

Separatum

PUBLICATIONES MATHEMATICAE

TOMUS 29.

FASC. 1—2.

**DEBRECEN
1982**

FUNDAVERUNT:

A. RÉNYI, T. SZELE ET O. VARGA

ADJUVANTIBUS

Z. DARÓCZY, B. GYIRES, A. RAPCSÁK, L. TAMÁSSY

REDIGIT:

B. BARNA

A. Pethő

Über die Verteilung der Lösungen von S -Normformen Gleichungen

**INSTITUTUM MATHEMATICUM UNIVERSITATIS DEBRECENIENSIS
HUNGARIA**

Über die Verteilung der Lösungen von S-Normformen Gleichungen

Von ATTILA PETHŐ (Debrecen)

1. Einleitung

Sei $P = \{p_1, \dots, p_\tau\}$ eine Menge verschiedener rationaler Primzahlen. Bezeichne Q bzw. Z die Menge der rationalen, bzw. der ganzrationalen Zahlen und Z_P die Menge derjenigen Elemente von Q , deren Nenner (in ihrer gekürzten Form) nur durch Primzahlen aus P teilbar sind, endlich $|\cdot|_p$ die p -adische Bewertung von Q , wo p eine rationale Primzahl ist. Der Einfachheit halber bezeichne $|\cdot|_{p_0} = |\cdot|$ den gewöhnlichen absoluten Betrag von Q . Ein altes Problem aus der Theorie der diophantischen Gleichungen lautet folgendermaßen: Wann hat die Gleichung

$$(1) \quad \prod_{i=0}^{\tau} |N_{K/Q}(\alpha_1 x_1 + \dots + \alpha_k x_k)|_{p_i} = a \quad 0 \neq a \in Q$$

unendlich viele Lösungen $(x_1, \dots, x_k) \in Z_P^k$ und wie ist die Struktur der Menge der Lösungen, falls $\alpha_1, \dots, \alpha_k$ über Q linear unabhängige Elemente eines Zahlkörpers K vom Grad $n \geq 2$ sind und $N_{K/Q}(\alpha)$ die Norm der Elemente $\alpha \in K$ bezeichnet.

Neuerdings hat H. P. SCHLICKWEI [8], als Verallgemeinerung des Ergebnisses für $P = \emptyset$ von W. M. SCHMIDT [9] bewiesen, daß (1) für ein beliebiges $a \in Q$ nur endlich viele maximale Lösungsfamilien besitzt.

Die Verteilung der Lösungen von (1) wurde für $P = \emptyset$ von vielen Autoren untersucht. (Darüber siehe die Einleitung von [3].) In einer Reihe von Arbeiten gelang es mir gemeinsam mit K. GYÖRY, für die Anzahl der Lösungen von (1) eine asymptotische Formel zu finden [2], [3]. Für den Fall da $\{\alpha_1, \dots, \alpha_k\}$ ein vollständiger Z -Modul war d. h. für $k = n$ bestimmten wir die Konstante im Hauptglied und wir gaben eine obere Schranke für die Konstante im Restglied an [4].

In dieser Arbeit werden $T_0, \dots, T_\tau \geq 0$ diejenigen reellen Zahlen bezeichnen, für welche $u_j \in Z$ (für alle $1 \leq j \leq \tau$) mit $T_j = p_j^{u_j}$ existieren. Es wird noch $\|\mathbf{T}\|$ für $T_0 \cdot \dots \cdot T_\tau$ geschrieben. Sei M der durch die Elemente $\alpha_1, \dots, \alpha_k$ in K erzeugte Z_P -Modul. Bezeichne $P_{M,a}(T_0, \dots, T_\tau) = P_{M,a}(\mathbf{T})$ die Anzahl der Lösungen $(x_1, \dots, x_k) \in Z^k$ von (1), für welche

$$(2) \quad \max_{1 \leq i \leq k} (|x_i|_{p_j}) \leq T_j \quad (j = 0, \dots, \tau)$$

gilt.

In der vorliegenden Arbeit geben wir unter Benutzung des Ergebnisses von H. P. SCHLICKWEI [8] eine asymptotische Formel für $P_{M,a}(\mathbf{T})$ an, vorausgesetzt,

daß dieselbe mit $\|T\|$ gegen Unendlich strebt. In gewissen Fällen werden die explizite Form der Konstanten im Hauptglied und eine obere Schranke der Konstanten im Restglied angegeben. Als Folgerung wird eine asymptotische Formel für die Anzahl der Lösungen $(x_1, \dots, x_k; z_1, \dots, z_r) \in Z^{k+r}$ der diophantischen Gleichung

$$(3) \quad |N_{K/Q}(\alpha_1 x_1 + \dots + \alpha_k x_k)| = a p_1^{\alpha_1} \cdot \dots \cdot p_r^{\alpha_r}$$

unter der Bedingung $\max_{1 \leq i \leq k} (|x_i|) \leq N$ hergeleitet, in gewissen Fällen ebenfalls mit expliziten Konstanten.

Zur Formulierung der Sätze benötigen wir noch einige Bezeichnungen. Die maximale Menge der nicht äquivalenten Fortsetzungen auf K der Elemente der Menge $S_0 = \{ | \cdot |_{p_0}, \dots, | \cdot |_{p_r} \}$ bezeichnen wir mit

$$S_K = \{ | \cdot |_{\mathcal{P}_{01}}, \dots, | \cdot |_{\mathcal{P}_{0e_0}}, \dots, | \cdot |_{\mathcal{P}_{\tau 1}}, \dots, | \cdot |_{\mathcal{P}_{\tau e_\tau}} \}.$$

Der erste Index von $\mathcal{P}_{ij}$ zeigt, daß diese Bewertung die Fortsetzung von p_i ist. Es wird außerdem vorausgesetzt, daß auf Q $\mathcal{P}_{ij}$ und p_i übereinstimmen. Der Einfachheit halber wird lieber $\mathcal{P} \in S_K$ oder $p \in S_0$ statt $| \cdot |_{\mathcal{P}} \in S_K$ oder $| \cdot |_p \in S_0$ geschrieben. Der lokale Grad von $\mathcal{P}_{ij}$ wird mit $n_{ij} = n(\mathcal{P}_{ij}/p_i)$ bezeichnet. Setzt man $e_0 + \dots + e_\tau = q_K + 1$, dann gilt $q_K + 1 \leq n(\tau + 1)$.

Sei $\mathcal{D}_M$ der Multiplikatorenring von M , also die Menge der Elemente α von K mit $\alpha M \subseteq M$. Bezeichne $\mathcal{E}^S$ die S -Einheitengruppe von K , d. h. die Menge der Elemente η von K , für welche $\prod_{i=0}^{\tau} |N_{K/Q}(\eta)|_{p_i} = 1$ gilt, ferner sei $\mathcal{E}_M^S = \mathcal{E}^S \cap \mathcal{D}_M$.

Wenn M ein nicht vollständiger Z_p -Modul ist, dann ist $\mathcal{D}_M = \{1\}$ und so gilt $\mathcal{E}_M^S = \{1\}$; wenn aber M ein vollständiger Z_p -Modul ist, dann ist nach der Verallgemeinerung des Einheitensatzes von Dirichlet (siehe z. B. [6]) $\mathcal{E}_M^S$ isomorph zu dem Produkt der endlichen zyklischen Gruppe der Einheitswurzeln von $\mathcal{D}_M$, deren Rang m_M ist, und $q = q_K$ unendlichen zyklischen Gruppen. Im weiteren wird q S -Einheitenrang, oder S -Rang von $\mathcal{E}_M^S$, bzw. $\mathcal{D}_M$ genannt. Die eben erwähnten unendlichen zyklischen Gruppen seien von den Elementen $\varepsilon_1, \dots, \varepsilon_q$ erzeugt. Dann besitzen die Determinanten q -ter Ordnung der Matrix

$$(4) \quad \begin{pmatrix} n_{01} \log |\varepsilon_1|_{\mathcal{P}_{01}} \dots n_{\tau e_\tau} \log |\varepsilon_1|_{\mathcal{P}_{\tau e_\tau}} \\ \vdots \\ n_{01} \log |\varepsilon_q|_{\mathcal{P}_{01}} \dots n_{\tau e_\tau} \log |\varepsilon_q|_{\mathcal{P}_{\tau e_\tau}} \end{pmatrix}$$

einen gemeinsamen, von 0 verschiedenen absoluten Betrag, den wir S -Regulator von $\mathcal{E}_M^S$ bzw. $\mathcal{D}_M$ nennen und mit R_M^S bezeichnen.

Die Lösungen $(x_1, \dots, x_k) \in Z_p^k$ von (1) zu bestimmen heißt nichts anderes, als die Lösungen $\mu \in M$ der Gleichung

$$(5) \quad \prod_{i=0}^{\tau} |N_{K/Q}(\mu)|_{p_i} = a$$

zu suchen. Wenn $\mu \in M$ eine Lösung von (5) ist, dann genügt auch jedes Element der Menge $\mu \cdot \mathcal{E}_M^S \subseteq M$ der Gleichung (5). Eine solche Menge $\mu \mathcal{E}_M^S$ nennen wir eine Lösungsfamilie von (5).

Ist L ein Teilkörper von K , dann bezeichnet M^L die Menge derjenigen Elemente μ von M , für welche für ein beliebiges $\lambda \in L$ ein $0 \neq z \in Z$ existiert, derart daß $z\lambda\mu \in M$

gilt. Bezeichne $\mathcal{D}_M^L$ den Multiplikatorenring von M^L . Es ist leicht einzusehen, daß $\mathcal{D}_M^L$ ein Ring und außerdem ein $\mathcal{D}_M$ -Modul ist, dann stimmt der S -Rang von $\mathcal{D}_M^L$ mit dem von $\mathcal{D}_M$ überein. Wir bezeichnen die Anzahl der Einheiten in $\mathcal{D}_M^L$ mit $\mu \in M^L$ eine Lösung von (5). Diese Menge nennen wir M^L . Wenn keine andere Lösung existiert, dann werden wir sie maximal nennend. Die Lösungsfamilien werden wir mit $\alpha \mathcal{E}_M^L(a)$ bezeichnen. Schließlich wird, wenn $\alpha \in M^L$ eine Lösung von (5) ist, die S -Höhe von α genannt.

die S -Höhe von α genannt.

die S -Höhe von α genannt.

