MÉMOIRES DE LA S. M. F.

ALBRECHT PFISTER

Systems of quadratic forms

Mémoires de la S. M. F., tome 59 (1979), p. 115-123

<http://www.numdam.org/item?id=MSMF_1979__59__115_0>

Col. sur les Formes Quadratiques (1977, Montpellier)
Bull. Soc. Math. France
Mémoire 59, 1979, p. 115-123

SYSTEMS OF QUADRATIC FORMS

by

Albrecht PFISTER

1. Introduction

In general it is very difficult to solve a system of algebraic equations in several variables. There are only a few theorems which say more than ordinary algebraic geometry and yet are not restricted to objects of special type such as elliptic curves. One of the best known results of the type in question are the theorems of Tsen-Lang on quasi-algebraically closed fields ([13], [8]) which are repeated in part 2. The essential point in these theorems is the possibility to go up from a given field K to an algebraic or transcendental extension field L of K.

In the theory of quadratic forms one would like to have similar "going-up theorems". Even if the given problem is about a single quadratic form over L one is automatically led to consider systems of quadratic forms over K. Unfortunately the theory of systems of quadratic forms seems to be nearly as difficult as the theory of systems of arbitrary forms. Nevertheless it appears to be useful to introduce the concept of $H\,C_i^q$-fields in analogy to C_i-fields and to derive the corresponding theorems of Tsen-Lang type. This is done in part 3. Full proofs can be found in the thesis of M. Amer [1].

The main part of the present paper is part 4. Theorem 3 shows the existence of fields which are C_0^q but not C_0. The proof uses two recent theorems on places by Jón K. Arason (Theorems 1,2) which are published here with his kind permission. Theorem 3 also contains the main theorem of the paper [9] of S. Lang.

The final part 5 contains a collection of related results, examples and open problems. Needless to say that it would be most desirable to get further results on C_i^q-fields for $i > 0$ or at least for $i = 1$ in order to solve some of these problems.

2. C_i-fields

Definition. A field K is called C_i-field if for any $d \geq 1$ and for any form f of degree d in $n > d^i$ variables with coefficients from K the equation $f(x_1,\ldots,x_n) = 0$ has a non-trivial solution in K, i.e. $f(a_1,\ldots,a_n) = 0$ for suitable $a_k \in K$, not all zero.

Examples

1) K is C_o if and only if K is algebraically closed.
2) If K is not C_o then K has an algebraic extension field L of degree $d > 1$ and the norm-form φ of L over K is anisotropic in $n = d = d^1$ variables (anisotropic means : has no nontrivial zero).
   By substituting φ into itself we get anisotropic forms φ_i of degree d^i in $n_i = d^i$ variables :

$$\varphi_2 = (\underbrace{\varphi|\ldots|\varphi}_{d}) = \varphi(\varphi(x_1,\ldots,x_d), \varphi(y_1,\ldots,y_d),\ldots,\underbrace{\varphi(z_1,\ldots,z_d)}_{d \text{ entries}})$$

$$\varphi_3 = \varphi(\varphi_2|\ldots|\varphi_2) \text{ etc.}$$

Proposition 1 (Artin's Trick). Let K be C_i and let $f_1,\ldots,f_r$ be forms of degree d over K in n common variables where $n > r.\, d^i$. Then the system $f_1 = 0,\ldots,f_r = 0$ has a non-trivial simultaneous solution in K.

Proof : See [8]. The idea of the proof consists in substituting the system $f_1,\ldots,f_r$ into an anisotropic form as follows : Since the case $d = 1$ is known from linear algebra and the case $i = 0$ is known as the main theorem of elimination theory (or dimension theory in the terminology of algebraic geometry) one may suppose $d \geq 2$, $i \geq 1$. By example 2 above there exists an anisotropic form φ_o in $n_o = d_o$ variables where n_o is arbitrarily large, e.g. $n_o \geq r$.
One defines φ_k inductively by

$$\varphi_{k+1} = \varphi_k(f_1,\ldots,f_r\,|\ldots|\,f_1\ldots f_r\,|\,\underbrace{0\ldots0}_{<r})$$

φ_k is of degree $d_k = d_o d^k$ and has n_k variables where $n_{k+1} = n.\lceil \frac{n_k}{r} \rceil$
If $f_1,\ldots,f_r$ have no nontrivial common zero then all the φ_k are anisotropic. But for large k we have $n_k > d_k^i$ which gives a contradiction.

