FIRST-ORDER THEORY OF A FIELD AND ITS INVERSE GALOIS PROBLEM

FRANCESCA BALESTRIERI, JENNIFER PARK, AND ALEXANDRA SHLAPENTOKH

Abstract. Consider a pair (K, G), where K is a field and G is a finite group. We want to investigate the Turing degree of the Inverse Galois Problem, namely the problem of determining whether K has a Galois extension with Galois group isomorphic to G. We show that the Turing degree of this problem is always less or equal to the degree of the first-order theory of the field in the language of rings and that, in some cases, the degree of the problem is less or equal to the degree of the existential theory of the field in the same language. It follows that if a field K has a decidable first-order theory, then there is an algorithm taking a finite group G as its input and determining whether K has a Galois extension with Galois group isomorphic to G.

A similar reduction can be used to show that the Turing degree of many variations of Inverse Galois Problem – namely, the Inverse Automorphism Problem and the Finite Split Embedding Problem –is also less than or equal to the Turing degree of the first order theory of the field.

1. Introduction

This paper discusses the connection between the *Inverse Galois Problem* (IGP) and decidability of the first-order and/or existential theory of fields. We state the IGP below.

Problem 1 (Inverse Galois Problem over a field K for a group G, IGP(K, G))**.** *Let K be a field, and let G be a finite group of size d. Does there exist a Galois extension L of K of degree d with the Galois group of the extension isomorphic to G?*

This problem has a long history dating back to the Kronecker-Weber theorem (which corresponds, in our notation, to IGP$(\mathbb{Q}, \mathbb{Z}/n\mathbb{Z})$) from the early XIX century. While many special cases of this problem and its variants are known [Har87], [Koe04], [Pop96], the general question remains open.

The first-order language of rings is the language $\mathcal{L}_{ring} = (0, 1, +, \times)$ using universal and existential quantifiers. The problem of deciding which statements of the language are true over a particular ring R can be reduced to the question whether the following type of statements is true:

$$E_1 x_1 \dots E_k x_k P(x_1, \dots, x_k) = 0,$$

where E_i is either a universal or an existential quantifier ranging over R and $P(x_1, \dots, x_k)$ is a polynomial with coefficients in the ring. The statements using existential quantifiers only form what is called the *existential theory* of the ring, which closely relates to Hilbert's 10th Problem, i.e. to the question of whether an arbitrary polynomial equation over the ring in several variables has solutions in the ring.

Date: January 26, 2023.

The fact that the Inverse Galois Problem for a field and a specific group can be coded into a first-order theory of a ring is apparently known ([Koe04]), though, to the best of the authors' knowledge, an explicit specific statement about this does not exist in the literature, nor is it established how uniform such a statement would be. In this paper, we produce a statement in $\mathcal{L}_R$ without any parameters and uniform across all fields that is true if and only if the Inverse Galois Problem over a given field is solvable for a specific finite group. (The statement depends only on the size of the group.) Our statement also makes it clear what is needed in order to make a transition from the first-order theory to the existential one; moreover, we point to a large class of fields where the IGP is indeed reducible to the existential theory of the field. (We make the reduction explicit below).

We also construct first-order or Diophantine statements coding generalizations of the IGP, namely the *Finite Split Embedding Problem* (FSEP) and what we call the *Inverse Automorphism Problem* (IAP). In the appendix, we briefly discuss the fact that if we consider the first-order theory of rings relative to the IGP of their fraction field, then the reduction of IGP to existential theory occurs in many more cases, primarily as a consequence of the result of M. Davis, J. Robinson, H. Putnam and Yu. Matijasevich.

1.1. **Turing degrees and reduction.** We first define Turing degrees and give a precise formulation of the problem we want to address.

1.1.1. *Computable and listable sets and Turing degrees.* A subset $S \subset \mathbb{Z}$ is **computable** if there exists an algorithm (or a computer program terminating on every input) that determines membership in the set. A subset $S \subset \mathbb{Z}$ is **listable** if there exists an algorithm (or a computer program) that lists the set. Given two subsets $A, B \subset \mathbb{Z}$, we say that $A \leq_T B$ (A is Turing reducible to B) if there exists an algorithm taking the characteristic function of B as its input and generating the characteristic function of A. If $A \leq_T B$ and $B \leq_T A$, then we say that $A \equiv_T B$ (A is Turing equivalent to B). The relation $\equiv_T$ is an equivalence relation and the corresponding equivalence classes are called Turing degrees.

A classical theorem of computability theory states that there are listable sets which are not computable, the most important example of such a set being the halting set. It is also a well-known fact that every listable set is Turing reducible to the halting set.

1.1.2. *Encoding the collection of the isomorphism classes of finite groups and the theory of a field.* We identify the set of isomorphism classes of finite groups with $\mathbb{N}$ via a map σ defined in the following way:

- Let $\mathcal{G}$ be a collection of representatives of isomorphism classes of finite groups (note that $\mathcal{G}$ is countable, so there is an effective bijection $\sigma : \mathcal{G} \to \mathbb{N}$ with the image being exactly $\mathbb{N}$.)
- We note that $\sigma(G)$ can be effectively determined once we are given a multiplication table of a group G and, vice versa, we can effectively recover a multiplication table for G from $\sigma(G)$.

Let K be any fixed field. For each $d \in \mathbb{N}$, let

$$\mathcal{H}_{K,d} = \{n \in \mathbb{N} : \#\sigma^{-1}(n) = d \text{ and } K \text{ has a Galois extension with Galois group } \sigma^{-1}(n)\}.$$

1.1.3. *Main theorem.* In this paper we investigate the Turing degree of $\mathcal{H}_{K,d}$. We will compare the Turing degree of $\mathcal{H}_{K,d}$ to the Turing degrees of the first-order and existential theory of K in the language of rings possibly augmented by countably many constant symbols. Recall that the *first-order theory (resp. existential theory) of a field K in the language of rings*, denoted Th(K) (resp. $\mathrm{Th}_\exists$(K)), is the collection of all sentences in the language of rings (resp. existential language of rings) that are true over K.

