COMPOSITIO MATHEMATICA

KLAUS LANGMANN

Lösungsanzahl der homogenen Normformengleichung

Compositio Mathematica, tome 94, n° 1 (1994), p. 29-49
<http://www.numdam.org/item?id=CM_1994__94_1_29_0>

Compositio Mathematica **94**: 29–49, 1994.

Lösungsanzahl der homogenen Normformengleichung

KLAUS LANGMANN
Mathematisches Institut, Einsteinstr 62, D-4400 Münster

Received 29 October 1992; accepted in final form 20 August 1993

Wenn N die Norm in einem Zahlkörper bedeutet, so sind Endlichkeitssätze für die Gleichung $N(\alpha_1 x_1 + \cdots + \alpha_m x_m) = p$ schon seit längerer Zeit bekannt [5]. Wir zeigen hier, daß unter gewissen Voraussetzungen für fast alle Primzahlen p diese Gleichung bis auf triviale Fälle höchstens eine Lösung hat (Satz 6). Dieser Satz 6 verallgemeinert den Satz 3 aus [3] auf mehrdimensionale Normformengleichungen; dazu muß der "3-Werte-Satz" aus [3] ebenfalls mehrdimensional verallgemeinert werden (Satz 3/4). Ganz entscheidend für dessen Beweis ist wieder der Einheitensatz von Evertse-Laurent-van der Poorten-Schlickewei [1]. Satz 8/9 schließlich gibt Abschätzungen der Lösungsanzahl dieser Normformengleichung auch für beliebige natürliche Zahlen p.

An dieser Stelle möchte ich dem Referenten für wertvolle Hinweise (insbesondere auf einen größeren Fehler im Bewis von Satz 6/9) herzlich danken.

In der ganzen Arbeit sei $K \supset \mathbb{Q}$ eine endliche Galoiserweiterung und S eine feste endliche Menge von Bewertungen von K, die alle archimedischen Bewertungen enthalte. R bezeichne stets den Ring der S-ganzen Zahlen von K. Für $x \in K$ bezeichen mit $\mathscr{D}_S(x)$ den Divisor $\Sigma_{\wp \notin S} \operatorname{ord}_\wp x$. Weiter heißen zwei Vektoren $(\alpha_{11}, \ldots, \alpha_{1m}) \in K^m$ und $(\alpha_{21}, \ldots, \alpha_{2m}) \in K^m$ untereinander konjugiert, wenn es einen Galoisautomorphismus σ von K über $\mathbb{Q}$ gibt, so daß $(\alpha_{11}, \ldots, \alpha_{1m}) = (\sigma(\alpha_{21}), \ldots, \sigma(\alpha_{2m}))$ ist.

Grundlegend für den Beweis des Hauptergebnisses ist folgendes Lemma (dessen Beweis in [2] 1.12.2 zu finden ist; dabei ging entscheidend der Einheitensatz [1] ein):

LEMMA 1. *Sei $X \subset \mathbb{C}^n$ eine abgeschlossene Untervarietät. Ist $X_0 \subset X$ ein irreduzibeler Unterraum, so daß $X_0 \cap (R^*)^n$ zariskidicht ist, so gibt es eine Zahl d und eine algebraische Abbildung $h: (\mathbb{C}^*)^d \to X_0 \subset \mathbb{C}^n$, so daß jede Komponente h_v von h die Gestalt $h_v(t_1, \ldots, t_d) = c_v t_1^{n_{v1}} \cdots t_d^{n_{vd}}$ mit $c_v \in \mathbb{C}$ und $n_{uv} \in \mathbb{Z}$ hat und so daß $h((\mathbb{C}^*)^d)$ zariskidicht in X_0 ist.*

Hiermit zeigen wir nun, daß die Lösungsmenge gewisser linearer Divisorengleichungen eine endliche Vereinigung linearer Teilräume ist (daß dies

im allgemeinen nicht richtig ist, zeigt die Divisorengleichung $\mathscr{D}(x+\sqrt{2}y) = \mathscr{D}(x-\sqrt{2}y)$, deren Lösungsmenge $(x,y)\in\mathbb{Q}^2$ aus unendlich vielen Geraden besteht):

LEMMA 2. *Gegeben seien zwei Vektoren* $\alpha_1=(\alpha_{11},\ldots,\alpha_{1m})\in K^m$ *und* $\tilde{\alpha}_1=(\tilde{\alpha}_{11},\ldots,\tilde{\alpha}_{1m})\in K^m$. *Bezeichne mit* $(\alpha_i,\tilde{\alpha}_i)\in K^{2m}$ *für* $1\leqslant i\leqslant k$ *die zu* $(\alpha_1,\tilde{\alpha}_1)$ *konjugierten Vektoren. Für eine feste Zahl g mit* $m\leqslant g\leqslant \frac{1}{2}(k+1)$ *sei für jede g-elementige Teilmenge* $\{i_1,\ldots,i_g\}\subset\{1,\ldots,k\}$ *stets*

$$Rang\{\alpha_{i_1},\ldots,\alpha_{i_g}\}=m=Rang\{\tilde{\alpha}_{i_1},\ldots,\tilde{\alpha}_{i_g}\}.$$

Betrachte die Menge

$$M_S:=\left\{(x_1,\ldots,x_m)\in\mathbb{Q}^m;\ \mathscr{D}_S\left(\sum_{v=1}^{m}\alpha_{1v}x_v\right)=\mathscr{D}_S\left(\sum_{v=1}^{m}\tilde{\alpha}_{1v}x_v\right)\right\}$$

Es gibt dann endlich viele über $\mathbb{Q}$ *definierte lineare Abbildungen* $f_u:=(f_{u1},\ldots,f_{um})$: $\mathbb{Q}^m\to\mathbb{Q}^m$, *so daß*

$$M_S=\bigcup_{u=1}^{<\infty} f_u(\mathbb{Q}^m)$$

ist und so daß für gewisse $c_u\in R^*$ *die Identitäten*

$$\sum_{v=1}^{m}\alpha_{1v}f_{uv}(t)=c_u\sum_{v=1}^{m}\tilde{\alpha}_{1v}f_{uv}(t)$$

für alle u und alle $t\in\mathbb{Q}^m$ *gelten.*

Beweis. Für $m=1$ ist die Aussage trivial. Sei die Behauptung für $(m-1)$ richtig. Bezeichne mit $\bar{M}_S$ den Zariskiabschluß von $M_S\subset\mathbb{C}^m$. Wir treffen Fallunterscheidung.

Fall (1). Es gibt eine irreduzibele Komponente Y_0 von $\bar{M}_S$, die nicht in einer Hyperebene der Form $\mathrm{Var}(\beta_1X_1+\cdots+\beta_mX_m)$ liegt.

Da alle $(\alpha_i,\tilde{\alpha}_i)$ zu $(\alpha_1,\tilde{\alpha}_1)$ konjugiert sind, gibt es auf Grund der Divisorengleichung zunächst von $x=(x_1,\ldots,x_m)\in Y_0\cap M_S$ abhängige S-Einheiten $e_i(x)\in K$, so daß gilt

$$\sum_{v=1}^{m}(\alpha_{iv}-e_i(x)\tilde{\alpha}_{iv})x_v=0\quad\text{für } 1\leqslant i\leqslant k \tag{1}$$

Nach eventueller Umnumerierung von $x_1,\ldots,x_m$ und nach Teilmengenbildung aller betrachteten $x\in Y_0\cap M_S$ erhalten wir eine in Y_0 zariskidichte

Teilmenge $T_S \subset M_S$ von Vektoren x, so daß für die zu $x \in T_S$ gehörenden $e_1(x), \ldots, e_k(x)$ in dem Gleichungssystem

$$\sum_{v=1}^{m} (\alpha_{iv} - e_i(x)\tilde{\alpha}_{iv})X_v = 0 \quad \text{für } 1 \leqslant i \leqslant k \tag{2}$$

stets die ersten r Variablen frei gewählt werden können (wobei $0 \leqslant r \leqslant m$ fest ist) und die anderen Variablen über rationale Funktionen

$$\bar{g}_v \in K(X_1, \ldots, X_r, Y_1, \ldots, Y_k)$$

berechnet werden können durch

$$X_v = \bar{g}_v(X_1, \ldots, X_r, e_1(x), \ldots, e_k(x)) \quad \text{für } 1 \leqslant v \leqslant m \tag{3}$$

mit $\bar{g}_v(X_1, \ldots, X_r, Y_1, \ldots, Y_k) = X_v$ für $v \leqslant r$; wobei der "Hauptnenner" der $\bar{g}_v$ gleich einem Polynom $\bar{g}_0(Y_1, \ldots, Y_k)$ mit $\bar{g}_0(e_1(x), \ldots, e_k(x)) \neq 0$ ist. Dabei ist für $x \in T_S$ insbesondere $(x_1, \ldots, x_m)$ eine Lösung des Gleichungssystems (2); und somit gilt auch (3), wenn wir $X_1, \ldots, X_m$ durch $x_1, \ldots, x_m$ ersetzen. Insbesondere ist $(x_1, \ldots, x_r, e_1(x), \ldots, e_k(x))$ ein Punkt der Varietät X im $\mathbb{C}^{r+k}$ mit

$$X = \bigcap_{i=1}^{k} \operatorname{Var}\left(\sum_{v=1}^{m} (\alpha_{iv} - Y_i\tilde{\alpha}_{iv})g_v(X_1, \ldots, X_r, Y_1, \ldots, Y_k) \right) \tag{4}$$

wobei $g_v := \bar{g}_0\bar{g}_v$ ist. Betrachte nun die Abbildung $g := (g_1, \ldots, g_m): X \to \mathbb{C}^m$. Für $x = (x_1, \ldots, x_m) \in T_S$ ist ja $A(x) := \mathbb{C}^r \times \{(e_1(x), \ldots, e_k(x))\}$ eine Teilmenge von X mit $g(A(x)) \supset \{\lambda x\}$ für eine gewisse Zahl $\lambda = \bar{g}_0(e_1(x), \ldots, e_k(x))$. Da $(R^*)^r$ zariskidicht in $\mathbb{C}^r$ ist, liegt $A(x) \cap (R^*)^{r+k}$ zariskidicht in $A(x)$ und damit auch $(\bigcup_{x \in T_S} A(x)) \cap (R^*)^{r+k}$ zariskidicht in $\bigcup_{x \in T_S} A(x)$. Ist dann $X_0 \subset X$ eine irreduzibele Komponente des Zariskiabschlußes von $\bigcup_{x \in T_S} A(x) \subset X$, so ist also $X_0 \cap (R^*)^{r+k}$ zariskidicht in X_0. Nach Lemma 1 gibt es nun eine Abbildung $h = (h_1, \ldots, h_r, \bar{h}_1, \ldots, \bar{h}_k)$: $(\mathbb{C}^*)^d \to X_0 \subset \mathbb{C}^{r+k}$, so daß jede Komponente $h_v, \bar{h}_v$ von h die Form $c_v t_1^{n_v} \cdots t_d^{n_{dv}}$ hat und so daß $h((\mathbb{C}^*)^d)$ zariskidicht in X_0 ist.

