БИБЛИОТЕКА
ЧЕБЫШЁВСКОГО
СБОРНИКА

Алгебра, теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории

Материалы
XVII Международной конференции,
посвящённой
100-летию со дня рождения
профессора Н. И. Фельдмана
и 90-летию со дня рождения
профессоров А. И. Виноградова,
А. В. Малышева и Б. Ф. Скубенко

Библиотека Чебышевского сборника

Министерство науки и высшего образования Российской Федерации
Российская академия наук
Московский государственный университет им. М. В. Ломоносова
Математический институт им. В. А. Стеклова РАН
Институт истории естествознания и техники им. С. И. Вавилова РАН
Московский педагогический государственный университет
Тульский государственный педагогический университет им. Л. Н. Толстого
Тульский государственный университет

АЛГЕБРА, ТЕОРИЯ ЧИСЕЛ И ДИСКРЕТНАЯ ГЕОМЕТРИЯ: СОВРЕМЕННЫЕ ПРОБЛЕМЫ, ПРИЛОЖЕНИЯ И ПРОБЛЕМЫ ИСТОРИИ

Материалы XVII Международной конференции, посвящённой 100-летию со дня рождения профессора Н. И. Фельдмана и 90-летию со дня рождения профессоров А. И. Виноградова, А. В. Малышева и Б. Ф. Скубенко

Тула,
23–28 сентября 2019 г.

Тула
ТГПУ им. Л. Н. Толстого
2019

ББК 22.1
УДК 51
А45

А45 **Алгебра,** теория чисел и дискретная геометрия: современные проблемы, приложения и проблемы истории: Материалы XVII Международ. конф., посвящённой 100-летию со дня рождения профессора Н. И. Фельдмана и 90-летию со дня рождения профессоров А. И. Виноградова, А. В. Малышева и Б. Ф. Скубенко.– Тула: Тул. гос. пед. ун-т им. Л. Н. Толстого, 2019. – 304 с.

ISBN 978-5-6042450-5-7

ББК 22.1
УДК 51

Сборник издан при финансовой поддержке Российского фонда фундаментальных исследований (проект № 19-41-710004_р_а) и федеральной целевой программы «Исследование и разработки по приоритетным направлениям развития научно-технологического комплекса России на 2014–2020 годы» (уникальный идентификатор проекта RFMEF 157717X0271)

ISBN 978-5-6042450-5-7

УДК 511.235

Системы корней и решётки корней в числовых полях

В. Л. Попов (Россия, г. Москва)
Математический институт им. В. А. Стеклова РАН
e-mail: popovvl@mi-ras.ru

Root systems and root lattices in number fields

V. L. Popov (Russia, Moscow)
Steklov Mathematical Institute, Russian Academy of Sciences
e-mail: popovvl@mi-ras.ru

Излагаемые ниже результаты получены автором совместно с Ю. Г. Зархиным.

Пусть L — свободная абелева группа конечного ранга $n > 0$. Мы рассматриваем ее как (аддитивную) подгруппу полного ранга в n-мерном линейном пространстве $V := L \otimes_{\mathbb{Z}} \mathbb{Q}$ над $\mathbb{Q}$. Поскольку в любой системе корней каждый корень является целочисленной линейной комбинацией простых, для любого типа R систем корней ранга n в L найдется подмножество R ранга n, являющееся системой корней типа R. Однако, если пара (V, L) снабжена какой-либо дополнительной структурой, группа Вейля $W(R)$ множества R может оказаться с ней не согласованной: например, $W(R)$ может не состоять из ортогональных преобразований, если V снабжено скалярным произведением. Интересно поэтому искать лишь такие R, что $W(R)$ согласована с какими-либо дополнительными структурами на (V, L).

Естественным источником пар (V, L) является алгебраическая теория чисел, в которой они возникают в виде $(K, \mathscr{O}_K)$, где K — числовое поле (т.е. поле алгебраических чисел) степени n над $\mathbb{Q}$, а $\mathscr{O}_K$ — его кольцо целых.

