Geometric Theories, Lazy Computations,

Constructive Algebra

Henri Lombardi

München, November 27, 2006

p. 1 ——— **Contents** ———

- Hilbert's Program
- Logical complexity
- Elimination of a generic prime, ... Serre's Problem, ...
- Elimination of several primes, ... Zariski Spectrum, Krull dimension, ...
- Elimination of maximal primes
- Elimination of minimal primes
- A new approach to constructive mathematics

p. 2 ——— **Hilbert's Program** ———

Since the work of Dedekind, and Hilbert, non effective methods have been more and more used in algebra

Dedekind: abstract definition of ideals as a set of elements

Reasoning by contradiction: to prove the existence of an object, show instead that it is absurd that this object does not exist

If we prove in commutative algebra the existence of an object satisfying a simple "concrete" property, it is not clear if this proof gives a way to compute this object

p. 3 ——— **Hilbert's Program** ———

This was one issue raised during the debate between Hilbert and Brouwer

Hilbert's program: if we prove using ideal methods a *concrete statement*, one can always **eliminate the use of these ideal elements** and obtain a purely elementary proof

Ideal methods: use of prime ideals, maximal ideals, valuation rings, local-global principle, non constructive reasoning, ...

Hilbert: (abstract) existence = logical consistency

p. 4 ——— **Hilbert's Program** ———

Warning! Hilbert's Program cannot work for all "concrete" statements.

E.g., the existence of a prime factorization for a polynomial in $K[X]$, K a field.

This is related to the logical complexity of the assertion: *any polynomial has an irreducible factor.*

This is a $\forall\ \exists\ \forall$ statement, and for this kind of statement, classical logic gives a radically new interpretation. So a classical proof may not in principle hide a constructive proof of the concrete result.

p. 5 ——— **Hilbert's Program** ———

Recent work in constructive mathematics shows that Hilbert's program works for a large part of abstract algebra providing a constructive explanation of some abstract methods used in mathematics.

Furthermore this follows Hilbert's idea of replacing an "infinite ideal object" by a syntactical theory that describes it.

p. 6 ——— **Hilbert's Program** ———

Before the introduction of non effective methods, any proof of an existence statement could be seen as an algorithm.

In logic, this is known as the *Brouwer-Heyting-Kolmogorov* interpretation.

Question: has the use of ideal/non effective arguments in mathematics some computational relevance?

p. 7 ——— **Hilbert's Program** ———

Question: has the use of ideal/non effective arguments in mathematics some computational relevance?

It has some connection with the idea of **lazy computation**.

We cannot compute completely an infinite object but we can use **partial finite amount of information** about this object during a computation.

As a striking case, logical inconsistency is always obtained from a finite amount of information.

p. 8 ——— **Logical complexity** ———

If we take a basic book in abstract algebra such as Atiyah-Macdonald *Introduction to Commutative Algebra* or Matsumura *Commutative ring theory* we discover that basic theorems are not formulated in a first-order way because of the introduction of abstract notions. Such abstract notions are

1. arbitrary ideals of the rings, that are defined as subsets, and thus not expressed in a first-order way,
2. *prime* or *maximal* ideals, whose existence relies usually on Zorn's lemma,
3. Noetherian hypotheses.

These notions have different levels of non effectivity.

p. 9 ——— **Logical complexity** ———

To be Noetherian can be captured by a generalised inductive definition:

C. Jacobsson and C. Löfwall. *Standard bases for general coefficient rings and a new constructive proof of Hilbert's basis theorem.* J. Symbolic Comput. 12 (1991), no. 3, 337–371,

But then we leave first-order logic.

The notion of prime ideals seems even more ineffective, the existence of prime ideals being usually justified by the use of Zorn's lemma.

Furthermore a notion such as "being nilpotent" cannot be expressed in a first-order way since it involves an infinite countable disjunction.

p. 10 ——— **Logical complexity** ———

G. Wraith points out the relevance of the notion of geometric formula for constructive algebra.

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.

