ЧЕБЫШЕВСКИЙ СБОРНИК
Том 16. Выпуск 4.

УДК 512

КВАДРАТИЧНЫЕ ФОРМЫ, АЛГЕБРАИЧЕСКИЕ ГРУППЫ И ТЕОРИЯ ЧИСЕЛ

Н. М. Глазунов (г. Киев)

Аннотация

Целью статьи является обзор некоторых важных результатов в теории квадратичных форм и алгебраических групп, которые оказали и оказывают влияние на развитие теории чисел. Статья ориентирована на избранные задачи и не является исчерпывающей. Представлены математические структуры, методы и результаты, в том числе и новые, связанные в той или иной степени с исследованиями В. П. Платонова.

Содержание статьи следующее. Во введении обращено внимание на классические исследования Коркина, Золотарева и Вороного по теории экстремальных форм и напоминаются соответствующие определения. В разделе "Квадратичные формы и решетки" представлены необходимые определения, результаты о решетках и квадратичных формах над полем вещественных чисел и над кольцом целых рациональных чисел. Раздел 3 "Алгебраические группы" содержит представление классов решеток в вещественных пространствах как факторов алгебраических групп, а также вариант критерия Малера компактности таких факторов. Приведен результат о компактности факторов ортогональных групп квадратичных форм, не представляющих рационально нуля, а также определения и понятия, связанные с кватернионными алгебрами над рациональными числами. Приведенные результаты явно или неявно используются в работах В. П. Платонова, а также в разделах 4 и 5. Раздел 4 "Точки Хигнера и их обобщения" содержит краткий обзор новых исследований в направлении нахождения точек Хигнера и их обобщений. В разделе 5 кратко представлены некоторые новые исследования и результаты по принципу Хассе для алгебраических групп. Для чтения статьи может быть полезным знакомство со статьей автора, опубликованной в 3-м выпуске "Чебышевского сборника" за 2015 год.

Я глубоко признателен Н. М. Добровольскому за помощь и поддержку в процессе подготовки статьи к печати.

Ключевые слова: положительно определенная квадратичная форма; тело над полем рациональных чисел; конечномерная алгебра; принцип Хассе; жесткость; точка Хигнера.

Библиография: 31 названий.

QUADRATIC FORMS, ALGEBRAIC GROUPS AND NUMBER THEORY

N. M. Glazunov (Kiev)

Abstract

The aim of the article is an overview of some important results in the theory of quadratic forms, and algebraic groups, and which had an impact on the development of the theory of numbers. The article focuses on selected tasks and is not exhaustive. A mathematical structures, methods and results, including the new ones, related in some extent with research of V.P. Platonov. The content of the article is following. In the introduction drawn attention to the classic researches of Korkin, Zolotarev and Voronoi on the theory of extreme forms and recall the relevant definitions. In section 2 "Quadratic forms and lattices"presented the necessary definitions, the results of the lattices and quadratic forms over the field of real numbers and over the ring of rational integers. Section 3 "Algebraic groups"contains a representation of the class of lattices in a real space as factors of algebraic groups, as well as the version of Mahler's compactness criterion of such factors. Bringing the results of the compactness of factors of orthogonal groups of quadratic forms which do not represent zero rationally, and the definitions and concepts related to the quaternion algebras over rational numbers. These results explicitly or implicitly are used in the works of V. P. Platonov and in sections 4 and 5. Section 4 "Heegner points and their generalizations" provides an overview of new research in the direction of finding Heegner points and their generalizations. Section 5 summarizes some new research and results on the Hasse principle for algebraic groups. For the reading of the article may be a useful another article which has published by the author in the Chebyshevsky sbornik, vol. 16, no. 3, in 2015.

I am deeply grateful to N. M. Dobrovolskii for help and support under the preparation of the article for publication.

Keywords: positive definite quadratic form; finite-dimensional associative division algebra over rationals; Hasse principle; rigidity; Heegner point.

Bibliography: 31 titles.

1. Introduction

Korkin and Zolotarev have investigated positively defined quadratic forms [1, 2] and proved [3] that every extreme form is perfect. Voronoi [4] has proved that every extreme form is eutactic and that perfect eutactic form extreme. Recall some definitions. We follow [1, 2, 3, 4, 5, 6, 7, 10] (and references therein).

