Space of Valuations

March 14, 2008

Introduction

The general framework of this paper is a reformulation of Hilbert's program using the theory of locales, also known as formal or point-free topology [28, 12, 33]. Formal topology presents a topological space, not as a set of points, but as a logical theory which describes the lattice of open sets. Points are then infinite ideal objects, defined as particular filters of neighborhoods, while basic open sets are thought of as primitive symbolic objects or observable facts [13]. This is a reverse of the traditional conceptual order in topology which defines opens as particular sets of points [33]. Some roots of this approach involve Brouwer's notion of choice sequences, and an analysis of the status of infinite objects and of universal quantification over these objects in constructive mathematics [30][1]. The application to Hilbert's program is then the following. Hilbert's *ideal objects* are represented by *points* of such a formal space. There are general methods to "eliminate" the use of points, close to the notion of forcing and to the "elimination of choice sequences" in intuitionistic mathematics, which correspond to Hilbert's required elimination of ideal objects[2]. Such a technique has been used in infinitary combinatorics, obtaining intuitionistic versions of highly non constructive arguments [4, 5, 6]. More recently, several works [7, 9, 10, 11, 16, 18, 27] following these ideas can be seen as achieving a partial realization of Hilbert's program in the field of commutative algebra.

This paper illustrates further this general program on the notion of *valuations*. They were introduced by Dedekind and Weber [17] to give a rigorous presentation of Riemann surfaces. It can be argued that it is one of the first example in mathematics of point-free representation of spaces [3]. It is thus of historical and conceptual interest to be able to represent this notion in formal topology.

In this work with Weber [17], Dedekind used his newly created theory of ideals, a theory that has played an important rôle in the development of non constructive methods in mathematics [19, 21]. It is thus also relevant to illustrate Hilbert's notion of introduction and elimination of ideal elements in this context. Our work relies here directly on [18], which pointed out the notion of Prüfer domain as the right constructive (and first-order) approximation of Dedekind rings. We extend this work and present several characterization of Prüfer domains.

We think that some of our proofs illustrate well Hilbert's ideas of elimination of ideal elements. The points (prime ideals, valuations, ...) constitute a powerful intuitive help, but they are used here only as suggestive means with no actual existence. We show that many of the results of [26, 35] can be naturally expressed and proved in this point-free framework, illustrating

[1] Logically, such a quantification is a priori a Π^1_1 statement and it is analyzed in the form of a Σ^0_1 equivalent assertion.

[2] Technically, the *introduction* of a point of a formal space corresponds to working in the sheaf model over this space, and the *elimination* of this point is achieved by the Beth-Kripke-Joyal explanation of the logic of this sheaf model. In most cases, this elimination can be carried out directly without involving explicitly the notion of sheaf models.

our method of eliminating the use of ideal objects and extracting the computational content of classical concepts and arguments. The analysis of a lemma of Seidenberg [26, 35] for instance suggests in this way a simple constructive proof of Gilmer-Hoffmann's Theorem [25] (Proposition 5.6). By combining this with a concrete algebraic definition of Krull dimension [9], we get new simple proofs of characterizations of Prüfer domains (Corollaries 5.7, 5.8). We obtain also a simple proof that the integral closure of a polynomial ring in an algebraic extension is a Prüfer domain.

This paper is organized as follow. After recalling basic notions related to distributive lattices, we present Joyal's point-free presentation of the Zariski spectrum [27]. By analogy, we introduce the main object of the paper, which is the space of valuations associated to any field. In our approach, it is a distributive lattice defined by generators and relations. We give then a point-free description of the notion of *algebraic curve*. We show how the cohomological description [36] of the *genus* of a curve, a notion which goes back to Abel [22], can also be interpreted constructively. We see this as a modest, but significant, first step towards the general program of analyzing logically contemporary algebraic geometry, and classifying its results and proofs by their logical complexity.

The paper is written in the usual style of constructive algebra, with [31] as a basic reference. In particular, we recall that an integral domain has a decidable equality and we consider only *discrete* fields. Each of our statement can be understood as a *specification of a program*, and its *proof* can be seen as a *program* realizing this specification together with its proof of correctness.

1 Distributive lattices

The general methodology is to represent Hilbert's notion of "ideal" elements as a generic point of a formal space. This formal space is especially simple in the case of *spectral spaces* [28], introduced in [37], since it is then a *distributive lattice*, the lattice of compact open subsets. Most of the topological spaces introduced in commutative algebra are spectral spaces. In our approach, we work instead directly with the corresponding distributive lattice of compact open, which is thought of as a formal presentation of the space. The analysis of the structure of the associated distributive lattice can be carried out using ideas from sequent calculus and cut-elimination [7].

1.1 Krull dimension

Let D be a distributive lattice. A *point* of D can be defined classically as a lattice map α from D to the lattice $\mathbf{2}$ with two elements. If u is an element of D, we may write $\alpha \in u$ for $\alpha(u) = 1$ and think of u as a (basic open) set of points. The set $Sp(D)$ of points of D is then a topological space, and D is thought of as a point-free description of this space. If α and β are points of D then we write $\alpha \leqslant \beta$ to mean that $\alpha \in u$ implies $\beta \in u$ for all u in D. One defines classically $\mathsf{Kdim}\ D < n$ as meaning that there is no strict chain $\alpha_1 < \ldots < \alpha_n$ of points of D. Inspired by Espanol and Joyal [23] we gave in [9] the following point-free characterization of this notion.

Proposition 1.1 *Let us consider the distributive lattice $K_n(D)$ generated by the symbols $u_1(r), \ldots, u_n(r)$ for r in D and relations expressing that each u_i is a lattice map and that we have $u_i(r) \leqslant u_{i+1}(r)$. We have $\mathsf{Kdim}\ D < n$ iff for any sequence $r_2, \ldots, r_n$ in D we have*

$$u_2(r_2) \wedge \ldots \wedge u_n(r_n) \leqslant u_1(r_2) \vee \ldots \vee u_{n-1}(r_n)$$

in the lattice $K_n(D)$.

In [10], we give the following alternative constructive definition.

Proposition 1.2 *We have* $\mathsf{Kdim}\ D < n$ *iff any sequences* $a_1, \ldots, a_n$ *has a* complementary sequence, *that is a sequence* $b_1, \ldots, b_n$ *such that*

$$1 = a_1 \vee b_1,\ a_1 \wedge b_1 \leqslant a_2 \vee b_2, \ldots,\ a_n \wedge b_n = 0$$

In particular, we have that $\mathsf{Kdim}\ D < 1$ iff any element has a complement, that is iff D is a Boolean algebra.

1.2 Going-up and going-down property

Any map $\phi : Z \to V$ between two distributive lattices defines by composition a continuous map $\phi^* : Sp(V) \to Sp(Z)$. In this subsection, we collect some point-free formulations of properties of the map ϕ^*. The proofs are omitted.

It can be seen classically that the map ϕ^* is *surjective* iff the map ϕ is injective. Notice that the lattice map ϕ is injective iff $u \leqslant v$ for u, v in Z is *equivalent* to $\phi(u) \leqslant \phi(v)$. If we see the lattices Z, V as formal theory presenting the points of the spaces $Sp(Z), Sp(V)$ it means that the surjectivity of the map ϕ^* can be interpreted formally as a *conservativity* statement. (A typical application is for expressing and proving constructively *extension* theorems, like the Hahn-Banach Theorem, which become conservativity statements between two propositional geometric theories when expressed in a point-free way [7, 15].)

Proposition 1.3 *The map* ϕ^* *has the going-up property iff whenever* $\phi(u) \leqslant y \vee \phi(v)$ *there exists* $w \in Z$ *such that* $\phi(w) \leqslant y$ *and* $u \leqslant w \vee v$. *The map* ϕ^* *has the going-down property iff whenever* $y \wedge \phi(u) \leqslant \phi(v)$ *there exists* $w \in Z$ *such that* $y \leqslant \phi(w)$ *and* $w \wedge u \leqslant v$.

The corresponding map on points $\phi^* : Sp(V) \to Sp(Z)$ satisfies the going-up property iff whenever $\phi^*(\beta) \leqslant \alpha_1$ there exists $\beta_1 \geqslant \beta$ such that $\alpha_1 = \phi^*(\beta_1)$. It satisfies the going-down property iff whenever $\alpha_1 \leqslant \phi^*(\beta)$ there exists $\beta_1 \leqslant \beta$ such that $\alpha_1 = \phi^*(\beta_1)$.

1.3 Going-up property and Krull dimension

If ϕ^* has the going-up or going-down property and is surjective, it is clear in term of points that this implies $\mathsf{Kdim}\ Sp(Z) \leqslant \mathsf{Kdim}\ Sp(V)$. The following proposition expresses this implication in a point-free way.

Proposition 1.4 *If* $\phi : Z \to V$ *has the going-up or going-down property and is injective and* $\mathsf{Kdim}\ V < n$ *then* $\mathsf{Kdim}\ Z < n$.

