Journal of the Mathematical Society of Japan Vol. 10, No. 3, July, 1958

On the Waring problem in an algebraic number field.

By Tikao TATUZAWA

(Received April 24, 1958)

Siegel succeeded in dealing with the Waring problem in an algebraic number field, and he extended the Hardy-Littlewood theory to the case of number fields by means of the circle method (see [4] and [5]).

Let K be an algebraic number field of degree n and k be a positive rational integer ($k\geqq 3$). Let $\mathfrak{o}$ be the integral domain consisting of all integers in K (the unit ideal of K) and J_k be the ring generated by k-th powers of all integers in K. On account of the identity

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

for $\gamma\in\mathfrak{o}$, the ring J_k is an order.

Using the Vinogradov method, we shall prove, in the present paper, the following

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

$$s\geqq 8nk(n+k)\,,$$

then the equation

$$\nu=\lambda_1{}^k+\lambda_2{}^k+\cdots+\lambda_s{}^k$$

is always soluble in totally non-negative integers

$$\lambda_r\ \ (1\leqq r\leqq s)\,,$$

subject to the conditions

$$N(\lambda_r)^k\leqq cN(\nu)\,,$$

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

Let $K^{(l)}(1\leqq l\leqq r_1)$ be r_1 real conjugate fields and $K^{(m)}$, $K^{(m+r_2)}(r_1+1\leqq m\leqq r_1+r_2)$ be r_2 pairs of complex conjugate fields, so that $r_1+2r_2=n$. We denote by $\gamma^{(q)}(1\leqq q\leqq n)$ the conjugates of γ, the number of K, and define

$$\mathrm{trace}(\gamma)=\sum_{q=1}^{n}\gamma^{(q)}\,.$$

Let γ_r $(1\leqq r\leqq n)$ be numbers of K and x_r $(1\leqq r\leqq n)$ be real variables. We set $\xi=\sum_{r=1}^{n}\gamma_r x_r$ and define $\xi^{(q)}=\sum_{r=1}^{n}\gamma_r^{(q)}x_r$,

$$\mathrm{trace}(\xi)=\sum_{q=1}^{n}\xi^{(q)}\,.$$

For brevity we write

$$E(\gamma)=e^{2\pi i\,\mathrm{trace}(\gamma)}\,,\quad E(\xi)=e^{2\pi i\,\mathrm{trace}(\xi)}\,,$$

and use the abbreviations

$$\|\gamma\|=\operatorname*{Max}_{1\leqq q\leqq n}|\gamma^{(q)}|\,,\quad \|\xi-\gamma\|=\operatorname*{Max}_{1\leqq q\leqq n}|\xi^{(q)}-\gamma^{(q)}|\,.$$

A number γ of K is called totally positive or totally non-negative according to

$$\gamma^{(l)}>0 \quad \text{or} \quad \gamma^{(l)}\geqq 0 \qquad (1\leqq l\leqq r_1)$$

respectively. If γ is a totally non-negative integer of K and satisfies $\|\gamma\|\leqq T$ for some positive T, then we write

$$\gamma\prec T\,.$$

We use a letter c (and similarly $c_0, c_1, \cdots$) to denote a positive constant depending on K, k and s. It is not necessarily the same one each time it occurs. The constant c may well depend on another parameter $*$. In this case we write as $c(*)$ to plain the meaning. We express by Δ a positive real number which can be taken arbitrarily small. If F and G are functions of certain variables and G is positive, then the notation

$$F=O(G)$$

means that there exists a positive constant c such that $|F|\leqq cG$ in the domain designated. In many cases, we use small Roman, Greek and German letters to denote rational integers, numbers of K and integral ideals of K, respectively.

Finally, I should like to express my warmest thanks to Prof. Siegel for his valuable advises during his stay in Japan, and also to Mr. Mitsui who read this paper and gave valuable remarks.

§ 1. Singular series.

Let $\mathfrak{d}$ be the ramification ideal of K, and D be the discriminant of K, so that $N(\mathfrak{d})=D$. For any number γ in K, we can determine uniquely integral ideals $\mathfrak{a}, \mathfrak{b}$ such that

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

We write, then,

$$\gamma\to\mathfrak{a}\,,$$

for convenience. Since, by definition (see [2], p. 131),

$$\mathfrak{d}^{-1}=\{\rho: E(\rho\alpha)=1 \text{ for every } \alpha\in\mathfrak{o}\}\,,$$

we obtain

$$E(\lambda^k\gamma)=E(\mu^k\gamma)\,, \tag{1}$$

provided

$$\gamma \rightarrow \mathfrak{a},\ \lambda, \mu \in \mathfrak{o} \text{ and } \lambda \equiv \mu \pmod{\mathfrak{a}}.$$

Now, we constitute the sum $\sum_{\lambda} E(\lambda^k \gamma)$, where the summation being over a complete system of residues to the modulus $\mathfrak{a}$. In view of (1), the sum mentioned above is independent of the choice of a system. We denote this exponential sum by

$$S(\gamma),$$

and write

$$S(\gamma) = \sum_{\lambda \bmod \mathfrak{a}} E(\lambda^k \gamma).$$

LEMMA 1. *Let γ_j $(1 \leqq j \leqq r)$ be numbers of K and $\gamma_j \rightarrow \mathfrak{a}_j$ in the sense just stated. If $\mathfrak{a}_j$ are relatively prime in pairs, then*

$$\gamma_1 + \gamma_2 + \cdots + \gamma_r \rightarrow \mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_r$$

$$S(\gamma_1 + \gamma_2 + \cdots + \gamma_r) = S(\gamma_1) S(\gamma_2) \cdots S(\gamma_r).$$

PROOF. The first part of the lemma is obvious. Suppose that

$$\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_r = \mathfrak{a}_1 \mathfrak{b}_1 = \mathfrak{a}_2 \mathfrak{b}_2 = \cdots = \mathfrak{a}_r \mathfrak{b}_r,$$

and choose β_j such that

$$\beta_j \in \mathfrak{o},\ (\beta_j) = \mathfrak{b}_j \mathfrak{c}_j,\ \mathfrak{c}_j \subseteqq \mathfrak{o} \text{ and } (\mathfrak{c}_j, \mathfrak{a}_j) = \mathfrak{o}.$$

Consequently, if λ_j runs over a complete residue system mod $\mathfrak{a}_j$, then $\lambda_j \beta_j$ constitute also a similar set. It is now easy to deduce that

$$\sum_{j=1}^{r} (\lambda_j \beta_j)^k \gamma_j - \Big(\sum_{j=1}^{r} \lambda_j \beta_j\Big)^k \Big(\sum_{j=1}^{r} \gamma_j\Big) \in \mathfrak{d}^{-1},$$

whence follows

$$\begin{aligned} S(\gamma_1) S(\gamma_2) \cdots S(\gamma_r) &= \sum_{\lambda_1 \bmod \mathfrak{a}_1} E(\lambda_1^k \gamma_1) \sum_{\lambda_2 \bmod \mathfrak{a}_2} E(\lambda_2^k \gamma_2) \cdots \sum_{\lambda_r \bmod \mathfrak{a}_r} E(\lambda_r^k \gamma_r) \\ &= \sum_{\lambda_1} \sum_{\lambda_2} \cdots \sum_{\lambda_r} E((\lambda_1 \beta_1)^k \gamma_1 + (\lambda_2 \beta_2)^k \gamma_2 + \cdots + (\lambda_r \beta_r)^k \gamma_r) \\ &= \sum_{\lambda_1} \sum_{\lambda_2} \cdots \sum_{\lambda_r} E((\lambda_1 \beta_1 + \lambda_2 \beta_2 + \cdots + \lambda_r \beta_r)^k (\gamma_1 + \gamma_2 + \cdots + \gamma_r)). \end{aligned}$$

Since $\lambda_1 \beta_1 + \lambda_2 \beta_2 + \cdots + \lambda_r \beta_r$ runs through a complete system of residues to the modulus $\mathfrak{a}_1 \mathfrak{a}_2 \cdots \mathfrak{a}_r$, we get the second part of the lemma.

