Algebraic Closure

Thierry Coquand

Preliminary version at May 30, 2000

Introduction

We present a construction of the algebraic closure due to Joyal [Joy75]. We use the notion of entailment relation [CC00, Sco74] to get a simple description of the various Boolean algebras involved.

1 Spectrum of a ring

All rings here are commutative with unit. The first step is to describe in a point-free way the spectrum of a ring A. We define a *notion of zero* to be a map $z : A \to D$ such that

- $z(0) = 1,\ z(1) = 0,$
- $z(x)z(y) \leq z(x+y),$
- $z(xy) = z(x) \vee z(y).$

The intuition is that we describe when an element is 0 modulo a "generic" prime ideal of A. The universal notion of zero on A is a point-free description $z : A \to D(A)$ of the Zariski spectrum of A. $D(A)$ can be described explicitely by the following result [CC00]: we let $X \vdash Y$ where X, Y are finite subsets of A, to mean that the multiplicative monoid generared by Y meets the ideal generated by X.

Theorem 1.1 *$\vdash$ is an entailment relation on A. It is the least entailment relation on A such that:*

$\vdash 0$
$x \vdash xy$
$x, y \vdash x + y$
$1 \vdash$
$xy \vdash x, y$

The boolean algebra generated by $B(A)$ can be similarly described with an entailment relation: we have no two kind of atomic statements a and $\bar{a}$ for $a \in A$ and, for instance $a, b, \bar{c} \vdash d, \bar{e}$ is defined to be $a, b, e \vdash c, d$.

Intuitively a may be read as $a = 0$ while $\bar{a}$ may be read as $a \neq 0$, this modulo a prime ideal.

Thus the picture is that to any ring A we associate a boolean algebra $A \to B(A)$. The natural question is how this boolean algebra varies with A. It is clear that to each morphism

$f : A \to A_1$ corresponds a morphism $\phi_f : B(A) \to B(A_1)$. Furthermore, the theorem above gives an explicit descrition of $B(A)$.

Classically, $B(A)$ is what is called the constructible topology on the set of all prime ideals of A. Constructively it may be impossible to build even one prime ideal of A, but the description above provides an elementary way of describing, without points, the constructible topology. If we let $X(A)$ be the space of primes with the constructible topology, ϕ_f is the inverse image of a continuous map $f^* : X(A_1) \to X(A)$ with $f^*(\beta) = f^{-1}(\beta)$.

2 Finitely Presented Morphisms

This is the key notion here. There are two basic kind of finitely presented morphisms: addition of indeterminate $A \to A[x]$ and quotient by a principal ideal $A \to A/(a)$. Intuitively this can be seen as: addition of new independent quantities or as addition of new relations between the already introduced quantities. In general a finitely presented morphism is a composition of such morphisms.

In each case the corresponding morphism ϕ_f has a left adjoint $\exists_f$ (this is a kind of elimination of quantifiers).

Furthermore in the first case we have $\exists_f(1) = 1$.

In term of points, this means that the map f^* is *open* and in the first case, open surjective.

We state first explicitely two facts that are crucial here

Lemma 2.1 *Let X be a finite subset of A. For $n > 0$*

$$X, a_n x^n + \ldots + a_0 \vdash c, a_n$$

in $A[x]$ iff $X \vdash c, a_n$ in A. Similarly, for any n

$$X \vdash a_n x^n + \ldots + a_0, c, a_n$$

in $A[x]$ iff $X \vdash c, a_n$ in A.

Proof. Both arguments reduce to purely elementary algebraic manipulation. For both arguments, reasoning modulo the ideal generated by X we can suppose $X = \emptyset$.

For the first, we suppose that we have a relation of the form

$$a_n^p c^q = (a_n x^n + \ldots + a_0)(b_m x^m + \ldots + b_0)$$

Such a relation implies directly $a_n^{m-k+1} b_k = 0$ and hence

$$a_n^{p+m+1} c^q = 0$$

For the second assertion, we suppose that we have a relation

$$(a_n x^n + \ldots + a_0)^p c^q a_n^r = 0$$

by looking at the coefficient of x^{np} we find $a_n^{p+r} c^q = 0$ which implies $\vdash c, a_n$ in A. $\square$

If $p(x) = a_n x^n + \ldots + a_0$ we say that a_n is the *leading coefficient* of $p(x)$ and n is the (formal) *degree* $d(p(x))$ of $p(x)$.

