Записки научных
семинаров ПОМИ
Том 394, 2011 г.

A. L. Glazman, P. B. Zatitski, A. S. Sivatski, D. M. Stolyarov

FORMS OF HIGHER DEGREE OVER CERTAIN FIELDS

Abstract. Let F be a nonformally real field, n, r positive integers. Suppose that for any prime number $p \leq n$ the quotient group F^*/F^{*p} is finite. We prove that if N is big enough, then any system of r forms of degree n in N variables over F has a nonzero solution. Also we show that if in addition F is infinite, then any diagonal form with nonzero coefficients of degree n in $|F^*/F^{*n}|$ variables is universal, i.e. its set of nonzero values coincides with F^*.

In contrast to the well developed algebraic theory of quadratic forms the theory of forms (homogeneous polynomials in several variables) of higher degree over fields is in rudimentary condition, and *the most of the known results here are rather scattered and depend* on the structure of the ground field. However, certain notions and definitions from the theory of quadratic forms make sense in the higher degree setting. Let F be a field. The number of variables of a form ϕ over F is called the dimension of ϕ. The form $a_1x_1^n + \cdots + a_mx_m^n$ in variables $x_1, \ldots, x_m$ is called diagonal and denoted by $\langle a_1, \ldots, a_m\rangle$ (if there is no ambiguity about the degree n). The form $\langle \lambda, \ldots, \lambda\rangle$ of dimension m is denoted by $m\langle\lambda\rangle$. If ϕ and ψ are forms of the same degree whose sets of variables do not intersect, we denote the sum $\phi + \psi$ by $\phi \perp \psi$. If ϕ is a form, by $D(\phi)$ we mean the set of nonzero values of ϕ. The form ϕ of dimension m over the field F is said to be isotropic if there exists a nonzero row $(a_1, \ldots, a_m) \in F^m$ such that $\phi(a_1, \ldots, a_m) = 0$ and anisotropic otherwise. The form ϕ is called universal if $D(\phi) = F^*$, i.e. any nonzero element of F is a value of ϕ. Following [3], we denote by $v_{d,r} = v_{d,r}(F)$ the smallest number, such that each system of r forms of degree d in more that $v_{d,r}$ variables has a nonzero solution, and write $v_{d,r} = \infty$ otherwise. Put $v_d = v_{d,1}$. For example, if k is an algebraically closed field and F/k is an extension of transcendental degree i (more generally, if F is a C_i-field), then $v_{d,r} \leq rd^i$ ([4, Ch. 2, Th. 15.8]). Define the number $\phi_d = \phi_d(F)$ similarly to v_d, except that in this case only diagonal forms are considered.

Key words and phrases: field, scalar product, system of equations, polynomial.

It has been proved in [1] that $v_{d,r}$ is finite provided $v_2, v_3, \dots, v_d$ are. On the other hand, later in [3] it has been shown that for any d and r there is a quantative upper bound for v_d via $\phi_2, \phi_3, \dots, \phi_d$. More precisely, $v_2 \leq 2\phi_2$, and if $d \geq 3$ and each of $\phi_2, \dots, \phi_d$ is finite, then $v_d \leq v_2 v_3^2 \dots v_{d-1}{}^{2^{d-3}} (2\phi_d)^{2^{d-2}}$ ([3, Th. 2]). Combining these results, we get that $v_{d,r}$ is finite provided $\phi_2, \phi_3, \dots, \phi_d$ are. This stimulates our interest in fields with finite ϕ_i. Obviously, if F is formally real (i.e. -1 is not a sum of squares), then $\phi_d = \infty$ for any even d. By this reason in the sequel we will consider only nonformally real fields.

We start with the following

Proposition 1. *Let F be an infinite nonformally real field, n a positive integer. If the group F^*/F^{*n} is finite, then any diagonal form with nonzero coefficients over F of degree n and dimension $|F^*/F^{*n}|$ is universal.*

Proof. We will need a few lemmas. The first of them (Lemma 2 below) is of some independent interest. Surprisingly enough, although the statement in this lemma is purely algebraic, its proof is not completely algebraic. Namely, at certain point we apply integration over the unit sphere in $\mathbb{R}^m$, which makes the proof not quite constructive.

