

A Sheaf Model of the Algebraic Closure

Bassel Mannaa

Thierry Coquand

Department of Computer Science and Engineering
University of Gothenburg*
Gothenburg, Sweden

bassel.mannaa@cse.gu.se

thierry.coquand@cse.gu.se

In constructive algebra one cannot in general decide the irreducibility of a polynomial over a field K . This poses some problems to showing the existence of the algebraic closure of K . We give a possible constructive interpretation of the existence of the algebraic closure of a field in characteristic 0 by building, in a constructive metatheory, a suitable site model where there is such an algebraic closure. One can then extract computational content from this model. We give examples of computation based on this model.

1 Introduction

Since in general it is not decidable whether a given polynomial over a field is irreducible, even when the field is given explicitly [6], the notion of algebraic field extension and consequently the notion of algebraic closure becomes problematic from a constructive point of view. Even in situations where one can constructively assert the existence of an algebraic closure of a field [14, Ch. 6] the computational content of such assertions are not always clear. We present a constructive interpretation of the algebraic closure of field K in characteristic 0 as a site model. Our approach is different from [15] in that we do not assume a polynomial over a field to be decomposable into irreducible factors. The model presented here has a direct computational content and can be viewed as a model of dynamical evaluation in the sense of Duval [5] (see also [4]). The site, described in section 3, is given by the category of finitely presented (von Neumann) regular algebras over K with the appropriate Grothendieck topology. In section 4 we prove that the topos $\mathcal{E}$ of sheaves on this site contains a model of an algebraically closed field extension of K . An alternative approach using profinite Galois group is presented in [8]. We also investigate some of the properties of the topos $\mathcal{E}$. Theorem 6.3 shows that the axiom of choice fails to hold in $\mathcal{E}$ whenever K is not algebraically closed. Theorem 6.4 shows that when the base field K is the rationals the weaker axiom of dependent choice fails to hold. We restrict ourselves to constructive metatheory throughout the paper with the exception of section 8 in which we show that in a classical metatheory the topos $\mathcal{E}$ is boolean (Theorem 8.6). As we will demonstrate by Theorem 8.8 this cannot be shown to hold in an intuitionistic metatheory.

2 Coverage, sheaves, and Kripke–Joyal semantics

In this section we recall some notions that we will use in the remainder the paper, mostly following the presentation in [7]. A *coverage* on a category $\mathcal{C}$ is a function $\mathbf{J}$ assigning to each object C of $\mathcal{C}$ a collection $\mathbf{J}(C)$ of families of morphisms with codomain C such that for any $\{f_i : C_i \rightarrow C\}_{i \in I} \in \mathbf{J}(C)$ and morphism $g : D \rightarrow C$ of $\mathcal{C}$ there exist $\{h_j : D_j \rightarrow D\}_{j \in J} \in \mathbf{J}(D)$ such that for each $j \in J$ the morphism

*The research leading to this work has been supported by ERC Advanced grant project 247219.

gh_j factors through f_ℓ for some $\ell \in I$. A family $S \in J(C)$ is called cover or covering family of C . A site is a category with coverage $(\mathcal{C}, \mathbf{J})$. For a presheaf $\mathbf{P} : \mathcal{C}^{op} \rightarrow \mathbf{Set}$ and family $S = \{g_i : A_i \rightarrow A\}_{i \in I}$ of morphisms of $\mathcal{C}$ we say that a family $\{s_i \in \mathbf{P}(A_i)\}_{i \in I}$ is compatible if for each $\ell, j \in I$ whenever we have $h : B \rightarrow A_\ell$ and $f : B \rightarrow A_j$ such that $g_\ell h = g_j f$ then $s_\ell h = s_j f$, where by $s_\ell h$ we mean the restriction of s_ℓ along h , i.e. $\mathbf{P}(h)s_\ell$. A presheaf $\mathbf{P}$ is a sheaf on the site $(\mathcal{C}, \mathbf{J})$ if for any object C and any cover $\{f_i : C_i \rightarrow C\}_{i \in I} \in \mathbf{J}(C)$ if $\{s_i \in \mathbf{P}(C_i)\}_{i \in I}$ is compatible then there exist a unique $s \in \mathbf{P}(C)$ such that $sf_i = s_i$. We call such s the amalgamation of $\{s_i\}_{i \in I}$.

We work with a typed language with equality $\mathcal{L}[V_1, \dots, V_n]$ having the basic types $V_1, \dots, V_n$ and type formers $- \times -, (-)^\perp, \mathcal{P}(-)$. The language $\mathcal{L}[V_1, \dots, V_n]$ has typed constants and function symbols. For any type Y one has a stock of variables $y_1, y_2, \dots$ of type Y . Terms and formulas of the language are defined as usual. We work within the proof theory of intuitionistic higher-order logic (IHOL). A detailed description of this deduction system is given in [1].

The language $\mathcal{L}[V_1, \dots, V_n]$ along with deduction system IHOL can be interpreted in an elementary topos in what is referred to as *topos semantics*. For a sheaf topos this interpretation takes a simpler form reminiscent of Beth semantics, usually referred to as *Kripke–Joyal sheaf semantics*. We describe this semantics here briefly following [15].

Let $\mathcal{E} = \mathbf{Sh}(\mathcal{C}, \mathbf{J})$ be a sheaf topos. An interpretation of the language $\mathcal{L}[V_1, \dots, V_n]$ in the topos $\mathcal{E}$ is given as follows: Associate to each basic type V_i of $\mathcal{L}[V_1, \dots, V_n]$ an object $\mathbf{V}_i$ of $\mathcal{E}$. If Y and Z are types of $\mathcal{L}[V_1, \dots, V_n]$ interpreted by objects $\mathbf{Y}$ and $\mathbf{Z}$, respectively, then the types $Y \times Z, Y^Z, \mathcal{P}(Z)$ are interpreted by $\mathbf{Y} \times \mathbf{Z}, \mathbf{Y}^{\mathbf{Z}}, \Omega^{\mathbf{Z}}$, respectively, where Ω is the subobject classifier of $\mathcal{E}$. A constant e of type E is interpreted by an arrow $\mathbf{1} \xrightarrow{e} \mathbf{E}$ where $\mathbf{E}$ is the interpretation of E . For a term τ and an object $\mathbf{X}$ of $\mathcal{E}$, we write $\tau : \mathbf{X}$ to mean τ has a type X interpreted by the object $\mathbf{X}$.

Let $\phi(x_1, \dots, x_n)$ be a formula with variables $x_1 : \mathbf{X}_1, \dots, x_n : \mathbf{X}_n$. Let $c_1 \in \mathbf{X}_1(C), \dots, c_n \in \mathbf{X}_n(C)$ for some object C of $\mathcal{C}$. We define the relation C forces $\phi(x_1, \dots, x_n)[c_1, \dots, c_n]$ written $C \Vdash \phi(x_1, \dots, x_n)[c_1, \dots, c_n]$ by induction on the structure of ϕ .

Definition 2.1 (Forcing). First we replace the constants in ϕ by variables of the same type as follows: Let $e_1 : \mathbf{E}_1, \dots, e_m : \mathbf{E}_m$ be the constants in $\phi(x_1, \dots, x_n)$ then $C \Vdash \phi(x_1, \dots, x_n)[c_1, \dots, c_n]$ iff

$$C \Vdash \phi[y_1/e_1, \dots, y_m/e_m](y_1, \dots, y_m, x_1, \dots, x_n)[\mathbf{e}_{1C}(*), \dots, \mathbf{e}_{mC}(*), c_1, \dots, c_n]$$

where $y_i : \mathbf{E}_i$ and $\mathbf{e}_i : \mathbf{1} \rightarrow \mathbf{E}_i$ is the interpretation of e_i .

Now it suffices to define the forcing relation for formulas free of constants by induction as follows:

- $\top$ $C \Vdash \top$.
- $\perp$ $C \Vdash \perp$ iff the empty family is a cover of C .
- $=$ $C \Vdash (x_1 = x_2)[c_1, c_2]$ iff $c_1 = c_2$.
- $\wedge$ $C \Vdash (\phi \wedge \psi)(x_1, \dots, x_n)[c_1, \dots, c_n]$ iff $C \Vdash \phi(x_1, \dots, x_n)[c_1, \dots, c_n]$ and $C \Vdash \psi(x_1, \dots, x_n)[c_1, \dots, c_n]$.
- $\vee$ $C \Vdash (\phi \vee \psi)(x_1, \dots, x_n)[c_1, \dots, c_n]$ iff there exist a cover $\{C_i \xrightarrow{f_i} C\}_{i \in I} \in \mathbf{J}(C)$ such that $C_i \Vdash \phi(x_1, \dots, x_n)[c_1 f_i, \dots, c_n f_i]$ or $C_i \Vdash \psi(x_1, \dots, x_n)[c_1 f_i, \dots, c_n f_i]$ for each $i \in I$.
- $\Rightarrow$ $C \Vdash (\phi \Rightarrow \psi)(x_1, \dots, x_n)[c_1, \dots, c_n]$ iff for every morphism $f : D \rightarrow C$ whenever $D \Vdash \phi(x_1, \dots, x_n)[c_1 f, \dots, c_n f]$ one has $D \Vdash \psi(x_1, \dots, x_n)[c_1 f, \dots, c_n f]$.

Let y be a variable of the type Y interpreted by the object $\mathbf{Y}$ of $\mathcal{E}$.

- $\exists$ $C \Vdash (\exists y \phi(x_1, \dots, x_n, y))[c_1, \dots, c_n]$ iff there exist a cover $\{C_i \xrightarrow{f_i} C\}_{i \in I} \in \mathbf{J}(C)$ such that for each $i \in I$ one has $C_i \Vdash \phi(x_1, \dots, x_n, y)[c_1 f_i, \dots, c_n f_i, d]$ for some $d \in \mathbf{Y}(C_i)$.

$\boxed{\forall}$ $C \Vdash (\forall y \phi(x_1, \dots, x_n, y))[c_1, \dots, c_n]$ iff for every morphism $f : D \rightarrow C$ and for all $d \in \mathbf{Y}(D)$ one has $D \Vdash \phi(x_1, \dots, x_n, y)[c_1 f, \dots, c_n f, d]$.

