

ÜBER SIMULTANE APPROXIMATION ALGEBRAISCHER ZAHLEN DURCH RATIONALE

VON

WOLFGANG M. SCHMIDT

University of Colorado, Boulder, Col., U.S.A.

1. Einleitung

1.1. Problemstellung. Ist ξ eine algebraische Irrationalzahl und $\varepsilon > 0$, so gibt es nach einem berühmten Satz von K. F. Roth [6] höchstens endlich viele rationale Zahlen p/q , so daß

$$\left| \xi - \frac{p}{q} \right| < |q|^{-2-\varepsilon}$$

ist. In diesem Satz darf die Konstante 2 in $|q|^{-2-\varepsilon}$ durch keine kleinere ersetzt werden.

Sind ξ_1, \dots, ξ_n algebraisch, aber $1, \xi_1, \dots, \xi_n$ linear unabhängig über dem rationalen Zahlkörper \mathbb{Q} , und ist $\varepsilon > 0$, so ist zu vermuten, daß es höchstens endlich viele $(n+1)$ -tupel ganzzahliger Zahlen $q > 0; p_1, \dots, p_n$ gibt, so daß

$$\left| \xi_j - \frac{p_j}{q} \right| < q^{-(1+1/n)-\varepsilon} \quad (j = 1, \dots, n)$$

gilt. Man kann leicht sehen, daß man in dieser Vermutung $1 + 1/n$ durch keine kleinere Konstante ersetzen darf.

Dual zum Problem der simultanen Approximation ist das Linearformenproblem. Macht man dieselben Voraussetzungen über ξ_1, \dots, ξ_n und ε wie vorhin, so ist zu vermuten, daß es höchstens endlich viele $(n+1)$ -tupel $q_1, \dots, q_n; p$ ganzzahliger Zahlen mit $q = \text{Max}(|q_1|, \dots, |q_n|) > 0$ gibt, so daß

$$|q_1 \xi_1 + \dots + q_n \xi_n - p| < q^{-n-\varepsilon}$$

erfüllt wird.

Leider können wir die angeführten Vermutungen, die übrigens nach dem Khintchine'schen Übertragungssatz [3] äquivalent sind, nicht beweisen. Wir werden hier Sätze

herleiten, die in die Richtung der Vermutungen weisen, wenngleich sie wesentlich schwächer sind als diese.

Andere Sätze aus diesem Problemkreis bewies Hasse [2].

1.2. Hauptresultate. Den Abstand einer reellen Zahl α zur nächsten ganzrationalen Zahl bezeichnen wir mit $\|\alpha\|$, die nächstkleinere ganze Zahl mit $[\alpha]$. Weiter bedeute

$$L(x) = \begin{cases} \log x, & \text{falls } x \geq e, \\ 1, & \text{falls } x < e. \end{cases}$$

Funktionen $L_1(x), L_2(x), \dots$ werden induktiv durch $L_1(x) = L(x)$ und $L_k(x) = L(L_{k-1}(x))$ definiert. Weiter sei $L_0(x) = x$.

Wir sagen von einer Menge Ω von natürlichen Zahlen, sie hat Eigenschaft E , falls Ω entweder endlich ist, oder falls die als wachsende Folge $q_1 < q_2 < \dots$ angeordneten Elemente von Ω für jedes k die Limesbeziehung

$$\limsup_{h \rightarrow \infty} L_k(q_{h+1})/L_k(q_h) = \infty$$

erfüllen.

SATZ 1. Die Zahlen ξ_1, ξ_2 seien algebraisch, und $1, \xi_1, \xi_2$ linear unabhängig über \mathbb{Q} . Sei $\varepsilon > 0$. Die Menge Ω aller natürlichen q , für die

$$\|q\xi_1\| \cdot \|q\xi_2\| q^{1+\varepsilon} < 1 \quad (1)$$

ist, hat Eigenschaft E .

FOLGERUNG. Seien $\xi_1, \xi_2, \varepsilon$ wie in Satz 1. Ω^* sei die Menge aller natürlichen q , zu denen es ganzrationale p_1, p_2 gibt, die

$$\left| \xi_1 - \frac{p_1}{q} \right| < q^{-3/2-\varepsilon}, \quad \left| \xi_2 - \frac{p_2}{q} \right| < q^{-3/2-\varepsilon}$$

erfüllen. Ω^* hat Eigenschaft E .

Diese Folgerung kommt der Vermutung über simultane Approximationen für $n=2$ nahe. Nach der Vermutung ist Ω^* endlich.

Bevor der Satz von Roth bewiesen war, hatte Schneider [7] für den Fall einer algebraischen Irrationalzahl ein ähnliches Ergebnis gezeigt.

Dual zu Satz 1 ist

SATZ 2. $\xi_1, \xi_2, \varepsilon$ seien wie in Satz 1. Die Menge \mathfrak{B} aller natürlichen q , zu denen es ganzrationale $q_1 \neq 0, q_2 \neq 0$ mit $q = \text{Max}(|q_1|, |q_2|)$ gibt, so daß

$$\|q_1\xi_1 + q_2\xi_2\| |q_1|^{1+\varepsilon} |q_2|^{1+\varepsilon} < 1 \quad (2)$$

gilt, hat Eigenschaft E .

FOLGERUNG. $\xi_1, \xi_2, \varepsilon$ seien wie in Satz 1. Sei \mathfrak{P}^* die Menge aller natürlichen q , zu denen es ganzrationale $q_1, q_2; p$ mit $q = \text{Max}(|q_1|, |q_2|)$ gibt, so daß

$$|q_1 \xi_1 + q_2 \xi_2 - p| < q^{-2-\varepsilon}$$

ist. Dann hat \mathfrak{P}^* Eigenschaft E.

1.3. Nebenresultate. Einige der zum Beweis der Hauptresultate benötigten Ergebnisse sind vielleicht für sich von gewissem Interesse.

In § 2.1 werden wir eine Eigenschaft F für Mengen von nichtnegativen reellen Zahlen definieren. Im Augenblick brauchen wir von dieser Eigenschaft nur zu wissen, daß jede Menge natürlicher Zahlen mit Eigenschaft F auch Eigenschaft E besitzt, und jede endliche Menge Eigenschaft F hat.

SATZ 3. Seien ξ_1, \dots, ξ_n algebraisch und $1, \xi_1, \dots, \xi_n$ linear unabhängig über \mathbf{Q} . Sei $\delta > 0$. Wir setzen $l = n + 1$.

Wir bilden die Menge \mathcal{M} aller positiven Zahlen Q , zu denen es n nichtnegative reelle Zahlen a_1, \dots, a_n mit

$$a_1 + a_2 + \dots + a_n \geq 1 + \delta \tag{3}$$

sowie eine Matrix

$$M = \begin{pmatrix} p_{11} & \dots & p_{1n} & p_{1l} \\ \vdots & & \vdots & \vdots \\ p_{n1} & \dots & p_{nn} & p_{nl} \end{pmatrix} \tag{4}$$

vom Rang n mit ganzrationalen Elementen gibt, so daß die Ungleichungen

$$|p_{ii} \xi_j - p_{ij}| \leq Q^{-a_j} \quad (1 \leq i \leq n; 1 \leq j \leq n), \tag{5}$$

$$|p_{ii}| \leq Q \quad (1 \leq i \leq n) \tag{6}$$

erfüllt sind.

\mathcal{M} hat Eigenschaft F .

Im Spezialfall $a_j = (1 + \delta)/n$ ($j = 1, \dots, n$) würde aus $p_{ii} = 0$ für $Q > 1$ wegen (5) folgen $p_{ij} = 0$ ($j = 1, \dots, n$), und die Matrix M könnte nicht Rang n besitzen. Somit gilt nun $p_{ii} \neq 0$ ($i = 1, \dots, n$), und (5) und (6) ergeben zusammen

$$\left| \xi_j - \frac{p_{ij}}{p_{ii}} \right| \leq |p_{ii}|^{-1-1/n-\delta/n} \quad (1 \leq i \leq n; 1 \leq j \leq n).$$

Man hat also n verschiedene simultane Approximationssysteme zu ξ_1, \dots, ξ_n (nämlich für $i = 1, \dots, n$), deren Nenner nach (6) alle dem Betrag nach höchstens gleich Q sind.

Für $n=2$ ist unsere Voraussetzung hier also in diesem Sinne stärker als in der Folgerung zu Satz 1, wo man nur *ein* simultanes Approximationssystem zu ξ_1, ξ_2 braucht. Ähnlich verhält sich der Fall $n=2$ des im folgenden zitierten Satzes 4 zur Folgerung aus Satz 2. Es zeigt sich aber, daß man durch Kombination der Fälle $n=2$ der Sätze 3 und 4 mit einem eigenartigen Übertragungssatz die Sätze 1 und 2 herleiten kann.

Die Fälle $n > 2$ der Sätze 3 und 4 werden zur Herleitung der „Hauptergebnisse“ nicht benötigt.

SATZ 4. Die Zahlen ξ_1, \dots, ξ_n seien algebraisch und irrational. Sei $\delta > 0$. Wir setzen $l = n + 1$.

\mathcal{N} sei die Menge aller positiven reellen Zahlen Q , zu denen es nichtnegative reelle Zahlen b_1, \dots, b_n gibt, so daß

$$b_1 + b_2 + \dots + b_n \leq 1 - \delta \quad (7)$$

ist, sowie eine Matrix M der Gestalt (4) vom Rang n mit ganzrationalen Elementen gibt, so daß

$$|p_{ij}| \leq Q^{b_j} \quad (1 \leq i \leq n; 1 \leq j \leq n) \quad (8)$$

und

$$|p_{i1}\xi_1 + \dots + p_{in}\xi_n - p_{ii}| \leq Q^{-1} \quad (1 \leq i \leq n) \quad (9)$$

gilt.

Dann hat \mathcal{N} Eigenschaft F .

Sind ξ_1, ξ_2 beliebige reelle Zahlen und $\varepsilon > 0$, so definieren wir $\mathfrak{D}(\xi_1, \xi_2, \varepsilon)$ so wie in Satz 1 und $\mathfrak{B}(\xi_1, \xi_2, \varepsilon)$ so wie in Satz 2. Weiter seien für $\delta > 0$ Mengen $\mathcal{M}(\xi_1, \xi_2, \delta)$ so wie $\mathcal{N}(\xi_1, \xi_2, \delta)$ definiert wie im Fall $n=2$ der Sätze 3 und 4. Ist ξ eine reelle Zahl, so sei $\mathcal{L}(\xi, \delta)$ die Menge der natürlichen q mit $\|\xi q\| < q^{-1-\delta}$, für die es also ein ganzes p mit $|\xi - p/q| < q^{-2-\delta}$ gibt. Nach dem Satz von Roth ist $\mathcal{L}(\xi, \delta)$ endlich, falls ξ irrational und algebraisch und $\delta > 0$ ist.

SATZ 5 (Übertragungssatz). ξ_1, ξ_2 seien reelle Zahlen, so daß

$$\|q\xi_1\| \geq q^{-c_1}, \quad \|q\xi_2\| \geq q^{-c_2} \quad (10)$$

für Konstanten $c_1 > 0, c_2 > 0$ und beliebige natürliche Zahlen $q > 1$ und

$$\|q_1\xi_1 + q_2\xi_2\| \geq q^{-c_3} \quad (11)$$

für eine Konstante $c_3 > 0$ und natürliche Zahlen q_1, q_2 mit $q = \max(|q_1|, |q_2|) > 1$ gilt.

(a) Sind $\mathcal{M}(\xi_1, \xi_2, \delta)$, $\mathcal{N}(\xi_1, \xi_2, \delta)$, $\mathcal{L}(\xi_1, \delta)$, $\mathcal{L}(\xi_2, \delta)$ für jedes $\delta > 0$ endlich, dann sind $\mathcal{D}(\xi_1, \xi_2, \varepsilon)$ und $\mathcal{P}(\xi_1, \xi_2, \varepsilon)$ für jedes $\varepsilon > 0$ endlich.

(b) Haben $\mathcal{M}(\xi_1, \xi_2, \delta)$, $\mathcal{N}(\xi_1, \xi_2, \delta)$, $\mathcal{L}(\xi_1, \delta)$, $\mathcal{L}(\xi_2, \delta)$ für jedes $\delta > 0$ Eigenschaft F , so haben auch $\mathcal{D}(\xi_1, \xi_2, \varepsilon)$, $\mathcal{P}(\xi_1, \xi_2, \varepsilon)$ für jedes $\varepsilon > 0$ diese Eigenschaft.

Sind nun ξ_1, ξ_2 algebraisch und $1, \xi_1, \xi_2$ l.u. über \mathbf{Q} , dann gilt bekanntlich (10) und (11). Nach dem Roth'schen Satz haben $\mathcal{L}(\xi_1, \delta)$ und $\mathcal{L}(\xi_2, \delta)$ für $\delta > 0$ höchstens endlich viele Elemente, und $\mathcal{M}(\xi_1, \xi_2, \delta)$ und $\mathcal{N}(\xi_1, \xi_2, \delta)$ haben nach den Sätzen 3 und 4 Eigenschaft F . Infolge Satz 5 b besitzen also $\mathcal{D}(\xi_1, \xi_2, \varepsilon)$ und $\mathcal{P}(\xi_1, \xi_2, \varepsilon)$ falls $\varepsilon > 0$ ist, Eigenschaft F und daher auch Eigenschaft E .

Die Sätze 1 und 2 folgen also aus dem Satz von Roth so wie aus den Sätzen 3, 4 und 5.

1.4. Transzendente Zahlen. Als einfache Anwendung von Satz 1 zeigen wir am Ende der Arbeit folgenden

SATZ 6. q_1, q_2, \dots seien die Näherungsnenner in der Kettenbruchentwicklung einer quadratischen Irrationalzahl. Sei $c > 1 + \sqrt{3}$, $n_k = [c^k]$. Dann ist

$$\xi = \sum_{k=1}^{\infty} (q_{n_k})^{-1} \tag{12}$$

transzendent.

Die Konvergenz der ξ definierenden Reihe ist klar. Man kann für die Folge q_1, q_2, \dots etwa die Fibonacci-Folge nehmen.

Mit dem Roth'schen Satz kann man die Transzendenz von ξ mit unserer Beweismethode nur für $c > 3$ zeigen. Es ist zu vermuten, daß die Behauptung sogar für $c > 1$ richtig bleibt.

1.5. Weitere Ergebnisse. Seien ξ_1, ξ_2, ξ_3 algebraisch und $1, \xi_1, \xi_2, \xi_3$ linear unabhängig über \mathbf{Q} . Dann kann man zeigen, daß die Menge der natürlichen q , zu denen es ganzrationale q_1, q_2, q_3 mit

$$q = \text{Max}(|q_1|, |q_2|, |q_3|) \quad \text{und} \quad \|q_1 \xi_1 + q_2 \xi_2 + q_3 \xi_3\| < q^{-5-\varepsilon}$$

gibt, für festes $\varepsilon > 0$ Eigenschaft E besitzt. Da aber die Schranke $q^{-5-\varepsilon}$ nicht mit der zu erhoffenden Schranke $q^{-3-\varepsilon}$ übereinstimmt, ist dieses Resultat weniger interessant, und es wird hier nicht bewiesen. Für mehr als 3 algebraische Zahlen ξ_1, ξ_2, \dots sind die Verhältnisse noch ungünstiger.

2. Die Eigenschaft F

2.1. Definitionen. Ist \mathcal{M} eine Menge von nichtnegativen reellen Zahlen, so sei $L_k(\mathcal{M})$ die Menge der Zahlen der Form $L_k(x)$, wobei $x \in \mathcal{M}$.

\mathcal{M} habe Eigenschaft G_m (m natürlich), falls es zu jedem $C_1 \geq 1$ ein $C_2 = C_2(C_1)$ gibt, so daß es m -tupel

$$x_1 < x_2 < \dots < x_m$$

von Elementen aus \mathcal{M} mit beliebig großem x_1 gibt, so daß

$$C_1 x_j < x_{j+1} \leq C_2 x_j \quad (j = 1, 2, \dots, m-1) \quad (1)$$

erfüllt wird.

\mathcal{M} hat Eigenschaft LG_m , falls es ein $k \geq 1$ gibt, so daß $\mathcal{M}_k = L_k(\mathcal{M})$ Eigenschaft G_m besitzt.

\mathcal{M} hat Eigenschaft F , falls \mathcal{M} nicht sämtliche Eigenschaften LG_m ($m = 1, 2, \dots$) besitzt.

2.2. Zusammenhang mit Eigenschaft E . Wie schon in der Einleitung angekündigt, zeigen wir hier

HILFSSATZ 1. Eine Menge \mathcal{M} natürlicher Zahlen, welche Eigenschaft F besitzt, besitzt auch Eigenschaft E .

Beweis. Wir dürfen annehmen, die Menge \mathcal{M} ist unendlich. Wir ordnen die Elemente von \mathcal{M} in einer wachsenden Folge $q_1 < q_2 < \dots$ an. Hat \mathcal{M} nicht Eigenschaft E , so gibt es ein k , so daß

$$\limsup_{h \rightarrow \infty} L_k(q_{h+1})/L_k(q_h) = D < \infty$$

ist. Es ist nun für $h > h_0$ $L_k(q_{h+1})/L_k(q_h) < D + 1$.

Ist $C_1 \geq 1$ gegeben, so setzen wir $C_2 = (D + 1)C_1$. Wir setzen $x_1 = q_h$, wobei $h > h_0$ ist. Es gibt nun ein $x_2 \in \mathcal{M}$, so daß $C_1 L_k(x_1) < L_k(x_2) \leq C_2 L_k(x_1)$ gilt. Ebenso gibt es ein $x_3 \in \mathcal{M}$, so daß $C_1 L_k(x_2) < L_k(x_3) \leq C_2 L_k(x_2)$ gilt. So fortfahrend sieht man, daß $L_k(\mathcal{M})$ die Eigenschaft G_m für jedes m besitzt.

Falls \mathcal{M} Eigenschaft F hat, so ist dies unmöglich. Dann hat also \mathcal{M} auch Eigenschaft E .

2.3. Hilfssätze.

HILFSSATZ 2. Die Vereinigungsmenge von endlich vielen Mengen mit Eigenschaft F hat wieder Eigenschaft F .

Bemerkung. Eine analoge Behauptung über die Eigenschaft E wäre falsch. Der Hauptvorteil der Eigenschaft F , von dem wir öfter Gebrauch machen werden, liegt eben in Hilfssatz 2.

Beweis. Offenbar genügt es, den Hilfssatz für die Vereinigung von zwei Mengen zu zeigen. Wir zeigen hier sogar etwas mehr, nämlich: *Hat $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$ Eigenschaft LG_{m^2} , so hat entweder \mathcal{M}_1 oder \mathcal{M}_2 Eigenschaft LG_m .* Daraus folgt der Hilfssatz, denn hätte \mathcal{M} nicht Eigenschaft F , so hätte \mathcal{M} Eigenschaft LG_{m^2} für jedes m . Entweder \mathcal{M}_1 oder \mathcal{M}_2 hätte nun Eigenschaft LG_m für beliebig große Zahlen m . Da aber aus $m' < m$ und Eigenschaft LG_m die Eigenschaft $LG_{m'}$ folgt, hätte nun eine der Mengen \mathcal{M}_j Eigenschaft LG_m für jedes m , somit nicht Eigenschaft F .

Um unsere oben formulierte Behauptung zu zeigen, genügt es, folgendes zu beweisen: *Hat $\mathcal{M} = \mathcal{M}_1 \cup \mathcal{M}_2$ Eigenschaft G_{m^2} , so hat entweder \mathcal{M}_1 oder \mathcal{M}_2 Eigenschaft G_m .*

Wir nehmen also an, \mathcal{M} habe Eigenschaft G_{m^2} . Zu jedem $C_1 \geq 1$ gibt es ein C_2 , so daß es m^2 -tupel $x_1 < x_2 < \dots < x_{m^2}$ von Elementen $x_j \in \mathcal{M}$ mit beliebig großem x_1 gibt, so daß

$$C_1 x_j < x_{j+1} \leq C_2 x_j \quad (j = 1, \dots, m^2 - 1)$$

ist. Jedem $K > 0$ ordnen wir ein solches m^2 -tupel mit $x_1 > K$ zu. Sei zunächst K fest. Wir unterscheiden zwei Möglichkeiten:

(a) Es gibt m aufeinanderfolgende Zahlen $x_{k+1}, x_{k+2}, \dots, x_{k+m}$ aus x_1, \dots, x_{m^2} , die alle zu \mathcal{M}_1 gehören. Nun ist also

$$C_1 x_{k+j} < x_{k+j+1} \leq C_2 x_{k+j} \quad (j = 1, \dots, m - 1).$$

(b) Gilt nicht (a), so gibt es m Zahlen $k_1 < k_2 < \dots < k_m$ zwischen 1 und m^2 , so daß $k_{j+1} \leq k_j + m$ ($j = 1, \dots, m - 1$), wobei $x_{k_j} \in \mathcal{M}_2$ ($j = 1, \dots, m$). Nun gilt mit $C'_2 = C_2^m$

$$C_1 x_{k_j} \leq x_{k_{j+1}} \leq C'_2 x_{k_j} \quad (j = 1, \dots, m - 1).$$

Tritt (a) für beliebig große K auf, so setzen wir $f(C_1) = 1$. Es gibt nun Elemente $y_1 < \dots < y_m$ aus \mathcal{M}_1 mit beliebig großem y_1 , so daß

$$C_1 y_j < y_{j+1} \leq C_2 y_j \quad (j = 1, \dots, m - 1). \tag{2}$$

Ansonst gilt (b) für beliebig große K , und wir setzen $f(C_1) = 2$. Nun gibt es Elemente $y_1 < \dots < y_m$ aus \mathcal{M}_2 mit beliebig großem y_1 , so daß

$$C_1 y_j < y_{j+1} \leq C'_2 y_j \quad (j = 1, \dots, m - 1). \tag{3}$$

Ist $f(C_1)=1$ für beliebig große C_1 , so hat \mathcal{M}_1 Eigenschaft G_m : Denn dann gibt es zu beliebig großem C_1 , daher zu jedem beliebigen $C_1 \geq 1$ ein C_2 , sowie y_1, \dots, y_m aus \mathcal{M}_1 mit beliebig großem y_1 , so daß (2) erfüllt ist. Ansonst ist $f(C_1)=2$ für beliebig großes C_1 , und \mathcal{M}_2 hat Eigenschaft G_m .

