A Method for Factorizing Multivariate Polynomials over Successive Algebraic Extension Fields*

DONGMING WANG
Research Institute for Symbolic Computation
Johannes Kepler University, A-4040 Linz, Austria
(wang@risc.uni-linz.ac.at)

Abstract

We present a method for factorizing multivariate polynomials over algebraic fields obtained from successive extensions of the rational number field. The basic idea underlying this method is the reduction of polynomial factorization over algebraic extension fields to the factorization over the rational number field via linear transformation and the computation of characteristic sets with respect to a proper variable ordering. The factors over the algebraic extension fields are finally determined via GCD (greatest common divisor) computation. We have implemented this method in the Maple system. Preliminary experiments show that it is rather efficient. We give timing statistics in Maple 4.3 on 40 test examples which were partly taken from the literature and partly randomly generated. For all those examples to which the Maple built-in algorithm is applicable, our algorithm is always faster.

1. Introduction

We refer to [1–4, 6–12, 15–16, 22–25] for the history, motivation and importance of polynomial factorization in the area of computer algebra. The method presented in this paper has been designed for factorizing multivariate polynomials over algebraic fields obtained from *successive extensions* of the rational number field. Our interest in considering factorization over such fields has been particularly stimulated by the need of it in decomposing polynomial sets into irreducible ascending sets [13, 14, 26, 27] which is necessary for Wu's method of geometry theorem proving [26, 27] and irreducible decomposition of algebraic varieties [18, 26, 27]. The usual way of treating multiple algebraic extensions is to determine single algebraic extensions by computing a minimal polynomial of higher degree from several minimal polynomials. Our method does not require this procedure. The method was discovered by the author during his implementation of the `charsets` package [20] in Autumn 1990. It was implemented in that package as a function `cfactor` and as subroutines of the functions `ics` and `ivd` which have been available in the Maple share library since January 1991. The implementation has been considerably modified and improved during the writing of this paper. The basic idea underlying our method is the reduction of polynomial factorization over algebraic extension fields to the factorization over the rational number field via linear transformation and the computation of characteristic sets with respect to a proper variable ordering. The factors over the algebraic extension fields are finally determined via GCD (greatest common divisor) computation. The method may be viewed in some sense as a variant of the well-known method of Trager [15]. However, we do not use the concept of norms, nor perform the computation of resultants. Instead the concept of ascending sets and the computation of characteristic sets play a central role in our method.

We shall give in the next section some preliminaries on ascending sets, characteristic sets, their irreducibility and their relation to successive algebraic extension fields. A few simple propositions useful for testing the reducibility of polynomials over algebraic extension fields will be presented. We shall state some lemmas which guarantee the correctness and termination of our main algorithm. A description of the factorization algorithm is given in Section 3. We

*This research is supported in part by the Austrian Ministry of Science and Research under ESPRIT Basic Research Action 3125 (MEDLAR).

give some implementation details and report timing statistics on a set of 40 test examples in comparison with the Maple built-in function (which seems to be based on Trager's algorithm [15]). The test examples were partly taken from the literature and partly randomly generated. For all those examples to which the Maple built-in function factor is applicable, the function cfactor implemented on the basis of our algorithm is always faster (even though it is much more general). Although we do not have a direct comparison on the efficiency of our algorithm with the well-known algorithm of Lenstra [10], we at least can say that our algorithm does not appear to be worse in practice according to an indirect comparison with the timings provided in [1]. Furthermore, by our algorithm we have rediscovered[1] the incompleteness of the factorization for the fifth example in [10] (which is the most difficult one), that is, the first factor of degree 6 there can be further factorized as the product of three factors of degree 2 (see the 17th example in the appendix). The theoretical complexity of our algorithm is expected to be analyzed in the future.

2. Ascending Sets, Characteristic Sets and Successive Algebraic Extensions

Let $\mathbb{Q}$ denote the field of rational numbers and $u_1, \ldots, u_d$ be a set of transcendental elements, abbreviated sometimes as u. The transcendental extension field obtained from $\mathbb{Q}$ by adjoining the elements $u_1, \ldots, u_d$ will be denoted by $\mathbb{K}_0$, i.e.,

$$\mathbb{K}_0 = \mathbb{Q}(u_1, \ldots, u_d) = \mathbb{Q}(u).$$

Let $y_1, \ldots, y_n$ be a set of n variables with a fixed ordering $y_1 \prec \cdots \prec y_n$. Then any polynomial $F = F(u_1, \ldots, u_d, y_1, \ldots, y_n)$ in the ring $\mathbb{Q}[u_1, \ldots, u_d, y_1, \ldots, y_n]$ can also be considered as a polynomial in the ring $\mathbb{K}_0[y_1, \ldots, y_n]$. The degree of F in some variable y_i will be denoted by $deg_{y_i}(F)$. A finite set $\mathcal{A}$ of polynomials is called an *ascending set* if it can be put in the form

$$A_1(u, y_1), A_2(u, y_1, y_2), \ldots, A_r(u, y_1, y_2, \ldots, y_r),$$

with $A_i \in \mathbb{Q}[u, y_1, \ldots, y_i]$, y_i actually occurs in A_i (i.e., $deg_{y_i}(A_i) > 0$) for each i and $deg_{y_j}(A_i) < deg_{y_j}(A_j)$ for each pair $j < i$. It is said to be *quasilinear* if $r = 1$, or $r > 1$ while $deg_{y_2}(A_2) = \cdots = deg_{y_r}(A_r) = 1$. For an ascending set $\mathcal{A}$, y_i will be called the *leading variable* of A_i, and the leading coefficient of A_i in y_i will be called the *initial* of A_i for each i. A polynomial F is said to be *reduced* with respect to $\mathcal{A}$ if $deg_{y_i}(F) < deg_{y_i}(A_i)$ for all i.

For any polynomial set $\mathcal{F}$ we denote the set of common zeros of the polynomials in $\mathcal{F}$ by $Zero(\mathcal{F})$. For any non-zero polynomial G, we write $Zero(\mathcal{F}/G)$ for $Zero(\mathcal{F}) \setminus Zero(G)$. An ascending set $\mathcal{C}$ is called a *characteristic set* of a polynomial set $\mathcal{F}$ if

$$Zero(\mathcal{C}/J) \subset Zero(\mathcal{F}) \subset Zero(\mathcal{C}),$$

where J is the product of initials of the polynomials in $\mathcal{C}$. For any polynomial set $\mathcal{F}$, one can either determine $Zero(\mathcal{F}) = \emptyset$ or compute a characteristic set $\mathcal{C}$ of $\mathcal{F}$ and a sequence of ascending sets $\mathcal{C}_1, \ldots, \mathcal{C}_t$, called a characteristic series of $\mathcal{F}$, such that

$$Zero(\mathcal{F}) = \bigcup_{i=1}^{t} Zero(\mathcal{C}_i/J_i),$$

where J_i is the product of initials of the polynomials in $\mathcal{C}_i$, by Ritt-Wu's characteristic sets method [13, 14, 26, 27, 28].