Proposition 2. If K is C_i and L is algebraic over K then L is also C_i.

Idea of proof : Let $f = f(x_1,\ldots,x_n)$ be the given form over L. Suppose $[L:K] = r$ and choose a basis $w_1,\ldots,w_r$. Put

$$x_k = \sum_{l=1}^{r} x_{kl}\, w_l \quad \text{where the } x_{kl} \text{ are variables over K. Then}$$

$f(x_1,\ldots,x_n) = f_1(x_{kl})\, w_1 + \ldots + f_r(x_{kl}) w_r$ and $f = 0$ over L if and only if $f_1 = \ldots = f_r = 0$ over K. This gives a system of degree d in $r.n > r.d^i$ variables over K to which prop. 1 applies.

Proposition 3. Ket K be C_i. Then the rational function field $K(t)$ and the formal power series field $K((t))$ are C_{i+1}.
Proof : See [8] for $K(t)$, [6] for $K((t))$.

Non-proposition 4. (Artin's Conjecture) Suppose L is complete with respect to a discrete valuation v. If the residue class field $K = L/v$ is C_i then L need not be C_{i+1}.

Counter-example : p-adic fields are not C_2 though finite fields are C_1. See [4] and [12].

3. C_i^q-fields.

Definition 1'. A field K is called C_i^q-field if every system of r quadratic forms over K in n common variables has a non-trivial simultaneous zero in K provided $n > r.2^i$.

Remark. This definition replaces prop. 1 for the special case $d = 2$. As is shown by the examples below it is impossible to deduce the property C_i^q from the corresponding assumption for $r = 1$.

Proposition 2'. If K is C_i^q and L is algebraic over K then L is also C_i^q.
Proof : Same as for prop. 2.

Proposition 3'. If K is C_i^q then $K(t)$ and $K(t))$ are C_{i+1}^q.
Proof : Same as for prop. 3.

Open Problem 4'. Suppose L is complete with respect to a discrete valuation v. Suppose the residue class field $K = L/v$ is a C_i^q-field. Is L a C_{i+1}^q-field ?

Remark. It seems unlikely that the answer to this problem is yes. However I do not know of any counter-examples. For one quadratic form ($r=1$) over L the answer is yes by the theorem of Springer [11]. For two or three quadratic forms the answer is yes in special cases, see the examples in §5.

Examples.

1) Let K be the quadratic closure of $\mathbb{Q}$ (in a fixed algebraic closure $\bar{\mathbb{Q}}$) that is the union of all towers $\mathbb{Q} = K_0 < K_1 < K_2 < \ldots < \bar{\mathbb{Q}}$ where $[K_{m+1} : K_m] = 2$ for all $m \geq 0$.

Every quadratic form in 2 or more variables over K is isotropic. But K is not C_0^q. To see this consider the system $x^2 - yz$, $z^2 + xy + y^2$ of $r = 2$ quadratic forms in $n = 3 > 2.2^0 = 2$ variables over K. If (x,y,z) is a non-trivial zero of the system then $y \neq 0$, so without loss a generality $y = 1$, $x^2 = z$ and $x^4 + x + 1 = 0$. But this equation has no solution in K since the order of the Galois group of the polynomial $x^4 + x + 1$ over $\mathbb{Q}$ is divisible by 3. There is another proof as follows : K is quadratically closed but has algebraic extensions L which are not quadratically closed. If K were C_0^q then by prop. 2' L were also C_0^q which implies L quadratically closed : contradiction.