Let ν be an integer and $\mathfrak{a}$ be an integral ideal in K. Now, we constitute the sum $\sum_{\gamma} N(\mathfrak{a})^{-s} S(\gamma)^s E(-\nu\gamma)$, where the summation being over a reduced residue system of $(\mathfrak{a}\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$, (obviously $\gamma \rightarrow \mathfrak{a}$). We denote this sum by

$$H(\mathfrak{a}),$$

and write

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

LEMMA 2. *Let $\mathfrak{a}_j$ $(1 \leqq j \leqq r)$ be integral ideals of K. If $\mathfrak{a}_j$ are relatively prime* *in pairs, then*

$$H(\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_r)=H(\mathfrak{a}_1)H(\mathfrak{a}_2)\cdots H(\mathfrak{a}_r).$$

PROOF. By Lemma 1,

$$H(\mathfrak{a}_1)H(\mathfrak{a}_2)\cdots H(\mathfrak{a}_r)=N(\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_r)^{-s}\sum_{\gamma_1}^{*}\sum_{\gamma_2}^{*}\cdots\sum_{\gamma_r}^{*} S(\gamma_1)^s S(\gamma_2)^s\cdots S(\gamma_r)^s E(-\nu\gamma_1)E(-\nu\gamma_2)\cdots E(-\nu\gamma_r)$$

$$=N(\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_r)^{-s}\sum_{\gamma_1}^{*}\sum_{\gamma_2}^{*}\cdots\sum_{\gamma_r}^{*} S(\gamma_1+\gamma_2+\cdots+\gamma_r)E(-\nu(\gamma_1+\gamma_2+\cdots+\gamma_r)).$$

If γ_j runs over a reduced residue system of $(\mathfrak{a}_j\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$, then $\gamma_1+\gamma_2+\cdots+\gamma_r$ runs through a reduced residue system of $(\mathfrak{a}_1\mathfrak{a}_2\cdots\mathfrak{a}_q\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$. Hence, we obtain the result stated.

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

$$\lambda_1^k+\lambda_2^k+\cdots+\lambda_s^k\equiv\nu \pmod{\mathfrak{a}},$$

when $\lambda_1,\lambda_2,\cdots,\lambda_s$ run independently through complete systems of residues to the modulus $\mathfrak{a}$.

LEMMA 3. $M(\mathfrak{a})=N(\mathfrak{a})^{s-1}\sum_{\mathfrak{f}\mid\mathfrak{a}}H(\mathfrak{f})$.

PROOF. If γ runs over a complete residue system of $(\mathfrak{a}\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$, then

$$\sum_{\gamma}E(\alpha\gamma)=\begin{cases} N\mathfrak{a} & (\alpha\in\mathfrak{a}) \\ 0 & (\alpha\notin\mathfrak{a},\ \alpha\in\mathfrak{o}) \end{cases}$$

(see [3], p. 45). Hence,

$$M(\mathfrak{a})N(\mathfrak{a})=\sum_{\gamma}\sum_{\lambda_1}\sum_{\lambda_2}\cdots\sum_{\lambda_s}E((\lambda_1^k+\lambda_2^k+\cdots+\lambda_s^k-\nu)\gamma), \tag{2}$$

where γ runs over a complete residue system $(\mathfrak{a}\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$, and $\lambda_r (1\leqq r\leqq s)$ runs through a complete residue set mod $\mathfrak{a}$. Let $\mathfrak{c}$ be a divisor of $\mathfrak{a}$ and $\mathfrak{a}=\mathfrak{c}\mathfrak{f}$. Choose ρ and α from $\mathfrak{c}$ and $(\mathfrak{d}\mathfrak{a})^{-1}$ respectively such that

$$(\rho)=\mathfrak{c}\mathfrak{m},\qquad (\mathfrak{m},\mathfrak{f})=\mathfrak{o},$$

and

$$(\alpha)=(\mathfrak{d}\mathfrak{a})^{-1}\mathfrak{b},\quad (\mathfrak{a},\mathfrak{b})=\mathfrak{o}.$$

Then, $\rho\alpha\beta$ runs over a reduced residue system F^* of $(\mathfrak{f}\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$, if β runs over a reduced residue system mod $\mathfrak{f}$. Let denote by F a complete residue system mod $\mathfrak{f}$. It follows, from (2), that

$$M(\mathfrak{a})N(\mathfrak{a})=\sum_{\mathfrak{c}\mid\mathfrak{a}}\left(\frac{N\mathfrak{a}}{N\mathfrak{f}}\right)^s\sum_{\gamma}^{*}(\sum_{\lambda}E(\lambda^k\gamma))^s E(-\nu\gamma), \tag{3}$$

where γ and λ run through F^* and F respectively. Clearly the right hand side of (3) is equal to

$$N(\mathfrak{a})^s \sum_{\mathfrak{c}|\mathfrak{a}} H(\mathfrak{f}) = N(\mathfrak{a})^s \sum_{\mathfrak{f}|\mathfrak{a}} H(\mathfrak{f}),$$

whence follows the result.

We can prove that

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

in a similar way as in the rational case (see [6]). The result was also obtained in more general form (see [3]). We define

$$G(\gamma) = N(\mathfrak{a})^{-1} S(\gamma) = N(\mathfrak{a})^{-1} \sum_{\lambda \bmod \mathfrak{a}} E(\lambda^k \gamma),$$

assuming that $\gamma \to \mathfrak{a}$.

LEMMA 4. *For any positive* Δ,

$$G(\gamma) = O(c(\Delta) N(\mathfrak{a})^{-\frac{1}{k}+\Delta}).$$

LEMMA 5. *Let* $\mathfrak{p}$ *be a prime ideal of* K, p *be a prime rational integer contained in* $\mathfrak{p}$, *and* $N(\mathfrak{p}) = p^f$. *Let* l *be a positive rational integer. There exist positive rational integers* d, q_r *and* $\eta_r \in \mathfrak{o}$ *such that the linear form*

$$a_1\eta_1^k + a_2\eta_2^k + \cdots + a_d\eta_d^k$$

$$a_r = 1, 2, \cdots, q_r \qquad (1 \leqq r \leqq d) \tag{4}$$

uniquely represents all numbers of J_k *modulo* $\mathfrak{p}^l$, *where* q_r *is a power of* p *and*

$$d \leqq fl.$$

PROOF. Let g be the number of residue classes to the modulus $\mathfrak{p}^l$ which contain integers of J_k. Suppose that $\eta_1 \notin \mathfrak{p}$ and $\mathfrak{p}_1$ is the smallest positive rational integer x satisfying the congruence

