Lineare algebraische Gruppen

Vorlesung 11 im Sommersemester 2021 (am 25.06.21):Additive Funktionen III

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 III: Eigenschaften des R(F)-Moduls $\mathcal{A}(G)(F)$

14.3 Additive Funktionen

14.3.3 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).[1] 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•b gerade das Produkt b•a in R(F) ist.
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

$$e_1,\ldots, e_r \text{ von } R^r \text{ und } e_1,\ldots, e_s \text{ von } R^s$$

so 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.[2]

---

[1] 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.

1. Schritt. Die Matrix von g bezüglich der Basis $e_1,...,e_{i-1}, e_i - \lambda\bullet e_j, e_{i+1},..., e_s$ des Urbildmoduls R^s hat die Spalten

$$a_1,..., a_{i-1}, a_i-\lambda\bullet a_j, a_{i+1},...,a_s$$

Es gilt

$$\begin{aligned} g(e_\nu) &= A\bullet e_\nu \\ &= a_\nu \\ &= a_{1\nu}\bullet e_1+...+a_{r\nu}\bullet e_r \\ &= \sum_{\alpha=1}^{r} a_{\alpha\nu}\bullet e_\alpha \end{aligned}$$

und

$$g(e_i - e_j\bullet\lambda) = \sum_{\alpha=1}^{r} a_{\alpha i}\bullet e_\alpha - \Big(\sum_{\alpha=1}^{r} a_{\alpha j}\bullet e_\alpha\Big)\bullet\lambda \qquad \text{(g ist R-linear)}$$

$$= \sum_{\alpha=1}^{r} a_{\alpha i}\bullet e_\alpha - \Big(\sum_{\alpha=1}^{r} a_{\alpha j}\bullet \lambda\bullet e_\alpha\Big) \qquad (e_\alpha\bullet\lambda = \lambda\bullet e_\alpha, \text{ denn 1 kommutiert mit } \lambda)$$

$$= (a_{1i}- \lambda\bullet e_{1j})\bullet e_1+...+(a_{ri}-\lambda\bullet e_{rj})\bullet e_r$$

Die Matrix der Abbildung g bezüglich der neuen Basis des Urbild-Moduls R^s hat somit die Spalten

$$a_1,..., a_{i-1}, a_i-\lambda\bullet a_j, a_{i+1},...,a_s$$

Mit $e_1,..., e_r$ und $\lambda\in R$ ist auch $e_1,...,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},..., e_r$ eine Basis von R^r.

2. Schritt. Die Matrix von g bezüglich der Basis $e_1,...,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},..., e_r$ des Bildmoduls R^r hat die Zeilen

$$a^1,..., a^{j-1}, a^j+a^i\bullet\lambda, a^{j+1}, ... , a^r.$$

Es gilt

$$\begin{aligned} g(e_\nu) &= A\bullet e_\nu \\ &= a_\nu \\ &= a_{1\nu}\bullet e_1+...+a_{r\nu}\bullet e_r \\ &= a_{1\nu}\bullet e_1+...+ a_{i-1\nu}\bullet e_{i-1}, a_{i\nu}(e_i - e_j\bullet\lambda)+a_{i+1\nu} e_{i+1}+...+ a_{r\nu}\bullet e_r \\ &\quad + a_{i\nu}\bullet e_j\bullet\lambda \end{aligned}$$

Die neue Linearkombination hat dieselben Koeffizienten wie die alte mit Ausnahme des Koeffizienten des j-ten Vektors. Wegen

$$\begin{aligned} a_{j\nu}\bullet e_j + a_{i\nu}\bullet e_j\bullet\lambda &= a_{j\nu}\bullet e_j + a_{i\nu}\bullet\lambda\bullet e_j \qquad (e_j\bullet\lambda = \lambda\bullet e_j, \text{ denn 1 kommutiert mit } \lambda) \\ &= (a_{j\nu} + a_{i\nu}\bullet\lambda)\bullet e_j \end{aligned}$$

---

[2] Weil sich jeder der Vektoren $e_1,...,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},..., e_s$ als R-Linearkombination von $e_1,..., e_s$ und jeder der Vektoren $e_1,..., e_s$ als R-Linearkombination von $e_1,...,e_{i-1}, e_i - e_j\bullet\lambda, e_{i+1},..., e_s$ schreiben läßt.

