Reverse Mathematics and Algebraic Field Extensions

François G. Dorais, Jeffry Hirst, and Paul Shafer

September 3, 2012

Abstract

This paper analyzes theorems about algebraic field extensions using the techniques of reverse mathematics. In section §2, we show that WKL_0 is equivalent to the ability to extend F-automorphisms of field extensions to automorphisms of $\overline{F}$, the algebraic closure of F. Section §3 explores finitary conditions for embeddability. Normal and Galois extensions are discussed in section §4, and the Galois correspondence theorems for infinite field extensions are treated in section §5.

Reverse mathematics is a foundational program in which mathematical theorems are analyzed using a hierarchy of subsystems of second order arithmetic. This paper uses three such subsystems. The base system RCA_0 includes Σ^0_1-IND (induction for Σ^0_1 formulas) and set comprehension for Δ^0_1 definable subsets of $\mathbb{N}$. The stronger system WKL_0 appends König's theorem restricted to $\{0,1\}$-trees. The even stronger system ACA_0 adds comprehension for arithmetically definable subsets of $\mathbb{N}$. For a detailed formulation of these subsystems and related analysis of many mathematical theorems, see Simpson's book [16].

Reverse mathematics of countable algebra, including topics from group theory, ring theory, and field theory, can be found in the paper of Friedman, Simpson, and Smith [4]. Further discussion appears throughout Simpson's book [16]. A field is a set of natural numbers with operations and constants satisfying the field axioms. Field embeddings and isomorphisms can be defined as sets of (codes for) ordered pairs of field elements. Polynomials can be encoded by finite strings of coefficients, so polynomial rings are sets of (codes for) finite strings, with related ring operations. For details pertaining to any of these definitions, see either of the references above.

Our study of fields begins in the next section with the definition of an algebraic field extension. To simplify the exposition in sections §1 through §3, we restrict our discussion to characteristic 0 fields. Consequently, in these sections all irreducible polynomials are separable. We indicate how to extend results of earlier sections to fields of other characteristics in section §6.

1 Isomorphism of algebraic closures

Our definition of an algebraic extension extends the definition of algebraic closure in Simpson's book [16, Definition II.9.2]. The definition uses the following notational shorthand. Given a field F, $a \in F$, $f(x) = \sum_{i \in I} c_i x^i$ a polynomial in $F[x]$, and φ a field embedding of F, we write $\varphi(f) = \sum_{i \in I} \varphi(c_i) x^i$ and $\varphi(f)(a) = \sum_{i \in I} \varphi(c_i) a^i$.

Definition 1. (RCA_0) An *algebraic extension* of a countable field F is a pair $\langle K, \varphi \rangle$ where K is a countable field, φ is an embedding of F into K, and for every $a \in K$ there is a nonzero $f(x) \in F[x]$ such that $\varphi(f)(a) = 0$. When appropriate, we drop the mention of φ and denote the extension by K alone.

If K is an algebraic extension of F that is algebraically closed, we say K is an *algebraic closure* of F, and often write $\overline{F}$ for K.

RCA_0 can prove the existence of algebraic closures, as shown in Theorem 2.5 of Friedman, Simpson, and Smith [4]. However, the notation $\overline{F}$ in the preceding definition is somewhat misleading, since RCA_0 does not prove the uniqueness of algebraic closures up to isomorphism. To be specific, Theorem 3.3 of Friedman, Simpson, and Smith [4] shows that the statement "for every field F, the algebraic closure of F is unique up to isomorphism" is equivalent to WKL_0. As for other algebraic extensions, we often drop φ and simply denote an algebraic closure by $\overline{F}$.

In order to describe the images of fields under embeddings, Friedman, Simpson, and Smith [4] introduce the notion of a Σ^0_1-subfield.

Definition 2. (RCA_0) Suppose K is a countable field. A Σ^0_1 formula $\theta(x)$ defines a Σ^0_1-subfield of K if

1. $\forall x(\theta(x) \to x \in K)$,
2. $\theta(0_K)$ and $\theta(1_K)$ (where 0_K and 1_K are the additive and multiplicative identities of K), and
3. $\forall x \forall y((\theta(x) \wedge \theta(y)) \to (\theta(x+y) \wedge \theta(x-y) \wedge \theta(x \cdot y) \wedge \theta(x/y)))$.

Additionally, if $\langle K, \varphi \rangle$ is an algebraic extension of F and $\theta(\varphi(x))$ for all $x \in F$, we say $\theta(x)$ defines a Σ^0_1-F-subfield of K.

As noted by Friedman, Simpson, and Smith [4], RCA_0 proves that every Σ^0_1-subfield is the isomorphic image of some field. The following transport of structure lemma shows that every Σ^0_1-F-subfield of an algebraic extension of F is the isomorphic image of some algebraic extension of F. The lemma simplifies the construction of a wide variety of useful field extensions in RCA_0.

Lemma 3. (RCA_0) *If $\langle K, \varphi\rangle$ is an algebraic extension of F and $\theta(x)$ defines a Σ^0_1-F-subfield of K, then there is an algebraic extension $\langle G, \psi\rangle$ of F and an embedding τ of G into K such that*

1. $\forall x \in F(\varphi(x) = \tau(\psi(x)))$, *and*
2. $\forall x \in K(\theta(x) \leftrightarrow \exists y \in G(\tau(y) = x))$.

Proof. If the subfield defined by θ is finite, then the theorem is trivial. Let $\langle K, \varphi\rangle$ be an algebraic extension of F and suppose θ defines an infinite Σ^0_1-F-subfield of K. Since θ is a Σ^0_1 formula, RCA_0 proves the existence of an injective function $\tau : \mathbb{N} \to K$ that enumerates all those elements of K for which θ holds. Without loss of generality, we may assume that $\tau(0) = 0_K$ and $\tau(1) = 1_K$. Define field operations $+$ and $\cdot$ on $\mathbb{N}$ by $i + j = \tau^{-1}(\tau(i) + \tau(j))$ and $i \cdot j = \tau^{-1}(\tau(i) \cdot \tau(j))$. Let G denote $\mathbb{N}$ with these operations. Define $\psi : F \to G$ by letting $\psi(x) = \tau^{-1}(\varphi(x))$ for each $x \in F$. Since θ defines a Σ^0_1-F-subfield of K, RCA_0 proves that ψ and the field operations of G all exist and are all total. Routine verifications show that $\langle G, \psi\rangle$ and τ satisfy the conclusions of the theorem. □

In later constructions, it is convenient to have ready access to familiar field extensions of $\mathbb{Q}$. Working in RCA_0, we can fix a representation of $\mathbb{Q}$, for example that in Theorem II.4.2 of Simpson [16]. By Theorem 2.5 of Friedman, Simpson, and Smith [4], we can find $\overline{\mathbb{Q}}$, an algebraic closure of $\mathbb{Q}$. As a concrete example of a specific extension, we can locate the first element of $\overline{\mathbb{Q}}$ satisfying $x^2 - 2 = 0$, and denote it by $\sqrt{2}$. The collection of quotients of terms of the form $q_0 + q_1\sqrt{2}$ with $q_0, q_1 \in \mathbb{Q}$ and nonzero denominators is a Σ^0_1-subfield of $\overline{\mathbb{Q}}$. By Lemma 3, RCA_0 proves that there is an algebraic extension of $\mathbb{Q}$ that is isomorphic to this Σ^0_1-subfield; we denote it by $\mathbb{Q}(\sqrt{2})$. In the minimal model of RCA_0 consisting of ω and the computable sets, this field is a computable presentation of $\mathbb{Q}(\sqrt{2})$; in this case, an algebraist might say it *is* $\mathbb{Q}(\sqrt{2})$. Similarly, for any sequence $\langle \alpha_i \mid i \in \mathbb{N}\rangle$ of elements in $\overline{\mathbb{Q}}$, RCA_0 proves the existence of the algebraic extension $\mathbb{Q}(\alpha_i \mid i \in \mathbb{N})$. If we like, we can apply Theorem 2.12 of [4], take the algebraic closure of the real closure of $\mathbb{Q}$, and adjoin a real (or non-real) cube root of 2 to $\mathbb{Q}$ in the same fashion. Similar constructions can be carried out over other base fields.

Besides proving the existence of all these field extensions, RCA_0 can prove many useful results about them. The following two examples play an important role in the next section.

Lemma 4. (RCA_0) *Let $p_1, \ldots, p_n$ and $q_1, \ldots, q_r$ be disjoint lists of distinct primes. Then $\sqrt{q_1 \cdots q_r} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$.*

Proof. This is a formalization of the main theorem in the paper of Roth [15]. His argument is essentially an application of Π^0_1-IND, which is provable in RCA_0 by Corollary II.3.10 of Simpson [16]. For a sketch of a generalization of this result to fields other than $\mathbb{Q}$, see Lemma 33 in section §6. □

Lemma 5. (RCA_0) *Let $p_1, \ldots, p_n$ and $q_1, \ldots, q_r$ be disjoint lists of distinct primes. Then $\sqrt{q_1} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}, \sqrt{q_1 q_2}, \ldots, \sqrt{q_1 q_r})$.*

Proof. Suppose $p_1, \ldots, p_n$ and $q_1, \ldots, q_r$ are as specified and the corollary fails. Write $\sqrt{q_1}$ as a linear combination of products of elements of $\{\sqrt{p_1}, \ldots, \sqrt{p_n}, \sqrt{q_1 q_2}, \ldots, \sqrt{q_1 q_r}\}$ with coefficients in $\mathbb{Q}$. Separating the summands in which $\sqrt{q_1}$ appears an even number of times from those in which it appears an odd number of times, we may write $\sqrt{q_1} = \alpha + \beta\sqrt{q_1}$ where α and β are elements of $F = \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}, \sqrt{q_2}, \ldots, \sqrt{q_r})$ and β contains some $\sqrt{q_i}$ for $2 \leq i \leq r$. Since $\beta \neq 1$ implies $\sqrt{q_1} \in F$, contradicting Lemma 4, we must have $\beta = 1$. Since β contains some $\sqrt{q_i}$ for $2 \leq i \leq r$, we can separate and solve for $\sqrt{q_i}$, showing that $\sqrt{q_i} \in \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}, \sqrt{q_2}, \ldots, \sqrt{q_{i-1}}, \sqrt{q_{i+1}}, \ldots, \sqrt{q_r})$, again contradicting Lemma 4. Thus, the corollary must hold. $\square$

2 Extension of isomorphisms

Definition 6. (RCA_0) Suppose $\langle K, \varphi\rangle$ and $\langle J, \psi\rangle$ are algebraic extensions of F. We say K *is embeddable in J over F* (and write $K \preceq_F J$) if there is an embedding $\tau : K \to J$ such that for all $x \in F$, $\tau(\varphi(x)) = \psi(x)$. We also say that τ *fixes* F and call τ an F-embedding. If τ is also bijective, we say K *is isomorphic to J over F*, write $K \cong_F J$, and call τ an F-isomorphism.