$$x\eta_1^k \equiv 0 \qquad (\mathrm{mod}\ \mathfrak{p}^l).$$

It is plain that q_1 is a power of p. Let η_2 be an integer such that

$$\eta_2^k \not\equiv a_1\eta_1^k \qquad (\mathrm{mod}\ \mathfrak{p}^l)$$

for every $a_1 (a_1 = 1, 2, \cdots, q_1)$, and q_2 be the smallest positive rational integer x satisfying the congruence

$$x\eta_2^k \equiv a_1\eta_2^k \qquad (\mathrm{mod}\ \mathfrak{p}^l)$$

for some $a_1 (a_1 = 1, 2, \cdots, q_1)$. It is plain that q_2 is a power of p. Let η_3 be an integer such that

$$\eta_3^k \not\equiv a_1\eta_1^k + a_2\eta_2^k \qquad (\mathrm{mod}\ \mathfrak{p}^l)$$

for every pair of a_1, a_2 $(a_1 = 1, 2, \cdots, q_1;\ a_2 = 1, 2, \cdots, q_2)$, and q_3 be the smallest positive rational integer x satisfying the congruence

$$x\eta_3^k \equiv a_1\eta_1^k + a_2\eta_2^k \qquad (\mathrm{mod}\ \mathfrak{p}^l)$$

for some pair of a_1, a_2 $(a_1 = 1, 2, \cdots, q_1;\ a_2 = 1, 2, \cdots, q_2)$. It is plain that q_3 is a power of p. Repeating this process, we are able to prove that every k-th power of integer in K and so every number of J_k can be expressed uniquely in the form (4). Because of

$$p^d \leqq q_1 q_2 \cdots q_d = g \leqq N(\mathfrak{p})^l = p^{fl},$$

the last assertion is also true.

We consider a non-archimedean valuation of K induced by a prime ideal $\mathfrak{p}$ of K. We denote by $K_{\mathfrak{p}}$ the completion of K with respect to this valuation. Let α be a number of K. We denote by

$$\mathrm{Ord}\,\alpha$$

the exponent to which $\mathfrak{p}$ enters into the canonical factorization of α. Suppose that A is a number of $K_{\mathfrak{p}}$ and is defined by Cauchy sequence $\{\alpha_n\}, \alpha_n \in K$. Since there exists $\lim_{n\to\infty} \mathrm{Ord}\,\alpha_n$, we denote it by

$$\mathrm{Ord}\,A.$$

It is independent of a choice of Cauchy sequence. Let p be a prime rational integer in $\mathfrak{p}$ and $\mathfrak{p}^e \| p$. (The notation means as usual that $\mathfrak{p}^e | p$, and $\mathfrak{p}^{e+1} \nmid p$.) It is well known (see [1], p. 416) that the series

$$1 + A + \frac{A^2}{2!} + \frac{A^3}{3!} + \cdots$$

is convergent in $K_{\mathfrak{p}}$, if

$$\mathrm{Ord}\,A > \frac{e}{p-1}. \tag{5}$$

We denote it by $\exp A$. Then, it is obvious that

$$\mathrm{Ord}(\exp A - 1) = \mathrm{Ord}\,A.$$

The series

$$A - \frac{A^2}{2} + \frac{A^3}{3} - \cdots$$

is convergent in $K_{\mathfrak{p}}$, if

$$\mathrm{Ord}\,A > 0. \tag{6}$$

We denote it by $\log(1+A)$. Then, it is obvious that

$$\mathrm{Ord}\,(\log(1+A)) = \mathrm{Ord}\,A.$$

LEMMA 6. *Let $\mathfrak{p}$ be a prime ideal of K and p be a prime rational integer contained in $\mathfrak{p}$. Assume that $\mathfrak{p}^e \| p, p^b \| k$, and*

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

Let α be an integer of K. If the congruence

$$\xi^k \equiv \alpha \pmod{\mathfrak{p}^{l_0}} \tag{7}$$

is soluble with ξ *not divisible by* $\mathfrak{p}$, *then for any rational integer* $l \geqq l_0$ *the congruence*

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

is also soluble.

PROOF. Firstly, we assume that k is not divisible by $\mathfrak{p}$ $(b=0)$, and $\mathfrak{p} \| \pi$, $\pi \in \mathfrak{o}$. If (7) is soluble, then

$$k\xi^{k-1}\pi^{l_0}\eta \equiv \alpha - \xi^k \pmod{\mathfrak{p}^{l_0+1}}$$

is also soluble with respect to η, since $(k\xi^{k-1}, \mathfrak{p}) = \mathfrak{o}$. Then,

$$(\xi + \pi^{l_0}\eta)^k \equiv \alpha \pmod{\mathfrak{p}^{l_0+1}}.$$

Repeating this process we get the result.

Secondly, we assume that k is divisible by $\mathfrak{p}$ $(b>0)$. If (7) is soluble, then

$$\frac{\alpha}{\xi^k} \equiv 1 \pmod{\mathfrak{p}^{l_0}}.$$

Hence, by (6), there exists

$$\log\left(1 + \left(\frac{\alpha}{\xi^k} - 1\right)\right) = \log \frac{\alpha}{\xi^k}.$$

Since,

$$\mathrm{Ord}\left(\frac{1}{k} \log \frac{\alpha}{\xi^k}\right) = \mathrm{Ord}\left(\log \frac{\alpha}{\xi^k}\right) - \mathrm{Ord}\, k$$

$$= \mathrm{Ord}\left(\frac{\alpha}{\xi^k} - 1\right) - \mathrm{Ord}\, k \geqq l_0 - eb > \frac{e}{p-1},$$

there exists also

$$\exp\left(\frac{1}{k} \log \frac{\alpha}{\xi^k}\right)$$

by (5). If we denote it by A, then we obtain $\alpha = (A\xi)^k$ by usual computation. Choose η in $\mathfrak{o}$ such that

$$\mathrm{Ord}(A\xi - \eta) \geqq l,$$

then

$$\mathrm{Ord}(\eta^k - \alpha) = \mathrm{Ord}(\eta^k - (A\xi)^k) \geqq l,$$

whence follows

$$\eta^k \equiv \alpha \pmod{\mathfrak{p}^l}.$$

LEMMA 7. *Let* $\mathfrak{p}$ *be a prime ideal of* K *and* p *a prime rational integer contained in* $\mathfrak{p}$. *Assume that* $\mathfrak{p}^e \| p$, $N(\mathfrak{p}) = p^f$, *and* $p^b \| k$ $(k \geqq 3)$, *and put*

$$l_0 = (b+2)e, \quad s_0 = [8nk(\log k + 1)].$$

If $l \geqq l_0$, $s \geqq s_0$ *and* $\nu \in J_k$, *then*

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

Proof. It is well known (see [6], p. 50) that, if $l_1 \geqq b+2$ and $r \geqq 4k\,(k \geqq 3)$, then, for any positive rational integer x, the equation of congruence

$$x \equiv y_1^k + y_2^k + \cdots + y_r^k \qquad (\mathrm{mod}\ p^{l_1})$$

is soluble with rational integers $y_j\,(1 \leqq j \leqq r), p \nmid y_1$. Using the result just stated, with the aid of Lemma 5, we can infer that, for any integer ν of J_n, the equation of congruence

$$\nu \equiv \zeta_1^k + \zeta_2^k + \cdots + \zeta_{rd}^k \qquad (\mathrm{mod}\ \mathfrak{p}^{el_1}) \tag{8}$$

is soluble with $\mathfrak{p} \nmid \zeta_1$ and

$$d \leqq fel_1 . \tag{9}$$

We put

$$l_1 = b+2,\ l_0 = el_1 = e(b+2),\ \text{and}\ r = 4k .$$

Since $2^b \leqq p^b \leqq k$, we obtain

$$4kfl_0 = 4kfe(b+2) \leqq 4kn(b+2) \leqq 4kn\left(\frac{\log k}{\log 2} + 2\right),$$

and so

$$rd \leqq rfel_1 \leqq [8nk(\log k + 1)] = s_0 . \tag{10}$$

It follows, from (8), (9) and (10), that the equation of congruence

$$\nu \equiv \zeta_1^k + \zeta_2^k + \cdots + \zeta_s^k \qquad (\mathrm{mod}\ \mathfrak{p}^{l_0}) \tag{11}$$

is soluble with $\mathfrak{p} \nmid \zeta_1$ provided $s \geqq s_0$.