Da $\bigcup_{x \in T_S} g(A(x))$ ja $\bigcup_{x \in T_S} \{\bar{g}_0(e_1(x), \ldots, e_k(x))x\}$ enthielt und da mit $x \in T_S$ auch für jedes $q \in \mathbb{Q}^*$ schon $xq \in T_S$ und $e_i(x) = e_i(qx)$ für $1 \leqslant i \leqslant k$ ist, enthält der Zariskiabschluß von $\bigcup_{x \in T_S} g(A(x))$ schon den Zariskiabschluß von T_S und damit die Menge Y_0. Somit läßt sich unsere Menge X_0 so wählen, daß der Zariskiabschluß von $g(X_0)$ die Menge Y_0 enthielt. Also ist auch der Zariskiabschluß von $g(h((\mathbb{C}^*)^d))$ mindestens so groß wie Y_0. Insbesondere liegt dann $g(h((\mathbb{C}^*)^d))$ nicht in einer durch $0 \in \mathbb{C}^m$ gehende

Hyperebene des $\mathbb{C}^m$.

Deshalb gibt es eine Kurve G der Gestalt $G = \{(z^{m_1}, \ldots, z^{m_d}); z \in \mathbb{C}^*\}$ mit $m_i \in \mathbb{Z}$, so daß auch $g \circ h|_G$ nicht in einer durch $0 \in \mathbb{C}^m$ gehenden Hyperebene liegt [Dazu setze $E := \{(z_1, \ldots, z_d) \in \mathbb{C}^d;\ |z_v| = 1 \text{ für } 1 \leqslant v \leqslant d\}$. Da E in $(\mathbb{C}^*)^d$ zariskidicht liegt, ist $F := (g \circ h)(E) \subset \mathbb{C}^m$ nicht in einer durch $0 \in \mathbb{C}^m$ gehenden Hyperebene enthalten. Dann gibt es endlich viele Punkte $\bar{y}_1, \ldots, \bar{y}_n \in F$ mit dazugehörigen Umgebungen $U(\bar{y}_1), \ldots, U(\bar{y}_n)$, so daß für alle $y_u \in U(\bar{y}_u) \cap F$ stets die Menge $\{y_1, \ldots, y_n\}$ nicht in einer durch $0 \in \mathbb{C}^m$ gehenden Hyperebene enthalten ist. Sind dann $\bar{z}_1, \ldots, \bar{z}_n \in E$ irgendwelche Urbilder von $\bar{y}_1, \ldots, \bar{y}_n$ unter der Abbildung $g \circ h$, so gilt für gewisse Umgebungen $U(\bar{z}_u)$ von $\bar{z}_u$, daß für alle $z_u \in U(\bar{z}_u) \cap E$ stets die Menge $\{g \circ h(z_1), \ldots, g \circ h(z_n)\}$ nicht in einer durch $0 \in \mathbb{C}^m$ gehenden Hyperebene liegt. Insbesondere können wir für groß genug gewählte paarweise teilerfremde Zahlen $p_1, \ldots, p_d$ die $z_j \in U(\bar{z}_j) \cap E$ in der Form

$$z_j = (e^{2\pi i k_{1j}/p_1}, \ldots, e^{2\pi i k_{dj}/p_d})$$

für $1 \leqslant j \leqslant n$ mit gewissen $k_{1j}, \ldots, k_{dj} \in \mathbb{Z}$ wählen. Suche $k_j \in \mathbb{Z}$ mit $k_j \equiv k_{vj} \bmod p_v$ für $1 \leqslant v \leqslant d$. Wird dann $m_i := p_1 \cdots p_{i-1} p_{i+1} \cdots p_d$ gesetzt, so ist bei $z := z(j) := e^{2\pi i k_j/p_1 \cdots p_d}$ schon $(z^{m_1}, \ldots, z^{m_d}) = z_j$. Somit liegt für

$$G = \{(z^{m_1}, \ldots, z^{m_d}); z \in \mathbb{C}^*\}$$

das Bild $(g \circ h)(G)$ nicht in einer durch $0 \in \mathbb{C}^m$ gehenden Hyperebene]. Setze dann $f_v(z) := g_v(h(z^{m_1}, \ldots, z^{m_d}))$. Da h nach X abbildete, folgt mit (4)

$$\sum_{v=1}^{m} (\alpha_{vi} - \bar{h}_i(z^{m_1}, \ldots, z^{m_d})\tilde{\alpha}_{iv}) f_v(z) = 0 \tag{5}$$

für $1 \leqslant i \leqslant k$. Nun war ja $\bar{h}_i$ ein Monom; somit ist $\bar{h}_i(z^{m_1}, \ldots, z^{m_d})$ von der Form $c_i z^{q_i}$ mit $c_i \in \mathbb{C}$, $q_i \in \mathbb{Z}$. Also erhalten wir die Identität

$$\sum_{v=1}^{m} \alpha_{iv} f_v(z) = c_i z^{q_i} \sum_{v=1}^{m} \tilde{\alpha}_{iv} f_v(z) \tag{6}$$

für $1 \leqslant i \leqslant k$. Dabei sind die $f_1(z), \ldots, f_m(z)$ rationale Funktionen von z (wobei der Nenner nur aus Potenzen von z bestehen kann). Bezeichnet $\operatorname{ord}_0 f$ die Null-bzw. Polstellenordnung von f im 0-Punkt, so sei $s := \min_{1 \leqslant v \leqslant m} \operatorname{ord}_0 f_v$. Dann ist $\bar{f}_v(z) := f_v(z) z^{-s}$ im Nullpunkt holomorph und nicht für alle $v \leqslant m$ dort gleich 0. Wir ordnen die Indizes $i \leqslant k$ jetzt so um, daß $\Sigma_{v=1}^m \alpha_{iv} \bar{f}_v(0) \neq 0$ für $i > (g-1)$ und $\Sigma_{v=1}^m \tilde{\alpha}_{iv} \bar{f}_v(0) \neq 0$ für $i > 2(g-1)$ ist (dies geht wegen der Rangvoraussetzung in Lemma 2).

Dann hat für $i > 2(g-1)$ sowohl $\Sigma_{v=1}^{m} \alpha_{iv}\overline{f}_v(z)$ als auch $\Sigma_{v=1}^{m} \tilde{\alpha}_{iv}\overline{f}_v(z)$ keine Null-oder Polstelle im Nullpunkt. Aus Gleichung (5) ergibt sich dann, daß für diese i jetzt q_i gleich 0 ist. Da es wegen $\frac{1}{2}(k+1) \geqslant g$ solche i überhaupt gibt, gibt es also Indizes i mit

$$\sum_{v=1}^{m} \alpha_{iv} f_v(z) = c_i \sum_{v=1}^{m} \tilde{\alpha}_{iv} f_v(z). \tag{7}$$

Da $\{(f_1(z), \ldots, f_m(z));\ z \in \mathbb{C}^*\}$ nicht in einer durch $0 \in \mathbb{C}^m$ gehenden Hyperebene lag, muß $\alpha_{iv} = e_i \tilde{\alpha}_{iv}$ für $1 \leqslant v \leqslant m$ und für $i > 2(g-1)$ sein. Da die Vektoren $(\alpha_i, \tilde{\alpha}_i)$ untereinander alle konjugiert sind, gibt es auch $c \in \mathbb{C}$, so daß $\alpha_1 = c\tilde{\alpha}_1$ ist. Dann folgt aus (1), daß schon $c = e(x)$ eine S-Einheit ist. Jetzt ist die Behauptung trivial, da wir für die gesuchte lineare Abbildung f einfach die Identität nehmen können.

Fall 2. Jede irreduzibele Komponente Y_0 von $\bar{M}_S$ liegt in einer Hyperebene der Form $\mathrm{Var}(\beta_1 X_1 + \cdots + \beta_m X_m)$.

Nach Umnumerierung der $x_1, \ldots, x_m$ haben wir also für $x \in M_S \cap Y_0$ eine Gleichung der Form $x_1 = \gamma_2 x_2 + \cdots + \gamma_m x_m$ mit $\gamma_v \in \mathbb{C}$. Indem wir eine Vektorraumbasis $\{w_j\}_{j \in I}$ von $\mathbb{C}$ über $\mathbb{Q}$ betrachten mit $w_1 := 1$, folgt aus der eindeutigen Darstellung $\gamma_v = \Sigma_{j \in I} \gamma_{vj} w_j$ die Gleichung

$$x_1 = \gamma_{21} x_2 + \cdots + \gamma_{m1} x_m$$

mit $\gamma_{v1} \in \mathbb{Q}$. Somit sind o.B.d.A. die $\gamma_v \in \mathbb{Q}$. Aux $\mathscr{D}_S(\Sigma_{v=1}^{m} \alpha_{1v} x_v) = \mathscr{D}_S(\Sigma_{v=1}^{m} \tilde{\alpha}_{1v} x_v)$ folgt dann für $x \in M_S \cap Y_0$

$$\mathscr{D}_S\left(\sum_{v=2}^{m} (\alpha_{1v} + \gamma_v \alpha_{11}) x_v\right) = \mathscr{D}_S\left(\sum_{v=2}^{m} (\tilde{\alpha}_{1v} + \gamma_v \tilde{\alpha}_{11}) x_v\right) \tag{8}$$

Der Vektor $\alpha_1^* := (\alpha_{12} + \gamma_2 \alpha_{11}, \ldots, \alpha_{1m} + \gamma_m \alpha_{11})$ und der entsprechend definierte Vektor $\tilde{\alpha}_1^*$ erfüllen jetzt die Voraussetzungen von Lemma 2, nur daß m durch $(m-1)$ ersetzt wird (wäre nämlich Rang $(\alpha_i^*)_{1 \leqslant i \leqslant g} < m-1$, so wäre Rang $(\alpha_i^*, \alpha_{i1})_{1 \leqslant i \leqslant g} < m$ und damit auch Rang $(\alpha_i)_{1 \leqslant i \leqslant g} \leqslant m$. Außerdem sind wegen $\gamma_v \in \mathbb{Q}$ die Vektoren $(\alpha_i^*, \tilde{\alpha}_i^*)$ für $1 \leqslant i \leqslant k$ untereinander konjugiert.) Somit gibt es nach Induktionsvoraussetzung eine über $\mathbb{Q}$ definierte endliche Familie $f_u^* = (f_{u2}^*, \ldots, f_{um}^*)$ mit

$$\sum_{v=2}^{m} \alpha_{1v}^* f_{uv}^* = c_u \sum_{v=2}^{m} \tilde{\alpha}_{1v}^* f_{uv}^* \tag{9}$$

für alle u mit $c_u \in R^*$ und mit

$$\pi(M_S \cap Y_0) \subset \bigcup_{u=1}^{<\infty} f_u^*(\mathbb{Q}^{m-1}) \tag{10}$$

wobei $\pi\colon \mathbb{Q}^m \to \mathbb{Q}^{m-1}$ die Projektion auf die letzten $(m-1)$ Koordinaten ist. Wird dann $f_{u1}(z_1,\ldots,z_m) := \Sigma_{v=2}^m \gamma_v f_{uv}^*(z_2,\ldots,z_m)$ und $f_{uv}(z_1,\ldots,z_m) := f_{uv}^*(z_2,\ldots,z_m)$ für $2 \leqslant v \leqslant m$ gesetzt, so ergibt sich aus (8) bzw. (9)

$$\sum_{v=1}^m \alpha_{1v} f_{uv} = c_u \sum_{v=1}^m \tilde{\alpha}_{1v} f_{uv} \tag{11}$$

$$M_S \cap Y_0 \subset \bigcup_{u=1}^{<\infty} f_u(\mathbb{Q}^m) \tag{12}$$

Da es nur endlich viele irreduzibele Komponenten Y_0 gab, sind wir fertig (die Inklusion $M_S \supset \bigcup_{u=1}^{<\infty} f_u(\mathbb{Q}^m)$ ist wegen (10) und $c_u \in R^*$ trivial).

