Lineare algebraische Gruppen

Vorlesungsreihe vom Sommersemester 2021
Fakultät für Mathematik, Universität Leipzig
frei nach
T.A.Springer: Linear algebraic groups
Birkhäuser-Verlag, Boston 1981
(zweite Auflage 1998)

Ort der Vorlesung: Seminargebäude, Raum 2-14
Zeit der Vorlesung: 13.15-14.45 Uhr Freitags

3 Kommutative algebraische Gruppen

3.1 Die Struktur der kommutativen algebraischen Gruppen

Dieses Kapitel beschäftigt sich mit Ergebnissen zur Theorie der kommutativen linearen algebraischen Gruppen, welche grundlegend sind für die in den nachfolgenden Kapiteln dargelegte Theorie. Die besonders wichtigen Tori werden in 3.2 eingeführt und in 3.4.9 beweissen wir den Klassifikationssatz für zusammenhängende eindimensionale Gruppen. Wir verwenden die Bezeichnungen des vorangehenden Kapitels.

3.1.1 Satz: Produkt-Zerlegung der kommutativen algebraischen Gruppen

Sei G eine kommutative lineare algebraische Gruppe. Dann gelten die folgenden Aussagen.

(i) Die Mengen G_s und G_u der halbeinfachen bzw. unipotenten Elemente von G sind abgeschlossene Untergruppen.

(ii) Die Produkt-Abbildung $\pi: G_s \times G_u \longrightarrow G, (x,y) \mapsto x \bullet y$, ist ein Isomorphismus von algebraischen Gruppen.

Beweis. Zu (i). Nach 2.4.3 sind G_s und G_u im kommutativen Fall Untergruppen von G. Es bleibt zu zeigen, daß diese Untergruppen abgeschlossen sind. Dazu können wir annehmen, G ist eine abgeschlossene Untergruppe einer allgemeinen linearen Gruppe, sagen wir

$$G \hookrightarrow \mathbf{GL}_n$$

(nach 2.3.7 und 2.4.8(ii)). Nach 2.4.10, Aufgabe 2, ist G_u abgeschlossen in G.

Nach 2.4.2(ii) und 2.4.8 (iii) gibt es eine Basis von

$$V := k^n,$$

welche aus Eigenvektoren besteht bezüglich aller Matrizen

$$g \in G_s \ (\subseteq G \subseteq \mathbf{GL}_n).$$

Mit anderen Worten, V zerfällt in eine direkte Summe

$$V = \oplus V_i$$

von linearen Unterräumen V_i mit

$$g \bullet v = \phi_i(g) \bullet v \text{ für alle } v \in V_i \text{ und alle } g \in G_s.$$

Dabei ist

$$\phi_i: G_s \longrightarrow k^*$$

ein Gruppen-Homomorphismus.[1] Wir wählen die V_i dabei so, daß gilt

$$V_i = \bigcap_{g\in G_s} \mathrm{Ker}(g - \phi_i(g)\bullet \mathrm{Id}) \text{ für jedes } i.^{[2]}$$

---

[1] Man beachte, jedes $g\in G_s \subseteq G \subseteq \mathbf{GL}_n$ ist eine umkehrbare Matrix, d.h. die Eigenwerte $\phi_i(g)$ dieser Matrix sind ungleich Null. Für g', g"$\in G_s$ und $v\in V_i$ gilt

$$\begin{aligned}
\phi_i(g'\bullet g")\bullet v &= (g'\bullet g")\bullet v && \text{(nach Definition von } \phi_i\text{)}\\
&= g'\bullet(g"\bullet v) && \text{(die Matrizenmultiplikation ist assoziativ)}\\
&= g'\bullet(\phi_i(g")\bullet v) && \text{(nach Definition von } \phi_i\text{)}\\
&= \phi_i(g")\bullet(g'\bullet v) && \text{(wegen } \phi_i(g")\in k\text{)}\\
&= \phi_i(g")\bullet\phi_\iota(g')\bullet v && \text{(nach Definition von } \phi_i\text{)}
\end{aligned}$$

Da dies für alle $v \in V_i$ gilt folgt $\phi_i(g'\bullet g") = \phi_i(g")\bullet\phi_\iota(g')$, d.h. die ϕ_i sind Gruppen-Homomorphismen. Wir nehmen hier an, alle V_i sind $\neq 0$.

[2] Das ist möglich. Nach Voraussetzung gibt es eine Zerlegung $V = \oplus V_i$ mit zum Beispiel eindimensionalen linearen Unterräume V_i. Wür jedes i setzen wir

$$W_i := \bigcap_{g\in G_s} \mathrm{Ker}(g - \phi_i(g)\bullet \mathrm{Id}).$$

Dann gilt $V_i \subseteq W_i$ also $V = \sum_i V_i \subseteq \sum_i W_i \subseteq V$, also

$$V = \sum_i W_i.$$

Diese Gleichheit bleibt erhalten, wenn wir rechts doppelt vorkommende W_i weglassen, d.h. wenn die Summe über die paarweise verschiedenen $\phi_i: G_s \longrightarrow k$ erstreckt wird. Wir haben zu zeigen, die Summen-Zerlegung ist dann direkt. Angenommen, sie ist es nicht. Dann gibt es Vektoren $w_i \in W_i - \{0\}$ mit

$$w_{i_1} + w_{i_2} + \ldots + w_{i_r} = 0. \qquad (1)$$

Wir können annehmen, die Vektoren sind so gewählt, daß $r > 0$ minimal wird. Für jedes $g\in G_s$ gilt dann auch

$$\phi_{i_1}(g)\bullet w_{i_1} + \phi_{i_2}(g)\bullet w_{i_2} + \ldots + \phi_{i_2}(g)\bullet w_{i_r} = 0. \qquad (2)$$

Weil die ϕ_{i_ν} paarweise verschieden sind, können wir $g\in G_s$ so wählen, daß gilt

$$\phi_{i_1}(g) \neq \phi_{i_2}(g)$$

Wir multiplizieren (1) mit $\phi_{i_1}(g)$ und ziehen das Ergebnis von (2) ab. Wir erhalten

$$(\phi_{i_2}(g) - \phi_{i_1}(g))\bullet w_{i_2} + \ldots + (\phi_{i_2}(g) - \phi_{i_1}(g))\bullet w_{i_r} = 0.$$

Der erste Koeffizient dieser Linearkombination ist ungleich Null. Die Anzahl der Summanden ist kleiner als r. Dies widerspricht der Minimalität von r in (1). Dieser Widerspruch zeigt die Zerlegung von V in die W_i ist direkt.

Dann sind die so gewählten linearen Unterraum V_i stabil bezüglich der Operation der Gruppe G. Sei nämlich $g \in G$ und $v \in V_i$ dann gilt für jedes $x \in G_s$

$$\begin{aligned}(x - \phi_i(x)\bullet Id)(g\bullet v) &= x\bullet(g\bullet v) - \phi_i(x)\bullet g\bullet v \\ &= g\bullet(x\bullet v - \phi_i(x)\bullet v) \qquad \text{(denn G ist kommutativ)} \\ &= g\bullet((x - \phi_i(x)\bullet Id)v) \\ &= g\bullet 0 \qquad \text{(wegen } v \in V_i\text{)} \\ &= 0,\end{aligned}$$

also

$$g\bullet v \in \mathrm{Ker}(x - \phi_i(x)\bullet Id)$$

Da dies für jedes $x \in G_s$ gilt, folgt $g\bullet v \in V_i$ für jedes $v \in V_i$ und jedes $g \in G$. Die V_i sind also tatsächlich G-stabil.
Weil G kommutativ ist, können wir nach 2.4.2 (i) für jedes i eine Basis von V_i derart finden, daß G auf V_i durch obere Dreiecksmatrizen operiert. Alle diese Basen zusammen bilden eine Basis von V, bezüglich der G auf V durch obere Dreiecksmatrizen operiert und G_s durch Diagonal-Matrizen. Durch Wechsel der Basis von $V = k^n$ können wir also erreichen, daß

$$G \subseteq \mathbf{T}_n \text{ und } G_s \subseteq \mathbf{D}_n$$

gilt (wir verwenden die Bezeichnungen von 2.1.4 Beispiel 4 (c)). Insbesondere ist

$$G_s \subseteq G \bigcap \mathbf{D}_n.$$

Nun ist aber jede Matrix von $\mathbf{D}_n$ halbeinfach. Weil jede halbeinfache Matrix von G in G_s liegt, besteht auch die umgekehrte Inklusion. Zusammen ist damit

$$G_s = G \bigcap \mathbf{D}_n.$$

Weil D_n abgeschlossen ist in GL_n, ist dann aber auch G_s abgeschlossen in G.
Zu (ii). Die Abbilung

$$\pi: G_s \times G_u \longrightarrow G, (x,y) \mapsto x\bullet y,$$

ist surjektiv auf Grund der Existenz der Jordan-Zerlegung und injektiv auf Grund von deren Eindeutigkeit (vgl. 2.4.8 (i)). Als Einschränkung der Gruppen-Multiplikation

$$G \times G \longrightarrow G, (x,y) \mapsto x\bullet y,$$

ist π eine reguläre Abbildung. Die Umkehrung von π ist gegeben durch

$$G \longrightarrow G_s \times G_u, g \mapsto (g_s, g_u).$$

Wir haben noch zu zeigen, daß die Koordinatenfunktionen dieser Abbildung regulär sind. Dazu reicht es zu zeigen, die Abbildung

$$G \longrightarrow G_s, g \mapsto g_s, \tag{3}$$

ist regulär (denn dann hängt auch $g_u = g\bullet g_s^{-1}$ in regulärer Weise von g ab). Wir wählen das im Beweis von (i) beschriebene Koordinatensystem, für welches $G_s = G \bigcap \mathbf{D}_n$ gilt. Bezüglich dieses Koordinatensystems ist (3) die Abbildung,

$$G \longrightarrow G_s, g_s\bullet g_u \mapsto g_s,$$

welche im Produkt $g = g_s \bullet g_u$ die Matrix g_u durch die Einheitsmatrix ersetzt. Bezeichne λ_i den i-ten Eintrag auf der Hauptdiagonalen von g_s. Dann hat die Diagonalmatrix g_s die Gestalt

$$g_s = (\lambda_1 \bullet e_1, ..., \lambda_n \bullet e_n),$$

wenn e_i die i-te Spalte der Einheitsmatrix bezeichnet. Weil g_u eine obere Dreiecksmatrix ist und die Einträge von $g_u = (\mu_{ij})$ auf der Hauptdiagonalen gleich 1 sind, hat $g_s \bullet g_u$ die Gestalt

$$g_s \bullet g_u = (\lambda_1 \bullet e_1 + \sum_{\alpha=2}^{n} \mu_{\alpha 1} \lambda_\alpha \bullet e_\alpha, \lambda_2 \bullet e_2 + \sum_{\alpha=3}^{n} \mu_{\alpha 1} \lambda_\alpha \bullet e_\alpha, ..., \lambda_n \bullet e_n).$$

Man beachte, die Summen $\sum_{\alpha=\nu+1}^{n} \mu_{\alpha\nu} \lambda_\alpha \bullet e_\alpha$ stehen für Einträge außerhalb der Hauptdiagonalen. Abbildung (3) bekommt so die Gestalt

$$(\lambda_1 \bullet e_1 + \sum_{\alpha=2}^{n} \mu_{\alpha 1} \lambda_\alpha \bullet e_\alpha, \lambda_2 \bullet e_2 + \sum_{\alpha=3}^{n} \mu_{\alpha 1} \lambda_\alpha \bullet e_\alpha, ..., \lambda_n \bullet e_n) \mapsto (\lambda_1 \bullet e_1, ..., \lambda_n \bullet e_n),$$

d.h. in jeder oberen Dreiecksmatriz werden alle Einträge außerhalb der Hauptdiagonalen durch Nullen ersetzt und die Einträge der Hauptdiagonalen unverändert gelassen. Insbesondere ist (3) eine reguläre Abbildung.
QED.

3.1.2 Folgerung: Erhaltung des Zusammenhangs beim Übergang zum halbeinfachen bzw. unipotenten Teil

Ist G eine zusammenhängende kommutative lineare algebraische Gruppe, so gilt dasselbe für deren halbeinfache und unipotente Teile G_s und G_u.

Beweis. Die Zusammensetzungen des Inversen

$$\pi^{-1}: G \longrightarrow G_s \times G_u$$

des Isomorphismus von 3.1.1 (ii) mit den Projektionen auf die beiden Faktoren, sind surjektive reguläre Abbildungen

$$G \longrightarrow G_s \text{ und } G \longrightarrow G_u.$$

Mit G sind aber auch die beiden stetigen (weil regulären) Bilder von G zusammenhängend.
QED.

3.1.3 Proposition: der zusammenhängende Fall der Dimension 1

Sei G eine zusammenhängende lineare algebraische Gruppe der Dimension 1,

$$\dim G = 1.$$

Dann gelten folgende Aussagen.
(i) G ist kommutativ.
(ii) $G = G_s$ oder $G = G_u$.
(iii) Ist G unipotent und k von positiver Charakteristik,

$$p := \mathrm{Char}(k) > 0,$$

so ist jedes Element von G - {e} von der Ordnung p.

Beweis. Zu (i). Sei

$$g \in G.$$

Wir betrachten die reguläre Abbildung

$$\phi: G \longrightarrow G,\ x \mapsto xgx^{-1}.$$

Mit G ist auch $\overline{\phi(G)}$ irreduzibel (nach 1.2.3 (i) und (ii)). Damit gilt

$$\overline{\phi(G)} = G \text{ oder } \dim \overline{\phi(G)} < \dim G = 1$$

(nach 1.8.2). Im zweiten Fall ist $\overline{\phi(G)}$ als 0-dimensionale zusammenhängende Menge einpunktig. Weil $g = \phi(e)$ in dieser Menge liegt, gilt also

$$\overline{\phi(G)} = G \text{ oder } \overline{\phi(G)} = \{g\}.$$

Nehmen wir an, es tritt der erste Fall ein,

$$\overline{\phi(G)} = G.$$

Weil $\phi(G)$ eine in G offene Teilmenge enthält (nach 1.9.5), d.h. eine Menge mit endlichem Komplement (wegen $\dim G = 1$)[3], ist auch

$$G - \phi(G) \text{ endlich.}$$

Wir können annehmen, daß G eine abgeschlossene Untergruppe vom $\mathbf{GL}_n$ ist (nach 2.3.7(i)). Die Einschränkung des für die Matrizen von $\mathbf{GL}_n$ definierten charakteristischen Polynoms auf G,

$$\det (T \cdot 1 - y) \text{ mit } y \in G \subseteq \mathbf{GL}_n$$

ist auf jeder Konjugationsklasse konstant, also insbesondere auf $\phi(G)$. Weil das Komplement von $\phi(G)$ in G endlich ist, ist die Menge

$$\{ \det (T \cdot 1 - y) \mid y \in G \}$$

endlich. Die Koeffizienten des charakteristischen Polynoms sind somit reguläre Funktionen

$$G \longrightarrow \mathbb{A}^1$$

mit nur endlich vielen Werten. Weil G zusammenhängend ist, ist es auch jedes Bild von G bei einer regulären Abbildung. Die Koeffizienten des charakteristischen Polynoms sind damit konstante Funktionen, d.h. $\det (T \cdot 1 - y)$ ist unabhängig von $y \in G$. Es folgt

$$\chi_y(T) = \det (T \cdot 1 - y) = \det (T \cdot 1 - e) = (T-1)^n.$$

Nach dem Satz von Caley-Hemilton gilt

$$0 = \chi_y(y) = (y - 1)^n \text{ für jedes } y \in G.$$

Mit anderen Worten, G ist eine unipotente Gruppe. Als solche ist G auflösbar (nach 2.4.13 B). Insbesondere gibt es einen iterierten Kommutator von G, welcher trivial ist,

$$G^{(\ell)} = \{e\} \text{ für eine natürliche Zahl } \ell$$

(vgl. Bemerkrung 2.4.13 A (iii)). Zur Erinnerung $G^{(0)} := G$, $G^{(i+1)} := (G^{(i)}, G^{(i)})$. Das ist nur möglich, wenn der Kommutator von G echt enthalten ist in G,

$$(G, G) \subset G.$$

Nun ist (G, G) eine zusammenhängende abgeschlossene Untergruppe von G (nach 2.2.8(i)). Insbesondere gilt $\dim (G,G) < \dim G = 1$ (nach 1.8.2), also $\dim (G,G) = 0$, d.h. (G,G) ist endlich und als irrreduzible Varietät sogar einpunktig. Es gilt also

$$(G, G) = \{e\}.$$

---

[3] $G - \phi(G)$ ist eine echte abgeschlossene Teilmenge von G. Weil G irreduzibel ist, gilt

$$\dim G - \phi(G) < \dim G = 1$$

(nach 1.8.2), also

$$\dim (G - \phi(G)) = 0.$$

Eine affine irreduzible affine Varietät der Dimension 0 ist eine einpunktige Menge. Da die Anzahl der irreduziblen Komponenten von $G-\phi(G)$ endlich ist, ist $G-\phi(G)$ eine endliche Menge.

Nach Definition von ϕ gilt aber $g^{-1}\phi(G) \subseteq (G, G)$. Das steht im Widerspruch zu unserer Annahme $\overline{\phi(G)} = G$. Diese ist somit falsch, und es gilt

$$\phi(G) \subseteq \overline{\phi(G)} = \{g\},$$

also $g = \phi(x) = xgx^{-1}$ für jedes $x \in G$, also

$$gx = xg \text{ für beliebige } x, g \in G.$$

Die Gruppe G ist kommutativ, wie behauptet.
Zu (ii). Weil G kommutativ ist, gilt

$$G \cong G_s \times G_u$$

(nach 3.1.1), wobei G_s imd G_u zusammenhängende abgeschlossene Untergruppen sind (vgl. 3.1.1 (i) und 3.1.2). Eine der beiden Untergruppen hat damit die Dimension 1 und die andere die Dimension 0 (nach 1.8.3). Die 0-dimensionale Untergruppe ist trivial (weil sie zusammenhängend ist). Damit gilt Aussage (ii).
Zu (iii). Wir betrachten die Untergruppen

$$<G^{p^k}>$$

von G, welche von den p^k-ten Potenzen der Elemente von G erzeugt werden. Es sind abgeschlossene und zusammenhängende Untergruppen von G (nach 2.2.5(ii) und 2.2.9 Aufgabe 3). Wegen dim G = 1 sind diese Untergruppen gleich G oder gleich {e),

$$<G^{p^k}> = G \text{ oder } <G^{p^k}> = \{e\}.$$

Wir können annehmen, daß G eine abgeschlossene Untergruppe der $\mathbf{GL}_n$ ist (nach 2.3.7). Weil G nach Voraussetzung unipotent ist, können wir sogar annehmen, G ist abgeschlossenen Untergruppe der Gruppe $\mathbf{U}_n$ der oberen Dreiecksmatrizen, deren Einträge auf der Hauptdiagonalen gleich 1 sind,

$$G \subseteq \mathbf{U}_n$$

(nach 2.4.12 B). Die Elemente der Gruppe G haben dann die Gestalt

$$g = 1 + n$$

mit einer oberen Dreiecksmatrix n, deren Einträge auf der Hauptdiagonalen gleich 0 sind. Weil die Charakteristik des Grundkörpers k gleich p ist und die Matrizen 1 und n kommutieren, gilt

$$g^p = \sum_{i=1}^{p} \binom{p}{i} \cdot n^i = 1 + n^p.$$

Wir iterieren diese Identität und erhalten

$$g^{p^k} = 1 + n^{p^k}.$$

Der zweite Summand rechts ist jedoch gleich 0 für $p^k \geq n$ (vgl. Formel (5) im dritten Schritt des Beweises zu Aufgabe 4 von 2.1.4). Also gilt

$$<G^{p^k}> = \{e\} \text{ für } p^k \geq n.$$

Damit ist der Fall $< G^p > = G$ ausgeschlossen, d.h. es ist

$$< G^p > = \{e\},$$

wie behauptet.
QED.
Bemerkung
Im Rest dieses Kapitels untersuchen wir zunächst die kommutativen linearen algebraischen Gruppen, deren Elemente halbeinfach sind, und anschließend diejenigen, welche der Bedingung von 3.1.3 (iii) genügen.

3.2 Diagonalisierbare Gruppen und Tori

3.2.1 Charaktere, Kocharaktere, Diagonalisierbarkeit

Sei G eine lineare algebraische Gruppe über dem algebraisch abgeschlossenen Körper k. Ein Homomorphismus von algebraischen Gruppen

$$\chi: G \longrightarrow \mathbf{G}_m$$

heißt rationaler Charakter oder auch einfach Charakter von G. Die Menge der rationalen Charaktere von G wird mit

$$\mathbf{X}^*(G)$$

bezeichnet. Ein Homomorphismus von algebraischen Gruppen

$$\lambda: \mathbf{G}_m \longrightarrow G$$

heißt Kocharakter von G oder auch multiplikative einparametrische Untergruppe von G. Die Menge der Kocharaktere von G wird mit

$$\mathbf{X}_*(G)$$

bezeichnet.

Eine lineare algebraische Gruppe heißt diagonalisierbar, wenn sie isomorph ist zu einer abgeschlossenen Untergruppe einer der Gruppen $\mathbf{D}_n$ (der n×n-Diagonalmatrizen über k, vgl. 2.1.4 Beispiel 4 (b)). Ist sie isomorph zu einer der Gruppen $\mathbf{D}_n$, so heißt sie auch algebraischer Torus.[4]

Bemerkungen

(i) Die Menge $\mathbf{X}^*(G)$ besitzt bezüglich der Multiplikation von Abbildungen mit Werten in der abelschen Gruppe $\mathbf{G}_m$ selbst die Struktur einer abelschen Gruppe.

Wir vereinbaren, die Operation dieser Gruppe additiv zu schreiben.

(ii) Nach Definition sind die Charaktere von G reguläre Funktionen auf G, d.h. Elemente des Koordinatenrings,

$$X^*(G) \subseteq k[G].$$

Nach dem Satz von Artin (vgl. Lang [2], Kapitel VIII, §4, Theorem 7) sind die Charaktere k-linear unabhängige Elemente von k[G].

(iii) Ist die lineare algebraische Gruppe G kommutativ, so besitzt

$$\mathbf{X}_*(G)$$

bezüglich der Multiplikation von Abbildungen mit Werten in der Gruppe G die Struktur eine abelschen Gruppe. Wir vereinbaren dann, die Operation dieser Gruppe additiv zu schreiben.

(iv) Ist die lineare algebraische Gruppe nicht-notwendig kommutativ, so denken wir uns

$$\mathbf{X}_*(G)$$

stets mit der Multiplikation mit ganzen Zahlen versehen[5],

$$< , >: \mathbb{Z} \times \mathbf{X}_*(G) \longrightarrow \mathbf{X}_*(G),\ (n, \lambda) \mapsto (x \mapsto <n, \lambda>(x) := \lambda(x)^n).$$

3.2.2 Beispiel

Sei $G = \mathbf{D}_n$. Wir schreiben die Elemente $x \in G$ in der Gestalt

---

[4] Die algebraischen Tori sind nicht zu verwechseln mit den geometrischen Tori, welche projektive algebraische Gruppen sind (und damit außer in der Dimension 0 keine linearen algebraischen Gruppen, vgl. Mumford [1]).

[5] Dabei betrachten wir die Elemente von $\mathbf{X}_*(G)$ als Abbildungen $k^* \longrightarrow G$.

$$x = \mathrm{diag}(\chi_1(x),...,\chi_n(x)) = \begin{pmatrix} \chi_1(x) & 0 & .. & 0 \\ 0 & \chi_2(x) & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \chi_n(x) \end{pmatrix} \in G$$

Dann sind die Abbildungen $\chi_i: G \longrightarrow k^* = \mathbf{G}_m$ (als Koordinaten-Funktionen) rationale Charaktere von G. Es gilt

$$\begin{aligned} k[\mathbf{D}_n] &= k[\chi_1,..., \chi_n, (\chi_1 \bullet ... \bullet \chi_n)^{-1}] \\ &= k[\chi_1,..., \chi_n, \chi_1^{-1},..., \chi_n^{-1}] \\ &= \sum_{(a_1,...,a_n)\in\mathbb{Z}^n} k \bullet \chi_1^{a_1} \bullet ... \bullet \chi_n^{a_n} \end{aligned}$$

(vgl. 2.2.2 Aufgabe 1). Nach dem Satz von Artin (vgl. Lang [2], Kapitel VIII, §4, Theorem 7) sind die (paarweise verschiedenen) Potenzprodukte

$$\chi_1^{a_1} \bullet ... \bullet \chi_n^{a_n} \text{ mit } (a_1,...,a_n) \in \mathbb{Z}^n \qquad (1)$$

linear unabhängig über k, bilden also eine Basis des k-Vektorraums $k[\mathbf{D}_n]$. Weil jeder Charakter von $\mathbf{D}_n$ in $k[\mathbf{D}_n]$ liegt, also eine k-Linearkombination der Charaktere (1) ist, gleichzeitig aber nach Artin paarweise verschiedende Charaktere linear unabhängig sind, hat jeder Charakter von $\mathbf{D}_n$ die Gestalt (1). Es besteht also ein Gruppen-Isomorphismus

$$\mathbb{Z}^n \xrightarrow{\cong} X^*(\mathbf{D}_n),\ (a_1,...,a_n) \mapsto \chi_1^{a_1} \bullet ... \bullet \chi_n^{a_n}. \qquad (2)$$

Speziell für n = 1 sehen wir, die Charaktere von $\mathbf{G}_m = \mathbf{D}_1$ sind gerade die Abbildungen

$$\mathbf{G}_m = k^* \longrightarrow k^* = \mathbf{G}_m,\ t \mapsto t^n, \text{ mit } n \in \mathbb{Z}.$$

Ein Homomorphismus $\mathbf{G}_m \longrightarrow \mathbf{D}_n$ hat damit die Gestalt

$$\mathbf{G}_m \longrightarrow \mathbf{D}_n,\ t \mapsto \mathrm{diag}(t^{a_1}, \dots, t^{a_n}) \text{ mit } (a_1,...,a_n) \in \mathbb{Z}^n$$

(weil die Zusammensetzung von $\mathbf{G}_m \longrightarrow \mathbf{D}_n$ mit $\chi_i: \mathbf{D}_n \longrightarrow \mathbf{G}_m$ für jedes i ein Charakter von $\mathbf{G}_m$ ist). Wir erhalten so einen Gruppen-Isomorphismus

$$\mathbb{Z}^n \xrightarrow{\cong} X_*(\mathbf{D}_n),\ (a_1,...,a_n) \mapsto (t \mapsto \mathrm{diag}(t^{a_1}, \dots, t^{a_n})). \qquad (3)$$

3.2.3 Satz: Charakterisierung der Diagonalisierbarkeit

Sei G eine algebraische Gruppe über k. Dann sind folgende Aussagen äquivalent.

(i) G ist diagonalisierbar.

(ii) $X^*(G)$ ist eine endlich erzeugte abelsche Gruppe, deren Elemente eine k-Vektorraumbasis des Koordinatenrings k[G] bilden.

(iii) Jede rationale Darstellung von G ist eine direkte Summe von 1-dimensionalen rationalen Darstellungen von G.

Beweis. (i) $\Rightarrow$ (ii). Nach Voraussetzung ist G eine abgeschlossene Untergruppe einer der Gruppen $\mathbf{D}_n$. Die natürliche Einbettung $G \hookrightarrow \mathbf{D}_n$ induziert einen surjektiven k-Algebra-Homomorphismus der Koordinatenringe,

$$k[\mathbf{D}_n] \twoheadrightarrow k[G],\ f \mapsto f|_G. \tag{1}$$

Die Einschränkung eines Charakters von $\mathbf{D}_n$ auf G ist ein Charakter von G. Durch Einschränken dieser Surjektion erhalten wir eine Abbildung

$$\mathbf{X}^*(\mathbf{D}_n) \longrightarrow \mathbf{X}^*(G),\ \chi \mapsto \chi|_G. \tag{2}$$

Da die Charaktere von $\mathbf{D}_n$ den Koordinatenring von $k[\mathbf{D}_n]$ als Vektorraum erzeugen, wird k[G] als Vektorraum von den Einschränkungen dieser Charaktere erzeugt:

$$k[G] = \sum_{\chi \in X^*(\mathbf{D}_n)} k \bullet \chi|_G \qquad \text{(weil (1) surjektiv ist)}$$

$$= \sum_{(a_1,\ldots,a_n)\in\mathbb{Z}^n} k \bullet \chi_1^{a_1} \bullet \ldots \bullet \chi_n^{a_n}|_G. \qquad \text{(nach 3.2.2 (2))}$$

Da jeder Charakter von G in k[G] liegt, ist er eine k-Linearkombination der Charaktere $\chi_1^{a_1} \bullet \ldots \bullet \chi_n^{a_n}|_G$. Nach dem Satz von Artin (vgl. Lang [2], Kapitel VIII, §4, Theorem 7), muß er gleich einem dieser Charaktere sein,

$$X^*(G) = \{ \chi_1^{a_1} \bullet \ldots \bullet \chi_n^{a_n}|_G \mid (a_1,\ldots,a_n) \in \mathbb{Z}^n \}.$$

Damit wird X*(G) von den endlich vielen Charakteren $\chi_1|_G , \ldots , \chi_n|_G$ erzeugt. Wie gerade gezeigt, erzeugen deren Potenzprodukte den k-Vektorraum k[G]. Nach dem Satz von Artin bilden sie eine k-Vektorraumbasis von k[G].

(ii) $\Rightarrow$ (iii). Sei

$$\phi: G \longrightarrow \mathbf{GL}(V)$$

eine rationale Darstellung von G. Wir fixieren einen Basis von V, welche es gestattet, ϕ als Homomorphismus

$$\phi: G \longrightarrow \mathbf{GL}_r$$

(mit r geeigneten) zu betrachten. Für jedes $x \in G$ gilt dann

$$\phi(x) = \begin{pmatrix} \phi_{11}(x) & \phi_{12}(x) & \ldots & \phi_{1r}(x) \\ \phi_{21}(x) & \phi_{22}(x) & \ldots & \phi_{2r}(x) \\ \ldots & \ldots & \ldots & \ldots \\ \phi_{r1}(x) & \phi_{r2}(x) & \ldots & \phi_{rr}(x) \end{pmatrix} = \sum_{i,j=1}^{n} \phi_{ij}(x) \bullet E_{ij}$$

mit regulären Funktion $\phi_{ij} \in k[G]$. Jede dieser regulären Funktion ϕ_{ij} ist eine k-Linearkombination von Charakteren von G. Deshalb läßt sich ϕ als Linearkombination von r×r-Matrizen mit Einträgen aus k schreiben, deren Koeffizienten Charaktere von G sind, sagen wir

$$\phi(x) = \sum_{\chi\in\mathbf{X}^*(G)} \chi(x)\cdot A_\chi$$

mit $A_\chi \in M_r(k)$ oder in einer von der Wahl der Basis von V unabhängigen Schreibweise,

$$A_\chi \in \mathrm{End}_k(V). \tag{3}$$

Dabei sind nur endlich viele der A_χ von Null verschieden,

$$A_\chi = 0 \text{ für fast alle } \chi\in\mathbf{X}^*(G).$$

Weil ϕ ein Gruppen-Homomorphismus ist, gilt für $x,y\in G$

$$\begin{aligned}\sum_{\chi\in\mathbf{X}^*(G)} \chi(x)\chi(y)\cdot A_\chi &= \sum_{\chi\in\mathbf{X}^*(G)} \chi(xy)\cdot A_\chi \\ &= \phi(xy) \\ &= \phi(x)\cdot\phi(y) \\ &= \sum_{\chi,\psi\in\mathbf{X}^*(G)} \chi(x)\cdot \psi(y)\cdot A_\chi\cdot A_\psi.\end{aligned}$$

Die Abbbildungen

$$G\times G \longrightarrow \mathbf{G}_m,\ (x,y) \mapsto \chi(x)\cdot \psi(y),$$

sind paarweise verschiedene[6] Charaktere von G×G. Die Identität

$$\sum_{\chi\in\mathbf{X}^*(G)} \chi(x)\chi(y)\cdot A_\chi = \sum_{\chi,\psi\in\mathbf{X}^*(G)} \chi(x)\cdot \psi(y)\cdot A_\chi\cdot A_\psi$$

ist somit eine Relation von Charakteren auf G×G. Weil die Charaktere von G×G linear unabhängig über k sind, folgt durch Koeffizientenvergleich

$$A_\chi\cdot A_\psi = \delta_{\chi,\psi}\cdot A_\chi \tag{4}$$

(wenn $\delta_{\chi,\psi}$ das Kronecker-Symbol bezeichnet).Weil $\phi(e)$ die identische Abbildung von V ist, gilt für $v \in V$

$$\begin{aligned} v &= \mathrm{Id}(v) \\ &= \phi(e)(v) && \text{(wegen } \phi(e) = \mathrm{Id}) \\ &= \Big(\sum_{\chi\in\mathbf{X}^*(G)} \chi(e)\cdot A_\chi\Big)(v) && \text{(nach Definition der } A_\chi) \\ &= \Big(\sum_{\chi\in\mathbf{X}^*(G)} A_\chi\Big)(v) && \text{(wegen } \chi(e) = 1 \text{ für alle } \chi)\end{aligned}$$

also

$$\sum_{\chi\in\mathbf{X}^*(G)} A_\chi = \mathrm{Id}. \tag{5}$$

---

[6] Man beachte, für Charaktere α, β, γ und δ gilt nur dann $\alpha(x)\beta(y) = \gamma(x)\cdot \delta(y)$ für alle $x, y \in G$, wenn $\alpha=\gamma$ und $\beta = \delta$ ist (man setze $y = e$ bzw. $x = e$).

Wir setzen

$$V_\chi := A_\chi(V).$$

Dann gilt

$$\begin{aligned} V &= \mathrm{Id}(V) \\ &= \Big(\sum_{\chi\in\mathbf{X}^*(G)} A_\chi\Big)(V) && \text{(nach (5))} \\ &\subseteq \sum_{\chi\in\mathbf{X}^*(G)} A_\chi(V) \\ &= \sum_{\chi\in\mathbf{X}^*(G)} V_\chi \\ &\subseteq V \end{aligned}$$

also

$$\sum_{\chi\in\mathbf{X}^*(G)} V_\chi = V,$$

Weiter gilt für $x \in G$ und $y \in V_\chi$, d.h. $y = A_\chi(v)$ für ein $v \in V$:

$$\begin{aligned} \phi(x)(y) &= \Big(\sum_{\psi\in\mathbf{X}^*(G)} \psi(x)\bullet A_\psi\Big)(y) && \text{(nach Definition der } A_\psi) \\ &= \sum_{\psi\in\mathbf{X}^*(G)} \psi(x)\bullet A_\psi A_\chi(v) \\ &= \chi(x)\bullet A_\chi A_\chi(v) && \text{(nach (4))} \\ &= \chi(x)\bullet A_\chi(v) && \text{(nach (4))} \\ &= \chi(x)\bullet y && \text{(nach Definition von y)} \end{aligned}$$

also

$$\phi(x)(y) = \chi(x)\bullet y \text{ für } x \in G \text{ und } y \in V_\chi \qquad (6)$$

Nach (4) ist A_χ auf V_ψ die identische Abbildung für $\chi=\psi$ und 0 sonst. Deshalb ist die gefundene Summenzerlegung von V direkt,

$$\bigoplus_{\chi\in\mathbf{X}^*(G)} V_\chi = V. \qquad (7)$$

Weil V endlich-dimensional ist, ist die Anzahl der von 0 verschiedenen V_χ endlich. Wir können also schreiben

$$V = V_{\chi_1} \oplus \ldots \oplus V_{\chi_t} \text{ mit } V_{\chi_i} \neq 0.$$

Nach (6) operiert G auf V_{χ_i} durch Multiplikation mit dem Charakter χ_i. Wenn wir V_{χ_i} in beliebiger Weise in eine direkte Summe von 1-dimensionalen Vektorräumen zerlegen, gilt die auch für jeden der direkten Summanden.

Die rationale Darstelleung ϕ ist somit eine direkte Summen der 1-dimensionalen Darstellungen, die mit den Charakterem $\chi_1, \ldots, \chi_t$ multiplizieren. Dabei ist

$$\dim V_{\chi_i}$$

gerade die Multiplizität, mit welcher der Charakter χ_i vorkommt.

(iii) $\Rightarrow$ (i). Nach 2.3.7 gibt es eine natürlichen Zahl n und einen Isomorphismus

$$h: G \xrightarrow{\cong} H$$

mit einer abgeschlossenen Untergruppe $H \hookrightarrow \mathbf{GL}_n$. Wir können h als einen injektiven Homomorphismus algebraischer Gruppen

$$h: G \longrightarrow \mathbf{GL}_n = \mathbf{GL}(V) \text{ mit } V = k^n$$

betrachten, d.h. als rationale Darstellung von G. Nach Voraussetzung (iii) ist h eine direkte Summe von 1-dimensionalen Darstellungen, d.h. der G-Modul V ist direkte Summe von 1-dimensionalen G-Moduln, sagen wir

$$V = V_1 \oplus \ldots \oplus V_n \text{ mit } \dim_k V_i = 1 \text{ für jedes i.}$$

Wegen $\dim_k V_i = 1$ opereriert G auf V_i durch einen Charakter von G, sagen wir

$$h(g)v = \chi_i(g) \bullet v \text{ für jedes } g \in G, \chi_i \in \mathbf{X}^*(G).$$

Man beachte, mit h ist auch $\chi_i: G \longrightarrow G_m$ ein Gruppen-Homomorphismus, denn für g',g"∈G und $v \in V_i$ gilt

$$\begin{aligned} \chi_i(g'g'') \bullet v &= h(g'g'')(v) \\ &= h(g')(h(g'')(v)) \\ &= h(g')(\chi_i(g'') \bullet v) \\ &= \chi_i(g'') \bullet h(g')(v) \\ &= \chi_i(g'') \bullet \chi_i(g') \bullet v. \end{aligned}$$

Da dies für jedes $v \in V_i$ gilt, folgt $\chi_i(g'g'') = \chi_i(g') \bullet \chi_i(g'')$ für beliebige $g', g'' \in G$.

Außerdem ist χ_i als Zusammensetzung

$$G \times V_i \xrightarrow{\alpha} G \times V \xrightarrow{\beta} V \xrightarrow{\gamma} V_i.$$

von regulären Abbildungen auch regulär. Dabei ist α induziert durch die natürliche Einbettung

$$V_i \hookrightarrow V,$$

β ist die Abbildung $G \times V \longrightarrow V$, $(g,v) \mapsto h(g)(v)$, und γ ist die Projektion

$$V = V_1 \oplus \ldots \oplus V_n \longrightarrow V_i$$

der direkten Summe auf den i-ten direkten Summanden.

Wir wählen aus jedem V_i einen von Null verschiedenen Vektor

$$v_i \in V_i - \{0\}.$$

Die Vektoren v_i zusammen bilden eine Basis von V. Bezeichne $\sigma: k^n \longrightarrow k^n$ den k-linearen Automorphismus, der den i-ten Standard-Einheitsvektor e_i von k^n in den Vektor v_i abbildet für i = 1,..., n. Dann gilt für jedes i

$$\begin{aligned}(\sigma^{-1}\bullet h(g)\bullet\sigma)(e_i) &= \sigma^{-1}\bullet h(g)(v_i)\\ &= \sigma^{-1}(\chi_i(g)\bullet v_i)\\ &= \chi_i(g)\bullet\sigma^{-1}(v_i)\\ &= \chi_i(g)\bullet e_i\end{aligned}$$

Die Matrix $\sigma^{-1}\bullet h(g)\bullet\sigma$ hat also Diagonalgestalt für jedes $g \in G$. Die Zusammensetzung von h mit dem inneren Automorphismus

$$a: \mathbf{GL}_n \xrightarrow{\cong} \mathbf{GL}_n,\ x \mapsto \sigma^{-1}\bullet x\bullet\sigma,$$

hat in der abgeschlossenen Untergruppe $\mathbf{D}_n$ von $\mathbf{GL}_n$:

$$a\circ h: G \xrightarrow[h]{\cong} H \xrightarrow[a]{\cong} \sigma^{-1}\bullet H\bullet\sigma \hookrightarrow \mathbf{D}_n \hookrightarrow \mathbf{GL}_n.$$

Wir haben gezeigt, G ist isomorph zu einer abgeschlossenen Untergruppe von $\mathbf{D}_n$, d.h. G ist diagonalisierbar.
QED.

3.2.4 Folgerung: Eigenschaften diagonalisierbarer Gruppen

Sei G eine diagonalisierbare lineare algebraische Gruppe über dem Körper k der Charakteristik p. Dann gelten die folgenden Aussagen.
(i) X*(G) ist eine endlich erzeugte abelsche Gruppe.
(ii) Der Koordinatenring k[G] ist isomorph zur Gruppen-Algebra von X*(G) über k.
(iii) Ist $p > 0$, so besitzt X*(G) keine p-Torsion.

Beweis. Zu (i). Dies gilt auf Grund der Implikation (i) $\Rightarrow$ (ii) des gerade bewiesenen Satzes 3.2.3.
Zu (ii). Die Gruppen-Algebra einer Gruppe H über k ist definiert als der k-Vektorraum

$$A := \sum_{h\in H} k\bullet e(h)$$

mit der Basis $\{e(h)\}_{h\in H}$, welcher die Struktur einer k-Algebra besitzt mit einer über k bilinearen Multiplikation, die auf den Basis-Elementen gerade mit der Multiplikation der Gruppe H übereinstimmt, d.h. mit der Multiplikation

$$A \times A \longrightarrow A,\ \Big(\sum_{h'\in H} c_{h'}\bullet e(h'),\ \sum_{h''\in H} d_{h''}\bullet e(h'')\Big) \mapsto \sum_{h',h''\in H} c_{h'}\bullet d_{h''}\bullet e(h'\bullet h'').$$

Speziell für H = X*(G) ist die Multiplikation in A gegeben durch

$$e(\chi')\bullet e(\chi'') := e(\chi'+\chi'').$$

In diesem Fall ist die k-lineare Abbildung

$$\varphi: A = \sum_{\chi \in X^*(G)} k \bullet e(\chi) \longrightarrow k[G],\ e(\chi) \mapsto \chi,$$

welche jedes Element der k-Vektorraumbasis $\{e(\chi)\}_{\chi \in X^*(G)}$ von A in den zugehörigen Charakter abbildet, ein k-Algebra-Homomorphismus, denn für je zwei Charaktere χ', $\chi'' \in X^*(G)$ gilt

$$\varphi(e(\chi') \bullet e(\chi'')) = \varphi(e(\chi' + \chi'')) = \chi' \bullet \chi'' = \varphi(e(\chi')) \bullet \varphi(e(\chi'')),$$

denn die Summe $\chi' + \chi''$ der beiden Charaktere in $X^*(G)$ ist definiert als das Produkt $\chi' \bullet \chi''$ der regulären Funktionen aus k[G].

Auf Grund des gerade bewiesenen Satzes 3.2.3 bilden die Charaktere von G eine Basis des k-Vektorraums k[G]. Die Abbildung φ bilden also eine k-Vektorraumbasis von A in eine k-Vektorraumbasis von k[G], ist also ein k-linearer Isomorphismus und damit ein Isomorphismus von k-Algebren.

Zu (iii). Wir beachten zunächst, daß k außer 1 keine p-te Einheitswurzel besistzt, denn aus $x^p = 1$ folgt

$$\begin{aligned} 0 &= x^p - 1 \\ &= x^p - 1^p \\ &= (x-1)^p \qquad \text{(wegen p = Char(k))} \end{aligned}$$

also

$$0 = x-1, \qquad \text{(weil k ein Körper ist)}$$

also $x = 1$.
Angenommen, $\mathbf{X}^*(G)$ besitzt p-Torsion.
Sei jetzt $\chi \in \mathbf{X}^*(G)$ ein Charakter mit

$$p \bullet \chi = 0.$$

Wir haben zu zeigen, dann gilt $\chi = 0$, d.h. χ ist der triviale Charakter.
Nach Voraussetung gilt

$$\chi(g)^p = 1 \text{ für jedes } g \in G.$$

Weil 1 die einzige p-te Einheitswurzel von k ist und die Werten der Abbildung χ in k liegen, folgt

$$\chi(g) = 1 \text{ für jedes } g \in G,$$

d.h. χ ist der triviale Charakter von G.
QED.

3.2.5 Die Gruppen-Algebra einer endlich erzeugten abelschen Gruppe

Sei M eine endlich erzeugte abelsche Gruppe (und k wie immer ein algebraisch abgeschlossener Körper). Die Gruppen-Algebra von M über k ist der k-Vektorraum

$$k[M] := \sum_{m \in M} k \bullet e(m)$$

mit der Vektorraum-Basis $\{e(m)\}_{m \in M}$ versehen mit der über k bilinearen Multiplikation

$$k[M] \times k[M] \longrightarrow k[M] \text{ mit } e(m') \bullet e(m'') := e(m' + m'') \text{ für } m', m'' \in M.$$

Man beachte, diese Multiplikation ist assoziativ und kommutativ, weil die Addition in M es ist.

Bemerkungen

(i) Für je zwei endlich erzeugte abelsche Gruppen M', M" besteht ein natürlicher Isomorphismus von k-Algebren

$$k[M']\otimes_k k[M''] \xrightarrow{\cong} k[M'\oplus M''],\ e(m')\otimes e(m'') \mapsto e((m',m'')).$$

(ii) Für jede endlich erzeugte abelsche Gruppe definieren wir k-lineare Abbildungen

$\Delta = \Delta_M: k[M] \longrightarrow k[M]\otimes_k k[M],\ e(m) \mapsto e(m)\otimes e(m),$

$\iota = \iota_M: k[M] \longrightarrow k[M],\ e(m) \mapsto e(-m),$

$e = e_M: k[M] \longrightarrow k,\ e(m) \mapsto 1.$

Es sind sogar Homomorphismen von k-Algebren.

(iii) Die k-Algebra-Homomorphismen von (ii) sind mit dem in (i) beschriebenen Isomorphismus verträglich.

Beweis. Zu (i). Die Abbildung

$$\varphi: k[M'] \times k[M''] \longrightarrow k[M'\oplus M''],$$

$$\Big(\sum_{m'\in M'} c_{m'}\bullet e(m'),\ \sum_{m''\in M''} d_{m''}\bullet e(m'')\Big) \mapsto \sum_{(m',m'')\in M'\oplus M''} c_{m'}\bullet d_{m''}\bullet e((m',m''))$$

ist wohldefiniert und bilinear über k. Sie faktorisiert sich deshalb eindeutig über das Tensorprodukt $k[M']\otimes_k k[M'']$, d.h. es gibt genau eine k-lineare Abbildung

$$\tilde{\varphi}: k[M']\otimes_k k[M''] \longrightarrow k[M'\oplus M''],\ e(m')\otimes e(m'') \mapsto e((m',m''))$$

für welche das Diagramm

$$\begin{array}{ccc} k[M']\times k[M'] & \xrightarrow{\varphi} & k[M'\oplus M''] \\ \otimes\downarrow & \swarrow\tilde{\varphi} & \\ k[M']\otimes_k k[M''] & & \end{array}$$

kommutativ ist. Dabei bezeichne die linke vertikale Abbildung die natürliche Abbildunge auf das Tensorprodukt $(a,b) \mapsto a\otimes b$. An der Abbildungsvorschrift liest man ab, daß $\tilde{\varphi}$ ein Homomorphismus von k-Algebren ist: für $x',y' \in M'$ und $x'',y''\in M''$ gilt

$$\begin{aligned}\tilde{\varphi}((e(x')\otimes e(x''))\bullet(e(y')\otimes e(y''))) &= \tilde{\varphi}((e(x')\bullet e(y'))\otimes(e(x'')\bullet e(y''))) \\ &= \tilde{\varphi}(e(x'+y')\otimes e(x''+y'')) \\ &= e((x'+y',x''+y'')) \\ &= e((x',x'')+(y',y'')) \\ &= e((x',x''))\bullet e((y',y'')) \\ &= \tilde{\varphi}(e(x')\otimes e(x''))\bullet\ \tilde{\varphi}(e(y')\otimes e(y''))\end{aligned}$$

d.h. $\tilde{\varphi}$ ist ein k-linearer Ring-Homomorphismus, also ein k-Algebra-Homomorphismus. Die k-Vektorraumbasis der $e(m')\otimes e(m'')$ von $k[M']\otimes_k k[M'']$ wird dabei in die k-Vektorraumbasis der $e((m', m''))$ von $k[M'\oplus M'']$ abgebildet, d.h. $\tilde{\varphi}$ ist ein k-linearer Isomorphismus. Insbesondere ist $\tilde{\varphi}$ bijektiv, also ein Isomorphismus von k-Algebren.

Zu (ii) Eine lineare Abbildung ist durch die Bilder der Basiselemente eindeutig festgelegt, wobei diese Bilder beliebig vorgegeben werden können. Die Abbildungen

Δ, ι und e sind deshalb wohldefiniert und k-linear. Es ist noch ihre Multiplikativität zu beweisen. Weil die Abbildungen k-linear sind (und die Multiplikation von k[M] bilinear über k), reicht es zu zeigen, ein Produkt von Basiselementen wird in das Produkt von deren Bildern überführt.

Für m', m" $\in$ M gilt

$\Delta(e(m')\bullet e(m")) = \Delta(e(m'+m"))$ (Definition der Muliplikation in k[M])
$= e(m'+m")\otimes e(m'+m")$ (Definition von Δ)
$= (e(m')\bullet e(m"))\otimes(e(m')\bullet e(m"))$ (Definition der Muliplikation in k[M])
$= (e(m')\otimes e(m'))\bullet(e(m")\otimes e(m"))$ (Definition der Muliplikation des Tensorprodukts)
$= \Delta(e(m'))\bullet\Delta(e(m"))$ (Definition von Δ)

$\iota(e(m')\bullet e(m")) = \iota(e(m'+m"))$ (Definition der Muliplikation in k[M])
$= e(-(m'+m"))$ (Definition von ι)
$= e((-m')+(-m"))$
$= e(-m')\bullet e(-m")$ (Definition der Muliplikation in k[M])
$= \iota(e(m'))\bullet\iota(e(m"))$ (Definition von ι)

und

$e_M(e(m')\bullet e(m")) = e_M(e(m'+m"))$
$= 1$
$= 1\bullet 1$
$= e_M(e(m'))\bullet e_M(e(m"))$.

Zu (iii). Δ ist verträglich mit dem Isomorphismus von (i), d.h. das Diagramm

$$\begin{array}{ccc} k[M']\otimes_k k[M"] & \xrightarrow{\alpha} & k[M'\oplus M"] \\ {\scriptstyle \Delta_{M'}\otimes\Delta_{M"}}\downarrow & & \downarrow{\scriptstyle \Delta_{M'\oplus M"}} \\ (k[M']\otimes_k k[M'])\otimes_k(k[M"]\otimes_k k[M"]) & \xrightarrow{(\alpha\otimes\alpha)\circ\tau} & k[M'\oplus M"]\otimes_k k[M'\oplus M"] \end{array}$$

ist kommutativ, wobei α den Isomorphismus von (i) bezeichnen soll und τ den Isomorphismus

$\tau:(k[M']\otimes_k k[M'])\otimes_k(k[M"]\otimes_k k[M"]) \xrightarrow{\cong} (k[M']\otimes_k k[M"])\otimes_k(k[M']\otimes_k k[M"])$,

welcher die beiden inneren Tensorfaktoren vertauscht.
Weil alle beteiligten Abbildungen k-linear sind, reicht es, die Kommutativität für die Basis-Elemente von $k[M']\otimes_k k[M"]$ zu überprüfen. Für m'$\in$M' und m"$\in$M" gilt

$(\Delta_{M'\oplus M"}\circ\alpha)(e(m')\otimes e(m")) = \Delta_{M'\oplus M"}(e((m',m"))$ (Definition von α)
$= e((m',m")\otimes e((m',m")$ (Definiton von $\Delta_{M'\oplus M"}$)
$= \alpha(e(m')\otimes e(m"))\otimes\alpha(e(m')\otimes e(m"))$ (Definition von α)
$= (\alpha\otimes\alpha)(e(m')\otimes e(m")\otimes e(m')\otimes e(m"))$
$= ((\alpha\otimes\alpha)\circ\tau)\,(e(m')\otimes e(m')\otimes e(m")\otimes e(m"))$ (Definition von τ)
$= ((\alpha\otimes\alpha)\circ\tau)\,(\Delta_{M'}(e(m'))\otimes\Delta_{M"}(e(m"))$ (Definition von Δ_M, und $\Delta_{M"}$)
$= ((\alpha\otimes\alpha)\circ\tau\circ(\Delta_{M'}\otimes\Delta_{M"})(e(m')\otimes e(m"))$

Da dies für alle m'$\in$M' und alle m"$\in$M" gilt, ist das Diagramm kommutativ.

ι ist verträglich mit dem Isomorphismus von (i), d.h. das Diagramm

$$\begin{array}{ccc} k[M']\otimes_k k[M''] & \xrightarrow{\alpha} & k[M'\oplus M''] \\ \downarrow \iota_{M'}\otimes\iota_{M''} & & \iota_{M'\oplus M''}\downarrow \\ k[M']\otimes_k k[M''] & \xrightarrow{\alpha} & k[M'\oplus M''] \end{array}$$

ist kommutativ. Weil alle beteiligten Abbildungen k-linear sind, reicht es, die Kommutativität für die Basis-Elemente von $k[M']\otimes_k k[M'']$ zu überprüfen. Für $m'\in M'$ und $m''\in M''$ gilt

$(\alpha\circ(\iota_{M'}\otimes\iota_{M''}))(e(m')\otimes e(m'')) = \alpha(e(-m')\otimes e(-m''))$ (Definition von $\iota_{M'}$ und $\iota_{M''}$)
$= e((-m',-m''))$ (Definition von α)
$= e(-(m',m''))$
$= \iota_{M'\oplus M''}(e((m',m''))$ (Definition von $\iota_{M'\oplus M''}$)
$= \iota_{M'\oplus M''}(\alpha(e((m')\otimes e(m''))$ (Definition von α)

d.h. auch das zweite Diagramm ist kommutativ.
e <u>ist verträglich mit dem Isomorphismus von</u> (i), d.h. das Diagramm

$$\begin{array}{ccc} k[M']\otimes_k k[M''] & \xrightarrow{\alpha} & k[M'\oplus M''] \\ e_{M'}\otimes e_{M''}\downarrow & & \downarrow e_{M'\oplus M''} \\ k\otimes_k k & = & k \end{array}$$

ist kommutativ, wenn wir k mit $k\otimes_k k$ identifzieren vermittels der Abbildung

$$k\otimes_k k \longrightarrow k,\ c\otimes d \mapsto c\bullet d.$$

Weil alle beteiligten Abbildungen k-linear sind, reicht es, die Kommutativität für die Basis-Elemente von $k[M']\otimes_k k[M'']$ zu überprüfen. Für $m'\in M'$ und $m''\in M''$ gilt

$e_{M'\oplus M''}(\alpha(e(m')\otimes e(m''))) = e_{M'\oplus M''}(e((m',m''))$ (Definition von α)
$= 1$ (Definition von $e_{M'\oplus M''}$)
$= 1\otimes 1$ (wir identifizieren $k\otimes_k k$ mit k)
$= e_{M'}(e(m'))\otimes e_{M''}(e(m''))$ (Definition von $e_{M'}$ und $e_{M''}$)
$= (e_{M'}\otimes e_{M''})(e(m')\otimes e(m''))$

Also ist auch das dritte Diagramm kommutativ.
QED.

3.2.6 Proposition: Rekonstruktion der diagonlisierbaren Gruppen aus deren Charaktergruppe

Seien p die Charakteristik des (algebraisch abgeschlossenen) Körpers k und M eine endlich erzeugte abelsche Gruppe ohne p-Torsion, falls $p \neq 0$ ist. Dann gelten die folgenden Aussagen.

(i) k[M] ist eine endlich erzeugte und reduzierte k-Algebra. Es gibt eine diagonalisierbare lineare algebraische Gruppe $\mathcal{G}(M)$ mit
$$k[\mathcal{G}(M)] = k[M],$$
wobei die Komultiplikation, der Antipode und die Auswertung im neutralen Element gerade die in 3.2.5 (ii) beschriebenen Abbildungen

$$\Delta = \Delta_M,\ \iota = \iota_M \text{ bzw. } e = e_M$$

sind.

(ii) Es gibt einen natürlichen Isomorphismus abelscher Gruppen

$$M \xrightarrow{\cong} \mathbf{X}^*(\mathcal{G}(M)),\ m \mapsto (x \mapsto e(m)(x))$$

(iii) Für jede diagonalisierbare lineare algebraische Gruppe besteht eine natürliche Isomorphie $\mathcal{G}(\mathbf{X}^*(G)) \cong G$ von algebraischen Gruppen.

Beweis. Zu (i). 1. Schritt. Reduktion auf den Fall M zyklisch.
Als endlich erzeugte abelsche Gruppe ist M eine endliche direkte Summe von zyklischen Gruppen. Es reicht also zu zeigen, Aussage (i) gilt für

$$M = M' \oplus M'',$$

falls sie für M' und M'' gilt.
Sei also

$$k[M'] = k[\mathcal{G}(M')] \text{ mit } k[\mathcal{G}(M'')]$$

mit diagonalisierbaren Gruppen

$$\mathcal{G}' := \mathcal{G}(M') \text{ und } \mathcal{G}'' := \mathcal{G}(M''),$$

deren Komulitplikationen, Antipoden und Auswertungen im neutralen Element die beschriebene Gestalt haben.
Dann ist

$$\mathcal{G} := \mathcal{G}' \times \mathcal{G}''$$

eine diagonalisierbare Gruppe mit dem Koordinatenring

$$k[\mathcal{G}] = k[\mathcal{G}(M')] \otimes_k k[\mathcal{G}(M'')] = k[M'] \otimes_k k[M''] = k[M' \oplus M''].$$

Nach 3.2.5 (iii) hat mit $\mathcal{G}'$ und $\mathcal{G}''$ auch $\mathcal{G}$ eine Komultiplikation, einen Antipoden und eine Auswertung im neutralen Element der behaupteten Gestalt.
2. Schritt. Der Fall $M \cong \mathbb{Z}$. einer unendlichen zyklischen Gruppe.
Es gilt

$$k[M] \cong k[\mathbb{Z}] \overset{7}{\cong} k[x, x^{-1}]\ \ (\subseteq k(x))$$

mit einer Unbestimmten x, d.h. $\mathcal{G}(M)$ ist bis auf Isomorphie gerade die multiplikative Gruppe

$$\mathcal{G}(M) = \mathbf{G}_m$$

(vgl. 2.1.4 Beispiel 2). Man beachte, die Komultiplikation, der Antipode und die Auswertung im neutralen Element von $\mathbf{G}_m$ haben die behauptete Gestalt.

4. Schritt. Der Fall $M \cong \mathbb{Z}/n\mathbb{Z}$ einer endlichen zyklischen Gruppe.
Weil M im Fall $p \neq 0$ keine p-Torsion haben soll, ist n in diesem Fall teilerfremd zu p.
Sei

$$\mathcal{G} := \{\xi \in \mathbf{G}_m \mid \xi^n = 1\} = \{\xi \in k^* \mid \xi^n = 1\}$$

die Gruppe der n-ten Einheitswurzeln. Als endliche Teilmenge von $\mathbf{G}_m$ ist $\mathcal{G}$ abgeschlossen, also eine abgeschlossene Untergruppe von $\mathbf{G}_m$ (und damit diagonalisierbar).
Weil n im Fall $p \neq 0$ teilerfremd zu p ist, hat das Polynom

$$x^n - 1$$

kein mehrfachen Nullstellen, d.h. es ist

$$x^n - 1 = (x - \alpha_1) \bullet \ldots \bullet (x - \alpha_n) \text{ mit } \alpha_1, \ldots, \alpha_n \in k \text{ paarweise verschieden.}$$

Die Faktoren $x - \alpha_i$ sind also paarweise teilerfremd. Nach dem Chinesichen Restesatz ist

---

[7] $\mathbb{Z}$ ist isomorph zur multiplikativen Gruppe der Potenzen einer Unbestimmten mit ganzzahligen Exponenten.

$$k[x]/(x^n-1) \cong k[x]/(x-\alpha_1) \times ... \times k[x]/(x-\alpha_n) \cong k \times ... \times k.$$

Die Multiplikation rechts ist dabei koordinatenweise definiert. Deshalb ist der Ring reduziert, und damit der Koordinatenring von $\mathcal{G}$,

$$k[\mathcal{G}] = k[x]/(x^n-1) = k\bullet 1 + k\bullet\alpha + ... + k\bullet\alpha^{n-1}. \qquad (1)$$

Dabei sei $\alpha := x|_{\mathcal{G}}$ die Einschränkung des Charakters $x: \mathbf{G}_m \longrightarrow k^*$, $t \mapsto t$. Als Einschränkung eines Charakters von $\mathbf{G}_m$ ist α ein Charakter von $\mathcal{G}$. Die Potenzen von α sind ebenfalls Charaktere von $\mathcal{G}$. Mit (1) gilt

$$X^*(\mathcal{G}) = \{1, \alpha, ..., \alpha^{n-1}\},$$

denn jeder Charakter von $\mathcal{G}$ liegt in $k[\mathcal{G}]$ und nach dem Satz von Artin sind verschiedene Charaktere linear unabhängig. Insbesonder ist $X^*(\mathcal{G})$ ist eine zyklische Gruppe der Ordnung n,

$$X^*(\mathcal{G}) \cong M,$$

und der Koordinatenring von $\mathcal{G}$ ist isomorph zur Gruppen-Algebra von M,

$$k[\mathcal{G}] = k[X^*(\mathcal{G})] = k[M].$$

Weil die natürliche Einbettung von $\mathcal{G}(M)$ in $\mathbf{G}_m$ ein Homomorphismus von linearen algebraischen Gruppen ist, bilden die Komultiplikationen, der Antipode und die Auswertungen im neutralen Element von $\mathcal{G}(M)$ und $\mathbf{G}_m$ kommutative Vierecke.

$$\begin{array}{ccc} k[x,x^{-1}] & \xrightarrow{\Delta} & k[x,x^{-1}]\otimes k[x,x^{-1}] \\ \rho\downarrow & & \downarrow\rho\otimes\rho \\ k[M] & \xrightarrow{\Delta_M} & k[M]\otimes k[M] \end{array} \qquad \begin{array}{ccc} k[x,x^{-1}] & \xrightarrow{\iota} & k[x,x^{-1}] \\ \rho\downarrow & & \downarrow\rho \\ k[M] & \xrightarrow{\iota_M} & k[M] \end{array} \qquad \begin{array}{ccc} k[x,x^{-1}] & \xrightarrow{e} & k \\ \rho\downarrow & & \| \\ k[M] & \xrightarrow{e_M} & k \end{array}$$

Dabei sei $\rho: k[\mathbf{G}_m] \twoheadrightarrow k[\mathcal{G}(M)]$ die Einschränkung auf die abgeschlossene Untergruppe. Auf Grund dieser kommutativen Vierecke haben Komultiplikation, Antipode und Auswertung im neutralen Element für $\mathcal{G}(M)$ die behauptete Gestalt (weil sie diese Gestalt für $\mathbf{G}_m$ auf Grund des dritten Schritts haben). Genauer, es gilt

$$\begin{aligned}
\Delta_M(\rho(x)^n) &= \Delta_M(\rho(x^n)) && (\rho \text{ ist Algebra-Homomorphismus}) \\
&= (\rho\otimes\rho)(\Delta(x^n)) && (\text{Kommutativität des ersten Diagramms}) \\
&= (\rho\otimes\rho)(x^n\otimes x^n)) && (\text{Definition von } \Delta) \\
&= \rho(x^n)\otimes\rho(x^n) \\
&= \rho(x)^n\otimes\rho(x)^n && (\rho \text{ ist Algebra -Homomorphismus}) \\
\iota_M(\rho(x)^n) &= \iota_M(\rho(x^n)) && (\rho \text{ ist Algebra -Homomorphismus}) \\
&= \rho(\iota(x^n)) && (\text{Kommutativität des zweiten Diagramms}) \\
&= \rho(x^{-n}) && (\text{Definition von } \iota) \\
&= \rho(x)^{-n} && (\rho \text{ ist Algebra -Homomorphismus}) \\
e_M(\rho(x)^n) &= e_M(\rho(x^n)) && (\rho \text{ ist Algebra -Homomorphismus}) \\
&= \rho(e(x^n)) && (\text{Kommutativität des dritten Diagramms}) \\
&= \rho(1) && (\text{Definition von } e) \\
&= 1 && (\rho \text{ ist Algebra -Homomorphismus})
\end{aligned}$$

Zu (ii). Wegen $k[\mathcal{G}(M)] = k[M]$ ist für jedes $m \in M$ das Elemente $e(m) \in k[M]$ eine reguläre Funktion

$$e(m): \mathcal{G}(M) \longrightarrow k.$$

Für $x,y \in \mathcal{G}(M)$ ist

$$\begin{aligned} e(m)(x \bullet y) &= (e(m) \circ \mu)(x,y) && (\mu \text{ sei die Multiplikation von } \mathcal{G}(M)) \\ &= \mu^*(e(m))(x,y) \\ &= \Delta_M(e(m))(x,y) && (\Delta_M \text{ ist die Komultiplikation}) \\ &= (e(m) \otimes e(m))(x,y) && (\text{Definition der Komultiplikation } \Delta_M) \\ &= e(m)(x) \bullet e(m)(y), \end{aligned}$$

d.h. $e(m)$ ist ein Charakter von $\mathcal{G}(M)$ und die Abbildung

$$\varphi: M \longrightarrow \mathbf{X}^*(\mathcal{G}(M)),\ m \mapsto (x \mapsto e(m)(x))$$

ist korrekt definiert. Für $m', m'' \in M$ und $x \in \mathcal{G}(M)$ gilt

$$\begin{aligned} \varphi(m'+m'')(x) &= e(m'+m'')(x) && (\text{Definition von } \varphi) \\ &= (e(m') \bullet e(m''))(x) && (\text{Definition der Multiplikation in } k[M]) \\ &= e(m')(x) \bullet e(m'')(x) && (\text{Definition der Multiplikation in } k[\mathcal{G}(M)]) \\ &= \varphi(m')(x) \bullet \varphi(m'')(x) && (\text{Definition von } \varphi) \\ &= (\varphi(m') + \varphi(m''))(x). && (\text{Definition der Addition in } \mathbf{X}^*(\mathcal{G}(M))) \end{aligned}$$

Da dies für beliebige $x \in \mathcal{G}(M)$ gilt, folgt

$$\varphi(m'+m'') = \varphi(m') + \varphi(m''),$$

d.h. φ ist ein Gruppen-Homomorphismus. Da die $e(m)$ mit $m \in M$ eine k-Vektorraumbasis von $k[\mathcal{G}(M)] = k[M]$ bilden und die Charaktere von $\mathcal{G}(M)$ in $k[\mathcal{G}(M)]$ liegen und k-linear unabhängig sind, ist jeder Charakter von $\mathcal{G}(M)$ von der Gestalt $e(m)$, d.h. φ ist surjektiv.

Wir haben noch zu zeigen, φ ist injektiv. Dazu reicht es zu zeigen, daß die Zusammensetzung von φ mit der natürlichen Einbettung

$$\mathbf{X}^*(\mathcal{G}(M)) \hookrightarrow k[\mathcal{G}(M)] = k[M]$$

der Charaktergruppe in den Koordinatenring injektiv ist. Diese Zusammensetzung

$$M \longrightarrow k[M],\ m \mapsto e(m),$$

bildet M bijektiv auf eine k-Vektorraumbasis von $k[M]$ ab, ist also insbesondere injektiv.

Zu (iii). Nach 3.2.3 (ii) sind die (rationalen) Charaktere von G Elemente des Koordinatenrings von G. Die natürliche Einbettung

$$M := \mathbf{X}^*(G) \hookrightarrow k[G],\ \chi \mapsto \chi, \tag{3}$$

der Charaktergruppe von G in den Koordinatenring von G läßt sich deshalb zu einer k-linearen Abbildung

$$k[M] \longrightarrow k[G],\ e(\chi) \mapsto \chi,$$

auf die Gruppen-Algebra von M fortsetzen. Diese Abbildung überführt eine k-Vektorraumbasis (nämlich die Erzeuger $e(\chi)$ der Gruppen-Algebra von M) in eine k-Vektorraumbasis des Koordinatenrings von G, und ist deshalb bijektiv. Die Addition der Elemente von $M := \mathbf{X}^*(G)$ entspricht der Multiplikation der Charaktere als Elemente von $k[G]$. Deshalb ist diese Abbildung ein k-Algebra-Isomorphismus.

Nach (i) steht links gerade der Koordinatenring der linearen algebraischen Gruppe $\mathcal{G}(M)$. Der Isomorphimus des Koordinatenrings dieser Gruppe mit dem Koordinatenring der Gruppe G induziert einen Isomorphismus affiner algebraischer Varietäten

$$\psi: G \xrightarrow{\cong} \mathcal{G}(M),$$

welche lineare algebraische Gruppen sind. Wir haben noch zu zeigen,

$$\psi \text{ ist ein Gruppen-Homomorphismus.}$$

Nach Konstruktion erhalten wir, wenn wir zu den Koordinatenringen übergehen und die induzierte Abbildung auf die Charaktergruppe von $\mathcal{G}(M)$ einschränken, einen Gruppen-Homomorphismus (nämlich nach (ii) gerade die natürliche Einbeittung (3)), d.h. es gilt

$$\psi^*(M) \subseteq \mathbf{X}^*(G),$$

und die Abbildung

$$\psi^*: M \longrightarrow \mathbf{X}^*(G),\ \chi \mapsto \chi\circ\psi,$$

ist ein Gruppen-Homomorphismus. Insbesondere ist

$$\chi\circ\psi: G \longrightarrow k^* \text{ ein Gruppen-Homomorphismus} \qquad (4)$$

für jeden Charakter $\chi: \mathcal{G}(M) \longrightarrow k^*$.

