Werk

Titel: Spezielle Algebren und transitive Operationen.

Autor: Pauer, Franz

Jahr: 1978

PURL: https://resolver.sub.uni-goettingen.de/purl?266833020_0160|log14

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

Math. Z. 160, 103–134 (1978)

Mathematische Zeitschrift
© by Springer-Verlag 1978

Spezielle Algebren und transitive Operationen

Franz Pauer

Institut für Mathematik, Universität Innsbruck, Innrain 52, A-6020 Innsbruck, Österreich

In der Literatur (z.B.: [3, 10–12, 14]) treten häufig Algebren der Form $k[X_1, \ldots, X_n]/\langle X_1^{p^{e_1}}, \ldots, X_n^{p^{e_n}}\rangle$ (und Verallgemeinerungen davon) auf. So haben etwa $\bar{k} \otimes l$, wenn $k \subset l$ eine rein inseparable Körpererweiterung und $\bar{k}$ der algebraische Abschluß von k ist [14], und das Zentroid einer differenzierbar einfachen Algebra [3] diese Gestalt. Ist k ein perfekter Körper, $\mathfrak{G}$ eine zusammenhängende affine algebraische Gruppe, $\mathfrak{G}'$ eine Untergruppe von $\mathfrak{G}$ und der Quotient $\mathfrak{G}/\mathfrak{G}'$ endlich, so ist die affine Algebra $A(\mathfrak{G}/\mathfrak{G}')$ ebenfalls von diesem Typ [7].

In dieser Arbeit soll ein Standpunkt gefunden werden, von dem aus sich all diese Ergebnisse einheitlich ableiten oder verallgemeinern lassen.

Alle auftretenden Ringe sind von der Charakteristik p, wobei p eine Primzahl ist. Statt p^e schreibe ich $p(e)$.

Im Kapitel 2 wird eine Klasse von endlichen, rein inseparablen Algebren charakterisiert. A sei eine endliche, rein inseparable Algebra. Für lokalen Grundring k ist das wesentlichste Ergebnis die Äquivalenz folgender Aussagen ((2.1.1), (2.1.9), (2.1.12)):

(1) $\forall\, m \in \mathbb{N}$ besitzt $A^{[m]} := k\,[A^{p(m)}]$ eine p-Basis.

(2) $\forall\, m \in \mathbb{N}$ ist der Differentialmodul $\Omega(A^{[m]}/k)$ von $A^{[m]}$ ein freier $A^{[m]}$-Modul.

(3) Es existieren Elemente $z_1, z_2, \ldots, z_r \in A$, $e_1, e_2, \ldots, e_r \in \mathbb{N}$ mit $e_1 \geqq e_2 \geqq \cdots \geqq e_r > 0$ und Polynome $P_i \in k\,[Z_1, \ldots, Z_{i-1}]$, so daß $A = k\,[z_1, \ldots, z_r]$ mit den Relationen $z_i^{p(e_i)} = P_i(z_1^{p(e_i)}, \ldots, z_{i-1}^{p(e_i)})$.

(4) Es gibt eine treuflache Ringerweiterung $k \subset l$, l lokal, und Elemente $z_1, z_2, \ldots, z_r \in A$, $e_1, e_2, \ldots, e_r \in \mathbb{N}$ mit $e_1 \geqq e_2 \geqq \cdots \geqq e_r > 0$, so daß $l \otimes A \cong l\,[z_1, \ldots, z_r]$ mit den Relationen $z_i^{p(e_i)} = 0$, $i = 1, \ldots, r$.

Eine Algebra über einem lokalen Ring, die (1)–(4) erfüllt, heißt *speziell*.

Für beliebigen Grundring wird die Äquivalenz folgender Aussagen bewiesen ((2.2.5), (2.2.9)):

(1) i) $k \subset A$ ist endlich präsentierbar.

ii) $\forall\, \mathfrak{m} \in \mathrm{Max}(k)$ ist $A_{\mathfrak{m}}$ speziell über $k_{\mathfrak{m}}$.

(2) $\forall\, m \in \mathbb{N}$ ist $\Omega(A^{[m]}/k)$ endlich projektiv.

0025-5874/78/0160/0103/$06.40

(3) Es existiert eine Zerlegung $k=k_1\times k_2\times\cdots\times k_n$ von k und für jedes i eine treuflache Ringerweiterung $k_i\subset l_i$, so daß $l_i\otimes A_i\cong l_i[z_1,\ldots,z_{r(i)}]$ mit den Relationen $z_j^{p^{(e_j(i))}}=0$, $e_1(i)\geqq\cdots\geqq e_{r(i)}>0$.

Eine Algebra, die (1)–(3) erfüllt, heißt *speziell.*

Ein Teil der Sätze von Kapitel 2 wurde bereits von Rasala in [14] für Algebren über einem Körper bewiesen. Neu ist neben der Verallgemeinerung auf Grundringe vor allem die Verwendung des Differentialmoduls zur Charakterisierung dieser Algebren.

Im Abschnitt 3.1 wird definiert, wann eine affine algebraische Gruppe auf einem endlichen affinen Schema „transitiv" operiert. Satz (3.1.6) charakterisiert solche transitiven Operationen. Besonders wichtig für das folgende ist, daß unter der Voraussetzung, daß $\mathfrak{Sp}\,S(k)$ nichtleer ist, eine Operation einer Gruppe $\mathfrak{G}$ auf $\mathfrak{Sp}\,S$ genau dann transitiv ist, wenn $\mathfrak{Sp}\,S$ zu einem homogenen Raum von $\mathfrak{G}$ isomorph ist. Dadurch wird es mit Hilfe des Satzes von Cartier-Dieudonné [7; III, 3, 6] möglich, die Begriffe „spezielle Algebra" und „transitive Operation" zu verbinden. Falls k Körper ist, gilt: Es gibt eine zusammenhängende Gruppe, die auf $\mathfrak{Sp}\,S$ transitiv operiert, genau dann, wenn die Algebra S speziell ist (3.2.5).

Ist S eine endlichdimensionale Algebra über einem Körper, so ist S endliches Produkt von lokalen Algebren ($S=\prod S_i$, S_i lokal). Mit S_{et} wird die größte étale Unteralgebra von S bezeichnet. Das Hauptergebnis dieser Arbeit ist die Äquivalenz der folgenden drei Aussagen (Satz (3.3.5)):

(1) Es gibt eine affine algebraische Gruppe, die auf $\mathfrak{Sp}\,S$ transitiv operiert.

(2) Jeder lokale Bestandteil S_i von S ist speziell über $(S_i)_{et}$, wobei die oben eingeführten Zahlen $e_1,\ldots,e_r$ von i unabhängig sind.

(3) $\forall\, m\in\mathbb{N}$ ist $\Omega(S^{[m]}/k)$ ein freier $S^{[m]}$-Modul.

Damit sind alle endlichen affinen Schemata (über einem Körper), auf denen eine algebraische affine Gruppe transitiv operiert, charakterisiert. Weiters wird dadurch der Satz von Cartier-Dieudonné verallgemeinert, da sich aus der Äquivalenz von (1) und (2) die Struktur der affinen Algebra jedes endlichen homogenen Raumes auch über nicht perfektem Grundkörper ableiten läßt.

Im Abschnitt (3.4) wird der Begriff der transitiven Operation für beliebigen Grundring definiert. Daraus ergibt sich eine Verallgemeinerung eines Satzes aus [12].

Im Kapitel 4 wird gezeigt, daß sich die Bestimmung des Zentroides einer differenzierbar einfachen Algebra (vgl. [3, 10]) als Spezialfall der Ergebnisse dieser Arbeit auffassen läßt.

Im Kapitel 5 wird für eine endliche Algebra S eine notwendige Bedingung angegeben, daß ${}^{\mathfrak{Aut}(S/k)}S=k$ (vgl. (1.1.3) und (1.2.3)).

Im Kapitel 1 sind die für das Verständnis dieser Arbeit nötigen Grundlagen über affine algebraische Gruppen zusammengestellt.

Die allgemeinen Vereinbarungen gelten in allen Kapiteln, die am Anfang eines Abschnittes getroffenen nur im jeweiligen Abschnitt.

Die vorliegende Arbeit war im wesentlichen meine Dissertation an der Universität Innsbruck (1975/76). Ich danke Herrn Professor U. Oberst für die Betreuung dieser Arbeit und für die vielen Ideen und eigenen Ergebnisse, die er mir zur Verfügung gestellt hat.

Allgemeine Vereinbarungen

Alle auftretenden Ringe sind von der Charakteristik p, wobei p eine Primzahl ist. Statt p^r wird immer $p(r)$ geschrieben.

Eine *endliche Algebra* ist eine Algebra, die als Modul endlich erzeugt ist. Von einer zu $k[Z_1, \ldots, Z_r]/\langle P_i; i \in I\rangle$ isomorphen Algebra $k[z_1, \ldots, z_r]$ sagt man, sie wird *von* $z_1, \ldots, z_r$ *erzeugt mit den Relationen* $P_i(z)=0$, $i \in I$.

Das Tensorprodukt über einem Ring k wird mit $\otimes_k$ oder $\otimes$ bezeichnet.

Eine k-Algebra A heißt *rein inseparabel*, wenn zu jedem $a \in A$ ein $m \in \mathbb{N}$ existiert, so daß $a^{p(m)} \in k$.

Ist $\mathscr{K}at$ eine Kategorie, so bedeutet „$K \in \mathscr{K}at$", daß K ein Objekt von $\mathscr{K}at$ ist.

Alle Limites und Colimites von k-Gruppen und k-Schemata werden in $\mathscr{S}cha_k$ gebildet.

Sind $\mathfrak{G}$ und $\mathfrak{H} \in \mathscr{S}cha_k$ und ist f ein Morphismus von $\mathfrak{G}$ nach $\mathfrak{H}$, so bedeutet

$$\begin{aligned} f\colon \mathfrak{G} &\to \mathfrak{H} \\ s &\mapsto f(s) \end{aligned}$$

immer: $\forall\, R \in \mathscr{A}\ell_k$, $\forall\, s \in \mathfrak{G}(R)$,

$$\begin{aligned} f_R\colon \mathfrak{G}(R) &\to \mathfrak{H}(R) \\ s &\mapsto f_R(s). \end{aligned}$$

Sind $A, B, C \in \mathscr{A}\ell_k$ und $g\colon A \to B \otimes C$, so wird oft

$$g(a)=\sum_{(a)} a_1 \otimes a_2 \quad \text{oder} \quad g(a)=\sum_{(a)} b \otimes c$$

geschrieben. (Diese Darstellung ist nicht eindeutig.)

$A \underset{k}{|} B$ bedeutet: A ist k-direkter Summand von B. $\square$ steht am Ende eines Beweises.

Abkürzungen

$\mathscr{A}\ell_k$	Kategorie der kommutativen k-Algebren
$\mathscr{A}\ell f_k$	Kategorie der endlichen Algebren in $\mathscr{A}\ell_k$
$\mathscr{A}\ell ff_k$	Kategorie der freien Algebren in $\mathscr{A}\ell f_k$
EZS	Erzeugendensystem
$J(k)$	Jacobsonradikal von k
KE	Körpererweiterung
$\mathrm{Max}(k)$	Menge der maximalen Ideale von k
$\mathscr{M}e$	Kategorie der Mengen
o.E.d.A.	ohne Einschränkung der Allgemeinheit
$\Omega(A/k)$	Differentialmodul von A über k
$\mathscr{R}i$	Kategorie der Ringe
$\mathscr{S}cha_k$	Kategorie der affinen algebraischen Schemata über k (kurz: k-Schemata)

1. Grundbegriffe

Ich halte mich im wesentlichen an die Terminologie von [7].

1.1. Affine algebraische Gruppen

Es sei $k \in \mathscr{R}i$.

(1.1.1) Unter einem *k-Schema* $\mathfrak{X}$ verstehe ich ein affines, algebraisches k-Schema. Die affine Algebra von $\mathfrak{X}$ wird mit $A(\mathfrak{X})$ bezeichnet. $\mathfrak{X}$ heißt *endlich*, wenn $A(\mathfrak{X})$ als Modul endlich erzeugt ist.
Es gilt die bekannte Dualität

$$\begin{aligned} \mathfrak{Sp}\colon \mathscr{A}\ell_k &\to \mathscr{S}cha_k & \qquad A\colon \mathscr{S}cha_k &\to \mathscr{A}\ell_k \\ A &\mapsto \mathfrak{Sp}\,A = \mathscr{A}\ell_k(A, -) & \mathfrak{X} &\mapsto A(\mathfrak{X}). \end{aligned}$$

Der funktorielle Isomorphismus $\mathscr{A}\ell_k(A(\mathfrak{X}), -) \cong \mathfrak{X}$ ist durch ein universelles Element $x_0 \in \mathfrak{X}(A(\mathfrak{X}))$ gegeben in der Form

$$\begin{aligned} \mathscr{A}\ell_k(A(\mathfrak{X}), R) &\cong \mathfrak{X}(R) \\ f &\mapsto \mathfrak{X}(f)(x_0) \end{aligned}$$

und wird mit $x_0^{\#}$ bezeichnet.

(1.1.2) Eine *k-Gruppe* $\mathfrak{G}$ bzw. $(\mathfrak{G}, \mu, \eta, \tau)$ ist eine Gruppe in der Kategorie $\mathscr{S}cha_k$. Dabei ist μ die Multiplikation, η das Einselement und τ der Inversionsmorphismus.

Einer k-Gruppe $(\mathfrak{G}, \mu, \eta, \tau)$ entspricht bezüglich der in (1.1.1) angegebenen Dualität die kommutative Hopfalgebra (vgl. [16]) $A(\mathfrak{G}) = (A(\mathfrak{G}), \Delta, \varepsilon, \sigma)$, Δ ist die Comultiplikation, ε die Augmentation und σ die Antipode.

Ist $x_0 \in \mathfrak{G}(A(\mathfrak{G}))$ ein universelles Element und ist u_1 bzw. u_2 gegeben durch $u_1(a) = a \otimes 1$ bzw. $u_2(a) = 1 \otimes a$, so sind Δ, ε, σ eindeutig bestimmt durch

$$\begin{aligned} G(\Delta)(x_0) &= \mu_{A \otimes A}(G(u_1)(x_0), G(u_2)(x_0)) \\ G(\varepsilon)(x_0) &= \eta_k(1) \\ G(\sigma)(x_0) &= \tau_A(x_0). \end{aligned}$$

(1.1.3) *Die Automorphismengruppe* [7; II, 1, 2.6]. A sei eine beliebige endlich projektive k-Algebra. Dann ist der Funktor

$$\begin{tikzcd} \mathfrak{Aut}(B/k)\colon \mathscr{A}\ell_k \arrow[r] & \mathscr{M}e \\ R \arrow[r, mapsto] \arrow[d] & \mathrm{Aut}(B \otimes_k R/R) \arrow[d] & f \arrow[d, mapsto] \\ R' \arrow[r, mapsto] & \mathrm{Aut}(B \otimes_k R'/R') & f \otimes_R R' \end{tikzcd}$$

eine k-Gruppe.

(1.1.4) *Grundringerweiterung* [7; I, 1, 6.5]. $f\colon k \to l$ sei ein Ringhomomorphismus und $\mathfrak{X}$ ein k-Schema. Man erhält das l-Schema

$$\begin{aligned} l\otimes\mathfrak{X}\colon \mathscr{A}\ell_l &\to \mathscr{M}e \\ R &\mapsto X({}_kR), \end{aligned}$$

wobei ${}_kR$ als Ring mit R übereinstimmt und vermöge f als k-Modul aufgefaßt wird. Es gilt: $l\otimes A(\mathfrak{X}) = A(l\otimes\mathfrak{X})$.

1.2. Operationen von k-Gruppen auf k-Schemata

(1.2.1) Eine *Operation* $Op\colon \mathfrak{X}\times\mathfrak{G}\to\mathfrak{X}$ einer k-Gruppe $\mathfrak{G}$ auf einem k-Schema $\mathfrak{X} = \mathfrak{Sp}\,S$ wird durch Operationen $Op_R\colon \mathfrak{X}(R)\times\mathfrak{G}(R)\to\mathfrak{X}(R)$ der abstrakten Gruppen $\mathfrak{G}(R)$ auf den Mengen $\mathfrak{X}(R)$, funktoriell in $R\in\mathscr{A}\ell_k$, gegeben. Dazu äquivalente Daten sind ein Morphismus von k-Gruppen $\rho\colon \mathfrak{G}\to\mathfrak{Aut}(S/k)$ oder ein Algebrenhomomorphismus $\Delta\colon S\to S\otimes A(\mathfrak{G})$, der S zu einem $A(\mathfrak{G})$-Comodul macht. Der Zusammenhang zwischen diesen Daten ist durch $Op = \mathfrak{Sp}(\Delta)$ und die durch $R\in\mathscr{A}\ell_k$ und $f\in\mathfrak{G}(R)$ indizierte Familie von kommutativen Diagrammen

$$\begin{tikzcd} S \arrow[r, "\Delta"] \arrow[dr, hook, "\mathrm{Inj}"'] & S\otimes A(\mathfrak{G}) \arrow[r, "S\otimes(x_R^{\#})^{-1}(f)"] & S\otimes R \\ & S\otimes R \arrow[ur, "\rho_R(f)"'] & \end{tikzcd}$$

gegeben.

