CONSTRUCTIONS OVER LOCALIZATIONS OF RINGS

ALESSANDRO LOGAR (Trieste) (*)

In this paper we construct a category of effective noetherian rings in which linear equations can be «solved». This category is closed with respect to some important constructions like transcendental extensions, quotients, finite products and localizations with respect to a large class of multiplicatively closed systems. Hence it gives a definition of «constructive» rings.

1. Introduction.

Motivated by the success of the concept of Gröbner bases to attack computational problems in the ideal theory for polynomial rings over a field, several authors have recently suggested different notions of effectivity over a ring powerful enough:

1) to guarantee ideal theoretic computations;

2) to be preserved from a ring $A$ to its polynomial extensions $A[X_1, X_2, \ldots, X_n]$;

3) to allow for a generalization of Buchberger algorithm for Gröbner

(*) Entrato in Redazione il 16 gennaio 1989
bases to polynomial rings with coefficients in a ring satisfying such a notion.

One of the most general of these notions, however quite powerful to produce feasible algorithms in many situations, is the one proposed by Zacharias ([15]; cf. also [4] and [8]).

We recall that if $A$ is an effective noetherian ring, $A$ satisfies Zacharias' conditions if, roughly speaking, in $A$ we can solve linear systems. In this paper we first consider the category $Z$ whose objects are all effective noetherian rings which satisfy such conditions. The category $Z$ results closed with respect to some important constructions like: transcendentals extensions, quotientations, finite products, and it is possible to compute the first $n$-modules of a free resolution of an ideal of an object of $Z$.

A class of rings, which are significant in algebraic geometry applications, is obtained by localizing rings (usually quotients of polynomial rings over a field) at multiplicatively closed systems (usually either finitely generated systems, or complements of a prime ideal [12]). Clearly it is of interest to have effective ideal theory on such rings. However only partial results are known, generally without explicetely given proofs (cf. [14], [8], [4]).

We propose here a class of multiplicatively closed subsets of rings which seems to be sufficiently large to contain all the interesting examples known but which is sufficiently specific to guarantee that Zacharias' conditions are preserved under localizations. In such a way we can construct a subcategory $A$ of $Z$ which contains all the most common rings usually considered and which is closed with respect to localizations (as well as the previously mentioned operations). Hence it probably gives a good example of definition of «constructive» rings.

The author is greatly indebted to Teo Mora for his suggestions, encouragements and patient help.
2. Preliminary results.

Throughout the paper, a ring $A$ is assumed to be Noetherian, commutative, with identity and "explicitly given", meaning that:

- we can represent (with a finite expression) every object of $A$;
- operations: $+,-,*$ are constructive;
- given an element in $A$ it is possible to decide whether it is 0 or not (and so, given two representations we can say if they give the same element).

We will say that an ideal $I$ of $A$ is "given" if we are given a finite set of generators of $I$.

**DEFINITION 2.1.** We will say that $A$ satisfies Zacharias' conditions if the following hold:

i) given $a,a_1,a_2,\ldots,a_m \in A$ it is possible to decide whether $a$ is in the ideal $(a_1,a_2,\ldots,a_m)$ and if so, find $b_1,b_2,\ldots,b_m$ such that $a = \sum b_ia_i$; (that is $A$ is detachable);

ii) given $a_1,a_2,\ldots,a_m \in A$ it is possible to find a finite set of generators for the $A$-module $\{(b_1,b_2,\ldots,b_m) \in A^m | a = \sum b_ia_i \}$; (that is we can determine the first module of syzygies of an ideal (Cf. [15])).

**PROPOSITION 2.2.** The following conditions on $A$ are equivalent:

i) $A$ satisfies Zacharias' conditions;

ii) If the following linear equation:

$$a_1x_1 + a_2x_2 + \ldots + a_mx_m = a \quad \text{with} \quad a,a_1,a_2,\ldots,a_m \in A$$

is given, then it is possible to determine all its solutions (or it is possible to see that there are none);

iii) $A$ satisfies condition i) with $a = 1$ and condition ii) of definition 2.1.
Proof. i)\(\Rightarrow\)ii) by definition; i)\(\Rightarrow\)iii) obvious; iii)\(\Rightarrow\)i): let \(a \in A\), let 
\(B_1 := (\beta_{11}, \beta_{12}, \ldots, \beta_{1m}, \beta_{1m+1})\), 
\(B_2 := (\beta_{21}, \beta_{22}, \ldots, \beta_{2m}, \beta_{2m+1})\), 
\(\ldots\), 
\(B_r := (\beta_{r1}, \beta_{r2}, \ldots, \beta_{rm}, \beta_{rm+1})\), a finite set of generators for the first module of syzygies of the ideal \((a_1, a_2, \ldots, a_m, -a)\). Then \(a \in (a_1, a_2, \ldots, a_m)\) iff 
\(a_1 b_1 + a_2 b_2 + \ldots + a_m b_m + (-a)1 = 0\) that is iff \((b_1, b_2, \ldots, b_m, 1) \in (B_1, B_2, \ldots, B_r)\), hence iff \(1 \in (\beta_{1m+1}, \beta_{2m+1}, \ldots, \beta_{rm+1})\). So if we can determine \(\lambda_1, \lambda_2, \ldots, \lambda_r\) such that \(\sum \lambda_i \beta_{im+1} = 1\), then we can determine \(b_1, b_2, \ldots, b_m\) such that \(a = a_1 b_1 + a_2 b_2 + \ldots + a_m b_m\).

We call \(Z\) the category whose objects \(A\) are all the commutative, Noetherian, explicitly given rings with identity, that satisfy Zacharias' conditions.

*Remark 2.3.* 1) If \(A \in Z\) then we can define the concept of Gröbner basis for any ideal of \(A[X_1, X_2, \ldots, X_n]\) (where \(X_1, X_2, \ldots, X_n\) are indeterminates) and we can define an algorithm which constructs a Gröbner basis of any given ideal as it is shown for instance in [14], [15], [10].