Following the well-known definition of nonformally real field, we say that a commutative ring R is nonformally real, if there exist a positive integer l and $b_1, \dots, b_l \in R$ not simultaneously zero such that $b_1^2 + \dots + b_l^2 = 0$.

Lemma 2. *Let R be a nonformally real commutative ring. Then for any positive integer n there exist a positive integer m and $a_1, \dots, a_m \in F$ not simultaneously zero such that $a_1^k + \dots + a_m^k = 0$ for any $1 \leq k \leq n$.*

Proof. We will call the system of equations in the statement of the lemma the power system and argue by induction on n. Let $b_1, \dots, b_l \in R$ be not simultaneously zero elements such that

$$b_1^2 + \dots + b_l^2 = 0.$$

Notice that the row $(b_1, \dots, b_l, -b_1, \dots, -b_l)$ is a solution of the power system for $n = 2$.

Assume that the lemma is true for some $n - 1 \geq 2$ and $a_1, \dots, a_m \in R$ is a solution of the power system for $n-1$. If n is odd, then similarly to the case $n = 2$ the row $(a_1, \dots, a_m, -a_1, \dots, -a_m)$ is a solution of the power system for n. Now assume that n is even. For all $1 \leq i \leq n$ consider the polynomials

$$f_i(x_1,\dots,x_m,t_1,\dots,t_m) = \sum_{\pi\in S_m}(x_1t_{\pi(1)}+\cdots+x_mt_{\pi(m)})^i \in \mathbb{Z}[x_1,\dots,x_m,t_1,\dots,t_m],$$

where $x_1,\dots,x_m,t_1,\dots,t_m$ are indeterminates, and S_m is the permutation group on the set $\{1,\dots,m\}$. This polynomial is symmetric with respect to the variables $x_1,\dots,x_m$, hence there exists a positive integer r such that for each $1\le i\le n$

$$rf_i(x_1,\dots,x_m,t_1,\dots,t_m) = g_i(t_1,\dots,t_m)s_n + h_i(s_1,\dots,s_{i-1}), \qquad (*)$$

where g_i and h_i are polynomials over $\mathbb{Z}$ and $\mathbb{Z}[t_1,\dots,t_m]$ respectively, and $s_i = x_1^i+\cdots+x_m^i$. Substituting $a_1,\dots,a_m$ for $x_1,\dots,x_m$, and taking into account that $s_i(a_1,\dots,a_m)=0$ for each $1\le i\le n-1$, we get from $(*)$

$$r\sum_{\pi\in Sm}(a_1t_{\pi(1)}+\cdots+a_mt_{\pi(m)})^n = rf_n(a_1,\dots,a_m,t_1,\dots,t_m) = g_n(t_1,\dots,t_m)(a_1^n+\cdots+a_m^n).$$

Suppose for a moment that there exist $\widetilde{t}_1,\dots,\widetilde{t}_m\in\mathbb{Z}$ such that $g_n(\widetilde{t}_1,\dots,\widetilde{t}_m)<0$. Let $g_n(\widetilde{t}_1,\dots,\widetilde{t}_m)=-u$. Notice that for any $1\le i\le n-1$

$$r\sum_{\pi\in Sm}(x_1\widetilde{t}_{\pi(1)}+\cdots+x_m\widetilde{t}_{\pi(m)})^i\in\mathbb{Z}[s_1,\dots,s_i],$$

hence

$$r\sum_{\pi\in Sm}(a_1\widetilde{t}_{\pi(1)}+\cdots+a_m\widetilde{t}_{\pi(m)})^i=0.$$

Therefore, we have

$$r\left(\sum_{\pi\in Sm}(a_1\widetilde{t}_{\pi(1)}+\cdots+a_m\widetilde{t}_{\pi(m)})^i\right)+u(a_1^i+\cdots+a_m^i)=0$$

for $1\le i\le n$, which gives a representation of zero as a sum of $rm!+um$ not simultaneously zero kth powers, completing the induction step.

