Dynamical Methods in Algebra

We present a possible realisation of *Hilbert's program* for (some part of) *abstract algebra*

Gödel's incompleteness theorem shows that there are abstract methods (like use of analytical methods to prove results in number theory) that cannot be eliminated

Surprisingly this is *not* the case for abstract algebra

Examples

If a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ *is* ≥ 0 *on* $\mathbb{R}^n$ *then it can be written as sum of square of rational functions*

(Artin, 1926, solving Hilbert 17th problem)

If a polynomial in $\mathbb{Q}[X_1, \ldots, X_n]$ *is* > 0 *on* $[0, 1]^n$ *then it can be written as a polynomial in* $X_i, 1 - X_i$ *with rational* positive *coefficents*

(Krivine, 1964)

In both cases the proofs are elegant but *non effective* (use of Zorn's lemma)

Can we use these proofs to compute the witnesses??

Dynamical Methods in Algebra

The solution I will present is based on

Coste M., Lombardi H., Roy M.F. “Dynamical method in algebra: Effective Nullstellensätze” J.P.A.A. 155 (2001)

which is inspired from the *computer algebra system* D5

Della Dora J., Dicrescenzo C, Duval D. “About a new method for computing in algebraic number fields” EUROCAL 85, LNCS 204, 1985

Furthermore, the main technique may be seen as a simple case of the *tableau method*

Hilbert's program in Algebra

existence of ideal objects	*non contradiction* of logical theory
ideal objects	logical theory of *finite approximations* (*)
semantics	*syntax*

(*) an idea that one finds also in domain theory

Some of these ideas, usually connected to Hilbert, seem to be present earlier in algebra, at least explicitely in the work of Drach, 1895, and maybe earlier in Kronecker

Example: prime ideals

If R commutative ring, an ideal I of R is *prime* iff

$$xy \in I \ \rightarrow \ [x \in I \vee y \in I]$$

iff the quotient ring R/I is an integral domain

Theorem: (Krull) *the intersection of all prime ideals is precisely the set of* nilpotent *elements*

where $x \in R$ is nilpotent iff there exists n such that $x^n = 0$

In particular any non trivial ring has at least one prime ideal

It may be impossible to build such an ideal effectively

Example

If a polynomial $P \in R[X]$ is nilpotent then all its coefficients are nilpotent

(This is a simple exercice in Atiyah-MacDonald)

For instance if $(a_2X^2 + a_1X^1 + a_0)^{17} = 0$ then there exists n_2, n_1, n_0 such that $a_2^{n_2} = a_1^{n_1} = a_0^{n_0} = 0$

The proof is easy with Krull's theorem: if I is prime then we should have $a_2 = a_1 = a_0 = 0$ $(mod.I)$

What are n_2? n_1? n_0?

Is it *at all* possible to compute n_1 from this argument, which is based on objects that may fail to exist effectively??

Logic

Instead of working with ideal objects (here prime ideals) we work with finitary concrete objects

Each of this object can be thought of as partial amount of information about the ideal object

One can describe directly the *logic* of these partial informations, and this description can be done in a weak metalogic

Prime Spectrum

If R commutative ring with unit, the finite informations are atomic formulae $Z(x)$, which means intuitively $x \in I$

We get a *propositional theory*

1. $\rightarrow Z(0)$
2. $Z(1) \rightarrow$
3. $Z(x) \wedge Z(y) \rightarrow Z(x+y)$
4. $Z(x) \rightarrow Z(xy)$
5. $Z(xy) \rightarrow Z(x) \vee Z(y)$

Propositional geometrical logic

All axioms have a simple form, known in logic as “geometrical”

Atomic formulae $F, F_1, \ldots$ will be called *facts*

Geometrical axioms are of the form

$$C \rightarrow C_1 \vee \ldots \vee C_n$$

where $C, C_1, \ldots, C_n$ are conjunctions of facts

One can have $n = 1$ and an axiom of the form $C \rightarrow F$ *Horn formula*

One can have $n = 0$ the axiom is $C \rightarrow \perp$ (written $C \rightarrow$)