Unter Benutzung von Lemma 2 beweisen wir folgenden Satz (der den "3-Werte-Satz" aus [3] mehrdimensional verallgemeinert für den Fall, daß die in [3] auftauchenden Zahlen untereinander konjugiert sind):

SATZ 3. *Gegeben seien zwei Vektoren* $\alpha_1 = (\alpha_{11},\ldots,\alpha_{1m}) \in K^m$ *und* $\tilde{\alpha}_1 := (\tilde{\alpha}_{11},\ldots,\tilde{\alpha}_{1\tilde{m}}) \in K^{\tilde{m}}$. *Bezeichne wieder mit* $(\alpha_i, \tilde{\alpha}_i) \in K^{m+\tilde{m}}$ *für* $1 \leqslant i \leqslant k$ *die zu* $(\alpha_1, \tilde{\alpha}_1)$ *konjugierten Vektoren. Für eine feste Zahl* g mit $\mathrm{Max}(m,\tilde{m}) \leqslant g \leqslant \frac{1}{3}(k+2)$ *sei für jede g-elementige Teilmenge* $\{i_1,\ldots,i_g\} \subset \{1,\ldots,k\}$ *stets Rang* $\{\alpha_{i_1},\ldots,\alpha_{i_g}\} = m$ *und Rang* $\{\tilde{\alpha}_{i_1},\ldots,\tilde{\alpha}_{i_g}\} = \tilde{m}$. *Betrachte für eine feste natürliche Zahl c die Menge*

$$\begin{aligned} M_{S,c} := \Big\{ & (x_1,\ldots,x_m,\tilde{x}_1,\ldots,\tilde{x}_{\tilde{m}}) \in \mathbb{Q}^{m+\tilde{m}}; \\ & \times c(x_1,\ldots,x_m,\tilde{x}_1,\ldots,\tilde{x}_{\tilde{m}}) \in \mathbb{Z}^{m+\tilde{m}}, \\ & \times \mathrm{ggT}(cx_1,\ldots,cx_m) \leqslant c^2,\ \mathrm{ggT}(c\tilde{x}_1,\ldots,c\tilde{x}_{\tilde{m}}) \leqslant c^2 \\ & \times \mathscr{D}_S\Big(\sum_{v=1}^m \alpha_{1v}x_v\Big) = \mathscr{D}_S\Big(\sum_{v=1}^{\tilde{m}} \tilde{\alpha}_{1v}\tilde{x}_v\Big)\Big\} \end{aligned}$$

Es gibt dann (bei o.B.d.A. $m \geqslant \tilde{m}$*) endlich viele über* $\mathbb{Q}$ *definierte lineare Abbildungen* $(f_u, \tilde{f}_u)\colon \mathbb{Q}^m \to \mathbb{Q}^{m+\tilde{m}}$, *so daß* $\dim_{\mathbb{Q}} f_u(\mathbb{Q}^m) = \dim_{\mathbb{Q}} \tilde{f}_u(\mathbb{Q}^m)$ *und*

$$M_{S,c} \subset \bigcup_{u=1}^{<\infty} (f_u, \tilde{f}_u)(\mathbb{Q}^m)$$

ist, und so daß für gewisse $c_u \in R^*$ *die Identitäten*

$$\sum_{v=1}^{m} \alpha_{1v} f_{uv}(t) = c_u \sum_{v=1}^{\tilde{m}} \tilde{\alpha}_{1v} \tilde{f}_{uv}(t)$$

für alle u und alle $t \in \mathbb{Q}^m$ *gelten.*

Beweis. Der Beweis geschieht angelehnt an den Beweis von Lemma 2 durch Induktion nach $(m + \tilde{m})$ und Fallunterscheidung. Der Induktionsanfang $m + \tilde{m} = 2$ ist wieder trivial.

Fall 1. Es gibt eine irreduzibele Komponente Y_0 des Zariskiabschlußes von $\mathbb{Q}M_{S,c} \subset \mathbb{C}^{m+\tilde{m}}$, die nicht in einer Hyperebene der Form

$$\mathrm{Var}(\beta_1 X_1 + \cdots + \beta_m X_m)$$

und nicht in einer Hyperebene $\mathrm{Var}(\tilde{\beta}_1 \tilde{X}_1 + \cdots \tilde{\beta}_{\tilde{m}} \tilde{X}_{\tilde{m}})$ enthalten ist.

Entsprechend (1) im Beweis von Lemma 2 gilt für $(x, \tilde{x}) \in Y_0 \cap \mathbb{Q}M_{S,c}$

$$\sum_{u=1}^{m} \alpha_{iv} x_v - \sum_{v=1}^{\tilde{m}} e_i(x, \tilde{x}) \tilde{\alpha}_{iv} \tilde{x}_v = 0 \quad \text{für } 1 \leqslant i \leqslant k \tag{1'}$$

mit S-Einheiten $e_i(x, \tilde{x}) \in K$. Entsprechend (2) wählen wir so eine zariskidichte Teilmenge $T_{S,c} \subset \mathbb{Q}M_{S,c}$, so daß für $(x, \tilde{x}) \in T_{S,c}$ in dem Gleichungssystem

$$\sum_{v=1}^{m} \alpha_{iv} X_v - \sum_{v=1}^{\tilde{m}} e_i(x, \tilde{x}) \tilde{\alpha}_{iv} \tilde{X}_v = 0 \quad \text{für } 1 \leqslant i \leqslant k \tag{2'}$$

die ersten r Variabeln $X_1, \ldots, X_r$ und die ersten $\tilde{r}$ Variabeln $\tilde{X}_1, \ldots, \tilde{X}_{\tilde{r}}$ frei gewählt werden können und entsprechend (3) die anderen Variabeln berechnet werden können durch

$$X_v = \bar{g}_v(X_1, \ldots, X_r, \tilde{X}_1, \ldots, \tilde{X}_{\tilde{r}}, e_1(x, \tilde{x}), \ldots, e_k(x, \tilde{x})) \quad \text{fur } 1 \leqslant v \leqslant m \tag{3'}$$

bzw. durch eine analoge Gleichung $\tilde{X}_v = \bar{g}_v$ für $1 \leqslant v \leqslant \tilde{m}$. Ist dann $\bar{g}_0$ der "Hauptnenner" aller $\bar{g}_v, \tilde{\bar{g}}_v$ und $g_v := \bar{g}_0 \tilde{\bar{g}}_v$, $\tilde{g}_v := \bar{g}_0 \tilde{\bar{g}}_v$, so betrachten wir entsprechend (4) die Varietät X im $\mathbb{C}^{r+\tilde{r}+k}$ mit

$$X = \bigcap_{i=1}^{k} \mathrm{Var}\Bigg(\sum_{v=1}^{m} \alpha_{iv} g_v(X_1, \ldots, X_r, \tilde{X}_1, \ldots, \tilde{X}_{\tilde{r}}, Y_1, \ldots, Y_k) - \sum_{v=1}^{\tilde{m}} \tilde{\alpha}_{iv} \tilde{g}_v(X_1, \ldots, X_r, \tilde{X}_1, \ldots, \tilde{X}_{\tilde{r}}, Y_1, \ldots, Y_k) \Bigg)$$

Entsprechend dem nach (4) Gesagten betrachten wir für $(x, \tilde{x}) \in T_{S,c}$ die

Menge $A(x, \tilde{x}) := \mathbb{C}^r \times \mathbb{C}^{\tilde{r}} \times \{(e_1(x, \tilde{x}), \ldots, e_k(x, \tilde{x})\} \subset X$. Dann wählen wir wieder eine irreduzibele Komponente $X_0 \subset X$ des Zariskiabschlußes von $\bigcup_{(x,\tilde{x}) \in T_{S,e}} A(x, \tilde{x})$ und bekommen eine Abbildung

$$h := (h_1, \ldots, h_r, \tilde{h}_1, \ldots, \tilde{h}_{\tilde{r}}, \bar{h}_1, \ldots, \bar{h}_k) : (\mathbb{C}^*)^d \to X_0 \subset \mathbb{C}^{r+\tilde{r}+k},$$

so daß $h((\mathbb{C}^*)^d)$ zariskidicht in X_0 liegt. Wie in Lemma 2 ist bei geeigneter Wahl von X_0 bei $g := (g_1, \ldots, g_m, \tilde{g}_1, \ldots, \tilde{g}_m)$ dann der Zariskiabschluß von $g(h((\mathbb{C}^*)^d))$ mindestens so groß wie Y_0 und damit nicht in einer Hyperebene $\mathrm{Var}(\beta_1 X_1 + \cdots + \beta_m X_m)$ oder in $\mathrm{Var}(\tilde{\beta}_1 \tilde{X}_1 + \cdots + \tilde{\beta}_m \tilde{X}_m)$ enthalten.

Indem wir $g \circ h$ auf eine geeignete Kurve G der Gestalt $\{(z^{m_1}, \ldots, z^{m_d}); z \in \mathbb{C}^*\}$ einschränken, ist dann bei $f_v(z) := g_v(h(z^{m_1}, \ldots, z^{m_d}))$ und entsprechend definierten $\tilde{f}_v(z)$ sowohl das Bild $(f_1, \ldots, f_m)(\mathbb{C}^*)$ als auch das Bild $(\tilde{f}_1, \ldots, \tilde{f}_{\tilde{m}})(\mathbb{C}^*)$ nicht in einer durch 0 gehenden Hyperebene das $\mathbb{C}^m$ bzw. $\mathbb{C}^{\tilde{m}}$ enhthalten. Außerdem folgt entsprechend (5)

$$\sum_{v=1}^{m} \alpha_{iv} f_v(z) = c_i z^{q_i} \sum_{v=1}^{\tilde{m}} \tilde{f}_v(z) \tag{5'}$$

Wie nach (5) definiere $s := \min_{1 \leqslant v \leqslant m} \mathrm{ord}_0 f_v$ und $\tilde{s} := \min_{1 \leqslant v \leqslant \tilde{m}} \mathrm{ord}_0 \tilde{f}_v$. Es folgt genauso wie in (7), daß für $i > 2(g-1)$ stets

$$\sum_{v=1}^{m} \alpha_{iv} f_v(z) z^{-s} = c_i \sum_{v=1}^{\tilde{m}} \tilde{\alpha}_{iv} \tilde{f}_v(z) z^{-\tilde{s}} \tag{7'}$$

gilt. Da $k > 2(g-1) + g$ ist und da ja g Vektoren α_i einen Rang m haben, kann über (7') die Funktion f_u berechnet werden:

$$f_u(z) = \sum_{v=1}^{\tilde{m}} \tilde{\varepsilon}_{vu} \tilde{f}_v(z) z^{s-\tilde{s}} \quad \text{für } 1 \leqslant u \leqslant m \tag{8'}$$

mit gewissen $\tilde{\varepsilon}_{vu} \in \mathbb{C}$. Genauso folgt

$$\tilde{f}_u(z) z^{s-\tilde{s}} = \sum_{v=1}^{m} \varepsilon_{vu} f_v(z) \quad \text{fur } 1 \leqslant u \leqslant \tilde{m} \tag{9'}$$

Wäre jetzt $\tilde{m} < m$, so müßten schon für $1 \leqslant u \leqslant m$ die rechten Seiten von (8') linear abhängig sein; somit wäre für gewisses $(\beta_1, \ldots, \beta_m) \in \mathbb{C}^m - \{0\}$ schon $\Sigma_{u=1}^{m} \beta_u f_u(z) = 0$, im Widerspruch zu dem vor (5') Gesagten.