Satz 1. Seien $M = \{\alpha_1, \dots, \alpha_n\}$ ein Z_p -Modul vom Grad $n \geq 2$ mit über Q linear unabhängigen α_i , eine rationale Zahl, für welche $c(a) > 0$ gilt. Bezeichne q das Maximum der S -Ränge der α_i . Dann existiert eine natürliche Zahl $c = c(a) > 0$ derart daß

$$(6) \quad P_{M,a}(T) = \sum_{i=0}^{\infty} c_i T^i$$

Die folgenden beiden Sätze sind Verallgemeinerungen von Satz 1. Wenn L ein Teilkörper vom Grad q über Q ist, setzen wir

$$\lambda(L, M, a) = \sum_{i=0}^{\infty} c_i T^i$$

Satz 2. Außer den Bedingungen von Satz 1, sei L ein Teilkörper von K mit S -Rang q , daß der S -Rang von $\mathcal{D}_M^L$ q ist. Bezeichne n_{L_i} den Grad von $\mathcal{D}_M^L$ über Q . Dann hat $\lambda(L, M, a)$ die Gestalt

$$(7) \quad \lambda(L, M, a) = \sum_{i=0}^{\infty} c_i T^i$$

Den Forderungen von Satz 2 kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

Satz 1 ist eine Verallgemeinerung von Satz 2. Sind c , q und die in O implizierten Konstanten gegeben, dann ist c effektiv bestimmt bzw. ablesbar. In gewissen Fällen aber, kann man sie sogar genau beschreiben. Sei L ein total reeller Körper und L ist [1]. Also hat c z. B. für $L = Q$ die Gestalt

gilt. Bezeichne $\mathcal{D}_M^L$ den Multiplikatorenring in L von M^L und sei ${}^L\mathcal{E}_M^S = \mathcal{E}^S \cap \mathcal{D}_M^L$. Es ist leicht einzusehen, daß $\mathcal{D}_M^L$ eine Z_p -Ordnung von L ist, falls $M^L \neq \{0\}$; (d. h. $\mathcal{D}_M^L$ ist ein Ring und außerdem ein vollständiger Z_p -Modul). Wenn jetzt $M \neq \{0\}$ ist, dann stimmt der S -Rang von ${}^L\mathcal{E}_M^S$ mit dem von $\mathcal{E}^S \cap L$ überein. Mit m_M^L bezeichnen wir die Anzahl der Einheitswurzeln von ${}^L\mathcal{E}_M^S$.

Ist $\mu \in M^L$ eine Lösung von (5), dann genügt jedes Element der Menge $\mu {}^L\mathcal{E}_M^S$ ebenfalls (5). Diese Menge nennen wir eine (M, L) Lösungsfamilie von (1) und auch von (5). Wenn keine andere Lösungsfamilie die Lösungsfamilie (M, L) enthält, dann werden wir sie maximal nennen. Die Anzahl der maximalen (M, L) Lösungsfamilien werden wir mit $\kappa_M^L(a)$ und den S -Regulator von ${}^L\mathcal{E}_M^S$ mit ${}^LR_M^S$ bezeichnen.

Schließlich wird, wenn $\alpha \in K$ ist,

$$h_s(\alpha) = \max_{\varphi \in S_K} |\alpha|_{\varphi}$$

die S -Höhe von α genannt.

2. Ergebnisse

Satz 1. Seien $M = \{\alpha_1, \dots, \alpha_k\}$ ein Z_p -Modul des algebraischen Zahlkörpers K vom Grad $n \geq 2$ mit über Q linear unabhängigen Erzeugenden $\alpha_1, \dots, \alpha_k$ und $a \neq 0$ eine rationale Zahl, für welche (1) unendlich viele Lösungen $(x_1, \dots, x_k) \in Z_p^k$ besitzt. Bezeichne q das Maximum der S -Ränge derjenigen Teilkörper $L \subseteq K$, für welche $M^L \neq \{0\}$. Dann existiert eine nur von $a, K, M, \alpha_1, \dots, \alpha_k$ und P abhängige Konstante $c = c(a) > 0$ derart daß

$$(6) \quad P_{M,a}(T) = c \log^q(\|T\|) + O(\log^{q-1}(\|T\|)).$$

Die folgenden beiden Sätze folgen aus Satz 1 nur in einer nicht effektiven Form. Wenn L ein Teilkörper vom Grad n_L und vom S -Rang q_L des Körpers K ist, dann setzen wir

$$\lambda(L, M, a) = \lambda(L) = n_L^q m_M^L \kappa_M^L(a) (q_L! {}^LR_M^S)^{-1}.$$

Satz 2. Außer den Bedingungen von Satz 1 gelte für alle Teilkörper $L_1, \dots, L_v$ von K mit S -Rang q , daß der S -Rang des Körpers $L_i \cap L_j$ kleiner als q ist für alle $1 \leq i < j \leq v$. Bezeichne n_{L_i} den Grad über Q des Körpers L_i . Dann hat die Konstante c von Satz 1 die Gestalt

$$(7) \quad c = \sum_{i=1}^v \lambda(L_i).$$

Den Forderungen von Satz 2 genügen sehr viele Zahlkörper, im Fall $P \neq \emptyset$ kann man sie sogar genau beschreiben. Es ist nämlich bekannt, daß der Rang eines Körpers K und eines echten Teilkörpers $L \subset K$ genau dann übereinstimmen wenn L ein total reeller Körper und K eine quadratische total imaginäre Erweiterung von L ist [1]. Also hat c z. B. für $P = \emptyset$ und $q > 1$ die Gestalt (7).

Satz 1 ist eine Verallgemeinerung von Satz 1 [3]. In den ersten beiden Sätzen sind c, q und die in O implizierte Konstante im allgemeinen nicht effektiv berechenbar. In gewissen Fällen aber, wenn z. B. der Modul vollständig ist, können auch sie effektiv bestimmt bzw. abgeschätzt werden. Im nächsten Satz wird der Fall eines vollständigen Moduls untersucht.

Satz 3. Sei M ein vollständiger Modul von K , außerdem seien M , K und a wie in Satz 1. Bezeichne q den S -Rang von K sowie D_M bzw. D_K die Diskriminante von M bzw. von K . Sei zuletzt $\mathcal{H} = \max_{1 \leq i \leq n} (h_S(\alpha_i))^n$. Dann gilt

$$(8) \quad |P_{M,a}(\mathbf{T}) - \lambda(K) \log^q(\|\mathbf{T}\|)| \leq 2^q \lambda(K) c_1(a) \log^{q-1}(\|\mathbf{T}\|),$$

$$\text{falls } \log(\|\mathbf{T}\|) \geq c_1(a) \quad \text{wo} \quad c_1(a) = \frac{n+3}{n} |\log a| + \frac{1}{n} \log \left(|D_M|^{1/2} \prod_{j=1}^{\tau} |D_M^{1/2}/D_K^{1/2}|_{p_j} \right) + |\log(n^{1/2} \mathcal{H}^{\tau+1})| + q^3(\tau+1) \left(\frac{7n^2 q}{\log n} \right)^{q-1} R_M^S.$$

Dieser Satz ist eine Verallgemeinerung von Satz 1 [4]. Die nächste Folgerung beschäftigt sich mit der Verteilung der Lösungen von (3). Es bezeichne $P_{M,a}^*(N)$ die Anzahl der Lösungen $(x_1, \dots, x_k; z_1, \dots, z_\tau) \in Z^{k+\tau}$ von (3), für welche $\max_{1 \leq i \leq k} |x_i| \leq N$ gilt.

Folgerung. Seien M bzw. M' der durch die über Q linear unabhängigen Elemente $\alpha_1, \dots, \alpha_k$ von K erzeugte Z - bzw. Z_p -Modul. Wenn für M' , K und $a' = \prod_{j=0}^{\tau} |a|_{p_j}$ die Bedingungen von Satz 1 erfüllt sind dann gilt

$$P_{M,a}^*(N) = c(a', M') \log^q N + O(\log^{q-1} N)$$

mit denselben Konstanten $c(a', M') > 0$ und q wie in Satz 1.

Wenn auch die zusätzlichen Bedingungen von Satz 2 gelten, dann hat $c(a', M')$ die dort angegebene Gestalt.

Wenn endlich M vollständig ist, dann gilt

$$|P_{M,a}^*(N) - \lambda(K, M', a') \log^q N| \leq 2^q \lambda(K, M', a') c_1(a', M') \log^{q-1} N,$$

falls $\log N > c_1(a', M')$ mit der in Satz 3 angegebenen Konstante $c_1(a', M')$.

Der letzte Satz gibt eine asymptotische Formel für die Anzahl der Elemente gegebener Norm und beschränkter S -Höhe eines vollständigen Z_p -Moduls eines Zahlkörpers K .

Sei M ein vollständiger Z_p -Modul von K und bezeichne $P_{M,a}^{**}(\mathbf{T}) = P_{M,a}^{**}(T_0, \dots, T_\tau)$ die Anzahl derjenigen Elemente α von M , für welche

$$(9) \quad |\alpha|_{\varphi_{ij}} \leq T_i \quad (i = 0, \dots, \tau; j = 1, \dots, e_i)$$

und

$$(10) \quad \prod_{i=0}^{\tau} |N_{K/Q}(\alpha)|_{p_i} = a$$

gelten.

Satz 4. Wenn (10) mindestens eine Lösung hat, dann gilt

$$|P_{M,a}^{**}(\mathbf{T}) - \lambda(K) \log^q(\|\mathbf{T}\|)| \leq 2^q q \lambda(K) c_2(a) \log^{q-1}(\|\mathbf{T}\|),$$

$$\text{falls } \log(\|\mathbf{T}\|) \geq c_2(a) = \frac{1}{n} |\log a| + \frac{1}{n} q^2(q+1) \left(\frac{7n^2 q}{\log n} \right)^{q-1} R_M^S.$$

Dieser Satz ist für $M=Z$ Spezialfall von Lemma 9 von V. Die Verteilung der relativen S -Höhen (K und L sind algebraische Zahlkörper) während die Konstante in

Zum Beweis der Sätze braucht man nur jene, welche bei allen Beweisen

Sei Λ ein vollständiger Gitter. $d(\Lambda)$ bezeichne den Grundmesser der Grundmaschen von Λ . [4] angewandt.

