Rez. exemplar

Appeared in
Proc. "Rekursive Kombinatorik",
Münster, Germany, May 1983,
LNCS. 171, Springer 1984,
pp. 137-161.

A CRITICAL-PAIR/COMPLETION ALGORITHM IN REDUCTION RINGS

B. BUCHBERGER

May 1983

CAMP-Publ.-Nr.: 83-21.0
Type: Technical Report

Sponsored by: Österr. Fonds zur Förderung
der wissenschaftl. Forschung
Projekt P4567

Working Group CAMP-LINZ
(Computer-Aided Mathematical Problem Solving)

Address: Ordinariat Mathematik III
Johannes Kepler Universität
A4040 Linz, Austria (Europe)

A CRITICAL-PAIR/COMPLETION ALGORITHM IN REDUCTION RINGS

B.Buchberger

Mathematisches Institut
Johannes Kepler Universität
A4040 LINZ, Austria

ABSTRACT

In 1965, the author introduced a "critical-pair/completion" algorithm that starts from a finite set F of polynomials in $K[x_1,...,x_n]$ (K a field) and produces a set G of polynomials such that the ideals generated by F and G are identical, but G is in a certain standard form (G is a "Gröbner-basis"), for which a number of important decision and computability problems in polynomial ideal theory can be solved elegantly. In this paper, it is shown how the critical-pair/completion approach can be extended to general rings. One of the difficulties lies in the fact that, in general, the generators of an ideal in a ring do not naturally decompose into a "head" and a "rest" (left-hand side and right-hand side). Thus, the crucial notions of "reduction" and "critical pair" must be formulated in a new way that does not depend on any "rewrite" nature of the generators. The solution of this problem is the starting point of the paper. Furthermore, a set of reduction axioms is given, under which the correctness of the algorithm can be proven and which are preserved when passing from a ring R to the polynomial ring $R[x_1,...,,x_n]$. $Z[x_1,...,x_n]$ is an important example of a ring in which the critical-pair/completion approach is possible.

INTRODUCTION

In /Buchberger 65, 70/ the "critical-pair/completion" approach for solving algorithmical problems in polynomial ideal theory was introduced: Let F be a (finite) set of polynomials in $K[x_1,\ldots,x_n]$ (K a field). In order to solve an algorithmic problem for the ideal Ideal(F) generated by F, first transform F into a certain canonical form G (which was called "Gröbner-basis" in /Buchberger 76/) such that Ideal(F) = Ideal(G) and then solve the problem for G.

Essentially, G is a "Gröbner-basis" iff a certain reduction relation $\rightarrow_G$ induced by G on $K[x_1,\ldots,x_n]$ has the Church-Rosser property (see definition below). It turns out that, in fact, a number of important algorithmic problems for polynomials ideals Ideal(G) can be easily solved as soon as G is a Gröbner-basis, whereas they are extremely complex in general. (Examples: deciding congruence; canonical simplification modulo polynomial "side relations"; computing the multiplication table of the residue class ring modulo polynomial ideals; computation of the elimination ideals of a polynomial ideal; solution of linear diophantine equations in the polynomial ring; computation of the Hilbert function; deciding the solvability of systems of algebraic equations; etc.). Of course, the intrinsic computational complexity of these problems can not be annihilated by this approach either and, in fact, it reappears in the construction of the Gröbner-bases. The advantage of the method, however, is that, as soon as a Gröbner-basis G for F has been constructed once and for all, quite diverse algorithmic problems for Ideal(F) (=Ideal(G)) can be solved easily. Also, for a specific input F, the algorithm for constructing a Gröbner-basis for F may stop quickly (for example, in the extreme case, when F is already a Gröbner-basis) and, then, gives us the legitimation to use the simple algorithmic methods available for Gröbner-bases.

The two basic ideas in our 1965 algorithm for the construction of Gröbner-bases are the consideration of "critical pairs" of polynomials in the basis F and the successive "completion" of the basis by the differences of the reduced forms of critical pairs. More concretely, the algorithm has the following overall structure

```
G:= F
while not all "critical pairs" of G are considered do
```

```
$(b_1,b_2)$ := a "critical pair" of G which has not yet been considered
$(b_1,b_2)$ := the reduced forms of $b_1,b_2$ w.r.t. G;
    if $b_1 \neq b_2$ then "complete" G by $b_1-b_2$.
```

In the context of general first order terms instead of polynomials, the same two ideas appeared later (1967) in the well known algorithm of /Knuth-Bendix 67/, which now is widely used in computer algebra and software technology, in particular in the manipulation of abstract data type specifications. In fact, the critical-pair/ completion algorithm shown above can as well be read as the Knuth-Bendix algorithm if the appropriate notion of "critical pair" is used and "complete G by b_1-b_2" is replaced by "complete G by the equation $b_1=b_2$".

In subsequent papers (1976, 1979, 1981, 1982, 1983) the present author has been working on the improvement and the complexity analysis of the 1965 algorithm. Starting from 1976, also quite a few other authors (R. Schrader, M. Lauer, W. Trinks, D. Spear, M. Bergman, G. Zacharias, F. Winkler, S. Schaller, M. Pohst, D. Yun, F. Mora, J. Guiver, D. Bayer, H. Möller, D. Lazard) worked on the algorithm and gave various applications and generalizations. The special case of the algorithm where all polynomials in F have the form t_1-t_2 (t_1 and t_2 power products) was reinvented two times (in /Ballantyne, Lankford 81/ and in /Bauer 81/). In this case, the algorithm yields a decision procedure for finitely generated commutative semigroups. A fairly complete bibliography on the algorithm with further motivation and hints to applications may be found in /Buchberger, Loos 82/. Some very recent papers on the algorithm are /Buchberger 83/, /Winkler, Buchberger 83/ and /LLopis 83/.

Various authors generalized the algorithm to $Z[x_1,\ldots,x_n]$ (/Lauer 76/) and to $R[x_1,\ldots,x_n]$, where R is a ring that satisfies certain axioms (/Trinks 77/, /Spear 77/, /Zacharias 79/, /Schaller 79/). Roughly, these axioms are:

8321-2

(R1) the decision problem "$f \in \mathrm{Ideal}(F)$?" ($f \in R$, $F \subseteq R$) must have an algorithmical solution and

(R2) a finite set of generators for the solutions of linear equations in R can be found algorithmically.

In these papers it is also shown that, if R satisfies these axioms, then also $R[x_1,\ldots,x_n]$ satisfies the axioms: if R satisfies the axioms then (a variant of) the above algorithm may be applied to sets $F \subseteq R[x_1,\ldots,x_n]$ yielding Gröbner bases G for which the problems mentioned in (R1) and (R2) are seen to be easily solvable.

/Bergman 78/ is a generalization of the algorithm to the case of associative R-algebras. However, the "left-hand sides" of the generators are supposed to be pure power products. /Bauer 81/ shows also how the commutative semigroup case can be viewed in a much broader perspective.

In the present paper, we present a different generalization of the algorithm, which in various respects is more satisfactory than the generalizations given so far:

(1) The generalization works in general rings (satisfying certain axioms (A)), not only in polynomial rings.

(2) The algorithm preserves its extremely simple structure. A general concept of "critical pair" specializes to a concrete computational step in the various example domains. In particular, it specializes to the authors algorithm in the case $K[x_1,\ldots,x_n]$, whereas in the generalizations reported in the literature at the place where "critical pairs" have to be computed in the 1965 algorithm, linear equations have to be solved, essentially.

(3) The formulation of the axioms (A) involves only the basic ring operations, a noetherian order relation and variables over ring elements.

(4) The notion of "reduction" is basic (and not the notion of "ideal" or "equation").

(5) The construction of Gröbner-bases in $R[x_1,\ldots,x_n]$ does not presuppose the solution of equally hard algorithmical problems in R (as it is the case in the generalizations cited above, see (R1) and (R2)).

(6) The properties (A), again, carry over from R to $R[x_1,\ldots,x_n]$. However, the proof of this fact does not involve the solvability of algorithmic problems of the type (R1), (R2) either.

(7) The construction has various degrees of freedom: Given R, a wide variety of different sets M of "multipliers", of different noetherian orderings $\succ$ on R

and of different notions of reduction "steps" can be chosen. Every choice leads to a correct algorithm. The particular choice can be made in depen-dence or complexity considerations and other criteria.

(1)-(7) may be conceived as a first attempt to achieve a "constructive ring theory" based on the notion of "reduction" with a "critical-pair/completion algorithm" for enforcing the Church-Rosser property for reduction relations as the basic algorithmic tool.

8321-3

The specific difficulty of this objective is twofold:

(1) The notion of "reduction" and of "critical pair" in polynomial rings (and also in the general framework of rewrite rules) presupposes the distinction of a "head" and a "rest" ("left-hand side" and a "right-hand side") of the generators (generating equations). In general rings, however, one has to find a way to formulate the concepts of "reduction" and "critical pair" without any appeal to an underlying "left-right" structure of elements.

(2) The axioms (A), at the same time, should be strong and weak. Strong axioms (A) make the correctness proof for the algorithm easier. Weak axioms extend the class of rings, to which the approach is applicable. In the proof of "R satisfies (A) ==> $R[x_1,\ldots,x_n]$ satisfies (A)" strong axioms (A) would be nice in the premise, whereas weak axioms (A) would be nice in the conclusion!

(3) The definition of "critical pair", at the same time, should be strong and week. A strong definition guarantees that only a few critical pairs remain. Hopefully in a given ring R, only finitely many cirtical pairs should remain because we aim at a critical-pair/completion algorithm which needs to consider only finitely many critical pairs. A weak definition leaves us with more critical pairs, which makes the proof of the correctness theorem for the algorithm easier. Furthermore, the definition of "critical pair" should be such that, in the special case $K[x_1,\ldots,x_n]$, it specializes exactly to the author's 1965 concept.

Quite a few attempts were necessary in order to arrive at appropriate concepts of "reduciblity" and "critical pair" and to get a feasible balance for the axioms (A). Finally, our notions of "reducibility" and "critical pair", in addition to being appropriate, seem to be fairly natural. Still, most of our axioms (A) seem to be natural. Only (A5) (see below) can not be motivated easily.

From now on, the presentation will be "bottom-up": Section 1. presents the general definition of "reduction" and "critical pairs", which is applicable to arbitrary rings. Section 2. introduces axioms for rings, in which the critical-pair/completion algorithm can be correctly executed. For the moment, such rings will be called "reduction rings". In Section 3., the central theorem and its proof is presented: for checking the Church-Rosser property of the reduction relations in reduction rings, the consideration of the critical pairs is sufficient. Based on this theorem, the general critical-pair/completion algorithm for reduction rings is formulated. In Section 4. it is shown that, if R is a reduction ring, then also $R[x_1,\ldots,x_n]$ is a reduction ring. In Section 5., the example of the ring **Z** is considered . It turns out, that our algorithm specializes to Euclid's algorithm (in fact, to a whole spectrum of Euclidean algorithms, which seems to be very satisfactory from an aesthetical, historical and systematical point of view). In Section 6., the particular example of $Z[x_1,\ldots,x_n]$ is considered in more detail. The reader who is interested in this example only, after having read the definition of the reduction relation $\rightarrow_C$ in Section 1., can immediately pass to the description of the algorithm in Section 3. and the explanation of the subalgorithms in Sections 5. and 6. He, then, should be able to compute Gröbner-bases for ideals in $Z[x_1,\ldots,x_n]$ and to program the algorithm for this domain. In section 7., Z_m and $Z_m[x_1,\ldots,x_n]$ is considered.

8321-4

1. REDUCTION AND CRITICICAL PAIRS

Let R be a commutative ring with 1 (possibly with zero divisors), $<$ a noetherian (partial) order relation on R and $M \subseteq R$ (set of "multipliers"). (Typed variables: a,b,c,d,e for elements in R; C,D for subsets of R; l,m for elements in M; i,j,k,n for natural numbers. $<$ is noetherian means that there are no infinite sequences $a_1 > a_2 > a_3 > \ldots$)

<u>Definition</u>: $a \rightarrow_c b$ iff $a - m.c = b$ for some m and

$a \succ b$

(read: "a <u>reduces</u> to b modulo c").

<u>Definition</u>: $a \rightarrow_C b$ iff $a \rightarrow_c b$ for some $c \in C$

(read: "a <u>reduces</u> to b modulo C").

(For reduction relations $\rightarrow$, the following additional notation is used: $\leftarrow$ is the inverse relation to $\rightarrow$. $\leftrightarrow$, $\rightarrow^+$, $\rightarrow^*$, $\leftrightarrow^*$ are the symmetric, transitive, reflexive-transitive, and reflexive-symmetric-transitive closure of $\rightarrow$, respectively. Furthermore:

$a \rightarrow$ iff $a \rightarrow b$ for some b

(read: "a is <u>reducible</u> (w.r.t. $\rightarrow$)").

$\underline{a}$ iff $a \rightarrow b$ for no b (i.e. not $a \rightarrow$)

(read: "a is <u>irreducible</u>" or "a is <u>in normal form</u>").

$a \downarrow^* b$ iff $a \rightarrow^* d \leftarrow^* b$ for some d

(read: "a and b have a <u>common successor</u>").

$a \leftrightarrow^*(\prec d)\ b$ iff for some $e_0,\dots,e_n$:

$a=e_0 \leftrightarrow e_1 \leftrightarrow e_2 \leftrightarrow \dots \leftrightarrow e_{n-1} \leftrightarrow e_n=b$ and

$e_0,e_1,\dots,e_n \prec d$

(read: "a and b can be <u>connected below</u> d").

The notation is used quite flexibly: for example, "$a \rightarrow^* d \leftarrow^* b$" is an abbreviation for "$a \rightarrow^* d$ and $d \leftarrow^* b$"; "$\leftarrow_{c_1} a \rightarrow_{c_2}$" is an abbreviation for "$a \rightarrow_{c_1}$ and $a \rightarrow_{c_2}$"; etc.).

