Factoring Polynomials Over Algebraic Number Fields

P. J. WEINBERGER
Bell Laboratories
and
L. P. ROTHSCHILD
Columbia University

An algorithm for factoring polynomials in one variable with algebraic coefficients is presented. The algorithm is based on Hensel's lemma; it is intended to be usable.

Key Words and Phrases: polynomial factorization, Henselian algorithms
CR Categories: 5.24, 5.7

1. INTRODUCTION

A method for factoring polynomials whose coefficients are in an algebraic number field is presented. This method is a natural extension of the usual Henselian technique for factoring polynomials with integral coefficients. In addition to working in any number field, our algorithm has the advantage of factoring nonmonic polynomials without inordinately increasing the amount of work, essentially by allowing denominators in the coefficients of the polynomial and its factors.

We have not yet written a computer program to implement this algorithm, but we give enough information, including examples, to enable the assiduous reader to program his own version. He will need a lot of enthusiasm and the ability to handle polynomials in two variables with large integer coefficients or with coefficients taken modulo p. The examples given in Section 11 and the notes and comments given in Section 12 should be helpful. Knuth [2] contains most of the information that is necessary for coding this algorithm. Narkiewicz [4] is an excellent reference for algebraic number theory. All recent work on polynomial factoring owes a great debt to Zassenhaus [5], in which the Henselian technique for factorization was suggested, and to Berlekamp (see [1] and its bibliography).

2. NOTATION

We assume our number field K is given by specifying an irreducible monic polynomial with integral coefficients $F(T)$ such that $F(\alpha) = 0$; then $K = Q(\alpha)$, the field of polynomials in α with rational coefficients.

This research was supported in part by the National Science Foundation.
Authors' addresses: P.J. Weinberger, Bell Laboratories, Murray Hill, NJ 07974; L.P. Rothschild, Columbia University, New York, NY.

We extend the usual denotation of mod by taking it to be a binary operation defined as follows. If b is a polynomial in one or more indeterminates with rational coefficients whose denominators are relatively prime to an integer n, then $b \bmod n$ is b with coefficients taken mod n. Thus $\frac{2}{3}x + 5 \bmod 4 = -2x + 1 \bmod 4$. If b and c are polynomials in an indeterminate, with coefficients in a ring, and c is monic, then $b \bmod c$ is the remainder obtained from the division of b by c. We take mod to have the lowest precedence of all binary operators, so that $a + b \bmod c$ means $(a + b) \bmod c$. If its second argument is fixed, mod generally represents a ring homorphism; so we may reasonably take $a = b \bmod c$ to be the same as $a \bmod c = b \bmod c$. We extend the notation to allow mod to have as its righthand operand a list of operands defining $a \bmod (b, c)$ as $(a \bmod b) \bmod (c \bmod b)$. Thus $5xT + 7T + 4x \bmod (3, x + 2)$ is 1, because $5xT + 7T + 4x = 2xT + T + x \bmod 3$, and $2xT + T + x = 2T(x + 2) + (x + 2) + 1 = 1 \bmod x + 2$. Since $F(\alpha) = 0$, any polynomial, $h(\alpha)$, in α may be identified with $h(T) \bmod F(T)$.

Small Greek letters α, β, γ, δ, ϕ denote algebraic numbers. We use $f(x)$, $g(x)$, $h(x)$ to denote polynomials in the indeterminate x with coefficients in K. Hence these polynomials are elements of $Q[x, \alpha]$. Henceforth, a, b, c denote integers; m, n, d, D are positive integers; and B is a positive real number. Otherwise, we use standard mathematical notation, In particular, Z is the ring of integers, and Q, $\mathbf{R}$, $\mathbf{C}$ are the fields of rationals, reals, and complexes, respectively. Also, $(1/d)Z[\alpha] = \{$polynomials in α whose coefficients are of the form a/d, $a \in Z\}$.

3. ALGORITHM FOR Q[x]

In this section we give the standard algorithm for factoring polynomials in $Z[T]$, slightly generalized.

We are given a polynomial,

$$F(T) = \sum_{j=0}^{n} a_j T^j \in Q[T],$$

of degree n, so $a_n \neq 0$. For our purposes the polynomial is best rewritten in the form,

$$F(T) = a_n \sum_{j=0}^{n} b_j T^j / d,$$

where $b_0, \ldots, b_n, d \in Z$ and $b_n = d$. This reduces the problem of factoring $F(T)$ to the problem of factoring $G(T) = \sum_{j=0}^{n} b_j T^j / d$, a monic polynomial of degree n with coefficients in $(1/d)Z$, the set of rational numbers with denominators dividing d. Then (it is not hard to prove that) any monic factor in $Q[T]$ of $G(T)$ has all its coefficients in $(1/d)Z$. Therefore, to factor $G(T)$ it is sufficient to find the irreducible monic factors of $G(T)$ which are in $(1/d)Z[T]$; this is what the algorithm in this section does. Furthermore, if $F(T)$ has integral coefficients, then one can take $d = a_n$, and if $G = \prod_{i=1}^{r} G_i$ is a factorization of $G(T)$ into irreducible monic factors in $(1/d)Z[T]$, then there is a factorization $d = \prod_{j=1}^{r} d_i$ such that $d_i G_i(T) \in Z[T]$, so that $F(T) = \prod_{i=1}^{r} d_i G_i(T)$. The d_i can be determined by greatest-common-divisor calculations. This last operation, restoring the integrality of coefficients, generally does not work in number fields; so we do not say any more about it.

Here, then, is the algorithm. Let $F(T)$ be a monic polynomial of degree n with coefficients in $(1/d)Z$.

Step Q1. Use the Euclidean algorithm in $Q[T]$ to calculate $H(T) = \mathrm{GCD}(F(T), F'(T))$, which is a monic polynomial in $(1/d)Z(T)$. Then the new $F(T)$, obtained by dividing the original $F(T)$ by $H(T)$, has no multiple factors, while all the factors of $H(T)$ are also factors of the new $F(T)$. Hence, factoring $F(T)$ is sufficient to factor the original polynomial.

Step Q2. Find a prime number p such that p does not divide d and such that $F(T)$ mod p has no multiple factors. If the first condition is not met, $F(T)$ mod p is not defined.

Step Q3. Factor $F(T)$ into irreducible monic factors modulo p, using one of the algorithms in [1], obtaining $F(T) = \prod_{i=1}^{s} F_i^{(1)}(T) \bmod p$. Define $H_j(T) = \prod_{i=1,\ i\neq j}^{s} F_i^{(1)}(T) \bmod p$, and find polynomials $U_j(T)$ of minimal degree such that

$$\sum_{j=1}^{s} U_j(T)H_j(T) = 1 \bmod p.$$

The $U_j(T)$ can be calculated using the Euclidean algorithm.

Step Q4. For each j, $1 \leq j \leq M$, calculate monic polynomials $F_i^{(j)}(T)$, $1 \leq i \leq s$, such that

$$F_i^{(j)}(T) = F_i^{(j-1)}(T) \bmod p^{j-1} \quad \text{and} \quad F(T) = \prod_{i=1}^{s} F_i^{(j)}(T) \bmod p^j$$

as follows. Let

$$A_j(T) = (F(T) - \prod_{i=1}^{s} F_i^{(j-1)}(T))/p^{j-1}$$

and

$$F_i^{(j)}(T) = F_i^{(j-1)}(T) + p^{j-1}(U_i(T)A_j(T) \bmod (P, F_i^{(1)}(T))).$$

M is a constant, depending on $F(T)$, whose calculation is described in Section 8.

