Hidden constructions in abstract algebra (3)
Krull Dimension of distributive lattices and commutative rings

Thierry Coquand (*) Henri Lombardi (†),

may 2002

Abstract

We present constructive versions of Krull's dimension theory for commutative rings and distributive lattices. The foundations of these constructive versions are due to Joyal, Español and the authors. We show that the notion of Krull dimension has an explicit computational content in the form of existence (or lack of existence) of some algebraic identities. We can then get an explicit computational content where abstract results about dimensions are used to show the existence of concrete elements. This can be seen as a partial realisation of Hilbert's program for classical abstract commutative algebra.

MSC 2000: 13C15, 03F65, 13A15, 13E05

Key words: Krull dimension, distributive lattices, Constructive Mathematics.

* Chalmers, University of Göteborg, Sweden, email: coquand@cs.chalmers.se

† Equipe de Mathématiques, CNRS UMR 6623, UFR des Sciences et Techniques, Université de Franche-Comté, 25 030 BESANCON cedex, FRANCE, email: lombardi@math.univ-fcomte.fr

Contents

Introduction **3**

1 Distributive lattice, Entailment relations **4**
1.1 Distributive lattices, filters and spectrum 4
1.2 Distributive lattices and entailment relations 8
1.3 Spectrum and completeness theorem 9

2 Krull dimension of distributive lattices **10**
2.1 Definition of $\mathrm{Kr}_\ell(L)$ 10
2.2 Partially specified chains of prime ideals 12
2.3 Krull dimension of a distributive lattice 12
2.4 Implicative lattice 13
2.5 Decidability 14
2.6 Dimension of Spectral Spaces 14
2.7 Connections with Joyal's definition 14

3 Zariski and Krull lattice **15**
3.1 Zariski lattice 15
3.2 Krull lattices of a commutative ring 16
3.3 Krull dimension of a polynomial ring over a discrete field 18

Bibliographie **20**

Annex: The completeness theorem and LLPO **22**
A.4 Theories and models 22
A.5 Completeness theorem 22
A.6 Compactness theorem 22
A.7 LPO and LLPO 23
A.8 Geometric formulae and theories 23

Introduction

We present constructive versions of Krull's dimension theory for commutative rings and distributive lattices. The foundations of these constructive versions are due to Joyal, Español and the authors. We show that the notion of Krull dimension has an explicit computational content in the form of existence (or lack of existence) of some algebraic identities. This confirms the feeling that commutative algebra can be seen computationally as a machine that produces algebraic identities (the most famous of which being called Nullstellensatz). This can be seen as a partial realisation of Hilbert's program for classical abstract commutative algebra.

Our presentation follows Bishop's style (cf. in algebra [19]). As much as possible, we kept minimum any explicit mention to logical notions. When we say that we have a constructive version of an abstract algebraic theorem, this means that we have a theorem the proof of which is constructive, which has a clear computational content, and from which we can recover the usual version of the abstract theorem by an immediate application of a well classified non-constructive principle. An abstract classical theorem can have several distinct interesting constructive versions.

In the case of abstract theorem in commutative algebra, such a non-constructive principle is the completeness theorem, which claims the existence of a model of a formally consistent propositional theory. We recall the exact formulation of this theorem in the appendix, as well as its derivation from the compactness theorem When this is used for algebraic structures of enumerable presentation (in a suitable sense) the compactness and completeness theorem can be seen as a reformulation of Bishop **LLPO** (a real number is ≥ 0 or ≤ 0).

To avoid the use of completeness theorem is not motivated by philosophical but by practical considerations. The use of this principle leads indeed to replace quite direct (but usually hidden) arguments by indirect ones which are nothing else than a double contraposition of the direct proofs, with a corresponding lack of computational content. For instance [2] the abstract proof of 17th Hilbert's problem claims : if the polynomial P is not a sum of rational fractions there is a field K in which one can find an absurdity by reading the (constructive) proof that the polynomial is everywhere positive or zero. The direct version of this abstract proof is: from the (constructive) proof that the polynomial is everywhere positive or zero, one can show (using arguments of the abstract proofs) that any attempt to build K will fail. This gives explicitly the sum of squares we are looking for. In the meantime, one has to replace the abstract result: "any real field can be ordered" by the constructive theorem: "in a field in which any attempt to build an ordering fails -1 is a sum of squares". One can go from this explicit version to the abstract one by completeness theorem, while the proof of the explicit version is hidden in the algebraic manipulations that appear in the usual classical proof of the abstract version.

Here is the content of the paper.

Distributive lattices
In this section, we present basic theorems on distributive lattices. An important simplification of proofs and computations is obtained via the systematic use of the notion of entailment relation, which has its origin in the cut rule in Gentzen's sequent calculus, with the fundamental theorem 1.7.

Dimension of distributive lattices In this section, we develop the theory of Krull dimension of distributive lattices, explaining briefly the connection with Español's developments of Joyal' s theory. We show that the property to have a Krull dimension $\leq \ell$ can be formulated as the existence of concrete equalities in the distributive lattice.

Zariski and Krull lattice In section 3 we define the Zariski lattice of a commutative ring (whose elements are radicals of finitely generated ideals), which is the constructive counterpart of Zariski spectrum : the points of Zariski spectrum are the prime ideals of Zariski lattice, and the constructible subsets of Zariski spectrum are the elements of the Boolean algebra generated by the Zariski lattice. Joyal's idea is to define Krull dimension of a commutative ring as the dimension of its Zariski lattice. This avoids any mention of prime ideals. We show the equivalence between this (constructive) point of view and the (constructive) presentation given in [14], showing that the property to have a Krull dimension $\leq \ell$ can be formulated as the existence of concrete equalities in the ring.

Conclusion
This article confirms the actual realisation of Hilbert's program for a large part of abstract commutative algebra. (cf. [2, 4, 10, 11, 12, 13, 14, 15, 16, 17]). The general idea is to replace ideal abstract structures by *partial specifications* of these structures. The very short elegant abstract proof which uses these ideal objects has then a corresponding computational version at the level of the partial specifications of these objects. Most of classical results in abstract commutative algebra, the proof of which seem to require in an essential way excluded middle and Zorn's lemma, seem to have in this way a corresponding constructive version. Most importantly, the abstract proof of the classical theorem always contains, more or less implicitly, the constructive proof of the corresponding constructive version.
Finally, we should note that the explicit characterisations of Krull dimension of distributive lattices, theorem 2.9, of spectral spaces, theorem 2.14, and of rings, corollary 3.6, are new.

1 Distributive lattice, Entailment relations

Elementary though it has become after successive presentations and simplifications, the theory of distributive lattices is the ideal instance of a mathematical theory, where a syntax is specified together with a complete description of all models, and what is more, a table of semantic concepts and syntactic concepts is given, together with a translation algorithm between the two kinds of concepts. Such an algorithm is a "completeness theorem" (G. C. Rota [20]).

1.1 Distributive lattices, filters and spectrum

As indicated by the quotation above, the structure of distributive lattices is fundamental in mathematics, and G.C. Rota has pointed out repeatedly its potential relevance to commutative algebra and algebraic geometry. A distributive lattice is an ordered set with finite sups and infs, a minimum element (written 0) and a maximum element (written 1). The operations sup and inf are supposed to be distributive w.r.t. the other. We write these operations $\vee$ and $\wedge$. The relation $a \leq b$ can then be defined by $a \vee b = b$ or, equivalently, $a \wedge b = a$. The theory of distributive lattices is then purely equational. It makes sense then to talk of distributive lattices defined by generators and relations.

A quite important rule, the *cut rule*, is the following

$$(((x \wedge a) \leq b) \quad \& \quad (a \leq (x \vee b))) \implies a \leq b.$$

In order to prove this, write $x \wedge a \wedge b = x \wedge a$ and $a = a \wedge (x \vee b)$ hence

$$a = (a \wedge x) \vee (a \wedge b) = (a \wedge x \wedge b) \vee (a \wedge b) = a \wedge b.$$

A totally ordered set is a distributive lattice as soon as it has a maximum and a minimum element. We write $\mathbf{n}$ for the totally ordered set with n elements (this is a distributive lattice for $n \neq 0$.) A product of distributive lattices is a distributive lattice. Natural numbers with the divisibility relation form a distributive lattice (with minimum element 1 and maximum element 0). If L and L' are two distributive lattices, the set $\mathrm{Hom}(L, L')$ of all morphisms (*i.e.*, maps preserving sup, inf, 0 and 1) from L to L' has a natural order given by

$$\varphi \leq \psi \quad \overset{\text{def}}{\Longleftrightarrow} \quad \forall x \in L \;\; \varphi(x) \leq \psi(x).$$

A map between two totally ordered distributive lattices L and S is a morphism if, and only if, it is nondecreasing and 0_L and 1_L are mapped into 0_S and 1_S.

The following proposition is direct.

