ЧЕБЫШЕВСКИЙ СБОРНИК
Том 25. Выпуск 5.

УДК 511 DOI 10.22405/2226-8383-2024-25-5-113-125

О группе классов форм высоких степеней

С. А. Мешаик

Мешаик Сеймур Ариф оглы — доктор философии по математике, Гянджинский государственный университет (г. Гянджа, Азербайджан).
e-mail: seymurmeshaik82@gmail.com

Аннотация

В теории чисел группы классов форм были введены Гауссом для бинарных квадратичных форм. Гаусс ввел понятия эквивалентности и композиции и определил групповую структуру во множестве классов эквивалентности в семействе квадратичных форм с дискриминантами, не делящимися на квадрат целого числа. Дальнейшие исследования были развиты в разных направлениях. Одним из них является обобщение теории на квадратичные формы от большего числа переменных, где широко изучены вопросы, связанные с представлением целых чисел различными квадратичными формами. Другое направление относится к понятию композиции. Однако с ростом количества переменных становится все труднее введение понятия композиции форм. В 1898 г. А. Гурвиц показал, что для квадратичных форм с числом переменных больше 8 очень сложно ввести удовлетворительное понятие композиции. Этот феномен впоследствии был разъяснен Ю. В. Линником с точки зрения теории некоммутативных алгебр с делением. Установлено, что понятие «дискриминанта» не имеет столь существенного значения для форм высших степеней, чем для квадратичных форм. Хорошо известна строгая разница между свойствами форм степени выше 2 с одинаковыми дискриминантами. Для устранения этих трудностей удобно рассмотреть формы, связанные с данным расширением.

Ключевые слова: группы, классы форм, алгебраические расширения, дедекиндовы поля.

Библиография: 9 названий.

Для цитирования:
Мешаик, С. А. О группе классов форм высоких степеней // Чебышевский сборник, 2024, т. 25, вып. 5, с. 113–125.

CHEBYSHEVSKII SBORNIK
Vol. 25. No. 5.

UDC 511 DOI 10.22405/2226-8383-2024-25-5-113-125

On the group of form classes of large degree

S. A. Meshaik

Meshaik Seymur Arif ogly —PhD in mathematics, Ganja State University (Ganja, Azerbaijan).
e-mail: seymurmeshaik82@gmail.com

Abstract

Groups of form classes were introduced in Number Theory by Gauss, for binary quadratic forms. He defined the notions of equivalence and composition and introduced a group structure in classes of equivalence for the family of quadratic forms with discriminants not divisible by a square of integral number. Further investigations of Gauss were developed in various directions. One of them is a generalization of the theory to multivariate quadratic forms, in which widely studied questions on representation of integral numbers by various quadratic forms. Other direction concerns the notion of composition. But with the growth of the number of variables the question stands very difficult. In 1898, A. Hurwits showed that for quadratic forms with the number of variables greater than 8, it is hard to introduce suitable notion of composition. This result of A. Hurwits was explaned by Y. V. Linnik from non-associative algebras' point of a view. It is established that the notion of discriminant for forms of high degree is not so substantive as for quadratic forms. Sometimes, strict difference between forms having one and the same discriminant, is well known. To overcome these difficulties, it is convenient to consider forms connected with given extension of the field.

Keywords: groups, form classes, algebraic extensions, dedekind rings.

Bibliography: 9 titles.

For citation:
Meshaik, S. A. 2024, "On the group of form classes of large degree" , *Chebyshevskii sbornik*, vol. 25, no. 5, pp. 113–125.

1. Introduction

Groups of form classes were introduced in Number Theory by Gauss, for binary quadratic forms. He defined the notions of equivalence and composition and introduced a group structure in classes of equivalence for the family of quadratic forms with discriminants not divisible by a square of integral number. Further investigations of Gauss were developed in various directions.

One of them is a generalization of the theory to multivariate quadratic forms, in which widely studied questions on representation of integral numbers by various quadratic forms. Other direction concerns the notion of composition. But with the growth of the number of variables the question stands very difficult. In 1898, A. Hurwitz ([6]) showed that for quadratic forms the number of variables greater than 8, it is hard to introduce suitable notion of composition (see also [8-9]). This result of A. Hurwitz was explained by y. V. Linnik from non-associative algebras' point of a view ([7]).

It is established that the notion of discriminant for forms of high degree is not so substantive as for quadratic forms. Sometimes, strict difference between forms having one and the same discriminant, is well known ([5]). To overcome these difficulties, it is convenient to consider forms connected with given extension of the field.

One of mostly studied questions of Number Theory is a question on representation of natural numbers by quadratic forms. Simplest problem of such category serves the Pell equation [1-2, 5]:

$$x^2 - 2y^2 = 1.$$

The form $F(x, y) = x^2 - 2y^2$ in the left hand side can not be represented as a product of two linear forms over the field of rational numbers. Easily this may be proved supposing contrary. Really, let we have, for some rationlal numbers a and b:

$$x^2 - 2y^2 = (x - ay)(x - by) = x^2 - (a + b)xy + aby^2;\ a, b \in \mathbf{Q}.$$

It is obvious that $a = -b$ and $ab = -a^2 = -2 \Rightarrow a^2 = 2$. But this is impossible. The obtained contradiction gives the result.