The conjunction C may be empty; the axiom has the form
$T \rightarrow C_1 \vee \ldots \vee C_n$ (written $\rightarrow C_1 \vee \ldots \vee C_n$)

The Method of Trees

A natural generalisation of the “closure” of a list of facts by a theory of Horn clauses

Since some axioms are not Horn clauses we may have to do a branching

Each branch represents a list of facts

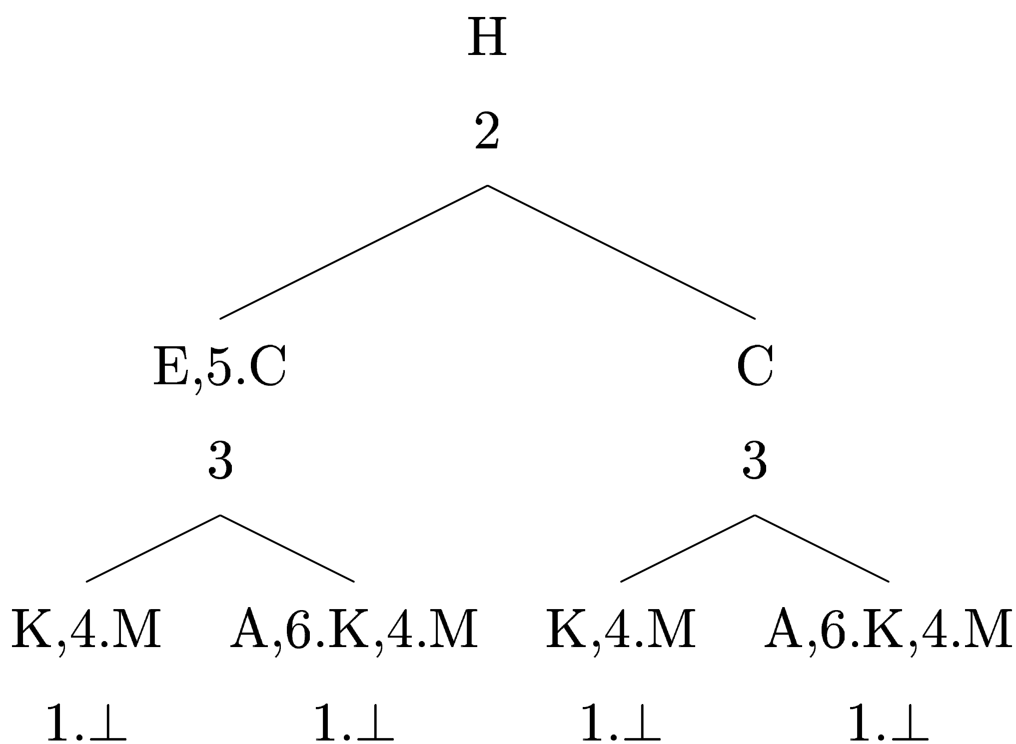
A branch *collapses* if it proves $\perp$