Let $\mathcal{A}$ be an ascending set as before with $r = 1$. It is said to be *irreducible* if A_1, as a polynomial in $\mathbb{K}_0[y_1]$, is irreducible. In the case it is, let η_1 an extended zero of A_1. Then the field obtained from $\mathbb{K}_0$ by adjoining the algebraic element η_1 is called a *single algebraic extension field* of $\mathbb{K}_0$, denoted as $\mathbb{K}_1 = \mathbb{K}_0(\eta_1)$, and the irreducible polynomial A_1 is called the *minimal polynomial* of η_1 or the *adjoining polynomial* of $\mathbb{K}_0(y_1)$ for y_1, where $\mathbb{K}_0(y_1)$ is written for $\mathbb{K}_0(\eta_1)$.

Consider now an ascending set $\mathcal{A}$ as before with $r > 1$. It is said to be *irreducible* if A_i, as a polynomial in $\mathbb{K}_{i-1}[y_i]$, is irreducible, where $\mathbb{K}_{i-1} = \mathbb{K}_{i-2}(y_{i-1})$ with A_{i-1} as adjoining polynomial, for each $i \geq 2$. The fields $\mathbb{K}_1, \mathbb{K}_2, \ldots, \mathbb{K}_r$ are called the *successive algebraic extension fields* of $\mathbb{K}_0$ with adjoining polynomials $A_1, \ldots, A_r$, or simply with adjoining ascending set $\mathcal{A}$. Clearly, all the fields $\mathbb{K}_2, \ldots, \mathbb{K}_r$ are multiple algebraic extensions.

From the definition, we see that if in an ascending set $\mathcal{A}$ there is only one polynomial A_i with $deg_{y_i}(A_i) > 1$ for some i (e.g., a quasilinear ascending set), then $\mathcal{A}$ is irreducible if and only if A_i, as a polynomial in $\mathbb{K}_0[y_i]$, is irreducible.

Let us first give two propositions without proof which provide some simple criteria for the irre-

[1] This was first discovered by Abbott, Bradford and Davenport as pointed out in [3] and [4], but no detail was published.

ducibility test and the factorization of a polynomial over an algebraic extension field.

Proposition 1. *Let $A(x)$ and $F(y)$ be two irreducible polynomials of degrees m and n in x and y, respectively, with coefficients in some extension field $\mathbb{K}$ of $\mathbb{Q}$. If m and n are relatively prime, then F is always irreducible over the algebraic extension field $\mathbb{K}(x)$ with $A(x)$ as adjoining polynomial.*

Proposition 2. *Let $A(x)$ and $F(y)$ be two irreducible polynomials in x and y with coefficients in some extension field $\mathbb{K}$ of $\mathbb{Q}$, and let $A^*(x,z)$ and $F^*(y,z)$ be the homogenization of A and F by z with respect to x and y, respectively. Let R^* be the pseudo-remainder of F^* with respect to A^* in z with I the leading coefficient of A^* (in z) such that $I^sF^* = Q^*A^* + R^*$ for some integer $s \geq 0$. Then the factorization[2] of $R = R^*|_{z=1}$ over $\mathbb{K}$ divided by I^s is a factorization (not necessarily complete) of F over the algebraic extension field $\mathbb{K}(x)$ with $A(x)$ as adjoining polynomial.*

Although the second proposition is quite trivial, it is useful for some cases. For instance, among the 23 factorization examples taken from the literature listed in the appendix, 6 benefit from a simple test using this proposition. Similarly, the following proposition is also sometimes useful for the reducibility test when the extension field involves transcendental elements.

Proposition 3. *Let $A(u,x)$ and $F(u,y)$ be two irreducible polynomials in u,x and u,y with coefficients in some extension field $\mathbb{K}$ of $\mathbb{Q}$. Let R be the pseudo-remainder of F with respect to A in u with I the leading coefficient of A (in u) such that $I^sF = QA + R$ for some integer $s \geq 0$. Then the factorization of R over $\mathbb{K}$ divided by I^s, upon reducing the higher powers of x in each component by $A(u,x)$, is a factorization (not necessarily complete) of $F(u,y)$ over the extension field $\mathbb{K}(u,x)$ with u a transcendental element and $A(u,x)$ the adjoining polynomial for x.*

In what follows $\mathcal{A} = \{A_1(u,y_1),\ldots,A_r(u,y_1,\ldots,y_r)\}$ will always be understood as an irreducible ascending set and $\mathbb{K}_r = \mathbb{K}_0(y_1,\ldots,y_r)$ the successive algebraic extension field of $\mathbb{K}_0$ with $\mathcal{A}$ as adjoining ascending set as before. Let $F(u,y_1,\ldots,y_r,y)$ be a polynomial irreducible over the rational number field $\mathbb{Q}$ and reduced with respect to $\mathcal{A}$, and set $\mathcal{A}^+ = \{A_1,\ldots,A_r,F\}$. Clearly $\mathcal{A}^+$ is an ascending set with respect to the variable ordering $y_1 \prec \cdots \prec y_r \prec y$. The polynomial F is irreducible over the algebraic extension field $\mathbb{K}_r$ if and only if the ascending set $\mathcal{A}^+$ is irreducible. While speaking that F' is a factor of F over $\mathbb{K}_r$, we shall always mean $deg_y(F') > 0$ (i.e., F' is not a number in $\mathbb{K}_r$). F' is said to be a true factor of F if $0 < deg_y(F') < deg_y(F)$. For an expression E, $E|_{y=g}$ denotes the expression obtained from E by substituting the expression g for the variable y occurring in E as usual.

In the rest of this section we fix the above notations and state two lemmas which guarantee the correctness and termination of our factorization algorithm to be described in the next section. The formal proofs of these lemmas require some knowledge about characteristic sets and algebraic geometry and are left for a forthcoming paper.

Lemma 1. *Let $c_1,\ldots,c_r$ be a set of numbers in $\mathbb{K}_0$, $\mathcal{C}$ a characteristic set and $\mathcal{C}_1,\ldots,\mathcal{C}_t$ a characteristic series of $\{A_1,\ldots,A_r,F|_{y=y-c_1y_1-\cdots-c_ry_r}\}$ with respect to the variable ordering $y \prec y_1 \prec \cdots \prec y_r$.*

(a) Let $\mathcal{C}_i^* = \mathcal{C}_i|_{y=y+c_1y_1+\cdots+c_ry_r}$ for each i. If $\mathrm{Zero}(\mathcal{A}^+ \cup \mathcal{C}_i^*) \neq \emptyset$ (over some extension field of $\mathbb{K}_0$), then the characteristic set $\bar{\mathcal{C}}_i$ of $\mathcal{A}^+ \cup \mathcal{C}_i^*$ with respect to the variable ordering $y_1 \prec \cdots \prec y_r \prec y$ contains exactly $r+1$ polynomials. In this case, the last polynomial F_i in $\bar{\mathcal{C}}_i$ is a factor of F over $\mathbb{K}_r$. If $\mathcal{C}_i$ is irreducible (with respect to the variable ordering $y \prec y_1 \prec \cdots \prec y_r$), then $\mathrm{Zero}(\mathcal{A}^+ \cup \mathcal{C}_i^*) \neq \emptyset$ and F_i is an irreducible factor of F over $\mathbb{K}_r$.