<u>Definition</u>: a is a common reducible for c_1 and c_2 iff $\leftarrow_{c_1} a \rightarrow_{c_2}$.

<u>Definition</u>: $c_1 \overset{a}{\Delta} c_2$ iff a is a common reducible for c_1 and c_2 and for no m_1,m_2:

$a-m_1c_1 \leftarrow_{c_1} a \rightarrow_{c_2} a-m_2c_2$ and

$(a-m_1c_1 \rightarrow_{c_2} a-m_1c_1-m_2c_2$ or

$a-m_2c_2 \rightarrow_{c_1} a-m_2c_2-m_1c_1)$

(read: "a is a non-trivial common reducible for c_1 and c_2").

(It will become clear in Section 3. why, in the above situation, the reducibility of a is called "non-trivial". Roughly, "trivial" common reducibilities present no problem in establishing the Church-Rosser property for the reducibility relations considered. The "diagram"

$$\begin{tikzcd}
 & a \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\
b_1 := a - m_1c_1 & & a - m_2c_2 =: b_2
\end{tikzcd}$$

can always be "closed"

$$\begin{tikzcd}
 & a \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\
b_1 \arrow[dr, "*"'] & & b_2 \arrow[dl, "*"] \\
 & \bullet &
\end{tikzcd}$$

in the case of a "trivial" reducibility.)

8321-5

Definition: $c_1 \underline{\overset{a}{\Delta}} c_2$ iff $c_1 \overset{a}{\Delta} c_2$ and for no $a' < a$: $c_1 \overset{a'}{\Delta} c_2$
(read: "a is a minimal non-trivial common reducible for c_1 and c_2").

(It will turn out that the minimal non-trivial common reducibles play the crucial role in establishing the Church-Rosser property: the "critical pairs", to which the minimal non-trivial common reducibles can be reduced, are the only pairs of elements where the Church-Rosser property might be injured).

Definition: b_1, b_2 form a critical pair for c_1, c_2 w.r.t. a iff

$$c_1 \overset{a}{\underline{\Delta}} c_2 \quad \text{and} \quad b_1 \leftarrow_{c_1} a \rightarrow_{c_2} b_2.$$

Although the reduction $\rightarrow_C$ looks very much as "one directed step" in the ideal theoretical congruence $\equiv_C$, in general, it is not true that $\leftrightarrow_C^{*} = \equiv_C$. (We use the notation:

$$a \equiv_C b \qquad \text{iff} \quad a = b + \sum_{1 \leq i \leq n} d_i.c_i \qquad \text{for some } n,\ d_i \varepsilon R,\ c_i \varepsilon C$$

(read: "a is congruent b modulo (the ideal generated by) C").)

However, under very weak additional assumptions (see M(5) and (A2) below), $\leftrightarrow_C^{*} = \equiv_C$ can be derived and, of course, this is what is needed in order that knowledge about the reduction relations (in particular, the knowledge about the Church-Rosser property) can be used for an algorithmic solution to ideal theoretical problems.

2. REDUCTION RINGS

Definition: A commutative ring R with 1 (possibly with zero divisors) together with a noetherian (partial) order relation $<$ on R and a set $M \subseteq R$ (set of "multipliers") constitute a reduction ring iff the following axioms are satisfied:

Axioms for multipliers:

(M0) 0 not in M

(M1) $1 \varepsilon M$

(M2) if $m \varepsilon M$ then $-m \varepsilon M$

(M3) if $m_1, m_2 \varepsilon M$ then $m_1.m_2 \varepsilon M$

(M4) if $m \varepsilon M$ then m is not a zero divisor

(M5) if $a \equiv_C b$ then there exist n, $m_i \varepsilon M$, $c_i \varepsilon C$ such that

$$a = b + \sum_{1 \leq i \leq n} m_i.c_i$$

(In the case of rings without zero divisors, sometimes M may be taken equal to R-{0}. Of course, in this case, the axioms (M) are trivially satisfied. However, the consideration of $M \neq R$ provides an additional degree of freedom. For example, in the case of polynomial rings over fields, by taking M:= set of monomials, we obtain the original reduction relation in /Buchberger 65, 70, 76/. In the presence of zero divisors, the availability of sets $M \neq R$ is crucial.) (M1),(M2) could be replaced by (M1') $-1 \in M$, because then $1= (-1).(-1) \in M$ by (M1') and (M3), and, if $m \in M$, then $-m = (-1).m \in M$ again by (M1') and (M3).

Axioms for the reduction relation:
(in the case when no zero divisors are in R):

(A1) if $a \neq 0$ then $a \succ 0$
(A2) if $a \rightarrow_c b$ then $a + d \downarrow_c^* b + d$
(A3) if $a \rightarrow_c b$ then $m.a \leftrightarrow_c m.b$
(A4) if $b_1 \leftarrow_c a \rightarrow_c b_2$ then $b_1 \leftrightarrow_c^{*}(\prec a)\ b_2$

(A5) if $c_1 \overset{a}{\Delta} c_2$ then there exist $a' \preceq a$ and m such that
$c_1 \overset{a'}{\underline{\Delta}} c_2$ and
for all c: (if $a'+c \prec a'$ then $a+m.c \prec a$)
8321-6

In the case when zero divisors are present the axioms (A2) and (A4) must be formulated in the following way:

(A2) if $a \rightarrow_c a-m'.c$ then there exist l_i,m_j such that

$$a + d \rightarrow_c a + d - l_1c \rightarrow_c \ldots \rightarrow_c a + d - l_1c - \ldots l_kc =$$

$$= a - m'.c + d - m_1c - \ldots - m_nc \leftarrow_c \ldots \leftarrow_c a - m'.c + d - m_1c \leftarrow_c a - m'.c + d$$

and

$$l_1 + \ldots + l_k = m' + m_1 + \ldots + m_n$$

(A4) if $a - m_1c \leftarrow_c a \rightarrow_c a -m_2c$

then there exist l_i such that

$$a - m_1c \leftrightarrow_c a - m_1c - l_1c \leftrightarrow_c \ldots$$

$$\ldots \rightarrow_c a - m_1c - l_1c - \ldots - l_kc = a - m_2c,$$

$$a - m_1c - l_1c, \ldots , a - m_1c - l_1c - \ldots - l_kc < a, \text{ and}$$

$$m_1 + l_1 + \ldots + l_k = m_2$$

In the proofs we will not prosuppose that R contains no zero divisor. We will, therefore, work with the second version of (A2) and (A4). In rings without zero divisors we only have to check whether the first version of (A2), (A4) is satisfied because, then, the second version is satisfied also.

(These axioms connect the ring operations with reduction. Note that no appeal is made to the solution of "higher" algorithmic problems in R, as was the case with (R1), (R2). Stronger forms of the axioms, which naturally might come to ones mind, do not even hold in the original example of polynomial rings. For example, (A2) can not be replaced by: if $a \rightarrow_c b$ then $a+d \rightarrow_c b+d$.)

Axioms of effectiveness:

Addition, multiplication, reduction and the formation of critical pairs must be effectively possible in R (as will be explained in more detail in Section 3. after the presentation of the critical-pair/completion algorithm).

Axioms of termination:

(T1) There exists no infinite sequence of subsets D_1, D_2,... of R such that $\text{Red}(D_1) \subset \text{Red}(D_2) \subset \ldots$
(where "c" is strict set inclusion, and $\text{Red}(D) := \{ a \mid a \rightarrow_D \}$).

(T2) For all c_1, c_2: $\{ a \mid c_1 \overset{a}{\underline{\Delta}} c_2 \}$ is finite.

(These axioms will guarantee the termination of the general critical-pair/completion algorithm.)

Some more remarks about the axioms:

1. Note that the axioms, essentially, are formulated in terms of the arithmetical operations in the ring and the reduction relation $\rightarrow_C$. No appeal to the notion of an ideal is made. Actually, the whole investigation described in this paper could be carried out without any appeal to ideals at all ((M5) could be canceled), i.e., finally, what one gets is always a decision procedure for $\longleftrightarrow_C$. Only, if we want that our investigation is relevant for ideal theory then we must try to establish $\longleftrightarrow_C = \equiv_C$, which can be done by using (M5).

8321-7

2. (M5) is equivalent to

(M5') for all a there exist $m_i \in M$, $n \in \mathbf{N}$ such that

$$a = \sum_{1 \leq i \leq n} m_i$$

(Proof: Assume (M5). Consider $C := \{1\}$ and an arbitrary a. Then $a \equiv_C 0$. Hence, by (M5), $a = 0 + \sum_{1 \leq i \leq n} m_i c_i$ for certain $m_i \in M$, $c_i \in C$, i.e. $a = \sum (m_i . 1) = \sum m_i$.

Conversely, assume (M5'). If $a \equiv_C b$, then $a = b + \sum_{1 \leq i \leq n} d_i . c_i$ for certain $d_i \in R$, $c_i \in C$. By (M5'), each of the d_i can be represented in the form:

$$d_i = \sum_{1 \leq j \leq n_i} m_{i,j}.$$

Hence, $a = b + \sum_i (\sum_j m_{i,j}) c_i = b + \sum_{i,j} (m_{i,j}\ c_i)$, which is a representation of the form required in (M5).)

(M5') shows more clearly the power of (M5). For example, in the case of polynomial rings, (M5) = (M5') displays the fact that every polynomial can be built up from monomials. (Compare the notion of a "graded ring"!).

It should also be noted that the stronger versions of (A2), (A4) are only needed for carrying the axioms from R to $R[x_1,\dots,x_n]$ but not for the proof of the main theorem.

3. By the generalized Newman-Lemma (see below), (A4) is equivalent to

   (A4') $\rightarrow_c$ has the Church-Rossen property.

4. The motivation for (A5) will become clear in the proof of the main theorem. Roughly, (A5) guarantees that in every "non-trivial" situation

$$\begin{tikzcd} & a \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\ {} & & {} \end{tikzcd}$$

   we can find a "non-trivial" situation

$$\begin{tikzcd} & a' \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\ {} & & {} \end{tikzcd}$$

   "below" a such that if the second diagram can be closed

$$\begin{tikzcd} & a' \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\ {} \arrow[rr, no head, squiggly] & & {} \end{tikzcd}$$

   then this closure can be "lifted" to the level of a by the multiplication of all intermediate points by a suitable constant multiple m.

3. CHURCH-ROSSER PROPERTY AND GRÖBNER BASES

The following definition is standard:
$\rightarrow$ has the Church-Rosser property iff for all a,b: (if $a \leftrightarrow^* b$ then $a \downarrow^* b$).

The importance of the Church-Rosser property for reduction relations stems from the following well known fact:
If $\rightarrow$ has the Church-Rosser property then

$a \leftrightarrow^* b$ iff $S(a) = S(b)$

(where S is an arbitrary function (a "canonical simplifier") satisfying:

$$S(a) = \begin{cases} a, & \text{if } \underline{a} \\ S(b), & \text{if } a\rightarrow \text{ and } b \text{ is some element such that } a \rightarrow b). \end{cases}$$

8321-8

This means that, for Church-Rosser relations $\rightarrow$,"$a \leftrightarrow^* b$" can be decided by simply comparing $S(a)$ and $S(b)$. (A review of known results on Church-Rosser relations may be found, for example, in /Buchberger, Loos 82/). In the case of those rings, in which $\leftrightarrow_C^* = \equiv_C$ holds, one hence has an easy decision procedure for the ideal theoretic congruence $\equiv_C$ as soon as it is known that the reduction relation $\rightarrow_C$ has the Church-Rosser property. (In fact, as was pointed out in the introduction, also a number of other algorithmic ideal theoretical problems can then be solved easily).

Unfortunately, for an arbitrary (finite) C, in general $\rightarrow_C$ is not Church-Rosser. The critical-pair/completion approach sketched in the introduction now suggests to "complete" C by suitable elements (derived from critical pairs) without changing the ideal until a set D is reached, whose coressponding reduction relation $\rightarrow_D$ is Church-Rosser. The feasibility of this approach in the general context of this paper is established by the following theorem.

Presupposition: From now on presuppose that R, $<$, M constitute a reduction ring.

Main Theorem: $\rightarrow_C$ has the Church-Rosser property iff

for all c_1, $c_2 \in C$ and a such that $c_1 \overset{a}{\underline{\Delta}} c_2$
there exists a critical pair b_1, b_2 for c_1, c_2 w.r.t.a such that
$b_1 \leftrightarrow_C^*(<a)\ b_2$.

(Note that the condition formulated in this theorem is even weaker than announced in the rough sketch of the method: we do not require all critical pairs to have a common successor and, also, we do not insist on the existence of common successors but only require that b_1, b_2 may be connected "below" a).

Using this theorem, the following algorithm can be shown to correctly solve the following problem.

Problem: Given: A finite set $C \subseteq R$.
Find: A finite set $D \subseteq R$ such that

$\leftrightarrow_C^* = \leftrightarrow_D^*$ and

$\to_D$ has the Church-Rosser property.

<u>Algorithm</u>:

```
D:= C
B:= { ({$c_1$,$c_2$},a) | $c_1$,$c_2$ ε C, $c_1 \overset{a}{\underline{\Delta}} c_2$ }

while  B ≠ ∅ do

    ({$c_1$,$c_2$},a) := one triple out of B
    B                 := B - { ({$c_1$,$c_2$},a) }
    ($b_1$,$b_2$)         := two elements such that  $b_1 \leftarrow_{c_1} a \to_{c_2} b_2$
    ($b_1$,$b_2$)         := ($S_D(b_1)$,$S_D(b_2)$)

    if $b_1 \neq b_2$ then

            c:= $b_1$-$b_2$
            B:= B u { ({c,c'},a) |  c'εD, $c \overset{a}{\underline{\Delta}} c'$ }
            D:= D u {c}.
```

(Here, S_D is a "simplifier" for $\to_D$ of the kind described above. The "algorithm" is effective in the precise sense of algorithm theory provided that the basic operations appearing in the instructions of the algorithm can be effectively executed in the ring considered. This means that, in addition to the axioms (M), (A), and (T) one must stipulate for reduction rings that the ring operations, the determination of a "b such that a $\to_D$ b, in case a $\to_D$", and the determination of all "a such that $c_1 \overset{a}{\underline{\Delta}} c_2$" are effective operations. Stated differently, the above algorithm is an algorithm "relative" to the effectiveness of the operations mentioned above. A reasonable stipulation for making reduction effective would be: one requires that

(E1) $<$ is decidable on R,

(E2) there exists an algorithm A such that for all a,c:

$$a \to_C \Longrightarrow \begin{array}{l} a - A(a,c).c < a, \\ A(a,c) \in M. \end{array}$$

"$a \rightarrow_C$" is then also decidable, assuming that M is a decidable subset of R.