Despite that, the fact on decomposability of this form into two linear forms over the field of real numbers plays important role:

$$F(x,y) = (x - \sqrt{2}y)(x + \sqrt{2}y).$$

Definition. The form $F(x_1, ..., x_n)$ in n variables is called a decomposable form if it can be factorized into linear forms in some extension of the field of rational numbers $E/\mathbf{Q}$.

As an example of decomposable forms in two variables it can be taken any form of a view

$$F(x,y) = a_0x^n + a_1x^{n-1}y + \cdots + a_ny^n$$

with rational coefficients. It is obvious that if the polynomial

$$F(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n$$

have roots $\alpha_1, ..., \alpha_n$, then the considered form can be written as follows:

$$F(x,y) = a_0(x - \alpha_1 y)\cdots(x - \alpha_n y).$$

2. Normal form (principle form)

Let a polynomial $F(x)$ be irreducible over a field $\boldsymbol{K}$. Then the extension $\boldsymbol{K}(\alpha)$ of the field by joining of some its root is an simple extension of degree n. Since the polynomial $F(x)$ is irreducible, then it has not repeated roots. From the theory of matrices [3, 10-15] it is known that in some extension $\boldsymbol{E/K}$ of the field $\boldsymbol{K}$ the matrix

$$A = \begin{pmatrix} 0 & 0 & \cdots & -a_n \\ 1 & 0 & \cdots & -a_{n-1} \\ 0 & 0 & \cdots & -a_{n-2} \\ \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & \cdots & 1 - a_1 \end{pmatrix}$$

is similar to diagonal matrix, that is

$$A = L\Lambda L^{-1},$$

and the matrix Λ is a diagonal matrix with diagonal entries $\alpha_1, \ldots, \alpha_n$. Then we have:

$$\Phi(c_0, c_1, ..., c_{n-1}) = \det C_0 + C_1A + \cdots + C_{n-1}A^{n-1}) =$$

$$= \det(LL^{-1}) \det(C_0I + C_1A + \cdots + C_{n-1}A^{n-1});\ C_i = diag\{c_i, ..., c_i\}.$$

It is clear that using properties of determinants, we can write:

$$\Phi(c_0, c_1, ..., c_{n-1}) = \det(C_0I + C_1A + \cdots + C_{n-1}A^{n-1}) =$$

$$= \prod_{i=1}^{n} \left(c_0 + c_1\alpha_i + ... + c_{n-1}\alpha_i^{n-1}\right).$$

The expression in the last right hand side is called a norm of the element α. As it is obvious, the equality

$$\Phi(c_0, c_1, ..., c_{n-1}) = 0$$

is possibly then and only then when for some root α_i of the polynomial $F(x)$ we have

$$c_0 + c_1\alpha_i + ... + c_{n-1}\alpha_i^{n-1} = 0.$$

From here one derives:

$$c_0 = c_1 = ... = c_{n-1} = 0.$$

So,

$$c_0 = c_1 = ... = c_{n-1} = 0 \Leftrightarrow N(\xi) = 0;$$

here $\xi = c_0 + c_1\alpha + ... + c_{n-1}\alpha^{n-1}$ and $N(\xi)$ denotes the norm of the element ξ. Since

$$N(\xi) = \det(C_0 I + C_1 A + \cdots + C_{n-1}A^{n-1}),$$

then the equality $N(\xi) = 0$ is equivalent to the equality

$$\det(C_0 I + C_1 A + \cdots + C_{n-1}A^{n-1}) = 0.$$

Isomorphism $F(\alpha) \cong F(A)$ shows that we again must have $c_0 = c_1 = ... = c_{n-1} = 0$.

Suppose now the equation

$$\Phi(c_0, c_1, ..., c_{n-1}) = 0$$

has trivial zero solutions only. To show that the polynomial $F(x)$ is irreducible, suppose the contrary. Let there exist polynomials $g(x)$ and $h(x)$ such that $F(x) = g(x)h(x)$, with $degg(x) \geq 1$ and $degh \geq 1$. Then, $g(\alpha) = 0$ and the isomorphism $F(\alpha) \cong F(A)$ shows that $g(A) = 0$. Therefore, if the numbers $g_0, \ldots, g_k, k < n$ are coefficients of the polynomial $g(x)$, then taking

$$c_0 = g_0, \ldots, c_k = g_k, c_{k+1} = 0, \ldots, c_{n-1} = 0,$$

we get: $\Phi(c_0, c_1, ..., c_{n-1}) = N(g(A)) = 0$. That means that the equation $\Phi(c_0, c_1, ..., c_{n-1}) = 0$ has non-trivial solution. But this contradicts the isomorphism $F(\alpha) \cong F(A)$, because in consent with this isomorphism we must have

$$g(\alpha_i) = c_0 + c_1\alpha_i + ... + c_{k-1}\alpha_i^{k-1} = 0,$$

for some index i. Therefore, denoting by $\varphi(x)$ a minimal polynomial of this element we see that $g(x) \vdots \varphi(x)$ which shows that the polynomial $F(x)$ is decomposable.

