stichting
mathematisch
centrum

MC

AFDELING INFORMATICA
(DEPARTMENT OF COMPUTER SCIENCE)

IW 213/82 NOVEMBER

A.K. LENSTRA

FACTORING POLYNOMIALS OVER ALGEBRAIC NUMBER FIELDS

Preprint

kruislaan 413 1098 SJ amsterdam

Printed at the Mathematical Centre, 413 Kruislaan, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O.).

1980 Mathematics subject classification: 12A20, 68C25

1982 CR. Categories: F.2.1, I.1.2

Factoring polynomials over algebraic number fields [*)]

by

A.K. Lenstra

ABSTRACT

This paper describes a polynomial-time algorithm for the factorization of polynomials in one variable with coefficients in an algebraic number field. The algorithm generalizes the polynomial-time algorithm for the factorization of polynomials in one variable with rational coefficients.

KEY WORDS & PHRASES: *polynomial algorithm, polynomial factorization*

[*)] This report will be submitted for publication elsewhere.

Factoring polynomials over algebraic number fields.

In [8] a polynomial-time algorithm was given to factorize polynomials in one variable with rational coefficients. In this paper we generalize this result to polynomials in one variable with coefficients in an algebraic number field.

The existence of a polynomial-time algorithm for this problem is not surprising in view of [8]. According to Trager [12] the problem is reducible to the factorization of univariate polynomials with integral coefficients, and in [6] it is shown that this reduction is polynomial-time. Here we pursue a direct approach to the factorization of polynomials over algebraic number fields. As suggested in [7: Section 5] we regard the irreducible factor we are looking for as an element of a certain integral lattice, and we prove that it is the 'smallest' element in this lattice. As we have seen in [8] this enables us to effectively compute this factor by means of a basis reduction algorithm for lattices.

Section 1 contains some notation and definitions; furthermore we recall there some results from [8: Section 1]. Section 2 deals with the connection between factors and lattices. It generalizes the first part of [8: Section 2]. In Section 3 we give a global description of the factoring algorithm and we analyze its running time.

For a polynomial f we denote by δf the *degree* of f, by $\ell c(f)$ the *leading coefficient* of f, and f is said to be *monic* if $\ell c(f) = 1$.

1. Preliminaries.

Let the algebraic number field $\mathbb{Q}(\alpha)$ be given as the field of rational numbers $\mathbb{Q}$ extended by a root α of a prescribed monic irreducible polynomial $F \in \mathbb{Z}[T]$, i.e. $\mathbb{Q}(\alpha) \simeq \mathbb{Q}[T]/(F)$. This implies that the elements of $\mathbb{Q}(\alpha)$ can be represented as polynomials in α over $\mathbb{Q}$ of degree $< \delta F$. We may assume that the degree of the *minimal polynomial* F is at least 2.

Similarly, we define $\mathbb{Z}[\alpha] = \mathbb{Z}[T]/(F)$ as the ring of polynomials in α over $\mathbb{Z}$ of degree $< \delta F$, where multiplication is done 'modulo F'.

Let f be a monic polynomial in $\mathbb{Q}(\alpha)[X]$. In Section 3 we will describe how to choose a positive integer D such that

(1.1) f and all monic factors of f in $\mathbb{Q}(\alpha)[X]$ are in $\frac{1}{D}\mathbb{Z}[\alpha][X]$.

The algorithm to determine the irreducible factors of f in $\mathbb{Q}(\alpha)[X]$ that we will present, is very similar to the algorithm for factorization in $\mathbb{Z}[X]$ as described in [8]: first determine the factorization of f over some finite field ($\mathbb{Z}/p\mathbb{Z}$ in [8]), next extend this factorization to a factorization over a large enough ring ($\mathbb{Z}/p^k\mathbb{Z}$ in [8]), and finally use a lattice reduction algorithm to determine the factors over $\mathbb{Q}(\alpha)$. Therefore, we first describe how to choose this finite field and this ring.

Let p be a prime number such that

(1.2) p does not divide D,

and let k be a positive integer. For $G = \Sigma_i\, a_i T^i \in \mathbb{Z}[T]$ and some integer ℓ we denote by G_ℓ or $(G \bmod p^\ell)$ the polynomial $\Sigma_i (a_i \bmod p^\ell) T^i \in (\mathbb{Z}/p^\ell\mathbb{Z})[T]$. In Section 3 we will see that we are able to determine p

in such a way that we can compute a polynomial $H \in \mathbb{Z}[T]$ such that

(1.3) H is monic,

(1.4) H_k divides F_k in $(\mathbb{Z}/p^k\mathbb{Z})[T]$,

(1.5) H_1 is irreducible in $(\mathbb{Z}/p\mathbb{Z})[T]$,

(1.6) $(H_1)^2$ does not divide F_1 in $(\mathbb{Z}/p\mathbb{Z})[T]$.

It follows that H_1 divides F_1 in $(\mathbb{Z}/p\mathbb{Z})[T]$, and that $0 < \delta H \leq \delta F$.

This polynomial H, together with the prime number p and the integer k, gives us the possibility to construct the finite field and the ring we were looking for. We denote by q the prime-power $p^{\delta H}$ and by $\mathbb{F}_q$ the finite field containing q elements. From (1.5) we derive that $\mathbb{F}_q \simeq (\mathbb{Z}/p\mathbb{Z})[T]/(H_1)$. Remark that $\mathbb{F}_q \simeq \{\Sigma_{i=0}^{\delta H-1} a_i\alpha_1^i : a_i \in \mathbb{Z}/p\mathbb{Z}\}$ where $\alpha_1 = (T \bmod (H_1))$ is a zero of H_1. This enables us to represent the elements of $\mathbb{F}_q$ as polynomials in α_1 over $\mathbb{Z}/p\mathbb{Z}$ of degree $< \delta H$. The finite field $\mathbb{F}_q$ corresponds to $\mathbb{Z}/p\mathbb{Z}$ in [8]; we now define the ring which will play the role of $\mathbb{Z}/p^k\mathbb{Z}$ in [8]. Let $W_k(\mathbb{F}_q) = (\mathbb{Z}/p^k\mathbb{Z})[T]/(H_k)$ be a ring containing q^k elements. We have that $W_k(\mathbb{F}_q) = \{\Sigma_{i=0}^{\delta H-1} a_i\alpha_k^i : a_i \in \mathbb{Z}/p^k\mathbb{Z}\}$ where $\alpha_k = (T \bmod (H_k))$ is a zero of H_k. So elements of $W_k(\mathbb{F}_q)$ can be represented as polynomials in α_k over $\mathbb{Z}/p^k\mathbb{Z}$ of degree $< \delta H$, and $W_k(\mathbb{F}_q)$ can be mapped onto $\mathbb{F}_q$ by reducing the coefficients of these polynomials modulo p. For $a \in W_k(\mathbb{F}_q)[X]$ we denote by $(a \bmod p) \in \mathbb{F}_q[X]$ the result of applying this mapping coefficient-wise to a. Remark that $W_1(\mathbb{F}_q) \simeq \mathbb{F}_q$.