Proposition 1.1 *Let L be a distributive lattice and J a subset of L. We consider the distributive lattice L' generated by L and the relations $x = 0$ for $x \in J$ (L' is a quotient of L). Then*

- *the equivalence class of* 0 *is the set of a such that for some finite subset J_0 of J:*

$$a \;\leq\; \bigvee_{x \in J_0} x \quad \text{in } L$$

- *the equivalence class of* 1 *is the set of b such that for some finite subset J_0 of J:*

$$1 \;=\; \left(b \;\vee\; \bigvee_{x \in J_0} x \right) \quad \text{in } L$$

- *More generally $a \leq_{L'} b$ if, and only if, for some finite subset J_0 of J:*

$$a \;\leq\; \left(b \;\vee\; \bigvee_{x \in J_0} x \right)$$

In the previous proposition, the equivalence class of 0 is called an *ideal* of the lattice; it is the ideal generated by J. We write it $\langle J \rangle_L$. We can easily check that an ideal I is a subset such that:

$$\begin{array}{rcl} & & 0 \in I \\ x, y \in I & \Longrightarrow & x \vee y \in I \\ x \in I,\; z \in L & \Longrightarrow & x \wedge z \in I \end{array}$$

(the last condition can be written $(x \in I,\; y \leq x) \Rightarrow y \in I$).

Furthermore, for any morphim $\varphi : L_1 \to L_2$, $\varphi^{-1}(0)$ is an ideal of L_1.

A *principal ideal* is an ideal generated by one element a. We have $\langle a \rangle_L = \{x \in L \;;\; x \leq a\}$. Any finitely generated ideal is principal.

The dual notion of ideal is the one of *filter*. A filter F is the inverse image of 1 by a morphism. This is a subset such that:

$$\begin{array}{rcl} & & 1 \in F \\ x, y \in F & \Longrightarrow & x \wedge y \in F \\ x \in F,\; z \in T & \Longrightarrow & x \vee z \in F \end{array}$$

Notation 1.2 We write $\mathrm{P_f}(X)$ for the set of all finite subsets of the set X. If A is a finite subset of a distributive lattice L we define

$$\bigvee A := \bigvee_{x\in A} x \qquad \text{and} \qquad \bigwedge A := \bigwedge_{x\in A} x$$

We write $A \vdash B$ or $A \vdash_L B$ for the relation defined on the set $\mathrm{P_f}(L)$:

$$A \vdash B \quad \overset{\text{def}}{\Longleftrightarrow} \quad \bigwedge A \leq \bigvee B$$

Note the relation $A \vdash B$ is well defined on finite subsets because of associativity commutativity and idempotence of the operations $\wedge$ and $\vee$. Note also $\emptyset \vdash \{x\} \Rightarrow x = 1$ and $\{y\} \vdash \emptyset \Rightarrow y = 0$. This relation satisfies the following axioms, where we write x for $\{x\}$ and A, B for $A \cup B$.

$$\begin{array}{rcccl} & & a & \vdash & a & (R) \\ (A \vdash B)\ \&\ (A \subseteq A')\ \&\ (B \subseteq B') & \Longrightarrow & A' & \vdash & B' & (M) \\ (A, x \vdash B)\ \&\ (A \vdash B, x) & \Longrightarrow & A & \vdash & B & (T) \end{array}$$

we say that the relation is reflexive, monotone and transitive. The last rule is also called emphcut rule. Let us also mention the two following rules of "distributivity":

$$\begin{array}{rcl} (A,\ x \vdash B)\ \&\ (A,\ y \vdash B) & \Longleftrightarrow & A,\ x \vee y \vdash B \\ (A \vdash B,\ x)\ \&\ (A \vdash B,\ y) & \Longleftrightarrow & A \vdash B,\ x \wedge y \end{array}$$

The following is proved in the same way as proposition 1.1.

Proposition 1.3 *Let L be a distributive lattice and (J, U) a pair of subsets of L. We consider the distributive lattice L' generated by L and by the relations $x = 0$ for $x \in J$ and $y = 1$ for $y \in U$ (L' is a quotient of L). We have that:*

- *the equivalence class of 0 is the set of elements a such that:*

$$\exists J_0 \in \mathrm{P_f}(J),\ U_0 \in \mathrm{P_f}(U) \qquad a,\ U_0 \vdash_L J_0$$

- *the equivalence class of 1 is the set of elements b such that: vérifient:*

$$\exists J_0 \in \mathrm{P_f}(J),\ U_0 \in \mathrm{P_f}(U) \qquad U_0 \vdash_L b,\ J_0$$

- *More generally $a \leq_{L'} b$ if, and only if, there exists a finite subset J_0 of J and a finite subset U_0 of U such that, in L:*

$$a,\ U_0 \vdash_L b,\ J_0$$

We shall write $L/(J = 0, U = 1)$ for the quotient lattice L' described in proposition 1.3. Let $\psi : L \to L'$ be the canonical surjection. If I is the ideal $\psi^{-1}(0)$ and F the filter $\psi^{-1}(1)$, we say that the *ideal I and the filter F are conjugate*. By the previous proposition, an ideal I and a filter F are conjugate if, and only if, we have:

$$\begin{array}{l} [I_0 \in \mathrm{P_f}(I),\ F_0 \in \mathrm{P_f}(F),\ (x,\ F_0 \vdash I_0)] \Longrightarrow x \in I \qquad \text{and} \\ [I_0 \in \mathrm{P_f}(I),\ F_0 \in \mathrm{P_f}(F),\ (F_0 \vdash x,\ I_0)] \Longrightarrow x \in F. \end{array}$$

This can also be formulated as follows:

$$(f \in F,\ x \wedge f \in I) \Longrightarrow x \in I \quad \text{and} \quad (j \in I,\ x \vee j \in F) \Longrightarrow x \in F.$$

When an ideal I and a filter F are conjugate, we have

$$1 \in I \iff 0 \in F \iff (I, F) = (L, L).$$

We shall also write $L/(I, F)$ for $L' = T/(J = 0, U = 1)$. By proposition 1.3, a homomorphism φ from L to another lattice L_1 satisfying $\varphi(J) = \{0\}$ and $\varphi(U) = \{1\}$ can be factorised in an unique way through the quotient L'.

As shown by the example of totally ordered sets a quotient of distributive lattices is not in general characterised by the equivalence classes of 0 and 1.

Classically a *prime ideal* I of a lattice is an ideal whose complement F is a filter (which is then a *prime filter*). This can be expressed by

$$1 \notin I \qquad \text{and} \qquad (x \wedge y) \in I \implies (x \in I \text{ or } y \in I) \qquad\qquad (*)$$

which can also be expressed by saying that I is the kernel of a morphism from L into the lattice with two elements written **2**. Constructively, at least in the case where L is discrete, it seems natural to take the definition $(*)$, where "or" is used constructively. The notion of prime filter is then defined in a dual way.

Definition 1.4 *Let L be a distributive lattice.*

- *An* idealistic prime *in L is given by a pair (J, U) of finite subsets of L. We consider this as an incomplete specification for a prime ideal P satisfying $J \subseteq P$ and $U \cap P = \emptyset$.*
- *To any idealistic prime (J, U) we can associate a pair (I, F) as described in proposition 1.3 where I is an ideal, F is a filter and I, F are conjugate.*
- *We say that the idealistic prime (J, U)* collapses *iff we have $I = F = L$. This means that the quotient lattice $L' = T/(J = 0, U = 1)$ is a singleton i.e., $1 \leq_{L'} 0$, which means also $U \vdash J$.*

Theorem 1.5 (Simultaneous collapse for idealistic primes) *Let (J, U) be an idealistic prime for a lattice L and x be an element of L. If the idealistic primes $(J \cup \{x\}, U)$ and $(J, U \cup \{x\})$ collapse, then so does (J, U).*

Proof.
We have two finite subsets J_0, J_1 of J and two finite subsets U_0, U_1 of U such that

$$x,\ U_0 \vdash J_0 \quad \text{and} \quad U_1 \vdash x,\ J_1$$

hence

$$x,\ U_0,\ U_1 \vdash J_0,\ J_1 \quad \text{and} \quad U_0,\ U_1 \vdash x,\ J_0,\ J_1$$

By the cut rule

$$U_0,\ U_1 \vdash J_0,\ J_1$$

□

Notice the crucial role of the cut rule.

1.2 Distributive lattices and entailment relations

An interesting way to analyse the description of distributive lattices defined by generators and relations is to consider the relation $A \vdash B$ defined on the set $\mathrm{P_f}(L)$ of finite subsets of a lattice L. Indeed if $S \subseteq L$ generates the lattice L, then the relation $\vdash$ on $\mathrm{P_f}(S)$ is enough to characterise the lattice L, because any formula on S can be rewritten, in normal conjunctive form (inf of sups in S) and normal disjunctive form (sup of infs in S). Hence if we want to compare two elements of the lattice generated by S we write the first in normal disjunctive form, the second in normal conjunctive form, and we notice that

$$\bigvee_{i\in I}\Big(\bigwedge A_i\Big) \leq \bigwedge_{j\in J}\Big(\bigvee B_j\Big) \qquad \Longleftrightarrow \qquad \&_{(i,j)\in I\times J}\ (A_i \vdash B_j)$$

Definition 1.6 *For an arbitrary set S, a relation over $\mathrm{P_f}(S)$ which is reflexive, monotone and transitive (see page 6) is called an* entailment relation.

