

# Set-theoretic Definability of Constructions

Progress Report on a  
Disgracefully Old Problem

Wilfrid Hodges  
Queen Mary, University of London  
September 2007

3

1974 Problem: Show there is no formula of set theory which—provably from ZFC—defines for each field  $A$  an algebraic closure  $B$  of that field.

(NB  $B$  is definable up to automorphism over  $A$ . We will consider only constructions with this property.)

1976 No such formula is  $\Sigma_1$ .

1980 Main conjecture: The reason why there is no such formula is that  $\text{Aut}(B)$  is a nonsplit extension of  $\text{Aut}(A)$ .

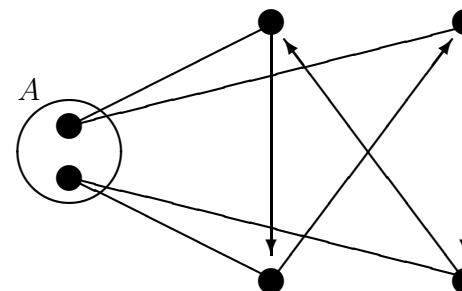
4

1986 Main conjecture proved for set theory with urelements.

2001 (Shelah) An approximate form of the main conjecture holds. (Hodges, *Logic, Methodology and Phil. Science* Oviedo 2003, ed. Hájek et al. 2005.) It solves the 1974 problem.

1

But it fails to show the following case of the main conjecture.



2

The solution of the 1974 problem has three parts:

- (a) We construct a model of ZFC with a structure  $A$  such that for every definable extension of  $A$ ,  $\text{Aut}(B)$  is (almost) a split extension of  $\text{Aut}(A)$ .
- (b) We iterate the construction of (a) a proper class of times.
- (c) We show that  $A$  can be chosen to be a field such that if  $B$  is its algebraic closure then  $\text{Aut}(B)$  is not (almost) a split extension of  $\text{Aut}(A)$ .

This talk concentrates on (a).

(b) is routine but messy. (c) is in the Oviedo paper.

7

$M$  a transitive model of ZFC + GCH containing the structure  $A$  with elements  $0, 1, 2, \dots$ . Choose a cardinal  $\lambda > |A|$ .

Force to extend  $M$  to  $N$  by adding  $\lambda^+$  sets  $a'_i$ , each consisting of  $\lambda^+$  generic subsets of  $\lambda^+$ .

I.e. construct generic  $G : \lambda^+ \times \lambda^+ \times \lambda^+ \rightarrow 2$ , and put  $a'_i = \{\{k : G(i, j, k) = 1\} : j < \lambda^+\}$ .

Put  $a_i$  the set of sets of subsets of  $\lambda^+$  differing from  $a'_i$  in at most  $\lambda$  sets.

8

Construct a copy  $A^*$  of  $A$  in  $N$  whose elements are  $a_0, a_1, a_2, \dots$

By assumption  $A^*$  has a definable extension  $B^*$ . We aim to show  $\text{Aut}(B^*)$  is (almost) a split extension of  $\text{Aut}(A^*)$ .

By a *neat map* we mean an eventually constant function  $\alpha : \lambda^+ \rightarrow \text{Aut}(A)$  in  $M$ .

Put  $\pi(\alpha) = \text{eventual value of } \alpha$ .

Then  $\alpha$  acts on the notion of forcing  $\mathbb{P}$  by

$$\alpha(i, j, k) = (\alpha(j)(i), j, k).$$

5

LEMMA. If  $\alpha$  is neat, then the action of  $\alpha$  on the boolean universe  $M^{\mathbb{P}}$  permutes the set of names of elements of  $A^*$  by

$$\alpha(\dot{a}_i) = \dot{a}_{\pi(\alpha)(i)}.$$

Thus since  $\alpha$  is in  $M$ , it induces in  $N$  the automorphism of  $A^*$  corresponding to  $\pi(\alpha)$ .

6

We want to see what  $\alpha$  does to  $B^*$  in  $N$ .

By assumption  $A^*$  has a defined extension  $B^*$ , and in  $N$  there is an isomorphism  $\varepsilon : B \rightarrow B^*$  extending the isomorphism  $i \mapsto a_i$ .

Choose a boolean name  $\dot{\varepsilon}$  of this isomorphism.

11

$$\begin{array}{ccc} B & \xrightarrow{\varepsilon} & B^* \\ \uparrow \subseteq & & \uparrow \subseteq \\ A & \longrightarrow & A^* \end{array}$$

LEMMA. For every neat map  $\alpha$  and generic  $G$ ,

$$(\dot{\varepsilon}^{-1} \circ \alpha \dot{\varepsilon})[G]$$

is an automorphism of  $B$  which extends  $\pi(\alpha)$ .

