The Zariski Spectrum of a ring

Thierry Coquand

September 2010

Use of prime ideals

Let R be a ring. We say that $a_0, \ldots, a_n$ is *unimodular* iff $\langle a_0, \ldots, a_n \rangle = 1$

We say that $\Sigma a_i X^i$ is *primitive* iff $a_0, \ldots, a_n$ is unimodular

Theorem: *The product of two primitive polynomials is primitive*

Lemma: *A sequence $a_0, \ldots, a_n$ is unimodular iff it is not zero modulo any prime ideal*

Lemma: *The product of two non zero polynomials modulo a prime ideal $\mathfrak{p}$ is not zero modulo $\mathfrak{p}$*

Product of primitive polynomials

$$A = a_0 + a_1X \qquad B = b_0 + b_1X \qquad C = c_0 + c_1X + x_2X^2$$

$$c_0 = a_0b_0 \qquad c_1 = a_0b_1 + a_1b_0 \qquad c_2 = a_1b_1$$

By completeness theorem, in the theory of rings (equational theory) we can show the implication

$$a_0x_0 + a_1x_1 = 1 \quad \wedge \quad b_0y_0 + b_1y_1 = 1 \ \rightarrow$$

$$\exists z_0 \ z_1 \ z_2. \ a_0b_0z_0 + (a_0b_1 + a_1b_0)z_1 + a_1b_1z_2 = 1$$

Use of prime ideals

We analyze the proof

Let $\mathfrak{p}$ be a prime ideal of R, we are interested in the property $D_{\mathfrak{p}}(a)$ meaning a is *not* in the ideal $\mathfrak{p}$

If $A = a_0 + a_1 X + \cdots + a_n X^n$ is a polynomial in $R[X]$ we write $D_{\mathfrak{p}}(A)$ for $D_{\mathfrak{p}}(a_0) \vee \cdots \vee D_{\mathfrak{p}}(a_n)$

A is primitive iff $D_{\mathfrak{p}}(A)$ holds for *all* $\mathfrak{p}$

We want to show $D_{\mathfrak{p}}(A) \wedge D_{\mathfrak{p}}(B) \rightarrow D_{\mathfrak{p}}(AB)$

Use of prime ideals

The property $D_{\mathfrak{p}}(x)$ satisfies

$$(D_{\mathfrak{p}}(a) \wedge D_{\mathfrak{p}}(b)) \leftrightarrow D_{\mathfrak{p}}(ab) \qquad D_{\mathfrak{p}}(a+b) \rightarrow D_{\mathfrak{p}}(a) \vee D_{\mathfrak{p}}(b) \qquad \neg D_{\mathfrak{p}}(0) \qquad D_{\mathfrak{p}}(1)$$

$$A = a_0 + a_1 X + \cdots + a_n X^n$$

$$B = b_0 + b_1 X + \cdots + b_m X^m$$

$$C = AB = c_0 + c_1 X + \cdots + c_l X^l$$

Use of prime ideals

We want to show $D_{\mathfrak{p}}(A) \wedge D_{\mathfrak{p}}(B) \rightarrow D_{\mathfrak{p}}(C)$

We show $D_{\mathfrak{p}}(a_i) \wedge D_{\mathfrak{p}}(b_j) \rightarrow \bigvee_{k \leqslant i+j} D_{\mathfrak{p}}(c_k)$ by induction on $i + j$

Use of prime ideals

For instance $A = a_0 + a_1 X$ and $B = b_0 + b_1 X + b_2 X^2$

$c_0 = a_0 b_0$ $\qquad$ $c_1 = a_0 b_1 + a_1 b_0$

$c_2 = a_0 b_2 + a_1 b_1$ $\qquad$ $c_3 = a_1 b_2$

In general

$$a_{i_0} b_{j_0} = c_{k_0} - \sum_{i<i_0 \ i+j=k_0} a_i b_j - \sum_{j<j_0 \ i+j=k_0} a_i b_j$$

Use of prime ideals

If A and B are primitive we have $D_{\mathfrak{p}}(A)$ and $D_{\mathfrak{p}}(B)$ for all $\mathfrak{p}$ and so we have $D_{\mathfrak{p}}(AB)$ for all $\mathfrak{p}$