Die Gruppen G und $\mathcal{G}(M)$ sind beide diagonaliserbar. Wir können uns beide Gruppen als abgeschlossene Untergruppen geeigneter allgemeiner linearer Gruppen vorstellen, die aus Diagonalmatrizen bestehen.

Die Abbildung ψ überführt deshalb gewisse Diagonalmatrizen, sagen wir

$$a = \mathrm{diag}(a_1,...,a_n) \text{ und } b = \mathrm{diag}(b_1,...,b_1)$$

in Diagonalmatrizen, sagen wir

$$\psi(a) = \mathrm{diag}(\psi_1(a),...,\psi_r(a)) \text{ und } \psi(b) = \mathrm{diag}(\psi_1(b),...,\psi_r(b)).$$

Bezeichne

$$\chi_i: \mathcal{G}(\mathbf{X}^*(G)) \longrightarrow k^*$$

den Charater, der jede Matrix von $\mathcal{G}(\mathbf{X}^*(G))$ auf den i-ten Eintrag auf der Hauptdiagonalen abbildet. Dann gilt

$$\chi_i(\psi(a)) = \psi_i(a)\ ,\ \chi_i(\psi(b)) = \psi_i(b)$$

und

$$\begin{aligned}
\chi_i(\psi(ab)) &= (\chi_i\circ\psi)(ab) \\
&= (\chi_i\circ\psi)(a)\bullet(\chi_i\circ\psi(b)) && \text{(nach (4))} \\
&= \psi_i(a)\bullet\psi_i(b). && \text{(Definition von } \chi_i)
\end{aligned}$$

Da dies für jedes i gilt, ist $\psi(ab)$ die Diagonalmatrix

$$\begin{aligned}
\psi(ab) &= \mathrm{diag}(\psi_1(a)\bullet\psi_1(b),..., \psi_r(a)\bullet\psi_r(b)) \\
&= \mathrm{diag}(\psi_1(a),...,\psi_r(a))\bullet\ \mathrm{diag}(\psi_1(b),...,\psi_r(b)) \\
&= \psi(a)\bullet\psi(b).
\end{aligned}$$

Wir haben gezeigt, daß ψ ein Gruppen-Homomorphismus ist.
QED.
Aus dem obigen Beweis ergeben sich die folgenden

Bemerkungen

(i) Eine reguläre Abbildung

$$\psi: G' \longrightarrow G''$$

von diagonalisierbaren linearen algebraischen Gruppen G' und G'' ist genau dann ein Homomorphismus von linearen algebraischen Gruppen, wenn die beiden folgenden Bedingungen erfüllt sind.

1. Die induzierte Abbildung der Koordinatenringe

$$\psi^*: k[G''] \longrightarrow k[G']$$

bildet die Charaktergruppen ineinander ab,

$$\psi^*(X^*(G'')) \subseteq X^*(G')$$

2. Die auf den Charaktergruppen induzierte Abbildung,

$$\psi^*: X^*(G'') \longrightarrow X^*(G'),$$

ist ein Gruppen-Homomorphismus.

(ii) Für beliebige endlich erzeugte abelsche Gruppen M, M', M'' (ohne p-Torsion, falls die Charakteristik p des Grundkörpers k ungleich Null ist) gilt

(a) $\mathcal{G}(M' \oplus M'') \cong \mathcal{G}(M') \times \mathcal{G}(M'')$
(Isomorphie von linearen algebraischen Gruppen).

(b) $\mathcal{G}(\mathbb{Z}) \cong \mathbf{G}_m$
(Isomorphie von linearen algebraischen Gruppen).

(c) $\mathcal{G}(\mathbb{Z}/n\mathbb{Z})$ ist als lineare algebraische Gruppe isomorph zur Gruppe der n-ten Einheitswurzeln. Dabei sei n teilerfremd zu p, falls $p \neq 0$ ist.

(d) $\# \mathcal{G}(M) = \# M$ falls M endlkich ist.

Beweis von (ii)(d). Nach (ii)(c) haben $\mathbb{Z}/n\mathbb{Z}$ und $\mathcal{G}(\mathbb{Z}/n\mathbb{Z})$ dieselbe Ordnung n, d.h. Aussage (d) gilt trivialerweise. Im allgemeinen Fall ist M direkte Summe endlicher zyklischer Gruppen, sagen wir

$$M \cong (\mathbb{Z}/n_1\mathbb{Z}) \oplus \ldots \oplus (\mathbb{Z}/n_r\mathbb{Z})$$

Für die Ordnungen erhalten wir damit

$$\# M = \#(\mathbb{Z}/n_1\mathbb{Z}) \bullet \ldots \bullet (\mathbb{Z}/n_r\mathbb{Z}) = n_1 \bullet \ldots \bullet n_r$$

und

$$\begin{aligned} \# \mathcal{G}(M) &= \#(\mathcal{G}(\mathbb{Z}/n_1\mathbb{Z}) \times \ldots \times \mathcal{G}(\mathbb{Z}/n_r\mathbb{Z})) \\ &= \# \mathcal{G}(\mathbb{Z}/n_1\mathbb{Z}) \bullet \ldots \bullet \# \mathcal{G}(\mathbb{Z}/n_r\mathbb{Z}) \\ &= n_1 \bullet \ldots \bullet n_r, \end{aligned}$$

d.h. auch im allgemeinen Fall sind die Ordnungen gleich.
QED.

3.2.7 Folgerung: Charakterisierung der Tori

Sei G eine diagonalisierbare lineare algebraische Gruppe über dem (algebraisch abgeschlossenen) Körper k der Charakteristik p. Dann gelten folgende Aussagen.

(i) G ist das Produkt eines Torus mit einer endlichen abelschen Gruppe, deren Ordnung teilerfremd zu p ist im Fall $p \neq 0$.

(ii) G ist genau dann ein Torus, wenn G zusammenbängend ist.

(iii) G ist genau dann ein Torus, wenn die Charaktergruppe $\mathbf{X}^*(G)$ eine freie[8] abelsche Gruppe ist.

Beweis. Zu (i). Nach 3.2.6 (iii) hat G bis auf Isomorphie die Gestalt

$$G \cong \mathcal{G}(M)$$

---

[8] d.h. die Gruppe ist torsionsfrei, d.h. in der Zerlegung in eine direkte Summe zyklischer Gruppen kommt kein direkter Summand von endlicher Ordnung vor, d.h. die Gruppe ist eine direkte Summe von endlich vielen Exemplaren von $\mathbb{Z}$.

mit einer endlich erzeugten abelschen Gruppe M ohne p-Torsion, falls $p \neq 0$ ist. Die Gruppe M ist direktes Produkt von zyklischen Gruppen, d.h.

$$M = \mathbb{Z}^n \oplus M'$$

mit einer endlichen abelschen Gruppe M' ohne p-Torsion.Nach Bemerkung 3.2.6 (ii)(a) folgt

$$G \cong \mathcal{G}(\mathbb{Z}^n) \times \mathcal{G}(M').$$

Es reicht zu zeigen, dies ist eine Faktorzerlegung der behaupteten Gestalt.
Nach den Bemerkungen 3.2.6 (a) und (b) ist der erste Faktor

$$\begin{aligned} \mathcal{G}(\mathbb{Z}^n) &\cong \mathcal{G}(\mathbb{Z}) \times \ldots \times \mathcal{G}(\mathbb{Z}) \quad \text{(n-mal)} \\ &\cong \mathbf{G}_m \times \ldots \times \mathbf{G}_m \quad \text{(n-mal)} \\ &\cong \mathbf{D}_n \end{aligned}$$

ein Torus.
Weil M' endlich ist, ist nach Bemerkung 3.2.6(ii) (d) auch $\mathcal{G}(M')$ endlich und besitzt im Fall $p \neq 0$ keine p-Torsion, also eine zu p teilerfremde Ordnung.

Zu (ii). Wenn die Gruppe G' im obigen Beweis die Ordnung m hat, so ist

$$G \cong \mathbf{D}_n \times G'$$

disjunkte Vereinigung der m abgeschlossenenen Teilmengen

$$\mathbf{D}_n \times \{x\} \text{ mit } x \in G'.$$

Als Varität G genau dann zusammenhängend, wenn deren Anzahl gleich 1 ist, d.h. wenn G' die triviale Gruppe und

$$G \cong \mathbf{D}_n$$

ein Torus ist.
Zu (iii). Ist $\mathbf{X}^*(G)$ eine freie abelsche Gruppe, d.h.

$$\mathbf{X}^*(G) \cong \mathbb{Z}^n,$$

so ist

$$\begin{aligned} G &\cong \mathcal{G}(\mathbf{X}^*(G)) && \text{(nach 3.2.6 (iii))} \\ &\cong \mathcal{G}(\mathbb{Z}^n) \\ &\cong \mathbf{D}_n && \text{(nach dem Beweis von (i))} \end{aligned}$$

ein Torus (nach der Definition in 3.2 1). Ist umgekehrt G ein Torus, d.h.

$$G \cong \mathbf{D}_n,$$

so ist $X^*(G) \cong X^*(\mathbf{D}_n) = \mathbb{Z}^n$ (nach Beispiel 3.2.2).

QED.

3.2.8 Proposition (Starrheit der diagonalisierbaren Gruppen)

Seien

$$G \text{ und } H$$

diagonalisierbare lineare algebraische Gruppen und

$$V$$

eine zusammenhängende affine algebraische Varietät. Weiter sei eine reguläre Familie von Homomorphismen algebraischer Gruppen

$$\phi_t : G \longrightarrow H,\ t \in V,$$

gegeben, d.h. ein Morphismus von algebraischen Varietäten

$$\phi : V \times G \longrightarrow H,\ (t, x) \mapsto \phi(t,x),$$

für welchen die Einschränkungen

$$\phi_t : G \cong \{t\} \times G \longrightarrow H,\ x \mapsto \phi(t,x),$$

mit $t \in V$ Gruppen-Homomorphismen sind. Dann hängt $\phi_t(x) = \phi(t,x)$ nicht von t ab.

Beweis. Sei

$$\psi \in X^*(H) \subseteq k[H]$$

ein Charakter von H (vgl. 3.2.3 (i)). Dann ist

$$\psi\circ\phi\colon V\times G \xrightarrow{\phi} H \xrightarrow{\psi} k$$

eine reguläre Funktion auf $V\times G$,

$$\psi\circ\phi \in k[V\times G] = k[V]\otimes_k k[G].$$

Weil die Charaktere von G eine k-Vektorraumbasis von k[G] bilden,

$$k[G] = \sum_{\chi\in \mathbf{X}^*(G)} k\bullet\chi = \bigoplus_{\chi\in \mathbf{X}^*(G)} k\bullet\chi$$

(nach 3.2.3 (i)), bilden die Elemente $1\otimes\chi$ ein linear unabhängiges Erzeugendensystem von $k[V]\otimes_k k[G]$ über k[V],

$$k[V]\otimes_k k[G] = \sum_{\chi\in \mathbf{X}^*(G)} k[V]\bullet(1\otimes\chi) = \bigoplus_{\chi\in \mathbf{X}^*(G)} k[V]\bullet(1\otimes\chi)$$

(weil das Tensorprodukt mit direkten Summen kommutiert). Damit gibt es eindeutig bestimmte $f_{\chi,\psi} \in k[V]$ mit

$$\psi\circ\phi = \sum_{\chi\in \mathbf{X}^*(G)} f_{\chi,\psi}\otimes\chi,$$

d.h. mit

$$\psi(\phi(t,x)) = \sum_{\chi\in \mathbf{X}^*(G)} f_{\chi,\psi}(t)\bullet\chi(x) \text{ für beliebige } t \in V \text{ und beliebige } x\in G.$$

Für jedes fest gewählte $t \in V$ steht auf der linken Seite ein Charakter von G. Weil die Charaktere von G eine k-Vektorraumbasis von k[G] bilden, ist von den Koeffizienten $f_{\chi,\psi}(t)$ genau einer gleich 1 und alle anderen gleich 0 (für jedes feste t). Insbesondere liegt das Bild der regulären Abbildung

$$f_{\chi,\psi}\colon V \longrightarrow k$$

für jedes χ und jedes ψ in der Menge {0,1}. Weil V zusammenhängend ist, muß auch das Bild bei $f_{\chi,\psi}$ zusammenhängend sein, d.h. die Funktionen sind konstant. Damit ist genau ein $f_{\chi,\psi}$ konstant gleich 1 und alle übrigen $f_{\chi,\psi}$ sind konstant gleich 0: für ein $\chi_0 \in \mathbf{X}^*(G)$ gilt

$$\psi(\phi(t,x)) = \chi_0(x) \text{ für jedes } t\in V \text{ und jedes } x\in G$$

(und jedes $\psi\in\mathbf{X}^*(H)$). Dabei kann χ_0 natürlich von der Wahl des Charakters ψ abhängen. Ersetzt man ψ durch eine k-Linearkombination von Charakteren von H, so steht auf der rechten Seite die zugehörige k-Linearkombination von solchen Charakteren χ_0 von G. Unter diesen Linearkombinationen der ψ sind auch die

Koordinatenfunktionen der Einbettung der algebraischen Varietät H in einen k^n. Die Zusammensetzungen von ϕ mit diesen Koordinatenfunktionen sind gerade die Koordinatenfunktionen der Abbildung ϕ. Diese sind also von t unabhängig. Damit ist auch ϕ von t unabhängig.
QED.

3.2.9 Zentralisator und Normalisator einer abgeschlossenen Untergruppe

3.2.9.1 Definition

Seien G eine lineare algebraische Gruppe und $H \subseteq G$ eine abgeschlossene Untergruppe. Dann heißen

$$\mathbf{Z}_G(H) := \{x \in G \mid xyx^{-1} = y \text{ für jedes } y \in H\}$$

Zentralisator von H in G und

$$\mathbf{N}_G(H) := \{x \in G \mid xHx^{-1} = H\}$$

Normalisator von H in G.

Bemerkungen

(i) $\mathbf{Z}_G(H)$ und $\mathbf{N}_G(H)$ sind abgeschlossene Untergruppen von G.

(ii) $\mathbf{Z}_G(H)$ ist ein Normalteiler von $\mathbf{N}_G(H)$.

Beweis. Zu (i). $\mathbf{Z}_G(H)$ ist Untergruppe von G.

Wegen $eye^{-1} = y$ liegt das neutrale Element e in $\mathbf{Z}_G(H)$.

Mit x', x" $\in \mathbf{Z}_G(H)$ gilt

$$\begin{aligned} (x'x")\bullet y\bullet(x'x")^{-1} &= x'\bullet(x"\bullet y\bullet x"^{-1})\bullet x'^{-1} \\ &= x'\bullet y\bullet x'^{-1} && \text{(wegen } x" \in \mathbf{Z}_G(H)) \\ &= y && \text{(wegen } x' \in \mathbf{Z}_G(H)) \end{aligned}$$

also gilt $x'x" \in \mathbf{Z}_G(H)$.

Mit $x \in \mathbf{Z}_G(H)$ gilt $xyx^{-1} = y$, also $y = x^{-1}y(x^{-1})^{-1}$, also $x^{-1} \in \mathbf{Z}_G(H)$.

$\mathbf{N}_G(H)$ ist Untergruppe von G.

Wegen $eHe^{-1} = H$ liegt das neutrale Element e in $\mathbf{N}_G(H)$.

Mit x', x" $\in \mathbf{N}_G(H)$ gilt

$$\begin{aligned} (x'x")\bullet H\bullet(x'x")^{-1} &= x'\bullet(x"\bullet H\bullet x"^{-1})\bullet x'^{-1} \\ &= x'\bullet H\bullet x'^{-1} && \text{(wegen } x" \in \mathbf{N}_G(H)) \\ &= H && \text{(wegen } x' \in \mathbf{N}_G(H)) \end{aligned}$$

also gilt $x'x" \in \mathbf{N}_G(H)$.

Mit $x \in \mathbf{N}_G(H)$ gilt $xHx^{-1} = H$, also $H = x^{-1}H(x^{-1})^{-1}$, also $x^{-1} \in \mathbf{H}_G(H)$.

$\mathbf{Z}_G(H)$ ist abgeschlossen in G.

Für $x \in G$ bezeichen mit mit σ_x die reguläre Abbildung

$\sigma_x: G \longrightarrow G, y \mapsto xyx^{-1}$.

Dann gilt nach Definition

$$\begin{aligned}\mathbf{Z}_G(H) &= \{x \in G \mid xyx^{-1} = y \text{ für jedes } y \in H\} \\ &= \{x \in G \mid x = yxy^{-1} \text{ für jedes } y \in H\} \\ &= \{x \in G \mid x = \sigma_y(x) \text{ für jedes } y \in H\} \\ &= \bigcap_{y \in H} \{x \in G \mid \sigma_y(x) = Id(x)\}\end{aligned}$$

Zum Beweis der Behauptung reicht es zu zeigen, daß für jedes $y \in H$ die Menge

$\{x \in G \mid \sigma_y(x) = Id(x)\}$ = Urbild der Diagonalen $\Delta_G \subseteq G \times G$ bei $(\sigma_y, Id): G \longrightarrow G \times G$

abgeschlossen ist in G. Als affine Varietät ist G separiert. Deshalb ist die Diagonale

$$\Delta_G := \{(x,x) \mid x \in G\} \subseteq G \times G$$

abgeschlossen in $G \times G$. Dann ist aber auch das Uribild von Δ_G bei der regulären Abildung

$$(\sigma_y, Id): G \longrightarrow G \times G,\ x \mapsto (\sigma_y(x), x)$$

abgeschlossen (vgl. auch Beispiel 1.6.6).

Alternativer Beweis. Sei $x_1,...,x_n \in k[G]$ ein Erzeugendensystem der k-Algebra k[G].

Zwei Punkte $p,q \in G$ sind genau dann gleich, wenn gilt

$$x_i(p) = x_i(q) \text{ für } i = 1,..., n$$

(weil diese dann dieselben Koordinaten haben). Damit gilt

$$\begin{aligned}\mathbf{Z}_G(H) &= \{p \in G \mid qpq^{-1} = p \text{ für jedes } q \in H\} \\ &= \{p \in G \mid x_i(qpq^{-1}) = x_i(p) \text{ für jedes } q \in H \text{ und für } i = 1,...,n\} \\ &= \{p \in G \mid (x_i \circ \sigma_q)(p) = x_i(p) \text{ für jedes } q \in H \text{ und für } i=1,...,n\} \\ &= V(\sigma_q^*(x_1)-x_1,..., \sigma_q^*(x_n)-x_n),\end{aligned}$$

Dies ist eine abgeschlossene Teilmenge von G.

$\mathbf{N}_G(H)$ ist abgeschlossen in G.

Als abgeschlossene Teilmenge hat H die Gestalt

$$H = V(f_1,...,f_m) \text{ mit } f_i \in k[G].$$

Damit gilt

$$\begin{aligned}\mathbf{N}_G(H) &= \{x \in G \mid xHx^{-1} = H\} \\ &= \{x \in G \mid xHx^{-1} \subseteq H \text{ und } x^{-1}Hx \subseteq H\} \\ &= \{x \in G \mid xhx^{-1} \subseteq H \text{ und } x^{-1}hx \subseteq H \text{ für jedes } h \in H\} \\ &= \{x \in G \mid f_i(xhx^{-1}) = 0 \text{ und } f_i(x^{-1}hx) = 0 \text{ für jedes } h \in H\}\end{aligned}$$

Seien $\mu: G \times G \longrightarrow G$ die Multiplikation von G und $i: G \longrightarrow G$ der Übergang zum Inversen. Dann gilt

$$\begin{aligned}xhx^{-1} &= \mu(x, hx^{-1}) \\ &= \mu(x,\mu(x, i(h)))\end{aligned}$$

$$= (\mu\circ(Id\times\mu)\circ(Id\times\ Id\times i))(x,h,x)$$
$$= (\mu\circ(Id\times\mu)\circ(Id\times\ Id\times i)\circ(Id\times\tau))(x,x,h)$$
$$= (\mu\circ(Id\times\mu)\circ(Id\times\ Id\times i)\circ(Id\times\tau)\circ(\Delta\times Id))(x,h)$$
$$= \varphi(x,h)$$

mit einer regulären Abbildung φ. Dabei bezeichne

$$\tau: G\times G \longrightarrow G\times G,\ (u,v) \mapsto (v,u),$$

die reguläre Abbildung,welche die Koordinaten vertauscht und

$$\Delta: G \longrightarrow G\times G,\ x \mapsto (x,x),$$

die Diagonaleinbettung. Analog erhält man

$$x^{-1}hx = \psi(x,h)$$

mit ener regulären Abbildung ψ. Mit diesen Bezeichnungen gilt

$$\mathbf{N}_G(H) = V(\varphi^*(f_i)(x,h), \psi^*(f_i)(x,h) \mid h \in H,\ i = 1,...,m).$$

Dies ist eine abgeschlossene Teilmenge von G.

Zu (ii). Für jedes $g \in \mathbf{N}_G(H)$ gilt

$$g\mathbf{Z}_G(H)g^{-1} = \{gxg^{-1} \mid x \in G \text{ und } xyx^{-1} = y \text{ für jedes } y\in H\ \}$$
$$= \{x \mid x \in G \text{ und } (g^{-1}xg)y(g^{-1}xg)^{-1} = y \text{ für jedes } y\in H\ \}$$
$$= \{x \mid x \in G \text{ und } g^{-1}xgyg^{-1}x^{-1}g = y \text{ für jedes } y\in H\ \}$$
$$= \{x \mid x \in G \text{ und } xgyg^{-1}x^{-1} = gyg^{-1} \text{ für jedes } y\in H\ \}$$
$$= \{x \mid x \in G \text{ und } xyx^{-1} = y \text{ für jedes } y\in gHg^{-1}\ \}$$

Wegen $g \in \mathbf{N}_G(H)$ gilt $gHg^{-1} = H$, also

$$g\mathbf{Z}_G(H)g^{-1} = \{x \mid x \in G \text{ und } xyx^{-1} = y \text{ für jedes } y\in H\ \} = \mathbf{Z}_G(H).$$

QED.

3.2.9.2 Folgerung

Seien G eine diagonalisierbare lineare algebraische Gruppe und $H \subseteq G$ eine abgeschlossene Untergruppe. Dann gelten die folgenden Aussagen.

(i) $\mathbf{Z}_G(H)$ und $\mathbf{N}_G(H)$ haben dieselbe Komponenten der Eins,

$$\mathbf{Z}_G(H)^0 = \mathbf{N}_G(H)^0$$

(ii) $\mathbf{N}_G(H)/\mathbf{Z}_G(H)$ ist endlich.

Beweis. Zu (i). Wir betrachten die Abbildung

$$V\times H \longrightarrow H,\ (t, x) \mapsto txt^{-1},$$

mit $V = \mathbf{N}_G(H)^0$. Als abgeschlossene Untergruppe einer diagonaliserbaren Gruppe ist H diagonalisierbar (vgl. die Definition in 3.2.1). Wir können deshalb 3.2.8 auf diese Abbildung anwenden, und sehen, daß die Abbildung nicht von t abhängt, d.h. es gilt $txt^{-1} = exe^{-1} = x$ für jedes $t \in \mathbf{N}_G(H)^0$ und jedes $x \in H$. Mit anderen Worten, es gilt

$$\mathbf{N}_G(H)^0 \subseteq \mathbf{Z}_G(H),$$

also

$$\mathbf{N}_G(H)^0 \subseteq \mathbf{Z}_G(H)^0.$$

Wegen

$$\mathbf{Z}_G(H)^0 \subseteq \mathbf{Z}_G(H) \subseteq \mathbf{N}_G(H)$$

liegt $\mathbf{Z}_G(H)^0$ auch in der Zusammenhangskomponente der Eins von $\mathbf{N}_G(H)$, d.h. zusammen gilt $\mathbf{N}_G(H)^0 = \mathbf{Z}_G(H)$.

Zu (ii). $\mathbf{N}_G(H)/\mathbf{Z}_G(H)$ ist eine Faktorgruppe der Gruppe

$$\mathbf{N}_G(H)/\mathbf{Z}_G(H)^0,$$

welche nach (i) gleich

$$\mathbf{N}_G(H)/\mathbf{N}_G(H)^0.$$

Es reicht zu zeigen, letztere Gruppe ist endlich. Das ist aber der Fall nach 2.2.1(i). **QED**.

3.2.10 Aufgaben

Sei G eine diagonalisierbare lineare algebraische Gruppe über k mit der Charaktergruppe

$$X := \mathbf{X}^*(G).$$

Bezeichne

$$p$$

die Charakteristik des Grundkörpers k.

3.2.10 Aufgabe 1: Eine Anti-Äquivalenz von Kategorien

Beschreiben Sie Kategorien, deren Objekte die diagonalisierbaren linearen algebraischen Gruppe über k sind bzw. die endlich erzeugten abelschen Gruppen ohne p-Torsion. Geben sie eine Anti-Äquivalenz zwischen diesen Kategorien an.

Konstruktion der Anti-Äquivalenz.

Sei

Ab'

die Kategorie der endlich erzeugten abelschen Gruppen ohne p-Torsion, deren Morphismen die Gruppen-Homomorphismen sind. Auf der anderen Seite sei

Diag

die Kategorie der diagonalisierbaren linearen algebraischen Gruppen, deren Morphismen die Homomorphismen algebraischer Gruppen seien. Für jedes Objekt G der Kategorie **Diag** ist die Charaktergruppe $\mathbf{X}^*(G)$ ein Objekt der Kategorie **Ab**' (nach 3.2.4),

$$G \in |\mathbf{Diag}| \Rightarrow \mathbf{X}^*(G) \in |\mathbf{Ab}'|.$$

Für jeden Homomorphismus $h:G \longrightarrow G'$ diagonalisierbarer Gruppen und jeden Charakter $\chi:G' \longrightarrow \mathbf{G}_m$ ist die Zusammensetzung

$$\mathbf{X}^*(h)(\chi) := h^*(\chi) = \chi \circ h: G \xrightarrow{h} G' \xrightarrow{\chi} \mathbf{G}_m$$

ein Homomomorphismus von algebraischen Gruppen, also ein Charakter von G. Für je zwei Charaktere χ', $\chi'': G' \longrightarrow \mathbf{G}_m$ gilt für $\chi = \chi'$, χ'' und $x \in G$ außerdem

$$\begin{aligned}
h^*(\chi)(x) &= \chi(h(x)) \\
&= (\chi'+\chi'')(h(x)) && \text{(Definition von } \chi) \\
&= \chi'(h(x)) \bullet \chi''(h(x)) && \text{(Definition der Summe von Charakteren)} \\
&= h^*(\chi')(x) \bullet h^*(\chi'')(x) && \text{(Definition von } h^*)
\end{aligned}$$

$= (h^*(\chi')+h^*(\chi''))(x)$ (Definition der Summe von Charakteren)

Da dies für alle $x \in G$ gilt, folgt

$$h^*(\chi'+\chi'') = h^*(\chi')+h^*(\chi''),$$

d.h. $\mathbf{X}^*(h) = h^*$ ist ein Gruppen-Homomorphismus $\mathbf{X}^*(G') \longrightarrow \mathbf{X}^*(G)$.

$$h \in \mathrm{Hom}_{\mathbf{Diag}}(G, G') \Rightarrow \mathbf{X}^*(h) \in \mathrm{Hom}_{\mathbf{Ab}},(\mathbf{X}^*(G'), \mathbf{X}^*(G)).$$

Tatsächlich ist auf diese Weise ein kontravarianter Funktor

$$\mathbf{X}^*: \mathbf{Diag} \longrightarrow \mathbf{Ab}'$$

definiert, denn für je zwei Homomorphismen $G \xrightarrow{h} G' \xrightarrow{h'} G''$ diagonalisierbarer Gruppen und jeden Charakter $\chi: G'' \longrightarrow G$ gilt

$$\begin{aligned}\mathbf{X}^*(h\circ h')(\chi) &= \chi\circ h\circ h' \\ &= \mathbf{X}^*(h')(\chi\circ h) \\ &= \mathbf{X}^*(h')(\mathbf{X}^*(h)(\chi)) \\ &= (\mathbf{X}^*(h')\circ\mathbf{X}^*(h))(\chi),\end{aligned}$$

also

$$\mathbf{X}^*(h\circ h') = \mathbf{X}^*(h')\circ\mathbf{X}^*(h).$$

(und trivialerweise $\mathbf{X}^*(\mathrm{Id}_G) = \mathrm{Id}_{X^*(G)}$). Wir haben zu zeigen, der Funktor

$$\mathbf{X}^*: \mathbf{Diag}^{\mathrm{op}} \longrightarrow \mathbf{Ab}'$$

des Duals von **Diag** mit Werten in **Ab**' ist eine Äquivalenz von Kategorien. Dazu reicht es, die folgenden beiden Aussagen zu beweisen.

(a) Für je zwei diagonalisierbare Gruppen G', G'', ist die Abbildung

$$\mathrm{Hom}_{\mathbf{Diag}}(G', G'') \longrightarrow \mathrm{Hom}_{\mathbf{Ab}},(\mathbf{X}^*(G''), \mathbf{X}^*(G')),\ h \mapsto (\chi \mapsto \chi\circ h),\ \text{bijektiv.}$$

(b) Jede endlich erzeugte abelsche Gruppe $M \in |\mathbf{Ab}'|$ ohne p-Torsion ist isomorph zu einer abelschen Gruppe der Gestalt $X^*(G)$ mit $G \in |\mathbf{Diag}|$.

(siehe zum Beispiel Bucur & Deleanu [1], Kapitel I,§6, Proposition 1.19). Aussage (b) ergibt sich direkt aus 3.2.6 (ii).

Injektivität der Abbildung von (a). Direkt aus der Definition der Abbildung liest man ab, daß es sich um einen Gruppen-Homomorphismus handelt. Es reicht also zu zeigen, daß der Kern dieser Abbildung trivial ist. Sei also

$$h: G' \longrightarrow G''$$

ein Element aus dem Kern der Abbildung von (a). Dann ist

$$h^*: \mathbf{X}^*(G'') \longrightarrow \mathbf{X}^*(G'),\ \chi \mapsto \chi\circ h,$$

die Null-Abbildung, d.h. $\chi\circ h$ ist für jedes $\chi \in X^*(G'')$ der triviale Charakter,

$$\chi\circ h(x) = 1 \text{ für jedes } x \in G' \text{ und jedes } \chi \in \mathbf{X}^*(G'').$$

Da jedes Element von $k[G'']$ eine k-Linearkombination von Elementen aus $X^*(G'')$ ist (nach 3.2.3 (ii)), ist für jedes $f \in k[G'']$ die Abbildung

$$f\circ h: G' \longrightarrow G'' \longrightarrow k,\ x \mapsto f(h(x)),$$

eine konstante Abbildung (als k-Linearkombination von konstanten Abbildungen), d.h. $f(h(x))$ hängt nicht von x ab. Weil unter den $f \in k[G'']$ insbesondere die Koordinatenfunktionen auf G'' sind, hängt $h(x)$ nicht von $x \in G'$ ab. Weil h ein Gruppen-Homomorphismus ist, besteht

Im(h)

nur aus dem neutralen Element von G. Wir haben gezeigt, der Kern der Abbildung von (a) ist trivial.
Surjektivität der Abbildung von (b). Jeder Gruppen-Homomorphismus

$$h: \mathbf{X}^*(G'') \longrightarrow \mathbf{X}^*(G'')$$

der Charaktergruppen induziert einen k-Algebra-Homomorphismus

$$h: k[\mathbf{X}^*(G'')] \longrightarrow k[\mathbf{X}^*(G'')]$$

der zugehörigen Gruppen-Algebren, den wir ebenfalls mit h bezeichnen wollen (seine Einschränkung auf die Charaktergruppe von G" ist das ursprüngliche h). Dieser läßt sich interpretieren als k-Algebra-Homomorphismus

$$h: k[\mathcal{G}(X^*(G''))] \longrightarrow k[\mathcal{G}(X^*(G'))]$$

von Koordinatenringen diagonalisierbarer Gruppen (nach 3.2.6 (i)). Die Gruppen

$$\mathcal{G}(X^*(G'')) \text{ und } \mathcal{G}(X^*(G'))$$

sind nach 3.2.6 (iii) isomorph zu G" bzw. G'. Die Identifikation der Gruppen-Algebren mit den Koordinatenringen läß sich deshalb so wählen, daß der k-Algebra-Homomorphismus h die Gestalt

$$h: k[G''] \longrightarrow k[G']$$

bekommt. Dann kommt h von einer regulären Abbildung

$$\varphi: G' \longrightarrow G'',$$

d.h. es ist $\varphi^* = h$, d.h.

$$h(\chi) = \varphi^*(\chi) = \chi \circ \varphi.$$

Nach der Bemerkung von 3.2.6 ist φ ein Homomorphismus von linearen algebraischen Gruppen. sDer vorgegebene Gruppen-Homorphismus h liegt also im Bild der Abbildung von (a).
QED.

3.2.10 Aufgabe 2: Eine problematische Aufgabe

Sei $\phi: G \longrightarrow H$ ein Homomorphismus von diagonalisierbaren linearen algebraischen Gruppen und bezeichne

$$\phi^*: X^*(H) \longrightarrow X^*(G)$$

die induzierte Abbildung der Charaktergruppen. Beweisen sie die folgenden Implikationen.

(i) ϕ ist injektiv $\Rightarrow$ ϕ^* ist surjektiv.

(ii) ϕ ist surjektiv $\Rightarrow$ ϕ^* ist injektiv.

Bemerkungen

(i) Zur Implikation von Aussage (i) in der angegebenen Formulierung kann man ein Gegenbeispiel angeben. Die Implikation besteht jedoch, wenn eine zusätzliche Bedingung erfüllt ist oder wenn man die Formulierung durch deren kategoriale Variante ersetzt.

(ii) Das Gegenbeispiel. Ist die Charakteristik p des Grundkörpers k positiv, so ist der Homomorphismus von diagonalisierbaren linearen algebraischen Gruppen

$$\varphi: G_m = k^* \longrightarrow k^* = G_m,\ t \mapsto t^p,$$

injektiv. Die induzierte Abbildung auf den Charaktergruppen hat bis auf Isomorphie (in additiver Schreibweise) die Gestalt

$$\varphi^*: \mathbb{Z} \longrightarrow \mathbb{Z},\ n \mapsto p \bullet n,$$

ist also nicht surjektiv.

(iii) Die kategoriale Variante. Wir verwenden die in der Konstruktion zu 3.2.10 Aufgabe 1 eingeführten Bezeichnungen

Diag

für die Kategorie der diagonalisierbaren linearen algebraischen Gruppen und Homomorphismen algebraischer Gruppen und

Ab'

für die Kategorie der endlich erzeugten abelschen Gruppen ohne p-Torsion. Dann bestehen die folgenden beiden Implikationen.

ϕ ist ein Monomorphismus von **Diag** $\Rightarrow$ ϕ^* ist ein Epimorphismus von **Ab**'.

ϕ ist ein Epimorphismus von **Diag** $\Rightarrow$ ϕ^* ist ein Monomorphismus von **Ab**'.

Beide Implikationen sind eine Konsequenz der in 3.2.10 Aufgabe 1 konstruierten Anti-Äquivalenz (siehe zum Beispiel Schubert [1], Band II, Kapitel 16, Abschnitt 16.2, Theorem 16.2.4, Aussage (b) und die Erklärung der Bedeutung der Wörter "respektieren" in 1.2.3, 2.1.1,7.4.5 und "entdecken" in 7.7.6 und 7.7.9).

(iv) Die Implikation von Aussage (i) besteht unter der Zusatzbedingung, daß ϕ ein <u>separabler Morphismus</u> , d.h. $k(G^0)$ ist eine separable Körpererweiterung von $k(H^0)$, vgl. Hartshorne [1], Kapitel IV, Abschnitt 2, Definition vor Proposition 2.1). Siehe den Beweis zu (i).

(v) Man beachte, der Homomorphismus φ^* des Gegenbeispiels ist in **Ab**' ein Epimorphismus: für je zwei Gruppen-Homomorphismen

$$f,g: \mathbb{Z} \longrightarrow M$$

von abelschen Gruppen ohne p-Torsion mit $f\circ\varphi^* = g\circ\varphi^*$ gilt für jedes $n \in \mathbb{Z}$:

$$p\bullet f(n) = f(p\bullet n) = g(p\bullet n) = p\bullet g(n)$$

also

$$p\bullet(f(n)-g(n)) = 0.$$

Weil M keine p-Torsion besitzt folgt $f(n) = g(n)$ für jedes n, also $f = g$.

Der Kokern von φ^* in **Ab**' ist Null, denn für jeden Morphismus $f: \mathbb{Z}\longrightarrow M$ in **Ab**' mit $f\circ \varphi^* = 0$ gilt $0 = f(p\bullet n) = p\bullet f(n)$ für jedes $n \in \mathbb{Z}$. Weil M keine p-Torsion besitzt, folgt $f = 0$, d.h. f faktorisiert sich über das Null-Objekt.

Weil der Kokern $\mathbb{Z}/p\mathbb{Z}$ von φ^* in Ab, eine abelsche Gruppe mit p-Torsion ist,

Beweis. <u>Zu (ii)</u>. Seien χ' und χ" Charaktere von H mit

$$\phi^*(\chi') = \phi^*(\chi''),$$

d.h.

$$\chi'\circ\phi = \xi''\circ\phi.$$

Weil ϕ surjektiv ist, folgt $\chi' = \xi''$.

<u>Zu (i)</u>. <u>Beweis im Fall φ separabel</u>.

1. <u>Schritt</u>. Reduktion auf den Fall φ bijektiv,

Nach 2.2.5 (ii) ist das Bild von G eine abgeschlossene Untergruppe von H. Die natürliche Einbettung $\phi(G) \hookrightarrow H$ induziert einen surjektiven k-Algebra-Homomorphismus

$$k[H] \twoheadrightarrow k[\phi(G)].$$

Weil die Charaktere von H den Koordinatenring k[H] erzeugen (vgl. 3.2.3 (ii)), erzeugen deren Bilde in $k[\phi(G)]$ den Koordinatenring $k[\phi(G)]$. Diese Bilder sind aber Charaktere von $\phi(G)$ (weil ϕ eine Homomorphismus von algebraischen Gruppen ist). Wegen linearen Unabhängigkeit der Charaktere von $\phi(G)$(nach 3.2.3 (ii)) ist die Einschränkungshomomorphismus

$$\mathbf{X}^*(H) \twoheadrightarrow \mathbf{X}^*(\phi(G))$$

ebenfalls surjektiv. Zum Beweis der Behauptung reicht es zu zeigen, daß der bijektive Homomorphismus diagonalisierbarer Gruppen

$$G \longrightarrow \phi(G)$$

eine Surjektion $\mathbf{X}^*(\phi(G)) \longrightarrow \mathbf{X}^*(G)$ induziert.

und damit einen surjektiven Gruppen-Homomorphismus

$$X^*(H) \twoheadrightarrow X^*(\varphi(G)),\ \chi \mapsto \chi|_{\varphi(G)}$$

(vgl.3.2.3(ii)).

2. Schritt. Sei $\varphi: G \longrightarrow H$ bijektiv. Wir beweisen die folgenden Aussagen.

1. $\varphi(G^0) = H^0$.

2. $\dim G = \dim G^0 = \dim H^0 = \dim H$.

3. $G = G^0 \times G'$ und $H \cong H^0 \times H'$ mit endlichen Gruppen Untergruppen G' und H' von G bzw. H..

4. φ induziert einen Isomorphismus $\varphi^0 = \varphi|_{G^0} : G^0 \xrightarrow{\cong} H^0$.

5. Bei geeigneter Wahl von H' gilt $\varphi(G') = H'$ und φ induziert einen Isomorphismus von linearen algebraischen Gruppen

$$\phi' = \varphi|_{G'} : G' \xrightarrow{\cong} H'.$$

6. $\phi: G \longrightarrow H$ ist ein Isomorphismus (so daß auch $X^*(\phi): X^*(H) \longrightarrow X^*(G)$ ein Isomorphismus und als solcher surjektiv ist).

Beweis von Aussage 1 des zweiten Schritts.

Weil die Komponente der Eins G^0 zusammenhängend ist und das neutrale Element von G enthält, ist auch $\varphi(G^0)$ zusammenhängend und enthält das neutrale Element von H. Deshalb gilt

$$\varphi(G^0) \subseteq H^0$$

(weil H^0 die Zusammenhangskomponente ist, welche das neutrale Element enthält, und jede zusammenhängende Teilmenge ganz in einer Zusammenhangskomponente liegt). Es folgt

$$G^0 \subseteq \phi^{-1}(H^0).$$

Wir zerlegen $\phi^{-1}(H^0)$ in Nebenklassen modulo G^0 sagen wir

$$\phi^{-1}(H^0) = g_1 G^0 \cup \ldots \cup g_r G^0 \text{ mit } g_1 = e \text{ und die } g_i G^0 \text{ paarweise disjunkt.}$$

Wir wenden φ an und erhalten

$$H^0 = \varphi(g_1)\ \varphi(G^0) \cup \ldots \cup \varphi(g_r)\varphi(G^0). \qquad (1)$$

Weil φ bijektiv ist, sind auch die $\varphi(g_i)\ \varphi(G^0)$ paarweise disjunkt. Nach 2.2.5 (ii) ist

$$\varphi(G^0)$$

eine abgeschlossene Untergruppe von H^0. Deshalb ist (1) eine Zerlegung von H^0 in paarweise disjunkte abgeschlossene Teilmengen. Weil H^0 zusammenhängend ist, gilt

$$H^0 = \varphi(g_i)\ \varphi(G^0)$$

für ein i. Weil das neutrale Element von H in H^0 und $\varphi(G^0)$ liegt, muß i = 1 gelten, d.h. g_i ist das neutrale Element und

$$H^0 = \varphi(G^0),$$

wie behauptet.

Beweis von Aussage 2 des zweiten Schritts.

Es reicht zu zeigen dim G^0 = dim H^0 (nach Bemerkung 2.2.1.2 (ii)). Weil

$$\varphi^0: G^0 \longrightarrow H^0$$

surjektiv ist, ist die induzierte Abbildung der Koordinatenringe

$$k[H^0] \longrightarrow k[G^0],\ f \mapsto f\circ\varphi^0,$$

injektiv. Deshalb ist

$$\dim H^0 = \text{tr. deg}_k\, k[H^0] \leq \text{tr.deg}_k\, k[G^0] = \dim G^0$$

(nach Definition der Dimension im irreduziblen Fall in 1.8.1.3), d.h.

$$\dim H^0 \leq \dim G^0.$$

Wir haben noch die umgekehrte Ungleichung zu beweisen.

Als zusammenhängende diagonalisierbare Gruppe ist G^0 ein Torus (nach 3.2.7 (ii)), d.h.

$$G^0 \cong \mathbf{D}_n = \mathbf{G}_m \times ... \times \mathbf{G}_m \text{ (n-mal mit } n = \dim G^0)$$

Auf Grund von

$$\{1\}\times\{1\}\times...\times\{1\} \subset \mathbf{G}_m\times\{1\}\times...\times\{1\} \subset \mathbf{G}_m\times \mathbf{G}_m\times...\times\{1\}\subset...\subset \mathbf{G}_m\times...\times\mathbf{G}_m$$

gibt es in G^0 eine echt aufsteigende Kette von abgeschlossenen Untergruppen der Länge n = dim G^0. Weil ϕ bijektiv ist erhalten wir durch Anwenden von ϕ eine echt aufsteigenden Kette von Untergruppen von H^0. Die Untergruppen der Kette sind abgeschlossen (nach 2.2.5 (ii)). Deshalb gilt

$$\dim H^0 \geq n = \dim G^0.$$

Beweis von Aussage 3 des zweiten Schritts.

Nach 3.2.7 ist G das Produkt eine Torus $T \cong \mathbf{D}_n$ mit einer endlichen abelschen Gruppe, sagen wir $G' = \{g_1,...,g_r\}$ mit $g_1 = e$, d.h.

$$G = T\times G' = T\times\{g_1\} \bigcup ... \bigcup T\times\{g_r\}$$

Dies ist eine Zerlegung in paarweise disjunkte abgeschlossene und irreduzible Teilmengen, d.h. die Zerlegung in irreduzible Komponenten. Die Komponene der Eins ist gerade

$$G^0 = T\times\{g_1\} = T\times\{e\}.$$

Wenn wir T mit der Untergruppe T×{e) von G identifizieren, wird T gerade die Komponente der 1 von G und G wird zum (inneren) direkten Produkt

$$G = G^0\times G'.$$

Analog sieht man

$$G = H^0\times H'.$$

mit $H' \subseteq H$ endlich.

Beweis von Aussage 4 des zweiten Schritts.

Als zusammenhängende diagonalisierbare Gruppen derselben Dimension sind G^0 und H^0 Tori derselben Dimension, sagen wir n, d.h

$$\begin{aligned} G^0 &\cong \mathbf{D}_n \\ &\cong \mathbf{G}_m\times...\times\mathbf{G}_m \qquad \text{(n-mal)} \\ &\cong \mathcal{G}(\mathbb{Z})\times...\times\mathcal{G}(\mathbb{Z}) \qquad \text{(n-mal)} \end{aligned}$$

$$\cong \mathcal{G}(\mathbb{Z}^n)$$

und analog

$$H^0 \cong \mathcal{G}(\mathbb{Z}^n).$$

Weil $\phi^0: G^0 \longrightarrow H^0$ bijektiv, also surjektiv ist, ist die induzierte Abbildung der Charaktergruppen injektiv und hat die Gestalt

$$X^*(\phi^0):X^*(H^0) \cong \mathbb{Z}^n \hookrightarrow \mathbb{Z}^n \cong X^*(G^0).$$

Wir identifizieren die Gruppe $X^*(H^0)$ mit deren Bild bei dieser Abbildung, d.h. mit einer Untergruppe von $X^*(G^0)$.
Nach dem Elementarteilersatz kann man eine Basis $\{e_i\}$ der freien abelschen Gruppe $X^*(G^0)$ so wählen,

$$\mathbb{Z}^n = \mathbb{Z}\bullet e_1+...+\mathbb{Z}\bullet e_n,$$

daß die Untergruppe $X^*(H^0)$ die Gestalt

$$X^*(H^0) = \mathbb{Z}\bullet d_1\bullet e_1+...+\mathbb{Z}\bullet d_n\bullet e_n$$

bekommt mit natürlichen Zahlen, die sich sukzessive teilen: $d_1|d_2|...|d_n$. Zerlegt man G^0 und H^0 in direkte Produkt bezüglich dieser neu gewählten Basis, so bekommt h die Gestalt eines direkten Produkts

$$\varphi = \varphi_1\times...\times \varphi_n: G^0= \mathbf{G}_m\times ...\times \mathbf{G}_m \longrightarrow \mathbf{G}_m\times ... \times \mathbf{G}_m = H^0$$

von Abbildungen

$$\varphi_i: k^* = \mathbf{G}_m \longrightarrow \mathbf{G}_m = k^*, c \mapsto c^{d_i}.$$

Als Einschränkungen von φ müssen auch die φ_i injektiv sein. Das ist aber nur für

$$d_i \in \{\pm 1, \pm p^\nu \mid \nu = 1,2, ...\}$$

der Fall (andernfalls haben alle d_i-ten Einheitswurzeln dasselbe Bild). Indem wir bei Bedarf einige der e_i durch ihr Negatives ersetzen, erreichen wir

$$d_i \in \{1, p^\nu \mid \nu = 1,2, ...\},$$

sagen wir

$$d_i = p^{\nu_i}.$$

Falls eines der ν_i ungleich 0 ist, ist die durch ϕ induzierte Abbildung der Funktionenkörper der Komponenten der Eins,

$$\varphi^*: k(H^0) \longrightarrow k(G^0),$$

eine inseparable Körpererweiterung. Deshalb muß

$$d_i = 1$$

gelten für jedes i, d.h. jedes der φ_i ist ein Isomorphismus. Damit ist aber auch φ ein Isomorphismus.

Bemerkung

Der allgemeine Fall unterscheidet sich vom separablen Fall nur durch zusätzliche Frobenius-Abbildungen, die sich "kürzen" lassen: weil k ein algebraisch abgeschlossener Körper ist, ist die Abbildung

$$k^* \longrightarrow k^*, x \mapsto x^p, \qquad (2)$$

ein Isomorphismus von Körpern. Indem wir die Koordinaten-Darstellung des i-ten Faktors $\mathbf{G}_m$ von H^0 mit Hilfe der ν_i-fach iterierten Frobenius-Abbildung (2) abändern, erreichen wir

$$d_i = 1.$$

Dadurch wird aber jedes φ_i und damit auch φ ein Isomorphismus.

Beweis von Aussage 5 des zweiten Schritts.
Betrachten wir die Zerlegung

$$G = G^0 \bullet G' = \bigcup_{x \in G'} G^0 \bullet x$$

von G in Nebenklassen modulo G^0. Auf Grund von Aussage 1 des ersten Schritts erhalten wir durch Anwenden der Bijektion φ eine Zerlegung

$$H = \bigcup_{x \in G'} H^0 \bullet \varphi(x) = H^0 \bullet \varphi(G')$$

von H in paarweise disjunkte zusammenhängende Teilmengen, welche Nebenklassen von H modulo H^0 sind. Die endiche (also abgeschlossene) Untergruppe $\varphi(G')$ von H besteht somit gerade aus einem Repräsentantensystem H/H^0 und es gilt

$$H = H^0 \bullet \varphi(G') = H^0 \times \varphi(G')$$

Wir können deshalb annehmen,

$$\varphi(G') = H'.$$

Als Bijektion von endlichen (also abgeschlossenen) Untergruppen von G bzw. H ist die Einschränkung

$$\phi' = \varphi|_{G'} : G' \xrightarrow{\cong} H'.$$

ein Isomorphismus von linearen algebraischen Gruppen.

Beweis von Aussage 6 des zweiten Schritts.
Nach der Wahl von H' wie in Aussage 5 des zweiten Schritts bekommt φ die Gestalt

$$\varphi = (\varphi|_{G^0}) \times (\varphi|_{G'}) : G^0 \times G' \longrightarrow H^0 \times H',$$

wenn wir die beiden direkten Produkte als innere direkte Produkte auf auffassen und diese so mit

$$G^0 \times G' = G^0 \bullet G' = G \text{ bzw. } H^0 \times H' = H^0 \bullet H' = H$$

identifizieren: für $g \in G^0$ und $x \in G'$ gilt

$$\begin{aligned}
\varphi((g,x)) &= \varphi(g \bullet x) && \text{(Identifikation von } G^0 \times G' \text{ mit G)} \\
&= \varphi(g) \bullet \varphi(x) && (\varphi \text{ ist Gruppen-Homomorphismus)} \\
&= (\varphi(g), \varphi(x)) && \text{(Identifikation von } h^0 \times h' \text{ mit H)} \\
&= ((\varphi|_{G^0}) \times (\varphi|_{G'}))(g,x),
\end{aligned}$$

also

$$\varphi = (\varphi|_{G^0}) \times (\varphi|_{G'})$$

Als direktes Produkt von Isomorphismen linearer algebraischer Gruppen ist φ ein Isomorphismus von linearen algebraischen Gruppen. Weil auf Grund von Aufgabe 1 der Funktor

$$\mathbf{X}^* : \mathbf{Diag} \longrightarrow \mathbf{Ab}'$$

eine Äquivalenz von Kategorien ist, ist das Bild des Isomorphismus φ von **Diag** bei diesem Funktor,

$$\varphi^* = \mathbf{X}^*(\varphi): \mathbf{X}^*(H) \longrightarrow \mathbf{X}^*(G)$$

ein Isomorphismus von **Ab**'. Insbesondere ist φ^* bijektiv, also auch surjektiv.
QED.

3.2.10 Aufgabe 3

Konstruieren Sie einen natürlichen Isomorphismus abelscher Gruppen

$$G \cong \mathrm{Hom}(\mathbf{X}^*(G), k^*).$$

Bemerkungen

(i) Nach 3.2.10 Aufgabe 1 ist $\mathbf{X}^*$: $\mathbf{Diag}^{op} \longrightarrow \mathbf{Ab}$' eine Äquivalenz von Kategorien. Es gibt also einen zu $\mathbf{X}^*$ quasi-inversen[9] Funktor

$$\mathbf{Ab}' \longrightarrow \mathbf{Diag}.$$

(ii) Die funktoriellen Isomorphismen von 3.2.6 (ii) und (iii),

$$\mathrm{Id} \overset{\cong}{\longrightarrow} X^* \circ \mathcal{G} \text{ von Funktoren } \mathbf{Ab}' \longrightarrow \mathbf{Ab}'$$

und

$$\mathcal{G} \circ X^* \longrightarrow \mathrm{Id} \text{ von Funktoren } \mathbf{Diag} \longrightarrow \mathbf{Diag}$$

zeigen, daß der in 3.2.6 konstruierte Funktor

$$\mathcal{G}: \mathbf{Ab}' \longrightarrow \mathbf{Diag}$$

gerade dieser zu $\mathbf{X}^*$ quasi-inverse Funktor ist.

(iii) Der unten konstruierte funktorielle Morphismus zeigt, daß $\mathcal{G}(M)$ als als abelsche Gruppe gerade gleich

$$\mathcal{G}(M) = \mathrm{Hom}_{\mathbf{Ab}}(M, k^*)$$

ist.

Konstruktion.

1. Schritt Konstruktion eines Morphismus von Funktoren $\mathbf{Diag} \longrightarrow \mathbf{Ab}$

Für jede diagonalisierbare lineare algebraische Gruppe G betrachten wir die Abbildung

$$\varphi = \varphi_G: G \longrightarrow \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(G), k^*),\ x \mapsto (\chi \mapsto \chi(x)), \qquad (1)$$

d.h. für $x \in G$ und $\chi \in \mathbf{X}^*(G)$ sei

$$\varphi(x)(\chi) = \chi(x).$$

Diese Abbildung ist wohldefiniert, denn $\varphi(x)$ ist für jedes $x \in G$ ein Homomorphismus abelscher Gruppen: für χ' , $\chi'' \in X^*(G)$ gilt

$$\begin{aligned}\varphi(x)(\chi'+\chi'') &= (\chi'+\chi'')(x)\\ &= \chi'(x)\bullet\chi''(x)\\ &= \varphi(x)(\chi')\bullet\ \varphi(x)(\chi'').\end{aligned}$$

Abbildung (1) ist ein Gruppen-Homomorphismus, denn für $x,y \in G$ und $\chi \in \mathbf{X}^*(G)$ gilt

$$\begin{aligned}\varphi(x\bullet y)(\chi) &= \chi(x\bullet y)\\ &= \chi(x)\bullet\chi(y)\\ &= \varphi(x)(\chi)\bullet\varphi(y)(\chi)\\ &= (\varphi(x)\bullet\varphi(y))(\chi)\end{aligned}$$

also

$$\varphi(x\bullet y) = \varphi(x)\bullet\varphi(y).$$

---

[9] Schubert [1] benutzt die Bezeichnung "äquivalenzinvers", vgl. Band II, Kapitel 16, Abschnitt 16.2, Definitin 16.2.1.

Wir haben noch zu zeigen, der Gruppen-Homomorphismus (1) ist einfunktoriell bezüglich G, d.h. ein Morphismus

$$\mathrm{Id} \longrightarrow \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(?),k^*),$$

von Funktoren **Diag** $\longrightarrow$ **Ab** (wenn Id, den Vergiß-Funktor **Diag** $\hookrightarrow$ **Ab** bezeichnet).

Sei h: G $\longrightarrow$ H ein Homomorphismus von diagonalisierbaren linearen algebraischen Gruppen. Wir haben die Kommutativität des Diagramms

$$\begin{array}{ccc} G & \xrightarrow{\varphi_G} & \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(G),k^*) \\ h\downarrow & & \downarrow h^* \\ H & \xrightarrow{\varphi_H} & \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(H),k^*) \end{array}$$

Sei $x \in G$. Dann gilt für $\chi \in \mathbf{X}^*(H)$:

$$\begin{aligned} h^*(\varphi_G(x))(\chi) &= \varphi_G(x)(\chi\circ h) && \text{(Definition von } h^*) \\ &= (\chi\circ h)(x) && \text{(Definition von } \varphi_G) \\ &= \chi(h(x)) \\ &= \varphi_H(h(x))(\chi) && \text{(Definition von } \varphi_H) \end{aligned}$$

Da dies für alle $\chi \in X^*(H)$ gilt, folgt

$$\mathrm{Hom}(\mathbf{X}^*(h),k^*)\circ\varphi_G(x)) = \varphi_H\circ h.$$

Das Diagramm ist also tatsächlich kommutativ.

Wir haben noch zu zeigen, daß die Abbildung (1) bijektiv ist.

2. Schritt: Reduktion auf den Fall $G \cong \mathcal{G}(Z)$ mit einer zyklischen Gruppe Z ohne p-Torsion.

Als diagonalisierbare Gruppe hat G die Gestalt $G = \mathcal{G}(M)$ mit einer endlich erzeugten abelschen Gruppe M ohne p-Torsion (nach 3.2.6 (iii)). Die abelsche Gruppe M ist direktes Produkt von endlich vielen zyklischen Gruppen, sagen wir

$$M = Z_1 \times \ldots \times Z_r \text{ mit } Z_i \text{ zyklisch und ohne p-Torsion.}$$

Wegen Bemerkung 3.2.5 (i) ist

$$G = \mathcal{G}(M) = \mathcal{G}(Z_1) \times \ldots \times \mathcal{G}(Z_r).$$

Die natürlichen Projektionen auf die Faktoren

$$p_i : G \longrightarrow \mathcal{G}(Z_i)$$

sind Homomorphismen von algebraischen Gruppen und liefern kommutative Diagramme

$$\begin{array}{ccc} G & \xrightarrow{\varphi_G} & \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(G),k^*) \\ p_i\downarrow & & \downarrow p_i^* \\ Z_i & \xrightarrow{\varphi_{Z_i}} & \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(Z_i),k^*) \end{array}$$

Diese setzen sich zu einem kommutativen Diagramm

$$\begin{array}{ccc} G & \xrightarrow{\varphi_G} & \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(G),k^*) \\ \prod_{i=1}^{r} p_i \downarrow \cong & & \downarrow p_i^* \\ \prod_{i=1}^{r} Z_i & \xrightarrow{\prod_{i=1}^{r} \varphi_{Z_i}} & \prod_{i=1}^{r} \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(Z_i),k^*) \end{array}$$

zusammen. Da der Hom-Funktor direkte Summen im ersten Argument in direkte Produkte überführt, können wir dieses Diagramm auch in der folgenden Gestalt schreiben.

$$\begin{array}{ccc} G & \xrightarrow{\varphi_G} & \mathrm{Hom}_{\mathbf{Ab}}(\mathbf{X}^*(G),k^*) \\ \prod_{i=1}^{r} p_i \downarrow \cong & & \downarrow p_i^* \\ \prod_{i=1}^{r} Z_i & \xrightarrow{\prod_{i=1}^{r} \varphi_{Z_i}} & \mathrm{Hom}_{\mathbf{Ab}}(\sum_{i=1}^{r} \mathbf{X}^*(Z_i),k^*) \end{array}$$

Die rechte vertikale Abbildung erhält man durch Anwenden des kontravarianten Hom-Funktors auf die Abbildung

$$\sum_{i=1}^{r} X^*(Z_i) \longrightarrow X^*(G),\ (\chi_1,\ldots,\chi_r) \mapsto \sum_{i=1}^{r} \chi_i \circ p_i$$

Letztere Abbildung ist ein Isomorphismus (nach 3.2.6 (ii))[10]. Die rechte vertikale Abbildung des Diagramms ist deshalb bijektiv. Zum Beweis der Bijektivität von φ_G reicht es also, die Bijektivität der unteren horizontalen Abbildung zu beweisen. Damit aber reicht es zu zeigen, daß φ_G bijektiv ist im Fall

$$G = \mathcal{G}(Z)$$

mit einer zyklischen Gruppe Z ohne p-Torsion.

3. Schritt. Der Fall $G = \mathcal{G}(Z)$ mit $Z = \mathbb{Z}$.

In diesem Fall ist

$$G = \mathbf{G}_m\ ,$$

die multiplikative Gruppe (vgl. den dritten Schritt im Beweis von 3.2.6(i)). Die Abbildung φ_G hat die Gestalt

$$\varphi = \varphi_G : \mathbf{G}_m = k^* \longrightarrow \mathrm{Hom}(\mathbb{Z}, k^*),\ t \mapsto (n \mapsto t^n).$$

Sei ψ die Abbildung

$$\psi\colon \mathrm{Hom}(\mathbb{Z}, k^*) \longrightarrow k^* = \mathbf{G}_m,\ \ell \mapsto \ell(1).$$

Dann gilt mit $c \in k^*$:

$$\psi(\varphi(c)) = \psi(n \mapsto c^n) = c, \text{ also } \psi\circ\varphi = \mathrm{Id}$$

und mit $\ell \in \mathrm{Hom}(\mathbb{Z}, k^*)$:

$$\varphi(\psi(\ell)) = \varphi(\ell(1)) = (n \mapsto \ell(1)^n).$$

Dabei ist

$$\ell(1)^n) = \ell(1)\bullet\ldots\bullet\ \ell(1) \qquad \text{(n-mal)}$$

---

[10] zusammen mit $\mathcal{G}(M'\oplus M'') = \mathcal{G}(M')\times\mathcal{G}(M'')$ wegen Bemerkung 3.2.5 (i).

$= \ell(1+...+1)$ (ℓ ist Gruppen-Homomorphismus)
$= \ell(n)$,

also

$\varphi(\psi(\ell)) = \ell$, also $\varphi\circ\psi = Id$.

Die Abbildungen sind zueinander invers. Insbesondere ist φ bijektiv.

4. Schritt. Der Fall $G = \mathcal{G}(\mathbb{Z}/m\mathbb{Z})$ mit einer zu p teilerfremden natürlichen Zahl m.
In diesem Fall ist

$$G = \mu_m$$

die Gruppe der m-ten Einheitswurzeln von k (vgl. den vierten Schritt im Beweis 3.2.6 (i)). Die Abbildung φ_G hat die Gestalt

$$\varphi = \varphi_G: \mu_m \longrightarrow \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, k^*),\ t \mapsto (n \bmod m \mapsto t^n).$$

Man beachte die Charaktere von μ_m sind die Einschränkungen der Charaktere von G_m auf μ_m (weil μ_m abgeschlossene Untergruppe von G_m und die Einschränkungsabbildung $k[G_m] \longrightarrow k[\mu_m]$ surjektiv ist). Analog zum dritten Schritt betrachten wir die Abbildung

$$\psi: \mathrm{Hom}(\mathbb{Z}/m\mathbb{Z}, k^*) \longrightarrow k^* = \mu_m,\ \ell \mapsto \ell(1 \bmod m).$$

Die Abbildung ist korrekt definiert, denn es gilt

$\ell(1 \bmod m)^m = \ell(1+...+1 \bmod m)$ (m Summanden)
$= \ell(m \bmod m)$
$= \ell(0)$
$= 1$ (ℓ ist Gruppen-Homomorphismus)

Wie im dritten Schritt erhalten wir für $c \in \mu_m$:

$\psi(\varphi(c)) = \psi(n \bmod m \mapsto c^n) = c$, also $\psi\circ\varphi = Id$

und mit $\ell \in \mathrm{Hom}(\mathbb{Z}, k^*)$:

$\varphi(\psi(\ell)) = \varphi(\ell(1 \bmod m)) = (n \mapsto \ell(1)^n) = \ell$, also $\varphi\circ\psi = Id$.

Die Abbildungen sind zueinander invers. Insbesondere ist φ bijektiv.

Die Injektivität der Abbildung (1) kann man leicht ohne die obige Reduktion auf den Fall, daß die Charaktergruppe zyklisch ist, beweisen:

5. Schritt Abbildung (1) ist injektiv.
Weil die Abbildung ein Gruppen-Homomorphismus ist, reicht es zu zeigen, daß deren Kern die triviale Untergruppe von G ist. Dazu reicht es zu zeigen, der Kern von φ_G besteht aus nur einem Element. Dazu wiederum reicht es zu zeigen, je zwei Kern-Elemente haben dieselben Koordinaten (bezüglich irgendeiner Einbettung von G in einen k^n). Es reicht also, wenn wir zeigen,

$$\text{Jede Funktion } f \in k[G] \text{ ist konstant auf } \mathrm{Ker}(\varphi_G) \qquad (2)$$

Sei also $f \in k[G]$. Weil die Charaktere von G eine k-Vektorraumbasis von k[G] bilden (nach 3.2.3 (ii)), hat f die Gestalt

$$f = c_1\chi_1 + ... + c_r\chi_r \text{ mit } c_i \in k \text{ und } \chi_i \in \mathbf{X}^*(G).$$

Für $g \in \mathrm{Ker}(\varphi_G)$ gilt $\chi(g) = 1$ für jedes $\chi \in \mathbf{X}^*(G)$, also ist der Wert

$$f(g) = c_1\chi_1(g)+...+ c_r\chi_r(g) = c_1 +...+ c_r$$

von f in g unabhänig von g.

Ein direkter Beweis der Surjektivität, ohne Reduktion auf den zyklischen Fall, ist weniger offensichtlich. Wir brauchen zunächst eine Vorbereitung (vgl. Springer [3], 2.5.3).

6. Schritt. Seien G eine diagonalisierbare lineare algebraische Gruppe und $H \subseteq G$ eine abgeschlossene Untergruppe. Dann ist H der Durchschnitt der Kerne von endlich vielen Charakteren von G,

$$H = V(\chi_1-1,...,\chi_r-1) \text{ mit } \chi_1,...,\chi_r \in X^*(G).$$

Wir betrachten die folgenden Ideale von k[G].

$I := \{f \in k[G] \mid f(H) = 0\}$ (das Ideal I(H) von H in k[G])

$J := (\chi-1 \mid \chi\in X^*(G) \text{ und } \chi(H) = 1)\bullet k[G]$

Es reicht zu zeigen, $I \subseteq J$ (die umgekehrte Inklusion besteht trivialerweise). Sei

$$f \in I - \{0\}.$$

Weil die Elemente von X*(G) eine Basis von k[G] bilden (vgl. 3.2.3 (ii)), hat f die Gestalt

$$f = c_1\chi_1+...+ c_r\chi_r \text{ mit } c_i\in k - \{0\} \text{ und } \chi_i \in \mathbf{X}^*(G). \qquad (3)$$

Wir schränken auf H ein und erhalten

$$0 = c_1\chi_1|_H+...+ c_r\chi_r|_H.$$

Weil Familien von paarweise verschiedenen Charakteren linear unabhängig sind über k, gibt es unter den Charakteren $\chi_\nu|_H$ zwei gleiche, sagen wir

$$\chi_i|_H = \chi_j|_H .$$

Dann ist $\chi := (\chi_i)^{-1}\chi_j$ ein Charakter von G, welcher identisch 1 ist auf H. Wegen

$$\chi_j = \chi_i + (\chi_j - \chi_i) = \chi_i + \chi_i \bullet(\chi - 1) \text{ und } \chi_i \bullet(\chi - 1) \in J$$

also

$$\chi_j = \chi_i \mod J$$

können wir die Anzahl der Summanden auf der rechten Seite von (3) verkleinern (wobei wir anstelle der Identität eine Kongruenz modulo J erhalten,

$$f \equiv c_1\chi_1+...+ c_{j-1}\chi_{j-1}+ c_{j+1}\chi_1+...+ c_{j+1}\chi_r \mod J$$

wobei der Koeffizient von c_i von χ_i durch c_i+c_j zu ersetzen ist. Durch erneutes Einschränken auf H können wir die obigen Argumente wiederholen und so die Anzahl der Summanden auf der rechten Seite weiter verkleinern. Nach endlich vielen Schritten erhalten wir $f \equiv 0 \mod J$, d.h. $f \in J$, wie behauptet.

7. Schritt. Abbildung (1) ist surjektiv.
Wir können annehmen, G ist eine abgeschlossene Untergruppe von $\mathbf{D}_r$,

$$G \subseteq \mathbf{D}_r = \{ \begin{pmatrix} c_1 & 0 & .. & 0 \\ 0 & c_2 & \dots & 0 \\ & & & \\ 0 & 0 & \dots & c_r \end{pmatrix} \mid c_i \in k^* \}.$$

Bezeichne

$$x_i : \mathbf{D}_r \longrightarrow k^*, \begin{pmatrix} c_1 & 0 & .. & 0 \\ 0 & c_2 & \dots & 0 \\ & & & \\ 0 & 0 & \dots & c_r \end{pmatrix} \mapsto c_i ,$$

die Abbildung, welche jede Matrix auf den i-ten Eintrag der Hauptdiagonalen abbildet. Die x_i sind Charaktere von $\mathbf{D}_n$, welche die Charaktergruppe $X^*(G)$ erzeugen,

$$X^*(\mathbf{D}_n) = \mathbb{Z} \bullet x_1 + ... + \mathbb{Z} \bullet x_r .$$

Jeder Charakter $\chi \in \mathbf{X}^*(\mathbf{D}_n)$ ist als reguläre Funktion ein Potenzprodukt der x_i mit ganzzahligen Exponenten,

$$\chi = (x_1)^{\nu_1} \bullet ... \bullet (x_r)^{\nu_r} \text{ mit } \nu_i = \nu_i(\chi) \in \mathbb{Z}.$$

Nach dem 6. Schritt gibt es Charaktere

$$\chi_1, \dots , \chi_s \in X^*(G)$$

mit

$$G = V(\chi_1 - 1, \dots , \chi_s - 1) = \{ A \in \mathbf{D}_n \mid \chi_i(A) = 1 \text{ für } i = 1,..., s \}$$

Sei $\ell \in \mathrm{Hom}(\mathbf{X}^*(G), k^*)$. Ist $\chi \in X^*(G)$ identisch 1 auf G, so gilt - weil ℓ ein Gruppen-Homomorphismus ist -

$$\begin{aligned} 1 = \ell(1) = \ell(\chi|_G) &= \ell((x_1)^{\nu_1} \bullet ... \bullet (x_r)^{\nu_r}|_G) \\ &= \ell((x_1|_G)^{\nu_1} \bullet ... \bullet (x_r|_G)^{\nu_r}) \\ &= \ell(x_1|_G)^{\nu_1} \bullet ... \bullet \ell(x_r|_G)^{\nu_r}) \\ &= \chi(\ell(x_1|_G), ..., \ell(x_r|_G)) \end{aligned}$$

Dies gilt insbesondere für $\chi = \chi_i$ für i = 1,..., s. Mit anderen Worten, die Matrix

$$\mathrm{diag}(\ell(x_1|_G), ..., \ell(x_r|_G))$$

ist eine gemeinsame Nullstelle von der Gleichungen von G in $\mathbf{D}_n$, d.h.

$$\mathrm{diag}(\ell(x_1|_G), ..., \ell(x_r|_G)) \in G.$$

Damit ist die Abbildung

$$\psi : \mathrm{Hom}(\mathbf{X}^*(G), k^*) \longrightarrow G, \ell \mapsto \mathrm{diag}(\ell(x_1|_G), ..., \ell(x_r|_G)),$$

wohldefiniert. Direkt an der Abbildungsvorschrift liest man ab, daß es sich um einen Gruppen-Homomorphismus handelt.

