Notre Dame Journal of Formal Logic
Volume 52, Number 4, 2011

Rank and Dimension in Difference-Differential Fields

Ronald F. Bustamante Medina

Abstract Hrushovski proved that the theory of difference-differential fields of characteristic zero has a model-companion, which we shall denote DCFA. Previously, the author proved that this theory is supersimple. In supersimple theories there is a notion of rank defined in analogy with Lascar U-rank for superstable theories. It is also possible to define a notion of dimension for types in DCFA based on transcendence degree of realization of the types. In this paper we compute the rank of a model of DCFA, give some properties regarding rank and dimension, and give an example of a definable set with finite rank but infinite dimension. Finally we prove that for the case of definable subgroup of the additive group being finite-dimensional and having finite rank are equivalent.

1 Introduction and Preliminaries

The theory of differentially closed fields is ω-stable; thus complete types are ranked by Lascar's U-rank. The U-rank of a generic type (the type of a differentially-transcendental element) of a differentially closed field is ω. Given a differentially closed field (K, D), a differential subfield F of K, and an element $a \in K$, we define the dimension of a over F to be $\mathrm{tr.dg}(F(a)_D/F)$ where $F(a)_D$ denotes the differential field generated by F and a. It is easily proved that $U(\mathrm{tp}(a/F))$ is finite if and only if a has finite dimension over F. For more details on the differentially closed fields the reader may consult [4].

The theory of difference fields has a model-companion denoted ACFA and all completions of this theory are supersimple; thus every complete type in a model of ACFA is ranked by the SU-rank. As for differentially closed fields, the SU-rank of a generic element of a model of ACFA is ω. We define dimension in the same way as for differentially closed fields. That is, let (K, σ) be a model of ACFA, F

Received January 9, 2008; accepted November 8, 2010; printed October 5, 2011
2010 Mathematics Subject Classification: Primary, 11U09, 12H05, 12H10
Keywords: model theory of fields, supersimple theories, difference-differential fields, definable sets
 10.1215/00294527-1499363

a difference subfield of K and $a \in K$, and define the dimension of a over F to be tr.dg$(F(a)_\sigma/F)$ where $F(a)_\sigma$ denotes the (inversive) difference field generated by F and a. We can prove that $SU(\text{tp}(a/F))$ is finite if and only if a has finite dimension over F. We refer to [2] for details on ACFA.

Our goal in this paper is to study rank and dimension, and their relation, in difference-differential fields. A difference-differential field is a differential field with an automorphism which commutes with the derivation. Hrushovski proved that, in characteristic zero, the theory of difference-differential fields has a model-companion (see [1] for the proof). This theory is called DCFA and it is not complete, but its completions are easily described.

Given difference-differential field F and a difference-differential subfield E, if $a \in F$, we denote by $E(a)_{\sigma,D}$ the difference-differential field generated by E and a. If $A \subseteq F$ we denote by $\text{acl}_{\sigma,D}(A)$ the (field-theoretic) algebraic closure of the difference-differential field generated by A.

The following results are proved in [1].

Proposition 1.1 *Let (K, σ, D) be a model of* DCFA. *Let $A \subset K$. Then the (model-theoretic) algebraic closure* $\text{acl}(A)$ *of A is* $\text{acl}_{\sigma,D}(A)$.

Using linear disjointness of fields we can define independence in models of DCFA.

Definition 1.2 Let K be a model of DCFA; let A, B, C be subsets of K. We say that *A is independent from B over C*, denoted $A \mathop{\smile\!\!\!\!\!\!\,|}_C B$, if $\text{acl}(A, C)$ is linearly disjoint from $\text{acl}(B, C)$ over $\text{acl}(C)$.

Theorem 1.3

1. *The independence relation defined above coincides with nonforking.*
2. *Every completion of* DCFA *is supersimple.*

Remark 1.4 We have thus the next notion of forking for types: Let (K, σ, D) be a saturated model of DCFA. Let $E = \text{acl}(E) \subseteq F = \text{acl}(F) \subset K$ and a be a tuple of K. Let $p = \text{tp}(a/E)$ and $q = \text{tp}(a/F)$. We say that q is a forking extension of p, or that p forks over F, if $a \not\mathop{\smile\!\!\!\!\!\!\,|}_E F$; otherwise, we say that q is a nonforking extension of p.

Definition 1.5 Let $E \subseteq F$ be two difference-differential fields; let $a \in F$.

1. We define $\deg_{\sigma,D}(a/E)$ to be the transcendence degree of $E(a)_{\sigma,D}$ over E if it is finite; in this case we say that a is finite-dimensional over E. Otherwise, we set $\deg_{\sigma,D}(a/E) = \infty$ and we say that a is infinite-dimensional over E.
2. We say that *a is (σ, D)-transcendental over E* if a does not satisfy any (σ, D)-polynomial equation (an equation of the form $P(X) = 0$ where P is a polynomial over E in the variables $\{\sigma^i(D^j X) : i \in \mathbb{Z}, j \in \mathbb{N}\}$). Otherwise, we say that it is *(σ, D)-algebraic over E*.

2 The SU-Rank

Since, by Theorem 1.3(2), every completion of DCFA is supersimple, types are ranked by the SU-rank. This section is devoted to the study of the SU-rank in DCFA. Given an element of a model of DCFA, we will construct a numeric sequence, we will define a rank for this sequence, and we will show that this rank bounds the SU-rank of the element. With this we prove that the SU-rank of a generic element of a model of DCFA is ω^2.

Definition 2.1 Let (K, σ, D) be a model of DCFA. Let $E = \mathrm{acl}(E) \subset K$ and a be a tuple of K. We define the SU-rank of $p = \mathrm{tp}(a/E)$, $SU(p)$ (we can write it also $SU(a/E)$), by induction as follows.

1. $SU(p) \geq 0$.
2. For an ordinal α, $SU(p) \geq \alpha + 1$ if and only if there is a forking extension q of p such that $SU(q) \geq \alpha$.
3. If α is a limit ordinal, then $SU(p) \geq \alpha$ if and only if $SU(p) \geq \beta$ for all $\beta \in \alpha$.