8321-9

Due to the following lemma the above problem can also be stated in the following form.

Lemma: $\leftrightarrow_C^* \; = \; \equiv_C$.

Problem: Given: A finite set $C \subseteq R$.

Find: A finite set $D \subseteq R$ such that

$\equiv_C \; = \; \equiv_D$ and

$\rightarrow_D$ has the Church-Rosser property.

Summarizing, this means that, for an ideal generated by an arbitrary set C, the above algorithm constructs a new basis D for the same ideal such that $\rightarrow_D$ has the Church-Rosser property and, hence, an easy decision procedure for the congruence $\equiv_C \; = \; \equiv_D$ is available (namely, $a \equiv_C b$ iff $S_D(a) = S_D(b)$). Extending the terminology introduced in /Buchberger 76/, sets D, whose corresponding reduction relation $\rightarrow_D$ is Church-Rosser, will be called Gröbner bases.

Proof of the lemma:

If $a \leftrightarrow_C^* b$ then $a \equiv_C b$: easy! (Iterate: if $a \rightarrow_C b$ then $a \equiv_C b$).

If $a \equiv_C b$ then $a \leftrightarrow_C^* b$:

Proceed by induction on n in $a = b + \sum_{1 \leq i \leq n} m_i c_i$ (where the m_i, by (M5), can be chosen in M and the c_i are in C). The case n=0 is clear. Case n≠0:

$$a = b + \sum_{1 \leq i \leq n} m_i c_i = b + \sum_{1 \leq i \leq n-1} m_i c_i + m_n c_n \overset{(1)}{\leftrightarrow_{c_n}^*} b + \sum_{1 \leq i \leq n-1} m_i c_i \overset{(\text{ind. hyp.})}{\leftrightarrow_C^*} b.$$

(1) is a special instance of the following general law in reduction rings: $d \leftrightarrow_C^* d+m.c$. (Proof: Case $m.c=0$ trivial. In case $m.c \neq 0$, $m.c \rightarrow_C 0$ and, hence, by (A2) $d+m.c \leftrightarrow_C^* d+0 = d$.)

Proof of the theorem:

The proof can be structured by the following "generalized Newman-Lemma", which seems to be the strongest form of a Newman-type lemma known so far, i.e. it singles out a very weak condition under which the Church-Rosser property of reduction relations can be guaranteed. The author introduced this lemma and its proof in /Winkler, Buchberger 83/, where it is used for a different purpose.

Generalized Newman-Lemma: Let $\rightarrow$ and $>$ be binary relations on a set T, $>$ noetherian and $\rightarrow \subseteq >$. Then $\rightarrow$ has the Church-Rosser property iff for all $a, b_1, b_2 \in T$:

$$\text{if} \quad b_1 \leftarrow a \rightarrow b_2 \quad \text{then} \quad b_1 \leftrightarrow^*(<a)\; b_2.$$

For proving the theorem, we take arbitrary $a, b_1, b_2 \in R$, $c_1, c_2 \in C$ and assume

(1) $b_1 \leftarrow_{c_1} a \rightarrow_{c_2} b_2$.

According to the generalized Newman-Lemma it suffices to show

(2) $b_1 \leftrightarrow_C^*(<a)\; b_2$.

For notational convenience, $\rightarrow$ etc. will be used instead of $\rightarrow_C$ etc. in this proof. Also, the axioms (M) about the multipliers will be used tacitly.

Case: for some m_1, m_2: $a-m_1c_1-m_2c_2 \leftarrow_{c_2} a-m_1c_1 \leftarrow_{c_1} a \rightarrow_{c_2} a-m_2c_2$:
In this case (where a is a "trivial common reducible" for c_1 and c_2)

$$b_1 \overset{(A4)}{\leftrightarrow_{c_1}^*(<a)} a-m_1c_1 \overset{(3)}{\leftrightarrow^*(<a)} a-m_2c_2 \overset{(A4)}{\leftrightarrow_{c_2}^*(<a)} b_2.$$

8321-10

(3) needs some more details: $a \rightarrow_{c_1} a-m_1c_1$ implies $a-m_2c_2 \rightarrow_{c_1}^* a-m_1c_1-m_2c_2$, by (A2). Now, $a-m_1c_1 \rightarrow_{c_2} a-m_1c_1-m_2c_2$ by case assumption. Hence, (3) holds.

Case: for some m_1, m_2: $a-m_1c_1 \leftarrow_{c_1} a \rightarrow_{c_2} a-m_2c_2 \rightarrow_{c_1} a-m_2c_2-m_1c_1$: analogous.

Remaining Case: In this case $c_1 \overset{a}{\Delta} c_2$ holds (this is the "non-trivial" case: a is a "non-trivial common reducible" for c_1 and c_2). Using (A5), choose an $a' \leq a$ and an m such that

(4) $c_1 \overset{a'}{\underline{\Delta}} c_2$ and

(5) for all c: if $a'+c < a'$ then $a+m.c < a$.

By the assumption of the theorem, one can choose b_1', b_2' such that

(6) $b_1' \leftarrow_{c_1} a' \rightarrow_{c_2} b_2'$ and

(7) $b_1' \leftrightarrow^*(< a')\ b_2'$.

Let m_1, m_2 be such that

(8) $b_1' = a' - m_1 c_1$, $b_2' = a' - m_2 c_2$.

Because of (7) one can choose $e_0, \dots, e_k$ such that

(9) $b_1' = e_0 \leftrightarrow e_1 \leftrightarrow e_2 \leftrightarrow \dots \leftrightarrow e_{k-1} \leftrightarrow e_k = b_2'$ and

(10) $e_0, \dots, e_k < a'$.

Now, let $f_0, \dots, f_k$ be such that

(11) $e_i = a' + f_i$ (for $i=0,\dots,k$).

(10),(11), and (5), then, imply

(12) $a + m.f_i < a$ (for $i=0,\dots,k$).

Furthermore, using (A3), from (9) one gets

(13) $m.e_0 \leftrightarrow m.e_1 \leftrightarrow \dots \leftrightarrow m.e_k$

and, using (A2),

(14) $(a-m.a') + m.e_0 \ \downarrow^* \ (a-m.a') + m.e_1 \ \downarrow^* \ \dots \ \downarrow^* \ (a-m.a') + m.e_k$.

Now, by (11),

(15) $(a-m.a') + m.e_i = a + m.f_i$ (for $i=0,\dots,k$).

By (8), (9), and (11),

(16) $a + m.f_0 = a - m.m_1.c_1$, $a + m.f_k = a - m.m_2.c_2$.

Hence, by (12),(14),(15), and (16), one finally obtains

(17) $a - m.m_1.c_1 \ \leftrightarrow^*(< a)\ a - m.m_2.c_2$.

Because of (12) and (16), one also has

(18) $a \rightarrow_{c_1} a - m.m_1.c_1$, $a \rightarrow_{c_2} a - m.m_2.c_2$.

Hence, one is allowed to use (A4) obtaining

(19) $b_1 \leftrightarrow_{c_1}^*(< a)\ a - m.m_1.c_1$, $a - m.m_2.c_2 \leftrightarrow_{c_2}^*(< a)\ b_2$.

(17) together with (19) yields (2).

Summary of proof:

One has to "close"
$$\begin{tikzcd} & a \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\ b_1 & & b_2 \end{tikzcd}$$
in order to obtain
$$\begin{tikzcd} & a \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\ b_1 \arrow[rr, phantom, "\leftrightarrow^*(< a)"] & & b_2 \end{tikzcd}$$

By (A5) and the assumption of the theorem one can find $a' \underline{<} a$, m, m_1, m_2 such that

$$\begin{tikzcd}
 & a' \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\
b_1' & & b_2' \\
=a-m_1c_1 & & =a-m_2c_2
\end{tikzcd}$$

can be closed:

$$\begin{tikzcd}
 & a' \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\
b_1' \arrow[rr, "{}^*(\prec a')"] & & b_2'
\end{tikzcd}$$

and the closed triangle can be "lifted" to the level of a by an appropriate multiplication with m and an addition of a-m.a' yielding

$$\begin{tikzcd}
 & a \arrow[dl, "c_1"'] \arrow[dr, "c_2"] & \\
b_1'' \arrow[rr, "{}^*(\prec a)"] & & b_2'' \\
=a-mm_1c_1 & & =a-mm_2c_2
\end{tikzcd}$$

Finally using (A4), the desired interconnection between b_1 and b_2 can be established:

$$\begin{tikzcd}
 & & & a \arrow[dlll, "c_1"'] \arrow[dl, dashed, "c_1"'] \arrow[dr, "c_2"] \arrow[drrr, "c_2"] & & & \\
b_1 \arrow[rr, "{}_{c_1}^*(\prec a)"] & & b_1'' \arrow[rr, "{}^*(\prec a)"] & & b_2'' \arrow[rr, "{}_{c_2}^*(\prec a)"] & & b_2
\end{tikzcd}$$

8321-11

Partial Correctness of the Algorithm:

The partial correctness of the algorithm can be proven by the method of inductive assertions. The inductive assertion for the while-loop is:

$\equiv_C = \equiv_D$,

if $(\{c_1,c_2\},a) \in B$ then $c_1,c_2 \in D$, $c_1 \overset{a}{\underline{\Delta}} c_2$

if $c_1,c_2 \in D$, $c_1 \overset{a}{\underline{\Delta}} c_2$, and $(\{c_1,c_2\},a)$ not in B
then for some b_1, b_2: $b_1 \leftarrow_{c_1} a \rightarrow_{c_2} b_2$ and $b_1 \rightarrow_D^*(\prec a)\ b_2$.

Knowing the theorem, the other details of the correctness proof are easy.

Termination of the Algorithm:

The termination proof for the algorithm uses the axioms (T1) and (T2). (T2) guarantees that the block within the while-loop is always left after finitely many steps. Furthermore, one can prove:

(1) Let D_i be the value of the variable D after the if-statement in the while-loop has been executed for the i-th time ($D_0 = C$). Then

$$\mathrm{Red}(D_0) \subset \mathrm{Red}(D_1) \subset \mathrm{Red}(D_2) \subset \ldots$$

Knowing (1), it is clear that the while-loop can be executed only a finite number of times: Either the if-statement is executed only finitely many times, hence D stabilizes and B will get exhausted, or the if-statement is executed infinitely many times and hence, by (1), a sequence $\mathrm{Red}(D_0) \subset \mathrm{Red}(D_1) \subset \mathrm{Red}(D_2) \subset \ldots$ would exist in contradiction to (T2).

Proof of (1): Surely, $D_i \subseteq D_{i+1}$ and therefore $\mathrm{Red}(D_i) \subseteq \mathrm{Red}(D_{i+1})$ for $i=0,1,\ldots$ One has to show that $\mathrm{Red}(D_i) \neq \mathrm{Red}(D_{i+1})$. Let b_1, b_2 be the elements constructed in the algorithm before the if-statement is entered for the (i+1)-th time. One knows

(2) b_1 and b_2 are irreducible with respect to D_i and

(3) $b_1 \neq b_2$.

One can show:

(4) at least one of b_1, b_2 is reducible with respect to D_{i+1}

and, hence, $\mathrm{Red}(D_i)$ and $\mathrm{Red}(D_{i+1})$ can not be equal. For proving (4), the following law holding in arbitrary reduction rings may be applied:

(5) if $a \neq b$ then $a \downarrow^*_{a-b} b$.

(Proof: $a \neq b$ implies $a-b \to_{a-b} 0$. From this, by (A2), one gets $a \downarrow^*_{a-b} b$.)

Applying (5) to (3) yields

(6) $b_1 \to^*_{b_1-b_2} d \leftarrow^*_{b_1-b_2} b_2$ for some d.

Case $b_1=d=b_2$: not possible because of (3).

Case $b_1 \neq d$: In this case there is a d' such that $b_1 \to_{b_1-b_2} d' \to^*_{b_1-b_2} d$. Hence, $b_1 \to_{D_{i+1}}$ because $b_1-b_2 \in D_{i+1}$.

Case $b_2 \neq d$: Analogous: $b_2 \to_{D_{i+1}}$.

4. POLYNOMIAL REDUCTION RINGS

In the following, the typed variables f,p,q,r are used for polynomials and the typed variables s,t,u for n-variate power products (special polynomials of the form $x_1^{i_1} \ldots x_n^{i_n}$). Let $>_T$ be an arbitrary total ordering on the power products satisfying

(PP1) for all $s \neq 1$: $1 <_T s$

(PP2) for all s,t,u: if $s <_T t$ then $s.u <_T t.u$.

