Volume 72 (2026), pp. 353–361
Received: 18 May 2025
Revised: 25 November 2025
Accepted: 26 January 2026
DOI: 10.60866/CAM.293

ZML
Zeitschrift für Mathematische Logik und Grundlagen der Mathematik

Azumaya algebras and Barr's Theorem

Thierry Coquand[(1)] Henri Lombardi[(2)] Stefan Neuwirth[(2)]

[(1)] Institutionen för Data- och Informationsteknik, Chalmers tekniska högskola AB, 412 96 Göteborg, Sweden

[(2)] Laboratoire de mathématiques de Besançon, Université Marie et Louis Pasteur, CNRS, 16 route de Gray, FR-25000 Besançon, France

Abstract. We study étale topology and the notion of Azumaya algebra over a commutative ring constructively. As an application of the syntactic version of Barr's Theorem, we show the equivalence between two definitions of Azumaya algebra.

Introduction

The goal of this paper is to show how one can use the notion of classifying topos of a coherent theory [7; 6; 16], here the theory of separably closed local rings [16], to prove some basic results about Azumaya algebras in a constructive setting.

A fundamental invariant associated to a commutative field F is its *Brauer group*, whose elements are the division algebras over F, up to isomorphism. Alternatively an element of the Brauer group can be described as a central simple algebra, up to Morita equivalence, and the group operation is then the tensor product. Two important characterisations of the notion of central simple algebra are the following:[1]

(1) an algebra A over F which is finitely generated and such that the canonical map $A \otimes_F A^{\mathrm{op}} \to \mathrm{End}_F(A)$ is an isomorphism; or, equivalently,
(2) an algebra A which becomes a matrix algebra over an algebraic extension of F, or, equivalently, which becomes a matrix algebra over an algebraic and separable extension of F.

This notion of central simple algebra over a *field* has been generalised to the notion of Azumaya algebra over an arbitrary *commutative ring* k. The definition is a generalisation of the first characterisation: an algebra A which is finitely generated projective over the ring k and such that the canonical map $A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ is an isomorphism. In this paper, we show in a constructive setting that this definition is equivalent to a suitable generalisation of the second characterisation, using a constructively valid version of Barr's Theorem [7].

1 Some coherent theories

We consider some coherent theories [7] in the language of rings.

1.1 Theory of local rings

The theory of *local rings* can be formulated in a coherent way with the axioms $0 \neq 1$ and $\mathsf{inv}(x) \vee \mathsf{inv}(1-x)$, where $\mathsf{inv}(x)$ denotes $\exists_y\ 1 = xy$. If we add to our language a new predicate $\mathfrak{m}(x)$ with axioms $\mathsf{inv}(x) \vee \mathfrak{m}(x)$

Corresponding author: Thierry Coquand, coquand@chalmers.se

[1] We study these characterisations in a constructive setting in the reference [5].

This article is licensed under the Creative Commons BY 4.0 license.
Copyright is retained by the authors.

and $\neg(\mathfrak{m}(x) \wedge \mathsf{inv}(x))$, then we get the theory of local rings that are *residually discrete*,[2] i.e., where the property of being invertible is now decidable, and the predicate $\mathfrak{m}(x)$ corresponds to the unique maximal ideal of the ring. In this theory, we can express in a coherent way that the ring is Henselian by stating that for any monic polynomial f, if we have u such that $f(u) \in \mathfrak{m}$ and $f'(u) \notin \mathfrak{m}$ then we can find α such that $f(\alpha) = 0$ and $\alpha - u \in \mathfrak{m}$. Equivalently [1], any monic polynomial of degree $\ell + 1$ which is of the form $X^\ell(X-1)$ mod. $\mathfrak{m}$ has a root which is equal to 1 mod. $\mathfrak{m}$. The work [1] shows in a constructive setting for this theory the lifting property for idempotents of a finitely generated commutative algebra over a Henselian local ring.

It does not seem possible, however, to express the property of being Henselian in a coherent way in the language of local rings (i.e., without introducing the predicate $\mathfrak{m}(x)$). Surprisingly, as observed by G. Wraith [16], the property of being *separably closed*, corresponding classically to the property of being Henselian with the residue field being separably closed, *can be* expressed in a coherent way. In this paper, we present some remarks connected to this observation. The first one is a small variation of Wraith's axiomatisation. Both axiomatisations can be used to define the étale site over a ring. Finally, we show in a constructive setting that Azumaya algebras are exactly the algebras that are locally matrix algebras for the étale topology.