So, we have established the statement.

Theorem 1. For decomposability of a polynomial $F(x) = a_0x^n + a_1x^{n-1} + \cdots + a_n \in \boldsymbol{K}[x]$ it is necessary and sufficient that the homogeneous polynomial in n variables $c_0, c_1, ..., c_{n-1}$

$$\Phi(c_0, c_1, ..., c_{n-1}) = \det(C_0 + C_1 A + \cdots + C_{n-1}A^{n-1})$$

has in the field $\mathbf{K}$ non-trivial roots.

The form defined in Theorem 1 is called a normal form. We shall call it as a principle form also. The normal form is a decomposable form.

3. Criteria for divisibility by a prime ideal

Definition 1. Let $\mathbf{K}$ be some algebraically closed field, and $\alpha_1, ..., \alpha_n$ be some its elements. The set of all linear combinations with coefficients in $\mathbf{K}$ is called a module in the field $\mathbf{K}$. The numbers $\alpha_1, ..., \alpha_n$ are called the generators of the module.

One and same module can be defined by different generators. The module is denoted as $M = \{\alpha_1, ..., \alpha_n\}$, using generators.

Definition 2. Two modules M and M_1 are called similar, if for some element $\alpha \in \mathbf{K}$ the equaity $M_1 = \alpha M$ is satisfied.

The norm $N(c_1\alpha_1 + ... + c_n\alpha_n)$ of the element $c_1\alpha_1 + ... + c_n\alpha_n$ is a form which we call to be form connected to the module M.

Definition 3. If the module M given in algebraic extension $\mathbf{K}$ of the field of rational numbers degree n contains n elements linearly independent over the field of rational numbers, is called to be full module, otherwise this module is called non-full module.

The form connected to full module is called full form, otherwise it is called non-full form. For example, the numbers $1, \sqrt[3]{2}, \sqrt[3]{4}$ form a basis of the field $\mathrm{Q}(\sqrt[3]{2})$. By this reason the form below is a full form:

$$N(x + y\sqrt[3]{2} + z\sqrt[3]{4}) = x^3 + 2y^3 + 4z^3 - 6xyz.$$

But the form $F(x, y, z) = x^3 + 2y^3$ is non-full, which can be derived from the full form by taking z=0.

Studying of ideals and their properties are exclusively valuable for applications to the theory of Diophantine equations. This is caused by the uniqueness of decomposition of ideals in the ring of integral elements of the number field into the product of prime ideals. However, in applications it arises a problem of extracting necessary consequences concerning integral elements of the field, often. This is a difficult question the decision of which depends on properties of the group of ideals' classes. This idea which for the first time has been found by Kummer E. E. (in the terms of ideal complex numbers), was further developed by efforts of the subsequent generations of researchers, and has led to the creation of the modern theory of algebraic numbers. The questions related to the history of the problem is possible be found in [1-2]. We will adhere basically everywhere throughout the paper the notions and designations from [4]. Some properties of the ideals connected with the divisibility is possible to interpret in the language of congruencies for the elements of the basic field, and often this stands useful in a concrete case.

Let we are given with some Dedekind field $\mathbf{K}$ with a ring of integral elements K. κ is an algebraic extension of the field $\mathbf{K}$: $\kappa = \mathbf{K}(\theta)$, where $\theta \in \kappa$ is a primitive element with a minimal polynomial

$$f(x) = x^n + a_1x^{n-1} + \cdots + a_n,\ a_i \in K.$$

Let's assume that the natural basis generated by the powers of this element is fundamental, that is, the module generated by this basis coincides with K. Then, each element of a kind

$$\alpha = c_{n-1}\theta^{n-1} + \cdots + c_1\theta + c_0,\ c_i \in K$$

is an integral element of the field κ, and on the contrary, each integral element has the specified representation. We shall designate the set of all integral elements of the field κ by K'. Kummer had proved the following theorem.

Theorem 2. The decomposition of the prime ideal ρ of the ring K runs in κ parallel in every respect to the decomposition of $f(x)$ in K_ρ.

The theorem 1 means that if over the field K_ρ the polynomial $f(x)$ has a factorization

$$f = \varphi_1^{e_1} \cdots \varphi_g^{e_g},$$

or in congruencies

$$f(x) \equiv \varphi_1^{e_1} \cdots \varphi_g^{e_g} (mod\rho), \tag{1}$$

where the polynomials $\varphi_1, ..., \varphi_g$ are irreducible $(mod\rho)$, then the ideal ρ is decomposable over the κ into the product of prime ideals

$$\pi_i = (\rho, \varphi_i(\theta)), i = 1, ..., g$$

as follows:

$$\rho = \pi_1^{e_1} \cdots \pi_g^{e_g},$$

and degree of an ideal π_i is equal to the degree of corresponding polynomial $\varphi_i(x)$ (see [4, p. 83,] or [5, p. 267]). From here we receive a criterion for divisibility of an element by the prime ideal π_i:

Consequence 1. For divisibility of an element

$$\alpha = c_0 + c_1\theta + \cdots + c_{n-1}\theta^{n-1}$$

by the prime ideal π_i it is necessarily and sufficient that the polynomial

$$\alpha(x) = c_0 + c_1 x + \cdots + c_{n-1}x^{n-1}$$

was divisible by $\varphi_i(x)$ over the field K_ρ.