(b) If $\mathcal{C}$ is quasilinear and its first polynomial has an irreducible factor C (over $\mathbb{K}_0$) which is not a factor of the initial of any polynomial in $\mathcal{C}$, then the GCD of F and $C|_{y=y+c_1y_1+\cdots+c_ry_r}$ (performed over $\mathbb{K}_r$) is an irreducible factor of F over $\mathbb{K}_r$.

(c) Let Ψ be the set of polynomials obtained from all irreducible factors (over $\mathbb{K}_0$) of the first polynomial in $\mathcal{C}$ and Δ the set of polynomials obtained from all irreducible factors (over $\mathbb{K}_0$) of initials of the polynomials in $\mathcal{C}$ by substituting $y+c_1y_1+\cdots+c_ry_r$ for y. If $\mathcal{C}$ is quasilinear, then either there is a polynomial in Ψ which is not a factor of any polynomial in Δ, or there is a polynomial P in Δ such that the

[2]There is more possibility for R to be reducible when R^* does not contain the variable z.

GCD of F and P over $\mathbb{K}_r$ is a true factor of F over $\mathbb{K}_r$, or F is irreducible over $\mathbb{K}_r$.

Lemma 2. *If $F(u, y_1, \ldots, y_r, y)$ is squarefree over $\mathbb{K}_r$, then there are only finitely many sets of numbers $c_1, \ldots, c_r$ in $\mathbb{K}_0$, with all c_i's different from each other for every i, such that the characteristic set of $\{A_1, \ldots, A_r, F|_{y=y-c_1y_1-\cdots-c_ry_r}\}$ with respect to the variable ordering $y \prec y_1 \prec \cdots \prec y_r$ is not quasilinear.*

Since the factorization of a polynomial F over the algebraic extension field $\mathbb{K}_r$ is unique only up to a "constant" factor in $\mathbb{K}_r$ which in our case is represented as a polynomial in $u, y_1, \ldots, y_r$, the size of each factor of F may be dramatically affected by such a constant. Let F' be an irreducible factor of F. We may assume, without loss of generality, that F' is in $\mathbb{Q}[u, y_1, \ldots, y_r, y]$ with its leading coefficient $I' = I'(u, y_1, \ldots, y_r)$ in y. In general, I' involves both the variables u and $y_1, \ldots, y_r$. If I' involves only the variables u, we say that F' is a normal factor of F over $\mathbb{K}_r$. By an algorithm presented in [19], we can compute, from F' and $\mathcal{A}$, a polynomial $\bar{F}'$ in $\mathbb{Q}[u, y_1, \ldots, y_r, y]$ with its leading coefficient $\bar{I}' = \bar{I}'(u) \in \mathbb{Q}[u]$ in y such that $\bar{F}'$ differs from F' only by a factor in $\mathbb{K}_r$. $\bar{F}'$ is called the *normalization* of F' with respect to $\mathcal{A}$. We note that in many case the normalized polynomial is much simpler than the original one. But the opposite is also true in many other cases.

3. Description of the Factorization Algorithm

In this section we describe the main algorithm for factorizing multivariate polynomials over successive algebraic extension fields. Here we assume that one knows how to factorize multivariate polynomials over the field $\mathbb{Q}$ of rational numbers.

Algorithm F (*for factorizing multivariate polynomials over successive algebraic extension fields*). Let $\mathcal{A} = \{A_1(u_1, \ldots, u_d, y_1), \ldots, A_r(u_1, \ldots, u_d, y_1, \ldots, y_r)\}$ be an irreducible ascending set and $F(u_1, \ldots, u_d, y_1, \ldots, y_r, y)$ a polynomial reduced with respect to $\mathcal{A}$ and irreducible over $\mathbb{Q}$, with all polynomials having rational coefficients. This algorithm computes an irreducible factorization of F, considered as a polynomial in y, over the multiple, successive extension field $\mathbb{K}_r = \mathbb{Q}(u_1, \ldots, u_d, y_1, \ldots, y_r)$ obtained from $\mathbb{Q}$ by adjoining the transcendental elements $u_1, \ldots, u_d$ and the algebraic elements $y_1, \ldots, y_r$ with adjoining polynomials $A_1, \ldots, A_r$, assumed that F is squarefree over $\mathbb{K}_r$.

F1. [Test trivial cases.] If $deg_y(F) \le 1$, or $r = 1$ and $deg_{y_1}(A_1)$ and $deg_y(F)$ are relatively prime, then the procedure terminates and return F. Otherwise, let $\mathcal{A}^*$ be the set of those A_i in $\mathcal{A}$ with $deg_{y_i}(A_i) > 1$. If $\mathcal{A}^*$ is empty, then the procedure terminates and return F. Otherwise, try to obtain a factorization using Propositions 2 and 3 for F and $\mathcal{A}^*$ and, if successful, apply Algorithm F to each component of the obtained factorization. Otherwise, let $y_{p_1}, \ldots, y_{p_s}$ with $p_1 < \cdots < p_s$ be the leading variables of the polynomials in $\mathcal{A}^*$ and choose a set of integers $c_1, \ldots, c_s$.

F2. [Characteristic set computation.] Let $F^* = F|_{y=y-c_1y_{p_1}-\cdots-c_sy_{p_s}}$. Compute a characteristic set $\mathcal{C}^*$ of $\mathcal{A}^* \cup \{F^*\}$ with respect to the variable ordering $y \prec y_{p_1} \prec \cdots \prec y_{p_s}$. Let Δ be the set of all irreducible factors (over $\mathbb{K}_0$) of initials of the polynomials in $\mathcal{C}^*$ and Ψ the set of those irreducible factors (over $\mathbb{K}_0$) of the first polynomial in $\mathcal{C}^*$ which are not factors of any polynomial in Δ.

F3. [Test quasilinearity.] If $\mathcal{C}^*$ is quasilinear, then go to step F4; otherwise, if Ψ contains more than one polynomial, then set $\Delta \leftarrow \Delta \cup \Psi$, $\Psi \leftarrow \emptyset$ and go to step F4. Otherwise, choose a new set of integers $c_1, \ldots, c_s$, each new c_i different from all the previously chosen c_i's, and go to step F2.

