and $2k^{1/2}B'$ respectively. Further, as in [1], we see that the height of α'_n is at most $(2dA')^{4nD}A^{2D/p}$, whence, since $2D/p < \frac{1}{2}$ when $p > k^{1/2}$, it follows that $b'_1, \ldots, b'_n$ and α'_n have the properties asserted at the beginning.

3. Proof of Theorem 1. The proof is completed by induction. There is plainly no loss of generality in assuming that $B' \geqslant c_1^8$; to begin with we assume that also $A \geqslant c_2^8$, whence

$$\log A \log(\delta^{-1}B') > \log(c_2 A^{1/2}) \log(c_1^2 \delta^{-1} B').$$

Then all the hypotheses recorded in § 2 hold with $b'_1, \ldots, b'_n$ and α'_n in place of $b_1, \ldots, b_n$ and α_n respectively; the new values of A, B, B' are $c_2 A^{1/2}$, $c_1 B$, $c_1 B'$, and δ is replaced by δ/c_1. We suppose further, as we may, that d is taken, at the outset, as the degree of K so that the values of c_1, c_2 remain unaltered in the inductive discussion.

We now repeat the previous argument and obtain for each $s = 1, 2, \ldots$ a set of integers $b_1^{(s)}, \ldots, b_{n-1}^{(s)}$ and $b_n^{(s)}$ with absolute values at most $c_1^s B$ and $c_1^s B'$ respectively, and an element $\alpha_n^{(s)}$ in K with height at most $c_2^{1+\frac{1}{2}+\ldots+(\frac{1}{2})^{s-1}} A^{(\frac{1}{2})^s}$, such that (1) holds with $b_1^{(s)}, \ldots, b_n^{(s)}$ and $\alpha_n^{(s)}$ in place of $b_1, \ldots, b_n$ and α_n respectively. The algorithm terminates for some $s \leqslant 2 \log\log A$ when the height of $\alpha_n^{(s)}$ is at most c_2^8; and $b_1^{(s)}, \ldots, b_n^{(s)}$ then have absolute values at most

$$H = (\log A)^{c_3} \max(B, B').$$

But the number on the right of (1) is at most $H^{-\sqrt{C}}$; for if $B \geqslant B'$ then either $H \leqslant B^2$ or $H \leqslant (\log A)^{2c_3}$, and the assertion is obvious if $B < B'$. Thus one concludes from the result of [1] that the inequality is untenable if C is sufficiently large, and the theorem follows.

References

[1] A. Baker, *A sharpening of the bounds for linear forms in logarithms*, Acta Arith. 21 (1972), pp. 117–129.

[2] — *Contributions to the theory of Diophantine equations*; *I: On the representation of integers by binary forms*, Philos. Trans. Roy. Soc. London A263 (1968), pp. 173–191.

[3] N. I. Feldman, *An effective sharpening of the exponent in Liouville's theorem*, (in Russian), Izv. Akad. Nauk SSSR ser. mat. 35 (1971), pp. 973–990.

Received on 10. 5. 1972 (282)

ACTA ARITHMETICA
XXIV (1973)

On Waring's problem in algebraic number fields

by

TIKAO TATUZAWA (Tokyo)

Dedicated to Professor Carl Ludwig Siegel on his 75th birthday

Since Siegel succeeded in dealing with Waring's problem in algebraic number fields, there have appeared many works under almost the same title (see [8], [9], [12], [5] and [1]). I should like to use this opportunity to add some corrections and justification for my former results. The result presented at the United States–Japan seminar at Tokyo in 1971 is not the best. Nevertheless, we seem to be able to place our hope in its further developments, because the result is based on some remarkable new research due to Mitsui (see [7]). My concern is mainly the treatment of Fourier analysis.

1. Preliminaries and basic domains. In the first place, we shall summarize the main results obtained so far. Let K be an algebraic number field of degree n, let $K^{(l)}$ $(1 \leqslant l \leqslant r_1)$ be r_1 real conjugate fields, and let $K^{(m)}$, $K^{(m+r_2)}$ $(r_1+1 \leqslant m \leqslant r_1+r_2)$ be r_2 pairs of complex conjugate fields, so that $n = r_1+2r_2$. Let $\mathfrak{d}$ be the different of K, and d the discriminant of K. We can choose $\omega_1, \omega_2, \ldots, \omega_n$ as an integral basis of K and $\varrho_1, \varrho_2, \ldots, \varrho_n$ as a basis of $\mathfrak{d}^{-1}$, satisfying

$$\operatorname{trace}(\varrho_r \omega_s) = \begin{cases} 1 & (r = s), \\ 0 & (r \neq s). \end{cases}$$

We denote by $\mathfrak{o}$ the integral domain of all algebraic integers in K. We denote by $P(T)$ the set of $(z_1, \ldots, z_n)$ satisfying

$$0 \leqslant \lambda^{(l)} \leqslant T, \quad |\lambda^{(m)}| \leqslant T$$

where

$$\lambda = \omega_1 z_1 + \ldots + \omega_n z_n,$$

the indices l and m being over the set of numbers cited above. On the other hand,

$$\sum_{\lambda \in P(T)}$$

means that λ runs over all integers restricted as above. We write

$$\xi = \varrho_1 x_1 + \ldots + \varrho_n x_n,$$

$$L(\xi) = \sum_{\lambda \in P(T)} E(\lambda^k \xi) = \sum_{\lambda \in P(T)} \exp\{2\pi i \operatorname{trace}(\lambda^k \xi)\}.$$

Then the number of solutions of

$$\lambda_1^k + \lambda_2^k + \ldots + \lambda_s^k = \nu, \qquad \lambda_j, \nu \in \mathfrak{o}$$

is expressible by the integral

$$I(\nu) = \int_U \ldots \int L(\xi)^s E(-\nu\xi)\, dx,$$

where U is the unit cube; namely,

$$U = \{(x_1, \ldots, x_n);\ 0 \leqslant x_1 < 1, \ldots, 0 \leqslant x_n < 1\}.$$

Throughout the paper, we write

$$t = T^{1-a}, \qquad h = T^{k-1+a} \qquad (0 < a < 1).$$

We denote by Γ the set of

$$\gamma = \varrho_1 x_1 + \varrho_2 x_2 + \ldots + \varrho_n x_n,$$

fulfilling the conditions:

$$(x_1, \ldots, x_n) \in U, \qquad x_r \text{ rational numbers}, \qquad N(\mathfrak{a}) \leqslant t^n,$$

where $\mathfrak{a}$ is derived from the unique expression

$$\gamma\mathfrak{d} = \frac{\mathfrak{b}}{\mathfrak{a}}, \qquad (\mathfrak{a}, \mathfrak{b}) = \mathfrak{o},$$

writing $\gamma \to \mathfrak{a}$ for convenience. For a given $\mathfrak{a} \subseteq \mathfrak{o}$, the number of γ in Γ, subject to $\gamma \to \mathfrak{a}$, is $O(N(\mathfrak{a}))$. Define the basic domain B_γ, for every $\gamma \in \Gamma$, subject to $\gamma \to \mathfrak{a}$, by

$$\Big\{(x_1, \ldots, x_n);\ (x_1, \ldots, x_n) \in U,\ \xi = \varrho_1 x_1 + \ldots + \varrho_n x_n,$$

$$\prod_{j=1}^{n} \operatorname{Max}(h\,|\xi^{(j)} - \gamma_0^{(j)}|, t^{-1}) \leqslant N(\mathfrak{a})^{-1}, \text{ for any } \gamma_0 \equiv \gamma \bmod \mathfrak{d}^{-1},$$

whose contribution to ξ does not vanish$\Big\}$.

$S = U - \sum_{\gamma \in \Gamma} B_\gamma$ is termed the supplementary domain. To calculate $I(\nu)$, we divide the integral as follows:

$$I(\nu) = \sum_{\gamma \in \Gamma} \int_{B_\gamma} \ldots \int + \int_S \ldots \int$$

According to Siegel, if T is sufficiently large, and $\gamma_1 \neq \gamma_2$, then

$$B_{\gamma_1} \cap B_{\gamma_2} = \emptyset.$$

Suppose that

$$\gamma \in \Gamma, \qquad \gamma \to \mathfrak{a}, \qquad (x_1, \ldots, x_n) \in B_\gamma,$$

$$\xi = \varrho_1 x_1 + \ldots + \varrho_n x_n, \qquad \eta = \omega_1 y_1 + \ldots + \omega_n y_n.$$

Let

$$S(\gamma) = \sum_{\lambda} E(\lambda^k \gamma),$$

the summation being over a complete residue system mod $\mathfrak{a}$. It is known that the sum is independent of the choice of system and there exists a constant $c(\varepsilon)$ such that

$$|S(\gamma)| \leqslant c(\varepsilon) N(\mathfrak{a})^{1-\frac{1}{k}+\varepsilon},$$

for any positive ε. We can derive the formula

$$L(\xi) = N(\mathfrak{a})^{-1} S(\gamma) \int_{P(T)} \ldots \int E\left(\eta^k (\xi - \gamma)\right) dy + O(T^{n-a}).$$

If we write

$$T^k(\xi - \gamma) = \tau,$$

then we have

$$\int_{P(T)} \ldots \int E\left(\eta^k (\xi - \gamma)\right) dy \ll T^n N\{\operatorname{Min}(1, |\tau^{(j)}|^{-1/k})\},$$

$$\int_X \ldots \int N\{\operatorname{Min}(1, |\tau^{(j)}|^{-1/k})\}\, dx \ll T^{-nk},$$

provided $s > k$, X being the whole n-dimensional Euclidean space. With the aid of these results (see [12]), we may have the following

THEOREM 1. *If* $s \geqslant 4nk$, *then*

$$\sum_{\gamma \in \Gamma} \int_{B_\gamma} \ldots \int L(\xi)^s E(-\nu\xi)\, dx = \mathfrak{S}(\nu) J(\mu) T^{n(s-k)} + O(T^{n(s-k)-1/4})$$

provided $\nu \in P(T^k)$ *and* $\mu = \nu T^{-k}$.