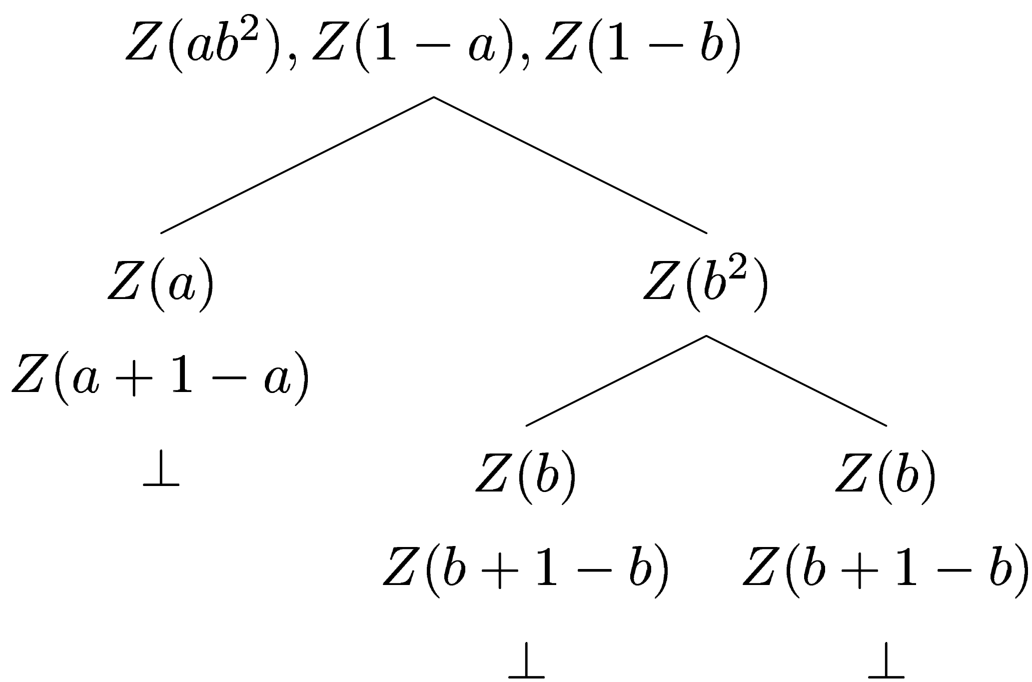
Each axiom is seen as a *rule* to infer new facts

We may have to open different branches and a branch may collapse

Branch = partial model/attempt to build a model of the theory

1	$M \wedge C \rightarrow$
2	$\rightarrow E \vee C$
3	$H \rightarrow K \vee A$
4	$C \wedge K \rightarrow M$
5	$H \wedge E \rightarrow C$
6	$A \rightarrow K$





$$Z(ab^2) \wedge Z(1-a) \wedge Z(1-b) \rightarrow$$

$$\boxed{\begin{array}{c} 1 \in (ab^2, 1-a, 1-b) \\ 1 = ab^2 + b^2(1-a) + (1+b)(1-b) \end{array}}$$

Theorem: (formal Nullstellensatz) *In the theory*

1. $\to Z(0)$
2. $Z(1) \to$
3. $Z(x) \wedge Z(y) \to Z(x+y)$
4. $Z(x) \to Z(xy)$
5. $Z(xy) \to Z(x) \vee Z(y)$

the collection of facts $Z(a_1), \ldots, Z(a_n)$ *is contradictory iff* $1 \in (a_1, \ldots, a_n)$

Tree induction

The proof is direct and elementary: by *tree induction* from any tree derivation of $\perp$ from $Z(a_1), \ldots, Z(a_n)$ we can build an algebraic certificate $1 = a_1u_1 + \ldots + a_nu_n$

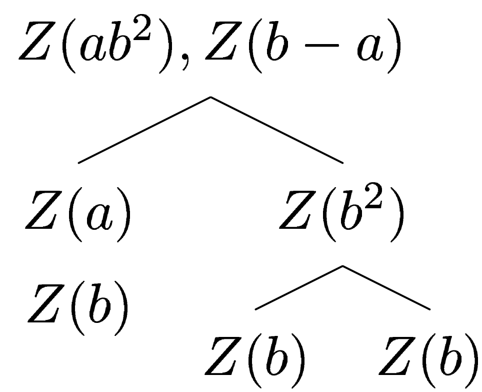
Tree induction proceeds from the leaves to the top of the tree

$$1 = b + (1 - b)$$

$$1 = b^2 + (1 + b)(1 - b)$$

$$1 = a + (1 - a)$$

$$1 = ab^2 + b^2(1 - a) + (1 + b)(1 - b)$$



$$Z(ab^2) \wedge Z(b-a) \rightarrow Z(b) \qquad\qquad (*)$$

$$\boxed{\begin{array}{c} b^3 \in (ab^2, b-a) \\ b^3 = ab^2 + b^2(b-a) \end{array}}$$

