ACTA ARITHMETICA
LIII (1990)

Эффективная нижняя граница для линейной формы с алгебраическими коэффициентами в архимедовых и неархимедовых метриках одновременно

С. В. Котов (Минск)

Светлой памяти моего учителя
В. Г. Спринджука посвящается

Пусть $\omega_1 = 1, \omega_2, \dots, \omega_l$ ($l \geqslant 2$) алгебраические числа, линейно независимые над полем рациональных чисел $\boldsymbol{Q}$, поле $\boldsymbol{K} = \boldsymbol{Q}(\omega_2, \dots, \omega_l)$ и $[\boldsymbol{K}:\boldsymbol{Q}] = n$. Из обобщения известной теоремы Лиувилля [1] следует существование такой эффективно вычисляемой константы $c_1 = c_1(\omega_2, \dots, \omega_l)$, что для всех $x_1, \dots, x_l \in \boldsymbol{Z}\setminus\{0\}$ ($\boldsymbol{Z}$ — кольцо целых рациональных чисел) выполняется неравенство

$$|x_1 + \omega_2 x_2 + \dots + \omega_l x_l| > c_1 X^{-(n-\tau)/\tau}, \tag{1}$$

где $X = \max\limits_{(i)} |x_i|$ ($1 \leqslant i \leqslant l$) и $\tau = 1$ или 2 в случае действительного или комплексного $\boldsymbol{K}$ соответственно. Теорема Туэ–Зигеля–Рота–Шмидта (см., например, [2], [3], [4] и [5], [6]) дает усиление (1): показатель степени в правой части (1) можно заменить на $\varkappa > (l-\tau)/\tau$, а c_1 на $c_2 = c_2(\varkappa, \omega_2, \dots, \omega_l)$. В работах Шмидта [7], [8] данная теорема обобщается для произведения линейных форм $\mu = x_1 + \omega_2 x_2 + \dots + \omega_l x_l$, а Дюбуа, Рен [9], [10] и Шликкевай [11], [12] дали p-адическое обобщение этих результатов [1].

В силу логики доказательств перечисленные результаты неэффективны, они скрывают истинное влияние величины c_2. Первые эффективные усиления показателя степени в неравенстве (1) были получены для алгебраических чисел $\omega_2, \dots, \omega_l$ специального вида в работах Бейкера [17], [18], Фельдмана [19], [20], Озгуда [21], Спринджука [22] и Чудновского [23]. Эффективный анализ уравнений Туэ и Туэ–Малера позволил в случае $l = 2$ добиться продвижения в эффективном усилении и p-адическом

[1] Мы не касаемся обзора различных усилений и обобщений неравенства Лиувилля для $l = 2$. Заинтересованный читатель может ознакомится с этим, например, в [13], [14], [15], [16].

обобщении неравенства Лиувилля. Здесь следует отметить результаты Бейкера [24], Коутеса [25], Спринджука [26], Фельдмана [27], Спринджука и автора настоящей статьи [28].

Позднее Дьёри и его ученики провели обширные исследования в области эффективного анализа диофантовых уравнений норменного вида. Это позволило получить эффективное степенное усиление неравенства (1) для широких классов алгебраических чисел $\omega_2, \dots, \omega_l$ при $l \geqslant 2$. Мы выделяем здесь работу Дьёри и Паппа [29], а также недавние статьи Гаала [30].

В [31] автор анонсировал результат (теорема 2) об эффективных приближениях линейной формы $\mu = x_1 + \omega_2 x_2 + \dots + \omega_l x_l$ ($l \geqslant 2$) с алгебраическими $\omega_2, \dots, \omega_l$ из достаточно широкого класса и алгебраическими $x_1, \dots, x_l$, как в архимедовых, так и в неархимедовых метриках одновременно. Аналогичный результат получил Дьёри [32] подходом, отличным от нашего.

