Lineare algebraische Gruppen

Vorlesung 12 im Sommersemester 2021 (am 2.07.21):
Elementare unipotente Gruppen I: polynomiale Kozyklen

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 I: polynomiale Kozyklen

14.4 Elementare unipotente Gruppen

14.4.1 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

14.4.2 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 $j_\nu \leq m_{i_\nu} < p$, 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

$$\binom{m}{n} \neq 0 \bmod p \quad \Leftrightarrow \binom{m_i}{n_i} \neq 0 \bmod p \text{ für jedes i.}$$

$$\Leftrightarrow n_i \leq m_i \text{ für jedes i.}$$

$$\Leftrightarrow n \leq_p m$$

QED.

14.4.3 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

$$(\partial f)(T, U, V) :=^{1} f(U, V) - f(T+U, V) + f(U+V,T) - f(T,U).$$

Bemerkungen

(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

---

[1] Diese Definition weicht von der in Lazard [1] ab. Sie vertauscht die Argumente des dritten Summanden in der dortigen Definition:
$$(\partial f)(T, U, V) := f(U, V) - f(T+U, V) + f(T,U+V) - f(T,U).$$

$$(x+y)^q = (x^{p^\ell} + y^{p^\ell})^s = x^q + s\bullet x^{(s-1)p^\ell} y^{p^\ell} + \ldots + y^q \pmod p,$$

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.

14.4.4 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,
$$f \text{ ist homogen vom Grad } d.$$
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

$$\frac{(d-j+1)\cdot(d-j+2)\cdot\ldots\cdot d}{(d-h-j+1)\cdot(d-h-j+2)\cdot\ldots\cdot(d-h)} = \frac{(d-h+1)\cdot(d-h+2)\cdot\ldots\cdot d}{(d-h-j+1)\cdot(d-h-j+2)\cdot\ldots\cdot(d-j)}$$

multiplizieren. Wegen

$$\frac{(d-j)!}{h!\cdot(d-h-j)!}\cdot\frac{(d-j+1)\cdot(d-j+2)\cdot\ldots\cdot d}{(d-h-j+1)\cdot(d-h-j+2)\cdot\ldots\cdot(d-h)} = \frac{d!}{h!\cdot(d-h)!} = \binom{d}{h}$$

und

$$\frac{(d-h)!}{j!\cdot(d-h-j)!}\cdot\frac{(d-h+1)\cdot(d-h+2)\cdot\ldots\cdot d}{(d-h-j+1)\cdot(d-h-j+2)\cdot\ldots\cdot(d-j)} = \frac{d!}{j!\cdot(d-j)!} = \binom{d}{j}$$

erhalten wir

$$\binom{d}{h}\cdot c_j = \binom{d}{j}\cdot c_h$$

also

$$\begin{aligned} c_j\cdot((T+U)^d - T^d - U^d) &= \sum_{h=1}^{d-1} c_j\cdot\binom{d}{h}T^h\cdot U^{d-h} \\ &= \sum_{h=1}^{d-1} c_h\cdot\binom{d}{j}T^h\cdot U^{d-h} \\ &= \binom{d}{j}\cdot\sum_{h=1}^{d-1} c_h\cdot T^h\cdot U^{d-h} \\ &= \binom{d}{j}\cdot f(T, U) \qquad (\text{wegen } c_0 = c_d = 0) \end{aligned}$$

Für $j = 1$ erhalten wir

$$c_1\cdot((T+U)^d - T^d - U^d) = d\cdot f(T, U).$$

Weil die Charakteristik gleich 0 ist, können wir durch d teilen und

$$g(T) = (c_1/d)\cdot T^d$$

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 $j = 1$:

$$(d-h)\cdot c_h = \binom{d-1}{h}\cdot c_1.$$

Wir ersetzen h durch d-h und erhalten

$$h\cdot c_{d-h} = \binom{d-1}{d-h}\cdot c_1$$

und mit (3)

$$h\cdot c_h = \binom{d-1}{d-h}\cdot c_1 \qquad (5)$$

für $0 < h < d$.

