Reverse Mathematics and Field Extensions

Preliminary Report

François Dorais, Jeff Hirst[1], Paul Shafer
Appalachian State University
Boone, NC

These slides are available at: www.mathsci.appstate.edu/~jlh

April 1, 2012

ASL 2012 North American Annual Meeting

[1] Jeff Hirst's research is partially supported by the John Templeton Foundation. Any opinions expressed here are those of the authors and do not necessarily reflect the views of the John Templeton Foundation.

Reverse field theory

In the reverse math setting (second order arithmetic with limits on comprehension and induction) a field is a countable set with operations that satisfy the usual field axioms. One can encode copies of familiar fields like $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{2})$.

If every non-constant polynomial in K has a root in K, we say K is algebraically closed. An algebraic closure of F is an algebraically closed field $\overline{F}$ with an embedding $\varphi : F \to \overline{F}$.

Reverse field theory

In the reverse math setting (second order arithmetic with limits on comprehension and induction) a field is a countable set with operations that satisfy the usual field axioms. One can encode copies of familiar fields like $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{2})$.

If every non-constant polynomial in K has a root in K, we say K is algebraically closed. An algebraic closure of F is an algebraically closed field $\overline{F}$ with an embedding $\varphi : F \to \overline{F}$.

$\mathrm{RCA}_0 \vdash$ *every field has an algebraic closure.*

RCA_0: recursive comprehension axiom

$\mathrm{WKL}_0 \leftrightarrow$ *algebraic closures are unique.*

WKL_0: weak König's lemma

$\mathrm{ACA}_0 \leftrightarrow$ *fields are subsets of their algebraic closures.*

ACA_0: arithmetic comprehension axiom

Reverse field theory

In the reverse math setting (second order arithmetic with limits on comprehension and induction) a field is a countable set with operations that satisfy the usual field axioms. One can encode copies of familiar fields like $\mathbb{Q}$ or $\mathbb{Q}(\sqrt{2})$.vskip .1in
If every non-constant polynomial in K has a root in K, we say K is algebraically closed. An algebraic closure of F is an algebraically closed field $\overline{F}$ with an embedding $\varphi : F \to \overline{F}$.

$\mathsf{RCA}_0 \vdash$ *every field has an algebraic closure.*

$\mathsf{WKL}_0 \leftrightarrow$ *algebraic closures are unique.*

$\mathsf{ACA}_0 \leftrightarrow$ *fields are subsets of their algebraic closures.*

These results appear in Friedman, Simpson, and Smith's paper [1] and also in Simpson's book [5]. They are related to earlier results in recursive (computable) algebra.

Extending automorphisms

For this talk, we will concentrate on characteristic 0 fields.

Extending automorphisms

For this talk, we will concentrate on characteristic 0 fields.

Theorem 1 (RCA_0) The following are equivalent:

(1) WKL_0.

(2) Let F be a field with an algebraic closure $\overline{F}$. If $\alpha \in \overline{F}$ and $\varphi : F(\alpha) \to F(\alpha)$ is an automorphism of $F(\alpha)$ that fixes F, then φ extends to an F-automorphism of $\overline{F}$.

Extending automorphisms

For this talk, we will concentrate on characteristic 0 fields.

Theorem 1 (RCA_0) The following are equivalent:

(1) WKL_0.

(2) Let F be a field with an algebraic closure $\overline{F}$. If $\alpha \in \overline{F}$ and $\varphi : F(\alpha) \to F(\alpha)$ is an automorphism of $F(\alpha)$ that fixes F, then φ extends to an F-automorphism of $\overline{F}$.

Ideas from the proof of $(1) \to (2)$:

Build a tree of initial segments of F-automorphisms of $\overline{F}$.

At each node map $x \in \overline{F}$ to some root of some polynomial it satisfies. (Bounded levels.)

Stop extending initial non-automorphisms.

Any infinite path codes an F-automorphism.

Theorem 1 (RCA_0) The following are equivalent:

(1) WKL_0.

(2) Let F be a field with an algebraic closure $\overline{F}$. If $\alpha \in \overline{F}$ and $\varphi : F(\alpha) \to F(\alpha)$ is an automorphism of $F(\alpha)$ that fixes F, then φ extends to an F-automorphism of $\overline{F}$.

Ideas from the proof of $(2) \to (1)$:

Separate the ranges of disjoint positive injections f and g.

Let $F = \mathbb{Q}[\sqrt{p_{f(i)}}, \sqrt{2p_{g(i)}}]$, note that $\sqrt{2} \notin F$.

Define $\varphi : F(\sqrt{2}) \to F(\sqrt{2})$ by $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$.

Use (2) to extend φ to $\overline{\mathbb{Q}}$.

Since φ fixes F, $\{j \mid \varphi(\sqrt{p_j}) = \sqrt{p_j}\}$ includes the range of f and avoids the range of g.

Nontrivial automorphisms

Theorem 2 (RCA_0) The following are equivalent:

1. WKL_0.
2. Let F be a field and let K be a proper algebraic extension of F. Suppose that every irreducible polynomial over F that has a root in K splits into linear factors in K. Then there is a non-trivial F-automorphism of K.