Since we are using a countable language and since a sentence is a finite string of symbols of the language, the collection of all sentences in the language (resp. existential language) is countable and can be put into an effective bijection with $\mathbb{N}$. Thus we can identify Th(K) (resp. $\mathrm{Th}_\exists$(K)) with a subset of $\mathbb{N}$ and define the Turing degree of the theory (resp. existential theory) to be the Turing degree of the corresponding subset of $\mathbb{N}$.

Using definitions above one of the main theorems of the paper can be stated as follows:

Theorem. *(Corollary 2.11)*

(1) *For any field K we have that $\mathcal{H}_{K,d} \leq_T$ Th(K).*
(2) *There exist fields K such that $\mathcal{H}_{K,d} \leq_T \mathrm{Th}_\exists$(K). In particular, this statement holds for K a global field.*

1.1.4. *Variations on the main theorem.* By similar methods, we also prove several variations of IGP, an example of which is stated below:

Theorem. *(Theorem 3.1) Let K be a field. Then, given a finite group H and a multiple n of $|H| = m$, there exists a polynomial equation, depending on H and K only, such that there exists a finite extension L of K degree n (not necessarily Galois over L) with $\mathrm{Aut}(L/K) \cong H$ if and only if the equation has solutions in K.*

Acknowledgments

F.B. and J.P. thank the Institut Henri Poincaré and the organizers of the trimester *À la rédecouverte des points rationnels* for allowing this project to begin. J.P. and A.S. thank American Institute of Mathematics for creating an environment where their collaboration could start. The authors thank Arno Fehm and Laurent Moret-Bailly for helpful comments. F.B. was partially supported by the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant 840684. J.P. was partially supported by NSF DMS-1902199 and DMS-2152182, A.S. was partially supported by NSF DMS-2152098.

2. The first-order theory of a field and its Inverse Galois Problem

Our goal is to prove the following theorem:

Theorem 2.1. *Let G be a finite group of size d. Then there exists an effective procedure taking as the input the multiplication table of the group and constructing a first-order statement in the language of rings such that the statement is true in K if and only if K has a Galois extension with the Galois group isomorphic to G.*

Remark 2.2. For any base field under consideration, we fix once and for all an algebraic closure of that field, and we consider any extension that we construct to be inside this algebraic closure.

Remark 2.3. There always exists a first-order statement such that it is true in K if and only if K has a Galois extension with the Galois group isomorphic to G. One could let the statement be a tautology if the extension exists, and the negation of the tautology otherwise. However, in order to determine which of the statements should be selected, one must already have the answer to IGP in this case. The point of the theorem above is that there is an algorithm to construct such a statement *without* knowing whether the extension we are looking for exists.

The following corollary is an obvious consequence of Theorem 2.1.

Corollary 2.4. *The Turing degree of IGP over any field or ring is less than or equal to the degree of the first-order theory of the field.*

For the remainder of the paper we use the following notation.

Notation 2.5.
- *K is a field;*
- *$I_{K,d} \subset K^d$ is such that $(a_0, \ldots, a_{d-1}) \in I_{K,d}$ if and only if the polynomial $a_0 + \ldots + a_{d-1}T^{d-1} + T^d$ is irreducible over K.*

In order to talk about extensions of a field we need a way to describe the irreducible (over the field) polynomials. This is not a hard task if we are using the full first-order (as opposed to existential) language.

Proposition 2.6. *Let K be a field. Let $(a_0, \ldots, a_{n-1}) \in K^n$. Then there exists a first-order statement in the language of rings without parameters that is true over K if and only if the polynomial $f(T) = a_0 + a_1T + \ldots + a_{n-1}T^{n-1} + T^n$ is irreducible.*

Proof. The case for $n = 1$ is clear, so we may assume that $n > 1$. The following existential statement S_d, for $d = 1, ..., n-1$, asserts that a polynomial can be factored into a degree d factor and a degree $n - d$ factor:

$$(S_d) \quad \exists c_{0,d}, \ldots, c_{d,d}, b_{0,d}, \ldots, b_{n-d,d} : \\ f(T) = (c_{0,d} + c_{1,d}T + \cdots + c_{d,d}T^d)(b_{0,d} + b_{1,d}T + \cdots + b_{n-d,d}T^{n-d}).$$

The fact that the polynomial f is reducible is then equivalent to the following disjunction

$$S_1 \vee \cdots \vee S_{n-1},$$

and therefore the theorem is proven by taking the negation of the above sentence. □

The proposition below shows that given an *irreducible* polynomial over K, the existential language of rings is enough to assert that the root of the polynomial generates a Galois extension of K. In this existential statement the coefficients of the polynomial occur as parameters.

Proposition 2.7. *Let K be a field, let L/K be a finite extension, and let $f \in K[x]$ be an irreducible polynomial of degree d over K such that for a root α of $f(x)$, we have $L = K(\alpha)$. Then there exists a system of polynomial equations with coefficients in $\mathbb{Z}$, a set of parameters (coefficients of f) ranging of K, a set of variables ranging over K and a set of variables ranging over L such that the field extension L/K is Galois of degree d if and only if the system of polynomial equations has a solution in K.*

Proof. Let $\alpha_1 := \alpha$ and consider the following set of equations (in the unknowns $s_{i,0}, \ldots, s_{i,d-1} \in K$), for $i \in \{1, \ldots, d\}$) over K:

$$\begin{cases} \sum_{j=0}^{d-1} s_{i,j}\alpha^j &= \alpha_i \quad \text{for } i \in \{2, \ldots, d\}, \\ f(\alpha_i) &= 0 \quad \text{for } i \in \{1, \ldots, d\}, \\ \alpha_i &\neq \alpha_j \quad \text{for all } i \neq j \text{ with } i, j \in \{1, \ldots, d\}. \end{cases} \tag{2.1}$$

The above set of conditions shows that if $f(T)$ has a root in L, then it has d distinct roots in L, so that the extension L/K is separable and normal, and hence Galois. The converse implication is obvious. □

Using $I_{K,d}$, we can re-write Proposition 2.7 converting the coefficients of an irreducible polynomial from parameters to variables.