В данной статье мы излагаем подробное доказательство теоремы 2 из [31], развивая рассуждения работы [28] (см. доказательство теоремы 3).

Пусть $\boldsymbol{F}$ — поле алгебраических чисел степени d над полем $\boldsymbol{Q}$, $\boldsymbol{Z_F}$ — его кольцо целых чисел, $\boldsymbol{K}$ — конечное расширение поля $\boldsymbol{F}$ степени $[\boldsymbol{K}:\boldsymbol{F}] = n$; числа $\omega_1 = 1, \omega_2, \dots, \omega_l$ ($l \geqslant 2$) принадлежат $\boldsymbol{K}$, линейно независимы над $\boldsymbol{F}$ и $\mu = x_1 + \omega_2 x_2 + \dots + \omega_l x_l$ — линейная форма от переменных $x_1, \dots, x_l \in \boldsymbol{Z_F}$, причем $m = [\omega_l : \boldsymbol{F}(\omega_2, \dots, \omega_{l-1})] \geqslant 3$. Пусть, далее, r_1 — число вещественных и r_2 — число комплексных изоморфизмов поля $\boldsymbol{K}$ в поле комплексных чисел ($r_1 + 2r_2 = dn$); $\boldsymbol{\Omega}$ — множество всех нормирований $|\dots|_v$ поля $\boldsymbol{K}$, где v — одно из натуральных чисел $1, 2, \dots, r_1 + r_2$ (архимедовы нормирования) или простой идеал поля $\boldsymbol{K}$ (неархимедовы нормирования); для $\alpha \in \boldsymbol{K}$ положим $\|\alpha\|_v = |\alpha|_v^{n_v}$, где $n_v = [\boldsymbol{K}_v : \boldsymbol{Q}_v]$; $\boldsymbol{S}$ — конечное подмножество $\boldsymbol{\Omega}$; $S = \{\mathfrak{P}_1, \dots, \mathfrak{P}_s\}$ — набор различных простых идеалов из $\boldsymbol{F}$, которым соответствуют неархимедовы нормирования поля $\boldsymbol{F}$, индуцированные неархимедовыми нормированиями поля $\boldsymbol{K}$ из $\boldsymbol{S}$; $\boldsymbol{\Gamma} = \{\gamma : \gamma$ — S-единица, $\operatorname{ord}_{\mathfrak{P}_j}\gamma \leqslant 0$ $(1 \leqslant j \leqslant s)\}$ (2).

Теорема. *Для каждого набора $x_1, \dots, x_l \neq 0$ из $\boldsymbol{Z_F}$ существует такая S-единица $\gamma \in \boldsymbol{\Gamma}$, что*

$$\prod_{v \in \boldsymbol{S}} \|\gamma\mu\|_v > c_3 X^{c_4 - dn + r_1' + 2r_2'}, \tag{2}$$

где $X = \max_{(i)} \overline{|\gamma x_i|}$ (3) $(1 \leqslant i \leqslant l)$, r_1' и r_2' — число вещественных и комплексных изоморфизмов поля $\boldsymbol{K}$ в $\boldsymbol{S}$ соответственно, величины $c_3 > 0$, $0 < c_4 < 1$ зависят только от поля $\boldsymbol{F}$, чисел $\omega_2, \dots, \omega_l$, множества $\boldsymbol{S}$ и эффективно определяются.

(2) S-единица определяется по аналогии с T-единицей из [33] (см. стр. 30).

(3) Через $\overline{|\alpha|}$ обозначаем максимум абсолютных величин, сопряженных с алгебраическим α.

