AN ENGLISH TRANSLATION OF CORPS ET CHIRURGIE (FIELDS AND SURGERY) BY ANAND PILLAY & BRUNO POIZAT

TRANSLATED BY: GREGORY COUSINS

ABSTRACT. Algebraically closed fields, real closed fields, and pseudofinite fields have, for every natural number n, have a finite number of extensions of degree n; we show they share this property with all fields which, like them, satisfy a very basic property of preservation of a type of model-theoretic dimension. This result is attained by showing that a certain action of the group GL_n on such a field has only a finite number of orbits.

The original article appeared in The Journal of Symbolic Logic, Volume 60, Number 2, June 1995 [4]. *We have attempted to provide a translation as faithful to the original wording as possible. The one exception is in the final remark where we elaborate slightly for the sake of exposition. Any mistakes, typos, or inconsistencies are likely due to the translator and should be brought to their attention by emailing them at* gcousins@nd.edu.

Dimension is the property that is conserved when one cuts something apart and puts the pieces back together or, similarly, if we replace one piece with two of its copies. This philosophy is what leads us to make the following definition:

Definition 1. If U and V are two definable sets in a structure M, we say the dimension of U is less than the dimension of V, and write $\dim(U) \leq \dim(V)$, if there exists a partition of U into a finite number of definable subsets $U_1, \ldots, U_n$ and definable functions $f_i : U_i \to V$, for $1 \leq i \leq n$, such that the f_i's have finite fibres (i.e. the preimage of any point is of size less than m for some fixed natural number m).

By "definable", we mean what others may call "interpretable", that is to say, we live in the structure M^{eq}; we also allow parameters in definitions. However, we use here the notion of dimension for sets definable without parameters in the cartesian product of the considered structure, which will be a field K.

As in set theory without choice where we introduce the expression $|U| \leq |V|$ to mean that we have an injection from U to V without worrying about defining an entity called the "cardinality of U", we consider the expression "$\dim(U) \leq \dim(V)$" on its own. The important thing is the transitivity: if $\dim(U) \leq \dim(V)$ and $\dim(V) \leq \dim(W)$, then $\dim(U) \leq \dim(W)$; this implies that the relation of "having the same dimension", that is, $\dim(U) \leq \dim(V)$ and $\dim(V) \leq \dim(U)$, is an equivalence. So, if the reader would like an object named "the dimension of U", take the monster model and quotient the set of all of its definable parts by this congruence.

In the context where this notion of dimension differs from others, we will call it the *surgical dimension*. When the structure M is a field K, with algebraic closure K_{alg}, we also consider the *geometric dimension* of a definable subset U of K^n, which is its dimension in the sense of geometers, or even the Morley rank of the Zariski closure of U in K^n_{alg}. It is also the maximum transcendence degree over K of a tuple, maybe in an elementary extension of K, satisfying U: we see that this notion is reasonable for a model theorists because nothing changes if we replace K with an elementary extension.

The referee - sorry Mr. Allgood - made us see that our definition of surgical dimension is not natural, since if $f : U \to V$ is a definable surjection with finite fibres, it is not necessarily the case that U and V have the same dimension. We agree, but we keep this definition in order to minimize the assumptions for the theorem that we wish to prove.

As this dimension exists in every structure M, we can exploit it if we assume it has particular properties; we require decent behaviour with respect to quotients, and we describe an *surgical structure* as any structure M (saturated enough!) satisfying the following property:

(1) *If E is a definable equivalence relation on the elements of a definable set U, there are only finitely many equivalence classes modulo E which have the same dimension as U.*

In fact, we will only use this hypothesis in the following weakened form:

(2) *For every definable action of a definable group G on a definable set U, there is only a finite number of orbits with the same dimension as U.*

We observe that this property is preserved under interpretation.

