Lineare algebraische Gruppen

Vorlesung 10 im Sommersemester 2021 (am 18.06.21)

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

Additive Funktionen II

14.3 Additive Funktionen

14.3.1 Defintionen, Bezeichnungen und Konstruktionen

3.3.1 A 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.

------> an dieser Stelle fortsetzen:

(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 additiven 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.

Beweis. Zu (i). Jede additive Fumkton $f: G \longrightarrow \mathbf{G}_a$ induziert als reguläre Abbildung einen k-Algebra-Homomorphismus

$$f^*: k[T] = k[\mathbf{G}_a] \longrightarrow k[G], (\mathbf{G}_a = k \xrightarrow{p} k) \mapsto (G \xrightarrow{p\circ f} k).$$

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

$$f: G \longrightarrow k = \mathbf{G}_a.$$

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

$$\begin{aligned}\mathcal{A}(G) &= \{f \in k[G] \mid \Delta(f) = 1\otimes f + f\otimes 1 \}\\ &= \mathrm{Ker}(\varphi: k[G] \longrightarrow k[G]\otimes_k k[G],\ f \mapsto \Delta(f) - 1\otimes f + f\otimes 1 \}\end{aligned}$$

Weil G eine F-Gruppe ist, ist $\Delta: k[G] \longrightarrow k[G]\otimes_k k[G]$ über F definiert, d.h. von der Gestalt

$$\Delta = k\otimes_F \Delta_F$$

mit einer F-linearen Abbildung

$$\Delta_F: F[G] \longrightarrow F[G]\otimes_F F[G].$$

Damit hat φ die Gestalt $k\otimes\varphi_F$ mit der F-linearen Abbildung

$$\varphi_F: F[G] \longrightarrow F[G]\otimes_F F[G],\ f \mapsto \Delta_F(f) - 1\otimes f + f\otimes 1.$$

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.
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).

$$(\sum_i a_i\bullet T^i)\bullet f := \sum_i a_i\bullet f^{p^i} \text{ für } f \in \mathcal{A}(F) \text{ und } \sum_i a_i\bullet T^i \in R(F). \qquad (1)$$

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.[1]

(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.

---

[1] Die Gleichung $0 = x^p - x = x\bullet(x^{p-1}-1)$ hat in F genau p Lösungen.

(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.

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

$$p \bullet q = (\sum_i a_i T^i) \bullet (\sum_j b_j T^j)$$

$$= \sum_{i,j} a_i \bullet \phi^i(b_j) \bullet T^{i+j}.$$

also

$$\deg(p \bullet q) = \max \{i+j \mid a_i \bullet \phi^i(b_j) \neq 0\}$$

$$= \max \{i+j \mid a_i \neq 0 \text{ und } \phi^i(b_j) \neq 0\}$$

$$= \max \{i+j \mid a_i \neq 0 \text{ und } b_j \neq 0\}.$$

Dies ist aber gerade der Grad des Produkts im gewöhnlichen Polynomring $F[T]$.

Zu (v). Seien $p, q \in R(F)$ 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 $p \bullet q$ von Null verschieden.

Zu (vi). Nach Voraussetzung gibt es Elemente $f_1, \ldots, f_r \in \mathcal{A}(G)$ mit

$$\mathcal{A}(G) = R(k) \bullet f_1 + \ldots + R(k) \bullet f_r. \qquad (1)$$

Wegen

$$k \otimes_F \mathcal{A}(G)(F) \xrightarrow{\cong} \mathcal{A}(G)(k)$$

gibt es Elemente $\tilde{f}_1, \ldots, \tilde{f}_s \in \mathcal{A}(G)(F)$ 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 $i = 1, \ldots, r$. 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,

$$f_1,\ldots,f_r \in \mathcal{A}(G)(F). \tag{2}$$

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

$$M \hookrightarrow \mathcal{A}(G)(F) \tag{3}$$

wird durch den Funktor $k\otimes_F$ in eine bijektive Abbildung

$$k\otimes_F M \longrightarrow k\otimes_F \mathcal{A}(G)(F)$$

überführt.[2] Weil k treuflach über F muß bereits (3) surjektiv sein[3], 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.

14.3.2 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,

$$p > 0.$$

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

$$b = c\bullet a + d \text{ und } \deg d < \deg a.$$

Beweis. Bezeichne

$$\phi: F \longrightarrow F,\ x \mapsto x^p$$

die in 3.3.1 B beschriebene Abbildung.
Zu (i). Die Eindeutigkeit von c und d.

Seien c, c', d, d' ∈ 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

---

[2] Unser Argumente zeigen, die Abbildung ist surjektiv. Sie ist injektiv, weil k flach ist über F.
[3] siehe auch Bemerkung 1.3.7 B (iv).

$$T^{N-n}\bullet a = \sum_{i=0}^{n} c_{N-n}\bullet\phi^{i}(a_i)T^{N-n+i}$$

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.

Index

Inhalt