HILFSSATZ 3. \mathcal{M}, \mathcal{N} seien zwei Mengen positiver reeller Zahlen.

(a) Entweder gebe es Konstante $0 < a < b$, so daß es zu jedem $x \in \mathcal{M}$ ein $y \in \mathcal{N}$ mit

$$x^a \leq y \leq x^b$$

gibt.

(b) Oder es gebe eine Konstante $d > 0$, so daß \mathcal{N} aus allen Zahlen dx , $x \in \mathcal{M}$, besteht.

Hat nun \mathcal{N} Eigenschaft F , dann auch \mathcal{M} .

Beweis. (a) \mathcal{M} habe Eigenschaft LG_m . Es gibt nun ein $k \geq 1$, so daß $L_k(\mathcal{M})$ Eigenschaft G_m hat. Wir dürfen annehmen, $a < 1$, $b > 1$. Ist nun x groß und $x \in L_k(\mathcal{M})$, so gibt es ein $y \in L_k(\mathcal{N})$ mit

$$ax \leq y \leq bx.$$

Zu jedem $D_1 \geq 1$ gibt es ein $D_2 = D_2(D_1)$, so daß es $x_1 < \dots < x_m$ aus $L_k(\mathcal{M})$ mit beliebig großem x_1 und

$$D_1 x_j < x_{j+1} \leq D_2 x_j \quad (j = 1, \dots, m-1) \quad (4)$$

gibt.

Ist insbesondere $C_1 \geq 1$ und $D_1 = ba^{-1}C_1$, so bilden wir $D_2 = D_2(D_1)$ und $C_2 = ba^{-1}D_2$. Es gibt $x_1 < \dots < x_m$ aus $L_k(\mathcal{M})$ mit beliebig großem x_1 und (4). Zu jedem x_j gibt es ein $y_j \in L_k(\mathcal{N})$ mit $ax_j \leq y_j \leq bx_j$ ($j = 1, \dots, m$). Man hat nun

$$C_1 y_j \leq C_1 b x_j = D_1 a x_j < a x_{j+1} \leq y_{j+1} \leq b x_{j+1} \leq D_2 b x_j = C_2 a x_j \leq C_2 y_j,$$

wobei $y_1 < \dots < y_m$ in $L_k(\mathcal{N})$ liegen. Es gibt offenbar solche m -tupel mit beliebig großem y_1 . Somit hat $L_k(\mathcal{N})$ Eigenschaft G_m , \mathcal{N} Eigenschaft LG_m . Hätte also \mathcal{M} alle Eigenschaften LG_m , dann auch \mathcal{N} .

(b) Für alle Elemente von \mathcal{M} , die groß genug sind, gilt (a) mit $a = \frac{1}{2}$, $b = 2$. Somit kann man den Fall (b) auf (a) zurückführen.

3. Der Index eines Polynoms

3.1. Kombinatorische Hilfssätze.

HILFSSATZ 4. Die Zahl der l -tupel nichtnegativer ganzer Zahlen i_1, \dots, i_l mit $i_1 + \dots + i_l = r$ ist gleich

$$\binom{r+l-1}{l-1} = \binom{r+l-1}{r}.$$

Der *Beweis* dieses einfachen Hilfssatzes, der am besten durch Induktion nach l geführt wird, kann dem Leser überlassen werden.

HILFSSATZ 5. Gegeben seien natürliche Zahlen $l; r_1, \dots, r_m$, sowie eine Zahl $\varepsilon, 0 < \varepsilon < 1$. Dann ist die Zahl der lm -tupel von nichtnegativen ganzen Zahlen

$$i_{11}, \dots, i_{1l}; i_{21}, \dots, i_{2l}; \dots; i_{m1}, \dots, i_{ml}$$

mit
$$i_{h1} + \dots + i_{hl} = r_h \quad (1 \leq h \leq m) \tag{1}$$

und
$$\left| \sum_{h=1}^m i_{h1} r_h^{-1} - ml^{-1} \right| \geq \varepsilon m \tag{2}$$

höchstens gleich
$$\binom{r_1+l-1}{l-1} \dots \binom{r_m+l-1}{l-1} \cdot 2e^{-\varepsilon^2 m/4}. \tag{3}$$

Einen Beweis für den Spezialfall $l=2$ von G. E. H. Reuter findet man im Appendix A des vorzüglichen Buches von Mahler [4]. Der Hilfssatz bleibt natürlich richtig, wenn man in (2) i_{h1} durch i_{hj} ersetzt, wo $1 \leq j \leq l$.

Beweis. Die Zahl der lm -tupel (i_{hk}) , die (1) erfüllen, und für die der Ausdruck

$$\sum_{h=1}^m i_{h1} r_h^{-1} - ml^{-1}$$

kleiner als $-\varepsilon m$ bzw. größer als εm ist, bezeichnen wir mit M_1 bzw. M_2 . Wir setzen $f_j(c_j)$ für die Zahl der nichtnegativen ganzen

$$i_{j2}, \dots, i_{jl} \text{ mit } i_{j2} + \dots + i_{jl} = r_j - c_j \quad (1 \leq j \leq m; 0 \leq c_j \leq r_j).$$

Nach Hilfssatz 4 ist
$$f_j(c_j) = \binom{r_j - c_j + l - 2}{l - 2}, \tag{4}$$

$$\sum_{c_j=0}^{r_j} f_j(c_j) = \binom{r_j + l - 1}{l - 1}. \tag{5}$$

Offenbar ist
$$M_1 = \sum f_1(c_1) \dots f_m(c_m), \tag{6}$$

wobei über alle ganzen c_1, \dots, c_m summiert wird, die $0 \leq c_j \leq r_j$ und

$$ml^{-1} - \sum_{h=1}^m c_h r_h^{-1} > \varepsilon m$$

leisten. Man erhält

$$\begin{aligned} M_1 e^{\varepsilon^2 m/2} &\leq \sum_{c_1=0}^{r_1} \dots \sum_{c_m=0}^{r_m} f_1(c_1) \dots f_m(c_m) \exp \left\{ \frac{1}{2} \varepsilon \left(ml^{-1} - \sum_{h=1}^m c_h r_h^{-1} \right) \right\} \\ &= \prod_{j=1}^m \left(\sum_{c_j=0}^{r_j} f_j(c_j) \exp \left\{ \frac{1}{2} \varepsilon (l^{-1} - c_j r_j^{-1}) \right\} \right). \end{aligned}$$

Nun sei im Augenblick j fest, $r = r_j$, $f = f_j$. Dann ist

$$\begin{aligned} \sum_{c=0}^r f(c) \exp \left\{ \frac{1}{2} \varepsilon (l^{-1} - cr^{-1}) \right\} &\leq \sum_{c=0}^r f(c) \left(1 + \frac{1}{2} \varepsilon (l^{-1} - cr^{-1}) + \frac{1}{4} \varepsilon^2 (l^{-1} - cr^{-1})^2 \right) \\ &\leq \sum_{c=0}^r f(c) \left(1 + \frac{1}{4} \varepsilon^2 \right) + \frac{1}{2} \varepsilon \sum_{c=0}^r f(c) (l^{-1} - cr^{-1}) \\ &\leq \binom{r+l-1}{l-1} e^{\frac{1}{4} \varepsilon^2} + \frac{1}{2} \varepsilon \left\{ \sum_{c=0}^r f(c) (l^{-1} - cr^{-1}) \right\}. \end{aligned}$$

Wir wollen zeigen, daß der Ausdruck in der geschwungenen Klammer verschwindet.

$$\begin{aligned} \sum_{c=0}^r f(c) (l^{-1} - cr^{-1}) &= \sum_{c=0}^r f(r-c) (l^{-1} + cr^{-1} - 1) \\ &= (l^{-1} - 1) \sum_{c=0}^r f(r-c) + r^{-1} \sum_{c=0}^r cf(r-c) \\ &= (1-l) l^{-1} \binom{r+l-1}{l-1} + r^{-1} \sum_{c=0}^r c \binom{c+l-2}{l-2}. \end{aligned}$$

Es ist daher die Formel

$$\sum_{c=0}^r c \binom{c+l-2}{l-2} = rl^{-1}(l-1) \binom{r+l-1}{l-1}$$

zu zeigen. Diese gilt für $r=0$, und aus der Richtigkeit für $r-1$ folgt

$$\begin{aligned} \sum_{c=0}^r c \binom{c+l-2}{l-2} &= (r-1) l^{-1} (l-1) \binom{r+l-2}{l-1} + r \binom{r+l-2}{l-2} \\ &= \frac{(r+l-2)!}{l! r!} (r(r-1)(l-1) + rl(l-1)) \\ &= rl^{-1}(l-1) \binom{r+l-1}{l-1}. \end{aligned}$$

Aus unseren Formeln ergibt sich

$$M_1 e^{\varepsilon^2 m/2} \leq \binom{r_1+l-1}{l-1} \dots \binom{r_m+l-1}{l-1} e^{\varepsilon^2 m/4},$$

somit
$$M_1 \leq \binom{r_1+l-1}{l-1} \dots \binom{r_m+l-1}{l-1} e^{-\varepsilon^3 m/4}. \tag{7}$$

Eine genau solche Abschätzung gibt es für M_2 , und der Hilfssatz folgt.

3.2. Der Index. Wir schreiben \mathfrak{R} für den Ring der Polynome in den Unbestimmten $X_{11}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml}$ mit reellen Koeffizienten. Gegeben seien nun m nicht identisch verschwindende Linearformen L_1, \dots, L_m , und zwar sei $L_h = L_h(X_{h1}, \dots, X_{hl})$. Weiter seien natürliche Zahlen r_1, \dots, r_m gegeben. Unter

$$I(c)$$

wobei $c \geq 0$, verstehen wir das Ideal im Ring \mathfrak{R} , das durch die Polynome

$$L_1^{i_1} L_2^{i_2} \dots L_m^{i_m}$$

mit
$$\sum_{h=1}^m i_h r_h^{-1} \geq c$$

erzeugt wird. $I(c)$ nimmt mit wachsendem c ab. Offenbar ist $I(0) = \mathfrak{R}$,

$$\bigcap_{c \geq 0} I(c) = (0).$$

Definition. Der *Index* eines Polynoms $P \in \mathfrak{R}$ bezüglich $(L_1, \dots, L_m; r_1, \dots, r_m)$ sei die größte Zahl c , so daß $P \in I(c)$, falls $P \not\equiv 0$, und er sei $+\infty$, falls $P \equiv 0$.

Bemerkung. Da die Menge der Zahlen der Form $\sum_{h=1}^m i_h r_h^{-1}$ diskret ist, gibt es für ein Polynom $P \not\equiv 0$ tatsächlich eine solche maximale Zahl c . Sind L_1, \dots, L_m und r_1, \dots, r_m fest gegeben, so bezeichnen wir den Index von P mit $\text{Ind } P$.

HILFSSATZ 6.
$$\text{Ind}(P + Q) \geq \text{Min}(\text{Ind } P, \text{Ind } Q)$$

$$\text{Ind}(PQ) = \text{Ind } P + \text{Ind } Q.$$

FOLGERUNG. Der Index kann zu einer Bewertung im Quotientenkörper von \mathfrak{R} fortgesetzt werden.

Beweis. Die behauptete Ungleichung folgt fast sofort aus der Definition. Um die Gleichung zu zeigen, dürfen wir $P \not\equiv 0, Q \not\equiv 0$ voraussetzen. Man darf weiter o.B.d.A. annehmen, $\partial L_h / \partial X_{h1} \neq 0$ ($h = 1, \dots, m$). P kann nun auf genau eine Weise als eine Summe

$$\sum c(j_1, a_{12}, \dots, a_{1l}; \dots; j_m, a_{m2}, \dots, a_{ml}) L_1^{j_1} X_{12}^{a_{12}} \dots X_{1l}^{a_{1l}} \dots L_m^{j_m} X_{m2}^{a_{m2}} \dots X_{ml}^{a_{ml}}$$

dargestellt werden. Unter dem führenden Polynom P_F von P verstehen wir die Summe über jene nicht verschwindenden Summanden dieser Summe, wo $\sum j_h r_h^{-1}$ minimal ist. Für alle diese Summanden ist offenbar $\sum j_h r_h^{-1} = \text{Ind } P = \text{Ind } P_F$. Definiert man Q_F und $(PQ)_F$ auf dieselbe Weise, so ist $(PQ)_F = P_F Q_F$, somit

$$\text{Ind}(PQ) = \text{Ind}((PQ)_F) = \text{Ind}(P_F Q_F) = \text{Ind } P_F + \text{Ind } Q_F = \text{Ind } P + \text{Ind } Q.$$

Sind die Zahlen s_h und j_h in $\tau = (s_1, \dots, s_m; j_1, \dots, j_m)$ ganz, und ist $1 \leq s_h \leq m$, $j_h \geq 0$ ($1 \leq h \leq m$), so setzen wir

$$P^{(\tau)} = (j_1! \dots j_m!)^{-1} \frac{\partial^{j_1 + \dots + j_m}}{\partial X_{1s_1}^{j_1} \dots \partial X_{ms_m}^{j_m}} P. \quad (8)$$

HILFSSATZ 7. *Der Index des Polynoms P bezüglich $(L_1, \dots, L_m; r_1, \dots, r_m)$ sei $c \neq \infty$. T sei der $((ml - m)$ -dimensionale) Teilraum des ml -dimensionalen Raumes R_{ml} , in welchem $L_1 = \dots = L_m = 0$ ist. s_1, \dots, s_m seien so gewählt, daß $\partial L_h / \partial X_{s_h} \neq 0$ ist ($h = 1, \dots, m$). Damit ist $P^{(\tau)}$ für*

$$\tau = (s_1, \dots, s_m; j_1, \dots, j_m)$$

auf T identisch null, falls $\sum j_h r_h^{-1} < c$ ist, aber es gibt j_1, \dots, j_m mit $\sum j_h r_h^{-1} = c$, so daß $P^{(\tau)}$ auf T nicht identisch verschwindet.

Ist weiter $\tau = (t_1, \dots, t_m; j_1, \dots, j_m)$ und $\sum j_h r_h^{-1} < c$, wo $1 \leq t_h \leq m$ beliebig ist, so ist $P^{(\tau)}$ auf T identisch Null.

Beweis. Man darf o.B.d.A annehmen, $s_1 = \dots = s_m = 1$. P ist nun ein Polynom in $L_1, \dots, L_m; X_{12}, \dots, X_{11}; \dots; X_{m2}, \dots, X_{m1}$, und kann auf genau eine Weise in der Gestalt

$$\sum P(j_1, \dots, j_m | X_{12}, \dots, X_{11}; \dots; X_{m2}, \dots, X_{m1}) L_1^{j_1} \dots L_m^{j_m}$$

geschrieben werden, wo $P(j_1, \dots, j_m | X_{12}, \dots, X_{m1})$ ein Polynom in den $ml - m$ Variablen X_{12}, \dots, X_{m1} ist. Dabei ist offenbar $P(j_1, \dots, j_m | \dots)$ identisch Null, falls $\sum j_h r_h^{-1} < c$ ist, aber es gibt j_1, \dots, j_m mit $\sum j_h r_h^{-1} = c$, für die $P(j_1, \dots, j_m | \dots)$ nicht identisch verschwindet. Somit ist $P^{(\tau)}$ auf T identisch Null, falls $\sum j_h r_h^{-1} < c$, aber es gibt j_1, \dots, j_m mit $\sum j_h r_h^{-1} = c$, so daß $P^{(\tau)}$ auf T nicht identisch gleich Null ist, wobei $\tau = (1, \dots, 1; j_1, \dots, j_m)$.

Die letzte Behauptung des Hilfssatzes folgt daraus, daß, wenn für ein h $\partial L_h / \partial X_{ht_h} = 0$ ist, der Index bezüglich $(L_1, \dots, L_m; r_1, \dots, r_m)$ bei Differentiation nach X_{ht_h} nicht verkleinert wird.

FOLGERUNG 1. *Ist $\tau = (t_1, \dots, t_m; j_1, \dots, j_m)$, so ist*

$$\text{Ind } P^{(\tau)} \geq \text{Ind } P - \sum_{h=1}^m j_h r_h^{-1}. \quad (9)$$

Oft ist der Spezialfall von Bedeutung, wo $L_h(X_{h1}, \dots, X_{hl}) = L(X_{h1}, \dots, X_{hl}) = \alpha_1 X_{h1} + \dots + \alpha_l X_{hl}$, wo $L = \alpha_1 X_1 + \dots + \alpha_l X_l$ eine vorgegebene, nicht identisch verschwindende Linearform ist. Dann schreiben wir $(L; r_1, \dots, r_m)$ an Stelle von $(L_1, \dots, L_m; r_1, \dots, r_m)$. Weiter schreiben wir

$$P_{j_1 \dots j_m}^{(s)} = P^{(\tau)}, \quad \text{wo } \tau = (s, \dots, s; j_1, \dots, j_m).$$

FOLGERUNG 2. Der Index von $P \in \mathfrak{R}$ bezüglich $(L; r_1, \dots, r_m)$ sei $c \neq \infty$. Es sei $\partial L / \partial X_s \neq 0$. Dann ist

$$P_{j_1 \dots j_m}^{(s)} \tag{10}$$

auf T identisch Null, falls $\sum j_h r_h^{-1} < c$, aber es gibt j_1, \dots, j_m mit $\sum j_h r_h^{-1} = c$, so daß (10) auf T nicht identisch verschwindet.

3.3. Polynomabschätzungen. Ist $P \in \mathfrak{R}$, so schreiben wir $|P|$ für das Maximum der Absolutbeträge der Koeffizienten von P .

HILFSSATZ 8. $P \in \mathfrak{R}$ sei homogen in X_{h1}, \dots, X_{hl} vom Grad r_h ($1 \leq h \leq m$). (Das heißt, P ist Summe von Monomen $cX_{11}^{i_1} \dots X_{ml}^{i_m}$ mit $i_{h1} + \dots + i_{hl} = r_h$ ($1 \leq h \leq m$)). Dann ist

$$|P^{(\tau)}| \leq 2^{r_1 + \dots + r_m} |P|$$

für beliebiges $\tau = (t_1, \dots, t_m; j_1, \dots, j_m)$.

Beweis. Es genügt, diese Abschätzung für Monome zu beweisen. Nun ist

$$(X_{11}^{t_1} \dots X_{ml}^{t_m})^{(\tau)} = \binom{i_{1t_1}}{j_1} \dots \binom{i_{mt_m}}{j_m} X_{11}^{i_{1t_1} - j_1} \dots X_{1l}^{i_{1l}} \dots X_{m1}^{i_{m1}} \dots X_{mt_m}^{i_{mt_m} - j_m} \dots X_{ml}^{i_{ml}}.$$

Wegen
$$\binom{i_{1t_1}}{j_1} \dots \binom{i_{mt_m}}{j_m} \leq 2^{i_{1t_1} + \dots + i_{mt_m}} \leq 2^{r_1 + \dots + r_m}$$

folgt hieraus das gewünschte Resultat.

$\alpha_1, \dots, \alpha_l$ seien ganzzahlige Zahlen. Der Körper $K = \mathbf{Q}(\alpha_1, \dots, \alpha_l)$ habe Grad Δ . $\beta_1, \dots, \beta_\Delta$ sei Ganzheitsbasis von K . Dann gilt eine Beziehung

$$\beta_i \beta_j = \sum_{k=1}^{\Delta} c_{ijk} \beta_k \quad (1 \leq i \leq \Delta, 1 \leq j \leq \Delta)$$

mit ganzrationalen Koeffizienten c_{ijk} . Wir setzen A für das Maximum der Beträge der c_{ijk} . Ist $\gamma \in K$, so kann γ auf genau eine Weise $\gamma = \sum_{j=1}^{\Delta} r_j \beta_j$ mit $r_j \in \mathbf{Q}$ geschrieben werden.

Wir setzen $|\bar{\gamma}| = A\Delta^2 \text{Max}_j (|r_j|)$.

