Extending automorphisms of normal algebraic fields

Matthew Harrison-Trainor

University of California, Berkeley

AMS Sectional Meeting, Charleston, SC, March 2017

This is joint work with Russell Miller and Alexander Melnikov.

I will be talking about the effective versions of the following facts about fields:

- Every embedding of a field F into an algebraically closed field K extends to an embedding of $\overline{F}$ into K.
- Every automorphism of a field F extends to an automorphism of $\overline{F}$.

First we will review some effective field theory.

Let F be a computable field.

Definition

The *splitting set* S_F of F is the set of all polynomials $p \in F[X]$ which are reducible over F. If S_F is computable, we say that F has a splitting algorithm.

Theorem (Rabin's embedding theorem)

There is a computable algebraically closed field $\overline{F}$ *and a computable field embedding* $\imath: F \to \overline{F}$ *such that* $\overline{F}$ *is algebraic over* $\imath(F)$.

For any such $\overline{F}$ *and* $\imath$, *the image* $\imath(F)$ *of* F *in* $\overline{F}$ *is Turing equivalent to the splitting set of* F.

Theorem (Kronecker)

If F *has a splitting algorithm, then every finite extension of* F *has a splitting algorithm.*

We want to know:

- When does a computable embedding of a field F into an algebraically closed field K extend to a computable embedding of $\overline{F}$ into K?
- When does a computable automorphism of a field F extend to a computable automorphism of $\overline{F}$?

Friedman, Simpson, and Smith, and Dorais, Hirst, and Shafer analyzed these questions using Reverse Mathematics. We can state their results in terms of effective algebra.

For embeddings into algebraically closed fields:

Theorem (Friedman-Simpson-Smith; Dorais-Hirst-Shafer)

Let F be a computable field and let $\imath: F \to \overline{F}$ be a computable embedding of F into its algebraic closure.

If F has a splitting algorithm, every computable embedding of F into a computable algebraically closed field K extends to a computable embedding of $\overline{F}$ into K.

Even if F does not have a splitting algorithm, every computable embedding of F into a computable algebraically closed field K extends to a low embedding of $\overline{F}$ into K.

For extensions of automorphisms:

Theorem (Friedman-Simpson-Smith; Dorais-Hirst-Shafer)

Let F be a computable field and let $\imath : F \to \overline{F}$ be a computable embedding of F into its algebraic closure.

If F has a splitting algorithm, every computable automorphism of F extends to a computable automorphism of $\overline{F}$.

Even if F does not have a splitting algorithm, every computable automorphism of F extends to a low automorphism of $\overline{F}$.

We will try to answer the question: is it necessary to have a splitting algorithm?

Theorem (HT-Miller-Melnikov)

Let F be a computable field and let $\imath\colon F \to \overline{F}$ be a computable embedding of F into its algebraic closure. The following are equivalent:

1. *F has a splitting algorithm.*
2. *Every computable embedding of F into a computable algebraically closed field K extends to a computable embedding of $\overline{F}$ into K.*

$$\begin{tikzcd} \overline{F} \arrow[r, dashed, "\beta"] & K \\ F \arrow[u, "\imath"] \arrow[ur, "\alpha"'] & \end{tikzcd}$$

Theorem (HT-Miller-Melnikov)

Let F be a computable normal algebraic extension of the prime field and let $\imath\colon F \to \overline{F}$ be a computable embedding of F into its algebraic closure. The following are equivalent:

1. *$\mathcal{F}$ has a splitting algorithm.*
2. *Every computable automorphism of F extends to a computable automorphism of $\overline{F}$.*

$$\begin{tikzcd} \overline{F} \arrow[r, dashed, "\beta"] & \overline{F} \\ \mathcal{F} \arrow[u, "\imath"] \arrow[r, "\alpha"'] & F \arrow[u, "\imath"'] \end{tikzcd}$$

Before, we fixed the embedding of F into $\overline{F}$. What happens if we let this embedding vary?

Question

Which fields F have the following property?

- For every computable automorphism α of F, there is a computable embedding $\imath\colon F \to \overline{F}$ of F into an algebraic closure and a computable automorphism β of $\overline{F}$ extending α.

We do not have a complete solution to this question, but towards a partial solution, we introduce the *non-covering property*.

Definition

We say that a group G has the *non-covering property* if for all finite index normal subgroups $M \subsetneq N$ of G and $g \in G$, there is $h \in gN$ such that for all $x \in G$, $x^{-1}hx \notin gM$.

Lemma

Let F/E be a separable normal extension. The following are equivalent:

1. *$Gal(F/E)$ has the non-covering property.*
2. *For all finite normal subextensions K_1/E and K_2/E with $K_2 \nsubseteq K_1$, and every pair of automorphisms σ of K_1 and τ of K_2 fixing E, there is an automorphism α of F extending σ and incompatible with τ (i.e., (K_2, τ) does not embed into (F, α) as a difference field).*

Theorem (HT-Miller-Melnikov)

Let F be a computable normal algebraic extension of the prime field $\mathbb{F}_p$ such that $Gal(F/\mathbb{F}_p)$ has the non-covering property. The following are equivalent:

1. *F has a splitting algorithm.*
2. *For every computable automorphism α of F, there is a computable embedding $\imath\colon F \to \overline{F}$ of F into an algebraic closure and a computable automorphism β of $\overline{F}$ extending α.*

$$\begin{tikzcd}
\overline{F} \arrow[r, dashed, "\beta"] & \overline{F} \\
\mathcal{F} \arrow[u, dashed, "\imath"] \arrow[r, "\alpha"'] & F \arrow[u, dashed, "\imath"']
\end{tikzcd}$$

The following groups have the non-covering property:

- abelian groups,
- simple groups,
- the quaternion group.

S_3 does not have the non-covering property.

Theorem (HT-Miller-Melnikov)

Let $\{G_i : i \in I\}$ be a collection of profinite groups, each of which has the non-covering property. Then $\prod_{i \in I} G_i$ has the non-covering property.

Theorem (HT-Miller-Melnikov)

Let F be a computable normal algebraic extension of $\mathbb{F}_p$ in characteristic $p > 0$. The following are equivalent:

1. *F has a splitting algorithm.*
2. *For every computable automorphism α of F, there is a computable embedding $\imath \colon F \to \overline{F}$ of F into an algebraic closure and a computable automorphism β of $\overline{F}$ extending α.*

Proof.

The Galois group of every normal extension $F/\mathbb{F}_p$ in characteristic $p > 0$ is abelian and hence has the non-covering property. $\square$

Question

Is this true in characteristic zero?