Lemma 1. Sei Λ wie oben. $\mathcal{X}(\delta)$ die Menge derjenigen Punkte vom Rand von $\mathcal{X}$ haben, wobei $\mathcal{X}(\delta)$ gleich $V(\mathcal{X})$ bzw. $V(\mathcal{X})$ Punkte des Gitters Λ , welche in

$$(11) \quad |W - V|$$

Lemma 2. Seien $U_0, \dots, U_g$ die Lebesguesche Maße, welche dem Ungleichungssystem

genügen. Dann gilt

$$C(U_0, \dots, U_g)$$

Beweis. Aus den Ungleichungen

$$x_i \geq -(\dots)$$

sowie

$$x_j \geq -(\dots)$$

Wenn die Transformation

$$\bar{x}_i = x_i + \dots$$

auf E^g angewandt wird, dann kann die Rechnung bestimmt werden.

Seien nun

$$L_j(a_1, \dots, a_g)$$

derartige Linearformen mit reellen Koeffizienten

$$(12) \quad \sum_{j=1}^g L_j(a_1, \dots, a_g)$$

Dieser Satz ist für $M = \mathbb{Z}_K^S$ (die S -ganzen Elemente von K) und $a=1$ ein Spezialfall von Lemma 9 von W. L. MAY [5]. Das angeführte Ergebnis gibt nämlich die Verteilung der relativen S -Einheiten der algebraischen Erweiterung K/L an (K und L sind algebraische Zahlkörper) mit einer expliziten Konstanten im Hauptglied während die Konstante im Restglied nicht näher spezifiziert ist.

3. Grundlemmata

Zum Beweis der Sätze brauchen wir mehrere Lemmata. Hier behandeln wir nur jene, welche bei allen Beweisen nötig sind.

Sei Λ ein vollständiger Gitter im r -dimensionalen reellen euklidischen Raum E^r . $d(\Lambda)$ bezeichne den Grundmascheninhalt und $\delta(\Lambda)$ das Minimum der Durchmesser der Grundmaschen von Λ . Das erste Lemma haben wir schon in [3] und in [4] angewandt.

Lemma 1. Sei Λ wie oben und $\mathcal{K}$ eine beschränkte Menge von E^r . Bezeichne $\mathcal{K}(\delta)$ die Menge derjenigen Punkte des Raumes E^r , die höchstens den Abstand δ vom Rand von $\mathcal{K}$ haben, wobei $\delta = \delta(\Lambda)$. Sei das Lebesguesche Maß von $\mathcal{K}$ bzw. $\mathcal{K}(\delta)$ gleich $V(\mathcal{K})$ bzw. $V(\mathcal{K}(\delta))$. Dann gilt für die Anzahl W derjenigen Gitterpunkte des Gitters Λ , welche in $\mathcal{K}$ liegen

$$(11) \quad |W - V(\mathcal{K})/d(\Lambda)| \leq V(\mathcal{K}(\delta))/d(\Lambda).$$

Lemma 2. Seien $U_0, \dots, U_g$ reelle Zahlen mit $U_0 + \dots + U_g \geq 0$. Bezeichne $C(U_0, \dots, U_g)$ das Lebesguesche Maß der Menge derjenigen Elemente $(x_1, \dots, x_g) \in E^g$, welche dem Ungleichungssystem

$$x_i \leq U_i \quad (i = 1, \dots, g)$$

$$-U_0 \leq x_1 + \dots + x_g$$

genügen. Dann gilt

$$C(U_0, \dots, U_g) = (U_0 + \dots + U_g)^n/n!.$$

Beweis. Aus den Ungleichungen folgt unmittelbar

$$x_i \geq -(U_0 + \dots + U_g) + U_i \quad (i = 1, \dots, g)$$

sowie

$$x_1 + \dots + x_g \leq U_1 + \dots + U_g.$$

Wenn die Transformation

$$\bar{x}_i = -x_i + U_i \quad (i = 1, \dots, g)$$

auf E^g angewandt wird, dann kann das Maß der erhaltenen Menge mit einfacher Rechnung bestimmt werden.

Seien nun

$$L_j(a_1, \dots, a_g) = \alpha_{j1}a_1 + \dots + \alpha_{jg}a_g \quad (j = 0, \dots, g)$$

derartige Linearformen mit reellen Koeffizienten, für welche

$$(12) \quad \sum_{j=0}^g \alpha_{jk} = 0 \quad (k = 1, \dots, g).$$

Es ist leicht einzusehen, daß die Determinanten g -ter Ordnung der aus den Koeffizienten dieser Linearformen gebildeten Matrix denselben absoluten Betrag besitzen, den wir mit B bezeichnen.

Lemma 3. Seien $L_j(a_1, \dots, a_g)$ ($j=0, \dots, g$) Linearformen der oben definierten Eigenschaft, $B \neq 0$ und $U_0, \dots, U_g, v_0, \dots, v_g$ reelle Zahlen. Es sei weiter $\max_{j,k} |\alpha_{jk}| \leq A$ und $|v_0 + \dots + v_g| \leq V$. Bezeichne $S(U_0, \dots, U_g)$ die Anzahl der Elemente $(a_1, \dots, a_g) \in Z^g$ für welche

$$(13) \quad L_j(a_1, \dots, a_g) \leq U_j + v_j \quad (j = 0, \dots, g)$$

sich erfüllt. Dann gilt

$$\left| S(U_0, \dots, U_g) - \frac{(U_0 + \dots + U_g)^g}{g! B} \right| \leq \frac{2^g}{g! B} [V + g^2(g+1)A] (U_0 + \dots + U_g)^{g-1},$$

falls $U_0 + \dots + U_g \geq V + g(g+1)A$.

Beweis. Bezeichne $\mathcal{D}$ die Menge der Punkte $(a_1, \dots, a_g) \in E^g$ die (13) genügen. Dann stimmt $S(U_0, \dots, U_g)$ mit der Anzahl der Elemente von $\mathcal{D} \cap Z^g$ überein. Z^g ist ein vollständiges Gitter in E^g mit $d(Z^g) = 1$ und mit $\delta(Z^g) = \sqrt{g}$. So müssen wir nur $V(\mathcal{D})$ bestimmen und $V(\mathcal{D}(\sqrt{g}))$ abschätzen, um das Lemma zu beweisen.

Zunächst ist es mit einfachen geometrischen Überlegungen einzusehen: das durch die Ungleichungen

$$(14) \quad v_j + U_j + \varepsilon_{j1} gA \leq L_j(a_1, \dots, a_g) \leq v_j + U_j + \varepsilon_{j2} gA$$

definierte Gebiet enthält die Menge derjenigen Punkte von E^g , die höchstens den Abstand $\sqrt{g}$ von der Hyperebene

$$L_j(a_1, \dots, a_g) = U_j + v_j$$

haben. In (14) muß man ε_{j1} und ε_{j2} gleich $+1$ oder gleich -1 wählen, und zwar so daß das Maß des erhaltenen Gebietes maximal ausfällt.

Bezeichne $\mathcal{D}_i$ ($i=1, 2$) die durch das Ungleichungssystem

$$L_j(a_1, \dots, a_g) \leq U_j + v_j + \varepsilon_{ji} gA \quad (j = 0, \dots, g)$$

definierte Menge. $\mathcal{D}_2 \setminus \mathcal{D}_1$ enthält dann $\mathcal{D}(\sqrt{g})$. $\mathcal{D}_1$ und $\mathcal{D}_2$ wurden durch Ungleichungssysteme vom Typ (13) definiert, so genügt es nur $V(\mathcal{D})$ zu bestimmen.

Verwenden wir zuerst die Transformation

$$y_j = L_j(a_1, \dots, a_g) \quad (j = 1, \dots, g)$$

auf E^g . Die Determinante dieser Transformation ist B . Aus (12) folgt

$$y_1 + \dots + y_g = -L_0(a_1, \dots, a_g).$$

Bezeichnen wir mit $\mathcal{F}$ die durch

$$y_j \leq U_j + v_j \quad (j = 1, \dots, g)$$

$$-v_0 - U_0 \leq y_1 + \dots + y_g$$

definierte Menge. Wegen den offensichtlich $B \cdot V(\mathcal{D}) = V(\mathcal{F})$, men wir

$$V(\mathcal{D}) =$$

woraus sich

$$\left| V(\mathcal{D}) - \frac{(U_0 + \dots + U_g)^g}{g! B} \right|$$

ergibt, falls $U_0 + \dots + U_g \geq V$ ist

$$V(\mathcal{D}_i) =$$

Auf Grund der Definitionen gel

$$V(\mathcal{D}(\sqrt{g})) \leq \frac{2}{\sqrt{g}}$$

falls $U_0 + \dots + U_g \geq V + g(g+1)A$

Wenn wir die Abschätzung binieren, dann bekommen wir

$$\left| S(U_0, \dots, U_g) - \frac{(U_0 + \dots + U_g)^g}{g! B} \right| + \left| V(\mathcal{D}) - \frac{(U_0 + \dots + U_g)^g}{g! B} \right|$$

falls $U_0 + \dots + U_g \geq V + g(g+1)A$

3.

In diesem Punkt wird $M = \{x_1, \dots, x_n\}$ einen vollständigen $\mathcal{O}_M$ den Multiplikatorenring von $\mathcal{O}_M$ bezeichnen.

Die folgenden zwei Lemmas sind der algebraischen Zahlentheorie entnommen.