We define $SU(p)$ to be the smallest ordinal α such that $SU(p) \geq \alpha$ but S $SU(p) \ngeq \alpha + 1$.

Given a definable set A, we define $SU(A)$ as the SU-rank of a generic type of A. Lascar's inequalities hold for the SU-rank (see [3]).

Lemma 2.2 *Let (K, σ, D) be a model of* DCFA. *Let a, b be tuples of K and E a difference-differential subfield of K. Let α be an ordinal. Then*

1. $SU(a/Eb) + SU(b/E) \leq SU(ab/E) \leq SU(a/Eb) \oplus SU(b/E)$ *where $\oplus$ denotes the natural sum of ordinals;*
2. *if $a \mathop{\smile\!\!\!\!\!\mid}_E b$, then $SU(ab/E) = SU(a/E) \oplus SU(b/E)$.*

Remark 2.3 Let $E = \mathrm{acl}(E)$, and let us suppose that $\deg_{\sigma,D}(a/E) < \infty$. Let $F = \mathrm{acl}(F) \supset E$. Then $a \not\mathop{\smile\!\!\!\!\!\mid}_E F$ if and only if $\deg_{\sigma,D}(a/F) < \deg_{\sigma,D}(a/E)$. Thus, by induction on $\deg_{\sigma,D}(a/E)$ we can prove that $SU(a/E) \leq \deg_{\sigma,D}(a/E)$.

Let $(I, \leq)$ be the class of nonincreasing sequences of $\mathbb{N} \cup \{\infty\}$ indexed by $\mathbb{N}$, partially ordered as follows: if $(m_n), (m'_n) \in I$, then $(m_n) \leq (m'_n)$ if and only if for every $n \in \mathbb{N}$, $m_n \leq m'_n$.

Remark 2.4 If $(m_n) \in I$, then there exist $A \in \mathbb{N} \cup \{\infty\}$ and $B, C \in \mathbb{N}$ such that $m_n = \infty$ if and only if $n < A$, and $m_n = C$ if and only if $n \geq A + B$.

Let $(m_n) \in I$. We will denote the Foundation Rank of (m_n) by $\mathrm{FR}(m_n)$.

Definition 2.5 Let (K, σ, D) be a model of DCFA, $E = \mathrm{acl}(E) \subset K$, and a a tuple of $\in K$. To a and E we associate the sequence (a_n^E) defined by

$$a_n^E = \mathrm{tr.dg}(E(a, Da, \ldots, D^n a)_\sigma / E(a, Da, \ldots, D^{n-1} a)_\sigma).$$

Remark 2.6

1. By 2.12 of [1], $(a_n^E) \in I$.
2. Assume that either a is a single element or that every element of a is a zero of a σ-polynomial (a polynomial in the variables $X, \sigma(X), \sigma^2(X), \ldots$, where X is a tuple of variables of the same length as a) over E. If $E \subset F = \mathrm{acl}(F)$, then $\mathrm{tp}(a/E)$ does not fork over F if and only if $a \mathop{\smile\!\!\!\!\!\mid}_E F$, if and only if for all $n \in \mathbb{N}$, $\mathrm{tr.dg}(E(a, Da, \ldots, D^n a)_\sigma / E(a, Da, \ldots, D^{n-1} a)_\sigma) = \mathrm{tr.dg}(F(a, Da, \ldots, D^n a)_\sigma / F(a, Da, \ldots, D^{n-1} a)_\sigma)$, if and only if $(a_n^E) = (a_n^F)$. Hence $SU(a/E) \leq \mathrm{FR}(a_n^E)$.

Proposition 2.7 *Let $(m_n) \in I$; let A, B, C as in Remark 2.4. If $A \neq \infty$ then* $\mathrm{FR}(m_n) = \omega \cdot (A + C) + \sum_{j=A}^{A+B-1} (m_j - C)$*; if $A = \infty$ then* $\mathrm{FR}(m_n) = \omega^2$.

Proof First we will consider the case that $A < \infty$. We observe that if $B' > B$, then $\sum_{j=A}^{A+B'-1}(m_j - C) = \sum_{j=A}^{A+B-1}(m_j - C)$. Let $\alpha = \omega \cdot (A+C) + \sum_{j=A}^{A+B-1}(m_j - C)$. We shall prove by induction on α that $\mathrm{FR}(m_n) = \alpha$.

For $\alpha = 0$ it is clear. Suppose that the proposition holds for α. Assume that α is a successor ordinal. Let $(m_n) \in I$, and A, B, C as in Remark 2.4 such that $\alpha + 1 = \omega \cdot (A + C) + \sum_{j=A}^{A+B-1}(m_j - C)$; this implies, in particular, that $B \neq 0$ and $m_{A+B-1} > C$.

Claim $\mathrm{FR}(m_n) > \alpha$. Define (m'_n) such that $m'_n = m_n$ for $n \neq A + B - 1$ and $m'_{A+B-1} = m_{A+B-1} - 1$. Then $(m'_n) \in I$ and $(m'_n) < (m_n)$. Let A', B', C' be the numbers associated to (m'_n) by Remark 2.4. Then $A' = A$, $C' = C$, $B' \leq B$, and $\omega \cdot (A' + C') + \sum_{j=A'}^{A'+B'-1}(m'_j - C') = \alpha$. By induction hypothesis $\mathrm{FR}(m'_n) = \alpha < \mathrm{FR}(m_n)$, and the claim is proved.

Claim $\mathrm{FR}(m_n) = \alpha + 1$. Let $(m'_n) \in I$ such that $(m'_n) < (m_n)$. Let A', B', C' be the numbers associated to (m'_n) by Remark 2.4. Then $A' \leq A$ and $C' \leq C$. We want to show that $\mathrm{FR}(m'_n) \leq \alpha$.

If $A' < A$ or $C' < C$, we have $A'+C' < A+C$, and thus $\omega \cdot (A'+C') < \omega \cdot (A+C)$. Since $\sum_{j=A'}^{A'+B'-1}(m'_j - C') \in \mathbb{N}$, $\alpha+1 = \omega \cdot (A+C) + \sum_{j=A}^{A+B-1}(m_j - C) > \omega \cdot (A'+C') + \sum_{j=A'}^{A'+B'-1}(m'_j - C')$ and by induction hypothesis the latter equals $\mathrm{FR}(m'_n)$.

