ON EXPONENTIAL SUMS OVER AN ALGEBRAIC NUMBER FIELD

LOO-KENG HUA

1. Introduction

LET K be an algebraic field of degree n over the rational field, and let $\mathfrak{d}$ be the ground ideal (differente) of the field. Let

$$f(x) = \alpha_k x^k + \ldots + \alpha_1 x + \alpha_0$$

be a polynomial of the kth degree with coefficients in the field K, and let $\mathfrak{a}$ be the fractional ideal generated by $\alpha_k, \ldots, \alpha_1$, that is, $\mathfrak{a} = (\alpha_k, \ldots, \alpha_1)$. Suppose $\mathfrak{a}\mathfrak{d} = \mathfrak{r}/\mathfrak{q}$, where $\mathfrak{r}$ and $\mathfrak{q}$ are two relatively prime integral ideals, and

$$S(f(x), \mathfrak{q}) = S(f(x)) = S(\mathfrak{q}) = \sum_{x \bmod \mathfrak{q}} e^{2\pi i \operatorname{tr}(f(x))},$$

where x runs over a complete residue system, mod $\mathfrak{q}$. It is the aim of the paper to prove the following:

THEOREM 1. *For any given* $\epsilon > 0$, *we have*

$$S(f(x), \mathfrak{q}) = O(N(\mathfrak{q})^{1-1/k+\epsilon})$$

where the constant implied by the symbol O depends only on k, n *and* ϵ.

As usual, we use $\operatorname{tr}(\alpha)$and $N(\mathfrak{q})$ to denote the trace of a number α and the norm of an ideal $\mathfrak{q}$ of K respectively.

This is a generalization of a theorem of the author's [1] over the rational field. The method used here is simpler and quite different from the original one.

1. A theorem on congruences

THEOREM 2. *Let* $\mathfrak{p}$ *be a prime ideal and let* $s(x)$ *be a polynomial with integral coefficients*, mod $\mathfrak{p}$. *Let* α *be a root of multiplicity* m *of the congruence*

$$s(x) \equiv 0 \pmod{\mathfrak{p}}.$$

Let λ *be an integer, divisible by* $\mathfrak{p}$ *but not by* $\mathfrak{p}^2$, *and let* u *be the greatest integer such that* $\mathfrak{p}^u$ *divides all the coefficients of* $s(\lambda x + \alpha) - s(\alpha)$. *Let*

$$t(x) \equiv \lambda^{-u}(s(\lambda x + \alpha) - s(\alpha)) \pmod{\mathfrak{p}}$$

be a polynomial with integral coefficients. Then $u \leqslant m$, *and the congruence*

$$t(x) \equiv 0 \pmod{\mathfrak{p}}$$

has at most m *solutions.*

Received September 14, 1949.

https://doi.org/10.4153/CJM-1951-006-4 Published online by Cambridge University Press

Proof. Without loss of generality, we may assume that $a = 0$. Then

$$s(x) = x^m s_1(x) + s_2(x),\ s_1(0) \not\equiv 0 \pmod{\mathfrak{p}}$$

where $s_2(x)$ is a polynomial of degree less than m and all its coefficients are divisible by $\mathfrak{p}$. Now we have

$$s(\lambda x) = \lambda^m x^m s_1(\lambda x) + s_2(\lambda x).$$

Since the coefficient of x^m is equal to $\lambda^m s_1(0)$ which is not divisible by $\mathfrak{p}^{m+1}$, we have $u \leqslant m$.

Since $\lambda^{-u} s(\lambda x)$ is congruent to a polynomial of degree not exceeding m, mod $\mathfrak{p}$, the theorem follows.

Remark. u is independent of the choice of λ. In fact, let λ' be another integer having the same property, then we have an integer τ such that

$$\lambda \equiv \lambda' \tau \pmod{\mathfrak{p}^{u+1}},\ \mathfrak{p} \nmid \tau.$$

Then

$$s(\lambda x + a) - s(a) \equiv s(\lambda'(\tau x) + a) - s(a) \qquad \pmod{\mathfrak{p}^{u+1}}$$

3. Several lemmas concerning algebraic numbers

Let $\mathfrak{g}$ be an ideal, fractional or integral, and $\mathfrak{a}$ be an integral ideal. It is clear that $\mathfrak{g} \mid \mathfrak{g}\mathfrak{a}$.