Suppose that $\mathfrak{p} \| \pi, \pi \in \mathfrak{o}$ and

$$\xi_r = \zeta_r + \pi^{l_0}\lambda \qquad (2 \leqq r \leqq s), \tag{12}$$

where λ runs over a complete residue system mod $\mathfrak{p}^{l-l_0}$. From (11), we see that

$$\nu - \zeta_2^k - \cdots - \zeta_s^k$$

is a reduced k-th power residue mod $\mathfrak{p}^{l_0}$. It follows, from Lemma 6, that

$$\nu - \xi_2^k - \cdots - \xi_s^k$$

are reduced k-th power residues mod $\mathfrak{p}^l$, and the number of such residues is greater than

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

by (12). This implies the result stated.

Theorem 1. *Assume that* $k \geqq 3$, $s \geqq s_0 = [8nk(\log k + 1)]$, *and* ν *is an integer of* J_k. *Then, the series* $\mathfrak{S}(\nu) = \sum_{\mathfrak{a}} H(\mathfrak{a})$ *is absolutely convergent, and there exists a constant* c_0 *such that*

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

The series $\chi(\mathfrak{p}) = \sum_{l=0}^{\infty} H(\mathfrak{p}^l)$ *is also absolutely convergent, and we obtain the product* *formula.*

$$\mathfrak{S}(\nu)=\prod_{\mathfrak{p}} \chi(\mathfrak{p}) . \tag{13}$$

PROOF. Since

$$H(\mathfrak{a})=O(c(\Delta)N(\mathfrak{a})^{1-\frac{s}{k}+\Delta}), \tag{14}$$

by Lemma 4, the series $\sum_{\mathfrak{a}} H(\mathfrak{a})$ and $\sum_{l=0}^{\infty} H(\mathfrak{p}^l)$ are absolutely convergent for $s\geqq s_0$. Hence, by Lemma 2,

$$\prod_{N\mathfrak{p}\leqq x} \chi(\mathfrak{p})=\prod_{N\mathfrak{p}\leqq x} \{\sum_{l=0}^{\infty} H(\mathfrak{p}^l)\}=\sum_{N\mathfrak{a}\leqq x} H(\mathfrak{a})+\sum_{x<N\mathfrak{a}}' H(\mathfrak{a})$$

where $\sum'$ runs over all ideals whose prime divisors having norms not exceeding x. Take the limit as $x\to\infty$ we get (13). It follows, from Lemma 3 and Lemma 7, that

$$\sum_{\mathfrak{f}|\mathfrak{p}^l} H(\mathfrak{f})\geqq N(\mathfrak{p})^{-l_0(s-1)}$$

provided $s\geqq s_0$ and $l\geqq l_0$. Take the limit as $l\to\infty$, we get

$$\chi(\mathfrak{p})\geqq N(\mathfrak{p})^{-l_0(s-1)} .$$

We know, from (14), that there exists c such that

$$|\sum_{l=1}^{\infty} H(\mathfrak{p}^l)|<N(\mathfrak{p})^{-2}$$

provided $N(\mathfrak{p})\geqq c$. Then,

$$\mathfrak{S}(\nu)=\prod_{N\mathfrak{p}<c} \chi(\mathfrak{p})\prod_{N\mathfrak{p}\geqq c} \chi(\mathfrak{p})>\prod_{N\mathfrak{p}<c} N(\mathfrak{p})^{-l_0(s-1)}\prod_{N\mathfrak{p}\geqq c}\left(1-\frac{1}{N(\mathfrak{p})^2}\right)=c_0 .$$

§ 2. Basic domain.

Throughout the paper, we write

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

for sufficiently large positive T. Let $\omega_1, \omega_2,\cdots, \omega_n$ be an integral basis of K. We can choose $\rho_1, \rho_2,\cdots, \rho_n$, a basis of $\mathfrak{d}^{-1}$, such that

$$\operatorname{trace}(\rho_r\omega_s)=\begin{cases} 1 & (r=s) \\ 0 & (r\neq s) \end{cases} \tag{15}$$

(see [2], p. 133). Let X be the whole n-dimensional Euclidean space and U be the unit cube

$$\{(x_1, x_2,\cdots, x_n):\ 0\leqq x_r\leqq 1 \quad (1\leqq r\leqq n)\} .$$

We denote by Γ the set consisting of

$$\gamma=\rho_1x_1+\rho_2x_2+\cdots+\rho_nx_n ,$$

fulfilling the conditions

$$(x_1, x_2, \cdots, x_n) \in U,\ x_r;\ \text{ rational number } (1 \leqq r \leqq u),\ N\mathfrak{a} \leqq t^n ,$$

where $\gamma \rightarrow \mathfrak{a}$ in the sense defined in the preceding section. Hence for a given $\mathfrak{a}$, the number of (γ) in Γ, subject to $\gamma \rightarrow \mathfrak{a}$, is $O(N\mathfrak{a})$. Next consider the number of γ in Γ satisfying $(\gamma)=(\gamma_0)$, for a given $\gamma_0 \in \Gamma$. By the theory of units (see [2], p. 124), we can choose a unit ε_0 such that

$$\gamma_1 = \gamma_0 \varepsilon_0 ,$$

$$c_1 N(\gamma_0)^{\frac{1}{n}} \leqq |\gamma_1^{(r)}| \leqq c_2 N(\gamma_0)^{\frac{1}{n}} \qquad (1 \leqq r \leqq n) .$$

Noting that $N(\gamma_0) \geqq \dfrac{1}{DN\mathfrak{a}}$ $(\gamma_0 \rightarrow \mathfrak{a})$, we obtain

$$|\gamma_1^{(r)}| > \frac{c}{\sqrt[n]{N\mathfrak{a}}} .$$

If we put $\gamma = \gamma_1 \varepsilon$, then ε is a unit and satisfies

$$\|\varepsilon\| \leqq c \sqrt[n]{N\mathfrak{a}}$$

since $\|\gamma\| = O(1)$ and $|\gamma_1^{(r)}|^{-1} = O(\sqrt[n]{N\mathfrak{a}})$. Consequently the number of ε is $O(N\mathfrak{a})$, and the number of $\gamma \in \Gamma$ satisfying $\gamma \rightarrow \mathfrak{a}$ is

$$O(N\mathfrak{a}^2) . \tag{16}$$

We set

$$\xi = \rho_1 x_1 + \rho_2 x_2 + \cdots + \rho_n x_n,\ \eta = \omega_1 y_1 + \omega_2 y_2 + \cdots + \omega_n y_n ,$$

with respect to real variables $x_1, x_2, \cdots, x_n$ and $y_1, y_2, \cdots, y_n$. We use abbreviations

$$dx = dx_1 dx_2 \cdots dx_n,\ dy = dy_1 dy_2 \cdots dy_n .$$

For every $\gamma \in \Gamma$, we define the basic domain B_γ by

$$\{(x_1, x_2, \cdots, x_n) :\ (x_1, x_2, \cdots, x_n) \in U,$$

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

The following fundamental lemmas were proved by Siegel.