Ebenfalls aus (4) erhalten wir

$$\binom{d-j}{d-h-j} \cdot c_j = \binom{d-h}{d-h-j} \cdot c_h$$

für $0 < h, j < d$ und speziel für $j = d-h-1$, d.h. $d-h-j = 1$ ist

$$(d-j) \cdot c_j = (d-h) \cdot c_h,$$

also

$$(h+1) \cdot c_{d-h-1} = (d-h) \cdot c_h \text{ für } h = 1,..., d-2.$$

Zusammen mit (3) folgt

$$(h+1) \cdot c_{h+1} = (d-h) \cdot c_h \text{ für } h = 1,..., d-2. \qquad (6)$$

Wir haben drei Fälle zu unterscheiden.

1. Fall: d ist teilerfremd zur Charakteristik p von k.
Es gilt

$$\begin{aligned}
\frac{\partial f(T,U)}{\partial T} &= \sum_{h=1}^{d-1} h \cdot c_h \cdot T^{h-1} \cdot U^{d-h} \\
&= \sum_{h=1}^{d-1} \binom{d-1}{d-h} \cdot c_1 \cdot T^{h-1} \cdot U^{d-h} && \text{(nach (5))} \\
&= c_1 \cdot \sum_{h=1}^{d-1} \binom{d-1}{d-h} \cdot T^{h-1} \cdot U^{d-h} \\
&= c_1 \cdot \sum_{h=1}^{d-1} \binom{d-1}{h-1} \cdot T^{h-1} \cdot U^{d-h} && \text{(wegen } \binom{n}{\nu} = \binom{n}{n-\nu}\text{)} \\
&= c_1 \cdot \sum_{h=0}^{d-2} \binom{d-1}{h} \cdot T^{h} \cdot U^{(d-1)-h} && \text{(Index-Verschiedung)} \\
&= c_1 \cdot ((T+U)^{d-1} - T^{d-1}) \\
&= (c_1/d) \cdot \frac{\partial}{\partial T} ((T+U)^d - T^d - U^d))
\end{aligned}$$

und

$$\begin{aligned}
\frac{\partial f(T,U)}{\partial U} &= \sum_{h=1}^{d-1} (d-h) \cdot c_h \cdot T^{h} \cdot U^{d-h-1} \\
&= \sum_{h=1}^{d-1} (d-h) \cdot c_{d-h} \cdot T^{h} \cdot U^{d-h-1} && \text{(nach (3))} \\
&= \sum_{h=1}^{d-1} \binom{d-1}{h} \cdot c_1 \cdot T^{h} \cdot U^{(d-1)-h} && \text{(nach (5) mit d-h anstelle von h)} \\
&= c_1 \cdot \sum_{h=1}^{d-1} \binom{d-1}{h} \cdot T^{h} \cdot U^{(d-1)-h} \\
&= c_1 \cdot ((T+U)^{d-1} - U^{d-1}) \\
&= (c_1/d) \cdot \frac{\partial}{\partial U} ((T+U)^d - T^d - U^d)
\end{aligned}$$

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

$$c_{p-j} = 0 \qquad (7)$$

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

$$(d-p+j+1)\bullet c_{p-j-1} = (p-j)\bullet c_{p-j} = 0,$$

wegen $d-p+j+1 = j+1 \pmod p$ und $j+1 \le p-1$ 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 $j \le p-2$ gilt, d.h. es gilt (7) mit $j = p-1$, also

$$c_{p-1} = c_{p-2} = \dots = c_1 = 0.$$

Mit $c_1 = 0$ gilt nach (5), $h\bullet c_h = 0$ für $h = 1,\dots, d-1$, also

$$c_h = 0 \text{ für jedes } h \in \{1,\dots,q-1\}, \text{ welches kein Vielfaches von p ist.}$$