Informally, when $\langle K, \varphi\rangle$ and $\langle J, \psi\rangle$ are algebraic extensions of F, one identifies F both with its image in K under φ and also with its image in J under ψ. Given such identifications, if τ fixes F as in the preceding definition, then F is in the domain of τ and for all $x \in F$, $\tau(x) = x$. In the formal setting, the preceding definition describes the relationship between K and J without asserting that F is a subset of K or J. Similarly in the following definition, the phrases "θ extends τ" and "θ restricts to τ" do not imply that F is a subset of K or that G is a subset of H.

Definition 7. (RCA_0) Suppose $\tau : F \to G$ is a field embedding, $\langle K, \varphi\rangle$ is an extension of F, $\langle H, \psi\rangle$ is an extension of G, and $\theta : K \to H$ satisfies $\theta(\varphi(v)) = \psi(\tau(v))$ for all $v \in F$. Then we say *θ extends τ*, *θ is an extension of τ*, *θ restricts to τ*, and *τ is a restriction of θ*.

Using the preceding definitions, we can formalize the following version of Theorem 1.8 of Hungerford [8] and prove it in RCA_0.

Theorem 8. (RCA_0) *If τ is an isomorphism from a field F onto a field G and $\alpha \in \overline{F}$ is a root of an irreducible polynomial $p(x)$ of $F[x]$, then for any root β of $\tau(p)(x)$ in $\overline{G}$, there is an isomorphism of $F(\alpha)$ onto $G(\beta)$ which extends τ. In particular, taking $F = G$, we have that if $p(x)$ is an irreducible polynomial over F with roots α and β then $F(\alpha) \cong_F F(\beta)$.*

Proof. Suppose F, G, τ, p, α, β are as in the hypothesis of the theorem, and let $\langle F(\alpha), \varphi\rangle$ and $\langle G(\beta), \psi\rangle$ be the associated algebraic extensions. In order to define a map $\theta : F(\alpha) \to G(\beta)$ extending τ, we need to characterize a typical element of $F(\alpha)$. Recall that $F(\alpha)$ is isomorphic to a Σ^0_1-F-subfield of $\overline{F}$ containing α, so let $\alpha_e \in F(\alpha)$ be the pre-image of α under this isomorphism. Define $\beta_e \in G(\beta)$ similarly. Then for every element $\gamma \in F(\alpha)$ we can uniformly find polynomials $q(x)$ and $r(x)$ in $F[x]$ such that $\gamma = \frac{\varphi(q)(\alpha_e)}{\varphi(r)(\alpha_e)}$. For any such γ, define $\theta(\gamma) = \frac{\psi(\tau(q))(\beta_e)}{\psi(\tau(r))(\beta_e)}$. Using the fact that $p(x)$ is irreducible over F, one can prove that if $\varphi(r)(\alpha_e) \neq 0$, then $\psi(\tau(r))(\beta_e) \neq 0$. Thus $\theta(x)$ is well-defined. The subset of $F(\alpha) \times G(\beta)$ defining θ exists by Δ^0_1 comprehension. Verification of the remaining properties of θ can be proved without further uses of comprehension or induction. In particular, the proof that θ is single-valued relies on the fact that $p(x)$ is irreducible over F. The proofs that θ preserves operations and is onto $G(\beta)$ rely on the fact that τ is an isomorphism of F onto G. Given that θ is single-valued and that the isomorphisms map multiplicative identities to multiplicative identities, one can prove that θ extends τ. □

Ordinarily, one can iterate Hungerford's theorem to create automorphisms of algebraic closures. Proving the existence of such extensions inherently demands greater logical strength than Hungerford's theorem alone, as shown by the following result. Other results related to iteration of Hungerford's theorem appear as Theorems 18 and 19 in section §3.

Theorem 9. (RCA_0) *The following are equivalent:*

1. WKL_0.
2. *Let F be a field with algebraic extensions K and K'. If φ is an isomorphism witnessing $K \cong_F K'$, then φ extends to an isomorphism witnessing $\overline{K} \cong_F \overline{K'}$. In the case when $\overline{K} = \overline{K'}$, φ extends to an F-automorphism of $\overline{K}$.*
3. *Let F be a field with an algebraic closure $\overline{F}$. If $\alpha \in \overline{F}$ and $\varphi : F(\alpha) \to F(\alpha)$ is an F-automorphism of $F(\alpha)$, then φ extends to an F-automorphism of $\overline{F}$.*

Furthermore, if K is a subset of $\overline{K}$ fixed by its embedding, then (2) is provable in RCA_0. *Similarly, if $F(\alpha)$ is a subset of $\overline{F}$ fixed by its embedding, then (3) is provable in* RCA_0.

Proof. We will work in RCA_0 throughout. To prove that (1) implies (2), assume WKL_0 and let F, K, K', and φ be as in the hypothesis of (2). Let $\langle \overline{K}, \tau\rangle$ and $\langle \overline{K'}, \tau'\rangle$ be algebraic closures of K and K'. Then $\langle \overline{K'}, \tau' \circ \varphi\rangle$ is an algebraic closure of K. By Theorem 3.3 of Friedman, Simpson, and Smith [4], WKL_0 implies the uniqueness of algebraic closures. (This theorem also appears as Lemma IV.5.1 in Simpson [16] in a formulation that serves our purposes particularly well.) Thus there is an isomorphism $\psi : \overline{K} \to \overline{K'}$ such that for all

$x \in K$, $\psi(\tau(x)) = \tau'(\varphi(x))$. By Definition 7, ψ extends φ. Since φ fixes F, so does ψ. Thus ψ witnesses $\overline{K} \cong_F \overline{K'}$.

Since (3) is a restriction of (2), we can complete the proof of the theorem by showing that (3) implies WKL_0. It suffices to use (3) to separate the ranges of two injections with no common values. Let f and g be injections such that for all i and j, $f(i) \neq g(j)$. Without loss of generality, we may assume that 0 is not in the range of either function. Let p_i denote the ith prime, where 2 is the 0th prime. By Lemma 3 the field $F = \mathbb{Q}(\sqrt{p_{f(i)}}, \sqrt{2p_{g(i)}} \mid i \in \mathbb{N})$ exists. By Lemma 5, $\sqrt{2} \notin F$. On the other hand, we may chose $\overline{F} = \overline{\mathbb{Q}}$, so $\sqrt{2} \in \overline{F}$. Define φ on $F(\sqrt{2})$ by $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$. Note that every value of $F(\sqrt{2})$ can be written uniquely in the form $a + b\sqrt{2}$. By (3), φ can be extended to an automorphism $\overline{\varphi}$ of $\overline{F}$ that fixes F. By recursive comprehension, the set $S = \{i \mid \overline{\varphi}(\sqrt{p_i}) = \sqrt{p_i}\}$ exists. For any i, $\sqrt{p_{f(i)}} \in F$, so $f(i) \in S$. Also, $\sqrt{2p_{g(i)}} \in F$, so $\overline{\varphi}(\sqrt{2p_{g(i)}}) = \sqrt{2p_{g(i)}} = \sqrt{2}\sqrt{p_{g(i)}}$. Since $\overline{\varphi}$ is a homomorphism, $\overline{\varphi}(\sqrt{2p_{g(i)}}) = \overline{\varphi}(\sqrt{2})\overline{\varphi}(\sqrt{p_{g(i)}}) = -\sqrt{2}\overline{\varphi}(\sqrt{p_{g(i)}})$. Thus $\overline{\varphi}(\sqrt{p_{g(i)}}) = -\sqrt{p_{g(i)}}$, so $g(i) \notin S$. Thus S is the desired separating set. This completes the proof of the equivalence results.

To prove the final two sentences of the theorem, consider item (2) and suppose K is a subset of $\overline{K}$. By Lemma 2.7 and Lemma 2.8 of Friedman, Simpson, and Smith [4], given any finite extension of K, we can uniformly find all the irreducible polynomials of the extension. In particular, we can locate the first such polynomial in some enumeration of all the polynomials in $\overline{K}[x]$. Let $\langle p_i \rangle_{i \in \mathbb{N}}$ and $\langle \langle r_{ij} \rangle_{j \leq j_i} \rangle_{i \in \mathbb{N}}$ be sequences such that for each i, p_i is the first irreducible polynomial of $K(r_{tj} \mid t < i \wedge j \leq j_t)[x]$, and $\langle r_{ij} \rangle_{j \leq j_i}$ are the roots of p_i in $\overline{K}$. Let $\langle r'_{0j} \rangle_{j \leq j_0}$ be the roots of $\varphi(p_0)$. Any k in $K(r_{0j} \mid j \leq j_0)$ can be written as $q(r_{00}, \ldots, r_{0j_0})$ for some $q \in K[x_0, \ldots, x_{j_0}]$. Define $\varphi^*(k) = \varphi(q)(r'_{00}, \ldots, r'_{0j_0})$. In general, if φ^* is defined on $K(r_{tj} \mid t < i \wedge j \leq j_t)$, let $\langle r'_{ij} \rangle_{j \leq j_i}$ be the roots of $\varphi^*(p_i)$ and for $k \in K(r_{tj} \mid t < i \wedge j \leq j_t)(r_{ij} \mid j \leq j_i)$, let $\varphi(k) = \varphi^*(q)(r'_{i0}, \ldots, r'_{ij_i})$. Routine arguments verify that φ^* witnesses $\overline{K} \cong_F \overline{K'}$ and extends φ. As noted before, item (3) is a special case of item (2), so RCA_0 also suffices to prove (3) when $F(\alpha) \subset \overline{F}$. $\square$

In section 5 of their paper [12], Metakides and Nerode construct a computably presented field F in an extension K such that the only computable F-automorphism of K is the identity. Their proof gradually constructs F while diagonalizing to avoid computable nontrivial automorphisms. The reversal of the following theorem may be viewed as the construction of a computably presented field such that every nontrivial F-automorphism of $\overline{F}$ encodes a separating set for computably inseparable computably enumerable sets.

Theorem 10. (RCA_0) *The following are equivalent:*

1. WKL_0.

2. *Let K be a proper algebraic extension of F and let $\overline{K}$ be an algebraic closure of K. Then there are at least two F-embeddings of K into $\overline{K}$.*

3. *Let $\langle K, \psi \rangle$ be an algebraic extension of F. Suppose that every irreducible polynomial over F that has a root in K splits into linear factors in K. (This is called* NOR1 *in Definition 20.) If $\alpha \in K$ and α is not in the range of ψ, then there is an F-automorphism φ of K such that $\varphi(\alpha) \neq \alpha$.*

4. *If F is not algebraically closed, then there is an F-automorphism of $\overline{F}$ that is not the identity.*

Proof. To see that (1) implies (2), assume WKL_0 and let $\langle K, \psi \rangle$ be an algebraic extension of F and let $\langle \overline{K}, \tau \rangle$ be an algebraic closure of K. Let α be an element of K that is not in the range of ψ. By the separability of F, the minimal polynomial of α in $F[x]$ has a root $\beta \in \overline{K}$ such that $\tau(\alpha) \neq \beta$. By Theorem 8, there is an isomorphism φ of $F(\alpha)$ onto $F(\beta)$. Using WKL_0, we can apply item (2) of Theorem 9 and extend φ to an F-automorphism of $\overline{K}$. Restricting this extended map to K yields an F-embedding of K into $\overline{K}$ which is distinct from τ.