The notion of entailment relations goes back to Gentzen sequent calculus, where the rule (T) (the cut rule) is first explicitly stated, and plays a key role. The connection with distributive lattices has been emphasized in [3, 4]. The following result (cf. [3]) is fundamental. It says that the three properties of entailment relations are exactly the ones needed in order to have a faithfull interpretation in distributive lattices.

Theorem 1.7 (fundamental theorem of entailment relations) *Let S be a set with an entailment relation $\vdash_S$ over $\mathrm{P_f}(S)$. Let L be the lattice defined by generators and relations as follows: the generators are the elements of S and the relations are*

$$\bigwedge A \leq \bigvee B$$

whenever $A \vdash_S B$. For any finite subsets A and B of S we have

$$A \vdash_L B \qquad \Longleftrightarrow \qquad A \vdash_S B.$$

Proof.
We give an explicit possible description of the lattice L. The elements of L are represented by finite sets of finite sets of elements of S

$$X = \{A_1, \ldots, A_n\}$$

(intuitively X represents $\bigwedge A_1 \vee \cdots \vee \bigwedge A_n$). We define then inductively the relation $A \prec Y$ with $A \in \mathrm{P_f}(S)$ and $Y \in L$ (intuitively $\bigwedge A \leq \bigvee_{C\in Y}(\bigwedge C)$)

- if $B \in Y$ and $B \subseteq A$ then $A \prec Y$
- if $A \vdash_S y_1, \ldots, y_m$ and $A, y_j \prec Y$ for $j = 1, \ldots, m$ then $A \prec Y$

It is easy to show that if $A \prec Y$ and $A \subseteq A'$ then we have also $A' \prec Y$. It follows that $A \prec Z$ holds whenever $A \prec Y$ and $B \prec Z$ for all $B \in Y$. We can then define $X \leq Y$ by $A \prec Y$ for all $A \in X$ and one can then check that L is a distributive lattice[1] for the operations

$$0 = \emptyset, \quad 1 = \{\emptyset\}, \quad X \vee Y = X \cup Y, \quad X \wedge Y = \{A \cup B \mid A \in X,\ B \in Y\}.$$

For establishing this one first show that if $C \prec X$ and $C \prec Y$ we have $C \prec X \wedge Y$ by induction on the proofs of $C \prec X$ and $C \prec Y$. We notice then that if $A \vdash_S y_1, \ldots, y_m$ and $A, y_j \vdash_S B$ for all j then $A \vdash_S B$ using m times the cut rule. It follows that if we have $A \vdash_L B$, *i.e.*, $A \prec \{\{b\} \mid b \in B\}$, then we have also $A \vdash_S B$. □

[1] L is actually the quotient of $\mathrm{P_f}(\mathrm{P_f}(S))$ by the equivalence relation: $X \leq Y$ and $Y \leq X$.

As a first application, we give the description of the Boolean algebra generated by a distributive lattice. A Boolean algebra can be seen as a distributive lattice with a complement operation $x \mapsto \overline{x}$ such that $x \wedge \overline{x} = 0$ and $x \vee \overline{x} = 1$. The application $x \mapsto \overline{x}$ is then a map from the lattice to its dual.

Proposition 1.8 *Let L be a distributive lattice. There exists a free Boolean algebra generated by L. It can be described as the distributive lattice generated by the set $L_1 = L \cup \overline{L}$ ([2]) with the entailment relation $\vdash_{L_1}$ defined as follows: if A, B, A', B' are finite subsets of L we have*

$$A, \overline{B} \vdash_{L_1} A', \overline{B'} \quad \overset{\text{def}}{\Longleftrightarrow} \quad A, B' \vdash A', B \quad \text{in } L$$

If we write L_{Bool} for this lattice (which is a Boolean algebra), there is a natural embedding of L_1 in L_{Bool} and the entailment relation of L_{Bool} induces on L_1 the relation $\vdash_{L_1}$.

Proof.
See [3]. □

Notice that by Theorem 1.7 we have $x \vdash_L y$ if, and only if, $x \vdash_{L_1} y$ hence the canonical map $L \to L_1$ is one-to-one and L can be identified to a subset of L_1.

1.3 Spectrum and completeness theorem

The *spectrum* of the lattice L, written $\mathrm{Spec}(L)$ is defined as the set $\mathrm{Hom}(L, \mathbf{2})$. It is isomorphic to the ordered set of all detachable prime ideals. The order relation is then reverse inclusion. We have $\mathrm{Spec}(\mathbf{2}) \simeq \mathbf{1}$, $\mathrm{Spec}(\mathbf{3}) \simeq \mathbf{2}$, $\mathrm{Spec}(\mathbf{4}) \simeq \mathbf{3}$, etc...

Proposition 1.9 *The completeness theorem implies the following result. If (J, U) is an idealistic prime which does not collapse then there exists $\varphi \in \mathrm{Spec}(L)$ such that $J \subseteq \varphi^{-1}(0)$ and $U \subseteq \varphi^{-1}(1)$. In particular if $a \not\leq b$, there exists $\varphi \in \mathrm{Spec}(L)$ such that $\varphi(a) = 1$ and $\varphi(b) = 0$. Also, if $L \neq \mathbf{1}$, $\mathrm{Spec}(L)$ is nonempty.*

Proof.
This follows from the completeness theorem for geometric theories (see Appendix). □

A corollary is the following representation theorem (Birkhoff theorem)

Theorem 1.10 (Representation theorem) *The completeness theorem implies the following result. The map $\theta_L : L \to \mathcal{P}(\mathrm{Spec}(L))$ defined by $a \mapsto \{\varphi \in \mathrm{Spec}(L) \ ; \ \varphi(a) = 1\}$ is an injective map of distributive lattice. This means that any distributive lattice can be represented as a lattice of subsets of a set.*

Another corollary is the following proposition.

Proposition 1.11 *The completeness theorem implies the following result. Let $\varphi : L \to L'$ a map of distributive lattices; φ is injective if, and only if, $\mathrm{Spec}(\varphi) : \mathrm{Spec}(L') \to \mathrm{Spec}(L)$ is surjective.*

[2] $\overline{L}$ is a disjoint copy of L.

Proof.
We have the equivalence

$$a \neq b \iff a \wedge b \neq a \vee b \iff a \vee b \not\leq a \wedge b$$

Assume that $\mathrm{Spec}(\varphi)$ is surjective. If $a \neq b$ in L, take $a' = \varphi(a)$, $b' = \varphi(b)$ and let $\psi \in \mathrm{Spec}(L)$ be such that $\psi(a \vee b) = 1$ and $\psi(a \wedge b) = 0$. Since $\mathrm{Spec}(\varphi)$ is surjective there exists $\psi' \in \mathrm{Spec}(L')$ such that $\psi = \psi'\varphi$ hence $\psi'(a' \vee b') = 1$ is $\psi'(a' \wedge b') = 0$, hence $a' \vee b' \not\leq a' \wedge b'$ and $a' \neq b'$.
Suppose that φ is injective. We identify L to a sublattice of L'. If $\psi \in \mathrm{Spec}(L)$, take $I = \psi^{-1}(0)$ and $F = \psi^{-1}(1)$. By the compactness theorem (see appendix), there exists $\psi' \in \mathrm{Spec}(L')$ such that $\psi'(I) = 0$ and $\psi'(F) = 1$, which means $\psi = \psi' \circ \varphi$. □

Of course, these three last results are hard to interpret in a computational way. An intuitive interpretation is that we can proceed "as if" any distributive lattice is a lattice of subsets of a set. The goal of Hilbert's program is to give a precise meaning to this sentence, and explain what is meant by "as if" there.

2 Krull dimension of distributive lattices

2.1 Definition of $\mathrm{Kr}_\ell(L)$

To develop a suitable constructive theory of the Krull dimension of a distributive lattice we have to find a constructive counterpart of the notion of increasing chains of prime ideals.

Definition 2.1 *To any distributive lattice L and $\ell \in \mathbb{N}$ we associate a distributive lattice $\mathrm{Kr}_\ell(L)$ which is the lattice defined by the generators $\varphi_i(x)$ for $i \leq \ell$ and $x \in L$ (thus we have $\ell+1$ disjoint copies of L and we let ϕ_i be the bijection between L and the ith copy) and relations*

- $\vdash \varphi_i(1)$
- $\varphi_i(0) \vdash$
- $\varphi_i(a), \varphi_i(b) \vdash \varphi_i(a \wedge b)$
- $\varphi_i(a \vee b) \vdash \varphi_i(a), \varphi_i(b)$
- $\varphi_i(a) \vdash \varphi_i(b)$ *whenever* $a \leq b$ *in* L
- $\varphi_{i+1}(a) \vdash \varphi_i(a)$ *for* $i < \ell$

Let S be the disjoint union $\bigcup \varphi_i(L)$ and $\vdash_S$ the entailment relation generated by these relations.

