Definability versus definability-up-to-isomorphism, in groups and fields

Wilfrid Hodges
Herons Brook, Sticklepath,
Okehampton EX20 2PY
http://wilfridhodges.co.uk

Antalya, May 2010

Many constructions F in algebra and analysis take the form:

> *For every structure A in a class $\mathbb{K}$ closed under isomorphism,*
> *the structure $F(A)$ extends A and is determined up to isomorphism over A,*
> *i.e. if $A, C \in \mathbb{K}$ with an isomorphism $f : A \to C$,*
> *then there is an isomorphism $g : F(A) \to F(C)$ extending f.*

Typical examples:
A a field and $F(A)$ the algebraic closure of A;
A a left R-module and $F(A)$ the injective hull of A.

Also A a poset and $F(A)$ its MacNeille completion.

Given $X \subseteq A$, put

$$\bar{X} = \{a \in A : (\forall b \in A)\ ((\forall c \in X)\ (c \leqslant b) \to (a \leqslant b))\}$$

Then $F(A) = \{X \subseteq A : \bar{X} = X\}$, $a \mapsto \overline{\{a\}}$.

From this explicit definition it's clear that automorphisms of A extend to automorphisms of $F(A)$.

A non-example:
A a formally real field and $F(A)$ a real closure of A.

This is not a construction in our sense.
E.g. if $A = \mathbb{Q}(X, Y)$,
then in $F(A)$ we have exactly one of $X < Y$ and $Y < X$,
so no automorphism of $F(A)$ switches X and Y.

In a set-theoretic universe, since $\mathbb{K}$ is a proper class
F is a restricted global choice function,
choosing a value $F(A)$ for each $A \in \mathbb{K}$.

Michael Makkai, 'Avoiding the axiom of choice in general category theory', *J. Pure and Applied Category Theory*, proposes the notion of 'anafunctor' to avoid having to choose a value $F(A)$ for each A.

Paraphrasing a comment of Paul Taylor:
This is poorly motivated. Category theory should not be understood platonically, so the truth of the axiom of choice (global or local) is irrelevant.

We will ignore these foundational questions.

Often F can be defined outright within ZF set theory.

Trivial example: $\mathbb{K}$ the class of structures $\cong \mathbb{Z}(2)$,
$F(A) \cong \mathbb{Z}(4)$ with $A = 2F(A)$.

Take C the cyclic group with elements $0, 1, 2, 3$.
Given any $A \in \mathbb{K}$, there is a unique group embedding $h : A \to C$.
In set theory we can define $F(A)$: replace $0, 2$ in C by their pre-images under h, and (if necessary) replace $1, 3$ by $\langle A, 1\rangle, \langle A, 3\rangle$.

By contrast no definition of F is known when $A \cong \mathbb{Z}(8)$,
$F(A) \cong \mathbb{Z}(16)$ with $A = 2F(A)$.

Historical reminiscence: This phenomenon first came to light in model theory in the 1970s.
In 1980 I spoke about it at Bowling Green Ohio, using an example with 625 elements.
Michael Morley in the audience said

> *'That's impossible. There aren't any finite structures in model theory'.*

(His neighbour Andreas Blass calmed him down.)

Until the mid 1970s model theory was about the compactness theorem, which is trivial for finite structures.
Definability theory is not always about compactness, so it can be nontrivial for finite structures.
This became very clear in the 1980s, thanks to work of Lachlan, Zilber etc.

We identify a crucial difference between the cases $\mathbb{Z}(2) \mapsto \mathbb{Z}(4)$ and $\mathbb{Z}(8) \mapsto \mathbb{Z}(16)$.

Write $\text{Aut}(A)$ for the group of all automorphisms of A, and $\text{Aut}(F(A))_{(A)}$ for the group of all automorphisms of $F(A)$ that fix A setwise.

Each automorphism $\alpha \in \text{Aut}(F(A))_{(A)}$ restricts to an automorphism $\nu(\alpha)$ of A, yielding a homomorphism

$$\nu : \text{Aut}(F(A))_{(A)} \to \text{Aut}(A).$$

By definition of constructions, ν is surjective.

We say ν *splits* if there is a 'splitting' homomorphism $\sigma : \text{Aut}(A) \to \text{Aut}(F(A))_{(A)}$ with $\nu\sigma = 1_{\text{Aut}(A)}$.

We say the construction F is *split* (or *natural*) if for every A in the domain of F, ν as above splits.

Fact. $F : \mathbb{Z}(2) \mapsto \mathbb{Z}(4)$ is split.