If $A' = A$ and $C' = C$, then there is $k \in \{A, \ldots, A + B - 1\}$ such that $m'_k < m_k$. In this case we have $\sum_{j=A}^{A+B-1}(m'_j - C) < \sum_{j=A}^{A+B-1}(m_j - C)$; hence $\alpha + 1 = \omega \cdot (A + C) + \sum_{j=A}^{A+B-1}(m_j - C) > \omega \cdot (A + C) + \sum_{j=A}^{A+B-1}(m'_j - C)$. This proves the claim.

Assume now that α is a limit ordinal $< \omega^2$, and let $(m_n) \in I$ (with the associated numbers $A, B = 0, C$) such that $\alpha = \omega \cdot (A + C)$ with $A + C \neq 0$. We shall prove that for every $k \in \mathbb{N}$ there is $(m'_n) \in I$ such that $(m'_n) < (m_n)$ and $\mathrm{FR}(m'_n) = \omega \cdot (A + C - 1) + k$.

If $A \neq 0$, let $(m'_n) \in I$ be such that $m'_{A-1} = C + k$, $m'_n = \infty$ for $n < A - 1$, and $m'_n = C$ for $n > A - 1$. We have $(m'_n) < (m_n)$ and by induction hypothesis $\mathrm{FR}(m'_n) = \omega \cdot (A + C - 1) + k$.

If $A = 0$, then $C \neq 0$. Let $(m'_n) \in I$ such that $m'_n = C - 1$ for $n \geq k$ and $m'_n = C$ if $n < k$. Then $(m'_n) < (m_n)$; by induction hypothesis $\mathrm{FR}(m'_n) = \omega \cdot (C - 1) + k$. Thus $\mathrm{FR}(m_n) \geq \alpha$.

Claim $\mathrm{FR}(m_n) = \alpha$. Let $(m'_n) \in I$ such that $(m'_n) < (m_n)$; let A', B', C' be the numbers associated to (m'_n) by Remark 2.4. Then $A' < A$ or $C' < C$; hence $A' + C' < A + C$, and $\omega \cdot (A' + C') + \sum_{j=A'}^{A'+B'-1}(m'_j - C') < \omega \cdot (A + C) = \alpha$. By induction hypothesis $\mathrm{FR}(m'_n) < \alpha$. This shows that $\mathrm{FR}(m_n) \ngeq \alpha + 1$; that is, $\mathrm{FR}(m_n) = \alpha$.

Now let us consider the case where $A = \infty$.

Claim $\alpha = \omega^2$. Let (m_n) be the sequence defined by $m_n = \infty$ for all $n \in \mathbb{N}$. By induction hypothesis we know that if $(m'_n) < (m_n)$ is in I, then $\mathrm{FR}(m'_n) < \omega^2$. Hence $\mathrm{FR}(m_n) \ngeq \omega^2 + 1$. On the other hand, for every $k \in \omega$, let (m^k_n) be the sequence with associated numbers $A = k$, $B = C = 0$. Then $\mathrm{FR}(m_n) > \mathrm{FR}(m^k_n) = \omega k$.

Now, for example, we can easily compute the rank of $\operatorname{Fix}\sigma \cap \mathcal{C}$ of a model K of DCFA, where $\operatorname{Fix}\sigma$ is the fixed field of K ($\operatorname{Fix}\sigma = \{x \in K : \sigma(x) = x\}$) and $\mathcal{C}$ is the field of constants of K ($\mathcal{C} = \{x \in K : Dx = 0\}$). □

Corollary 2.8 *Let $a \in K$ be a generic of* $\operatorname{Fix}\sigma \cap \mathcal{C}$ *over F. Then $SU(a/F) = 1$.*

Proof Since $(a_n^F) = (1, 0, 0, 0, \ldots)$, by Proposition 2.7, $\mathrm{FR}(a_n^F) = 1$. Thus $SU(a/F) = \mathrm{FR}(a_n^F) = 1$. □

Proposition 2.9 *Let (K, σ, D) be a model of* DCFA *and let $a \in K$ be a (σ, D)-transcendental element of K over $F = \operatorname{acl}(F) \subset K$. Let $(m_n) \in I$. Then there is a difference-differential field $E \subset K$ such that $(a_n^E) = (m_n)$.*

Proof Define $b_0 = a, b_1 = \sigma(a) - a, \ldots, b_{k+1} = \sigma(b_k) - b_k, \ldots$. Let A be as in Remark 2.4. Let $E = F(D^i b_{m_i} : i > A)_\sigma$. As (m_i) is nonincreasing, for all i, $D^{i+1} b_{m_i} \in F(D^{i+1} b_{m_{i+1}})_\sigma$; hence E is a difference-differential field. By construction and because a is (σ, D)-transcendental over F,

$$\operatorname{tr.dg}(E(a, \ldots, D^n a)_\sigma / E(a, \ldots, D^{n-1} a)_\sigma) = \operatorname{tr.dg}(F(a, \ldots, D^n a)_\sigma / F(a, \ldots, D^{n-1} a, D^n b_{m_n})_\sigma).$$

Because a is (σ, D)-transcendental over F, the latter equals m_n. Moreover, it is easily proved by induction that $\mathrm{FR}(a_n^E) = SU(a/E)$. □

Corollary 2.10 *Let a be a tuple of K such that the elements of $\{\sigma^i(D^j a) : i, j \in \mathbb{N}\}$ are algebraically independent over E. Let n be the transcendence degree of a over E. Then $SU(a/E) = \omega^2 \cdot n$.*

Proof The corollary is actually a consequence of the proof of Proposition 2.9 and Lemma 2.2(2). □

3 An Example

In this section we exhibit a set of SU-rank 1 which is infinite-dimensional. As we mentioned before in differentially closed fields and in ACFA, being finite-dimensional and having finite rank are equivalent and this is an important equivalence which has led, for example, to algebraic proofs of the dichotomies for those theories (see [6]).