Offenbar ist $|\overline{\gamma + \delta}| \leq |\bar{\gamma}| + |\bar{\delta}|$. (11)

Ist $\delta = \sum_{j=1}^{\Delta} s_j \beta_j$ mit rationalen s_j , so ist

$$\gamma\delta = \sum_i \sum_j r_i s_j \beta_i \beta_j = \sum_i \sum_j \sum_k r_i s_j c_{ijk} \beta_k.$$

Der Koeffizient von β_k hat also einen Betrag, der höchstens gleich

$$A\Delta^2 \text{Max} (|r_i|) \text{Max} (|s_j|) \leq (A\Delta^2)^{-1} |\bar{\gamma}| |\bar{\delta}|$$

ist. Somit erhalten wir $|\overline{\gamma\delta}| \leq |\bar{\gamma}| |\bar{\delta}|$. (12)

Schließlich setzen wir $B = \text{Max}_{1 \leq j \leq l} (|\bar{\alpha}_j|)$.

HILFSSATZ 9. Wir betrachten Polynome

$$P(X_{11}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml}) \\ = \sum c(j_{11}, \dots, j_{1l}; \dots; j_{m1}, \dots, j_{ml}) X_{11}^{j_{11}} \dots X_{1l}^{j_{1l}} \dots X_{m1}^{j_{m1}} \dots X_{ml}^{j_{ml}}, \quad (13)$$

welche in den Variablen X_{h1}, \dots, X_{hl} homogen vom Grad r_h ($1 \leq h \leq m$) oder identisch Null seien.

$\alpha_1, \dots, \alpha_l$ seien ganzzahlgemäß. Wir bilden

$$P^* = P^*(X_{12}, \dots, X_{1l}; \dots; X_{m2}, \dots, X_{ml}) \\ = P_{j_1, \dots, j_m}^{(1)} (-\alpha_2 X_{12} - \dots - \alpha_l X_{1l}, \alpha_1 X_{12}, \dots, \alpha_1 X_{1l}; \dots; -\alpha_2 X_{m2} - \dots - \alpha_l X_{ml}, \\ \alpha_1 X_{m2}, \dots, \alpha_1 X_{ml}).$$

Dann ist jeder Koeffizient von P^* eine Linearform in den Koeffizienten $c(j_{11}, \dots, j_{ml})$ von P . Die Koeffizienten γ dieser Linearformen sind ganze Zahlen von $K = \mathbf{Q}(\alpha_1, \dots, \alpha_l)$ und erfüllen

$$|\bar{\gamma}| \leq (2^l B)^{r_1 + \dots + r_m}.$$

(Die Bedeutung von $|\bar{\gamma}|$ und von B wurde vor dem Hilfssatz erklärt.)

Beweis. Nur die Schranke für $|\bar{\gamma}|$ ist zu beweisen. P^* ist Summe von höchstens

$$\binom{r_1 + l - 1}{l - 1} \dots \binom{r_m + l - 1}{l - 1} \leq (r_1 l)^{l-1} \dots (r_m l)^{l-1} \leq 2^{(l-1)(r_1 + \dots + r_m)}$$

Summanden S der Gestalt

$$\begin{aligned} S &= \pm c(\dots) \binom{j_{11}}{j_1} \dots \binom{j_{m1}}{j_m} (\alpha_2 X_{12} + \dots + \alpha_l X_{1l})^{j_{11}-j_1} (\alpha_1 X_{12})^{j_{12}} \dots \\ &\quad \dots (\alpha_1 X_{1l})^{j_{1l}} \dots (\alpha_2 X_{m2} + \dots + \alpha_l X_{ml})^{j_{m1}-j_m} (\alpha_1 X_{m2})^{j_{m2}} \dots (\alpha_1 X_{ml})^{j_{ml}} \\ &= \pm c(\dots) \binom{j_{11}}{j_1} \dots \binom{j_{m1}}{j_m} S_1 S_2 \dots S_m, \end{aligned}$$

wobei

$$\begin{aligned} S_h &= (\alpha_2 X_{h2} + \dots + \alpha_l X_{hl})^{j_{h1}-j_h} (\alpha_1 X_{h2})^{j_{h2}} \dots (\alpha_1 X_{hl})^{j_{hl}} \\ &= \sum_{\substack{c_2, \dots, c_l \\ c_2 + \dots + c_l = j_{h1} - j_h}} \frac{(j_{h1} - j_h)!}{c_2! \dots c_l!} \alpha_2^{c_2} \dots \alpha_l^{c_l} \alpha_1^{j_{h2} + \dots + j_{hl}} X_{h2}^{c_2 + j_{h2}} \dots X_{hl}^{c_l + j_{hl}}. \end{aligned}$$

Nun ist $(j_{h1} - j_h)! (c_2! \dots c_l!)^{-1} \leq l^{r_h}$ und

$$\left| \alpha_2^{c_2} \dots \alpha_l^{c_l} \alpha_1^{j_{h2} + \dots + j_{hl}} \right| \leq B^{c_2 + \dots + c_l + j_{h2} + \dots + j_{hl}} = B^{r_h - j_h} \leq B^{r_h}.$$

Somit ist jeder Koeffizient α von S_h ganz in K und er erfüllt $|\bar{\alpha}| \leq (lB)^{r_h}$. Daher ist jeder Koeffizient von S von der Form $c(\dots)\beta$, wobei $\beta \in K$,

$$|\bar{\beta}| \leq \binom{j_{11}}{j_1} \dots \binom{j_{m1}}{j_m} (lB)^{r_1 + \dots + r_m} \leq (2lB)^{r_1 + \dots + r_m}.$$

Da nun, wie schon bemerkt, P^* Summe von höchstens $2^{(l^2-l)(r_1 + \dots + r_m)}$ Polynomen vom Typ S ist, ist jeder Koeffizient von P^* eine Linearform in den $c(\dots)$ mit Koeffizienten γ , die

$$|\bar{\gamma}| \leq 2^{(l^2-l)(r_1 + \dots + r_m)} (2lB)^{r_1 + \dots + r_m} \leq (2^{l^2} B)^{r_1 + \dots + r_m}$$

erfüllen.

3.4. Der Indexsatz.

SATZ 7 (Indexsatz). Seien l, t natürlich, und seien $L^{(1)}, \dots, L^{(t)}$ nicht identisch verschwindende Linearformen in X_1, \dots, X_l , etwa

$$L^{(i)} = \alpha_{i1} X_1 + \dots + \alpha_{il} X_l,$$

wobei die α_{ij} ganze algebraische Zahlen seien. Wir setzen Δ_i für den Grad von $K_i = \mathbf{Q}(\alpha_{i1}, \dots, \alpha_{il})$, sowie $\Delta = \text{Max}(\Delta_1, \dots, \Delta_t)$.

Sei $\varepsilon > 0$. Sei m ganz und so groß, daß

$$m \geq 4\varepsilon^{-2} \log(2t\Delta). \tag{14}$$

Seien r_1, \dots, r_m beliebige natürliche Zahlen.

Dann gibt es ein Polynom $P(X_{11}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml}) \in \mathfrak{R}$, mit ganzrationalen Koeffizienten, das nicht identisch verschwindet, und das

- (i) in X_{h1}, \dots, X_{hl} homogen vom Grad r_h ist ($h=1, \dots, m$),
- (ii) bezüglich $(L^{(l)}; r_1, \dots, r_m)$ einen Index $\geq (l-1-\varepsilon)m$ besitzt ($1 \leq i \leq l$),

und das

- (iii) $|P| \leq D^{r_1 + \dots + r_m}$

leistet, wobei D eine Konstante ist, die nur von den Koeffizienten α_{ij} abhängt.

(Definiert man B_i bezüglich $(\alpha_{i1}, \dots, \alpha_{il})$ so wie B bezüglich $(\alpha_1, \dots, \alpha_l)$ in § 3.3, und setzt man $B = \text{Max}(B_1, \dots, B_l)$, so darf $D = 4^l B$ genommen werden.)

Beweis. Wir setzen P in der Form (13) an und untersuchen, welchen Bedingungen die Koeffizienten $c(j_{11}, \dots, j_{ml})$ durch (ii) unterworfen werden. Zuerst wollen wir untersuchen, was es für die Koeffizienten bedeutet, daß der Index bezüglich $(L^{(l)}; r_1, \dots, r_m)$ mindestens $(l-1-\varepsilon)m$ sein soll. Dabei nehmen wir der Einfachheit halber an, es sei $\alpha_{11} \neq 0$, also $\partial L^{(l)} / \partial X_1 \neq 0$. Nach Hilfssatz 7 erfüllt der Index die gewünschte Ungleichung, falls das Polynom

$$P_{i_1 \dots i_m}^{(l)}$$

für $\sum i_h r_h^{-1} < (l-1-\varepsilon)m$ im durch $L_1^{(l)} = L_2^{(l)} = \dots = L_m^{(l)} = 0$ definierten Teilraum verschwindet. Halten wir zunächst i_1, \dots, i_m fest. Dann lautet unsere Bedingung, daß

$$P^* = P_{i_1 \dots i_m}^{(l)} (-\alpha_{12} X_{12} - \dots - \alpha_{1l} X_{1l}, \alpha_{11} X_{12}, \dots, \alpha_{11} X_{1l}, \dots, \\ -\alpha_{12} X_{m2} - \dots - \alpha_{1l} X_{ml}, \alpha_{11} X_{m2}, \dots, \alpha_{11} X_{ml})$$

identisch verschwindet. Falls P^* nicht identisch verschwindet, ist es homogen in X_{h2}, \dots, X_{hl} vom Grad $r_h - i_h$ ($h=1, \dots, m$), besitzt also höchstens

$$\binom{r_1 - i_1 + l - 2}{l - 2} \dots \binom{r_m - i_m + l - 2}{l - 2} = f_1(i_1) \dots f_m(i_m)$$

nichtverschwindende Koeffizienten. Jeder Koeffizient ist nach Hilfssatz 9 eine Linearform in den $c(\dots)$ mit ganzen Zahlen aus K_1 als Koeffizienten. Wir erhalten so $f_1(i_1) \dots f_m(i_m)$ lineare homogene Gleichungen in den Koeffizienten $c(j_{11}, \dots, j_{ml})$ von P , und die Koeffizienten dieser Gleichungen sind ganze Elemente γ aus K_1 , die $|\gamma| \leq$

$(2^l B_1)^{r_1 + \dots + r_m}$ erfüllen. Da die $c(\dots)$ ganz sein sollen, ist jede dieser linearen Gleichungen äquivalent Δ_1 linearen homogenen Gleichungen mit ganzrationalen Koeffizienten k , die

$$|k| \leq (2^{2l} B_1)^{r_1 + \dots + r_m} \tag{15}$$

erfüllen.

Indem man nun über alle m -tupel i_1, \dots, i_m mit $\sum i_h r_h^{-1} < (l^{-1} - \varepsilon) m$ summiert, sieht man: Damit die Bedingung (ii) für $L^{(1)}$ erfüllt werde, sind von den $c(\dots)$

$$\Delta_1 \sum f_1(i_1) \dots f_m(i_m) \tag{16}$$

lineare homogene Gleichungen zu erfüllen, wobei die Summe (16) über alle m -tupel i_1, \dots, i_m mit $\sum i_h r_h^{-1} < (l^{-1} - \varepsilon) m$ zu erstrecken ist. Nach (6), § 3.1, ist die Summe in (16) gleich M_1 , also die Zahl der Gleichungen gleich

$$\Delta_1 M_1 \leq \Delta_1 \binom{r_1 + l - 1}{l - 1} \dots \binom{r_m + l - 1}{l - 1} e^{-\varepsilon^2 m/4} = \Delta_1 N e^{-\varepsilon^2 m/4},$$

wobei N die Zahl der Unbekannten des Gleichungssystems ist. Jeder Koeffizient k dieser Gleichungen wird durch (15) abgeschätzt.

Um nun (ii) zu befriedigen, erhält man insgesamt M Gleichungen, wobei

$$M \leq t \Delta N e^{-\varepsilon^2 m/4} \leq \frac{1}{2} N$$

wegen (14). Die Beträge der (ganzrationalen) Koeffizienten des Gleichungssystems sind höchstens gleich

$$A = (2^{2l} B)^{r_1 + \dots + r_m}.$$

Indem wir nun etwa Lemma 3 aus [1], Chapter IV heranziehen, sehen wir, daß es ganzrationale $c(\dots)$ gibt, die alle M linearen homogenen Gleichungen erfüllen, die nicht sämtlich verschwinden, und deren Absolutbeträge höchstens gleich

$$(NA)^{M/(N-M)} \leq NA \leq \binom{r_1 + l - 1}{l - 1} \dots \binom{r_m + l - 1}{l - 1} A \leq 2^{l(r_1 + \dots + r_m)} A = (4^{2l} B)^{r_1 + \dots + r_m}$$

sind.

Zusätzlich zu (i) und (ii) kann also noch (iii) befriedigt werden.

3.5. Der Polynomsatz.

SATZ 8 (Polynomsatz). Gegeben seien l lineare Formen $L^{(1)}, \dots, L^{(l)}$ in X_1, \dots, X_l mit ganzalgebraischen Koeffizienten und von Null verschiedener Determinante. Es sei $\varepsilon > 0$ und

$$m \geq 4\varepsilon^{-2} \log(2l\Delta), \tag{17}$$

wobei Δ so definiert ist wie im Indexsatz. r_1, \dots, r_m seien natürlich.

Dann gibt es ein Polynom $P(X_{11}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml}) \neq 0$ mit ganzrationalen Koeffizienten, so daß

- (i) P ist homogen in (X_{h1}, \dots, X_{hl}) vom Grad r_h ($h=1, \dots, m$).
- (ii) $|P| \leq D^{r_1 + \dots + r_m}$.
- (iii) Ist $\tau = (t_1, \dots, t_m; j_1, \dots, j_m)$ mit $\sum j_h r_h^{-1} \leq \varepsilon m$, und schreibt man

$$P^{(\tau)} = \sum d^{(\tau)}(i_{11}, \dots, i_{1l}; \dots; i_{m1}, \dots, i_{ml}) L_1^{(1)i_{11}} \dots L_1^{(l)i_{1l}} \dots L_m^{(1)i_{m1}} \dots L_m^{(l)i_{ml}}$$

(was ja auf genau eine Weise möglich ist) (wie $L_1^{(h)}, \dots, L_m^{(h)}$ mit $L^{(h)}$ zusammenhängt wurde am Ende von § 3.2 erklärt), so ist $d^{(\tau)}(i_{11}, \dots, i_{ml}) = 0$, außer es gilt

$$\left| \sum_{h=1}^m i_{hj} r_h^{-1} - ml^{-1} \right| \leq 2lm\varepsilon \quad (j=1, \dots, l).$$

- (iv) Für beliebige τ ist weiter

$$|d^{(\tau)}(i_{11}, \dots, i_{ml})| \leq E^{r_1 + \dots + r_m}.$$

Dabei hängen D, E nur von den Koeffizienten der Formen $L^{(j)}$ ab.

(Man darf z. B. D so wählen wie im Indexsatz. Ist $X_i = \sum_{j=1}^l \beta_{ij} L^{(j)}$ ($1 \leq i \leq l$) und $|\beta_{ij}| \leq G$ ($1 \leq i, j \leq l$), so darf man $E = 2^l DG$ setzen.)

Beweis. Wir werden sehen, daß das im Indexsatz bezüglich $L^{(1)}, \dots, L^{(l)}$ konstruierte Polynom P alles erfüllt. Für (i) und (ii) ist das klar. Da der Index von P bezüglich $(L^{(j)}; r_1, \dots, r_m)$ mindestens $(l^{-1} - \varepsilon)m$ ist, ist der Index von $P^{(\tau)}$ bezüglich $(L^{(j)}; r_1, \dots, r_m)$ mindestens $(l^{-1} - \varepsilon)m - \sum j_h r_h^{-1} \geq (l^{-1} - 2\varepsilon)m$. Sind also i_{11}, \dots, i_{ml} Indices, für die $d^{(\tau)}(i_{11}, \dots, i_{ml}) \neq 0$ ist, so gilt jedenfalls

$$\sum_{h=1}^m i_{hj} r_h^{-1} - ml^{-1} \geq -2m\varepsilon \quad (j=1, \dots, l). \quad (18)$$

Da nun $P^{(\tau)}$ homogen in $L_h^{(1)}, \dots, L_h^{(l)}$ vom Grad $r_h - j_h$ ist ($h=1, \dots, m$), gilt

$$\sum_{j=1}^l i_{hj} r_h^{-1} = 1 - \frac{j_h}{r_h} \quad (h=1, \dots, m),$$

$$\sum_{j=1}^l \left(\sum_{h=1}^m i_{hj} r_h^{-1} - ml^{-1} \right) = - \sum_{h=1}^m j_h r_h^{-1} \leq 0,$$

woraus sich zusammen mit (18) weiter

$$\sum_{h=1}^m i_{hj} r_h^{-1} - ml^{-1} \leq 2m(l-1)\varepsilon \tag{19}$$

ergibt. Aus (18) und (19) folgt (iii).

Da unsere Formen eine Determinante ungleich Null besitzen, gibt es β_{ij} , so daß $X_i = \sum_{j=1}^l \beta_{ij} L^{(j)}$ ($i = 1, \dots, l$). Dann ist allgemein

$$X_{hi} = \sum_{j=1}^l \beta_{ij} L_h^{(j)} \quad (1 \leq i \leq l, 1 \leq h \leq m). \tag{20}$$

Wir wählen G so groß, daß $|\beta_{ij}| \leq G$ ($1 \leq i, j \leq l$). Man erhält $P^{(v)}$ in der in (iii) gegebenen Gestalt, indem man in der Formel

$$P^{(v)} = \sum c^{(v)}(i_{11}, \dots, i_{ml}) X_{11}^{i_{11}} \dots X_{ll}^{i_{ll}} \dots X_{m1}^{i_{m1}} \dots X_{ml}^{i_{ml}} \tag{21}$$

für jedes X_{hi} gemäß (20) substituiert. Ein typisches Produkt in (21), nämlich

$$X_{h1}^{i_{h1}} \dots X_{hl}^{i_{hl}} \text{ mit } i_{h1} + \dots + i_{hl} = r_h - j_h$$

geht dabei über in $\left(\sum_{j=1}^l \beta_{1j} L_h^{(j)}\right)^{i_{h1}} \dots \left(\sum_{j=1}^l \beta_{lj} L_h^{(j)}\right)^{i_{hl}}$.

Setzen wir $S_h(Y_{h1}, \dots, Y_{hl}) = \left(\sum_{j=1}^l \beta_{1j} Y_{hj}\right)^{i_{h1}} \dots \left(\sum_{j=1}^l \beta_{lj} Y_{hj}\right)^{i_{hl}}$,

so ist der Koeffizient von $Y_{h1}^{c_1} \dots Y_{hl}^{c_l}$ ($c_1 + \dots + c_l = r_h - j_h$) in S_h dem Betrage nach höchstens gleich

$$\frac{(r_h - j_h)!}{c_1! \dots c_l!} G^{r_h - j_h} \leq l^{r_h - j_h} G^{r_h - j_h} \leq (lG)^{r_h},$$

und daher ist $|S_1 S_2 \dots S_m| \leq (lG)^{r_1 + \dots + r_m}$.

Hieraus folgt unter Benützung von Hilfssatz 8, und da (21) höchstens $2^{(l-1)(r_1 + \dots + r_m)}$ Summanden hat,

$$|d^{(v)}(i_{11}, \dots, i_{ml})| \leq |P^{(v)}| (2^{l-1} lG)^{r_1 + \dots + r_m} \leq |P| (2^l G)^{r_1 + \dots + r_m} \leq (2^l DG)^{r_1 + \dots + r_m}.$$

4. Linearformen M

4.1. In diesem Abschnitt wenden wir uns spezielleren Überlegungen zu, die auf den Beweis der Sätze 3 und 4 hinzielen. Dies steht im Gegensatz zu den Ergebnissen des § 3, welche natürliche Verallgemeinerungen der zum Satz von Roth führenden Argumente sind.

Wir nehmen nun an, w_1, \dots, w_{l-1} seien $l-1$ linear unabhängige Vektoren im R_l , $l > 1$. (Später werden wir dafür die Zeilenvektoren einer Matrix M aus (4), § 1, nehmen.) w_1, \dots, w_{l-1} spannen im R_l einen Teilraum der Dimension $l-1$, also eine Hyperebene H auf. Haben die Vektoren ganzrationale Koordinaten, etwa $w_i = (w_{i1}, \dots, w_{il})$ mit ganzen w_{ij} , so gibt es bis auf das Vorzeichen genau eine Linearform $M = m_1 X_1 + \dots + m_l X_l \neq 0$ mit ganzrationalen, relativ primen Koeffizienten m_1, \dots, m_l , so daß

$$M(w_i) = m_1 w_{i1} + \dots + m_l w_{il} = 0 \quad (i = 1, \dots, l-1)$$

ist. Wir schreiben $M = M\{w_1, \dots, w_{l-1}\}$.

