Lineare algebraische Gruppen

Vorlesung 14 im Sommersemester 2021 (am 16.07.21)
Elementare unipotente Gruppen III
Struktursatz für elementar unipotente Gruppen, Abschluß des Beweises.

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 III
Struktursatz für elementar unipotente Gruppen, Abschluß des Beweises.

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 <u>elementaren abelschen p-Gruppe</u> verstehen wir ein Produkt von zyklischen Gruppen der Ordnung p.

Beweis. **<u>Bemerkung</u>**.
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.

<u>(i) ⇒ (iii)</u>. 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. <u>Schritt</u>. Der Fall positiver Charakterisk p des Grundkörpers k.
Wir betrachten die exakte Sequenz

$$0 \longrightarrow G^0 \longrightarrow G \xrightarrow{\alpha} Z_1\times\ldots\times Z_r \longrightarrow 0.$$

Sei $z_i \in G$ ein Element dessen Bild in $Z_1\times\ldots\times Z_r$ ein Erzeuger von

$$Z_i = \{1\}\times\ldots\times\{1\}\times Z_i\times\{1\}\times\ldots\times\{1\} \hookrightarrow Z_1\times\ldots\times Z_r$$

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

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

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

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

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 $Z_1\times\ldots\times Z_r$ elementweise in sich ab, d.h. es gilt $\alpha\circ\beta = \mathrm{Id}$, d.h. β ist ein Schnitt von α. Die exakte Sequenz zerfällt und es gilt

$$G = G^0\times\beta(Z_1\times\ldots\times Z_r) = G^0\times Z_1\times\ldots\times Z_r.$$

Man beachte, weil $Z_1\times\ldots\times Z_r$ endlich ist, ist β eine reguläre Abbildung, also ein Homomorphismus von linearen algebraischen Gruppen. Insbesondere gilt (iii).

2. <u>Schritt</u>. 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

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

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

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

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

$$x^\ell \in G^0 \cong \mathbf{G}_a^n = k^n$$

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
$$x \in G^0 \bullet y \subseteq G^0 \bullet G^0 = G^0,$$
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.

<u>(ii) $\Rightarrow$ (i)</u>. Nach Voraussetzung wird k[G] von additiven Funktionen erzeugt, sagen wir
$$k[G] = k[f_1,\ldots,f_n],$$
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
$$\varphi: G \longrightarrow k^m,\ x \mapsto \begin{pmatrix} f_1(x) \\ \ldots \\ f_m(x) \end{pmatrix},$$
ein Isomorphismus mit einer abgeschlossnen Teilvarietät $V \subseteq k^m$ definiert (vgl. Bemerkung 1.3.1 (iii)). Weil die f_i additiv sind, ist
$$\varphi\colon G \longrightarrow k^m = \mathbf{G}_a^m$$
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).

<u>Zusammenfassung</u>.
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
$$\text{(iii)} \Rightarrow \text{(ii)}$$
zu beweisen.

<u>(iii) ⇒ (ii)</u>. 1. <u>Schritt</u>. 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) (siehe die Ergänzung unten) 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 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. <u>Schritt</u>. Mit (iii) gilt auch (ii).
Nach Voraussetzung gilt

$$G \cong \mathbf{G}_a\times...\times\mathbf{G}_a \text{ im Fall } p = 0$$

und

$$G \cong \mathbf{G}_a\times...\times\mathbf{G}_a\times\mathbb{Z}/p\mathbb{Z}\times...\times\mathbb{Z}/p\mathbb{Z} \text{ im Fall } p > 0.$$

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,

$$f(n \bmod p\mathbb{Z}) = n\cdot f(1 \bmod p\mathbb{Z}).$$

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.

Ergänzung zu Lemma 3.3.1A

(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

$$\psi: \mathcal{A}(G_1) \oplus \mathcal{A}(G_2) \longrightarrow \mathcal{A}(G_1 \times G_2),\ (f, g) \mapsto ((x,y) \mapsto f(x) + g(y)).$$

Beweis.

