The Abdus Salam
International Centre for Theoretical Physics

United Nations
Educational, Scientific and
Cultural Organization

IAEA
International Atomic Energy Agency

1958-4

Summer School and Conference Mathematics, Algorithms and Proofs

11 - 29 August 2008

Constructive Logic in Algebra

Thierry Coquand
Chalmers University, Computer Science Dept.,
Gothenberg, Sweden

Constructive logic in algebra

August 4, 2008

Introduction

This document contains two examples of the use of distributive lattices as spaces in commutative algebra. The first example is a simple proof of Forster's Theorem about the number of generators over a ring of finite Krull dimension. The second example is the beginning of the theory of Prüfer Domain, which has to be thought of as a non Noetherian version of the theory of Dedekind Domain.

The general framework of this paper is a reformulation Hilbert's program using the theory of locales, also known as formal or pointfree topology [33, 13, 40]. 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 filter of neighbourhoods, while basic open sets are thought of as primitive symbolic objects or observable facts [14]. This is a reverse of the traditional conceptual order in topology which defines opens as particular sets of points [40]. 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 [37][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. 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, 12, 17, 20, 32] can be seen as a partial realisation of Hilbert's program in the field of commutative algebra.

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 a suggestive mean with no actual existence.

The document is written in the usual style of constructive algebra, with [38] 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 realising this specification together with its proof of correctness.

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

1 Forster's Theorem

1.1 Zariski spectrum and Krull dimension

Let R be a commutative ring with unit. Following Joyal [32], we define the Zariski spectrum of R as the distributive lattice generated by symbols $D(f),\ f \in R$ and relations

$$D(0)=0 \qquad D(1)=1 \quad D(fg)=D(f)\wedge D(g) \qquad D(f+g)\leqslant D(f)\vee D(g)$$

We write $D(f_1,\ldots,f_m)$ for $D(f_1)\vee\ldots\vee D(f_m)$. It can be shown directly that

$$D(g_1)\wedge\ldots\wedge D(g_n)\leqslant D(f_1,\ldots,f_m)$$

holds if, and only if, the monoid generated by $g_1,\ldots,g_n$ meets the ideal generated by $f_1,\ldots,f_m$ [9]. Thus $D(f_1,\ldots,f_m)$ can be defined as the radical of the ideal generated by $f_1,\ldots,f_m$ (with inclusion as ordering), and we have a point-free and elementary description of the basic open sets of the Zariski spectrum of R.

In the case where R is a polynomial ring over a field K, $D(f_1,\ldots,f_m)$ can be thought of as the complement of the sets of common zeros of $f_1,\ldots,f_m$ in an algebraic closure of K. This is the content of the Nullstellensatz theorem. But our elementary presentation is actually closer to the one of Kronecker [34], for which the common zeros were symbols in a suitable extension of K.

If $a_1,\ldots,a_m$ and $b_1,\ldots,b_n$ generates the same ideal, we have

$$D(a_1,\ldots,a_m)=D(b_1,\ldots,b_n)$$

and hence, we can write $D(I)=D(a_1,\ldots,a_m)$ if I is the ideal generated by $a_1,\ldots,a_m$.

In [10] we present the following elementary caracterisation of Krull dimension. If $a\in R$ we define the *boundary* of a as being the the ideal generated by a and the elements b such that ab is nilpotent (or equivalently $D(ab)=0$). Thus an element of the boundary N_a of a is of the form $at+b$ with $D(ab)=0$.

Theorem 1.1 *The dimension of R is $<n+1$ if, and only if, for all $a\in R$ the dimension of R/N_a is $<n$.*

This can actually be taken as a constructive definition of Krull dimension, if we define a ring R to be of dimension <0 if, and only if, R is trivial. This inductive definition of being of dimension $<n$ is then equivalent to the usual definition that there is no strictly increasing chain of prime ideals of length n [10]. In [9] it is shown, in an elementary and constructive way, that the dimension of a polynomial ring with n variables over a discrete field is $\leqslant n$.

1.2 The stable range theorem

All the arguments will be based on the following trivial remark, that we state explicitely since it will motivate the notion of dimension that we present in the last section.

We shall the following two remarks.

Lemma 1.2 $D(a+b)\vee D(ab)=D(a)\vee D(b)$

Lemma 1.3 *If by is nilpotent then $1=D(b_1,\ldots,b_k,b,y)$ implies $1=D(b_1,\ldots,b_k,b+y)$. More generally, if $by\in R$ is nilpotent in $R[a^{-1}]$ then $D(a)\leqslant D(b_1,\ldots,b_k,b,y)$ implies $D(a)\leqslant D(b_1,\ldots,b_k,b+y)$.*

Our inductive definition of dimension allows more perspicuous proofs. For instance, here is a proof of the Bass “Stable Range” theorem.