1.2 Theory of separably closed local rings

If R is a ring, and $a_1, \ldots, a_n$ elements of R, we write $(a_1, \ldots, a_n)$ for the ideal of R generated by $a_1, \ldots, a_n$. We define, following Joyal [8], the *Zariski spectrum* of R as the universal support $D\colon R \to Z(R)$ over R. A *support* is a map $d\colon R \to M$ into a bounded distributive lattice M satisfying the relations

(1) $d(1) = 1$;
(2) $d(0) = 0$;
(3) $d(a+b) \leqslant d(a) \vee d(b)$;
(4) $d(ab) = d(a) \wedge d(b)$.

We write $d(a_1, \ldots, a_n)$ for $d(a_1) \vee \cdots \vee d(a_n)$. It is direct that $d(a) \leqslant d(a_1, \ldots, a_n)$ as soon as a belongs to the radical of the ideal $(a_1, \ldots, a_n)$. Conversely, it is elementary to check that we get a support if we define $D(a_1, \ldots, a_n)$ to be the radical of the ideal $(a_1, \ldots, a_n)$, and this is a concrete way to build the universal support. In particular, this shows that $D(a_1, \ldots, a_n) = 1$ if, and only if, $(a_1, \ldots, a_n) = 1$. It is also direct, for any support d, to see that $d(a, b) = d(a + b, ab)$, and more generally that $d(a_1, \ldots, a_n) = d(c_1, \ldots, c_n)$, where $c_1, \ldots, c_n$ are the elementary symmetric functions of $a_1, \ldots, a_n$.

For the formulation of the theory of separably closed local rings, we need the notion of universal splitting algebra [10, Sect. III-4] $L = R[x_1, \ldots, x_n] = R[X_1, \ldots, X_n]/I$ of a monic polynomial

$$f = X^n - u_1 X^{n-1} + u_2 X^{n-2} - \cdots$$

in $R[X]$, where I is the ideal generated by $u_1 - \sigma_1, \ldots, u_n - \sigma_n$, with $\sigma_1, \ldots, \sigma_n$ in $R[X_1, \ldots, X_n]$ the elementary symmetric polynomials. We know, using Cauchy modules [10, Fact III-4.3], that L is freely generated of rank $n!$ as a module over R and it follows from this that L is a faithfully flat extension of R.

For the notion of faithfully flat extension, we follow the definition in [10, Sect. VIII-6]: it is a commutative R-algebra $i\colon R \to S$ such that

(1) if u is a row vector in R^n and v a column vector in S^n such that $i(u)v = 0$ then we can find a matrix M with coefficients in R and w such that $uM = 0$ and $v = i(M)w$;
(2) if $i(a)$ belongs to the ideal $(i(a_1), \ldots, i(a_n))$ in S then a belongs to the ideal $(a_1, \ldots, a_n)$ in R.

It then follows [10, Sect. VIII-6] that i is injective. It is also clear from this definition that S is faithfully flat over R when it is a finitely generated free R-module of rank > 0.

[2] The terminology "discrete" for a set with a decidable equality, while conflicting with some topological intuitions, is well established in constructive mathematics since the work of Bishop [3], and we follow this usage in this paper.

We define $\delta_i(f)$ to be the element in R equal to $\sigma_i(f'(x_1),\dots,f'(x_n))$ and $\Delta(f)$ to be $D(\delta_1(f),\dots,\delta_n(f))$. We say that f is *unramifiable* if, and only if, $1=\Delta(f)$. Since $\Delta(f)=D(f'(x_1),\dots,f'(x_n))$, this condition is equivalent to $(f'(x_1),\dots,f'(x_n))=1$ in the universal splitting algebra L. Over a residually discrete local ring with maximal ideal $\mathfrak{m}$, to be unramifiable means that the polynomial f has a simple root in some extension of the residue field $R/\mathfrak{m}$. This holds in classical mathematics, but also constructively with a dynamical interpretation of extensions of $R/\mathfrak{m}$.