Let K be a field of characteristic not 2. An $n-$ary quadratic form over K is the expression of the form

$$f(x) = f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j, \tag{1}$$

for $a_{ij} \in K, a_{ij} = a_{ji}$. The $n \times n$ symmetric matrix $A = (a_{ij})$ is called the *matrix of the quadratic form* f. The matrix and the row vector $\mathbf{x} = (x_1, \ldots, x_n)$ give $f(\mathbf{x}) = \mathbf{x}A\mathbf{x}^{tr}$ (tr denotes the transposition). The *determinant* $d = d(f) = det(f)$ of the quadratic form f is called the determinant of the symmetric matrix A determined by f. Two quadratic forms f and g are called *equivalent* if there exists a nonsingular homogeneous linear change of variable i.e. if there exists $C \in GL_n(K)$ such that $g(\mathbf{x}) = f(\mathbf{x}C)$. Or in matrix notations $B = CAC^{tr}$ and $d(g) = d(f)det(C)^2$.

Let $f(x)$ be a positive defined quadratic form in n variables. For real ϵ, set

$$m(f;\epsilon) = \min_x f(x+\epsilon),$$

where minimum being taken over integer x,

$$m(f) = \max_\epsilon m(f;\epsilon),$$

$$\mu(f) = m(f)/d^{1/n}.$$

It is said that f is *extreme* if $\mu(f)$ is a local minimum.

Blichfeld have investigated minimum values of quadratic forms and packing of sphere. Recall that by Blichfeld [8] the spheres of the packing cannot be displaced without increasing the total volume occurred by them. Extreme forms correspond to packings that are *rigid*. A positive quadratic form corresponding to a densest lattice packing is called an *absolutely extreme*.

It is said that two $n-$ ary forms f and g with matrices A and B are properly or improperly integrally equivalent if their matrices are related by

$$B = MAM^{tr}$$

for some M with integer entries and determinant $+1$ or -1 respectively. We will consider mainly rings $\mathbb{Z}$ and $\mathbb{Z}_p$.

The norm of the vector $\mathbf{x} = (x_1, \ldots, x_n)$ is denoted by $N(\mathbf{x}) = (\mathbf{x}, \mathbf{x}) = x_1^2 + \ldots + x_n^2$.

The aim of the article is an overview of some important results in the theory of quadratic forms and algebraic groups, and which had an impact on the development of the theory of numbers. The article focuses on selected tasks and is not exhaustive. A mathematical structures, methods and results, including the new ones, related in some extent with research of V. P. Platonov [12, 13, 14, 11].

Further contents of the article the following.

In section 2 "Quadratic forms and lattices" presented the necessary definitions, the results of the lattices and quadratic forms over the field of real numbers and over the ring of rational integers [15, 16]. Section 3 "Algebraic groups" contains a representation of the class of lattices in a real space as factors of algebraic groups, as well as the version of Mahler's compactness criterion of such factors. Bringing the results of the compactness of factors of orthogonal groups of quadratic forms which do not represent zero rationally, and the definitions and concepts related to the quaternion algebras over rational numbers. These results explicitly or implicitly are used in the works of V. P. Platonov and in sections 4 and 5. Section 4 "Heegner points and their generalizations" provides an overview of new research in the direction of finding Heegner points and their generalizations. Section 5 summarizes some new research and results on the Hasse principle for algebraic groups. For the reading of the article may be a useful another article which has published by the author[31] in the Chebyshevskii sbornik in 2015.

2. Quadratic forms and lattices

2.1. Quadratic forms over fields and quadratic spaces

If $C = (\mathbf{c}_1, \ldots, \mathbf{c}_n),\ \mathbf{c}_i = (c_{1i}, \ldots, c_{ni})$ then $b_{ij} = f(\mathbf{c}_i, \mathbf{c}_j)$, where $f(\mathbf{u}, \mathbf{v}) = \mathbf{u}A\mathbf{v}^{tr}$ is the bilinear form that corresponds to f.

Let K^{n^2} be the linear space of the dimension n^2 over K with coordinate $(a_{11}, \ldots, a_{nn})$. The *moduli space* $MF(n, K)$ of quadratic forms (1) is defined in K^{n^2} by the system of equations

$$a_{ij} - a_{ji} = 0,\ 1 \leqslant i, j \leqslant n.$$

The dimension of $MF(n, K)$ is equal to $\frac{n(n+1)}{2}$. Operation of the group $GL_n(K)$ on forms (1) defines an operation on $MF(n, K)$.