LEMMA 8 (see [5], p. 326). *If $\gamma_1, \gamma_2 \in \Gamma$, $\gamma_1 \neq \gamma_2$ and $T > c$, then*

$$B_{\gamma_1} \cap B_{\gamma_2} = 0 .$$

LEMMA 9 (see [5], p. 330). *If we write*

$$L(\xi) = \sum_{\lambda < T} E(\lambda^k \xi),\ \xi - \gamma = \zeta ,$$

then

$$L(\xi) = G(\gamma) \int_{\eta < T} E(\eta^k \zeta) dy + O(T^{n-a}) .$$

LEMMA 10 (see [5], p. 335). *If we write*

$$\tau = T^k \zeta ,$$

then

$$\int_{\eta < T} E(\eta^k \zeta) dy = O(T^n N(\mathrm{Min}(1, |\tau|^{-\frac{1}{k}}))) .$$

LEMMA 11 (see [5], p. 335).

$$\int_U N(\mathrm{Min}(1, |\tau|^{-\frac{s}{k}})) dx = O(T^{-nk})$$

for $s > k$.

LEMMA 12 (see [5], p. 337). *If we define, for* $\mu < 1$ and $s > k+1$,

$$J(\mu) = \int_X \phi_1(\xi) E(-\mu\xi) dx, \quad \phi_1(\xi) = \Big(\int_{\eta < 1} E(\eta^k \xi) dy\Big)^s ,$$

then

$$J(\mu) = D^{\frac{1}{2}(1-s)} \prod_{l=1}^{r} F(\mu^{(l)}) \prod_{m=r_1+1}^{r_1+r_2} H(\mu^{(m)}) ,$$

with

$$F(\mu^{(l)}) = \frac{\Gamma^s\Big(1+\dfrac{1}{k}\Big)}{\Gamma\Big(\dfrac{s}{k}\Big)} (\mu^{(l)})^{\frac{s}{k}-1}$$

and

$$H(\mu^{(m)}) = k^{-1} \int \sum_{r=1}^{s} (k^{-1} u_r^{\frac{1}{k}-1}) du_1 \cdots du_{s-1} d\varphi_1 \cdots d\varphi_{s-1} ,$$

where the last integral extended over the domain

$$0 < u_r < 1 \ (1 \leqq r \leqq s), \ -\pi < \varphi_r < \pi \ (1 \leqq r \leqq s-1) ,$$

$$u_s = |\mu^{(m)} - (u_1^{\frac{1}{2}} e^{i\varphi_1} + u_2^{\frac{1}{2}} e^{i\varphi_2} + \cdots + u_{s-1}^{\frac{1}{2}} e^{i\varphi_{s-1}})|^2 .$$

Now we proceed to prove the following

THEOREM 2. *Let* ν *be a totally positive integer of* K. *If*

$$s \geqq \frac{1}{a} nk + 1 \ \Big(0 < a \leqq \frac{1}{4}\Big), \ \nu < T^k ,$$

then

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

where

$$\mu = T^{-k} \nu .$$

PROOF. It follows from Lemma 4, Lemma 9 and Lemma 10 that

$$L(\xi)^s = G(\gamma)^s \phi(\zeta) + O(T^{s(n-a)})$$

$$+ O(c(\Delta) N(\mathfrak{a})^{-\frac{s-1}{k}+\Delta} T^{n(s-1)} N(\mathrm{Min}(1, |\tau|^{-\frac{s-1}{k}})) T^{n-a}) ,$$

where

$$\phi(\zeta)=\Big(\int_{\eta\prec T}E(\eta^k\zeta)dy\Big)^s.$$

Put $\Delta=1/2$ and assume that $s\geqq 4k+1$, then

$$\sum_{\gamma\in\Gamma}N(\mathfrak{a})^{-\frac{s-1}{k}+\Delta}=O(1)\,,$$

by (16). Consequently, if

$$s\geqq\frac{1}{a}nk+1\,, \tag{17}$$

then

$$\sum_{\gamma\in\Gamma}\int_{B_\gamma}L(\xi)^sE(-\nu\xi)dx=\sum_{\gamma\in\Gamma}G(\gamma)^sE(-\nu\gamma)\int_{B_\gamma}\phi(\zeta)E(-\nu\zeta)dx$$

$$-O(T^{s(n-a)})+O(T^{n(s-1)+n-a})\int_U N(\mathrm{Min}(1,|\tau|^{-\frac{s-1}{k}}))dx$$

$$=\sum_{\gamma\in\Gamma}G(\gamma)^sE(-\nu\gamma)\int_{B_\gamma}\phi(\zeta)E(-\nu\zeta)dx+O(T^{n(s-k)-a})\,, \tag{18}$$

by Lemma 11.

If $(x_1, x_2,\cdots, x_n)$ is a point of $X-B_\gamma$, then the inequality

$$|\zeta^{(q)}|>\frac{1}{h\sqrt[n]{N\mathfrak{a}}} \tag{19}$$

is true for at least one index q. By Lemma 10,

$$\int_{X-B_\gamma}\phi(\zeta)E(-\nu\zeta)dx=O(T^{ns})\int_{X-B_\gamma}N(\mathrm{Min}(1,|\tau|^{-\frac{s}{k}}))dx$$

$$=O(1)\int_{X-B_\gamma}N(\mathrm{Min}(T^s,|\zeta|^{-\frac{s}{k}}))dx\,.$$

If we change the variables as follows

$$\zeta^{(l)}=u_l\ (1\leqq l\leqq r_1),\quad \zeta^{(m)}=u_me^{i\varphi_m}\ (r_1+1\leqq m\leqq r_1+r_2)\,,$$

then

$$\left|\frac{\partial(x_1,\ x_2,\ \cdots\cdots\cdots\cdots\cdots\cdots,\ x_n)}{\partial(u_1,\cdots,u_{r_1+r_2},\ \varphi_{r_1+1}\cdots\varphi_{r_1+r_2})}\right|=D^{\frac{1}{2}}\prod_{m=r_1+1}^{r_1+r_2}(2u_m)\,,$$

hence, by (19),

$$\int_{X-B_\gamma}\phi(\zeta)E(-\nu\zeta)dx=O(1)\Big(\int_{h^{-1}N(\mathfrak{a})^{-\frac{1}{n}}}^{\infty}u_q^{-\frac{s}{k}}du_q\Big)\prod_{\substack{1\leqq l\leqq r_1\\ l\neq q}}\int_0^\infty\mathrm{Min}(T^s,u_l^{-\frac{s}{k}})du_l$$

$$\times\prod_{r_1+1\leqq m\leqq r_1+r_2}2\int_{-\pi}^{\pi}\Big(\int_0^\infty\mathrm{Min}(T^{2s},u_m^{-\frac{2s}{k}})u_mdu_m\Big)d\varphi_m\,,$$

or

$$=O(1)\Big(\int_{h^{-1}N(\mathfrak{a})^{-\frac{1}{n}}}^{\infty}u_q^{1-\frac{2s}{k}}du_q\Big)\prod_{1\leqq l\leqq r_1}\int_0^\infty\mathrm{Min}(T^s,u_l^{-\frac{s}{k}})du_l$$

$$\times\prod_{\substack{r_1+1\leqq m\leqq r_1+r_2\\ m\neq q}}2\int_{-\pi}^{\pi}\Big(\int_0^\infty\mathrm{Min}(T^{2s},u_m^{-\frac{2s}{k}})u_mdu_m\Big)d\varphi_m\,.$$

