A NOTE ON FINITE EMBEDDING PROBLEMS
WITH NILPOTENT KERNEL

ARNO FEHM AND FRANÇOIS LEGRAND

Abstract. The first aim of this note is to fill a gap in the literature by giving a proof of the following refinement of Shafarevich’s theorem on solvable Galois groups: Given a global field $k$, a finite set $S$ of primes of $k$, and a finite solvable group $G$, there is a Galois field extension of $k$ of Galois group $G$ in which all primes in $S$ are totally split. To that end, we prove that, given a global field $k$ and a finite set $S$ 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 $S$ are totally split in $F/L$. We then use this to contribute to inverse Galois theory over division rings. Namely, given a finite split embedding problem with nilpotent kernel over a finite field $k$, we fully describe for which automorphisms $\sigma$ 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 (see [NSW08, 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, $S$ 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 $S$ is totally split.

Theorem 1.1 is stated as (part of) an exercise in [NSW08, p. 597], 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 [NSW08]. We point out that special cases of Theorem 1.1 were published in the literature after the first edition of [NSW08] appeared. For example, Klüners and Malle (see [KM04, Theorem 6.1]) assume $k$ is a number field and obtain the weaker conclusion that every prime in $S$ is unramified in $L/k$. This was later improved by Checcoli and the first author (see [CF20, 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 §3.1).

To that end, we will prove the following theorem (see §4) about finite split embedding problems with nilpotent kernels over global fields. Given a field $k$, recall (see, e.g., [FJ08 §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 $\alpha$ 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 $\alpha$ 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, $S$ a finite set of primes of $k$, and $\alpha : G \to \text{Gal}(L/k)$ a finite embedding problem over $k$. Assume $\ker(\alpha)$ is nilpotent and $\alpha$ splits. Then there is a solution $\text{Gal}(F/k) \to G$ to $\alpha$ such that every prime in $S$ is totally split in $F/L$.

Theorem 1.2 refines [NSW08 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. Let us also mention that special cases of Theorem 1.2 are contained in the already mentioned works [KM04] and [CF20].

Our second aim is to contribute to inverse Galois theory over division rings. See [DL20, ALP20, Beh21, BDL20, Des20, Leg20] for some very recent results in this area. To state our results, we recall some definitions (see §2.1 for more details). Firstly, for an automorphism $\sigma$ of a field $k$, we let $k[T, \sigma]$ be the ring of polynomials $a_0 + a_1 T + \cdots + a_n T^n$ with $n \geq 0$ and $a_0, \ldots, a_n \in k$, 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 $a, b \in k[T, \sigma]$ 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 $M/H$.

Now, every finite split embedding problem $\alpha : G \to \text{Gal}(L/k)$ with nilpotent kernel over a finite field $k$ acquires a solution over the global field $k(T)$. That is, we compose $\alpha$ and the inverse of the restriction map $\text{Gal}(L(T)/k(T)) \to \text{Gal}(L/k)$, which is an isomorphism, to get a finite embedding problem $G \to \text{Gal}(L(T)/k(T))$ over $k(T)$. The latter embedding problem splits and has nilpotent kernel, and so has a solution. We combine Theorem 1.2 and results from [BDL20], which extends the notion of finite embedding problems over fields to the situation of division rings of finite dimension over their centers, to prove the following generalization of this:

Theorem 1.3. Let $\alpha : G \to \text{Gal}(L/k)$ be a finite embedding problem over a finite field $k$, and let $\sigma$ be an automorphism of $k$. Assume $\ker(\alpha)$ is nilpotent and $\alpha$ splits. Then the following two conditions are equivalent:

1. there exists an automorphism $\tau$ of $L$ extending $\sigma$ such that
   (a) the extension $L(T, \tau)/k(T, \sigma)$ is Galois and there is a well-defined restriction map $\text{res} : \text{Gal}(L(T, \tau)/k(T, \sigma)) \to \text{Gal}(L/k)$, which is an isomorphism, and
   (b) there is an isomorphism $\beta : \text{Gal}(E/k(T, \sigma)) \to G$, where $E$ is a division ring which is Galois over $k(T, \sigma)$ and contains $L(T, \tau)$, such that $\text{res}^{-1} \circ \alpha \circ \beta$ is the well-defined restriction map $\text{Gal}(E/k(T, \sigma)) \to \text{Gal}(L(T, \tau)/k(T, \sigma))$.