It is possible to give a "numerical analogue"of this statement useful in concrete applications. For the formulation of this analogue we shall write down $\varphi(x) = \varphi_i(x)$ as

$$\varphi(x) = x^r + b_1 x^{r-1} + \cdots + b_r;\ b_1, ..., b_r \in K$$

and form on a companion matrix

$$B = \begin{pmatrix} 0 & 0 & \cdots & 0 & -b_1 \\ 1 & 0 & \cdots & 0 & -b_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -b_r \end{pmatrix}$$

of order r. Under the theorem of Keyley and Hamilton we have $\varphi(B) = 0$. Since the polynomial φ is indecomposable then it will be a minimal polynomial for B over the field K_ρ. By the property of the minimal polynomial and the theorem of Kummer the following relation is satisfied.

Consequence 2. Following relation is true:

$$\alpha \vdots \pi_i \Leftrightarrow c(B) \equiv 0(mod\rho).$$

Let α be an algebraic number with minimal polynomial

$$f(x) = x^n + b_1 x^{n-1} + \cdots + b_n.$$

Every element of the ring $Z[\alpha]$ can be written as an expression

$$c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

with integral coefficients. Suppose that π is a prime ideal of degree 1: $N(\pi) = p$. From the theory of algebraic numbers it is best known that the number $c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$ is divisible by π iff

$$c_0 + c_1 a + c_2 a^2 + \cdots + c_{n-1}a^{n-1} \equiv 0(modp);$$

here the number a is a solution of the congruence $f(a) \equiv 0(modp)$.

4. Group of units

Two integral algebraic numbers of Dedekind fields with equal norms differ each from other by multipliers with the norm 1. Elements of the norm 1 set up a group which is called a group of units. The structure of this group is settled by the theorem of Dirichlet. To introduce the Dirichlet's theorem, let us consider some auxiliary geometric constructions.

Consider some algebraic extension $\mathbf{K}$ of degree n of the field of rational numbers. Then, by Fundamental Theorem of Algebra, this extension has n various isomorphisms in the field of complex numbers.

Definition 1. If image of an isomorphism $\sigma : \mathbf{K} \to \mathrm{C}$ is a subset of real numbers then it called real isomorphism, otherwise it called complex isomorphism.

For example, if $\mathbf{K} = Q(\sqrt[3]{5})$ then an isomorphism $\theta \mapsto \sqrt[3]{5}$ is real (here $\theta^3 = 5$). But the isomorphism $\theta \mapsto \sqrt[3]{5}(\cos 2\pi/3 + i \sin 2\pi/3)$ is complex. Suppose that the isomorphism $\sigma : \mathbf{K} \to \mathrm{C}$ is real. Then the isomorphism $\bar{\sigma} : \mathbf{K} \to \mathrm{C}$ defined as

$$\bar{\sigma}(\alpha) = \overline{\sigma(\alpha)},\ \alpha \in \mathbf{K}$$

also is complex, which is called conjugate to σ.

Suppose that there is s real isomorphisms and $2t$ pairwisely conjugate complex ones. Construct some $s + 2t$ dimensional linear space with elements

$$(x_1, ..., x_s; x_{s+1}, ..., x_{s+t}),$$

where first s components are real, and others are complex numbers. This linear space will be a linear space of dimension $s+2t$ over the field of real numbers.

Definition 2. Let $e_1, \ldots, e_m$, $m \leqslant n$, be linearly independent elements of R^n. All of linear combinations of a view $a_1e_1 + \cdots + a_me_m$, with rational coefficients $a_1, \ldots a_m$, called a lattice in R^n. If $m = n$ then the lattice is called to be full, otherwise it called non-full.

The set of all linear combinations $a_1e_1 + \cdots + a_me_m$, with coefficients $a_1, \ldots a_m, 0 \leqslant a_i < 1$, is called to be fundamental parallelepiped of the lattice.

Lemma 1. In D there are units $\varepsilon_1, ..., \varepsilon_r,\ r \leqslant s + t - 1$ such that every unit ε of D is uniquely represented in the form

$$\varepsilon = \zeta\varepsilon_1^{\alpha_1} \cdots \varepsilon_r^{\alpha_r},$$

where $\alpha_1, ..., \alpha_r$ are rational numbers, and ζ is some root from 1 in D.

Lemma 2. Elements of full module M of the field K extension's degree of which is $n = s + 2t$, is represented as a lattice in the space R^n, the volume of fundamental parallelepiped of which is $2^{-t}\sqrt{D}$ (here D is a discriminant of the module M).

The basic result of the geometric theory is a theorem of Minkowski.

Lemma 3. Suppose that in n-dimensional space R^n is given some full lattice with the fundamental parallelepiped Δ. Then every central symmetric convex set X with the volume $v(X) \geqslant 2^n\Delta$ contains at least one point of the lattice different from the origin.