In recent years, a number of surgical structures have been studied in model theory, for example:

- finite structures;
- totally transcendental structures (since equal surgical dimension implies equal Morley rank); in the case where the structure is just superstable, condition 2 is true if stabilizers are (uniformly) finite (use Shelah degree); (infinite) fields definable in these structures are algebraically closed (see [5], [6]);
- o-minimal structures (since surgery preserves cellular dimension), which can only define real closed or algebraically closed fields (see [3]);
- bounded, pseudo-algebraically closed structures, as defined in Hrushovski [1][*Translator's Note: This reference seems to not exist or is under a different name than the one referenced in the original version of this paper.*], and in particular pseudo-finite fields (since surgery preserves S_1 rank);
- certain "geometric fields" defined in Hrushovski and Pillay [2]. Note that p-adic fields are "geometric", but are not surgical: indeed, the p-adic integers form a subgroup of infinite index of, and yet the same dimension as, the additive group of the field, contradicting condition 2. Regardless, p-adic fields satisfy the conclusion of the following theorem. It would be interesting to find a model theoretic fact for why this is the case.

The goal of this note is to understand in general context a clear property exhibited by all these examples:

Theorem 2. *Surgical fields are perfect and have, for every n, a finite number of extensions of degree n.*

Translator's Note. Surgical fields are then fields of type (F) as defined by Serre in Galois Cohomology [7].

It is easy to show perfection: K is our surgical field; if it is infinite of characteristic p, K^p is definably isomorphic to K, so of the same dimension; if it were a proper subfield of K, it would be an subgroup of the additive group of K of infinite index, which is incompatible with condition 2. K is therefore perfect, and this is also true if it is finite!

Let L be a separable extension of K of degree n. By the primitive element theorem, L is generated over K by a single element α. By $\alpha_1, \ldots, \alpha_n$, we denote the conjugates of α (in the algebraic closure of K). The field $N = K(\alpha_1, \ldots, \alpha_n)$ is a normal, separable (i.e. Galois) extension of K of degree $n!$. By the fundamental theorem of Galois theory, there are a finite number of intermediate fields in between K and N, each corresponding to a subgroup of the Galois group of the extension N/K. It remains to show that there are only a finite number of possibilities for N.

This undertaking will demand several pages. We start with two lemmas clarifying the relationship between the surgical dimension and the algebraic dimension.

Lemma 3. *For any field K, every non-empty, Zariski open subset of K^n has the same surgical dimension as K^n.*

Proof. In a finite structure, everything has the same dimension. We suppose, therefore, that K is infinite. Let $U \subseteq K^n$ be a Zariski open subset and let F be its complement. We translate F piecewise into U, via an induction argument on the geometric dimension of F.

Translator's Note. Clearly $\dim(U) \leq \dim(K^n)$. From the argument, we conclude that $\dim(K^n) \leq \dim(U)$, since we may partition K^n into the disjoint union $U \sqcup F$ and U maps into U via the identity, and F maps into U via a series of translations.

The result is clear if the geometric dimension of F is zero, that is, if F is finite, so we assume F has strictly positive dimension.

Let G be a closed, irreducible subset of K^n_{alg}. For every $a \in K^n_{alg}$, if $a + G$ is different from G, then the intersection $G \cap (a + G)$ has (geometric) dimension strictly less than that of G. Furthermore, those a such that $a + G = G$ form an algebraic subgroup of $(K^+_{alg})^n$ whose connected component is necessarily a K_{alg}-vector subspace of the latter; if G is non-empty, this vector space is of dimension (in any sense of the word) less than the dimension of G.

Let F' be the Zariski closure of F in K^n_{alg}, which, by hypothesis, is non-empty and not all of K^n_{alg}. If $(a + F') \cap F'$ is of the same dimension, say d as F', then it is the case that translation by a exchanges two irreducible components of F' of dimension d. The set of $a \in K^n_{alg}$ that have his property form a set $V_1 \cup \ldots \cup V_k$, where each V_i is an equivalence class modulo a vector subspace of dimension greater or equal to d, but strictly less than n. The intersection of any such V_i with K^n is either empty, or an affine space of of dimension less than d: in fact, the linear dimension, which is calculated via determinants, does not increase as one goes up from K to K_{alg}, or even to any other extension of K. As a consequence, since K is infinite, the $V_i \cap K^n$ cannot cover K^n, and so one can find $a \in K^n$ such that $(a+F') \cap F'$ is of dimension less than d. We translate $F \setminus (a+F)$ by $-a$ into U, and