2. the order of $\sigma$ and $[L : k]$ are coprime.

Moreover, if (2) holds, then an automorphism $\tau$ as in (1) is necessarily unique and, if (2) fails, then there is no automorphism $\tau$ of $L$ extending $\sigma$ such that (1)(a) holds.

See §2.2 for more on finite embedding problems over division rings, and Theorem 3.1 for a more general version of Theorem 1.3 which relaxes the split assumption.

2. Preliminaries

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

\footnote{See §2.1.3 for more on this slight abuse of terminology.}
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 [GW04 Theorem 6.8]). Moreover, such a division ring $H$ is unique up to isomorphism (see [Col95 Proposition 1.3.4]).

Let $H$ be a division ring and $\sigma$ an automorphism of $H$. The *twisted polynomial ring* $H[T, \sigma]$ is the ring of polynomials $a_0 + a_1 T + \cdots + a_n T^n$ with $n \geq 0$ and $a_0, \ldots, a_n \in H$, 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 [Ore33]), $H[T, \sigma]$ is the twisted polynomial ring $H[T, \sigma, \delta]$ in the variable $T$, where the derivation $\delta$ 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 [GW04 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 $H(T, \sigma)$. 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 $\text{Gal}(F/M) \to \text{Gal}(L/H)$ (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 [BDL20 §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 $\alpha : G \to \text{Gal}(L/H)$, where $G$ and $L/H$ are a finite group and a Galois extension of division rings, respectively. We say that $\alpha$ *splits* if there is an embedding $\alpha' : \text{Gal}(L/H) \to G$ with $\alpha \circ \alpha' = \text{id}_{\text{Gal}(L/H)}$. A *weak solution* to $\alpha$ is an isomorphism $\beta : \text{Gal}(F/H) \to G'$, where $G' \leq G$ and $F/H$ 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 $G' = G$, we say *solution* instead of weak solution.

**Remark 2.2.** Let $L$ be a Galois extension of a division ring $H$ of finite dimension over its center with $\text{Gal}(L/H)$ finite. Then $H$ is a field if and only if $L$ is (see [BDL20 lemme 2.1]). Hence, the above terminology generalizes that of the commutative case (see §1).
Finally, let $H$ be a division ring of finite dimension over its center and $\sigma$ an automorphism of $H$ of finite order. Let $\alpha : G \to \text{Gal}(L/H)$ be a finite embedding problem over $H$ and $\tau$ an automorphism of $L$ of finite order extending $\sigma$. Assume this condition holds:

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

Then

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

is a finite embedding problem over $H(T, \sigma)$, which is of finite dimension over its center (see [BDL20 lemme 2.3]). A $(\sigma, \tau)$-geometric solution to $\alpha$ 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 $\text{Gal}(E/H(T)) \to G$ a geometric solution to $\alpha$, 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, 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 and 1.3 under Theorem 1.2

#### 3.1. Proof of Theorem 1.1

We proceed, as in [NSW08 p. 596], by induction on $|G|$. Suppose Theorem 1.1 holds for any finite solvable group of order less than $|G|$. By [NSW08 Propositions 9.6.8 and 9.6.9], there is a surjection $\varphi : N \rtimes G' \to G$, 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 $S$ are totally split. Let $\gamma : G' \to \text{Gal}(L/k)$ be an isomorphism and $\text{pr} : N \rtimes G' \to G'$ the projection on the second coordinate. Consider the finite embedding problem $\gamma \circ \text{pr} : N \rtimes G' \to \text{Gal}(L/k)$ 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 $\text{Gal}(F/k) \to N \rtimes G'$ to $\gamma \circ \text{pr}$ such that all primes in $S$ are totally split in $F/L$. As the same holds in $L/k$, all primes in $S$
are totally split in $F/k$. Then $F^{\ker(\varphi)}/k$ is a Galois field extension of group $G$, in which all primes in $S$ are totally split.