Lemma 1. Let R be a local ring, residually discrete with maximal ideal $\mathfrak{m}$ and residue field $R/\mathfrak{m}$. If g is a monic polynomial in $R[X]$ which has a simple root in some nontrivial commutative $R/\mathfrak{m}$-algebra, then g is unramifiable. □

Lemma 2 (Lombardi & Quitté, [11, Lemme IX-7.1])**.** If $g=(X-a_1)\cdots(X-a_p)f$ in $R[X]$ with f monic of degree n, $\Delta(g)=1$, and R is local, then $g'(a_1)$ is invertible or … or $g'(a_p)$ is invertible or $\Delta(f)=1$.

Proof. We write $h=(X-a_1)\cdots(X-a_p)$. We have in $R[x_1,\dots,x_n]$, the universal splitting algebra of f,

$$\begin{aligned}1&=D(g'(a_1),\dots,g'(a_p),h(x_1)f'(x_1),\dots,h(x_n)f'(x_n))\\&=D(g'(a_1),\dots,g'(a_p),f'(x_1),\dots,f'(x_n))\\&=D(g'(a_1),\dots,g'(a_p))\vee\Delta(f).\end{aligned}$$

Since the universal splitting algebra is faithfully flat, we get $1=D(g'(a_1),\dots,g'(a_p))\vee\Delta(f)$ in R, and since R is local we have the conclusion. □

Definition 3 (Lombardi & Quitté, [11, Définition IX-7.2])**.** A local ring R is *separably closed* if every unramifiable monic polynomial has a root in R.

Lemma 4 (Lombardi & Quitté, [11, Lemme IX-7.3])**.** If R is a separably closed local ring then any unramifiable monic polynomial has a simple root in R.

Proof. Assume that R is separably closed local. Let g be a monic unramifiable polynomial. It has a root a_1 and we can write $g=(X-a_1)f_1$. By Lemma 2, a_1 is a simple root of g or $\Delta(f_1)=1$. If $\Delta(f_1)=1$ then it has a root a_2 and $g=(X-a_1)(X-a_2)f_2$. Then by Lemma 2 again, a_1 or a_2 is a simple root of g or $\Delta(f_2)=1$, and so on until we find a simple root of g. □

Let k be a ring. We can consider the following two coherent theories for a commutative k-algebra R:

(1) T_1 states that R is local, and that any monic unramifiable polynomial has a root.
(2) T_2 states that R is local, and that any monic unramifiable polynomial has a *simple* root.

We have just seen that these two theories are equivalent. The equivalence between these two theories can be seen as a logical formulation of the trick attributed to O. Gabber described in [15, Tag 02LI].

A morphism $S\longrightarrow S[X]/(f)$, with f monic, is finite locally free, and thus represents the "finite locally free" stage in Gabber's refinement of an étale covering. Étaleness is obtained by further localising, that is, by passing to the Zariski covering $S\longrightarrow S[X]/(f)[1/f']$. Lemma 4 provides the logical ingredient of this refinement: over a local base ring, the existence of a root of a monic unramifiable polynomial implies the existence of a simple root. Internally, this shows that coverings generated by finite locally free morphisms of the above form can be refined, after a Zariski localisation, to étale morphisms. In this sense, the equivalence between the two theories T_1 and T_2 is the internal counterpart of Gabber's trick: finite locally free coverings suffice to generate the same local objects as étale coverings, up to Zariski refinement.

These two coherent theories define two different *sites* (notions of covering), in the sense of Grothendieck (see, e.g., [7]), over the opposite of the category of finitely presented commutative k-algebras [7]. The first theory T_1 corresponds to:

(1) S is covered by $S \to S[1/s_1], \ldots, S \to S[1/s_n]$ if $1 = (s_1, \ldots, s_n)$;
(2) S is covered by $S \to S[X]/(f)$ if f is monic and unramifiable.

The second theory T_2 corresponds to:

(1) S is covered by $S \to S[1/s_1], \ldots, S \to S[1/s_n]$ if $1 = (s_1, \ldots, s_n)$;
(2) S is covered by $S \to S[X]/(f)[1/f']$ if f is monic and unramifiable.