(1.2.2) $\mathfrak{G}$ sei eine endlich projektive k-Gruppe, $A := A(\mathfrak{G})$ und $H := \mathrm{Hom}_k(A, k)$. Durch dualisieren wird H zu einer cokommutativen Hopfalgebra, die Coeinheit sei $\varepsilon_H\colon H\to k$ und die Comultiplikation

$$\begin{aligned} \Delta_H\colon H &\to H\otimes H \\ h &\mapsto \sum_{(h)} h_1\otimes h_2. \end{aligned}$$

$\mathfrak{Sp}\,S$ sei ein k-Schema und durch

$$\begin{aligned} \Delta\colon S &\to S\otimes A \\ s &\mapsto \sum_{(s)} s_1\otimes s_2 \end{aligned}$$

sei eine Operation von $\mathfrak{G}$ auf $\mathfrak{Sp}\,S$ gegeben. Dann entspricht Δ eindeutig der durch die Hintereinanderausführung der Abbildungen

$$\begin{tikzcd} H\otimes S \arrow[r, "H\otimes\Delta"] & H\otimes S\otimes A \arrow[r] & S \\ h\otimes s \arrow[r, mapsto] & h\otimes\sum_{(s)} s_1\otimes s_2 \arrow[r, mapsto] & \sum_{(s)} s_1\, h(s_2) \end{tikzcd}$$

gegebenen H-Modulstruktur $\mu\colon H\otimes S\to S$, die die folgenden Bedingungen erfüllt:

$$\mu(h\otimes 1)=\varepsilon_H(h),\qquad \forall\, h\in H,$$
$$\mu(h\otimes st)=\sum_{(h)}\mu(h_1\otimes s)\,\mu(h_2\otimes t),\qquad \forall\, h\in H,\ \forall\, s,\ t\in S.$$

(1.2.3) $\mathfrak{X}=\mathfrak{Sp}\,S$ sei ein k-Schema, $\mathfrak{G}$ eine k-Gruppe und $Op\colon \mathfrak{X}\times\mathfrak{G}\to\mathfrak{X}$ eine Operation.

Der Cokern (in $\mathscr{Sch}_k$) von $\mathfrak{X}\times\mathfrak{G}\underset{\text{proj}}{\overset{Op}{\rightrightarrows}}\mathfrak{X}$ wird mit $\mathfrak{X}/\mathfrak{G}$ bezeichnet.

Die Algebra $A(\mathfrak{X}/\mathfrak{G})$ wird mit ${}^{\mathfrak{G}}S$ bezeichnet und ist der Kern (in $\mathscr{A}\ell_k$) von $S\underset{\text{inj}}{\overset{\Delta}{\rightrightarrows}}S\otimes A$, also ${}^{\mathfrak{G}}S=\{x\in S/\Delta(x)=x\otimes 1\}$. k sei ein Körper, $\mathfrak{G}'$ eine k-Untergruppe von $\mathfrak{G}$ und $Op\colon \mathfrak{G}\times\mathfrak{G}'\to\mathfrak{G}$ die Einschränkung der Gruppenmultiplikation auf $\mathfrak{G}\times\mathfrak{G}'$. Ist der Cokern $\mathfrak{G}/\mathfrak{G}'$ endlich, so stimmt er mit dem in [7] definierten Quotienten von k-Gruppen überein. $\mathfrak{G}/\mathfrak{G}'$ wird dann *homogener Raum* genannt.

(1.2.4) k sei ein Körper, $\mathfrak{X}=\mathfrak{Sp}\,S$ ein k-Schema, $x\in\mathfrak{X}(k)$, $\mathfrak{G}$ eine k-Gruppe und $Op\colon \mathfrak{X}\times\mathfrak{G}\to\mathfrak{X}$ eine Operation.

Durch $\mathfrak{G}_x(R):=\{s\in\mathfrak{G}(R)/Op_R(x_R,s)=x_R\}$, $\forall\, R\in\mathscr{A}\ell_k$, ist eine Untergruppe $\mathfrak{G}_x$ von $\mathfrak{G}$ definiert. (Dabei ist x_R die Zusammensetzung von x mit der Strukturabbildung von k nach R.) Der Morphismus

$$\mathfrak{G}\to\mathfrak{X}$$
$$s\mapsto Op_R(x_R,s)$$

kann in $\mathfrak{G}\xrightarrow{\text{kan}}\mathfrak{G}/\mathfrak{G}_x\xrightarrow{\text{i}}\mathfrak{X}$ zerlegt werden. Ist $\mathfrak{X}$ ein endliches k-Schema, so ist auch $\mathfrak{G}/\mathfrak{G}_x$ endlich und i ist eine abgeschlossene Einbettung, d.h.: $A(i)$ ist surjektiv. [7; III, 3, 1.6 und III, 3, 5.2].

1.3. Zusammenhängende und étale k-Schemata

k sei ein Körper, $\mathfrak{X}$ ein k-Schema und $x\in\mathfrak{X}(k)$.

(1.3.1) Eine k-Algebra A ist „étale" genau dann, wenn A endlich und Produkt von separablen KE von k ist. Ist $A\in\mathscr{A}\ell_k$ als Algebra endlich erzeugt, so existiert eine größte étale Unteralgebra A_{et} von A.

$\mathfrak{X}$ heißt *étale*, wenn $A(\mathfrak{X})$ étale ist.

Zu $\mathfrak{X}$ existiert ein étales k-Schema $\mathfrak{X}_{et}$ und ein Morphismus $p_{et}\colon \mathfrak{X}\to\mathfrak{X}_{et}$ mit der universellen Eigenschaft: Zu jedem Morphismus $f\colon \mathfrak{X}\to\mathfrak{Y}$ in ein étales k-Schema $\mathfrak{Y}$ existiert genau ein Morphismus $g\colon \mathfrak{X}_{et}\to\mathfrak{Y}$, so daß $g\,p_{et}=f$. [7; I, 4, 6.5]. Es ist $A(\mathfrak{X}_{et})=A(\mathfrak{X})_{et}$.

(1.3.2) Das Faserprodukt $\mathfrak{X}\times_{\mathfrak{X}_{et}}1$ des Diagrammes $\mathfrak{X}\xrightarrow[p_{et}]{}\mathfrak{X}_{et}\xleftarrow[p_{et}x^{\#}]{}1$ wird mit $\mathfrak{X}_0$ bezeichnet.

$\mathfrak{X}$ heißt *zusammenhängend*, wenn $A(\mathfrak{X})$ unzerlegbar ist.

Ist $\mathfrak{X}$ endlich, so ist $\mathfrak{X}$ zusammenhängend genau dann, wenn $\mathfrak{X}=\mathfrak{X}_0$.

Ist $\mathfrak{G}$ eine k-Gruppe und $x^{\#}=\eta$ das Einselement, so ist $\mathfrak{G}_{et}$ eine endliche k-Gruppe, $\mathfrak{G}_0$ Normalteiler von $\mathfrak{G}$ und die Folge $1\to\mathfrak{G}_0\to\mathfrak{G}\to\mathfrak{G}_{et}\to 1$ ist exakt [7; II, 5, 1.8].

Ist $\mathfrak{X}$ ein endlicher homogener Raum und k algebraisch abgeschlossen, so ist $\mathfrak{X}\cong\mathfrak{X}_{et}\times\mathfrak{X}_0$.

(1.3.3) $A(\mathfrak{X})^+$ sei der Kern von x und $A(\mathfrak{X})^{+(r)}$ das Ideal, das von der Menge $\{a^{p(r)}/a\in A(\mathfrak{X})^+\}$ in $A(\mathfrak{X})$ erzeugt wird. Dann ist das endliche k-Unterschema $\mathfrak{X}_{(r)}\leqq\mathfrak{X}_0$ durch $A(\mathfrak{X}_{(r)})=A(\mathfrak{X})/A(\mathfrak{X})^{+(r)}$ definiert.

$\mathfrak{X}$ heißt *von der Höhe r*, falls $\mathfrak{X}=\mathfrak{X}_{(r)}$.

Ist $\mathfrak{X}$ ein k-Monoid und $\mathfrak{X}^*$ die größte in $\mathfrak{X}$ enthaltene Untergruppe, so ist $\mathfrak{X}_{(r)}=\mathfrak{X}^*_{(r)}$.

2. Spezielle Algebren

Es sei $k\in\mathscr{R}i$, $A\in\mathscr{A}l\mathscr{g}_k$ und $k\subset A$. Mit $A^{[m]}$ wird die Algebra $k[A^{p(m)}]=\{\sum\alpha_i a_i^{p(m)}/\alpha_i\in k, a_i\in A\}$ bezeichnet. Für einen flachen Ringhomomorphismus $k\to l$ gilt $l\otimes A^{[m]}=(l\otimes A)^{[m]}$, insbesondere ergibt sich für $l=k_{\mathfrak{m}}$, $\mathfrak{m}\in\mathrm{Max}(k)$: $A^{[m]}_{\mathfrak{m}}=(A^{[m]})_{\mathfrak{m}}$.

Ist k lokal und M ein endlich erzeugter k-Modul, so sei $[M:k]$ die Anzahl der Elemente eines minimalen EZS von M. (Bekanntlich hängt diese von der Wahl des EZS nicht ab.) $\Omega(A/k)$ sei der Differentialmodul von A und $d\colon A\to\Omega(A/k)$ die zugehörige universelle Derivation.

Für $A=k[z_1,\dots,z_r]$ mit den Relationen $P_i(z)=0$, $i\in I$, gilt:

$$\Omega(A/k)=\sum_{i=1}^{r}A\,dz_i \quad\text{mit den Relationen}\quad \sum_j\frac{\partial P_i}{\partial Z_j}(z)\,dz_j=0,\ i\in I.$$

Die in [9; 0, 20] angegebenen Eigenschaften von $\Omega(A/k)$ werden im folgenden ohne weiteren Hinweis verwendet.

Eine Menge $\{z_1,\dots,z_r\}\subset A$ heißt *p-Basis* (p-EZS) von A genau dann, wenn $\{z_1^{n_1}z_2^{n_2}\dots z_r^{n_r}/0\leqq n_i<p,\forall i\}$ eine $A^{[1]}$-Basis ($A^{[1]}-$EZS) von A ist [9; 0, 21.1.9].

2.1. *Spezielle Algebren über lokalen Ringen*

A sei rein inseparabel und $\exp(A/k):=\min\{m\in\mathbb{N}/A^{[m]}=k\}$.

(2.1.1) **Satz.** *Die folgenden Aussagen sind äquivalent:*

(1) $\forall\, m\in\mathbb{N}$ *besitzt* $A^{[m]}$ *eine p-Basis.*

(2) $\forall\, m\in\mathbb{N}$ *ist* $\Omega(A^{[m]}/k)$ $A^{[m]}$*-frei.*

Falls k lokal ist:

(3) $k\subset A$ *ist frei und* $[A:k]=p\left(\sum_{m=0}^{s}d(m)\right)$, *dabei ist* $s:=\exp(A/k)-1$ *und* $d(m):=[\Omega(A^{[m]}/k)\colon A^{[m]}]$.

Beweis. (1) $\Rightarrow$ (2): [9; 0, 21.2.5].

(2) $\Rightarrow$ (1): Induktion über $\exp(A/k)$

1) $\exp(A/k)=1$: $\{dz_1, \ldots, dz_r\}$ sei eine A-Basis von $\Omega(A/k)$. Nach [9; 0, 21.1.7] ist dann $\{z_1, \ldots, z_r\}$ ein p-EZS von A. Zeige: $\{z^m/m\in\mathbb{N}^r, 0\leqq m_i<p, \forall i\}$ ist linear unabhängig. Annahme: $0\neq P\in k[Z_1, \ldots, Z_r]$ sei ein Polynom minimalen Grades mit den Eigenschaften $P(z):=P(z_1, \ldots, z_r)=0$ und $\operatorname{grad}_{Z_i}(P)<p$, $i=1, \ldots, r$.

Aus $0=d(P(z))=\sum_i \frac{\partial P}{\partial Z_i}(z)\,dz_i$ folgt, daß $\frac{\partial P}{\partial Z_i}(z)=0$. Da der Grad der Polynome $\frac{\partial P}{\partial Z_i}$ kleiner als der Grad von P ist, folgt $\frac{\partial P}{\partial Z_i}=0$. Wegen $\operatorname{grad}_{Z_i}(P)<p$ ist dann $P\in k$. Also ist $P(z)\neq 0$ oder $P=0$. Widerspruch.

2) $\exp(A/k)>1$: Wegen $\Omega(A/k)=\Omega(A/A^{[1]})$ [9; 0, 21.1.5] und $\exp(A/A^{[1]})=1$ besitzt A nach 1) eine p-Basis. Nach Induktionsannahme besitzen die $A^{[m]}$ p-Basen, $\forall m\geqq 1$.

(1), (2) $\Rightarrow$ (3): Klar.
(3) $\Rightarrow$ (1): $\{d(z_{mi})/i=1, \ldots, d(m)\}$ sei ein minimales EZS von $\Omega(A^{[m]}/k)$. Nach [9; 0, 21.1.7] ist $\{z_{mi}/i=1, \ldots, d(m)\}$ ein p-EZS von $A^{[m]}$, d.h.: $A^{[m]}=\sum_{l\in I_m} A^{[m+1]} z_m^l$, dabei ist

$$z_m^l := z_{m1}^{l_1} z_{m2}^{l_2} \ldots z_{md(m)}^{l_{d(m)}} \quad \text{und} \quad I_m := \{l\in\mathbb{N}^{d(m)}/0\leqq l_i<p, \forall i\}.$$

Induktiv ergibt sich:

$$A=A^{[0]}=\sum_{m=0}^{s} \sum_{l(m)\in I_m} k z_0^{l(0)} \ldots z_s^{l(s)} = \sum_{l\in I} k z^l, \quad I:=I_0 x \ldots x I_s,$$

$$|I|=|I_0|\,|I_1| \ldots |I_s|=p\left(\sum_{m=0}^{s} d(m)\right).$$

Nach Voraussetzung ist $k\subset A$ frei mit der Dimension $|I|$, also ist $\{z^l/l\in I\}$ eine k-Basis von A. Daraus folgt leicht, daß auch $\{z_m^{l(m)}/l(m)\in I_m\}$ eine $A^{[m+1]}$-Basis von $A^{[m]}$ ist, $m\in\mathbb{N}$. Also ist $\{z_{mi}/i=1, \ldots, d(m)\}$ eine p-Basis von $A^{[m]}$, $m\in\mathbb{N}$. □

(2.1.2) *Bemerkung.* In [11; Satz 5 und Satz 6] wird der obige Satz für den Fall $\exp(A/k)=1$ bewiesen.

(2.1.3) **Definition.** Eine rein inseparable, endliche Algebra A über einem lokalen Ring k mit $k\subset A$ heißt *speziell* über k (vgl. [14]) genau dann, wenn eine der äquivalenten Aussagen von Satz (2.2.1) erfüllt ist.

(2.1.4) *Folgerung. Ist $K\subset L$ eine rein inseparable, endliche* KE, *so ist L speziell über K.*

Beweis: $\Omega(L^{[m]}/K)$ ist $L^{[m]}$-frei, da $L^{[m]}$ Körper ist. □

(2.1.5) **Definition.** Es sei $\{z_1, \ldots, z_r\}\subset A$.

Die Folge $z_1, \ldots, z_r$ heißt *NGS* (normal generating sequence, [14]) genau dann, wenn es Zahlen $e_1, \ldots, e_r\in\mathbb{N}$ mit $e_1\geqq e_2\geqq \cdots \geqq e_r>0$ und Polynome $P_i\in k[Z_1, \ldots, Z_{i-1}]$, $i=1, \ldots, r$, gibt, so daß $A=k[z_1, \ldots, z_r]$ mit den Relationen $z_i^{p(e_i)}=P_i(z_1^{p(e_i)}, \ldots, z_{i-1}^{p(e_i)})$.

(2.1.6) **Satz.** *$z_1, \ldots, z_r$ sei eine* NGS *von A.*

$$d(m) := \max\{j/e_j > m, j = 1, \ldots, r\}, \qquad 0 \leqq m < e_1.$$

Dann gilt:

1) *$\forall m$ ist $z_1^{p(m)}, \ldots, z_{d(m)}^{p(m)}$ eine* NGS *von $A^{[m]}$.*

2) *$\forall m$ ist $\Omega(A^{[m]}/k)$ $A^{[m]}$ – frei mit der Dimension $d(m)$. Insbesondere sind die Zahlen $e_1, \ldots, e_r$ nur von A abhängig, nicht von der ausgewählten* NGS *$z_1, \ldots, z_r$.*

Beweis. 1) Es genügt zu zeigen: $z_1^p, \ldots, z_{d(1)}^p$ ist eine NGS von $A^{[1]}$. $A = k[z_1, \ldots, z_r]$ mit den Relationen $z_i^{p(e_i)} = P_i(z_1^{p(e_1)}, \ldots, z_{i-1}^{p(e_i)})$. Also ist $A^{[1]} = k[z_1^p, \ldots, z_{d(1)}^p]$ und mindestens die Relationen $(z_i^p)^{p(e_i-1)} = P_i((z_1^p)^{p(e_i-1)}, \ldots, (z_{i-1}^p)^{p(e_i-1)})$ sind erfüllt, d.h.: die Abbildung

$$\begin{aligned} f\colon k[Z_1, \ldots, Z_{d(1)}]/\langle Z_i^{p(e_i-1)} - P_i(Z^{P(e_i-1)}), i\rangle &\to A^{[1]} \\ \bar{Z}_i \qquad &\longmapsto z_i^p \end{aligned}$$

ist ein surjektiver Algebrenhomomorphismus.

$$A = \sum_{n \in I} A^{[1]} z^n, \qquad I := \{n \in \mathbb{N}^r / n_j < p, \forall j\}$$

und

$$A^{[1]} = \sum_{l \in J} k z^{lp}, \qquad J := \{l \in \mathbb{N}^{d(1)} / l_j < p(e_j - 1), \forall j\},$$

also ist

$$A = \sum_{n \in I} \Big(\sum_{l \in J} k z^{lp}\Big) z^n = \sum_{l,n} k z^{lp+n}.$$

($J \subset \mathbb{N}^r$ durch Identifikation von $(l_1, \ldots, l_{d(1)})$ mit $(l_1, \ldots, l_{d(1)}, 0, \ldots, 0)$.)