From this definition, we get directly the following theorem.

Theorem 2.2 *The maps φ_i are morphisms from the lattice L to the lattice $\mathrm{Kr}_\ell(L)$. Furthermore the lattice $\mathrm{Kr}_\ell(L)$ with the maps φ_i is then a solution of the following universal problem: to find a distributive lattice K and $\ell+1$ homomorphisms $\varphi_0 \geq \varphi_1 \geq \cdots \geq \varphi_\ell$ from L to K such that, for any lattice L' and any morphism $\psi_0 \geq \psi_1 \geq \cdots \geq \psi_\ell \in \mathrm{Hom}(L, L')$ we have one and only one morphism $\eta : K \to L'$ such that $\eta\varphi_0 = \psi_0$, $\eta\varphi_1 = \psi_1$, ..., $\eta\varphi_\ell = \psi_\ell$.*

The next theorem is the main result of this paper, and uses crucially the notion of entailment relation.

Theorem 2.3 *If U_i and J_i $(i = 0, \ldots, \ell)$ are finite subsets of L we have in* $\mathrm{Kr}_\ell(L)$

$$\varphi_0(U_0) \wedge \ldots \wedge \varphi_\ell(U_\ell) \leq \varphi_0(J_0) \vee \ldots \vee \varphi_\ell(J_\ell)$$

if, and only if,

$$\varphi_0(U_0), \ldots, \varphi_\ell(U_\ell) \vdash_S \varphi_0(J_0), \ldots, \varphi_\ell(J_\ell)$$

if, and only if, there exist $x_1, \ldots, x_\ell \in L$ such that (where $\vdash$ is the entailment relation of L):

$$\begin{array}{rcl} x_1,\ U_0 & \vdash & J_0 \\ x_2,\ U_1 & \vdash & J_1,\ x_1 \\ \vdots & \vdots & \vdots \\ x_\ell,\ U_{\ell-1} & \vdash & J_{\ell-1},\ x_{\ell-1} \\ U_\ell & \vdash & J_\ell,\ x_\ell \end{array}$$

Proof.
The equivalence between the first and the second statement follows from theorem 1.7.

We show next that the relation on $\mathrm{P_f}(S)$ described in the statement of the theorem is indeed an entailment relation. The only point that needs explanation is the cut rule. To simplify notations, we take $\ell = 3$. We have then 3 possible cases, and we analyse only one case, where $X, \varphi_1(z) \vdash_S Y$ and $X \vdash_S Y, \varphi_1(z)$, the other cases being similar. By hypothesis we have $x_1, x_2, x_3, y_1, y_2, y_3$ such that

$$\begin{array}{rcl} x_1,\ U_0 & \vdash & J_0 \\ x_2,\ U_1,\ z & \vdash & J_1,\ x_1 \\ x_3,\ U_2 & \vdash & J_2,\ x_2 \\ U_3 & \vdash & J_3,\ x_3 \end{array} \qquad \begin{array}{rcl} y_1,\ U_0 & \vdash & J_0 \\ y_2,\ U_1 & \vdash & J_1, y_1,\ z \\ y_3, U_2 & \vdash & J_2, y_2 \\ U_3 & \vdash & J_3,\ y_3 \end{array}$$

The two entailment relations on the second line give

$$x_2,\ y_2,\ U_1,\ z \ \vdash\ J_1,\ x_1,\ y_1 \qquad x_2,\ y_2,\ U_1 \ \vdash\ J_1,\ x_1,\ y_1,\ z$$

hence by cut

$$x_2,\ y_2,\ U_1 \ \vdash\ J_1,\ x_1,\ y_1$$

i.e.,

$$x_2 \wedge y_2,\ U_1 \ \vdash\ J_1,\ x_1 \vee y_1$$

Finally, using distributivity

$$\begin{array}{rcl} (x_1 \vee y_1),\ U_0 & \vdash & J_0 \\ (x_2 \wedge y_2),\ U_1 & \vdash & J_1,\ (x_1 \vee y_1) \\ (x_3 \wedge y_3),\ U_2 & \vdash & J_2,\ (x_2 \wedge y_2) \\ U_3 & \vdash & J_3,\ (x_3 \wedge y_3) \end{array}$$

and hence $\varphi_0(U_0), \ldots, \varphi_3(U_3) \vdash_S \varphi_0(J_0), \ldots, \varphi_3(J_3)$.
Finally it is left to notice that the entailment relation we have defined is clearly the least possible relation ensuring the φ_i to form a non-increasing chain of morphisms. □

Notice that the morphisms φ_i are injective: it is easily seen that for $a, b \in L$ the relation $\varphi_i(a) \vdash_S \varphi_i(b)$ implies $a \vdash b$, and hence that $\varphi_i(a) = \varphi_i(b)$ implies $a = b$.

2.2 Partially specified chains of prime ideals

Definition 2.4 *In a distributive lattice L, a* partial specification for a chain of prime ideals *(that we shall call* idealistic chain*) is defined as follows. An idealistic chain of length ℓ is a list of $\ell+1$ idealistic primes of L: $\mathcal{C} = ((J_0, U_0), \ldots, (J_\ell, U_\ell))$. An idealistic chain of length 0 is nothing but an* idealistic prime.

We think of an idealistic chain of length ℓ as a partial specification of an increasing chains of prime ideals $P_0, \ldots, P_\ell$ such that $J_i \subseteq P_i$, $U_i \cap P_i = \emptyset$, $(i = 0, \ldots, \ell)$.

Definition 2.5 *We say that an idealist chain $((J_0, U_0), \ldots, (J_\ell, U_\ell))$* collapses *if, and only if, we have in $\mathrm{Kr}_\ell(L)$*

$$\varphi_0(U_0), \ldots, \varphi_\ell(U_\ell) \vdash_S \varphi_0(J_0), \ldots, \varphi_\ell(J_\ell)$$

Thus an idealistic chain $((J_0, U_0), \ldots, (J_\ell, U_\ell))$ collapses in L if, and only if, the idealistic prime $\mathcal{P} = (\varphi_0(J_0), \ldots, \varphi_\ell(J_\ell); \varphi_0(U_0), \ldots, \varphi_\ell(U_\ell))$ collapses in $\mathrm{Kr}_\ell(L)$. From the completeness theorem we deduce the following result which justifies this idea of partial specification.

Theorem 2.6 (formal Nullstellensatz for chains of prime ideals) *The completeness theorem implies the following result. Let L be a distributive lattice and $((J_0, U_0), \ldots, (J_\ell, U_\ell))$ be an idealistic chain in L. The following properties are equivalent:*

(a) *There exist $\ell+1$ prime ideals $P_0 \subseteq \cdots \subseteq P_\ell$ such that $J_i \subseteq P_i$, $U_i \cap P_i = \emptyset$, $(i = 0, \ldots, \ell)$.*

(b) *The idealistic chain does not collapse.*

Proof.
If (b) holds then the idealistic prime $\mathcal{P} = (\varphi_0(J_0), \ldots, \varphi_\ell(J_\ell); \varphi_0(U_0), \ldots, \varphi_\ell(U_\ell))$ does not collapse in $\mathrm{Kr}_\ell(L)$. It follows then from proposition 1.9 that there exists $\sigma \in \mathrm{Spec}(\mathrm{Kr}_\ell(L))$ such that σ is 0 on $\varphi_0(J_0), \ldots, \varphi_\ell(J_\ell)$ and 1 on $\varphi_0(U_0), \ldots, \varphi_\ell(U_\ell))$. We can then take $P_i = (\sigma \circ \varphi_i)^{-1}(0)$. That ($a$) implies ($b$) is direct. □

2.3 Krull dimension of a distributive lattice

Definition 2.7

1) *An* elementary idealistic chain *in a distributive lattice L is an idealistic chain of the form*

$$((0, x_1), (x_1, x_2), \ldots, (x_\ell, 1))$$

(with x_i in L).

2) *A distributive lattice L is* of dimension $\leq \ell - 1$ *iff it satisfies one of the equivalent conditions*

- *Any elementary idealistic chain of length ℓ collapses.*
- *For any sequence $x_1, \ldots, x_\ell \in L$ we have*

$$\varphi_0(x_1), \ldots, \varphi_{\ell-1}(x_\ell) \vdash \varphi_1(x_1), \ldots, \varphi_\ell(x_\ell)$$

in $\mathrm{Kr}_\ell(L)$,

The following result shows that this definition coincides with the classical definition of Krull dimension for lattices.

Theorem 2.8 *The completeness theorem implies that the Krull dimension of a lattice L is $\leq \ell - 1$ if, and only if, there is no strictly increasing chains of prime ideals of length ℓ.*

Using theorem 2.3, we get the following characterisation.