Theorem (Metakides and Nerode [4]) There is a recursively presented field F with a recursively presented algebraic extension K such that K has many F-automorphisms, but the only computable F-automorphism is the identity.

Nontrivial automorphisms

Theorem 2 (RCA$_0$) The following are equivalent:

1. WKL$_0$.
2. Let F be a field and let K be a proper algebraic extension of F. Suppose that every irreducible polynomial over F that has a root in K splits into linear factors in K. Then there is a non-trivial F-automorphism of K.

Ideas from the reversal:

Separate the ranges of disjoint positive injections f and g.

Let $K = \mathbb{Q}(\sqrt{p_i} \mid i \in \mathbb{N})$.

Let $F = \mathbb{Q}(\sqrt{p_i}\sqrt{p_{(i,g(j))}}, \sqrt{p_{(i,f(j))}} \mid i, j \in \mathbb{N})$.

Prove that $\sqrt{2} \notin F$.

If φ is a non-identity F-autom. of K, it moves some $\sqrt{p_i}$.

For that value of i, $\{j \mid \varphi(\sqrt{p_{(i,j)}}) = \sqrt{p_{(i,j)}}\}$ includes the range of f and avoids the range of g.

Notions of normality

Here are several versions of "K is a normal extension of F."
The first three are from Lang [3].

NOR1: Every irred. polynomial over F that has a root in K splits completely over K.

NOR2: K is the splitting field of some sequence of polynomials over F.

NOR3: If $\varphi : K \to \overline{F}$ is an F-embedding, then φ is an F-automorphism of K.

NOR4: If $\varphi : \overline{F} \to \overline{F}$ is an F-automorphism, then φ is an F-automorphism on K.

Thm 3: RCA_0 proves NOR1 $\leftrightarrow$ NOR2 $\to$ NOR3 $\to$ NOR4.

Thm 4 (RCA_0) **The following are equivalent:**

1. WKL_0
2. NOR4 $\to$ NOR2
3. NOR4 $\to$ NOR3
4. NOR3 $\to$ NOR2

Isomorphic towers

Theorem 5 (RCA_0) The following are equivalent:

1. ACA_0.
2. Suppose $K = \langle k_i \rangle_{i \in \mathbb{N}}$ and $J = \langle j_i \rangle_{i \in \mathbb{N}}$ are algebraic extensions of F. If for all $n \in \mathbb{N}$, $F(k_1, \ldots, k_n) \preceq_F J$ and $F(j_1, \ldots, j_n) \preceq_F K$, then $K \cong_F J$.

Isomorphic towers

Theorem 5 (RCA_0) The following are equivalent:

1. ACA_0.
2. Suppose $K = \langle k_i \rangle_{i\in\mathbb{N}}$ and $J = \langle j_i \rangle_{i\in\mathbb{N}}$ are algebraic extensions of F. If for all $n \in \mathbb{N}$, $F(k_1, \ldots, k_n) \preceq_F J$ and $F(j_1, \ldots, j_n) \preceq_F K$, then $K \cong_F J$.

Theorem 6 (RCA_0) The following are equivalent:

1. WKL_0.
2. Let $\langle F(\vec{\alpha}_i) \mid i \in \mathbb{N}\rangle$ and $\langle F(\vec{\beta}_i) \mid i \in \mathbb{N}\rangle$ be increasing sequences of finite NOR1-normal algebraic extensions of F. Let $K = \bigcup_{i\in\mathbb{N}} F(\vec{\alpha}_i)$ and let $J = \bigcup_{i\in\mathbb{N}} F(\vec{\beta}_i)$. If for all $i \in \mathbb{N}$, $F(\vec{\alpha}_i) \preceq_F J$ and $F(\vec{\beta}_i) \preceq_F K$, then $K \cong_F J$.

The reversal for Theorem 6 is a construction of Miller and Shlapentokh.

Bibliography

[1] Harvey M. Friedman, Stephen G. Simpson, and Rick L. Smith, *Countable algebra and set existence axioms*, Ann. Pure Appl. Logic **25** (1983), no. 2, 141–181.
DOI 10.1016/0168-0072(83)90012-X MR725732.

[2] ______, *Addendum to: "Countable algebra and set existence axioms" [Ann. Pure Appl. Logic* **25** *(1983), no. 2, 141–181]*, Ann. Pure Appl. Logic **28** (1985), no. 3, 319–320.
DOI 10.1016/0168-0072(85)90020-X MR790391.

[3] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556.

[4] G. Metakides and A. Nerode, *Effective content of field theory*, Ann. Math. Logic **17** (1979), no. 3, 289–320.
DOI 10.1016/0003-4843(79)90011-1 MR556895.

[5] Stephen G. Simpson, *Subsystems of second order arithmetic*, 2nd ed., Perspectives in Logic, Cambridge University Press, Cambridge, 2009.
DOI 10.1017/CBO9780511581007 MR2517689.