Both define the same corresponding *classifying topos* of the theory of separably closed local commutative k-algebras [7]. In this sheaf model, we have a generic local commutative k-algebra R which is separably closed.

We also may state, following Wraith:

Theorem 5 (Lombardi & Quitté, [11, Lemmes IX-7.4, IX–7.5])**.** If R is a local ring which is also residually discrete, then R is separably closed if, and only if, R is Henselian and its residue field is separably closed.

Proof. Let g be a monic polynomial which has residually a simple root u. We show by induction on the degree of g that g has a root in R which is equal to u mod. $\mathfrak{m}$. The polynomial g is unramifiable by Lemma 1, since it has residually a simple root, and it has a root a. If $a \neq u$ mod. $\mathfrak{m}$ then we write $g = (X - a)f$, and u is residually a simple root of f. □

Thus a residually discrete local ring is separably closed if and only if it is strictly Henselian.

2 Some lemmas about Henselian rings

In the next section, we need a generalisation of a result about Henselian rings. In order to make the paper self-contained we mention here this result, Theorem 7, taken from the reference [1].

We assume in this section that R is local residually discrete with maximal ideal $\mathfrak{m}$ and Henselian. Lemma 6 is a main step in the proof of Theorem 7: we provide a variation of the proof that requires less constructive Galois theory than the original one in [1].

Lemma 6 (Alonso, Lombardi & Perdry, [1, Proposition 5.7])**.** Let f be a monic polynomial of degree n in $R[X]$ and $R[x] = R[X]/(f)$. If we have $e(X)$ in $R[X]$ such that $e(x)$ is idempotent mod. $\mathfrak{m}R[x]$, then we can find u idempotent in $R[x]$ with $u = e(x)$ mod. $\mathfrak{m}R[x]$.

Proof. Let $L = R[x_1, \ldots, x_n]$ be the universal splitting algebra of f. This is a free R-module over R of dimension $n!$ and the symmetric group acts on it by [10, Fact III-4.4]. We may identify $R[x]$ with the subalgebra $R[x_1]$ and we have $e(x_1)$ in $R[x_1]$ which is idempotent mod. $\mathfrak{m}R[x_1]$. We show that we have u_1 in $R[x_1]$ which is idempotent in $R[x_1]$ and equal to $e(x_1)$ mod. $\mathfrak{m}R[x_1]$.

The product $e(x_1) \cdots e(x_n)$ is in R and it is an idempotent mod. $\mathfrak{m}$, so it is 1 or 0 mod. $\mathfrak{m}$. If it is 1, we have $e(x_1) = 1$ mod. $\mathfrak{m}R[x_1]$ and we can take $u_1 = 1$.

We can thus assume $e(x_1) \cdots e(x_n) = 0$ mod. $\mathfrak{m}$. We write $e_I = \prod_{i \in I} e(x_i)$ for I subset of $1, \ldots, n$. We let $k < n$ be such that $e_I \neq 0$ mod. $\mathfrak{m}L$ if $|I| = k$ and $e_I = 0$ mod. $\mathfrak{m}L$ if $|I| = k + 1$.[3] Note that the e_I for $|I| = k$ are pairwise orthogonal mod. $\mathfrak{m}L$. We have $\Sigma_{|I|=k} e_I = 1$ mod. $\mathfrak{m}$ since it is an element in R which is idempotent mod. $\mathfrak{m}$. Hence the family of the e_I, $|I| = k$, forms an FSOI mod. $\mathfrak{m}L$.[4]

[3] The e_I, $|I| = k$, are pairwise conjugate by the action of the symmetric group and equality is decidable mod. $\mathfrak{m}L$.

[4] A "Fundamental System of Orthogonal Idempotents", see [10, Section II-4].