To any quadratic form $f = f(\mathbf{x}) = \mathbf{x}A\mathbf{x}^{tr}$ and $V = K^n$ it is possible to associate a map $\mathbf{x}A\mathbf{x}^{tr} : V \to K$ and the foregoing bilinear form $\phi = f(\mathbf{u}, \mathbf{v})$. The space (V, ϕ) is called the *quadratic space* [9]. If $(V, \phi), (V', \phi')$ are quadratic spaces then it is said that they are *isometric* if there exists a linear isomorphism $\sigma : V \to V'$ such that $\phi'(\sigma(\mathbf{u}), \sigma(\mathbf{u})) = \phi(\mathbf{u}, \mathbf{u})$ for all $\mathbf{u} \in V$. There exists a one-to-one correspondence between equivalence classes of $n-$ary quadratic forms over K and isometry classes of $n-$dimensional quadratic spaces over K.

2.2. Lattices and quadratic forms over reals

Let

$$f(x) = f(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

be a real quadratic form.

PROPOSITION 1. *Let $f = f(\mathbf{x})$ be a real positively defined (non degenerate) quadratic form and $S = \{\mathbf{s}\}$ not empty set of integer points (i.e. points with integer coordinates). Then the function $f(\mathbf{x})$ reaches a minimum on the set S. There is point $\mathbf{s}_0 \in S$ with a condition $f(\mathbf{s}) \geqslant f(\mathbf{s}_0)$ for all $\mathbf{s} \in S$.*

Proof. For the proof of the lemma 1 it is enough to present f as the sum of squares:

$$f(\mathbf{x}) = \sum_{i=1}^{n} \left(\sum_{i=1}^{n} c_{ij} x_j \right)^2, \ \det(c_{ij}) \neq 0$$

and to notice, that from the boundness of $f(x)$ follows the boundness of $|\sum c_{ij}x_j|$, $i = 1, \ldots, n$. From this as $\det(c_{ij}) \neq 0$ follows boundness of $x_1, \ldots, x_n$. The next statements are consequences of discreteness of a lattice.

Corollary. Let $\{\mathbf{a}\}$ be a non empty set of vectors of a lattice Λ. Then there is a vector $\mathbf{a}_0 \in \{\mathbf{a}\}$ of the least length.

Let Λ be a lattice of points of n-dimensional Euclidean space; $\mathbf{a}_1, \ldots, \mathbf{a}_k$ linear independent vectors of the lattice Λ ($k \leqslant n$). The set of vectors $\mathbf{a}_1, \ldots, \mathbf{a}_k$ is called a *primitive system of vectors* of the lattice if from

$$\alpha_1 \mathbf{a}_1 + \cdots + \alpha_k \mathbf{a}_k \in \Lambda,$$

where $\alpha_1, \ldots, \alpha_k$ are real numbers, follows that $\alpha_1, \ldots, \alpha_k$ are integers. In particular for $k = 1$ the vector forms primitive system in only case when it is primitive, i.e. it cannot be presented as $\bar{\mathbf{a}} = \alpha \mathbf{a}', \mathbf{a}' \in \Lambda, \alpha > 1$.

Proposition 2. *[7] Let Λ be a lattice of points of $n-$dimensional Euclidean space; $k \leqslant n$; $\mathbf{a}_1, \ldots, \mathbf{a}_k$ linearly independent vectors of the lattice Λ. It is necessary and sufficient that $\mathbf{a}_1, \ldots, \mathbf{a}_k$ made primitive system of vectors of a lattice Λ so, that $\mathbf{a}_1, \ldots, \mathbf{a}_k$ was possible to add to a basis of the lattice Λ.*

For a lattice $\Lambda = \Lambda[\mathbf{a}_1, \ldots, \mathbf{a}_k]$, $k \leqslant n$, the set $|\Lambda| = v(\sum_i x_i \mathbf{a}_i, 0 \leqslant x_i \leqslant 1)$ is called the *fundamental parallelepiped* of the lattice Λ of the volume $|\Lambda|$.

Let $\Lambda = \Lambda[\mathbf{a}_1, \ldots, \mathbf{a}_n]$ be a full lattice of $n-$dimensional Euclidean space, $\Delta(\Lambda)$ the determinant of the lattice. Correspond to the lattice Λ with bases $[\mathbf{a}_1, \ldots, \mathbf{a}_n]$ the positive quadratic form $f(x)$ in n variables with real coefficients:

$$f(x) = f(x_1, \ldots, x_n) = (\mathbf{a}_1 x_1 + \ldots + \mathbf{a}_n x_n)^2 = \sum_{i,j=1}^{n} (\mathbf{a}_i, \mathbf{a}_j) x_i x_j.$$

Conversaly for a positive definite quadratic form f in n variables with real coefficients it is possible correspond a lattice Λ such that $\Delta(\Lambda) = \sqrt{d}$, where d is the determinant of f.