We have the following derivable *local character* and *monotonicity* laws

$\boxed{\text{LC}}$ If $\{C_i \xrightarrow{f_i} C\}_{i \in I} \in \mathbf{J}(C)$ and for all $i \in I$, $C_i \Vdash \phi(x_1, \dots, x_n)[c_1 f_i, \dots, c_n f_i]$ then $C \Vdash \phi(x_1, \dots, x_n)[c_1, \dots, c_n]$

$\boxed{\text{M}}$ If $C \Vdash \phi(x_1, \dots, x_n)[c_1, \dots, c_n]$ and $f : D \rightarrow C$ then $D \Vdash \phi(x_1, \dots, x_n)[c_1 f, \dots, c_n f]$

3 The topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$

Definition 3.1 (Regular ring). A commutative ring R is (*von Neumann*) regular if for every element $a \in R$ there exist $b \in R$ such that $aba = a$ and $bab = b$. This element b is called the quasi-inverse of a .

The quasi-inverse of an element a is unique for a [9, Ch. 4]. We thus use the notation a^* to refer to the quasi-inverse of a . A ring is regular iff it is zero-dimensional and reduced. To be regular is equivalent to the fact that any principal ideal (consequently, any finitely generated ideal) is generated by an idempotent. If R is regular and $a \in R$ then $e = aa^*$ is an idempotent such that $\langle e \rangle = \langle a \rangle$ and R is isomorphic to $R_0 \times R_1$ with $R_0 = R/\langle e \rangle$ and $R_1 = R/\langle 1 - e \rangle$. Furthermore a is 0 on the component R_0 and invertible on the component R_1 .

Definition 3.2 (Fundamental system of orthogonal idempotents). A family $(e_i)_{i \in I}$ of idempotents in a ring R is a fundamental system of orthogonal idempotents if $\sum_{i \in I} e_i = 1$ and $\forall i, j [i \neq j \Rightarrow e_i e_j = 0]$.

Lemma 3.3. Given a fundamental system of orthogonal idempotents $(e_i)_{i \in I}$ in a ring A we have a decomposition $A \cong \prod_{i \in I} A/\langle 1 - e_i \rangle$.

Proof. Follows by induction from the fact that $A \cong A/\langle e \rangle \times A/\langle 1 - e \rangle$ for an idempotent $e \in A$. $\square$

Definition 3.4 (Separable polynomial). Let R be a ring. A polynomial $p \in R[X]$ is separable if there exist $r, s \in R[X]$ such that $rp + sp' = 1$, where $p' \in R[X]$ is the derivative of p .

Definition 3.5. A ring R is a (strict) Bézout ring if for all $a, b \in R$ we can find $g, a_1, b_1, c, d \in R$ such that $a = a_1 g$, $b = b_1 g$ and $ca_1 + db_1 = 1$ [9, Ch. 4].

If R is a regular ring then $R[X]$ is a strict Bézout ring (and the converse is true [9]). Intuitively we can compute the gcd as if R was a field, but we may need to split R when deciding if an element is invertible or 0. Using this, we see that given $a, b \in R[X]$ we can find a decomposition $R_1, \dots, R_n$ of R and for each i we have g, a_1, b_1, c, d in $R_i[X]$ such that $a = a_1 g$, $b = b_1 g$ and $ca_1 + db_1 = 1$ with g monic.

Lemma 3.6. If R is regular and p in $R[X]$ is a separable polynomial then $R[a] = R[X]/\langle p \rangle$ is regular.

Proof. If $c = q(a)$ is an element of $R[a]$ with q in $R[X]$ we compute the gcd g of p and q . If $p = gp_1$, we can find u and v in $R[X]$ such that $ug + vp_1 = 1$ since p is separable. We then have $g(a)p_1(a) = 0$ and $u(a)g(a) + v(a)p_1(a) = 1$. It follows that $e = u(a)g(a)$ is idempotent and we have $\langle e \rangle = \langle g(a) \rangle$. $\square$

An algebra A over a field K is *finitely presented* if it is of the form $K[X_1, \dots, X_n]/\langle f_1, \dots, f_m \rangle$, i.e. the quotient of the polynomial ring over K in finitely many variables by a finitely generated ideal.

In order to build the classifying topos of a coherent theory T it is customary in the literature to consider the category of all finitely presented T_0 algebras where T_0 is an equational subtheory of T . The axioms of T then give rise to a coverage on the dual category [11, Ch. 9]. For our purpose consider the category $\mathcal{C}$ of finitely presented K -algebras. Given an object R of $\mathcal{C}$, the axiom schema of algebraic closure and the field axiom give rise to families (i.) $R \rightarrow R[X]/\langle p \rangle$ where $p \in R[X]$ is monic and

(ii.) $R \begin{array}{l} \nearrow R/\langle a \rangle \\ \searrow R[\frac{1}{a}] \end{array}$, for $a \in R$. Dualized, these are covering families of R in $\mathcal{C}^{op}$. We observe however

that we can limit our consideration only to those finitely presented K -algebras that are zero dimensional and reduced, i.e. regular. In this case we can assume a is an idempotent and we only consider extensions $R[X]/\langle p \rangle$ where p is separable.

Let $\mathcal{R}\mathcal{A}_K$ be the small category of finitely presented regular algebras over a fixed field K and K -homomorphisms. First we fix an countable set of names S . An object of $\mathcal{R}\mathcal{A}_K$ is a regular algebra of the form $K[X_1, \dots, X_n]/\langle f_1, \dots, f_m \rangle$ where $X_i \in S$ for all $1 \leq i \leq n$. Note that for any object R , there is a unique morphism $K \rightarrow R$. A finitely presented regular K -algebra A is a finite dimensional K -algebra, i.e. A has a finite dimension as a vector space over K [9, Ch 4, Theorem 8.16]. The trivial ring 0 is the terminal object in the category $\mathcal{R}\mathcal{A}_K$ and K is its initial object.

To specify a coverage $\mathbf{J}$ on the category $\mathcal{R}\mathcal{A}_K^{op}$, we define for each object A a collection $\mathbf{J}^{op}(A)$ of families of morphisms of $\mathcal{R}\mathcal{A}_K$ with domain A . We then take $\mathbf{J}(A)$ to be the dual of $\mathbf{J}^{op}(A)$ in the sense that $\{\bar{\varphi}_i : A_i \rightarrow A\}_{i \in I} \in \mathbf{J}(A)$ if and only if $\{\varphi_i : A \rightarrow A_i\}_{i \in I} \in \mathbf{J}^{op}(A)$ where φ_i of $\mathcal{R}\mathcal{A}_K$ is the dual of $\bar{\varphi}_i$ of $\mathcal{R}\mathcal{A}_K^{op}$. We call $\mathbf{J}^{op}$ cocoverage and elements of $\mathbf{J}^{op}(A)$ cocovers (cocovering families) of A . By a *separable extension* of a ring R we mean a ring $R[a] = R[X]/\langle p \rangle$ where $p \in R[X]$ is non-constant, monic and separable.

Definition 3.7 (Topology for $\mathcal{R}\mathcal{A}_K^{op}$). For an object A of $\mathcal{R}\mathcal{A}_K$ the cocovering families are given by:

- (i.) If $(e_i)_{i \in I}$ is a fundamental system of orthogonal idempotents of A , then $\{A \xrightarrow{\varphi_i} A/\langle 1 - e_i \rangle\}_{i \in I} \in \mathbf{J}^{op}(A)$ where for each $i \in I$, φ_i is the canonical homomorphism.
- (ii.) Let $A[a]$ be a separable extension of A . We have $\{A \xrightarrow{\vartheta} A[a]\} \in \mathbf{J}^{op}(A)$ where ϑ is the canonical embedding.
- (iii.) If $\{A \xrightarrow{\varphi_i} A_i\}_{i \in I} \in \mathbf{J}^{op}(A)$ and for each $i \in I$, $\{A_i \xrightarrow{\vartheta_{ij}} A_{ij}\}_{j \in J_i} \in \mathbf{J}^{op}(A_i)$ then $\{A \xrightarrow{\vartheta_{ij}\varphi_i} A_{ij}\}_{i \in I, j \in J_i} \in \mathbf{J}^{op}(A)$.

Note that in particular 3.7.(i.) implies that the trivial algebra 0 is covered by the empty family of morphisms since an empty family of elements in this ring form a fundamental system of orthogonal idempotents. Also note that 3.7.(ii.) implies that $\{A \xrightarrow{1_A} A\} \in \mathbf{J}^{op}(A)$.

Lemma 3.8. The function $\mathbf{J}$ of Definition 3.7 is a coverage on $\mathcal{R}\mathcal{A}_K^{op}$.

Proof. Let $\eta : R \rightarrow A$ be a morphism of $\mathcal{R}\mathcal{A}_K$ and $S \in \mathbf{J}^{op}(R)$. We show that there exist a cocover $T \in \mathbf{J}^{op}(A)$ such that for each $\vartheta \in T$, $\vartheta\eta$ factors through some $\varphi \in S$. By duality, this implies $\mathbf{J}$ is a coverage on $\mathcal{R}\mathcal{A}_K^{op}$. By case analysis on the clauses of Definition 3.7.

- (i.) If $S = \{\varphi_i : R \rightarrow R/\langle 1 - e_i \rangle\}_{i \in I}$, where $(e_i)_{i \in I}$ is a fundamental system of orthogonal idempotents of R . In A , the family $(\eta(e_i))_{i \in I}$ is fundamental system of orthogonal idempotents. We have a cocover $\{\vartheta_i : A \rightarrow A/\langle 1 - \eta(e_i) \rangle\}_{i \in I} \in \mathbf{J}^{op}(A)$. For each $i \in I$, the homomorphism η induces a K -homomorphism $\eta_{e_i} : R/\langle 1 - e_i \rangle \rightarrow A/\langle 1 - \eta(e_i) \rangle$ where $\eta_{e_i}(r + \langle 1 - e_i \rangle) = \eta(r) + \langle 1 - \eta(e_i) \rangle$. Since $\vartheta_i(\eta(r)) = \eta(r) + \langle 1 - \eta(e_i) \rangle$ we have that $\vartheta_i\eta = \eta_{e_i}\varphi_i$.
- (ii.) If $S = \{\varphi : R \rightarrow R[r]\}$ with $R[r] = R[X]/\langle p \rangle$ and $p \in R[X]$ monic, non-constant, and separable. since $sp + tp' = 1$. We have $\eta(s)\eta(p) + \eta(t)\eta(p') = \eta(s)\eta(p) + \eta(t)\eta(p)' = 1$. Then $q = \eta(p) \in$

$A[X]$ is separable. Let $A[a] = A[X]/\langle q \rangle$. We have a cocover $\{\vartheta : A \rightarrow A[a]\} \in \mathbf{J}^{op}(A)$ where ϑ is the canonical embedding. Let $\zeta : R[r] \rightarrow A[a]$ be the K -homomorphism such that $\zeta|_R = \eta$ and $\zeta(r) = a$. For $b \in R$, we have $\vartheta(\eta(b)) = \zeta(\varphi(b))$.