C(p,t) will denote the coefficient of the polynomial p at the power product t. H(p,t) and L(p,t) denote polynomials such that

$$p = H(p,t) + C(p,t).t + L(p,t)$$

and

$$\text{for all } s <_T t\text{: } C(H(p,t),s) = 0,$$
$$\text{for all } s >_T t\text{: } C(L(p,t),s) = 0.$$

H(p,t) and L(p,t) are called the "higher" and the "lower" part of p relative to t (w.r.t.$<_T$). LC(p), LP(t), LM(t) and R(p) are the "leading coefficient", the "leading power product", the "leading monomial" and the "rest" of p (w.r.t.$<_T$) in the usual sense. Hence,

$$p = LM(p) + R(p),$$
$$LM(p) = LC(p).LP(p).$$

Theorem: If R, M, $<$ constitute a reduction ring then $R[x_1,\ldots,x_n]$, $M\{x_1,\ldots,x_n\}$, $\ll$ constitute a reduction ring, where

$R[x_1,\ldots,x_n]$:= set of polynomials with coefficients in R,

$M\{x_1,\ldots,x_n\}$:= $\{ m.s \mid m \in M$, s is a power product $\}$,

$p \ll q$ iff there is a t such that

$$H(p,t) = H(q,t),$$
$$C(p,t) < C(q,t).$$

Remark: Of course, one also could formulate the theorem, first, for the transition from R to $R[x]$ and then obtain the above theorem by iteration. However, the direct transition from R to $R[x_1,\ldots,x_n]$ opens the possibility to use a big variety of different orderings $<_T$ and, hence, orderings $\ll$ as an additional degree of freedom, which may prove useful for the algorithmic aspects pursued in this paper. The iteration of the transition from R to $R[x]$ implies that, finally, the power products in $R[x_1,\ldots,x_n]$ would be ordered according to the "purely lexicographical" ordering.

Proof: The proof of this theorem is quite tedious:

Proof that $\ll$ is a noetherian partial ordering: It is easy to show that $\ll$ is a partial ordering. It is well known that (PP1) and (PP2) imply that $<_T$ is noetherian, see for example /Buchberger 80/. From this and the assumption that $<$ is noetherian it can be proven that $\ll$ is noetherian. Similar proofs are contained in /Lauer 76/, /Trinks 78/, /Zacharias 78/, /Schaller 79/ and other papers. In order to make this paper self-contained, the details of the proof are given.

We first show that $\ll$ is transitive. Let $p \ll q \ll r$. We have to show $p \ll r$. Let t and t' be such that

$$\begin{aligned}
p &= H(p,t) + C(p,t).t + L(p,t),\\
q &= H(q,t) + C(q,t).t + L(p,t),\\
&\quad H(p,t) = H(q,t),\ C(p,t) < C(q,t),\\
q &= H(q,t') + C(q,t').t' + L(q,t'),\\
r &= H(r,t') + C(r,t').t' + L(r,t'),\\
&\quad H(q,t') = H(r,t'),\ C(q,t') < C(r,t').
\end{aligned}$$

Case $t \gg t'$: In this case,

$$H(p,t) = H(q,t) = H(r,t),$$

$$C(p,t) < C(q,t) < C(r,t), \text{ i.e. } C(p,t) < C(r,t).$$

Hence, $p \ll r$.

8321-13

Case $t \ll t'$: In this case,

$H(p,t') = H(q,t') = H(r,t')$,

$C(p,t') = C(q,t') < C(r,t')$.
Hence, $p \ll r$.

We next show that $\ll$ is irreflexive: Assume $p \ll p$, then $C(p,t) < C(p,t)$ for some t. This contradicts the fact that $<$ is irreflexive.

We now show that $\ll$, restricted to $M\{x_1,\dots,x_n\}$, is noetherian. Note that for $a.s$, $b.t \in M\{x_1,\dots,x_n\}$, a, $b \neq 0$:

(1) $a.s \ll b.t \iff (s <_T t \text{ or } s = t \text{ and } a < b)$.

We use noetherian induction on $<_T$ in the following statement.
For all s:
there is no infinite sequence $a_1t_1 \gg a_2t_2 \gg \dots$ with $t_1 = s$.

Let s be arbitrary, but fixed and assume that
$a_1t_1 \gg a_2t_2 \gg \dots$
is an infinite sequence with $t_1 = s$.

Case $t_1 = t_2 = \dots$: In this case, by(1),
$a_1 > a_2 > \dots$
in contradiction to the fact that $<$ is noetherian.

Case $t_1 = t_2 = \dots = t_i \neq t_{i+1}$ for some i: In this case

$t_i >_T t_{i+1}$ (because $t_i <_T t_{i+1}$, by(1), would imply
$a_it_i \ll a_{i+1}t_{i+1}$).
Now, $a_{i+1}t_{i+1} \gg a_{i+2}t_{i+2} \gg \dots$ would be an infinite sequence with $t_{i+1} <_T s$. This contradicts the induction hypothesis.

We now show that $\ll$, on $R[x_1,\dots,x_n]$ is noetherian. We use noetherian induction on $\ll$, restricted to $M\{x_1,\dots,x_n\}$. In the following statement:
For all a,s:
there is no infinite sequence $p_1 \gg p_2 \gg \dots$
with $LM(p_1) = a.s$.

Case $LM(p_1) = LM(p_2) = \dots$: In this case

$$R(p_1) \gg R(p_2) \gg \dots$$

is an infinite sequence with $LM(R(p_1)) \ll LM(p_1) = a.s$. This contradicts the induction hypothesis.

Case $LM(p_1) = LM(p_2) = \dots = LM(p_i) \neq LM(p_{i+1})$

Subcase $LP(p_i) <_T LP(p_{i+1})$: not possible because, in this case, p_i would be $\ll p_{i+1}$.

Subcase $LP(p_i) = LP(p_{i+1})$: In this case
$LC(p_i) > LC(p_{i+1})$ and hence, by(1),
$LM(p_i) \gg LM(p_{i+1})$.

Subcase $LP(p_i) >_T LP(p_{i+1})$: In this case, again by(1),
$LM(p_i) \gg LM(p_{i+1})$.

In both subcases

$$p_{i+1} \gg p_{i+2} \gg \dots$$

would be an infinite sequence with

$$LM(p_{i+1}) \ll LM(p_i) = LM(p_1) = a.s$$

in contradiction to the induction hypothesis.

8321-14

<u>Proof</u> of (M0),...,(M4): Easy. For (M5) note that, by (M5') in R, all elements $a \in R$ can be represented in the form $a = \sum m_i$. In more detail, let $p \equiv_F q$, where $F \subseteq R[x_1,\dots,x_n]$,
i.e. $p = q + \sum_{1 \leq i \leq n} a_i.t_i.f_i$ for certain $a_i \in R$, t_i power products, $f_i \in F$, $n \in \mathbf{N}$.

By(M5'), each of the a_i may be represented in the form $a_i = \sum_{1 \leq j \leq k_i} m_{i,j}$,
where $m_{i,j} \in M$. Hence

$$p = q + \sum_i (\sum_j m_{i,j}) t_i f_i = q + \sum_{i,j} (m_{i,j} t_i) f_i .$$

This is a representation of the form required in (M5) for $R[x_1,\ldots,x_n]$, because all the $m_{i,j}t_i \in M[x_1,\ldots,x_n]$.

Proof of (A1): Clear.

Proof of (A2), (A3), (A4): All these proof are based on the fact that

(RED) $p \rightarrow_f p - m.u.f$ iff $(C(p,t) - m.LC(f) \prec C(p,t)$, where $t = u.LP(f))$.

Proof of (RED), $\Longleftarrow$: If the condition on the right-hand side is fulfilled, then clearly $p - m.u.f = H(p,t) + (C(p,t) - m.LC(f)).t + L(p,t) - m.u.R(f) \ll p$, i.e. $p \rightarrow_f p - m.u.f$ according to the definition of $\rightarrow_f$.

Proof of (RED), $\Longrightarrow$: If $p \rightarrow_f p$-$m.u.f$ then $p - m.u.f \ll p$.

Define $t := u.LP(f)$. Then

$$p - m.u.f = H(p,t) + C(p,t).t + L(p,t) - m.u.LC(f).LP(f) - m.u.R(f) =$$

$$= H(p,t) + (C(p,t) - m.LC(f)).t + L(p,t) - m.u.R(f).$$

One has to show

(1) $C(p,t) - m.LC(f) \prec C(p,t)$.

$C(p,t) - m.LC(f) \succ C(p,t)$ is not possible because otherwise $p - m.u.f$ would be $\gg p$.

$C(p,t) - m.LC(f) = C(p,t)$ is not possible because otherwise $m.LC(f) = 0$, i.e. m would be a zero divisor ($LC(f) \neq 0$ since $f \neq 0$: $f = 0$ would imply $p - m.u.f = p$ instead of $p - m.u.f \ll p$!)

$C(p,t) - m.LC(f)$ incomparable with $C(p,t)$ is not possible either because, otherwise, $p - m.u.f$ would be incomparable with p.

Hence, (1) is the only remaining possibility.

Proof of (A2): Assume $p \rightarrow_f p - m'.u.f$ and let r be arbitrary, but fixed. One has to construct $m_1,\dots,m_x$, $u_1,\dots,u_x$, $n_1,\dots,n_y$, $v_1,\dots,v_y$ such that

$$(1)\quad p + r \rightarrow_f p + r - m_1u_1f \rightarrow_f \dots \rightarrow_f p + r - m_1u_1f - \dots - m_xu_xf =$$

$$= p - m'uf + r - n_1v_1f - \dots - n_yv_yf \rightarrow_f \dots \rightarrow_f$$
$$\rightarrow_f p - m'uf + r - n_1v_1f \rightarrow_f p - m'uf + r$$

and

$$(2)\quad m_1u_1 + \dots + m_xu_x = m'u + n_1v_1 + \dots + n_yv_y.$$

Let $t := u.LP(f)$. From the assumption we get

$$p - m'uf = H(p,t) + (C(p,t) - m'.LC(f)).t + L(p,t) - m'uR(f).$$

and, by (RED),

8321-15

$$(3)\quad C(p,t) - m'.LC(f) < C(p,t).$$

Now,

$$p + r = H(p,t) + H(r,t) + (C(p,t) + C(r,t)).t + L(p,t) + L(r,t),$$

$$p - m'uf + r = H(p,t) + H(r,t) + (C(p,t) - m'.LC(f) + C(r,t)).t +$$
$$+ L(p,t) - m'uR(f) + L(r,t).$$

Because of (3) one has $C(p,t) \rightarrow_{LC(f)} C(p,t) - m'.LC(f)$. Hence, by (A2) in R, there are $m_1,\dots,m_x$, $n_1,\dots,n_y$ such that

$$(4)\quad C(p,t) + C(r,t) \rightarrow_{LC(f)} C(p,t) + C(r,t) - m_1.LC(f) \rightarrow_{LC(f)} \dots \rightarrow_{LC(f)}$$

$$\rightarrow_{LC(f)} C(p,t) + C(r,t) - m_1.LC(f) - \dots - m_x.LC(f) =$$

$$= C(p,t) + C(r,t) - m'.LC(f) - n_1.LC(f) - \dots - n_y.LC(f) \rightarrow_{LC(f)}$$

$$\rightarrow_{LC(f)} \dots \rightarrow_{LC(f)} C(p,t) + C(r,t) - m'.LC(f) - n_1.LC(f) \rightarrow_{LC(f)}$$

$$\rightarrow_{LC(f)} C(p,t) + C(r,t) - m'.LC(f).$$

and

(5) $m_1 + \ldots + m_x = m' + n_1 + \ldots + n_y$.

Define now:

$$u_1 := \ldots := u_x := v_1 := \ldots := v_y := u.$$

Then clearly (2) holds. For proving (1), note that

(6) $p + r - m_1u_1f - \ldots - m_iu_if =$

$$\begin{aligned} &H(p,t) + H(r,t) + \\ &+ (C(p,t) + C(r,t) - m_1.LC(f) - \ldots - m_i.LC(f)).t + \\ &+ L(p,t) + L(r,t) - m_1u_1R(f) - \ldots - m_iu_iR(f). \end{aligned}$$

By (4) one, hence, has

$$p + r \to_f p + r - m_1u_1f \to_f \ldots \to_f p + r - m_1u_1f - \ldots m_xu_xf.$$

Similarly,

$$\begin{aligned} &p - m'uf + r \to_f p - m'uf + r - n_1v_1f \to_f \ldots \to_f \\ &\to_f p - m'uf + r - n_1v_1f - \ldots - n_yv_yf. \end{aligned}$$

Finally, by (5),

$$\begin{aligned} &p + r - m_1u_1f - \ldots - m_xu_xf = \\ &= p - m'uf + r - n_1v_1f - \ldots - n_yv_yf. \end{aligned}$$

Thus, (1) is proven.

Proof of (A3): Assume $p \to_f q$. Let m' and v be arbitrary, but fixed. One has to show

(1) $m'vp \to_f m'vq$.

Let m,u be such that $q = p - muf$. Then by (RED)

$$C(p,t) - m.LC(f) < C(p,t), \text{ where}$$

$$t := u.LP(f).$$

$$q = H(p,t) + (C(p,t) - mLC(f)).t + L(p,t) - muR(f).$$

Hence,

(2) $C(p,t) \rightarrow_{LC(f)} C(p,t) - m.LC(f)$.

Now

$$m'vp = m'vH(p,t) + m'.C(p,t).vt + m'vL(p,t),$$

$$m'vq = m'vH(p,t) + (m'.C(p,t) - m'm.Lc(f)).vt + m'vL(p,t) - m'mvuR(f),$$

$$m'vq = m'v(p - muf) = m'vp - m'mvuf,$$

$$m'mvu \in M\{x_1,\dots,x_n\},$$

$$m'vH(p,t) = H(m'vp,vt),$$

$m'.C(p,t) \rightarrow_{LC(f)} m'.C(p,t) - m'.m.LC(f)$ (by (2) and (A3) in R).

Hence, by (RED), one has (1).

Proof of (A4): Assume $p - m_1u_1f \leftarrow_f p \rightarrow_f p - m_2u_2f$. We have to show that there exist $l_1,\dots,l_k$, $v_1,\dots,v_k$ such that

(1) $p - m_1u_1f \leftrightarrow_f$

$p - m_1u_1f - l_1v_1f \leftrightarrow_f$

...