Forms which are equivalent under a integer unimodular transform is united into a single class

2.3. Integral lattices and quadratic forms

A lattice or a quadratic form is called integral if the inner product of any two lattice vectors is an integer, or if the Gram matrix has integer entries.

Any $n-$dimensional lattice $\Lambda = \Lambda[\mathbf{a}_1, \ldots, \mathbf{a}_n]$ has a dual lattice Λ^* given by

$$\Lambda^* = \{\mathbf{x} \in \mathbb{R}^n : (\mathbf{x}, \mathbf{u}) \in \mathbb{Z} \text{ for all } \mathbf{u} \in \Lambda\}.$$

3. Algebraic groups

For algebraic groups $GL_n(\mathbb{R})$ and $GL_n(\mathbb{Z})$ the factorgroup

$$GL_n(\mathbb{R})/GL_n(\mathbb{Z})$$

is the set of all n-dimensional lattices in $\mathbb{R}^n$. Let

$$\mathcal{L} \subset GL_n(\mathbb{R})/GL_n(\mathbb{Z})$$

be a subset of the set of lattices.

3.1. Compactness criteria

Recall that there is the function

$$F : GL_n(\mathbb{R}) \to \mathbb{R}_+, F(g) = |\det g|\,, |\det g| : GL_n(\mathbb{Z}) \to 1.$$

3.1.1. Fundamental parallelepipeds of a lattice and its sublattice

If $(\Lambda : \Lambda') = k$ then $\left|\Lambda'\right| = k\,|\Lambda|\,.$

3.1.2. Hadamard inequality

If $\Lambda = \Lambda\left[\mathbf{a}_1, \ldots, \mathbf{a}_n\right]$, then $|\Lambda| \leqslant |\mathbf{a}_1| \cdots |\mathbf{a}_n|\,.$

3.1.3. Minkowski lemma

Let T be a convex central symmetric body and Λ be a full lattice in real space $\mathbb{R}^n$, $v(T) > 2^n\,|\Lambda|$. Then $\Lambda \bigcap T \neq 0$.

3.1.4. Compactness criteria

Recall the definition.
Definition A lattice $\Lambda \subset \mathcal{L}$ is relatively compact if
1) $|\Lambda| < b,\ \Lambda \subset \mathcal{L}$;
2) $|\mathbf{x}| > a, \mathbf{x} \in \Lambda \subset \mathcal{L}, \mathbf{x} \neq 0$.
Below we give a variant of Mahler's compactness theorem:

Theorem 1. *Let lattices from the set $\mathcal{L}$ are relatively compact. Then each lattice $\Lambda\left[\mathbf{a}_1, \ldots, \mathbf{a}_n\right]$ that satisfies conditions of the definition 3.1.4 has the bases such that $|\mathbf{a}_i| < C(a, b),\ i = 1. \ldots, n$.*

Sketch of the proof. The proof is by induction on n with applications of Minkowski lemma, Hadamard inequality and fundamental parallelepipeds of lattices and their sublattices as well as their volumes. Let $n = 1$. By denote. Consider $n-$ball of the radius $r > 2(b/V_n,)^{1/n}$, where V_n is the volume of the unit $n-$ball.

By Minkowski lemma there is an element $\mathbf{a} \neq 0$ of the lattice, $\mathbf{a}_1 \in \Lambda$, $\mathbf{a} = m\mathbf{a}_1$, $m \in \mathbb{Z}, |\mathbf{a}_1| < C, \mathbf{a}_1\mathbb{Q} \bigcap \Lambda = [\mathbf{a}_1]$.

By the induction hypothesis there are $\mathbf{a}_1, \dots, \mathbf{a}_{n-1} \in \Lambda$ such that $|\mathbf{a}_i| < C$ and $(\mathbf{a}_1\mathbb{Q} + \ldots + \mathbf{a}_{n-1}\mathbb{Q}) \bigcap \Lambda = [\mathbf{a}_1, \dots, \mathbf{a}_{n-1}]$. In the inductive step Minkowski lemma and Hadamard inequality are used. We omit the proof.

Proposition 3. *Let $f(\mathbf{x})$ be the quadratic form which do not represents zero rationally, $G = \mathcal{O}(f)$ the orthogonal group of the quadratic form. Then*

$$G(\mathbb{R})/G(\mathbb{Z})$$

is compact.