One defines first the notion of **positive formulae**: a positive formula is one formula of the language of rings built using positive atomic formula (equality between two terms) and the connectives $\vee, \wedge$. Special cases are the empty disjunction which is the false formula $\bot$, and the empty conjunction which is the true formula $\top$.

We allow also existential quantification and infinite disjunction indexed over natural numbers, or over the elements of the ring.

p. 11 ——— **Logical complexity** ———

A **geometric formula** is an implication between two positive formulae.

A **coherent formula** is a formula which is both geometric and first-order.

A **geometric theory** is a theory whose axioms are geometric.

A **coherent theory** is a theory whose axioms are coherent.

A **dynamical proof** (in a geometric theory) is a logic-free proof. Axioms are seen as inference rules. Only atomic formulae appear. One replaces the logical machinery by a purely computational one, inside a tree. Opening branches at a node means applying a rule with a disjunction in the conclusion.

p. 12 ——— **Logical complexity** ———

Notice that, as special cases, any positive formula is geometric, and the negation of a positive formula is geometric.

As a special case of coherent formula, we have the notion of **Horn** formula, which is an implication $C \to A$ where C is a conjunction of atomic formulae, and A an atomic formula. Horn theories correspond to the notion of **atomic systems** in Prawitz. For instance, equational theories are Horn theories.

D. Prawitz. *Ideas and results in proof theory.* Proceedings of the Second Scandinavian Logic Symposium, pp. 235–307. Studies in Logic and the Foundations of Mathematics, Vol. 63, North-Holland, Amsterdam, 1971.

p. 13 ——— **Logical complexity** ———

The notion for $a \in R$ to be nilpotent is not first-order but it can be expressed as a positive formula: a is nilpotent if and only if $a^n = 0$ for some $n \in \mathbb{N}$.

On the other hand, "to be reduced", that is to have only 0 as a nilpotent element, can be expressed by the following Horn formula

$$\forall x.\ x^2 = 0 \to x = 0$$

Another typical example of notion expressed geometrically is the notion of **flat** module M over a ring R.

It says that if we have a relation $PX = 0$ where P is a row vector with coefficient in R and X a column vector with elements in M then we can find a rectangular matrix Q and a vector Y such that $QY = X$ and $PQ = 0$. Since we don't say anything about the size of Q this statement involves implicitely an infinite disjunction over natural numbers. Thus the notion of flat module is not first-order but geometric.

p. 14 ——— **Logical complexity** ———

As stressed by G. Wraith the importance of geometric formula comes from *Barr's theorem.*

Theorem *If a geometric sentence is deducible from a geometric theory in classical logic, with the axiom of choice, then it is also deducible from it intuitionistically.*

Furthermore in this case there is always a proof with a simple branching tree form: a **dynamical** proof.

In general, this tree may be infinitely branching, but, if the theory is *coherent*, that is geometric *and* first-order, then the proof is a finitely branching tree.

p. 15 ——— **Elimination of "all primes"** ———

We will describe a general method in order to get a constructive proof when the (concrete) conclusion is obtained in classical abstract algebra by a reasoning that says:
After localization at any prime ideal of the ring, the concrete result is clear.
So by a particular kind of "local-global principle", the result is true.

You see that prime ideals are only here to make the proof easier.

Also: not "all primes" are really needed, only a generic one.

p. 16 **Elimination of a generic prime**

General recipe: 1) Consider a formalization where the concrete context is described (no prime).

2) Add a predicate $Z(x)$ with the intended meaning $x \in \mathfrak{P}$ where $\mathfrak{P}$ is a generic prime. Axioms are:

$\vdash Z(0), \quad \vdash \neg Z(1), \quad Z(x), Z(y) \vdash Z(x+y), \quad Z(x) \vdash Z(xy),$

$Z(xy) \vdash Z(x) \vee Z(y).$

3) Prove that the new theory is conservative over the first one (this proof is hidden in the classical proof of the corresponding local-global principle).

