

JOURNAL

de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux


Arno FEHM et François LEGRAND

A note on finite embedding problems with nilpotent kernel

Tome 34, n° 2 (2022), p. 549-562.

<https://doi.org/10.5802/jtnb.1215>

© Les auteurs, 2022.

 Cet article est mis à disposition selon les termes de la licence
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

A note on finite embedding problems with nilpotent kernel

par ARNO FEHM et FRANÇOIS LEGRAND

RÉSUMÉ. Le premier objectif de cet article est de combler une lacune de la littérature en montrant que, si K est un corps global et si \mathcal{S} est un ensemble fini de places de K , alors tout problème de plongement fini scindé $G \rightarrow \text{Gal}(L/K)$ sur K à noyau nilpotent admet une solution $\text{Gal}(F/K) \rightarrow G$ telle que toutes les places dans \mathcal{S} soient totalement décomposées dans F/L . Nous appliquons ensuite cela à la théorie inverse de Galois sur les corps non nécessairement commutatifs. Tout d'abord, étant donné un corps de nombres K de niveau au moins 4, nous montrons que tout groupe fini résoluble est groupe de Galois sur le corps des quaternions H_K à coefficients dans K . Ensuite, étant donné un problème de plongement fini scindé à noyau nilpotent sur un corps fini K , nous décrivons complètement les automorphismes σ de K pour lesquels le problème de plongement admet une solution sur le corps de fractions $K(T, \sigma)$ de l'anneau de polynômes $K[T, \sigma]$.

ABSTRACT. The first aim of this note is to fill a gap in the literature by proving that, given a global field K and a finite set \mathcal{S} of primes of K , every finite split embedding problem $G \rightarrow \text{Gal}(L/K)$ over K with nilpotent kernel has a solution $\text{Gal}(F/K) \rightarrow G$ such that all primes in \mathcal{S} are totally split in F/L . We then apply this to inverse Galois theory over division rings. Firstly, given a number field K of level at least 4, we show that every finite solvable group occurs as a Galois group over the division ring H_K of quaternions with coefficients in K . Secondly, given a finite split embedding problem with nilpotent kernel over a finite field K , we fully describe for which automorphisms σ of K the embedding problem acquires a solution over the skew field of fractions $K(T, \sigma)$ of the twisted polynomial ring $K[T, \sigma]$.

1. Introduction

The inverse Galois problem over a field K , a question which goes back to Hilbert and Noether, asks whether every finite group G occurs as the Galois group of a Galois field extension L/K . By Shafarevich's theorem

Manuscrit reçu le 6 janvier 2021, révisé le 24 mars 2021, accepté le 19 avril 2021.

Mathematics Subject Classification. 12F12, 12E30, 11R32, 12E15, 11R52.

Mots-clefs. Finite embedding problems, global fields, inverse Galois theory, division rings, quaternions.

Part of the present work fits into Project TIGANOCO, which is funded by the European Union within the framework of the Operational Programme ERDF/ESF 2014-2020.

(see [19, Theorem 9.6.1]), the answer to the latter question is affirmative if K is a global field and G is solvable. A refinement of the theorem, which is well-known to experts, is given by the following:

Theorem 1.1. *Let K be a global field, \mathcal{S} a finite set of primes of K , and G a finite solvable group. There exists a Galois field extension L/K of Galois group G in which every prime in \mathcal{S} is totally split.*

Theorem 1.1 is stated as (part of) an exercise on the last page of [19, Chapter IX], with the hint that the totally split condition can be guaranteed by going through the proof of Shafarevich's theorem. However, no detailed solution is provided in [19]. We point out that special cases of Theorem 1.1 were published in the literature after the first edition of [19] appeared. For example, Klüners and Malle (see [15, Theorem 6.1]) assume K is a number field and obtain the weaker conclusion that every prime in \mathcal{S} is unramified in L/K . This was later improved by Checcoli and the first author (see [4, Theorem 2.2 and Appendix A]), who prove Theorem 1.1 if K is a number field. To our knowledge, no proof of Theorem 1.1 is available in the literature. Our first aim is to explain how Theorem 1.1 can be deduced from the literature (see Section 3.1).

To that end, we will prove the following theorem (see Section 4) about finite split embedding problems with nilpotent kernels over global fields. Given a field K , recall (see, e.g., [8, §16.4]) that a *finite embedding problem over K* is an epimorphism $\alpha : G \rightarrow \text{Gal}(L/K)$, where G is a finite group and L/K a Galois field extension, and that α *splits* if there is an embedding $\alpha' : \text{Gal}(L/K) \rightarrow G$ such that $\alpha \circ \alpha' = \text{id}_{\text{Gal}(L/K)}$. A *solution to α* is an isomorphism $\beta : \text{Gal}(F/K) \rightarrow G$, where F is a Galois field extension of K containing L , such that $\alpha \circ \beta$ is the restriction map $\text{Gal}(F/K) \rightarrow \text{Gal}(L/K)$.

Theorem 1.2. *Let K be a global field, \mathcal{S} a finite set of primes of K , and $\alpha : G \rightarrow \text{Gal}(L/K)$ a finite embedding problem over K . Assume $\ker(\alpha)$ is nilpotent and α splits. Then there is a solution $\text{Gal}(F/K) \rightarrow G$ to α such that every prime $\mathfrak{P} \in \mathcal{S}$ is totally split in F/L (that is, every prime \mathfrak{Q} of L extending \mathfrak{P} is totally split in F/L).*

Theorem 1.2 refines [19, Theorem 9.6.6], the main tool to prove Shafarevich's theorem, which asserts that every finite split embedding problem with nilpotent kernel over any given global field has a solution. Some special cases of Theorem 1.2 are contained in the already mentioned works [15] and [4], other special cases can be deduced from [13, Theorem 14.3] and [14, Theorem B].