Step Q5. Form all possible products of the $F_i^{(M)}(T)$, each taken at most once. Each of these products is an entire residue class modulo p^M of polynomials in $(1/d)Z[T]$. From this residue class choose that monic polynomial each of whose coefficients has the smallest possible absolute value. Among the polynomials so obtained are all of the factors of $F(T)$.

If $H(T) = T^m + \sum_{i=0}^{m-1} b_i T^i$ is a monic factor of $F(T)$ taken modulo p^m, then the representative in $(1/d)Z[T]$ chosen above is $T^m + \sum_{i=0}^{m-1} c_i T^i/d$, where c_i is the integer of smallest absolute value satisfying $c_i = b_i d \bmod p^M$. Therefore M has to be chosen so large that any coefficient c_i/d of any factor of $F(T)$ satisfies $c_i < p^M/2$. The general construction in Section 8 will determine such an M, even in this special case.

Readers familiar with polynomial factorization will have noticed that we have not exploited the quadratic convergence which is possible in step Q4. That is, by a modification of step Q4 it is possible to go directly from a factorization of $F(T)$ mod p^j to a factorization mod p^{2j}. This complicates the notation, the description of the algorithm, and thus the program, but it would result in decreasing the running time by a factor which is asymptotically some constant greater than 1. There are other modifications which could be made in the algorithm which would speed it up, but we shall not discuss them.

The mathematically sophisticated reader should note that the algorithm is a special case of the following general factorization procedure. Let $f(x) \in L[x]$ be a polynomial with coefficients in some ring L. We try to factor $f(x)$ by performing the

following steps, each of which implicitly places conditions on L and on the form of $f(x)$.

Step H1. Make $f(x)$ square free.

Step H2. Embed L in a ring L' so that Hensel's lemma is true in $L'[x]$.

Step H3. Find a suitable approximate factorization of $f(x)$ in $L'[x]$.

Step H4. Factor $f(x)$ in $L'[x]$ using the constructive procedure from the proof of Hensel's lemma. Normally this is an infinite process, so stop with a sufficiently good approximation.

Step H5. From this factorization, reconstruct the factorization of $f(x)$ in $L[x]$.

In the algorithm steps Q1–Q5, L' was the ring of p-adic numbers, the approximate factorization of step H3 was factorization mod p, and the approximate factorization of step H4 was factorization mod p^M.

The algorithm of this paper is essentially another instance of algorithm H, in which L' is the direct sum of certain local fields, namely, $L' = K \otimes Q_p$.

4. STATEMENT OF THE PROBLEM

Let $F(T) \in Z[T]$ be an irreducible monic polynomial of degree n, and suppose $F(\alpha) = 0$. Then $Q(\alpha) = \{\sum_{j=0}^{n-1} r_j\alpha^j : r_j \in Q\}$ is an algebraic number field of degree n. In Section 6 we explain how to perform the four rational arithmetic operations in $Q(\alpha)$. Write $K = Q(\alpha)$. Then $K[x]$ is a unique factorization domain, and we ask for an algorithm to perform the factorization. Two examples follow.

Let $F(T) = T^2 + 1$, $f(x) = x^4 + 1$. Then $\alpha^2 + 1 = 0$ and $K = Q(\alpha)$ is the field of Gaussian numbers. Now $f(x)$ is irreducible in $Q[x]$ but reducible in $K[x]$, and $f(x) = (x^2 + \alpha)(x^2 - \alpha)$ is its factorization into an irreducible factor in $K[x]$.

Let $F(T) = T^6 + 3T^5 + 5T^4 + T^3 - 3T^2 + 12T + 16$, and let $f(x) = x^3 - 3$. Then $f(x)$ is irreducible in $Q[x]$, but

$$\begin{aligned} f(x) = {} & (x - (\tfrac{4}{3} + \tfrac{11}{12}\alpha - \tfrac{7}{12}\alpha^2 + \tfrac{1}{6}\alpha^3 + \tfrac{1}{12}\alpha^4 + \tfrac{1}{12}\alpha^5)) \\ & \cdot (x - (1 - \tfrac{1}{4}\alpha + \tfrac{5}{12}\alpha^2 + \tfrac{1}{2}\alpha^3 + \tfrac{1}{4}\alpha^4 + \tfrac{1}{12}\alpha^5)) \\ & \cdot (x - (-\tfrac{7}{3} - \tfrac{2}{3}\alpha + \tfrac{1}{6}\alpha^2 - \tfrac{2}{3}\alpha^3 - \tfrac{1}{3}\alpha^4 - \tfrac{1}{6}\alpha^5)) \end{aligned} \tag{4.1}$$

in $K[x]$. (This example is worked out in Section 11.)

Parenthetically we observe that this factorization shows that $K = Q(\alpha)$ is a field of degree 6 which contains the three cube roots of 3; so $K = Q(3^{1/3}, 3^{1/3}e^{2\pi i/3}, 3^{1/3}e^{4\pi i/3})$.

The next example illustrates a fundamental limitation to any algorithm for factoring in $K[x]$. To explain the difficulty, we must introduce the notion of an algebraic integer. The number β is an algebraic integer if it is a root of a monic irreducible polynomial in $Z[x]$. The set R of algebraic integers in K is a ring, that is, it is closed under addition, multiplication, and subtraction. The ring of algebraic integers of Q is exactly Z, the ring of ordinary integers, if n is a square-free integer, then the ring of algebraic integers in $Q(\sqrt{n})$ is $Z[\sqrt{n}]$ if $n \not\equiv 1 \pmod 4$, and $Z[(1 + \sqrt{n})/2]$ if $n \equiv 1 \pmod 4$. Now if $f(x) \in Z[x]$ is factored into its irreducible factors in $Z[x]$, the factorization is also a complete factorization in $Q[x]$. However, if R is not a principal ideal domain, which is frequently true when $K \neq Q$, then there may be polynomials which are irreducible in $R[x]$ but reducible in $K[x]$.

Here is an example. Let $F(T) = T^2 + 5$, and let $f(x) = 2x^2 + 2x + 3$. Then $K = Q(\sqrt{-5})$, $R = Z[\sqrt{-5}]$, $f(x)$ does not factor into linear factors with coefficients from R, but with $\alpha = \sqrt{-5}$, $f(x) = \frac{1}{2}(2x + 1 + \alpha)(2x + 1 - \alpha)$ is a factorization in $K[x]$.

Another way of describing this difficulty is to say that new denominators cannot occur when factoring in $Q[x]$, but can occur when factoring in $K[x]$.

5. ALGORITHM SUMMARIZED

We are given a number field $K = Q(\alpha)$ of degree n, where α is a root of an irreducible monic polynomial $F(T) \in Z(T)$. The algorithm presented in this section will factor a monic polynomial in $K[x]$ into monic irreducible factors in $K[x]$. Requiring that the polynomial to be factored be monic is no restriction, for if $f(x) \in K[x]$ is not monic, then $(1/\phi_m)f(x)$ is monic, where $\phi_m \in K$ is the leading coefficient of $f(x)$.