$p - m_1u_1f - l_1v_1f - \dots - l_kv_kf = p - m_2u_2f$,

(2) $p - m_1u_1f - l_1v_1f - \dots - l_jv_jf \ll p$ (for $j = 1,\dots,k$),

(3) $m_1u_1 + l_1u_1 + \dots + l_2v_k = m_2u_2$

By (RED),

(4) $C(p,t_1) - m_1.LC(f) < C(p,t_1)$,

(5) $C(p,t_2) - m_2.LC(f) < C(p,t_2)$, where

(6) $t_1 = u_1.LP(f)$, $t_2 = u_2.LP(f)$.

Let $q_1 := p - m_1u_1f$,

$q_2 := p - m_2u_2f$.

Case $t_1 >_T t_2$: In this case

(7) $C(q_2,t_1) = C(p,t_1)$.

Consider now

(8) $q_2' := q_2 - m_1u_1f$.

Then, by (3),

(9) $C(q_2,t_1) - m_1.LC(f) < C(q_2,t_1)$.

Hence, by (8) and (RED),

(10) $q_2 \rightarrow_f q_2'$.

From $p \rightarrow_f q_2$, $q_1 = p - m_1u_1f$, (8) and (A2), which we have already proven for $R[x_1,\dots,x_n]$, one obtains:

there exist $m_1',\dots,m_x'$, $u_1',\dots,u_x'$, $n_1',\dots,n_y'$, $v_1',\dots,v_y'$ such that

(11) $p - m_1u_1f \rightarrow_f p - m_1u_1f - m_1'u_1'f \rightarrow_f \dots$

$\rightarrow_f \underbrace{p - m_1u_1f - m_1'u_1'f - \dots - m_x'u_x'f}_{} =$

$= p - m_2u_2f - m_1u_1f - n_1'v_1'f - \dots - n_y'v_y'f \rightarrow_f \underbrace{p - m_2u_2f - n_1'v_1'f - \dots - n_{y-1}'v_{y-1}'f}_{}$

$\rightarrow_f \dots \rightarrow_f p - m_2u_2f - m_1u_1f - n_1'v_1'f \rightarrow_f \underbrace{p - m_2u_2f - n_1'v_1'f \dots - n_{y-i}'v_{y-i}'f}_{}$

$\rightarrow_f p - m_2u_2f - m_1u_1f \rightarrow_f \underbrace{p - m_2u_2f}_{}$,

$m_1'u_1' + \dots + m_x'u_x' = m_2u_2 + n_1'v_1' + \dots + n_y'v_y'$.

Hence,

$\overset{?}{=}$, weil

$\underbrace{\quad}_{} - n_{y-i+1}' - n_y' =$

$\underbrace{\quad}_{} =$

$\underbrace{\quad}_{} - n_{y-i+1}' - \dots n_y'$

$\overset{?}{=}$, weil

$\underbrace{\quad}_{} - n_y'v_y'f =$

$= \underbrace{\quad}_{} =$

$= \underbrace{\quad}_{} - n_y'v_y'f$

(12) $p - m_1u_1f \leftarrow_f \dots \leftarrow_f$

$\leftarrow_f p - m_1u_1f - m_1'u_1'f - \dots - m_x'u_x'f \leftarrow_f$

$\leftarrow_f \underbrace{p - \cancel{m_2u_2f} - m_1u_1f - m_1'u_1'f - \dots - m_x'u_x'f + n_y'v_y'f}_{} \leftarrow_f$

$\dots \leftarrow_f p - \cancel{m_2u_2f} - m_1u_1f - m_1'u_1'f - \dots - m_x'u_x'f +$

$+ n_y'v_y'f + \dots + \underbrace{n_1'v_1'f}_{n_{(y-i+1)}'v_{(y-i+1)}'f} \leftarrow_f$

$\leftarrow_f \underbrace{p - \cancel{m_1u_1f} - m_1'u_1'f - \dots - m_x'u_x'f +}_{}$

$$+ n_y'v_y'f + \ldots + n_1'v_1'f = p - m_2u_2f,$$

where, by (11), all the intermediate polynomials are $\ll$ p. This means that (1), (2), (3) are satisfied by taking as $l_1,v_1,\ldots,l_k,v_k$ the following objects

$$m_1',u_1',\ldots,m_x',u_x';\ -n_y',v_y',\ldots,-n_1',v_1';\ -m_1,u_1.$$

Case $t_1 <_T t_2$: analogous.

Case $t_1 = t_2$: (i.e. $u_1 = u_2$): in this case, by (4),(5)

8321-16a

(13) $b_1 \overset{*}{\leftarrow}_{LC(f)} C(p,t) \overset{*}{\rightarrow}_{LC(f)} b_2$, where

(14) $b_1 := C(p,t) - m_i.LC(f)$ $(i=1,2)$ and

(15) $t := t_1$ $(=t_2)$.

By (A4) in R, there exist $l_1,\ldots,l_k$ such that

(16) $b_1 = C(p,t) - m_1.LC(f) \rightarrow_{LC(f)}$

$$C(p,t) - m_1.LC(f) - l_1.LC(f) \rightarrow_{LC(f)}$$

$$\ldots \qquad\qquad \rightarrow_{LC(f)}$$

$$C(p,t) - m_1.LC(f) - l_1.LC(f) - \ldots - l_k.LC(f) =$$

$$= C(p,t) - m_2.LC(f) = b_2$$

(17) $C(p,t) - m_1.LC(f) - l_1.LC(f) - \ldots - l_j.LC(f) < C(p,t)$ (for $j = 1,\ldots,k$)

and

(18) $m_1 + l_1 + \ldots + l_k = m_2$. Let $u := u_1$. From (16),(17),(18) it follows that

(19) $p - m_1.u.f \rightarrow_f$

$p - m_1.u.f - l_1.u.f \rightarrow_f$

$\ldots \qquad \rightarrow_f$

$p - m_1.u.f - l_1.u.f - \ldots - l_k.u.f =$

$p - m_2.u.f,$

(20) $p - m_1.u.f - l_1.u.f - \ldots - l_j.u.f \ll p$, (for $j = 1,\ldots,k$),

(21) $m_1u + l_1u + \ldots + l_ku = m_2u$,

i.e. (1),(2),(3) are again satisfied.

8321-17

Remark:

Having established property (RED), the properties (A2), (A3), (A4) can be "lifted" from R to $R[x_1,\ldots,x_n]$ in a manner which is more or less straightforward. One should note at this point that this is in sharp contrast to the procedures reported in the literature so far, which need to apply the critical-pair/completion algorithm itself (in $R[x_1,\ldots,x_n]$) in order to "lift" the axioms of the type (R1), (R2) from R to $R[x_1,\ldots,x_n]$.

Proof of (A5): This proof is based on the following two properties:

(CR1) $f_1 \, \Delta^p \, f_2$ iff there do not exist t_1, t_2 such that $t_1 \neq t_2$ and
LP(f_1) divides t_1, $C(p,t_1) \rightarrow_{LC(f_1)}$,
LP(f_2) divides t_2, $C(p,t_2) \rightarrow_{LC(f_2)}$,
but there exists a t such that
LP(f_1) divides t,
LP(f_2) divides t and

$LC(f_1) \, \Delta^{C(p,t)} \, LC(f_2)$

(CR2) $f_1 \, \underline{\Delta}^p \, f_2$ iff $p = LC(p).LCM(LP(f_1),LP(f_2))$ and

$LC(f_1) \, \underline{\Delta}^{LC(p)} \, LC(f_2)$.

Here, $LCM(t_1,t_2)$ denotes the least common multiple of t_1, t_2).

Proof of (CR1), "$==>$":

Assume

(1) $f_1 \; \Delta^p \; f_2$

and assume, furthermore, that there exist t_1,t_2 with

(2) $t_1 >_T t_2$

(3) $LP(f_1) \mid t_1$,

(4) $C(p,t_1) \rightarrow\!\!\lnot LC(f_1)$,

(5) $LP(f_2) \mid t_2$,

(6) $C(p,t_2) \rightarrow\!\!\lnot LC(f_2)$.

(The case $t_1 <_T t_2$ is analogous). We show that there exist m_1,u_1,m_2,u_2 such that

(7) $p - m_1.u_1.f_1 \leftarrow_{f_1} p \rightarrow_{f_2} p - m_2.u_2.f_2 \rightarrow_{f_1}$

$\rightarrow_{f_1} p - m_2.u_2.f_2 - m_1.u_1.f_1$,

which contradicts (1). Let m_1,m_2 be such that

(8) $C(p,t_1) - m_1.LC(f_1) < C(p,t_1)$,

(9) $C(p,t_2) - m_2.LC(f_2) < C(p,t_2)$

(such m_1,m_2 exist by (4),(6)) and let u_1,u_2 be such that

(10) $LP(f_1).u_1 = t_1$,

(11) $LP(f_2).u_2 = t_2$

(use (3),(5)). Then, using (RED) and

8321-18

(12) $C(p,t_1) = C(p-m_2.u_2.f_2,t_1)$,

(7) follows.

On the other hand, by (1) and the fact that there do not exist $t_1 \neq t_2$ satisfying (3) - (6), one knows that there exists m_1,m_2,u_1,u_2 such that

(13) $p \rightarrow_{f_1} p - m_1.u_1.f_1$,

(14) $p \rightarrow_{f_2} p - m_2.u_2.f_2$,

(15) $C(p,t) \rightarrow_{LC(f_1)}$,

(16) $C(p,t) \rightarrow_{LC(f_2)}$, where

(17) $t = u_1.LP(f_1) = u_2.LP(f_2)$.

We show that

(18) $LC(f_1)\ \Delta^{C(p,t)}\ LC(f_2)$.

Assume that for some m_1',m_2'

(19) $C(p,t) - m_1'.LC(f_1) \leftarrow_{LC(f_1)} C(p,t) \rightarrow_{LC(f_2)}$

$C(p,t) - m_2'.LC(f_2) \rightarrow_{LC(f_1)}$

$C(p,t) - m_2'.LC(f_2) - m_1'.LC(f_1)$.

(The case where

$C(p,t) - m_1'.LC(f_1) \rightarrow_{LC(f_2)}$

$C(p,t) - m_1'.LC(f_1) - m_2'.LC(f_2)$ is similar.)

Then, using (RED),

(20) $p - m_1'.u_1.f_1 \leftarrow_{f_1} p \rightarrow_{f_2}$

$p - m_2'.u_2.f_2 \rightarrow_{f_1}$

$p - m_2'.u_2.f_2 - m_1'.u_1.f_1$,

which contradicts (1).

<u>Proof</u> of (CR1), "<==":

We first show that

(1) $\leftarrow_{f_1} p \rightarrow_{f_2}$.

By the assumption of (CR1) on the right-hand side there exist t,u_1,u_2 such that

(2) $LP(f_1).u_1 = t$,

(3) $LP(f_2).u_2 = t$, and that there exist m_1,m_2 such that

(4) $C(p,t) \rightarrow_{LC(f_1)} C(p,t) - m_1.LC(f_1)$,

(5) $C(p,t) \rightarrow_{LC(f_2)} C(p,t) - m_2.LC(f_2)$.

(2) - (5), however, imply that

(6) $p \rightarrow_{f_1} p - m_1.u_1.f_1$,

(7) $p \rightarrow_{f_2} p - m_2.u_2.f_2$.

8321-19

Assume now that there exist m_1',u_1',m_2',u_2' such that

(8) $p - m_1'.u_1'.f_1 \leftarrow_{f_1} p \rightarrow_{f_2}$

$$p - m_2'.u_2'.f_2 \rightarrow_{f_1} p - m_2'.u_2'.f_2 - m_1'.u_1'.f_1$$

(The case that

$p - m_1'.u_1'.f_1 \rightarrow_{f_2} p - m_1'.u_1'.f_1 - m_2'.u_2'.f_2$ is similarly ruled out.)

Define

(9) $t_i := u_i'.LP(f_i)$ $(i=1,2)$.

Case $t_1 >_T t_2$: By (RED), we have

(10) $C(p,t_i') \rightarrow_{LC(f_i)} C(p,t_i') - m_1'.LC(f_i)$ $(i=1,2)$. This contradicts the right-hand side of (CR1).

Case $t_1 <_T t_2$: analogous.

Case $t_1 = t_2$: In this case we have

(11) $t=t_1=t_2$, because otherwise we again would have a contradiction to the right-hand side of (CR1). From (8) it then follows by (RED) that

(12) $C(p,t) - m_1'.LC(f_1) \leftarrow_{LC(f_1)} C(p,t) \rightarrow_{LC(f_2)}$

$C(p,t) - m_2'.LC(f_2) \rightarrow_{LC(f_1)}$

$C(p,t) - m_2'.LC(f_2) - m_1'.LC(f_1)$.

This contradicts to

(13) $LC(f_1) \Delta^{C(p,t)} LC(f_2)$.

Proof of (CR2), "==>":

Assume

(1) $f_1 \underline{\Delta}^p f_2$.

Because of (CR1) one can choose t, u_1, u_2 such that

(2) $LP(f_i).u_i = t$, $(i=1,2)$,

(3) $LC(f_1)\ \Delta^{C(p,t)}\ LC(f_2)$,

and there doesn't exist a $t' \neq t$ and $i \in \{1,2\}$ such that

(4) $LP(f_i)$ divides t' and

(5) $C(p,t') \neg LC(f_i)$.

Case $(H(p,t) \neq 0$ or $L(p,t) \neq 0)$: In this case

(8) $p' := C(p,t).t \ll p$

and, still,

(9) $f_1\ \Delta^{p'}\ f_2$

(by (2) - (5) and (CR1)). (8) and (9) contradict (1).

8321-20

Case $H(p,t) = L(p,t) = 0$, $t = u.LCM(LP(f_1), LP(f_2))$, $u \neq 1$: In this case

(10) $p' := C(p,t).LCM(LP(f_1, LP(f_2)) \ll p = C(p,t).t$.

(From (PP1) and (PP2) it follows that

(PP3) (v divides t and $v \neq t$) $\Longrightarrow$ $v \ll t$.)