Theorem 1.4 *If the dimension of R if $<n$ and $1 = D(a, b_1, \ldots, b_n)$ there exists $x_1, \ldots, x_n$ such that $1 = D(b_1 + ax_1, \ldots, b_n + ax_n)$.*

Proof. The proof is by induction on n. Let I be the ideal boundary of b_n. We have $b_n \in I$ and the dimension of R/I is $<n-1$. By induction, we can find $x_1, \ldots, x_{n-1}$ such that

$$1 = D(b_1 + ax_1, \ldots, b_{n-1} + ax_{n-1})$$

in R/I. This means that there exists x_n such that $D(b_n x_n) = 0$ and

$$1 = D(b_1 + ax_1, \ldots, b_{n-1} + ax_{n-1}) \vee D(b_n) \vee D(x_n)$$

Since

$$1 = D(b_1 + ax_1, \ldots, b_{n-1} + ax_{n-1}) \vee D(b_n) \vee D(a)$$

this implies by distributivity

$$1 = D(b_1 + ax_1, \ldots, b_{n-1} + ax_{n-1}) \vee D(b_n) \vee D(ax_n)$$

hence the result by Lemma 1.3. □

It follows then for instance directly that a stably free module of rank $\geq n$ over a ring of dimension $<n$ is free [35], without any noetherianity hypotheses. We can in the same way prove Kronecker’s theorem about algebraic sets [11, 34].

We shall need a variation on this result. If $L \in R^n$ is a vector $(a_1, \ldots, a_n)$ we write $D(L)$ for $D(a_1, \ldots, a_n)$.

Lemma 1.5 *If $a \in R$ and the dimension of $R[a^{-1}]$ is $<n$ then for any $L \in R^n$ there exists $X \in R^n$ such that $D(a) \leqslant D(L - aX)$. Furthermore, we can find X of the form aY, $Y \in R^n$.*

Proof. We let L be $(b_1, \ldots, b_n)$ and we reason by induction on n. Let N be the ideal boundary of b_n *in* $R[a^{-1}]$, and I the ideal $N \cap R$. It can be checked that I that $(R/I)[a^{-1}]$ is isomorphic to $R[a^{-1}]/N$. Hence we can apply the induction hypothesis and compute $(x_1, \ldots, x_{n-1}) \in R^{n-1}$ such that

$$D(a) \leqslant D(b_1 - ax_1, \ldots, b_{n-1} - ax_{n-1})$$

in R/I. In turn, this means that we can find x_n such that $D(ax_n b_n) = 0$ and

$$D(a) \leqslant D(b_1 - ax_1, \ldots, b_{n-1} - ax_{n-1}) \vee D(b_n) \vee D(x_n)$$

in R. This implies

$$D(a) \leqslant D(b_1 - ax_1, \ldots, b_{n-1} - ax_{n-1}) \vee D(b_n) \vee D(ax_n)$$

hence the result by lemma 1.3. Finally, we can apply the result with a^2 instead of a since $R[a^{-2}] = R[a^{-1}]$ and $D(a) = D(a^2)$. □

Corollary 1.6 *Let M be a $n \times n$ matrix of element in R and δ its determinant. If the dimension of $R[\delta^{-1}]$ is $<n$ then for each $C \in R^n$ there exists $X \in R^n$ such that $D(\delta) \leqslant D(MX - C)$. Furthermore we can find X of the form δY, $Y \in R^n$.*

Proof. The proof is based on Cramer formulae. Let $\widetilde{M}$ be the adjoint matrix of M, and $L = \widetilde{M}C$. We have then $\widetilde{M}(MX - C) = \delta X - L$ for an arbitrary column vector $X \in R^n$. Hence the ideal generated by the coordinates of $\delta X - L$ is included in the one generated by the coordinates of $MX - C$, and

$$D(\delta X - L) \leqslant D(MX - C)$$

By Lemma 1.5 we can find *one* $X \in R^n$ such that $D(\delta) \leqslant D(\delta X - L)$, and hence $D(\delta) \leqslant D(MX - C)$ as desired. □

1.3 The Basic Element Theorem

Let F be a rectangular matrix of elements in R of columns $C_1, \ldots, C_p$, and G the matrix of columns $C_2, \ldots, C_p$. Let $\Delta_k = \Delta_k(F)$ be the ideal generated by all minors of F of order k.