Offenbar liegt ξ genau dann auf der Hyperebene, falls $M(\xi) = 0$ ist. Schließlich setzen wir

$$\langle M \rangle = \text{Max}(|m_1|, \dots, |m_l|).$$

4.2. Raster. Wieder seien w_1, \dots, w_{l-1} $l-1$ linear unabhängige Vektoren des R_l , die eine Hyperebene H aufspannen. Sei r natürlich. Wir schreiben dann $\varrho(r; w_1, \dots, w_{l-1})$ für die Menge aller Vektoren

$$w(t_1, \dots, t_{l-1}) = t_1 w_1 + \dots + t_{l-1} w_{l-1},$$

wobei die Koeffizienten t_i natürlich sind und im Intervall $1 \leq t_i \leq r+1$ liegen. Wir nennen $\varrho(r; w_1, \dots, w_{l-1})$ ein *Raster der Größe r auf H mit Basisvektoren w_1, \dots, w_{l-1}* .

Im folgenden fassen wir jede Funktion von l Variablen X_1, \dots, X_l als eine Funktion im R_l auf.

HILFSSATZ 10. Sei $P(X_1, \dots, X_l)$ eine Form in X_1, \dots, X_l vom Grad r . Sei ϱ ein Raster der Größe r auf einer Hyperebene H des R_l , so daß P auf ϱ verschwindet. Dann ist P auf H identisch gleich Null.

Beweis. Durch eine lineare Transformation kann man erreichen, daß die Basisvektoren w_1, \dots, w_{l-1} des Rasters ϱ von der Gestalt $w_1 = (1, 0, \dots, 0)$, $w_2 = (0, 1, 0, \dots, 0)$, \dots , $w_{l-1} = (0, \dots, 0, 1, 0)$ sind. Nach Voraussetzung ist nun

$$P(t_1, \dots, t_{l-1}, 0) = 0 \quad (t_i = 1, \dots, r+1 \quad (i = 1, \dots, l-1)).$$

Halten wir nun t_1, \dots, t_{l-2} fest. Da $P(t_1, \dots, t_{l-2}, X_{l-1}, 0)$ in X_{l-1} höchstens Grad r besitzt, jedoch mindestens $r+1$ Nullstellen hat, ist $P(t_1, \dots, t_{l-2}, X_{l-1}, 0)$ in X_{l-1} identisch gleich Null. Durch $(l-1)$ -fache Anwendung dieses Schlusses sieht man, daß $P(X_1, \dots, X_{l-1}, 0)$ identisch verschwindet, daß also P auf H identisch verschwindet.

HILFSSATZ 11. Das Polynom $P(X_{11}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml}) \in \mathfrak{R}$ sei homogen vom Grad r_h in X_{h1}, \dots, X_{hl} ($h = 1, \dots, m$). Wir fassen (X_{h1}, \dots, X_{hl}) zu \mathfrak{X}_h zusammen, schreiben also kürzer $P(\mathfrak{X}_1, \dots, \mathfrak{X}_m)$ und fassen P als Funktion im m -fachen Produkt $R_1 \times R_1 \times \dots \times R_l$ auf.

Gegeben seien nun Hyperebenen H_1, \dots, H_m des R_l , und auf jeder Hyperebene H_h liege ein Raster ϱ_h der Größe r_h ($h = 1, \dots, m$). Der Teilraum $T = H_1 \times \dots \times H_m$ des R_{ml} bestehe aus allen $(\mathfrak{X}_1, \dots, \mathfrak{X}_m)$ mit $\mathfrak{X}_h \in H_h$ ($h = 1, \dots, m$), und $\varrho^* = \varrho_1 \times \dots \times \varrho_m$ bestehe aus allen $(\mathfrak{X}_1, \dots, \mathfrak{X}_m)$ mit $\mathfrak{X}_h \in \varrho_h$ ($h = 1, \dots, m$).

Verschwundet nun P auf ϱ^* , so verschwindet P auf T identisch.

Beweis. Dieser Hilfssatz folgt durch m -malige Anwendung des vorhergehenden. Die Details des Beweises können dem Leser überlassen werden.

4.3. Der Index bezüglich Linearformen M .

SATZ 9. Gegeben seien reelle Zahlen c_1, \dots, c_l mit $c_1 + \dots + c_l < 0$. Wir setzen $c = \text{Max}(|c_i|)$. Die Zahl $\varepsilon > 0$ sei so klein, daß

$$c_1 + \dots + c_l \leq -\varepsilon l^3(4c + 9). \tag{1}$$

Die Zahl m und die l Linearformen $L^{(1)}, \dots, L^{(l)}$ mögen die Voraussetzungen des Polynomsatzes erfüllen, E sei die Konstante aus Teil (iv) dieses Satzes, und P sei das in diesem Satz beschriebene Polynom in bezug auf vorgegebene Zahlen r_1, \dots, r_m .

Weiter seien reelle Zahlen $Q^{(1)}, \dots, Q^{(m)}$ gegeben, so daß

$$(a) \quad Q^{(h)\varepsilon/2} > 2^{l^2} E \quad (1 \leq h \leq m),$$

$$(b) \quad Q^{(h)\varepsilon} \geq (r_h + 1)l \quad (1 \leq h \leq m),$$

$$(c) \quad r_1 \log Q^{(1)} \leq r_h \log Q^{(h)} \leq (1 + \varepsilon)r_1 \log Q^{(1)} \quad (1 \leq h \leq m).$$

Schließlich seien für $h = 1, \dots, m$ je $l-1$ linear unabhängige Vektoren $w_1^{(h)}, \dots, w_{l-1}^{(h)}$ im R_l mit ganzrationalen Koordinaten gegeben, so daß

$$(d) \quad |L^{(i)}(w_j^{(h)})| \leq Q^{(h)c_i} \quad (1 \leq i \leq l; 1 \leq j \leq l-1; 1 \leq h \leq m).$$

Ist nun $M_h = M\{w_1^{(h)}, \dots, w_{l-1}^{(h)}\}$, so hat P bezüglich $(M_1, \dots, M_m; r_1, \dots, r_m)$ mindestens Index

$m\varepsilon$.

Beweis. Wir bezeichnen die durch $w_1^{(h)}, \dots, w_{l-1}^{(h)}$ aufgespannte Hyperebene des R_l mit H_h . $\mathfrak{X} = (X_1, \dots, X_l) \in H_h$ genau dann, wenn $M_h(\mathfrak{X}) = 0$ ist. T sei der Teilraum aller $(\mathfrak{X}_1, \dots, \mathfrak{X}_m) = (X_{11}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml})$ mit $\mathfrak{X}_h \in H_h$ ($h = 1, \dots, m$).

Zahlen s_1, \dots, s_m seien so gewählt, daß $\partial L^{(l)}/\partial X_{s_i} \neq 0$ ($i = 1, \dots, m$). Nach Hilfssatz 7 genügt es zu zeigen, daß $P^{(\tau)}$ für $\tau = (s_1, \dots, s_m; j_1, \dots, j_m)$ und $\sum_{h=1}^m j_h r_h^{-1} < \varepsilon m$ auf T identisch verschwindet. Ist

$$\varrho_h = \varrho(r_h; \mathfrak{w}_1^{(h)}, \dots, \mathfrak{w}_{l-1}^{(h)}),$$

so genügt es daher infolge Hilfssatz 11, nachzuweisen, daß

$$P^{(\tau)}(\mathfrak{v}_1, \dots, \mathfrak{v}_m) = 0 \text{ für } \mathfrak{v}_h \in \varrho_h \quad (h = 1, \dots, m).$$

Nun ist $P^{(\tau)}(\mathfrak{v}_1, \dots, \mathfrak{v}_m)$ gleich

$$\sum d^{(\tau)}(\dots) L^{(1)}(\mathfrak{v}_1)^{i_{11}} \dots L^{(l)}(\mathfrak{v}_1)^{i_{1l}} \dots L^{(1)}(\mathfrak{v}_m)^{i_{m1}} \dots L^{(l)}(\mathfrak{v}_m)^{i_{ml}}. \quad (2)$$

Dabei ist nach (b) und (d)

$$|L^{(j)}(\mathfrak{v}_h)| \leq Q^{(h)c_j}(r_h + 1) l \leq Q^{(h)(c_j + \varepsilon)} \quad (1 \leq j \leq l, 1 \leq h \leq m),$$

also

$$|L^{(j)}(\mathfrak{v}_1)^{i_{1j}} \dots L^{(j)}(\mathfrak{v}_m)^{i_{mj}}| \leq (Q^{(1)i_{1j}} \dots Q^{(m)i_{mj}})^{c_j + \varepsilon}.$$

Weiter ist für die Indices i_{11}, \dots, i_{ml} , für die $d^{(\tau)}(i_{11}, \dots, i_{ml}) \neq 0$ ist nach (iii) des Polynomsatzes und nach (c)

$$\sum_{h=1}^m i_{hj} \log Q^{(h)} \geq r_1 \log Q^{(1)} \sum_{h=1}^m i_{hj} r_h^{-1} \geq r_1 \log Q^{(1)} (l^{-1} - 2l\varepsilon) m > r_1 \log Q^{(1)} (l^{-1} - 4l\varepsilon) m,$$

$$\begin{aligned} \sum_{h=1}^m i_{hj} \log Q^{(h)} &\leq (1 + \varepsilon) r_1 \log Q^{(1)} \sum_{h=1}^m i_{hj} r_h^{-1} \leq r_1 \log Q^{(1)} (l^{-1} + 2l\varepsilon) (1 + \varepsilon) m \\ &\leq r_1 \log Q^{(1)} (l^{-1} + 4l\varepsilon) m, \end{aligned}$$

$$\text{somit} \quad \left| \sum_{h=1}^m i_{hj} \log Q^{(h)} - r_1 \log Q^{(1)} l^{-1} m \right| \leq 4l m \varepsilon r_1 \log Q^{(1)} \quad (1 \leq j \leq l).$$

Hieraus folgt

$$\begin{aligned} \left| (c_j + \varepsilon) \sum_{h=1}^m i_{hj} \log Q^{(h)} - c_j r_1 \log Q^{(1)} l^{-1} m \right| &\leq \varepsilon 4l m r_1 \log Q^{(1)} (|c_j| + \varepsilon + (4l^2)^{-1}) \\ &\leq \varepsilon 4l m r_1 \log Q^{(1)} (c_j + 2) \quad (1 \leq j \leq l). \end{aligned}$$

$$\text{Daher ist} \quad |L^{(j)}(\mathfrak{v}_1)^{i_{1j}} \dots L^{(j)}(\mathfrak{v}_m)^{i_{mj}}| \leq Q^{(1)r_1(l^{-1}mc_j + \varepsilon lm(4c + 8))},$$

also jeder Summand von (2) höchstens gleich

$$\begin{aligned} E^{r_1 + \dots + r_m} Q^{(1)r_1 m(l^{-1}(c_1 + \dots + c_l) + \varepsilon l^2(4c + 8))} \\ \leq E^{r_1 + \dots + r_m} Q^{(1) - r_1 m l^2 \varepsilon} \leq E^{r_1 + \dots + r_m} (Q^{(1) - r_1 \varepsilon} \dots Q^{(m) - r_m \varepsilon})^{1/(1 + \varepsilon)} \\ \leq (E Q^{(1) - \varepsilon/2})^{r_1} \dots (E Q^{(m) - \varepsilon/2})^{r_m} \end{aligned}$$

infolge (iv) des Polynomsatzes, sowie infolge (1) und (c). Da die Summe (2) weniger als $2^{r_1 + \dots + r_m}$ Summanden besitzt, folgt hieraus wegen (a)

$$|P^{(r)}(v_1, \dots, v_m)| \leq \prod_{h=1}^m (2^r E Q^{(h) - \epsilon/2})^{r_h} < 1.$$

Da aber $P^{(r)}(v_1, \dots, v_m)$ ganzrational ist, muß $P^{(r)}(v_1, \dots, v_m) = 0$ sein, und alles ist bewiesen.

4.4. *Der Linearformensatz.* Im folgenden sind ξ_1, \dots, ξ_n ganzzahlig. Gegeben seien $l = n + 1$ Linearformen $L^{(1)}, \dots, L^{(l)}$ in X_1, \dots, X_l und l reelle Zahlen c_1, \dots, c_l mit $c_1 + \dots + c_l < 0$, die eine der folgenden beiden Bedingungen (I) und (II) erfüllen.

(I) Die Zahlen $1, \xi_1, \dots, \xi_n$ sind linear unabhängig über \mathbb{Q} , und $L^{(1)}, \dots, L^{(l)}$ sind von der Gestalt

$$\begin{aligned} L^{(1)} &= X_1 - \xi_1 X_{n+1}, \\ &\dots \\ L^{(n)} &= X_n - \xi_n X_{n+1}, \\ L^{(l)} &= X_{n+1}. \end{aligned}$$

Weiter ist $c_1 = -a_1, \dots, c_n = -a_n, c_l = 1$, wobei $a_i > 0$ ($i = 1, \dots, n$) und $a_1 + \dots + a_n > 1$ ist.

(II) Die Zahlen ξ_1, \dots, ξ_n sind alle irrational, und es ist

$$\begin{aligned} L^{(1)} &= X_1, \\ &\dots \\ L^{(n)} &= X_n, \\ L^{(l)} &= \xi_1 X_1 + \dots + \xi_n X_n - X_{n+1}. \end{aligned}$$

Weiter ist $c_1 = b_1, \dots, c_n = b_n, c_l = -1$, wobei $b_i > 0$ ($i = 1, \dots, n$) und $b_1 + \dots + b_n < 1$ ist.

SATZ 10 (*Linearformensatz*). $L^{(1)}, \dots, L^{(l)}; c_1, \dots, c_l$ seien von der Form (I) oder (II). Es sei $Q > 1$ und es gebe $n = l - 1$ linear unabhängige Vektoren w_1, \dots, w_{l-1} im R_l mit ganzrationalen Koordinaten, die

$$|L^{(i)}(w_j)| \leq Q^{\epsilon_i} \quad (1 \leq i \leq l, 1 \leq j \leq l - 1 = n). \tag{3}$$

erfüllen. Wir bilden $M = M\{w_1, \dots, w_{l-1}\}$. Dann ist

$$\gamma_1 Q^{\gamma_2} \leq \langle M \rangle \leq \gamma_3 Q^{\gamma_4}, \tag{4}$$

wobei $\gamma_1, \dots, \gamma_4$ von Q unabhängige positive Konstante sind.

Bemerkung. Für $Q \geq 2$ gilt somit eine Abschätzung $Q^{\nu} \leq \langle M \rangle \leq Q^{\nu}$.

Beweis. Es sei etwa $w_i = (w_{i1}, \dots, w_{in}, w_{il})$ ($i = 1, \dots, n$). Wir bilden die Matrix

$$W = \begin{pmatrix} w_{11} & \dots & w_{1n} & w_{1l} \\ \cdot & \cdot & \cdot & \cdot \\ w_{n1} & \dots & w_{nn} & w_{nl} \end{pmatrix}.$$

Nach Voraussetzung hat diese Matrix Rang n . Mit W_j bezeichnen wir die $n \times n$ -Teilmatrix, die aus W durch Weglassen der j -ten Spalte entsteht ($j = 1, \dots, n, l$), mit $|W_j|$ den Betrag der Determinante von W_j . Ist $M = m_1 X_1 + \dots + m_l X_l$, so ist m_j ein Teiler von $|W_j|$, somit $|m_j| \leq |W_j|$ ($j = 1, \dots, l$). Wir betrachten nun die Fälle (I) und (II) getrennt.

(I). Wir zeigen hier $\gamma_1 Q^{a/\Theta} \leq \langle M \rangle \leq \gamma_3 Q^n$, wobei $a = \text{Min}(a_1, \dots, a_n) > 0$, $\Theta = \text{Körpergrad von } \mathbf{Q}(\xi_1, \dots, \xi_n) = K$.

Wir setzen $C = \text{Max}(|\xi_1|, \dots, |\xi_n|)$. Aus (3) folgt nun $|w_{il}| \leq Q$ ($i = 1, \dots, n$), sowie

$$|w_{ij}| \leq C|w_{il}| + Q^{-a_j} \leq CQ + 1 \leq (C+1)Q \quad (i = 1, \dots, n; j = 1, \dots, n).$$

Jedes Matrixelement von W hat also einen Absolutbetrag, der kleiner oder gleich $(C+1)Q$ ist, und hieraus folgt $|W_j| \leq n!(C+1)^n Q^n$, $|W_j| \leq \gamma_3 Q^n$, also $\langle M \rangle \leq \gamma_3 Q^n$.

Zum Beweis der unteren Schranke benützen wir bloß, daß es ein i gibt, so daß $M(w_i) = 0$ ist. Wir benützen o. B. d. A. die Tatsache, daß $M(w_1) = 0$ ist, also

$$m_1 w_{11} + \dots + m_n w_{1n} + m_l w_{1l} = 0 \quad (5)$$

gilt. Dabei ist $w_{1l} \neq 0$, denn aus $w_{1l} = 0$ folgte nach (3) $w_{1j} = 0$ für jedes j , daher $w_1 = 0$. Unter neuerlicher Benützung von (3) schließen wir aus (5), daß

$$|(m_1 \xi_1 + \dots + m_n \xi_n + m_l) w_{1l}| \leq |m_1| Q^{-a_1} + \dots + |m_n| Q^{-a_n} \leq n \langle M \rangle Q^{-a}.$$

Bildet man $\eta = m_1 \xi_1 + \dots + m_n \xi_n + m_l$, so gilt also

$$|\eta| \leq n \langle M \rangle Q^{-a}.$$

Sind $\eta_1 = \eta, \eta_2, \dots, \eta_\Theta$ die Konjugierten von η in K , so gilt $|\eta_j| \leq \gamma_7 \langle M \rangle$, wobei γ_7 nur von den Zahlen ξ_1, \dots, ξ_n abhängt. Ist N die Normfunktion von K über \mathbf{Q} , so ist daher

$$1 \leq |N(\eta)| \leq (\gamma_7 \langle M \rangle)^{\Theta-1} n \langle M \rangle Q^{-a} = \langle M \rangle^\Theta Q^{-a} \gamma_8.$$

Dabei gilt $1 \leq |N(\eta)|$ deshalb, weil $1, \xi_1, \dots, \xi_n$ l. u. über \mathbf{Q} sind, und daher $\eta \neq 0$ ist, und weil weiter η ganzzahlig ist. Aus der letzten Ungleichung folgt sofort $\langle M \rangle \geq \gamma_1 Q^{a/\Theta}$.

(II). Wir zeigen nun $\gamma_1 Q^{1/n\Lambda} \leq \langle M \rangle \leq \gamma_3 Q^{nb}$, wobei

$$b = \text{Max}(b_1, \dots, b_n), \quad \Lambda = \text{Max}(\Lambda_1, \dots, \Lambda_n)$$

und Λ_i der Grad von ξ_i über \mathbf{Q} ist.

Wieder sei $C = \text{Max}(|\xi_j|)$. Aus (3) folgt jetzt $|w_{ij}| \leq Q^{b_j}$ ($1 \leq i \leq n, 1 \leq j \leq n$), somit $|w_{il}| \leq |\xi_1| Q^{b_1} + \dots + |\xi_n| Q^{b_n} + Q^{-1} \leq nCQ^b + 1$. Jedes Matrixelement von W ist dem Betrag nach kleiner oder gleich $(nC + 1) Q^b$. Daher ist $|W_j| \leq n! (nC + 1)^n Q^{bn} = \gamma_3 Q^{nb}$ ($j = 1, \dots, l$), folglich $\langle M \rangle \leq \gamma_3 Q^{nb}$.

Um die untere Schranke nachzuweisen, zeigen wir zuerst, daß W_l nichtsingulär ist, daß also $|W_l| \geq 1$ gilt, falls $n! Q^{b_1 + \dots + b_{n-1}} < 1$, also falls $Q > Q_0$ ist. Angenommen, W_l hätte Rang $n - 1$ trotz $Q > Q_0$. O.B.d.A. dürfen wir annehmen, die aus den ersten $n - 1$ Zeilen und Spalten von W_l gebildete Teilmatrix sei nicht singulär. Wir bilden die Matrix

$$U = \begin{pmatrix} w_{11} & \dots & w_{1\ n-1} \\ \dots & \dots & \dots \\ w_{n-1\ 1} & \dots & w_{n-1\ n-1} \\ w_{n\ 1} & \dots & w_{n\ n-1} \end{pmatrix}$$

und setzen u_i ($1 \leq i \leq n$) für die mit $(-1)^i$ multiplizierte Determinante der $(n - 1) \times (n - 1)$ Teilmatrix von U , die durch Weglassen der i -ten Zeile entsteht. Dann ist $u_n \neq 0$,

$$|u_i| \leq (n - 1)! Q^{b_1 + \dots + b_{n-1}} < (n - 1)! Q^{b_1 + \dots + b_n} \quad (i = 1, \dots, n).$$

Es bestehen die Gleichungen

$$u_1 w_{1j} + \dots + u_n w_{nj} = 0 \quad (j = 1, \dots, n). \tag{6}$$

Wegen (3) folgt hieraus

$$|u_1 w_{1l} + \dots + u_n w_{nl}| \leq (|u_1| + \dots + |u_n|) Q^{-1} \leq n! Q^{b_1 + \dots + b_{n-1}} < 1.$$

Somit wäre (6) auch für $j = l$ erfüllt, im Widerspruch zur Tatsache, daß W Rang n besitzt.

