A logical approach to abstract algebra

Thierry Coquand <coquand@cs.chalmers.se>

Nov. 24, 2004

Abstract

Recent work in constructive algebra establishes experimentally that Hilbert's program of elimination of ideal elements works for a large part of abstract algebra. We present an example.

Brouwer's Fan Theorem

Constructive analysis of the notion of compactness

We consider *infinite sequences* $\alpha, \beta, \ldots$ of $0, 1$ and *finite sequences* $\sigma, \ldots$

As usual we write $\overline{\alpha}(n)$ for $\alpha(0) \ldots \alpha(n-1)$

Let V be a monotone set of finite sequences

Two different ways of saying that V is a *bar*

First way $\forall \alpha \exists n. \overline{\alpha}(n) \in V$

Brouwer’s Fan Theorem

Second way, we define inductively $V|\sigma$, and express $V|()$

$$\frac{\sigma \in V}{V|\sigma} \qquad \frac{V|\sigma 0 \quad V|\sigma 1}{V|\sigma}$$

Simple deduction system

Brouwer’s Fan Theorem is best understood as an analysis of the *meaning* of an universal quantification over all infinite sequences

Elimination of choice sequences (Kreisel,Troelstra)

Brouwer's Fan Theorem

This explanation of the Fan Theorem is important for constructive mathematics (à la Bishop), because in this framework, the equivalence

$$(\forall \alpha \exists n. \overline{\alpha}(n) \in V) \quad \equiv \quad V|()$$

cannot be proved, as it follows from Kleene's counter-example

One needs instead to take $V|()$ as the *rigourous definition* of what it means for V to be a bar, and as an explanation of the quantification over all sequences

Introduction of *Notes on constructive mathematics*, P. Martin-Löf

Hilbert's Program

Abstract methods are used to prove elementary statements (typically analytical methods in number theory, like for Dirichlet's theorem)

These methods may use abstract existence statements, "ideal" objects, that may fail to exist effectively (typically, Hilbert's proof of the basis theorem)

Hilbert's program: if one proves a *concrete statement*, one can always *eliminate* the use of these ideal objects, and obtain a purely elementary proof

Hilbert's Program

Gödel's Incompleteness Theorem shows that Hilbert's program fails in number theory

Recent work in constructive mathematics shows that Hilbert's program works for a large part of abstract algebra (and functional analysis), providing a constructive explanation of some abstract methods used in mathematics

Hilbert's program = constructive explanation of ideal elements

"Thus propositions of actualist mathematics seem to have a certain utility, but no *sense*. The major part of my consistency proof, however, consists precisely in *ascribing a finitist sense* to actualist propositions." (Gentzen)

Logical approach to algebra

We analyse some concepts and statements of abstract algebra, using suitable reformulation of the “elimination of choice sequences”

What we “eliminate” is the use of prime ideals and maximal ideals (but, like for choice sequences, we keep the same intuitions)

In each case we pay attention to the *logical complexity* of these statements

We get statements that are not only *logically* simpler, but also mathematically simpler, with simpler proofs

Zariski Spectrum

A typical example: the notion of *prime ideal* $\mathfrak{p}$ of a commutative ring R

Elimination of prime ideals

Theorem: (Krull) $(\forall \mathfrak{p}. a \in \mathfrak{p}) \quad \equiv \quad \exists n. a^n = 0$

The set of all prime ideals have a topological structure: the *Zariski spectrum* Sp(R) of R, the basic open being

$$D(a) = \{\mathfrak{p} \in \mathsf{Sp}(R) \mid a \notin \mathfrak{p}\}$$

Zariski Spectrum

Constructively, the Zariski spectrum is defined to be the distributive lattice generated by symbols $D(a)$ and relations

$$D(0) = 0$$

$$D(1) = 1$$

$$D(ab) = D(a) \wedge D(b)$$

$$D(a + b) \leq D(a) \vee D(b)$$

Formal Krull's Theorem: $D(a) = 0$ is provable if, and only if, a is nilpotent

Zariski Spectrum

Notice the complete analogy with the analysis of the Fan Theorem.