Theorem 1.7 *Fix $0<k \leqslant p$. Suppose that for each minor ν of G of order k the ring $R[\nu^{-1}]$ is of dimension $<k$. Then there exists $t_2, \ldots, t_p$ such that $D(\Delta_k) \leqslant D(C_1 + t_2C_2 + \ldots + t_pC_p)$ and $D(C_1) \leqslant D(C_1 + t_2C_2 + \ldots + t_pC_p)$.*

Proof. Clearly, if $D(\nu) \leqslant D(C_1 + t_2C_2 + \ldots + t_pC_p)$ for all minor ν of G of order k then this holds also for all minor ν of F of order k. It is also enough to show that for *one* minor ν of G of order k we can find $t_2, \ldots, t_p$ such that $D(\nu) \leqslant D(C_1 + t_2C_2 + \ldots + t_pC_p)$ and $D(C_1) \leqslant D(C_1 + t_2C_2 + \ldots + t_pC_p)$ because we can then apply this successively to all minors of G of order k. But this is a direct consequence of Corollary 1.6: by this lemma, we find $t_2, \ldots, t_p$ (with $t_i = 0$ for the columns outside the minor ν) that are multiple of ν and such that

$$D(\nu) \leqslant D(C_1 + t_2C_2 + \ldots + t_pC_p)$$

Since $t_2, \ldots, t_p$ are all multiple of ν we have also $D(C_1) \leqslant D(\nu) \vee D(C_1 + t_2C_2 + \ldots + t_pC_p)$ and hence $D(C_1) \leqslant D(C_1 + t_2C_2 + \ldots + t_pC_p)$ as required. □

Corollary 1.8 *Suppose that $1 \in \Delta_1$ and that for each $k > 0$ and for each minor ν of G of order k the ring $R[\nu^{-1}]/\Delta_{k+1}$ is of dimension $<k$. Then there exists $t_2, \ldots, t_p$ such that the vector $C_1 + t_2C_2 + \ldots + t_pC_p$ is unimodular.*

Proof. Using the theorem, we define a sequence of vectors C_1^i, $i = 1, \ldots$ with $C_1^1 = C_1$. For each $k > 0$, reasoning in R/Δ_{k+1}, we build C_1^{k+1} of the form $C_1^k + u_2C_2 + \ldots + u_pC_p$ such that $D(\Delta_k) \leqslant D(C_1^{k+1})$ and $D(C_1^k) \leqslant D(C_1^{k+1})$ in R/Δ_{k+1}. This means that we have, in R

$$D(C_1^k) \vee D(\Delta_k) \leqslant D(C_1^{k+1}) \vee D(\Delta_{k+1})$$

Hence the result since $D(\Delta_1) = 1$ and $D(\Delta_k) = 0$ for k large enough. □

From this follows directly, like in [25, 30], the version of Serre's "Splitting-off" theoremand Forster-Swan theorem, with Krull dimension (and without noetheriannity hypothesis). For instance, here is a version of Forster's theorem [27], without noetherianity hypothesis.

Corollary 1.9 *Let M be a module which is finitely generated over a ring R of dimension $\leqslant d$. If M is locally generated by k elements then M can be generated by $d + k$ elements.*

Proof. M is a quotient of a finitely presented module M' which has a Fitting ideal of order k which contains 1, and we can as well suppose that $M' = M$. Let $m_1, \ldots, m_p$ be a system of generators of M and F be a presentation matrix of M. If $p > d + k$ we have $1 \in \Delta_k(F)$ and using theorem 1.7, we can find $t_2, \ldots, t_p$ such that M is generated by $m_2 - t_2m_1, \ldots, m_p - t_pm_1$. Hence we can generate M by $p - 1$ elements. □

2 Prüfer Domain and Algebraic Curves

2.1 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* [33], introduced in [44], 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].

2.1.1 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 pointfree 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. Inpired by Espanol and Joyal [26] we gave in [9] the following pointfree characterisation of this notion.

Proposition 2.1 *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 2.2 *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.

2.1.2 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 pointfree 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 pointfree way [7, 15].)

Proposition 2.3 *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 $\phi^* : Sp(V) \rightarrow Sp(Z)$ 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 $\alpha_1 = \phi^*(\beta_1)$.

2.1.3 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 pointfree way.

Proposition 2.4 *If $\phi : Z \rightarrow V$ 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 result for 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. □

2.2 The Zariski lattice of a ring

Joyal [32] 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 [32])

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

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[2]. 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 characterises 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 realisation of a lattice satisfying the support relations is obtained by taking the lattice of radical of finitely generated ideals[3] 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 satisying

[2] But we have for instance $D(a, b) = D(a + b)$ if $D(ab) = 0$ [12].

[3] In general the lattice of ideals of R is *not* distributive, for instance in the case $R = k[X, Y]$. If it is, the ring is said to be *arithmetic*. The importance of this notion for constructive algebra is stressed in [20].

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 2.5 *$\mathsf{Kdim}\ R < n$ 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 [46], but not first-order.

2.3 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 $\mathsf{Val}(L, R)$.