Since F-embeddings must map any roots of a polynomial over F to roots of the same polynomial, adding the splitting hypothesis to (3) insures that the F-embedding of (2) is also an automorphism on K. Thus (2) implies (3). Since $\overline{F}$ satisfies the splitting hypothesis of (3) and the automorphism of (3) is not the identity, (3) implies (4). It remains only to show that (4) implies WKL_0.

As in the proof of the reversal of Theorem 9, it suffices to use (4) to separate the ranges of injections f and g satisfying $0 \neq f(s) \neq g(t) \neq 0$ for all s and t. As a notational convenience, we identify the ordered pair (i, j) with its integer code $(i + j)^2 + i$. (This coding of pairs is described in Section II.2 of Simpson's book [16].) Enumerate the polynomials in $\mathbb{Q}[x]$, with $x^2 - 2$ occurring first in the ordering. Because we will be working with finite extensions of $\mathbb{Q}$, Lemma 2.8 of Friedman, Simpson, and Smith [4] shows that RCA_0 suffices to determine which polynomials are irreducible over any of these extensions. Their Lemma 2.6 [4] proves the existence of primitive elements in RCA_0. Define sequences $\langle v_i \rangle_{i \in \mathbb{N}}$ of algebraic numbers and $\langle d_i \rangle_{i \in \mathbb{N}}$ of degrees of polynomials as follows. If $i = (j, 0)$ for some j, let $g(x)$ be the next irreducible polynomial which does not split into linear factors over $\mathbb{Q}(v_k \mid k < i)$. Let G be the splitting field of $g(x)$ over $\mathbb{Q}(v_k \mid k < i)$. Let v_i be a primitive element for G over $\mathbb{Q}(v_k \mid k < i)$, and let d_i be the degree of v_i over $\mathbb{Q}(v_k \mid k < i)$. Since $x^2 - 2$ is the first polynomial and $(0, 0) = 0$, $v_0 = \sqrt{2}$ (or some other primitive element for $\mathbb{Q}(\sqrt{2})$) and $d_i = 2$. If $i = (j, n)$ and $n > 0$, let d_j be the degree of v_j over $\mathbb{Q}$ and let p be the first prime such that $x^{d_j} - p$ is irreducible over $\mathbb{Q}(v_k \mid k < i)$. Let $v_i = \frac{p^{1/d_j}}{v_j}$ and let d_i be the degree of v_i over $\mathbb{Q}(v_k \mid k < i)$. Note that the degree of $v_j v_i$ over $\mathbb{Q}(v_k \mid k < i)$ is d_j and

$d_j \leq d_i$. By Lemma 2.6 and Lemma 2.8 of Friedman, Simpson, and Smith [4], the sequences $\langle v_i \rangle_{i \in \mathbb{N}}$ and $\langle d_i \rangle_{i \in \mathbb{N}}$ can be constructed in RCA_0. By our construction, for each i the set of products $\{\prod_{j<i} v_j^{e_j} \mid \forall j (0 \leq e_j < d_j)\}$ is a vector space basis for $\mathbb{Q}(v_k \mid k < i)$ over $\mathbb{Q}$. Also, $\{1, v_i, \ldots, v_i^{d_i - 1}\}$ is a basis for $\mathbb{Q}(v_k \mid k \leq i)$ over $\mathbb{Q}(v_k \mid k < i)$. These claims can be proved in RCA_0 by imitating the proof of Proposition 1.2 in Lang [11].

In order to apply (4), use Lemma 3 and let $F = \mathbb{Q}(v_{(i,f(j))}, v_{(i,g(j))} \cdot v_i \mid i, j \in \mathbb{N})$ and $\overline{F} = \overline{\mathbb{Q}}$. Assume for a moment that $\overline{\mathbb{Q}}$ is a nontrivial extension; details are given below. Applying (4), there is a nontrivial F-automorphism φ of $\overline{\mathbb{Q}}$. If φ fixed every v_i, then φ would be the identity on $\overline{\mathbb{Q}}$, so we can fix some i such that $\varphi(v_i) \neq v_i$. Since φ fixes F, for every $j \in \mathbb{N}$, $\varphi(v_{(i,f(j))}) = v_{(i,f(j))}$, and $\varphi(v_{(i,g(j))} \cdot v_i) = v_{(i,g(j))} \cdot v_i$. Since $\varphi(v_{(i,g(j))}) = v_{(i,g(j))}$ implies $\varphi(v_i) = v_i$, we must have $\varphi(v_{(i,g(j))}) \neq v_{(i,g(j))}$. By Δ^0_1 comprehension, the separating set $\{k \mid \varphi(v_{(i,k)}) = v_k\}$ exists.

To complete the proof of the reversal and the proof of the theorem, it remains only to show that the field F defined above is a proper subfield of $\overline{\mathbb{Q}}$. Suppose by way of contradiction that $\sqrt{2} \in F$. Since F is generated by elements of the bases we constructed, we may write $\sqrt{2}$ as a linear combination of products of generators of F. We will use j_0 and j_1 to denote components of the pair encoded by j, so $j = (j_0, j_1)$. Let

$$\sqrt{2} = \sum_{i \in I} q_i \prod_{j \in J_i} (v_{j_0} v_{(j_0, g(j_1))})^{e_j} \prod_{k \in K_i} v_{(k_0, f(k_1))}^{e_k}$$

where I, J_i, and K_i denote finite sets of integers, $0 < e_j < d_{j_0}$, and $0 < e_k < d_{(k_0, f(k_1))}$. For a sufficiently large value of i, all the products on the right are elements of the basis $B_i = \{\prod_{j<i} v_j^{e_j} \mid \forall j (0 \leq e_j < d_j)\}$ for $\mathbb{Q}(v_k \mid k < i)$ over $\mathbb{Q}$, as is $v_0 = \sqrt{2}$. By linear independence of B_i, there must be some i_0 and some $q \in \mathbb{Q}$ such that:

$$\sqrt{2} = q \prod_{j \in J_{i_0}} (v_{j_0} v_{(j_0, g(j_1))})^{e_j} \prod_{k \in K_{i_0}} v_{(k_0, f(k_1))}^{e_k}$$

Let s be the largest subscript appearing on a v in this product. Since g is nonzero, $g(j_1) > 0$, so by the definition of the pairing function we have $j_0 < (j_0, g(j_1))$. Thus s is of the form $(j_0, g(j_1))$ or $(k_0, f(k_1))$. Since the ranges of f and g are disjoint, only one of these may hold. Thus for some $0 < e < d_s$, $v_s^e \in \mathbb{Q}(v_i \mid i < s)$, contradicting our construction of F. This shows that $\sqrt{2} \notin F$ and completes the proof. $\square$

As noted before the presentation of the preceding theorem, it has an immediate corollary in computable field theory.

Corollary 11. *Given any pair of disjoint computably enumerable sets, there is a computable field F that is not algebraically closed and has a computable algebraic closure $\overline{F}$ such that any*

nontrivial F-automorphism of $\overline{F}$ computes a separating set for the computably enumerable sets. In particular, if the computably enumerable sets are computably inseparable, then any nontrivial F-automorphism is noncomputable. Additionally, every computable field F that is not algebraically closed has a computable algebraic closure $\overline{F}$, and any such closure has a nontrivial F-automorphism φ such that $\varphi' \leq_T 0'$.

Proof. To prove the first part of the corollary, imitate the construction from Theorem 10, using computable enumerations of the disjoint c.e. sets as the functions with disjoint ranges. To prove the last sentence, note that Theorem VIII.2.17 of [16] proves the existence of a model of WKL_0 consisting of only low sets. This model contains all the computable fields, an algebraic closure of each one, and by Theorem 10, the desired nontrivial automorphism. One could avoid the discussion of models by applying the Jockusch/Soare low basis theorem, Theorem 2.1 of [9], to a computably bounded computable tree constructed as in the proof of Theorem 9. □

The constructions of this section can be used to find computable $\{0,1\}$-trees whose infinite paths can be matched in a degree preserving fashion with the F-automorphisms of K for appropriately chosen fields F and K. Since the degree of K over F is either finite or countable, the number of F-automorphisms of K is either finite or the continuum. Many computable $\{0,1\}$-trees have countably many infinite paths. Thus, given an arbitrary computable $\{0,1\}$-tree, we cannot expect to be able to construct fields so that the automorphisms match the infinite paths. This is reminiscent of the argument for why Remmel's result on 3-colorings of graphs [14] does not extend to 2-colorings. It would be nice to know if some analog of Remmel's result holds in an algebraic setting.

Question 12. Is there a nice characterization of those computable $\{0,1\}$-trees whose infinite paths can be matched via a degree preserving bijection to the F-automorphisms of K for some computable extension K of a computable field F? How does this class of trees compare with similar classes for automorphisms of other computable algebraic structures?

3 Extension of embeddings

Ordinarily, given two algebraic extensions of a field F, if each can be F-embedded in the other then the extensions must be F-isomorphic. This statement can be proved in RCA_0.

Theorem 13. (RCA_0) *If $J \preceq_F K$ and $K \preceq_F J$, then $J \cong_F K$.*

Proof. Suppose $\langle J, \psi \rangle$ and $\langle K, \varphi \rangle$ are algebraic extensions of F, $\theta : J \to K$ embeds J into K, and $\tau : K \to J$ embeds K into J. We need only show that θ is onto. Fix $k_0 \in K$. Let $p \in F[x]$ be the minimal polynomial for k_0 over F and let $k_0, \ldots, k_n$ be the roots of

$\varphi(p)$ in K. Let $j_0, \ldots, j_m$ be the roots of $\psi(p)$ in J. Since θ maps $j_0, \ldots, j_m$ one-to-one into $k_0, \ldots, k_n$ and τ maps $k_0, \ldots, k_n$ one-to-one into $j_0, \ldots, j_m$, by the finite pigeonhole principle (which is provable in RCA_0) we must have that $m = n$ and k_0 is in the range of θ. $\square$

In light of Theorem 13, our next goal is to formulate existence theorems for embeddings. Of course, in any embedding $K \preceq_F J$, each element $k \in K$ must map to a root in J of its irreducible polynomial. The next two definitions describe functions that are helpful for bounding the search for acceptable images of roots. If we code finite sets as in Theorem 11.2.5 of Simpson [16], then the integer code for the set is always greater than the maximum element.

Definition 14. (RCA_0) Suppose $\langle K, \varphi \rangle$ is an algebraic extension of F. A function $r : F[x] \to K^{<\mathbb{N}}$ is a *root modulus for K over F* if for every $p \in F[x]$, $r(p)$ is (a code for) the finite set of all the roots of $\varphi(p)$ in K. By our choice of coding, $r(p)$ is also an upper bound on the roots of $\varphi(p)$ in K.

Definition 15. (RCA_0) Suppose $\langle K, \varphi \rangle$ and $\langle J, \psi \rangle$ are algebraic extensions of F. An *F embedding bound* of K into J is a function $f : K \to J^{<\mathbb{N}}$ such that for each $k \in K$, $f(k)$ contains all the roots in J of the minimal polynomial of k over F. Equivalently, for $k \in K$ and $j \in J$, if $\forall p \in F[x](\psi(p)(j) = 0 \to \varphi(p)(k) = 0)$ then $j \in f(k)$. By our choice of coding, $f(k)$ is also an upper bound on the roots in J of the minimal polynomial of k over F.