2) If \(A\) is a field, it is shown in [3] and [11] that Gröbner basis for a module \(U \subseteq A[X_1, X_2, \ldots, X_n]\) can also be defined. It is not difficult to see that in the same way we can give the concept of Gröbner basis for any module \(U \subseteq A[X_1, X_2, \ldots, X_n]\) where \(A\) is in \(Z\). It is also possible to construct an algorithm which gives a Gröbner basis from any system of generators of \(U\). The details are very easy but cumbersome, so we omit them.

**Lemma 2.4.** Let \(A \in Z\). If \(I \subseteq A[X_1, X_2, \ldots, X_n]\) is a given ideal, where \(X_1, X_2, \ldots, X_n\) are indeterminates, then it is possible to determine a system of generators for the ideal \(I \cap A\).

*Proof.* It is easy to see that if \(G\) is a Gröbner basis of \(I\) then \(G \cap I\) is a set of generators of \(I \cap A\) (See [4]; prop. 3.3).

**Proposition 2.5.** \(A \in Z\), \(f \in A\), and \(I, J \subseteq A\) are given ideals, then we can determine a finite set of generators for the following ideals:
i) \( I \cap J; \)

ii) \( I + J; \)

iii) \( (0) : f; \)

iv) \( I : f; \)

v) \( I : J; \)

and it is possible to decide if \( I \subseteq J \) (See [4], corollary 3.2).

Proof. i) We have: \( I \cap J = (tI, (1 - t)J)A[t] \cap A \), where \( t \) is an indeterminate and so a system of generators for \( I \cap J \) can be computed by lemma 2.4. An other proof is as follows: let \( I := (f_1, f_2, \ldots, f_m) \) and \( J := (g_1, g_2, \ldots, g_k) \). By hypothesis we can compute a system of generators of the module \( \{(u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_k) \in A^{m+k} | \sum u_if_i + \sum v_i(-g_i) = 0\} \). Let's call it: \( (c_{i1}, c_{i2}, \ldots, c_{im}, d_{i1}, d_{i2}, \ldots, d_{ik}) \), \( i = 1, \ldots, s \). Then it is easy to see that \( I \cap J \) is generated by \( \sum_{j} c_{ij}g_j \), \( i = 1, \ldots, s \).

ii) trivial.

iii) \( (0) : f = \{a \in A | af = 0\} \) and a set of generators for this ideal can be determined because of ii) of def. 2.1.

iv) \( I : f = \{a \in A | af \in I\} \). Let \( \{u_1, u_2, \ldots, u_m\} \) be a set of generators of \( I \cap (f) \), (it can be computed because of i)), then \( u_i = f v_i \), for suitable \( v_i \in A \) (\( v_i \) can be computed because of i) of def. 2.1). Then \( I : f = (0) : f + (v_1, v_2, \ldots, v_m) \).

v) If \( J = (f_1, f_2, \ldots, f_m) \), then \( I : J = \bigcap_{i=1}^{m}(I : f_i) \).

Lemma 2.6. Let \( A \in Z, r \in \mathbb{N}, M, N \subseteq A^r \) \( A \)-modules (given via a finite set of generators); then it is possible to compute a finite set of generators for the \( A \)-module \( M \cap N \).

Proof. We have: \( M \cap N = [(tM, (1 - t)N)A[t]'] \cap A^r \), where \( t \) is an indeterminate. As we have remarked previously, we can compute a Gröbner basis of the module \( (tM, (1 - t)N)A[t]' \). Then (as in prop. 2.5 i)) we can see that the elements of this Gröbner basis that are in \( A^r \) are a set of generators of \( M \cap N \).
Proposition 2.7. Let \( A \in Z, \ n \in \mathbb{N} \) then:

i) given \( B, B_1, B_2, \ldots, B_m \in A^n \), it is possible to decide whether \( B \) is in the \( A \)-module \( (B_1, B_2, \ldots, B_m) \subseteq A^n \) and if so, find \( c_1, c_2, \ldots, c_m \) such that \( B = \sum c_i B_i \);

ii) given \( B_1, B_2, \ldots, B_m \in A^n \), (with \( B_i := (b_{i1}, b_{i2}, \ldots, b_{in}) \), \( i = 1, \ldots, m \)), it is possible to find a finite set of generators for the \( A \)-module \( M := \{(c_1, c_2, \ldots, c_m) \in A^m | \sum c_i B_i = 0 \} \).

Proof. ii) is a consequence of lemma 2.6 in fact:

\[
M = \{(c_1, c_2, \ldots, c_m) \in A^m | \sum c_i B_i = 0 \} = \bigcap_{q=1}^{n} \{C \in A^m | (C|\beta_q) = 0 \},
\]

where \( \beta_q := (b_{1q}, b_{2q}, \ldots, b_{mq}) \).

i) is as follows:

\[
B = c_1 B_1 + c_2 B_2 + \ldots + c_m B_m \quad \text{iff} \quad c_1 B_1 + c_2 B_2 + \ldots + c_m B_m + 1(-B) = 0.
\]

If \( D_i := (d_{i1}, d_{i2}, \ldots, d_{im+1}) \in A^{m+1}, i = 1, \ldots, r \) is a set of generators for the \( A \)-module \( \{(d_1, d_2, \ldots, d_{m+1}) \in A^{m+1} | d_1 B_1 + d_2 B_2 + \ldots + d_m B_m + d_{m+1}(-B) = 0 \} \) (which can be computed by ii) of this proposition) then \( B \in (B_1, B_2, \ldots, B_m) \) iff 1 is in the ideal \( (d_{1m+1}; d_{2m+1}, \ldots, d_{rm+1}) \). So if we can determine \( \lambda_1, \lambda_2, \ldots, \lambda_r \) such that \( \sum \lambda_i d_{im+1} = 1 \), then we can determine \( c_1, c_2, \ldots, c_m \) such that \( B = c_1 B_1 + c_2 B_2 + \ldots + c_m B_m \).