Lemma 4. Bezeichne ϱ den Grad von $\mathcal{O}_M$ über $\mathbb{Q}$. Dann gilt

$$(15) \quad n_{ij} |\log |\eta_k|_{\mathcal{O}_M}| \leq$$

für alle $\mathcal{P}_{ij} \in S_K$ gilt.

definierte Menge. Wegen den Eigenschaften der linearen Transformationen gilt offensichtlich $B \cdot V(\mathcal{D}) = V(\mathcal{F})$. Infolge des Obengesagten und Lemma 2 bekommen wir

$$V(\mathcal{D}) = \frac{(U_0 + \dots + U_g + v_0 + \dots + v_g)^g}{g!B},$$

woraus sich

$$\left| V(\mathcal{D}) - \frac{(U_0 + \dots + U_g)^g}{g!B} \right| \leq \frac{2^g V}{g!B} (U_0 + \dots + U_g)^{g-1}$$

ergibt, falls $U_0 + \dots + U_g \geq V$ ist. Auf ähnliche Weise erhält man

$$V(\mathcal{D}_i) = \left[\sum_{j=0}^g (U_j + v_j + \varepsilon_{ji} g A) \right]^g (g!B)^{-1}.$$

Auf Grund der Definitionen gelten $\mathcal{D}(\sqrt{g}) \subseteq \mathcal{D}_2 \setminus \mathcal{D}_1$ und $\mathcal{D}_2 \supseteq \mathcal{D}_1$, und somit auch

$$V(\mathcal{D}(\sqrt{g})) \leq \frac{2g(g+1)A}{g!B} 2^{g-1} g (U_0 + \dots + U_g)^{g-1},$$

falls $U_0 + \dots + U_g \geq V + g(g+1)A$ ist.

Wenn wir die Abschätzungen für $V(\mathcal{D})$ und $V(\mathcal{D}(\sqrt{g}))$ sowie Lemma 2 kombinieren, dann bekommen wir

$$\begin{aligned} \left| S(U_0, \dots, U_g) - \frac{(U_0 + \dots + U_g)^g}{g!B} \right| &\leq |S(U_0, \dots, U_g) - V(\mathcal{D})| + \\ &+ \left| V(\mathcal{D}) - \frac{(U_0 + \dots + U_g)^g}{g!B} \right| \leq \frac{2^g}{g!B} [V + g^2(g+1)A] (U_0 + \dots + U_g)^{g-1}, \end{aligned}$$

falls $U_0 + \dots + U_g \geq V + g(g+1)A$, womit Lemma 3 bewiesen ist.

3. Beweis von Satz 3 und 4

In diesem Punkt wird K immer einen Zahlkörper vom Grad n und $M = \{\alpha_1, \dots, \alpha_n\}$ einen vollständigen Z_p -Modul von K bezeichnen. Wir werden mit $\mathcal{O}_M$ den Multiplikatorring von M und mit $\mathcal{E}_M^S$ die S -Einheitengruppe von $\mathcal{O}_M$ bezeichnen.

Die folgenden zwei Lemmata sind Verallgemeinerungen wohlbekannter Ergebnisse der algebraischen Zahlentheorie. Ihre Beweise sind in [7] erschienen.

Lemma 4. Bezeichne ϱ den S -Rang und R_M^S den S -Regulator von $\mathcal{O}_M$. Es existieren in $\mathcal{O}_M$ multiplikativ unabhängige S -Einheiten $\eta_1, \dots, \eta_{\varrho}$, für welche

$$(15) \quad n_{ij} |\log |\eta_k|_{\mathcal{P}_{ij}}| \leq \varrho \left(\frac{7n^2 \varrho}{\log n} \right)^{g-1} R_M^S = c_3 \quad (k = 1, \dots, \varrho)$$

für alle $\mathcal{P}_{ij} \in S_K$ gilt.

Bezeichne in diesem Punkt $\mathcal{E}$ die durch die S -Einheiten $\eta_1, \dots, \eta_e$ erzeugte multiplikative Gruppe von K .

Lemma 5. Es sei $\mu \in M$ eine Lösung von (5). Dann existieren $\mu' \in M$ und $\varepsilon \in \mathcal{E}$ mit $\mu' = \varepsilon \mu$ und mit

$$(16) \quad n_{ij} |\log |\mu'|_{\mathcal{P}_{ij}}| \leq \frac{1}{2} q^2 \left(\frac{7n^2 q}{\log n} \right)^{e-1} R_M^S + \frac{1}{\tau+1} |\log a| = c_4$$

für alle $\mathcal{P}_{ij} \in S_K$.

Bemerkung. In [7] lauten die Lemmata 4 und 5 etwas anders, aber um die Konstante $c_1(a)$ nicht noch komplizierter zu machen, wenden wir jetzt dieselben in der hier gegebenen Fassung an.

Die nächste Behauptung ist grundlegend für den Beweis von Satz 3 und von Satz 4.

Lemma 6. Seien K, M und $\mathcal{E}$ wie früher, sowie $\mu \in M$ eine (16) genügende Lösung der zu (1) äquivalenten Gleichung (5). Es bezeichne $P_{\mu\mathcal{E}}(\mathbf{T})$ die Anzahl derjenigen Elemente von $\mu\mathcal{E}$, in deren Darstellungen der Gestalt

$$(17) \quad \alpha_1 x_1 + \dots + \alpha_n x_n, \quad (x_1, \dots, x_n) \in Z_P^n$$

die Koeffizienten (2) genügen. Dann gilt

$$\left| P_{\mu\mathcal{E}}(\mathbf{T}) - \frac{n^e}{q! R_{\mathcal{E}}} \log^e (\|\mathbf{T}\|) \right| \leq \frac{(2n)^e}{q! R_{\mathcal{E}}} c_1 \log^{e-1} (\|\mathbf{T}\|),$$

falls $\log (\|\mathbf{T}\|) \geq c_1$, mit der in Satz 1 definierten Konstante c_1 .

Beweis. Zuerst geben wir eine obere Abschätzung für $P_{\mu\mathcal{E}}(\mathbf{T})$.

Wenn $\alpha \in \mu\mathcal{E}$ eine Lösung von (5) ist, dann ist $\alpha \in M$ und so kann α in der Form (17) geschrieben werden. Infolge der Voraussetzungen genügen die x_i (2). Wegen den wohlbekannten Eigenschaften der Bewertungen gelten

$$(18) \quad |\alpha|_{\mathcal{P}_{0i}} \leq n \mathcal{H} T_0 \quad (i = 1, \dots, e_0)$$

und

$$(19) \quad |\alpha|_{\mathcal{P}_{ji}} \leq \mathcal{H} T_j \quad (j = 1, \dots, \tau; i = 1, \dots, e_j).$$

Wegen $\alpha \in \mu\mathcal{E}$ existieren andererseits $a_1, \dots, a_e \in Z$ mit

$$\alpha = \mu \eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}.$$

Aus (18) und (19) folgen nun

$$(20) \quad |\eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}|_{\mathcal{P}_{0i}}^{n_{0i}} \leq \left(\frac{n \mathcal{H}}{|\mu|_{\mathcal{P}_{0i}}} \right)^{n_{0i}} V_{0i} = B_{0i} V_{0i} \quad (i = 1, \dots, e_0)$$

und

$$(21) \quad |\eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}|_{\mathcal{P}_{ji}}^{n_{ji}} \leq \left(\frac{\mathcal{H}}{|\mu|_{\mathcal{P}_{ji}}} \right)^{n_{ji}} V_{ji} = B_{ji} V_{ji} \quad (j = 1, \dots, \tau; i = 1, \dots, e_j)$$

mit $V_{ji} = T_j^{n_{ji}}$ ($j=0, \dots, \tau; i=1, \dots, e_j$).

Es sei

$$L_{ji}(a_1, \dots, a_e) = n_{ji} a_1 \log |\eta_1|_{\mathcal{P}_{ji}} + \dots + n_{ji} a_e \log |\eta_e|_{\mathcal{P}_{ji}}.$$

Die Determinanten q -ter Ordnung gebildeten Matrix haben den ge

Mit dieser Bezeichnung fol

$$(22) \quad L_{ji}(a_1, \dots, a_e) \leq \log$$

Auf (22) ist schon Lemma 3 an

$$V = \left| \sum_{j=0}^{\tau} \sum_{i=1}^{e_j} \right|$$

und mit

$$(23) \quad U_0 + \dots + U$$

Daher erhalten wir

$$(24) \quad P$$

$$+ \frac{(2n)^e}{q! n R_{\mathcal{E}}} [n |\log n|$$

$$\text{falls } \log (\|\mathbf{T}\|) \geq |\log n \mathcal{H}^{\tau+1}| + \frac{1}{n}$$

ausgenutzt.

Jetzt geben wir eine untere Abschätzung für $P_{\mu\mathcal{E}}(\mathbf{T})$ an. Wir betrachten wir (22) früher, und betrachten wir (22) später zu bestimmenden Konstanten c_1 und c_2 .

Seien $(a_1, \dots, a_e) \in Z^e$ eine

Zuerst können wir feststellen, dass (17) geschrieben werden. Aus (17) folgt

und aus dem letzten Ungleichung

$$(25) \quad |\alpha|_{\mathcal{P}_{ji}} \leq$$

für alle $\mathcal{P}_{ji} \in S_K$.

Betrachten wir zuerst nur das Ungleichungssystem kan. Der Beweis stimmt mutatis mutandis mit dem Beweis von Satz 3. Wir brauchen nur das Resultat des Verfa

$$|x_j|_{\mathcal{P}_0} \leq (n^{n/2} \mathcal{H})$$

Wenn sogar

$$B_0 =$$

gewählt wird, dann gilt offensichtl

Die Determinanten q -ter Ordnung der aus den Koeffizienten dieser Linearformen gebildeten Matrix haben den gemeinsamen absoluten Betrag $R_\varepsilon \neq 0$.

Mit dieser Bezeichnung folgt aus (20) und (21)

$$(22) \quad L_{ji}(a_1, \dots, a_q) \leq \log V_{ji} + \log B_{ji} \quad (j = 0, \dots, \tau; i = 1, \dots, e_j).$$

Auf (22) ist schon Lemma 3 anwendbar mit $g = q$, $A = c_3$, $B = R_\varepsilon$

$$V = \left| \sum_{j=0}^{\tau} \sum_{i=1}^{e_j} \log B_{ji} \right| \leq n |\log(n\mathcal{H}^{\tau+1})| + |\log a|$$

und mit

$$(23) \quad U_0 + \dots + U_q = \sum_{j=0}^{\tau} \sum_{i=1}^{e_j} \log V_{ji} = n \log(\|\mathbf{T}\|).$$

Daher erhalten wir

$$(24) \quad P_{\mu\varepsilon}(\mathbf{T}) \leq \frac{n^q \log^q(\|\mathbf{T}\|)}{q! R_\varepsilon} + \frac{(2n)^q}{q! n R_\varepsilon} [n |\log n\mathcal{H}^{\tau+1}| + |\log a| + q^2(q+1)c_3] \log^{q-1}(\|\mathbf{T}\|),$$

falls $\log(\|\mathbf{T}\|) \geq |\log n\mathcal{H}^{\tau+1}| + \frac{1}{n} |\log a| + q(\tau+1)c_3$. Hier wird auch $q+1 \leq n(\tau+1)$ ausgenutzt.