3.1.5. Finite-dimensional associative division algebras over rationals

Let $\mathcal{D} = \mathbb{Q}\alpha_1 + \cdots + \mathbb{Q}\alpha_n$ be finite-dimensional associative division algebra over rationals. For any $\mathbf{u} \in \mathcal{D}$ put $T_u(\mathbf{x}) = \mathbf{u}\mathbf{x}, \mathbf{x} \in \mathcal{D}$. We have $T_{u_1u_2} = T_{u_1}T_{u_2}$. Put $\det T_u = N(\mathbf{u})$.

It is well known that $N(\mathbf{u_1}\mathbf{u_2}) = N(\mathbf{u_1})N(\mathbf{u_2})$, and $N(\mathbf{u}) = 0$ if and only if $\mathbf{u} = 0$.

Lemma 1. *Suppose that G_D^N is the set of all $\mathbf{d} \in \mathcal{D}$ such that $N(\mathbf{d}) = 1$. Then $G_D^N = G$ is the group.*

Proof. For $\mathbf{x} = x_1\alpha_1 + \cdots + x_n\alpha_n$ we can write the group in the space of dimension $n+1$ in coordinates $(x_1, \dots, x_n, t)$ as $N(x_1\alpha_1 + \cdots + x_n\alpha_n)t = 1$. Denote the group by G_D. When $N(\mathbf{d}) = 1$ we obtain the group G_D^N.

Proposition 4. *Put $G = G_D^N$. Then*

$$G(\mathbb{R})/G(\mathbb{Z})$$

is compact.

3.1.6. Quaternion algebras over rationals

Let $B = \{\mathbf{u} = x + y\mathbf{i} + z\mathbf{j} + t\mathbf{k},\ x, y, z, t \in \mathbb{Q}\}$ be the quaternion algebra over $\mathbb{Q}$ with relations $\mathbf{i}^2 = a, \mathbf{j}^2 = b, a, b \in \mathbb{Q}, \mathbf{ij} = \mathbf{k}, \mathbf{ji} = -\mathbf{k}$.

Denote by $\mathbf{u}^*$ the conjugate quaternion. Then $n(\mathbf{u}) = \mathbf{u}\mathbf{u}^*$ is by definition the reduced norm of $\mathbf{u}$. It is easy to see that $N(\mathbf{u}) = (x^2 - ay^2 - bz^2 + abt^2)^2 = n(\mathbf{u})^2$.

3.2. Algebraic groups and critical lattices

Extreme lattices and Mahler's compactness theorem are connected with critical lattices [7, 29]. In this subsection we recall the connection between critical lattices and algebraic groups. In the two-dimensional real case after complexification of the space and critical lattices in it we obtain the interesting class of complete one-dimensional projective algebraic groups. These are elliptic curves which correspond to the critical lattices [28, 29].

4. Heegner points and their generalizations

Heegner points on elliptic curves have defined by Birch and Heegner-like points have defined by several authors (see [18] and references therein). There are open problems in the theory of Heegner-Stark (Darmon) and Darmon-like points in elliptic curves E over $\mathbb{Q}$ of conductor N with a prime p such that $N = pDM$, where D is the product of even (possible zero) distinct primes and $(D, M) = 1$, namely:

Suppose K be a real quadratic field in which all prime dividing M are split, and all primes dividing pD are inert and let $\mathcal{H}_p = K_p \setminus \mathbb{Q}_p$ be the K_p- points on the $p-$ adic upper half plane.

Then in the case $D = 1$ there is the conjecture by H. Darmon [19] that local points $P_\tau \in E(K_p)$ associated to elements $\tau \in K \bigcap \mathcal{H}_p$ defined as certain Coleman integrals of a modular form attached to E to be rational over specific ring class field of K, and to behave in many aspects as the classical Heegner points arising from imaginary quadratic fields;

in the case $D > 1$ there is a construction of Darmon-like points on $E(K_p)$, by means of certain $p-$adic integrals related to modular forms on quaternion division algebras of discriminant D. Greenberg conjectured that these points behave in many aspects as Heegner points and, in particular, that they are rational over ring class of K.

The authors of the paper [20] developed the (co)homological techniques for effective construction of the quaternionic Darmon points on $E(K_p)$.

They use the reinterpretation of Darmon's theory of modular symbols and mixed period integrals by M. Greenberg [21]and relate $p-$adic integration to certain overconvergent cohomology classes in order to derive an efficient algorithm for the computation of quaternionic Darmon points.

In the Introduction authors describe the contents of the paper under review and fixes notation.

The second Section is devoted to preliminaries on Hecke operators, the Bruhat-Tits tree, and measures.

In Section 3 Greenberg's construction of quaternionic $p-$adic Darmon points is dealt with. The main results of the paper [20] are presented in Sections 4–6.