4) Read the classical proof in the second theory.

p. 17 **Elimination of a generic prime**

This general recipe has been used in order to obtain concrete proofs of

- Nullstellensatz (algebraically closed fields as ideal objects above a field)
- Positivstellensatz (real closed fields as ideal objects above a real field)
- "Valued"-stellensatz (algebraically closed valued fields as ideal objects above a valued field)

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

p. 18 **Elimination of a generic prime**

This dynamical method can be seen as lazy evaluation.

In general the dynamical method can be explained through purely algebraic arguments translating (and hiding) the logical machinery.

In the next slides we see an example with Quillen's solution of Serre's problem.

p. 19 **Serre's Problem**

Theorem: (Quillen-Suslin) *Any finitely generated projective module on a polynomial ring (over a field) is free*

Theorem: (Quillen-Suslin, concrete version) *Any idempotent matrix on a polynomial ring is similar to a canonical projection matrix*

Remark that in the theory of fields, if you are able to bound the degrees in the solution, this is a scheme of $\forall\ \exists$ statements. It has a good logical form, a constructive deciphering is a priori feasible.

Generalization (by Maroscia, and Brewer & Costa) to the case of a polynomial ring over a Prüfer ring of Krull dimension ≤ 1.

p. 20 **Serre's Problem**

The proofs of Quillen and Brewer & Costa has been understood constructively (H. Lombardi, C. Quitté, I. Yengui), by an analysis of some local-global principles.

These works give *new* algorithms, which do not rely on computation of Gröbner's basis, for solving Serre's problem.

H. Lombardi, C. Quitté
Constructions cachées en algèbre abstraite (2) Le principe local-global, in:

Commutative ring theory and applications. Eds: Fontana M., Kabbaj S.-E., Wiegand S. LNPAM vol 231. M. Dekker. (2002) 461–476.
H. Lombardi, C. Quitté, I. Yengui
Hidden constructions in abstract algebra (6) The theorem of Maroscia, Brewer and Costa. (2005). Preprint.

p. 21 ——— **Serre's Problem, Quillen's patching** ———

Example of constructive rereading of a local-global principle.

Theorem *Let P be a finitely presented module over $R[X]$.*

(Quillen's patching, original form) *P is extended from R if and only if after localisation at any prime ideal $\mathfrak{P}$, $P_{\mathfrak{P}}$ is extended from $R_{\mathfrak{P}}$.*

(Quillen's patching, constructive form) *Consider $S_1, \ldots, S_n$ comaximal multiplicative subsets of R. Then P is extended from R if and only if after localisation at each S_i, P_{S_i} is extended from R_{S_i}.*

p. 22 ——— **Serre's Problem, Quillen's patching** ———

Lemma *Let P be a projective module over $R[X]$, R a Prüfer domain with Krull dimension ≤ 1. Then P is extended.*

Original proof: After localization at any prime $\mathfrak{P}$, R becomes a valuation domain with Krull dimension ≤ 1. In this case we give a proof showing that $V^{-1}R_{\mathfrak{P}}[X]$ is a Bezout domain (here V is the monoid of monic polynomials). As a consequence, $V^{-1}P_{\mathfrak{P}}$ is free. By Horrocks theorem, $P_{\mathfrak{P}}$ is itself free, thus extended from $R_{\mathfrak{P}}$. So, by Quillen's abstract patching, P is extended.

Constructive rereading: Reread the previous proof as a proof saying that, after localization at comaximal multiplicative subsets S_i (these S_i are constructed dynamically during the proof from the idempotent matrix F defining P), the module $V^{-1}P_{S_i}$ is free. By Horrocks theorem, P_{S_i} is itself free, thus extended from R_{S_i}. So, by Quillen's concrete patching, P is extended.

p. 23 ——— **Elimination of "several primes"** ———

In the next slides we face the problem of a constructive interpretation for theorems that use "several primes" in the hypothesis.

E.g., the hypothesis says: *assume the ring has Krull dimension $\leq d$* and the conclusion has a concrete form.