We deduce that

$$g(X) = \prod_{|I|=k} (X - e_I),$$

which is a monic polynomial in $R[X]$, is of the form $X^{N-1}(X-1)$ mod. $\mathfrak{m}R[X]$ with $N = \binom{n}{k}$. Since R is Henselian, we have α in R, $\alpha = 1$ mod. $\mathfrak{m}$, such that $g(\alpha) = 0$; furthermore $\lambda = g'(\alpha)$ is invertible with $\lambda = 1$ mod. $\mathfrak{m}$. If we write $g_I = g/(X - e_I)$ then $g'(X) = \Sigma_I g_I$. We take $v_I = \frac{1}{\lambda} g_I(\alpha)$ and we then have that the v_I, $|I| = k$, form an FSOI in $R[x_1, \ldots, x_n]$. We have $v_I = \prod_{J \neq I}(1 - e_J) = e_I$ mod. $\mathfrak{m}L$. Let $\mathcal{I}_1$ be the set of all I such that 1 is in I and $|I| = k$. If we write u_1 for $\sum_{I \in \mathcal{I}_1} v_I$, we have u_1 in $R[x_1]$ and u_1 is equal to $\sum_{I \in \mathcal{I}_1} e_I = e(x_1)$ mod. $\mathfrak{m}L$. This equality follows from $e(x_1) = e(x_1)\big(\sum_I e_I\big) = \sum_I e(x_1)e_I = \sum_{I \in \mathcal{I}_1} e_I$ mod. $\mathfrak{m}L$. Hence $e(x_1) - u_1 \in R[x_1] \cap \mathfrak{m}L = \mathfrak{m}R[x_1]$. □

Theorem 7 (Alonso, Lombardi & Perdry, [1, Theorem 5.9])**.** If A is a commutative R-algebra which is finitely generated as an R-module and a in A is idempotent mod. $\mathfrak{m}A$, then we can find e in A idempotent in A and such that $e = a$ mod. $\mathfrak{m}A$. □

The following generalisation is not in [1] and will be crucial in the proof of Lemma 11.

Corollary 8. If A is a (not necessarily commutative) R-algebra which is finitely generated as an R-module and a in A is idempotent mod. $\mathfrak{m}A$, then we can find e in A idempotent in A and such that $e = a$ mod. $\mathfrak{m}A$.

Proof. Write $\varphi(x) = x^2 - x$ and consider the finitely generated algebra $B = R[a]$. Since $\varphi(a) = a^2 - a$ is in $\mathfrak{m}A$, the constant term of its characteristic polynomial is in $\mathfrak{m}A \cap R = \mathfrak{m}$, so that we have N such that $\varphi(a)^N$ is in $\mathfrak{m}B$. We can then consider the following Newton quadratic iteration of a inside B by defining inductively $u_0 = a$ and $u_{n+1} = u_n - (2u_n - 1)\varphi(u_n)$ (compare [10, Corollary III.10.4]). One checks that $u_n = a$ mod. $\mathfrak{m}A$ and that $\varphi(u_n)$ is in $\varphi(u_{n-1})^2 B$, so that it is in $\mathfrak{m}B$ for n big enough, i.e., u_n is idempotent mod. $\mathfrak{m}B$. We can now use Theorem 7 for the commutative R-algebra B to lift u_n to an idempotent e in B such that $e = u_n$ mod. $\mathfrak{m}B$. We also have $e = a$ mod. $\mathfrak{m}A$. □

3 Azumaya algebras

An *Azumaya algebra* A over a ring k is an algebra such that

(1) A is finitely generated projective;
(2) the canonical map $A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ is an isomorphism.

Note that we allow the trivial algebra to be an Azumaya algebra. Note also that any matrix algebra is Azumaya.

In this section k will denote a commutative base ring, and R will denote the generic separably closed commutative k-algebra, model of the coherent theory T_1 described in the first section.

One can equivalently describe the algebra structure by a bilinear map $\mu\colon A \times A \to A$; its scalar extension along $k \to S$ is the unique S-algebra A_S through which every bilinear map extending μ factors. Thus all subsequent arguments can be phrased without explicit tensor notation.

Over a finitely generated free k-module, an algebra structure is given concretely by a multiplication table. A module A, finitely generated projective over k, is given concretely by a projection matrix over k [10, Chap. I], and we can similarly represent the algebra structure by a multiplication table (so m^3 elements of k if the projection matrix has finite size m). We can then compute (see [10, Theorem X-1.6]) comaximal elements $s_1, \ldots, s_\ell$ such that $A[1/s_i]$ is free over $k[1/s_i]$, and the second condition for being an Azumaya algebra becomes then that ℓ determinants are invertible.[5] From this discussion, it follows that if A is an Azumaya algebra, given

[5] After localisation to s_i the Azumaya algebra becomes free of rank $r_i = n_i^2 \leqslant m$.

by a multiplication table, and we have a commutative k-algebra $k \to S$, then the algebra A_S over S, with the same multiplication table, is also an Azumaya algebra.

