Constructive Algebra and Point-Free Topology

Thierry Coquand

Computer Science Department, University of Gothenburg

Introduction

Topological ideas play an important rôle in algebra, bringing geometrical intuitions and powerful methods from algebraic topology, such as the use sheaf theoretical notions [62]. The goal of this paper is to survey some recent constructive interpretations of these methods.

One *constructive* issue in using these topological ideas in algebra is that the various spaces one considers, such as Zariski spectrum, space of valuations, ..., may fail to have enough points[1]. For instance Tierney [69] describes an example, due to Joyal, of a non trivial ring without any point in its Zariski spectrum. Often however, these spaces are used by introducing a generic point, which is shown to exist using classical methods, such as Zorn's Lemma, and one needs a way to interpret such arguments constructively[2].

One general method to "force" a space to have a (generic) point in a constructive setting is the following [38, 18]. While a space may fail to have a point constructively, it *always* gets a generic point when working in the *sheaf model* over this space. In several cases, it is possible to analyse proof theoretically the presentation of the space and show that we can "eliminate" the use of this generic point. This is actually similar to the technique of elimination of choice sequences used in intuitionistic mathematics [70]. This method works as well for the generalized notion of space, as a topos given by a site, introduced by Grothendieck. For instance, the algebraic closure of a field can be represented as a *point* of a suitable sheaf topos. As stressed by Joyal [39], this is also reminiscent of Hilbert's notion of *introduction* and *elimination* of ideal elements[3].

This approach comes from two complementary lines of research: on one side, the idea of using point-free topology [38, 60, 26] for representing topological spaces in constructive mathematics[4], and on the other side, the *dynamical* method in algebra [30, 43, 44]. The dynamical method originated first in computer algebra [31], where it was used to explain how to do computations in an algebraic closure of an arbitrary computable field. As stressed in [43], this is quite paradoxical, since it is well known that such object *cannot* exist in general in constructive mathematics [52, 9].

This paper is organized as follows. We first study some examples corresponding to this analysis of *topological* spaces, such as Zariski spectrum or the space of minimal or maximal primes, and in a second part, we present an example corresponding to the analysis of more general *Grothendieck sites.* We end by listing some open questions and research directions.

[1] To some extent, there are similarities with the worries that there might not be, in a constructive setting, "enough" points in Cantor space or the real lines, worries that motivated Brouwer's "second act of intuitionism" [10], and the introduction of the notion of choice sequences. The methods we present in this survey also have some analogy with this development.

[2] Typical examples of such arguments are provided by several proofs in Nothcott's book [55], which simplifies the treatment of Buchsbaum and Eisenbud [11]. Using the method we describe in the present paper, we can eliminate completely these non constructive arguments, and obtain an effective and elementary presentation of the theory of finite free resolutions [24].

[3] Yet another connection is with the notion of "descent" in algebraic geometry [63, 13].

[4] In several ways, this line of research was already suggested in the work of Lorenzen [46, 47, 20]. In particular, the paper [48] suggests a point-free analysis of Cantor-Bendixson. Also, one important tool in analysing the presentation of a space is the notion of *entailment relation* [12, 44], which already appears in Lorenzen's paper on cut elimination [46]. (The concept of entailment relation is now being used for an abstract development of proof theory [58, 57, 61].) One can also mention some remarks of Troelstra [70], suggesting the use of elimination of choice sequences for a constructive reading of some classical proofs, which is strongly reminiscent of the present method based on point-free topology.

1 Zariski spectrum

1.1 Point-free representation

The Zariski spectrum of a commutative ring R is, in classical mathematics, the following topological space $Sp(R)$. The *points* of this space are prime ideals. The basic open are the subsets $D(a) = \{I \in Sp(R) \mid a \notin I\}$. We have by definition

$$D(1) = Sp(R) \quad D(0) = \emptyset \quad D(ab) = D(a) \cap D(b) \quad D(a+b) \subseteq D(a) \cup D(b)$$

Let us write $D(b_1, \ldots, b_m)$ for $D(b_1) \cup \cdots \cup D(b_m)$. It is also a classical theorem (Krull's theorem) that a is nilpotent[5] if, and only if, $D(a)$ is empty. A corollary of this result is that $D(a) \subseteq D(b_1, \ldots, b_m)$ if, and only if, a belongs to the radical of the ideal $\langle b_1, \ldots, b_m \rangle$.

Krull's Theorem relies on Zorn's Lemma[6]. In constructive mathematics, a non trivial ring may fail to have prime ideals [69], and it thus seems impossible to use Zariski spectrum in a constructive setting.

As we wrote in the introduction, the solution of this problem has some similarity to Brouwer's analysis of the notion of choice sequences [10, 14]. We consider $Sp(R)$ as a *point-free* space, defined simply by the lattice of its compact open subsets. We see then $D(a)$ as a pure symbol, generating a distributive lattice given by the relations, first formulated by Joyal [39]

$$D(1) = 1 \quad D(0) = 0 \quad D(ab) = D(a) \wedge D(b) \quad D(a+b) \leqslant D(a) \vee D(b)$$

This lattice is thus presented by generators and relations. A direct argument shows that one can realize this lattice as the lattice of the *radicals* of finitely generated ideals [7].

We get then that $D(a) = 0$ if, and only if, a is nilpotent, and this argument was obtained by pure universal algebra, without ever having to build any prime ideals!

It is then possible to develop notions connected classically to Zariski spectrum in a constructive setting. A typical example is provided by the notion of *Krull dimension* of a ring.

