

Model theory of Galois actions

(joint work with Özlem Beyarslan)

Piotr Kowalski

Uniwersytet Wrocławski

ALaNT 5

*Joint Conferences on **A**lgebra, **L**ogic and **N**umber **T**heory
12th Czech, Polish and Slovak Conference on Number Theory
21st Colloquiumfest on Algebra and Logic
Będlewo, 24-29 June 2018.*

- Model-theoretic analysis of first-order properties of algebraic structures such as: rings, groups, fields, valued fields, ordered fields, differential fields or difference fields.
- For example, quantifier elimination results give a full description (having some geometric flavour) of definable sets and definable functions between them, e.g. *Chevalley's Theorem on Constructible Sets* corresponds to quantifier elimination for the theory of algebraically closed fields.
- In this work, we perform the above kind of analysis for *group actions on fields*.

G -fields as first-order structures

We fix a finitely generated (marked) group:

$$G = \langle \rho \rangle, \quad \rho = (\rho_1, \dots, \rho_m).$$

By a G -field, we mean a field together with a G -action by field automorphisms. Similarly, we have G -field extensions, G -rings, etc. We consider a G -field as a first-order structure in the following way

$$\mathbf{K} = (K, +, -, \cdot, \rho_1, \dots, \rho_m).$$

Note that any ρ_i above denotes *three* things at the same time:

- an element of G ,
- a function from K to K ,
- a formal function symbol.

Existentially closed G -fields: definition

Let us fix a G -field (K, ρ) .

Systems of G -polynomial equations

Let $x = (x_1, \dots, x_n)$ be a tuple of variables and $\varphi(x)$ be a **system of G -polynomial equations over K** , i.e.:

$$\varphi(x) : F_1(g_1(x_1), \dots, g_n(x_n)) = 0, \dots, F_n(g_1(x_1), \dots, g_n(x_n)) = 0$$

for some $g_1, \dots, g_n \in G$ and $F_1, \dots, F_n \in K[X_1, \dots, X_n]$.

Existentially closed G -fields

The G -field (K, ρ) is **existentially closed (e.c.)**, if any system $\varphi(x)$ of G -polynomial equations over K which is solvable in a G -extension of (K, ρ) is already solvable in (K, ρ) .

Existentially closed G -fields: first properties

- Any G -field has an e.c. G -field extension (a general property of inductive theories).
- For $G = \{1\}$, the class of e.c. G -fields coincides with the class of algebraically closed fields.
- For $G = \mathbb{Z}$, the class of e.c. G -fields coincides with the class of **transformally** (or **difference**) **closed fields**.
- An e.c. G -field is usually *not* algebraically closed.
- The complex field \mathbb{C} with the complex conjugation automorphism is *not* an e.c. C_2 -field. (By C_n , we denote the cyclic group of order n written multiplicatively.)

Properties of existentially closed G -fields: Sjögren

Let K be an e.c. G -field, and $F := K^G$ be the fixed field.

- Both K and F are perfect.
- Both K and F are pseudo algebraically closed (PAC), hence their absolute Galois groups are projective profinite groups.
- The profinite group $\text{Gal}(F^{\text{alg}} \cap K/F)$ coincides with the profinite completion \hat{G} of G .
- The profinite group $\text{Gal}(F)$ (the absolute Galois group of F) coincides with the **universal Frattini cover** $\tilde{\hat{G}}$ of \hat{G} .
- The field K is algebraically closed iff \hat{G} is projective (iff $\tilde{\hat{G}} = \hat{G}$), more precisely:

$$\text{Gal}(K) \cong \ker \left(\tilde{\hat{G}} \rightarrow \hat{G} \right).$$

Model companions in general

Definition

The theory of existentially closed models of an inductive theory T is called **Model Companion** of T .

Warning

Model companion of T need *not* exist, i.e. for some theories T the class of existentially closed models of T is not **elementary**.

Example

- Fields \Rightarrow Algebraically Closed Fields;
- Ordered Fields \Rightarrow Real Closed Fields;
- Linear Orders \Rightarrow Dense Linear Orders;
- Graphs \Rightarrow Random Graphs;
- Theory of groups does not have model companion.

Definition

If the class of existentially closed G -fields is elementary, then we call the resulting theory G -TCF and say that G -TCF exists (i.e. G -TCF is model companion of the theory of G -fields).

Example

- For $G = \{1\}$, we get G -TCF = ACF.
- For $G = F_m$ (free group), we get G -TCF = ACFA $_m$.
- If G is finite, then G -TCF exists (Sjögren, independently Hoffmann-K.)
- $(\mathbb{Z} \times \mathbb{Z})$ -TCF does *not* exist (Hrushovski).

Axioms for ACFA

We fix now a difference field (K, σ) , i.e. $(G, \rho) = (\mathbb{Z}, 1)$ (or, for technical reasons, $(G, \rho) = (\mathbb{Z}, 0, 1)$).