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 $V_R(s) \wedge V_R(s^{-1}) = V_R(s + s^{-1})$[4]. We also have $V_R(r_1^{-1}) \wedge V_R(r_2^{-1}) = V_R((r_1 r_2)^{-1})$ if $V_R(r_1) = V_R(r_2) = 1$.

Lemma 2.6 *$V_R((x{+}y)^{-1}) \leqslant V_R(x^{-1}, y^{-1})$ 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 2.7 *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 $V_R(x_i/x_n) \wedge \wedge_{j<n} V_R(x_j/x_i) \leqslant \wedge_j V_R(x_j/x_n)$. □

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

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, since this can also be written $s = -p_1 - p_2 s^{-1} - \ldots - p_k s^{-1+k}$ and $1 = V_R(s, s^{-1})$, we have $V_R(t_1) \wedge \ldots \wedge V_R(t_n) \leqslant V_R(s)$. The converse will follow from the following characterisation of $\mathsf{Val}(L, R)$, which is proved by a cut-elimination argument.

Theorem 2.8 *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 $1 = <s_1^{-1}, \ldots, s_n^{-1}>$ 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 pointfree 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 [17] 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* [41]. The proof involves the algebraic elimination of variables.

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 2.9 *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.

2.4 Center of a valuation

2.4.1 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 pointfree 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 2.10 *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 2.6. □

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 $\phi(0) = 0$.

2.4.2 An application: Dedekind's Prague Theorem

The simple existence of the center map, which has been proved without using Theorem 2.8, 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 $P = a_0 + \ldots + a_n X^n$ is a poynomial in $R[X]$ we write $c(P) = D(a_0, \ldots, a_n)$ the *radical content* of P [26].

Lemma 2.11 *(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 *indeterminates*; we write $c_k = \Sigma_{i+j=k} a_i b_j$. 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[5]

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

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

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

By Lemma 2.7 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[6].

Theorem 2.12 *In the lattice $\mathsf{Val}(L, \mathbb{Z})$ we have $1 = \vee_k V(a_i b_j/c_k)$ for any i, j, hence by Corollary 2.9, each element $a_i b_j$ is integral over the ideal generated by $c_0, \ldots, c_{n+m}$.*

This result, which generalises a famous Theorem of Gauss [22], is described by O. Neumann to be "one of the most basic result in commutative algebra of the XIXth century" [39]. Our argument is a computational interpretation of its modern non constructive proof based on valuations [3], and is a direct generalisation of the reasoning of Gauss. One can follow this proof and produce explicitely from it the required polynomial identity using Theorem 2.8. 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 it is used only as an ideal and suggestive mean.

2.4.3 Properties of the center map

The next result expresses in a pointfree way that the center map is *surjective*, i.e. any prime ideal is the center of some valuation rings. There the use of Theorem 2.8 seems essential.

Proposition 2.13 *The center map $\phi : \mathsf{Zar}(R) \to \mathsf{Val}(R)$ is injective.*

[5] 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 $P = 1/a_{i_0} \Sigma a_i X^i$, $Q = 1/b_{j_0} \Sigma b_j X^j$ are in $V[X]$. Since P and Q have 1 as coefficient, it follows from Lemma 2.11 that at least one coefficient of the product PQ is not in $\mathfrak{m}_V$. This is what the inequality (1) expresses.

[6] Our argument precises the sketch which is presented at the end of [17].

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 2.8, 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 $1 = s_1 q_1 + \dots + s_m q_m$. 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 2.14 *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 $1 = \Sigma s_j^{-1} q_j + \Sigma r_i p_i$. By multiplying by a power of r we find a relation of the form $r^k - \Sigma t_i r_i = \Sigma s_j^{-1} l_j$ with t_i in R and l_j in $R[1/s_1, \dots, 1/s_m]$. The element $w = r^k - \Sigma t_i r_i$ 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 2.3. □

Corollary 2.15 *If* $\mathsf{Vdim}\ R \leqslant n$ *then* $\mathsf{Kdim}\ R \leqslant n$.

Proof. This follows from Proposition 2.4. □

2.5 Prüfer domain

The importance of the notion of Prüfer domain for constructive mathematics is stressed in [20]: it is 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 [20], 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. $a_{11} + \dots + a_{nn} = 1$
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 localisation matrix* of $x_1, \dots, x_n$ [20][7]. 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 $<a_{1i}, \dots, a_{ni}> \cdot <x_1, \dots, x_n> = <x_i>$. We find in this way explicitely an *inverse* of the ideal $<x_1, \dots, x_n>$ [20][8].