We fix the following notation: $f(x) = \sum_{j=0}^{m} \phi_j x^j$, $\phi_m = 1$, where each $\phi_j \in (1/d)Z[\alpha]$. That is, each ϕ_j is written in the form

$$\phi_j = (1/d) \sum_{i=0}^{n-1} a_{ij}\alpha^i, \quad d, \alpha_{ij} \in Z. \tag{5.1}$$

It is easy to put any monic polynomial in $K[x]$ in this form by using the description of the arithmetic operations for K given in Section 6 and by choosing d as described in Section 7. All polynomials in the algorithm are to be monic.

Step K1. Let $h(x) = \mathrm{GCD}(f(x), f'(x))$ and replace $f(x)$ by $f(x)/h(x)$. Then the new $f(x)$ is square free and each factor of $h(x)$ is also a factor of the new $f(x)$, so that a factorization of the new $f(x)$ easily yields a factorization of the old $f(x)$.

Step K2a. Find a prime number p not dividing d such that $F(T)$ is square free modulo p.

Step K2b. Factor $F(T)$ modulo p, obtaining

$$F(T) \equiv \prod_{k=1}^{g} F_k^{(1)}(T) \bmod p, \quad \deg(F_k^{(1)}(T)) = n_k, \quad \sum_{k=1}^{g} n_k = n.$$

Step K3a. For each k, $1 \le k \le g$, factor $f(x)$ in the finite field with p^{n_k} elements using, for instance, an algorithm of [1], obtaining

$$f(x) = \prod_{l} f_{lk}^{(1)}(x) \bmod (p, F_k^{(1)}(\alpha)).$$

Here $\alpha \bmod (p, F_k^{(1)}(\alpha))$ generates the finite field (see Section 9). If, for some k, $f(x) \bmod (p, F_k^{(1)}(\alpha))$ is not square free, then choose a new p and return to step K2a.

Step K3b. Define

$$h_{jk}(x) = \prod_{l \neq j} f_{lk}^{(z)}(x) \bmod (p, F_k^{(1)}(\alpha))$$

and find polynomials $u_{jk}(x, \alpha) = u_{jk}(x)$ of minimal degree such that

$$\sum_{j} u_{jk}(x) h_{jk}(x) = 1 \bmod (p, F_k^{(1)}(\alpha)).$$

The u_{jk} can be found by using the Euclidean algorithm.

Step K4a. Using the procedure of step Q4, determine a factorization

$$F(T) = \prod_{k=1}^{g} F_k^{(M)}(T) \bmod p^M,$$

where

$$F_k^{(M)}(T) = F_k^{(1)}(T) \bmod p$$

and every $F_k^{(M)}(T)$ is monic. Here M is the constant determined in Section 8.

Step K4b. For each k, $1 \leq k \leq g$, and for each j, $2 \leq j \leq M$, calculate monic polynomials $f_{lk}^{(j)}(x)$, such that $f(x) = \prod_l f_{lk}^{(j)}(x) \bmod (p^j, F_k^{(M)}(\alpha))$. $f_{lk}^{(j)}(x) = f_{lk}^{(j-1)}(x) \bmod p^{j-1}$, as follows. Let $a_k^{(j)}(x) = (f(x) - \prod_l f_{lk}^{(j-1)}(x))/p^{j-1}$; then

$$f_{lk}^{(j)}(x) = f_{lk}^{(j-1)}(x) + p^{j-1}(u_{jk}(x)a_k^{(j)}(x) \bmod (p, F_k^{(1)}(\alpha), f_{lk}^{(1)}(x))).$$

Step K5. At this point we have g factorizations,

$$f(x) = \prod_l f_{lk}^{(M)}(x) \bmod (p^M, F_k^{(M)}(\alpha)), \quad 1 \leq k \leq g. \tag{5.2}$$

If $f(x) = h(x)g(x)$ is a factorization of $f(x)$, then clearly for each k,

$$f(x) = h_k(x)g_k(x) \bmod (p^M, F_k^{(M)}(\alpha)), \tag{5.3}$$

where $h_k(x)$ and $g_k(x)$ are polynomials whose degrees in x are $\deg(h(x))$, $\deg(g(x))$, respectively, and whose degrees in α are no greater than $\deg(F_k^{(M)})$, and which satisfy

$$h(x) = h_k(x), \quad g(x) = g_k(x) \bmod (p^M, F_k^{(M)}(\alpha)).$$

Therefore, we can generate all possible factorizations of $f(x)$ as follows. From (5.2) find all monic factorizations (5.3) that satisfy the consistency condition

$$h_1(x) = h_k(x), \quad g_1(x) = g_k(x) \bmod p^M, \ 1 \leq k \leq g. \tag{5.4}$$

Then use the Chinese remainder theorem (see Section 10) to determine monic $h(x)$, $g(x)$, with coefficients in $(1/d)Z[\alpha]$, such that

$$\begin{aligned} f(x) &= h(x)g(x) \bmod p^M, \\ \deg(h(x)) &= \deg(h_1(x)), \\ \deg(g(x)) &= \deg(g_1(x)). \end{aligned} \tag{5.5}$$

Since $h(x)$, $g(x)$ are determined only modulo p^M, choose for each of them that polynomial whose coefficients, when written in the form (5.1), have a_{ij} of minimal absolute value. If M, d have been chosen correctly, than a factor of $f(x)$ which equals $(h(x) \bmod p^M)$ must actually be $h(x)$. Therefore, the factorizations (5.3) generate all the factors of $f(x)$.

The trial divisions in this step should be done constant term first, as most will fail.

The reasons given in Section 3 for not using quadratic convergence in the description of step 4 are even more cogent here.

6. ARITHMETIC IN NUMBER FIELDS

In this section we present the fundamental procedures for arithmetic in $K = Q(\alpha)$, where α is a zero of the irreducible monic polynomial $F(T) \in Z(T)$, with $\deg(F(T)) = n$.

The elements of K are all of the form

$$\beta = \sum_{j=0}^{n-1} r_j \alpha^j, \qquad r_j \in Q.$$

Combining the r_j using a common denominator, d, allows us to write

$$\beta = \sum_{j=0}^{n-1} b_j \alpha^j / d, \qquad b_j \in Z.$$

Since $F(\alpha) = 0$, $T \bmod F(T)$ satisfies the same polynomials that α does. This observation determines the arithmetic of K.

Thus if $\gamma = \sum c_j \alpha^j / d$, then $\beta \pm \gamma = \sum (b_j \pm c_j)\alpha^j / d$. One calculates $\beta\gamma$ by reducing $(\sum b_j T^j)(\sum c_j T^j)$ modulo $F(T)$, to obtain $\sum e_j T^j$. Then $\beta\gamma = \sum e_j \alpha^j / d^2$. This is consistent with the notational conventions given in Section 2. Notice that the denominator can increase. Our prescription for choosing d in Section 7 will ensure that the same denominator can be used throughout algorithm K. One important case where the denominator does not increase is the case where β, γ are algebraic integers. In this case, each e_j must be divisible by d.