Example 3.1 $\sigma(x) = x^2 + 1$.

Let A be the set defined by $\sigma(x) = x^2 + 1$. Let $A_1 = \{x \in A : Dx = 0\}$ and let $A_2 = \{x \in A : Dx \neq 0\}$.

Theorem 3.2 *A has SU rank 1 and infinite dimension.*

The proof of this theorem follows from the next two lemmas.

Lemma 3.3 *A_1 is strongly minimal and stably embedded.*

Lemma 3.4 *A_2 is strongly minimal and stably embedded.*

Proof of Lemma 3.3 If $a \in A_1$, then by 6.1 of [2] $K(a)_{\sigma,D} = K(a)_\sigma$ has no finite σ-stable extension. Then all extensions of σ over $\operatorname{acl}(Ka)$ are conjugates over $K(a)_{\sigma,D}$ (see [2], 2.8). Thus $qf\operatorname{tp}(a/K) \vdash \operatorname{tp}(a/K)$ and this holds for an arbitrary difference-differential field K. This means that $\operatorname{tp}(a/K)$ is the only nonrealized type of A_1, and A_1 is strongly minimal. By 6.1 of [2], we know that A_1 is trivial. As the full induced structure of A_1 is stable, A_1 is stably embedded. $\square$

Lemma 3.4 is a consequence of the following.

Proposition 3.5 *Let $K = \operatorname{acl}(K)$ and let $a \in A_2 \setminus K$. Then a is differentially transcendental over K.*

Proof Let $K_0 = K(a)_\sigma$ and $K_{n+1} = K_n(D^{n+1}a)$. Since

$$\sigma(D^n a) = \sum_{i=0}^{n} \binom{n}{i} D^i a D^{n-i} a \tag{1}$$

for $n > 0$, each K_n is a difference field.

Let $f_n(X) = 2aX + b_n$ where $b_n = \sum_{i=1}^{n-1} \binom{n}{i} D^i a D^{n-i} a$ when $n > 0$, and $f_0(X) = X^2 + 1$. By (1) we have that $\sigma(D^n a) = f_n(D^n a)$.

Set $f_n^1(X) = f_n(X)$ and $f_n^{k+1}(X) = (f_n^k)^\sigma(f_n(X))$. Then $\sigma^k(D^n a) = f_n^k(D^n a)$. We have then that $f_n^k(X) = 2^k a\sigma(a)\ldots\sigma^{k-1}(a)X + C$ where C is a constant. Then f_0^k is the composition of f_0 with itself k times, so $f_0^{k+1}(X) = (f_0^k(X))^2 + 1$. In particular, $f_0^k(0) \in \mathbb{N}$. Note that $f_0^{k+1}(0) = f_0^k(0)^2 + 1$, so that $f_0^k(0) \neq 0$ for all $k \geq 0$, and the numbers $f_0^k(0)$ form a strictly increasing sequence. Given a difference field E, a *finite σ-stable extension* of E is a finite field extension F of E such that $\sigma(F) \subseteq F$.

We shall prove the following for $n \geq 1$:

- **I**$_n$ K_{n-1} contains no finite subset S such that $\sigma(S) = f_n(S)$, unless $n = 1$ in which case $S = \{0\}$.
- **II**$_n$ $K_{n-1}^{\mathrm{alg}}(D^n a)$ has no proper finite σ-stable extensions.
- **III**$_n$ Any solution of $\sigma(x) = x$ in K_n is in K. This implies that, if $n > 0$, the solutions of $\sigma(x) = (2a)^m x$ in K_n are of the form $c(Da)^m$ where $c \in \operatorname{Fix}\sigma \cap K$; and the solutions of $\sigma^k(x) = 2^k a\sigma(a)\ldots\sigma^{k-1}(a)x$ in K_n are of the form cDa where $c \in \operatorname{Fix}\sigma^k$; and if $n = 0$ there is no solution in K_0 of $\sigma(X) = (2a)^m X$ for $m > 0$.

It will be useful to consider some variants of the first two statements:

- **I**$'_n$ K_{n-1} contains no finite subset S such that $\sigma^k(S) = f_n^k(S)$, unless $n = 1$ in which case $S = \{0\}$.
- **I**$''_n$ K_{n-1}^{alg} contains no finite subset S such that $\sigma^k(S) = f_n^k(S)$, unless $n = 1$ in which case $S = \{0\}$.
- **II**$'_n$ K_n has no proper σ-stable finite extensions.

II$'_0$ holds By 6.1 of [2] we know that K_0 has no proper finite σ-stable extension.

III$_0$ holds Let $\alpha \in K_0$ be a solution of $\sigma(X) = (2a)^m X$. Choose $N \geq 0$ minimal such that $\sigma^N(\alpha) \in K(a)$ (such N exists because, as $\sigma(a) = a^2 + 1$, $K_0 = K(a)_\sigma = K(\ldots, \sigma^{-1}(a), a)$). Then $\sigma^N(\alpha)$ satisfies $\sigma(X) = (2\sigma^N(a))^m X$. If $N > 0$, this implies that $\sigma^N(\alpha) \in K(\sigma(a))$ and contradicts the minimality of N. Hence $N = 0$.

Let $P, Q \in K[X]$ be relatively prime with Q monic and such that $\alpha = \frac{P(a)}{Q(a)}$. Then

$$\frac{P^\sigma(X^2+1)}{Q^\sigma(X^2+1)} = (2X)^m \frac{P(X)}{Q(X)}.$$

Comparing the number of poles and zeros, we get $\deg(Q) = 0$ and $\deg(P) = m$. If $m > 0$, then $P^\sigma(f_0(0)) = 0 = P^\sigma(1)$; hence $P(1) = 0$. By induction, one then shows that for all $k > 0$, $f_0^k(0)$ is a zero of P. Since the sequence $f_0^k(0)$ is strictly increasing, this is impossible and $\mathbf{III}_0$ is proved.

Now suppose $n \geq 1$.

$\mathbf{I}_n \implies \mathbf{I}'_n$. Replace S by $S \cup \sigma^{-1} f_n(S) \cup \cdots \cup (\sigma^{-1} f_n)^{k-1}(S)$.