Let $\mathsf{Div}(R)$ be the monoid of fractional ideals, also called *divisors* of R [22]. 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[9] important properties [3, 14]: $\mathsf{Div}(R)$ 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* [38] and we can solve any linear system over it [20]. We stress that

[7] In the localisation $R[1/u_i]$ the ideal $<x_1, \dots, x_n>$ is principal and equal to $<x_i>$.

[8] 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 2.25 shows that this ring is a Prüfer domain.

[9] The structure of lattice group was discovered by Dedekind and rediscovered independently by F. Riesz. It plays an important rôle in abstract functional analysis [14].

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 2.16 *The spectrum of the lattice group* $\mathsf{Div}(R)$ *[14] is the dual of the Zariski spectrum of* R.

Proof. The spectrum of $\mathsf{Div}(R)$ is shown in [14] 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 2.17 *If R is a Prüfer domain then the center map* $\phi : \mathsf{Zar}(R) \to \mathsf{Val}(R)$ *is an isomorphism.*

Proof. By Proposition 2.13 it is enough to show that the map ϕ is surjective[10]. 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 2.17 holds if R is integrally closed. For proving this converse, we state a general lemma, which expresses in a pointfree way that an integral domain is arithmetical iff any localisation at a prime ideals is a valuation domain.

Lemma 2.18 *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 $(1-u)1/s = w$. □

Lemma 2.19 *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[11]. □

Proposition 2.20 *If R is an integral domain which is integrally closed and such that the center map* $\phi : \mathsf{Zar}(R) \to \mathsf{Val}(R)$ *is an isomorphism then R is a Prüfer domain.*

[10] Proposition 2.13 relies on cut-elimination (Theorem 2.8). One can prove directly, by a somewhat longer argument, that ϕ is a bijection without using Theorem 2.8.

[11] 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.

Proof. We use Lemma 2.18. 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

$$V_R(s) = \phi(D(a_1, \ldots, a_n)), \quad V_R(1/s) = \phi(D(b_1, \ldots, b_m)).$$

We have $1 = \phi(D(a_1, \ldots, a_n, b_1, \ldots, b_m))$ and hence $1 = D(a_1, \ldots, a_n, b_1, \ldots, b_m)$ 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 2.8. □

The following proposition was obtained while analysing Seidenberg's Lemma ([31], Chapitre III, Proposition 2) in a pointfree setting. We rediscovered in this way Gilmer-Hoffmann's Theorem [29]. 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 2.21 *(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 $\mathsf{Zar}(R)$*[12] *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 2.18.

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

$$b_n = a_n,\ b_{n-1} = b_ns + a_{n-1},\ b_{n-2} = b_{n-1}s + a_{n-2}, \ldots,\ b_1 = b_2s + a_1$$

Notice that $P(s) = b_1s + a_0 = 0$. We have $c(P) \leqslant D(b_n, b_ns, b_{n-1}, b_{n-1}s, \ldots, b_1, b_1s)$ since $D(a_n) = D(b_n)$ and $D(a_i) \leqslant D(b_{i+1}s, b_i)$ for $0 < i < n$ and $D(a_0) = D(b_1s)$. Since we have $P(s) = a_ns^n + \ldots + a_0 = 0$ and R is integrally closed, we can prove successively that $b_n, b_ns, b_{n-1}, \ldots$ are all in R. Finally, we have $1/s$ in $R[1/b_is]$ and s in $R[1/b_i]$. □

Corollary 2.22 *If $\mathsf{Kdim}\ R[X] \leqslant 2$ and R is integrally closed then R is a Prüfer domain.*

Proof. We use Proposition 2.21. 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 2.5 to the 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. □

Corollary 2.23 *If R is an integral domain which is integrally closed and such that $\mathsf{Vdim}\ R \leqslant 1$ then R is a Prüfer ring.*

[12] 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.

Proof. We proceed like in the proof of Corollary 2.22. 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 2.15. Hence we can apply Theorem 2.5 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 characterisation in [20]: 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 2.24 *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 2.21 it is enough to show that $R[s]$ is integrally closed. Like in the proof of Proposition 2.17 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 2.19. 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[13] in an extension of its field of fractions is a Prüfer domain.

Theorem 2.25 *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*[14].

Proof. We use Proposition 2.21. 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 $R[X]$.) □

2.6 Towards pointfree algebraic geometry

We apply the previous results to give a simple pointfree description of the notion of algebraic curves as a scheme. For this we need to develop some sheaf theory in a pointfree setting, up to the cohomological definition of the genus, following the fundamental paper of Serre [43]. 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.

[13] A *Bezout* domain is a domain where any finitely generated ideal is principal [38].

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

2.6.1 Sheaves over lattices

We will analyse 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 *preheaf* 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 glueing conditions are satisfied:

1. if $u = u_1 \vee u_2$, and x_i in $\mathcal{F}(u_i)$ 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 $x|u_i = x_i$ and

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[15].

