AUTOMORPHISMS OF MODELS OF ARITHMETIC

ALI ENAYAT

Sixth Panhellenic Conference

Volos, Greece

July 8, 2007

Prehistory

- $(\mathbb{N}, <)$ is rigid. Indeed any well-founded extensional relational structure is rigid.

- **Question** (Hasenjäger): *Is there a model of PA with a nontrivial automorphism*?

- **Equivalent Question**: *Is there a model of $ZF \setminus \{\text{Infinity}\} \cup \{\neg\text{Inf}\}$ with a nontrivial automorphism*?

The Answer

- **Theorem** (Ehrenfeucht and Mostowski). *Given an infinite model $\mathfrak{M}$ and a linear order $\mathbb{L}$, there is an elementary extension $\mathfrak{M}^*_{\mathbb{L}}$ of $\mathfrak{M}$ such that*

$$Aut(\mathbb{L}) \hookrightarrow Aut(\mathfrak{M}^*_{\mathbb{L}}).$$

The Standard Proof of EM

*abrakadabra (*Ramsey's Theorem)

ajji majji latarrajji (Compactness Theorem)

EM with one ABRAKADABRA

- $\mathfrak{M} = (M, \cdots)$ is a infinite structure, and $\mathbb{L}$ is a linear order.

- Fix a nonprincipal ultrafilter $\mathcal{U}$ over $\mathcal{P}(\mathbb{N})$.

- One can build the $\mathbb{L}$-iterated ultrapower of $\mathfrak{M}$ modulo $\mathcal{U}$, denoted $\mathfrak{M}^*_{\mathcal{U},\mathbb{L}}$, with 'bare hands'.

- **Theorem.** *There is a group embedding $j \mapsto \hat{\jmath}$ of $Aut(\mathbb{L})$ into $Aut(\mathfrak{M}^*_{\mathcal{U},\mathbb{L}})$ such that for every fixed point free j,*

$$fix(\hat{\jmath}) = M.$$

Skolem Ultrapowers (1)

- Suppose $\mathfrak{M}$ has definable Skolem functions (e.g., $\mathfrak{M}$ is a *RCF*, or a model of *PA*, or a model of *ZF* + *V*=*OD*).

- The *Skolem ultrapower* $\mathfrak{M}^*_{\mathcal{U}}$ can be constructed as follows:

  (a) Let $\mathcal{B}$ be the Boolean algebra of $\mathfrak{M}$-definable subsets of M, and $\mathcal{U}$ be an ultrafilter over $\mathcal{B}$.

  (b) Let $\mathcal{F}$ be the family of functions from M into M that are parametrically definable in $\mathfrak{M}$.

Skolem Ultrapowers (2)

- (c) The universe of $\mathfrak{M}^*_{\mathcal{U}}$ is

$$\{[f] : f \in \mathcal{F}\},$$

where

$$f \sim g \Longleftrightarrow \{m \in M : f(m) = g(m)\} \in \mathcal{U}$$

(d) Define functions, relations, and constants on $\mathfrak{M}^*_{\mathcal{U}}$ as in the usual theory of ultraproducts.

- The analogue of the Łoś theorem is true in this context as well, therefore

$$\mathfrak{M} \prec \mathfrak{M}^*_{\mathcal{U}}.$$

Skolem Ultrapowers (3)

- **Theorem** (MacDowell-Specker, 1961)

  Every model of PA has an elementary end extension.

- **Idea of the Proof :** Construct $\mathcal{U}$ with the property that every definable map with bounded range is constant on a member of $\mathcal{U}$. Then,

$$\mathfrak{M} \prec_e \mathfrak{M}^*_{\mathcal{U}}.$$

- The construction of $\mathcal{U}$ above is a more refined version of the proof of the existence of 'p-points' in $\beta\omega$ using CH.

Skolem-Gaifman Ultrapowers (1)

- For each parametrically definable $X \subseteq M$, and $m \in M$, $(X)_m = \{x \in M : \langle m, x\rangle \in X\}$.

- $\mathcal{U}$ is an *iterable* ultrafilter if for every $X \in \mathcal{B}$, $\{m \in M : (X)_m \in \mathcal{U}\} \in \mathcal{B}$.