$\mathfrak{S}(\nu)$ and $J(\mu)$ can be defined in the following way. If γ runs over a reduced residue system of $(\mathfrak{a}\mathfrak{d})^{-1} \bmod \mathfrak{d}^{-1}$, then the sum

$$H(\mathfrak{a}) = \sum_{\gamma} N(\mathfrak{a})^{-s} S(\gamma)^s E(-\nu\gamma)$$

for $\nu \in \mathfrak{o}$, is independent of the choice of system. The series

$$\mathfrak{S}(\nu) = \sum_{\mathfrak{a}} H(\mathfrak{a})$$

is called a singular series which is absolutely convergent for $s \geqslant 4k$ and can be expressed as

$$\mathfrak{S}(\nu) = \prod_{\mathfrak{p}} \chi_{\mathfrak{p}}(\nu)$$

where

$$\chi_{\mathfrak{p}}(\nu) = \sum_{l=0}^{\infty} H(\mathfrak{p}^l).$$

When Landau introduced Vinogradov's new circle method for Waring's problem (see [6]), he derived the following formula:

$$I(c) = \int_{-\infty}^{\infty} e^{-2\pi i c v}\Big(\int_0^1 e^{2\pi i v w^k}\,dw\Big)^s\,dv = \frac{\Gamma^s\Big(1+\frac{1}{k}\Big)}{\Gamma\Big(\frac{s}{k}\Big)}\,c^{\frac{s}{k}-1}$$

for $0 < c \leqslant 1$ and $s > k$. In proving the formula he used the Dirichlet integral theorem. Later on Siegel extended this integral to algebraic number fields (see [9]) and considered the integral

$$J(\mu) = \int_X \dots \int E(-\mu\xi)\Big\{\int_P \dots \int E(\xi\eta^k)\,dy\Big\}^s dx,$$

setting

$$\xi = \varrho_1 x_1 + \dots + \varrho_n x_n, \qquad \eta = \omega_1 y_1 + \dots + \omega_n y_n,$$

where $P = P(1)$ and $\mu \neq 0$, $\mu \in P(1)$. By means of Fourier transformation, he proved

$$J(\mu) = |d|^{(1-s)/2} \prod_{l=1}^{r_1} F(\mu^{(l)}) \prod_{m=r_1+1}^{r_1+r_2} H(\mu^{(m)})$$

for $s > k$. The definitions of these new functions can be seen in the following section.

2. Local theory of Waring's problem in algebraic number fields. We shall sketch, in the first place, the non-Archimedean valuation theory of a field K. Let $\mathfrak{p}$ be a prime ideal of K and let $K_{\mathfrak{p}}$ be the completion of K with respect to this valuation. Let α be a number of K. We denote by $w_{\mathfrak{p}}(\alpha)$ or briefly $w(\alpha)$ the exponent with which $\mathfrak{p}$ enters into the canonical factorization of α. Suppose that A is a number of $K_{\mathfrak{p}}$ and is defined by the Cauchy sequence $\{\alpha_n\}$, $\alpha_n \in K$. Since there exists a $\lim_{n\to\infty} w(\alpha_n)$, we denote it by $w(A)$. Then we have

$$w(AB) = w(A) + w(B), \qquad w(A+B) \geqslant \operatorname{Min}\big(w(A), w(B)\big),$$

for every A, B in $K_{\mathfrak{p}}$. The last inequality can be replaced by an equality when $w(A) \neq w(B)$.

In $K_{\mathfrak{p}}$, the series

$$A_1 + A_2 + \dots + A_n + \dots$$

converges if and only if $w(A_n) \to \infty$ (as $n \to \infty$). Let $f(x)$, $g(x)$ and $h(x)$ be power series in $K_{\mathfrak{p}}$, formally satisfying $f(x)g(x) = h(x)$. Let $A \in K_{\mathfrak{p}}$. If $f(A)$ and $g(A)$ is convergent, then $h(A)$ is also convergent and satisfies $f(A)g(A) = h(A)$. Let p be a prime contained in $\mathfrak{p}$ and $\mathfrak{p}^e \| p$. We denote by $w_p(n)$ the exponent with which p enters into the canonical factorization of n, where n does not necessarily mean the degree of K for a little while. Let

$$n = a_0 + a_1 p + \dots + a_r p^r \qquad (0 \leqslant a_j < p)$$

be a p-adic representation of n, and

$$s(n) = a_0 + a_1 + \dots + a_r.$$

Clearly $s(n) \geqslant 1$ for $n \geqslant 1$. It follows from

$$w_p(n!) = \frac{n - s(n)}{p-1}$$

that

$$w\Big(\frac{A^n}{n!}\Big) = w(A) + (n-1)\Big(w(A) - \frac{e}{p-1}\Big) + \frac{s(n)-1}{p-1}e$$

and from

$$w_p(n) \leqslant \frac{\log n}{\log p} \leqslant \frac{n-1}{p-1}$$

that

$$w\Big(\frac{B^n}{n}\Big) \geqslant w(B) + (n-1)\Big(w(B) - \frac{e}{p-1}\Big)$$

(see [2]). Because of what we have just proved, we know that the series

$$1 + A + \frac{1}{2!}A^2 + \dots + \frac{1}{n!}A^n + \dots$$

is convergent provided

$$w(A) > \frac{e}{p-1},$$

so we denote it by $\exp A$, and the series

$$B - \frac{1}{2}B^2 + \frac{1}{3}B^3 - \dots + (-1)^{n-1}\frac{1}{n}B^n + \dots$$

is also convergent provided

$$w(B) > \frac{e}{p-1},$$

so we denote it by $\log(1+B)$.

We now define an additive group $\{A\}$ in $K_\mathfrak{p}$ by

$$\left\{A;\ A \in K_\mathfrak{p},\ w(A) > \frac{e}{p-1}\right\},$$

and a multiplicative group $\{M\}$ in $K_\mathfrak{p}$ by

$$\left\{M;\ M \in K_\mathfrak{p},\ w(M-1) > \frac{e}{p-1}\right\}.$$

On account of

$$w(\exp A - 1) = w(A) \quad \text{and} \quad w(\log M) = w(M-1),$$

we have

$$A \in \{A\} \Rightarrow \exp A \in \{M\} \quad \text{and} \quad M \in \{M\} \Rightarrow \log M \in \{A\}.$$

By usual computation, putting $B = \exp A - 1$, we have

$$B - \frac{1}{2}B^2 + \ldots + (-1)^{n-1}\frac{1}{n}B^n = A + \sum_{k>n}\sum_{\substack{p_1+\ldots+p_m=k \\ 1\leqslant m\leqslant n}}\left(\pm\frac{1}{m}\frac{A^{p_1+\ldots+p_m}}{p_1!\ldots p_m!}\right),$$

whence follows

$$\log[\exp A] = A$$

if $w(A) > \dfrac{e}{p-1}$, namely if $A \in \{A\}$, since

$$w\left(\frac{1}{m}\frac{A^{p_1+\ldots+p_m}}{p_1!\ldots p_m!}\right)$$

$$\geqslant (p_1+\ldots+p_m)w(A) - \frac{p_1-s(p_1)}{p-1}e - \ldots - \frac{p_m-s(p_m)}{p-1}e - \frac{m-1}{p-1}e$$

$$\geqslant k\left(w(A) - \frac{e}{p-1}\right) + \frac{e}{p-1}.$$

Also by usual computation, putting $A = \log(1+B)$, we have

$$1 + A + \ldots + \frac{1}{n!}A^n = 1 + B + \sum_{k>n}\sum_{\substack{p_1+\ldots+p_m=k \\ 1\leqslant m\leqslant n}}\left(\pm\frac{1}{m!}\frac{B^{p_1+\ldots+p_m}}{p_1\ldots p_m}\right),$$

whence follows $\exp[\log(1+B)] = 1+B$ if $w(B) > \dfrac{e}{p-1}$; in other words,

$$\exp[\log M] = M$$

if $M \in \{M\}$, since

$$w\left(\frac{1}{m!}\frac{B^{p_1+\ldots+p_m}}{p_1\ldots p_m}\right)$$

$$\geqslant (p_1+\ldots+p_m)w(B) - \frac{p_1-1}{p-1}e - \ldots - \frac{p_m-1}{p-1}e - \frac{m-s(m)}{p-1}e$$

$$\geqslant k\left(w(B) - \frac{e}{p-1}\right) + \frac{e}{p-1}.$$

We can also prove that

$$w\left(\frac{A_1^q}{q!}\frac{A_2^r}{r!}\right) > (q+r)\left\{\operatorname{Min}\left(w(A_1), w(A_2)\right) - \frac{e}{p-1}\right\}.$$

Hence we have

$$A_1, A_2 \in \{A\} \Rightarrow \exp(A_1+A_2) = \exp A_1 \cdot \exp A_2.$$

We put $X = \log M_1 + \log M_2$ when $M_1, M_2 \in \{M\}$. It follows that

$$\exp X = \exp[\log M_1]\cdot\exp[\log M_2] = M_1 M_2.$$

Since $X \in \{A\}$, we obtain

$$M_1, M_2 \in \{M\} \Rightarrow \log(M_1 M_2) = \log M_1 + \log M_2.$$

Under the full use of these results we get the following lemma. Its formulation, not using the terminology of p-adic numbers, is due to the late Prof. Takagi.