Now we divide the elements of $\mathfrak{g}$ into residue classes according to the modulus $\mathfrak{g}\mathfrak{a}$. The number of different classes is known to be $N(\mathfrak{a})$. We take an element from each class; the set so formed is called a complete residue system of $\mathfrak{g}$, mod $\mathfrak{g}\mathfrak{a}$.

The definition of the ground ideal $\mathfrak{d}$ can be stated in the following way:

$$\mathfrak{d}^{-1} \text{ is the aggregate of all numbers } \xi \text{ of } K$$

such that

$$e^{2\pi i \operatorname{tr}(\xi a)} = 1$$

for all integers a of K. Consequently, if β belongs to $(\mathfrak{q}\mathfrak{d})^{-1}$ and $a_1 \equiv a_2 \pmod{\mathfrak{q}}$, then

$$e^{2\pi i \operatorname{tr}(\beta a_1)} = e^{2\pi i \operatorname{tr}(\beta a_2)}.$$

This asserts that the sum $S(f(x), \mathfrak{q})$, which was defined at the beginning of the paper, is independent of the choice of the residue system, mod $\mathfrak{q}$.

THEOREM 3. *Let $\mathfrak{q}$ be an integral ideal. As ξ runs over a complete residue system of* $(\mathfrak{q}\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$, *we have, for integral a,*

$$\sum_{\xi} e^{2\pi i \operatorname{tr}(\xi a)} = \begin{cases} N(\mathfrak{q}) & \text{if } \mathfrak{q} \mid a, \\ 0 & \text{if } \mathfrak{q} \nmid a. \end{cases}$$

Proof. If $\mathfrak{q} \mid a$, then ξa belongs to $\mathfrak{d}^{-1}$. Then $e^{2\pi i \operatorname{tr}(\xi a)} = 1$ for all ξ. Hence, we have the first conclusion.

https://doi.org/10.4153/CJM-1951-006-4 Published online by Cambridge University Press

If $\mathfrak{q} \nmid \mathfrak{a}$, there is an element ξ_0, which belongs to $(\mathfrak{d}\mathfrak{q})^{-1}$, but $\xi_0 \alpha$ does not belong to $\mathfrak{d}^{-1}$. In fact, if for all ξ_0 belonging to $(\mathfrak{d}\mathfrak{q})^{-1}$ we have $\xi_0 \alpha$ belonging to $\mathfrak{d}^{-1}$, then we have

$$\mathfrak{d}^{-1} \mid \alpha(\mathfrak{d}\mathfrak{q})^{-1}.$$

Consequently $\mathfrak{q} \mid \alpha$. This is impossible. By the definition of $\mathfrak{d}^{-1}$ there is an integer γ such that

$$e^{2\pi i \operatorname{tr}(\gamma \xi_0 \alpha)} \neq 1.$$

Since $\gamma \xi_0$ belongs to $(\mathfrak{d}\mathfrak{q})^{-1}$, we can write $\gamma \xi_0 = \xi_1$. Then

$$\sum_{\xi} e^{2\pi i \operatorname{tr}(\xi \alpha)} = \sum_{\xi} e^{2\pi i \operatorname{tr}((\xi + \xi_1)\alpha)} = e^{2\pi i \operatorname{tr}(\xi_1 \alpha)} \cdot \sum_{\xi} e^{2\pi i \operatorname{tr}(\xi \alpha)}.$$

Thus we have the second conclusion of our theorem.

4. Proof of the theorem for $\mathfrak{q} = \mathfrak{p}$

In case $\mathfrak{q}$ is a prime ideal $\mathfrak{p}$, the exponential sum considered here reduces to a type of exponential sum over a finite field which has been discussed before [2]. But the author could not find an easy way to establish an explicit relationship between the exponential sums considered here and those over a finite field. Also, for the sake of completeness, the following proof is included here. The method is an adaptation of one due to Mordell [3].