Somit ist Fall (1) nur bei $m = \tilde{m}$ möglich. Wir behaupten, daß jetzt Fall (1) auf einer der beiden folgenden Unterfälle führt:

Fall (1a). Für jede invertierbare Matrix $(\varepsilon_{v\mu}) \in Gl_m(\mathbb{C})$ ist

$$Y_0 \not\subset \bigcap_{\nu,\mu \leqslant m} \mathrm{Var}\left(\tilde{X}_\nu \sum_{v=1}^{m} \varepsilon_{v\mu} X_v - \tilde{X}_\mu \sum_{v=1}^{m} \varepsilon_{v\nu} X_v\right)$$

Fall (1b). Es gibt endlich viele zariskidünne Teilmengen $Y_{0\lambda} \subset Y_0$ der Form $Y_{0\lambda} := Y_0 \cap \mathrm{Var}(\beta_{1\lambda} X_1 + \cdots + \beta_{m\lambda} X_m)$ für $1 \leqslant \lambda \leqslant s_1 - 1$ und endlich viele Teilmengen $Y_{0\lambda} \subset Y_0$ für $s_1 \leqslant \lambda \leqslant s_2$ mit $Y_0 = \bigcup_{\lambda=1}^{s_2} Y_{0\lambda}$, so daß rationale Zahlen $q_\lambda, \tilde{q}_\lambda \in \mathbb{Q}^*$ und invertierbare Matrizen $(\varepsilon_{v\mu}) \in Gl_m(\mathbb{Q})$, $(\tilde{\varepsilon}_{v\mu}) \in Gl_m(\mathbb{Q})$ existieren mit

$$q_\lambda x_\mu = \sum_{v=1}^{m} \tilde{\varepsilon}_{v\mu} \tilde{x}_v$$

$$\tilde{q}_\lambda \tilde{x}_\mu = \sum_{v=1}^{m} \varepsilon_{v\mu} x_v$$

für $1 \leqslant \mu \leqslant m$, $s_1 \leqslant \lambda \leqslant s_2$ und für alle $(x, \tilde{x}) \in Y_{0\lambda} \cap M_{S,c}$.

Beweis der Zwischenbehauptung. Wenn Fall (1a) nicht auftritt, ist also für ein gewisses $(\varepsilon_{v\mu}) \in Gl_m(\mathbb{C})$ schon für alle $v, \mu \leqslant m$.

$$Y_0 \subset \mathrm{Var}\left(\tilde{X}_\nu \sum_{v=1}^{m} \varepsilon_{v\mu} X_v - \tilde{X}_\mu \sum_{v=1}^{m} \varepsilon_{v\nu} X_v\right) \subset \mathbb{C}^{m+\tilde{m}} \tag{I}$$

Seien dann $Y_{0\lambda}$ für $1 \leqslant \lambda < s_1 - 2$ die nach der Obervoraussetzung von Fall (1) zariskidünnen Mengen $\mathrm{Var}(\Sigma_{v=1}^{m} \varepsilon_{v\mu} X_v)$ und $\mathrm{Var}\, \tilde{X}_\mu$ für $1 \leqslant \mu \leqslant m$. Falls für die oben definierte Menge $\mathbb{Q}M_{S,c} \subset \mathbb{C}^{m+\tilde{m}}$ jetzt

$$(x, \tilde{x}) \in (Y_0 \cap \mathbb{Q}M_{S,c}) - \bigcup_{\lambda=1}^{s_1-2} Y_{0\lambda}$$

ist, muß es dann wegen (I) Zahlen $\tilde{q}(x) \in \mathbb{C}^*$ (die unabhängig von $\mu \leqslant m$ sind) mit

$$\tilde{q}(x)\tilde{x}_\mu = \sum_{v=1}^{m} \varepsilon_{v\mu} x_v \quad \text{für } 1 \leqslant \mu \leqslant m \tag{II}$$

geben. Setze $(\tilde{\varepsilon}_{v\mu}) := (\varepsilon_{v\mu})^{-1}$. Aus (II) ergibt sich dann bei $q(x) := 1/\tilde{q}(x) \in \mathbb{C}^*$

$$q(x)x_\mu = \sum_{v=1}^{m} \tilde{\varepsilon}_{v\mu} \tilde{x}_v \quad \text{für } 1 \leqslant \mu \leqslant m \tag{III}$$

Indem $\tilde{q}(x)$ eventuell noch mit einer von x unabhängigen Konstanten multipliziert wird, ist mindestens ein $\varepsilon_{v\mu} \in \mathbb{Q}^*$. O.B.d.A. $\varepsilon_{11} \in \mathbb{Q}^*$. Indem wir

eine Basis von $\mathbb{C}$ über $\mathbb{Q}$ betrachten, folgt entsprechend dem Beweis von Fall (2) in Lemma 2 aus (II) eine gleichlautende Relation mit neuen $\tilde{q}(x) \in \mathbb{Q}$ und neuen $\varepsilon_{v\mu} \in \mathbb{Q}$, wobei $\varepsilon_{11} \in \mathbb{Q}^*$ ist. Auf Grund der Obervoraussetzung von Fall (1) ist die Teilmenge $Y_{0,s_1-1} := Y_0 \cap \mathrm{Var}(\Sigma_{v=1}^m \varepsilon_{v1} X_v)$ (mit den neuen ε_{v1}) zariskidünn, und außerhalb ist stets $\tilde{q}(x) \neq 0$. Somit gilt eine Relation (II) mit $\tilde{q}(x) \in \mathbb{Q}^*$ und $\varepsilon_{v\mu} \in \mathbb{Q}$ für alle

$$(x, \tilde{x}) \in (Y_0 \cap \mathbb{Q}M_{S,c}) - \bigcup_{\lambda=1}^{s_1-1} Y_{0\lambda}.$$

Aus (II) folgt nun, da der Nenner aller $\varepsilon_{v\mu} x_v$ unterhalb einer festen Schranke liegt und da der ggT aller Zähler von $\tilde{x}_\mu$ ebenfalls beschränkt ist für $(x, \tilde{x}) \in M_{S,c}$, daß auch der Nenner aller $\tilde{q}(x)$ unterhalb einer festen Schranke liegt. Aus (II) folgt aber auch für die neuen $\varepsilon_{v\mu}$, daß die Matrix $(\varepsilon_{v\mu})$ invertierbar sein muß [sonst lägen nämlich die $\tilde{q}(x)\tilde{x}$ in einer festen Hyperebene der Form $\mathrm{Var}(\beta_1 \tilde{X}_1 + \cdots + \beta_m \tilde{X}_m)$; da $q(x)$ für eine zariskidichte Teilmenge von Y_0 ungleich 0 ist, läge dann doch Y_0 in einer solchen Hyperebene]. Wir erhalten also aus (II) bei $(\tilde{\varepsilon}_{v\mu}) := (\varepsilon_{v\mu})^{-1}$ und bei $q(x) := 1/\tilde{q}(x) \in \mathbb{Q}^*$ eine Gleichung (III) mit neuen rationalen $q(x)$, $\tilde{\varepsilon}_{v\mu}$. Genauso wie eben folgt, daß der Nenner aller $q(x)$ beschränkt ist. Damit ist auch der Zähler aller $\tilde{q}(x)$ beschränkt, und somit kommen für $\tilde{q}(x)$ und damit für $q(x)$ nur endlich viele Werte in Frage. Werden diese mit $\tilde{q}_\lambda$ bzw. q_λ für $s_1 \leqslant \lambda \leqslant s_2$ bezeichnet, so haben wir die Behauptung des Falles (1b).

Wir haben also gezeigt, daß unter der Obervoraussetzung von Fall (1) nur die Unterfälle (1a) und (1b) auftreten können. Wir zeigen nun, daß in Wirklichkeit Fall (1a) gar nicht möglich ist. Dies geschieht dadurch, daß wie am Anfang unseres Beweises von Satz 3 die Gleichungen (1′)–(4′) gezeigt werden. Die Abbildung h, die nach (4′) konstruiert wird, hat jetzt die Eigenschaft, daß $g(h((\mathbb{C}^*)^d))$ nicht in einer Varietät der Form

$$Z_0 := \mathrm{Var}(\beta_1 X_1 + \cdots + \beta_m X_m) \cup \mathrm{Var}(\tilde{\beta}_1 \tilde{X}_1 + \cdots + \tilde{\beta}_m \tilde{X}_m)$$
$$\cup \bigcup_{v,\mu \leqslant m} \mathrm{Var}\left(\tilde{X}_v \sum_{v=1}^m \varepsilon_{v_\mu} X_v - \tilde{X}_\mu \sum_{v=1}^m \varepsilon_{vv} X_v \right)$$

Dann schränken wir wie vor (5′) die Abbildung $g \circ h$ auf geeignete Kurven G der Gestalt $\{(z^{m_1}, \ldots, z^{m_d}),\ z \in \mathbb{C}^*\}$ ein und bekommen wie vor (5′) eine Abbildung $(f_1, \ldots, f_m, \tilde{f}_1, \ldots, \tilde{f}_m) : \mathbb{C}^* \to \mathbb{C}^{m+\tilde{m}}$, so daß deren Bild nicht in einer Varietät der Form Z_0 liegt. Weiter erhalten wir wie oben die Gleichung (9′). Da $(f_1, \ldots, f_m)(\mathbb{C}^*)$ nicht in einer durch 0 gehenden Hyperebene liegt, folgt aus (9′), daß die Matrix $(\varepsilon_{v\mu})$ invertierbar sein muß. Außerdem folgt aus (9′), daß für $v, \mu \leqslant m$ schon

$$\tilde{f}_\nu(z) \sum_{\nu=1}^{m} \varepsilon_{\nu\mu} f_\nu(z) = \tilde{f}_\mu(z) \sum_{\nu=1}^{m} \varepsilon_{\nu\nu} f_\nu(z)$$

ist. Damit liegt $(f_1, \ldots, f_m, \tilde{f}_1, \ldots, \tilde{f}_m)(\mathbb{C}^*)$ doch in einer Hyperfläche der Form Z_0. Somit kann Fall (1a) nicht auftreten.