Thus, it remains to find $\widetilde{t}_1,\dots,\widetilde{t}_m\in\mathbb{Z}$ such that $g_n(\widetilde{t}_1,\dots,\widetilde{t}_m)<0$. To do this consider the function $p(x)=\int\limits_{t\in S^{m-1}}(x,t)^n dt$ on $\mathbb{R}^m$, where $x=(x_1,\dots,x_m)$, and (x,t) is the scalar product of x and t as elements of

$\mathbb{R}^m$. Obviously, p is homogeneous of degree n and constant on the sphere S^{m-1}. Hence

$$p(x_1,\dots,x_m) = c(x_1^2+\dots+x_m^2)^{\frac{n}{2}} = cs_2^{\frac{n}{2}}$$

for some $c>0$ depending only on m and n. It follows from $(*)$ that

$$cm!s_2^{\frac{n}{2}} = \int\limits_{t\in S^{m-1}} f_n(x,t)dt = r^{-1}s_n \int\limits_{t\in S^{m-1}} g_n(t)dt + \sum_{i=1}^{n-1} q_i \qquad (**)$$

for some $q_i \in \mathbb{Q}[s_1,\dots,s_{n-1}]$. Since the representation of any symmetric polynomial in $x_1,\dots,x_m$ as a polynomial in s_i is unique, we obtain from $(**)$ that

$$\int\limits_{t\in S^{m-1}} g_n(t)dt = 0.$$

Obviously, g_n is not identically zero

$$(\text{for example, } \ g_n(1,0,\dots,0) = (m-1)!),$$

which implies that there exist $\widetilde{t}_1,\dots,\widetilde{t}_m \in \mathbb{R}^m$ such that $g_n(\widetilde{t}_1,\dots,\widetilde{t}_m) < 0$. Since $\mathbb{Q}$ is dense in $\mathbb{R}$ and g_n is continuous, we can assume that $(\widetilde{t}_1,\dots,\widetilde{t}_m) \in \mathbb{Q}^m$. Moreover, since g_n is homogeneous, we can assume that $(\widetilde{t}_1,\dots,\widetilde{t}_m) \in \mathbb{Z}^m$, which finishes the proof. □

Lemma 3. *Let n be a positive integer and F a field such that -1 is a sum of a few nth powers of elements of F. Then the subset $F_0 \subset F$ consisting of all finite sums of nth powers of elements of F is a subfield of F.*

Proof. Obviously, $0,1\in F_0$, and if $x,y\in F_0$, then $x+y\in F_0$ and $xy\in F_0$. Since $-1\in F_0$, $x-y = x+(-1)y \in F_0$. Finally, $xy^{-1} = x(y^{-1})^n y^{n-1} \in F_0$. □

By Lemma 2 there are some $a_1,\dots,a_m \in F$, $a_m \neq 0$ such that $a_1^n + \dots + a_m^n = 0$, or, equivalently,

$$(a_m^{-1}a_1)^n + \dots + (a_m^{-1}a_{m-1})^n = -1.$$

By Lemma 3 sums of nth powers in F form a subfield F_0 of F, and by the hypothesis of Proposition 1 the factorgroup $F^*/{F_0}^*$ is finite. In particular, F_0 is infinite. Suppose $F_0 \neq F$. Choose any $\alpha \in F\setminus F_0$. If $a,b\in F_0$ are distinct, then, obviously, the images of the elements $\alpha+a$ and $\alpha+b$ are distinct in $F^*/{F_0}^*$, hence $\infty = |F_0^*| \le |F^*/F_0^*|$, a contradiction to finiteness of the group $F^*/{F_0}^*$. Therefore, $F_0 = F$, i.e. any element of F is a sum of nth powers.