Our second aim is to contribute to inverse Galois theory over division rings. See [1, 2, 3, 6, 7, 18] for some very recent results in this area. To state our results, we recall some definitions (see Section 2.1 for more details). Firstly, for an automorphism σ of a field K , we let $K[T, \sigma]$ be the ring of

polynomials $a_0 + a_1T + \dots + a_nT^n$ with $n \geq 0$ and $a_0, \dots, a_n \in K$, whose addition is defined componentwise and multiplication fulfills $Ta = \sigma(a)T$ for $a \in K$. By $K(T, \sigma)$, we mean the unique division ring which contains $K[T, \sigma]$ and every element of which can be written as ab^{-1} with $a \in K[T, \sigma]$ and $b \in K[T, \sigma] \setminus \{0\}$. If $\sigma = \text{id}_K$, we retrieve the usual commutative polynomial ring $K[T]$ and the rational function field $K(T)$, respectively. Secondly, recall that an extension M/H of division rings is *Galois* (after Artin) if every element of M which is fixed under every automorphism of M fixing H pointwise is in H . If M/H is Galois, the automorphism group of M/H is the *Galois group* $\text{Gal}(M/H)$ of M/H .

Firstly, we combine Theorem 1.1 and the main result from [7] to get the following analogue of Shafarevich’s theorem over division rings of quaternions. Recall that the *level* of a field K is either the smallest positive integer n such that there exist $x_1, \dots, x_n \in K$ with $-1 = x_1^2 + \dots + x_n^2$ (if -1 can be written as the sum of finitely many squares in K), or ∞ (otherwise). See, e.g., [16, Chapter XI, §2] for more details.

Theorem 1.3. *Let K be a number field of level at least 4 and G a finite solvable group. Then G occurs as the Galois group of a Galois extension of the division ring $H_K = K \oplus K\mathbf{i} \oplus K\mathbf{j} \oplus K\mathbf{k}$ ($\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = \mathbf{ijk} = -1$) of quaternions with coefficients in K .*

Secondly, we combine Theorem 1.2 and results from [3], which extends the notion of finite embedding problems over fields to the situation of division rings of finite dimension over their centers. To state our result, note that every finite split embedding problem $\alpha : G \rightarrow \text{Gal}(L/K)$ with nilpotent kernel over a finite field K acquires a solution over the global field $K(T)$. That is, we compose α and the inverse of the restriction map $\text{Gal}(L(T)/K(T)) \rightarrow \text{Gal}(L/K)$, which is an isomorphism, to get a finite embedding problem $G \rightarrow \text{Gal}(L(T)/K(T))$ over $K(T)$. The latter embedding problem splits and has nilpotent kernel, and so has a solution. The next theorem fully describes the automorphisms σ of K for which α acquires a solution over the division ring $K(T, \sigma)$.

Theorem 1.4. *Let $\alpha : G \rightarrow \text{Gal}(L/K)$ be a finite split embedding problem with nilpotent kernel over a finite field K and σ an automorphism of K . Then α acquires a solution over $K(T, \sigma)$ if and only if the order of σ is coprime to $[L : K]$.*

For a precise formulation of this, see Theorem 3.1, which is more general and relaxes the split assumption. The relevant definitions on finite embedding problems over division rings will be introduced in Section 2.2.

2. Preliminaries

We collect the material about division rings, finite embedding problems, and primes of global fields that will be used in the sequel.

2.1. Division rings. In the following, a *division ring* is a non-zero (unital) ring in which all non-zero elements are invertible. Commutative division rings are nothing but *fields*.

Let L/H be an extension (i.e., $H \subseteq L$) of division rings. The group of automorphisms of L fixing H pointwise is the *automorphism group* $\text{Aut}(L/H)$ of L/H . Following Artin, we say that L/H is *Galois* if every element of L which is fixed under every element of $\text{Aut}(L/H)$ is in H . If L/H is Galois, $\text{Aut}(L/H)$ is the *Galois group* $\text{Gal}(L/H)$ of L/H .

A ring $R \neq \{0\}$ with no zero divisor is a *right Ore domain* if, for all $x, y \in R \setminus \{0\}$, there are $r, s \in R$ with $xr = ys \neq 0$. If R is a right Ore domain, there is a division ring H which contains R and every element of which can be written as ab^{-1} with $a \in R$ and $b \in R \setminus \{0\}$ (see [10, Theorem 6.8]). Moreover, such a division ring H is unique up to isomorphism (see [5, Proposition 1.3.4]).

Let H be a division ring and σ an automorphism of H . The *twisted polynomial ring* $H[T, \sigma]$ is the ring of polynomials $a_0 + a_1T + \cdots + a_nT^n$ with $n \geq 0$ and $a_0, \dots, a_n \in H$, whose addition is defined componentwise and multiplication is given by

$$\left(\sum_{i=0}^n a_i T^i \right) \cdot \left(\sum_{j=0}^m b_j T^j \right) = \sum_{k=0}^{n+m} \sum_{\ell=0}^k a_\ell \sigma^\ell(b_{k-\ell}) T^k.$$

Note that $H[T, \sigma]$ is commutative if and only if H is a field and $\sigma = \text{id}_H$. In the sense of Ore (see [20]), $H[T, \sigma]$ is the twisted polynomial ring $H[T, \sigma, \delta]$ in the variable T , where the σ -derivation δ is 0. The ring $H[T, \sigma]$ has no zero divisor, as the degree is additive on products, and is a right Ore domain (see [10, Theorem 2.6 and Corollary 6.7]). The unique division ring which contains $H[T, \sigma]$ and each element of which can be written as ab^{-1} with $a \in H[T, \sigma]$ and $b \in H[T, \sigma] \setminus \{0\}$ is then denoted by $H(T, \sigma)$. If $\sigma = \text{id}_H$, we write $H[T]$ and $H(T)$ instead of $H[T, \text{id}_H]$ and $H(T, \text{id}_H)$, respectively. If H is a field, $H(T)$ is nothing but the usual field of fractions of the commutative polynomial ring $H[T]$.