Для доказательства теоремы мы существенно используем следующую ниже лемму. Прежде чем её сформулировать, рассмотрим норменное диофантово уравнение

$$\operatorname{Nm}_{\boldsymbol{K}/\boldsymbol{F}}(\mu) = \sigma \varrho \varrho_1^{z_1} \dots \varrho_s^{z_s} \tag{3}$$

относительно неизвестных $x_1, \dots, x_l \in \boldsymbol{Z_F}$, $(x_1, \dots, x_l) | a \in \boldsymbol{Z_F}$ и целых рациональных $z_1 \geqslant 0, \dots, z_s \geqslant 0$, где σ — неизвестная единица из поля $\boldsymbol{F}$, ϱ, $\varrho_1, \dots, \varrho_s \in \boldsymbol{Z_F}$, причем (ϱ_j) — степени простых идеалов $\mathfrak{P}_j$ $(1 \leqslant j \leqslant s)$.

Лемма. *Для каждого целочисленного решения $x_1, \dots, x_l \neq 0, z_1, \dots, z_s$ уравнения* (3) *существует такая единица $\varepsilon \in \boldsymbol{F}$, что справедлива оценка*

$$\max\left(\overline{|\varepsilon x_1|}, \dots, \overline{|\varepsilon x_l|}\right) \leqslant c_5 \left(|\operatorname{Nm}(\varrho)|\right)^{c_6},$$

где $c_5 > 0$, $c_6 > 0$ имеют тот же смысл, что и c_3.

В случае $m \geqslant 5$ лемма является фактически теоремой 1 из [31]. Если же дополнить эту теорему соображениями, которые приведены в [34] (см. стр. 18), то можно заменить 5 на 3. Для $m \geqslant 3$ эта лемма доказана независимо в [36], теорема 4.

Переходим непосредственно к доказательству исходной теоремы.

Пусть

$$\left(\operatorname{Nm}_{\boldsymbol{K}/\boldsymbol{F}}(\mu)\right) = \mathfrak{a}\mathfrak{P}_1^{v_1} \dots \mathfrak{P}_s^{v_s}, \tag{4}$$

где идеалы $\mathfrak{a} \subset \boldsymbol{Z_F}$, $\mathfrak{P}_1, \dots, \mathfrak{P}_s \in S$ и $(\mathfrak{a}, \mathfrak{P}_1 \dots \mathfrak{P}_s) = 1$. Полагаем $v_j = hz_j' + z_j''$, где h — число классов идеалов поля $\boldsymbol{F}$, $(\varrho_j) = \mathfrak{P}_j^h$ $(1 \leqslant j \leqslant s)$, $(\varrho) = \mathfrak{a}\mathfrak{P}_1^{z_1''} \dots \mathfrak{P}_s^{z_s''}$. Очевидно, что $\operatorname{ord}_{\mathfrak{P}_j}(\varrho) < h$ $(1 \leqslant j \leqslant s)$. Переходим в (4) от идеалов к числам

$$\operatorname{Nm}_{\boldsymbol{K}/\boldsymbol{F}}(\mu) = \sigma \varrho \varrho_1^{z_1'} \dots \varrho_s^{z_s'}. \tag{5}$$

Допустим вначале, что $(x_1, \dots, x_l)$ — главный идеал. Если $\mathfrak{P}_j^{u_j} \| (x_1, \dots, x_l)$, то полагая $u_j = hu_j' + u_j''$ $(1 \leqslant j \leqslant s)$, $\lambda = \varrho_1^{u_1'} \dots \varrho_s^{u_s'}$, $x_i' = \lambda^{-1} x_i$ $(1 \leqslant i \leqslant l)$ и $\mu' = \lambda^{-1}\mu$, из (5) получаем

$$\operatorname{Nm}_{\boldsymbol{K}/\boldsymbol{F}}(\mu') = \sigma \varrho \varrho_1^{z_1'} \dots \varrho_s^{z_s'} \tag{6}$$

и $\operatorname{ord}_{\mathfrak{P}_j}(x_1', \dots, x_l') < h$ $(1 \leqslant j \leqslant s)$. К уравнению (6) применим лемму. Тогда для каждого его решения $x_1', \dots, x_l' \neq 0$ существует единица $\varepsilon \in \boldsymbol{F}$, что имеет место оценка

$$X = \max_{(i)} \left(\overline{|\gamma x_i|}\right) = \max_{(i)} \left(\overline{|\varepsilon x_i'|}\right) < c_7 \left(|\operatorname{Nm}(\varrho)|\right)^{c_8} \quad (1 \leqslant i \leqslant l), \tag{7}$$

где $\gamma = \varepsilon\lambda^{-1} \in \boldsymbol{\Gamma}$, величины c_7 и c_8 (в дальнейшем $c_9, \dots, c_{12}$ аналогично) имеют смысл c_3.