This kind of hypothesis involves not only a generic prime, but a *generic chain of primes.*

To understand if a concrete meaning of the hypothesis is possible we need a constructive interpretation of Zariski spectrum.

p. 24 ——— **Zariski spectrum** ———

Fundamental object in abstract algebra, usually defined as the set of prime ideals of a ring R with the basic opens

$$D(a) = \{\mathfrak{p} \mid a \notin \mathfrak{p}\}.$$

However, even if the ring R is given concretely (i.e., we are able to make basic computations in it) it may be difficult to show effectively the existence of prime.

Often, what matters is not *one* particular prime ideal, but the collection of *all* prime ideals.

p. 25 ——— **Zariski spectrum** ———

Zariski spectrum is best seen as a *point-free* space

A. Joyal (1972) definition of the Zariski spectrum

A *support* on R is a map $D : R \to L$ in a *distributive lattice* L satisfying the conditions

$$D(0) = 0 \qquad D(1) = 1 \qquad D(ab) = D(a) \wedge D(b) \qquad D(a+b) \leq D(a) \vee D(b)$$

The Zariski spectrum can then be defined as **the free support** on R

p. 26 ——— **Zariski spectrum** ———

This definition is purely algebraic (no need of Zorn's Lemma)

Theorem: *$D(a) \leq D(b_1) \vee \cdots \vee D(b_n)$ holds iff a is in the radical ideal generated by $b_1, \ldots, b_n$.*

This is also known as the *formal* version of the Nullstellensatz.

The proof is direct: one shows that the lattice of finitely generated radical ideals is the free support.

$D(u)$: finite piece of information about a prime ideal.

p. 27 ——— **Gauss-Joyal** ———

Interesting supports, distinct from the Zariski support, are to be analysed.

Proposition: *If $D : R \to L$ is a support then so is*

$$D_X : \begin{cases} R[X] & \longrightarrow & L \\ & & \\ a_0X^k + \cdots + a_k & \longmapsto & D(a_0, \ldots, a_k) \in \mathsf{Zar}\, R \end{cases}$$

p. 28 ——— **Krull dimension of a ring** ———

The *Krull dimension* of a ring is defined to be the maximal length of chain of prime ideals.

This definition seems hopelessly non effective.

Following the pioneering work of Joyal and L. Español, one can give a purely algebraic definition of the Krull dimension of a ring.

As a test case, we have analysed in this way a paper of R. Heitmann "*Generating non-Noetherian modules efficiently*" Michigan Math. J. 31 (1984), 167-180, which contains non effective proofs of basic results in commutative algebra.

p. 29 ——— **Krull dimension of a ring** ———

Definition: *We say that $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are* complementary *iff*
$1 = D(a_1, b_1),\ D(a_1b_1) \leq D(a_2, b_2),\ \ldots, D(a_nb_n) = 0$.

For $n = 1$ this means that $D(a_1)$ is the complement of $D(b_1)$.

Definition: *R, D is of dimension $< n$ iff any n-ary sequence has a complementary sequence.*

Definition: *$\mathsf{Kdim}\, R < n$ iff R, D is of dimension $< n$ for the free support D.*

p. 30 ——— **Krull dimension of a ring** ———

Notice that this definition is first-order (in the multi-sorted language of rings and lattices).

It states the condition in term of the elements of the *ring* (that are "concrete") and not in term of prime ideals.

p. 31 ——— **Nullstellensatz** ———

We get the following (new) Nullstellensatz.

Theorem: *$\mathsf{Kdim}(R) < n$ iff for any $a_1, \ldots, a_n$ there exist $k_1, \ldots, k_n$ and $u_1, \ldots, u_n$ such that $a_1^{k_1}(a_2^{k_2}(\ldots a_n^{k_n}(1 - a_nu_n) \cdots - a_2u_2) - a_1u_1) = 0$.*

Using this characterization, one can give a simple (constructive) proof that the dimension of $K[X_1, \ldots, X_m]$ is m (K a field). This follows directly from the fact that $m + 1$ polynomials on m variables are algebraically dependent.

p. 32 ——— **Kronecker's Theorem** ———

Theorem: *If R, D is of dimension $< n$ then for any $u_0, u_1, \ldots, u_n$ there exist $w_1, \ldots, w_n$ such that $D(u_0, \ldots, u_n) = D(w_1, \ldots, w_n)$.*

This is a (non Noetherian) generalisation of Kronecker's Theorem.