2.2. Finite embedding problems. First, let L/H and F/M be two Galois extensions of division rings with finite Galois groups, and such that $L \subseteq F$ and $H \subseteq M$. We write

$$\text{res}_{L/H}^{F/M}$$

for the restriction map $\text{Gal}(F/M) \rightarrow \text{Gal}(L/H)$ (that is, $\text{res}_{L/H}^{F/M}(\sigma)(x) = \sigma(x)$ for every $\sigma \in \text{Gal}(F/M)$ and every $x \in L$), if it is well-defined.

Unlike the commutative case, $\text{res}_{L/H}^{F/M}$ is not always well-defined. The next result (see the special case III) of [3, §3.1]) gives a practical situation where it is well-defined:

Proposition 2.1. *Let H be a division ring of finite dimension over its center. Let L/H and F/H be two Galois extensions of division rings with finite Galois groups and such that $L \subseteq F$. Then the restriction map $\text{res}_{L/H}^{F/H}$ is well-defined.*

Now, let H be a division ring of finite dimension over its center. A *finite embedding problem* over H is an epimorphism $\alpha : G \rightarrow \text{Gal}(L/H)$, where G and L/H are a finite group and a Galois extension of division rings, respectively. We say that α *splits* if there is an embedding $\alpha' : \text{Gal}(L/H) \rightarrow G$ with $\alpha \circ \alpha' = \text{id}_{\text{Gal}(L/H)}$. A *weak solution* to α is a monomorphism $\beta : \text{Gal}(F/H) \rightarrow G$, where F/H is a Galois extension of division rings with $L \subseteq F$, such that $\alpha \circ \beta$ is the restriction map $\text{res}_{L/H}^{F/H}$ (which is well-defined by Proposition 2.1). If β is an isomorphism, we say *solution* instead of weak solution.

Remark 2.2. Let L/H be a Galois extension of division rings such that $\text{Gal}(L/H)$ is finite. Then H is a field if and only if L is (see [3, lemme 2.1 and théorème 2.2]). Hence, the above terminology generalizes that of the commutative case (see Section 1).

Finally, let H be a division ring of finite dimension over its center and σ an automorphism of H of finite order. Let $\alpha : G \rightarrow \text{Gal}(L/H)$ be a finite embedding problem over H and τ an automorphism of L of finite order extending σ . Assume this condition holds:

$$(2.1) \quad L(T, \tau)/H(T, \sigma) \text{ is Galois with finite Galois group, and the restriction map } \text{res}_{L/H}^{L(T, \tau)/H(T, \sigma)} \text{ exists and is an isomorphism.}$$

Then

$$(2.2) \quad \alpha_{\sigma, \tau} = (\text{res}_{L/H}^{L(T, \tau)/H(T, \sigma)})^{-1} \circ \alpha : G \rightarrow \text{Gal}(L(T, \tau)/H(T, \sigma))$$

is a finite embedding problem over $H(T, \sigma)$, which is of finite dimension over its center (see [3, lemme 2.3]). A (σ, τ) -*geometric solution* to α is a solution to $\alpha_{\sigma, \tau}$. If $\tau = \text{id}_L$ (and so $\sigma = \text{id}_H$), we say *geometric solution* for simplicity. By Remark 2.2, if H is a field and $\text{Gal}(E/H(T)) \rightarrow G$ a geometric solution to α , then E is a field.

2.3. Primes of global fields. Recall that a field K is *global* if K is either a number field or a finitely generated field extension of a finite field with transcendence degree 1. If K is a global field of characteristic $p > 0$, there is a transcendental T such that K is a finite separable extension of $\mathbb{F}_p(T)$.

Let K be a global field. A *prime* of K is an equivalence class of non-trivial absolute values on K . If K is a number field, *non-archimedean primes* of K are in 1-to-1 correspondence with maximal ideals of the ring of integers of K , and *archimedean primes* of K are equivalence classes of non-trivial absolute values on K whose restriction to \mathbb{Q} is equivalent to the “usual” absolute value. Now, if K is global of characteristic $p > 0$, every prime of K is *non-archimedean*. If T is a transcendental as above, the set of primes of K is in bijection with the set $\mathfrak{S}_1 \cup \mathfrak{S}_2$, where \mathfrak{S}_1 is the set of maximal ideals of the integral closure of $\mathbb{F}_p[T]$ in K , and \mathfrak{S}_2 is the set of maximal ideals of the integral closure of $\mathbb{F}_p[1/T]$ in K containing $1/T$.

For a prime \mathfrak{P} of a global field K , we let $K_{\mathfrak{P}}$ denote the completion of K at \mathfrak{P} . If L/K is a Galois extension of global fields, we say that a prime \mathfrak{P} of K is *totally split in L/K* if $K_{\mathfrak{P}}$ equals the completion $L_{\mathfrak{P}'}$ of L at any prime \mathfrak{P}' of L extending \mathfrak{P} . If \mathfrak{P} is non-archimedean, then \mathfrak{P} is totally split in L/K if and only if both the ramification index and the residue degree of L/K at (the maximal ideal corresponding to) \mathfrak{P} equal 1.

If $K \subseteq L \subseteq F$ are global fields such that F/K and L/K are Galois, and if \mathfrak{P} is a prime of K , we say that \mathfrak{P} is *totally split in F/L* if any prime \mathfrak{Q} of L extending \mathfrak{P} is totally split in F/L . We also say that the completion of L at \mathfrak{Q} is the *completion of L at \mathfrak{P}* . If \mathfrak{P} is non-archimedean, the ramification index of F/L at \mathfrak{Q} and the residue field of L at \mathfrak{Q} are the *ramification index of F/L at \mathfrak{P}* and the *residue field of L at \mathfrak{P}* , respectively.

