Constructive Homological Algebra

Thierry Coquand

September 2010

Application of proof theory

Elements of Mathematical Logic, by Kreisel and Krivine

Herbrand's Theorem: If one proves $\exists x.A(x)$ and A is quantifier free, then one can find terms $t_1, \ldots, t_n$ such that $A(t_1) \vee \cdots \vee A(t_n)$ is a propositional tautology

For $\exists x.\forall y.A(x,y)$ we introduce a new function symbol f and we can find terms $t_1, \ldots, t_n$ such that $A(t_1, f(t_1)) \vee \cdots \vee A(t_n, f(t_n))$ is a propositional tautology

Proof theory

A. Joyal, Théorème de Chevalley-Tarski et remarque sur l'algèbre constructive, Cahiers de Topologie et Géométrie Différentielle 16 (1975) 256-258

G. Wraith, *Intuitionistic algebra, some recent development in topos theory*, Proceeding of ICM, 1978

M. Coste, H. Lombardi and M.F. Roy, *Dynamical method in algebra*, Ann. Pure Appl. Logic 111 (2001), 203-256

We say that a formula φ is positive iff it does not contain $\forall$, $\rightarrow$

$$\varphi ::= \bot \mid t = u \mid P(t_1, \ldots, t_n) \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \exists x.\varphi$$

Proof theory

A *coherent* formula is a formula of the form

$$\forall x_1 \ \ldots \ x_n. \ \ \varphi \to \psi$$

where φ and ψ are positive formulae

It is clear that any such formula is equivalent to a conjunction of formulae of the form

$$\varphi(\vec{x}) \to \exists \vec{y_1}.\varphi_1(\vec{x}, \vec{y_1}) \vee \cdots \vee \exists \vec{y_n}.\varphi_n(\vec{x}, \vec{y_n})$$

where $\varphi, \ \varphi_1, \ \ldots, \ \varphi_n$ are conjunctions of atomic formulae

Proof theory

A *coherent* theory T is a set of coherent formulae

Proposition: *if a coherent formula is proved with classical logic from a coherent theory, it can also be proved in intuitionistic logic.*

This follows directly from the soundness theorem: if $\vdash \varphi$ then $\Vdash \varphi$

Coherent Theories

For the theory of ACF.

If $\vdash t_1 = 0 \wedge \cdots \wedge t_k = 0 \rightarrow t = 0$ in ACF

We have, by *soundness* of the forcing relation

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle t_1, \ldots, t_k \rangle \Vdash t = 0$$

and (Lemma from the previous lecture) this means that t is in the radical of the ideal generated by $t_1, \ldots, t_k$ (Nullstellensatz). This gives an algebraic identity.

This holds also for the theory of fields.

For the theory of rings we have t in $\langle t_1, \ldots, t_k \rangle$

Coherent Theories

If we prove $t_1 = 0 \wedge t_k = 0 \rightarrow \exists x.t(x) = 0$ in the theory of *ring* we have

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle t_1, \ldots, t_k \rangle \Vdash \exists x.t(x) = 0$$

and since we have no branching this means

$$\mathbb{Z}[x_1, \ldots, x_n]/\langle t_1, \ldots, t_k \rangle \Vdash t(p) = 0$$

for for polynomial p in $\mathbb{Z}[x_1, \ldots, x_n]$

Proof theory

$$a_0x_0 + a_1x_1 = 1 \quad \wedge \quad b_0y_0 + b_1y_1 = 1 \quad \rightarrow$$

$$\exists z_0\ z_1\ z_2.\ a_0b_0z_0 + (a_0b_1 + a_1b_0)z_1 + a_1b_1z_2 = 1$$

is valid in the theory of rings by lecture 3

It follows that we should be able to find p_0, p_1, p_2 polynomials in $a_0, a_1, x_0, x_1, b_0, b_1, y_0, y_1$ such that

$$a_0x_0 + a_1x_1 = 1 \quad \wedge \quad b_0y_0 + b_1y_1 = 1 \quad \rightarrow$$

$$a_0b_0p_0 + (a_0b_1 + a_1b_0)p_1 + a_1b_1p_2 = 1$$

Proof theory

A priori more subtle than what we get from Herbrand's Theorem (which would give a disjunction)

In general, the truth of an existential statement does not imply that we can compute a witness

$$\exists x.\forall y.\ \ P(x) \to P(y)$$

In mathematics $\exists N.\forall m > N.\ f(m) = 0$, existence of bounds

Local rings

The basic covering are $R \to R[a^{-1}]$ and $R \to R[(1-a)^{-1}]$

The general covering are $R \to R[a_1^{-1}], \ldots, R \to R[a_n^{-1}]$ with $1 = \langle a_1, \ldots, a_n \rangle$