LEMMA 1. *Let* $\mathfrak{p}$ *be a prime ideal in* K *and let* p *be a prime contained in* $\mathfrak{p}$. *Assume that* $N(\mathfrak{p}) = p^f$, $\mathfrak{p}^e \| p$, $p^\theta \| k$, *and*

$$l_0 \geqslant \begin{cases} 1 & (\theta = 0), \\ \left[\dfrac{e}{p-1}\right] + \theta e + 1 & (\theta > 0). \end{cases}$$

If the congruence

$$\xi^k \equiv \alpha \bmod \mathfrak{p}^\theta,$$

for $\alpha \in \mathfrak{o}$, *is solvable with* ξ *not divisible by* $\mathfrak{p}$, *then the congruence*

$$\xi^k \equiv \alpha \bmod \mathfrak{p}^l$$

is also solvable for any $l \geqslant l_0$.

Proof (see [12], p. 328).

LEMMA 2. *Let* a_{ij} $(1 \leqslant i \leqslant r, 1 \leqslant j \leqslant s)$ *be rational integers. Then the congruence*

$$\begin{cases} a_{11}x_1 + \ldots + a_{1s}x_s \equiv 0 \\ \cdots\cdots\cdots\cdots \\ a_{r1}x_1 + \ldots + a_{rs}x_s \equiv 0 \end{cases} \bmod p^l$$

has a non-trivial solution; namely, there exists a solution $(x_1, \ldots, x_s)$ *in which at least one* x_j *cannot be divided by a prime* p, *provided* $s > r$.

Proof. Suppose that $(a_{1j}, \ldots, a_{rj}) = d_j$ and

$$p^m \| (d_1, \ldots, d_s) \quad \text{for} \quad 0 \leqslant m < l,$$

since the lemma is trivial for the case $m \geqslant l$. Let $a_{ij} = p^m a'_{ij}$. Then the equations can be reduced to

$$\begin{cases} a'_{11}x_1 + \ldots + a'_{1s}x_s \equiv 0 \\ \ldots\ldots\ldots\ldots \\ a'_{r1}x_1 + \ldots + a'_{rs}x_s \equiv 0 \end{cases} \mod p^{l-m}.$$

Hence we may assume that $p \nmid d'_1$ and $p \nmid a'_{11}$ without loss of generality. As Artin indicated, the congruence equations can be reduced to

$$\begin{cases} a'_{11}x_1 + a'_{12}x_2 + \ldots + a'_{1s}x_s \equiv 0 \\ \qquad b'_{22}x_2 + \ldots + b'_{2s}x_s \equiv 0 \\ \qquad \ldots\ldots\ldots\ldots \\ \qquad b'_{r2}x_2 + \ldots + b'_{rs}x_s \equiv 0 \end{cases} \mod p^{l-m}.$$

Now the proof can be obtained by induction, as Artin showed in the first part of his Galois theory.

Lemma 3. *Let* ϱ *be a primitive root* $\bmod \mathfrak{p}$ *and let* π *be an integer satisfying* $\pi \in \mathfrak{p}$, $\pi \notin \mathfrak{p}^2$ (*write briefly by* $\mathfrak{p} \| \pi$), *where* $\mathfrak{p}$ *is a prime ideal. Then* $\alpha \in \mathfrak{o}$ *is always expressible as*

$$\alpha \equiv \Big(\sum_{j=0}^{f-1} a_{0j}\varrho^j\Big) + \Big(\sum_{j=0}^{f-1} a_{1j}\varrho^j\Big)\pi + \ldots + \Big(\sum_{j=0}^{f-1} a_{e-1,j}\varrho^j\Big)\pi^{e-1} \bmod \mathfrak{p}^{le}$$

for any positive integer l, *where* $N(\mathfrak{p}) = p^f$, $\mathfrak{p}^e \| p$ *and* a_{ij} *can be uniquely determined* $\bmod p$.

Proof. It is known that there exist $c_{0j} \bmod p$ such that

$$\alpha \equiv c_{00} + c_{01}\varrho + \ldots + c_{0,f-1}\varrho^{f-1} \bmod \mathfrak{p}.$$

Furthermore, we can determine $c_{rj} \bmod p$ such that

$$\alpha \equiv \sum_{r=0}^{le-1} \Big(\sum_{j=0}^{f-1} c_{rj}\varrho^j\Big)\pi_r \bmod \mathfrak{p}^{le},$$

π_j being taken in $\mathfrak{o}$ satisfying

$$\mathfrak{p}^j \| \pi_j.$$

Let $r = eq + i$ $(0 \leqslant i < e)$. If we put

$$\pi_r = p^q \pi^i,$$

then the congruence mentioned above turns to

$$\alpha \equiv \sum_{q=0}^{l-1} p^q \Big\{\sum_{i=0}^{e-1}\Big(\sum_{j=0}^{f-1} c_{eq+i,j}\varrho^j\Big)\pi^i\Big\} \bmod \mathfrak{p}^{le}.$$

The lemma follows by taking

$$a_{ij} = c_{ij} + c_{i+e,j}p + \ldots + c_{i+(l-1)e,j}p^{l-1}.$$

Let J_k be the ring generated by the kth powers of all integers in K. On account of the identity

$$k!\gamma = \sum_{l=0}^{k-1} (-1)^{k-1-l}\binom{k-1}{l}\{(\gamma + l)^k - l^k\}$$

where $\gamma \in \mathfrak{o}$, the ring J_k becomes an order.

Lemma 4 (Siegel). *Let* $\mathfrak{p}$ *be a prime ideal of* K, *let* p *be a prime contained in* $\mathfrak{p}$ *and let* $N(\mathfrak{p}) = p^f$. *Let* l *be a positive rational integer. There exist* η_r *in* $\mathfrak{o}$ *and positive rational integers* s $(\leqslant fl)$, q_r (*some power of* p) *such that the linear form*

$$a_1\eta_1^k + a_2\eta_2^k + \ldots + a_s\eta_s^k, \qquad a_j = 0, 1, \ldots, q_j - 1 \qquad (1 \leqslant j \leqslant s)$$

uniquely represents all numbers of $J_k \bmod \mathfrak{p}^l$.

Proof. Let g be the order of the module generated by the classes represented by elements of $J_k \bmod \mathfrak{p}^l$. Take $\eta_1 \notin \mathfrak{p}$. Then the set

$$\{x;\ x \text{ rational integer},\ x\eta_1^k \equiv 0 \bmod \mathfrak{p}^l\}$$

becomes a module and contains p^l. Hence the smallest positive integer in this set, say q_1, is a power of p. Next we take η_2 such that

$$\eta_2^k \not\equiv a_1\eta_1^k \bmod \mathfrak{p}^l \quad \text{for} \quad a_1 = 0, 1, \ldots, q_1 - 1.$$

If there exists no such η_2, then $g = q_1$. Next we consider the set

$$\{x;\ x\eta_2^k \equiv a_1\eta_1^k \bmod \mathfrak{p}^l \text{ for some } a_1\}.$$

This is also a module and contains p^l. Hence the smallest positive integer x in this set, say q_2, is a power of p. Then the numbers

$$a_1\eta_1^k + a_2\eta_2^k \qquad \begin{cases} a_1 = 0, 1, \ldots, q_1 - 1, \\ a_2 = 0, 1, \ldots, q_2 - 1 \end{cases}$$

are relatively incongruent $\bmod \mathfrak{p}^l$. Next we take η_3 such that

$$\eta_3^k \not\equiv a_1\eta_1^k + a_2\eta_2^k \bmod \mathfrak{p}^l \quad \text{for} \quad \begin{cases} a_1 = 0, 1, \ldots, q_1 - 1, \\ a_2 = 0, 1, \ldots, q_2 - 1. \end{cases}$$

If there exists no such η_3, then $g = q_1 q_2$.

In this way we can infer that

$$g = q_1 q_2 \cdots q_s,$$

and any number in J_k can be uniquely expressed as

$$a_1\eta_1^k + \ldots + a_s\eta_s^k \bmod \mathfrak{p}^l,$$

where a_j runs over $0, 1, \ldots, q_j - 1$ $(1 \leqslant j \leqslant s)$. Since $p^s \leqslant q_1 q_2 \ldots q_s = g \leqslant N(\mathfrak{p})^l = p^{fl}$, we obtain

$$s \leqslant fl.$$

LEMMA 5. *Under the same assumption as in Lemma 4, we have*

$$s \leqslant ef,$$

for whatever l, e being determined by $\mathfrak{p}^e \| p$.