1.2 An example: Krull dimension

Classically, the Krull dimension n of a ring is the maximal length of strict chains of prime ideal $I_0 \subsetneqq I_1 \subsetneqq \cdots \subsetneqq I_n$. So a ring is of dimension 0 if we cannot have $I \subsetneqq J$ for two prime ideals I and J, i.e. any prime ideal is a maximal ideal.

A field, or a Boolean algebra, is a ring of dimension 0.

This notion can be analysed in a point-free way. It is actually simpler to define first the Krull dimension of a distributive lattice L. Such a definition goes back to works of Joyal and Espanol [8, 35], but it was realized later [23] that it can be seen as a simple case of Menger's dimension of topological space. Define the *boundary* $B(a)$ of an element a. It is the ideal generated by a and the ideal of elements x such that $x \wedge a = 0$. We say then[8] that L is of dimension < 0 if $1 = 0$ in L, and L is of dimension $< n+1$ if each $L/B(a)$ is of dimension $< n$.

The Krull dimension of a ring R is then defined to be $< n$ if, and only if, $Sp(R)$ is of dimension $< n$.

Since we have $D(ab) = D(a) \wedge D(b)$ any element of $Sp(R)$ is of the form $D(a_1, \ldots, a_n)$. A natural question is if we can make n as small as possible. It can be checked that $D(a, b) = D(a+b, ab)$. In particular, if $ab = 0$ we have $D(a, b) = D(a+b)$. Using this remark, one can show that if R is a Boolean algebra, any element of $Sp(R)$ can be written on the form $D(a)$. This can be generalized in the following version of Kronecker's Theorem [15].

Theorem 1.1. *If R is of dimension $< n$ any element of $Sp(R)$ can be written $D(a_1, \ldots, a_m)$ with $m \leqslant n$.*

The point here is that this has a simple effective proof, following the fact that all notions involved are defined in an elementary and effective way.

[5] This means that we have $a^n = 0$ for some n.

[6] Stricly speaking, it relies on a weaker form of the axiom of choice, the Boolean prime ideal theorem, but it is usually proved using Zorn's Lemma.

[7] In general, finitely generated ideals are not closed by intersection, while if $D(a_1, \ldots, a_n)$ is the *radical* of the ideal $\langle a_1, \ldots, a_n \rangle$ we always have $D(a_1, \ldots, a_n) \cap D(b_1, \ldots, b_m) = D(a_1 b_1, \ldots, a_n b_m)$.

[8] In a constructive setting, the dimension is not given as a natural number, but as a downward set of natural number.

Reformulating basic notions of algebra in this point-free setting may reveal connections that were hidden in a classical setting. For instance the following result, which also has an elementary proof [22, 44], contains *both* Forster-Swan and Serre splitting off Theorem, while the classical version of these results look quite different. If F is a matrix over R we write $\Delta_n(F)$ the ideal generated by the $n \times n$ minors of F and we say that a vector is *unimodular* if the ideal generated by its elements contains 1.

Theorem 1.2. *If R is of dimension $< n$ and F a rectangular matrix such that $\Delta_n(F) = 1$ then some linear combination of the column of F is unimodular.*

Serre's splitting off Theorem is the special case when the matrix is a square idempotent matrix.

2 Minimal and Maximal Primes

This "phenomenological" approach to prime ideals extends to the notion of *maximal* and *minimal* prime ideals. We restrict ourselves to explaining the case of minimal prime ideals, and only mention a spectacular application of the analysis of maximal ideals: the computational interpretation in [72] of a Lemma of Suslin used in his proof of Serre's problem (any idempotent matrix over a polynomial ring is similar to a canonical projection matrix). The existence of a maximal ideal is the only non effective element in Suslin'a proof[9].

The lattice $Sp(R)$ can be seen as a point-free presentation of the Zariski spectrum. This presentation is *finitary* and this corresponds to the fact that this space is coherent [66, 38]. For the space of minimal prime ideals, we need a presentation of a general point-free space [60, 26] with finite conjunctions and *infinitary* disjunctions. To find the presentation of this space, we give a *classical* characterisation of minimal prime ideals. We define a *multiplicative monoid* of a ring to be a subset closed by multiplication and containing 1. This monoid is *proper* if it does not contain 0.

Lemma 2.1. *A subset of a ring is a minimal prime ideal if, and only if, its complement is a maximal proper multiplicative monoid. Furthermore, such a maximal proper multiplicative monoid D is exactly a mutiplicative monoid such that if $a \notin D$ then there exists b in D such that ab is nilpotent.*

We refer to [55] for the proof.

We can then use as a presentation of the space of the minimal prime ideals the following theory.

$$D(0) = 0 \qquad D(1) = 1 \qquad D(a) \wedge D(b) \leqslant D(ab) \qquad 1 = D(a) \vee \bigvee_{b \in N(a)} D(b)$$

where $N(a)$ is the ideal of elements b such that ab is nilpotent.

One can then show [19], in an elementary way, the following result.

Theorem 2.2. *We have $D(a) \leqslant D(b_1) \vee \cdots \vee D(b_m)$ if, and only if, for all x, xa is nilpotent as soon as all $xb_1, \ldots, xb_m$ are nilpotent.*

Corollary 2.3. *We have $D(a) = 0$ if, and only if, a is nilpotent.*

This corresponds to the classical fact that the intersection of all minimal prime ideals is the set of nilpotent elements.

An example where minimal prime ideals are used is Swan-Traverso's characterisation of seminormal rings [17, 44]. Here again, it is actually possible to implement the constructive proof and run it on small examples [2].

We explain here in details a simpler example: a Theorem of Vasconcellos, the proof of which [55] uses a generic minimal prime ideal. For this example, this analysis produces an elementary argument, which does not mention minimal prime ideals.