3. Proofs of Theorems 1.1, 1.3, and 1.4 under Theorem 1.2

3.1. Proof of Theorem 1.1. We proceed, as in the proof of Shafarevich’s theorem given right after [19, Proposition 9.6.9], by induction on $|G|$. Suppose Theorem 1.1 holds for any finite solvable group of order less than $|G|$. By [19, Propositions 9.6.8 and 9.6.9], there is a surjection $\varphi : N \rtimes G' \rightarrow G$, where N is the (nilpotent) Fitting subgroup of G and G' is a proper subgroup of G . By the induction hypothesis, there is a Galois field extension L/K of group G' in which all primes in \mathcal{S} are totally split. Let $\gamma : G' \rightarrow \text{Gal}(L/K)$ be an isomorphism and $\text{pr} : N \rtimes G' \rightarrow G'$ the projection on the second coordinate. Consider the finite embedding problem $\gamma \circ \text{pr} : N \rtimes G' \rightarrow \text{Gal}(L/K)$ over K ; it splits and has nilpotent kernel $N \times \{1\}$. We may then apply Theorem 1.2 to get the existence of a solution $\text{Gal}(F/K) \rightarrow N \rtimes G'$ to $\gamma \circ \text{pr}$ such that all primes in \mathcal{S} are totally split in F/L . As the same holds in L/K , all primes in \mathcal{S} are totally split in F/K .

Then $F^{\ker(\varphi)}/K$ is a Galois field extension of group G , in which all primes in \mathcal{S} are totally split.

3.2. Proof of Theorem 1.3. As the number field K has level at least 4, we may apply the Hasse–Minkowski theorem (see, e.g., [16, p. 170]) to get the existence of a prime \mathfrak{P} of K such that the completion $K_{\mathfrak{P}}$ of K at \mathfrak{P} has level at least 4. By Theorem 1.1, there exists a Galois field extension L/K of group G such that $L \subseteq K_{\mathfrak{P}}$. In particular, L has level at least 4. It then remains to apply [7, théorème 7] to conclude that the division ring H_L of quaternions with coefficients in L is a Galois extension of H_K with Galois group G .

3.3. Proof of Theorem 1.4. It is well-known that if α is a finite embedding problem with nilpotent kernel over a finite field K , then α has a geometric solution. Indeed, by the projectivity of the absolute Galois group of the finite field K (see, e.g., [8, Proposition 11.6.6] and [9, Proposition 6.1.3]), α has a weak solution. The existence of the latter and the *weak \rightarrow split reduction* (see [21, §1B) 2]) then provide a finite split embedding problem α' over K which fulfills the following two properties:

- (i) $\ker(\alpha') \cong \ker(\alpha)$,
- (ii) if α' has a geometric solution, then α has a geometric solution.

By (i) and the assumption that $\ker(\alpha)$ is nilpotent, $\ker(\alpha')$ is nilpotent. Hence, by [19, Theorem 9.6.6], the finite split embedding problem α' over the finite field K has a geometric solution. It then remains to use (ii) to get that α has a geometric solution, as claimed.

We now provide the same conclusion over more division rings of the form $K(T, \sigma)$, where σ is an automorphism of K . The next theorem generalizes Theorem 1.4.

Theorem 3.1. *Let $\alpha : G \rightarrow \text{Gal}(L/K)$ be a finite embedding problem with nilpotent kernel over a finite field K , let $\sigma \in \text{Aut}(K)$, and let d be the order of σ . Consider these three conditions:*

- (a) α has a weak solution $\gamma : \text{Gal}(L'/K) \rightarrow G$ such that d and $[L' : K]$ are coprime,
- (b) there exists $\tau \in \text{Aut}(L)$ extending σ such that α has a (σ, τ) -geometric solution,
- (c) d and $[L : K]$ are coprime.

Then we have the following four conclusions:

- (1) (a) \Rightarrow (b) \Rightarrow (c),
- (2) if α splits, then (a) \Leftrightarrow (b) \Leftrightarrow (c),
- (3) if (a) holds, then an automorphism τ of L as in (b) is unique,
- (4) if (c) fails, then (2.1) fails for every $\tau \in \text{Aut}(L)$ extending σ .

Note that the existence of some weak solution to α is automatic from the projectivity of the absolute Galois group of the finite field K .

As defined in Section 2.2, a (σ, τ) -geometric solution to a finite embedding problem α over a division ring H of finite dimension over its center is a solution to the finite embedding problem $\alpha_{\sigma, \tau}$ over $H(T, \sigma)$, which is introduced in (2.2). To make sure that $\alpha_{\sigma, \tau}$ is well-defined, we assumed (2.1). In the next lemma, of which Condition (1) is nothing but (2.1), we make (2.1) explicit, if H is a finite field.

Lemma 3.2. *Let L/K be an extension of finite fields, $\sigma \in \text{Aut}(K)$, and $\tau \in \text{Aut}(L)$ extending σ . Let d denote the order of σ . The following three conditions are equivalent:*

- (i) $L(T, \tau)/K(T, \sigma)$ is Galois with finite Galois group, and the restriction map $\text{res}_{L/K}^{L(T, \tau)/K(T, \sigma)}$ exists and is an isomorphism,
- (ii) τ has order d , and d and $[L : K]$ are coprime,
- (iii) τ has order d , and the subgroup $\langle \tau, \text{Gal}(L/K) \rangle$ of $\text{Aut}(L)$ equals $\langle \tau \rangle \times \text{Gal}(L/K)$.