To find $1/\gamma$, use the Euclidean algorithm to find polynomials with rational coefficients e_j, e_j^1 satisfying

$$\left(\sum c_j T^j / d\right)\left(\sum_{j=0}^{n-1} e_j T^j\right) + F(T) \sum_{j=0}^{n-1} e_j^1 T^j = 1.$$

Then $(\sum c_j \alpha^j / d)(\sum e_j \alpha^j) = 1$, since $F(\alpha) = 0$, so $1/\gamma = \sum e_j \alpha^j$.

7. ALGEBRAIC INTEGERS AND CHOOSING A DENOMINATOR

The ring of integers R in a number field K is the collection of all $\beta \in k$ such that $G(\beta) = 0$, where $G(T)$ is some monic polynomial in $Z(T)$. In some cases it may be possible to find an $\alpha \in R$ such that $R = Z[\alpha]$. Frequently this is not the case, and then the exact determination of the members of R is more difficult. In either case, for any $\beta \in R$ such that $K = \mathbf{Q}(\beta)$, define defect $(\beta) = \min\{d > 0 : R \subset (1/d)Z[\beta]\}$. Clearly, defect $(\beta) = 1$ exactly when $R = Z[\beta]$. Note that defect $(\beta + j) = $ defect (β) for all $j \in Z$.

There are two kinds of frequently occurring fields for which $R = Z[\alpha]$. The first is the quadratic fields, $K = \mathbf{Q}(\sqrt{n})$, where n is a square free integer. In this case we may take $\alpha = \sqrt{n}$ if $n = 2, 3 \bmod 4$; so $F(T) = T^2 - n$, and $\alpha = (1 + \sqrt{n})/2$ if $n = 1 \bmod 4$ with $F(T) = T^2 - T + (1 - n)/4$. The second case is the cyclotomic fields. Here $K = Q(\alpha)$ with $\alpha = e^{2\pi i/n}$, a primitive nth root of 1. In this case $F(T)$ is the nth cyclotomic polynomial,

$$F(T) = \prod_{d \mid n} (x^{n/d} - 1)^{\mu(d)},$$

where $\mu(d)$ is the Möbius μ-function,

$$\mu(d) = 0 \qquad \text{if } d \text{ is not square free,}$$

$$\mu(p_1 \ldots p_s) = (-1)^s \quad \text{otherwise.}$$

There is no known algorithm for finding $\beta \in R$ with defect (β) minimal, but it is possible to calculate defect (α) for any $\alpha \in R$ given as a zero of an irreducible monic polynomial $F(T) \in Z[T]$, with $K = Q(\alpha)$. The algorithm is involved, and its running time has not been analyzed. The following weak bound is sufficient. Let disc $(F(T))$ be the discriminant of $F(T)$ (which can be easily calculated) and let D be the largest positive integer such that D^2 divides disc $(F(T))$. (D may be harder to find.) Then defect (α) divides D, so that $(1/D)Z[\alpha] \supset R$.

We need the following lemmas.

GAUSS'S LEMMA. *Let* $h(x) = \sum_{j=0}^{p} \phi_j x^j$, $g(x) = \sum_{j=0}^{q} \gamma_j x^j$ *be in* $R[x]$, *with* ϕ_p, $\gamma_q \neq 0$. *Suppose that every coefficient of* $h(x)g(x)$ *is divisible by* δ, *where* $\delta \in R$. *Then each product* $\phi_i\gamma_j$ $(0 \leq i \leq p,\ 0 \leq j \leq q)$ *is divisible by* δ.

An algebraic integer β is said to be divisible by δ if $\beta/\delta \in R$.

LEMMA 7.1. *Let* $f(x) \in (1/a)R[x]$ *be monic, and suppose* $f(x) = g(x)h(x) \in K[x]$, *where* $g(x)$, $h(x)$ *are monic. Then* $g(x)$, $h(x) \in (1/a)R[x]$.

PROOF. Let $g(x), h(x) \in (1/b)R[x]$. Then $b^2 f(x) = bg(x)bh(x)$, and if we write

$$g(x) = \sum_{j=0}^{q} \gamma_j x^j, \qquad h(x) = \sum_{j=0}^{p} \phi_j x^j,$$

Gauss's lemma implies that

$$(b^2/a) \mid b\gamma_i b\phi_j \quad \text{for all} \quad i, j.$$

This, in turn, is equivalent to the assertion that $a\gamma_i\phi_j \in R$ for all i, j. Since $\gamma_q = \phi_p = 1$, it follows that $a\gamma_i$, $a\phi_j \in R$ for all i, j. Q.E.D.

This lemma enables us to choose a satisfactory denominator for the representation of the coefficients of $f(x)$.

Suppose that the coefficients of $f(x)$ are in $(1/b)Z[\alpha]$. Clearly $f(x) \in (1/b)R[x]$. Hence, by Lemma 7.1, the monic factors of $f(x)$ will also be in $(1/b)R[x]$ and will have coefficients in $(b \cdot \text{defect } (\alpha))^{-1}Z[\alpha]$; so the factors of $f(x)$ will have their coefficients in $(bD)^{-1}Z[\alpha]$, where D is any positive integer divisible by defect (α).

For instance, $\alpha = \sqrt{-15}$, index$(\alpha) = 2$; so $f(x) = x^2 + x/2 + 1 = (x + (1 + \sqrt{-15})/4)(x + (1 - \sqrt{-15})/4)$.

It is occasionally useful to note that if $f(x)$ is in $(1/b)R[x]$, this argument works with $(1/b)Z[\alpha]$ replaced by $(1/b)R$. For instance, in some cases one might know that $b = 1$, although the coefficients of $f(x)$ are not in $Z[\alpha]$.

8. COEFFICIENT BOUND FOR FACTORS

We have a monic irreducible polynomial $F(T) \in Z[T]$ of degree n, with $F(\alpha) = 0$. We also have a monic polynomial, $f(x)$, of degree m, whose coefficients are all in $(1/d)Z[\alpha]$, where d is chosen (Section 7) so that any monic factor of $f(x)$ must also have its coefficients in $(1/d)Z[\alpha]$. Let $\sum_{j=0}^{n-1} c_j\alpha^j/d$, $c_j \in Z$ be a coefficient of such a factor. In this section we show how to calculate a bound B such that $|c_j| < B$ for

any c_j in any coefficient of any factor of $f(x)$. Our bound is certainly not the best possible, and the reader could easily improve on it in any particular case by calculating numbers which are estimated in the proofs that follow.

For an algebraic number β let $\| \beta \|$ denote the largest absolute value of any of the conjugates of β. A conjugate of β is a root of the minimal polynomial of β over Q. If $g(x) = \sum_{j=0}^{q} \gamma_j x^j \in K[x]$, define $\| g(x) \| = \max \{ \| \gamma_j \| : 0 \leq j \leq q \}$. If $F(T) = \sum_{j=0}^{n} a_j T^j$, then it is clear that $\| \alpha \|$ is no greater than the positive root of

$$T^n - | a_{n-1} | T^{n-1} - \cdots - | a_0 | = 0,$$

which, in turn, is no larger than $\sum_{j=0}^{n-1} | a_j |$. This gives two upper bounds for $\| \alpha \|$, while $\| \alpha \|$ itself can be calculated to any desired accuracy by finding the roots of $F(T) = 0$.