If E is a module over R we define $Ann_R(E)$ to be the ideal of elements a in R such that $aE = 0$. We say that an ideal I of R is *regular* if $Ann_R(I) = 0$.

[9] It is even possible to realize this constructive version as a functional program and run it on small examples [42].

Theorem 2.4. *Let E be a module over R which admits a finite free resolution*

$$0 \to F_m \to F_{m-1} \to \cdots \to F_0 \to E \to 0$$

Each F_i is of the form R^{p_i} and we define[10] $\mathsf{Char}_R(E)$ *to be $p_0 - p_1 + p_2 - \ldots$. Then*

- *If* $\mathsf{Char}_R(E) = 0$ *then $Ann_R(E)$ is regular*
- *If* $\mathsf{Char}_R(E) > 0$ *then $Ann_R(E) = 0$*
- *If* $\mathsf{Char}_R(E) < 0$ *then the ring R is trivial*

This corresponds to Theorem 12 of Chapter 4 [55], which is proved using minimal prime ideals.

We will analyse a special case of this Theorem, which then suggests a direct proof of the general case [24].

We assume that we have an exact sequence $0 \to R \to R^2 \to E \to 0$ and we analyse a non effective proof that $Ann_R(E) = 0$.

The fact that we have an exact sequence $0 \to R \to R^2 \to E \to 0$ can be unfolded as follows: E is generated by two elements e_1, e_2 and we have a_1, a_2 *regular* such that $b_1 e_1 + b_2 e_2 = 0$ if, and only if, (b_1, b_2) is a multiple of (a_1, a_2).

We will make use of the following Lemma, which has a direct proof.

Lemma 2.5. *Let $a_1, \ldots, a_n$ be a regular sequence. Then $a_1^l, \ldots, a_n^l$ is also regular for all l.*

Let x be an element of $Ann_R(E)$. We need to show that we have $x = 0$. The classical reasoning proceeds as follows [55]. We assume $x \neq 0$ and we consider a minimal prime ideal M over $(0 : x) = \{a \in R \mid ax = 0\}$. Using Lemma 2.1, we know that, if b is in M, then there exists a not in M and n such that ab^n is in $(0 : x)$.

If a_1 is not in M, then a_1 is invertible in R_M, the localization of R at the prime ideal M. Since $xe_2 = 0$ we have $(0, x) = r(a_1, a_2)$ for some r, and so $ra_1 = 0$ and $x = ra_2$. This implies $r = 0$ since a_1 invertible and so $x = 1x = 0$ in R_M. We thus have 1 in $(0 : x)_M$ and so 1 in M, contradiction. So a_1 is in M, and similarly a_2 is in M.

Using Lemma 2.1, this implies a_1^n and a_2^n in $(0 : x)_M$ for some n. Since a_1^n, a_2^n is regular by Lemma 2.5, this implies $1x = 0$ in R_M, and we have 1 in $(0 : x)_M$ and so 1 in M and a contradiction.

This reasoning was using a minimal prime ideal over $(0 : x)$ in a generic way and Lemma 2.1. We can follow it and give the following derivation of $\bot$ in the theory T_M of minimal prime ideal over $(0 : x)$, where we add the axiom $\neg D(a)$ for $ax = 0$. This reasoning is now *constructive* and we can furthermore later eliminate the use of the theory T_M.

We first prove $\neg D(a_1)$. We have $xe_2 = 0$ and hence $(0, x) = r(a_1, a_2)$ for some r. This means that we have $0 = ra_1$ and $x = ra_2$. We get then $xa_1 = 0$ which implies $\neg D(a_1)$. Similarly we have $\neg D(a_2)$. Using the axioms

$$1 = D(a_1) \vee \bigvee b \in N(a_1) D(b) \qquad 1 = D(a_2) \vee \bigvee b \in N(a_2) D(b)$$

of T_M, this means that we can find b_1, b_2 such that $D(b_1)$, $D(b_2)$ and $a_1 b_1$, $a_2 b_2$ are nilpotent mod. $(0 : x)$. If $b = b_1 b_2$ we have $D(b)$ and $a_1 b$, $a_2 b$ nilpotent mod. $(0 : x)$. Using Lemma 2.5, we get b nilpotent mod. $(0 : x)$, which contradicts $D(b)$ in the theory T_M.

It is then direct to eliminate the reference to this theory T_M. The fact that we can prove $\neg D(a_1)$ in T_M means that we can show $a_1^n x = 0$ for some n. Indeed, since we have $xe_2 = 0$ we get $0 = ra_1$ and $x = ra_2$ for some r, which implies that we have $x = 0$ in $R[1/a_1]$, that is $a_1^n x = 0$ for some n. Similarly, $xa_2^n = 0$ for some n, and then $x = 0$ by Lemma 2.5.

So the core of the argument is the following global-local principle for regular ideals [24], which does not mention any minimal prime ideal.

Lemma 2.6. *Let $a_1, \ldots, a_n$ be a regular sequence. If $x = 0$ in $R[1/a_1], \ldots, R[1/a_n]$ then $x = 0$ in R. If I is an ideal of R which becomes regular in $R[1/a_1], \ldots, R[1/a_n]$ then I is regular.*

[10] It can be shown [55] that this number $\mathsf{Char}_R(E)$ is the same for any given finite free resolution of E.

Proof. The first statement follows from Lemma 2.5, since $x = 0$ in $R[1/a_i]$ if, and only if, we can find l such that $xa_i^l = 0$. For the second statement, assumes $xI = 0$. We then have $x = 0$ in $R[1/a_1], \ldots, R[1/a_n]$ and hence $x = 0$ by the first statement. □

The proof of the *general* case of Theorem 2.4 is direct from this Lemma: we look at the first column of the matrix corresponding to the map $F_m \rightarrow F_{m-1}$. This column is regular, and we prove 2.4 by induction by localising over each element of this column and applying Lemma 2.6.