by the induction hypothesis applied to $(a + F) \cap F$, we can translate $(a + F) \cap F$ piecewise into its complement, which is $U \cup (F \setminus (a + F))$: each piece is divided into two, one which translates into U, and one that translates into $F \setminus (a + F)$, which can then be translated into U by a new translation. And voila. □

Lemma 4. *Let K be a field and U a definable subset of K^n. Then $\dim(U) \leq \dim(K^d)$, where d is the geometric dimension of U.*

Proof. Let U' be the Zariski closure of U in K_{alg}^n; since U' is fixed setwise by all K-automorphisms of K_{alg}, it is defined by a set polynomial equations with parameters in K. Let p be a generic point of U', that is, a type over K_{alg} of rank d concentrating on U'. Let $a = (a_1, \ldots, a_n)$ be a realization of p in some elementary extension of K_{alg}. The coordinates of a are algebraic over d of them; to simplify notation, we suppose the first $a_1, \ldots, a_d$ are algebraically independent over K_{alg}, whereas a is algebraic over $K_{alg}(a_1, \ldots, a_d)$.

By compactness, and the fact that U' cannot contain a point of transcendence degree $d + 1$, there exists an integer k such that $(a_1, \ldots, a_d)$ has no more than k extensions to an n-tuple of U'. The subset U_1' of U' of points whose first d coordinates have no more than k extensions to an n-tuple of U' is a definable subset of K_{alg}^n. By quantifier elimination, U_1' is definable by a quantifier-free formula in the language of fields (geometers would call such a set "constructible"), and with parameters in K. The intersection $U_1' \cap K^n$ is therefore a definable subset over K. Here, we do an induction on the Morley rank and degree of U' to obtain a decomposition of U into $U_1, \ldots, U_r$, such that for each U_i there is a projection $\pi_i : U_i \to K^d$ such that π_i has finite fibres (i.e. size less than k). □

We now proceed with the proof of our theorem by elimination of imaginaries.

Proof of Theorem 2. We consider the group $\mathrm{GL}_n(K_{alg})$ of n-by-n invertible matrices with coefficients in the algebraic closure of K and its subgroup S, isomorphic to the permutation group S_n, consisting of the permutation matrices, i.e. those matrices formed by permuting the columns of the identity matrix. Two matrices are congruent modulo S acting on the right if and only if one is a permutation of the columns of the other.

Since the theory of algebraically closed fields eliminates imaginaries, the quotient of $\mathrm{GL}_n(K_{alg})$ by the right action of S can be identified with a definable subset U of some cartesian power of K_{alg}: we have, therefore, a definable surjection $F : \mathrm{GL}_n(K_{alg}) \to U(K_{alg})$ such that $F(X) = F(Y)$ if and only if one is a permutation of the columns of the other. By quantifier elimination, U is definable by a quantifier-free formula, and furthermore, is definable without parameters, since both GL_n and S are definable without parameters. Similarly, the action of GL_n on U is definable by a quantifier-free formula without parameters.

For the reader unfamiliar with the notion of elimination of imaginaries, we explicitly work through the case of $n = 2$; to a matrix with rows $(x, y; u, v)$, F assigns five values, $A = xy$, $B = x + y$, $C = uv$, $D = u + v$, $E = xv + yu$, that characterize a permutation of it's columns: only the matrix $(y, x; v, u)$ has the same value under F. The set U is the subset of K_{alg}^5 defined by the equation $E^2 + BDE + AD^2 + CB^2 - 4AC = 0$ and the inequality $E^2 - 4AC \neq 0$. As for the action of a matrix $M = (a, b; c, d)$ on U, it transforms (A, B, C, D, E) into $(a^2A + b^2C + abE, aB + bD, c^2A + d^2C + cdE, cA + dD, 2acA + 2bdC + (ad + bc)E)$.