This algebraic identity can be seen as a *proof certificate* of the implication $(*)$ in the theory of prime ideals

$$Z(ab^2), Z(1-a), Z(ba+b-a)$$

$$\begin{array}{ccc} Z(a) & & Z(b^2) \\ Z(1) & Z(b) & Z(b) \\ \perp & Z(ba+b-a-ba) & Z(b-a) \end{array}$$

$$Z(ab^2) \wedge Z(1-a) \wedge Z(ba+b-a) \to Z(b-a)$$

$$\boxed{\begin{array}{c} (b-a)^2 \in (ab^2, 1-a, ba+b-a) \\ (b-a)^2 = (b-a)^2(1-a) + a^2ab^2 + a(b-a-ba)(ba+b-a) \end{array}}$$

Theorem: (formal Nullstellensatz) *In the theory*

1. $\rightarrow Z(0)$
2. $Z(1) \rightarrow$
3. $Z(x) \wedge Z(y) \rightarrow Z(x+y)$
4. $Z(x) \rightarrow Z(xy)$
5. $Z(xy) \rightarrow Z(x) \vee Z(y)$

$Z(b)$ *is derivable from the collection of facts* $Z(a_1), \ldots, Z(a_n)$ *iff some power of* b *is in* $(a_1, \ldots, a_n)$

In particular $Z(b)$ is derivable iff b is nilpotent!

Remark: $Z(b)$ is derivable from the collection of facts $Z(a_1), \ldots, Z(a_n)$ from the rules $1, 3, 4$ iff b is in $(a_1, \ldots, a_n)$

Elimination of ideal elements

If $(a_2X^2 + a_1X + a_0)^{17} = 0$ for proving that a_1 is nilpotent: instead of taking

$I =$ an arbitrary *prime* ideal

we take

$I =$ the ideal of all nilpotent elements

This is a good enough approximation for this argument: we show (constructively) that $a_2 \in I$ and hence $a_1 \in I$

Semantics/Syntax

Existence = non contradiction of a theory

This viewpoint originates from algebra: Drach (1895) and maybe earlier in Kronecker's work

For instance, we may want to add new 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

$$x_1 + x_2 + x_3 - a = x_1 x_2 + x_2 x_3 + x_3 x_1 - b = x_1 x_2 x_3 - c = 0$$

which shows the formal existence of the splitting field of the equation $x^3 - ax^2 + bx - c = 0$

Ordered Group

The same method works for most of simple abstract arguments in algebra that uses Zorn's lemma

Let $R, \leq$ be an abelian preordered group

The theory of total ordering is

- $P(a) \wedge P(b) \rightarrow P(a+b)$
- $\rightarrow P(a) \vee P(-a)$
- $\rightarrow P(a)$ if $0 \leq a$

Ordered Group

Theorem: *The implication*

$$P(a_1) \wedge \ldots \wedge P(a_n) \rightarrow P(b)$$

holds iff some multiple of b *is* $\geq$ *a sum of* a_i

Corollary: $P(b)$ *is derivable iff some multiple of* b *is* ≥ 0

Non constructively this corresponds to the fact that $0 \leq b$ in *all* total extensions of the preordering iff some multiple of b is positive

This is known as Lorenzen-Dieudonné realisation theorem

Dieudonné, J. "Sur la théorie de la divisibilité" Bull. Soc. Math. France 69, (1941)

This is related to well-known theorems in linear programming over $\mathbb{Q}$ (variant of Farkas' lemma)

Valuation

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

The atoms are $V(x)$, meaning $x \in R$

The theory is

- $V(x) \wedge V(y) \rightarrow V(x+y) \wedge V(xy)$
- $\rightarrow V(x) \vee V(x^{-1})$ if $x \neq 0$

Theorem: *The implication*

$$V(a_1) \wedge \ldots \wedge V(a_n) \rightarrow V(a)$$

holds iff a is integral over $a_1, \ldots, a_m$

Valuation

Application: *If* $z_k = \Sigma_{i+j=k} x_i y_j$ *then each* $x_i y_j$ *is integral over* $z_0, \ldots, z_{n+m}$