Lemma 2.26 *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 2.26. 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 $\Gamma(\mathsf{Zar}(R), \mathcal{O}) = \mathcal{O}(D(1)) = R$.

2.6.2 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 on $k[x]$ 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 on k, in which case a is said to be a *constant* of L, or if x is algebraic on $k[a]$, 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 $E(p)$.

[15] 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 lattice $\mathsf{Val}(L, k)$ 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 $\mathcal{F}(u)$ to be the set of elements q in L such that $u \leqslant V(q)$ in $\mathsf{Val}(L, k)$. In particular $\mathcal{F}(V(a_1) \wedge \ldots \wedge V(a_n))$ is the set $E(a_1, \ldots, a_n)$, by Theorem 2.8. Thus $\Gamma(X, \mathcal{F}) = \mathcal{F}(1)$, the global sections of $\mathcal{F}$, is the field of constants of L. The fact that $\Gamma(X, \mathcal{F})$ is the field of constants of L is an algebraic counterpart of the fact that the global holomorphic functions on the Riemann sphere are the constant functions.

A point α of $\mathsf{Val}(L, k)$ can be identified with the valuation ring A_α of elements a such that $\alpha \in V(a)$. The *fiber* of $\mathcal{F}$ at a point α is defined to be the inductive limit of $\mathcal{F}(u)$ with $\alpha \in u$. The fiber at α is nothing else than A_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 $\mathcal{F}(V(a) \wedge V(1/b_1, \ldots, 1/b_m)) = E(a)[1/b_1] \cap \ldots \cap E(a)[1/b_m]$.

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

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

It follows also from Theorem 2.25 that $E(p)$ is a Prüfer domain, and so by Proposition 2.17 that the sublattice $\downarrow V(p)$ of $\mathsf{Val}(L, k)$, which is isomorphic to $V(E(p))$, is isomorphic to $\mathsf{Zar}(E(p))$. We thus see that the sheaf $\mathcal{F}$ restricted to the basic open $V(p)$ is isomorphic to the affine scheme $\mathsf{Zar}(E(p)), \mathcal{O}$.

The pair $(X, \mathcal{F})$, 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 $\mathcal{F}$ reduces to the structure sheaf over each open U_i. (Suprisingly, I was unable to find this example in the literature.)

Notice that, even in the simplest case where $L = k(t)$, the sheaf $\mathcal{F}$ is not isomorphic to an affine scheme. This follows from the observation that $\Gamma(X, \mathcal{F})$ 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.

2.6.3 The genus of an algebraic curve

Lemma 2.27 *For all parameters p and q 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 2.24 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[16]. □

Corollary 2.28 *The k-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 *$H^1(L)$ of the field L.*

Proof. Our argument is a specialisation of the general cohomological argument [43]. 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 2.27, we show that this relation defines an isomorphism between $H^1(p)$ and $H^1(q)$.

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

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 2.27, 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 [28, 24]. In this case, an element of $E(x)$ is an element $p + yq$ with $p, q \in \mathbb{Q}[x]$. Also, an element of $E(1/x)$ is of the form $a + (y/x^2)b$, with $a, b \in \mathbb{Q}[1/x]$. 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 $p, q \in \mathbb{Q}[x],\ a, b \in \mathbb{Q}[1/x]$.

Proposition 2.29 *We have* $H^1(L, \mathcal{F}) = E(x, 1/x)/E(x) \oplus E(1/x) = \mathbb{Q}$.

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 2.30 *We have* $H^1(S, \mathcal{F}) = 0$.

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

Proposition 2.31 $L = \mathbb{Q}(x, y),\ y^2 = 1 - x^4$ *cannot be written on the form* $L = \mathbb{Q}(t)$.

While it is possible to prove this Proposition by direct methods, we think that it is a good illustration of the power of cohomological methods. Here is a simple application.

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.

[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. Sur un théorème de Kronecker concernant les variétés algébriques *C. R. Acad. Sci. Paris*, Ser. I 338 (2004), Pages 291-294

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

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

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

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

[16] 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.

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

[18] Th. Coquand, L. Ducos, H. Lombardi and C. Quitté. Constructive Krull Dimension. I: Integral Extensions. to appear in the Journal of Algebra and its Applications, 2007.

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

[20] 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.

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

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

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

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

[25] D. Eisenbud and E. G. Evans, Jr. Generating modules efficiently: theorems from algebraic K-theory. J. Algebra 27 (1973), 278–305.

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

[27] O. Forster. Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring. Math. Z. 84 1964 80–87.

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

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

[30] R. Heitmann. Generating non-Noetherian modules efficiently. Michigan Math. J. 31 (1984), no. 2, 167–180.