Suppose K and J are fields, f is an F embedding bound, and p is the minimal polynomial of k over F. Under our definition, $f(k)$ may contain a finite number of elements that are not roots of $\psi(p)$ in J. Also, $f(k)$ might be empty if K is not embeddable into J. The next two theorems explore relationships between root moduli and F embedding bounds. The first theorem shows that a root modulus can act as a sort of universal F embedding bound.

Lemma 16. (RCA_0) *Suppose J is an algebraic extension of F. J has a root modulus over F if and only if for every algebraic extension K of F, there is an F embedding bound of K into J. If there is an F embedding bound of $\overline{F}$ into J, then J has a root modulus.*

Proof. Suppose $\langle J, \psi \rangle$ is an algebraic extension of F. First, let r be a root modulus for J and let $\langle K, \varphi \rangle$ be an extension of F. For each $k \in K$, let p_k be the first polynomial in some enumeration of $F[x]$ such that $\varphi(p_k)(k) = 0$. Define $f : K \to J^{<\mathbb{N}}$ by $f(k) = r(p_k)$. For $k \in K$, the minimal polynomial of k over F divides p_k, so all of its roots are in $f(k)$. Thus f is an F embedding bound of K into J.

Since $\overline{F}$ is an algebraic extension of F, the remaining implication of the second sentence follows from the third sentence. To prove the third sentence, suppose f is an F embedding bound of $\overline{F}$ into J. Given any polynomial $p \in F[x]$, let $q_0, \ldots, q_n$ be a list of all the roots of $p(x)$ in $\overline{F}$, and define $r(p) = f(q_0) \cup f(q_1) \cup \cdots \cup f(q_n)$. RCA_0 proves that r exists and is a root modulus for J. $\square$

General assertions of the existence of F embedding bounds and root moduli require additional set comprehension.

Theorem 17. (RCA_0) *The following are equivalent:*

1. ACA_0.
2. *If J is an algebraic extension of F, then J has a root modulus.*
3. *If K and J are algebraic extensions of F, then there is an F embedding bound of K into J.*

Proof. Working in RCA_0, we begin by proving the equivalence of (1) and (2). To prove that (1) implies (2), suppose $\langle J, \psi \rangle$ is an algebraic extension of F. Since the finite set of all roots of $\psi(p)$ in J is uniformly arithmetically definable using p as a parameter, ACA_0 proves the existence of a root modulus for J.

To prove that (2) implies (1), let $g : \mathbb{N} \to \mathbb{N}$ be an injection. ACA_0 follows from the existence of the range of g. Let $F = \mathbb{Q}$. Let p_i denote the ith prime and consider $\mathbb{Q}(\sqrt{p_{g(i)}} \mid i \in \mathbb{N})$ as a Σ^0_1-subfield of some algebraic closure $\overline{\mathbb{Q}}$ of the rationals. We can find $\langle J, \psi \rangle$, a field extension of $\mathbb{Q}$, such that $\mathbb{Q}(\sqrt{p_{g(i)}} \mid i \in \mathbb{N})$ is an isomorphic image of J in $\overline{\mathbb{Q}}$. Apply (2) to find a root modulus for J. Note that for every natural number k,

$$\exists t(g(t) = k) \leftrightarrow r(x^2 - p_k) \neq \emptyset.$$

Since $r(x^2 - p_k)$ is a code for a finite set, $\{k \mid r(x^2 - p_k) \neq \emptyset\}$ exists by Δ^0_1-comprehension. Thus RCA_0 and (2) suffice to prove the existence of the range of g.

Now we turn to the equivalence of (1) and (3). Since (1) implies (2), by Lemma 16, (1) also implies (3). To prove that (3) implies (1), let g, $F = \mathbb{Q}$, and $\langle J, \psi \rangle$ be as in the preceding paragraph. Let $\langle K, \varphi \rangle$ be a field extension of F such that $\mathbb{Q}(\sqrt{p_i} \mid i \in \mathbb{N})$ is an isomorphic image of K in $\overline{\mathbb{Q}}$; let τ be that isomorphism. Apply (3) to find $f : K \to J^{<\mathbb{N}}$, an F embedding bound of K into J. Note that for every natural number k,

$$\exists t(g(t) = k) \leftrightarrow \exists a(a \in f(\tau^{-1}(\sqrt{p_k})) \wedge \psi(a)^2 = p_k).$$

Since $f(\tau^{-1}(\sqrt{p_k}))$ is a finite set, the range of g exists by Δ^0_1-comprehension, completing the proof. $\square$

Despite the fact that root moduli and embedding bounds are not interchangeable, they both can serve to formulate bounded versions of an embedding theorem.

Theorem 18. (RCA_0) *The following are equivalent:*

1. WKL_0.

2. *Suppose K and J are algebraic extensions of F and f_K is an F embedding bound of K into J. If $F(k) \preceq_F J$ for all $k \in K$, then $K \preceq_F J$.*

3. *Suppose K and J are algebraic extensions of F and r_J is a root modulus of J over F. If $F(k) \preceq_F J$ for all $k \in K$, then $K \preceq_F J$.*

Proof. To prove that WKL_0 implies (2), let K, J, F, and f_K be as in (2) and suppose $F(k) \preceq_F J$ for all $k \in K$. Consider the formula $\theta(\varphi, k)$ that asserts:

- φ is a subset of $K \times J$.
- φ preserves field operations.
- φ is one-to-one.
- If $k \in K$, then there is some $j \in f_K(k)$ such that $(k, j) \in \varphi$.

Because $f_K(k)$ is always finite, $\theta(\varphi, k)$ is a Π^0_1 formula. For any n, we can find a primitive element k_0 for $F(k \mid k \in K \wedge k < n)$. Any φ witnessing $F(k_0) \preceq_F J$ will also witness $\exists\varphi\forall k < n\ \theta(\varphi, k)$. By Lemma VIII.2.4.1 of Simpson [16], WKL_0 proves $\exists\varphi\forall k\ \theta(\varphi, k)$. Any φ satisying this formula F-embeds K into J.

The proof that (2) implies (3) is immediate from Lemma 16. To prove that (3) implies (1), note that given two algebraic closures of a field, RCA_0 can prove the existence of the root moduli and embeddings as in (3). The conclusion of (3) shows that each algebraic closure is embeddable in the other. By Theorem 13, the algebraic closures are F-isomorphic. This implies WKL_0 by Theorem 3.3 of Friedman, Simpson, and Smith [4]. □

The construction used by Miller and Shlapentokh [13] to prove their Proposition 4.3 can be used as an interesting alternative proof that (2) implies (1) in the preceding theorem. The fields in their construction have computable embedding bounds, but do not have computable root moduli.

In the absence of root moduli and embedding bounds, the theorem is much stronger.

Theorem 19. (RCA_0) *The following are equivalent:*

1. ACA_0.

2. *Suppose K and J are algebraic extensions of F. If $F(k) \preceq_F J$ for all $k \in K$ then $K \preceq_F J$.*

Proof. To show that ACA_0 implies (2), it suffices to note that given K and J as in (2), a root moduli for K over F is arithmetically definable. Since ACA_0 implies WKL_0, we may apply Theorem 18 to find the desired isomorphism.

To prove the converse, let $g\colon \mathbb{N} \to \mathbb{N}$ be an injection. We prove that the range of g exists. First, extend $\mathbb{Q}$ to a real closure, then extend the real closure to an algebraic closure $\overline{\mathbb{Q}}$. Since the algebraic closure is a finite separable extension of the real closure, the image of the real closure exists inside the algebraic closure by Friedman, Simpson, and Smith [4] Lemma 2.6. This allows us to distinguish the real elements of $\overline{\mathbb{Q}}$ from the complex elements of $\overline{\mathbb{Q}}$. Fix an enumeration of $\overline{\mathbb{Q}}$, let $\langle p_m \rangle_{m\in\mathbb{N}}$ enumerate the odd primes, and for each $m > 0$, let $\zeta_m \in \overline{\mathbb{Q}}$ be the first enumerated primitive m^{th} root of unity. The fields $\mathbb{Q}(\{2^{1/p_n}, \zeta_{p_n} \mid \exists m(g(m) = n)\})$, $\mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{2^{1/p_m} \mid m \in \mathbb{N}\})$, and $\mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{\zeta_{p_m} 2^{1/p_m} \mid m \in \mathbb{N}\})$ are all Σ^0_1-$\mathbb{Q}$-subfields of $\overline{\mathbb{Q}}$. By Lemma 3, let F, K, and J, be algebraic extensions of $\mathbb{Q}$ together with embeddings τ_F, τ_K, and τ_J of F, K, and J, respectively, into $\overline{\mathbb{Q}}$ such that

$$\begin{aligned}
\operatorname{ran}(\tau_F) &= \mathbb{Q}(\{2^{1/p_n}, \zeta_{p_n} \mid \exists m(g(m) = n)\});\\
\operatorname{ran}(\tau_K) &= \mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{2^{1/p_m} \mid m \in \mathbb{N}\});\\
\operatorname{ran}(\tau_J) &= \mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{\zeta_{p_m} 2^{1/p_m} \mid m \in \mathbb{N}\}).
\end{aligned}$$

The field $\mathbb{Q}(\{2^{1/p_n}, \zeta_{p_n} \mid \exists m(g(m) = n)\})$ is a subfield of both $\mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{2^{1/p_m} \mid m \in \mathbb{N}\})$ and $\mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{\zeta_{p_m} 2^{1/p_m} \mid m \in \mathbb{N}\})$, so we define maps $\psi_K\colon F \to K$ and $\psi_J\colon F \to J$ by $\psi_K = \tau_K^{-1} \circ \tau_F$ and $\psi_J = \tau_J^{-1} \circ \tau_F$ which witness that K and J are both algebraic extensions of F.

To see that $F(k) \preceq_F J$ for all $k \in K$, fix a $k \in K$ and let M be such that $\tau(k) \in \mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{2^{1/p_m} \mid m < M\})$. By bounded Π^0_1 comprehension, let $X = \{n < M \mid \neg\exists m(g(m) = n)\}$. Then $k \in F(\tau_K^{-1}(2^{1/p_n}) \mid n \in X)$, which embeds into J by extending ψ_J so that $\psi_J(2^{1/p_n}) = \zeta_{p_n} 2^{1/p_n}$ for each $n \in X$.