3.2. Proof of Theorem 3.3. It is well-known that if $\alpha : G \rightarrow \text{Gal}(L/k)$ is a finite embedding problem with nilpotent kernel over a finite field $k$, then $\alpha$ has a geometric solution $\text{Gal}(E/k(T)) \rightarrow G$. Indeed, by the projectivity of the absolute Galois group of the finite field $k$ (see, e.g., [FJ08, Proposition 11.6.6] and [GS17, Proposition 6.1.3]), $\alpha$ has a weak solution. Hence, by the weak→split reduction (see [Pop96, §1 B 2]), we may assume that $\alpha$ splits. It then remains to apply [NSW08, Theorem 9.6.6] to get the claim.

We now provide the same conclusion over more division rings of the form $k(T, \sigma)$, where $\sigma$ is an automorphism of $k$. The next theorem generalizes Theorem 3.3.

**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 $\sigma$. Consider these three conditions:

(a) $\alpha$ 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 $\sigma$ such that $\alpha$ has a $(\sigma, \tau)$-geometric solution,
(c) $d$ and $[L : k]$ are coprime.

Then we have the following four conclusions:

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

Note that the existence of some weak solution to $\alpha$ is automatic from the projectivity of the absolute Galois group of the finite field $k$.

As defined in (2.2), a $(\sigma, \tau)$-geometric solution to a finite embedding $\alpha$ 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 $\sigma$. Let $d$ denote the order of $\sigma$. The following three conditions are equivalent:

1. $L(T, \tau)/k(T, \sigma)$ 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,
2. $\tau$ has order $d$, and $d$ and $[L : k]$ are coprime,
3. $\tau$ 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 $(1) \Leftrightarrow (3)$ is a special case of [BDL20, propositions 3.5 & 3.7]. It then suffices to show that $(2)$ and $(3)$ 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 $\tau$ and $[L : k]$ are coprime, thus showing $(2) \Leftrightarrow (3)$. □

**Proof of Theorem 3.1.** We first prove $(1)$ and $(3)$ simultaneously. Since $(b) \Rightarrow (c)$ follows from $(1) \Rightarrow (2)$ in Lemma 3.2, it suffices to prove $(a) \Rightarrow (b)$ and the uniqueness of $\tau$ under $(a)$. To that end, let $\gamma : \text{Gal}(L'/k) \rightarrow G'$ be a weak solution to $\alpha$ 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 $\sigma$, and $\tau$ is necessarily unique. From $(2) \Leftrightarrow (3)$ 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 $\sigma$, which actually extends $\tau$, and, from $(2) \Leftrightarrow (3)$ 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→split reduction for finite embedding problems over division rings [BDL20 Proposition 5.3] to get the existence of a finite embedding problem \( \alpha' : G'' \to \text{Gal}(L'/k) \) over \( k \) fulfilling the following three conditions:

(i) \( \alpha' \) splits,
(ii) \( \ker(\alpha') \cong \ker(\alpha) \),
(iii) if \( \alpha' \) has a \((\sigma, \tau')\)-geometric solution, then \( \alpha \) has a \((\sigma, \tau)\)-geometric solution.