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

$$0 = f(T,U,V) = (\partial\tilde{f})(T^p,U^p, V^p). \qquad (3.9)$$

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

$$d = p^{\ell}\bullet s \text{ mit } s \neq 1 \text{ und } s \neq 0 \pmod p,$$

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

$$g(T) = a\bullet T^d \text{ und } \mathcal{L} = 0.$$

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 $\mathbb{Z}[T]$:

$$\begin{aligned} \sum_{i=1}^{p-1} ((T+iT)^d - T^d - (iT)^d) &= \sum_{i=1}^{p-1} ((1+i)^d - 1 - i^d)\bullet T^d \\ &= ((2^d+3^d+...+p^d) - (p-1)\bullet 1 - (1^d+2^d+...+(p-1)^d)\bullet T^d \\ &= (p^d - (p-1) - 1^d)\bullet T^d \\ &= (p^d - p)\bullet T^d \\ &= p\bullet(p^{d-1} - 1)\bullet T^d \end{aligned}$$

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

$$0 = \sum_{i=1}^{p-1} f(T,iT)$$
$$= \sum_{i=1}^{p-1} g(T+iT) - g(T) - g(U) + \sum_{i=1}^{p-1} a \bullet c(T,iT) p^{\ell-1}.$$

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.

14.4.5 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

$$(\partial f)(\mathbf{T}, \mathbf{U}, \mathbf{V}) = f(\mathbf{U},\mathbf{V}) - f(\mathbf{T}+\mathbf{U}, \mathbf{V}) + f(\mathbf{U}+\mathbf{V}, \mathbf{T}) - f(\mathbf{T},\mathbf{U}).$$

Das Polynom f heißt <u>polynomialer 2-Kozyklus</u>, wenn $\partial f = 0$ gilt.

14.4.6 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

$$f(\mathbf{T}, \mathbf{U}) \in F[\mathbf{T}, \mathbf{U}]$$

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

$$\binom{d}{j} / \binom{d-h}{j} = \frac{d!}{j!\bullet(d-j)!} / \frac{(d-h)!}{j!\bullet(d-h-j)!} = \frac{d!\bullet(d-h-j)!}{(d-j)!\bullet(d-h)!}.$$

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

$$d_{\mathbf{T}}(G) := \max \{\deg_{T_1} G,...,\deg_{T_n} G\}$$

das Maximum der Grade von G als Polynom einer der Unbestimmten T_i. Die Einschränkung des F-Algebra-Homomorphismus

$$\psi^{\mathbf{T}}_{q,n}:F[\mathbf{T}] \longrightarrow F[T],\ f(\mathbf{T}) \mapsto f(T,T^q,T^{q^2},...,T^{q^{n-1}}),$$

auf den F-linearen Unterraum

$$F[\mathbf{T}]_{<q} = \{G \in F[\mathbf{T}] \mid \deg_{T_i} G < q \text{ für } i = 1,...,n\}$$

der Polynome G mit $d_{\mathbf{T}}(G) < q$ induziert dann einen F-linearen Isomorphismus

$$\psi^{\mathbf{T}}_{q,n}|_{F[\mathbf{T}]_{<q}}:F[\mathbf{T}]_{<q} \xrightarrow{\cong} F[T]_{<q^n}, \qquad (6)$$

auf den F-linearen Unterraum der Polynome vom Grad $< q^r$. Man beachte, $F[\mathbf{T}]_{<q}$ besitzt die Potenzprodukte

$$T^{\ell} = T_1^{\ell_1} \bullet ... \bullet T_n^{\ell_n} \text{ mit } \ell_\nu < q$$

als Basis. Das Bild dieser Basis-Elemente ist gerade die Menge der Potenzen

$$\begin{aligned}\psi^{\mathbf{T}}_{q,n}(T^{\ell}) &= \psi^{\mathbf{T}}_{q,n}(T_1^{\ell_1} \bullet ... \bullet T_n^{\ell_n}) \\ &= T^{\ell_1} \bullet (T^q)^{\ell_2} \bullet ... \bullet (T^{q^{n-1}})^{\ell_n} \\ &= T^{\ell_1 + \ell_2 \bullet q + \ell_3 \bullet q^2 + ... + \ell_n \bullet q^{n-1}} \\ &= T^{\varphi_{q,n}(\ell)}\end{aligned}$$

