

A COUNTABLE STRUCTURE DOES NOT HAVE A FREE UNCOUNTABLE AUTOMORPHISM GROUP

SAHARON SHELAH

ABSTRACT

It is proved that the automorphism group of a countable structure cannot be a free uncountable group. The idea is that instead of proving that every countable set of equations of a certain form has a solution, it is proved that this holds for a co-meagre family of appropriate countable sets of equations.

Can a countable structure have an automorphism group that is a free uncountable group? This was a well-known problem in group theory, at least in England. David Evans posed the question at the Durham meeting on model theory and groups which Wilfrid Hodges organised in 1987, and we thank Simon Thomas for telling us about it. Later and independently, in descriptive set theory, Becker and Kechris [1] asked if there is an uncountable free Polish group, that is, one which is on a complete, separable metric space, and for which the operations are continuous. Motivated by this, Solecki [4] proved that the group of automorphisms of a countable structure cannot be an uncountable free Abelian group. For further information, see [2] from which, as a byproduct, we can say something on uncountable structures.

Here, we prove the following theorem.

THEOREM 1. *If \mathbf{A} is a countable model, then $\text{Aut}(\mathbf{A})$ cannot be a free uncountable group.*

The proof follows from the following two claims, one establishing a property of G , and the other proving that free groups do not have it.

A proof of a similar result for general Polish groups is under preparation (see [3]; this also gives more on the Remark 5(2)).

We thank Dugald Macpherson for pointing out some inaccuracies in an earlier version of the paper.

NOTATION 2.

- (1) Let ω denote the set of natural numbers, and let $x < \omega$ mean ‘ x is a natural number’.
- (2) Let a, b, c and d denote members of G (the group).
- (3) Let \mathbf{d} denote the ω -sequence $\langle d_n : n < \omega \rangle$, and similarly in other cases.
- (4) Let $k, \ell, m, n, i, j, r, s$ and t denote natural numbers (and so also elements of the structure \mathbf{A} , which, for notational simplicity, we assume is the set of natural numbers).

Received 6 November 2000; revised 19 November 2001.

2000 *Mathematics Subject Classification* 20B27 (primary); 03E15, 03C60 (secondary).

This research was partially supported by the Israel Science Foundation.

PROPOSITION 3. Assume that \mathbf{A} is a countable structure with automorphism group G , and for notational simplicity assume that its set of elements is ω (also, of course, it is infinite; otherwise, the proposition is trivial).

We define a metric \mathfrak{d} on G by

$$\mathfrak{d}(f, g) = \sup\{2^{-n} : f(n) \neq g(n) \text{ or } f^{-1}(n) \neq g^{-1}(n)\}.$$

Then the following statements hold.

(1) G is a complete, separable metric space under \mathfrak{d} , in fact, a separable topological group.

(2) If \mathbf{d} is an ω -sequence of members of $G \setminus \{e_G\}$ converging to e_G , then for some (strictly increasing) ω -sequence \mathbf{j} of natural numbers, the pair (\mathbf{d}, \mathbf{j}) satisfies the following conditions.

(*) For any sequence $\langle w_n(x_1, x_2, \dots, x_{\ell_{1,n}}; y_1, y_2, \dots, y_{\ell_{2,n}}) : n < \omega \rangle$ (that is, an ω -sequence of non-degenerate group words) obeying \mathbf{j} (see below), we can find a sequence \mathbf{b} from G , that is, $b_n \in G$ for $n < \omega$ such that

$$b_n = w_n(d_{n+1}, d_{n+2}, \dots, d_{n+\ell_{1,n}}; b_{n+1}, b_{n+2}, \dots, b_{n+\ell_{2,n}}) \text{ for any } n.$$

We say that $\langle w_n(x_1, x_2, \dots, x_{\ell_{1,n}}; y_1, y_2, \dots, y_{\ell_{2,n}}) : n < \omega \rangle$ obeys \mathbf{j} whenever:

- (*)₁ if $m < j_n$, then $m + \ell_{1,m} < j_{n+1}$ and $m + \ell_{2,m} < j_{n+1}$, and
- (*)₂ for any $n^*, m^* < \omega$ we can find $i(0)$ and $i(1)$ such that
- (*)₃ $m^* < i(0)$, $n^* < i(0)$, $i(0) < i(1)$, and w_t is trivial (which means that $w_t = y_1$) for $t = j_{i(0)}, j_{i(0)} + 1, \dots, j_{i(1)}$, and $f_2(j_{i(0)}, n^*, j_{i(0)}) < i(1) - i(0)$, where
- (*)₄ (i) the length of a word $w = w(z_1, \dots, z_r)$, which in canonical form is $z_{\pi(1)}^{i(1)} z_{\pi(2)}^{i(2)} \dots z_{\pi(s)}^{i(s)}$, where $t(i) \in \mathbb{Z}$ and π is a function from $\{1, 2, \dots, s\}$ into $\{1, \dots, r\}$, is

$$\text{length}(w) = \sum_{i=1, \dots, s} |t(i)|;$$

(ii) for $s \leq i$, we let

$$f_1(i, s) = \prod_{t=s, \dots, i-1} \text{length}(w_t)$$

(note that this is greater than or equal to 1, as all values of w_t are non-degenerate);

(iii) for $n \leq s \leq i$, we let

$$f_2(i, n, s) = \sum_{r=n, \dots, s-1} f_1(i, r+1) \times \text{length}(w_r),$$

and $f_2(i, n, s) = f_2(i, n, i)$ if $n \leq i < s$.

Proof.

(1) This should be clear.

(2) So we are given the sequence \mathbf{d} . We choose the increasing sequence \mathbf{j} of natural numbers by letting $j_0 = 0$, j_{n+1} be the first $j > j_n$ such that

(*)₅ for every $\ell \leq n$ and $m < j_n$, we have $d_\ell(m) < j$ and $(d_\ell)^{-1}(m) < j$, and $[k \geq j \Rightarrow d_k(m) = m]$.

Note that j_{n+1} is well defined, as the sequence \mathbf{d} converges to e_G ; so for each $m < \omega$ and for every large enough $k < \omega$, we have $d_k(m) = m$.

We shall prove that $\mathbf{j} = \langle j_n : n < \omega \rangle$ is as required in part (2) of the proposition. So let a sequence

$$\mathbf{w} = \langle w_n(x_1, x_2, \dots, x_{\ell_{1,n}}; y_1, y_2, \dots, y_{\ell_{2,n}}) : n < \omega \rangle$$

of group words obeying \mathbf{j} be given (see $(*)_1$, $(*)_2$ and $(*)_3$ above). Then $f_1(i, s)$ and $f_2(i, n, i)$ are well defined.

For each $k < \omega$, we define the sequence $\langle b_n^k : n < \omega \rangle$ of members of G as follows. For $n > k$, we let b_n^k be e_G , and now we define b_n^k by downward induction on $n \leq k$, letting

$$(*)_6 \quad b_n^k = w_n(d_{n+1}, d_{n+2}, \dots, d_{n+\ell_{1,n}}; b_{n+1}^k, b_{n+2}^k, \dots, b_{n+\ell_{2,n}}^k).$$

Now we shall work on proving that

$$(*)_7 \quad \text{for each } n^*, m^* < \omega, \text{ the sequence } \langle b_n^{k^*}(m^*) : k < \omega \rangle \text{ is eventually constant.}$$

[Why does $(*)_7$ hold? By the definition of ‘ \mathbf{w} obeys \mathbf{j} ’, we can find $i(0)$ and $i(1)$ such that

$$(*)_8 \quad m^* < i(0), n^* < i(0), i(0) < i(1), \text{ and } w_t \text{ is trivial for } t = j_{i(0)}, j_{i(0)} + 1, \dots, j_{i(1)}, \\ \text{and } f_2(j_{i(0)}, n^*, j_{i(0)}) < i(1) - i(0); \text{ actually, } m^* < j_{i(0)} \text{ suffices.}]$$

Now let $k(*) = \text{df } j_{i(1)+1}$; we claim that

$$(*)_9 \quad \text{if } k \geq k(*) \text{ and } s \geq j_{i(1)}, \text{ then } b_s^k \text{ restricted to the interval } [0, j_{i(1)-1}] \text{ is the identity.}$$

[Why? If $s > k$, this holds by the choice of the b_s^k as the identity everywhere. Now we prove $(*)_9$ by downward induction on $s \leq k$ (but, of course, $s \geq j_{i(1)}$). However, by the definition of composition of permutations, it suffices to show that

$$(*)_{9a} \quad \text{every permutation mentioned in the word}$$

$$w_s(d_{s+1}, \dots, d_{s+\ell_{1,s}}, b_{s+1}^k, \dots, b_{s+\ell_{2,s}}^k)$$

maps every $m < j_{i(1)-1}$ to itself.