Proof. For simplicity, we denote by

$$\omega_1, \ldots, \omega_r \quad (r = ef)$$

the basis $\pi^i \varrho^j \bmod \mathfrak{p}^{le}$ in Lemma 3. As to η_j in Lemma 4, we can determine a_{ij} such that

$$\begin{aligned} \eta_1^k &\equiv a_{11}\omega_1 + \ldots + a_{r1}\omega_r \\ &\cdots\cdots\cdots\cdots \\ \eta_s^k &\equiv a_{1s}\omega_1 + \ldots + a_{rs}\omega_r. \end{aligned} \quad \bmod \mathfrak{p}^{le}$$

If $s > r$, then we can take $x_1, \ldots, x_k$ such that

$$\begin{aligned} a_{11}x_1 + \ldots + a_{1s}x_s &\equiv 0 \\ &\cdots\cdots\cdots\cdots \\ a_{r1}x_1 + \ldots + a_{rs}x_s &\equiv 0 \end{aligned} \quad \bmod p^l,$$

where at least one x_j cannot be divided by p. This leads to the contradiction

$$x_1\eta_1^k + \ldots + x_s\eta_s^k \equiv 0 \bmod \mathfrak{p}^{le},$$

whence follows

$$s \leqslant r = ef.$$

Denote by $M(\nu, \mathfrak{a})$ the number of solutions of the congruence

$$\lambda_1^k + \ldots + \lambda_s^k \equiv \nu \bmod \mathfrak{a}.$$

LEMMA 6. *Assume that $N(\mathfrak{p}) = p^f$, $\mathfrak{p}^e \| p$, $\mathfrak{p}^\theta \| k$, $\gamma = \theta + 1$ $(p > 2)$, $\theta + 2$ $(p = 2)$. Write $l_0 = \gamma e$, $s_0 = 4kef$. If $l \geqslant l_0$, $s \geqslant s_0$ and $\nu \in J_k$, then*

$$M(\nu, \mathfrak{p}^l) \geqslant N(\mathfrak{p})^{(l-l_0)(s-1)}.$$

Proof. It is well known that if $m \geqslant 4k$ $(k \geqslant 3)$, then any positive rational integer x can be expressed as

$$x \equiv y_1^k + \ldots + y_m^k \bmod p^\nu$$

satisfying $p \nmid y$. Hence we can infer from Lemma 5 that, for any $\nu \in J_k$, the equation of congruence

$$\nu \equiv \zeta_1^k + \ldots + \zeta_{ms}^k \bmod \mathfrak{p}^{l_0} \ (= \mathfrak{p}^{\nu e})$$

is solvable with $\mathfrak{p} \nmid \zeta_1$ provided $s \geqslant ef$.

Take π such that $\mathfrak{p} \| \pi$ and set

$$\xi_r = \zeta_r + \pi^{l_0}\lambda \qquad (2 \leqslant r \leqslant s),$$

where λ runs over a complete residue system $\bmod \mathfrak{p}^{l-l_0}$. Then

$$\nu - \zeta_2^k - \ldots - \zeta_{ms}^k \quad \text{and also} \quad \nu - \xi_2^k - \ldots - \xi_{ms}^k$$

becomes a reduced kth power residue $\bmod \mathfrak{p}^{l_0}$. With the aid of Lemma 1, this is also a reduced kth power residue $\bmod \mathfrak{p}^l$, and we know that the number of such residues is greater than

$$N(\mathfrak{p})^{(l-l_0)(s-1)},$$

by virtue of the above choice of ξ_r. The result is almost the same as was obtained by R. M. Stemmler (see [10]).

Collecting these results we can prove, as in [12], the following

THEOREM 2. *If $s \geqslant 4kn$ $(\geqslant 4kef)$ and $\nu \in J_k$, then the singular series*

$$\mathfrak{S}(\nu) = \sum_{\mathfrak{a}} H(\mathfrak{a})$$

is absolutely convergent and there exists a constant $c_0 = c_0(k, K)$ satisfying

$$\mathfrak{S}(\nu) > c_0.$$

3. Fourier integrals. Before going into the Siegel formula, we shall develop the Dirichlet integral theory for many variables.

If $\Phi(t_1, \ldots, t_n)$ is non-decreasing for variables $t_{r_1}, \ldots, t_{r_l}$ and non-increasing for other variables $t_{s_1}, \ldots, t_{s_m}$ $(l + m = n)$ over the interval

$$I = \{(t_1, \ldots, t_n);\ a_j \leqslant t_j \leqslant b_j \ (1 \leqslant j \leqslant n)\},$$

then Φ is said to be monotonic over I.

LEMMA 1. *Let $\Phi(t_1, \ldots, t_n)$ be a bounded monotonic function over the interval I. Then $\Phi(t_1, \ldots, t_n)$ is summable; namely it, is measurable and absolutely integrable, over I.*

Proof. For brevity, we shall consider the case where the number of variables n equals 2, and assume that $\Phi(t_1, t_2)$ is non-decreasing for t_1 and t_2 over

$$I = \{(t_1, t_2);\ a_1 \leqslant t_1 \leqslant b_1,\ a_2 \leqslant t_2 \leqslant b_2\}.$$

From points (a, b_1) $(a_1 \leqslant a \leqslant a_2)$ and (a_1, β) $(b_1 \leqslant \beta \leqslant b_2)$, we draw lines parallel to the diagonal of I, joining (a_1, b_1) to (a_2, b_2). Let γ be any given number. On one of these lines we take a point p_α or a point p_β with the smallest coordinates (r, s) such that

$$\Phi(x, y) \geqslant \gamma \quad \text{whenever } x \geqslant r \text{ and } y \geqslant s,$$

except a set of measure zero consisting of points lying upon the lines $x = r$ and $y = s$. We denote by Q_α or R_β the set

$$\{(x, y);\ \Phi(x, y) \geqslant \gamma,\ x \geqslant r,\ y \geqslant s\}$$

and by S the set

$$\{(x, y);\ (x, y) \in I,\ \Phi(x, y) \geqslant \gamma\}.$$

Clearly

$$S = \bigcup Q_\alpha \cup \bigcup R_\beta.$$

Take rational numbers a, b from the intervals $[a_1, a_2]$ and $[b_1, b_2]$ respectively and set

$$S = \bigcup Q_a \cup \bigcup R_b \cup E.$$

For any positive ε, we can make

$$\overline{m}E < \varepsilon$$

by taking sufficiently many a, b. Consequently, we can infer that

$$S = \bigcup Q_a \cup \bigcup R_b \cup E_0, \quad mE_0 = 0,$$

where a and b run over all rational numbers lying in the intervals cited above. Therefore, S becomes a measurable set.

LEMMA 2. *Let $\Phi(t_1, \ldots, t_n)$ be a positive bounded monotonic function over the interval*

$$I = \{(t_1, \ldots, t_n);\ 0 \leqslant t_j \leqslant a_j\ (1 \leqslant j \leqslant n)\}.$$

If we write

$$\chi_\lambda(t) = \frac{\sin 2\pi\lambda t}{\pi t},$$

then

$$\lim_{\lambda_j (1 \leqslant j \leqslant n) \to \infty} \int_0^{a_1} \ldots \int_0^{a_n} \Phi(t_1, \ldots, t_n)\, \chi_{\lambda_1}(t_1) \ldots \chi_{\lambda_n}(t_n)\, dt_1 \ldots dt_n = \left(\frac{1}{2}\right)^n \Phi(+0, \ldots, +0).$$

Proof. For brevity, we shall consider the case where $n = 2$, and assume that $\Phi(t_1, t_2)$ is non-decreasing for t_1 and non-increasing for t_2 over I. To prove the theorem, we may assume that $\Phi(+0, +0) = 0$, whereas

$$\lim_{\lambda \to \infty} \int_0^\infty \chi_\lambda(t)\, dt = \frac{1}{\pi} \int_0^\infty \frac{\sin x}{x}\, dx = \frac{1}{2}.$$

We divide the integral as follows:

$$\int_0^{a_1}\int_0^{a_2} = \int_0^{c_1}\int_0^{c_2} + \int_{c_1}^{a_1}\int_0^{a_2} + \int_0^{a_1}\int_{c_2}^{a_2} - \int_{c_1}^{a_1}\int_{c_2}^{a_2},$$

where c_1 and c_2 are taken so as to satisfy

$$0 \leqslant |\Phi(c_1, c_2)| < \varepsilon, \quad 0 < c_1 < a_1, \quad 0 < c_2 < a_2.$$

With the aid of the second mean value theorem, we obtain

$$\int_0^{c_1}\int_0^{c_2} \Phi(t_1, t_2)\, \chi_{\lambda_1}(t_1)\, \chi_{\lambda_2}(t_2)\, dt_1 dt_2 = \int_0^{c_1} \Phi(t_1, +0)\, \chi_{\lambda_1}(t_1)\, dt_1 \int_0^{\eta} \chi_{\lambda_2}(t_2)\, dt_2$$

$$= \Phi(c_1 - 0, +0) \int_\xi^{c_1} \chi_{\lambda_1}(t_1)\, dt_1 \int_0^{\eta} \chi_{\lambda_2}(t_2)\, dt_2,$$

where $0 \leqslant \xi \leqslant c_1$, $0 \leqslant \eta \leqslant c_2$. Accordingly,

$$\int_0^{c_1}\int_0^{c_2} = O(\varepsilon),$$

and the other integrals

$$\int_{c_1}^{a_1}\int_0^{a_2}, \quad \int_0^{a_1}\int_{c_2}^{a_2}, \quad \int_{c_1}^{a_1}\int_{c_2}^{a_2}$$

can be made arbitrarily small in absolute values by taking λ_1 and λ_2 sufficiently large.