Для простых идеалов $\mathfrak{p} \in \boldsymbol{K}$ получаем

(8) $$\prod_{\mathfrak{p}\nmid\mathfrak{P}_1\dots\mathfrak{P}_s} \|\varepsilon\mu'\|_{\mathfrak{p}} = \prod_{\substack{\mathfrak{p}\mid(\varrho)\\ \mathfrak{p}\nmid\mathfrak{P}_1\dots\mathfrak{P}_s}} = \|\varrho\|_{\mathfrak{p}}.$$

Из „формулы произведения" [35] (см. стр. 92)

$$\prod_{v\in\Omega} \|\varrho\|_v = |\mathrm{Nm}(\varrho)| \prod_{v\in\Omega^*} \|\varrho\|_v = 1,$$

где Ω^* — все неархимедовы нормирования в Ω, и соотношений (7), (8) следует

(9) $$\prod_{v\in\Omega^*\setminus S^*} \|\gamma\mu\|_v < c_9 (|\mathrm{Nm}(\varrho)|)^{-1} < c_{10} X^{-c_{11}},$$

S^* — все неархимедовы нормирования в S, $c_{10} = c_7^{c_{11}} \cdot c_9$, $c_{11} = 1/c_8$. Обращаясь вновь к „формуле произведения", из (9) выводим

(10) $$1 = |\mathrm{Nm}(\gamma\mu)| \prod_{v\in S^*} \|\gamma\mu\|_v \prod_{v\in\Omega^*\setminus S^*} \|\gamma\mu\|_v$$
$$< c_{10} X^{-c_{11}} |\mathrm{Nm}(\gamma\mu)| \prod_{v\in S^*} \|\gamma\mu\|_v.$$

Так как $\overline{|\gamma\mu|} \leqslant c_{12} X$ то из (10) вытекает

$$1 \leqslant c_{10} c_{12}^{dn} X^{dn - r_1' - 2r_2' - c_{11}} \prod_{v\in S} \|\gamma\mu\|_v,$$

откуда следует (2).

Допустим теперь, что $(x_1, \dots, x_l)$ не является главным идеалом. Погружаем поле K в его абсолютное поле классов $\tilde{K}$ и анализируем в нем уравнение (6). Переход от нормирований w поля $\tilde{K}$ к нормированиям v поля K осуществляем по формуле

$$\prod_{w\mid v} \|\alpha\|_w = |\mathrm{Nm}_{\tilde{K}/K}(\alpha)|_v$$

для $0 \neq \alpha \in \tilde{K}$ [35] (см. стр. 47). Величины c_5 и c_6 в лемме сохранят свой смысл, поскольку относительная степень $[\tilde{K}:K] = h_K$ — числу классов идеалов поля K, а относительный дискриминант $D_{\tilde{K}/K}$ равен единице.

Из теоремы можно вывести

Следствие. *Пусть $F = Q$, μ удовлетворяет условиям теоремы, причем $(x_1, \dots, x_l) = 1$, $T = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ — конечный набор различных простых идеалов поля K. Имеет место оценка*

(11) $$|\mu|^{\tau} \prod_{j=1}^{t} |\mu|_{\mathfrak{p}_j}^{n_{\mathfrak{p}_j}} > c_{13} X^{c_{14} - n + \tau},$$

где $X = \max_{(i)} (|x_i|) (1 \leqslant i \leqslant l)$, $\tau = 1$ или 2 в случае действительного или комплексного K соответственно, величины $c_{13} > 0$, $0 < c_{14} < 1$ зависят лишь от $\omega_2, \dots, \omega_l$, T и эффективно определяются.