F4. [GCD computation.] Set $G \leftarrow F$, $\Psi \leftarrow \Psi|_{y=y+c_1y_{p_1}+\cdots+c_sy_{p_s}}$ and $\Delta \leftarrow \Delta|_{y=y+c_1y_{p_1}+\cdots+c_sy_{p_s}}$. For each $P \in \Psi \cup \Delta$, compute the GCD F_P of G and P with respect to y with normalization, and then set $G \leftarrow G/F_P$ over $\mathbb{K}_r$. If some true factors of F (over $\mathbb{K}_r$) are found, then apply Algorithm F to F_P (and $\mathcal{A}^*$) and let the obtained irreducible factorization of F_P be F_P^* for all $P \in \Delta \cup \{G\}$, the procedure terminates, and return $\prod_{P\in\Psi} F_P \prod_{P\in\Delta\cup\{G\}} F_P^*$. Otherwise, if $\mathcal{C}^*$ is quasilinear, then the procedure terminates and return F. Otherwise, choose a new set of integers $c_1, \ldots, c_s$, each new c_i different from all the previously chosen c_i's, and go to step F2.

An immediate variation of the above algorithm is to compute not only the characteristic set but also the characteristic series in step F2. The irreducible factors of F are determined from those ascending sets in the series whose irreducibility can be easily verified. An advantage of using characteristic series is that one can employ the various strategies developed for characteristic series computation, for example, factorizing some intermediate polynomials at an early stage. Also, the ordering for the variables $y, y_{p_1}, \ldots, y_{p_s}$ may be arbitrary as long as y is arranged with the lowest order. Moreover, the basic idea used in this step is to obtain polynomials in $\mathbb{Q}[u, y]$ by successive elimination of the variables; therefore, other elimination methods might also be used for this purpose. We shall investigate such possibilities in our future work.

The method described above is of sufficient generality. If the transcendental elements u do not appear in the minimal polynomials (adjoining ascending set), the factorization can be viewed as performed over the usually called *algebraic number field* $\mathbb{Q}(y_1, \ldots, y_r)$. If the u appear in the minimal polynomials, the factorization is then performed over the usually called *algebraic function field* $\mathbb{K}_r$. We have realized that in the case of having transcendentals the algorithm is relatively slow. This is mainly because the involvement of the free variables u greatly increases the complexity of computing characteristic sets and GCDs. It turns out that in this case the modular methods [12, 24, 22, 23] of using integer substitution and Hensel lifting are better and thus the use of this substitution technique for our algorithm is desirable and remain for further investigation. We also plan to borrow integer substitution to reduce multivariate polynomials to unary ones but use other techniques such as solving polynomial equations to finally construct the multivariate factors. One possible way is to generalize the method proposed in [6, 17]. Here we sketch another heuristic procedure we have tried and which works in some cases.

If the polynomial $F(u, y_1, \ldots, y_r, y)$ has a complete factorization $F_1(u, y_1, \ldots, y_r, y) \cdots F_t(u, y_1, \ldots, y_r, y)$ over $\mathbb{K}_r$ with adjoining ascending set $\mathcal{A}$ and $a = (a_1, \ldots, a_d)$ is a set of suitable integers which, while substituted for $(u_1, \ldots, u_d)$, does not make the leading coefficient of F in y vanishing nor change the irreducibility of $\mathcal{A}$ and $F_1, \ldots, F_t$, then $F_1(a, y_1, \ldots, y_r, y) \cdots F_t(a, y_1, \ldots, y_r, y)$ is a complete factorization of $F(a, y_1, \ldots, y_r, y)$. If for some suitably chosen integers $F(a, y_1, \ldots, y_r, y)$ is irreducible, then $F(u, y_1, \ldots, y_r, y)$ is also irreducible. Now, let F_1 be written as a polynomial of total degree m in the variables u with intertermi-nate coefficients, say $z_1, \ldots, z_M$. Then by substituting the integers $a_1, \ldots, a_d$ for $u_1, \ldots, u_d$ respectively, we have a linear equation of the form $b_1 z_1 + \cdots + b_M z_M = F_1(a, y_1, \ldots, y_r, y)$ with all $b_1, \ldots, b_M$ integers. Therefore, if we choose M sets of integers for the substitution, we should obtain a system of M linear equations. For each set a of suitable integers, $F_1(a, y_1, \ldots, y_r, y)$ is one of the factors of $F(a, y_1, \ldots, y_r, y)$ factorized over $\mathbb{Q}(y_1, \ldots, y_r)$. Hence, the indeterminate coefficients can be determined by simply solving systems of linear equations. It occurs that this procedure is feasible only when we are able to determine the correspondence of factors in the factorization of $F(a, y_1, \ldots, y_r)$ and the corresponding factors are not shifted with some constant for different a. Otherwise, though we may determine the indeterminate coefficients still by trying all combinations and thus solving many systems of linear equations, the procedure has no practical value.

We are also aware that the modular methods may be used for irreducibility test in our algorithm when no transcendental element is involved.

4. Implementation Details and Experiments

The described algorithm was implemented together with the charsets package by this author in the Maple system in Autumn 1990. The implementation has been considerably modified and improved during the preparation of this paper. It is clear that the efficiency of our algorithm heavily depends upon the computation of characteristic sets and the computation of GCDs over algebraic fields. In our implementation, the later is realized also via the computation of so-called *nearly characteristic sets* (which in the present case is mainly the formation of polynomial remainder sequences). We have noticed a few implementation details which may affect the efficiency of our algorithm and should be carefully taken into account. Let us mention some of them as follows.

- During the computation of characteristic sets some possible initial factors should be removed from the occurring polynomials in order to control their expansion.

- It is helpful to use the strategy presented in [21] for the computation of characteristic sets which has a speed-up of several times in many cases.
- The normalization in step F4 is crucial for some cases. Since normalization may produce more complicated polynomials and thus increase the computational expenses, the use of normalization should be heuristic. In our implementation, whether the normalization process continues depends on the growth of the number of terms of the occurring polynomials.
- The choice of smaller integers $c_1, \ldots, c_s$ is recommendable. In case F involves some of the variables $y_1, \ldots, y_r$, 0 is first used (i.e., no linear transformation is made).
- In step F4 the computation of GCDs should be performed for a proper order of the polynomials in $\Psi \cup \Delta$. We have observed that it is better to compute the GCDs first for polynomials in Ψ, starting from those of lower degree, and then for polynomials in Δ, also starting from those of lower degree.
- In practice we do not actually need the assumption on the squarefreeness of F and thus do not need the squarefree decomposition as long as we can still produce a quasilinear characteristic set. This is the case almost for all examples. Moreover, we usually only need to do the linear transformation once.

Our implementation of the algorithm also contains a routine for the heuristic procedure explained in the end of the last section. We feel that the current implementation has plenty of scope for further improvement. At the moment, the author's general-purpose implementation of the characteristic sets package is used. As for the characteristic set computation in step F2 of Algorithm F where the input set of polynomials has a special form, we may improve the computation by taking this form into account. In the characteristic set and GCD computation pseudo-division may all be replaced by subresultant computation. We shall investigate and compare the different variants in the future.