Proof. The equivalence (i) \Leftrightarrow (iii) is a special case of [3, corollaire 3.4 and proposition 3.8]. It then suffices to show that (ii) and (iii) are equivalent. To that end, note that $\langle \tau \rangle$ and $\text{Gal}(L/K)$ are subgroups of the cyclic group $\text{Aut}(L)$. Hence, $\langle \tau, \text{Gal}(L/K) \rangle = \langle \tau \rangle \times \text{Gal}(L/K)$ if and only if the order of τ and $[L : K]$ are coprime, thus showing (ii) \Leftrightarrow (iii). \square

Proof of Theorem 3.1. We first prove (1) and (3) simultaneously. Since (b) \Rightarrow (c) follows from (i) \Rightarrow (ii) in Lemma 3.2, it suffices to prove (a) \Rightarrow (b) and the uniqueness of τ under (a). To that end, let $\gamma : \text{Gal}(L'/K) \rightarrow G$ be a weak solution to α such that d and $[L' : K]$ are coprime. In particular, $\gcd(d, [L' : K]) = 1$ and, consequently, there is $\tau \in \text{Aut}(L')$ of order d extending σ , and τ is necessarily unique. From (ii) \Leftrightarrow (iii) in Lemma 3.2, we get $\langle \tau, \text{Gal}(L'/K) \rangle = \langle \tau \rangle \times \text{Gal}(L'/K)$. Similarly, there is a unique $\tau' \in \text{Aut}(L')$ of order d extending σ , which actually extends τ , and, from (ii) \Leftrightarrow (iii) in Lemma 3.2, we get $\langle \tau', \text{Gal}(L'/K) \rangle = \langle \tau' \rangle \times \text{Gal}(L'/K)$. We may then apply the weak \rightarrow split reduction for finite embedding problems over division rings [3, proposition 5.3] to get the existence of a finite split embedding problem $\alpha' : G' \rightarrow \text{Gal}(L'/K)$ over K fulfilling the following two properties:

- (P1) $\ker(\alpha') \cong \ker(\alpha)$,
- (P2) if α' has a (σ, τ') -geometric solution, then α has a (σ, τ) -geometric solution.

Now, let $K^{(\sigma)}$ (resp., $L'^{\langle \tau' \rangle}$) be the fixed field of $\langle \sigma \rangle$ (resp., of $\langle \tau' \rangle$) in K (resp., in L'). As $\langle \tau', \text{Gal}(L'/K) \rangle = \langle \tau' \rangle \times \text{Gal}(L'/K)$ (see the previous paragraph), we may apply [3, lemme 3.5] to get that $L'^{\langle \tau' \rangle}/K^{(\sigma)}$ is Galois. Moreover, as the orders of σ and τ' are equal, we may apply [3, lemme 2.4] to

get that $L'^{\langle\tau'\rangle}$ and K are linearly disjoint over $K^{\langle\sigma\rangle}$, and that $L' = L'^{\langle\tau'\rangle}K$. Therefore, $\text{res}_{L'^{\langle\tau'\rangle}/K^{\langle\sigma\rangle}}^{L'/K}$ is an isomorphism. Hence,

$$\overline{\alpha'}_{\sigma,\tau'} = \text{res}_{L'^{\langle\tau'\rangle}/K^{\langle\sigma\rangle}}^{L'/K} \circ \alpha' : G' \rightarrow \text{Gal}(L'^{\langle\tau'\rangle}/K^{\langle\sigma\rangle})$$

is a finite embedding problem over $K^{\langle\sigma\rangle}$, which splits and has nilpotent kernel (by (P1) and the assumption on $\ker(\alpha)$). Theorem 1.2 then yields that $\overline{\alpha'}_{\sigma,\tau'}$ has a geometric solution $\text{Gal}(F'/K^{\langle\sigma\rangle}(T)) \rightarrow G'$ such that $F' \subseteq L'^{\langle\tau'\rangle}(T)$. Hence, by [3, lemme 4.2], α' has a (σ, τ') -geometric solution. It then remains to apply (P2) to conclude.

Now, we prove (2). To that end, assume α splits. By (1), it suffices to prove (c) \Rightarrow (a). As α splits, there is an embedding $\alpha' : \text{Gal}(L/K) \rightarrow G$ such that $\alpha \circ \alpha' = \text{id}_{\text{Gal}(L/K)}$. Then α' is a weak solution to α and, if (c) holds, then (a) holds with $\gamma = \alpha'$.

Finally, we prove (4). If (c) fails, then Condition (ii) from Lemma 3.2 fails too. Then, from (i) \Leftrightarrow (ii) in Lemma 3.2, we get that (2.1) also fails. \square

4. Proof of Theorem 1.2

Finally, we proceed to the proof of Theorem 1.2. For the convenience of the reader, we restate the theorem here:

Theorem 4.1. *Let K be a global field, \mathcal{S} a finite set of primes of K , and $\alpha : G \rightarrow \text{Gal}(L/K)$ a finite embedding problem over K . Assume $\ker(\alpha)$ is nilpotent and α splits. Then there exists a solution $\text{Gal}(F/K) \rightarrow G$ to α such that every prime $\mathfrak{P} \in \mathcal{S}$ is totally split in F/L .*

The structure of the proof is similar to that of [19, Theorem 9.6.6]. Namely, we first reduce Theorem 4.1 to the case of finite split embedding problems whose kernels are certain p -groups (see Section 4.1). The latter case is then proved in two steps, depending on whether p equals the characteristic of K (see Sections 4.2 and 4.3).