С полем K естественно связана описанная в следующем разделе группа $\mathcal{L}(K)$ линейных преобразований этого поля. Ниже мы формулируем наши результаты по классификации типов R систем корней, допускающих такой выбор R, что $W(R)$ является подгруппой группы $\mathcal{L}(K)$.

Числовые поля K являются также естественным источником пар (L, b), где $b\colon L \times L \to \mathbb{Z}$ — невырожденная симметрическая билинейная форма (далее такие пары кратко называются *решётками*). А именно, зафиксируем автоморфизм $\theta \in \operatorname{Aut} K$, для которого $\theta^2 = \mathrm{id}$. Тогда

$$\mathrm{tr}_\theta\colon K \times K \to \mathbb{Q}, \quad \mathrm{tr}_\theta(x, y) := \mathrm{trace}_{K/\mathbb{Q}}(x \cdot \theta(y))$$

— такая невырожденная симметрическая билинейная форма, что для любого идеала I в $\mathscr{O}$ пара $(I, \mathrm{tr}_\theta|_{I \times I}) =: (I, \mathrm{tr}_\theta)$ является решёткой ранга n. Некоторые замечательные решетки изоморфны (т.е. изометричны) решеткам вида (I, tr_θ): например, это так для части корневых решеток, решетки Кокстера–Тодда, решетки Лича и ряда других; см. [2], [3]. Поэтому естественно возникает задача о классификации получающихся таким способом решеток. Среди всех ненулевых идеалов в $\mathscr{O}$ имеется выделенный, а именно, само кольцо $\mathscr{O}$. Это приводит к вопросу о том какие замечательные решетки имеют вид $(\mathscr{O}, \mathrm{tr}_\theta)$. Ниже мы формулируем наши результаты о подобии решеток вида $(\mathscr{O}, \mathrm{tr}_\theta)$ и корневых решеток.

Системы корней

В группе $\mathrm{GL}_\mathbb{Q}(K)$ невырожденных линейных преобразований линейного пространства K над $\mathbb{Q}$ естественно выделяются три подгруппы. Первой является группа $\mathrm{Aut}\, K$ автоморфизмов поля K. Второй — образ мономорфизма $\mathrm{mult}\colon K^* \hookrightarrow \mathrm{GL}_\mathbb{Q}(K)$, где $\mathrm{mult}(a)$ — оператор умножения на элемент $a \in K^*$, т.е. $\mathrm{mult}(a)\colon K \to K,\ x \mapsto ax$. Третьей — подгруппа $\mathcal{L}(K)$ в $\mathrm{GL}_\mathbb{Q}(K)$, порожденная $\mathrm{Aut}\, K$ и $\mathrm{mult}(K^*)$.

Определение 1 ([1, Def. 1]). *Мы говорим, что тип* R *(не обязательно приведённой) системы корней допускает реализацию в числовом поле* K*, если*

(a) $[K : \mathbb{Q}] = \mathrm{rk}(\mathsf{R})$*;*

(b) *в* $\mathscr{O}_K$ *существует подмножество* R *ранга* $\mathrm{rk}(\mathsf{R})$*, являющееся системой корней типа* R*;*

(c) $W(R)$ *является подгруппой группы* $\mathcal{L}(K)$*.*

В этом случае подмножество R *называется реализацией типа* R *в поле* K*.*

Отметим, что, заменяя $\mathscr{O}_K$ в п. (b) определения 1 на K, мы не получаем нового понятия (т.е. если R допускает реализацию в K в смысле измененного определения 1, то допускает и в смысле исходного).