Theorem 2.9 *A distributive lattice L is of Krull dimension $\leq \ell - 1$ if, and only if, for all $x_1, \ldots, x_\ell \in L$ there exist $a_1, \ldots, a_\ell \in L$ such that*

$$a_1 \wedge x_1 = 0, \quad a_2 \wedge x_2 \leq a_1 \vee x_1, \quad , \ldots, a_\ell \wedge x_\ell \leq a_{\ell-1} \vee x_{\ell-1}, \quad 1 = a_\ell \vee x_\ell$$

In this way we have given a concrete form of the statement that the distributive lattice L has a dimension $\leq \ell - 1$ in the form of an existence of a sequence of inequalities.

In particular the distributive lattice L is of dimension ≤ -1 if, and only if, $1 = 0$ in L, and it is of dimension ≤ 0 if, and only if, L is a Boolean algebra (any element has a complement).

We have furthermore.

Lemma 2.10 *A distributive lattice L generated by a set G is of dimension $\leq \ell - 1$ if, and only if, for any sequence $x_1, \ldots, x_\ell \in G$*

$$\varphi_0(x_1), \ldots, \varphi_{\ell-1}(x_\ell) \vdash \varphi_1(x_1), \ldots, \varphi_\ell(x_\ell)$$

in $\mathrm{Kr}_\ell(L)$.

Indeed using distributivity, one can deduce

$$a \vee a', A \vdash b \vee b', B \quad a \wedge a' \vdash b \wedge b', B$$

from $a, A \vdash b, B$ and $a', A \vdash b', B$. Furthermore any element of L is an inf of sups of elements of G.

2.4 Implicative lattice

A lattice L is said to be an *implicative lattice* [5] or *Heyting algebra* [8] if, and only if, there is a binary operation $\to$ such that

$$a \wedge b \leq c \Longleftrightarrow a \leq b \to c$$

Theorem 2.11 *If L is an implcative lattice, we have in* $\mathrm{Kr}_\ell(L)$

$$\varphi_0(U_0), \ldots, \varphi_\ell(U_\ell) \vdash_S \varphi_0(J_0), \ldots, \varphi_\ell(J_\ell)$$

if, and only if,

$$1 = u_\ell \to (j_\ell \vee (u_{\ell-1} \to (j_{\ell-1} \vee \ldots (u_0 \to j_0))))$$

where $u_j = \wedge U_j$ and $j_k = \vee J_k$.

In the case where L is an implicative lattice, we can write explicitely that L is of dimension $\leq \ell - 1$ as an identity. For instance that L is of dimension ≤ 0 is equivalent to the identity

$$1 = x \vee \neg x$$

where $\neg x = x \to 0$ and that L is of dimension ≤ 1 is equivalent to the identity

$$1 = x_2 \vee (x_2 \to (x_1 \vee \neg x_1))$$

and so on.

Corollary 2.12 *An implicative lattice L is of dimension $\leq \ell - 1$ if, and only if, for any sequence $x_1, \ldots, x_\ell$*

$$1 = x_\ell \vee (x_\ell \to \ldots (x_2 \vee (x_2 \to (x_1 \vee \neg x_1))) \ldots)$$

2.5 Decidability

To any distributive lattice L we have associated a family of distributive lattices $\mathrm{Kr}_\ell(L)$ with a complete description of their ordering. A lattice is *discrete* if, and only if, its ordering is decidable, which means intuitively that there is an algorithm to decide the ordering (or, equivalently, the equality) in this lattice. It should be intuitively clear that we could find a discrete lattice L such that $\mathrm{Kr}_1(L)$ is not discrete since, by 2.3, the ordering on $\mathrm{Kr}_1(L)$ involves an existential quantification on the set L, that may be infinite (this point is discussed in [1], with another argument). However we can use the characterisation of theorem 2.3 to give a general sufficient condition ensuring that all $\mathrm{Kr}_\ell(L)$ are discrete.

Theorem 2.13 *Suppose that the lattice L is a discrete implicative lattice then each $\mathrm{Kr}_\ell(L)$ is discrete.*

Proof.
This is direct from theorem 2.11. □

2.6 Dimension of Spectral Spaces

This subsection is written from a classical point of view. Following [7], a topological space X is called a spectral space if it satisfies the following conditions: (a) X is a compact T_0-space; (b) X has a compact open basis which is closed under finite intersections; (c) each irreducible closed subspace of X has a generic point. $\mathrm{Spec}(R)$, with the Zariski topology, is spectral for any commutative ring R with identity. Similary, if we take for basic open the sets $U_a = \{\phi \in \mathrm{Spec}(L) \mid \phi(a) = 1\}$ then $\mathrm{Spec}(L)$ is spectral for any distributive lattice. The compact open subsets of a spectral space form a distributive lattice, and it is well-known [21, 8] that, if L is an arbitrary distributive lattice, then L is isomorphic to the lattice of compact open subsets of the space $\mathrm{Spec}(L)$.

If U, V are open subsets of a topological space X we define $U \to V$ to be the largest open W such that $W \cap U \subseteq V$ and $\neg\, U = U \to \emptyset$. In a classical setting a spectral space X is said to be of dimension $\leq \ell - 1$ if, and only if, there is no strictly increasing chains of length ℓ of irreducible closed subsets of X. We can reformulate theorem 2.9 as follows.

Theorem 2.14 *A spectral space X is of dimension $\leq \ell - 1$ if, and only if, for any compact open subsets $x_1, \ldots, x_\ell$ of X*

$$X = x_\ell \vee (x_\ell \to \ldots (x_2 \vee (x_2 \to (x_1 \vee \neg x_1))) \ldots)$$

2.7 Connections with Joyal's definition

Let L be a distributive lattice, Joyal [6] gives the following definition of $\dim(L) \leq \ell$. Let $\varphi_i^\ell : L \to \mathrm{Kr}_\ell(L)$ be the $\ell + 1$ universal morphisms. By universality of $\mathrm{Kr}_{\ell+1}(L)$, we have $\ell + 1$ morphisms $\sigma_i : \mathrm{Kr}_{\ell+1}(L) \to \mathrm{Kr}_\ell(L)$ such that $\sigma_i \circ \varphi_j^{\ell+1} = \varphi_j^\ell$ if $j \leq i$ and $\sigma_i \circ \varphi_j^{\ell+1} = \varphi_{j-1}^\ell$ if $j > i$. Joyal defines then $\dim(L) \leq \ell$ to mean that $(\sigma_0, \ldots, \sigma_\ell) : \mathrm{Kr}_{\ell+1}(L) \to \mathrm{Kr}_\ell(L)^{\ell+1}$ is injective. This definition can be motivated by proposition 1.11: the elements in the image of $Sp(\sigma_i)$ are the chains of prime ideals $(\alpha_0, \ldots, \alpha_\ell)$ with $\alpha_i = \alpha_{i+1}$, and $Sp(\sigma_0, \ldots, \sigma_\ell)$ is surjective if, and only if, for any chain $(\alpha_0, \ldots, \alpha_\ell)$ there exists $i < \ell$ such that $\alpha_i = \alpha_{i+1}$. This means exactly that there is no nontrivial chain of prime ideals of length $\ell + 1$. Using the completeness theorem, one can then see the equivalence with definition 2.7. One could check directly this equivalence using a constructive metalanguage, but for lack of space, we shall not present here this argument. Similarly, it would be possible to establish the equivalence of our definition with the one of Español [6] (here also, this connection is clear via the completeness theorem).

3 Zariski and Krull lattice

3.1 Zariski lattice

Let R be a commutative ring. We write $\langle J\rangle$ or explicitly $\langle J\rangle_R$ for the ideal of R generated by the subset $J \subseteq R$. We write $\mathcal{M}(U)$ for the monoid ([3]) generated by the subset $U \subseteq R$. Given a commutative ring R the *Zariski lattice* $\mathrm{Zar}(R)$ has for elements the radicals of finitely generated ideals (the order relation being inclusion). It is well defined as a lattice. Indeed $\sqrt{I_1} = \sqrt{J_1}$ and $\sqrt{I_2} = \sqrt{J_2}$ imply $\sqrt{I_1 I_2} = \sqrt{J_1 J_2}$ (which defines $\sqrt{I_1} \wedge \sqrt{I_2}$) and $\sqrt{I_1 + I_2} = \sqrt{J_1 + J_2}$ (which defines $\sqrt{I_1} \vee \sqrt{I_2}$). The Zariski lattice of R is always distributive, but may not be discrete, even if R is discrete. Nevertheless an inclusion $\sqrt{I_1} \subseteq \sqrt{I_2}$ can always be certified in a finite way if the ring R is discrete. This lattice contains all the informations necessary for a constructive development of the abstract theory of the Zariski spectrum.
We shall write $\widetilde{a}$ for $\sqrt{\langle a\rangle}$. Given a subset S of A we write $\widetilde{S}$ for the subset of $\mathrm{Zar}(R)$ the elements of which are $\widetilde{s}$ for $s \in S$. We have $\widetilde{a_1} \vee \cdots \vee \widetilde{a_m} = \sqrt{\langle a_1, \ldots, a_m\rangle}$ and $\widetilde{a_1} \wedge \cdots \wedge \widetilde{a_m} = \widetilde{a_1 \cdots a_m}$
Let U and J be two finite subsets of R, we have

$$U \vdash_{\mathrm{Zar}(R)} J \quad \Longleftrightarrow \quad \prod_{u \in U} u \in \sqrt{\langle J\rangle} \quad \Longleftrightarrow \quad \mathcal{M}(U) \cap \langle J\rangle \neq \emptyset$$