2) Let $\mathbb{Q}_2$ be the field of 2-adic numbers, let $\bar{\mathbb{Q}}_2$ be a fixed algebraic closure of $\mathbb{Q}_2$. The Galois group of G of $\bar{\mathbb{Q}}_2$ over $\mathbb{Q}_2$ is soluble (as a profinite group) therefore contains a $(3,5)$-Hall-subgroup H. Let K be the fixed field of H. K has thefollowing property : Every finite extension of K has degree $3^i.5^j$ for some $i \geq 0$, $j \geq 0$; every finite extension of $\mathbb{Q}_2$ contained in K has degree prime to 3 and 5. The polynomial

$$f(x) = (x^3 + x + 1)(x^5 + x^2 + 1)$$

of degree 8 has no zero in K since both factors are irreducible over $\mathbb{Q}_2$. On the other hand the non-trivial zeros of a form $x^8 + a_6x^6z^2 + a_5x^5z^3 + \ldots + a_0z^8$ with $a_0 \neq 0$ are in 1-1-correspondence with the non-trivial zeros (x,y,z,w) of the system

$$x^2-yz,\ y^2-zw,\ w^2+a_6yw+a_4y^2+a_2yz+a_0z^2+a_5xw+a_3xy+a_1xz$$

of 3 quadratic forms in 4 variables. This implies that K is not a C_0^q-field though K has an "odd" Galois group H which furthermore contains only the two primes 3 and 5.

We will show in §4 that a field K whose Galois group is a p-group for some odd prime p is actually a C_0^q-field.

4. C_o^q-fields

Definition. Let p be a prime. A field K is called p-field if any finite extension field of K has p-power degree (over K).

We start with two recent theorems of Jón K. Arason.

Theorem 1. Let L be a field, let K be a p-field and let $\lambda : L \to K \cup \{\infty\}$ be a place. For any finite extension field M of L with $p \mid [M : L]$ the place can be extended to a place $\mu : M \to K \cup \{\infty\}$.

Proof : Let v be a Krull valuation of L belonging to λ. We may suppose that the residue class field L/v of v is contained in K.

We shall first treat the case where (L,v) is henselian. Then v has exactly one extension w to M. Furthermore by a theorem of Ostrowski ([10], ch. G, th. 2)

$$[M : L] = \chi^d\,[w(M^*) : v(L^*)].[M/w : L/v]$$

where $w(M^*)$, $v(L^*)$ denote the value groups, χ denotes the characteristic exponent of K (i.e. $\chi = \operatorname{char} K$ if $\operatorname{char} K$ is a prime, $\chi = 1$ if $\operatorname{char} K = 0$) and d is an integer, $d \geq 0$.
By assumption on $[M : L]$ it follows that $[M/w : L/v]$ is prime to p. Since $L/v \subset K$ and K is a p-field the embedding $L/v \subset K$ can be extended to an embedding $M/w \subset K$. This gives rise to a place $\mu : M \to K \cup \{\infty\}$ extending λ.
It remains to reduce the general case to the henselian case. Let $(\tilde{L},\tilde{v})$ be a henselian of (L,v) (See [10], ch. F, th. 2). Then $\tilde{L}/\tilde{v} = L/v \subset K$, the place $\tilde{\lambda} : \tilde{L} \to K \cup \{\infty\}$ belonging to $\tilde{v}$ extends λ, and $\tilde{L}/L$ is separable. From the last statement it follows that $\tilde{L} \otimes_L M$ is isomorphic to a direct sum $\bigoplus_{i=1}^{r} \tilde{M}_i$ where the $\tilde{M}_i$ are finite field extensions of $\tilde{L}$. For each i there is an embedding $\alpha_i : M \to \tilde{M}_i$ which is the identity on L. The equation $\sum_{i=1}^{r} [\tilde{M}_i : \tilde{L}] = [M : L]$ and the assumption $p \mid [M : L]$ imply that there is at least one j with $p \mid [\tilde{M}_j : \tilde{L}]$. By what we have shown above $\tilde{\lambda}$ can be extended to $\tilde{\mu} : \tilde{M}_j \to K \cup \{\infty\}$. $\tilde{\mu} \circ \alpha_j : M \to K \cup \{\infty\}$ is the desired extension of λ to M.