Proof. We give only the proof for the going-up property (the going-down property follows by duality). Let $a_1, \ldots, a_n$ be an arbitrary sequence in Z. Since $\mathsf{Kdim}\ V < n$ we can find $v_1, \ldots, v_n$ in V such that

$$1 = \phi(a_1) \vee v_1,\ \phi(a_1) \wedge v_1 \leqslant \phi(a_2) \vee v_2, \ldots,\ \phi(a_n) \wedge v_n = 0$$

Since ϕ has the going-up property, we find successively $b_1, \ldots, b_n$ such that

$$\phi(b_1) \leqslant v_1, \ldots, \phi(b_n) \leqslant v_n$$

and

$$1 = a_1 \vee b_1,\ a_1 \wedge b_1 \leqslant a_2 \vee b_2, \ldots,\ a_{n-1} \wedge b_{n-1} \leqslant a_n \vee b_n$$

Since ϕ is injective we get also $a_n \wedge b_n = 0$ from $\phi(a_n \wedge b_n) = 0$ and this shows that $a_1, \ldots, a_n$ has a complementary sequence. □

2 The Zariski lattice of a ring

Joyal [27] defines the Zariski lattice of a commutative ring R to be the lattice $\mathsf{Zar}(R)$ generated by the symbols $D(a),\ a \in R$ and relations (called *support* relations [27])

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

If $b_1, \ldots, b_n$ are elements in R we write $D(b_1, \ldots, b_n)$ for $D(b_1) \vee \ldots \vee D(b_n)$. Because of the equality $D(a) \wedge D(b) = D(ab)$, any element of $\mathsf{Zar}(R)$ can be written in the form $D(b_1, \ldots, b_n)$. In general this cannot be simplified further[3]. It is direct to check from the support relations that we have $D(a) \leqslant D(b_1, \ldots, b_m)$ whenever a, or more generally some power of a, belongs to the ideal generated by $b_1, \ldots, b_m$. The reverse implication, which characterizes the lattice $\mathsf{Zar}(R)$ can be obtained by a cut-elimination argument [7]. In this case, it can be presented in the following algebraic way. A particular realization of a lattice satisfying the support relations is obtained by taking the lattice of radical of finitely generated ideals[4] of R and $D(b_1, \ldots, b_n)$ to be the radical of the ideal generated by $b_1, \ldots, b_n$. Since $\mathsf{Zar}(R)$ is the *free* lattice satisfying the support relations it follows from this remark that if $D(a) \leqslant D(b_1, \ldots, b_n)$ in $\mathsf{Zar}(R)$ then a belongs to the radical of the ideal generated by $b_1, \ldots, b_n$.

It is suggestive to think of $D(a)$ as the proposition $a \in S$, where S is the complement of a generic prime ideal of R. Another possible interpretation, in the case where $R = k[X_1, \ldots, X_n]$, is to see $D(a)$ as the complement of the set of zeros of the polynomials a in an algebraic closure of k. This is indeed a possible reading of Hilbert's Nullstellensatz Theorem.

The *Krull dimension* $\mathsf{Kdim}\ R$ of the ring R is defined to be the Krull dimension of the Zariski lattice $\mathsf{Zar}(R)$.

Theorem 2.1 *$\mathsf{Kdim}\ R < n$ iff for any sequence $x_1, \ldots, x_n$ in R there exists $k_1, \ldots, k_n$ in $\mathbb{N}$ and $a_1, \ldots, a_n$ in R such that*

$$x_1^{k_1}(x_2^{k_2} \cdots (x_n^{k_n}(1 + a_n x_n) + \cdots + a_2 x_2) + a_1 x_1) = 0.$$

Proof. See [9]. □

In particular, $\mathsf{Kdim}\ R < 1$ iff for any x in R there exists k and a such that $x^k(1 + ax) = 0$. This expresses the notion of Krull dimension directly in term of the ring structure. Notice that this statement involves an existential quantification over natural numbers, and is geometric [39], but not first-order.

3 The space of valuations

Let R be an integral domain and L be a field containing R. By analogy with Joyal's construction of the Zariski lattice, we consider the distributive lattice $\mathsf{Val}(L, R)$ generated by the symbols $V_R(s),\ s \in L$ and relations $1 = V_R(r)$ for r in R and for $s \neq 0, u_1, u_2$ in L

$$1 = V_R(s) \vee V_R(s^{-1}), \qquad V_R(u_1) \wedge V_R(u_2) \leqslant V_R(u_1 u_2) \wedge V_R(u_1 + u_2).$$

We write $V_R(u_1, \ldots, u_n)$ for $V_R(u_1) \vee \ldots \vee V_R(u_n)$. Intuitively, $V_R(s)$ means that s belongs to the "generic" valuation ring V of L containing R. In the case where L is the fraction field of R we write simply $\mathsf{Val}(R)$ instead of $\mathsf{Val}(L, R)$.

[3] But we have for instance $D(a, b) = D(a + b)$ if $D(ab) = 0$ [11].

[4] In general the lattice of ideals of R is *not* distributive, for instance in the case $R = k[X, Y]$.

Since we have only $V_R(x) \wedge V_R(y) \leqslant V_R(xy)$, in general we cannot simplify $V_R(x) \wedge V_R(y)$. However, we always have the equality $V_R(s) \wedge V_R(s^{-1}) = V_R(s+s^{-1})$[5]. We also have $V_R(r_1^{-1}) \wedge V_R(r_2^{-1}) = V_R((r_1r_2)^{-1})$ if $V_R(r_1) = V_R(r_2) = 1$.

Lemma 3.1 *$V_R((x+y)^{-1}) \leqslant V_R(x^{-1}, y^{-1})$ in $\mathsf{Val}(R)$. It follows from this that if $1 = s_1+\ldots+s_n$ then $1 = V_R(1/s_1, \ldots, 1/s_n)$ in $\mathsf{Val}(R)$.*

Proof. Let s be y/x. We have $1 = V_R(s, 1/s)$. Also $x^{-1} = (x+y)^{-1}(1+1/s)$ and $y^{-1} = (x+y)^{-1}(1+s)$. Hence the result. □

If V is a valuation ring containing R we can define a linear ordering on $L^\times$ by taking $x \leqslant_R y$ to mean $y/x \in V$. For any finite family $x_1, \ldots, x_n$ we have i such that $x_i \leqslant_R x_j$ for all j. The formal representation of this remark is expressed as follow.

Lemma 3.2 *For any $x_1, \ldots, x_n$ we have $1 = \vee_i \wedge_j V_R(x_j/x_i)$ in the lattice $\mathsf{Val}(R)$.*

Proof. By induction on n. Assume $1 = \vee_{i<n} \wedge_{j<n} V_R(x_j/x_i)$. We have also $1 = V_R(x_i/x_n, x_n/x_i)$ for each $i < n$. We can conclude from $V_R(x_i/x_n) \wedge \wedge_{j<n} V_R(x_j/x_i) \leqslant \wedge_j V_R(x_j/x_n)$. □

It follows from the axioms of V_R that $V_R(t_1) \wedge \ldots \wedge V_R(t_n) \leqslant V_R(p)$ whenever p belongs to $R[t_1, \ldots, t_n]$. More generally, if s is integral over $t_1, \ldots, t_n$, that is, if have a relation $s^k + p_1 s^{k-1} + \ldots + p_k = 0$ with $p_1, \ldots, p_k$ in $R[t_1, \ldots, t_n]$, then the equalities $s = -p_1 - p_2 s^{-1} - \ldots - p_k s^{-1+k}$ and $1 = V_R(s, s^{-1})$ show that we have $V_R(t_1) \wedge \ldots \wedge V_R(t_n) \leqslant V_R(s)$. The converse will follow from the following characterization of $\mathsf{Val}(L, R)$, which is proved by a cut-elimination argument.

Theorem 3.3 *If $t_1, \ldots, t_n, s_1, \ldots, s_m \in L^\times$ we have*

$$V_R(t_1) \wedge \ldots \wedge V_R(t_n) \leqslant V_R(s_1, \ldots, s_m)$$

iff $1 = <s_1^{-1}, \ldots, s_m^{-1}>$ in $R[t_1, \ldots, t_n, s_1^{-1}, \ldots, s_m^{-1}]$.

In particular, $V_R(t_1) \wedge \ldots \wedge V_R(t_n) \leqslant V_R(s)$ iff s is integral over $R[t_1, \ldots, t_n]$. For $n = 0$, we get that $1 = V_R(s)$ iff s is integral over R.

The last result can be seen as a point-free statement of the fact that the intersection of all valuation rings containing R is the integral closure of R.

Proof. This is proved, for another presentation of the lattice $\mathsf{Val}(R)$, in [16] by showing that the existence of such a polynomial identity, seen as relation between $\{t_1, \ldots, t_n\}$ and $\{s_1, \ldots, s_m\}$ defines an *entailment relation* [34].

For $V_R(t_1) \wedge \ldots \wedge V_R(t_n) \leqslant V_R(s)$ we get a polynomial identity $1 = s^{-1}q$ with $q \in R[t_1, \ldots, t_n, 1/s]$. By multiplying this equality by a large enough power of s we get a relation of the form $s^k = p_1 s^{k-1} + \ldots + p_k$ with $p_1, \ldots, p_m \in R[t_1, \ldots, t_n]$. □

Corollary 3.4 *We have $1 = V_R(s/t_1, \ldots, s/t_n)$ iff s is integral over the ideal generated by $t_1, \ldots, t_n$.*

That s is integral over the ideal I generated by $t_1, \ldots, t_n$ means that we can find a relation $s^m + a_1 s^{m-1} + \ldots + a_m = 0$ with a_1 in I, …, a_m in I^m.