This is equivalent to $1 = D(a_1, \ldots, a_n)$ in the Zariski spectrum

Local rings

Theorem: *A (finitely generated) projective module over a local ring* R *is free*

Concretely this means that if we have an idempotent matrix $M^2 = M$ over R then this matrix is similar to a canonical projection matrix

By applying the soundness theorem, we get the following result: for *any* ring R and any $n \times n$ matrix M, $M^2 = M$ there exists a covering $1 = D(a_1, \ldots, a_k)$, and matrix $P_1, \ldots, P_k$ such that P_i is invertible in $R[a_i^{-1}]$ and $P_i^{-1} M P_i$ is a canonical projection matrix

Local rings

Let φ be $\neg(x = 0) \longrightarrow \mathsf{inv}(x)$

We have $\Vdash \varphi$ but $\vdash \varphi$ does not hold

If $R \Vdash \neg(a = 0)$ then we have, for all $f : R \longrightarrow S$ if $f(a) = 0$ then $1 = 0$ in S. In particular $1 = 0$ in $R/\langle a \rangle$ and so a is invertible

This formula is not valid in a local ring which is not a field

All this applies for any coherent theory extending the theory of rings

Example: theory of ordered fields

We have the relations $\leqslant, <$and the axioms

$0 \leqslant x^2$

$0 < x \wedge 0 \leqslant y \rightarrow 0 < x + y$

$x^2 = 0 \rightarrow x = 0$

$x = 0 \vee x^2 > 0$

$x > 0 \rightarrow \exists z.1 = xz$

From these axioms we can prove $x^3 - y^3 = 0 \rightarrow x - y = 0$

Homological Algebra

Linear algebra over a ring

For a finitely generated ideal I we have a map $R^m \xrightarrow{A} I \longrightarrow 0$ and we can build a sequence, if R is coherent

$$\ldots \longrightarrow R^{m_3} \xrightarrow{A_3} R^{m_2} \xrightarrow{A_2} R^{m_1} \xrightarrow{A_1} R^m \xrightarrow{A} I \longrightarrow 0$$

Free Resolution

In particular if we have a finitely generated ideal I we have a map $R^m \xrightarrow{A} I \longrightarrow 0$ and we can build a sequence

$$\ldots \longrightarrow R^{m_3} \xrightarrow{A_3} R^{m_2} \xrightarrow{A_2} R^{m_1} \xrightarrow{A_1} R^m \xrightarrow{A} I \longrightarrow 0$$

This is called a *free resolution* of the ideal

This measures the "complexity" of the ideal: relations between generators, then relations between relations, and so on.

Free Resolution

If we have $m_k = 0$ for $k > N$ we say that I has a *finite free resolution*

$$0 \longrightarrow R^{m_N} \xrightarrow{A_N} \ldots \xrightarrow{A_2} R^{m_1} \xrightarrow{A_1} R^{m} \xrightarrow{A} I \longrightarrow 0$$

Regular rings

A ring is *regular* iff any finitely generated ideal has a finite free resolution

For instance $k[X_1, \ldots, X_n]$ is regular (Hilbert's syzygies Theorem)

This notion was introduced by Serre to capture the properties of a local ring at a smooth (non singular) point of an algebraic variety (to show that this notion is stable under localisation)

Theorem: *If R is Noetherian and regular, then R is an UFD. If R is regular then R is a GCD domain*

Noetherianity

Most presentation of homological algebra assumes the ring R to be Noetherian

A remarquable exception is the book by Northcott *Finite Free Resolution*

In this context most results are first-order schema, and we can hope to have direct elementary proofs.

Regular element and ideal

We say that a is *regular* iff $ax = 0 \rightarrow x = 0$

We say that $a_1, \ldots, a_n$ is *regular* iff $a_1 x = 0 \wedge \cdots \wedge a_n x = 0 \rightarrow x = 0$

We say that I is regular iff $xI = 0 \rightarrow x = 0$

Lemma: *If $a_1, \ldots, a_n, a$ and $a_1, \ldots, a_n, b$ are regular then so is $a_1, \ldots, a_n, ab$*

Simple logical form

Corollary: *If $a_1, \ldots, a_n$ is regular then so is $a_1^k, \ldots, a_n^k$*

Vasconcellos Theorem

If we have

$$0 \longrightarrow R^{m_k} \xrightarrow{A_k} \ldots \xrightarrow{A_2} R^{m_1} \xrightarrow{A_1} R^{m} \xrightarrow{A} I \longrightarrow 0$$