Now, let \( k(\sigma) \) (resp., \( L(\sigma') \)) be the fixed field of \( (\sigma) \) (resp., of \( (\tau') \)) in \( k \) (resp., in \( L' \)). The extension \( L(\sigma')/k(\sigma) \) is finite Galois and \( \text{res}_{L(\sigma')/k(\sigma)}^{L'/k} \) is an isomorphism (see [BDL20 Lemme 2.7]). Hence,

\[
\overline{\sigma}_{\alpha, \alpha'} = \text{res}_{L(\sigma')/k(\sigma)}^{L'/k} \circ \alpha' : G'' \to \text{Gal}(L(\sigma')/k(\sigma))
\]

is a finite embedding problem over \( k(\alpha') \), which splits (by (i)) and has nilpotent kernel (by (ii) and the assumption on \( \ker(\alpha) \)). Theorem 1.2 then yields that \( \overline{\sigma}_{\alpha, \alpha'} \) has a geometric solution \( \text{Gal}(F'/k(\sigma)(T)) \to G'' \) such that \( F' \subseteq L(\tau')(T) \). Hence, by [BDL20 Lemme 4.4], \( \alpha' \) has a \((\sigma, \tau')\)-geometric solution. It then remains to apply (iii) to conclude.

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

Finally, we prove (4). If (c) fails, then Condition (2) from Lemma 3.2 fails too. Then, from (1) \( \Leftrightarrow \) (2) 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, \( S \) a finite set of primes of \( k \), and \( \alpha : G \to \text{Gal}(L/k) \) a finite embedding problem over \( k \). Assume \( \ker(\alpha) \) is nilpotent and \( \alpha \) splits. Then there exists a solution \( \text{Gal}(F/k) \to G \) to \( \alpha \) such that every prime \( \mathfrak{p} \in S \) is totally split in \( F/L \).

The structure of the proof is similar to that of [NSW08 Theorem 9.6.6]. Namely, we first reduce Theorem 1.1 to the case of finite split embedding problems whose kernels are certain \( p \)-groups (see 4.11). The latter case is then proved in two steps, depending on whether \( p \) equals the characteristic of \( k \) (see 4.12 and 4.13).

#### 4.1. General Reduction

For a prime number \( p \) and an integer \( n \geq 1 \), let \( F_p(n) \) be the free \( p \)-pro-\( \text{Gal}(L/k) \) operator group of rank \( n \) as defined in [NSW08 p. 578]. For \( \nu = (i, j) \) with \( i \geq j \geq 1 \), we let \( F_p(n)^{(\nu)} \) denote the filtration of \( F_p(n) \) refining the descending \( p \)-central series as in [NSW08 Chapter III, §8]. 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 \( F_p(n)/F_p(n)^{(\nu)} \) for some \( n \) and \( \nu \) (see [NSW08 p. 584]), Theorem 1.2 reduces to proving the following statement, which partially refines [NSW08 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

\[
\text{pr} : F_p(n)/F_p(n)^{(\nu)} \times \text{Gal}(L/k) \to \text{Gal}(L/k)
\]

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

\[
\gamma : \text{Gal}(F/k) \to F_p(n)/F_p(n)^{(\nu)} \times \text{Gal}(L/k)
\]

such that every prime \( \mathfrak{p} \in S \) 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 \( S \) ramify in \( L/k \), then \([4,11]\) follows from \([\text{NSW08}, \text{Theorem 9.6.7}]\). 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 \( \mathfrak{P} \in S \).

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 \( \mathfrak{P} \in S \):

(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 \( S = \{ \mathfrak{P}_1, \ldots, \mathfrak{P}_r \} \). For \( i = 1, \ldots, r \), 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 \( q^2 - 1 = (q - 1)(q^2 + q + 1) \), there is some odd prime number \( p' \) with \( q^3 \equiv 1 \mod p' \). 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 \([\text{Has80}, \text{pp. 253-254}]\). In particular, \( F_i/k_{\mathfrak{P}_i} \) ramifies and \( [F_i : k_{\mathfrak{P}_i}] = 3p' \) is odd.

We also let \( \mathfrak{P}_{i+1} \) be a prime of \( k \) not in \( \{ \mathfrak{P}_1, \ldots, \mathfrak{P}_r \} \) that is non-archimedean and unramified in \( L/k \), and choose a ramified quadratic field extension \( F_{r+1} \) of \( k_{\mathfrak{P}_{r+1}} \).