We now show how we map polynomials in $\frac{1}{D}\mathbb{Z}[\alpha][X]$ to polynomials in $\mathbb{F}_q[X]$ and $W_k(\mathbb{F}_q)[X]$ respectively. Clearly, the canonical mapping from

$\mathbb{Z}[T]/(F)$ to $(\mathbb{Z}/p^{\ell}\mathbb{Z})[T]/(H_{\ell})$ defines a mapping from $\mathbb{Z}[\alpha]$ to $W_{\ell}(\mathbb{F}_q)$, for $\ell = 1,k$. (Informally, this mapping works by reducing the polynomial in α modulo p^{ℓ} and $H_{\ell}(\alpha)$.) For $a \in \mathbb{Z}[\alpha]$ we denote by $(a \bmod (p^{\ell},H_{\ell})) \in W_{\ell}(\mathbb{F}_q)$ the result of this mapping. Finally, for $g = \Sigma_i \frac{a_i}{D} X^i \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ we denote by $(g \bmod (p^{\ell},H_{\ell}))$ the polynomial $\Sigma_i(((D^{-1} \bmod p^{\ell})a_i) \bmod (p^{\ell},H_{\ell}))X^i \in W_{\ell}(\mathbb{F}_q)[X]$. Notice that $D^{-1} \bmod p^{\ell}$ exists due to (1.2).

(1.7) We conclude this section with some results from [8: Section 1]. Let n be a positive integer, and let $b_1,b_2,\ldots,b_n \in \mathbb{R}^n$ be linearly independent. The *lattice* $L \subset \mathbb{R}^n$ of *rank* n spanned by $b_1,b_2,\ldots,b_n$ is defined as

$$L = \Sigma_{i=1}^{n} \mathbb{Z}\, b_i = \{\Sigma_{i=1}^{n} r_i b_i : r_i \in \mathbb{Z}\ (1 \le i \le n)\}.$$

We assume that the $n\times n$ matrix having $b_1,b_2,\ldots,b_n$ as columns is upper-triangular, i.e. the $(j+1)$-th up to the n-th coordinate of b_j is zero, for $1 \le j \le n$. This implies that we can regard the lattice L_j of rank j spanned by $b_1,b_2,\ldots,b_j$ as a lattice contained in $\mathbb{R}^j$, for $1 \le j \le n$; notice that $L = L_n$. Furthermore we assume that $b_1,b_2,\ldots,b_n \in (\frac{1}{D}\mathbb{Z})^n$, so that $L_j \subset (\frac{1}{D}\mathbb{Z})^j$.

Let $B \in \mathbb{Z}_{\ge 2}$ be chosen in such a way that $|Db_i|^2 \le B$ for $1 \le i \le n$, where $|\,|$ denotes the ordinary Euclidean length.

In [8: (1.15)] a *basis reduction algorithm* is given that transforms a basis $b_1,b_2,\ldots,b_j$ of a lattice L_j into a *reduced* basis $\tilde{b}_1,\tilde{b}_2,\ldots,\tilde{b}_j$ for L_j. We won't recall the definition of a reduced basis here [8: (1.4), (1.5)], it suffices to say that the first vector $\tilde{b}_1$ in such a reduced basis satisfies

(1.8) $|b_1|^2 \le 2^{j-1}|x_j|^2$

for every $x_j \in L_j$, $x_j \neq 0$ [8: (1.11)]. The number of arithmetic operations needed by the basis reduction algorithm is $O(j^4 \log B)$, and the integers on which these operations are performed each have binary length $O(j \log B)$ [8: (1.26)].

The first time that the vector b_j is considered during the computation of a reduced basis for L_j, is at the moment that a reduced basis for L_{j-1} is obtained already; i.e. the computation of a reduced basis for L_{j-1} constitutes the first part of the computation of a reduced basis for L_j [8: (1.37)].

It follows that we can find an approximation of the shortest vector in L_n in $O(n^4 \log B)$ operations on integers having binary length $O(n \log B)$, and as a byproduct of the computation we get approximations of the shortest vectors in the lattices L_j without any time loss. If the approximation of the shortest vector in L_j, for some j, satisfies our needs already, then we break off the computation as soon as we have found this approximation, and the computation then takes $O(j^4 \log B)$ operations on integers having binary length $O(j \log B)$.

2. Factors and lattices.

This section is similar to the first part of [8: Section 2]. We formulate the generalizations of [8: (2.5),(2.6),(2.7),(2.13)] to polynomials over algebraic number fields. Let f, D, p, k, F, and H be as in Section 1. We put $n = \delta f$; we may assume that $n > 0$.

Suppose that we are given a polynomial $h \in \mathbb{Z}[\alpha][X]$ such that

(2.1) h is monic,

(2.2) $(h \bmod (p^k, H_k))$ divides $(f \bmod (p^k, H_k))$ in $W_k(\mathbb{F}_q)[X]$,

(2.3) $(h \bmod (p, H_1))$ is irreducible in $\mathbb{F}_q[X]$,

(2.4) $(h \bmod (p, H_1))^2$ does not divide $(f \bmod (p, H_1))$ in $\mathbb{F}_q[X]$.