Andererseits ist $\{z^{lp+n}/(n, l) \in I \times J\}$ eine k-Basis von A. Daher ist $A^{[1]}$ k-frei mit der Basis $\{z^{pl}/l \in J\}$, $[A^{[1]}\colon k] = |J| = p\left(\sum_{j=1}^{d(1)} e_j - d(1)\right)$.

Somit haben Bild und Urbild von f die gleiche Dimension. f ist also ein Isomorphismus, d.h.: $z_1^p, \ldots, z_{d(1)}^p$ ist eine NGS von $A^{[1]}$.

2) Wegen 1) genügt es, die Behauptung für $m = 0$ zu zeigen. $\Omega(A/k)$ ist aber frei mit der Basis $\{dz_1, \ldots, dz_r\}$ und $r = d(0)$. $e_i = m$, falls $d(m) + 1 \leqq i \leqq d(m-1)$, also sind die e_i durch die Dimensionen der $\Omega(A^{[m]}/k)$ eindeutig bestimmt. □

Von jetzt ab sei k immer ein lokaler Ring und $d(m) := [\Omega(A^{[m]}/k)\colon A^{[m]}]$.

(2.1.7) **Satz.** *A werde als Algebra von einer Teilmenge M erzeugt. Dann existieren Elemente $z_1, \ldots, z_{d(0)} \in M$ derart, daß für jedes m die Mengen $\{d(z_i^{p(m)})/i = 1, \ldots, d(m)\}$ ein minimales $A^{[m]}$-EZS von $\Omega(A^{[m]}/k)$ bilden.*

Beweis. Induktion nach $\exp(A/k)$, $\exp(A/k) = 0$: $k = A$, $\exp(A/k) > 0$: 1) $A = k[M]$, daher ist $A^{[1]} = k[M^p]$ und $[\Omega(A^{[1][m]}/k)\colon A^{[1][m]}] = d(m+1)$. Nach Induktionsannahme gibt es Elemente $y_1 = z_1^p, \ldots, y_{d(1)} = z_{d(1)}^p \in M^p$ mit: $\forall m \in \mathbb{N}$ ist $\{d(y_i^{p(m)})/i = 1, \ldots, d(m)\}$ ein minimales EZS von $\Omega(A^{[1][m]}/k)$. Für $n \geqq 1$ ist daher $\{d(z_i^{p(n)})/i = 1, \ldots, d(n)\}$ ein minimales EZS von $\Omega(A^{[n]}/k)$.

2) Die Abbildung

$$(-)^p\colon A \to A^{[1]}$$
$$a \mapsto a^p$$

ist ein lokaler Ringhomomorphismus, auf diese Weise kann $\Omega(A^{[1]}/k)$ auch als A-Modul betrachtet werden. Dann ist die Abbildung

$$d\cdot(-)^p\colon A \to \Omega(A^{[1]}/k)$$
$$z \mapsto d(z^p)$$

eine k-Derivation. Daher gibt es genau eine A-lineare Abbildung f, so daß das Diagramm

$$\begin{tikzcd}
A \arrow[r, "d"] \arrow[dr, "d\cdot(-)^p"'] & \Omega(A/k) \arrow[d, "f"] & d(a) \arrow[d, mapsto] \\
& \Omega(A^{[1]}/k) & d(a^p)
\end{tikzcd}$$

kommutativ ist. Durch Skalarenerweiterung bezüglich $(-)^p\colon A \to A^{[1]}$ läßt sich die A-lineare Abbildung f eindeutig zu der $A^{[1]}$-linearen Abbildung

$$g\colon A^{[1]} \underset{A}{\otimes} \Omega(A/k) \to \Omega(A^{[1]}/k)$$
$$1 \otimes dz_i \mapsto d(z_i^p)$$

fortsetzen. Wegen $A^{[1]} = k[A^p]$ und $\Omega(A^{[1]}/k) = {}_{A^{[1]}}\langle d(A^{[1]})\rangle$ ist g surjektiv.

3) $(-)^p\colon A \to A^{[1]}$ ist lokal, g ist surjektiv und $\{d(z_1^p), \ldots, d(z_{d(1)}^p)\}$ ist ein minimales EZS von $\Omega(A^{[1]}/k)$. Also kann mit Hilfe des Lemmas von Nakayama gezeigt werden, daß Elemente $z_{d(1)+1}, \ldots, z_{d(0)}$ in M existieren, so daß $d(z_1), \ldots, d(z_{d(0)})$ ein minimales EZS von $\Omega(A/k)$ ist. □

(2.1.8) **Definition.** Die Folge $z_1, \ldots, z_{d(0)}$ mit den im Satz (2.1.7) angegebenen Eigenschaften heißt *GNGS* (generalized normal generating sequence) von A.

(2.1.9) **Satz.** *Die folgenden Aussagen sind äquivalent:*

(1) *A ist speziell über k.*

(2) *Jede* GNGS *von A ist eine* NGS *von A.*

(3) *Aus jeder Teilmenge M von A, die A als Algebra erzeugt, kann eine* NGS *ausgewählt werden.*

Beweis. (1) ⇒ (2): Induktion nach $\exp(A/k)$

$\exp(A/k) = 0$: $A = k$,

$\exp(A/k) > 0$: Sei $z_1, \ldots, z_{d(0)}$ GNGS, $r := d(0)$.

Dann ist $z_1^p, \ldots, z_{d(1)}^p$ eine GNGS von $A^{[1]}$. Nach Induktionsannahme ist $z_1^p, \ldots, z_{d(1)}^p$ NGS von $A^{[1]}$, d.h.: $A^{[1]} = k[z_1^p, \ldots, z_{d(1)}^p]$ mit den Relationen

$$(z_i^p)^{p(f_i)} = P_i((z_1^p)^{p(f_i)}, \ldots, (z_{i-1}^p)^{p(f_i)}).$$

Setze

$$e_i := \begin{cases} f_i + 1 & \text{falls } 1 \leqq i \leqq d(1) \\ 1 & \text{falls } d(1) < i \leqq d(0), \end{cases}$$

Für $d(1) < i \leqq d(0)$ gilt: $z_i^p \in A^{[1]}$, d.h.: $z_i^p = P_i(z_1^p, \ldots, z_{d(1)}^p)$, $P_i \in k[Z_1, \ldots, Z_{d(1)}]$.

Daher ist die Abbildung

$$\begin{aligned} f\colon k[Z_1, \ldots, Z_r]/\langle Z_i^{p(e_i)} - P_i(Z_1^{p(e_i)}, \ldots, Z_{i-1}^{p(e_i)});\ i \in \{1, \ldots, r\}\rangle &\to A \\ \bar{Z}_i &\longmapsto z_i \end{aligned}$$

wohldefiniert und surjektiv.

Beide Seiten sind frei und von gleicher Dimension, weil: $[A\colon A^{[1]}] = p(r)$ (*Satz* (2.1.1))

$$\begin{aligned} [A\colon k] = [A\colon A^{[1]}][A^{[1]}\colon k] &= p(r) \cdot p\left(\sum_{i=1}^{d(1)} f_i\right) = p\left(r + \sum_{i=1}^{d(1)} e_i - d(1)\right) \\ &= p\left(\sum_{i=1}^{r} e_i\right). \end{aligned}$$

Daher ist f Isomorphismus, also $z_1, \ldots, z_r$ NGS.

(2) $\Rightarrow$ (3): Nach Satz (2.1.7) ist in M eine GNGS enthalten, diese ist nach Voraussetzung eine NGS.
(3) $\Rightarrow$ (1): Klar. □

(2.1.10) *Bemerkung.* Die Eigenschaft „speziell" ist im allgemeinen nicht transitiv, d.h.: Aus „A ist speziell über k" und „B ist speziell über A" folgt nicht „B ist speziell über k".

Gegenbeispiel. k sei ein Körper, $k \subset A := k(\alpha)$ eine rein inseparable KE mit $\alpha^p \in k \setminus k^p$ und $B := A[z_1, z_2]$, $z_1^{p(2)} = 0$, $z_2^p = \alpha z_1^p$.

A ist speziell über k, B ist speziell über A. $B = k[\alpha, z_1, z_2]$ mit den Relationen $\alpha^p \in k$, $z_1^{p(2)} = 0$, $z_2^p = \alpha z_1^p$. B ist nicht speziell über k, da z_1, z_2, α zwar eine GNGS, aber keine NGS von B über k ist.

(2.1.11) **Hilfssatz.** *$k \subset l$ sei treuflach und l lokal. Dann sind folgende Aussagen äquivalent:*

(1) *A ist speziell über k.*

(2) *$l \otimes A$ ist speziell über l.*

Beweis. Da $k \subset l$ treuflach ist, ist $k \subset A$ endlich und rein inseparabel genau dann, wenn $l \subset l \otimes A$ endlich und rein inseparabel ist.

Nach [5; I, 3, 6, Prop. 12] ist $\Omega(l \underset{k}{\otimes} A/l) \cong (l \underset{k}{\otimes} A) \underset{A}{\otimes} \Omega(A/k)$ genau dann $l \otimes A$-frei, wenn $\Omega(A/k)$ A-frei ist. □

(2.1.12) **Satz.** *Die folgenden Aussagen sind äquivalent:*

(1) *A ist speziell über k.*

(2) *Es gibt eine treuflache Ringerweiterung $k \subset l$, l lokal, und eine* NGS $z_1, \ldots, z_r \in A$ *derart, daß $l \otimes A \cong l[z_1, \ldots, z_r]$ mit den Relationen $z_i^{p(e_i)} = 0$, $i = 1, \ldots, r$.*

(3) i) *$k \subset A$ ist frei.*

ii) $\forall m \in \mathbb{N}$ *gilt:* $A^{[m]} \underset{k}{|} A$.

iii) $k/J(k) \otimes A$ *ist speziell über* $k/J(k)$.

Falls k perfekt ist:

(4) *Es gibt eine* NGS $z_1, \ldots, z_r \in A$ *derart, daß* $A = k[z_1, \ldots, z_r]$ *mit den Relationen* $z_i^{p(e_i)} = 0$, $i = 1, \ldots, r$.

Beweis. (4) $\Rightarrow$ (1): Klar.

(1) $\Rightarrow$ (4): Nach Satz (2.1.9) besitzt A eine NGS $y_1, \ldots, y_r$, wobei $y_i^{p(e_i)} = P_i(y_1^{p(e_i)}, \ldots, y_{i-1}^{p(e_i)})$ mit $P_i \in k[Z_1, \ldots, Z_{i-1}]$. Weil k perfekt ist, gilt: $k[Z_1, \ldots, Z_{i-1}] = k^p[Z_1, \ldots, Z_{i-1}]$, insbesondere existiert für jedes i ein Polynom $Q_i \in k[Z_1, \ldots, Z_{i-1}]$, so daß $(Q_i(y))^{p(e_i)} = P_i(y^{p(e_i)})$.

Setzt man $z_i := y_i - Q_i(y_1, \ldots, y_{i-1})$, so ist $A = k[z_1, \ldots, z_r]$ mit $z_i^{p(e_i)} = 0$.

(1), (4) $\Rightarrow$ (2): Man definiert eine Folge von Ringerweiterungen $k_i \subset k_{i+1}$ durch: $k_0 := k$, $k_{i+1} := k_i[y_a; a \in k_i]$ mit $y_a^p = a$. $k_\infty := \bigcup_{i \in \mathbb{N}} k_i$.

k_∞ ist perfekt und lokal, die Erweiterung $k \subset k_\infty$ ist treuflach. Nach Hilfssatz (2.1.11) ist $k_\infty \otimes A$ speziell über k_∞ und die Behauptung folgt aus (4).

(2) $\Rightarrow$ (1): Folgt aus Hilfssatz (2.1.11).

(1) $\Rightarrow$ (3): Klar.

(3) $\Rightarrow$ (1): Induktion nach $\exp(A/k)$: $\bar{k} := k/J(k)$, $\bar{A} := A/J(k)A$.

a) $\exp(A/k) = 1$: $\bar{k} \subset \bar{A}$ ist speziell, d.h.: es existiert eine p-Basis $\bar{x}_1, \ldots, \bar{x}_r$.

$\{\bar{x}_1^{k_1} \ldots \bar{x}_r^{k_r} / 0 \leqq k_i < p\}$ ist dann $\bar{k}$-Basis von $\bar{A}$, also ist $\{x_1^{k_1} \ldots x_r^{k_r} / 0 \leqq k_i < p\}$ ein minimales EZS von A. A ist aber k-frei, daraus folgt, daß $\{x_1^{k_1} \ldots x_r^{k_r} / 0 \leqq k_i < p\}$ schon eine k-Basis von A ist, d.h.: $k \subset A$ ist speziell.

b) $\exp(A/k) > 1$: Wegen $A^{[m]} \underset{k}{|} A$, $\forall m$, gilt: $\bar{k} \otimes A^{[m]} \subset \bar{k} \otimes A$ und damit $(\bar{k} \otimes A)^{[m]} = \bar{k} \otimes A^{[m]}$.

Also ist $\bar{k} \subset \bar{k} \otimes A^{[1]}$ frei mit der Basis $1 \otimes b_i$, $i \in I$, I endlich, $\bar{k} \otimes A^{[1]} \subset \bar{k} \otimes A$ frei mit der Basis $1 \otimes c_j$, $j \in J$, J endlich und $\bar{k} \subset \bar{k} \otimes A$ frei mit der Basis $1 \otimes b_i c_j$, $(i, j) \in I \times J$.

Daher ist $(b_i)_{i \in I}$ ein minimales EZS von $k \subset A^{[1]}$, $(c_j)_{j \in J}$ ein minimales EZS von $A^{[1]} \subset A$ und $(b_i c_j)_{i,j}$ eine Basis von $k \subset A$. (Nach Voraussetzung ist $k \subset A$ frei!)

Somit ist $(c_j)_{j \in J}$ eine Basis von $A^{[1]} \subset A$, d.h.: $A^{[1]} \subset A$ ist frei. Nach a) besitzt $A^{[1]} \subset A$ eine p-Basis und nach Induktionsvoraussetzung ist $A^{[1]}$ speziell über k. Daher ist auch A speziell über k. □

(2.1.13) *Bemerkung.* Aus (3) i) und iii) allein folgt nicht (1). *Gegenbeispiel:* l sei Körper. $k := l[y]$, $y^p = 0$.

$J(k) = {}_k\langle y \rangle$, $k/J(k) \cong l$. $A := k[z_1, z_2]$ mit den Relationen $z_1^{p(2)} = 0$, $z_2^p = z_1^p + y z_1^{p-1}$.

$l \otimes A \cong l[z_1, z_2]$ mit den Relationen $z_1^{p(2)} = 0$, $z_2^p = z_1^p$. $l \subset l \otimes A$ ist also speziell. $k \subset A$ ist nicht speziell.

(2.1.14) *Bemerkung.* In [14; 2, Th. 2] wird Satz (2.1.12), (1) $\Rightarrow$ (2), für den Fall, daß k Körper ist, bewiesen.

2.2. Spezielle Algebren über beliebigen kommutativen Ringen

(2.2.1) **Hilfssatz.** *Es sei $k \in \mathcal{R}i$ und $k \subset S \in \mathcal{A}\ell_k$ eine projektive k-Algebra.*
Ist k noethersch oder S als k-Modul endlich erzeugt, so ist k ein k-direkter Summand von S.

Beweis. 1) Falls S endlich projektiv ist: [5; II, 5, Ex. 4].

2) Ist k noethersch, so kann k in direkt unzerlegbare Faktoren zerlegt werden: $k = \prod_{i=1}^{n} k\varepsilon_i$, dabei ist $\{\varepsilon_1, \ldots, \varepsilon_n\}$ eine vollständige Familie orthogonaler Idempotenter. $k\varepsilon_i$ ist noethersch und zusammenhängend, $k\varepsilon_i \subset S\varepsilon_i$ ist projektiv.

Ist $k\varepsilon_i \subset S\varepsilon_i$ endlich projektiv, so existiert nach 1) eine $k\varepsilon_i$-lineare Retraktion R_i zu $\mathrm{Inj}_i\colon k\varepsilon_i \hookrightarrow S\varepsilon_i$. Ist $k\varepsilon_i \subset S\varepsilon_i$ nicht endlich erzeugt, so ist $k\varepsilon_i \subset S\varepsilon_i$ nach [1; Corr. 4.5] sogar frei und daher existiert eine $k\varepsilon_i$-lineare Retraktion R_i. Die Abbildung

$$\prod_i R_i\colon \prod_i A\varepsilon_i \to \prod_i k\varepsilon_i$$

ist dann eine k-lineare Retraktion von $\mathrm{Inj}\colon k \hookrightarrow S$. □

(2.2.2) **Definition.** A heißt speziell über k genau dann, wenn:
1) $k \subset A$ ist endlich präsentierbar,
2) $\forall\, \mathfrak{m} \in \mathrm{Max}(k)$ ist $A_{\mathfrak{m}}$ speziell über $k_{\mathfrak{m}}$ (im Sinne von Definition (2.1.3)).

(2.2.3) *Bemerkung.* Ist $k \subset A$ rein inseparabel, so werden wegen
$\mathrm{Max}(A) \cong \mathrm{Max}(A^{[m]}) \cong \mathrm{Max}(k)$

$$\mathfrak{m} \mapsto \mathfrak{m} \cap A^{[m]} \mapsto \mathfrak{m} \cap k$$

im folgenden $\mathrm{Max}(A)$, $\mathrm{Max}(A^{[m]})$ und $\mathrm{Max}(k)$ identifiziert.

(2.2.4) **Hilfssatz.** *Ist A speziell, so gilt*
1) *$k \subset A$ ist rein inseparabel*
2) *$\forall\, m \in \mathbb{N}$ gilt: $A^{[m]} \underset{k}{|} A$.*

Beweis. 1) Klar.

2) Zeige: $A^{[m]} \subset A$ ist endlich projektiv. Dann folgt die Behauptung aus (2.2.1).

A ist $A^{[m]}$-endlich erzeugt, daher gibt es ein $s \in \mathbb{N}$ und eine surjektive $A^{[m]}$-lineare Abbildung $f\colon (A^{[m]})^s \to A$.