[5] This follows from $V_R(s, s^{-1}) = 1$ and $V_R(t) \wedge V_R(s^{-1}) \leqslant V_R(s)$, $V_R(t) \wedge V_R(s) \leqslant V_R(s^{-1})$ where $t = s + s^{-1}$.

4 Center of a valuation

4.1 The center map

If V is a valuation ring containing R, then V is a local ring and its maximal ideal $\mathfrak{m}_V$ is the set of non invertible elements of V. The prime ideal $R\cap\mathfrak{m}_V$ of R is called the *center* of V. In point-free terms, this map $V\longmapsto R\cap\mathfrak{m}_V$ can be represented as the lattice map $\phi:\mathsf{Zar}(R)\to\mathsf{Val}(R)$ which is defined on generators by $\phi(D(0))=0$ and $\phi(D(r))=V_R(r^{-1})$ if $r\in R,\ r\neq 0$. Indeed, if $r\in R$ and $r\neq 0$ then $r\notin\mathfrak{m}_V$ iff r is invertible in V.

For defining formally this map, we need only, by initiality, to check that the support relations defining the lattice $\mathsf{Zar}(R)$ are validated by this interpretation.

Lemma 4.1 *In the lattice* $\mathsf{Val}(R)$ *the following relations hold, for any* $r,s\in R-\{0\}$

$$V_R(1)=1,\qquad V_R(1/rs)=V_R(1/r)\wedge V_R(1/s),\qquad V_R(1/(r+s))\leqslant V_R(1/r,1/s)$$

where in the last relation, we suppose also $r+s\neq 0$.

Proof. The relation $V_R(1/rs)=V_R(1/r)\wedge V_R(1/s)$ follows from $1=V_R(r)=V_R(s)$, and the last relation is a special case of Lemma 3.1. □

It follows from this that we can define a lattice map $\phi:\mathsf{Zar}(R)\to\mathsf{Val}(R)$ by $\phi(D(r))=V_R(1/r)$ if $r\neq 0$ and $\phi(0)=0$.

4.2 An application: Dedekind's Prague Theorem

The simple existence of the center map, which has been proved without using Theorem 3.3, allows us to transfer some results from the Zariski spectrum to the space of valuations. For instance, we have the following general on the Zariski spectrum. If $P=a_0+\ldots+a_nX^n$ is a polynomial in $R[X]$ we write $c(P)=D(a_0,\ldots,a_n)$ the *radical content* of P [23], which is an element of $\mathsf{Zar}(R)$.

Lemma 4.2 *(Gauss-Joyal) For any* P,Q *in* $R[X]$ *we have* $c(PQ)=c(P)\wedge c(Q)$.

Proof. See for instance [2]. □

Let now $a_0,\ldots,a_n,b_0,\ldots,b_m$ be *indeterminate*; we write $c_k=\Sigma_{i+j=k}a_ib_j$. We consider the ring $R=\mathbb{Z}[a_i/a_{i_0},b_j/b_{j_0}]$. Let $L=\mathbb{Q}(a_0,\ldots,a_n,b_0,\ldots,b_m)$ be the field of fractions of R. In the lattice $\mathsf{Zar}(R)$ we have $1=\vee D(c_k/a_{i_0}b_{j_0})$ by the previous Lemma. Using the center map for the ring R we deduce that we have $1=\vee V(a_{i_0}b_{j_0}/c_k)$ in the lattice $\mathsf{Val}(L,R)$. Hence in the lattice $\mathsf{Val}(L,\mathbb{Z})$ we have[6]

$$(1)\qquad \wedge V(a_i/a_{i_0})\wedge\wedge V(b_j/b_{j_0})\leqslant\vee V(a_{i_0}b_{j_0}/c_k).$$

Since $a_ib_j/c_k=a_i/a_{i_0}\cdot b_j/b_{j_0}\cdot a_{i_0}b_{j_0}/c_k$ this implies

$$\wedge V(a_i/a_{i_0})\wedge\wedge V(b_j/b_{j_0})\leqslant\wedge_{i,j}\vee_k V(a_ib_j/c_k)$$

By Lemma 3.2 we have $1=\vee_{i_0}\wedge V(a_i/a_{i_0})=\vee_{j_0}\wedge V(b_j/b_{j_0})$. We deduce from this discussion the following result[7].

[6] Our argument has the following suggestive interpretation. Let V be a generic valuation ring of L containing all elements a_i/a_{i_0} and b_j/b_{j_0}. The polynomials $P=1/a_{i_0}\Sigma a_iX^i,\ Q=1/b_{j_0}\Sigma b_jX^j$ are in $V[X]$. Since P and Q have 1 as coefficient, it follows from Lemma 4.2 that at least one coefficient of the product PQ is not in $\mathfrak{m}_V$. This is what is expressed by the inequality (1).

[7] Our argument precises the sketch which is presented at the end of [16].

Theorem 4.3 *In the lattice* $\mathsf{Val}(L,\mathbb{Z})$ *we have* $1 = \vee_k V(a_ib_j/c_k)$ *for any* i,j*, and hence by Corollary 3.4, each element* a_ib_j *is integral over the ideal generated by* $c_0,\dots,c_{n+m}$*.*

This result, which generalizes a famous Theorem of Gauss [20], is described by O. Neumann to be "one of the most basic result in commutative algebra of the XIXth century" [32]. Our argument is a computational interpretation of its modern non constructive proof based on valuations [3], which is a direct generalization of the reasoning of Gauss. Using Theorem 3.3, one can follow this proof and produce from it explicit polynomial identities. Via this general method of elimination of points, the map $L \to \mathsf{Val}(L,R)$ can thus be described as a (clever) system of notations which records polynomial identities. This is to be compared with the "actualist" interpretation of $\mathsf{Val}(L,R)$ as a set of points. In the spirit of Hilbert's program, we are helped by our intuition in term of points, but use it only as an ideal and suggestive mean.

4.3 Properties of the center map

The next result expresses in a point-free way that the center map is *surjective*, i.e. any prime ideal is the center of some valuation rings. The use of Theorem 3.3 seems essential.

Proposition 4.4 *The center map* $\phi : \mathsf{Zar}(R) \to \mathsf{Val}(R)$ *is injective.*

Proof. We show that we have $D(r) \leqslant D(s_1,\dots,s_m)$ iff, in the lattice $\mathsf{Val}(R)$, we have $V_R(r^{-1}) \leqslant V_R(s_1^{-1},\dots,s_m^{-1})$. By Theorem 3.3, this last relation means that we can find m polynomials $q_1,\dots,q_m$ in $R[r^{-1},s_1,\dots,s_m]$ such that $1 = s_1q_1 + \dots + s_mq_m$. This is then equivalent to the fact that r is in the radical of the ideal generated by $s_1,\dots,s_m$, which is equivalent to $D(r) \leqslant D(s_1,\dots,s_m)$. □

Proposition 4.5 *The center map* $\phi : \mathsf{Zar}(R) \to \mathsf{Val}(R)$ *has the going-up property.*

Proof. Assume, for some non zero elements $r, r_1,\dots,r_m$ in R and elements $s_1,\dots,s_m$ in L, that we have $\phi(D(r)) \leqslant V_R(s_1,\dots,s_m) \vee \phi(D(r_1,\dots,r_n))$. We can then find $q_1,\dots,q_m,p_1,\dots,p_n$ in $R[r^{-1},s_1^{-1},\dots,s_m^{-1}]$ such that $1 = \Sigma s_j^{-1}q_j + \Sigma r_ip_i$. By multiplying by a power of r we find a relation of the form $r^k - \Sigma t_ir_i = \Sigma s_j^{-1}l_j$ with t_i in R and l_j in $R[1/s_1,\dots,1/s_m]$. The element $w = r^k - \Sigma t_ir_i$ satisfies then both $D(r) \leqslant D(w,r_1,\dots,r_n)$ and $\phi(D(w)) \leqslant V_R(s_1,\dots,s_m)$ and we can apply Proposition 1.3. □

Corollary 4.6 *If* $\mathsf{Vdim}\ R \leqslant n$ *then* $\mathsf{Kdim}\ R \leqslant n$*.*

Proof. This follows from Proposition 1.4. □

5 Prüfer domain

The importance of the notion of Prüfer domain for constructive mathematics is stressed in [18]: it can be seen as a non Noetherian version of Dedekind domains, and several of the important properties of Dedekind domains can be proved at this level. (Classically, a Dedekind domain can be defined to be a Prüfer domain which is Noetherian.) We say that R is a Prüfer domain iff it is a domain satisfying

$$(*) \qquad \forall x\ y\ \exists\ u\ v\ w.\ \ ux = vy \wedge (1-u)y = wx.$$

Notice that being of Prüfer domain is a first-order property.