For instance with $n = m = 2$ a proof certificate of

$$V(z_0) \wedge \ldots \wedge V(z_4) \to V(x_0 y_1)$$

is

$$(x_0y_1)^6 = p_1(x_0y_1)^5 + p_2(x_0y_1)^4 + p_3(x_0y_1)^3 + p_4(x_0y_1)^2 + p_5(x_0y_1) + p_6$$

where

$$p_1 = 3z_1, \quad p_2 = -3z_1^2 - 2z_0z_2, \quad p_3 = z_1^3 + 4z_0z_1z_2$$

$$p_4 = -z_0^2z_1z_3 - 2z_0z_1^2z_2 - z_0^2z_2^2 + 4z_0^3z_4$$

$$p_5 = z_0^2z_1^2z_3 + z_0^2z_1z_2^2 - 4z_0^3z_1z_4 \qquad p_6 = -z_0^3z_1z_2z_3 + z_0^4z_3^2 + z_0^3z_1^2z_4$$

This is known as *Kronecker's theorem*

Geometrical first-order logic

So far only propositional logic

A *geometric formula* is the form

$$C \to (\exists \vec{u_1}) C_1(\vec{u_1}) \vee \ldots \vee (\exists \vec{u_n}) C_1(\vec{u_n})$$

Example: Axiom of *field*; the atomic formulae are now of the form $Z(t)$ with $t \in \mathbb{Z}[x_1, \ldots, x_n]$

$$\to Z(x) \vee \exists y. Z(xy - 1)$$

Intuitively, we can open two branches: in one branch we add the fact $a = 0$, in the other branch we introduce a new variable y and the fact $ay = 1$

Geometrical first-order logic

Axiom schema of *algebraic closure*

$$\exists x. Z(x^n + x_{n-1}x^{n-1} + \ldots + x_0)$$

We can introduce new indeterminates submitted to some constraints (like in Kronecker/Gauss use of indeterminates)

We can extend in a natural way the *Method of Trees* to this case

Theorem: *In the theory*

1. $\rightarrow Z(0)$
2. $Z(1) \rightarrow$
3. $Z(x) \wedge Z(y) \rightarrow Z(x+y)$
4. $Z(x) \rightarrow Z(xy)$
5. $Z(xy) \rightarrow Z(x) \vee Z(y)$
6. $\rightarrow Z(x) \vee \exists y. Z(xy-1)$

$Z(b)$ *is derivable from the collection of facts* $Z(a_1), \ldots, Z(a_n)$ *iff some power of* b *is in* $(a_1, \ldots, a_n)$

Notice that in these clauses, x, y are now *first-order* variables, that are implicitely universally quantified

Form of the trees

To each branch of the tree is associated a *finitely presented rings* and hence a finite set of equations $p_1 = \ldots = p_m = 0$ $p_j \in \mathbb{Z}[X_1, \ldots, X_n]$

In the theory of ordered fields to each branch is associated a system of *sign conditions*: $p_j > 0$ or $p_j = 0$

$$Z(a-b+c), Z(ab), Z(b^2-c)$$

$$\begin{array}{cc}
Z(a) & Z(ax-1) \\
Z(b-c) & Z(b) \\
 & Z(b^2) \\
 & Z(c) \\
 & Z(b-c)
\end{array}$$

$$Z(a-b+c) \wedge Z(ab) \wedge Z(b^2-c) \rightarrow Z(b-c)$$

$$\boxed{\begin{array}{c} (b-c)^2 \in (a+b-c, ab, b^2-c) \\ (b-c)^2 = (a+b-c)(b-c) + ab(b-1) + (b^2-c)(-a) \end{array}}$$

Theorem: (formal existence of algebraic closure) *In the theory*

1. $\rightarrow Z(0)$
2. $Z(1) \rightarrow$
3. $Z(x) \wedge Z(y) \rightarrow Z(x+y)$
4. $Z(x) \rightarrow Z(xy)$
5. $Z(xy) \rightarrow Z(x) \vee Z(y)$
6. $\rightarrow Z(x) \vee \exists y. Z(xy-1)$
7. $\rightarrow \exists x. Z(x^n + x_{n-1}x^{n-1} + \ldots + x_0)$

$Z(b)$ *is derivable from the collection of facts* $Z(a_1), \ldots, Z(a_n)$ *iff some power of* b *is in* $(a_1, \ldots, a_n)$