LEMMA 3. *The assertion of Lemma 2 is also valid for a finite product of positive bounded monotonic functions.*

Proof. For brevity, we shall consider the case where $n = 2$ and assume that

$$\Phi(t_1, t_2) = \Phi_1(t_1, t_2)\, \Phi_2(t_1, t_2),$$

where $\Phi_1(t_1, t_2)$ is non-decreasing for t_1 and non-increasing for t_2 and $\Phi_2(t_1, t_2)$ is contrariwise. We assume further that

$$0 \leqslant \Phi_1(t_1, t_2),\ \Phi_2(t_1, t_2) \leqslant A$$

in I. We take c_1 and c_2 such that

$$0 \leqslant \Phi_1(c_1, c_2),\ \Phi_2(c_1, c_2) < \varepsilon, \quad 0 < c_1 < a_1,\ 0 < c_2 < a_2.$$

With the aid of the second mean value theorem, we obtain

$$\begin{aligned}
&\int_0^{c_1}\int_0^{c_2} \Phi(t_1,t_2)\chi_{\lambda_1}(t_1)\chi_{\lambda_2}(t_2)\,dt_1dt_2\\
&\quad=\int_0^{c_1}\int_0^{c_2} A\Phi_2(t_1,t_2)\chi_{\lambda_1}(t_1)\chi_{\lambda_2}(t_2)\,dt_1dt_2-\\
&\qquad-\int_0^{c_1}\int_0^{c_2}\{A-\Phi_1(t_1,t_2)\}\Phi_2(t_1,t_2)\chi_{\lambda_1}(t_1)\chi_{\lambda_2}(t_2)\,dt_1dt_2\\
&\quad=\int_0^{c_1} A\Phi_2(t_1,c_2-0)\chi_{\lambda_1}(t_1)\,dt_1\int_{\eta_1}^{c_2}\chi_{\lambda_2}(t_2)\,dt_2-\\
&\qquad-\int_0^{c_1}\{A-\Phi_1(t_1,c_2-0)\}\Phi_2(t_1,c_2-0)\chi_{\lambda_1}(t_1)\,dt_1\int_{\eta_2}^{c_2}\chi_{\lambda_2}(t_2)\,dt_2\\
&\quad=A\Phi_2(+0,c_2-0)\int_0^{\xi_1}\chi_{\lambda_1}(t_1)\,dt_1\int_{\eta_1}^{c_2}\chi_{\lambda_2}(t_2)\,dt_2-\\
&\qquad-\{A-\Phi_1(+0,c_2-0)\}\Phi_2(+0,c_2-0)\int_0^{\xi_2}\chi_{\lambda_1}(t_1)\,dt_1\int_{\eta_2}^{c_2}\chi_{\lambda_2}(t_2)\,dt_2\\
&\quad=O(\varepsilon),
\end{aligned}$$

where $0\leqslant\xi_1,\xi_2\leqslant c_1$, $0\leqslant\eta_1,\eta_2\leqslant c_2$. We omit the remaing part of the proof.

We now deduce the Siegel formula. If we put

$$\eta^{(l)}=\tau_l,\qquad \eta^{(m)}=\tau_m e^{i\varphi_m},$$

then

$$\int_P\dots\int E(\xi\eta^k)\,dy=|d|^{-1/2}\prod_{l=1}^{r_1}\int_0^1\exp\{2\pi i(\xi^{(l)}\tau_l^k)\}\,d\tau_l\times$$

$$\times\prod_{m=r_1+r}^{r_1+r_2}2\int_0^1\int_{-\pi}^{\pi}\exp\left\{2\pi i\{\xi^{(m)}(\tau_m e^{i\varphi_m})^k+(\xi^{(m)})^{-1}(\tau_m e^{-i\varphi_m})^k\}\right\}\tau_m\,d\tau_m\,d\varphi_m,$$

whence follows

$$\int_P\dots\int E(\xi\eta^k)\,dy=O\Big\{\prod_{l=1}^{r_1}\mathrm{Min}(1,|\xi^{(l)}|^{-1/k})\prod_{m=r_1+1}^{r_1+r_2}\mathrm{Min}(1,|\xi^{(m)}|^{-2/k})\Big\},$$

where $\xi=\varrho_1x_1+\dots+\varrho_nx_n$ and $\eta=\omega_1y_1+\dots+\omega_ny_n$. Further, if we put

$$\xi^{(l)}=\varkappa_l,\qquad \xi^{(m)}=\varkappa_m e^{i\theta_m},$$

then

$$\begin{aligned}
&\int_X\dots\int\Big|\int_P\dots\int E(\xi\eta^k)\,dy\Big|^s\,dx\\
&\quad=O\Big\{\prod_{l=1}^{r_1}\int_0^{\infty}\mathrm{Min}(1,\varkappa_l^{-s/k})\,d\varkappa_l\prod_{m=r_1+1}^{r_1+r_2}\int_{-\pi}^{\pi}\Big(\int_0^{\infty}\mathrm{Min}(1,\varkappa_m^{-2s/k})\varkappa_m\,d\varkappa_m\Big)\,d\theta_m,
\end{aligned}$$

which clearly converges for $s>k$. Hence the integral

$$J(\mu)=\int_X\dots\int E(-\mu\xi)\Big\{\int_P\dots\int E(\xi\eta^k)\,dy\Big\}^s\,dx$$

converges absolutely for $s>k$, and can be expressed as

$$J(\mu)=\lim_{\lambda_l,\lambda_m,\lambda'_m\to\infty}J(\Omega),\qquad J(\Omega)=\int_\Omega\dots\int E(-\mu\xi)\Big\{\int_P\dots\int E(\xi\eta^k)\,dy\Big\}^s\,dx,$$

Ω being the closed region of x determined by

$$|v_l|\leqslant\lambda_l,\qquad |v_m|\leqslant\lambda_m,\qquad |v'_m|\leqslant\lambda'_m$$

where

$$v_l=\xi^{(l)},\qquad v_m=\frac{\xi^{(m)}+\xi^{(m+r_2)}}{\sqrt{2}},\qquad v'_m=\frac{\xi^{(m)}-\xi^{(m+r_2)}}{\sqrt{2}\,i}.$$

Further, if we put

$$z_p=\eta_1^{(p)k}+\dots+\eta_s^{(p)k}-\mu^{(p)}\qquad(1\leqslant p\leqslant n),$$

$$u_l=z_l,\qquad u_m=\frac{z_m+z_{m+r_2}}{\sqrt{2}},\qquad u'_m=\frac{z_m-z_{m+r_2}}{\sqrt{2}\,i},$$

then

$$\begin{aligned}
\sum_{p=1}^{n}\xi^{(p)}(\eta_1^{(p)k}+\dots+\eta_s^{(p)k}-\mu^{(p)})&=\sum_{p=1}^{n}\xi^{(p)}z_p\\
&=\sum_{l=1}^{r_1}u_lv_l+\sum_{m=r_1+1}^{r_1+r_2}u_mv_m+\sum_{m=r_1+1}^{r_1+r_2}u'_mv'_m,
\end{aligned}$$

and

$$\begin{aligned}
J(\Omega)&=\int_{P_1}\dots\int_{P_s}dy_1\dots dy_s\int_\Omega\dots\int\exp\Big\{2\pi i\sum_{p=1}^{n}\xi^{(p)}(\eta_1^{(p)k}+\dots+\eta_s^{(p)k}-\mu^{(p)})\Big\}\,dx\\
&=\sqrt{|d|}\int_{P_1}\dots\int_{P_s}\Big\{\prod_{l=1}^{r_1}\chi_{\lambda_l}(u_l)\prod_{m=r_1+1}^{r_1+r_2}\chi_{\lambda_m}(u_m)\prod_{m=r_1+1}^{r_1+r_2}\chi_{\lambda'_m}(u'_m)\Big\}\,dy_1\dots dy_s.
\end{aligned}$$

In place of

$$\eta_s^{(p)k} = z_p + \mu^{(p)} - (\eta_1^{(p)k} + \ldots + \eta_{s-1}^{(p)k}) \qquad (1 \leqslant p \leqslant n),$$

we write more precisely

$$(y_{s1}\omega_1^{(p)} + \ldots + y_{sn}\omega_n^{(p)})^k = (t_1\omega_1^{(p)} + \ldots + t_n\omega_n^{(p)}) + \mu^{(p)} - (\eta_1^{(p)k} + \ldots + \eta_s^{(p)k})$$

and briefly

$$J(\Omega) = \int_{P_1} \ldots \int_{P_s} * dy_1 \ldots dy_s.$$

Make a change of variables in the following way:

$$J(\Omega) = \int \ldots \int dy_1 \ldots dy_{s-1} \int * dy_s = \int \ldots \int dy_1 \ldots dy_{s-1} \int * |J_1| dt$$
$$= \int * dt \int |J_1| dy_1 \ldots dy_{s-1} = \int * |J_2| du \int |J_1| dy_1 \ldots dy_{s-1},$$

where the Jacobians are afforded by

$$J_1 = \frac{\partial(y_{s1} \ldots y_{sn})}{\partial(t_1 \ldots t_n)} = \begin{vmatrix} k\eta_s^{(1)k-1}\omega_1^{(1)} & \ldots & k\eta_s^{(1)k-1}\omega_n^{(1)} \\ \ldots\ldots\ldots\ldots\ldots\ldots \\ k\eta_s^{(n)k-1}\omega_1^{(n)} & \ldots & k\eta_s^{(n)k-1}\omega_n^{(n)} \end{vmatrix}^{-1} \cdot \begin{vmatrix} \omega_1^{(1)} & \ldots & \omega_n^{(1)} \\ \ldots\ldots\ldots \\ \omega_1^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}$$

and

$$J_2 = \frac{\partial(t_1 \ldots t_n)}{\partial(u_1 \ldots u_{r_1} u_{r_1+1} u'_{r_1+1} \ldots u_{r_1+r_2} u'_{r_1+r_2})} = \begin{vmatrix} \omega_1^{(1)} & \ldots & \omega_n^{(1)} \\ \ldots\ldots\ldots \\ \omega_1^{(n)} & \ldots & \omega_n^{(n)} \end{vmatrix}^{-1} (-i)^{-r_2},$$

so that

$$|J_1| = N(k^{-1}|\eta_s|^{1-k}), \qquad |J_2| = \frac{1}{\sqrt{|d|}}.$$

Therefore

$$J(\Omega) = \int_Q \Big\{\prod_{l=1}^{r_1} \chi_{\lambda_l}(u_l) \prod_{m=r_1+1}^{r_1+r_2} \chi_{\lambda_m}(u_m) \prod_{m=r_1+1}^{r_1+r_2} \chi_{\lambda'_m}(u'_m)\Big\} du \times$$
$$\times \int_{P_1} \ldots \int_{P_{s-1}} N(k^{-1}|\eta_s|^{1-k}) dy_1 \ldots dy_{s-1},$$

where Q is the closed region containing the origin of u in its interior and

$$du = \prod_{l=1}^{t_1} du_l \prod_{m=r_1+1}^{r_1+r_2} du_m \prod_{m=r_1+1}^{r_1+r_2} du'_m.$$