Es gelten die Gleichungen

$$m_1 w_{i1} + \dots + m_n w_{in} + m_i w_{il} = 0 \quad (i = 1, \dots, n).$$

Unter Zuhilfenahme von (3) erhält man hieraus

$$\begin{aligned} |m_1 w_{i1} + \dots + m_n w_{in} + m_i (\xi_1 w_{i1} + \dots + \xi_n w_{in})| &\leq |m_i| Q^{-1} \leq \langle M \rangle Q^{-1}, \\ |w_{i1} (m_1 + \xi_1 m_i) + \dots + w_{in} (m_n + \xi_n m_i)| &\leq \langle M \rangle Q^{-1} \quad (i = 1, \dots, n). \end{aligned} \tag{7}$$

Da W_l nichtsingulär ist, muß $m_i \neq 0$ sein.

Nun sei o.B.d.A. $b = b_n$. Dann ist $b_1 + \dots + b_{n-1} \leq 1 - 1/n$. Durch Auflösung des Ungleichungssystems (7) nach der Cramerschen Regel findet man

$$|W_i| |m_n + \xi_n m_i| \leq \langle M \rangle Q^{-1} (|u_1| + \dots + |u_n|).$$

Es ist $|u_i| \leq (n-1)! Q^{b_1 + \dots + b_{n-1}} \leq (n-1)! Q^{1-1/n}$. Hieraus folgt für $\eta = m_n + \xi_n m_i$, $Q > Q_0$

$$|\eta| \leq n! \langle M \rangle Q^{-1/n}.$$

Sind $\eta_1 = \eta, \eta_2, \dots, \eta_{\Delta_n}$ die Konjugierten von η in $K_n = \mathbf{Q}(\xi_n)$, so gilt $|\eta_i| \leq \gamma_7 \langle M \rangle$. Ist N die Norm von K_n über \mathbf{Q} , so ist

$$1 \leq |N(\eta)| \leq (\gamma_7 \langle M \rangle)^{\Delta_n - 1} n! \langle M \rangle Q^{-1/n} \leq \gamma_8 \langle M \rangle^{\Delta_n} Q^{-1/n},$$

und daher schließlich $\langle M \rangle \geq \gamma_1 Q^{1/n \Delta_n}$.

5. Eine Variante des Rothschen Lemmas

5.1. Der Rothsche Index. $P(X_1, \dots, X_m)$ sei ein Polynom, $\sigma = (\sigma_1, \dots, \sigma_m)$ ein Punkt im R_m , r_1, \dots, r_m seien natürliche Zahlen.

Roth definiert den Index von P in σ bezüglich (r_1, \dots, r_m) wie folgt: Ist $P \not\equiv 0$, so ist der Index die kleinste Zahl c , so daß es nichtnegative ganze i_1, \dots, i_m gibt, so daß $\sum_{h=1}^m i_h r_h^{-1} = c$, und daß

$$\frac{\partial^{i_1 + \dots + i_m}}{\partial X_1^{i_1} \dots \partial X_m^{i_m}} P$$

im Punkt σ nicht verschwindet. Ist $P \equiv 0$, so ist der Index $+\infty$. Wir werden diesen Index *Rothschen Index* nennen.

HILFSSATZ 12 (Rothsches Lemma). Sei $0 < \varepsilon < 1/12$, m natürlich,

$$\omega = \omega(m, \varepsilon) = 24 \cdot 2^{-m} (\varepsilon/12)^{2^m - 1}. \quad (1)$$

Seien r_1, \dots, r_m natürliche Zahlen, so daß

$$\omega r_h \geq r_{h+1} \quad (1 \leq h < m). \quad (2)$$

Sei $0 < C \leq 1$, und seien $q_h \neq 0, p_h$ Paare relativ primärer ganzzahliger Zahlen, so daß

$$|q_h|^{r_h} \geq |q_1|^{r_1 C} \quad (1 \leq h \leq m), \quad (3)$$

$$|q_h|^{\omega C} \geq 2^{3m} \quad (1 \leq h \leq m). \tag{4}$$

Sei $P(X_1, \dots, X_m) \equiv 0$ ein Polynom mit ganzrationalen Koeffizienten, das in X_h höchstens Grad r_h besitzt ($1 \leq h \leq m$), und so daß

$$|P| \leq |q_1|^{\omega r_1 C}, \tag{5}$$

wobei $|P|$ den maximalen Absolutbetrag der Koeffizienten von P bedeutet.

Dann hat P höchstens Rothschen Index ε in $(p_1/q_1, \dots, p_m/q_m)$ bezüglich (r_1, \dots, r_m) .

Beweis. Hilfssatz 12 ist fast genau das Rothsche Lemma, wie es etwa in Cassels [1] (Chapter VI, Th. 4) wiedergegeben ist. Wir haben nur einerseits die Bedingung $q_h > 0$ durch $q_h \neq 0$ ersetzt, und daher an einigen Stellen q_h durch $|q_h|$ ersetzen müssen. Offenbar bereitet diese Verallgemeinerung keine Schwierigkeit, da man ja, falls $q_h < 0$ ist, q_h, p_h durch $-q_h, -p_h$ ersetzen kann. Andererseits beweist Roth (und Cassels in [1]) das Lemma nur für $C=1$. Man muß daher im Beweis folgende Änderungen vornehmen:

Für $m=1$ wird (3) nicht gebraucht, und die Voraussetzungen (4), (5) sind für $C < 1$ stärker als für $C=1$. Also ist unsere Behauptung für $m=1$ richtig.

Im Induktionsschritt nach m ist folgendes zu beachten. An Stelle von

$$|S_{i_1 \dots i_{m-1}, j-1}| \leq 2^{r_1 + \dots + r_m} |q_1|^{\omega r_1}$$

(siehe Cassels [1], Seite 115) tritt nun

$$|S_{i_1 \dots i_{m-1}, j-1}| \leq 2^{r_1 + \dots + r_m} |q_1|^{\omega r_1 C},$$

dann weiter

$$|\bar{W}| \leq (2^{3m} |q_1|^{\omega C})^{r_1 h} \leq |q_1|^{2 \omega r_1 C h}$$

infolge (4). An die Stelle der Formel (21) in [1], Chapter VI, tritt

$$|\bar{u}| \leq |q_1|^{2 \omega r_1 C h}, \quad |\bar{v}| \leq |q_1|^{2 \omega r_1 C h}.$$

Genau so wie in Cassels [1] schließt man nun, daß der Index von $v(X_1, \dots, X_{m-1})$ als Funktion von X_1, \dots, X_m in $(p_1/q_1, \dots, p_m/q_m)$ bezüglich (r_1, \dots, r_m) höchstens gleich $h \varepsilon^2/12$ ist. ([1], Seite 116, Zeilen 5-12).

Aus $|\bar{u}| \leq |q_1|^{2 \omega r_1 C h}$ folgt $|\bar{u}| \leq |q_m|^{2 \omega r_m h}$. Man kann nun den Satz mit 1 an Stelle von m , $h r_m$ an Stelle von r_1 , $\varepsilon^2/12$ an Stelle von ε und $C=1$ auf $u(X_m)$ anwenden. Der Index von $u(X_m)$ in $(p_1/q_1, \dots, p_m/q_m)$ bezüglich (r_1, \dots, r_m) ist daher höchstens $h \varepsilon^2/12$ ([1], Seite 116, Zeilen 13-17).

Alles weitere geht wie in [1].

5.2. Ein Hilfssatz.

HILFSSATZ 13. Seien m_1, \dots, m_l relativ prim, $m_1 \neq 0$. Dann gibt es ein j , $2 \leq j \leq l$, so daß

$$(m_1, m_j) \stackrel{\text{Def}}{=} \text{g. g. T. } (m_1, m_j) \leq |m_1|^{(d-2)/(d-1)}.$$

Beweis. Setze $d_j = (m_1, m_j)$ ($2 \leq j \leq l$). Da d_2, \dots, d_l relativ prim sind, kann ein Primfaktor p höchstens in $l-2$ der d_j vorkommen. Da weiter $d_j | m_1$ (d.h. „ d_j teilt m_1 “) ($2 \leq j \leq l$), ist $(d_2 d_3 \dots d_l) | m_1^{l-2}$, somit $d_2 d_3 \dots d_l \leq |m_1|^{l-2}$. Hieraus folgt die Behauptung.

5.3. Die Variante.

SATZ 11 (Rothsches Linearformenlemma). Sei wieder $0 < \varepsilon < 1/12$, m natürlich,

$$\omega = 24 \cdot 2^{-m} (\varepsilon/12)^{2^{m-1}}. \quad (6)$$

r_1, \dots, r_m seien natürlich, und es gelte

$$\omega r_h \geq r_{h+1} \quad (1 \leq h < m). \quad (7)$$

Es sei $l = n + 1 \geq 2$, und $M_h = m_{h1} X_{h1} + \dots + m_{hl} X_{hl}$ ($1 \leq h \leq m$) seien Linearformen mit ganzrationalen, relativ primen Koeffizienten. Es sei $0 < T \leq n$ und es gelte

$$\langle M_h \rangle^{r_h} \geq \langle M_1 \rangle^{r_1 T} \quad (1 \leq h \leq m), \quad (8)$$

$$\langle M_h \rangle^{\omega T} \geq 2^{3mn^2} \quad (1 \leq h \leq m). \quad (9)$$

Schließlich sei $P(X_{11}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml})$ ein nicht identisch verschwindendes Polynom mit ganzrationalen Koeffizienten, das in den Variablen X_{h1}, \dots, X_{hl} eine Form vom Grad r_h ist ($1 \leq h \leq m$), so daß

$$|P|^{n^2} \leq \langle M_1 \rangle^{\omega r_1 T} \quad (10)$$

erfüllt sei. Dann ist der Index von P bezüglich $(M_1, \dots, M_m; r_1, \dots, r_m)$ höchstens gleich ε .

Beweis. Man darf o.B.d.A. annehmen, es sei $\langle M_h \rangle = |m_{h1}|$ ($h = 1, \dots, m$). Nach Hilfssatz 13 darf man weiter annehmen, es gelte

$$(m_{h1}, m_{h2}) \leq \langle M_h \rangle^{(d-2)/(d-1)} = \langle M_h \rangle^{(n-1)/n} \quad (h = 1, \dots, m). \quad (11)$$

Angenommen, P habe bezüglich $(M_1, \dots, M_m; r_1, \dots, r_m)$ einen Index größer als ε . Dann liegt P im Ideal $I_+(\varepsilon)$, das durch alle Polynome

$$M_1^{i_1} \dots M_m^{i_m}$$

mit $\sum i_n r_n^{-1} > \varepsilon$ erzeugt wird.

Wir wollen nun eine Form $P^0(X_{11}, X_{12}; \dots; X_{m1}, X_{m2})$ in $2m$ Variablen konstruieren. Ist $l=2$, so setzen wir $P^0 = P$. Ansonst müssen wir erst die $z = m(l-2)$ Variablen $X_{13}, \dots, X_{1l}; \dots; X_{m3}, \dots, X_{ml}$ los werden!

Man kann P als Polynom in $M_1, X_{12}, \dots, X_{1l}; \dots; M_m, X_{m2}, \dots, X_{ml}$ ausdrücken. Falls X_{13}^a das Polynom P teilt, aber X_{13}^{a+1} nicht mehr P teilt, setzen wir $\bar{P} = X_{13}^{-a} P$. Dann liegt \bar{P} wieder in $I_+(\varepsilon)$. Weiter bilden wir

$$P^{(1)} = \bar{P}(X_{11}, X_{12}, 0, X_{14}, \dots, X_{1l}; \dots; X_{m1}, X_{m2}, \dots, X_{ml}).$$

Dann ist $P^{(1)}$ ein nicht identisch verschwindendes Polynom in $lm-1$ Variablen mit ganzrationalen Koeffizienten, und zwar ist $P^{(1)}$ eine Form in $X_{11}, X_{12}, X_{14}, \dots, X_{1l}$ vom Grad $r_1 - a \leq r_1$ und eine Form in X_{h1}, \dots, X_{hl} vom Grad r_h ($2 \leq h \leq m$). Weiter ist $|P^{(1)}| \leq |P|$. Schließlich liegt $P^{(1)}$ im Ring der Polynome in

$$X_{11}, X_{12}, X_{14}, \dots, X_{1l}; \dots; X_{m1}, \dots, X_{ml}$$

im Ideal $I_+^{(1)}(\varepsilon)$, das durch die Polynome

$$M_1(X_{11}, X_{12}, 0, X_{14}, \dots, X_{1l})^{i_1} \dots M_m(X_{m1}, \dots, X_{ml})^{i_m}$$

mit $\sum_{h=1}^m i_h r_h^{-1} > \varepsilon$ erzeugt wird.

Indem man dieses Verfahren z mal durchführt, erhält man schließlich ein Polynom $P^{(z)} = P^0(X_{11}, X_{12}; \dots; X_{m1}, X_{m2})$, das nicht identisch verschwindet, ganzrationale Koeffizienten besitzt, in X_{h1}, X_{h2} eine Form von einem Grad $\leq r_h$ ist ($1 \leq h \leq m$), $|P^{(z)}| \leq |P|$ leistet, und das im Ideal $I_+^0(\varepsilon)$ liegt, das von den Polynomen

$$(m_{11} X_{11} + m_{12} X_{12})^{i_1} \dots (m_{m1} X_{m1} + m_{m2} X_{m2})^{i_m}$$

mit $\sum i_h r_h^{-1} > \varepsilon$ erzeugt wird.

Nun definieren wir ein Polynom $\tilde{P}(X_1, \dots, X_m)$ in m Variablen durch

$$\tilde{P}(X_1, \dots, X_m) = P^0(X_1, 1; \dots; X_m, 1).$$

\tilde{P} besitzt ganze Koeffizienten und hat in X_h einem Grad $\leq r_h$ ($1 \leq h \leq m$). Man findet

$$\tilde{P} \neq 0, \quad |\tilde{P}| \leq |P|.$$

\tilde{P} liegt im Ideal $\tilde{I}_+(\varepsilon)$, das von den Polynomen

$$(X_1 + m_{12}/m_{11})^{i_1} \dots (X_m + m_{m2}/m_{m1})^{i_m} \tag{12}$$

mit $\sum i_h r_h^{-1} > \varepsilon$ erzeugt wird.

Wir setzen

$$q_h = m_{h1}(m_{h1}, m_{h2})^{-1}, \quad p_h = -m_{h2}(m_{h1}, m_{h2})^{-1} \quad (1 \leq h \leq m).$$

Die Polynome (12) können jetzt auch in der Gestalt

$$(X_1 - p_1/q_1)^{i_1} \dots (X_m - p_m/q_m)^{i_m}$$

geschrieben werden. Für j_1, \dots, j_m mit $\sum j_h r_h^{-1} \leq \varepsilon$ ist daher

$$\frac{\partial^{j_1 + \dots + j_m}}{\partial X_1^{j_1} \dots \partial X_m^{j_m}} \tilde{P}$$

in $(p_1/q_1, \dots, p_m/q_m)$ gleich Null. Das bedeutet aber doch, daß \tilde{P} in $(p_1/q_1, \dots, p_m/q_m)$ bezüglich (r_1, \dots, r_m) einen Rothschen Index größer als ε besitzt.

Dies wird einen Widerspruch ergeben, sobald wir gezeigt haben, daß \tilde{P}, q_h, p_h die Voraussetzungen vom Hilfssatz 12 (Rothsches Lemma) mit $C = T/n$ erfüllen. Offenbar ist $q_h \neq 0$ und sind p_h, q_h relativ prim ($1 \leq h \leq m$). Es ist infolge (11)

$$\langle M_h \rangle^{1/n} \leq |q_h| \leq \langle M_h \rangle \quad (h = 1, \dots, m),$$

also gilt

$$|q_h|^{r_h} \geq \langle M_h \rangle^{r_h/n} \geq \langle M_1 \rangle^{r_1 T/n} \geq |q_1|^{r_1 T/n} = |q_1|^{r_1 C},$$

also (3). Weiter ist (4) erfüllt, denn

$$|q_h|^{\omega C} = |q_h|^{\omega T/n} \geq |M_h|^{\omega T/n^2} \geq 2^{3m} \quad (h = 1, \dots, m).$$

Schließlich ist

$$|\tilde{P}| \leq |P| \leq |M_1|^{\omega r_1 T/n^2} = |M_1|^{\omega r_1 C/n} \leq |q_1|^{\omega r_1 C},$$

und (5) wird erfüllt.

6. Beweis der Sätze 3 und 4

6.1. Neuformulierung.

SATZ 12. Seien ξ_1, \dots, ξ_n algebraisch, $\delta > 0$. $L^{(1)}, L^{(2)}, \dots, L^{(l)}$, wobei $l = n + 1$, seien Linearformen in X_1, \dots, X_l , von der Gestalt (I) oder (II) aus § 4.4.

Wir betrachten die Menge \mathcal{M} der positiven reellen Zahlen Q , so daß es reelle Zahlen c_1, \dots, c_l mit

$$c_1 + \dots + c_l \leq -\delta \tag{1}$$

gibt, so daß im Fall (I) $c_1 = -a_1 \leq 0, \dots, c_n = -a_n \leq 0, c_l = 1$, im Fall (II) $c_1 = b_1 \geq 0, \dots$

$c_n = b_n \geq 0, c_1 = -1$ ist⁽¹⁾ sowie $n = l - 1$ linear unabhängige Vektoren w_1, \dots, w_n im R_l mit ganzrationalen Koordinaten gibt, so daß

$$|L^{(i)}(w_j)| \leq Q^{c_i} \quad (1 \leq i \leq l, 1 \leq j \leq n) \quad (2)$$

ist.

Dann hat \mathcal{M} Eigenschaft F.

FOLGERUNG. Die Sätze 3 und 4 gelten.

Tatsächlich ist Satz 3 genau Fall (I) des obigen Satzes, Satz 4 Fall (II). Um dies einzusehen, braucht man bloß den Vektor w_j in der Form

$$w_j = (p_{j1}, \dots, p_{jn}, p_{j1})$$

zu schreiben.

Es ist also jetzt Satz 12 zu beweisen.

6.2. Erste Zurückführung. Es genügt, Satz 12 für den speziellen Fall zu beweisen, in welchem c_1, \dots, c_l feste Konstante sind, die von Q unabhängig sind.

Um dies einzusehen, betrachtet man die Fälle (I) und (II) separat.

(I) Ist $Q \in \mathcal{M}$, so gibt es $c_1(Q), \dots, c_l(Q)$ mit den angegebenen Eigenschaften, und zwar ist für den Fall (I) $c_1(Q) = -a_1(Q), \dots, c_n(Q) = -a_n(Q), c_l(Q) = 1$, wobei $a_j(Q) \geq 0$ ($j = 1, \dots, n$), und wobei $a_1(Q) + \dots + a_n(Q) \geq 1 + \delta$.

Man darf annehmen, $0 \leq a_j(Q) < 1 + 2\delta$. Ist nämlich ein $a_j(Q) \geq 1 + 2\delta$, so kann man dieses $a_j(Q)$ durch $1 + \delta$ ersetzen, und alle Voraussetzungen bleiben erhalten.

Wir wählen z und Zahlen $0 = \alpha(0) < \alpha(1) < \dots < \alpha(z) = 1 + 2\delta$ so, daß

$$\alpha(i) - \alpha(i-1) < \delta/2n \quad (i = 1, \dots, z),$$

und wir bezeichnen das halboffene Intervall $[\alpha(i-1), \alpha(i))$ mit $I(i)$ ($1 \leq i \leq z$). Ist

$$\sigma = (s_1, \dots, s_n), \quad 1 \leq s_i \leq z, s_i \text{ ganz,}$$

so sei \mathcal{M}^σ die Teilmenge von \mathcal{M} , die aus allen $Q \in \mathcal{M}$ besteht, so daß $a_j(Q) \in I(s_j)$ ($1 \leq j \leq n$). Ist $Q \in \mathcal{M}^\sigma$, so gilt $a_j(Q) \geq \alpha(s_j - 1)$, folglich

$$a_1(Q) + \dots + a_n(Q) \geq \alpha(s_1 - 1) + \dots + \alpha(s_n - 1) \geq a_1(Q) + \dots + a_n(Q) - n\delta/2n \geq 1 + \delta/2.$$

Die Zahlen $Q \in \mathcal{M}^\sigma$ erfüllen daher die Voraussetzungen des Satzes für feste Konstante $c_1 = -\alpha(s_1 - 1), \dots, c_n = -\alpha(s_n - 1)$ und $\delta/2$ an Stelle von δ .

⁽¹⁾ Da nun auch $a_i = 0$ oder $b_i = 0$ zugelassen ist, sind $L^{(1)}, \dots, L^{(l)}$ zusammen mit c_1, \dots, c_l nicht notwendigerweise von der Gestalt (I) oder (II) aus § 4.4.

Ist also der Satz für feste Konstante c_1, \dots, c_n, c_l bewiesen, so hat \mathcal{M}^c Eigenschaft F . Da aber \mathcal{M} Vereinigungsmenge von endlich vielen Teilmengen \mathcal{M}^c ist, hat auch \mathcal{M} selbst Eigenschaft F .

(II) wird ähnlich gezeigt.