Furthermore,

(11) $f_1\ \Delta^{p'}\ f_2$

because of (CR1),(3) and

(12) $LP(f_i)$ divides $LCM(LP(f_1), LP(f_2))$ $(i=1,2)$,

and the fact that there can not exist two distinct t_1,t_2 with $C(p',t_i) \neq 0$ $(i=1,2)$. (10) and (11) contradict (1).

Case $H(p,t) = L(p,t) = 0$, $t = LCM(LP(f_1), LP(f_2))$,
and not $LC(f_1)\ \underline{\Delta}^{C(p,t)}\ LC(f_2)$:

By (3) and the case assumption, one can choose an $a \prec C(p,t)$ such that

(13) $LC(f_1)\ \Delta^{a}\ LC(f_2)$.

Consider

(14) $p' := a.LCM(LP(f_1), LP(f_2))$.

Then

(16) $p' \prec\prec p$

and

(17) $f_1\ \Delta^{p'}\ f_2$

because of (CR1), (13), (12) and the fact that there can not exist two distinct t_1,t_2 with $C(p',t_i) \neq 0$ $(i=1,2)$.

The only remaining case, hence, is

$p = a.v$, where a and v are such that

$v = LCM(LP(f_1), LP(f_2))$,

$LC(f_1)\ \underline{\Delta}^{a}\ LC(f_2)$.

Proof of (CR2), "$\prec$==":

Assume

(1) $p = a.\mathrm{LCM}(\mathrm{LP}(f_1), \mathrm{LP}(f_2))$, where a is such that

(2) $\mathrm{LC}(f_1) \, \underline{\Delta}^a \, \mathrm{LC}(f_2)$.

By (CR1) it follows that

(3) $f_1 \, \Delta^p \, f_2$.

Assume now that there exists a p' such that

(4) $p' \ll p$

and also

(5) $f_1 \, \Delta^{p'} \, f_2$.

Let

(6) $v := \mathrm{LCM}(\mathrm{LP}(f_1), \mathrm{LP}(f_2))$.

8321-21

Case $H(p',v) \neq 0$: This case is not possible, because in this case one would have

(7) $p' \gg p$, a contradiction to (4).

Case $H(p',v) = 0$, $b := C(p',v) \neq 0$, $b \neq a$: In this case, because of (4),

(8) $b < a$.

By (5), (6) and (CR1), it follows that

(9) $\mathrm{LC}(f_1) \, \Delta^b \, \mathrm{LC}(f_2)$.

(8) and (9) contradict (2).

Case $H(p',v) = 0$, $b := C(p',v) = a$, $L(p,v) \neq 0$:

This case is not possible, because in this case one would have

(10) $p' \gg p$, a contradiction to (4).

Case $H(p',v) = 0$, $b := C(p',v) = a$, $L(p,v) = 0$: In this case

(11) $p' = p$, a contradiction to (4).

Case $H(p',v) = 0$, $b := C(p',v) = 0$: In this case

(12) $p' = L(p',v)$.

By (5) and (CR1) there exists a t that occurs in p' such that

(13) $LP(f_i)$ divides t $(i=1,2)$,

hence,

(14) $v \leq_T t$.

(Compare (PP3)!). This contradicts

(15) $t <_T v$.

((15) is valid, because $C(p',t) \rightarrow_{LC(f_1)}$, hence, $C(p',t) \neq 0$, and because of the case assumption).

Thus (4) and (5) always lead to a contradiction. Together with (3) this establishes

(16) $f_1 \underline{\Delta}^{p} f_2$.

Proof of (A5) using (CR1) and (CR2):

Assume

(1) $f_1 \Delta^p f_2$.

One has to construct p',m,u such that

(2) $p' \underline{\ll} p$,

(3) $f_1 \underline{\Delta}^{p'} f_2$,

(4) for all q:

$p' + q \ll p' \Longrightarrow p + m.u.q \ll p$.

From (1), using (CR1), it follows that there exists a t such that

(5) $LP(f_i)$ divide t $(i=1,2)$,

(6) $LC(f_1) \Delta^{C(p,t)} LC(f_2)$, and not exist t' and $i \in \{1,2\}$ such that

8321-22

(7) $t' \neq t$,

(8) $LP(f_i)$ divides t',

(9) $C(p,t') \mid LC(f_i)$.

Let

(10) $v := LCM(LP(f_1), LP(f_2))$.

By (A5) in R and (6) one can choose an a' and an m' such that

(11) $a' \underline{<} C(p,t)$,

(12) $LC(f_1) \underline{\Delta}^{a'} LC(f_2)$,

(13) for all c: $a' + c < a' \Longrightarrow C(p,t) + m'.c < C(p,t)$.

Define

(14) $p' := a'.v$,

(15) $m := m'$,

(16) u such that $v.u = t$.

Then from (CR2), (14), (12), (10), one obtains (3).

Furthermore $p \;\underline{\gg}\; C(p,t).t + L(p,t) \;\underline{\gg}$

$\underline{\gg}\; C(p,t).t$.

Case $v <_T t$:

$$C(p,t).t \overset{(PP3)}{\gg} C(p,t).v \overset{(11)}{\underline{\gg}} a'.v = p'.$$

Case $v = t$:

$$C(p,t).t \overset{(11)}{\underline{\gg}} a'.v = p'.$$

Hence, in any case, one obtains (2).

Assume now

(17) $p' + q \ll p'$.

Then

(18) $H(q,v) = 0$ (otherwise, $p' + q$ would be $\gg p'$).

Furthermore,

(19) $C(p' + q,v) = a' + C(q,v) < a'$.

(*Case* $a' + C(q,v) > a'$: not possible, because in this case $p' + q$ would
be $\gg p'$.

Case $a' + C(q,v) = a'$, $L(q,v) \neq 0$: not possible, because in this case, again p' + q would be $\gg$ p'. (Note that $L(p',v)=0$!).

Case a' + C(q,v) = a', L(q,v) = 0: not possible, because in this case p' + q would be = p'.

Case a' + C(q,v) incomparable with a': not possible, because in this case, p' + q would be incomparable with p'.)

From (19) and (13) one obtains

$$C(p,t) + m'.C(q,v) < C(p,t) \tag{20}$$

and, hence,

$$p + m.u.q = H(p + m.u.q,t) + C(p + m.u.q,t).t + L(p + m.u.q,t) =$$

$$\overset{(15),(16),(18)}{=} \quad H(p,t) + (C(p,t) + m'.C(q,v)).t + L(p,t) + m'.u.L(q,v) \overset{(20)}{\ll} p.$$

Proof of the axioms of effectiveness: The effectiveness of addition and multiplication, of course, easily carries over from R to $R[x_1,\ldots,x_n]$. (RED) and (CR2) show that reduction and formation of critical pairs are effective in $R[x_1,\ldots,x_n]$ if they are effective in R. In particular, (E1), (E2) are satisfied in $R[x_1,\ldots,x_n]$ if they are satisfied in R.

Proof of (T1): This proof, again is tedious. The techniques involved, however, are similar to those used in showing that $\gg$ is noetherian.

Assume that F_1, F_2, ... is a sequence of subsets of $R[x_1,\ldots,x_n]$ (with $F_1 \neq \emptyset$ w.l.o.g.) such that

(1) $\mathrm{Red}(F_1) \subset \mathrm{Red}(F_2) \subset \ldots$

(where "$\subset$" is strict set inclusion). Recall that, for $F \subseteq R[x_1,\ldots,x_n]$

(2) $\mathrm{Red}(F) := \{p \in R[x_1,\ldots,x_n] \mid p \rightarrow_F \}$.

Note also that for arbitrary p,f:

(3) $p \rightarrow_f \iff p \rightarrow_{LM(f)}$.

(Use (RED)!). Furthermore, define for $F \subseteq R[x_1,\ldots,x_n]$

(4) $LM(F) := \{LM(f) \mid f \in F\}$.

Define now inductively sequences b_1, b_2, ... and t_1, t_2, ... by

(5) $b_1 t_1$ arbitrary in $LM(F_1)$,

and for $i \geq 1$:

(6) $b_{i+1} t_{i+1} = LM(f)$, where
$f \in F_{i+1}$ such that
$p \rightarrow_f$ for some p with
$p \in \mathrm{Red}(F_{i+1}) - \mathrm{Red}(F_i)$.

(Such a p exists and, hence, also such an f can be chosen).

For this sequence $b_1 t_1$, $b_2 t_2$, ... the following holds:

(7) $\mathrm{Red}(\{b_j t_j \mid j<i\}) \subset \mathrm{Red}(\{b_j t_j \mid j<i+1\})$ (for $i=1,2,\ldots$).

((7) holds because the p in (6) is in $\mathrm{Red}(\{b_j t_j \mid j<i+1\})$ but not in $\mathrm{Red}(\{b_j t_j\})$ for a $j<i$: Otherwise, by (3), p would be in $\mathrm{Red}(F_j)$ and, hence, in $\mathrm{Red}(F_i)$.)

We now show that the sequence $b_1 t_1$, $b_2 t_2$, ... and, hence, the sequence F_1, F_2, ... is finite.

We prove this by assuming that $b_1 t_1$, $b_2 t_2$, ... is infinite and constructing an infinite sequence t_{l_1}, t_{l_2}, ... such that for all j,i with $j<i$

(8) t_{l_j} does not divide t_{l_i}.

However, by the Lemma of /Dickson 1910/ (see also /Buchberger 70/), an infinite sequence t_{l_1}, t_{l_2}, ... satisfying (8) can not exist.

Define now, first, a function S by

(9) $S(i) := \begin{cases} \text{some } j>i \text{ such that } t_i \mid t_j, & \text{if such a j exists,} \\ i & \text{otherwise} \end{cases}$

We show:

(10) For all i there exists a k such that
$i < S(i) < S^2(i) < \ldots < S^k(i)$ and
not exists $j > S^k(i)$ such that
$t_{S^k(i)} \mid t_j$.

(Notation: $S^k(i) = \underbrace{S(S(\ldots S}_{k \text{ times}}(i)\ldots))$, $S^0(i) = i$.)

Assume (10) to be false. Then one would have the infinite sequence

(11) $i < S(i) < S^2(i) < \ldots$

It then also would be true that

(12) $\mathrm{Red}(b_i) \subset \mathrm{Red}(b_i, b_{S(i)}) \subset \mathrm{Red}(b_i, b_{S(i)}, b_{S^2(i)}) \subset \ldots,$

which contradicts (T1) in R. ((12) is true, because if, for some k, $\mathrm{Red}(b_i,\ldots,b_{S^k(i)}) = \mathrm{Red}(b_i,\ldots,b_{S^{k+1}(i)})$ then

$$\mathrm{Red}(b_{S^{k+1}(i)}) \subseteq \mathrm{Red}(b_i,\ldots,b_{S^k(i)}).$$

Hence,

(13) $\mathrm{Red}(b_{S^{k+1}(i)} t_{S^{k+1}(i)}) \subseteq \mathrm{Red}(b_i t_i,\ldots,b_{S^k(i)} t_{S^i(i)}),$

because $t_i \mid t_{S^{k+1}(i)}, \ldots, t_{S^k(i)} \mid t_{S^{k+1}(i)}$ by construction of S. (13) contradicts to (7).)

Let now the function N be defined as follows

(14) $N(i) := S^k(i)$, where k is such that the condition in (10) is satisfied.

By (10) N is a total function. One now can define

(15) $l_1 := N(1),$
$l_{i+1} := N(l_i + 1).$

It is clear that $l_1 < l_2 < l_3 < \ldots$, because $N(i) > i$. Furthermore, (8) is satisfied because, for $j<i$,

$l_j = N(x)$ for some natural number x,
$l_j < l_i$,

and hence, by (14) and (10),

t_{l_j} does not divide t_{l_i}.

<u>Proof</u> of (T2): (T2) in $R[x_1,\ldots,x_n]$ follows immediately from (CR2) and (T2) in R.

5. EXAMPLE: Z

If we consider R:= Z, an example of suitable $<$ and M are

$$0 < -1 < 1 < -2 < 2 < \ldots$$

$$M := Z-\{0\}.$$

$<$ is a notherian total ordering, (M0) - (M1) and (A1) are easily proven.

Proof of (A2): If $a \to_c b$, then $b = a - mc < a$ for some m and $b+d = a+d-mc$.

Case $a+d = b+d$: not possible, because in this case $a = b$, a contradiction to $b < a$.

Case $a+d < b+d$: in this case $b+d \to_c a+d$.

Case $a+d > b+d$: in this case $a+d \to_c b+d$.

Hence, in every case $a+d \downarrow_c^* b+d$.

Proof of (A3): similar. Use (M3).

Proof of (A4): similar. The totality of $<$ makes these proofs easy.

Let now $C \subseteq Z$. We define:

(D1) $LCR(C) := \min_<\{a \mid \text{for all } c \in C\text{: } a \to_c \}$
(read: "the least common reducible of C").

One can now show for c_1, c_2, $a \in Z$:

(L1) $LCR(\{c\}) = \begin{cases} |c| / 2, & \text{if c is even,} \\ -(|c| + 1)/2, & \text{if c is odd.} \end{cases}$

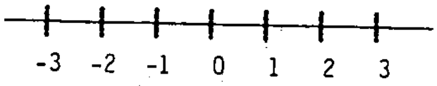
(L2) $LCR(\{c_1,c_2\}) = \max_<(LCR(c_1),LCR(c_2))$.