Lemma 4. *$D(\phi \perp \langle\lambda\rangle) \neq D(\phi)$ for any nonuniversal diagonal form ϕ and any $\lambda \in F^*$.*

Proof. In the case of quadratic forms this is just Kneser's Lemma ([2, Ch. 11, 6.5.]), and we will modify its proof for forms of higher degree. However, the proof of Kneser's Lemma uses the fact that any nondegenerate isotropic quadratic form is universal. This is not true for forms of higher degree, and, indeed, as is shown in Proposition 5 below, Proposition 1 is not always true for finite fields. So assume that $D(\phi \perp \langle\lambda\rangle) = D(\phi)$. Then, iterating, it is easy to see that $D(\phi \perp N\langle\lambda\rangle) = D(\phi)$ for any positive integer N. Since $F_0 = F$ and the group F^*/F^{*n} is finite, the form $N\langle\lambda\rangle$ is universal if N is big enough, hence the form $\phi \perp N\langle\lambda\rangle$ is universal as well. But this is a contradiction to the equality $D(\phi \perp N\langle\lambda\rangle) = D(\phi)$, since ϕ is not universal. The lemma is proved. □

Now we can finish the proof of Proposition 1. Let $|F^*/F^{*n}| = m$. Consider any form $\langle a_1, \dots, a_m\rangle$ of degree n, where $a_i \in F^*$. Let

$$\pi : F^* \to F^*/F^{*n}$$

be the projection map. We may assume that the form $\langle a_1, \dots, a_{m-1}\rangle$ is not universal. Obviously, $D(\phi) = \pi^{-1}(\pi(D(\phi)))$ for any form ϕ of degree n. In particular, by Lemma 4

$$\pi(D(\langle a_1, \dots, a_i\rangle)) \neq \pi(D(\langle a_1, \dots, a_{i+1}\rangle))$$

for any $1 \leq i \leq m-1$. Hence $|\pi(D(\langle a_1, \dots, a_m\rangle))| \geq m$, which implies that $|\pi(D(\langle a_1, \dots, a_m\rangle))| = m$ and the form $\langle a_1, \dots, a_m\rangle$ is universal. Proposition 1 is proved. □

Example. The proof of Lemma 2 does not give us an upper bound on m as a function of n. Moreover, in fact, we prove only existence of a_i, not expressing them via the coordinates of a solution of the equation $x_1^2 + \dots + x_l^2 = 0$. However, if $n = 4$ we can find a concrete solution of the required system. More precisely, if $b_1^2 + \dots + b_l^2 = 0$, then

$$\sum_{(\epsilon_1,\dots,\epsilon_l)} \left(\sum_{i=1}^{l} \epsilon_i b_i\right)^4 = 2^l \left(\sum_{i=1}^{l} b_i^4 + 6 \sum_{1\le i<j\le l} b_i^2 b_j^2\right)$$
$$= 2^l \left(3\left(\sum_{i=1}^{l} b_i^2\right)^2 - 2\sum_{i=1}^{l} b_i^4\right) = -2^{l+1} \sum_{i=1}^{l} b_i^4,$$

where $\epsilon_i \in \{1,-1\}$. Obviously, we may assume that $l+1$ is divisible by 4. Then

$$\sum_{(\epsilon_1,\dots,\epsilon_l)} \left(2^{\frac{-l-1}{4}} \sum_{i=1}^{l} \epsilon_i b_i\right)^4 + \sum_{i=1}^{l} b_i^4 = 0.$$

The last equality shows that zero can be represented as a sum of $2^l + l$ 4th powers of certain $c_1, \dots, c_{2^l+l} \in R$ not simultaneously zero. Then $(c_1, \dots, c_{2^l+l}, -c_1, \dots, -c_{2^l+l})$ is a solution of the corresponding power system in $2(2^l + l)$ variables for $n = 4$. As we have mentioned already, the condition that the field F in Proposition 1 is infinite is essential. For a finite field F the subfield F_0 from Lemma 3 does not necessarily coincide with F, and Proposition 1 is no longer true. More precisely, keeping the notation in Lemma 3, we have the following

Proposition 5. *Let F be a finite field of order p^m. Then the following conditions are equivalent:*

1) *There exists a nonuniversal diagonal form with nonzero coefficients of dimension $|F^*/F^{*n}|$ and degree n over F.*

2) $F_0 \neq F$.