Наконец заметим, что если $\omega_1 \neq 1$, $\omega_2, \dots, \omega_l$ линейно независимы над F, то наши рассуждения остаются в силе и оценки (2) и (11) сохраняют свой вид.

Литература

[1] J. Liouville, *Sur des classes très étendues de quantités dont la valeur n'est ni algébrique, ni meme réductible à des irrationnelles algébriques*, C. R. Acad. Sci. Paris 18 (1844), стр. 883–885, 910–911.

[2] A. Thue, *Über Annäherungswerte algebraischer Zahlen*, J. Reine Angew. Math. 135 (1909), стр. 284–305.

[3] C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Zeitschr. 10 (1921), стр. 173–213.

[4] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), стр. 1–20.

[5] W. M. Schmidt, *Simultaneous approximation to algebraic numbers by rationals*, Acta Math. 125 (1970), стр. 189–201.

[6] — *Approximation to algebraic numbers*, Enseignement Math. 17 (1971), стр. 187–253.

[7] — *Linearformen mit algebraischen Koeffizienten. II*, Math. Ann. 191 (1971), стр. 1–20.

[8] — *Norm form equations*, Ann. of Math. 96 (1972), стр. 526–551.

[9] E. Dubois, G. Rhin, *Approximations rationnelles simultanées de nombres algébriques réels et de nombres algébriques p-adiques*, Soc. Math. France, Astérisque 24-25 (1975), стр. 211–227.

[10] — *Sur la majoration de formes linéaires à coefficients algébriques réels et p-adiques. Démonstration d'une conjecture de K. Mahler*, C. R. Acad. Sci. Paris, Ser. A, 282 (1976), стр. 1211–1214.

[11] H. P. Schlickewei, *Die p-adische Verallgemeinerung des Satzes von Thue–Siegel–Roth–Schmidt*, J. Reine Angew. Math. 288 (1976), стр. 86–105.

[12] — *The p-adic Thue–Siegel–Roth–Schmidt theorem*, Archiv der Math. 29 (1977), стр. 267–270.

[13] W. J. Leveque, *Topics in number theory*, Reading, Mass. 1956.

[14] K. Mahler, *Lectures on diophantine approximation*, Notre Dame University 1961.

[15] S. Lang, *Diophantine geometry*, New York and London 1962.

[16] E. Wirsing, *On approximations of algebraic numbers by algebraic numbers of bounded degree*, Proc. Symp. in Pure Math. XX, 1971, стр. 213–247.

[17] A. Baker, *Rational approximations to certain algebraic numbers*, Proc. London Math. Soc. 14 (1964), стр. 385–398.

[18] — *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers*, Quart. J. Math. Oxford 15 (1964), стр. 375–383.

[19] Н. И. Фельдман, *Оценки неполной линейной формы от некоторых алгебраических чисел*, Матем. заметки 7 (5) (1970), стр. 569–580.

[20] — *Некоторые диофантовы уравнения с конечным числом решений*, Вестник Моск. ун-та 26 (1971), стр. 52–58.

[21] C. F. Osgood, *On the simultaneous diophantine approximation of values of certain algebraic functions*, Acta Arith. 19 (1971), стр. 343–386.

[22] V. G. Sprindžuk, *Representation of numbers by the norm forms with two dominating variables*, J. Number Theory 26 (1974), стр. 481–486.

[23] G. V. Chudnovsky, *The Gelfond–Baker method in problems of diophantine approximation*, Coll. Math. Soc. J. Bolyai 13, Debrecen 1974, стр. 19–39.