We define $c(I) = m - m_1 + m_2 - \ldots$ to be the *Euler characteristic* of I

One can show that it depends only on I and not on the choice of the resolution

Theorem: *If $c(I) = 0$ then $I = 0$. If $c(I) = 1$ then I is regular. In all the other cases then $1 = 0$ in R*

Vasconcellos Theorem

The proof of Vasconcellos Theorem in Northcott's book relies on the existence of minimal prime ideals, which is proved using Zorn's Lemma

If we fix the size of the resolution, for instance

$$0 \to R^2 \xrightarrow{A} R^3 \to \langle a_0, a_1, a_2 \rangle \to 0$$

the statement becomes first-order

Logical form of the statement? It is a coherent implication, hence we know a priori that it should have a simple logical proof

Vasconcellos Theorem

We explain the elementary proof in this case

This relies on the following glueing principle

Lemma: *If* $u_1, \ldots, u_n$ *is regular and* $b = 0$ *in* $R[1/u_1], \ldots, R[1/u_n]$ *then* $b = 0$ *in* R

The proof is direct since $u_1^k, \ldots, u_n^k$ is regular

Local-global principle, compare with $1 = \langle u_1, \ldots, u_n \rangle$

Vasconcellos Theorem

We write $A = \begin{pmatrix} u_0 & v_0 \\ u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}$

Since A represents an injective map both u_0, u_1, u_2 and v_0, v_1, v_2 are regular

Vasconcellos Theorem

I prove that $I = \langle a_0, a_1, a_2 \rangle$ is regular in $R[1/u_0], R[1/u_1], R[1/u_2]$

In $R[1/u_0]$, we can by change of basis, consider the sequence

$$0 \to R^2 \xrightarrow{A'} R^3 \to I \to 0$$

with $A' = \begin{pmatrix} 1 & 0 \\ 0 & v_1 - u_1 v_0/u_0 \\ 0 & v_2 - u_2 v_0/u_0 \end{pmatrix}$

Vasconcellos Theorem

We can then simplify the sequence to

$$0 \to R \longrightarrow R^2 \to I \to 0$$

Reasoning in a similar way, we reduce the problem to

$$0 \to R \to I \to 0$$

and it is clear that I is regular in this case

Regular Ring

Assume that any finitely generated ideal has a finite free resolution

In particular $\langle a \rangle$ has a finite free resolution

Hence we have $a = 0$ or a is regular

Classically, this means that R is an integral domain

Injective maps

The glueing property for regular elements has replaced the use of minimal prime ideals

The same method gives a proof of the following result.

Lemma: If A is a $n \times m$ matrix with $n \leqslant m$ and $\Delta_n(A)$ is regular then $R^n \xrightarrow{A} R^m$ is injective

Injective maps

The converse holds

Lemma: If A is a $n \times m$ matrix with $n \leqslant m$ and $R^n \xrightarrow{A} R^m$ is injective then and $\Delta_n(A)$ is regular

The same method proves the converse, by induction on n and considering the first column which is regular

Regular Element Theorem

The following result holds only for Noetherian rings

Theorem: *If a finitely generated ideal is regular then it contains a regular element*

It is one reason why most treatment considers only Noetherian rings

Northcott presents a beautiful way to avoid this Noetherianity condition (due to Hochster).

Regular Element Theorem

Theorem: (McCoy) *If* $a_0, \ldots, a_n$ *is regular in* R *then* $a_0 + a_1X + \cdots + a_nX^n$ *is regular in* $R[X]$

Thus, in general, we have a regular element but in $R[X]$

The solution exists in an enlarged universe

This result can be used instead of the Regular Element Theorem

McCoy's Theorem

We write $P = a_0 + \cdots + a_n X^n$ and we show by induction on m that if $PQ = 0$ with $Q = b_0 + b_1 X + \cdots + b_m X^m$, then $Q = 0$

We have $a_n b_m = 0$ and $P(a_n Q) = 0$. Hence by induction, $a_n Q = 0$

Similarly, we get $a_{n-1} Q = \cdots = a_0 Q = 0$ and since $a_0, \ldots, a_n$ is regular we have $Q = 0$

McCoy's Theorem

The same argument shows that

Theorem: (McCoy) *If* $a_0, \ldots, a_n$ *is regular in* R *then* $a_0X_0+a_1X_1+\cdots+a_nX_n$ *is regular in* $R[X_0, \ldots, X_n]$

We have replaced the ideal $\langle a_0, \ldots, a_n \rangle$ by the polynomial $a_0X_0 + \cdots + a_nX_n$

H. Edwards *Divisor Theory*, Kronecker works with such polynomial (instead of working with ideals)

Hilbert-Burch Theorem

Theorem: *If we have an exact sequence*

$$0 \to R^n \xrightarrow{A} R^{n+1} \to \langle a_0, \ldots, a_n \rangle \to 0$$

then the elements $a_0, \ldots, a_n$ *have a GCD, which is regular*

Here again, for a fixed size, this is a first-order statement

Logical form of the statement?

