Point-free topology and constructive mathematics

Original idea in de Bruijn, van der Meiden

"Notes on Gelfand's theory." Indag. Math. 29, 1967

A proof of Wiener's theorem on absolutely convergent Fourier series which is independent of Zorn's lemma

Instead of working with maximal ideals, it is enough to work with "large enough" ideals

The proof has the same structure as the classical proof

Point-free topology and constructive mathematics

"De Bruijn's suggestion was inspired by an old idea outlined already in Menger Dimensionstheorie in 1928, ...; this promising topology without points, which did not find applications until now, appears to provide an appropriate setting for discussion of Gelfand's theory."

Replace points by suitable approximations, that can be thought of as basic open sets

(using ideas from Bishop it is actually possible to write an algorithm for computing the inverse, see

The Wiener lemma and certain of its generalizations. Bull. Amer. Math. Soc. (N.S.) 24 (1991), no. 1, 1–9.)

Logic

Instead of working with *points* (ideal objects) we work with finitary (concrete) objects, the *basic open*, that can be thought of as partial amount of information about the points

One can describe directly the *logic* of these partial informations. This description can be done in a weak metalogic.

Systematic way of associating propositional logics (distributive lattices) to algebraic structure

Prime Spectrum

Basic example: due to Lawvere/Joyal

If R commutative ring with unit, the basic open are

$$D(a) = \{\alpha \mid a \notin \alpha\}$$

The propositional theory is

- $D(0) \vdash$
- $\vdash D(1)$
- $D(a+b) \vdash D(a), D(b)$
- $D(a), D(b) \vdash D(ab)$
- $D(ab) \vdash D(a)$

Prime Spectrum

Main Theorem: (Krull's theorem)

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

iff the ideal generated by the b_j *meets* the mutiplicative monoid generated by the a_i

The proof can be done in a weak metalogic, and is best presented using the notion of *entailment relation* due to Dana Scott

A relation $\Pi a_i^{k_i} = \Sigma r_j b_j$ can be seen as a *proof certificate* of the entailment $D(a_1), \ldots, D(a_m) \vdash D(b_1), \ldots, D(b_n)$

We never need to build effectively points (prime ideal) but we can reason about them

Prime Spectrum

This is a formal version of Hilbert's Nullstellensatz

cf. Lifschitz, Vladimir Semantical completeness theorems in logic and algebra. Proc. Amer. Math. Soc. 79 (1980), no. 1, 89–96

Algebraic identity comes from an abstract proof

Can be seen as a completness theorem, but here we never try to build effectively models

Semantics/Syntax

Existence = non contradiction

This viewpoint originates from algebra Kronecker(?) $\rightarrow$ Drach (1895)

For instance, we may want to add symbols $x_1, \ldots, x_n$ with the constraints

$$f_1(x_1, \ldots, x_n) = \ldots = f_k(x_1, \ldots, x_n) = 0$$

The theory is inconsistent iff $1 \in (f_1, \ldots, f_k)$

For instance the following theory is always consistent (Drach's formulation of Galois theory)

$$x_1 + x_2 + x_3 - a = x_1x_2 + x_2x_3 + x_3x_1 - b = x_1x_2x_3 - c = 0$$

Ordered Group

Let $R, \leq$ be an preordered group

The theory is

- $D(a+b) \vdash D(a), D(b)$
- $D(a), D(-a) \vdash$
- $D(a) \vdash$ if $a \leq 0$

One can prove $D(a), D(b) \vdash D(a+b)$

Prime Spectrum

Main Theorem:

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

iff a nonempty sum of some a_i is equal to a sum of b_j

Such a relation can be seen as a *proof certificate* of the entailment $D(a_1), \ldots, D(a_m) \vdash D(b_1), \ldots, D(b_n)$

A point (model of the propositional theory) is here a total preordering that extends the given order relation

Fundamental in measure theory, Hahn-Banach

Valuation

If K is a field, a valuation ring is a subring A such that for all $x \neq 0$ we have $x \in A$ or $x^{-1} \in A$

The atoms are $D(a)$ for a nonzero

The theory is

- $\vdash D(a), D(b)$ if $ab = a + b$
- $\vdash D(a), D(a^{-1})$
- $D(a) \vdash D(-a)$
- $D(a), D(b) \vdash D(ab)$

Valuation

Main Theorem:

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

iff we have $\Sigma b_j^{-1} q_j$ for some polynomials $q_j(a_1, \ldots, a_n, b_1^{-1}, \ldots, b_m^{-1})$

In particular

$$D(a_1), \ldots, D(a_m) \vdash D(b)$$

iff b is integral over $a_1, \ldots, a_m$

Valuation

This can be used to show the following theorem of Kronecker

Theorem: If $c_k = \Sigma_{i+j=k} a_i b_j$ then each $a_i b_j$ is integral over $c_0, \ldots, c_{n+m}$

For instance with $n = m = 2$ we have that $a_0 b_1$ is integral over $c_0, \ldots, c_4$

$(a_0 b_1)^6 = p_1 (a_0 b_1)^5 + p_2 (a_0 b_1)^4 + p_3 (a_0 b_1)^3 + p_4 (a_0 b_1)^2 + p_5 (a_0 b_1) + p_6$

where

$$p_1 = 3c_1, \quad p_2 = -3c_1^2 - 2c_0 c_2, \quad p_3 = c_1^3 + 4c_0 c_1 c_2$$

$$p_4 = -c_0^2 c_1 c_3 - 2c_0 c_1^2 c_2 - c_0^2 c_2^2 + 4c_0^3 c_4$$

$$p_5 = c_0^2 c_1^2 c_3 + c_0^2 c_1 c_2^2 - 4c_0^3 c_1 c_4 \qquad p_6 = -c_0^3 c_1 c_2 c_3 + c_0^4 c_3^2 + c_0^3 c_1^2 c_4$$

l-group

Fundamental structure (Dedekind, Riesz, Stone)

The theory is

- $D(a+b) \vdash D(a), D(b)$
- $D(a \vee b) \vdash D(a), D(b)$
- $D(a), D(-a) \vdash$
- $D(a) \vdash$ if $a \leq 0$

One defines as usual $a^+ = a \vee 0$

Prime Spectrum

Main Theorem:

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

iff $a_1^+ \wedge \ldots \wedge a_m^+ \leq N(b_1^+ \vee \ldots \vee b_n^+)$ for some N

Spectral theorems of self-adjoint operators

Ordered Ring

Also fundamental structure (Stone), the positive elements $P \subseteq R$ satisfy

$$P + P \subseteq P, \quad P.P \subseteq P, \quad x^2 \in P$$

The theory is

- $D(a+b) \vdash D(a), D(b)$
- $D(a), D(-a) \vdash$
- $D(a) \vdash$ if $a \leq 0$
- $\vdash D(1)$
- $D(a), D(b) \vdash D(ab)$
- $D(ab) \vdash D(a), D(-b)$

Prime Spectrum

Main Theorem: (formal Positivstellensatz)

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

iff we have a relation $m + p = 0$ where m is in the multiplicative monoid generated by a_i and p is in the positive cone generated by $a_i, -b_j$

The points are the total preorder that extends the given order

This space is called the *real spectrum*

Corollary: We have $\vdash D(a)$ iff $r \leq a$ for some rational $r > 0$

Lemma: (Krivine) If $at = 1 + t_1$ with $t, t_1 \geq 0$ then $a \geq r$ for some $r > 0$

Compact Hausdorff Spaces

So far we have only looked at *spectral spaces*, spaces of *prime* ideals

It is remarkable that we can give a logical description of compact Hausdorff spaces such as the space of *maximal* ideals

In several cases, the spectral spaces are *normal*: any prime is contained in a *unique* maximal ideal

In this case the lattice is enough to describe the space of *maximal* ideals

Archimedian Ordered Ring

Suppose that R is archimedian and contain a copy of $\mathbb{Q}$ with $\mathbb{Q}^+ \subseteq P$

The maximal ideals of R correspond to the model of $Max(R)$

- $D(a+b) \vdash D(a), D(b)$
- $D(a), D(-a) \vdash$
- $D(a) \vdash$ if $a \leq 0$
- $\vdash D(1)$
- $D(a), D(b) \vdash D(ab)$
- $D(ab) \vdash D(a), D(-b)$
- $D(a) \vdash \bigvee_{r>0} D(a-r)$

Archimedian Ordered Ring

The models of $Max(R)$ can be seen as maps $\phi : R \to \mathbb{R}$ such that $\phi(a) \geq 0$ if $a \geq 0$

Theorem: The map $D(a) \longmapsto \bigvee_{r>0} D(a-r)$ is an *interpretation* of the theory $Max(R)$ in the theory $Sp(R)$