Below we give in table form the timing statistics on a set of 40 test examples for our current implementation of Algorithm F in Maple 4.3. These examples together with an indication on their source are listed in the appendix. The experiments were made on an Apollo DN10000 under a Unix operating system OS 10.3. The timings are given in CPU seconds and include the time for garbage collection. The computation was interrupted manually after 3600 CPU seconds, which is indicated by > 3600. The meaning of the headings of the table is explained as follows: Ex — the example number; d — the number of transcendental elements for the extension field; $deg(\mathcal{A})$ — the degrees of polynomials in the adjoining ascending set, separated by the slant; $deg(F)$ — the degree of the polynomial to be factorized; factor — time for the Maple 4.3 built-in factorization function; cfactor — time for our implementation of Algorithm F in Maple 4.3. Those examples to which the Maple built-in factor is not applicable for the reason "multivariate algebraic factorisation not implemented" are indicated by the long dash ——.

The table shows that our algorithm is feasible for factorizing polynomials of a reasonable size over algebraic extension fields. The efficiency of the algorithm does not much depend on the reducibility of the polynomial to be factorized. Since our implementation is based on the Maple system and it uses a number of Maple's built-in functions, it seems appropriate to take the Maple built-in function factor which is professionally implemented as a bed for our comparison. From the table, one sees that for all those example to which the Maple built-in function is applicable, our implemented function based on Algorithm F is always faster. We have also noticed the early timings of Wang [22] in Macsyma, the timings of Lenstra [10] in Algol 68 and the recent timings of Abbott [1] in Reduce. Both the timings in [22] and in [10] still remain encouraging (though some examples given there are rather simple). According to an indirect comparison with the timings provided in [1], our algorithm does not seem to be worse than the algorithm of Lenstra in practice. Since the factorization for the fifth example in [10] is incomplete, we are not quite sure whether the doubt on the implementation of his algorithm has been completely cleared up. Wang was able to factorize the polynomials for the 10th and 11th example in about hundred seconds in Macsyma 254 on a PDP-10, while our algorithm at the present stage has difficulties to deal with these two examples as indicated with *** in the table. The main reason for this is that

Timing Statistics in Maple 4.3

Ex	d	$deg(\mathcal{A})$	$deg(F)$	factor	cfactor
1	0	2	4	1.667	0.100
2	0	2	4	——	1.083
3	0	2	4	——	1.417
4	0	2	2	——	0.133
5	0	2	2	1.250	0.867
6	0	2	4	2.783	0.800
7	0	3	6	3.734	1.667
8	0	4	4	19.383	4.884
9	1	4	4	——	1.734
10	2	4	4	——	***
11	4	4	5	——	***
12	0	2	2	——	0.500
13	0	6	3	6.816	5.000
14	0	2	14	6.250	5.933
15	0	2	6	10.167	3.550
16	0	4	8	34.083	18.250
17	0	9	9	>3600	393.166
18	0	2/2/2	4	76.900	33.266
19	0	9	9	29.284	14.700
20	1	2	2	——	0.166
21	0	2	2	1.767	0.803
22	0	3	5	——	7.883
23	1	2/2	3	——	12.850
24	0	32	4	——	209.567
25	1	3	4	——	2.216
26	1	5	2	——	2.266
27	0	5	6	55.066	18.417
28	0	6	8	♦>160	61.000
29	0	7	9	398.283	211.483
30	0	8	10	♦>720	294.166
31	0	11	9	——	673.950
32	1	3	4	——	3.717
33	0	2/2	3	——	8.833
34	1	2/2	3	——	15.133
35	2	5	7	——	40.217
36	0	5	6	——	55.617
37	0	5	7	——	14.400
38	1	3	5	——	5.867
39	0	3/2	6	——	769.033
40	0	3/2/2	2	——	2204.484

♦Computation terminated after the indicated time due to a Maple bug. The cases indicated with *** are explained below.

Wang's modular technique of reducing multivariate polynomials to unary ones by integer substitution is very powerful, whereas this substitution technique has not yet been considered in our algorithm. For the above mentioned two examples, if we substitute some variables by integers then the obtained polynomials can be easily factorized over the algebraic extension fields by our algorithm as well. However, the heuristic procedure discussed in the end of Section 3 does not work for either of these two examples. If we straightforwardly apply Algorithm F to them, the computation may run out of a reasonable time limit. We shall concentrate our work on improving our method on this aspect in the future.

References

[1] Abbott, J. A., *On the Factorization of Polynomials over Algebraic Fields*, Ph.D thesis, School of Math. Scis., University of Bath, England (1989).

[2] Abbott, J. A., Bradford, R. J. and Davenport, J. H., A Remark on Factorization, *ACM SIGSAM Bulletin* **19**, 31–33 & 37 (1985).

[3] Abbott, J. A., Bradford, R. J. and Davenport, J. H., The Bath Algebraic Number Package, *Proc. SYMSAC'86* (Waterloo, July 21–23, 1986), 250–253.

[4] Abbott, J. A. and Davenport, J. H., Polynomial Factorization: an Exploration of Lenstra's Algorithm, *Proc. EUROCAL'87* (Leipzig, June 2–5, 1987), 391–402.

[5] Hodge, W. V. D. and Pedoe, D., *Methods of Algebraic Geometry*, Vol. I, II, Cambridge University Press, Cambridge (1947/1952).

[6] Hu, S. and Wang, D. M., Fast Factorization of Polynomials over Rational Number Field or its Extension Fields, *Kexue Tongbao* **31**, 150–156 (1986).

[7] Kaltofen, E., Factorization of Polynomials, *Computer Algebra: Symbolic and Algebraic Computation (B. Buchberger, G. E. Collins and R. Loos, eds.)*, Springer-Verlag, Wien-New York, 95–113 (1982).

[8] Kaltofen, E., Polynomial Factorization 1982–1986, *Computers in Mathematics* (D. V. Chudnovsky and R. D. Jenks, eds.), Marcel Dekker, Inc., New York-Basel, 285–209 (1990).

[9] Landau, S., Factoring Polynomials over Algebraic Number Fields, *SIAM J. Comput.* **14**, 184–195 (1985).

[10] Lenstra, A. K., Lattices and Factorization of Polynomials over Algebraic Number Fields, *Proc. EUROCAM'82* (Marseille, April 5–7, 1982), 32–39.

[11] Lenstra, A. K., Factoring Multivariate Polynomials over Algebraic Number Fields, *SIAM J. Comp.* **16**, 591–598 (1987).

[12] Musser, D. R., Multivariate Polynomial Factorization, *J. ACM* **22**, 291–308 (1975).

[13] Ritt, J. F., *Differential Equations from the Algebraic Standpoint*, Amer. Math. Soc., New York (1932).

[14] Ritt, J. F., *Differential Algebra*, Amer. Math. Soc., New York (1950).

[15] Trager, B. M., Algebraic Factoring and Rational Function Integration, *Proc. 1976 ACM Symp. Symbolic and Algebraic Comp.* (Yorktown Heights, New York, August 10–12, 1976), 219–226.

[16] van der Waerden, B. L., *Modern Algebra*, Vol. 1, Frederick Ungar Publ. Co., New York (1953).

[17] Wang, D. M., *Mechanical Approach for Polynomial Set and its Related Fields (in Chinese)*, Ph.D thesis, Institute of Systems Science, Academia Sinica, China (1987).