In Section 4 the explicit algorithms that allow for the effective calculation of the quaternionic $p-$adic Darmon points are presented (Theorem 4.1, Theorem 4.2). Theorems and their proofs describe the algorithms and contain a correctness proof of the algorithms.

Section 5 treats the integration pairing via overconvergent cohomology. Authors of the paper [20] reduce the problem of computing integrals under consideration to that of computing moments and give an algorithm for computing the moments by means of the overconvergent cohomology lifting techniques by D. Pollack and

R. Pollack [22]. Finally last section treats results of extensive calculations and numerical evidence obtained by the authors of the paper [20] in support of the conjectured rationality of Greenberg's Darmon points.

5. Hasse principle

Let $\mathcal{M}$ be a class of algebraic varieties over algebraic number field F. The Hasse principle by[16, 17] for the class $\mathcal{M}$ is the next assertion: Suppose that $V \in \mathcal{M}$ and V is nonempty for all places v of the field F. Then $V(F)$ is nonempty. For algebraic number field there exists an exact sequence $0 \to Br(F) \to \bigoplus_v Br(F_v) \to \mathbb{Q}/\mathbb{Z} \to 0$, where $Br(F)$ is the Brauer group of F. The injectivity of $Br(F) \to \bigoplus_v Br(F_v)$ is called the Hasse principle for central simple algebra over F.

Let Ω_K denotes the set of (normalized) discrete valuations of rank 1 over a field K.

Yong in his paper [17] proves the conjecture by Colliot-Thèlène, Parimala, Suresh [24] on the triviality of the natural map $H^1(K,G) \to \prod_{v\in\Omega_K} H^1(K_v,G)$ (Hasse principle with respect to Ω_K for G-torsors over K) for groups of some classical types, where K is a field and G is a smooth connected linear algebraic group over K.

The main results of the paper [23] are two theorems. Theorem 1.6: Let K be a function field of p-adic arithmetic surface and G a semisimple simply connected group over K. Assume $p \neq 2$ if G contains an almost simple factor of type ${}^2A_n^*$ of even index. If every almost simple factor of G is of type ${}^1A_n^*, {}^2A_n^*, B_n, C_n^*, D_n^*, F_4^{red}$ or G_2, then the natural map $H^1(K,G) \to \prod_{v\in\Omega_K} H^1(K_v,G)$ has a trivial kernel.

Some results in the direction has also been proven by Preeti [25].

In Theorem 1.7 the author of [23] obtains (with applications of the Rost invariant) sufficient as well as necessary and sufficient conditions for the Hasse principle with respect to Ω_K when the field K is a function field of a local henselian surface with finite residue field of characteristic p.

The important tools in the proofs are theory of involutions and hermitian forms over central simple algebras, Witt groups, exact sequence of Parimala, Sridharan and Suresh by Bayer-Fluckiger and Parimala [26], invariants of hermitian forms, norm principle for spinor norms by Merkurjev [27].

6. Conclusion

Classical and novel results on quadratic forms and algebraic groups which have influenced the development of the theory of numbers are presented.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Korkin A., Zolotarev G. Sur les formes quadratiques positives quaternaires // Math. Ann. 1872. Vol. 5. P. 581–583.

2. Korkin A., Zolotarev G. Sur les formes quadratiques // Math. Ann. 1873. vol. 6. P. 366–389.

3. Korkin A., Zolotarev G. Sur les formes quadratiques positives // Math. Ann. 1877. Vol. 11. P. 242–292.

4. Voronoi G. Sur quelques proprietes des formes quadratiques positives parfaites // J. Reine Angew. Math. 1907. Vol. 133. P. 97–178.

5. Малышев А. В. О представлении целых чисел положительными квадратичными формами // Тр. МИАН СССР. 1962. Т. 65. С. 3–212.

6. Рышков С. С., Барановский Е. П. Классические методы теории решетчатых упаковок // УМН. 1979. Т. 34, вып. 4. 208. С. 3–63.

7. Касселс Дж. Введение в геометрию чисел. М.: Мир, 1965. 422 с.

8. Blichfeldt H. F. The minimum values of quadratic forms, and the closest packing of spheres // Math. Ann. Vol. 39.1935. P. 1–15.

9. Касселс Дж. Рациональные квадратичные формы. М.: Мир, 1982. 436 с.

10. Шафаревич И. Р. Основы алгебраической геометрии. Т. 1. Т. 2. М.: Наука. Гл. ред. физ.–мат. лит., 1988. 352 с. 304 с.