Hence AB is primitive

Prime filters

The property $D_{\mathfrak{p}}(x)$ satisfies

$$\neg D_{\mathfrak{p}}(0) \quad D_{\mathfrak{p}}(1) \quad (D_{\mathfrak{p}}(a) \wedge D_{\mathfrak{p}}(b)) \leftrightarrow D_{\mathfrak{p}}(ab) \qquad D_{\mathfrak{p}}(a+b) \rightarrow D_{\mathfrak{p}}(a) \vee D_{\mathfrak{p}}(b)$$

A subset of R having these properties (complement of a prime ideal) is called a *prime filter*

Use of prime ideals

It can be shown that, even if the ring is given effectively, it is not possible in general to define effectively a prime ideal on this ring

Lawvere (ICM 1970) conjectured the existence of a prime filter for any non trivial ring in an arbitrary topos. Joyal built topos where a ring does not have any prime filter

This indicates that we cannot follow naively the previous proof in an effective context or in an arbitrary topos

Use of prime ideals

In the previous argument, we use a prime filter in a generic way

We are going to use a method similar the one of forcing in set theory, to "force" the existence of a generic prime ideal. This method is also due to Joyal

Zariski spectrum

The set of all prime ideals of a ring R has a natural topology with basic open

$$D(a) = \{\mathfrak{p} \mid a \notin \mathfrak{p}\}$$

We clearly have $D(a) \cap D(b) = D(ab) \quad D(0) = \emptyset$

The space of all prime ideals with this topology is called the *Zariski spectrum* of R

This is a compact topology, in general non Hausdorff

Zariski spectrum

Though we cannot describe the points of this space effectively in general, we can describe the topology of the space effectively

The compact open of the spectrum are of the form

$$D(a_1, \dots, a_n) = D(a_1) \cup \cdots \cup D(a_n)$$

The compact open form a distributive lattice

We give a direct effective description of this lattice

Zariski lattice

We consider now $D(a)$ as pure symbolic expression for each a in R and we consider the lattice generated by these symbols and the relations

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

This lattice is called the *Zariski lattice* of the ring R. This is a purely *algebraic* notion.

Zariski lattice

We write $D(a_1,\ldots,a_n) = D(a_1) \vee \cdots \vee D(a_n)$ so that the last relation can be written $D(a+b) \leqslant D(a,b)$

We have $D(a^2) = D(a^3) = \cdots = D(a)$

Since we have $D(a) \wedge D(b) = D(ab)$ all elements of the lattice are of the form $D(a_1,\ldots,a_n)$

In general we don't have $D(a,b) = D(a+b)$ only $D(a+b) \leqslant D(a,b)$

We have $D(a,b) = D(a{+}b)$ if $D(ab) = 0$ and in general $D(a,b) = D(a{+}b, ab)$

Also $D(a,b,c) = D(a+b+c, ab+bc+ca, abc)$

Gauss-Joyal

Theorem: *If* $(\Sigma a_i X^i)(\Sigma b_j X^j) = \Sigma c_k X^k$ *then we have*

$$D(a_0, \ldots, a_n) \wedge D(b_0, \ldots, b_m) = D(c_0, \ldots, c_l)$$

It is clear that we have $D(c_k) \leqslant D(a_0, \ldots, a_n) \wedge D(b_0, \ldots, b_m)$ for all k and we have to show, for all i_0, j_0

$$D(a_{i_0} b_{j_0}) \leqslant D(c_0, \ldots, c_{k_0})$$

where $k_0 = i_0 + j_0$

Gauss-Joyal

We can write

$$a_{i_0}b_{j_0} = c_{k_0} - \sum_{i<i_0 \;\; i+j=k_0} a_i b_j - \sum_{j<j_0 \;\; i+j=k_0} a_i b_j$$

and so

$$D(a_{i_0}b_{j_0}) \leqslant D(c_{k_0}) \vee \bigvee_{i<i_0} D(a_i) \vee \bigvee_{j<j_0} D(b_j)$$