We have the following characterisation, which generalises the result that an algebra is central simple over a field if, and only if, it can be split by a separable extension of this field.

Theorem 9. *A is an Azumaya algebra over k if, and only if, we can build a finite covering tree rooted at k using the following, where at every leave the scalar extension A_S is a matrix algebra:*

(1) *S is covered by $S \to S[1/s_1]$, …, $S \to S[1/s_n]$ if $1 = (s_1, \ldots, s_n)$;*
(2) *S is covered by $S \to S[X]/(f)$ if f is monic and unramifiable.*

We shall use the local-global principle and the descent principle with respect to faithfully flat extension for projective modules (see [10, Theorem VIII-6.7]). For completeness, we recall the statement. Note that the proof in [10] is constructive, using the concrete definition of faithfully flat extension and the fact that, also constructively, a module is finitely generated projective if, and only if, it is finitely presented and flat.

Theorem 10 (Descent)**.** *Let $A \to B$ be a faithfully flat extension and M an A-module. If $M \otimes_A B$ is finitely generated projective, then so is M. If we have $1 = (s_1, \ldots, s_n)$ in A and each $M[1/s_i]$ is finitely presented and projective over $A[1/s_i]$, then so is M.*

We prove first that if we have such a covering tree, then the algebra A is Azumaya. If we have such a covering tree rooted at k, notice that each extension $S \to S[X]/(f)$ for f monic is faithfully flat, and $S \to \prod_i S[1/s_i]$ is also faithfully flat if $1 = (s_1, \ldots, s_n)$. It follows then that A is finitely generated projective by Theorem 10. The map $A \otimes_k A^{\mathrm{op}} \to \mathrm{End}_k(A)$ is then a bijection, since it becomes a bijection by a faithfully flat extension. (As we saw before, to be a bijection is witnessed by the fact that some determinants are invertible, and an element is invertible if it becomes invertible by a faithfully flat extension.)

For the converse, we look at the algebra A (given concretely by its multiplication table) inside the étale topos over k, using the site defined in the first section. (This is similar to the constructive use of the algebraic closure in [12].) The generic ring R, defined by $R(S) = S$ for S a finitely presented commutative k-algebra, is, in the internal logic of this topos, a separably closed local ring. The algebra A defines then an R-algebra $A_R(S) = A_S$, which is the Azumaya algebra given by the same multiplication table as the one for A. If we can prove in intuitionistic logic that an Azumaya algebra over a separably closed ring is a matrix algebra, we will get, using the interpretation of intuitionistic logic in a sheaf model [7; 12], a covering tree rooted at k, which yields Theorem 9.

Internally in the classifying topos of separably closed local commutative k-algebras, the object R is separably closed local and the claim that A_R is a matrix algebra is a coherent statement, provable in intuitionistic logic. Such a proof yields externally a finite covering tree rooted at k satisfying the conditions above.

The converse is a consequence of the following two results.

Lemma 11. *If A is an Azumaya algebra over R, which is a residually discrete separably closed local commutative k-algebra, then A is a matrix algebra over R.*

Proof. We know that R is Henselian and that $R/\mathfrak{m}$ is separably closed by Theorem 5.

We simplify (and correct slightly) the argument in Milne's course notes [13, Chapter IV, Proposition 1.6], using the constructive development in [1; 5]. If $\mathfrak{m}$ is the maximal ideal of R, we have that A is split over $R/\mathfrak{m}$ (cf. [5]), and hence we have a matrix algebra decomposition e_{ij} mod. $\mathfrak{m}A$. We lift the idempotent e_{11} mod. $\mathfrak{m}A$ to some idempotent e in A using Corollary 8.

The R-module Ae is finitely generated projective and hence free, since R is a local ring. The map $A \to \mathrm{End}_R(Ae)$ is then an isomorphism, since it is a map between two free R-modules of same dimension, and it is residually an isomorphism. □

The next proof uses Barr's Theorem in a way similar to [14; 16], but the difference is that we only need a constructively valid version of this theorem.