Corollary 2.8. Let \( A \in Z, I \subseteq A \) a given ideal and \( n \in \mathbb{N} \). Then it is possible to compute the first \( n \) modules of a free resolution of \( I \).

Proof. It is an obvious consequence of ii) of the previous proposition.

Remark 2.9. a) Prop. 2.7 is enounced in [8], theorem 1.1.

b) Conditions i) and ii) of prop. 2.7 are considered in [9].
It is clear that Zacharias' conditions and the two conditions of prop. 2.7 are equivalent.


THEOREM 3.1. If $A \in Z$ and if $X_1, X_2, \ldots, X_n$ are indeterminates, then $A[X_1, X_2, \ldots, X_n] \in Z$.

Proof. See [14] or [15].

PROPOSITION 3.2. $Z$ is closed under quotients, that is, if $A \in Z$, and $I \subseteq A$ is a given ideal, then $A/I \in Z$.

Proof. If $A \in Z$, every element of $A/I$ can be represented if we give an element of its equivalence class, so it is clear that $+, -, \cdot$ are constructive in $A/I$. If an element $[a] \in A/I$ is given, $[a] = 0$ in $A/I$ iff $a \in I$, so we can also decide if an element of $A/I$ is 0.

If $[a], [a_1], [a_2], \ldots, [a_s] \in A/I$, $[a] \in ([a_1], [a_2], \ldots, [a_s])$ in $A/I$ iff $a \in (a_1, a_2, \ldots, a_s, f_1, f_2, \ldots, f_r)$ in $A$ (where $I := (f_1, f_2, \ldots, f_r)$) so i) of def. 2.1 is satisfied.

Let $[a_1], [a_2], \ldots, [a_s] \in A/I$, and let $J := (a_1, a_2, \ldots, a_s) \subseteq A$. In the following commutative diagram we define the maps as follows:

$e_1([u_1], [u_2], \ldots, [u_s]) := [a_1 u_1 + a_2 u_2 + \ldots + a_s u_s]$;

$e_2(c_1, c_2, \ldots, c_s, d_1, d_2, \ldots, d_r) := a_1 c_1 + a_2 c_2 + \ldots + a_s c_s + d_1 f_1 + d_2 f_2 + \ldots + d_r f_r$;

$e_3(u_1, u_2, \ldots, u_s, v_1, v_2, \ldots, v_r) := a_1 u_1 + a_2 u_2 + \ldots + a_s u_s + v_1 f_1 + v_2 f_2 + \ldots + v_r f_r$;

$\beta_1$ is the canonical projection;

$\beta_2(c_1, c_2, \ldots, c_s, d_1, d_2, \ldots, d_r) := (c_1, c_2, \ldots, c_s)$;

$\gamma_1$ and $\gamma_2$ are the canonical immersion;

$\beta_3$ and $\gamma_3$ are defined by the universal property of the kernel (and so are the restriction of $\beta_2$ and $\gamma_2$ respectively).
\[
\begin{array}{ccc}
0 & 0 & 0 \\
\uparrow & \uparrow & \uparrow \\
0 \to \ker \alpha_1 \to (A/I)^s & \xrightarrow{\alpha_1} & (I + J)/I \to 0 \\
\uparrow \beta_3 & \uparrow \beta_2 & \uparrow \beta_1 \\
0 \to \ker \alpha_2 \to A^s \oplus A^t & \xrightarrow{\alpha_2} & I + J \to 0 \\
\uparrow \gamma_3 & \uparrow \gamma_2 & \uparrow \gamma_1 \\
0 \to \ker \alpha_3 \to I^s \oplus A^t & \xrightarrow{\alpha_3} & I \to 0 \\
\uparrow & \uparrow & \uparrow \\
0 & 0 & 0 \\
\end{array}
\]

In this diagram every row is exact and also the last two columns, and so, by \(3 \times 3\) lemma ([13], 6.16), the first column is exact. Since \(\beta_3\) is surjective, the image under \(\beta_3\) of a system of generators of \(\ker \alpha_2\) can be computed since \(A \in Z\) and \(\beta_3\), being the restriction of \(\beta_2\), is computable. We can then obtain explicitly a system of generators of \(\ker \alpha_1\) as an \(A\)-module and hence as an \(A/I\)-module, and so the second condition of def. 2.1 is satisfied.

\textbf{Remark 3.3.} From corollary 2.8 and from prop. 3.2 it follows that if \(A \in Z\) and \(I \subseteq A\) is a given ideal then it is possible to compute a free resolution for an ideal of \(A/I\). We observe however that there is a faster way to compute such resolution, using the commutativity of the following diagram (which is a straightforward generalization of the previous one):

\[
\begin{array}{ccc}
0 & 0 & 0 \\
\uparrow & \uparrow & \uparrow \\
0 \to \ker \alpha_1 \to (A/I)^s & \xrightarrow{\alpha_1} & M \to 0 \\
\uparrow \beta_3 & \uparrow \beta_2 & \uparrow \beta_1 \\
0 \to \ker \alpha_2 \to A^s \oplus A^{rt} & \xrightarrow{\alpha_2} & M' \to 0 \\
\uparrow \gamma_3 & \uparrow \gamma_2 & \uparrow \gamma_1 \\
0 \to \ker \alpha_3 \to I^s \oplus A^{rt} & \xrightarrow{\alpha_3} & I^t \to 0 \\
\uparrow & \uparrow & \uparrow \\
0 & 0 & 0 \\
\end{array}
\]
where
\[ M := ([m_1], [m_2], \ldots, [m_i]) \subseteq (A/I)^t \]
([m_i] indicates ([m_{i1}], [m_{i2}], \ldots, [m_{it}]) \in (A/I)^t);

\[ M' := (m_1, m_2, \ldots, m_s, (f_1, 0, \ldots, 0), (f_2, 0, \ldots, 0), \ldots, (f_r, 0, \ldots, 0), (0, f_1, \ldots, 0), (0, f_2, \ldots, 0), \ldots, (0, f_r, \ldots, 0), \ldots, (0, 0, \ldots, f_1), \ldots, (0, 0, \ldots, f_r)) \]

\[ (m_i \text{ indicates } (m_{i1}, m_{i2}, \ldots, m_{it})). \]