11. Платонов В. П. Арифметические свойства функциональных квадратичных полей и кручение в якобианах // Чебышевский сборник. 2010. Т.11, вып. 1. С. 234–238.

12. Платонов В. П. Арифметическая теория линейных алгебраических групп и теория чисел // Труды МИАН. 1973. Т. 132. С.162–168.

13. Платонов В. П. Проблема Таннака–Артина и приведенная K-теория // Изв. АН СССР, сер. мат. 1976. Т. 40, №2. С. 227–261.

14. Платонов В. П. 1976, Замечания к моей работе “Проблема Таннака–Артина и приведенная K-теория"// Изв. АН СССР, сер. мат. 1976. Т. 40, №5. С. 1198.

15. Боревич З. И., Шафаревич И.Р. Теория чисел. М.: Наука, 1985. 510 с.

16. Манин Ю. И. Кубические формы. М.: Наука, 1972. 304 с.

17. Hasse principle. Encyclopedia of Mathematics.
URL: http://www.encyclopediaofmath.org

18. Birch B. Heegner points: the beginnings // MSRI Publications. 2004. Vol. 40. P. 1–10.

19. Darmon H. Integration on $H_p \times H$ and arithmetic applications // Ann. of Math. 2001. 154. No. 3. 589 – 639.

20. Guitart X., Masdeu M. Overconvergent cohomology and quaternionic Darmon points // J. Lond. Math. Soc. II. 2014. Ser. 90. No. 2. P.393–403.

21. Greenberg M. Stark-Heegner points and the cohomology of quaternionic Shimura varieties // Duke Math. J. 2009. 147. No. 3. P. 541–575.

22. Pollack D., Pollack R. A construction of rigid analitic cohomology classes for congruence subgroups of $SL_3(\mathbb{Z})$ // Canad. J. Math. 2009. 61. No. 3. P. 674–690.

23. Yong H. Hasse principle for simply connected group over function fields of surfaces // J. Ramanujan Math. 2014. 29. No. 2. P. 155–199.

24. Colliot-Thèlène J.-I., Parimala R., Suresh V. Patching and local-global principles for homogeneous spaces over function fields of p-adic curves // Commut. Math. Helv. 2012. 87. P. 1011–1033.

25. Preeti R. Classification theorems for hermitien forms, the Rost kernel and Hasse principle over fields with $cd_2(k) \leqslant 3$, // J. Algebra. 2013. 385. P. 294–313.

26. Bayer-Fluckiger E., Parimala R. Galois cohomology of the classical groups over fields of cohomological dimension $\leqslant 2$ // Invent. Math. 1995. 122. P. 195–229.

27. Merkurjev A. Norm principle for algebraic groups // St. Petersburg J. Math. 1996. 7. P. 243–264.

28. Glazunov N. M. Minkowski's Conjecture on Critical Lattices and the Quantifier Elimination // Algoritmic algebra and logic. Proc. of the A3L Int. Conf. Passau. Germany. 2005. P. 111–114.

29. Glazunov N. M. Critical lattices, elliptic curves and their possible dynamics // Proceedings of the Third Int. Voronoj Conf. Part 3, Kiev. 2005. P. 146–152.

30. Glazunov N. M. Modular curves, Hecke operators, periods and formal groups // X International Conference dedicated to the 70th anniversary of Yu. A. Drozd. Odessa: I.I. Mechnikov Odessa National University, 2015. C. 42.

31. Glazunov N. M. Extremal forms and rigidity in arithmetic geometry and in dynamics // Чебышевский сборник. 2015. Т.16, вып. 3. С. 124–146.

REFERENCES

1. Korkin A., Zolotarev G. 1872, "Sur les formes quadratiques positives quaternaires", *Math. Ann.*, vol. 5, 581–583.

2. Korkin A., Zolotarev G. 1873, “Sur les formes quadratiques”, *Math. Ann.*, vol. 6, 366–389.

3. Korkin A., Zolotarev G. 1877, “Sur les formes quadratiques positives”, *Math. Ann.*, vol. 11, 242–292.

4. Voronoi G. 1907, “ Sur quelques proprietes des formes quadratiques positives parfaites”, *J. Reine Angew. Math.*, vol. 133, P. 97–178.

5. Malyshev A. V. 1962, “On the representation of integers by positive quadratic forms”, *Trudy Mat. Inst. Steklov., ed. I. G. Petrovskii, Acad. Sci. USSR, Moscow*, vol. 65, P. 3–212.

6. Ryshkov S. S., Baranovskii E. P. 1979, “Classical methods in the theory of lattice packings”, *Uspekhi Mat. Nauk*, vol. 34, no. 4, P. 3–63.