Now, let \( n \) be an integer with \( n \geq [F_i : k_{\mathfrak{P}_i}] \) for \( i = 1, \ldots, r + 1 \). For \( i = 1, \ldots, r \), let \( G_i \) be any subgroup of \( S_n \) that is isomorphic to \( \text{Gal}(F_i/k_{\mathfrak{P}_i}) \). Moreover, let \( G_{r+1} \) be any subgroup of \( S_n \) generated by a transposition, and let \( G_{r+2}, \ldots, G_s \) be the cyclic subgroups of \( S_n \). Let \( \mathfrak{P}_{r+2}, \ldots, \mathfrak{P}_s \) be distinct non-archimedean primes of \( k \) not in \( \{ \mathfrak{P}_1, \ldots, \mathfrak{P}_{r+1} \} \). For \( i = r + 2, \ldots, s \), let \( F_i \) be the unramified Galois field extension of \( k_{\mathfrak{P}_i} \) of degree \( |G_i| \).

We want to apply \([\text{Sal82}, \text{Theorem 5.9}]\) to get a Galois extension \( L'/k \) of group \( S_n \) such that, for \( i = 1, \ldots, s \), the completion of \( L'/k \) at \( \mathfrak{P}_i \) is isomorphic to \( F_i/k_{\mathfrak{P}_i} \), and the decomposition group of \( L'/k \) at some prime lying above \( \mathfrak{P}_i \) equals \( G_i \). From our choice of \( F_i/k_{\mathfrak{P}_i} \) for \( i = 1, \ldots, r \), the extension \( L'/k \) fulfills (1) and (2). Note that, to apply \([\text{Sal82}, \text{Theorem 5.9}]\), we need that \( S_n \) has a generic extension as defined in \([\text{Sal82}, \text{Definition 1.1}]\), which is guaranteed by the example at the end of \([\text{JLY02}, \text{§5.1}]\). Moreover, Condition (1) in \([\text{Sal82}, \text{Theorem 5.9}]\) that any \( G \leq S_n \) containing a conjugate of \( G_i \) for \( i = 1, \ldots, s \) equals \( S_n \) holds since, from our choice of \( G_{r+2}, \ldots, G_s \), such \( G \) intersects every conjugacy class of \( S_n \), and so equals \( S_n \) by a theorem of Jordan (see \([\text{Ser92}, \text{Lemma 4.6.1}]\)).

Finally, we show the remaining claim that \( L \) and \( L' \) are linearly disjoint over \( k \). As \( G_{r+1} \nsubseteq A_n \), the prime \( \mathfrak{P}_{r+1} \) ramifies already in the quadratic subfield \( L'' = L''A_n \) of \( L' \). Since \( \mathfrak{P}_{r+1} \) 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 and there is no need to apply \([\text{Sal82}, \text{Theorem 5.9}]\). In the case \( p = 2 \), the proof uses only the simplest instance of \([\text{Sal82}, \text{Theorem 5.9}]\). In fact, one can construct \( L' \) as the splitting field of a monic polynomial in \( k[X] \) obtained by approximating suitable local polynomials.
Proof of (1.1) in the case $p \neq p_0$. Let $n \geq 1$ be an integer and $\nu = (i,j)$. Consider the finite split embedding problem $pr : F_p(n)/F_p(n)^{(\nu)} \rtimes \text{Gal}(L/k) \to \text{Gal}(L/k)$ 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

$$
\text{res} : \left\{ \begin{array}{c}
\text{Gal}(L/k) \to \text{Gal}(L'/k) \\
\sigma \mapsto (\text{res}_{L/k}^{LL'/k}(\sigma), \text{res}_{L'/k}^{LL/k}(\sigma))
\end{array} \right.
$$