Für $g \in G$ gilt

$$\psi(\varphi(g)) = \psi(\chi \mapsto \chi(g))$$

$$= \mathrm{diag}(\ell(x_1|_G), ..., \ell(x_r|_G)) \text{ mit } \ell(\chi) = \chi(g)$$
$$= \mathrm{diag}(x_1|_G(g), ..., x_r|_G(g))$$
$$= \mathrm{diag}(x_1(g), ..., x_r(g))$$
$$= g,$$

Da dies für jedes $g \in G$ gilt, folgt

$$\psi \circ \varphi = \mathrm{Id}. \tag{4}$$

Insbesondere ist φ injektiv und ψ surjektiv. Zum Beweis der Behauptung reicht es zu zeigen, daß ψ auch injektiv ist.

Für zwei ℓ', ℓ'' $\in \mathrm{Hom}(\mathbf{X}^*(G), k^*)$ mit $\psi(\ell') = \psi(\ell'')$ gilt

$$\mathrm{diag}(\ell'(x_1|_G), ..., \ell(x_r|_G)) = \mathrm{diag}(\ell''(x_1|_G), ..., \ell(x_r|_G)),$$

also

$$\ell'(x_i|_G) = \ell''(x_i|_G) \text{ für } i = 1,...,r.$$

Die x_i bilden ein Erzeugendensystem der Charaktergruppe $X^*(\mathbf{D}_n)$. Weil G eine abgeschlossene Untergruppe von $\mathbf{D}_n$ ist, d.h. die Einschränkung auf G,

$$k[\mathbf{D}_n] \twoheadrightarrow k[G],$$

ist surjektiv, induziert also eine Surjektion

$$\mathbf{X}^*(\mathbf{D}_n) \twoheadrightarrow \mathbf{X}^*(G).$$

Deshalb bilden die $x_i|_G$ ein Erzeugendensystem von $\mathbf{X}^*(G)$. Die Homomorphismen ℓ' und ℓ'' stimmen also auf einem Erzeugendensystem ihres Definitonsbereicht überein, sind also gleich

$$\ell' = \ell''.$$

Wir haben gezeigt, daß ψ bijektiv ist. Also ist auch φ bijektiv, insbesondere also surjektiv.
QED.

*Error! Bookmark not defined.**3.2.10 Aufgabe 4***
Sei

$$H \subseteq G$$

eine abgeschlossene Untergruppe von G und

$$Y \subseteq X$$

eine Untergruppe von $X := \mathbf{X}^*(G)$. Wir definieren

$$H^{\perp} := \{\chi \in X \mid \chi(H) = \{1\}\}$$

$$Y^{\perp} := \{x \in G \mid \chi(x) = 1 \text{ für jedes } \chi \in Y\}.$$

Beweisen Sie die folgenden Aussagen.

(i) $(H^{\perp})^{\perp} = H$.

(ii) $(Y^{\perp})^{\perp} = Y$ falls X/Y keine p-Torsion besitzt.

Beweis. Zu (i). 1. Schritt. $H \subseteq (H^{\perp})^{\perp}$

Seien $x \in H$ und $Y := H^{\perp}$. Nach Definition von Y ist jedes $\chi \in Y$ in allen Punkten von H gleich 1. Insbesondere ist

$$\chi(x) = 1.$$

Das dies für jedes $\chi \in Y$ gilt, folgt

$$x \in Y^{\perp} = (H^{\perp})^{\perp}.$$

2. Schritt. $H \supseteq (H^{\perp})^{\perp}$.
Weil H eine abgeschlossene Untergruppe von G, ist H der Durchschnitt der Kerne von endlich vielen Charakteren von G (nach dem sechsten Schritt im Beweis von 3.2.10 Aufgabe 3), d.h. es gibt $\chi_1,...,\chi_r \in X^*(G)$ mit

$$\begin{aligned} H &= \mathrm{Ker}(\chi_1) \cap ... \cap \mathrm{Ker}(\chi_r) \\ &= \{x \in G \mid \chi_i(x) = \{1\} \text{ für } i = 1,...,r\} \end{aligned}$$

Nach Definition ist

$$(H^{\perp})^{\perp} = \{ x \in G \mid \chi(x) = \{1\} \text{ für } \chi \in H^{\perp}\}$$

Weil jedes χ_i identisch 1 auf H ist, also in $H^{\perp}$ liegt, folgt

$$(H^{\perp})^{\perp} \subseteq \{ x \in G \mid \chi_i (x) = 1 \text{ für } i = 1,...,r\} = H.$$

Zu (ii). 3. Schritt. $Y \subseteq (Y^{\perp})^{\perp}$.
Sei

$$H := Y^{\perp} = \{x \in G \mid \chi(x) = 1 \text{ für jedes } \chi \in Y\}.$$

Dann ist jedes $\chi \in Y$ auf H identisch 1,

$$\chi(H) = \{1)$$

also

$$\chi \in H^{\perp} = (Y^{\perp})^{\perp}$$

4. Schritt: $(Y^{\perp})^{\perp} \subseteq Y$.
Wir nutzen die Tatsache, daß die Funktoren

$$X^*: \mathbf{Diag} \longrightarrow \mathbf{Ab}', G \mapsto \mathbf{X}^*(G) \text{ und } \mathcal{G}: \mathbf{Ab}' \longrightarrow \mathbf{Diag}, M \mapsto \mathcal{G}(M)$$

zueinander quasi-inverse Anti-Äquivalenzen von Kategorien sind (vgl. 3.2.10 Aufgaben 1 und 3). Diese Funktoren sind additiv (induzieren Gruppen-Homomorphismen auf den Hom-Mengen) und überführen Kerne in Kokerne und Kokerne in Kerne (siehe zum Beispiel Schubert [1], Band II, Kapitel 16, Abschnitt 16.2, Theorem 16.2.4, Aussage (b) und die Erklärung der Bedeutung der Wörter "respektieren" in 1.2.3, 2.1.1,7.4.5 und "entdecken" in 7.7.6 und 7.7.9).

Wir wenden den Funktor $\mathcal{G}$ auf die natürliche Inklusion $Y \hookrightarrow X$ an und erhalten einen Homomorphismus von diagonalisierbaren Gruppen

$$G \overset{\cong}{\longrightarrow} \mathcal{G}(X) \longrightarrow \mathcal{G}(Y)$$

Der Isomorphismus links ist dabei der Isomorphismus von 3.2.6 (iii) (wegen X = X*(G)). Dieser Homomorphismus läßt sich nach 3.2.10 Aufgabe 3 in ein kommutatives Viereck

$$\begin{array}{ccc} & \mathrm{Hom}(X,k^*) & \longrightarrow & \mathrm{Hom}(Y,k^*) \\ & \cong\uparrow & & \uparrow\cong \\ G = & \mathcal{G}(X) & \longrightarrow & \mathcal{G}(Y) \end{array}$$

einbetten. Die obere Zeile dieses Diagramms läßt sich erweitern: wir wenden den Hom-Funktor $\mathrm{Hom}_{\mathbf{Ab}}(?,k^*)$ auf die kurze exakte Sequenz

$$0 \longrightarrow Y \longrightarrow X \longrightarrow X/Y \longrightarrow 0$$

von abelschen Gruppen ohne p-Torsion an und erhalten die exakte Sequenz

$$1 \longrightarrow \mathrm{Hom}(X/Y, k^*) \longrightarrow \mathrm{Hom}(X, k^*) \longrightarrow \mathrm{Hom}(Y, k^*)$$

und damit das kommutative Diagramm mit exakten Zeilen

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Hom}(X/Y,k^*) & \longrightarrow & \mathrm{Hom}(X,k^*) & \longrightarrow & \mathrm{Hom}(Y,k^*) & \longrightarrow & 1 \\ & & \cong\uparrow & & \cong\uparrow & & \uparrow\cong & & \\ 1 & \longrightarrow & \mathrm{Ker}(G\longrightarrow \mathcal{G}(Y)) & \longrightarrow & G & \longrightarrow & \mathcal{G}(Y) & \longrightarrow & 1 \end{array}$$

Die Exaktheit an den Stellen Hom(Y,k*) und $\mathcal{G}(Y)$ ergibt sich wie folgt. Die natürliche Inklusion

$$Y \hookrightarrow X$$

induziert eine Inklusion der Gruppen-Algebren

$$k[Y] \hookrightarrow k[X]$$

und damit einen injektiven k-Algebra-Homomorphismus

$$k[\mathcal{G}(Y)] \hookrightarrow k[\mathcal{G}(X)] \cong k[G]$$

(vgl. 3.2.6). Die Injektivität des letzteren bedeutet, das Bild des Homomomorphismus algebraischer Gruppen

$$G \longrightarrow \mathcal{G}(Y)$$

liegt dicht in $\mathcal{G}(Y)$.Nach 2.2.5 (ii) ist dieses Bild aber abgeschlossen in $\mathcal{G}(Y)$, d.h.

$$G \twoheadrightarrow \mathcal{G}(Y)$$

ist surjektiv.

Den Kern links unten können wir identifizieren mit

$$\begin{aligned} \mathrm{Ker}(G\longrightarrow \mathcal{G}(Y)) &= \mathrm{Ker}(G \longrightarrow \mathrm{Hom}(X,k^*) \longrightarrow \mathrm{Hom}(Y,k^*),\ x \mapsto (\chi\mapsto\chi(x)) \\ &= \{x \in G \mid \chi(x) = 1 \text{ für } \chi\in Y\} \\ &= Y^{\perp} \end{aligned}$$

Wir erhalten so eine exakte Sequenz von diagonalisierbaren linearen algebraischen Gruppen

$$1 \longrightarrow Y^{\perp} \longrightarrow G \longrightarrow \mathcal{G}(Y) \longrightarrow 1.$$

Insbesondere ist $\mathcal{G}(Y) = \mathrm{Koker}(Y^{\perp} \longrightarrow G)$. Wir gehen zu den Charakteren über und erhalten auf Grund der Bemerkungen am Anfang des Beweises und wegen 2.3.6 (ii):

$$\begin{aligned} \mathbf{X}^*(\mathcal{G}(Y)) &= \mathrm{Ker}(\mathbf{X}^*(G) \longrightarrow \mathbf{X}^*(Y^{\perp}),\ \chi \mapsto \chi|_{Y^{\perp}}) \\ &= \{\chi\in\mathbf{X}^*(G) \mid \chi(x) = 1 \text{ für jedes } x \in Y^{\perp}\} \\ &= (Y^{\perp})^{\perp}. \end{aligned}$$

Nach 2.3.6 (ii) besteht eine natürliche Isomorphie $Y \cong \mathbf{X}^*(\mathcal{G}(Y))$. Wenn wir die Surjektion $G \twoheadrightarrow \mathcal{G}(Y)$ des obigen Diagramms verwenden, um die Charaktergruppe von $\mathcal{G}(Y)$ mit einer Charaktergruppe von G und damit mit einer Untergruppe von X zu identifizieren, wird aus dieser Isomorphie eine Gleichheit,

$$Y = \mathbf{X}^*(\mathcal{G}(Y)).$$

Zusammen erhalten wir die Behauptung.

QED.

3.2.10 Aufgabe 5

Für jede natürliche zu p teilerfremde Zahl n sei

$$G_n := \{x \in G \mid x^n = e\}$$

die Untergruppe der n-Torsionspunkte (d.h. der Punkte, deren Ordnung ein Teiler von n ist). Beweisen Sie die folgenden Aussagen.

(i) $(G_n)^{\perp} = n \bullet X^*(G)$.

(ii) Die Untergruppe der Elemente endlicher Ordnung von G liegt dicht in G.

Beweis. Zu (i). 1. Schritt. Die Abbildung $\varphi: G \longrightarrow G$, $x \mapsto x^n$, induziert auf den Charaktergruppen die Multiplikation mit n,

$$\varphi^*: X^*(G) \longrightarrow X^*(G),\ \chi \mapsto n \bullet \chi.$$

Wir können annehmen, G ist eine abgeschlossene Untergruppe von $\mathbf{D}_r$,

$$G \hookrightarrow \mathbf{D}_r .$$

Die Abbildung

$$\varphi: \mathbf{D}_r \longrightarrow \mathbf{D}_r,\ A = \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{rr} \end{pmatrix} \mapsto A^n = \begin{pmatrix} a_{11}^n & 0 & \dots & 0 \\ 0 & a_{22}^n & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{rr}^n \end{pmatrix},$$

ist ein Homomorphismus von linearen algebraischen Gruppen. Wir betrachten das kommutative Diagramm

$$\begin{array}{ccc} \mathbf{D}_r & \xrightarrow{\varphi} & \mathbf{D}_r \\ \cup & & \cup \\ G & \xrightarrow{\varphi|G} & G \end{array}$$

Sei

$$T_{ii}: \mathbf{D}_r \longrightarrow k^*,\ \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & a_{rr} \end{pmatrix} \mapsto a_{ii},$$

die Projektion auf den i-ten Eintrag auf der Hauptdiagonalen. Dann ist $\mathbf{X}^*(\mathbf{D}_r)$ die von den T_{ii} erzeugte freie abelsche Gruppe,

$$\mathbf{X}^*(\mathbf{D}_r) = \mathbb{Z} \bullet T_{11} + \dots + \mathbb{Z} \bullet T_{rr}.$$

Wegen $T_{ii}(\varphi(A)) = T_{ii}(A^n) = a_{ii}^n = (n \bullet T_{ii})(A)$, d.h. $\varphi^*(T_{ii}) = n \bullet T_{ii}$, ist

$$\varphi^*: \mathbf{X}^*(\mathbf{D}_r) \longrightarrow \mathbf{X}^*(\mathbf{D}_r),\ \chi \mapsto n \bullet \chi,$$

gerade die Multiplikation mit n. Wegen der Kommutativität des Diagramms

$$\begin{array}{ccc} \mathbf{X}^*(\mathbf{D}_r) & \xrightarrow{\varphi^*} & \mathbf{X}^*(\mathbf{D}_r) \\ \downarrow & & \downarrow \\ \mathbf{X}^*(G) & \xrightarrow{\varphi|_G^*} & \mathbf{X}^*(G) \end{array}$$

ist auch $\varphi|_G^*: \mathbf{X}^*(G) \longrightarrow \mathbf{X}^*(G)$ die Multiplikation mit n. Wegen

$$G_n = \mathrm{Ker}(\varphi|_G: G \longrightarrow G, x \mapsto x^n)$$

ist

$$G_n^{\perp} = \{\chi \in X^*(G) \mid \chi(x) = 1 \text{ für } x \in G_n\}$$

$$= \{\chi \in X^*(G) \mid \chi(x) = 1 \text{ für jedes } x \in G \text{ mit } x^n = 1\}$$

$X^*(G_n) = \mathrm{Koker}(X^*(\varphi|_G): X^*(G) \longrightarrow X^*(G), \chi \mapsto n \bullet \chi)$

2. Schritt. Das Bild einer kurzen exakten Sequenz

$$0 \longrightarrow M' \longrightarrow M \longrightarrow M'' \longrightarrow 0$$

von endlich erzeugten abelschen Gruppen ohen p-Torsion (p = Char(k)) ist beim Funktor

$$\mathcal{G}: \mathrm{Ab}' \longrightarrow \mathrm{Diag}, M \mapsto \mathcal{G}(M),$$

(vgl. 3.2.6) ist eine exakte Sequenz

$$1 \longrightarrow \mathcal{G}(M'') \longrightarrow \mathcal{G}(M) \longrightarrow \mathcal{G}(M') \longrightarrow 1.$$

Dieses fügt sich in ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Hom}(M'',k^*) & \longrightarrow & \mathrm{Hom}(M,k^*) & \longrightarrow & \mathrm{Hom}(M',k^*) & \longrightarrow & 1 \\ & & \cong\uparrow & & \uparrow\cong & & \uparrow\cong & & \\ 1 & \longrightarrow & \mathcal{G}(M'') & \longrightarrow & \mathcal{G}(M) & \longrightarrow & \mathcal{G}(M') & \longrightarrow & < \end{array}$$

von Gruppen-Homomorphismen ein, dessen vertikale Pfeile Isomorphismen bezeichnen und dessen untere Zeile aus Homomorphismen linearer algebraischer Gruppen besteht.

Wir wenden den kontravarianten Hom-Funktor $\mathrm{Hom}_{\mathbf{Ab}}(?,k^*)$ auf die gegebene exakte Sequenz an und erhalten, weil der Hom-Funtor linksexakt ist eine exakte Sequenz

$$1 \longrightarrow \mathrm{Hom}(M'', k^*) \longrightarrow \mathrm{Hom}(M, k^*) \longrightarrow \mathrm{Hom}(M', k^*)$$

Auf Grund von 3.2.10 Aufgabe 3 und dem funktoriellen Morphismus von 3.2.6 (ii) fügt sich diese exakte Sequenz in ein kommutatives Diagramm

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Hom}(M'',k^*) & \longrightarrow & \mathrm{Hom}(M,k^*) & \longrightarrow & \mathrm{Hom}(M',k^*) & & \\ & & \cong\uparrow & & \uparrow\cong & & \uparrow\cong & & \\ 1 & \longrightarrow & \mathcal{G}(M'') & \longrightarrow & \mathcal{G}(M) & \longrightarrow & \mathcal{G}(M') & & \end{array}$$

mit exakten Zeilen ein, des vertikale Abbildungen Isomorphismen abelscher Gruppen sind und desssen untere Zeile aus Homomorphismen linearer algebraischer Gruppen besteht. Wegern der Injektivität des Homomorphismus $M' \longrightarrow M$ ist auch die Induzierte Abbildung der Gruppen-Algebren $k[M'] \longrightarrow k[M]$ injektiv, und damit auch der k-Algebra-Homomorphismus der Koordinatenringe

$$k[\mathcal{G}(M')] \longrightarrow k[\mathcal{G}(M)]$$

(vgl. 3.2.6(i9).Deshalb liegt das Bild der regulären Abbildung $\mathcal{G}(M) \longrightarrow \mathcal{G}(M')$ dicht in $\mathcal{G}(M')$. Nach 2.2.5 (ii) ist dieses Bild aber eine abgeschlossene Untergruppe von $\mathcal{G}(M')$. Die untere rechte Abbildung des Diagramm ist somit surjektiv. Wir erhalten ein kommutatives Diagramm mit mit exakten Zeilen

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Hom}(M'',k^*) & \longrightarrow & \mathrm{Hom}(M,k^*) & \longrightarrow & \mathrm{Hom}(M',k^*) & \longrightarrow & 1 \\ & & \cong\uparrow & & \uparrow\cong & & \uparrow\cong & & \\ 1 & \longrightarrow & \mathcal{G}(M'') & \longrightarrow & \mathcal{G}(M) & \longrightarrow & \mathcal{G}(M') & \longrightarrow & 1 \end{array}$$

3. Schritt. Berechnung von $G_n^{\perp}$.

Wir betrachten die exakte Sequenz von endlich erzeugten abelschen Gruppen ohne p-Torsion

$$X \xrightarrow{n} X \longrightarrow X/nX \longrightarrow 0. \qquad (1)$$

Dabei sei $X = \mathbf{X}^*(G)$ und die linke Abbildung bezeichne die Multiplikation mit n. Wir wenden den Funktor $\mathcal{G}$ an und erhalten eine Sequenz

$$1 \longrightarrow \mathcal{G}(X/nX) \longrightarrow \mathcal{G}(X) \xrightarrow{\mathcal{G}(n)} \mathcal{G}(X).$$

Weil $\mathcal{G}$ eine Anti-Äquivalenz von Kategorien ist und $X/nX = \mathrm{Koker}(X \xrightarrow{n} X)$ gilt, folgt

$$\mathcal{G}(X/nX) = \mathrm{Ker}(\mathcal{G}(X) \xrightarrow{\mathcal{G}(n)} \mathcal{G}(X))$$

(vgl. die Bemerkungen am Anfang des vierten Schritts im Beweis zu 3.2.10 Aufgabe 4 (i)). Nach 3.2.10 Aufgabe 3 kommt die Abbildung $\mathcal{G}(n)$ auch im folgenden kommutativen Diagramm vor.[11]

$$\begin{array}{ccc} \mathrm{Hom}(X,k^*) & \xrightarrow{n} & \mathrm{Hom}(X,k^*) \\ \cong\uparrow & & \uparrow\cong \\ \mathcal{G}(X) & \xrightarrow{\mathcal{G}(n)} & \mathcal{G}(X) \\ \| & & \| \\ G & & G \end{array}$$

Dabei wird die obere horizontale Abbildung induziert durch die Multiplikation $X \xrightarrow{n} X$ mit n. Nach dem ersten Schritt wird letztere induziert durch die Abbildung

$$\varphi: G \longrightarrow G,\ x \mapsto x^n.$$

Das Viereck bleibt also kommutativ, wenn wir $\mathcal{G}(n)$ durch φ ersetzt. Weil die vertikalen Abbildungen bijektiv sind, ist die untere Abbildung durch die obere und die Kommutativität des Diagramm eindeutig festgelegt. Also ist

$$\mathcal{G}(n) = \varphi: G \longrightarrow G,\ x \mapsto x^n.$$

Damit gilt

$$\mathcal{G}(X/nX) = \mathrm{Ker}(G \xrightarrow{\mathcal{G}(n)} G,\ x \mapsto x^n) = G_n\ .$$

Das Diagramm des zweiten Schritts zur gegebenen exakten Sequenz (1) hat damit die Gestalt

[11] Wegen $X = X^*(G)$ können wir $\mathcal{G}(X)$ mit G identifizieren.

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Hom}(X/nX,k^*) & \longrightarrow & \mathrm{Hom}(X,k^*) & \longrightarrow & \mathrm{Hom}(nX,k^*) & \longrightarrow & 1 \\ & & \cong\uparrow & & \uparrow\cong & & \uparrow\cong & & \\ 1 & \longrightarrow & \mathcal{G}(X/nX) & \longrightarrow & \mathcal{G}(X) & \longrightarrow & \mathcal{G}(nX) & \longrightarrow & 1 \\ & & \| & & \| & & & & \\ & & G_n & & G & & & & \end{array}$$

Wegen der Exaktheit der Zeilen gilt

$$\mathcal{G}(nX) = \mathrm{Koker}(G_n \hookrightarrow G). \qquad (2)$$

Wir wenden den Funktor $\mathbf{X}^*$ an und erhalten

$nX = \mathbf{X}^*(\mathcal{G}(nX))$ (nach 3.2.6 (ii))

$= \mathbf{X}^*(\mathrm{Koker}(G_n \hookrightarrow G))$ (nach (2))

$= \mathrm{Ker}(\mathbf{X}^*(G) \longrightarrow \mathbf{X}^*(G_n), \chi \mapsto \chi|_{G_n})$ (X^* ist Anti-Äquivalenz von Kategorien)[12]

$= \{\chi \in X^*(G) \mid \chi(x) = 1 \text{ für } x \in G_n\}$

$= G_n^{\perp}$ (nach Definition, vlg. 3.2.10 Aufgabe 4)

d.h. es gilt $G_n^{\perp} = n\bullet X$ wie behauptet.

Zu (ii). Sei H die von den Torsionspunkten von G erzeugte Gruppe und $\overline{H}$ deren Abschließung in G. Wir haben zu zeigen,

$$\overline{H} = G.$$

Als abgeschlossene Untergruppe der diagonalisierbaren linearen algebraischen Gruppe G ist $\overline{H}$ eine diagonalisierbare lineare algebraische Gruppe. Nach dem sechsten Schritt im Beweis von 3.2.10 Aufgabe 3 ist $\overline{H}$ der Durchschnitt der Kerne von endlich vielen Charakteren von G,

$$\overline{H} = V(\chi_1 - 1, \ldots, \chi_r - 1) \text{ mit } \chi_1, \ldots, \chi_r \in X^*(G).$$

Zum Beweis der Behauptung reicht es zu zeigen, nur der triviale Charakter ist identisch 1 auf $\overline{H}$, d.h. es besteht die Implikation

$$\chi \in X^*(G) \text{ und } \chi(\overline{H}) = \{1\} \Rightarrow \chi = 0.$$

Zu zeigen ist

$$\overline{H}^{\perp} = \{0\}.$$

Wegen $G_n \subseteq \overline{H}$ für jede zu p teilerfremde natürliche Zahl, gilt $\overline{H}^{\perp} \subseteq G_n^{\perp}$. Nach (i) folgt

$$\overline{H}^{\perp} \subseteq n\bullet X \text{ für jedes natürliche n mit } (n,p) = 1.$$

Deshalb reicht es zu zeigen

$$\bigcap_{(n,p)=1} n\bullet X = 0.$$

Als endlich erzeugte abelsche Gruppe ohne p-Torsion hat X die Gestalt

$$X = \mathbb{Z}^r \oplus M$$

mit einer endlichen abelschen Gruppe M, deren Ordnung zu p Teilerfremd ist. Wegen

$$\bigcap_{(n,p)=1} n\bullet X = \left(\bigcap_{(n,p)=1} n\bullet\mathbb{Z}\right)^r \oplus \left(\bigcap_{(n,p)=1} n\bullet M\right)$$

reicht es zu zeigen,

---

[12] vgl. die Bemerkungen am Anfang des vierten Schritts im Beweis zu 3.2.10 Aufgabe 4 (i).

1. $\bigcap_{(n,p)=1} n\bullet\mathbb{Z} = 0.$

2. $\bigcap_{(n,p)=1} n\bullet M = 0.$

Zu 1. Der Durchschnitt besteht aus ganzen Zahlen, die durch jede von p verschiedene Primzahl teilbar sind. Die einzige solche ganze Zahl ist die Null.
Zu 2. Sei g die ordnung von M. Weil nach Voraussetzung zu p teilerfremd ist, gilt

$$\bigcap_{(n,p)=1} n\bullet M \subseteq g\bullet M = 0.$$

QED.

3.2.10 Aufgabe 6

Die Gruppe der Automorphismen eines n-dimensionalen Torus ist isomorph zur Gruppe $GL_n(\mathbb{Z})$ der n×n-Matrizen mit Einträgen aus $\mathbb{Z}$, deren Inverses ebenfalls Einträge aus $\mathbb{Z}$ besitzt.

Beweis. 1. Schritt. Sei G eine diagonlisierbare Gruppe. Der Übergang zu den Charaktergruppen definiert einen Anti-Isomorphimus

$$\mathbf{X}^*: \mathrm{Hom}(G, G) \longrightarrow \mathrm{Hom}(\mathbf{X}^*(G), \mathbf{X}^*(G)),\ f \mapsto f^* = X^*(f),$$

von Ringen mit Eins.
Hom (G, G) ist ein kommutativer Ring mit 1, dessen Addition gerade die Addition von Abbildungen mit Werten in G ist (d.h. die Addition kommt von der Operation der Bildmenge), und dessen Multiplikation die Zusammensetzung von Abbildungen ist:

$$(f+g)(x) = f(x)+g(x) \text{ für } f,g \in \mathrm{Hom}(G,G) \text{ und } x \in G.$$

$$(f\bullet g)(x) = f(g(x)) \quad \text{für } f,g \in \mathrm{Hom}(G,G) \text{ und } x \in G.$$

In analoger Weise ist die Ringstruktur von Hom($\mathbf{X}^*(G)$, $\mathbf{X}^*(G)$) definiert. Die Abbildung ist ein Anti-Homomorphismus von Ringen mit Eins, weil X* ein additiver Funktor ist. Es ist Anti-Isomorphismus, weil X* eine Anti-Äquivalenz von Kategorien ist.
2. Schritt. In der Situation des ersten Schritts besteht ein Anti-Isomorphismus

$$\mathrm{Aut}(T) \overset{\cong}{\longrightarrow} \mathrm{Aut}(\mathbf{X}^*(T)).$$

Der Anti-Isomorphismus des ersten Schritt induziert einen Anti-Isomorphismus der Einheitengruppen der beteiligten Ringe. Diese Einheitengruppen sind gerade

$$\mathrm{Hom}(G,G)^* = \mathrm{Aut}(G) \text{ bzw. } \mathrm{Hom}(\mathbf{X}^*(G), \mathbf{X}^*(G)) = \mathrm{Aut}\ \mathbf{X}^*(G).$$

3. Schritt. Ist G = T ein n-dimensionaler Torus, so gilt $\mathrm{Aut}(T) \cong GL_n(\mathbb{Z})$.
Die Charaktergruppe eines n-dimensionalen Torus T ist isomorph zu

$$X^*(T) \cong \mathbb{Z}^n.$$

Nach dem zweiten Schritt gilt damit

$$\mathrm{Aut}(T) \cong \mathrm{Aut}(\mathbb{Z}^n).$$

Die $\mathbb{Z}$-linearen Automorphismen von $\mathbb{Z}^n$ lassen sind in derselben Weise durch Matrizen beschreiben, wie die k-linearen Automorphismen des k-Vektorraums k^n. Damit ist

$$\mathrm{Aut}(T) \cong GL_n(\mathbb{Z}),$$

wenn rechts die umkehrbaren n×n-Matrizen mit Einträgen aus $\mathbb{Z}$ stehen, deren Umkehrungen ebenfalls Einträge aus $\mathbb{Z}$ besitzen.
QED.

3.2.11 Die Paarung $\mathbf{X}^*(T) \times \mathbf{X}_*(T) \longrightarrow \mathbb{Z}$

3.2.11 A Bezeichnungen und Definitionen

Wir schließen diesen Abschnitt ab mit Material zur Theorie der Tori. Bezeichne

$$T$$

einen Torus. Wir setzen

$$X := \mathbf{X}^*(T) \text{ und } Y := \mathbf{X}_*(T)$$

(vgl. 3.2.1). Für $\chi \in X$, $\lambda \in Y$, $a \in k^*$ ist die Abbildung

$$\mathbf{G}_m \longrightarrow k^*,\ a \mapsto \chi(\lambda(a)),$$

ein Charakter der multiplikativen Gruppe $\mathbf{G}_m$. Nach 3.2.2 (mit n = 1) hat jeder Charakter von $\mathbf{G}_m$ die Gestalt

$$\mathbf{G}_m \longrightarrow \mathbf{G}_m,\ t \mapsto t^s,$$

mit einer ganzen Zahl s. Im Fall des Charakters $\chi \circ \lambda$ wollen wir diese Zahl mit $<\chi, \lambda>$ bezeichnen, d.h. $<\chi, \lambda>$ sei die eindeutig bestimmte ganze Zahl mit

$$\chi(\lambda(t)) = t^{<\chi,\lambda>}$$

für jedes $t \in k^*$.

Bemerkung

Auf Grund der Definition[13] der Addition von Charakteren und Kocharakteren gilt

$$(\chi' + \chi'') \circ \lambda = (\chi' \circ \lambda) + (\chi'' \circ \lambda)$$

und

$$\chi \circ (\lambda' + \lambda'') = (\chi \circ \lambda') + (\chi \circ \lambda'')$$

für $\chi, \chi', \chi'' \in X^*(T)$ und $\lambda, \lambda', \lambda'' \in X_*(T)$. Die Abbildung

$$< , >: X \times Y \longrightarrow \mathbb{Z},\ (\chi, \lambda) \mapsto <\chi , \lambda >,$$

ist deshalb bilinear über $\mathbb{Z}$.

3.2.11 B F-Tori und zerfallende F-Tori

Sei F ein Teilkörper von k. Ein F-Torus ist eine F-Gruppe, die ein Torus ist. Ein zerfallender F-Torus T ist ein F-Torus, der F-isomorph ist zu einem $\mathbf{D}_n$.

Bemerkung

Die Untersuchung der nicht zerfallenden F-Tori, welche Galois-Theorie erfordert, wird auf Kapitel 13 verschoben.

3.2.11 C Lemma

Sei T ein Torus. Wir setzen

$$X := \mathbf{X}^*(T) \text{ und } Y := \mathbf{X}_*(T).$$

Dann gelten die folgenden Aussagen.

(i) Durch

$$< , >: X \times Y \longrightarrow \mathbb{Z},\ (\chi, \lambda) \mapsto <\chi, \lambda>$$

eine perfekte Paarung definiert, d.h.

- jeder Homomorphismus $X \longrightarrow \mathbb{Z}$ ist von der Gestalt $\chi \mapsto <\chi, \lambda>$ für genau ein $\lambda \in Y$.

---

[13] Die Addition der (Ko-)Charaktere stimmt mit der Multiplikation der regulären Abbildungen überein.

- jeder Homomorphismus $Y \longrightarrow \mathbb{Z}$ ist von der Gestalt $\lambda \mapsto <\chi, \lambda>$ für genau ein $\chi \in X$.

Insbesondere ist Y eine freie abelsche Gruppe vom selben Rang wie X.

(ii) Die Abbildung

$$k^* \otimes Y \longrightarrow T,\ a \otimes \lambda \mapsto \lambda(a),$$

ist wohldefiniert und ein Isomorphismus von abelschen Gruppen.

Beweis. Zu (i). Zum Beweis können wir annehmen, der Torus T ist gleich

$$T = \mathbf{D}_n$$

Wir setzen die Isomorphismen von Beispiel 3.2.2 zur folgenden Abbildung zusammen.

$$\varphi: \mathbb{Z}^n \times \mathbb{Z}^n \quad \overset{\cong}{\longrightarrow} \quad X^*(G) \times X_*(G) \quad \longrightarrow \quad \text{Aut } k^*$$

$$((a_1,...,a_n), (b_1,...,b_n)) \mapsto (\chi := \chi_1^{a_1} \bullet ... \bullet \chi_n^{a_n},\ \lambda := (t \mapsto \text{diag}(t^{b_1}, ..., t^{b_n})) \mapsto \chi \circ \lambda.$$

Dabei bezeichne χ_i: $T \longrightarrow k^*$ den Charakter von T, welcher jede Matrix auf den i-ten Eintrag der Hauptdiagonalen abbildet. Es gilt also

$$\begin{aligned} \varphi((a_1,...,a_n), (b_1,...,b_n))(t) &= \chi_1(\text{diag}(t^{b_1}, ..., t^{b_1}))^{a_1} \bullet ... \bullet \chi_n(\text{diag}(t^{b_1}, ..., t^{b_n}))^{a_n} \\ &= (t^{b_1})^{a_1} \bullet ... \bullet (t^{b_n})^{a_n} \\ &= t^{a_1 b_1 + ... + a_n b_n}. \end{aligned}$$

Wenn wir $X^*(G)$ und $X_*(G)$ mit Hilfe der Isomorphismen von 3.2.2 mit $\mathbb{Z}^n$ identifizieren, so bekommt die Abbildung $<\ ,\ >$ die Gestalt

$$<,>: \mathbb{Z}^n \times \mathbb{Z}^n \longrightarrow \mathbb{Z},\ ((a_1,...,a_n), (b_1,...,b_n)) \mapsto a_1 b_1 + ... + a_n b_n.$$

Dies ist aber gerade eine in oben beschriebenen Sinne perfekte Paarung, denn jede $\mathbb{Z}$-lineare Abbildung

$$\mathbb{Z}^n \longrightarrow \mathbb{Z}$$

ist durch ihre Werte in den Standard-Einheitsvektoren e_i eindeutig festgelegt, wobei es zu beliebig vorgegebenen ganzzahligen Werten in den e_i genau eine solche $\mathbb{Z}$-lineare Abbildung gibt.

Zu (ii). Wir können ebenfalls annehmen, daß der Torus T gleich

$$T = \mathbf{D}_n$$

ist. Die Abbildiung von (ii) hat dann die Gestalt

$$k^* \otimes \mathbb{Z}^n \longrightarrow \mathbf{D}_n,\ c \otimes (b_1,...,b_n) \mapsto \text{diag}(c^{b_1}, ..., c^{b_n}). \qquad (1)$$

Das Tensorprodukt links ist isomorph zu einer direkten Summe von n Exemplaren von $k^* \otimes \mathbb{Z} = k^* \otimes_{\mathbb{Z}} \mathbb{Z} = k^*$. Genauer, die Abbildung

$$k^* \otimes \mathbb{Z}^n \longrightarrow (k^*)^n,\ c \otimes (b_1,...,b_n) \mapsto (c^{b_1}, ..., c^{b_n}),$$

ist ein Gruppen-Isomorphismus mit der Inversen

$$(k^*)^n \longrightarrow k^* \otimes \mathbb{Z}^n,\ (c_1,...,c_n) \mapsto c_1 \otimes e_1 + ... + c_n \otimes e_n.$$

Wir setzen (1) mit dieser Inversen zusammen und erhalten die Abbildung

$$(c_1,...,c_n) \mapsto c_1 \otimes e_1 + ... + c_n \otimes e_n \mapsto \prod_{i=1}^{n} \text{diag}\ (1,...,c_i,...,1) = \text{diag}(c_1, ..., c_n).$$

Dies ist ein Gruppen-Isomorphismus. Also ist auch (1) ein solcher.
QED.

3.2.12 Proposition

Sei F ein Teilkörper des algebraisch abgeschlossenen Körpers k.

(i) Ein F-Torus T zerfällt genau dann über F, wenn alle seine Charaktere über F definiert sind. Ist dies der Fall, so bilden die Charaktere eine F-Vektorraumbasis von F[T].

(ii) Jede über F definerte rationale Darstellung eines über F zerfallenden Torus T ist eine direkte Summe von eindimensionalen über F definierten Darstellungen.

Beweis. Zu (i). 1. Schritt. Die Charaktere eines über F zerfallenden Torus sind über F definiert.

Die F-Struktur von $\mathbf{D}_n$ ist gegeben durch die Teilalgebra

$$F[\mathbf{D}_n] = F[T_{11},...,T_{nn}, T_{11}^{-1}, ..., T_{nn}^{-1}]$$

von

$$k[\mathbf{D}_n] = k[T_{11},...,T_{nn}, T_{11}^{-1}, ..., T_{nn}^{-1}].$$

Die Charaktere von $\mathbf{D}_n$ sind gerade die Potenzprodukte

$$T_{11}^{a_1} \bullet ... \bullet T_{nn}^{a_n}: \mathbf{D}_n \longrightarrow \mathbf{G}_m \text{ mit } a_1,...,a_n \in \mathbb{Z}.$$

der T_{ii} mit ganzzahligen Exponenten. Weil T_{ii}^* gerade der k-Algebra-Homomorphismus

$$T_{ii}^*: k[T,T^{-1}] = k[\mathbf{G}_m] \longrightarrow k[\mathbf{D}_n] = k[T_{11},...,T_{nn}, T_{11}^{-1}, ..., T_{nn}^{-1}],$$

$$T \mapsto T_{ii},$$

ist, also $F[\mathbf{G}_m]$ in $F[\mathbf{D}_n]$ abbildet, ist der Charakter T_{ii} für jedes i über F definiert.

Wir sehen so, die Charaktere des F-Torus $\mathbf{D}_n$ sind über F definiert und sie bilden eine F-Vektorraumbasis von $F[\mathbf{D}_n]$.

Ist T ein zerfallender F-Torus, so gibt es einen über F definierten Isomorphismus

$$\varphi: T \longrightarrow \mathbf{D}_n.$$

Für jeden Charakter χ von $\mathbf{D}_n$ ist $\chi \circ \varphi$ ein über F definierter Charakter von T, und man erhält so alle Charaktere von T.

Außerdem induziert der F-Isomorphismus φ einen über F definierten Isomorphismus

$$\varphi^*: k[\mathbf{D}_n] \longrightarrow k[T],$$

also einen Isomorphismus von F-Algebren

$$\varphi^*|_{F[\mathbf{D}_n]}: F[\mathbf{D}_n] \longrightarrow F[T].$$

Letzterer überführt die F-Vektorraumbasis der Charaktere von $\mathbf{D}_n$ in die F-Vektorraumbasis der Charaktere von T.

2. Schritt. Ein F-Torus T, dessen Charaktere über F definiert sind, zerfällt über F.

Weil T ein Torus ist, gibt es einen Isomorphismus linearer algebraischer Gruppen

$$\varphi: T \longrightarrow \mathbf{D}_n \quad t \mapsto \varphi(t) = \mathrm{diag}(\varphi_1(t), ... , \varphi_n(t)).$$

die Koordinatenfunktionen φ_i von φ sind Charaktere von T, also nach Vorausetzung über F definiert. Deshalb ist φ über F definiert. Die induzierte Abbildung der Koordinatenringe

$$\varphi^*: k[\mathbf{D}_n] \longrightarrow k[T]$$

bildet die F-Strukturen dieser Koordinatenringe ineinander ab,

$$\varphi^*(F[\mathbf{D}_n]) \subseteq F[T].$$

Es reicht zu zeigen, daß sogar das Gleichheitszeichen gilt, denn dann ist auch φ^{-1} über F definiert, also ein F-Isomorphismus, d.h. T zerfüllt über F.

Weil φ ein Isomorphismus ist, ist auch φ^* ein solcher, also insbesondere injektiv. Wir erhalten eine exakte Sequenhz von F-Vektorräumen

$$0 \longrightarrow F[\mathbf{D}_n] \overset{\varphi^*|_{k[\mathbf{D}_n]}}{\longrightarrow} F[T] \longrightarrow F[T]/\varphi^*(F[\mathbf{D}_n]) \longrightarrow 0.$$

Wir wenden den Funktor $k\otimes_F$ an und erhalten - nach Definition des Begriffs F-Struktur - die exakte Sequenz

$$0 \longrightarrow k[\mathbf{D}_n] \overset{\varphi^*}{\longrightarrow} k[T] \longrightarrow k\otimes_F(F[T]/\varphi^*(F[\mathbf{D}_n])) \longrightarrow 0.$$

Weil φ^* ein Isomorphismus ist, gilt $0 = k\otimes_F(F[T]/\varphi^*(F[\mathbf{D}_n]))$, also

$$0 = \dim_k k\otimes_F(F[T]/\varphi^*(k[\mathbf{D}_n])) = \dim_F F[T]/\varphi^*(F[\mathbf{D}_n]),$$

also $\varphi^*(F[\mathbf{D}_n]) = F[T]$. Wir haben gezeigt, φ^* induziert einen Isomorphismus der F-Strukturen, ist also ein F-Isomorphismus.

Zu (ii). Der Beweis ist eine Variante des Beweises der Implikation 3.2.3 (ii) $\Rightarrow$ (iii). Wir können annehmen, $T = \mathbf{D}_n$. Sei

$$\phi: T \longrightarrow \mathbf{GL}(V)$$

eine über F definierte rationale Darstellung von T. Wir fixieren eine F-Vektorraumbasis der F-Struktur V_F von V. Diese ist auch eine k-Vektorraumbasis von V und gestattet es, ϕ als Homomorphismus

$$\phi: \mathbf{D}_n \longrightarrow \mathbf{GL}_r$$

(mit r geeignet) zu betrachten. Weil ϕ über F definiert ist, bildet

$$\phi^*: k[\mathbf{GL}_r] \longrightarrow k[T]$$

die F-Struktur

$$F[\mathbf{GL}_r] = F[T_{ij}, \det^{-1} \mid i,j = 1,...,r]$$

von $k[\mathbf{GL}_r]$ in die F-Struktur

$$F[T] = F[T_{11},...,F_{nn}, T_{11}^{-1},...,T_{nn}^{-1}]$$

von k[T] ab. Insbesondere liegen die Bilder $\phi^*(T_{ij})$ der T_{ij} in F[T], d.h. für jedes $x \in T$ gilt

$$\phi(x) = \begin{pmatrix} \phi_{11}(x)\ \phi_{12}(x) \dots \phi_{1r}(x) \\ \phi_{21}(x)\ \phi_{22}(x) \dots \phi_{2r}(x) \\ \dots \quad \dots \quad \dots \quad \dots \\ \phi_{r1}(x)\ \phi_{r2}(x) \dots \phi_{rr}(x) \end{pmatrix} = \sum_{i,j=1}^{n} \phi_{ij}(x) \bullet E_{ij}$$

mit regulären Funktion $\phi_{ij} \in F[T]$. Jede dieser regulären Funktion ist nach (i) eine F-Linearkombination von Charakteren von T. Deshalb läßt sich ϕ als Linearkombination von r×r-Matrizen mit Einträgen aus F schreiben, deren Koeffizienten Charaktere von T sind, sagen wir

$$\phi(x) = \sum_{\chi \in \mathbf{X}^*(G)} \chi(x) \bullet A_\chi \tag{1}$$

mit $A_\chi \in M_r(F)$ oder in einer von der Wahl der Basis von V unabhängigen Schreibweise,

$$A_\chi \in \mathrm{End}_k(V) \text{ mit } A_\chi(V_F) \subseteq V_F \tag{2}$$

Dabei sind nur endlich viele der A_χ von Null verschieden,

$$A_\chi = 0 \text{ für fast alle } \chi \in \mathbf{X}^*(G).$$

Weil ϕ ein Gruppen-Homomorphismus ist, gilt für $x,y \in G$

$$\begin{aligned} \sum_{\chi \in \mathbf{X}^*(G)} \chi(x)\chi(y) \bullet A_\chi &= \sum_{\chi \in \mathbf{X}^*(G)} \chi(xy) \bullet A_\chi \\ &= \phi(xy) \\ &= \phi(x) \bullet \phi(y) \\ &= \sum_{\chi,\psi \in \mathbf{X}^*(G)} \chi(x) \bullet \psi(y) \bullet A_\chi \bullet A_\psi . \end{aligned}$$

Dies ist eine Relation von Charakteren auf G×G. Weil die Charaktere von G×G linear unabhängig über k sind, folgt durch Koeffizientenvergleich[14]

$$A_\chi \bullet A_\psi = \delta_{\chi,\psi} \bullet A_\chi \tag{3}$$

(wenn $\delta_{\chi,\psi}$ das Kronecker-Symbol bezeichnet).Weil $\phi(e)$ die identische Abbildung von V ist, folgt

$$\sum_{\chi \in \mathbf{X}^*(G)} A_\chi = \mathrm{Id}. \tag{4}$$

Wir setzen

$$V_\chi := A_\chi(V).$$

Wegen (4) gilt dann

---

[14] Man beachte, für Charaktere α, β, γ und δ gilt nur dann $\alpha(x)\beta(y) = \gamma(x) \bullet \delta(y)$ für alle $x, y \in G$, wenn $\alpha=\gamma$ und $\beta = \delta$ ist (man setze $y = e$ bzw. $x = e$).

$$\sum_{\chi\in\mathbf{X}^*(G)} V_\chi = V.$$

Nach (3) ist A_χ auf V_ψ die identische Abbildung für $\chi=\psi$ und 0 sonst. Deshalb ist die gefundene Summenzerlegung von V direkt,

$$\bigoplus_{\chi\in\mathbf{X}^*(G)} V_\chi = V.$$

Nach Definition der A_χ sind die Räume V_χ stabil bezüglich der Operation von T auf V mit Hilfe von ϕ. Da die Anzahl der von Null verschiedenen A_χ endlich ist, gilt dasselbe für die Räume V_χ, d.h. wir können schreiben

$$V = V_{\chi_1} \oplus \ldots \oplus V_{\chi_t}$$

Zusammen mit (1) erhalten wir so für die Matrix von $\phi(x)$ bezüglich einer mit dieser Zerlegung verträglichen Basis

$$\phi(x) = \begin{pmatrix} \chi_1(x)\bullet Id_{V_{\chi_1}} & 0 & \ldots & 0 \\ 0 & \chi_2(x)\bullet Id_{V_{\chi_2}} & \ldots & 0 \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & \chi_t(x)\bullet Id_{V_{\chi_t}} \end{pmatrix}$$

Mit anderen Worten, ϕ ist direkte Summe der 1-dimensionalen Darstellungen χ_i (wobei die Dimensionen der Räume V_{χ_i} die Vielfachheiten sind mit denen die χ_i vorkommen).

Als Charaktere von $T = \mathbf{D}_n$ sind die χ_i über F definiert.

QED.

3.2.13 Limites, die Graduierung von $k[D_n]$ und die Mengen $V(\pm\lambda)$

Wir betrachten hier die multiplikative Gruppe

$$\mathbf{G}_m = k^* \hookrightarrow k = \mathbb{A}^1$$

als offene Teilmenge der affinen Geraden, d.h. als affine Gerade ohne den Urprung, und die affine Gerade

$$\mathbb{A}^1 \hookrightarrow \mathbb{P}^1,\ x \mapsto [1,x],$$

als offene Teilmenge der projektiven Geraden, d.h. als projektive Gerade ohne den unendlich fernen Punkt. Außerdem beachten wir, daß der Automorphismus

$$\mathbf{G}_m \xrightarrow{\cong} \mathbf{G}_m,\ t \mapsto \frac{1}{t},$$

der multiplikativen Gruppe sich zu einem Automorphismus der projektiven Geraden

$$\mathbb{P}^1 \longrightarrow \mathbb{P}^1,\ [x,y] \mapsto [y,x],$$

fortsetzen läßt welcher Ursprung und unendlich fernen Punkt vertauscht. Dies motiviert die nachfolgenden Bezeichnungen $\lim_{a\to 0}$ und $\lim_{a\to\infty}$.

(i) Für jede reguläre Abbildung

$$\phi: \mathbf{G}_m \longrightarrow Z$$

mit Werten in einer algebraischen Varietät Z, welche sich zu einer regulären Abbildung

$$\overline{\phi}: \mathbb{A}^1 \longrightarrow Z,$$

fortsetzen läßt, schreiben wir

$$\lim_{a\to 0} \phi(a) = \overline{\phi}(0).$$

Wenn sich ϕ': $\mathbf{G}_m \longrightarrow Z$, $t \mapsto \phi(1/t)$, zu einer regulären Abbildung $\overline{\phi}'$:$\mathbb{A}^1 \longrightarrow Z$, forsetzen läßt, schreiben wir

$$\lim_{a\to\infty} \phi(a) = \overline{\phi}'(0).$$

(ii) Seien

$$T$$

ein Torus, V eine affine Varietät,

$$a: T \times V \longrightarrow V$$

eine Operation von T auf V (d.h. V sei ein affiner T-Raum). Wie in 2.3.5 bezeichnen wir mit

$$s: T \longrightarrow \mathbf{GL}(k[V]),\ t \mapsto s(t),$$

die zugehörige lokal endliche Operation von G auf dem Koordinatenring k[V] (vgl. 2.3.6 A), d.h.

$$(s(t)f)(x) = f(a(t^{-1},x))$$

für $t \in T$, $f \in k[V]$ und $x \in V$. Wie bisher setzen wir

$$X := \mathbf{X}^*(T) \text{ und } Y := \mathbf{X}_*(T)$$

(vgl. 3.2.1). Für $\chi \in X$ sei

$$k[V]_\chi := \{f \in k[V] \mid s(t)f = \chi(t)\bullet f \text{ für jedes } t \in T\}$$

der Eigenraum der Operation s bezüglich des Charakters χ. Nach 3.2.3 besteht eine direkte Summenzerlegung[15]

$$k[V] = \oplus_{\chi\in X} k[V]_\chi$$

Nach Definiton der Eigenräume gilt

---

[15] Jedes $f \in k[V]$ liegt in einem endlich-dimensionalen T-stabilen Unterraum $W \subseteq k[V]$. Die zugehörige rationale Darstellung $T \longrightarrow \mathbf{GL}(W)$ zerfällt in eine direkte Summe 1-dimensionale Darstellungen (nach 3.2.3), d.h. es gilt

$$f \in W = \sum_{\chi\in X} W\bigcap k[T]_\chi \subseteq \sum_{\chi\in X} k[V]_\chi \subseteq k[V]$$

also

$$k[V] \subseteq \sum_{\chi\in X} k[V]_\chi \subseteq k[V].$$

Wegen der linearen Unabhängigkeit der Charaktere ist die Summenzerlegung direkt.

$$k[V]_\chi \cdot k[V]_\psi = k[V]_{\chi+\psi} \text{ für } \chi, \psi \in X.$$

Der Koordinatenring k[V] besitzt eine X-Graduierung. Im Fall $T = \mathbf{D}_n$ ist $X = \mathbb{Z}^n$ und wir erhalten eine graduierte k-Algebra im üblichen Sinne.

(iii) Für jedes $\lambda \in Y$ definieren wir

$$V(\lambda) := \{v \in V \mid \lim_{a \to 0} \lambda(a) \cdot v \text{ existiert } \}$$

$$V(-\lambda) := \{v \in V \mid \lim_{a \to \infty} \lambda(a) \cdot v \text{ existiert } \}$$

Man beachte, nur eine der beiden Relationen ist eine Definition und jede von ihnen eine Folge der anderen. Zum Beispiel gilt wegen $(-\lambda)(a) = \frac{1}{\lambda(a)}$ auf Grund der ersten Definition

$$\begin{aligned} V(-\lambda) &= \{v \in V \mid \lim_{a \to 0} (-\lambda)(a) \cdot v \text{ existiert } \} \\ &= \{v \in V \mid \lim_{a \to 0} \lambda(a)^{-1} \cdot v \text{ existiert } \} \\ &= \{v \in V \mid \lim_{a \to 0} \lambda(a^{-1}) \cdot v \text{ existiert } \} \ (\lambda \text{ ist ein Gruppen-Homomorphismus}) \\ &= \{v \in V \mid \lim_{a \to \infty} \lambda(a) \cdot v \text{ existiert } \} \end{aligned}$$

3.2.14 Die Mengen V(λ)

Seien V eine affine Varietät, T ein Torus und

$$a: T \times V \longrightarrow V$$

eine Operation von T auf V (d.h. V sei ein T-Raum). Für jedes $\lambda \in X_*(T)$ gilt dann mit den Bezeichnungen von 3.2.13:

(i) $V(\lambda)$ ist ein abgeschlossener Unterraum von V.

(ii) $V(\lambda) \bigcap V(-\lambda) = \{v \in V \mid \lambda(c) \cdot v = v \text{ für jedes } c \in k^*\}$
ist die Menge der Fixpunkte von $\mathrm{Im}(\lambda)$.

Beweis. Zu (i). Sei $v \in V$. Dann gilt

$$\begin{aligned} v \in V(\lambda) &\Leftrightarrow \lim_{t \to 0} \lambda(t) \cdot v \text{ existiert} \qquad \text{(vgl. 3.2.13 (iii))} \\ &\Leftrightarrow \mathbf{G}_m \longrightarrow V,\ t \mapsto \lambda(t) \cdot v, \text{ läßt sich auf } \mathbb{A}^1 \text{ fortsetzen}[16] \\ &\Leftrightarrow k[V] \longrightarrow k[\mathbf{G}_m],\ f \mapsto (c \mapsto f(\lambda(c) \cdot v)), \\ &\qquad \text{faktorisiert}[17] \text{ sich über } k[\mathbb{A}^1] = k[x] \hookrightarrow k[x, x^{-1}] = k[\mathbf{G}_m] \end{aligned}$$

---

[16] d.h. die Abbildung ist Teil eines kommutativen Diagramms $\begin{array}{ccc} & & G_m \\ & \nearrow & \downarrow \\ \mathbb{A}^1 & & \longrightarrow V \end{array}$ von regulären Abbildungen.

Dabei ist $\lambda(c)\bullet v$ das Bild von v bei der Operation a von $\lambda(c) \in T$ auf V. Für die zu a gehörige lokal endliche Operation s: $T \longrightarrow \mathbf{GL}(k[V])$ der abstrakten Gruppe T auf k[V] gilt (vgl. 2.3.6 A)

$$(s(t)f)(v) = f(a(t^{-1}, v)) = f(t^{-1}v),$$

also

$$f(\lambda(c)\bullet v) = (s(\lambda(c)^{-1})f)(v) = (s(\lambda(c^{-1}))f)(v). \qquad (1)$$

Wir können also die Bedingung $v \in V(\lambda)$ mit Hilfe von s wie folgt ausdrücken.

$$v \in V(\lambda) \quad \Leftrightarrow k[V] \longrightarrow k[\mathbf{G}_m],\ f \mapsto (t \mapsto (s(\lambda(t^{-1}))f)(v)),$$

faktorisiert sich über $k[\mathbb{A}^1] \longrightarrow k[\mathbf{G}_m]$.

Nach 3.2.13 (ii) hat f die Gestalt

$$f = \sum_{\chi \in X^*(T)} f_\chi \text{ mit } f_\chi \in k[V]_\chi.$$

Weil $s(t) \in \mathbf{GL}(k[V])$ eine k-lineare Abbildung ist, folgt

$$s(t)f = \sum_{\chi \in X^*(T)} s(t)f_\chi$$

$$= \sum_{\chi \in X^*(T)} \chi(t)f_\chi. \qquad \text{(nach Definition von } k[V]_\chi)$$

Wir setzen für $t \in T$ den Wert $\lambda(c)$ mit $c \in k^*$ ein und erhalten

$$s(\lambda(c))f = \sum_{\chi \in X^*(T)} \chi(\lambda(c))f_\chi$$

$$= \sum_{\chi \in X^*(T)} c^{<\chi,\lambda>} f_\chi \qquad \text{(nach Definition von } <\ ,\ > \text{ in 3.2.11 A)}$$

also

$$(s(\lambda(c))f)(v) = \sum_{\chi \in X^*(T)} c^{<\chi,\lambda>} f_\chi(v). \qquad (2)$$

Damit bekommt die Bedingung für $v \in V(\lambda)$ die Gestalt

$$v \in V(\lambda) \quad \Leftrightarrow k[V] \longrightarrow k[\mathbf{G}_m],\ f \mapsto (c \mapsto \sum_{\chi \in X^*(T)} c^{-<\chi,\lambda>} f_\chi(v)).$$

faktorisiert sich über $k[\mathbb{A}^1] \longrightarrow k[\mathbf{G}_m]$

Nun ist $k[\mathbb{A}^1]$ eine Polynomalgebra über k in einer Unbestimmten, sagen wir,

---

[17] d.h. die Abbildung ist Teil eines kommutativen Diagramms $\begin{array}{ccc} & & k[G_m] \leftarrow k[V] \\ & \nearrow & \uparrow \quad \swarrow \\ k & \rightarrow & k[\mathbb{A}^1] \end{array}$ von k-Algebra-Homomorphismen.

$$k[\mathbb{A}^1] = k[x]$$

und

$$k[\mathbf{G}_m] = k[x, x^{-1}].$$

Beide Algebren sind Teilalgebren des rationalen Funktionenkörpers k(x), also auch Teilringe voneinander. Die Aussage, daß sich die angegebene Abbildung über k[x] faktorisiert, bedeutet einfach, daß ihr Bild in k[x] liegt. Es folgt

$$v \in V(\lambda) \quad \Leftrightarrow \quad \sum_{\chi \in X^*(T)} x^{-<\chi,\lambda>} f_\chi(v) \in k[x] \text{ für jedes } f \in k[V]$$

$$\Leftrightarrow f_\chi(v) = 0 \text{ für jedes } f \in k[V] \text{ und jedes } \chi \in X^*(T) \text{ mit } <\chi, \lambda> > 0.$$

$$\Leftrightarrow f(v) = 0 \text{ für jedes } \chi \in X^*(T) \text{ und jedes } f \in k[V]_\chi \text{ mit } <\chi, \lambda > > 0.$$

$$\Leftrightarrow v \in V(f \in k[V]_\chi \mid \chi \in X^*(T) \text{ und } 0 < <\chi, \lambda >)$$

Wir haben gezeigt,

$$V(\lambda) = V(f \in k[V]_\chi \mid \chi \in X^*(T) \text{ und } 0 < <\chi, \lambda >). \qquad (3)$$

Insbesondere ist V(λ) eine abgeschlossene Teilmenge von V, d.h. es gilt (i).
Zu (ii). Aus der gerade bewiesenen Identität (3) erhalten wir

$$V(\lambda) \bigcap V(-\lambda) = V(f \in k[V]_\chi \mid \chi \in X^*(T) \text{ und } 0 \neq <\chi, \lambda >). \qquad (4)$$

Wir haben zu zeigen, diese Menge ist gleich

$$\{v \in V \mid \lambda(c) \bullet v = v \text{ für jedes } c \in k^*\}. \qquad (5)$$

1. Schritt. Die Menge (5) liegt ganz in $V(\lambda) \bigcap V(-\lambda)$.

Sei v ein Element der Menge (5) und $f \in k[V]_\chi$ mit $\chi \in X^*(T)$ und $0 \neq <\chi, \lambda >$. Wir haben zu zeigen f(v) = 0.

Für jedes $c \in k^*$ gilt

$$f(v) = f(\lambda(c) \bullet v) \qquad \text{(weil v in der Menge (5) liegt).}$$

Die rechte Seite ist nach (1) gleich $(s(\lambda(c^{-1}))f)(v)$ und zusammen mit (2) gleich

$$c^{-<\chi,\lambda>} f(v),$$

denn wegen $f \in k[V]_\chi$ ist höchsten ein Summand auf der rechten Seite von (2) ungleich Null. Es folgt

$$f(v) = c^{-<\chi,\lambda>} f(v) \text{ für jedes } c \in k^*,$$

also

$$0 = (1 - c^{-<\chi,\lambda>}) \bullet f(v) \text{ für jedes } c \in k^*$$

Weil nach Vorausetzung $<\chi, \lambda >$ ungleich 0 ist, hat die Gleichung $1 - c^{-<\chi,\lambda>} = 0$ nur endlich viele Lösungen $c \in k^*$. Weil k algebraische abgeschlossen, also unendich ist, kann man $c \in k^*$ so wählen, daß $1 - t^{-<\chi,\lambda>} \neq 0$ gilt. Es folgt f(v) = 0, wie behauptet.

2. Schritt. Jeder Punkt von $V(\lambda) \bigcap V(-\lambda)$ liegt in der Menge (5).

Sei $v \in V(\lambda) \bigcap V(-\lambda)$. Angenommen, v liegt nicht in der Menge (5). Dann gibt es ein $c \in k^*$ mit

$$\lambda(c) \bullet v \neq v.$$

Die Punkte $\lambda(c)\bullet v$ und v haben unterschiedliche Koordinaten (bezüglich irgendeiner Einbettung von V in einen k^n). Es gibt also ein $f \in k[V]$ mit

$$f(\lambda(c)\bullet v) \neq f(v). \qquad (6)$$

Nach 3.2.13 (ii) hat f die Gestalt

$$f = \sum_{\chi \in X^*(T)} f_\chi \text{ mit } f_\chi \in k[V]_\chi.$$

Wenn man in (6) die Funktion f durch f_χ ersetzt, so kann nicht für alle χ das Gleichheitszeichen gelten (weil es dann auf für f gelten würde). Es gibt also ein $\chi \in X^*(T)$ mit

$$f_\chi(\lambda(t)\bullet v) \neq f_\chi(v).$$

Wegen (1), (2) und $f_\chi \in k[V]_\chi$ ist das äquivalent zu

$$c^{-<\chi,\lambda>}\bullet f_\chi(v) \neq f_\chi(v),$$

also zu

$$0 \neq (1 - t^{-<\chi,\lambda>}) f_\chi(v)$$

Das bedeutet aber,

$$0 \neq 1 - t^{-<\chi,\lambda>} \text{ und } 0 \neq f_\chi(v)$$

Die erste Bedingung bedeutet $<\chi, \lambda> \neq 0$. Zusammen mit der zweiten Bedingung und mit (4) bedeutet dies, daß v nicht in $V(\lambda) \bigcap V(-\lambda)$ liegt. Das steht aber im Widerspruch zur Wahl von v. Die Annahme, daß v nicht in der Menge (5) liegt ist somit falsch. **QED**.

3.2.15 Beispiel

Seien G eine beliebige lineare algebraische Gruppe und $\lambda: \mathbf{G}_m \longrightarrow G$ ein Kocharakter von G. Wir betrachten die folgende Operation von $\mathbf{G}_m$ auf G,

$$a: \mathbf{G}_m \times G, (t, x) \mapsto t\bullet x = \lambda(t)\bullet x \bullet \lambda(t)^{-1}.$$

Weiter sei wie in 3.2.13 (iii)

$$P(\lambda) := \{x \in G \mid \lim_{t \to 0} t\bullet x \text{ existiert } \}.$$

Dann gelten die folgenden Aussagen.

(i) $P(\lambda)$ ist eine abgeschlossene Untergruppe von G.

(ii) $P(\lambda) \bigcap P(-\lambda) = Z_G(\lambda(\mathbf{G}_m))$.

Zu (i). Nach 3.2.14 (i) ist $P(\lambda)$ eine abgeschlossene Teilmenge von G. Für $x \in G$ gilt

$$x \in P(\lambda) \Leftrightarrow \mathbf{G}_m \longrightarrow G, t \mapsto \lambda(t)\bullet x \bullet \lambda(t)^{-1}, \text{ läßt sich auf } \mathbb{A}^1 = k \text{ fortsetzen}$$

Für $x = e$ ist die Abbildung rechts die konstante Abbildung $t \mapsto e$, welche trivialerweise eine Fortsetzung besitzt, d.h. es gilt

$$e \in P(\lambda).$$

Sind $x, y \in P(\lambda)$ und $f_x, f_y: \mathbb{A}^1 \longrightarrow G$ die zugehörigen Fortsetzungen auf $\mathbb{A}^1$. Dann sind die regulären Abbildungen

$$\mathbb{A}^1 \longrightarrow G,\ t \mapsto f_x(t) \bullet f_y(t) = \mu(f_x(t), f_y(t)),$$

und

$$\mathbb{A}^1 \longrightarrow G,\ t \mapsto f_x(t)^{-1} = i(f_x(t)),$$

die zu $x \bullet y$ bzw. x^{-1} gehörigen Fortsetzungen. Es bestehen also die Implikationen

$$x, y \in P(\lambda) \Rightarrow x \bullet y \in P(\lambda) \text{ und } x \in P(\lambda) \Rightarrow x^{-1} \in P(\lambda).$$

Wir haben gezeigt, $P(\lambda)$ ist eine abgeschlossene Untergruppe.
Zu (ii). Nach 3.2.14 (ii) ist

$$P(\lambda) \bigcap P(-\lambda) = \{v \in V \mid \lambda(c) \bullet v = v \bullet \lambda(c) \text{ für jedes } c \in k^*\}$$
$$= Z_G(\mathrm{Im}(\lambda))$$

der Zentralisator von $\mathrm{Im}(\lambda)$ in G (vgl. 3.2.8).

Bemerkung

Die Verwendung der Ergebnisse von 3.2.14 in der hier vorliegenden Situation erscheint zunächst problematisch, da in 3.2.14 der Kocharakter λ ein Kocharakter eines Torus sein soll. Tatsächlich ist dies auch hier der Fall: betrachtet man G als abgeschlossene Untergruppe einer $\mathbf{GL}_n$ so besteht $\lambda(\mathbf{G}_m)$ aus kommutierenden halbeinfachen Matrizen. Nach 2.4.2 A (ii) kann man durch einen inneren Automorphismus von $\mathbf{GL}_n$ dafür sorgen, daß $\lambda(\mathbf{G}_m)$ aus Diagonalmatrizen besteht. Man kann dann λ als Abbildung

$$\lambda: \mathbf{G}_m \longrightarrow \mathbf{D}_n$$

betrachten, d.h. als Kocharakter des Torus $\mathbf{D}_n$.

3.2.16 Aufgaben

3.2.16 Aufgabe 1

Die Kategorie der $\mathbf{G}_m$-Moduln ist äquivalent zur Kategorie der graduierten endlich-dimensionalen k-Vektorräume.

Beweis. Wir bezeichnen mit

$$\mathrm{grVect}_k$$

die Kategorie der endlich-dimensionalen k-Vektorräume $V = \oplus_{n \in \mathbb{Z}} V_n$ und k-linearen Abbildungen $\varphi: V \longrightarrow W$, welche die Graduierung respektieren, d.h. $\varphi(V_n) \subseteq W_n$ für jedes $n \in \mathbb{Z}$ und mit

$$\mathbf{G}_m\text{-Mod}$$

die Kategorie der $\mathbf{G}_m$-Moduln.