From this theorem, as a consequence we get the following statement.

Lemma 4. (Dirichlet's theorem). In every algebraic field K of degree $n=s+2t$, with module U of integral elements, there are $r = s + t - 1$ number of such units $\varepsilon_1, ..., \varepsilon_r$ that for every unit $\varepsilon \in U$ uniquely can be represented in the view

$$\varepsilon = \zeta\varepsilon_1^{\alpha_1} \cdots \varepsilon_r^{\alpha_r},$$

in which $\alpha_1, ..., \alpha_r$ are rational numbers, and ζ is a root from 1 in U.

5. Group of form classes

The basic result of the Gauss' theory of quadratic forms is that that the group of binary quadratic forms' classes is isomorphic to the ideal classes' group of quadratic ring. This fact can be taken as a principle argument in the issue on seeking of suitable generalization of the Gauss' theory. We put the following question. Let we are given with some Dedekind field k with a ring of integral elements K. Is it possible define a family of forms of degree being equal to the degree of field's extension, in which is possible introduce a group of form classes being isomorphic to the group of ideal classes of the given field? We establish that the answer to this question is positive. Main tool

in our investigations is the criteria of divisibility by a prime ideal given in Consequence 2. This criteria shows that in such sort of questions, as in the case of quadratic forms, essential role plays the fact on representability of prime ideals' norms by forms. Here, naturally it arises the family of forms closely connected with considered extension. The question, put above, is solvable in this family. The group of ideal classes seems very useful in the process of construction of the group of form classes. We suffice with consideration of the field of rational numbers as a basic field.

Let $K = Q(\alpha)$ be an algebraic extension of the field of rational numbers by joining of integral algebraic element α. A minimal polynomial of the element α denote as

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n.$$

This polynomial is irreducible over the field of rational numbers. Suppose that the numbers 1, α, $\alpha^2, ..., \alpha^{n-1}$ set up the fundamental basis, that is the maximal order is generated by natural basis. We have $K \cong Q(A)$.

Take some prime number p. Decomposition of prime number p in the field K, in consent with Kummer's theorem, runs in Z_p parallel in all respects to the decomposition

$$f(x) \equiv f_1(x) \cdots f_k(x)(modp). \tag{2}$$

Moreover, if the polynomial f_i has a degree k_i, then the expansion of the number p will be of form $p = \pi_1 \cdots \pi_k$, where π_i is a prime ideal of degree k_i. The norm of the prime ideal π_i equals to p^{k_i}.

Theorem 3. The number of ideal classes of field K is equal to 1, iff the norm of every prime ideal can be represented by Principle Form.

Proof. Suppose that the field K has only one class of ideals, that is, the maximal order D is a ring of principle ideals. Suppose that π is some prime ideal and its norm is equal to p^k. Then, there is an element $c(\alpha) \in D$ such that $\pi = (c(\alpha))$. So, we must have $\pi \backslash c(\alpha)$ and $c(\alpha) \backslash \pi$. It means that $N(c(\alpha)) = p^k$. Therefore, p^k is representable by Principle Form.

Suppose now that the norm of every prime ideal can be represented by Principle Form. Taking arbitrary prime number p consider its decomposition into the product of prime ideals:

$$p = \pi_1 \cdots \pi_k,$$

with $N(\pi_i) = p^{k_i}$. Then for each $i, i = 1, ..., k$ there is an element $c_i(\alpha) \in D$ such that $N(c_i(\alpha)) = p^{k_i}$. Therefore, taking an element $c(\alpha) = c_1(\alpha) \cdots c_k(\alpha)$ we have $N(c(\alpha)) = p^n$. By this reason, one has $p \backslash c(\alpha)$. Then $c(\alpha) = pe(\alpha)$ and $e(\alpha)$ is a unit. From unique decomposition of non-zero ideal by the product of prime ideals it follows that every prime ideal is defined by some element $c_i(\alpha)$. So, D is a ring of principle ideals. Theorem 3 is proved.

From multiplicatives of the norm it follows that if the field has more than 1 classes of ideals, then there exists such a prime ideal that its norm cannot be represented by Principle Form. Now the question is arising: is there a form which presents the norm of that ideal? Following theorem answers this question positively.

Theorem 4.The norm of every prime ideal can be represented by a form of degree n which is reduced from the Principle Form using some parameterization (linear transformation) of variables.