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

$$\psi^{\mathbf{T}}_{q,n} \otimes \psi^{\mathbf{U}}_{q,n}:F[\mathbf{T},\mathbf{U}] = F[\mathbf{T}] \otimes_F F[\mathbf{U}] \longrightarrow F[T] \otimes_F F[U] = F[T,U],$$

$$f(\mathbf{T},\mathbf{U}) \mapsto f(T,T^q,T^{q^2},...,T^{q^{n-1}},\ U,U^q,U^{q^2},...,U^{q^{n-1}}),$$

induziert dann einen F-linearen Isomorphismus

$$F[\mathbf{T},\mathbf{U}]_{<q} = F[\mathbf{T}]_{<q} \otimes_F F[\mathbf{U}]_{<q} \longrightarrow F[T]_{<q^n} \otimes_F F[U]_{<q^n} = F[T,U]_{<q^n}. \qquad (7)$$

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

$$\begin{aligned}
\psi(\partial(\mathbf{T}^i\mathbf{U}^j)) &= \psi(\mathbf{U}^i)\,\psi(\mathbf{V}^j) - \psi((\mathbf{T}+\mathbf{U})^i)\,\psi(\mathbf{V}^j) + \psi((\mathbf{U}+\mathbf{V})^i)\,\psi(\mathbf{T}^j)) - \psi(\mathbf{T}^i)\psi(\mathbf{U}^j)\\
&= \psi(\mathbf{U}^i)\,\psi(\mathbf{V}^j)\\
&\quad - \psi(\textstyle\prod_{\nu=1}^{n}(T_\nu+U_\nu)^{i_\nu})\,\psi(\mathbf{V}^j)\\
&\quad + \psi(\textstyle\prod_{\nu=1}^{n}(U_\nu+V_\nu)^{i_\nu})\,\psi(\mathbf{T}^j))\\
&\quad - \psi(\mathbf{T}^i)\psi(\mathbf{U}^j)\\
&= \psi(\mathbf{U}^i)\,\psi(\mathbf{V}^j)\\
&\quad - \textstyle\prod_{\nu=1}^{n}(\psi(T_\nu)+\psi(U_\nu))^{i_\nu}\,\psi(\mathbf{V}^j)\\
&\quad + \textstyle\prod_{\nu=1}^{n}(\psi(U_\nu)+\psi(V_\nu))^{i_\nu}\,\psi(\mathbf{T}^j))\\
&\quad - \psi(\mathbf{T}^i)\psi(\mathbf{U}^j)\\
&= U^{\varphi_{q,n}(i)}V^{\varphi_{q,n}(j)}\\
&\quad - \textstyle\prod_{\nu=1}^{n}(T^{q^{\nu-1}}+U^{q^{\nu-1}})^{i_\nu}\bullet V^{\varphi_{q,n}(j)}\\
&\quad + \textstyle\prod_{\nu=1}^{n}(U^{q^{\nu-1}}+V^{q^{\nu-1}})^{i_\nu}\bullet T^{\varphi_{q,n}(j)}\\
&\quad - T^{\varphi_{q,n}(i)}U^{\varphi_{q,n}(j)}
\end{aligned}$$

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

$$g(\mathbf{T}) = \mathbf{T}^m \text{ mit } m \neq (0,...,0)$$

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

$$0 = \sum_{j=0}^{n-1} a_j\bullet (p^{p-1} - 1)\, T_{j+1}^p.$$

Weil die Charakteristik von F gleich p ist, folgt

$$0 = \sum_{j=0}^{n-1} a_j\bullet T_{j+1}^p,$$

also $a_0 = a_1 = ... = a_{n-1} = 0$.
QED.

Index

Inhalt