7. Cassels J. W. S. An Introduction to the Geometry of Numbers. — Berlin, Springer-Verlag, 1959.

8. Blichfeldt H. F. 1935, “The minimum values of quadratic forms, and the closest packing of spheres”, *Math. Ann.*, vol. 39, P. 1–15.

9. Cassels J. W. S. Rational quadratic forms. – London-New York, Academic Press, 1978.

10. Shapharevich I. R. 1988, "Foundations of Algebraic Geometry" , vol. 1, vol. 2. (in Russian), Moscow, Nauka, 352 p., 304 p.

11. Platonov V. P. 2010, “Arithmetic properties of quadratic function fields and torsion in Jacobians”, *Chebyshevskii Sb.*, vol. 11, no. 1, P. 234–238.

12. Platonov V. P. 1973, “The arithmetic theory of linear algebraic groups and number theory”, *Proc. Steklov Inst. Math.*, 132, P. 184–191.

13. Platonov V. P. 1976, “The Tannaka–Artin problem and reduced K-theory”, *Math. USSR-Izv.*, vol. 40, no. 2, P. 211–243.

14. Platonov V. P. 1976, “Remarks on my paper ‘The Tannaka–Artin problem and reduced K -theory”, *Izv. Akad. Nauk SSSR Ser. Mat.*, vol. 40, no.5, P. 1198.

15. Borevich Z. I, Shapharevich I. R., Number Theory(in Russian). — Moscow: Nauka, 1985. 503 p.

16. Manin Ju. I. Kubicheskie Formy, (in Russian). – Moscow: Nauka, 1972. 304 p. Cubic forms. Algebra, geometry, arithmetic, North-Holland, 1974.

17. Hasse principle. Encyclopedia of Mathematics. URL: http://www.encyclopedia ofmath.org

18. Birch B. 2004, “Heegner points: the beginnings *MSRI Publications*, vol. 40, P. 1–10.

19. Darmon H. 2001, “Integration on $H_p \times H$ and arithmetic applications *Ann. of Math.* 2, 154, no. 3, 589 –639.

20. Guitart X., Masdeu, M. 2014, “Overconvergent cohomology and quaternionic Darmon points”, *J. Lond. Math. Soc., II*, ser. 90, no. 2, P.393–403.

21. Greenberg M. 2009, “Stark-Heegner points and the cohomology of quaternionic Shimura varieties, *Duke Math. J.*, 147, no. 3, P. 541–575.

22. Pollack D., Pollack R. 2009, “A construction of rigid analitic cohomology classes for congruence subgroups of $SL_3(\mathbb{Z})$”, *Canad. J. Math.*, 61, no. 3, P. 674–690.

23. Yong H. 2014, “Hasse principle for simply connected group over function fields of surfaces”, *J. Ramanujan Math.*, 29, no. 2, P. 155–199.

24. Colliot-Thèlène J.-I., Parimala R., Suresh V. 2012, “Patching and local-global principles for homogeneous spaces over function fields of p-adic curves”, *Commut. Math. Helv.*, 87, 1011–1033.

25. Preeti R. 2013, Classification theorems for hermitien forms, the Rost kernel and Hasse principle over fields with $cd_2(k) \leqslant 3$, *J. Algebra*, 385, 294–313.

26. Bayer-Fluckiger E., Parimala R. 1995, Galois cohomology of the classical groups over fields of cohomological dimension $\leqslant 2$, *Invent. Math.*, 122, 195–229.

27. Merkurjev A. 1996, Norm principle for algebraic groups, *St. Petersburg J. Math.*, 7, 243–264.

28. Glazunov N. M. 2005, “Minkowski’s Conjecture on Critical Lattices and the Quantifier Elimination”, *Algoritmic algebra and logic. Proc. of the A3L Int. Conf., Passau, Germany*, P. 111–114.

29. Glazunov N. M. 2005, “Critical lattices, elliptic curves and their possible dynamics”, *Proceedings of the Third Int. Voronoj Conf., Part 3, Kiev*, P. 146–152.

30. Glazunov N. M. 2015, “Modular curves, Hecke operators, periods and formal groups”, *X International Conference dedicated to the 70th anniversary of Yu. A. Drozd. Odessa: I. I. Mechnikov Odessa National University*, P. 42.

31. Glazunov N. M. 2015, “Extremal forms and rigidity in arithmetic geometry and in dynamics”, *Chebyshevskii Sbornik*, vol.16, no. 3, P.124–146.

National Aviation University.
Received 9.11.2015.