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

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

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

[34] L. Kronecker. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *J. reine angew. Math.* 92, 1-123 (1882). Réimprimé dans *Leopold Kronecker's Werke*, II, 237–387.

[35] T.Y. Lam. Serre's conjecture. Lecture Notes in Mathematics, Vol. 635. Springer-Verlag, Berlin-New York, 1978.

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

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

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

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

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

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

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

[43] J.P. Serre. Faisceaux Algébriques Cohérents. *Annals of Mathematics*, 1955.

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

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

[46] 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.

Exercises on the course on Constructive Logic

August 4, 2008

Exercises on intuitionistic logic

1. Prove that the schema $\neg\neg A \rightarrow A$ is equivalent to the law of excluded middle $A \vee \neg A$

2. (To get a feeling about the difference between constructive and classical reasoning.) Consider the sequence z_n in $[0, 1]$ defined by $z_0 = 1$ and $z_{n+1} = z_n - z_n^2/2$. Prove classically that z_n converges to 0 as follows. First show that $0 \leqslant z_{n+1} \leqslant z_n$ and hence that z_n converges. Let l be the limit. Show that $l^2 = 0$ and hence $l = 0$. Where have we used the law of excluded-middle in this reasoning? This result implies that given $\epsilon > 0$ we can find N such that $z_N \leqslant \epsilon$. Try to see if we can extract such a N from this reasoning, and then find a constructive justification of the existence of such a N.

3. (Constructive version of classical results.) Show classically that if X is a compact metric space and $f : X \rightarrow X$ is such that $d(f(x), f(y)) < d(x, y)$ if $x \neq y$ then f has a unique fixed-point. For this, consider a point where the function $x \longmapsto d(x, f(x))$ is minimum. The goal of this exercice is to present a constructive reading of this result. The condition

   $$x \neq y \rightarrow d(f(x), f(y)) < d(x, y)$$

   can be written

   $$(\exists n. d(x, y) \leqslant 1/2^n) \rightarrow (\exists m. d(f(x), f(y)) \leqslant (1 - 1/2^m) d(x, y))$$

   A natural constructive reading is

   $$(1) \qquad \forall n \exists m.\ \ d(x, y) \leqslant 1/2^n \rightarrow d(f(x), f(y)) \leqslant (1 - 1/2^m) d(x, y))$$

   Show from (1) only that for any $\epsilon > 0$ and any a in X there exists N such that

   $$d(f^{N+1}(a), f^N(a)) < \epsilon$$

   Using (1), show also that we have

   $$(2) \qquad \forall \epsilon > 0. \exists \eta > 0.\ \ d(x, f(x)) < \eta \wedge d(y, f(y)) < \eta \rightarrow d(x, y) < \epsilon$$

   Explain why (2) can be seen as a constructive reading of the implication

   $$x = f(x) \wedge y = f(y) \rightarrow x = y$$

   Using this, show constructively that if X is a metric space which satisfies (1) and is *complete* (no need of compactness) then f has a unique fixed-point, and furthermore, that for any point a in X the sequence $f^n(a)$ is a Cauchy sequence which converges to this fixed-point.

   This example is extracted from the work of Ulrich Kohlenbach, who had developped remarkable constructive reading of multiple results in analysis (especially fixed-point theory) using techniques from logic.

4. Define in the theory of rings $J(x)$ as $\forall y.inv(1-xy)$, where $inv(x)$ means $\exists y.1 = xy$. Classically $J(x)$ means that x belongs to all maximal ideals. Prove this using Zorn's Lemma. It follows in particular that $J(x)$ defines an ideal and hence $J(x) \wedge J(y) \rightarrow J(x+y)$ is a semantical consequence of the theory of rings. Check the validity of the completeness theorem of the first-order theory of rings by giving a direct first-order proof of this implication.

5. The notion of principal ideal domain is subtle constructively: the classical notion involves a quantification over all ideals. Constructively, one tries to work instead with a first-order approximation, which is the notion of *Bezout domain*: any *finitely generated* ideal is principal. Check that this notion is first-order and is even coherent. Show that if K is a field then $K[X]$ is a Bezout domain.

6. The notion of *Unique Factorization Domain* (any element is in a unique way a product of irreducible elements) is not a first-order notion. Constructively, one replaces this notion by the notion of *gcd domain*: for any a, b there exists g which divides a and b and such that if c divides a and b then c divides g. Check that this is a first-order notion. Show that such an element g is defined uniquely up to a unit. Such an element g is called a *gcd* of a and b. Show that any Bezout domain is a gcd domain.

   If R is a gcd domain we define the *content* of a polynomial P in $R[X]$ to be the gcd of all its coefficient, and we say that a polynomial is *primitive* iff its content is 1. Show that the product of two primitive polynomials is primitive. Deduce from this that the content of the product of two polynomials is the product of the content of these polynomials. Show that if K is the field of fractions of R then $K[X]$ is a gcd domain. Using this show that if R is a gcd domain then so is $R[X]$. (This is similar to the result that $R[X]$ is UFD if R is UFD.)