We put $\ell = \delta h$; so $0 < \ell \leq n$. In Section 3 we will see which extra conditions have to be imposed on p so that such a polynomial h can be determined.

(2.5) Proposition. *The polynomial* f *has a unique monic irreducible factor* h_0 *in* $\frac{1}{D}\mathbb{Z}[\alpha][X]$ *for which* $(h \bmod (p, H_1))$ *divides* $(h_0 \bmod (p, H_1))$ *in* $\mathbb{F}_q[X]$. *Further, if a monic polynomial* $g \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ *divides* f *in* $\mathbb{Q}(\alpha)[X]$, *then the following assertions are equivalent:*

(i) $(h \bmod (p, H_1))$ *divides* $(g \bmod (p, H_1))$ *in* $\mathbb{F}_q[X]$,

(ii) $(h \bmod (p^k, H_k))$ *divides* $(g \bmod (p^k, H_k))$ *in* $W_k(\mathbb{F}_q)[X]$,

(iii) h_0 *divides* g *in* $\mathbb{Q}(\alpha)[X]$.

In particular $(h \bmod (p^k, H_k))$ *divides* $(h_0 \bmod (p^k, H_k))$ *in* $W_k(\mathbb{F}_q)[X]$.

Proof. Use (1.1) and the proof of [8: (2.5)]. □

(2.6) In the remainder of this section we fix an integer m with $m \geq \ell$. We define L to be the collection of polynomials $g \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ such that:

(i) $\delta g \leq m$,

(ii) if $\delta g = m$, then $\ell c(g) \in \mathbb{Z}$,

(iii) $(h \bmod (p^k, H_k))$ divides $(g \bmod (p^k, H_k))$ in $W_k(\mathbb{F}_q)[X]$.

We identify such a polynomial $g = \Sigma_{i=0}^{m-1} \Sigma_{j=0}^{\delta F-1} a_{ij}\alpha^j X^i + a_{m0}X^m$ (where $a_{ij} \in \frac{\mathbb{Z}}{D}$) with the $(m\delta F+1)$-dimensional vector $(a_{00}, a_{01}, \ldots, a_{0\ \delta F-1}, a_{10}, \ldots,$

$a_{m-1\,\delta F-1}, a_{m0})$. Using this identification between vectors and polynomials, it is not difficult to see that L is a lattice in $\mathbb{R}^{m\delta F+1}$; from the fact that both H and h are monic ((1.3) and (2.1)) it follows that a basis for L is given by

$$\{\frac{1}{D}\, p^k\alpha^j X^i \;:\; 0 \le j < \delta H,\;\; 0 \le i < \ell\} \;\cup$$

$$\{\frac{1}{D}\, \alpha^{j-\delta H} H(\alpha)X^i \;:\; \delta H \le j < \delta F,\;\; 0 \le i < \ell\} \;\cup$$

$$\{\frac{1}{D}\, \alpha^j h X^{i-\ell} \;:\; 0 \le j < \delta F,\;\; \ell \le i < m\} \;\cup$$

$$\{hX^{m-\ell}\}.$$

Notice that the matrix having these vectors as columns is upper-triangular.

We define the *length* $|g|$ of g as the ordinary Euclidean length of the vector identified with g, so $|g| = (\Sigma_{i=0}^{m-1}\, \Sigma_{j=0}^{\delta F-1} |a_{ij}|^2 + |a_{m0}|^2)^{\frac{1}{2}}$; the *height* $g_{\max}$ of g is defined as $\max\{|a_{ij}|\}$. Similarly we define the length and the height of polynomials in $\mathbb{Z}[T]$.

(2.7) Proposition. *Let* $b \in L$ *satisfy*

$$p^{k\ell\delta H/\delta F} > \left(Df_{\max}((n+1)\delta F(1+F_{\max})^{\delta F-1})^{\frac{1}{2}}\right)^m \cdot \left(Db_{\max}((m+1)\delta F(1+F_{\max})^{\delta F-1})^{\frac{1}{2}}\right)^n . \tag{2.8}$$

Then b *is divisible by* h_0 *in* $\mathbb{Q}(\alpha)[X]$, *where* h_0 *is as in* (2.5). *In particular* $\gcd(f,b) \ne 1$.

The proof of this proposition is very similar to the proof of [8: (2.7)]; we therefore omit the details

Proof. Put $g = \gcd(f,b)$, and $e = \delta g$. We may assume that g is monic. Identify the polynomials

$$(2.9) \qquad \{\alpha^j X^i f : 0 \le j < \delta F,\ 0 \le i < \delta b - e\} \cup \{\alpha^j X^i b : 0 \le j < \delta F,\ 0 \le i < n-e\}$$

with $(\delta F(n+\delta b-e))$-dimensional vectors. The projections of these vectors on $\frac{1}{D}\mathbb{Z}X^e + \frac{1}{D}\mathbb{Z}\alpha X^e + \ldots + \frac{1}{D}\mathbb{Z}\alpha^{\delta F-1}X^e + \frac{1}{D}\mathbb{Z}X^{e+1} + \ldots + \frac{1}{D}\mathbb{Z}\alpha^{\delta F-1}X^{n+\delta b-e-1}$ form a basis for a $(\delta F(n+\delta b-2e))$-dimensional lattice M'. Using induction on j one proves that

$$(\alpha^j X^i f)_{\max} = (\alpha^j f)_{\max} \le f_{\max}(1+F_{\max})^j,$$

so that, for $0 \le j < \delta F$ and $0 \le i < \delta b - e$,

$$|\alpha^j X^i f| \le f_{\max}\sqrt{(n+1)\delta F}\,(1+F_{\max})^j.$$

With Hadamard's inequality, and a similar bound on $|\alpha^j X^i b|$ we get

$$d(M')^{1/\delta F} \le \left(f_{\max}((n+1)\delta F(1+F_{\max})^{\delta F-1})^{\frac{1}{2}}\right)^m \cdot \left(b_{\max}((m+1)\delta F(1+F_{\max})^{\delta F-1})^{\frac{1}{2}}\right)^n,$$

where $d(M')$ denotes the determinant of M'. With (2.8) this gives

$$(2.10) \qquad d(M') < \frac{p^{k\ell\delta H}}{D^{(n+m)\delta F}}.$$

Assume that $(h \bmod (p,H_1))$ does not divide $(g \bmod (p,H_1))$ in $\mathbb{F}_q[X]$. By Proposition (2.5) it is sufficient to derive a contradiction from this. Let $v \in \frac{1}{D}\mathbb{Z}[\alpha][X]$ be some integral linear combination of the polynomials in (2.9) such that $\delta v < e+\ell$. As in the proof of [8: (2.7)] it follows from our assumption that $(v \bmod (p^k,H_k)) = 0$ in $W_k(\mathbb{F}_q)[X]$. Therefore, if we regard $\ell c(v)$ as a polynomial in α, we have

(2.11) $\ell c(\ell c(v)) \equiv 0$ modulo p^k if $\delta \ell c(v) < \delta H$.

