ON SUPERSTABLE FIELDS WITH AUTOMORPHISMS

Ehud Hrushovski

The Lie-Kolchin theorem states, essentially, that every connected solvable algebraic group over an algebraically closed field has a nilpotent derived group. This was generalized by Zil'ber and Nesin (independently) to groups of finite Morley rank. It was known that all ingredients of Nesin's proof generalize easily to superstable groups (satisfying an appropriate connectedness condition), except for the non-existence of definable groups of automorphisms of the field. The purpose of this note is to prove this fact: if F is a field, G a group of automorphisms of F, and (F,G) is superstable, then G = (1).

All groups are taken to be ∞-definable in $\mathbb{C}$, the universal domain of a superstable theory. We will use the notation of [M], and the theory of local weight in groups from [H, §3.3]. The basic definition is that of a regular type. The idea is that the elements of the group are co-ordinatized by n-tuples of realizations of the regular type. Thus for example if $A = (Z/2Z)^{\omega}$, with generic type p, then $B = A \times A$ is p-simple: an element of B is a pair of elements of A. But if $B = (Z/4Z)^{\omega}$, and A is identified with 2B, then B is not p-simple: an element of B can be analyzed in terms of p, but not in one step. Call a group p-connected if it is p-simple, connected, and has a generic type domination-equivalent to a power of p. One has the following existence property.

Fact 1. Let G be a group, H a group acting on G, and suppose the generic type of G is non-orthogonal to the regular type p. Then G has a normal, H-invariant subgroup N such that G/N is p-simple.

If p is chosen to have minimal possible U-rank, so that every forking extension of p is orthogonal to G, then every generic type of G/N will necessarily be $\equiv p^n$ for some n. In particular, every (superstable) group G has a filtration $G = G_n \supset G_{n-1} \supset \ldots \supset G_j = (1)$ such that each G_j is normal in G, and G/G_n is p-connected for some regular type p. So every simple group is p-connected for some p. The same is true for fields: If $G = G_a$ is the additive group of a field, then the multiplicative group $H = G_m$ acts transitively on G_a-(0). Since the filtration can be chosen to consist of H-invariant groups, it follows that $n = 1$ and G_a is p-connected.

Lemma 2 (Zil'ber): Let G be a p-connected group acting on the p-connected Abelian group V. Assume that V has no nontrivial G-invariant p-connected subgroups of smaller p-weight. Let $F = \mathrm{End}_G(V)$. Then F is a definable field, and V is definably an F-vector space.

Proof: Let $a \in V$- (0). By the indecomposability lemma (to be proved below), the subset of V generated by $\{x \cdot a : x$ realizes the generic type of G over $a\}$ by the operation $(u,v,w) \longrightarrow u - v + w$ is a coset of some ∞-definable subgroup of V. By minimality, this subgroup must be all of V. A fortiori, Ga generates V. Thus V is a simple $Z[G]$-module. By Schur's lemma, F is a division ring. Now F-(0) is the set of G-automorphisms of V: by [H, §4.2, lemma 2 and §3.4, theorem 2], it is definable. Hence so is F.

The use of the "indecomposability lemma" could have been avoided, but this seems pointless.

Proposition 3: Let F be a field, G a group of automorphisms of F, and assume that the structure $(F,+,\cdot,G$, action of G on $F)$ is superstable. Then $G = 1$.

Proof : If G is finite, then F must be algebraic over the fixed field F_0 of G. F_0 is a definable subfield, so it is algebraically closed; so $F = F_0$, i.e. $G = 1$.

Suppose G is infinite. Let F_0 be the algebraic closure of the prime field of F. Note that each element of F_0 has finite orbit under the action of G, so the connected component $G°$ of G must fix F_0 pointwise. Choose any element $\sigma \in G°$, $\sigma \neq 1$. We will show that the structure $(F,+,\cdot,\sigma)$ is already unsuperstable.