Proof.It is best known the fact that for every ideal π there is such an ideal τ that their product $\pi\tau$ is a principle ideal, that is, there exists an element $c(\alpha) = c_0 + \cdots + c_{n-1}\alpha^{n-1} \in D$ for which

$$\pi\tau = (c(\alpha)).$$

Suppose at first that τ is a prime ideal and its norm is q^k (q is a prime number). Assume also that in the decomposition (1) for the prime number q to the ideal τ corresponds the polynomial $g(x)$ of degree $\deg g = k$ and $g(x) = b_0 + \cdots + b_k x^k, b_k = 1$. In this case, by the criteria of divisibility by prime ideal, we must have

$$c(B) \equiv 0(modq), \tag{3}$$

where B is a companion matrix of the polynomial $g(x)$, that is

$$B = \begin{pmatrix} 0 & 0 & \cdots & -b_0 \\ 1 & 0 & \cdots & -b_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & b_{k-1} \end{pmatrix}.$$

Consider the congruence (3) as a system of linear equations over the field $\mathbf{Z}_q$ with respect to the coefficients $c_0, ..., c_{n-1}$. This is a homogeneous system and their solutions set up a subspace in the space $(Z_q)^n$. Suppose that the basis minor of the system's matrix is placed at first k rows and columns (note that the case when the systems' matrix has a rank 0 over the field $\mathbf{Z}_q$ is trivial, in which q is not decomposable). Then the variables $c_k, ..., c_{n-1}$ $(0 \leqslant k \leqslant n-1)$ are free and can take arbitrary values. Basic variables are $c_0, ..., c_{k-1}$. So, the general solution to the system (3) is as follows:

$$c_i \equiv \sum_{j=k}^{n-1} b_{ij} c_j (mod q); i = 0, ..., k-1.$$

Replace this system of congruences by a system of equalities, adding the multipliers of modulus as below:

$$c_i = \sum_{j=k}^{n-1} b_{ij} c_j + q t_i; t_i \in Z, i = 0, ..., k-1.$$

Substituting the values of the coefficients in the expression for $c(A)$ and taking the determinant, we get some form of variables $t_0, ..., t_{k-1}, c_k, ..., c_{n-1}$.

As it is known ([3]), the matrix A is possible to reduce to natural normal form over the field $\mathbf{Z}_q$ and in diagonal will stay blocks of a view B. Since in the diaconal stays the block B then $\det c(A)$ is divisible by q^k. As it seen from the said above, this relation is satisfied for all possible values of variables $t_0, ..., t_{k-1}, c_k, ..., c_{n-1}$. It means that the coefficients of the last form are divisible by q^k. After of division the form by q^k we get a new form. Taking specified values of coefficients, we have

$$N(\pi\tau) = N(\pi) q^k = N(c(\alpha)).$$

So, the equality

$$N(\pi) = q^{-k} N(c(\alpha))$$

is satisfied for some non-zero values of variables $t_0, ..., t_{k-1}, c_k, ..., c_{n-1}$. It means that the theorem 4 is established for the case of prime ideal τ.

Consider now the case when τ is a square of prime ideal, that is

$$\pi\tau^2 = (c(\alpha)),$$

fore some $c(\alpha) = c_0 + \cdots + c_{n-1}\alpha^{n-1} \in D$. Taking the congruence (3) with respect to the modulus q^2, let us investigate the congruence

$$c(B) \equiv 0 (mod q^2).$$

We will seek the solutions among the solutions of the congruence (3). We have found the general its solution

$$c_i = \sum_{j=k}^{n-1} b_{ij} c_j + q t_i; t_i \in Z, i = 0, ..., k-1. \tag{4}$$

Rewrite the congruence as below

$$B_1 \bar{c}_1 + q B_2 \bar{c}_2 \equiv 0 (mod q^2), \tag{5}$$

where the block matrix $(B_1|B_2)$ is an initial matrix of the congruence (3), $\bar{c}_1 = (c_0, \cdots, \bar{c}_{k-1}), \bar{c}_2 = = (c_k, \cdots, \bar{c}_{n-1})$. Since the vector $\bar{c} = (\bar{c}_1, \bar{c}_2)$ found in (4) is a solution of the system (3), then the solution of the system (5) we shall seek in the form

$$\bar{c}_2 = \bar{t}_1 + q\bar{t}_2.$$

Substituting into (5) and reducing we find:

$$B_1\bar{c}_1 + qB_2\bar{t} + q^2B_2\bar{t}_2 \equiv 0(modq^2).$$

We have $B_1\bar{c}_1 \equiv 0(\mathrm{mod}q)$ and note that the matrix B_1 has a block-view

$$\begin{pmatrix} M \\ N \end{pmatrix},$$

where M is a basic minor above. By this reason all of its elements are not divisible by q, so,

$$\bar{c}_1 \equiv M^{-1}B_2\bar{c}_2(\mathrm{mod}q).$$

But elements of the block N are divisible by q and $N{=}qN_1$. So, after of reducing we find a new system:

$$\tilde{B}_1\bar{x}_1 + B_2\bar{t} + qB_2\bar{t}_2 \equiv 0(modq),$$

or

$$\tilde{B}_1\bar{x}_1 + B_2\bar{t} \equiv 0(modq).$$

We again arrived at the congruence (3) but with different main matrix and basic minor. The solution of this system can be found as above. Note that

$$\tilde{B}_1 = \begin{pmatrix} M \\ N_1 \end{pmatrix},$$

and $\bar{x}_1 = \bar{c}_1$. Using the method of bordering, we can find a basic minor of the matrix $(\tilde{B}_1, B_2)$ over the field $\mathbf{Z}_q$, and continue solving of the the last congruence. The vector $\bar{x}_1$ of basic variables can increase the number of its components. So, linear parameterization is more complicated in this case, but we have find a new paramterization, and substituting found values of the coeffients in the expression for $c(A)$ and taking the determinant, we get new form which represents the norm of the ideal π:

$$N(\pi) = q^{-2k}N(c(\alpha)),$$

becaus in the relation $\pi\tau^2 = (c(\alpha))$ both sides are divisible by τ^2. Theorem 4 is proved in the case of τ^2. Analogical reasonings allows the complete proof in the case of arbitrary degree of the ideal τ.