We now define the maps as follows:

\[ \alpha_1([u_1], [u_2], \ldots, [u_s]) := [u_1 m_1 + u_2 m_2 + \ldots + u_s m_s]; \]

\[ \alpha_2(c_1, c_2, \ldots, c_s, d_{11}, d_{12}, \ldots, d_{1r}, \ldots, d_{41}, d_{42}, \ldots, d_{4r}) := \]

\[ = \sum_i c_i m_i + \sum_j d_{1j} (f_j, 0, \ldots, 0) + \ldots + \sum_j d_{4j} (0, \ldots, 0, f_j); \]

\[ \alpha_3(c_1, c_2, \ldots, c_s, d_{11}, d_{12}, \ldots, d_{1r}, \ldots, d_{41}, d_{42}, \ldots, d_{4r}) := \]

\[ = \sum_i c_i m_i + \sum_j d_{1j} (f_j, 0, \ldots, 0) + \ldots + \sum_j d_{tj} (0, \ldots, 0, f_j). \]

\[ \beta_1(m_i) := [m_i], i = 1, \ldots, s; \beta_1(f_i, 0, \ldots, 0) = \]

\[ \ldots = \beta_1(0, \ldots, 0, f_i) = 0 \ i = 1, \ldots, r; \]

\[ \beta_2(c_1, c_2, \ldots, c_s, d_{11}, d_{12}, \ldots, d_{1r}, \ldots, d_{41}, d_{42}, \ldots, d_{4r}) := ([c_1], [c_2], \ldots, [c_s]); \]

\[ \gamma_1 \text{ and } \gamma_2 \text{ inclusions.} \]

As in the previous proposition, we can compute a system of generators of \( \ker \alpha_2 \) which gives via \( \beta_3 \) (or \( \beta_2 \)) a system of generators of \( \ker \alpha_1 \).

**Proposition 3.4.** The category \( Z \) is closed for finite products.

**Proof:** If \( A, B \in Z \), then it is clear that +, −, ⋅ are constructive in \( A \times B \) and that it is possible to decide if \( (a, b) \in A \times B \) is 0.

i) of def 2.1 is trivial:

\[ (a, b) \in ((a_1, b_1), \ldots, (a_m, b_m)) \iff a \in (a_1, \ldots, a_m), b \in (b_1, \ldots, b_m). \]
ii) is as follows: if \((a_1, b_1), \ldots, (a_m, b_m) \in A \times B\) then
\[
M := \left\{ ((t_1, \tau_1), \ldots, (t_m, \tau_m)) \mid \sum_{i=1}^{m} (t_i, \tau_i)(a_i, b_i) = 0 \right\} = \\
= \left\{ ((t_1, \tau_1), \ldots, (t_m, \tau_m)) \mid \sum_{i=1}^{m} t_i a_i = 0, \sum_{i=1}^{m} \tau_i b_i = 0 \right\}.
\]

Clearly the \(A \times B\)-module \(M\) is isomorphic to the \(A \times B\)-module:
\[
M' := \left\{ (t_1, \ldots, t_m, \tau_1, \ldots, \tau_m) \mid \sum_{i=1}^{m} t_i a_i = 0, \sum_{i=1}^{m} \tau_i b_i = 0 \right\}.
\]

If \((t_{i_1}, \ldots, t_{i_q}), q = 1, \ldots, p\) is a system of generators for the \(A\)-module \(\left\{ (t_1, \ldots, t_m) \mid \sum_{i=1}^{m} t_i a_i = 0 \right\}\), and if \((\tau_{k_1}, \ldots, \tau_{k_j})\) \(k = 1, \ldots, j\) is a system of generators for the \(B\)-module \(\left\{ (\tau_1, \ldots, \tau_m) \mid \sum_{i=1}^{m} \tau_i b_i = 0 \right\}\), then
\((t_{i_1}, \ldots, t_{i_q}, 0, \ldots, 0), \ldots, (t_{i_p}, \ldots, t_{i_p}, 0, \ldots, 0), (0, \ldots, 0, \tau_{k_1}, \ldots, \tau_{k_j}), \ldots, (0, \ldots, 0, \tau_{j_1}, \ldots, \tau_{j_m})\) is a system of generators of \(M'\).

We remark that by an effective \(PID\) we mean a ring \(A\) which is a \(PID\) and, moreover, such that given \(a, b \in A\) we can:

- compute \(d := \text{MCD}(a, b)\);
- compute \(u, v \in A\) such that \(d = au + bv\);
- if \(c \in A\) decide if \(c\) is a multiple of \(d\) and in this case determine \(k \in A\) such that \(c = dk\).

**Proposition 3.5.** If \(A\) is an effective \(PID\) then \(A \in \mathbb{Z}\).

**Proof.** (cf. [2], [4], [10]). Given \(a, a_1, a_2, \ldots, a_r\) we compute \(b := \text{GCD}(a_1, a_2, \ldots, a_r)\) and \(b_1, b_2, \ldots, b_r\) s.t. \(\sum b_i a_i = b\). \(a \in (a_1, a_2, \ldots, a_r)\) iff \(a = cb\), in which case \(a = \sum cb_i a_i\).

By [10], prop. 3.6, it is possible to compute a basis \(u_1, u_2, \ldots, u_s\) of \((a_1, a_2, \ldots, a_{r-1}) : a_r\); \(u_i a_r \in (a_1, a_2, \ldots, a_{r-1})\) and it is possible to compute \(b_{ij}\) s.t. \(u_i a_r = \sum b_{ij} a_j\).

\[\{(a_{i_1}, a_{i_2}, \ldots, a_{i_{r-1}}, u_i) \mid i = 1, \ldots, s\}\] is then clearly a basis for the syzygies of \((a_1, a_2, \ldots, a_r)\).
PROPOSITION 3.6. Let \( A \in \mathbb{Z} \), \( S \subseteq A \) a multiplicatively closed subset of \( A \). Then if \( I \subseteq A_S \) is a given ideal, we can compute the first \( n \) modules of a free resolution of \( I \) for every \( n \in \mathbb{N} \).