It follows easily from $(*)$, see [18], that if R is a Prüfer domain, for any sequence of elements $x_1,\dots,x_n$ of R we can find $a_{11} = u_1,\dots,a_{nn} = u_n$ in R such that

1. $a_{11} + \ldots + a_{nn} = 1$
2. for any j there exists a_{ij} such that $u_i x_j = a_{ij} x_i$

The matrix (a_{ij}) is a *principal localization matrix* of $x_1, \ldots, x_n$ [18][8]. We get $a_{ji} x_k x_j = a_{jj} x_k x_i = a_{jk} x_j x_i$ and hence $a_{ji} x_k = a_{jk} x_i$ if $x_j \neq 0$. It follows that we have $<a_{1i}, \ldots, a_{ni}> \cdot <x_1, \ldots, x_n> = <x_i>$. We find in this way explicitly an *inverse* of the ideal $<x_1, \ldots, x_n>$ [18][9].

Let $\mathsf{Div}(R)$ be the monoid of fractional ideals, also called *divisors* of R [20]. We have just proved that, if R is a Prüfer domain then $\mathsf{Div}(R)$ is a group. If we order $\mathsf{Div}(R)$ by reverse inclusion, we see that $\mathsf{Div}(R)$ is a *lattice group.* From this simple fact follows directly[10] important properties [3, 13]: $\mathsf{Div}(R)$ is a *distributive* lattice, and the intersection of two fractional ideals I, J can be computed as $I \cap J = I \cdot J \cdot (I + J)^{-1}$ (and is thus finitely generated). Hence any Prüfer domain is *coherent* [31] and we can solve any linear system over it [18]. We stress that all these arguments are constructive and can be seen as (relatively simple) algorithms on R, which use as a basic procedure the hypothesis $(*)$.

Classically, the lattice group $\mathsf{Div}(R)$ is defined to be the free lattice group on the set of prime ideals of R. In our setting, this is captured by the following result.

Proposition 5.1 *The spectrum of the lattice group* $\mathsf{Div}(R)$ *[13] is the dual of the Zariski spectrum of R.*

Proof. The spectrum of $\mathsf{Div}(R)$ is shown in [13] to be isomorphic to the lattice of positive elements of $\mathsf{Div}(R)$, that is the finitely generated ideal of R, with the order $I \preceq J$ iff there exists n such that $I \leqslant J^n$. This is equivalent to say that J is included into the radical of I. □

Proposition 5.2 *If R is a Prüfer domain then the center map $\phi : \mathsf{Zar}(R) \to \mathsf{Val}(R)$ is an isomorphism.*

Proof. By Proposition 4.4 it is enough to show that the map ϕ is surjective[11]. Since $\mathsf{Val}(R)$ is generated by the elements $V_R(s)$, we show that each such element is in the image of ϕ. We write $s = x/y$ with $x, y \in R$. Since R is a Prüfer domain there exist $u, v, w \in R$ such that $ux = vy$ and $(1 - u)y = wx$. We can then check that we have $V_R(s) = \phi(D(u, w))$ if $s \neq 0$. □

The converse of Proposition 5.2 holds if R is integrally closed. For proving this converse, we state a general lemma, which expresses in a point-free way that an integral domain is arithmetical iff any localization at a prime ideal is a valuation domain.

Lemma 5.3 *Let R be an integral domain, and K its field of fractions. The following is a sufficient condition for R to be a Prüfer domain: for any s in $K^\times$ there exists $a_1, \ldots, a_n, b_1, \ldots, b_m$ in R such that $1 = D(a_1, \ldots, a_n, b_1, \ldots, b_m)$ and s is in $R[1/a_i]$ for all i and $1/s$ is in $R[1/b_j]$ for all j.*

Proof. We can find N big enough and u_i, v_j in R such that $s = v_i/a_i^N$ and $1/s = w_j/b_j^N$. Since $1 = D(a_1, \ldots, a_n, b_1, \ldots, b_m)$ we can find x_i and y_j such that $1 = \Sigma x_i a_i^N + \Sigma y_j b_j^N$. If $u = \Sigma x_i a_i^N$, $v = \Sigma x_i v_i$ and $w = \Sigma w_j b_j^N$ we have then $us = v$ and $(1 - u)1/s = w$. □

[8] In the localization $R[1/u_i]$ the ideal $<x_1, \ldots, x_n>$ is principal and equal to $<x_i>$.

[9] Dedekind himself thought that the existence of such an inverse was *the* fundamental result about the ring of integers of an algebraic field of numbers [1]. Theorem 5.10 shows that this ring is a Prüfer domain.

[10] The structure of lattice group was discovered by Dedekind and rediscovered independently by F. Riesz. It plays an important rôle in abstract functional analysis [13].

[11] Proposition 4.4 relies on cut-elimination (Theorem 3.3). One can prove directly, by a somewhat longer argument, that ϕ is a bijection without using Theorem 3.3.

Lemma 5.4 *If R is a Prüfer domain then R is integrally closed.*

Proof. Let K be the field of fractions of R. Assume s in in K and $s \neq 0$ and we have a relation $s^n + r_1 s^{n-1} + \ldots + r_n = 0$ with $r_1, \ldots, r_n$ in R. We can find u, v, w in R such that $su = v,\ sw = 1-u$. If $u = 1$ then s is in R. If $u = 0$ we have $s = -r_1 - r_2 w - \ldots - r_n w^{n-1}$ is in R. Finally if $u \neq 0$ and $u \neq 1$ we have s in $R[1/u]$ and, since $s(1-u)^{n-1} = -r_1(1-u)^{n-1} - r_2 w(1-u)^{n-2} - \ldots - r_n w^n$, it is also in $R[1/1-u]$. Hence s is in $R[1/u] \cap R[1/1-u] = R$, as desired[12]. □

Proposition 5.5 *If R is an integrally closed domain such that the center map $\phi : \mathsf{Zar}(R) \to \mathsf{Val}(R)$ is an isomorphism then R is a Prüfer domain.*

Proof. We use Lemma 5.3. Let s be an element of $K^\times$. We have $1 = V_R(s, 1/s)$. Since the center map ϕ is surjective we can find $a_1, \ldots, a_n$ and $b_1, \ldots, b_m$ in R such that $V_R(s) = \phi(u)$ and $V_R(1/s) = \phi(D(b_1, \ldots, b_m))$ where $u = D(a_1, \ldots, a_n)$ and $v = D(b_1, \ldots, b_m)$. We have $1 = \phi(u \vee v)$ and hence $1 = u \vee v$ in $\mathsf{Zar}(R)$. Also $V_R(1/a_i) \leqslant V_R(s)$ and $V_R(1/b_j) \leqslant V_R(1/s)$ in $\mathsf{Val}(R)$. Since R is integrally closed, so are $R[1/a_i]$ and $R[1/b_j]$, and so $V_R(1/a_i) \leqslant V_R(s)$ implies $s \in R[1/a_i]$ and $V_R(1/b_j) \leqslant V_R(1/s)$ implies $1/s \in R[1/b_j]$ by Theorem 3.3. □

The following proposition was obtained while analyzing Seidenberg's Lemma ([26], Chapitre III, Proposition 2) in a point-free setting. We rediscovered in this way Gilmer-Hoffmann's Theorem [25]. As above, let R be an integral domain and K be its field of fractions. For $s \in K$ we let $I(s)$ to be the set of all polynomials P in $R[X]$ such that $P(s) = 0$.

Proposition 5.6 *(Gilmer-Hoffmann's Theorem) If for all $s \in K^\times$ there exists $P_1, \ldots, P_n$ in $I(s)$ such that $1 = c(P_1) \vee \ldots \vee c(P_n)$ in $\mathsf{Zar}(R)$*[13] *and R is integrally closed then R is a Prüfer domain.*

Proof. For any P in $I(s)$ we show how to build a family $u_1, \ldots, u_m$ in R such that $c(P) \leqslant D(u_1, \ldots, u_m)$ and we have s or $1/s$ in $R[1/u_i]$ for each i. The result follows then from Lemma 5.3.

Write $P = a_n X^n + \ldots + a_0$. We define

$$b_n = a_n,\ b_{n-1} = b_n s + a_{n-1},\ b_{n-2} = b_{n-1} s + a_{n-2}, \ldots,\ b_1 = b_2 s + a_1$$

Notice that $P(s) = b_1 s + a_0 = 0$. We have

$$c(P) \leqslant D(b_n, b_n s, b_{n-1}, b_{n-1} s, \ldots, b_1, b_1 s)$$

since $D(a_n) = D(b_n)$ and $D(a_i) \leqslant D(b_{i+1} s, b_i)$ for $0 < i < n$ and $D(a_0) = D(b_1 s)$. Since we have $P(s) = a_n s^n + \ldots + a_0 = 0$ and R is integrally closed, we can prove successively that $b_n, b_n s, b_{n-1}, \ldots$ are all in R. Finally, we have $1/s$ in $R[1/b_i s]$ and s in $R[1/b_i]$. □

Corollary 5.7 *If $\mathsf{Kdim}\ R[X] \leqslant 2$ and R is integrally closed then R is a Prüfer domain.*

Proof. We use Proposition 5.6. Given s in K we build P, Q in $I(s)$ such that $1 = c(P) \vee c(Q)$ in $\mathsf{Zar}(R)$. For this, we write $s = a/b$ with a, b in R and $b \neq 0$. We apply Theorem 2.1 to the

[12] This reasoning can be seen as the interpretation that a valuation ring is integrally closed in the sheaf model over the Zariski spectrum of R.