Die Folge $0 \to \mathrm{Ker}(f) \to (A^{[m]})^s \xrightarrow{f} A \to 0$ von $A^{[m]}$-linearen Abbildungen ist exakt. $k \subset A$ ist endlich präsentierbar und $k \subset (A^{[m]})^s$ ist endlich erzeugt. Nach [5; I, 2, 8, Lemme 9] folgt daraus, daß $\mathrm{Ker}(f)$ als k-Modul endlich erzeugt ist. Somit ist $\mathrm{Ker}(f)$ auch als $A^{[m]}$-Modul endlich erzeugt, also ist $A^{[m]} \subset A$ endlich präsentierbar. Außerdem ist $A^{[m]}_{\mathfrak{m}} \subset A_{\mathfrak{m}}$ frei, $\forall\, \mathfrak{m} \in \mathrm{Max}(A^{[m]})$. Nach [5; II, 5, 2, Th. 1] ist daher $A^{[m]} \subset A$ endlich projektiv. □

Von jetzt ab sei $k \subset A$ immer rein inseparabel.

(2.2.5) **Satz.** *Die folgenden Aussagen sind äquivalent:*
(1) *A ist speziell über k.*

(2) $\forall m \in \mathbb{N}$ *ist* $\Omega(A^{[m]}/k)$ *endlich projektiv.*

(3) i) $k \subset A$ *ist endlich projektiv.*

ii) $\forall \mathfrak{m} \in \mathrm{Max}(k)$ *gilt:* $[A_{\mathfrak{m}}:k_{\mathfrak{m}}] = p(\sum_n [\Omega(A^{[n]}/k)_{\mathfrak{m}}: A_{\mathfrak{m}}^{[n]}])$.

(4) i) $k \subset A$ *ist endlich projektiv.*

ii) $\forall m \in \mathbb{N}$ *gilt:* $A^{[m]} \underset{k}{|} A$.

iii) $\forall \mathfrak{m} \in \mathrm{Max}(k)$ *ist* $k/\mathfrak{m} \otimes A$ *speziell über* $k/\mathfrak{m}$.

Beweis. (1) $\Leftrightarrow$ (3): klar nach Verwendung von Satz (2.1.1) und [5; II, 5, 2, Th. 1].
(1) $\Leftrightarrow$ (4): klar nach Verwendung von Satz (2.1.12) und [5; II, 5, 2, Th. 1].
(1) $\Rightarrow$ (2): Da $k \subset A$ endlich präsentierbar ist, hat $k \subset A$ nur endlich viele Erzeugende und endlich viele Relationen, also ist auch $A \subset \Omega(A/k)$ endlich präsentierbar.

$\forall \mathfrak{m} \in \mathrm{Max}(k) = \mathrm{Max}(A)$ ist $A_{\mathfrak{m}}$ speziell über $k_{\mathfrak{m}}$, also ist $\Omega(A/k)_{\mathfrak{m}} \cong \Omega(A_{\mathfrak{m}}/k_{\mathfrak{m}})$ endlich und frei.

Daher folgt (2) aus [5; II, 5, 2, Th. 1].

(2) $\Rightarrow$ (1): $\Omega(A/k)$ ist endlich projektiv, daher gibt es nach [2; II, 5, 2, Th. 1] Elemente $s_1, \ldots, s_r \in A$, so daß ${}_A\langle s_1, \ldots, s_r \rangle = A$ und $\Omega(A/k)_{s_i}$ A_{s_i}-frei ist, $i = 1, \ldots, r$.

Wähle $a_1, \ldots, a_r \in A$, so daß $1 = \sum_i a_i s_i$. $A^{p(e)} \subset k$, also ist $1 = \sum_i a_i^{p(e)} s_i^{p(e)}$, $a_i^{p(e)} \in k$, $s_i^{p(e)} \in k$.

Nach [2; II, 2, 3, Prop. 8] gilt: $\Omega(A/k)_{s_i} = \Omega(A/k)_{s_i^{p(e)}}$. Also kann man o.E.d.A. annehmen, daß $a_i \in k$ und $s_i \in k$. Ebenso für $\Omega(A^{[m]}/k)$ mit den gleichen s_i.

$$\Omega(A^{[m]}/k)_{s_i} \cong \Omega(A_{s_i}^{[m]}/k_{s_i}) \quad \text{ist } A_{s_i}^{[m]}\text{-frei}, \ m \in \mathbb{N}.$$

Nach Satz (2.1.1) besitzt dann $A_{s_i}^{[m]}$ eine p-Basis, $\forall m$, $\forall i$, insbesondere ist $k_{s_i} \subset A_{s_i}$ endlich und frei, $i = 1, \ldots, r$.

Nach [5; II, 5, 2, Th. 1] ist $k \subset A$ endlich projektiv, insbesondere endlich präsentierbar.

Außerdem ist $\forall \mathfrak{m} \in \mathrm{Max}(k)$ $A_{\mathfrak{m}}$ speziell über $k_{\mathfrak{m}}$ (weil $\Omega(A^{[m]}/k)_{\mathfrak{m}}$ frei ist, $\forall m$). Somit ist A speziell über k. □

(2.2.6) *Folgerung.* $k \subset l$ *sei eine treuflache Ringerweiterung. Dann sind die folgenden Aussagen äquivalent:*

(1) A *ist speziell über* k.

(2) $l \otimes A$ *ist speziell über* l.

Beweis. Nach [5; I, 3, 6, Prop. 12] ist $\Omega(A/k)$ endlich projektiver A-Modul genau dann, wenn $l \otimes \Omega(A/k) \cong \Omega(l \otimes A/l)$ endlich projektiver $l \otimes A$-Modul ist. □

(2.2.7) **Satz.** A *sei speziell über* k, $\mathfrak{m} \in \mathrm{Max}(k)$ *und* $d(m) := [\Omega(A_{\mathfrak{m}}^{[m]}/k_{\mathfrak{m}}): A_{\mathfrak{m}}^{[m]}]$. *Dann existieren Elemente* $z_1, \ldots, z_r \in A$ *und ein* $s \in k \setminus \mathfrak{m}$ *mit:*

1) $\forall m \in \mathbb{N}$ *ist* $\Omega(A^{[m]}/k)_s$ $A_s^{[m]}$*-frei.*

2) $\forall m \in \mathbb{N}$ *ist* $\{d(z_i^{p(m)})/i = 1, \ldots, d(m)\}$ *eine* $A_s^{[m]}$*-Basis von* $\Omega(A^{[m]}/k)_s$ *und* $d(0) = r$.

3) $z_1, \ldots, z_r$ *ist* NGS *von* $k_s \subset A_s$.

Beweis. 1) und 2). Nach Satz (2.1.7) gibt es Elemente $y_1, \ldots, y_r \in A_{\mathfrak{m}}$, so daß für alle $m\{d(y_i^{p(m)})/i = 1, \ldots, d(m)\}$ eine $A_{\mathfrak{m}}^{[m]}$-Basis von $\Omega(A^{[m]}/k)_{\mathfrak{m}}$ ist. Aber $y_i = z_i/t_i$, wobei $t_i \in k \setminus \mathfrak{m}$, $z_i \in A$. $d(y_i^{p(m)}) = \frac{1}{t_i^{p(m)}} d(z_i^{p(m)})$, also ist auch $\{d(z_i^{p(m)})/i = 1, \ldots, d(m)\}$ eine $A_{\mathfrak{m}}^{[m]}$-Basis von $\Omega(A_{\mathfrak{m}}^{[m]}/k_{\mathfrak{m}})$.

Da $\Omega(A^{[m]}/k)$ endlich projektiv ist, existiert nach [5; II, 5, 2, Th.1] zu jedem m ein $s(m)\in k\setminus\mathfrak{m}$ derart, daß $\Omega(A^{[m]}/k)_{s(m)}$ $A^{[m]}_{s(m)}$-frei ist mit der Basis $\{d(z_i^{p(m)})/i=1,\dots,d(m)\}$. Ist $e:=\exp(A/k)$, so ist $A^{[e]}=k$, also $\Omega(A^{[m]}/k)=0$ für $m\geqq e$. Setze $s:=\prod_{m=0}^{e} s(m)\in k\setminus\mathfrak{m}$.

$\Omega(A^{[m]}/k)_{s(m)}$ ist frei, daher ist auch $\Omega(A^{[m]}/k)_s=(\Omega(A^{[m]}/k)_{s(m)})_{\frac{s}{s(m)}}$ frei, mit der $A^{[m]}_s$-Basis $\{d(z_i^{p(m)})/i=1,\dots,d(m)\}$.

3) Wird durch Induktion nach $\exp(A/k)$ wie Satz (2.1.9), (1) $\Rightarrow$ (2), bewiesen. □

(2.2.8) **Hilfssatz.** *Sind $P_1,\dots,P_n$ endlich projektive k-Moduln, so gibt es eine vollständige Familie $\{\varepsilon_1,\dots,\varepsilon_r\}$ von orthogonalen Idempotenten in k, so daß alle $\varepsilon_i P_j$ endlich projektive $\varepsilon_i k$-Moduln von konstantem Rang sind $(i=1,\dots,r;\ j=1,\dots,n)$.*

Beweis. Nach [5; II, 5, 2, Th.1] ist

$$\begin{aligned} rg_i\colon \operatorname{Max}(k) &\to \mathbb{Z}\\ \mathfrak{m} &\mapsto [P_{i\mathfrak{m}}:k_{\mathfrak{m}}]\end{aligned}$$

lokal konstant, d.h. stetig (Max(k) mit der Zariskitopologie, $\mathbb{Z}$ diskret), $\forall i$. Daher ist auch

$$\begin{aligned} rg\colon \operatorname{Max}(k) &\to \mathbb{Z}^n\\ \mathfrak{m} &\mapsto ([P_{i\mathfrak{m}}:k_{\mathfrak{m}}])_{i=1,\dots,n}\end{aligned}$$

stetig und $\operatorname{Max}(k)=\dot{\bigcup}_{(s_1,\dots,s_m)\in\mathbb{N}^n} rg^{-1}(s_1,\dots,s_n)$ ist eine disjunkte Zerlegung von Max(k) in offene Mengen.

Weil Max(k) kompakt ist, ist die Zerlegung endlich, d.h.: $\operatorname{Max}(k)=U_1\dot{\cup}\cdots\dot{\cup}U_r$, U_i offen, $U_i\neq\varnothing$.

Nach [5; II, 4, 3, Prop. 15] existiert daher eine Familie $(\varepsilon_i)_i$ mit den gewünschten Eigenschaften. □

(2.2.9) **Satz.** *Es sei $k\in\mathfrak{Ri}$ und A eine rein inseparable Algebra in $\mathfrak{Alf}_k$.*

Die folgenden Aussagen sind äquivalent:

(1) *A ist speziell über k.*

(2) *Es gibt eine Familie vollständiger orthogonaler Idempotenter $\{\varepsilon_1,\dots,\varepsilon_n\}$ und für jedes i eine treuflache, rein inseparable Ringerweiterung $k\varepsilon_i\subset l_i$, so daß $l_i\otimes A\varepsilon_i\cong l_i[z_1,\dots,z_{r(i)}]$ mit den Relationen $z_j^{p(e_j(i))}=0$, $j=1,\dots,r(i)$; $e_1(i)\geqq\cdots\geqq e_{r(i)}(i)>0$.*

Beweis. (1) $\Rightarrow$ (2): 1) Nach (2.2.8) gibt es eine Zerlegung $k=k\varepsilon_1\times\cdots\times k\varepsilon_n$, so daß $\varepsilon_i A^{[m]}$ über $\varepsilon_i k$ von konstantem Rang ist (für jedes i und m). Daher genügt es, unter der Annahme, daß für jedes m $k\subset A^{[m]}$ von konstantem Rang ist, zu zeigen: Es gibt eine treuflache, rein inseparable Ringerweiterung $k\subset l$, so daß $l\otimes A\cong l[z_1,\dots,z_r]$ mit den Relationen $z_i^{p(e_i)}=0$, $e_1\geqq\cdots\geqq e_r>0$.

2) Es sei $\mathfrak{m}\in\operatorname{Max}(k)$. $k\subset A^{[m]}$ ist von konstantem Rang, $\forall m$, und $[A^{[m]}_{\mathfrak{m}}:A^{[m+1]}_{\mathfrak{m}}]\,[A^{[m+1]}_{\mathfrak{m}}:k_{\mathfrak{m}}]=[A^{[m]}_{\mathfrak{m}}:k_{\mathfrak{m}}]$, also ist auch $[A^{[m]}_{\mathfrak{m}}:A^{[m+1]}_{\mathfrak{m}}]$ von $\mathfrak{m}$ unabhängig.

Nach Satz (2.2.5) ist $[A^{[m]}_{\mathfrak{m}}:A^{[m+1]}_{\mathfrak{m}}]=p([\Omega(A^{[m]}/k)_{\mathfrak{m}}:A^{[m]}_{\mathfrak{m}}])$, daraus folgt, daß auch $[\Omega(A^{[m]}/k)_{\mathfrak{m}}:A^{[m]}_{\mathfrak{m}}]$ von $\mathfrak{m}$ unabhängig ist, d.h.: $\Omega(A^{[m]}/k)$ ist $A^{[m]}$-Modul von konstantem Rang.

3) A ist speziell über k, also existiert nach (2.2.7) für jedes $\mathfrak{m}\in\operatorname{Max}(k)$ ein $s=s(\mathfrak{m})\in k\setminus\mathfrak{m}$, so daß $k_s\subset A_s$ eine NGS $z_1,\dots,z_r$ besitzt.

4) Wähle $\mathfrak{m}_1,\dots,\mathfrak{m}_t\in\operatorname{Max}(k)$ so, daß ${}_k\langle s(\mathfrak{m}_1),\dots,s(\mathfrak{m}_t)\rangle=k$. $s_i:=s(\mathfrak{m}_i)$. Dann ist $k\subset\prod_{i=1}^{t}k_{s_i}$ treuflach [5; II, 5, 1, Prop. 3].

Wie in Satz (2.1.12), (1) $\Rightarrow$ (2), folgt aus 3): Zu jedem i gibt es eine treuflache Ringerweiterung $k_{s_i}\subset l_i$ und eine NGS $z_1,\dots,z_{r(i)}\in A_{s_i}$ derart, daß $l_i\otimes A_{s_i}\cong l[z_1,\dots,z_{r(i)}]$ mit den Relationen $z_j^{p(e_j(i))}=0$.

$k\subset l:=\prod_{i=1}^{t}l_i$ ist treuflach.

Wegen 2) und Satz (2.1.6) hängen die $r(i)$ und $e_j(i)$ von i nicht ab, also ist $l\otimes A=\prod_i(l_i\otimes A_{s_i})\cong l[z_1,\dots,z_r]$ mit den Relationen $z_j^{p(e_j)}=0$.

(2) $\Rightarrow$ (1): Nach (2) und Satz (2.2.5) ist für jedes i $\Omega(l_i\otimes A\varepsilon_i/l_i)$ endlich projektiv. Daher ist auch $\prod_i\Omega(l_i\otimes A\varepsilon_i/l_i)\cong\Omega((\prod_i l_i)\otimes A/\prod_i l_i)$ endlich projektiv, d.h.: $(\prod_i l_i)\otimes A$ ist speziell über $(\prod_i l_i)$. (2.2.5). $k\subset(\prod_i l_i)$ ist treuflach, also ist A nach (2.2.6) speziell über k. □

(2.2.10) *Folgerung. k sei ein endliches Produkt von lokalen Ringen $k_i=k\varepsilon_i$, $\{\varepsilon_1,\dots,\varepsilon_n\}$ eine Familie vollständiger orthogonaler Idempotenter und $A_i:=A\varepsilon_i$.*

Dann sind die folgenden Aussagen äquivalent:

(1) *$\forall m$ ist $\Omega(A^{[m]}/k)$ $A^{[m]}$-frei.*

(2) *$\forall i$ ist $A_i=k_i[z_1,\dots,z_r]$ mit den Relationen $z_j^{p(e_j)}=P_{ij}(z_1^{p(e_j)},\dots,z_{j-1}^{p(e_j)})$, $j=1,\dots,r$; $e_1\geqq e_2\geqq\cdots e_r>0$. ($(e_1,\dots,e_r)$ ist von i unabhängig!).*

Beweis. (1) $\Rightarrow$ (2): $\Omega(A^{[m]}/k)\cong\prod_i\Omega(A_i^{[m]}/k_i)$ ist $A^{[m]}$-frei, daher sind auch alle $\Omega(A_i^{[m]}/k_i)$ $A_i^{[m]}$-frei und $[\Omega(A_i^{[m]}/k_i):A_i^{[m]}]=[\Omega(A^{[m]}/k):A^{[m]}]$ ist von i unabhängig. Daher besitzt $k_i\subset A_i$ eine NGS, (Satz (2.1.9)) und die Folge $e_1,\dots,e_r$ hängt von i nicht ab (Satz (2.1.6)).

(2) $\Rightarrow$ (1): Klar. □

3. Transitive Operationen

3.1. Charakterisierung der transitiven Operationen

k sei ein Körper, $\bar{k}$ ein algebraischer Abschluß von k, $\mathfrak{X}=\mathfrak{Sp}\,S$ ein endliches k-Schema und $\mathfrak{G}=(\mathfrak{G},\mu,\eta,\tau)$ eine k-Gruppe. $A=A(\mathfrak{G})$ sei die affine Algebra von $\mathfrak{G}$ und $x_0\in\mathfrak{G}(A)$ ein universelles Element, also

$$\begin{aligned} x_0^{\#}:\ \mathfrak{Sp}\,A &\xrightarrow{\cong}\mathfrak{G}\\ \mathrm{id}_A &\mapsto x_0. \end{aligned}$$

Durch Op: $\mathfrak{X}\times\mathfrak{G}\to\mathfrak{X}$ sei eine Operation von $\mathfrak{G}$ auf $\mathfrak{X}$ gegeben. Dieser entsprechen $\Delta:=A(Op)$: $S\to S\otimes A$ und ρ: $\mathfrak{G}\to\mathfrak{Aut}(S/k)$ (vgl. (1.2.1)).