(iii.) Let $S = \{\xi_{ij}\gamma_i : R \rightarrow R_{ij}\}_{i \in I, j \in J_i}$ with $\{\gamma_i : R \rightarrow R_i\}_{i \in I} \in \mathbf{J}^{op}(R)$ and for each $i \in I$, $\{\xi_{ij} : R_i \rightarrow R_{ij}\}_{j \in J_i} \in \mathbf{J}^{op}(R_i)$. By induction we obtain a cocover $\{\vartheta_v : A \rightarrow A_v\}_{v \in V} \in \mathbf{J}^{op}(A)$ such that for each $v \in V$, $\vartheta_v \eta = \pi_{iv} \gamma_i$ for some $i \in I$ and $\pi_{iv} : R_i \rightarrow A_v$. From this, by induction, we get for each $v \in V$ a cocover $\{\sigma_{v\ell} : A_v \rightarrow A_{v\ell}\}_{v \in V, \ell \in L_v} \in \mathbf{J}^{op}(A_v)$ such that for each $\ell \in L_v$, $\sigma_{v\ell} \pi_{iv}$ factor through some ξ_{ij} . But $\sigma_{v\ell} \vartheta_v \eta = \sigma_{v\ell} \pi_{iv} \gamma_i$ for some i , hence, $\sigma_{v\ell} \vartheta_v \eta$ factors through some $\xi_{ij} \gamma_i$. $\square$

Lemma 3.9. *Let $\mathbf{P} : \mathcal{R}\mathcal{A}_K \rightarrow \mathbf{Set}$ be a presheaf on $\mathcal{R}\mathcal{A}_K^{op}$ such that $\mathbf{P}(0) = 1$. Let R be an object of $\mathcal{R}\mathcal{A}_K$ and let $(e_i)_{i \in I}$ be a fundamental system of orthogonal idempotents of R . For each $i \in I$, let $R_i = R/\langle 1 - e_i \rangle$ and let $\varphi_i : R \rightarrow R_i$ be the canonical homomorphism. Any family $\{s_i \in \mathbf{P}(R_i)\}$ is compatible.*

Proof. Let B be an object and for some $i, j \in I$ let $\vartheta : R_i \rightarrow B$ and $\zeta : R_j \rightarrow B$ be such that $\vartheta \varphi_i = \zeta \varphi_j$. We will show that $\mathbf{P}(\vartheta)(s_i) = \mathbf{P}(\zeta)(s_j)$.

(i.) If $i = j$, then since φ_i is surjective we have $\vartheta = \zeta$ and $\mathbf{P}(\vartheta) = \mathbf{P}(\zeta)$.

(ii.) If $i \neq j$, then since $e_i e_j = 0$, $\varphi_i(e_i) = 1$ and $\varphi_j(e_j) = 1$ we have $\varphi_j(e_i) = \varphi_j(e_i e_j) = 0$. But then

$$1 = \vartheta(1) = \vartheta(\varphi_i(e_i)) = \zeta(\varphi_j(e_i)) = \zeta(0) = 0$$

Hence B is the trivial algebra 0. By assumption $\mathbf{P}(0) = 1$, hence $\mathbf{P}(\vartheta)(s_i) = \mathbf{P}(\zeta)(s_j) = *$. $\square$

Corollary 3.10. *Let $\mathbf{F}$ be a sheaf on $(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$. Let R be an object of $\mathcal{R}\mathcal{A}_K$ and $(e_i)_{i \in I}$ a fundamental system of orthogonal idempotents of R . Let $R_i = R/\langle 1 - e_i \rangle$ and $\varphi_i : R \rightarrow R_i$ be the canonical homomorphism. The map $f : \mathbf{F}(R) \rightarrow \prod_{i \in I} \mathbf{F}(R_i)$ such that $f(s) = (\mathbf{F}(\varphi_i)s)_{i \in I}$ is an isomorphism.*

Proof. Since $\mathbf{F}(0) = 1$, by Lemma 3.9 any family $\{s_i \in \mathbf{F}(R_i)\}_{i \in I}$ is compatible. Since $\mathbf{F}$ is a sheaf, the family $\{s_i \in \mathbf{F}(R_i)\}_{i \in I}$ has a unique amalgamation $s \in \mathbf{F}(R)$ with restrictions $s \varphi_i = s_i$. The isomorphism is given by $f s = (s \varphi_i)_{i \in I}$. We can then use the tuple notation $(s_i)_{i \in I}$ to denote the element s in $\mathbf{F}(R)$. $\square$

One say that a polynomial $f \in R[X]$ has a *formal degree* n if f can be written as $f = a_n X^n + \dots + a_0$ which is to express that for any $m > n$ the coefficient of X^m is known to be 0.

Lemma 3.11. *Let R be a regular ring and $p_1, p_2 \in R[X]$ be monic polynomials of degrees n_1 and n_2 respectively. Let $R[a, b] = R[X, Y]/\langle p_1(X), p_2(Y) \rangle$. Let $q_1, q_2 \in R[Z]$ be of formal degrees $m_1 < n_1$ and $m_2 < n_2$ respectively. If $q_1(a) = q_2(b)$ then $q_1 = q_2 = r \in R$.*

Proof. The statement follows immediately since the R -basis $a^i, i > 0$ and $b^j, j > 0$ are linearly independent. $\square$

Corollary 3.12. *Let R be an object of $\mathcal{R}\mathcal{A}_K$ and $p \in R[X]$ separable and monic. Let $R[a] = R[X]/\langle p \rangle$ and $\varphi : R \rightarrow R[a]$ the canonical morphism. Let $R[b, c] = R[X, Y]/\langle p(X), p(Y) \rangle$. The commuting diagram*

$$\begin{array}{ccc} R[a] & \xrightarrow{\vartheta} & R[b, c] \\ \uparrow \varphi & & \uparrow \zeta \\ R & \xrightarrow{\varphi} & R[a] \end{array} \quad \vartheta|_R = \zeta|_R = 1_R, \vartheta(a) = b, \zeta(a) = c$$

is a pushout diagram of $\mathcal{R}\mathcal{A}_K$. Moreover, φ is the equalizer of ζ and ϑ .

Proof. Let $R[a] \xrightarrow[\rho]{\eta} B$ be morphisms of $\mathcal{R}\mathcal{A}_K$ such that $\eta\varphi = \rho\varphi$. Then for all $r \in R$ we have $\eta(r) = \rho(r)$. Let $\gamma : R[b, c] \rightarrow B$ be the homomorphism such that $\gamma(r) = \eta(r) = \rho(r)$ for all $r \in R$ while $\gamma(b) = \eta(a), \gamma(c) = \rho(a)$. Then γ is the unique map such that $\gamma\vartheta = \eta$ and $\gamma\zeta = \rho$.

Let A be an object of $\mathcal{R}\mathcal{A}_K$ and let $\varepsilon : A \rightarrow R[a]$ be a map such that $\zeta\varepsilon = \vartheta\varepsilon$. By Lemma 3.11 if for some $f \in R[a]$ one has $\zeta(f) = \vartheta(f)$ then $f \in R$ (i.e. f is of degree 0 as a polynomial in a over R). Thus $\varepsilon(A) \subset R$ and we can factor ε uniquely (since φ is injective) as $\varepsilon = \varphi\mu$ with $\mu : A \rightarrow R$. $\square$

Let $\{\varphi : R \rightarrow R[a]\}$ be a singleton cocover. Since one can form the pushout of φ with itself, the compatibility condition on a singleton family $\{s \in \mathbf{F}(R[a])\}$ can be simplified as: Let $R \xrightarrow{\varphi} R[a] \xrightarrow[\vartheta]{\eta} A$ be a pushout diagram. A family $\{s \in \mathbf{F}(R[a])\}$ is compatible if and only if $s\vartheta = s\eta$.

Corollary 3.13. *The coverage $\mathbf{J}$ is subcanonical, i.e. all representable presheaves in $\mathbf{Set}^{\mathcal{R}\mathcal{A}_K}$ are sheaves on $(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$.* $\square$

4 The algebraically closed field extension

We define the presheaf $\mathbf{F} : \mathcal{R}\mathcal{A}_K \rightarrow \mathbf{Set}$ to be the forgetful functor. That is, for an object A of $\mathcal{R}\mathcal{A}_K$, $\mathbf{F}(A) = A$ and for a morphism $\varphi : A \rightarrow C$ of $\mathcal{R}\mathcal{A}_K$, $\mathbf{F}(\varphi) = \varphi$. Before we show that $\mathbf{F}$ is a sheaf we recall the following fact:

Fact 4.1. *Let $(\mathcal{C}, \mathbf{T})$ be a site and $\mathbf{P} : \mathcal{C}^{op} \rightarrow \mathbf{Set}$ a presheaf. If $\mathbf{P}$ satisfies the sheaf axiom for a family $\{C_i \xrightarrow{f_i} C\}_{i \in I}$ and for each i , $\mathbf{P}$ satisfies the sheaf axiom for a family $\{C_{ij} \xrightarrow{g_{ij}} C_i\}_{i \in I, j \in J_i}$, then $\mathbf{P}$ satisfies the sheaf axiom for the family $\{C_{ij} \xrightarrow{f_i g_{ij}} C\}_{i \in I, j \in J_i}$, (See [7, C2.1, Lemma 2.1.7]).*

Thus in order to show that a presheaf on $\mathcal{R}\mathcal{A}_K$ is a sheaf it will suffice to check the sheaf condition for cocovers of the forms 3.7.(i.) and 3.7.(ii.) only.

Lemma 4.2. *$\mathbf{F}$ is a sheaf of sets on the site $(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$*

Proof. By case analysis on the clauses of Definition 3.7.

(i.) Let $\{R \xrightarrow{\varphi_i} R/\langle 1 - e_i \rangle\}_{i \in I} \in \mathbf{J}^{op}(R)$, where $(e_i)_{i \in I}$ is fundamental system of orthogonal idempotents of R . The presheaf $\mathbf{F}$ has the property $\mathbf{F}(0) = 1$. By Lemma 3.9 a family $\{a_i \in R/\langle 1 - e_i \rangle\}_{i \in I}$ is a compatible family. By the isomorphism $R \xrightarrow{(\varphi_i)_{i \in I}} \prod_{i \in I} R/\langle 1 - e_i \rangle$ the element $a = (a_i)_{i \in I} \in R$ is the unique element such that $\varphi_i(a) = a_i$.