[18] Wang, D. M., *Characteristic Sets and Zero Structure of Polynomial Sets*, Lecture Notes, RISC-LINZ, Johannes Kepler University, Austria (1989).

[19] Wang, D. M., Some Notes on Algebraic Methods for Geometry Theorem Proving, *Preprint*, RISC-LINZ, Johannes Kepler University, Austria (1990).

[20] Wang, D. M., An Implementation of the Characteristic Set Method in Maple, *RISC-Linz Series* no. 91-25.0, Johannes Kepler University, Austria (1991).

[21] Wang, D. M., A Strategy for Speeding up the Computation of Characteristic Sets, *Preprint*, Johannes Kepler University, Austria (1991).

[22] Wang, P. S., Factoring Multivariate Polynomials over Algebraic Number Fields, *Math. Comp.* **30**, 324–336 (1976).

[23] Wang, P. S., An Improved Multivariate Polynomial Factoring Algorithm, *Math. Comp.* **32**, 1215–1231 (1978).

[24] Wang, P. S. and Rothschild, L. P., Factoring Multivariate Polynomials over the Integers, *Math. Comp.* **29**, 935–950 (1975).

[25] Weinberger, P. J. and Rothschild, L. P., Factoring Polynomials over Algebraic Number Fields, *ACM Trans. Math. Software* **2**, 335–350 (1976).

[26] Wu, W. T., Basic Principles of Mechanical Theorem Proving in Elementary Geometries, *J. Sys. Sci. & Math. Scis.* **4**, 207–235 (1984); *J. Automated Reasoning* **2**, 221–252 (1986).

[27] Wu, W. T., *Basic Principles of Mechanical Theorem Proving in Geometries* (Part on Elementary Geometries, in Chinese), Science Press, Beijing (1984).

[28] Wu, W. T., On Zeros of Algebraic Equations — An application of Ritt principle, *Kexue Tongbao* **31**, 1–5 (1986).

Appendix. Test Examples

We have collected some examples (1–23 below) appeared in the literature for the test of our algorithm. However, these examples are not quite sufficient for observing the overall behavior of the algorithm for the following reasons. First, the algebraic extension fields in all but one from [2] and one from [20] of these examples are single algebraic extensions, while our algorithm is designed for multiple, successive algebraic extensions. Second, the polynomials in all but a trivial one from [25] of these examples are reducible, while in application most of the occurring polynomials to be factorized are irreducible. Third, most of these examples seem to have been constructed artificially and thus have a strong mathematical flavor, while the polynomials required to be factorized in general problem solving may not always be in such a case. For these reasons, we have randomly generated 14 examples (27–40) in addition to the known examples in the literature for our test. Since the randomly generated polynomials (except some trivial factors) are always irreducible, the reducible polynomials (36–40) were obtained by multiplying some randomly generated polynomials. We have also included 3 examples (24–26) which appeared in some application problems and have been used for author's test for a period of time. The source of the examples taken from the literature is as follows: 1–11 from [22], 12–13 from [25], 14 from [15], 15–17 from [10], 18 from [2], 19–20 from [1], 21 from [6] and 22–23 from [20]. In each item of the following list, the first entry is the polynomial F to be factorized together with its factorization if reducible or an indication of its irreducibility (except for two incomplete examples 10 and 11), the second is the adjoining ascending set $\mathcal{A}$ (consisting of the minimal polynomials) and the third is the variable ordering (corresponding to $y_1 \prec \cdots \prec y_r \prec y$ used throughout the paper). Those variables which do not appear in the third entry are considered as transcendental elements.