Definition 2.8. Let K be as above, let $d \in \mathbb{Z}_{\geq 1}$. The **Galois set of degree d over K** is

$$\begin{aligned} \mathrm{Gal}_d(K) := \quad & \{(a_0, \ldots, a_{d-1}) \in I_{K,d} : x^d + a_{d-1}x^{d-1} + \cdots + a_0 \\ & \text{generates a Galois field extension of degree } d \text{ over } K\}. \end{aligned}$$

Theorem 2.9. *Let K be as above, and let $d \in \mathbb{Z}_{\geq 1}$.*

1. *$\mathrm{Gal}_d(K)$ is first-order definable over K.*
2. *If $I_{K,d}$ is Diophantine over K for every $d \in \mathbb{Z}_{\geq 0}$, then $\mathrm{Gal}_d(K)$ is Diophantine over K for every $d \in \mathbb{Z}_{\geq 0}$.*

Proof. Proving (1) amounts to rewriting Proposition 2.7 without reference to α. We get rid of α by using the isomorphism $K(\alpha) \cong K[x]/f(x)$ sending $\alpha \mapsto x$, and rewriting (2.1) as the following system of equations with coefficients in $\mathbb{Z}$ and the unknowns $a_0, \ldots, a_{d-1}, s_{2,0}, \ldots, s_{d,d-1}$ in K, where for clarity we add some unnecessary equations and use a variable x transcendental over K:

$$\begin{cases} (a_0, \ldots, a_{d-1}) \in I_{K,d}, \\ f(x) := a_0 + a_1 x + \ldots + a_{d-1}x^{d-1} + x^d, \\ h_1(x) := x, \\ h_i(x) := s_{i,0} + s_{i,1}x + \cdots + s_{i,d-1}x^{d-1} \text{ for } i \in \{1, \ldots, d\}, \\ f(h_i(x)) \equiv 0 \bmod f(x), \\ h_i(x) \not\equiv h_j(x) \bmod f(x) \text{ for } i, j \in \{1, \ldots, d\} \text{ with } i \neq j. \end{cases} \tag{2.2}$$

We now proceed to getting rid of the extra equations and x. We will need several steps to accomplish this. First we rewrite our system in a clearly equivalent form below:

$$\begin{cases} (a_0, \ldots, a_{d-1}) \in I_{K,d}, \\ h_1(x) = x \\ f(\sum_{j=0}^{d-1} s_{i,j}x^j) \equiv 0 \bmod f(x), i \in \{2, \ldots, d\}, \\ h_i(x) \not\equiv h_j(x) \bmod f(x) \text{ for } i, j \in \{1, \ldots, d\} \text{ with } i \neq j. \end{cases} \tag{2.3}$$

Observe that, for each i,

$$f\left(\sum_{j=0}^{d-1} s_{i,j}x^j\right) = \left(\sum_{j=0}^{d-1} s_{i,j}x^j\right)^d + \sum_{r=0}^{d-1} a_r \left(\sum_{j=0}^{d-1} s_{i,j}x^j\right)^r.$$

For each i, the statement $f(\sum_{j=0}^{d-1} s_{i,j}x^j) \equiv 0 \bmod f(x)$ now becomes

$$\left(\sum_{j=0}^{d-1} s_{i,j}x^j\right)^d + \sum_{r=0}^{d-1} a_r \left(\sum_{j=0}^{d-1} s_{i,j}x^j\right)^r = \left(x^d + \sum_{k=0}^{d-1} a_k x^k\right)\left(\sum_{n=0}^{(d-1)^2} u_{i,n}x^i\right),$$

where $u_{i,1}, \ldots, u_{i,(d-1)^2}$ are variables ranging over K. Multiplying all products out and comparing the coefficients corresponding to the same powers of x will yield a system of polynomial equations

$$P_i(a_0, \ldots, a_{d-1}, s_{i,0}, \ldots, s_{i,d-1}, u_{i,0}, \ldots, u_{i,(d-1)^2}) = 0$$

for each $i = 2, \ldots, d$. Observe that the coefficients of this system remain in $\mathbb{Z}$, and they depend on d only.

We now rewrite the non-equivalence $h_i(x) \not\equiv h_j(x) \bmod f(x)$. Since both $h_i(x)$ and $h_j(x)$ are polynomials of degree less than d, the only way they can be equivalent modulo $f(x)$ is if they are equal. Thus, the last condition is equivalent to the disjunctions

$$(s_{i,0} \neq s_{j,0}) \vee \ldots \vee (s_{i,d-1} \neq s_{j,d-1})$$

for all $i, j \in \{1, \ldots, d\}$ with $i \neq j$.

It is obvious from the above that if the first condition in (2.3) is Diophantine, then $\mathrm{Gal}_d(K)$ is Diophantine. □

Now, we wish to recognize the Galois group of a Galois extension L/K. Note that if $L = K(\alpha)$, then the Galois group is completely determined by its action on α.