7. The goal of this exercise is to show that we cannot derive $(\exists x.x^2+1=0) \vee \forall x.x^2+1 \neq 0$ in the theory of discrete field (this can be interpreted as the fact that we cannot decide the irreducibility of polynomials). We consider the forcing associated to the theory of dicsrete fields where a covering of R is given by $R \rightarrow R/{<}a{>}$ and $R \rightarrow R[1/a]$. Show first that $R \Vdash \forall x.x^2+1 \neq 0$ holds iff R is the trivial ring. Show next that $R \Vdash \exists x.x^2+1=0$ iff there exists $x_1, \ldots, x_n$ in R such that $0 = (1+x_1^2)\ldots(1+x_n^2)$.

Local-global principle

1. If L is a distributive lattice we say that b is a complement of a iff $a \wedge b = 0$ and $a \vee b = 1$. Prove that if b' is also a complement of b then $b' = b$.

2. Find an example of a ring which has a lattice of ideals which is *not* distributive

3. We consider three sequences $X = (a_i)$, $Y = (b_j)$, $Z = (c_k)$ in a ring R connected by $c_k = \Sigma_{i+j=k} a_i b_j$. This can be written as $\Sigma c_k X^k = PQ$ where $P = \Sigma a_i X^i$ and $Q = \Sigma b_j X^j$. The following is a classical proof that if a_i and b_j are unimodular then so is c_k. We consider an arbitrary prime ideal $\mathfrak{p}$. Show that if P and Q are not 0 mod. $\mathfrak{p}$ then PQ is not 0 mod. $\mathfrak{p}$ and conclude by using the fact that a sequence is unimodular iff it is not 0 mod. any prime ideal. Read this argument in a point free way to give a proof of Gauss-Joyal identity $D(Z) = D(X) \wedge D(Y)$.

   Give an example of a ring where we don't have ${<}Z{>} = {<}X{>}{<}Y{>}$ (we recall that ${<}A{>}$ denotes the ideal generated by the elements of the sequence A).

If R is a domain of field of fractions K, prove that we have also $V_R(Z) = V_R(X) \wedge V_R(Y)$, where $V_R : K \to Val(K, R)$ is the space of valuations of K/R.

4. Use the previous exercise to give a constructive proof that if P in $R[X]$ is nilpotent then each coefficient of P is nilpotent.

5. Prove that $D(a + b, ab) = D(a, b)$ first by using prime ideals and then by using only the universal characterisation of the map $D : R \to Z(R)$.

Krull dimension

1. (Kronecker's Theorem) Implement an algorithm that given P_0, P_1, P_2, P_3 in $K[X, Y]$ compute Q_0, Q_1, Q_2 such that $V(P_0, P_1, P_2, P_3)$ the set of commun zeros of P_0, P_1, P_2, P_3 in the algebraic closure of K is equal to $V(Q_0, Q_1, Q_2)$.

2. Show that to be of Krull dimension $< n$ is a local property: if we have $a_1, \ldots, a_l$ such that $1 = D(a_1, \ldots, a_l)$ and $\mathsf{Kdim}\ R[1/a_i] < n$ for all i then we have also $\mathsf{Kdim}\ R < n$.

3. (Local Kronecker's Theorem) We say that two sequences $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are *disjoint* iff we have

$$D(a_1b_1) = 0,\ D(a_2b_2) \leqslant D(a_1, b_1), \ldots,\ D(a_nb_n) \leqslant D(a_{n-1}, b_{n-1})$$

Show that in this case we have

$$D(a_1, \ldots, a_k, b_1, \ldots, b_k, a_{k+1}b_{k+1}) = D(a_1 + b_1, \ldots, a_k + b_k)$$

for all $k < n$. Use this to show that if R is a local ring residually discrete of Krull dimension n such that its maximal ideal is finitely radically generated, then the maximal ideal can be radically generated by n elements.

Exercises on Prüfer Domain

1. Given an algorithm which witnesses

$$\forall x\ y. \exists u\ v\ w.\ \ xu = yv \wedge y(1 - u) = xw$$

we can compute an inverse of any ideal generated by two elements. Compute from this the inverse of an arbitrary finitely generated ideal (hint: given a finite sequence of elements, show that, locally, one element divides all the others)

2. Show that $\mathbb{Q}[x, y]$ defined by $y^2 = x^3$ is not a Prüfer domain.

3. Compute an inverse of the ideal $<x, y>$ in the ring $\mathbb{Q}[x, y]$ with $y^2 = 1 - x^4$