- By a **variety**, we always mean an affine K -variety which is K -irreducible and K -reduced (i.e. a prime ideal of $K[\bar{X}]$).
- For any variety V , we also have the variety ${}^\sigma V$ and the bijection (not a morphism!)

$$\sigma_V : V(K) \rightarrow {}^\sigma V(K).$$

Our definition of “ \mathbb{Z} -pair”

A pair of varieties (V, W) is called a **\mathbb{Z} -pair**, if $W \subseteq V \times {}^\sigma V$ and the projections $W \rightarrow V, W \rightarrow {}^\sigma V$ are dominant.

Axioms for ACFA (Chatzidakis-Hrushovski)

The difference field (K, σ) is e.c. if and only if for any \mathbb{Z} -pair (V, W) , there is $a \in V(K)$ such that $(a, \sigma_V(a)) \in W(K)$.

Axioms for G -TCF, G finite

Let $G = \{\rho_1, \dots, \rho_e\} = \rho$ be a finite group and (K, ρ) be a G -field.

Definition of G -pair

A pair of varieties (V, W) is a **G -pair**, if:

- $W \subseteq \rho^1 V \times \dots \times \rho^e V$;
- all projections $W \rightarrow \rho^i V$ are dominant;
- **Iterativity Condition**: for any i , we have $\rho^i W = \pi_i(W)$, where

$$\pi_i : \rho^1 V \times \dots \times \rho^e V \rightarrow \rho^i \rho^1 V \times \dots \times \rho^i \rho^e V$$

is the appropriate coordinate permutation.

Axioms for G -TCF, G finite (Hoffmann-K.)

The G -field (K, ρ) is e.c. if and only if for any G -pair (V, W) , there is $a \in V(K)$ such that

$$((\rho_1)_V(a), \dots, (\rho_e)_V(a)) \in W(K).$$

Our strategy 1

- Find a generalization of the known results (mentioned above) about free groups and finite groups.
- Natural class of groups for such a generalization: *virtually free* groups.
- For a fixed (G, ρ) , the general scheme of axioms should be as follows: for any “ G -pair” (V, W) , there is $a \in V(K)$ such that

$$\rho_V(a) := ((\rho_1)_V(a), \dots, (\rho_m)_V(a)) \in W(K).$$

Hence one needs to find the right notion of a G -pair.

G -pairs in general (looking for this “right notion”)

A pair of varieties (V, W) will be called a **G -pair**, if:

- $W \subseteq \rho V := \rho_1 V \times \dots \times \rho_m V$;
- all projections $W \rightarrow \rho_i V$ are dominant;
- **Iterativity Condition** (to be found) is satisfied.

Our strategy 2

We aim to find a good Iterativity Condition for a virtually free, finitely generated group (G, ρ) .

- G free: trivial Iterativity Condition.
- G finite: Iterativity Condition as before.

We need a convenient procedure to obtain virtually free groups from finite groups. Luckily, such a procedure exists and gives the right Iterativity Condition.

Theorem (Karrass, Pietrowski and Solitar)

Let H be a finitely generated group. Then TFAE:

- H is virtually free;
- H is isomorphic to the *fundamental group* of a finite *graph of finite groups*.

Graph of groups (slightly simplified)

A **graph of groups** $G(-)$ is a connected graph $(\mathcal{V}, \mathcal{E})$ and:

- a group G_i for each vertex $i \in \mathcal{V}$;
- a group A_{ij} for each edge $(i, j) \in \mathcal{E}$ together with monomorphisms $A_{ij} \rightarrow G_i, A_{ij} \rightarrow G_j$.

Fundamental group of graph of groups

For a fixed maximal subtree \mathcal{T} of $(\mathcal{V}, \mathcal{E})$, the **fundamental group** of $(G(-), \mathcal{T})$ (denoted by $\pi_1(G(-), \mathcal{T})$) can be obtained by successively performing:

- one free product with amalgamation for each edge in \mathcal{T} ;
- and then one HNN extension for each edge not in \mathcal{T} .

$\pi_1(G(-), \mathcal{T})$ does not depend on the choice of \mathcal{T} (up to \cong).

Iterativity Condition for amalgamated products

- Let $G = G_1 * G_2$, where G_i are finite. We take $\rho = \rho_1 \cup \rho_2$, where $\rho_i = G_i$ and the neutral elements of G_i are identified in ρ . We also define the projection morphisms $p_i : {}^\rho V \rightarrow {}^{\rho_i} V$. Let $W \subseteq {}^\rho V$ satisfy the dominance conditions.

Iterativity Condition for $G_1 * G_2$

$(V, p_i(W))$ is a G_i -pair for $i = 1, 2$ (up to Zariski closure).