is an isomorphism. Then consider the finite embedding problem

$$
\alpha = \text{res}^{-1} \circ (\text{pr} \times \text{id}_{\text{Gal}(L'/k)}) : \left\{ \begin{array}{c}
(F_p(n) / F_p(n)^{(\nu)} \rtimes \text{Gal}(L/k))^x \times \text{Gal}(L'/k) \to \text{Gal}(L'/k) \\
((x,y), z) \mapsto \text{res}^{-1}(y, z)
\end{array} \right.
$$

over $k$; it splits and has nilpotent kernel. As all non-archimedean primes in $S$ are ramified in $LL'/k$ and $p \neq p_0$, [NSW08] Theorem 9.6.7 gives a solution

$$
\beta : \text{Gal}(F/k) \to (F_p(n) / F_p(n)^{(\nu)} \rtimes \text{Gal}(L/k)) \times \text{Gal}(L'/k)
$$

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

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

Then $L \subseteq M$ and $\beta$ induces a solution $\text{Gal}(M/k) \to F_p(n)/F_p(n)^{(\nu)} \rtimes \text{Gal}(L/k)$ to $pr$.

It remains to show that every prime $\mathfrak{p} \in S$ 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 $\overline{\mathfrak{p}}$, we have $\overline{F} = \overline{LL'} = \overline{L} \cdot \overline{L'}$ (see [FJ08] Lemma 2.4.8) for the last equality). Since $\overline{L'} = \overline{k}$, we get that $\overline{F} = \overline{L}$, and so $\overline{M} = \overline{L}$.

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 $LL'/k$ either. As $\mathfrak{p}$ is totally split in $F/LL'$, we get that the ramification index at $\mathfrak{p}$ of $F/L$ is 1 and hence the same holds for $[LL'/L]$ and $p$. As $\mathfrak{p}$ is totally split in $F/LL'$, this implies that $p$ does not divide $[\overline{L} : \overline{k}]$, and so $p$ does not divide $[\overline{M} : \overline{L}]$ either. As $[\overline{M} : \overline{L}]$ is a power of $p$, we get $\overline{M} = \overline{L}$.

Finally, assume $\mathfrak{p} \in S$ is archimedean and $k_{\mathfrak{p}} = \mathbb{R}$. 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, $M_{\mathfrak{p}} = \mathbb{R}$. \hfill\qed

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

$$
\alpha' : \left\{ \begin{array}{c}
\text{Gal}(L/k) \to F_p(n)/F_p(n)^{(\nu)} \rtimes \text{Gal}(L/k) \\
\sigma \mapsto (1, \sigma)
\end{array} \right.
$$

For a prime $\mathfrak{p}$ of $k$, set

$$
\psi_{\mathfrak{p}} = \alpha' \circ \text{res}_{k_{\mathfrak{p}}/k}^{k_{\mathfrak{p}}/k} : \text{Gal}(k_{\mathfrak{p}}^{\text{sep}}/k_{\mathfrak{p}}) \to F_p(n)/F_p(n)^{(\nu)} \rtimes \text{Gal}(L/k).
$$

Since $\text{pr} \circ \alpha' = \text{id}_{\text{Gal}(L/k)}$, we have $\text{pr} \circ \psi_{\mathfrak{p}} = \text{res}_{k_{\mathfrak{p}}/k}^{k_{\mathfrak{p}}/k} \circ \text{res}_{k_{\mathfrak{p}}^{\text{sep}}/k_{\mathfrak{p}}}^{(k_{\mathfrak{p}})^{\text{sep}}/k_{\mathfrak{p}}}$. Moreover, $F_p(n)/F_p(n)^{(\nu)}$ is a $p_0$-group. Hence, we may apply [JR19] Theorem B to get that pr has a solution

$$
\text{Gal}(F/k) \to F_p(n)/F_p(n)^{(\nu)} \rtimes \text{Gal}(L/k)
$$
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

[ALP20] Gil Alon, François Legrand, and Elad Paran. Galois groups over rational function fields over skew fields. 2020. To appear in Comptes Rendus - Mathématique.