Noting that

$$\int_0^\infty \mathrm{Min}(T^s, u^{-\frac{s}{k}})du=O(T^{s-k}), \quad \int_0^\infty \mathrm{Min}(T^{2s}, u^{-\frac{2s}{k}})udu=O(T^{2(s-k)}),$$

we have

$$\int_{X-B_\gamma}\phi(\zeta)E(-\nu\zeta)dx=O(T^{(n-1)(s-k)}h^{\frac{s}{k}-1}N(\mathfrak{a})^{\frac{1}{n}\left(\frac{s}{k}-1\right)})$$

or

$$=O(T^{(n-2)(s-k)}h^{\frac{2s}{k}-2}N(\mathfrak{a})^{\frac{2}{n}\left(\frac{s}{k}-1\right)}).$$

From Lemma 4 and (16), by taking $\Delta=1$, we obtain

$$\sum_{\gamma\in\Gamma}G(\gamma)^s N(\mathfrak{a})^{\frac{1}{n}\left(\frac{s}{k}-1\right)} \quad \text{or} \quad \sum_{\gamma\in\Gamma}G(\gamma)^s N(\mathfrak{a})^{\frac{2}{n}\left(\frac{s}{k}-1\right)}$$

$$=O(\sum_{N\mathfrak{a}\leqq t^n}N(\mathfrak{a})^2)=O(t^{3n}).$$

Hence,

$$\sum_{\gamma\in\Gamma}G(\gamma)^s E(-\nu\gamma)\int_{X-B_\gamma}\phi(\zeta)E(-\nu\zeta)dx=O(T^{(n-1)(s-k)}T^{(k-1+a)\left(\frac{s}{k}-1\right)}t^{3n})$$

$$=O(T^{n(s-k)}T^{-(1-a)\left(\frac{s}{k}-1-3n\right)})$$

$$=O(T^{n(s-k)-a}), \tag{20}$$

if $a<(1-a)\left(\frac{s}{k}-1-3n\right)$, which is true provided that (17) and

$$0<a\leqq\frac{1}{4}$$

hold.

It follows, from (18) and (20), that

$$\sum_{\gamma\in\Gamma}\int_{B_\gamma}L(\xi)^s E(-\nu\xi)dx=\sum_{\gamma\in\Gamma}G(\gamma)^s E(-\nu\gamma)\int_X\phi(\zeta)E(-\nu\zeta)dx$$

$$+O(T^{n(s-k)-a}). \tag{21}$$

Now, we put,

$$\nu=T^k\mu, \quad \xi=T^{-k}\xi_0, \quad \eta=T\eta_0,$$

$$T^k x_r=x_{0r}, \quad T^{-1}y_r=y_{0r}, \quad (1\leqq r\leqq n),$$

then we have

$$\int_X\phi(\xi)E(-\nu\xi)dx=\int_X\phi(T^{-k}\xi_0)E(-\mu\xi_0)T^{-kn}dx_0,$$

$$\phi(T^{-k}\xi_0)=T^{ns}\left(\int_{\eta_0<1}E(\eta_0{}^k\xi_0)dy_0\right)^s,$$

where

$$\xi_0=\rho_1x_{01}+\rho_2x_{02}+\cdots+\rho_nx_{0n}, \quad \eta_0=\omega_1y_{01}+\omega_2y_{02}+\cdots+\omega_ny_{0n},$$

with the abbreviations

$$dx_0 = dx_{01}dx_{02}\cdots dx_{0n},\ dy_0 = dy_{01}dy_{02}\cdots dy_{0n}.$$

It is now easy to deduce, from (21), that

$$\sum_{\gamma\in\Gamma}\int_{B_\gamma} L(\xi)^s E(-\nu\xi)dx = \sum_{\gamma\in\Gamma} G(\gamma)^s E(-\nu\gamma) T^{n(s-k)}$$

$$\times\int_X \phi_1(\xi)E(-\mu\xi)dx + O(T^{n(s-k)-a}) \tag{22}$$

where

$$\phi_1(\xi) = \left(\int_{\eta<1} E(\eta^k\xi)dy\right)^s.$$

Since $\mu<1$, we can infer that

$$J(\mu) = O(1),$$

by Lemma 12. Further, if $s\geqq 4k$, then

$$\sum_{\gamma\in\Gamma} G(\gamma)^s E(-\nu\gamma) = \mathfrak{S}(\nu) + O(T^{-1})$$

by Lemma 4, whence follows the theorem by (22) and Lemma 12.

§ 3. Supplementary domain.

We define the supplementary domain S by

$$S = U - \sum_{\gamma\in\Gamma} B_\gamma.$$

The following lemmas were proved by Siegel.

LEMMA 13 (see [5], p. 326). *If $(x_1, x_2, \cdots, x_n)\in S$, then there exist α and β in K such that*

$$\alpha\in\mathfrak{o},\ \beta\in\mathfrak{d}^{-1},\ \ ||\alpha\xi-\beta|| < h^{-1},\ \ t < ||\alpha|| \leqq h.$$

LEMMA 14 (see [5], p. 326). *If $|\alpha^{(q)}| < D^{-1/2}$ in Lemma 13, then*

$$h|\alpha^{(q)}\xi^{(q)} - \beta^{(q)}| \geqq D^{-1/2} \qquad (1\leqq q\leqq n).$$

LEMMA 15 (see [5], p. 326). *In Lemma 13,*

$$N((\alpha, \beta\mathfrak{d})) \leqq D^{1/2}.$$

LEMMA 16. *Let $\omega_r (1\leqq r\leqq n)$ be basis of all integers in K. Let A, B be positive functions of T such that $A/h\to 0$ $(T\to\infty)$. If $(x_1, x_2, \cdots, x_n)\in S$, then*

$$\underset{|\mu|<A}{\mathrm{Min}}\left\{B^n, \frac{B^{n-1}}{|1-E(\xi\mu\omega_r)|}\ (1\leqq r\leqq n)\right\}$$

$$= O\left\{(hB)^{n-1}\left(1+\frac{A}{||\alpha||}\right)(B+||\alpha||\log||\alpha||)\right\},$$

where α is the number satisfying the conditions of above three lemmas.