Now let $g(x)$ be as given, with the additional assumptions that $\gamma_q = 1$ and that $g(x)$ is a factor of $h(x)$. If δ is any zero of $g(x)$, then δ is also a zero of $f(x)$, and it is clear that $\max \{ \| \delta \| : f(\delta) = 0 \}$ can be calculated to any desired accuracy. For our purposes, an upper bound is sufficient. We note the following trivial facts:

$$\| \beta + \gamma \| \leq \| \beta \| + \| \gamma \|; \qquad \| \beta\gamma \| \leq \| \beta \| \, \| \gamma \|. \tag{8.1}$$

Suppose $f(x) = \sum_{j=0}^{m} \beta_j x^j$ with $\beta_m = 1$. Clearly, if $f(\delta) = 0$, then $\| \delta \|$ is no greater than the positive root of $x^m - \sum_{j=0}^{m-1} B_j^{\,1} x^j = 0$, where $B_j^{\,1} \geq \| \beta_j \|$ for all j. Finally, if

$$\beta = \sum_{j=0}^{n-1} c_j \alpha^j / d, \qquad c_j \in Z, \tag{8.2}$$

then $\| \beta \| \leq \sum_{j=0}^{n-1} | c_j | \, \| \alpha \|^j / d$. These observations prove the following lemma.

LEMMA 8.1. *There is an effectively computable bound B_1 depending only on $F(T)$ and $f(x)$, such that $f(\delta) = 0$ implies $\| \delta \| < B_1$.*

LEMMA 8.2. *Let $g(x)$ be a monic polynomial of degree q which divides $f(x)$. Let B_1 be any real number such that $f(\delta) = 0$ implies $\| \delta \| < B_1$. Then the coefficient γ_j of x^j in $g(x)$ must satisfy $\| \gamma_j \| \leq B_2 = \binom{q}{j} B_1^{\,j}$.*

PROOF. The truth of the lemma is a consequence of eq. (8.1) repeatedly applied to the expression $g(x) = \prod (x - \delta)$, where the product is taken over j zeros, δ, of $f(x)$. Q.E.D.

LEMMA 8.3. *If β is written in the form (8.2) and $\| \beta \| < B_2$, then there is an effectively computable constant B_3, depending only on $F(T)$, such that $| c_j | < dB_2B_3$.*

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be the conjugates of α. If $\gamma = \sum_{j=0}^{n-1} r_j \alpha^j$, $r_j \in \mathbf{C}$, let $\gamma_i = \sum_{j=0}^{n-1} r_j \alpha_i^{\,j}$. The map $L : \mathbf{C}^n \to \mathbf{C}^n$, defined by $(r_0, \ldots, r_{n-1}) \to (\gamma_1, \ldots, \gamma_n)$, is an invertible linear map. It is invertible because it is a Vandermonde matrix formed from $\alpha_1, \ldots, \alpha_n$. Hence the determinant of L is $| \operatorname{disc} (F(T)) |^{1/2}$. Write $| \gamma |_\infty = \max \{ | \gamma_i | \}$, $| r |_\infty = \max \{ | r_i | \}$, where $\gamma = (\gamma_1, \ldots, \gamma_n)$, $r = (r_0, \ldots, r_{n-1})$. Clearly, if all the $r_i \in Q$, then $\gamma \in K$ and $| \gamma |_\infty = \| \gamma \|$. Now the action of L is multiplication by a matrix, which we shall also call L; so $rL = \gamma$. Hence $r = \gamma L^{-1}$ and $| r |_\infty \leq | \gamma |_\infty \, | L^{-1} |_\infty$, where, if M is a matrix (m_{ij}),

$$| M |_\infty = \max \{ \sum_{i=1}^{n} m_{ij} : 1 \leq j \leq n \}.$$

Clearly L^{-1} can be calculated arbitrarily accurately; so if we write $r_j = c_j/d$, then $| c_j | < dB_2 \, | L^{-1} |_\infty$, which proves the theorem.

It is convenient to have an easily calculated upper bound for $|L^{-1}|_\infty$. From the expression for L^{-1} in terms of cofactors of L, it is clear that each entry in L^{-1} is bounded by $(n-1)!\,\|\alpha\|^{n(n-1)/2}/|\det(L)|$ so that $B_3 = |L^{-1}|_\infty \le n!\,\|\alpha\|^{n(n-1)/2}/|\operatorname{disc}(F(T))|^{1/2}$. Q.E.D.

Lemmas 8.2 and 8.3 show immediately that factorization in $K[x]$ is effective.

The bound for $|L^{-1}|_\infty$ just given is fairly crude, but very easily calculated.

If one uses the integral bases for quadratic fields given in Section 7, then $|L^{-1}|_\infty = 1$.

To find M for algorithm K, let $B = dB_2B_3$ and choose $M \ge (\log 2B)/\log p$.

9. CALCULATIONS IN FINITE FIELDS

In this section we provide some further explication of the finite fields used in algorithm K. Let p be a prime dividing neither $\operatorname{disc}(F(T))$ nor d. Recall that d is the denominator chosen in Section 7 to represent the coefficients of $f(x)$ in the form (5.1).

As in step K2, for such a prime p, factor $F(T)$ modulo p to obtain

$$F(T) = \prod_{i=1}^{g} F_k(T) \bmod p, \quad \deg(F_k(T)) = n_k, \quad \sum_{k=1}^{g} n_k = n.$$

The rational integers taken modulo p form a finite field $\mathbf{F}_p$ with p elements. With the algebraic integers of K, and with $(1/d)Z[\alpha]$, are associated g extensions of this field. In this section we denote these by $\mathbf{F}_p(\alpha; k)$, $1 \le k \le g$. This is not standard notation. $\mathbf{F}_p(\alpha; k)$ is the field with p^{n_k} elements, with its elements represented by polynomials in α taken modulo p and $F_k(\alpha)$. That is,

$$\mathbf{F}_p(\alpha; k) = \left\{ \sum_{j=0}^{n_k-1} b_j\alpha^j : 0 \le b_j < p \right\},$$

with addition and multiplication done as follows. For addition,

$$\sum b_j\alpha^j + \sum c_j\alpha^j = \sum d_j\alpha^j \bmod (p, F_k(\alpha)),$$

so

$$d_j = b_j + c_j \bmod p.$$

For multiplication,

$$\left(\sum b_j\alpha^j\right)\left(\sum c_j\alpha^j\right) = \sum_{j=0}^{n_k-1} d_j\alpha^j \bmod (p, F_k(\alpha)).$$

Here are some examples. Let $F(T) = T^3 - 2$, $d = 1$, $p = 5$; so that $F(T) = F_1(T)F_2(T) \bmod 5$, with $F_1(T) = T - 3$, $F_2(T) = T^2 + 3T - 1$. Then $\mathbf{F}_p(\alpha; 1) = \mathbf{F}_p$, while $\mathbf{F}_p(\alpha; 2) = \{b_0 + b_1\alpha : 0 \le b_0, b_1 < 5\}$. $\mathbf{F}_p(\alpha; 2)$ has $25 = 5^2$ elements and the reader should check that $\alpha^2 = 2\alpha + 1$, $\alpha^3 = 2$ (not surprisingly), $\alpha^4 = 2\alpha$, $\alpha^5 = 4\alpha + 2$, etc.