Here is one simple application.

Corollary 2.7. *If each principal ideal of R has a finite free resolution then R is an integral domain.*

Proof. Indeed, by Theorem 2.4, each element is either 0 or is regular. □

The paper [24] presents an effective proof that if each finitely generated ideal of R has a finite free resolution, then R is a g.c.d. domain. For further development, see [29], and the PhD thesis of Claire Tête [68].

3 Forcing over a site

In all previous examples, we can interpret what is going on as follows. We have a space X described in a point-free way, and we "force" the existence of a point by working inside $Sh(X)$, the collection of *sheaves* over X. So we move from the usual framework of usual sets to the frame of sheaves over the space X. We can then "descend" what is going on in $Sh(X)$ back to the frame of sets[11].

Grothendieck has generalized the notion of topological space to the notion of topos over a *site*. It turns out that we can use this notion as well in a constructive setting. A *point* for this notion of topos becomes now an *algebraic structure*. A prime example of this situation is to "force" the existence of a separable algebraic closure of a given field, by using that such an algebraic closure can be seen as a point of a suitable topos. As before, by moving from the framework of sets to the framework of sheaves over the given site, we can do "as if" we had access to this algebraic structure. As before also, the main problem is if we can "descend" from this framework of sheaves to the framework of sets. For the case of separable algebraic closure of a field, this is similar to Galois descent (see e.g. [63], Chapter X) going back to the work of Châtelet [13].

For constructive mathematics, this method was first suggested by A. Joyal in two short papers [39, 8]. The method in [39] can be described as an elegant purely algebraic presentation of quantifier elimination. What we present is a variation of this basic idea, which does not proceed via quantifier elimination. This variation can be directly connected with the one of *dynamical* algebra [30], first introduced in computer algebra [31] for computing inside the algebraic closure of an *arbitrary* computable field.

3.1 Algebraic closure in constructive mathematics

First, we recall what is the problem in constructive mathematics for building the algebraic closure of a given field. The first step in building such a closure is to to add a root of a given monic polynomial P over a field F. This is simple if P is irreducible: $F[X]/\langle P\rangle$ is the desired extension of F containing a root of P. But if P is not irreducible, we need to consider an irreducible factor Q of P, and we add a root by working with $F[X]/\langle Q\rangle$.

The problem is that in general, for a computable field, we *cannot* decide if a given polynomial is irreducible or not and cannot compute in general an irreducible factor of a given polynomial. This observation goes back at least to van der Waerden's paper [71] (which was using a Brouwerian counter-example, since this was done before the formal definition of recursive functions). One possible formulation of this result is the following.

Theorem 3.1. *In the intuitionistic theory of field, we cannot show $\exists_x\ (x^2 + 1 = 0) \vee \forall_x\ (x^2 + 1 \neq 0)$.*

Proof. The theory of fields is the theory of rings, together with the axioms $1 \neq 0$ and $x = 0 \vee \exists_y\ (xy = 1)$. Consider the following Kripke counter-model. At time 0, we have $F_0 = \mathbb{Q}$ and at time 1, we have $F_1 = \mathbb{Q}[i]$ with $i^2 + 1 = 0$. Then we don't have $\exists_x\ (x^2 + 1 = 0)$ at time 0, and we don't have $\forall_x\ (x^2 + 1 \neq 0)$ at time 0 neither, since $x^2 + 1$ has a root at time 1. □

[11] See [3] for a suggestive analogy with the notion of change of frames in physics.

This means that we have problem in constructive mathematics in adding a root of a given polynomial P (even a simple polynomial such as X^2+1) since we cannot decide if this polynomial is irreducible or not.

In [9, 52], a solution of this problem is given in the case the field F is *countable*. But, in the general case, there are actually results [52], Chapter VI, 3 Exercise 1, that we cannot show in intuitionistic mathematics that a field has an algebraic closure.

3.2 Dynamical method

Given this impossibility result, it is quite surprising that a technique has been developped, originally in computer algebra, showing how to compute in an algebraic closure of an arbitrary computable field!

This technique was introduced in [31], following a suggestion of Daniel Lazard. It replaces the "computation", which is impossible in general, as explained above, of an irreducible factor, by computations of g.c.d. of two polynomials, which is always possible. This method might be interesting even in the case where we can decide irreducibility (e.g. over algebraic extensions of $\mathbb{Q}$), since deciding irreducibility might be computationally difficult compared to computations of g.c.d. of two polynomials.

The main idea is best explained on examples. Assume we want to add a root of X^2-3X+2 without deciding irreducibility. We work in the formal extension $F[a]$, $a^2-3a+2=0$, proceeding "lazily". If we are required to compute an inverse, e.g. the inverse of $a+1$, we compute the g.c.d. of $X+1$ and X^2-3X+2, producing the equality $X^2-3X+2=(X+1)(X-4)+6$ and this gives that the inverse of $a+1$ is $(4-a)/6$. If we want to compute the inverse of $a-1$, we compute the g.c.d. of $X-1$ and X^2-3X+2, which produces the equality $X^2-3X+2=(X-1)(X-2)$. We *discover* in this way the factorisation $X^2-3X+2=(X-1)(X-2)$, without the need of a factorisation algorithm. This was simply produced by asking to compute the inverse of $a-1$. We then open two branches: one with $a-1=0$ and one with $a-2=0$, and continue the computations.