By (2), let φ be an F-embedding of K into J. Let X be the set of numbers n such that $\tau_J(\varphi(\tau_K^{-1}(2^{1/p_n}))) \in \overline{\mathbb{Q}}$ is real. We show that X is the range of g. Suppose $n = g(m)$ for some m. Then $\tau_F^{-1}(2^{1/p_n})$ exists and $\tau_K^{-1}(2^{1/p_n}) = \psi_K(\tau_F^{-1}(2^{1/p_n}))$. Thus $\varphi(\tau_K^{-1}(2^{1/p_n})) = \varphi(\psi_K(\tau_F^{-1}(2^{1/p_n})))$, and the fact that φ is an F-embedding means that $\varphi(\psi_K(\tau_F^{-1}(2^{1/p_n}))) = \psi_J(\tau_F^{-1}(2^{1/p_n})) = \tau_J^{-1}(2^{1/p_n})$. All together, this gives $\tau_J(\varphi(\tau_K^{-1}(2^{1/p_n}))) = \tau_J(\tau_J^{-1}(2^{1/p_n})) = 2^{1/p_n}$, which is real. On the other hand, if there is no m such that $n = g(m)$, then the only root of $x^{p_n} - 2$ in $\mathbb{Q}(\{\zeta_{p_n} \mid \exists m(g(m) = n)\} \cup \{\zeta_{p_m} 2^{1/p_m} \mid m \in \mathbb{N}\})$ is $\zeta_{p_n} 2^{1/p_n}$, and $\tau_J(\varphi(\tau_K^{-1}(2^{1/p_n})))$ must be a root of $x^{p_n} - 2$. Thus $\tau_J(\varphi(\tau_K^{-1}(2^{1/p_n}))) = \zeta_{p_n} 2^{1/p_n}$, which is not real. $\square$

4 Normal extensions and Galois extensions

Lang [11] lists three equivalent versions for the definition of a normal algebraic extension, corresponding to NOR1, NOR2, and NOR3 in the following definition. We add a fourth version to the list that makes use of the notion of restriction presented in Definition 7.

Definition 20. (RCA_0) Let $\langle K, \psi \rangle$ be an algebraic extension of F. For $1 \leq i \leq 4$, we say K is a NORi*-normal extension of* F if the condition NORi in the list below holds.

NOR1: If $p(x) \in F[x]$ is irreducible and $\psi(p)(x)$ has a root in K, then $\psi(p)(x)$ splits into linear factors in K.

NOR2: There is a sequence of polynomials over F such that the image under ψ of each polynomial in the sequence splits into linear factors in K, and K is generated by the roots of these polynomials. That is, K is the splitting field of the images under ψ of some sequence of polynomials over F.

NOR3: If $\varphi : K \to \overline{K}$ is an F-embedding, then φ is an F-automorphism of K.

NOR4: If $\varphi : \overline{K} \to \overline{K}$ is an F-automorphism, then φ restricts to an F-automorphism of K.

Lang [11] defines Galois extensions as normal separable extensions. In light of the preceding list, this yields four reasonable definitions. Before addressing the equivalence of the various definitions, we append the following definition from Hungerford [8].

Definition 21. (RCA_0) A *Galois extension* of the field F is an algebraic extension K of F such that the only elements of K that are fixed by all F-automorphisms of K are the elements of F. To parallel our NORi notation, we will say that Galois extensions have the property GAL.

Usage of the terms "normal" and "Galois" is far from standardized. Emil Artin uses "normal" for GAL in his Galois Theory [1], as does Irving Kaplansky in Fields and Rings [10]. Artin and Kaplansky do not use the term "Galois" in this sense. David Hilbert uses "Galoisscher" for NOR3 in Theorie der algebraischen Zahlenkörper [6]. Normal doesn't appear in Hilbert's index. Zariski and Samuel use "normal" for NOR1, pointing out the equivalence with NOR2, in their Commutative Algebra [19]. They only use "Galois" in the context of finite fields.

Theorem 22. (RCA_0) *For every field F and every algebraic extension K of F we have:*

$$\mathsf{GAL} \to \mathsf{NOR1} \leftrightarrow \mathsf{NOR2} \to \mathsf{NOR3} \to \mathsf{NOR4}$$

Moreover, if F is a subset of K fixed by its embedding and K is a subset of $\overline{K}$ fixed by its embedding, then the four versions of normal are equivalent. If the previous conditions hold and K is separable, then all five conditions are equivalent.

Proof. We will work in RCA_0 throughout. $\mathsf{NOR1}$ can be deduced from $\mathsf{NOR2}$ by a straightforward formalization of the proof of the last theorem in section §6.5 of Van der Waerden's text [18]. We now turn to the left to right implications.

To see that GAL implies $\mathsf{NOR1}$, let K be a Galois extension of F. Suppose $p(x)$ is a monic irreducible polynomial over F and that $\psi(p)(x)$ has a root in K. Let $\alpha_1, \ldots, \alpha_k$ be all the roots of $\psi(p)(x)$ in K. Consider the polynomial $q(x) = (x - \alpha_1) \cdots (x - \alpha_k)$. Every F-automorphism φ of K must permute the set $\{\alpha_1, \ldots, \alpha_k\}$ and thus the coefficients of $q(x)$ are all fixed by φ. Since K is a Galois extension of F, it follows that $q(x) = \psi(r)(x)$ for some $r(x) \in F[x]$. Since $r(x)$ divides $p(x)$ and $p(x)$ is monic irreducible, it follows that $p(x) = r(x)$ and hence that $\psi(p)(x)$ (which is $q(x)$) factors completely in K.

To see that $\mathsf{NOR1}$ implies $\mathsf{NOR2}$, let $\langle p_n \rangle_{n \in \mathbb{N}}$ be an enumeration of all the elements of $F[x]$ whose images under ψ are finite products of linear terms in $K[x]$. This list consists of all those polynomials over F whose images under ψ split completely in K. Since $\mathsf{NOR1}$ holds, the splitting field of the images under ψ of this sequence of polynomials is a subfield of K. Also, if $a \in K$, then the minimal polynomial of a is $\psi(p_n)$ for some n. Thus, K is equal to the splitting field of the images under ψ of the sequence of polynomials.

To see that $\mathsf{NOR2}$ implies $\mathsf{NOR3}$, suppose $\mathsf{NOR2}$ holds. Let $\langle \overline{K}, \tau \rangle$ be an algebraic closure of K, and let $\varphi : K \to \overline{K}$ be an F-embedding. If $p(x) \in F[x]$ is a defining polynomial of K and α is any root of $\psi(p)$, then there must be a root β of $\psi(p)$ such that $\varphi(\alpha) = \tau(\beta)$. Since every element of K is expressible as a sum of products of these roots, φ must map K into the image of K in $\overline{K}$ under τ. Thus we can find an automorphism $\varphi^* : K \to K$ such that for all $k \in K$, $\varphi(k) = \tau(\varphi^*(k))$. Since φ fixes F, so does the restriction φ^*.

To see that $\mathsf{NOR3}$ implies $\mathsf{NOR4}$, suppose that φ is an F-automorphism of $\overline{K}$. Then the restriction of φ to K is an F-embedding of K into $\overline{K}$. By $\mathsf{NOR3}$, this restriction is an F-automorphism of K, as desired.

To prove the penultimate sentence of the theorem, we will work in RCA_0, assume that $F \subset K \subset \overline{K}$, and prove that the negation of $\mathsf{NOR1}$ implies the negation of $\mathsf{NOR4}$. Let p be a polynomial irreducible over F that does not split in K but has a root α in K. Let β be a root of p not lying in K. By Theorem 8 there is an F-isomorphism $\varphi : F(\alpha) \to F(\beta)$. By the last sentence of Theorem 9, φ extends to an F-automorphism of $\overline{K}$. The restriction of φ to K maps α to β, so it is not an F-automorphism of K. Thus, $\mathsf{NOR4}$ fails as desired.

To prove the final sentence of the theorem, we continue working in RCA_0. Assume that $F \subset K \subset \overline{K}$ and $\mathsf{NOR4}$ holds. Suppose $\alpha \in K \setminus F$. Let p be the minimal polynomial of α over F and apply the separability of F to find a root β of p that is not equal to α. By Theorem 8 there is an F-isomorphism $\varphi : F(\alpha) \to F(\beta)$. By the last sentence of Theorem

9, φ extends to an F-automorphism of $\overline{K}$. By $\mathsf{NOR4}$, this restricts to an F-automorphism of K that moves α. So K is a Galois extension of F. $\square$

Each converse omitted from the preceding theorem is equivalent to WKL_0.

Theorem 23. (RCA_0) *The following are equivalent:*

1. WKL_0.
2. *For every field F and every algebraic extension K of F,* $\mathsf{NOR4} \to \mathsf{NOR1}$.
3. *For every field F and every algebraic extension K of F,* $\mathsf{NOR4} \to \mathsf{NOR3}$.
4. *For every field F and every algebraic extension K of F,* $\mathsf{NOR3} \to \mathsf{NOR1}$.
5. *For every field F and every separable algebraic extension K of F,* $\mathsf{NOR1} \to \mathsf{GAL}$.

In light of Theorem 22, the equivalences hold with $\mathsf{NOR1}$ *replaced by* $\mathsf{NOR2}$.

Proof. To prove that (1) implies (2), we will use WKL_0 and $\neg\mathsf{NOR1}$ to deduce $\neg\mathsf{NOR4}$. Let $\langle K, \psi\rangle$ be an algebraic extension of F. On the basis of $\neg\mathsf{NOR1}$, let $p(x)$ be an irreducible polynomial in $F[x]$ such that $\alpha \in K$ is a root of $\psi(p)(x)$ and $\psi(p)(x)$ does not split completely over K. Let $q(x)$ be a nonlinear irreducible factor of $\psi(p)(x)$ in $K[x]$, and let β be a root of $q(x)$. By Theorem 8, $F(\alpha) \cong_F F(\beta)$. Using WKL_0, we can apply Theorem 9 and extend this isomorphism to an F-automorphism of $\overline{K}$. Since this automorphism does not restrict to an automorphism of K, we have $\neg\mathsf{NOR4}$.

By Theorem 22, RCA_0 proves $\mathsf{NOR1} \to \mathsf{NOR3}$. Thus RCA_0 proves that (2) implies (3). Before dealing with (4), we will prove that (3) implies (1). Our plan is to assume the contrapositive of (3), that is that $\neg\mathsf{NOR3} \to \neg\mathsf{NOR4}$, and construct a separating set for the ranges of disjoint injections. Let f and g be disjoint injections and without loss of generality, assume that 0 is not in either of their ranges. Suppose $\overline{\mathbb{Q}}$ is an algebraic closure of a real closure of $\mathbb{Q}$ in which the positive roots and the elements $\sqrt[4]{2}$, $-\sqrt[4]{2}$, $i\sqrt[4]{2}$, and $-i\sqrt[4]{2}$ have been designated. Using the notation for primes from the reversal of Theorem 9, define $F = \mathbb{Q}(\sqrt{p_{f(i)}}, \sqrt{2p_{g(i)}} \mid i \in \mathbb{N})$ and consider $F(\sqrt[4]{2})$. RCA_0 proves that the usual F-isomorphism from $F(\sqrt[4]{2})$ to $F(i\sqrt[4]{2})$ exists and that it is an embedding of $F(\sqrt[4]{2})$ into $\overline{F}$ which is not an automorphism of $F(\sqrt[4]{2})$. Since $\neg\mathsf{NOR3}$ holds, we may apply $\neg\mathsf{NOR4}$ to find an F-automorphism of ψ of $\overline{F}$ which maps some element of $F(\sqrt[4]{2})$ to an element not in $F(\sqrt[4]{2})$. Thus $\psi(\sqrt[4]{2}) = \pm i\sqrt[4]{2}$ and so $\psi(\sqrt{2}) = -\sqrt{2}$. As in the reversal of Theorem 9, $S = \{i \mid \psi(\sqrt{p_i}) = \sqrt{p_i}\}$ is a separating set for the ranges of f and g.