Fall (1*b*). Ist in der Terminologie des Falles (1b) jetzt $(x, \tilde{x}) \in M_{S,c} \cap Y_{0\lambda}$ für $1 \leqslant \lambda < s_1$, so haben wir eine nichttriviale Beziehung $\Sigma_{\nu=1}^{m} \beta_{\nu\lambda} x_\nu = 0$. Entsprechend dem Beweis von Fall (2) in Lemma 2 können wir dann o.B.d.A. jetzt $\beta_{\nu\lambda} \in \mathbb{Q}$ annehmen und dann o.B.d.A. das x_1 linear durch $x_2, \ldots, x_m$ ausdrücken. Dann erhalten wir mit Induktion unsere Behauptung für die $(x, \tilde{x}) \in M_{S,c} \cap Y_{0\lambda}$ mit $\lambda < s_1$ (hierbei muß natürlich für die $(x, \tilde{x}) \in M_{S,c} \cap Y_{0\lambda}$ beachtet werden, daß beim Induktionsbeweis alle Voraussetzungen erhalten bleiben. So ist z.B. bei $\Sigma_{\nu=1}^{m} \beta_{\nu\lambda} x_\nu = 0$ mit $\beta_{1\lambda} \neq 0$ auch schon der ggT der Zähler von $x_2, \ldots, x_m$ beschränkt, falls der ggT der Zähler von $x_1, \ldots, x_m$ beschränkt war).

Ist aber $(x, \tilde{x}) \in M_{S,c} \cap Y_{0\lambda}$ für $s_1 \leqslant \lambda \leqslant s_2$, so können wir die $\tilde{x}_u$ durch die x_ν gemäß $\tilde{x}_\mu = \Sigma_{\nu=1}^{m} (\varepsilon_{\nu\mu}/\tilde{q}_\lambda) x_\nu$ ausdrücken. Wird jetzt

$$\tilde{\alpha}_{1\nu\lambda} := \sum_{\mu=1}^{m} \tilde{\alpha}_{1\mu} \varepsilon_{\nu\mu}/\tilde{q}_\lambda$$

gesetzt, so ist also

$$\sum_{\mu=1}^{m} \tilde{\alpha}_{1\mu} \tilde{x}_\mu = \sum_{\nu=1}^{m} \tilde{\alpha}_{1\nu\lambda} x_\nu$$

Auf Grund unserer vorausgesetzten Divisorengleichung gilt also

$$\mathscr{D}_S\left(\sum_{\nu=1}^{m} \tilde{\alpha}_{1\nu\lambda} x_\nu\right) = \mathscr{D}_S\left(\sum_{\nu=1}^{m} \alpha_{1\nu} x_\nu\right)$$

für $(x, \tilde{x}) \in M_{S,c} \cap Y_{0\lambda}$. Jetzt können wir Lemma 2 anwenden (wieder sind alle Voraussetzungen erfüllt) und erhalten, daß alle betrachteten $(x_1, \ldots, x_m)$ im Bild endlich vieler linearer Abbildungen $f: \mathbb{Q}^m \to \mathbb{Q}^m$ liegen, für die die Divisorengleichungen in eine Identität übergehen. Durch Rücktransformation

$$\tilde{x}_\mu = \sum_{\nu=1}^{m} (\varepsilon_{\nu\mu}/\tilde{q}_\lambda) x_\nu$$

liegen dann auch alle $(x, \tilde{x}) \in M_{S,c} \cap Y_{0\lambda}$ für $s_1 \leqslant \lambda \leqslant s_2$ im Bild endlich vieler linearer Abbildungen $(f, \tilde{f})$: $\mathbb{Q}^m \to \mathbb{Q}^{2m}$, so daß auch dafür die Div-

isorengleichung in eine Identität

$$\sum_{v=1}^{m} \alpha_{1v} f_v(t) = c_1 \sum_{v=1}^{m} \tilde{\alpha}_{1v} \tilde{f}_v(t)$$

mit $c_1 \in R^*$ übergeht. Damit ist Fall (1) abgeschlossen.

Fall (2). Jede irreduzibele Komponente Y_0 des Zariskiabschlußes von $M_{S,c}$ liegt in einer Hyperebene der Form $\mathrm{Var}(\Sigma_{v=A}^{m} \beta_v X_v)$ oder der Form $\mathrm{Var}(\Sigma_{v=1}^{\tilde{m}} \tilde{\beta}_v \tilde{X}_v)$.

Dieser Fall wird analog zum Fall (2) im Beweis von Lemma 2 durch Ersetzen einer Variablen auf einen niederdimensionalen Fall zurückgeführt. Damit ist Satz 3 bewiesen.

FOLGERUNG 4. Gegeben sei ein Vektor $\alpha_1 = (\alpha_{11}, \ldots, \alpha_{1m}) \in K^m$, so daß es mindestens $k := 3m - 2$ viele Konjugierte α_i von α_1 gibt und so daß je m Vektoren $\alpha_{i_1}, \ldots, \alpha_{i_m}$ linear unabhängig sind.

Es gibt dann endlich viele über $\mathbb{Q}$ definierte Hyperebenen $H_u \subset \mathbb{Q}^m$, so daß für $(x_1, \ldots, x_m) \in \mathbb{Z}^m - \bigcup_u^{<\infty} H_u$ mit $\mathrm{ggT}(x_1, \ldots, x_m) = 1$ und für $(\tilde{x}_1, \ldots, \tilde{x}_m) \in \mathbb{Z}$ mit $\mathrm{ggT}(\tilde{x}_1, \ldots, \tilde{x}_m) = 1$ aus

$$\mathscr{D}_S\left(\sum_{v=1}^{m} \alpha_{1v} x_v\right) = \mathscr{D}_S\left(\sum_{v=1}^{m} \alpha_{1v} \tilde{x}_v\right)$$

schon $(x_1, \ldots, x_m) = \pm(\tilde{x}_1, \ldots, \tilde{x}_m)$ folgt

Beweis. Zunächst liefert die Divisorengleichung nach Satz 3 eine endliche Menge von über $\mathbb{Q}$ definierten Funktionentupeln $f_u = (f_{u1}, \ldots, f_{um})$, $\tilde{f}_u = (\tilde{f}_{u1}, \ldots, \tilde{f}_{um})$ und Einheiten $c_u \in R^*$ mit

$$\sum_{v=1}^{m} \alpha_{1v} f_{uv}(t) = c_u \sum_{v=1}^{m} \alpha_{1v} \tilde{f}_{uv}(t) \tag{1}$$

Falls $\dim f_u(\mathbb{Q}^m) < m$ ist, so definiere $H_u := f_u(\mathbb{Q}^m)$ und wir haben damit die geforderten Ausnahmehyperebenen. Falls $f_u: \mathbb{Q}^m \to \mathbb{Q}^m$ ein Automorphismus ist, ist auch $\tilde{f}_u$ ein Automorphismus (dies folgt leicht aus (1), indem man darauf alle Konjugierten anwendet und benutzt, daß $\alpha_1, \ldots, \alpha_m$ nach Voraussetzung linear unabhängig sind.) Somit folgt aus (1), daß es zu jedem $s \leqslant m$ Zahlen $q_{uvs} := f_{uv}(\tilde{f}_u^{-1}((\delta_{s1}, \ldots, \delta_{sm})) \in \mathbb{Q}$ (δ = Kroneckersymbol) gibt mit

$$\sum_{v=1}^{m} \alpha_{1v} q_{uvs} = c_u \alpha_{1s} \tag{2}$$

Aus nachfolgendem Lemma 5 ergibt sich, daß $c_u \in \mathbb{Q}$ ist. Nun folgt aus (1) durch Konjugieren für $1 \leqslant i \leqslant k$

$$\sum_{v=1}^{m} \alpha_{iv}(f_{uv}(t) - c_u \tilde{f}_{uv}(t)) = 0 \tag{3}$$

Wegen der linearen Unabhängigkeit von $\alpha_1, \ldots, \alpha_m$ ist dann $f_u(t) = c_u \tilde{f}_u(t)$. Da die Lösungstupel $x = (x_1, \ldots, x_m) \in \mathbb{Z}^m$ bzw. $\tilde{x} \in \mathbb{Z}^m$ ganzzahlig mit insgesamt teilerfremden Koordinaten sein sollen, ergibt sich $c_u = \pm 1$ und damit die Behauptung.

LEMMA 5. *Sei* $\alpha_1 := (\alpha_{11}, \ldots, \alpha_{1m}) \in K^m$ *ein Vektor, so daß es mindestens* $k := 2m - 1$ *viele Konjugierte* α_i *von* α_1 *gibt und so daß je m Vektoren* $\alpha_{i_1}, \ldots, \alpha_{i_m}$ *linear unabhängig sind. Es sei c eine feste algebraische Zahl mit*

$$c\alpha_{1s} \in (\alpha_{11}, \ldots, \alpha_{1m})\mathbb{Q} \quad \textit{für } 1 \leqslant s \leqslant m$$

(*wobei* $(\alpha_{11}, \ldots, \alpha_{1m})\mathbb{Q}$ *der von* $\alpha_{11}, \ldots, \alpha_{1m}$ *erzeugte* $\mathbb{Q}$*-Vektorraum bedeutet*). *Dann ist* $c \in \mathbb{Q}$.

Beweis. OBdA ist $\alpha_{11} = 1$: Denn es folgt

$$c(\alpha_{1s}/\alpha_{11}) \in (1, \alpha_{12}/\alpha_{11}, \ldots, \alpha_{1m}/\alpha_{11})\mathbb{Q} \quad \textit{für } 1 \leqslant s \leqslant m,$$

und bei dem Vektorsystem $\tilde{\alpha}_i := (1, \alpha_{i2}/\alpha_{i1}, \ldots, \alpha_{im}/\alpha_{i1})$ sind wieder je m Vektoren linear unabhängig, und wir haben auch wieder mindestens $k := 2m - 1$ viele verschiedene Konjugierte $\tilde{\alpha}_i$ (denn wäre $\tilde{\alpha}_i = \tilde{\alpha}_j$ für $i \neq j$, so wären α_i und α_j linear abhängig, im Widerspruch zur Voraussetzung.) Also ist oBdA $\alpha_{11} = 1$.