(ii.) Let $\{R \xrightarrow{\varphi} R[a]\} \in \mathbf{J}^{op}(R)$ where $R[a] = R[X]/\langle p \rangle$ with $p \in R[X]$ monic, non-constant and separable polynomial. Let $\{r \in R[a]\}$ be a compatible family. Let $R \xrightarrow{\varphi} R[a] \xrightarrow[\zeta]{\vartheta} R[b, c]$

be the pushout diagram of Corollary 3.12. Compatibility then implies $\vartheta(r) = \zeta(r)$ which by the same Corollary is true only if the element r is in R . We then have that r is the unique element restricting to itself along the embedding φ . $\square$

We fix a field K of characteristic 0. Let $\mathcal{L}[F, +, \cdot]$ be a language with basic type F and function symbols $+, \cdot : F \times F \rightarrow F$. We extend $\mathcal{L}[F, +, \cdot]$ by adding a constant symbol of type F for each element $a \in K$, to obtain $\mathcal{L}[F, +, \cdot]_K$. Define $\text{Diag}(K)$ as : if ϕ is an atomic $\mathcal{L}[F, +, \cdot]_K$ -formula or the negation of one such that $K \models \phi(a_1, \dots, a_n)$ then $\phi(a_1, \dots, a_n) \in \text{Diag}(K)$. The theory T equips the type F with axioms of the geometric theory of algebraically closed field containing K

Definition 4.3. The theory T has the following sentences (with all the variables having the type F).

1. $\text{Diag}(K)$.
2. The axioms of a commutative group: (a) $\forall x [0 + x = x + 0 = x]$ (b) $\forall x \forall y \forall z [x + (y + z) = (x + y) + z]$ (c) $\forall x \exists y [x + y = 0]$ (d) $\forall x \forall y [x + y = y + x]$
3. The axioms of a commutative ring: (a) $\forall x [x1 = x]$ (b) $\forall x [x0 = 0]$ (c) $\forall x \forall y [xy = yx]$ (d) $\forall x \forall y \forall z [x(yz) = (xy)z]$ (e) $\forall x \forall y \forall z [x(y + z) = xy + xz]$
4. The field axioms: (a) $1 \neq 0$. (b) $\forall x [x = 0 \vee \exists y [xy = 1]]$.
5. The axiom schema for algebraic closure: $\forall a_1 \dots \forall a_n \exists x [x^n + \sum_{i=1}^n x^{n-i} a_i = 0]$.
6. F is algebraic over K : $\forall x [\bigvee_{p \in K[Y]} p(x) = 0]$.

With these axioms the type F becomes the type of an algebraically closed field containing K . We proceed to show that with the interpretation of the type F by the object $\mathbf{F}$ the topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{\text{op}}, \mathbf{J})$ is a model of T , i.e. $\mathbf{F}$ is a model, in Kripke–Joyal semantics, of an algebraically closed field containing K . First note that since there is a unique map $K \rightarrow C$ for any object C of $\mathcal{R}\mathcal{A}_K$, an element $a \in K$ gives rise to a unique map $\mathbf{1} \xrightarrow{a} \mathbf{F}$, that is the map $* \mapsto a \in \mathbf{F}(K)$. Every constant $a \in K$ of the language is then interpreted by the corresponding unique arrow $\mathbf{1} \xrightarrow{a} \mathbf{F}$. (we use the same symbol for constants and their interpretation to avoid cumbersome notation). That $\mathbf{F}$ satisfies $\text{Diag}(K)$ then follows directly.

Lemma 4.4. $\mathbf{F}$ is a ring object.

Proof. For an object C of $\mathcal{R}\mathcal{A}_K$ the object $\mathbf{F}(C)$ is a commutative ring. □

Lemma 4.5. $\mathbf{F}$ is a field.

Proof. For any object R of $\mathcal{R}\mathcal{A}_K$ one has $R \Vdash 1 \neq 0$ since for any $R \xrightarrow{\varphi} C$ such that $C \Vdash 1 = 0$ one has that C is trivial and thus $C \Vdash \perp$. Next we show that for variables x and y of type $\mathbf{F}$ and any object R of $\mathcal{R}\mathcal{A}_K^{\text{op}}$ we have $R \Vdash \forall x [x = 0 \vee \exists y [xy = 1]]$. Let $\varphi : A \rightarrow R$ be a morphism of $\mathcal{R}\mathcal{A}_K^{\text{op}}$ and let $a \in A$. We need to show that $A \Vdash a = 0 \vee \exists y [ay = 1]$. The element $e = aa^*$ is an idempotent and we have a cover $\{\varphi_1 : A/\langle e \rangle \rightarrow A, \varphi_2 : A/\langle 1 - e \rangle \rightarrow A\} \in \mathbf{J}(A)$ with $A/\langle e \rangle \Vdash a\varphi_1 = 0$ and $A/\langle 1 - e \rangle \Vdash (a\varphi_2)(a^*\varphi_2) = e\varphi_2 = 1$. Hence by $\exists$ we have $A/\langle 1 - e \rangle \Vdash \exists y [(a\varphi_2)y = 1]$ and by $\bigvee$, $A/\langle 1 - e \rangle \Vdash a\varphi_2 = 0 \vee \exists y [(a\varphi_2)y = 1]$. Similarly, $A/\langle e \rangle \Vdash a\varphi_1 = 0 \vee \exists y [(a\varphi_1)y = 1]$. By $\bigvee$ we get $R \Vdash \forall x [x = 0 \vee \exists y [xy = 1]]$. □

To show that $A \Vdash \forall a_1 \dots \forall a_n \exists x [x^n + \sum_{i=1}^n x^{n-i} a_i = 0]$ for every n , we need to be able to extend an algebra R of $\mathcal{R}\mathcal{A}_K$ with the appropriate roots. We need the following lemma.

Lemma 4.6. Let L be a field and $f \in L[X]$ a monic polynomial. Let $g = \langle f, f' \rangle$, where f' is the derivative of f . Writing $f = hg$ we have that h is separable. We call h the separable associate of f .

Proof. Let a be the gcd of h and h' . We have $h = l_1 a$. Let d be the gcd of a and a' . We have $a = l_2 d$ and $a' = m_2 d$, with l_2 and m_2 coprime.

The polynomial a divides $h' = l_1 a' + l_1' a$ and hence that $a = l_2 d$ divides $l_1 a' = l_1 m_2 d$. It follows that l_2 divides $l_1 m_2$ and since l_2 and m_2 are coprime, that l_2 divides l_1 .

Also, if a^n divides p then $p = qa^n$ and $p' = q'a^n + nqa'a^{n-1}$. Hence da^{n-1} divides p' . Since l_2 divides l_1 , this implies that $a^n = l_2 da^{n-1}$ divides $l_1 p'$. So a^{n+1} divides $al_1 p' = hp'$.

Since a divides f and f' , a divides g . We show that a^n divides g for all n by induction on n . If a^n divides g we have just seen that a^{n+1} divides $g'h$. Also a^{n+1} divides $h'g$ since a divides h' . So a^{n+1} divides $g'h + h'g = f'$. On the other hand, a^{n+1} divides $f = hg = l_1 ag$. So a^{n+1} divides g which is the gcd of f and f' . This implies that a is a unit. □

The next lemma captures the intuition that the separable associate contains all the roots of the polynomial.

Lemma 4.7. *Let L be a field of characteristic 0 and $f \in L[X]$ a nonzero monic polynomial of degree n . If h be the separable associate of f , then $f \mid h^n$.*

Proof. Let $g = \langle f, f' \rangle$ and $f = hg$. We prove $f \mid h^n$ by induction on the degree of g . If $\deg g = 0$, then if $\deg f = 0$ we get $f \mid h^0 = 1$. Otherwise, $f \mid h$. Let $f' = qg$ and $rh + sq = 1$. Assuming the statement holds for $\deg g \leq m$. Let $\deg g = m + 1$. Let g' be the derivative of g we can find l, d, m, r_1, s_1 such that $g = l_1d, g' = l_2d, r_1l_1 + r_2l_2 = 1$. Since $\deg d < \deg g = m + 1$, by induction hypothesis we get that $g \mid l_1^{m+1}$. Let $ge = l_1^{m+1}$. We have $f' = qg = h'g + hg'$, substituting we get $h'l_1d + hl_2d = ql_1d$. We know that $d \neq 0$, hence $h'l_1 + hl_2 = ql_1$. From this and $r_1l_1 + r_2l_2 = 1$ we get $r_2h'l_1 + h - hr_1l_1 = r_2ql_1$. Thus $l_1(r_2q + hr_1 - r_2h') = h$. If we let $c = r_2q + hr_1 - r_2h'$ and since $f = hg$, we have $fec^{m+1} = h(ge)c^{m+1} = hl_1^{m+1}c^{m+1} = h^{m+2}$. $\square$

Since $\mathbf{F}$ is a field, the two previous lemmas hold for polynomials over $\mathbf{F}$. This means that for all objects R of $\mathcal{R}\mathcal{A}_K^{op}$ we have $R \Vdash \text{Lemma 4.6} \wedge \text{Lemma 4.7}$. Thus we have the following Corollary.