If we make a change of variables such that

$$\eta_p^{(l)} = y_{p1}\omega_1^{(l)} + \ldots + y_{pn}\omega_n^{(l)} = u_{pl}^{\frac{1}{k}} \qquad (1 \leqslant p \leqslant s-1),$$
$$\eta_p^{(m)} = y_{p1}\omega_1^{(m)} + \ldots + y_{pn}\omega_n^{(m)} = u_{pm}^{\frac{1}{2k}} e^{i\frac{\varphi_{pm}}{k}}$$

then

$$\left| \frac{\partial(y_{p1} \ldots y_{pn})}{\partial(u_{p1} \ldots u_{pr_1} u_{p,r_1+1} \ldots u_{p,r_1+r_2} \varphi_{p,r_1+1} \ldots \varphi_{p,r_1+r_2})} \right| = |d|^{-1/2} N(k^{-1}|\eta_p|^{1-k}).$$

Consequently,

$$J(\Omega) = \int_Q \Big\{\prod_{l=1}^{r_1} \chi_{\lambda_l}(u_l) \prod_{m=r_1+1}^{r_1+r_2} \chi_{\lambda_m}(u_m) \prod_{m=r_1+1}^{r_1+r_2} \chi_{\lambda'_m}(u'_m)\Big\} du \times$$
$$\times |d|^{\frac{1}{2}(1-s)} \int_{0 \leqslant u_{pj} \leqslant 1,\ -\pi \leqslant \varphi_{pk} \leqslant \pi} \ldots \int \prod_{p=1}^{s} N(k^{-1}|\eta_p|^{1-k}) \times$$
$$\times \prod_{p=1}^{s} (du_{p_1} \ldots du_{p,r_1+r_2} d\varphi_{p,r_1+1} \ldots d\varphi_{p,r_1+r_2}).$$

Therefore, by Fubini's theorem,

$$J(\mu) = \lim J(\Omega) = |d|^{\frac{1}{2}(1-s)} \prod_{l=1}^{r_1} F(\mu^{(l)}) \prod_{m=r_1+1}^{r_1+r_2} H(\mu^{(m)})$$

where

$$F(\mu^{(l)}) = \lim_{\lambda_l \to \infty} \frac{1}{k^s} \int_{Q_l} \chi_{\lambda_l}(u_l) du_l \int_{C_l} \ldots \int \frac{u_{1l}^{\frac{1}{k}-1} \ldots u_{s-1,l}^{\frac{1}{k}-1} du_{1l} \ldots du_{s-1,l}}{|\mu^{(l)} + u_l - (u_{1l} + \ldots + u_{s-1,l})|^{1-\frac{1}{k}}},$$

C_l being the closed region determined by $0 \leqslant u_{jl} \leqslant 1$, $0 \leqslant \mu^{(l)} + u^{(l)} - (u_{1l} + \ldots + u_{s-1,l}) \leqslant 1$, and

$$H(\mu^{(m)}) = \lim_{\lambda_m, \lambda'_m \to \infty} \frac{1}{k^{2s}} \int_{Q_m} \chi_{\lambda_m}(u_m) \chi_{\lambda'_m}(u'_m) du_m du'_m \times$$
$$\times \int_{C_m} \ldots \int \frac{u_{1m}^{\frac{1}{k}-1} \ldots u_{s-1}^{\frac{1}{k}-1} du_{1m} \ldots du_{s-1,m} d\varphi_{1m} \ldots d\varphi_{s-1,m}}{\left| u^{(m)} + \frac{u_m - iu'_m}{\sqrt{2}} - (u_{1m}^{\frac{1}{k}} e^{i\varphi_{1m}} + \ldots + u_{s-1,m}^{\frac{1}{k}} e^{i\varphi_{s-1,m}}) \right|^{1-\frac{1}{k}}},$$

C_m being the closed region determined by

$$0 \leqslant u_{jm} \leqslant 1, \quad -\pi \leqslant \varphi_{jm} \leqslant \pi, \quad |\mu^{(m)} + z_m - (u_{1m}^{\frac{1}{k}} e^{i\varphi_{1m}} + \ldots + u_{s-1,m}^{\frac{1}{k}} e^{i\varphi_{s-1,m}})| \leqslant 1.$$

By applying Lemma 3, we have the following

THEOREM 3. *If $s > k$, then*

$$J(\mu) = |d|^{(1-s)/2} \prod_{l=1}^{r_1} F(\mu^{(l)}) \prod_{m=r_1+1}^{r_1+r_2} H(\mu^{(m)}),$$

where

$$F(\mu^{(l)}) = \int\dots\int_{D_l} \prod_{j=1}^{s} (k^{-1}u_j^{\frac{1}{k}-1})\, du_1 \dots du_{s-1}, \qquad u_s = \mu^{(l)} - (u_1 + \dots + u_{s-1}),$$

D_l being the closed region determined by

$$0 \leqslant u_j \leqslant 1 \qquad (1 \leqslant j \leqslant s),$$

and

$$H(\mu^{(m)}) = k^{-s} \int\dots\int_{D_m} \prod_{j=1}^{s} (k^{-1}u_j^{\frac{1}{k}-1})\, du_1 \dots du_{s-1} d\varphi_1 \dots d\varphi_{s-1},$$

$$u_s = |\mu^{(m)} - (u_1^{1/2} e^{i\varphi_1} + \dots + u_{s-1}^{1/2} e^{i\varphi_{s-1}})|^2,$$

D_m being the closed region determined by

$$0 \leqslant u_j \leqslant 1 \ (1 \leqslant j \leqslant s), \qquad -\pi \leqslant \varphi_j \leqslant \pi \ (1 \leqslant j \leqslant s-1).$$

Finally we note that

$$F(\mu^{(l)}) = \frac{\Gamma\left(1+\frac{1}{k}\right)^s}{\Gamma\left(\frac{s}{k}\right)} (\mu^{(l)})^{\frac{s}{k}-1}.$$

4. Supplementary domain and consequences. By virtue of the following Lemma 1 of Mitsui, we can improve the Siegel result based on the Weyl method over the supplementary domain.

LEMMA 1. *Let $(x_1, \dots, x_n)$ be a point of the supplementary domain $S = U - \sum_{\gamma \in \Gamma} B_\gamma$. Let A, B be positive and $1 \leqslant B < 2^{-4-r_2}|d|^{-1/n}h$. If $\xi = \varrho_1 x_1 + \dots + \varrho_n x_n$, then*

$$\sum_{|\mu| \in P(B)} \mathrm{Min}\{A, |1 - E(\xi\mu\omega_j)|^{-1} \ (1 \leqslant j \leqslant n)\} = O\left\{AB^n\left(\frac{1}{t} + \frac{1}{B} + \frac{h\log h}{AB} + \frac{\log h}{A}\right)\right\}.$$

Proof. See [7].

LEMMA 2. *Let $\xi = \varrho_1 x_1 + \dots + \varrho_n x_n$, $L(\xi) = \sum_{\lambda \in P(T)} E(\lambda^k \xi)$ and let θ be any positive integer satisfying $2^{k-1}\theta < 1 - a$. If $(x_1, \dots, x_n) \in S$, then*

$$L(\xi) = O\left(c(\theta) T^{n-\theta}\right).$$

Proof. Let $1 \leqslant q \leqslant k-1$. By Hölder's inequality,

$$\begin{aligned}
|L(\xi)|^{2^q} &= \Big|\sum_{\lambda,\, \lambda+\lambda_1 \in P(T)} E\left\{\left((\lambda+\lambda_1)^k - \lambda^k\right)\xi\right\}\Big|^{2^{q-1}} \\
&\leqslant \Big[\sum_{|\lambda_1| \in P(2T)} \Big|\sum_{\lambda \in P(T)} E\left(\lambda_1(k\lambda^{k-1} + \dots)\,\xi\right)\Big|\Big]^{2^{q-1}} \\
&\leqslant (cT^n)^{2^{q-1}-1} \sum_{|\lambda_1| \in P(2T)} \Big|\sum_{\lambda \in P(T)} E\left\{\lambda_1(k\lambda^{k-1} + \dots)\,\xi\right\}\Big|^{2^{q-1}} \\
&\leqslant (cT^n)^{2^{q-1}-1} \sum_{|\lambda_1| \in P(2T)} (cT^n)^{2^{q-2}-1} \sum_{|\lambda_2| \in P(2T)} \Big|\sum_{\lambda \in P(T)} E\left\{\lambda_1\lambda_2\left(k(k-1)\lambda^{k-2} + \dots\right)\xi\right\}\Big|^{2^{q-1}} \\
&\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
&\leqslant (cT^n)^{2^q-q-1} \sum_{|\lambda_1|, \dots, |\lambda_{q-1}| \in P(2T)} \dots \sum_{\lambda} \sum_{\lambda+\lambda_q \in P(T)} E\{\lambda_1 \dots \lambda_q f(\lambda, \lambda_1, \dots, \lambda_q)\,\xi\},
\end{aligned}$$