Aus der Voraussetzung folgt leicht $c^q \alpha_{1s} \in (\alpha_{11}, \ldots, \alpha_{1m})\mathbb{Q}$ für alle $s \leqslant m$ und für alle q und damit $\mathbb{Q}(c)\alpha_{1s} c\,(\alpha_{11}, \ldots, \alpha_{1m})\mathbb{Q}$ für alle $s \leqslant m$. Falls $c \notin \mathbb{Q}$ wäre, enthält $\mathbb{Q}(c)$ ein Element d, so daß alle Potenzen d^p für $p \in \mathbb{N}$ modulo $\mathbb{Q}^*$ verschieden sind. Wir haben für alle $q \in \mathbb{N}$ ja $d^q \alpha_{11} \in (\alpha_{11}, \ldots, \alpha_{1m})\mathbb{Q}$. Indem wir Ganzheitsbasen betrachten, erhalten wir nach eventueller Vergrößerung der Bewertungsmenge S schon S-ganze Elemente

$$\beta_q := (\beta_{1q}, \ldots, \beta_{mq}) \in \mathbb{Q}^m$$

mit

$$d^q = \sum_{v=1}^{m} \alpha_{1v}\beta_{vq}$$

OBdA sind alle Konjugierten d_i von d schon S-Einheiten. Wird jetzt

$$P_i(X) := 1 + \sum_{v=2}^{m} (\alpha_{iv} - \alpha_{1v})X_v \quad \text{für } 2 \leqslant i \leqslant k$$

gesetzt, so haben wir also für $2 \leqslant i \leqslant k$ wegen $\alpha_{i1} = \alpha_{11}$ bei $\beta'_q := (\beta_{2q}, \ldots, \beta_{mq})$

$$P_i(\beta'_q/d^q) = (d_i/d)^q \tag{1}$$

stets S-Einheiten vor uns. Jetzt sieht man wegen der linearen Unabhängigkeit von $\alpha_{i_1}, \ldots, \alpha_{i_m}$, daß die Varietäten $\operatorname{Var} P_2, \ldots, \operatorname{Var} P_k \subset \mathbb{C}^{m-1}$ in allgemeiner Lage im Sinne von [4] sind (d.h. je m verschiedene Varietäten haben einen leeren Durchschnitt, und je $(m-1)$ verschiedene Polynome $P_{i_2}, \ldots, P_{i_m}$ liefern eine eigentliche Abbildung $(P_{i_2}, \ldots, P_{i_m}): \mathbb{C}^{m-1} \to \mathbb{C}^{m-1}$, wobei "eigentlich" bedeutet, daß Urbilder von kompakten Mengen wieder kompakt sind. Zu dieser Aussage vergl. [4], Beweis 1.9) Nach [4] 1.7 ist dann wegen $k - 1 \geqslant 2(m-1)$ die Menge der S-ganzen Punkte $x = (x_2, \ldots, x_m)$, für die $P_i(x)$ eine S-Einheit für $2 \leqslant i \leqslant k$ ist, eine endliche Menge [hier ging wieder der Einheitensatz [1] ein]. Mit (1) ist also die Menge der β'_q/d^q endlich und damit wieder wegen (1) auch die Menge der $(d_i/d_1)^q$ bei laufendem q endlich. Es folgt, daß für eine Zahl $p_i > 0$ schon $(d_i/d_1)^{p_i} = 1$ ist. Somit unterscheiden sich alle Konjugierten von d um höchstens eine Einheitswurzel, im Widerspruch zur Wahl von d.

Mittels Satz 3 können wir nun auch den Satz 3 aus [3] auf höhere Dimensionen ausdehnen:

SATZ 6. *Gegeben seien zwei Vektoren* $\alpha_1 = (\alpha_{11}, \ldots, \alpha_{1m}) \in K^m$ *und* $\tilde{\alpha}_1 = (\tilde{\alpha}_{11}, \ldots, \tilde{\alpha}_{1\tilde{m}}) \in K^{\tilde{m}}$, so daß $K := \mathbb{Q}(\alpha_{11}, \ldots, \alpha_{1m}) = \mathbb{Q}(\tilde{\alpha}_{11}, \ldots, \tilde{\alpha}_{1\tilde{m}})$ *galoisch ist. Weiter mögen* α_1, $\tilde{\alpha}_1$ *die Voraussetzungen von Satz* 3 *erfüllen. N bezeichne die Norm im Körper K.*

Es gibt dann zu fester Zahl $a \in \mathbb{Z}$ *bei o.B.d.A.* $m \geqslant \tilde{m}$ *endlich viele lineare Abbildungen* $(f_u, \tilde{f}_u): \mathbb{Q}^m \to \mathbb{Q}^{m+\tilde{m}}$ *für* $1 \leqslant u \leqslant r$, *so daß* $\dim_{\mathbb{Q}} f_u(\mathbb{Q}^m) = \dim_{\mathbb{Q}} \tilde{f}_u(\mathbb{Q}_m) \geqslant 2$ *ist und so daß für fast alle Primzahlen p jede Lösung* $(x_1, \ldots, x_m) \in \mathbb{Z}^m$, $(\tilde{x}_1, \ldots, \tilde{x}_{\tilde{m}}) \in \mathbb{Z}^{\tilde{m}}$ *von*

$$N(\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m) = ap = N(\tilde{\alpha}_{11}\tilde{x}_1 + \cdots + \tilde{\alpha}_{1\tilde{m}}\tilde{x}_{\tilde{m}}) \tag{*}$$

sich schreiben läßt als

$$(x, \tilde{x}) = (f_u(t), \tilde{f}_u(t))$$

für geeignetes $u \leqslant r$ *und* $t \in \mathbb{Q}^m$, *und außerdem für alle* $u \leqslant r$ *und für alle* $t \in \mathbb{Q}^m$ *die Identität*

$$N(\alpha_{11}f_{u1}(t) + \cdots + \alpha_{1m}f_{um}(t)) = N(\tilde{\alpha}_{11}\tilde{f}_{u1}(t) + \cdots + \tilde{\alpha}_{1\tilde{m}}\tilde{f}_{u\tilde{m}}(t))$$

gilt.

Beweis. Sei G die Galoisgruppe von K über $\mathbb{Q}$. Wähle S so groß, daß a eine S-Einheit ist. Wieder sei R der Ring der S-ganzen Zahlen von K. Die Primzahl p zerfällt in R in höchstens $d := \operatorname{ord} G$ viele Primideale $\wp_1, \ldots, \wp_d$. Es gibt nun ein $\sigma(x) \in G$ mit $\alpha_1 x = \alpha_{11}x_1 + \cdots + \alpha_{1m}x_m \in \sigma(x)(\wp_1)$. Entsprechend gilt für ein $\tilde{\sigma}(\tilde{x}) \in G$ auch $\tilde{\alpha}_1\tilde{x} \in \tilde{\sigma}(\tilde{x})(\wp_1)$. Da $N(\alpha_1 x) = N(\tilde{\alpha}_1\tilde{x})$ bis auf den Faktor a prim ist, ist $\alpha_1 xR = \sigma(x)(\wp_1)$ und $\tilde{\alpha}_1\tilde{x}R = \tilde{\sigma}(\tilde{x})(\wp_1)$. Damit folgt nun bei $\tilde{\tilde{\alpha}}_{1v} := \sigma(x)\tilde{\sigma}^{-1}(\tilde{x})(\tilde{\alpha}_{1v})$ für $1 \leqslant v \leqslant \tilde{m}$

$$(\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m)R = (\tilde{\tilde{\alpha}}_{11}\tilde{x}_1 + \cdots + \tilde{\tilde{\alpha}}_{1\tilde{m}}\tilde{x}_{\tilde{m}})R \tag{1}$$

Für $\alpha_1 := (\alpha_{11}, \ldots, \alpha_{1m})$ und $\tilde{\tilde{\alpha}}_1 := (\tilde{\tilde{\alpha}}_{11}, \ldots, \tilde{\tilde{\alpha}}_{1\tilde{m}})$ sind nun die Voraussetzungen von Satz 3 erfüllt. Da weiter $\operatorname{ggT}(x_1, \ldots, x_m)$ und $\operatorname{ggT}(\tilde{x}_1, \ldots, \tilde{x}_{\tilde{m}})$ beschränkt ist und da nach Zerlegung aller betrachteten $(x, \tilde{x}) \in \mathbb{Z}^{m+\tilde{m}}$ in höchstens d viele Teilmengen $T_1, \ldots, T_d$ schon $\tilde{\tilde{\alpha}}_1$ von $(x, \tilde{x}) \in T_j$ unabhängig ist, folgt aus (1) mittels Satz 3, daß die Lösungstupel $(x, \tilde{x})$ in endlich vielen Bildräumen $\bigcup_{u=1}^{r}(f_u, \tilde{f}_u)(\mathbb{Q}^m)$ liegen, wobei $(f_u, \tilde{f}_u)$ eine lineare Abbildung von $\mathbb{Q}^m$ nach $\mathbb{Q}^{m+\tilde{m}}$ bedeutet mit $\dim_{\mathbb{Q}} f_u(\mathbb{Q}^m) = \dim_{\mathbb{Q}} \tilde{f}_u(\mathbb{Q}^m)$, und die Identität

$$\sum_{v=1}^{m} \alpha_{1v}f_{uv}(t) = c_u \sum_{v=1}^{\tilde{m}} \tilde{\alpha}_{1v}\tilde{f}_{uv}(t) \tag{2}$$

gilt mit geeignetem $c_u \in K$. Werden in (2) alle Konjugierte betrachtet, so folgt durch Produktbildung

$$N(\alpha_{11}f_{u1}(t) + \cdots + \alpha_{1m}f_{um}(t)) = \left[\prod_{i=1}^{k} (c_u)^{(i)}\right] N(\tilde{\alpha}_{1m}\tilde{f}_{u1}(t) + \cdots + \tilde{\alpha}_{1\tilde{m}}\tilde{f}_{u\tilde{m}}(t))$$

Da für gewisses $t \in \mathbb{Q}^m$ und für gewisses $u \leqslant r$ schon $(x, \tilde{x}) = (f_u(t), \tilde{f}_u(t))$ war, folgt daraus für alle wirklich auftauchend u, daß $\prod_{i=1}^{k} (c_u)^{(i)} = 1$ ist. Da die endlich vielen $(f_u, \tilde{f}_u)$ mit $\dim f_u(\mathbb{Q}^m) = \dim \tilde{f}_u(\mathbb{Q}^m) \leqslant 1$ auf nur endlich viele Primzahlen führen, ist Satz 6 gezeigt.

Im Spezialfall $m = 2$, $\alpha_{11} = \tilde{\alpha}_{11} = 1$, $\alpha_{12} = \tilde{\alpha}_{12} = \alpha$ ergibt sich aus Satz 6 das schon in [3] Satz 3 bewiesene Ergebnis, daß für fast alle Primzahlen p die Gleichung $N(x_1 + \alpha x_2)$ bis auf triviale Fälle höchstens eine Lösung hat, falls $[\mathbb{Q}(\alpha): \mathbb{Q}] \geqslant 4$ ist. Im Spezialfall $m = 2$, $\alpha_{11} = 1$, $\alpha_{12} = \alpha$ und $\tilde{\alpha}_{11} = 1$, $\tilde{\alpha}_{12} = \tilde{\alpha}$ ergibt sich eine leichte Verschärfung von Satz 6 aus [3]. Allerdings war in den beiden Sätzen aus [3] die Voraussetzung "galoisch" unterschlagen worden.