[13] It is direct to see that this is equivalent to $c(P) = 1$ for *one* P in $I(s)$, but our formulation is more convenient in the applications.

sequence $bX - a, b, X$ in $R[X]$, using $\mathsf{Kdim}\ R[X] < 3$. It follows that there exists p_1, p_2, p_3 in $R[X]$ and k_1, k_2, k_3 in $\mathbb{N}$ such that

$$(bX - a)^{k_1}(b^{k_2}(X^{k_3}(1 + Xp_3) + bp_2) + (bX - a)p_1) = 0$$

Since R is an integral domain, this can be simplified to $b^{k_2}(X^{k_3}(1+Xp_3)+bp_2)+(bX-a)p_1 = 0$. If we specialise X to s we get $b^{k_2}(s^{k_3}(1 + sp_3(s)) + bp_2(s)) = 0$ and hence since $b \neq 0$ we have $s^{k_3}(1 + sp_3(s)) + bp_2(s) = 0$. If we take $P = bX - a$ and $Q = X^{k_3}(1 + Xp_3(X)) + bp_2(X)$ we have P, Q in $I(s)$ and $1 = c(P) \vee c(Q)$ in $\mathsf{Zar}(R)$ as desired. □

Here is another application, which was first obtained as a corollary of Proposition 6.5 and Corollary 5.7.

Corollary 5.8 *If R is an integral domain which is integrally closed and such that* $\mathsf{Vdim}\ R \leqslant 1$ *then R is a Prüfer ring.*

Proof. We proceed like in the proof of Corollary 5.7. We write $s = a/b$ with a, b in R and $b \neq 0$. Since $\mathsf{Vdim}\ R \leqslant 1$ we have $\mathsf{Kdim}\ R[s] \leqslant 1$ by Corollary 4.6. Hence we can apply Theorem 2.1 to the sequence b, s: there exists p_1, p_2 in $R[X]$ and k_1, k_2 in $\mathbb{N}$ such that $b^{k_1}(s^{k_2}(1 + sp_2(s)) + bp_1(s)) = 0$. Since $b \neq 0$ this simplifies to $s^{k_2}(1 + sp_2(s)) + bp_1(s) = 0$. If we take $P = bX - a$ and $Q = X^{k_2}(1 + Xp_2(X)) + bp_1(X)$ we have P, Q in $I(s)$ and $1 = c(P) \vee c(Q)$ in $\mathsf{Zar}(R)$ as desired. □

This can be compared with the characterization in [18]: if R is integrally closed and *coherent* and such that $\mathsf{Kdim}\ R \leqslant 1$ then R is a Prüfer ring.

The following Lemma will be needed in the definition of the genus of an algebraic curve.

Lemma 5.9 *Let R be a Prüfer domain, and K its field of fractions. If s is in K then $R[s]$ is a Prüfer domain. It follows that if $s_1, \dots, s_n$ are in K then $R[s_1, \dots, s_n]$ is a Prüfer domain.*

Proof. Using Proposition 5.6 it is enough to show that $R[s]$ is integrally closed. Like in the proof of Proposition 5.2 we find u, v, w in R such that $us = v,\ ws = 1-u$. If $u = 0$ then $R[s] = R[1/w]$ is integrally closed. If $u = 1$ then $s = v$ is in R and $R[s] = R$ is integrally closed by Lemma 5.4. If $u \neq 0$ and $u \neq 1$ we claim that $R[s] = R[1/u] \cap R[1/w]$, which will show that $R[s]$ is integrally closed since both $R[1/u]$ and $R[1/w]$ are integrally closed. Indeed we have s in $R[1/u]$ and $R[1/w]$. Conversely if x is in $R[1/u]$ and $R[1/w]$ we can write $x = p/u^n = q/w^n = qs^n/(1-u)^n$. We can then find a, b in R such that $au^n + b(1-u)^n = 1$ and we have $x = ap + bqs^n$ in $R[s]$. □

Another more direct application is a simple proof of the fundamental fact that the integral closure of a Bezout domain[14] in an extension of its field of fractions is a Prüfer domain.

Theorem 5.10 *If S is the integral closure of a Bezout domain R in a field extension of the field of fractions of R then S is a Prüfer domain*[15].

Proof. We use Proposition 5.6. Given s in the field of fractions of S we have a non zero polynomial P in in $R[X]$ such that $P(s) = 0$. Since R is a Bezout domain, we can compute the gcd g of the coefficients of P and we can then write $P = gQ$ with $Q(s) = 0$ and $c(Q) = 1$. (Notice that we find a polynomial in $I(s)$ which is even in $R[X]$.) □

[14] A *Bezout* domain is a domain where any finitely generated ideal is principal [31].

[15] Two particular important cases are $R = \mathbb{Z}$ (algebraic integers) and $R = k[X]$ (algebraic curves).

6 Polynomial rings

Proposition 6.1 *An integral domain R satisfies $\mathsf{Vdim}\ R \leqslant n$ iff in the Boolean algebra generated by the symbols $V_0(s), \ldots, V_n(s)$ and relations*

$$\begin{array}{rcl} 1 = V_i(r), & & 1 = V_i(s) \vee V_i(s^{-1}), \\ V_i(u_1) \wedge V_i(u_2) & \leqslant & V_i(u_1 u_2) \wedge V_i(u_1 + u_2), \\ V_i(s) & \leqslant & V_{i+1}(s) \end{array}$$

we have $1 = \bigvee_{1 \leqslant i \leqslant n}(V_i(s_i) \leftrightarrow V_{i-1}(s_i))$ for any sequence $s_1, \ldots, s_n$.

Proof. This follows from Proposition 1.1. □

Using the distributive laws of Boolean algebra, we deduce that for any finite subset $Z \subseteq L$ we have

$$1 = \bigvee_{1 \leqslant i \leqslant n} \bigwedge_{s \in Z} (V_i(s) \leftrightarrow V_{i-1}(s))$$

It is suggestive to write $V_i =_Z V_{i-1}$ for $\bigwedge_{s \in Z}(V_i(s) \leftrightarrow V_{i-1}(s))$ and to rewrite the previous equality as $1 = \bigvee_{1 \leqslant i \leqslant n} V_i =_Z V_{i-1}$. Classically, given a chain of valuation rings $V_0, \ldots, V_n$ we have i such that $V_i = V_{i-1}$. Our constructive version is weaker, stating only that we have i such that V_i and V_{i-1} coincides on a given finite subset Z of L. Similarly, one can show the following result.

Lemma 6.2 *If we have $\mathsf{Vdim}\ R \leqslant n$ then in the theory representing a chain of $n + 2$ valuation rings $V_0, \ldots, V_{n+1}$, for any finite subset $Z \subseteq L$ we have*

$$1 = \bigvee_{1 \leqslant i < j \leqslant n+1} (V_i =_Z V_{i-1} \wedge V_j =_Z V_{j-1})$$

Classically, given any such chain $V_0, \ldots, V_{n+1}$ there exists $i < j$ such that $V_{i-1} = V_i$ and $V_{j-1} = V_j$.

We now prove constructively that we have $\mathsf{Vdim}\ R[X] \leqslant n+1$ if $\mathsf{Vdim}\ R \leqslant n$. The argument is a syntactical version of the proof in [26].

Lemma 6.3 *For any integral domain R if we have $s_1 + \ldots + s_n = 0$, with $s_1, \ldots s_n \in L^\times$ then $1 = \bigvee_{1 \leqslant i < j \leqslant n} V_R(s_i/s_j) \wedge V_R(s_j/s_i)$.*

Proof. Let u be the right hand-side of this equality. Since $1 + \Sigma_{j \neq k} s_j/s_k = 0$, by Lemma 3.1 we have $1 = \vee_{j \neq k} V(s_k/s_j)$ for all k. It follows that we have $\wedge_j V(s_j/s_k) \leqslant u$ for all k. The result follows then from Lemma 3.2. □

Lemma 6.4 *For any p, q in $L(X)$ there exists a finite subset Z of L such that, in the propositional theory generated by symbols $V_1(p), V_2(p), V_3(p), V_4(p)$ for $p \in L(X)$ and relations expressing that V_1, V_2, V_3, V_4 is a chain of valuation rings of $L(X)$ containing $R[X]$,*

$$(V_2 =_Z V_1 \wedge V_4 =_Z V_3) \leqslant (V_2(p) \leftrightarrow V_1(p)) \vee (V_4(q) \leftrightarrow V_3(q))$$

Classically, if we have such a chain of valuation rings containing $R[X]$ and such that $V_1 \cap L = V_2 \cap L$ and $V_3 \cap L = V_4 \cap L$ then we have $V_1 = V_2$ or $V_3 = V_4$.