Consider item (4). Since Theorem 22 shows $\mathsf{NOR3} \to \mathsf{NOR4}$ and by (2), WKL_0 implies that $\mathsf{NOR4} \to \mathsf{NOR1}$, WKL_0 implies (4). To prove the converse, we will use $\neg\mathsf{NOR1} \to \neg\mathsf{NOR3}$

to find a separating set for the ranges of disjoint injections with nonzero ranges. Let f, g, and F be as in the preceding paragraph and let $K = F(\sqrt[4]{2})$. The polynomial $x^4 - 2$ has a root in K, but $x^4 - 2$ does not split in K, since $i\sqrt[4]{2}$ is not in K. Since $\neg$NOR1 holds for F and K, by the contrapositive of (4), $\neg$NOR3 holds. Let $\psi : K \to \overline{K}$ be an F-embedding which maps some element of K outside K. Then $\psi(\sqrt[4]{2}) = \pm i\sqrt[4]{2}$, so $\psi(\sqrt{2}) = -\sqrt{2}$ and $S = \{i | \psi(\sqrt{p_i}) = \sqrt{p_i}\}$ is a separating set.

The equivalence of WKL_0 and (5) is immediate from part (3) of Theorem 10, using terminology from Definition 21. □

We conclude this section by recasting Theorem 18 using normal field extensions. The resulting formulation avoids root moduli, but is interestingly weaker than the unbounded statement in Theorem 19.

Theorem 24 (RCA_0)**.** *The following are equivalent.*

1. WKL_0.
2. *Suppose that J and K are* NOR1 *algebraic extensions of F. If $F(k) \preceq_F J$ for all $k \in K$ then $K \preceq_F J$.*

Moreover, the equivalence holds if NOR1 *is replaced by* NOR2, NOR3, *or* NOR4. *If K and J are separable extensions, then the equivalence holds if* NOR1 *is replaced by* GAL.

Proof. The proof follows from two simple observations. Given NOR1 field extensions as in (2), RCA_0 can prove the existence of F-embedding bounds of J into K and of K into J. The forward implication follows immediately from Theorem 18. The proof of the reversal of Theorem 18 also proves this reversal, since every algebraic closure of F satisfies NOR1. □

5 Galois correspondence theorems

Lemma 2.11 of Friedman, Simpson, and Smith [4] shows that Galois correspondence for field extensions of finite degree is provable in RCA_0. In this section, we analyze Galois correspondence for infinite extensions. If $\langle E, \psi \rangle$ is an algebraic extension of F and $\langle K, \varphi \rangle$ is an algebraic extension of E, then $\langle K, \varphi \circ \psi \rangle$ is an algebraic extension of F. In this case we say E is an intermediate extension between F and K. By Lemma 3, every Σ^0_1-F-subfield of K is the isomorphic image of an intermediate extension field between F and K.

Theorem 25. (RCA_0) *The following are equivalent:*

1. WKL_0

2. *If K is a Galois extension of F and E is an intermediate extension, then K is a Galois extension of E.*

Proof. By Theorem 22, if K is a Galois extension of F, then it is a $\mathsf{NOR2}$-normal extension. It is easy to see that if K is a $\mathsf{NOR2}$-normal extension of F and E is an intermediate extension, then K is necessarily a $\mathsf{NOR2}$-normal extension of E. Therefore, (1) implies (2) by Theorem 23.

The fact that (2) implies (1) follows from the reversal of Theorem 10. The field F constructed there is strictly intermediate between $\overline{\mathbb{Q}}$ and $\mathbb{Q}$. It is not hard to see that $\overline{\mathbb{Q}}$ is a Galois extension of $\mathbb{Q}$. By (2), $\overline{\mathbb{Q}}$ is a Galois extension of F, so there must be a F-automorphism of $\overline{\mathbb{Q}}$ that is not the identity. As in the proof of Theorem 10, this automorphism encodes the desired separating set. □

We now turn to the group-theoretic aspects of Galois theory. The group Sym of permutations of $\mathbb{N}$ has a topology which makes it into a complete separable metric space with respect to the distance

$$d(\varphi, \psi) = \inf\{2^{-n} : (\forall i < n)(\varphi(i) = \psi(i) \wedge \varphi^{-1}(i) = \psi^{-1}(i))\}.$$

Note that composition and inversion are both continuous operations with respect to this topology. Furthermore, Sym is easily understood even in RCA_0 with the usual representation of complete metric spaces in subsystems of second-order arithmetic. See section II.5 of Simpson's book [16].

If F is a subfield of K, the class $\mathrm{Aut}(K/F)$ of F-automorphisms of K corresponds to a closed subgroup of Sym. Indeed, if φ is a permutation of K which is not an F-automorphism, then there is a finite initial segment of φ that cannot be extended to an F-automorphism of K. The Galois correspondence says that there is an inclusion-reversing correspondence between intermediate fields $F \subset E \subset K$ and closed subgroups of $\mathrm{Aut}(K/F)$; this correspondence is provable in WKL_0.

Theorem 26 (WKL_0)**.** (Galois Correspondence.) *Suppose K is a Galois extension of F.*

- *For every intermediate extension E between F and K, K is a Galois extension of E, and $\mathrm{Aut}(K/E)$ is a closed subgroup of $\mathrm{Aut}(K/F)$.*
- *For every closed subgroup H of $\mathrm{Aut}(K/F)$, there is an intermediate extension E such that K is a Galois extension of E, and $H = \mathrm{Aut}(K/E)$.*

Proof. The first part of the theorem is immediate from Theorem 25, but the second part requires proof.

The first observation is that $\mathrm{Aut}(K/F)$ is a bounded subgroup of Sym. Indeed, since K is a normal extension of F, for every $k \in K$, we can effectively find a polynomial $p_k(x) \in F[x]$ such that $p_k(k) = 0$ and $p_k(x)$ splits completely in K. Consequently, RCA_0 proves the existence of an F embedding bound, $b : K \to K^{<\mathbb{N}}$. Any F-automorphism of K must send k to some element of $b(k)$. By the last sentence of Definition 15, if φ is an F-automorphism of K, then $\varphi(k) \leq b(k)$ for all $k \in K$.

Applying Δ^0_1-comprehension, we can prove the existence of a b-bounded tree of initial segments of elements of $\mathrm{Aut}(K/F)$. Briefly, given an enumeration $\langle k_i \rangle_{i \in \mathbb{N}}$ of K, place σ in the tree if for all $i, j < \mathrm{lh}(\sigma)$ we have (1) $\sigma(i) \leq b(k_i)$, (2) if j witnesses that $k_i \in F$ then $\sigma(i) = k_i$, and (3) σ preserves field operations. A closed subgroup H of $\mathrm{Aut}(K/F)$ corresponds to branches through a b-bounded subtree T_H. By WKL_0, an element k_n of K is fixed by every automorphism in H if and only if there is a level $m > n$ such that every element of $T_H \cap \mathbb{N}^m$ fixes n. Since T_H is b-bounded, this is a Σ^0_1 definition of the fixed field K^H. By Lemma 3, there is an isomorphic intermediate extension $\langle E, \tau \rangle$. By Theorem 25, K is a Galois extension of E.

It remains to see that $H = \mathrm{Aut}(K/E)$. The inclusion $H \subset \mathrm{Aut}(K/E)$ is clear, so suppose that ψ is an E-automorphism of K. We need to show that every initial segment of ψ is in the tree T_H. Let $p(x)$ be a polynomial in $E(x)$ such that $\tau(p)$ splits in K and the roots of $\tau(p)$ include $k_0, \ldots, k_{n-1}$. Let L be the splitting field of $\tau(p)$. Then ψ restricts to an E-automorphism $\overline{\psi}$ of L. Every element φ of H also restricts to an E-automorphism $\overline{\varphi}$ of L and these restrictions form a group $\overline{H}$ of automorphisms of L. Furthermore, E is the subfield of L fixed by $\overline{H}$ since E is the subfield of K fixed by H. It follows from finite Galois theory that $\overline{H} = \mathrm{Aut}(L/E)$ [4, Lemma 2.11], which means that $\overline{\psi} = \overline{\varphi}$ for some $\varphi \in H$. Since $k_0, k_1, \ldots, k_{n-1} \in L$, it follows that $\psi(m) = \varphi(m)$ for all $m < n$ and hence that the initial segment of ψ with length n belongs to T_H. $\square$

We already saw in Theorem 23 that the first part of the Galois correspondence requires WKL_0 (though $\mathrm{Aut}(K/E)$ is always a closed subgroup of $\mathrm{Aut}(K/F)$). In the second part of the correspondence theorem, E is essentially the fixed field for H, and the fixed field associated with a closed subgroup of $\mathrm{Aut}(K/F)$ is difficult to define in subsystems weaker than WKL_0.

Although $\mathrm{Aut}(K/F)$ is always a closed subgroup of Sym, this does not mean that $\mathrm{Aut}(K/F)$ is a complete separable metric space like Sym. Indeed, $\mathrm{Aut}(K/F)$ could fail to have a countable dense subset. The following definitions are related to those of Brown [2].

Definition 27. (RCA_0) Let F be a subfield of K.

- We say $\mathrm{Aut}(K/F)$ is *separably closed* if there is a sequence $\langle \varphi_i \rangle_{i \in \mathbb{N}}$ of elements of $\mathrm{Aut}(K/F)$ such that for every $\psi \in \mathrm{Aut}(K/F)$ and every $n \in \mathbb{N}$, there is an $i \in \mathbb{N}$ such that $d(\varphi_i, \psi) \leq 2^{-n}$.

- We say $\mathrm{Aut}(K/F)$ is *separably closed and totally bounded* if there is a sequence $\langle \varphi_i \rangle_{i \in \mathbb{N}}$ of elements of $\mathrm{Aut}(K/F)$ and a function $b : \mathbb{N} \to \mathbb{N}$ such that for every $\psi \in \mathrm{Aut}(K/F)$ and every $n \in \mathbb{N}$, there is an $i \leq b(n)$ such that $d(\varphi_i, \psi) \leq 2^{-n}$.

When $\mathrm{Aut}(K/F)$ is separably closed, this group can also be understood using the usual representation of complete metric spaces in second-order arithmetic. However, this is not always the case unless we assume ACA_0 (in which case every closed subgroup of Sym is separably closed).

Lemma 28 (RCA_0)**.** *Suppose K is a Galois extension of F. Then the following are equivalent:*

1. $\mathrm{Aut}(K/F)$ *is separably closed and totally bounded.*
2. $\mathrm{Aut}(K/F)$ *is separably closed.*
3. *F is a subset of K fixed by its embedding.*

Proof. It is clear that (1) implies (2).