Nach 3.2.3 (iii) ist jeder $\mathbf{G}_m$-Modul V eine direkte Summe von 1-dimensionalen Darstellungen. Eine 1-dimensionale Darstellung von $\mathbb{G}_m$ besteht gerade in der Multiplikation mit dem Wert eines Charakters (vgl. Beispiel 2.2.2). Deshalb besitzt V eine Zerlegung in eine direkte Summe

$$V = \oplus_{\chi \in X^*(\mathbf{G}_m)} V_\chi \text{ mit } V_\chi := \{ v \in V \mid r(t)\bullet v = \chi(t)\bullet v \text{ für } t \in \mathbf{G}_m \}.$$

Dabei bezeichne $r = r_V$: $\mathbf{G}_m \longrightarrow \mathbf{GL}(V)$ die rationale Darstellung, welche die $\mathbb{G}_m$-Modul-Struktur von V definiert.
Wegen $X^*(\mathbf{G}_m) \cong \mathbb{Z}$ bekommt V auf diese Weise die Struktur eines Graduierten k-Vektorraums:

$$V = \oplus_{n \in \mathbb{Z}} V_n \text{ mit } V_n := \{v \in V \mid r(t)\bullet v = t^n \text{ für jedes } t \in k^*\}.$$

Sie $f: V \longrightarrow W$ ein Homomorphismus von $\mathbf{G}_m$-Moduln. Dann gilt

$$f(r_V(t)\bullet v) = r_W(t)\bullet f(v) \text{ für jedes } v \in V \text{ und jedes } t \in k^*.$$

Insbesondere ist für $v \in V_n$

$$r_W(t)\bullet f(v) = f(r_V(t)\bullet v) = f(t^n \bullet v) = t^n \bullet f(v),$$

d.h. $f(v) \in W_n$. Da dies für jedes $v \in V_n$ gilt, folgt

$$f(V_n) \subseteq W_n \text{ für jedes } n \in \mathbb{Z}.$$

Mit anderen Worten f respektiert die Graduierung der beteiligten Moduln. Wir erhalten so einen Funktor

$$\mathbf{G}_m\text{-Mod} \longrightarrow \text{grVect}_k,\ V \mapsto V.$$

Es reicht zu zeigen, dieser Funktor ist eine Äquivalenz von Kategorien. Dazu reicht es zu zeigen (vgl. Bucur & Deleanu [1], Kapitel 1, §6, Proposition 1.17),

1. Jedes Objekt von grVect_k ist zu einem $\mathbf{G}_m$-Modul isomorph.
2. Für je zwei $\mathbf{G}_m$-Moduln V und W ist die Abbildung

$$\text{Hom}_{G_m}(V, W) \longrightarrow \text{Hom}_{\text{grVect}_k}(V, W),\ V \xrightarrow{f} W \mapsto V \xrightarrow{f} W,$$

bijektiv.

Zu 2. Die Abbildung ist trivialerweise injektiv. Es reicht die Surjektivität zu beweisen. Sei

$$h: V \longrightarrow W$$

eine k-lineare Abbildung, welche die Graduierungen von V und W respektiert, d.h. es gelte

$$h(V_n) \subseteq W_n \text{ für jedes } n \in \mathbb{Z}.$$

Dann gilt für jedes $t \in \mathbf{G}_m$ ($= k^*$).

$$\begin{aligned} r_W(t)\bullet h(V_n) &= t^n \bullet h(V_n) && \text{(wegen } h(V_n) \subseteq W_n \text{ und der Definition von } W_n) \\ &= h(t^n \bullet V_n) && \text{(h ist k-linear und } t^n \in k^* \subseteq k) \\ &= h(r_V(t)\bullet V_n) \end{aligned}$$

Da dies für jedes $n \in \mathbb{Z}$ gilt, folgt $r_W(t)\bullet h(V) = h(r_V(t)\bullet V)$ für jedes t, d.h. h ist ein Homomorphimus von $\mathbf{G}_m$-Moduln (und liegt damit im Bild der Abbildung von 2).

Zu 1. Sei $V = \oplus_{n \in \mathbb{Z}} V_n$ ein graduierter k-Vektorraum endlicher Dimension. Wir definieren für jedes n auf V_n die Struktur eines G_m-Moduls durch

$$G_m \longrightarrow \mathbf{GL}(V_n),\ t \mapsto (v \mapsto t^n \bullet v).$$

Dies ist ein Gruppen-Homomorphismus und - weil durch $\chi(t) = t^n$ ein Charakter von $\mathbf{G}_m$, d.h. eine reguläre Abbildung auf $\mathbf{G}_m$ definiert ist, ein Homomorphismus von linearen algebraischen Gruppen. Wir erhalten auf diese Weise für jedes $n \in \mathbb{Z}$ eine rationale Darstellung von $\mathbf{G}_m$. Die direkte Summe aller dieser Darstellungen (von denen nur endlich viele von 0 verschieden sind) ist ist ein $\mathbf{G}_m$-Modul, dessen zugehöriger graduierter Vektorraum gerade V ist.
QED.

3.2.16 Aufgabe 2

Sei $A := \oplus_{n\in\mathbb{Z}} A_n$ eine graduierte k-Algebra, welche über k endlich erzeugt und nullteilerfrei ist. Wir nehmen an, A ist von A_0 verschieden,

$$A \neq A_0.$$

Sei

$$d\bullet\mathbb{Z} = < n \in \mathbb{Z} \mid A_n \neq 0 \}$$

die von den Graden erzeugte Untergruppe, für welche es von 0 verschiedene homogene Elemente von A gibt. Weiter seien zwei von 0 verschiedene homogene Elemente gegeben, sagen wir

$$f \in A_i - \{0\} \text{ und } g \in A_j - \{0\} \text{ mit } i-j = d.$$

Wir betrachten den Quotientenring (vgl. 1.4.6)

$$B := A_{fg}.$$

Beweisen sie folgende Aussagen.

(i) Die Graduierung von A definiert eine Graduierung von B,

$$B = \oplus_{n\in\mathbb{Z}} B_n.$$

(ii) Es gibt einen Isomorphismus von graduierten Ringen $B_0 \otimes k[\frac{f}{g}, \frac{g}{f}] \cong B$.

(iii) B_0 ist endlich erzeugt und nullteilerfrei.

Beweis. Zu (i). Jedes Element von B hat die Gestalt

$$\frac{a}{(fg)^{\ell}} \text{ mit } a \in A \text{ und } \ell \in \mathbb{Z}.$$

Wir setzen

$$B_n := \{\frac{a}{(fg)^{\ell}} \in B \mid a \in A_{n+(i+j)\bullet\ell}\}.$$

Die B_n sind additive Untergruppen von B mit

$$B_n, \bullet B_n, \subseteq B_n, +n,$$

und

$$\sum_{n\in\mathbb{Z}} B_n = B.$$

Wir haben zu zeigen, die Summe auf der linken Seite ist direkt. Seien $b_{n_i} \in B_{n_i}$ mit

$$b_{n_1} + \ldots + b_{n_r} = 0,$$

wobei die n_μ paarweise verschieden seien. Wir haben zu zeigen, daß dann $b_{n_\mu} = 0$ gilt für jedes μ. Weil A nullteilerfrei ist, gilt dasselbe für B und wir können A als Teilring von B betrachten. Deshalb gibt es eine natüliche Zahl n derart, daß für jedes μ das Produkt

$$b_{n_\mu} \cdot (fg)^n \tag{1}$$

in A liegt. Es ist dann ein homogenes Element von A des Grades

$$(n_\mu + (i+j)\cdot\ell) + (i+j)\cdot(n-\ell) = n_\mu + (i+j)\cdot n.$$

Weil die n_μ paarweise verschieden sind, sind auch die Grade der homogenen Elemente (1) paarweise verschieden. Ihre Summe ist

$$\sum_{\mu=1}^{r} b_{n_\mu} \cdot (fg)^n = \Big(\sum_{\mu=1}^{r} b_{n_\mu}\Big) \cdot (fg)^n = 0 \cdot (fg)^n = 0.$$

Damit ist jedes der Elemente (1) gleich Null in A, also auch in B. Weil B nullteilerfrei ist, ist auch jedes b_{n_μ} gleich 0.

Zu (ii). Nach Definition von d können wir den Ring A als graduierten Ring mit den homogenen Bestandteilen

$$A(\mu) := A_{d\cdot\mu}$$

betrachten,

$$A = \oplus_{n\in\mathbb{Z}} A(n).$$

Es ist derselbe Ring, nur daß wir alle Grade durch d geteilt haben. Die Grade der homogenen Elemente f und g unterscheiden sich bezüglich dieser neuen Graduierung um 1. In analoger Weise wie oben erhalten wir eine Graduierung von B,

$$B = \oplus_{n\in\mathbb{Z}} B(n)$$

bei welcher ebenfalls alle Grade durch d geteilt sind im Vergleich zur ursprünglichen Graduierung von B. Die Elemente f/g und g/f sind homogene Elemente von Grad 1 bzw. -1 von B bezüglich der neuen Graduierung. O.B.d.A. sei

$$i > j$$

(andernfalls müssen wir im folgenden die Rollen von f und g vertauschen). Dann sind f/g und g/f homogene Elemente von Grad 1 bzw. -1 bezüglich der neuen Graduierung. Insbesondere gilt für jedes $n \in \mathbb{Z}$:

$$B(n)\cdot\frac{f}{g} \subseteq B(n+1) \text{ und } B(n)\cdot\frac{g}{f} \subseteq B(n-1).$$

Weil f/g und g/f zueinander inverse Einheiten von B sind, gilt sogar überall das Gleichheitszeichen,

$$B(n)\cdot\frac{f}{g} = B(n+1) \text{ und } B(n)\cdot\frac{g}{f} = B(n-1).$$

Damit ist

$$B = \oplus_{n\in\mathbb{Z}} B(n) = \oplus_{n\in\mathbb{Z}} B(0)\cdot\left(\frac{f}{g}\right)^n$$

und

$$B(0)\otimes k\left[\frac{f}{g},\frac{g}{f}\right] = B(0)\otimes\left(\oplus_{n\in\mathbb{Z}} k\cdot\left(\frac{f}{g}\right)^n\right)$$

$$\cong \oplus_{n\in\mathbb{Z}} B(0)\otimes k\cdot\left(\frac{f}{g}\right)^n \qquad (\otimes \text{ und } \oplus \text{ kommutieren})$$

$$\cong \oplus_{n\in\mathbb{Z}} B(0)\cdot\left(\frac{f}{g}\right)^n \qquad (\text{wegen } B(0)\otimes_k k \cong B(0)$$

$= B.$

Zu (iii). B_0 ist als Teilring des Quotientenrings B der nullteilerfreien Algebra ebenfalls nullteilerfrei. Wir haben noch zu zeigen, B_0 ist endlich erzeugt über k. Dazu reicht es zu zeigen, B_0 ist eine Faktor-Algebra von B.

Weil die ganzzahligen Potenzen des homogenen Elements f/g in paarweise verschiedenen B(n) liegen, sind sie linear unabhängig über k. Deshalb ist durch

$$k[T, T^{-1}] \longrightarrow k[\tfrac{f}{g}, \tfrac{g}{f}],\ T \mapsto \tfrac{f}{g},\ T^{-1} \mapsto \tfrac{g}{f},$$

ein Isomorphismus von k-Algebren definiert. Damit ist

$$\begin{aligned} B/(\tfrac{f}{g} - 1) &\cong (B(0) \otimes k[\tfrac{f}{g}, \tfrac{g}{f}]) / (1 \otimes \tfrac{f}{g} - 1 \otimes 1) \\ &\cong (B(0) \otimes k[T, T^{-1}]) / (1 \otimes T - 1 \otimes 1) \\ &\cong B(0) \otimes_k (k[T, T^{-1}]/(T-1)) \end{aligned}$$

Zum Beweis der Behauptung reicht es zu zeigen, es gilt

$$k[T, T^{-1}] / (T-1) \cong k, \qquad (2)$$

denn dann ist

$$B/(\tfrac{f}{g} - 1) \cong B(0) \otimes_k k \cong B(0)$$

und B(0) ist als Faktorring von B endlich erzeugt. Beweisen wir also (2). Mit einer weiteren Unbestimmten S gilt

$$\begin{aligned} k[T, T^{-1}]/ (T-1) \quad &\cong k[T, S] / (TS - 1, T-1) \\ &= k[T, S] / (S - 1, T-1) \\ &\cong k. \end{aligned}$$

QED.

3.2.16 Aufgabe 3

Verwenden Sie die vorangehende Aufgabe zum Beweis der folgenden Eigenschaften einer $\mathbf{G}_m$-Operation auf einer affinen Varietät V. Es gibt eine disjunkte Zerlegung

$$V = \bigvee_{i=0}^{N} V_i$$

in irreduzible und lokal abgeschlossene Teilmengen V_i mit

(i) V_0 ist die Menge der Fixpunkte.

(ii) Für $i > 0$ gibt es eine affine Varietät V_i', einen Isomorphismus $\phi_i: V_i' \times k^* \longrightarrow V_i$ und eine ganze Zahl d_i mit $\phi_i(x, t^{d_i} \bullet u) = t \bullet \phi_i(x, u)$ für $x \in V_i'$, $t, u \in k^*$.

(iii) Die Abschließung von V_i ist für jedes i eine Vereinigung von gewissen V_j.

Bemerkungen

(i) Die Formulierung der Aufgabe bedarf einer Modifikation wie das folgende Beispiel zeigt. Sei V die disjunte Vereinigung zweier affiner Geraden, sagen wir

$$V = Z' \bigcup Z'',\ Z' \cong \mathbb{A}^1 \cong Z''$$

auf denen $\mathbf{G}_m$ nicht-trivial operiert, sagen wir

$$a(t, x') := t^{d'} \bullet x' \text{ und } a(t, x'') := t^{d''} \bullet x'' \text{ für } t \in G_m,\ x' \in Z',\ x'' \in Z''$$

mit von 0 verschiedenen ganzen Zahlen d' und d'', und sei

$$V = \bigvee_{i=0}^{N} V_i$$

eine disjunkte Zerlegung von V in lokal abgeschlossene und $\mathbf{G}_m$-stabile Teilmengen von V, wobei V_0 die Menge der Fixpunkte der Operation sei. Diese Menge besteht gerade aus den beiden Ursprüngen von Z' und Z", sagen wir

$$V_0 = \{0', 0"\}$$

Wegen

$$V = \bigcup_{i=0}^{N} \overline{V}_i$$

gilt dann für jede irreduzible Komponente Z von V,

$$Z = \bigcup_{i=0}^{N} \overline{V}_i \cap Z.$$

Die ist eine Darstellung der irreduziblen Menge Z als Vereinigung von abgeschlossenen Teilmengen. Deshalb gibt es ein in i mit

$$Z = \overline{V}_i \cap Z$$

also $Z \subseteq \overline{V}_i$. Dabei ist die Abschließung $\overline{V}_i$ der irreduziblen Mengen V_i ebensfalls irreduzibel (nach 1.2.3 (i)). Als irreduzible Komponente von V ist Z maximal unter den irreduziblen Teilmengen, d.h. es gilt

$$Z = \overline{V}_i.$$

Wir haben gezeigt, die Komponenten Z' und Z" von V sind Abschließungen von Mengen der Gestalt V_i, sagen wir

$$Z' = \overline{V}_{i'}, \text{ und } Z" = \overline{V}_{i"},$$

Nun zerfällt Z' in die beiden Orbits {0'} und Z' - {0'} und analog Z" in die Orbits {0"} und Z" - {0"}. Damit gilt

$$V_{i'} = Z' - \{0'\} \text{ und } V_{i"} = Z" - \{0"\}.$$

Wären die beiden Abschließungen $\overline{V}_{i'}$ und $\overline{V}_{i"}$ Vereinigungen von Mengen der Gestalt V_j, so müßten die Mengen {0'} und {0"} von der Gestalt V_j sein. Diese sind aber von V_0 verschieden und nicht disjunkt zu V_0. In der beschriebenen Situation gibt es somit keine Zerlegung der geforderten Art.
Nachfolgend findet sich eine modifizierte (und beweisbare) Formulierung der Aussage.

(ii) Die Zahlen d_i von Bedingung (ii) sind notwendig von 0 verschieden, denn andernfalls würde V_i aus Fixpunkten bestehen und wäre nicht disjunkt zu V_0.

(iii) Der nachfolgende Beweis macht keinen Gebrauch der Aussage von Aufgabe 2. Es wäre interessant, einen Beweis zu sehen, der sich wesentlich auf diese Aufgabe stützt.

Modifizierte Formulierung der zu beweiseneden Aussage
Sei V eine affine $\mathbf{G}_m$-Varietät. Dann gibt es eine disjunkte Zerlegung

$$V = \bigvee_{i=0}^{N} V_i$$

in irreduzible und lokal abgeschlossene Teilmengen V_i, welche als geometrische Räume isomorph zu affinen Varietäten sind, mit folgenden Eigenschaften.

(i) Die Menge der Fixpunkte der $\mathbf{G}_m$-Operation auf V ist eine Vereinigung von gewissen V_i. Insbesondere besteht jedes V_i, welches einen Fixpunkt enthält, ausschließlich aus Fixpunkten.

(ii) Für jedes V_i , welches keinen Fixpunkt enthält gibt es eine affine Varietät V'_i, einen Isomorphismus affiner Varietäten

$$\phi_i: V'_i \times k^* \longrightarrow V_i$$

und eine von 0 verschiedene ganze Zahl d_i mit

$$\phi_i(x, t^{d_i} \cdot u) = t \cdot \phi_i(x, u) \text{ für } x \in V'_i,\ t, u \in k^*.$$

(iii) Für jedes i ist die Abschließung von V_i Vereinigung von gewissen V_j. Mit anderen Worten, die Zerlegung von V in die V_i ist eine gute Stratifikation mit Sinne des vierten Anhangs, Definition 4.2.

Beweis. 1. Schritt. Seien $V = \mathbb{A}^n$ der euklidische Raum k^n und der zur gegebenen Operation

$$a: \mathbf{G}_m \times V \longrightarrow V$$

gehörige Gruppen-Homomorphismus eine rationale Darstellung

$$r: \mathbf{G}_m \longrightarrow \mathbf{GL}_n,$$

(d.h. ein Kocharakter von $\mathbf{GL}_n$). Dann existiert eine Zerlegung

$$V = \bigvee_{i=0}^{N} V_i$$

in lokal abgeschlossene Teilmengen V_i , welche als geometrische Räume isomorph zu irreduziblen affinen Varietäten sind, wobei die Aussgen (i)-(iii) des Satzes gelten. Eine der Teilmengen V_i , sagen wir

$$V_i = V_0$$

ist die Menge der Fixpunkte der Operation. Diese Menge ist abgeschlossen. Es besteht die Implikation

$$\overline{V}_i \bigcap V_0 \neq \varnothing \Rightarrow V_0 \subseteq \overline{V}_i.$$

Die Elemente von $\mathbf{G}_m$ sind (trivialerweise) halbeinfach, also sind es auch die Elemente von $r(\mathbf{G}_m)$ (nach 2.4.8(ii)), und zwar sind sie es auch als n×n-Matrizen (nach 2.4.9). Weil außerdem je zwei Matrizen von $r(\mathbf{G}_m)$ miteinander kommutieren, gibt es eine Matrix $A \in \mathbf{GL}_n$ mit $A \cdot r(\mathbf{G}_m) \cdot A^{-1} \in \mathbf{D}_n$ (nach 2.4.2). Wir können r um den Isomorphismus σ_A mit $\sigma_A(x) = A \cdot x \cdot A^{-1}$ abändern, d.h. ersetzen durch die Zusammensetzung

$$\sigma_A \circ r: \mathbf{G}_m \xrightarrow{r} \mathbf{GL}_n \xrightarrow{\sigma_A} \mathbf{GL}_n,\ r \mapsto r(t) \mapsto A \cdot r(t) \cdot A^{-1},$$

und V durch die Varietät A•V. Dadurch wird r ein Homomorphismus algebraischer Gruppen, dessen Bild in $\mathbf{D}_n$ liegt, d.h. eine Abbildung der Gestalt

$$r: \mathbf{G}_m \longrightarrow \mathbf{GL}_n\ ,\ r \mapsto \mathrm{diag}(t^{d_1},...,t^{d_n}), \tag{1}$$

mit ganzen Zahlen $d_1,...,d_n$.

Falls einige der d_i gleich Null sind, so können wir durch eine Permutation der Koordinaten erreichen, daß die ersten n' von ihnen ungleich 0 und alle übrigen gleich 0 sind,

$$d_1 \neq 0,...,d_{n'} \neq 0 \text{ und } d_{n'+1} = d_{n'+2} = ... = d_n = 0,$$

und wir können die rationale Darstellung

$$r': \mathbf{G}_m \longrightarrow \mathbf{GL}_{n'},\ ,\ t \mapsto \mathrm{diag}(t^{d_1},...,t^{d_{n'}}),$$

betrachten. Ist eine zu r' gehörige Zerlegung

$$\mathbb{A}^r = \bigcup_{i=0}^{N} V_i$$

gegeben, welche den drei Bedingungen des Satzes genügt, so ist

$$\mathbb{A}^n = \mathbb{A}^r \times \mathbb{A}^{n-r} = \bigcup_{i=0}^{N} V_i \times \mathbb{A}^{n-r}$$

eine Zerlegung der gesuchten Art des $\mathbb{A}^n$. Die in Aussage (ii) beschriebenen Isomorphismen sind dabei die Abbildungen

$$\psi_i: (V'_i \times \mathbb{A}^{n-r}) \times k^* \longrightarrow V_i \times \mathbb{A}^{n-r},\ (x,y,t) \mapsto (\phi_i(x,t), y),$$

wenn die ϕ_i die entsprechenden Abbildungen für die Zerlegung des $\mathbb{A}^r$ sind: für $x \in V'_i$, $y \in \mathbb{A}^{n-r}$ und $t \in k^*$ gilt nämlich

$$\begin{aligned}
\psi_i(x,y,t^{d_i} \bullet u) &= (\phi_i(x, t^{d_i} \bullet u), y) && \text{(nach Definition von } \psi_i) \\
&= (r'(t) \bullet \phi_i(x,u), y) && \text{(nach Wahl der } \phi_i) \\
&= r(t) \bullet (\phi_i(x,u), y) && \text{(wegen } r(t) = r'(t) \times Id) \\
&= r(t) \bullet \psi_i(x,y,u). && \text{(nach Definition von } \psi_i).
\end{aligned}$$

Wir können deshalb annehmen, die ganzen Zahlen d_i in (1) sind sämtlich von 0 verschieden:

$$d_i \neq 0 \text{ für } i = 1,...,n. \tag{2}$$

In dieser Situation zerlegen wir den $\mathbb{A}^n$ wie folgt in lokal abgeschlossene Teilmengen. Für jedes Element $\mathbf{i} := \{i_1,...,i_r\} \in P_n$ der Potenzmenge P_n der ersten n natürlichen Zahlen (d.h. für jede Teilmenge $\mathbf{i}$ von $\{1,...,n\}$) sei

$$V_{\mathbf{i}} := \{x = \begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} \in k^n \mid x_i = 0 \text{ für } i \in \mathbf{i} \text{ und } x_i \neq 0 \text{ für } i \notin \mathbf{i}\}$$

$$= V(x_{i_1},...,x_{i_r}) \cap D(\prod_{i \notin \mathbf{i}} x_i)$$

der Durchschnitt der abgeschlossenen Teilmenge $V(x_{i_1},...,x_{i_r})$ von $\mathbb{A}^n$ mit der offenen Hauptmenge $D(\prod_{i \notin \mathbf{i}} x_i)$. Diese Menge ist lokal abgeschlossen im $\mathbb{A}^n$. Zum Beispiel ist

$$V_{\varnothing} = D(x_1 \bullet ... \bullet x_n) \text{ und } V_{\{1,...,n\}} = V(x_1,...,x_n) = \{\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}\}$$

Bei der Multiplikation mit den von Null verschiedenen Elementen t^{d_i} bleiben von Null verschiedene Koordinaten eines Punktes von $\mathbb{A}^n$ von Null verschieden, und sie bleiben gleich Null, wenn sie es vor der Multiplikation waren. Deshalb ist

$V_{\mathbf{i}}$ eine $\mathbf{G}_m$-stabile lokal abgeschlossene Teilmenge von $\mathbb{A}^n$ für jedes $\mathbf{i} \in P_n$.

Die $V_{\mathbf{i}}$ sind paarweise disjunkt und jeder Punkt des $\mathbb{A}^n$ liegt in einem $V_{\mathbf{i}}$, d.h.

$$\mathbb{A}^n = \bigcup_{\mathbf{i} \in P_n} V_{\mathbf{i}}$$

ist eine Zerlegung des $\mathbb{A}^n$ in paarweise disjunkte lokal abgeschlossene Teilmengen. Außerdem ist $V_{\mathbf{i}}$ eine offene Teilmenge der irreduziblen Varietät $V(x_{i_1},...,x_{i_r})$, und damit irreduzibel,

$$V_{\mathbf{i}} \text{ ist irreduzibel für jedes } \mathbf{i} \in P_n.$$

Weil $V(x_{i_1},...,x_{i_r})$ irreduzibel ist, liegt jede nicht-leere offene Teilmenge dicht, d.h. die Abschließung von $V_{\mathbf{i}}$ ist gleich

$$\overline{V}_{\mathbf{i}} = V(x_{i_1},...,x_{i_r}) = \bigcup_{\mathbf{i} \subseteq \mathbf{j} \subseteq \{1,...,n\}} V_{\mathbf{j}}$$

Mit anderen Worten, die Abschließung jedes $V_{\mathbf{i}}$ ist eine Vereinigung von Mengen der Gestalt $V_{\mathbf{i}}$, die Zerlegung des $\mathbb{A}^n$ in die $V_{\mathbf{i}}$ ist eine gute Stratifikation. Es ist Bedingung (iii) des Satzes erfüllt.

Der einzige Punkt $\begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ von $V_{\{1,...,n\}}$ ist ein Fixpunkt bei der Operation von $\mathbf{G}_m$. Wie in

Es gibt also ein Stratum, welches nur aus Fixpunkten besteht. Dieses Stratum ist abgeschlossen, und mit $\overline{V}_{\mathbf{i}} \bigcap V_0 \neq \varnothing$ gilt sogar $V_0 \subseteq \overline{V}_{\mathbf{i}}$.

Es reicht zu zeigen, daß daß es für jedes **i** != {1,...,n} die in (ii) beschriebenen Isomorphismen gibt. Denn dann gibt es insbesondere keine weieren Fixpunkte und $V_{\{1,...,n\}}$ ist die Mengen aller Fixpunkte. Sei also

$$\mathbf{i} \in P_n$$

vorgegeben. Es gilt

$$V_{\mathbf{i}} \subseteq \overline{V}_{\mathbf{i}} = V(x_{i_1},...,x_{i_r}).$$

Außerdem ist mit $V_{\mathbf{i}}$ auch die Abschließung $V(x_{i_1},...,x_{i_r})$ von $V_{\mathbf{i}}$ stabil bei der Operation von $\mathbf{G}_m$. Wir können deshalb zum Beweis den $\mathbb{A}^n$ durch den linearen Unterraum $V(x_{i_1},...,x_{i_r})$ ersetzen, d.h. wir können uns auf den Fall $i = \varnothing$ beschränken, d.h. auf den Fall

$$V_{\mathbf{i}} = D(x_1 \bullet ... \bullet x_n) \subseteq \mathbb{A}^n.$$

Der Koordinatenring von $V_{\mathbf{i}}$ hat dann die Gestalt

$$k[V_{\mathbf{i}}] = k[T_1, T_1^{-1},..., T_n, T_n^{-1}] = k[T_1, T_1^{-1}] \otimes ... \otimes k[T_n, T_n^{-1}].$$

Die algebraische Varietät $V_{\mathbf{i}}$ ist isomorph zum direkten Produkt von n Exemplaren der Gruppe $\mathbf{G}_m$,

$$V_{\mathbf{i}} = (\mathbf{G}_m)^n \subseteq \mathbf{D}_n \subseteq \mathbf{GL}_n.$$

Identifiziert man $V_{\mathbf{i}}$ auf diese Weise mit einer (abgeschlossenen) Teilmenge der $\mathbf{GL}_n$, so ist die Operation von $\mathbf{G}_m$ auf $V_{\mathbf{i}}$ gerade durch die Multiplikation von Matrizen definiert,

$$\mathbf{G}_m \times V_{\mathbf{i}} \longrightarrow V_{\mathbf{i}}, (t, x) \mapsto r(t) \bullet x \text{ (Matrizen-Multiplikation).}$$

Wir setzen wie folgt die gegebene rationale Darstellung

$$r: \mathbf{G}_m \longrightarrow \mathbf{GL}_n, r \mapsto \operatorname{diag}(t^{d_1},...,t^{d_n})$$

($d_i \neq 0$ für i = 1,...,n), mit einem Automorphismus von $V_{\mathbf{i}}$ zusammen, um die Abbildungsvorschrift von r zu vereinfachen. Sei

$$d := ggT(d_1,...,d_n)$$

der größte gemeinsame Teiler der d_i. Dann können wir r als Zusammensetzung

$$r = r'' \circ r': \mathbf{G}_m \xrightarrow{r'} \mathbf{G}_m \xrightarrow{r''} \mathbf{GL}_n$$

schreiben mit

$$r'(t) := t^d \text{ und } r''(t) := \operatorname{diag}(t^{\alpha_1},...,t^{\alpha_n}),\ \alpha_i = d_i/d \in \mathbb{Z},\ t \in \mathbf{G}_m.$$

Weil der größte gemeinsame Teiler der α_1 gleich 1 ist, gibt es ganze Zahlen $\beta_{in} \in \mathbb{Z}$ mit

$$\sum_{i=1}^{n} \alpha_i \beta_{in} = 1$$

Zur Konstruktion des Automorphismus von $V_{\mathbf{i}}$ betrachten wir die $\mathbb{Z}$ lineare Abbildung

$$\rho: \mathbb{Z}^n = \sum_{i=1}^{n} \mathbb{Z} \bullet e_i \longrightarrow \mathbb{Z},\ \sum_{i=1}^{n} x_i \bullet e_i \mapsto \sum_{i=1}^{n} x_i \bullet \alpha_i.$$

Die e_i sollen dabei die Standard-Einheitsvektoren bezeichnen. Nach Wahl der β_{in} gilt

$$\rho(b_n) = 1 \text{ mit } b_n := \sum_{i=1}^{n} \beta_{in} \bullet e_i, \tag{3}$$

d.h. ρ ist surjektiv und definert eine kurze exakte Sequenz

$$0 \longrightarrow \mathrm{Ker}(\rho) \longrightarrow \mathbb{Z}^n \xrightarrow{\rho} \mathbb{Z} \longrightarrow 0.$$

Die Einschränkung von ρ auf $\mathbb{Z}\bullet b_n$ ist ein Isomorphismus. Die Sequenz zerfällt und führt zu einer Zerlegung von $\mathbb{Z}^n$ in eine direkte Summe

$$\mathbb{Z}^n = \mathrm{Ker}(\rho) \oplus \mathbb{Z}\bullet b_n.$$

Als Untegruppe einer freien abelschen Gruppe $\mathbb{Z}^n$ ist Ker(ρ) selbst eine freie abelsche Gruppe. Wir wählen ein linear unabhängiges Erzeugendensystem von Ker(ρ), sagen wir

$$\mathrm{Ker}(\rho) = \mathbb{Z}\bullet b_1 + \ldots + \mathbb{Z}\bullet b_{n-1},$$

und erhalten

$$\sum_{i=1}^{n} \mathbb{Z}\bullet e_i = \mathbb{Z}^n = \mathrm{Ker}(\rho) \oplus \mathbb{Z}\bullet b_n = \sum_{i=1}^{n} \mathbb{Z}\bullet b_i.$$

Indem wir jedes Element der beiden Basen als Linearkombination der Elemente der anderen schreiben, erhalten zwei zueinander inverse Matrizen mit ganzzahligen Einträgen,

$$(\beta_{ij}), (\gamma_{ij}) \in M_n(\mathbb{Z}), (\beta_{ij})\bullet(\gamma_{ij}) = (\delta_{ij})$$

mit

$$b_i = \sum_{j=1}^{n} \beta_{ji}\bullet e_j \text{ und } e_j = \sum_{i=1}^{n} \gamma_{ij}\bullet b_i,$$

wobei die β_{ij} für j = n mit den oben eingeführten β_{in} übereinstimmen (auf Grund der Definition (3) von b_1). Weil die b_i für i < n im Kern von ρ liegen, gilt

$$\sum_{j=1}^{n} \beta_{ji}\bullet\alpha_j = 0 \text{ für } i = 1,\ldots,n-1. \qquad (4)$$

Die Einträge der Matrizen (β_{ij}) und (γ_{ij}) definieren k-Algebra-Homomorphismen

$$\varphi: k[V_{\mathbf{i}}] = k[T_1, T_1^{-1}, \ldots, T_n, T_n^{-1}] \longrightarrow k[T_1, T_1^{-1}, \ldots, T_n, T_n^{-1}] = k[V_{\mathbf{i}}],\ T_i \mapsto \prod_{\mu=1}^{n} T_\mu^{\gamma_{\mu i}},$$

und

$$\psi: k[V_{\mathbf{i}}] = k[T_1, T_1^{-1}, \ldots, T_n, T_n^{-1}] \longrightarrow k[T_1, T_1^{-1}, \ldots, T_n, T_n^{-1}] = k[V_{\mathbf{i}}],\ T_i \mapsto \prod_{\nu=1}^{n} T_\nu^{\beta_{\nu i}}.$$

Wegen

$$\begin{aligned} \varphi(\psi(T_i)) &= \varphi\Big(\prod_{\nu=1}^{n} T_\nu^{\beta_{\nu i}}\Big) = \prod_{\nu=1}^{n} \varphi(T_\nu)^{\beta_{\nu i}} = \prod_{\nu=1}^{n}\prod_{\mu=1}^{n} (T_\mu^{\gamma_{\mu\nu}})^{\beta_{\nu i}} \\ &= \prod_{\mu=1}^{n} T_\mu^{\sum_{\nu=1}^{n} \gamma_{\mu\nu}\beta_{\nu i}} = \prod_{\mu=1}^{n} T_\mu^{\delta_{\mu i}} \\ &= T_i \end{aligned}$$

und

$$\begin{aligned}\psi(\varphi(T_i)) &= \psi(\prod_{\mu=1}^{n} T_\mu^{\gamma_{\mu i}}) = \prod_{\mu=1}^{n} \psi(T_\mu)^{\gamma_{\mu i}} = \prod_{\mu=1}^{n}\prod_{\nu=1}^{n} (T_\nu^{\beta_{\nu\mu}})^{\gamma_{\mu i}} \\ &= \prod_{\nu=1}^{n} T_\nu^{\sum_{\mu=1}^{n} \beta_{\nu\mu}\gamma_{\mu i}} = \prod_{\nu=1}^{n} T_\nu^{\delta_{\nu i}} \\ &= T_i\end{aligned}$$

Also sind φ und ψ zueinander inverse k-Algebra-Isomorphismen. Sie definieren deshalb zueinander inverse Isomorphismen afffiner algebraischer Varietäten

$$\varphi^{\#}: V_{\mathbf{i}} \longrightarrow V_{\mathbf{i}}, \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \prod_{\mu=1}^{n} x_\mu^{\gamma_{\mu 1}} \\ \cdots \\ \prod_{\mu=1}^{n} x_\mu^{\gamma_{\mu n}} \end{pmatrix}$$

und

$$\psi^{\#}: V_{\mathbf{i}} \longrightarrow V_{\mathbf{i}}, \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} \mapsto \begin{pmatrix} \prod_{\nu=1}^{n} x_\nu^{\beta_{\nu 1}} \\ \cdots \\ \prod_{\nu=1}^{n} x_\nu^{\beta_{\nu n}} \end{pmatrix}.$$

Wir können deshalb $V_{\mathbf{i}}$ durch die isomorphe Varietät $\psi^{\#}(V_{\mathbf{i}})$ ersetzen. Die Operation von $\mathbf{G}_m$ auf $V_{\mathbf{i}}$,

$$\mathbf{G}_m \times V_{\mathbf{i}} \longrightarrow V_{\mathbf{i}}, (t, x) \mapsto r(t)\bullet x,$$

wird dann zur folgenden Operation von $\mathbf{G}_m$ auf $\psi^{\#}(V_{\mathbf{i}})$

$$\mathbf{G}_m \times \psi^{\#}(V_{\mathbf{i}}) \longrightarrow \psi^{\#}(V_{\mathbf{i}}), (t, x) \mapsto s(t)(x) := \psi^{\#}(r(t)\bullet\varphi^{\#}(x)).$$

Es gilt

$$\psi^{\#}(\mathrm{diag}(t^{d_1},\ldots,t^{d_n})\bullet\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}) = \psi^{\#}(\begin{pmatrix} t^{d_1}\bullet x_1 \\ \cdots \\ t^{d_n}\bullet x_n \end{pmatrix}) = \begin{pmatrix} \prod_{\nu=1}^{n} (t^{d_\nu}\bullet x_\nu)^{\beta_{\nu 1}} \\ \cdots \\ \prod_{\nu=1}^{n} (t^{d_\nu}\bullet x_\nu)^{\beta_{\nu n}} \end{pmatrix}$$

$$= \begin{pmatrix} \prod_{\nu=1}^{n} ((t^d)^{\alpha_\nu \bullet x_\nu})^{\beta_{\nu 1}} \\ \cdots \\ \prod_{\nu=1}^{n} ((t^d)^{\alpha_\nu \bullet x_\nu})^{\beta_{\nu n}} \end{pmatrix} = \begin{pmatrix} (t^d)^{\sum_{\nu=1}^{n} \alpha_\nu \bullet \beta_{\nu 1}} \bullet \prod_{\nu=1}^{n} (x_\nu)^{\beta_{\nu 1}} \\ (t^d)^{\sum_{\nu=1}^{n} \alpha_\nu \bullet \beta_{\nu 2}} \bullet \prod_{\nu=1}^{n} (x_\nu)^{\beta_{\nu 2}} \\ \cdots \\ (t^d)^{\sum_{\nu=1}^{n} \alpha_\nu \bullet \beta_{\nu n}} \bullet \prod_{\nu=1}^{n} (x_\nu)^{\beta_{\nu n}} \end{pmatrix}$$

$$= \begin{pmatrix} \prod_{\nu=1}^{n} (x_\nu)^{\beta_{\nu 2}} \\ \cdots \\ \prod_{\nu=1}^{n} (x_\nu)^{\beta_{\nu n}} \\ t^d \bullet \prod_{\nu=1}^{n} (x_\nu)^{\beta_{\nu 1}} \end{pmatrix} \qquad \text{(wegen (3) und (4))}$$

$$= \mathrm{diag}(1,...,1,\, t^d) \bullet \psi^{\#}\left(\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}\right)$$

Wir setzen $\varphi^{\#}\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}$ für $\begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}$ ein und erhalten (weil $\varphi^{\#}$ und $\psi^{\#}$ invers zueinander sind)

$$s(t) \bullet \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix} = \mathrm{diag}(1,...,1,\, t^d) \bullet \begin{pmatrix} x_1 \\ \cdots \\ x_n \end{pmatrix}.$$

Durch den Koordinatenwechsel bekommt die Darstellung r die Gestalt

$$r: \mathbf{G}_m \longrightarrow GL_n\,,\ t \mapsto \mathrm{diag}(1,...,1,\, t^d).$$

Wenn wir $\mathbf{G}_m$ mit dem letzten Faktor von $V_{\mathbf{i}} = (\mathbf{G}_m)^n$ identifizieren und $V'_{\mathbf{i}}$ definieren als die affine Varietät

$$V'_{\mathbf{i}} := (\mathbf{G}_m)^{n-1},$$

so bekommt die identische Abbildung die Gestalt

$$\phi_{\mathbf{i}}: V'_{\mathbf{i}} \times \mathbf{G}_m \overset{\cong}{\longrightarrow} V_{\mathbf{i}}\,,\ (x_1,...,x_{n-1},\, t) \mapsto (t,\, x_1,...,x_{n-1},t).$$

Für die gegebene Operation von $\mathbf{G}_m$ auf $V_{\mathbf{i}}$ erhalten wir

$$a(t, (x_1,...,x_{n-1},u)) = (x_1,...,x_{n-1}, t^d \bullet u) = \phi_i((x_1,...,x_{n-1}), t^d \bullet u),$$

d.h. ϕ_i ist ein Isomorphismus der gesuchten Art.

2. Schritt. Die Behauptung des Satzes gilt, wenn man auf die Forderung verzichtet, daß die V_i für $i > 0$ irreduzibel sein sollen, und anstelle der Bedingung (iii) nur fordert, daß für jedes i die Inklusion

$$\overline{V}_i \subseteq \bigcup_{V_j \subseteq \overline{V}_i} V_j$$

besteht, d.h. die Zerlegung von V in die V_i ist eine Stratifikation im Sinne der Definition 4.3 des vierten Anhangs sein, wenn man die Index-Menge der i wie folgt mit einer Halbordnung versieht.

$$i \leq j \Leftrightarrow V_i \subseteq \overline{V}_j.$$

Nach 2.3.9 Aufgabe 2 gibt es ein n, eine abgeschlossene Teilvarietät $W \subseteq \mathbb{A}^n$ einen Isomorphismus affiner algebraischer Varietäten

$$\phi: V \xrightarrow{\cong} W \ (\hookrightarrow \mathbb{A}^n)$$

und eine rataionale Darstellung

$$r: \mathbf{G}_m \longrightarrow \mathbf{GL}_n$$

mit

$$\phi(a(t,x)) = r(t) \bullet \phi(x) \text{ für beliebige } t \in \mathbf{G}_m \text{ und beliebige } x \in V.$$

Nach dem ersten Schritt gibt es eine disjunkte Zerlegung

$$\mathbb{A}^n = \bigvee_{i=0}^{N} V_i$$

in lokal abgeschlossenene Teilmengen V_i, welche als geometrische Räume isomorph zu irreduziblen affinen Varietäten und welche den Bedingungen (i)-(iii) genügen. Insbesondere gibt es für jedes V_i, welches keinen Fixpunkt enthält eine affine Varietät V'_i und Isomorphismen affiner Varietäten

$$\phi_i: V'_i \times k^* \xrightarrow{\cong} V_i$$

mit

$$\phi_i(x, t^{d_i} \bullet u) = t \bullet \phi_i(x, u) \text{ für } x \in V'_i,\ t, u \in k^*.$$

Wir können die affine Varietät V durch deren Bild beim Isomorphismus ϕ ersetzen und annehmen, daß V eine abgeschlossene Teilvarietät von k^n ist,

$$V = W \subseteq k^n.$$

Wir bilden den Durchschnitt der obigen Zerlegung von $k^n = \mathbb{A}^n$ mit V und erhalten eine disjunkte Zerlegung

$$V = \bigvee_{i=0}^{N} (V_i \bigcap V) \tag{5}$$

von V in lokal abgeschlossene Teilmengen von V (welche isomorph zu affinen Varietäten sind)[18].
Weil V_0 aus den Fixpunkten der Operation von $\mathbf{G}_m$ besteht und die übrigen V_i keine Fixpunkte enthalten, gilt dasselbe für $V_0 \bigcap V$ und die übrigen $V_i \bigcap V$, d.h. Bedinung (i) ist für die Zerlegung (5) trivialerweise erfüllt.

Weil für jedes i die Abschließung $\overline{V}_i$ von V_i im $\mathbb{A}_n$ eine Vereinigung gewisser V_j ist (nämlich die Vereinigung aller V_j die ganz in $\overline{V}_i$ liegen), ist

$$\overline{V}_i \bigcap V = \bigcup_{V_j \subseteq \overline{V}_i} V_j \bigcap V$$

also

$$\overline{V_i \bigcap V} \subseteq^{19} \overline{V}_i \bigcap V = \bigcup_{V_j \subseteq \overline{V}_i} V_j \bigcap V.$$

Also ist die Zerlegung (5) ist eine Stratifikation von V.
Weil die fixpunkt freien Mengen V_i der Zerlegung des $\mathbb{A}^n$ der Bedingung (ii) genügen, sind die V_i stabil unter der Operation von $\mathbf{G}_m$. Weil auch V eine $\mathbf{G}_m$-stabile Teilmenge von $\mathbb{A}^n$ ist, ist auch der Durchschnitt

$$V_i \bigcap V \text{ eine } \mathbf{G}_m\text{-stabile Menge.}$$

Deshalb folgt die noch zu beweisenden Aussage aus der des nachfolgenden Schritts.

3. Schritt. Seien X' eine affine (bzw. quasi-affine[20]) Varietät, X eine affine (bzw. quasi-affine) $\mathbf{G}_m$-Varietät,

$$\varphi: X' \times k^* \longrightarrow X$$

ein Isomorphimus von Varietäten und d eine von 0 verschiedene ganze Zahl mit

$$\varphi(x, t^d \bullet u) = t \bullet \varphi(x, u) \text{ für } x \in X', t, u \in k^*.$$

Dann gilt für jede abgeschlossene (bzw. offene bzw. lokal abgeschlossene) $\mathbf{G}_m$-stabile Teilvarietät $Y \subseteq X$

$$\varphi^{-1}(Y) = Y' \times k^*$$

mit einer abgeschlossenen (bzw. offenen bzw. lokal abgeschlossenen) Teilvarietät $Y' \subseteq Y$. Insbesondere ist die Einschränkung

$$\psi := \varphi|_{Y' \times k^*}: Y' \times k^* \longrightarrow Y$$

ein Isomorphismus von Varietäten mit

---

[18] denn der Durchschnitt zweier affiner Teilvarietäten X und Y einer affinen Varietät Z ist (als Varietät) isomorph zum Durchschnitt

$X \bigcap Y \cong X \times Y \bigcap \Delta$ der affinen Teilvarietät $X \times Y$ von $Z \times Z$ mit der Diagonalen Δ von Z.

Also ist $X \bigcap Y$ isomorph zu einer abgeschlossenen Teilmenge der affinen Varietät $X \times Y$ und damit selbst eine affine Varietät.

[19] Trivialerweise gilt $V_i \bigcap V \subseteq \overline{V}_i \bigcap V$. Weil V abgeschlossen ist, ist auch $\overline{V}_i \bigcap V$ abgeschlossen, also gilt

$$\overline{V_i \bigcap V} \subseteq \overline{V}_i \bigcap V.$$

[20] Eine quasi-affine Varietät ist eine offene Teilvarietät einer affinen Varietät.

$$\psi(x, t^d \bullet u) = t \bullet \psi(x, u) \text{ für } x \in Y', t, u \in k^*.$$

Weil φ ein Isomorphismus ist, ist auch

$$\psi := \varphi|_{\varphi^{-1}(Y)} : \varphi^{-1}(Y) \longrightarrow Y$$

ein solcher. Es reicht zu zeigen

$$\varphi^{-1}(Y) = Y' \times k^*$$

mit Y' abgeschlossen (bzw. offen bzw lokal abgeschlossen) in Y'.
Die Identität

$$\psi(x, t^d \bullet u) = t \bullet \psi(x, u) \text{ für } x \in Y', t, u \in k^*.$$

ist dann eine Folge der analogen Identität für φ.

Für $(x, u) \in \varphi^{-1}(Y) \subseteq X' \times k^*$ und $t \in k^*$ gilt

$$\varphi(x, t^d \bullet u) = t \bullet \varphi(x, u) \in t \bullet Y \subseteq Y$$

Die Inklusion rechts besteht, weil Y stabil ist unter der Operation von $\mathbf{G}_m$. Damit gilt

$$(x, t^d \bullet u) \in \varphi^{-1}(Y) \text{ für beliebige } (x,u) \in \varphi^{-1}(Y) \text{ und beliebige } t \in k^*.$$

Weil k algebraisch abgeschlossen ist, folgt

$$\{x\} \times k^* \subseteq \varphi^{-1}(Y) \; (\subseteq X' \times k^*)$$

für jedes x, welches als erste Koordinate eines Paars aus $\varphi^{-1}(Y)$ auftritt. Zusammen mit der Inklusion $\varphi^{-1}(Y) \subseteq X' \times k^*$ ergibt sich,

$$(x, u) \in \varphi^{-1}(Y) \Leftrightarrow (x,1) \in \varphi^{-1}(Y) \text{ und } u \in k^*.$$

also

$$\varphi^{-1}(Y) = Y' \times k^*$$

mit

$$Y' := \{x \in X' \mid (x,1) \in \varphi^{-1}(Y) \}.$$

Als vollständiges Urbild der abgeschlossenen (bzw. offenen bzw. lokal abgeschlossenen) Teilmenge $\varphi^{-1}(Y)$ bei der regulären Abbildung

$$X' \longrightarrow X' \times k^*, \; x \mapsto (x,1),$$

ist Y' abgeschlossen (bzw. offen bzw. lokal abgeschlossen) in der affinen (bzw. quasi-affinen) Varietät X', also selbst eine (quasi-) affine Varietät.

Bemerkung. Zum Beweis der Behauptung des Satzes bleibt noch zu zeigen, daß sich die im zweiten Schritt gefundene Stratifikation zu einer guten Stratifikation verfeinern läßt, deren Teile affin und irreduzibel sind. Dazu beweisen wir zunächst eine Variante des Satzes 4.8 des vierten Anhangs von der Verfeinerung einer Stratifikation eines noetherschen Raums zu einer guten Stratifikation. Der Beweis dieser Variante ist fast derselbe wie der des zitierten Satzes.

4. Schritt. Sei V eine Varietät (vgl. die Definitionen 1.6.9 und 1.6.1). Dann kann jede endliche Partition von V zu einer endlichen guten Stratifikation verfeinert werden, deren Teile irreduzible affine Varietäten sind.

Sei

$$V = \vee_{i \in I} V_i$$

eine endliche Partition. Wir fixieren eine irreduzible Komponente Z von V. Wegen

$$V = \bigcup_{i \in I} \overline{V}_i$$

gilt

$$Z = \bigcup_{i\in I} Z \cap \overline{V}_i.$$

Rechts steht eine endliche Vereinigung abgeschlossener Teilmengen von V. Weil Z irreduzibel ist, gibt es ein i mit $Z = Z \cap \overline{V}_i$, also

$$Z \subseteq \overline{V}_i .$$

Weil V_i lokal abgeschlossen ist, ist V_i offen in $\overline{V}_i$, also

$$Z \cap V_i \text{ offen in } Z \cap \overline{V}_i = Z.$$

Indem wir von V die von Z verschiedenen Komponenten von V abziehen, erhalten wir eine nicht-leere offene Teilmenge Z' von V, welche ganz in Z liegt. Der Durchschnitt

$$Z' \cap Z \cap V_i \text{ ist offen in } Z', \text{ also offen in } V.$$

Damit enthält $Z \cap V_i$ eine offene Teilmenge von V, sagen wir

$$U \text{ offen in } V \text{ und } U \subseteq Z \cap V_i.$$

Als offene Menge ist U Vereinigung affiner offener Mengen. Wir können U so verkleinern, daß U selbst eine affine offene Menge ist. Als offene Teilmenge der irreduziblen Varietät ist U selbst irreduzibel:

> U ist affine offene und irreduzible Teilmenge von V
> (also eine irreduzible affine Varietät).

Wir betrachten die folgende Partition von V_i ,

$$V_i = U \vee V_i^1 \vee V_i^2$$

mit

$$V_i^1 := (V_i - U) \cap \overline{U}$$

$$V_i^2 := ((V_i - U) \cap (V - \overline{U}).$$

zusammen mit der folgenden Partition von V_i, für jedes $i' \neq i$,

$$V_{i'} = V_{i'}^1 \vee V_{i'}^2$$

mit

$$V_{i'}^1 := V_{i'} \cap \overline{U}$$

$$V_{i'}^2 := V_{i'} \cap (V - \overline{U}).$$

Weil die V_i eine Partition von V bilden, bilden V_i^1 und V_i^2 zusammen mit den $V_{i'}^1$, , $V_{i'}^2$ eine Partition von

$$V - U = \vee V_\ell^k. \qquad (1)$$

Die Menge V-U ist abgeschlossen in V und echt kleiner als V. Wir wenden noethersche Induktion an und erhalten eine endliche gute Stratifikation

$$V - U = \vee_{\alpha\in A} T_\alpha$$

welche die Partition (1) verfeinert und deren Teile irreduzible affine Varietäten sind.

Nach Konstruktion bilden U und V_i^1 zusammen mit den $V_{i'}^1$, eine Partion von $\overline{U}$,

$$\overline{U} = U \vee V_i^1 \vee_{i', \neq i} V_{i'}^1 . \qquad (2)$$

Damit ist

$$V = U \vee \vee_{\alpha \in A} T_\alpha$$

eine gute Stratifikation[21] von V aus irreduziblen affinen Varietäten, welche die vorgegebene Partition mit den V_i als Teilen verfeinert.

5. Schritt. Beweis des Satzes.
Nach dem vierten Schritt gibt es eine Verfeinerung der im zweiten Schritt konstruierten (nicht-notwendig guten) Stratifikation

$$V = \bigvee_{i=0}^{N} V_i ,$$

welche eine gute Stratifikation aus irreduziblen affinen Varietäten ist. Dabei können wir auf Grund der Existenz der Isomomorphismen

$$\phi_i : V'_i \times k^* \longrightarrow V_i \text{ mit } \phi_i(x, t^{d_i} \bullet u) = t \bullet \phi_i(x, u) \text{ für } x \in V'_i,\ t, u \in k^*$$

die Konstruktion der Menge U im vierten Schritt noch etwas modifizieren.

Es reicht zu zeigen, daß man durch diese Modifikation zusätzlich zur Affinität und Irreduzibilität auch die $\mathbf{G}_m$-Stabilität von U erreichen kann. Weil die Vereinigung, der Durchschnitt, die Differenz und die Abschließung $\mathbf{G}_m$-stabiler Mengen $\mathbf{G}_m$-stabil ist, führen dann die Konstruktionen des vierten Schritts zu einer guten Stratifikation von V in affine, irreduzible und $\mathbf{G}_m$-stabile Teilmengen. Auf diese Weise erhält man also die gesuchte Stratifikation.

Sei

$$Z \text{ irreduzible Komponente von } V.$$

Aus

$$V = \bigcup_{i=0}^{N} \overline{V}_i$$

erhalten wir eine Darstellung von Z als Vereinigung abgeschlossener Teilmengen,

$$Z = \bigcup_{i=0}^{N} \overline{V}_i \bigcap Z.$$

Weil Z irreduzibel ist, gibt es ein i mit $Z = \overline{V}_i \bigcap Z$, also

$$Z \subseteq \overline{V}_i .$$

Wir zerlegen V'_i in irreduzible Komponenten, sagen wir

$$V'_i = W_1 \bigcup \ldots \bigcup W_n .$$

Weil $k^* = \mathbf{G}_m$ irrreduzibel ist, erhalten wir eine Darstellung des Produkts

$$V'_i \times k^* = W_1 \times k^* \bigcup \ldots \bigcup W_n \times k^*$$

als Vereinigung abgeschlossener[22] irrreduzibler Teilvarietäten. Nach 1.2.4 (ii) sind alle irreduziblen Komponenten von $V'_i \times k^*$ von der Gestalt $W_J \times k^*$. Da man kein $W_J \times k^*$ in

---

[21] Die definierende Bedingung an eine gute Partition ist für jedes T_α erfüllt (nach Wahl der T_α) und sie ist es auch für U (nach (2)).

der Darstellung weglassen kann (denn dann könnte man ein W_j in der Darstellung von V'_i weglassen), sind die

$$W_j \times k^*$$

gerade die irreduziblen Kompoenten von $V'_i \times k^*$. Weil ϕ_i ein Isomorphismus ist, sind die

$$\phi_i(W_j \times k^*) \tag{3}$$

die irreduziblen Komponenten von V_i.. Die Abschließungen der Mengen (3) sind die irreduziblen Komponenten von $\overline{V}_i$ (nach 1.2.9). Weil Z irreduzibel ist, gibt es ein j mit

$$Z \subseteq \overline{\phi_i(W_j \times k^*)}.$$

Weil Z als Komponente von V eine maximale irreduzible Teilmenge von V ist, folgt

$$Z = \overline{\phi_i(W_j \times k^*)}.$$

Weil die Menge $\phi_i(W_j \times k^*)$ stabil ist bezüglich der Operation von $\mathbf{G}_m$ gilt dasselbe für die Abschließung dieser Menge (weil $\mathbf{G}_m$ durch Isomorphismen algebraischer Varietäten also durch Homömorphismen operiert). Wir haben damit gezeigt:

Jede irreduzible Komponente von V ist $\mathbf{G}_m$-stabil.

Als Komponente von V_i ist die Menge (3) abgeschlossen in V_i , also lokal abgeschlossen in V, also ist

$$\phi_i(W_j \times k^*) \text{ offen in } \overline{\phi_i(W_j \times k^*)} = Z.$$

Wir ziehen von $\phi_i(W_j \times k^*)$ die von Z verschiedenen Komponenten von V ab und erhalten eine in V offene Teilmenge U. Als Differenz von $\mathbf{G}_m$-stabilen Mengen ist diese offene Teilmenge ebenfalls $\mathbf{G}_m$-stabil,

$$U \text{ offen in V und } \mathbf{G}_m\text{-stabil, } U \subseteq \phi_i(W_j \times k^*).$$

Weil U eine $\mathbf{G}_m$-stabile Teilmenge ist, hat sie die Gestalt

$$U = \phi_i(U' \times k^*).$$

(nach dem dritten Schritt).Dabei ist U' das vollständige Urbild von U bei der Abbildung

$$V'_i \xrightarrow{\cong} V'_i \times \{1\} \hookrightarrow V'_i \times k^* \xrightarrow{\phi_i} V_i \text{ , } x \mapsto \phi_i(x, 1)$$

(nach dem dritten Schritt). Insbesondere ist U' offen. Als offene Teilmenge von V'_i enthält U' eine affine offene Teilmenge. Wir können U' durch diese kleinere Menge ersetzen. Dadurch wird U durch eine Menge ersetzt die affin, offen und $\mathbf{G}_m$-stabil ist. Als offene Teilmenge einer offenen Teilmenge von V ist diese kleinere Menge weiterhin offen in V. Als offene Teilmenge der irreduziblen Menge Z ist sie irreduzibel.
QED.

---

[22] $W_i \times k^*$ ist als vollständiges Urbild von W_i bei der natürlichen Projektion $V'_i \times k^* \longrightarrow V'_i$ abgeschlossen.

3.2.16 Aufgabe 4

In der Situation von Beispiel 3.2.5 sei λ: $\mathbf{G}_m \longrightarrow G$ ein Kocharakter von $G := \mathbf{GL}(V)$ und a unverändert die zugehörige Operation

$$a: \mathbf{G}_m \times G, (t, x) \mapsto t \bullet x = \lambda(t) \bullet x \bullet \lambda(t)^{-1}.$$

Die abgeschlossenen Untergruppen

$$P(\lambda) := \{x \in G \mid \lim_{t \to 0} t \bullet x \text{ existiert } \}.$$

lassen sich dann wie folgt beschreiben. Es gibt eine Fahne von V, d.h. eine echt absteigende Kette von Unterräumen

$$V = V_0 \supset V_1 \supset \ldots$$

von V derart, daß $P(\lambda)$ die Gruppe der umkehrbaren Automorphismen von V ist, welche jedes V_i in sich abbildet. Hinweis: man betrachte den Falls $G = \mathbf{GL}_n$ und $\lambda(a) = \mathrm{diag}(a^{h_1},\ldots, a^{h_n})$ mit $h_1 \geq h_2 \geq \ldots \geq h_n$.

Beweis. 1. Schritt. Der Spezialfall

$$G = \mathbf{GL}_n,$$

$$\lambda(a) = \mathrm{diag}(a^{h_1},\ldots, a^{h_n})$$

mit $h_1 \geq h_2 \geq \ldots \geq h_n$.

Für $A = (a_{ij})$ gilt

$$\begin{aligned} t \bullet A &:= \lambda(t) \bullet A \bullet \lambda(t)^{-1} \\ &= \mathrm{diag}(t^{h_1},\ldots, t^{h_n}) \bullet (a_{ij}) \bullet \mathrm{diag}(t^{-h_1},\ldots, t^{-h_n}) \\ &= (t^{h_i} \bullet a_{ij} \bullet t^{-h_j}) \\ &= (t^{h_i - h_j} \bullet a_{ij}) \end{aligned}$$

Damit gilt

$$\begin{aligned} A \in P(\lambda) &\Leftrightarrow \lim_{t \to 0} \lambda(t) \bullet A \\ &\Leftrightarrow \lim_{t \to 0} (t^{h_i - h_j} \bullet a_{ij}) \text{ existiert} \\ &\Leftrightarrow a_{ij} = 0 \text{ für } h_i - h_j < 0 \\ &\Leftrightarrow a_{ij} = 0 \text{ für } h_i < h_j . \end{aligned}$$

Wir wählen $r_1,\ldots,r_s$ derart, daß gilt $r_1 + \ldots + r_s = n$ und

$$(h_{r_1+\ldots+r_{\nu-1}} >) \; h_{r_1+\ldots+r_{\nu-1}+1} = \ldots = h_{r_1+\ldots+r_\nu}$$

für $\nu = 1,\ldots,s$. Die Bedingungen an die a_{ij} bedeuten dann, daß A in Blöcke zerfällt,

$$A = \begin{pmatrix} A_{11} & A_{12} & \ldots & A_{1s} \\ 0 & A_{22} & \ldots & A_{2s} \\ \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & \ldots & A_{ss} \end{pmatrix},$$

wobei A_{ij} eine $r_i \times r_j$-Matrix mit Einträgen aus k bezeichne. Wir betrachten die folgenden von den Standart-Einheitsvektoren e_i erzeugten k-linearen Unterräume des k^n.

$$V_i = k \bullet e_1 + ... + k \bullet e_{r_1 + ... + r_i}.$$

Die Bedingungen an die a_{ij} bedeuten dann, es gilt

$$A(V_i) \subseteq V_i \text{ für } i = 1,...,s.$$

Für eine Matrix $A \in \mathbf{GL}_n$ gilt dann

$$A \in P(\lambda) \Leftrightarrow \text{die Fahne } V = V_s \supset V_{s-1} \supset ... \supset V_0 = 0 \text{ ist A-stabil.}$$

2. Schritt. Der allgemeine Fall.

Wir fixieren eine Basis von V um V mit dem k^n und G mit einer abgeschlossenen Untergruppe von $\mathbf{GL}_n$ zu identifizieren (vgl. 2.3.7). Die Gruppe $\mathbf{G}_m$ ist kommutativ und besteht aus halbeinfachen Elementen. Dasselbe gilt damit auch für das Bild $\lambda(\mathbf{G}_m)$ in $\mathbf{GL}_n$ (2.4.8(ii)). Nach 2.4.2 gibt es eine umkehrbare Matrix $S \in \mathbf{GL}_n$ mit

$$S \bullet \lambda(G_m) \bullet S^{-1} \subseteq \mathbf{D}_n,$$

d.h.

$$(\sigma_S \circ \lambda)(t) = S \bullet \lambda(t) \bullet S^{-1} = \text{diag}(a^{h_1}, ..., a^{h_n}) \text{ für } t \in \mathbf{G}_m.$$

Durch geeignetes Permutieren der Koordinaten erreichen wir

$$h_1 \geq h_2 \geq ... \geq h_n.$$

Es gilt

$$\begin{aligned} A \in P(\lambda) \quad &\Leftrightarrow \lim_{t \to 0} \lambda(t) \bullet A \text{ existiert} \\ &\Leftrightarrow \lim_{t \to 0} S \bullet \lambda(t) \bullet A \bullet S^{-1} \text{ existiert (S ist umkehrbare Matrix)} \\ &\Leftrightarrow \lim_{t \to 0} S \bullet \lambda(t) \bullet S^{-1} \bullet (S \bullet A \bullet S^{-1}) \text{ existiert} \end{aligned}$$

Weil die Zusammensetzung von λ mit der Konjugation bezüglich S die Gestalt des Kocharakters im ersten Schritt hat, erhalten wir

$$\begin{aligned} &A \in P(\lambda) \Leftrightarrow \text{die Fahne } V = V_s \supset V_{s-1} \supset ... \supset V_0 = 0 \text{ ist } S \bullet A \bullet S^{-1}\text{-stabil} \\ &\Leftrightarrow S \bullet A \bullet S^{-1}(V_i) \subseteq V_i \text{ für } i = 0,...,s \\ &\Leftrightarrow A \bullet S^{-1}(V_i) \subseteq A \bullet S^{-1}(V_i) \text{ für } i=0,...,s \\ &\Leftrightarrow V = S^{-1}(V_s) \supset S^{-1}(V_{s-1}) \supset ... \supset S^{-1}(V_0) = 0 \text{ ist A-stabil} \end{aligned}$$

QED.

3.2.16 Aufgabe 5

Eine affine Einbettung eines Torus T ist ein irreduzibler affiner T-Raum V, welcher T als offene Teilvarientät enthält,

$$T \hookrightarrow V \text{ (offene Einbettung),}$$

wobei die Operation

$$T \times V \longrightarrow V$$

die Produkt-Abbildung

$$T \times T \longrightarrow T$$

fortsetzt. In dieser Situation heißt V toroidale Varietät (toric varietiy).

(i) Es gibt eine endlich erzeugte Unterhalbgruppe S von X := X*(T), welche X erzeugt und für welche k[V] isomorph ist zur Halbgruppen-Algebra k[S]. Hinweis: man betrachte k[V] als T-stabilen Unterraum des Koordinatenrings k[T] des Torus.

(ii) Für jede Unterhalbgruppe S von X, mit der in (i) beschriebenen Eigenschaft gibt es eine äquivariante Einbettung der toroidalen Varietät V mit $k[V] \cong k[S]$. Diese ist eindeutig bis auf Isomorphie von T-Räumen.

Für weitere Informationen zu toroidalen Varietäten siehe Oda [1].

Bemerkung

Weil k[V] das Einelement enthält, d.h. den trivialen Charakter, sollte es oben Monoid statt von Halbgruppe heißen.

Beweis. Zu (i). Sei

$$i: T \hookrightarrow V$$

eine Torus-Einbettung. Weil V irreduzibel ist und T offen in V, ist T eine dichte Teilmenge von V. Deshalt induziert die Einbettung einen injektiven k-Algebra-Homomorphismus

$$i^*: k[V] \hookrightarrow k[T].$$

Nach Definition besteht ein kommutative Diagramm

$$\begin{array}{ccc} T\times T & \overset{1\times i}{\hookrightarrow} & T\times V \\ \mu\downarrow & & \downarrow a \\ T & \overset{i}{\hookrightarrow} & V \end{array} \qquad (1)$$

mit μ als der Multiplikation des Torus und a der Operation von T auf V. Die Operation von T auf k[V] definiert auf k[V] eine graduierte Struktur

$$k[V] = \oplus_{\chi\in X^*(T)} k[V]_\chi \qquad (2)$$

mit

$$k[V]_\chi := \{ f\in k[V] \mid s(t)\bullet f = \chi(t)\bullet f \text{ für jedes } t \in t\}$$

(vgl. 3.2.13).

Speziell für V = T erhält man die analoge Zerlegung von

$$k[T] = \oplus_{\chi\in X^*(T)} k[T]_\chi \qquad (3)$$

Die Operation von T auf k[T], welche von der Operation von T auf sich selbst durch Multiplikation kommt, ist gegeben ist durch

$$T \longrightarrow GL(k[T]),\ t \mapsto s(t),$$

mit

$$(s(t)f)(x) = f(\mu(t^{-1},x)) = f(t^{-1}x) \text{ für } t,x \in T \text{ und } f \in k[T].$$

ist f ein Charakter, $f = \chi\in X^*(T)$, so gilt

$$(s(t)\chi)(x) = \chi(t^{-1}x) = \chi(t)^{-1}\bullet\chi(x),$$

d.h.

$$s(t)\chi = \chi(t)^{-1}\bullet\chi.$$

Insbesondere gilt

$$k\bullet\chi \subseteq k[T]_{-\chi}$$

Nach 3.2.3(ii) bilden die Charaktere von T eine k-Vektorraumbasis von k[T],

$$k[T] = \oplus_{\chi\in X^*(T)} k\bullet\chi.$$

Vergleich mit (3) zeigt,

$$k[T]_{-\chi} = k\bullet\chi \text{ für jedes } \chi\in X^*(T).$$

Wenn wir k[V] mit seinem Bild bei i* in k[T] identifizieren, so erhalten wir wegen der Kommutativität des Diagramms (1),

$$k[V]_{-\chi} = k[T]_{-\chi} \bigcap k[V] = k\bullet\chi \bigcap k[V]$$

(auf Grund der Definition von $k[V]_{\chi}$ und $k[T]_{\chi}$). Insbesondere ist $k[V]_{-\chi}$ eindimensional oder gleich 0. Genauer:

$$k[V]_{-\chi} = \begin{cases} k\bullet\chi \text{ falls } \chi\in k[V] \\ 0 \quad \text{sonst} \end{cases}$$

Sei

$$S := \{\chi\in X^*(T) \mid \chi\in k[V]\}.$$

Weil k[V] eine k-Algebra ist (und insbesondere den trivialen Charakter $1\in k[V]$ enthält), gilt

$$\chi', \chi'' \in S \Rightarrow \chi'+\chi''\in S \text{ und } 0 \in S,$$

d.h. S ist ein Monoid. Nach Konstruktion ist

$$k[V] = \oplus_{\chi\in S} k[V]_{-\chi} = \oplus_{\chi\in S} k\bullet\chi.$$

Insbesondere ist S eine k-Vektorraumbasis von k[V] und die Addition in S entspricht der Multiplikation von k[V], d.h. der Koordinatenring von V ist gerade

$$k[V] = k[S]$$

die Halbgruppen-Algebra von S. Weil k[V] endlich erzeugt ist, ist S als Monoid endlich erzeugt. Weil T offen ist in V, haben T und V denselben rationalen Funktionenkörper,

$$k(V) = k(T).$$

Insbesondere liegt jeder Charakter von T in k(V), d.h. für jedes $\chi\in X^*(T)$ gibt es reguläre Funktionen

$$f = c_1\bullet\chi_1+...+c_r\bullet\chi_r \text{ und } g = d_1\bullet\chi_1+...+d_r\bullet\chi_r \text{ mit } \chi_i \in S, c_i,d_i \text{ mit}$$

$$\chi = \frac{f}{g},$$

d.h.

$$g\bullet\chi = f.$$

Wegen der k-linearen Unabhängigkeit der Charaktere gilt $\chi_i\bullet\chi\in\{\chi_1,...,\chi_r\}$ für jedes i mit $c_i \neq 0$. Damit hat χ die Gestalt χ_i/χ_j, d.h. χ liegt in der von S erzeugten Gruppe.

Da dies für jedes $\chi \in X^*(T)$ gilt, ist

$$X^*(T) = < S >$$

die von S erzeute Gruppe.

Zu (ii). Weil die Charaktere von T eine k-Vektorraumbasis von k[T] bilden (nach 3.2.3(ii)) bilden ist

k[S] eine Teilalgebra von k[T].