Going down now to K; the intersection $U(K)$ in $U(K_{alg})$ with K^m remains a definable set in K, on which the action of $\mathrm{GL}_n(K)$ is still definable; for this action, the stabilizer of a point will never have more than $n!$ elements, since this action extends to the algebraic closure of K. However, there is no reason why this action should have only one orbit!

Now we calculate dimensions. As $U(K_{alg})$ has the same Morley rank as $\mathrm{GL}_n(K)$, which is n^2, Lemma 4 tells us that the surgical dimension of $U(K)$ is less than or equal to that of K^{n^2}. By Lemma 3, $\mathrm{GL}_n(K)$, since it is Zariski open in K^{n^2}, has the same surgical dimension as K^{n^2}, and that dimension is less than or equal to the surgical dimension of $U(K)$, since, as each stabilizer of a point in $U(K)$ is finite, each orbit of a point of the action of $\mathrm{GL}_n(K)$ on $U(K)$ has the same surgical dimension as $\mathrm{GL}_n(K)$. In other words, $\mathrm{GL}_n(K)$ and $U(K)$ have the same surgical dimension. If, as we assumed, that our field K is surgical, then the action of $\mathrm{GL}_n(K)$ on $U(K)$ has a finite number or orbits.

It remains to show the relevance of the proceeding considerations to the initially posed problem.

For this, we recall our n-tuple $\bar{\alpha} = (\alpha_1, \ldots, \alpha_n)$ of elements in the algebraic closure of K, which are conjugate and separable over K. To $\bar{\alpha}$, we associate a matrix A for which the i^{th}-column, which we write as a row to be economical with paper, is $(1, \alpha_i, \alpha_i^2, \ldots, \alpha_i^{n-1})$; the determinant of this matrix is a Vandermonde determinant, nightmare of DEUG students; it is non-zero since the α_i are distinct.

The value of $F(A)$ is not changed by permuting the α_i, so that, as the extension $K(\alpha_1, \ldots, \alpha_n)/K$ is separable, each of its coordinates is in K: $F(A)$ is in $U(K)$.

Therefore, if we assume the field K is surgical, $\mathrm{GL}_n(K)$ has a finite number of orbits in $U(K)$; if we take another tuple $\bar{\alpha}'$ to which we associate a matrix A', if $F(A)$ and $F(A')$ are in the same $\mathrm{GL}_n(K)$ orbit, then we can find $M \in \mathrm{GL}_n(K)$ such that $A' = MAB$, where B is a permutation matrix. This implies that α and α' generate the same extension of K. The theorem is proven. □

Remark 5. Dr. Zoé Chatzidakis has proposed an alternate proof for our theorem. It is more direct, but it uses the full strength of property (1) instead of only its consequence, property (2), for group actions.

Let K a surgical field and let U be the set of tuples $\bar{a} = (a_0, \ldots, a_{n-1})$, such that the polynomial $P_{\bar{a}}(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$ is irreducible over K. U is a definable subset of K^n.

Consider the equivalence relation E on U given by $\bar{a}E\bar{b}$ if and only if $P_{\bar{a}}(x)$ and $P_{\bar{b}}(x)$ generate isomorphic extensions of K; this means that $P_{\bar{b}}(x)$ has a zero modulo $P_{\bar{a}}(x)$ and so the equivalence relation E is definable. As an extension of degree n has no more than $n!$ conjugates over K, it is enough to show that there are only a finite number of degree n extensions up to isomorphism; furthermore, if K is perfect all extensions are primitive: we want to show that E has only finitely many classes; for that, it suffices to show that each of these classes is of the same surgical dimension as K^n.