Hilbert-Burch Theorem

We prove it for $n = 2$ with $A = \begin{pmatrix} u_0 & v_0 \\ u_1 & v_1 \\ u_2 & v_2 \end{pmatrix}$

Question: how do we compute the gcd from the given data?

Hilbert-Burch Theorem

Write $\Delta_i = u_j v_k - u_k v_j$ we know that $\Delta_0, \Delta_1, \Delta_2$ is regular. Hence the element $w = \Delta_0 X_0 + \Delta_1 X_1 + \Delta_2 X_2$ is regular by McCoy's Theorem

We change R to $R[X_0, X_1, X_2]$ we still have an exact sequence

$$0 \to R[X_0, X_1, X_2]^2 \xrightarrow{A} R[X_0, X_1, X_2]^3 \xrightarrow{(a_0\ a_1\ a_2)} IR[X_0, X_1, X_2] \to 0$$

It follows from this that $0 \to R[X_0, X_1, X_2]^2 \xrightarrow{A} R[X_0, X_1, X_2]^3$ is still exact modulo w, using the fact that w is regular

Regular Element

Lemma: *If* $0 \to E \xrightarrow{\varphi} F \xrightarrow{\psi} G$ *is exact and* a *is regular for* G *then* φ *is still mono modulo* a

a regular for G means $az = 0$ implies $z = 0$ for z in G

If we have $\varphi(x) = ay$ then we have $a\psi(y) = 0$ and hence $\psi(y) = 0$, since a is regular for G. Hence there exists x_1 such that $y = \varphi(x_1)$ and we have $\varphi(x - ax_1) = 0$ and hence $x = 0$ modulo a

Hilbert-Burch Theorem

Hence $\Delta_0, \Delta_1, \Delta_2$ is still regular *modulo* w

Since we have $\Delta_i a_j = \Delta_j a_i$ it follows that

$$\Delta_j(a_0X_0 + a_1X_1 + a_2X_2) = a_j w = 0$$

modulo w. Hence $a_0X_0 + a_1X_1 + a_2X_2 = 0$ modulo w

Hence we have one element g such that $a_i = g\Delta_i$

By Vasconcellos Theorem, a_0, a_1, a_2 is regular and so g is regular

Hilbert-Burch Theorem

I claim that g is the GCD of a_0, a_1, a_2

If we have $a_i = tb_i$ then t is regular since a_0, a_1, a_2 is regular

We have $t(b_i\Delta_j - b_j\Delta_i) = 0$ and hence $b_i\Delta_j = b_j\Delta_i$

Like before, we deduce that there exists s such that $b_i = s\Delta_i$

We then have $\Delta_i(ts - g) = 0$ and so $g = ts$

References

G. Kreisel and J.L. Krivine, *Elements of Mathematical Logic*

A. Joyal, Théorème de Chevalley-Tarski et remarque sur l'algèbre constructive, Cahiers de Topologie et Géométrie Différentielle 16 (1975) 256-258

H. Lombardi and C. Quitté *Algèbre Commutative, méthode constructive; modules projectifs de type fini*, available from the home page of Henri Lombardi

Northcott *Finite Free Resolution*

G. Wraith, *Intuitionistic algebra, some recent development in topos theory*, Proceeding of ICM, 1978

Some variation on McCoy's Theorem

R arbitary ring

$A = a_0 + a_1X + \cdots + a_nX^n \qquad c(A) = \langle a_0, \ldots, a_n \rangle$

$B = b_0 + b_1X + \cdots + b_mX^m$

$C = AB = c_0 + c_1X + \cdots + c_lX^l$

Some variation on McCoy's Theorem

Gauss-Joyal $D(A) \wedge D(B) = D(C)$ or $\sqrt{c(A)}\sqrt{c(B)} = \sqrt{c(C)}$

Artin $\exists p \quad c(A)^{p+1}c(B) = c(A)^p c(C)$

McCoy $Ann(c(A)) = 0,\ AB = 0 \quad \rightarrow B = 0$

Kronecker $c_0, \ldots, c_l$ are integral over $a_0b_0, \ldots, a_nb_m$

Dedekind-Mertens $c(A)^{m+1}c(B) = c(A)^m c(C)$