Theorem 2.10. *Let K be a field, let $d \in \mathbb{Z}_{\geq 0}$, and let G be a finite group of order d.*

(1) *There exists a first-order statement over K that is satisfied over K if and only if K has a Galois extension of degree d with Galois group isomorphic to G. That is, the set of the coefficients of monic polynomials over K generating degree d Galois extensions of K with Galois group isomorphic to G is first-order definable over K.*

(2) *If $I_{K,d}$ is Diophantine over K, then there exists a system of equations (reducible to a single equation by Lemma 1.2.3 of* [Shl06]*) that has solutions in K if and only if K has a Galois extension of degree d with Galois group isomorphic to G. That is, the set of the coefficients of monic polynomials over K generating degree d Galois extensions of K with Galois group isomorphic to G is Diophantine over K.*

Proof. For a d-tuple $\bar{a} = (a_0, \ldots, a_{d-1})$, let $f_{\bar{a}}(x) := a_0 + a_1x + \ldots + a_{d-1}x^{d-1} + x^d$. By Theorem 2.9(1), the set

$$\mathrm{Gal}_d(K) := \{(a_0, \ldots, a_{d-1}) \in K^d : K[x]/f_{\bar{a}}(x) \text{ is a Galois extension of } K\}$$

is first-order definable over K.

We wish to show that its subset

$$T_G := \{\bar{a} = (a_0, \ldots, a_{d-1}) \in K^d : K[x]/f_{\bar{a}}(x) \text{ is a Galois extension of } K \text{ with Galois group } G\}$$

is also definable by a set of first-order formulas with coefficients in K. To this end, we note that the extra set of first-order formulas that define T_G are actually polynomial equations defined over K, described as follows.

If $K(\alpha)/K$ is a Galois extension of K with Galois group G and if the conjugates of α are given by $\alpha_1 := \alpha, \alpha_2, \ldots, \alpha_d$, let $\sigma_i \in G$ denote the automorphism sending α to α_i, for $i = 1, \ldots, d$, with $\sigma_1 = \mathrm{id}$. Then G is completely described by its table of multiplication

$$\sigma_i \sigma_j = \sigma_r, \quad i, j \in \{1, \ldots, d\}. \tag{2.4}$$

We now show that this multiplication table can be written in terms of polynomial equations. We write the conjugates of α in $K(\alpha)$ as linear combinations of powers of α with coefficients $s_{i,j} \in K$, namely

$$\alpha_i = \sum_{j=0}^{d-1} s_{i,j} \alpha^j,$$

and then we translate the relation in (2.4) to

$$\begin{aligned} \sigma_j(\sigma_i(\alpha)) &= \sigma_j(\alpha_i) \\ &= \sigma_j(s_{i,0} + s_{i,1}\alpha + \cdots + s_{i,d-1}\alpha^{d-1}) \\ &= (s_{i,0} + s_{i,1}\alpha_j + \cdots + s_{i,d-1}\alpha_j^{d-1}) \\ &= \left(s_{i,0} + s_{i,1} \left(\sum_{u=0}^{d-1} s_{j,u}\alpha^u \right) + \cdots + s_{i,d-1} \left(\sum_{u=0}^{d-1} s_{j,u}\alpha^u \right)^{d-1} \right) \\ = \sigma_r(\alpha) &= (s_{r,0} + s_{r,1}\alpha + \cdots + s_{r,d-1}\alpha^{d-1}) \end{aligned} \tag{2.5}$$

for all valid triples (i, j, r) with $i, j \in \{1, \ldots, d\}$.

Now T_G is cut out from $\mathrm{Gal}_d(K)$ by a set of polynomial equations with coefficients in K: in addition to the formulas (2.3), we use the equations obtained from the equations (2.5). A priori, these equations involve α, but once again we can rewrite these equations so that all coefficients are in $\mathbb{Z}$ and all the variables range over K.

For the proof of (2), since $I_{K,d}$ is existentially definable, by Theorem 2.9(2), $\mathrm{Gal}_d(K)$ is Diophantine over K. Since T_G is defined from $\mathrm{Gal}_d(K)$ by a set of polynomial equations over K, we see that T_G is also Diophantine over K. □

The theorem above provides an explicit link between $\mathrm{IGP}(K, G)$ and $\mathrm{Th}(K)$. Recall from Section 1.1.2 that $\mathcal{H}_{K,d}$ is in bijection with the collection of all groups G of size d for which a Galois extension of K with Galois group G exists. Thus we have:

Corollary 2.11. *Let K be a countable field. Then*

(1) $\mathcal{H}_{K,d} \leq_T \mathrm{Th}(K)$.
(2) *if* $\mathrm{Th}(K)$ *is decidable, then there is an algorithm to decide whether* $\mathrm{IGP}(K, G)$ *is true.*
(3) *If $I_{K,d}$ is Diophantine in K, then* $\mathrm{IGP}(K, G) \leq_T \mathrm{H10}(K)$.

Remark 2.12. Note that if $\mathrm{Th}(K)$ is decidable and $\mathrm{IGP}(K, G)$ is true, then there is an algorithm to explicitly construct a polynomial with coefficients in K producing the required extension. We need only to systematically check all d-tuples of elements of K to find one that corresponds to an irreducible polynomial and such that the resulting system of equations has solutions in other variables in K.

3. Translating generalizations of IGP into the first-order language of rings

In this section, we consider two generalizations of IGP. The first generalization is the *Finite Split Embedding Problem* (FSEP), while the second one is the *Inverse Automorphism Problem* (IAP).

3.1. **Translating FSEP into the first-order language of fields.**

The Finite Split Embedding Problem (FSEP) takes the following input:

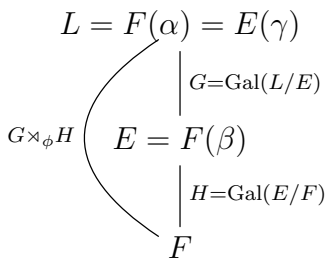
- a base field F and a finite Galois extension E/F with $\mathrm{Gal}(E/F) =: H$;
- a finite group G with an action $\phi : H \to \mathrm{Aut}(G)$, which gives rise to the semi-direct product $G \rtimes_\phi H$;
- the semi-direct product $G \rtimes_\phi H$ comes equipped with an epimorphism $\pi : G \rtimes_\phi H \longrightarrow H$ of finite groups.