Theorem 2. Let K be a p-field and let $t_1,\ldots,t_N$ be independent indeterminates over K. Then the rational function field $K(t_1,\ldots,t_N)$ has an algebraic extension M with the following properties :

(i) M is a p-field
(ii) For each N-tuple $(a_1,\ldots,a_N) \in K^N$ there is a K-place $\lambda : M \to K \cup \{\infty\}$ with $\lambda(t_i) = a_i$ for $i = 1,\ldots,N$.

Proof : To simplify notation we write $\underline{t} = (t_1,\dots,t_N)$. Let $\overline{K(\underline{t})}$ be the algebraic closure of $K(\underline{t})$ and let M with $K(\underline{t}) \subset M \subset \overline{K(\underline{t})}$ be maximal with the property that each finite extension M_o of $K(\underline{t})$ contained in M has degree prime to p. Such an M exists by Zorn's lemma. We will sho that M is a p-field. Assume first that M has a separable extension whose degree is not a power of p. Then there is a Galois extension with the same property. Applying Sylow theory we get a proper extension of M with degree prime to p contradicting the maximality of M. Assume second that M has an inseparable extension N of degree not a power of p. Then char K = char $M = q$ is a prime different from p and the separable part N_s of N is of p-power degree over M. Consider the subfield $N_s^q = \{a^q : a \in N_s\}$ of N_s. Since M has no immediate extension of degree prime to p we must have $M = M^q \subset N_s^q$. Therefore $[N_s : N_s^q]/[N_s : M]$ is a power of p. Since $[N_s : N_s^q]$ is a power of q too we must have $N_s = N_s^q$.
But then $N = N_s$ is separable over M : Contradiction.

Now let $\lambda_0 : K(\underline{t}) \to K \cup \{\infty\}$ be a K-place with $\lambda_0(t_i) = a_i$ for $i = 1,\dots,N$ (Such a place can easily be constructed by induction on N). Consider all pairs $(L;\lambda)$ where L is a field, $K(\underline{t}) \subset L \subset M$, and $\lambda : L \to K \cup \{\infty\}$ is a K-place extending λ_0. By Zorn's lemma there exists a maximal pair (L,λ) of this kind. Applying Theorem 1 to L we conclude that there is no finite extension M_o of L, $L \subset M_o \subset M$, with $[M_o : L]$ prime to p. But $p|[M_o : L]$ is also impossible since the "degree" $[M : K(\underline{t})]$ is "p-free" by construction of M. Thus $L = M$ which proves (ii).
We are now able to prove a theorem on systems of forms over a p-field which in particular shows that p-fields are C_o^q if $p \neq 2$.

Theorem 3. Let K be a p-field. Let $f_1,\dots,f_r$ be forms over K of degrees $d_1,\dots,d_r$ in n common variables. Suppose $n > r$ and $p \nmid d_i$ for $i = 1,\dots,r$. Then $f_1,\dots,f_r$ have a non-trivial simultaneous zero over K.

Proof : We may suppose $n = r+1$. The ideal $(f_1,\dots,f_r)$ defines a certain algebraic set W in projective r-space. The idea of the proof is asfollows : By a specialization argument using Theorem 2 one reduces to the case dim $W = 0$. Then Bézout's theorem is applicable and provides a K-rational point on W.

Let $F_1,\dots,F_r$ be the generic n-variable forms of degrees $d_1,\dots,d_r$ over K. Thus the coefficients of $F_1,\dots,F_r$ are independent indeterminates $t_1,\dots,t_N$ over K and $N = \binom{d_1+r}{r} + \dots + \binom{d_r+r}{r}$.