where

$$f(\lambda, \lambda_1, \dots, \lambda_q) = k(k-1)\dots(k-q+1)\lambda^{k-q} + \dots$$

is a polynomial of $\lambda, \lambda_1, \dots, \lambda_q$ with integral coefficients. Therefore,

$$|L(\xi)|^{2^{k-1}} = O\left\{T^{n(2^{k-1}-k)} \sum_{|\lambda_1|, \dots, |\lambda_{k-1}| \in P(2T)} \dots \sum \Big|\sum_{\lambda \in P(T)} E(\mu\lambda\eta)\Big|\right\}$$

where $\mu = k!\lambda_1 \dots \lambda_{k-1}$. Denote by $A(\mu)$ the number of solutions of this equality, subject to the conditions

$$|\lambda_j| \in P(2T) \qquad (1 \leqslant j \leqslant k-1).$$

Then obviously

$$A(\mu) = \begin{cases} O(T^{n(k-2)}) & (\mu = 0), \\ O\left(c(\varepsilon)T^{\varepsilon}\right) & (\mu \neq 0). \end{cases}$$

Hence

$$|L(\xi)|^{2^{k-1}} = O(T^{n(2^{k-1}-2)}) + O\left(c(\varepsilon)\, T^{n(2^{k-1}-k+\varepsilon)} \sum_{\mu} \Big|\sum_{\lambda} E(\mu\lambda\eta)\Big|\right),$$

where the summation is extended over all μ, λ satisfying $|\mu| \in P(k!2^{k-1}T^{k-1})$, $\lambda \in P(T)$.

As Siegel showed, we have

$$\Big\{\sum_{\lambda \in P(T)} E(\mu\lambda\eta)\Big\}\left(1 - E(\mu\omega\eta)\right) = O(T^{n-1}).$$

Therefore,

$$\begin{aligned}
|L(\xi)|^{2^{k-1}} &= O(T^{n(2^{k-1}-2)}) + \\
&+ O\left[c(\varepsilon)\, T^{n(2^{k-1}-k+\varepsilon)} \sum_{\mu} O\left\{T^{n-1}\mathrm{Min}\left(T, |1 - E(\mu\omega_j\xi)|^{-1} \ (1 \leqslant j \leqslant n)\right)\right\}\right],
\end{aligned}$$

where the sum is over all μ satisfying $|\mu| \in P(k!2^{k-1}T^{k-1})$.

By taking $A = T$ and $B = k!2^{k-1}T^{k-1}$, we obtain from Lemma 1

$$\sum_{\mu} O\{T^{n-1}\mathrm{Min}(T, |1-E(\mu\omega_j\xi)|^{-1}\ (1\leqslant j\leqslant n))\}$$
$$= O\left\{T^{n-1}T(k!2^{k-1}T^{k-1})^n\left(\frac{1}{t}+\frac{1}{T^{k-1}}+\frac{h\log h}{T^k}+\frac{\log h}{T^{k-1}}\right)\right\}$$
$$= O(T^{nk-1+a}\log T),$$

since $t = T^{1-a}$ and $h = T^{k-1+a}$. If we put $1-a-2^{k-1}\theta = 2\varepsilon$, then we have

$$L(\xi) = O\big(c(\theta)T^{n-\theta}\big)$$

over the supplementary domain.

Lemma 3. *If $s > 2^k$, then*

$$\int_S\dots\int |L(\xi)|^s\,dx = O\big(c(\theta)T^{n(s-k)-\theta}\big).$$

Proof. Extending Hua's method (see [4]), and using the previous arguments, we get

$$|L(\xi)|^{2q} = O(T^{n(2q-1)}) +$$
$$+ O\Big[T^{n(2q-q-1)}\sum_{|\lambda_1|,\dots,|\lambda_{q-1}|\in P(2T)}\dots\sum\ \sum_{\lambda,\,\lambda+\lambda_q\in P(T)}{}^{*}\ E\{\lambda_1\dots\lambda_q f(\lambda,\lambda_1,\dots,\lambda_q)\xi\}\Big],$$

where the asterisk means that

$$\lambda_1\dots\lambda_q f(\lambda,\lambda_1,\dots,\lambda_q)\neq 0.$$

Multiplying both sides by $|L(\xi)|^{2q}$ and integrating with respect to x over the unit cube, we obtain

$$\int_U\dots\int |L(\xi)|^{2q+1}\,dx = O(T^{n(2q-1)})\int_U\dots\int |L(\xi)|^{2q}\,dx +$$
$$+ O\Big[T^{n(2q-q-1)}\int_U\dots\int\sum_{|\lambda_1|,\dots,|\lambda_{q-1}|\in P(2T)}\dots\sum\ \sum_{\lambda,\,\lambda+\lambda_q\in P(T)}{}^{*}$$
$$\sum_{\substack{\mu_j,\nu_j\in P(T)\\(1\leqslant j\leqslant 2q)}}\dots\sum E\{\lambda_1\dots\lambda_q f(\lambda,\lambda_1,\dots,\lambda_q)+\mu_1^k+\dots+\mu_{2q-1}^k-\nu_1^k-\dots-\nu_{2q-1}^k\}\,dy\Big].$$

The contribution from the second integral on the right does not exceed the number of solutions of the equation

$$\lambda_1\dots\lambda_q f(\lambda,\lambda_1,\dots,\lambda_q) = \nu_1^k+\dots+\nu_{2q-1}^k-\mu_1^k-\dots-\mu_{2q-1}^k$$

under the conditions cited above. Therefore,

$$\int_U\dots\int |L(\xi)|^{2q+1}\,dx = O(T^{n(2q-1)})\int_U\dots\int |L(\xi)|^{2q}\,dx + O(T^{n(2q-q-1)}c(\varepsilon)T^{n2q+\varepsilon}),$$

whence follows, by induction,

$$\int_U\dots\int |L(\xi)|^{2q}\,dx = O\big(c(q,\varepsilon)T^{n(2q-q)+\varepsilon}\big).$$

Put

$$\theta_1 = \frac{\theta}{2}+\frac{1-a}{2^k}.$$

Then $2^{k-1}\theta < 2^{k-1}\theta_1 < 1-a$. By Lemma 1, we have

$$\int_S\dots\int |L(\xi)|^s\,dx = O\big(c(\theta_1)T^{(n-\theta_1)(s-2^k)}\big)\int_S\dots\int |L(\xi)|^{2^k}\,dx$$
$$= O\big(c(\theta_1)T^{(n-\theta_1)(s-2^k)}\big)O\big(c(k,\theta_1-\theta)T^{n(2^k-k)+\theta_1-\theta}\big)$$
$$= O\big(c(k,\theta)T^{n(s-k)-\theta}\big),$$

provided $s > 2^k$.

Theorem 4. *If $s > \mathrm{Max}(4nk, 2^k)$, $0\neq\nu\in J_k$, $\mu = \nu T^{-k}$ and $\mu\in P(1)$, then*

$$I(\nu)\sim\mathfrak{S}(\nu)J(\mu)T^{n(s-k)}.$$

Proof. It follows from Lemma 2 that

$$\int_S\dots\int L(\xi)^s E(-\nu\xi)\,dx = O(T^{n(s-k)-\frac{1}{2^k}})$$

by taking $\theta = 1/2^k$ if $s\geqslant 2^k+1$. Now the result follows from Theorem 1.

Let $G(k)$ denote the least value of r with the property that every sufficiently large positive integer m is representable in the form

$$m = x_1^k+\dots+x_r^k.$$

The best value obtained so far as an upper bound of $G(k)$ can be seen in [15].

Lemma 4. *Let T_1 be a sufficiently large positive number and $s_1 = nG(k)$. Let $W_{s_1}(T_1)$ denote the set of integers in K which can be expressed in the form*

$$\lambda_1^k+\dots+\lambda_{s_1}^k$$

subject to the conditions

$$\lambda_j\in P(T_1)\qquad(1\leqslant j\leqslant s_1)$$

and let $N_{s_1}(T_1)$ denote the number of integers belonging to $W_{s_1}(T_1)$. Then we have, for suitably chosen c_3,

$$N_{s_1}(T_1)\geqslant c_3T_1^{nk}.$$

Proof. Take θ in o such that

$$1,\ \theta,\dots,\theta^{n-1}$$

are linearly independent over the rational number field. Let ζ_k denote the kth roots of unity. If we take a suitable z, a positive rational integer, sufficiently large, then $\theta+z$ becomes totally positive and satisfying

$$\theta^{(p)}+z \neq (\theta^{(q)}+z)\zeta_k \qquad (1 \leqq p, q \leqq n,\ p \neq q)$$

for every ζ_k. It follows that

$$1, (\theta+z)^k, \ldots, (\theta+z)^{k(n-1)}$$

are totally positive and linearly independent over the rational number field, on account of

$$\begin{vmatrix} 1 & (\theta^{(1)}+z)^k & \ldots & (\theta^{(1)}+z)^{k(n-1)} \\ \cdots & \cdots & \cdots & \cdots \\ 1 & (\theta^{(n)}+z)^k & \ldots & (\theta^{(n)}+z)^{k(n-1)} \end{vmatrix} = \prod_{1 \leqq p < q \leqq n} \left((\theta^{(p)}+z)^k - (\theta^{(q)}+z)^k\right) \neq 0.$$

Let x_j $(0 \leqq j \leqq n-1)$ be positive integers satisfying

$$x_j(\theta+z)^{jk} \in P(T_1^k).$$

It follows from the definition of $G(k)$ that almost all numbers of the form

$$x_0+x_1(\theta+z)^k+\ldots+x_{n-1}(\theta+z)^{k(n-1)}$$

belong to $W_{s_1}(T_1)$, which gives the desired result.