1. $x^4 - 1 = (x-1)(x+1)(x-a)(a+x)$; $\{a^2+1\}$; $a \prec x$.
2. $x^4 + ax^3 + 2x^3 + 2ax^2 + 5x^2 + 2ax + 6x + 6 = (x+1+a)(x+1-a)(x^2+ax+3)$; $\{a^2+1\}$; $a \prec x$.
3. $2ax^4 + 3x^4 + 3ax^3 - 2x^3 - 2ax^2 - 2x^2 + ax - 1 = (2a+3)(-2a+3+13x^2)(x^2+ax-1)/13$; $\{a^2+1\}$; $a \prec x$.
4. $y^2 + x^2 = -(ay-x)(ay+x)$; $\{a^2+1\}$; $a \prec x$.
5. $x^2 + x - 1 = (2x+1+a)(2x+1-a)/4$; $\{a^2-5\}$; $a \prec x$.
6. $x^4 + 3x^2 + 4 = (a+x)(x-1-a)(x-a)(x+1+a)$; $\{a^2+a+2\}$; $a \prec x$.
7. $64x^6 - 4 = (2x+a)(4x^2-2ax+a^2)(2x-a)(4x^2+2ax+a^2)$; $\{a^3+2\}$; $a \prec x$.
8. $16x^4 + 8x^3 + 4x^2 + 2x + 1 = (2x-a)(2x-a^3)(-a^2+2x)(2x+a^3+a^2+a+1)$; $\{a^4+a^3+a^2+a+1\}$; $a \prec x$.
9. $x^4 + y^4 = (ay-x)(ay+x)(a^3y-x)(a^3y+x)$; $\{a^4+1\}$; $a \prec x$.
10. $x^8 + 2x^7 + (-y-z^2-8)x^6 + (-4y+6z^2-40)x^5 + (y^2+(2z^2-48)y+z^4+32z^2+256)x^4 + (-4y^2+(2z^2+32)y-4z^4+32z^2+960)x^3 + (-y^3+(-3z^2+28)y^2+(2z^4-4z^2+384)y-z^6-32z^4+144z^2-1152)x^2 + (2y^3+(-4z^2+72)y^2+(6z^4+24z^2-576)y+2z^6-48z^4-576z^2+3456)x + y^4 + (-z^2-12)y^3 + (z^4+24z^2+144)y^2 + (-z^6+24z^4-432z^2-1728)y + z^8 - 12z^6 + 144z^4 - 1728z^2 + 20736$; $\{a^4+a^3+a^2+a+1\}$; $a \prec y$.
11. $x^5 - 5vyx^3 - 5uzx^3 + 5uy^2x^2 + 5z^2yx^2 + 5v^2zx^2 + 5vu^2x^2 - 5zy^3x + 5v^2y^2x - 5vuzyx - 5u^3yx - 5vz^3x + 5u^2z^2x - 5v^3ux + y^5 - 5vuy^3 + 5vz^2y^2 + 5u^2zy^2 - 5uz^3y - 5v^3zy + 5v^2u^2y + z^5 + 5v^2uz^2 - 5vu^3z + u^5 + v^5$; $\{a^4+a^3+a^2+a+1\}$; $a \prec x$.
12. $x^2 + ax + 1$ (irreducible); $\{a^2+1\}$; $a \prec x$.
13. $x^3 - 3 = (12x - 11a - 2a^3 - a^5 + 7a^2 - a^4 - 16)(6x + 4a + 4a^3 + a^5 - a^2 + 2a^4 + 14)(12x + 3a - 6a^3 - a^5 - 5a^2 - 3a^4 - 12)/864$; $\{a^6 + 3a^5 + 6a^4 + a^3 - 3a^2 + 12a + 16\}$; $a \prec x$.
14. $x^{14} - 2x^8 - 2x^7 - 2x^4 - 4x^3 - x^2 + 2x + 1 = (ax - 2x + ax^2 - x^2 + x^7 - 1)(x^7 - ax^2 + x^2 - ax - 1)$; $\{a^2 - 2a - 1\}$; $a \prec x$.
15. $(47x^6 + 21x^5 + 598x^4 + 1561x^3 + 1198x^2 + 261x + 47)/47 = (-121ax - 70x - 121ax^2 + 71x^2 + 47x^3 - 47)(47x^3 - 50x^2 + 121ax^2 - 191x + 121ax - 47)/2209$; $\{a^2 - a + 3\}$; $a \prec x$.
16. $x^8 - x^7 - x^6 + x^4 - x^2 + x + 1 = (-x + ax + x^2 + a^2x + a^3x - 1)(-1 - ax + 2ax^3 + 3x^2 - 3x^4 - a^2x + a^2x^4 + a^3x^3 + x^6 + 2a^2x^3 - 2a^3x^2 - a^3x - a^2x^2 - ax^5 - a^3x^5 - a^2x^5 + 2a^3x^4)$; $\{a^4 - a + 1\}$; $a \prec x$.
17. $x^9 + 9x^8 + 36x^7 + 69x^6 + 36x^5 - 99x^4 - 303x^3 - 450x^2 - 342x - 226 = (x+1-a)(a+ax+a^2+1+x^2+2x)(25x^2+25ax+50x+25a+25-87a^2-15a^5+a^8)(395a+3a^8+395ax-45a^5-261a^2-10a^7+175a^4+175a^4x-10a^7x+75+150x+75x^2)(75x^2-470ax+150x-175a^4x+10a^7x-45a^5+3a^8+75-261a^2-470a-175a^4+10a^7)/140625$; $\{a^9 - 15a^6 - 87a^3 - 125\}$; $a \prec x$.
18. $x^4 + 2x^3 + x^2 - 1 = (2x - ac + 1)(2x + 1 + ac)(2x + 1 + ab)(2x + 1 - ab)/16$; $\{a^2+1, b^2-3, c^2+5\}$; $a \prec b \prec c \prec x$.
19. $x^9 - 54 = (x-a)(a^2+x^2+ax)(x^6+x^3a^3+a^6)$; $\{a^9 - 54\}$; $a \prec x$.
20. $x^2 - z^4 + 2z^2a - z = (x + a - z^2)(x - a + z^2)$; $\{a^2 - z\}$; $a \prec x$.
21. $x^2 + x + 1 = (2x+1+a)(2x+1-a)/4$; $\{a^2+3\}$; $a \prec x$.
22. $745092b - 252156 + 540900c + 21032664c^2b^2 + 2010720b^2 + 7117713c^2b - 132367c^2 + 3076830c^3 - 7843500c^3b^2 + 2792322c^3b - 3779244bc - 10724400b^2c + 21225240bc^5 + 26306208b^2c^5 + 8257464c^5 - 436536c^4 + 6094008b^2c^4 + 594432bc^4 = 8(24b^2 + 36b - 16 + 27c)(12b^2 + 7b + 3c - 1)(-32c - 27b + 48b^2c + 27b^2 + 27c^2 + 72bc + 18)(32755bc + 12743c + 40596b^2c - 4846b - 2118 - 4664b^2)/27$; $\{-1 + b + 6b^2 + 12b^3\}$; $b \prec c$.
23. $-370x^2y - 10x^3 + 60x^2z + 4xy - 24zy + 74rzy + 2rzx + 37rz - 37y + 12r^3 - 24r = 2(37y + x - 6z)(2y - 5x^2 + rz)$; $\{r^2 - 2 + z^2, -rz + y + 4y^2\}$; $z \prec y \prec x$.
24. $7x^4 - 20a^2$ (irreducible); $\{761038687880048862537750000a - 10842909266386108209323717470464a^4 - 325577720150105105056746125600a^3 - 174868672571180176972218224444160a^5 + 604045455339075650979215375 0a^2 - 1873917969609345968295082668021120a^6 - 1477732045457732857484737621838 4384a^7 - 4386291583209472370608922382226 63680a^9 - 55949382070401401986219158050467 02080a^{11} + 137454646239245673597656 25 - 173058379284209289065392566142775 5008a^{10} - 901872299778088222240710696041 01120a^8 - 686828900324480166783877705214459 90400a^{15} + 953995988786499790200359533884211 20000a^{17} + 548033463712323993600000000000000 00000a^{32} - 358879430087500960127882253073121 28000a^{16} - 553713931309456243598998887787108 76160a^{14} - 130528951592084110835712000000000 00000000a^{28} + 233305674551817928704000000000000 000000a^{31} - 379039147753503876710400000000000 00000000a^{29} + 559393438086807446512516202496000 000000a^{22} - 373212208770452264086142976000000 0000000a^{26} - 251320674909543873206707814400000 000000a^{24} - 371935283296778815465429401600000 000000a^{25} + 116159132279153381860419211100160 0000000a^{21} - 322165757969237516152366952085502 03392a^{13} - 148641449489028067654080326483840 20480a^{12} + 366165541639546056314932007691878 400000a^{18} + 754105941740753012036565070774272 000000a^{19} + 111501723482575650226641869733888 00000000a^{20} - 266189705331706922941808640000000 00000000a^{27} - 801954273356818654530266726400000 0000000a^{23} - 222604109534224554393600000000000 000000a^{30}\}$; $a \prec x$.

25. $-y^4 - y^2z^2 + y^2r^2 + z^2 - 2 - z + r^2z + r^2$ (irreducible); $\{-1 + z^3 - z^2 + r^2\}$; $z \prec y$.

26. $2yz^3 + t^3 + zty^2 - t^2 + 2t^5 - t^8$ (irreducible); $\{-z^5 + t^4\}$; $z \prec y$.

27. $-338574x^3 - 98119x^6 - 560253x^2 + 403637x^4 + 822750x + 78$ (irreducible); $\{98885a + 93335a^3 + 75167a^5 + 74791\}$; $a \prec x$.

28. $22884x^6 - 2397x^5 + 5896 + 116x^8$ (irreducible); $\{-455a - 449a^6 + 894a^4 - 89a^5 + 669a^2 + 203\}$; $a \prec x$.

29. $-1479x - 896x^7 + 256x^5 - 532x^9 + 948x^6 - 128x^3 + 87$ (irreducible); $\{-64 - 82a^5 - 50a^7 + 26a + 98a^4\}$; $a \prec x$.

30. $-16x^7 + 4x^5 + 125 - 70x^{10} + 14x^3 + 18x^6 + 42x^4$ (irreducible); $\{-56 + 10a^8 - a + 8a^4 + 10a^5 - 10a^3 - 6a^7\}$; $a \prec x$.