Since $n = r+1$ the algebraic set V in projective r-space over the algebraically closed field $\overline{K(\underline{t})}$ defined by $F_1,\dots,F_r$ has dimension 0. By Bézout's theorem the number of points of V counted with multiplicity equals $d_1 \cdot \dots \cdot d_r$. Let

now $M \subset \overline{K(\underline{t})}$ be as in Theorem 2. We shall show that V contains H at least one M-rational point P. For this we note that any point $P = (\xi_1,\ldots,\xi_{r+1}) \in V \subset P_r(\overline{K(\underline{t})})$ uniquely defines its fields of rationality over M, namely $M(P) = M(\frac{\xi_1}{\xi_j},\ldots,\frac{\xi_{r+1}}{\xi_j})$ if $\xi_j \neq 0$. Suppose $M(P) \neq M$.

Then $[M(P) : M]$ is a finite power of p since M is a p-field.
If $M(P)/M$ is inseparable then necessarily $p = \operatorname{char} K = \operatorname{char} M$ and the multiplicity of $P \in V$ is divisible by p. If $M(P)/M$ is separable then the number of conjugate points of P over M equals $[M(P) : M]$ which again is divisible by p. It follows that the number of points $P \in V$ with $M(P) \neq M$ - counted with multiplicity - is divisible by p. Since the total number $d_1 \cdot \ldots \cdot d_r$ of points of V is not divisible by p there must be a t least one $P \in V$ with $M(P) = M$ i.e. P is M-rational. From now on let $P = (\xi_1,\ldots,\xi_{r+1}) \in V$ be M-rational.

Let $f_1,\ldots,f_r$ be the given forms over K. Let $a_1,\ldots,a_N$ be the coefficients of $f_1,\ldots,f_r$ corresponding to $t_1,\ldots,t_N$. By Theorem 2 there exists a K-place $\lambda : M \to K \cup \{\infty\}$ with $\lambda(t_i) = a_i$, $i = 1,\ldots,N$. λ may be further extended to a map $\lambda : M[x_1,\ldots,x_{r+1}] \to K[x_1,\ldots,x_{r+1}] \cup \{\infty\}$ by defining $\lambda(x_j) = x_j$, $j=1,\ldots,r+1$. Then $\lambda(F_i) = f_i$ for $i = 1,\ldots,r$. Since $P = (\xi_1,\ldots,\xi_{r+1}) \in V$ is M-rational we can suppose $\xi_j \in M$ for $j=1,\ldots,r+1$. Let v be the multiplicative valuation of M belonging to λ. Since not all $\xi_j = 0$ the $v(\xi_j)$ are not all zero and there is some i such that $v(\xi_j) \leq v(\xi_i)$ for all $j=1,\ldots,r+1$ and $v(\xi_i) > 0$. Scaling P by $\frac{1}{\xi_i}$ shows that we may suppose $v(\xi_j) \leq 1$ for all j, $\xi_i = 1$. Then $\lambda(\xi_j)$ is finite for all j, and $\lambda(\xi_i) = 1$. Thus $\lambda(P) = (\lambda(\xi_1),\ldots,\lambda(\xi_{r+1}))$ is a point in $P_r(K)$. Clearly $f_i(\lambda(P)) = (\lambda F_i)(\lambda P) = \lambda(F_i(P)) = 0$ for $i=1,\ldots,r$, i.e. $\lambda(P) \in W$. This proves the theorem.

Corollary 1. Let K be a p-field, $p \neq 2$. Then K is C_0^q.
Corollary 2. (S. Lang [9]) Let K be a real closed. Then K is "oddly C_0" that is any system $f_1,\ldots,f_r$ of forms of odd degrees over K in $n > r$ variables has a common non-trivial zero over K.

Conjecture (Converse of Cor. 1). If K is C_0^q then K is a p-field for some prime $p \neq 2$.
For the motivation of this conjecture see Exemple 2 in §3.

5. Related results and problems

a) $\mathfrak{p}$-adic fields
Though $\mathfrak{p}$-adic fields are not C_2 there are some remarkable positive results

on systems of quadratic forms.

Proposition 5. (Demyanov, Birch-Lewis-Murphy [3])
Let f_1, f_2 be two quadratic forms in at least 9 variables over a $\mathfrak{p}$-adic field K. Then f_1, f_2 have a non-trivial common zero in K.