Ввиду определения 1, если тип R системы корней допускает реализацию в числовом поле K, то группа $\mathcal{L}(K)$ содержит подгруппу, изоморфную группе Вейля системы корней типа R. Следующая теорема дает классификацию всех случаев, когда выполнено это последнее свойство:

Теорема 1 ([1, Thm. 1]). *Следующие свойства группы Вейля* $W(R)$ *приведённой системы корней* R *типа* R *и ранга* n *эквивалентны:*

(i) $W(R)$ *изоморфна подгруппе группы* $\mathcal{L}(K)$*, где* K *— числовое поле степени* n *над* $\mathbb{Q}$*;*

(ii) R *содержится в следующем списке:*

$$\mathsf{A}_1,\ \mathsf{A}_2,\ \mathsf{B}_2,\ \mathsf{G}_2,\ 2\mathsf{A}_1,\ 2\mathsf{A}_1 \dot{+} \mathsf{A}_2,\ \mathsf{A}_2 \dot{+} \mathsf{B}_2. \tag{1}$$

То, что для числового поля K подгруппа G группы $\mathcal{L}(K)$ изоморфна группе Вейля системы корней ранга $n = [K : \mathbb{Q}]$ и типа R, не эквивалентно тому, что $G = W(R)$, где R — система корней типа R в $\mathscr{O}_K$. Это видно из сравнения теоремы 2 со следующей теоремой, отвечающей на вопрос о том, какие типы корней из списка (1) реализуются в числовых полях:

Теорема 2 ([1, Thm. 2]). *Для каждого типа* R *(не обязательно приведённой) системы корней следующие свойства эквивалентны:*

(i) *существвет числовое поле, в котором* R *допускает реализацию;*

(ii) $\mathrm{rk}(\mathsf{R}) = 1$ *or* 2.

Ниже указаны явные реализации всех типов R систем корней рангов 1 и 2 в числовых полях [1, Sect. 2]. Через A_1' мы обозначаем единственный тип неприведенныз систем корней ранга 1, а через $\mathscr{O}_K(d)$ множество всех элементов из $\mathscr{O}_K$, норма которых равна d.

Системы корней типов A_1 *и* A_1'.

В этом случае $K = \mathbb{Q}$, $\mathscr{O}_K = \mathbb{Z}$. Если $\alpha \in \mathbb{Z}$, $\alpha \neq 0$, то $R := \{\pm\alpha\}$ (соответственно, $R := \{\pm\alpha, \pm 2\alpha\}$) является реализацией типа A_1 (соответственно, A_1') в поле K.

Системы корней типов A_2 *и* G_2.

Пусть K — третье циклотомическое поле: $K = \mathbb{Q}(\sqrt{-3})$. Тогда $\mathscr{O}_K = \mathbb{Z} + \mathbb{Z}\omega$, где $\omega = (1+\sqrt{-3})/2$. Пусть $\alpha_1 = 1$, $\alpha_2 = \omega^2$, $\beta_1 = (1+\omega)\alpha_1$, $\beta_2 = (1+\omega)\alpha_2$. В этом случае

$$\mathscr{O}_K(1) = \{\pm\alpha_1, \pm\alpha_2, \pm(\alpha_1+\alpha_2)\}, \quad \mathscr{O}_K(3) = (1+\omega)\mathscr{O}_K(1).$$

Можно доказать, что каждое из множеств $\mathscr{O}_K(1)$ и $\mathscr{O}_K(3)$ является реализацией типа A_2 в поле K, а множество

$$\mathscr{O}_K(1) \bigcup \mathscr{O}_K(3) = \{\pm\alpha_1, \pm\beta_2, \pm(\alpha_1+\beta_2), \pm(2\alpha_1+\beta_2), \pm(3\alpha_1+\beta_2), \pm(3\alpha_1+2\beta_2)\},$$

— реализацией типа G_2 в поле K.

Системы корней типов B_2, $2\mathsf{A}_1$, BC_2, $2\mathsf{A}_1$, $2\mathsf{A}_1'$ *и* $\mathsf{A}_1 \dot{+} \mathsf{A}_1'$.