Proof. The elements p, q are algebraically dependent over L and there exists $s_{l,m}$ in $L^\times$ such that $\Sigma s_{l,m} p^l q^m = 0$. Using Lemma 6.3 it follows from this that we have a finite number of elements t_i in $L^\times$ with $l_i \neq 0$ or $m_i \neq 0$ such that

$$1 = \bigvee_i (V_1(t_i p^{l_i} q^{m_i}) \wedge V_1(t_i^{-1} p^{-l_i} q^{-m_i}))$$

For each i it follows from the axioms of V_i that we have

$$\begin{array}{rcl} V_2 =_Z V_1 \wedge V_4 =_Z V_3 & \wedge & V_1(t_i p^{l_i} q^{m_i}) \wedge V_1({t_i}^{-1} p^{-l_i} q^{-m_i}) \\ & \leqslant & (V_2(p) \leftrightarrow V_1(p)) \vee (V_4(q) \leftrightarrow V_3(q)) \end{array}$$

where Z is the set of all elements t_i and t_i^{-1}. It follows from this that we have

$$(V_2 =_Z V_1 \wedge V_4 =_Z V_3) \leqslant (V_2(p) \leftrightarrow V_1(p)) \vee (V_4(q) \leftrightarrow V_3(q))$$

as desired. □

Proposition 6.5 *If* $\mathsf{Vdim}\ R \leqslant n$ *then* $\mathsf{Vdim}\ R[X] \leqslant n + 1$.

Proof. We consider the propositional theory of the chain of $n + 2$ valuation rings $V_0, \ldots, V_{n+1}$ containing $R[X]$. Given any sequence $p_1, \ldots, p_{n+1}$ of elements in $L(X)$ we find, using Lemma 6.4 a finite subset Z of L such that, for each $i < j$

$$(V_i =_Z V_{i-1} \wedge V_j =_Z V_{j-1}) \leqslant (V_i(p_i) \leftrightarrow V_{i-1}(p_i)) \vee (V_j(p_j) \leftrightarrow V_{j-1}(p_j))$$

From Lemma 6.2 we also have

$$1 = \bigvee_{1 \leqslant i < j \leqslant n+1} (V_i =_Z V_{i-1} \wedge V_j =_Z V_{j-1})$$

It follows that we have $1 = \bigvee_{1 \leqslant i \leqslant n+1} (V_i(p_i) \leftrightarrow V_{i-1}(p_i))$ as desired. □

An important consequence of Proposition 6.5, Theorem 5.2 and Corollary 4.6 is the following.

Theorem 6.6 *If* R *is a Prüfer domain and* $\mathsf{Kdim}\ R \leqslant n$ *then the Krull dimension of* $R[X_1, \ldots, X_m]$ *is* $\leqslant n + m$.

For instance for $R = \mathbb{Z}$ we get a constructive proof that the Krull dimension of $\mathbb{Z}[X_1, \ldots, X_m]$ is $m + 1$. A challenge is to have a direct proof of this result. A proof of $\mathsf{Kdim}\ \mathbb{Z}[X] = 2$ with the characterization of Theorem 2.1 is not so easy to derive directly.

7 Towards point-free algebraic geometry

We apply the previous results to give a simple point-free description of the notion of algebraic curves as a scheme. For this we need to develop some sheaf theory in a point-free setting, up to the cohomological definition of the genus, following the fundamental paper of Serre [36]. All our definitions and proofs are constructive, but follow closely the intuitions given by the classical picture. Once the basic definitions are in place (but this was the main difficulty here), the logical structures of proofs using cohomology theory are quite elementary, most arguments being of a direct algebraic nature.

7.1 Sheaves over lattices

We will analyze now how to represent the notion of sheaves of abelian groups in our setting. Since for us, a space is a distributive lattice, we have to define what is a sheaf $\mathcal{F}$ over a distributive lattice D.

A *presheaf* of rings $\mathcal{F}$ over a distributive lattice D is a family $\mathcal{F}(U)$ of rings for each U in D together with restriction maps $\rho_{VU} : \mathcal{F}(U) \to \mathcal{F}(V),\ x \longmapsto x|V$ whenever $V \leqslant U$. We require furthermore that $x|U = x$ if x is in $\mathcal{F}(U)$, and that $(x|V)|W = x|W$ if $W \leqslant V \leqslant U$. If x is in $\mathcal{F}(U)$ and y is in $\mathcal{F}(V)$, we may write simply $x = y$ on $U \wedge V$ for expressing that $x|U \wedge V = y|U \wedge V$ in $\mathcal{F}(U \wedge V)$. We say that $\mathcal{F}$ is a *sheaf* iff the following gluing conditions are satisfied:

1. if $u = U_1 \vee U_2$, and x_1 in $\mathcal{F}(U_1)$, x_2 in $\mathcal{F}(U_2)$ satisfy $x_1 = x_2$ on $U_1 \wedge U_2$ then there exists one and only one $x \in \mathcal{F}(U)$ such that $x|U_i = x_i$,

2. $\mathcal{F}(0)$ is the trivial ring 0.

It follows from the first condition that if $u = U_1 \vee U_2$ and x, y in $\mathcal{F}(U)$ are such that $x = y$ on both U_1 and U_2 then $x = y$. If $\mathcal{F}$ is a sheaf on a lattice D, it is clear that it defines by restriction a sheaf on any lattice $\downarrow U$ for U in D.

If R is an arbitrary integral domain, an important sheaf on the lattice $\mathsf{Zar}(R)$ is the *structure sheaf* on R[16].

Lemma 7.1 *If $D(b) \leqslant D(a_1, \ldots, a_n)$ in $\mathsf{Zar}(R)$, where $b, a_1, \ldots, a_n$ are $\neq 0$, then $R[1/a_1] \cap \ldots \cap R[1/a_n] \subseteq R[1/b]$.*

Proof. Assume that u is in $R[1/a_1] \cap \ldots \cap R[1/a_n]$. One can find k and $r_1, \ldots, r_n$ in R such that $u = r_i/a_i^k$. Since $D(a_i) = D(a_i^k)$, we know that some power b^l of b is of the form $\Sigma s_i a_i^k$ with s_i in R. We have then $u = (\Sigma s_i r_i)/b^l$ and hence u is in $R[1/b]$. □

An element of $\mathsf{Zar}(R)$ is 0 or of the form $D(a_1, \ldots, a_n)$ where all a_i are $\neq 0$. We define $\mathcal{O}(D(a_1, \ldots, a_n))$ to be $R[1/a_1] \cap \ldots \cap R[1/a_n]$, and $\mathcal{O}(0)$ to be 0. This definition is justified by Lemma 7.1. If $V = D(b_1, \ldots, b_m) \leqslant D(a_1, \ldots, a_n) = U$ and x is in $R[1/a_1] \cap \ldots \cap R[1/a_n]$, we have also x in $R[1/b_1] \cap \ldots \cap R[1/b_m]$ and we define $x|V$ to be x itself. The sheaf condition is then clearly satisfied.

A structure sheaf is also called an *affine scheme*.

Notice that, by definition, the global sections of this sheaf are the elements of $\Gamma(\mathsf{Zar}(R), \mathcal{O}) = \mathcal{O}(D(1)) = R$.

7.2 Algebraic curves and schemes

Let k be a field. An *algebraic curve* is defined to be an algebraic extension L of a a field of rational functions $k(x)$, where x is an indeterminate. If $a_1, \ldots, a_n$ are elements of L we write $E(a_1, \ldots, a_n)$ the set of elements of L that are integral over $k[a_1, \ldots, a_n]$. If a is an element of L it is algebraic over $k(x)$ and hence we have a polynomial relation $P(a, x) = 0$. Since equality is decidable in L, we can test if this equality is of the form $P(a) = 0$, that is a is algebraic over k, in which case a is said to be a *constant* of L, or if x is algebraic over $k(a)$, in which case a is said to be a *parameter* of L. If p is a parameter, L is the field of fractions of $E(p)$, since this field contains x because x is algebraic over $E(p)$.

[16] This can be defined for an arbitrary ring, but the definition is a little simpler for an integral domain, and we shall only need this case.

Any non zero element of the formal space $X = \mathsf{Val}(L, k)$ can be written as a disjunction of elements of the form $V(a_1) \wedge \ldots \wedge V(a_n)$. If U is such a non zero element, we define $\mathcal{O}_X(U)$ to be the set of elements q in L such that $U \leqslant V(q)$ in $\mathsf{Val}(L, k)$[17]. In particular $\mathcal{O}_X(V(a_1) \wedge \ldots \wedge V(a_n))$ is the set $E(a_1, \ldots, a_n)$, by Theorem 3.3. Thus $\Gamma(X, \mathcal{O}_X) = \mathcal{O}_X(X)$, the global sections of $\mathcal{O}_X$, is the field of constants k_0 of L (algebraic closure of k in L). The fact that $\Gamma(X, \mathcal{O}_X) = k_0$ is an algebraic counterpart of the fact that the global holomorphic functions on a Riemann surface are the constant functions.