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

$$a^1, ..., a^{j-1}, a^j + a^i \bullet \lambda, a^{j+1}, ..., a^r.$$

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)[3]. 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

$$A = \begin{pmatrix} \lambda_1 & 0 & .. & 0 \\ 0 & \lambda_2 & ... & 0 \\ ... & ... & ... & ... \\ ... & ... & ... & ... \end{pmatrix}.$$

Die Abbildung g hat dann die Gestalt

$$g: R^s \longrightarrow R^r, \begin{pmatrix} y_1 \\ ... \\ y_s \end{pmatrix} \mapsto \begin{pmatrix} \lambda_1 \bullet y_1 \\ ... \\ \lambda_t \bullet y_t \\ ... \\ ... \end{pmatrix},$$

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

$$Ker(f) = Im(g) = e_1\lambda_1 \bullet R + ... + e_t\lambda_t \bullet R.$$

---

[3] Dabei müssen wir bei Spalten-Operationen von links und bei Zeilen-Operationen von rechts multiplizieren.

Wir können annehmen, alle $\lambda_i \in R$ sind ungleich 0. Es gilt

$$M \cong R^r/Ker(f) \cong (R/\lambda_1 R) \oplus ... \oplus (R_t/\lambda_t R) \oplus R^{r-t}.$$

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.

14.3.4 Der Fall $G = G_a^n$

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

$$\begin{array}{ccccc} k[G] & \xleftarrow{\phi^*} & k[\mathbf{G}_a] & = k[T] & f(T_1,...,T_n) \quad \mapsfrom \quad T \\ \mu^*\downarrow & & \downarrow\mu_a^* & & \downarrow \qquad\qquad \downarrow \\ k[G]\times k[G] & \xleftarrow{\phi^*\otimes\phi^*} & k[\mathbf{G}_a]\otimes k[\mathbf{G}_a] & = k[T,U] & f(T_1+U_1,...,T_n+U_n) \\ & & & & \| \\ & & & & f(T_1,...,T_n)+f(U_1,...,U_n) \mapsfrom T+U \end{array}$$

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 gilt

$$T \bullet f = f^p$$

Die Modulstruktur ist eine Folge der Tatsache, daß die p-te Potenz eines additiven Polynoms ein additives Polynom ist.

14.3.5 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.

14.3.6 Lemma: Relationen in $\mathcal{A}$(G)(F) über F und R(F)

Seien F ein Teilkörper des algebraisch abgeschlossenen Körpers k und G affine 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[4]

$$r = T^{\ell} + a_1 \bullet T^{\ell-1} + ... + a_{\ell} \in R(F).$$

Auf Grund der in 3.3.1 B definierten R(F)-Modul-Struktur von $\mathcal{A}(G)(F)$ gilt dann

[4] 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.[5] 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

$$(T_1,\ldots,T_s) = (f_1,\ldots,f_s)$$

---

[5] 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.

Index

—A—

additives Polynom, 5

—E—

Elementaroperationen, 4
entgegengesetzter Ring, 2

—P—

Polynom
additives, 5

—R—

Ring
entgegengesetzter, 2

Inhalt

LINEARE ALGEBRAISCHE GRUPPEN 1

14 KOMMUTATIVE LINEARE ALGEBRAISCHE GRUPPEN 1

14.3 Additive Funktionen 1
14.3.3 Lemma: Zerlegung von R-Moduln in zyklische 1
14.3.4 Der Fall $G = G_a^n$ 5
14.3.5 Lemma: die Struktur von $A(G_a^n)(F)$ als R(F)-Modul 6
14.3.6 Lemma: Relationen in A(G)(F) über F und R(F) 8

INDEX 11

INHALT 11