For the second example, let $F(T) = T^4 + 1$, $d = 1$, $p = 5$. Then $F(T) = F_1(T)F_2(T) \bmod 5$, with $F_1(T) = T^2 + 2$, $F_2(T) = T^2 + 3$. Here $\mathbf{F}_p(\alpha; 1)$ and $\mathbf{F}_p(\alpha; 2)$ are isomorphic as abstract fields, both having 25 elements, but it is necessary for our purposes to distinguish them. For instance, in $\mathbf{F}_p(\alpha; 1)$, $(\alpha + 1)^2 = 2\alpha + 4$, while in $\mathbf{F}_p(\alpha; 2)$, $(\alpha + 1)^2 = 2\alpha + 3$.

Finally, consider $\beta = \sum_{j=0}^{n-1} b_j\alpha^j/d \in (1/d)Z[\alpha]$. To each such β there corresponds a unique element of $\mathbf{F}_p(\alpha; k)$ with the property that the correspondence is a ring homomorphism of $(1/d)Z[\alpha]$ onto $\mathbf{F}_p(\alpha; k)$ taking α to α. This element is obtained by first treating β as a polynomial in α with coefficients in $\mathbf{F}_p$, and then by taking the remainder after division by $F_k(\alpha)$. That is, β goes to $\beta \bmod (p, F_k(\alpha))$.

In the first example, take $d = 2$, $\beta = (1 + \alpha^2)/2$. Then, considered as a polynomial in $\mathbf{F}_5[\alpha]$, $\beta = 3\alpha^2 + 3$; so β corresponds to 0 in $\mathbf{F}_5(\alpha; 1)$ and to $1 + \alpha$ in $\mathbf{F}_5(\alpha; 2)$.

Using these notions, we can now carry out step K3a in Section 5, as in [1]. Steps K3b and K4 need no special explanation other than the examples given in Section 11.

10. CHINESE REMAINDER THEOREM

In this section we give some details on step K5. Suppose we have a factorization

$$F(T) = \prod_{k=1}^{g} F_k^{(M)}(T) \bmod p^M, \quad \deg(F_k^{(M)}) = n_k,$$

into pairwise prime monic factors, an integer d not divisible by p, and $\gamma_1, \ldots, \gamma_g$ with

$$\gamma_k = \sum_{j=0}^{n_k-1} c_{kj}\alpha^j, \quad c_{kj} \in Z, \ 1 \le k \le g.$$

The Chinese remainder theorem guarantees the existence of

$$\gamma = \frac{1}{d}\sum_{j=0}^{n-1} c_j\alpha^j, \quad c_j \in Z,$$

where the c_j are uniquely determined modulo p^M and

$$\gamma = \gamma_k \bmod (p^M, F_k^{(M)}(\alpha)), \quad 1 \le k \le g.$$

This enables one to go from eq. (5.3) to eq. (5.5), by letting γ_k run through the coefficients of h_k, g_k in eq. (5.3).

To find γ, first find monic polynomials $G_k(T) \in Z[T]$, preferably of least degree, satisfying

$$G_k(T) = 1 \bmod (p^M, F_k^{(M)}(T)); \quad G_k(T) = 0 \bmod (p^M, F_j^{(M)}(T)) \text{ if } j \ne k.$$

Note that these would give the same polynomials if T were replaced by α.

One way of doing this is to let $G_k(T) = (\prod_{j\ne k} F_j^{(M)}(T))\ H'_k(T) \bmod p^M$, where $H'_k(T)$ is chosen, using the Euclidean algorithm, so that $G_k(T) = 1 \bmod (p^M, F_k^{(M)}(T))$. Then we are done, because

$$\sum_{k=1}^{g} G_k(\alpha)\gamma_k = \gamma_k \bmod (p^M, F_k^{(M)}(\alpha)),$$

so the desired $\gamma = (1/d)\sum_{k=1}^{g} dG_k(\alpha)\gamma_k \bmod p^M$.

The details of step K5 are now fairly clear. For each of the factorizations (5.3), satisfying eq. (5.4), apply the aforementioned procedure to determine the factorization (5.5) and the corresponding trial factors $h(x)$, $g(x) \in ((1/d)\ Z[\alpha])[x]$. For

each pair of trial factors so obtained, divide one of them into $f(x)$. If it divides evenly, it is a true factor, and we continue to generate trial factors for the rest of $f(x)$. We suggest dividing constant term first, as this encourages trial division to fail before the remainder is found.

11. EXAMPLES

Example 1. $F(T) = T^2 + 1$, $f(x) = x^2 + \alpha x + 1$. Here defect $(\alpha) = 1$; so $f(x)$ will factor in $(Z[\alpha])[x]$ if it factors in $K[x]$; so $d = 1$. For a coefficient bound, $\| \alpha \| = 1$; so $f(\gamma) = 0$ implies $\| \gamma \| \leq x_0$, if $x_0 > 0$ satisfies $x_0^2 - x_0 - 1 = 0$; so $\| \gamma \| \leq 2$. Therefore, any coefficient β of any factor of $f(x)$ satisfies $\| \beta \| \leq 2$; so if $c_0 + c_1\alpha = \beta$, then $| c_i | \leq 2$, by Lemma 8.3. Hence we may determine M of step K4 by $p^M/2 > 2$; so $p^M > 4$. Step K1 has no effect since $\text{GCD}(f(x), f'(x)) = 1$. In step K2, $p = 2$ does not work since

$$\text{GCD}\,(F(T), F'(T)) = F(T) \not\equiv 1 \bmod 2.$$

However, $p = 3$ is satisfactory, since $F(T)$ mod 3 is irreducible. Hence $g = 1$ and $F_1^{(1)}(T) = T^2 + 1$. Having chosen p, we see that $M = 2$ suffices. Next we factor $f(x)$, as in step K3a, over the field $\mathbf{F}_3[\alpha]$, of 9 elements, obtaining

$$f(x) = (x + 2\alpha + 1)(x + 2\alpha + 2) \bmod (3, F(\alpha)),$$

so $f_{11}^{(1)}(x) = x + 2\alpha + 1$, $f_{21}^{(1)}(x) = x + 2\alpha + 2$. In step K3b we get $h_{11}(x) = x + 2\alpha + 2$, $h_{21}(x) = x + 2\alpha + 1$, $u_{11}(x) = 1$, $u_{21}(x) = 2$. In step K4, $F_1^{(2)}(T) = F(T) = T^2 + 1$. Then $a_1^{(2)}(x) = (f(x) - (x + 2\alpha + 1)(x + 2\alpha + 2))/3 = (-\alpha - 1)x - 2\alpha + 1$, $f_{11}^{(2)}(x) = (x + 2\alpha + 1) + 3(\alpha) = x + 5\alpha + 1$, $f_{21}^{(2)}(x) = (x + 2\alpha + 2) + 3(\alpha + 2) = x + 5\alpha + 8$; so $f(x) = (x + 5\alpha + 1)(x + 5\alpha + 8)$ mod 9. In step K5, we choose residue classes of least absolute value modulo 9, obtaining the trial factors $(x - 4\alpha + 1)$, $(x - 4\alpha - 1)$. Neither is actually a factor; so $f(x)$ is irreducible.