A solution to the FSEP is a Galois extension L of F that extends E, together with an isomorphism $i : \mathrm{Gal}(L/F) \xrightarrow{\sim} G \rtimes_\phi H$ such that $\pi \circ i = \mathrm{res}_E : \mathrm{Gal}(L/F) \to \mathrm{Gal}(E/F)$. We consider a generalized version of FSEP, where the data consists of the base field F, the three groups G, H, $G \rtimes_\phi H$, and the projection π only. In other words, we will look for a field extension E/F with $\mathrm{Gal}(E/F) \cong H$ so that the original FSEP is solvable with respect to this field.

We use the following given data to translate the generalized FSEP into the language of rings: that is, we will use the following to obtain a system of polynomial equations over F that has a solution over F if and only if the FSEP with the data F, H, G, ϕ has a solution. Later, we will indicate how to adjust our equations for the original FSEP. We start with a list of the equations that we are going to need to specify a field L where FSEP is solvable.

(1) We assume that we are given the tables of multiplication for $G \rtimes_\phi H, G$ and H. Thus we can write down equations corresponding to a Galois extension L of F with $G \rtimes_\phi H$ as its Galois group.
(2) Let $f(T)$ be irreducible polynomial over F such that its root α generates L over F. Its degree is $|G \rtimes_\phi H| = |G||H| =: m$. Let $f(T) = a_0 + \ldots + T^m$ and stipulate that $f(T)$ is irreducible over F.
(3) Let $\alpha = \alpha_1 \in \bar{\mathbb{Q}}$ be a root of $f(T)$. Let α_i for $i = 1, \ldots, m$ be all the roots of $f(T)$ in $L = F(\alpha)$, with $\alpha_i \neq \alpha_j$.
(4) Let $|H| = r$ and let $g(T)$ be an irreducible polynomial over F of degree r of some generator of H over F.
(5) Let β be a root of $g(T)$ and write β in terms of its coordinates with respect to the power basis of α. We write down equations saying that $\mathrm{Gal}(F(\alpha)/F(\beta)) \cong G$ and $\mathrm{Gal}(F(\beta)/F) \cong H$.
(6) To determine the restriction of an element τ of $\mathrm{Gal}(F(\alpha)/F)$ to $F(\beta)$, we consider $\tau(\beta)$ which we can determine since β is represented as a linear combination of powers of α over F. Then we identify the element $\mu \in H$ such that $\mu(\beta) = \tau(\beta)$.
(7) We assume that we are given an explicit epimorphism $\pi : \mathrm{Gal}(F(\alpha)/F) \to \mathrm{Gal}(F(\beta)/F)$. Thus we can check whether $\pi(\tau)(\beta) = \mu(\beta)$.

To summarise, we have the following diagram:



We now write down equations discussed above, starting with the equations defining a Galois extension L/F with Galois group isomorphic to $G \rtimes_\phi H$. We remind the reader that there is a sentence in the language of rings stating that an m-tuple of elements of F corresponds to a monic irreducible polynomial over F. The statements defining an extension L/F with $\mathrm{Gal}(L/F) \cong G \rtimes_\phi H$ are:

$$\begin{cases} f(T) = a_0 + a_1 T + \ldots + T^m \text{ with } a_0, \ldots, a_{m-1} \in F \text{ is irreducible over } F, \\ f(\alpha_i) = 0, \text{ for } i = 1, \ldots, m, \text{ where } \alpha_1 := \alpha, \ldots, \alpha_m \text{ are elements of our fixed algebraic closure}, \\ \alpha_i \neq \alpha_j \text{ for } i \neq j, \\ \alpha_j = \sum_{i=0}^{m-1} c_{i,j} \alpha_1^i \text{ for some } c_{i,j} \in F, \\ \sigma_j(\alpha_1) = \alpha_j = \sum_{i=0}^{m-1} c_{i,j} \alpha_1^i, \\ \sigma_j \circ \sigma_i = \sigma_k, \text{ where the result of the composition is taken from the multiplication table of } G \rtimes_\phi H. \end{cases}$$

We now continue with the equations defining a Galois extension E/F with Galois group isomorphic to H and such that $E \subset L$. These are:

$$\begin{cases} g(T) = b_0 + b_1 T + \ldots + T^r \text{ with } b_0, \ldots, b_{r-1} \in F \text{ is irreducible over } F, \\ g(\beta_i) = 0, \text{ for } i = 1, \ldots, r \text{ where } \beta_1 := \beta, \ldots, \beta_r \text{ are elements of the same algebraic closure as above}, \\ \beta_i \neq \beta_j \text{ for } i \neq j, \\ \beta_j = \sum_{i=0}^{r-1} d_{i,j} \alpha_1^i \text{ for some } d_{i,j} \in F, \\ \tau_j(\beta_1) = \beta_j = \sum_{i=0}^{r-1} d_{i,j} \beta_1^i, \\ \tau_j \circ \tau_i = \tau_k, \text{ where the result of the composition is taken from the multiplication table of } H, \\ \beta_1 = \sum_{i=0}^{m-1} u_i \alpha_1^i \text{ where } u_i \in F. \end{cases}$$

We now write down the equations assuring $\mathrm{Gal}(L/E) \cong G$, namely:

$$\begin{cases} \mu_s(\beta) = \beta, \text{ for } s = 1, \ldots, \frac{m}{r}, \\ \mu_s \circ \mu_\ell = \mu_u, \text{ where the result of the composition is taken from the multiplication table of } G. \end{cases}$$

We now find restrictions for elements of $\mathrm{Gal}(L/F)$ to E. These are:

For every i, find j such that $\sigma_i(\beta) = \tau_j(\beta)$ (such a j always exists and is unique). (3.1)

We write down the requirements that the restriction map from $G \rtimes_\phi H$ to H is consistent with the given epimorphism $\pi : G \rtimes_\phi H \to H$, namely:

$$\pi(\sigma_i) = \tau_j, \text{ where } \sigma_i \text{ and } \tau_j \text{ satisfy the equality above.} \tag{3.2}$$

Finally, we note that if the field E is given as a part of the data for the problem, we simply take the polynomial g to be the irreducible polynomial of some generator of E over F.