Here $D(a) = 0$ is taken to provide the rigourous meaning of

$$\forall \mathfrak{p}. a \in \mathfrak{p}$$

exactly as $V|()$ was understood to be the rigourous meaning of

$$\forall \alpha \exists n. \overline{\alpha}(n) \in V$$

Working with ideal elements

Krull's theorem may fail constructively if formulated in the form

$$(\forall \mathfrak{p}.a \in \mathfrak{p}) \quad \equiv \quad \exists n.a^n = 0$$

There are examples of rings which do not have (constructively) any prime ideals

Because of this, the notion of prime ideals usually plays a minor rôle in constructive algebra

But the formal version of Krull's theorem holds

$$(D(a) = 0) \quad \equiv \quad \exists n.a^n = 0$$

Logical complexity

We emphasize the difference between the two approaches

(1) Zariski spectrum as a set of prime ideals with a topological structure

(2) Zariski spectrum as a “distributive lattice” approximation of a ring

The two approaches are classically equivalent, because spectral spaces are sober, *but* there is a difference in *logical complexity*

Working with ideal elements

Write $D(b_1, \ldots, b_m)$ for $D(b_1) \vee \cdots \vee D(b_m)$

Formal Nullstellensatz Theorem: We can prove $D(a) \leq D(b_1, \ldots, b_m)$ if and only if $a^k \in \langle b_1, \ldots, b_m \rangle$ for some k.

In particular $1 = D(b_1, \ldots, b_m)$ if, and only if, $1 \in \langle b_1, \ldots, b_m \rangle$

This equivalence can be proved in a very weak formal system

Good example where Hilbert's program works

Krull dimension

A ring is of Krull dimension $< n$ if, and only if, there is no proper chain of prime ideals of length n

This can be expressed as the non consistency of the theory of proper chains of length n

$$\mathfrak{p}_0 \subset \cdots \subset \mathfrak{p}_n$$

Several arguments in abstract algebra prove a statement of the form: "if a ring has dimension $< n$ then there exists . . ."

One can thus hope to have a computational interpretation of these proofs

Krull dimension

The proof-theretical definition can be reformulated as an inductive definition (à la Menger)

A ring R is of Krull dimension < 0 if, and only if, it is trivial. Define the *bounday ideal* of $a \in R$ to be the ideal N_a generated by a and the elements x such that ax is nilpotent, then R is of Krull dimension $< n+1$ if, and only if, R/N_a is of Krull dimension $< n$ for all $a \in R$.

We don't talk about prime ideals any more. Only about elements of the rings

Krull dimension

The definition can be adapted for a distributive lattice (spectral space)

Define the boundary N_a of an element $a \in D$ as the ideal generated by a and the elements x such that $a \wedge x = 0$

Then $Kdim\ D < n+1$ iff $Kdim\ D/N_a < n$ for all $a \in D$

A spectral space is of dimension $< n+1$ iff all compact open have a boundary of dimension $< n$

History of Forster-Swan theorem

Algebraic formulations of topological concepts (1950s, Serre)

The notion of *vector bundle* over a compact space can be represented algebraically as a *finitely generated projective module* over a ring

A compact space X is represented as a ring $C(X)$

Free module corresponds to *trivial* vector bundle

This is precised later by Swan (1961)

Example

The tangent vector bundle on S^2 is not trivial

Hairy ball theorem: any continuous tangent vector field on the sphere must have a point where the vector is 0

Using the dictionnary above, this gives an example of a projective module which is not free over a ring

Projective modules

Concretely a finiteley generated projective module over a ring R is nothing more than an *idempotent matrix* over R

A finitely presented module over a ring R is nothing more than a rectangular matrix over R

Serre's splitting-off theorem

Geometrically we expect that if we have a vector bundle over a compact space, and the dimension of each fiber is high, then there is a non zero section.

The algebraic version of this is the following result

Theorem: (Serre, 1955) if M is a finitely generated projective module over a *noetherian* ring of Krull dimension $< n$ and if locally M is generated by n elements, then M can be written $M' \oplus R$

Actually a finer notion of dimension is used (maximal ideals instead of prime ideals)

Forster's theorem

Geometrical examples suggested the following algebraic result

Forster's theorem: (1964) If M is a finitely generated module over a *Noetherian* ring of Krull dimension $\leq n$ locally generated by r elements, then M can be generated by $n + r$ elements

This theorem is not optimal: if R is a local ring M will be generated by n elements

Swan's theorem

Swan's theorem: (1967) If M is a finitely generated module over a *Noetherian* ring whose maximal spectrum is of Krull dimension $\leq n$ and is locally generated by r elements, then M can be generated by $n + r$ elements

The main obstacle to analyse these theorems constructively is the *Noetherian* condition, which is logically very complex

Heitmann's theorem

This is a non Noetherian version of Forster's theorem

Heitmann's theorem: (1984) If M is a finitely generated module over a ring of Krull dimension $\leq n$ locally generated by r elements, then M can be generated by $n + r$ elements

Heitmann introduced also a new notion of dimension for the maximal spectrum, appropriate for the non Noetherian case, but could not see if Swan's theorem holds in the non Noetherian case

Constructive analysis of Forster's theorem

We understand constructively Krull dimension. What does Forster's theorem mean "concretely"?