6.3. Zweite Zurückführung. Man darf weiter annehmen, $c_j \neq 0$ ($j = 1, \dots, l$). (Dies bedeutet im Fall (I), $-c_1 = a_1 > 0, \dots, -c_n = a_n > 0, c_l = 1$, und im Fall (II) $c_1 = b_1 > 0, \dots, c_n = b_n > 0, c_l = -1$. Nun sind $L^{(1)}, \dots, L^{(l)}$ zusammen mit c_1, \dots, c_l von der Gestalt (I) oder (II) aus § 4.4.) Wir betrachten die Fälle (I), (II) getrennt.

(I) Wir zeigen hier diese Zurückführung durch Induktion nach n . Ist $n = 1$, so ist $a_1 \geq 1 + \delta$, also von vornherein $a_1 > 0$. Im allgemeinen sei etwa $a_n = 0$. Dann ist $a_1 + \dots + a_{n-1} \geq 1 + \delta$, und man kann den Satz mit $n-1$ an Stelle von n anwenden: Man entfernt in der Matrix (4), § 1, die n -te Spalte sowie eine Zeile (welche Zeile wird von Q abhängen), so daß eine $(n-1) \times n$ -Matrix vom Rang $n-1$ übrig bleibt.

(II) ist noch einfacher. Man braucht bloß b_j durch $b'_j = b_j + \delta/2n$ zu ersetzen. Dann ist $b'_j > 0$ ($j = 1, \dots, n$), und alle Voraussetzungen des Satzes mit b'_1, \dots, b'_n an Stelle von b_1, \dots, b_n und $\delta/2$ an Stelle von δ sind erfüllt.

6.4. Dritte Zurückführung. Man darf annehmen, ξ_1, \dots, ξ_n seien ganzzahlgemäß. Dies sieht man so ein: Im allgemeinen Fall gibt es ein natürliches q , so daß $q\xi_1, \dots, q\xi_n$ ganzzahlgemäß sind.

(I) Wir wählen eine Zahl η , so daß $0 < \eta < \text{Min}(a_1, \dots, a_n, \delta/2n)$. Man darf sich auf $Q \in \mathcal{M}$ mit $Q^\eta > q$ beschränken. Aus (2) folgt nun

$$|p_{ji}(\xi_i q) - (p_{ji} q)| \leq Q^{-a_i} q \leq Q^{-(a_i - \eta)} \quad (1 \leq i \leq n, 1 \leq j \leq n).$$

Die Voraussetzungen des Satzes werden nun durch $q\xi_1, \dots, q\xi_n$ an Stelle von ξ_1, \dots, ξ_n , qp_{ji} an Stelle von p_{ji} ($1 \leq i, j \leq n$), $a_i - \eta$ an Stelle von a_i ($1 \leq i \leq n$), sowie $\delta/2$ an Stelle von δ erfüllt. Ist also der Satz für ganzzahlgemäße ξ_1, \dots, ξ_n bereits gezeigt, so folgt, daß \mathcal{M} auch in unserem Fall Eigenschaft F besitzt.

(II) Jedem $Q \in \mathcal{M}$ ordnen wir die Zahl $\tilde{Q} = Qq^{-1}$ zu. Die Menge der so erhaltenen Zahlen \tilde{Q} sei $\tilde{\mathcal{M}}$. Für großes Q ist $q \leq \tilde{Q}^{\delta/2n}$. Aus (2) oder, was dasselbe ist, (8) und (9) aus § 1, folgt nun

$$|p_{ji}| \leq Q^{b_i} = (q\tilde{Q})^{b_i} \leq q\tilde{Q}^{b_i} \leq \tilde{Q}^{(b_i + \delta/2n)} \quad (1 \leq i, j \leq n),$$

sowie $|p_{i1}(q\xi_1) + \dots + p_{in}(q\xi_n) - (qp_{ii})| \leqq qQ^{-1} = \tilde{Q}^{-1} \quad (1 \leqq i \leqq n).$

Die Voraussetzungen des Satzes werden also durch $q\xi_1, \dots, q\xi_n$ an Stelle von ξ_1, \dots, ξ_n , qp_{ii} an Stelle von p_{ii} , $b_j + \delta/2n$ an Stelle von b_j , $\delta/2$ an Stelle von δ , und $\tilde{Q} \in \tilde{\mathcal{M}}$ an Stelle von $Q \in \mathcal{M}$ erfüllt.

Ist der Satz also für ganzalgebraische Zahlen gezeigt, so hat $\tilde{\mathcal{M}}$ Eigenschaft F , nach Hilfssatz 3 also auch \mathcal{M} .

6.5. *Aufmarsch der Hilfsmittel.* Wir wenden uns nun dem Beweis des Satzes zu. c_1, \dots, c_l seien Konstante, die den Voraussetzungen des Satzes genügen. Wir setzen $c = \text{Max}(|c_1|, \dots, |c_l|) > 0$. Wir wählen $\varepsilon > 0$ so klein, daß

$$\varepsilon l^3(4c + 9) < \delta \tag{3}$$

ist. Wenn wir, was offenbar erlaubt ist, $0 < \delta < 1/12$ annehmen, ist auch $0 < \varepsilon < 1/12$. Als nächstes wählen wir m natürlich, und so groß, daß

$$m \geqq 4\varepsilon^{-2} \log(2l\Delta), \tag{4}$$

wobei $\Delta = [\mathbf{Q}(\xi_1, \dots, \xi_n): \mathbf{Q}]$ im Fall (I), $\Delta = \text{Max}([\mathbf{Q}(\xi_i): \mathbf{Q}])$ im Fall (II).

Wir werden nun zeigen: \mathcal{M} hat nicht Eigenschaft LG_m . Daraus folgt offenbar Satz 12.

Im folgenden nehmen wir indirekt an, \mathcal{M} habe Eigenschaft LG_m . Dann gibt es ein k , so daß $L_k \mathcal{M}$ Eigenschaft G_m besitzt.

Wir bilden

$$\omega = 24 \cdot 2^{-m} (\varepsilon/12)^{2m-1}. \tag{5}$$

Infolge $\varepsilon < 1$ und $m \geqq 1$ ist $0 < \omega < 1$, $\omega^{-1} > 1$.

Nach Annahme besitzt $L_k \mathcal{M}$ Eigenschaft G_m . Wir setzen $C_1 = 2\omega^{-1} > 1$. Es gibt nun ein C_2 , so daß es $Q^{(1)} < Q^{(2)} < \dots < Q^{(m)}$ mit beliebig großem $Q^{(1)}$ aus \mathcal{M} gibt, so daß

$$2\omega^{-1} L_k(Q^{(h)}) \leqq L_k(Q^{(h+1)}) \leqq C_2 L_k(Q^{(h)}) \quad (h = 1, \dots, m-1) \tag{6}$$

gilt.⁽¹⁾

Wir wählen Q_0 so groß, daß für $Q \geqq Q_0$ folgende Ungleichungen gelten:

$$(a) \quad Q^\varepsilon \geqq 4l^2 \varepsilon^{-2}, \quad Q^\varepsilon \geqq 2^{2l} E^2,$$

wobei E die Konstante aus (iv) des Polynomsatzes bedeutet. (Die Voraussetzungen dieses Satzes werden durch $L^{(1)}, \dots, L^{(l)}$ erfüllt.)

⁽¹⁾ Eine Verwechslung der iterierten Logarithmen L_k mit Linearform $L^{(1)}, \dots, L^{(l)}$ ist hier wohl kaum zu befürchten.

$$(b) \quad Q^{\gamma_5 \omega} \geq 2^{3m^2 \gamma_6}, \quad Q^{\gamma_6 \omega} \geq D^{m^2 \gamma_6},$$

wobei γ_5, γ_6 Konstanten aus der Bemerkung nach dem Linearformensatz sind, während D die Konstante aus (ii) des Polynomsatzes ist.

$$(c) \quad C_2^{m-1} L_k(Q) \leq L_{k-1}(Q^{\varepsilon/2})$$

$$(d) \quad L(L_t(Q) 2 \omega^{-1}) \leq 2 \omega^{-1} L_{t+1}(Q) \quad (t=0, 1, \dots, k-1).$$

Aus (a) folgt

$$L_k(Q \cdot 2 \omega^{-1}) \leq L_{k-1}(L(Q) \cdot 2 \omega^{-1}) \leq L_{k-2}(L_2(Q) \cdot 2 \omega^{-1}) \leq \dots \leq 2 \omega^{-1} L_k(Q). \quad (7)$$

Nun wählen wir $Q^{(1)}, \dots, Q^{(m)}$ aus \mathcal{M} so, daß (6) gilt und außerdem

$$Q^{(h)} \geq Q_0 \quad (h=1, \dots, m) \quad (8)$$

ist.

Aus (6) und (7) folgt

$$L_{k-1}(L(Q^{(h)}) 2 \omega^{-1}) \leq 2 \omega^{-1} L_k(Q^{(h)}) \leq L_k(Q^{(h+1)}),$$

$$\text{somit} \quad 2 \omega^{-1} L(Q^{(h)}) \leq L(Q^{(h+1)}) \quad (h=1, \dots, m-1). \quad (9)$$

Aus (6) und (c) folgt

$$L_k(Q^{(m)}) \leq C_2^{m-1} L_k(Q^{(1)}) \leq L_{k-1}(Q^{(1)\varepsilon/2}),$$

$$\text{also} \quad L(Q^{(m)}) \leq Q^{(1)\varepsilon/2}. \quad (10)$$

Aus (a) folgt wegen $\varepsilon < 1/12$ sofort $Q \geq e^2$, $\log Q \geq 2$, und infolge (8) ist daher

$$\log Q^{(m)} - \log Q^{(m)}/\log Q^{(1)} \geq 2(1 - \frac{1}{2}) = 1,$$

und wir können eine ganze Zahl r_1 so wählen, daß

$$\varepsilon^{-1} \log Q^{(m)} \geq r_1 \geq \varepsilon^{-1} \log Q^{(m)}/\log Q^{(1)} > 0 \quad (11)$$

ist. Weiter setzen wir für $h=2, \dots, m$

$$r_h = [r_1 \log Q^{(1)}/\log Q^{(h)}] + 1. \quad (12)$$

Dann ist

$$r_1 \log Q^{(1)} \leq r_h \log Q^{(h)} \leq r_1 \log Q^{(1)} + \log Q^{(h)} \leq (1 + \varepsilon) r_1 \log Q^{(1)}. \quad (13)$$

Aus (9) und (13) folgt

$$\begin{aligned} \omega r_h \log Q^{(h)} &\geq (1 + \varepsilon)^{-1} \omega r_{h+1} \log Q^{(h+1)} \geq (1 + \varepsilon)^{-1} \omega r_{h+1} (2 \omega^{-1}) \log Q^{(h)}, \\ \omega r_h &\geq 2(1 + \varepsilon)^{-1} r_{h+1} \geq r_{h+1}, \\ \omega r_h &\geq r_{h+1} \quad (h = 1, \dots, m-1). \end{aligned} \tag{14}$$

Infolge (a), (10) und (11) ist

$$r_1 \leq \varepsilon^{-1} \log Q^{(m)} \leq \varepsilon^{-1} Q^{(1)\varepsilon/2} \leq Q^{(1)\varepsilon}/(2l).$$

Da $Q^{(1)} < \dots < Q^{(m)}$, und da nach (14) $r_1 > \dots > r_m$, gilt allgemein

$$(r_h + 1)l \leq Q^{(h)\varepsilon} \quad (h = 1, \dots, m). \tag{15}$$

6.6. *Ende des Beweises.* Den Beweis von Satz 12 führen wir nun wie folgt zu Ende.

Unsere Linearformen $L^{(1)}, \dots, L^{(l)}, \varepsilon, m$ sowie r_1, \dots, r_m erfüllen die Voraussetzungen des Polynomsatzes. $P(X_{11}, \dots, X_{ml})$ sei das im Polynomsatz beschriebene Polynom.

Aber auch die Voraussetzungen von Satz 9 sind erfüllt. Die erste in diesem Satz vorausgesetzte Ungleichung folgt aus (1), (3). Die Bedingungen (a), (b), (c) von Satz 9 folgen aus unseren Formeln (a), (15), (13). Weiter gibt es für $h = 1, \dots, m$ je $n = l - 1$ l. u. Vektoren $w_1^{(h)}, \dots, w_n^{(h)}$, welche die Bedingungen von Satz 9 erfüllen. $M^{(1)}, \dots, M^{(m)}$ seien die in diesem Satz konstruierten Linearformen. Nach diesem Satz schließen wir also.

P hat mindestens Index $m\varepsilon$ bezüglich $(M_1, \dots, M_m; r_1, \dots, r_m)$.

Nach dem Linearformensatz ist

$$Q^{(h)\gamma_5} \leq \langle M_h \rangle \leq Q^{(h)\gamma_6} \quad (h = 1, \dots, m). \tag{16}$$

Also ist $\langle M_h \rangle^{r_h} \geq Q^{(h)r_h\gamma_5} \geq Q^{(1)r_1\gamma_5} \geq \langle M_1 \rangle^{r_1\gamma_5/\gamma_6},$

und setzt man $T = \frac{\gamma_5}{\gamma_6},$

so folgt $\langle M_h \rangle^{r_h} \geq \langle M_1 \rangle^{r_1 T} \quad (h = 1, \dots, m). \tag{17}$

Weiter ist $\langle M_h \rangle^{\omega T} \geq Q^{(h)\omega T\gamma_5} \geq 2^{3mn^2} \tag{18}$

nach (b), (8) und (16). Nach dem Polynomsatz ist

$$|P| \leq D^{r_1 + \dots + r_m} \leq D^{mr_1},$$

daher nach (b) und (16)

$$|P|^{n^2} \leq D^{mn^2 r_1} \leq Q^{(1)\omega r_1 \gamma_1^2 / \gamma_0} \leq \langle M_1 \rangle^{\omega r_1 \gamma_1^2 / \gamma_0} = \langle M_1 \rangle^{\omega T r_1},$$

also
$$|P|^{n^2} \leq \langle M_1 \rangle^{\omega r_1 T}. \quad (19)$$

$\varepsilon, m, \omega, r_1, \dots, r_m$ erfüllen nach unserer Wahl von ε und ω und nach (14) die Voraussetzungen des Rothschen Linearformenlemmas. Ebenso erfüllen T , die Linearformen M_1, \dots, M_m , sowie das Polynom $P(X_{11}, \dots, X_{ml})$ die Voraussetzungen. Die Bedingungen (8), (9), (10) des Rothschen Lemmas sind unsere Formeln (17), (18), (19). Also sind sämtliche Voraussetzungen erfüllt, und wir sehen:

P hat bezüglich $(M_1, \dots, M_m; r_1, \dots, r_m)$ höchstens Index ε .

Dies steht im Widerspruch zur oben gegebenen Abschätzung des Index nach unten, da infolge (4) $m > 1$ ist. Die in § 6.5 gemachte Annahme, daß \mathcal{M} Eigenschaft LG_m besitzt, wurde so ad absurdum geführt, und \mathcal{M} hat Eigenschaft F .

7. Übertragungssätze

7.1. Erster kleiner Übertragungssatz.

HILFSSATZ 14 (1. kleiner Übertragungssatz). Sei $\varepsilon > 0$, $\sigma_1 > 0$, $\sigma_2 > 0$, $\sigma_1 + \sigma_2 \leq 1$. Dann gibt es Zahlen $\delta > 0$, $\tau_1 > 0$, $\tau_2 > 0$ mit $\delta < 1$,

$$\tau_1 + \tau_2 > \frac{2 - \sigma_1 - \sigma_2 - \varepsilon}{\sigma_1 + \sigma_2} \quad (1)$$

und folgenden Eigenschaften:

Seien ξ_1, ξ_2 reell, $q > 1$, $(p_1, p_2, p_l) \neq (0, 0, 0)$ mit ganzrationalen p_j ($j = 1, 2, l$). Es gelte

$$|p_1| \leq q^{\sigma_1}, \quad |p_2| \leq q^{\sigma_2}, \quad |p_1 \xi_1 + p_2 \xi_2 - p_l| = q^{-1}. \quad (2)$$

Entweder (A) gibt es dann ganzrationale $(v_1, v_2, v_l) \neq (0, 0, 0)$ mit

$$|v_1 \xi_1 - v_l| \leq (Q/2)^{-\tau_1}, \quad |v_1 \xi_2 - v_l| \leq (Q/2)^{-\tau_2}, \quad |v_l| \leq Q, \quad (3)$$

wobei $Q = 2 q^{\delta + \sigma_1 + \sigma_2}$.

Oder (B) es gibt eine ganzrationale Matrix

$$\begin{pmatrix} v_1 & v_2 & v_l \\ v'_1 & v'_2 & v'_l \end{pmatrix}$$

vom Rang 2, so daß

$$\begin{aligned} |v_1 \xi_1 - v_l| &\leq (Q'/2)^{-\alpha_1}, & |v_1 \xi_2 - v_l| &\leq (Q'/2)^{-\alpha_2}, & |v_l| &\leq Q', \\ |v'_1 \xi_1 - v'_l| &\leq (Q'/2)^{-\alpha_1}, & |v'_1 \xi_2 - v'_l| &\leq (Q'/2)^{-\alpha_2}, & |v'_l| &\leq Q', \end{aligned} \quad (4)$$

wobei $a_1 \geq 0, a_2 \geq 0, a_1 + a_2 - 1 \geq \delta > 0$ und

$$Q' = 2q^{1-\delta}.$$

Beweis. Wir wählen $\delta > 0$ so klein, daß $\delta < 1 - \sigma_1, \delta < 1 - \sigma_2$, und

$$\frac{2 - \sigma_1 - \sigma_2 - 2\delta}{\sigma_1 + \sigma_2 + \delta} > \frac{2 - \sigma_1 - \sigma_2}{\sigma_1 + \sigma_2} - \varepsilon. \quad (5)$$

Weiter setzen wir $\tau_1 = \frac{1 - \sigma_2 - \delta}{\sigma_1 + \sigma_2 + \delta}, \tau_2 = \frac{1 - \sigma_1 - \delta}{\sigma_1 + \sigma_2 + \delta}$.

Offenbar gilt nun (1).

Nun sei (2) erfüllt. Wir bilden $f_1 = p_1 q^{-\sigma_1}, f_2 = p_2 q^{-\sigma_2}, f_i = (p_1 \xi_1 + p_2 \xi_2 - p_i) q$. Dann ist $|f_1| \leq 1, |f_2| \leq 1$, aber $|f_i| = 1$.

Wir bilden folgende drei Linearformen in den Variablen v_1, v_2, v_i :

$$g_1 = -(v_1 \xi_1 - v_i) q^{\sigma_1}, \quad g_2 = -(v_1 \xi_2 - v_2) q^{\sigma_2}, \quad g_i = v_i q^{-1}.$$

Weiter bilden wir die Linearform

$$\phi(v_1, v_2, v_i) = f_1 g_1 + f_2 g_2 + f_i g_i = p_1 v_1 + p_2 v_2 - p_i v_i.$$

Die Linearform ϕ besitzt ganzrationale Koeffizienten. Ist also $|\phi(v_1, v_2, v_i)| < 1$ wobei v_1, v_2, v_i ganzrational sind, so folgt $\phi(\dots) = 0$,

$$|g_i| \leq |f_1| |g_1| + |f_2| |g_2| \leq 2 \text{Max}(|g_1|, |g_2|).$$

Die Determinante der 3 Linearformen g_1, g_2, g_i ist $\pm q^{\sigma_1 + \sigma_2 - 1}$, die Determinante von g_1, g_2, ϕ ist ebenfalls $\pm q^{\sigma_1 + \sigma_2 - 1}$.

\mathfrak{K}_v sei der Körper im R_3 , der durch die Ungleichungen

$$|g_1| \leq q^{-v}, \quad |g_2| \leq q^{-v}, \quad |\phi| < 1$$

gegeben ist. \mathfrak{K}_v hat Volumen $2^3 q^{1 - \sigma_1 - \sigma_2 - 2v}$. ν_0 sei die größte Zahl, so daß \mathfrak{K}_{ν_0} Gitterpunkte (d. h. Punkte $v = (v_1, v_2, v_i)$ mit ganzrationalen Koordinaten $v_j \neq 0$) besitzt. Nach dem Minkowskischen Linearformensatz ist

$$2\nu_0 \geq 1 - \sigma_1 - \sigma_2 \geq 0. \quad (6)$$

Sei $v = (v_1, v_2, v_i) \neq (0, 0, 0)$ Gitterpunkte in \mathfrak{K}_{ν_0} . Dann ist dort entweder $|g_1| = q^{-\nu_0}$ oder $|g_2| = q^{-\nu_0}$. Ist o. B. d. A. $|g_1| \geq |g_2|$, so gilt

$$|g_1| = q^{-\nu_0}, \quad |g_2| \leq q^{-\nu_0}, \quad |g_i| \leq 2q^{-\nu_0}, \quad (7)$$

$$\text{also} \quad |v_l \xi_1 - v_1| \leq q^{-\sigma_1 - \nu_0}, \quad |v_l \xi_2 - v_2| \leq q^{-\sigma_2 - \nu_0}, \quad |v_l| \leq 2 q^{1 - \nu_0}. \quad (8)$$

Wir unterscheiden nun zwei Fälle (A) und (B).