Jetzt geben wir eine untere Schranke für $P_{\mu\varepsilon}(\mathbf{T})$. Seien $L_{ji}(a_1, \dots, a_q)$ wie früher, und betrachten wir (22) mit den, den früheren nicht unbedingt gleichen, später zu bestimmenden Konstanten B_{ji} .

Seien $(a_1, \dots, a_q) \in Z^e$ eine Lösung von (22) und

$$\alpha = \mu \eta_1^{a_1} \cdot \dots \cdot \eta_q^{a_q} = \mu \varepsilon.$$

Zuerst können wir feststellen, daß $\alpha \in \mu\varepsilon$ und so $\alpha \in M$, damit kann α in der Form (17) geschrieben werden. Aus (22) folgt

$$|\varepsilon|_{\mathcal{P}_{ji}}^{n_{ji}} \leq B_{ji} V_{ji}$$

und aus dem letzten Ungleichungssystem

$$(25) \quad |\alpha|_{\mathcal{P}_{ji}} \leq |\mu|_{\mathcal{P}_{ji}} B_{ji}^{1/n_{ji}} T_j = |\mu|_{\mathcal{P}_{ji}} B_j T_j$$

für alle $\mathcal{P}_{ji} \in S_K$.

Betrachten wir zuerst nur die Ungleichungen vom Index $j=0$ von (25). Aus diesem Ungleichungssystem kann eine obere Schranke für die $|x_i|$ bewiesen werden. Der Beweis stimmt mutatis mutandis mit dem von Satz 1 [6] überein, deshalb geben wir nur das Resultat des Verfahrens an:

$$|x_j|_{p_0} \leq (n^{n/2} \mathcal{H}^{n-1} e^{c_4} B_0 |D_M|^{-1/2}) T_0 \quad (j = 1, \dots, n).$$

Wenn sogar

$$B_0 = (n^{n/2} \mathcal{H}^{n-1} e^{c_4} |D_M|^{-1/2})^{-1}$$

gewählt wird, dann gilt offensichtlich

$$\max_{1 \leq i \leq n} |x_i|_{p_0} \leq T_0.$$

Bezeichne $\Omega = \Omega_K$ bzw. $S_\infty = S_{K, \infty}$ die Menge sämtlicher nicht äquivalenten, bzw. sämtlicher nicht äquivalenten archimedischen Bewertungen von K . Für alle $\alpha \in K$ unterscheiden sich die $|\alpha|_{\mathcal{P}}$ von 1 nur für endlich viele $\mathcal{P} \in \Omega$.

Für alle $\mathcal{P} \in \Omega \setminus S_K$ seien

$$B_{\mathcal{P}} = \max_{1 \leq k \leq n} |\alpha_k|_{\mathcal{P}}.$$

Bezeichne α die Menge derjenigen Elemente ω von K , für die

$$|\omega|_{\mathcal{P}_{ji}} \leq |\mu|_{\mathcal{P}_{ji}} B_j T_j \quad (\text{für alle } \mathcal{P}_{ji} \in S_K \setminus S_\infty),$$

$$|\omega|_{\mathcal{P}} \leq B_{\mathcal{P}} \quad (\text{für alle } \mathcal{P} \in \Omega \setminus S_K)$$

gelten. Im weiteren werden wir fordern, daß für jeden möglichen Index j ein $z_j \in Z$ mit $B_j = p_j^{z_j}$ existiere. α ist ein gebrochenes Ideal in K mit Norm

$$N(\alpha) = \left(\prod_{\mathcal{P} \in \Omega \setminus S_K} B_{\mathcal{P}}^{-n_{\mathcal{P}}} \right) \prod_{j=1}^{\tau} \left[(T_j B_j)^{-n} \prod_{i=1}^{e_j} |\mu|_{\mathcal{P}_{ji}}^{-n_{ji}} \right],$$

wo $n_{\mathcal{P}}$ den lokalen Grad von $\mathcal{P} \in \Omega \setminus S_K$ bezeichnet.

Die Koeffizienten von (17) gehören zu Z_p , oder äquivalent formulierend gilt $|x_k|_{\mathcal{P}} \leq 1$ für jede $\mathcal{P} \in \Omega \setminus S_K$. So gilt

$$(26) \quad |\alpha|_{\mathcal{P}} \leq \max_{1 \leq k \leq n} |\alpha_k x_k|_{\mathcal{P}} \leq \max_{1 \leq k \leq n} |\alpha_k|_{\mathcal{P}} = B_{\mathcal{P}}$$

für alle $\mathcal{P} \in \Omega \setminus S_K$. Infolge (25) und (26) gehört α zu α .

Seien $a_j = \min_{a \in Z} \left\{ \max_{\substack{1 \leq k \leq n \\ 1 \leq i \leq e_j}} |\alpha_k|_{\mathcal{P}_{ij}} \leq p_j^a \right\}$, $b_j = \max_{b \in Z} \left\{ \min_{1 \leq i \leq e_j} |\mu|_{\mathcal{P}_{ji}} \leq p_j^b \right\}$, $F_j = p_j^{a_j}$,

$$C_j = p_j^{b_j} \quad (j = 1, \dots, \tau) \text{ und endlich}$$

$$\bar{\alpha}_k = \alpha_k \prod_{j=1}^{\tau} (F_j (C_j B_j T_j)^{-1}) \quad (k = 1, \dots, n).$$

Wegen der Wahl von F_j , C_j , B_j und T_j existieren $u_j \in Z$ mit $F_j (C_j B_j T_j)^{-1} = p_j^{u_j}$ für alle $j = 1, \dots, \tau$. So gelten

$$|\bar{\alpha}_k|_{\mathcal{P}} = |\alpha_k|_{\mathcal{P}} \quad (k = 1, \dots, n)$$

für alle $\mathcal{P} \in \Omega \setminus S_K$ und

$$|\bar{\alpha}_k|_{\mathcal{P}_{ji}} = |\alpha_k|_{\mathcal{P}_{ji}} C_j B_j T_j / F_j \quad (k = 1, \dots, n)$$

für alle $\mathcal{P}_{ji} \in S_K \setminus S_\infty$. Wiederum wegen der Wahl von F_j und C_j gelten

$$|\bar{\alpha}_k|_{\mathcal{P}_{ji}} \leq |\mu|_{\mathcal{P}_{ji}} B_j T_j \quad (k = 1, \dots, n)$$

für alle $\mathcal{P}_{ji} \in S_K \setminus S_\infty$, d. h. α enthält auch die $\bar{\alpha}_k$ für $k = 1, \dots, n$.

Als additive Abelsche Gruppe besitzt α eine Basis $\beta_1, \dots, \beta_n$. Die durch $\bar{\alpha}_1, \dots, \bar{\alpha}_n$ erzeugte freie additive Abelsche Gruppe wird mit $\mathfrak{A}$ bezeichnet. Sie ist eine Unter-

gruppe von α ; so existieren eine

$i = 1, \dots, j)$

mit

(27)

$$\omega_k = a_{kk} \beta_k$$

$$0 \leq a_{kj} \leq$$

$$a_{11} \cdot \dots \cdot a_{nn}$$

$$D = [\alpha: \mathfrak{A}]$$

wo

Die β -s können aus (27) mit

$$\beta_k = \frac{D_{k1}}{D} \omega_k$$

mit $D_{kk} \in Z$ ausgedrückt werden
Außerdem existiert eine un

$$(\omega_1,$$

wo T die Transponierte des Vek
mit

(28)

$$\beta_k = \frac{E_{k1}}{D} \omega_k$$

Wir haben schon $\alpha \in \alpha$ gez

woraus man infolge (28)

mit

$$d_k = z_1 k$$

erhalten kann. So können die

$$x_k = \frac{d_k}{D} \prod_{j=1}^{\tau} p_j^{u_j}$$

geschrieben werden, woraus

(29)

$$|x_k|_{p_j} \leq |D^{-1}|_{p_j} F_j$$

folgt.

Es gilt weiter $D^{1/2}(\beta_1, \dots,$

$$D^{1/2}(\bar{\alpha}_1, \dots,$$

gruppe von α ; so existieren eine Basis $\omega_1, \dots, \omega_n$ von $\mathfrak{A}$ und $a_{ij} \in Z$ ($j=1, \dots, n$; $i=1, \dots, j$)

mit

$$(27) \quad \omega_k = a_{kk}\beta_k + \dots + a_{kn}\beta_n \quad (k=1, \dots, n)$$

$$0 \leq a_{kj} \leq a_{kk} \quad (j=k, \dots, n)$$

$$a_{11} \cdot \dots \cdot a_{nn} = D$$

wo

$$D = [\alpha : \mathfrak{A}] = [D(\bar{\alpha}_1, \dots, \bar{\alpha}_n) / D(\beta_1, \dots, \beta_n)]^{1/2}$$

Die β -s können aus (27) mit den ω -s in der Form

$$\beta_k = \frac{D_{k1}}{D} \omega_1 + \dots + \frac{D_{kn}}{D} \omega_n \quad (k=1, \dots, n)$$

mit $D_{kh} \in Z$ ausgedrückt werden.