PROOF. Let

$$\mathrm{trace}(\xi\mu\omega_r)=a_r+d_r,\quad -\frac{1}{2}\leqq d_r<\frac{1}{2}\qquad (1\leqq r\leqq n),$$

with integral rational a_r, and define

$$\sum_{r=1}^{n} a_r\rho_r=\sigma,\quad \sum_{r=1}^{n} d_r\rho_r=\tau,$$

then $\mathrm{trace}((\sigma+\tau)\omega_r)=a_r+d_r$ and so $\xi\mu=\sigma+\tau$ by (15). Then

$$\underset{1\leqq r\leqq n}{\mathrm{Min}}(|1-E(\xi\mu\omega_r)|^{-1})=O(|\tau^{(q)}|^{-1},\quad (1\leqq q\leqq n)). \tag{23}$$

Define

$$z_l=\tau^{(l)}\qquad (1\leqq l\leqq r_1)$$

$$z_m=\frac{\tau^{(m)}+\bar{\tau}^{(m)}}{\sqrt{2}},\quad z_{m+r_2}=\frac{\tau^{(m)}-\bar{\tau}^{(m)}}{\sqrt{2}\,i}\quad (r_1+1\leqq m\leqq r_1+r_2),$$

moreover, let $g_1, g_2, \cdots, g_n$ be rational integers, and let $W=W(g_1, g_2, \cdots, g_n)$ denote the number of integers μ, fulfilling the conditions

$$|\mu|\prec A,$$
$$g_r\leqq 2D^{1/n}z_r\,\mathrm{Max}(|\alpha^{(r)}|, D^{-1/2})<g_{r+1}\qquad (1\leqq r\leqq n). \tag{24}$$

Let v and $n-v$ be numbers of $\alpha^{(p)}$ and $\alpha^{(q)}$ satisfying the inequalities

$$|\alpha^{(p)}|<D^{-1/2}\quad\text{and}\quad |\alpha^{(q)}|\geqq D^{-1/2}$$

respectively, moreover, let $\|\alpha\|=|\alpha^{(b)}|$, we get

$$\sum_{g_1,g_2,\cdots,g_n}^{*} W(g_1, g_2, \cdots, g_n)=O(h^{n-v-1}+h^vA^{n-v}|\alpha^{(b)}|^{-1}) \tag{25}$$

where the summation $\sum^*$ means to exclude g_b. This may be deduced by a similar argument as in [5] (p. 333). Since, by (24),

$$|\tau^{(b)}|^{-1}=O(g_r^{-1}|\alpha^{(b)}|),$$

we have, by (23) and (25),

$$\begin{aligned}&\sum_{|\mu|\prec A}\left\{B^n, \frac{B^{n-1}}{|1-E(\xi\mu\omega_r)|}\ (1\leqq r\leqq n)\right\}\\&=O(h^{n-v-1}+h^vA^{n-v}|\alpha^{(b)}|^{-1})\sum_{0\leqq g<O(|\alpha^{(b)}|)}\{\mathrm{Min}(B^n, B^{n-1}|\alpha^{(b)}|g^{-1})\}\\&=O(h^{n-1}+h^{n-1}A|\alpha^{(b)}|^{-1})((B^n+B^{n-1}|\alpha^{(b)}|\log|\alpha^{(b)}|)\\&=O\left\{(hB)^{n-1}\left(1+\frac{A}{\|\alpha\|}\right)(B+\|\alpha\|\log\|\alpha\|)\right\}.\end{aligned}$$

THEOREM 3. *If* $(x_1, x_2, \cdots, x_n)\in S$ *and* $0<a\leqq\frac{1}{4n}$, *then*

$$L(\xi)=O(T^{n-\frac{1}{2^k}}).$$

PROOF. Because of $L(\xi)=\sum_{\lambda<T} E(\lambda^k \xi)$,

$$|L(\xi)|^{2^{k-1}}=|\sum_{\lambda}\sum_{\lambda_1} E((\lambda+\lambda_1)^k\xi-\lambda^k\xi)|^{2^{k-2}} \qquad (\lambda<T,\ \lambda+\lambda_1<T)$$

$$\leqq\{\sum_{\lambda_1}|\sum_{\lambda} E(k\lambda_1\lambda^{k-1}\xi+\cdots)|\}^{2^{k-2}}$$

$$\leqq(cT^n)^{2^{k-2}-1}\sum_{\lambda_1}|\sum_{\lambda} E(k\lambda_1\lambda^{k-1}\xi+\cdots)|^{2^{k-2}},$$

by Hölder's inequality, and similarly,

$$\leqq(cT^n)^{2^{k-2}-1}(cT^n)^{2^{k-3}-1}\sum_{\lambda_1}\sum_{\lambda_2}|\sum_{\lambda} E(k(k-1)\lambda_1\lambda_2\lambda^{k-2}\xi+\cdots)|^{2^{k-2}}$$

$$\leqq(cT^n)^{2^{k-2}-1+\cdots+2^0-1}\sum_{\lambda_1}\sum_{\lambda_2}\cdots\sum_{\lambda_{k-1}}|\sum_{\lambda} E(\mu\lambda\xi)|, \tag{26}$$

where

$$\mu=k!\,\lambda_1\lambda_2\cdots\lambda_{k-1},\ |\lambda_r|<2T \qquad (r=1,2,\cdots,k-1), \tag{27}$$

and λ runs over all solutions of 2^{k-1} conditions

$$\lambda+\lambda_{p_1}+\cdots+\lambda_{p_g}<T$$

$$(1\leqq p_1<p_2<\cdots<p_g\leqq k-1,\ g=0,1,\cdots,k-1).$$

Let $A(\mu)$ denote the number of solutions of (27). It is easy to deduce that

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

This, combined with (26), gives

$$|L(\xi)|^{2^{k-1}}=O(T^{n(2^{k-1}-2)})+O(c(\Delta)T^{n(2^{k-1}-k)+\Delta}\sum_{\mu}|\sum_{\lambda} E(\mu\lambda\xi)|)$$

where

$$|\mu|<A=k!\,2^{k-1}T^{k-1}.$$

We know from [5] (p. 332) that

$$\sum_{\lambda} E(\mu\lambda\xi)=\mathrm{Min}(T,\ |1-E(\xi\mu\omega_r)|^{-1}\ (1\leqq r\leqq n))O(T^{n-1}),$$

whence follows, from Lemma 16, that

$$|L(\xi)|^{2^{k-1}}=O(T^{n(2^{k-1}-2)})+O(c(\Delta)T^{n2^{k-1}-1+an+\Delta}).$$

Now the lemma follows by taking $0<a\leqq\frac{1}{4n}$ and $\Delta=\frac{1}{4}$.

§ 4. Main theorem.

LEMMA 17. *Let $Q_s(T)$ denote the set of integers μ of K which can be expressed in the form*

$$\mu=\sigma_1{}^k+\sigma_2{}^k+\cdots+\sigma_s{}^k, \tag{28}$$

where σ_r $(1\leqq r\leqq s)$ *is a totally non-negative integer of* K *with*

$$\sigma_r \prec T.$$

Let $R_s(T)$ *be the number of integers belonging to* $Q_s(T)$, *then*

$$R_s(T)\geqq cT^{nk\{1-(1-\frac{1}{k})^l\}}$$

where $l=[s/n]$.

PROOF. There exists an integer θ in K such that

$$1, \theta, \theta^2, \cdots, \theta^{n-1}$$

are linearly independent over the rational field. If a is a sufficiently large positive rational integer, then $\theta+a$ is totally positive. Hence, we may assume that numbers mentioned above are all totally positive. Further we may assume that

$$1, \theta^k, \theta^{2k}, \cdots, \theta^{(n-1)k}$$

are totally positive and are linearly independent. Let Q be the set of integers which can be expressed as at most l sums of k-th powers of positive rational integers not exceeding T_0. It is well known (see [6], p. 63) that the number of integers in Q is greater than

$$c(l)T_0{}^{k\{1-(1-\frac{1}{k})^l\}}.$$

We put

$$\mu=u_1+u_2\theta^k+\cdots+u_n\theta^{(n-1)k},$$

letting u_r $(1\leqq r\leqq n)$ run through the set Q. Then we get (28) with

$$\sigma_r \prec cT_0, \quad s=ln.$$

Now the assertion follows by putting $cT_0=T$.