(3.1.1) **Definition.** $\mathfrak{a}$ sei ein Ideal von S und $\mathfrak{Y} := \mathfrak{Sp}(S/\mathfrak{a})$

1) $\mathfrak{Y}$ heißt *$\mathfrak{G}$-stabiles Unterschema von $\mathfrak{X}$* (kurz: *$\mathfrak{G}$-stabil*), falls Op den Morphismus $Op|_{\mathfrak{Y}\times\mathfrak{G}}: \mathfrak{Y}\times\mathfrak{G}\to\mathfrak{Y}$ induziert.

2) $\mathfrak{a}$ heißt „*$\mathfrak{G}$-stabiles Ideal von S*" (kurz: *$\mathfrak{G}$-stabil*), falls $\Delta(\mathfrak{a})\subset\mathfrak{a}\otimes A$.

(3.1.2) **Hilfssatz.** *Die folgenden Aussagen sind äquivalent:*

(1) *$\mathfrak{Sp}(S/\mathfrak{a})$ ist $\mathfrak{G}$-stabil.*

(2) *$\mathfrak{a}$ ist $\mathfrak{G}$-stabil.*

(3) $\forall R\in\mathscr{A}\ell_k$, $\forall f\in\mathfrak{G}(R)$, $\rho_R(f)(\mathfrak{a}\otimes R)\subset\mathfrak{a}\otimes R$.

Beweis. (1.2.1). □

(3.1.3) **Definition.** Die Operation Op ist *transitiv* genau dann, wenn

1) ${}^{\mathfrak{G}}S=k$,

2) S enthält kein $\mathfrak{G}$-stabiles echtes Ideal.

(3.1.4) *Beispiel.* Die Gruppenverknüpfung μ: $\mathfrak{G}\times\mathfrak{G}\to\mathfrak{G}$ ist eine transitive Operation von $\mathfrak{G}$ auf $\mathfrak{G}$.

Beweis. Das Diagramm

$$\begin{tikzcd} A \arrow[rr, "A(\mu)"] \arrow[dr, "\cong"'] & & A\otimes A \arrow[dl, "A(\eta)\otimes A"] \\ & k\otimes A & \end{tikzcd}$$

ist kommutativ. $\varepsilon := A(\eta)$.

Ist $x\in{}^{\mathfrak{G}}S$, so ist $\varepsilon(x)\cdot 1=x$, also $x\in k$.

Ist $\mathfrak{a}\neq 0$ ein Ideal von A, so ist $\varepsilon(\mathfrak{a})=k$ oder $\varepsilon(\mathfrak{a})=0$, also folgt aus $A(\mu)(\mathfrak{a})\subset\mathfrak{a}\otimes A$: $\mathfrak{a}=\varepsilon(\mathfrak{a})\,A=A$. □

(3.1.5) **Hilfssatz.** *M und N seien S-Moduln, $[M:k]<\infty$, $f\in\mathrm{Hom}_S(M,N)$, $k\subset l$ eine* KE *und $l\otimes f\in\mathrm{Hom}_{l\otimes S}(l\otimes M, l\otimes N)$ besitze eine $l\otimes S$-lineare Retraktion.*

Dann besitzt f eine S-lineare Retraktion.

Beweis. Folgt aus [6; 29.5]. □

(3.1.6) **Satz.** *Die folgenden Aussagen sind äquivalent:*

(1) *Op ist transitiv.*

(2) (Inj,Δ): $S\otimes S\to S\otimes A$ *besitzt eine links-S-lineare Retraktion.*
$s\otimes t\mapsto(s\otimes 1)\,\Delta(t)$

(3) *Ist $k\subset l$ eine* KE, *so ist $l\otimes Op$: $l\otimes\mathfrak{X}\times l\otimes\mathfrak{G}\to l\otimes\mathfrak{X}$ transitiv.*

(4) *Es gibt eine* KE *$k\subset l$, so daß $l\otimes Op$ transitiv ist.*

Falls $\mathfrak{X}(k)$ nichtleer ist:

(5) *Für $x\in\mathfrak{X}(k)$ gilt: $\mathfrak{X}\cong\mathfrak{G}/\mathfrak{G}_x$.*

Beweis. (2) $\Rightarrow$ (1): a) Ist $x\in{}^{\mathfrak{G}}S$, so ist $(\mathrm{Inj},\Delta)(1\otimes x)=x\otimes 1=(\mathrm{Inj},\Delta)(x\otimes 1)$. Da (Inj,Δ) insbesondere injektiv ist, folgt: $x\otimes 1=1\otimes x$, also ist $x\in k$.

b) $0\neq\mathfrak{a}$ sei ein $\mathfrak{G}$-stabiles Ideal von S und R eine links-S-lineare Retraktion von (Inj,Δ). Dann ist $R(\mathrm{Inj},\Delta)(S\otimes\mathfrak{a})\subset R(\mathfrak{a}\otimes A)\subset\mathfrak{a}\otimes S$.

Andererseits ist $R(\mathrm{Inj}, \Delta) = \mathrm{id}_{S\otimes S}$, also $R(\mathrm{Inj}, \Delta)(S\otimes\mathfrak{a}) = S\otimes\mathfrak{a}$. Somit ist $S\otimes\mathfrak{a}\subset\mathfrak{a}\otimes S$, d.h.: $\mathfrak{a}=S$.

(1) $\Rightarrow$ (5): Sei $x\in\mathfrak{X}(k)$. Der Morphismus

$$\begin{aligned}\mathfrak{G} &\to \mathfrak{X}\\ s &\mapsto Op_R(x_R, s)\end{aligned}$$

kann in $\mathfrak{G} \xrightarrow{\mathrm{kan}} \mathfrak{G}/\mathfrak{G}_x \xrightarrow{i} \mathfrak{X}$ zerlegt werden, dabei ist $A(i)$ surjektiv (vgl. (1.2.4)). $\mathfrak{G}/\mathfrak{G}_x$ ist daher ein $\mathfrak{G}$-stabiles Unterschema von $\mathfrak{X}$, also muß i ein Isomorphismus sein.

(5) $\Rightarrow$ (2): o.E.d.A.: $S = A(\mathfrak{G}/\mathfrak{G}_x)$ und $\Delta = A(\mu)|_S$. Nach [13; 4.10] ist A ein projektiver S-Modul. S ist noethersch, also besitzt $\mathrm{Inj}: S\subset A$ nach (2.2.1) eine S-lineare Retraktion R.

Die Morphismen $\mathfrak{G}\times\mathfrak{G} \xrightarrow{(\mathrm{proj},\mu)} \mathfrak{G}\times\mathfrak{G} \xrightarrow{(\mathrm{proj},\mu(\tau\times\mathrm{Id}))} \mathfrak{G}\times\mathfrak{G}$ sind zueinander inverse Schemaisomorphismen.

In $\mathscr{A}\ell_k$ erhält man dann das Diagramm

$$\begin{tikzcd}
A\otimes A \arrow[r, "(\mathrm{Inj}, A(\mu))"] & A\otimes A \arrow[r, "(\mathrm{Inj}, (A(\tau)\otimes\mathrm{id})A(\mu))"] & A\otimes A \arrow[d, "R\otimes R"'] \\
S\otimes S \arrow[u, phantom, "\cup"] \arrow[r, "(\mathrm{Inj}, \Delta)"] & S\otimes A \arrow[u, phantom, "\cup"] & S\otimes S
\end{tikzcd}$$

$(R\otimes R)(\mathrm{Inj}, (A(\tau)\otimes\mathrm{id})\Delta)$ ist daher eine Retraktion von (Inj, Δ) und links-S-linear.

(1) $\Rightarrow$ (3) $\Rightarrow$ (4): Klar.

(1) $\Rightarrow$ (2): Op ist transitiv, also auch $\bar{k}\otimes Op$. $(\bar{k}\otimes\mathfrak{X})(\bar{k})$ ist nichtleer, für diesen Fall ist (1) $\Rightarrow$ (2) schon gezeigt. $\bar{k}\otimes(\mathrm{Inj}, \Delta)$ besitzt somit eine links-$\bar{k}\otimes S$-lineare Retraktion. Die Behauptung folgt nun aus (3.1.5).

(4) $\Rightarrow$ (2): Klar wegen (3.1.5). $\square$

3.2. Existenz einer transitiven Operation einer zusammenhängenden Gruppe

Sei $k\in\mathscr{R}\mathscr{i}$, $R\in\mathscr{A}\ell_k$ und $k[z] := k[z_1, \ldots, z_r]$ mit den Relationen $z_i^{p(e_i)} = 0$, wobei $e_1 \geqq \cdots \geqq e_r > 0$, $e_i\in\mathbb{N}$.

Nach der Identifikation $R\otimes k[z] = R[z]$ erhält man wegen

$$\mathscr{A}\ell_R(R[Z_1, \ldots, Z_r], R[z]) \cong R[z]^r$$

die (in R) funktorielle Bijektion

$$\begin{aligned}\mathrm{End}(R[z]/R) &\cong \{(s_1, \ldots, s_r)\in R[z]^r / s_i^{p(e_i)} = 0, \forall i\}.\\ f &\longmapsto (f(z_1), \ldots, f(z_r))\end{aligned}$$

$$I := \{m\in\mathbb{N}^r / 0 \leqq m_i < p(e_i), \forall i\}.$$

$\{z^m/m\in I\}$ ist eine k-Basis von $k[z]$, daher ist

$$f(z_i)=\sum_{m\in I} z^m r_i(m), \qquad r_i(m)\in R. \quad \text{(a)}$$

$$0=f(z_i)^{p(e_i)}=\sum_{m\in I} z^{p(e_i)m} r_i(m)^{p(e_i)}$$
$$=\sum \{z^{p(e_i)m} r_i(m)^{p(e_i)}/m\in I,\ m_j<p(e_j-e_i),\ \forall j\} \quad \text{(b)}.$$

Aus (a) und (b) ergibt sich die funktorielle Bijektion

$$\begin{aligned} \mathrm{End}(R[z]/R)&\cong\{r=(r_i(m))_{\substack{i=1,\dots,r\\ m\in I}}/r_i(m)^{p(e_i)}=0, \text{ falls } m_j<p(e_j-e_i),\ \forall j\}=:\mathfrak{M}(R)\\ f&\longmapsto r\\ &\qquad f(z_i)=\sum_{m\in I} z^m r_i(m). \end{aligned}$$

(3.2.1) **Satz.** 1) *Die funktorielle Bijektion* $\mathrm{End}(R[z]/R)\cong\mathfrak{M}(R)$ *induziert auf* $\mathfrak{M}(R)$ *folgende Monoidstruktur:* $f\longmapsto r$

$$\forall r, s\in\mathfrak{M}(R), \qquad (r\,s)_i(m)=\sum\{((\alpha))\, s_i(|\alpha|)\, r^\alpha/|\alpha|\in I,\ \mathrm{gew}(\alpha)=m\},$$

$$(1_{M(R)})_i(m)=\begin{cases}1 & \textit{falls } m=(0,\dots,0,\underset{i}{1},0,\dots,0)\\ 0 & \textit{sonst}\end{cases}$$

wobei

$$\alpha:=(\alpha_1,\dots,\alpha_r)\in(\mathbb{N}^I)^r,$$
$$\alpha_i:=(\alpha_i(m))_{m\in I},$$
$$|\alpha|:=(\sum_{m\in I}\alpha_1(m),\dots,\sum_{m\in I}\alpha_r(m)),$$
$$((\alpha)):=\prod_{i=1}^{r}\frac{(\sum_{m\in I}\alpha_i(m))!}{\prod_{m\in I}(\alpha_i(m)!)},$$
$$\mathrm{gew}(\alpha):=\sum_{i,m}\alpha_i(m)\, m\in\mathbb{N}^r.$$

2) $A(\mathfrak{M})=A(\mathfrak{End}(k[z]/k)=k[x_i(m);\ m\in I,\ i\in\{1,\dots,r\}]$ *mit den Relationen* $x_i(m)^{p(e_i)}=0$, *falls* $\forall j\ \ 0\leqq m_j<p(e_j-e_i)$.

Coalgebrenstruktur:

$$\begin{aligned} \Delta:\ & A(\mathfrak{M})\to A(\mathfrak{M})\otimes A(\mathfrak{M})\\ & x_i(m)\mapsto\sum\{x^\alpha\otimes((\alpha))\, x_i(|\alpha|)/\alpha\in(N^I)^r,\ \mathrm{gew}(\alpha)=m,\ |\alpha|\in I\},\\ \varepsilon:\ & A(\mathfrak{M})\to k\\ & x_i(m)\mapsto\begin{cases}1 & \textit{falls } m=(0,\dots,0,\underset{i}{1},0,\dots,0)\\ 0 & \textit{sonst}.\end{cases} \end{aligned}$$

Beweis. 1) $\mathrm{End}(R[z]/R) \cong \mathfrak{M}(R)$

$$\begin{aligned} f &\longmapsto r \\ g &\longmapsto s \\ \mathrm{id} &\longmapsto 1_{M(R)}, \end{aligned}$$

$$f(z_i) = \sum_{m \in I} z^m r_i(m), \qquad g(z_i) = \sum_{m \in I} z^m s_i(m),$$

$$\begin{aligned} \sum_{m \in I} z^m (r\,s)_i(m) &= f\,g(z_i) = \sum_{m \in I} f(z^m)\, s_i(m) \\ &= \sum_{m \in I} \Big(\sum_{\substack{\alpha \in (\mathbb{N}^I)^r \\ |\alpha| = m}} ((\alpha))\, z^{\mathrm{gew}(\alpha)}\, r^\alpha \Big) s_i(m) = \sum_{m \in I} z^m \Big(\sum_{\substack{\alpha \\ \mathrm{gew}(\alpha) = m \\ |\alpha| \in I}} ((\alpha))\, r^\alpha\, s_i(|\alpha|) \Big) \Rightarrow \\ &\Rightarrow (r\,s)_i(m) = \sum_\alpha \{((\alpha))\, s_i(|\alpha|)\, r^\alpha / |\alpha| \in I,\ \mathrm{gew}(\alpha) = m\}, \end{aligned}$$

$$\mathrm{id}(z_i) = \sum_{m \in I} z^m (1_{\mathfrak{M}(R)})_i(m) = z_i \Rightarrow (1_{\mathfrak{M}(R)})_i(m) = \begin{cases} 1 & m = (0, \ldots, \underset{i}{1}, \ldots, 0) \\ 0 & \text{sonst}. \end{cases}$$

2) Es gilt: $\mathfrak{M}(\Delta(x)) = \mathfrak{M}(u_1)(x) \cdot \mathfrak{M}(u_2)(x)$, d.h.:

$$(\Delta(x_i(m)))_{i,m} = (x_i(m) \otimes 1)_{i,m} \cdot (1 \otimes x_i(m))_{i,m} \qquad \text{(vgl. (1.2.2))}.$$

Nach 1) ist daher

$$\begin{aligned} \Delta(x_i(m)) &= \sum_\alpha \{((\alpha))\, (x \otimes 1)^\alpha\, (1 \otimes x_i(|\alpha|)) / |\alpha| \in I,\ \mathrm{gew}(\alpha) = m\} \\ &= \sum_\alpha \{((\alpha))\, x^\alpha \otimes x_i(|\alpha|) / |\alpha| \in I,\ \mathrm{gew}(\alpha) = m\}. \end{aligned}$$

$$M(\varepsilon(x)) = 1_{\mathfrak{M}(k)}, \text{ d.h.: } \varepsilon(x_i(m)) = (1_{\mathfrak{M}(k)})_i(m) \underset{1)}{=} \begin{cases} 1 & m = (0, \ldots, \underset{i}{1}, \ldots, 0) \\ 0 & \text{sonst}. \end{cases} \qquad \square$$

(3.2.2) *Folgerung.* $A(\mathfrak{Aut}(k[z]/k)_{(s)}) = k[x_i(m);\ m \in I,\ i = 1, \ldots, r]$ *mit den Relationen*

$$x_i(m)^{p(e_i)} = 0, \qquad \textit{falls } \forall j\ \ 0 \leqq m_j < p(e_j - e_i)$$

und

$$x_i(m)^{p(s)} = \varepsilon(x_i(m)), \qquad m \in I,\ i = 1, \ldots, r.$$

(Insbesondere ist diese Algebra endlich und speziell über k.)

Beweis. (1.3.3). $\square$

(3.2.3) **Hilfssatz.** *k sei ein Körper,* $S \in \mathscr{Alf}_k$ *und* $\mathfrak{G}$ *eine k-Gruppe. Op:* $\mathfrak{X} \times \mathfrak{G} \to \mathfrak{X}$ *sei eine transitive Operation von* $\mathfrak{G}$ *auf* $\mathfrak{X} = \mathfrak{Sp}\, S$.

Dann gilt:

1) $\mathfrak{Aut}(S/k)$ *operiert transitiv auf* $\mathfrak{X}$.

2) *Ist* $\mathfrak{G} = \mathfrak{G}_0$ *bzw.* $\mathfrak{G} = \mathfrak{G}_{(r)}$, *so operiert* $\mathfrak{Aut}(S/k)_0$ *bzw.* $\mathfrak{Aut}(S/k)_{(r)}$ *transitiv auf* $\mathfrak{X}$.

Beweis. Es sei $A := A(\mathfrak{G})$, $B := A(\mathfrak{Aut}(S/k))$ und $\Delta := A(Op)$. $\mathrm{id}: \mathfrak{Aut}(S/k) \to \mathfrak{Aut}(S/k)$ induziert die Operation Δ_B: $S \to S \otimes B$. Der Operation Op entspricht ein Morphismus $\rho: \mathfrak{G} \to \mathfrak{Aut}(S/k)$.