Außerdem existiert eine unimodulare Matrix U von ganzen Elementen mit

$$(\omega_1, \dots, \omega_n) = U(\bar{\alpha}_1, \dots, \bar{\alpha}_n)^T$$

wo T die Transponierte des Vektors bezeichnet. So existieren $E_{ij} \in Z$ ($i, j=1, \dots, n$)

mit

$$(28) \quad \beta_k = \frac{E_{k1}}{D} \bar{\alpha}_1 + \dots + \frac{E_{kn}}{D} \bar{\alpha}_n \quad (k=1, \dots, n).$$

Wir haben schon $\alpha \in \mathfrak{a}$ gezeigt, deswegen existieren $z_1, \dots, z_n \in Z$ mit

$$\alpha = z_1 \beta_1 + \dots + z_n \beta_n$$

woraus man infolge (28)

$$\alpha = \frac{d_1}{D} \bar{\alpha}_1 + \dots + \frac{d_n}{D} \bar{\alpha}_n$$

mit

$$d_k = z_1 E_{1k} + \dots + z_n E_{nk} \quad (k=1, \dots, n)$$

erhalten kann. So können die Koeffizienten von (17) in der Form

$$x_k = \frac{d_k}{D} \prod_{j=1}^{\tau} (F_j (C_j B_j T_j)^{-1}) \quad (k=1, \dots, n)$$

geschrieben werden, woraus

$$(29) \quad |x_k|_{p_j} \leq |D^{-1}|_{p_j} F_j^{-1} B_j C_j T_j \quad (k=1, \dots, n; j=1, \dots, \tau)$$

folgt.

Es gilt weiter $D^{1/2}(\beta_1, \dots, \beta_n) = N(\alpha) |D_K|^{1/2}$ und

$$D^{1/2}(\bar{\alpha}_1, \dots, \bar{\alpha}_n) = \left[\prod_{j=1}^{\tau} F_j^n (C_j B_j T_j)^{-n} \right] |D_M|^{1/2}.$$

Wenn man jetzt den expliziten Ausdruck von $N(a)$ und von D anwendet, dann bekommt man

$$|D^{-1}|_{p_j} = C_j^{-n} F_j^n |D_K^{1/2}/D_M^{1/2}|_{p_j} \prod_{i=1}^{e_j} |\mu|_{\mathcal{P}_{ji}}^{n_{ji}} \quad (j = 1, \dots, \tau).$$

Aus (29) folgt nun

$$|x_k|_{p_j} = T_j B_j (F_j/C_j)^{n-1} |D_K^{1/2}/D_M^{1/2}|_{p_j} \prod_{i=1}^{e_j} |\mu|_{\mathcal{P}_{ji}}^{n_{ji}} \quad (j = 1, \dots, \tau).$$

Wenn sogar

$$(30) \quad B_j = (C_j/F_j)^{n-1} |D_M^{1/2}/D_K^{1/2}|_{p_j} \prod_{i=1}^{e_j} |\mu|_{\mathcal{P}_{ji}}^{-n_{ji}}$$

gewählt wird, dann existiert für jedes j ein $u_j \in \mathbb{Z}$ mit $B_j = p_j^{u_j}$ und es gilt noch

$$\max_{1 \leq k \leq n} |x_k|_{p_j} \leq T_j \quad (j = 1, \dots, \tau).$$

Wenn man also in (22) die den obigen Bedingungen entsprechenden Konstanten $B_{ji} = B_j^{n_{ji}}$ ($j=0, \dots, \tau$; $i=1, \dots, e_j$) nimmt, dann gibt es zu jeder Lösung $(a_1, \dots, a_\varrho) \in \mathbb{Z}^\varrho$ von (22) ein $\alpha \in \mu \mathcal{E}$ mit den geforderten Eigenschaften. So ist $P_{\mu \mathcal{E}}(\mathbf{T})$ nicht größer, als die Lösungsanzahl von (22).

Lemma 3 kann wieder mit den bei der oberen Abschätzung bestimmten Konstanten bis auf V angewandt werden. Jetzt ist nämlich

$$V = \left| \sum_{j=0}^{\tau} \sum_{i=1}^{e_j} \log B_{ji} \right| = n \left| \log \prod_{j=0}^{\tau} B_j \right|,$$

wo

$$\prod_{j=0}^{\tau} B_j = (n^{n/2} \mathcal{H}^{n-1} e^{c_4})^{-1} |D_M|^{1/2} \prod_{j=1}^{\tau} \left[|D_M^{1/2}/D_K^{1/2}|_{p_j} (C_j/F_j)^{n-1} \prod_{i=1}^{e_j} |\mu|_{\mathcal{P}_{ji}}^{-n_{ji}} \right].$$

Danach ist

$$V \leq \left| \log \left(|D_M|^{1/2} \prod_{j=1}^{\tau} |D_M^{1/2}/D_K^{1/2}|_{p_j} \right) \right| + |\log a| + n(\tau+2)c_4 + n |\log n^{1/2} \mathcal{H}^{\tau+1}| = c_5$$

mit einfacher Rechnung einzusehen.

Es gilt also

$$P_{\mu \mathcal{E}}(\mathbf{T}) \leq \frac{n^q \log^q(\|\mathbf{T}\|)}{\varrho! R_{\mathcal{E}}} - \frac{(2n)^q}{\varrho! n R_{\mathcal{E}}} (c_5 + \varrho^2(\varrho+1)c_3) \log^{q-1}(\|\mathbf{T}\|),$$

falls $\log(\|\mathbf{T}\|) \geq c_5/n + \varrho(\tau+1)c_3$.

Man kann wieder mit einfacher Rechnung prüfen, daß die in Satz 3 definierte Konstante c_1 größer ist, als die Konstante im Restglied sowohl der oberen als auch der unteren Abschätzung. Damit ist Lemma 6 bewiesen.

Beweis von Satz 3. (1) besitzt unendlich viele Lösungen. M ist in K vollständig, somit gehört jede maximale Lösungsfamilie zu K , deswegen sind die maximalen Lösungsfamilien paarweise disjunkt und ihre Anzahl ist κ_M . Seien $\omega_1, \dots, \omega_{\kappa_M}$ die erzeugenden Elemente der maximalen Lösungsfamilien.

$\mathcal{E}$ hat endlichen Index in $\mathcal{E}_M^S$

$[\mathcal{E}_M^S]$

Sei $\gamma_1, \dots, \gamma_I$ ein vollständiges I
und $\mu_t = \omega_i \gamma_t$ ($i=1, \dots, \kappa_M$; $t=1, \dots, I$)

$\omega_i \mathcal{E}_M^S =$

und die verallgemeinerten Lösun
Wir haben also

$P_{M,a}$

wo $P_{\mu \mathcal{E}}(\mathbf{T})$ die Anzahl der (2)

In Lemma 6 wurde eine we
Formel für $P_{\mu \mathcal{E}}(\mathbf{T})$ bewiesen. Al

$P_{M,a}(\mathbf{T}) = I \cdot \kappa$

und damit ist Satz 3 bewiesen.

Beweis von Satz 4. Man kör
Dann wäre aber die erhaltene K
die Methode des Beweises von S
keine neue Ideen, deshalb überla

4. F

Seien M ein $\mathbb{Z}_p$ -Modul und
 $\varrho \geq 1$ von K . Wenn $\mathcal{E}$ eine Unter
 $\mathcal{E}_M^S$ von L und $0 \neq \mu \in M^L$ mit
Lösungsfamilie von (1) genannt.

Die Anzahl derjenigen Elem
man sie in der Basis $\alpha_1, \dots, \alpha_k$

Lemma 7. Bei den obigen B
und m_t die Anzahl der zu $\mathcal{E}$ gehö

$$P_{\mu \mathcal{E}}(\mathbf{T}) = \frac{(n_1)}{\varrho}$$

und die in O implizierte Konstan

Beweis. Unser Gedankenga
benutzen, daher werden wir il

Seien S_L bzw. S_K die ma
auf L bzw. auf K der Elemente
 K , dem früheren entgegen, drei

$\mathcal{E}$ hat endlichen Index in $\mathcal{E}_M^S$ und sogar

$$[\mathcal{E}_M^S : \mathcal{E}] = m_M R_{\mathcal{E}} / R_M^S = I.$$

Sei $\gamma_1, \dots, \gamma_I$ ein vollständiges Representativesystem der Nebenklassen von $\mathcal{E}_M^S / \mathcal{E}$ und $\mu_{it} = \omega_i \gamma_t$ ($i=1, \dots, \kappa_M$; $t=1, \dots, I$). Dann gilt

$$\omega_i \mathcal{E}_M^S = \bigcup_{t=1}^I \mu_{it} \mathcal{E} \quad (i=1, \dots, \kappa_M)$$

und die verallgemeinerten Lösungsfamilien sind sogar paarweise disjunkt. Wir haben also

$$P_{M,a}(\mathbf{T}) = \sum_{i=1}^{\kappa_M} \sum_{t=1}^I P_{\mu_{it}\mathcal{E}}(\mathbf{T}),$$

wo $P_{\mu_{it}\mathcal{E}}(\mathbf{T})$ die Anzahl der (2) genügenden Elemente von $\mu_{it}\mathcal{E}$ bezeichnet.

In Lemma 6 wurde eine weder von i noch von t abhängende asymptotische Formel für $P_{\mu_{it}\mathcal{E}}(\mathbf{T})$ bewiesen. Also gilt

$$P_{M,a}(\mathbf{T}) = I \cdot \kappa_M P_{\mu_{11}\mathcal{E}}(\mathbf{T}) = m_M \kappa_M \frac{R_{\mathcal{E}}}{R_M} P_{\mu_{11}\mathcal{E}}(\mathbf{T})$$

und damit ist Satz 3 bewiesen.

Beweis von Satz 4. Man könnte Satz 4 auch als Folgerung von Satz 3 beweisen. Dann wäre aber die erhaltene Konstante im Restglied viel schlechter, als wenn man die Methode des Beweises von Satz 3 anwendet. Die ausführliche Darlegung braucht keine neue Ideen, deshalb überlassen wir dieselbe dem Leser.

4. Beweis von Satz 1 und 2

Seien M ein Z_p -Modul und L ein Teilkörper vom Grad n_L und vom S -Rang $q \geq 1$ von K . Wenn $\mathcal{E}$ eine Untergruppe von endlichem Index der S -Einheitengruppe $\mathcal{E}_M^S$ von L und $0 \neq \mu \in M^L$ mit $\mu \mathcal{E} \subseteq M$ sind, dann wird $\mu \mathcal{E}$ eine verallgemeinerte Lösungsfamilie von (1) genannt.