Notice that choosing p in step K2 so that $g = 1$ simplifies everything and makes step 5 much simpler. Unfortunately this is not always possible. For instance, if $F(T) = T^4 + 1$, then g is never 1.

Example 2. We derive the factorization (4.1). Here

$$F(T) = T^6 + 3T^5 + 6T^4 + T^3 - 3T^2 + 12T + 16, \quad f(x) = x^3 - 3.$$

For clarity we use 12 for the denominator d, because the estimate for defect (α) in Section 7 is too large. Next we calculate M. Clearly the B_1 of Lemma 8.1 is $3^{1/3}$. Since $f(x)$ must have a linear factor if it is reducible, the B_2 of Lemma 8.2 is also $3^{1/3}$. Using the first technique for estimating $\| \alpha \|$ gives $\| \alpha \| < 4.467$. Now $\text{disc}\,(F(T)) = -2^6 \cdot 3^{19}$; so the estimate for B_3 at the end of Lemma 8.3 gives $B_3 \leq 1.48 \times 10^7$; so $B \leq 8 \times 10^8$. Since 2 and 3 divide $\text{disc}\,(F(T))$, let $p = 5$. Then $M = 10$. If we compare this with the actual factorization (4.1), we see that $M = 3$ would have been enough; so we take $M = 3$. For step K2 we get

$$F(T) = (T^2 + 2T + 3)(T^2 + 3T + 3)(T^2 + 3T + 4) \bmod 5$$

$$= F_1^{(1)}(T) \quad F_2^{(1)}(T) \quad F_3^{(1)}(T) \quad \text{respectively.}$$

Then

$$H_1(T) = T^4 + T^3 + T^2 + T + 2 \mod 5,$$
$$H_2(T) = T^4 + 3T^2 + 2T + 2 \mod 5,$$
$$H_3(T) = T^4 + 2T^2 + 4 \mod 5,$$
$$U_1(T) = T + 4, \quad U_2(T) = 2T + 1, \quad U_3(T) = 2T + 4 \mod 5.$$

This gives $A_1(T) = 4T^5 + T^3 + 4T + 1$; so $F_1^{(2)}(T) = T^2 + 2T + 8$, $F_2^{(2)}(T) = T^2 + 13T + 8$, $F_3^{(2)}(T) = T^2 + 13T + 19$. This, in turn, gives $A_2(T) = 4T^5 + 2T^3 + 3T^2 + T + 2$, so that $F_1^{(3)}(T) = T^2 + 77T + 108$, $F_2^{(3)}(T) = T^2 + 88T + 108$, and $F_3^{(3)}(T) = T^2 + 88T + 119$. Step K3 gives

$f_{11}^{(1)}(x) = x + 3$, $f_{21}^{(1)}(x) = x + 4 + 3\alpha$, $f_{31}^{(1)}(x) = x + 3 + 2\alpha$,
$f_{12}^{(1)}(x) = x + 3 + 3\alpha$, $f_{22}^{(1)}(x) = x + 3$, $f_{32}^{(1)}(x) = x + 4 + 2\alpha$,
$f_{13}^{(1)}(x) = x + \alpha$, $f_{23}^{(1)}(x) = x + 2 + 4\alpha$, $f_{33}^{(1)}(x) = x + 3$,

$h_{11}(x) = x^2 + 2x + 4$, $h_{21}(x) = x^2 + (1 + 2\alpha)x + 4 + \alpha$, $h_{31}(x) = x^2 + (2 + 3\alpha)x + 2 + 4\alpha$,
$h_{12}(x) = x^2 + (2 + 2\alpha)z + 2 + \alpha$, $h_{22}(x) = x^2 + 2x + 4$, $h_{32}(x) = x^2 + (1 + 3\alpha)x + 4 + 4\alpha$,
$h_{13}(x) = x^2 + 4\alpha x + 1 + 2\alpha$, $h_{23}(x) = x^2 + (3 + \alpha)x + 3\alpha$, $h_{33}(x) = x^2 + 2x + 4$,

$U_{11}(x) = 3$, $U_{21}(x) = 4 + 3\alpha$, $U_{31}(x) = 3 + 2\alpha$,
$U_{12}(x) = 3 + 3\alpha$, $U_{22}(x) = 3$, $U_{32}(x) = 2\alpha + 4$,
$U_{13}(x) = \alpha$, $U_{23}(x) = 2 + 4\alpha$, $U_{33}(x) = 3$.

At the end of step K4 we have

$f_{11}^{(3)}(x) = x + 38$, $f_{21}^{(3)}(x) = x + 69 + 38\alpha$, $f_{31}^{(3)}(x) = x + 18 + 87\alpha$,
$f_{12}^{(3)}(x) = x + 108 + 108\alpha$, $f_{22}^{(3)}(x) = x + 38$, $f_{32}^{(3)}(x) = x + 104 + 17\alpha$,
$f_{13}^{(3)}(x) = x + 26\alpha$, $f_{23}^{(3)}(x) = x + 87 + 99\alpha$, $f_{33}^{(3)}(x) = x + 38$.

In step K5 we get

$F_2^{(3)}(T)F_3^{(3)}(T) = T^4 + 51T^3 + 96T^2 + 101T + 102$, $H'_1(T) = 26T + 44$,
$G_1(T) = 26T^5 + 120T^4 + 115T^3 + 100T^2 + 96T + 113$,
$F_1^{(3)}(T)F_3^{(3)}(T) = T^4 + 40T^3 + 3T^2 + 42T + 102$, $H_2'(T) = 57T + 16$,
$G_2(T) = 57T^5 + 46T^4 + 61T^3 + 67T^2 + 111T + 7$,
$F_1^{(3)}(T)F_2^{(3)}(T) = T^4 + 40T^3 + 117T^2 + 70T + 39$, $H'_3(T) = 42T + 29$,
$G_3(T) = 42T^5 + 84T^4 + 74T^3 + 83T^2 + 6$.

Then, looking for a factor $x + \gamma$, with $\gamma = \gamma_1 = 38 \bmod (5^3, F_1^{(3)}(\alpha))$, $\gamma = \gamma_2 = 108 + 108\alpha \bmod (5^3, F_2^{(3)}(\alpha))$, $\gamma = \gamma_3 = 26\alpha \bmod (5^3, F_3^{(3)}(\alpha))$, gives $\gamma = 82 + 72\alpha + 11\alpha^2 + 104\alpha^3 + 52\alpha^4 + 52\alpha^5 \bmod 5^3$. Since $d = 12$, the trial factor is

$$x - (-\tfrac{4}{3} + \tfrac{11}{12}\alpha - \tfrac{7}{12}\alpha^2 + \tfrac{1}{6}\alpha^3 + \tfrac{1}{12}\alpha^4 + \tfrac{1}{12}\alpha^5),$$

which turns out to actually be a factor.