Completion of Theorem based on the Chines theorem on reminders. Let $\tau = \tau_1^{k_1} \cdots \tau_m^{k_m}$ is a decomposition into the product of prime ideals. Then the congruence (3) is equivalent to the system of congruences

$$c(B) \equiv 0(modq_j^{s_j}),\ j = 1, ..., m.$$

Applying Chines theorem on reminders we find general solution of the congruence

$$c(B) \equiv 0(modq_1^{s_1} \cdots q_m^{s_m}),$$

which delivers a needed parameterizations also. The representation of the norm of the ideal π we find now from the relation

$$N(\pi) = (N(\tau))^{-1}N(c(\alpha)).$$

Theorem 4 is completely proved.

Consequence. The norm of every ideal is representable by some form, got from the Principle Form by some parametrization.

As it is seen the forms which reduced from the Principle Form by parameterizations plays an important role. For every prime ideal τ, as above, we can construct the form

$$\Psi(t_0, ..., t_{n-1}) = q^{-ks} \det c(A), \tag{6}$$

where k is a degree of prime ideal τ and s is its multiplicity. Denote by $\mathbf{F}_n(\alpha)$ the set of all forms got by this way. Let introduce in $\mathbf{F}_n(\alpha)$ an equivalence relation.

Suppose that $a(\alpha) \in D$ is an element of maximal order D. Consider transformation of Principle Form by this element as follows. At first define usual product $a(A)t(A)$. We find a sum $u_0 + u_1 A + \cdots + u_{n-1}A^{n-1}$ in which every variable u_i is a linear combination of variables $t_0, ..., t_{n-1}$. Therefore, $\det(a(A)t(A)$ will be some form. Denote this form as $a * F$.

Definition. Two forms F_1 and F_2 we call to be equivalent and denote as $F_1 \sim F_2$ if for some elements $a(\alpha)$ and $b(\alpha)$ the equality $a * F_1 = b * F_2$ is satisfied, that is

$$\det(a(A)t_1(A)) = \det(b(A)t_2(A)).$$

Lemma 5. The relation $F_1 \sim F_2$ is an equivalence relation.

Proof. It is clear that $F_1 \sim F_1$. Also, if $F_1 \sim F_2$, then $F_2 \sim F_1$. Suppose $F_1 \sim F_2$ and $F_2 \sim F_3$. Prove that $F_1 \sim F_3$. We have

$$\det(a(A)t_1(A)) = \det(b(A)t_2(A))$$

and

$$\det(c(A)t_2(A)) = \det(d(A)t_3(A)).$$

Then

$$\det(b(A)c(A)t_2(A)) = \det(b(A)d(A)t_3(A)) = \det(c(A)a(A)t_1(A)).$$

This relation shows that $F_1 \sim F_3$. Lemma 5 is proved.

Theorem 5.If the form F_1 represents the norm of the prime ideal π then this form represents the norm of every ideal equivalent to π.

Proof. Let the norm of the ideal π is representable by the form F_1. Then there exists an ideal τ and element $c(\alpha)$ such that $\pi\tau = (c(\alpha))$. Denote by π' some ideal equivalent to π. We can find such two elements $a(\alpha)$ and $b(\alpha)$ that

$$a(\alpha)\pi = b(\alpha)\pi'. \tag{7}$$

Then,

$$a(\alpha)c(\alpha) = a(\alpha)\pi\tau = b(\alpha)\pi'\tau.$$

Left hand side is divisible by $b(\alpha)$, and reducing we get the relation

$$\pi'\tau = (h(\alpha))$$

Repeating the conclusions of Theorem 2 we find, in some values of variables:

$$Nm\pi' = q^{-k} \det(t(A)).$$

Theorem 5 is proved.

Theorem 6.If the form F_1 defined as (6) represents some natural number m then every form $F_2 \sim F_1$ also represents the number m.

Proof of this theorem easily follows from definition and the relation (7).

Obtained above results is applicable to various questions of Number Theory. We have seen that the representability of the norm of ideal is substantive for the theory of form developed here. As we observed above, representability the norm of the prime ideal is a fact closely connected with the structure of the field. The norm of the ideal is representable by forms of a class simultaneously. In other hand, by Theorem 3, one and the same form represents the norm of every ideal equivalent to given one. So, there is a natural correspondence between classes of forms and ideals. This correspondence is possible to extend to the group structure. It is natural to take as a product of two forms as a form which represents the norm of the product of taken ideals. Let us show that the notion of the product defined by such way is defined correctly and the set of form classes defined above sets up a group.