<u>Case 1</u> F has characteristic 2.
Let $h(x) = \sigma(x)+x$. h is an additive endomorphism of F. The kernel K of h is precisely the fixed field of F. Let p be a regular type such that K is p-connected. As K is a proper subfield of F, we have $w_p(K) = 0$. By additivity of weight, $w_p(\text{range}(h)) = w_p(F)$; so by semi-regularity, the range of h is all of F. In particular, there exists $x \in F$ such that $h(x) = 1$. So $\sigma(x) = x + 1 \neq x$, but $\sigma^2(x) = \sigma(x+1) = x+2 = x$. Let $K_0 = \{x: \sigma x = x\}$, $K_1 = \{x: \sigma^2 x = x\}$. Then K_1 is an extension of degree 2 of K_0, contradicting the fact that K_0 is algebraically closed.

<u>Case 2</u> F has characteristic other than 2.
Define h by: $h(x) = \sigma(x)/x$ for $x \neq 0$. Then h is a multiplicative endomorphism whose kernel is a proper subfield (minus $\{0\}$), so h is onto. Choose x such that $h(x) = -1$, and continue as in the previous case.

Problem 3. If σ is an automorphism of a field F, and (F,σ) is superstable, must σ be a power of the Frobenius automorphism? (Note that σ must have a finite fixed field by the above proof, so in particular F has prime characteristic).

Proposition 4: Let G be a p-connected group acting on the p-connected Abelian group V. Let N be a normal Abelian subgroup of G. Assume that V,G,N are non-trivial, and that every proper G-invariant p-connected subgroup of V is trivial. Let $R = \text{End}_N(V)$ and let F be the center of R.

Then F is a definable field, V is (definably) a finite-dimensional F-vector space, and G acts F linearly on V.

Proof: Let U be a p-connected, N-invariant subgroup of V of least possible non-zero p-weight. By the minimality of A and the finiteness of p-weight, V is a finite direct sum of G-conjugates of U. It follows that R is isomorphic to the $n \times n$ matrix ring over $End_N(U)$, so the center F of R is isomorphic to $End_N(U)$. By lemma 2, F is a definable field; so R is definable. Since N is Abelian, each $\sigma \in N$ acts on V as an N-endomorphism. This gives an embedding of N into the center of R, i.e. into F. In particular, $w_p(F) > 0$, so V is finite-dimensional as an F-space. R and its action on V are clearly 0-definable, hence so is F=center(R). Thus G acts on F naturally. By proposition (3), the action is trivial. So G acts F-linearly on V.

The rest of Nesin's proof of the Lie-Kolchin theorem is routine.

We now present a version of Zil'ber's indecomposability theorem in the context of regular types; Lascar and Berline have proved it at the same level of generality using U-rank, so it is only presented in order to demonstrate the technique. A subset C of G is a (left) coset of some subgroup if and only if C is closed under the operation: $(x,y,z) \rightarrow xy^{-1}z$. If this is the case, then C is a right translate of a unique subgroup S of G, namely $S = CC^{-1}$. If C is (∞-) definable, then so is S, and a type of C is called generic iff it is a translate of a generic type of S. The coset generated by a subset X of G is by definition the closure of X under the above operation.

Remark 5: Let q be a type of elements of a group G.
(a) q is the generic type of some ∞-definable subgroup of G iff q satisfies: for $(a_1,a_2) \models q^2$, $a_1a_2 \models q$.
(b) q is the generic type of a ∞-definable coset of G iff q satisfies: for $(a_1,a_2,a_3) \models q^3$, $a_1a_2^{-1}a_3 \models q$.

Proof:

(a) Let $S = \{ab: a \models q \text{ and } b \models q\}$. Note that if $(a_1,a_2) \models q^2$, then $a_1a_2 \models q \mid a_1$: for any translation-invariant rank, $rk(q) = rk\,(a_1a_2/\varnothing) \geq rk\,(a_1a_2/a_1) = rk\,(a_2/a_1) = rk\,(a_2/\varnothing) = rk(q)$, so equality holds. It follows that whenever $(b_1b_2) \models q^2$, $b_1^{-1}b_2 \models q$. To see that S is a group, it suffices to show that if a,b,c each realize q, then $abc=de$ for some d, e realizing q. Let $f \models q \mid \{a,b,c\}$. Then $abc = (af)(f^{-1}bc)$. By the previous remark, $f^{-1}b \models q$, and one sees easily that $f^{-1}b \downarrow C$; so $f^{-1}bc \models q$. Let $d = (af)$, $e = (f^{-1}bc)$.

