalt

$$B \longrightarrow B/B \cap K^\infty \xrightarrow{\overline{f}} D^\infty/K^\infty .$$

mit surjektivem $\overline{f}$. Aus Dimensionsgründen ist $\overline{f}$ bijektiv, also auch injektiv.

Lemma 1 und 2 besagen, dass die auf D^∞/K^∞ durch R induzierte Relation durch einen (σ^n-semilinearen) Automorphismus

$$T : D^\infty/K^\infty \longrightarrow D^\infty/K^\infty$$

beschrieben wird. d.h. es gilt $T(\bar{x}) = \bar{y}$ genau dann, wenn für ein geeignetes $z \in K$ die Relation $x \mapsto y+z$ richtig ist.

Zerlegungssatz: Für die auf D^∞ induzierte Relation gibt es eine Zerlegung

$$(D^\infty, R|D^\infty) = (K^\infty, R|K^\infty) \oplus (D^\infty/K^\infty, T) .$$

Beweis: Sei $\varrho : D^\infty/K^\infty \longrightarrow D^\infty$ irgend ein linearer Schnitt der kanonischen Projektion. Dann gibt es eine σ^n-semilineare Abbildung $\kappa = \kappa_1 : D^\infty/K^\infty \longrightarrow K^\infty$ mit

$$\varrho(x) \longmapsto \varrho(Tx) + \kappa(x) \qquad \text{für alle } x \in D^\infty/K^\infty.$$

(Wähle eine k-Basis von D^∞/K^∞!). Folglich findet man auch Abbildungen $\kappa_i : D^\infty/K^\infty \longrightarrow K^\infty$, κ_i σ^{in}-semilinear, mit

$$\kappa(x) \mapsto \kappa_2(x) \mapsto \kappa_3(x) \mapsto \ldots \mapsto \kappa_m(x) \mapsto 0$$

für alle $x \in D^\infty/K^\infty$. Wir definieren dann eine lineare Abbildung

$$\tau : D^\infty/K^\infty \longrightarrow K^\infty$$

durch $$\tau(x) = \kappa T^{-1}(x) + \kappa_2 T^{-2}(x) + \ldots + \kappa_m T^{-m}(x)$$

und setzen $\varrho' = \varrho + \tau : D^\infty/K^\infty \longrightarrow D^\infty$. Nach Konstruktion gilt:

$$\varrho'(x) - \tau(x) \longmapsto \varrho'(Tx) - \tau(Tx) + \kappa(x)$$

also

$$\varrho'(x) - \kappa T^{-1}(x) - \ldots - \kappa_m T^{-m}(x) \longmapsto \varrho'(Tx) - \kappa_2 T^{-1}(x) - \ldots - \kappa_m T^{-m+1}(x)$$

woraus $\varrho'(x) \mapsto \varrho'(Tx)$ und damit die Behauptung folgt.

8. Beweis des Struktursatzes

p. 20

Lemma: Es sei $f : M \longrightarrow N$ ein Homomorphismus von $\mathcal{A}$-Moduln, derart dass die induzierten Abbildungen

$$D^+f/D^-f : D^+M/D^-M \longrightarrow D^+N/D^-N \quad , \quad A''f/A'f : A''M/A'M \longrightarrow A''N/A'N$$

bijektiv sind für alle $D \in \mathcal{H}(b,a^{-1})$, $A \in \mathcal{H}^{\infty}(b,a^{-1})$. Dann ist f ein Isomorphismus.

Beweis: Nach den Ergebnissen des folgenden Abschnitts 9 gibt es eine Normalreihe sowohl von M als auch von N, deren Faktoren die Gestalt D^+M/D^-M , D^+N/D^-N oder $A''M/A'M$, $A''N/A'N$ haben.

Zum Beweis des Struktursatzes bleibt uns noch der Nachweis der folgenden Behauptung (vgl. Abschnitt 4):

Behauptung: Ist $f : M \longrightarrow N$ ein $\mathcal{A}$-Modulhomomorphismus mit $V_E(f)$ und $W_B(f)$ bijektiv für alle $E \in \mathcal{H}(a,b^{-1})$ und alle minimalen nicht-periodischen $B \in \mathcal{H}(b,a^{-1})$, so ist f ein Isomorphismus.

Beweis: Nach Abschnitt 3 ist unter obiger Voraussetzung $W_B(f) = B^{\infty''}(f)/B^{\infty'}(f)$ bijektiv auch für alle nicht-periodischen $B \in \mathcal{H}(b,a^{-1})$, woraus mit dem Satz von Abschnitt 5 die Bijektivität von $A''f/A'f$ für alle $A \in \mathcal{H}^{\infty}(b,a^{-1})$.