$\mathbf{I}'_n \wedge \mathbf{II}'_{n-1} \implies \mathbf{I}''_n$. Let $S \subset K_{n-1}^{\mathrm{alg}}$ be finite and such that $\sigma^k(S) = f_n^k(S)$ for some $k \in \mathbb{N}$. Then $K_{n-1}(S)_\sigma = K_{n-1}(S \cup \sigma(S) \cup \cdots \cup \sigma^{k-1}(S))$. By $\mathbf{II}'_{n-1}$, $S \subset K_{n-1}$ and this implies $n = 1$ and $S = \{0\}$.

$\mathbf{I}''_n \implies \mathbf{II}_n$. Suppose that L is a finite σ-stable extension of $K_{n-1}^{\mathrm{alg}}(D^n a)$ (by $\mathbf{I}''_n$, $D^n a$ is transcendental over K_{n-1}). Then the ramification locus of L over K_n gives us a finite set $S \subset K_{n-1}^{\mathrm{alg}}$ such that $\sigma(S) = f_n(S)$ (see the proof of 4.8 in [2]), and this contradicts $\mathbf{I}''_n$.

$\mathbf{II}_n \wedge \mathbf{II}'_{n-1} \implies \mathbf{II}'_n$. As before, we know that $\mathbf{II}'_0$ holds. Let L be a finite σ-stable extension of $K_n = K_{n-1}(D^n a)$. By $\mathbf{II}'_{n-1}$, $L \cap K_{n-1}^{\mathrm{alg}} = K_{n-1}$. Hence $[LK_{n-1}^{\mathrm{alg}} : K_{n-1}^{\mathrm{alg}} K_n] = [L : K_n] = 1$ by $\mathbf{II}_n$.

$\mathbf{I}''_n \wedge \mathbf{III}_{n-1} \implies \mathbf{III}_n$. Suppose there is such a solution $b \in K_n$. Applying σ to b we get $h(X), g(X) \in K_{n-1}[X]$ relatively prime with $g(X)$ monic such that $b = \frac{h(D^n a)}{g(D^n a)}$. As $\sigma(b) = b$,

$$\frac{h^\sigma(f_n(D^n a))}{g^\sigma(f_n(D^n a))} = \frac{h(D^n a)}{g(D^n a)}. \tag{2}$$

Note that, as $h(X)$ and $g(X)$ are relatively prime, $h^\sigma(f_n(X))$ and $g^\sigma(f_n(X))$ are relatively prime. Otherwise, they would have a common root α in K. This implies that $h(\beta) = g(\beta) = 0$ for $\beta = \sigma^{-1} f_n(\alpha)$. Also we have, by $\mathbf{III}_{n-1}$, that one of $h(X)$ and $g(X)$ is nonconstant.

As stated above, $\mathbf{I}''_n$ implies that $D^n a$ is transcendental over K_{n-1}; then in (1) we can replace $D^n a$ by X. We know that the left side and the right side of (2) should have the same poles, say, $\alpha_1, \ldots, \alpha_m \in K_{n-1}^{\mathrm{alg}}$.

Suppose $g(X)$ is not constant. Then $g(X) = \Pi_{i=1}^m (X - \alpha_i)$ and $g^\sigma(f_n(X)) = \Pi_{i=1}^m (f_n(X) - \sigma(\alpha_i))$ and they must have the same roots. Thus $f_n(\{\alpha_1, \ldots, \alpha_m\}) = \sigma(\{\alpha_1, \ldots, \alpha_m\})$ which contradicts $\mathbf{I}''_n$ unless $n = 1$ and $\{\alpha_1, \ldots, \alpha_m\} = \{0\}$. The same argument applies to h, but as remarked above, one of $h(X)$ and $g(X)$ is nonconstant, so $n = 1$ and we have $\frac{h(X)}{g(X)} = \alpha X^l$ with $\alpha \in K_0$ and $l \in \mathbb{Z}$.

Inverting b if necessary, we get $m \in \mathbb{N}$ such that α satisfies $\sigma(X) = (2a)^m X$. By $\mathbf{III}_0$ we have that $m = 0$ and $b = \alpha \in K$. ☐

Proof of $\mathbf{I}_1$ $K_0 = K(a)_\sigma$ and $f_1(X) = 2aX$. Suppose that there is a finite subset $S \subset K_0$ such that $\sigma(S) = f_1(S)$. $(\sigma^{-1} f_1)$ defines a permutation on S, so $(\sigma^{-1} f_1)^k = \mathrm{id}$ for some $k > 0$ (if $|S| = 1$, $k = 1$) and this implies that K_0 contains a solution b of $\sigma^k(x) = 2^k a\sigma(a)\dots\sigma^{k-1}(a)x$ with $b \in S$. In fact, any element of S is a solution of the equation.

Let $N \in \mathbb{N}$ be minimal such that $\sigma^N(b) \in K(a)$ (such N exists because $K_0 = K(a)_\sigma = K(\dots, \sigma^{-1}(a), a)$). Write $\sigma^N(b) = \frac{g(a)}{h(a)}$ with $g(X), h(X) \in K[X]$ relatively prime and $h(X)$ monic.

Applying σ^N to the equation satisfied by b we get

$$\frac{g^{\sigma^k}(f_0^k(a))}{h^{\sigma^k}(f_0^k(a))} = 2^k f_0^N(a)\dots f_0^{N+k-1}(a)\frac{g(a)}{h(a)}.$$

By minimality of N, $\frac{g(a)}{h(a)} \notin K(\sigma(a))$, but this is impossible if $N \geq 1$. Thus $N = 0$ and the equation is

$$\frac{g^{\sigma^k}(f_0^k(a))}{h^{\sigma^k}(f_0^k(a))} = 2^k a f_0(a)\dots f_0^{k-1}(a)\frac{g(a)}{h(a)}.$$

Since a is transcendental over K the last equation holds if we replace a by X. As the right-hand side and left-hand side should have the same poles and $g^{\sigma^k}(f_0^k(X))$ and $h^{\sigma^k}(f_0^k(X))$ are relatively prime, we have that $h^{\sigma^k}(f_0^k(X))$ and $h(X)$ have the same zeros. Comparing degrees and using the fact that h is monic, we conclude that $h(X) = 1$.