[24] A. Baker, *Contributions to the theory of Diophantine equations*, Philos. Trans. Royal Soc. London Ser. A, 263 (1968), стр. 173–208.

[25] J. Coates, *An effective p-adic analogue of a theorem of Thue*, Acta Arith. 15 (1969), стр. 279–305.

[26] В. Г. Спринджук, *О рациональных приближениях к алгебраическим числам*, Изв. АН СССР 35 (1971), стр. 991–1007.
[27] Н. И. Фельдман, *Эффективное степенное усиление неравенства Лиувилля*, ibid. стр. 973–990.
[28] С. В. Котов, В. Г. Спринджук, *Уравнение Туэ–Малера в относительном поле и приближение алгебраических чисел алгебраическими числами*, Изв. АН СССР 41 (1977), стр. 723–751.
[29] K. Győry, Z. Z. Papp, *Norm form equations and explicit lower bounds for linear forms with algebraic coefficients*, Studies in Pure Mathematics, Akadémiai Kiadó, Budapest 1983, стр. 245–257.
[30] J. Gaál, *Norm form equations with several dominating variables and explicit lower bounds for inhomogeneous linear forms with algebraic coefficients*, I, II, Studia Sci. Math. Hungar. 19 (1984), стр. 399–411, 20 (1985), стр. 333–344.
[31] С. В. Котов, *Эффективная оценка линейной формы с алгебраическими коэффициентами в архимедовых и p-адических метриках*, Институт математики Акад. наук БССР, Препринт № 24 (125), Минск 1981.
[32] K. Győry, *Explicit lower bounds for linear forms with algebraic coefficients*, Arch. Math. (Basel) 35 (1980), стр. 438–446.
[33] S. V. Kotov, L. A. Trelina, *S-ganze Punkte auf elliptischen Kurven*, J. Reine Angew. Math. 306 (1979), стр. 28–41.
[34] С. В. Котов, *О диофантовых уравнениях норменного вида. I*, Институт математики, Акад. наук БССР, Препринт № 9 (89), Минск 1980.
[35] С. Ленг, *Алгебраические числа*, Мир, Москва 1966.
[36] K. Győry, *On the representation of integers by decomposable forms in several variables*, Publ. Math. Debrecen 28 (1981), стр. 89–98.

БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. В. И. ЛЕНИНА
Минск, СССР

Поступило 5.7.1988 (1844)

ACTA ARITHMETICA
LIII (1990)

A matrix paraphrase of cyclotomy

by

D. H. LEHMER (Berkeley, Cal.)

Dedicated to the memory of V. G. Sprindžuk

1. Introduction. In a recent letter Albert Whiteman [3] enclosed a preprint of a note on block designs in which he introduced a set of matrices whose properties mimicked the Gaussian periods of classic cyclotomy. I suggested to him that the matrices should be examined further. In reply he gave me permission to make this examination myself. This paper is the result.

2. Notation and nomenclature. Throughout this paper, capital letters will be used to denote matrices. We consider square matrices of a kind known as circulants. A circulant is an n by n matrix of the form

$$M = \begin{bmatrix} a_0 & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_0 & a_1 & \dots & a_{n-2} \\ a_{n-2} & a_{n-1} & a_0 & \dots & a_{n-3} \\ \dots & \dots & \dots & \dots & \dots \\ a_1 & a_2 & a_3 & \dots & a_0 \end{bmatrix}.$$

The matrix M depends only on its top row, and to save space we write

$$M = \operatorname{cir}(a_0, a_1, a_2, \dots, a_{n-1}).$$

We number the rows and columns from 0 to $n-1$ to allow the use of residue classes modulo n.

If we write

$$M = (\alpha_{ij}) \quad (i, j = 0, 1, \dots, n-1),$$

then

$$\alpha_{ij} = a_{j-i}$$

where we take the subscript modulo n.

We define Z_1 by

$$Z_1 = \operatorname{cir}(0, 1, 0, \dots, 0).$$