Lineare algebraische Gruppen

Vorlesung 13 im Sommersemester 2021 (am 9.07.21):
Elementare unipotente Gruppen II
Charakterisierung der elementaren unipotenten Gruppen.

Hinweis zu den im Text verwendeten Referenzen

Referenz	Bedeutung
x.y.z	verweist auf den Abschnitt x.y.z im PDF-File zu Kapitel x, z.B verweist 3.2.1 auf Abschnitt 3.2.1 im PDF-File zu Kapitel 3.
WS 20.x, y.z	verweist auf den Abschnitt y.z im Text zur Vorlesung x im Wintersemester 2020.
SS 21.x, y.z	verweist auf den Abschnitt y.z im Text zur Vorlesung x im Sommersemester 2021.
y.z	verweist auf Aussage y.z des aktuellen Abschnitts der aktuellen Vorlesung

Wir werden die Zitate des ersten Typs bevorzugt verwenden und die Verweise der anderen Type nur für erst vor kurzem oder häufig verwendete Ergebnisse oder Definition zusätzlich angeben.

14 Kommutative lineare algebraische Gruppen

Elementare unipotente Gruppen *V*

14.4 Elementare unipotente Gruppen

14.4.7 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) $\Rightarrow$ (i). Wir erinnern zunächst an zwei früher bewiesene Aussagen. Es bestehten die folgenden Implikationen.

Aussage 1. G ist unipotent $\Leftrightarrow$ G ist isomorph zu einer abgeschlossenen Untergruppe einer $\mathbf{U}_n$

Die Implikation '$\Leftarrow$' 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

$$G \cong \mathbf{G}_a^n = \mathbf{G}_a \times \ldots \times \mathbf{G}_a$$

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.

$$G \cong \mathbf{G}_a^n \times (\mathbb{Z}/p\mathbb{Z})^r = (\mathbb{Z}/p\mathbb{Z}) \times \ldots \times (\mathbb{Z}/p\mathbb{Z})$$

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

$$\mathcal{A}(G) = R(k)\bullet f_1+...+R(k)\bullet f_m \text{ mit } f_1,...,f_m \text{ linear unabhängig über } R(k).$$

Nach 3.3.6 (ii) sind

$$f_1,...,f_m \text{ algebraisch unabhängig über k.}$$

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

$$T^j\bullet f_i = f_i^{p^j},\ i=1,...,m,\ j = 0,1,2,...$$

(vgl. 3.3.4 A) und im Fall p = 0 von den $f_1,...,f_m$. Damit hat der Koordinatenring von G die Gestalt

$$k[G] = k[f_1,...,f_m]$$

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

$$f:G \xrightarrow{\cong} X \subseteq k^m,\ x \mapsto \begin{pmatrix} f_1(x) \\ \cdots \\ f_m(x) \end{pmatrix},$$

ein Isomorphismus von affinen algebraischen Varietäten definiert (vgl. Bemerkung 1.3.1 (iii)) mit sagen wir

$$X = V(g_1,...,g_s),\ g_i \in k[T_1,...,T_m].$$

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).

<u>(i) $\Rightarrow$ (ii) im Fall, daß G zusammenhängend ist</u>.

Nach Aussage 1 können wir annehmen G ist eine abgeschlossene Untergruppe einer der Gruppen $\mathbf{U}_m$,

$$G \subseteq \mathbf{U}_m = \left\{ \begin{pmatrix} 1 & x_{12} & x_{13} & \cdots & x_{1,m-1} & x_{1m} \\ 0 & 1 & x_{23} & \cdots & x_{2,m-1} & x_{2m} \\ \cdots & \cdots & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & 0 & \cdots & 1 & x_{m-1,m} \\ 0 & 0 & 0 & \cdots & 0 & 1 \end{pmatrix} \middle|\ x_{ij} \in k \right\}$$

Wir führen den Beweis durch Induktion nach m.