To see that (2) implies (3), suppose that $\langle \varphi_i \rangle_{i \in \mathbb{N}}$ enumerates a dense set of elements of $\mathrm{Aut}(K/F)$. We claim that

$$\alpha \in F \leftrightarrow (\forall i)(\varphi_i(\alpha) = \alpha).$$

Since the displayed formula is Π^0_1, this shows that F is a Δ^0_1 subset of K. Since $\langle \varphi_i \rangle_{i \in \mathbb{N}}$ consists of elements of $\mathrm{Aut}(K/F)$, the forward implication is clear. For the converse, suppose α is an element of K that is not in F. Then, since K is a Galois extension of F, there is an F-automorphism φ of K such that $\varphi(\alpha) \neq \alpha$. By density, there is an i such that $\varphi_i(\alpha) = \varphi(\alpha)$ and so $\varphi_i(\alpha) \neq \alpha$.

To see that (3) implies (1), assume that F is a set. Given the first n elements of K, by Lemma 2.8 of Friedman, Simpson, and Smith [4] we can find polynomials irreducible over F corresponding to each element and the roots of these polynomials in K. From these construct the finite list of all possible related initial segments of F-automorphisms of K. Emulating the construction at the end of the proof of Theorem 9, we can extend these to F-automorphisms of K. For every $\psi \in \mathrm{Aut}(K/F)$ there will be a φ in this collection such that $d(\psi, \varphi) \leq 2^{-n}$. This construction can be carried out uniformly, yielding the sequence and function witnessing that $\mathrm{Aut}(K/F)$ is separably closed and totally bounded. □

Theorem 29 (RCA_0)**.** (Strong Galois Correspondence.) *Suppose K is a Galois extension of F.*

- *For every set E which is a field that contains F and is contained in K, K is a Galois extension of E, and* $\mathrm{Aut}(K/E)$ *is a separably closed and totally bounded subgroup of* $\mathrm{Aut}(K/F)$.

- *For every separably closed and totally bounded subgroup H of* $\mathrm{Aut}(K/F)$*, the collection E of elements fixed by H is a set contained in K, K is a Galois extension of E, and* $H = \mathrm{Aut}(K/E)$.

Proof. The first part of the theorem follows from the last sentence of Theorem 22 and Lemma 28.

For the second part of the theorem, suppose that $\langle \varphi_i \rangle_{i \in \mathbb{N}}$ and $b : \mathbb{N} \to \mathbb{N}$ witness that H is separably closed and totally bounded. Then, the subfield E of K fixed by H can be defined by the bounded formula $(\forall i \leq b(k))(\varphi_i(k) = k)$, which therefore exists by Δ^0_1-comprehension.

It remains to see that $H = \mathrm{Aut}(K/E)$. The inclusion $H \subset \mathrm{Aut}(K/E)$ is clear, so suppose that ψ is an E-automorphism of K. Pick n elements $\{k_0, \ldots, k_{n-1}\}$ of K. Let L be the normal closure of $E(k_0, \ldots, k_{n-1})$. (That is, L is the splitting field for the minimal polynomials of $k_0, \ldots, k_{n-1}$.) For each $i < n$, let $p_i \in F[x]$ be a polynomial with root k_i that splits into linear factors in K, and let m be the largest root of these polynomials. Now ψ restricts to an E-automorphism $\overline{\psi}$ of L. Every φ_i also restricts to an E-automorphism $\overline{\varphi}_i$ of L and the first $b(m) + 1$ such restrictions actually form a group $\overline{H} = \{\overline{\varphi}_0, \ldots, \overline{\varphi}_{b(m)}\}$ of automorphisms of L. Furthermore, E is the subfield of L fixed by $\overline{H}$ since E is the subfield of K fixed by H. It follows from finite Galois theory that $\overline{H} = \mathrm{Aut}(L/E)$ [4, Lemma 2.11], which means that $\overline{\psi} = \overline{\varphi}_i$ for some $i \leq b(m)$. Since $k_0, k_1, \ldots, k_{n-1} \in L$, it follows that $d(\varphi_i, \psi) \leq 2^{-n}$. Since this holds for every $n \in \mathbb{N}$ we see that $\varphi \in H$. □

Galois theory also says that if K is a Galois extension of F and L is an intermediate field, then L is a Galois extension of F if and only if $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$, in which case $\mathrm{Aut}(L/F)$ is isomorphic to the quotient group $\mathrm{Aut}(K/F)/\mathrm{Aut}(K/L)$. To analyze this, we first prove a variant of Theorem 23 in RCA_0.

Theorem 30 (RCA_0)**.** *Let K be a Galois extension of F and let L be an intermediate extension. The following are equivalent:*

1. *L is a Galois extension of F.*
2. *L is a* NOR1*-normal extension of F.*
3. *L is a* NOR2*-normal extension of F.*
4. *If $\varphi : L \to K$ is an F-embedding, then φ is an F-automorphism of L. (This is a variant of* NOR3*.)*
5. *Every F-automorphism of K restricts to an F-automorphism of L. (This is a variant of* NOR4 *and uses the notion of restriction from Definition 7.)*

Proof. Theorem 22 shows that (1) implies (2) and that (2) implies (3). The proof that (3) implies (4) is analogous to the proof that NOR2 implies NOR3 in Theorem 22. The proof that (4) implies (5) is analogous to the proof that NOR3 implies NOR4 in Theorem 22. Since K is a Galois extension of F it follows immediately that (5) implies (1). □

The next theorem uses the following terminology. If G is a class that is a group and N is a subclass that is also a group, we say that N is a *normal subgroup* of G if for all $\varphi \in N$ and $\psi \in G$, $\psi\varphi\psi^{-1}$ is in N.

Theorem 31 (RCA_0)**.** *Let K be a Galois extension of F and let L be an intermediate extension.*

1. *If L is a Galois extension of F then $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$.*
2. *If K is a Galois extension of L and $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$ then L is a Galois extension of F.*
3. *If L is also a subset of K, then $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$ if and only if L is a Galois extension of F.*

Proof. For the first statement, suppose φ is an element of $\mathrm{Aut}(K/L)$ and ψ is an element of $\mathrm{Aut}(K/F)$. Then ψ^{-1} is also in $\mathrm{Aut}(K/F)$. Consider $\psi\varphi\psi^{-1}$ and let $x \in L$. Since L is a Galois extension of F, by part (5) of Theorem 30, $\psi^{-1}(x) \in L$. Thus $\varphi(\psi^{-1}(x)) = \psi^{-1}(x)$ and $\psi(\varphi\psi^{-1}(x)) = x$. Thus $\psi\varphi\psi^{-1} \in \mathrm{Aut}(K/L)$ and so $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$.

For the second statement, a simple algebraic computation shows that if φ is an F-automorphism of K, then $\mathrm{Aut}(K/\varphi[L]) = \varphi\,\mathrm{Aut}(K/L)\varphi^{-1}$. If $\mathrm{Aut}(K/L)$ is a normal subgroup of $\mathrm{Aut}(K/F)$ then $\varphi\,\mathrm{Aut}(K/L)\varphi^{-1} = \mathrm{Aut}(K/L)$. Assuming that K is Galois over L, it follows that $L = \varphi[L]$ and hence that φ restricts to an automorphism of L. By part (5) of Theorem 30, it follows that L is a Galois extension of F.

The last statement follows from the previous two and Theorem 29 which shows that K is necessarily a Galois extension of L. □

Informally, if L is an intermediate Galois extension of F, then the restriction map from K to L takes each element of $\mathrm{Aut}(K/F)$ and restricts its domain to create an automorphism of L. Consequently, the restriction map as described in part (5) of Theorem 30 is a homomorphism from $\mathrm{Aut}(K/F)$ to $\mathrm{Aut}(L/F)$ whose kernel is $\mathrm{Aut}(K/L)$. However, the homomorphism from $\mathrm{Aut}(K/F)$ to $\mathrm{Aut}(L/F)$ needs to be surjective in order to conclude that $\mathrm{Aut}(L/F)$ is isomorphic to the quotient of $\mathrm{Aut}(K/F)$ by $\mathrm{Aut}(K/L)$, which we can't really talk about in second-order arithmetic other than via the First Isomorphism Theorem.

Theorem 32. *The following are equivalent over* RCA_0*:*

1. WKL_0
2. *If K is a Galois extension of F and L is an intermediate extension of F, then the restriction map is a surjective homomorphism from* $\mathrm{Aut}(K/F)$ *onto* $\mathrm{Aut}(L/F)$ *whose kernel is* $\mathrm{Aut}(K/L)$*.*

If L is a subset of K fixed by its embedding, then (2) is provable in RCA_0*.*

Proof. Note that (2) simply states that any F-automorphism of L can be extended to an F-automorphism of K. The proof is similar to that of Theorem 9. □

6 Other characteristics

Results in sections §2 and §3 can be extended to fields of finite characteristic. In many cases, separability conditions must be appended to the hypotheses. Additionally, when the characteristic is specified in the result, any reversal must reflect this. The final result of this section, based on Theorem 10, illustrates the adaptation process.

Many of the reversals in previous sections involve extensions of $\mathbb{Q}$. Adaptation of these arguments relies on the following observation. Let p be a prime and let $\mathsf{GF}(p^n)$ denote the field of integers mod p^n. The field of rational functions $\mathsf{GF}(p^n)(x)$ is an infinite field of characteristic p and is the quotient field of the Euclidean ring $\mathsf{GF}(p^n)[x]$. Because $\mathsf{GF}(p^n)$ is finite, RCA_0 can prove the existence of the set of monic irreducible polynomials of $\mathsf{GF}(p^n)[x]$. These irreducible polynomials can play the role the prime numbers in our prior constructions. For example, we have the following versions of Lemma 4.

Lemma 33. RCA_0 *Let R be a Euclidean ring with quotient ring Q of characteristic not equal to 2. Let $p_1, \ldots, p_n$ and $q_1, \ldots, q_r$ be disjoint lists of distinct primes (irreducible elements). Then*

$$\sqrt{q_1 \cdots q_r} \notin Q(\sqrt{p_1}, \ldots, \sqrt{p_n}) \quad \textit{and} \quad \sqrt{q_1} \notin Q(\sqrt{p_1}, \ldots, \sqrt{p_n}, \sqrt{q_1 q_2}, \ldots, \sqrt{q_1 q_r}).$$

Proof. We will work in RCA_0. Fix R. Note that the first conjunct of the conclusion can be written as: for every n, for every list of ps, for every list of qs, for every quotient of Q-linear combinations of products of roots of ps, the square of the linear combination is not equal to the product of the qs. Since this conjunct can be expressed as a Π^0_1 formula, we can proceed to prove it in RCA_0 by induction on n.

For the base case, suppose by way of contradiction that $\sqrt{q_1 \cdots q_r} \in Q$. Let $\sqrt{q_1 \cdots q_r} = \frac{r_0}{r_1}$ where $r_0, r_1 \in Q$ and $\gcd(r_0, r_1) = 1$. Thus $r_1^2 q_1 \ldots q_r = r_0^2$. Since q_1 is prime and $q_1 | r_0^2$, we

have $q_1|r_0$. So $r_0^2 = q_1^{2m}r_2$ where $m \geq 1$ and $\gcd(q_1, r_2) = 1$. Since $q_1^2|r_1^2 q_1 \dots q_r$ and $q_1, \dots, q_r$ are distinct primes, $q_1|r_1^2$. Thus $q_1|r_1$ and so $r_1^2 q_1 \dots q_r = q_1^{2k+1}r_3$ where $k \geq 1$ and $\gcd(q_1, r_3) = 1$. Summarizing, $q_1^{2k+1}r_3 = q_1^{2m}r_2$ where $q_1 \not| \, r_3$ and $q_1 \not| \, r_2$, a contradiction.