- **Theorem** (Gaifman, 1976)

  (1) *Every countable model of PA carries an iterable $\mathcal{U}$.*

  (2) *If $\mathcal{U}$ is iterable, then the $\mathbb{L}$-iterated ultrapower of $\mathfrak{M}$ modulo $\mathcal{U}$ can be meaningfully defined.*

Skolem-Gaifman Ultrapowers (2)

- Let $\mathfrak{M}^*_{\mathcal{U},\mathbb{L}}$ be the $\mathbb{L}$-iterated ultrapower of $\mathfrak{M}$ modulo $\mathcal{U}$.

- **Theorem** (Gaifman, 1976)

  (1) *If $\mathcal{U}$ is iterable, and $\mathbb{L}$ is a linear order, then*

  $$\mathfrak{M} \prec_e \mathfrak{M}^*_{\mathcal{U},\mathbb{L}}.$$

  (2) *Moreover, if $\mathcal{U}$ is a 'Ramsey ultrafilter' over $\mathfrak{M}$, then there is an isomorphism*

  $$j \longmapsto \widehat{\jmath}$$

  between Aut($\mathbb{L}$) and Aut($\mathfrak{M}^*_{\mathbb{L}}; M$) such that

  $$\textit{fix}(\widehat{\jmath}) = M$$

  for every fixed-point-free j.

Two Corollaries of Gaifman's Theorem

- **Corollary 1.** *There are rigid models of* PA *of arbitrarily large cardinalty.*

- **Corollary 2.** *For every* $\mathbb{L}$*, there is some model* $\mathfrak{M}$ *of* PA *such that* $Aut(\mathfrak{M}) \cong Aut(\mathbb{L})$.

Schmerl's Generalization

- **Theorem** (Schmerl, 2002) *The following are equivalent for a group G.*

  (a) $G \leq Aut(\mathbb{L})$ *for some linear order* $\mathbb{L}$.

  (b) G *is left-orderable.*

  (c) $G \cong Aut(\mathfrak{A})$ *for some linearly ordered structure* $\mathfrak{A} = (A, <, \cdots)$.

  (d) $G \cong Aut(\mathfrak{M})$ *for some* $\mathfrak{M} \models PA$.

  (e) $G \cong Aut(\mathbb{F})$ *for some ordered field* $\mathbb{F}$.

- Schmerl's methodology: using a partition theorem of Nešteřil-Rödl/Abramson-Harrington to refine Gaifman's technique.

Countable Recursively Saturated Models (1)

- **Theorem** (Schlipf, 1978). *Every countable recursively saturated model has continuum many automorphisms.*

- **Theorem** (Schmerl, 1985)

  (1) *If a countable recursively saturated model $\mathfrak{M}$ is equipped with a 'β-function" β, then for any countable linear order $\mathbb{L}$ without a last element, $\mathfrak{M}$ is generated by a set of indiscernibles of order-type $\mathbb{L}$ (via β).*

  (2) *Consequently, there is a group embedding from $Aut(\mathbb{Q})$ into $Aut(\mathfrak{M})$.*

Countable Recursively Saturated Models (2)

- **Theorem**. (Smoryński, 1982) *If $\mathfrak{M}$ is a countable recursively saturated model of PA and I is a cut of $\mathfrak{M}$ that is closed under exponentiation, then there are continuum many $j \in Aut(\mathfrak{M})$ such that I is the longest initial segment of $\mathfrak{M}$ that is pointwise fixed by j*

- **Question.** Can Smoryński's theorem be combined with part (2) of Schmerl's theorem above?

Paris-Mills Ultrapowers

- The *index set* is of the form

$$\overline{c} = \{0, 1, \cdots, c-1\}$$

for some nonstandard c in $\mathfrak{M}$.

- The family of functions used, denoted $\mathcal{F}$, is $({}^{\overline{c}}M)^{\mathfrak{M}}$.

- The Boolean algebra at work will be denoted $\mathcal{P}^{\mathfrak{M}}(\overline{c})$.