<u>Induktionsanfang</u>: m = 1.

Es gilt dann $G = \mathbf{U}_1 = \{e\}$, $k[G] = k$, also $\mathcal{A}(G) =^{1} 0$. 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.

$$\varphi: \mathbf{U}_m \longrightarrow\!\!\!\!\rightarrow \mathbf{U}_{m-1},\ A \mapsto A',$$

wobei A' aus A entstehe durch Streichen der ersten Zeile und ersten Spalte, und

$$\psi: \mathbf{U}_m \longrightarrow\!\!\!\!\rightarrow \mathbf{U}_{m-1},\ A \mapsto A'',$$

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[2] und im Fall $j < m$ nicht von den letzten Koordinaten der Faktoren[3]. 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,

$$\varphi(G) \text{ und } \psi(G) \text{ sind sind elementar unipotent,}$$

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:

$$\begin{aligned} &\mathcal{A}(\varphi(G)) \text{ und } \mathcal{A}(\psi(G)) \text{ endlich erzeugte R(k)-Moduln,} \\ &\text{die } k[\varphi(G)] \text{ bzw. } k[\psi(G)] \text{ als k-Algebren erzeugen.} \end{aligned} \qquad (1)$$

---

[1] 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

[2] denn die erste Koordinate des ersten Faktors ist im Fall $1 < i$ gleich 0.

[3] denn die letzte Koordinate des zweiten Faktors ist mit Fall $j < m$ gleich 0.

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 ∈ 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

$$x_{1m}(uv) = 1\bullet x_{1m}(v) + x_{12}(u)\bullet x_{2m}(v) + ... + x_{1,m-1}(u)\bullet x_{m-1,m}(v) + x_{im}(u)\bullet 1,$$

also

$$x(uv) - x(v) - x(u) = x_{12}(u)\bullet x_{2m}(v) + ... + x_{1,m-1}(u)\bullet x_{m-1,m}(v)$$

Unter den auf der rechten Seite auftretenden Funktionen x_{ij} kommt x_{1m} nicht vor, d.h. diese x_{ij} liegen in $k[a_1,...,a_n]$. Es gibt also ein Polynom $f(\mathbf{T},\mathbf{U}) \in k[\mathbf{T},\mathbf{U}]$ mit

$$x(uv) - x(u) - x(v) = f(a_1(u),...,a_n(u), a_1(v),...,a_n(v))$$

für beliebige $u, v \in G$. Im folgenden werden wir abkürzend

$$a(u) \text{ für } (a_1(u),...,a_n(u)$$

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)

$$\begin{aligned}(\partial f)(a(u), a(v), a(w)) &= f(a(v),a(w)) - f(a(u)+a(v),a(w))+f(a(u), a(v)+a(w))-f(a(u),a(v)) \\ &=^4 f(a(v),a(w)) - f(a(uv),a(w))+f(a(u),a(vw))-f(a(u),a(v)) \\ &= \quad x(vw)-x(v)-x(w) \\ &\quad -x(uvw)+x(uv)+x(w) \\ &\quad +x(uvw)-x(u)-x(vw) \\ &\quad -x(uv)+x(u)+x(v) \\ &= 0\end{aligned}$$

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[5]

$$\begin{aligned}&(\partial f)(p_1^*(a), p_2^*(a), p_3^*(a))\ (u,v,w) \\ &\quad =^6 (\partial f)(p_1^*(a)(u,v,w), p_2^*(a)\ (u,v,w), p_3^*(a)(u,v,w)) \\ &\quad = (\partial f)((a\circ p_1)(u,v,w), (a\circ p_2)(u,v,w),(a\circ p_3)(u,v,w)) \\ &\quad = (\partial f)(a(u), a(v), a(w)) \\ &\quad = 0.\end{aligned}$$

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

$$\begin{aligned}p_1^*(a_j) &= a_j\otimes 1\otimes 1 \\ p_2^*(a_j) &= 1\otimes a_j\otimes 1 \\ p_3^*(a_j) &= 1\otimes 1\otimes a_j.\end{aligned}$$

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

---

[4] die a_ν sind additive Funktionen auf G.