Пусть K — четвертое циклотомическое поле: $K = \mathbb{Q}(\sqrt{-1})$. Тогда $\mathscr{O}_K = \mathbb{Z}+\mathbb{Z}i$, где $i = \sqrt{-1}$. Пусть $\alpha_1 = 1$, $\alpha_2 = i$, $\beta_1 = (1+i)\alpha_1$, $\beta_2 = (1+i)\alpha_2$. В этом случае

$$\mathscr{O}_K(1) = \{\pm\alpha_1, \pm\alpha_2\}, \quad \mathscr{O}_K(2) = (1+i)\mathscr{O}_K(1), \quad \mathscr{O}_K(4) = 2\mathscr{O}_K(1).$$

Можно доказать, что каждое из множеств $\mathscr{O}_K(1)$, $\mathscr{O}_K(2)$ и $\mathscr{O}_K(4)$ является реализацией типа $2\mathsf{A}_1$ в поле K, множество

$$\mathscr{O}_K(1) \bigcup \mathscr{O}_K(2) = \{\pm\alpha_1, \pm\beta_2, \pm(\alpha_1+\beta_2), \pm(2\alpha_1+\beta_2)\},$$

— реализацией типа B_2 в поле K, множество

$$\mathscr{O}_K(1) \bigcup \mathscr{O}_K(2) \bigcup \mathscr{O}_K(4) = \{\pm\alpha_1, \pm 2\alpha_1, \pm\beta_2, \pm(\alpha_1+\beta_2), \pm 2(\alpha_1+\beta_2), \pm(2\alpha_1+\beta_2)\}$$

— реализацией типа BC_2 в поле K, множество $\mathscr{O}_K(1) \bigcup \mathscr{O}_K(4)$ — реализацией типа $2\mathsf{A}_1'$ в поле K, а множество и $\mathscr{O}_K(1) \bigcup \{\pm 2\}$ — реализацией типа $\mathsf{A}_1 \dot{+} \mathsf{A}_1'$ в поле K.

Корневые решётки

Мы по-прежнему обозначаем через K числовое поле степени n над $\mathbb{Q}$. Напомним, что решетка (L_1, b_1) называется *подобной* решетке (L_2, b_2), если найдутся такие ненулевые целые числа m_1, m_2, что $(L_1, m_1 b_1)$ и $(L_2, m_2 b_2)$ — изоморфные решетки. Пусть множество $\mathcal{R}$ решеток является объединением двух бесконечных серий $\mathbb{A}_n$ $(n \geqslant 1)$, $\mathbb{D}_n$ $(n \geqslant 4)$ и четырёх спорадических решеток $\mathbb{Z}^1$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$, краткое описание которых мы напоминаем в приложении ниже (дальнейшие детали см., например в [3], [4]). Все решетки из $\mathcal{R}$ неприводимы, а всевозможные их ортогональные суммы называются *корневыми решетками.* Согласно классической теореме Витта, корневые решетки — это в точности такие решетки (L, b), что билинейная форма b положительно определена, а L является $\mathbb{Z}$-линейной оболочкой множества $\{x \in L \mid b(x,x) = 1 \text{ или } 2\}$.

Теорема 3 (об изоморфизме). *Определённая парой (K, θ) решётка $(\mathscr{O}_K, \mathrm{tr}_\theta)$ изоморфна корневой решётке тогда и только тогда, когда выполнено одно из следующих условий:*
(a) $K = \mathbb{Q}$, $\theta = \mathrm{id}$;
(b) $K = \mathbb{Q}(\sqrt{-3})$, *$\theta$ является комплексным сопряжением;*
(c) $K = \mathbb{Q}(\sqrt{-1})$, *$\theta$ является комплексным сопряжением.*

Теорема 4 (о подобии решётке $\mathbb{A}_n$). *Пусть определённая парой (K, θ) решётка $(\mathscr{O}_K, \mathrm{tr}_\theta)$ подобна корневой решётке $\mathbb{A}_n$ с $n > 1$. Тогда n четно, $n+1$ свободно от квадратов и пара (K, θ) обладает следующими свойствами:*
(a) *если $n = 2$, то $K = \mathbb{Q}(\sqrt{-3})$, а θ — комплексное сопряжение;*
(b) *если $n \geqslant 4$, то $K/\mathbb{Q}$ не является расширением Галуа и выполнено одно из условий:*
 (i) *K является вполне вещественным полем, $\theta = \mathrm{id}$, $n \equiv 0 \pmod 4$ и $n \geqslant 36$;*
 (ii) *K является CM-полем, θ — комплексное сопряжение, а $n \geqslant 50$.*