Das Diagramm

$$\begin{tikzcd} & S\otimes A \\ S \arrow[ur, "\Delta"] \arrow[dr, "\Delta_B"'] & \\ & S\otimes B \arrow[uu, "S\otimes A(\rho)"'] \end{tikzcd}$$

ist kommutativ.

Also ist auch

$$\begin{tikzcd} & S\otimes A \\ S\otimes S \arrow[ur, "(\mathrm{Inj},\Delta)"] \arrow[dr, "(\mathrm{Inj},\Delta_B)"'] & \\ & S\otimes B \arrow[uu, "S\otimes A(\rho)"'] \end{tikzcd}$$

kommutativ.

1) (Inj, Δ) besitzt eine Retraktion R, daher ist $R(S\otimes A(\rho))$ eine Retraktion von (Inj, Δ_B).

2) Ist $\mathfrak{G}=\mathfrak{G}_0$ bzw. $\mathfrak{G}=\mathfrak{G}_{(r)}$, so induziert $A(\rho)$ den Morphismus

$$A(\rho)_0\colon B_0 \to A = A_0 \quad \text{bzw.} \quad A(\rho)_{(r)}\colon B_{(r)} \to A = A_{(r)}.$$

Die Behauptung folgt nun wie in 1). □

(3.2.4) **Hilfssatz.** *k sei ein Körper, $\mathfrak{G}$ eine k-Gruppe, $A(\mathfrak{G})=A=(A, \Delta, \varepsilon, \sigma)$ und S eine endlichdimensionale Unteralgebra von A.*

Dann sind die folgenden Aussagen äquivalent:

(1) *Es gibt eine Untergruppe $\mathfrak{G}'$ von $\mathfrak{G}$, so daß $S=A(\mathfrak{G}/\mathfrak{G}')$.*

(2) i) $\Delta(S)\subset S\otimes A$,

ii) *$S\subset A$ ist treuflach.*

Beweis. (1) $\Rightarrow$ (2): i) Klar.

ii) [7; III, 3.2.5].

(2) $\Rightarrow$ (1): $\mathfrak{G}$ operiert durch $\mathfrak{Sp}(\Delta|_S)$ auf $\mathfrak{Sp}\, S$.

$$k\subset A \underset{\mathrm{Inj}}{\overset{\Delta}{\rightrightarrows}} A\otimes A \quad \text{ist exakt (vgl. (3.1.4)), also auch}$$

$$k\subset S \underset{\mathrm{Inj}}{\overset{\Delta}{\rightrightarrows}} S\otimes A, \quad \text{d.h.:} \quad {}^{\mathfrak{G}}S=k.$$

Ist $\mathfrak{a}\trianglelefteq S$ ein stabiles Ideal von S, so ist $A\mathfrak{a}$ stabil bezüglich $\Delta\colon A\to A\otimes A$, also $A\mathfrak{a}=0$ oder $A\mathfrak{a}=A$ (vgl. (3.1.4)). $S\subset A$ ist treuflach, daher ist $A\mathfrak{a}\cap S=\mathfrak{a}$ [5; I, 3, 5, Prop. 9]. Insbesondere ist $A\mathfrak{a}\neq A$. Somit ist $\mathfrak{a}=0$. $\mathfrak{G}$ operiert also transitiv auf $\mathfrak{Sp}\, S$ und $\varepsilon|_S\in\mathfrak{Sp}\, S(k)$. Aus Satz (3.1.6) folgt die Behauptung. □

(3.2.5) **Satz.** *k sei ein Körper und $S\in\mathscr{A}\ell\mathscr{f}_k$.*

Die folgenden Aussagen sind äquivalent:

(1) *Es gibt eine zusammenhängende k-Gruppe $\mathfrak{G}$, die transitiv auf $\mathfrak{Sp}\, S$ operiert.*

(2) *S ist speziell über k.*

Falls $\mathscr{A}\ell_k(S, k)$ nichtleer ist:

(3) *Es gibt eine zusammenhängende k-Gruppe $\mathfrak{G}$ und eine Untergruppe $\mathfrak{G}'$ von $\mathfrak{G}$, so daß $\mathfrak{Sp}\, S \cong \mathfrak{G}/\mathfrak{G}'$.*

Beweis. (1) $\Leftrightarrow$ (3): Satz (3.1.6).

(1) $\Rightarrow$ (2): $\mathfrak{G}$ operiert transitiv auf $\mathfrak{Sp}\, S$, also operiert $\bar{k}\otimes\mathfrak{G}$ transitiv auf $\mathfrak{Sp}(\bar{k}\otimes S)$. $\mathfrak{Sp}(\bar{k}\otimes S)(\bar{k})$ ist nichtleer, also gibt es nach Satz (3.1.6) eine Untergruppe $\mathfrak{G}'$ von $\bar{k}\otimes\mathfrak{G}$, so daß $\bar{k}\otimes S = A(\bar{k}\otimes\mathfrak{G}/\mathfrak{G}')$. Nach [7; III, 3, 6.3] ist $\bar{k}\otimes S$ speziell über $\bar{k}$, daraus folgt mit (2.1.11): S ist speziell über k.

(2) $\Rightarrow$ (1): Nach Satz (2.1.12) hat $\bar{k}\otimes S$ die Gestalt $\bar{k}[z_1, \ldots, z_r]$, $z_i^{p(e_i)} = 0$, $e_1 \geqq \cdots \geqq e_r > 0$. $e := e_1$, $I := \{m \in \mathbb{N}^r / 0 \leqq m_i < p(e_i),\ \forall i\}$. Nach Satz (3.2.1) und (3.2.2) ist $A(\bar{k}\otimes\mathfrak{Aut}(S/k)_{(e)}) = A(\mathfrak{Aut}(\bar{k}\otimes S/\bar{k})_{(e)}) = \bar{k}[x_i(m);\ m\in I,\ i=1, \ldots, r]$ mit den Relationen $x_i(m)^{p(e_i)} = 0$, falls $0 \leqq m_j < p(e_j - e_i)$, $(j = 1, \ldots, r)$, $x_i(m)^{p(e)} = 1$, falls $m = (0, \ldots, 0, \underset{i}{1}, 0, \ldots, 0)$ und $x_i(m)^{p(e)} = 0$ sonst.

$$\Delta(x_i(m)) = \sum \{x^\alpha \otimes ((\alpha))\, x_i(|\alpha|) / \alpha \in (\mathbb{N}^I)^r,\ \mathrm{gew}(\alpha) = m,\ |\alpha| \in I\}.$$

Für $m = 0$ erhält man:

$$x_i(0)^{p(e_i)} = 0,\ \forall i,$$

$$\Delta(x_i(0)) = \sum \{x(0)^{\alpha(0)} \otimes ((\alpha))\, x_i(\alpha(0)) / \alpha(0) \in I\}$$

(denn: $\mathrm{gew}(\alpha) = 0$ genau dann, wenn $\forall m \neq 0$, $\alpha_i(m) = 0$).

$$B := \bar{k}[x_1(0), \ldots, x_r(0)] \cong \bar{k}\otimes S.$$

$B \subset A$ ist frei, insbesondere treuflach, und $\Delta(B) \subset B\otimes A$. Damit sind die Voraussetzungen des Hilfssatzes (3.2.4) erfüllt. Es gibt also eine Untergruppe $\mathfrak{G}'$ von $\bar{k}\otimes\mathfrak{Aut}(S/k)_{(e)}$, so daß $B = A(\bar{k}\otimes\mathfrak{Aut}(S/k)_{(e)}/\mathfrak{G}')$. Insbesondere operiert $\bar{k}\otimes\mathfrak{Aut}(S/k)_{(e)}$ transitiv auf $\mathfrak{Sp}(\bar{k}\otimes S)$, und $\mathfrak{Aut}(S/k)_{(e)}$ operiert transitiv auf $\mathfrak{Sp}\, S$ (Satz (3.1.6)). □

(3.2.6) *Bemerkung.* Aus dem Beweis folgt, daß die Gruppe $\mathfrak{G}$ sogar endlich gewählt werden kann.

3.3. Existenz einer transitiven Operation

k sei ein Körper und $S \in \mathscr{A}\ell_k$.

(3.3.1) **Hilfssatz.** *$\mathfrak{Sp}\, S(k)$ sei nichtleer und die k-Gruppe $\mathfrak{G}$ operiere transitiv auf $\mathfrak{Sp}\, S$.*

Dann ist S_0 speziell über k.

Beweis. Nach Satz (3.1.6) gibt es eine Untergruppe $\mathfrak{G}'$ von $\mathfrak{G}$ mit $\mathfrak{Sp}\, S \cong \mathfrak{G}/\mathfrak{G}'$. Dann ist $\mathfrak{Sp}\, S_0 \cong (\mathfrak{G}/\mathfrak{G}')_0$.

Mittels der universellen Eigenschaften von $\mathfrak{G}/\mathfrak{G}'$ und $\mathfrak{G}_0$ kann gezeigt werden, daß $\mathfrak{G}_0/\mathfrak{G}'_0 \cong (\mathfrak{G}/\mathfrak{G}')_0$. Also ist $\mathfrak{G}_0/\mathfrak{G}'_0 \cong \mathfrak{Sp}\, S_0$ und die Behauptung folgt aus Satz (3.2.5). □

(3.3.2) *Bemerkung.* Im allgemeinen folgt aus „S_0 ist speziell über k" nicht, daß eine k-Gruppe existiert, die auf $\mathfrak{Sp}\,S$ transitiv operiert.

Gegenbeispiel. $S:=k\times k[z]$, $z^p=0$. $S_0\cong k[z]$, $z^p=0$, S_0 ist speziell über k. Satz (3.3.5) wird aber ergeben, daß auf $\mathfrak{Sp}\,S$ keine Gruppe transitiv operiert.

(3.3.3) **Hilfssatz.** *Es sei* $0\neq n\in\mathbb{N}$ *und* $T\in\mathscr{A}\ell_k$. *Wenn* $\mathfrak{Aut}(T/k)$ *transitiv auf* $\mathfrak{Sp}(T)$ *operiert, so operiert* $\mathfrak{Aut}(T^n/k)$ *transitiv auf* $\mathfrak{Sp}(T^n)$.

Beweis. 1) Es sei $R\in\mathscr{A}\ell_k$.

$T^n\otimes R\cong(T\otimes R)^n$ ist R-Algebrenisomorphismus,
$(t_1,\dots,t_n)\otimes r\mapsto(t_1\otimes r,\dots,t_n\otimes r)$

$\mathrm{Aut}(T\otimes R/R)$ wird durch

$$\begin{aligned}\mathrm{Aut}(T\otimes R/R)&\to\mathrm{Aut}((T\otimes R)^n/R)\\ f&\longmapsto(f,\dots,f)\end{aligned}$$

als Untergruppe von $\mathrm{Aut}(T^n\otimes R/R)$ aufgefaßt. Eine n-Permutation σ definiert einen Automorphismus $\tilde\sigma\in\mathrm{Aut}(T^n\otimes R/R)$ durch

$$\tilde\sigma(x_1\otimes 1,\dots,x_n\otimes 1):=(x_{\sigma^{-1}(1)}\otimes 1,\dots,x_{\sigma^{-1}(n)}\otimes 1).$$

2) Ist $x:=(x_1,\dots,x_n)\in^{\mathfrak{Aut}(T^n/k)}(T^n)$, so gilt insbesondere $\tilde\sigma(x\otimes 1)=x\otimes 1$, daher ist $\forall i,j\ x_i\otimes 1=x_j\otimes 1$, bzw. $x_i=x_j$. Außerdem: $\forall R$, $\forall f\in\mathrm{Aut}(T\otimes R/R)$,

$$(f,\dots,f)(x\otimes 1)=(f(x_1\otimes 1),\dots,f(x_1\otimes 1))=x\otimes 1.$$

Also ist $\forall R$, $\forall f\in\mathrm{Aut}(T\otimes R/R)$, $f(x_1\otimes 1)=x_1\otimes 1$. Nach Voraussetzung ist $^{\mathfrak{Aut}(T/k)}T=k$, daher ist $x_1\in k\subset T$ und $\left(\begin{array}{l}\text{nach Identifikation von } k \text{ mit } Bi(i),\\ i\colon k\to T^n\\ \quad 1\mapsto(1,\dots,1)\end{array}\right)$ $x\in k\subset T^n$.

3) Sei $\mathfrak{a}\trianglelefteq T^n$ ein $\mathfrak{Aut}(T^n/k)$-stabiles Ideal. Dann gilt insbesondere: $\forall R$, $\forall f\in\mathrm{Aut}(T\otimes R/R)$ ist $(f,\dots,f)(\mathfrak{a}\otimes R)=\mathfrak{a}\otimes R$. Daher ist $\mathrm{pr}_i(\mathfrak{a})$ $\mathfrak{Aut}(T/k)$-stabil. (pr_i bezeichnet die i-te Projektion von T^n nach T). Nach Voraussetzung ist dann $\mathrm{pr}_i(\mathfrak{a})=T$ oder $\mathrm{pr}_i(\mathfrak{a})=0$, $\forall i$, d.h.: $\mathfrak{a}$ ist isomorph zu einem Ideal der Form $0\times T^m$, $m\leqq n$. Weil $\mathfrak{a}$ unter allen $\tilde\sigma$, (σ n-Permutation), stabil ist, muß $\mathfrak{a}=0$ oder $\mathfrak{a}=T^n$ sein. □

(3.3.4) **Hilfssatz.** *Die folgenden Aussagen sind äquivalent:*

(1) *Es gibt eine k-Gruppe $\mathfrak{G}$, die transitiv auf $\mathfrak{Sp}\,S$ operiert.*
(2) *Es gibt eine spezielle Algebra $T\in\mathscr{A}\ell_{\bar k}$ und ein $n\in\mathbb{N}$, $n\neq 0$, so daß $\bar k\otimes S\cong T^n$.*

Beweis. (1)⇒(2): $\mathfrak{G}$ operiert transitiv auf $\mathfrak{Sp}S$, also auch $\bar k\otimes\mathfrak{G}$ auf $\mathfrak{Sp}(\bar k\otimes S)$. Da $\mathfrak{Sp}(\bar k\otimes S)(\bar k)$ nicht leer ist, sind die Voraussetzungen von Satz (3.3.1) erfüllt, daher ist $(\bar k\otimes S)_0$ speziell über $\bar k$. Setze $T:=(\bar k\otimes S)_0$.

$\bar k$ ist algebraisch abgeschlossen, somit ist $\bar k\otimes S=(\bar k\otimes S)_{et}\otimes(\bar k\otimes S)_0$ (vgl. (1.3.2)). Es gibt ein $n\neq 0$, so daß $(\bar k\otimes S)_{et}\cong\bar k^n$. Deshalb ist $\bar k\otimes S\cong\bar k^n\otimes T\cong T^n$.

(2)⇒(1): Nach Satz (3.2.5) operiert $\mathfrak{Aut}(T/k)$ transitiv auf $\mathfrak{Sp}\,T$. Nach (3.3.3) operiert dann auch $\mathfrak{Aut}(T^n/\bar k)\cong\mathfrak{Aut}(\bar k\otimes S/k)\cong\bar k\otimes\mathfrak{Aut}(S/k)$ transitiv auf $\mathfrak{Sp}(T^n)\cong\mathfrak{Sp}(\bar k\otimes S)$. Die Behauptung folgt aus Satz (3.1.6). □

(3.3.5) **Satz.** *k sei ein Körper und $S \in \mathscr{A}\ell_k$. $S_1, \ldots, S_n$ seien die lokalen Bestandteile von S $\left(dh.: S = \prod_{i=1}^{n} S_i,\ S_i \text{ lokal}\right)$ und $l_i := (S_i)_{et}$, $l := \prod_{i=1}^{n} l_i = S_{et}$. Dann sind die folgenden Aussagen äquivalent:*

(1) *Es gibt eine k-Gruppe $\mathfrak{G}$, die transitiv auf $\mathfrak{S}\mathfrak{p}S$ operiert.*

(2) *Es gibt Zahlen $r, e_1, \ldots, e_n \in \mathbb{N}$ mit $e_1 \geqq e_2 \geqq \cdots \geqq e_r > 0$, so daß für jedes $i \in \{1, \ldots, r\}$ gilt: Es existieren Elemente $z_1, \ldots, z_r \in S_i$ und Polynome $P_{ij} \in l_i[Z_1, \ldots, Z_{j-1}]$, so daß $S_i = l_i[z_1, \ldots, z_r]$ mit den Relationen*

$$z_j^{p(e_j)} = P_{ij}(z_1^{p(e_j)}, \ldots, z_{j-1}^{p(e_j)}), \qquad j = 1, \ldots, r.$$

(r und $(e_1, \ldots, e_r)$ sind von i unabhängig!)

(3) *$\forall j \in \mathbb{N}$ ist $\Omega(S^{[j]}/k)$ frei als $S^{[j]}$-Modul.*

Beweis. (1)⇒(3): Nach (3.3.4) gibt es eine spezielle Algebra $T \in \mathscr{A}\ell_{\bar{k}}$ und ein $n \in \mathbb{N}$, $n \neq 0$, so daß $\bar{k} \otimes S \cong T^n$.

Es sei $m \in \mathbb{N}$. Dann ist $\bar{k} \otimes S^{[m]} \cong (T^{[m]})^n$. T ist speziell, also ist $\Omega(T^{[m]}/k)$ ein freier $T^{[m]}$-Modul und $\bar{k} \otimes \Omega(S^{[m]}/k) \cong \Omega(T^{[m]}/\bar{k})^n$ ein freier $\bar{k} \otimes S^{[m]} \cong (T^{[m]})^n$-Modul. Mit dem Satz von Deuring-Noether [6; 29.11] folgt nun, daß $\Omega(S^{[m]}/k)$ $S^{[m]}$-frei ist.

(3)⇒(2): Die Erweiterung $S_{et} \subset S$ ist rein inseparabel. Also folgt die Behauptung unter Berücksichtigung von $\Omega(S/k) = \Omega(S/S_{et})$ direkt aus (2.2.10).