- This type of ultrapower was first considered by Paris and Mills (1978) to show that one can arrange a model of PA in which there is an externally countable nonstandard integer H such that the external cardinality of $Superexp(2, H)$ is of any prescribed infinite cardinality.

More on Ultrafilters

- $\mathcal{U}$ is *I-complete* if for every $f \in \mathcal{F}$, and every $i \in I$, if $f : \overline{c} \to \overline{i}$, then f is constant on a member of $\mathcal{U}$.

- $\mathcal{U}$ is *I-tight* if for every $f \in \mathcal{F}$, and every $n \in \mathbb{N}^+$, if $f : [\overline{c}]^n \to M$, then there is some $H \in \mathcal{U}$ such either f is constant on H, or there is some $m_0 \in M \backslash I$ such that $f(\mathbf{x}) > m_0$ for all $\mathbf{x} \in [H]^n$.

- $\mathcal{U}$ is *I-conservative* if for every $n \in \mathbb{N}^+$ and every $\mathfrak{M}$-coded sequence $\langle K_i : i < c \rangle$ of subsets of $[\overline{c}]^n$ there is some $X \in \mathcal{U}$ and some $d \in M$ with $I < d \leq c$ such that $\forall i < d$ X *decides* K_i, i.e., either $[X]^n \subseteq K_i$ or $[X]^n \subseteq [\overline{c}]^n \backslash K_i$.

Desirable Ultrafilters

- **Theorem.** *$\mathcal{P}^{\mathfrak{M}}(\overline{c})$ carries a nonprincipal ultrafilter $\mathcal{U}$ satisfying the following four properties :*

(a) *$\mathcal{U}$ is I-complete;*

(b) *$\mathcal{U}$ is I-tight;*

(c) $\{Card^{\mathfrak{M}}(X) : X \in \mathcal{U}\}$ is *downward cofinal in* $M \backslash I$;

(d) *$\mathcal{U}$ is I-conservative.*

Fundamental Theorem

- **Theorem.** *Suppose I is a cut closed exponentiation in a countable model of PA, $\mathbb{L}$ is a linearly ordered set, and $\mathcal{U}$ satisfies the four properties of the previous theorem. One can use $\mathcal{U}$ to build an elementary $\mathfrak{M}^*_{\mathbb{L}}$ of $\mathfrak{M}$ that satisfies the following:*

(a) $I \subseteq_e \mathfrak{M}^*_{\mathbb{L}}$ *and* $SSy(\mathfrak{M}^*_{\mathbb{L}}, I) = SSy(\mathfrak{M}, I)$.

(b) $\mathbb{L}$ *is a set of indiscernibles in* $\mathfrak{M}^*_{\mathbb{L}}$;

(c) *Every* $j \in Aut(\mathbb{L})$ *induces an automorphism* $\widehat{j} \in Aut(\mathfrak{M}^*_{\mathbb{L}})$ *such that* $j \mapsto \widehat{j}$ *is a group embedding of* $Aut(\mathbb{L})$ *into* $Aut(\mathfrak{M}^*_{\mathbb{L}})$;

(d) *If* $j \in Aut(\mathbb{L})$ *is nontrivial, then* $I_{fix}(\widehat{j}) = I$.

Combining Smoryński and Schmerl

- **Theorem.** *Suppose $\mathfrak{M}$ is a countable recursively saturated model of PA and I is a cut of $\mathfrak{M}$ that is closed under exponentiation. There is a group embedding $j \longmapsto \hat{\jmath}$ from $Aut(\mathbb{Q})$ into $Aut(\mathfrak{M})$ such that for every nontrivial $j \in Aut(\mathbb{Q})$ the longest initial segment of $\mathfrak{M}$ that is pointwise fixed by $\hat{\jmath}$ is I.*

- **Proof:** Use part (c) of the previous theorem, plus the following isomorphism theorem.