(L3) $c_1 \overset{a}{\underline{\Delta}} c_2 \quad \Longleftrightarrow \quad a = LCR(c_1,c_2).$

(L4) $a+c \prec a,\ a \preceq b \quad \Longrightarrow \quad b + S(a,b).c \prec b$
(Here $S(a,b) :=$ $\begin{array}{ll} 1, & \text{if a and b have the same sign,} \\ -1, & \text{otherwise} \end{array}$)

(L5) $a \rightarrow_c \quad \Longleftrightarrow \quad a \succeq LCR(\{c\}).$

These properties can be shown by a (tedious) case analysis. However, the proofs are easily seen if one visualizes the meaning of $\prec$ and of $a \rightarrow_c b$ in the following picture:



Proof of (A5): If $c_1 \overset{a}{\underline{\Delta}} c_2$ then $a \rightarrow_{c_1}$, $a \rightarrow_{c_2}$. Hence, by (L5) and (L2), $a > LCR(c_1,c_2)$. Now take $a' := LCR(c_1,c_2)$ and $m := S(a,a')$. Then, by (L4), for all c:

$$a'+c \prec a' \quad \Longrightarrow \quad a+mc \prec a.$$

Of course, $c_1 \overset{a}{\underline{\Delta}} c_2$ by (L3).

Proof of the axioms of effectiveness: (E1) is clear. For A(a,c) in (E2) take S(a,c).

For practical purposes, it is better to define A(a,c) to be the result of iteratively subtracting S(a,c).c until this is not possible any more (this corresponds to a modified "division"). However, we emphasize that this is only one possibility in a whole spectrum of possible reduction processes all proven correct by our theorem.

Proof of (T1): Note that

$$Red(c) = \{a \mid a \rightarrow_c \} = \{a \succ 0 \mid a > |c|/2\} \cup \{a \prec 0 \mid a \prec -|c|/2\}.$$

Hence, the complement of Red(D) ($D \subseteq \mathbb{Z}$) contains only finitely many numbers.

Proof of (T2): By (L3) and (L2) the number a such that $c_1 \overset{a}{\underline{\Delta}} c_2$ can be computed by an (easy) algorithm.

Let us consider the example $D := C := \{12,16,20\}$. The first step in the application of the algorithm could be

$(c_1,c_2) := (12,16)$

$a = LCR(c_1,c_2) = 8$

$b_1 = -4$, $b_2 = -8$

b_1, b_2 are in normal form w.r.t. C

b_1-b_2 must be adjoined to the basis D.

A next step could be:

$(c_1,c_2) := (16,20)$

$a = LCR(c_1,c_2) = 10$

$b_1 = -6$, $b_2 = -10$

$S_D(b_1) = -2$, $S_D(b_2) = -2$

No new element has to be adjoined to D.

Actually, all elements $\neq 4$ in D can be reduced by 4. So $\{4\}$ is the "reduced Gröbner basis" corresponding to C, i.e. the algorithm for computing the Gröbner basis, of course, computes the GCD of the elements in C. Furthermore, Euclid's algorithm is just one of the whole spectrum of possible realizations of our algorithm over Z.

20 $\{4\ 8, 12, 16\}$ 20

6. EXAMPLE: $Z[x_1,\ldots x_n]$

The example of $Z[x_1,\ldots,x_n]$ will be considered in detail. As in the general case, also in this example the algorithm of Section 3. yields ideal bases for which ideal congruence can be decided by reduction and, furthermore, the Gröbner bases constructed are "invariants" in the sense that the ideals generated by C_1, C_2 are equal iff the Gröbner bases constructed for C_1, C_2 are equal. (The latter statement is true if, after the construction of the Gröbner bases according to the algorithm in Section 3., every polynomial in the Gröbner basis is reduced to normal form with respect to the other polynomials in the basis. This is totally analogous to the situation in $K[x_1,\ldots,x_n]$, see /Buchberger 76a/.) The problem of deciding congruence and of constructing invariants for ideals in $Z[x_1,\ldots,x_n]$ has a long and interesting history involving work of /Kronecker, Hensel 01/, /Szekeres 52, 65, 75/, /Redei 56/, /Trotter 69, 78/, /Simmons 70/, /Hurd 70/, /Richman 74/, /Lauer 76/, /Trinks 77/, /Zacharias 78/, /Sims 78/, /Schaller 79/, /Ayoub 81/. For some of the details of the history, see /Ayoub 81/. The first general solution of both problems, based on the critical-pair completion approach, but needing two different versions of "critical pairs" at the same time, was given in /Lauer 76/. Other solutions based on the critical-pair/completion approach using (R1), (R2) were given in /Trinks 77/, /Zacharias 78/, /Schaller 79/. The first general solution based on a different approach was given in /Ayoub 81/. Our solution seems to be much more concise than the solutions given so far.

In order to get the specialization of the general critical-pair completion algorithm of Section 3. for $Z[x_1,\ldots,x_n]$, according to (RED), (CR1) and (CR2), one has to fix a suitable M, $<$ and $<_T$, and to give effective procedures for finding b if $a \to_C$ ($a \in Z$, $C \subseteq Z$) and for finding (all) a such that $c_1 \overset{a}{\Delta} c_2$ (c_1, c_2 $\in Z$). One possible choice has been described in Section 5.

Consider now the following set $F := \{f_1,f_2,f_3\}$ of polynomials (the same example is considered in /Ayoub 81/):

$$f_1 := 3x^2y+2xy+y+9x^2+5x-3$$
$$f_2 := 2x^3y-xy-y+6x^3-2x^2-3x+3$$
$$f_3 := x^3y+x^2y+3x^3+2x^2.$$

We fix the "purely lexicographical" ordering for the bivariate power products: 1 $<_T$ $<_T$ x $<_T$ x^2 $<_T$ x^3 $<_T$ .... $<_T$ y $<_T$ xy $<_T$ x^2y $<_T$ x^3y $<_T$ ... $<_T$ y^2 $<_T$ xy^2 $<_T$ $<$ x^2y^2 $<_T$... Then, $LP(f_1)=x^2y$, $LP(f_2)=LP(f_3)=x^3y$, The polynomial x^3y may be reduced by f_2 in the following way (compare (RED)):

Take a:=1, t:=x^3y, m:=1, u:=1.
Hence, $x^3y \rightarrow_{f_2} -x^3y+xy+y-6x^3+2x^2+3x-3$ =: g.

g may be further reduced modulo f_3:

Take a:=1, t:=x^3y, m:=-1, u:=1.
Hence, $g \rightarrow_{f_3} x^2y+xy+y-3x^3+4x^2+3x-3$ =:g'.

g' is irreducible with respect to F. The polynomial x^3y may also be reduced by f_3:

Take a:=1, t:=x^3y, m:=1, u:=1.
Hence, $x^3y \rightarrow_{f_3} -x^2y-3x^3-2x^2$ =: h.

Also h is irreducible with respect to F, i.e. we have the following situation

$$\underline{g'}_F \leftarrow_F^* x^3y \rightarrow_F^* \underline{h}_F, \quad g'\neq h,$$

which shows that $\rightarrow_F$ does not possess the Church-Rosser property.

In order to "complete" F by the critical-pair/completion algorithm one has to consider "critical pairs" of polynomials in F (in any order). For example, one can start with f_2, f_3, and compute (all) p such that $f_2 \underline{\Delta}^p f_3$. This can be done by (CR2): $LC(f_2)=2$, $LC(f_3)=1$, hence by (2) above LC(p)=LCR(2,1) = 1. Furthermore, $LCM(LP(f_2),LP(f_3)) = x^3y$. Thus, $p=x^3y$. One reduction step of x^3y modulo f_2 and f_3 yields (the "critical pair") g and h, respectively. (Actually, in $Z[x_1,\dots,x_n]$, there exists only one critical pair for a given pair of polynomials). Further reduction of g and h to normal forms modulo F yields g' and h, respectively. g'≠h and, hence,

$$f_4 := g'-h = 2x^2y+xy+y+6x^2+3x-3$$

must be adjoined to the basis. Similarly, one now has to consider the next critical pair, for example, the one corresponding to f_1, f_4: $p=-2x^2y$. Reduction of p modulo f_1 and f_4 yields $x^2y+2xy+y+9x^2+5x-3$ and $xy+y+6x^2+3x-3$, respectively. Reduction to normal forms yields $-x^2y+xy+3x^2+2x$ (using f_4) and $xy+y+6x^2+3x-3$. Thus, the difference of these two polynomials must be adjoined to the basis:

$$f_5 := -x^2y-y-3x^2-x+3.$$

Similarly, the consideration of the critical pair of f_4 and f_5 leads to

$$f_6 := -xy+y-x-3.$$

The consideration of the critical pair of f_5 and f_6 leads to

$$f_7 := 2y+2x^2-3x-6.$$

Finally, the consideration of the critical pair of f_6 and f_7 leads to

$$f_8 := 2x^3-5x^2-5x.$$

The consideration of all the other critical pairs leads to identical normal forms. Hence, $G := \{f_1,\ldots,f_8\}$ is a Gröbner basis corresponding to F, i.e. F and G generate the same ideal in $Z[x_1,\ldots,x_n]$ and $\rightarrow_G$ has the Church-Rosser property. Reduction of all the f_i modulo $G-\{f_i\}$ leaves us with $G' := \{f_6', f_7, f_8\}$, where

$$f_6' := -xy-y-2x^2+2x+3.$$

Summarizing, the algorithm produced G' such that F and G' generate the same ideal, $\rightarrow_{G'}$ has the Church-Rosser property (hence, $S_{G'}$ decides the congruence $\equiv_F$) and, given the ideal generated by F, G' is uniquely determined.

8321-26

7. EXAMPLE: Z_z

The proof that $\mathbf{Z}_z$, with suitable $\prec$ and M, is a reduction ring was given by H. Rolletschek and will be published in a separate report /Rolletschek/. For the sake of completeness, H. Rolletschek allowed me to include his proof in the present report. The case of $\mathbf{Z}_z$ (and, hence, $Z_z[x_1,\ldots,x_2]$) is interesting because, for z non-prime, $\mathbf{Z}_z$ contains zero divisors.

Z_z is in the congruence class ring mod z in the domain Z of rational integers. First we have to define the set M of multipliers and the partial order relation appropriately. We will denote this ordering by $\leq'$ rather than $<$ to distinguish it clearly from the standard ordering $<$ for integers.

We put $M := \{m \in Z_z \mid m \neq 0$ and m is not a zerodivisor in $Z_z\}$. It is easy to see that the conditions (M0) - (M5) are satisfied. (M0), (M1), (M2) and (M4) are trivial. As for (M3), it is a well-known fact that a product of non-zero-divisors in an arbitrary ring is again a non-zero-divisor. Finally, (M5) follows from the fact that every element f of Z_z has the representation $\underbrace{1 + 1 + \ldots + 1}_{f}$

Then, if $a \equiv_C b$, by definition there exist n, $d_i \in Z_z - \{0\}$, $c_i \in C$ such that

$$a = b + \sum_{1<i<n} d_i c_i = b + \sum_{1<i<n} \sum_{1<j<d_i} 1.c_i.$$

Since $1 \in M$, axiom (M5) follows.

Next we have to define the order relation $\leq'$. Surprisingly, it turns out that the simplest possible ordering is appropriate. For $a \in Z$ let $\lfloor a \rfloor$ be the congruence class of a mod Z. Then we define $\leq'$ by

$$\lfloor 0 \rfloor < \lfloor 1 \rfloor < \ldots < \lfloor z-1 \rfloor.$$

Before we show that the axioms (A1) - (A5) are satisfied, we introduce some more notation. For $a \in Z_z$ let $a^* \in Z$ be the smallest nonnegative representative of a, that is, $a = \lfloor a^* \rfloor$, $0 < a^* < z$. For $x,y \in Z$, $x \mid y$ means that x is a divisor of y. GCD(x,y) is the greatest common divisor of x and y, and for a prime number p, $\nu_p(x)$ is the largest ν such that $p^\nu \mid x$.

(A1): Trivial.

(A3): Assume $a \rightarrow_C b$, that is, $b = a - m_1.c$, $m_1 \in M$, $b <' a$.

$$\begin{aligned} \text{Then} \quad mb &= ma - mm_1 c, \\ ma &= mb - (-mm_1)c, \end{aligned}$$

and by (M2), (M3), mm_1 and $-mm_1$ are elements of M. This implies either $ma \to_c mb$ or $mb \to_c ma$, depending on whether ma or mb is larger. The case ma = mb is impossible for, since m is not a zero-divisor, it would imply a = b.

(A5): Assume $c_1 \; \Delta^a \; c_2$. Trivially, there exists an element a' such that $a' \underline{<}' a$ and $c_1 \; \underline{\Delta}^{a'} \; c_2$. We have to show that there exists an $m \in M$ such that for all c

$$a' + c <' a' \Longrightarrow a + m.c <' a.$$

This holds for m=1:

$$a' + c <' a' \Longleftrightarrow a'^* + c^* \underline{>} z \Longrightarrow a^* + c^* \underline{>} z \Longleftrightarrow a + 1.c <' a.$$

For (A2) and (A4) we need two auxiliary results. The first concerns division in the congruence class ring mod z.

Lemma 1: Consider the congruential equation

$$x \; a \equiv b \mod z \qquad (1).$$

Let d = GCD(a,z), d' = z/d.

a) (1) has at least one solution x, if and only if $d \mid GCD(b,z)$.

b) If (1) has a solution x, then the set of all such solutions forms exactly one congruence class mod d'.

c) If b = d, then the solution set from b) is a relatively prime congruence class, that is, every solution x satisfies GCD(x,d') = 1.

8321-27

Proof: a) and b) are well-known number-theoretic facts, see, for instance, /Hasse 64/, section 4.3.

c): Let x be a solution of (1), b=d, and assume x and d' contains a common prime divisor p. If $\nu_p(a) \underline{>} \nu_p(z)$, then $\nu_p(d) = \nu_p(z)$, hence $\nu_p(d') = 0$, contrary to our assumption $p \mid d'$. If $\nu_p(a) < \nu_p(z)$, then our assumption $p \mid x$ implies $\nu_p(d) > \nu_p(a)$, since $d = xa - kz$ for some $k \in Z$; this is again a contradiction.

From Lemma 1 we derive

Lemma 2: Let $u,v \varepsilon Z_z$, $u \succ v$, $u^* \equiv v^* \bmod d = GCD(c^*,z)$. Then $u \rightarrow_c v$.