3.2. **Translating the Inverse Automorphism Problem into the first-order language of the fields.** The Inverse Automorphism Problem (IAP), suggested to us by Arno Fehm, takes the following input:

- a base field K;
- a finite group H, say of size $|H| =: m$;
- an positive integer n which is a multiple of m.

A solution to the IAP is a finite extension L of K of degree n (not necessarily Galois over K) with automorphism group over K isomorphic to H.

We prove the following result.

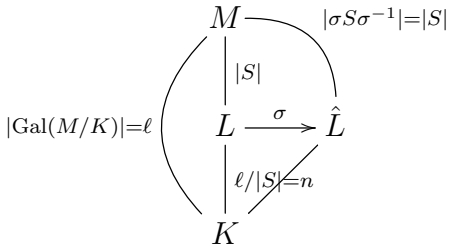
Theorem 3.1. *Let K be a field. Then, given a finite group H and a multiple n of $|H| = m$, there exists a polynomial equation over K, depending on H and K only, such that there exists a finite extension L of K degree n (not necessarily Galois over K) with automorphism group over K isomorphic to H if and only if the polynomial equation has solutions in K.*

To prove the theorem we use the following proposition.

Proposition 3.2. *Let m, n be given positive integers with $n \equiv 0 \bmod m$. Let K be a field, let M be a Galois extension of K of degree ℓ, and $n \leq \ell \leq n!$. A degree n extension L of K inside M with exactly m automorphisms exists if and only if there exists a subgroup S of $G := \mathrm{Gal}(M/K)$ with exactly n/m conjugates in G. In this case, $L = M^S$, the fixed field of S in M.*

Proof. Assume first that there exists a Galois extension M of K of degree ℓ such that $\ell \equiv 0 \bmod n$ with $\ell \leq n!$, and $G = \mathrm{Gal}(M/K)$ contains a subgroup S of G of size ℓ/n with exactly n/m conjugates in G. Then we claim that $L = M^S$ gives the desired extension.

Clearly, $[L : K] = \ell/|S| = n$. We now show that L has m automorphisms over K. Let $S_1 = S, \ldots, S_{n/m}$ be all of the distinct conjugates of S in G. If $S_i = \sigma_i S \sigma_i^{-1}$ for some $\sigma_i \in \mathrm{Gal}(M/K)$, then $\sigma_1(L) = L, \ldots, \sigma_{n/m}(L)$ are distinct conjugates of L over K in M since $S_i = \mathrm{Gal}(M/\sigma_i(L))$. Further, if $\hat{L} = \sigma(L) \neq L$ is a conjugate of L, then $\sigma S \sigma^{-1} = \hat{S} = \mathrm{Gal}(M/\hat{L})$ and $\hat{S} \neq S$ is a conjugate of S. Thus, there are exactly n/m conjugate subfields $\hat{L}$ of L in M.



Fix a $\sigma \in G$ with an induced isomorphism $L \to \hat{L}$. If $\phi \in G$ induces an automorphism of L, then $\sigma \circ \phi$ restricts to an isomorphism $L \to \hat{L}$ as well. Conversely, given any $\tau \in G$ inducing an isomorphism $L \to \hat{L}$, we get a K-automorphism of L via $\tau^{-1}|_{\hat{L}} \circ \sigma|_L : L \to L$.

Now, we know that there are $n = [L : K]$ embeddings of L into M, and by the above argument, these automorphisms can be broken up as

$$n = \#\{K\text{-automorphisms of } L\} \cdot \#\{\text{conjugate fields } \hat{L} \text{ of } L \text{ in } M\} \tag{3.3}$$

$$= \#\{K\text{-automorphisms of } L\} \cdot \#\{\text{conjugate groups } \hat{S} \text{ of } S \text{ in } G\}. \tag{3.4}$$

Therefore, we have that the number of distinct K-automorphisms of L is equal to $n/(n/m) = m$, as required.

Conversely, suppose now that $K \subseteq L \subseteq M$, where M/K is Galois, satisfies $[L : K] = n$ and L has exactly m automorphisms. Let $S = \mathrm{Gal}(M/L)$. We assume that $m < n$, since otherwise L/K is Galois, and we are in the case considered in the preceding section. Since $m < n$, the extension L/K is not Galois, and therefore $S = \mathrm{Gal}(M/L)$ is not normal. Now we use Equation (3.3) to conclude that the number of conjugates of S is n/m, as required. □

We now prove Theorem 3.1.

Proof of Theorem 3.1. The proof will consist of two steps:

(1) We will first determine all possible tables of multiplication for groups G of size ℓ less than or equal to $n!$.
(2) For each such G, we will then add equations that require it to contain a subgroup S of order m with exactly k conjugates.

We identify all m-subgroups by running through all subsets of size m of G (viewed as a set) containing $\sigma_1 = \mathrm{id}$, and for each subset we check that it satisfies group axioms (group operations, as in the previous theorem, plus inverses) and that it has exactly k conjugates. More precisely, to check that an m element subset is a subgroup, given a subset $\{\sigma_1 = \mathrm{id}, \sigma_{i_2}, \ldots, \sigma_{i_m}\}$ of G, we add the following equations:

$$\bigwedge_{j=2}^{m} \bigvee_{r=2}^{m} \big(\sigma_{i_j}\sigma_{i_r} = \sigma_1\big), \tag{3.5}$$

and

$$\bigwedge_{i,k=2}^{m} \bigvee_{r=1}^{m} \big(\sigma_{i_j}\sigma_{i_k} = \sigma_{i_r}\big), \tag{3.6}$$

where the equations are derived from the group operations of G.