In this way, we can proceed *as if* we were working in a field, computing only g.c.d, but we may have to open some branches: the computation is "dynamic". This method is presented in depth in [30, 44, 53]. In [43], it is shown how this method also provides a constructive explanation of the real algebraic closure and in [41] how to do computation in the algebraic closure of a valued field.

3.3 Topos theoretic formulation of the dynamical method

In [39, 8], A. Joyal suggested the following approach to solve the problem of algebraic closure in an effective way: the algebraic closure may not exist in the framework of sets, but it *always* exist in a suitable *sheaf extension*. The argument suggested in [39] is an algebraic version of quantifier elimination, but this can also be explained in a way which stresses the analogy with the dynamical method described above.

For the Zariski spectrum, the point-free description of the space was a *propositional* theory. For the algebraic closure, it will be a *geometric* theory: the geometric theory of the algebraic closure of a given field F. The language is the language of the theory of ring, with a constant for each element of F. The axioms are the axioms of rings with the diagram of F and the following axioms:

1. $x=0 \vee \exists_y\ (xy=1)$
2. $\exists_x\ (x^n+a_1x^{n-1}+\cdots+a_0=0)$
3. $\bigvee_P P(x)=0$ where P varies over monic polynomials

Note that the last axiom is infinitary.

There is *always* a sheaf extension in which these axioms are satisfied. This is the *classifying topos* of this theory [8]. This topos might be degenerate however. What happens in the present case is that we have a *direct* description of a site which defines this classifying topos. From this direct description follows in particular the consistency of the theory[12].

[12] This is similar to the case of the Zariski spectrum of a ring, where we have a direct description of the Zariski lattice in term of radical of finitely generated ideals. As in this previous analysis, this also can be presented as a cut-elimination result [12, 18, 44].

To simplify the discussion, we will limit ourselves to the case where the base field F is of characteristic 0.

A *triangular* algebra over F is a F-algebra obtained by a sequence of monic separable extensions. We can then prove [49, 50].

Lemma 3.2. *If R is a triangular F-algebra then for any element a of R both $R/\langle a\rangle$ and $R[1/a]$ are product of triangular F-algebras. We also have $R = R/\langle a\rangle \times R[1/a]$ for all a in R.*

We then consider the following site $\mathcal{S}_F$. The base category is the category of triangular F-algebras. A basic *covering* of R is given by decomposing R as a product by $R = R_1 \times \cdots \times R_n$ or by adding a formal root of a a monic separable polynomial $R \to R[X]/\langle P\rangle$. We obtain, in an elementary and constructive way the following result [50].

Theorem 3.3. *The topos defines by this site $\mathcal{S}_F$ is the classifying topos of the theory of algebraic closure of F. The presheaf $L(R) = Hom(F[X], R)$ is a sheaf and is separably closed in the internal logic of this topos.*

One can think of a triangular algebra as an *approximation* of the algebraic closure of F. Intuitively, we don't consider the algebraic closure given "actually", but we proceed by adding roots of polynomials as needed, and, at any point, we only have added finitely many roots. This is strongly reminiscent of Edwards' description of Kronecker's compared to Dedekind's approach of the theory of algebraic curves [33]. *The necessity of using an algebraically closed ground field introduced -and has perpetuated for 110 years- a fundamentally* transcendental *construction at the foundation of the theory of* algebraic curves. *Kronecker's approach, which calls for adjoining new constants algebraically as they are needed, is much more consonant with the nature of the subject*

It is possible to interpret computationally in this way any argument which makes use of an algebraic closure of a field F, by working in the sheaf topos over $\mathcal{S}_F$. An example is a variation of Abhyankar proof of Newton-Puiseux Theorem [1]. We first prove constructively [50] the following result.

Theorem 3.4. *If L is separably closed, then $\cup_n L((x^{1/n}))$ is separably closed.*

By reading such a proof in the topos over the site $\mathcal{S}_{\mathbb{Q}}$, we get an effective way to compute Puiseux series. The interpretation of $L[[X]]$ is given by the exponential $L^{\mathbb{N}}$ in the sheaf model. Since we have $L^{\mathbb{N}}(R) = R^{\mathbb{N}}$, this also gives a purely logical a priori explanation of the fact that we don't need to keep adding new algebraic numbers when computing a Puiseux expansion: the *existence* of an element of $L[[X]]$ provides a *finite* triangular extension of $\mathcal{S}$ which contains all the coefficients of this series.

For instance, we can solve in this way a polynomial equation over $\mathbb{Q}$ such as $y^4 - 3y^2 + xy + x^2 = 0$ finding y as a formal series in some $x^{1/n}$. Since this interpretation is *effective*, we can "run" the proof [49, 50] and actually find a triangular algebra $\mathbb{Q}[a, b]$ with $a^2 = 13/36$ and $b^2 = 3$ over which we can write y as a power series in x. This illustrates the following point: in this approach, the algebraic closure L is only given *potentially*, but *finite approximations* of L become *actual* for solving specific questions.

Yet another remark about this constructive analysis of sheaf models is that it represents a combination of the "computational" aspect of constructive mathematics and the "epistemological" aspect present in sheaf models, where a basic open represents a "stage" of knowledge. For instance, a computational problem, such as the problem of finding an inverse of $a - 2$ in $\mathbb{Q}[a]$, $a^2 - 3a + 2 = 0$, provides the knowledge of a factorization $X^2 - 3X + 2 = (X - 2)(X - 1)$, knowledge which itself may simplify further computations. There is thus a feedback between "computational" and "epistemological" aspects of constructive mathematics. This is reminiscent of some remarks of Goodman [37] about the combination of forcing and realizability.