THEOREM 4. *We have*

$$|S(f(x), \mathfrak{p})| \leqslant k^n N(\mathfrak{p})^{1-1/k}.$$

Proof. Without loss of generality, we may assume that α_k does not belong to $\mathfrak{d}^{-1}$, for otherwise

$$S(f(x), \mathfrak{p}) = S(f(x) - \alpha_k x^k, \mathfrak{p}),$$

since $e^{2\pi i \operatorname{tr}(\alpha_k x^k)} = 1$ for all integral x. Thus we now assume that α_k belongs to $(\mathfrak{p}\mathfrak{d})^{-1}$ but not to $\mathfrak{d}^{-1}$. The theorem is trivial for $N(\mathfrak{p}) \leqslant k^n$, since

$$|S(f(x), \mathfrak{p})| \leqslant N(\mathfrak{p}) \leqslant k^n N(\mathfrak{p})^{1-1/k}.$$

Now we assume $N(\mathfrak{p}) > k^n$ and consequently $\mathfrak{p} \nmid k!$ We have

$$|S(f(x))|^{2k} = \frac{1}{N(\mathfrak{p})(N(\mathfrak{p}) - 1)} \sum_{\lambda \bmod \mathfrak{p}}' \sum_{\mu \bmod \mathfrak{p}} |S(f(\lambda x + \mu))|^{2k},$$

where λ runs over a reduced residue system, mod $\mathfrak{p}$. Write

$$f(\lambda x + \mu) = \beta_k x^k + \ldots + \beta_0,$$

where

$$\beta_k \equiv \alpha_k \lambda^k \pmod{\mathfrak{d}^{-1}}, \tag{1}$$

$$\beta_{k-1} \equiv k\alpha_k \lambda^{k-1} + \alpha_{k-1}\lambda^{k-1} \pmod{\mathfrak{d}^{-1}}, \tag{2}$$

and so on.

For fixed $\beta_k, \beta_{k-1}, \ldots$ belonging to $(\mathfrak{p}\mathfrak{d})^{-1}$, the number of integers λ and μ does not exceed k. In fact, (1) asserts that $\beta_k - \alpha_k\lambda^k$ belongs to $\mathfrak{d}^{-1}$. (β_k and α_k belong to $(\mathfrak{p}\mathfrak{d})^{-1}$.) There is an integer τ belonging to $\mathfrak{p}\mathfrak{d}$ but not to $\mathfrak{p}$. Consequently $\tau\alpha_k$ and $\tau\beta_k$ are integers and $\mathfrak{p} \nmid \tau\alpha_k$; the congruence $\tau\beta_k \equiv \tau\alpha_k\lambda^k$ (mod $\mathfrak{p}$) has evidently at most k solutions. For a fixed λ, the same argument proves that μ is uniquely determined by (2), since $\mathfrak{p} \nmid k$.

Therefore, we have

$$\left| S(f(x), \mathfrak{p}) \right|^{2k} \leqslant \frac{k}{N(\mathfrak{p})\ (N(\mathfrak{p}) - 1)} \sum_{\beta_k} \cdots \sum_{\beta_1} \left| S(\beta_k x^k + \ldots + \beta_1 x) \right|^{2k},$$

where each β runs over a complete residue system of $(\mathfrak{p}\mathfrak{d})^{-1}$, mod $\mathfrak{d}^{-1}$.

We have

$$\sum_{\beta_k} \cdots \sum_{\beta_1} \left| S(\beta_k x^k + \ldots + \beta_1 x) \right|^{2k} = \sum_{\beta_k} \cdots \sum_{\beta_1} \sum_{x_1} \cdots \sum_{x_k} \sum_{y_1} \cdots \sum_{y_k} e^{2\pi i \operatorname{tr}(\psi)}$$
$$= N(\mathfrak{p})^k M,$$

where

$$\psi = \beta_k(x_1^k + \ldots + x_k^k - y_1^k - \ldots - y_k^k) + \beta_{k-1}(x_1^{k-1} + \ldots + x_k^{k-1} - y_1^{k-1} - \ldots - y_k^{k-1}) + \ldots + \beta_1(x_1 + \ldots + x_k - y_1 - \ldots - y_k),$$

and, by Theorem 3, M is equal to the number of solutions of the system of congruences

$$x_1^h + \ldots + x_k^h \equiv y_1^h + \ldots + y_k^h, \text{ mod } \mathfrak{p}, \qquad 1 \leqslant h \leqslant k.$$