4.1. General reduction. For a prime number p and an integer $n \geq 1$, let $\mathcal{F}_p(n)$ be the free pro- p - $\text{Gal}(L/K)$ operator group of rank n as defined before [19, Proposition 9.6.3]. For $\nu = (i, j)$ with $i \geq j \geq 1$, we let $\mathcal{F}_p(n)^{(\nu)}$ denote the filtration of $\mathcal{F}_p(n)$ refining the descending p -central series as in [19, Definition 3.8.7]. Since every finite nilpotent group is a direct product of its Sylow subgroups, and each finite $\text{Gal}(L/K)$ -operator p -group is a quotient of $\mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)}$ for some n and ν (see right after [19, Theorem 9.6.6]), Theorem 1.2 reduces to proving the following statement, which

partially refines [19, Theorem 9.6.7], for every prime number p :

For each integer $n \geq 1$ and each $\nu = (i, j)$, the finite split embedding problem

$$\text{pr} : \mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K) \rightarrow \text{Gal}(L/K)$$

(4.1) *over the field K , given by the projection on the second coordinate, has a solution*

$$\gamma : \text{Gal}(F/K) \rightarrow \mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K)$$

such that every prime $\mathfrak{P} \in \mathcal{S}$ is totally split in F/L .

We break the proof into two parts. Let $p_0 \geq 0$ be the characteristic of K .

4.2. The case $p \neq p_0$. First, assume $p \neq p_0$. If all non-archimedean primes in \mathcal{S} ramify in L/K , then (4.1) follows from [19, Theorem 9.6.7 (i)]. To reduce to this case, we replace L by the compositum LL' of L and some finite Galois field extension L' of K which is linearly disjoint from L over K , and which has specified local behaviour at primes $\mathfrak{P} \in \mathcal{S}$.

Lemma 4.2. *There is a finite Galois field extension L' of K which is linearly disjoint from L over K , and which satisfies the following for every prime $\mathfrak{P} \in \mathcal{S}$:*

- (1) *if \mathfrak{P} is non-archimedean and unramified in L/K , then the completion at \mathfrak{P} of L'/K ramifies and its degree is not divisible by p ,*
- (2) *if \mathfrak{P} is either archimedean or non-archimedean and ramified in L/K , then \mathfrak{P} is totally split in L'/K .*

Proof. First, write $\mathcal{S} = \{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$. For $i = 1, \dots, r$, we let F_i denote the following Galois field extension of $K_{\mathfrak{P}_i}$:

- (a) $F_i = K_{\mathfrak{P}_i}$ if \mathfrak{P}_i is either archimedean or non-archimedean and ramified in L/K ,
- (b) F_i is a ramified quadratic field extension of $K_{\mathfrak{P}_i}$, if $p \neq 2$ and \mathfrak{P}_i is non-archimedean and unramified in L/K ,
- (c) F_i is a ramified finite Galois field extension of $K_{\mathfrak{P}_i}$ of odd degree, if $p = 2$ and \mathfrak{P}_i is non-archimedean and unramified in L/K .

We briefly explain why an extension F_i as in (c) exists: If q is the cardinality of the residue field of K at \mathfrak{P}_i , then as $q^3 - 1 = (q - 1)(q^2 + q + 1)$, there is some odd prime number p' with $q^3 \equiv 1 \pmod{p'}$. The latter congruence is a sufficient condition for the existence of a Galois extension F_i of $K_{\mathfrak{P}_i}$ with ramification index p' and residue degree 3, see [11, pp. 253-254]. In particular, $F_i/K_{\mathfrak{P}_i}$ ramifies and $[F_i : K_{\mathfrak{P}_i}] = 3p'$ is odd.

We also let \mathfrak{P}_{r+1} be a prime of K not in $\{\mathfrak{P}_1, \dots, \mathfrak{P}_r\}$ that is non-archimedean and unramified in L/K , and choose a ramified quadratic field extension F_{r+1} of $K_{\mathfrak{P}_{r+1}}$. Moreover, let n be an integer with $n \geq$

$[F_i : K_{\mathfrak{P}_i}]$ for $i = 1, \dots, r + 1$. Let $\mathfrak{P}_{r+2}, \mathfrak{P}_{r+3}, \mathfrak{P}_{r+4}$ be distinct non-archimedean primes of K not in $\{\mathfrak{P}_1, \dots, \mathfrak{P}_{r+1}\}$. For $i = r + 2, r + 3, r + 4$, let F_i be the unramified Galois field extension of $K_{\mathfrak{P}_i}$ of degree n_i , where $(n_{r+2}, n_{r+3}, n_{r+4}) = (n, n - 1, 2)$.

Now, for $i = 1, \dots, r + 4$, let $P_i(X) \in K_{\mathfrak{P}_i}[X]$ be the minimal polynomial of a primitive element of F_i over $K_{\mathfrak{P}_i}$, and let $Q_i(X) \in K_{\mathfrak{P}_i}[X]$ be a monic separable polynomial of degree n which is the product of $P_i(X)$ and $n - [F_i : K_{\mathfrak{P}_i}]$ monic degree 1 polynomials with coefficients in $K_{\mathfrak{P}_i}$. By the weak approximation theorem (see, e.g., [17, Chapter XII, Theorem 1.2]) and Krasner’s lemma (e.g., in the form of [12, Proposition 12.3]), there exists a monic separable polynomial $Q(X) \in K[X]$ of degree n which fulfills this property:

$$(4.2) \quad \begin{aligned} & \text{For } i = 1, \dots, r + 4, \text{ if } x_1, \dots, x_n \text{ are the roots of } Q(X), \text{ then} \\ & \text{the roots of } Q_i(X) \text{ can be enumerated as } y_{i,1}, \dots, y_{i,n} \text{ such that} \\ & K_{\mathfrak{P}_i}(x_j) = K_{\mathfrak{P}_i}(y_{i,j}) \text{ for } j = 1, \dots, n. \end{aligned}$$

In particular, the splitting field L' of $Q(X)$ over K satisfies $L'K_{\mathfrak{P}_i} = F_i$ for $i = 1, \dots, r + 4$. From the definition of F_i for $i = 1, \dots, r$, we get that L'/K fulfills (1) and (2) in the statement of the lemma.