Since it is formulated as a *first-order schema* the proof cannot be complicated *a priori*.

The proof can be seen as a general algorithm which computes $w_1, \ldots, w_n$ from $u_0, u_1, \ldots, u_n$.

p. 33 ——— **Kronecker's Theorem** ———

Constructive proof:

Take $v_1, \ldots, v_n$ a complementary sequence for $u_1, \ldots, u_n$.

Define $w_1 = u_1 + u_0 v_1, \ \ldots, \ w_n = u_n + u_0 v_n$.

This concrete proof, which gives an explicit algorithm, is *extracted* from an abstract proof in the paper of Heitmann.

The abstract proof, which seems unfeasible (use of prime ideals, topological arguments on the Zariski spectrum) contains implicitely a clever and simple algorithm (computation of the polynomials $v_1, v_2, \ldots, v_n$).

p. 34 ——— **Forster-Swan's and Serre's Splitting-Off Theorem** ———

T. Coquand. *Sur un théorème de Kronecker concernant les variétés algébriques.* C.R.Acad.Sci., Paris, Ser I, 338 (2004), Pages 291-294

T. Coquand, H. Lombardi, C. Quitté. *Generating non-Noetherian modules constructively.* Manuscripta Mathematica, 115 (2004), Pages 513-520

T. Coquand, H. Lombardi, C. Quitté. *Dimension de Heitmann des treillis distributifs et des anneaux commutatifs.* Publications mathématiques de Besançon (2006), 51 pages.

Heitmann's paper contains also non-Noetherian versions of Forster-Swan's Theorem and Serre splitting-off Theorem (1958)

p. 35 ——— **Forster-Swan's and Serre's Splitting-Off Theorem** ———

Theorem: (Serre, 1958) *If $\Delta_n(M) = 1$ and R, D is of dimension $< n$ and M is a square idempotent matrix then there exists an unimodular combination of the column vectors of M.*

Forster's Theorem can be deduced as a corollary of a generalization of the previous theorem.

Theorem: *Let M an arbitrary matrix. If $\Delta_n(M) = 1$ and R, D is of dimension $< n$ then there exists an unimodular combination of the column vectors of M.*

Since it is formulated as a *first-order schema* the proof cannot be complicated *a priori*. For a given n and given size of the matrix, the constructive proof can be interpreted as an algorithm which produces the unimodular combination.

p. 36 ——— **Elimination of maximal primes** ———

From a logical point of view, eliminating a (generic) maximal prime from an abstract reasoning seems *much more difficult* than eliminating a (generic) prime.

Reasoning with a generic prime in order to prove some concrete thing is something like:
in order to prove that a ring (which is obtained from the hypotheses after some computations) is trivial, show that it does'nt contain any prime ideal.

From a logical point of view: if you are able to prove $1 = 0$ after you added a predicate and axioms for a generic prime, then you are able to prove $1 = 0$ without using this facility.

This conservativity theorem is the constructive content of the "construction à la Zorn" of a prime ideal in a nontrivial ring.

p. 37 ——— **Elimination of maximal primes** ———

The case of a generic maximal ideal is different.

Reasoning with a generic maximal prime in order to prove some concrete thing is something like:
in order to prove that a ring is trivial, show that it does'nt contain any maximal ideal.

This cannot be captured by an argument using only first order logic.

p. 38 ——— **Elimination of maximal primes** ———

The minimal models of the first order theory "the ring R, plus predicate and axioms for a maximal ideal" are not:
(an homomorphic image of) *R with a maximal ideal*, but
(an homomorphic image of) *the localization of R at a prime ideal.*

In order to capture the notion of maximal ideal you have to use an infinite disjunction (a disjunction over all elements of the ring).

$$x \in \mathfrak{M} \quad \vee \quad \bigvee_{y \in R} 1 - xy \in \mathfrak{M}$$

p. 39 — **Serre's Problem (again)** —

In fact, the proof of Suslin for Serre's Problem, which uses a maximal ideal in a generic way, can also be interpreted constructively.