In der Regel wird die Gleichung (∗) in Satz 6 für fast alle Primzahlen p *keine* Lösung haben, wenn $k := [K: \mathbb{Q}] \geqslant 2(m + \tilde{m})$ ist: Denn da

$$N(\alpha_1 X_1 + \cdots + \alpha_m X_m)$$

ein homogenes Polynom von Grad k ist, würden wir bei der Existenz von linearen Abbildungen $(f_u, \tilde{f}_u)$ gemäß der Aussage von Satz 6 wegen $\dim f_u(\mathbb{Q}^m) = \dim \tilde{f}_u(\mathbb{Q}^m) \geqslant 2$ schon $(k + 1)$ viele Gleichungen mit den $2(m + \tilde{m})$ vielen Unbekannten $a_v, b_v, \tilde{a}_v, \tilde{b}_v$ haben [denn dann existierte insbesondere ein $(f, \tilde{f})$ der Form $f(t) = (a_1 t_1 + b_1 t_2, \ldots, a_m t_1 + b_m t_2)$, $\tilde{f}(t) = (\tilde{a}_1 t_1 + \tilde{b}_1 t_2, \ldots, \tilde{a}_{\tilde{m}} t_1 + \tilde{b}_{\tilde{m}} t_2)$, das in der Normgleichung eine Identität hervorruft]. Wegen $k + 1 > 2(m + \tilde{m})$ wird dieses Gleichungssystem in der Regel nicht lösbar sein. Analog wird die Normgleichung

$$N(\alpha_1 x_1 + \cdots + \alpha_m x_m) = p = N(\alpha_1 \tilde{x}_1 + \cdots + \alpha_m \tilde{x}_m)$$

für fast alle Primzahlen p in der Regel nur durch

$$(x_1, \ldots, x_m) = \pm(\tilde{x}_1, \ldots, \tilde{x}_m)$$

lösbar sein. Im vorgegebenen konkreten Fall ist allerdings die Feststellung, ob ein solcher "Regelfall' vorliegt, sehr mühsam, da wir nachrechnen müssen, ob $k + 1$ viele Gleichungen mit $4m \leqslant k$ vielen Unbekannten eine Lösung haben. Einfacher zu verifizieren sind im konkreten Fall die Voraussetzungen der nachstehenden Folgerung:

FOLGERUNG 7. Sei α eine algebraische Zahl mit $\mathbb{Q}(\alpha) \supset \mathbb{Q}$ galoisch vom Grad k. Ist $m \leqslant \frac{1}{3}(k + 2)$ und hat keine Konjugierte $\tilde{\alpha}$ von α mit $\tilde{\alpha} \neq \alpha$ [bzw. mit $\tilde{\alpha} \neq \alpha, \alpha^{-1}$] die Form

$$\tilde{\alpha} = \frac{q_{21}\alpha^0 + \cdots + q_{2m}\alpha^{m-1}}{q_{11}\alpha^0 + \cdots + q_{1m}\alpha^{m-1}}$$

mit $q_{ij} \in \mathbb{Q}$, so gibt es endlich viele Hyperebenen $H_1, \ldots, H_r \subset \mathbb{Q}^m$, so daß für alle Primzahlen p die Gleichung

$$N(x_1\alpha^0 + \cdots + x_m\alpha^{m-1}) = p = N(\tilde{x}_1\alpha^0 + \cdots + x_m\alpha^{m-1})$$

mit $x_1, \ldots, x_m, \tilde{x}_1, \ldots, \tilde{x}_m \in \mathbb{Z}$ und $(x_1, \ldots, x_m) \notin \bigcup_{u=1}^{r} H_u$ schon $(x_1, \ldots, x_m) = \pm(\tilde{x}_1, \ldots, \tilde{x}_m)$ impliziert [bzw. schon $(x_1, \ldots, x_m) = \pm(\tilde{x}_1, \ldots, \tilde{x}_m)$ oder $(x_1, \ldots, x_m) = \pm(\tilde{x}_m, \ldots, \tilde{x}_1)$ impliziert].

Beweis. Andernfalls gäbe es nach Satz 6 schon Vektorraumisomorphismen $f: \mathbb{Q}^m \to \mathbb{Q}^m$, $\tilde{f}: \mathbb{Q}^m \to \mathbb{Q}^m$ mit $f \neq \pm\tilde{f}$, so daß für eine gewisse Kon-

jugierte $\tilde{\alpha}$ von α und für eine gewisse Einheit $c \in \mathcal{O}(\mathbb{Q}(\alpha))$

$$\sum_{v=1}^{m} \alpha^{v-1} f_v(t) = c \sum_{v=1}^{m} (\tilde{\alpha})^{v-1} \tilde{f}_v(t)$$

wäre. Wende auf diese Gleichung m viele Galoisautomorphismen an, wobei α bzw. $\tilde{\alpha}$ bzw. c auf $\alpha^{(u)}$ bzw. $\tilde{\alpha}^{(u)}$ bzw. $c^{(u)}$ für $1 \leqslant u \leqslant m$ abgebildet werden möge. Setze dann

$$A := ((\alpha^{v-1})^{(u)})_{1 \leqslant v,u \leqslant m}$$
$$\tilde{A} := ((c\tilde{\alpha}^{v-1})^{(u)})_{1 \leqslant v,u \leqslant m}$$

Es folgt

$$\begin{pmatrix} f_1(t) \\ \vdots \\ f_m(t) \end{pmatrix} = A^{-1}\tilde{A} \begin{pmatrix} \tilde{f}_1(t) \\ \vdots \\ \tilde{f}_m(t) \end{pmatrix}$$

Es ergibt sich, daß $A^{-1}\tilde{A} \in M_{m,m}(\mathbb{Q})$ ist (denn indem wir wieder eine Vektorraumbasis der normalen Hülle K von $\mathbb{Q}(\alpha)$ betrachten, ergäbe sich andernfalls eine nichttriviale Relation zwischen $\tilde{f}_1(t), \ldots, \tilde{f}_m(t)$ im Widerspruch dazu, daß $\tilde{f}$ ein Isomorphismus ist). Sei also $A^{-1}\tilde{A} = (q_{ij})_{1 \leqslant i,j \leqslant m}$. Es folgt $\tilde{A} = A(q_{ij})$ und damit bei Betrachtung der ersten Zeile

$$c((\tilde{\alpha})^0, \ldots, (\tilde{\alpha})^{m-1}) = \left(\sum_{v=1}^{m} \alpha^{v-1} q_{1v}, \ldots, \sum_{v=1}^{m} \alpha^{v-1} q_{mv} \right)$$

Speziell folgt

$$\tilde{\alpha} = \left(\sum_{v=1}^{m} \alpha^{v-1} q_{2v} \right) \Big/ \left(\sum_{v=1}^{m} \alpha^{v-1} q_{1v} \right),$$

woraus auf Grund unserer Voraussetzung schon $\tilde{\alpha} = \alpha$ folgt. Analog ergibt sich

$$\alpha = \left(\sum_{v=1}^{m} \alpha^{v-1} q_{uv} \right) \Big/ \left(\sum_{v=1}^{m} \alpha^{v-1} q_{u-1,v} \right)$$

für $2 \leqslant u \leqslant m$. Daraus folgt wegen $[\mathbb{Q}(\alpha): \mathbb{Q}] > m$, daß $q_{u1} = 0$, $q_{u-1,m} = 0$ und $q_{u-1,v-1} = q_{u,v}$ für $2 \leqslant u, v \leqslant m$ ist. Damit ist (q_{uv}) ein Vielfaches der Einheitsmatrix. Somit ist $(f_1(t), \ldots, f_m(t))$ ein festes Vielfaches von $(\tilde{f}_1(t), \ldots, \tilde{f}_m(t))$. Damit ist auch $(x_1, \ldots, x_m)$ ein Vielfaches von $(\tilde{x}_1, \ldots, \tilde{x}_m)$ und somit

$(x_1,\ldots,x_m) = \pm(\tilde{x}_1,\ldots,\tilde{x}_m)$.—Die zweite Aussage im Fall, daß α^{-1} zu α konjugiert ist, wird ähnlich bewiesen.

Übrigens ist leicht zu sehen, daß im Fall "α^{-1} zu α konjugiert" schon $N(x_1\alpha^0 + \cdots + x_m\alpha^{m-1}) = N(x_m\alpha^0 + \cdots + x_1\alpha^{m-1})$ ist, so daß also wirklich der Fall $(\tilde{x}_1,\ldots,\tilde{x}_m) = (x_m,\ldots,x_1)$ auftauchen kann. Ganz konkrete Beispiele zu Folgerung 7 lassen sich leicht angeben.

Wir können natürlich auch Abschätzungen der Normformengleichung $N(\alpha_1x_1 + \cdots + \alpha_mx_m) = h$ mit beliebigem h geben (wobei jetzt im Gegensatz zu [3] die Primfaktoren von h mit ihren Vielfachheiten gezählt werden müssen, da jetzt die verschiedenen Faktoren von $N(\alpha_1x_1 + \cdots + \alpha_mx_m)$ trotz ggT $(x_1,\ldots,x_m) = 1$ nicht mehr teilerfremd zu sein brauchen).

SATZ 8. *Sei $\alpha_1 = (\alpha_{11},\ldots,\alpha_{1m})$ ein Vektor mit algebraischen Koordinaten, so daß je m Konjugierte α_i von α_1 linear unabhängig sind und so daß es mindestens $3m-2$ viele Konjugierte gibt. N sei die Norm in $K' := \mathbb{Q}(\alpha_{11},\ldots,\alpha_{1m})$. Wieder sei S eine feste endliche Menge von Bewertungen von $\mathbb{Q}$. Es gibt dann endlich viele durch den Nullpunkt gehende Hyperebenen $H_u \subset \mathbb{Q}^m$, so daß für alle $h \in \mathbb{Z}$ die Divisorengleichung*

$$\mathscr{D}_S(N(\alpha_{11}x_1 + \cdots + \alpha_{1m}x_m)) = \mathscr{D}_S(h)$$

höchstens $2d^{t(h)}$ viele verschiedene Lösungen $(x_1,\ldots,x_m) \in \mathbb{Z}^m - \bigcup^{<\infty} H_u$ mit ggT $(x_1,\ldots,x_m) = 1$ *hat, wobei $t(h)$ die Anzahl der Primfaktoren von h bedeutet und $d := [K':\mathbb{Q}]$ ist.*

Beweis. Sei K die normale Hülle von K'. Es gibt eine endliche Menge von Bewertungen von K (die wieder mit S bezeichnet wird), die alle Fortsetzungen der vorausgesetzten Bewertungen von $\mathbb{Q}$ enthält und so daß alle $\alpha_{11},\ldots,\alpha_{1m}$ schon S-ganze Elemente von K sind. Mit G bezeichnen wir wieder die Galoisgruppe von $K \supset \mathbb{Q}$, und U sei die Untergruppe, die K' festläßt. Ist R der Ring der S-ganzen Zahlen von K, so sei $h = \prod_{j=1}^{\tilde{t}} p_j^{m_j}$ mit verschiedenen Primzahlen $p_j \in \mathbb{Z}$, die oBdA keine S-Einheiten sind.