Let us check this criterion. The $d_{s+\ell}$ for $\ell = 1, \dots, \ell_{1,s}$ satisfy this, as the indexes $(s + \ell)$ are greater than or equal to $j_{i(1)}$ and $m < j_{i(1)-1}$; now we apply the choice of $j_{i(1)}$.

The $b_{s+1}^k, \dots, b_{s+\ell_{2,s}}^k$ satisfy this by the induction hypothesis on s . So the demand in $(*)_{9a}$ holds, and hence we complete the downward induction on s . So $(*)_9$ holds.]

$$(*)_{10} \quad \text{If } k \geq k(*) \text{ and } s \in [j_{i(0)}, j_{i(1)}], \text{ then } b_s^k \text{ is the identity on the interval } [0, j_{i(1)-1}].$$

[Why? We prove this by downward induction; for $s = j_{i(1)}$ this holds by $(*)_9$. If it holds for $s + 1$, recall that w_s is trivial; that is, $w_s = y_1$, and hence $b_s^k = b_{s+1}^k$, so this follows.]

$$(*)_{11} \quad \text{For every } k \geq k(*) \text{ we find that for every } s \geq j_{i(0)}, \text{ the functions } b_s^k, b_s^{k(*)} \\ \text{agree on the interval } [0, j_{i(1)-1}], \text{ and they are both the identity on it. Also, } (b_s^k)^{-1} \\ \text{and } (b_s^{k(*)})^{-1} \text{ agree on this interval, and both are the identity on it.}$$

[Why? For $s \geq j_{i(1)}$, this holds by $(*)_9$; for $s \in [j_{i(0)}, j_{i(1)}]$, by $(*)_{10}$.]

$$(*)_{12} \quad \text{For any } s \in [n^*, \omega) \text{ and } m < j_{i(0)+f_2(j_{i(0)}, n^*, s)}, \text{ we find that } k \geq k(*) \text{ (equal to } j_{i(1)+1}) \\ \text{implies that}$$

$$b_s^k(m) = b_s^{k(*)}(m) \quad \text{and} \quad (b_s^k)^{-1}(m) = (b_s^{k(*)})^{-1}(m).$$

If, in addition, t satisfies $t \leq i(0) + f_2(j_{i(0)}, n^*, s)$ and $m < j_t$, then $b_s^{k(*)}(m)$ and $(b_s^{k(*)})^{-1}(m)$ are less than $j_{t+f_1(j_{i(0)}, s)}$.

Before proving this, as we assume that

$$f_2(j_{i(0)}, n^*, s) \leq f_2(j_{i(0)}, n^*, j_{i(0)}) < i(1) - i(0),$$

we note that necessarily $m < j_{i(0)+(i(1)-i(0)-1)} = j_{i(1)-1}$.

Case 1: $s \geq j_{i(0)}$.

[Why? This holds by $(*)_{11}$, because (as was noted above) $m < j_{i(1)-1}$.]

We prove this by downward induction on s (for all m and k , as above).

Case 2: We now prove it for $s < j_{i(0)}$, assuming that we have it for all relevant $s' > s$ (and $s \geq n^*$, of course).

Let $k \geq k^*$, let $t \leq i(0) + f_2(j_{i(0)}, n^*, s)$, and let $m < j_t$. Note that

$$\begin{aligned} t + f_1(j_{i(0)}, s + 1) \times \text{length}(w_s) &\leq i(0) + f_2(j_{i(0)}, n^*, s) + f_1(j_{i(0)}, s) \\ &= i(0) + f_2(j_{i(0)}, n^*, s + 1), \end{aligned}$$

and hence for $s' = s + 1, s + 2, \dots, s + \ell_{1,s}$, the induction hypothesis applies to every

$$t' \leq t + f_1(j_{i(0)}, s + 1) \times \text{length}(w_s).$$

(Recall that $f_1(j_{i(0)}, s')$ is non-increasing in s' .)