Next let $S = \{\sigma_1, \sigma_{i_2}, \ldots, \sigma_{i_m}\}$ be a subgroup of G. We now check that S has exactly k conjugates. For $\tau \in G$, let $S_\tau = \{\sigma_1, \tau^{-1}\sigma_{i_2}\tau, \ldots, \tau^{-1}\sigma_{i_m}\tau\}$. Let U be the collection of all k-subsets of G containing $\sigma_1 = \mathrm{id}$. Then the requirement that S has exactly k conjugates in G can be translated into the following equations with variables being elements of G, where as above, $G = \{\sigma_1, \ldots, \sigma_\ell\}$:

$$\bigvee_{\{\sigma_1,\sigma_{j_2},\ldots,\sigma_{j_k}\}\in S} \bigwedge_{r=1}^{\ell} \bigvee_{\tau\in\{\sigma_1,\sigma_{j_2},\ldots,\sigma_{j_k}\}} \big(S_{\sigma_r} = S_\tau\big) \tag{3.7}$$

The equality $S_{\sigma_r} = S_\tau$ can be rewritten as

$$\bigwedge_{\gamma\in S_{\sigma_r}} \bigvee_{\delta\in S_\tau} (\gamma = \delta). \tag{3.8}$$

The last part of the proof of Theorem 3.1 is very similar to the proofs we have done in the earlier sections of the paper. We proceed using the steps below.

(1) We run through all possible degrees ℓ of a field M. We remind the reader that ℓ ranges between n and $n!$. This amounts to considering the sets of coefficients of irreducible polynomials generating Galois extensions of all possible degrees ℓ.
(2) For each degree ℓ we could explicitly add equations corresponding to the tables of multiplications of groups having requisite subgroups. Alternatively, we can note that once we choose an irreducible polynomial generating a Galois extension (i.e. a tuple from $I_{K,\ell}$), the Galois group is fixed via the requirement of existence of solutions to the corresponding polynomial equations, and by running through all possible coefficients of the irreducible polynomials we run through all possible Galois groups of size ℓ. In other words, solutions to the system (2.1) for each $\ell = d$ run through all possible Galois groups of size ℓ.
(3) The next step is to add equations checking the existence of a subgroup of size n with n/m conjugates. This is where we add polynomial equations corresponding to Equations (3.5)–(3.8).
(4) The final steps are to check that the automorphism group of L over K is isomorphic to the given group H. So for each subgroup S of the group G corresponding to the solutions of the equations we have written so far, we will choose an irreducible polynomial $h(t)$ of degree n over K and require that exactly m of its roots are fixed by S. Let $\beta_1, \ldots, \beta_m$ be the m roots of $h(t)$ fixed by S. As usual we identify elements of $\mathrm{Aut}(L/K)$, where L is the fixed field of S, with the roots of $h(t)$ in L. In other words $\sigma_i(\beta) = \beta_i$. Now we add polynomial equations corresponding to the table of multiplication of H to make sure that $\mathrm{Aut}(L/K) \cong H$. □

4. Appendix: IGP and existential theory of rings

4.1. **IGP and the first-order theory of rings.** Instead of considering equations with solutions in a field K we can consider solutions to our equations over some subring R of K such that K is finitely generated over R. This ring R can be chosen so that the fraction field of R is K or a finite subextension of K. The reason for considering solutions over a ring rather than a field is that, over many rings, we know all listable sets to be Diophantine. Let R be such a ring and for simplicity assume that K is the fraction field of R. Then the set of non-zero elements of R is Diophantine over R. Let N be the set of non-zero elements of R. Let $I_{R,d} \subset R^{d+1}$ be defined by

$$I_{R,d} = \{a_0, \ldots, a_{d-1}, b | b \in N, (a_0/b, , a_{d-1}/b) \in I_{K,d}\}.$$

Assuming R is a computable ring, i.e. the set of its elements is computable and the graphs of the ring operations are computable, the set N is computable and therefore listable If R is computable, then its fraction field K is also computable. Further, assuming the field has the splitting algorithm, the set $I_{K,d}$ is computable, and so is the set $I_{R,d}$. Thus, in this case $I_{R,d}$ is Diophantine over R. As we pointed out to reduce IGP of a field to the existential theory of a field, we just needed the set of coefficients of irreducible polynomials of a fixed degree to be Diophantine over the field. Thus, if we replace a field by its subring R and the field has a splitting algorithm, we can reduce IGP for the field to the existential theory of the ring.

4.2. **Rings where all listable sets are Diophantine.** In this section we present a short list of computable rings where all c.e. sets are known to be Diophantine.

4.2.1. *Subrings of number fields.* Of course the most famous ring with the property that all its listable sets are Diophantine is $\mathbb{Z}$ by the DPRM Theorem. Further, all rings of integers of number fields where $\mathbb{Z}$ has a Diophantine definition also have the property that all their listable subsets are Diophantine. The list of such rings is fairly long by now and is growing (see [Den75], [Phe88], [Shl89], [SS89], [CPZ05], [MR10], [MR18], [MP18], [GFP20]). There are also subrings of number fields bigger than rings of integers where all listable sets are Diophantine ([Shl97] [Shl00], [Shl02a], [Shl07], [Shl08] or [Shl06]).

4.2.2. *Subrings of global function fields where all listable subsets are Diophantine.* Moving to global function fields, we have by a result of J. Demeyer ([Dem07]) that all listable subsets of a polynomial ring in one variable over a finite field are Diophantine over the ring. We also know that rings of S-integers and bigger rings of function fields have Diophantine definitions of polynomial rings. So, by the same argument as for number fields, these rings also have the property that all their listable sets are Diophantine. (See [Shl93], [Shl98], [Shl02b] or [Shl06].)

4.2.3. *Subrings of function fields of characteristic 0, where all listable subsets are Diophantine.* Finally as far as function fields of characteristic 0 go, by another result of Demeyer ([Dem10]), polynomial rings in one variable over function fields over number fields also satisfy the condition that all listable sets are Diophantine over these rings. As in the case of positive characteristic, these polynomial rings are existentially definable over the rings of S-integers of function fields in one variable over number fields ([MS22]). Therefore, over these rings of S-integers all listable sets are also Diophantine.