Suppose that we are given with two forms: F_1 and F_2. There are such classes of ideals that the norms of their elements are representable respectively by forms F_1 and F_2. Denote them by π_1 and π_2. As we have established above, there exists a form F such that it represents the norm of the product $\pi_1\pi_2$. In the set $\mathbf{F}_n(\alpha)$ of forms, introduce the product $F_1 * F_2$ of forms by equality $F = F_1 * F_2$. By Theorems 5 and 6, from $F_2 \sim F_3$ it follows that $F_1 * F_2 \sim F_1 * F_3$. So, the operation of multiplication is defined correctly. Namely, the product of form classes includes all of products of equivalent forms of corresponding classes. So, the factor group $\mathbf{F}_n(\alpha)/\sim$ is correctly defined and includes the classes of forms reduced from Principle Form.

Resuming the all of said above we can formulate our basic result.

Theorem 7. The group $\mathbf{F}_n(\alpha)/\sim$ of form classes is isomorphic to the group of ideal classes.

6. Conclusion

In the section 5 we have introduced the group structure in the family of form classes. All of forms are reduced from the principle form by linear parametrization. The constructed group is isomorphic to the group of ideal classes.

СПИСОК ЦИТИРОВАННОЙ ЛИТЕРАТУРЫ

1. Эдвардс, Х. М. Последняя теорема Ферма: Общее введение в алгебраическую теорию чисел. Нью-Йорк: изд-во «Шпрингер», 1977.

2. Постников М. М. Введение в теорию алгебраических чисел // 1982.- М: Наука.

3. Мальцев И. А. Линейная алгебра: 2-е изд. // СПб: изд-во «Лань».- 384 с.

4. Вейль Х. Алгебраическая теория чисел // Издательство Принстонского университета.- 1940.- 225 с.

5. Боревич З.И., Шафаревич И.Р. Теория чисел: 2-е изд. // М:Наука.- 1972.

6. Гурвиц А. О композиции квадратичных форм больших чисел переменных // Новости Геттингена.- 1898.- С. 309–316.

7. Линник Ю. В. Обобщение теоремы Фребебиуса и установление связи с теоремой Гурвица о композиции квадратичных форм // Изв. Акад. Наук СССР, сер.математика.- 1938.- Т.2.- С. 41–52.

8. Альбурт А. Квадратичные формы, разрешающие композицию // Анналы Математики.- 1942.- Т. 43.- № 1.- С. 161–177.

9. Дубиш Р. Композиция квадратичных форм // Анналы Математики.- 1946.- Т.47.- № 3.- С. 510–527.

10. Кострикин А.И. Введение в алгебру // М:Наука.- 2009.- 495 с.

11. Ленг К. Алгебра // М:Мир.- 1968.- 564 с.

12. Гельфанд И. М. Лекции по линейной алгебре // М:Наука.- 1971.- 271 с.

13. Мальцев А. И. Основы линейной алгебры // М: Наука.- 2005.- 470 с.

14. Бурбаки Н. Коммутативная алгебра // М: Мир.- 2000.

15. Родосский К. А. Алгоритм Евклида // М: Наука.- 1988.

REFERENCES

1. Edwards, H. M. 1977, "The Last Theorem of Fermat: A General Introduction to Algebraic Number Theory", *Springer*, New York.

2. Postnikov, M. M. 1982, "Introduction to the Theory of Algebraic Numbers", *Nauka*, Moscow.

3. Mal'tsev, I. A. "Linear Algebra: 2nd ed.", *Lan*, St. Petersburg. 384 p.

4. Weil, A. 1940, "Algebraic Number Theory", *Princeton University Press*. 225 p.

5. Borevich, Z. I. and Shafarevich, I. R. 1972, "Number Theory: 2nd ed.", *Nauka*, Moscow.

6. Gurwitz, A. 1898, "On the composition of quadratic forms of large numbers of variables", *News of Göttingen*, pp. 309–316.

7. Linnik, Yu. V. 1938, "Generalization of the Frobenius theorem and establishing a connection with Hurwitz's theorem on the composition of quadratic forms", *Izvestiya of the Academy of Sciences of the USSR, Series Mathematics*, 2, pp. 41–52.

8. Alburt, A. 1942, "Quadratic forms allowing composition", *Annals of Mathematics*, 43(1), pp. 161–177.

9. Dubish, R. 1946, "Composition of quadratic forms", *Annals of Mathematics*, 47(3), pp. 510–527.

10. Kostrikhin, A. I. 2009, "Introduction to Algebra", *Nauka*, Moscow. 495 p.

11. Lang, S. 1968, "Algebra", *Mir*, Moscow. 564 p.

12. Gelfand, I. M. 1971, "Lectures on Linear Algebra", *Nauka*, Moscow. 271 p.

13. Mal'tsev, A. I. 2005, "Foundations of Linear Algebra", *Nauka*, Moscow. 470 p.

14. Bourbaki, N. 2000, "Commutative Algebra", *Mir*, Moscow.

15. Rodossky, K. A. 1988, "Euclid's Algorithm", *Nauka*, Moscow.

Получено: 22.06.24
Принято в печать: 26.12.2024