12

Consider a condition  $p$  and a set  $\mathbf{N}$  of neat maps.

Define

$$\begin{aligned} t(p, \mathbf{N}) = \{ (f, g) : & \exists \alpha \in \mathbf{N}, \\ & \pi(\alpha) = f, \\ & p \Vdash \dot{\varepsilon}^{-1} \circ \alpha \dot{\varepsilon} = \check{g} \} \end{aligned}$$

Then  $t(p, \mathbf{N})$  is an approximation to a lifting  $\text{Aut}(A) \rightarrow \text{Aut}(B)$ .

Shelah's idea: Choose large independent family of  $(p_i, \mathbf{N}_i)$ .

9

$\Delta$ -system lemma gives a family  $\{(p_i, \mathbf{N}_i) : i < \lambda^+\}$  s.t.

- $t(p_i, \mathbf{N}_i)$  is constant, say  $t$ .
- $q \leq p_i \Rightarrow t(q, \mathbf{N}_i) = t$ .
- There are  $\mu_0 < \mu_1 < \dots$  so that for each  $i$ ,
  - support of  $p_i$  is in  $[0, \mu_0) \cup [\mu_i, \mu_{i+1})$ ,
  - $p_i \upharpoonright \mu_0$  is independent of  $i$ ,
  - each  $\alpha \in \mathbf{N}_i$  is 1 below  $\mu_i$  and constant on  $[\mu_{i+1}, \lambda^+)$ .

10

We can read off properties of  $t$ .

FACT 1. The left domain of  $t$  is  $\text{Aut}(A)$ .

15

FACT 2. If  $(f_1, g_1)$  and  $(f_2, g_2)$  are in  $t$  then so is  $(f_1 f_2, g_1 g_2)$ .

SKETCH PROOF. Choose  $\alpha_0 \in \mathbf{N}_1$  and  $\alpha_1 \in \mathbf{N}_0$  such that for  $i = 0, 1$

$$p_{1-i} \Vdash \dot{\varepsilon}^{-1} \circ \alpha_i \dot{\varepsilon} = \check{g}_i.$$

Then

$$p_1 \Vdash \dot{\varepsilon}^{-1} \circ (\alpha_0 \alpha_1)(\dot{\varepsilon}) = \dot{\varepsilon}^{-1} \circ \alpha_0(\dot{\varepsilon}) \circ (\alpha_0(\dot{\varepsilon}))^{-1} \circ (\alpha_0 \alpha_1)(\dot{\varepsilon}),$$

and

$$p_1 \Vdash \dot{\varepsilon}^{-1} \circ \alpha_0(\dot{\varepsilon}) = \check{g}_0.$$

16

But also

$$p_0 \Vdash \dot{\varepsilon}^{-1} \circ \alpha_1(\dot{\varepsilon}) = \check{g}_1,$$

so

$$\alpha_0 p_0 \Vdash \alpha_0 \dot{\varepsilon}^{-1} \circ \alpha_0 \alpha_1(\dot{\varepsilon}) = \alpha_0 \check{g}_1.$$

By the independence conditions,

$$p_0 \Vdash \alpha_0 \dot{\varepsilon}^{-1} \circ \alpha_0 \alpha_1(\dot{\varepsilon}) = \check{g}_1.$$

Also  $p_0, p_1$  are compatible, and we have shown

$$p_0 \cup p_1 \Vdash \dot{\varepsilon}^{-1} \circ (\alpha_0 \alpha_1)(\dot{\varepsilon}) = \check{g}_0 \check{g}_1.$$

Now use maximality of  $t$ . □

13

FACT 3. If  $(1, g_0) \in t$  then  $g_0$  is central in  $\text{Aut}(B)$ .

SKETCH PROOF. For any  $g_1$ , choose  $\alpha_0 \in \mathbf{N}_0$  and  $\alpha_1 \in \mathbf{N}_1$  such that for  $i = 0, 1$

$$p_i \Vdash \dot{\varepsilon}^{-1} \circ \alpha_i \dot{\varepsilon} = \check{g}_i.$$

Then  $\alpha_0 \alpha_1 = \alpha_1 \alpha_0$ , and so

$$\begin{aligned} p_0 \Vdash \dot{\varepsilon}^{-1} \circ (\alpha_0 \alpha_1)(\dot{\varepsilon}) &= \dot{\varepsilon}^{-1} \circ \alpha_0(\dot{\varepsilon}) \circ (\alpha_0(\dot{\varepsilon}))^{-1} \circ (\alpha_0 \alpha_1)(\dot{\varepsilon}) \\ &= \dot{\varepsilon}^{-1} \circ \alpha_1(\dot{\varepsilon}) \circ (\alpha_1(\dot{\varepsilon}))^{-1} \circ (\alpha_1 \alpha_0)(\dot{\varepsilon}). \end{aligned}$$