Note that in this case $\mathrm{Aut}(F(A))_{(A)} = \mathrm{Aut}(F(A))$, since A is a characteristic subgroup of $F(A)$.
(And similarly for $\mathbb{Z}(8) \mapsto \mathbb{Z}(16)$.)

Now $\mathrm{Aut}(\mathbb{Z}(2))$ is trivial, so the required splitting $\sigma : \mathrm{Aut}(\mathbb{Z}(2)) \to \mathrm{Aut}(\mathbb{Z}(4))$ is the identity. □

Fact. $F : \mathbb{Z}(8) \mapsto \mathbb{Z}(16)$ is not split.

Here $\mathrm{Aut}(\mathbb{Z}(8)) = \mathbb{Z}(2) \oplus \mathbb{Z}(2)$ and
$\mathrm{Aut}(\mathbb{Z}(16)) = \mathbb{Z}(4) \oplus \mathbb{Z}(2)$.
So we have a short exact sequence

$$0 \longrightarrow \mathbb{Z}(2) \longrightarrow \mathbb{Z}(4) \oplus \mathbb{Z}(2) \xrightarrow{\nu} \mathbb{Z}(2) \oplus \mathbb{Z}(2) \longrightarrow 0$$

If ν splits then $\mathbb{Z}(4) \oplus \mathbb{Z}(2) = \mathbb{Z}(2) \oplus \mathbb{Z}(2) \oplus \mathbb{Z}(2)$, which is false.

□

Theorem. Suppose that all structures in the domain $\mathbb{K}$ of F are isomorphic, F is split, and there exists a definable pair $(C, F(C))$ with a definable splitting
$\sigma : \mathrm{Aut}(C) \to \mathrm{Aut}(F(C))_{(C)}$.
Then F is definable.

Proof. Given $A \in \mathbb{K}$, let G be the set of all isomorphisms $g : A \to C$.
For each $g \in G$ let $F(C)_g$ be a distinct copy of $F(C)$.
Define

$$e : A \to \prod_{g \in G} F(C)_g, \quad e(a)_g = g(a).$$

Then e is a definable embedding.

We will define a substructure of $\prod_{g \in G} F(C)_g$ isomorphic to $F(C)$.
We say $x \in \prod_{g \in G} F(C)_g$ is *symmetric* if for all $f, g \in G$,

$$x_g = \sigma(gf^{-1})x_f.$$

This makes sense since $gf^{-1} \in \mathrm{Aut}(A)$.
We define $F(A)$ to be the set of symmetric elements in $\prod_{g \in G} F(C)_g$
(or strictly this set with elements in image of e replaced by their pre-images etc. etc.).

Various things to check:

(1) $F(A)$ is a substructure of $\prod_{g\in G} F(C)_g$.

E.g. if A is an abelian group and x, y are symmetric elements, we want $x + y$ symmetric, thus:

$$\begin{aligned}(x+y)_g = x_g + y_g &= \sigma(gf^{-1})x_f + \sigma(gf^{-1})y_f \\ &= \sigma(gf^{-1})(x_f + y_f)\end{aligned}$$

because values of σ are in $\mathrm{Aut}(F(C))_{(C)}$

$$= \sigma(gf^{-1})(x+y)_f.$$

(2) $e(A) \subseteq F(A)$.

Suppose $a \in A$. We must show $e(a)$ is symmetric, i.e. $g(a) = \sigma(gf^{-1})f(a)$ for all $f, g \in G$.
Since $f(a) \in C$ (or strictly in the image of C in $F(C)_f$),

$$\sigma(gf^{-1})f(a) = (\nu\sigma)(gf^{-1})f(a)$$

and this by the splitting

$$= 1_A(gf^{-1})f(a) = gf^{-1}f(a) = ga.$$

(3) For each $g \in G$, the map $x \mapsto x_g$ is an isomorphism from $F(A)$ to $F(C)$ extending $g : A \to C$.

The map is clearly a homomorphism. We must show it is a surjective embedding.

Surjective: for each $d \in F(C)$ and each f define
$x_f = \sigma(fg^{-1})d$.
Then x is symmetric since σ is a *group homomorphism*, and $x_g = d$ since $\sigma(1_C) = 1_{F(C)}$.

Embedding: suppose x, y are symmetric and $x_g = y_g$.
Then for all f,

$$x_f = \sigma(fg^{-1})x_g = \sigma(fg^{-1})y_g = y_f$$

(and similarly with relations). □

By contrast no non-split construction is known to be definable. So a natural conjecture is:

> *A construction is definable if and only if it is split.*

But caution: in the constructible universe there is a global choice function so *all* constructions are definable.
So the conjecture has to say something like:

> *(Main conjecture) If a construction F is definable-up-to-isomorphism in ZFC, and is non-split (provably in ZFC),*
> *then there is a model of ZFC in which F is not definable.*

(What about parameters? For simplicity we ignore them here.)