Now choose a basis $b_{e0}, b_{e1}, \ldots, b_{e\ \delta F-1}, b_{e+1\ 0}, \ldots, b_{n+\delta b-e-1\ \delta F-1}$ for M' such that $\delta b_{ij} = i$ and $\delta \ell c(b_{ij}) = j$ for $e \le i < n+\delta b-e$ and $0 \le j < \delta F$, where $\ell c(b_{ij})$ is regarded as a polynomial in α. From (2.11) we derive that

$$\ell c(\ell c(b_{ij})) \equiv 0 \text{ modulo } p^k \text{ for } 0 \le j < \delta H \text{ and } e \le i < e+\ell.$$

Since $\ell c(\ell c(b_{ij})) \in \frac{\mathbb{Z}}{D}$, we obtain

$$|\ell c(\ell c(b_{ij}))| \ge \frac{p^k}{D} \text{ for } 0 \le j < \delta H \text{ and } e \le i < e+\ell$$

and

$$|\ell c(\ell c(b_{ij}))| \ge \frac{1}{D} \text{ for } \delta H \le j < \delta F \text{ or } e+\ell \le i < n+\delta b-e.$$

The determinant of M' equals the product of $|\ell c(\ell c(b_{ij}))|$, so that

$$d(M') \ge \frac{p^{k\ell\delta H}}{D^{(n+\delta b-2e)\delta F}} \ge \frac{p^{k\ell\delta H}}{D^{(n+m)\delta F}} .$$

Combined with (2.10) this is the desired contradiction. □

(2.12) To be able to formulate the generalization of [8: (2.13)] we need an upper bound on the length of monic factors of f in $\frac{1}{D}\mathbb{Z}[\alpha][X]$. In Section 4 (4.8) we prove that a monic factor of degree $\le m$ has length at most

$$f_{\max}\left(2(n+1)\delta F^3(\delta F-1)^{\delta F-1}\binom{2m}{m}\right)^{\frac{1}{2}} |F|^{2(\delta F-1)} |\mathrm{discr}(F)|^{-\frac{1}{2}},$$

where $\mathrm{discr}(F)$ denotes the discriminant of F (so $\mathrm{discr}(F) \ne 0$, since F is an irreducible polynomial in $\mathbb{Z}[T]$).

(2.13) Proposition. *Suppose that* $\bar{b}_1, \bar{b}_2, \ldots, \bar{b}_{m\delta F+1}$ *is a reduced basis for* L *(see* (1.7)*), and that*

$$(2.14) \qquad p^{k\ell\delta H/\delta F} > \Big(2^{n(m\delta F+1)}(n+1)^{n+m}(m+1)^n\binom{2m}{m}^n \delta F^{4n+m}(\delta F-1)^{n(\delta F-1)} (1+F_{\max})^{(n+m)(\delta F-1)}|\mathrm{discr}(F)|^{-n}\Big)^{\frac{1}{2}}\cdot(Df_{\max})^{n+m}|F|^{2n(\delta F-1)}.$$

Then we have $\delta h_0 \leq m$ *if and only if* (2.8) *is satisfied with* b *replaced by* $\bar{b}_1$.

Proof. Use (2.12), (1.8), and the proof of [8: (2.13)]. □

3. Description of the algorithm.

Let f be a polynomial in $\mathbb{Q}(\alpha)[X]$ of degree n, with $n > 0$. We describe an algorithm to compute the irreducible factors of f in $\mathbb{Q}(\alpha)[X]$.

For the moment we assume that f is monic. If D, p, H, and h are chosen in such a way that the conditions in Sections 1 and 2 are satisfied, then we can determine the factor h_0 of f by means of Propositions (2.7) and (2.13); this is described in more detail in Algorithm (3.1). After that, we explain in (3.4) how we choose D, p, H, and h, and we analyze the running time of the resulting factorization algorithm.

(3.1) Suppose that a positive integer D, a prime number p, and polynomials $H \in \mathbb{Z}[T]$ and $h \in \mathbb{Z}[\alpha][X]$ are given such that (1.1), (1.2), (1.3), (1.5), (1.6), (2.1), (2.3), and (2.4), and (1.4) and (2.2) with k replaced by 1, are satisfied. We describe an algorithm that determines h_0, the monic irreducible factor of f for which $(h \bmod (p,H_1))$ divides $(h_0 \bmod (p,H_1))$, cf. (2.5).

Put $\ell = \delta h$; we may assume that $\ell < n$. We calculate the least positive integer k for which (2.14) holds with m replaced by $n-1$:

$$(3.2) \qquad p^{k\ell\delta H/\delta F} > \Big(2^{n((n-1)\delta F+1)}(n+1)^{2n-1}\, n^{n}\tbinom{2(n-1)}{n-1}^{n}\delta F^{5n-1}(\delta F-1)^{n(\delta F-1)}$$
$$(1+F_{\max})^{(2n-1)(\delta F-1)}|\mathrm{discr}(F)|^{-n}\Big)^{\frac{1}{2}}\cdot(Df_{\max})^{2n-1}|F|^{2n(\delta F-1)}.$$

Next we modify H in such a way that (1.4) holds for the value of k just calculated. The factor $H_k = (H \bmod p^k)$ of $(F \bmod p^k)$ gives us the possibility to compute in $W_k(\mathbb{F}_q)$. Therefore we now modify h, without changing $(h \bmod(p,H_1))$ in such a way that (2.2) holds for the above value of k. The computations of the new H and h can both be done by means of Hensel's lemma [5: exercise 4.6.22; 14; 13]; notice that Hensel's lemma can be applied because of (1.6) and (2.4).