3) *n is a multiple of $\frac{p^m-1}{p^k-1}$, where k is a divisor of m and $k \neq m$.*

4) *The form $x_1^n + \dots + x_l^n$ over F is not universal for any l.*

Proof. 1) $\Longrightarrow$ 2). This follows from the proof of Proposition 1.

2) $\Longrightarrow$ 3). Let the order of F_0 be p^k. Obviously, k is a divisor of m and the order of F^*/F^{*n} is a multiple of the order of $F^*/{F_0}^*$, which is equal to $\frac{p^m-1}{p^k-1}$. Consider the exact sequence

$$1 \longrightarrow \ker n \longrightarrow F^* \xrightarrow{n} F^* \longrightarrow F^*/F^{*n} \longrightarrow 1,$$

where the map n is taking the nth power. We have $|\ker n| = |F^*/F^{*n}|$, and $|\ker n|$ is a divisor of n. Therefore, n is a multiple of $\frac{p^m-1}{p^k-1}$.

3) $\Longrightarrow$ 4) Let K be the subfield of F of order p^k. Then $x^{\frac{p^m-1}{p^k-1}} \in K$ for any $x \in F$. In particular, $D(x_1^n + \cdots + x_l^n) \subset K \neq F$.

4) $\Longrightarrow$ 1). Trivial. □

Corollary 6. *For a fixed power n there exist only finitely many finite fields F with a nonuniversal form over F of degree n, dimension $|F^*/F^{*n}|$ and nonzero coefficients.*

Proof. Let a field F satisfy the required properties and $|F| = p^m$. Proposition 5 implies that $p^{\frac{m}{2}} + 1 = \frac{p^m-1}{p^{\frac{m}{2}}-1} \leq n$, which makes the assertion obvious. □

The following statement, which is similar to Proposition 1, shows that a diagonal form is isotropic provided its dimension is big enough.

Proposition 7. *Let F be a nonformally real field, n a positive integer. Suppose that the group F^*/F^{*n} is finite. Then any diagonal form of degree n in more than $|F^*/F^{*n}|$ variables is isotropic.*

Proof. We may assume that all the coefficients of the form are nonzero. Then for an infinite field F the statement follows immediately from Proposition 1. However, to cover the case of a finite field we have to modify a bit the argument from Proposition 1. So suppose that F is finite, and the form $\langle a_1, \ldots, a_N \rangle$ of degree n is anisotropic, where $N > |F^*/F^{*n}|$. Obviously, there exists $1 \leq i \leq |F^*/F^{*n}|$ such that

$$D(\langle a_1, \ldots, a_i \rangle) = D(\langle a_1, \ldots, a_{i+1} \rangle).$$

Iterating as in the proof of Lemma 4, it is easy to see that

$$D(\langle a_1, \ldots, a_i \rangle) = D(\langle a_1, \ldots, a_i \rangle \perp m\langle a_{i+1} \rangle)$$

for arbitrary m, and the form $\langle a_1, \ldots, a_i \rangle \perp m\langle a_{i+1} \rangle$ is anisotropic. This is a contradiction, since the form $p\langle a_{i+1} \rangle$ is isotropic, where $p = \mathrm{char} F$. □

So far all considered forms have been diagonal, which, of course, is very restrictive. In the following result, which is a main purpose of this paper, we omit this condition and consider *systems* of forms for certain fields.

Corollary 8. *Let F be a nonformally real field, n, r positive integers. Suppose that for any prime number $p \leq n$ the factorgroup F^*/F^{*p} is finite. Then, if N is big enough, any system of r forms of degree n in N variables over F has a nonzero solution.*

Proof. It is easy to see that for any $k \le n$ the factorgroup F^*/F^{*k} is finite. We should prove that $v_{n,r}$ is finite. This follows from Proposition 6 and the results in [1] and [3] discussed in the beginning of the paper. □

It is easy to see that multidimensional local fields satisfy the conditions of Corollary 8. Here is another example, which is due to Artin. For the sake of completeness we consider it in detail.