Then $g^{\sigma^k}(f_0^k(X)) = 2^k X f_0(X)\dots f_0^{k-1}(X)g(X)$. So $2^k \deg(g) = \deg(g)+2^k-1$, which implies $\deg(g) = 1$. Then $g(X) = cX + d$ with $c, d \in K$. Substituting in the equation we have $\sigma^k(c)f_0^k(X)+\sigma^k(d) = 2^k X^2 f_0(X)\dots f_0^{k-1}(X)c+2^k X f_0(X)\dots f_0^{k-1}(X)d$. Since the left-hand side has only even degrees and the degree of $Xf_0(X)\dots f_0^{k-1}(X)$ is odd we have $d = 0$. Finally, as $f_0^k(0) \neq 0$, the right-hand side has no constant term and we obtain $c = 0$; hence $b = 0$ and $\mathbf{I}_1$ is proved.

Now we assume that $\mathbf{I}_k$ holds for all $1 \leq k < n$, where $n \geq 2$. By what we have shown before, the following statements hold:

$$\mathbf{I}'_k \text{ for } 1 \leq k < n.$$
$$\mathbf{II}_k \text{ for } 1 \leq k < n.$$
$$\mathbf{II}'_k \text{ for } 0 \leq k < n.$$
$$\mathbf{I}''_k \text{ for } 1 \leq k < n.$$
$$\mathbf{III}_k \text{ for } 1 \leq k < n.$$

□

Proof of $\mathbf{I}_n$ Assume that there is a finite set $S \subset K_{n-1}$ such that $\sigma(S) = f_n(S)$. Let $\{a_1, \dots, a_m\}$ be a cycle in S (i.e., $\sigma(a_i) = f_n(a_{i+1})$ for $1 \leq i \leq m$ and $\sigma(a_m) = f_n(a_1)$). Then $\sigma(a_1 + \cdots + a_m) = 2a(a_1 + \cdots + a_m) + mb_n$. Let $e = \frac{1}{m}(a_1 + \cdots + a_m)$. Then $\sigma(e) = 2ae + b_n$ and as $f_n(X) = 2aX + b_n$, we have $\sigma(e) = f_n(e)$.

We will show that $\sigma(X) = 2aX + b_n$ has no solutions in K_{n-1}.

Case $n \neq 2$ We can write $b_n = 2nDaD^{n-1}a + c_1$ where $c_1 \in K_{n-2}$. Let us assume that there is a solution for $\sigma(X) = 2aX + b_n$ in K_{n-1}. We can write this solution as $g(D^{n-1}a)$ where $g(X) \in K_{n-2}(X)$. Since $\sigma(D^{n-1}a) = f_{n-1}(D^{n-1}a)$, we have the equation

$$g^\sigma(f_{n-1}(D^{n-1}a)) = 2ag(D^{n-1}a) + 2nDaD^{n-1}a + c_1.$$

By $\mathbf{I}''_{n-1}$ we know that $D^{n-1}a$ is transcendental over K_{n-2}, so replacing $D^{n-1}a$ by X we get $g^\sigma(2aX + b_{n-1}) = 2ag(X) + 2nDaX + c_1$.

If we take the derivative of this equation with respect to X we get

$$2a(g')^\sigma(2aX + b_{n-1}) = 2ag'(X) + 2nDa;$$

that is, $D^{n-1}a$ satisfies the equation

$$(g')^\sigma(2aX + b_{n-1}) = g'(X) + \frac{nDa}{a}. \tag{3}$$

We also have $2a(g'')^\sigma(2aX+b_{n-1}) = g''(X)$, and by $\mathbf{III}_{n-1}$, $g'(D^{n-1}a) = d(Da)^{-1}$ for some $d \in \operatorname{Fix}\sigma \cap K$. Thus $g''(X)$ is constant, so $g'(X)$ is a polynomial of degree at most 1 in X and its leading coefficient is $d(Da)^{-1}$. Now we look at the degrees in a of the equation (3): $\deg_a b_{n-1} = 0$, and as $\deg_a(d(Da)^{-1}) = 0$, $\deg_a(g'(X)) = \deg_a(g'(0)) = u$. If $u \le 0$ we have $\deg_a((g')^\sigma(2aX + b_{n-1})) = 1$ and if $u > 0$ we have $\deg_a((g')^\sigma(2aX + b_{n-1})) = \deg_a(g'(0)) = 2u$. In both cases, if we compute the degrees in (3) we get a contradiction.

Case $n = 2$ Then $b_2 = 2(Da)^2$, and the equation satisfied by e is $\sigma(e) = 2ae + 2(Da)^2$. We will show this equation has no solutions in K_1. If it has, and as by $\mathbf{I}''_1$ we can replace Da by X, there is $g(X) \in K_0(X)$ such that $g^\sigma(2aX) = 2ag(X) + 2X^2$. Taking the second derivative we get $4a^2(g'')^\sigma(2aX) = 2ag''(X) + 4$; that is,

$$(g'')^\sigma(2aX) = \frac{g''(X)}{2a} + \frac{1}{a^2}. \tag{4}$$

Taking the third derivative we obtain $4a^2(g''')^\sigma(2aX) = g'''(X)$; by $\mathbf{III}_1$, $g'''(Da) = d(Da)^{-2}$, which implies $g'''(X) = dX^{-2}$ and as $\frac{1}{X^2}$ is not the third derivative of a rational function, we have $d = 0$. Thus $g''(X) = b \in K_0$. Recall that $\sigma(a) = a^2 + 1$ and this implies that $K(\sigma(a)) = K(\sigma(a), \sigma^2(a), \ldots)$. Let M be the smallest natural number such that $\sigma^M(b) \in K(a)$. Write $\sigma^M(b) = \frac{P(a)}{Q(a)}$ where P and Q are relatively prime polynomials over K. Hence $\frac{P(a)}{Q(a)} \in K(\sigma(a))$. Then

$$\frac{\sigma(P(a))}{\sigma(Q(a))} = \frac{P(a)}{2Q(a)\sigma^M(a)} + \frac{1}{(\sigma^M(a))^2}.$$