This method of introducing and eliminating the algebraic closure of a field can also been used for a constructive reading of the theory of simple central algebras over a field. See [21], where we give a dynamical reading of Wedderburn's Theorem representing central simple algebras as matrix algebras over a division algebra[13]. We can prove constructively that any central simple algebra is split over an algebraically closed field. We deduce from this [21] that the dimension of a central simple algebra over any field F is a *square*, by "descending" the fact that its dimension is the one of a matrix algebra in the sheaf topos over $\mathcal{S}_F$.

[13] This result can also be represented using negative translation, as has been done in formalisation of algebra in type theory, see the works [36, 4].

4 Conclusion and some open questions

This paper presents some applications of point-free topology and sheaf models for the constructive analysis of several concepts and proofs in algebra. Note that this is *different*, but complementary, to the use of sheaf models suggested in [54, 8]: if we prove intuitionistically a theorem, this theorem will hold in any sheaf models, and by looking externally at this proof, we may get a new result, or a new proof of a classical result[14]. Here, instead, we use point-free methods to give a computational interpretation of classical proofs relying on ideal objects, such as prime, maximal or minimal prime ideals, or separable algebraic closures.

This technique can also be used in abstract functional analysis, where spaces are now *compact separated*. For instance [28] presents an analysis of a representation theorem, and [27] a constructive proof of Peter-Weyl's Theorem. These works rely on the paper [16] which presents an analysis of some general representation results of Stone [64, 65], reading constructively some results presented in [38] and applying a fundamental result from Krivine [40] for obtaining a suitable cut-elimination result. The paper [12] presents a constructive reading of Hahn-Banach extension theorem.

A general remark about this approach is that it avoids the use of a non canonical enumeration, which is necessary in the algebraic closure of a countable field [9], or in representation theorems for separable spaces[15] in [5, 6]. The computations associated to our arguments thus feel more natural, not relying on an arbitrary enumeration. As we have seen, in most cases, it is actually possible to carry the out by hand or with the help of a computer algebra system, for small examples [2, 42, 50, 29]. The notion of dynamical computations, connected to the idea of lazy evaluation, is also very interesting algorithmically [31], and the book [73] presents several algorithms inspired by the technique of dynamical algebra.

We end by presenting some specific open problems, and a possible future research direction.

The first problem is about the theory algebraic curves, and in particular the proof of Riemann-Roch Theorem. This is covered in [34, 32], but relying on an irreducibility algorithm. Is it possible to instead follow a dynamical approach, without such irreducibility algorithm? If so, can we have a constructive treatment which avoids, as in the classical approach, an actual computation of an integral basis?

The second problem is about valuation domains. A remarkable consequence of the work of Raynaud-Gruson [56] is that if V is a valuation domain, then $V[X_1, \ldots, X_n]$ is coherent. While this result has a constructive proof [45], this proof was found directly without relying on the work [56]. The problem is to understand the computational content of this highly non effective argument and its connection with the algorithm presented in [45].

The third problem is similar. Merkurjev's Theorem [51] provides a complete description by generators and relations of the 2-torsion part of the Brauer group of a field. While the argument in [51] is effective, the first version of this proof was non constructive and relied on a paper of Suslin [67], itself based on arguments of Quillen using the highly non effective homotopy theory of simplical sets. What is the computational content of this non effective proof?

Finally, one can hope that the constructive approach to sheaf models we have presented here can be generalised to higher toposes, providing in particular an effective treatment of cohomology groups which avoids the use of injective resolutions; for preliminary results in this direction, see [25].

References

[1] Shreeram S. Abhyankar. *Algebraic geometry for scientists and engineers*, volume 35. Providence, RI: American Mathematical Society, 1990.

[2] Sami Barhoumi. Seminormality and polynomial rings. *J. Algebra*, 322:1974–1978, 2009.

[3] J. L. Bell. From absolute to local mathematics. *Synthese*, 69:409–426, 1986.

[4] Sophie Bernard, Cyril Cohen, Assia Mahboubi, and Pierre-Yves Strub. Unsolvability of the Quintic Formalized in Dependent Type Theory. In *ITP 2021 - 12th International Conference on Interactive Theorem Proving*, 2021.

[14] The example given in [8] is Weirstrass preparation theorem, which if it is proved intuitionistically in *one* variable, gives the multivariable version by this method of interpretation in sheaf models [59]. Another recent example is Blechschmidt's [7] simple proof of Grothendieck's generic freeness lemma.

[15] Compare for instance the statements and proofs of Gelfand representation theorem in [28] and in [5, 6].

[5] Errett Bishop. *Foundations of Constructive Analysis.* McGraw-Hill, New York, 1967.

[6] Errett Bishop and Douglas Bridges. *Constructive Analysis.* Springer, 1985.

[7] Ingo Blechschmidt. *Using the internal language of toposes in algebraic geometry.* Doctoral dissertation, Universität Augsburg, 2017.

[8] André Boileau and André Joyal. La logique des topos. *J. Symbolic Logic*, 46:6–16, 1981.

[9] Douglas Bridges and Fred Richman. *Varieties of constructive mathematics*, volume 97 of *London Mathematical Society Lecture Note Series.* Cambridge University Press, Cambridge, 1987.

[10] L.E.J. Brouwer. Historica background, principles and methods of intuitionism. *South African Journal of Science*, pages 139–146, 1952.

[11] David A. Buchsbaum and David Eisenbud. Some structure theorems for finite free resolutions. *Advances in Mathematics*, 12(1):84–139, 1974.

[12] Jan Cederquist and Th. Coquand. Entailment relations and distributive lattices. In Samuel R. Buss, Petr Hájek, and Pavel Pudlák, editors, *Logic Colloquium '98. Proceedings of the Annual European Summer Meeting of the Association for Symbolic Logic, Prague, Czech Republic, August 9–15, 1998*, volume 13 of *Lect. Notes Logic*, pages 127–139. 2000.