Es bleibt noch zu zeigen, dass D^+f/D^-f bijektiv ist für alle $D \in \mathcal{H}(b,a^{-1})$. Dazu betrachten wir die folgenden Unterfunktoren von V :

$$Db \subseteq Db + a \cap Da^{-1} \subseteq Db + b^{-1} \cap Da^{-1} \subseteq Da^{-1} .$$

Die Multiplikation mit b induziert einen Isomorphismus

$$Da^{-1}/(Db + b^{-1} \cap Da^{-1}) \xrightarrow{\sim} bDa^{-1}/bDb$$

und die Multiplikation mit a einen I-

Induziert daher f einen Isomorphismus

$$Da^{-1}(O_M)/Db(M) \xrightarrow{\sim} Da^{-1}(O_N)/Db(N) \ ,$$

so erhalten wir auch Isomorphismen

$$bDa^{-1}(O_M)/bDb(M) \xrightarrow{\sim} bDa^{-1}(O_N)/bDb(N)$$

und
$$a^{-1}Da^{-1}(O_M)/a^{-1}Db(M) \xrightarrow{\sim} a^{-1}Da^{-1}(O_N)/a^{-1}Db(N) \ .$$

Mittels Induktion über die Länge von D genügt es daher nachzuweisen, dass f einen Isomorphismus

$$a^{-1}(O_M)/b(M) \xrightarrow{\sim} a^{-1}(O_N)/b(N)$$

induziert. Hierzu brauchen wir nur zu zeigen, dass diese Vektorräume Normalreihen mit Faktoren der Gestalt $V_E(M)$, $V_E(N)$ mit $E \in \mathcal{H}(a,b^{-1})$ besitzen. Nun wissen wir, dass Normalreihen von V mit Faktoren der Gestalt E^+/E^- und W_A existieren, $E,A \in \mathcal{H}(a,b^{-1})$, A nicht periodisch. Die induzierten Faktoren für $a^{-1}(O_M)/b(M)$ sind dann

$$V_E(M) \quad \text{und} \quad \overline{W}_A(M) := A^{\infty}(M) \cap a^{-1}(O_M) \ / \ (A^{\infty}(M) \cap a^{-1}(O_M) + A^{\infty}(M) \cap b(M)).$$

Es bleibt zu zeigen, dass $\overline{W}_A(M) = 0$ ist. Man überlege sich das an einem Beispiel.

9. Normalreihen des Vergissfunktors

Zum Schluss wollen wir nochmals auf die im Laufe dieser Arbeit mehrfach benützten Unterfunktoren des Vergissfunktors V eingehen.

Wir betrachten hierzu das Kompaktum $K = \{0,2\}^{\mathbb{N}}$ versehen mit der lexikographischen Ordnung und veranschaulichen es mit Hilfe des bekannten Ordnungshomöomorphismus

$$\gamma : \ K \longrightarrow \mathcal{C} = \text{Cantorsches Diskontinuum}$$

gegeben durch $\quad (x_0,x_1,x_2,\ldots) \longmapsto \frac{x_0}{3} + \frac{x_1}{3^2} + \frac{x_2}{3^3} + \ldots$

Die Randpunkte von $\mathcal{C}$ sind die Bilder der konvergierenden Folgen, d.h. derjenigen Folgen, welche mit lauter Nullen oder lauter

Zweien enden.

Jeder konvergenten Folge D ordnen wir einen Unterfunktor DV von V zu :

$$DV(M) = D(M) = D(0) .$$

<u>Beispiele</u>: a) $D = (2,2,0,0,0,2,0,\overline{2}...)$

$$DV(M) = a^{-2}b^{3}a^{-1}ba^{-\infty}(M) = a^{-2}b^{3}a^{-1}ba^{-\infty}(0) = a^{-2}b^{3}a^{-1}b(M).$$

b) $D = (2,2,0,0,0,2,\overline{0}...)$

$$DV(M) = a^{-2}b^{3}a^{-1}b^{\infty}(M) = a^{-2}b^{3}a^{-1}b^{\infty}(0) = a^{-2}b^{3}a^{-1}(0).$$

Es ist leicht zu sehen, dass die Abbildung $D \longmapsto DV$ injektiv und ordnungstreu ist. Wir erhalten somit eine <u>total geordnete Untermenge der Unterfunktoren</u> von V. Sei $\mathcal{V}$ der durch diese Untermenge erzeugte <u>vollständige Verband</u>. Wir wollen $\mathcal{V}$ beschreiben.