Now apply the basis reduction algorithm [8: (1.15)] to the $(m\delta F+1)$-dimensional lattice L as defined in (2.6), for each of the values $m = \ell, \ell+1,\ldots,n-1$ in succession; but we stop as soon as for one of these values of m we find a basis $\breve{b}_1,\breve{b}_2,\ldots,\breve{b}_{m\delta F+1}$ for L such that (2.8) is satisfied with b replaced by $\breve{b}_1$. If such a basis is found for a certain value m_0 of m, then we know from (2.13) that $\delta h_0 \le m_0$. Since we try the values $m = \ell,\ell+1,\ldots,n-1$ in succession we also know from (2.13) that $\delta h_0 > m_0-1$, so $\delta h_0 = m_0$. By (2.7) the polynomial h_0 divides $\breve{b}_1$ in $\mathbb{Q}(\alpha)[X]$ which implies, together with $\delta\breve{b}_1 \le m_0$, that $\delta\breve{b}_1 = m_0$. From (2.6)(ii) and from the fact that h_0 is monic we find that $\breve{b}_1 = ch_0$, for some constant $c \in \mathbb{Z}$. Using that $h_0 \in L$ and that $\breve{b}_1$ belongs to a basis for L, we conclude that $c = \pm 1$, so that $\breve{b}_1 = \pm h_0$.

If on the other hand we did not find such a basis for L, then we know from (2.13) that $\delta h_0 > n-1$. This implies that $h_0 = f$. This finishes the description of Algorithm (3.1).

(3.3) Proposition. *Denote by* $m_0 = \delta h_0$ *the degree of the irreducible factor* h_0 *of* f *that is found by Algorithm* (3.1). *Then the number of arithmetic operations needed by Algorithm* (3.1) *is* $O(m_0(n^5\delta F^6 + n^4\delta F^6 \log(\delta F|F|) + n^4\delta F^5 \log(Df_{max}) + n^3\delta F^4 \log p))$ *and the integers on which these operations are performed each have binary length* $O(n^3\delta F^3 + n^2\delta F^3 \log(\delta F|F|) + n^2\delta F^2 \log(Df_{max}) + n\delta F \log p)$.

Proof. Let m_1 be the largest value of m for which the basis reduction algorithm is performed, so $m_1 = m_0$ or $m_1 = m_0-1$. From (1.7) it follows that during the computation of the reduced basis for the $(m_1\delta F+1)$-dimensional lattice, also reduced bases were obtained for the $(m\delta F+1)$-dimensional lattices, for $\ell \leq m < m_1$. Therefore the number of arithmetic operations needed for the applications of the basis reduction algorithm is $O((m_1\delta F)^4 \log B)$, and the integers on which these operations are performed each have binary length $O(m_1\delta F \log B)$, where B bounds the length of the vectors in the initial basis for L (cf. (2.6)). Assuming that the coefficients of the initial basis are reduced modulo p^k, we derive from (3.2), $|\mathrm{discr}(F)| \geq 1$, $\delta H \geq 1$, and $\ell \geq 1$ that

$$\log B = O(n^2\delta F^2 + n\delta F^2 \log(\delta F|F|) + n\delta F \log(Df_{max}) + \log p).$$

Combined with $m_1 = O(m_0)$ this yields the estimates given in (3.3).

It is straightforward to verify that the same estimates are valid for both applications of Hensel's lemma and for the computation of $\mathrm{discr}(F)$.

□

(3.4) We now describe how to choose D, p, H, and h in such a way that Algorithm (3.1) can be applied. The algorithm to factor f into its monic irreducible factors in $\mathbb{Q}(\alpha)[X]$ then easily follows.

First we choose a positive integer D such that (1.1) holds, i.e. f and all monic factors of f in $\mathbb{Q}(\alpha)[X]$ are in $\frac{1}{D}\mathbb{Z}[\alpha][X]$. From [14] it follows that we can take $D = dc$, where d is such that $f \in \frac{1}{d}\mathbb{Z}[\alpha][X]$, and c is the largest integer such that c^2 divides $\operatorname{discr}(F)$. This integer c however might be difficult to compute; therefore we take $D = d\,|\operatorname{discr}(F)|$ as denominator, which clearly also suffices.

We may assume that the resultant $R(f,f') \in \mathbb{Q}(\alpha)$ of f and its derivative f' is unequal to zero, i.e. f has no multiple factors in $\mathbb{Q}(\alpha)[X]$. We apply the algorithm from [10] to determine p as the smallest prime number not dividing $D\cdot\operatorname{discr}(F)\cdot R(f,f')$; so (1.2) is satisfied.

Using Berlekamp's algorithm [5: Section 4.6.2] we compute the irreducible factorization $(F \bmod p) = \Pi_{i=1}^{t} (G_i \bmod p)$ of $(F \bmod p)$ in $(\mathbb{Z}/p\,\mathbb{Z})[T]$. This factorization does not contain multiple factors because $\operatorname{discr}(F) \not\equiv 0$ modulo p. Combined with $R(f,f') \not\equiv 0$ modulo p this implies that there exists an integer $i_0 \in \{1,2,\ldots,t\}$ such that

$$(R(f,f') \bmod (p,(G_{i_0} \bmod p))) \neq 0;$$

Let H be such a polynomial G_{i_0}. We may assume that H is monic, so that (1.3), (1.5), (1.6), and (1.4) with k replaced by 1 are satisfied.

Next we determine the irreducible factorization of $(f \bmod (p,H_1))$ in $\mathbb{F}_q[X]$ by means of Berlekamp's algorithm [2: Section 5], where $q = p^{\delta H}$ and $\mathbb{F}_q \simeq (\mathbb{Z}/p\,\mathbb{Z})[T]/(H \bmod p)$. (Notice that we use a modified version of Berlekamp's algorithm here, one that is polynomial-time in p and δH rather than polynomial-time in the number of elements of the finite field.)