(2)⇒(1):

A) Beweis für „S lokal":

1) Weil S lokal ist, ist l ein Körper.

Sei $P := \sum_{i \in \mathbb{N}^r} a_i Z^i \in l[Z_1, \ldots, Z_r]$ und $\mathscr{A}\ell_k(l, \bar{k}) = \{\alpha_1, \ldots, \alpha_n\}$. $n = [l:k]$, weil $k \subset l$ separabel ist.

$P^{(j)}$ bezeichne dann das Polynom $\sum_{i \in \mathbb{N}^r} \alpha_j(a_i) Z^i \in \bar{k}[Z_1, \ldots, Z_r]$. Sei $T_j := \bar{k}[z_1, \ldots, z_r]$ mit den Relationen $z_i^{p(e_i)} = Q_{ij}(z_1^{p(e_i)}, \ldots, z_{i-1}^{p(e_i)})$ wobei $Q_{ij} := (P_i)^{(j)} \in \bar{k}[Z_1, \ldots, Z_{i-1}]$.

$\bar{k} \subset T_j$ ist also speziell.

2) Für jedes $j \in \{1, \ldots, n\}$ ist

$$f_j\colon \bar{k} \otimes l[z] \to T_j$$
$$\beta \otimes P(z) \mapsto \beta P^{(j)}(z)$$

wohldefiniert und Algebrenhomomorphismus.

Also ist auch

$$f\colon \bar{k} \otimes l[z] \to \prod_{j=1}^{n} T_j$$
$$\beta \otimes P(z) \mapsto (\beta P^{(j)}(z))_{j=1,\ldots,n}$$

ein Algebrenhomomorphismus.

Zeige: f ist Isomorphismus.

$l[z]$ hat die l-Basis $\{z^m / m \in I\}$; $I := \{m \in \mathbb{N}^r / m_i < p(e_i), \forall i\}$.

Ist also $f(\sum_i a_i \otimes (\sum_{j \in I} b_{ij} z^j)) = 0$, $a_i \in \bar{k}$, $b_{ij} \in l$, so ist $\forall s \in \{1, \ldots, n\}$ $\sum_j (\sum_i a_i \alpha_s(b_{ij})) z^j = 0$ und daher $\forall j \in I$, $\forall s$, $\sum_i a_i \alpha_s(b_{ij}) = 0$.

Aber

$$\bar{k}\otimes l \xrightarrow{\cong} \bar{k}^n$$
$$\sum_i a_i\otimes b_{ij} \mapsto (\sum_i a_i\alpha_s(b_{ij}))_{s=1,\dots,n}$$

ist Isomorphismus, deshalb ist $\forall j\in I$ $\sum_i a_i\otimes b_{ij}=0$.

Also ist f injektiv.

$$[\bar{k}\otimes S:\bar{k}]=[S:k]=[S:l]\,[l:k]=p\left(\sum_{i=1}^r e_i\right)n,$$

$$\left[\prod_{j=1}^n T_j:\bar{k}\right]=\sum_{j=1}^n [T_j:\bar{k}]=np\left(\sum_{i=1}^r e_i\right).$$

Daher ist $[\bar{k}\otimes S:\bar{k}]=\left[\prod_{j=1}^n T_j:\bar{k}\right]$.

Eine injektive Abbildung zwischen Vektorräumen gleicher Dimension ist auch surjektiv, daher ist f Isomorphismus.

3) $\bar{k}\subset T_j$ ist speziell und $\bar{k}$ ist perfekt, also folgt aus (2.1.12): Es existieren Elemente $y_1,\dots,y_r\in T_j$, so daß $T_j=\bar{k}[y_1,\dots,y_r]$ mit den Relationen $y_i^{p(e_i)}=0$, $i=1,\dots,r$. Weil $(e_1,\dots,e_r)$ und r von j nicht abhängen, gilt: $T_i\cong T_j$, $\forall i,j$.

Zusammen mit 2) folgt daraus: $\bar{k}\otimes S\cong T_1^n$ und die Behauptung folgt aus (3.3.4).

B) Allgemeiner Beweis: Aus A) und (3.3.4) folgt: Für jedes i gibt es eine spezielle Algebra T_i und ein $n_i\in\mathbb{N}$, $n_i\neq 0$, so daß $\bar{k}\otimes S_i\cong T_i^{n_i}$.

T_i hat die Gestalt $\bar{k}[z_1,\dots,z_r]$, $z_j^{p(e_j)}=0$. Weil r und $(e_1,\dots,e_r)$ nach Voraussetzung von i nicht abhängen, gilt: $T_i\cong T_j$, $i,j=1,\dots,n$.

Also ist $\bar{k}\otimes S\cong T_1^m$, $m:=\sum_i n_i$, und die Behauptung folgt aus (3.3.4). □

(3.3.6) **Folgerung.** Ist $k\subset K$ eine endliche Körpererweiterung, so ist $^{\mathfrak{Aut}(K/k)}K=k$.

Beweis. $K_{et}\subset K$ ist speziell (2.1.4). □

(3.3.7) *Bemerkung.* Rasala beweist in [14; II, Th. 5]: $\bar{k}\otimes S$ ist isomorph zu einem Produkt von über $\bar{k}$ speziellen Algebren genau dann, wenn alle lokalen Bestandteile S_i von S speziell über $(S_i)_{et}$ sind.

3.4. Verallgemeinerung des Satzes von Cartier-Dieudonné

Der Satz von Cartier-Dieudonné [7; III, 3,6.1] klassifiziert die affinen Algebren von endlichdimensionalen Quotienten von k-Gruppen über perfektem Grundkörper.

Die Sätze (3.1.6) und (3.3.5) ermöglichen eine Verallgemeinerung auf beliebigen Grundkörper.

(3.4.1) **Satz.** Die affinen Algebren endlicher homogener Räume über einem Körper k haben die Gestalt $S=\prod_{i=1}^n S_i$ mit

1) S_i lokal,

2) S ist speziell über $(S_i)_{et}$ und die zugehörigen Zahlen $r, e_1, \ldots, e_r$ sind von i unabhängig.

3) $\exists j \in \{1, \ldots, n\}$, $S_j/J(S_j) \cong k$.

Beweis. 1) und 2) sind genau dann erfüllt, wenn es eine k-Gruppe G gibt, die transitiv auf $\mathfrak{Sp}S$ operiert (3.3.5). Dann ist 3) die Bedingung dafür, daß $\mathfrak{Sp}S(k)$ nicht leer ist. Also folgt die Behauptung aus (3.1.6). □

3.5. Transitive Operationen über beliebigem Grundring

(3.5.1) **Definition.** Es sei $k \in \mathscr{R}i$, $\mathfrak{G}$ eine k-Gruppe und $\mathfrak{X}$ ein endliches k-Schema. $\mathfrak{G}$ operiere durch Op: $\mathfrak{X} \times \mathfrak{G} \to \mathfrak{X}$ auf $\mathfrak{X}$.

Die Operation Op ist transitiv genau dann, wenn für jedes $\mathfrak{m} \in \operatorname{Max}(k)$ $k/\mathfrak{m} \otimes Op$ transitiv ist (im Sinne von Definition (3.1.3)).

(3.5.2) **Satz.** *Es sei $k \in \mathscr{R}i$ und S eine endlich projektive Algebra in $\mathscr{A}\ell_k$. $\mathfrak{G}$ sei eine endlich projektive k-Gruppe, $H := \operatorname{Hom}_k(A, k)$ und durch Δ: $S \to S \otimes A$ sei eine Operation von $\mathfrak{G}$ auf $\mathfrak{Sp}S$ gegeben. Die Δ bezüglich des Isomorphismus*

$$\operatorname{Hom}_k(S, S \otimes A) \cong \operatorname{Hom}_k(H \otimes S, S)$$

entsprechende Moduloperation sei

$$\begin{aligned} \mu\colon\ & H \otimes S \to S \qquad \text{(vgl. (1.2.2))}. \\ & h \otimes s \mapsto h \circ s \end{aligned}$$

Dann sind die folgenden Aussagen äquivalent:

(1) Die Operation von $\mathfrak{G}$ auf $\mathfrak{Sp}S$ ist transitiv.

(2) kan: $H \otimes S \to \operatorname{End}_k(S)$ ist surjektiv.

$$h \otimes s \mapsto (h \circ (-))s$$

Beweis. Nach [4; 5.3, Prop. 7, (i)] erhält man das Diagramm

$$\begin{array}{ccc} \operatorname{Hom}_S(S \otimes A, S \otimes S) & \xrightarrow{\operatorname{Hom}((\operatorname{Inj}, \Delta), S \otimes S)} & \operatorname{Hom}_S(S \otimes S, S \otimes S) \\ \wr\| & & \wr\| \\ H \otimes S \otimes S & \xrightarrow{\operatorname{kan} \otimes S} & \operatorname{End}_k(S) \otimes S \end{array}$$

S-linearer Abbildungen, dieses ist kommutativ:

$$\begin{array}{ccc} f & \longmapsto & f(\operatorname{Inj}, \Delta): \\ \downarrow & & \downarrow \\ h \otimes m & \longmapsto & m(h \circ (-)) \quad f\Delta \end{array}$$

$(f(t \otimes a) = m\,t\,h(a), \forall t \in S, a \in A)$

$$m(h \circ s) = m \sum_{(s)} s_1 h(s_2) = \sum_{(s)} f(s_1 \otimes s_2) = f\Delta(s).$$

Also ist $\mathrm{kan}\otimes S$ surjektiv genau dann, wenn $\mathrm{Hom}((\mathrm{Inj}, \Delta), S\otimes S)$ surjektiv ist.
(1)⇒(2): $\forall \mathfrak{m}\in \mathrm{Max}(k)$ besitzt $k/\mathfrak{m}\otimes(\mathrm{Inj}, \Delta)$ eine Retraktion, dh.: $\mathrm{Hom}(k/\mathfrak{m}\otimes(\mathrm{Inj}, \Delta), k/\mathfrak{m}\otimes S\otimes S)$ ist surjektiv (3.1.6). Aus dem Lemma von Nakayama folgt: $\mathrm{Hom}((\mathrm{Inj}, \Delta), S\otimes S)$ ist surjektiv. Also ist $\mathrm{kan}\otimes S$ surjektiv. Da $k\subset S$ treuflach ist, ist auch kan surjektiv.
(2)⇒(1): kan ist surjektiv, also auch $\mathrm{kan}\otimes S$ und somit $\mathrm{Hom}(k/\mathfrak{m}\otimes(\mathrm{Inj}, \Delta), k/\mathfrak{m}\otimes S\otimes S)$, $\forall \mathfrak{m}\in \mathrm{Max}(k)$. Die Behauptung folgt aus Definition (3.4.1) und Satz (3.1.6). □

(3.5.3) **Satz.** *Es sei $k\in\mathcal{R}i$ und $S\in\mathcal{A}lf_k$. Die folgenden Aussagen sind äquivalent:*

(1) i) Es gibt eine geometrisch zusammenhängende k-Gruppe $\mathfrak{G}$ (dh.: Ist K ein algebraisch abgeschlossener Körper und $k\to K$ ein Morphismus, so ist $K\otimes_k\mathfrak{G}$ eine zusammenhängende K-Gruppe), die transitiv auf $\mathfrak{Sp}S$ operiert.

ii) $k\subset S$ ist endlich projektiv.

iii) $\forall m\in\mathbb{N}$, $S^{[m]}|_k S$.

(2) S ist speziell über k.

Beweis. (1)⇒(2): $\mathfrak{G}$ operiert transitiv auf $\mathfrak{Sp}S$, dh.: $\forall \mathfrak{m}\in \mathrm{Max}(k)$ operiert $k/\mathfrak{m}\otimes\mathfrak{G}$ transitiv auf $\mathrm{Sp}(k/\mathfrak{m}\otimes S)$. $\overline{k/\mathfrak{m}}$ sei der algebraische Abschluß von $k/\mathfrak{m}$. Da $\mathfrak{G}$ geometrisch zusammenhängend ist, ist $\overline{k/\mathfrak{m}}\otimes_k\mathfrak{G}=\overline{k/\mathfrak{m}}\otimes_{k/\mathfrak{m}}(k/\mathfrak{m}\otimes_k\mathfrak{G})$ zusammenhängend, also auch $k/\mathfrak{m}\otimes\mathfrak{G}$.

Nach Satz (3.2.5) ist somit für jedes $\mathfrak{m}\in\mathrm{Max}(k)$ $k/\mathfrak{m}\otimes S$ speziell über $k/\mathfrak{m}$.

$k/\mathfrak{m}\otimes S$ ist insbesondere rein inseparabel, also gibt es ein $m\in\mathbb{N}$, so daß $(k/\mathfrak{m}\otimes S)^{[m]}=k/\mathfrak{m}$. $S^{[m]}$ ist k-direkter Summand von S, daher ist $(k/\mathfrak{m}\otimes S)^{[m]}=k/\mathfrak{m}\otimes S^{[m]}=S^{[m]}/\mathfrak{m}S^{[m]}$. $S^{[m]}=k+\mathfrak{m}S^{[m]}$, somit folgt aus dem Lemma von Nakayama: $S^{[m]}=k$, d.h.: S ist rein inseparabel. Zusammen mit (ii) und (iii) folgt nun die Behauptung aus Satz (2.2.5).
(2)⇒(1): 1) (ii) und (iii) sind nach Hilfssatz (2.2.4) erfüllt.

2) *Annahme:* Es gibt eine Zerlegung $k=k\varepsilon_1\times\cdots\times k\varepsilon_n$, $k_i:=k\varepsilon_i$, so daß $S=\prod_{i=1}^{n}S\varepsilon_i$, $S_i:=S\varepsilon_i$, und $S_i=k_i[z_1,\ldots,z_{r(i)}]$ mit den Relationen $z_j^{p(e_j(i))}=0$, $j=1,\ldots,r(i)$, $e_1(i)\geqq\cdots\geqq e_{r(i)}(i)>0$.

Ist $\mathfrak{m}\in\mathrm{Max}(k)$, so gibt es ein $i=i(\mathfrak{m})\in\{1,\ldots,n\}$ und ein $\mathfrak{n}_i\in\mathrm{Max}(k_i)$ derart, daß $\mathfrak{m}=\prod_{j\neq i}k_j\times\mathfrak{n}_i$. Daher ist $k/\mathfrak{m}\otimes S\cong k_i/\mathfrak{n}_i\otimes S_i\cong k_i/\mathfrak{n}_i[z_1,\ldots,z_{r(i)}]$, $z_j^{p(e_j(i))}=0$, $j=1,\ldots,r(i)$.

Aus Satz (3.2.5) und Bemerkung (3.2.6) folgt, daß $\mathfrak{Aut}(k/\mathfrak{m}\otimes S/k/\mathfrak{m})_{(e_1(i(\mathfrak{m})))}$ transitiv auf $\mathfrak{Sp}(k/\mathfrak{m}\otimes S)$ operiert.

Es sei $e:=\max\{e_1(i)/i=1,\ldots,n\}$. Dann gilt für alle $\mathfrak{m}\in\mathrm{Max}(k)$: $\mathfrak{Aut}(k/\mathfrak{m}\otimes S/k/\mathfrak{m})_{(e)}$ operiert transitiv auf $\mathfrak{Sp}(k/\mathfrak{m}\otimes S)$.

Da S nach Voraussetzung endlich projektiv ist, ist $\mathfrak{Aut}(S/k)$ affin und algebraisch.

$k/\mathfrak{m}\otimes\mathfrak{Aut}(S/k)\cong\mathfrak{Aut}(k/\mathfrak{m}\otimes S/k/\mathfrak{m})$, also auch $k/\mathfrak{m}\otimes\mathfrak{Aut}(S/k)_{(e)}\cong\mathfrak{Aut}(k/\mathfrak{m}\otimes S/k/\mathfrak{m})_{(e)}$.

$\forall \mathfrak{m}\in\mathrm{Max}(k)$ operiert daher $k/\mathfrak{m}\otimes\mathfrak{Aut}(S/k)_{(e)}$ transitiv auf $k/\mathfrak{m}\otimes\mathfrak{Sp}S$, d.h.: $\mathfrak{Aut}(S/k)_{(e)}$ operiert transitiv auf $\mathfrak{Sp}S$.

3) S ist speziell, also existiert nach Satz (2.2.9) eine treuflache Ringerweiterung $k\subset l$, so daß $l\otimes S$ von der in 2) vorausgesetzten Gestalt ist.

Somit gibt es ein $e \in \mathbb{N}$ derart, daß $\mathfrak{Aut}(l \otimes S/l)_{(e)} \cong l \otimes \mathfrak{Aut}(S/k)_{(e)}$ transitiv auf $\mathfrak{Sp}(l \otimes S) \cong l \otimes \mathfrak{Sp} S$ operiert. Es seien $l = \prod_{i=1}^{n} l_i$ und $(l \otimes S) = \prod_{i=1}^{n} (l \otimes S)_i$ Zerlegungen wie in 2).

Es ist $\mathfrak{Aut}(l \otimes S/l)_{(e)} \cong \prod_{i=1}^{n} \mathfrak{Aut}((l \otimes S)_i/l_i)_{(e)}$.

Nach (3.2.2) ist für jedes i die Gruppe $\mathfrak{Aut}((l \otimes S)_i/l_i)_{(e)}$ endlich projektiv.

Somit sind auch $l \otimes \mathfrak{Aut}(S/k)_{(e)}$ und (weil $k \subset l$ treuflach ist) $\mathfrak{Aut}(S/k)_{(e)}$ endlich projektiv.

Es sei $A := A(\mathfrak{Aut}(S/k)_{(e)})$ und $H := \mathrm{Hom}_k(A, k)$. Nach Satz (3.5.2) ist $l \otimes \mathrm{kan}\colon l \otimes H \otimes S \to \mathrm{End}_l(l \otimes S)$ surjektiv. Da $k \subset l$ treuflach ist, ist auch kan surjektiv, nach (3.5.2) operiert also $\mathfrak{Aut}(S/k)_{(e)}$ transitiv auf $\mathfrak{Sp} S$.