Weil S endlich erzeugt ist, ist k[S] eine endlich erzeugte k-Algebra. Als Teilalgebra von k[T] ist k[S] reduziert, also von der Gestalt

$$k[S] = k[V]$$

mit einer affinen algebraischen Varietät.

Nach Voraussetzung wird X*(T) von S erzeugt, d.h.

$$X^*(T) = \{a\text{-}b \mid a,b \in S\}.$$

Außerdem soll S endlich erzeugt sein, sagen wir von $a_1,..., a_n \in S$. Mit

$$\chi = a_1,..., a_n$$

kann man dann jedes Element von X*(T) in der Gestalt

$$a - n\bullet\chi$$

schreiben mit $a \in S$ und n eine natürliche Zahl. Deshalb gilt

$$\begin{aligned} k[T] &= k[X^*(T)] && \text{(Gruppen-Algebra)} \\ &= k[S]_\chi && \text{(Quotientenring bzgl. der Potenzen von } \chi) \\ &= k[V]_\chi, \end{aligned}$$

d.h. T läßt sich mit der offenen Hauptmenge $D(\chi)$ von V identifizieren. Deshalb definiert die natürliche Einbettung

$$k[S] \hookrightarrow k[T]$$

der Koordinatenringe eine reguläre Abbildung

$$T \longrightarrow S,$$

welche T mit einer offenen Hauptmenge identifiziert.

Weil k[V] = k[S] als k-Vektorraum von den Charakteren von $S \subseteq X^*(T)$ erzeugt wird und weil die Operation von T auf sich selbst durch Multiplikation

$$\mu: T\times T \longrightarrow T,\ (x,y) \mapsto x\bullet y,$$

auf

$$k[T] = \oplus_{\chi\in X^*(T)}\, k\bullet\chi$$

eine Operation induziert, bei welcher die 1-dimensionalen Unterräume $k\bullet\chi$ stabil sind, ist auch k[S] = k[V] als direkte Summe solcher $k\bullet\chi$ stabil, d.h. für die durch μ induzierte Operation

$$s: T \longrightarrow \mathbf{GL}(k[T])$$

gilt $s(t)(k[V]) \subseteq k[V]$, also

$$\mu^*(k[V]) \subseteq k[T]\otimes k[V]$$

(vgl. 2.3.6 (ii))[23]. Damit besteht ein kommutatives Diagramm von k-Algebra-Homomorphismen

$$\begin{array}{ccc} k[T]\otimes k[T] & \overset{1\otimes i^*}{\longleftarrow} & k[T]\otimes k[V] \\ \mu^*\uparrow & & \uparrow a^* \\ k[T] & \overset{i^*}{\longleftarrow} & k[V] \end{array}$$

[23] Das für endlich-dimensionale k-linere Unterräume von k[T] bewiesene Kriterium funktioniert auch für unendliche Dimensionen.

Dabei bezeichnet i* die natürliche Einbettung des Unterraum k[V] in k[T] und a* die Einschränkung von μ^* auf k[V]. Wir gehen zu den induzierten Abbildungen affiner algebraischer Varietäten über und erhalten ein kommutatives Diagramm

$$\begin{array}{ccc} T\times T & \overset{1\times i}{\hookrightarrow} & T\times V \\ \mu\downarrow & & \downarrow a \\ T & \overset{i}{\hookrightarrow} & V \end{array} \qquad (4)$$

von regulären Abbildung. Damit ist a die Fortsetzung der Operation von T auf sich durch Multiplikation auf a. Weil die offene Menge T von V in der irreduziblen Varietät V dicht liegt, ist die Fortsetzung a von μ durch μ eindeutig bestimmt und ebenfalls eine Operation.
Wegen $k[V] \cong k[S]$ ist V bis auf Isomorphie eindeutig bestimmt. Wegen der Kommutativität von (4) und weil T dicht liegt in V, ist a durch μ und i eindeutig festgelegt.
QED.

3.3 Additive Funktionen

In 3.1 wurde bewiesen, daß jede kommutative lineare algebraische Gruppe G die Gestalt

$$G = G_s \times G_u$$

hat mit einer diagonalisierbaren abelschen Gruppe G_s und einer unipotenten abelschen Gruppe G_u. In 3.2 haben wir einen vollständigen Überblick gewonnen über alle diagonlisierbaren linearen algebraischen Gruppen: zu jeder vorgebenen endlich erzeugten abelschen Gruppe X (die im Fall einer positiven Charakteristik p des Grundkörper keine p-Torsion haben darf) gibt es bis auf Isomorphie genau eine abelsche unipotente Gruppe mit der Charaktergruppe X.

Eine ähnlich vollständige Übersicht gibt es auch im unipotenten Fall. Allerdings muß man dann anstelle der von uns betrachteten linearen algebraischen Gruppen affine Gruppen-Schemata zulassen, d.h. algebraische Gruppen, deren Strukturgarben nilpotente Elemente besitzen dürfen. Die unipotenten abelschen Gruppen-Schemata entsprechen dann den Moduln endlicher Länge über dem Dieudonné-Ring. Dies ist ein nicht-kommutativer Ring, der den Witt-Ring des (algebraisch abgeschlossenen) Grundkörpers enthält und von zwei Elementen erzeugt wird. Leider ist diese Theorie jenseits der Möglichkeiten dieser Vorlesung. Außerdem würde uns die Theorie von unserem eigentlichen Ziel, der Klassifikation der halbeinfachen und der reduktiven linearen algebraischen Gruppen mit Hilfe von Wurzelsystemen, entfernen.

Wir beschränken uns deshalb auf einen Kompromis, nämlich auf die Klassifikation der elementaren unipotenten Gruppen. Die Klassifikation ist in der Charakteristik 0 vollständig und ignoriert einige Fälle bei positiver Charakteristik. Trotzdem ist die Behandlung des unipotenten Falls aufwendiger als die des diagonalisierbaren. Wir beginnen deshalb mit einem separaten Abschnitt, der sich ausschließlich mit den additiven Funktionen beschäftigt, die im unipotenten Fall ähnlich bedeutsam sind, wie die Charaktere im diagonlisierbaren Fall.

Auch im nachfolgenden Abschnitt, der sich mit den elementaren unipotenten Gruppen beschäftigt, wird es die meiste Zeit um die additiven Funktionen gehen. Eine Anwendung ist die Klassifikation der elementaren unipotenten Gruppen. Als eine Folgerung erhalten wir eine vollständige Übersicht über die zusammenhängenden linearen algebraischen Gruppen der Dimension 1. Letztere ist das eigentliche Ziel dieses

Kapitels. Alle anderen Ergebnisse finden sich hier hauptsächlich deshalb, weil sie sich ohne großen zusätzlichen Aufwand beweisen lassen.

3.3.1 Defintionen, Bezeichnungen und Konstruktionen

3.3.1A Begriff der additiven Funktion

Eine additive Funktion auf einer linearen algebraischen Gruppe G ist ein Homomorphismus von algebraischen Gruppen

$$f: G \longrightarrow \mathbf{G}_a.$$

Bemerkungen

(i) Die additiven Funktionen auf G bilden (als Funktionen mit Werten in $\mathbf{G}_a = k$) einen k-linearen Unterraum

$$\mathcal{A} = \mathcal{A}(G)$$

des Koordinaten-Rings k[G].

(ii) Ist $F \subseteq k$ ein Teilkörper des Grundkörpers k und G eine F-Gruppe, so bezeichne

$$\mathcal{A}(F) = \mathcal{A}(G)[F] \qquad (\subseteq \mathcal{A}(G))$$

die Menge der über F definierten additiven Funktionen auf G. Dies ist ein linearer Unterraum des F-Vektorraums F[G]. Für jedes $f \in F[G]$ sind die folgenden Aussagen äquivalent.

(a) $f \in \mathcal{A}(G)(F)$.

(b) $\Delta f = f\otimes 1 + 1\otimes f$.

Dabei bezeichne Δ die Komultiplikation von G.

(iii) Ist G eine F-Gruppe, so ist $\mathcal{A}(G)(F)$ eine F-Struktur von $\mathcal{A}(G)$, d.h. die natürliche Einbettung

$$\mathcal{A}(G)(F) \hookrightarrow \mathcal{A}(G)$$

induziert einen linearen Isomorphismus von k-Vektorräumen

$$k\otimes_F \mathcal{A}(G)(F) \xrightarrow{\cong} \mathcal{A}(G)$$

(iv) Ist die Charakteristik p des Grundkörpers k von Null verschieden,

$$p > 0,$$

so ist die p-te Potenz einer addiven Funktion erneut eine additive Funktion auf G. Diese Tatsache ist der Grund für die Einführung eines Rings, über welchem der Vektorraum $\mathcal{A}$ ein Modul ist.

(v) Seien G_1 und G_2 zwei lineare algebraische Gruppen und

$$q_1: G_1 \longrightarrow G_1\times G_2,\ x \mapsto (x,e_2),$$

$$q_2: G_2 \longrightarrow G_1\times G_2,\ y \mapsto (e_1, y),$$

die eindeutig bestimmten regulären Abbildungen mit

$$p_i\circ q_j = \begin{cases} \text{id für } i=j \\ e_i \text{ sonst} \end{cases}$$

wobei $p_i: G_1\times G_2 \longrightarrow G_i$ die Projektion auf den i-ten Faktor und e_i das neutrale Element von G_i bzw. die konstante reguläre Funktion mit dem einzigen Wert e_i bezeichne. Dann ist die Abbildung

$$\varphi:\mathcal{A}(G_1\times G_2) \longrightarrow \mathcal{A}(G_1) \oplus \mathcal{A}(G_2),\ f \mapsto (f\circ q_1, f\circ q_2)$$

ein wohldefinierter k-linearer Isomorphismus mit der Umkehrung

$$\psi\colon \mathcal{A}(G_1) \oplus \mathcal{A}(G_2) \longrightarrow \mathcal{A}(G_1 \times G_2),\ (f, g) \mapsto ((x,y) \mapsto f(x) + g(y)).$$

Beweis. Zu (i). Jede additive Fumkton $f\colon G \longrightarrow \mathbf{G}_a$ induziert als reguläre Abbildung einen k-Algebra-Homomorphismus

$$f^*\colon k[T] = k[\mathbf{G}_a] \longrightarrow k[G],\ (\mathbf{G}_a = k \xrightarrow{p} k) \mapsto (G \xrightarrow{p\circ f} k).$$

Dabei bezeichnet T eine einzelne Unbestimmte (vgl. 2.1.4 Beispiel 1). Insbesondere gilt $f^*(T) \in k[G]$. Das Polynom $p = T$ ist als Abbildung $k \longrightarrow k$ gerade die identische Abbildung, d.h. es gilt

$$f^*(T) = T\circ f = Id\circ f = f,$$

Damit ist $f = f^*(T) \in k[G]$ ein Element des Koordinatenrings von G. Wir haben gezeigt, die Menge der additiven Funktionen ist eine Teilmenge der Koordinatenrings,

$$\mathcal{A}(G) \subseteq k[G].$$

Eine Funktion des Koordinatenrings k[G] ist eine reguläre Abbildung

$$f\colon G \longrightarrow k = \mathbf{G}_a.$$

Sie ist genau dann eine additive Funktion, wenn sie ein Gruppen-Homomorphismus ist, d.h. es gilt

$$\mathcal{A}(G) = \{f \in k[G] \mid f(x\bullet y) = f(x) + f(y) \text{ für } x,y \in G\ \}$$

Aus dieser Beschreibung lesen wir ab, $\mathcal{A}(G)$ ist ein k-linearer Unterraum von k[G].
Zu (ii). Nach Definition gilt

$$\mathcal{A}(G)(F) = \mathcal{A}(G) \bigcap F[G].$$

Weil $\mathcal{A}(G)$ nach (i) ein linearer Unterraum des k-Vektorraums k[G] ist, ist der Durchschnitt ein F-linearer Unterraum von F[G]. Sei jetzt

$$f \in F[G]$$

eine über F definierte reguläre Funktion auf G (also insbesondere eine reguläre Abbildung $G \longrightarrow k = G_a$). Dann ist f genau dann eine additive Funktion auf G, wenn das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} G\times G & \xrightarrow{f\times f} & \mathbf{G}_a \times \mathbf{G}_a \\ \mu\downarrow & & \downarrow\mu_a \\ G & \xrightarrow{f} & \mathbf{G}_a \end{array}$$

Dabei sollen die vertikalen Abbildungen die Gruppen-Multiplikation bezeichnen. Die Kommutativität dieses Diagramms ist äquivalent zu der des zugehörigen Diagramms der Koordinatenringe und k-Algebra-Homomorphismen

$$\begin{array}{ccccc} k[G]\otimes_k k[G] & \xleftarrow{f^*\otimes f^*} & k[\mathbf{G}_a]\otimes_k k[\mathbf{G}_a] & = & k[T]\otimes_k k[T] \\ \Delta\uparrow & & \uparrow\Delta_a & & \\ k[G] & \xleftarrow{f^*} & k[\mathbf{G}_a] & = & k[T] \end{array}$$

Die vertikalen Abbildungen sollen dabei die Komultiplikationen von G bzw. $\mathbf{G}_a$ bezeichnen. Die Komulitiplikation von $\mathbf{G}_a$ ist der k-Algebra-Homomorphismus mit

$$\Delta_a(T) = 1\otimes T + T\otimes 1$$

(vgl. 2.1.4 Beispiel 1). Der k-Algebra-Homomorphismus f* ist durch dessen Wert f an der Stelle T gegeben. Die Kommutativität des Diagramm ist äquivalent zu der Bedingung

$$\Delta(f^*(T)) = (f^*\otimes f^*)(\Delta_a(T).$$

d.h. zu

$$\Delta(f^*(T)) = (f^*\otimes f^*)(1\otimes T+T\otimes 1) = 1\otimes f^*(T) + f^*(T)\otimes 1,$$

also zu

$$\Delta(f) = 1\otimes f + f\otimes 1.$$

Wir haben gezeigt, $f \in F[G]$ ist genau dann additiv, wenn $\Delta f = 1\otimes f + f\otimes 1$ gilt, d.h. f liegt genau dann in $\mathcal{A}(G)\bigcap F[G] = \mathcal{A}(G)(F)$, wenn Bedingung (b) erfüllt ist.

Zu (iii). Nach Bemerkung (ii) gilt

$$\mathcal{A}(G) = \{f \in k[G] \mid \Delta(f) = 1\otimes f + f\otimes 1 \}$$
$$= \mathrm{Ker}(\varphi{:}k[G] \longrightarrow k[G]\otimes_k k[G],\ f \mapsto \Delta(f) - 1\otimes f + f\otimes 1 \}$$

Weil G eine F-Gruppe ist, ist $\Delta\colon k[G] \longrightarrow k[G]\otimes_k k[G]$ über F definiert, d.h. von der Gestalt

$$\Delta = k\otimes_F \Delta_F$$

mit einer F-linearen Abbildung

$$\Delta_F\colon F[G] \longrightarrow F[G]\otimes_F F[G].$$

Damit hat φ die Gestalt $k\otimes\varphi_F$ mit der F-linearen Abbildung

$$\varphi_F\colon F[G] \longrightarrow F[G]\otimes_F F[G],\ f \mapsto \Delta_F(f) - 1\otimes f + f\otimes 1.$$

Als exakter Funktor kommutiert $k\otimes_F$ mit Kernen, d.h. es ist

$$\begin{aligned}\mathcal{A}(G) &= \mathrm{Ker}(\phi)\\ &= \mathrm{Ker}(k\otimes_F\varphi_F)\\ &= k\otimes_F\mathrm{Ker}(\varphi_F).\end{aligned}$$

Damit wird $\mathcal{A}(G)$ als k-Vektorraum von Elementen aus

$$\mathrm{Ker}(\varphi_F) \subseteq F[G]$$

erzeugt, d.h. von additiven Funktionen von G, die über F definiert sind, nämlich von Elementen aus

$$\mathrm{Ker}(\varphi_F) \subseteq \mathcal{A}(G)(F)\ (\subseteq F[G])$$

Aus den natürlichen Einbettungen

$$\mathrm{Ker}(\varphi_F) \hookrightarrow \mathcal{A}(G)(F) \hookrightarrow F[G]$$

erhalten wir durch Anwenden des Funktor $k\otimes_F$ die injektiven k-linearen Abbildungen

$$\mathcal{A}(G) = k\otimes_F\mathrm{Ker}(\varphi_F) \hookrightarrow k\otimes_F\mathcal{A}(G)(F) \hookrightarrow k\otimes_F F[G] = k[G].$$

Wegen $\mathcal{A}(G)(F) \subseteq \mathcal{A}(G)$ und weil $\mathcal{A}(G)$ ein k-Vektorraum ist, liegt das Bild des Tensorprodukts $k\otimes_F\mathcal{A}(G)(F)$ bei der rechten Inklusion ganz in $\mathcal{A}(G)$, d.h. wir haben injektive k-lineare Abbildungen

$$\mathcal{A}(G) = k\otimes_F\mathrm{Ker}(\varphi_F) \hookrightarrow k\otimes_F\mathcal{A}(G)(F) \hookrightarrow \mathcal{A}(G).$$

Deren Zusammensetzung die ist identische Abbildung. Die Injektionen sind sogar Bijektionen und die natürliche Einbettung

$$\mathcal{A}(G)(F) \hookrightarrow \mathcal{A}(G)(k)$$

induziert einen Isomorphismus

$$k\otimes_F \mathcal{A}(G)(F) \xrightarrow{\cong} \mathcal{A}(G)(k).$$

Zu (iv). Für $f \in \mathcal{A}(G)$ gilt

$\Delta(f^p) = (\Delta f)^p$ (Δ ist ein k-Algebra-Homomorphismus)
$= (f\otimes 1+1\otimes f)^p$ (nach Bemerkung (ii) mit F = k)
$= (f\otimes 1)^p+(1\otimes f)^p$ (die Charakteristik von k ist $p > 0$)
$= f^p\otimes 1 +1\otimes f^p$ (Definition der Multiplikation in $k[G]\otimes k[G]$)

Nach Bemerkung (ii) ist f^p eine additive Funktion.

Zu (v). 1. Schritt. Die Abbildung φ ist eine korrekt definierte k-lineare Abbildung. Weil die q_i Homomorphismen von linearen algebraischen Gruppen sind, sind für jede additive Funktion

$$f: G_1\times G_2 \longrightarrow \mathbf{G}_a$$

die Zusammensetzungen $f\circ q_i: G_i \longrightarrow \mathbf{G}_a$ additive Funktionen. Damit ist

$$\varphi:\mathcal{A}(G_1\times G_2) \longrightarrow \mathcal{A}(G_1) \oplus \mathcal{A}(G_2),\ f \mapsto (f\circ q_1, f\circ q_2)$$

eine korrekt definiert Abbildung. Für $f, g \in \mathcal{A}(G_1\times G_2)$ und $c,d \in k$ gilt

$\varphi(c\bullet f+d\bullet g) = ((c\bullet f+d\bullet g)\circ q_1, (c\bullet f+d\bullet g)\circ q_2)$
$= (c\bullet f\circ q_1+d\bullet g\circ q_1, c\bullet f\circ q_2+d\bullet g\circ q_2)$
$= c\bullet(f\circ q_1, f\circ q_2) + d\bullet (g\circ q_1, g\circ q_2)$
$= c\bullet\varphi(f) + d\bullet\varphi(g).$

Wir haben gezeigt, die Abbildung φ ist linear.

2. Schritt. Die Abbildung ψ ist wohldefiniert.
Seien

$$f \in \mathcal{A}(G_1)\ (\subseteq k[G_1]) \text{ und } g \in \mathcal{A}(G_2)\ (\subseteq k[G_2]).$$

Wir haben zu zeigen, $\psi(f,g)$ ist eine additive Funktion von $G_1\times G_2$. Nach Definition gilt

$\psi(f,g)(x,y) = f(x) + g(y)$
$= f(p_1(x,y)) + g(p_2(x,y))$
$= (p_1^*(f) + p_1^*(g))(x,y),$

also

$\psi(f,g) = p_1^*(f) + p_1^*(g) \in k[G_1\times G_2],$

d.h. $\psi(f,g)$ ist eine auf $G_1\times G_2$ reguläre Funktion. Weiter gilt für beliebige Punkte $x,x' \in G_1$ und $y,y' \in G_2$:

$\psi(f,g)((x,y)\bullet(x',y')) = \psi(f,g)((xx', yy'))$
$= f(xx') + g(yy')$ (nach Definition von ψ)

$= f(x) + f(x') + g(y) + g(y')$ (f und g sind additive Funktionen).
$= (f(x) + g(y)) + (f(x')+g(y'))$ ($\mathbf{G}_a$ ist eine abelsche Gruppe)
$= \psi(f,g)(x,y) + \psi(f,g)(x', y')$ (nach Definition von ψ)

Wir haben gezeigt, $\psi(f,g)$ ist eine additive Funktion auf $G_1 \times G_2$, d.h. ψ ist korrekt definiert.

3. Schritt. φ und ψ sind zueinander invers.

Für $f \in \mathcal{A}(G_1 \times G_2)$, $x \in G_1$ und $y \in G_2$ gilt

$\psi(\varphi(f))(x,y) = \psi(f \circ q_1, f \circ q_2)(x,y)$ (nach Definition von φ
$= f \circ q_1(x) + f \circ q_2(y)$ (nach Definition von ψ)
$= f(x,e_2) + f(e_1,y)$
$= f(x,e_2) \bullet (e_1,y))$ (f ist additv)
$= f(x,y)$,

also $\psi(\varphi(f)) = f$ für jedes f also

$$\psi \circ \varphi = \mathrm{id}.$$

Weiter gilt für $f \in \mathcal{A}(G_1)$, $g \in \mathcal{A}(G_2)$, $x \in G_1$ und $y \in G_2$:

$\varphi(\psi(f,g)) = (\psi(f,g) \circ q_1, \psi(f,g) \circ q_2)$ (nach Definition von φ).

Dabei ist

$\psi(f,g) \circ q_1(x) = \psi(f,g)(x,e_2)$ (nach Definition von q_1)
$= f(x) + g(e_2)$ (nach Definition von ψ)
$= f(x) + 0$ (g ist additiv)
$= f(x)$.

Da dies für jedes $x \in G_1$ gilt, folgt

$\psi(f,g) \circ q_1 = f$.

Analog ist

$\psi(f,g) \circ q_2(y) = \psi(f,g)(e_1,y)$ (nach Definition von q_2)
$= f(e_1) + g(y)$ (nach Definition von ψ)
$= 0 + g(y)$ (f ist additiv)
$= g(x)$.

für jedes $y \in G_2$, also

$\psi(f,g) \circ q_1 = g$.

Zusammen erhalten wir

$\varphi(\psi(f,g)) = (\psi(f,g) \circ q_1, \psi(f,g) \circ q_2)$
$= (f,g)$

für beliebige $\in \mathcal{A}(G_1)$ und $g \in \mathcal{A}(G_2)$, also

$$\varphi \circ \psi = \mathrm{id}.$$

Wir haben gezeigt, φ und ψ sind zueinander inverse Abbildungen.

QED.

3.3.1 B Konstruktion des Rings R = R(F)

Sei F ein Teilkörper des algebraisch abgeschlossenen Körpers k. Wir nehmen zunächst an, die Charakteristik p des Grundkörpers k ist positiv,

$$p > 0.$$

Wir bezeichnen dann mit ϕ den Isomorphismus

$$\phi: F \xrightarrow{\cong} F^p,\ x \mapsto x^p.$$

Wir definieren einen Ring

$$R = R(F),$$

dessen additive Gruppe die additive Gruppe des Polynomrings

$$F[T]$$

über F in der Unbestimmten T ist. Seine Multiplikation sei definiert durch

$$(\sum_i a_i T^i)\bullet(\sum_j b_j T^j) := \sum_{i,j} a_i \bullet \phi^i(b_j)\bullet T^{i+j}.$$

Ist G eine F-Gruppe, so definieren wir auf dem F-Vektorraum

$$\mathcal{A}(F) = \mathcal{A}(G)(F)$$

der additiven Funktionen von G, welche über F definiert sind (vgl. 3.3.1 A), wie folgt die Struktur eines Moduls über dem Ring R = R(F).

$$(\sum_i a_i \bullet T^i)\bullet f := \sum_i a_i \bullet f^{p^i} \text{ für } f \in \mathcal{A}(F) \text{ und } \sum_i a_i \bullet T^i \in R(F).$$

Im Fall p = 0 setzen wir

$$R = R(F) := F.$$

Bemerkungen

(i) R ist ein assoziativer Ring. Dies gilt auch für den Fall, daß ϕ ein beliebiger Isomorphismus $F \longrightarrow F'$ auf einen Teilkörper F' von F ist. Der Ring ist nicht kommutativ außer im Fall p = 0 und im Fall, daß ϕ die identische Abbildung von F ist. Im Fall $\phi(x) = x^p$ bedeutet dies, F besteht aus genau p Elementen.[24]

(ii) Durch die Multiplikationsvorschrift (1) bekommt $\mathcal{A}(G)(F)$ tatsächlich die Struktur eines R(F)-Moduls.

(iii) Der Teilkörper F von R liegt, im Fall $\phi \neq Id$ nicht im Zentrum von R.

(iv) Die gewöhnliche Grad-Funktion auf dem Polynomring F[T] hat auch bezüglich der neuen Multiplikation die üblichen Eigenschaften. Zum Beispiel ist

$$\deg(p\bullet q) = \deg(p)+\deg(q)$$

und

$$\deg(p+q) \leq \max\{\deg p, \deg q\}$$

für $p, q \in R$, wobei in der Ungleichung das Gleichheitszeichen gilt, falls die Grade der beiden Polynome p und q verschieden sind.

(v) Der Ring R ist nullteilerfrei.

(vi) Sei G eine F-Gruppe und $\mathcal{A}(G)$ ein endlich erzeugter (linker) R(k)-Modul. Dann ist auch $\mathcal{A}(G)(F)$ ein endlich erzeugter (linker) R(F)-Modul.

Beweis der Bemerkungen. Zu (i). Auf Grund der Definition sind nur diejenigen Ring-Axiome zu überprüfen, in welchen die Multiplikation vorkommt. Direkt aus der Definition der Multiplikation liest man ab, daß die Distributivgesetze gelten und die Multiplikation mit 1 die identische Abbildung auf R definiert. Es bleibt also nur das Assoziativgesetz der Multiplikation.

---

[24] Die Gleichung $0 = x^p - x = x\bullet(x^{p-1}-1)$ hat in F genau p Lösungen.

1. Schritt. Es gilt das Assoziativgesetz der Multiplikation.
Für R erhalten wir

$$((\sum_i a_i T^i)\bullet(\sum_j b_j T^j))\bullet(\sum_\ell c_\ell T^\ell) = (\sum_{i,j} a_i\bullet\phi^i(b_j)\bullet T^{i+j}))\bullet(\sum_\ell c_\ell T^\ell))$$

$$= \sum_{i,j,\ell} a_i\bullet\phi^i(b_j)\bullet\phi^{i+j}(c_\ell)\bullet T^{i+j+\ell}$$

$$= \sum_{i,j,\ell} a_i\bullet\phi^i(b_j\bullet\phi^j(c_\ell))\bullet T^{i+j+\ell}$$

$$= (\sum_i a_i T^i)\bullet(\sum_{j,\ell} b_j\bullet\phi^j(c_\ell)\bullet T^{j+\ell})$$

$$= (\sum_i a_i T^i)\bullet((\sum_j b_j T^j))\bullet(\sum_\ell c_\ell T^\ell)).$$

2. Schritt. R ist nicht kommutativ außer im Fall $\phi(x) = x$.
Es gilt

$$T^i\bullet(bT^j) = \phi^i(b)\bullet T^{i+j}) = (\phi^i(b)\bullet T^j)\bullet T^i.$$

Das Kommutativgesetz würde fordern, daß

$$\phi^i(b) = b$$

gilt für jedes $b\in F$ und jedes i, d.h. ϕ müßte die identische Abbildung sein.
Zu (ii). Wir im Fall des Rings R(R) sind nur die Rechengesetze zu überprüfen, in denen die Multiplikation vorkommt (weil $\mathcal{A}(G)(F)$ ein k-Vektorraum ist). Direkt aus der Definition der Multiplikation liest man ab, daß die Distributivgesetze gelten (denn die Muiltiplikation ist bilinear über k) und daß die Multiplikation mit $1 \in R(F)$ auf $\mathcal{A}(G)(F)$ die identische Abbildung definiert. Damit ist der Beweis wieder auf den Beweis des Assoziativitätsgesetzes der Multiplikation reduziert. Die Rechnung für $\mathcal{A}(G)(F)$ ist fast dieselbe wie im Fall des Rings R(F).

$$((\sum_i a_i T^i)\bullet(\sum_j b_j T^j))\bullet f = (\sum_{i,j} a_i\bullet(b_j)^{p^i}\bullet T^{i+j}))\bullet f$$

$$= \sum_{i,j} a_i\bullet(b_j)^{p^i}\bullet f^{p^{i+j}}$$

$$= \sum_i \sum_j a_i\bullet(b_j\bullet f^{p^j})^{p^i}$$

$$= (\sum_i a_i T^i)\bullet(\sum_j b_j\bullet f^{p^j})$$

$$= (\sum_i a_i T^i)\bullet((\sum_j b_j T^j)\bullet f).$$

Zu (iii). Die Aussage ergibt sich aus dem zweiten Schritt im Beweis von (i), wenn man dort $j = 0$ setzt.
Zu (iv). Außer für die Identität

$$\deg(p\bullet q) = \deg(p)+\deg(q)$$

spielt die Wahl der Multiplikation in den Aussagen keine Rolle. Es reicht diese Identität zu beweisen. Für

$$p = \sum_i a_i T^i \text{ und } q = \sum_j b_j T^j$$

gilt nach Definition des Produkts

$$\begin{aligned} p \bullet q &= (\sum_i a_i T^i) \bullet (\sum_j b_j T^j) \\ &= \sum_{i,j} a_i \bullet \phi^i(b_j) \bullet T^{i+j}. \end{aligned}$$

also

$$\begin{aligned} \deg(p \bullet q) &= \max \{i+j \mid a_i \bullet \phi^i(b_j) \neq 0\} \\ &= \max \{i+j \mid a_i \neq 0 \text{ und } \phi^i(b_j) \neq 0\} \\ &= \max \{i+j \mid a_i \neq 0 \text{ und } b_j \neq 0\}. \end{aligned}$$

Dies ist aber gerade der Grad des Produkts im gewöhnlichen Polynomring F[T].

Zu (v). Seien p, q ∈ R(F) von Null verschiedene Elemente. Wir haben zu zeigen, auch das Produkt ist ungleich Null,

$$p \bullet q \neq 0.$$

Sind p und q vom Grad Null, so ist dies der Fall, weil F als Körper nullteilerfrei ist. Ist mindestens einer der Faktoren vom Grad > 0. so ist auch der Grad

$$\deg(p \bullet q) = \deg p + \deg q > 0,$$

also p•q von Null verschieden.

Zu (vi). Nach Voraussetzung gibt es Elemente $f_1,...,f_r \in \mathcal{A}(G)$ mit

$$\mathcal{A}(G) = R(k) \bullet f_1 + ... + R(k) \bullet f_r. \qquad (1)$$

Wegen

$$k \otimes_F \mathcal{A}(G)(F) \xrightarrow{\cong} \mathcal{A}(G)(k)$$

gibt es Elemente $\tilde{f}_1,..., \tilde{f}_s \in \mathcal{A}(G)(F)$ und $c_{ij} \in k$ mit

$$f_i = \sum_{j=1}^{s} c_{ij} \bullet \tilde{f}_j \in \sum_{j=1}^{s} k \bullet \tilde{f}_j$$

für i = 1,...,r. Es folgt

$$\begin{aligned} \mathcal{A}(G) &= \sum_{i=1}^{r} R(k) \bullet f_i && \text{(nach Wahl der } f_i\text{)} \\ &\subseteq \sum_{i=1}^{r} R(k) \bullet \sum_{j=1}^{s} k \bullet \tilde{f}_j && \text{(nach Wahl der } \tilde{f}_j\text{)} \\ &\subseteq \sum_{j=1}^{s} R(k) \bullet k \bullet \tilde{f}_j && \text{(die Multiplikation ist bilinear über k)} \\ &\subseteq \sum_{j=1}^{s} R(k) \bullet \tilde{f}_j && \text{(wegen } R(k) \bullet k \subseteq R(k) \bullet R(k) \subseteq R(k)\text{)} \end{aligned}$$

Damit wird $\mathcal{A}(G)$ als R(k)-Modul von endlich vielen Elementen aus $\mathcal{A}(G)(F)$ erzeugt. Wir können in (1) also annehmen,

$$f_1,...,f_r \in \mathcal{A}(G)(F). \qquad (2)$$

Wegen (1) hat jedes Element $f \in \mathcal{A}(G)$ die Gestalt

$$f = \sum_{i=1}^{r} a_i f_i \text{ mit } a_i \in R(k).$$

Wegen $R(k) = k \otimes_F R(F)$ hat jedes a_i die Gestalt

$$a_i = \sum_{j=1}^{N} d_{ij} \bullet r_{ij} \text{ mit } d_{ij} \in k \text{ und } r_{ij} \in R(F).$$

Damit gilt

$$\begin{aligned} f &= \sum_{i=1}^{r} \sum_{j=1}^{N} d_{ij} \bullet r_{ij} f_i \\ &\in \sum_{i=1}^{r} \sum_{j=1}^{N} d_{ij} \bullet R(F) \bullet f_i \\ &\subseteq \sum_{j=1}^{N} d_{ij} \bullet M \end{aligned}$$

mit

$$M := \sum_{i=1}^{r} R(F) \bullet f_i ,$$

also

$$f \in k \otimes_F M,$$

wenn wir den Modul $k \otimes_F M$ mit dessen Bild bei der Abbildung

$$k \otimes_F M \longrightarrow k \otimes_F \mathcal{A}(G)(F) = \mathcal{A}(G),\ c \otimes m \mapsto c \bullet m,$$

identifizieren. Weil dies für jedes $f \in \mathcal{A}(G)$ gilt, folgt

$$\mathcal{A}(G) \subseteq k \otimes_F M.$$

Wir haben gezeigt, die natürliche Einbettung

$$M \hookrightarrow \mathcal{A}(G)(F) \qquad (3)$$

wird durch den Funktor $k \otimes_F$ in eine bijektive Abbildung

$$k \otimes_F M \longrightarrow k \otimes_F \mathcal{A}(G)(F)$$

überführt.[25] Weil k treuflach über F muß bereits (3) surjektiv sein[26], d.h. es gilt

$$\mathcal{A}(G)(F) = M = \sum_{i=1}^{r} R(F) \bullet f_i .$$

Mit anderen Worten, $\mathcal{A}(G)(F)$ ist ein endlich erzeugter Modul über R(F).
QED.

3.3.2 Lemma: der euklidische Algorithmus für R(F)

Seien F ein Teilkörper des algebraisch abgeschlossenen Körpers k und ein G eine lineare algebraische Gruppe (über k). Die Charakteristik p des Grundkörpers k sei ungleich Null,

---

[25] Unser Argumente zeigen, die Abbildung ist surjektiv. Sie ist injektiv, weil k flach ist über F.
[26] siehe auch Bemerkung 1.3.7 B (iv).

$$p > 0.$$

Weiter seien $a, b \in R = R(F)$ Elemente mit $\deg a > 0$.

(i) Es gibt ein eindeutig bestimmte Elemente $c,d \in R(F)$ mit
$$b = ca + d \text{ und } \deg d < \deg a.$$

(ii) Ist F perfekt (d.h. $F^p = F$), so gibt es eindeutig bestimmte Elemente $c,d \in R(F)$ mit
$$b = ac + d \text{ und } \deg d < \deg a.$$

Beweis. Die Aussagen sind trivial, falls die Charakteristik p des Grundkörpers k gleich Null ist (denn dann ist R(F) = F). Sei also
$$p > 0.$$
Bezeichne
$$\phi: F \longrightarrow F, x \mapsto x^p$$
die in 3.3.1 B eingeführte Abbildung.
Zu (i). Die Eindeutigkeit von c und d.
Seien c, c', d, d' $\in R(F)$ mit
$$b = ca+d = c'a+d' \text{ und } \deg d < \deg a \text{ und } \deg d' < \deg a.$$
Dann gilt
$$ca + d = c'a+d',$$
also
$$(c-c')a = d-d'.$$
Im Fall $c-c' \neq 0$ würde
$$\deg a \leq \deg(c-c') + \deg a = \deg (d-d') < \deg a$$
gelten, was nicht möglich ist. Also gilt
$$c = c'$$
und damit auch
$$d = d'.$$
Existenz von c und d.
Im Fall $\deg b < \deg a$ können wir $c = 0$ und $d = b$ setzen. Betrachten wir den verbleibenden Fall
$$\deg b \geq \deg a. \qquad (1)$$
Als Element von R(F) haben a und b die Gestalt

$$a = \sum_{i=0}^{n} a_i T^i \text{ mit } n = \deg a, a_i \in F$$

und

$$b = \sum_{j=0}^{N} b_j T^j \text{ mit } N = \deg b, b_j \in F.$$

Die Polynom b und

$$T^{N-n} \bullet a = \sum_{i=0}^{n} c_{N-n} \bullet \phi^i(a_i) T^{N-n+i}$$

haben dann denselben Grad. Es gibt also ein $c \in F$ derart, daß b und $c \bullet T^{N-n} \bullet a$ dasselben höchste Glied besitzten, also
$$\deg (b - c \bullet T^{N-n} \bullet a) < \deg b$$
gilt. Falls (1) gilt, können wir also von b ein linksseitiges Vielfaches von a so abziehen, daß sich der Grad verkleinert. Wir können dies solange tun, bis der Grad der Differenz kleiner als deg a wird, d.h. es gibt ein $c \in R(F)$ mit
$$\deg (b - c \bullet a) < \deg a.$$
Mit $d := b - c \bullet a$ gilt dann die Behauptung.

Zu (ii). Die Argumentation ist im wesentlichen dieselbe wie beim Beweis von (i). Beim Exiatenzbeweis müssen wir jedoch a von rechts mit einer Potenz von T bzw. mit einem Element $c \in F$ multiplizieren. Wir erhalten Polynome gleichen Grades

$$b \text{ und } a \bullet T^{N-n} = \sum_{i=0}^{n} a_i T^{N-n+i}$$

und müssen ein $c \in F$ finden, für welches die höchsten Glieder von

$$b \text{ und } a \bullet T^{N-n} \bullet c$$

übereinstimmen, d.h. für welches

$$b_N \bullet T^N \text{ und } a_n \bullet T^N \bullet c = a_n \bullet \phi^N(c) \bullet T^N$$

gleich sind, d.h. ein $c \in F$ mit

$$\phi^N(c) = a_n^{-1} \bullet b_N.$$

Im Fall F perfekt, d.h. $F^p = F$ ist ϕ surjektiv, d.h. es gibt ein solches c.
QED.

3.3.3 Lemma: Zerlegung von R-Moduln in zyklische

Seien F ein Teilkörper des algebraisch abgeschlossenen Körpers k und G eine lineare algebraische Gruppe (über k).

(i) Die linken Ideale von R = R(F) sind Hauptideale. Ist der Körper F perfekt, so gilt dies auch für die rechten Ideale.
(ii) R = R(F) ist links-noethersch. Ist F perfekt, so ist R auch rechts-noethersch.
(iii) Ist F perfekt, so ist jeder endlich erzeugte R-Modul M eine direkte Summe von zyklischen Moduln. Ist M außerdem torsionsfrei, so ist M sogar frei.

Beweis. Die Aussagen sind trivial, falls die Charakteristik p des Grundkörpers k gleich Null ist (denn dann ist R(F) = F). Sei also

$$p > 0.$$

Zu (i). Die Aussagen sind eine Folge des Euklidischen Algorithmus (d.h. von 3.3.2) und werden wie im Fall eines gewöhnlichen Polynomrings über einem Körper bewiesen.
Sei I ein linkes Ideal von R. Wir haben zu zeigen, I ist ein Hauptideal. Dazu können wir annehmen, I ist nicht das Nullideal. Wir wählen in I - {0} Polnom minimalen Grades, sagen wir

$$0 \neq a \in I.$$

Es reicht zu zeigen,

$$I = R \bullet a.$$

Nach Wahl von a gilt "$\supseteq$". Sei $b \in I$. Nach 3.3.2 (i) gibt es Elemente $c, d \in R$ mit

$$b = ca + d \text{ und } \deg d < \deg a.$$

Weil I ein linkes Ideal ist, gilt dann

$$d = ca - b \in I.$$

Wegen $\deg d < \deg a$ und der Wahl von a muß dann $d = 0$ gelten, also $b = ca \in R \bullet a$.
Wir haben gezeigt, daß auch die umgekehrte Inklusion besteht.
Die Aussage zu den rechten Idealen von R wird analog behandelt.
Zu (ii). Die Aussage ist eine Folge von (i).
Zu (iii).[27] Sei R := R(F) oder der zu R(F) entgegengesetzte Ring, d.h. der Ring $R(F)^{op}$ mit der additiven Gruppe R(F), für welchen das Produkt $a \bullet b$ gerade das Produkt $b \bullet a$ in R(F) ist.

---

[27] Für einen Beweis in einem algemeineren Kontext (der nicht die konkrete Gestalt von R benutzt sondern nur die Aussage (ii), siehe Jacobson [4], Kapitel 3, Abschnitt 3.5.

Wir beschränken uns auf die Betrachtung von rechten R-Moduln. Die Behauptung von (iii) für linke R(F)-Moduln ergibt sich dann aus der für $R = R(F)^{op}$ und rechte R-Moduln.

Seien M ein endlich erzeugter (rechter) R-Modul und $m_1, \ldots, m_r$ ein Erzeugendensystem von M. Wir betrachten die R-lineare Surjektion

$$f: R^r \twoheadrightarrow M, \begin{pmatrix} x_1 \\ \cdots \\ x_r \end{pmatrix} \mapsto m_1x_1+\ldots+m_r x_r .$$

Weil R noethersch ist, ist der Kern von f endlich erzeugt. Es gibt also ein endliches Erzeugendensystem $n_1,\ldots,n_s$ von Ker(f) über R und eine R-lineare Surjektion

$$g: R^s \twoheadrightarrow \mathrm{Ker}(f), \begin{pmatrix} y_1 \\ \cdots \\ y_s \end{pmatrix} \mapsto n_1 y_1+\ldots+n_s y_s.$$

Als R-lineare Abbildung $R^s \longrightarrow R^r$ ist g durch eine Matrix gegeben, sagen wir

$$g: R^s \longrightarrow R^r, x \mapsto A\bullet x,$$

mit einer r×s-Matrix

$$A = \begin{pmatrix} a_{11} \cdots a_{1s} \\ \cdots \cdots \cdots \\ a_{r1} \cdots a_{rs} \end{pmatrix}, a_{ij} \in R.$$

Die Behauptung von Aussage (iii) wird sich dadurch ergeben, daß wir die Basen

$$e_1,\ldots, e_r \text{ von } R^r \text{ und } e_1,\ldots, e_s \text{ von } R^s$$

s abändern, daß die Matrix A eine möglichst einfache Gestalt bekommt (wir geben einen Beweis des Elementarteilersatzes in diesem Kontext an). Dazu führen wir zunächst Bezeichnungen $a_1,\ldots,a_s$ und $a^1,\ldots,a^r$ für die Spalten und Zeilen von A ein und schreiben

$$A = (a_1,\ldots,a_s) = \begin{pmatrix} a^1 \\ \cdots \\ a^r \end{pmatrix}$$

Die Abbildungsvorschrift für g bekommt dann die Gestalt

$$g\begin{pmatrix} y_1 \\ \cdots \\ y_s \end{pmatrix} = a_1y_1+\ldots+a_s\bullet y_s.$$

Mit $e_1,\ldots, e_s$ und $\lambda\in R$ ist auch $e_1,\ldots,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},\ldots, e_s$ eine Basis von R^s.[28]

1. Schritt. Die Matrix von g bezüglich der Basis $e_1,\ldots,e_{i-1}, e_i - \lambda\bullet e_j, e_{i+1},\ldots, e_s$ des Urbildmoduls R^s hat die Spalten

[28] Weil sich jeder der Vektoren $e_1,\ldots,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},\ldots, e_s$ als R-Linearkombination von $e_1,\ldots, e_s$ und jeder der Vektoren $e_1,\ldots, e_s$ als R-Linearkombination von $e_1,\ldots,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},\ldots, e_s$ schreiben läßt.

$$a_1,\dots, a_{i-1}, a_i-\lambda\bullet a_j, a_{i+1},\dots,a_s$$

Es gilt

$$\begin{aligned} g(e_\nu) &= A\bullet e_\nu \\ &= a_\nu \\ &= a_{1\nu}\bullet e_1+\dots+a_{r\nu}\bullet e_r \\ &= \sum_{\alpha=1}^{r} a_{\alpha\nu}\bullet e_\alpha \end{aligned}$$

und

$$g(e_i - e_j\bullet\lambda) = \sum_{\alpha=1}^{r} a_{\alpha i}\bullet e_\alpha - \Big(\sum_{\alpha=1}^{r} a_{\alpha j}\bullet e_\alpha\Big)\bullet\lambda \qquad \text{(g ist R-linear)}$$

$$= \sum_{\alpha=1}^{r} a_{\alpha i}\bullet e_\alpha - \Big(\sum_{\alpha=1}^{r} a_{\alpha j}\bullet \lambda\bullet e_\alpha\Big) \qquad (e_\alpha\bullet\lambda = \lambda\bullet e_\alpha, \text{ denn 1 kommutiert mit } \lambda)$$

$$= (a_{1i}- \lambda\bullet e_{1j})\bullet e_1+\dots+(a_{ri}-\lambda\bullet e_{rj})\bullet e_r$$

Die Matrix der Abbildung g bezüglich der neuen Basis des Urbild-Moduls R^s hat somit die Spalten

$$a_1,\dots, a_{i-1}, a_i-\lambda\bullet a_j, a_{i+1},\dots,a_s$$

Mit $e_1,\dots, e_r$ und $\lambda\in R$ ist auch $e_1,\dots,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},\dots, e_r$ eine Basis von R^r.

2. Schritt. Die Matrix von g bezüglich der Basis $e_1,\dots,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},\dots, e_r$ des Bildmoduls R^r hat die Zeilen

$$a^1,\dots, a^{j-1}, a^j+a^i\bullet\lambda, a^{j+1}, \dots , a^r.$$

Es gilt

$$\begin{aligned} g(e_\nu) &= A\bullet e_\nu \\ &= a_\nu \\ &= a_{1\nu}\bullet e_1+\dots+a_{r\nu}\bullet e_r \\ &= a_{1\nu}\bullet e_1+\dots+ a_{i-1\nu}\bullet e_{i-1}, a_{i\nu}(e_i - e_j\bullet\lambda)+a_{i+1\nu} e_{i+1}+\dots+ a_{r\nu}\bullet e_r \\ &\quad + a_{i\nu}\bullet e_j\bullet\lambda \end{aligned}$$

Die neue Linearkombination hat dieselben Koeffizienten wie die alte mit Ausnahme des Koeffizienten des j-ten Vektors. Wegen

$$\begin{aligned} a_{j\nu}\bullet e_j + a_{i\nu}\bullet e_j\bullet\lambda &= a_{j\nu}\bullet e_j + a_{i\nu}\bullet\lambda\bullet e_j \qquad (e_j\bullet\lambda = \lambda\bullet e_j, \text{ denn 1 kommutiert mit } \lambda) \\ &= (a_{j\nu} + a_{i\nu}\bullet\lambda)\bullet e_j \end{aligned}$$

ist der Koeffizient von e_j ist gleich

$$a_{j\nu} + a_{i\nu}\bullet\lambda$$

Die Matrix der Abbildung g bezüglich der neuen Basis von R^r hat somit die Zeilen

$$a^1,\dots, a^{j-1}, a^j+a^i\bullet\lambda, a^{j+1}, \dots , a^r.$$

Zusammenfassung:

Wenn wir in der Matrix A ein R-Vielfaches einer Zeile zu einer anderen Zeile addieren oder ein R-Vielfaches einer Spalte zu einer anderen Spalte addieren, so erhalten wir eine Matrix, welcher weiterhin die Matrix der Abbildung g ist (bezüglich anderer Basen von R^r bzw. R^s)[29]. Außerdem können wir durch Permutieren der Basisvektoren auch die Zeilen oder Spalten der Matrix A beliebig permutieren. Wir wollen die beschriebnen Operationen, mit denen wir die Matrix A so verändern können, daß wir dabei weiterhin Matrizen der Abbildung g erhalten, Elementaroperationen nennen.

3. Schritt. Durch Elementaroperationen kann man die Metrix A so abändern, daß A Diagonalgestalt bekommt.

Betrachten wir einen von 0 verschiedenen Eintrag von A, dessen Grad unter allen von 0 verschiedenen Einträgen seiner Zeile oder Spalte mininal ist. Dann können wir nach mit Hilfe des Euklidischen Algorithmus durch Elementaroperationen errreichten, daß die übrigen Einträge dieser Zeile oder Spalten entweder 0 werden oder einen kleineren Grad bekommen. Da alle Grade ≥ 0 sind, erhalten wir nach endlich vielen Schritten eine Matrix mit Einträgen, deren Grade sich nicht weiter verkleinern lassen (falls die Einträge ungleich 0 sind). Durch Permultieren von Zeilen bzw. Spalten erreichen wir, daß a_{11} unter allen von 0 verschiedenen Einträgen einen minimalen Grad besitzt. Da sich kein Grad weiter verkleinern läßt, sind alle anderen Einträge der ersten Zeile und der ersten Spalte gleich 0.

Indem wir erste Zeile und erste Spalte streichen und das Verfahren mit der verbleibenden Matrix wiederholen, erreichen wir nach endlich vielen Schritten, daß A Diagonalgestalt bekommt.

4. Schriit. Beweis der Behauptung.

Auf Grund des dritten Schritts können wir annehmen, daß A Diagonalgestalt besitzt, sagen wir

$$A = \begin{pmatrix} \lambda_1 & 0 & .. & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}.$$

Die Abbildung g hat dann die Gestalt

$$g: R^s \longrightarrow R^r, \begin{pmatrix} y_1 \\ \dots \\ y_s \end{pmatrix} \mapsto \begin{pmatrix} \lambda_1 \bullet y_1 \\ \dots \\ \lambda_t \bullet y_t \\ \dots \\ \dots \end{pmatrix},$$

wobei im Fall $r \leq s$ und $t = r$ gilt und die beiden unteren punktierten Zeilen fehlen und im Fall $s < r$ gilt $t=s$ und diese punktierten Zeilen stehen für r-s Koordinaten, die gleich 0 sind. Damit ist

$$\mathrm{Ker}(f) = \mathrm{Im}(g) = e_1\lambda_1 \bullet R + ... + e_t\lambda_t \bullet R.$$

Wir können annehmen, alle $\lambda_i \in R$ sind ungleich 0. Es gilt

$$M \cong R^r/\mathrm{Ker}(f) \cong (R/\lambda_1 R) \oplus ... \oplus (R_t/\lambda_t R) \oplus R^{r-t}.$$

Mit anderen Worten, M ist eine direkte Summe von zyklischen R-Moduln. Ist M torsionsfrei, so gilt $t = 0$ und $M \cong \mathbb{R}^r$, d.h. M ist frei.

QED.

---

[29] Dabei müssen wir bei Spalten-Operationen von links und bei Zeilen-Operationen von rechts multiplizieren.

3.3.4 Die Modul-Struktur von $\mathcal{A}(G)(F)$ über R(F)

3.3.4 A Definition

Seien F ein Teilkörper des Grundkörpers k, G eine F-Gruppe (über k) und wie bisher

$$\mathcal{A}(F) = \mathcal{A}(G)(F)$$

der F-Vektorraum der additiven Funktionen von G, welche über F definiert sind. Ist die Charakteristik p des Grundkörpers k ungleich 0,

$$p > 0,$$

so definieren wir auf $\mathcal{A}(F)$ wie folgt die Struktur eines Moduls über dem Ring R = R(F) von 3.3.1 B.

$$(\sum_i a_i \bullet T^i) \bullet f := \sum_i a_i \bullet f^{p^i} \text{ für } f \in \mathcal{A}(F) \text{ und } \sum_i a_i \bullet T^i \in R(F).$$

Im Fall p = 0 ist R = F und $\mathcal{A}(F)$ ist trivialerweise ein R-Modul.

3.3.4 B Beispiel

Sei $G = \mathbf{G}_a^n$. Dann ist $F[G] = F[T_1,...,T_n]$. Eine additive über F definierte Funktion auf G ist dann gegeben durch ein <u>additives Polynom</u> $f \in F[G] = F[T_1,...,T_n]$, d.h. ein Polynom mit

$$f(T_1+U_1,...,T_n+U_n) = f(T_1,...,T_n) + f(U_1,...,U_n). \qquad (1)$$

Dabei sollen die U_i weitere Unbestimmte bezeichnen.

Man beachte, ein Homomorphismus $\phi: G \longrightarrow \mathbf{G}_a$ von linearen algebraischen Gruppen ist eine reguläre Abbildung, für welche das folgende Diagramm kommutativ ist.

$$\begin{array}{ccc} G & \xrightarrow{\phi} & \mathbf{G}_a \\ \mu\uparrow & & \uparrow\mu_a \\ G\times G & \xrightarrow{\phi\times\phi} & \mathbf{G}_a\times\mathbf{G}_a \end{array}$$

Die vertikalen Pfeile sollen dabei die Gruppen-Multiplikation von bezeichnen. Dabei ist ϕ durch das Bild der Unbestimmten T bei

$$\phi^*: k[\mathbf{G}_a] = k[T] \longrightarrow k[G] = k[T_1,...,T_n]$$

gegeben, d.h. durch ein Polynom $f := \phi^*(T) \in k[T_1,...,T_n]$. Die Relationstreue von ϕ ist dann äquivalent zu Kommutativität des Diagramms von k-Algebren

$$\begin{array}{ccccc} k[G] & \xleftarrow{\phi^*} & k[\mathbf{G}_a] & = k[T] & f(T_1,...,T_n) \quad \mapsfrom \quad T \\ \mu^*\downarrow & & \downarrow\mu_a^* & & \downarrow \qquad\qquad \downarrow \\ k[G]\times k[G] & \xleftarrow{\phi^*\otimes\phi^*} & k[\mathbf{G}_a]\otimes k[\mathbf{G}_a] & = k[T,U] & \begin{array}{l} f(T_1+U_1,...,T_n+U_n) \\ \| \\ f(T_1,...,T_n)+f(U_1,...,U_n) \end{array} \mapsfrom T+U \end{array}$$

Die Kommutativität dieses Diagramms ist gerade äquivalent zu (1). Die Forderung, daß ϕ über F definiert sein soll, bedeutet, f soll in $F[G] = F[T_1,...,T_n]$ liegen.

Die Menge der additiven Polynome ist ein linker Modul über R(F): im Fall der Charakteristik p = 0, d.h. R(F) = F, ist das trivial und im Fall p > 0 folgt dies aus der Tatsache, daß die p-te Potenz eines additive1n Polynoms ein additives Polynom ist.

3.3.5 Lemma: die Struktur von $\mathcal{A}(G_a^n)(F)$ als R(F)-Modul

$\mathcal{A}(\mathbf{G}_a^n)(F)$ ist ein freier Modul über dem Ring R(F) mit der Basis $T_1, \ldots, T_n$.

Beweis. Bezeichne wie bisher

$$p = \mathrm{Char}(k)$$

die Charakteristik des Grundkörpers k.

1. Schritt. Im Fall $p \neq 0$ reicht es zu zeigen, daß die Elemente von $\mathcal{A}(\mathbf{G}_a^n)(F)$ gerade die Polynome der Gestalt

$$f = \sum_{j=1}^{n} \sum_{i\geq 0} c_{ij} \cdot T_j^{p^i} \text{ mit } c_{ij} \in F. \qquad (1)$$

sind.

Wegen $T^i \cdot T_j = T_j^{p^i}$ können wir diese Polynome in der Gestalt folgenden Gestalt schreiben.

$$\begin{aligned} f &= \sum_{j=1}^{n} \sum_{i\geq 0} c_{ij} \cdot (T^i \cdot T_j) \\ &= \Big(\sum_{j=1}^{n} \sum_{i\geq 0} c_{ij} \cdot T^i\Big) \cdot T_j \\ &= \sum_{j=1}^{n} r_j \cdot T_j \text{ mit } r_j = \sum_{i\geq 0} c_{ij} \cdot T^i \in R(F), \end{aligned}$$

d.h. $\mathcal{A}(\mathbf{G}_a^n)(F)$ wird über R(F) von den $T_1,\ldots,T_n$ erzeugt. Wir haben noch die lineare Unabhängigkeit der $T_1,\ldots,T_n$ über R zu beweisen. Weil die $T_1,\ldots,T_n$ algebraisch unabhängig über F sind, ist das Polynom (1) genau dann gleich 0, wenn alle $c_{ij} = 0$ sind. Aus

$$\sum_{j=1}^{n} r_j \cdot T_j = 0 \text{ mit } r_j = \sum_{i\geq 0} c_{ij} \cdot T^i \in R(F)$$

folgt somit $c_{ij} = 0$ für alle i und j, also $r_j = 0$ für alle j.

2. Schritt. Im Fall $p \neq 0$ sind die Elemente von $\mathcal{A}(\mathbf{G}_a^n)(F)$ gerade die Polynome der Gestalt (1).

Weil die Charakteristik des Körpers F ungleich 0 ist, gilt

$$(T_j + U_j)^{p^i} = T_j^{p^i} + U_j^{p^i},$$

also

$$f(T_1+U_1,\ldots,T_n+U_n) = f(T_1,\ldots,T_n) + f(U_1,\ldots,U_n), \qquad (2)$$

d.h. die Funktionen der Gestalt (1) sind additiv (vgl. 3.3.4 B). Sei umgekehrt

$$f \in F[\mathbf{G}_a^n] = F[T_1,\ldots,T_n]$$

eine additive Funktion, d.h. es gelte (2). Insbesondere ist dann

$$f(0,\ldots,0) = f(0,\ldots,0) + f(0,\ldots,0),$$

also

$$f(0,\ldots,0) = 0.$$

Das Absolutglied von f ist gleich 0. Wir haben zu zeigen, f hat die Gestalt (1).
Wir führen den Beweis durch Induktion nach dem Grad von f.
Induktionsanfang. deg f = 1.

Dann ist f trivialerweise eine F-Linearkombination von Potenzen der Gestalt $T_j = T_j^{p^i}$ (mit i = 0).
Induktionsschritt. deg f > 1.
Bezeichne D_i die partielle Ableitung nach T_i. Wegen (2) gilt dann

$$D_i f(T_1+U_1,...,T_n+U_n) = D_i f(T_1,...,T_n).$$

Mit

$$f(T_1,...,T_n) = \sum_{\alpha_1,...,\alpha_n} f_{\alpha_1,...,\alpha_n} \cdot T_1^{\alpha_1} \cdot ... \cdot T_n^{\alpha_n}$$

folgt

$$D_i f(T_1,...,T_n) = \sum_{\alpha_1,...,\alpha_n} D_i f_{\alpha_1,...,\alpha_n} \cdot (T_1+U_1)^{\alpha_1} \cdot ... \cdot (T_n+U_n)^{\alpha_n}$$

$$= \sum_{\alpha_1,...,\alpha_n} \alpha_i \cdot f_{\alpha_1,...,\alpha_n} \cdot (T_1+U_1)^{\alpha_1} \cdot ... \cdot (T_i+U_i)^{\alpha_i-1} \cdot ... \cdot (T_n+U_n)^{\alpha_n}$$

Dieses Polynom hängt nicht von den U_j ab. Deshalb ist

$$\alpha_i \cdot f_{\alpha_1,...,\alpha_n} = 0$$

für jedes $(\alpha_1,...,\alpha_i,...,\alpha_n)$, das von allen Standard-Einheitsvektoren e_i verschieden ist.
Wir setzen alle U_j gleich 0 und erhalten

$$D_i f(T_1,...,T_n) = \sum_{(\alpha_1,...,\alpha_i) := e_i} \alpha_i \cdot f_{\alpha_1,...,\alpha_n} \cdot T_1^{\alpha_1} \cdot ... \cdot T_i^{\alpha_i-1} \cdot ... \cdot T_n^{\alpha_n}$$

$$i=1,...,n$$

$$= D_i\Big(\sum_{j=1}^{n} f_{e_j} \cdot T_j\Big),$$

also

$$D_i\Big(f - \sum_{j=1}^{n} f_{e_j} \cdot T_j\Big) = 0 \text{ für } i = 1,...,n.$$

Die in $f - \sum_{j=1}^{n} f_{e_j} \cdot T_j$ tatsächlich auftretenden Potenzprodukte der T_j haben sämtlich durch p teilbare Exponenten, d.h.

$$f - \sum_{j=1}^{n} f_{e_j} \cdot T_j = g(T_1^p,...,T_n^p) \text{ mit } g \in F[T_1,...,T_n]$$

Mit f ist auch $f - \sum_{j=1}^{n} f_{e_j} \cdot T_j$ additiv. Da die $T_1^p,...,T_n^p$ algebraisch unabhängig sind, ist dann aber auch g additiv. Wegen deg g < deg f können wir die Induktionsvoraussetzung auf g anwenden, d.h. g ist von der Gestalt (1). Dann gilt dasselbe aber auch für

$$f = \sum_{j=1}^{n} f_{e_j} \bullet T_j + g(T_1^p,...,T_n^p).$$

3. Schritt. Sei p = 0. Dann gilt

$$\mathcal{A}(\mathbf{G}_a^n)(F) = F\bullet T_1 + ... + F\bullet T_n.$$

Insbesondere ist $\mathcal{A}(\mathbf{G}_a^n)(F)$ ein freier Modul über R(F) = F mit dem linear unabhängigen Erzeugendensystem $T_1,..., T_n$.

Sei

$$f \in F[\mathbf{G}_a^n] = F[T_1,...,T_n]$$

eine über F definierte additive Funktion. Wir schreiben

$$f(T_1,...,T_n) = \sum_{\alpha_1,...,\alpha_n} f_{\alpha_1,...,\alpha_n} \bullet T_1^{\alpha_1} \bullet ... \bullet T_n^{\alpha_n}$$

Wie im ersten Schritt folgt

$$\alpha_i \bullet f_{\alpha_1,...,\alpha_n} = 0$$

für jedes $(\alpha_1,...,\alpha_i,...,\alpha_n)$, das von allen Standard-Einheitsvektoren e_i verschieden ist. Die einzigen eventuell von 0 verschiedenen Koeffizienten sind die mit

$$(\alpha_1,...,\alpha_n) = (0,...,1,...,0) = e_i,$$

d.h. es ist

$$f = \sum_{j=1}^{n} f_{e_j} \bullet T_j \in F\bullet T_1 + ... + F\bullet T_n.$$

Umgekehrt sind alle linearen homogenen Polynome von F[T] additiv. Deshalb ist

$$\mathcal{A}(\mathbf{G}_a^n)(F) = F\bullet T_1 + ... + F\bullet T_n$$

ein freier Modul über R(F) = F mit der Basis $T_1,..., T_n$.

QED.

3.3.6 Lemma: Relationen in $\mathcal{A}$(G)(F) über F und R(F)

Seien F ein Teilkörper des algebraisch abgeschlossenen Körpers k und G eine F-Gruppe. Dann gelten folgende Aussagen.

(i) Ist G zusammenhängend, so ist der R(F)-Modul $\mathcal{A}(G)(F)$ torsionsfrei.

(ii) Sind $f_1,...,f_s \in \mathcal{A}(G)(F)$ algebraisch abhängig über k, so sind sie linear abhängig über R(F).

Beweis. Zu (i). Sei

$$f \in \mathcal{A}(G)(F) \subseteq F[G],$$

ein Element, dessen Produkt mit einen Element $r \in R(F) - \{0\}$ gleich 0 ist, sagen wir[30]

$$r = T^{\ell} + a_1 \bullet T^{\ell-1} + ... + a_{\ell} \in R(F).$$

Auf Grund der in 3.3.1 B definierten R(F)-Modul-Struktur von $\mathcal{A}(G)(F)$ gilt dann

---

[30] Der höchste Koeffizient des "Polynoms" r ist ungleich 0 und wir können r mit dem Inversen dieses Koeffizienten multiplizieren.

$$f^{p^\ell}+a_1 \bullet f^{p^{\ell-1}}+\ldots+a_\ell \bullet f = 0 \text{ mit } a_i \in F.$$

Das bedeutet, der Homomorphismus linearer algebraischer Gruppen $f: G \longrightarrow G_a = k$ kann nur endlich viele Werte annehmen.[31] Weil G zusammenhängend ist, ist die endliche Menge der Werte von f auch zusammenhängend, d.h. es ist

$$f(x) = 0 \text{ für jedes } x \in G,$$

d.h. f ist als Element von $\mathcal{A}(G)(F) \subseteq F[G]$ gleich 0. Wir haben gezeigt, $\mathcal{A}(G)(F)$ besitzt keine Torsion.

Zu (ii). Nach Voraussetzung gibt es ein Polynom

$$H \in k[T_1,\ldots,T_s] - \{0\}$$

mit

$$H(f_1,\ldots,f_s) = 0.$$

Wir können annehmen, H ist ein unter den von 0 verschiedenen Polynomen mit dieser Eigenschaft eines mit minimalem Grad,

$$\deg H \text{ minimal.}$$

Für je zwei Punkte $x,y \in G$ gilt

$$\begin{aligned} 0 &= H(f_1,\ldots,f_s)(y \bullet x) \\ &= H(f_1(y \bullet x),\ldots,f_s(y \bullet x)). \\ &= H(f_1(y)+ f_1(x),\ldots,f_s(y)+ f_s(x)) \qquad (\text{die } f_i \text{ sind additiv}). \end{aligned}$$

d.h. für jedes $x \in G$ ist

$$H(T_1+ f_1(x),\ldots,T_s+ f_s(x)) \in k[T_1,\ldots,T_s] - \{0\}.$$

gleich Null in an der Stelle $(f_1,\ldots,f_s)$.

Damit ist aber auch

$$H(T_1+ f_1(x),\ldots,T_s+ f_s(x)) - H(T_1,\ldots,T_s) \in k[T_1,\ldots,T_s]$$

für jedes $x \in G$ gleich Null an der Stelle $(f_1,\ldots,f_s)$. Da diese Differenz einen Grad hat, der kleiner als deg H ist und deg H minimal gewählt wurde, folgt,

$$\begin{aligned} 0 &= H(T_1+ f_1(x),\ldots,T_s+ f_s(x)) - H(T_1,\ldots,T_s) \\ &= H(T_1+ f_1(x),\ldots,T_s+ f_s(x)) - H(T_1,\ldots,T_s) - H(f_1(x),\ldots,f_s(x)) \end{aligned}$$

für jedes $x \in G$, also

$$0 = H(T_1+ f_1,\ldots,T_s+ f_s) - H(T_1,\ldots,T_s) - H(f_1,\ldots,f_s).$$

Deshalb wird das Polynom

$$H(T_1+ U_1,\ldots,T_s+ U_s) - H(T_1,\ldots,T_s) - H(U_1,\ldots,U_s) \qquad (1)$$

identisch 0 wenn man für jedes U_i das entsprechende f_i einsetzt. Aus Symmetrie-Gründen gilt das auch, wenn man für jedes T_i das entprechende f_i einsetzt, d.h. (1) ist identisch Null an der Stelle

$$(T_1,\ldots,T_s) = (f_1,\ldots,f_s)$$

---

[31] Weil diese Nullstellen eines von Null verschiedenen Poylnoms mit Koeffizienten aus F sind.

Wir betrachten jetzt das Polynom (1) als Polynom in den U_i mit Koeffizieten, welche Polynome in den $T_1,...,T_s$ sind. Bezeichne

$$\tilde{H}_{\alpha_1,...,\alpha_n}(T_1,...,T_s), \tag{2}$$

den Koeffizienten von

$$T_1^{\alpha_1}\bullet...\bullet T_n^{\alpha_n}$$

in diesem Polynom. Weil (1) identisch Null ist an der Stelle $(T_1,...,T_s) = (f_1,...,f_s)$, müssen alle Koeffizienten von (1) an dieser Stelle Null sein, d.h. jedes der Polynome (2) ist Null an der Stelle $(f_1,...,f_s)$.

Weil (1) als Polynom in den T_i einen Grad < deg H hat, hat jedes der Polynome (2) einen Grad < deg H. Wegen der Minimalität des Grades von H sind deshalb die Polynome (2) identisch 0, d.h. auch (1) ist identisch Null, d.h.

$$H(T_1,...,T_s) \in k[T_1,...,T_s] = k[G_a^s]$$

ist ein additives Polynom, d.h.

$$H(T_1,...,T_s) \in \mathcal{A}(G_a^s)(k) = k\otimes_F\mathcal{A}(G_a^s)(F)$$

(vgl. Bemerkung 3.3.1 A (iii)). Wir können H in der Gestalt

$$H = c_1\bullet H_1+...+c_r\bullet H_r \text{ mit } c_i \in k$$

schreiben mit additiven Polynomen

$$H_i \in F[T_1,...,T_s] - \{0\}.$$

Ist eines der c_i eine F-Linearkombination der übrigen, so besteht eine solche Identität auch für ein kleineres r. Wir können also annehmen, die c_i sind über F linear unabhängig. Dann sind aber die

$$c_i\otimes 1 \in k\otimes_F F[G] = k[G]$$

linear unabhängig über F[G]. Wegen

$$0 = H(f_1,...,f_s) = c_1\bullet H_1(f_1,...,f_s)+...+c_r\bullet H_r(f_1,...,f_s)$$

und $H_i(f_1,...,f_s) \in k[G]$ folgt

$$H_i(f_1,...,f_s) = 0$$

für jedes i. Wie wir gerade bewiesen haben, hat jedes $H_i \in \mathcal{A}(G_a^s)(F)$ die Gestalt

$$H_i = \sum_{i,j,\ell} c_{i,j,\ell}\bullet T_j^{p^\ell} \text{ mit } c_{i,j,\ell} \in F,$$

d.h. es ist

$$\begin{aligned} 0 &= H_i(f_1,...,f_s) \\ &= \sum_{i,j,\ell} c_{i,j,\ell}\bullet f_j^{p^\ell} \\ &= \sum_{j=1}^{s}\sum_{i,\ell} c_{i,j,\ell}\bullet T^{p^\ell}\bullet f_j \end{aligned}$$

$$= \sum_{j=1}^{s} r_j \cdot f_j \text{ mit } r_j := \sum_{i,\ell} c_{i,j,\ell} \cdot T^{\ell} \in R(F).$$

Wir haben gezeigt, die $f_1,...,f_s$ sind über R(F) linear abhängig (weil die H_i nicht identisch Null sind, d.h. nicht alle $c_{i,j,\ell}$ sind gleich Null).