This describes completely the lattice $\mathrm{Zar}(R)$. More precisely we have:

Proposition 3.1 *The lattice* $\mathrm{Zar}(R)$ *of a commutative ring* R *is (up to isomorphism) the lattice generated by* $(R, \vdash)$ *where* $\vdash$ *is the least entailment relation over* R *such that*

$$\begin{array}{lllllllll} 0 & \vdash & & x,\ y & \vdash & xy & & & \\ & \vdash & 1 & xy & \vdash & x & & x+y & \vdash\ x,\ y \end{array}$$

Proof.
It is clear that the relation $U \vdash J$ defined by "$\mathcal{M}(U)$ meets $\langle J\rangle$" satisfies these axioms. It is also clear that the entailment relation generated by these axioms contains this relation. Let us show that this relation is an entailment relation. Only the cut rule is not obvious. Assume that $\mathcal{M}(U, a)$ meets $\langle J\rangle$ and that $\mathcal{M}(U)$ meets $\langle J, a\rangle$. There exist then $m_1, m_2 \in \mathcal{M}(U)$ and $k \in \mathbb{N}, x \in R$ such that $a^k m_1 \in \langle J\rangle$, $m_2 + ax \in \langle J\rangle$. Eliminating a this implies that $\mathcal{M}(U)$ intersects $\langle J\rangle$. □

We have $\widetilde{a} = \widetilde{b}$ if, and only if, a divides a power of b and b divides a power of a.

Proposition 3.2 *In a commutative ring* R *to give an ideal of the lattice* $\mathrm{Zar}(R)$ *is the same as to give a radical ideal of* R*. If* I *is a radical ideal of* R *one associates the ideal*

$$\mathcal{I} = \{J \in \mathrm{Zar}(R) \mid J \subseteq I\}$$

of $\mathrm{Zar}(R)$*. Conversely if* $\mathcal{I}$ *is an ideal of* $\mathrm{Zar}(R)$ *one can associate the ideal*

$$I = \bigcup_{J \in \mathcal{I}} J = \{x \in A \mid \widetilde{x} \in \mathcal{I}\},$$

which is a radical ideal of R*. In this bijection the prime ideals of the ring correspond to the prime ideals of the Zariski lattice.*

[3] A monoid will always be multiplicative.

Proof.
We only prove the last assertion. If I is a prime ideal of R, if $J, J' \in \mathrm{Zar}(R)$ and $J \wedge J' \in \mathcal{I}$, let $a_1, \ldots, a_n \in R$ be some "generators" of J (*i.e.*, $J = \sqrt{\langle a_1, \ldots, a_n \rangle}$) and let $b_1, \ldots, b_m \in A$ be some generators of J'. We have $a_i b_j \in I$ and hence $a_i \in I$ or $b_j \in I$ for all i, j. It follows from this (constructively) that we have $a_i \in I$ for all i or $b_j \in I$ for all j. Hence $J \in \mathcal{I}$ or $J' \in \mathcal{I}$ and $\mathcal{I}$ is a prime ideal of $\mathrm{Zar}(R)$.
Conversely if $\mathcal{I}$ is a prime ideal of $\mathrm{Zar}(R)$ and if we have $\widetilde{xy} \in \mathcal{I}$ then $\widetilde{x} \wedge \widetilde{y} \in \mathcal{I}$ and hence $\widetilde{x} \in \mathcal{I}$ or $\widetilde{y} \in \mathcal{I}$. This shows that $\{x \in A \mid \widetilde{x} \in \mathcal{I}\}$ is a prime ideal of R. □

3.2 Krull lattices of a commutative ring

Definition 3.3 *We define* $\mathrm{Kru}_\ell(R) := \mathrm{Kr}_\ell(\mathrm{Zar}(R))$. *This is called the* Krull lattice of order ℓ *of the ring R. We say also that R is of Krull dimension $\leq \ell$ iff the distributive lattice* $\mathrm{Zar}(R)$ *is of dimension $\leq \ell$.*

Theorem 3.4 *The ring R is of dimension $\leq \ell - 1$ if, and only if, for any $x_1, \ldots, x_n \in R$ we have in* $\mathrm{Kru}_\ell(R)$

$$\varphi_0(\widetilde{x_1}), \ldots, \varphi_{\ell-1}(\widetilde{x_\ell}) \vdash \varphi_1(\widetilde{x_1}), \ldots, \varphi_\ell(\widetilde{x_\ell})$$

Proof.
This is a direct consequence of lemma 2.10 and the fact that the elements $\widetilde{x}$ generates $\mathrm{Zar}(R)$. □

Theorem 3.5 *Let $\mathcal{C} = ((J_0, U_0), \ldots, (J_\ell, U_\ell))$ be a list of $\ell + 1$ pairs of finite subsets of R, the following properties are equivalent:*

1. *there exist $j_i \in \langle J_i \rangle$, $u_i \in \mathcal{M}(U_i)$, $(i = 0, \ldots, \ell)$, such that*

$$u_0 \cdot (u_1 \cdot (\cdots (u_\ell + j_\ell) + \cdots) + j_1) + j_0 = 0$$

2. *there exist $L_1, \ldots, L_\ell \in \mathrm{Zar}(R)$ such that in* $\mathrm{Zar}(R)$*:*

$$\begin{array}{rcl} L_1,\ \widetilde{U_0} & \vdash & \widetilde{J_0} \\ L_2,\ \widetilde{U_1} & \vdash & \widetilde{J_1},\ L_1 \\ \vdots & \vdots & \vdots \\ L_\ell,\ \widetilde{U_{\ell-1}} & \vdash & \widetilde{J_{\ell-1}},\ L_{\ell-1} \\ \widetilde{U_\ell} & \vdash & \widetilde{J_\ell},\ L_\ell \end{array}$$

3. *there exist $x_1, \ldots, x_\ell \in R$ such that (for the entailment relation described in proposition 3.1):*

$$\begin{array}{rcl} x_1,\ U_0 & \vdash & J_0 \\ x_2,\ U_1 & \vdash & J_1,\ x_1 \\ \vdots & \vdots & \vdots \\ x_\ell,\ U_{\ell-1} & \vdash & J_{\ell-1},\ x_{\ell-1} \\ U_\ell & \vdash & J_\ell,\ x_\ell \end{array}$$

Proof.
It is clear that 1 entails 3: simply take

$$x_\ell = u_\ell + j_\ell,\ x_{\ell-1} = x_\ell u_{\ell-1} + j_{\ell-1}, \ldots,\ x_0 = x_1 u_0 + j_0$$

and that 3 entails 2.

Let us prove that 2 implies 3. We assume:

$$\begin{array}{rcl} L_1,\ \widetilde{U_0} & \vdash & I_0 \\ L_2,\ \widetilde{U_1} & \vdash & I_1,\ L_1 \\ \widetilde{U_2} & \vdash & I_2,\ L_2 \end{array}$$

The last line means that $\mathcal{M}(U_2)$ intersects $I_2 + L_2$ and hence $I_2 + \langle x_2 \rangle$ for some element x_2 of L_2. Hence we have $\widetilde{U}_2 \vdash I_2,\ \widetilde{x}_2$. Since $\widetilde{x}_2 \leq L_2$ in $\mathrm{Zar}(R)$ we have $\widetilde{x}_2,\ \widetilde{U}_1 \vdash I_1,\ L_1$. We have then replaced L_2 by $\widetilde{x}_2$. Reasoning as previously one sees that one can replace as well L_1 by a suitable $\widetilde{x}_1$. One gets then 3.