- **Theorem.** *Suppose I is a cut closed under exponentiation in a countable recursively saturated model $\mathfrak{M}$ of PA, and $\mathfrak{M}^*$ is a cofinal countable elementary extension of $\mathfrak{M}$ such that $I \subseteq_e \mathfrak{M}^*$ with $SSy(\mathfrak{M}, I) = SSy(\mathfrak{M}^*, I)$. Then $\mathfrak{M}$ and $\mathfrak{M}^*$ are isomorphic over I.*

Key Results of Kaye, Kossak, Kotlarski, and Schmerl

- **Theorem** (K^3, 1991). *Suppose $\mathfrak{M}$ is a countable recursively saturated model of PA.*

(1) *If $\mathbb{N}$ is a strong cut of $\mathfrak{M}$, then there is some $j \in Aut(\mathfrak{M})$ such that every undefinable element of $\mathfrak{M}$ is moved by j.*

(2) *If $I \prec_{e,strong} \mathfrak{M}$, then I is the fixed point set of some $j \in Aut(\mathfrak{M})$.*

- **Theorem** (Kossak-Schmerl 1995, Kossak-1997). *In the above, j can be arranged to be expansive on the complement of the convex hull of its fixed point set.*

Strong Cuts and Arithmetic Saturation

- I is a *strong cut* of $\mathfrak{M}$ if, for each function f whose graph is coded in $\mathfrak{M}$ and whose domain includes I, there is some s in M such that for all $m \in M$, $f(m) \notin I$ iff $s < f(m)$.

- **Theorem** (Kirby-Paris, 1977) *The following are equivalent for a cut I of* $\mathfrak{M} \models PA$:

(a) I *is strong in* $\mathfrak{M}$.

(b) $(\mathbf{I}, SSy(\mathfrak{M}, I)) \models ACA_0$.

- **Proposition.** *A countable recursively saturated model of* PA *is arithmetically saturated iff* $\mathbb{N}$ *is a strong cut of* $\mathfrak{M}$.

Schmerl's Conjecture

- **Conjecture** (Schmerl). *If* $\mathbb{N}$ *is a strong cut of countable recursively saturated model* $\mathfrak{M}$ *of PA, then the isomorphism types of fixed point sets of automorphisms of* $\mathfrak{M}$ *coincide with the isomorphism types of elementary substructures of* $\mathfrak{M}$.

Kossak's Evidence

- **Theorem** (Kossak, 1997).

(1) *The number of isomorphism types of fixed point sets of* $\mathfrak{M}$ *is either* $2^{\aleph_0}$ *or* 1*, depending on whether* $\mathbb{N}$ *is a strong cut of* $\mathfrak{M}$*, or not.*

(2) *Every countable model of* PA *is isomorphic to a fixed point set of some automorphism of some countable arithmetically saturated model of* PA.

A New Ultrapower (1)

- Suppose $\mathfrak{M} \preceq \mathfrak{N}$, *where* $\mathfrak{M} \models PA^*$, I *is a cut of both* $\mathfrak{M}$ *and* $\mathfrak{N}$, *and* I *is strong in* $\mathfrak{N}$ *(N.B.,* I *need not be strong in* $\mathfrak{M}$*).*

- $\mathcal{F} := \left({}^{I}M\right)^{\mathfrak{N}}$.

- Both Skolem-Gaifman, and Kirby-Paris ultrapowers can be viewed as special cases of the above.

- **Proposition.** *There is an* $\mathcal{F}$*-Ramsey ultrafilter* $\mathcal{U}$ *on* $B(\mathcal{F})$ *if* M *is countable.*

- **Theorem.** *One can use* $\mathcal{F}$, *and an* $\mathcal{F}$*-Ramsey ultrafilter* $\mathcal{U}$ *to build* $\mathfrak{M}^*_{\mathbb{L}}$, *and a group embedding* $j \mapsto \hat{\jmath}$ *of* $Aut(\mathbb{L})$ *into* $Aut(\mathfrak{M}^*_{\mathbb{L}})$.

A New Ultrapower (2)

- **Theorem.**

(a) $\mathfrak{M} \prec \mathfrak{M}^*_{\mathbb{L}}$.