I. Yengui
Making the use of maximal ideals constructive. (2004) preprint.

p. 40 — **Elimination of maximal primes** —

When you reread dynamically a proof saying
"after localisation at a prime ideal the ring becomes trivial",
you construct a tree by using the disjunctions

$$x \in \mathfrak{P} \quad \vee \quad x \notin \mathfrak{P}$$

At the leaves of the tree you get comaximal monoids S_i with $1 = 0$ in each R_{S_i}.

But now you have to reread dynamically a proof saying
"after quotient by a maximal ideal the ring becomes trivial".
The tree is no more a finite tree, it contains infinite disjunctions.

p. 41 — **Elimination of maximal primes** —

Idea: when rereading dynamically the proof follow systematically the branch $x_i \in \mathfrak{M}$ any time you find a disjunction $x \in \mathfrak{M} \ \vee \ x \notin \mathfrak{M}$ in the proof.

Once you get $1 = 0$ in the quotient, this means $1 \in \langle x_1, \ldots, x_k \rangle$, so this leaf has the good answer and moreover, at the node $\langle x_1, \ldots, x_{k-1} \rangle \subseteq \mathfrak{M}$ you know a concrete $a \in R$ such that $1 - ax_k \in \langle x_1, \ldots, x_{k-1} \rangle$.

So you can follow the proof.

If the proof given for a generic maximal ideal is sufficiently "uniform" you know a bound for the depth of the (infinite branching) tree. So your "finite branching dynamic evaluation" is finite: you get an algorithm.

p. 42 — **Elimination of maximal primes** —

NB: within classical mathematics, using König's lemma, you know that the finite branching dynamic evaluation is finite.

So it is not surprising that the deciphering works: in each case we are able to find a constructive proof for the case of a generic maximal ideal.

But this can be seen rather as an experimental fact.

The methods always works, even we have not a constructive theorem saying that the method always works: Barr's theorem (page 3) is proven only inside classical mathematics.

p. 43 — **Elimination of minimal primes** —

Reasoning with a generic minimal prime in order to prove some concrete thing is something like:
in order to prove that a ring is trivial, show that it does'nt contain any minimal prime ideal.

This cannot be captured by an argument using only first order logic. The corresponding models are not:

(an homomorphic image of) *the ring with a minimal ideal*, but
(an homomorphic image of) *the localization of the ring at a prime ideal.*

p. 44 ——— **Elimination of minimal primes** ———

In order to capture the notion of minimal prime ideal you have to use an infinite disjunction (a disjunction over all elements of the ring).

If $\mathfrak{F}$ is the corresponding maximal filter (complement of the minimal prime) here is the infinite disjunction

$$x \in \mathfrak{F} \quad \vee \quad \bigvee_{y \in \mathfrak{F}} xy \text{ nilpotent}$$

p. 45 ——— **Traverso-Swan theorem** ———

R is *seminormal* iff
If $b^2 = c^3$ *there exists* a *such that* $b = a^3$ *and* $c = a^2$
If R is reduced we have
Theorem: (Swan 1980) *The canonical map* $\mathsf{Pic}(R[X]) \to \mathsf{Pic}(R)$ *is an isomorphism if* R *is seminormal*
This is a schema of first-order theorems

p. 46 ——— **Traverso-Swan Theorem** ———

This Theorem has a concrete interpretation: given polynomials f_i, g_i $(1 \leq i, j \leq n)$ with $\Sigma f_i g_i = 1$, $f_1(0) = g_1(0) = 1$ and $f_i(0) = g_i(0) = 0$ for $i > 1$ let S the ring generated by the coefficients of f_i and g_j

Then the coeffcients of f_i and g_j are in the *seminormal closure* of the subring R generated by the coefficients of the matrix $(f_i g_j)$