PROOF OF THE MAIN THEOREM.

Let ν be a totally positive integer in J_k. We write

$$P=\sqrt[n]{N(\nu)}.$$

Let ε_0 be a totally positive unit and $\nu_0=\nu\varepsilon_0{}^k$. By the theory of units (see [2], p. 124), we can choose ε_0 such that

$$c_1P<\nu_0{}^{(l)}<c_2P \qquad (1\leqq l\leqq r_1),$$
$$c_1P<|\nu_0{}^{(m)}|<c_2P \qquad (r_1+1\leqq m\leqq r_1+r_2), \tag{29}$$

for suitably chosen c_1 and c_2. We use

$$s_1=nk^2 \quad \text{and} \quad T_1=(c_1P/4s_1)^{1/k} \tag{30}$$

in the place of s and T in Lemma 17, and put

$$\rho=\nu_0-\mu_1-\mu_2, \quad \mu_1, \mu_2 \in Q_{s_1}(T_1).$$

Then, by (29) and (30),

$$\frac{c_1}{2} P<\rho^{(l)}<c_2 P,$$

$$\frac{c_1}{2} P<|\rho^{(m)}|<\left(c_2+\frac{c_1}{2}\right)P.$$

Let ε_1 be a totally positive unit and $\rho_0=\rho\varepsilon_1{}^k$. By the theory of units, for a given Δ $(0<\Delta<1)$, we can choose ε_1 such that

$$\frac{c_3}{\Delta^{2r_2}} P<\rho_0{}^{(l)}<\frac{c_4}{\Delta^{2r_2}} P,$$

$$|\rho_0{}^{(m)}|<c_4\Delta^{r_1}P, \tag{31}$$

for suitably chosen c_3 and c_4. It should be noticed that c_3 and c_4 can be taken independently of Δ.

We put

$$T=(c_4 P/\Delta^{2r_2})^{1/k}, \tag{32}$$

and define

$$L(\xi)=\sum_{\lambda<T} E(\lambda^k\xi), \quad V(\xi)=\sum_{\mu\in Q_{s_1}(T_1)} E(\mu\varepsilon_1{}^k\xi).$$

Further, we assume that

$$a=\frac{1}{4n}, \quad s\geqq 4n^2k+1 \tag{33}$$

and $\varepsilon_0\varepsilon_1=\varepsilon$. Hence, by Theorem 2,

$$\sum_{\gamma\in\Gamma}\int_{B_\gamma} L(\xi)^s V(\xi)^2 E(-\nu\varepsilon^k\xi)dx=\sum_{\rho_0}\sum_{\gamma\in\Gamma}\int_{B_\gamma} L(\xi)^s E(-\rho_0\xi)dx$$

$$=\sum_{\rho_0}(\mathfrak{S}(\rho_0)J(\mu_0)T^{n(s-k)}+O(T^{n(s-k)-a})), \tag{34}$$

where $\mu_0=T^{-k}\rho_0$. Consequently,

$$c_3/c_4<\mu_0{}^{(l)}<1,$$

$$|\mu_0{}^{(m)}|<\Delta^n, \tag{35}$$

by (31) and (32). By Lemma 12 and (35)

$$J(\mu_0)=D^{\frac{1}{2}(1-s)}\prod_{l=1}^{r_1} F(\mu^{(l)})\prod_{m=r_1+1}^{r_1+r_2} H(\mu^{(m)}),$$

with

$$F(\mu^{(l)})=\frac{\Gamma^s\left(1+\frac{1}{k}\right)}{\Gamma\left(\frac{s}{k}\right)}(\mu^{(l)})^{\frac{s}{k}-1}>c_5$$

and

$$H(\mu^{(m)})\to H(0)>c_6 \quad (\Delta\to 0).$$

Hence, if we take Δ sufficiently small, then

$$J(\mu_0)>c_7 .$$

It follows, from (33), (34) and Theorem 1, that

$$\Re\sum_{\gamma\in\Gamma}\int_{B_\gamma}L(\xi)^s V(\xi)^2 E(-\nu\varepsilon^k\xi)dx>c_8 T^{n(s-k)}R_{s_1}^2(T_1) \tag{36}$$

for $T>c_9$, if

$$s\geqq 4n^2k+1,\ [8nk(\log k+1)], \tag{37}$$

where $\Re$ means taking real part. In virtue of Theorem 3,

$$\int_S L(\xi)^s V(\xi)^2 E(-\nu\varepsilon^k\xi)dx=O(T^{ns-\frac{s}{2^k}})\int_U |V(\xi)|^2 dx$$

$$=O(T^{ns-\frac{s}{2^k}})\int_U \sum_{\mu_1,\mu_2\in Q_{s_1}(T_1)}^{U} E((\mu_1-\mu_2)\varepsilon_1{}^k\xi)dx$$

$$=O(T^{ns-\frac{s}{2^k}})R_{s_1}(T_1). \tag{38}$$

We can infer, from (36) and (38), that, if

$$R_{s_1}(T_1)>c_{10}T^{nk-\frac{s}{2^k}} \tag{39}$$

then

$$\Re\int_U L(\xi)^s V(\xi)^2 E(-\nu\varepsilon^k\xi)dx>0 ,$$

and this implies that there exist integers λ_r $(1\leqq r\leqq s)$, σ_q and τ_q $(1\leqq q\leqq s_1)$ such that

$$\nu\varepsilon^k=\lambda_1{}^k+\cdots+\lambda_s{}^k+\sigma_1{}^k+\cdots+\sigma_{s_1}^k+\tau_1{}^k+\cdots+\tau_{s_1}^k ,$$

with

$$N(\lambda_r)\leqq T^n\leqq c_{11}P^{n/k}=c_{11}N(\nu)^{1/k} ,$$

$$N(\sigma_q)\leqq T_1{}^n\leqq c_{12}P^{n/k}=c_{12}N(\nu)^{1/k} ,\quad N(\tau_q)\leqq c_{12}N(\nu)^{1/k} .$$

On account of (30), (32) and Lemma 17, we see that (39) is true, if

$$\frac{s}{2^k}>nk\left(1-\frac{1}{k}\right)^{k^2} \tag{40}$$

and $T>c_{13}$. If we put

$$s=[4n^2k+8nk\log k+4nk] ,$$

then the inequalities which we imposed on (37) and (40) are satisfied. Since $s+2s_1<8nk(n+k)$, we get the main theorem.

Gakushuin University.

Bibliography

[1] C. Chevalley, Sur la theorie du corps de classes dans les corps finis et les corps locaux, J. Fac. Sci. Univ., **2** (1933), 365–476.

[2] E. Hecke, Vorlesungen über die Theorie der algebraischen Zahlen, Leipzig, 1923.

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

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

[5] C. L. Siegel, Sums of m-th powers of algebraic integers, Ann. of Math., **46** (1945), 313–339.

[6] I. M. Vinogradov, The method of trigonometrial sums in the theory of numbers, 1947, translated from the Russian by K. F. Roth and Anne Davenport, London.