Lambdafunktionen

Martin Ziegler

2.4.2003*

Sei K ein separabel abgeschlossener Körper der Charakteristik p mit (endlicher) p–Basis $b_1, \ldots b_e$. Die Lambdafunktionen $\lambda_\nu : K \to K$ sind definiert durch

$$x = \sum \lambda_\nu(x)^p b^\nu,$$

dabei sind die ν Multiindices $(\nu_1, \ldots, \nu_e)$ mit $0 \leq \nu_i < p$ und b^ν bezeichnet $b_1^{\nu_1} \cdots b_e^{\nu_e}$.

Wenn man die Sprache $L = \{0, 1, +, -, \cdot\}$ um Konstanten für die b_i und Funktionzeichen für die λ_ν erweitert, hat K bekanntlich Quantorenelimination. Françoise Delon zufolge kann man auf die Konstanten für die b_i verzichten. Ich geben einen neuen Beweis dafür, der gleichzeitig etwas mehr beweist.

Sei also L_λ die Erweiterung von L durch die λ_ν und $L_{\lambda,b}$ die Erweiterung von L_λ durch Konstanten für die b_i, die wir der Einfachheit auch b_i nennen. Wir werden zeigen:

Satz 1. *Zu jeder quantorenfreien $L_{\lambda,b}$–Formel ϕ gibt es eine quantorenfreie L_λ-Formel, die in allen Körpern mit ausgezeichneter p–Basis $b_1, \ldots, b_e$ zu ϕ äquivalent ist.*

Wir geben den Beweis **nur im Fall** $e = 1$. Der allgemeine Fall wird analog behandelt. Wir schreiben jetzt b für b_1 und λ_i für $\lambda_{(i)}$. Der Satz ergibt sich aus einer Folge von Lemmas.

Lemma 2. *Jeder $L_{\lambda,b}$-Term ist äquivalent zu einem Term*

$$t_0 + t_1 b + \cdots + t_N b^N \tag{1}$$

für L_λ-Terme t_i.

Beweis. 0, 1 und b haben die Form (1). Die Menge der Terme der Form (1) ist (bis auf Äquivalenz) abgeschlossen unter $+$, $-$ und $\cdot$. Es bleibt also nur die Abgeschlossenheit unter den λ_i, $(i < p)$, zu zeigen. Nun ist aber (in allen Körpern mit p–Basis (b))

$$\lambda_i(t_0 + t_1 b + \cdots + t_N b^N) = \lambda_i(t_0) + \lambda_i(t_1 b) + \cdots + \lambda_i(t_N b^N),$$

und Behauptung folgt aus der Identität

$$\lambda_i(x b^n) = \lambda_r(x) b^k,$$

*5.6.2009: Einige Schreibfehler korrigiert.

wobei sich $r < p$ und k durch $r + n = pk + i$ bestimmen. Wir bemerken noch, daß $k < n$, wenn $n > 1$. $\square$

Aus dem Beweis ergibt sich sofort

Lemma 3. *Sei $N > 1$. Dann ist jeder Term $\lambda_i(t_0+t_1b+\cdots+t_Nb^N)$ äquivalent zu einem Term der Form $s_0 + s_1b + \cdots + s_{N-1}b^{N-1}$, für L_λ-Terme s_i.* $\square$

Lemma 4. *Jede Gleichung $S \doteq T$ zwischen $L_{\lambda,b}$-Termen ist äquivalent zu einer Konjunktion von Gleichungen der Form $s + tb \doteq 0$, für L_λ-Terme s und t.*

Beweis. Wegen Lemma 2 genügt es Gleichungen der Form

$$t_0 + t_1b + \cdots + t_Nb^N \doteq 0$$

zu betrachten. Diese Gleichung ist aber äquivalent zur Konjunktion der Gleichungen $\lambda_i(t_0+t_1b+\cdots+t_Nb^N) \doteq 0$ für alle $i < p$. Mit Lemma 3 und Induktion folgt die Behauptung. $\square$

Satz 1 folgt jetzt sofort aus Lemma 4 und dem nächsten Lemma.

Lemma 5. *Die Gleichung*

$$xb \doteq y \tag{2}$$

ist äquivalent zu einer quantorenfreien L_λ-Formel.

Beweis. Wenn $x \neq 0$, ist $\dfrac{y}{x} = b$ äquivalent mit der Konjunktion von $\left(\dfrac{y}{x}\right)^{p-1} = b^{p-1}$ und $\left(\dfrac{y}{x}\right)^{p-2} = b^{p-2}$. Daraus folgt, daß (2) und

$$(x \doteq 0 \wedge y \doteq 0) \ \vee \ (\neg x \doteq 0 \ \wedge \ xy^{p-1} \doteq x^pb^{p-1} \ \wedge \ x^2y^{p-2} \doteq x^pb^{p-2})$$

äquivalent sind. $xy^{p-1} \doteq x^pb^{p-1}$ ist aber äquivalent zu

$$\lambda_{p-1}(xy^{p-1}) \doteq x \wedge \bigwedge_{i\neq p-1} \lambda_i(xy^{p-1}) \doteq 0,$$

und $x^2y^{p-2} \doteq x^pb^{p-2}$ ist äquivalent zu

$$\lambda_{p-2}(x^2y^{p-2}) \doteq x \wedge \bigwedge_{i\neq p-2} \lambda_i(x^2y^{p-2}) \doteq 0.$$

$\square$