Infinite objects in constructive mathematics

Thierry Coquand

May 7 2007

Content of the tutorial

Lecture I: Hilbert's program, prime ideals, Zariski spectrum, Alaoglu (unit ball for the weak* topology), Hahn-Banach, spectrum of an lattice ordered group

Lecture II: Stone-Yosida representation theorem, Prüfer ring, space of valuations, Riemann surfaces, cohomological definition of the genus of a curve

formal space = distributive lattice (almost)

Hilbert's program

In mathematics, success of non effective methods to prove concrete statements

concrete: existence of a "finitary" object satisfying a decidable property

Hilbert's program

Examples: Dirichlet Theorem proved with complex analysis, or

Theorem (Krivine): *If* $P \in \mathbb{Q}[x_1, \ldots, x_k]$ *is* > 0 *on* $[0,1]^n$ *then it can be written as a polynomial in* $x_i, 1 - x_i$ *with rational* positive *coefficients*

This is also proved with the Axiom of Choice

It is not true if P is only ≥ 0: take $(2x-1)^2$

(but it works for $(2x-1)^2 + \epsilon$ if $\epsilon > 0$)

Hilbert's program

Whenever we use "ideal methods" to prove a concrete statement we should be able to explain the use of these ideal methods and replace this argument by a proof which has a direct algorithmic content

In particular, if we prove the existence of an object, this proof should give us a way to find this object

"ideal methods": Axiom of Choice, prime ideals

Analogy with physics

Prime ideals were introduced by Kummer by analogy with chemistry

"These ideal complex numbers are comparable to hypothetical radicals that do not exist by themselves, but only in their combinations."

Kummer gave then an example of an element that, at the time, existed only hypothetically comparable to a prime ideal (this element was isolated later)

We describe the elements/atoms (points) by their *observable properties*

They should be thought of as *symbols*

Formal topology

Formal topology gives a way to precise the status of infinite/ideal objects in constructive mathematics

Ideal objects form a formal space

This space is described as the logical theory of the observable properties of these infinite objects; generalisation of domain theory

Zariski spectrum

R commutative ring

The prime filters (classically complement of prime ideals) may be very difficult to build (prime factorisation), but it is simple to describe their logical theory of "observable" properties

Joyal's definition: free distributive lattice generators $D(a)$, thought of as a pure symbols, and relations

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

Zariski spectrum

We have a *complete* description of this free lattice: this is the lattice of radical of finitely generated ideals; we write $D(a_1, \ldots, a_n)$ for $D(a_1) \vee \cdots \vee D(a_n)$

It is *always* a distributive lattice; the product is also the intersection

In general the lattice of (finitely generated) ideals of a ring is *not* distributive: take in $\mathbb{Z}[X, Y]$ the ideals $<X>, <Y>$ and $<X + Y>$

A ring is *arithmetical* iff its lattice of ideals is distributive

Zariski spectrum, application

Gauss-Joyal identity: $D(a_1, \ldots, a_n) \wedge D(b_1, \ldots, b_m) = D(c_1, \ldots, c_l)$ if $(\Sigma a_i X^i)(\Sigma b_j X^j) = \Sigma c_k X^k$

Application: the product of primitive polynomials (ideal of coefficient is 1) if primitive

More generally $c(PQ) = c(P)c(Q)$ if $c(a_0 + \cdots + a_n X^n) = D(a_0, \ldots, a_n)$

Other applications: Krull dimension, basic theory of finitely generated projective modules (Serre 1958)

Topological space

Classically the Zariski spectrum is the *set* of prime ideals with basic open

$D(a)$ set of ideals which do *not* contain a

This is a space which is *not* Haussdorf in general

Introduced by Zariski; Serre showed it can be used for cohomology; used for *arbitrary* rings by Grothendieck

Points

A point of a lattice L is classically a lattice map $Sp(L) = L \to 2$

Any map $f : L_1 \to L_2$ defines by composition $f^* : Sp(L_2) \to Sp(L_1)$ $f^*(\phi) = \phi f$

We *do not* get in this way all continuous maps $Sp(L_2) \to Sp(L_1)$

Theorem: f^* *is* surjective *iff* f *is conservative, i.e.* $a \leq b$ *iff* $f(a) \leq f(b)$

Thus *extension* theorems becomes formally *conservativity* results

Hahn-Banach (Mulvey)