[5] $p_i^*(a)$ steht hier abkürzend für $p_1^*(a_1),..., p_1^*(a_n)$

[6] Die Auswertung an der Stelle (u,v,w) ist ein k-Algebra-Homomorphismus.

$$k[a_1,...,a_n] \longrightarrow k[U_1,...,U_n],\ a_i \mapsto U_i,$$

mit Unbestimmten U_i, also ein k-Algebra-Isomorphismus

$$k[a_1,...,a_n]\otimes_k k[a_1,...,a_n]\otimes_k k[a_1,...,a_n]$$

$$\longrightarrow k[U_1,...,U_n]\otimes_k k[V_1,...,V_n]\otimes_k k[W_1,...,W_n] = k[U,V,W]$$

$$a_j\otimes 1\otimes 1 \mapsto U_j,\ \ 1\otimes a_j\otimes 1 \mapsto V_j,\ 1\otimes 1\otimes a_j \mapsto W_j.$$

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

$$\left(\sum_{i=1}^{p-1} f(a,\ i\bullet a)\right)(u) \ = \ \sum_{i=1}^{p-1} f(a(u),\ i\bullet a(u))$$

$$= \sum_{i=1}^{p-1} f(a(u),\ a(u^i)) \qquad \text{(die } a_j \text{ sind additive Funktionen)}$$

$$= \sum_{i=1}^{p-1} (x(u \bullet u^i) - x(u) - x(u^i)) \qquad \text{(nach Definition von f)}$$

$$= \sum_{i=1}^{p-1} x(u^{i+1}) - (p-1) \bullet x(u) - \sum_{i=1}^{p-1} x(u^i)$$

$$= x(u^p) - (p-1) \bullet x(u) - x(u)$$

$$= x(u^p) - p \bullet x(u)$$

$$= x(u^p) \qquad \text{(p ist die Charakteristik von k)}$$

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,

$$f:G \xrightarrow{\cong} X = V(g_1,...g_s) \subseteq k^\ell,\ x \mapsto \begin{pmatrix} f_1(x) \\ \dots \\ f_r(x) \end{pmatrix}.$$

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 $<z_i>$ von G hat die Ordnung p,

$$\# <z_i> = p.$$

Die Einschränkung von α auf $<z_i>$ ist surjektiv, also ein Isomorphismus

$$\alpha|_{<z_i>} : <z_i> \xrightarrow{\cong} Z_i \ (\hookrightarrow Z_1 \times ... \times Z_r)$$

(weil Definitionsbereich und Bild dieselbe Ordnung haben). Deshalb ist

$$\beta: Z_1 \times ... \times Z_r \longrightarrow G, (x_1,...,x_r) \mapsto \alpha|^{-1}_{<z_1>}(x_1) \bullet ... \bullet \alpha|^{-1}_{<z_r>}(x_r)),$$

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

$x = Id + n$, mit $n \in \sum_{\ell(E_{ij})=1} k \bullet E_{ij} \subseteq N_n^1$, wegen $x \neq e$ gilt $n \neq 0$.

(Bezeichnungen wir in 2.1.5 Aufgabe 4, dritter Schritt).
Für die i-te Potenz von x erhalten wir

$$x^i = \sum_{\alpha=0}^{i} \binom{i}{\alpha} \bullet n^\alpha = Id + i \bullet n + y(i) \text{ mit } y(i) \in N_n^1 \bullet N_n^1 \subseteq N_n^2$$

Weil die Charakteristik von k gleich 0 ist, gilt $i \bullet n \neq 0$, 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

$$i^*: k[T] = k[\mathbf{G}_a] \twoheadrightarrow k[G] \qquad (9)$$

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.

Index

Inhalt