(A) $\nu_0 \geq 1 - \sigma_1 - \sigma_2 - \delta$. Nun ist

$$1 - \nu_0 \leq \sigma_1 + \sigma_2 + \delta, \quad \sigma_1 + \nu_0 \geq 1 - \sigma_2 - \delta = \tau_1(\sigma_1 + \sigma_2 + \delta), \quad \sigma_2 + \nu_0 \geq 1 - \sigma_1 - \delta = \tau_2(\sigma_1 + \sigma_2 + \delta).$$

Setzen wir $Q = 2 q^{\sigma_1 + \sigma_2 + \delta}$, so folgt aus (8) gerade (3).

(B) $\nu_0 < 1 - \sigma_1 - \sigma_2 - \delta$. Wir betrachten den Körper \mathfrak{K}' , der durch

$$|g_1| < q^{-\nu_0}, \quad |g_2| \leq q^{\sigma_1 + \sigma_2 - 1 + \nu_0}, \quad |\phi| < 1$$

definiert ist. \mathfrak{K}' hat Volumen 2^3 , und enthält daher nach Minkowski einen primitiven Gitterpunkt $\mathfrak{v}' = (v'_1, v'_2, v'_l)$. (Ein Gitterpunkt $\mathfrak{v} \neq \mathfrak{o}$ heißt *primitiv*, falls seine Koordinaten relativ prim sind.) Da offenbar der oben konstruierte Gitterpunkt \mathfrak{v} ebenfalls primitiv und von $\pm \mathfrak{v}'$ verschieden ist, sind $\mathfrak{v}, \mathfrak{v}'$ linear unabhängig. Wir schreiben

$$g_i = g_i(v_1, v_2, v_l), \quad g'_i = g_i(v'_1, v'_2, v'_l) \quad (i = 1, 2, l).$$

Außer (7) gilt nun

$$|g'_1| \leq q^{-\nu_0}, \quad |g'_2| \leq q^{\sigma_1 + \sigma_2 - 1 + \nu_0}, \quad |g'_l| \leq 2 q^{\sigma_1 + \sigma_2 - 1 + \nu_0}. \quad (9)$$

Aus (7) folgt wieder (8), und aus (9) folgt

$$|v'_l \xi_1 - v'_1| \leq q^{-\sigma_1 - \nu_0}, \quad |v'_l \xi_2 - v'_2| \leq q^{\sigma_1 - 1 + \nu_0}, \quad |v'_l| \leq 2 q^{\sigma_1 + \sigma_2 + \nu_0}. \quad (10)$$

Wegen (6) sind die Schranken (8) schärfer als (10), also gilt noch

$$|v_l \xi_1 - v_1| \leq q^{-\sigma_1 - \nu_0}, \quad |v_l \xi_2 - v_2| \leq q^{\sigma_1 - 1 + \nu_0}, \quad |v_l| \leq 2 q^{\sigma_1 + \sigma_2 + \nu_0}. \quad (11)$$

Setzen wir $Q' = 2 q^{1 - \delta}$, $a_1 = (\sigma_1 + \nu_0)(1 - \delta)^{-1} > 0$, $a_2 = (1 - \sigma_1 - \nu_0)(1 - \delta)^{-1}$, so gilt unter Benützung der Voraussetzung (B): $a_2 \geq (\sigma_2 + \delta)(1 - \delta)^{-1} > 0$, sowie

$$|v_l \xi_1 - v_1| \leq (Q'/2)^{-a_1}, \quad |v_l \xi_2 - v_2| \leq (Q'/2)^{-a_2}, \quad |v_l| \leq Q',$$

$$|v'_l \xi_1 - v'_1| \leq (Q'/2)^{-a_1}, \quad |v'_l \xi_2 - v'_2| \leq (Q'/2)^{-a_2}, \quad |v'_l| \leq Q',$$

also (4). Dabei ist $a_1 + a_2 - 1 = \delta(1 - \delta)^{-1} > \delta$.

7.2. Zweiter kleiner Übertragungssatz.

HILFSSATZ 15 (2. kleiner Übertragungssatz). Sei

$$\varepsilon > 0, 0 \leq \tau_1 \leq 1, 0 \leq \tau_2 \leq 1, \tau_1 + \tau_2 \geq 1.$$

Dann gibt es Zahlen $\delta > 0, \sigma_1 > 0, \sigma_2 > 0$ mit $\delta < 1$,

$$\sigma_1 + \sigma_2 < \frac{2 - \tau_1 - \tau_2}{\tau_1 + \tau_2} + \varepsilon \quad (12)$$

und folgenden Eigenschaften:

Seien ξ_1, ξ_2 reell, $q > 1, (p_1, p_2, p_i) \neq (0, 0, 0)$ mit ganzrationalen p_i . Es gelte

$$|p_i \xi_1 - p_1| \leq q^{-\tau_1}, \quad |p_i \xi_2 - p_2| \leq q^{-\tau_2}, \quad |p_i| = q. \quad (13)$$

Entweder (A) gibt es dann ganzrationale $(v_1, v_2, v_i) \neq (0, 0, 0)$ mit

$$|v_1| \leq (2Q)^{\sigma_1}, \quad |v_2| \leq (2Q)^{\sigma_2}, \quad |v_1 \xi_1 + v_2 \xi_2 - v_i| \leq Q^{-1}, \quad (14)$$

wobei

$$Q = \frac{1}{2} q^{\tau_1 + \tau_2 - \delta}.$$

Oder (B), gibt es eine ganzrationale Matrix

$$\begin{pmatrix} v_1 & v_2 & v_i \\ v'_1 & v'_2 & v'_i \end{pmatrix}$$

vom Rang 2, so daß

$$\begin{aligned} |v_1| &\leq (2Q')^{b_1}, & |v_2| &\leq (2Q')^{b_2}, & |v_1 \xi_1 + v_2 \xi_2 - v_i| &\leq Q'^{-1}, \\ |v'_1| &\leq (2Q')^{b_1}, & |v'_2| &\leq (2Q')^{b_2}, & |v'_1 \xi_1 + v'_2 \xi_2 - v'_i| &\leq Q'^{-1}, \end{aligned} \quad (15)$$

wobei $b_1 \geq 0, b_2 \geq 0, b_1 + b_2 = (1 + \delta)^{-1} < 1$ und

$$Q' = \frac{1}{2} q^{1 + \delta}.$$

Beweis. Wir wählen δ im Intervall $0 < \delta < 1$ so klein, daß

$$\frac{2 - \tau_1 - \tau_2 + 2\delta}{\tau_1 + \tau_2 - \delta} < \frac{2 - \tau_1 - \tau_2}{\tau_1 + \tau_2} + \varepsilon. \quad (16)$$

Weiter sei

$$\sigma_1 = \frac{1 - \tau_2 + \delta}{\tau_1 + \tau_2 - \delta}, \quad \sigma_2 = \frac{1 - \tau_1 + \delta}{\tau_1 + \tau_2 - \delta}.$$

Dann gilt (12).

Wir setzen $f_1 = -(p_i \xi_1 - p_1) q^{\tau_1}, f_2 = -(p_i \xi_2 - p_2) q^{\tau_2}, f_i = p_i q^{-1}$. Dann ist $|f_1| \leq 1, |f_2| \leq 1, |f_i| = 1$.

Wir bilden folgende drei Linearformen in Variablen v_1, v_2, v_i :

$$g_1 = v_1 q^{-\tau_1}, \quad g_2 = v_2 q^{-\tau_2}, \quad g_i = (v_1 \xi_1 + v_2 \xi_2 - v_i) q.$$

Weiter bilden wir $\phi(v_1, v_2, v_l) = f_1 g_1 + f_2 g_2 + f_l g_l = p_1 v_1 + p_2 v_2 - p_l v_l$. Die Linearform ϕ besitzt ganzrationale Koeffizienten. Die Determinante von g_1, g_2, ϕ ist $\pm q^{1-\tau_1-\tau_2}$.

\mathfrak{K}_v sei der durch die Ungleichungen

$$|g_1| \leq q^{-v}, \quad |g_2| \leq q^{-v}, \quad |\phi| < 1$$

definierte Körper im R_3 . \mathfrak{K}_v hat Volumen $2^3 q^{\tau_1+\tau_2-1-2v}$. v_0 sei die größte Zahl, so daß \mathfrak{K}_{v_0} Gitterpunkte $v \neq 0$ enthält. Nach Minkowski ist

$$2v_0 \geq \tau_1 + \tau_2 - 1 \geq 0. \quad (17)$$

Sei $v \neq 0$ Gitterpunkt in \mathfrak{K}_{v_0} . Ist o. B. d. A. für diesen Gitterpunkt $|g_1| \geq |g_2|$, so gilt dort

$$|g_1| = q^{-v_0}, \quad |g_2| \leq q^{-v_0}, \quad |g_l| \leq 2q^{-v_0}, \quad (18)$$

und daraus folgt

$$|v_1| = q^{\tau_1-v_0}, \quad |v_2| \leq q^{\tau_2-v_0}, \quad |v_1 \xi_1 + v_2 \xi_2 - v_l| \leq 2q^{-1-v_0}. \quad (19)$$

Wir unterscheiden nun zwei Fälle (A) und (B).

(A) $v_0 \geq \tau_1 + \tau_2 - 1 - \delta$. Jetzt ist $1 + v_0 \geq \tau_1 + \tau_2 - \delta$,

$$\tau_1 - v_0 \leq 1 + \delta - \tau_2 = \sigma_1(\tau_1 + \tau_2 - \delta); \quad \tau_2 - v_0 \leq 1 + \delta - \tau_1 = \sigma_2(\tau_1 + \tau_2 - \delta).$$

Setzen wir $Q = \frac{1}{2} q^{\tau_1+\tau_2-\delta}$, so folgt aus (19)

$$|v_1| \leq (2Q)^{\sigma_1}, \quad |v_2| \leq (2Q)^{\sigma_2}, \quad |v_1 \xi_1 + v_2 \xi_2 - v_l| \leq Q^{-1}.$$

Das ist aber bereits Formel (14),

(B) $v_0 < \tau_1 + \tau_2 - 1 - \delta$. Wir betrachten den Körper \mathfrak{K}' :

$$|g_1| < q^{-v_0}, \quad |g_2| \leq q^{1-\tau_1-\tau_2+v_0}, \quad |\phi| < 1.$$

Nach Minkowski liegt ein primitiver Gitterpunkt $v' = (v'_1, v'_2, v'_l)$ in \mathfrak{K}' . Offenbar sind v, v' linear unabhängig. Wir schreiben

$$g_i = g_i(v_1, v_2, v_l), \quad g'_i = g_i(v'_1, v'_2, v'_l) \quad (i = 1, 2, l).$$

Man hat nun

$$|g'_1| < q^{-v_0}, \quad |g'_2| \leq q^{1-\tau_1-\tau_2+v_0}, \quad |g'_l| \leq 2q^{1-\tau_1-\tau_2+v_0}, \quad (20)$$

und hieraus folgt

$$|v'_1| \leq q^{\tau_1-v_0}, \quad |v'_2| \leq q^{1-\tau_1+v_0}, \quad |v'_1 \xi_1 + v'_2 \xi_2 - v'_l| \leq 2q^{-\tau_1-\tau_2+v_0}. \quad (21)$$

Infolge (17) sind die Schranken (19) schärfer als (21) und es gilt

$$|v_1| \leq q^{\tau_1-v_0}, \quad |v_2| \leq q^{1-\tau_1+v_0}, \quad |v_1 \xi_1 + v_2 \xi_2 - v_l| \leq 2q^{-\tau_1-\tau_2+v_0}. \quad (22)$$

Setzen wir

$$Q' = \frac{1}{2} Q^{1+\delta}, \quad b_1 = \frac{\tau_1 - \nu_0}{1 + \delta} > \frac{1 + \delta - \tau_2}{1 + \delta} > 0, \quad b_2 = \frac{1 - \tau_1 + \nu_0}{1 + \delta} \geq 0,$$

so gilt $|v_1| \leq (2Q')^{b_1}, \quad |v_2| \leq (2Q')^{b_2}, \quad |v_1 \xi_1 + v_2 \xi_2 - v_l| \leq Q'^{-1},$

sowie das analoge Ungleichungssystem für v'_1, v'_2, v'_l , also (15). Dabei ist $b_1 + b_2 = (1 + \delta)^{-1}$.

7.3. Konstante σ_0 und τ_0 . ξ_1, ξ_2 seien reelle Zahlen. Wir setzen $\sigma_0 = \sigma_0(\xi_1, \xi_2)$ für das Infimum der reellen Zahlen σ , so daß die Menge \mathfrak{S}_σ der $Q > 1$, zu denen ganzrationale $(p_1, p_2, p_l) \neq (0, 0, 0)$ existieren, die

$$\text{Max}(|p_1|, 1) \cdot \text{Max}(|p_2|, 1) \leq Q^\sigma, \quad |p_1 \xi_1 + p_2 \xi_2 - p_l| \leq Q^{-1} \tag{23}$$

leisten, *nicht* Eigenschaft F besitzt. Offenbar ist $\sigma_0 \geq 0$. Weiter gilt

$$\sigma_0 \leq 1, \tag{24}$$

denn das System

$$|p_1| \leq Q^\dagger, \quad |p_2| \leq Q^\dagger, \quad |p_1 \xi_1 + p_2 \xi_2 - p_l| \leq Q^{-1}$$

hat für jedes $Q > 1$ eine ganzzahlige Lösung $(p_1, p_2, p_l) \neq (0, 0, 0)$.

$\tau_0 = \tau_0(\xi_1, \xi_2)$ sei das Supremum der reellen Zahlen τ , so daß die Menge \mathfrak{T}_τ der $Q > 1$, zu denen es ganze $(p_1, p_2, p_l) \neq (0, 0, 0)$ gibt, die

$$|p_l \xi_1 - p_1| |p_l \xi_2 - p_2| \leq Q^{-\tau}, \quad |p_l| \leq Q \tag{25}$$

erfüllen, *nicht* Eigenschaft F hat. Man sieht leicht, daß

$$\tau_0 \geq 1 \tag{26}$$

ist.

HILFSSATZ 16. Für die beiden Zahlen ξ_1, ξ_2 gelte (11) aus § 1, und $\mathcal{M}(\xi_1, \xi_2, \delta)$ besitze für jedes $\delta > 0$ Eigenschaft F . Dann ist $\sigma_0 > 0$ und

$$\tau_0 \geq (2 - \sigma_0) \sigma_0^{-1}. \tag{27}$$

Beweis. Aus Formel (11), § 1, folgt sofort $\sigma_0 \geq c_3^{-1} > 0$. Ist $\sigma_0 = 1$, so folgt die Behauptung aus (26), so daß man also $0 < \sigma_0 < 1$ annehmen darf. σ sei eine Zahl im Intervall $\sigma_0 < \sigma < 1$. \mathfrak{S}_σ hat nicht Eigenschaft F .

Zu jedem $Q \in \mathfrak{S}_\sigma$ gibt es Zahlen $p_i(Q)$ ($i = 1, 2, l$), die (23) erfüllen. Wir definieren $Q^* = Q^*(Q)$ durch $|p_1(Q) \xi_1 + p_2(Q) \xi_2 - p_l(Q)| = Q^{*-1}$. Mit $p_i = p_i(Q)$ ($i = 1, 2, l$) hat man jetzt

$$\text{Max}(|p_1|, 1) \cdot \text{Max}(|p_2|, 1) \leq Q^{*\sigma}, \quad |p_1 \xi_1 + p_2 \xi_2 - p_i| = Q^{*-1}. \quad (28)$$

Dabei ist $Q^* \geq Q$ und wegen (11) aus § 1 außerdem $Q^* \leq Q^{c\sigma}$. Ist also \mathfrak{S}_σ^* die Teilmenge von \mathfrak{S}_σ bestehend aus allen $Q^* \in \mathfrak{S}_\sigma$, für die nicht nur (23), sondern sogar (28) erfüllt werden kann, so gibt es zu jedem $x \in \mathfrak{S}_\sigma$ ein $y \in \mathfrak{S}_\sigma^*$ mit $x \leq y \leq x^{c\sigma}$. Infolge Hilfssatz 3 hat \mathfrak{S}_σ^* nicht Eigenschaft F .

Nun sei η im Intervall $0 < \eta < (1 - \sigma)/2$. Ist $Q \in \mathfrak{S}_\sigma^*$, so seien $p_i(Q)$ ($i = 1, 2, l$) Zahlen, die (28) erfüllen. Wir definieren $\sigma_1(Q)$, $\sigma_2(Q)$ durch

$$\text{Max}(Q^\eta, |p_i(Q)|) = Q^{\sigma_i(Q)} \quad (i = 1, 2).$$

Es ist $\sigma_i(Q) \geq \eta$, $\sigma_1(Q) + \sigma_2(Q) \leq \sigma + 2\eta < 1$.

Für jedes $Q \in \mathfrak{S}_\sigma^*$ werden die Voraussetzungen des ersten kleinen Übertragungssatzes durch $q = Q$, $\sigma_1 = \sigma_1(Q)$, $\sigma_2 = \sigma_2(Q)$, $p_i = p_i(Q)$ ($i = 1, 2, l$) erfüllt. Sei $\varepsilon > 0$. Für jedes $Q \in \mathfrak{S}_\sigma^*$ gibt es Zahlen $\delta(Q)$, $\tau_1(Q)$, $\tau_2(Q)$, so daß die Behauptungen dieses Übertragungssatzes gelten. Daher gilt für jedes $Q \in \mathfrak{S}_\sigma^*$ entweder (A) oder (B) dieses Übertragungssatzes. Die Menge \mathfrak{S}_σ^* teilen wir entsprechend in zwei Teilmengen $\mathfrak{S}_\sigma(A)$ und $\mathfrak{S}_\sigma(B)$ ein. Nach Hilfssatz 2 können nicht beide Mengen $\mathfrak{S}_\sigma(A)$, $\mathfrak{S}_\sigma(B)$ Eigenschaft F haben.

Aus dem Beweis des ersten kleinen Übertragungssatzes geht hervor, daß man für die dort auftretende Größe δ irgend eine Zahl nehmen darf, so daß $\delta > 0$, $\delta < 1 - \sigma_1$, $\delta < 1 - \sigma_2$, und daß (5) gilt. Ist nun δ eine Zahl mit $0 < \delta < 1$, $\delta < 1 - \sigma - 2\eta$,

$$\frac{2 - 2\eta - 2\delta}{2\eta + \delta} > \frac{2 - 2\eta}{2\eta} - \varepsilon,$$

so gilt für jedes $Q \in \mathfrak{S}_\sigma^*$: $\delta < 1 - \sigma_1(Q)$, $\delta < 1 - \sigma_2(Q)$,

$$\frac{2 - \sigma_1(Q) - \sigma_2(Q) - 2\delta}{\sigma_1(Q) + \sigma_2(Q) + \delta} > \frac{2 - \sigma_1(Q) - \sigma_2(Q)}{\sigma_1(Q) + \sigma_2(Q)} - \varepsilon,$$

also (5). Man darf daher $\delta = \delta(Q)$ setzen.

Nun sei $\mathfrak{S}_\sigma(A)'$ die Menge der Zahlen $Q' = 2Q^{\sigma_1(Q) + \sigma_2(Q) + \delta}$, wobei $Q \in \mathfrak{S}_\sigma(A)$, und $\mathfrak{S}_\sigma(B)'$ die Menge der Zahlen $Q' = 2Q^{1-\delta}$, wobei $Q \in \mathfrak{S}_\sigma(B)$. Es gilt

$$0 < 1 - \delta, \quad 0 < \delta \leq \sigma_1(Q) + \sigma_2(Q) + \delta \leq 1 + \delta.$$

Infolge Hilfssatz 3 hat daher mit $\mathfrak{S}_\sigma(A)'$ auch $\mathfrak{S}_\sigma(A)$, und mit $\mathfrak{S}_\sigma(B)'$ auch $\mathfrak{S}_\sigma(B)$ Eigenschaft F , so daß nach dem früher Gesagten nicht beide Mengen $\mathfrak{S}_\sigma(A)'$ und $\mathfrak{S}_\sigma(B)'$ Eigenschaft F besitzen.

Für $Q' \in \mathfrak{S}_\sigma(\mathbf{B})'$ gibt es die in der Alternative (B) von Hilfssatz 14 beschriebene Matrix, die (4) befriedigt. Setzen wir $a'_1 = a_1(1 - \delta/3)$, $a'_2 = a_2(1 - \delta/3)$, und ist Q' so groß, daß $Q'^{\delta/3} \geq 2$, ist, so kann man die Schranken $(Q'/2)^{-a_1}$, $(Q'/2)^{-a_2}$ in (4) durch $Q'^{-a'_1}$ bzw. $Q'^{-a'_2}$ ersetzen. Dabei ist

$$a'_1 \geq 0, \quad a'_2 \geq 0, \quad a'_1 + a'_2 \geq (a_1 + a_2)(1 - \delta/3) \geq (1 + \delta)(1 - \delta/3) \geq 1 + \delta/3.$$

Dader ist $\mathfrak{S}_\sigma(\mathbf{B})'$ in $\mathfrak{M}(\xi_1, \xi_2, \delta/3)$ enthalten, hat also Eigenschaft F . Somit kann $\mathfrak{S}_\sigma^*(\mathbf{A})'$ nicht Eigenschaft F haben.