Since f is monic the resultant $R(f,f')$ is, up to sign, equal to the discriminant of f, so that it follows from the construction of H that the discriminant of f is unequal to zero in $\mathbb{F}_q$. Therefore (2.4) holds for all irreducible factors $(h \bmod (p,H_1))$ of $(f \bmod (p,H_1))$ in $\mathbb{F}_q[X]$; we may assume that these factors are monic.

The algorithm to factorize f now follows by repeated application of Algorithm (3.1).

(3.5) Proposition. *The algorithm sketched above computes the irreducible factorization of any monic polynomial* $f \in \frac{1}{d}\mathbb{Z}[\alpha][X]$ *of degree* $n > 0$. *The number of arithmetic operations needed by the algorithm is* $O(n^6\delta F^6 + n^5\delta F^6\log(\delta F|F|) + n^5\delta F^5\log(df_{max}))$, *and the integers on which these operations are performed each have binary length* $O(n^3\delta F^3 + n^2\delta F^3\log(\delta F|F|) + n^2\delta F^2\log(df_{max}))$.

Proof. It follows from [3] that the calculations of $R(f,f')$ and $\mathrm{discr}(F)$ satisfy the above estimates. From Hadamard's inequality we obtain

$$|\mathrm{discr}(F)| \le \delta F^{\delta F}|F|^{2\delta F-1};$$

it follows that

$$\log D = O(\log d + \delta F \log(\delta F|F|)).$$

Let A be a matrix having entries $A_{ij} = \Sigma_{\ell=0}^{\delta F-1} a_{ij\ell}T^{\ell} \in \mathbb{Z}[T]$, for $1 \le i,j \le m$, and some positive integer m. The determinant $d(A)$ of A is a polynomial of degree $\le m(\delta F-1)$ in $\mathbb{Z}[T]$. According to [4] the length, and therefore the height, of $d(A)$ is bounded from above by

$$\left(\Pi_{j=1}^{m} \Sigma_{i=1}^{m} (\Sigma_{\ell=0}^{\delta F-1}|a_{ij\ell}|)^2\right)^{\frac{1}{2}}.$$

Using this bound it is easily proven that the height of $d(A)$ modulo F is bounded by

$$\left(\Pi_{j=1}^{m} \Sigma_{i=1}^{m} (\Sigma_{\ell=0}^{\delta F-1} |a_{ij\ell}|)^2\right)^{\frac{1}{2}} (1+F_{\max})^{(m-1)(\delta F-1)}.$$

It follows that

$$(R(f,f'))_{\max} \leq (\sqrt{n+1}\delta F f_{\max})^{n-1} (\sqrt{n}\delta F n f_{\max})^{n} (1+F_{\max})^{(2n-2)(\delta F-1)},$$

where $R(f,f')$ is regarded as a polynomial in α. We find from the definitions of D and p that

$$\Pi_{q \text{ prime}, q < p}\, q \leq d \cdot \text{discr}(F) \cdot (R(df,df'))_{\max}$$

and this yields in a similar way as in [8] that

$$p = O(\log d + n\delta F \log(\delta F|F|) + n \log n + n \log(df_{\max})).$$

This implies that the computation of the prime number p, and the computation of the factorizations of $(F \bmod p)$ in $(\mathbb{Z}/p\mathbb{Z})[T]$ and $(f \bmod (p,H_1))$ in $\mathbf{F}_q[X]$ satisfy the estimates in (3.5). Proposition (3.5) now easily follows from the bounds on $\log D$ and p, and from the observation that a monic factor g of f in $\mathbb{Q}(\alpha)[X]$ satisfies $\log(g_{\max}) = O(\delta F \log(\delta F|F|) + n + \log(f_{\max}))$ (see (4.7)). □

(3.6) We now drop the assumption that f is monic, so let f be a polynomial of degree $n > 0$ in $\mathbb{Z}[\alpha][X]$. We show that there exists a monic polynomial $\tilde{f} = \ell c(f)^{-1} f \in \frac{1}{d}\mathbb{Z}[\alpha][X]$, such that $\log(d\tilde{f}_{\max}) = O(\delta F \log(\delta F|F|) + \delta F \log(f_{\max}))$, for some non-zero integer d.

Denote by $C(\alpha) = \Sigma_{i=0}^{\delta F-1} C_i \alpha^i \in \mathbb{Z}[\alpha]$ the leading coefficient of f. The resultant $R(C,F) \in \mathbb{Z}$ of C and F is defined as the determinant of the following matrix:

$$\begin{array}{cc}
\left(\begin{matrix}
C_0 & 0 & \cdots & 0\\
\vdots & \ddots & & \vdots\\
\vdots & & \ddots & 0\\
C_{\delta F-1} & & & C_0\\
0 & \ddots & & \vdots\\
\vdots & & \ddots & \vdots\\
0 & \cdots & 0 & C_{\delta F-1}
\end{matrix}\right.
&
\left.\begin{matrix}
F_0 & 0 & \cdots & 0\\
\vdots & \ddots & & \vdots\\
\vdots & & \ddots & 0\\
\vdots & & & F_0\\
F_{\delta F} & & & \vdots\\
0 & \ddots & & \vdots\\
0 & \cdots & 0 & F_{\delta F}
\end{matrix}\right)
\\
\longleftarrow \delta F \longrightarrow & \longleftarrow \delta F-1 \longrightarrow
\end{array}$$

where $F(T) = \Sigma_{i=0}^{\delta F} F_i T^i$. We add, for $2 \le i \le 2\delta F-1$, the i-th row times T^{i-1} to the first row, so that the first row of the matrix becomes $(C(T), TC(T), \ldots, T^{\delta F-1}C(T), F(T), TF(T), \ldots, T^{\delta F-2}F(T))$. Expanding the determinant of the resulting matrix with respect to the first row gives

$$R(C,F) = C(T)\cdot(R_{\delta F-1}T^{\delta F-1}+\ldots+R_1T+R_0) + F(T)\cdot(S_{\delta F-2}T^{\delta F-2}+\ldots+S_1T+S_0),$$

where $R_i, S_j \in \mathbb{Z}$ for $0 \le i < \delta F$ and $0 \le j < \delta F-1$.