Zu jedem $j \leqslant \tilde{t}$ fixiere Primideale $\wp_{1j},\ldots,\wp_{dj} \subset R$ über p_j, so daß für $r \neq s \leqslant d$ und $\sigma_r, \sigma_s \in U$ stets $\sigma_r(\wp_{rj}) \neq \sigma_s(\wp_{sj})$ ist und so daß jedes Primideal $\wp_j \subset R$ über p_j schon die Form $\wp_j = \sigma(\wp_{rj})$ für ein $\sigma \in U$, $r \leqslant d$ hat (falls es weniger als d viele solcher Primideale $\wp_{rj}$ geben sollte, erhalten wir im folgenden noch bessere Abschätzungen). Setze bei einem festen $x \in \mathbb{Z}^m$ mit $\mathscr{D}_S(N(\alpha_1(x)) = \mathscr{D}_S(h)$ jetzt $n_{rj}(x) := \mathrm{ord}_{\wp_{rj}}(\alpha_1x)$ für $r \leqslant d$, $j \leqslant \tilde{t}$. Da für $\sigma \in U$ ja $\sigma(\alpha_1x) = \alpha_1x$ ist, ist auch $n_{rj}(x) = \mathrm{ord}_{\sigma(\wp_{rj})}(\alpha_1x)$ für $\sigma \in U$. Weil die $\sigma(\wp_{rj})$ mit laufendem $\sigma \in U$, $r \leqslant d$ und $j \leqslant \tilde{t}$ alle Primoberideale von α_1x durchlaufen, haben wir

$$\alpha_1xR = \prod_{1 \leqslant j \leqslant \tilde{t}} \prod_{1 \leqslant r \leqslant d} \prod_{\sigma \in U}{}' \sigma(\wp_{rj})^{n_{rj}(x)} \tag{1}$$

(dabei soll der Strich hinter dem letzten Produktzeichen andeuten, daß bei $\sigma_1(\wp_{rj}) = \sigma_2(\wp_{rj}) = \cdots$ der entsprechende Faktor insgesamt nur einmal genommen werden soll). Es folgt für feste Galoisautomorphismen $\tau_1, \ldots, \tau_d \in G$, die auf K' eingeschränkt paarweise verschieden sind, daß

$$\begin{aligned} N(\alpha_1 x)R &= \prod_{i=1}^{d} \tau_i(\alpha_1 x)R \\ &= \prod_{1 \leqslant j \leqslant \tilde{t}} \prod_{1 \leqslant r \leqslant d} \left[\prod_{i=1}^{d} \prod_{\sigma \in U}{}' \tau_i \sigma(\wp_{rj}) \right]^{n_{rj}(x)} \\ &= \prod_{1 \leqslant j \leqslant \tilde{t}} \prod_{1 \leqslant r \leqslant d} (p_j)^{v_{rj} n_{rj}(x)} R \end{aligned} \tag{2}$$

ist, wobei v_{rj} von x unabhängige natürliche Zahlen sind [die letzte Gleichung von (2) sieht man so: Sei $U_{rj} \subset U$ die Untergruppe aller $\sigma \in U$ mit $\sigma(\wp_{rj}) = \wp_{rj}$ und G_{rj} die entsprechende Untergruppe von G. Dann ist

$$\begin{aligned} \left[\prod_{i=1}^{d} \prod_{\sigma \in U}{}' \tau_i \sigma(\wp_{rj}) \right]^{\operatorname{ord} U_{rj}} &= \prod_{i=1}^{d} \prod_{\sigma \in U} \tau_i \sigma(\wp_{rj}) \\ &= \prod_{\sigma \in G} \sigma(\wp_{rj}) = \left[\prod_{\sigma \in G}{}' \sigma(\wp_{rj}) \right]^{\operatorname{ord} G_{rj}} \end{aligned}$$

wobei wieder der Strich bedeutet, daß gleiche Faktoren $\sigma(\wp_{rj})$ nur einmal im Produkt auftauchen. Da $\Pi'_{\sigma \in G} \sigma(\wp_{rj})$ gleich $p_j R$ ist, falls p_j größer als die Diskriminante D von K ist (was oBdA der Fall ist, da wir alle Primzahlen $\leqslant D$ als S-Einheiten auffassen können), ist $\prod_{\sigma \in G} \sigma(\wp_{rj}) = p_j^{\operatorname{ord} G_{rj}} R$ und deshalb

$$\prod_{i=1}^{d} \prod_{\sigma \in U}{}' \tau_i \sigma(\wp_{rj}) = p_j^{\operatorname{ord} G_{rj} / \operatorname{ord} U_{rj}} R =: p_j^{v_{rj}} R \Big].$$

Wegen $N(\alpha_1 x)R = \Pi_{j=1}^{\tilde{t}} p_j^{m_j} R$ folgt aus (2),

$$\sum_{1 \leqslant r \leqslant d} v_{rj} n_{rj}(x) = m_j \quad \text{für alle } j \leqslant \tilde{t} \tag{3}$$

ist. Bei festem j, v_{rj}, d und m_j gibt es höchstens d^{m_j} viele Tupel $(n_{1j}(x), \ldots, n_{dj}(x)) \in \mathbb{N}_0^d$ mit (3) [denn man sieht leicht durch Induktion nach m_j, daß man für m_j viele gleichartige Objekte höchstens d^{m_j} viele Möglichkeiten hat, einen gewissen Teil dieser Objekte in $d-1$ viele Schubfächer zu verteilen. Dann sei die Anzahl der in dem r. Schubfach liegenden Objekte gleich $n_{rj}(x) \in \mathbb{N}_0$ für $1 \leqslant r \leqslant d-1$. Da wir wegen (3), also wegen $\Sigma_{r=1}^{d-1} n_{rj}(x) \leqslant m_j$ in unserem Fall höchstens m_j viele Objekte haben, und da das letzte Element $n_{dj}(x)$ eindeutig durch die

anderen Elemente $n_{1j}(x), \ldots, n_{d-1,j}(x)$ nach (3) gegeben ist, ergibt sich diese Zwischenbehauptung].

Somit gibt es $\prod_{j=1}^{\tilde{t}} d^{m_j} = d^{t(h)}$ viele Möglichkeiten für die Tupel $(n_{rj}(x))_{\substack{1 \leqslant r \leqslant d \\ 1 \leqslant j \leqslant \tilde{t}}}$. Nach (1) gibt es also für das Ideal $\alpha_1 xR$ höchstens $d^{t(h)}$ viele Möglichkeiten. Falls wir nun mehr als $2d^{t(h)}$ viele Lösungen der Gleichung $\mathscr{D}_S(N(\alpha_1 x)) = \mathscr{D}_S(h)$ hätten, hätten wir zwei Lösungen $x, \tilde{x} \in \mathbb{Z}^m$ mit $x \neq \pm\tilde{x}$ (von daher kommt der Faktor "2" im Ausdruck $2d^{t(h)}$) und mit $\alpha_1 xR = \alpha_1 \tilde{x}R$. Nach Folgerung 4 ergibt sich für x außerhalb endlich vieler Hyperebenen, daß doch $x = \pm\tilde{x}$ wäre. Damit haben wir einen Widerspruch.

Falls $\mathbb{Q}(\alpha_{11}, \ldots, \alpha_{1m}) \supset \mathbb{Q}$ galoisch ist, erhalten wir analog zu Satz 6/7 oft bessere Abschätzungen. Dabei heißen zwei Lösungen $x = (x_1, \ldots, x_m)$ und $\tilde{x} = (\tilde{x}_1, \ldots, \tilde{x}_m)$ von $N(\alpha x) = h = N(\alpha\tilde{x})$ "äquivalent", wenn es eine Matrix $M \in GL_m(\mathbb{Q})$ gibt, so daß $\tilde{x} = Mx$ ist und für Variable $X = (X_1, \ldots, X_m)$ auch $N(\alpha X) = N(\alpha(MX))$ ist:

SATZ 9. *Sei $\alpha = (\alpha_1, \ldots, \alpha_m)$ ein Vektor, so daß $\mathbb{Q}(\alpha_1, \ldots, \alpha_m) \supset \mathbb{Q}$ galoisch vom Grad d ist, je m Konjugierte von α linear unabhängig sind und so daß es mindestens $3m - 2$ viele verschiedene Konjugierte von α gibt. N sei die Norm in $K := \mathbb{Q}(\alpha_1, \ldots, \alpha_m)$. Es gibt dann endlich viele durch den Nullpunkt gehende Hyperebenen $H_u \subset \mathbb{Q}^m$, so daß für alle $h \in \mathbb{Z}$ die Gleichung*

$$N(\alpha_1 x_1 + \cdots + \alpha_m x_m) = h$$

höchstens d^{t-1} viele untereinander nicht äquivalente Lösungen $(x_1, \ldots, x_m) \in \mathbb{Z}^m - \bigcup^{<\infty} H_u$ mit $\mathrm{ggT}(x_1, \ldots, x_m) = 1$ hat, wobei $t = t(h)$ die Anzahl der Primfaktoren von h bedeutet.

Beweis. Sei $h = \prod_{j=1}^{t} p_j$ die Primfaktorzerlegung in $\mathbb{Z}$. Dann ist (wobei wir im ganzen Beweis die Terminologie des Beweises von Satz 6 übernehmen)

$$hR = \prod_{j=1}^{t} \left[\prod_{i=1}^{d} \wp_{ij} \right]$$

Sei dann $N(\alpha x) = h = N(\alpha\tilde{x})$. Da das Produkt über alle Konjugierten von αx gleich h ist, ist dann $(\alpha x)R$ ein Teilprodukt $\prod_{j=1}^{t} \wp_{i(j),j}$. Weiter kann wie im Beweis von Satz 6 Ziffer (1) erreicht werden, daß für eine gewisse Konjugierte $\tilde{\tilde{\alpha}}$ von α in dieser Teilproduktdarstellung für $(\alpha x)R$ und für $(\tilde{\tilde{\alpha}}\tilde{x})R$ beidesmal dieselben Primfaktoren $\wp_{i(1),1}$ (die zu p_1 gehören) vorkommen. Wenn wir mehr als d^{t-1} viele untereinander nicht äquivalente Lösungen von $N(\alpha x) = h$ hätten, müssten dann nach dem Schubfachprinzip für zwei nicht äquivalente Lösungen $x, \tilde{x}$ schon $(\alpha x)R = (\tilde{\tilde{\alpha}}\tilde{x})R$ sein. Auf die Divisorengleichung $\mathscr{D}(\alpha x) = \mathscr{D}(\tilde{\tilde{\alpha}}\tilde{x})$ wenden wir Satz 3 an: Die $f_u, \tilde{f}_u$ aus Satz 3 mit $\dim \tilde{f}_u(\mathbb{Q}^m) < m$ liefern die endlich vielen Hyperebenen $H_u \subset \mathbb{Q}^m$ unserer Aussage, und die $f_u, \tilde{f}_u$ mit

dim $f_u(\mathbb{Q}^m) = m = \dim \tilde{f}_u(\mathbb{Q}^m)$ liefern invertierbare lineare über $\mathbb{Q}$ definierte Abbildungen $M_u: \mathbb{Q}^m \to \mathbb{Q}^m$ mit $\tilde{x} = M_u x$ für ein u und $N(\alpha X) = N(\alpha(M_u X))$. Somit wären x und $\tilde{x}$ doch äquivalent.

Literatur

1. Evertse, J. H., On sums of S-units and linear recurrences, *Compos. Math.* 53 (1984), 225–244.
2. Langmann, K., Picard-Borel-Räume, *Math. Ann*, 284 (1989), 138–160.
3. Langmann, K., Eindeutigkeit der Lösungen der Gleichung $x^d + y^d = ap$, *Compos. Math.* 88 (1993), 25–38.
4. Langmann, K., Picardindex und ganzalgebraische Punkte, *Math. Ann.* 291 (1991), 663–690.
5. Schmidt, W. M., Norm form equations, *Annals of Math.* 96 (1972), 526–551.