We concentrate on proving that $b_s^k(m) = b_s^{k^*}(m) < j_{t+f_1(j_{i(0)}, s)}$, as the proof of $(b_s^k)^{-1}(m) = (b_s^{k^*})^{-1}(m) < j_{t+f_1(j_{i(0)}, s)}$ is the same. So

$$b_s^k(m) = w_s(d_{s+1}, \dots, d_{s+\ell_{1,s}}, b_{s+1}^k, \dots, b_{s+\ell_{2,s}}^k).$$

Let us write this group expression as the product $u_{s,1}^k \dots u_{s,\text{length}(w_s)}^k$, where each $u_{s,r}^k$ is one of $\{d_{s+1}, \dots, d_{s+\ell_{1,s}}, b_{s+1}^k, \dots, b_{s+\ell_{2,s}}^k\}$, or is an inverse of one of them.

For $r = 0, 1, \dots, \text{length}(w_s)$, let

$$v_{s,r}^k = u_{s,\text{length}(w_s)+1-r}^k \dots u_{s,\text{length}(w_s)}^k,$$

so $v_{s,r}^k \in G$ is the identity permutation for $r = 0$, and is

$$w_s(d_{s+1}, \dots, d_{s+\ell_{1,s}}, b_{s+1}^k, \dots, b_{s+\ell_{2,s}}^k) = b_s^k$$

for $r = \text{length}(w_s)$ and

$$j_{t+f_1(j_{i(0)}, s+1) \times \text{length}(w_s)} = j_{t+f_1(j_{i(0)}, s)}$$

by the definition of f_1 . Hence it suffices to prove the following statement.

(*)_{12a} if $r \in \{0, \dots, \text{length}(w_s)\}$ and $m < j_t$, then

$$v_{s,r}^k(m) = v_{s,r}^{k^*}(m) < j_{t+f_1(j_{i(0)}, s+1) \times r}.$$

[Why does (*)_{12a} hold? We do it by induction on r ; now for $r = 0$, the permutation is the identity, and thus trivial. For $r + 1$, we have

$$v_{s,r+1}^k(m) = u_{s,\text{length}(w_s)-r}^k(v_{s,r}^k(m)).$$

Note that if

$$u_{s,\text{length}(w_s)-r}^k \in \{b_{s+1}^k, \dots, (b_{s+1}^k)^{-1}, \dots\},$$

then $u_{s,\text{length}(w_s)-r}^k$ can map any $m' < j_{t+f_1(j_{i(0)}, s+1) \times r}$ only to numbers

$$m'' < j_{t+f_1(j_{i(0)}, s+1) \times r + f_1(j_{i(0)}, s+1)}$$

because (*)₁₂ has been proved for $b_{s'}^k$ and $b_{s'}^{k^*}$ when $s' > s$ is appropriate. Together with the induction hypothesis, this gives the conclusion of (*)_{12a} if

$$u_{s,\text{length}(w_s)-r}^k \in \{b_{s+1}^k, \dots, (b_{s+1}^k)^{-1}, \dots\}.$$

Otherwise,

$$u_{s,\text{length}(w_s)-r}^k \in \{d_{s+1}, \dots, d_{s+1}^{-1}, \dots\},$$

so the equality

$$u_{s,\text{length}(w_s)-r}^k(m') = u_{s,\text{length}(w_s)-r}^{k^*}(m')$$

is trivial. For the inequality (that this is less than $j_{l+f_1(j_{i(0),s+1}) \times (r+1)}$), just remember the definition of j_i ; here, adding 1 was enough.]

So we have proved $(*)_{12a}$, and hence $(*)_{12}$. Thus, using $(*)_{12}$ for $s = n^*$, we have

$$k \geq k(*) \& m < j_{i(0)} \quad \Rightarrow \quad b_n^k(m) = b_n^{k(*)}(m);$$

in particular, this holds for $m = m^*$ (as $m^* < j_{i(0)}$). Hence $(*)_7$ holds true.

Lastly,

$(*)_{13}$ for each $n^*, m^* < \omega$ the sequence $\langle (b_n^k)^{-1}(m^*) : k < \omega \rangle$ is eventually constant.

[Why? See the proof of $(*)_7$.]