Finally, let us show that 3 entails 1: if we have for instance

$$\begin{array}{rcl} x_1,\ U_0 & \vdash & I_0 \\ x_2,\ U_1 & \vdash & I_1,\ x_1 \\ U_2 & \vdash & I_2,\ x_2 \end{array}$$

by the last line we know that we can find y_2 both in the monoid $M_2 = \mathcal{M}(U_2) + \langle I_2 \rangle$ and in $\langle x_2 \rangle$. Since $y_2 \vdash x_1$

$$y_2,\ U_1 \vdash I_1,\ x_1$$

and since $y_2 \in M_2$ we can find y_1 both in the monoid $M_1 = M_2\mathcal{M}(U_1) + \langle I_1 \rangle$ and in $\langle x_1 \rangle$. We have $y_1 \vdash x_1$ and hence

$$y_1, U_0 \vdash I_0$$

and since $y_1 \in M_1$ this implies $0 \in M_1\mathcal{M}(U_0) + \langle I_0 \rangle$ as desired. □

Corollary 3.6 *A ring R is of Krull dimension $\leq \ell - 1$ iff for any sequence $x_1, \ldots, x_\ell$ there exist $a_1, \ldots, a_\ell \in R$ and $m_1, \ldots, m_\ell \in \mathbb{N}$ such that*

$$x_1^{m_1}(\cdots(x_\ell^{m_\ell}(1 + a_\ell x_\ell) + \cdots) + a_1 x_1) = 0$$

Proof.
By Theorem 3.4, we have in $\mathrm{Kru}_\ell(R)$

$$\varphi_0(\widetilde{x}_1), \ldots, \varphi_{\ell-1}(\widetilde{x}_\ell) \vdash \varphi_1(\widetilde{x}_1), \ldots, \varphi_\ell(\widetilde{x}_\ell)$$

we can then apply theorem 3.5 to the elementary idealistic chain

$$((0, \widetilde{x}_1), (\widetilde{x}_1, \widetilde{x}_2), \ldots, (\widetilde{x}_\ell, 1))$$

and we get in this way $j_i \in \langle x_i \rangle$, $j_0 = 0$ and $u_i \in \mathcal{M}(x_i), u_0 = 1$ such that

$$u_0 \cdot (u_1 \cdot (\cdots(u_\ell + j_\ell) + \cdots) + j_1) + j_0 = 0$$

as desired. □

This concrete characterisation of the Krull dimension of a ring can be found in [14], where it is derived using dynamical methods [2].

Lemma 3.7 *If R is coherent and noetherian then $\mathrm{Zar}(R)$ is an implicative lattice.*

Proof.
Let $L \in \mathrm{Zar}(R)$, radical of an ideal generated by elements $y_1, \ldots, y_n$ and $x \in R$, we show how to define an element $\widetilde{x} \to L \in \mathrm{Zar}(R)$ such that, for any $M \in \mathrm{Zar}(R)$

$$M \wedge \widetilde{x} \leq L \quad \Longleftrightarrow \quad M \leq \widetilde{x} \to L$$

For this, we consider the sequence of ideals

$$I_k = \{z \in R \mid zx^k \in \langle y_1, \ldots, y_n \rangle\}$$

Since R is coherent, each I_k is finitely generated. Since furthermore R is noetherian and $I_k \subseteq I_{k+1}$ the sequence I_k is stationary and $\bigcup_k I_k$ is finitely generated. We take for $\widetilde{x} \to L$ the radical of this ideal.

If $M \in \mathrm{Zar}(R)$ then M is the radical of an ideal generated by finitely many elements $x_1, \ldots, x_m$ and we can take $M \to L = (\widetilde{x_1} \to L) \wedge \ldots \wedge (\widetilde{x_m} \to L)$. □

Corollary 3.8 *If R is coherent, noetherian and strongly discrete then each lattice $\mathrm{Kr}_n(R)$ is discrete.*

Proof.
Using theorem 2.13 and lemma 3.7 we are left to show that $\mathrm{Zar}(R)$ is discrete. We have $M \leq L$ if, and only if, $1 = M \to L$. But to test if an element of $\mathrm{Zar}(R)$ is equal to the ideal $\langle 1 \rangle$ is decidable since R is strongly discrete. □

The hypotheses of this corollary are satisfied if R is a polynomial ring $K[X_1, \ldots, X_n]$ over a discrete field K [19].

3.3 Krull dimension of a polynomial ring over a discrete field

Let R be a commutative ring, let us say that a sequence $x_1, \ldots, x_\ell$ is *singular* if, and only if, there exists $a_1, \ldots, a_\ell \in R$ and $m_1, \ldots, m_\ell \in \mathbb{N}$ such that

$$x_1^{m_1}(\cdots(x_\ell^{m_\ell}(1 + a_\ell x_\ell) + \cdots) + a_1 x_1) = 0$$

A sequence is *pseudo regular* if, and only if, it is not singular. Corollary 3.6 can be reformulated as: a ring R is of Krull dimension $\leq \ell - 1$ if, and only if, any sequence in R of length ℓ is singular.

Proposition 3.9 *Let K be a discrete field, R a commutative K-algebra, and $x_1, \ldots, x_\ell$ in R algebraically dependent over K. The sequence $x_1, \ldots, x_\ell$ is singular.*

Proof.
Let $Q(x_1, \ldots, x_\ell) = 0$ be a algebraic dependence relation over K. Let us order the nonzero monomials of Q along the lexicographic ordering. We can suppose that the coefficient of the first monomial is 1. Let $x_1^{m_1} x_2^{m_2} \cdots x_\ell^{m_\ell}$ be this momial, it is clear that Q can be written on the form

$$Q = x_1^{m_1} \cdots x_\ell^{m_\ell} + x_1^{m_1} \cdots x_\ell^{1+m_\ell} R_\ell + x_1^{m_1} \cdots x_{\ell-1}^{1+m_{\ell-1}} R_{\ell-1} + \cdots + x_1^{m_1} x_2^{1+m_2} R_2 + x_1^{1+m_1} R_1$$

and this is the desired collapsus. □

Let us say that a ring is of dimension ℓ if it is of dimension $\leq \ell$ but not of dimension $\leq \ell - 1$. It follows that we have:

Theorem 3.10 *Let K be a discrete field. The Krull dimension of the ring $K[X_1, \ldots, X_\ell]$ is equal to ℓ.*

Proof.
Given proposition 3.9 it is enough to check that the sequence $(X_1, \ldots, X_\ell)$ is pseudo regular, which is direct. $\square$

Notice that we got this basic result quite directly from the characterisation of corollary 3.6, and that our argument is of course also valid classically (with the usual definition of Krull dimension). This contradicts the current opinion that constructive arguments are necessarily more involved than classical proofs.

References

[1] Boileau, A., Joyal, A. *La logique des topos* J. Symbolic Logic **46** (1981), no. 1, 6–16

[2] Coste M., Lombardi H., Roy M.-F. *Dynamical method in algebra: Effective Nullstellensätze* Annals of Pure and Applied Logic **111**, (2001) 203–256

[3] Cederquist, Coquand T. *Entailment relations and Distributive Lattices* Logic Colloquium '98 (Prague), 127–139, Lect. Notes Log., 13. Assoc. Symbol. Logic, Urbana, (2000).

[4] Coquand T., Persson H. *Valuations and Dedekind's Prague Theorem.* J. Pure Appl. Algebra **155** (2001), no. 2-3, 121–129.

[5] Curry, H. B. *Foundations of mathematical logic* McGraw-Hill Book Co., Inc., New York-San Francisco, Calif.-Toronto-London 1963

[6] Español L. *Constructive Krull dimension of lattices.* Rev. Acad. Cienc. Zaragoza (2) **37** (1982), 5–9.

[7] Hochster M. *Prime ideal structure in commutative rings.* Trans. Amer. Math. Soc. **142** 1969 43–60.

[8] Johnstone P. *Stone Spaces.* Cambridge Studies in Advanced Mathematics, 3. Cambridge University Press, Cambridge, 1986.

[9] Joyal A. *Le théorème de Chevalley-Tarski.* Cahiers de Topologie et Géometrie Differentielle, 1975.

[10] Kuhlmann F.-V., Lombardi H. *Construction du hensélisé d'un corps valué.* Journal of Algebra **228**, (2000), 624–632.

[11] Lombardi H. *Un nouveau positivstellensatz effectif pour les corps valués.* Séminaire "Structures Ordonnées" (Paris 6-7) (18 pages, published in 96. Editeurs: F. Delon, A. Dickmann, D. Gondard)

[12] Lombardi H. *Le contenu constructif d'un principe local-global avec une application à la structure d'un module projectif de type fini* . Publications Mathématiques de Besançon. Théorie des nombres. (1997). Fascicule 94–95 & 95–96.

[13] Lombardi H. *Relecture constructive de la théorie d'Artin-Schreier.* Annals of Pure and Applied Logic, **91**, (1998), 59–92.

[14] Lombardi H. *Dimension de Krull, Nullstellensätze et Évaluation dynamique.* Math. Zeitschrift, **242**, (2002), 23–46.

[15] Lombardi H. *Platitude, localisation et anneaux de Prüfer: une approche constructive.* Preprint (1999).

[16] Lombardi H. *Hidden constructions in abstract algebra. I. Integral dependance.* J. Pure Appl. Algebra **167** (2002), 259–267.

[17] Lombardi H., Quitté C. *Constructions cachées en algèbre abstraite (2) Le principe local-global.* Preprint 1999.

[18] MacNeille H. M. *Partially ordered sets.* Trans. Amer. Math. Soc. **42** (1937), no. 3, 416–460.

[19] Mines R., Richman F., Ruitenburg W. *A Course in Constructive Algebra.* Universitext. Springer-Verlag, 1988.