The values R_i and S_j are determinants of $(2\delta F-2)\times(2\delta F-2)$ submatrices of the above matrix, and therefore, using Hadamard's inequality, $|R_i|$ and $|S_j|$ are both bounded from above by

$$(\sqrt{\delta F}|F|f_{\max})^{\delta F}.$$

The evaluation of these determinants can be done by means of the methods described in [1]. Putting $R(T) = \Sigma_{i=0}^{\delta F-1} R_i T^i$ and $d = R(C,F)$ we find that $C(T)R(T) \equiv d \bmod F(T)$, so that $\frac{R(\alpha)}{d} \in \frac{1}{d}\mathbb{Z}[\alpha]$ is the inverse of $C(\alpha)$. Now use Hadamard's inequality to derive an upper bound for d, and we find that the monic polynomial $\tilde{f} = \frac{R(\alpha)}{d} f \in \frac{1}{d}\mathbb{Z}[\alpha][X]$ satisfies the estimates given above.

(3.7) Theorem. *Let* f *be a polynomial of degree* $n > 0$ *in* $\mathbb{Z}[\alpha][X]$. *The irreducible factorization of* f *in* $\mathbb{Q}(\alpha)[X]$ *can be computed in* $O(\delta F^6(n^6 + n^5\log(\delta F|F|) + n^5\log(f_{\max})))$ *arithmetic operations on integers having binary length* $O(\delta F^3(n^3 + n^2\log(\delta F|F|) + n^2\log(f_{\max})))$.

Proof. The proof follows from (3.6) and (3.5). □

4. Coefficient bound for factors.

We use the method sketched in [14] to derive an explicit upper bound for the height and the length of a monic divisor of a monic polynomial in $\mathbb{Q}(\alpha)[X]$.

For polynomials in $\mathbb{Q}(\alpha)[X]$ the height and the length are defined as in (2.6); for a polynomial $g = \Sigma_i c_i X^i \in \mathbb{C}[X]$, where $\mathbb{C}$ denotes the complex numbers, the length $|g|$ is defined as $(\Sigma_i |c_i|^2)^{\frac{1}{2}}$.

Let $\alpha_1,\alpha_2,\ldots,\alpha_{\delta F}$ denote the conjugates of α, i.e. $\alpha_1,\alpha_2,\ldots,\alpha_{\delta F} \in \mathbb{C}$ are the roots of the minimal polynomial F. For an element $\beta = \Sigma_{i=0}^{\delta F-1} b_i\alpha^i \in \mathbb{Q}(\alpha)$ the conjugates of β are defined as $\Sigma_{i=0}^{\delta F-1} b_i\alpha_j^i$ for $1 \le j \le \delta F$. We define $\|\beta\| \in \mathbb{R}$ as the largest absolute value of any of the conjugates of β; so $\|\alpha\|$ is the largest absolute value of any of the roots of F.

For any choice of $\alpha \in \{\alpha_1,\alpha_2,\ldots,\alpha_{\delta F}\}$ a polynomial $g \in \mathbb{Q}(\alpha)[X]$ can be regarded as a polynomial $\Sigma_{i=0}^{\delta g} c_{ji}X^i \in \mathbb{C}[X]$; we define $\|g\|$ as $\max_{1 \le j \le \delta F} \{|\Sigma_{i=0}^{\delta g} c_{ji}X^i|\}$.

Now let $f \in \mathbb{Q}(\alpha)[X]$ be a monic polynomial of degree n, and let $g = \Sigma_{i=0}^{m} g_iX^i \in \mathbb{Q}(\alpha)[X]$ be a monic factor of degree m of f. Since both f and g are monic, we obtain from [9] that

(4.1) $\|g_i\| \leq \binom{m}{i} \| f \|$, for $0 \leq i \leq m$.

From (4.1) we will derive bounds on the height and the length of g.

Let $S = (s_{ij})_{i,j=0}^{\delta F-1}$ be the $\delta F \times \delta F$ matrix with $s_{ij} = \alpha_{j+1}^{i}$. Since S is a Vandermonde matrix and because the roots of F are distinct, it follows that S is invertible, and that the absolute value of the determinant of S equals $|\mathrm{discr}(F)|^{\frac{1}{2}}$. We denote by $T = (t_{ij})_{i,j=0}^{\delta F-1}$ the matrix S^{-1}, and by $|T| = \max\{\Sigma_{i=0}^{\delta F-1} |t_{ij}| : 0 \leq j < \delta F\}$ (this is the L_∞-norm for matrices).

Let $r_j \in \mathbb{C}$ be the conjugates of $g_i = \Sigma_{k=0}^{\delta F-1} g_{ik}\alpha^k \in \mathbb{Q}(\alpha)$, for $1 \leq j \leq \delta F$, then we have

$$(g_{i0}, g_{i1}, \ldots, g_{i\,\delta F-1}) \cdot S = (r_1, r_2, \ldots, r_{\delta F}),$$

and therefore

(4.2) $$(g_{i0}, g_{i1}, \ldots, g_{i\,\delta F-1}) = (r_1, r_2, \ldots, r_{\delta F}) \cdot T$$

for $0 \leq i \leq m$. From (4.1) we have that

$$|r_j| \leq \binom{m}{i} \| f \| \quad \text{for} \quad 1 \leq j \leq \delta F$$

and this gives, combined with (4.2),

$$|g_{ik}| \leq \binom{m}{i} |T| \ \| f \| \quad \text{for} \quad 1 \leq k < \delta F \quad \text{and} \quad 0 \leq i \leq m.$$

This implies that

(4.3) $$g_{\max} \leq \binom{m}{m/2} |T| \ \| f \| ,$$

and

$$(4.4)\qquad |g| = (\Sigma_{i=0}^{m} \Sigma_{k=0}^{\delta F-1} g_{ik}^{2})^{\frac{1}{2}} \le \left(\delta F \Sigma_{i=0}^{m} \binom{m}{i}^{2}\right)^{\frac{1}{2}} |T| \;\|f\|$$

$$= \left(\delta F \binom{2m}{m}\right)^{\frac{1}{2}} |T| \;\|f\|.$$

It remains to give upper bounds for $|T|$ and $\|f\|$.