Die Anzahl derjenigen Elemente von $\mu \mathcal{E}$, deren Koeffizienten (2) genügen, falls man sie in der Basis $\alpha_1, \dots, \alpha_k$ von M aufschreibt wird mit $P_{\mu \mathcal{E}}(\mathbf{T})$ bezeichnet.

Lemma 7. Bei den obigen Bezeichnungen seien noch $R_{\mathcal{E}}$ der S -Regulator von $\mathcal{E}$ und $m_{\mathcal{E}}$ die Anzahl der zu $\mathcal{E}$ gehörigen Einheitswurzeln. Dann gilt

$$P_{\mu \mathcal{E}}(\mathbf{T}) = \frac{(n_L)^q m_{\mathcal{E}}}{q! R_{\mathcal{E}}} \log^q(\|\mathbf{T}\|) + O(\log^{q-1}(\|\mathbf{T}\|))$$

und die in O implizierte Konstante hängt nur von $K, L, \mathcal{E}, \alpha_1, \dots, \alpha_k$ und μ ab.

Beweis. Unser Gedankengang ist ähnlich dem, den wir im Beweis von Lemma 6 benutzten, daher werden wir ihn nur dort ausführlich darlegen, wo es nötig ist.

Seien S_L bzw. S_K die maximale Menge der nicht äquivalenten Fortsetzungen auf L bzw. auf K der Elemente von S_0 . Die Elemente von S_L werden zwei, die von K , dem früheren entgegen, drei Indizes besitzen. Der erste Index von $\mathcal{P}_{ij} \in S_L$ oder

von $\mathcal{P}_{ijh} \in S_K$ zeigt, daß die fragliche Bewertung die Fortsetzung von $p_i \in S_0$ ist. Der zweite Index von $\mathcal{P}_{ijh} \in S_K$ zeigt sinngemäß, daß diese die Fortsetzung von $\mathcal{P}_{ij} \in S_L$ ist. Wir werden noch fordern: wenn eine Bewertung des Oberkörpers nur auf dem Teilkörper betrachtet wird dann stimme sie mit der Bewertung überein, woraus sie fortgesetzt wurde. Es wird noch $n_{ijh} = n(\mathcal{P}_{ijh}/p_i)$ und $n_{ij} = n(\mathcal{P}_{ij}/p_i)$ für alle möglichen Indizes gesetzt.

Eine wohlbekannte Eigenschaft des lokalen Grades lautet:

$$n_{ijh} = n(\mathcal{P}_{ijh}/\mathcal{P}_{ij}) n_{ij}.$$

Im weiteren besagt $A \ll B$, daß eine nur von $K, L, \mathcal{E}, \alpha_1, \dots, \alpha_k$ und μ abhängende Konstante E mit $A \leq EB$ existiert.

Wenn nun $\alpha \in \mu\mathcal{E} \subseteq M$ ist, dann gibt es ein $(x_1, \dots, x_k) \in Z_p^k$ mit

$$(31) \quad \alpha = \alpha_1 x_1 + \dots + \alpha_k x_k.$$

Es wird zuerst angenommen, daß die Koeffizienten $x_1, \dots, x_k$ (2) genügen. Dann gilt

$$(32) \quad |\alpha|_{\mathcal{P}_{ijh}} \ll T_i$$

wegen den Eigenschaften der Bewertungen für alle $\mathcal{P}_{ijh} \in S_K$.

Es sei $\eta_1, \dots, \eta_e$ ein Grundeinheitensystem von $\mathcal{E}$. Infolge $\alpha \in \mu\mathcal{E}$ existiert eine Einheitswurzel $\zeta \in \mathcal{E}$ und ein $(a_1, \dots, a_e) \in Z^e$ mit

$$\alpha = \mu \zeta \cdot \eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}.$$

Aus (32) folgt

$$(33) \quad |\eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}|_{\mathcal{P}_{ijh}} \ll T_i$$

für alle $\mathcal{P}_{ijh} \in S_K$.

$\eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}$ ist ein Element von L , und es gilt

$$|\eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}|_{\mathcal{P}_{ij}} \ll T_i$$

für alle $\mathcal{P}_{ij} \in S_L$ wegen (33) und der Normierung der Bewertungen. Aus letzterem folgt

$$(34) \quad a_1 n_{ij} \log |\eta_1|_{\mathcal{P}_{ij}} + \dots + a_e n_{ij} \log |\eta_e|_{\mathcal{P}_{ij}} \leq n_{ij} \log T_i + B_{ij}$$

für alle $\mathcal{P}_{ij} \in S_L$ mit den nur von $K, L, \mathcal{E}, \alpha_1, \dots, \alpha_k$ und μ abhängenden Konstanten B_{ij} .

Man kann Lemma 3 wieder anwenden, um die Anzahl der Lösungen $(a_1, \dots, a_e) \in Z^e$ von (34) zu bestimmen. Damit bekommt man

$$P_{\mu\mathcal{E}}(\mathbf{T}) \leq \frac{(n_L)^e m_{\mathcal{E}}}{e! R_{\mathcal{E}}} \log^e(\|\mathbf{T}\|) + O(\log^{e-1}(\|\mathbf{T}\|)).$$

Um eine obere Abschätzung für $P_{\mu\mathcal{E}}(\mathbf{T})$ zu bestimmen, betrachten wir (34) mit geeignet gewählten, mit den früheren nicht notwendig übereinstimmenden, Konstanten B_{ij} . Es sei $(a_1, \dots, a_e) \in Z^e$ eine Lösung von (34) und

$$\varepsilon = \zeta \eta_1^{a_1} \cdot \dots \cdot \eta_e^{a_e}$$

mit einer beliebigen Einheitswurzel $\zeta \in \mathcal{E}$.

Es wird eine Ganzheitsbasis $\lambda_1, \dots, \lambda_{n_L}$ mit der Diskriminante D gewählt. Dann enthält der durch $z_1, \dots, z_{n_L} \in Z_p$ mit

$$(35) \quad \sum_{i=1}^{n_L} \lambda_i z_i = \alpha$$

Man kann sogar ebenso wie in

$$\max_{1 \leq i \leq n_L} |z_i|_p \leq \frac{1}{p}$$

beweisen.

Wegen $\mu \in M^L$ existieren

$$\mu \lambda_i d_i =$$

mit $b_i \in Z_p$ und die d_i sowie b_i genügen (2). Wenn nun

gesetzt wird, dann ergibt sich

$$(36) \quad \mu \varepsilon = \sum_{i=1}^k b_i \lambda_i d_i$$

Es gilt sogar

$$\max_{i=1, \dots, k} |b_i|_p \leq \frac{1}{p}$$

Also kann durch geeignete Wahl von b_i die (36) (2) genügen. So ergibt sich

$$P_{\mu\mathcal{E}}(\mathbf{T}) \leq \frac{(n_L)^e}{e!}$$

mittels wiederholter Anwendung

Seien L_1 und L_2 Teilkörper von L und (M, L_2) zwei Lösungsfamilien. Dann kann man sie in der Form μ^{L_2} darstellen, die zum demselben Körper M disjunkt. Das folgende Lemma besagt, daß man sie zu verschiedenen Teilkörpern

Lemma 8. Sind $L_1, \dots, L_r$

Lösungsfamilien der Gleichung

$$\sum_{i=1}^r \lambda_i x_i = \alpha$$

Außerdem stimmen der S-Rang

gruppe des Körpers $\bigcap_{i=1}^r L_i$ überein.

Es wird eine Ganzheitsbasis $\lambda_1, \dots, \lambda_{n_L}$ von L so gewählt, daß die Konjugierten von $\lambda_1, \dots, \lambda_{n_L}$ mit der Diskriminanten und mit dem Grad von L abgegrenzt sind. Dann enthält der durch $\lambda_1, \dots, \lambda_{n_L}$ erzeugte Z_P -Modul $\mathcal{O}$. So existieren $z_1, \dots, z_{n_L} \in Z_P$ mit

$$(35) \quad \varepsilon = \lambda_1 z_1 + \dots + \lambda_{n_L} z_{n_L}.$$

Man kann sogar ebenso wie in Lemma 6

$$\max_{1 \leq t \leq n_L} |z_t|_{p_j} \ll T_j \quad (j = 0, \dots, \tau)$$

beweisen.

Wegen $\mu \in M^L$ existieren $0 \neq d_i \in Z$ ($i = 1, \dots, n_L$) mit $\mu \lambda_i d_i \in M$. Somit gilt

$$\mu \lambda_i d_i = \sum_{t=1}^k b_{it} \alpha_t \quad (i = 1, \dots, n_L)$$

mit $b_{it} \in Z_P$ und die d_i sowie die b_{it} hängen nur von $M, L, \alpha_1, \dots, \alpha_k$ und μ ab.

Wenn nun

$$x_i = \sum_{t=1}^{n_L} b_{it} z_t / d_i$$

gesetzt wird, dann ergibt sich

$$(36) \quad \mu \varepsilon = \alpha = \alpha_1 x_1 + \dots + \alpha_k x_k.$$

Es gilt sogar

$$\max_{i=1, \dots, k} |x_i|_{p_j} \ll \max_{t=1, \dots, n_L} |z_t|_{p_j} \quad j = 0, \dots, \tau.$$

Also kann durch geeignete Wahl der B_{ij} erreicht werden, daß die Koeffizienten in (36) (2) genügen. So ergibt sich

$$P_{\mu \varepsilon}(\mathbf{T}) \cong \frac{(n_L)^q m_\varepsilon}{q! R_\varepsilon} \log^q(\|\mathbf{T}\|) + O(\log^{q-1}(\|\mathbf{T}\|))$$

mittels wiederholter Anwendung von Lemma 3. Damit ist Lemma 7 bewiesen.

Seien L_1 und L_2 Teilkörper, sowie M ein Z_P -Modul von K . Wenn (M, L_1) und (M, L_2) zwei Lösungsfamilien von (1) mit nichtleerem Durchschnitt sind, dann kann man sie in der Form $\mu^{L_1} \mathcal{O}_M^S$ bzw. $\mu^{L_2} \mathcal{O}_M^S$ aufschreiben. Also fallen Lösungsfamilien die zum demselben Körper gehören entweder zusammen oder sie sind disjunkt. Das folgende Lemma beschreibt den Durchschnitt solcher Lösungsfamilien, welche zu verschiedenen Teilkörpern gehören.