Corollary 4.8. *Let R be an object of $\mathcal{R}\mathcal{A}_K$ and let f be a monic polynomial in $R[X]$ and f' its derivative. There is a cocover $\{\varphi_i : R \rightarrow R_i\}_{i \in I} \in \mathbf{J}^{op}(R)$ and for each R_i we have $h, g, q, r, s \in R_i[X]$ such that $\varphi_i f = hg$, $\varphi_i f' = qg$ and $rh + sq = 1$. Moreover, h is monic and separable and $\varphi_i f \mid h^n$.* $\square$

Lemma 4.9. *The field object $\mathbf{F} \in \text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$ is algebraically closed.*

Proof. We prove that for all $n > 0$ and all $(a_1, \dots, a_n) \in \mathbf{F}^n(R) = R^n$, one has $R \Vdash \exists x [x^n + \sum_{i=1}^n x^{n-i} a_i = 0]$. Let $f = x^n + \sum_{i=1}^n x^{n-i} a_i$. By Corollary 4.8 we have a cover $\{\vartheta_j : R_j \rightarrow R\}_{j \in I} \in \mathbf{J}(R)$ such that in each R_j we have $g = \langle f\vartheta_j, f'\vartheta_j \rangle$ and $f\vartheta_j = hg$ with $h \in R_j[X]$ monic and separable. Note that if $\deg f > 1$, h is non-constant. For each R_j we have a singleton cover $\{\varphi : R_j[b] \rightarrow R_j \mid R_j[b] = R_j[X]/\langle h \rangle\} \in \mathbf{J}(R_j)$. That is, we have $R_j[b] \Vdash b^n + \sum_{i=1}^n b^{n-i} (a_i \vartheta_j \varphi) = 0$. By $\exists$ we get $R_j[b] \Vdash \exists x [x^n + \sum_{i=1}^n x^{n-i} (a_i \vartheta_j \varphi) = 0]$ and by LC we have $R_j \Vdash \exists x [x^n + \sum_{i=1}^n x^{n-i} (a_i \vartheta_j) = 0]$. Since this is true for each $R_j, j \in J$ we have by LC $R \Vdash \exists x [x^n + \sum_{i=1}^n x^{n-i} a_i = 0]$. $\square$

Lemma 4.10. *$\mathbf{F}$ is algebraic over K .*

Proof. We will show that for any object R of $\mathcal{R}\mathcal{A}_K$ and element $r \in R$ one has $R \Vdash \bigvee_{p \in K[X]} p(r) = 0$. Since R is a finitely presented K -algebra we have that R is a finite integral extension of a polynomial ring $K[Y_1, \dots, Y_n] \subset R$ where $Y_1, \dots, Y_n$ are elements of R algebraically independent over K and that R has Krull dimension n [9, Ch 13, Theorem 5.4]. Since R is zero-dimensional (i.e. has Krull dimension 0) we have $n = 0$ and R is integral over K , i.e. any element $r \in R$ is the zero of some monic polynomial over K . $\square$

5 Constant sheaves, natural numbers, and power series

Here we describe the object of natural numbers in the topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$ and the object of power series over the field $\mathbf{F}$. This will be used in section 6 to show that the axiom of dependent choice does not hold when the base field K is the rationals and later in the example of Newton–Puiseux theorem (section 7).

Let $\mathbf{P} : \mathcal{R}\mathcal{A}_K \rightarrow \mathbf{Set}$ be a constant presheaf associating to each object A of $\mathcal{R}\mathcal{A}_K$ a discrete set B . That is, $\mathbf{P}(A) = B$ and $\mathbf{P}(A \xrightarrow{\varphi} R) = 1_B$ for all objects A and all morphism φ of $\mathcal{R}\mathcal{A}_K$. Let $\tilde{\mathbf{P}} : \mathcal{R}\mathcal{A}_K \rightarrow \mathbf{Set}$ be the presheaf such that $\tilde{\mathbf{P}}(A)$ is the set of elements of the form $\{(e_i, b_i)\}_{i \in I}$ where $(e_i)_{i \in I}$ is a fundamental

system of orthogonal idempotents of A and for each $i, b_i \in B$. We express such an element as a formal sum $\sum_{i \in I} e_i b_i$. Let $\varphi : A \rightarrow R$ be a morphism of $\mathcal{R}\mathcal{A}_K$, the restriction of $\sum_{i \in I} e_i b_i \in \tilde{\mathbf{P}}(A)$ along φ is given by $(\sum_{i \in I} e_i b_i)\varphi = \sum_{i \in I} \varphi(e_i) b_i \in \tilde{\mathbf{P}}(R)$. In particular with canonical morphisms $\varphi_i : A \rightarrow A/\langle 1 - e_i \rangle$, one has for any $j \in I$ that $(\sum_{i \in I} e_i b_i)\varphi_j = b_j \in \tilde{\mathbf{P}}(A/\langle 1 - e_j \rangle)$. Two elements $\sum_{i \in I} e_i b_i \in \tilde{\mathbf{P}}(A)$ and $\sum_{j \in J} d_j c_j \in \tilde{\mathbf{P}}(A)$ are equal if and only if $\forall i \in I, j \in J [b_i \neq d_j \Rightarrow e_i d_j = 0]$.

To prove that $\tilde{\mathbf{P}}$ is a sheaf we will need the following lemmas.

Lemma 5.1. *Let R be a regular ring and let $(e_i)_{i \in I}$ be a fundamental system of orthogonal idempotents of R . Let $R_i = R/\langle 1 - e_i \rangle$ and $([d_j])_{j \in J_i}$ be a fundamental system of orthogonal idempotents of R_i , where $[d_j] = d_j + \langle 1 - e_i \rangle$. The family $(e_i d_j)_{i \in I, j \in J_i}$ is a fundamental system of orthogonal idempotents of R .*

Proof. In R one has $\sum_{j \in J_i} e_i d_j = e_i \sum_{j \in J_i} d_j = e_i(1 + \langle 1 - e_i \rangle) = e_i$. Hence, $\sum_{i \in I, j \in J_i} e_i d_j = \sum_{i \in I} e_i = 1$. For some $i \in I$ and $t, k \in J_i$ we have $(e_i d_t)(e_i d_k) = e_i(0 + \langle 1 - e_i \rangle) = 0$ in R . Thus for $i, \ell \in I, j \in J_i$ and $s \in J_\ell$ one has $i \neq \ell \vee j \neq s \Rightarrow (e_i d_j)(e_\ell d_s) = 0$. $\square$

Lemma 5.2. *Let R be a regular ring, $f \in R[Z]$ a polynomial of formal degree n and $p \in R[Z]$ a monic polynomial of degree $m > n$. If in $R[X, Y]$ one has $f(Y)(1 - f(X)) = 0 \pmod{\langle p(X), p(Y) \rangle}$ then $f = e \in R$ with e an idempotent.*

Proof. Let $f(Z) = \sum_{i=0}^n r_i Z^i$. By the assumption, for some $q, g \in R[X, Y]$

$$f(Y)(1 - f(X)) = \sum_{i=0}^n r_i (1 - \sum_{j=0}^n r_j X^j) Y^i = qp(X) + gp(Y)$$

One has $\sum_{i=0}^n r_i (1 - \sum_{j=0}^n r_j X^j) Y^i = g(X, Y)p(Y) \pmod{\langle p(X) \rangle}$. Since $p(Y)$ is monic of Y -degree greater than n , one has that $r_i (1 - \sum_{j=0}^n r_j X^j) = 0 \pmod{\langle p(X) \rangle}$ for all $0 \leq i \leq n$. But this means that $r_i r_n X^n + r_i r_{n-1} X^{n-1} + \dots + r_i r_0 - r_i$ is divisible by $p(X)$ for all $0 \leq i \leq n$ which because $p(X)$ is monic of degree $m > n$ implies that all coefficients are equal to 0. In particular, for $1 \leq i \leq n$ one gets that $r_i^2 = 0$ and hence $r_i = 0$ since R is reduced. For $i = 0$ we have $r_0 r_0 - r_0 = 0$ and thus r_0 is an idempotent of R . $\square$

Lemma 5.3. *The presheaf $\tilde{\mathbf{P}}$ described above is a sheaf on $(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$.*

Proof. By case analysis on Definition 3.7.

(i.) Let $\{R \xrightarrow{\varphi_i} R/\langle 1 - e_i \rangle\}_{i \in I} \in \mathbf{J}^{op}(R)$ where $(e_i)_{i \in I}$ be a fundamental system of orthogonal idempotents of an object R . Let $R/\langle 1 - e_i \rangle = R_i$. Since $\tilde{\mathbf{P}}(0) = 1$ by Lemma 3.9 any set $\{s_i \in \tilde{\mathbf{P}}(R_i)\}_{i \in I}$ is compatible. For each i , Let $s_i = \sum_{j \in J_i} [d_j] b_j$. By Lemma 5.1 we have an element $s = \sum_{i \in I, j \in J_i} (e_i d_j) b_j \in \tilde{\mathbf{P}}(R)$ the restriction of which along φ_i is the element $\sum_{j \in J_i} [d_j] b_j \in \tilde{\mathbf{P}}(R_i)$.

It remains to show that this is the only such element. Let there be an element $\sum_{\ell \in L} c_\ell a_\ell \in \tilde{\mathbf{P}}(R)$ that restricts to $u_i = s_i$ along φ_i . We have $u_i = \sum_{\ell \in L} [c_\ell] a_\ell$. One has that for any $j \in J_i$ and $\ell \in L$, $b_j \neq a_\ell \Rightarrow [c_\ell d_j] = 0$ in R_i , hence, in R one has $b_j \neq a_\ell \Rightarrow c_\ell d_j = r(1 - e_i)$. Multiplying both sides of $c_\ell d_j = r(1 - e_i)$ by e_i we get $b_j \neq a_\ell \Rightarrow c_\ell (e_i d_j) = 0$. Thus proving $s = \sum_{\ell \in L} c_\ell a_\ell$.

(ii.) Let $\{\varphi : R \rightarrow R[a] = R[X]/\langle p \rangle\} \in \mathbf{J}^{op}(R)$ where $p \in R[X]$ is monic non-constant and separable. Let the singleton $\{s = \sum_{i \in I} e_i b_i \in \tilde{\mathbf{P}}(R[a])\}$ be compatible. We can assume w.l.o.g. that $\forall i, j \in I [i \neq j \Rightarrow b_i \neq b_j]$ since if $b_k = b_\ell$ one has that $(e_k + e_\ell) b_l + \sum_{j \in I, j \neq k} e_j b_j = s$. (Note that an idempotent e_i of $R[a]$ is a polynomial $e_i(a)$ in a of formal degree less than $\deg p$). Let $R[c, d] =$

$R[X, Y]/\langle p(X), p(Y) \rangle$, by Corollary 3.12, one has a pushout diagram $R \xrightarrow{\varphi} R[a] \xrightarrow[\vartheta]{\zeta} R[c, d]$ where $\zeta|_R = \vartheta|_R = 1_R$, $\zeta(a) = d$ and $\vartheta(a) = c$. That the singleton $\{s\}$ is compatible then means $s\vartheta = \sum_{i \in I} e_i(c)b_i = s\zeta = \sum_{i \in I} e_i(d)b_i$, i.e. $\forall i, j \in I [b_i \neq b_j \Rightarrow e_i(c)e_j(d) = 0]$. By the assumption that $b_i \neq b_j$ whenever $i \neq j$ we have in $R[c, d]$ that $e_j(d)e_i(c) = 0$ for any $i \neq j \in I$. Thus $e_j(d)\sum_{i \neq j} e_i(c) = e_j(d)(1 - e_j(c)) = 0$, i.e. in $R[X, Y]$ one has $e_j(Y)(1 - e_j(X)) = 0 \mod \langle p(X), p(Y) \rangle$. By Lemma 5.2 we have that $e_j \in R$. We have thus shown s is equal to $\sum_{j \in J} d_j b_j \in \tilde{\mathbf{P}}(R[a])$ such that $d_j \in R$ for $j \in J$. That is $\sum_{j \in J} d_j b_j \in \tilde{\mathbf{P}}(R)$. Thus we have found a unique (since $\tilde{\mathbf{P}}(\varphi)$ is injective) element in $\tilde{\mathbf{P}}(R)$ restricting to s along φ . $\square$

Lemma 5.4. *Let $\mathbf{P}$ and $\tilde{\mathbf{P}}$ be as described above. Let $\Gamma : \mathbf{P} \rightarrow \tilde{\mathbf{P}}$ be the presheaf morphism such that $\Gamma_R(b) = b \in \tilde{\mathbf{P}}(R)$ for any object R and $b \in B$. If $\mathbf{E}$ is a sheaf and $\Lambda : \mathbf{P} \rightarrow \mathbf{E}$ is a morphism of presheaves, then there exist a unique sheaf morphism $\Delta : \tilde{\mathbf{P}} \rightarrow \mathbf{E}$ such that the following diagram, of $\mathbf{Set}^{\mathcal{R}\mathcal{A}_K}$, commutes.*

$$\begin{array}{ccc} \mathbf{P} & \xrightarrow{\Lambda} & \mathbf{E} \\ \downarrow \Gamma & \nearrow \Delta & \\ \tilde{\mathbf{P}} & & \end{array}$$

That is to say, $\Gamma : \mathbf{P} \rightarrow \tilde{\mathbf{P}}$ is the sheafification of $\mathbf{P}$.