Zu (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

$$\begin{aligned} \varphi(c \cdot f + d \cdot g) &= ((c \cdot f + d \cdot g) \circ q_1, (c \cdot f + d \cdot g) \circ q_2) \\ &= (c \cdot f \circ q_1 + d \cdot g \circ q_1, c \cdot f \circ q_2 + d \cdot g \circ q_2) \\ &= c \cdot (f \circ q_1, f \circ q_2) + d \cdot (g \circ q_1, g \circ q_2) \\ &= c \cdot \varphi(f) + d \cdot \varphi(g). \end{aligned}$$

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

$$\begin{aligned} \psi(f,g)(x,y) &= f(x) + g(y) \\ &= f(p_1(x,y)) + g(p_2(x,y)) \\ &= (p_1^*(f) + p_1^*(g))(x,y), \end{aligned}$$

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 $y,y' \in G_2$:

$$\begin{aligned}
\psi(f,g)((x,y)\bullet(x',y')) &= \psi(f,g)((xx', yy')) \\
&= f(xx') + g(yy') && \text{(nach Definition von } \psi) \\
&= f(x) + f(x') + g(y) + g(y') && \text{(f und g sind additive Funktionen).} \\
&= (f(x) + g(y)) + (f(x')+g(y')) && (\mathbf{G}_a \text{ ist eine abelsche Gruppe}) \\
&= \psi(f,g)(x,y) + \psi(f,g)(x', y') && \text{(nach Definition von } \psi)
\end{aligned}$$

Wir haben gezeigt, $\psi(f,g)$ ist eine additive Funktion auf $G_1 \times G_2$, d.h. ψ ist korrekt definiert.

3. <u>Schritt</u>. 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

$$\begin{aligned}
\psi(\varphi(f))(x,y) &= \psi(f\circ q_1, f\circ q_2)(x,y) && \text{(nach Definition von } \varphi \\
&= f\circ q_1(x) + f\circ q_2(y) && \text{(nach Definition von } \psi) \\
&= f(x,e_2) + f(e_1,y) \\
&= f(x,e_2)\bullet(e_1,y)) && \text{(f ist additv)} \\
&= f(x,y),
\end{aligned}$$

also $\psi(\varphi(f)) = f$ für jedes f also

$$\psi\circ\varphi = \text{id}.$$

Weiter gilt für $f \in \mathcal{A}(G_1)$, $g \in \mathcal{A}(G_2)$, $x \in G_1$ und $y \in G_2$:

$$\varphi(\psi(f,g)) = (\psi(f,g)\circ q_1, \psi(f,g)\circ q_2) \quad \text{(nach Definition von } \varphi).$$

Dabei ist

$$\begin{aligned}
\psi(f,g)\circ q_1(x) &= \psi(f,g)(x,e_2) && \text{(nach Definition von } q_1) \\
&= f(x) + g(e_2) && \text{(nach Definition von } \psi) \\
&= f(x) + 0 && \text{(g ist additiv)} \\
&= f(x).
\end{aligned}$$

Da dies für jedes $x \in G_1$ gilt, folgt

$$\psi(f,g)\circ q_1 = f.$$

Analog ist

$$\begin{aligned}
\psi(f,g)\circ q_2(y) &= \psi(f,g)(e_1,y) && \text{(nach Definition von } q_2) \\
&= f(e_1) + g(y) && \text{(nach Definition von } \psi) \\
&= 0 + g(y) && \text{(f ist additiv)} \\
&= g(x).
\end{aligned}$$

für jedes $y \in G_2$, also

$$\psi(f,g)\circ q_1 = g.$$

Zusammen erhalten wir

$$\begin{aligned}
\varphi(\psi(f,g)) &= (\psi(f,g)\circ q_1, \psi(f,g)\circ q_2) \\
&= (f,g)
\end{aligned}$$

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.

Index

Inhalt