31. $7a^7x + 7a - 4a^8x + 3a^4x^9 + 7a^3x^8 - 4a^8x^7 + a^8x^5 + 8a^6x^6 + 7x^5 + a^5x^3 + 5$ (irreducible); $\{-9a^8 + 18a^6 + 4a^4 + 9a^{11} + 10a^2 + 19\}$; $a \prec x$.

32. $28446u^5x^4 - 64736u^5a^2 + 35836u^2 - 81532u^4x^4 + 91392u^4a^2 - 50592u - 3910au^7x^4 - 3910au^4x^4 + 42576u^3x^4 - 32256u^3a^2 + 17856 + 2760au^6x^4 + 2760au^3x^4 - 23800u^3a^2x^4 + 16800u^2a^2x^4 - 980u^7a^2x^4 - 1610u^8x^4 - 39100ux^4 + 27600x^4$ (irreducible); $\{34ua^3 - 24a^3 - 14u^2a^2 - 23u^3 - 23\}$; $a \prec x$;

33. $-7806763730576844a + 10532827396776207600ba - 70050816975335427 + 38797250054987952abx^2 - 116792447148711734 4abx^3 - 1535845309390585710b + 348131332847121516bx^2 + 161712096025873536bx^3$ (irreducible); $\{-41 - 33a^2, -76230 - 39237b^2a + 2706b^2\}$; $a \prec b \prec x$.

34. $20ux^2ab + 56ux^2a^2 - 144au^5 - 2ux^3 + 76ux^3a^2 - 25abu^3 + 79ux - 95uxa + 45ab + 1 + 74u^4x$ (irreducible); $\{600639u^2a^2 + 6256052ua - 53117u^2a + 2544232u^3 - 2553, -4172795267 - 8120187857u - 4985396964u^3b + 463782u^2b^2\}$; $a \prec b \prec x$.

35. $63689v - 18924u^5vx^2 + 49301u^7 - 19024v^3x^7 + 76684u^7v^6x^6 - 86539u^7v^7x^5 + 77548u^3vx^6 + 90071u^2 - 31994u^4v^4x^5 - 76084u^5v^5x^2 + 59049$ (irreducible); $\{-429u^2v^3 + 6707u^5v^6a^2 + 13209u^4v^3a + 4094u^6va^5 - 7756u^6v^2 + 1156u^3v^5a - 1062882\}$; $a \prec x$.

36. $-10751498505384714a^4x^4 - 121954295675520a^4x^5 - 2047559767793694a^2x^3 + 2192898039411618a^4x^3 - 687166614219393a^2x^2 - 214279510583061x + 229489329705867a^2x + 44287414504641 + 3900606029320896a^4x^6 - 3926714503412736ax^6 + 811575648930816ax^5 - 1665720647059392a^2x^6 + 344272117033152a^2x^5 - 475174228471488a^3x^6 + 98209287304128a^3x^5 = 18333a(747a^3 - 752 - 319a - 91a^2)(479x - 99)(32233728x + 6498503a - 2621223a^2 - 5616688a^3 + 2382611a^4 + 366619)(19495509a - 7863669a^2 - 16850064a^3 + 184354304x^2 + 7147833a^4 + 1099857)(-21443499a^4 + 50550192a^3 + 23591007a^2 - 58486527a + 18096128x^2 - 3299571)/180845223885144064$; $\{747a^3 - 752 - 679a^5 - 319a - 91a^2\}$; $a \prec x$.

37. $16172800a^4x^2 - 2553600a^4x^5 + 10282720a^3x^4 - 1787520a^3x^7 + 23566080a^2x^2 - 3720960a^2x^5 + 2085440a^4x^3 - 329280a^4x^6 + 6575520a^3x + 43411200a^2 - 6854400a^2x^3 + 30387840ax^2 - 4798080ax^5 + 63256320 - 9987840x^3 + 9775500x - 1543500x^4 + 3351600a^2x - 529200a^2x^4 = -64a^3(3x^3 - 19)(1226a - 816a^2 + 1715x^2 + 1088a^4)(1088a^3 - 816a + 245ax + 1330x^2 - 1224)/245$; $\{-48a^3 + 64a^5 - 210 - 72a^2\}$; $a \prec x$.

38. $2916u^3a^2x^3 - 648u^4a^2 - 34020u - 2205uax^2 + 4347x^5 - 966ux^2 + 567u^4ax^5 - 126u^5ax^2 - 504u^2ax^5 + 112au^3x^2 + 189a^2x^5 - 42ua^2x^2 = 3u(9u^2a^2x^3 - 105 - 2u^3a^2)(108 + 7ax^2)$; $\{-69 - 9u^4a + 3a^3u^3 + 8u^2a - 3a^2\}$; $a \prec x$.

39. $-1411699917684bx^4a - 391282832250bx^3a + 131077373175x^2 + 404325593325 + 215074138500a^2bx^5 + 1517297482224abx^5 - 973376428375abx^2 - 442220639544bx^5 - 130427610750bx + 54014191875a^2x^2 + 250908094800ax^6 - 1159429063650ax^3 + 1275035638725x^2a - 33201454500x^4a - 28897562250x^4a^2 + 51088117500a^2x^3 - 482225626800x^5a - 419714897400x^5a^2 + 218382971400a^2x^6 + 392099102679bx^4 - 149400956250bx^4a^2 + 469539398700a^2bx^2 + 13636112350x^3 + 139933050525x^4 - 91628301600x^6 + 71962276950x^5 = 25(183654a + 159847a^2 - 67068)(23x + 54b - 47ab)(3327387x - 8750773b + 3006675a^2x + 438012x^2 + 833175xa - 7907325a^2b - 2887650ab)(-2025a^2 + 1495bx^2 - 1863x^2 + 1518x^3 - 2241)/279841$; $\{75a^3 + 83a - 23, 19322609b^2 + 3810525a^2 + 4378050a + 9247081\}$; $a \prec b \prec x$.

40. $76508025792b - 199449169920c + 1032309269376x + 624894448320cx + 1544744157120abx^2 - 206024417280cb + 787935520944ba^2cx - 2093645256720a^2cx - 1363009550400ca^2bx^2 + 53847290880bcx^2 + 2280107898000ax - 2106965243592ca - 753862072320cx^2 + 343459073232a^2x - 1071112361088 - 78976026624bx + 2148915057120cax^2 - 1319509245600a^2cx^2 - 220449800160bcx + 843551154864acx + 671296226304a^2b + 940971264024ca^2 + 2155706729328cabx + 1766605725984abc = -1193424(-20398c - 51136a - 43146abx - 60021acx - 1504bcx - 117312abc + 38070ba^2cx + 36855a^2cx + 21056cx + 1457cb + 45120ca^2)(510x - 924c + 1716b - 660a + 66cb + 187ab)/17$; $\{46a^3 + 98a - 16, 94b^2 + 35a - 57, 3c^2b - 42c^2 - 30ca + 78cb + 34\}$; $a \prec b \prec c \prec x$.