Proof. Let $a = \sum_{i \in I} e_i b_i \in \tilde{\mathbf{P}}(A)$ and let $A_i = A/\langle 1 - e_i \rangle$ with canonical morphisms $\varphi_i : A \rightarrow A_i$.

Let $\mathbf{E}$ and Λ be as in the statement of the lemma. If there exist a sheaf morphism $\Delta : \tilde{\mathbf{P}} \rightarrow \mathbf{E}$, then Δ being a natural transformation forces us to have for all $i \in I$, $\mathbf{E}(\varphi_i)\Delta_A = \Delta_{A_i}\tilde{\mathbf{P}}(\varphi_i)$. By Lemma 3.10, we know that the map $d \in \mathbf{E}(A) \mapsto (\mathbf{E}(\varphi_i)d \in \mathbf{E}(A_i))_{i \in I}$ is an isomorphism. Thus it must be that $\Delta_A(a) = (\Delta_{A_i}\tilde{\mathbf{P}}(\varphi_i)(a))_{i \in I} = (\Delta_{A_i}(b_i))_{i \in I}$. But $\Delta_{A_i}(b_i) = \Delta_{A_i}\Gamma_{A_i}(b_i)$. To have $\Delta\Gamma = \Lambda$ we must have $\Delta_{A_i}(b_i) = \Lambda_{A_i}(b_i)$. Hence, we are forced to have $\Delta_A(a) = (\Lambda_{A_i}(b_i))_{i \in I}$. Note that Δ is unique since its value $\Delta_A(a)$ at any A and a is forced by the commuting diagram above. $\square$

The constant presheaf of natural numbers $\mathbf{N}$ is the natural numbers object in $\mathbf{Set}^{\mathcal{R}\mathcal{A}_K}$. We associate to $\mathbf{N}$ a sheaf $\tilde{\mathbf{N}}$ as described above. From Lemma 5.4 one can easily show that $\tilde{\mathbf{N}}$ satisfy the axioms of a natural numbers object in $\mathbf{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$.

Definition 5.5. Let $\mathbf{F}[[X]]$ be the presheaf mapping each object R of $\mathcal{R}\mathcal{A}_K$ to $\mathbf{F}[[X]](R) = R[[X]] = R^{\mathbb{N}}$ with the obvious restriction maps.

Lemma 5.6. $\mathbf{F}[[X]]$ is a sheaf.

Proof. The proof is immediate as a corollary of Lemma 4.2. $\square$

Lemma 5.7. The sheaf $\mathbf{F}[[X]]$ is naturally isomorphic to the sheaf $\mathbf{F}^{\tilde{\mathbf{N}}}$.

Proof. Let C be an object of $\mathcal{R}\mathcal{A}_K^{op}$. Since $\mathbf{F}^{\tilde{\mathbf{N}}}(C) \cong \mathbf{y}_C \times \tilde{\mathbf{N}} \rightarrow \mathbf{F}$, an element $\alpha_C \in \mathbf{F}^{\tilde{\mathbf{N}}}(C)$ is a family of elements of the form $\alpha_{C,D} : \mathbf{y}_C(D) \times \tilde{\mathbf{N}}(D) \rightarrow \mathbf{F}(D)$ where D is an object of $\mathcal{R}\mathcal{A}_K^{op}$. Define $\Theta : \mathbf{F}^{\tilde{\mathbf{N}}} \rightarrow \mathbf{F}[[X]]$ as $(\Theta\alpha)_C(n) = \alpha_{C,C}(1_C, n)$. Define $\Lambda : \mathbf{F}[[X]] \rightarrow \mathbf{F}^{\tilde{\mathbf{N}}}$ as

$$(\Lambda\beta)_{C,D}(C \xrightarrow{\varphi} D, \sum_{i \in I} e_i n_i) = (\vartheta_i \varphi(\beta_C(n_i)))_{i \in I} \in \mathbf{F}(D)$$

where $D \xrightarrow{\vartheta_i} D/\langle 1 - e_i \rangle$ is the canonical morphism. Note that by Lemma 3.10 one indeed has that $(\vartheta_i \varphi(\beta_C(n_i)))_{i \in I} \in \prod_{i \in I} \mathbf{F}(D_i) \cong \mathbf{F}(D)$. One can easily verify that Θ and Λ are natural. It remains to show the isomorphism. On one hand we have

$$\begin{aligned} (\Lambda \Theta \alpha)_{C,D}(\varphi, \sum_{i \in I} e_i n_i) &= (\vartheta_i \varphi((\Theta \alpha)_C(n_i)))_{i \in I} = (\vartheta_i \varphi(\alpha_{C,C}(1_C, n_i)))_{i \in I} \\ &= ((\alpha_{C,D_i}(\vartheta_i \varphi, n_i)))_{i \in I} = \alpha_{C,D}(\varphi, \sum_{i \in I} e_i n_i) \end{aligned}$$

Thus showing $\Lambda \Theta = 1_{\mathbf{F}^{\mathbf{N}}}$. On the other hand, $(\Theta \Lambda \beta)_C(n) = (\Lambda \beta)_{C,C}(1_C, n) = 1_C 1_C(\beta_C(n)) = \beta_C(n)$. Thus $\Theta \Lambda = 1_{\mathbf{F}[[X]]}$. $\square$

Lemma 5.8. *The power series object $\mathbf{F}[[X]]$ is a ring object.*

Proof. A Corollary to Lemma 4.4. $\square$

6 Choice axioms

The axiom of choice fails to hold (even in a classical metatheory) in the topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$ whenever the field K is not algebraically closed. To show this we will show that there is an epimorphism in $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$ with no section.

Fact 6.1. *Let $\Theta : \mathbf{P} \rightarrow \mathbf{G}$ be a morphism of sheaves on a site $(\mathcal{C}, \mathbf{J})$. Then Θ is an epimorphism if and only if for each object C of $\mathcal{C}$ and each element $c \in \mathbf{G}(C)$ there is a cover S of C such that for all $f : D \rightarrow C$ in the cover S the element cf is in the image of Θ_D . [10, Ch. 3].*

Lemma 6.2. *Let K be a field of characteristic 0 not algebraically closed. There is an epimorphism in $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$ with no section.*

Proof. Let $f = X^n + \sum_{i=1}^n r_i X^{n-i}$ be a non-constant polynomial for which no root in K exist. w.l.o.g. we assume f separable. One can construct $\Lambda : \mathbf{F} \rightarrow \mathbf{F}$ defined by $\Lambda_C(c) = c^n + \sum_{i=1}^{n-1} r_i c^{n-i} \in C$. Given $d \in \mathbf{F}(C)$, let $g = X^n + \sum_{i=1}^{n-1} r_i X^{n-i} - d$. By Corollary 4.8 there is a cover $\{C_\ell \xrightarrow{\varphi_\ell} C\}_{\ell \in L} \in \mathbf{J}(C)$ with $h_\ell \in C_\ell[X]$ a separable non-constant polynomial dividing g . Let $C_\ell[x_\ell] = C_\ell[X]/\langle h_\ell \rangle$ one has a singleton cover $\{C_\ell[x_\ell] \xrightarrow{\vartheta_\ell} C_\ell\}$ and thus a composite cover $\{C_\ell[x_\ell] \xrightarrow{\vartheta_\ell \varphi_\ell} C\}_{\ell \in L} \in \mathbf{J}(C)$. Since x_ℓ is a root of $h_\ell \mid g$ we have $\Lambda_{C_\ell[x_\ell]}(x_\ell) = x_\ell^n + \sum_{i=1}^{n-1} r_i x_\ell^{n-i} = d$ or more precisely $\Lambda_{C_\ell[x_\ell]}(x_\ell) = d \varphi_\ell \vartheta_\ell$. Thus, Λ is an epimorphism (by Fact 6.1) and it has no section, for if it had a section $\Psi : \mathbf{F} \rightarrow \mathbf{F}$ then one would have $\Psi_K(-r_n) = a \in K$ such that $a^n + \sum_{i=1}^n r_i a^{n-i} = 0$ which is not true by assumption. $\square$

Theorem 6.3. *Let K be a field of characteristic 0 not algebraically closed. The axiom of choice fails to hold in the topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$.* $\square$

We note that in Per Martin-Löf type theory one can show that (see [13])

$$(\prod x \in A)(\sum y \in B[x])C[x, y] \Rightarrow (\sum f \in (\prod x \in A)B[x])(\prod x \in A)C[x, f(x)]$$

As demonstrated in the topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$ we have an example of an intuitionistically valid formula of the form $\forall x \exists y \phi(x, y)$ where no function f exist for which $\exists f \forall x \phi(x, f(x))$ holds.

We demonstrate further that when the base field is $\mathbb{Q}$ the weaker axiom of *dependent choice* does not hold in the topos $\text{Sh}(\mathcal{R}\mathcal{A}_{\mathbb{Q}}^{op}, \mathbf{J})$. For a relation $R \subset Y \times Y$ the axiom of dependent choice is stated as

$$\forall x \exists y R(x, y) \Rightarrow \forall x \exists g \in Y^{\mathbf{N}} [g(0) = x \wedge \forall n R(g(n), g(n+1))] \quad (\text{ADC})$$

Theorem 6.4. $\text{Sh}(\mathcal{R}\mathcal{A}_{\mathbb{Q}}^{\text{op}}, \mathbf{J}) \Vdash \neg \text{ADC}$.