By a theorem on symmetric functions, we deduce immediately

$$(X - x_1) \ldots (X - x_k) \equiv (X - y_1) \ldots (X - y_k), \text{ mod } \mathfrak{p},$$

since $\mathfrak{p} \nmid k!$ Then we have that $x_1, \ldots, x_k$ are a permutation of $y_1, \ldots, y_k$ and then

$$M \leqslant k! N(\mathfrak{p})^k.$$

Consequently, we have

$$\left| S(f(x), \mathfrak{p}) \right|^{2k} \leqslant \frac{k \cdot k!}{N(\mathfrak{p})(N(\mathfrak{p}) - 1)} N(\mathfrak{p})^{2k}$$
$$\leqslant 2k \cdot k! N(\mathfrak{p})^{2k-2}$$
$$\leqslant k^{2k} N(\mathfrak{p})^{2k-2}$$

and the theorem follows.

5. Proof of the theorem for $\mathfrak{q} = \mathfrak{p}^l$

THEOREM 5. *If $\mathfrak{q} = \mathfrak{p}^l$, and $\mathfrak{p}$ is a prime ideal, then*

(1) $$|S(f(x), \mathfrak{p}^l)| \leqslant k^{2n+1} N(\mathfrak{p}^l)^{1-1/k}.$$

https://doi.org/10.4153/CJM-1951-006-4 Published online by Cambridge University Press

Proof. Let

$$\mathfrak{b} = (k\alpha_k, (k-1)\alpha_{k-1}, \ldots, 2\alpha_2, \alpha_1).$$

Evidently $\mathfrak{a} \mid \mathfrak{b}$. Let t be the highest exponent of $\mathfrak{p}$ dividing $\mathfrak{b}\mathfrak{a}^{-1}$. Let m be the number of solutions, multiplicities being counted, of the congruence

$$f'(x) \equiv 0 \pmod{\mathfrak{p}^{t+1-l}} \tag{2}$$

as x runs over a complete residue system, mod $\mathfrak{p}$. (We have $m \leqslant k-1$.)

Evidently, (1) is a conseqeunce of the sharper result

$$|S(f(x), \mathfrak{p}^l)| \leqslant k^{2n} \max(1, m)\, N(\mathfrak{p}^l)^{1-1/k}. \tag{3}$$

If $t \geqslant 1$, then $\mathfrak{p}^t$ divides at least one of the integers $k, k-1, \ldots, 1$. Then

$$N(\mathfrak{p}^t) \leqslant k^n,$$

that is

$$N(\mathfrak{p}) \leqslant k^{n/t}. \tag{4}$$

Suppose that $l < 2(t+1)$. For $t = 0$, we have $l = 1$ and (3) follows from Theorem 4. If $t \geqslant 1$, then, by (4)

$$\begin{aligned} |S(f(x), \mathfrak{p}^l)| &\leqslant N(\mathfrak{p})^l \leqslant (N(\mathfrak{p}))^{l(1-1/k)}\ (N(\mathfrak{p}))^{(2t+1)/k} \\ &\leqslant N(\mathfrak{p})^{l(1-1/k)}\ k^{n(2+1/t)/k} \\ &\leqslant k^{2n} \cdot N(\mathfrak{p})^{l(1-1/k)}. \end{aligned}$$

Therefore (3) is true for $l \leqslant 2t+1$. Now we assume that $l \geqslant 2(t+1)$ and that (3) is true for smaller l.

Let $\mu_1, \ldots, \mu_r$ be the distinct roots of (2) with multiplicities $m_1, \ldots, m_r$ respectively. Then $m_1 + \ldots + m_r = m$. Evidently

$$S(f(x)) = \sum_x e^{2\pi i \operatorname{tr}(f(x))} = \sum_\nu \sum_{\substack{x \\ x \equiv \nu \pmod{\mathfrak{p}}}} e^{2\pi i \operatorname{tr}(f(x))} = \sum_\nu S_\nu$$

say, where ν runs over a complete residue system, mod $\mathfrak{p}$. If ν is not one of the μ's then, letting

$$x = y + \lambda^{l-t-1} z,$$

where λ is an integer belonging to $\mathfrak{p}$ but not to $\mathfrak{p}^2$, we have