Finally, we show the remaining claim that L and L' are linearly disjoint over K . For $i = r + 2, r + 3, r + 4$, the definition of $Q_i(X)$ and (4.2) yield that the Galois group G_i of $Q(X)$ over $K_{\mathfrak{P}_i}$ acts on x_1, \dots, x_n as an n_i -cycle. Since $(n_{r+2}, n_{r+3}, n_{r+4}) = (n, n - 1, 2)$ and $G_{r+2}, G_{r+3}, G_{r+4}$ are subgroups of the Galois group G of $Q(X)$ over K , we get that G contains an n -cycle, an $(n - 1)$ -cycle, and a transposition. Hence, $G = S_n$ (see, e.g., [22, Lemma 4.4.3]). Moreover, we get similarly that the Galois group of $Q(X)$ over $K_{\mathfrak{P}_{r+1}}$ acts on x_1, \dots, x_n as a transposition, in particular as an odd permutation. Since $F_{r+1}/K_{\mathfrak{P}_{r+1}}$ ramifies, we obtain that \mathfrak{P}_{r+1} ramifies already in the quadratic subfield $L'' = L'^{A_n}$ of L' and, as \mathfrak{P}_{r+1} is unramified in L/K , this implies that $L \cap L'' = K$. As every proper normal subgroup of S_n is contained in A_n , we eventually get that $L \cap L' = K$, as needed. \square

Remark 4.3. In the case $p \neq 2$, the proof shows that L'/K may be chosen to be quadratic.

Proof of (4.1) in the case $p \neq p_0$. Let $n \geq 1$ be an integer and $\nu = (i, j)$. Consider the finite split embedding problem

$$\text{pr} : \mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K) \rightarrow \text{Gal}(L/K)$$

over K , given by the projection on the second coordinate. Let L'/K be as in Lemma 4.2.

Since L and L' are linearly disjoint over K , the map

$$\text{res} : \begin{cases} \text{Gal}(LL'/K) & \rightarrow & \text{Gal}(L/K) \times \text{Gal}(L'/K) \\ \sigma & \mapsto & (\text{res}_{L/K}^{LL'/K}(\sigma), \text{res}_{L'/K}^{LL'/K}(\sigma)) \end{cases}$$

is an isomorphism. Then consider the finite embedding problem $\alpha = \text{res}^{-1} \circ (\text{pr} \times \text{id}_{\text{Gal}(L'/K)})$ over K , i.e.,

$$\alpha : \begin{cases} (\mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K)) \times \text{Gal}(L'/K) & \rightarrow \text{Gal}(LL'/K) \\ ((x, y), z) & \mapsto \text{res}^{-1}(y, z) \end{cases} ;$$

it splits and has nilpotent kernel. As all non-archimedean primes in \mathcal{S} are ramified in LL'/K and $p \neq p_0$, [19, Theorem 9.6.7 (i)] gives a solution

$$\beta : \text{Gal}(F/K) \rightarrow (\mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K)) \times \text{Gal}(L'/K)$$

to α such that every prime $\mathfrak{P} \in \mathcal{S}$ is totally split in F/LL' . Set

$$M = F^{\beta^{-1}(\{\{1\} \times \{1\} \times \text{Gal}(L'/K))}.$$

Then $L \subseteq M$ and β induces a solution $\text{Gal}(M/K) \rightarrow \mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K)$ to pr .

It remains to show that every prime $\mathfrak{P} \in \mathcal{S}$ is totally split in M/L . First, assume \mathfrak{P} is non-archimedean and ramified in L/K . Then \mathfrak{P} is unramified in L'/K . Hence, the ramification index at \mathfrak{P} of LL'/L is 1. As \mathfrak{P} is totally split in F/LL' , we get that the ramification index at \mathfrak{P} of F/L is 1, and so the same holds for M/L . Moreover, denoting residue fields at \mathfrak{P} by $\bar{\bullet}$, we have $\bar{F} = \overline{LL'} = \bar{L} \cdot \bar{L}'$ (see [8, Lemma 2.4.8] for the last equality). Since $\bar{L}' = \bar{K}$, we get that $\bar{F} = \bar{L}$, and so $\bar{M} = \bar{L}$.

Now, assume \mathfrak{P} is non-archimedean and unramified in L/K . Then p does not divide the ramification index at \mathfrak{P} of L'/K , and so does not divide that of LL'/L either. As \mathfrak{P} is totally split in F/LL' , we get that the ramification index at \mathfrak{P} of F/L is not divisible by p . Since $[M : L]$ is a power of p , the ramification index at \mathfrak{P} of M/L is then 1. The argument is similar for residue fields. Namely, with the notation from above, $[\bar{L}' : \bar{K}]$ and p are coprime, and hence the same holds for $[\overline{LL'} : \bar{L}]$ and p . As \mathfrak{P} is totally split in F/LL' , this implies that p does not divide $[\bar{F} : \bar{L}]$, and so p does not divide $[\bar{M} : \bar{L}]$ either. As $[\bar{M} : \bar{L}]$ is a power of p , we get $\bar{M} = \bar{L}$.

Finally, assume $\mathfrak{P} \in \mathcal{S}$ is archimedean and $L_{\mathfrak{P}} = \mathbb{R}$. By the definition of L' , we have $(L')_{\mathfrak{P}} = K_{\mathfrak{P}} = \mathbb{R}$, hence $(LL')_{\mathfrak{P}} = \mathbb{R}$. Since \mathfrak{P} is totally split in F/LL' , we get that $F_{\mathfrak{P}} = \mathbb{R}$. In particular, $M_{\mathfrak{P}} = \mathbb{R}$. □

4.3. The case $p = p_0$. Now, assume $p = p_0$. Given n and ν , consider the embedding

$$\alpha' : \begin{cases} \text{Gal}(L/K) & \rightarrow \mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K) \\ \sigma & \mapsto (1, \sigma) \end{cases} .$$