Proof. The only thing to verify is the following: given \( u_1, u_2, \ldots, u_k \in (A_S)^r \), we can determine a system of generators for the \( A_S \)-module 
\[
M := \{(b_1, b_2, \ldots, b_k) \in (A_S)^k | \sum_{i=1}^k b_i u_i = 0\}.
\]

Let \( U \) be the matrix whose rows are the vectors \( u_1, u_2, \ldots, u_k \) and let's call \( U_1, U_2, \ldots, U_r \) its columns.

Then \( M = \{(b_1, b_2, \ldots, b_k) \in (A_S)^k | (B|U_j) = 0, j = 1, \ldots, r\} \), where, as usual, \((..|..)\) is the scalar product. If \( B \in (A_S)^k \) then we can compute \( t_B \in S : t_B B \in A^k \) and \( s_j \in S : s_j U_j \in A^k, j = 1, \ldots, r \). But \((B|U_j) = 0 \) in \( A_S \) iff \( (t_B B|s_j U_j) = 0 \) in \( A_S \) iff there exists \( v \in S \) such that \((v t_B B|s_j U_j) = 0 \) in \( A \).

Let's consider in \( A^k \) the \( A \)-module:

\[
N := \{C := (c_1, c_2, \ldots, c_k) \in A^k | (C|s_j U_j) = 0, j = 1, \ldots, r\}.
\]

If \( C_1, C_2, \ldots, C_p \) is a system of generators for \( N \) (we can compute it by prop. 2.7), then \( C_1, C_2, \ldots, C_p \) is a system of generators of \( M \) as an \( A_S \)-module: \((C_i|U_j) = 1/s_j (C_i|s_j U_j) = 0 \) hence \( C_i \in M \); and if \( B \in M \), then \( t_B B \in A^k \) and \((t_B B|s_j U_j) = t_B s_j (B|U_j) = 0 \) then \( t_B B \in N \), so \( t_B B \) is a linear combination, with coefficients in \( A \) of \( C_1, C_2, \ldots, C_p \) therefore \( B \) is a linear combination, with coefficients in \( A_S \) of \( C_1, C_2, \ldots, C_p \).

COROLLARY 3.7. If \( A \) and \( S \) are as in prop. 3.6, then \( A_S \) satisfies condition ii) of def. 2.1.

DEFINITION 3.8. Let \( A \) be a ring and \( S \subseteq A \) a multiplicatively closed subset. We will call it admissible (a.m.c.s.) if 
\[
S := S_1 + \alpha
\]
where \( \alpha \subseteq A \) is a given ideal and where \( S_1 \) is a multiplicatively closed subset of the following kinds:
- $S_1 := \langle s_1, s_2, \ldots, s_m \rangle$ (that is $S_1$ is finitely generated by $s_1, s_2, \ldots, s_m \in A$).

or

- $S_1 := \bigcup_{i=1}^{n} \mathcal{P}_i$ with $\mathcal{P}_i \subseteq A$ given prime ideals.

Examples of a.m.c.s.: $S := 1 + \alpha$, $S := CT$, $S :=$ finitely generated.

**Proposition 3.9.** Let $A \in \mathbb{Z}$, $S \subseteq A$ an a.m.c.s., then $A_S$ is detachable (i.e. it satisfies i) of def. 2.1).

**Proof.** We have $\frac{a}{s} \in \left( \frac{a_1}{s_1}, \frac{a_2}{s_2}, \ldots, \frac{a_m}{s_m} \right)$ (where $a, a_1, a_2, \ldots, a_m \in A$, $s_1, s_2, \ldots, s_m \in S$) iff $a \in S(a_1, a_2, \ldots, a_m)$ where $S(a_1, a_2, \ldots, a_m) := \{ a \in A | \text{ there exists } t \in S : ta \in (a_1, a_2, \ldots, a_m) \}$ is the saturation of $(a_1, a_2, \ldots, a_m)$ in $A$ w.r.t. $S$.

Moreover, in case $\frac{a}{s} \in \left( \frac{a_1}{s_1}, \frac{a_2}{s_2}, \ldots, \frac{a_m}{s_m} \right)$, it is clear that we can give a representation of $\frac{a}{s}$ of the king required in def. 2.1 i) if we can construct an element $t \in S$ such that $ta \in (a_1, a_2, \ldots, a_m)$.

**Case 1.** Let $S := \langle s_1, s_2, \ldots, s_m \rangle$, and let $I := (a_1, a_2, \ldots, a_m)$ be a given ideal of $A$. In this case we have:

$$S(I) = (I, s_1 T_1 - 1, \ldots, s_m T_m - 1)A[T_1, T_2, \ldots, T_m] \cap A$$

where $T_1, T_2, \ldots, T_m$ are indeterminates. We can compute a Gr"obner basis for the ideal $(I, s_1 T_1 - 1, \ldots, s_m T_m - 1)A[T_1, T_2, \ldots, T_m]$ and from lemma 2.4 we can compute a system of generators of $S(I)$.

Moreover, if $a \in S(I)$ then:

$$a = v f(T_1, \ldots, T_m) + (s_1 T_1 - 1)g_1(T_1, \ldots, T_m) + \ldots + (s_m T_m - 1)g_m(T_1, \ldots, T_m), (v \in I)$$

and $a \cdot s_1 q_1 \cdot s_2 q_2 \cdot \ldots \cdot s_m q_m \in I$ where $q_i$ are the maximum of the degrees of $T_i$ in the polynomials $f, g_1, g_2, \ldots, g_m$. 