$$\begin{aligned} S_\nu &= \sum_{\substack{y \bmod \mathfrak{p}^{l-t-1} \\ y \equiv \nu \pmod{\mathfrak{p}}}} \sum_{z \bmod \mathfrak{p}^{t+1}} e^{2\pi i \operatorname{tr}(f(y) + \lambda^{l-t-1} z f'(y))} \\ &= \sum e^{2\pi i \operatorname{tr}(f(y))} \sum_{z \bmod \mathfrak{p}^{t+1}} e^{2\pi i \operatorname{tr}(\lambda^{l-t-1} z f'(y))} \\ &= 0 \end{aligned}$$

by Theorem 3, since $\mathfrak{p}^{t+1-l} \nmid f'(y)$.

Therefore

$$| S(f(x)) | \leqslant \sum_{s=1}^{r} \left| \sum_{x \bmod \mathfrak{p}^{l-1}} e^{2\pi i \operatorname{tr}(f(\mu_s + \lambda y))} \right|$$

$$= \sum_{s=1}^{r} \left| \sum_{x \bmod \mathfrak{p}^{l-1}} e^{2\pi i \operatorname{tr}(f(\mu_s + \lambda y) - f(\mu_s))} \right|$$

$$(5) \qquad = \sum_{s=1}^{r} N(\mathfrak{p})^{\sigma_s - 1} S(f(\mu_s + \lambda y) - f(\mu_s), \mathfrak{p}^{l-\sigma_s}),$$

where σ_s is defined in the following way: Let $\mathfrak{c}$ be the ideal generated by the coefficients of

$$f_s(y) = f(\mu_s + y) - f(\mu_s).$$

Evidently $\mathfrak{a}$ divides $\mathfrak{c}$, and σ_s is the highest power of $\mathfrak{p}$ dividing $\mathfrak{c}\mathfrak{a}^{-1}$. Also, if $l \leqslant \sigma_s$, we use the conventional meaning

$$S(f(\mu_s + y) - f(\mu_s), \mathfrak{p}^{l-\sigma_s}) = \mathfrak{p}^{l-\sigma_s}.$$

Now we are going to prove that

$$(6) \qquad 1 \leqslant \sigma_s \leqslant k.$$

If (6) is not true, then $\mathfrak{p}^{-l+k+1}$ divides all the coefficients of $f(\sigma_s + y) - f(\sigma_s)$; that is

$$\mathfrak{p}^{-l+k+1} \,\Big|\, \frac{f^{(r)}(\mu_s)}{r!} \lambda^r, \qquad 1 \leqslant r \leqslant k.$$

Consequently

$$\mathfrak{p}^{-l+1} \,\Big|\, \frac{f^{(r)}(\mu_s)}{r!},$$

which is equal to α_r plus a linear combination of $\alpha_k, \ldots, \alpha_{r-1}$ with integral coefficients. Thus we deduce successively $\mathfrak{p}^{-l+1}|\alpha_k$, $\mathfrak{p}^{-l+1}|\alpha_{k-1}, \ldots, \mathfrak{p}^{-l+1}|\alpha_1$. This contradicts $\mathfrak{q} = \mathfrak{p}^l$.

From (5) and (6), we have, for $l \geqslant \max(\sigma_1, \ldots, \sigma_r)$,

$$| S(f(x), \mathfrak{p}^l) | \leqslant \sum_{s=1}^{r} N(\mathfrak{p})^{\sigma_s(1-1/k)} \, | S(f_s(y), \mathfrak{p}^{l-\sigma_s})|.$$

By the hypothesis of induction, we have

$$| S(f(x), \mathfrak{p}^l)| \leqslant k^{2n} \sum_{s=1}^{r} N(\mathfrak{p})^{\sigma_s(1-1/k)} m_s N(\mathfrak{p})^{(l-\sigma_s)(1-1/k)}$$

$$= k^{2n} \, m \, N(\mathfrak{p})^{l(1-1/k)}.$$

In case $l \leqslant \max(\sigma_1, \ldots, \sigma_r)$, we have $l \leqslant k$ and, by (5)

$$| S(f(x)) | \leqslant r \, \mathfrak{p}^{l-1} \leqslant m \, \mathfrak{p}^{l(1-1/k)}.$$

We have (3) and consequently (1). (Notice that if $\sum_{s=1}^{r} m_s = 0$, the method shows that $S(f(x)) = 0$, if $l \geqslant 2(t+1)$.)