We consider a $\mathbb{Q}$-vector space E

Normable in the following sense: we have subsets $N(r)$ for r rational > 0 (intuitively $x \in N(r)$ iff $|x| < r$, but $|x|$ is not a Dedekind real)

The axioms are

$\exists r > 0. x \in N(r), \quad x \in N(r) \to \exists s < r. x \in N(s)$

$0 \in N(r), \quad x \in N(r) \to -x \in N(r)$

$x \in N(r) \wedge y \in N(s) \to x + y \in N(r + s)$

Hahn-Banach

Free distributive lattice $W(E)$ with generators $[u(x) < r]$, symbols with relations

$$[u(x+y) < r+s] \leq [u(x) < r] \vee [u(y) < s]$$

$$[u(x) < r] \wedge [u(-x) < -r] = 0$$

$[u(x) < r] = 1$ if $x \in N(r)$

We can then prove in this theory

$$[u(x) < r] \wedge [u(y) < s] \leq [u(x+y) < r+s]$$

Hahn-Banach

Theorem: *If* $E_1 \subseteq E_2$ *then the map* $W(E_1) \to W(E_2)$ *is* conservative

This is a simple consequence of the following result

Lemma: $\wedge[u(x_i) < r_i] \leq \vee[u(y_j) < s_j]$ *iff there exists rationals* $a_i, b_j \geq 0$ *such that* $\Sigma a_i x_i = \Sigma b_j y_j$ *and* $\Sigma a_i r_i \leq \Sigma b_j s_j$ *and* $\Sigma b_j > 0$

From lattices to compact regular spaces

To get the formal space $Fn(E)$ of the unit ball for the weak* topology we need to add the further (infinitary) condition

$$[u(x) < r] = \bigvee_{s<r} [u(x) < s]$$

(We then restrict the space to the *maximal* points)

Definition: *A lattice is* normal *iff whenever* $a \vee b = 1$ *there exists* x, y *such that* $x \wedge y = 0,\ a \vee x = b \vee y = 1$. *A lattice is* strongly normal *iff for any* a, b *there exists* x, y *such that* $a \leq b \vee x$ *and* $b \leq a \vee y$

Lemma: *A strongly normal lattice is normal*

From lattices to compact regular spaces

Proposition: *The lattice $W(E)$ is strongly normal*

Enough to check the condition on generators of the lattice

Any normal lattice defines a compact regular space in a canonical way. If we apply this construction to $W(E)$ we get the space $Fn(E)$

Corollary: *If $E_1 \subseteq E_2$ then the map $Fn(E_1) \to Fn(E_2)$ is* conservative

This is the formal version of Hahn-Banach

Geometric Hahn-Banach

K totally bounded subset of E

Theorem: *If we have in the theory* $Fn(E)$ *that* $[u(x) < r] \leq \vee_{y \in K}[u(y) < r]$ *then* x *belongs to the compact convex hull of* K

This is the formal version of a geometrical form of Hahn-Banach's Theorem

Lattice group

Assume that the vector space E is an ordered space which is a lattice (automatically distributive) and that it contains a special element 1 which is a *strong unit*: for all $a \in E$, there exists n such that $a \leq n.1$

Then we can define $N(r)$

We can define the space of integrals $I(E)$: points of $Fn(E)$ such that $u(1) = 1$

We can replace $u(a) < r$ by $0 < u(r.1 - a)$.

Generators $I(a)$ and relations $I(a) = 0$ if $a \leq 0$ and

$I(a) \wedge I(-a) = 0, \quad I(a + b) \leq I(a) \vee I(b), \qquad I(1) = 1$

Spectrum of a lattice group

We take the generators $D(a)$ and same relations

$D(a) = 0$ if $a \leq 0$

$D(a) \wedge D(-a) = 0, \quad D(a+b) \leq D(a) \vee D(b), \qquad D(1) = 1$

We get a strongly normal lattice $Sp(E)$

We add the relation $D(a) = \vee_{r>0} D(a-r)$

We get a compact space $X = Sp_r(E)$. The space $I(E)$ can be thought of as the space of probability measure on X

Spectrum of a lattice group

We have a complete description of $Sp(E)$

We take the set P elements that are ≥ 0 in E

We define the new relations $a \leq' b$ iff there exists n such that $a \leq n.b$

P for this relation is a distributive lattice, and this is a concrete description of $Sp(E)$

Corollary: *We have $D(a) = 1$ in $Sp(E)$ iff there exists n such that $1 \leq na$.*