A point α of $\mathsf{Val}(L, k)$ can be identified with the valuation ring V_α of elements a such that $\alpha \in V(a)$. The *fiber* of $\mathcal{O}_X$ at a point α is defined to be the inductive limit of $\mathcal{O}_X(U)$ with $\alpha \in u$. The fiber at α is nothing else than V_α itself.

If b is a non zero element of $E(a)$ we have $E(a, 1/b) = E(a)[1/b]$. More generally, if $b_1, \ldots, b_m$ are non zero elements of $E(a)$, we have

$$\mathcal{O}_X(V(a) \wedge V(1/b_1, \ldots, 1/b_m)) = E(a)[1/b_1] \cap \ldots \cap E(a)[1/b_m].$$

If p is a parameter of L, and ϕ is the center map of $E(p)$ and $q_1, \ldots, q_m$ are non zero elements of $E(p)$ and U is the element $D(q_1, \ldots, q_m)$ of $\mathsf{Zar}(E(p))$ we deduce from our discussion the equality

$$\mathcal{O}_{E(p)}(U) = E(p)[1/q_1] \cap \ldots \cap E(p)[1/q_m] = \mathcal{O}_X(\phi(U)).$$

By Theorem 5.10, $E(p)$ is a Prüfer domain. By Proposition 5.2, the sub-lattice $\downarrow V(p)$ of $\mathsf{Val}(L, k)$, which is isomorphic to $\mathsf{Val}(E(p))$, is isomorphic to $\mathsf{Zar}(E(p))$. Hence, the sheaf $\mathcal{O}_X$ restricted to the basic open $V(p)$ is isomorphic to the affine scheme $\mathsf{Zar}(E(p)), \mathcal{O}$.

The pair $(X, \mathcal{O}_X)$, where $X = \mathsf{Val}(L, k)$, is a most natural example of a *scheme*. For each parameter p of L the space X is the union of two basic open sets $U_0 = V(p)$, $U_1 = V(1/p)$. The open U_0 is isomorphic to $\mathsf{Zar}(E(p))$ and U_1 is isomorphic to $\mathsf{Zar}(E(1/p))$. Furthermore the sheaf $\mathcal{O}_X$ reduces to the structure sheaf over each open U_i. (Surprisingly, I was unable to find this example in the literature.)

Notice that, even in the simplest case where $L = k(t)$, the sheaf $\mathcal{O}_X$ is not isomorphic to an affine scheme. This follows from the observation that $\Gamma(X, \mathcal{O}_X)$ is the field of constants of L, while we have seen that $\Gamma(\mathsf{Zar}(R), \mathcal{O}) = R$ for the structure sheaf of an integral domain R.

7.3 Places

Following [20], a *place* P of L/k is given by two parameters α, β such that $V(\alpha^{-1}, \beta^{-1}) \neq 1$ and $L = k_0(\alpha, \beta)$ and α, β satisfy a polynomial relation $f(\alpha, \beta) = 0$ with $f(X, Y)$ in $k_0[X, Y]$ such that $f(0, 0) = 0$ and $f'_X(0, 0) \neq 0$ or $f'_Y(0, 0) \neq 0$. (For instance $x - 1/2, y - 1/2$ determines a place of $L/\mathbb{Q}$ if L is defined by the equation $x^3 + y^3 = xy$.) The set

$$V_P = \{z \in L \mid 1 = V(\alpha^{-1}, \beta^{-1}, z)\}$$

is then a (discrete) valuation ring of L and it is possible to define a valuation function $v_P : L^\times \to \mathbb{Z}$ such that z is in V_P iff $v_P(z) \geqslant 0$ [20].

We can *decide* if the point V_P is in a given open $V(t_1) \wedge \ldots \wedge V(t_k)$ of X since this is equivalent to having $v_P(t_1) \geqslant 0, \ldots, v_P(t_k) \geqslant 0$[18]. It is also possible to represent $X - \{P\}$ as the formal open $V(\alpha^{-1}, \beta^{-1})$ and we can express formally that an element g has a unique pôle of order l at the point P on the open U of X by the inequality $U \wedge V(\alpha^{-1}, \beta^{-1}) \leqslant V(g)$ and $v_P(g) = -l$.

[17] Intuitively, q is a meromorphic function on the abstract Riemann surface X, and $U \leqslant V(q)$ expresses that q is holomorphic over the open U.

[18] The membership in a general valuation ring of L needs not to be decidable a priori.

Lemma 7.2 *There exist a formal covering of X by two open W_0, W_1 and an element g such that P is not in W_0 and g has a unique (simple) pôle at P on W_1.*

Proof. If for instance $f'_x(0,0) \neq 0$, we have a relation of the form $\beta l = \alpha h$ with l in $k_0[\beta]$ and $v_P(h) = 0$. We can then check that β^{-1} has a unique (simple) pôle at the point P on the open $V(h^{-1})$: we have $V(h^{-1}) \wedge V(\alpha^{-1}) \leqslant V(\beta^{-1})$ which follows from the relation $\beta l = \alpha h$. We get two open $W_0 = V(\alpha^{-1}, \beta^{-1})$ and $W_1 = V(h^{-1})$ that cover X and are such that P is not in W_0 and β^{-1} has a unique (simple) pôle at P on W_1. □

7.4 The genus of an algebraic curve

Lemma 7.3 *For any parameter p we have $E(p, q, 1/q) = E(p, q) \oplus E(p, 1/q)$.*

Proof. Let R be $E(p)$ which is a Prüfer ring of field of fractions L. It follows from Lemma 5.9 that we have $E(p, q) = R[q]$, $E(p, 1/q) = R[1/q]$ and $E(p, q, 1/q) = R[q, 1/q]$. We clearly have $R[q, 1/q] = R[q] \oplus R[1/q]$, hence the result[19]. □

Theorem 7.4 *The k_0-vector space $H^1(p) = E(p, 1/p)/E(p) \oplus E(1/p)$ is* independent *of the parameter p and hence it defines an* invariant *$H^1(X, \mathcal{O}_X)$ of the extension L/k.*

Proof. Our argument is a specialization of the general cohomological argument [36][20]. Let p and q be two parameters. Write $p_0 = p,\ p_1 = 1/p$ and $q_0 = q,\ q_1 = 1/q$. We say that x in $E(p, 1/p)$ and y in $E(q, 1/q)$ are related iff there exists a_{ij} in $E(p_i, q_j)$ such that $x = a_{10} - a_{00} = a_{11} - a_{01}$ and $y = a_{01} - a_{00} = a_{11} - a_{10}$. Using Lemma 7.3, we show that this relation defines an isomorphism between $H^1(p)$ and $H^1(q)$.

We have first that y is uniquely determined modulo $E(q) \oplus E(1/q)$. Indeed, if we have other elements b_{ij} in $E(p_i, q_j)$ such that

$$x = b_{10} - b_{00} = b_{11} - b_{01}, \qquad y' = b_{01} - b_{00} = b_{11} - b_{10}$$

then $b_{10} - a_{10} = b_{00} - a_{00}$ belongs to $E(q, p) \cap E(q, 1/p) = E(q)$. Similarly $b_{11} - a_{11} = b_{01} - a_{01}$ belongs to $E(1/q, p) \cap E(1/q, 1/p) = E(1/q)$. Hence $y' - y$ belongs to $E(q) \oplus E(1/q)$.

We show that any element x in $E(p, 1/p)$ is related to at least one element y in $E(q, 1/q)$. Indeed x belongs to $E(p, 1/p, q)$, which is $E(q, p) \oplus E(q, 1/p)$ by Lemma 7.3, and hence it can be written $x = a_{10} - a_{00}$ with a_{i0} in $E(p_i, q_0)$. Similarly x can be written $a_{11} - a_{01}$ with a_{i1} in $E(p_i, q_1)$. We can then let y to be $a_{11} - a_{10} = a_{01} - a_{00}$ which belongs to $E(q, 1/q, p) \cap E(q, 1/q, 1/p) = E(q, 1/q)$. □

We illustrate these notions in the cases of the curve $S = \mathbb{Q}(t)$ and in the case of the algebraic curve $L = \mathbb{Q}(x, y)$ with $y^2 = 1 - x^4$, an example which played historically an important rôle [24, 22]. In this case, $1, y$ is a basis of $E(x)$ over $\mathbb{Q}[x]$ and $1, y/x^2$ a basis of $E(1/x)$ over $\in \mathbb{Q}[1/x]$. It follows that the elements of $E(x, 1/x) = E(x)[1/x]$ can be written (uniquely) in the form $p + qy + ry/x + a + (y/x^2)b$ with $r \in \mathbb{Q}$ and $p, q \in \mathbb{Q}[x],\ a, b \in \mathbb{Q}[1/x]$[21].

Proposition 7.5 *We have $H^1(L, \mathcal{O}_X) = E(x, 1/x)/E(x) \oplus E(1/x) = \mathbb{Q}$.*

[19] This result has a direct cohomological interpretation since it follows from the fact that the sheaf $\mathcal{O}_X$ restricted to the basic open $V(p)$ is isomorphic to an affine scheme and that a structure sheaf is acyclic.