[13] Francois Châtelet. Variations sur un thème de H. Poincaré. *Ann. Sci. Éc. Norm. Supér. (3)*, 61:249–300, 1944.

[14] Th. Coquand. About brouwer's fan theorem. *Revue internationale de philosophie*, 230:483 – 489, 2004.

[15] Th. Coquand. Sur un théorème de Kronecker concernant les variétés algébriques. *C. R. Math. Acad. Sci. Paris*, 338(4):291–294, 2004.

[16] Th. Coquand. About Stone's notion of spectrum. *J. Pure Appl. Algebra*, 197(1-3):141–158, 2005.

[17] Th. Coquand. On seminormality. *J. Algebra*, 305(1):577–584, 2006.

[18] Th. Coquand. Space of valuations. *Ann. Pure Appl. Logic*, 157:97–109, 2009.

[19] Th. Coquand and Henri Lombardi. A logical approach to abstract algebra. *Math. Struct. Comput. Sci.*, 16(5):885–900, 2006.

[20] Th. Coquand, Henri Lombardi, and Stefan Neuwirth. Lattice-ordered groups generated by an ordered group and regular systems of ideals. *Rocky Mt. J. Math.*, 49(5):1449–1489, 2019.

[21] Th. Coquand, Henri Lombardi, and Stefan Neuwirtz. Constructive basic theory of central simple algebras, 2021.

[22] Th. Coquand, Henri Lombardi, and Claude Quitté. Generating non noetherian modules constructively. *Manuscripta Math.*, 115:513–520, 2004.

[23] Th. Coquand, Henri Lombardi, and Marie-Françoise Roy. An elementary characterisation of Krull dimension. In L. Crosilla and P. Schuster, editors, *From Sets and Types to Topology and Analysis*, volume 48 of *Oxford Logic Guides*, pages 239–244. Oxford University Press, 2005.

[24] Th. Coquand and Claude Quitté. Constructive finite free resolutions. *Manuscr. Math.*, 137(3-4):331–345, 2012.

[25] Th. Coquand, Fabian Ruch, and Christian Sattler. Constructive sheaf models of type theory. preprint, https://arxiv.org/abs/1912.10407, 2020.

[26] Th. Coquand, Giovanni Sambin, Jan Smith, and Silvio Valentini. Inductively generated formal topologies. *Ann. Pure Appl. Logic*, 124:71–106, 2003.

[27] Th. Coquand and Bas Spitters. A constructive proof of the Peter–Weyl theorem. *Math. Log. Q.*, 51(4):351–359, 2005.

[28] Th. Coquand and Bas Spitters. Formal topology and constructive mathematics: the Gelfand and Stone–Yosida representation theorems. *J.UCS*, 11(12):1932–1944, 2005.

[29] Th. Coquand and Claire Tête. An elementary proof of Wiebe's Theorem. *J. Algebra*, 499:103–110, 2018.

[30] Michel Coste, Henri Lombardi, and Marie-Françoise Roy. Dynamical method in algebra: Effective Nullstellensätze. *Ann. Pure Appl. Logic*, 111(3):203–256, 2001.

[31] Jean Della Dora, Claire Dicrescenzo, and Dominique Duval. About a new method for computing in algebraic number fields. In *European Conference on Computer Algebra (2)*, pages 289–290, 1985.

[32] Harold M. Edwards. *Divisor Theory.* Birkhäuser, Boston, MA, 1990.

[33] Harold M. Edwards. Mathematical ideas, ideals, and ideology. *Math. Intelligencer*, 14(2):6–19, 1992.

[34] Harold M. Edwards. *Essays in Constructive Mathematics.* Springer, New York, 2005.

[35] Luis Espanol. Le spectre d'un anneau dans l'algèbre constructive et applications à la dimension. *Cahiers Topologie Géom. Différentielle*, 24(2):133–144, 1983.

[36] G. Gonthier. Point-free, set-free concrete linear algebra. In *Interactive theorem proving. Second international conference, ITP 2011, Berg en Dal, The Netherlands, August 22–25, 2011. Proceedings*, pages 103–118. 2011.

[37] Nicolas D. Goodman. Relativized realizability in intuitionistic arithmetic of all finite types. *J. Symb. Log.*, 43:23–44, 1978.

[38] Peter T. Johnstone. *Stone Spaces.* Number 3 in Cambridge Studies in Advanced Mathematics. Cambridge University Press, 1982.

[39] André Joyal. Les théoremes de Chevalley–Tarski et remarques sur l'algèbre constructive. *Cah. Topol. Géom. Differ. Catég.*, 16:256–258, 1976.

[40] J. L. Krivine. Anneaux preordonnes. *J. Anal. Math.*, 12:307–326, 1964.

[41] Franz-Viktor Kuhlmann, Henri Lombardi, and Hervé Perdry. Dynamic computations inside the algebraic closure of a valued field. In S. Kuhlmann F.-V. Kuhlmann and M. Marshall, editors, *Valuation Theory and its Applications. Vol 2*, volume 33 of *Fields Institute Communications*, pages 133–156, 2003.

[42] Anders Leino. An Implementation of Quillen-Suslin Theorem. Master's thesis. Chalmers University, 2011.

[43] Henri Lombardi. Relecture constructive de la théorie d'Artin-Schreier. *Ann. Pure Appl. Logic*, 91(1):59–92, 1998.

[44] Henri Lombardi and Claude Quitté. *Algèbre commutative. Méthodes constructives. Modules projectifs de type fini.* Calvage & Mounet, Paris, 2012.