4.3. **Fields that satisfy the conditions of Theorem 2.3.** As of now, we do not have any examples of infinite fields where all listable sets are known to be Diophantine. However, P. Dittmann ([Dit18]) proved that coefficients of irreducible polynomials of a fixed degree form Diophantine sets over all global fields. This implies that the sets $I_{K,d}$ are Diophantine over K for any global field K. We also note that, over any field, the set of non-zero elements is always Diophantine.

References

[CPZ05] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi, *Division-ample sets and diophantine problem for rings of integers*, Journal de Théorie des Nombres Bordeaux **17** (2005), 727–735. ↑4.2.1

[Dem07] Jeroen Demeyer, *Recursively enumerable sets of polynomials over a finite field are Diophantine*, Invent. Math. **170** (2007), no. 3, 655–670. MR2357505 (2009f:03053) ↑4.2.2

[Dem10] ———, *Diophantine sets of polynomials over number fields*, Proc. Amer. Math. Soc. **138** (2010), no. 8, 2715–2728. MR2644887 ↑4.2.3

[Den75] Jan Denef, *Hilbert's tenth problem for quadratic rings*, Proc. Amer. Math. Soc. **48** (1975), 214–220. ↑4.2.1

[Dit18] Philip Dittmann, *Irreducibility of polynomials over global fields is diophantine*, Compos. Math. **154** (2018), no. 4, 761–772. MR3778193 ↑4.3

[GFP20] Natalia Garcia-Fritz and Hector Pasten, *Towards Hilbert's tenth problem for rings of integers through Iwasawa theory and Heegner points*, Math. Ann. **377** (2020), no. 3-4, 989–1013. MR4126887 ↑4.2.1

[Har87] David Harbater, *Galois coverings of the arithmetic line*, Number theory (New York, 1984–1985), 1987, pp. 165–195. MR894511 ↑1

[Koe04] Jochen Koenigsmann, *The regular inverse Galois problem over non-large fields*, J. Eur. Math. Soc. (JEMS) **6** (2004), no. 4, 425–434. MR2094398 ↑1

[MP18] M. Ram Murty and Hector Pasten, *Elliptic curves, L-functions, and Hilbert's tenth problem*, J. Number Theory **182** (2018), 1–18. MR3703929 ↑4.2.1

[MR10] Barry Mazur and Karl Rubin, *Ranks of twists of elliptic curves and Hilbert's Tenth Problem*, Inventiones Mathematicae **181** (2010), 541–575. ↑4.2.1

[MR18] ———, *Diophantine stability*, Amer. J. Math. **140** (2018), no. 3, 571–616. With an appendix by Michael Larsen. MR3805014 ↑4.2.1

[MS22] Russell Miller and Alexandra Shlapentokh, *On existential definitions of c.e. subsets of rings of functions of characteristic 0*, Ann. Pure Appl. Logic **173** (2022), no. 4, Paper No. 103076, 50. MR4359365 ↑4.2.3

[Phe88] Thanases Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers*, Proceedings of American Mathematical Society **104** (1988), no. 2, 611–620. ↑4.2.1

[Pop96] Florian Pop, *Embedding problems over large fields*, Ann. of Math. (2) **144** (1996), no. 1, 1–34. MR1405941 ↑1

[Shl00] Alexandra Shlapentokh, *Defining integrality at prime sets of high density in number fields*, Duke Mathematical Journal **101** (2000), no. 1, 117–134. ↑4.2.1

[Shl02a] ———, *Defining integrality at prime sets of high density over function fields*, Monatshefte fuer Mathematik **135** (2002), 59–67. ↑4.2.1

[Shl02b] ———, *On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2*, Journal of Number Theory **95** (2002), 227–252. ↑4.2.2

[Shl06] ———, *Hilbert's tenth problem: Diophantine classes and extensions to global fields*, Cambridge University Press, 2006. ↑2, 4.2.1, 4.2.2

[Shl07] ———, *Diophantine definability and decidability in the extensions of degree 2 of totally real fields*, Journal of Algebra **313** (2007), no. 2, 846–896. ↑4.2.1

[Shl08] ———, *Elliptic curves retaining their rank in finite extensions and Hilbert's tenth problem for rings of algebraic numbers*, Trans. Amer. Math. Soc. **360** (2008), no. 7, 3541–3555. MR2386235 ↑4.2.1

[Shl89] ———, *Extension of Hilbert's tenth problem to some algebraic number fields*, Communications on Pure and Applied Mathematics **XLII** (1989), 939–962. ↑4.2.1

[Shl93] ———, *Diophantine relations between rings of S-integers of fields of algebraic functions in one variable over constant fields of positive characteristic*, J. Symbolic Logic **58** (1993), no. 1, 158–192. ↑4.2.2

[Shl97] ———, *Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator*, Inventiones Mathematicae **129** (1997), 489–507. ↑4.2.1

[Shl98] ———, *Diophantine definability over holomorphy rings of algebraic function fields with infinite number of primes allowed as poles*, International Journal of Mathematics **9** (1998), no. 8, 1041–1066. ↑4.2.2

[SS89] Harold Shapiro and Alexandra Shlapentokh, *Diophantine relations between algebraic number fields*, Communications on Pure and Applied Mathematics **XLII** (1989), 1113–1122. ↑4.2.1

The American University of Paris, 5 Boulevard de La Tour-Maubourg, 75007 Paris, France
Email address: fbalestrieri@aup.edu

The Ohio State University, Department of Mathematics, Columbus, OH 43210, USA
Email address: park.2720@osu.edu

East Carolina University, Department of Mathematics, Greenville, NC 27858, USA
Email address: shlapentokha@ecu.edu
URL: http://myweb.ecu.edu/shlapentokha/