Corollary 12. If A is an Azumaya algebra over R, which is a separably closed local commutative k-algebra, then A is a matrix algebra over R.

Proof. For a given Azumaya algebra, the conclusion is coherent [7; 12], and the hypothesis that A is an Azumaya algebra is formulated in a coherent theory. Since it is proved with the extra hypothesis that R is residually discrete, the syntactic version of Barr's Theorem (constructively valid) shows that it can be proved without this hypothesis.[6] □

Theorem 9 follows by interpreting this result in the classifying topos of the theory of separably closed local commutative k-algebras. The statement of Theorem 9 can be seen as a generalisation of the fact that over a field, a central simple algebra becomes a matrix algebra by a faithfully flat extension [5] (classically over an algebraic extension). We can use such a covering tree to give arguments by *tree induction*. We give some simple examples.

Lemma 13. Any Azumaya algebra A is central.

Proof. This means that if a in A satisfies $ax = xa$ for all x in A then a is in k. We prove this by tree induction using Theorem 9. The statement holds on the leaves (it holds for a matrix algebra) and descends to the root. □

Lemma 14. If R is a local ring and A a matrix algebra of rank $\geqslant 1$ [10, Definition X-2.2] then any automorphism of A is of the form $x \mapsto axa^{-1}$ for some a in $\mathrm{GL}_n(A)$.

Proof. Let $A = \mathrm{End}_R(R^n)$ with $v_1, \ldots, v_n$ the canonical basis of R^n and define $e_{ij}v_k = \delta_{jk}v_i$. Let ψ be an automorphism of A. If $p_{ij} = \psi(e_{ij})$, we have that the $p_i = p_{ii}$ form an FSOI and $p_{ij}p_{k\ell} = \delta_{jk}p_{i\ell}$. Since R is local, each $V_i = p_i(R^n)$ is free. Furthermore R^n is a direct sum of the V_i's; the V_i's are pairwise isomorphic, since p_{ji} defines an isomorphism between V_i and V_j. So they are all free of rank 1. Let w_1 be a basis of V_1 and $w_j = p_{j1}w_1$. If $a(v_i) = w_i$ then we have $\psi(x) = axa^{-1}$. □

Theorem 15 (Skolem–Noether)**.** If A is an Azumaya algebra, of rank $\geqslant 1$ as a projective module over a ring k, and ψ is an automorphism of A, then $M = \{a \in A \mid \forall_x\, ax = \psi(x)a\}$ is a projective k-module of rank 1.

Proof. We use Theorem 9. The statement holds on the leaves (M is even *free* of rank 1 on the leaves by Lemma 14) and descends to the root by tree induction using Theorem 10. □

If k is local, the module M is free of rank 1 and any generator u of M is invertible (since it is invertible on the leaves) and ψ is the inner automorphism defined by u, so we recover the usual form of the Skolem–Noether Theorem (any automorphism of a central simple algebra is an inner automorphism).

Claude Quitté has suggested the following refinement.

Theorem 16. If A is an Azumaya algebra, of rank $\geqslant 1$ as a projective module over a ring k, and ψ is an automorphism of A, then $M = \{a \in A \mid \forall_x\, ax = \psi(x)a\}$ and $N = \{a \in A \mid \forall_x\, a\psi(x) = xa\}$ are projective k-modules of rank 1 and $M \otimes_k N \simeq k$ and $MN = k1$. Furthermore, M and N are direct factors in A.

Proof. We have on the leaves $M_S N_S \subseteq S1$ and this statement descends to the root by tree induction. This can be used to define a map $M \to \mathrm{Hom}(N, k)$, $x \mapsto (y \mapsto xy)$. This map is an isomorphism on the leaves, and this statement also descends to the root by tree induction. Finally, M and N are direct factors on the leaves, and this fact descends as well. □

[6] We can actually follow the argument in [7] and apply Friedman–Dragalin's translation [2] with respect to the proposition expressing that A is a matrix algebra.

4 Theory of algebraically closed local rings

To get the theory of algebraically closed local rings, we add to the theory of local rings the axioms $\exists_x\ f(x) = 0$ for any monic nonconstant polynomial f. Wraith conjectured in [16] that this should define the classifying theory of the fppf topos. This question is discussed further in Blechschmidt's PhD thesis [4].