[45] Henri Lombardi, Claude Quitté, and Ihsen Yengui. Un algorithme pour le calcul des syzygies sur $V[X]$ dans le cas où V est un domaine de valuation. *Commun. Algebra*, 42(9):3768–3781, 2014.

[46] Paul Lorenzen. Algebraische und logistische Untersuchungen über freie Verbände. *J. Symb. Logic*, 16(2):81–106, 1951.

[47] Paul Lorenzen. Die Erweiterung halbgeordneter Gruppen zu Verbandsgruppen. *Math. Z.*, 58(1):15–24, 1953.

[48] Paul Lorenzen. Logical reflection and formalism. *J. Symb. Log.*, 23:241–249, 1959.

[49] Bassel Mannaa and Th. Coquand. Dynamic Newton–Puiseux theorem. *J. Log. Anal.*, 5, 2013.

[50] Bassel Mannaa and Th. Coquand. A sheaf model of the algebraic closure. In Paulo Oliva, editor, *Proceedings Fifth International Workshop on Classical Logic and Computation, CL&C 2014, Vienna, Austria, July 13, 2014*, volume 164 of *EPTCS*, pages 18–32, 2014.

[51] Alexander Merkurjev. On the norm residue homomorphism of degree two. In *Proceedings of the St. Petersburg Mathematical Society. Vol. XII. Transl. from the Russian*, pages 103–124. 2006.

[52] Ray Mines, Fred Richman, and Wim Ruitenburg. *A Course in Constructive Algebra.* Springer, New York, 1988. Universitext.

[53] Teo Mora. *Solving polynomial equation systems. I: The Kronecker-Duval philosophy*, volume 88. Cambridge: Cambridge University Press, 2003.

[54] Christopher Mulvey. Intuitionistic algebra and representations of rings. In *Recent advances in the representation theory of rings and C^*-algebras by continuous sections. A seminar held at Tulane University, New Orleans, LA, USA, March 28 – April 5, 1973*, pages 3–57. Providence, RI: American Mathematical Society (AMS), 1974.

[55] D. G. Northcott. *Finite free resolutions*, volume 71. Cambridge University Press, Cambridge, 1976.

[56] Michel Raynaud and Laurent Gruson. Critères de platitude et de projectivité. Techniques de "platification" d'un module. (Criterial of flatness and projectivity. Technics of "flatification of a module.). *Invent. Math.*, 13:1–89, 1971.

[57] Davide Rinaldi and Peter Schuster. A universal Krull–Lindenbaum theorem. *J. Pure Appl. Algebra*, 220:3207–3232, 2016.

[58] Davide Rinaldi, Peter Schuster, and Daniel Wessel. Eliminating disjunctions by disjunction elimination. *Indag. Math. (N.S.)*, 29(1):226–259, 2018. Virtual Special Issue – L.E.J. Brouwer, fifty years later. Communicated first in *Bull. Symb. Logic* 23 (2017), 181–200.

[59] Christiane Rousseau. Topos theory and complex analysis. *J. Pure Appl. Algebra*, 10:299–313, 1978.

[60] Giovanni Sambin. Intuitionistic formal spaces—a first communication. In D. Skordev, editor, *Mathematical Logic and its Applications, Proc. Adv. Internat. Summer School Conf., Druzhba, Bulgaria, 1986*, pages 187–204. Plenum, New York, 1987.

[61] Peter Schuster and Daniel Wessel. Resolving finite indeterminacy: A definitive constructive universal prime ideal theorem. In *LICS '20: 35th Annual ACM/IEEE Symposium on Logic in Computer Science, Saarbrücken, Germany, July 8-11, 2020*, pages 820–830. ACM, 2020.

[62] Jean-Pierre Serre. Faisceaux algébriques cohérents. *Ann. of Math. (2)*, 61:197–278, 1955.

[63] Jean-Pierre Serre. Corps locaux. Publications de l'Institut de Mathématique de l'Université de Nancago. 8; Actualités Scientifiques et Industrielles 1296. Paris: Hermann & Cie. 243 p. (1962)., 1962.

[64] M. H. Stone. A general theory of spectra. I. *Proc. Natl. Acad. Sci. USA*, 26:280–283, 1940.

[65] M. H. Stone. A general theory of spectra. II. *Proc. Natl. Acad. Sci. USA*, 27:83–87, 1941.

[66] Marshall Harvey Stone. Topological representations of distributive lattices and brouwerian logics. *Časopis pro pěstování matematiky a fysiky*, 067(1):1–25, 1938.

[67] A. A. Suslin. The quaternion homomorphism for the function field on a conic. *Sov. Math., Dokl.*, 26:72–77, 1982.

[68] Claire Tête. *Profondeur, dimension et résolutions en algèbre commutative : quelques aspects effectifs.* Phd thesis, Université de Poitier, 2014.

[69] Myles Tierney. On the spectrum of a ringed topos. Algebra, Topol., Category Theory; Collect. Pap. Honor S. Eilenberg, 189-210 (1976)., 1976.

[70] A. S. Troelstra. *Choice sequences. A chapter of intuitionistic mathematics.* Oxford University Press, Oxford, 1977.

[71] B. L. van der Waerden. Eine Bemerkung über die Unzerlegbarkeit von Polynomen. *Math. Ann.*, 102:738–739, 1930.

[72] Ihsen Yengui. Making the use of maximal ideals constructive. *Theor. Comput. Sci.*, 392(1-3):174–178, 2008.

[73] Ihsen Yengui. *Constructive commutative algebra. Projective modules over polynomial rings and dynamical Gröbner bases*, volume 2138. Cham: Springer, 2015.