14

Now  $p_0 \Vdash \dot{\varepsilon}^{-1} \circ \alpha_0(\dot{\varepsilon}) = \check{g}_0$ , so as before

$$p_0 \Vdash \alpha_1 \dot{\varepsilon}^{-1} \circ \alpha_1 \alpha_0(\dot{\varepsilon}) = \check{g}_0.$$

Likewise  $p_1 \Vdash \dot{\varepsilon}^{-1} \circ \alpha_1(\dot{\varepsilon}) = \check{g}_1$ ,

but  $\alpha_0$  is 1 from  $\mu_1$  upwards, so

$$p_1 \Vdash \alpha_0 \dot{\varepsilon}^{-1} \circ \alpha_0 \alpha_1(\dot{\varepsilon}) = \check{g}_1.$$

Then

$$p_0 \cup p_1 \Vdash \check{g}_0 \check{g}_1 = \check{g}_1 \check{g}_0,$$

so  $g_0 g_1 = g_1 g_0$  in the ground model.  $\square$

19

FACT 4. If  $(f, g_1), (f, g_2) \in t$  then  $g_1 g_2^{-1}$  is central in  $\text{Aut}(B)$ .

PROOF. Take  $h$  so that  $(f^{-1}, h) \in t$ . Then  $g_1 h$  and  $g_2 h$  are central by Facts 2, 3. So

$$g_1 g_2^{-1} = g_1 h (g_2 h)^{-1}$$

is central.  $\square$

So  $t$  induces a homomorphism

$$t^* : \text{Aut}(A) \rightarrow \text{Aut}(B)/Z(\text{Aut}(B)).$$

20

EXAMPLE.  $G$  the multiplicative group of  $3 \times 3$  upper unitriangular matrices over the ring  $\mathbb{Z}/(8\mathbb{Z})$ .

$F$  the corresponding group over  $\mathbb{Z}/(2\mathbb{Z})$ .

Let  $f_1, f_2$  be the two matrices

$$f_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad f_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

in  $F$ , and  $g_1, g_2$  liftings to  $G$ . Then  $f_1^2 = 1$ , but  $g_1^2$  is not central (since all entries of  $g_1 - f_1$  in  $G$  are divisible by 2).

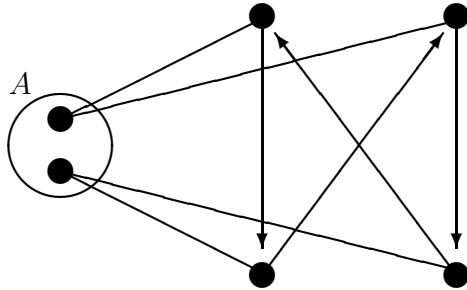
17

Hence there is no set-theoretically definable extension construction  $A \mapsto B$  where  $\text{Aut}(A) = F$  and  $\text{Aut}(B) = G$  as above.

Choose algebraic number fields  $k_1 \subseteq k_2$  with these automorphism groups over  $\mathbb{Q}$ , a Galois extension. Then there is no definable construction taking fields isomorphic to  $k_1$  to their algebraic closures.

18

This doesn't help with the construction



since both automorphism groups are abelian.

WORK IN PROGRESS

Shelah's idea hardly uses the assumption that the construction is defined on an isomorphism class.

We need to increase the contrast between the definability of  $\varepsilon$  and the intangibility of the generic elements.

For this we replace  $N$  by the class of sets relatively constructible from  $G$ .

Consider the construction on pairs.

The structure  $A^*$  has elements  $a_0, a_1$ .

$$\text{Aut}(A) = \{1, f\}, \text{Aut}(B) = \{1, g, g^2, g^3\}.$$

$\varepsilon$  becomes  $\dot{F}(\check{k}, \dot{a}_0, \dot{a}_1)$  for some ordinal  $k$ , with  $F$  a term defined by a  $\Sigma_1$  formula.

Then for each neat map  $\alpha$ ,

$$\dot{F}(\check{k}, \dot{a}_0, \dot{a}_1)^{-1} \circ \alpha \dot{F}(\check{k}, \dot{a}_0, \dot{a}_1)$$

is with boolean value 1 equal to one of two automorphisms of  $B$ .

If  $\pi(\alpha) = 1$  then the value must be  $\check{1}$ .

If  $\pi(\alpha) = f$  then the value must be one of  $\check{g}, \check{g}^3$ .

So  $t$  is single-valued.

IF this works, then I think Shelah's construction will still be needed, essentially to show  $\{a_0, a_1\}$  is an indiscernible set over  $A^*$ .

And IF it works, it extends at least to cases where  $\text{Aut}(A)$  is finite.

But past experience suggests the details won't be straightforward.