If $M \ge 1$, by minimality of M, $\frac{P(a)}{Q(a)} \notin K(\sigma(a))$, but this is absurd. Hence $M = 0$. So the equation is

$$\frac{\sigma(P(a))}{\sigma(Q(a))} = \frac{P(a)}{2Q(a)a} + \frac{1}{a^2}. \tag{5}$$

Now we replace a by X. Then the zeros of $Q^\sigma(X^2+1)$ are contained in the zeros of $X^2Q(X)$. Moreover, to each zero α of $Q(X)$ correspond two zeros of $Q^\sigma(X^2+1)$, namely, $\sqrt{\sigma(\alpha)-1}$ and $-\sqrt{\sigma(\alpha)-1}$ (if $\alpha = 1$ the corresponding zero is 0 with multiplicity 2). Comparing the degrees in (5) we have that $\deg(Q) < 3$.

If $Q(0) = 0$, then $Q^\sigma(1) = 0$; hence $Q(1) = 0$ and $Q^\sigma(2) = 0$. Thus $Q(2) = 0$ which is a contradiction.

If $Q(0) \ne 0$ then in case $Q^\sigma(0) = 0$ we have that X divides $Q^\sigma(X^2+1)$. But all the occurrences of X in $Q^\sigma(X^2+1)$ have an even exponent; thus $Q^\sigma(X^2+1) = cX^2$. This implies that $Q(X)$ and $Q^\sigma(X^2+1)$ are relatively prime. If $r(X)$ is a prime divisor of $Q(X)$, then it is not a pole of the left side of (5), so $r(X)$ must divide $XP(X)+2XQ(X)$ and this implies that $r(X)$ divides $P(X)$ which is absurd. Hence $Q^\sigma(X^2+1)$ divides $Q(X)$ and this implies $\deg(Q)=0$. We have then $Q=1$. The equation is reduced to

$$P^\sigma(a^2+1)=\frac{P(a)}{2a}+\frac{1}{a^2}$$

and comparing the degrees in a we get a contradiction. Hence (4) has no solutions in K_1. This finishes the proof of $\mathbf{I}_n$.

Now, by $\mathbf{I}''_{n+1}$, $D^{n+1}a \notin K_n^{\text{alg}}$ so $\text{tr.dg}(K_{n+1}/K_n)=1$, and this implies that a is differentially transcendental over K. □

Proof of Lemma 3.4 Let $a \in A_2$ and $a \notin K$. By Proposition 3.5, a is differentially transcendental over K. Then $\text{tp}(a/K)$ is the only nonrealized type of A_2. As before, this implies that A_2 is strongly minimal.

Thus, in particular, $SU(A_2)=1$. Moreover, $\text{tp}(a/K)$ is trivial, thus 1-based. Indeed, let $a_1, a_2, a_3 \in A_2$ be such that $a_1 \perp_K a_2$, $a_1 \perp_K a_3$, and $a_3 \perp_K a_2$. We will show that $a_3 \perp_K a_1 a_2$. By 6.1 of [2], $\text{tp}_{\text{ACFA}}(a_3/Ka_1a_2)$ is orthogonal to $\text{Fix}\,\sigma$ and $\text{tp}_{\text{ACFA}}(Da_1Da_2\ldots/Ka_1a_2)$ is $\text{Fix}\,\sigma$-analyzable (recall that $D^n a_1$, $D^n a_2$, and $D^n a_3$ satisfy the equation $\sigma(X)=f_n(X)$). Thus, if $a_3 \in \text{acl}(Ka_1a_2)$, then $a_3 \in \text{acl}_\sigma(Ka_1a_2)$ and by 6.1 of [2], $a_3 \in \text{acl}_\sigma(Ka_1)$ or $a_3 \in \text{acl}_\sigma(Ka_2)$, which is absurd. As for Lemma 3.3, A_2 is stably embedded. □

4 Definable Subgroups of the Additive Group

We shall prove that a generic element of a definable subgroup of an additive group is finite-dimensional if and only if it has finite SU-rank. First, we will mention some properties of definable groups in supersimple theories. We refer to [5] for the definitions and proofs.

Let T be a supersimple theory, M a saturated model of T, and G an ∞-definable (definable by an infinite number of formulas) group over some set of parameters $A \subset M$.

Definition 4.1 Let $p \in S(A)$. We say that p is a left generic type of G over A if it is realized in G and for every $a \in G$ and b realizing p such that $a \perp_A b$, we have $b \cdot a \perp_A a$.

Proposition 4.2 *Let G be a $\varnothing$-definable group, H a $\varnothing$-definable subgroup of G, and let $A=\text{acl}(A)$.*

1. *Let $p \in S(A)$; then p is a generic of G over A if and only if $SU(G)=SU(p)$.*
2. *$SU(G)=SU(H)$ if and only if $[H:G]<\infty$.*
3. *$SU(H)+SU(G/H) \le SU(G) \le SU(H) \oplus SU(G/H)$.*

We call an element $a \in G$ a generic point of G if its type is a generic type. Thus a is a generic point if and only if its SU-rank equals $SU(G)$.

Now we reduce some questions concerning groups definable in a model of DCFA to questions on groups definable in differentially closed fields. These ideas are actually implicit in the axioms of DCFA. As for differentially closed fields, ACFA and algebraically closed fields, using ideals we can define a Noetherian topology for subsets of a power of a model of DCFA. We call it the (σ, D)-topology (see [1]).

Let $\mathcal{U}$ be a saturated model of DCFA, let $E=\text{acl}(E) \subset \mathcal{U}$, and let G be a connected differential algebraic group defined over E. For each $n \in \mathbb{N}$, let

$G^{(n)} = G \times \sigma(G) \times \cdots \times \sigma^n(G)$ and let q_n be the group homomorphism from G to $G^{(n)}$ defined by $q_n(g) = (g, \sigma(g), \ldots, \sigma^n(g))$. Let g be a generic point of G such that the tuples $g, \sigma(g), \ldots, \sigma^n(g)$ are differentially independent over E (such a generic exists because of the axioms of DCFA). Then $q_n(g)$ is a generic point of $G^{(n)}$ (in DCF); thus $q_n(G)$ is dense in $G^{(n)}$ (for the D-topology) and $G^{(n)}$ is connected.