[20] Rota G.C. *Indiscrete Thoughts* Birkhauser, 1995.

[21] Stone, M.H. *Topological representations of distributive lattices and Brouwerian logics.* Cas. Mat. Fys. **67**, 1-25 (1937).

Annex: Completeness, compactness theorem, LLPO and geometric theories

A.4 Theories and models

We fix a set V of *atomic propositions* or *propositional letters*. A proposition $\phi, \psi, \ldots$ is a syntactical object built from the atoms $p, q, r \in V$ with the usual logical connectives

$$0, \;\; 1, \;\; \phi \wedge \psi, \;\; \phi \vee \psi, \;\; \phi \to \psi, \;\; \neg\phi$$

We let P_V be the set of all propositions. Let F_2 be the Boolean algebra with two elements. A *valuation* is a function $v \in F_2^V$ that assigns a truth value to any of the atomic propositions. Such a valuation can be extended to a map $P_V \to \{0,1\}$, $\phi \longmapsto v(\phi)$ in the expected way. A *theory* T is a subset of P_V. A *model* of T is a valuation v such that $v(\phi) = 1$ for all $\phi \in T$.

More generally given a Boolean algebra B we can define B-valuation to be a function $v \in B^V$. This can be extended as well to a map $P_V \to B$, $\phi \longmapsto v(\phi)$. A B-*model* of T is a valuation v such that $v(\phi) = 1$ for all $\phi \in T$. The usual notion of model is a direct special case, taking for B the Boolean algebra F_2. For any theory there exists always a free Boolean algebra over which T is a model, the *Lindenbaum* algebra of T, which can be also be defined as the Boolean algebra generated by T, thinking of the elements of V as generators and the elements of T as relations. The theory T is *formally consistent* if, and only if, its Lindenbaum algebra is not trivial.

A.5 Completeness theorem

Theorem A.11 *(Completeness theorem) Let T be a theory. If T is formally consistent then T has a model.*

This theorem is the completeness theorem for propositional logic. Such a theorem is strongly related to Hilbert's program, which can be seen as an attempt to replace the question of existence of model of a theory by the formal fact that this theory is not contradictory.

Let B the Lindenbaum algebra of T. To prove completeness, it is enough to find a morphism $B \to F_2$ assuming that B is not trivial, wich is the same as finding a prime ideal (which is then automatically maximal) in B. Thus the completeness theorem is a consequence of the existence of prime ideal in nontrivial Boolean algebra. Notice that this existence is clear in the case where B is finite, hence that the completeness theorem is direct for finite theories.

A.6 Compactness theorem

The completeness theorem for an arbitrary theory can be seen as a corollary of the following fundamental result.

Theorem A.12 *(Compactness theorem) Let T be a theory. If all finite subsets of T have a model then so does T.*

Suppose indeed that the compactness theorem holds, and let T be a formally consistent theory. Then an arbitrary finite subset T_0 of T is also formally consistent. Furthermore, we have seen that this implies the existence of a model for T_0. It follows then from the compactness theorem that T itself has a model.

Conversely, it is clear that the compactness theorem follows from the completeness theorem, since a theory is formally consistent as soon as all its finite subsets are.

A simple general proof of the compactness theorem is to consider the product topology on $\{0,1\}^V$ and to notice that the set of models of a given subset of T is a closed subset. The theorem is then a corollary of the compactness of the space $W := \{0,1\}^V$ when compactness is expressed (in classical mathematics) as: if a family of closed subsets of W has non-void finite intersections, then its intersection is non-void.

A.7 LPO and LLPO

If V is countable (*i.e.*, discrete and enumerable) we have the following alternative argument. One writes $V = \{p_0, p_1, \ldots\}$ and builds by induction a partial valuation v_n on $\{p_i \mid i < n\}$ such that any finite subset of T has a model which extends v_n, and v_{n+1} extends v_n. To define v_{n+1} one first tries $v_{n+1}(p_n) = 0$. If this does not work, there is a finite subset of T such that any of its model v that extends v_n satisfies $v(p_n) = 1$ and one can take $v_{n+1}(p_n) = 1$.

The non-effective part of this argument is contained in the choice of $v_{n+1}(p_n)$, which demands to give a gobal answer to an infinite set of (elementary) questions.

Now let us assume also that we can enumerate the infinite set T. We can then build a sequence of finite subsets of T in a nondecreasing way $K_0 \subseteq K_1 \subseteq \ldots$ such that any finite subset of T is a subset of some K_n. Assuming we have construct v_n such that all K_j's have a model extending v_n, in order to define $v_{n+1}(p_n)$ we have to give a global answer to the questions: do all K_j's have a model extending v_{n+1} when we choose $v_{n+1}(p_n) = 1$? For each j this is an elementary question, having a clear answer. More precisely let us define $g_n : \mathbb{N} \to \{0,1\}$ in the following way: $g_n(j) = 1$ if there is a model $v_{n,j}$ of K_j extending v_n with $v_{n,j}(p_n) = 1$, else $g_n(j) = 0$. By induction hypothesis if $g_n(j) = 0$ then all K_ℓ have a model $v_{n,\ell}$ extending v_n with $v_{n,\ell}(p_n) = 1$, and all models $v_{n,\ell}$ of K_ℓ extending v_n satisfy $v_{n,\ell}(p_n) = 1$ if $\ell \geq j$. So we can "construct" inductively the infinite sequence of partial models v_n by using at each step the non-constructive Bishop's principle LPO (Least Principle of Omniscience): given a function $f : \mathbb{N} \to \{0,1\}$, either $f = 1$ or $\exists j \in \mathbb{N}\ f(j) \neq 1$. This principle is applied at step n to the function g_n.

In fact we can slightly modify the argument and use only a combination of Dependant Choice and of Bishop's principle LLPO (Lesser Limited Principle of Omniscience), which is known to be strictly weaker than LPO: given two non-increasing functions $g, h : \mathbb{N} \to \{0,1\}$ such that, for all j

$$g(j) = 1 \vee h(j) = 1$$

then we have $g = 1$ or $h = 1$. Indeed let us define $h_n : \mathbb{N} \to \{0,1\}$ in a symmetric way: $h_n(j) = 1$ if there is a model $v_{n,j}$ of K_j extending v_n with $v_{n,j}(p_n) = 0$, else $h_n(j) = 0$. Cleraly g_n and h_n are non-increasing functions. By induction hypothesis, we have for all j $g_n(j) = 1 \vee h_n(j) = 1$. So, applying LLPO, we can define $v_{n+1}(p_n) = 1$ if $g_n = 1$ and $v_{n+1}(p_n) = 1$ if $h_n = 1$. Nevertheless, we have to use dependant choice in order to make this choice inifnitely often since the answer "$g = 1$ or $h = 1$" given by the oracle LLPO may be ambiguous.

In a reverse way it is easy to see that the completeness theorem restricted to the countable case implies LLPO.

A.8 Geometric formulae and theories

What would have happened if topologies without points had been discovered before topologies with points, or if Grothendieck had known the theory of distributive lattices? (G. C. Rota [20]).

A formula is *geometric* if, and only if, it is built only with the connectives $0, 1, \phi \wedge \psi, \phi \vee \psi$ from the propositional letters in V. A theory if a (propositional) *geometric* theory iff all the formula in T are of the form $\phi \to \psi$ where ϕ and ψ are geometric formulae.

It is clear that the formulae of a geometric theory T can be seen as relations for generating a distributive lattice L_T and that the Lindenbaum algebra of T is nothing else but the free Boolean algebra generated by the lattice L_T. It follows from proposition 1.8 that T is formally consistent if, and only if, L_T is nontrivial. Also, a model of T is nothing else but an element of $\mathrm{Spec}(L_T)$.

Theorem A.13 *(Completeness theorem for geometric theories) Let T be a geometric theory. If T generates a nontrivial distributive lattice, then T has a model.*

The general notion of geometric formula allows also existential quantification, but we restrict ourselves here to the propositional case. Even in this restricted form, the notion of geometric theory is fundamental. For instance, if R is a commutative ring, we can consider the theory with atomic propositions $D(x)$ for each $x \in R$ and with axioms

- $D(0_R) \to 0$
- $1 \to D(1_R)$
- $D(x) \wedge D(y) \to D(xy)$
- $D(xy) \to D(x)$
- $D(x + y) \to D(x) \vee D(y)$

This is a geometric theory T. The model of this theory are clearly the complement of the prime ideals. What is remarkable is that, while the existence of models of this theory is a nontrivial fact which may be dependent on set theoretic axioms (such as dependent axiom of choices) its formal consistency is completely elementary (as explained in the beginning of the section 3). This geometric theory, or the distributive lattice it generates, can be seen as a point-free description of the Zariski spectrum of the ring. The distributive lattice generated by this theory (called in this paper the Zariski lattice of R) is isomorphic to the lattice of compact open of the Zariski spectrum of R, while the Boolean algebra generated by this theory is isomorphic to the algebra of the constructible sets.