[20] $H^1(p)$ is the quotient $H^1(U_0, U_1)$ of $\mathcal{O}_X(U_0 \wedge U_1)$ by $\mathcal{O}_X(U_0) \oplus \mathcal{O}_X(U_1)$ where $U_0 = V(p)$ and $U_1 = V(1/p)$.

[21] More generally, as soon as we have a basis of $E(x)$ over $k[x]$ and a basis of $E(1/x)$ over $k[1/x]$ a simple argument shows that $H^1(X, \mathcal{O}_X)$ is a finite dimensional vector space over k [22]. This gives also a way to compute the field of constants k_0.

For $S = \mathbb{Q}(t)$ we have $E(t, 1/t) = k[t, 1/t]$ and $E(t) = k[t],\ E(1/t) = k[1/t]$.

Proposition 7.6 *We have $H^1(S, \mathcal{O}_X) = 0$.*

Since these are invariant attached to the function field L we get the result.

Proposition 7.7 *$L = \mathbb{Q}(x, y),\ y^2 = 1 - x^4$ cannot be written on the form $L = \mathbb{Q}(t)$.*

While it is possible to prove directly this Proposition, we think that it is a good illustration of the power of cohomological methods.

Here is another simple application.

Proposition 7.8 *If $H^1(X, \mathcal{O}_X) = 0$ and P is a place of X then there exists a function on X having P as the only (simple) pôle*[22].

Proof. By Lemma 7.2, we have a function g and a covering W_0, W_1 of X such that P is not in W_0 and g has P as the only (simple) pôle on W_1. It follows that g is in $\mathcal{O}_X(W_0 \wedge W_1)$. Since $H^1(X, \mathcal{O}_X) = 0$, we have[23] $\mathcal{O}_X(W_0 \wedge W_1) = \mathcal{O}_X(W_0) \oplus \mathcal{O}_X(W_1)$ and we can write g on the form $h_1 - h_0$ with h_i in $\mathcal{O}_X(W_i)$. The element $f = h_1 = h_0 + g$ is the required function[24]. □

8 Conclusion

Our work is complementary to existing constructive presentations of Riemann surfaces [19, 20, 21, 22]. Our use of formal topology, which is a reformulation of Hilbert's notion of introduction and elimination of ideal elements, allows us to have access to the power of abstract methods (prime ideals, valuations), in the same way as [13, 14] simplify some proofs of Bishop.

One motivation for the present work comes actually from a formalization of the associativity property of elliptic curves in type theory [38]. Our setting should contain all the elements for a conceptual and constructive proof of this result, which should be directly representable in type theory.

Acknowledgement

I would like to thank Henri Lombardi, Claude Quitté and Peter Schuster for several discussions on the topic of this paper.

References

[1] J. Avigad. Methodology and metaphysics in the development of Dedekind's theory of ideals. In *The architecture of modern mathematics*, 159–186, Oxford Univ. Press, Oxford, 2006.

[2] B. Banaschewski and J. J. C. Vermeulen. Polynomials and radical ideals. *Journal of pure and applied algebra*, (113):219–227, 1996.

[3] N. Bourbaki. *Eléments de Mathématique. Algèbre commutative. Chapitre 7.* Paris, Hermann, 1965.

[22] More generally, if $H^1(X, \mathcal{O}_X) = k_0^n$ the same argument shows the existence of a function f having P as the only pôle, of order $\leqslant n + 1$.

[23] This follows by an argument similar to the proof of Theorem 7.4.

[24] It can then be shown that we have $L = k_0(f)$. One can instantiate this argument on simple cases such as $y^2 = x(1 - x)$, finding in this way the function y/x.

[4] Th. Coquand. Constructive topology and combinatorics. Constructivity in computer science (San Antonio, TX, 1991), 159–164, Lecture Notes in Comput. Sci., 613.

[5] Th. Coquand. An analysis of Ramsey's theorem. *Inform. and Comput.* 110 (1994), no. 2, 297–304.

[6] Th. Coquand. Minimal invariant spaces in formal topology. *J. Symbolic Logic* 62 (1997), no. 3, 689–698.

[7] J. Cederquist and Th. Coquand. Entailment Relations and Distributive Lattices. *Proceeding of Logic Colloquium 1998.*

[8] Th. Coquand and H. Lombardi. A logical approach to abstract algebra. *Math. Structures Comput.* Sci. 16 (2006), no. 5, 885–900.

[9] Th. Coquand and H. Lombardi. Hidden constructions in abstract algebra (3) Krull dimension. in *Commutative ring theory and applications* (Fez, 2001), 477–499, Lecture Notes in Pure and Appl. Math., 231, Dekker, New York, 2003.

[10] Th. Coquand, H. Lombardi and M.F. Roy. An elementary characterization of Krull dimension. in *From sets and types to topology and analysis*, 239–244, Oxford Logic Guides, 48, 2005.

[11] Th. Coquand, H. Lombardi, C. Quitte. Generating non-Noetherian modules constructively. *Manuscripta mathematica*, 115, 513-520 (2004)

[12] Th. Coquand, G. Sambin, J. Smith, S. Valentini. Inductively generated formal topologies. *Ann. Pure Appl. Logic* 124 (2003), no. 1-3, 71–106.

[13] Th. Coquand. About Stone's notion of spectrum. *J. Pure Appl. Algebra* 197 (2005), no. 1-3, 141–158.

[14] Th. Coquand and B. Spitters. Formal topology and constructive mathematics: the Gelfand and Stone-Yosida representation theorems. *J.UCS* 11 (2005), no. 12, 1932–1944.

[15] Th. Coquand. Geometric Hahn-Banach theorem. *Math. Proc. Cambridge Philos. Soc.* 140 (2006), no. 2, 313–315.

[16] Th. Coquand and H. Persson. Valuations and Dedekind's Prague Theorem. *J. Pure Appl. Algebra* 155 (2001), no. 2-3, 121–129.

[17] R. Dedekind and H. Weber Theorie des algebraischen Funktionen einer Veränderlichen. *J. de Crelle*, t. XCII (1882), p. 181-290.

[18] L. Ducos, H. Lombardi, C. Quitté and M. Salou. Théorie algorithmique des anneaux arithmétiques, des anneaux de Prüfer et des anneaux de Dedekind. *J. Algebra* 281 (2004), no. 2, 604–650.

[19] H.M. Edwards. The genesis of ideal theory. *Arch. Hist. Ex. Sci.*, pages 321–378, 1980.

[20] H.M. Edwards. *Divisor Theory.* Birkauser Boston, 1990.

[21] H.M. Edwards. Mathematical ideas, ideals, and ideology. *Math. Intelligencer* 14 (1992), no. 2, 6–19.

[22] H.M. Edwards. *Essays in Constructive Mathematics.* Springer-Verlag, New York, 2005.

[23] L. Espanol. The spectrum lattice of Baer rings and polynomials. *Categorical algebra and its applications (Louvain-La-Neuve, 1987)*, pages 118–124, 1988.

[24] K.F. Gauss. *Disquisitiones Arithmeticae.* 1802.

[25] R. Gilmer, J.F. Hoffmann. A characterization of Prüfer domains in terms of polynomials. *Pacific J. Math.* 60 (1), 81-85 (1975).

[26] P. Jaffard. *Théorie de la dimension dans les anneaux de polynomes.* Mémor. Sci. Math., Fasc. 146 Gauthier-Villars, Paris 1960.

[27] A. Joyal. Le théorème de Chevalley-Tarski. *Cahiers de Topologie et Géométrie Différentielle* 16, 256–258 (1975).

[28] P. T. Johnstone. *Stone Spaces.* Cambridge studies in advanced mathematics 3, 1982.

[29] H. Lombardi, C. Quitté. *Algèbre Commutative, Modules projectifs de type fini.* forthcoming. Preliminary version available at the home page of H. Lombardi.

[30] P. Martin-Löf. *Notes on constructive mathematics.* Almqvist and Wiksell, Stockholm, 1970. 109 pp.

[31] R. Mines, F. Richman and W. Ruitenburg. *A course in constructive algebra.* Springer-Verlag, 1988

[32] O. Neumann. On the early history of commutative algebra. Talk at MSRI.

[33] G. Sambin. Intuitionistic formal spaces—a first communication. In *Mathematical Logic and its Applications*, D. Skordev (Ed.), Plenum, New York, 1987, pp. 187–204.

[34] D. Scott. Completeness and axiomatizability. *Proceedings of the Tarski Symposium, (1974), p. 411-435.*

[35] Seidenberg A note on the dimension theory of rings. *Pacific J. Math.* 3, (1953). 505–512.

[36] J.P. Serre. Faisceaux Algébriques Cohérents. *Ann. of Math.*, (2) 61, (1955), 197–278.

[37] M. Stone. Topological representations of distributive lattices and Brouwerian logics. *Cas. Mat. Fys.* 67, (1937), 1-35.

[38] L. Thery and G. Hanrot. Primality Proving with Elliptic Curves. to appear in the proceeding of TPHOL, 2007.

[39] G. C. Wraith. Intuitionistic algebra: some recent developments in topos theory. Proceedings of the International Congress of Mathematicians (Helsinki, 1978), pp. 331–337, Acad. Sci. Fennica, Helsinki, 1980.