Für jedes $D = (x_0,x_1,x_2,...) \in K$ setzen wir

$$D'_n = (x_0,x_1,..,x_{n-1},\overline{0}...) \quad , \quad D''_n = (x_0,x_1,..,x_{n-1},\overline{2}...).$$

Dann gilt

$$D'_n \leqslant D \leqslant D''_n \quad \text{und} \quad D'_n \longrightarrow D \ , \quad D''_n \longrightarrow D \quad \text{für } n \to \infty.$$

Setzen wir $D'V = \bigcup\limits_n D'_nV$ und $D''V = \bigcap\limits_n D''_nV$, so erhalten wir folgenden Satz:

<u>Satz</u>: <u>Die Elemente von</u> $\mathcal{V}$ <u>sind von folgender Art:</u>

1) DV <u>mit</u> D <u>konvergent</u>,
2) $D'V = D''V$ <u>mit</u> D <u>nicht-konvergent und nicht-periodisch</u>,
3) $D'V \subsetneqq D''V$ <u>mit</u> D <u>periodisch</u>, $D \neq (\overline{0}...), (\overline{2},...)$.

<u>Die Elemente von</u> $\mathcal{V}$ <u>mit einem Nachfolger sind dabei folgende:</u>

a) DV <u>mit</u> $D = (x_0,x_1,..,x_n,\overline{2}...)$, $D \neq (\overline{2}...)$,
b) $D'V$ <u>mit</u> D <u>wie in</u> 3).

<u>Die "Löcher" von</u> $\mathcal{V}$ <u>werden somit durch</u> a) <u>und</u> b) <u>beschrieben</u>!

Bemerkung: 1) $\mathfrak{V}$ überdeckt das Cantorsche Diskontinuum : Über jeder periodischen Cantorschen Zahl besitzt die Familie zwei Elemente. Dementsprechend hat $\mathfrak{V}$ mehr Löcher als $\mathfrak{C}$!

2) Die Rollen von a und b können vertauscht werden, und man erhält so einen weiteren vollständigen Verband von Unterfunktoren, welcher sich in analoger Weise beschreiben lässt.

Literaturverzeichnis

[GA] Demazure M. - Gabriel P. Groupes algébriques
Masson, North-Holland; Paris-Amsterdam (1970)

[PG] Demazure M. Lectures on p-Divisible Groups
Lecture Notes in Math. 302; Springer (1972)

[AV] Mumford D. Abelian Varieties
Oxford University Press; Bombay (1970)

[BA8] Bourbaki N. Algèbre VIII
Hermann; Paris (1958)

[1] Gelfand I.M. - Ponomarev V.A. Indecomposable representations of the Lorentz group Russ. Math. Surv. 23, 1-58

[2] Honda T. Isogeny Classes of Abelian Varieties over Finite Fields
J.Math.Soc. Japan 20 (1968) 83-95

[3] Kraft H. Kommutative algebraische Gruppen und Ringe
Lecture Notes in Math. 455; Springer (1975)

[4] Lenstra H.W. - Oort F. Simple Abelian Varieties Having a prescribed Formal Isogeny Type
J. pure appl. Algebra 4 (1974) , 47-53

[5] Manin Y. The Theory of Commutative Formal Groups over Fields of Finite Characteristic
Russian Math. Surveys 18 (1963), 1-81

[6] Oort F. Commutative Group Schemes
Lecture Notes in Math. 15; Springer (1966)

[7] - Subvarieties of Moduli Spaces
Invent. Math. 24 (1974), 95-119

[8] - Which Abelian Surfaces are Products of Elliptic Curves? Report 74-06 , University of Amsterdam

[9] Poletti M. Differenziali esatti di prima specie su varietà abeliane
Sc. Norm. Sup. Pisa 21 (1967), 107-116

[10] Raynaud M. Schêmas en groupes de type (p,..,p)
Bull. Soc. Math France 102 (1974), 241-280

[11] Serre J.P. Groupes p-divisibles (d'aprês J. Tate)
Sém. Bourbaki 318 (1966)

[12] Tate J. Classes d'isogénie des variétés abéliennes sur un corps fini (d'après T. Honda)
Sém. Bourbaki 352, Springer Lec. Notes 179 (1971)

[13] - Endomorphisms of Abelian Varieties over Finite Fields Invent. math. 2 (1966), 134-144

[14] Ringel C.M. The Indecomposable Representations of the Dihedral 2-Groups Math. Ann. 214 (1975), 19-34