QED.

3.4 Elementare unipotente Gruppen

3.4.1 Definitionen und Bezeichnungen

Eine unipotente lineare algebraische Gruppe G heißt elementar, wenn sie abelsch ist und wenn im Fall einer positiven Charakteristik p des Grundkörpers außerdem die Ordnung jedes Elements von G - {e} gleich p ist. Die Gruppe G heißt Vektor-Gruppe, wenn sie isomorph ist zu einem Produkt $\mathbf{G}_a^n$ von endlich vielen Exemplaren der additiven Gruppe $\mathbf{G}_a$.

Bemerkungen

(i) Wir beginnen mit verschiedenartigen Ergebnissen, die wir zur Untersuchung der Struktur der elementaren unipotenten Gruppen brauchen.

(ii) Seien p ein Primzahl, n eine nicht-negative ganze Zahl und

$$n = \sum_{i=0}^{\infty} n_i \cdot p^i$$

deren p-adische Entwicklung (mit ganzen Zahlen n_i aus dem Intervall [0, p-1], von denen fast alle gleich 0 sind). Ist

$$m = \sum_{i=0}^{\infty} m_i \cdot p^i$$

eine weitere solche p-adische Entwicklung, so schreiben wir

$$n \leq_p m,$$

wenn $n_i \leq m_i$ gilt für jedes i.

(iii) Für nicht-negative ganze Zahlen m,n sei

$$(m, n) := \binom{m}{n} = \begin{cases} \frac{m!}{n! \cdot (m-n)!} & \text{für } m \geq n \\ 0 & \text{für } m < n \end{cases}$$

der zugehörige Binomial-Koeffizient

3.4.2 Lemma: Binomial-Koeffizienten und p-adische Entwicklung

Mit den Bezeichnungen der Bemerkungen von 3.4.1 gilt

(i) $\binom{m}{n} = \prod_i \binom{m_i}{n_i} \bmod p.$

(ii) $\binom{m}{n} \not\equiv 0 \bmod p \Leftrightarrow n \leq_p m.$

Beweis. Zu (i). Im Polynomring $(\mathbb{Z}/p\mathbb{Z})[T]$ in einer Unbestimmten T über einem Körper der Charakteristik p gilt

$$(T+1)^m = \prod_i (T+1)^{m_i \cdot p^i} = \prod_i (T^{p^i}+1)^{m_i} \pmod p$$

also

$$\sum_{i=0}^{m} \binom{m}{i} \cdot T^i = \prod_i \sum_{j=0}^{m_i} \binom{m_i}{j} \cdot T^{j \cdot p^i} \bmod p.$$

Vergleich der Koeffizienten von T^n liefert modulo p:

$$\binom{m}{n} = \text{Summe über alle Produkte } \binom{m_{i_1}}{j_1} \cdot \ldots \cdot \binom{m_{i_r}}{j_r} \text{ mit } \sum_{\nu=1}^{r} j_\nu \cdot p^{i_\nu} = n$$

Dabei ist für jedes ν stets $j_\nu \le m_{i_\nu} < p$, d.h. die j_ν sind die Koeffizienten der p-adischen Entwicklung von n. Die Summe rechts besteht aus dem einzigen Summanden $\prod_i \binom{m_i}{n_i}$, d.h. es gilt

$$\binom{m}{n} = \prod_i \binom{m_i}{n_i} \bmod p.$$

Damit gilt (i).
Zu (ii). Es gilt

$$\binom{m}{n} \not\equiv 0 \bmod p \quad \Leftrightarrow \binom{m_i}{n_i} \not\equiv 0 \bmod p \text{ für jedes i.}$$

$$\Leftrightarrow n_i \le m_i \text{ für jedes i.}$$

$$\Leftrightarrow n \le_p m$$

QED.

3.4.3 Polynomiale 2-Kozyklen

Seien p eine Primzahl und T, U zwei Unbestimmte. Dann setzen wir

$$c(T, U) := \frac{1}{p} \cdot ((T+U)^p - T^p - U^p) = \sum_{i=1}^{p-1} \frac{1}{p} \cdot \binom{p}{i} \cdot T^{p-i} U^i \in \mathbb{Z}[T, U].$$

Man beachte, für $0 < i < p$ ist p ein Teiler von $\binom{p}{i} = \frac{p!}{i! \cdot (p-i)!}$.

Ein polynomialer 2-Kozyklus über dem Körper F ist ein Polynom $f \in F[T,U]$ mit

$$f(T+U, V) + f(T, U) = f(U+V, T) + f(U, V).$$

Für jedes Polynom $f \in A[T,U]$ mit Koeffizienten in einem kommutativen Ring A mit 1 definieren wir den polynomialen Korand-Operator

$$(\partial f)(T, U, V) :=^{32} f(U, V) - f(T+U, V) + f(U+V,T) - f(T,U).$$

Bemerkungen

---

[32] Wir verwenden hier die Definition des Korand-Operators von Lazard [1] und nicht die von Springer. In der Definiton von Springer sind die Argumente des dritten Summanden vertauscht:

$$(\partial f)(\mathbf{T}, \mathbf{U}, \mathbf{V}) := f(\mathbf{U}, \mathbf{V}) - f(\mathbf{T}+\mathbf{U}, \mathbf{V}) + f(\mathbf{U}+\mathbf{V}, \mathbf{T}) - f(\mathbf{T},\mathbf{U}).$$

Da alle Anwendungen sich nur auf den Fall von abelschen Gruppen beziehen, ist diese Abweichung nicht wirklich wesentlich. An einigen Stellen erfordern sich aber eine kompliziertere Argumentation und einige Argumente im Buch von Springer sind sind schwer zu verstehen. Es handelt sich vermutlich um einen Tippfehler.

(i) Die polynomialen 2-Kozyklen von F[T,U] sind gerade die Polynome $f \in F[T,U]$ mit

$$\partial f = 0.$$

(ii) Für jede natürlichen Zahl $q \geq 2$ definieren ganzzahlige Polynome

$$B_q(x,y) := (x+y)^q - x^q - y^q \in \mathbb{Z}[x,y]$$

$$C_q(x,y) = \begin{cases} B_q(x,y) & \text{falls q keine Potenz einer Primzahl ist} \\ \frac{1}{p} \bullet B_q(x,y) & \text{wenn q eine Potenz der Primzahl p ist} \end{cases} \in \mathbb{Z}[x,y]$$

Die natürlichen Bilder dieser dieser Polynome in $\mathbb{Q}[x,y]$ und in $\mathbb{F}_p[x,y]$ sind polynomiale 2-Kozyklen.

(iii) Falls q keine Potenz der Primzahl p ist, sind nicht alle Koeffizienten von B_q durch p teilbar,

$$B_q(x,y) \not\equiv 0 \pmod{p}.$$

(vgl. Lazard [1], (3.1)).

(iv) Für jede Primzahl p und jede natürliche Zahl ℓ gilt

$$C_{p^\ell}(x,y) = C_p(x^{p^{\ell-1}}, y^{p^{\ell-1}}) \not\equiv 0 \pmod{p}.$$

(vgl. Lazard [1], (3.3)).

(v) Für jede Primzahl p und jede natürliche Zahl ℓ gilt

$$C_p(x^{p^\ell}, y^{p^\ell}) = C_p(x,y)^{p^\ell} \pmod{p}.$$

Beweise. Zu (ii). Es gilt

$$\begin{aligned} \partial B_q(x,y) &= B_q(y,z) - B_q(x+y,z) + B_q(x,y+z) - B_q(x,y) \\ &= (y+z)^q - y^q - z^q \\ &\quad - (x+y+z)^q + (x+y)^q + z^q \\ &\quad + (x+y+z)^q - x^q - (y+z)^q \\ &\quad - (x+y)^q + x^q + y^q \\ &= 0 \end{aligned}$$

Ist q die Potenz einer Primzahl p, so gilt damit auch

$$p \bullet \partial C_q(x,y) = 0.$$

Dies ist eine Relation im Polynomring $\mathbb{Z}[x,y]$. Weil $\mathbb{Z}[x,y]$ nullteilerfrei ist, folgt

$$\partial C_q(x,y) = 0.$$

Zu (iii). Sei

$$q = p^\ell \bullet s \text{ mit } s \not\equiv 1 \text{ und s teilerfremd zu p.}$$

Dann gilt

$$(x+y)^q = (x^{p^\ell} + y^{p^\ell})^s = x^q + s \bullet x^{(s-1)p^\ell} y^{p^\ell} + \ldots + y^q \pmod{p},$$

also

$$B_q(x,y) = s \bullet x^{(s-1)p^\ell} y^{p^\ell} + \ldots \not\equiv 0 \pmod{p}$$

Zu (iv). Es gilt

$$(x+y)^{p^{\ell-1}} = x^{p^{\ell-1}} + y^{p^{\ell-1}} \pmod{p},$$

also

$$(x+y)^{p^{\ell-1}} = x^{p^{\ell-1}} + y^{p^{\ell-1}} + p\bullet f(x,y).$$

Wir gehen zur p-ten Potenz über und erhalten

$$(x+y)^{p^{\ell}} = \sum_{i=0}^{p} \binom{p}{i}(x^{p^{\ell-1}} + y^{p^{\ell-1}})^{i}\bullet(p\bullet f(x,y))^{p-i}$$

$$= (x^{p^{\ell-1}} + y^{p^{\ell-1}})^{p} + \binom{p}{p-1}(x^{p^{\ell-1}} + y^{p^{\ell-1}})^{p-1}\bullet(p\bullet f(x,y)) \pmod{p^2}$$

Wegen $\binom{p}{p-1} = \binom{p}{1} = p$ ist der dritte Summand durch p^2 teilbar, also

$$(x+y)^{p^{\ell}} = (x^{p^{\ell-1}} + y^{p^{\ell-1}})^{p} \pmod{p^2}$$

also

$$(x+y)^{p^{\ell}} - x^{p^{\ell}} - y^{p^{\ell}} = (x^{p^{\ell-1}} + y^{p^{\ell-1}})^{p} - (x^{p^{\ell-1}})^{p} - (y^{p^{\ell-1}})^{p} \pmod{p^2}$$

also

$$C_{p^{\ell}}(x,y) = C_{p}(x^{p^{\ell-1}}, y^{p^{\ell-1}}) \pmod{p}.$$

Weiter ist

$$C_{p}(x,y) = \sum_{i=1}^{p-1} \frac{1}{p}\bullet\binom{p}{i}\bullet x^{i}\bullet y^{p-i}.$$

Der Koeffizientn von $x\bullet y^{p-1}$ ist $\frac{1}{p}\bullet\binom{p}{1} = 1$, d.h. nicht durch p teilbar. Weil $C_p(x,y)$ und $C_p(x^{p^{\ell-1}}, y^{p^{\ell-1}})$ dieselben Koeffizientenmangen haben, folgt

$$C_{p}(x^{p^{\ell-1}}, y^{p^{\ell-1}}) \not\equiv 0 \pmod{p}.$$

Zu (v). Weil

$$\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$$

ein Körper ist und die Einheitengruppe von $\mathbb{F}_p$ die Ordnung p-1 hat, gilt $\alpha^{p-1} = 1$ für jede Einheit α von $\mathbb{F}_p$, also

$$\alpha^{p} = \alpha \text{ (modp) für jedes } \alpha \in \mathbb{F}_p,$$

also

$$\alpha^{p} = \alpha \bmod p \text{ für jede ganze Zahl } \alpha.$$

Weil $C_p(x,y)$ ein Polynom mit Koeffizienten aus $\mathbb{Z}$ ist folgt

$$C_{p}(x,y)^{p^{\ell}} = C_{p}(x^{p^{\ell}},y^{p^{\ell}}) \bmod p.$$

QED.

3.4.4 Lemma: Kriterium für 2-Koränder

Sei F ein perfekter Körper der Charakteristik p und $f \in F[T, U]$ ein polynomialer 2-Kozyklus.

(i) Ist $p = 0$, so gibt es ein Polynom $g \in F[T]$ mit

$$f(T, U) = g(T+U) - g(T) - g(U).$$

(ii) Ist $p > 0$, so gibt es ein Polynom $g \in F[T]$ derart, daß

$$f(T, U) - g(T+U) + g(T) + g(U)$$

eine Linearkombination $\mathcal{L}$ von Polynomen der Gestalt $c(T, U)^{p^i}$ ist mit $c(T,U)$ wie in 3.4.3.

(iii) Ist $p > 0$ und gilt außerdem

$$\sum_{i=1}^{p-1} f(T, iT) = 0,$$

so ist die Linearkombination $\mathcal{L}$ von (ii) gleich 0.

Beweis. Zu (i) und (ii). Ist f ein polynomialer 2-Kozyklus, so gilt dasselbe für jede homogene Komponente des Polynoms f. Wir können also annehmen,

f ist homogen vom Grad d.

Wir führen den weiteren Beweis durch Induktion nach dem Grad d von f.

Induktionsanfang: $d = 0$.

Die Aussage von (i) ist dann trivial: weil f das konstante Polynom ist, sagen wir

$$f(T,U) = c \in k,$$

so kann man $g(T) = -c$ setzen.

Induktionsschritt: $d > 0$.

Wegen

$$f(T+U, V) + f(T, U) = f(U+V, T) + f(U, V) \qquad (1)$$

erhalten wir für $T = U = 0$

$$f(0, V) + 0 = f(V, 0) + f(0, V),$$

also

$$f(V,0) = 0,$$

und für $U = V = 0$

$$f(T, 0) + f(T, 0) = f(0, T) + 0,$$

also

$$f(0, T) = 2 \cdot f(T, 0) = 0.$$

Wir können f in der Gestalt

$$f(T, U) = \sum_{h=0}^{d} c_h \cdot T^h \cdot U^{d-h} \text{ mit } c_0 = c_d = 0$$

schreiben. Wir vergleichen die Koeffizienten von $T^h U^i V^j$ auf beiden Seiten von (1) und erhalten

$$\binom{h+i}{h} \cdot c_{h+i} + \delta_{j,0} \cdot c_h = \binom{i+j}{j} \cdot c_{i+j} + \delta_{h,0} \cdot c_j \text{ für } h+i+j = d. \qquad (2)$$

Für h=0 oder j=0 erhalten wir aus (2)

$$c_h = c_{d-h}, \qquad (3)$$

denn für $h = 0$ erhalten wir $i+j = d$, also $j = d-i$, also

$$c_i + \delta_{j,0} \cdot c_0 = \binom{d}{d-i} \cdot c_d + c_{d-i}$$

und wegen $c_0 = c_d = 0$ folgt $c_i = c_{d-i}$.

Für $j = 0$ ist $i+h = d$, also $i = d-h$, erhalten wir

$$\binom{d}{h} \cdot c_d + c_h = c_{d-h} + \delta_{h,0} \cdot c_0$$

und wegen $c_0 = c_d = 0$ folgt $c_h = c_{d-h}$.

Seien jetzt $0 < h, j < d$. Wegen $h+i = d- j$ und $i+j = d-h$ folgt dann aus (2)

$$\binom{d-j}{h} \cdot c_{d-j} = \binom{d-h}{j} \cdot c_{d-h}$$

also zusammen mit (3)

$$\binom{d-j}{h} \cdot c_j = \binom{d-h}{j} \cdot c_h \qquad (4)$$

für $0 < h, j < d$.

In der Situation von (i) können wir wegen p = 0 beide Seiten von (4) mit

$$\frac{(d-j+1)\bullet(d-j+2)\bullet\ldots\bullet d}{(d-h-j+1)\bullet(d-h-j+2)\bullet\ldots\bullet(d-h)} = \frac{(d-h+1)\bullet(d-h+2)\bullet\ldots\bullet d}{(d-h-j+1)\bullet(d-h-j+2)\bullet\ldots\bullet(d-j)}$$

multiplizieren.Wegen

$$\frac{(d-j)!}{h!\bullet(d-h-j)!}\bullet\frac{(d-j+1)\bullet(d-j+2)\bullet\ldots\bullet d}{(d-h-j+1)\bullet(d-h-j+2)\bullet\ldots\bullet(d-h)} = \frac{d!}{h!\bullet(d-h)!} = \binom{d}{h}$$

und

$$\frac{(d-h)!}{j!\bullet(d-h-j)!}\bullet\frac{(d-h+1)\bullet(d-h+2)\bullet\ldots\bullet d}{(d-h-j+1)\bullet(d-h-j+2)\bullet\ldots\bullet(d-j)} = \frac{d!}{j!\bullet(d-j)!} = \binom{d}{j}$$

erhalten wir

$$\binom{d}{h}\bullet c_j = \binom{d}{j}\bullet c_h$$

also

$$\begin{aligned} c_j\bullet((T+U)^d - T^d - U^d) &= \sum_{h=1}^{d-1} c_j\bullet\binom{d}{h}T^h\bullet U^{d-h} \\ &= \sum_{h=1}^{d-1} c_h\bullet\binom{d}{j}T^h\bullet U^{d-h} \\ &= \binom{d}{j}\bullet\sum_{h=1}^{d-1} c_h\bullet T^h\bullet U^{d-h} \\ &= \binom{d}{j}\bullet f(T, U) \qquad (\text{wegen } c_0 = c_d = 0) \end{aligned}$$

Für j = 1 erhalten wir

$$c_1\bullet((T+U)^d - T^d - U^d) = d\bullet f(T, U).$$

Weil die Charakteristik gleich 0 ist, können wir durch d teilen und

$$g(T) = (c_1/d)\bullet T^d$$

setzen. Wie behauptet ist dann

$$f(T, U) = g(T+U) - g(T) - g(U).$$

In der Situation von (ii) erhalten wir aus (4) mit j = 1:

$$(d-h)\bullet c_h = \binom{d-1}{h}\bullet c_1.$$

Wir ersetzen h durch d-h und erhalten

$$h\bullet c_{d-h} = \binom{d-1}{d-h}\bullet c_1$$

und mit (3)

$$h\bullet c_h = \binom{d-1}{d-h}\bullet c_1 \qquad (5)$$

für $0 < h < d$.

Ebenfalls aus (4) erhalten wir

$$\binom{d-j}{d-h-j}\bullet c_j = \binom{d-h}{d-h-j}\bullet c_h$$

für $0 < h, j < d$ und speziel für j = d-h-1, d.h. d-h-j = 1 ist

$$(d-j)\bullet c_j = (d-h)\bullet c_h,$$

also

$$(h+1)\bullet c_{d-h-1} = (d-h)\bullet c_h \text{ für } h = 1,\ldots, d-2.$$

Zusammen mit (3) folgt

$$(h+1)\bullet c_{h+1} = (d-h)\bullet c_h \text{ für } h = 1,\ldots, d-2. \qquad (6)$$

Wir haben drei Fälle zu unterscheiden.

1. Fall: d ist teilerfremd zur Charakteristik p von k.
Es gilt

$$\frac{\partial f(T,U)}{\partial T} = \sum_{h=1}^{d-1} h \cdot c_h \cdot T^{h-1} \cdot U^{d-h}$$

$$= \sum_{h=1}^{d-1} \binom{d-1}{d-h} \cdot c_1 \cdot T^{h-1} \cdot U^{d-h} \qquad \text{(nach (5))}$$

$$= c_1 \cdot \sum_{h=1}^{d-1} \binom{d-1}{d-h} \cdot T^{h-1} \cdot U^{d-h}$$

$$= c_1 \cdot \sum_{h=1}^{d-1} \binom{d-1}{h-1} \cdot T^{h-1} \cdot U^{d-h} \qquad \text{(wegen } \binom{n}{\nu} = \binom{n}{n-\nu}\text{)}$$

$$= c_1 \cdot \sum_{h=0}^{d-2} \binom{d-1}{h} \cdot T^{h} \cdot U^{(d-1)-h} \qquad \text{(Index-Verschiedung)}$$

$$= c_1 \cdot ((T+U)^{d-1} - T^{d-1})$$

$$= (c_1/d) \cdot \frac{\partial}{\partial T} ((T+U)^d - T^d - U^d))$$

und

$$\frac{\partial f(T,U)}{\partial U} = \sum_{h=1}^{d-1} (d-h) \cdot c_h \cdot T^{h} \cdot U^{d-h-1}$$

$$= \sum_{h=1}^{d-1} (d-h) \cdot c_{d-h} \cdot T^{h} \cdot U^{d-h-1} \quad \text{(nach (3))}$$

$$= \sum_{h=1}^{d-1} \binom{d-1}{h} \cdot c_1 \cdot T^{h} \cdot U^{(d-1)-h} \quad \text{(nach (5) mit d-h anstelle von h)}$$

$$= c_1 \cdot \sum_{h=1}^{d-1} \binom{d-1}{h} \cdot T^{h} \cdot U^{(d-1)-h}$$

$$= c_1 \cdot ((T+U)^{d-1} - U^{d-1})$$

$$= (c_1/d) \cdot \frac{\partial}{\partial U} ((T+U)^d - T^d - U^d)$$

Mit

$$f_1 := f(T,U) - (c_1/d) \cdot ((T+U)^d - T^d - U^d)$$

gilt also $\frac{\partial f_1}{\partial T} = \frac{\partial f_1}{\partial U} = 0$, d.h. $f_1(T,U)$ ist ein Polynom in T^p und U^p. Weil

$$d = \deg f = \deg f_1$$

teilerfremd zu p ist, folgt $f_1 = 0$. Damit gilt (ii) (mit $g(T) = (c_1/d) \cdot T^d$ und $\mathcal{L} = 0$).

Bemerkung
Die Argumentation des im Buch von Springer behandelten zweiten Falls,

$$p \mid d \text{ und es gibt ein } h \text{ mit } p \nmid h \text{ und } c_h \neq 0,$$

scheint einen Fehler zu enthalten. Dort wird aus $d-h \geq p$ geschlossen, daß die Bedingung von 3.4.2 erfüllt ist (d.h. $p \leq_p (d-h)$) und deshalb nach 3.4.2 (ii) der Binomialkoeffizient $\binom{d-h}{p}$ nicht durch p teilbar ist. Für

$$h = d - p^2 - 1 \text{ (d.h. } d = h + p^2 + 1, \text{ d.h. } d-h = p^2+1)$$

ist aber die Bedingung $p \leq_p (d-h)$ nicht erfüllt und auch die Folgerung $d-h < p$ falsch. Wir folgen deshalb an dieser Stelle dem Beweis von Lemma 3 in der Arbeit von Lazard [1].

2. Fall. $d = p$.
Wir betrachten das Polynom

$$\tilde{f}(T,U) := f(T,U) - c_1 \cdot C_p(T,U).$$

Dann gilt mit $\partial P = 0$ nach Bemerkung 3.4.3 (ii) auch

$$\partial \tilde{f}(T,U,V) = 0.$$

Es reicht zu zeigen

$$\tilde{f} = 0,$$

denn dann ist

$$f(T,U) = c_1 \cdot C_p(T,U)$$

ein Vielfaches von C(T,U) und es gilt (ii) mit $g(T) = 0$ und $\mathcal{L} = c_1 \cdot c(T,U)$.

Wegen $\partial \tilde{f} = 0$ gelten die oben für f abgeleiteten Formeln analog auch für $\tilde{f}$. Nach (5) reicht es zu zeigen, der Koeffizient von $T \cdot U^{p-1}$ in $\tilde{f}$ ist gleich 0 (denn für $h = 1,\ldots, p-1$ ist h eine Einheit im Körper F der Charakteristik p). Nach 3.4.3 ist der Koeffizient von $T \cdot U^{p-1}$ im Polynom $c(T,U) = C_p(T,U)$ gleich $\frac{1}{p}\binom{p}{p-1} = \frac{1}{p} \cdot \binom{p}{1} = 1$. Also ist der Koeffizient von $T \cdot U^{p-1}$ in $\tilde{f}$ gleich $c_1 - c_1 \cdot 1 = 0$. Es gilt also tatsächlich, $\tilde{f} = 0$, und es gilt die Behauptung.

3. Fall. p ist ein Teiler von d aber $d \neq p$ (d.h. $p < d$)
Aus (6) mit $h = p-1$ ($\leq d-2$) erhalten wir

$$(d-p+1) \cdot c_{p-1} = p \cdot c_p = 0,$$

also

$$c_{p-1} = 0.$$

Nehmen wir an, wir haben bereits gezeigt, daß

$$c_{p-j} = 0 \tag{7}$$

gilt. Für $1 \leq j \leq p-2$ gilt

$$1 \leq h := p-j-1 \leq p-2 \leq d-2.$$

Wir können also (6) anwenden und erhalten

$$(d-p+j+1) \cdot c_{p-j-1} = (p-j) \cdot c_{p-j} = 0,$$

wegen $d-p+j+1 = j+1 \pmod p$ und $j+1 \leq p-1$ ist $d-p+j+1$ nicht durch p teilbar, d.h. es gilt

$$c_{p-j-1} = 0.$$

Es gilt also (7) mit einem um 1 vergrößerten j. Wir können j solange vergrößern, solang $j \leq p-2$ gilt, d.h. es gilt (7) mit $j = p-1$, also

$$c_{p-1} = c_{p-2} = ... = c_1 = 0.$$

Mit $c_1 = 0$ gilt nach (5), $h \bullet c_h = 0$ für h = 1,..., d-1, also

$$c_h = 0 \text{ für jedes } h \in \{1,...,q-1\}, \text{ welches kein Vielfaches von p ist.}$$

Damit ist $f(T, U) = \sum_{h=1}^{d-1} c_h \bullet T^h \bullet U^{d-h}$ ein Polynom in T^p und U^p, sagen wir,

$$f(T, U) = \tilde{f}(T^p, U^p).$$

Wegen

$$\begin{aligned} 0 &= \partial f(T,U,V) \\ &= f(U,V) - f(T+ U, V) + f(U+V,T) - f(T,U) \\ &= \tilde{f}(U^p,V^p) - \tilde{f}((T+ U)^p, V^p) + \tilde{f}((U+V)^p, T^p) - \tilde{f}(T^p, U^p) \\ &= \tilde{f}(U^p,V^p) - \tilde{f}(T^p+U^p,V^p) + \tilde{f}(U^p+V^p,T^p) - \tilde{f}(T^p,U^p) \text{ (wegen Char(F)=p)} \\ &= (\partial\tilde{f})(T^p,U^p, V^p), \end{aligned}$$

ist

$$0 = f(T,U,V) = (\partial\tilde{f})(T^p,U^p, V^p). \tag{3.9}$$

Weil T^p, U^p, V^p algebraisch unabhängig sind, folgt

$$\partial\tilde{f}(T,U,V) = 0.$$

Die Behauptung ist damit auf den Fall eines Polynoms des Grades $d' := \frac{d}{p}$ zurückgeführt. Ist auch d' ein Teiler von p, so können wir diese Reduktion fortsetzen. Im Fall, daß d eine Potenz von p ist, sagen wir

$$d = p^{\ell},$$

ergibt sich zusammen mit dem zweiten Fall, daß f die Gestalt

$$f(T,U) = a \bullet C_p(T^{p^{\ell}},U^{p^{\ell}}) \text{ mit } a \in F$$

hat. Auf Grund von Bemerkungen 3.4.3 (v) folgt

$$f(T,U) = a \bullet C_p(T,U)^{p^{\ell}},$$

d.h. es gilt die Aussage von (ii) mit g = 0 und $\mathfrak{L} = a \bullet c(T,U)^{p^{\ell}}$
Im Fall, daß d keine Potenz von p ist, sagen wir

$$d = p^{\ell} \bullet s \text{ mit } s \neq 1 \text{ und } s \neq 0 \text{ (mod p)},$$

ist f von der Gestalt

$$f(T,U) = \tilde{f}(T^{p^{\ell}},U^{p^{\ell}}),$$

wobei $\tilde{f}$ ein homogenes Polynom des Grades s mit $\partial\tilde{f} = 0$ ist. Weil s teilerfremd zu p ist, erhalten wir auf Grund des ersten Falls

$$\tilde{f}(T,U) = a \bullet ((T+U)^s - T^s - U^s) \text{ mit } a \in F,$$

also

$$\begin{aligned} f(T,U) &= a \bullet ((T^{p^{\ell}}+U^{p^{\ell}})^s - T^{p^{\ell}s} - U^{p^{\ell}s}) \\ &= a \bullet ((T+U)^{p^{\ell}s} - T^{p^{\ell}s} - U^{p^{\ell}s}) \\ &= a \bullet ((T+U)^d - T^d - U^d). \end{aligned}$$

Die Behauptung gilt also mit

$g(T) = a \bullet T^d$ und $\mathcal{L} = 0$.

Zu (iii). 1. Schritt. $\sum_{i=1}^{p-1} ((T+iT)^d - T^d - (iT)^d) = p \bullet (p^{d-1} - 1) \bullet T^d$.

Es gilt in $\mathbb{Z}[T]$:

$$\begin{aligned}\sum_{i=1}^{p-1} ((T+iT)^d - T^d - (iT)^d) &= \sum_{i=1}^{p-1} ((1+i)^d - 1 - i^d) \bullet T^d \\ &= ((2^d+3^d+\ldots+p^d) - (p-1) \bullet 1 - (1^d+2^d+\ldots+(p-1)^d) \bullet T^d \\ &= (p^d - (p-1) - 1^d) \bullet T^d \\ &= (p^d - p) \bullet T^d \\ &= p \bullet (p^{d-1} - 1) \bullet T^d\end{aligned}$$

2. Schritt. $\sum_{i=1}^{p-1} C_p(T, iT) = (p^{p-1} - 1) \bullet T^p$.

Es gilt in $\mathbb{Z}[T]$:

$$\begin{aligned}p \bullet \sum_{i=1}^{p-1} C_p(T, iT) &= \sum_{i=1}^{p-1} B_p(T, iT) \qquad \text{(nach Bemerkung 3.4.3 (ii))} \\ &= \sum_{i=1}^{p-1} (T+iT)^p - T^p - (iT)^p \\ &= p \bullet (p^{p-1} - 1) \bullet T^p \qquad \text{(nach dem ersten Schritt mit d=p)}\end{aligned}$$

Weil $\mathbb{Z}[T]$ nullteilerfrei ist, folgt.

$$\sum_{i=1}^{p-1} C_p(T, iT) = (p^{p-1} - 1) \bullet T^p$$

3. Schritt. $\sum_{i=1}^{p-1} (g(T+iT) - g(T) - g(iT)) = 0$ für jedes $g(T) \in F[T]$.

Die Summe auf der linken Seite ist linear in g. Es reicht also, die Aussage für $g = T^d$ zu beweisen. In diesem Fall folgt die Aussage aus dem ersten Schritt.

4. Schritt. Beweis der Behauptung.

Zum Beweis können wir annehmen, f und g sind homogene Polynome des Grades d. Dann ist auch $\mathcal{L}$ ein homogenes Polynom des Grades d. Das ist nur möglich, wenn d eine Potenz von p ist, sagen wir

$$d = p^{\ell}.$$

Weil c(T,U) homogen vom Grad p ist, folgt

$$f(T, U) - g(T+U) + g(T) + g(U) = a \bullet c(T,U)^{p^{\ell}-1} \text{ mit } a \in F.$$

Nach Voraussetzung gilt

$$\begin{aligned}0 &= \sum_{i=1}^{p-1} f(T,iT) \\ &= \sum_{i=1}^{p-1} g(T+iT) - g(T) - g(U) + \sum_{i=1}^{p-1} a \bullet c(T,iT)^{p^{\ell}-1}.\end{aligned}$$

Nach dem dritten Schritt ist die ersten Summe gleich Null. Also ist es auch die zweite Summe, d.h.

$$0 = (a \bullet \sum_{i=1}^{p-1} c(T,iT))^{p^{\ell-1}}.$$

Weil F[T] nullteilerfrei ist, folgt

$$0 = a \bullet \sum_{i=1}^{p-1} c(T,iT).$$

Nach dem zweiten Schritt ist der zweite Faktor rechts von 0 verschieden. Deshalb gilt

$$a = 0,$$

d.h. es gilt die Behauptung.
QED.

3.4.5 Mehrdimensionale polynomiale 2-Kozyklen

Wir benötigen eine mehrdimensionale Verallgemeinerung. Deshalb betrachten wir jetzt zwei n-Tupel von Unbestimmten,

$$\mathbf{T} := (T_1,...,T_n) \text{ und } \mathbf{U} := (U_1,...,U_n).$$

Wir verwenden die Bezeichnung

$$F[\mathbf{T}, \mathbf{U}] := F[T_1,...,T_n, U_1,...,U_n]$$

für den Polynomring in den Unbestimmten T_i und U_j mit i,j = 1,...,n. Weiter sei

$$c_h(T, U) := c(T_h,U_h) \text{ für } h = 1,...,n.$$

Für Polynome $f \in A[\mathbf{T}, \mathbf{U}]$ in den T_i und U_j mit Koeffizienten aus einem kommutativen Ring A mit 1 definieren wir den 2-Korand als das Polynom

$$(\partial f)(\mathbf{T}, \mathbf{U}, \mathbf{V}) =^{33} f(\mathbf{U},\mathbf{V}) - f(\mathbf{T}+\mathbf{U}, \mathbf{V}) + f(\mathbf{T}, \mathbf{U}+\mathbf{V}) - f(\mathbf{T},\mathbf{U}).$$

Das Polynom f heißt polynomialer 2-Kozyklus, wenn $\partial f = 0$ gilt.

3.4.6 Lemma: Kriterium für mehrdimensionale 2-Koränder

Sei F ein perfekter Körper der Charakteristik p und $f \in F[\mathbf{T}, \mathbf{U}]$ ein polynomialer 2-Kozyklus.

(i) Ist p = 0, so gibt es ein Polynom $g \in F[\mathbf{T}]$ mit

$$f(\mathbf{T}, \mathbf{U}) = g(\mathbf{T}+\mathbf{U}) - g(\mathbf{T}) - g(\mathbf{U}).$$

(ii) Ist p > 0, so gibt es ein Polynom $g \in F[\mathbf{T}]$ derart, daß

$$f(\mathbf{T}, \mathbf{U}) - g(\mathbf{T}+\mathbf{U}) + g(\mathbf{T}) + g(\mathbf{U})$$

eine Linearkombination $\mathcal{L}$ von Polynomen der Gestalt $c_h(\mathbf{T}, \mathbf{U})^{p^i}$ ist mit

$$c_h(\mathbf{T},\mathbf{U})$$

wie in 3.4.5.

(iii) Ist p > 0 und gilt außerdem

$$\sum_{i=1}^{p-1} f(\mathbf{T}, i\mathbf{T}) = 0,$$

so ist die Linearkombination $\mathcal{L}$ von (ii) gleich 0.

Beweis. Zu (i). Die Aussage wird in analoger Weise bewiesen wie die von 3.4.4 (i). Sei

---

[33] Wir verwenden hier die Definition des Korand-Operators von Lazard [1] und nicht die von Springer. In der Definiton von Springer sind die Argumente des dritten Summanden vertauscht:

$$(\partial f)(T, U, V) := f(U, V) - f(T+U, V) + f(U+V, T) - f(T,U).$$

Da alle Anwendungen sich nur auf den Fall von abelschen Gruppen beziehen, ist diese Abweichung nicht wirklich wesentlich. An einigen Stellen erfordern sich aber eine kompliziertere Argumentation und einige Argumente im Buch von Springer sind sind schwer zu verstehen. Es handelt sich vermutlich um einen Tippfehler.

$$f(\mathbf{T}, \mathbf{U}) \in F[\mathbf{T}, \mathbf{U}]$$

ein polynomialer 2-Kozyklus. Dann gilt dasselbe auch für jede homogene Komponente von f. Wir können also annehmen,

$$f \text{ ist homogen vom Grad } d = (d_1,...,d_n), \text{d.h.}$$

$$f \text{ ist homogen vom Grad } d_i \text{ in } T_i \text{ und } U_i \text{ für } i = 1,...,n$$

Wegen

$$f(\mathbf{T}+\mathbf{U}, \mathbf{V}) + f(\mathbf{T}, \mathbf{U}) = f(\mathbf{U}+\mathbf{V}, \mathbf{T}) + f(\mathbf{U}, \mathbf{V}) \qquad (1)$$

erhalten wir für $\mathbf{T} = \mathbf{U} = 0$

$$f(0, \mathbf{V}) + 0 = f(\mathbf{V}, 0) + f(0, \mathbf{V}),$$

also

$$f(\mathbf{V},0) = 0,$$

und für $\mathbf{U} = \mathbf{V} = 0$

$$f(\mathbf{T}, 0) + f(\mathbf{T}, 0) = f(0, \mathbf{T}) + 0,$$

also

$$f(0, \mathbf{T}) = 2 \bullet f(\mathbf{T}, 0) = 0.$$

Wir können f in der Gestalt

$$f(\mathbf{T}, \mathbf{U}) = \sum_{0 \le h \le d} c_h \bullet \mathbf{T}^h \bullet \mathbf{U}^{d-h} \text{ mit } c_0 = c_d = 0.$$

schreiben. Die Summe werde dabei über alle n-Tupel h nicht-negativer ganzer Zahlen erstreckt, die den angegebenen Bedingungen genügen. Für

$$h = (h_1,...,h_n)$$

sei dabei

$$T^h := T_1^{h_1} \bullet ... \bullet T_n^{h_n} \text{ und } \mathbf{U}^{d-h} = U_1^{d_1-h_1} \bullet ... \bullet U_n^{d_n-h_n}.$$

Für

$$i = (i_1,...,i_n) \text{ und } j = (j_1,...,j_n)$$

bedeute

$$i \le j,$$

daß $i_\nu \le j_\nu$ für $\nu = 1,...,n$ gilt. Außerdem bedeute

$$i < j,$$

daß $i \le j$ und $i \ne j$ gilt. Wir werden weiter die folgenden Bezeichnungen verwenden,

$$|i| := i_1+...+i_n$$

$$i! := (i_1)! \bullet ... \bullet (i_n)!$$

$$\binom{m}{i} := \frac{m!}{i! \bullet (m-i)!}$$

so daß gilt

$$(\mathbf{T}+\mathbf{U})^m = (T_1+U_1)^{m_1} \bullet ... \bullet (T_n+U_n)^{m_n}$$

$$= \Big(\sum_{i_1+j_1=m_1} \frac{(m_1)!}{(i_1)! \bullet (j_1)!} \bullet T_1^{i_1} \bullet U_1^{j_1}\Big) \bullet ... \bullet \Big(\sum_{i_n+j_n=m_n} \frac{(m_n)!}{(i_n)! \bullet (j_n)!} \bullet T_n^{i_n} \bullet U_n^{j_n}\Big)$$

$$= \sum_{i+j=m} \frac{m!}{i! \bullet j!} \mathbf{T}^i \mathbf{U}^j$$

$$= \sum_{i+j=m} \binom{i+j}{i} \mathbf{T}^i \mathbf{U}^j$$

Wir vergleichen die Koeffizienten von $\mathbf{T}^h\mathbf{U}^i\mathbf{V}^j$ auf beiden Seiten von (1).
Der in $f(\mathbf{U},\mathbf{V})$ ist gleich $\delta_{h,0}\cdot c_j$, der in $f(\mathbf{T},\mathbf{U})$ ist gleich $\delta_{j,0}\cdot c_h$, der in

$$\begin{aligned} f(\mathbf{T}+\mathbf{U},\mathbf{V}) &= \sum_{\nu+j=d} c_\nu \cdot (\mathbf{T}+\mathbf{U})^\nu \cdot \mathbf{V}^j \\ &= \sum_{\nu+j=d} c_\nu \cdot \sum_{h+i=\nu} \binom{\nu}{h} \mathbf{T}^h \cdot \mathbf{U}^i \cdot \mathbf{V}^j \\ &= \sum_{h+i+j=d} c_{h+i} \cdot \binom{h+i}{h} \mathbf{T}^h \cdot \mathbf{U}^i \cdot \mathbf{V}^j \end{aligned}$$

ist

$$c_{h+i} \cdot \binom{h+i}{h},$$

und der in

$$\begin{aligned} f(\mathbf{U}+\mathbf{V},\mathbf{T}) &= \sum_{\nu+h=d} c_\nu \cdot (\mathbf{U}+\mathbf{V})^\nu \cdot \mathbf{T}^h \\ &= \sum_{\nu+h=d} c_\nu \cdot \sum_{i+j=\nu} \binom{\nu}{i} \mathbf{U}^i \cdot \mathbf{V}^j \cdot \mathbf{T}^h \\ &= \sum_{i+j+h=d} c_{i+j} \cdot \binom{i+j}{i} \mathbf{T}^h \cdot \mathbf{U}^i \cdot \mathbf{V}^j \end{aligned}$$

ist

$$c_{i+j} \cdot \binom{i+j}{i}.$$

Bedingung (1) bekommt damit die Gestalt

$$\binom{h+i}{h} \cdot c_{h+i} + \delta_{j,0} \cdot c_h = \binom{i+j}{j} \cdot c_{i+j} + \delta_{h,0} \cdot c_j \text{ für } h+i+j = d. \qquad (2)$$

Für $j = 0$ ist $i+h = d$, also $i = d-h$. Wir erhalten

$$\binom{d}{h} \cdot c_d + c_h = c_{d-h} + \delta_{h,0} \cdot c_0$$

und wegen $c_0 = c_d = 0$ folgt

$$c_h = c_{d-h}, \qquad (3)$$

Seien jetzt $0 < h, j < d$. Wegen $h+i = d- j$ und $i+j = d-h$ folgt dann aus (2)

$$\binom{d-j}{h} \cdot c_{d-j} = \binom{d-h}{j} \cdot c_{d-h}$$

also zusammen mit (3)

$$\binom{d-j}{h} \cdot c_j = \binom{d-h}{j} \cdot c_h \qquad (4)$$

für $0 < h, j < d$.
Wir die Charakteristik des Grundkörpers gleich 0 ist, können wir die beiden Quotienten

$$\binom{d}{h} / \binom{d-j}{h} = \frac{d!}{h!\cdot(d-h)!} / \frac{(d-j)!}{h!\cdot(d-j-h)!} = \frac{d!\cdot(d-h-j)!}{(d-j)!\cdot(d-h)!}$$

und

$$\binom{d}{j} / \binom{d-h}{j} = \frac{d!}{j!\cdot(d-j)!} / \frac{(d-h)!}{j!\cdot(d-h-j)!} = \frac{d!\cdot(d-h-j)!}{(d-j)!\cdot(d-h)!}.$$

bilden. Sie sind gleich. Indem wir (4) mit diesen Quotienten multiplizieren, erhalten wir

$$\binom{d}{h}\bullet c_j = \binom{d}{j}\bullet c_h \qquad (5)$$

für $0 < h, j < d$. Damit gilt

$$\begin{aligned} c_j\bullet((\mathbf{T}+\mathbf{U})^d - \mathbf{T}^d - \mathbf{U}^d) &= \sum_{0\le h\le d} c_j\bullet\binom{d}{h}\mathbf{T}^h\bullet\mathbf{U}^{d-h} - c_j\bullet\mathbf{T}^d - c_j\bullet\mathbf{U}^d \\ &= \sum_{0<h<d} c_j\bullet\binom{d}{h}\mathbf{T}^h\bullet\mathbf{U}^{d-h} \\ &= \sum_{0<h<d} c_h\bullet\binom{d}{j}\mathbf{T}^h\bullet\mathbf{U}^{d-h} \qquad \text{(wegen (5))} \\ &= \binom{d}{j}\bullet\sum_{0<h<d} c_h\bullet\mathbf{T}^h\bullet\mathbf{U}^{d-h} \\ &= \binom{d}{j}\bullet f(\mathbf{T},\mathbf{U}) \qquad \text{(wegen } c_0 = c_d = 0) \end{aligned}$$

Für $j = (0,...,1,...,0) = e_i$ ergibt sich

$$c_j\bullet((\mathbf{T}+\mathbf{U})^d - \mathbf{T}^d - \mathbf{U}^d) = d_i\bullet f(\mathbf{T},\mathbf{U}).$$

Falls d != 0 ist, könne wir i so wählen, daß $d_i \neq 0$ ist, und

$$f(\mathbf{T},\mathbf{U}) = (c_{e_i}/d_i)\bullet((\mathbf{T}+\mathbf{U})^d - \mathbf{T}^d - \mathbf{U}^d)$$

gilt, d.h. die Behauptung gilt mit $g(\mathbf{T}) := (c_{e_i}/d_i)\bullet\mathbf{T}^d$. Im Fall d = 0 ist

$$f(\mathbf{T},\mathbf{U}) = \sum_{0\le h\le 0} c_h\bullet\mathbf{T}^h\bullet\mathbf{U}^{d-h}$$

identisch 0 (wegen $c_0 = c_d = 0$), und die Behauptung gilt mit $g(\mathbf{T}) = 0$.

Zu (ii) und (iii).

1. Schritt. Konstruktion von F-Algebra-Homomorphismen

$$\psi^{\mathbf{T}}_{q,n}: F[\mathbf{T}] \longrightarrow F[T]$$

$$\psi^{\mathbf{T}}_{q,n}\otimes\psi^{\mathbf{U}}_{q,n}: F[\mathbf{T},\mathbf{U}] \longrightarrow F[T,U]$$

$$\psi := \psi^{\mathbf{T}}_{q,n}\otimes\psi^{\mathbf{U}}_{q,n}\otimes\psi^{\mathbf{V}}_{q,n}: F[\mathbf{T},\mathbf{U},\mathbf{V}] \longrightarrow F[T,U,V],$$

welche in kleinen Graden Isomorphismen sind.

Wir beweisen die Aussagen mit Hilfe der entsprechenden Aussagen von 3.4.4. Dazu verwenden wir die q-adischen Entwicklungen der nicht-negativen ganzen Zahlen bezüglich einer gegebenen Basis q.

Bezeichne

$$\mathbf{N}$$

die Menge der nicht-negativen ganzen Zahlen. Dann ist für jede natürliche Zahl $q \geq 2$ und jede natürliche Zahl r die Abbildung

$$\varphi_{q,r}: [0,q)^r \bigcap \mathbf{N}^{r+1} \overset{\cong}{\longrightarrow} [0,q^r)\bigcap\mathbf{N},$$

$$(\ell_1,...,\ell_r) \mapsto \ell_1 + \ell_2\bullet q + \ell_3\bullet q^2 + ... + \ell_r\bullet q^{r-1}$$

bijektiv. Für jedes Polynom

$$G \in F[T]$$

bezeichne

$$d_{\mathbf{T}}(G) := \max\{\deg_{T_1} G,\ldots,\deg_{T_n} G\}$$

das Maximum der Grade von G als Polynom einer der Unbestimmten T_i. Die Einschränkung des F-Algebra-Homomorphismus

$$\psi^{\mathbf{T}}_{q,n}:F[\mathbf{T}] \longrightarrow F[T],\ f(\mathbf{T}) \mapsto f(T,T^q,T^{q^2},\ldots,T^{q^{n-1}}),$$

auf den F-linearen Unterraum

$$F[\mathbf{T}]_{<q} = \{G \in F[\mathbf{T}] \mid \deg_{T_i} G < q \text{ für } i = 1,\ldots,n\}$$

der Polynome G mit $d_{\mathbf{T}}(G) < q$ induziert dann einen F-linearen Isomorphismus

$$\psi^{\mathbf{T}}_{q,n}|_{F[\mathbf{T}]_{<q}}:F[\mathbf{T}]_{<q} \xrightarrow{\cong} F[T]_{<q^n}, \tag{6}$$

auf den F-linearen Unterraum der Polynome vom Grad $< q^r$. Man beachte, $F[\mathbf{T}]_{<q}$ besitzt die Potenzprodukte

$$T^{\boldsymbol{\ell}} = T_1^{\ell_1}\bullet\ldots\bullet T_n^{\ell_n} \text{ mit } \ell_\nu < q$$

als Basis. Das Bild dieser Basis-Elemente ist gerade die Menge der Potenzen

$$\begin{aligned}\psi^{\mathbf{T}}_{q,n}(T^{\boldsymbol{\ell}}) &= \psi^{\mathbf{T}}_{q,n}(T_1^{\ell_1}\bullet\ldots\bullet T_n^{\ell_n})\\ &= T^{\ell_1}\bullet(T^q)^{\ell_2}\bullet\ldots\bullet(T^{q^{n-1}})^{\ell_n}\\ &= T^{\ell_1+\ell_2\bullet q+\ell_3\bullet q^2+\ldots+\ell_n\bullet q^{n-1}}\\ &= T^{\varphi_{q,n}(\boldsymbol{\ell})}\end{aligned}$$

von T des Grades $< q^n$ (wegen der Surjektivität von $\varphi_{q,n}$). Wegen der Bijektivität von $\varphi_{q,n}$ bildet $\psi^{\mathbf{T}}_{q,n}$ eine Basis von $F[\mathbf{T}]_{<q}$ bijektiv auf eine Basis von $F[T]_{<q^n}$ ab, d.h. die Einschränkung (6) ist ein F-linearer Isomorphismus.

Sei jetzt q eine Potenz der Charakteristik p (>0) von F mit

$$q > d_{\mathbf{T},\mathbf{U}}(f(T,U))$$

Der F-Algebra-Homomorphismus

$$\psi^{\mathbf{T}}_{q,n}\otimes\psi^{\mathbf{U}}_{q,n}:F[\mathbf{T},\mathbf{U}] = F[\mathbf{T}]\otimes_F F[\mathbf{U}] \longrightarrow F[T]\otimes_F F[U] = F[T,U],$$

$$f(\mathbf{T},\mathbf{U}) \mapsto f(T,T^q,T^{q^2},\ldots,T^{q^{n-1}},\ U,U^q,U^{q^2},\ldots,U^{q^{n-1}}),$$

induziert dann einen F-linearen Isomorphismus

$$F[\mathbf{T},\mathbf{U}]_{<q} = F[\mathbf{T}]_{<q}\otimes_F F[\mathbf{U}]_{<q} \longrightarrow F[T]_{<q^n}\otimes_F F[U]_{<q^n} = F[T,U]_{<q^n}. \tag{7}$$

Analog induziert der F-Algebra-Homomorphismus

$$\psi := \psi^{\mathbf{T}}_{q,n}\otimes\psi^{\mathbf{U}}_{q,n}\otimes\psi^{\mathbf{V}}_{q,n}:F[\mathbf{T},\mathbf{U},\mathbf{V}] \longrightarrow F[T,U,V]$$

einen F-linearen Isomorphismus

$$F[\mathbf{T},\mathbf{U},\mathbf{V}]_{<q} \longrightarrow F[T,U,V]_{<q^n}. \tag{8}$$

Wegen von $q > d_{\mathbf{T},\mathbf{U}}(f(T,U))$ liegt $f(\mathbf{T},\mathbf{U})$ im Definitionsbereich des Isomorphismus (7).

2. Schritt. $\psi(f)$ ist ein Kozyklus, d.h. $\partial(\psi(f)) = 0$.
Es reicht zu zeigen,

$$\partial(\psi(f)) = \psi(\partial f), \tag{9}$$

denn wegen $\partial f = 0$ und weil ψ ein F-Algebra-Homomorphismus ist, ist die rechte Seite gleich 0 (also mit (9) auch die linke). Nach Definition von ∂ und ψ sind beide Seiten von (9) k-lineare Funktionen in f. Weil f eine Linearkombination von Potenzprodukten der Gestalt $\mathbf{T}^i\mathbf{U}^j$ ist, reicht es zu zeigen,

$$\partial(\psi(\mathbf{T}^i\mathbf{U}^j)) = \psi(\partial(\mathbf{T}^i\mathbf{U}^j)). \tag{10}$$

Nach Definition gilt

$$\partial(\mathbf{T}^i\mathbf{U}^j) = \mathbf{U}^i\mathbf{V}^j - (\mathbf{T}+\mathbf{U})^i\mathbf{V}^j + (\mathbf{U}+\mathbf{V})^i\mathbf{T}^j - \mathbf{T}^i\mathbf{U}^j.$$

Weil ψ ein F-Algebra-Homomorphismus ist, folgt

$$\begin{aligned}
\psi(\partial(\mathbf{T}^i\mathbf{U}^j)) &= \psi(\mathbf{U}^i)\,\psi(\mathbf{V}^j) - \psi((\mathbf{T}+\mathbf{U})^i)\,\psi(\mathbf{V}^j) + \psi((\mathbf{U}+\mathbf{V})^i)\,\psi(\mathbf{T}^j)) - \psi(\mathbf{T}^i)\psi(\mathbf{U}^j) \\
&= \psi(\mathbf{U}^i)\,\psi(\mathbf{V}^j) \\
&\quad - \psi\Big(\prod_{\nu=1}^{n}(T_\nu+U_\nu)^{i_\nu}\Big)\,\psi(\mathbf{V}^j) \\
&\quad + \psi\Big(\prod_{\nu=1}^{n}(U_\nu+V_\nu)^{i_\nu}\Big)\,\psi(\mathbf{T}^j)) \\
&\quad - \psi(\mathbf{T}^i)\psi(\mathbf{U}^j) \\
&= \psi(\mathbf{U}^i)\,\psi(\mathbf{V}^j) \\
&\quad - \prod_{\nu=1}^{n}(\psi(T_\nu)+\psi(U_\nu))^{i_\nu}\,\psi(\mathbf{V}^j) \\
&\quad + \prod_{\nu=1}^{n}(\psi(U_\nu)+\psi(V_\nu))^{i_\nu}\,\psi(\mathbf{T}^j)) \\
&\quad - \psi(\mathbf{T}^i)\psi(\mathbf{U}^j) \\
&= U^{\varphi_{q,n}(i)}V^{\varphi_{q,n}(j)} \\
&\quad - \prod_{\nu=1}^{n}(T^{q^{\nu-1}}+U^{q^{\nu-1}})^{i_\nu\bullet}V^{\varphi_{q,n}(j)} \\
&\quad + \prod_{\nu=1}^{n}(U^{q^{\nu-1}}+V^{q^{\nu-1}})^{i_\nu\bullet}T^{\varphi_{q,n}(j)} \\
&\quad - T^{\varphi_{q,n}(i)}U^{\varphi_{q,n}(j)}
\end{aligned}$$

Weil q eine große Potenz der Charakteristik p (>0) des Körpers F ist, erhalten wir damit

$$\psi(\partial(\mathbf{T}^i\mathbf{U}^j)) = U^{\varphi_{q,n}(i)}V^{\varphi_{q,n}(j)}$$

$$
\begin{aligned}
&\quad - \prod_{\nu=1}^{n} (T+U)^{i_\nu \cdot q^{\nu-1}} \cdot V^{\varphi_{q,n}(j)} \\
&\quad + \prod_{\nu=1}^{n} (U+V)^{i_\nu \cdot q^{\nu-1}} \cdot T^{\varphi_{q,n}(j)} \\
&\quad - T^{\varphi_{q,n}(i)} U^{\varphi_{q,n}(j)} \\
&= U^{\varphi_{q,n}(i)} V^{\varphi_{q,n}(j)} \\
&\quad - (T+U)^{\varphi_{q,n}(i)} \cdot V^{\varphi_{q,n}(j)} \\
&\quad + (U+V)^{\varphi_{q,n}(i)} \cdot T^{\varphi_{q,n}(j)} \\
&\quad - T^{\varphi_{q,n}(i)} U^{\varphi_{q,n}(j)} \\
&= \partial(T^{\varphi_{q,n}(i)} U^{\varphi_{q,n}(j)}) \\
&= \partial(\psi(\mathbf{T}^i) \cdot \psi(\mathbf{U}^j)) \\
&= \partial(\psi(\mathbf{T}^i \mathbf{U}^j)).
\end{aligned}
$$

Bemerkungen.

(i) Die obige Rechnung läßt sich etwas abkürzen, wenn man beachtet, daß

$$(\mathbf{T}+\mathbf{U})^i = \sum_{0 \le \alpha \le i} \binom{i}{\alpha} \cdot \mathbf{T}^\alpha \cdot \mathbf{U}^{i-\alpha}$$

$$(T+U)^{\varphi_{q,n}(i)} = \sum_{0 \le \varphi_{q,n}(\alpha) \le \varphi_{q,n}(i)} \binom{\varphi_{q,n}(i)}{\varphi_{q,n}(\alpha)} \cdot \mathbf{T}^{\varphi_{q,n}(\alpha)} \cdot U^{\varphi_{q,n}(i-\alpha)}$$

und

$$\binom{\varphi_{q,n}(i)}{\varphi_{q,n}(\alpha)} \equiv \binom{i}{\alpha} \pmod{p}$$

gilt (vgl. 3.4.2 (i)).

(ii) Genaugenommen braucht man eine Verallgemeinerung von 3.4.2 (i), in welcher anstelle der Koeffizienten m_i, n_i der p-adischen Entwicklungen von m und n die der $q = p^\ell$-adischen Entwicklungen betrachtet werden. Den Beweis erhält man aus dem von 3.4.2 (i), indem man an allen Stellen, an denen p im Exponenten auftritt, p durch $q = p^\ell$ ersetzt.

3. Schritt.

Nach dem zweiten Schritt und nach 3.4.4 (ii) gibt es ein Polynom $\tilde{g}(T) \in F[T]$ und Elemene $a_i \in F$ mit

$$\psi(f) = \tilde{g}(T+U) - \tilde{g}(T) - \tilde{g}(U) + \sum_i a_i \cdot c(T,U)^{p^i}$$

$$= \tilde{g}(T+U) - \tilde{g}(T) - \tilde{g}(U) + \sum_i a_i \bullet C_p(T^{p^i}, U^{p^i}) \qquad \text{(Bemerkung 3.4.3 (v))}$$

Dabei können wir auf der rechten Seite alle homogenen Komponenten der auftretenden Polynome weglassen, welche in $\psi(f)$ nicht vorkommen, d.h. wir können $\tilde{g}$ und die Koeffizienten a_i so wählen, daß alle Summanden $\tilde{g}(T'+U)$, $\tilde{g}(T)$, $\tilde{g}(U)$, $a_i \bullet c(T,U)^{p^i}$ auf der rechten Seite im Bild der Abbildung (7) liegen. Zum Beispiel ist dann

$$a_i \bullet C_p(T^{p^i}, U^{p^i}) = \psi(a_i \bullet C_p(T_{i+1}, U_{i+1})).$$

Weil nach dem zweiten Schritt $\partial(\psi(f)) = 0$ gilt, ist das Absolutglied von f gleich Null. Weil dies auch für die $C_p(T^{p^i}, U^{p^i})$ gilt, ist auch das Absolutglied von $\tilde{g}$ gleich Null.

Wir wählen ein $g(\mathbf{T}) \in F[\mathbf{T}]$ mit

$$\tilde{g}(T) = \psi(g(\mathbf{T})). \qquad (11)$$

Es gilt dann auch

$$\tilde{g}(U) = \psi(g(\mathbf{U})) \text{ und } \tilde{g}(T+U) = \psi(g(\mathbf{T}+\mathbf{U}))$$

(man ersetze jedes T_i auf der rechten Seite von (11) durch U_i bzw. durch T_i+U_i). Außerdem ist das Absolutglied von g gleich Null, und es gilt

$$\psi(f - g(\mathbf{T}+\mathbf{U}) + g(\mathbf{T}) + g(\mathbf{U}) - \sum_i a_i \bullet C_p(T_{i+1}, U_{i+1})) = 0,$$

Weil die Einchränkung von ψ auf den Definitonsbereich der Abbildung (7) injektiv ist (ψ stimmt dort mit (7) überein), folgt

$$f - g(\mathbf{T}+\mathbf{U}) + g(\mathbf{T}) + g(\mathbf{U}) - \sum_i a_i \bullet C_p(T_{i+1}, U_{i+1}) = 0,$$

also

$$f(\mathbf{T},\mathbf{U}) = g(\mathbf{T}+\mathbf{U}) - g(\mathbf{T}) - g(\mathbf{U}) + \sum_i a_i \bullet C_p(T_{i+1}, U_{i+1}),$$

d.h. es gilt (ii).

Zu (iii). Die Argumentation ist im wesentlichen dieselbe wie im Beweis von 3.4.4 (iii).

1. Schritt. Für jedes Polynom $g(\mathbf{T}) \in F[\mathbf{T}]$ ohne Absolutglied gilt

$$\sum_{i=1}^{p-1} (g(\mathbf{T}+i\mathbf{T}) - g(\mathbf{T}) - g(i\mathbf{T})) = 0.$$

Die Summe auf der linken Seite hängt F-linear von g ab. Es reicht deshalb, die Identität im Fall

$$g(\mathbf{T}) = \mathbf{T}^m \text{ mit } m \neq (0,\ldots,0)$$

zu beweisen. Es gilt dann

$$\sum_{i=1}^{p-1} (g(\mathbf{T}+i\mathbf{T}) - g(\mathbf{T}) - g(i\mathbf{T})) = \sum_{i=1}^{p-1} ((\mathbf{T}+i\mathbf{T})^m - \mathbf{T}^m - (i\mathbf{T})^m)$$

$$= \sum_{i=1}^{p-1} ((1+i)\mathbf{T})^m - \sum_{i=1}^{p-1} \mathbf{T}^m - \sum_{i=1}^{p-1} (i\mathbf{T})^m$$

$$= \sum_{i=1}^{p-1} (1+i)^{|m|}\mathbf{T}^m - \sum_{i=1}^{p-1} \mathbf{T}^m - \sum_{i=1}^{p-1} i^{|m|}\mathbf{T}^m$$
$$= \sum_{i=2}^{p} i^{|m|}\mathbf{T}^m - \sum_{i=1}^{p-1} \mathbf{T}^m - \sum_{i=1}^{p-1} i^{|m|}\mathbf{T}^m$$
$$= p^{|m|}\mathbf{T}^m - (p-1)\mathbf{T}^m - 1^{|m|}\mathbf{T}^m$$
$$= (p^{|m|} - (p-1) - 1)\mathbf{T}^m$$
$$= (p^{|m|} - p)\mathbf{T}^m$$
$$= p\bullet(p^{|m|-1}-1)\bullet\mathbf{T}^m \qquad \text{(es gilt } m \neq (0,...,0))$$
$$= 0 \qquad \text{(p ist die Charakteristik von F).}$$

2. Schritt. Beweis der Behauptung.
Wir haben zu zeigen, in der Formel

$$f(\mathbf{T},\mathbf{U}) = g(\mathbf{T}+\mathbf{U})-g(\mathbf{T})-g(\mathbf{U}) + \sum_{j=0}^{n-1} a_j\bullet C_p(T_{j+1},U_{j+1})$$

von Aussage (ii) sind alle a_i gleich Null. Nach Voraussetzung gilt

$$\sum_{i=1}^{p-1} f(\mathbf{T}, i\mathbf{T}) = 0.$$

Zusammen mit dem ersten Schritt folgt

$$0 = \sum_{i=1}^{p-1}\sum_{j=0}^{n-1} a_j\bullet C_p(T_{j+1},iT_{j+1}) = \sum_{j=0}^{n-1} a_j\bullet \sum_{i=1}^{p-1} C_p(T_{j+1},iT_{j+1})$$

Nach dem zweiten Schritt im Beweis von 3.4.4 (iii) ist dies äquivalent zu

$$0 = \sum_{j=0}^{n-1} a_j\bullet (p^{p-1} - 1)\, T^p_{j+1}.$$

Weil die Charakteristik von F gleich p ist, folgt

$$0 = \sum_{j=0}^{n-1} a_j\bullet T^p_{j+1},$$

also $a_0 = a_1 = ... = a_{n-1} = 0$.
QED.

3.4.7 Kriterium für elementare unipotente Gruppen

Sei G eine lineare algebraische Gruppe über dem Körper k der Charakteristik p. Dann sind folgende Aussagen äquivalent.

(i) G ist elementar unipotent.
(ii) $\mathcal{A}$(G) ist ein endlich erzeugter R(k)-Modul und die Elemente von $\mathcal{A}$(G) erzeugen k[G] als k-Algebra.
(iii) G ist im Fall p = 0 eine Vektorgruppe und im Fall p > 0 ein Produkt aus einer Vektorgruppe und einer endlichen elementaren abelschen p-Gruppe.

Unter einer elementaren abelschen p-Gruppe verstehen wir ein Produkt von zyklischen Gruppen der Ordnung p.

Beweis. (iii) ⇒ (i). Wir erinnern zunächst an zwei früher bewiesene Aussagen. Es bestehen die folgenden Implikationen.

Aussage 1. G ist unipotent ⇔ G ist isomorph zu einer abgeschlossenen Untergruppe einer $\mathbf{U}_n$

Die Implikation '⇐' ist trivial, weil alle Elemente von

$$\mathbf{U}_n = \{ \begin{pmatrix} 1 & c_{12} & c_{13} & \dots & c_{1,n-1} & c_{1n} \\ 0 & 1 & c_{23} & \dots & c_{2,n-1} & c_{2n} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & c_{n-1,n} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \mid c_{ij} \in k \}$$

unipotent sind. Die Implikation '$\Rightarrow$' folgt aus 2.3.7 und 2.4.12B.

Aussage 2.
Das Produkt zweier unipotenter Gruppen ist unipotent.

Die Aussage ergibt sich aus Aussage 1 und der Tatsache, daß der injektive Homomorphismus von linearen algebraischen Gruppen

$$\mathbf{U}_m \times \mathbf{U}_n \hookrightarrow \mathbf{U}_{m+n}\ ,\ (A,B) \mapsto \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix}$$

das direkte Produkt links mit einer abgeschlossenen Untergruppe von $\mathbf{U}_{m+n}$ identifiziert.

Beweisen wir die Implikation (iii) $\Rightarrow$ (i).

1. Schritt. Der Fall $p = 0$.

Nach Voraussetzung ist $G \cong \mathbf{G}_a^n$ (vgl. 3.4.1). Wegen des Isomorphismus

$$\mathbf{G}_a \xrightarrow{\cong} \mathbf{U}_1,\ c \mapsto \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix},$$

von linearen algebraischen Gruppen ist $\mathbf{G}_a$ unipotent. Nach Aussage 2 ist auch

$$G \cong \mathbf{G}_a^n = \mathbf{G}_a \times \dots \times \mathbf{G}_a$$

unipotent. Nun ist $\mathbf{G}_a^n$ gerade die additive Gruppe des k-Vektorraums k^n also insbesonere kommutativ. Zusammen ergibt sich, daß G elementar unipotent ist.

2. Schritt. Der Fall $p > 0$.

Nach Vorausetzung ist

$$G \cong \mathbf{G}_a^n \times H$$

mit einem Produkt H von endlich vielen (sagen wir r) Gruppen der Ordnung p, d.h.

$$G \cong \mathbf{G}_a^n \times (\mathbb{Z}/p\mathbb{Z})^r = (\mathbb{Z}/p\mathbb{Z}) \times \dots \times (\mathbb{Z}/p\mathbb{Z})$$

Die additive Gruppe $\mathbb{Z}/p\mathbb{Z}$ ist die additive Gruppe des Körpers $\mathbb{F}_p$ mit p Elementen, d.h. des Primkörpers von k. Die natürliche Inklusion $\mathbb{F}_p \hookrightarrow k$ identifiziert $\mathbb{Z}/p\mathbb{Z}$ mit einer endlichen Untergruppe der additiven Gruppe $\mathbf{G}_a$ von k,

$$\mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbf{G}_a \cong \mathbf{U}_1$$

Weil jede endliche Teilmenge einer algebraischen Varietät abgeschlossen ist, wird so $\mathbb{Z}/p\mathbb{Z}$ mit einer abgeschlossenen Untergruppe von $\mathbf{U}_1$ identifiziert. Insbesondere ist $\mathbb{Z}/p\mathbb{Z}$ eine unipotente Gruppe. Als Produkt unipotenter Gruppen (die isomorph zu $\mathbf{G}_a$ oder $\mathbb{Z}/p\mathbb{Z}$ sind) ist

G unipotent.

Als Produkt abelscher Gruppen ist G abelsch. Als additive Gruppe von

$$k^n \times (\mathbb{F}_p)^r$$

ist G elementar unipotent (weil das p-fache jedes (n+r)-Tupels das neutrale Element ist).

(ii) $\Rightarrow$ (iii) im Fall, daß G zusammenhängend ist.

Nach Voraussetzung ist $\mathcal{A}(G)$ ein endlich erzeugter R(k)-Modul. Weil G zusammenhängend ist, ist $\mathcal{A}(G)$ als R(k)-Modul torsionsfrei (nach 3.3.6 (i)). Als algebraisch abgeschlossener Körper ist k perfekt. Deshalb ist $\mathcal{A}(G)$ (nach 3.3.3 (iii)) als R(k)-Modul eine direkte Summe von (endlich vielen) zyklischen R(k)-Moduln und sogar frei über R(k), sagen wir

$$\mathcal{A}(G) = R(k)\bullet f_1 + \ldots + R(k)\bullet f_m \text{ mit } f_1,\ldots,f_m \text{ linear unabhängig über } R(k).$$

Nach 3.3.6 (ii) sind

$$f_1,\ldots,f_m \text{ algebraisch unabhängig über k.}$$

Nach Voraussetzung wird k[G] von den Elementen von $\mathcal{A}(G)$ erzeugt, d.h. im Fall $p \neq 0$ von den Elementen der Gestalt

$$T^j \bullet f_i = f_i^{p^j},\ i=1,\ldots,m,\ j = 0,1,2,\ldots$$

(vgl. 3.3.4 A) und im Fall $p = 0$ von den $f_1,\ldots,f_m$. Damit hat der Koordinatenring von G die Gestalt

$$k[G] = k[f_1,\ldots,f_m]$$

mit algebraisch unabhängigen additiven Funktionen f_i, d.h. Homomorphismen von linearen algebraischen Gruppen $f_i: G \longrightarrow G_a$. Weil die f_i den Koordinatenring erzeugen, ist durch

$$f: G \xrightarrow{\cong} X \subseteq k^m,\ x \mapsto \begin{pmatrix} f_1(x) \\ \ldots \\ f_m(x) \end{pmatrix},$$

ein Isomorphismus von affinen algebraischen Varietäten definiert (vgl. Bemerkung 1.3.1 (iii)) mit sagen wir

$$X = V(g_1,\ldots,g_s),\ g_i \in k[T_1,\ldots,T_m].$$

Weil die f_i algebraisch unabhängig sind, müssen alle g_i identisch Null sein, d.h. $X = k^m$ und f ist ein Isomorphismus

$$f: G \xrightarrow{\cong} k^m = \mathbf{G}_a^m$$

Weil die f_i additive Funktionen sind, ist es sogar ein Isomorphismus von linearen algebraischen Gruppen, d.h. G ist eine Vektorgruppe, d.h. es gilt (iii).