12. NOTES AND COMMENTS

1. The bound for defect (α) given in Section 2 is frequently much too large, as happens in the second example given in Section 11. The calculation of defect(α) is related to finding an integral basis for R. (A short bibliography on this topic is given in [7]; also see [7, p. 24].) $\{w_0, \ldots, w_{n-1}\}$ is an integral basis of R if $\sum a_i w_i \in R$, $a_i \in Q$, exactly when all $a_i \in \mathbf{Z}$. It is possible to take $w_i = \phi_i(\alpha)/D_i$, $0 \leq i < m$, where $D_0 = 1$, $D_i \mid D_{i+1}$, and each $\phi_i(\alpha)$ is a monic polynomial of degree i in $\mathbf{Z}[\alpha]$. Then defect$(\alpha) = D_{n-1}$. A particularly nasty example is $F(T) = T^9 - 54$, disc$(F(T)) = 3^{42} \cdot 2^8$, so the D given in Section 2 is $D = 3^{21} \cdot 2^4$. However, $\{1, \alpha, \alpha^2, \alpha^3/3, \alpha^4/3, \alpha^5/3, \alpha^6/9, \alpha^7/9, \alpha^8/9\}$ is an integral basis, so defect $(\alpha) = 3^2$.

2. Because the "average" polynomial is irreducible, the algorithm should be able to tell as soon as possible if $f(x)$ is irreducible. Some information is available at the end of step K3a, and more is available if, in a search for a convenient p, step K3a has been done for more than one p. The test is a simple generalization of the observation that a polynomial is irreducible if it is irreducible modulo some prime. Let $N(j, k)$ be the number of factors of $f(x)$ of degree $j \bmod (p, F_k^{(1)}(\alpha))$, $1 \leq k \leq g$. Let $N(j)$ be the number of trial factors (as in step K5) of $f(x)$ of degree j. Then

$$N(j) = \prod_{i=1}^{g} \sum_{S} \prod_{k=1}^{j} \binom{N(k, i)}{b(k)}$$

where S is the set of solutions of $\sum_{k=1}^{j} k \cdot b(k) = j$, $b(k) \geq 0$. This formula is easier to calculate than to contemplate, and if $N(j) = 0$ for all j, $1 \leq j \leq \deg(f(x))/2$, then $f(x)$ must be irreducible. With several p, $f(x)$ is surely irreducible if for each j there is a p with $N(j) = 0$. The numbers $N(j)$ are worth calculating because they reveal how much work step K5 can be, since $N(j)$ is the number of trial divisors of degree j.

3. The trial divisions in step K5 may be speeded up by dividing constant term first. The usual division algorithm always proceeds to completion; so each unsuccessful division takes as long as a successful one. We advocate finding the constant term of the quotient first, in the hope that it will not be in $(1/d)Z[\alpha]$. This way unsuccessful divisions would usually fail at the first step. We could even calculate the constant term of the trial factor, perform the preceding division, and then calculate the rest of the trial factor.

4. Another way to eliminate many divisions of trial factors is to use a value of M somewhat larger than necessary. Then we would expect most of the trial factors to have coefficients which are too large to be coefficients of actual factors.

5. The time complexity of algorithm K is clearly much like the complexity of algorithm Q, although all constants are larger. The principal contribution to the cases

which require long times to complete is step K5, where there may be very many trial factors. For instance, let $K = Q(\sqrt{p_1}, \ldots, \sqrt{p_n})$, where the p_i are the first n primes. Now suppose $K = Q(\alpha) = Q(\beta)$, and $F(T)$, $f(x)$ are the minimal polynomials of α, β, respectively. Then all $F_k^{(i)}(T)$ are quadratic or linear, and all $f_{ik}^{(i)}(x)$ are linear. Hence finding one of the linear factors of f requires around $m^{m/2}$ trial factors, where $m = \deg(F) = 2^n$.

6. There are two algebraic problems which can obviously be solved using this algorithm. The first problem is to determine when one of two algebraic number fields is contained in the other. Suppose $K = \mathbf{Q}(\alpha)$, where $F(T)$ is the minimal polynomial of α, and suppose $L = \mathbf{Q}(\beta)$, where $f(x)$ is the minimal polynomial of β. A necessary condition that $L \subset K$ is $\deg f(x) \mid \deg F(T)$. K contains L exactly when $f(x)$ has a linear factor when factored over K, for $\beta = g(\alpha)$ for some polynomial g with integral coefficients exactly when $x - g(\alpha)$ is a factor of $f(x)$. Zassenhaus and Liang [6] give an example using an algorithm much like ours for a special case.

The second problem is to determine if K is normal. In this case the algorithm is applied with $f(x) = F(x)$. K is normal exactly when all the conjugates of α lie in K, and this is equivalent to $f(x)$ having only linear factors. Further, if $f(x) = \prod_{i=1}^{n}(x - g_i(\alpha))$, $g_1(\alpha) = \alpha$, then the elements of the Galois group can be taken to be the g_i, and the multiplication of the Galois group becomes the composition of the g_i. In particular, the group is Abelian if and only if $g_i(g_j(\alpha)) = g_j(g_i(\alpha))$ for all i, j. If K is normal, but not cyclic, step K5 will probably require a lot of time.

7. We briefly discuss the extension of our algorithm to polynomials in several variables. Musser's algorithm [3] goes through without essential difficulties. The following outline mentions the necessary changes. We are factoring $f_1 \in K[v_1, \ldots, v_s, x]$, where $\{v_i\}$, x are indeterminates.

Step MK0. Find coefficient bounds using Gelfond's inequality (as in [3]) and Lemma 8.3. Musser's height of a polynomial g must be replaced by $\| g \|$ as given in Section 8.

Step MK1. Remove multiple factors and factors of the form $h(v_1, \ldots, v_s)$ by greatest-common-divisor calculations.

Step MK2a. Same as step K2a.

Step MK2b. Same as step K2b.

Step MK2c. Find $a_1, \ldots, a_s \in K$ so that $f(x) = f_1(a_1, \ldots, a_s, x) \in K[x]$ is square free and has the same degree in x as $f_1(x)$. This is done by trial and error.

Step MK3. This step consists of steps K3a through K5. Now proceed exactly as in [3], except that Musser's single factorization mod $(p^j, (v_1 - a_1)^{j_1}, \ldots, (v_s - a_s)^{j_s})$ must be replaced by g factorizations mod $(p^j, F_k^{(j)}(\alpha), (v_1 - a_1)^{j_1}, \ldots, (v_s - a_s)^{j_s})$, $1 \leq k \leq g$, and the Chinese remainder theorem must be used to reconstruct the trial factors.

ACKNOWLEDGMENT

We are indebted to Joel Moses, who suggested this problem to each of us.

REFERENCES

1. Berlekamp, E. Factoring polynomials over large finite fields. *Math. Computation 24* (1970), 713–735.

2. KNUTH, D. *The Art of Computer Programming, Vol. 2.* Addison-Wesley, Reading, Mass., 1969.
3. MUSSER, D.R. Multivariate polynomial factorization. *J. ACM 22* (1975), 291–308.
4. NARKIEWICZ, W. *Elementary and Analytic Theory of Algebraic Numbers.* Panstwowe Wydawnictwo Naukowe, Warsaw, Poland, 1974.
5. ZASSENHAUS, H. On Hensel factorization, Part I. *J. Number Theory 1* (1969), 291–311.
6. ZASSENHAUS, H., AND LIANG, J. On a problem of Hasse. *Math. Computation 23* (1969), 515–519.
7. ZIMMER, H. *Computational Problems, Methods, and Results in Algebraic Number Theory.* Lecture Notes in Mathematics No. 262, Springer-Verlag, New York, 1972.

Received August 1974; revised October 1975