- Let $G = \pi_1(G(-))$, where $G(-)$ is a tree of groups. We take $\rho = \bigcup_{i \in \mathcal{V}} G_i$, where for $(i, j) \in \mathcal{E}$, G_i is identified with G_j along A_{ij} .

Iterativity Condition for the fundamental group of tree of groups

$(V, p_i(W))$ is a G_i -pair for all $i \in \mathcal{V}$ (up to Zariski closure).

Let us fix:

- a presentation $H = \langle X \mid R \rangle$ of a group H ;
- two subgroups $H_1, H_2 \leq H$;
- an isomorphism $\alpha : H_1 \rightarrow H_2$.

The **HNN-extension of H relative to α** , denoted by $H*_\alpha$, is:

$$H*_\alpha = \langle X, t \mid R, h_1 t = t \alpha(h_1); \quad \forall h_1 \in H_1 \rangle.$$

H is a subgroup of $H*_\alpha$ (a theorem of Graham **H**igman, B. H. **N**eumann and Hanna **N**eumann), and α is given by an inner automorphism of $H*_\alpha$ in the “most free” way.

Example

- $H*_{\text{id}_{\{1\}}} = H * \mathbb{Z}$, in particular $\mathbb{Z} = \{1\}*_\text{id}$.
- For $\alpha \in \text{Aut}(H)$, we get $H*_\alpha = H \rtimes_\alpha \mathbb{Z}$, e.g. $H*_{\text{id}_H} = H \times \mathbb{Z}$.

Iterativity Condition for HNN extensions

Let $C_2 \times C_2 = \{1, \sigma, \tau, \gamma\}$ and consider the following:

$$\alpha : \{1, \sigma\} \cong \{1, \tau\}, \quad G := (C_2 \times C_2) *_{\alpha}.$$

Then the crucial relation defining G is $\sigma t = t\tau$.

We take:

- $\rho := (1, \sigma, \tau, \gamma, t, t\sigma, t\tau, t\gamma)$;
- $\rho_0 := (1, \sigma, \tau, \gamma)$;
- $t\rho_0 := (t, t\sigma, t\tau, t\gamma)$.

Let $W \subseteq {}^{\rho}V$ satisfy the dominance conditions.

Iterativity Condition for $(C_2 \times C_2) *_{\alpha}$

- ${}^t(p_{\rho_0}(W)) = p_{t\rho_0}(W)$.
- $(V, p_{\rho_0}(W))$ is a $(C_2 \times C_2)$ -pair.

Main Theorem

We find a complicated Iterative Condition for virtually free groups using the two previous conditions as building blocks.

Theorem (Beyarslan-K.)

If G is finitely generated and virtually free, then G -TCF exists.

Model-theoretic properties of G -TCF

- If G is finite, then G -TCF is **supersimple** of finite rank(= $|G|$).
- If G is infinite and free, then G -TCF is **simple** (not supersimple, for non-cyclic G).
- As we already know (Sjögren), for any G , if (K, ρ) is an e.c. G -field then K is PAC and K^G is PAC.
- Chatzidakis: for a PAC field K , the theory $\text{Th}(K)$ is simple iff K is bounded (i.e. the profinite group $\text{Gal}(K)$ is small).

New theories are not simple

Theorem (Beyarslan-K.)

Assume that G is finitely generated, virtually free, infinite and not free. Then the following profinite group

$$\ker \left(\tilde{\hat{G}} \rightarrow \hat{G} \right)$$

is not small.

Corollary

Putting everything together, we get the following.

- If G is finitely generated and virtually free, then the theory G -TCF is simple if and only if G is finite or G is free.
- If G is finitely generated, virtually free, infinite and not free, then the theory G -TCF is not even **NTP₂**.

Hierarchy and other types of groups

How G -TCF mat fit into “neo-stability hierarchy”

It looks possible that if the group G is finitely generated and virtually free, then the theory G -TCF is NSOP_1 (Nick Ramsey communicated a sketch of an argument to us).

Non-finitely generated groups

- The theory \mathbb{Q} -TCF exists (Medvedev’s \mathbb{Q} ACFA).
- After a discussion with Alice Medvedev, we seem to have an argument showing that the theory C_{p^∞} -TCF exists, where C_{p^∞} is the Prüfer p -group.

Conjecture (G finitely generated)

The theory G -TCF exists if and only if G is virtually free.

- There is a long list of equivalent conditions characterising the class of finitely generated, virtually free groups e.g.:
 - fundamental groups of finite graphs of finite groups;
 - groups that are recognized by pushdown automata;
 - groups whose Cayley graphs have finite tree width.
- It would be interesting to have one more equivalent condition (as in the conjecture above) coming from model theory!
- Main challenge for a proof of this conjecture: infinite Burnside groups (finitely generated and of bounded exponent).