The same argument as in Lemma 11 shows the following result.

Lemma 17. If A is an Azumaya algebra over R, which is a residually discrete algebraically closed local commutative k-algebra, then A is a matrix algebra.

We can then prove as in the previous section:

Theorem 18. *A is an Azumaya algebra over k if, and only if, we can build a finite covering tree rooted at k using the following, where all leaves are matrix algebras:*

(1) *S is covered by $S \to S[1/s_1]$, …, $S \to S[1/s_n]$ if $1 = (s_1, \dots, s_n)$;*
(2) *S is covered by $S \to S[X]/(f)$ if f is monic nonconstant.*

5 Conclusion

This paper is a beginning of the theory of Azumaya algebras in a constructive setting. The natural next step will be to analyse Gabber's Theorem [9] that the group of Azumaya algebras is the torsion part of the second cohomology group with coefficients in $\mathrm{GL}_n(k)$ for the étale topology.

References

[1] M. E. Alonso, H. Lombardi & H. Perdry. Elementary constructive theory of Henselian local rings. *Math. Log. Q.* 54:3 (2008), pp. 253–271. DOI: 10.1002/malq.200710057.

[2] J. Avigad. Interpreting classical theories in constructive ones. *J. Symb. Log.* 65:4 (2000), pp. 1785–1812. DOI: 10.2307/2695075.

[3] E. Bishop. *Foundations of Constructive Analysis*. New York: McGraw-Hill, 1967.

[4] I. Blechschmidt. *Using the Internal Language of Toposes in Algebraic Geometry*. PhD thesis. University of Augsburg, 2017.

[5] T. Coquand, H. Lombardi & S. Neuwirth. *Constructive basic theory of central simple algebras*. Preprint. 2023. arXiv: 2102.12775.

[6] M. Coste, H. Lombardi & M.-F. Roy. Dynamical method in algebra: effective Nullstellensätze. *Ann. Pure Appl. Log.* 111:3 (2001), pp. 203–256. DOI: 10.1016/S0168-0072(01)00026-4.

[7] P. T. Johnstone. *Topos Theory*. London Mathematical Society Monographs, Vol. 10. London: Academic Press, 1977.

[8] A. Joyal. Les théorèmes de Chevalley–Tarski et remarques sur l'algèbre constructive. *Cah. Topol. Géom. Différ.* 16 (1975), pp. 256–258.

[9] M. Kervaire & M. Ojanguren, eds. *Groupe de Brauer : séminaire, Les Plans-sur-Bex, Suisse 1980*. Lecture Notes in Mathematics, Vol. 844. Berlin, Heidelberg: Springer, 1981. DOI: 10.1007/BFb0090474.

[10] H. Lombardi & C. Quitté. *Commutative Algebra: Constructive Methods: Finite Projective Modules*. Algebra and Applications, Vol. 20. Dordrecht: Springer, 2015. DOI: 10.1007/978-94-017-9944-7.

[11] H. Lombardi & C. Quitté. *Algèbre commutative : méthodes constructives*. Nouvelle édition revue et augmentée. Mathématiques en devenir. Calvage & Mounet, 2021.

[12] B. Mannaa & T. Coquand. Dynamic Newton–Puiseux theorem. *J. Log. Anal.* 5:5 (2013). DOI: 10.4115/jla.2013.5.5.

[13] J. S. Milne. *Étale Cohomology*. Princeton Mathematical Series, Vol. 33. Princeton University Press, 1980.

[14] J. Penon. *De l'infinitésimal au local*. PhD thesis. Université Paris 7, 1985.

[15] The Stacks project authors. *Stacks project*. `https://stacks.math.columbia.edu`. 2026.

[16] G. Wraith. Generic Galois theory of local rings. In: M. P. Fourman, C. J. Mulvey & D. S. Scott, eds. *Applications of Sheaves: Proceedings of the Research Symposium on Applications of Sheaf Theory to Logic, Algebra, and Analysis, Durham, July 9-21, 1977*. Lecture Notes in Mathematics, Vol. 753. Berlin, Heidelberg: Springer, 1979, pp. 739–767. DOI: `10.1007/BFb0061844`.