Proof: By Lemma 1 a), there exists an $m' \varepsilon Z$ s.t. $d \equiv m'c^* \bmod z$. Let m_0 be one such m'. By b), c) the set of all such m' forms one congruence class mod $d' = z/d$, and $GCD(m_0,d') = 1$. By the Chinese remainder theorem there exists an element $m_1 \varepsilon Z$ s.t.

$m_1 \equiv m_0 \bmod d'$,

$m_1 \equiv 1 \bmod p$ for every prime p such that $p \mid z$, but p doesn't divide d'.

Then $GCD(m_1,z) = 1$, and $d \equiv m_1c^* \bmod z$. Let $m = \lfloor m_1 \rfloor$. Then $m \varepsilon M$ and $\lfloor d \rfloor = mc$. This gives the desired reduction

$$u \rightarrow_c u - mc = u - \lfloor d \rfloor \rightarrow_c u - 2.\lfloor d \rfloor \rightarrow \ldots \rightarrow v,$$

since $v^* = u^* - ld$ for some $l \varepsilon Z$.

Now we can proof axioms (A2) and (A4):

(A2): Let $a \rightarrow_c a - mc$ for some $m \varepsilon M$ and let $b:=a-mc$. Without loss of generality let $a + d \succ' b + d$. Then $b^* \equiv a^* - m^*c^* \bmod z$, hence $a^* \equiv b^* \bmod t = GCD(c^*,z)$, and $(a + d)^* \equiv (b + d)^* \bmod t$.
By Lemma 2, $a + d \rightarrow_c b + d$, hence $b + d$ is the desired common successor of $a + d$ and $b + d$. Generally, if f is a common successor of $a + d$ and $b + d$ modulo c:

$$\left.\begin{array}{l} a + d \rightarrow a + d - l_1 c \rightarrow a + d - l_1 c - l_2 c \rightarrow \ldots \\ \qquad \rightarrow a + d - \sum_{i=1}^{k} l_i c = f, \\ b + d \rightarrow a + d - mc \rightarrow a + d - mc - m_1 c \rightarrow \ldots \rightarrow \end{array}\right] \qquad (2)$$

$$\rightarrow a + d - mc - \sum_{i=1}^{j} m_i c = f,$$

then the following additional condition is required for (A2):

$$\sum_{i=1}^{k} l_i \quad = \quad m + \sum_{i=1}^{j} m_i \ .$$

In our case, where k = 0, we have to show that $0 = m + \sum_{i=1}^{j} m_i$,

can be guaranteed by an appropriate choice of $m_1,\ldots,m_j$. (2) implies in our case:

$$0 = mc + \sum_{i=1}^{j} m_i c = (m + \sum_{i=1}^{j} m_i)c.$$

8321-28

Hence, by Lemma 1b) $m^* + \sum_{i=1}^{j} m_i^* \equiv 0 \mod t' = z/t.$ (3)

But m_1 is determined by $m_1^* c \equiv d \mod z$, hence, again by Lemmma 1b), we may replace m_1 by $m_1 + gt'$ for an arbitrary $g \in Z_z$. It follows from (3), that one such choice guarantees

$$m^* + \sum_{i=1}^{j} m_i^* = 0.$$

Fall $b_1 = b_2$?

(A4): Let $b_1 \, {}_c\!\leftarrow a \rightarrow_c b_2$, and without loss of generality, $b_1 \succ' b_2$. Then it follows exactly as in the proof of (A2), that $b_1 \rightarrow_c^* b_2$; we only have to note that

$$a \succ' b_1 - d,\ a \succ' b_1 - 2d,\ \ldots\ ,\ a \succ' b_2 + d.$$

9. <u>EXAMPLE:</u> Fields K and $K[x_1,\dots,x_n]$

Fields K can be viewed as (trivial) reduction rings (with all $C \subseteq K$ being Gröbner bases) by defining

$$M := K-\{0\},$$

$$a \prec b \;:\Longleftrightarrow\; a=0,\ b\neq 0$$

$\prec$ is a noetherian partial(!) ordering. It is straight forward to see that (M0),...,(M5),(A1),...(A5) are satisfied. Furthermore, $\prec$ is decidable and

$$a \to_c \;\Longrightarrow\; a - \frac{a}{c}.c \prec a,$$

hence $A(a,c) := \frac{a}{c}$ can be taken in (E2).
Finally,

(1) $\emptyset \neq D \subseteq K \;\Longrightarrow\; \mathrm{Red}(D) = K-\{0\}$

and

(2) $c_1 \overset{a}{\underline{\Delta}} c_2 \;:\Longleftrightarrow\; a,\ c_1,\ c_2 \neq 0.$

From (1) it follows that (T1) trivially is satisfied. (2) shows that, for given $c_1,\ c_2 \neq 0$, there may be infinitely many a such that $c_1 \overset{a}{\underline{\Delta}} c_2$, namely all $a \in K$.

In $K[x_1,\dots,x_n]$, by (CR2), one therefore has

$$f_1 \overset{p}{\underline{\Delta}} f_2 \;\Longleftrightarrow\; p=a.\mathrm{LCM}(\mathrm{LP}(f_1),\mathrm{LP}(f_2))$$

However, it es easy to see that it suffices to guarantee

$$b_1 \overset{*}{-} (\prec p)\ b_2$$
$$\text{for } b_1 \;{}_{f_1}\!\!\leftarrow p_0 \to_{f_2} b_2$$
$$(\text{where } p_0 := \mathrm{LCM}(\mathrm{LP}(f_1),\mathrm{LP}(f_2))\ )$$

in order to guarantee

$$b_1 \overset{*}{-} (\prec p)\ b_2$$
$$\text{for } b_1 \;{}_{f_1}\!\!\leftarrow p \to_{f_2} b_2$$
$$\text{for arbitrary } p=a.\mathrm{LCM}(\mathrm{LP}(f_1),\mathrm{LP}(f_2)).$$

This shows that in the case of $K[x_1,\ldots,x_n]$ the general algorithm developed in this paper specializes to our original 1965 algorithm.

CONCLUSIONS

We have shown that an axiomatic approach to a constructive ring theory based on the notion of reduction and on a critical-pair/completion is possible. The general critical-pair completion algorithm presented in this paper specializes to our 1965 algorithm in $K[x_1,\ldots,x_n]$ (K a field) (which, again, specializes to Euclid's algorithm in $K[x]$ and to Gauß' algorithm in the case of linear polynomials in $K[x_1,\ldots,x_n]$), it specializes to (a whole spectrum) of Euclidean algorithms in Z and it yields an elegant algorithm for deciding congruence and related problems in $Z[x_1,\ldots,x_n]$.

The major weakness of this paper is that, at the present stage of the investigations, only a few other examples of rings satisfying the axioms are known. Further research is necessary in order to clarify whether a sufficiently wide class of rings satisfies the axioms or whether a further attempt at weakening the axioms must be made. Both tasks are challenging: The first task leads to the investigation of new properties of rings that so far have not received any attention. The second task requires to develop new ideas for the proof of the main theorem in Section 3. and will clarify the insight, which properties of rings lie "really" at the basis of the critical-pair/completion approach.

REFERENCES

Ayoub, C. W., 81:
On Constructing Bases for Ideals in Polynomial Rings over the Integers.
The Pennsylvania State University, Dept. of Mathematics, Report Nr. 8184, 1981, submitted to publication.

Ballantyne, A. M., Lankford, D. S., 81:
New Decision Algorithms for Finitely Presented Commutative Semigroups.
Comp. and Maths. with Appls. 7 (1981), 159-165.

Bauer, G., 81:
The Representation of Monoids by Confluent Rule Systems.
University of Kaiserlautern, FRG, Fachbereich Informatik, Ph.D. Thesis, 1981.

Bergman, G. M., 78:
The Diamond Lemma for Ring Theory.
Adv. Math. 29, (1978), 178-218.

Buchberger, B., 65:
An Algorithm for Finding a Basis for the Residue Class Ring of a Zero-Dimensional Polynomial Ideal (German).
Univ. of Innsbruck, Austria, Math. Inst., Ph.D. Thesis, 1965.

Buchberger, B., 70:
An Algorithmical Criterion for the Sovability of Algebraic Systems of Equations (German).
Aequationes mathematicae 4/3 (1970), 374-383.

Buchberger, B., 76:
A Theoretical Basis for the Reduction of Polynomials to Canonical Form.
ACM SIGSAM Bull. 10/3 (1976), 19-29.

Buchberger, B., 76a:
Some Properties of Gröbner Bases for Polynomial Ideals.
ACM SIGSAM Bull. 10/4 (1976), 19-24.

Buchberger, B., 79:
A Criterion for Detecting Unnecessary Reductions in the Construction of Gröbner-Bases.
Proc. EUROSAM 79, Marseille (Ng, W., ed.), Lecture Notes in Computer Science 72 (1979), 3-21.

Buchberger, B. 8 :
H-Bases and Gröber Bases.
Univ. Linz, Institut f. Mathematik, CAMP-Rep.Nr. 81-1.

Buchberger, B., 83:
A Note on the Complexity of Constructing Gröbner-Bases.
Proc. of the EUROCAL 83 Conf., London, Lecture Notes in Computer Science, Sringer, 1983, to appear.

Buchberger, B., Loos, R., 82:
Algebraic Simplification.
In: Computer Algebra (B. Buchberger, G. Collins, R. Loos eds.), Springer, Wien - New York, 1982, 11-43.

Dickson L., 1913:
Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors.
Am. J. Math. 35, 1913, pp. 413-422.

Guiver, J. P., 82:
Contributions to Two-Dimensional System Theory.
Univ. of Pittsburgh, Math. Dept., Ph.D. Thesis, 1982.

Hasse H., 64:
Vorlesungen über Zahlentheorie.
Springer, 1964.

Hurd, C. B., 70:
Concerning Ideals in $Z[x]$ and $Z_{p^n}[x]$.
The Pennsylvania State University, Department of Mathematics, Ph.D. Thesis, 1970.

Knuth, D. E., Bendix, P. B., 67:
Simple Word Problems in Universal Algebras.
Proc. of the Conf. on Computational Problems in Abstract Algebra, Oxford, 1967, (Leech, J., ed.), Oxford: Pergamon Press, 1970.

Kronecker, L., Hensel, K., 01:
Lectures on Number Theory (German).
Leipzig, 1901.

Lauer, M., 76:
Canonical Representatives for the Residue Classes of a Polynomial Ideal.
University of Kaiserslautern, FRG, Dept. of Mathematics, Diploma Thesis, 1976.

Llopis de Trias, R., 83:
Canonical Forms for Residue Classes of Polynomial Ideals and Term Rewriting Systems.
Univ. Aut. de Madrid, Division de Matematicas, submitted to publication, 1983.

Redei, L., 56:
Equivalence of the Theorems of Kronecker-Hensel and Szekeres (German).
Acta Sci. Math. Szeged 17 (1956), 198-202.

Richman, F., 74:
Constructive Aspects of Noetherian Rings.
Proc. AMS 44/2 (1974), 436-441.

Schaller, S., 79:
Algorithmic Aspects of Polynomial Residue Class Rings.
University of Wisconsin, Madison, Ph.D. Thesis, Comput. Sci. Tech. Rep. 370, 1979.

Simmons, H., 70:
The Solution of a Decision Problem for Several Classes of Rings.
Pac. J. Math. 34 (1970), 547-557.

Sims, C., 78:
The Role of Algorithms in the Teaching of Algebra.
In: Topics in Algebra (Newman, M. F. ed.), Lecture Notes in Mathematics 697 (1978), Springer, 95-107.

Spear, D., 77:
A Constructive Approach to Commutative Ring Theory.

Proc. of the MACSYMA Users' Conference, Berkeley, 1977, (Fateman, R.J., ed.), published by MIT, 369-376.

Szekeres, G., 52:
A Canonical Basis for the Ideals of a Polynomial Domain.
Am. Math. Monthly 59 (1952), 379-386.

Szekeres, G., 65:
Metabelian Groups with Two Generators.
Proc. Internat. Conf. Theory of Groups (Canberra 1965), Gordon & Breach, 1967, 323-346.

Szekeres, G., 75:
Homogeneous Ideals in K[x,y,z].
Acta Math. Acad. Sci. Hungar. 26 (1975), 355-367.

Trinks, W., 78:
On B. Buchberger's method for Solving Algebraic Equations (German).
J. Number Theory 10/4 (1978), 475-488 (preprint 1977).

Trotter, P. G., 69:
A Canonical Basis for Ideals of Polynomials in Several Variables and With Integer Coefficients.
Univ. of New South Wales, Ph.D. Thesis, 1969.

Trotter, P. G., 78:
Ideals in Z[x,y].
Acta Math. Acad. Sci. Hungar. 32 (1-2) (1978), 63-73.

Winkler, F., Buchberger, B., 83:
A Criterion for Eliminating Unnecessary Reductions in the Knuth-Bendix Algorithm.
Coll. on Algebra, Combinatorics and Logic in Computer Science, Györ, Sept. 12-16, 1983, 21 p.

Zacharias, G., 78:
Generalized Gröbner Bases in Commutative Polynomial Rings.
MIT, Dept. Comput. Sci., Bachelor Thesis, 1978.

ACKNOWLEDGEMENT: The research described in this paper is supported by the Austrian Research Fund, Project Nr. 4567. Part of the work was carried out while the author was visiting the University of Delaware, the IBM Thomas Watson Research Center, Yorktown Heights, and the University of Wisconsin-Madison, January-September 1982.

Added July 1984:

In a personal communication, D. Lankford pointed out to me that the solution of the simplification problem modulo ideals in $Z[x_1,\ldots,x_n]$, which is a special case in our approach, subsumes also the uniform word problem for finitely generated dommutative rings ($x_1,\ldots,x_n$ ... generators). See also:

G. Butler, D. Lankford:
Dickson's Lemma, Hilbert's Basis Theorem and Applications to Completion in Commutative Noetherian Rings.
Dept. of Math. and Stat., Louisiana, Tech. Univ., Ruston, LA 71272.