Let H be a definable subgroup of G. For each $n \in \mathbb{N}$, let $H^{(n)}$ be the differential Zariski closure of $q_n(H)$ in $G^{(n)}$. Then $H^{(n)}$ is a differential algebraic subgroup of $G^{(n)}$.

Let $\tilde{H}^{(n)} = \{g \in G : q_n(g) \in H^{(n)}\}$. These subgroups of G form a decreasing sequence of quantifier-free definable groups containing H. Let $\tilde{H} = \bigcap_{n\in\mathbb{N}} \tilde{H}^{(n)}$; since the (σ, D)-topology is Noetherian, there is $N \in \mathbb{N}$ such that $\tilde{H} = \tilde{H}^{(N)}$. Then $\tilde{H}$ is the (σ, D)-Zariski closure of H.

Lemma 4.3 *Let G be a connected differential algebraic group and let H be a definable subgroup of G defined over $E = \mathrm{acl}(E)$, $\tilde{H}$ its (σ, D)-Zariski closure. Then $[\tilde{H} : H] < \infty$.*

Proof Let $g, h \in G$. By definition, $g \mathop{\smile\!\!\!\!\!\!|}_E h$ if and only if for every $n \in \mathbb{N}$ $q_n(g)$ and $q_n(h)$ are independent over E in the sense of DCF. By Definition 4.1 and the fact that $q_n(ab) = q_n(a)q_n(b)$ we have that given $g \in H$, then g is a generic of H if and only if, for every $n \in \mathbb{N}$, $q_n(g)$ is a generic of $H^{(n)}$ (in the sense of DCF). Thus a generic of H will be a generic of $\tilde{H}$ and, by Proposition 4.2, $SU(H) = SU(\tilde{H})$ and $[\tilde{H} : H] < \infty$. □

Lemma 4.4

1. *Let H be a quantifier-free definable subgroup of $\mathbb{G}_a^n$. Then H is a $(\mathrm{Fix}\,\sigma \cap \mathcal{C})$-vector space, so it is divisible and has therefore no proper subgroup of finite index. This implies that every definable subgroup of $\mathbb{G}_a^n$ is quantifier-free definable.*
2. *Let G be a definable subgroup of $\mathbb{G}_a^n$, and H a definable subgroup of G. Then G/H is definably isomorphic to a subgroup of $\mathbb{G}_a^l$ for some l.*

Proof (1) Using the fact that every algebraic subgroup of a vector group is defined by linear equations, it follows easily that every differential subgroup of a vector group is defined by linear differential equations. Hence, in the notation introduced above, each $\tilde{H}^n$ is defined by linear differential equations, and this implies that H is defined by linear (σ, D)-equations. Thus H is stable by multiplication by elements of $\mathrm{Fix}\,\sigma \cap \mathcal{C}$, and is therefore a $(\mathrm{Fix}\,\sigma \cap \mathcal{C})$-vector space.

This proves the first assertion. The others are clear, using the fact that every definable group has finite index in its (σ, D)-closure (by Lemma 4.3).

(2) Let L be an l-tuple of linear difference-differential equations such that $H = \mathrm{Ker}(L)$. Then L defines a group homomorphism $G \to \mathbb{G}_a^l$ with kernel H. $L(G)$ is a definable subgroup of $\mathbb{G}_a^l$. □

Theorem 4.5 *Let G be a definable subgroup of $\mathbb{G}_a^n$. If G has infinite dimension then $SU(G) \geq \omega$.*

Proof By Lemma 4.4, G is quantifier-free definable and is a $(\mathrm{Fix}\,\sigma \cap \mathcal{C})$-vector space.

Clearly, having infinite dimension as in Section 1 implies having infinite dimension as a vector space. If $g_1, \dots, g_n \in G$ are $(\operatorname{Fix}\sigma \cap \mathcal{C})$-linearly independent, then the subgroup H they generate is definable and has SU-rank n (since it is definably isomorphic to $(\operatorname{Fix}\sigma \cap \mathcal{C})^n$). Thus our hypothesis implies that G contains elements of arbitrarily high finite SU-rank, and therefore that $SU(G) \geq \omega$. $\square$

References

[1] Bustamante Medina, R., "Differentially closed fields of characteristic zero with a generic automorphism," *Revista de Matemática: Teoría y Aplicaciones*, vol. 14 (2007), pp. 81–100, http://simmac.emate.ucr.ac.cr/index.php/revista/article/view/181/166. 404, 405, 412

[2] Chatzidakis, Z., and E. Hrushovski, "Model theory of difference fields," *Transactions of the American Mathematical Society*, vol. 351 (1999), pp. 2997–3071. Zbl 0922.03054. MR 1652269. 404, 407, 408, 409, 412

[3] Kim, B., and A. Pillay, "Simple theories," Joint AILA-KGS Model Theory Meeting (Florence, 1995), *Annals of Pure and Applied Logic*, vol. 88 (1997), pp. 149–64. Zbl 0897.03036. MR 1600895. 405

[4] Marker, D., M. Messmer, and A. Pillay, *Model Theory of Fields*, vol. 5 of *Lecture Notes in Logic*, Springer-Verlag, Berlin, 1996. Zbl 0911.12005. MR 1477154. 403

[5] Pillay, A., "Definability and definable groups in simple theories," *The Journal of Symbolic Logic*, vol. 63 (1998), pp. 788–96. Zbl 0922.03056. MR 1649061. 412

[6] Pillay, A., and M. Ziegler, "Jet spaces of varieties over differential and difference fields," *Selecta Mathematica. New Series*, vol. 9 (2003), pp. 579–99. Zbl 1060.12003. MR 2031753. 407

Centro de Investigaciones en Matemática Pura y Aplicada
Escuela de Matemáticas
Universidad de Costa Rica
Sede Rodrigo Facio
2060, San José
COSTA RICA
ronald.bustamante@ucr.ac.cr