Logical interpretation

"Lattice-valued" model: the predicate $a \longmapsto D(a)$ is a predicate on the ring R with values in the Zariski lattice

This predicate defines a prime filter on the ring

This is a generic prime filter. This prime filter exists, but in a forcing extension/sheaf model over the Zariski spectrum

Zariski lattice

All this can be derived from the relations, but we did not use that the lattice is *generated* by these relations

We have shown that the product of two non zero polynomials is non zero modulo a prime ideal

We have to show that if $D(a_1, \dots, a_n) = 1$ holds then $a_0, \dots, a_n$ is unimodular

Zariski lattice

Theorem: *We have* $D(a) \leqslant D(b_1, \dots, b_m)$ *iff* a *is in the radical of the ideal generated by* $b_1, \dots, b_m$. *In particular* $D(a_1, \dots, a_n) = 1$ *iff* $a_1, \dots, a_n$ *is unimodular*

If I is an ideal the *radical* $\sqrt{I}$ of I is the set of elements a that have a power in I i.e. $\{a \in R \mid (\exists N)\ a^N \in I\}$

The *formal Nullstellensatz* states precisely that this lattice will coincide with the lattice of compact open subsets of the Zariski spectrum

Zariski lattice

For proving the Theorem, we give a *realization* of the Zariski lattice, by interpreting $D(a_1, \ldots, a_n)$ as the radical of the ideal $\langle a_1, \ldots, a_n \rangle$

Clearly if $a^N = b_1 v_1 + \cdots + b_m v_m$ then we have $D(a) \leqslant D(b_1, \ldots, b_m)$

The theorem can be seen as a kind of normal form for proofs: any proof of $D(a) \leqslant D(b_1, \ldots, b_m)$ is given by an algebraic equality $a^N = b_1 v_1 + \cdots + b_m v_m$

Zariski lattice

In general the lattice of ideals of R is not distributive

$$\langle X+Y\rangle \cap \langle X,Y\rangle \neq (\langle X+Y\rangle \cap \langle X\rangle) + (\langle X+Y\rangle \cap \langle Y\rangle)$$

However the lattice of radical ideals is distributive

$$\sqrt{\langle a_1,\dots,a_n\rangle} \wedge \sqrt{\langle b_1,\dots,b_m\rangle} = \sqrt{\langle a_1 b_1,\dots,a_n b_m\rangle}$$

$$\sqrt{\langle a_1,\dots,a_n\rangle} \vee \sqrt{\langle b_1,\dots,b_m\rangle} = \sqrt{\langle a_1,\dots,a_n,b_1,\dots,b_m\rangle}$$

If $u^N = \Sigma a_i x_i$ and $u^M = \Sigma b_j y_j$ then $u^{N+M} = \Sigma a_i b_j x_i y_j$

Application 1: Primitive polynomials

In particular, if both $\Sigma a_i X^i$ and $\Sigma b_j X^j$ are primitive we have

$$D(a_0,\dots,a_n) = D(b_0,\dots,b_m) = 1$$

and so, by Gauss-Joyal

$$D(c_0,\dots,c_l) = 1$$

We have an elementary product of two primitive polynomials is primitive, which corresponds to the non effective argument

Logical interpretation

There is always a generic prime filter of this formal space, in a sheaf model (introduction), and we can then eliminate the use of this prime filter

This is a possible interpretation of Hilbert's method of introduction and elimination of ideal elements

Gauss-Joyal

We have only used the relations, and not the fact that the lattice is generated by these relations, so the result applies to $\mathbb{R}$ or to $k[[X]]$ with $D(a)$ being a apart from 0

Gauss-Joyal

In general we do not have

$$\langle a_0, \ldots, a_n\rangle\langle b_0, \ldots, b_m\rangle = \langle c_0, \ldots, c_l\rangle$$

This holds over a Prüfer domain

Constructible topology

The Boolean algebra $B(R)$ generated by the Zariski lattice corresponds to the *constructible topology* $B(R)$

We add new generators $V(a)$ with new axioms

$$V(a) \wedge D(a) = 0 \qquad V(a) \vee D(a) = 1$$

Clearly this associates a Boolean algebra to any ring in a functorial way; any map $R \to S$ defines a map $B(R) \to B(S)$