Proof. Consider the binary relation on the algebraically closed object $\mathbf{F}$ defined by the characteristic function $\phi(x, y) := y^2 - x = 0$. Assume $C \Vdash \text{ADC}$ for some object C of $\mathcal{R}\mathcal{A}_K$. Since $C \Vdash \forall x \exists y [y^2 - x = 0]$ we have $C \Vdash \forall x \exists g \in \mathbf{F}^{\tilde{\mathbf{N}}}[g(0) = x \wedge \forall n [g(n)^2 = g(n+1)]]$. That is for all morphisms $C \xrightarrow{\xi} A$ of $\mathcal{R}\mathcal{A}_K$ and elements $a \in \mathbf{F}(A)$ one has $A \Vdash \exists g \in \mathbf{F}^{\tilde{\mathbf{N}}}[g(0) = a \wedge \forall n [g(n)^2 = g(n+1)]]$. Taking $a = 2$ we have $A \Vdash \exists g \in \mathbf{F}^{\tilde{\mathbf{N}}}[g(0) = 2 \wedge \forall n [g(n)^2 = g(n+1)]]$. Which by $\boxed{\exists}$ implies the existence of a cocover $\{\eta_i : A \rightarrow A_i \mid i \in I\}$ and power series $\alpha_i \in \mathbf{F}^{\tilde{\mathbf{N}}}(A_i)$ such that $A_i \Vdash \alpha_i(0) = 2 \wedge \forall n [\alpha_i(n)^2 = \alpha_i(n+1)]$. By Lemma 5.7 we have $\mathbf{F}^{\tilde{\mathbf{N}}}(A_i) \cong A_i[[X]]$ and thus the above forcing implies the existence of a series $\alpha_i = 2 + 2^{1/2} + \dots + 2^{1/2^j} + \dots \in A_i[[X]]$. But this holds only if A_i contains a root of $X^{2^j} - 2$ for all j which implies A_i is trivial as will shortly show after the following remark.

Consider an algebra R over $\mathbb{Q}$. Assume R contains a root of $X^{2^n} - 2$ for some n . Then letting $\mathbb{Q}[x] = \mathbb{Q}[X]/\langle X^{2^n} - 2 \rangle$, one will have a homomorphism $\xi : \mathbb{Q}[x] \rightarrow R$. By Eisenstein's criterion the polynomial $X^{2^n} - 2$ is irreducible over $\mathbb{Q}$, making $\mathbb{Q}[x]$ a field of dimension 2^n and ξ either an injection with a trivial kernel or $\xi = \mathbb{Q}[x] \rightarrow 0$.

Now we continue with the proof. Until now we have shown that for all $i \in I$, the algebra A_i contains a root of $X^{2^j} - 2$ for all j . For each $i \in I$, let A_i be of dimension m_i over $\mathbb{Q}$. We have that A_i contains a root of $X^{2^{m_i}} - 2$ and we have a homomorphism $\mathbb{Q}(\sqrt[2^{m_i}]{2}) \rightarrow A_i$ which since A_i has dimension $m_i < 2^{m_i}$ means that A_i is trivial for all $i \in I$. Hence, $A_i \Vdash \perp$ and consequently $C \Vdash \perp$. We have shown that for any object D of $\mathcal{R}\mathcal{A}_{\mathbb{Q}}^{\text{op}}$ if $D \Vdash \text{ADC}$ then $D \Vdash \perp$. Hence $\text{Sh}(\mathcal{R}\mathcal{A}_{\mathbb{Q}}^{\text{op}}, \mathbf{J}) \Vdash \neg \text{ADC}$. $\square$

7 Eliminating the algebraic closure assumption

Let K be a field of characteristic 0. We consider a typed language $\mathcal{L}[N, F]_K$ of the form described in Section 2 with two basic types N and F and the elements of the field K as its set of constants. Consider a theory T in the language $\mathcal{L}[N, F]_K$, such that T has as an axiom every atomic formula or the negation of one valid in the field K , T equips N with the (Peano) axioms of natural numbers and equips F with the axioms of a field containing K . If we interpret the types N and F by the objects $\tilde{\mathbf{N}}$ and $\mathbf{F}$, respectively, in the topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{\text{op}}, \mathbf{J})$ then we have, by the results proved earlier, a model of T in $\text{Sh}(\mathcal{R}\mathcal{A}_K^{\text{op}}, \mathbf{J})$. Let AlgCl be the axiom schema of algebraic closure with quantification over the type F , then one has that $T + \text{AlgCl}$ has a model in $\text{Sh}(\mathcal{R}\mathcal{A}_K^{\text{op}}, \mathbf{J})$ with the same interpretation. Let ϕ be a sentence in the language such that $T + \text{AlgCl} \vdash \phi$ in IHOL deduction system. By soundness [1] one has that $\text{Sh}(\mathcal{R}\mathcal{A}_K^{\text{op}}, \mathbf{J}) \Vdash \phi$, i.e. for all finite dimensional regular algebras R over K , $R \Vdash \phi$ which is then a constructive interpretation of the existence of the algebraic closure of K .

This model can be implemented, e.g. in Haskell. In the paper [12] by the authors, an algorithm for computing the Puiseux expansions of an algebraic curve based on this model is given. The statement with the assumption of algebraic closure is:

“ Let K be a field of characteristic 0 and $G(X, Y) = Y^n + \sum_{i=1}^n b_i(X)Y^{n-i} \in K[[X]][Y]$ a monic, non-constant polynomial separable over $K((X))$. Let F be the algebraic closure of K , we have a positive integer m and a factorization $G(T^m, Y) = \prod_{i=1}^n (Y - \alpha_i)$ with $\alpha_i \in F[[T]]$ ”

We can then extract the following computational content

“ Let K be a field of characteristic 0 and $G(X, Y) = Y^n + \sum_{i=1}^n b_i(X)Y^{n-i} \in K[[X]][Y]$ a monic, non-constant polynomial separable over $K((X))$. Then there exist a (von Neumann) regular algebra R over K and a positive integer m such that $G(T^m, Y) = \prod_{i=1}^n (Y - \alpha_i)$ with $\alpha_i \in R[[T]]$ ”

For example applying the algorithm to $G(X, Y) = Y^4 - 3Y^2 + XY + X^2 \in \mathbb{Q}[X, Y]$ we get a regular algebra $\mathbb{Q}[b, c]$ with $b^2 - 13/36 = 0$ and $c^2 - 3 = 0$ and a factorization

$$\begin{aligned} G(X, Y) = & (Y + (-b - \frac{1}{6})X + (-\frac{31}{351}b - \frac{7}{162})X^3 + (-\frac{1415}{41067}b - \frac{29}{1458})X^5 + \dots) \\ & (Y + (b - \frac{1}{6})X + (\frac{31}{351}b - \frac{7}{162})X^3 + (\frac{1415}{41067}b - \frac{29}{1458})X^5 + \dots) \\ & (Y - c + \frac{1}{6}X + \frac{5}{72}cX^2 + \frac{7}{162}X^3 + \frac{185}{10368}cX^4 + \frac{29}{1458}X^5 + \dots) \\ & (Y + c + \frac{1}{6}X - \frac{5}{72}cX^2 + \frac{7}{162}X^3 - \frac{185}{10368}cX^4 + \frac{29}{1458}X^5 + \dots) \end{aligned}$$

Another example of a possible application of this model is as follows: suppose one want to show that

“For discrete field K , if $f \in K[X, Y]$ is smooth, i.e. $1 \in \langle f, f_x, f_y \rangle$, then $K[X, Y]/\langle f \rangle$ is a Prüfer ring.”

To prove that a ring is Prüfer one needs to prove that it is arithmetical, that is $\forall x, y \exists u, v, w [yu = vx \wedge yw = (1 - u)x]$. Proving that $K[X, Y]/\langle f \rangle$ is arithmetical is easier in the case where K is algebraically closed [3]. Let $\mathbf{F}$ be the algebraic closure of K in $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$. Now $\mathbf{F}[X, Y]/\langle f \rangle$ being arithmetical amounts to having a solution u, v , and w to a linear system $yu = vx$, $yw = (1 - u)x$. Having obtained such solution, by Rouché–Capelli–Fontené theorem we can conclude that the system have a solution in $K[X, Y]/\langle f \rangle$.

8 The logic of $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$

In this section we will demonstrate that in a *classical metatheory* one can show that the topos $\text{Sh}(\mathcal{R}\mathcal{A}_K^{op}, \mathbf{J})$ is boolean. In fact we will show that, in a classical metatheory, the boolean algebra structure of the subobject classifier is the one specified by the boolean algebra of idempotents of the algebras in $\mathcal{R}\mathcal{A}_K$. Except for Theorem 8.8 the reasoning in this section is classical. Recall that the idempotents of a commutative ring form a boolean algebra with the meaning of the logical operators given by : $\top = 1$, $\perp = 0$, $e_1 \wedge e_2 = e_1 e_2$, $e_1 \vee e_2 = e_1 + e_2 - e_1 e_2$ and $\neg e = 1 - e$. We write $e_1 \leq e_2$ iff $e_1 \wedge e_2 = e_1$ and $e_1 \vee e_2 = e_2$.

A sieve S on an object C is a set of morphisms with codomain C such that if $g \in S$ and $\text{cod}(h) = \text{dom}(g)$ then $gh \in S$. A cosieve is defined dually to a sieve. A sieve S is said to cover a morphism $f : D \rightarrow C$ if $f^*(S) = \{g \mid \text{cod}(g) = D, fg \in S\}$ contains a cover of D . Dually, a cosieve M on C is said to cover a morphism $g : C \rightarrow D$ if the sieve dual to M covers the morphism dual to g .

Definition 8.1 (Closed cosieve). A sieve M on an object C of $\mathcal{C}$ is closed if for all f with $\text{cod}(f) = C$ if M covers f then $f \in M$. A closed cosieve on an object C of $\mathcal{C}^{op}$ is the dual of a closed sieve in $\mathcal{C}$.

Fact 8.2 (Subobject classifier). The subobject classifier in the category of sheaves on a site $(\mathcal{C}, \mathbf{J})$ is the presheaf Ω where for an object C of $\mathcal{C}$ the set $\Omega(C)$ is the set of closed sieves on C and for each $f : D \rightarrow C$ we have a restriction map $M \mapsto \{h \mid \text{cod}(h) = D, fh \in M\}$.