The entries of T are determinants of $(\delta F-1)\times(\delta F-1)$ submatrices of S, divided by $|\mathrm{discr}(F)|^{\frac{1}{2}}$. Using Hadamard's inequality we get the upper bound

$$\Pi_{j=1}^{\delta F-1} (\Sigma_{i=1}^{\delta F-1} |\alpha_j|^{2i})^{\frac{1}{2}}$$

for the determinant of such a $(\delta F-1)\times(\delta F-1)$ submatrix of S. This easily yields the bound

$$\Pi_{|\alpha_j| \le 1} (\delta F-1)^{\frac{1}{2}} \cdot \Pi_{|\alpha_j| > 1} (\delta F-1)^{\frac{1}{2}} |\alpha_j|^{\delta F-1}$$

$$= (\delta F-1)^{(\delta F-1)/2} (\Pi_{|\alpha_j| > 1} |\alpha_j|)^{\delta F-1}$$

Since F is monic we know from [9: Theorem 2] that $\Pi_{|\alpha_j| > 1} |\alpha_j| \le |F|$, so that we arrive at the bound

$$(\delta F-1)^{(\delta F-1)/2} |F|^{\delta F-1} |\mathrm{discr}(F)|^{-\frac{1}{2}}$$

for the absolute values of the entries of T. It follows that

$$(4.5)\qquad |T| \le \delta F(\delta F-1)^{(\delta F-1)/2} |F|^{\delta F-1} |\mathrm{discr}(F)|^{-\frac{1}{2}}.$$

A straightforward computation yields the bound

$$\|f\| \le \max_{1 \le j \le \delta F} (\Sigma_{i=0}^{n} f_{\max}^{2} \Sigma_{k=0}^{\delta F-1} |\alpha_j|^{2k})^{\frac{1}{2}}$$

$$\le \sqrt{n+1}\,(\Sigma_{k=0}^{\delta F-1} \|\alpha\|^{2k})^{\frac{1}{2}} f_{\max}.$$

There are several easily calculated upper bounds for $\|\alpha\|$, for instance $\|\alpha\| \leq 1 + F_{\max}$ and $\|\alpha\| \leq |F|$ (cf. [11]). For simplicity we take $\|\alpha\| \leq |F|$, so that we obtain

$$(4.6)\qquad \|f\| \leq \sqrt{n+1}\,(\Sigma_{k=0}^{\delta F-1}|F|^{2k})^{\frac{1}{2}} f_{\max} = \sqrt{n+1}\left(\frac{|F|^{2\delta F}-1}{|F|^{2}-1}\right)^{\frac{1}{2}} f_{\max}$$
$$\leq \sqrt{n+1}\left(\frac{|F|^{2\delta F}}{\frac{1}{2}|F|^{2}}\right)^{\frac{1}{2}} f_{\max} = \sqrt{n+1}\sqrt{2}\,|F|^{\delta F-1} f_{\max}.$$

Combining (4.3), (4.4), (4.5), and (4.6) we finally get

$$(4.7)\qquad g_{\max} \leq f_{\max}\left(2(n+1)(\delta F-1)^{\delta F-1}\right)^{\frac{1}{2}} |F|^{2(\delta F-1)}\,\delta F\binom{m}{m/2}|\mathrm{discr}(F)|^{-\frac{1}{2}}$$

and

$$(4.8)\qquad |g| \leq f_{\max}\left(2(n+1)\delta F^{3}(\delta F-1)^{\delta F-1}\binom{2m}{m}\right)^{\frac{1}{2}} |F|^{2(\delta F-1)}|\mathrm{discr}(F)|^{-\frac{1}{2}}.$$

Acknowledgements.

Acknowledgements are due to H.W. Lenstra, Jr. and P. van Emde Boas for several helpful remarks.

References.

1. E.H. Bareiss, Sylvester's identity and multistep integer-preserving Gaussian elimination, Math. Comp. 22 (1968), 565-578.
2. E.R. Berlekamp, Factoring polynomials over large finite fields, Math. Comp. 24 (1970), 713-735.
3. W.S. Brown, The subresultant PRS algorithm, ACM Transactions on mathematical software 4 (1978), 237-249.
4. A.J. Goldstein, R.L. Graham, A Hadamard-type bound on the coefficients of a determinant of polynomials, SIAM Rev. 16 (1974), 394-395.

5. D.E. Knuth, The art of computer programming, vol. 2, Seminumerical algorithms, Addison-Wesley, Reading, second edition 1981.

6. S. Landau, Factoring polynomials over algebraic number fields is in polynomial time, unpublished manuscript.

7. A.K. Lenstra, Lattices and factorization of polynomials over algebraic number fields, Proceedings Eurocam 82, LNCS 144, 32-39.

8. A.K. Lenstra, H.W. Lenstra, Jr., L. Lovász, Factoring polynomials with rational coefficients, Report IW 195/82, Mathematisch Centrum, Amsterdam 1982.

9. M. Mignotte, An inequality about factors of polynomials, Math. Comp. 28 (1974), 1153-1157.

10. P. Pritchard, A sublinear additive sieve for finding prime numbers, Comm. ACM 24 (1981), 18-23.

11. J. Stoer, Einführung in die numerische Mathematik I, Springer, Berlin 1972.

12. B.M. Trager, Algebraic factoring and rational function integration, Proceedings of the 1976 ACM symposium on symbolic and algebraic computation, 219-226.

13. P.S. Wang, Factoring multivariate polynomials over algebraic number fields, Math. Comp. 30 (1976), 324-336.

14. P.J. Weinberger, L.P. Rothschild, Factoring polynomials over algebraic number fields, ACM Transactions on mathematical software 2 (1976), 335-350.

15. D.Y.Y. Yun, The Hensel lemma in algebraic manipulation, MIT, Cambridge 1974; reprint: Garland Publ. Co., New York 1980.