Case 2. let $S := \bigcup_{i=1}^{n} P_i$. Then if $a \in A$, $a \in S(I)$ iff there exists $s \notin P_i$ for every $i$ such that $sa \in I$ iff $(I : a) \notin P_i$ for every $i$ and this last condition can be verified using prop. 2.5. Moreover, if such an $s$ exists, then it can be constructed by induction as follows: if $n = 1$, then we have only to find one of the generators of $(I : a)$ that is not in $P_1$.

If $n > 1$ and $(I : a) \notin P_i$ for every $i$, then, by induction, we can construct, for every $j$, $x_j$ s.t. $x_j \notin P_i$, for $i \neq j$. If there exists $j$ such that $x_j \notin P_j$, then $s := x_j$ is the desired element.

Otherwise we put $s := \sum_{i} x_1x_2\ldots x_{i-1}x_{i+1}\ldots x_n$ (cf. [G], prop. 1.11).

Case 3. $S := S_1 + \alpha$ then $a \in S(I)$ iff there exists $s_1 \in S_1$ and there exists $r \in \alpha$ such that $(s_1 + r)a \in I$ iff $s_1a \in I + \alpha a$ iff $a \in S_1(I + \alpha a)$ and so we have reduced the problem to one of the two problems considered above. Suppose $\alpha := (u_1, u_2, \ldots, u_k)$; once we have constructed $s_1 \in S_1$ such that $s_1a \in I + \alpha a$ then we can write $s_1a = \sum b_j a_j + \sum c_j au_j$, that is: $(s_1 - \sum c_j u_j)a \in I$ and $s_1 - \sum c_j u_j \in S$.

As an immediate consequence of prop. 3.9 and prop. 3.6 we have:

COROLLARY 3.10. If $A \in Z$ and if $S \subseteq A$ is an a.m.c.s. then $A_S \in Z$.

4. The category $\mathcal{A}$.

Denote by $A_0$ a class of domains which are contained in $Z$, and denote by $A$ the smallest category that contains $A_0$ and closed for the following operations:

1) transcendental extensions;

2) finite products;
3) quotients;
4) localisations w.r.t. an a.m.c.s.

Therefore $A$ satisfies:
1) $A \in A \Rightarrow A[X] \in A$ ($X$ is an indeterminate);
2) $A \in A$, $I \subseteq A$ a given ideal $\Rightarrow A/I \in A$;
3) $A, B \in A \Rightarrow A \times B \in A$;
4) $A \in A$, $S \subseteq A$ is an a.m.c.s. $\Rightarrow A_S \in A$.

**Proposition 4.1.** The category $A$ is a subcategory of $\mathcal{Z}$.

**Proof.** It follows immediately from teor. 3.1, prop. 3.4, prop. 3.2 and cor. 3.10.

Any object of $A$ can be constructed from one (or more) objects of $A_0$ using a finite number of times 1), 2), 3), and 4).

The following propositions show that some of the operations 1), 2), 3), and 4) commutes.

**Lemma 4.2.** Let $A, B$ be rings, $\alpha \subseteq A \times B$ an ideal, $\mathcal{P} \subseteq A \times B$ a prime ideal, $p : A \times B \rightarrow A$ and $q : A \times B \rightarrow B$ the two projections. Then we have:

1) $\alpha = p(\alpha) \times q(\alpha)$;
2) $\mathcal{P} = \mathcal{P}_1 \times B$ (or $\mathcal{P} = A \times \mathcal{P}_2$) where $\mathcal{P}_1$ is a prime ideal of $A$
   (respectively $\mathcal{P}_2$ is a prime ideal of $B$).

**Proof.** 1) is obvious. 2) $\mathcal{P} = p(\mathcal{P}) \times q(\mathcal{P})$ and $(0, 0) = (1, 0)(0, 1) \in \mathcal{P}$
   therefore $(1, 0) \in \mathcal{P}$, for instance.

**Proposition 4.3.** $A, B$ be rings, $S \subseteq A \times B$ an a.m.c.s. Then we can construct an a.m.c.s. $T \subseteq A$ and an a.m.c.s. $U \subseteq B$ such that:

$$(A \times B)_S \cong A_T \times B_U.$$
Proof. Case 1. \( S = \langle s_1, s_2, \ldots, s_m \rangle \). Then \( (A \times B)_S \cong A_T \times B_U \) where \( T := \langle ps_1, ps_2, \ldots, ps_m \rangle \) and \( U := \langle qs_1, qs_2, \ldots, qs_m \rangle \).

Case 2. \( S = C \bigcup_{i=1}^{n} \mathcal{P}_i, \mathcal{P}_i \subseteq A \times B \) given prime ideals. From lemma 4.2 we know that \( \mathcal{P}_i = \mathcal{R}_i \times B \) or \( \mathcal{P}_i = A \times Q_i \) (\( \mathcal{R}_i \) and \( Q_i \) prime ideals). We can suppose that \( \mathcal{P}_i = A \times Q_i \) for \( i = 1, \ldots, m \) and \( \mathcal{P}_i = \mathcal{R}_i \times B \) for \( i = m + 1, \ldots, n \). Then we have: \( \mathcal{C} \bigcup_{i=1}^{n} \mathcal{P}_i = \left( \mathcal{C} \bigcup_{i=m+1}^{n} \mathcal{R}_i \right) \times \left( \mathcal{C} \bigcup_{i=1}^{n} Q_i \right) \), \( (A \times B)_S \cong A_T \times B_U \) where \( T := C \bigcup_{i=m+1}^{n} \mathcal{R}_i \), \( U := C \bigcup_{i=1}^{n} Q_i \).

Case 3. \( S = 1 + \alpha, \alpha \subseteq A \times B \) a given ideal. Then from lemma 4.2 we obtain: \( S = (1 + p\alpha) \times (1 + q\alpha) \) and so the thesis follows with \( T := 1 + p\alpha \) and \( U := 1 + q\alpha \).