(i) $\Rightarrow$ (ii) im Fall, daß G zusammenhängend ist.

Nach Aussage 1 können wir annehmen G ist eine abgeschlossene Untergruppe einer der Gruppen $\mathbf{U}_m$,

$$G \subseteq \mathbf{U}_m = \left\{ \begin{pmatrix} 1 & x_{12} & x_{13} & \dots & x_{1,m-1} & x_{1m} \\ 0 & 1 & x_{23} & \dots & x_{2,m-1} & x_{2m} \\ \dots & \dots & \dots & \dots & \dots & 0 \\ 0 & 0 & 0 & \dots & 1 & x_{m-1,m} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix} \Big| \; x_{ij} \in k \right\}$$

Wir führen den Beweis durch Induktion nach m.
Induktionsanfang: m = 1.
Es gilt dann $G = \mathbf{U}_1 = \{e\}$, k[G] = k, also $\mathcal{A}(G) =^{34} 0$. Insbesondere ist $\mathcal{A}(G)$ ein endlich erzeugter R(k)-Modul. Trivialerweise wird k[G] = k als k-Algebra von $\mathcal{A}(G)$ erzeugt: k ist die kleineste k-Algebra, in der $\mathcal{A}(G)$ enthalten ist.
Induktionsschritt: m > 1.
Wir betrachten die beiden folgenden Abbildungen.

$$\varphi: \mathbf{U}_m \twoheadrightarrow \mathbf{U}_{m-1}, A \mapsto A',$$

wobei A' aus A entstehe durch Streichen der ersten Zeile und ersten Spalte, und

$$\psi: \mathbf{U}_m \twoheadrightarrow \mathbf{U}_{m-1}, A \mapsto A'',$$

wobei A'' aus A entstehe durch Streichen der letzten Zeile und letzten Spalte. Beide Abbildungen sind regulär,

$$\varphi \text{ und } \psi \text{ sind reguläre Abbildungen,}$$

denn die Einträge von A' und A'' sind reguläre Funktionen der Einträge von A. Beide Abbildungen sind surjektiv,

$$\varphi \text{ und } \psi \text{ sind sind surjektiv,}$$

denn indem man A' durch eine erste Zeile und eine erste Spalte ergänzt, wobei der einzige von 0 verschiedene neue Eintrag sich in der Position (1,1) befindet und gleich 1 ist, erhält man zu vorgegebenen A' eine Matrix A mit $\varphi(A) = A'$. Indem man analog A'' durch eine letzte Zeile und eine letzte Spalte ergänzt, wobei nur der Eintrag in der Position (m,m) von 0 verschieden ist (und gleich 1 ist), findet man auch ein Urbild von A'' bei ψ. Schließlich sind

$$\varphi \text{ und } \psi \text{ Gruppenhomomorphismen.}$$

Wenn man nämlich die i-te Zeile eines Elements von $\mathbf{U}_m$ mit der j-ten Spalte eines Elements von $\mathbf{U}_m$ multipliziert, so hängt das Ergebnis im Fall 1 < i nicht von den ersten Koordinaten der Faktoren ab[35] und im Fall j < m nicht von den letzten Koordinaten der Faktoren[36]. Zusammen erhalten wir,

$$\varphi \text{ und } \psi \text{ sind surjektive Homomorphismen linearer algebraischer Gruppen.}$$

Insbesondere sind die Bilder $\varphi(G)$ und $\psi(G)$ abgeschlossene Untergruppen von $\mathbf{U}_{m-1}$ (nach 2.2.5). Sie sind unipotent (weil sie ganz in $\mathbf{U}_{m-1}$ liegen). Sie sind elementar unipotent,

---

[34] Jede additive Funktion $f: G = \{e\} \longrightarrow k = G_a$ ist ein Homomorphismus der multiplikativen Gruppe G mit Werten in der additiven Gruppe G_a, d.h. es ist f(e) = 0 und die einzige additve Funktion auf G ist identisch Null

[35] denn die erste Koordinate des ersten Faktors ist im Fall 1 < i gleich 0.

[36] denn die letzte Koordinate des zweiten Faktors ist mit Fall j < m gleich 0.

$\varphi(G)$ und $\psi(G)$ sind sind elementar unipotent,

weil das homomorphe Bild einer abelschen Gruppe abelsch und (im Fall $p > 0$) das Bild eines Elements der Ordnung p die Ordnung p hat oder gleich dem neutralen Element ist.

Wir wenden die Induktionsvoraussetzung auf $\varphi(G)$ und $\psi(G)$ an und erhalten:

$$\begin{aligned} &\mathcal{A}(\varphi(G)) \text{ und } \mathcal{A}(\psi(G)) \text{ endlich erzeugte } R(k)\text{-Moduln,} \\ &\text{die } k[\varphi(G)] \text{ bzw. } k[\psi(G)] \text{ als k-Algebren erzeugen.} \end{aligned} \tag{1}$$

Weil die Abbildungen $\varphi: G \longrightarrow \varphi(G)$ und $\psi: G \longrightarrow \psi(G)$ surjektiv sind, induzieren sie Injektionen

$$k[\varphi(G)] \hookrightarrow k[G] \text{ und } k[\psi(G)] \hookrightarrow k[G]. \tag{2}$$

Wir können die Koordinatenringe von $\varphi(G)$ und $\psi(G)$ als Teilalgebren von $k[G]$ betrachten. Sei jetzt $x_{ij}: G \longrightarrow k$ die reguläre Abbildung, welche jede Matrix auf deren Eintrag in der Position (i,j) abbildet. Dann gilt (vgl. 2.2.2 Aufgabe 1)

$$k[G] = k[x_{ij} \mid 1 \le i < j \le m]$$

$$k[\varphi(G)] = k[x_{ij} \mid 2 \le i < j \le m]$$

$$k[\psi(G)] = k[x_{ij} \mid 1 \le i < j \le m-1]$$

Nach (1) werden $\mathcal{A}(\varphi(G))$ und $\mathcal{A}(\psi(G))$ über $R(k)$ von jeweils endlich vielen additiven Funktionen auf $\varphi(G)$ bzw. $\psi(G)$ erzeugt. Durch die natürlichen Einbettungen (2) werden diese zu additiven Funktionen auf G, es gibt also endlich viele additive Funktionen $a_1,...,a_n$ auf G mit

$$\mathcal{A}(\varphi(G)) + \mathcal{A}(\psi(G)) = R(k)\bullet a_1 + ... + R(k)\bullet a_n. \tag{3}$$

Dieser $R(k)$-Modul liegt ganz in $\mathcal{A}(G)$. Weil G nach Voraussetzung zusammenhängend ist, ist $\mathcal{A}(G)$ torsionsfrei (nach 3.3.6(i)). Damit ist aber auch der Teilmodul (3) torsionsfrei. Weil letzterer endlich erzeugt ist, ist er sogar frei über $R(k)$ (nach 3.3.3(iii), denn k ist als algebraisch abgeschlossener Körper perfekt). Wir können also annehmen,

$$a_1,...,a_n \text{ sind linear unabhängig über } R(k).$$

Nach 3.3.6(ii) sind dann die a_i algebraisch unabhängig über k,

$$a_1,...,a_n \text{ sind algebraisch unabhängig über k.} \tag{4}$$

Nach (1) erzeugen diese additiven Funktionen a_i eine k-Algebra, welche die Koordinatenringe von $\varphi(G)$ und $\psi(G)$ enthält,

$$k[\varphi(G)] \subseteq k[a_1,...,a_n] \text{ und } k[\psi(G)] \subseteq k[a_1,...,a_n]. \tag{5}$$

Insbesondere gilt

$$x_{ij} \in k[a_1,...,a_n] \ (\subseteq k[G]) \text{ für alle (i,j) mit } 2 \le i < j \le m \text{ oder } 1 \le i < j \le m-1.$$

Damit liegen alle x_{ij} in $k[a_1,...,a_n]$ mit eventueller Ausnahme des Falls $i = 1$ und $j = m$. Wir setzen

$$x := x_{1m}.$$

Für $u, v \in G$ gilt

$$\begin{pmatrix} 1 & x_{12}^{(uv)} & \dots & x_{1m}^{(uv)} \\ 0 & 1 & \dots & x_{2m}^{(uv)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} = \begin{pmatrix} 1 & x_{12}^{(u)} & \dots & x_{1m}^{(u)} \\ 0 & 1 & \dots & x_{2m}^{(u)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix} \bullet \begin{pmatrix} 1 & x_{12}^{(v)} & \dots & x_{1m}^{(v)} \\ 0 & 1 & \dots & x_{2m}^{(v)} \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 \end{pmatrix}$$

also

$$x_{1m}^{(uv)} = 1 \bullet x_{1m}^{(v)} + x_{12}^{(u)} \bullet x_{2m}^{(v)} + \dots + x_{1,m-1}^{(u)} \bullet x_{m-1,m}^{(v)} + x_{im}^{(u)} \bullet 1,$$

also

$$x^{(uv)} - x^{(v)} - x^{(u)} = x_{12}^{(u)} \bullet x_{2m}^{(v)} + \dots + x_{1,m-1}^{(u)} \bullet x_{m-1,m}^{(v)}$$

Unter den auf der rechten Seite auftretenden Funktionen $x_{ij}^{.}$ kommt x_{1m} nicht vor, d.h. diese $x_{ij}^{.}$ liegen in $k[a_1,\dots,a_n]$. Es gibt also ein Polynom $f(\mathbf{T},\mathbf{U}) \in k[\mathbf{T},\mathbf{U}]$ mit

$$x(uv) - x(u) - x(v) = f(a_1(u),\dots,a_n(u), a_1(v),\dots,a_n(v))$$

für beliebige $u, v \in G$. Im folgenden werden wir abkürzend

$$a(u) \text{ für } (a_1(u),\dots,a_n(u)$$

schreiben (für beliebige $u \in G$), so daß diese Identität die Gestalt

$$x(uv) - x(u) - x(v) = f(a(u), a(v))$$

bekommt.

Für beliebige $u, v, w \in G$ erhalten wir (vgl. 3.4.5)

$$\begin{aligned} (\partial f)(a(u), a(v), a(w)) &= f(a(v),a(w)) - f(a(u)+a(v),a(w))+f(a(u), a(v)+a(w))-f(a(u),a(v)) \\ &=^{37} f(a(v),a(w)) - f(a(uv),a(w))+f(a(u),a(vw))-f(a(u),a(v)) \\ &= x(vw)-x(v)-x(w) \\ &\quad -x(uvw)+x(uv)+x(w) \\ &\quad +x(uvw)-x(u)-x(vw) \\ &\quad -x(uv)+x(u)+x(v) \\ &= 0 \end{aligned}$$

Es gilt also

$$(\partial f)(a(u),a(v), a(w)) = 0 \text{ für beliebige } u, v, w \in G.$$

Wir betrachten die linke Seite dieser Identität als reguläre Funktion von

$$(u,v,w) \in G \times G \times G.$$

Bezeichnet $p_i: G\times G\times G \longrightarrow G$ die Projektion auf den i-ten Faktor, so gilt[38]

$$\begin{aligned} &(\partial f)(p_1^*(a), p_2^*(a), p_3^*(a))\ (u,v,w) \\ &\quad =^{39} (\partial f)(p_1^*(a)(u,v,w),\ p_2^*(a)\ (u,v,w),\ p_3^*(a)(u,v,w)) \\ &\quad = (\partial f)((a\circ p_1)(u,v,w),\ (a\circ p_2)(u,v,w),(a\circ p_3)(u,v,w)) \\ &\quad = (\partial f)(a(u), a(v), a(w)) \\ &\quad = 0. \end{aligned}$$

Als Elemente von $k[G\times G\times G] = k[G]\otimes_k k[G]\otimes_k k[G]$ sind die Funktionen $p_i^*(a_j)$ gerade die Tensorprodukte

---

[37] die a_ν sind additive Funktionen auf G.

[38] $p_i^*(a)$ steht hier abkürzend für $p_1^*(a_1),\dots, p_1^*(a_n)$

[39] Die Auswertung an der Stelle (u,v,w) ist ein k-Algebra-Homomorphismus.

$$p_1^*(a_.) = a_.\otimes 1\otimes 1$$
$$p_2^*(a_.) = 1\otimes a_.\otimes 1$$
$$p_3^*(a_.) = 1\otimes 1\otimes a_.$$

Sie liegen in der Teilalgebra

$$k[a_1,...,a_n]\otimes_k k[a_1,...,a_n]\otimes_k k[a_1,...,a_n]$$

und $(\partial f)(p_1^*(a), p_2^*(a), p_3^*(a))$ ist als Element dieser Teilalgebra gleich 0.
Nach (4) besteht ein k-Algebra-Isomorphismus

$$k[a_1,...,a_n] \longrightarrow k[U_1,...,U_n],\ a_i \mapsto U_i,$$

mit Unbestimmten U_i, also ein k-Algebra-Isomorphismus

$$k[a_1,...,a_n]\otimes_k k[a_1,...,a_n]\otimes_k k[a_1,...,a_n]$$
$$\longrightarrow k[U_1,...,U_n]\otimes_k k[V_1,...,V_n]\otimes_k k[W_1,...,W_n] = k[U,V,W]$$

$$a_.\otimes 1\otimes 1 \mapsto U_.,\ 1\otimes a_.\otimes 1 \mapsto V_.,\ 1\otimes 1\otimes a_. \mapsto W_.$$

Das Bild von

$$(\partial f)(p_1^*(a), p_2^*(a), p_3^*(a)) = (\partial f)(a\otimes 1\otimes 1, 1\otimes a\otimes 1, 1\otimes 1\otimes a)$$

bei diesem Isomorphismus ist $(\partial f)(U, V, W)$, d.h. es gilt

$$(\partial f)(U, V, W) = 0.$$

Wir haben gezeigt,

$$f(U,V) \in k[U,V] = k[U_1,...,U_n, V_1,...,V_n]$$

ist ein polynomialer 2-Kozyklus. Wir können unser Kriterium für (multidimensionale) polynomiale 2-Koränder 3.4.6 anwenden, und erhalten im Fall der Charakteristik

$$p = 0,$$

daß es ein $g \in k[U]$ gibt mit

$$f(U,V) = g(U+V) - g(U) - g(V). \qquad (6)$$

Behauptung: im Fall einer positiven Charakteristik hat f ebenfalls diese Gestalt.
Auf Grund unseres Kriteriums 3.4.6 reicht es zu zeigen, es gilt

$$\sum_{i=1}^{p-1} f(U,\ i\bullet U) = 0.$$

Weil die a_i algebraische unabhängig sind, reicht es zu zeigen, die reguläre Funktion

$$\sum_{i=1}^{p-1} f(a,\ i\bullet a)$$

ist identisch Null auf G. Für $u \in G$ gilt

$$\Big(\sum_{i=1}^{p-1} f(a, i\bullet a)\Big)(u) = \sum_{i=1}^{p-1} f(a(u), i\bullet a(u))$$

$$= \sum_{i=1}^{p-1} f(a(u), a(u^i)) \qquad \text{(die } a_j \text{ sind additive Funktionen)}$$

$$= \sum_{i=1}^{p-1} (x(u\bullet u^i) - x(u) - x(u^i)) \qquad \text{(nach Definition von f)}$$

$$= \sum_{i=1}^{p-1} x(u^{i+1}) - (p-1)\bullet x(u) - \sum_{i=1}^{p-1} x(u^i)$$

$$= x(u^p) - (p-1)\bullet x(u) - x(u)$$

$$= x(u^p) - p\bullet x(u)$$

$$= x(u^p) \qquad \text{(p ist die Charakteristik von k)}$$

Nun ist nach Voraussetzung (i) die Gruppe G elementar unipotent. Wegen $p > 0$ hat jedes Element von G eine Ordnung, welche p teilt. Deshalb ist $u^p = e$, also

$$\sum_{i=1}^{p-1} f(a, i\bullet a))(u) = x(e) = x_{1m}(e) = 0$$

(der Eintrag in der Position (1,m) der Einheitsmatrix ist wegen $m > 1$ gleich 0).

Damit hat f auch im Fall postiver Charakteristik die Gestalt (6). Für jede Charakteristik gilt

$$\begin{aligned} x(uv) - x(u) - x(v) &= f(a(u), a(v)) && \text{(nach Definition von f)} \\ &= g(a(u)+a(v)) - g(a(u)) - g(a(v)) && \text{(nach (6))} \\ &= g(a(uv)) - g(a(u)) - g(a(v)) && \text{(die } a_i \text{ sind additive Funktionen)} \end{aligned}$$

zusammen also

$$x(uv) - x(u) - x(v) = g(a(uv)) - g(a(u)) - g(a(v)) \qquad (7)$$

für beliebige $u, v \in G$. Wir setzen

$$h(u) := x(u) - g(a(u)) = x_{im}(u) - g(a_1(u),...,a_n(u))$$

Wegen (7) gilt dann

$$h(uv) - h(u) - h(v) = 0$$

für $u, v \in G$, d.h.

h ist eine additive Funktion.

Wir sind jetzt soweit, daß wir zeigen können, der Koordinatenring k[G] wird von additiven Funktionen erzeugt (d.h. es gilt der zweite Teil von Aussage (ii)).
Es gilt

$$k[G] = k[x_{ij} \mid 1 \le i < j \le m]$$

Dabei liegt jedes x_{ij} mit eventueller Ausnahme von $x = x_{1m}$ in $k[\varphi(G)]$ oder in $k[\psi(G)]$,

$$x_{ij} \in k[\varphi(G)] \bigcup k[\psi(G)]$$

für $(i,j) \neq (1,m)$, also

$$x_{ij} \in k[a_1,...,a_n]$$

für jedes (i,j) $\neq$ (1,m) (wegen (5)). Damit gilt

$$\begin{aligned} k[G] &= k[a_1,...,a_n, x_{1m}] \\ &= k[a_1,...,a_n, x_{1m}-g(a_1,...,a_n)] \\ &= k[a_1,...,a_n, h] \end{aligned}$$

Der Koordinatenring k[G] wird von endlich vielen additiven Funktionen erzeugt.

Wir haben noch zu zeigen, $\mathcal{A}(G)$ ist als R(k)-Modul endlich erzeugt. Weil G zusammenhängend ist, ist $\mathcal{A}(G)$ torsionsfrei (nach 3.3.6(i)). Insbesondere ist damit der endlich erzeugte Teilmodul

$$R(k)\bullet a_1+...+R(k)\bullet a_n+R(k)\bullet h$$

von $\mathcal{A}(G)$ torsionsfrei, also frei über R(k) (nach 3.3.3 (iii)), sagen wir

$$R(k)\bullet a_1+...+R(k)\bullet a_n = R(k)\bullet f_1+...+R(k)\bullet f_\ell \qquad (8)$$

mit $f_1,...,f_\ell$ linear unabhängig über R(k), also algebraisch unabhängig über k (nach 3.3.6 (ii)). Wegen (8) sind die a_i und h Polynome in den f_j und die f_j Polynome in den a_i und h. Es gilt also

$$\begin{aligned} k[G] &= k[a_1,...,a_n, h] \\ &= k[f_1,...,f_\ell] \end{aligned}$$

Weil die f_i den Koordinatenring von G erzeugen, definieren sie einen Isomorphismus algebraischer Varietäten von G mit einer abgeschlossenen Teilmenge

$$X = V(g_1,...g_s)$$

des k^ℓ,

$$f:G \xrightarrow{\cong} X = V(g_1,...g_s) \subseteq k^\ell,\ x \mapsto \begin{pmatrix} f_1(x) \\ \cdots \\ f_r(x) \end{pmatrix}.$$

Weil die f_i algebraisch unabhängig sind, müssen die definierenden Polynome g_ν von X identisch Null sein, d.h. $X = k^\ell$ und f ist ein Isomorphimus algebraischer Varietäten

$$f:G \xrightarrow{\cong} k^\ell = G_a^\ell$$

Weil die f_i additive Funktionen sind, ist f ein Gruppen-Homomorphismus, also ein Isomorphismus von linearen algebraischen Gruppen,

$$G \xrightarrow{\cong} \mathbf{G}_a^\ell$$

Nach 3.3.5 ist $\mathcal{A}(G) \cong \mathcal{A}(G_a^\ell)$ endlich erzeugt über R(k) (mit einer Basis aus ℓ Elementen).

Bemerkung.
Wir haben im Fall einer zusammenhängenden linearen algebraischen Gruppe G gezeigt, daß die Aussagen (i), (ii) und (iii) äquivalent sind, wobei die Implikation

$$\text{(iii)} \Rightarrow \text{(i)}$$

auch im allgemeinen Fall besteht. Wir zeigen als nächstes, daß (i) und (iii) im allgemeinen Fall auch äquivalent sind.

(i) $\Rightarrow$ (iii). Sei G eine elementare unipotente Gruppe über k. Dann ist auch G^0 eine elementare unipotente Gruppe (vgl. 3.4.1). Weil G^0 zusammenhängend ist (und die Äquivalenz von (i)- (iii) im zusammenhängenden Fall bereits bewiesen wurde), ist

$$G^0 \text{ eine Vektorgruppe, sagen wir } G^0 \cong \mathbf{G}_a^n.$$

Weil G abelsch ist (vgl. 3.4.1) ist G/G^0 eine endliche abelsche Gruppe und als solche ein direktes Produkt von endlich vielen zyklischen Gruppen, sagen wir

$$G/G^0 = Z_1 \times ... \times Z_r.$$

1. Schritt. Der Fall positiver Charakterisk p des Grundkörpers k.
Wir betrachten die exakte Sequenz

$$0 \longrightarrow G^0 \longrightarrow G \xrightarrow{\alpha} Z_1 \times ... \times Z_r \longrightarrow 0.$$

Sei $z_i \in G$ ein Element dessen Bild in $Z_1 \times ... \times Z_r$ ein Erzeuger von

$$Z_i = \{1\} \times ... \times \{1\} \times Z_i \times \{1\} \times ... \times \{1\} \hookrightarrow Z_1 \times ... \times Z_r$$

ist. Dann ist z_i != e und die von z_i erzeugte Untergruppe $\langle z_i \rangle$ von G hat die Ordnung p,

$$\# \langle z_i \rangle = p.$$

Die Einschränkung von α auf $\langle z_i \rangle$ ist surjektiv, also ein Isomorphismus

$$\alpha|_{\langle z_i \rangle} : \langle z_i \rangle \xrightarrow{\cong} Z_i \ (\hookrightarrow Z_1 \times ... \times Z_r)$$

(weil Definitionsbereich und Bild dieselbe Ordnung haben). Deshalb ist

$$\beta: Z_1 \times ... \times Z_r \longrightarrow G, (x_1,...,x_r) \mapsto \alpha|^{-1}_{\langle z_1 \rangle}(x_1) \bullet ... \bullet \alpha|^{-1}_{\langle z_r \rangle}(x_r)),$$

ein Gruppen-Homomorphismus mit

$$\alpha(\beta(\alpha(z_i))) = \alpha(\beta(\alpha(z_i))) = \alpha(z_i).$$

Zu Zusammensetzung $\alpha \circ \beta$ bildet ein Erzeugendensystem von $Z_1 \times ... \times Z_r$ elementweise in sich ab, d.h. es gilt $\alpha \circ \beta = Id$, d.h. β ist ein Schnitt von α. Die exakte Sequenz zerfällt und es gilt

$$G = G^0 \times \beta(Z_1 \times ... \times Z_r) = G^0 \times Z_1 \times ... \times Z_r.$$

Man beachte, weil $Z_1 \times ... \times Z_r$ endlich ist, ist β eine reguläre Abbildung, also ein Homomorphismus von linearen algebraischen Gruppen. Insbesondere gilt (iii).

2. Schritt. Der Fall der Charakterisk p = 0 des Grundkörpers k, ist $G = G^0 = \mathbf{G}_a^n$
Weil können annehmen, G ist abgeschlossene Untergruppe einer $\mathbf{GL}_n$.

Angenommen, es gibt ein $x \in G - G^0$. Dann gilt $x \in G - \{e\}$.Weil x unipotent ist, sind alle Eigenwerte von x gleich 1, und wir können durch Konjugation erreichen, daß x mit seiner Jordanschen Normalform übereinstimmt, sagen wir

$$x = Id + n, \text{ mit } n \in \sum_{\ell(E_{ij})=1} k \bullet E_{ij} \subseteq N_n^1, \text{ wegen } x \neq e \text{ gilt } n \neq 0.$$

(Bezeichnungen wir in 2.1.5 Aufgabe 4, dritter Schritt).

Für die i-te Potenz von x erhalten wir

$$x^i = \sum_{\alpha=0}^{i} \binom{i}{\alpha} \cdot n^\alpha = Id + i \cdot n + y(i) \text{ mit } y(i) \in N_n^1 \cdot N_n^1 \subseteq N_n^2$$

Weil die Charakteristik von k gleich 0 ist, gilt $i \cdot n \neq 0$, d.h.

$$x^i \neq 0.$$

d.h. x hat unendliche Ordung.

Weil G/G^0 endliche Ordnung besitzt, gibt es eine natürliche Zahl ℓ mit

$$x^\ell \in G^0 \cong G_a^n = k^n$$

Dann gibt es aber auch ein $y \in k^n = G_a^n = G^0$ mit $y^\ell = x^\ell$, also $(xy^{-1})^\ell = e$, d.h. xy^{-1} hat endliche Ordnung, kann also nicht in $G\text{-}G^0$ liegen. Also gilt

$xy^{-1} \in G^0$,

also

$$x \in G^0 \cdot y \subseteq G^0 \cdot G^0 = G^0,$$

im Widerspruch zur Wahl von x. Unsere Annahme führt zu einem Widerspruch. Also gilt

$$G - G^0 = \varnothing,$$

also

$$G = G^0 = G_a^n.$$

Wir haben gezeigt, die Aussagen (i) und (iii) sind für beliebige lineare algebraische Gruppen G äquivalent (und im zusammenhängenden Fall sind (i), (ii) und (iii) äquivalent.

(ii) $\Rightarrow$ (i). Nach Voraussetzung wird k[G] von additiven Funktionen erzeugt, sagen wir

$$k[G] = k[f_1,...,f_n],$$

wobei jedes $f_i: G \longrightarrow \mathbf{G}_a$ ein Homomorphismus von linearen algebraischen Gruppen ist. Weil die f_i den Koordinatenring erzeugen, ist durch

$$\varphi: G \longrightarrow k^m,\ x \mapsto \begin{pmatrix} f_1(x) \\ \cdots \\ f_m(x) \end{pmatrix},$$

ein Isomorphismus mit einer abgeschlossnen Teilvarietät $V \subseteq k^m$ definiert (vgl. Bemerkung 1.3.1 (iii)). Weil die f_i additiv sind, ist

$$\varphi: G \longrightarrow k^m = \mathbf{G}_a^m$$

ein Homomorphismus von linearen algebraischen Gruppen, $\varphi(G)$ eine abgeschlossene Untergruppe von $\mathbf{G}_a^m$ (vgl. 2.2.5 (ii)) und die durch φ induzierte Abbildung

$$G \longrightarrow \varphi(G)$$

ein Isomorphismus von linearen algebraischen Gruppen (vgl. das Ende von Schritt 3 im Beweis von 2.3.7 (i)). Wir können die Gruppe G mit deren Bild bei φ identifizieren.

Als Untergruppe der elementaren unipotenten Gruppe $\mathbf{G}_a^m$ ist G unipotent und elementar, d.h. es gilt (i).

Zusammenfassung.

Wir haben bisher die folgenden Implikationen bewiesen.

(ii) $\Rightarrow$ (i) $\Leftrightarrow$ (iii)

(i) $\Leftrightarrow$ (ii) $\Leftrightarrow$ (iii) falls G zusammenhängend ist.

Zum Abschluß des Beweises reicht es somit, die Implikation

(iii) $\Rightarrow$ (ii)

zu beweisen.

(iii) $\Rightarrow$ (ii). 1. Schritt. Sind G_1 und G_2 zwei lineare algebraische Gruppen, für welche Bedingung (ii) erfüllt ist, so ist Bedingung (ii) auch für G'×G" erfüllt.

Nach Bemerkung 3.3.1A(v) die Abbildung

$$\varphi: \mathcal{A}(G_1 \times G_2) \longrightarrow \mathcal{A}(G_1) \oplus \mathcal{A}(G_2),\ f \mapsto (f \circ q_1, f \circ q_2)$$

ein k-linearer Isomorphismus. Ist die Charakteristik p des Grundkörpers k positiv, dies sogar ein Isomorphismus von R(k)-Moduln, denn es ist

$$\begin{aligned}
\varphi(T \bullet f) &= \varphi(f^p) \\
&= (f^p \circ q_1, f^p \circ q_2) \\
&= ((f \circ q_1)^p, (f \circ q_2)^p) \\
&= ((f \circ q_1)^p, (f \circ q_2)^p) \\
&= (T \bullet f \circ q_1, T \bullet f \circ q_2) \\
&= T \bullet (f \circ q_1, f \circ q_2) \\
&= T \bullet \varphi(f).
\end{aligned}$$

Nach Voraussetzung sind $\mathcal{A}(G_1)$ und $\mathcal{A}(G_2)$ endlich erzeugte R(k)-Moduln. Auf Grund des Isomorphismus ist dann aber auch $\mathcal{A}(G_1 \times G_2)$ endlich erzeugt über R(k).

Wir haben noch zu zeigen, $\mathcal{A}(G_1 \times G_2)$ erzeugt $k[G_1 \times G_2]$ als k-Algebra. Nach Voraussetzung wird $k[G_i]$ von $\mathcal{A}(G_i)$ erzeugt (für i = 1,...,2).

Nach Bemerkung 3.3.1A(v) ist

$$\psi: \mathcal{A}(G_1) \oplus \mathcal{A}(G_2) \longrightarrow \mathcal{A}(G_1 \times G_2),\ (f,g) \mapsto p_1^*(f) + p_2^*(g),$$

die zu φ inverser Abbildung. Insbesondere gilt

$$p_1^*(\mathcal{A}(G_1)) \subseteq \mathcal{A}(G_1 \times G_2) \text{ und } p_2^*(\mathcal{A}(G_2)) \subseteq \mathcal{A}(G_1 \times G_2).$$

Dieselben Inklusionen bestehen deshalb auch zwischen den von diesen Mengen erzeugten k-Algebren.

$$k[p_1^*(\mathcal{A}(G_1))] \subseteq k[\mathcal{A}(G_1 \times G_2)] \text{ und } k[p_2^*(\mathcal{A}(G_2))] \subseteq k[\mathcal{A}(G_1 \times G_2)].$$

Weil

$$p_1^*: k[G_1] \longrightarrow k[G_1 \times G_2] \text{ und } p_2^*: k[G_2] \longrightarrow k[G_1 \times G_2]$$

k-Algebra-Homomorphismen sind, gilt

$$k[p_1^*(\mathcal{A}(G_1))] = p_1^*(k[\mathcal{A}(G_1)]) = k[G_1] \otimes k$$

und

$$k[p_2^*(\mathcal{A}(G_2))] = p_2^*(k[\mathcal{A}(G_2)]) = k\otimes k[G_2].$$

Die Inklusionen können wir deshalb in der Gestalt

$$k[G_1]\otimes k \subseteq k[\mathcal{A}(G_1\times G_2)] \text{ und } k\otimes k[G_2] \subseteq k[\mathcal{A}(G_1\times G_2)].$$

Es folgt

$$k[G_1]\otimes k[G_2] \subseteq k[\mathcal{A}(G_1\times G_2)] \subseteq k[G_1]\otimes k[G_2],$$

also

$$k[\mathcal{A}(G_1\times G_2)] = k[G_1]\otimes k[G_2].$$

Mit anderen Worten, der Koordinatenring von $G_1\times G_2$ wird also k-Algebra von den additiven Funktionen auf $G_1\times G_2$ erzeugt.

2. Schritt. Mit (iii) gilt auch (ii).
Nach Voraussetzung gilt

$$G \cong \mathbf{G}_a\times\ldots\times\mathbf{G}_a \text{ im Fall } p = 0$$

und

$$G \cong \mathbf{G}_a\times\ldots\times\mathbf{G}_a\times\mathbb{Z}/p\mathbb{Z}\times\ldots\times\mathbb{Z}/p\mathbb{Z} \text{ im Fall } p > 0.$$

Nach dem ersten Schritt reicht es zu zeigen, daß $\mathbf{G}_a$ und (im Fall p>0) $\mathbb{Z}/p\mathbb{Z}$ den Bedingungen von (ii) genügen. Für $\mathbf{G}_a$ haben wir dies bereits gezeigt, denn $\mathbf{G}_a$ ist zusammenhängen, d.h. es besteht die Implikation (iii) $\Rightarrow$ (ii). Wir können also annehmen,

$$G = \mathbb{Z}/p\mathbb{Z} \text{ und } p > 0.$$

Wie wir bereits gesehen haben, induziert die natürliche Einbettung

$$\mathbb{F}_p \hookrightarrow k$$

des Primkörpers $\mathbb{F}_p$ in den Körper k der Charakteristik p eine reguläre Abbildung linearer algebraischer Gruppen

$$i: G = \mathbb{Z}/p\mathbb{Z} \hookrightarrow \mathbf{G}_a$$

welche G mit einer abgeschlossenen Untergruppe von $\mathbf{G}_a$ identifiziert. Insbesondere ist der induzierte k-Algebra-Homomorphismus der Koordinatenringe

$$i^*: k[T] = k[\mathbf{G}_a] \twoheadrightarrow k[G] \tag{9}$$

surjektiv. Dabei bezeichnet T eine einzelne Unbestimmte, nämlich die additive Funktion, welche jedes Element von $\mathbf{G}_a = k$ auf seine einzige Koordinate abbildet (d.h. die identische Abbildung $k \longrightarrow k$). Weil i ein Homomorphismus von linearen algebraischen Gruppe ist, ist

$$i^*(T) = T|_G$$

eine additive Funktion auf G. Weil der k-Algebra-Homomorphismus (9) surjektiv ist, wird bei i* jedes Erzeugendensystem der k-Algebra $k[\mathbf{G}_a]$ in ein Erzeugendensystem der k-Algebra k[G] gebildet. Insbesondere wird k[G] von $i^*(T) = T|_G$ als k-Algebra erzeugt:

k[G] wird als k-Algebra von additiven Funktionen erzeugt.

Wir haben noch zu zeigen, $\mathcal{A}(G)$ ist ein endlich erzeugter R(k)-Modul. Wegen $k \subseteq R(k)$ reicht es zu zeigen, $\mathcal{A}(G)$ ist ein endlich-dimensiionaler k-Vektorraum.

Weil die Restklasse von 1 die zyklische Gruppe $G = \mathbb{Z}/p\mathbb{Z}$ erzeugt, ist eine additive Funktion f auf G bereits durch deren Wert in dieser Restklasse eindeutig festgelegt,

$$f(n \bmod p\mathbb{Z}) = n \bullet f(1 \bmod p\mathbb{Z}).$$

Deshalb ist die Abbildung

$$\mathcal{A}(G) \longrightarrow k,\ f \mapsto f(1 \bmod p\mathbb{Z}),$$

injektiv. An der Abbildungsvorschrift lesen wir ab, daß sie auch k-linear ist, also ein Isomorphismus von k-Vektorraumen. Damit ist $\mathcal{A}(G)$ ein endlich erzeugter k-Vektorraum, also erst recht ein endlich erzeugter R(k)-Modul.
QED.

3.4.8 Kriterium für elementare unipotente F-Gruppen

Seien F ein Teilkörper von k und G eine F-Gruppe. Dann sind folgende Aussagen äquivalent.

(i) G ist elementar unipotent.

(ii) $\mathcal{A}(G)(F)$ erzeugt F[G] als F-Algebra.

(iii) G ist F-isomorph zu einer abgeschlossenen F-Untergruppe einer $\mathbf{G}_a^n$.

Sind diese Bedingungen erfüllt, so erzeugen bereits endlich viele Elemente von $\mathcal{A}(G)(F)$ die F-Algebra F[G].

Beweis. (i) $\Rightarrow$ (ii). Nach Bemerkung 3.3.1 A (iii) ist $\mathcal{A}(G)(F)$ eine F-Struktur von $\mathcal{A}(G)(k)$, d.h.

$$k \otimes_F \mathcal{A}(G)(F) = \mathcal{A}(G).$$

Nach 3.4.7 (ii) wird die k-Algebra k[G] durch Elemente aus A(G) erzeugt. Weil letztere k-Linearkombinationen von Elementen aus $\mathcal{A}(G)(F)$ sind, wird k[G] durch Elemente aus $\mathcal{A}(G)(F)$ erzeugt. Damit enthält die von $\mathcal{A}(G)(F)$ erzeugte F-Teilalgebra von F[G],

$$F[\mathcal{A}(G)(F)] \hookrightarrow F[G], \qquad (1)$$

ein Erzeugendensystem der k-Algebra k[G]. Es folgt

$$k[G] \subseteq k \otimes_F F[\mathcal{A}(G)(F)] \subseteq k \otimes_F F[G] = k[G].$$

Der Funktor $k \otimes_F$ überführt also die Inklusion (1) in einen Isomorphismus. Weil der Funktor $k \otimes_F$ treuflach ist, muß (1) selbst schon ein Isomorphismus sein, d.h. es gilt

$$F[\mathcal{A}(G)(F)] = F[G].$$

(ii) $\Rightarrow$ (iii). Weil G eine affine Varietät ist, ist k[G] als k-Algebra endlich erzeugt, sagen wir

$$k[G] = k[x_1,...,x_n].$$

Wegen $k[G] = k \otimes_F F[G]$ ist jedes x_i eine k-Linearkombination von (endlich vielen) Elementen aus F[G]. Wir können deshalb annehmen,

$$x_1,...,x_n \in F[G].$$

Weil F[G] nach Voraussetzung als F-Algebra durch $\mathcal{A}(G)(F)$ erzeugt wird, ist jedes x_i ein Polynom in endlich vielen Elementen aus $\mathcal{A}(G)(F)$. Wir können deshalb annehmen,

$$x_1,...,x_n \in \mathcal{A}(G)(F).$$

Weil die x_i die k-Algebra k[G] erzeugen, ist die reguläre Abbildung

$$G \longrightarrow k^n,\ p \mapsto \begin{pmatrix} x_1(p) \\ \cdots \\ x_n(p) \end{pmatrix},$$

ein Isomorphismus der algebraischen Varietät G mit einer abgeschlossenen Teilvarietät $V \subseteq k^n$ (vgl. Bemerkung 3.1.3 (iii) oder das Ende dritten Schritts im Beweises des Einbettungssatzes 2.3.7 (i)). Weil die x_i additive Funktionen sind, ist

$$G \longrightarrow k^n = \mathbf{G}_a^n$$

ein Homomorphismus von linearen algebraischen Gruppen, der einen Isomorphismus mit einer abgeschlossenen Untergruppe von $\mathbf{G}_a^n$ induziert. Weil die x_i über F definiert sind, ist dieser Isomorphismus ein F-Isomorphismus mit einer abgeschlossenen F-Untergruppe von $\mathbf{G}_a^n$.

(iii) $\Rightarrow$ (i). Nach Voraussetzung können wir G mit einer abgeschlossenen Untergruppe einer $\mathbf{G}_a^n$ identifizieren. Deshalb besteht G vollständig aus unipotenten Elementen. Ist die Charakteristik p des Grundkörpers positiv, so hat jedes Element von G - {e} die Ordnung p (weil dies für jedes Elemente von $\mathbf{G}_a^n$ - {e} = k^n - {0} gilt). Deshalb ist G elementar unipotent (vgl. 3.4.1).
QED.

3.4.9 Theorem: die zusammenhängenden linearen algebraischen Gruppen der Dimension 1

Sei G eine zusammenhängende lineare algebraische Gruppe der Dimension 1. Dann ist G isomorph zu $\mathbf{G}_a$ oder $\mathbf{G}_m$.

Beweis. Nach 3.1.3 ist G kommutative und die Gruppe G stimmt mit ihrem halbeinfachen oder mit ihrem unipotenten Teil überein,

$$G = G_s \text{ oder } G = G_u.$$

Im zweiten Fall ist G sogar elementar unipotent (vgl. 3.1.3 (iii) und 3.4.1)
1. Fall. $G = G_s$.
Wir können annehmen, G ist eine abgeschlossene Untergruppe einer $\mathbf{GL}_n$. Weil G abelsch ist und aus halbeinfachen Elementen besteht, können wir annehmen, G besteht aus Diagonal-Matrizen,

$$G \subseteq \mathbf{D}_n,$$

(vgl. 2.4.2 (ii)), d.h. G ist diagonalisierbar (vgl. 3.2.1). Weil G nach Voraussetzung zusammenhängend ist, ist G ein Torus (vgl. 3.2.7 (ii)), d.h. wir können annehmen,

$$G \cong \mathbf{D}_n = \mathbf{G}_m^n$$

(vgl. 3.2.1). Weil G eindimensional sein soll, muß n = 1 sein, d.h. $G \cong \mathbf{G}_m$.
2. Fall. $G = G_u$ und G elementar unipotent.
Nach 3.4.7 (iii) hat G die Gestalt

$$G \cong \mathbf{G}_a^n \times Z_1 \times \ldots \times Z_r$$

mit endlichen zyklischen Gruppen Z_i.. Weil G zusammenhängend sein soll folgt

$$G \cong \mathbf{G}_a^n,$$

und weil G eindimensional ist, muß n = 1 sein, d.h.

$$G \cong \mathbf{G}_a.$$

QED.

3.4.10 Aufgaben

3.4.10 Aufgabe 1

Sei R = R(k) wie in 3.3.1. Zeigen Sie, die elementar unipotenten Gruppen über k bilden eine Kategorie, welche anti-äquivalent ist zur Kategorie

R-f-Mod

der linken endlich erzeugten R-Moduln (Für weitere Ergebnisse in dieser Richtung siehe 14.3.6).

Bemerkungen

(i) In 14.3.6 wird eine Konstruktion angegeben, die nahelegt, daß mit der behaupteten Anti-Äquivalenz der Funktor

$$\mathcal{A}: \left(\begin{array}{c}\text{Kategorie der elementar unipotenten}\\ \text{linearen algebraischen Gruppen über k}\end{array}\right) \longrightarrow \text{R-f-Mod}, \; G \mapsto \mathcal{A}(G),$$

(vgl. 3.3.1 und 3.3.4) gemeint ist. Zumindeste wir dort die Existenz eines Isomorphismus

$$M \overset{\cong}{\longrightarrow} \mathcal{A}(\mathcal{G})$$

für jeden endlich erzeugten R(k)-Modul M behauptet mit einer elementar unipotenten Gruppe $\mathcal{G} = \mathcal{G}(M)$. Die nachfolgende Bemerkung gibt ein Argument an, welches darauf hinweist, daß dies unmöglich der Fall sein kann. Man muß die Bild-Kategorie

R-f-Mod

der endlich erzeugten R-Moduln durch die Kategorie der endlich erzeugten R-Moduln ohne T-Torsion ersetzen.

(ii) Sei n > 1 eine natürliche Zahl. Der linke R-Modul

$$M = R/R \bullet T^n$$

ist endlich erzeugt, denn die Restklasse von $1 \in R$ erzeugt M über R. Das Element

$$T^n \in R$$

liegt wegen $T \bullet R = R \bullet T$, also $T^n \bullet R = R \bullet T^n$ im Annullator von M. Ist M isomorph zum Modul der additiven Funktionen einer elementar unipotenten Gruppe G,

$$R/R \bullet T^n = M \cong \mathcal{A}(G),$$

so gilt

$$0 = T^n f = f^{p^n} \text{ für jedes } f \in \mathcal{A}(G) \; (\subseteq k[G]).$$

Als additive Funktion ist f eine Abbildung mit Werten in k. Weil ein Potenz von f gleich 0 ist, ist f selbst gleich 0,

$$f = 0 \text{ für jedes } f \in \mathcal{A}(G),$$

d.h. es gilt $\mathcal{A}(G) = 0$ im Widerspruch zu $\mathcal{A}(G) \cong R/R \bullet T^n \neq 0$.
Allgemein bestehen für jede lineare algebraische Gruppe G die Implikationen

$$f \in \mathcal{A}(G) \text{ und } T \bullet f = 0 \Rightarrow f^p = 0 \Rightarrow f = 0,$$

d.h $\mathcal{A}(G)$ besitzt keine T-Torsion.

(ii) <u>Eine Beschreibung der endlich erzeugten R-Moduln ohne T-Torsin im Fall der Charateristik</u> p > 0.
Sei

M

ein endlich erzeugter R-Modul. Nach 3.3.3 (iii) ist M eine direkte Summe von zyklischen R-Moduln, sagen wir

$$M = M_1 \oplus ... \oplus M_r$$

mit M_i zyklisch, d.h.

$$M_i \cong R/R\bullet\lambda_i \text{ mit } \lambda_i \in R. \tag{1}$$

Wir können annehmen, λ_i ist ein nicht-konstantes Polynom (denn andernfalls ist $R/R\bullet\lambda_i = 0$). Die folgenden Bedingungen sind äquivalent.

(a) M besitzt T-Torsion.
(b) Einer der direkten Summanden M_i besitzt T-Torsion.
(c) Ein λ_i hat die Gestalt $\lambda_i = T\bullet\mu_i$ mit $\mu_i \in R$.

Die Äquivalenz der ersten beiden Bedingungen ergibt sich einfach aus der Tatsache, daß ein Element $m = (m_1,...,m_r) \in M$ genau dann von T annulliert anulliert wird, wenn T jede der Koordinaten m_i annulliert.

Falls $\lambda = \lambda_i$ die Gestalt $\lambda = T\bullet\mu$ hat mit $\mu \in R$, so ist die Restklasse $[\mu]$ von μ in M_i ein von Null verschiedenes Element[40] mit

$$T\bullet[\mu] = [T\bullet\mu] = [\lambda] = 0,$$

d.h. M_i besitzt T-Torsion. Also besteht die Implikation (c) $\Rightarrow$ (b).

Falls M_i ein R-Modul mit T-Torsion ist, gibt es ein $r \in R - R\circ\lambda$ mit $T\bullet r \in R\circ\lambda$, d.h. es ist

$$T\circ r = s\circ\lambda \text{ für ein } s \in R. \tag{2}$$

Weil k algebraisch abgeschlossen ist, können wir s und λ in der Gestalt

$$s = \sum_\alpha (s_\alpha)^p\bullet T^\alpha \text{ und } \lambda = \sum_\beta (\lambda_\beta)^p\bullet T^\beta$$

schreiben. Auf Grund der Identität (2) ist das Absolutglied $(r_0\bullet\lambda_0)^p$ von $s\circ\lambda$. gleich 0. Also gilt

$$s_0 = 0 \text{ oder } \lambda_0 = 0.$$

Im ersten Fall gilt $s = T\bullet \sum_\alpha s_\alpha\bullet T^{\alpha-1}$ also $T\circ r = T\bullet (\sum_\alpha s_\alpha\bullet T^{\alpha-1})\circ\lambda$. Weil R nullteilerfrei ist, folgt $r = (\sum_\alpha s_\alpha\bullet T^{\alpha-1})\circ\lambda \in R\circ\lambda$ im Widerspruch zur Wahl von r.

Also tritt der erste Fall nicht ein und es gilt $\lambda_0 = 0$, d.h. λ hat die Gestalt

$$\lambda = T\bullet(\sum_\alpha \lambda_\alpha\bullet T^{\alpha-1})$$

---

[40] Jedes Element von $R\bullet\lambda$ hat einen Grad $\geq \deg(\lambda)$ (nach Bemerkung 3.3.1 B (iii)). Wegen $\deg(\mu) = \deg(\lambda) - 1$ liegt also μ nicht in $R\bullet\lambda$.

Damit ist auch die Implikation (b) $\Rightarrow$ (c) bewiesen.

Beweis. 1. Schritt. Der Übergang zum R-Modul der additiven Funktionen definiert einen kontravarianten Funktor

$$\mathcal{A}: \begin{pmatrix}\text{Kategorie der elementar unipotenten Gruppen}\\ \text{und Homorphismen algebraischer Gruppen}\end{pmatrix} \longrightarrow \begin{pmatrix}\text{Kategorie der endlich}\\ \text{erzeugten R(k)-Moduln}\\ \text{ohne T-Torsion}\end{pmatrix}$$

Für jede elementar unipotente Gruppe G ist $\mathcal{A}(G)$ ein R(k)-Modul (vgl. 3.3.4 A). Dieser Modul ist endlich erzeugt nach 3.4.7 (ii). Er besitzt keine T-Torsion, weil eine Funktion $f:G \longrightarrow k$ mit Werten im Körper k gleich Null ist, falls eine Potenz von ihr gleich Null ist. Man beachte, nach Definition der R(k)-Modulstruktur von $\mathcal{A}(G)$ in 3.3.4 A ist $T\bullet f = f^p$.

Für jeden Homomorphismus $h: G \longrightarrow G'$ und jede additive Funktion $f: G' \longrightarrow \mathbf{G}_a$ ist $h^*(f) = f\circ h: G \longrightarrow G' \longrightarrow \mathbf{G}_a$ eine additive Funktion. Deshalb ist die Abbildung

$$\mathcal{A}(G') \longrightarrow \mathcal{A}(G),\ f \mapsto h^*(f) = f\circ h,$$

eine wohldefinierte Abbildung. Diese Abbildung ist k-linear,

$$\begin{aligned} h^*(c'\bullet f' + c''\bullet f'') &= (c'\bullet f' + c''\bullet f')\circ h\\ &= c'\bullet f'\circ h + c''\bullet f''\circ h\\ &= c'\bullet h^*(f') + c''\bullet h^*(f''), \end{aligned}$$

und es gilt

$$\begin{aligned} h^*(T\bullet f) &= (T\bullet f)\circ h\\ &= f^p\circ h\\ &= (f\circ h)^p\\ &= T\bullet h^*(f). \end{aligned}$$

Damit ist

$$h^*: \mathcal{A}(G') \longrightarrow \mathcal{A}(G)$$

ein Homomorphismus von linken Moduln über R(k).

2. Schritt. Konstruktion eines kontravarianten Funktors

$$\mathcal{G}: \begin{pmatrix}\text{Kategorie der endlich}\\ \text{erzeugten R(k)-Moduln}\\ \text{ohne T-Torsion}\end{pmatrix} \longrightarrow \begin{pmatrix}\text{Kategorie der elementar unipotenten Gruppen}\\ \text{und Homorphismen algebraischer Gruppen}\end{pmatrix}$$

im umgekehrter Richtung (vgl. 14.3.6).

Sei M ein endlich erzeugter (linker) R(k)-Modul ohne T-Torsion. Wir bezeichen mit

$$S := S_k(M)$$

die symmetrische Algebra des k-Moduls M und mit

$$I = I(M) := (T\bullet m - m^p \mid m \in M)\bullet S \quad (\subseteq S)$$

das Ideal von S, welches von den Differenzen $T\bullet m - m^p$ erzeugt wird. Es reicht, die folgende Aussagen zu beweisen.

Die k-Algebra

$$k[M] := S/I$$

ist der Koodinatenring einer elementar unipotenten Gruppe $\mathcal{G} = \mathcal{G}(M)$, für welche die folgenden Bedingungen erfüllt sind.

1. $\Delta: k[M] \longrightarrow k[M] \otimes_k k[M], m \mapsto m \otimes 1 + 1 \otimes m$, ist die Komultiplikation von $\mathcal{G}$
2. $\iota: k[M] \longrightarrow k[M], m \mapsto -m$, ist der Antipode von $\mathcal{G}$
3. Die Projektion $S \twoheadrightarrow k$ auf die homogene Kompoente des Grades 0 faktorisiert sich über $k[M]$ und induziert so die Auswertung im neutralen Elment von $\mathcal{G}$

(1)

Die Funktorialität dieser Konstruktion ergibt sich dann nämlich wie folgt. Sei

$$h: M \longrightarrow M'$$

ein Homomorphismus von endlich erzeugten linken R(k)-Moduln ohne T-Torsion. Dann ist h insbesondere eine k-lineare Abbildung und induziert auf Grund der Universalitätseigenschaft der symmetrischen Algebra einen k-Algebra-Homomorphismus

$$s := S(h) := S_k(h): S_k(M) \longrightarrow S_k(M'),$$

dessen Einschränkung auf M gerade h ist. Insbesondere ist

$$s(m^p) = s(m)^p$$

und weil h eine R-lineare Abbildung ist, gilt

$$\begin{aligned} s(T \bullet m) &= h(T \bullet m) && \text{(wegen } s|_M = h) \\ &= T \bullet h(m) && \text{(h ist R-linear)} \\ &= T \bullet s(m). \end{aligned}$$

Zusammen ist $s(T \bullet m - m^p) = T \bullet s(m) - s(m)^p$ für jedes $m \in M$, d.h. es gilt

$$s(I(M)) \subseteq I(M').$$

deshalb induziert der k-Algebra-Homomorphismus s einen k-Algebra-Homomorphismus

$$\overline{s}: k[M] \longrightarrow k[M']$$

und damit eine reguläre Abbildung von algebraischen Varietäten

$$\mathcal{G}(h): \mathcal{G}(M') \longrightarrow \mathcal{G}(M).$$

Zum Beweis der Aussage des zweiten Schritts ist - neben der Aussage (1) - noch zu zeigen, daß dies ein Gruppen-Homomorphismus ist, d.h. daß das Diagramm

$$\begin{array}{ccc} \mathcal{G}(M') \times \mathcal{G}(M') & \xrightarrow{\mathcal{G}(h) \times \mathcal{G}(h)} & \mathcal{G}(M) \times \mathcal{G}(M) \\ \mu \downarrow & & \downarrow \mu' \\ \mathcal{G}(M') & \xrightarrow{\mathcal{G}(h)} & \mathcal{G}(M) \end{array}$$

kommutativ ist (wobei μ und μ' die Gruppen-Multiplikationen bezeichnet). Dazu reicht es die Kommutativität des zugehörigen Diagramms der Koordinatenringe zu beweisen. Zu zeigen ist die Kommutativität des Diagramms

$$\begin{array}{ccc} k[M] \otimes_k k[M] & \xrightarrow{\overline{s} \otimes \overline{s}} & k[M'] \otimes_k k[M'] \\ \Delta \uparrow & & \uparrow \Delta' \\ k[M] & \xrightarrow{\overline{s}} & k[M'] \end{array} \quad , \qquad (2)$$

wobei die verkalen Abbildungen gerade die Komultiplikationen sein sollen. Weil die Abbildungen des Diagramms k-Algebra-Homomorphismen sind, reicht es, die Kommutativität für die Elemente eines Erzeugengensystems der k-Algbra k[M] zu überprüfen, zum Beispiel für die Elemente [m] ∈ k[M] die durch ein m∈M repräsentiert werden. Es gilt

$$\begin{aligned}
\Delta'(\bar{s}([m])) &= \Delta'([h(m)]) && \text{(nach Definition von } \bar{s}) \\
&= [h(m)\otimes 1+1\otimes h(m)] && \text{(nach Definiton von } \Delta', \text{ vgl. (1))} \\
&= [h(m)]\otimes 1+1\otimes[h(m)] \\
&= \bar{s}([m])\otimes 1+1\otimes\bar{s}([m]) && \text{(nach Definition von } \bar{s}) \\
&= (\bar{s}\otimes\bar{s})([m]\otimes 1+1\otimes[m]) && (\bar{s} \text{ ist k-Algebra-Homomorphismus}) \\
&= (\bar{s}\otimes\bar{s})(\Delta([m]) && \text{(nach Definition von } \Delta, \text{ vgl. (1))}
\end{aligned}$$

Das Diagramm (2) ist somit tatsächlich kommutativ.
Weiter ist zu zeigen, daß die Gruppe $\mathcal{G}(M)$ elementar unipotent ist. Die k-Algebra $S_k(M)$ wird nach Definition durch die Elemente aus M erzeugt. Dasselbe gilt damit auch für die Faktoralgebra

$$k[M] = k[\mathcal{G}(M)].$$

Nach Definiton von Δ in (1) besteht das Bild von M in k[M] aus additiven Funktionen von $\mathcal{G}(M)$ (vgl. Bemerkkung 3.3.1 A (ii)). Deshalb wird der Koordintenring $k[\mathcal{G}(M)]$ von den additiven Funktionen erzeugt. Nach 3.4.8 (mit F = k) ist $\mathcal{G}(M)$ elementar unipotent.

Der Beweis der Aussage des zweiten Schritts ist damit auf den Beweis der Aussage (1) zurückgeführt. Die Beweise erfolgen in den nachfolgenden Schritten.
3. Schritt. k[M] ist eine endlich erzeugte und reduzierte k-Algebra im Fall M = R(k). Wir betrachten die natürliche Einbetttung

$$i: M \hookrightarrow S := S_k(M),$$

welche M mit der homogenen Komponente von S des Grades 1 identifiziert und bezeichnen das Bild von T^i bei dieser Einbettung mit T_i (für i = 0, 1, 2, ...). Das Bild von M bei dieser Einbettung ist dann gerade der k-Vektorraum

$$i(M) = \sum_{i\geq 0} k\bullet T_i$$

mit der Basis $\{T_i\}_{i\geq 0}$. Die symmetrische Algebra

$$S = S_k(M) \cong k[T_0,T_1,T_2,...]$$

ist isomorph zum Polynomring über k in den abzählbar vielen Unbestimmten T_i. Die Multplikation der Elemente von M mit denen aus R(k) ist auf i(M) gegeben durch

$$T\bullet T_i = T_{i+1}.$$

Weil die Multiplikation in S kommutativ und multilinear über k ist, folgt für

$$m = \sum_{i\geq 0} m_i\bullet T_i \in i(M) = \sum_{i\geq 0} k\bullet T_i$$

auf Grund der positiven Charakteristik p von k

$$\begin{aligned}
T\bullet m - m^p &= \sum_{i\geq 0} m_i^p\bullet T_{i+1} - \sum_{i\geq 0} m_i^p\bullet T_i^p \\
&= \sum_{i\geq 0} m_i^p\bullet(T_{i+1} - T_i^p)
\end{aligned}$$

Deshalb wird das Ideal I = I(M) von den Elmenten der Gestalt $T_{i+1} - T_i^p$ erzeugt, d.h. es ist

$$k[M] = S/I \cong k[T_0,T_1,T_2,...] / (T_{i+1} - T_i^p \mid i= 0,1,2, ...)$$
$$\cong k[T_0]$$

Dies ist tatsächlich eine endlich erzeugte k-Algebra ohne nilpotente Elemente.

4. Schritt. k[M] ist eine endlich erzeugte und reduzierte k-Algebra im Fall

$$M = R(t)/R(t)\bullet\lambda$$

$$\text{mit } \lambda = T^n + T^{n-1}\bullet c_1 + ... + T\bullet c_{n-1} + c_n \in R(t).$$

Weil M keine T-Torsion haben soll, ist auf Grund von Bemerkung (ii)

$$c_n \neq 0.$$

Weil die von 0 verschiedenen Elemente von $R\bullet\lambda$ einen Grad $\geq \deg(\lambda) = n$ haben (vgl. Bemerkung 3.3.1 B (iii)), bilden die Potenzen

$$T^i \text{ mit } i = 0, 1, ... ,, n-1$$

eine k-Vektorraumbasis von M. Wir bezeichnen das Bild des Basiselements T^i bei der natürlichen Einbettung von M in S mit T_i,

$$M \hookrightarrow S = S_F(M),\ T^i \mapsto T_i \text{ für } i = 0,...,n-1.$$

Dann gilt

$$S = S_F(M) \cong F[T_0,T_1,T_2,...,T_{n-1}],$$

Identifizieren wir den Modul M mit seinem Bild in S, so ist die Multiplikation mit T auf diesem Bild in S gegeben durch

$$T\bullet T_i = T_{i+1} \text{ für } i = 0,...,n-1$$
$$T\bullet T_{n-1} = -T_{n-1}c_1-...-T_1\bullet c_1 - T_0\bullet c_n$$

Die letzte Identität kommt von der Tatsache, daß die Restklasse von λ in M gleich 0 ist, also in M die Identität

$$T\bullet T^{n-1} = - T^{n-1}\bullet c_1 - ... - T\bullet c_{n-1} - c_n \text{ in M}$$

besteht. Weil jedes Element von M die Gestalt

$$m = \sum_{i=0}^{n-1} m_i\bullet T^i \text{ mit } m_i \in F$$

hat, also

$$T\bullet m - m^p = \sum_{i=0}^{n-2} m_i^p\bullet T_{i+1} - \sum_{i=0}^{n-2} m_i^p\bullet T_i^p + m_{n-1}\bullet(-T_{n-1}c_1-...-T_1\bullet c_{n-1} - T_0\bullet c_n - T_{n-1}^p)$$
$$= \sum_{i=0}^{n-2} m_i^p\bullet(T_{i+1} - T_i^p) - m_{n-1}\bullet(T_{n-1}^p + T_{n-1}c_1+...+T_1\bullet c_{n-1} + T_0\bullet c_n)$$

gilt, wird das Ideal I von den Elementen

$$T_{i+1} - T_i^p \text{ mit } i = 0,...,n- 2 \text{ und } T_{n-1}^p + T_{n-1}c_1+...+T_1\bullet c_{n-1} + T_0\bullet c_n$$

erzeugt, d.h. es ist

$$k[M] = S/I$$
$$\cong k[T_0,T_1,T_2,...,T_{n-1}] / (T_{i+1}-T_i^p\ ,\ T_{n-1}^p+T_{n-1}c_1+...+T_1\bullet c_{n-1}+T_0\bullet c_n \mid i=0,...,n-2)$$
$$\cong k[T_0] / (T_0^{pn}+T_0^{p(n-1)}\bullet c_1+...+T_0^p\bullet c_{n-1}+T_0\bullet c_n).$$

Diese k-Algebra ist als Faktoralgebra einer Polynomalgebra über k in einer Unbestimmten endlich erzeugt. Wir haben noch zu zeigen,

$$k[M] \cong k[T_0] / (T_0^{p^n} + T_0^{p^{n-1}} \cdot c_1 + \ldots + T_0^{p} \cdot c_{n-1} + T_0 \cdot c_n)$$

ist reduziert, d.h. das Polynom

$$\tilde{\lambda} := T_0^{p^n} + T_0^{p^{n-1}} \cdot c_1 + \ldots + T_0^{p} \cdot c_{n-1} + T_0 \cdot c_n$$

hat keine mehrfachen Nullstellen (in k). Da $\tilde{\lambda}$ die Nullstelle 0 hat, ist dies äquivalent dazu, daß die folgenden beiden Bedingungen erfüllt sind.

1. $\tilde{\tilde{\lambda}} := \tilde{\lambda}/T_0 = T_0^{p^n-1} + T_0^{p^{n-1}-1} \cdot c_1 + \ldots + T_0^{p-1} \cdot c_{n-1} + c_n$ hat keine mehrfache Nullstellen.

2. 0 ist keine Nullstelle von $\tilde{\tilde{\lambda}}$.

Weil M keine T-Torsion haben soll, ist der Koeffizient c_n ungleich Null, d.h.

Bedingung 2 ist erfüllt. Das Polynom $\tilde{\tilde{\lambda}}$ besitzt genau dann eine mehrfache Nullstelle, wenn dessen Ableitung

$$(p^{n-1}-1) \cdot T_0^{p^n-2} + (p^{n-1}-1) \cdot T_0^{p^{n-1}-2} \cdot c_1 + \ldots + (p-1) \cdot T_0^{p-2} \cdot c_{n-1}$$

identisch Null ist, d.h. wenn gilt

$$(p^{n-1}-1) \cdot 1_k = (p^{n-1}-1) \cdot c_1 = \ldots = (p^2-1) \cdot c_{n-2} = (p-1) \cdot c_{n-1} = 0.$$

Weil die Charakteristik des Grundkörpers gleich $p > 0$ ist, ist dies äquivalent zu

$$1_k = c_1 = \ldots = c_{n-2} = c_{n-1} = 0$$

Die Bedingung $1_k = 0$ ist nie erfüllt, d.h. es gilt 1.

5. Schritt. Für endlich erzeugte R(k)-Moduln M' und M'' gilt

$$k[M' \oplus M''] \cong k[M'] \otimes_k k[M''].$$

Sind insbesondere die k-Algebren k[M'] und k[M''] endlich erzeugt und reduziert, so gilt dasselbe für k[M'⊕M''] und für die zugehörigen affinen algebraischen Varietietäten ist

$$\mathcal{G}(M' \oplus M'') \cong \mathcal{G}(M') \times \mathcal{G}(M'').$$

Sei

$$M := M' \oplus M''.$$

Dann gilt

$$S_F(M) = S_F(M') \otimes_F S_F(M'').$$

(vgl. Anhang 2.10 (iv)). Seien I, I', I'' die Ideale von

$$S := S_F(M),\ S' := S_F(M') \text{ bzw. } S'' := S_F(M'')$$

mit

$$k[M] = S/I,\ k[M'] = S'/I' \text{ bzw. } k[M''] = S''/I''.$$

Für $m = m' + m'' \in M$ mit $m' \in M'$ und $m'' \in M''$ gilt

$$\begin{aligned} T \cdot m - m^p &= T \cdot m' + T \cdot m'' - (m' + m'')^p \\ &= T \cdot m' + T \cdot m'' - m'^p - m''^p \text{ (weil } p>0 \text{ die Charakteristik von F ist)} \\ &= (T \cdot m' - m'^p) + (T \cdot m'' - m''^p) \\ &\in I' \otimes 1 + 1 \otimes I'' \ (\subseteq I). \end{aligned}$$

Das dies für jedes m gilt, folgt

$$I = I' \otimes S'' + S' \otimes I'',$$

also

$$\begin{aligned} S/I &= S' \otimes S''/(I' \otimes S'' + S' \otimes I'') \\ &= (S'/I') \otimes (S''/I''), \end{aligned}$$

d.h. es ist

$$k[M] = k[M'] \otimes k[M''].$$

Die Behauptung des fünften Schritts folgt damit aus 1.5.2 und der Definition des Produkts von Varietäten (vgl. 1.5.1).

6. Schritt. Für jeden endlich erzeugten R-Modul ohne T-Torsion ist k[M] der Koordinaten-Ring einer (bis auf Isomorphie eindeutig bestimmten) affinen Varietät $\mathcal{G}(M)$.

Nach 3.3.3 (iii) ist M eine direkte Summe

$$M = M_1 \oplus \ldots \oplus M_r$$

von zyklischen Teilmoduln $M_i \cong R/R \bullet \lambda_i$ mit $\lambda_i \in R$. Weil M keine T-Torsion besitzt, gilt dasselbe für die M_i. Nach dem dritten und vierten Schritt sind die $k[M_i]$ endlich erzeugte und reduzierte k-Algebren. Nach dem fünften Schritt gilt dies auch für k[M]. Damit ist k[M] der Koordinatenring einer affinen algebraischen Varietät $\mathcal{G}(M)$:

7. Schritt. Für jeden endlich erzeugten R(k)-Modul M ohne T-Torsion besitzt $\mathcal{G}(M)$ die Struktur einer linearen algebraischen Gruppe, die den Bedingungen von (1) genügt.

Wir betrachten die k-linearen Abbildungen

$$i': M \cong M \otimes_k k \hookrightarrow S_k(M) \otimes_k S_k(M),\ m \mapsto m \otimes 1 \mapsto m \otimes 1,$$

und

$$i'': M \cong k \otimes_k M \hookrightarrow S_k(M) \otimes_k S_k(M),\ m \mapsto 1 \otimes m \mapsto 1 \otimes m.$$

Sie definieren eine k-lineare Abbildung,

$$i'+i'': M \longrightarrow S_k(M) \otimes_k S_k(M),\ m \mapsto m \otimes 1 + 1 \otimes m,$$

und damit einen k-Algebra-Homomorphismus

$$\Delta: S_k(M) \longrightarrow S_k(M) \otimes_k S_k(M),\ m \mapsto m \otimes 1 + 1 \otimes m.$$

Analog definiert die k-lineare Abbildung

$$M \longrightarrow S_k(M),\ m \mapsto -m,$$

einen k-Algebra-Homomorphismus

$$\iota: S_k(M) \longrightarrow S_k(M),\ m \mapsto -m.$$

Die Projektion auf den homogenen Bestandteil des Grades 0 bezeichnen wir mit

$$\varepsilon: S_k(M) \longrightarrow k.$$

Es ist ebenfalls ein k-Algebra-Homomorphismus. Wir zeigen als erstes, daß zu den gerade definierten Abbildungen Δ, ι und ε kommutative Diagramme gehören, die den Gruppen-Axiomen einer linearen algebraischen Gruppe ensprechen (vgl. 2.1.2). Zunächst betrachten wir das dem Assoziativgesetz entsprechende Diagramm

$$\begin{array}{ccc} A \otimes A \otimes A & \xleftarrow{\Delta \otimes id} & A \otimes A \\ {\scriptstyle id \otimes \Delta}\uparrow & & \uparrow{\scriptstyle \Delta} \\ A \otimes A & \xleftarrow{\Delta} & A \end{array}$$

(mit $A = S_k(M)$). Da es sich um ein Diagramm von k-Algebra-Homomorphismen handelt, reicht es die Kommutativität für die Elemente einer Teilmenge von A zu

überprüfen, welche die k-Algebra erzeugen, zum Beispiel für die Elemente aus $M \subseteq A$.