(b) Let $r = stp(a_1a_2^{-1})$ for $(a_1,a_2) \models q^2$. r clearly satisfies the condition for being the generic type of a group S. By definition of r, q is the generic type of Sa_2 whenever $a_2 \models q$.

Proposition 6 (Indecomposability): Let G be a group, p a regular type. Let $F^* = \{s: s = stp(a/\varnothing)$ for some $a \in G$, $s \,\square\, p^n$ for some $n > 0$, and s is p-simple$\}$. Assume $w_p(s)$ is bounded for $s \in F^*$. Then:

(a) If $r \in F^*$, then the coset generated by $\{x \in G: x \models r\}$ is ∞-definable, with generic type in F^*.

(b) Let G_i $(i \in I)$ be a collection of ∞-definable connected groups whose generic types are in F^*. Then the group generated by $\cup_i G_i$ is ∞-definable, and its generic type is in F^*.

Proof: Define two operations on F^*: if $q,r \in F^*$, choose $(a,b) \models q \otimes r$, and let $q^{-1} = stp(a^{-1})$, $q \cdot r = stp(a \cdot b)$. Note that $\cdot$ is associative. Also, $w_p(q^{-1}) = w_p(q)$, and $w_p(q \cdot r) \geq w_p(q)$. $[w_p(ab) \geq w_p(ab/b) = w_p(a/b) = w_p(a)]$.

Let F be a subset of F^* closed under the operation: $(q_1,q_2,q_3) \to q_1 \cdot q_2^{-1} \cdot q_3$. Choose $q \in F$ of largest p-weight. Then for any $r \in F$ one has $w_p(q) \geq w_p\,(q \cdot r^{-1}) = w_p(q)$. Recall that if t is p-simple and $\square\, p^n$ then every forking extension of t has smaller p-weight than t. It follows that if $(a,b,c) \models q \otimes r \otimes r$ then $ab^{-1} \downarrow b$. Since we also have $ab^{-1} \downarrow c$, $stp(b/ab^{-1}) = stp(c/ab^{-1})$, so there exists $a' \models q$ such that $ab^{-1} = a'c^{-1}$. So $ab^{-1}c = a'c^{-1}c = a'$. This shows that with our choice of q, $q \cdot r^{-1} \cdot r = q$ for any $r \in F$. In particular,

$q \cdot q^{-1} \cdot q = q$, so by Remark 5, q is the generic type of some ∞-definable coset.

To prove (b), let q_i be the generic type of G_i, and let F be the closure of $\{q_i : i \in I\}$ under the operation defined in the first line of the previous paragraph. One obtains an ∞-definable coset C with generic type q such that $q \cdot q_i^{-1} \cdot q_i = q$ for each i. It follows that each $G_i \subset S$, where S is the subgroup of G for which C is a right coset of S. From the construction of C it is clear that S is contained in the subgroup generated by the union of the G_i's (indeed C is). So this subgroup equals S.

For (a), let F be the closure of $\{r\}$ under the same operation. So $F = \{r_n : n \text{ odd}\}$, where $r_n = r \cdot r^{-1} \cdot r \cdot \ldots \cdot r^{\nu(n)}$ (n times; $\nu(n) = (-1)^n$). Let q, C be as in the first paragraph. Then it is clear that C is contained in the coset generated by r. Conversely, say $q = r_n$. From $q \cdot r^{-1} \cdot r = q$ one sees that r_m depends only on the parity of m for $m \geq n$. So $q = r_{2n+1} = r_n \cdot r_n^{-1} \cdot r = q \cdot q^{-1} \cdot r$. From this, one sees easily that every realization of r lies in the coset generated by the realizations of q.

References

[H] Hrushovski, E., Doctoral Dissertation, Berkeley 1986.

[N] Nesin, A., Doctoral Dissertation, Yale 1985.

[M] Makkai, M., A survey of basic stability theory, Isr. J. Math. v. 49 Nos. 1-3 (1981), pp. 181-238.

[Z] Zil'ber, B., Some model theory of simple algebraic groups over algebraically closed fields, Coll. Math. XLVII (1984),pp. 175-180.