Case 4. \( S = S_1 + \alpha \) with \( S_1 \) finitely generated or \( S_1 = C \bigcup_{i=1}^{n} \mathcal{P}_i \). If we call \( \beta \) the extension of \( \alpha \) in \( (A \times B)_{S_1} \), we have:

\( (A \times B)_S \cong ((A \times B)_{S_1})_{1+\beta} \).

PROPOSITION 4.4. Let \( A \) be a ring, \( I \subseteq A \) an ideal, \( S \subseteq A/I \) an a.m.c.s. and \( p : A \to A/I \) the quotient map. If we define \( T := p^{-1}S \) we have:

1) \( T \) is an a.m.c.s. of \( A \);

2) \( (A/I)_S \cong A_T/I_T \).

Proof. Let \( S := S_1 + \alpha \) with \( \alpha \subseteq A/I \) ideal then \( p^{-1}S = p^{-1}S_1 + p^{-1}\alpha \) and if \( S_1 \) is finitely generated with \( [s_1], [s_2], \ldots, [s_m], s_i \in A \), the \( p^{-1}S_1 = \langle s_1, s_2, \ldots, s_m \rangle + I \); if \( S_1 = C \bigcup_{i=1}^{n} \mathcal{P}_i \) then \( p^{-1}S_1 = C \bigcup_{i=1}^{n} p^{-1}\mathcal{P}_i \) and \( p^{-1}\mathcal{P}_i \) are prime ideals of \( A \).

Observe that the localizations w.r.t. an a.m.c.s. do not commute, in general, with the transcendental extensions, as it is showed by the following example:
EXAMPLE 4.5. Let $\mathcal{P} \subseteq \mathbb{Z}$, $\mathcal{P} := (0)$; $S := C\mathcal{P}$ is an a.m.c.s.. We will prove that $\mathbb{Z}_S[X]$ is not isomorphic to $\mathbb{Z}_T[X]$ for every $T$ a.m.c.s. of $\mathbb{Z}[X]$. Since $\mathbb{Z}_S = \mathbb{Q}$, it suffices to prove that $\mathbb{Q}[X]$ is not isomorphic to $\mathbb{Z}_T[X]$ for every $T$.

Let's assume on the contrary that $\phi : \mathbb{Z}_T[X] \rightarrow \mathbb{Q}[X]$ is a ring isomorphism. It is clear that $\phi(z) = z$ for every $z \in \mathbb{Z}$. To get the contradiction it is enough to find a non constant polynomial $g \in \mathbb{Z}_T[X]$ invertible in $\mathbb{Z}_T[X]$. In fact in this case $\phi(g) = \frac{a}{b}(a, b \in \mathbb{Z})$, hence $\phi(bg) = a = \phi(a)$, therefore $bg = a$, a contradiction.

Case 1. Let $T := \langle s_1, s_2, \ldots, s_m \rangle + \alpha$ with $s_i \in \mathbb{Z}[X]$, $\alpha \subseteq \mathbb{Z}[X]$.

If there exists $s_i \notin \mathbb{Z}$, let $g := s_i$; if $s_i \in \mathbb{Z}$ for every $i = 1, \ldots, m$, but $\alpha \neq (0)$, let be $f \in \alpha$ non constant. In this case it is enough, for example, to put $g := f + s_1$. If $\alpha = (0)$ $\mathbb{Z}_T[X] = \mathbb{Z}_T[X]$, i.e. $\mathbb{Z}_T[X] \cong \mathbb{Q}[X]$ therefore $\mathbb{Z}_T \cong \mathbb{Q}$, a contradiction.

Case 2. $T := C \bigcup_{i=1}^{n} \mathcal{P}_i + \alpha$ and $\alpha \neq (0)$. If $f \in \alpha$ is not constant, let $g := 1 + f \in T$.

Finally we have to consider the case $T := \bigcup_{i=1}^{n} \mathcal{P}_i$. In this case either $X + r \in T$ for some $r \in \mathbb{Z}$, and then we define $g := X + r$, or $X + r \in \mathcal{P}_i$, for every $r$. In this last case there exist an $i \in \{1, 2, \ldots, n\}$ and $r, s \in \{1, 2, \ldots, n+1\}$ with $r \neq s$, such that $X + r, X + s \in \mathcal{P}_i$. Hence $r - s \in \mathcal{P}_i \cap \mathbb{Z}$. But $r - s$ must be invertible in $\mathbb{Z}_T[X]$ since $\phi(r - s)$ is such in $\mathbb{Q}[X]$, therefore there exist $a \in \mathbb{Z}[X], b \in T$ such that $(r - s)a = b$, hence $(r - s)a \notin \mathcal{P}_i$, a contradiction.

As a consequence of the previous propositions and of the (obvious) fact that, if $U, V, W$ are rings, $I \subseteq U$ is an ideal, and $X$ is an indeterminate, then it is possible to construct the following isomorphisms:

$$(V \times W)[X] \cong V[X] \times W[X] \text{ and } U/I[X] \cong U[X]/IU[X],$$

we get that every object of $A$ can be constructed as a quotient
of a finite product of rings \( A_i \), where every ring \( A_i \) is obtained starting from an object of \( A_0 \) localizing w.r.t. an a.m.c.s. and/or adding indeterminates for a finite number of times as is showed by the following scheme:

\[
\begin{array}{c}
A_0 \\
\text{localizing, } \text{w.r.t.} \text{ an a.m.c.s.} \\
\text{transcendental} \\
\text{extensions} \\
\text{product} \\
\text{quotient} \rightarrow \ A \\
\end{array}
\]

Remark 4.6: 1) It is possible to take several different subclasses \( A_0 \) of rings: for instance all the effective PID (considering in such a way every effective field).

2) If the ring of integers \( \mathbb{Z} \) is in \( A_0 \), then every finite field is in \( A \).