Теорема 5 (о подобии решётке $\mathbb{D}_n$). *Пусть определённая парой (K,θ) решётка $(\mathscr{O}_K, \mathrm{tr}_\theta)$ подобна корневой решётке $\mathbb{D}_n$ с $n \geqslant 4$. Тогда n четно и пара (K,θ) обладает одним из следующих свойств:*

(a) *K является вполне вещественным полем, $\theta = \mathrm{id}$, $n \equiv 0 \pmod 4$ и $n \geqslant 76$;*

(b) *K является CM-полем, θ — комплексное сопряжение, а $n \geqslant 46$.*

Теорема 6 (о подобии решётке $\mathbb{E}_n$). *Не существует такой пары (K,θ), что решётка $(\mathscr{O}, \mathrm{tr}_\theta)$ подобна какой-либо из решеток $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$.*

Приложение: решетки $\mathbb{A}_n$, $\mathbb{D}_m$ и $\mathbb{E}_r$

Пусть $\mathbb{R}^n$ — координатное n-мерное вещественное линейное пространство строк со стандартной структурой евклидова пространства

$$\mathbb{R}^n \times \mathbb{R}^n \to \mathbb{R}, \quad ((x_1,\dots,x_n),(y_1,\dots,y_n)) := \textstyle\sum_{i=1}^n x_i y_i. \tag{2}$$

Пусть e_j — строка $(0,\dots,0,1,0,\dots,0)$, в которой число нулей слева от 1 равно $j-1$.

Если L — такая $\mathbb{Z}$-линейная оболочка множества линейно независимых векторов в $\mathbb{R}^n$, что $b(L\times L) \subseteq \mathbb{Z}$, где b — ограничение на $L \times L$ отображения (2), то (L,b) называется *решеткой в* $\mathbb{R}^n$ и обозначается просто через L.

$\mathbb{Z}^n$ — это решетка $\{(x_1,\dots,x_n) \mid x_j \in \mathbb{Z}\ \text{ для всех } j\}$ в $\mathbb{R}^n$.

$\mathbb{A}_n$ — это решетка $\{(x_1,\dots,x_{n+1}) \in \mathbb{Z}^{n+1} \mid \sum_{j=1}^{n+1} x_j = 0\}$ в $\mathbb{R}^{n+1}$.

$\mathbb{D}_n$ — это решетка $\{(x_1,\dots,x_n) \in \mathbb{Z}^n \mid \sum_{j=1}^{n} x_j \equiv\ 0 \pmod 2\}$ в $\mathbb{R}^n$, $n \geqslant 2$.

$\mathbb{E}_8$ — это решетка $\mathbb{D}_8 \bigcup \left(\mathbb{D}_8 + \frac{1}{2}(e_1+\dots+e_8)\right)$ в $\mathbb{R}^8$.

$\mathbb{E}_7$ — это ортогонал в $\mathbb{E}_8$ к подрешетке $\mathbb{Z}(e_7+e_8)$.

$\mathbb{E}_6$ — это ортогонал в $\mathbb{E}_8$ к подрешетке $\mathbb{Z}(e_7+e_8)+\mathbb{Z}(e_6+e_8)$.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Popov V. L., Zarhin Yu. G. Root systems in number fields, accepted for publication in Indiana Univ. Math. J., arXiv:1808.01136v3. 2019.

2. Bayer-Fluckiger E. Lattices and number fields. Contemporary Math. 1999. Vol. 241. P. 69–84.

3. Конвей Дж., Слоэн Н. Упаковки шаров, решетки и группы. Тт. I и II. — Москва: Изд-во Мир, 1990.791 с.

4. Martinet J. Perfect Lattices in Euclidean spaces. Grundlehren der mathematischen Wissenschaften, Bd. 327, Springer-Verlag, 2003. 523 pp.