If we take a totally positive unit ε appropriately, and put $\varkappa = \nu\varepsilon^k$ for a given $\nu \in J_k$, then we can make

$$c_4 M \leqq \varkappa^{(l)} \leqq c_5 M, \qquad c_4 M \leqq |\varkappa^{(m)}| \leqq c_5 M$$

where $M = \sqrt[n]{N(\nu)}$ and c_4, c_5 are constants chosen suitably. Take σ_1, σ_2 in $W_{s_1}(T_1)$ where

$$T_1 = \left(\frac{c_4 M}{4 s_1}\right)^{1/k}$$

and set $\tau = \varkappa - \sigma_1 - \sigma_2$ and $\mu = T^{-k}\tau$ where

$$T = \{(c_5 + \tfrac{1}{2}c_4) M\}^{1/k}.$$

Then there exists a positive c_6 such that

$$c_6 \leqq \mu^{(l)} \leqq 1, \qquad c_6 \leqq |\mu^{(m)}| \leqq 1,$$

so that, by taking c_7 sufficiently small, it follows from the definition that

$$F(\mu^{(l)}) \geqslant k^{-s} c_7^{\frac{1}{k}-1} \int_0^{c_7} \ldots \int_0^{c_7} u_1^{\frac{1}{k}-1} \ldots u_{s-1}^{\frac{1}{k}-1}\, du_1 \ldots du_{s-1},$$

$$H(\mu^{(m)}) \geqslant (2\pi)^{s-1} k^{-2s} c_7^{\frac{1}{k}-1} \int_0^{c_7} \ldots \int_0^{c_7} u_1^{\frac{1}{k}-1} \ldots u_{s-1}^{\frac{1}{k}-1}\, du_1 \ldots du_{s-1},$$

whence follows $J(\mu) > c_8$ provided $s > k$. With these preparations, we obtain

THEOREM 5. *Let ν be a totally positive integer in J_k, and let $N(\nu)$ be sufficiently large. If*

$$s > 4nk + 2nG(k),$$

then the equation

$$\nu = \lambda_1^k + \ldots + \lambda_s^k$$

is always solvable in totally non-negative integers λ_j $(1 \leqq j \leqq s)$, subject to the conditions

$$N(\lambda_j)^k \leqslant c_9 N(\nu) \qquad (1 \leqq j \leqq s)$$

where c_9 is a positive constant depending on K, k and s.

Proof. We write

$$L(\xi) = \sum_{\lambda \in P(T)} E(\lambda^k \xi), \qquad V(\xi) = \sum_{\sigma \in W_{s_1}(T_1)} E(\sigma\xi)$$

where $\xi = \varrho_1 x_1 + \ldots + \varrho_n x_n$. It follows from Theorem 1 that

$$\sum_{\gamma \in \Gamma} \int_{B_\gamma} \ldots \int L(\xi)^s V(\xi)^2 E(-\varkappa\xi)\, d\xi = \sum_{\tau} \sum_{\gamma \in \Gamma} \int_{B_\gamma} \ldots \int L(\xi)^s E(-\tau\xi)\, d\xi$$
$$= \sum_{\tau} \{\mathfrak{S}(\tau) J(\mu) T^{n(s-k)} + O(T^{n(s-k)-\frac{1}{4}})\},$$

provided $s > 4nk$. This yields

$$\mathscr{R} \sum_{\gamma \in \Gamma} \int_{B_\gamma} \ldots \int L(\xi)^s V(\xi)^2 E(-\varkappa\xi)\, d\xi > c_9 T^{n(s-k)} N_{s_1}^2(T_1).$$

On the other hand, by Lemma 2 (take $\theta = \frac{1}{2^k}$),

$$\int_S \ldots \int L(\xi)^s V(\xi)^2 E(-\varkappa\xi)\, d\xi = O(T^{ns-\frac{s}{2^k}}) \int_S \ldots \int |V(\xi)|^2\, d\xi$$
$$= O(T^{ns-\frac{s}{2^k}}) \int_U \ldots \int \sum_{\sigma_1, \sigma_2 \in W_{s_1}(T_1)} E\big((\sigma_1-\sigma_2)\xi\big)\, d\xi$$
$$= O(T^{ns-\frac{s}{2^k}}) N_{s_1}(T_1).$$

From these results, we have

$$\int_U \ldots \int L(\xi)^s V(\xi)^2 E(-\varkappa\xi)\, d\xi > 0.$$

This means that $\varkappa$ is expressible as

$$\nu\varepsilon^k = \varkappa = \lambda_1^k + \ldots + \lambda_s^k + \tau_1^k + \ldots + \tau_{2s_1}^k$$

subject to the conditions

$$\lambda_j \in P(T), \qquad \tau_j \in P(T_1),$$

whence follows the desired result.

References

[1] Y. Eda, *On the Waring problem in an algebraic number field*, in *Seminar on Modern Methods in Number Theory*, Tokyo 1971.

[2] H. Hasse, *Vörlesungen über Klassenkörpertheorie*, Würzburg 1967.

[3] L. K. Hua, *Exponential sums over algebraic fields*, Canadian J. Math. 3 (1951), pp. 44–51.

[4] — *On Waring's problem*, Quart. Journ. of Math. 9 (1938), pp. 199–201.

[5] O. Körner, *Über das Waringsche Problem in algebraischen Zahlkörpern*, Math. Ann. 144 (1961), pp. 224–238.

[6] E. Landau, *Über die neue Winogradoffsche Behandlung des Waringschen Problems*, Math. Zeitschr. 31 (1930), pp. 319–338.

[7] T. Mitsui, *On the Goldbach problem in algebraic number field I*, Journ. Math. Soc. Japan 12 (1960), pp. 325–372.

[8] C. L. Siegel, *Generalization of Waring's problem to algebraic number fields*, Amer. Journ. Math. 66 (1944), pp. 122–136.

[9] — *Sums of m-th powers of algebraic integers*, Ann. of Math. 46 (1945), pp. 313–339.

[10] R. M. Stemmler, *The easier Waring problem in algebraic number fields*, Acta Arith. 6 (1961), pp. 447–468.

[11] T. Takagi, *Algebraic number theory* (in Japanese), Tokyo 1948.

[12] T. Tatuzawa, *On the Waring problem in an algebraic number field*, Journ. Math. Soc. Japan 10 (1958), pp. 322–341.

[13] — *On the Waring problem in an algebraic number field*, in *Seminar on Modern Methods in Number Theory*, Tokyo 1971.

[14] И. М. Виноградов, *Избранные труды*, Москва 1952.

[15] — *К вопросу о верхней границе для G(n)*, Изв. Акад. Наук 23 (1959), pp. 637–642.

INSTITUTE OF MATHEMATICS, COLLEGE OF GENERAL EDUCATION
UNIVERSITY OF TOKYO

Received on 24. 5. 1972 (290)

ACTA ARITHMETICA
XXIV (1973)

Zur Theorie der symplektischen Gruppen

von

Ulrich Christian (Göttingen)

Carl Ludwig Siegel zum 75. Geburtstag und zum 50-jährigen Professorenjubiläum gewidmet

Will man den Rang der Schar der Modulformen mit Hilfe der Selbergschen Spurformel berechnen, so stößt man auf ein Problem, welches man grob so beschreiben kann: Es sei M eine Modulmatrix n-ten Grades. Wann gibt es eine Modulmatrix n-ten Grades R, so daß die Matrix $R^{-1}MR$ eine Randkomponente der verallgemeinerten oberen Halbebene im Unendlichen festläßt?

Zur Lösung dieses Problems führen wir zunächst einige Bezeichungen ein.

1. Man bilde die $(2n)\times(2n)$ Matrix

$$I(n) = \begin{pmatrix} 0 & E \\ -E & 0 \end{pmatrix} \tag{1}$$

mit $n\times n$ Null- bzw. Einheitsmatrix 0 und E. Für einen Körper K bezeichnen wir mit $\Sigma(n, K)$ die symplektische Gruppe, bestehend aus allen $(2n)\times(2n)$ Matrizen M mit Elementen in K, die der Bedingung

$$M' I(n) M = I(n) \tag{2}$$

genügen. Hierbei bedeutet M' die Transponierte von M. Zwei Matrizen M, $M^* \in \Sigma(n, K)$ heißen konjugiert über K, wenn es ein $R \in \Sigma(n, K)$ mit

$$R^{-1}MR = M^* \tag{3}$$

gibt. Es seien $M, R \in \Sigma(n, K)$. Wir sagen, daß $R^{-1}MR$ aus M hervorgeht, indem man M mit R „konjugiert". In der üblichen Weise bezeichne man mit $\boldsymbol{Q}$, $\boldsymbol{C}$ die Körper der rationalen, bzw. komplexen Zahlen. Für diese gesamte Arbeit gelte

$$\boldsymbol{Q} \subset K \subset \boldsymbol{C}. \tag{4}$$