Proposition 9. *Let k be a field, k_{sep} its separable closure, $\alpha \in k_{\mathrm{sep}} \setminus k$. Let F be a maximal algebraic extension of k not containing α (the existence of F is provided by Zorn's lemma). Then*

1) *$p = [F(\alpha) : F]$ is a prime.*

2) *If $\mathrm{char}F = p$, then $|F^*/F^{*p}| = 1$. If $\mathrm{char}F \ne p$, then $|F^*/F^{*p}| = p$.*

3) *Any finite field extension of F is a cyclic p-primary Galois extension. In particular, $F^* = F^{*q}$ for any prime number $q \ne p$.*

4) *If k is nonformally real, then F satisfies the hypothesis of Corollary 7.*

Proof. Let K/F be a finite extension and L/K the normal closure of K. Consider the tower $F \subset F' \subset L$, where F'/F is purely inseparable and L/F' is separable. If $F \ne F'$, then $\alpha \in F'$, a contradiction, since α is separable over F. Therefore, $F = F'$ and the extension L/F is separable, hence Galois. Let $G = \mathrm{Gal}(L/F)$. Consider the tower $F \subset F(\alpha) \subset L$. Let $H = \mathrm{Gal}(L/F(\alpha))$. Pick any $\sigma \in G \setminus H$. Let $\langle\sigma\rangle$ be the cyclic group generated by σ. If $L^{\langle\sigma\rangle} \ne F$, then $F(\alpha) \subset L^{\langle\sigma\rangle}$, or, in other words, $\sigma \in H$, a contradiction. Therefore, $L^{\langle\sigma\rangle} = F$, i.e. $G = \langle\sigma\rangle$. In particular, any finite extension of F is a cyclic Galois extension. Since any finite extension of F contains $F(\alpha)$, we conclude that $[F(\alpha) : F] = p$ is a prime, and any finite extension of F is p-primary. If $\mathrm{char}F = p$, and $a \in F^*$, then the field extension $F(a^{\frac{1}{p}})/F$ is purely inseparable. Since any finite extension of F is separable, we get $F(a^{\frac{1}{p}}) = F$, i.e. $F^* = F^{*p}$. If $\mathrm{char}F \ne p$, consider any $a, b \in F^*$. Since any field extension of F is cyclic,

$$\mathrm{Gal}(F(a^{\frac{1}{p}}, b^{\frac{1}{p}})/F) \ne \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

This implies that the images of a and b in the linear space F^*/F^{*p} over $\mathbb{Z}/p\mathbb{Z}$ are linearly dependent. Since the extension $F(\alpha)/F$ is cyclic of degree p we get $|F^*/F^{*p}| = p$. Thus, parts $1) - 3)$ are proven, and part 4) follows at once from them. □

Remark. If the prime number p in Proposition 9 is odd, then by part 3) of this proposition $F(\sqrt{-1}) = F$, hence F is nonformally real.

Open question. Suppose the field F in Proposition 9 is nonformally real. Is F a C_1 field, i.e. for each $d \geq 1$ any form of degree d in at least $d+1$ variables isotropic? Notice that this is the case if the field k in Proposition 9 is finite.

References

1. R. Brauer, *A note on systems of homogeneous algebraic equations.* — Bull. AMS. **51** (1945), 749–755.
2. T. Y. Lam, *Introduction to quadratic forms over fields.* Graduate studies in Mathematics **67** (2005).
3. D. B. Leep, W. M. Schmidt, *Systems of homogeneous equations.* — Invent. Math. **71**, No. 3 (1983), 539–549.
4. W. Scharlau, *Quadratic and Hermitian Forms.* Springer, Berlin–Heidelberg–New York (1985).

St. Petersburg State University
St.Petersburg, Russia
E-mail: alev729@mail.ru

St. Petersburg State University
St.Petersburg, Russia
E-mail: paxa239@ya.ru

St.Petersburg Electrotechnical University
St.Petersburg, Russia
E-mail: sivatsky@AS3476.spb.edu

St. Petersburg State University
St.Petersburg, Russia
E-mail: dms239@mail.ru

Поступило 15 сентября 2011 г.