It is clear if U is empty; if not, we consider $\bar{a} \in U$, as well as the zeros $\alpha_1, \ldots, \alpha_n$ of $P_{\bar{a}}(x)$, which live in the algebraic closure of K. It is easy to see that the tuples $(x_0, \ldots, x_{n-1}) \in K^n$ such that $\beta_1 = x_0 + x_1\alpha_1 + \ldots x_{n-1}\alpha_1^{n-1}$ generates the same extension as α_1 form a Zariski open subset V of K^n: it suffices to express that $1, \beta_1, \beta_1^{n-1}$ are linearly independent over K. Observe that any K-conjugate of β_1 is of the form $\beta_i = x_0 + x_1\alpha_i + \ldots x_{n-1}\alpha_i^{n-1}$ for some i. Let $Q(x)$ be the minimal

polynomial of β_1 over K. We can write

$$Q(x) = x^n + \sum_{i=1}^{n} (-1)^i \mathbf{e}_i(\beta_1, \ldots, \beta_n) x^{n-i},$$

where $\mathbf{e}_i(y_1, \ldots, y_n)$ is the i^{th}-elementary symmetric polynomial. Consider the polynomial map $G(x_0, \ldots, x_{n-1})$ whose i^{th}-coordinate function is given by

$$\mathbf{e}_i(x_0 + x_1\alpha_1 + \ldots x_{n-1}\alpha_1^{n-1}, \ldots, x_0 + x_1\alpha_n + \ldots x_{n-1}\alpha_n^{n-1}),$$

which is a polynomial in $x_0, \ldots, x_n$ with coefficients which are symmetric polynomials in $\alpha_1, \ldots, \alpha_n$. Since every symmetric polynomial $P(y_1 \ldots, y_n)$ can be expressed uniquely as $R(\mathbf{e}_1(y_1, \ldots, y_n), \ldots, \mathbf{e}_n(y_1, \ldots, y_n))$ for some $R(\bar{y}) \in K[y_1, \ldots, y_n]$, and since $\mathbf{e}_i(\alpha_1, \ldots, \alpha_n) = a_i$, we have that $G(x_0, \ldots, x_{n-1})$ is a polynomial map with parameters in $\bar{a} \in K$. Observe that, for $(v_0, \ldots, v_{n-1}) \in V$, $G(v_0, \ldots, v_{n-1})$ determines an irreducible polynomial for which each root is of the form $v_0 + v_1\alpha_i + \ldots + v_{n-1}\alpha_i^{n-1}$ for some i, and so G is a polynomial map from V to the E-class of $\bar{a}$. Furthermore, for $\bar{b}E\bar{a}$, the fibre $G^{-1}(\bar{b})$ is precisely the set of permutations of the tuple of zeros of the polynomial $P_{\bar{b}}(x)$, and so the fibres are size $n!$. Thus, we have a polynomial map with finite fibres from V to the E-class of $\bar{a}$ and the conclusion follows from Lemma 3.

Thanks. This article was written when the first author was a guest of the Université Claude Bernard (Lyon 1); he wants to eagerly thank the mathematical faculty of this university, which received him as professor first class, third grade, during the month of May of the year 1994.

Added in proof. The same methods show the the conclusion of the theorem holds for any field F such that $\text{Th}(F)$ has ordinal valued Shelah degree.

References

[1] Ehud Hrushovski. Pseudo-algebraically closed structures. 199?

[2] Ehud Hrushovski and Anand Pillay. Groups definable in local fields and pseudo-finite fields. *Israel J. Math.*, 85(1-3):203–262, 1994.

[3] Anand Pillay. On groups and fields definable in o-minimal structures. *Journal of Pure and Applied Algebra*, 53(3):239 – 255, 1988.

[4] Anand Pillay and Bruno Poizat. Corps et chirurgie. *The Journal of Symbolic Logic*, 60(02):528–533, 1995.

[5] Bruno Poizat. *Stable Groups.* American Mathematical Soc.

[6] Bruno Poizat. *Cours de theorie des modeles : une introduction a la Logique mathematique contemporaine.* B. Poizat, Villeurbanne, France, 1985.

[7] Jean-Pierre Serre. *Galois cohomology.* Springer Science & Business Media, 2013.