The conjecture is true for ZFC with urelements. (Hodges and Shelah, 'Naturality and definability 1', *Journal of London Mathematical Society* 33 (1986) 1–12.)

For ZFC it is still open, though Shelah has shown (in preparation) that there is no model of ZFC in which the definable constructions are exactly the split ones.

Let $\nu : G \to F$ be any surjective group homomorphism. By a *weak splitting* of ν we mean a map $\sigma : F \to G$ such that

- $\nu\sigma = 1_F$ and
- the composed map

$$F \xrightarrow{\sigma} G \xrightarrow{\text{nat}} G/\mathcal{Z}(G)$$

(where $\mathcal{Z}(G)$ is the centre of G) is a homomorphism.

We say that ν *weakly splits* if it has a weak splitting σ.

Fact. If σ is a weak splitting of ν and $\alpha^n = 1$ in F then $\sigma(\alpha)^n$ is central in G.

Thus writing z, z' for elements of the centre of G,

$$\sigma(1) = \sigma(1^2) = \sigma(1)^2.z.$$

Hence $1 = \sigma(1).z$ and so $\sigma(1)$ *is central*.

If $\alpha^n = 1$ in F then

$$z = \sigma(1) = \sigma(\alpha^n) = \sigma(\alpha)^n.z'$$

for some central z, z', and so $\sigma(\alpha)^n$ is central. □

We say that a construction F is *weakly split* if for every A in the domain of F,
$\nu : \text{Aut}(F(A))_{(A)} \to \text{Aut}(A)$ weakly splits.

Theorem. There is a model of ZFC in which every definable construction is weakly split.
(Hodges and Shelah, in preparation.)

So if (provably in ZFC) a construction F is not weakly split, then there is no formula which (provably in ZFC) defines F.

Let G be the multiplicative group of 3×3 upper unitriangular matrices over the ring $\mathbb{Z}/(8\mathbb{Z})$,
F the corresponding group over $\mathbb{Z}/(2\mathbb{Z})$.
We show the natural $\nu : G \to F$ has no weak splitting.

Let g_1, g_2 be the two matrices

$$g_1 = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad g_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix}$$

in G, and f_1 the homomorphic image of g_1 in F.
Then $f_1^2 = 1$.

For contradiction suppose σ is a weak splitting of ν.
Consider $h_1 = \sigma(f_1) \in G$.
By above, h_1^2 is central in G, so h_1^2 and g_2 commute.

But by construction $h_1 = g_1 + 2M$ for some matrix $M \in \mathbb{Z}(8)^{3\times 3}$, so $h_1^2 = g_1^2 + 4N$ for some matrix N.

So

$$h_1^2 g_2 = g_1^2 g_2 + 4N g_2 \in g_1^2 g_2 + 4\mathbb{Z}(8)^{3\times 3}$$

and similarly

$$g_2 h_1^2 \in g_2 g_1^2 + 4\mathbb{Z}(8)^{3\times 3}.$$

So if h_1^2 and g_2 commute then

$$g_1^2 g_2 - g_2 g_1^2 \in 4\mathbb{Z}(8)^{3\times 3}.$$

But

$$g_1^2 g_2 - g_2 g_1^2 = \begin{pmatrix} 0 & 0 & 2 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \notin 4\mathbb{Z}(8)^{3\times 3}.$$

Contradiction. $\square$

Hence there is no provably definable construction $A \mapsto B$ where $\mathrm{Aut}(A) = F$ and $\mathrm{Aut}(B) = G$ as above.

Choose algebraic number fields $k_1 \subseteq k_2$ with these automorphism groups over $\mathbb{Q}$, a Galois extension. (Possible by Shafarevich, since G is a soluble group.) Then the construction $k_1 \mapsto k_2$ is not provably definable.

Hence algebraic closure for fields is not provably definable.

A similar argument shows that divisible hull of abelian groups is not provably definable.

But we still don't know about the construction

$$\mathbb{Z}(8) \mapsto \mathbb{Z}(16).$$

Here ν weakly splits for the trivial reason that both automorphism groups are abelian.

In particular the definability of the construction $\mathbb{F}_{p^8} \mapsto \mathbb{F}_{p^{16}}$ (p a prime) is open.

I still conjecture that there is a model of ZFC in which every definable construction is split.

The proof of the result with weak splittings uses a very indirect combinatorial argument due to Shelah.
It works but I can't offer any explanation why it's the right approach to take.