Lemma 8.3. Let R be an object of $\mathcal{R}\mathcal{A}_K$. If R is a field the closed cosieves on R are the maximal cosieve $\{f \mid \text{dom}(f) = R\}$ and the minimal cosieve $\{R \rightarrow 0\}$.

Proof. Let S be a closed cosieve on R and let $\varphi : R \rightarrow A \in S$ and let I be a maximal ideal of A . If A is nontrivial we have a field morphism $R \rightarrow A/I$ in S where A/I is a finite field extension of R . Let $A/I = R[a_1, \dots, a_n]$. But then the morphism $\vartheta : R \rightarrow R[a_1, \dots, a_{n-1}]$ is covered by S . Thus $\vartheta \in S$ since S is closed. By induction on n we get that a field automorphism $\eta : R \rightarrow R$ is in S but then by composition of η with its inverse we get that $1_R \in S$. Consequently, any morphism with domain R is in S . $\square$

Corollary 8.4. *For an object R of $\mathcal{RA}_K$. If R is a field $\Omega(R)$ is a 2-valued boolean algebra.*

Proof. This is a direct Corollary of Lemma 8.3. The maximal cosieve (1_R) correspond to the idempotent 1 of R , that is the idempotent e such that, $\ker 1_R = \langle 1 - e \rangle$. Similarly the cosieve $\{R \rightarrow 1\}$ correspond to the idempotent 0. $\square$

Corollary 8.5. *For an object A of $\mathcal{RA}_K$, $\Omega(A)$ is isomorphic to the set of idempotents of A and the Heyting algebra structure of $\Omega(A)$ is the boolean algebra of idempotents of A .*

Proof. Classically a finite dimension regular algebra over K is isomorphic to a product of field extensions of K . Let A be an object of $\mathcal{RA}_K$, then $A \cong F_1 \times \dots \times F_n$ where F_i is a finite field extension of K . The set of idempotents of A is $\{(d_1, \dots, d_n) \mid 1 \leq j \leq n, d_j \in F_j, d_j = 0 \text{ or } d_j = 1\}$. But this is exactly the set $\Omega(F_1) \times \dots \times \Omega(F_n) \cong \Omega(A)$. It is obvious that since $\Omega(A)$ is isomorphic to a product of boolean algebras, it is a boolean algebra with the operators defined pointwise. $\square$

Theorem 8.6. *The topos $\text{Sh}(\mathcal{RA}_K^{op}, \mathbf{J})$ is boolean.*

Proof. The subobject classifier of $\text{Sh}(\mathcal{RA}_K^{op}, \mathbf{J})$ is $1 \xrightarrow{\text{true}} \Omega$ where for an object A of $\mathcal{RA}_K$ one has $\text{true}_A(*) = 1 \in A$. $\square$

It is not possible to show that the topos $\text{Sh}(\mathcal{RA}_K^{op}, \mathbf{J})$ is boolean in an intuitionistic metatheory as we shall demonstrate. First we recall the definition of the *Limited principle of omniscience* (LPO for short).

Definition 8.7 (LPO). For any binary sequence α the statement $\forall n[\alpha(n) = 0] \vee \exists n[\alpha(n) = 1]$ holds.

LPO cannot be shown to hold intuitionistically. One can, nevertheless, show that it is weaker than the law of excluded middle [2].

Theorem 8.8. *Intuitionistically, if $\text{Sh}(\mathcal{RA}_K^{op}, \mathbf{J})$ is boolean then LPO holds.*

Proof. Let $\alpha \in K[[X]]$ be a binary sequence. By Lemma 5.7 one has an isomorphism $\Lambda : \mathbf{F}[[X]] \xrightarrow{\sim} \mathbf{F}^{\tilde{N}}$. Let $\Lambda_K(\alpha) = \beta \in \mathbf{F}^{\tilde{N}}(K)$. Assume the topos $\text{Sh}(\mathcal{RA}_K^{op}, \mathbf{J})$ is boolean. Then one has $K \Vdash \forall n[\beta(n) = 0] \vee \exists n[\beta(n) = 1]$. By $\boxed{\vee}$ this holds only if there exist a cocover of K

$$\{\vartheta_i : K \rightarrow A_i \mid i \in I\} \cup \{\xi_j : K \rightarrow B_j \mid j \in J\}$$

such that $B_j \Vdash \forall n[(\beta \xi_j)(n) = 0]$ for all $j \in J$ and $A_i \Vdash \exists n[(\beta \vartheta_i)(n) = 1]$ for all $i \in I$. Note that at least one of I or J is nonempty since K is not covered by the empty cover.

For each $i \in I$ there exist a cocover $\{\eta_\ell : A_i \rightarrow D_\ell \mid \ell \in L\}$ of A_i such that for all $\ell \in L$, we have $D_\ell \Vdash (\beta \vartheta_i \eta_\ell)(m) = 1$ for some $m \in \tilde{N}(D_\ell)$. Let $m = \sum_{t \in T} e_t n_t$ then we have a cocover $\{\xi_t : D_\ell \rightarrow C_t = D_\ell / \langle 1 - e_t \rangle \mid t \in T\}$ such that $C_t \Vdash (\beta \vartheta_i \eta_\ell \xi_t)(n_t) = 1$ which implies $\xi_t \eta_\ell \vartheta_i(\alpha(n_t)) = 1$. For each t we can check whether $\alpha(n_t) = 1$. If $\alpha(n_t) = 1$ then we have witness for $\exists n[\alpha(n) = 1]$. Otherwise, we have $\alpha(n_t) = 0$ and $\xi_t \eta_\ell \vartheta_i(0) = 1$. Thus the map $\xi_t \eta_\ell \vartheta_i : K \rightarrow C_t$ from the field K cannot be injective, which leaves us with the conclusion that C_t is trivial. If for all $t \in T$, C_t is trivial then D_ℓ is trivial as well. Similarly, if for every $\ell \in L$, D_ℓ is trivial then A_i is trivial as well. At this point one either have either (i) a natural number m such that $\alpha(m) = 1$ in which case we have a witness for $\exists n[\alpha(n) = 1]$. Or (ii) we have shown that for all $i \in I$, A_i is trivial in which case we have a cocover $\{\xi_j : K \rightarrow B_j \mid j \in J\}$ such that $B_j \Vdash \forall n[(\beta \xi_j)(n) = 0]$ for all $j \in J$. Which by $\boxed{\text{LC}}$ means $K \Vdash \forall n[\beta(n) = 0]$ which by $\boxed{\vee}$ means that for all arrows $K \rightarrow R$ and elements $d \in \tilde{N}(R)$, $R \Vdash \beta(d) = 0$. In particular for the arrow $K \xrightarrow{1_K} K$ and every natural number m one has $K \Vdash \beta(m) = 0$ which implies $K \Vdash \alpha(m) = 0$. By $\boxed{=}$ we get that $\forall m \in \mathbb{N}[\alpha(m) = 0]$. Thus we have shown that LPO holds. $\square$

Corollary 8.9. *It cannot be shown in an intuitionistic metatheory that the topos $\text{Sh}(\mathcal{RA}_K^{\text{op}}, \mathbf{J})$ is boolean.* $\square$

References

- [1] Steven Awodey (1997): *Logic in topoi: Functorial Semantics for Higher-Order Logic*. Ph.D. thesis, The University of Chicago.
- [2] Douglas Bridges & Fred Richman (1987): *Varieties of Constructive Mathematics*. Lecture note series, Cambridge University Press, doi:10.1017/cbo9780511565663.
- [3] Thierry Coquand, Henri Lombardi & Claude Quitté (2010): *Curves and coherent Prüfer rings*. *J. Symb. Comput.* 45(12), pp. 1378–1390, doi:10.1016/j.jsc.2010.06.016.
- [4] Michel Coste, Henri Lombardi & Marie-Françoise Roy (2001): *Dynamical method in algebra: effective Nullstellensätze*. *Annals of Pure and Applied Logic* 111(3), pp. 203 – 256, doi:10.1016/S0168-0072(01)00026-4.
- [5] Jean Della Dora, Claire Dicrescenzo & Dominique Duval (1985): *About a new method for computing in algebraic number fields*. In Bob Caviness, editor: *EUROCAL '85, Lecture Notes in Computer Science* 204, Springer Berlin / Heidelberg, pp. 289–290, doi:10.1007/3-540-15984-3_279.
- [6] A. Fröhlich & J. C. Shepherdson (1956): *Effective Procedures in Field Theory*. *Philosophical Transactions of the Royal Society of London. Series A, Mathematical and Physical Sciences* 248(950), pp. 407–432, doi:10.1098/rsta.1956.0003.
- [7] Peter T. Johnstone (2002): *Sketches of an Elephant: A Topos Theory Compendium - Volume 2*. *Oxford Logic Guides* 44, Oxford University Press.
- [8] John F. Kennison (1982): *Separable algebraic closure in a topos*. *Journal of Pure and Applied Algebra* 24(1), pp. 7 – 24, doi:10.1016/0022-4049(82)90055-X.
- [9] Henri Lombardi & Claude Quitté (2011): *Algèbre Commutative, Méthodes Constructives*. *Mathématiques en devenir*, Calvage et Mounet.
- [10] Saunders MacLane & Ieke Moerdijk (1992): *Sheaves in Geometry and Logic: A First Introduction to Topos Theory*, corrected edition. Springer, doi:10.1007/978-1-4612-0927-0.
- [11] Michael Makkai & Gonzalo E. Reyes (1977): *First order categorical logic: model-theoretical methods in the theory of topoi and related categories*. *Lecture notes in mathematics* 611, Springer-Verlag, doi:10.1007/BFb0066201.
- [12] Bassel Manna & Thierry Coquand (2013): *Dynamic Newton-Puiseux theorem*. *J. Logic & Analysis* 5, doi:10.4115/jla.2013.5.5.
- [13] Per Martin-Löf (1972): *An intuitionistic theory of types*. Reprinted in *Twenty-five years of constructive type theory*, Oxford University Press, 1998, 127–172.
- [14] Ray Mines, Fred Richman & Wim Ruitenburg (1988): *A course in constructive algebra*. Universitext (1979), Springer-Verlag, doi:10.1007/978-1-4419-8640-5.
- [15] Andrej Ščedrov (1984): *Forcing and classifying topoi*. *Memoirs of the AMS* 48, American Mathematical Society (AMS), doi:10.1090/memo/0295.