This means that we have a chain of elements $q_1, \ldots, q_k \in S$ with $q_{i+1}^2,\ q_{i+1}^3$ in $R[q_1, \ldots, q_i]$ and $S = R[q_1, \ldots, q_k]$

Problem: compute this chain

p. 47 ——— **Traverso-Swan Theorem** ———

An algorithm can be extracted from the abstract proof of Traverso-Swan, which uses a minimal prime ideal in a generic way

Th. Coquand *On seminormality*, Journal of Algebra, to appear

H. Lombardi *Elimination of minimal primes. Seminormal rings*
http://www.lombardi.fr/publis/LectSlides3.pdf

p. 48 ——— **A new approach to constructive mathematics** ———

New: the non-effective arguments contain interesting computational ideas

This is suggested by Hilbert's program: using non-effective methods we can get simple and elegant proofs of concrete results

Computer algebra: dynamical methods (system D5) allow to do computations in the algebraic closure of a discrete field, despite the fact that this algebraic closure may not exist (without any further hypothesis of the field)

p. 49 ——— **A new approach to constructive mathematics** ———

Avoid *complete* factorization: "point-free" statements (statements not in term of prime ideals but in term of basic open for Zariski topology)

Try to get first-order, or even equational statements

Avoid Noetherian hypotheses which are not yet completely understood from a constructive point of view

p. 50 ——— **References (Forster and Serre's theorem)** ———

R. Heitmann
Generating non-Noetherian modules efficiently
Michigan Math. J. 31 (1984), 167-180
O. Forster
Über die Anzahl der Erzeugenden eines Ideals in einem Noetherschen Ring
Math.Z. 84 1964, 80-87
J.-P. Serre
Modules projectifs et espaces fibrés à fibre vectorielle
Séminaire P. Dubreil, Année 1957/1958
R.G. Swan
The Number of Generators of a Module
Math.Z. 102 (1967), 318-322

p. 51 **References (Books: constructive algebra)**

R. Mines, F. Richman, W. Ruitenburg
A Course in Constructive Algebra.
Universitext. Springer-Verlag, (1988).
H. M. Edwards
Essays in Constructive Mathematics.
New York, Springer (2005)

p. 52 **References (constructive Krull dimension)**

A. Joyal
Le théorème de Chevalley-Tarski. Cahiers de Topologie et Géometrie Differentielle, (1975).
L. Español
Constructive Krull dimension of lattices. Rev. Acad. Cienc. Zaragoza (2) 37 (1982), 5–9.
L. Español
Dimension of Boolean valued lattices and rings. J. Pure Appl. Algebra 42 (1986), no. 3, 223–236.
T. Coquand, H. Lombardi, M.-F. Roy
An elementary characterisation of Krull dimension
From Sets and Types to Analysis and Topology (L. Crosilla, P. Schuster, eds.). Oxford University Press. (2005) 239–244.

p. 53 **References (recent constructive papers)**

L. Ducos *Vecteurs unimodulaires et système générateurs.*
Journal of Algebra 297, 566-583 (2005)
L. Ducos, H. Lombardi, C. Quitté and M. Salou.
Théorie algorithmique des anneaux arithmétiques, de Prüfer et de Dedekind.
Journal of Algebra 281, (2004), 604-650.
G. Díaz-Toca, H. Lombardi, C. Quitté
L'algèbre de décomposition universelle.
Actes du colloque TC2006, Grenade 169-184.

p. 54 **References (recent constructive papers)**

H. Perdry
Strongly Noetherian rings and constructive ideal theory
J. Symb. Comput. 37(4): 511-535 (2004)
F.-V. Kuhlmann, H. Lombardi, H. Perdry
Dynamic computations inside the algebraic closure of a valued field. in:
Valuation Theory and its Applications (Vol 2). Fields Institute Communications vol 33. (2003) 133–156.
M.-E. Alonso, H. Lombardi, H. Perdry

Elementary Constructive Theory of Henselian Local Rings.
Preprint 2005.