Proposition 6. (Birch-Lewis [2]) Let f_1, f_2, f_3 be three quadratic forms in at least 13 variables over a $\mathfrak{p}$-adic field K. Suppose in addition that K is non-dyadic and that the residue class field k of K has at least 49 elements. Then f_1, f_2, f_3 have a non-trivial common zero in K.

For $K = \mathbb{Q}_2$ the corresponding result onthree quadratic forms has been verified by F. Ellison [5] provided f_1, f_2, f_3 are all in diagonal form.

b) Extensions of odd degree

A well-known theorem of T. Springer says that a quadratic form f over K which becomes isotropic in a field-extension L with $[L : K]$ odd already must be isotropic over K. This theorem does not generalize to systems of quadratic forms.

Counter-example : $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt[3]{2})$,

$$f_1 = f_1(x_1,x_2,x_3) = x_1^2 - 2x_2x_3,\ f_2 = x_2^2 - x_1x_3,\ f_3 = 2x_3^2 - x_1x_2.$$

For any non-trivial solution of the system we have $x_1x_2x_3 \neq 0$.
Then $x_1^3 = 2x_1x_2x_3 = 4x_3^3$, $x_2^3 = x_1x_2x_3 = 2x_3^3$, $(x_1,x_2,x_3) \sim (\sqrt[3]{4}, \sqrt[3]{2}, 1)$.
Thus we have a non-trivial solution in L but none in K.
Remark : M Colliot-Thélène has pointed out that the counter-example is in a sense non-geometric and that it would be more interesting to have a counter-example with $n > r$ (n variables, r quadratic forms).

c) Function fields over $\mathbb{R}$

Conjecture (S. Lang [9]). Suppose K is of transcendence degree n over a real closed field $\mathbb{R}$. Suppose also that K is non-real, i.e. -1 is a sum of squares in K. Is it true that K is a C_n-field ?
Besides the case of forms of odd degree mentioned in Corollary 2 above the only case where the conjecture is known to be true is the following : $n = 1$, one quadratic form. This goes back to Witt. A modern proof can be founc in [7, ch. XI, th. 1.8]. The next cases to look at are :

n = 1, two quadratic forms in 5 variables

or n = 1, one biquadratic form in 5 variables

or n = 2, one quadratic form in 5 variables.

An attempt in this direction has been made in [1] but without final success.

REFERENCES

[1] AMER M., Quadratische Formen über Funktionenkörpern. Dissertation, Mainz 1976.

[2] BIRCH-LEWIS., Systems of three quadratic forms. Acta Arithm. 10 (1965) 423-442.

[3] BIRCH-LEWIS-MURPHY., Simultaneous quadratic forms. Amer. J. Math. 84, (1962) 110-115

[4] BROWKIN J., On forms over p-adic fields. Bull. Ac. Polon. Sci. 14, (1966) 489-492.

[5] ELLISON F., Three diagonal quadratic forms. Acta Arithm. 23, (1973) 137-151.

[6] GREENBERG M., Rational points in henselian discrete valuation rings. IHES Publ. Math. 31, (1966) 59-64.

[7] LAM T.Y., The algebraic theory of quadratic forms. Benjamin, Reading/Mass., (1973).

[8] LANG S., On quasi-algebraic closure. Ann. of Math. 55, (1952) 373-390.

[9] LANG S., The theory of real places. Ann. of Math. 57, (1953) 378-391.

[10] RIBENBOIM P., Théorie des valuations. Les Presses de l'Université de Montréal Montréal (1968).

[11] SPRINGER T.A., Quadratic forms over a field with a discrete valuation. Indag Math. 17, (1965) 352-362.

[12] TERJANIAN G., Un contre-exemple à une conjecture d'Artin. C.R. Acad. Sci. Paris 262, (1966) 612-615.

[13] TSEN C., Zur Stufentheorie der quasialgebraisch-Abgeschlossenheit kommutativer Körper. J. Chin. Math. Soc. 1 (1936) 81-92.

A. PFISTER

Fachbereich Mathematik
Johannes Gutenberg-Universität

6500 MAINZ GERMANY