A vector of elements in a ring is *unimodular* iff it generates the unit ideal

If M matrix, let $\Delta_n(M)$ be the ideal generated by all minors of order n

Forster's theorem, non Noetherian version: If we have a matrix M of columns $C_0, \dots, C_n$, and $Kdim\ R < n$ and $\Delta_n(M) = 1$ then there exists $t_1, \dots, t_n$ such that $C_0 + \Sigma t_i C_i$ is unimodular

Constructive analysis of Forster's theorem

Analysis of the logical complexity

To be of dimension $< n$ is a *geometrical* formula (not first-order because we have an infinite disjunction), for each given size of the matrix M we have an implication of an existential statement from a geometrical statement

Hence by a general metamathematical result (Barr's theorem), we should expect a direct constructive proof

In this case it is "enough" to follow Heitmann's paper and to extract the argument from it (that it we produce an algorithm that computers $t_1, \ldots, t_n$)

NonNoetherian version of Swan's theorem

Heitmann's paper uses implicitely the following notion of dimension (for the maximal spectrum)

$Hdim\ R < 0$ if and only if R is trivial. Let H_a be generated by a and the elements x such that ax is in the Jacobson radical, then $Hdim\ R < n+1$ if and only if $Hdim\ R/H_a < n$ for all $a \in R$.

This is like $Kdim\ R$ but we replace the intersection of all prime ideals by the intersection of all maximal ideals

$$J = \{x \in R \mid \forall y \exists z.\ z(1 - xy) = 1\}$$

NonNoetherian version of Swan's theorem

Fact: $Hdim\ R < n$ is *first-order definable*

Swan's theorem, non Noetherian version: (2004) If we have a matrix M of columns $C_0, \dots, C_n$, and $Hdim\ R < n$ and $\Delta_n(M) = 1$ then there exists $t_1, \dots, t_n$ such that $C_0 + \Sigma t_i C_i$ is unimodular

Logical complexity: for each given size of M this is now a *first-order statement*

By completness, if it is true, it has to have a first-order proof

How to search for a proof?

We look at the simplest non trivial case

$Hdim\ R < 2$ and $\Delta_2(M) = 1$ with M a 2×3 matrix

We have to find t_1, t_2, t_3 such that $C_0 + \Sigma t_i C_i$ is unimodular

Write l_{ij} the determinant of $C_i C_j$

Assume $1 = <l_{01}, l_{02}, l_{03}, l_{12}, l_{23}, l_{13}>$. We want

$$1 = <l_{01} + t_2 l_{21} + t_3 l_{31}, l_{02} + t_1 l_{12} + t_3 l_{32}, l_{03} + t_1 l_{13} + t_2 l_{23}>$$

How to search for a proof?

Since we are looking for a *first-order* proof the search space is much restricted (quite difficult to find otherwise)

Luckily the argument in this special case generalises directly for all dimension and matrices

How to search for a proof?

Trivial case of Swan's theorem: if R is *local* and $1 = <a, b, c, d>$ then there exists x such that

$$<a + cx, b + dx> = 1$$

This statement is a first-order statement

The hypothesis and the conclusion are geometric statements (in this case, forall exists statements)

If it is true, it has a not only a first-order proof, but also one which is particularly simple

Other results

The concrete formulation of Swan's theorem contains as a special case

Serre's theorem, non Noetherian version: (2004) If M is a finitely generated projective module locally generated by n elements over a ring R such that $Hdim\ R < n$ then M can be written $M' \oplus R$

Conclusion

Using ideas from formal topology (elimination of choice sequences) one can formulate results about prime/maximal ideals in an elementary way (but keeping the same intuitions)

The logical analysis of statements in algebra is fruitful

Can one always eliminate the Noetherian hypothesis (apparent counter-example: Krull's principal ideal theorem)?

Complexity of the corresponding algorithms?

References

Über die Anzahl der Erzeugenden einers Ideals in einem Noetherschen Ring
O. Forster, Math. Z. 84 (1964)

The Number of Generators of a Module
R.G. Swan, Math. Z. 102 (1967)

Generating non-Noetherian modules efficiently
R. Heitmann, Michigan Math. J. 31 (1984)

On a theorem of Kronecker about algebraic sets
Th. C., C.R. Acad. Sci. Paris, Ser. I 338 (2004) 291-294

Generating non-Noetherian modules constructively
Th. C., H. Lombardi and C. Quitté, Manuscripta Math. (2004)