$\mathfrak{Aut}(S/k)_{(e)}$ ist von endlicher Höhe, also insbesondere geometrisch zusammenhängend. □

(3.5.4) *Bemerkung.* Nach Satz (2.2.9) ist S speziell über k genau dann, wenn es eine treuflache Ringerweiterung $k \subset l$ und eine Zerlegung $k = k_1 \times \cdots \times k_n$ bzw. $S = S_1 \times \cdots \times S_n$ gibt, so daß $l \otimes S_i \cong l_i[z_1, \ldots, z_{r(i)}]$, $z_j^{p(e_j(i))} = 0$. Deshalb ergeben die Sätze (3.5.2) und (3.5.3) eine Verallgemeinerung eines Teiles eines Satzes von Knus und Ojanguren [12; II, Theorem 7.8] (für Höhe 1) auf beliebige Höhe.

4. Das Zentroid einer Algebra, auf der eine Gruppe ohne stabile Ideale operiert

k sei ein algebraisch abgeschlossener Körper und A eine beliebige (nicht notwendig kommutative oder assoziative) endlichdimensionale Algebra mit $A^2 = A$.

(4.1) **Hilfssatz.** *Es sei $S \in \mathscr{A}\ell_k$ und $\mathfrak{G}$ eine k-Gruppe, die auf $\mathfrak{Sp} S$ operiert. S besitze kein $\mathfrak{G}$-stabiles Ideal. Dann operiert $\mathfrak{G}$ transitiv auf $\mathfrak{Sp} S$.*

Beweis. Zeige: ${}^{\mathfrak{G}}S = k$.

Ist $x \in {}^{\mathfrak{G}}S$, so ist Sx ein $\mathfrak{G}$-stabiles Ideal. Nach Voraussetzung ist daher $Sx = 0$ oder $Sx = S$, d.h.: $x = 0$ oder x ist invertierbar. Also ist ${}^{\mathfrak{G}}S$ ein Körper. Weil k algebraisch abgeschlossen ist, ist ${}^{\mathfrak{G}}S = k$. □

(4.2) **Definition.** $C(A) := \mathrm{End}({}_A A) \cap \mathrm{End}(A_A)$ heißt *Zentroid* von A.

(4.3) *Bemerkung.* $C(A)$ ist eine kommutative Algebra. [2; VI, 1, Th. 3].

(4.4) **Satz.** *$\mathfrak{G}$ sei eine k-Gruppe und $\rho\colon \mathfrak{G} \to \mathfrak{Aut}(A/k)$ ein Morphismus von k-Gruppen.*

Annahme. $\mathfrak{G}$ läßt keine echten Ideale von A stabil, d.h.: Ist $\mathfrak{a}$ ein echtes Ideal von A, so gibt es ein $R \in \mathscr{A}\ell_k$ und ein $f \in \mathfrak{G}(R)$ derart, daß $\rho_R(f)(\mathfrak{a} \otimes R) \not\subset \mathfrak{a} \otimes R$.

Behauptung. $\mathfrak{G}$ operiert transitiv auf $\mathfrak{Sp}\, C(A)$.

Beweis.

1) $\mathrm{Int}\colon \mathfrak{Aut}(A/k) \longrightarrow \mathfrak{Aut}(C(A)/k)$

$$f \longmapsto \mathrm{Int}_f \qquad \mathrm{Int}_f(g) := f g f^{-1}|_{C(A)}$$

ist ein Morphismus, also operiert $\mathfrak{G}$ durch $\mathrm{Int} \circ \rho$ auf $\mathfrak{Sp}(C(A))$.

2) Zeige: Ist $\mathfrak{a} \trianglelefteq C(A)$ $\mathfrak{G}$-stabil, so ist $\mathfrak{a}A(:=\sum_{g\in\mathfrak{a}} g(A))$ ein Ideal von A und $\mathfrak{G}$-stabil.

Ist $g\in\mathfrak{a}$ und $a, b\in A$, so ist $ag(b)=g(ab)=g(a)b$, also ist $\mathfrak{a}A$ ein Ideal von A.

Es sei

$$R\in\mathscr{A}\ell_k, \quad f\in\rho_R(\mathfrak{G}(R)) \quad \text{und} \quad \sum_{g\in\mathfrak{a}} g(a_g)\otimes r_g\in \mathfrak{a}A\otimes R.$$

$$f(\sum_{g\in\mathfrak{a}} g(a_g)\otimes r_g)=\sum_{g\in\mathfrak{a}} f(g\otimes\mathrm{id})(a_g\otimes r_g)=(*)$$

f ist bijektiv, also existiert für jedes $g\in\mathfrak{a}$ ein $b_g\in A\otimes R$ mit $f^{-1}(b_g)=a_g\otimes r_g$.

$$(*)=\sum_{g\in\mathfrak{a}} f(g\otimes\mathrm{id})\, f^{-1}(b_g)$$

$f(g\otimes\mathrm{id})\, f^{-1}$ ist nach Voraussetzung wieder in $\mathfrak{a}\otimes R$, also ist $(*)\in\mathfrak{a}A\otimes R$.

3) Zeige: Ist $\mathfrak{a}$ ein echtes Ideal von $C(A)$, so ist $\mathfrak{a}A$ ein echtes Ideal von A.

Annahme. $\mathfrak{a}A=A$.

Wegen $A=A^2$ gilt: $\forall m\in\mathbb{N}$ ist $(\mathfrak{a}A)^m=A^m=A$. Wegen $fg(ab)=f(a)\,g(b)$, $\forall f, g\in C(A)$, $\forall a, b\in A$, gilt andererseits: $(\mathfrak{a}A)^m=\mathfrak{a}^m A^m=\mathfrak{a}^m A$.

Also ist auch $\mathfrak{a}^m A=A$, $m\in\mathbb{N}$.

Wegen $C(A)\in\mathscr{A}\ell_k$ und $\mathfrak{a}^m\subset C(A)^m$ gibt es ein $m\in\mathbb{N}$, so daß $\mathfrak{a}^m\subset C(A)_{et}$. Ist $\{\varepsilon_i/i\in I\}$ eine Familie vollständiger orthogonaler Idempotenter in $C(A)_{et}$, so gibt es wegen $\mathfrak{a}\ntrianglelefteq C(A)$ ein $i_0\in I$, so daß $\varepsilon_{i_0}\neq 0$ und $\mathfrak{a}^m\leqq\sum_{i\neq i_0} k\varepsilon_i$. Da $\mathfrak{a}^m A=A$ ist, folgt:

$$\sum_{i\neq i_0}\varepsilon_i A=A=(\sum_{i\in I}\varepsilon_i)A \quad \text{und} \quad 0=\varepsilon_{i_0}(\sum_{i\neq i_0}\varepsilon_i A)=\varepsilon_{i_0}(\sum_{i\in I}\varepsilon_i A)=\varepsilon_{i_0}A.$$

Also ist $\varepsilon_{i_0}(a)=0$, $a\in A$, d.h.: $\varepsilon_{i_0}=0$. Widerspruch.

4) Nach 2) und 3) besitzt $C(A)$ keine $\mathfrak{G}$-stabilen Ideale. Nach Hilfssatz (4.1) operiert $\mathfrak{G}$ transitiv auf $C(A)$. □

(4.5) **Spezialfall.** Die durch

$$\begin{aligned} \mathrm{Der}_k(A)\,x\,A &\to A \\ (d, a) &\mapsto d(a) \end{aligned}$$

gegebene Operation von $\mathrm{Der}_k(A)$ auf A induziert $U_p(\mathrm{Der}_k(A))\otimes A\to A$ und somit eine Operation von $\mathfrak{Aut}(A/k)_{(1)}$ auf A.

Ein Ideal $\mathfrak{a}$ von A heißt $\mathrm{Der}_k(A)$-Ideal, falls $\forall d\in\mathrm{Der}_k(A)$, $d(\mathfrak{a})\subset\mathfrak{a}$. Man sieht leicht, daß ein Ideal genau dann ein $\mathrm{Der}_k(A)$-Ideal ist, wenn es $\mathfrak{Aut}(A/k)_{(1)}$-stabil ist.

A heißt *differenzierbar einfach*, wenn es keine (echten) $\mathrm{Der}_k(A)$-Ideale gibt bzw. wenn es keine $\mathfrak{Aut}(A/k)_{(1)}$-stabilen Ideale gibt.

Ist A eine kommutative Algebra, so ist

$$\begin{aligned} C(A) &\cong A. \\ f &\mapsto f(1) \end{aligned}$$

Aus den Sätzen (4.4) und (3.2.5) folgt unmittelbar das Hauptergebnis einer Arbeit von Harper [10]:

(4.6) **Satz.** *Ist k algebraisch abgeschlossen und $A=A^2$ eine endlich dimensionale differenzierbar einfache kommutative Algebra, so ist A isomorph zu $k[Z_1,\ldots,Z_n]/\langle Z_1^p,\ldots,Z_n^p\rangle$.*

(4.7) *Bemerkung.* Das allgemeinste Ergebnis über differenzierbar einfache Algebren stammt von Block [3]:

Satz. *Ist A eine differenzierbar einfache Algebra über einem Ring k und besitzt A ein minimales Ideal, so gibt es eine einfache Algebra E, so daß $A\cong E\otimes C(A)$ und $C(A)$ ist isomorph zu $k[Z_1,\ldots,Z_n]/\langle Z_1^p,\ldots,Z_n^p\rangle$.*

5. Fixmengen

k sei ein Körper.

(5.1) **Satz.** *Es sei $S\in\mathscr{A}\ell\mathscr{f}_k$ und $\mathfrak{G}$ eine k-Gruppe, die auf $\mathfrak{S}\mathfrak{p}S$ operiert.*
Ist ${}^{\mathfrak{G}}S=k$, so gibt es ein $n\in\mathbb{N}$ und eine lokale Algebra $T\in\mathscr{A}\ell\mathscr{f}_{\bar{k}}$, so daß $\bar{k}\otimes S\cong T^n$.

Beweis. 1) ${}^{\mathfrak{Aut}(S/k)}S=k$ genau dann, wenn ${}^{\bar{k}\otimes\mathfrak{Aut}(S/k)}(\bar{k}\otimes S)=\bar{k}$. Also sei im folgenden o.E.d.A. k algebraisch abgeschlossen.

$A:=A(\mathfrak{Aut}(S/k))$ sei die affine Algebra von $\mathfrak{Aut}(S/k)$. Wegen (1.2.1) ist ${}^{\mathfrak{Aut}(S/k)}S=\{s\in S/\forall f\in\mathrm{Aut}(S\otimes A/A),\ \ f(s\otimes 1)=s\otimes 1\}$.

2) A ist noethersch, daher existiert eine endliche Zerlegung $A=\prod_{j=1}^{m}A_j$ in direkt unzerlegbare Faktoren A_j. $A_j=:Af_j$, f_j idempotent.

$S=\prod_{i=1}^{m}S_i$ sei die Zerlegung von S in lokale Faktoren.

$S_i=:Se_i$, e_i idempotent.

Also ist $S\otimes A=\prod_{i,j}S_i\otimes A_j$ eine Zerlegung in direkt unzerlegbare Faktoren. Das zu $S_i\otimes A_j$ gehörige Idempotent ist $e_i\otimes f_j$.

3) Es sei $g\in\mathrm{Aut}(S\otimes A/A)$. Dann gibt es zu jedem Paar (i,j) ein Paar (k,l), so daß $g(e_i\otimes f_j)=e_k\otimes f_l$. Wegen $g(e_i\otimes f_j)=g(e_i\otimes 1)(1\otimes f_j)$ muß $j=l$ sein.

Insbesondere gibt es eine Permutation α, so daß $g(e_i\otimes f_1)=e_{\alpha(i)}\otimes f_1$.

Da g ein Automorphismus ist, ist $S_i\otimes A_1$ isomorph zu $S_{\alpha(i)}\otimes A_1$. O.E.d.A. seien $S_1\otimes A_1, S_2\otimes A_1,\ldots,S_r\otimes A_1$ die zu $S_1\otimes A_1$ isomorphen Komponenten von $S\otimes A_1$.

Dann gilt für jedes

$$g\in\mathrm{Aut}(S\otimes A/A):\ g\left(\sum_{i=1}^{r}e_i\otimes f_1\right)=\sum_{i=1}^{r}e_i\otimes f_1.$$

Nach Voraussetzung ist daher $\sum_{i=1}^{r}e_i\in k$, also $r=n$ und $S\otimes A_1\cong(S_1^n\otimes A_1)$.

4) Es sei $R\in\mathscr{A}\ell_k$. Der Funktor $\mathfrak{X}:=\mathfrak{Isom}(S,S_1^n)$ ist durch $\mathfrak{X}(R):=$(Menge der R-Algebrenisomorphismen von $S\otimes R$ nach $S_1^n\otimes R$) definiert.

$\mathfrak{X}$ ist algebraisch und affin. Nach 3) ist $\mathfrak{X}(A_1)\neq\Phi$, also auch $\mathfrak{X}\neq\Phi$.

Da k algebraisch abgeschlossen ist, ist $\mathfrak{X}(k)\neq\Phi$, d.h.: S und S_1^n sind isomorph. □

(5.2) **Satz.** *k sei algebraisch abgeschlossen. $\mathfrak{a}$ sei ein homogenes Ideal von $k[Z_1, \ldots, Z_n]$ derart, daß $S := k[Z_1, \ldots, Z_n]/\mathfrak{a}$ lokal und endlich dimensional ist.*

Dann sind in ${}^{\mathrm{Aut}(S/k)}S := \{x \in S / \forall f \in \mathrm{Aut}(S/k)$ ist $f(x) = x\}$ nur die Elemente von k enthalten.

Beweis. Es sei $S = k[z_1, \ldots, z_n]$ mit den Relationen $P_i(z) := P_i(z_1, \ldots, z_n) = 0$; $i = 1, \ldots, r$. Die Polynome P_i seien homogen vom Grad d_i. Ist $\alpha \in k$, so ist $P_i(\alpha z) = \alpha^{d_i} P_i(z) = 0$.

Somit ist die Abbildung

$$f_\alpha\colon S \to S$$
$$z_j \mapsto \alpha z_j$$

wohldefiniert. Für $\alpha \neq 0$ gilt: $f_\alpha \in \mathrm{Aut}(S/k)$.

$\{z^i / i \in I \subset \mathbb{N}^n\}$ sei eine k-Basis von S.

Annahme. $x := \sum_{i \in I} a_i z^i \in {}^{\mathrm{Aut}(S/k)}S$ $(a_i \in k)$. Dann ist insbesondere $f_\alpha(x) = x$. Es ist $f_\alpha(\sum_{i \in I} a_i z^i) = \sum_{i \in I} a_i \alpha^{|i|} z^i$. Somit ist $\sum_{i \in I} a_i(\alpha^{|i|} - 1) z^i = 0$. Wähle α so, daß für alle $i \neq 0$ gilt: $\alpha^{|i|} \neq 1$. Dann ist für jedes $i \neq 0$ der Koeffizient a_i gleich 0, d.h.: $x = a_0 \in k$. □

(5.3) *Bemerkung.* Um die Umkehrung von Satz (5.1) zu beweisen, würde es genügen, sie für den Fall, daß k algebraisch abgeschlossen und S lokal ist, zu beweisen. Unter den in Satz (5.2) gemachten zusätzlichen Voraussetzungen gilt sie also, aber nicht allgemein.

Gegenbeispiel. k sei algebraisch abgeschlossen und von der Charakteristik $p > 7$.

$S := k[x, y]$ mit den Relationen $3x^2 + y^5 = 0$, $7y^6 + 5xy^4 = 0$.

Das Element y^7 ist nicht in k, aber $y^7 \in {}^{\mathfrak{Aut}(S/k)}S$.

Literatur

1. Bass, H.: Big projective modules are free. Illinois J. Math. **7**, 24–31 (1963)
2. Behrens, E.-A.: Ring Theory. New York: Academic Press 1972
3. Block, R.: Differentiably simple rings. Ann. of Math., II. Ser. **90**, 433–459 (1969)
4. Bourbaki, N.: Algèbre. Chapitres 1 à 3. Paris: Hermann 1970
5. Bourbaki, N.: Algèbre commutative. Chapitre 1 et 2. Paris: Hermann 1961
6. Curtis, C., Reiner, I.: Representation theory of finite groups and associative algebras. New York: John Wiley & Sons 1962
7. Demazure, M., Gabriel, P.: Groupes algèbriques. Paris: Masson 1970
8. Demazure, M., Grothendieck, A.: Schémas en groupes I. Lecture Notes in Mathematics 151. Berlin-Heidelberg-New York: Springer 1970
9. Grothendieck, A.: Éléments de géométrie algébrique IV. Publications Mathématiques Nr. 20. Bures-sur-Yvette: Presses Universitaires de France 1964
10. Harper, L.: On differentiably simple algebras. Trans. Amer. Math. Soc. **100**, 63–72 (1961)
11. Kiehl, R., Kunz, E.: Vollständige Durchschnitte und p-Basen. Arch. der Math. **16**, 348–362 (1965)
12. Knus, M.-A., Ojanguren, M.: Théorie de la Descente et Algèbres d'Azumaya. Lecture Notes in Mathematics 389. Berlin-Heidelberg-New York: Springer 1974

13. Oberst, U.: Affine Quotientenschemata nach affinen algebraischen Gruppen und induzierte Darstellungen. J. Algebra **44**, 503 – 538 (1977)
14. Rasala, R.: Inseparable splitting theory. Trans. Amer. Math. Soc. **162**, 411 – 448 (1971)
15. Reiner, I.: Maximal Orders. New York: Academic Press 1975.
16. Sweedler, M.: Hopf Algebras. New York: Benjamin 1970

Eingegangen am 27. Oktober 1977