Für $Q' \in \mathfrak{S}_\sigma(\mathbf{A})'$ gibt es v_1, v_2, v_l , so daß (3) gilt. Setzen wir $\tau'_i = \tau_i(1 - \delta/3)$ ($i = 1, 2$), und ist Q' groß, so kann man die Schranken $(Q'/2)^{-\tau_1}$, $(Q'/2)^{-\tau_2}$ in (3) durch $Q'^{-\tau'_1}$ bzw. $Q'^{-\tau'_2}$ ersetzen, und es gilt

$$|v_l \xi_1 - v_1| |v_l \xi_2 - v_2| \leq Q'^{-\tau'_1 - \tau'_2}, \quad |v_l| \leq Q'.$$

Dabei ist

$$\tau'_1 + \tau'_2 = (\tau_1 + \tau_2)(1 - \delta/3) > \left(\frac{2 - \sigma_1(Q) - \sigma_2(Q)}{\sigma_1(Q) + \sigma_2(Q)} - \varepsilon \right) (1 - \delta/3) \geq \left(\frac{2 - \sigma - 2\eta}{\sigma + 2\eta} - \varepsilon \right) (1 - \delta/3).$$

Also liegt $\mathfrak{S}_\sigma(\mathbf{A})'$ in \mathfrak{X}_τ für $\tau = ((2 - \sigma - 2\eta)(\sigma + 2\eta)^{-1} - \varepsilon)(1 - \delta/3)$. Dabei hat \mathfrak{X}_τ nicht Eigenschaft F , somit ist $\tau \leq \tau_0$. Da $\delta > 0$ beliebig klein sein kann, folgt hieraus $\tau_0 \geq (2 - \sigma - 2\eta)(\sigma + 2\eta)^{-1} - \varepsilon$, weiter $\tau_0 \geq (2 - \sigma - 2\eta)(\sigma + 2\eta)^{-1}$, $\tau_0 \geq (2 - \sigma)\sigma^{-1}$, schließlich (27).

HILFSSATZ 17. Für die beiden Zahlen ξ_1, ξ_2 gelte (10) aus § 1, und $\mathfrak{L}(\xi_1, \delta)$, $\mathfrak{L}(\xi_2, \delta)$ und $\mathfrak{N}(\xi_1, \xi_2, \delta)$ möge für jedes $\delta > 0$ Eigenschaft F besitzen. Dann ist $\tau_0 \leq 2$ und

$$\sigma_0 \leq (2 - \tau_0)\tau_0^{-1}. \tag{29}$$

Beweis. Ist $\tau_0 = 1$, so ist die behauptete Ungleichung für σ_0 eine Folge von (24). Sei also $1 < \tau_0$ und τ eine Zahl in $1 < \tau < \tau_0$. \mathfrak{X}_τ hat nicht Eigenschaft F .

Zu jedem $Q \in \mathfrak{X}_\tau$ gibt es Zahlen $p_i(Q)$ ($i = 1, 2, l$), die (25) erfüllen. Man darf dabei noch $|p_l \xi_i - p_i| \leq \frac{1}{2}$ ($i = 1, 2$) verlangen. Wir definieren $Q^* = Q^*(Q)$ durch $|p_l(Q)| = Q^*$. Mit $p_i = p_i(Q)$ ($i = 1, 2, l$) hat man jetzt

$$|p_l \xi_1 - p_1| |p_l \xi_2 - p_2| \leq Q^{*- \tau}, \quad |p_l| = Q^*. \tag{30}$$

Dabei ist $Q^* \leq Q$ und wegen (10) aus § 1 außerdem $Q^{*c_1 + c_2} \geq Q^\tau$. Ist also \mathfrak{X}_τ^* die Teilmenge von \mathfrak{X}_τ bestehend aus allen $Q^* \in \mathfrak{X}_\tau$, für die nicht nur (25), sondern sogar (30) erfüllt werden kann, so hat \mathfrak{X}_τ^* nicht Eigenschaft F .

Für $Q \in \mathfrak{I}_\tau^*$ seien $p_1(Q)$, $p_2(Q)$, $p_i(Q)$ Zahlen, die (30) erfüllen. Wir definieren $\tau_1(Q)$, $\tau_2(Q)$ durch

$$|p_i(Q) \xi_i - p_i(Q)| = Q^{-\tau_i(Q)} \quad (i = 1, 2).$$

Dann ist $\tau_i(Q) \geq 0$, $\tau_1(Q) + \tau_2(Q) \geq \tau > 1$.

Nun sei $0 < \eta < (\tau - 1)/2$. $\mathfrak{I}_\tau(1)$ bzw. $\mathfrak{I}_\tau(2)$ sei die Teilmenge jener $Q \in \mathfrak{I}_\tau^*$, für die $\tau_1(Q) \geq 1 + \eta$ bzw. $\tau_2(Q) \geq 1 + \eta$ ist. Nun ist $\mathfrak{I}_\tau(1) \subset \mathcal{L}(\xi_1, \eta)$, $\mathfrak{I}_\tau(2) \subset \mathcal{L}(\xi_2, \eta)$, also haben $\mathfrak{I}_\tau(1)$ und $\mathfrak{I}_\tau(2)$ Eigenschaft F . Ist $\mathfrak{I}_\tau(3)$ das Komplement von $\mathfrak{I}_\tau(1)$ und $\mathfrak{I}_\tau(2)$ in \mathfrak{I}_τ^* , so hat $\mathfrak{I}_\tau(3)$ nicht Eigenschaft F .

Für $Q \in \mathfrak{I}_\tau(3)$ ist $\tau_i(Q) \leq 1 + \eta$ ($i = 1, 2$), $\tau \leq \tau_1(Q) + \tau_2(Q) \leq 2 + 2\eta$. Da $\eta > 0$ beliebig klein sein darf, folgt $\tau \leq 2$, $\tau_0 \leq 2$.

Für $Q \in \mathfrak{I}_\tau(3)$ bilden wir

$$\bar{\tau}_i(Q) = \text{Min}(1, \tau_i(Q)) \quad (i = 1, 2).$$

Dann ist $0 \leq \bar{\tau}_i(Q) \leq 1$, $\bar{\tau}_1(Q) + \bar{\tau}_2(Q) \geq \tau - 2\eta > 1$, $|p_i(Q)| = Q$,

$$|p_i(Q) \xi_i - p_i(Q)| \leq Q^{-\bar{\tau}_i(Q)} \quad (i = 1, 2).$$

Also werden für jedes $Q \in \mathfrak{I}_\tau(3)$ die Voraussetzungen des zweiten kleinen Übertragungssatzes durch $q = Q$, $\tau_1 = \bar{\tau}_1(Q)$, $\tau_2 = \bar{\tau}_2(Q)$, $p_i = p_i(Q)$ ($i = 1, 2, l$) erfüllt. Sei $\varepsilon > 0$. Für jedes $Q \in \mathfrak{I}_\tau(3)$ gibt es Zahlen $\delta(Q)$, $\sigma_1(Q)$, $\sigma_2(Q)$, so daß die Behauptungen dieses Übertragungssatzes gelten. Dabei kann man $\delta(Q) = \delta$ setzen, wobei δ eine Zahl mit $0 < \delta < 1$,

$$\frac{2 - \tau + 2\eta + 2\delta}{\tau - 2\eta - \delta} < \frac{2 - \tau + 2\eta}{\tau - 2\eta} + \varepsilon$$

ist. Für jedes $Q \in \mathfrak{I}_\tau(3)$ gilt entweder (A) oder (B) des zweiten kleinen Übertragungssatzes, und entsprechend teilen wir $\mathfrak{I}_\tau(3)$ in zwei Teilmengen $\mathfrak{I}_\tau(A)$ und $\mathfrak{I}_\tau(B)$ ein.

Nun sei $\mathfrak{I}_\tau(A)'$ die Menge der Zahlen $Q' = \frac{1}{2} Q^{\bar{\tau}_1(Q) + \bar{\tau}_2(Q) - \delta}$, wo $Q \in \mathfrak{I}_\tau(A)$, $\mathfrak{I}_\tau(B)'$ die Menge der $Q' = \frac{1}{2} Q^{1 + \delta}$, wo $Q \in \mathfrak{I}_\tau(B)$. Es ist $0 < 1 - \delta \leq \bar{\tau}_1(Q) + \bar{\tau}_2(Q) - \delta \leq 2 - \delta$. Hätten sowohl $\mathfrak{I}_\tau(A)'$ als auch $\mathfrak{I}_\tau(B)'$ Eigenschaft F , so auch $\mathfrak{I}_\tau(A)$ und $\mathfrak{I}_\tau(B)$, was unmöglich ist.

Für $Q' \in \mathfrak{I}_\tau(B)'$ gibt es die in der Alternative (B) von Hilfssatz 15 beschriebene Matrix, die (15) befriedigt. Wir schließen, ganz ähnlich wie im entsprechenden Teil des Beweises von Hilfssatz 16, daß $\mathfrak{I}_\tau(B)'$ Eigenschaft F , also $\mathfrak{I}_\tau(A)'$ nicht Eigenschaft F besitzt.

Analog zu einer Ungleichung am Ende des Beweises von Hilfssatz 16 erhält man jetzt

$$\sigma_0 \leq ((2 - \tau + 2\eta)(\tau - 2\eta)^{-1} + \varepsilon)(1 + \delta/3),$$

schließlich (29).

HILFSSATZ 18. ξ_1, ξ_2 mögen die Voraussetzungen der beiden Hilfssätze 16 und 17 erfüllen. Dann ist

$$\sigma_0 = \tau_0 = 1.$$

Beweis. Nach Hilfssatz 16 und 17 sind σ_0, τ_0 endliche positive Zahlen, und es ist $\tau_0 \geq (2 - \sigma_0)\sigma_0^{-1}$, $\sigma_0 \leq (2 - \tau_0)\tau_0^{-1}$. Hieraus folgt $2 - \sigma_0 \leq \sigma_0 \tau_0 \leq 2 - \tau_0$, $\sigma_0 \geq \tau_0$, also $\sigma_0 = \tau_0 = 1$ wegen (24) und (26).

7.4. Beweis von Satz 5. Wir beweisen hier Teil (b) von Satz 5. Teil (a) geht ähnlich und etwas leichter zu zeigen. Alle Voraussetzungen des Satzes seien erfüllt, so daß also Hilfssatz 18 gilt, und es sei $\varepsilon > 0$.

Ist $q \in \mathfrak{Q}(\xi_1, \xi_2, \varepsilon)$, so gibt es ganze p_1, p_2 mit

$$|q\xi_1 - p_1| |q\xi_2 - p_2| q^{1+\varepsilon} < 1, \text{ also } |q\xi_1 - p_1| |q\xi_2 - p_2| \leq q^{-1-\varepsilon}, |q| = q.$$

$\mathfrak{Q}(\xi_1, \xi_2, \varepsilon)$ ist in \mathfrak{I}_τ mit $\tau = 1 + \varepsilon > \tau_0$. Mit \mathfrak{I}_τ hat nun auch \mathfrak{Q} Eigenschaft F .

Ist $q \in \mathfrak{B}(\xi_1, \xi_2, \varepsilon)$, so gibt es $q_1 \neq 0, q_2 \neq 0, p$ mit $q = \text{Max}(|q_1|, |q_2|)$, wobei

$$|q_1|^{1+\varepsilon} |q_2|^{1+\varepsilon} |q_1\xi_1 + q_2\xi_2 - p| < 1.$$

Wir bilden $Q = |q_1 q_2|^{1+\varepsilon}$. Dann ist mit $\sigma = (1 + \varepsilon)^{-1} < \sigma_0$

$$|q_1| |q_2| = Q^\sigma, \quad |q_1\xi_1 + q_2\xi_2 - p| < Q^{-1},$$

also Q in \mathfrak{S}_σ . Die Menge der so gebildeten Q hat daher Eigenschaft F . Wegen $q^{1+\varepsilon} \leq Q \leq q^{2+\varepsilon}$ muß nach Hilfssatz 3 auch die Menge der $q \in \mathfrak{B}$ diese Eigenschaft besitzen.

8. Transzendenz

8.1. Die Näherungsnenner einer quadratischen Irrationalzahl.

HILFSSATZ 19.⁽¹⁾ q_1, q_2, \dots sei die Folge der Näherungsnenner einer quadratischen Irrationalzahl α . Dann existiert

$$\lim_{n \rightarrow \infty} \sqrt[n]{q_n}, \tag{1}$$

und ist gleich einer Zahl $\beta > 1$.

⁽¹⁾ Leider konnte ich diesen einfachen Hilfssatz in der Literatur nicht finden.

Beweis. Sei $\alpha = [\overline{b_0 b_1, \dots, b_m, a_1, \dots, a_k}]$, das heißt, der Kettenbruch von α habe Vorperiode b_0, b_1, \dots, b_m und Periode a_1, \dots, a_k . Ist allgemein $c_0 = b_0, c_1 = b_1, \dots, c_m = b_m, c_{m+1} = a_1, c_{m+2} = a_2$, also $\alpha = [c_0, c_1, c_2, \dots]$ und p_n/q_n der Näherungsbruch $[c_0, c_1, \dots, c_n]$, so ist bekanntlich $q_n/q_{n-1} = [c_n, c_{n-1}, \dots, c_2, c_1]$, ([5], § 11, Formel (3)). Ist speziell $n = m + lk$, so ist

$$q_n/q_{n-1} = [a_k, a_{k-1}, \dots, a_1, \dots, a_k, a_{k-1}, \dots, a_1, b_m, b_{m-1}, \dots, b_1],$$

wobei a_k, a_{k-1}, \dots, a_1 genau l mal vorkommt, und somit liegt q_n/q_{n-1} zwischen

$$r_l = [a_k, a_{k-1}, \dots, a_1, \dots, a_k, a_{k-1}, \dots, a_1]$$

und dem vorhergehenden Näherungsbruch

$$r'_l = [a_k, a_{k-1}, \dots, a_1, \dots, a_k, a_{k-1}, \dots, a_2]$$

von r_l . Folglich ist $\lim_{l \rightarrow \infty} q_{m+lk}/q_{m+lk-1} = \lim_{l \rightarrow \infty} r_l = [\overline{a_k, a_{k-1}, \dots, a_1}] = \delta_0$, etwa.

Auf ganz ähnliche Weise findet man

$$\lim_{l \rightarrow \infty} q_{m+lk+j}/q_{m+lk+j-1} = \delta_j \quad (0 \leq j \leq k-1),$$

und hieraus folgt

$$\lim_{n \rightarrow \infty} q_{n+k}/q_n = \delta_0 \delta_1, \dots, \delta_{k-1} = \eta. \quad (2)$$

Dabei muß $\eta > 1$ sein, da bekanntlich $q_{n+2} \geq 2q_n$ ist.

Aus (2) folgt, daß der Limes in (1) existiert und gleich $\beta = \sqrt[k]{\eta}$ ist.

8.2. Berechnung gewisser Grenzwerte. Im folgenden mögen $q_1, q_2, \dots; c; n_1, n_2, \dots; \xi$ die Voraussetzungen von Satz 6 erfüllen, und zwar seien q_1, q_2, \dots Näherungsnenner der quadratischen Irrationalzahl α . β sei der Grenzwert (1). Wir bilden

$$r_k = q_{n_k}, \quad s_k = r_1 r_2, \dots, r_k \quad (k = 1, 2, \dots).$$

HILFSSATZ 20.

$$\lim c^{-k} \log r_k = \log \beta, \quad (3)$$

$$\lim c^{-k} \log s_k = \frac{c}{c-1} \log \beta, \quad (4)$$

$$\lim c^{-k} \log \|\xi s_k\| = -c \frac{c-2}{c-1} \log \beta, \quad (5)$$

$$\lim c^{-k} \log \|\alpha s_k\| = -\frac{c-2}{c-1} \log \beta. \tag{6}$$

Beweis. Es ist $\lim n^{-1} \log q_n = \log \beta$, $\lim [c^k]^{-1} \log r_k = \log \beta$, und (3) folgt.

$$\begin{aligned} c^{-k} \log s_k &= c^{-k} \sum_{j=1}^k \log r_j = c^{-k} \left(\sum_{j=1}^k c^j \log \beta + \sum_{j=1}^k (\log r_j - c^j \log \beta) \right) \\ &= \frac{c}{c-1} \log \beta - \frac{c^{1-k}}{c-1} \log \beta + \sum_{j=1}^k c^{j-k} (c^{-j} \log r_j - \log \beta). \end{aligned}$$

Da hier die letzte Summe infolge (3) gegen 0 strebt, folgt (4).

Aus der Definition von ξ ergibt sich $\|\xi s_k\| = \|(r_{k+1}^{-1} + r_{k+2}^{-1} + \dots) s_k\|$. Dabei ist offenbar für $k \geq k_1$, $r_{k+2} \geq 2r_{k+1}$, daher

$$r_{k+1}^{-1} \leq r_{k+1}^{-1} + r_{k+2}^{-1} + \dots \leq 2r_{k+1}^{-1}.$$

Man hat nun

$$\begin{aligned} \left| c^{-k} \log ((r_{k+1}^{-1} + r_{k+2}^{-1} + \dots) s_k) + c \frac{c-2}{c-1} \log \beta \right| \\ \leq \left| c^{-k} \log (r_{k+1}^{-1} s_k) + c \frac{c-2}{c-1} \log \beta \right| + c^{-k} \log 2. \end{aligned} \tag{7}$$

Infolge (3) und (4) strebt dieser Ausdruck für $k \rightarrow \infty$ gegen Null. Daher ist für großes k der Logarithmus von $(r_{k+1}^{-1} + r_{k+2}^{-1} + \dots) s_k$ kleiner als $\log \frac{1}{2}$, also

$$|(r_{k+1}^{-1} + r_{k+2}^{-1} + \dots) s_k| < \frac{1}{2}, \quad \|(r_{k+1}^{-1} + r_{k+2}^{-1} + \dots) s_k\| = \|\xi s_k\| = |(r_{k+1}^{-1} + r_{k+2}^{-1} + \dots) s_k|,$$

und (5) folgt, weil (7) gegen Null strebt.

Es ist $C r_k^{-1} \leq \|\alpha r_k\| < r_k^{-1}$, wo $C > 0$ nur von α abhängt. Nach (3) und (4) ist für große k

$$s_{k-1} r_k^{-1} < \frac{1}{2},$$

und für solche k ist weiter

$$C s_{k-1} r_k^{-1} < \|\alpha s_k\| = \|\alpha r_k s_{k-1}\| < s_{k-1} r_k^{-1}.$$

Hieraus und aus (3) und (4) folgt aber (6).

8.3. *Beweis von Satz 6.* Aus (4), (5) und (6) folgt, daß für $k > k_0(\delta, \epsilon)$

$$\log (s_k^{1+\delta} \|\xi s_k\| \|\alpha s_k\|) \leq c^k ((c(1+\delta) - c(c-2) - (c-2)) (c-1)^{-1} \log \beta + \epsilon) \tag{8}$$

ist. Nun ist infolge $c > 1 + 3^{\frac{1}{2}}$

$$c - c(c-2) - (c-2) < 0.$$

Wir wählen $\delta > 0$ so klein, daß auch noch $c(1 + \delta) - c(c - 2) - (c - 2) < 0$ ist, und nachher wählen wir $\varepsilon > 0$ so klein, daß die rechte Seite der Formel (8) negativ wird.

Somit ist für $k > k^*$

$$s_k^{1+\delta} \|\xi s_k\| \|\alpha s_k\| < 1.$$

Da weiter nach (4) $\lim \log s_{k+1}/\log s_k = c < \infty$, ist nach Satz 1 entweder ξ transzendent, oder sind $1, \alpha, \xi$ linear abhängig über \mathbb{Q} . Wir wollen zeigen, daß der zweite Fall nicht zutrifft.

In diesem Fall wäre $a\xi = b\alpha + c$, wobei $a > 0$ und a, b, c ganzrational sind. Nun ist infolge (5)

$$\lim c^{-k} \log \|a\xi s_k\| = -c \frac{c-2}{c-1} \log \beta,$$

also $\|a\xi s_k\| \neq 0$, also $a\xi \neq c$. Für $b \neq 0$ ist nach (6)

$$\lim c^{-k} \log \|(b\alpha + c)s_k\| = -\frac{c-2}{c-1} \log \beta.$$

Somit ist für großes k $\|a\xi s_k\| \neq \|(b\alpha + c)s_k\|$, und $a\xi$ kann nicht gleich $b\alpha + c$ sein.

Literatur

- [1]. CASSELS, J. W. S., *An introduction to diophantine approximation*. Cambridge Tracts 45 (1957).
- [2]. HASSE, H., Simultane Approximation algebraischer Zahlen durch algebraische Zahlen. *Monatsh. Math.*, 48 (1939), 205–225.
- [3]. KHINTCHINE, A. YA., Über eine Klasse linearer Diophantischer Approximationen. *Rend. Circ. Mat. Palermo*, 50 (1926), 170–195.
- [4]. MAHLER, K., *Lectures on diophantine approximations*. Univ. of Notre Dame (1961).
- [5]. PERRON, O., *Die Lehre von den Kettenbrüchen*. 3. Aufl. Stuttgart (1954).
- [6]. ROTH, K. F., Rational approximations to algebraic numbers. *Mathematika*, 2 (1955), 1–20.
- [7]. SCHNEIDER, TH., Über die Approximation algebraischer Zahlen. *Journal f. d. reine u. angew. Math.*, 175 (1936), 182–192.

Eingegangen am 13. August 1964.