Ein Elemenent $m \in M$ wird wie folgt abgebildet,

$$\begin{array}{ccc} m\otimes 1\otimes 1+1\otimes m\otimes 1+1\otimes 1\otimes m & \mapsfrom & m\otimes 1+1\otimes m \\ \uparrow & & \uparrow \\ m\otimes 1+1\otimes m & \mapsfrom & m \end{array}$$

Man beachte, 1 ist ein Element vom Grad 0 und wird beim k-Algebra-Homomorphismus in sich abgebildet. Das Diagramm ist tatsächlich kommutativ.

Betrachten wir als nächstes das Diagramm

$$\begin{array}{ccc} m & \xleftarrow{id\otimes\varepsilon} & A\otimes A \\ \varepsilon\otimes id\uparrow & \nwarrow id & \uparrow\Delta \\ A\otimes A & \xleftarrow{\Delta} & A \end{array}$$

zur Existenz des Einselements. Ein Elemenent $m \in M$ wird wie folgt abgebildet,

$$\begin{array}{ccc} A & \mapsfrom & m\otimes 1+1\otimes m \\ \uparrow & \nwarrow & \uparrow \\ m\otimes 1+1\otimes m & \mapsfrom & m \end{array}$$

Man beachte die Elemente $m \in M$ werden als Elemente vom Grad 1 aus A durch die Abbildung ε in die Null abgebildet. Weil ε ein k-Algebra-Homomorphismus ist, geht das Element 1 des Grades 0 in sich über. Auch dieses Diagramm ist kommutativ.

Betrachten wir als letztes das Diagramm

$$\begin{array}{ccc} A\otimes A & \xrightarrow{\iota\otimes id} & A\otimes A \\ \Delta\uparrow & & \downarrow m \\ A & \xrightarrow{\varepsilon} & A \\ \Delta\downarrow & & \uparrow m \\ A\otimes A & \xrightarrow{id\otimes\iota} & A\otimes A \end{array}$$

zur Existenz des Inversen. Ein Elemenent $m \in M$ wird wie folgt abgebildet,

$$\begin{array}{ccc} m\otimes 1+1\otimes m & \mapsto & -m\otimes 1+1\otimes m \\ \uparrow & & \downarrow \\ m & \xrightarrow{\varepsilon} & 0 \\ \downarrow & & \uparrow \\ m\otimes 1+1\otimes m & \mapsto & m\otimes 1-1\otimes m \end{array}$$

Auch dieses Diagramm ist kommutativ. Zum Beweis der Behauptung des siebten Schritts reicht es zu zeigen, daß die Abbildungen

$$\Delta: S_k(M) \longrightarrow S_k(M)\otimes_k S_k(M),\ m \mapsto m\otimes 1 + 1\otimes m,$$

$$\iota: S_k(M) \longrightarrow S_k(M),\ m \mapsto -m,$$

$$\varepsilon: S_k(M) \longrightarrow k,$$

jeweils entsprechende Abbildungen mit der Faktoralgebra k[M] anstelle von $S_k(M)$ induzieren. Die Kommutativität der obigen Diagramme bleibt dann beim Übergang zur Faktoralgebra k[M] erhalten, so daß k[M] tatsächlich der Koordinatenring einer lineare algebraischen Gruppe ist, welche den Bedingungen von (1) genügt.

Sei $\rho: S_k(M) \longrightarrow k[M]$ die natürliche Abbildung auf die Faktoralgebra. Für $m \in I$ gilt

$$\Delta(m) = m\otimes 1+1\otimes m \in I\otimes S_k(M) + S_k(M)\otimes I,$$

also

$$(\rho\otimes\rho)(\Delta(m)) = 0\otimes S_k(M) + S_k(M)\otimes 0 = 0.$$

Deshalb liegt I im Kern von $(\rho\otimes\rho)\circ\Delta$. Die Abbildung faktorisiert sich über ρ und wir erhalten einen k-Algebra-Homomorphismus

$$\overline{\Delta}: k[M] \longrightarrow k[M]\otimes_k k[M],\ \overline{m} \mapsto \overline{m}\otimes 1 + 1\otimes\overline{m},$$

für welchen das Diagramm

$$\begin{array}{ccc} S_k(M) & \xrightarrow{\Delta} & S_k(M)\otimes S_k(M) \\ \rho\downarrow & & \downarrow\rho\otimes\rho \\ k[M] & \xrightarrow{\overline{\Delta}} & k[M]\otimes k[M] \end{array}$$

kommutativ ist.

Für $m \in I$ gilt $\iota(m) = -m \in I$. Deshalb liegt I im Kern der Zusammensetzung $\rho\circ\iota$. Die Abbildung faktorisiert sich über ρ und wir erhalten einen k-Algebra-Homomorphismus

$$\overline{\iota}: k[M] \longrightarrow k[M],\ \overline{m} \mapsto -\overline{m},$$

für welchen das Diagramm

$$\begin{array}{ccc} S_k(M) & \xrightarrow{\iota} & S_k(M) \\ \rho\downarrow & & \downarrow\rho \\ k[M] & \xrightarrow{\overline{\iota}} & k[M] \end{array}$$

kommutativ ist.

Das Ideal $I \subseteq S_k(M)$ wird von Elementen erzeugt, deren homogener Bestandteil der Grades 0 gleich 0 ist. Deshalb liegt I im Kern von $\varepsilon: S_k(M) \longrightarrow k$ und faktorisiert sich ε über ρ und definiert so einen k-Algebra-Homomorphismus $\overline{\varepsilon}: k[M] \longrightarrow k$, für welchen das Diagramm

$$\begin{array}{ccc} S_k(M) & \xrightarrow{\varepsilon} & k \\ \rho\downarrow & \nearrow_{\overline{\varepsilon}} & \\ k[M] & & \end{array}$$

kommutativ ist.

Nach Konstruktion bleibt die Kommutativität der obigen Diagramme erhalten, wenn man $S_k(M)$ durch k[M] und Δ, ι und ε durch $\overline{\Delta}$, $\overline{\iota}$ und $\overline{\varepsilon}$ ersetzt. Die Abbildungen $\overline{\Delta}$,

$\overline{\iota}$ und $\overline{\varepsilon}$ definieren damit auf der affinen algebraischen Varietät $\mathcal{G}(M)$ des fünften Schritts mit dem Koordinatenring k[M] die Struktur einer linearen algebraischen Gruppe mit der Komultiplikation $\overline{\Delta}$, dem Antipoden $\overline{\iota}$ und der Auswertung $\overline{\varepsilon}$ im neutralen Element. Diese genügen den Bedingungen von (1). Damit sind die Aussagen des zweiten Schritts bewiesen.

Bemerkungen

1. Damit ist der Beweis der Behauptung reduziert auf den Beweis der Aussage, daß die Funktoren $\mathcal{A}$ und $\mathcal{G}$ der ersten beiden Schritte quasi-invers zueinander sind. Dazu betrachten wir für jeden endlich erzeugten R(k)-Modul M ohne T-Torsion die Zusammensetzung

$$j := j_M : M \overset{i}{\hookrightarrow} S_k(M) \overset{\rho}{\twoheadrightarrow} k[M] = k[\mathcal{G}(M)] \tag{3}$$

der natrülichen Einbettung i des k-Vektorraums M in die symmetrische Algebra mit der natürlichen Abbildung ρ auf die Faktor-Algebra k[M], die nach Definition von $\mathcal{G}(M)$ gerade der Koordinatenring der elementar unipotenten Gruppe $\mathcal{G}(M)$ ist. Nach Definition ist j eine k-lineare Abbildung. Bezeichnet $\Delta = \Delta_M$ die Komultiplikation der Gruppe $\mathcal{G}(M)$, so gilt

$$\Delta(j(m)) = j(m)\otimes 1 + 1\otimes j(m)$$

für jedes $m \in M$ (nach Definition von Δ). Deshalb liegt das Bild von j ganz im R(k)-Modul der additiven Funktionen von $\mathcal{G}(M)$,

$$j(M) \subseteq \mathcal{A}(\mathcal{G}(M)), \tag{4}$$

(nach Bemerkung 3.3.1 A (ii), zur R(k)-Modulstruktur von M, siehe 3.3.4). Weiter ist

$j(T\bullet m) = j(m^p)$ (nach Defintion von k[M])
$= j(m)^p$ (ρ ist ein k-Algebra-Homomorphismus)
$= T\bullet j(m)$ (Definition der R-Modulstruktur von $\mathcal{A}(\mathcal{G}(M))$ in 3.3.4)

Damit ist die Abbildung j ein Homomorphismus von R-Moduln, wenn wir sie als Abbildng mit Werten in $\mathcal{A}(\mathcal{G}(M))$ betrachten,

$$j: M \longrightarrow \mathcal{A}(\mathcal{G}(M)) \text{ ist R(k)-linear.} \tag{5}$$

Man beachte,

j ist funktorieller Morphismus bezüglich M

(als Zusammensetzung von funktoriellen Morphismen). Als nächstes wollen wir zeigen, daß (5) ein Isomorphismus von R(k)-Moduln ist. Wir gehen vor wie bisher und beweisen dies zunächst für die zyklischen direkten Summanden von M.

2. Weiter betrachten wir für jede elementar unipotente Gruppe G die natürliche Einbettung

$$i: \mathcal{A}(G) \hookrightarrow k[G].$$

Weil die k-Algebra k[G] von $\mathcal{A}(G)$ erzeugt wird (nach 3.4.7 (ii)), ist der induzierte k-Algebra-Homomorphismus

$$s := S(i): S_k(\mathcal{A}(G)) \longrightarrow\!\!\!\!\!\rightarrow k[G] \tag{7}$$

surjektiv (und stimmt auf $\mathcal{A}(G) \subseteq S_k(\mathcal{A}(G))$ mit der identischen Abbildung

überein). Für $m \in \mathcal{A}(G)$ gilt

$s(T\bullet m - m^p) = s(T\bullet m) - s(m)^p$ (s ist ein k-Algebra-Homomorphismus)
$= i(T\bullet m) - i(m)^p$ (s ist eine Fortsetzung von i)

$= T\bullet m - m^p$ (i ist die identische Abbildung)
$= 0$ (nach Definition der Operation von R(k) auf $\mathcal{A}(G)$)

Damit wird das (im zweiten Schritt definierte) Ideal $I = I(\mathcal{A}(G))$ in die Null abgebildet, d.h. s faktorisiert sich über $k[\mathcal{A}(G)]$ und induziert einen surjektiven k-Algebra-Homomorphismus

$$\overline{s}: k[\mathcal{G}(\mathcal{A}(G))] = k[\mathcal{A}(G)] \twoheadrightarrow k[G]. \qquad (8)$$

Nach Konstruktion ist die Zusammensetzung

$$\mathcal{A}(G) \longrightarrow k[\mathcal{G}(\mathcal{A}(G))] \xrightarrow{\overline{s}} k[G]$$

der natürlichen Abbildung mit $\overline{s}$ die identische Abbildung. Weil j_M auch für $M = \mathcal{A}(G)$ ein Isomorphismus ist, haben G und $\mathcal{G}(\mathcal{A}(G))$ dieselben addititiven Funktionen. Wegen der Surjektivität von $\overline{s}$ können wir G als abgeschlossene Untergruppe von $\mathcal{G}(\mathcal{A}(G))$ betrachten,

$$\overline{s}^{\#}: G \hookrightarrow \mathcal{G}(\mathcal{A}(G)). \qquad (9)$$

Wir wollen zeigen, daß diese beiden Gruppen sogar gleich sind. Nach 3.4.7 (iii) ist G ein direktes Produkt von endlich vielen abgeschlossenen Untergruppen der Gestalt $\mathbf{G}_a$ und endlich vielen endlichen Gruppen der Ordnung p. Auch hier beweisen wir die Aussage zunächst für die direkten Faktoren.

8. Schritt. Im Fall M = R(k) ist (5) ein Isomorphismus.
Nach dem dritten Schritt ist j als Abbildung mit Werten in $k[\mathcal{G}(R(k))] = k[R(k)]$ von der Gestalt

$$R(k) \longrightarrow k[T_0], \ \sum_{i\geq 0} f_i \bullet T^i \mapsto \sum_{i\geq 0} f_i \bullet T_0^{p^i}.$$

Insbesondere ist der Koordinatenring von $\mathcal{G}(R(k))$ ein Polynomring über k in einer Unstimmten,

$$k[\mathcal{G}(R(k)] = k[T_0],$$

und

$$\mathcal{G}(R(k) \cong \mathbf{G}_a$$

die additive Gruppe.

Die Abbildung j ist injektiv (wegen der linearen Unabhängigkeit der $T_0^{p^i}$). Wir haben noch zu zeigen, ihr Bild ist gleich $\mathcal{A}(\mathcal{G}(R(k)))$, d.h. daß jede additive Funktion auf $\mathcal{G}(R(k)) = \mathbf{G}_a$ hat die Gestalt

$$\sum_{i\geq 0} f_i \bullet T_0^{p^i} \in k[T_0].$$

Das ist aber der Fall nach 3.3.5 (mit n = 1, vgl. auch die Aussage des ersten Schritts im Beweis).

9. Schritt. Im Fall $M = R(k)/R(k)\bullet\lambda$ mit einem $\lambda \in R(k)-\{0\}$ ist (5) ein Isomorphismus.

Nach dem vierten Schritt hat λ die Gestalt

$$\text{mit } \lambda = T^n + T^{n-1}\bullet c_1 + \ldots + T\bullet c_{n-1} + c_n \text{ mit } c_i \in k \text{ für jedes i und } c_n \neq 0.$$

und die Restklassen der T^i mit i = 0, ... , n-1 bilden eine Basis von M als als k-Vektorraum, d.h. mit

$$t := T \bmod R(k)\bullet\lambda$$

ist

$$M = k + k\bullet t + k\bullet t^2 + ... + k\bullet t^{n-1} \text{ mit } 1, t, t^2,...,t^{n-1} \text{ linear unabhängig über k.} \quad (10)$$

Ebenfalls nach dem vierten Schritt ist

$$k[M] = k[T_0] / k[T_0](T_0^{p^n}+T_0^{p^{n-1}}\bullet c_1+...+T_0^{p}\bullet c_{n-1}+T_0\bullet c_n),$$

mit

$$t_0 := T_0 \bmod k[T_0](T_0^{p^n}+T_0^{p^{n-1}}\bullet c_1+...+T_0^{p}\bullet c_{n-1}+T_0\bullet c_n)$$

also

$$k[M] = k + k\bullet t_0 + ... + k\bullet t_0^{p^n-1} \text{ mit } 1, t_0,...,t_0^{p^n-1} \text{ linear unabhängig über k,} \quad (11)$$

und j ist die Abbildung

$$M \longrightarrow k[M], \sum_{i=0}^{n-1} f_i\bullet t^i \mapsto \sum_{i=0}^{n-1} f_i\bullet t_0^{p^i}.$$

Wegen der linearen Unabhängigkeit der $1, t_0,...,t_0^{p^n-1}$ über k ist auch diese Abbildung injektiv. Wir haben zu zeigen ist Bild ist gleich $\mathcal{A}(\mathcal{G}(M))$, d.h. zu zeigen ist, jede additive Funktion aus $k[M] = k[\mathcal{G}(M)]$ hat die Gestalt

$$\sum_{i=0}^{n-1} f_i\bullet t_0^{p^i} \text{ mit } f_i \in k \text{ für jedes i.}$$

Sei also

$$f = \sum_{i=0}^{p^n-1} f_i\bullet t_0^{i}$$

eine additive Funktion auf der Untergruppe

$$\mathcal{G}(M) = V(\tilde{\lambda})$$

$$= \{c \in k \mid \tilde{\lambda}(c) = 0\}$$

der additiven Gruppe $\mathbf{G}_a$ mit der Gleichung

$$\tilde{\lambda}(T_0) := T_0^{p^n}+T_0^{p^{n-1}}\bullet c_1+...+T_0^{p}\bullet c_{n-1}+T_0\bullet c_n = 0.$$

Man beachte $\tilde{\lambda}$ ist ein additves Polynom. Dann gilt

$$f(x+y) - f(x) - f(y) = 0 \text{ für beliebige } x,y \in \mathcal{G}(M) \subseteq \mathbf{G}_a = k.$$

Nach (11) können wir k[M] mit dem k-lineare Unterraum von $k[T_0]$ identifizieren, der von den Potenzen T_0^i mit $i = 0,..., p^{n-1}$ erzeugt wird (indem wir t_0 mit T_0 identifizieren). Dann ist das Polynom

$$f(T_0+y) - f(T_0) - f(y)$$

für jedes $x \in \mathcal{G}(M)$ an der Stelle x gleich Null. Dieses Polynom hat einen Grad $<p^n$ hat aber p^n verschiedene Nullstellen, denn die Gruppe

$$\mathcal{G}(M) = V(c)$$

besteht aus genau p^n Punkten (weil $\tilde{\lambda} = T_0^{p^n} + T_0^{p^{n-1}} \cdot c_1 + \ldots + T_0^{p} \cdot c_{n-1} + T_0 \cdot c_n$ den Grad p^n besitzt und nach dem vierten Schritt keine mehrfachen Nullstellen hat). Deshalb ist das Polynom

$$f(T_0+y) - f(T_0) - f(y) = 0$$

identisch Null. Alle seine Koeffizienten sind also gleich Null. Diese Koeffizienten sind Polynome in y, deren Grad ebenfalls $< p^n$ ist. Da aber $y \in \mathcal{G}(M)$ genau p^n verschiedene Werte annehmen kann, sind es ebenfalls Polynome, die identisch Null sein müssen. Damit ist das Polynom

$$f(T_0+U_0) - f(T_0) - f(U_0) \in \bigoplus_{i,j=}^{p^{n-1}} k \cdot T_0^i U_0^j \subseteq k[T_0, U_0]$$

ebenfalls identisch Null. Wir haben gezeigt, die vorgegeben additive Funktion

$$f \in \mathcal{A}(\mathcal{G}(M))$$

von $\mathcal{G}(M)$ ist die Einschränkung einer addiven Funktion auf $\mathbf{G}_a$,

$$f = \tilde{f}|_{\mathcal{G}(M)} \text{ mit } \tilde{f} \in \mathcal{A}(\mathbf{G}_a) \text{ und } \deg \tilde{f} < p^n.$$

Als additive Funktion auf $\mathbf{G}_a$ ist aber $\tilde{f}$ eine k-Linearkombination von Funktionen der Gestalt $T_0^{p^i}$ (mit $i < p^n$ wegen $\deg \tilde{f} < p^n$). Dann ist aber die Einschränkung $f = \tilde{f}|_{\mathcal{G}(M)}$ eine k-Linearkombination von Funktionen der Gestalt $t_0^{p^i}$ mit $i < p^n$, wie behauptet.

10. Schritt. Sei $M = M' \oplus M''$ eine direkte Summe von endlich erzeugten R(k)-Moduln M' und M'' ohne T-Torsion, für welche die natürlichen Abbildungen (3), sagen wir,

$$j': M' \longrightarrow k[\mathcal{G}(M')] \text{ und } j'': M'' \longrightarrow k[\mathcal{G}(M'')]$$

Isomorphismen von R(k)-Moduln

$$j': M' \xrightarrow{\cong} \mathcal{A}(\mathcal{G}(M')) \text{ und } j'': M'' \xrightarrow{\cong} \mathcal{A}(\mathcal{G}(M''))$$

sind. Dann ist auch

$$j := j_M : M \longrightarrow \mathcal{A}(\mathcal{G}(M))$$

ein Isomorphismus von R-Moduln.

Nach (5) ist j eine R-lineare Abbildung. Wir haben zu zeigen, daß sie bijektiv ist. Weil (5) ein funktorieller Morphismus ist, führen die natürlichen Einbettungen

$$M' \hookrightarrow M' \oplus M'' \text{ und } M'' \hookrightarrow M' \oplus M''$$

zu kommutativen Diagrammen

$$\begin{array}{ccc} M' & \hookrightarrow & M' \oplus M'' \\ j' \downarrow \cong & & \downarrow j \\ \mathcal{A}(\mathcal{G}(M')) & \longrightarrow & \mathcal{A}(\mathcal{G}(M' \oplus M'')) \end{array} \quad \text{und} \quad \begin{array}{ccc} M'' & \hookrightarrow & M' \oplus M'' \\ j'' \downarrow \cong & & \downarrow j \\ \mathcal{A}(\mathcal{G}(M'')) & \longrightarrow & \mathcal{A}(\mathcal{G}(M' \oplus M'')) \end{array}$$

Nach dem fünften Schritt gilt

$$G = G' \times G''$$

und die Projektionen auf die beiden Faktoren induzieren (als surjektive Abbildungen) Injektionen der Koordinatenringe

$$k[\mathcal{G}(M')] = k[G'] \hookrightarrow k[G' \times G] = k[\mathcal{G}(M' \oplus M'')] \text{ und}$$

$$k[\mathcal{G}(M'')] = k[G''] \hookrightarrow k[G'\times G] = k[\mathcal{G}(M'\oplus M'')],$$

deren Einschränkungen auf die additiven Funktionen gerade die unteren horizontalen Abbildungen der beiden Diagramme sind. Letztere sind also injektiv und können als natürlichen Einbettungen betrachtete werden.

$$\begin{array}{ccc} M' & \overset{q'}{\hookrightarrow} & M'\oplus M'' \\ {\scriptstyle j'}\downarrow\cong & & \downarrow{\scriptstyle j} \\ \mathcal{A}(\mathcal{G}(M')) & \overset{\widetilde{q}'}{\hookrightarrow} & \mathcal{A}(\mathcal{G}(M'\oplus M'')) \end{array} \quad \text{und} \quad \begin{array}{ccc} M'' & \overset{q''}{\hookrightarrow} & M'\oplus M'' \\ {\scriptstyle j''}\downarrow\cong & & \downarrow{\scriptstyle j} \\ \mathcal{A}(\mathcal{G}(M'')) & \overset{\widetilde{q}''}{\hookrightarrow} & \mathcal{A}(\mathcal{G}(M'\oplus M'')) \end{array}$$

Ist

$$h\colon G = G'\times G'' \longrightarrow \mathbf{G}_a$$

eine additive Funktion auf G, so sind

$$h'\colon G' = G'\times\{e''\} \hookrightarrow G'\times G'' \xrightarrow{h} \mathbf{G}_a$$

und

$$h''\colon G'' = \{e'\}\times G' \hookrightarrow G'\times G'' \xrightarrow{h} \mathbf{G}_a$$

additve Funktionen auf G' bzw. G''. Außerdem gilt für $x \in G'$ und $y \in G''$:

$$h(x,y) = h((x,e'')\bullet(e',y)) = h(x,e'')+h(e',y) = h'(x)+h''(y).$$

Nach Voraussetzung liegt h' im Bild von j' und h'' im Bild von j''. Beide liegen also im Bild von j. Dann liegt aber auch $h = h' + h''$ im Bild von j. Wir haben gezeigt,

j ist surjektiv.

Wir haben noch die Injektivität von j zu beweisen. Sei

$$(m',m'') \in \mathrm{Ker}(j).$$

Wir betrachten die additiven Funktionen

$$h' = j'(m')\colon G' \longrightarrow \mathbf{G}_a \text{ und } h'' = j''(m'')\colon G'' \longrightarrow \mathbf{G}_a$$

von G' bzw. G''. Dann ist

$$h := h' + h''\colon G = G'\times G'' \longrightarrow \mathbf{G}_a,\ (x,y) \mapsto h'(x) + h''(y),$$

eine additive Funktion auf G mit

$$\begin{aligned} h &= \widetilde{q}'j'(m') + \widetilde{q}''j''(m'') \\ &= j(q'(m')) + j(q''(m'')) \\ &= j((m',0) + (0,m'')) \\ &= j(m',m'') \\ &= 0 \qquad \text{(weil } (m', m'') \text{ im Kern von j liegt).} \end{aligned}$$

Weil die Abbildung h identisch Null ist, sind auch die Einschränkungen

$$h' = h|_{G'}, \text{ und } h'' = h|_{G''}$$

identisch Null,

$$0 = h' = j'(m') \text{ und } 0 = h'' = j''(m'').$$

Weil j' und j'' injektiv sind, gilt $m' = 0$ und $m'' = 0$. Wir haben gezeigt, der Kern von j ist trivial, d.h. j ist injektiv.

11. Schritt. Für jeden endlich erzeugten R-Modul M ohne T-Torsion ist die natürliche Abbildung

$$j := j_M\colon M \longrightarrow \mathcal{A}(\mathcal{G}(M))$$

von (5) ein (funktorieller) Isomorphismus von R(k)-Moduln.

Nach 3.3.3 (iii) zerfällt M in eine direkte Summe von zyklischen R-Moduln. Nach dem achten und neunten Schritt ist j_M für zyklische M ein Isomorphismus. Nach dem

zehnten Schritt ist damit auch j_M für beliebige (endlich erzeugte M ohne T-Torsion) ein Isomorphimus. Weil j funktoriell ist, erhalten wir so einen funktoriellen Isomorphismus

$$j: \mathrm{Id} \xrightarrow{\cong} \mathcal{A}\circ\mathcal{G}.$$

12. Schritt. Für $G = \mathbf{G}_a$ gilt in (9) das Gleichheitszeichen.

Der Koordinatenring von G ist ein Polynomring über k in einer Unbestimmten, sagen wir

$$k[G] = k[T].$$

Für den R(k)-Modul der additiven Funktionen erhalten wir

$$\mathcal{A}(G) = \sum_{i\geq 0} k\bullet T^{p^i}$$

(nach 3.3.5, erster Schritt im Beweis). Wenn wir das Bild von T^{p^i} bei der natürlichen Einbettung

$$\mathcal{A}(G) \hookrightarrow S_k(\mathcal{A}(G))$$

mit T_i bezeichnen, bekommt die symmetrische Algebra die Gestalt

$$S_k(\mathcal{A}(G)) = k[T_0, T_1, T_2, ...]$$

und der k-Algebra-Homomorphismus (11) läßt sich in der Gestalt

$$S_k(\mathcal{A}(G)) = k[T_0, T_1, T_2, ...] \longrightarrow k[T] = k[G],\ T_i \longrightarrow T^{p^i},$$

schreiben. Das Ideal $I = I(\mathcal{A}(G))$ wird von den Elementen $T_{i+1} - T_i^p$ erzeugt, es gilt

$$\overline{s}: k[\mathcal{G}(\mathcal{A}(G))] = k[\mathcal{A}(G)] = S_k(\mathcal{A}(G))/(T_{i+1} - T_i^p \mid i = 0, 1, ...) = k[T_0].$$

und die induzierte Abbildung (8) ist der k-Algebra-Homomorphismus

$$\overline{s}: k[\mathcal{G}(\mathcal{A}(G))] = k[\mathcal{A}(G)] = k[T_0] \twoheadrightarrow k[T] = k[G],\ T_0 \mapsto T.$$

Weil $\overline{s}$ ein Isomorphismus ist, gilt dasselbe für die abgeschlossene Einbettung

$$\overline{s}^{\#}: G \hookrightarrow \mathcal{G}(\mathcal{A}(G)),$$

d.h. ist (9) gilt das Gleichheitszeichen.

13. Schritt. Für $G = \mathbb{Z}/p\mathbb{Z}$ gilt in (9) das Gleichheitszeichen.

Wir können G mit der abgeschlossenen Untergruppe von $\mathbf{G}_a = k$ mit der Gleichung

$$T^p - T = 0$$

identifizieren,

$$G = \{c \in k \mid x^p - x = 0\}.$$

Der Koordinatenring von G bekommt so die Gestalt

$$k[G] = k[T]/(T^p - T) = k\bullet 1 + k\bullet t + ... + k\bullet t^{p-1}.$$

mit

$$t = T \bmod (T^p - T).$$

Für den R(k)-Modul der additiven Funktionen erhalten wir

$$\mathcal{A}(G) = k\bullet t,$$

denn rechts steht ein k-Vektorraum aus additiven Funktionen, und der k-Vektorraum $\mathcal{A}(G)$ hat eine Dimension ≤ 1, weil eine additive Funktion f auf einer zyklischen Gruppe bereits durch ihren Wert im Erzeuger $1_k \in k$ festgelegt ist:

$$f(n\bullet 1_k) = n\bullet f(1_k) \text{ für } n = 0, 2,3,..., p-1.$$

Die symmetrische k-Algebra über $\mathcal{A}(G)$ hat die Gestalt

$$S_k(\mathcal{A}(G)) \cong k[T_0]$$

und die Abbildung (11) ist der k-Algebra-Homomorphismus[41]

$$S_k(\mathcal{A}(G)) = k[T_1] \twoheadrightarrow k[T]/(T^p - T) = k[G],\ T_1 \mapsto t = T \bmod (T^p - T).$$

Das Ideal $I = I(\mathcal{A}(G))$ wird erzeugt von $T \bullet T_1 - T_1^p = T_1 - T_1^p$ (wegen $T \bullet t = t^p = t$ in $k \bullet t$).

Damit gilt

$$k[\mathcal{G}(\mathcal{A}(G))] = k[\mathcal{A}(G)] = k[T_1]/(T_1^p - T_1)$$

und der induzierte k-Algebra-Homomorphismus $\bar{s}$ hat die Gestalt

$$\bar{s}: k[\mathcal{G}(\mathcal{A}(G))] = k[T_1]/(T_1^p - T_1) \twoheadrightarrow k[T]/(T^p - T) = k[G],$$

$$T_1 \bmod (T_1^p - T_1) \mapsto T \bmod (T^p - T),$$

ist also ein Isomorphismus. Die abgeschlossenene Einbettung (9) ist damit bijektiv, d.h. es gilt das Gleichheitszeichen in (9).

14. Schritt. Seien G' und G" elementar abelsche Gruppen, für welche in (9) das Gleichheitszeichen gilt,

$$G' = \mathcal{G}(\mathcal{A}(G')) \text{ und } G'' = \mathcal{G}(\mathcal{A}(G''))$$

Dann gilt für $G := G' \times G''$ in (9) ebenfalls das Gleichheitszeichen,

$$G = \mathcal{G}(\mathcal{A}(G)).$$

Nach dem fünften Schritt gilt

Es gilt

$$\begin{aligned} G &= G' \times G'' && \text{(nach Definition von G)} \\ &= \mathcal{G}(\mathcal{A}(G')) \times \mathcal{G}(\mathcal{A}(G'')) && \text{(nach Voraussetzung)} \\ &= \mathcal{G}(\mathcal{A}(G') \oplus \mathcal{A}(G'')) && \text{(nach dem fünften Schritt)} \end{aligned}$$

Nach dem zehnten Schritt ist deshalb

also

$$\begin{aligned} \mathcal{A}(G) &= \mathcal{A}(\mathcal{G}(\mathcal{A}(G') \oplus \mathcal{A}(G''))) \\ &= \mathcal{A}(G') \oplus \mathcal{A}(G'') && \text{(nach dem 10.Schritt mit } M = \mathcal{A}(G') \oplus \mathcal{A}(G'')) \end{aligned}$$

Es folgt

$$\begin{aligned} \mathcal{G}(\mathcal{A}(G)) &= \mathcal{G}(\mathcal{A}(G') \oplus \mathcal{A}(G'')) \\ &= G. \end{aligned}$$

15. Schritt. Für jede elementar unitäre Gruppe G gilt in (9) das Gleichheitszeichen. Als elementar unitäre Gruppe ist G ein Produkt von endliche vielen Gruppen, die isomorph sind zu $\mathbf{G}_a$ oder zu einer zyklischen Gruppe der Ordnung p. Nach dem 14. Schritt reicht es zu zeigen, daß die Behauptung für jeden dieser Faktoren gilt. Das ist aber nach dem 12. und 13 Schritt der Fall.

16. Schritt. Der Funktor

$$\mathcal{A}: \begin{pmatrix} \text{Kategorie der elementar unipotenten Gruppen} \\ \text{und Homorphismen algebraischer Gruppen} \end{pmatrix} \longrightarrow \begin{pmatrix} \text{Kategorie der endlich} \\ \text{erzeugten R(k)-Moduln} \\ \text{ohne T-Torsion} \end{pmatrix}$$

eine Anti-Äquivalenz von Kategorien.

Auf Grund der funktoriellen Isomorphie des 11.ten Schritts, ist jeder endlich erzeugte R(k)-Modul M ohne T-Torsion isomorph zu einem Modul der Gestalt $\mathcal{A}(G)$ mit einer elementar unipotenten Gruppe G (nämlich $G = \mathcal{G}(M)$).

---

[41] Wir verwenden die Bezeichnung T_1 für das Bild des Erzeugers $t = t^1$ von $\mathcal{A}(G)$ in der symmetrischen Algebra.

Zum Beweis der Behauptung reicht es daher zu zeigen, für je zwei elementar unipotente Gruppen G und G' ist die Abbildung

$$\mathrm{Hom}(G, G') \longrightarrow \mathrm{Hom}_R(\mathcal{A}(G), \mathcal{A}(G')),\ h \mapsto \mathcal{A}(h) = h^*, \qquad (12)$$

bijektiv (vgl. Bucur & Deleanu [1], Kapitel I, §6, Proposition 1.19).
Beweis der Injektivität der Abbildung (12).
Abbildung (12) ist ein Homomorphismus von abelschen Gruppen, denn für je zwei Elemente $a, b \in \mathrm{Hom}(G, G')$, jedes $f \in \mathcal{A}(G')$ und jedes $x \in G$ gilt

$$\begin{aligned}((a\bullet b)^*(f))(x) &= (f\circ(a\bullet b))(x)\\ &= f((a\bullet b)(x))\\ &= f(a(x)\bullet b(x))\\ &= f(a(x)) + f(b(x)) \qquad \text{(weil f additiv ist)}\\ &= a^*(f)(x) + b^*(f)(x)\\ &= ((a^*+b^*)(f))(x).\end{aligned}$$

Weil dies für alle $x \in G$ und alle $f \in \mathcal{A}(G')$ gilt, folgt

$$(a\bullet b)^* = a^* + b^*,$$

d.h. (12) ist ein Gruppen-Homomorphismus. Sei $h \in \mathrm{Hom}(G, G')$ im Kern der Abbildung (12). Dann gilt $h^*(f) = 0$ für jedes $f \in \mathcal{A}(G')$, d.h.

$$G \xrightarrow{h} G' \xrightarrow{f} \mathbf{G}_a$$

ist für jedes $f \in \mathcal{A}(G')$ die Null-Abbildung. Weil die additiven Funktionen auf G' die k-Algebra k[G] erzeugen (nach 3.4.7 (ii)), gibt es additive Funktionen $f_1,\ldots f_r : G' \longrightarrow \mathbf{G}_a$ derart, daß

$$G \longrightarrow \mathbf{G}_a^r = k^r,\ x \mapsto \begin{pmatrix} f_1(x) \\ \cdots \\ f_{r(x)} \end{pmatrix},$$

eine abgeschlossene Einbettung von G in die $\mathbf{G}_a^r$ ist. Wegen $(f_i\circ h)(x) = 0$ für jedes i und jedes $x \in G$ ist $h(x)$ das neutrale Element von G' für jedes $x \in h$, d.h. $h: G \longrightarrow G'$ ist der triviale Homomorphismus (der alles ins neutrale Element von G' abbildet). Wir haben gezeigt, der Kern der Abbildung (12) ist trivial.
Beweis der Surjektivität der Abbildung (12).
Wir betrachten den funktoriellen Morphismus (5),

$$j = j_M : M \longrightarrow \mathcal{A}(\mathcal{G}(M)) \hookrightarrow k[\mathcal{A}(\mathcal{G}(M))],$$

zusammen mit der natürlichen Einbettung der additiven Funktionen in den Koordinatenring für den Spezialfall $M = \mathcal{A}(G)$. Auf Grund der Funktorialität erhalten wir für jeden Homomorphismus

$$h: \mathcal{A}(G) \longrightarrow \mathcal{A}(G')$$

von R-Moduln ein kommutatives Diagramm

$$\begin{array}{ccc} \mathcal{A}(G) & \longrightarrow & k[\mathcal{G}(\mathcal{A}(G))] \\ h\downarrow & & \mathcal{G}(\mathcal{A}(h))^*\downarrow \\ \mathcal{A}(G') & \longrightarrow & k[\mathcal{G}(\mathcal{A}(G'))] \end{array}$$

Dabei ist die rechte vertikale Abbildung der k-Algebra-Homomorphismus welcher induziert wird durch den Homomorphismus algebraischer Gruppen

$$\mathcal{G}(\mathcal{A}(h)): \mathcal{G}(\mathcal{A}(G')) \longrightarrow \mathcal{G}(\mathcal{A}(G)).$$

Weil nach dem 15.ten Schritt in (9) das Gleichheitszeichen gilt, können wir das Diagramm auch in der folgenden Gestalt schreiben.

$$\begin{array}{ccc} \mathcal{A}(G) & \longrightarrow & k[G] \\ h\downarrow & & \mathcal{G}(\mathcal{A}(h))^*\downarrow \\ \mathcal{A}(G') & \longrightarrow & k[G'] \end{array}$$

Es gibt also einen Homomorphismus linearer algebraischer Gruppen

$$\mathcal{G}(\mathcal{A}(h)): G' \longrightarrow G,$$

für welchen die induzierte Abbildung der Koordinantenringe

$$k[G] \longrightarrow k[G']$$

eine Einschränkung auf $\mathcal{A}(G)$ besitzt, die mit h übereinstimmt. Mit anderen Worten, h liegt im Bild der Abbildung (12). Weil dies für jedes h gilt, ist (12) surjektiv.
QED.

3.4.10 Aufgabe 2

Die Charakteristik p des Grundkörpers k sei > 0. Bezeichne c =c(T,U) den 2-Kozyklus von 3.4.3. Weiter G die algebraische Gruppe

$$G := k^2$$

mit der Multiplikation

$$(x,x')\bullet(y,y') = (x+x',\ y+y'+c(x,x')) \text{ für } x,x,y,y' \in k.$$

Zeigen Sie, G ist nicht isomorph zu $\mathbf{G}_a^2$.

Bemerkungen

(i) Wenn die angegebene Definition des Produkts $(x,x')\bullet(y,y')$ die Operatation einer Gruppe wäre, so müßte diese Gruppe ein neutrales Element besitzten, sagen wir

$$(e, e') \in k^2,$$

mit der Eigenschaft, daß

$$(e,e')\bullet(y,y') = (y, y')$$

gilt für beliebige $y, y' \in k$, d.h.

$$(e+e',\ y+y'+c(e,e')) = (y, y'),$$

d.h.

$$e+e' = y \text{ und } y+y' + c(e,e') = y',$$

d.h.

$$y = e+e' = -c(e,e').$$

Diese Relation besteht aber nicht für alle $(y, y') \in k^2$, nur für die mit

$$y = e+e' = -c(e,e').$$

(ii) Die Theorie der Erweiterung von Gruppen und der Begriff des halbdirekten Produkts (vgl. MacLane [1], Kapitel IV, §1 oder Weibel [1], Kapitel 6, Abschnitt 6.4 unmittelbar vor Definitin 6.4.9) legen es nahe, daß die obige Definition durch die folgende ersetzt werden sollte.

$$(x,x')+(y,y') = (x+y,\ x'+y'+c(x,y)) \text{ für } x,x,y,y' \in k.$$

Wir haben hier das Pluszeichen zur Bezeichnung der Gruppen-Operation verwendet, damit in den folgenden Ausführungen unmißverständlich klar ist, von welcher Operation die Rede ist. Die Verwendung von "+" ist auch deshalb naheliegend, weil die betrachteten Gruppen abelsch sind.

(iii) Die nachfolgenden Betrachtungen legen nahe, daß die in 3.4.3 eingeführte Kozyklenbedingung $\partial f = 0$ durch die ursprünglich von Lazard eingeführte ersetzt werden sollte. Die im Buch von Springer verwendete Definition funktioniert nur, weil die betrachteten Gruppen kommutativ und die Funktionen c(x,y) symmetrisch in x und y sind.

Beweis. Zeigen wir zunächst, daß der k^2 mit der in Bemerkung (ii) angegebenen Operation eine lineare algebraische Gruppe ist. Nach Definition sind die Koodinaten der Summe zweier Punkte Polynome in den Koordinaten der Summanden. Die Operation ist somit eine reguläre Abbildung. Wir haben noch zu zeigen, daß es eine Gruppen-Operaton ist.

1. Schritt. Es gilt das Assoziativgesetzt, d.h. es ist

$$((x,x')+(y,y')) + (z,z') = (x,x') + ((y, y') + (z,z'))$$

für beliebige x, y, z, x',y', z' ∈ k.

Nach Defintion gilt

$$\begin{aligned}((x,x')+(y,y')) + (z,z') &= (x+y, x'+y'+c(x,y)) + (z,z') \\ &= (x+y+z, x'+y'+z' + c(x,y) + c(x+y,z))\end{aligned}$$

und

$$\begin{aligned}(x,x') + ((y, y') + (z,z')) &= (x,x') + (y+z,y'+z'+c(y,z)) \\ &= (x+y+z, x'+y'+z'+c(y,z) + c(x,y+z)).\end{aligned}$$

Die Gültigkeit des Assoziativgesetzes ist somit äquivalent zu

$$c(x,y) + c(x+y,z) = c(y,z) + c(x,y+z),$$

d.h. zu

$$c(y,z) - c(x+y,z) + c(x, y+z) - c(x,y) = 0.$$

Bis auf die Reihenfolgt der Argumente im dritten Glied rechts ist dies gerade die 2-Kozykel-Bedingung von 3.4.3, d.h. die Bedingung

$$\partial c = 0.$$

Nach Definition von c in 3.4.3 gilt aber c(U,V) = c(V,U), d.h. die Assoziativgesetzt ist tatsächlich äquivalent zu

$$\partial c = 0.$$

Diese Bedingung ist jedoch erfüllt nach Bemerkung 3.4.3 (ii).

2. Schritt. Es gilt das Kommutativgesetz: es gilt

$$(x,x') + (y, y') = (y,y') + (x,x') \text{ für beliebige } x,x', y, y' \in k.$$

Das folgt unmittelbar aus der Definition der Operation, der Kommutativität von k und aus c(T,U) = c(U, T) (vgl. die Definition in 3.4.3).

3. Schritt. Existenz des neutralen Elements: es gilt

$$(0,0) + (y,y') = (y, y') + (0,0) = (y,y') \text{ für beliebiges } (y,y') \in k^2.$$

Dies ergibt sich unmittelbar aus der Definition der Operation und der Tatsache, daß c(0,U) = c(T, 0) = 0

gilt, denn c(T,U) ist ein homogenes Polynom des Grades p in T und U, in welchem T^p und U^p den Koeffizienten 0 besitzen (vgl. die Definition in 3.4.3).

4. Schritt. Existenz des Inversen: es gilt

$$(x, x') + (-x, -x') = 0 \text{ für beliebige } x, x' \in k.$$

Es gilt

$$\begin{aligned}(x,x')+(y,y') = (0,0) &\Leftrightarrow (x+y, x'+y'+c(x,y)) = (0,0) \\ &\Leftrightarrow x+y = 0 \text{ und } x'+y' + c(x,y) = 0 \\ &\Leftrightarrow y = -x \text{ und } y' = -x' - c(x, y) = -x' - c(x,-x) \\ &\Leftrightarrow (y, y') = (-x, -x') \quad (\text{wegen } c(x,-x) = 0)\end{aligned}$$

Die letzte Äquivalenz basiert auf der Tatsache, daß die Charakteristik des Grundkörpers k von 0 verschieden sein soll (und die Defintionvon c(T,U) in 3.4.3).

Bemerkung

Wir haben gezeigt, k^2 ist mit der angegebenen Operation eine abelsche lineare algebraische Gruppe (der Dimension 2). Wir haben noch zu zeigen, daß diese Gruppe nicht isomorp ist zu $\mathbf{G}_a^2$.

5. Schritt. Die lineare algebraische Gruppe $G := k^2$ mit der in Bemerkung (ii) definierten Operation ist nicht isomorph zu $\mathbf{G}_a^2$.

Angenommen, es gibt einen Isomorphismus

$$h: \mathbf{G}_a^2 \longrightarrow G.$$

Seien

$$\pi: G = k^2 \longrightarrow k,\ (x,y) \mapsto x,$$

$$\rho: G = k^2 \longrightarrow k,\ (x,y) \mapsto y,$$

die Projektionen auf die beiden Koordinaten. Es gilt

$$\begin{aligned} h((x,x') + (y,y') &= h(x,x') + h(y,y') \\ &= (\pi h(x,x'),\rho h(x,x')) + (\pi h(y,y'), \rho h(y,y')) \\ &= (\pi h(x,x')+\pi h(y,y'), \rho h(x,x')+\rho h(y,y')+c(\pi h(x,x'), \pi h(y,y')) \end{aligned}$$

also

$$\pi h((x,x') + (y,y')) = \pi h(x,x')+\pi h(y,y') \text{ und}$$

$$\rho h((x,x') + (y,y')) = \rho h(x,x')+\rho h(y,y')+c(\pi h(x,x'), \pi h(y,y')$$

Die ersten Identität bedeutet,

$$\pi\circ h: \mathbf{G}_a^2 \longrightarrow G \xrightarrow{\pi} k \text{ ist eine additive Funktion.}$$

Die zweite Identität schreiben wir in der Gestalt

$$f(p+q) - f(p) - f(q) = c(\pi h(p), \pi h(y)) \text{ für } p,q \in \mathbf{G}_a.$$

Dabei haben wir $f(p) := \rho h(p)$ gesetzt. Es reicht zu zeigen, daß eine solche Gleichung unmöglich bestehen kann. Nach 3.4.6 (iii) reicht es zu zeigen:

1. $g(p, q) := f(p+q) - f(p) - f(q)$ ist ein polynomialer 2-Kozyklus.
2. $\sum_{i=1}^{p-1} g(p, i\bullet p) = 0.$

Zu 1. Es gilt

$$\begin{aligned} (\partial g)(x,y,z) &= g(y,z) - g(x+y, z) + g(x, y+z) - g(x, y) \\ &= f(y+z) - f(y) - f(z) \\ &\quad - f(x+y+z) + f(x+y) + f(z) \\ &\quad +f(x+y+z) - f(x) - f(y+z) \\ &\quad - f(x+y) + f(x) + f(y) \\ &= 0 \end{aligned}$$

Zu 2. Als reguläre Funktion

$$f = \rho\circ h: k^2 = \mathbf{G}_a^2 \xrightarrow{h} G \xrightarrow{\rho} k$$

ist f ein Polynom in zwei Unbestimmten. Weil f ein Gruppen-Homomorphismus ist, gilt

$$f(0,0) = 0,$$

d.h. das Absolutglied des Polynoms f ist Null. Die Identität wird im ersten Schritt des Beweises von 3.4.6 (iii) bewiesen.

QED.

3.4.10 Aufgabe 3

Seien F ein perfekter Teilkörper des Grundkörpers k und G eine zusammenhängende elementar unipotente F-Gruppe, welche F-isomorph ist zu einer abgeschlossenen Untergruppe von $\mathbf{U}_m$. Zeigen Sie, dann ist G über F isomorph zu einer F-Gruppe der Gestalt $\mathbf{G}_a^n$ (Bemerkung: die Triangulierbarkeitsbedingung $G \hookrightarrow \mathbf{U}_m$ kann weggelassen werden, vgl. 14.1.2).

Bemerkkung
Der nachfolgende Beweis kommt ohne die Bedingung aus, daß G zu einer abgeschlossenen Untergruppe von $\mathbf{U}_m$ F-isomorph sein soll.

Beweis. Der Beweis ist im wesentlichen eine Modifikation des Beweises der Implikation (ii) $\Rightarrow$ (iii) von 3.4.7 im Fall, daß die Gruppe zusammenhängend ist.

Nach Voraussetzung ist G eine zusammenhängende elementar unipotente Gruppe. Nach 3.4.7 ist damit

> $\mathcal{A}(G)$ ein endlich erzeugter R(k)-Modul, welcher den Koordinatenring k[G] als k-Algebra erzeugt.

Die k-Algebra k[G] ist endlich erzeugt, sagen wir

$$k[G] = k[f_1,...,f_m]. \tag{1}$$

Weil k[G] von $\mathcal{A}(G)$ erzeugt wird, ist jedes f_i ein Polynom in endlich vielen Elementen aus $\mathcal{A}(G)$. Wir können also annehmen,

$$f_1,...,f_m \in \mathcal{A}(G).$$

Nach Bemerkung 3.3.1 A (iii) ist jedes f_i eine k-Linearkombination von endlich vielen Elementen aus $\mathcal{A}(G)(F)$. Wir können also annehmen

$$f_1,...,f_m \in \mathcal{A}(G)(F).$$

Weil $\mathcal{A}(G)$ endlich erzeugt ist über R(k), ist auch

$$\mathcal{A}(G)(F) \text{ endlich erzeugt über } R(F)$$

(nach Bemerkung 3.3.1 A (iv)). Die Multiplikation der Elemente von $\mathcal{A}(G)(F)$ mit Elementen aus R(F) besteht in der wiederholten Anwendung der folgenden beiden Operationen: man erhebt die Elemente in die p-te Potenz und man multipliziert sie mit Elementen aus F. Als f_i kann man deshalb in (1) ein beliebiges Erzeugendensystem von $\mathcal{A}(G)(F)$ über R(F) verwenden, d.h. (1) gilt für beliebige f_i mit

$$\mathcal{A}(G)(F) = R(F)\bullet f_1+...+R(F)\bullet f_r.$$

Weil G zusammenhängend ist, ist $\mathcal{A}(G)(F)$ als R(F)-Modul torsionsfrei (nach 3.3.6 (i)). Weil F nach Voraussetzung perfekt ist, ist $\mathcal{A}(G)(F)$ als R(F)-Modul sogar frei (nach 3.3.3 (iii)). Wir können also annehmen,

$$f_1,...,f_m \text{ sind algebraisch unabhängig über } k$$

(nach 3.3.6 (ii)). Als Elemente von $\mathcal{A}(G)(F) \subseteq \mathcal{A}(G)$ sind die f_i Homomorhismen

$$f_i: G \longrightarrow \mathbf{G}_a$$

von linearen algebraischen Gruppen. Weil sie den Koordinatenring k[G] erzeugen, ist durch

$$G \longrightarrow k^m,\ x \mapsto \begin{pmatrix} f_1(x) \\ \cdots \\ f_m(x) \end{pmatrix},$$

ein Isomorphismus von affinen algebraischen Varietäten definiert.[42] Weil die f_i additive Funktionen sind, ist es sogar ein Isomorphismus von linearen algebraischen Gruppen

$$G \xrightarrow{\cong} \mathbf{G}_a^m$$

Weil die f_i in $\mathcal{A}(G)(F) \subseteq F[G]$ liegen, ist dieser Isomorphismus über F definiert, d.h. es ist ein F-Isomorphismus.
QED.

3.4.10 Aufgabe 4

Die Charakteristik des Grundkörpers k sei $p > 0$, der Teilkörper $F \subseteq k$ sei nicht perfekt und

$$a \in F - F^p.$$

Zeigen sie,

$$G := \{(x,y) \in \mathbf{G}_a^2 \mid x^p - x = ay^p \}$$

ist eine F-Gruppe, welche isomorph aber nicht F-isomorph ist zu $\mathbf{G}_a$ (Hinweis: verwenden Sie Aufgabe 5 von 2.1.5).
Beweis. 1. Schritt. G ist isomorph zu $\mathbf{G}_a$ über k.
Die Funktion

$$f(x,y) = x^p - x - ay^p$$

auf $\mathbf{G}_a^2 = k^2$ additiv (als Linearkompination von Potenzen der Gestalt x^{p^i} und y^{p^j}) und G ist nach Definition gerade der Kern des Homomorphismus

$$f: \mathbf{G}_a^2 \longrightarrow \mathbf{G}_a$$

von linearen algebraischen Gruppen. Zum Beweis der Behauptung reicht es zu zeigen,

$$f(x,y) = x^p - x - ay^p \text{ ist ein irreduzibles Polynom von } k[x,y], \qquad (1)$$

Denn dann ist

$$k[G] = k[x,y]/(f(x,y)),$$

G ist irreduzibel und

$$\dim G = \text{tr. deg}_k\, k[G] = 1.$$

Als zusammenhängende algebraische Gruppe der Dimension 1 ist

$$G \cong \mathbf{G}_a \text{ oder } G \cong \mathbf{G}_m$$

(nach 3.4.9). Wegen $G \subseteq \mathbf{G}_a^2$ besteht G ausschließlich aus unipotenten Elementen. Es kommt also nur der Fall

$$G \cong \mathbf{G}_a$$

in Frage. Beweisen wir also (1). Dazu betrachten wir f also Polynom in y mit Koeffizienten aus k[x]. Nach dem Kriterium von Eisenstein (van der Waerden [1], Kapitel 5, §31) reicht es zu zeigen,

$$x^p - x \text{ hat keine mehrfachen Nullstellen in k.}$$

Wegen $x^p - x = x\bullet(x^{p-1}-1)$ und weil die Nullstellen von $x^{p-1}-1$ ungleich 0 sind, reicht es zu zeigen,

---

[42] Zunächst ist dies nur ein Isomorphismus der algebraischen Varietät G mit einer abgeschlossenen Teilmenge von k^m (vgl. Bemerkung 1.3.1 (iii)). Weil die f_i algebraisch unabhängig sind, ist das Ideal dieser abgeschlossenen Teilvarietät das Nullideal, d.h. die Teilvarietät ist der ganze k^n.

x^{p-1}-1 hat keine mehrfachen Nullstellen in k.
Das ist aber tatsächlich der Fall, denn die Ableitung des Polynoms,

$$(p-1)\cdot x^{p-2} = -x^{p-2},$$

ist in jeder Nullstelle von x^{p-1}-1 von 0 verschieden. Man beachte k ist ein Körper der Charakteristik $p > 0$.

2. Schritt. G ist eine F-Gruppe mit der F-Struktur $F[G] = F[x,y]/(ay^p - (x^p-x))$.
Wir betrachten die F-Algebra-Homomorphismen

$$\Delta\colon F[x,y] \longrightarrow F[x,y,x',y'],\ f(x,y) \mapsto f(x+x',y+y'),$$

$$\iota\colon F[x,y] \longrightarrow F[x,y],\ f(x,y) \mapsto f(-x,-y),$$

$$\varepsilon\colon F[x,y] \longrightarrow F,\ f(x,y) \mapsto f(0,0),$$

welche der Funktor $k\otimes_F$ in die Komultiplikation, den Antipoden bzw. die Auswertung im netralen Element von G_a^2 überführt. Deshalb sind die Diagramme von 2.1.2 A mit

$$A := F[x,y]$$

kommutativ für diese Abbildungen kommutativ.
Diese Abbildungen induzieren F-Algebra-Homomorphismen

$$\overline{\Delta} : \Delta\colon F[G] \longrightarrow F[G]\otimes F[G]$$

$$\overline{\iota}\colon F[G] \longrightarrow F[G]$$

$$\overline{\varepsilon}\colon F[G] \longrightarrow F$$

für welche die Diagramme von 2.1.2 A kommutativ mit

$$A := F[G]$$

sind. Durch Anwenden des Funktors $k\otimes_F$ erhalten wir kommuttive Diagramme, welche die Gruppen-Struktur der algebraischen Gruppe G definieren.. Die untensorierten Abbildung definieren zusammen mit A = F[G] also gerade die F-Struktur der algebraischen Gruppe G.

Bemerkungen

1. Wir haben noch zu zeigen, daß G nicht F-isomorph zu G_a ist. Dazu reicht es zu zeigen, die R(F)-Moduln $\mathcal{A}(G)(F)$ und $\mathcal{A}(\mathbf{G}_a)(F)$ sind nicht isomorph.
2. Nach 3.3.5 ist

   $$\mathcal{A}(\mathbf{G}_a)(F) \text{ frei vom Rang 1 über } R(F).$$

   und im ersten Schritt des Beweises von 3.3.5 wird $\mathcal{A}(\mathbf{G}_a)(F)$ explizit als Teilmenge von F[T] beschrieben,

   $$\mathcal{A}(\mathbf{G}_a)(F) = \{ \sum_{i\geq 1} c_i \cdot T^{p^i} \mid c_i \in F,\ c_i = 0 \text{ für fast alle } i \} = R(F)\cdot T, \qquad (1)$$

   d.h. $\mathcal{A}(\mathbf{G}_a)(F)$ ist frei vom Rang 1 mit der einelementigen Basis {T}.
3. Weil $\mathcal{A}(\mathbf{G}_a)(F)$ frei vom Rang 1 über R(F) ist, besteht ein Isomorphismus von linken R(F)-Moduln

   $$R(F) \xrightarrow{\cong} \mathcal{A}(\mathbf{G}_a)(F).$$

   Durch Anwenden des Funktors $R(F)/R(F)\cdot T\otimes_{R(F)}$ erhalten wir einen Isomorphismus von F-Vektorräumen

   $$F \xrightarrow{\cong} R(F)/R(F)\cdot T \xrightarrow{\cong} \mathcal{A}(\mathbf{G}_a)(F)/R(F)\cdot T\cdot\mathcal{A}(\mathbf{G}_a)(F).$$

   Insbesondere ist

$$\dim_F \mathcal{A}(\mathbf{G}_a)(F)/R(F)\bullet T\bullet\mathcal{A}(\mathbf{G}_a)(F) = 1.$$

Zum Beweis der Behauptung reicht es zu zeigen,

$$\dim_F \mathcal{A}(G)(F)/R(F)\bullet T\bullet\mathcal{A}(G)(F) \neq 1. \qquad (2)$$

4. Zum Beweis von (2) brauchen wir eine hinreichend genaue Beschreibung von $\mathcal{A}(G)(F)$. Der einfachste Weg zu einer solchen Beschreibung scheint darin zu bestehen, die Beschreibung (1) von $\mathcal{A}(\mathbf{G}_a)(F)$ und einen explizit gegebenen Isomorphismus

$$G_a \xrightarrow{\cong} G$$

(über k), wie er auf Grund des ersten Schritts existiert, zu verwenden.

3. Schritt. Konstruktion von zueinander inversen Isomorphismen

$$\varphi: \mathbf{G}_a \longrightarrow G \text{ und } \psi: G \longrightarrow \mathbf{G}_a.$$

Wir betrachten die Abbildung

$$\varphi: \mathbf{G}_a \longrightarrow k^2, t \mapsto (t^p , a^{-1/p}\bullet(t^p - t)),$$

Die Abbildung ist regulär und über k definiert (nicht jedoch über F, weil $a^{-1/p}$ nicht in F liegt). Das Bild von φ liegt in

$$V(ay^p - x^p+x) = G,$$

denn es ist

$$a\bullet(a^{-1/p}\bullet(t^p - t))^p - (t^p)^p + t^p = (t^p)^p - t^p - (t^p)^p + t^p = 0.$$

Wir können damit φ als reguläre Abbildung

$$\varphi: \mathbf{G}_a \longrightarrow G, t \mapsto (t^p , a^{-1/p}\bullet(t^p - t)),$$

betrachten. Da die Koordinatenfunktionen von φ additive Polynome sind, ist φ ein (über k definierter) Homomorphismus von linearen algebraischen Gruppen.

Als nächstes betrachten wir die Abbildung

$$\psi: G \subseteq \mathbf{G}_a^2 \longrightarrow k = \mathbf{G}_a, (x,y) \mapsto x - a^{1/p}\bullet y$$

Die Projektionen $\mathbf{G}_a^2 \longrightarrow k, (x,y) \mapsto x$, und $\mathbf{G}_a^2 \longrightarrow k, (x,y) \mapsto y$, sind additive Funktionen auf $\mathbf{G}_a^2$. Also sind deren Einschränkungen auf die abgeschlossene Untergruppe G ebenfalls additiv. Damit ist aber auch ψ eine additive Funktion, d.h. ein Homomorphismus von lineare algebraischen Gruppen.

Wir haben noch zu zeigen, daß φ und ψ zueinander invers sind. Für $t \in \mathbf{G}_a$ gilt

$$\begin{aligned}
\psi(\varphi(t)) &= \psi(t^p , a^{-1/p}\bullet(t^p - t)) && \text{(nach Definition von } \varphi) \\
&= t^p - a^{1/p}\bullet(a^{-1/p}\bullet(t^p - t)) && \text{(nach Definition von } \psi) \\
&= t^p - (t^p - t) \\
&= 0
\end{aligned}$$

Weiter gilt für $(x,y) \in G$:

$$\begin{aligned}
\varphi(\psi(x,y)) &= \varphi(x - a^{1/p}\bullet y) && \text{(nach Definition von } \psi) \\
&= ((x - a^{1/p}\bullet y)^p, a^{-1/p}\bullet((x - a^{1/p}\bullet y)^p - (x - a^{1/p}\bullet y))) && \text{(Definiton von } \varphi) \\
&= (x^p - a\bullet y^p, a^{-1/p}\bullet(x^p - a\bullet y^p - x + a^{1/p}\bullet y))
\end{aligned}$$

$$= (x^p - a\bullet y^p,\ a^{-1/p}\bullet(x^p - a\bullet y^p - x + a^{1/p}\bullet y))$$

Wegen $(x,y) \in G$, d.h. $ay^p - x^p + x = 0$ folgt

$$\varphi(\psi(x,y)) = (x,\ a^{-1/p}\bullet(x - x + a^{1/p}\bullet y))$$
$$= (x,\ y).$$

Die Abbildungen φ und ψ sind also tatsächlich Isomorphismen von linearen algebraische Gruppen (über). Diese Tatsachte gestattet es uns den R(k)-Modul $\mathcal{A}(G)$ als Teilmenge von k[G] zu bestimmen.

4. Schritt. Abschluß des Beweises.

Wir bezeichnen die Restklassen von x und y in $k[G] = k[x, y]/(x^p - x - ay^p)$ mit

$$\overline{x} := x \bmod (x^p - x - ay^p) \text{ und } \overline{y} := y \bmod (x^p - x - ay^p)$$

und die einzige Koordinaten-Funktion auf $\mathbf{G}_a$ mit T, sodaß gilt

$$k[\mathbf{G}_a] = k[T]$$
$$k[G] = k[\overline{x},\overline{y}] \qquad (3)$$
$$0 = \overline{x}^p - \overline{x} - a\overline{y}^p$$

Die Teilmenge $\mathcal{A}(G) \subseteq k[G]$ der additiven Funktionen auf G ist gerade das Bild der Teilmenge $\mathcal{A}(\mathbf{G}_a) \subseteq k[\mathbf{G}_a]$ beim k-Algebra-Isomorphismus $\psi^*: k[\mathbf{G}_a] \longrightarrow k[G]$, d.h. es ist

$$\mathcal{A}(G) = \psi^*(\mathcal{A}(\mathbf{G}_a))$$

$$= \psi^*(\{ \sum_{i\geq 0} c_i \bullet T^{p^i} \mid c_i \in k \}) \qquad \text{(nach dem 1.Schritt von 3.3.5 mit n = 1)}$$

$$= \{ \sum_{i\geq 0} c_i \bullet \psi^*(T)^{p^i} \mid c_i \in k \} \qquad (\psi^* \text{ ist k-Algebra-Homomorphismus})$$

$$= \{ \sum_{i\geq 0} c_i \bullet (\overline{x} - a^{1/p}\bullet\overline{y})^{p^i} \mid c_i \in k \} \qquad \text{(nach Definition von } \psi \text{ im 3. Schritt)}$$

$$= \{c_0\bullet(\overline{x} - a^{1/p}\bullet\overline{y}) + \sum_{i\geq 1} c_i \bullet ((\overline{x} - a^{1/p}\bullet\overline{y})^p)^{p^{i-1}} \mid c_i \in k, \}$$

$$= \{c_0\bullet(\overline{x} - a^{1/p}\bullet\overline{y}) + \sum_{i\geq 1} c_i \bullet \overline{x}^{p^{i-1}} \mid c_i \in k, \}.$$

Das letzte Gleichheitszeichen gilt, wegen $\overline{x}^p - a\overline{y}^p = \overline{x}$ (nach (3)) also $(\overline{x} - a^{1/p}\bullet\overline{y})^p = \overline{x}$. Damit ist $\mathcal{A}(G)$ der k-lineare Unterraum von k[G] mit der Basis

$$\overline{x} - a^{1/p}\bullet\overline{y},\ \overline{x},\ \overline{x}^p,\ \overline{x}^{p^2},\ \overline{x}^{p^3},\ \ldots \in k[G]$$

Damit ist aber auch

$$\overline{y},\ \overline{x},\ \overline{x}^p,\ \overline{x}^{p^2},\ \overline{x}^{p^3},\ \ldots$$

eine Basis von $\mathcal{A}(G)$ über k. Die Elemente letzterer liegen aber sogar in der F-Struktur

$$F[G] = F[x,y]/(ay^p - (x^p - x)) \ (\subseteq k[G] = k[x,y]/(ay^p - (x^p - x)) = k[\overline{x},\overline{y}])$$

von k[G], d.h. es ist

$$\overline{y},\ \overline{x},\ \overline{x}^p,\ \overline{x}^{p^2},\ \overline{x}^{p^3},\ \ldots \in \mathcal{A}(G) \bigcap F(G) = \mathcal{A}(G)(F)$$

(nach Definition von $\mathcal{A}(G)(F)$ in Bemerkung 3.3.1 A (ii)). Es folgt

$$\mathcal{A}(G)(F) = F\bullet\overline{y} + F\bullet\overline{x} + F\bullet\overline{x}^p + F\bullet\overline{x}^{p^2} + F\bullet\overline{x}^{p^3} + \ldots$$

(nach Bemerkung 1.3.7 B (iv)).
Für $i \geq 1$ erhalten wir

$$T^i \bullet \mathcal{A}(G)(F) = F^{p^i} \bullet \overline{y}^{p^i} + F^{p^i} \bullet \overline{x}\, p^i + F^{p^i} \bullet \overline{x}^{p^{i+1}} + F^{p^i} \bullet \overline{x}\, p^{i+2} + \ldots$$

Für den von dieser Menge erzeugten F-Vektorraum gilt

$$F \bullet T^i \bullet \mathcal{A}(G)(F) = F \bullet \overline{y}^{p^i} + F \bullet \overline{x}\, p^i + F \bullet \overline{x}^{p^{i+1}} + F \bullet \overline{x}\, p^{i+2} + \ldots$$

Nach (3) ist $\overline{y}^p = (\overline{x}^p - \overline{x})/a$, also $\overline{y}^{p^i} = (\overline{x}^p - \overline{x})^{p^i}/a^{p^i} = (\overline{x}\, p^{i+1} - \overline{x}^{p^i})/a^{p^i}$. Es folgt

$$F \bullet T^i \bullet \mathcal{A}(G)(F) = F \bullet \overline{x}\, p^i + F \bullet \overline{x}^{p^{i+1}} + F \bullet \overline{x}\, p^{i+2} + \ldots$$

also

$$R(F) \bullet T \bullet \mathcal{A}(G)(F) = \sum_{i \geq 1} F \bullet T^i \bullet \mathcal{A}(G)(F) = F \bullet \overline{x}\, p + F \bullet \overline{x}\, p^2 + F \bullet \overline{x}\, p^3 + \ldots$$

also

$$\mathcal{A}(G)(F) \,/\, R(F) \bullet T \bullet \mathcal{A}(G)(F) = F \bullet \overline{y} + F \bullet \overline{x}$$

also

$$\dim_F \mathcal{A}(G)(F) \,/\, R(F) \bullet T \bullet A(G)(F) = 2.$$

Damit ist (2) bewiesen, und damit die Behauptung.
QED.

3.5 Anmerkungen

(i) Die Aussagen von 3.1.1 gehen auf Kolchin [2, §3] zurück. Die Bezeichnung "Torus" für eine zusammenhängende diagonlisierbare Gruppe wurde von Borel [1] geprägt. Er hat die bedeutende Rolle erkannt, die diese Gruppen spielen, die vergleichbar ist mit der Rolle der kompakten Tori in der Theorie der kompaktten Lie-Gruppen.

(ii) Abschnitt 3.2 enthält Standard-Ergebnisse zu den Tori. Der Beweis des Starrheitssatzes 3.2.8 liefert eine stärkere Aussage: die affine Varietät V des Satzes kann durch ein beliebiges zusammmenhängendes Schema über k ersetzt werden. Als Konsequenz haben diagolisierbare Gruppen keine "infinitesimalen Automorphismen".

(iii) Die Theorie der elementaren unipotenten Gruppen weist eine gewissen Analogie zur Theorie der Tori auf, bei der die Charakttergruppe durch den R(k)-Modul $\mathcal{A}$ von 3.3.1 ersetzt wird. Die Verwendung des Rings R(k) scheint auf Demazure & Gabriel [1, Kapitel IV, 3.6] zurückzugehen. In Demazure & Gabriel [1, Kapitel V, 3.4] findet man allgemeinere Ergebnisse für beliebige kommutative unipotente Gruppen. Diese werden als "Dieudonné-Moduln" beschrieben.

(iv) Eins der Hauptergebnisse dieses Kapitels ist der Klassifikationssatz 3.4.9. Der erste publizierte Beweis scheint der von Grothendieck zu sein (Demazur&Grothendieck [1, Kapitel 4, Expose 7]). In Borel [3, Kapitel III, §10] wird ein Beweis angegeben, der die Tatsache verwendet, daß eine irreduzible glatte projektive Kurve mit unendlicher Automorphismengruppe, die einen Punkt fest läßt, isomorph ist zum $\mathbb{P}^1$. Der hier angegebene Beweis ist elementarer. Wir nutzen die Klassifikation der elementar unipotenten Gruppen. Wir brauchen auch das Ergebnis zu den polynomialen Kozyklen von 3.4.4, welche auf Lazard [1, Lemma 3] zurückgeht. Einen anderen Beweis des Klassifikationssatzes, der ebenfalls additive Polynome verwendet, kann man in Humphreys [1, Abschnitt 20] finden.

Index

Inhalt