(b) *I is an initial segment of $\mathfrak{M}^*$, and $B(\mathcal{F}) = SSy(\mathfrak{M}^*_{\mathbb{L}}, I)$.*

(c) *For every $\mathcal{L}$-formula $\varphi(x_1, \cdots, x_n)$, and every $(l_1, \cdots, l_n) \in [\mathbb{L}]^n$, the following two conditions are equivalent:*

(i) $\mathfrak{M}^*_{\mathbb{L}} \models \varphi(l_1, l_2, \cdots, l_n)$;

(ii) $\exists H \in \mathcal{U}$ *such that for all* $(a_1, \cdots, a_n) \in [H]^n$, $\mathfrak{M} \models \varphi(a_1, \cdots, a_n)$.

(d) *If $j \in Aut(\mathbb{L})$ is fixed point free, then fix($\hat{\jmath}$) $= M$.*

(e) *If $j \in Aut(\mathbb{L})$ is expansive on $\mathbb{L}$, then $\hat{\jmath}$ is expansive on $M^* \backslash \overline{M}$.*

Proof of Schmerl's Conjecture (1)

- **Theorem.** *Suppose $\mathfrak{M}_0$ is an elementary submodel of a countable arithmetically saturated model $\mathfrak{M}$ of PA. There is $\mathfrak{M}_1 \prec \mathfrak{M}$ with $\mathfrak{M}_0 \cong \mathfrak{M}_1$ and an embedding $j \mapsto \hat{\jmath}$ of $Aut(\mathbb{Q})$ into $Aut(\mathfrak{M})$, such that fix$(\hat{\jmath}) = \mathfrak{M}_1$ for every fixed point free $j \in Aut(\mathbb{Q})$.*

Proof:

(1) Let $\mathcal{F} := ({}^{\mathbb{N}}M_0)^{\mathfrak{M}}$.

(2) Build an ultrafilter $\mathcal{U}$ on $B(\mathcal{F})$ that is $\mathcal{F}$-Ramsey.

(3) $\mathfrak{M}^* := \prod_{\mathcal{F},\mathcal{U},\mathbb{Q}} \mathfrak{M}_0$.

Proof of Schmerl's Conjecture (2)

(4) $\mathfrak{M}^*$ *is recursively saturated (*key idea: $\mathfrak{M}^*$ has a satisfaction class).

(5) Therefore $\mathfrak{M}^* \cong \mathfrak{M}$.

(6) Let θ be an isomorphism between $\mathfrak{M}^*$ and $\mathfrak{M}$ and let $\mathfrak{M}_1$ be the image of $\mathfrak{M}_0$ under θ.

(7) The embedding $j \overset{\lambda}{\longmapsto} \widehat{j}$ of $Aut(\mathbb{Q})$ into $Aut(\mathfrak{M}^*)$ has the property that *fix*$(\widehat{j}) = M_0$ for every fixed point free $j \in Aut(\mathbb{Q})$.

Proof of Schmerl's Conjecture (3)

(8) The desired embedding $j \overset{\alpha}{\longmapsto} \widetilde{j}$ by:

$$\alpha = \theta^{-1} \circ \lambda \circ \theta.$$

This is illustrated by the following commutative diagram:

$$\begin{array}{ccc} \mathfrak{M} & \xrightarrow{\widetilde{j}=\alpha(j)} & \mathfrak{M} \\ \downarrow\theta & & \uparrow\theta^{-1} \\ \mathfrak{M}^* & \xrightarrow{\widehat{j}=\lambda(j)} & \mathfrak{M}^* \end{array}$$

1. A. Enayat, *From bounded to second order arithmetic via automorphisms*, in **Logic in Tehran**, Lecture Notes in Logic, vol. 26, 2006, pp. 87-113.

2. ______, *Automorphisms of models of bounded arithmetic*, **Fundamenta Mathematicae**, vol. 192 (2006), pp. 37-65.

3. ______, *Automorphisms of models of arithmetic: a unified view*, **Annals of Pure and Applied Logic**, vol. 145, (2007), pp. 16-36.

4. R. Kaye, **Models of Peano Arithmetic**, Oxford University Press, 1991.

5. R. Kossak and J. Schmerl, **The Structure of Models of Peano Arithmetic**, Oxford University Press, 2006.