Together, we can define for any $m, n < \omega$ the natural number $b_n^*(m)$ as the eventual value of $\langle b_n^k(m) : k < \omega \rangle$. So b_n^* is a well-defined function from the natural numbers to themselves (by $(*)_7$); in fact, it is one-to-one (as each b_n^k is) and is onto (by $(*)_{13}$), so it is a permutation of \mathbf{A} . Clearly, the sequence $\langle b_n^k : k < \omega \rangle$ converges to b_n^* as a permutation, the metric is actually defined on the group of permutations of the family of members of \mathbf{A} , and G is a closed subgroup; so b_n^* actually is an automorphism of \mathbf{A} . Similarly, the required equations

$$b_n^* = w_n(d_{n+1}, \dots, d_{n+\ell_{1,n}}, b_{n+1}^*, \dots, b_{n+\ell_{2,n}}^*)$$

hold. □

PROPOSITION 4. *The conclusion (parts 1 and 2) of Proposition 3 fails for any uncountable free group G .*

Proof. Let Y be a free basis of G ; as G is a separable metric space, there is a sequence $\langle c_n : n < \omega \rangle$ of (pairwise distinct) members of Y with $\mathfrak{d}(c_n, c_{n+1}) < 2^{-n}$. Let $d_n = (c_{2n})^{-1}c_{2n+1}$, so $\langle d_n : n < \omega \rangle$ converges to e_G and $d_n \neq e_G$. Assume that $\mathbf{j} = \langle j_n : n < \omega \rangle$ is as in the conclusion of Proposition 3, and we shall eventually get a contradiction. Let H be a subgroup of G generated by some countable $Z \subseteq Y$, and including $\{c_n : n < \omega\}$.

Now

$(*)_1$ $\langle d_n : n < \omega \rangle$ satisfies the conclusion of Proposition 3 in H as well.

[Why? We know that there is a projection from G onto H , and $d_n \in H$.]

For each $v \in {}^\omega\omega$, let $\mathbf{w}_v = \langle w_n^v : n < \omega \rangle$, where

$$w_n^v = w_n^v(x_1, y_1) = \begin{cases} x_1(y_1)^{k+1}, & \text{if } v(n) = 2k + 1, \\ (y_1)^{k+1}, & \text{if } v(n) = 2k, \end{cases}$$

so this is a sequence of words as mentioned in Proposition 3, and $v(n) = 0$ implies that w_n is trivial; that is, it equals y_1 . Recalling that we consider ${}^\omega\omega$ as a Polish space in the standard way,

$(*)_2$ the set of $v \in {}^\omega\omega$ for which \mathbf{w}_v obeys \mathbf{j} is co-meagre.

[Why? This is easy; for each $n^*, m^* < \omega$ the set of $v \in {}^\omega\omega$ for which \mathbf{w}_v fail to satisfy the demand for n^* and m^* is nowhere dense (and closed); hence the set of those failing it is the union of countably many nowhere dense sets, and thus is meagre.]

$(*)_3$ For each $a \in H$, the family of $v \in {}^\omega\omega$ such that there is a solution \mathbf{b} for $(\mathbf{d}, \mathbf{w}_v)$ in H satisfying $b_0 = a$ is nowhere dense.

[Why? Given a finite sequence v of natural numbers, note that for any sequence $\rho \in {}^\omega\omega$ of which v is an initial segment and solution \mathbf{b} for $(\mathbf{d}, \mathbf{w}_\rho)$ satisfying $b_0 = a$, we can show by induction on $n \leq \text{lg}(v)$ that b_n is uniquely determined (that is, it does not depend on ρ). We call it $b[n, v, \mathbf{d}]$, and we use the fact that in a free group, for every $k \geq 1$, any member of the group has at most one k th root. Now, if $b[\text{lg}(v), v, \mathbf{d}]$, which is a member of G , is not e_G , then for some $t < \omega$ it has no t th root, and if we let $v_1 = v \frown \langle 2t - 2 \rangle$, we are done. If not, and if we let $v_0 = v \frown \langle 1 \rangle$, then $b[\text{lg}(v) + 1, v_0, \mathbf{d}]$ is also well defined and equal to $d_{\text{lg}(v)}$; hence (by the choice of the values of d_n) it is not e_G . Therefore, for some $t < \omega$ it has no t th root, and so $v_1 = v_0 \frown \langle 2t - 2 \rangle$ is as required.]