For the induction step, suppose the lemma is true for $n-1$. Fix distinct primes $p_1, \dots, p_n$. Let $F_0 = Q(\sqrt{p_1}, \dots, \sqrt{p_{n-1}})$. Let $q_1, \dots, q_r$ be a list of distinct primes disjoint from $p_1, \dots, p_n$. Suppose by way of contradiction that $\sqrt{q_1 \dots q_r} \in F_0(\sqrt{p_n})$. Then we may write $\sqrt{q_1 \dots q_r} = \alpha + \beta\sqrt{p_n}$ where $\alpha, \beta \in F_0$. Squaring yields $q_1 \dots q_r = \alpha^2 + \beta^2 p_n + 2\alpha\beta\sqrt{p_n}$. Consider three cases: (1) If $\alpha\beta \neq 0$ then $\sqrt{p_n} \in F_0$, contradicting the induction hypothesis. (2) If $\beta = 0$ then $\sqrt{q_1 \dots q_r} = \alpha \in F_0$, contradicting the induction hypothesis. (3) If $\alpha = 0$ then $\sqrt{q_1 \dots q_r} = \beta\sqrt{p_n}$ so $\sqrt{q_1 \dots q_r p_n} = p_n\beta \in F_0$, contradicting the induction hypothesis.

This completes the induction proof of the first conjunct of the conclusion of the lemma. The remaining conjunct is proved by the same argument as Lemma 5. □

Lemma 34. (RCA_0) *Let $\{p_i \mid i \leq n\}$ be a sequence of distinct irreducible elements of $\mathsf{GF}(4)[x]$. For each $i \leq n$, let r_i be a solution of $x^3 - p_i = 0$. Then the set $A = \{\prod_{i \leq n} r_i^{\varepsilon_i} \mid \forall i \ 0 \leq \varepsilon_i \leq 2\}$ is linearly independent over $\mathsf{GF}(4)(x)$. Consequently, if $Q = \mathsf{GF}(4)(x)$ and $p_1, \dots, p_n$ and $q_1, \dots, q_r$ are disjoint lists of distinct primes, then*

$$\sqrt[3]{q_1 \dots q_r} \notin Q(\sqrt[3]{p_1}, \dots, \sqrt[3]{p_n}) \quad \text{and} \quad \sqrt[3]{q_1} \notin Q(\sqrt[3]{p_1}, \dots, \sqrt[3]{p_n}, \sqrt[3]{q_1 q_2}, \dots, \sqrt[3]{q_1 q_r}).$$

Proof. A straightforward algebraic argument proves that A is pairwise linearly independent over $\mathsf{GF}(4)(x)$. The first sentence of the lemma follows from Theorem 1.3 of Carr and O'Sullivan [3], substituting $\mathsf{GF}(4)(x)$ for their K, $\overline{K}$ for L, and A (as in the statement) for A. This instance of their theorem can be proved in RCA_0. The remainder of the lemma can be proved in much the same fashion as Lemma 33. □

Theorem 35. (RCA_0) *Let p be a prime or 0. The following are equivalent:*

1. WKL_0.
2. *Let F be an infinite field of characteristic p and let K be an algebraic extension of F that includes a separable element $\alpha \notin F$. Then there is an F-embedding of K into $\overline{K}$ that is not the identity.*

Proof. To prove that (1) implies (2), assume WKL_0. Since α is separable, it is a root of a polynomial $p(x) \in F[x]$ with no repeated roots. Since $\alpha \notin F$, the degree of $p(x)$ is greater than 1. Let $\beta \neq \alpha$ be another root of this polynomial. Imitate the proof of Theorem 10. Since the proof of Theorem 9 does not rely on the characteristic of F, it can be used to complete the proof.

Next, we will prove the reversal for characteristic 0, and then adapt the argument for other characteristics. Let f and g be injections such that $\forall s \forall t (0 \neq f(s) \neq f(t) \neq 0)$. As

in the proof of Theorem 10, let (i, j) denote both the ordered pair and the integer code for that ordered pair. Let p_i denote the ith prime. Define the fields F and K by:

$$F = \mathbb{Q}(\sqrt{p_{(i,f(j))}}, \sqrt{p_i p_{(i,g(j))}} \mid i, j \in \mathbb{N}) \qquad K = \mathbb{Q}(\sqrt{p_i} \mid i \in \mathbb{N})$$

By Lemma 5, $\sqrt{2}$ is not an element of F, so K is a nontrivial extension of F. Suppose φ is a nontrivial F-embedding of K into $\overline{K}$. Then for some prime p_i, $\varphi(\sqrt{p_i}) \neq \sqrt{p_i}$. For this i and any j, $\varphi(\sqrt{p_{(i,g(j))}}) \neq \sqrt{p_{(i,g(j))}}$ and $\varphi(\sqrt{p_{(i,f(j))}}) = \sqrt{p_{(i,f(j))}}$. The separating set $S = \{k \mid \varphi(\sqrt{p_{(i,k)}}) = \sqrt{p_{(i,k)}}\}$ exists by Δ^1_0 comprehension using the parameter φ. Since S includes the range of f and avoids the range of g, this proves WKL_0.

Now suppose p is an odd prime and (2) holds for fields of characteristic p. Our goal is to adapt the previous construction to the characteristic p setting. Let $\{p_i \mid i \in \mathbb{N}\}$ be a list of distinct irreducible monic polynomials in $\mathsf{GF}(p)[x]$. These will play the role that the prime numbers played in the preceding argument. For each p_i, the polynomial $z^2 - p_i$ and its derivative have no common roots, so $z^2 - p_i$ is separable. Let r_i denote a root of $z^2 - p_i$. Given disjoint injections f and g that never take the value 0, define the fields F and K by

$$F = \mathsf{GF}(p)(x)(r_{(i,f(j))}, r_i r_{(i,g(j))} \mid i, j \in \mathbb{N}) \qquad K = \mathsf{GF}(p)(x)(r_i \mid i \in \mathbb{N})$$

By Lemma 33, K is a nontrivial extension of F. To complete the proof, use a nontrivial F-embedding of K to find a separating set for the ranges of f and g.

To carry out the reversal for characteristic 2, modify the previous argument by using $\mathsf{GF}(4)(x)$, $z^3 - p_i$, and Lemma 34. □

Some of the reversals in previous sections use algorithms for factoring polynomials over $\mathbb{Q}$. One can find factoring algorithms for the characteristic p fields used in this section by adapting work of Stoltenberg-Hansen and Tucker [17].

References

[1] Emil Artin, *Galois theory*, 2nd ed., Dover Publications Inc., Mineola, NY, 1998. Edited and with a supplemental chapter by Arthur N. Milgram. MR1616156 (98k:12001)

[2] Douglas K. Brown, *Notions of closed subsets of a complete separable metric space in weak subsystems of second-order arithmetic*, Logic and computation (Pittsburgh, PA, 1987), Contemp. Math., vol. 106, Amer. Math. Soc., Providence, RI, 1990, pp. 39–50, DOI 10.1090/conm/106/1057814, (to appear in print). MR1057814 (91i:03108)

[3] Richard Carr and Cormac O'Sullivan, *On the linear independence of roots*, Int. J. Number Theory **5** (2009), no. 1, 161–171, DOI 10.1142/S1793042109002018. MR2499028 (2010c:11041)

[4] Harvey M. Friedman, Stephen G. Simpson, and Rick L. Smith, *Countable algebra and set existence axioms*, Ann. Pure Appl. Logic **25** (1983), no. 2, 141–181, DOI 10.1016/0168-0072(83)90012-X. MR725732 (85i:03157)

[5] ———, *Addendum to: "Countable algebra and set existence axioms" [Ann. Pure Appl. Logic* **25** *(1983), no. 2, 141–181; MR0725732 (85i:03157)]*, Ann. Pure Appl. Logic **28** (1985), no. 3, 319–320, DOI 10.1016/0168-0072(85)90020-X. MR790391 (87f:03141)

[6] David Hilbert, *Die Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein **4** (1897), 175–546.

[7] Jeffry L. Hirst, *Representations of reals in reverse mathematics*, Bull. Pol. Acad. Sci. Math. **55** (2007), no. 4, 303–316, DOI 10.4064/ba55-4-2. MR2369116 (2009j:03015)

[8] Thomas Hungerford, *Abstract Algebra*, Graduate Texts in Mathematics, Springer Science+Business Media, New York, NY, 1980.

[9] Carl G. Jockusch Jr. and Robert I. Soare, Π^0_1 *classes and degrees of theories*, Trans. Amer. Math. Soc. **173** (1972), 33–56. MR0316227 (47 #4775)

[10] Irving Kaplansky, *Fields and rings*, Chicago Lectures in Mathematics, University of Chicago Press, Chicago, IL, 1995. Reprint of the second (1972) edition. MR1324341 (96a:12001)

[11] Serge Lang, *Algebra*, 3rd ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002. MR1878556 (2003e:00003)

[12] G. Metakides and A. Nerode, *Effective content of field theory*, Ann. Math. Logic **17** (1979), no. 3, 289–320, DOI 10.1016/0003-4843(79)90011-1. MR556895 (82b:03082)

[13] R. Miller and A. Shlapentokh, *Computable categoricity for algebraic fields with spitting algorithms* (November 7, 2011). Preprint, http://arxiv.org/pdf/1111.1205.pdf.

[14] J. B. Remmel, *Graph colorings and recursively bounded* Π^0_1*-classes*, Ann. Pure Appl. Logic **32** (1986), no. 2, 185–194, DOI 10.1016/0168-0072(86)90051-5. MR863333 (87m:03065)

[15] R. L. Roth, *Classroom Notes: On Extensions of Q by Square Roots*, Amer. Math. Monthly **78** (1971), no. 4, 392–393, DOI 10.2307/2316910. MR1536291

[16] Stephen Simpson, *Subsystems of second order arithmetic*, 2nd ed., Perspectives in Logic, Cambridge University Press, Cambridge, 2009. MR2517689 (2010e:03073)

[17] V. Stoltenberg-Hansen and J. V. Tucker, *Computable rings and fields*, Handbook of computability theory, Stud. Logic Found. Math., vol. 140, North-Holland, Amsterdam, 1999, pp. 363–447, DOI 10.1016/S0049-237X(99)80028-7, (to appear in print). MR1720739 (2000g:03100)

[18] B. L. van der Waerden, *Algebra. Vol. I*, Springer-Verlag, New York, 1991. Based in part on lectures by E. Artin and E. Noether; Translated from the seventh German edition by Fred Blum and John R. Schulenberger. MR1080172 (91h:00009a)

[19] Oscar Zariski and Pierre Samuel, *Commutative algebra. Vol. II*, Springer-Verlag, New York, 1975. Reprint of the 1960 edition; Graduate Texts in Mathematics, Vol. 29. MR0389876 (52 #10706)