[BDL20] Angelot Behajaina, Bruno Deschamps, and François Legrand. Problèmes de plongement finis sur les corps non commutatifs. (French). Manuscript, 2020. arXiv:2008.08333.

[Beh21] Angelot Behajaina. Théorie inverse de Galois sur les corps de fractions rationnelles tordus. (French). J. Pure Appl. Algebra, 225(4), 2021. 106549, 10 pp.

[CF20] Sara Checcoli and Arno Fehm. On the Northcott property and local degrees. 2020. To appear in Proc. Amer. Math. Soc.. arXiv:2005.10609.

[Coh95] Paul Moritz Cohn. Skew fields. Theory of general division rings. Encyclopedia of Mathematics and its Applications, 57. Cambridge University Press, Cambridge, 1995. xvi+500 pp.

[Des20] Bruno Deschamps. La méthode Behajaina appliquée aux corps de fractions tordus par une dérivation. (French). Manuscript, 2020. Available at http://perso.univ-lemans.fr/~bdesch/24.pdf.

[DL20] Bruno Deschamps and François Legrand. Le problème inverse de Galois sur les corps des fractions tordus à indéterminée centrale. (French). J. Pure Appl. Algebra, 224(5), 2020. 106240.

[FJ08] Michael D. Fried and Moshe Jarden. Field arithmetic. Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], 11. Springer-Verlag, Berlin, third edition, 2008. Revised by Jarden. xxiv+792 pp.

[GS17] Philippe Gille and Tamás Szamuely. Central simple algebras and Galois cohomology, volume 165 of Cambridge Studies in Advanced Mathematics. Cambridge University Press, Cambridge, 2017. xi+417 pp. Second edition.

[GW04] Kenneth R. Goodearl and Robert Breckenridge Warfield, Jr. An Introduction to noncommutative Noetherian rings. London Mathematical Society Student Texts, 61. Cambridge University Press, Cambridge, 2004. Second edition. xxiv+344 pp.

[Has80] Helmut Hasse. Number theory. Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], 229. Springer-Verlag, Berlin-New York, 1980. Translated from the third German edition and with a preface by Horst Günter Zimmer. xvii+638 pp.

[JLY02] Christian U. Jensen, Arne Ledet, and Noriko Yui. Generic polynomials. Constructive Aspects of the Inverse Galois Problem. Mathematical Sciences Research Institute Publications, 45. Cambridge University Press, 2002. x+258 pp.

[JR19] Moshe Jarden and Cynthia Nantsoina Ramiharimanana. Embedding problems with bounded ramification over global fields of positive characteristic. J. Lond. Math. Soc. (2), 100(1):323–340, 2019.

[KM04] Jürgen Klüners and Gunter Malle. Counting nilpotent Galois extensions. J. Reine Angew. Math., 572:1–26, 2004.

[Leg20] François Legrand. On finite embedding problems with abelian kernels. Manuscript, 2020. Available at https://sites.google.com/site/francoislegrandfr/recherche.

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg. Cohomology of number fields, volume 323 of Grundlehren der mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]. Springer-Verlag, Berlin, second edition, 2008. xvi+825 pp.

[Ore33] Oystein Ore. Theory of non-commutative polynomials. Ann. of Math. (2), 34(3):480–508, 1933.

[Pop96] Florian Pop. Embedding problems over large fields. Ann. of Math. (2), 144(1):1–34, 1996.

[Sal82] David J. Saltman. Generic Galois extensions and problems in field theory. Adv. in Math., 43(3):250–283, 1982.

[Ser92] Jean-Pierre Serre. Topics in Galois Theory, volume 1 of Research Notes in Mathematics. Jones and Bartlett Publishers, Boston, MA, 1992. Lecture notes prepared by Henri Darmon [Henri Darmon]. With a foreword by Darmon and the author. xvi+117 pp.

Email address: arno.fehm@tu-dresden.de
Email address: francois.legrand@tu-dresden.de

Institut für Algebra, Fachrichtung Mathematik, TU Dresden, 01062 Dresden, Germany