Now we can finish the proof of Proposition 4, as follows. Just by $(*)_2$, $(*)_3$ and the Baire theorem, for some $v \in {}^\omega\omega$, the sequence \mathbf{w}_v of group words obeys \mathbf{j} , and there is no solution for $(\mathbf{d}, \mathbf{w}_v)$ in H . There is hence no solution in G . \square

Proof of Theorem 1. This follows from Propositions 3 and 4. \square

CONCLUDING REMARKS 5.

(1) In the proof of Proposition 4, we do not use the full strength of ‘ G is free’. For example, it is enough to assume that the following statements hold.

- (a) If $g \in G$, $g \neq e_G$, then for some $t > 1$, g has no t th root, and for every $t > 1$ it has at most one t th root (in G).
- (b) If X is a countable subset of G , then there is a countable subgroup H of G which includes X , and there is a projection from G onto H .
- (c) G is uncountable.

The uncountable free Abelian groups fall under this criterion; in fact by Proposition 3, G is ‘large’ and ‘rich’.

(2) What about uncountable structures? Sometimes a parallel result holds, an approximation to ‘if $\lambda = \beth_\omega$ ’, replacing ‘countable’ by ‘of cardinality less than \beth_ω ’. More generally, we assume that

$$\aleph_0 < \lambda = \sum_{n < \omega} \lambda_n \quad \text{and} \quad 2^{\lambda_n} < 2^{\lambda_{n+1}}, \quad \text{for } n < \omega;$$

hence $\mu = \text{df} \sum_{n < \omega} 2^{\lambda_n} < 2^\lambda$, and we have

- (*) if \mathbf{A} is a structure with exactly λ elements, $\mathbf{A} = \bigcup_{n < \omega} P_n^{\mathbf{A}}$ and $|P_n^{\mathbf{A}}| < \lambda$ for $n < \omega$, and G is its group of automorphisms, then G cannot be a free group of cardinality greater than μ .

The proof is similar, but now without loss of generality the set of elements of \mathbf{A} is $\lambda = \{\alpha : \alpha < \lambda\}$, and we define \mathfrak{d} by

$$\begin{aligned} \mathfrak{d}(f, g) = \sup \{ 2^{-n} : & \text{there is } \alpha < \lambda_n \text{ such that} \\ & \text{for some } (f', g') \in \{(f, g), (f^{-1}, g^{-1}), (g, f), (g^{-1}, f^{-1})\} \\ & \text{one of the following possibilities holds:} \\ & \text{(a) for some } m < \omega \text{ we have } f'(m) < \lambda_m \leq g'(m); \\ & \text{(b) } f'(n) < g'(n) < \lambda_n \}. \end{aligned}$$

Under this metric, G is a complete metric space with density less than or equal to $\sum_{n < \omega} 2^{\lambda_n} = \mu$, and the conclusion of Proposition 3 holds.

(3) By [2], for $\kappa = \kappa^{<\kappa} > \aleph_0$, there is a forcing, adding such a group and not changing the cardinalities or cofinalities. A parallel result in Zermelo–Fraenkel set theory together with the axiom of choice (ZFC) is in preparation.

References

1. H. BECKER and A. S. KECHRIS, *The descriptive set theory of Polish group actions*, London Math. Soc. Lecture Notes Ser. 232 (Cambridge University Press, Cambridge, 1996).
2. W. JUST, S. SHELAH and S. THOMAS, 'The automorphism tower problem revisited', *Adv. in Math.* 148 (1999) 243–265; <http://front.math.ucdavis.edu/math.LO/0003120>.
3. S. SHELAH, 'Polish algebras shy from freedom', *Israel J. Math.*, submitted.
4. S. SOLECKI, 'Polish group topologies', *Sets and proofs (Leeds, 1997)*, London Math. Soc. Lecture Note Ser. 258 (Cambridge University Press, Cambridge, 1999) 339–364.

Saharon Shelah
Institute of Mathematics
The Hebrew University
of Jerusalem
Jerusalem 91904
Israel

shelah@math.huji.ac.il

Institute Mittag-Leffler
The Royal Swedish Academy
of Sciences
Auravagen 17, S182 62
Djursholm
Sweden

Department of Mathematics
Rutgers University
New Brunswick, NJ 08854
USA