Geometrical first-order logic

One can present the theory of real closed field, algebraically closed valued fields, differentially closed fields ... in this way

This provides a beginning of explanation of computation in a system à la D5: we can make sense of the notion of algebraic closure by showing in a constructive way that the theory of algebraic closure is consistent

Furthermore we get a non standard interpretation (Beth models), where forcing conditions are finite sets of atomic formulae

In most cases the consistency of the forcing conditions is decidable

This is connected to quantifier eliminations

Classical and intuitionistic coincide for this fragment (Barr's theorem)

Related work: propositional geometrical logic

The analysis of such propositional theories goes back at least to Lewis Carroll "Symbolic Logic", Part II W. Bartley 1977

Abeles, F "Lewis Carroll's method of trees: its origins in Studies in logic." Modern Logic 1 (1990), no. 1, 25–35.

One can naturally analysed the consequences of sets of atoms as a tree (similar to "genealogical trees")

An early example of the "tableau method" with hyperresolution

Non trivial examples, with memorization in order to avoid duplication of branches

Related Work: first-order geometrical logic

An early example comes also from Skolem “Logisch-kombinatorische Untersuchungen …” (1920)

Two sorts: lines $l, m, \ldots$ and points $P, B, \ldots$

(PP), $(PQ) \to (QP)$, $(PQ) \land (QR) \to (PR)$ (equality axioms for points)

(ll), $(lm) \to (ml)$, $(lm) \land (mn) \to (ln)$ (equality axioms for lines)

$(PQ) \land (Ql) \to (Pl)$, $(Pl) \land (lm) \to (Pm)$ (congruence axioms)

$(Pl) \land (Ql) \land (Pm) \land (Qm) \to (PQ) \lor (lm)$ (projective uniqueness axiom)

$(\exists l)((Pl) \land (Ql))$, $(\exists P)((Pl) \land (Pm))$ (projective axioms of incidence)

Related Work: SATCHMO

The same class of theories has been analysed in a similar way in automatic theorem proving

Manthey R., Bry F. “SATCHMO: a theorem prover implemented in Prolog” Proc. of 9th Conf. on Automated Deduction , LNAI 310, 1988

(thanks to Wolfgang Ahrendt for references to this work)

See also

Bezem, M, C. Th. “Newman’s lemma—a case study in proof automation and geometric logic.” Bull. Eur. Assoc. Theor. Comput. Sci. EATCS No. 79 (2003)

top-down derivation “dynamic programming” for the Horn part of the theory

Related Work: dynamical evaluation

Dynamic evaluation is a method of evaluating expressions and obtaining different answers dependent on the values of some auxilliary parameters, doing a case-by-case analysis.

D. Duval
Algebraic numbers : an example of dynamic evaluation Journal of Symbolic Computation (18) 429-445 (1994)

D. Duval, L. Gonzalez Vega
Dynamic evaluation and real closure Mathematics and Computers in Simulation (42) 551-560 (1996)

T. Mora
Solving Polynomial Equation Systems I. The Kronecker-Duval Philosophy Encyclopedia of Mathematics and its Applications 88 Cambridge University Press (2003)

Proof Theory in Algebra and Combinatorics

Scarpellini, B. On the metamathematics of rings and integral domains. Trans. Amer. Math. Soc. 138 (1969) 71–96.

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

This last work refers to earlier applications in combinatorics by Matiyasevich (also based on completness of hyper-resolution)

Related work: Intuitionistic Algebra

Wraith, G. C.

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.

Stresses the importance of geometrical logic to formulate results in intuitionistic algebra

The construction of the classifying model is similar to the Method of Trees

Conclusion

By working systematically at the syntactical level, but inspired by the semantics, we can give constructive meaning to some reasoning used in abstract algebra, that seems to require classical logic and choice

We can thus *exploit computationally* the concepts of abstract algebra

We provide a *logical basis* for dynamical evaluation: algebraic closure may fail to exist effectively, but it is possible to build effectively a *Beth model* of the theory of algebraic closures where branching correspond to case analysis