Lemma 8. Sind $L_1, \dots, L_v$ verschiedene Teilkörper von K und sind

$$\mu^{L_1} \mathcal{O}_M^S, \dots, \mu^{L_v} \mathcal{O}_M^S$$

Lösungsfamilien der Gleichung (1), dann gilt

$$\bigcap_{i=1}^v \mu^{L_i} \mathcal{O}_M^S = \mu \left(\bigcap_{i=1}^v L_i \mathcal{O}_M^S \right).$$

Außerdem stimmen der S -Rang der Einheitengruppe $\bigcap_{i=1}^v L_i \mathcal{O}_M^S$ und der S -Einheitengruppe des Körpers $\bigcap_{i=1}^v L_i$ überein.

Beweis. Im Beweis von Lemma 4 von [3] ist überall S -Einheitengruppe statt Einheitengruppe zu lesen, dann ist der Beweis identisch mit dem in [3].

Beweis von Satz 1. Nach Voraussetzung hat (1) unendlich viele Lösungen bei dem gegebenen a . Sie gehören nach dem Satz von H. P. SCHLICKWEI ([8] Theorem 1) zu endlich vielen maximalen Lösungsfamilien. Seien diese mit $(M, L_1), \dots, (M, L_g)$ bezeichnet. Unter den Teilkörpern $L_1, \dots, L_g$ können auch gleiche vorkommen. Bezeichne $P_{i_1, \dots, i_t}(\mathbf{T})$ die Anzahl derjenigen Elemente des Durchschnittes der Lösungsfamilien $(M, L_{i_1}), \dots, (M, L_{i_t})$ $1 \leq t \leq g$ für welche (2) erfüllt ist. Auf Grund von Lemma 5 ist der Durchschnitt entweder leer, oder eine verallgemeinerte Lösungsfamilie derart, daß die entsprechende S -Einheitengruppe endlichen Index in der S -Einheitengruppe des Körpers $\bigcap_{j=1}^t L_{i_j}$ hat. Die Anzahl der endlichen maximalen Lösungsfamilien ist $O(1)$. Daher gilt

$$(37) \quad P_M(\mathbf{T}) = \sum_{i=1}^g P_i(\mathbf{T}) - \sum_{1 \leq i_1 < i_2 \leq g} P_{i_1 i_2}(\mathbf{T}) + \dots \\ + (-1)^{t-1} \sum_{1 \leq i_1 < \dots < i_t \leq g} P_{i_1 \dots i_t}(\mathbf{T}) + \dots + (-1)^{g-1} P_{1 \dots g}(\mathbf{T}) + O(1).$$

Bei der Bestimmung der Hauptglieder von $P_M(\mathbf{T})$ spielen selbstverständlich nur diejenigen Summanden eine Rolle, für welche der S -Rang von $\bigcap_{j=1}^t L_{i_j}$ genau q ist. Denn nach Lemma 7 gilt

$$P_{i_1 \dots i_t}(\mathbf{T}) = \begin{cases} c_{i_1 \dots i_t} \log^q(\|\mathbf{T}\|) + O(\log^{q-1}(\|\mathbf{T}\|)), & \text{wenn der } S\text{-Rang von } \bigcap_{j=1}^t L_{i_j} \text{ gleich } q \text{ ist,} \\ O(\log^{q'}(\|\mathbf{T}\|)), & \text{wenn der } S\text{-Rang von } \bigcap_{j=1}^t L_{i_j} \text{ gleich } q' < q \text{ ist.} \end{cases}$$

Folglich haben wir

$$P_M(\mathbf{T}) = c \log^q(\|\mathbf{T}\|) + O(\log^{q-1}(\|\mathbf{T}\|)),$$

wo

$$(38) \quad c = \sum_{i=1}^g c_i + \dots + (-1)^{t-1} \sum_{1 \leq i_1 < \dots < i_t \leq g} c_{i_1 \dots i_t} + \dots$$

ist, und wo der Strich an der Summe bedeutet, daß nur über t -Tupel $(i_1, \dots, i_t)$ summiert wird, für welche der S -Rang des Körpers genau q ist.

Da für alle $1 \leq i \leq g$ $P_M(\mathbf{T}) \geq P_i(\mathbf{T})$ ist, gilt $c \geq c_i$ für alle in (38) vorkommenden c_i . Nach der Voraussetzung gilt $\sum_{i=1}^g c_i > 0$; also gibt es ein i mit $c_i > 0$, und somit gilt auch $c > 0$. Damit ist Satz 1 bewiesen.

Beweis von Satz 2. Seien die maximalen Lösungsfamilien von (1) so geordnet, daß $(M, L_1), \dots, (M, L_r)$ $r \leq g$ zu den Körpern $L_1, \dots, L_v$ gehören. Dann haben die Lösungsfamilien (M, L_i) mit $i > r$, ebenso die Durchschnitte $(M, L_j) \cap (M, L_k)$

mit $j, k > r$ und schließlich auch $k > r$ jeweils einen S -Rang

Um das Hauptglied von $P_M(\mathbf{T})$ der (2) genügenden Elemente des $\dots < j_k \leq r$ in Betracht ziehen. Körpers $L_i \cap L_j$ ($1 \leq i < j \leq r$) ($1 \leq i_1 < \dots < i_t \leq r$) kleiner als q .

$$P_M(\mathbf{T}) =$$

mit einem $q' < q$. Es gilt aber für

$$(29) \quad P_i(\mathbf{T}) = \frac{(n_i)^q}{q! L_i}$$

nach Lemma 4.

Die Konstanten im Hauptglied der (2) gehörigen Lösungsfamilien dieses Körpers L_i gehörigen maximalen L dieses Satzes.

Beweis der Folgerung. Man k

$$P_{M,s}^*(\mathbf{T})$$

einfach zeigen. Kombiniert man unmittelbar die Folgerung.

[1] K. Györy, Sur une classe des corps (Debrecen) 22 (1975), 151.

[2] K. Györy et A. Pethő, Sur la distribution des solutions des équations (Acta Math. Acad. Sci. Hungaricae) 31 (1977), 349–363.

[3] —, Über die Verteilung der Lösungen der Gleichungen (Math. Ann.) 237 (1977), 349–363.

[4] —, Über die Verteilung der Lösungen der Gleichungen (Math. Ann.) 237 (1979), 143–165.

[5] W. L. MAY, Binary forms over number fields (Math. Ann.) 237 (1979), 143–165.

[6] O. O'MEARA, Introduction to Quadratic Forms (Math. Ann.) 237 (1979), 143–165.

[7] A. PETHŐ, Beiträge zur Theorie der Gleichungen (Math. Ann.) 237 (1979), 143–165.

[8] H. P. SCHLICKWEI, On norm form equations (Math. Ann.) 237 (1979), 143–165.

[9] W. M. SCHMIDT, Norm form equations (Math. Ann.) 237 (1979), 143–165.

(Eingegangen am 1. März 1980)

mit $j, k > r$ und schließlich auch die Durchschnitte $(M, L_j) \cap (M, L_k)$ mit $j \leq r$ und $k > r$ jeweils einen S -Rang $< q$.

Um das Hauptglied von $P_M(\mathbf{T})$ zu bestimmen, muß man also nur die Anzahl der (2) genügenden Elemente der Lösungsfamilien $(M, L_{j_1}) \cap \dots \cap (M, L_{j_r})$ $1 \leq j_1 < \dots < j_r \leq r$ in Betracht ziehen. Nach Voraussetzung ist aber der S -Rang des Körpers $L_i \cap L_j$ ($1 \leq i < j \leq r$) und folglich auch des Körpers $L_{i_1} \cap \dots \cap L_{i_t}$ ($1 \leq i_1 < \dots < i_t \leq r$) kleiner als q . Daher haben wir

$$P_M(\mathbf{T}) = \sum_{i=1}^r P_i(\mathbf{T}) + O(\log^{q'}(\|\mathbf{T}\|))$$

mit einem $q' < q$. Es gilt aber für alle $i = 1, \dots, r$

$$(29) \quad P_i(\mathbf{T}) = \frac{(n_i)^q m_M^{L_i}}{q! L_i R_M^S} \log^q(\|\mathbf{T}\|) + O(\log^{q-1}(\|\mathbf{T}\|))$$

nach Lemma 4.

Die Konstanten im Hauptglied von (39) sind für alle, zum gleichen Körper gehörigen Lösungsfamilien dieselben. Benutzen wir nun, daß die Anzahl der zum Körper L_i gehörigen maximalen Lösungsfamilien $\kappa_M^{L_i}$ ist, so erhalten wir den Beweis dieses Satzes.

Beweis der Folgerung. Man kann

$$P_{M,a}^*(N) = P_{M',a'}(N, 1, \dots, 1)$$

einfach zeigen. Kombiniert man dies mit dem entsprechenden Satz, so ergibt sich unmittelbar die Folgerung.

Literatur

- [1] K. GYÖRY, Sur une classe des corps de nombres algébriques et ses applications, *Publ. Math. (Debrecen)* **22** (1975), 151—175.
- [2] K. GYÖRY et A. PETHŐ, Sur la distribution des solutions des équations du type "norm-forme", *Acta Math. Acad. Sci. Hungar.* **26** (1975), 135—142.
- [3] —, Über die Verteilung der Lösungen von Normformen Gleichungen II, *Acta Arith.* **32** (1977), 349—363.
- [4] —, Über die Verteilung der Lösungen von Normformen Gleichungen III, *Acta Arith.* **37** (1979), 143—165.
- [5] W. L. MAY, Binary forms over number fields, *Ann. of Math.* **79** (1964), 597—615.
- [6] O. O'MEARA, *Introduction to Quadratic Forms*, Berlin 1963.
- [7] A. PETHŐ, Beiträge zur Theorie der S -Ordnungen, *Acta Math. Acad. Sci. Hungar.* **37** (1981), 51—57.
- [8] H. P. SCHLICKWEI, On norm form equations, *J. Number Theory* **9** (1977), 370—380.
- [9] W. M. SCHMIDT, Norm form equations, *Ann. of Math.* **96** (1972), 526—551.

(Eingegangen am 4. September 1978)