THEOREM 6. *If* $(\mathfrak{q}_1, \mathfrak{q}_2) = 1$ *and* $f(0) = 0$, *then there are polynomials* $f_1(x)$ *and* $f_2(x)$ *each of degree* k *such that*

$$S(f(x), \mathfrak{q}_1\mathfrak{q}_2) = S(f_1(x), \mathfrak{q}_1)\ S(f_2(x), \mathfrak{q}_2).$$

Proof. We can find two integers λ_1 and λ_2 such that

$$(\lambda_1, \mathfrak{q}_1\mathfrak{q}_2) = \mathfrak{q}_2, \quad (\lambda_2, \mathfrak{q}_1\mathfrak{q}_2) = \mathfrak{q}_1.$$

Putting

$$x = \lambda_1 y_2 + \lambda_2 y_1,$$

then, as y_1 and y_2 run over complete residue systems mod $\mathfrak{q}_1$ and mod $\mathfrak{q}_2$ respectively, x runs over a complete residue system, mod $\mathfrak{q}_1\mathfrak{q}_2$. Then

$$\begin{aligned} S(f(x), \mathfrak{q}_1\mathfrak{q}_2) &= \sum_{y_1 \bmod \mathfrak{q}_1} \sum_{y_2 \bmod \mathfrak{q}_2} e^{2\pi i \operatorname{tr}(f(\lambda_1 y_2 + \lambda_2 y_1))} \\ &= \sum_{y_1 \bmod \mathfrak{q}_1} e^{2\pi i \operatorname{tr}(f(\lambda_2 y_1))} \sum_{y_2 \bmod \mathfrak{q}_2} e^{2\pi i \operatorname{tr}(f(\lambda_1 y_2))} \\ &= S(f_1(x), \mathfrak{q}_1))\ S(f_2(x), \mathfrak{q}_2)\ , \end{aligned}$$

where $f_1(x) = f(\lambda_2 x)$ and $f_2(x) = f(\lambda_1 x)$. Now we have to verify that the ideal generated by the coefficients of $f_1(x)$ can be expressed as $\mathfrak{r}(\mathfrak{d}\mathfrak{q}_1)^{-1}$, where $\mathfrak{r}$, $\mathfrak{q}$ are relatively prime integral ideals, but this is quite evident.

6. Proof of Theorem 1

Let
$$\mathfrak{q} = \mathfrak{p}_1^{l_1} \ldots \mathfrak{p}_s^{l_s}.$$

Then we have, by repeated application of Theorem 6,

$$S(f(x), \mathfrak{q}) = \prod_{i=1}^{s} S(f_i(x), \mathfrak{p}_i^{l_i})\ .$$

By Theorem 5, we have

$$\begin{aligned} |\ S(f(x), \mathfrak{q})\ | &\leqslant \sum_{i=1}^{s} k^{2n+1} N(\mathfrak{p}_i^{l_i})^{1-1/k} \\ &\leqslant \sum_{i=1}^{s} (1 + l_i)^{(2n+1)\log k/\log 2} N(\mathfrak{p}_i^{l_i})^{(1-1/k)} \\ &= d(\mathfrak{q})^{(2n+1)\log k/\log 2} N(\mathfrak{q})^{1-1/k} \\ &= O(N(\mathfrak{q})^{1-1/k+\epsilon}) \end{aligned}$$

where $d(\mathfrak{q})$ denotes the number of divisors of $\mathfrak{q}$.

Remarks. The previous method is practically an algorithm; more precisely, for a given polynomial, if we know the value of $S(f(x), \mathfrak{p}^l)$, $l \leqslant 2t + 1$, then we can find the value of $S(f(x), \mathfrak{p}^l)$.

References

[1] L. K. Hua, *On an exponential sum*, Jour. of Chinese Math. Soc., vol. 2 (1940), 301-312.
[2] L. K. Hua and S. H. Min, *On a double exponential sum*, Acad. Sinica Sci. Record, vol. 1 (1942), 23-25.
[3] L. J. Mordell, *On a sum analogous to a Gauss's sum*, Quart. J. Math. (Oxford), vol. 3 (1932), 161-167.

Tsing Hua University,
Peking, China