3) If \( A \in A \) (or, more generally, \( A \in \mathbb{Z} \)) and if \( f_1, f_2, \ldots, f_m \in A[X_1, X_2, \ldots, X_n] \) where \( X_1, X_2, \ldots, X_n \) are indeterminates, then \( A[f_1, f_2, \ldots, f_m] \in A \) (or \( A[f_1, f_2, \ldots, f_m] \in \mathbb{Z} \)). This is an immediate consequence of the following isomorphism:

\[
A[f_1, f_2, \ldots, f_m] \cong A[Y_1, Y_2, \ldots, Y_m]/J \quad \text{where } Y_1, Y_2, \ldots, Y_m \text{ are indeterminates, and } J := (Y_1 - f_1, \ldots, Y_m - f_m)A[X_1, X_2, \ldots, X_n, Y_1, Y_2, \ldots, Y_m] \cap A[Y_1, Y_2, \ldots, Y_m] \quad (\text{Cfr. [4], corollary 3.2}).
\]

5. A particular case.

Let \( A := k[X_1, X_2, \ldots; X_n] \) and let \( M \subseteq A \) be a maximal ideal. Let's fix a Gröbner basis of \( M \) and let \( \tau : A \to A \) be the reduction, that is \( \tau(f) \) is the reduced of \( f \) w.r.t. the given Gröbner basis of \( M \).

Let \( v_1, v_2, \ldots, v_m \) be a basis of \( \tau(A) \) as a \( k \)-vector space (and so a basis of \( A/M \) as a \( k \)-vector space).

Let \( S := CM \) and let \( \alpha \subseteq A \) be a given ideal (\( \alpha \subseteq M \) so to avoid trivial cases). We want to see how to determine if \( \alpha \in S(\alpha) \) in this particular case. This will allow us to find in some specific cases an algorithm in general faster than the one given in proposition 3.9.
PROPOSITION 5.1. If \( a \in A \), \( a \in S(\alpha) \) iff there exists \( s \in S \) such that \( r(s)a \in (aM+\alpha) \).

Proof: If \( a \in S(\alpha) \) then \( sa \in \alpha \) with \( s \in S \). \( s - r(s) \in M \) and so \( r(s)a \in (aM+\alpha) \).

Conversely: \( r(s)a \in (aM+\alpha) \) then \( r(s)a = am + b \) with \( m \in M \), \( b \in \alpha \), so \( (r(s) - m)a \in \alpha \) and therefore \( a \in S(\alpha) \), since obviously \( r(s) - m \in S \).

Moreover we have: \( r(s) = f_1v_1 + f_2v_2 + \ldots + f_mv_m \) with \( f_i \in k \), hence \( r(s)a \in (aM+\alpha) \) iff there exist \( f_1, f_2, \ldots, f_m \in k \) such that \( (f_1v_1 + f_2v_2 + \ldots + f_mv_m)a \in (aM+\alpha) \). We fix a Gröbner basis \( g_1, g_2, \ldots, g_k \) of \( aM+\alpha \), and we reduce \( r(s)a = (f_1v_1 + f_2v_2 + \ldots + f_mv_m)a \) w.r.t. this Gröbner basis; what we obtain is a polynomial \( F(X_1, X_2, \ldots, X_n, f_1, f_2, \ldots, f_m) \) where \( f_1, f_2, \ldots, f_m \) are all of degree at most 1. Then \( r(s)a \in (aM+\alpha) \) iff there exist \( f_1, f_2, \ldots, f_m \in k \) such that \( F(X_1, X_2, \ldots, X_n, f_1, f_2, \ldots, f_m) \) is the zero polynomial in \( X_1, X_2, \ldots, X_n \). Hence we obtain a homogeneous linear system in \( f_1, f_2, \ldots, f_m \) with coefficients in \( k \).

Therefore \( r(s)a \in (aM+\alpha) \) iff this linear system has a non-trivial solution.

Let now \( P \subseteq A \) be a given prime ideal of dimension \( d \). It is well known that there exist \( d \) indeterminates \( X_{i_1}, X_{i_2}, \ldots, X_{i_d} \) such that \( P \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}] = (0) \) and \( P \cap k[X_{i_1}, X_{i_2}, \ldots, X_{i_d}, X_{i_j}] \neq (0) \) for \( j > d \) (cfr. [6], Cap II, 1 satz 1). In [7] and [5] it is shown that to determine \( X_{i_1}, X_{i_2}, \ldots, X_{i_d} \) we need only to compute the Gröbner basis of \( P \) with respect to the lexicographical order on the monomials.

Let \( M := PB \) (where \( B := k(X_{i_1}, X_{i_2}, \ldots, X_{i_d}) [X_1, \ldots, X_{i_1-1}, X_{i_1+1}, \ldots, X_n] \)).

Let \( S := CP \), and let \( \alpha \subseteq A \) be a given ideal (contained in \( P \)).

PROPOSITION 5.2. if \( a \in A \), then \( a \in S(\alpha) \) iff \( a \in S'(\beta) \) where \( \beta := \alpha B \), \( S'(\beta) \) is the saturated ideal of \( \beta \) w.r.t. \( S' := B \setminus M \), and \( a \) is considered as an element of \( B \).

Proof: \( a \in S(\alpha) \) iff \( \frac{a}{1} \in \alpha A_P \). But \( A_P = B_M \subseteq Q(A) \) then
\[ \frac{a}{l} \in \alpha A \iff \frac{a}{l} \in \beta B_M \iff a \in S'(\beta). \]

From this proposition and the previous consideration we have:

**PROPOSITION 5.3.** If \( a \in A, \ P \subseteq A \) is a prime ideal, and \( \alpha(\subseteq P) \) is a given ideal, then we can establish if \( a \in S(\alpha) \) \( (S := A \setminus P) \) solving a suitable linear system in \( K := k(X_{i_1}, X_{i_2}, \ldots, X_{i_d}) \).

**REFERENCES**


*Dipartimento di Matematica*

*Università di Trieste*

*Ple Europa, 1*

*34100 Trieste (Italy)*