Lemma 2.2 *If $p(x), q(x) \in A[x]$ of leading coefficient a, b respectively and $u \in B(A)$ is such that $u \leq [ab \neq 0]$ then there exists a family $u_i \in B(A),\ r_i, s_i \in A,\ a_i(x), b_i(x), c_i(x), d_i(x), g_i(x)$ such that $u \leq \vee u_i \in B(A)$ and $u \leq [r_i s_i \neq 0]$ and $d(c_i(x)) < d(p_i(x))$ and*

$$u_i \leq [a_i(x)p(x) + b_i(x)q(x) = g_i(x)] \wedge [r_i p(x) = c_i(x)g_i(x)] \wedge [s_i q(x) = d_i(x)g_i(x)]$$

Theorem 2.3 *If $f : A \to A'$ is a finitely presented morphism then ϕ_f has a left adjoint $\exists_f$. This means that we have $\exists_f(u) \leq v$ in $B(A)$ iff $u \leq \phi_f(v)$ in $B(A')$.*

This is a purely algebraic way of stating elimination of quantifiers. There is a theorem of Chevalley which states that $f^* : X(A') \to X(A)$ is *open*. We see the connection between this theorem and Tarski's elimination of quantifiers: $\exists_f(u)$ is exactly the open image of the basic open u.

Proof. We analyse the two cases: $A \to A/(a)$ and $A \to A[x]$.

In the first case, let $s : A \to A/(a)$ be the surjection $x \longmapsto x + (a)$. We notice that in this case $B(A/(a)) = B(A)/(\bar{a})$ and ϕ_s is the surjection $\psi : B(A) \to B(A)/(\bar{a})$. But we have $ua \leq v$ iff $\psi(u) \leq \psi(v)$ so that ψ has a left adjoint $\exists_s(\psi(u)) = ua$.

Notice that we have $\exists_s(1) = a$ in this case.

In the second case, for the injection $i : A \to A[x]$, like for elimination of quantifiers, we notice first that any element of $A[x]$ is a disjunction of propositions of the form

$$p_1(x) = 0 \wedge \ldots \wedge p_n(x) = 0 \wedge q(x) \neq 0$$

and we have thus to define

$$\exists x\ (p_1(x) = 0 \wedge \ldots \wedge p_n(x) = 0 \wedge q(x) \neq 0)$$

We notice then that any such conjunction can be written further as a disjunction of statements of the form

$$u \wedge p_1(x) = 0 \wedge \ldots \wedge p_n(x) = 0 \wedge q(x) \neq 0$$

where u is a conjunction of statements of the form $a = 0$ or $a \neq 0$, for $a \in A$, containing at least all assertions that the leading coefficients of p_i, q are $\neq 0$.

There are then two cases. The first case is $n = 0$:

$$\exists x\ [u \wedge q(x) \neq 0]$$

is u by the lemma 2.1.

In general we see that $\exists x\ [a_n x^n + \ldots + a_0 \neq 0]$ is $a_n \neq 0 \vee \ldots \vee a_0 \neq 0$.

We reduce the case $n > 0$ to the case $n = 1$ by dividing successively $p_i(x)$ by one of smallest degree, and we have to define

$$\exists x\ [u' \wedge p(x) = 0 \wedge q(x) \neq 0]$$

where u' is a conjunction of terms containing u, and contains also the assertions that the leading coefficient of $p(x)$ is $\neq 0$. We can then suppose $p(x)$ prime with $q(x)$, otherwise, using lemma 2.2, we can replace $p(x)$ by a polynomial with a smaller degree. But then

$$\exists x\ [u' \wedge p(x) = 0 \wedge q(x) \neq 0]$$

can be defined as

$$\exists x\ [u' \wedge p(x) = 0]$$

By the lemma 2.1 this is u' if $p(x)$ is of the form $a_n x^n + \ldots + a_0$ with $n > 0$ and 0 if $p(x)$ is of the form a_0. $\square$

Acknowledgement

Thanks to Henri Lombardi who explained to me some crucial part in this construction. This work is indeed closely connected to [Lomb96], and it may be interesting to rethink as well the other parts (real closure, valued field closure) of this paper.

References

[CC00] J. Cederquist and Th. Coquand. Entailment Relations and Distributive Lattices. *Proceeding of Logic Colloquium 1998.*

[Joy75] A. Joyal. Le theoreme de Chevalley-Tarski. Cahiers de Topologie et Géometrie Differentielle, 1975.

[Lomb96] H. Lombardi. Coste Roy Dynamical Methods in Algebras. to appear, 2000.

[Sco74] D. Scott. Completeness and axiomatizability. *Proceedings of the Tarski Symposium*, pages 411–435, 1974.