Theorem: We have $\vdash D(a)$ iff $r \leq a$ for some rational $r > 0$

This can be interpreted as saying that the map $R \to C(Max(R))$

$$a \longmapsto (\phi \longmapsto \phi(a))$$

preserves the norm (Gelfand duality theorem)

Archimedian Ordered Ring

In this way, we get constructive proofs (= algorithms) for the following theorems

Theorem: (Schmüdgen) If we have $f, h_1, \dots, h_k \in \mathbb{Q}[X_1, \dots, X_n]$ such that

$$W = \{u \in \mathbb{R}^n \mid h_1(u) \geq 0, \dots, h_k(u) \geq 0\}$$

is bounded and if $f(u) > 0$ for $u \in W$ then f belongs to the positive cone generated by $h_1, \dots, h_k$

We consider the ordering on $R = \mathbb{Q}(x_1, \dots, x_n)$ generated by the conditions $h_i \geq 0$

The space defined by $Max(R)$ is W

Example

Lemma: For any n we can write $x^2 + 1 = P(n - x, n + x)$ where $P(X, Y)$ has all its coefficients ≥ 0

Theorem: (Krivine) If we have $f(u) > 0$ for all $u \in [0, 1]^n$ we can write $f = P(x_1, \ldots, x_n, 1 - x_1, \ldots, 1 - x_n)$ where all the coefficients of P are ≥ 0.

We consider the ordering on $R = \mathbb{Q}(x_1, \ldots, x_n)$ generated by the conditions $x_i \geq 0, 1 \geq x_i$

The space defined by $Max(R)$ is $[0, 1]^n$

We have $\vdash D(f)$ in the theory $Max(R)$

Spectral Theorem

Another example of application is given by the *spectral theorem*

R is a commutative ring of auto-adjoint operators

$A \geq 0$ means $(Ax, x) \geq 0$ for all x

Main Lemma: (Riesz) If $A, B \geq 0$ then $AB = BA \geq 0$

The spectral theorem says that we can think of the elements of R as continuous functions on the compact Hausdorff space $Max(R)$

Fourier Analysis

(Inspired by Bas Spitters thesis, february 2003)

For instance if G compact group with $I : C(G) \to \mathbb{C}$ Haar measure

$$I(f) = \int f(x)dx$$

We have the convolution product on $C(G)$

$$(f \times g)(y) = \int f(x)g(x^{-1}y)dx$$

and scalar product

$$(f, g) = \int f(x)\overline{g(x)}dx$$

Fourier Analysis

We define from this a ring R of operators

The space $Max(R)$ is the space of *characters* over G

$f \geq 0$ means $(f \times g, g) \geq 0$ for all g

It is *discrete*: there is a proof using dependent choices and I conjecture that dependent choice is needed

Further work to be done: it can be proved that if two ≥ 0 continuous functions have a l.u.b. that is continuous

Thus we have also an l-group structure (Krein 1941)

Conclusion

Systematic way to rewrite basic parts of algebra and functional analysis

Even classically, this formulation is sharper than the usual one: weak metatheory and the statements are *absolute*

Dependent choices/non canonical choices are needed only if one wants to build points effectively

In a point-free setting, dependent choice is not needed

Conclusion

When possible, the algorithms corresponding to point-free proofs are better (=feasible??)

For instance in algebra, we don't require explicit decomposition in primes, we can do *as if* there is one

Typical example: x^2 divides y^2 implies x divides y

The "point-free proof" (Riesz space) is feasible

Lemma: In a l-group $2x \leq 2y$ implies $x \leq y$

This does not require to have the complete decomposition in primes: we need only the gcd operation $x \wedge y$

Related Work

J. Avigad "Forcing in proof theory" at http://www.andrew.cmu.edu/~avigad/

M. Coste, H. Lombardi,M.F. Roy " Dynamical method in algebra: effective Nullstellenstze." Ann. Pure Appl. Logic 111 (2001), no. 3, 203–256.

L. Ducos, H. Lombardi, C. Quitte, M. Salou "Théorie algorithmique des anneaux arithmtíques, de Prüfer et de Dedekind " Preprint

H. Lombardi "Hidden constructions in abstract algebra (3) Krull dimension of distributive lattices and commutative rings" in Lecture notes in pure and applied mathematics vol 131. M. Dekker. (2002) pp. 477-499.