Hilbert's program in abstract algebra

Thierry Coquand <coquand@cs.chalmers.se>

Aug. 23, 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 explain the main idea behind this approach and present some examples.

Brouwer's Fan Theorem

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 Incompletness 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)

Zariski Spectrum

We describe 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* $\mathsf{Sp}(R)$ 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

A course in Constructive Algebra
R. Mines, F. Richman, W. Ruitenburg

But the formal version of Krull's theorem holds

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, $1 \in \langle b_1, \ldots, b_m \rangle$

Historical remark

The axiomatic idea of reducing the problem of *existence* of an ideal object to the problem of *consistency* of a theory that describes this object can be traced back to the algebraic problem of existence of roots of equations (Gauss, Kronecker, Drach)

Kronecker's approach on this is described in H. Edwards work, cf. his MSRI talk on

Kronecker's "Fundamentalstz der Allgemeinen Arithmetic" and its relations to the fundamental theorem of algebra

Historical remark

Similarly, in Drach's presentation of Galois theory (1895) the *existence* of a splitting field for a polynomial $x^3 - a_1x^2 + a_2x - a_3$ is reduced to the problem of *proving*

$$1 \notin \langle x_1 + x_2 + x_3 - a_1, x_1x_2 + x_2x_3 + x_3x_1 - a_2, x_1x_2x_3 - a_3 \rangle$$

The same philosophy is applied for explaining the formal existence of solution to differential equations

Constructive algebra

Building effectively a splitting field, for instance, requires an algorithm for deciding if a polynomial is irreducible or not, which is not always possible

With this point-free or representation-free approach, one does not need to build effectively a splitting field, but can proceed "as if it exists". One can follow constructively classical ideas, revealing their implicit computational content

Remark: For proofs using prime ideals, classically shown to exist with the axiom of choice (or dependent choice), it is not possible to use the negative translation interpretation

Some Examples

I will now present some examples in algebra where the method of elimination of ideal elements provides a computational interpretation of abstract arguments

Krull dimension

Algebraic and real closure

Dedekind rings

Krull dimension

We say that 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 $a \in R$.

Krull dimension: Applications

Fundamental theorems in algebra which uses Krull dimension have been given abstract (topological) proofs in the following paper of R. Heitmann

Generating non-Noetherian modules efficiently.
Michigan Math. J. 31 (1984), no. 2, 167–180

Heitmann stresses the apparent non effective character of his arguments

A simple example is a proof of the following statement

Theorem: If R is of Krull dimension $\leq n$ then for any finite set of elements $a_0, \ldots, a_m \in R$ there exists $b_0, \ldots, b_n$ such that $D(a_0, \ldots, a_m) = D(b_0, \ldots, b_n)$.

Krull dimension: Kronecker's theorem

Corollary: (Kronecker) Given any number of polynomials in $\mathbb{Q}[X_1, \ldots, X_n]$ the algebraic set of common zeros of these polynomials in $\mathbb{C}^n$ is the intersection of $n+1$ hypersurfaces

Heitmann's proof appears at first highly non effective, but it is possible to read it constructively and this provides an elementary (and algorithmic) proof (that would have been accepted by Kronecker)

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

Krull dimension: Forster-Swan's theorem

Similarly, one obtains an elementary proof of Forster's theorem (1964) which bounds the number of generator of a module over a ring of finite Krull dimension.

One can also adapt this to get a non Noetherian version of Swan's generalisation (1966) of this theorem. This was raised as an open problem in Heitmann's paper.

Generating non-Noetherian modules constructively
Th. C., H. Lombardi and C. Quitté, Manuscripta Math., to appear

Algebraic closure

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

provides (among other things) a constructive analysis of the theory of algebraic closure and real closure, which shows, in an elementary way, the *formal consistency* of these theories

In particular, it gives a constructive understanding of Artin-Schreier's argument for the 17th Hilbert's problem

Dedekind rings

Théorie algorithmique des anneaux de Dedekind
L. Duclos, H. Lombardi, C. Quitté and M. Salou, Journal of Algebra, to appear

gives a constructive theory of Dedekind rings, without relying on the existence of decomposition of any ideals in prime ideals

One relies instead on the existence of a *partial* decomposition

General idea of lazy evaluation

a finite approximation of an infinite object is enough for a finite computation

Feasible computation?

Previous constructive approaches (Kronecker, Edwards) required complete decomposition in primes

This is not feasible for rings such as $\mathbb{Q}[X_1, \ldots, X_n]$ or $\mathbb{Z}$

One can hope to get relevant computational contents with this point-free or "representation-free" approach

The treatment of the existence of a splitting field in *A course on constructive algebra* is intermediary between these two approaches (does not require irreducibility)

Feasible computation?

This point is well illustrated by the following exercice (S. Cook)

"If x^2 divides y^2 then x divides y. The simple proof relying on unique decomposition in primes is not feasible. Find a feasible proof."

Here is a possible solution which uses only gcd. If $u = gcd(x, y)$ then $x = ua,\ y = ub$ and a, b are relatively primes. It follows that a^2, b^2 are relatively primes and hence $u^2 = gcd(x^2, y^2)$. If x^2 divides y^2 we have $u^2 = x^2$ and hence $u = x$.

We replace a *total* decomposition of x and y by a *partial* decomposition $x = ua,\ y = ub$.

Conclusion

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

Even classically, it is important to give the best formulation of results, without relying on Zorn's lemma when it is not necessary

This work provides a way to analyse some mathematical structures constructively, which hopefully may lead to relevant computational insights