Classically, we have two topology on the same set of points, which is the set of all prime ideals

Chevalley Theorem and quantifier elimination

The map $B(R) \rightarrow B(R[X])$ has an *adjoint* which defines an existential quantifier

The projection of $V(aX-1)$ is $D(a)$ (read $V(r)$ as $r=0$ and $D(r)$ as $r\neq 0$)

The projection of $V(aX+b)$ is $D(a)\vee V(b)$

This corresponds to both Tarski's quantifier elimination and Chevalley's projection theorem (the projection of a constructible set is constructible)

Chevalley Theorem and quantifier elimination

Chevalley Theorem holds for any finitely presentated extensions: the following map has an adjoint

$$B(R) \to B(R[X_1, \dots, X_n]/\langle p_1, \dots, p_m \rangle)$$

By composition it is enough to show it for $R \to R[X]$ and $R \to R/\langle p \rangle$

Thus Chevalley Theorem can be seen as a refinement of Tarski quantifier elimination

$B(\mathbb{Z}[X_1, \dots, X_n])$ is $S_n(T)$ where T is the theory of algebraically closed fields

Zariski spectrum

Any element of the Zariski lattice is of the form

$$D(a_1,\dots,a_n) = D(a_1) \vee \cdots \vee D(a_n)$$

We have seen that $D(a,b) = D(a+b)$ if $D(ab) = 0$

In general we cannot write $D(a_1,\dots,a_n)$ as $D(a)$ for *one* element a

We can ask: what is the least number m such that *any* element of $\mathsf{Zar}(R)$ can be written on the form $D(a_1,\dots,a_m)$. An answer is given by the following version of *Kronecker's Theorem*: this holds if $\mathsf{Kdim}\ R < m$

Krull dimension

The *Krull dimension* of a ring is defined to be the maximal length of proper chain of prime ideals.

Surprisingly it is possible to define Kdim $R<n$ directly on the Zariski spectrum

We define the boundary of an element a of a lattice: it is the lattice quotiented by the ideal $a \vee \neg a$, which is the ideal containing all $u \vee v$ with $u \leqslant a$ and $v \wedge a = 0$

Then Kdim $L < 0$ iff the lattice is trivial, i.e. $1 = 0$ in L, and Kdim $L<n+1$ iff all boundary lattices have a dimension $< n$

To be 0-dimensional $=$ to be a Boolean lattice

Original statement of Kronecker's theorem

Kronecker (1882) proves a theorem which is now stated in the following way

An algebraic variety in $\mathbb{C}^n$ *is the intersection of* $n+1$ *hypersurfaces*

In particular if R is a polynomial ring $k[X_1, \ldots, X_l]$ then this says that given finitely many polynomials we can find $l+1$ polynomials that have the *same* set of zeros (in an algebraic closure of k)

Forster's Theorem

This concrete proof/algorithm, is *extracted* from R. Heitmann "*Generating non-Noetherian modules efficiently*" Michigan Math. J. 31 (1984), 167-180

If M is a matrix over R we let $\Delta_n(M)$ be the ideal generated by all the $n \times n$ minors of M

Theorem: *Let* M *be a matrix over a commutative ring* R. *If* $\Delta_n(M) = 1$ *and* Kdim $R < n$ *then there exists an unimodular combination of the column vectors of* M

This is a non Noetherian version of Forster's 1964 Theorem

Application 2: GCD domain

Theorem: *If R is a GCD domain then so is $R[X]$*

The Noetherian version of this theorem is that $R[X]$ is UFD if R is UFD

The main Lemma is that if the GCD of the coefficients of $\Sigma a_i X^i$ is 1 and the GCD of the coefficients of $\Sigma b_j X^j$ is 1 then so is the GCD of the coefficients of the product $\Sigma c_k X^K$

This follows from Gauss-Joyal since we have N such that if u divides all c_k then it divides all $a_i^N b_j^N$

Lemma: *In a GCD domain if an element is relatively prime to two elements then it is relatively prime to their product*

References

P. Johnstone *Stone spaces*, Cambridge University Press

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