For a prime \mathfrak{P} of K , let

$$\psi_{\mathfrak{P}} : \text{Gal}((K_{\mathfrak{P}})^{\text{sep}}/K_{\mathfrak{P}}) \rightarrow \mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K)$$

be the composed map $\alpha' \circ \text{res}_{L/K}^{K^{\text{sep}}/K} \circ \text{res}_{K^{\text{sep}}/K}^{(K_{\mathfrak{P}})^{\text{sep}}/K_{\mathfrak{P}}}$. As $\text{pr} \circ \alpha' = \text{id}_{\text{Gal}(L/K)}$, we have $\text{pr} \circ \psi_{\mathfrak{P}} = \text{res}_{L/K}^{K^{\text{sep}}/K} \circ \text{res}_{K^{\text{sep}}/K}^{(K_{\mathfrak{P}})^{\text{sep}}/K_{\mathfrak{P}}}$. Moreover, $\mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)}$ is a p_0 -group. Hence, we may apply [14, Theorem B] to get that pr has a solution

$$\text{Gal}(F/K) \rightarrow \mathcal{F}_p(n)/\mathcal{F}_p(n)^{(\nu)} \rtimes \text{Gal}(L/K)$$

such that, for every prime $\mathfrak{P} \in \mathcal{S}$, the completion of F at \mathfrak{P} is the fixed field in $(K_{\mathfrak{P}})^{\text{sep}}$ of $\ker(\psi_{\mathfrak{P}})$. As the latter is the completion of L at \mathfrak{P} (for every prime \mathfrak{P} of K), this shows that (4.1) also holds in the case $p = p_0$, thus ending the proof of Theorem 1.2.

References

- [1] G. ALON, F. LEGRAND & E. PARAN, “Galois groups over rational function fields over skew fields”, *C. R. Math. Acad. Sci. Paris* **358** (2020), no. 7, p. 785-790.
- [2] A. BEHAJAINA, “Théorie inverse de Galois sur les corps de fractions rationnelles tordus”, *J. Pure Appl. Algebra* **225** (2021), no. 4, article no. 106549 (10 pages).
- [3] A. BEHAJAINA, B. DESCHAMPS & F. LEGRAND, “Problèmes de plongement finis sur les corps non commutatifs”, *Isr. J. Math.* **249** (2022), no. 2, p. 617-650.
- [4] S. CHECCOLI & A. FEHM, “On the Northcott property and local degrees”, *Proc. Am. Math. Soc.* **149** (2021), no. 6, p. 2403-2414.
- [5] P. M. COHN, *Skew fields. Theory of general division rings*, Encyclopedia of Mathematics and Its Applications, vol. 57, Cambridge University Press, 1995.
- [6] B. DESCHAMPS, “La méthode Behajaina appliquée aux corps de fractions tordus par une dérivation”, *Res. Number Theory* **7** (2021), no. 2, article no. 39 (11 pages).
- [7] B. DESCHAMPS & F. LEGRAND, “Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale”, *J. Pure Appl. Algebra* **224** (2020), no. 5, article no. 106240 (13 pages).
- [8] M. D. FRIED & M. JARDEN, *Field Arithmetic*, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge, vol. 11, Springer, 2008.
- [9] P. GILLE & T. SZAMUELY, *Central simple algebras and Galois cohomology*, Cambridge Studies in Advanced Mathematics, vol. 165, Cambridge University Press, 2017.
- [10] K. R. GOODEARL & R. B. WARFIELD, JR, *An Introduction to noncommutative Noetherian rings*, London Mathematical Society Student Texts, vol. 61, Cambridge University Press, 2004.
- [11] H. HASSE, *Number theory*, Grundlehren der Mathematischen Wissenschaften, vol. 229, Springer, 1980.
- [12] M. JARDEN, “Intersections of local algebraic extensions of a Hilbertian field”, in *Generators and relations in groups and geometries*, NATO ASI Series. Series C. Mathematical and Physical Sciences, vol. 333, Kluwer Academic Publishers, 1991, p. 343-405.
- [13] M. JARDEN & N. C. RAMIHARIMANANA, “Solving embedding problems with bounded ramification”, *Proc. Lond. Math. Soc.* **117** (2018), no. 1, p. 149-191.
- [14] ———, “Embedding problems with bounded ramification over global fields of positive characteristic”, *J. Lond. Math. Soc.* **100** (2019), no. 1, p. 323-340.
- [15] J. KLÜNERS & G. MALLE, “Counting nilpotent Galois extensions”, *J. Reine Angew. Math.* **572** (2004), p. 1-26.
- [16] T.-Y. LAM, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, 2005.
- [17] S. LANG, *Algebra*, Graduate Texts in Mathematics, vol. 211, Springer, 2002.
- [18] F. LEGRAND, “On finite embedding problems with abelian kernels”, *J. Algebra* **595** (2022), p. 633-659.
- [19] J. NEUKIRCH, A. SCHMIDT & K. WINGBERG, *Cohomology of number fields*, Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2008.

- [20] Ø. ORE, “Theory of non-commutative polynomials”, *Ann. Math.* **34** (1933), p. 480-508.
- [21] F. POP, “Embedding problems over large fields”, *Ann. Math.* **144** (1996), no. 1, p. 1-34.
- [22] J.-P. SERRE, *Topics in Galois Theory*, Research Notes in Mathematics, vol. 1, Jones and Bartlett Publishers, 1992.

Arno FEHM
Institut für Algebra
Fakultät Mathematik, TU Dresden
01062 Dresden, Germany
E-mail: arno.fehm@tu-dresden.de
URL: <https://tu-dresden.de/mn/math/algebra/fehm>

François LEGRAND
Normandie Univ., UNICAEN, CNRS
Laboratoire de Mathématiques Nicolas Oresme
14000 Caen, France
E-mail: francois.legrand@unicaen.fr
URL: <https://sites.google.com/site/francoislegranden/>